



Avaya Proactive Outreach Manager Integration

Release 4.1
Issue 1
November 2025

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

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](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](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](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	8
Purpose	8
Change history	8
Chapter 2: Configuring Avaya Aura® Communication Manager	10
Overview	10
Checklist	10
Log in to the Avaya Aura® Communication Manager server	11
Adding the IP Address of Session Manager	11
Adding an IP address of Call Management System	12
Making a connection between Communication Manager and Call Management System	13
Creating a signaling-group	14
Creating a Trunk group	15
Creating Hunt group	17
Adding the IP network region	18
Adding the IP codec set	19
Creating a CM login for POM in the CC Elite CTI configuration page	20
Chapter 3: Configuring Avaya Aura® Session Manager	21
Overview	21
Checklist	21
Adding SIP Entities	22
Adding SIP Entity for SIP Gateway or Session Border Controller	22
Adding SIP Entities for Communication Manager	23
Adding SIP Entity for Avaya Experience Portal	24
Adding SIP Entity links	24
Adding SIP Entity Link for SIP Gateway or Session Border Controller	24
Adding SIP Entity Link for Communication Manager	25
Adding SIP Entity Link for Avaya Experience Portal	26
Defining Policies and Time of Day	26
Adding Routing Policy for Communication Manager	26
Adding Routing Policy for Avaya Experience Portal	27
Dial Patterns	28
Adding dial patterns for Avaya Experience Portal and Communication Manager	28
Chapter 4: Configuring Avaya Experience Portal	30
Overview	30
Adding a SIP connection for Session Manager	30
Chapter 5: Configuring Call Management System	32
Overview	32
Checklist	32
Configuring Call Management System	32

Verifying the installation and configuration of the CMS rt_socket.....	34
Chapter 6: Configuring External Selection.....	36
Overview.....	36
Checklist.....	36
Configuring an external system on POM.....	37
Configuring external selection parameters.....	37
Deploying a .jar file from the External system on the POM server.....	38
Configuring external selection settings.....	39
External selection configuration page field descriptions.....	39
External system configuration page field descriptions.....	41
Chapter 7: Configuring External Application Server.....	42
Checklist.....	42
Configuring the POM database on the primary POM server.....	42
Configuring Apache Tomcat.....	46
Exchanging and configuring certificates.....	47
Configuring External Application Server- WebSphere.....	52
Configuring External Application Server- WebSphere version 8.5.5.....	53
Exchanging and configuring certificates for WebSphere application server.....	55
Chapter 8: Configuring Avaya Contact Recorder.....	60
Overview.....	60
Checklist.....	60
Adding ACR configuration on CM.....	63
Verify the Communication Manager license.....	63
Administering CTI link for TSAPI.....	64
Creating Universal Call ID (UCID).....	64
Administering Class of Restriction (COR).....	65
Administering Agent Stations.....	66
Administering Codec Set.....	66
Administering Network Region.....	67
Administering Virtual IP Softphones.....	68
Assigning Virtual IP Softphones to Network Region.....	70
Configuring AES for ACR.....	70
Administering TSAPI Link.....	70
Obtaining a Tlink Name.....	71
Obtaining H.323 Gatekeeper IP Address.....	71
Disabling Security Database.....	71
Restarting TSAPI Service.....	71
Administering Avaya Contact Recorder User for DMCC.....	72
Administering Avaya Contact Recorder User for TSAPI.....	72
Configuring Proactive Outreach Manager on Avaya Aura Application Enablement Services..	73
Verifying Avaya Aura® Application Enablement Services.....	73
Configuring POM.....	74
Enabling Work Force Optimization integration.....	74

Configuring POM Applications.....	74
ACR Configuration.....	74
Administering Recorder Information.....	74
Administering Contact Center Information.....	75
Administering Bulk Recording.....	75
Administering POM Interface.....	76
Chapter 9: Integrating POM with Avaya Oceana™	77
Overview.....	77
POM - Oceana Integration checklist.....	78
Loading and installing the OBService SVAR.....	79
Setting OBService attributes.....	80
OBService attributes.....	81
Importing the POM server certificate to Avaya Oceana® Cluster 3.....	82
Oceana Server page field descriptions.....	83
Adding trusted Certificate Authority certificates.....	83
Configuring an Outbound Provider.....	84
Enabling Callback feature.....	84
Adding Disposition Codes for Outbound contacts.....	85
Creating a user to handle Outbound contacts.....	85
Configuring After Contact Work time.....	87
Chapter 10: Integrating POM with Avaya Workspaces for Elite	88
Overview.....	88
Prerequisites.....	89
POM - Elite Workspaces Integration checklist.....	89
Exporting the Authorization Certificate from Breeze nodes.....	91
Importing authorization certificate to POM trusted certificate.....	91
Configuring POM system details on Avaya Aura® System Manager.....	92
POM system configuration field descriptions.....	92
Deploying POM widgets.....	93
Configuring an agent in Avaya Control Manager.....	96
Installing web server root certificate.....	96
Connector widget configuration.....	97
Customer Interaction Card.....	105
Changing Workspaces layout for an outbound enabled agent.....	105
POMAgentSDK failover.....	106
Agent Manager failover.....	107
Configuring POM Workspaces with WebRTC	107
Overview.....	107
Checklist for configuring Avaya Workspaces for Call Center Elite with remote WebRTC enabled agents.....	107
Chapter 11: Resources	109
Documentation.....	109
Support.....	110

Appendix A: Cipher requirements of Java implementation.....	111
Overview.....	111
Appendix B: TLSv1.2 configuration on WebSphere.....	112
Configuring TLSv1.2 on WebSphere.....	112

Chapter 1: Introduction

Purpose

This document provides information on how to integrate Avaya Proactive Outreach Manager with:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya Experience Portal
- Call Management System
- Avaya Contact Recorder
- Avaya Oceana®
- Avaya Workspaces for Call Center Elite
- Avaya Control Manager

This document is intended for users who want to integrate Avaya Proactive Outreach Manager with any of these products. Before starting the integrations, ensure you have working knowledge of these products. For more information, refer to the respective product documentation suite.

Change history

Issue	Date	Summary of changes
Release 4.0.2 SP 2, Issue 2.1	October 2023	Updated the topic for configuring POM database on primary POM server. Updated the topic Connector widget configuration. Updated the topic Deploying POM widgets. Updated the topic Configuring Apache Tomcat with a new cipher value. Updated the topic Exchanging and configuring certificates with a new cipher value.

Table continues...

Issue	Date	Summary of changes
Release 4.0.2, Issue 2.0	October, 2022	Updated the topic Connector Widget Configuration to add new parameters.
Release 4.0.1, Issue 1.0	August, 2021	Added the following topic on WebRTC integration: • Checklist for configuring POM Avaya Workspaces for Call Center Elite with remote WebRTC enabled agents.

Chapter 2: Configuring Avaya Aura® Communication Manager

Overview

Avaya Aura® Communication Manager is an open, highly-reliable, and extensible IP Telephony foundation on which Avaya delivers intelligent communications to large and small enterprises. Communication Manager is a core component of the Avaya Aura® platform and the foundation for delivering real-time voice, video, messaging, mobility, and other services.

Checklist

Use the following checklist to configure Avaya Aura® Communication Manager:

No.	Task	Description	✓
1	Log in to the Avaya Aura® Communication Manager server.	See Log in to the Avaya Aura Communication Manager server on page 11.	
2	Add the Session Manager IP address to Communication Manager node-names list.	See Adding the IP Address of Session Manager on page 11.	
3	Add an IP address of Call Management System to the node-names list of Communication Manager.	See Adding an IP address of Call Management System on page 12.	
4	Add the communication-interface processor-channels between Communication Manager and Call Management System.	See Making a connection between Communication Manager and Call Management System on page 13.	
5	Create a signaling-group on Communication Manager.	See Creating a signaling-group on page 14.	
6	Create a Trunk group	See Creating a Trunk group on page 15.	

Table continues...

No.	Task	Description	✓
7	Create Hunt group	See Creating Hunt group on page 17.	
8	Add the IP network region	See Adding the IP network region on page 18.	
9	Add the IP codec set	See Adding the IP codec set on page 19.	

Log in to the Avaya Aura® Communication Manager server

Log in to the Avaya Aura® Communication Manager server and select the SAT terminal type as **SUNT**.

For details on connecting to Avaya Aura® Communication Manager server using Putty, see *Administering Avaya Aura® Communication Manager* document.

Adding the IP Address of Session Manager

About this task

Configure Communication Manager to communicate with Session Manager. Add the Session Manager IP address to Communication Manager node-names list.

Procedure

1. Log in to the Communication Manager system and select the SAT terminal type as **SUNT**.
2. On the SAT session, in the **Command:** prompt, type `change node-names ip` and press **Enter**.

The system displays the IP NODE Names screen.

3. Use the **up** or **down** arrow key and scroll to a blank line.
4. In the **Name** column, type the name of the Session Manager server.
5. In the **IP address** column, type the IP address of the Session Manager Security Module.

* Note:

Do not use the management IP address in the **IP address** field.

The IP NODE Names screen displays the information similar to the following:

```
=====
change node-names ip                               Page 1 of 2
IP NODE NAMES
```

```

Name                IP Address
ASM_Server_Name    192.168.1.11
default             0.0.0.0
procr               192.168.1.12
procr6             ::

( 5 of 5 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
=====

```

6. Press **F3** key to save the changes.

Adding an IP address of Call Management System

About this task

Configure Communication Manager to communicate with Call Management System. Add an IP address of Call Management System to the node-names list of Communication Manager.

Procedure

1. Log in to the Communication Manager system and select the SAT terminal type as **SUNT**.
2. On the SAT session, in the **Command:** prompt, type `change node-names ip` and press Enter.

The system displays the IP NODE Names screen.

3. Use the **up** or **down** arrow key and scroll to a blank line.
4. In the **Name** column, type the name of the Call Management System.
5. In the **IP address** column, type the IP address of the Call Management System.

The IP NODE Names screen displays the information similar to the following:

```

=====
change node-names ip                                     Page 1 of 2
IP NODE NAMES
Name                IP Address
CMS_Server_Name    192.168.1.13
default             0.0.0.0
procr               192.168.1.12
procr6             ::

(5 of 5 administered node-names were displayed)
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
=====

```

6. Press **F3** key to save the changes.

Making a connection between Communication Manager and Call Management System

About this task

To receive the call center data from Communication Manager to Call Management System, you must establish a connection between Communication Manager and Call Management System. Add the communication-interface processor-channels between Communication Manager and Call Management System.

Procedure

1. Log in to the Communication Manager system and select the SAT terminal type as **SUNT**.
2. On the SAT session, in the **Command:** prompt, type `change communication-interface processor-channels` and press **Enter**.

The system displays the change communication-interface processor-channels screen similar to the following:

```
=====
change communication-interface processor-channels          Page 1 of 24
                                PROCESSOR CHANNEL ASSIGNMENT
Proc      Gtwy      Interface Destination      Session      Mach
Chan Enable Appl. To Mode Link/Chan Node      Port Local/Remote ID
1:  y    mis    s    pv4 5000  CMS_server 0      1      1
2:  n
3:  n
=====
```

3. Use the **up** or **down** arrow key and scroll to a blank line.
4. In the **Enable** column, type `y`.
5. In the **Appl.** column, type `mis`.
6. In the **Mode** column, type `s`.
7. In the **Link/Chan** column, type `pv4 5001` for procr.
Set the channel value between 5000 to 64500 for Ethernet.
8. In the **Node** column, type the node name of Call Management System.
9. In the **Port** column, type `0`.
10. In the **Local/Remote ID** column, type `1 1`.
11. Press **F3** key to save the changes.

Creating a signaling-group

About this task

Create a signaling-group on Communication Manager.

* Note:

You must create a separate SIP signaling group for BSR polling.

Procedure

1. On the SAT session, in the **Command: terminal**, type `add signaling-group n` and press **Enter**.

The system displays the **SIGNALING GROUP** screen.

The *n* is the signaling-group number.

2. Use the **up** or **down** arrow key and scroll to the **Group Type** option.
3. In the **Group Type** option, type `SIP` and press **tab** key.

The **SIGNALING GROUP** screen displays the information similar to the following:

```

=====
add signaling-group n                                     Page 1 of 1

SIGNALING GROUP

Group Number: 2          Group Type: sip
IMS Enabled? n          Transport Method: tcp
Q-SIP? n                SIP Enabled LSP? n

Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: Others

Near-end Node Name: procr          Far-end Node Name: ASM_SERVER_NAME
Near-end Listen Port: 5060        Far-end Listen Port: 5060
Far-end Network Region:

Far-end Domain:

Incoming Dialog Loopbacks: eliminate      Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload                 RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3        Direct IP-IP Audio Connections? y
Enable Layer 3 Test? n                   IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n    Initial IP-IP Direct Media? n
Alternate Route Timer(sec): 6

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
=====

```

4. Update the following values:

Group Type	SIP
Transport Method	TLS or TCP. * Note: Ensure that you set the same value for transport method while configuring Entity link on Session Manager
Near-end Node Name	procr + Tip: This is the Communication Manager node name.
Near-end Listen Port	An unused port number for the near-end listen port.
Far-end Node Name	+ Tip: This is the node name configured for Session Manager.
Far-end Listen Port	An unused port number for the far-end listen port.
Far-end Network Region	The number of the network region that is assigned to the far-end of the signaling group. The region is used to obtain the codec set used for negotiation of trunk bearer capability.
Far-end Domain	The name of the IP domain that is assigned to the far-end of the signaling group.

5. Press **F3** key to save the changes.

Creating a Trunk group

Procedure

1. On the SAT session, in the Command terminal, type `add trunk-group n` and press **Enter**.

Where, *n* is the trunk group number.

The system displays the **TRUNK GROUP** screen.

2. Use the **up** or **down** arrow key and scroll to the **Group Type** option.
3. In the **Group Type** option, type `SIP` and press the **TAB** key.

The system displays the **TRUNK GROUP** screen with information similar to the following:

```

=====
add trunk-group n                                     Page 1 of 22
                                TRUNK GROUP

Group Number: 2          Group Type: sip          CDR Reports: y
Group Name: trunk to ASM  COR: 1          TN: 1          TAC: #2
Direction: two-way      Outgoing Display? n
Dial Access? n          Night Service:
Queue Length: 0
Service Type: tie          Auth Code? n

```

```

Signaling Group: 2
Number of Members: 255
=====

```

4. Update the following values:

Group Type	sip
Signaling Group	Signaling group * Note: You must configure the signaling group value that you created earlier.
Number of Members	The number of ports for this SIP connection.
Service Type	Tie
TAC	The trunk access code as per the dial plan.

5. Press **F7** key to go to the next page.

There are no changes required on screen 2.

6. Press **F7** key to go to the next page.

The page 3 of 22, displays the following information:

```

=====
Page      3 of  22
TRUNK FEATURES
  ACA Assignment? n           Measured: none
                               Maintenance Tests? y

                               Numbering Format: public
                               UI Treatment: shared
                               Maximum Size of UI Contents: 128
                               Replace Restricted Numbers? n
                               Replace Unavailable Numbers? n

                               Modify Tandem Calling Number: no
                               Send UCID? y

  Show ANSWERED BY on Display? y
=====

```

7. Update the following values:

UI Treatment	This value must be set to <i>shared</i> .
Send UCID	Set to Yes

8. Press **F3** key to save the changes.

Creating Hunt group

Procedure

1. On the SAT session, in the **Command: terminal**, type `add hunt-group n` and press **Enter**. The *n* is the hunt group number.

The system displays the HUNT GROUP screen. Use the **up** or **down** arrow key to scroll.

2. Update the following values:

Group Number	Numeric value
Group Extension	Extension of the group
Group Type	ead-mia Following are the possible values: • ead-mia • ucd-mia • ead-loa • ucd-loa  Note: Ensure that the Group Type that you configure on the Hunt group screen matches with the agent strategy that you select on the ICR Skill page.
ACD?	Y
Vector?	Y
Queue?	Y
Measured	external or both  Note: In CMS based routing, if you need the agent and skill data, you must set the Measured field to <code>external</code>.

The HUNT GROUP screen displays the information similar to the one provided below.

```

=====
add hunt-group n                               Page 1 of 4
                                         HUNT GROUP

Group Number: 1                                ACD? y
Group Name: english                           Queue? y
Group Extension: 2000                         Vector? y
Group Type: ead-mia
      TN: 1
      COR: 1                                MM Early Answer? n
Security Code:                               Local Agent Preference? n
ISDN/SIP Caller Display:

```

```

Queue Limit: unlimited
Calls Warning Threshold:      Port:
Time Warning Threshold:      Port:
=====

```

3. Press **F7** to go to the next page.
4. Use the **up** or **down** arrow key to scroll. Type the value of the parameter skill? as Y.
The HUNT GROUP screen displays the information similar to the one provided below.

```

=====
add hunt-group n                               Page 2 of 4
                                HUNT GROUP

                                Skill? y      Expected Call Handling Time (sec): 180
                                AAS? n        Service Level Target (% in sec): 80 in 20
                                Measured: external
Supervisor Extension:

Controlling Adjunct: none

VuStats Objective:
Timed ACW Interval (sec):
Multiple Call Handling: none
=====

```

5. Press **F3** to save the changes.

Adding the IP network region

You must define the authoritative domain name on the IP-network-region form.

Procedure

1. On the SAT session, in the **Command: prompt**, type `change ip-network-region 1` and press **Enter**.

The system displays the IP NETWORK REGION screen.

2. Use the **up** or **down** arrow key to scroll.
3. In the first page, provide the following information:

- Define the Authoritative Domain name.

