



Avaya Solution & Interoperability Test Lab

Application Notes for NICE Behavioral Analytics for POM Outbound with Avaya Proactive Outreach Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for NICE Behavioral Analytics for POM Outbound 4.2 to interoperate with Avaya Proactive Outreach Manager 3.1.3 and Avaya Aura® Application Enablement Services 8.1.2 using Single Step Conference to records calls.

NICE Behavioral Analytics for POM Outbound connected to the Avaya solution to allow recording of outbound calls generated by Avaya Proactive Outreach Manager and used the Single Step Conference feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture media associated with the monitored agent stations for call recording.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for NICE Behavioral Analytics for POM Outbound 4.2 to interoperate with Avaya Proactive Outreach Manager 3.1.3 and Avaya Aura® Application Enablement Services 8.1.2 using Single Step Conference to records calls.

The primary focus of these Application Notes is the connection to Proactive Outreach Manager (POM) in order to record outbound campaign calls from agent phones. NICE Behavioral Analytics for POM Outbound made use of the Call Recorder Application Programming Interface (API) on POM and used the Single Step Conference feature via the Application Enablement Services Device, Media, and Call Control (DMCC) interface to capture media associated with the monitored agent stations for call recording.

A number of blended calls were also recorded that being a mixture of both outbound calls using POM and inbound calls to a VDN. To facilitate the recording of both the outbound and inbound calls, the DMCC interface on Application Enablement Services was leveraged. Behavioral Analytics for POM Outbound used the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services to monitor skill groups and agent stations on Communication Manager, along with the Single Step Conference feature via the Application Enablement Services (DMCC) for call recording of inbound calls.

DMCC works by allowing software vendors to create soft phones, in memory on a recording server, and use them to monitor and record other phones. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure. The DMCC API associated with Application Enablement Services monitors the digital and VoIP stations or extensions. The application uses the DMCC service to register itself as a recording device at the target extension. When the target extension joins a call, the application automatically receives the call's aggregated RTP media stream via the recording device by using Single Step Conference and records the call.

Note: The primary focus of these Application Notes is the connection to the POM recording API for recording of outbound calls. Although a connection to TSAPI was made to allow for blended calls, this connection has previously been certified and the resulting Application Notes are titled *Application Notes for Mattersight Call Recording Solution with Avaya Aura® Communication Manager Using Single Step Conference with Avaya Aura® Application Enablement Services*.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of Behavioral Analytics for POM Outbound, the application automatically performed device queries and requested monitoring of POM agents using the POM Call Recorder API. Behavioral Analytics for POM Outbound also registered the virtual IP softphones using DMCC.

For the manual part of the testing, each call was handled manually using the POM Agent Desktop application for user actions such as hold, resume, transfer and conference.

When there was an active call at a monitored agent station, Behavioral Analytics for POM Outbound was informed of the call either by reports from POM via the Call Recorder API during an outbound call or by event reports from the TSAPI interface only for an inbound call as part of a blended call. It started call recording using Single Step Conference via the DMCC interface to add a virtual IP softphone to the active call and obtain the media. The event reports were also used to determine when to stop the call recordings.

The primary focus of the compliance testing was on the recording of outbound calls using POM to generate calls from a list associated with a campaign. Both Preview and Progressive campaigns were used during testing. Some blended calls were made using the POM agent desktop to transfer callers to incoming VDN's. All calls were expected to be recorded.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Behavioral Analytics for POM Outbound.

The verification of tests included use of a 'test GUI' that was provided to DevConnect from NICE to allow the playback of all recordings. This tool is only used for DevConnect recording validation and is not provided to customers. Customers using this recording solution would have access to the standard Behavioral Analytics Portal to find and play back recordings.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Application Enablement Services and Behavioral Analytics for POM Outbound did not include use of any specific encryption features as requested by NICE.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on Behavioral Analytics for POM Outbound.

- **Handling of POM messaging** in areas of event notification and value queries.

- **Use of DMCC services** to register virtual IP softphones, and to activate Single Step Conference to obtain the media for call recording.
- **Outbound calls in a Preview Campaign** – Test call recording for outbound calls in a preview campaign created on POM made to PSTN endpoints over a SIP trunk.
- **Outbound calls in a Progressive Campaign** - Test call recording for outbound calls in a progressive campaign created on POM made to a simulate SIP PSTN endpoints.
- **Hold/Transferred/Conference calls** – Test call recording of outbound calls in a preview campaign on hold, transferred and conferenced.
- **Blended calls** – The recording of both inbound and outbound calls together using the same agent.
- **Serviceability testing** - The behaviour of Behavioral Analytics for POM Outbound under different simulated failure conditions.

