Upgrading Avaya Proactive Outreach Manager

Release 4.0.2 SP3
Issue 1
July 2024

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

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

Licenses

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

This document provides procedures to upgrade Avaya Proactive Outreach Manager on Red Hat Enterprise Linux and Avaya Enterprise Linux.

This document is intended for anyone who wants to upgrade, configure, and verify Avaya Proactive Outreach Manager. The audience includes and is not limited to implementation engineers, field technicians, business partners, and customers.

Change history

Issue	Date	Summary of changes
Release 4.0.2 SP3, Issue 1	July 2024	Added a Note to the topic Upgrading POM.
Release 4.0.2 SP2, Issue 1.2	October 2023	Updated the topic Configuring the POM database on the primary POM server. Updated the topic Configuring applications and licenses with a new cipher value. Updated the topic Exchanging and configuring certificates with a new cipher value.
Release 4.0.2 SP1, Issue 1.1	December 2022	Updated or removed content related to Cache for operational database.
Release 4.0.2, Issue 1.0	October 2022	Initial issue of the document for POM 4.0.2. The following topics are updated: • About Upgrade • Upgrade prerequisites • POM upgrade Checklist • Upgrading POM • Upgrade fallback

Chapter 2: Upgrading to POM 4.0.2

About upgrade

You can upgrade POM to release 4.0.2 only from POM release 4.0.1.

Important:

In addition to POM, you must do the following actions:

- Upgrade Avaya Experience Portal to release 8.1.2.
- Avaya Orchestration Designer to release 8.1.2.

To upgrade Avaya Experience Portal, see the *Upgrading Avaya Experience portal* guide.

Before you upgrade POM, ensure that the POM database runs.

Note:

- The customer is responsible for the following:
  - The administration and the support of the POM system.
  - The contents in the POM database that undergoes a release upgrade.
- In a production environment, do not install a POM database schema on a local PostgreSQL database. Ensure that you install a PostgreSQL, an Oracle, or a Microsoft SQL Server database only on an external server.

Prerequisites

Before upgrading POM to release 4.0.2, do the following:

- Ensure your current release is POM 4.0.1.
- See the Interoperability matrix.
- For more information about hardware and software requirements for upgrading to release 4.0.2, see *Implementing Proactive Outreach Manager*.
- Check the existing system customizations and take necessary inputs for changes in Java, Hibernate, and the operating system of the POM server.
- Ensure you upgrade POM in lab systems first.

  If the POM upgrade in the lab is successful, upgrade POM in the production environment.

POM upgrade checklist

Use the following checklist in the given order for upgrading to POM 4.0.2:

Sr. no.	Task	Notes	√
1	Back up your database	See Backing up the POM database on page 12.	
2	Upgrade Experience Portal to 8.1.2.	See *Upgrading Avaya Experience Portal* on Avaya Support website at https://support.avaya.com.	
3	Upgrade POM Upgrade primary POM server first. Upgrade the auxiliary POM servers after the primary POM server is installed and is operational.	See Upgrading POM on page 8	
4	Verify the system after upgrade is complete	See Configuring and verifying the system post upgrade on page 15	

Running scripts before upgrading POM

About this task

Do the following procedure:

- After the POM server connects to an Oracle database.
- After you upgrade the current version of EP to 8.1.2.
- Before you upgrade the current version of POM to a later version.

Procedure

1. On Avaya Experience Portal, to stop the `vpms` service, run the following script:

   `systemctl stop vpms`

2. **(Optional)** If you upgrade EP, run the following script:

   `$POM_HOME/bin/updateVPMSConf.sh`

3. To go to the database directory, run the following command:

   `cd $AVAYA_HOME/Support/Database`

4. To install the JDBC driver, run the following bash command:

   `./InstallOracleJDBC.sh`

Upgrading POM

Before you begin

Ensure that you are on the supported releases of Avaya Experience Portal.

Procedure

1. Log in to Avaya Experience Portal by using one of the following user profiles:
   - root
   - sroot
2. Based on your operating system, do one of the following:
   - For Red Hat Enterprise Linux (RHEL), use the root user profile.
   - For Avaya Enterprise Linux (AEL), use the sroot user profile.
3. Run the following command to mount the POM iso image to the server:

   mount —o loop <absolute path of the iso image> /mnt
4. Run the following command to change the directory to mnt:

   cd /mnt
5. Run the following command:

   ./installPOM

   The system displays the following message:

```
*** Starting POM Installation ***
************************************************************
** *** Restarting and checking vpms
service status, please wait... ***
************************************************************
** tomcatd ( pid xxxxx ) is running... SL ( pid xxxxx ) is
running... ActiveMQ is running ... Overall Status: VPMS is running
************************************************************
** *** EP service status [OK]***
************************************************************
** "
```

   Before starting the installation, the installer checks for VPMS services and the state of the components such as Tomcat, SL, ActiveMQ, and VPMS. If any of the components is not running, the installer aborts the upgrade. Therefore, you must ensure that all components are functional. If all the VPMS services and the components are functional, the installer stops the VPMS service and the system displays the `Running CLI installation program` message.

   While the installer stops the VPMS service, the system displays the following message:

```
************************************************************
** *** Stopping vpms service, please wait... ***
```

```
**************************************************************
** Stopping individual components: Stopping
Tomcat.............Counter: 10. Tomcat is not running: 0 Tomcat
not shut down gracefully; forceful shut down being enacted
Will kill tomcat PIDs: xxxxx Stopping SL...... successful
Stopping ActiveMQ...... successful VPMS Shutdown Status: [ OK ]
Overall Status: VPMS is stopped (all processes are stopped )
**************************************************************
** *** vpms service stopped... Starting POM Installation... ***
**************************************************************
**
```

After the VPMS service stops, the system displays a message as follows:

```
Running CLI installation program

POM.04.00.02.00.00.xxx Welcome to the installation of Avaya POM
POM.04.00.02.00.00.xxx! The homepage is at: http://www.avaya.com/"
```

6. Type `1` to continue.

   If the installer detects an earlier release of POM, it provides the following options:

   - POM Upgrade
   - POM Un-Install

     For information about uninstallation, see *Implementing Avaya Proactive Outreach Manager*.

7. Type `0` to upgrade.
8. **(Optional)** To quit the upgrade process at any point, do the following:
   a. Press `4`.
   b. On the confirmation screen, press `1`.
9. Type `1` to continue.

   The installer displays the POM Upgrade Warning window as follows:

```
**************************************************************
*** POM Upgrade Warning***
**************************************************************
POM Upgrade will delete the existing $POM_HOME folder and reinstall
the new binaries of this version. Please take the backup of
any user created files and log files. Also this will upgrade
the existing POM database schema. BEFORE CONTINUING, THE DATABASE
ADMINISTRATOR SHOULD TAKE A CURRENT BACKUP OF THE POM DATABASE
Press 1 to Continue, 2 for Previous, 3 to Redisplay or 4 to Quit
[1] "
```

10. Type `1` to continue.

    The installer displays the Upgrade Summary window displaying the following:

```
Upgrade Summary Note: The last portion of the upgrade might
take several minutes to complete. Please be patient and wait
for the Post Upgrade Summary to be displayed. IMPORTANT :
PLEASE DO NOT ABORT -------------- --------------------------
Following packages will be upgraded. VPMS/EPMS Plugin POM Server
DD/AAOD Applications Installed Version: POM.04.xx.xx.xx.xxx will
be upgraded to New Version: POM.04.00.01.00.00.xxx Press 1 to
Continue, 2 for Previous, 3 to Redisplay or 4 to Quit [1] 1 "
```

- All packages that get upgraded
- From and To releases of the upgraded packages.

Caution:

If you type `1` on the **Upgrade Summary** window, you cannot navigate back to the upgrade.

Do not quit the upgrade until the installer completes the upgrade and displays the Post Upgrade Summary window.