The first screen of IP NETWORK REGION displays the information similar to the following:

```

=====
change ip-network-region 1                     Page 1 of 20
                                IP NETWORK REGION

Region: 1
Location:      Authoritative Domain: avaya.com
Name:
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
    Codec Set: 1      Inter-region IP-IP Direct Audio: yes
    UDP Port Min: 2048      IP Audio Hairpinning? n
    UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS

```

```

Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5    AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                      RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
=====

```

4. Press **F3** key to save the changes.

Adding the IP codec set

You must add the IP codec set in Communication Manager to establish a successful RTP path with the customer.

Procedure

1. On the SAT session, in the **Command:** prompt, type `change ip-codec-set n` and press Enter.

The *n* is the ip codec set number.

The system displays the IP Codec Set screen.

2. Use the **up** or **down** arrow key to scroll.

On the first page, provide the following information:

- Audio Codec
- Silence Suppression
- Frames Per Packet
- Packet Size in milliseconds

The system displays the first screen of IP Codec Set with the information similar to the following:

```

=====
change ip-codec-set 1                                     Page 1 of 2

                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size (ms)
1: G.729   n             2          20
2: G.711A  n             2          20
3: G.729A  n             2          20
4: G.711MU n             2          20
5:

```

```
6:
7:
=====
```

3. Press the **F3** key to save the changes.

Creating a CM login for POM in the CC Elite CTI configuration page

About this task

Use this procedure to create a CM login for POM in the CC Elite CTI configuration page.

Procedure

1. Log in to CM server from the Web browser `https://<CMIP>`
Enter the **Username** as `init` or `sroot` and enter the **Password**.
2. Select the **Administration** menu and choose **Server (Maintenance)**.
3. Select the **Administrator Accounts** option.
4. On the Administrator Accounts page, select the **Add Login** option and select **Privileged Administrator** and click **Submit**.
5. Enter the **Login name** `pomcti`.
6. Select the **Additional groups (profile)** as `prof18`.
7. Select the **Select type of authentication** as `Password`.
8. Enter and confirm the password.
9. Select **No** in Force password/key change on next login.
10. Click **Submit**.
11. Add the **Username** on POM server by clicking **Manager > CC Elite Configurations > Add CTI details**.

Chapter 3: Configuring Avaya Aura[®] Session Manager

Overview

Avaya Aura[®] Session Manager is a SIP routing tool that integrates all SIP devices across the entire enterprise network. Session Manager simplifies the existing communication infrastructure by combining existing PBXs and other communications systems, regardless of the vendor, into a cohesive and centrally managed SIP-based communications network.

You must configure Session Manager to work with POM. For more information, see *Administering Avaya Aura[®] Session Manager* from the Avaya Support site at: [http:// support.avaya.com](http://support.avaya.com).

The following table explains the SIP/Campaign manager requirement for the agent-based and notification campaigns.

Table 1: Connection Requirement for Campaigns

Campaign type	Connection requirement	
Agent-based	SIP	Campaign manager
Voice notification	SIP PROXY	Not required
Email notification	Not required	Not required
SMS notification	Not required	Not required

Checklist

Use the following checklist to configure Avaya Aura[®] Session Manager:

No.	Task	Description	✓
Add SIP Entities			
1	Add SIP Entity for SIP Gateway or Avaya Aura [®] Session Border Controller	See Adding SIP Entity for SIP Gateway or Session Border Controller on page 22.	

Table continues...

No.	Task	Description	✓
2	Add SIP Entities for Communication Manager	See Adding SIP Entities for Communication Manager on page 23.	
3	Add SIP Entity for Avaya Experience Portal	See Adding SIP Entity for Avaya Experience Portal on page 24.	
Add SIP Entity links			
4	Add SIP Entity Link for SIP Gateway or Avaya Aura® Session Border Controller	See Adding SIP Entity Link for SIP Gateway or Session Border Controller on page 24.	
5	Add SIP Entity Link for Communication Manager	See Adding SIP Entity Link for Communication Manager on page 25.	
6	Adding SIP Entity Link for Avaya Experience Portal	See Adding SIP Entity Link for Avaya Experience Portal on page 26.	
Define Policies and Time of Day			
7	Add Routing Policy for Communication Manager	See Adding Routing Policy for Communication Manager on page 26.	
8	Add Routing Policy for Avaya Experience Portal	See Adding Routing Policy for Avaya Experience Portal on page 27.	
Dial Patterns			
9	Add dial patterns for Avaya Experience Portal and Communication Manager	See Adding dial patterns for Avaya Experience Portal and Communication Manager on page 28.	

Adding SIP Entities

Adding SIP Entity for SIP Gateway or Session Border Controller

Procedure

1. Log in to the System Manager interface with the Administration user role.
2. From the System Manager main menu, select **Elements > Routing > SIP Entities**.
3. On the SIP Entities page, click **New**.
4. On the SIP Entities Details page, do the following:
 - a. In the **Name** field, enter the name of the SIP Gateway or Session Border Controller.
This name must be unique and can have between 3 and 64 characters.

- b. In the **FQDN or IP Address** field, enter the fully qualified domain name or IP address of the SIP Gateway or Session Border Controller configured in the signaling-group on Communication Manager.
 - c. In the **Type** field, click *Gateway*.
 - d. In the **Notes** field, specify additional notes about the SIP entity.
 - e. In the **Location** field, click the SIP entity location from the list of previously defined locations.
 - f. In the **Time Zone** field, click the default time zone to be used for the entity.
 - g. In the **SIP Timer B / F (in seconds)** field, keep the default value 4.
 - h. In the **Minimum TLS Version** field, keep the default value *Use Global Setting*.
5. Click **Commit**.

Adding SIP Entities for Communication Manager

Procedure

1. Log in to the System Manager interface with the Administration user role.
2. From the System Manager main menu, select **Elements > Routing > SIP Entities**.
3. On the SIP Entities page, click **New**.
4. On the SIP Entities Details page, do the following:
 - a. In the **Name** field, enter the name of the Communication Manager server.
This name must be unique and can have between 3 and 64 characters.
 - b. In the **FQDN or IP Address** field, enter the fully qualified domain name or IP address of the CLAN/Procr configured in the signaling-group on Communication Manager.
 - c. In the **Type** field, click *CM*.
 - d. In the **Notes** field, specify additional notes about the SIP entity.
 - e. In the **Location** field, click the SIP entity location from the list of previously defined locations.
 - f. In the **Time Zone** field, click the default time zone to be used for the entity.
 - g. In the **SIP Timer B / F (in seconds)** field, keep the default value 4.
 - h. In the **Minimum TLS Version** field, keep the default value *Use Global Setting*.
5. Click **Commit**.

Perform these steps to create SIP Entities for all the required Communication Manager servers.

Adding SIP Entity for Avaya Experience Portal

Procedure

1. Log in to the System Manager interface with the Administration user role.
2. From the System Manager main menu, select **Elements > Routing > SIP Entities**.
3. On the SIP Entities page, click **New**.
4. On the SIP Entities Details page, do the following:
 - a. In the **Name** field, enter the name of the Avaya Experience Portal server.
This name must be unique and can have between 3 and 64 characters.
 - b. In the **FQDN or IP Address** field, enter the fully qualified domain name or IP address of Media Processing Platform.

If you have multiple Media Processing Platform, add all Media Processing Platform with a single FQDN under Local Host Name configured.
 - c. In the **Type** field, click `Voice Portal`.
 - d. In the **Notes** field, specify additional notes about the SIP entity.
 - e. In the **Location** field, click the SIP entity location from the list of previously defined locations.
 - f. In the **Time Zone** field, click the default time zone to be used for the entity.
 - g. In the **SIP Timer B / F (in seconds)** field, keep the default value 4.
 - h. In the **Minimum TLS Version** field, keep the default value `Use Global Setting`.
5. Click **Commit**.

Adding SIP Entity links

Adding SIP Entity Link for SIP Gateway or Session Border Controller

Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, select **Elements > Routing > Entity Links**.
3. Click **New**.
4. On the Entity Links page, do the following:
 - a. In the **Name** field, enter the name of the SIP Entity Link for SIP Gateway or Session Border Controller.

This name must be unique and can have between 3 and 64 characters.

- b. In the **SIP Entity 1** field, select a SIP entity from the drop-down list.
This entity must always be a Session Manager instance.
 - c. In the **Protocol** field, select the protocol for the entity link.
 - d. In the **Port** field, enter the port number for SIP Entity 1.
 - e. In the **SIP Entity 2** field, select the entity that you created for SIP Gateway or Session Border Controller.
 - f. In the **Port** field, enter the port number for SIP Entity 2.
 - g. In the **Connection Policy** field, click `trusted` to specify that the link between the two SIP entities is trusted.
 - h. In the **Notes** field, specify additional notes about the entity link.
5. Click **Commit**.

Adding SIP Entity Link for Communication Manager

Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, select **Elements > Routing > Entity Links**.
3. Click **New**.
4. On the Entity Links page, do the following:
 - a. In the **Name** field, enter the name of the Communication Manager server.
This name must be unique and can have between 3 and 64 characters.
 - b. In the **SIP Entity 1** field, select a SIP entity from the drop-down list.
This entity must always be a Session Manager instance.
 - c. In the **Protocol** field, select the protocol for the entity link.
 - d. In the **Port** field, enter the port number for SIP Entity 1.
 - e. In the **SIP Entity 2** field, select the entity that you created for Communication Manager.
 - f. In the **Port** field, enter the port number for SIP Entity 2.
 - g. In the **Connection Policy** field, click `trusted` to specify that the link between the two SIP entities is trusted.
 - h. In the **Notes** field, specify additional notes about the entity link.
5. Click **Commit**.

Adding SIP Entity Link for Avaya Experience Portal

Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, select **Elements > Routing > Entity Links**.
3. Click **New**.
4. On the Entity Links page, do the following:
 - a. In the **Name** field, enter the name of the Avaya Experience Portal server.
This name must be unique and can have between 3 and 64 characters.
 - b. In the **SIP Entity 1** field, select a SIP entity from the drop-down list.
This entity must always be a Session Manager instance.
 - c. In the **Protocol** field, select the protocol for the entity link.
 - d. In the **Port** field, enter the port number for SIP Entity 1.
 - e. In the **SIP Entity 2** field, select the entity that you created for Media Processing Platform.
 - f. In the **Port** field, enter the port number for SIP Entity 2.
 - g. In the **Connection Policy** field, click `trusted` to specify that the link between the two SIP entities is trusted.
 - h. In the **Notes** field, specify additional notes about the entity link.
5. Click **Commit**.

Defining Policies and Time of Day

Adding Routing Policy for Communication Manager

Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, select **Elements > Routing > Routing Policies**.
3. On the Routing Policies page, click **New**.
System Manager displays the Routing Policy Details page.
4. In the General area, do the following:
 - a. In the **Name** field, enter the name of the routing policy.
 - b. In the **Retries** field, enter the number of retries for the destination SIP entity.
The permissible values are 0-5 and the default value is 0.

5. In the SIP Entity as Destination area, do the following:
 - a. Click **Select**.
 - b. On the Sip Entities page, select the Communication Manager SIP Entity and click **Select**.
6. In the Time of Day area, do the following:
 - a. Click **Add**.
 - b. On the Time Ranges page, select the appropriate time range and click **Select**.
7. Click **Commit**.

Adding Routing Policy for Avaya Experience Portal

Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, select **Elements > Routing > Routing Policies**.
3. On the Routing Policies page, click **New**.

System Manager displays the Routing Policy Details page.
4. In the General area, do the following:
 - a. In the **Name** field, enter the name of the routing policy.
 - b. In the **Retries** field, enter the number of retries for the destination SIP entity.

The permissible values are 0-5 and the default value is 0.
5. In the SIP Entity as Destination area, do the following:
 - a. Click **Select**.
 - b. On the Sip Entities page, select the Avaya Experience Portal SIP Entity and click **Select**.
6. In the Time of Day area, do the following:
 - a. Click **Add**.
 - b. On the Time Ranges page, select the appropriate time range and click **Select**.
7. Click **Commit**.

Dial Patterns

Adding dial patterns for Avaya Experience Portal and Communication Manager

About this task

 Note:

You must configure a minimum of two dial patterns.

- Pattern to route calls to Experience Portal Manager for incoming calls to Avaya Experience Portal.
- Pattern to route calls to agents and for polling/queuing VDN's to Communication Manager.

Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, select **Elements > Routing > Dial Patterns**.
3. On the Dial Patterns page, click **New**.

System Manager displays the Dial Pattern Details page.

4. In the General area, do the following:
 - a. In the **Pattern** field, enter the dial pattern.

The pattern can have between 1 and 49 characters.

The following are the valid formats for pattern types:

 - For regular patterns, `[+*#0-9x][0-9x]{0,35}`
 - For pattern ranges, `[+0-9][0-9]{0,23}:[+0-9][0-9]{0,23}`

If you specify a pattern range, System Manager disables the **Min**, **Max**, and **Emergency Call** fields.
 - For patterns with Emergency number, `[0-9]{0,35}`
 - b. In the **Min** field, enter the minimum number of digits to match in the dial pattern.
 - c. In the **Max** field, enter the maximum number of digits to match in the dial pattern.
 - d. In the **SIP Domain** field, select the domain for which you want to restrict the dial pattern.
 - e. In the **Notes** field, specify additional information about the dial pattern.
5. In the Originating Locations and Routing Policies area, do the following:
 - a. Click **Add**.

System Manager displays the Originating Location page.

- b. In the Originating Location area, select the originating location.
 - c. In the Routing Policies area, select the routing policy.
 - d. Click **Select**.
6. Click **Commit**.

Chapter 4: Configuring Avaya Experience Portal

Overview

POM reads the SIP proxy server configuration from the VoIP Connections Web page of Avaya Experience Portal. POM is a managed application of Avaya Experience Portal. Media Processing Platform (MPP), Speech servers, SMS server, e-mail server, and VOIP connections are already configured on Avaya Experience Portal.

Adding a SIP connection for Session Manager

Procedure

1. Log on to the Experience Portal Manager web page using and Administrator account.
2. In the navigation pane, click **System Configuration > VoIP Connections**.
3. On the VoIP Connections page, click the **SIP** tab.
4. Click **Add**.
5. On the Add SIP Connection page, do the following:
 - a. In the **Name** field, enter an appropriate name for the SIP connection.
 - b. In the **Enable** field, keep the default value **Yes**.
 - c. In the **Proxy Transport** field, select **TCP** or **TLS** based on your configuration.
 - d. Select one of the following:
 - **Proxy Servers**
 - **DNS SRV Domain**
 - e. **(Optional)** If you select **Proxy Servers**, enter the IP address of the Security module of Session Manager in the **Address** field.
 - f. **(Optional)** If you select **DNS SRV Domain**, enter the domain name of the DNS server in the **DNS SRV Domain** field.

For example, `abc.com`.

- g. In the **SIP Domain** field, enter the domain of Session Manager.
 - h. In the **Maximum Simultaneous Calls** field, enter the maximum number of calls that this trunk can handle at a time.
6. Click **Save**.

Chapter 5: Configuring Call Management System

Overview

Avaya Call Management System (CMS) is a software product for businesses and organizations that receive a large volume of telephone calls processed through the Automatic Call Distribution (ACD) feature of the Avaya Aura® Communication Manager system.

Checklist

Use the following checklist to configure Avaya Call Management System:

No.	Task	Description	✓
1	Configure Call Management System.	See Configuring Call Management System on page 32.	
2	Verify the installation and configuration of the CMS rt_socket.	See Verifying the installation and configuration of the CMS rt_socket on page 34.	

Configuring Call Management System

Before you begin

Note down the port number that you configured when making a connection between Communication Manager and Call Management System.

 Note:

For enabling FIPS mode on CMS, see *CMS Connectors* documentation.

In FIPS mode, please ensure that the connection to CMS is in secure mode and we have CMS CA or Identity certificate imported into POM Truststore.

Procedure

1. Log on to the Call Management System as a root user.
2. At the prompt, type `cmsadm` and press **Enter**.

The SSH client displays the Call Management System administration menu.

3. To turn off the Avaya CMS service, do the following:
 - a. At the prompt, type 8.
 - b. Press **Enter**.
 - c. At the prompt, type 2.
 - d. Press **Enter**.
4. After the Avaya CMS service stops, type `cmsadm` and press **Enter**.

The SSH client displays the Call Management System administration menu.

5. To define a new ACD, do the following:
 - a. At the prompt, type 1.
 - b. Press **Enter**.

The SSH client displays the list of supported versions of the Communication Manager for the ACD.

- c. Type the appropriate choice.

For the selected Communication Manager, the SSH client starts displaying the parameters for which you must type appropriate values.

- d. Type the appropriate values for the following parameters:
 - **Is Vectoring enabled on the switch**
 - **Is Expert Agent Selection enabled on the switch**
 - **Does the Central office have disconnect supervision**
 - **Type the local port assigned to switch**
 - **Type the remote port assigned to switch**
 - **Select the transport to the switch**
 - **Type switch host name or IP Address**
 - **Type switch TCP port number (5001-5999)**
 - **Number of splits/skills (0-8000)**
 - **Total split/skill members, summed over all splits/skills (0-100000)**
 - **Number of shifts (1-4)**
 - **Type the start time for the shift 1 (hh:mmXM)**

- **Type the stop time for the shift 1(hh:mmXM)**
- **Number of agents logged into all splits/skills during shift 1 (0-10)**
- **Number of trunk groups (0-2000)**
- **Number of trunks (0-12000)**
- **Number of unmeasured facilities (0-6000)**
- **Number of call work codes (1-500)**
- **Type number of vectors (0-8000)**
- **Type number of VDNs (0-22990)**

After you type the appropriate values for all parameters, the system updates the database with the specified values.

