# Avaya Proactive Outreach Manager Port Matrix

Release 4.0.0
Issue 1.0.1
December 21, 2020

### Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

### Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

### Link disclaimer

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

### Warranty

Avaya provides a limited warranty on Avaya hardware and software. 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if 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.

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

### Hosted Service

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

YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

### License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose. 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.

### Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” 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 as set forth below in the Designated System(s) License (DS) section as applicable. 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 computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) 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.

### Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

### 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

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

### Third Party Components

“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 products, Documentation or on Avaya’s website at: https:// support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

### Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE

OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

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

### Compliance with Laws

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

### Preventing Toll Fraud

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

### Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, 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: https://support.avaya.com or such successor site as designated by Avaya.

### Security Vulnerabilities

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

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

### Downloading Documentation

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

### Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or 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: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

### Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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.

Java is a registered trademark of Oracle and/or its affiliates.

# 1. Proactive Outreach Manager Components

Data flows and their sockets are owned and directed by an application. Here a server running on RHEL 6.8 has many applications, such as Tomcat, Postgres, Apache Kafka, POM components, EP components. For all applications, sockets are created on the network interfaces on the server. For the purposes of firewall configuration, these sockets are sourced from the server, so the firewall (iptables service) should be running on the same server. Application components in the Proactive Outreach Manager Application Server are listed as follows.

| Component | Interface | Description |
|---|---|---|
| ActiveMQ | Eth0 | This is a messaging component used for Inter process communication between POM components.<br>For example – Values modified at runtime on POM Dashboard are sent to corresponding POM processes using ActiveMQ. |
| Agent Manager | Eth0 | The core POM component that manages agent operations. This component interfaces with the agent desktop, rule engine, nailer and driver applications, WFO, CMS and Campaign Manager. |
| WFO | Eth0 | Agent Manager provides interface to communicate with Avaya WFO (ACR) for recording events. |
| JMX | Eth0 | Used for process monitoring of POM components. |
| Campaign Manager | Eth0 | The core POM component that manages the execution of campaigns. It interfaces with Agent Manager, EPM web services and rule engine for contact processing and dialing. |
| Campaign Director | Eth0 | The core POM component that manages the life-cycle of campaigns, data imports and exports. It interfaces with the POM vpms_plugin installed on primary experience portal management system (EPMS) and campaign manager for contact processing. |
| Rule Engine | Eth0 | The core POM component that evaluates system rules and campaign rules for each campaign. It interfaces with Campaign Manager and Agent Manager at runtime for rule evaluation of the contacts. |
| Application Sever | Eth0 | The POM nailer and driver CCXML are hosted on the application server that manages the customer dialing and agent dialog. These application interfaces with agent manager for sending the call and agent events and receiving agent operation events. |
| VPMS_Plugin | Eth0 | The core POM component that provides management interfaces for configuring POM servers, campaign, strategies etc. This component is deployed on Primary Experience Portal Management System. |
| Agent Desktop | Eth0 | The desktop application that interfaces with the agent manager component for providing agent related features like Preview, Redial, callbacks, agent scripts etc. |
| Kafka Server,<br>Zookeeper | Eth0 | This is used for event framework in POM.POM generates and sends various events such as Job events, Agent events and also sends real-time statistics such as Job statistics, Agent statistics to Apache Kafka server. |

| Component | Interface | Description |
|---|---|---|
| EventSDK | Eth0 | Event SDK is used for receiving events from Apache Kafka server and the events are generated by POM to Kafka server and it will also provide interface to clients for their customization. |
| Advanced List and Campaign Management service | Eth0 | New Springboot based microservice used for Splitting Master contact list file using filter templates into smaller set of files and subsequently into contact lists. |
| Agent SDK Service | Eth0 | New Springboot based microservice which wraps up AgentManager APIs for WebSocket interface consumed by Workspace for Elite Agent Desktop for POM |
| Dashboard Service | Eth0 | New Springboot based microservice for showing supervisor dashboard |
| Multitenancy Service | Eth0 | New Service for Tenant and User management |
| POMCache | Eth0 | New Cache cluster based on Apache Ignite |

# 2. Port Usage Tables

## 2.1 Port Usage Table Heading Definitions

**Source System:** System name or type that initiates connection requests.

**Source Port:** This is the default layer-4 port number of the connection source. Valid values include: 0 – 65535. A "(C)" next to the port number means that the port number is configurable.