After the upgrade begins, the system displays the following message:

```
[ Starting to unpack ] [ Processing package: (1/4) ] [ Processing
package: EPMS plugin (2/4) ] .[ Processing package: POM
Server (3/4) ] [ Processing package: AAOD Application (4/4) ] ..
[ Unpacking finished ] After the upgrade is complete, the
system displays the following message: Installation was
successful. Application installed on <installation path>
================================================================
[ Console installation done ] /etc/alternatives/
java_sdk_1.8.0//bin/java Entry for alias pomservercert successfully
imported. Import command completed: 1 entries successfully
imported, 0 entries failed or cancelled MAC verified OK
Making Appserver server configuration changes... SSL is NOT
enabled in /opt/AppServer/Tomcat/tomcat/conf/server.xml at port
7443, now making POM specific changes..... mv: `/opt/AppServer/
Tomcat/tomcat/conf/server.xml.ssl' and `/opt/ AppServer/Tomcat/
tomcat/conf/server.xml.ssl' are the same file /opt/AppServer/
Tomcat/tomcat/conf/server.xml changes done ..... Updating the
catalina.sh JAVA_OPTS_POM_APP Variable is already found /opt/
AppServer/Tomcat/tomcat/bin/catalina.sh changes done ....
================================================================
=== It has been found that the existing
POM certificate is a selfsigned certificate. IT
IS RECOMMENDED TO GENERATE A NEW CERTIFICATE
BY EXECUTING SCRIPT $POM_HOME/bin/pomCertificateGenerate.sh
================================================================
=== Moving installation log
files to: /opt/Avaya/avpom/POManager/logs
```

```
================================================================
If you are using an external application server and you have
installed the POM DD/AAOD Application package while installing
POM, you need to: a--> Copy the *.war files from $POM_HOME/DDapps
to $CATALINA_HOME/ webapps of the external application server.
b--> Copy files from $POM_HOME/DDapps/lib/* to $CATALINA_HOME/lib
of your external application server. c--> Enable the SSL
Configurations for application server. d--> Restart the external
application server. Please restart the system now !"
```

Note:

Continue with the upgrade procedure without restarting the system. You can restart after the system as instructed in step 14.

11. To enable Advanced Campaign and List Management, press `y`.

    After this feature is enabled, you cannot disable it. You can choose to enable this later. For more information, see *Administering Avaya Proactive Outreach Manager*.

12. To start migration of campaign filters to filter templates, press `y`.

    You must migrate filter conditions in all campaigns to filter templates. The migration associates the configured contact list to the campaigns and newly created filter templates to contact lists. This is a mandatory step for the campaign to run. You can choose to enable this later. For more information, see *Administering Avaya Proactive Outreach Manager.*

13. POM prompts you `Do you want to enable Advanced guard time now?` Press `y` if you want to enable advanced guard times. Enabling this option requires all contact lists to be re-imported. You can choose to skip by pressing `n` if you do not want to enable Advanced guard time. The option can be enabled any time later by executing the command **`$POM_HOME/bin/enable_Advanced_Guard_Time`**. When you enable the option, you must re-import all the Contact lists. If the option is already enabled in your system, POM does not prompt you during install or upgrade. The Advanced Guard Time encompasses the following features:

- Timezone based record selection
- User configurable allowed and disallowed times for calling
- List distribution

You can read more about these features in the Release Notes and enable them anytime later. Enabling this feature makes existing contact lists non-usable. All contact lists will have to re-imported. After the option is enabled, you cannot disable Advanced Guard Time.

14. To enable classification of SIP response code 403 as ‘CALL_FORBIDDEN’ then run the following command as root user: **`$POM_HOME/bin/updatePOMConfig CallForbidden true`**

Note:

During the upgrade process, FIPS enabled POM system loses all FIPS related configuration. You must enable and configure FIPS again. For more information, see Enabling FIPS topic in the *Implementing Avaya Proactive Outreach Manager* guide.

15. Restart the system.
16. If you have a multiple POM server environment, you must follow the same steps for upgrading POM on auxiliary servers.

    You must restart the Campaign Manager service.

Caution:

Do not run the `installDB.sh` script post upgrade to recreate the POM schema as POM uses the existing schema.

Note:

After upgrading POM to release 4.0.2, all purges are:

- Configured for all organizations.
- Scheduled to run daily at 00:00 hours.

POM deletes the Purge schedules that are configured earlier to release 4.0.2.

Note:

When the POM system executes campaign export, the export files containing the campaign processed contact records are available in the respective organization directory. When you upgrade to POM 4.0.2, take a backup of old export directory. You can see the details of the old export directory in the Global configurations page.

Backing up the POM database

About this task

If you use an Oracle database, use this procedure to enable Oracle Recovery Manager (RMAN) to take a backup of the POM database.

After you take a backup, ensure that you take an incremental backup of the POM database.

Before you begin

Ensure that:

- POM does not run any active imports.
- The POM database is in the `ARCHIVELOG` mode.
- You have the `SYSDBA` privileges such as `sqlplus` or `sysdba`.

Do the following:

- Stop all the running campaigns on the POM server.
- Log off all the agents.
- Connect RMAN to the POM database.

Procedure

1. Open an SSH session to the POM server.

   You can use an application such as PuTTY.
2. To shut down the running instance of the POM database, run the following command:

   ```
   shutdown immediate;
   ```
3. To start the instance and mount the POM database, run the following command:

   ```
   startup mount;
   ```
4. To place the POM database in the `ARCHIVELOG` mode, run the following command:

   ```
   alter database archivelog;
   ```
5. To open the POM database, run the following command:

   ```
   alter database open;
   ```
6. Run the following command:

   ```
   archive log list;
   ```
7. To identify the name of a POM database, run the following commands:

   `ORACLE_SID`;

   ```
   set ORACLE_SID=pomdb
   ```

   ```
   echo %ORACLE_SID%
   ```
8. To connect RMAN to the POM database, run the following command:

   ```
   RMAN rman target /
   ```
9. To back up the POM database, run the following command:

   ```
   BACKUP DATABASE PLUS ARCHIVELOG
   ```
10. To take an incremental backup of the POM database, run the following command:

    `BACKUP INCREMENTAL LEVEL 0 DATABASE`;

Recovering and restoring the POM database

About this task

If you use an Oracle database, use this procedure to do the following:

- Recover the backup file of the POM database.
- Restore the backup file on a POM server.

Before you begin

Ensure that you have `SYSDBA` user privileges.

Procedure

1. To connect to the POM database as a user with `SYSDBA` privileges, run the following command:

   `sqlplus / as sysdba`

2. To shut down the current instance of the POM database, run the following command:

   `shutdown abort`;

3. To delete all CTL files and DBF files, run the following command:

   `oradata\pomdb`

4. To connect RMAN to the POM database, run the following command:

   `rman target /`

5. To start the instance and mount the database, run the following command:

   `startup nomount;`

6. To reconnect RMAN to the POM database, run the following command:

   `rman target /`

7. To restore the control file, run the following command:

   `restore controlfile from 'control_file_name'`;

8. To mount an instance of the POM database, run the following command:

   `alter database mount`;

9. To restore the POM database, run the following command:

   `restore database`;

10. To recover the POM database, run the following command:

    `recover database`;

11. To open the POM database, run the following command:

    `alter database open resetlogs`;

Configuring and verifying the system post upgrade

Procedure

1. Log on to the POM server as a root user.

   You can use an application such as PuTTY to open an SSH session to the POM server.

2. Go to `$POM_HOME/config` and ensure that the `PIMHibernate.cfg.xml` file contains Hikari properties instead of c3p0 properties.

3. Run the `Create Indices` script on the primary server from `$POM_HOME/bin/createCustomIndices.sh`.

4. If you have regenerated the Experience Portal certificate, to ensure that you have the latest root certificates post upgrade, run the following command: `bash $POM_HOME/bin/do_UpdatePOMCerts`.

5. If you upgrade VPMS after installing or upgrading POM, the soft links break. To resolve this, run the command `vpUpgrade.sh`.