6. At the prompt, type `cmsadm` and press **Enter**.

The SSH client displays the Call Management System administration menu.

7. To turn on the Avaya CMS service, do the following:
 - a. At the prompt, type 8.
 - b. Press **Enter**.
 - c. At the prompt, type 1.
 - d. Press **Enter**.

Verifying the installation and configuration of the CMS rt_socket

Procedure

1. Log on to the Call Management System as a root user.
2. At the prompt, type `cmsadm` and press **Enter**.

The SSH client displays the Call Management System administration menu.
3. Press `Enter` till the system displays the main menu of Call Management System.

```
=====
MainMenu
Reports>
Dictionary>
Exceptions>
Agent Administration>
Call Center Administration>
Custom Reports>
User Permissions>
System Setup>
Maintenance>
RT_Socket>
Logout
```

```

;
=====

```

4. Verify that the following reports are present inside the **Custom Report > Real-time** menu.
 - **tvi**: This report is for the skill feeds.
5. Verify that the main menu displays the **RT_Socket** menu.
6. Select the **RT_Socket** menu and press **Enter**.

The SSH client displays the Rt_Socket Menu screen.

```

=====
----- RT_Socket Menu -----
1) Start RT_Socket Interface
2) Stop RT_Socket Interface
3) Check Status
4) Display License Info
5) View Maintenance Log
6) Show Version
7) Change Input Parameters
8) Display Configuration
0) Exit
=====
Choice ==>
=====

```

7. At the prompt, type 8 for the **Display configuration** menu and press **Enter**.
8. Verify that the following columns display the information based on the configuration of the CMS RT_Socket.

Columns	Description
Session	The session ID of the rt_socket session.
ACD	The ACD number from which POM receives the data feed.
Dest IP	The IP address of the POM system.
Port	The port number of the POM system.
Report	The following data feed reports: • POM for ACD skills

9. From the **Sessions** column, note the RT_Socket sessions that you configured with POM.
10. Press **Enter** to return to the RT_Socket menu.
11. Type the choice 3 for the **Check Status** menu and press **Enter**.
12. Verify that the system displays the status of RT_Socket sessions as **running** and **is connected**.

Chapter 6: Configuring External Selection

Overview

POM supports the External Selection feature. With this feature, external applications can pair agents and contacts for POM agent-based campaigns.

With this feature, POM exposes the interface and supporting classes. External applications select an agent for a contact or a contact for an agent through the interface and supporting classes. External applications can also apply the logic to select the agent-contact pair.

Connection management to the external system is a part of the external selection class and is implemented by a third party.

POM must provide the configuration data of the external system while initializing the external selection class. POM must also provide KeyStore or certificate path to the external selection class to secure the connection to the external system.

External selection interface must have methods to send a request and receive a response, overridden by the external selection class to implement the logic of sending a request and a receiving response. External selection class is deployed in the POM custom folder.

Checklist

Use the following checklist to integrate the external system with POM:

No.	Task	Description	✓
1	Configure an external system on the POM server.	Whitelist an external system for POM. See Configuring an external system on POM on page 37.	
2	Configure the external selection parameters on the POM server.	Load class files from the external system to POM. See Configuring external selection parameters on page 37.	

Table continues...

No.	Task	Description	✓
3	Deploy External Selection Application jar file on the POM server.	Load a .jar file from the external system to the directory of .jar files in POM. See Deploying a .jar file from the External system on the POM server on page 38.	
4	Configure the external selection settings on the POM server.	Enable POM to display contact list attributes. See Configuring external selection settings on page 39.	

Configuring an external system on POM

About this task

Add external systems to the list of approved systems for POM. Applications from these external systems can access POM to select an agent for a contact or a contact for an agent.

Before you begin

Ensure that the external system is active.

Procedure

1. Log on to the Avaya Experience Portal web console as an administrator.
2. In the navigation pane, click **Proactive Outreach > Manager**.
3. In the content pane, click **Configurations > External Selection Configuration**.
POM displays the External Selection Configuration page.
4. Click **Add**.
POM displays the External System Configuration dialog box.
5. In **IP**, type the server IP address of the external system.
6. In **Hostname**, type the server Fully Qualified Domain Name (FQDN) of the external system.
7. Click **Save**.

Configuring external selection parameters

About this task

Use this procedure to configure an external system on POM and load class files from the external system to POM.

Procedure

1. Log on to the Avaya Experience Portal web console as an administrator.
2. In the navigation pane, click **Proactive Outreach > Manager**.
3. In the content pane, click **Configurations > External Selection Configuration**.
4. In **Server Port**, type the port number to which the external system connects.
5. In **Failsafe Timer (msec)**, type any value between 20 to 500.
6. In **Maximum consecutive response timeout**, type any value between 3 to 100.
7. In **Next attempt interval after maximum timeout (sec)**, type any value between 30 to 300.
8. In **Heartbeat interval (sec)**, type any value between 15 to 600.
9. In **External selection class**, type the name of the external selection class file.
10. Select **Enable external selection for all campaigns**.
11. Click **Save**.

Deploying a .jar file from the External system on the POM server

About this task

Use this procedure to load a .jar file from the external system to the directory of jar files in POM.

Before you begin

Ensure that you enable External Selection in POM.

Procedure

1. Log on to the POM server as a root user.
2. Move the .jar file to the location of the POM directory.
You can use software such as WinSCP.
3. Copy the .jar file at the following location:
`$POM_HOME/lib/custom/`
4. Run the following command to receive permission to access the .jar file:
`chmod 777 <jar file name>`
5. Run the following command to take ownership of the .jar file:

`chown avayavp:avayavpgroup <jar file name>`

You must restart the Agent Manager service for the deployed file to take effect.

6. Run the following command to restart the Agent Manager service:

```
service agtmgr restart
```

Configuring external selection settings

About this task

Use this procedure to ensure POM displays contact list attributes.

Procedure

1. Log on to the Avaya Experience Portal web console as an administrator.
2. In the navigation pane, click **Proactive Outreach > Manager**.
3. In the content pane, click **Configurations > Global Configurations**.

POM displays the Manage Global Configuration page.

4. In the **Agent settings** area, select **External Selection**.
5. Click **Apply**.

Result

The agent manager invokes the selection class from an external system. This external system is connected to POM.

External selection configuration page field descriptions

Use this page to view the field descriptions that are used for the external selection configuration.

External system configuration parameters

Field or Button	Description
IP	The IP address of an external system that you select for whitelisting.
Hostname	The FQDN of the external system that is on the network to which you connect POM.
Action	To edit or delete the IP address and the FQDN.

External selection configuration parameters

Field or Button	Description
Server Port	The server port to which the external system connects. The default port is 11,000.
Failsafe Timer (msec)	The time for which POM waits for the external selection system to respond to the selection request sent by POM. The default minimum failsafe time is 20 milliseconds. The default maximum failsafe time is 500 milliseconds. The failsafe time configured on the system by default is 100 milliseconds.
Maximum consecutive response timeout	The maximum number of consecutive attempts after which POM stops sending requests to the external server. If the external system does not respond for x consecutive (x is configurable) requests from POM within the failsafe time, POM does not send subsequent requests to the external selection class and continues with the POM selection logic. POM tries to send the selection request after y seconds (y is configurable). The default minimum timeout is 3 seconds. The default maximum timeout is 5 seconds.
Next attempt interval after maximum timeout (sec)	The duration between the last attempt in which POM stops sending requests to the external server and the next attempt in which POM starts sending requests to the external server.
Heartbeat interval (sec)	The Heartbeat interval in seconds. The default minimum interval is 15 seconds. The default maximum interval is 600 seconds.
External selection class	The class path of the external selection class that resides on the external selection server.
Enable external selection for all campaigns	By default, this flag is disabled on POM. If you enable this flag, external selection becomes applicable for all preview/predictive and progressive campaigns. However, if you disable this flag, external selection becomes applicable after you enable the campaign level flag.

Table continues...

Field or Button	Description
Add	Use this button to configure the details of an external system, such as FQDN and IP address.
Edit	Use this button to edit the existing details of an external system, such as FQDN and IP address.
Delete	Use this button to delete the configured details of an external system.
Save	Use this button to save the parameters that you configure for external selection.
Reset	Use this button to reset parameters to the last saved values.

External system configuration page field descriptions

This page defines the field descriptions for the external system configuration.

Field or Button	Description
IP	The IP address of an external system that you select for white listing.
Hostname	The FQDN of the external system that connects to the POM server.

Chapter 7: Configuring External Application Server

Checklist

Use the following checklist to configure External Application Server:

No.	Task	Description	✓
1	Configure the POM database on the primary POM server	See Configuring POM database on the primary POM server on page 42.	
2	Configure Apache Tomcat	See Configuring Apache Tomcat on page 46.	
3	Exchange and configure the certificates for single application server	See Exchanging and configuring certificates on page 47.	
4	Configure External Application Server- WebSphere	See External Application Server- WebSphere on page 52.	
5	Configure External Application Server- WebSphere version 8.5.5	See Configuring External Application Server- WebSphere version 8.5.5 on page 53.	
6	Exchange and configure the certificates for WebSphere application server	See Exchanging and configuring certificates for WebSphere application server on page 55.	

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 Apache Tomcat

Before you begin

Ensure that you have installed the following:

- Java 7 or 8.
- Tomcat 7 or 8.

For more information on the Cipher requirements of Java implementation, see *Appendix A*.

Procedure

1. Copy the `*.war` files from `$POM_HOME/DDapps` to `<APPSERVER_HOME>/webapps` of the application server to the `$APPSERVER_HOME/lib/` folder.
2. Copy files from `$POM_HOME/DDapps/lib/*` to `<APPSERVER_HOME>/lib` of the application server to the `$APPSERVER_HOME/lib/` folder.
3. Edit `<APPSERVER_HOME>/conf/server.xml` and add the following connector node:

```
<<!-- <Connector port="7080" protocol="HTTP/1.1"
URIEncoding="UTF-8" useBodyEncodingForURI="true"
connectionTimeout="20000" redirectPort="7443" />-->
<!-- ....CHANGES for AVAYA POM START .... --> <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" keystorePass="changeit"
clientAuth="false" sslEnabledProtocols="TLSv1.2"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH
_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECD
HE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA
384,TLS_EMPTY_RENEGOTIATION_INFO_SCSV"/>

```

4. 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=TLSv`
`1.2". 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.

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_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_EMPTY_RENEGOTIATION_INFO_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**.

- I. 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.

Configuring External Application Server- WebSphere

About this task

Use this procedure to configure the WebSphere application server to work with POM.

Before you begin

- Copy `runtimeSupportWebsphere.zip` from `$POM_HOME//DDapps/WebSphere` files to the `$WS_HOME\AppServer\lib\ext` folder.
- Restart the WAS server through `services.msc` or the tools that are available on the user interface of the server.
- Ensure that you have installed the following:
 - Java 7 or 8.
 - WebSphere 8.5.5 or a higher version.

For more information on the Cipher requirements of Java implementation, see *Appendix A*.

Procedure

1. In the navigation pane, select **Application > Application type > WebSphere enterprise applications** and browse **WebSphere enterprise applications**.
2. On Specify the EAR, WAR, JAR, or SAR module to upload and install page, browse and upload `runtimeconfig.ear` from the local system.
3. Click **Next**.
4. Select **Show me all installation options and parameters**.
5. Click **Next**.

The system displays the resulting security warnings from an analysis of this application.
6. Click **Continue**.
7. On the Select installation options page, select **Precompile JavaServer Pages files** and retain the other default values.
8. Click **Next**.
9. On the Map modules to servers page, select the `runtimeconfig.ear`.
10. Click **Next**.
11. On the Choose to generate default bindings and mappings page, click **Next**.
12. On the Map modules to servers page, select `runtimeconfig.ear`.
13. Click **Next**.
14. On the Provide options to compile JSPs page, select `runtimeconfig.ear`, **WEB-INF/web.xml**
15. In the **JDK Source Level**, type 15.
16. Click **Next**.

17. On the Provide JSP reloading options for Web modules page, click **Next**.
18. On the Map shared libraries page, click **Next**.
19. On the Map virtual hosts for Web modules page, select **runtimeconfig.ear**.
20. Click **Next**.
21. On the Map context roots for Web modules page, click **Next**.
22. On the Summary page, click **Finish**.
23. Click **Save**.

 Caution:

Verify that the configuration is saved.

24. Restart the application server.

Next steps

Verify if you can access POM OD runtime.

1. To login browse `http://<App server IP :<port number>/runtimeconfig/login.jsp`
2. Type username and password as `ddadmin`.
3. Navigate to **Home > Certificates > Change Keystore**, and define keystore path as `C:\Program Files\IBM\WebSphere\AppServer\lib\ext\myTrustStoreNew`.
4. Type the password as `changeit`.

Configuring External Application Server- WebSphere version 8.5.5

About this task

Use this procedure to configure WebSphere version 8.5.5 and later with POM.

Before you begin

On the POM server, enable **Mutual Certification Authentication** for email and SMS.

Procedure

1. On IBM Console, select **Environment > Shared libraries**.
2. On the Shared Libraries page, select the appropriate **Scope** from the drop-down.
3. Click **New**.
4. Define a name for the newly created shared library.
5. In the **Classpath** field, paste the following entries:

For Linux	For Windows
<pre> \${WAS_INSTALL_ROOT}/lib/ext/axiom- api-1.2.13.jar \${WAS_INSTALL_ROOT}/lib/ext/axiom- dom-1.2.13.jar \${WAS_INSTALL_ROOT}/lib/ext/axiom- impl-1.2.13.jar \${WAS_INSTALL_ROOT}/lib/ext/axis2- adb-1.6.2.jar \${WAS_INSTALL_ROOT}/lib/ext/axis2- adb- codegen-1.6.2.jar \${WAS_INSTALL_ROOT}/lib/ext/axis2- json-1.6.2.jar \${WAS_INSTALL_ROOT}/lib/ext/axis2- kernel-1.6.2.jar \${WAS_INSTALL_ROOT}/lib/ext/axis2- saaaj-1.6.2.jar \${WAS_INSTALL_ROOT}/lib/ext/axis2- transport-http-1.6.2.jar \${WAS_INSTALL_ROOT}/lib/ext/axis2- transport-local-1.6.2.jar \${WAS_INSTALL_ROOT}/lib/ext/ neethi-3.0.2.jar \${WAS_INSTALL_ROOT}/lib/ext/woden- api-1.0M9.jar \${WAS_INSTALL_ROOT}/lib/ext/woden-impl- dom-1.0M9.jar \${WAS_INSTALL_ROOT}/lib/ext/woden- tool-1.0M9.jar \${WAS_INSTALL_ROOT}/lib/ext/ XmlSchema-1.4.7.jar \${WAS_INSTALL_ROOT}/lib/ext/ VPWebServiceClient-1.0.jar \${WAS_INSTALL_ROOT}/lib/ext/ VPAppLogClientWS_x.0.0.jar </pre>	<pre> \$WAS_HOME\AppServer\lib\ext\axiom- api-1.2.13.jar \$WAS_HOME\AppServer\lib\ext\axiom- dom-1.2.13.jar \$WAS_HOME\AppServer\lib\ext\axiom- impl-1.2.13.jar \$WAS_HOME\AppServer\lib\ext\axis2- adb-1.6.2.jar \$WAS_HOME\AppServer\lib\ext\axis2- adb- codegen-1.6.2.jar \$WAS_HOME\AppServer\lib\ext\axis2- json-1.6.2.jar \$WAS_HOME\AppServer\lib\ext\axis2- kernel-1.6.2.jar \$WAS_HOME\AppServer\lib\ext\axis2- saaaj-1.6.2.jar \$WAS_HOME\AppServer\lib\ext\axis2- transport-http-1.6.2.jar \$WAS_HOME\AppServer\lib\ext\axis2- transport-local-1.6.2.jar \$WAS_HOME\AppServer\lib\ext\neethi-3.0. 2.jar \$WAS_HOME\AppServer\lib\ext\woden- api-1.0M9.jar \$WAS_HOME\AppServer\lib\ext\woden-impl- dom-1.0M9.jar \$WAS_HOME\AppServer\lib\ext\woden- tool-1.0M9.jar \$WAS_HOME\AppServer\lib\ext\XmlSchema-1 .4.7.jar \$WAS_HOME\AppServer\lib\ext\VPAppLogCli entWS_x.0.0.jar \$WAS_HOME\AppServer\lib\ext\VPWebServic eClient-0x.00.00.01.jar </pre>

6. Click **Apply**.
7. Save the changes into the Master Configuration.
8. On IBM Console, select **Servers > Server Types > WebSphere application servers**.
The system displays the Application Servers page.
9. On the right pane, select **Server Infrastructure > Java and Process Management > Class Loader**.
10. Click **New**.
11. Select **Classes loaded with local class loader first (parent last)** from the drop-down menu.
12. Click **Apply**.

On the Configuration page, the system displays the shared library reference link.

 Note:

Save the changes into the Master Configuration.

13. Click shared library reference link.

14. Click **Add**.

The system displays the list of all the shared libraries.

15. Select **Servers > Server Types > WebSphere application servers > <Server_name>**.
16. On the Server Infrastructure page, select **Java and process management > Process definition > Java virtual machine**.
17. In the **Generic JVM arguments** field, type
`Dorg.xsocket.connection.client.ssl.sslengine.enabledProtocols=TLSv1.2.`
18. Retain all the other default values.
19. Click **Apply**.
20. Click **Save**.

 Caution:

Make sure you verify all the configuration has been saved.

21. WebSphere requires additional configurations to enforce communication over TLSv1.2. for both incoming and outgoing connections. For more information, see [Configuring TLSv1.2 on Websphere](#) on page 112.
22. Restart the application server.