The serviceability testing focused on verifying the ability of Behavioral Analytics for POM Outbound to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Behavioral Analytics for POM Outbound.

2.2. Test Results

All test cases were executed. The following observations were noted on POM from the compliance testing.

1. The Signaling Group involved with SIP trunks required that Direct IP-IP Audio Connections be set to no and that IP Audio Hairpinning be set to Y, this was at the request of NICE for this setup. Please see **Section 5.4** to see how this is implemented.
2. NICE provided two batch files and a unique GUI to allow the playback of recordings from both POM events and from TSAPI events. The bespoke nature of this setup meant that these batch files need to be manually run in order to process the calls and populate the GUI to allow the playback of recordings, this would not necessarily be the case for a production setup.

2.3. Support

Technical support on Behavioral Analytics for POM Outbound can be obtained through the following.

- **Phone:** + 1 800.642.3611
- **Web:** <http://wiser.nice.com>

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test Behavioral Analytics for POM Outbound with POM, Communication Manager and Application Enablement Services.

During compliance testing, Behavioral Analytics for POM Outbound monitored the skill groups and agent stations shown in the table below.

Device Type	Extension
VDN	1900, 1901
Skill Group	90, 91
Supervisor	1002
Agent Station	1100 (SIP), 1001 (H.323), 1050 (Digital)
Agent ID	1400, 1401, 1402
Virtual DMCC Stations	18901, 18902, 18903