6. Run the command `POM status` and verify that all services are running.

   The system displays a message:

   ```
   # service POM status
   Checking POM <version POM.04.00.02.00.yyy> Status at Mon Jun 13 15:57:47 IST 2022
   Checking individual components:
   STATE=RUNNING
   Agent Manager ( pid xxxxx  ) is running...

   STATE=RUNNING
   Campaign Manager ( pid xxxx  ) is running...

   STATE=RUNNING
   Campaign Director ( pid xxxx  ) is running...

   STATE=RUNNING
   POM ActiveMQ ( pid xxxx ) is running...

   STATE=RUNNING
   POM Rule Engine ( pid xxxx ) is running...

   STATE=RUNNING

   zookeeper ( pid xxxxx ) is running...

   STATE=RUNNING
   kafka ( pid xxxxx ) is running...

   STATE=RUNNING

   Overall Status: POM is running
   ```

   where xxxx is the pid of corresponding process and yyy is the POM release.

7. You must fetch the EPM certificate after upgrade:

   a. In the navigation pane, click **Proactive Outreach** > **Manager**.

   b. Click **Configurations** > **Trusted Certificate**.

c. To fetch an Avaya Experience Portal certificate, click **Fetch**.

d. In the **Name** field, type a unique name of an EPM certificate.

e. In the **Location** field, type `https://<EPM IP Address>`

f. Click **Continue**.

8. You must reconfigure the POM certificate after upgrade:

   a. From the left pane, select, **EPMS** > **Proactive Outreach** > **Manager** > **Configurations** > **Servers**

   b. Click the POM Server to edit.

   c. Click **Apply** to fetch the certificate.

   d. Trust the certificate.

   e. Click **Save**.

   Note:

   Repeat Step 4 and Step 5 for each auxiliary POM server.

9. Reconfigure the outcall password using the menu option **Proactive Outreach** > **Manager** > **Configurations** > **Servers** > **Outbound settings** > **Edit Voice Server**. You must provide the Avaya Experience Portal user name and the password, which has the Outcall privilege under the Web Services role, to connect to the voice server.

   Post upgrade, POM sets the default Home Country in the Global Configurations to “USA & Canada”.

10. To change the Home Country, log in to EPM as admin user, go to **Proactive Outreach** > **ManagerConfigurations** > **Global Configurations** to change the values and save the changes.

11. Ensure that Nailer and POMDriverApp applications' URL has https (if not set already), and the port is set to 7443 instead of 7080.

12. Ensure that Email settings are configured on Avaya Experience Portal under **Multi-Media Configuration** > **Email**.

13. Ensure that SMS settings are configured on Avaya Experience Portal under **Multi-Media Configuration** > **SMS**.

14. Restart mmsserver service by typing `mmsserver restart`.

15. Restart appserver service by typing `appserver restart`.

16. If the campaign strategy has used Email channel, then provide AvayaPOMEmail application (configured in step 9 above) in the Email node. While configuring email settings on AEP, ensure that you specify the same sender’s address as specified in Experience Portal . Also in the text item node, ensure that the subject is specified.

17. If the campaign strategy has used SMS channel, then provide AvayaPOMSMS application (configured in step 10 above) in the SMS node. Also ensure that the sender's address matches with short code specified in SMS settings of Experience Portal.

18. To check the system health:
    - Log in to the EPM Web administration and select **Proactive Outreach** > **ManagerConfigurations** > **Servers** > **POM Manager** to check if the POM server is functional.

      Note:

      Ensure that none of the POM service is in the **STOPPED** state.
    - For multiple server setup, in the left pane select, **Real-Time Monitoring** > **System Monitor** and check the EPM state is running for auxiliary EPM server.
    - Check if Avaya Experience Portal is running successfully by making at least one inbound and outbound call.
19. If you have a multiple POM server environment, restart the Campaign Manager Service on all Auxiliary servers.