Next steps

Verify if you can access POM OD runtime.

1. In your web browser, enter the following URL:
`http://<App server IP ><port number>/runtimeconfig/login.jsp`
2. Type the username and password as ddadmin.
3. Navigate to **Home > Certificates > Change Keystore** and define the keystore path as
`C:\Program Files\IBM\WebSphere\AppServer\lib\ext\myTrustStoreNew.`
4. Type the password as changeit.

Exchanging and configuring certificates for WebSphere application server

About this task

Use this procedure to exchange and configure certificates on a single, or multiple application servers.

 Important:

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

Before you begin

Configure the WebSphere application server to work with POM.

Procedure

1. Using the browser window, log in to the WAS web console as an administrator.
2. Select **Security > SSL certificate and key management > Key stores and certificates**.
3. Create a new key store with name **myTrustStore**.
4. Type the valid path of the key store and type the password **changeit**.
5. Fill the mandatory details and click **OK** to create the key store.

The system displays **myTrustStore** on the SSL certificate and key management page.

6. Select **myTrustStore > Signer Certificates**.

The system displays the root certificate generated by WAS.

7. Select the **Root Certificate** tab and click **Extract** and save the certificate to your local system.
8. Type a file name where this certificate is extracted.
9. Using the browser window, log in to the primary EPM as administrator.

Note:

For multiple POM servers, that is, primary or auxiliary, log in to the primary EPM.

10. Select **Security > Certificates > Upload Trusted Certificate**.
11. On the **Upload Trusted Certificate** tab, specify the name and browse to the path where you save the certificate extracted in Step 5.

WAS does not provide the option to configure SAN in its self-signed/ root certificates. Therefore, you must do the following:

- a. On the Experience Portal, navigate to **System Configurations > Applications**.
 - b. Configure POM application URL using the hostname of the Application Server on `https://<IP address>/VoicePortal/faces/home.jsf`.
 - c. For the hostname resolution, add the entry of the Application Server on EP/MPP and vice versa.
12. Import the axis2 certificate.
 13. Select **Import > Security > Certificates > Trusted Certificate**.
 14. On the **Root Certificate** tab, click **Export** and save the certificate to your local system.

Note:

The name of the file is `sipCA.pem`.

15. In the navigation pane, select **Proactive Outreach > Manager**.

16. From the drop-down menu, select **Configurations > Servers**.
17. Click **Export** on the listed certificate tab and save it on your local system.

 Note:

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

18. On the WAS web console, select **Security > SSL certificate and key management > Key stores and certificates > myTrustStore > Personal certificates**.
19. Create a new personal certificate.
20. Fill the mandatory details and click **OK**.
A common name must be hostname of the WAS system.
21. Click **Extract** and save the certificate to your local system.
22. On EPM, click **Security > Certificate Trusted Certificates** and upload the certificate saved in Step 21.
23. 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.

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

- a. In the navigation pane, click **Certificates**.
- b. Click **Change**.

The system displays Change Keystore page.

- c. In the **Keystore Path** field, type the path used in Step 5 for myTrustStore.
- d. In the **Password** field, type `changeit`.
- e. In the **Confirm** field, type `changeit`.
- f. Click **Save**.
- g. Click **Add**.

The system displays the Add Certificate page.

- h. Type a name for the EPM certificate and browse to find the path where you saved the primary EPM root certificate exported in Step 14.
- i. Click **Continue**. The system displays the Certificates page.
- j. Click **Save**.
- k. Click **Add**. The system displays the Add Certificate page.
- l. Type a name for the POM certificate and browse to find the path where you saved the primary POM root certificate exported in Step 17.

- m. Click **Continue**.
The system displays the Certificates page.
 - n. Click **Save**.
Install all POM applications one by one using detailed option and repeat steps used for deploying `runtimeconfig.ear` file.
 - o. Click **Fetch** to fetch the axis2 certificate for primary EPM.
In a multiple POM server environment, you must fetch the axis2 certificate from all auxiliary EPM servers.
The system displays the Add Certificate page.
 - p. In the **Name** field, type the name of the certificate. For example, `axis_prim` or `axis_aux`.
 - q. In the **Location** 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.
 - r. Click **Continue**. The system displays the Certificates page.
 - s. Click **Save**.
25. On the WAS system, in POM Nailer application select data directory. Open `WASConfig.properties` file and provide location of the `keystoreFile`, `keystoreType`, and `keystorePass`.
26. Repeat above step for POM Driver application.
27. Using the browser window, log in to the EPM as an administrator and do the following:
- * **Note:**
For multiple POM servers, log in to the primary EPM.
28. In the navigation pane, click **Proactive Outreach > Manager**.
29. Click **Configurations > Trusted Certificates**.
- * **Note:**
In a multiple POM server environment, you must fetch the axis2 certificate from all auxiliary EPM servers.
30. In the **Name** field, type the name of the certificate. For example, `axis_prim` or `axis_aux`.
31. In the **Location** field, type the client URL as `https://<EPM IP address>/axis2`.
32. Click **Continue**.
The system displays the Certificates page.
33. Click **Save**.
34. Click **Import**.
The system displays the Add Certificates page.

35. Type a name for the EPM certificate and browse to find the path where you saved the primary EPM root certificate exported in Step 14.

36. Click **Continue**.

The system displays the Certificates page.

37. Click **Save**.

38. Click **Import**.

The system displays the Add Certificates page.

39. Type a name for the WAS personal certificate and browse to find the path where you saved the WAS personal certificate exported in Step 22.

40. Click **Continue**.

The system displays the Certificates page.

41. Click **Save**.

 Note:

Install all POM applications one by one using detailed option and repeat steps used for deploying `runtimeconfig.ear` file.

42. On the WAS system, in POM Nailer application select data directory. Open `WASConfig.properties` file and provide location of the `keystoreFile` and `keystorePass`.

43. Repeat these steps for the POM Driver application.

44. Restart the application server, MPP's, and all auxiliary servers.

Chapter 8: Configuring Avaya Contact Recorder

Overview

Avaya Contact Recorder provides an efficient and scalable voice recording platform, running on the standard PC hardware.

You use Avaya Contact Recorder to:

- Find and retrieve recordings
- Observe in-progress calls using the recorder's integral search, replay, and live monitoring features

Checklist

Use the following checklist to configure Avaya Contact Recorder:

No.	Task	Description	✓
1	Add Avaya Contact Recorder(ACR) on Communication Manager	See the following sections to add ACR on communication manager: • Verify the Communication Manager license on page 63 • Administering CTI link for TSAPI on page 64 • Creating Universal Call ID (UCID) on page 64 • Administering Class of Restriction (COR) on page 65 • Administering Agent Stations on page 66 • Administering Codec Set on page 66 • Administering Network Region on page 67 • Administering Virtual IP Softphones on page 68 • Assigning Virtual IP Softphones to Network Region on page 70	

Table continues...

No.	Task	Description	✓
2	Configure AES for Avaya Contact Recorder	See the following sections to configure AES for ACR: • Administering TSAPI Link on page 70 • Obtaining Tlink Name on page 71 • Obtaining H.323 Gatekeeper IP Address on page 71 • Disabling Security Database on page 71 • Restarting TSAPI Service on page 71 • Administering Avaya Contact Recorder User for DMCC on page 72 • Administering Avaya Contact Recorder User for TSAPI on page 72 • Verifying Avaya Aura® Application Enablement Services on page 73	
3	Configure POM	See the following sections to configure POM: • Enabling WFO integration on page 74 • Configuring POM Applications on page 74	
4	Configure Avaya Contact Recorder	See the following sections to configure ACR: • Administering Recorder Information on page 74 • Administering Contact Center Information on page 75 • Administering Bulk Recording on page 75 • Administering POM Interface on page 76	

Adding ACR configuration on CM

Verify the Communication Manager license

Procedure

1. Log in to the Communication Manager system and select the SAT terminal.
2. On the SAT session, in the Command prompt, type `display system-parameters customer-options` and press Enter.
3. Navigate to page 3.
4. Verify that the **Computer Telephony Adjunct Links** customer option is set to **Y**.

The OPTIONAL FEATURES screen on page 3 displays the information similar to the following:

```
display system-parameters customer-options                               Page   3 of 11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
      Access Security Gateway (ASG)? y        Authorization Codes? y
      Analog Trunk Incoming Call ID? y         CAS Branch? n
    A/D Grp/Sys List Dialing Start at 01? y    CAS Main? n
    Answer Supervision by Call Classifier? y    Change COR by FAC? n
      ARS? y      Computer Telephony Adjunct Links? y
      ARS/AAR Partitioning? y      Cvg Of Calls Redirected Off-net? y
      ARS/AAR Dialing without FAC? y      DCS (Basic)? y
      ASAI Link Core Capabilities? y      DCS Call Coverage? y
      ASAI Link Plus Capabilities? y      DCS with Rerouting? y
    Async. Transfer Mode (ATM) PNC? n
    Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
      ATM WAN Spare Processor? n          DS1 MSP? y
      ATMS? y      DS1 Echo Cancellation? y
      Attendant Vectoring? y
```

5. Navigate to page 4.
6. Verify that the **Enhanced Conferencing** customer option is set to **Y**.

The OPTIONAL FEATURES screen on page 4 displays the information similar to the following:

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y	IP Stations? y	
Enable 'dadmin' Login? y		
Enhanced Conferencing? y	ISDN Feature Plus? n	
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n	ISDN-BRI Trunks? y	
Enterprise Wide Licensing? n	ISDN-PRI? y	
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? y	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
IP Trunks? y		
IP Attendant Consoles? y		

7. If any option specified in this section does not have a proper value, contact the Avaya sales team or business partner for a proper license file.

Administering CTI link for TSAPI

Procedure

1. On the SAT session, in the Command terminal, type `add cti-link n`, where `n` is the CTI link number from 1 to 64.
2. Press `Enter`.
The Communication Manager system displays the CTI Link screen.
3. In **Extension**, type the available extension number.

 Note:

CTI link number and extension number vary.

4. In **Type**, type `ADJ-IP`.
5. In **Name**, type the descriptive name.
6. Save the changes.

Creating Universal Call ID (UCID)

Procedure

1. On the SAT session, in the command terminal, type `change system-parameters features`.
2. Navigate to page 5.
3. Update the following values:

Create Universal Call ID (UCID)	Y
UCID Network ID	Enter an available node ID

- Navigate to page 13.
- In **Send UCID to ASAI**, type Y.

 Note:

This parameter enables a universal call ID to be sent to Avaya Contact Recorder (ACR).

- Save the changes.

Administering Class of Restriction (COR)

Procedure

- On the SAT session, in the Command terminal, type `change cor n`, where n is the Class Of Restriction (COR) number to be assigned to the target stations and virtual IP softphones.
- Press `Enter`.
- Set **Calling Party Restriction** to `none`.

The CLASS OF RESTRICTION screen displays the information similar to the one provided below.

change cor 1		Page 1 of 23
CLASS OF RESTRICTION		
COR Number: 1		
COR Description:		
FRL: 0	APLT? y	
Can Be Service Observed? y	Calling Party Restriction: none	
Can Be A Service Observer? y	Called Party Restriction: none	
Time of Day Chart: 1	Forced Entry of Account Codes? n	
Priority Queuing? n	Direct Agent Calling? y	
Restriction Override: none	Facility Access Trunk Test? n	
Restricted Call List? n	Can Change Coverage? n	
Access to MCT? y	Fully Restricted Service? n	
Group II Category For MFC: 7	Hear VDN of Origin Annc.? n	
Send ANI for MFE? n	Add/Remove Agent Skills? n	
MF ANI Prefix:	Automatic Charge Display? n	
Hear System Music on Hold? y	PASTE (Display PBX Data on Phone)? n	
	Can Be Picked Up By Directed Call Pickup? n	
	Can Use Directed Call Pickup? n	
	Group Controlled Restriction: inactive	

- Save the changes.

Administering Agent Stations

About this task

Use this procedure to configure physical stations used by the POM agents. After the configuration, the stations can be used in outbound calls using Class of Restriction (COR).

Procedure

1. On the SAT session, in the Command terminal, type `change station n`, where `n` is the station extension.
2. Press `Enter`.

The Communication Manager system displays the change station screen.

3. In **COR**, type `1`.

Caution:

Ensure that the **Name** field is populated with the name of the station. Otherwise, Avaya Contact Recorder reports an error and no recording is done.

4. Save the changes.

Administering Codec Set

Procedure

1. On the SAT session, in the Command terminal, type `change ip-codec-set n`, where `n` is the codec set for the virtual IP softphones.
2. Press `Enter`.

The system displays the codec set screen.

3. Update the following values:

Audio Codec	Frames Per Packet
G.729A	6
 Note: Avaya Contact Recorder uses G.729A recording format in the test configuration.	
G.711MU	6

4. Retain the values of other fields.

The IP Codec Set screen displays similar to the one provided below:

```
change ip-codec-set 1
```

Page 1 of 2

```

                                IP Codec Set

    Codec Set: 1

    Audio      Silence      Frames      Packet
    Codec      Suppression  Per Pkt    Size(ms)
1: G.729A      n            6          20
2: G.711MU     n            6          20
3: G.711A      n            6          20
4:
5:
6:
7:

    Media Encryption
1: none
2:
3:

```

5. Save the changes.

Administering Network Region

About this task

Configure the network region for the virtual IP softphones.

Procedure

1. On the SAT session, in the Command terminal, type `change ip-network-region n`, where `n` is the network region.
2. Press `Enter`.

The system displays the IP Network Region Link screen.

3. Type the **Codec Set** field values as added in the *Administer Codec Set*.

The IP NETWORK REGION screen displays similar to the one provided below:

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1
Location: 1           Authoritative Domain: sol002.fst.silpunelab.com
Name: CM1A           Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
                      Inter-region IP-IP Direct Audio: yes
                      IP Audio Hairpinning? n
Codec Set: 1
UDP Port Min: 2048
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
H.323 IP ENDPOINTS    AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y      RSVP Enabled? n
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

4. Save the changes.

Administering Virtual IP Softphones

About this task

Configure Virtual IP Softphones to conference into calls involving target stations and to capture media.

Procedure

1. On the SAT session, in command terminal type, add station n, where n is the available extension number.
2. Update the following values:

Type	4624
Name	Enter a descriptive name
Security Code	Enter a desired value
COR	1
IP SoftPhone	Y

 Note:

Retain the default values for the remaining fields.

The STATION screen displays similar to the one provided below:

```

add station 3011450                                     Page 1 of 6
                                                    STATION
Extension: 301-1450                                     Lock Messages? n      BCC: 0
  Type: 4624                                           Security Code: 123456  TN: 1
  Port: S00009                                         Coverage Path 1:      COR: 1
  Name: Avaya Contact Recorder Test 1                 Coverage Path 2:
COS: 1
                                                    Hunt-to Station:      Tests? y

STATION OPTIONS
  Location:                                           Time of Day Lock Table:
  Loss Group: 19                                     Personalized Ringing Pattern: 1
                                                    Message Lamp Ext: 301-1450
  Speakerphone: 2-way                               Mute Button Enabled? y
  Display Language: english
  Survivable GK Node Name:
  Survivable COR: internal                           Media Complex Ext:
  Survivable Trunk Dest? y                           IP SoftPhone? y
                                                    IP Video Softphone? n
                                                    Short/Prefixed Registration Allowed: default

```

3. Navigate to page 4.
4. In **BUTTON ASSIGNMENT 4** field, type `conf-dsp`.
5. Clear the **BUTTON ASSIGNMENT 3** field.

```

change station 3011450                                     Page 4 of 6
                                                    STATION
SITE DATA
  Room:                                           Headset? n
  Jack:                                           Speaker? n
  Cable:                                           Mounting: d
  Floor:                                           Cord Length: 0
  Building:                                       Set Color:

ABBREVIATED DIALING
  List1:                                           List2:
                                                    List3:

BUTTON ASSIGNMENTS
  1: call-appr                                     7:
  2: call-appr                                     8:
  3:                                                9:
  4: conf-dsp                                       10:
  5:                                                11:
  6:                                                12:

```

 Note:

Repeat the above steps to administer the desired number of virtual IP softphones, using sequential extension numbers and the same security code for all virtual IP softphones.

6. Save the changes.

Assigning Virtual IP Softphones to Network Region

About this task

Add the IP address of the Application Enablement Services server to the network region.

Procedure

On the SAT session, in the Command terminal, type `change ip-network-map`.

As all the virtual IP softphones register through the Application Enablement Services server, they are automatically assigned to that network region.

change ip-network-map

Page 1 of 63

IP ADDRESS MAPPING

IP Address	Subnet Bits	Network Region	VLAN	Emergency Location	Ext
FROM: x.x.x.x	/	1	1		
TO: x.x.x.x					

Next steps

Run the `save translation` command to save changes.

Configuring AES for ACR

Administering TSAPI Link

Procedure

1. Log in to the Application Enablement Services interface as an administrator.
2. In the left navigation pane, click **AE Services > TSAPI > TSAPI Links**.
The Application Enablement Services system displays the **TSAPI Links** page.
3. Click **Add Link**.
Application Enablement Services displays the **Add TSAPI Links** page.
4. In **Link**, type a local available numeric value.
5. In **Switch Connection**, select a relevant switch connection.
6. In **Switch CTI Link Number**, select the CTI link number that you configured in the section [AdministeringCTILinkForTSAPI](#) on page 64.



Note:

Retain the default values in the remaining fields.

7. Click **Apply Changes**.

Obtaining a Tlink Name

Procedure

1. Log in to the Application Enablement Services interface as an administrator.
2. In the left navigation pane, click **Security > Security Database > Tlinks**.
Application Enablement Services generates a new Tlink name for the TSAPI service.
3. Locate the Tlink name associated with the relevant switch connection.