**Destination System:** System name or type that receives connection requests.

**Destination Port:** This is the default layer-4 port number to which the connection request is sent. Valid values include: 0 – 65535. A "(C)" next to the port number means that the port number is configurable.

**Network/Application Protocol:** This is the name associated with the layer-4 protocol and layers-5-7 application.

**Optionally Enabled / Disabled:** This field indicates whether customers can enable or disable a layer-4 port changing its default port setting. Valid values include: Yes or No

"No" means the default port state cannot be changed (e.g. enable or disabled).

"Yes" means the default port state can be changed and that the port can either be enabled or disabled.

**Default Port State:** The "product" source or destination port is either open, closed, filtered or N/A.

Open: ports will respond to queries

Closed: ports may or may not respond to queries and are listed when they can be optionally enabled.

Filtered: ports can be open or closed, filtered UDP ports will not respond to queries, filtered TCP will respond to queries but will not allow connectivity.

N/A: primarily ephemeral ports used to connect to external sources such as DNS, NTP, etc.

**Description:** Connection details. Add a reference to refer to the Notes section after each table for specifics on any of the row data, if necessary.

## 2.2 Port Tables

Below are the tables which document the port usage for this product.

**Table 1.** Ports for Proactive Outreach Manager 3.1.2 (eth0)

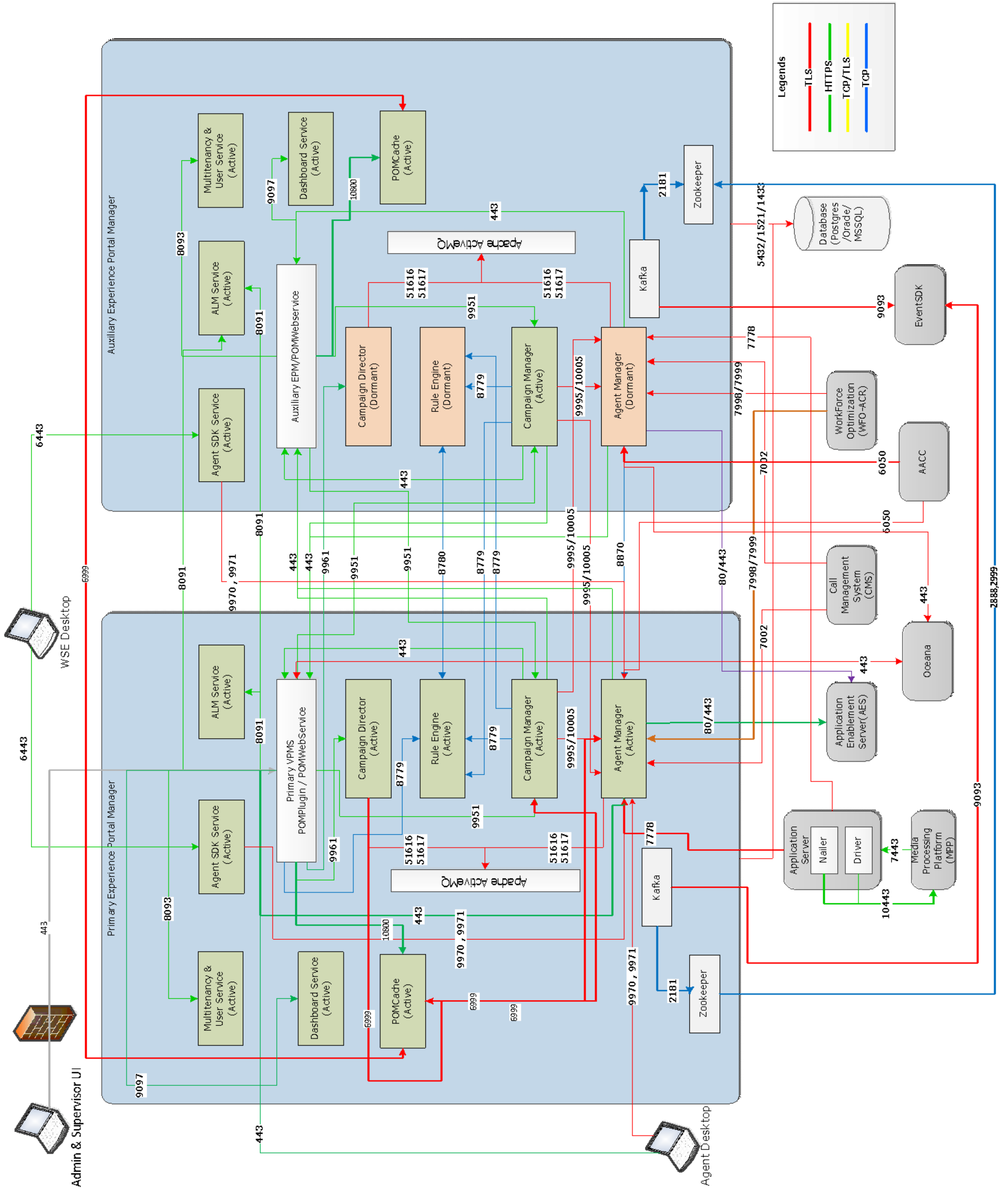
| Source | | Destination | | Network / Application Protocol | Optionally Enabled / Disabled? | Default Port State | Description |
|---|---|---|---|---|---|---|---|
| **System** | **Port (Configurable Range)** | **System** | **Port (Configurable Range)** | | | | |
| Campaign Manager | 1024-65535 | Agent Manager | 9995 – maximum number of zones (C) | TLS | No | Open | Pacer for each zone uses to communicate changes in pacing to the Campaign Manager. |