Chapter 3: Common procedures

Process flow to exchange and configure certificates

Process flow to exchange and configure certificates on a single POM server

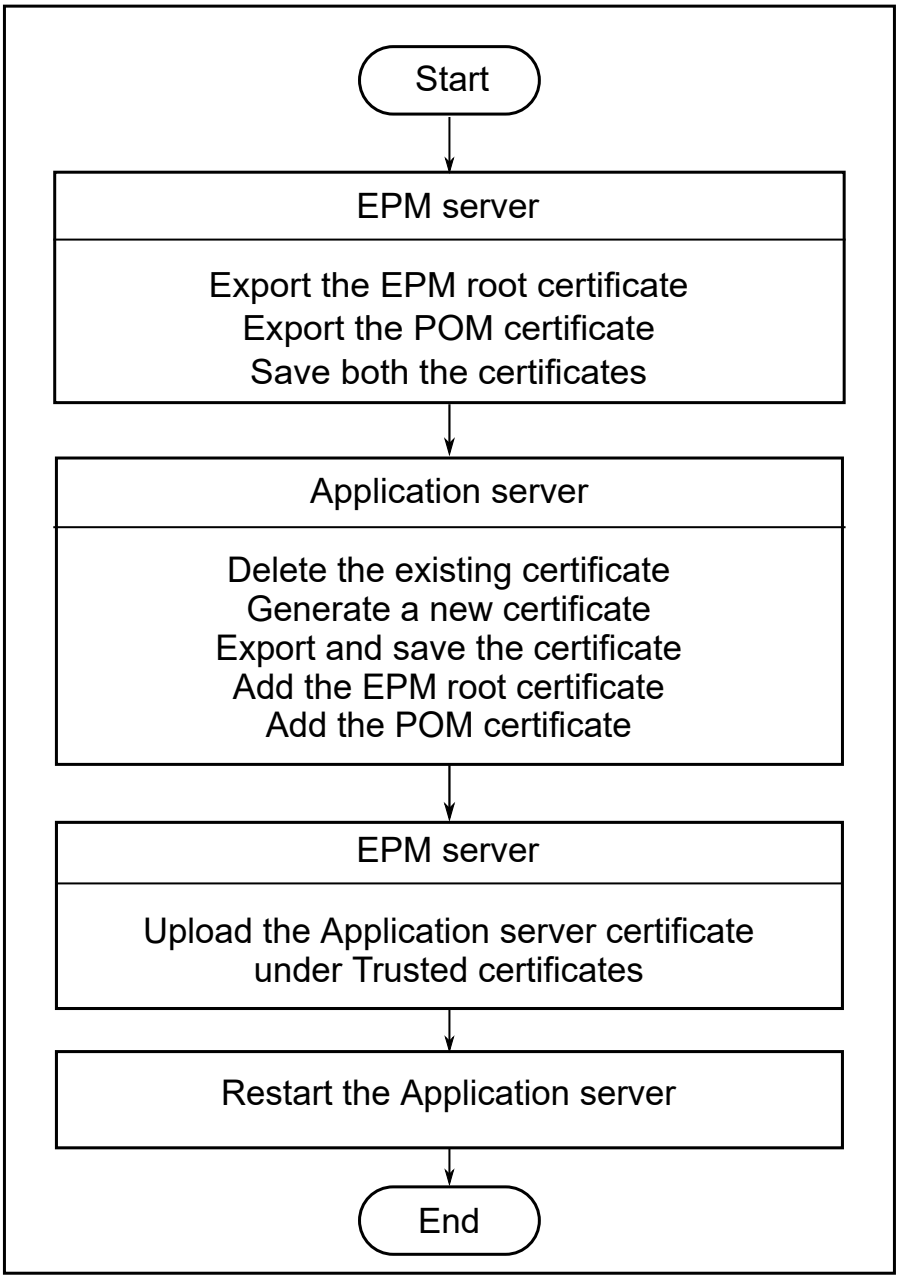

Figure 1: Exchange and configure certificates on a single POM server

Process flow to exchange and configure certificates on multiple POM servers

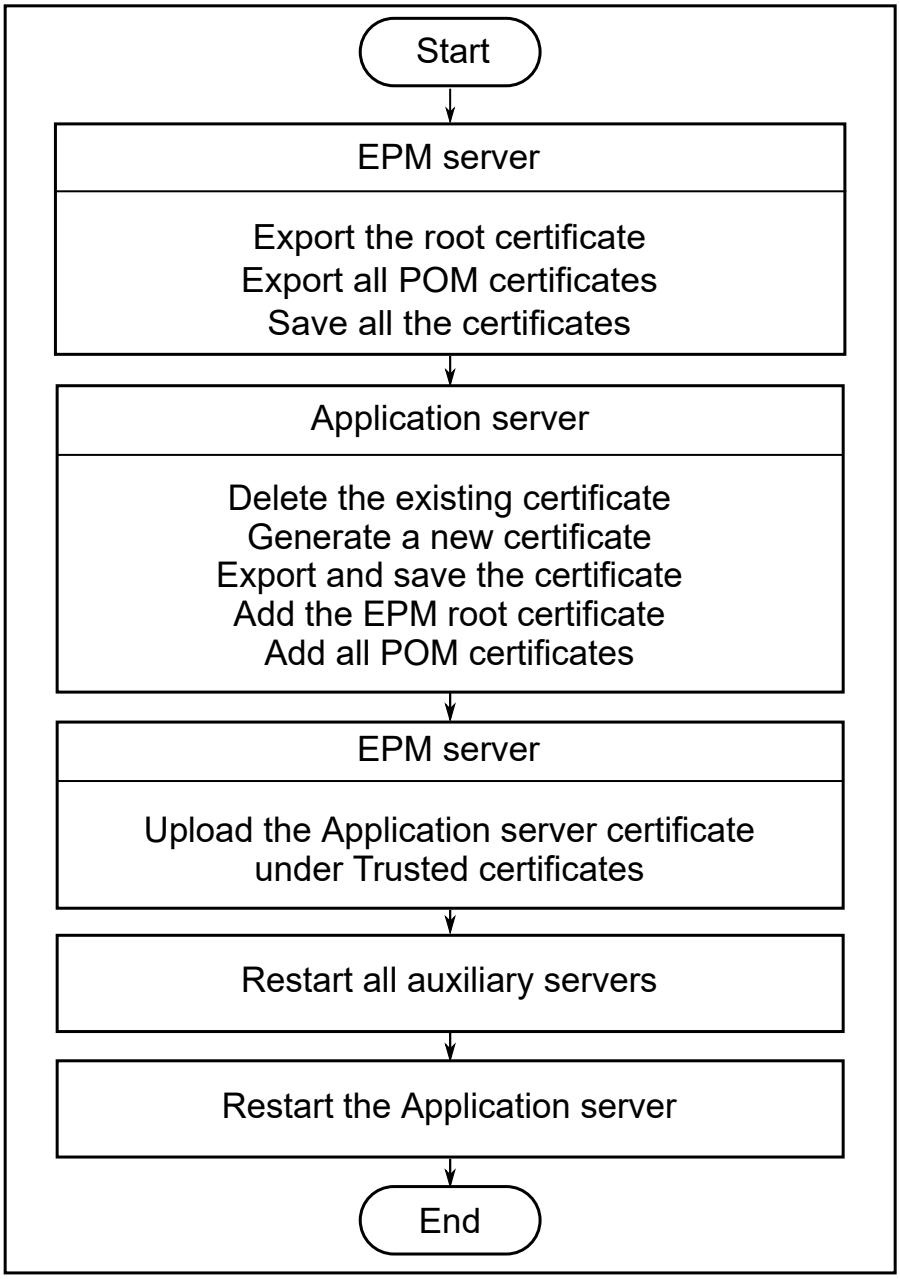

Figure 2: Exchange and configure certificates on multiple POM servers

Process flow to exchange and configure certificates on multiple Application servers

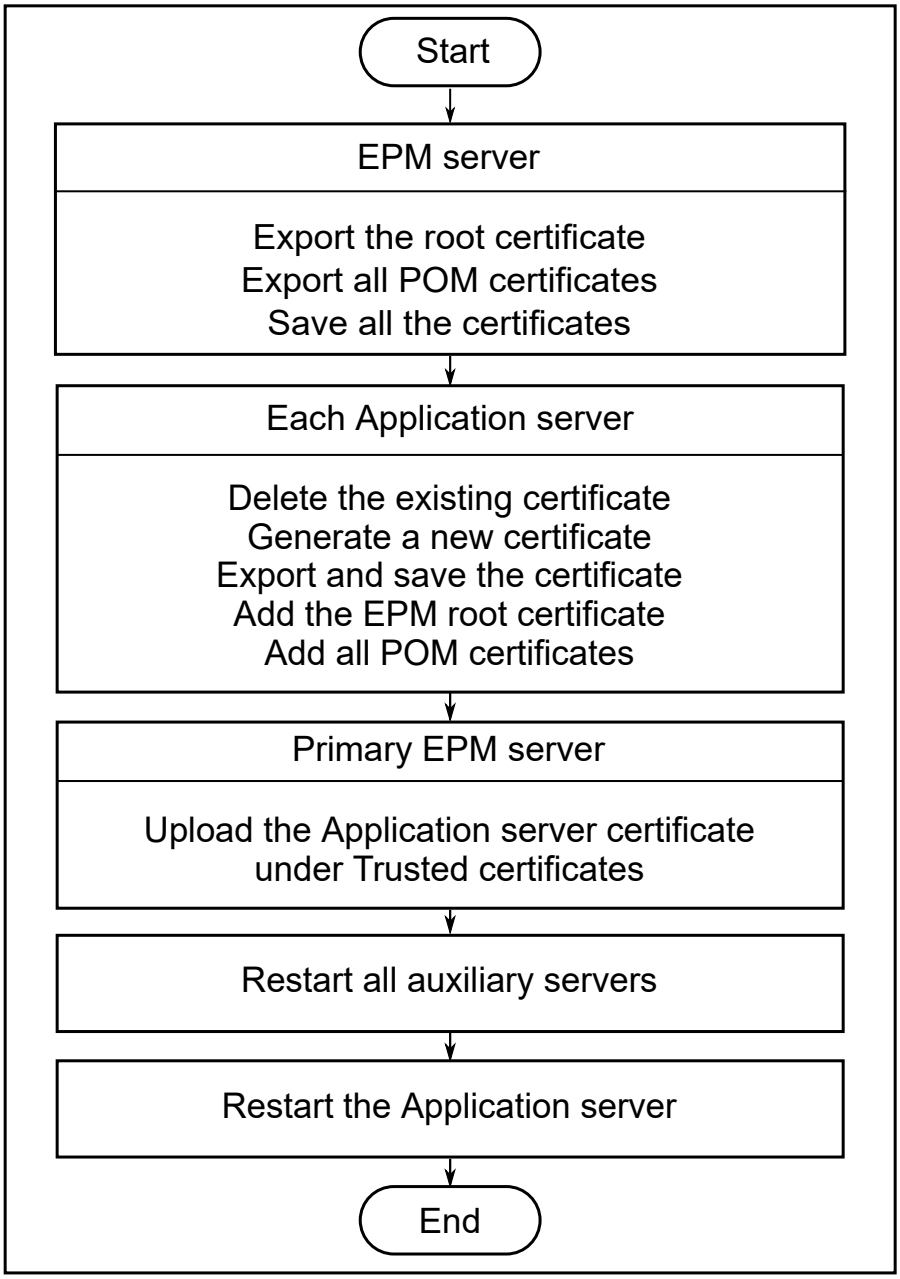

Figure 3: Exchange and configure certificates on multiple Application servers

Exchanging and configuring certificates

About this task

Use this procedure to exchange and configure certificates for Avaya Orchestration Designer on a single or multiple application servers.

Important:

For multiple application servers, repeat all steps for each application server.

Before you begin

Configure the POM database.

Procedure

1. Using the browser window, log in to the EPM as an administrator.

   Note:

   For multiple POM servers, log in to the primary EPM.

2. In the navigation pane, click **Security** > **Certificates**.
3. On the **Root Certificates** tab, click **Export**, and then save the certificate on the local system.
4. In the navigation pane, click **Proactive Outreach** > **Manager**.
5. Click **Configurations** > **Servers**.
6. Click **Export** on the listed certificate tab and save it on your local system.

   Note:

   For multiple POM servers, you must export and save all the POM certificates.

7. You can install the Avaya Orchestration Designer application server on the same server where you install POM. In such cases the IP address of the application server and the IP address of the EPM primary server is the same. The default port is 7443. If you are using an external application server and you have installed POM Avaya Orchestration Designer application package then while installing POM, you must:

   a. Copy the `*.war` files from `$POM_HOME/DDapps` to `$APPSERVER_HOME/webapps` of the external application server.

   b. If the file `log4j-1.2.15.jar` is present in `$CATALINA_HOME/lib`, then delete it from your external application server.