Obtaining H.323 Gatekeeper IP Address

Procedure

1. Log in to the Application Enablement Services interface as an administrator.
2. In the left navigation pane, click **Communication Manager Interface > Switch Connections**.
Application Enablement Services displays a list of the existing switch connections on the **Switch Connections** page.
3. Locate the **Connection** name associated with the relevant Communication Manager.

Disabling Security Database

Procedure

1. Log in to the Application Enablement Services interface as an administrator.
2. In the left navigation pane, click **Security > Security Database > Control**.
Application Enablement Services displays the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen.
3. Clear the following check boxes:
 - **Enable SDB for DMCC Service**
 - **Enable SDB TSAPI Service**
 - **TAPI and Telephony Service**
4. Click **Apply Changes**.

Restarting TSAPI Service

Procedure

1. Log in to the Application Enablement Services interface as an administrator.
2. In the left navigation pane, click **Maintenance > Service Controller**.
Application Enablement Services displays the **Service Controller** page.
3. Select **TSAPI Service**.

4. Click **Restart Service**.

Administering Avaya Contact Recorder User for DMCC

Procedure

1. Log in to the Application Enablement Services interface as an administrator.
2. In the left navigation pane, click **User Management > User Admin > Add User**.
Application Enablement Services displays the **Add User** page.
3. Enter the appropriate value in the following fields:
 - **User Id**
 - **Common Name**
 - **Surname**
 - **User Password**
 - **Confirm Password**
4. In **CT User**, select **Yes**.
5. Retain the default values in the remaining fields.
6. Click **Apply**.

Administering Avaya Contact Recorder User for TSAPI

Procedure

1. Log in to the Application Enablement Services interface as an administrator.
2. In the left navigation pane, click **User Management > User Admin > Add User**.
In the right pane, Application Enablement Services displays the **Add User** page.
3. Enter values in the following fields:
 - **User Id**
 - **Common Name**
 - **Surname**
 - **User Password**
 - **Confirm Password**
4. From the **CT User** drop-down list, select **Yes**.
5. Retain the default value in the remaining fields.
6. Click **Apply**.

Configuring Proactive Outreach Manager on Avaya Aura Application Enablement Services

About this task

Use this procedure to configure Avaya Proactive Outreach Manager on Application Enablement Services.

Before you begin

- Ensure no firewalls between the POM servers and CMS prevent RT_Socket connection.
- In FIPS mode, ensure that the connection to AES is in secure mode and you have AES CA or Identity certificate imported into POM Truststore.

For information about enabling FIPS mode on AES, see *Administering Avaya Aura® Application Enablement Services*.

Procedure

1. Log in to Application Enablement Services.
2. Enable the **Standard Reserved Ports** on the AES web page.
3. Configure the Avaya Aura Application Enablement Services on the **SMS Properties** page.
4. Use the Avaya Aura Application Enablement Services test client:
`http://<IP address of AES>/sms/sms_test.php`
5. Enter the same username and password that you use to configure POM.
6. Enter all the parameter details on the Connection Information page.
7. Verify that the output has a password and a skill name is present.

Verifying Avaya Aura® Application Enablement Services

Procedure

1. Log in to the Application Enablement Services interface as an administrator.
2. In the navigation pane, click **Status > Status and Control > DMCC Service Summary**.
 In the right pane, Application Enablement Services displays the **DMCC Service Summary – Session Summary** page.
3. Verify that an active session with the username configured in the section *Administer Avaya Contact Recorder User for DMCC* is present.
4. Verify that the **# of Associated Devices** column reflects the number of virtual IP softphones that Avaya Contact Recorder uses.
5. In the navigation pane, click **Status > Status and Control > TSAPI Service Summary**.
 In the right pane, Application Enablement Services displays the **TSAPI Link Details** screen.
6. Verify that the **Status** column reflects the status as **Talking**.

Configuring POM

Enabling Work Force Optimization integration

Before you begin

Enable the Avaya Contact Recorder port on the POM server.

Procedure

1. Log in to the POM interface as an administrator.
2. In the navigation pane, click **Proactive Outreach > Manager**.
3. On the **Configuration** tab, click **Global Configurations**.
4. In the Recorder settings area, select the following check boxes:
 - a. **Enable Recorder**
 - b. **Enable Secured Connection**
5. In the **Recorder port** field, type the port number of the Avaya Contact Recorder port.
6. Click **Apply**.

Configuring POM Applications

Procedure

1. Log in to the POM interface as an administrator.
2. In the left navigation pane, click **System Configuration > Applications**.
3. In the right pane, click to edit the driver and nailer app. For more information about nailer app, see, *Administering Avaya Proactive Outreach Manager*.

Next steps

To restart the POM service:

- Log in to the POM server with root credentials.
- Run the command: `service POM restart`

ACR Configuration

Administering Recorder Information

Procedure

1. Log in to the Avaya Contact Recorder interface as an administrator.
2. Navigate to **General Setup > Recorder**.

3. In **IP Address on this server to use for recordings (RTP, screen content etc.)**, type the IP address of Avaya Contact Recorder.

Administering Contact Center Information

Procedure

1. Log in to the Avaya Contact Recorder interface as an administrator.
2. Navigate to **General Setup > Contact Center Interface**.
3. Update the following values:

Heading for Column 1	Heading for Column 2
Switch Type	Select Communication Manager .
Audio format	The default value is G.729A (8kbps) .
Avaya Communication Manager Name	Type H.323 Gatekeeper IP address obtained in Section <i>Obtain Tlink Name</i> .
AE Server Address(es)	Type IP address of the Avaya AES server.
DMCC Username	Type User Id configured in Section <i>Administer Avaya Contact Recorder User for DMCC</i> .
DMCC Password	Type User Password configured in Section <i>Administer Avaya Contact Recorder User for DMCC</i> .
IP Station Security Code	Type Security Code configured in Section <i>Administer Virtual IP Softphones</i> .
AES TSAPI Server(s)	Type IP address of the Avaya AES server.
AES TSAPI Service Identifier(s)	Type Tlink Name configured in Section <i>Administer TSAPI Link</i> .
AES TSAPI Service Login ID	Type User Id configured in Section <i>Administer Avaya Contact Recorder User for TSAPI</i> .
AES TSAPI Service password	Type User Password configured in Section <i>Administer Avaya Contact Recorder User for TSAPI</i> .
Extensions assigned to recorder	Use Add Port(s) to add the virtual IP softphone extensions configured in Section <i>Administer Virtual IP Softphones</i> .

Administering Bulk Recording

Procedure

1. Log in to the Avaya Contact Recorder interface as an administrator.
2. Navigate to **Operations > Bulk Recording**.
3. In the **Record calls to or from** group, click **Add address(s)** tab to add the target stations.
4. Retain the default values for other fields.

Administering POM Interface

Procedure

1. Log in to the Avaya Contact Recorder interface as an administrator.
2. Navigate to **Operations > Bulk Recording**.
3. Edit the Avaya Contact Recorder properties file to include all the following lines:

```
acr.dialerlist=POM1
POM1.class=com.swhh.cti.pomdialer.POMDialer
POM1.dialer=x.x.x.x
POM1.port=7999
POM1.username=wfo
POM1.password=Avaya135
POM1.tracing=true
POM1.blockagentids=true
```

 Note:

The **Dialer** field must be set to the IP address of the POM as obtained in Section *Configure POM*. The **User** and **Password** fields must be set to the user name and password that have the access permission to the POM admin page.

4. To separate the dialer list, use “,” delimiter in case of the multiple dialers.

Provide the required information for other dialers as shown below:

```
acr.dialerlist=POM1, POM2
POM1.class=com.swhh.cti.pomdialer.POMDialer
POM1.dialer=x.x.x.x
POM1.port=7999
POM1.username=wfo
POM1.password=Avaya135
POM1.tracing=true
POM1.blockagentids=true
POM2.class=com.swhh.cti.pomdialer.POMDialer
POM2.dialer=y.y.y.y
POM2.port=7999
POM2.username=wfo
POM2.password=Avaya135
POM2.tracing=true
POM2.blockagentids=true
```

5. Save and close the file.
6. Restart the Avaya Contact Recorder service.

Chapter 9: Integrating POM with Avaya Oceana™

Overview

POM integrates with Avaya Oceana® so that Avaya Oceana® can support a fully integrated Outbound channel.

For POM agents to log on to Avaya Workspaces, POM provides JAVA SDK. Avaya Workspaces provides the unified desktop for inbound and outbound channels. JAVA SDK provides API to integrate the POM Agent functionality for desktop implementation. Java SDK is inline with the existing .NET-based SDK except the login-specific enhancements. SDK APIs only support secure communication. Therefore, you must configure the POM certificate in the client API while connecting the client API to POM.

 Note:

For Avaya Workspaces to dispose calls, Custom Completion Code Name and Completion Code ID in POM and Avaya Oceana® must be same.

For Avaya Oceana® integration, you must install POM in the `Oceana` mode. After installing POM, you must log on to the Experience Portal web console, click **Proactive Outreach > Manager > Configurations > Oceana Configuration**, and configure the IP address or hostname of Avaya Oceana® Cluster 3 that hosts OBService.

OBService exposes the REST services through which POM fetches the agent attributes configured in Avaya Oceana®. You must log on to the Experience Portal web console, click **Proactive Outreach > Manager > Campaigns > Campaign Strategies**, and select the agent attributes as an outbound skill. POM agents can log on to Avaya Workspaces with attributes assigned to them.

 Note:

POM does not support skill-based pacing if you install POM in the `Oceana` mode. POM restricts the campaign having skill-based pacing.

Context Store Integration

POM provides outbound attempt information to the Context Store server for customer journey completeness. You can send the data to Context Store in all the POM installation modes. POM uses the Context Store REST web service to create the context. Context Store provides an auto-generated unique identifier that is work request ID for the context record. POM persists this work request ID into the POM database.

While creating the context, POM sets the **persistToEDM** field to `true` to persist the context data in an external database. POM also provides **groupID**, which is presented as Customer ID. One of the contact attributes is configured as Customer ID. Contact browser is enhanced to capture this configuration. The Customer ID uniquely identifies the specific customer record. POM derives the Customer ID based on the **Customer ID Retrieval Mode** configuration on the Contact Browser page.

The following are the retrieval mode configurations:

Retrieval mode	Description
Always	Select if POM does not have a customer ID or administrator chooses to use the customer ID from the customer management snap-in. POM fetches a Customer ID from the Customer Management snap-in. The selected attribute value and the attempt address are an input to fetch Customer ID. POM uses the same network address as that of the configured Context Store server while retrieving to the Customer Management snap-in.
Never	POM uses the value of the selected attribute as Customer ID.
Attribute value is blank	If the attribute value is blank, POM retrieves the Customer ID from the Customer Management snap-in. Otherwise, POM uses the attribute value as Customer ID.

 Note:

To see the customer journey, do not mark the contact as `done` in a campaign strategy unless it is with the agent. If you mark the contact as `done` while it is with the agent, the customer journey might not be displayed in the Avaya Workspaces.

POM REST web services

The existing SOAP web services are converted into equivalent REST web services. The Engagement Designer workflow in Avaya Oceana® can use the REST web services to modify entities related to the POM outbound campaign. For more information about POM REST web services, see *Developer Guide for Proactive Outreach Manager*.

POM - Oceana Integration checklist

Use the following checklist for POM - Avaya Oceana® integration:

No.	Task	Reference	✓
1	Install POM in the Oceana mode.	See <i>Implementing Avaya Proactive Outreach Manager</i> .	

Table continues...

No.	Task	Reference	✓
2	Deploy Avaya Oceana®.	See <i>Deploying Avaya Oceana®</i> .	
3	Load and install the OBService SVAR.	See Loading and installing the OBService SVAR on page 79.	
4	Set OBService attributes.	See Setting OBService attributes on page 80.	
5	Import the POM server certificate to Avaya Oceana® Cluster 3.	See Importing the POM server certificate to Avaya Oceana Cluster 3 on page 82.	
6	Configure Context Store.	For information about how to configure Context Store, see <i>Avaya Context Store Snap-in Reference</i> .	
7	Configure the IP address or FQDN of Avaya Oceana® Cluster 3.	For information about the fields on the Oceana Server page, see <i>Administering Avaya Proactive Outreach Manager</i> .	
8	Add the following to the POM Trust store. • Certificates of all nodes of Avaya Oceana® Cluster 1 • Certificates of all nodes of Avaya Oceana® Cluster 3 • Certificates of AES	For information about how to add certificates to the POM Trust store, see <i>Implementing Avaya Proactive Outreach Manager</i> .	
9	Complete POM configurations such as contact list, campaign strategies, completion codes, and campaigns.	See <i>Administering Avaya Proactive Outreach Manager</i> .	
10	Configure an Outbound Provider.	See Configuring an Outbound Provider on page 84.	
11	Add Disposition Codes for Outbound contacts.	See Adding Disposition Codes for Outbound contacts on page 85	
12	Create a user to handle Outbound contacts.	See Creating a user to handle Outbound contacts on page 85.	
13	Configure After Contact Work (ACW) time.	See Configuring After Contact Work time on page 87.	

Loading and installing the OBService SVAR

About this task

Use this procedure to load the OBService SVAR in System Manager and install it to Avaya Oceana® Cluster 3.

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze™ > Service Management > Services**.
2. On the Services page, click **Load**.
3. In the Load Service dialog box, perform the following steps:
 - a. Click **Browse**.
 - b. Select the SVAR and click **Open**.
 - c. Click **Load**.
4. In the Accept End User License Agreement dialog box, click **Accept**.
5. On the Services page, verify that the state of the SVAR is `Loaded`.
6. On the Services page, select the check box for the SVAR and click **Install**.
7. In the Confirm install service: OBService dialog box, select the check box for Avaya Oceana® Cluster 3 and click **Commit**.
8. On the Services page, verify that the state of the SVAR is `Installing`.

The state changes to `Installed` when the installation is complete.
9. Set OBService attributes.
10. Restart the Avaya Breeze® platform nodes that are added to Avaya Oceana® Cluster 3.

Setting OBService attributes

About this task

Use this procedure to configure the OBService attributes for POM integration.

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze™ > Configuration > Attributes**.
2. On the Service Clusters tab, do the following:
 - a. From **Cluster** drop-down, select Avaya Oceana® Cluster 3.
 - b. From the **Service** drop-down, select **OBService**.
3. Configure the service attributes.
4. Click **Commit**.

OBService attributes

Startup Configuration

Name	Description
Deployment type	Determines the memory size of processing units. The available deployment types are: • For an Avaya Oceana[®] deployment that supports up to <> active agents, select <code>OCEANA_XLARGE</code>. • For an Avaya Oceana[®] deployment that supports up to <> active agents, select <code>OCEANA_4XLARGE</code>. • For an Avaya Oceana[®] deployment that supports up to 4500 active agents, select <code>OCEANA_3XLARGE</code>. • For an Avaya Oceana[®] deployment that supports up to 2000 active agents, select <code>OCEANA_XLARGE</code>. • For an Avaya Oceana[®] deployment that supports up to 1000, 500, or 250 active agents, select <code>OCEANA_LARGE</code>. • For an Avaya Oceana[®] deployment that supports up to 100 active agents, select <code>OCEANA_SMALL</code>.
POM Server	The IP address or FQDN of the POM server that the Outbound Connector services.
UAC Cluster	The cluster that hosts the Unified Agent Controller services. • For an Avaya Oceana[®] deployment that supports up to 100 active agents, select Avaya Oceana[®] Cluster 1. • For an Avaya Oceana[®] deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, select Avaya Oceana[®] Cluster 2.
UCA Cluster	The cluster that hosts the Unified Collaboration Administrator (UCA) service. To set this attribute, select Avaya Oceana[®] Cluster 1.
UCM Cluster	The cluster that hosts Unified Collaboration Model (UCM) services. To set this attribute, select Avaya Oceana[®] Cluster 1.

Advanced Configuration

Name	Description
Enable Authentication	If you set the JSON Web Tokens (JWT) authentication to true, the authentication server sends the token to the Unified Agent Controller (UAC) component through XML Paper Specification (XPS) API. If you set the authentication token to false, the authentication server does not send a JWT authentication token.
UAC URL	The service URL of the UnifiedAgentController service API. For example, /services/UnifiedAgentContextService/XpsAPI.

Importing the POM server certificate to Avaya Oceana® Cluster 3

Before you begin

Ensure you log in to the POM server web interface and export the POM server certificate.

Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Elements**.
2. Select the check box for one of the nodes of Avaya Oceana® Cluster 3 and click **More Actions > Manage Trusted Certificates**.
3. Click **Add**.
4. On the Add Trusted Certificate page, do the following:
 - a. Click **Import from file**.
 - b. In **Please select a file**, click **Browse**.
 - c. In the **Choose File to Upload** dialog box, browse to the POM server certificate, and click **Open**.
 - d. Click **Retrieve Certificate**.
 - e. Click **Commit**.
5. Repeat Step 2 to 4 for the other nodes of Avaya Oceana® Cluster 3.
6. Click **Done**.

Oceana Server page field descriptions

Field or Button	Description
Server Name	The name of the Oceana server.
Network Address	The IP address or hostname of the cluster on which the Oceana outbound service is deployed.
Action	The Delete icon to delete a server entry.
Add	The button to add an Oceana server.

Adding trusted Certificate Authority certificates

About this task

Use this procedure to do the following:

- Download a CA certificate file to the POM server.
- Place the downloaded CA certificate file into the trust store of the POM server.

On Experience Portal, if you install a custom CA certificate and then POM with a custom certificate, ensure that you establish communication among all internal POM servers.