| Campaign Manager | 1024-65535 | Rule Engine | 8779 | TLS | No | Open | Campaign Manager request Rule Engine for rule evaluation for the contact to be attempted. |
| Campaign Manager | 1024-65535 | EPM | 443 | HTTPS | No | Open | This port is used for invoking Outcall Web services. |
| Campaign Manager | 1024-65535 | Agent Manager | 10005 – maximum number of zones (C) | TLS | No | Open | Pacer for each zone request agent records from campaign manager when attribute based or personal agenda based campaign is running. For each zone next port is opened So, we have 10006, 10007 for each new zone. |
| Agent Manager | 1024-65535 | ActiveMQ | l | TCP/TLS | No | Open | Agent manager uses ActiveMQ for inter process communication between self and EPM. |
| Agent Manager | 1024-65535 | AES | 80/443 | HTTP/HTTPS | No | Open | Agent Manager communicates with AES to fetch agent information from Communication Manager on agent login. |
| Agent Manager | 1024-65535 | Agent Manager | 8870 | TCP | No | Open | In multi POM environment for high availability of Agent Manager, the processes monitor the health of other servers on this port. |
| Agent Manager | 1024-65535 | EPM | 443 | HTTPS | No | Open | This port is used for invoking Outcall Web services. |
| Campaign Director | 1024-65535 | ActiveMQ | 51616 (C)/51617 | TCP/TLS | No | Open | Campaign Director uses ActiveMQ for inter process communication between self and EPM. |
| Rule Engine | 1024-65535 | Rule Engine | 8780 | TCP | No | Open | In multi POM environment for high availability of Rule Engine, the processes monitor the health of other servers on this port. |
| VPMS_Plugin | 1024-65535 | Campaign Manager | 9951 | HTTPS | No | Open | POM web services and user interface sends contact events to Campaign Manager on this port. |
| VPMS_Plugin | 1024-65535 | Rule Engine | 8779 | TLS | No | Open | POM user interface sends rule configuration to Rule Engine on this port. |
| VPMS_Plugin | 1024-65535 | Campaign Director | 9961 | HTTPS | No | Open | POM user interfaces sends JOB start event to Campaign Director on this port. |