      Note:

      The Primary server folder `$POM_HOME/DDapps/lib*` and the External Application Server folder `$CATALINA_HOME/lib` must contain the same files. If the External Application Server folder `$CATALINA_HOME/lib` contains any other

files than the Primary server folder `$POM_HOME/DDapps/lib`, ensure you keep only JAR versions of files that are available in `$POM_HOME/DDapps/lib`.

c. Copy files from `$POM_HOME/DDapps/lib/*` to `$APPSERVER_HOME/lib` of your external application server. After copying the files, edit `$APPSERVER_HOME/conf/server.xml` and add the following:

```
<Connector protocol="HTTP/1.1"
port="7443" minSpareThreads="5" maxSpareThreads="75"
enableLookups="true" disableUploadTimeout="true"
acceptCount="100"  maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="/opt/AppServer/Tomcat/tomcat/conf/myTrustStore"
keystoreType="JKS" keystorePass="changeit"
clientAuth="false" sslEnabledProtocols="TLSv1.2"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_G
CM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_12
8_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_EMPTY_RENEGOTIATION_IN
FO_SCSV"/>
```

Note:

d. In the Command Line Interface (CLI), navigate to `$APPSERVER_HOME/conf`.

e. Run the command **`keytool -keystore myTrustStore -genkey -alias dummy -keyalg RSA`**

f. Type the password as `changeit` and type other appropriate details.

8. Using the browser window, log in to the Avaya Orchestration Designer application server by specifying the URL *https://<application server IP address>:port number/runtimeconfig* using the default user name and the password as *ddadmin*.

   The system prompts to set runtimeconfig password at the first login to the local application server.

9. On the Avaya Orchestration Designer web interface, do the following:

   a. In the navigation pane, Click **Certificates**.

   b. On the Certificates page, select the default certificate and click **Delete**.

   c. Click **Change**.

      The system displays Change Keystore page.

   d. In the **Keystore Path** field, type *`Absolute-path appserver-home>/conf/myTrustStore`*.

      If you have installed the application server on the same server where you install POM, then the *<Absolute-path-appserver-home>* is set in the *{$APPSERVER_HOME}* environmental variable.

   e. In the **Password** field, type `changeit`.

Note:

To use a different trust store and the password, change the *Absolute-path-appserver-home>/conf/server.xml* file accordingly, and ensure that the *server.xml* keystore path is valid and matches with Avaya Orchestration Designer application certificate as *<Absolute-pathappserver-home>/conf/myTrustStore.*

f. In the **Confirm** field, type `changeit`.

g. Click **Save**.

h. On the Certificates page, click **Generate**.

i. Enter the appropriate values in all fields. Input for all fields is mandatory. You can enter any custom defined values.

Note:

For SAN field, enter the values in the `IP:<IP address> or DNS:<hostname>` format.

The self-signed certificate is valid only for 1186 days.

The Common Name (CN) field should have Hostname/FQDN.

If Enable Server Identity Validation parameter is set to Yes under the security settings, in the Certificate tab of the Experience Portal, then you must have Hostname/FQDN set in SAN field.

If you have configured orchestration designer applications with the URI containing the IP address under the **Applications** tab of the system configuration in the Experience Portal, then you must have the IP address set in the SAN field.

j. Click **Continue**.

The system displays the Certificates page.

k. Click **Save**.

l. Click **Add**.

The system displays the Add Certificate page.

m. Type a name for the EPM certificate and browse to find the path where you saved the primary EPM root certificate exported in step 3.

n. Click **Continue**.

The system displays the Certificates page.

o. Click **Save**.

p. Select the application server self-signed certificate generated and export the certificate on your local system.

q. Click **Fetch** to fetch the primary EPM certificate.

The system displays the Add Certificate page.

Note:

In a multiple POM server environment, you must fetch the primary EPM certificate from all auxiliary EPM servers.

If EPM certificate signing is disabled using the **Disable Signing** button from **Security** > **Certificate** > **EP signing certificate** and custom CA signed certificates are used, you must import all the CA certificates into POM truststore using POM trusted certificates page under Configurations.

If EPM signing is enabled, you must import the EP root certificate, that is, EP signing certificate, into POM trust store using POM trusted certificate page.

r. In the **Name** field, type the name of the certificate. For example, axis_prim or axis_aux.

s. In the **Enter Certificate Path** field, type the client URL as *https://<EPM IP address>/axis2*.

The Avaya Orchestration Designer application fetches the axis2 certificate and adds it to the list of certificates.

t. Click **Continue**.

The system displays the Certificates page.

u. Click **Save**.

a. Click **Add**.

The system displays the **Add Certificate** page.

b. In the **Name** field, type a name of the POM certificate.

c. In the **Enter Certificate path** field, click **Browse** and browse the path where you saved the certificate exported in the step 6.

d. Click **Continue**.

The system displays the Certificates page.

e. Click **Save**.

f. Restart the application server.

10. Using the browser window, log in to the primary EPM as administrator.
11. Click **Security** > **Certificates**.
12. Click the **Trusted Certificates** tab and do the following:

a. Click **Upload**.

b. On the Upload Trusted Certificate page, type the name and browse the path where you have saved the certificate exported in step 9p.

c. Click **Continue**.

The system displays the Certificates page.

d. Click **Save**.

e. Click **Import**.

The system displays the Import Trusted Certificate page.

f. On the Import Trusted Certificate page, type the name and type the axis2 certificate path as *https://<EPM Server IP address>/axis2*.

For a multiple POM server environment, you must fetch the primary EPM certificate from all auxiliary EPM servers.

g. Click **Continue**.

The system displays the Certificates page.

h. Click **Save**.

13. Using the browser window, log in to the EPM as an administrator.

Note:

For multiple POM servers, log in to the primary EPM.

14. In the navigation pane, click **Proactive Outreach** > **Manager**.
15. Click **Configurations** > **Trusted Certificates**.
16. Import the certificate exported in step 9h.
17. In the **Name** field, type the name of the certificate. For example, appserver.
18. Click **Continue**.
19. Click **Save**.
20. Restart the application server, all MPPs, and all auxiliary servers.

Checking the POM server installation status

About this task

Use this procedure to check the POM server installation status on the primary or auxiliary server.

Before you begin

Configure at least one POM server.

Procedure

1. Log in to EPM as an administrator.
2. In the left pane, select **Proactive Outreach** > **Manager**.
3. In the drop-down menu, click **Configurations > Servers > POM Manager**.
4. Check whether the status of POM Campaign Manager is Running.

5. Log in to the CLI of the EPM as a root user.
6. Type `POM status`. Ensure that this command returns a confirmation from the system that the Campaign Manager, Campaign Director, Agent Manager and Rule Engine, Advance List Management, Kafka server, and Agent SDK are running successfully.

   The POM service is a wrapper service around the Campaign Manager and Campaign Director. You can start and stop or get the status of these services.

   You can also use **"journalctl –f –u <service name>"** to check the beginning date and time of the logs.

   - To start, stop, and get the status of the POM Manager service

     - `POM start`
     - `POM stop`
     - `POM status`

   On the command prompt, type the following commands to start, stop, or get the status of the services such as Advance list management, Kafka server, and Agent SDK.

   - To start, stop, and get the status of the Campaign Manager service you can use **systemctl start <service name>** or **service <service name> start** .

     For example, for campaign manager you can use **systemctl start cmpmgr** or **service cmpmgr start** .