To establish communication, you must first ensure that POM completes the exchange of certificates, and copies the updated trust store of the primary POM server on all auxiliary POM servers.

Location of the trust store on the POM primary server: `$POM_HOME/config/pomTrustStore`

Procedure

1. Log in to Avaya Experience Portal with the credentials of an administrator.
2. In the navigation pane, click **Proactive Outreach > Manager**.
3. In the content pane, click **Configurations > Trusted Certificates**.

POM displays all trusted certificates that you can import.

4. On the Trusted Certificates page, click **Import**.
5. On the Add Certificates page, do the following:
 - a. In **Name**, type the name of the certificate.
 - b. In **Enter Certificate Path**, click **Choose File**.

From the location of the file, select the file.

- c. Click **Continue**.
6. Open a command prompt terminal to the POM server.
 7. In the terminal, run the following command:

POM restart

8. For the changes to take effect, restart all POM services on the server.

Configuring an Outbound Provider

About this task

Use this procedure to create a new Outbound Provider through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Server Details**.
2. On the Avaya Oceana Server List page, double-click the UCAServer.
3. Select the **Providers** tab.
4. To add the Outbound Provider, do the following:
 - a. Click **Add**.
 - b. In **Type**, select **Outbound**.
 - c. In **Name**, type `POM`.
 - d. In **Address**, type `POM`.
 - e. Click **Save**.



Important:

To make the new provider available to Avaya Workspaces agents, you must restart the clusters.

Enabling Callback feature

About this task

Use this procedure to enable the callback feature.

Procedure

1. To enable the callback feature in the Avaya Oceana® integration with Avaya Proactive Outreach Manager, you must enable the **AutoDialCallback** parameter to true in the `pim_config` table.

2. Run the following select command to check the value of AutoDialCallback:

```
select * from pim_config where config_name='AutoDialCallback'
```

3. To enable the "AutoDialCallback" then execute the following command:

```
update pim_config set config_value = 'true' where  
config_name='AutoDialCallback'
```

Adding Disposition Codes for Outbound contacts

About this task

Use this procedure to add Disposition Codes for Outbound contacts through Avaya Control Manager.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

A POM Completion Code is automatically generated. Therefore, add Completion Codes to the POM server before adding them to Avaya Oceana®.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Work Codes**.
2. Click the **Disposition Codes** tab.
3. Click **Add** and do the following:
 - a. In the **Name** and **Number** fields, type the name and number of the Completion Code configured on the POM server.

Important:

The complete list of Avaya Oceana® Outbound Disposition Codes, including numeric codes and text, must match the complete list of POM Completion Codes.

While creating a POM campaign, the campaign must contain the complete list of all POM Completion Codes.

- b. In **Contact Type**, select the **Outbound** check box.
- c. Click **Save**.

Creating a user to handle Outbound contacts

About this task

Use this procedure to create an agent to handle Outbound contacts.

Before you begin

Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Select the location for your Avaya Oceana®.
4. Perform one of the following steps:
 - Click **Add**.
 - Select an existing user and click **Edit**.
5. Enter appropriate value in each of the following fields:
 - a. In the **First Name (English)** field, enter the first name of the user in English.
 - b. In the **Surname (English)** field, enter the surname of the user in English.
 - c. In the Available applications section, select the **Avaya Oceana** check box.
 - d. In the **LDAP Username** field, enter the LDAP user name of the user.

The LDAP user name must be in the username@domain.com format. This user name is used to log on to Avaya Workspaces.
 - e. In the **Username** field, enter a user name.

In this release, the user name is the internal handle.
 - f. In the **Password** field, enter a password.

This password is used to log on to Avaya Control Manager.
 - g. In the **Confirm Password** field, re-enter the password.
 - h. In the **Extension** field, enter the station associated with this agent.

This is used when logging on to Avaya Workspaces.
 - i. In the **AVAYA Login** field, enter the Elite agent login ID only if the agent also supports Voice contacts. Otherwise, leave this field blank.
 - j. Click **Save**.
6. Scroll to the right and select the **Avaya Oceana** tab.
7. Select the **Outbound** check box.



Important:

- Outbound users can have only Outbound account.
- Avaya Oceana® supports Hot Desking for Inbound Voice agents but does not support it for POM Outbound agents.

- To change the channel of an agent while the agent is live, the agent must be logged out and logged in again.
8. Select the **Attributes** tab.
 9. Move the attributes from the **Available Attributes** list to the **Agent Attributes** list.
-  **Important:**
- Ensure that the attributes assigned to the agent match the attributes configured in POM.
 - Do not assign a Work Assignment skill to the user.
10. Click **Save**.

Configuring After Contact Work time

About this task

Use this procedure to configure After Contact Work (ACW) time through Avaya Control Manager.

 Important:

Enabling ACW time is a mandatory global setting that impacts all interaction types.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration > Avaya Oceana™ > Server Details**.
3. Either double-click the administered Avaya Oceana® UCA server, or select the administered Avaya Oceana® UCA server and click **Edit**.
4. Select the **System Properties** tab.
5. Expand **After Contact Work**.
6. Select the **Enable After Contact Work** check box.
7. In the **After Contact Work Timer (Seconds)** field, enter the same time as the POM completion timer.

 Note:

Avaya Oceana® supports **After Contact Work Timer** settings only up to version 3.8. From version 3.8.1, Avaya Oceana® supports **After Contact Work Timer for Voice (Seconds)** for POM.

8. Click **Save**.

Chapter 10: Integrating POM with Avaya Workspaces for Elite

Overview

Avaya Workspaces for Call Center Elite is a browser-based agent desktop with which the contact center agents can handle customer interactions. Using the widget framework, the Avaya Workspaces for Call Center Elite administrators can configure POM widgets for the agents. After the POM widget is configured, the agents can interact and communicate with the POM contacts. Agents can sign in to POM through the POM widget and work with the contacts that they receive. Through this integration, agents can view customer journey visualization for the POM contacts.

This integration also allows agents to change the Agent Workspaces layout. Each customer interaction is displayed as an interaction card. The Agent Workspaces user interface has an intuitive layout that provides a visual representation of voice interactions.

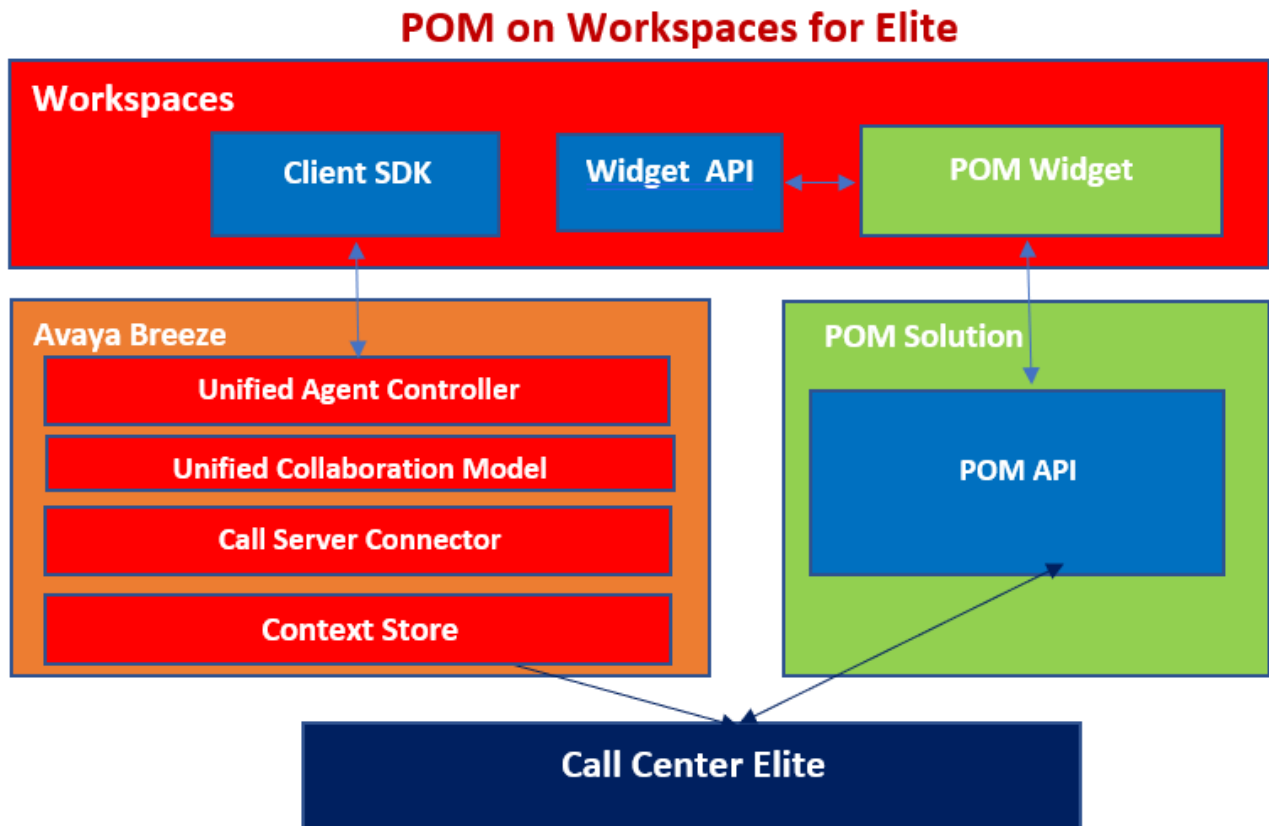


Figure 1: High level architecture

The diagram depicts the architecture for the POM integration with Avaya Workspaces for Call Center Elite.

Prerequisites

Before starting the POM and Avaya Workspaces integration, ensure that you have the following systems in functional state:

- Avaya Experience Portal, EPM, and MPP
- Avaya Aura®
- Avaya Control Manager
- Avaya Workspaces for Call Center Elite

POM - Elite Workspaces Integration checklist

Use the following checklist for POM - Avaya Workspaces for Call Center Elite integration:

No.	Task	Description	✓
1	Install POM and POM database in the Call Center Elite mode.	See the following two sections in <i>Implementing Avaya Proactive Outreach Manager</i> : • Installing POM on Avaya Experience Portal • Configuring the POM database on the primary POM server	
2	Deploy Avaya Workspaces for Call Center Elite.	See <i>Deploying Avaya Workspaces for Elite</i> .	
3	(Optional) Configure Context Store.	See <i>Avaya Context Store Snap-in Reference</i> .	
4	(Optional) Configure POM for Customer Journey feature.	See the topic Associating attributes for customer journey information in the <i>Administering Avaya Proactive Outreach Manager</i> guide.	
5	Configure POM by following the sequence of tasks in the checklist for configuring a POM server.	See POM Configuration in <i>Implementing Avaya Proactive Outreach Manager</i> .	
6	Add the LDAP server certificates to the three Avaya Breeze® platform nodes of Avaya Workspaces for Call Center Elite Cluster 1 only. For Avaya Workspaces for Call Center Elite large solutions, add the LDAP server certificates to the two Avaya Breeze® platform nodes of Avaya Workspaces for Call Center Elite Cluster 2 only.	See Configuring LDAP server certificates for Avaya Breeze® platform nodes in <i>Deploying Avaya Workspaces for Elite</i> .	
7	Export the Authorization Certificate from Avaya Breeze® platform nodes and import it to POM trusted certificate.	See Exporting the Authorization Certificate from Breeze nodes on page 91 and Importing authorization certificate to POM trusted certificate on page 91.	
8	Configure POM server details on System Manager.	See Configuring POM system details on Avaya Aura System Manager on page 92.	

Table continues...

No.	Task	Description	✓
9	Complete POM configurations such as contact list, campaign strategies, completion codes, and campaigns.  Note: To avoid Network Time Protocol (NTP) error, POM server time must be synchronized with Avaya Breeze® platform server time.	See <i>Administering Avaya Proactive Outreach Manager</i> .	
10	Deploy widgets.	See Deploying POM widgets on page 93.	
11	Configure an agent in Avaya Control Manager.	See Configuring an agent in Avaya Control Manager on page 96.	

Exporting the Authorization Certificate from Breeze nodes

Procedure

1. Log in to the Avaya Aura® System Manager web console.
2. Click **Services > Inventory > Manage Elements**.
3. Select the Breeze node.
4. Click **Manage Identity Certificates**.
5. Select **Authorization**.
6. Click **Export**.
7. Repeat steps 1 to 6 for all Breeze nodes.

Importing authorization certificate to POM trusted certificate

Procedure

1. Log in to Avaya Experience Portal.
2. In the navigation pane, click **Proactive Outreach > Manager**.

3. In the content pane, click **Configurations > Trusted Certificates**.

4. Select the certificate, and click **Import**.

Import the Breeze node certificate you exported in [Exporting the Authorization Certificate from Breeze nodes](#) on page 91. Import all node certificates to POM trusted certificate.

5. Repeat step 2 to step 4 for additional Breeze nodes.

6. Restart the POM services.

Configuring POM system details on Avaya Aura® System Manager

About this task

Use this procedure to configure POM server details on System Manager. You can configure a maximum of four POM servers.

Procedure

1. Log in to System Manager.
2. Click **Elements > Avaya Breeze® > Configuration > Attributes**.
3. Click the **Service Clusters** tab.
4. In **Cluster**, select the required cluster.
5. In **Service**, select **UCAStoreService**.
6. To configure a POM server, do the following:
 - a. Click **Override Default**.
 - b. In the **Effective Value**, enter the appropriate value.

You can configure up to four POM servers.

7. Click **Commit**.

POM system configuration field descriptions

Name	Description
POM name	The name of the POM system. This is a mandatory field.
POM primary administration interface FQDN or IP address	The Fully Qualified Domain Name (FQDN) or IP address for the primary administration interface of this POM system. This is a mandatory field.

Table continues...

Name	Description
POM secondary administration interface FQDN or IP address name	The FQDN or IP address for the secondary administration interface of this POM system.
POM administration interface username	The user name for the administration interface of this POM system.
POM administration password	The user password for the administration interface of this POM system. If the password field changed, the change is effective after a re-install of the SVAR, otherwise, it is effective immediately. This is a mandatory field.
POM primary widget interface FQDN or IP address	The FQDN or IP address of the POM server. This is a mandatory field.
POM primary widget interface port	The port number of the primary POM system where the Agent SDK service is operational. For example, 6443. This is a mandatory field.  Note: Port interfaces operate only in secured mode.
POM secondary widget interface FQDN or IP address	The FQDN or IP address for the secondary widget interface to the POM system.
POM secondary widget interface port	The port number for the secondary widget interface to the POM system. For example, 6443.
POM widget download location URL	The URL for the widget download location of the POM system.
POM calling line identifier	The Nailup call CLID. The value in this field must be the same as the Nailup call CLID on the POM Global Configurations page. This is a mandatory field.

Deploying POM widgets

About this task

Use this procedure to deploy POM widgets on the web server.

Before you begin

Log in to Avaya Workspaces with administrator credentials and download the Avaya Workspaces Widget Framework document. Widget Framework is a feature that extends the customization capabilities of Avaya Workspaces.

With this feature, contact centers can:

- Customize the layout and behavior of Avaya Workspaces for an entire contact center
- Access Widget API so that developers can create custom widgets that can be configured and deployed in Avaya Workspaces

Choose the web server to deploy the widgets and ensure:

- The web server is hosted on the same network as Avaya Oceana®.
- The web server has a network RTT of less than 120 milliseconds.
- The web server is configured for CORS.
- If you host the library on POM Tomcat server, edit the file:

For example: `/opt/AppServer/Tomcat/apache-tomcat-8.5.15/webapps/conf/web.xml` and add the following content to the configuration within the `</web-app>` tag.

```
<filter>
<filter-name>CorsFilter</filter-name>
<filter-class>org.apache.catalina.filters.CorsFilter</filter-class>
<init-param>
<param-name>cors.allowed.origins</param-name>
<param-value>*</param-value></init-param>
<init-param>
<param-name>cors.allowed.methods</param-name>
<param-value>GET,POST,PUT,DELETE,HEAD,OPTIONS</param-value>
</init-param>
<init-param>
<param-name>cors.exposed.headers</param-name>
<param-value>Access-Control-Allow-Origin</param-value>
</init-param>
</filter>
<filter-mapping>
<filter-name>CorsFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>
```

- Change the `cors.allowed.origins` value to the `*`.
- For IIS Server version 7.0, merge the following into the `web.config` file at the root of your application or site:

```
<?xml version="1.0" encoding="utf-8"?> <configuration>
<system.webServer> <httpProtocol> <customHeaders> <add name="Access-
```

```
Control-Allow-Origin" value="*" /> </customHeaders> </httpProtocol>
</system.webServer> </configuration>
```

The Access-Control-Allow-Origin value is the Workspaces FQDN URL.

- The web server is configured in HTTPS mode.

You can use the POM tomcat server to deploy the widgets, which is available at the following location:

```
/opt/AppServer/Tomcat/apache-tomcat-8.5.15/webapps/widgets
```

*** Note:**

- The web server supports a maximum of 1000 POM agents.
- The web server will not have overload issues because the server hosts only the static version of files.

Procedure

1. Ensure that all agents are logged out.
2. Stop or pause all running campaigns.
3. Stop the web server.
4. Download the widget from the download location.
5. Unzip the widget file into a folder on the web server.

All files are unzipped in the current directory.

*** Note:**

Modify the permission of the folder `pom-connectorwidget` which got created after unzipping the widgets by using the following command:

```
chmod -R 755 pom-connectorwidget
```

6. Delete the old widget directory from the main widget directory.
7. Copy unzipped files to the main widget directory for example "widget-library" and maintain the structure names as present in the zip file.
8. Restore the configurations:
 - a. Make changes to the parameters in the `properties.json` looking at the backup file from the `pom-connectorwidget\conf\properties.json` if there were any changes.
 - b. Restore `reasonCode.json` if you are using the file based not ready reason codes.
9. After installing the widgets on the web server, restart the web server.