| Source | | Destination | | Network / Application Protocol | Optionally Enabled / Disabled? | Default Port State | Description |
|---|---|---|---|---|---|---|---|
| System | Port (Configurable Range) | System | Port (Configurable Range) | | | | |
| Application Server | 1024-65535 | Agent Manager | 7778-maximum number of zones (C) | TLS | No | Open | Router uses to communicate agent information with application servers |
| Agent Desktop | 1024-65535 | Agent Manager | 9970, 9971-maximum number of zones (C) | TLS | No | Open | Agent desktops using POM Desktop API library connect to Agent Manager on these ports. |
| WFO | 1024-65535 | Agent Manager | 7999 (C) | TCP | No | Open | Avaya WFO connects to POM for recording events on this TCP port. |
| WFO | 1024-65535 | Agent Manager | 7998 (C) | TLS | No | Open | Avaya WFO connects to POM for recording events on this TLS port. |
| CMS Rt_socket | 1024-65535 | Agent Manager | 7002 (C) | TLS | No | Open | Agent Manager receives Skill data feed from Rt_socket package. |
| JMX Console | 1024-65535 | Agent Manager | 10010 | TCP | No | Open | These are JMX ports used for monitoring Campaign Manager, Campaign Director and the Agent Manager process. |
| JMX Console | 1024-65535 | Campaign Manager | 10011 | TCP | No | Open | These are JMX ports used for monitoring Campaign Manager, Campaign Director and the Agent Manager process. |
| JMX Console | 1024-65535 | Campaign Director | 10012 | TCP | No | Open | These are JMX ports used for monitoring Campaign Manager, Campaign Director and the Agent Manager process. |
| Agent Manager, Campaign Director, Campaign Manager, Rule Engine | 1024-65535 | Postgres | 5432 (C) | TCP/TLS | No | Open | Database Port |
| Agent Manager, Campaign Director, Campaign Manager, Rule Engine | 1024-65535 | Oracle | 1521 (C) | TCP/TLS | No | Open | Database Port |
| Agent Manager, Campaign Director, Campaign Manager, Rule Engine | 1024-65535 | MSSQL | 1433 (C) | TCP/TLS | No | Open | Database Port |
| Application Server | 1024-65535 | MPP | 10443 | HTTPS | No | Open | This port is used for sending events to MPP server. |
| EventSDK | 1024-65535 | Kafka | 9093 (C) | TLS | No | Open | Kafka server listens on this port and it is used for getting request/response from Kafka clients (EventSDK). |

| Source | | Destination | | Network / Application Protocol | Optionally Enabled / Disabled? | Default Port State | Description |
|---|---|---|---|---|---|---|---|
| System | Port (Configurable Range) | System | Port (Configurable Range) | | | | |
| Kafka | 1024-65535 | Zookeeper | 2181 | TCP | No | Open | Kafka server and Zookeeper talks internally on this port. |
| Agent Manager, Campaign Director, Campaign Manager | 1024-65535 | Kafka | 9093 (C) | TLS | No | Open | Producers send data event to kafka server on this port. |
| Advanced List Management Service | 1024-65535 | Advanced List Management Service | 8091 | TLS | No | Open | This port is used for communicating to ALM service via TLS |
| Agent SDK Service | 1024-65535 | Agent SDK Service | 6443 | TLS | No | Open | This port is used form Workspace for Elite POM desktop to Websocket based service |
| External Selection | 1024-65535 | Agent Manager | 11000 | TLS | No | Open | This port is used for connecting External selection system to Agent Manager |
| ZooKeeper | 1024-65535 | Zookeeper | 2888, 2999 | TCP | Yes | Open | ZooKeeper nodes use a pair of ports -<br>2888 and 3888 for follower nodes to connect to the leader node and for leader election, respectively. |
| EPM | 1024-65535 | Dashboard Service | 9097 | HTTPS | Yes | Open | Forwarding HTTPS requests from main EPM Tomcat to Dashboard Service |
| EPM | 1024-65535 | Multitenancy Sevice | 8093 | HTTPS | Yes | Open | Forwarding HTTPS requests from main EPM Tomcat to Multitenancy Service |
| Multitenancy Service(Ignite Cache) | 1024-65535 | Multitenancy Sevice | 10850 | TLS | Yes | Open | This port is used by Ignite Cache in Multitenancy service |
| Agent Manager | 1024-65535 | POMCache | 6999 | TLS | Yes | Open | This port is used for communication between AM and POMCache |
| Campaign Manager | 1024-65535 | POMCache | 6999 | TLS | Yes | Open | This port is used for communication between Campaign Manager and POMCache |
| Campaign Director | 1024-65535 | POMCache | 6999 | TLS | Yes | Open | This port is used for communication between Campaign Director and POMCache |
| EPM | 1024-65535 | POMCache | 10800 | TLS | Yes | Open | This port is used for communication between VPMS and POMCache service |
| POMCache | 1024-65535 | POMCache | 6999, 47100-47102, 10800-10802, 11211, 7445 | TLS | Yes | Open | Cache Service uses this port to synchronize between each other |
| POMCache | 1024-65535 | POMCache | 6999 | TLS | Yes | Open | Cache Service uses this port to synchronize between each other |
| POMCache | 1024-65535 | POMCache | 47100-47102 | TCP | Yes | Open | Cache Service uses this port for Internal TCP communication |