     - `service cmpmgr start`
     - `service cmpmgr stop`
     - `service cmpmgr status` or `cmpmgrstatus`
   - To start, stop, and get the status of the Campaign Director service, type:

     - `service cmpdir start`
     - `service cmpdir stop`
     - `service cmpdir status` or `cmpdirstatus`
   - To start, stop and get the status of the Agent Manager, type:

     - `service agtmgr start`
     - `service agtmgr stop`
     - `service agtmgr status` or `agtmgrstatus`
   - To start, stop and get the status of the Active MQ, type:

     - `service pomactmq start`
     - `service pomactmq stop`
     - `service pomactmq status` or `pomactmqstatus`

- To start, stop and get the status of the Rule Engine, type:
  - `service ruleeng start`
  - `service ruleeng stop`
  - `service ruleeng status` or `rulengstatus`
- To start, stop and get the status of the POM Kafka, type:
  - `service pomkafka start`
  - `service pomkafka stop`
  - `service pomkafka status` or `pomkafkastatus`
- To start, stop and get the status of the Advance List Management, type:
  - `service advlistmgmt start`
  - `service advlistmgmt stop`
  - `service advlistmgmt status` or `advlistmgmtstatus`
- To start, stop and get the status of the POM Agent SDK, type:
  - `service pomagentsdk start`
  - `service pomagentsdk stop`
  - `service pomagentsdk status` or `pomagentsdkstatus`
- To start, stop, and get the status of POM dashboard service, type:
  - `service pomdashboard start`
  - `service pomdashboard stop`
  - `service pomdashboard status` or `pomdashboardstatus`
- To start, stop, and get the status of POM zookeeper service, type:
  - `service pomzookeeper start`
  - `service pomzookeeper stop`
  - `service pomzookeeper status`

Adding users to the POM system

About this task

By default, the Avaya Experience Portal administrator has all POM privileges. The administrator can add new users similar to that in Avaya Experience Portal.

Before you begin

POM installation must be in running status.

Procedure

1. In the navigation pane, click **User Management** > **Users**. You can add a new user or assign the following POM administration privileges to a user:
   - POM Administration
   - POM Campaign Manager
   - Org POM Campaign Manager

     Note:

     Org POM Campaign Manager privilege is available only if organizations are enabled on Avaya Experience Portal.
   - POM Supervisor
   - Org POM Supervisor

     Note:

     Org POM Supervisor privilege is available only if organizations are enabled on Avaya Experience Portal.
2. Log off and log in with the user credentials that you create.

   The action ensures that the changes are in effect.

   When you assign the POM administration privileges, you can view the POM menu options in the left pane of EPM.

Changing the Home country setting

Before you begin

Ensure that you set the Home country at initial installation and do not change the Home country setting.

Procedure

1. In the navigation pane of Experience Portal, click **Proactive Outreach** > **Manager** > **Configurations** > **Global Configurations**.
2. In the Contact settings, select a **Home country**.
3. Click **Apply** to save the change.

Provisioning a Kafka server

When you enable an event SDK in the POM system, POM stores the events at the following location:

`$POM_HOME/kafka_server/kafka-store`

By default, POM keeps event-specific data of the last seven days in the `kafka-store` file and generates approximately 50 GB of data per one million attempts. Therefore, you must provision disk space on the POM server.

To reduce the disk requirement, you can reduce the retention period and the purge interval of the Kafka server.

The default retention period is three days (72 hours). To modify the retention period, you can set the properties in the following files:

File name	Property name
server.properties	`log.retention.hours` = *72*
zookeeper.properties	`autopurge.purgeInterval` = *168*

Upgrading Kafka

Before you begin

- Refer to the Zookeeper/Kafka upgrade documentation for detailed steps on backup and restore the kafka config and event data.
- Refer Kafka documentation on how to backup and restore of event data.
- Confirm that the Kafka and Zookeeper version are in sync with the Kafka and Zookeeper installed with POM server.

Procedure

1. Back up all configuration files before upgrading. This includes, for example, /kafka, /kafka-rest, and /etc/schema-registry.
2. Event Data Backup: In the case of POM server, the event data is stored at $KAFKA_HOME/kafka-store/kafka location. Take a backup of the kafka-store directory.

   Note:

   The location may vary.
3. Upgrade the software by following instructions available at https://kafka.apache.org/10/documentation/streams/upgrade-guide.
4. Update the server config to match with the older one.
5. Restore the event data.
6. Start the zookeeper and kafka server.

Creating appserver.service

Before you begin

Use this procedure if you are using an application server installed locally on any of the primary or auxiliary POM servers.

Procedure

1. On POM system where application server is installed and is being used, verify whether the `appserver.service` file exists. Use the command **`ls -l /etc/systemd/system/appserver.service`**.

   If the file exists, you do not need to take any further action.

2. If the file is not present, ensure the following environment variables are set:

   a. echo $APPSERVER_HOME

   b. echo $VP_HOME

3. Ensure that each command mentioned in step 2 returns a valid path.

4. If the paths are valid, run the command: **`sed "s@%%APPSERVER_HOME%%@$APPSERVER_HOME@" $VP_HOME/Support/AppServer/appserver.service > /etc/systemd/system/appserver.service`**

Chapter 4: Configuring POM

Checklist for configuring a POM server

Planning tasks

Perform the following planning tasks.

No.	Task	Reference	Notes	✔
1	Enable FIPS.	See Enabling FIPS on page 32.	You can enable FIPS in Proactive Outreach Manager after installing Proactive Outreach Manager. Enabling FIPS is optional.	
2	Configure the POM servers.	See Configuring the POM server on page 36.	After you install the POM server, configure the POM server using the web interface.	
3	Configure Avaya Aura® Call Center Elite or Avaya Aura® Contact Center.	See *Administering Avaya Proactive Outreach Manager*.	Integrate POM with Avaya Aura® Call Center Elite or Avaya Aura® Contact Center for agent functionality and running agent-based campaigns.	
4	Add users or assign POM specific privileges to existing users.	See Adding users on page 27.	Add users after adding the POM server.	
5	Change the default country setting.	See Changing Home Country on page 28.	Change the default country to a country of your choice.	
6	Exchange certificates for the Avaya Orchestration Designer application server.	See Exchanging certificates for Avaya Aura® Orchestration Designer application server on page 21.	To use the Avaya Orchestration Designer application server, you must exchange certificates between each application server and POM.	
7	Configure the application server.	See Configuring the applications and licenses on page 38.	Specify the external applications and license requirements.	

Enabling FIPS

About this task

Use this procedure to enable FIPS mode in Proactive Outreach Manager. The following changes occur when you enable FIPS on POM:

- The Fetch button on POM Trusted Certificates page is disabled. Use the Import button instead for any operations related to fetching the certificates.
- Existing certificate stores convert from `JKS` format to `BCFKS` format as follows:
  - `pomKeyStore` converts to `pomKeyStore.bks`.
  - `pomTrustStore` converts to `pomTrustStore.bks`.

  POM uses the new formats.

If you enable FIPS on the primary server, you must enable FIPS on the auxiliary server.

Procedure

1. Log in to the POM server as a root user.
2. Stop the VPMS, POM, and APPSERVER processes.
3. Run the following command on the POM server to enable FIPS:

   ```
   $POM_HOME/bin/POM_FIPS_setup.sh
   ```

4. Reboot the POM system.

Configuring the POM database on the primary POM server

About this task

Use this procedure to configure the POM database only on the primary POM server. For the auxiliary POM server, you do not need to configure the POM database explicitly. When you add an auxiliary POM server from the POM Servers page, the auxiliary server can access the database.

Before you begin

Complete POM implementation.

Procedure

1. Determine the type of database and the server where you want to install the database. For example, a local server for lab environment or an external server for production environment.

   Tip:

   When you install the POM database schema on a local or an external database, you are responsible for the administration of the database.

2. Create a database instance for the POM database.
3. For the external postgres server, in the `pg_hba.conf` file located at `/var/lib/pgsql/data/`, type the IP address of the POM server.

   Note:

   If you edit the `pg_hba.conf` file, restart the postgres service by running the **`postgresql restart`** command.
4. For a secure database connection, add the third-party certificate in the POM Truststore by using **`$POM_HOME/bin/importCertInPomTruststore.sh`**

   For more information, see the section on Importing Certificate in POM truststore through Command Line Interface in *Implementing Avaya Proactive Outreach Manager*.
5. Configure a desired server such as Postgres, Oracle, or Microsoft SQL Server.

   For installing Oracle drivers and Microsoft SQL drivers, see the instructions in the chapter *Installing POM*.
6. Log in to the primary EPM as a root or sroot user.
7. Type `cd $POM_HOME/bin` and press `Enter`.
8. Type `./installDB.sh` and press `Enter`.