Next steps

Verify the widget version:

Use the following link from the Workspace client to verify the version of the JSON:

```
https://<widgetserver-baseURL>/pom-connectorwidget/pom-connector.json
```

The widget version is displayed in the JSON format. For example: "version": "3.7-3.1.3.1.2-4.0.0.0.47"

Configuring an agent in Avaya Control Manager

Procedure

1. Log in to Avaya Control Manager.
2. Click **Users**.
3. Click the agent that you want to configure.
4. Click the **Avaya Oceana** tab.
5. In the **POM instances** field, select the instance that you configure on System Manager.
6. In the **Organization** field, select the required organization.
7. In the Zone field, select the required zone.
8. Click **Save**.

Installing web server root certificate

If the web server is using self signed certificates, these web server root certificates must be installed at the browser client by accessing the below URLs and importing the certificates to the trust store of the client machine.

`https://<widgetserver-baseURL>/pom-connectorwidget/css/pom-connector.css`

Procedure

1. On the UCA configuration page, verify whether you can access the URL of the widget location base.
2. In the browser that you are using to access Workspaces, verify whether you can access the URL of the widget location base.
3. In the browser that you are using to access Workspaces, verify whether you can access the URL of POM Server Agent SDK Service.

You can access the widget location base at `https://<pomserver-ip>:6443/health>`.

Connector widget configuration

The connector widget has configuration information stored on the widget location in the JSON format. The JSON file to change the configurations is `<widget-deploy-location>/pom-connectorwidget/conf/properties.json`.

For example, if widgets are deployed on POM Tomcat Application server, the default location of the `properties.json` file is `/opt/AppServer/Tomcat/apache-tomcat-8.5/webapps/widgets/`.

* Note:

After making changes to any configurations in `properties.json`, you must restart the web container such as Tomcat on which widgets are deployed. Agents must log out and log in to POM Workspaces to notice the changes.

The parameters can be configured based on the requirement.

```
{
  "FORCE_LOGIN" : "false",
  "API_TIMEOUT" : "30",
  "TRANSPORT" : "websocket",
  "FALLBACK_TRANSPORT" : "long-polling",
  "LOG_LEVEL" : "info",
  "POM_CON_RETRY_COUNT" : "3",
  "POM_REFRESH_TIMEOUT" : "15",
  "CALLBACK_DUE_IN_UTC" : "FALSE",
  "DISABLE_IS_IN_DO_NOT_CALL_LIST" : "FALSE",
  "DISABLE_ADD_TO_DO_NOT_CALL_LIST" : "FALSE",
  "USE_ELITE_NOT_READY_REASON_CODES" : "TRUE",
  "AGENT_SCRIPT_FOR_SCREENPOP" : "FALSE",
  "REPLACE_CHAR_FOR_SCREENPOP" : "$",
  "PENDING_CALLBACK_TIMEOUT" : "0",
  "MAX_CALLBACK_DAYS" : "-1",
  "TWENTY_FOUR_HOUR_CLOCK_FORMAT" : "TRUE",
  "DISABLE_DTMF" : "FALSE",
  "DISABLE_NOTES" : "FALSE",
  "DISABLE_CALLBACK" : "FALSE",
  "DISABLE_CALLBACK_WIDGET_IN_PREVIEW" : "FALSE",
  "WALK_AWAY_AGENT_CALLS_COUNT" : "2",
  "SHOW_BLENDING_NOTIFICATIONS" : "TRUE",
  "BLENDING_MODE" : "NOTIFY-CARD",
  "CONTACT_CARD_TITLE" : "$title Predefined$ $Last Name$ $First Name$",
  "SHOW_DEFAULT_COMPLETION_CODE" : "FALSE",
  "JOB_NOTIFICATIONS" : "TRUE",
  "SORT_COMPLETION_CODE" : "FALSE",
  "SORT_REASON_CODES" : "FALSE",
  "SHOW_DEFAULT_EXPIRY_TIME" : "TRUE",
  "SHOW_EXTERNAL_NUMBER_IN_CALLBACK" : "TRUE",
  "SHOW_FREEFORM_IN_CONSULT" : "TRUE",
  "SHOW_FREEFORM_IN_PREVIEW" : "TRUE",
  "SHOW_FREEFORM_IN_REDIAL" : "TRUE",
  "MAINTAIN_CALLBACK_NOTES_HISTORY" : "TRUE",
  "SHOW_WARNING_FOR_OVERRIDING_CALLBACK" : "FALSE",
  "MANUAL_BLEND" : "FALSE",
  "REVERSE_BUTTONS_IN_COMPRESSED" : "TRUE",
  "SHOW_COMPLETION_CODE_IN_TALKING" : "FALSE",
  "SORT_COMPLETION_CODE_ON" : "codeID",
  "ENABLE_SEMI_AUTOMATION_FOR_MANUAL_CAMPAIGN" : "TRUE",
  "DISPLAY_CONTACT_LIST_NAME" : "FALSE",
  "CUSTOMER_DETAIL_WIDGET_TITLE" : ""
}
```

```

"CUSTOMER_DETAIL_WIDGET_HEADING"      : "$Title Predefined$ $Last Name$ $First Name$",
"CUSTOM_COMPLETION_CODE"              : {"Default": "FALSE"},
"PREVIEW_DIAL_FAILED_NOTIFICATION"    : "info"
}

```

Attribute name	Description
FORCE_LOGIN	Controls the permissions to do a force login to POM every time while logging in. The default value of the attribute is FALSE. The values are: • TRUE = The agent selects the Force login check box. • FALSE = The agent does not select the Force login check box. If the login attempt fails, the agent can select the Force login check box to do a force login to POM.
API_TIMEOUT	The number of seconds to wait for an API response from the POM server. If the server does not send a response within the stipulated time, the request times out. The possible value of this attribute is any positive integer. The default value is 30 seconds.
TRANSPORT	Controls the socket connection type. The values are: • websocket • long-polling The default value is websocket.
FALLBACK_TRANSPORT	Controls the fallback socket connection type if the TRANSPORT connection type fails. The values are: • websocket • long-polling The default value is long-polling.
LOG_LEVEL	Controls the debug level of the widgets in the Browser Console. The values are: • debug • info • warning • error The default value is debug.
POM_CON_RETRY_COUNT	Controls the number of reconnect attempts to be made if there is a disconnect from the POM server. Possible value is any positive integer. The default value is 3.

Table continues...

Attribute name	Description
POM_REFRESH_TIME OUT	Controls the number of reconnect attempts to be made if there is a disconnect from the POM server. Possible value is any positive integer. The default value is 15.
CALLBACK_DUE_IN_U TC	Converts the Callback Due Time to local Agent Desktop Time. The default value is FALSE. The values are: • TRUE = Callback Due Time is converted to Local Desktop Time of Agent. • FALSE = Callback Due Time is the time in which the POM server is currently located.
DISABLE_IS_IN_DO_N OT_CALL_LIST	Enables or disables the “Is In DNC” functionality. The default value is FALSE. The values are: • TRUE = “Is In DNC” functionality is disabled. • FALSE = “Is In DNC” functionality is enabled.
DISABLE_ADD_TO_DO _NOT_CALL_LIST	Enables or disables the “Add to DNC” functionality. The default value is FALSE. The values are: • TRUE = “Add to DNC” functionality is disabled. • FALSE = “Add to DNC” functionality is enabled.
USE_ELITE_NOT_REA DY_REASON_CODES	Determines whether to use the Elite Not Ready codes for Outbound or use the reason codes configured in the Not Ready Reason code file. The default value is TRUE.
AGENT_SCRIPT_FOR _SCREENPOP	Controls whether the Agent Script configured for the campaign is used for Screenpop in Agent Script widget. The parameters can be configured using the Replace character. Possible values are either TRUE or FALSE. The default value is FALSE.
REPLACE_CHAR_FOR _SCREENPOP	Determines whether to replace the customer field value. Any field enclosed in this character is replaced while reconstructing the Screenpop URL. For example, \$First Name\$ is replaced by the value of the First Name Attribute value. Possible value is any valid character. The default value is \$.
PENDING_CALLBACK _TIMEOUT	Sets the time duration for which the Pending callback Card persists. The default value is zero. The values are: • 0 = Pending Callback Card persists till callback expires or callback is successful. • any value > 0 = Pending Callback Card persists for the specified time only.
MAX_CALLBACK_DAY S	Controls the date selection in callback widget. Only these many days can be selected for Callback. If the value is -1 then no restriction is applied. Possible value is any integer >=-1. The default value is -1.

Table continues...

Attribute name	Description
DISABLE_DTMF	Enables or disables DTMF functionality. The default value is FALSE. The values are: • TRUE = "DTMF" functionality is disabled. • FALSE = "DTMF" functionality is enabled.
WALK_AWAY_AGENT_CALLS_COUNT	Controls the setting of the Agent state to walkaway. For example, if for two consecutive calls the agent is not pressing any buttons on the screen, then the agent is set to Not Ready with walkaway. Possible value is any integer >=1. The default value is 2.
TWENTY_FOUR_HOUR_CLOCK_FORMAT	Determines whether to show the callback start and expiry time in 24-hour or 12-hour format. Possible values are either TRUE or FALSE. The default value is TRUE.
SHOW_BLENDING_NOTIFICATIONS	Shows the blending notifications. The default value is TRUE. The values are: • TRUE = Get inbound/outbound blending notifications. • FALSE = Do not get the notifications.
BLENDING_MODE	Controls the system behavior when Agent is blended to Inbound or Outbound. The values are: • NOCARD = If the agent is released to inbound or outbound mode by the blending engine then there is no card displayed to the agent to switch the state if the Agent is in Not Ready State in the destination mode. • NOTIFY-CARD = A custom card is displayed to the agent with a button to switch to the destination Ready state if the agent is in the Not Ready state for the destination mode. • AUTO = Switches the agent states to READY automatically if not in the READY state. The default value is NOTIFY-CARD.
CONTACT_CARD_TITLE	Controls any attribute of the Contact list to be displayed in the Contact card. Place the attribute name inside \$ \$ characters. For example, \$Title Predefined\$ \$Last Name\$ \$First Name\$. The possible value is any String, with a replaceable parameter name. The default value of this parameter is \$Title Predefined\$ \$Last Name\$ \$First Name\$".
SHOW_DEFAULT_COMPLETION_CODE	Determines whether to show or hide the default completion code in the completion code list used for wrap-up. Possible values are either TRUE or FALSE. The default value is FALSE.
JOB_NOTIFICATIONS	Determines whether to show or hide the job attached notification to the agent. Possible values are either TRUE or FALSE. The default value is TRUE.

Table continues...

Attribute name	Description
SORT_COMPLETION_CODE	Determines whether to sort the completion code list in alphabetical order and display to the Agent as there is a limit to display only 20 codes in the UI. The rest of the codes can be searched. Possible values are either TRUE or FALSE. The default value is FALSE.
SORT_REASON_CODES	Determines whether to sort the Not Ready Reason codes list in alphabetical order and display to the Agent as there is a limit to display only 20 codes in the UI. The rest of the codes can be searched. Possible values are either TRUE or FALSE. The default value is FALSE.
SHOW_DEFAULT_EXPIRY_TIME	Determines whether to show or hide the Callback Expiry Time in the callback widget. Possible values are either TRUE or FALSE. The default value is TRUE.
SHOW_EXTERNAL_NUMBER_IN_CALLBACK	Determines whether to allow or restrict setting External Number in the callback widget. Possible values are either TRUE or FALSE. The default value is TRUE.
SHOW_FREEFORM_IN_CONSULT	Determines whether to show or hide the free-form number input for the consult operation in the outbound contact card. Possible values are either TRUE or FALSE. The default value is TRUE.
SHOW_FREEFORM_IN_PREVIEW	Determines whether to show or hide the free-form number input in case of Preview-Dial Operation in the outbound contact card. Possible values are either TRUE or FALSE. The default value is TRUE.
SHOW_FREEFORM_IN_REDIAL	Determines whether to show or hide the free-form number input in case of Redial Operation in the outbound contact card. Possible values are either TRUE or FALSE. The default value is TRUE.
SHOW_WARNING_FOR_OVERRIDING_CALLBACK	Determines whether all controls of callback tab in outbound tools widget should be disabled, after a callback is set for a particular POM contact. Select the override check box to override the existing callback. Possible values are either TRUE or FALSE. The default value is FALSE.
DISABLE_NOTES	Enable or disable the Agent Notes feature. The default value is FALSE. The values are: • TRUE = Agent Notes functionality would be disabled. • FALSE = Agent Notes functionality would be enabled.
MAINTAIN_CALLBACK_NOTES_HISTORY	Determines whether callback notes history should be maintained while creating a callback. The default value is TRUE. The values are: • TRUE = Callback notes history is maintained while creating a callback • FALSE = Callback notes history is not maintained while creating a callback
DISABLE_CALLBACK	Enable or disable the Callback feature. The default value is FALSE. The values are: • TRUE = Callback functionality would be disabled. • FALSE = Callback functionality would be enabled.

Table continues...

Attribute name	Description
DISABLE_CALLBACK_WIDGET_IN_PREVIEW	Enable or disable the Callback widget in preview feature. You can customize the feature using the following options: • 1: The feature is removed from the options. The parameter is removed from <code>properties.json</code>. • 2: The default value is set to FALSE. <code>"DISABLE_CALLBACK_WIDGET_IN_PREVIEW": "FALSE"</code> • 3: The default value is set to TRUE. <code>"DISABLE_CALLBACK_WIDGET_IN_PREVIEW": "TRUE"</code> • 4: The parameter is available but organization can be different than the organization of the logged-in agent. <code>DISABLE_CALLBACK_WIDGET_IN_PREVIEW": "org": "FALSE"</code> • 5: The parameter is available and the organization remains the same as the organization of the logged-in agent. The value is set to TRUE. <code>"DISABLE_CALLBACK_WIDGET_IN_PREVIEW": "DEFAULT": "TRUE"</code> • 6: The parameter is available and the organization remains the same as the organization of the logged-in agent. The value is set to FALSE. <code>"DISABLE_CALLBACK_WIDGET_IN_PREVIEW": "DEFAULT": "FALSE"</code>
MANUAL_BLEND	Enable or disable the Manual Blend feature. The default value is FALSE. The values are: • TRUE = The Manual Blend functionality is enabled. • FALSE = The Manual Blend functionality is disabled.
SHOW_COMPLETION_CODE_IN_TALKING	Enable or disable the Show Completion Code In Talking State feature. The default value is FALSE. The values are: • TRUE: The Show Completion Code In Talking State feature is enabled. • FALSE: The Show Completion Code In Talking State feature is disabled.
ENABLE_SEMI_AUTO_MOTION_FOR_MANUAL_CAMPAIGN	Enable or disable the Semi Automation For Manual Campaign feature. The default value is TRUE. The values are: • TRUE: The Semi Automation For Manual Campaign feature is enabled. • FALSE: The Semi Automation For Manual Campaign feature is disabled.

Table continues...

Attribute name	Description
REVERSE_BUTTONS_IN_COMPRESSED	Use this parameter to enable Workspaces to control the positions of the buttons displayed in the Contact card. You can use this parameter only if you use the compressed layout. The default value of this parameter is TRUE. TRUE = Workspaces displays the most frequently used buttons on the right on the Contact card. FALSE = Workspaces displays the buttons as were displayed in the previous release.
CUSTOMER_DETAIL_WIDGET_TITLE	Use this parameter to configure customer details title of the customer detail widget. The default value of this parameter is None. Nothing is displayed in front of customer detail title. • \$Campaign Name\$: Campaign name is displayed in front of customer detail title. • \$Contact List Name\$: Contact list name is displayed in front of customer detail title. • \$Campaign Name\$ \$Contact List Name\$: Campaign name and contact list name is displayed in front of customer card title. You can also add separators in between the keywords like &, *, → , etc (i.e → \$Campaign Name\$ & \$Contact List Name\$).
CUSTOMER_DETAIL_WIDGET_HEADING	Use this parameter to configure customer details heading of the customer detail widget. • The default value of this parameter is \$Title Predefined\$ \$Last Name\$ \$First Name\$. In this case the first name and last name is displayed • \$Title Predefined\$ \$Last Name\$ \$First Name\$ \$Campaign Name\$: In this case campaign name is displayed in front of the first name and last name. • \$Title Predefined\$ \$Last Name\$ \$First Name\$ \$Contact List Name\$: In this case, the contact list name is displayed in front of first name and last name. • \$Title Predefined\$ \$Last Name\$ \$First Name\$ \$Campaign Name\$ \$Contact List Name\$: In this case, campaign name and contact list name is displayed in front of first name and last name.  Note: You can remove the title, first name and last name to display only campaign name or contact list name in heading. You can add separators in between the keywords like &, *, → , etc (i.e → \$Campaign Name\$ & \$Contact List Name\$).

Table continues...