| Source | | Destination | | Network / Application Protocol | Optionally Enabled / Disabled? | Default Port State | Description |
|---|---|---|---|---|---|---|---|
| System | Port (Configurable Range) | System | Port (Configurable Range) | | | | |
| POMCache | 1024-65535 | POMCache | 10800-10802 | TCP | Yes | Open | Cache Service uses this port for Thin client discovery ports |
| POMCache | 1024-65535 | POMCache | 11211 | HTTP/S | Yes | Open | HTTP internal |
| POMCache | 1024-65535 | POMCache | 7445 | HTTP/S | Yes | Open | Cache Spring boot server port |
| AACC | 1024-65535 | Agent Manager | 6050 | TLS | Yes | Open | AACC broadcast |
| EPM | 1024-65535 | AACC/ Oceana | 443 | TLS | Yes | Open | UI makes a call to AACC/Oceana for skills |

## 3. Port Usage Diagram



Legends
TLS
HTTPS
TCP/TLS
TCP
Auxiliary Experience Portal Manager
Primary Experience Portal Manager
Multitenancy & User Service (Active)
Dashboard Service (Active)
POMCache (Active)
ALM Service (Active)
Agent SDK Service (Active)
Auxiliary EPM/POMWebservice
Primary VPMS POMPlugin / POMWebService
Campaign Director (Dormant)
Campaign Director (Active)
Rule Engine (Dormant)
Rule Engine (Active)
Campaign Manager (Active)
Agent Manager (Dormant)
Agent Manager (Active)
Apache ActiveMQ
Kafka
Zookeeper
Database (Postgres /Oracle/ MSSQL)
EventSDK
WorkForce Optimization (WFO-ACR)
AACC
Call Management System (CMS)
Oceana
Application Enablement Server(AES)
Application Server
Nailer
Driver
Media Processing Platform (MPP)
WSE Desktop
Admin & Supervisor UI
Agent Desktop
8093
9097
10800
443
8091
51616 51617
9951
8779
9995/10005
2181
5432/1521/1433
9093
7778
7998/7999
7002
6050
80/443
8870
8780
9961
9970 , 9971
6443
6999
2888,2999
7443
10443

# Appendix A: Overview of TCP/IP Ports

## What are ports and how are they used?

TCP and UDP use ports (defined at http://www.iana.org/assignments/port-numbers) to route traffic arriving at a particular IP device to the correct upper layer application. These ports are logical descriptors (numbers) that help devices multiplex and de-multiplex information streams. For example, your PC may have multiple applications simultaneously receiving information: email using destination TCP port 25, a browser using destination TCP port 443 and a ssh session using destination TCP port 22. These logical ports allow the PC to de-multiplex a single incoming serial data packet stream into three mini-streams inside the PC. Each of the mini-streams is directed to the correct high-level application identified by the port numbers. Every IP device has incoming (Ingress) and outgoing (Egress) data streams.

Ports are used in TCP and UDP to name the ends of logical connections which carry data flows. TCP and UDP streams have an IP address and port number for both source and destination IP devices. The pairing of an IP address and a port number is called a socket. Therefore, each data stream is uniquely identified with two sockets. Source and destination sockets must be known by the source before a data stream can be sent to the destination. Some destination ports are “open” to receive data streams and are called “listening” ports. Listening ports actively wait for a source (client) to make contact with the known protocol associated with the port number. HTTPS, as an example, is assigned port number 443. When a destination IP device is contacted by a source device using port 443, the destination uses the HTTPS protocol for that data stream conversation.

## Port Types

Port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic Ports (sometimes called Private Ports). The Well Known and Registered ports are assigned by IANA (Internet Assigned Numbers Authority) and are found here: http://www.iana.org/assignments/port-numbers.

### Well Known Ports

Well Known Ports are those numbered from 0 through 1023.
For the purpose of providing services to unknown clients, a service listen port is defined. This port is used by the server process as its listen port. Common services often use listen ports in the well-known port range. A well-known port is normally active meaning that it is “listening” for any traffic destined for a specific application. For example, well known port 23 on a server is actively waiting for a data source to contact the server IP address using this port number to establish a Telnet session. Well known port 25 is waiting for an email session, etc. These ports are tied to a well understood application and range from 0 to 1023.

In UNIX and Linux operating systems, only root may open or close a well-known port. Well Known Ports are also commonly referred to as “privileged ports”.