   The system displays the following message:

   ```
   Please select Contact Center Configuration mode from the following options:
   1. CCElite
   2. AACC-SBP [Skills-Based Pacing for Agentless POM]
   3. None
   4. AACC [Integrated & Blending]
   5. Oceana
   6. CCaaS-Outbound
   ```
9. Type `1` ,`2`, `3`, `4`, `5` or `6` and press `Enter`:

   The system displays the following message:

   ```
   This script can modify $POM_HOME/config/PIMHibernate.cfg.xml or Test the DB connection.
   Do you like to continue? (y/n)
   ```
10. Type `y` and press `Enter`.

    The system displays the following message:

    ```
    Please select from one of the following choices:
    1. Test DB Connection
    ```

```
2. Create POM Schema on the given DB
3. Save database configuration
4. Configure database settings
5. Configure database settings for reports (Optional)
6. Exit from this utility
```

Type `4` and press `Enter`.

11. Type the database type. You can configure a Postgres, Oracle, or Microsoft SQL server. For installing Oracle drivers and Microsoft SQL drivers, see the instructions in the chapter *Installing POM*.
12. If you select the `MSSQL` database, do the following:
    a. The system displays the following message `Do you want to enable the POM Geo configuration? Please select(y/n)`, type `y` to enable Geo-redundancy.

       POM supports Geo-Redundancy on Standard/Enterprise edition of MS SQL database.

       If you enable Geo-redundancy, POM displays the Data Center Configuration page. For details, see *Administering Avaya Proactive Outreach Manager*.
    b. Type the Availability Group Listener FQDN.
    c. For all other databases, type the database server IP address or hostname.
13. Type the port number.

    The default port is 5432 for Postgres database, 1521 for Oracle database, and 1433 for Microsoft SQL Server.
14. If you select the database type as `MSSQL`, then the system displays the following message:

    ```
    Please select an option connecting to MSSQL DB using SQL Server or
    Windows Authentication.
    1.SQLServer
    2.Windows
    Enter an option (1/2):
    ```

    If you select the database type as `Oracle`, then the system displays the following message:

    ```
    Please select an option connecting to Oracle DB using SID or
    Service Name.
    1.SID
    2.Service Name
    Enter an option (1/2):
    ```

    Type the appropriate option and press `Enter`.

15. Type the name of the database.
16. Type the username and password to connect to the database.

    The POM system displays the message:

    ```
    Does Database require secured connection (Y/N):
    ```

    Note:

    To configure the Microsoft SQL Server database as a secured connection, type the hostname or FQDN of the database server.

17. To enable Secure Connection, type `y`, or to disable type `n`.

    POM displays the following message after the database connection is created:

    ```
    Please select from one of the following choices:
    1. Test DB Connection
    2. Create POM Schema on the given DB
    3. Save database configuration
    4. Configure database settings
    5. Configure database settings for reports (Optional)
    6. Exit from this utility
    ```

18. **(Optional)** Type `1` to verify the database connection.

    If the command returns `SUCCESS`, go to the next step.

    If the command returns `FAILURE`, the system displays the reason for failure on the console.

19. To create a POM schema on the specified database, type `2`

    The system displays the following message:

    ```
    Do you want to save the values on the config file(y/n)?
    ```

    To save the values in the configuration file, type `y`.

    It creates the POM schema. You cannot use the database immediately, unless you save this configuration by using option 3 because EPM restarts after you save the configuration.

20. To reconfigure the settings, such as changing the login credentials, the type of the database, the server IP address or the hostname, or the port number, type `4`.
21. POM displays the following message after the database connection is created:

    ```
    Please select from one of the following choices:
    1. Test DB Connection
    2. Create POM Schema on the given DB
    3. Save database configuration
    ```

```
4. Configure database settings
5. Configure database settings for reports (Optional)
6. Exit from this utility
```

To exit, type `6`.

Caution:

Ensure that the POM and VPMS services are not running before you restart your database.

22. For any errors or exceptions, see the log file at `$POM_HOME/logs/installDB.log`.

    For information about configuring a separate database for POM reports, refer Configuring separate database for POM Reports in *Implementing Avaya Proactive Outreach Manager guide*

Configuring the POM server

About this task

POM runs with both the primary and the auxiliary EPM. Use this procedure to configure the POM server on the primary EPM and perform similar steps for auxiliary servers.

Before you begin

Avaya Experience Portal uses Network Time Protocol (NTP) to control and synchronize the clocks when the EPM, POM software, and POM database are running on different servers. The POM database server and the primary EPM refer to the same time source to sync with each other. The auxiliary EPM can point to the primary EPM as a reference clock. The time and the time zones on all systems must be the same.

Procedure

1. Log in to the web interface by using Avaya Experience Portal administrator credentials. The Avaya Experience Portal administrator role inherits all POM specific roles.
2. In the navigation pane, click **Proactive Outreach** > **Manager**.
3. Click **Configurations** > **Trusted Certificates**, and do the following:
   a. To fetch an Avaya Experience Portal certificate, click **Fetch**.
   b. In the **Name** field, type the unique name of an EPM certificate.
   c. In the **Location** field, type `https://<EPM IP Address>`.
   d. Click **Continue**.

      The system adds the Avaya Experience Portal certificate.

4. Click **Configurations** > **Servers**, and do the following:
    a. To add the POM server, click **Add**.
    b. Type the POM server name and IP address.

       After you configure the POM server, you can change the IP address of the POM server. For more information, see *Administering Avaya Proactive Outreach Manager*.
    c. Click **Continue**.
    d. Select the **Trust this certificate** check box.
    e. Click **Save**.
5. Click **Configurations** > **Servers** > **Outbound Settings** > **EPM** and provide the user name and password with Outcall privileges.
6. Click **Save**.
7. To start POM Manager, click **Configurations** > **Servers** > **POM Manager**.
8. If you have enabled Geo-redundancy, do the following:
    a. Click **Proactive Outreach** > **Data Center Configuration**.
    b. Click **Add**.

       The system displays the Add data center group page.
    c. In the **Group Name** field, type the name of the data center.
    d. Select the **Active** or **Standby** for the **Mode** button.
    e. Click **Save**.

       You can add only one active data center.

Configuring the POM server after enabling geo-redundancy

Procedure

1. Log on to Avaya Experience Portal by using the credentials of an administrator.
2. In the navigation pane, click **Proactive Outreach** > **Manager**.
3. Click **Configurations** > **Data Center Configuration**.
4. Click **Add**.

   The system displays the Add data center group page.
5. In the **Group Name** field, type the name of a data center.

6. In the **Mode** field, click one of the following:
   - Click **Active** to configure the selected data center as an active data center.

     You can configure only one active data center.
   - Click **Standby** to configure the selected data center as a standby data center.
7. Click **Save**.

Configuring applications and licenses

Before you begin

If you are using an external application server, ensure that you install Java 1.8.0_121 and Apache Tomcat version 8.5.11 and later.

Procedure

1. Log in to EPM using the username and password provided during the Avaya Experience Portal installation.
2. To configure the applications locally on primary or auxiliary EPM using the web interface, in the left pane, click **System Configuration** > **Applications**. All application names, except PomDriverApp and Nailer, are case-sensitive. You must spell the application names exactly as follows:
   a. PomDriverApp: *https://<application server ip>:port-number-configured-on-application-server/PomDriverApp/ccxml/start.jsp* where the application type is POM:Driver, Enable TTS, Outbound Type
   b. Nailer:*https://<application server ip>:port-number-configured-on-application-server/Nailer/ccxml/start.jsp* Application Type= POM:Nailer, Outbound Type
   c. AvayaPOMNotifier: *https://<application server ip>:port-number-configured-on-application-server/AvayaPOMNotifier/Start* Application Type = POM:Application/VXML, Outbound Type
   d. AvayaPOMAnnouncement: *https://<application server ip>:port-number-configured-on-application-server/AvayaPOMAnnouncement/Start* Application Type = POM:Application/VXML, Outbound Type
   e. AvayaPOMAgent: *https://<application server ip>:port-number-configured-on-application-server/AvayaPOMAgent/Start* Application Type = POM:Application/VXML, Outbound Type
   f. AvayaPOMSMS: *https://<application server ip>:port-number-configured-on-application-server/AvayaPOMSMS/Start* Application Type = SMS, Inbound Type
   g. AvayaPOMEmail: *https://<application server ip>:port-number-configured-on-application-server/AvayaPOMEmail/Start* Application Type = Email, Inbound Type

Note:

You must configure at least one application with the name Nailer and PomDriverApp respectively with POM:Nailer and POM:Driver type.