Attribute name	Description
DISPLAY_CONTACT_LIST_NAME	This parameter is used for configuring whether to display contact list name or campaign name on customer card leg title. The default value for this parameter is FALSE which means campaign name is displayed by default.
SORT_COMPLETION_CODE_ON	This parameter works only work if the existing "SORT_COMPLETION_CODE" flag is set to "TRUE". The possible values are codeId , and codeValue. The default value is codeId. When SORT_COMPLETION_CODE is enabled the Default sorting will be performed on completion code Id (codeId). And if Completion Code Name (codeValue) is configured for SORT_COMPLETION_CODE_ON parameter, then it will follow Alphanumeric Sorting.
CUSTOM_COMPLETION_CODE	This parameter enables or disables the Completion code selection button on the custom card in POM widgets. You can set two values for this parameter as follows: TRUE = To disable the Completion code selection button. FALSE = To enable the Completion code selection button. The default value of this parameter is set to FALSE. Even if you set the CUSTOM_COMPLETION_CODE to FALSE, an agent can still use the custom widget to select the custom completion codes and release the line. You can specify the organization for which you want to enable or disable the Completion code selection button. For example, <pre>"CUSTOM_COMPLETION_CODE": { "Default": "FALSE", "Org1": "TRUE", "Org2": "TRUE", "Org3": "TRUE" }</pre> By default, the flag is disabled for the Default organization. Only the Default organization is present in the widget configuration file. This means the completion code selection button is available in the custom card only for the Default organization. You cannot set a value for this parameter if the campaign is running in the Preview or Dialing or Callback state. Third party widgets can set the completion code by using the following API: <pre>POMCONNECTORWIDGET.setCustomCompletionCodeAndReleaseLine (Completion code, Line Release)</pre> If a client invokes this API with the line release flag set to "Yes" , POM automatically releases the line and puts the Agent in wrap-up.

Table continues...

Attribute name	Description
PREVIEW_DIAL_FAILED_NOTIFICATION	Controls the severity of the <code>Dial Failed</code> notification displayed on Workspaces. The default value of this attribute is set to <code>INFO</code>. The possible values are: <code>INFO</code> = displays the notification as an information message. <code>ERROR</code> = displays the notification as an error message. You can set this value to ensure backward compatibility.

Customer Interaction Card

The customer interaction card leg title format is `<Pacing Type> Campaign : <Campaign Name>` or List as `<List Name>`

The customer interaction card is configurable by the `DISPLAY_CONTACT_LIST_NAME` parameter from `properties.json` file of pom-connector widget. The default value for this parameter is `FALSE`, which means the campaign name is displayed by default.

When the agent is in talking, on hold, and dialing state, then agent state is shown in leg title instead of campaign or list name. However, the leg title tooltip always shows the campaign name and list name.

The tooltip format is:

`<Pacing Type> Campaign : <Campaign Name> , List : <List Name>`

Changing Workspaces layout for an outbound enabled agent

About this task

Use this procedure to change the layout of the agent Workspaces.

Procedure

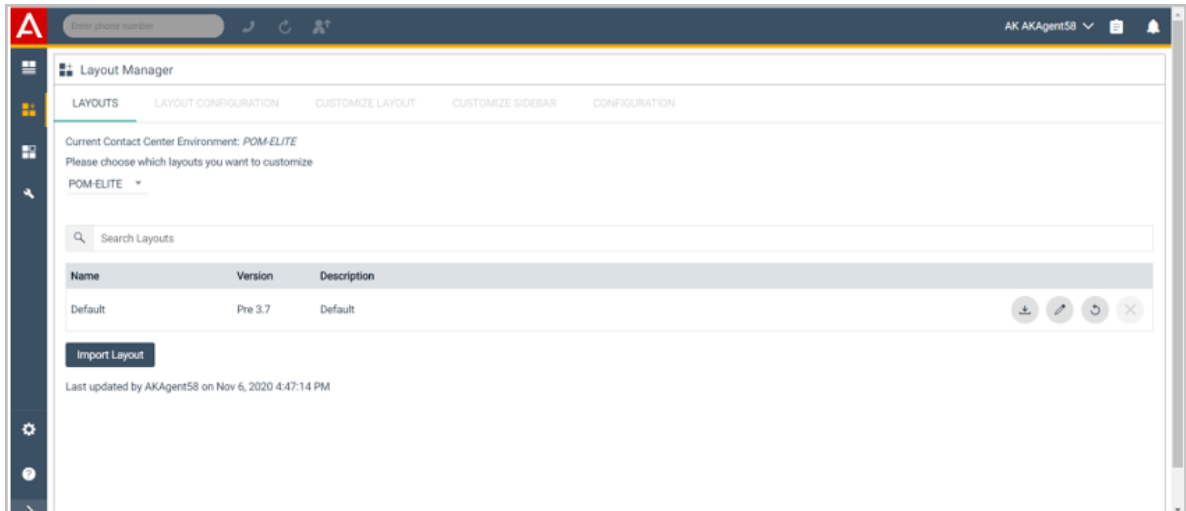
1. Log in to Avaya Workspaces for Call Center Elite with administrator credentials.

2. Click the  icon.

Avaya Workspaces for Call Center Elite displays the Layout Manager page. By default, Avaya Workspaces for Call Center Elite displays the **CUSTOMIZE LAYOUT** tab.

3. In the **Please choose which layout you want to customise**, select `POM-ELITE`.

Avaya Workspaces for Call Center Elite reloads and opens in `POM-ELITE` mode:



4. Click the Edit icon.

Avaya Workspaces for Call Center Elite displays the LAYOUT CONFIGURATION tab.

5. Click the **CUSTOMIZE LAYOUT** tab
6. Click **CUSTOM**.

Avaya Workspaces for Call Center Elite displays the **CUSTOMIZE SIDEBAR** tab.

7. In the **Please select a sidebar tab** area, click the edit icon corresponding to **CUSTOM (Default Tab)**

Avaya Workspaces for Call Center Elite displays the **CONFIGURATION** tab.

8. In the **Select Layout** area, select the required layout.
9. In the **Select Widgets** area, click the required widgets.
10. Click **Save Changes**.

*** Note:**

Ensure that you configure the connector widget on the home layout and the customer details, agent script, and outbound widgets on the custom card layout.

POMAgentSDK failover

When the POMAgentSDK service fails, *Outbound Server* removes all outbound work cards except the agent acquired call card. The widgets attempt to retry connecting to the secondary SDK service.

Depending on whether the agent is in an active customer call or not, the scenarios are as follows:

The default connection retry count is 3 and the administrator can configure this value as required.

- Agent is on an active customer call - The on-going customer call continues. The widgets attempt to connect to the secondary server. To connect to the secondary server, the agent must click **Start Outbound Work**. Internally during the failover process, the *Outbound Server* marks that agent for pending logout. After the agent disconnects the customer call, the agent is logged out of the system.
- Agent is not on an active customer call - Agent logs in to the secondary service and clicks **Go Ready** if in a Not Ready state. The agent does not need to take any further action.

Agent Manager failover

When an Agent Manager failover occurs, POM blocks all the user operations and if the agent is on an active customer call, the agent cannot perform any operations until the Agent Manager service is functional. POM retains the active customer call. The agent does not need to take any further action.

Configuring POM Workspaces with WebRTC

Overview

POM supports WebRTC enabled agents, allowing the agents to handle interactions using their browser, without a physical phone or a softphone. POM can nail up WebRTC enabled agents and the agents can then handle outbound calls if Avaya Workspaces is integrated with WebRTC.

Important:

Do not select the **Hide nailed-up interaction card** option because if the nail-up call is hidden in WebRTC mode, an agent cannot drop the nail-up call, or hold or unhold the nail-up call.

Checklist for configuring Avaya Workspaces for Call Center Elite with remote WebRTC enabled agents

Use the following checklist to configure Avaya Workspaces for Call Center Elite with remote WebRTC enabled agents so that the agents can handle PSTN Voice, Web Voice, and Web Video calls:

For detailed instructions about configuration, see the *Configuring Avaya Workspaces for Call Center Elite with Avaya WebRTC Connect* guide on Avaya Support website at <https://support.avaya.com/>.

Note:

You do not need to perform any configuration on Avaya Proactive Outreach Manager.

No.	Task	Reference topics in the <i>Configuring Avaya Workspaces for Call Center Elite with Avaya WebRTC Connect</i> guide	✓
1	Deploy Avaya Aura® Web Gateway	Deploying Avaya Aura® Web Gateway	
2	Set up LDAP (optional)	Configure LDAP	
3	Install and configure Avaya Aura® Device Services	Avaya Aura® Device Services deployment	
4	Configure Avaya Aura® Web Gateway: Device services, HTTP clients, Media servers, CORS, Trusted hosts	Configuring Avaya Aura® Web Gateway	
5	Enable Token service	Enabling Token Service and TestApp	
6	Install and configure Avaya Aura® Media Server	Install and configure Avaya Aura Media Server for Avaya Aura Web Gateway	
7	Configure authorization on Avaya Aura® Web Gateway	Avaya Aura Web Gateway authorization: • Creating the common certificate • Importing the authorization certificate	
8	Create agents that can use media in browsers	Creating a user in Avaya Control Manager	
9	Configure VDN's and Vectors for Workspaces for Elite	Configuring VDN's and vectors for Avaya Workspaces for Elite	
10	Install and configure Avaya Aura® Session Border Controller to enable customer PSTN Voice, Web Voice, and Web Video calls from the public internet	See Install and configure Avaya Aura® Session Border Controller	

Chapter 11: Resources

Documentation

For information on feature administration, interactions, considerations, and security, see the following documents available on the Avaya Support site at <https://www.avaya.com/support>.

Install Avaya Experience Portal before implementing POM. References to Avaya Experience Portal documentation are available at various places in the POM documentation.

Title	Description	Audience
Overview		
<i>Avaya Proactive Outreach Manager Overview and Specification</i>	Provides general information about the product overview and the integration with other products.	Users
Implementing		
<i>Implementing Avaya Proactive Outreach Manager</i>	Provides information about installing and configuring Proactive Outreach Manager.	Implementation engineers
<i>Upgrading Avaya Proactive Outreach Manager</i>	Provides information about upgrading and migrating Proactive Outreach Manager.	Implementation engineers
<i>Troubleshooting Avaya Proactive Outreach Manager</i>	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
<i>Avaya Proactive Outreach Manager Integration</i>	Provides information on Proactive Outreach Manager integration with Avaya Oceana [®] , Avaya Workspaces for Elite, Avaya Aura [®] Communication Manager, Avaya Experience Portal, Call Management System, Avaya Contact Recorder, Avaya Control Manager, and Avaya Aura [®] System Manager.	Administrators
<i>Avaya Proactive Outreach Manager High Availability</i>	Provides information for implementing high available POM system in a single data center, and also explains POM behavior in case of failure and high availability.	Administrators
Using and administering		

Table continues...

Title	Description	Audience
<i>Administering Avaya Proactive Outreach Manager</i>	Provides general information about field descriptions and procedures for <i>Administering Avaya Proactive Outreach Manager</i> .	Users and system administrators
<i>Using Avaya Proactive Outreach Manager supervisor dashboard</i>	Provides instructions on using Proactive Outreach Manager supervisor dashboard.	Supervisors
<i>Using Avaya Workspaces for Avaya Proactive Outreach Manager</i>	Provides instructions on using Avaya Workspaces for Proactive Outreach Manager.	Agents
<i>Using Avaya Proactive Outreach Manager Reports</i>	Provides information about reports in Proactive Outreach Manager.	Users System administrators

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.

Appendix A: Cipher requirements of Java implementation

Overview

POM uses a set of cipher suites that might not be supported by the Java implementation installed on the application server. This includes the cipher suites that use AES_256 and require installation of the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. To use a stronger algorithm, obtain the JCE Unlimited Strength Jurisdiction Policy Files and install it in the JDK/JRE.

 Note:

It is the responsibility of the customer to verify that this action is permissible under local regulations. If not, customer can remove the unsupported ciphers from the connector in the `server.xml` of Apache Tomcat. Customers can also use the default ciphers of the installed Java implementation by removing the ciphers attribute from the connector element of `$APPSERVER_HOME/conf/server.xml`. For more information, see *Troubleshooting Avaya Proactive Outreach Manager*.

For WebSphere, POM uses the default cipher suites provided by the IBMJSSE2 provider. However, if the customer wants to use specific cipher suites, then the customer must configure the `enabledCiphers` property in the `WASConfig.properties` file and set those ciphers suites as comma separated values.

For example:

```
enabledCiphers=TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256.
```

For more information, see the following Java Implementation links:

- For Oracle Java, see <https://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html>.
- For IBM Java, see https://www.ibm.com/support/knowledgecenter/en/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/ciphersuites.html.

If there is a mismatch between configured ciphers on the application server and the supported ciphers by the underlying Java implementation, application server logs display the following exception:

```
java.lang.IllegalArgumentException: Cannot support <Unsupported Cipher name> with currently installed providers.
```

Appendix B: TLSv1.2 configuration on WebSphere

Configuring TLSv1.2 on WebSphere

About this task

Use this procedure to configure TLSv1.2 on a WebSphere application server to work with POM for each incoming and outgoing communication.

When you use IBM WebSphere as an application server in a POM deployment, IBM WebSphere must meet the CEC-security requirement to communicate over TLSv1.2 on each of its interfaces.

Before you begin

Use the following:

- Java 7 or 8.
- WebSphere 8.5.5 or later versions.

Procedure

1. Log on to the WebSphere Application Server Integrated Solutions Console by using a web browser.
2. In the navigation pane, click **Security > SSL certificate and key management**.
3. On the **Related Items** tab, click **SSL configurations**.
4. Click the **Default SSL settings** link.
5. On the Additional Properties page, click **Quality of protection (QoP) settings**.
6. On the General Properties page, from the **Protocol** list, select **TLSv1.2**.
7. In the **Cipher suite settings** area, from the **Cipher suite groups** list, select **Strong**.
8. In the **Cipher suite settings** area, click **Update selected ciphers**.
9. Click **OK**.

Save the updated cipher files in the same location as the master configuration.

10. In the navigation pane, click **Security > SSL certificate and key management > Manage FIPS**.
11. On the **Manage FIPS** page, click **Enable SP800-131** and then click **Transition**.

12. Click **OK**.
13. If the system displays a non-compliant certificate error, perform the following steps:
 - a. On the **Related Items**, click **Convert certificates**.
 - b. Set the **Algorithm** setting to **Strict**.
 - c. From the **New certificate key size** list, select **2048 bits**.
 - d. Click **OK**.

You can save the file in the same location as the master configuration.

14. Navigate to the following location to access the `ssl.client.props` file:

`WAS_Profile_Dir/properties`

15. Open the `ssl.client.props` file and edit the following:
 - a. Set the `com.ibm.security.useFIPS` property to `true`.
 - b. Set the `com.ibm.websphere.security.FIPSLevel` property to `SP800-131`.
If this line already exists, do not write this line again.
 - c. Set the `com.ibm.ssl.protocol` property to `TLSv1.2`.
16. Click **Server > Server Types > WebSphere application servers > server1**.
17. On the Server Infrastructure page, click **Java and Process Management > Process definition**.
18. On the **Additional Properties** tab, click **Java Virtual Machine > Custom properties**.
19. On the Preferences page, create custom properties as follows:
 - a. Select the `com.ibm.team.repository.transport.client.protocol` check box and set the corresponding value to **TLSv1.2**.
 - b. Select the `com.ibm.jsse2.sp800-131` check box and set the corresponding value to **strict**.
 - c. Select the `com.ibm.rational.rpe.tls12only` check box and set the corresponding value to **true**.

Index

A

ACR	74
add	
Disposition Codes	85
add IP codec set	19
add IP network region	18
adding	
OBCService SVAR	79
SIP connection for Session Manager	30
adding IP address of CMS	12
AEP	26
AES	73
Agent station	66
application server	47
authorization certificate	91
Avaya Contact Recorder	60
Avaya support website	110

B

Bulk recording	75
----------------------	--------------------

C

Call Management System	
configuring	32
connecting with CM	13
Call Management System checklist	32
certificate authority	
adding	83
certificates, application server	47
change history	8
checklist	60
Codec set	66
communication manager	10
Communication Manager	23, 24
communication manager checklist	10
configure	
ACW time	87
configuring	
Outbound Provider	84
configuring agent	96
configuring Avaya Experience Portal	30
configuring call management system	32
configuring POM server	91
configuring the database	42
Configuring,	
TLSv1.2	112
configuring, connection to an external system	37
configuring, external selection settings	39
configuring, selecting class files	37
connecting CMS with CM	13

Contact Center	75
context store	77
COR	65
create	
user to handle outbound contacts	85
creating a CM login for POM in the CC Elite CTI	
configuration page	20
CTI link	64
customer interaction card	105

D

database configuration	42
deploying, .jar file	38
deployment	
prerequisites	89
dial patterns	28

E

Elite workspaces integration checklist	89
enabling callback feature	84
enabling, WFO integration	74
exchanging	
certificates	47
Exchanging certificate	55
External Application server	53
External application server checklist	42
external selection checklist	36
external selection configuration	39
external system configuration	41

G

Gatekeeper	71
------------------	--------------------

H

hunt group	17
------------------	--------------------

I

importing	
POM server certificate	82
installing web server root certificate	96
integration	
Oceana	77
POM	77
Workspaces	88, 107
IP softphones	68

J		Tomcat server	46
Java implementation	111	trunk group	15
java SDK	77	TSAPI	70–72
L		U	
layout	105	Universal call ID	64
license	63	V	
login to CM	11	verification	
N		CMS rt_socket installation	34
Network Region	67	W	
node names	11	WebRTC agents	107
O		WebSphere	52
OBCService attributes	81		
Oceana integration checklist	78		
Oceana server field descriptions	83		
overview	10, 21, 32		
P			
POM AES Configuration	73		
POM Applications	74		
POM service	93		
POM system configuration	92		
POM trusted certificate	91		
POM widgets	93		
primary POM server	42		
product information	109		
purpose	8		
R			
Routing Policy	26, 27		
S			
Security Code	68		
Session Manager checklist	21		
setting			
OBCService attributes	80		
signaling group	14		
SIP Entities	22–24		
SIP Entity	25, 26		
SIP Entity link	24		
softphones	70		
support	110		
T			
Tlink	71		