### Registered Ports

Registered Ports are those numbered from 1024 through 49151.
Unlike well-known ports, these ports are not restricted to the root user. Less common services register ports in this range. Avaya uses ports in this range for call control. Some, but not all, ports used by Avaya in this range include: 1719/1720 for H.323, 5060/5061 for SIP, 2944 for H.248 and others. The registered port range is 1024 – 49151. Even though a port is registered with an application name, industry often uses these ports for different applications. Conflicts can occur in an enterprise when a port with one meaning is used by two servers with different meanings.

### Dynamic Ports

Dynamic Ports are those numbered from 49152 through 65535.
Dynamic ports, sometimes called “private ports”, are available to use for any general purpose. This means there are no meanings associated with these ports (similar to RFC 1918 IP Address Usage). These are the safest ports to use because no application types are linked to these ports. The dynamic port range is 49152 – 65535.

## Sockets

A socket is the pairing of an IP address with a port number. An example would be 192.168.5.17:3009, where 3009 is the socket number associated with the IP address. A data flow, or conversation, requires two sockets – one at the source device and one at the destination device. The data flow then has two sockets with a total of four logical elements. Each data flow must be unique. If one of the four elements is unique, the data flow is unique. The following three data flows are uniquely identified by socket number and/or IP address.

Data Flow 1: 172.16.16.14:1234 - 10.1.2.3:2345
two different port numbers and IP addresses and is a valid and typical socket pair

Data Flow 2: 172.16.16.14.123**5** - 10.1.2.3:2345
same IP addresses and port numbers on the second IP address as data flow 1, but since the port number on the first socket differs, the data flow is unique

Data Flow 3: 172.16.16.14:1234 - 10.1.2.4:2345

If one IP address octet changes, or one port number changes, the data flow is unique.

Socket Example Diagram

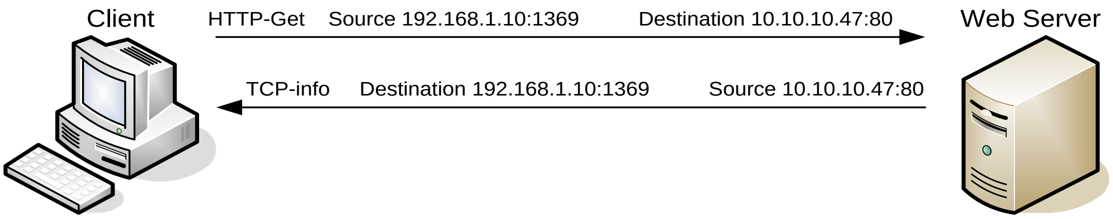


**Figure 1.** Socket example showing ingress and egress data flows from a PC to a web server

The client egress stream includes the client’s source IP and socket (1369) and the destination IP and socket (80). The ingress stream from the server has the source and destination information reversed.

## Understanding Firewall Types and Policy Creation

### Firewall Types

There are three basic firewall types:

- Packet Filtering
- Application Level Gateways (Proxy Servers)
- Hybrid (Stateful Inspection)

Packet Filtering is the most basic form of the firewalls. Each packet that arrives or leaves the network has its header fields examined against criterion to either drop the packet or let it through. Routers configured with Access Control Lists (ACL) use packet filtering. An example of packet filtering is preventing any source device on the Engineering subnet to telnet into any device in the Accounting subnet.

Application level gateways (ALG) act as a proxy, preventing a direct connection between the foreign device and the internal destination device. ALGs filter each individual packet rather than blindly copying bytes. ALGs can also send alerts via email, alarms or other methods and keep log files to track significant events.

Hybrid firewalls are dynamic systems, tracking each connection traversing all interfaces of the firewall and making sure they are valid. In addition to looking at headers, the content of the packet, up through the application layer, is examined. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Stateful inspection firewalls close off ports until the connection to the specific port is requested. This is an enhancement to security against port scanning[1].

## Firewall Policies

The goals of firewall policies are to monitor, authorize and log data flows and events. They also restrict access using IP addresses, port numbers and application types and sub-types.

This paper is focused with identifying the port numbers used by Avaya products so effective firewall policies can be created without disrupting business communications or opening unnecessary access into the network.

Knowing that the source column in the following matrices is the socket initiator is key in building some types of firewall policies. Some firewalls can be configured to automatically create a return path through the firewall if the initiating source is allowed through. This option removes the need to enter two firewall rules, one for each stream direction, but can also raise security concerns.

Another feature of some firewalls is to create an umbrella policy that allows access for many independent data flows using a common higher layer attribute. Finally, many firewall policies can be avoided by placing endpoints and the servers that serve those endpoints in the same firewall zone.

[1] The act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.