For a multi zone setup, configure minimum one nailer application and one driver application on a POM system for each zone.

For an organization enabled system, you must configure both the `Nailer` and `PomDriverApp` applications for the default organization for each zone.

Each organization in the zone must have the same URL.

3. The following steps are to configure the Avaya Orchestration Designer applications only locally on primary EPM using the `$POM_HOME/bin/insert_POM_Apps.sh` script. This step is not applicable for configuring auxiliary EPM setup. In case the application server is local to EPM, the IP address of the aux hosting the application server must be mentioned as an alternate IP in the applications configuration.
   a. Log in to command line interface using root credentials.
   b. Type `cd $POM_HOME/bin`.
   c. Type `./insert_POM_Apps.sh`
   d. Type the EPM web administrator username.
   e. Type the EPM web administrator password.
   f. Reenter the password for verification.
   g. Type the IP address of the EPM application server on which the Avaya Orchestration Designer applications are installed.
   h. On web user interface click **System Configurations** > **Applications** to verify the applications added by Avaya Experience Portal.
   i. Select **PomDriverApp**, and from the Speech Servers option, select the TTS resource and add a selected voice.
4. If you use an external application server, do the following:
   a. Copy the `*.war` files from *$POM_HOME/DDapps* to *$CATALINA_HOME/webapps* of the application server.
   b. If the file `log4j-1.2.15.jar` is present in `$CATALINA_HOME/lib`, then delete it from your external application server.

      Note:

      The Primary server folder `$POM_HOME/DDapps/lib*` and the External Application Server folder `$CATALINA_HOME/lib` must contain the same files. If the External Application Server folder `$CATALINA_HOME/lib` contains any other files than the Primary server folder `$POM_HOME/DDapps/lib`, ensure you keep only JAR versions of files that are available in `$POM_HOME/DDapps/lib`.

c. Copy files from *$POM_HOME/DDapps/lib/** to *$CATALINA_HOME/lib* of the application server.

d. Edit `<APPSERVER_HOME>/conf/server.xml` and add the following connector node:

```
<Connector protocol="HTTP/1.1" port="7443" minSpareThreads="5"
maxSpareThreads="75" enableLookups="true" disableUploadTimeout="true"
acceptCount="100"  maxThreads="200" scheme="https" secure="true"
SSLEnabled="true" keystoreFile="/opt/AppServer/Tomcat/tomcat/conf/
myTrustStore" keystoreType="JKS" "keystorePass="changeit" clientAuth="false"
sslEnabledProtocols="TLSv1.2"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_G
CM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_12
8_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_EMPTY_RENEGOTIATION_IN
FO_SCSV"/>
```

e. Edit `<APPSERVER_HOME>/bin/catalina.sh` file to append the *JAVA_OPTS* variable `export JAVA_OPTS="$JAVA_OPTS -Dorg.xsocket.connection.client.ssl.sslengine.enabledProtocols=TLSv1.2”`. If it is not defined, then declare new *JAVA_OPTS* variable `export JAVA_OPTS="-Dorg.xsocket.connection.client.ssl.sslengine.enabledProtocols=TLSv1.2"`

5. Restart the external application server.

Note:

The Primary server folder `$POM_HOME/DDapps/lib*` and the External Application Server folder `$CATALINA_HOME/lib` must contain the same files. If the External Application Server folder `$CATALINA_HOME/lib` contains any other files than the Primary server folder `$POM_HOME/DDapps/lib`, ensure you keep only JAR versions of files that are available in `$POM_HOME/DDapps/lib`.

6. Use Avaya WebLM to configure the license information for POM. Configure licenses for the following three channels:
   - SMS channel: Sends SMS using Short Message Peer-Peer Protocol (SMPP). Ensure you have an SMS channel configured license on Avaya Experience Portal.
   - Email channel: Sends email messages using Simple Mail Transfer Protocol (SMTP). Ensure you have an email channel configured license on Avaya Experience Portal.
   - Voice channel: Assigns various Avaya Orchestration Designer applications for live voice or answering machine as part of the contact strategy.
7. Specify the hostname or IP address of the License Server with the port number on Avaya Experience Portal. The administrator allocates licenses for telephony ports, ASR, and TTS connections.

Chapter 5: Upgrade fallback

Rolling back from POM 4.0.2 to 4.0.1

About this task

Use this procedure to change the state of the POM database to a pre-upgrade state after an upgrade of the database fails.

If an upgrade of the POM database fails due to a power outage, restart the POM server.

There is no data loss while changing the state of the POM database to a pre-upgrade state.

Procedure

1. Ensure that the system displays the following console message:

```
POM Upgrade Failed! System can be restored to pre-upgrade version
[POM.04.00.01.00.00.xxx].
Upon POM.04.00.01.00.00.xxx restore completion, it is recommended user to restore
the POM database manually.
Do you want to continue with restore [y/n]? (y/n)
```

2. To rollback, type `y`.

   The system begins to restore the pre-upgrade POM version and displays the following message:

```
-----------------------------------------
POM 4.0.1 restore process completed successfully.
-----------------------------------------------
Please restore the POM Database.
Moving installation log files to: /opt/Avaya/avpom/POManager/logs

================================================================
===

If you are using an external application server and you have
installed the POM DD/AAOD
Application package while installing POM, you need to:
a--> Copy the *.war files from $POM_HOME/DDapps to $CATALINA_HOME/
webapps of the external application server
b--> Copy files from $POM_HOME/DDapps/lib/* to $CATALINA_HOME/lib
of your external application server.
c--> Enable the SSL configurations for application server.
d--> Restart the external application server.

================================================================
```

```
===
Please restart the system now!
```

3. Reboot the system.

Chapter 6: Resources

Documentation

You must install Avaya Experience Portal before you install POM. You will find references to Avaya Experience Portal documentation at various places in the POM documentation.

For information about the POM feature administration, interactions, considerations, and security, see the POM documents mentioned in the following table. The following documents are available on the Avaya Support site at: https://support.avaya.com

Title	Description	Audience
Overview		
Avaya Proactive Outreach Manager Overview and Specification	Provides general information about the product overview and the integration with other products.	Users
Implementing		
Implementing Avaya Proactive Outreach Manager	Provides information about installing and configuring Proactive Outreach Manager.	Implementation engineers
Implementing Avaya Experience Portal on a single server	Provides procedures to install and configure the Avaya Experience Portal software on a single server.	Implementation engineers
Implementing Avaya Experience Portal on multiple servers	Provides procedures to install and configure the Avaya Experience Portal software on two or more dedicated servers.	Implementation engineers
Administering		
Administering Avaya Experience Portal	Provides general information about and procedures for administering and configuring specific Experience Portal functions and features using a web-based interface.	Implementation engineers
Administering Avaya Proactive Outreach Manager	Provides general information about field descriptions and procedures for administering Proactive Outreach Manager.	System administrators and Users
Using Avaya Workspaces for Avaya Proactive Outreach Manager	Provides instructions on using Avaya Workspaces for Proactive Outreach Manager.	Users

Table continues…

Title	Description	Audience
Using Avaya Proactive Outreach Manager supervisor dashboard	Provides instructions on using Proactive Outreach Manager supervisor dashboard.	Supervisors
Upgrading		
Upgrading Avaya Experience Portal	Describes how to upgrade to Experience Portal.	Implementation engineers
Troubleshooting		
Troubleshooting Avaya Proactive Outreach Manager	Provides general information about troubleshooting and resolving system problems, and detailed information about and procedures for finding and resolving specific problems.	System administrators Implementation engineers Users

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Login** at the top of the screen and then enter your login credentials when prompted.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Choose Release**, select the appropriate release number.

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

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

Support

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

Index