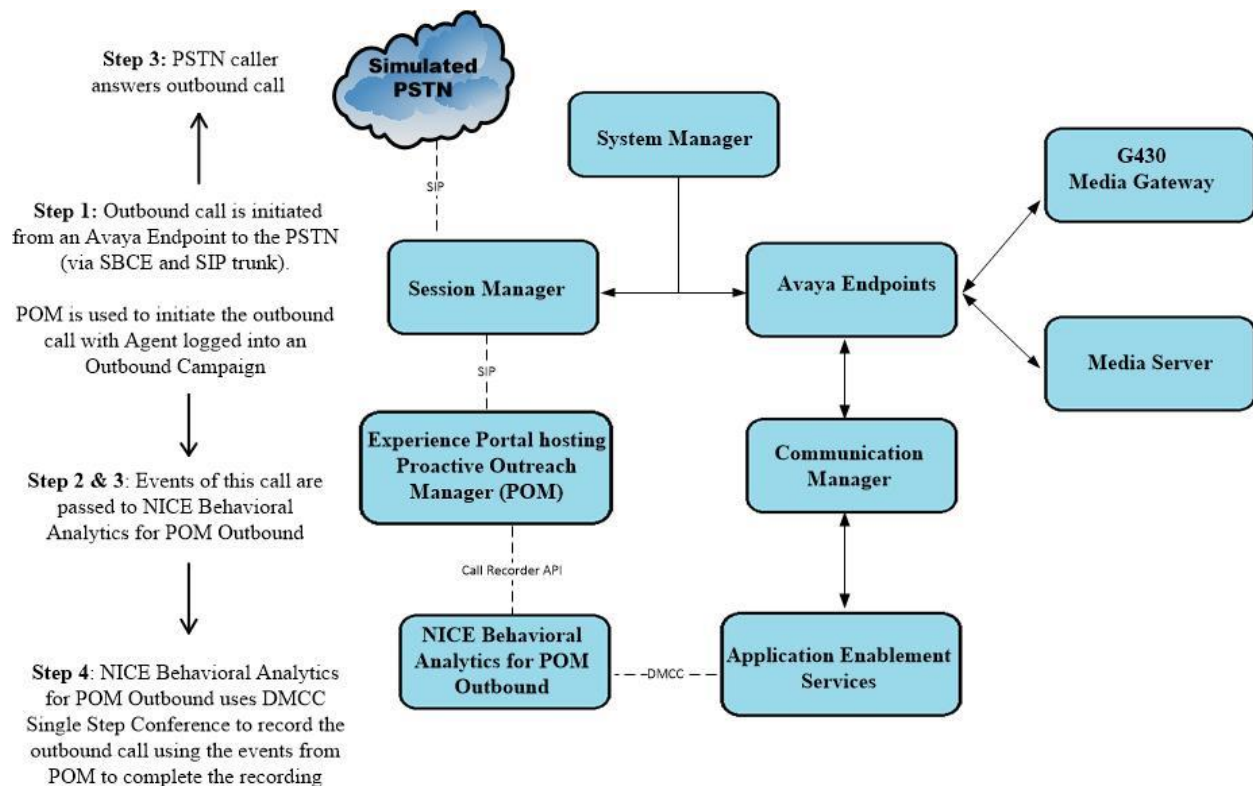


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Avaya Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 8.1.2.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.2.0.0611261 Feature Pack 2
Avaya Aura® Session Manager running on a virtual server	Session Manager R8.1.2 Build No. – 8.1.2.0.812039
Avaya Aura® Communication Manager running on a virtual server	R8.1.2.0 – FP2 R018x.00.0.890.0 Update ID 01.0.890.0-26095
Avaya Aura® Experience Portal used to host POM Avaya Proactive Outreach Manager -EPM (Experience Portal Manager) -MPP (Media Processing Platform)	R7.2.3 R03.01.03.01.03.013 R7.2.3.0.0505 R7.2.3.0.0505
Avaya Aura® Application Enablement Services	8.1.2
Avaya Aura® Media Server	8.0.0.169
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 H.323 Deskphone	6.8304
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Avaya Digital 9408	2.00
NICE Equipment/Software	Release/Version
NICE Behavioral Analytics for POM Outbound running on Windows 2016 server with MS SQL 2017	4.2
<ul style="list-style-type: none"> Avaya TSAPI Windows Client (csta32.dll) 	8.0.0.38
<ul style="list-style-type: none"> Avaya DMCC XML 	8.0.0.38

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer CTI link
- Administer IP codec set
- Administer Signalling Group
- Administer virtual IP softphones
- Administer agent stations (SIP)

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **Computer Telephony Adjunct Links** customer option is set to **y** on **Page 4**. If this option is not set to **y**, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page 4 of 12
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	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? n	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	

5.2. Administer CTI Link

Add a CTI link using the **add cti-link n** command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 1990		
Type: ADJ-IP		
		COR: 1
Name: aes81xvmpg		

5.3. Administer IP Codec Set

Use the **change ip-codec-set n** command, where “n” is an existing codec set number used for integration with Behavioral Analytics for POM Outbound.

For customer network that use encrypted media, make certain that **none** is included for **Media Encryption**, and that **Encrypted SRTP** is set to **best-effort**, these settings are needed for support of non-encrypted media from the virtual IP softphones used by Behavioral Analytics for POM Outbound.

In the compliance testing, this IP codec set was assigned to the virtual IP softphones used by Behavioral Analytics for POM Outbound.

change ip-codec-set 1

Page1 of 2

IP Codec Set

Codec Set: 1

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

Media Encryption

Encrypted SRTP: best-effort

1:	1-srtp-aescm128-hmac80
2:	none
3:	
4:	
5:	

5.4. Administer Signalling Group

The following must be set on each signalling group involved with SIP traffic. Set **Direct IP-IP Audio Connections** to **n**, set **IP Audio Hairpinning** to **y**. This is to ensure that SIP phones will be recorded properly using Single Step Conference.

change signaling-group 1	SIGNALING GROUP	Page 1 of 3
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: SM80vmppg	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
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? n	
Enable Layer 3 Test? y	IP Audio Hairpinning? y	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

5.5. Administer Virtual IP Softphones

Add a virtual IP softphone using the **add station n** command, where “n” is an available extension number. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Extension:** The available extension number
- **Type:** Any IP telephone type, such as **4620**
- **Name:** A descriptive name
- **Security Code:** A desired code
- **IP SoftPhone:** **y**

add station 18901		Page 1 of 5
STATION		
Extension: 18901	Lock Messages? n	BCC: 0
Type: 4620	Security Code: 1234	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: Virtual Recorder1	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: 18901	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Expansion Module? n	
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	

Note: For compliance testing there were three recorders configured to ensure there were enough recorders for each agent used.

5.6. Administer Agent Stations (SIP)

Each Avaya SIP endpoint or station that needs to be monitored and used for 3rd party call control will need to have “Type of 3PCC Enabled” set to “Avaya”. Changes of SIP phones must be carried out from System Manager by entering **http://<FQDN>/network-login**, where <FQDN> is the fully qualified domain name of System Manager or **http://<IP Address>/network-login**. Log in using appropriate credentials.

Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

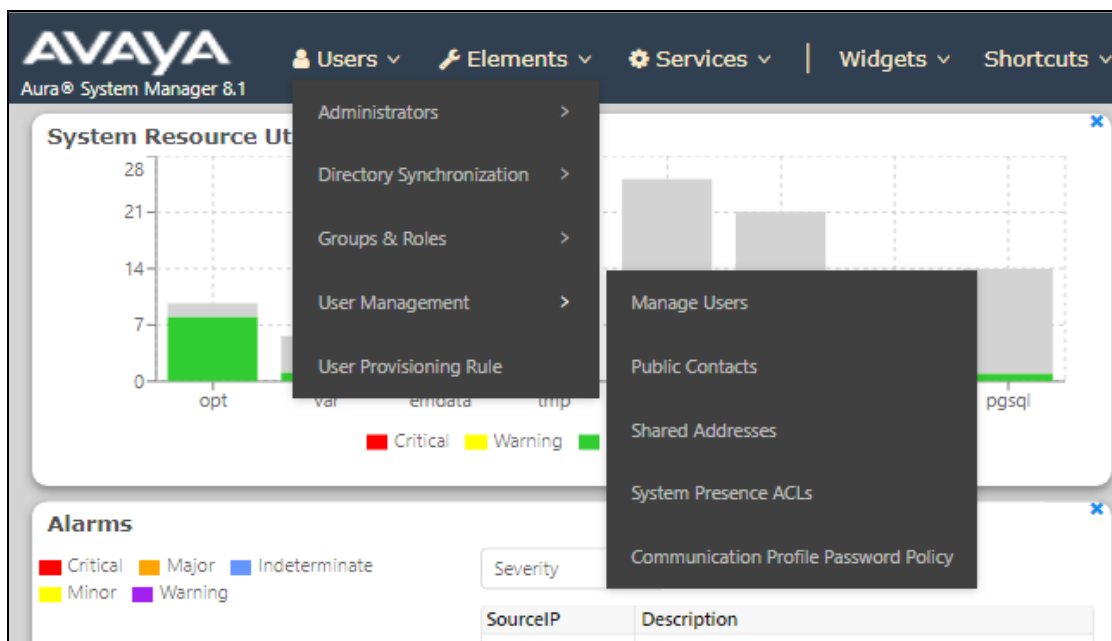
User ID:

Password:

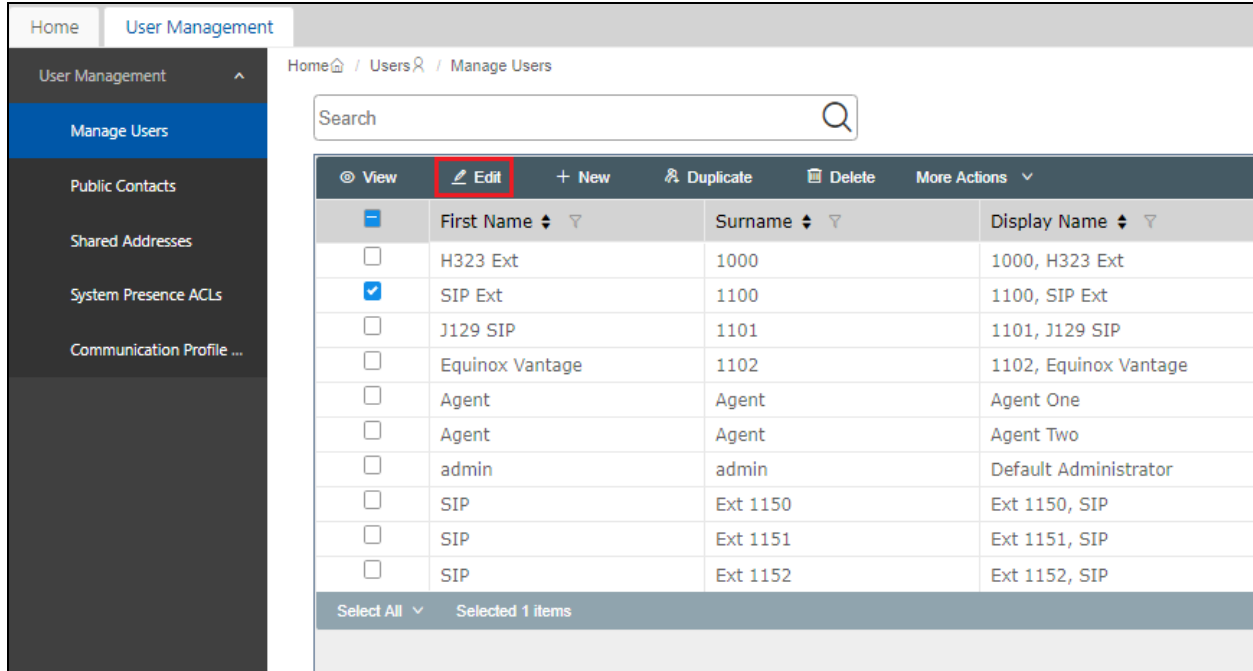
[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

From the home page, click on **Users** → **User Management** → **Manage Users**, as shown below.



Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.

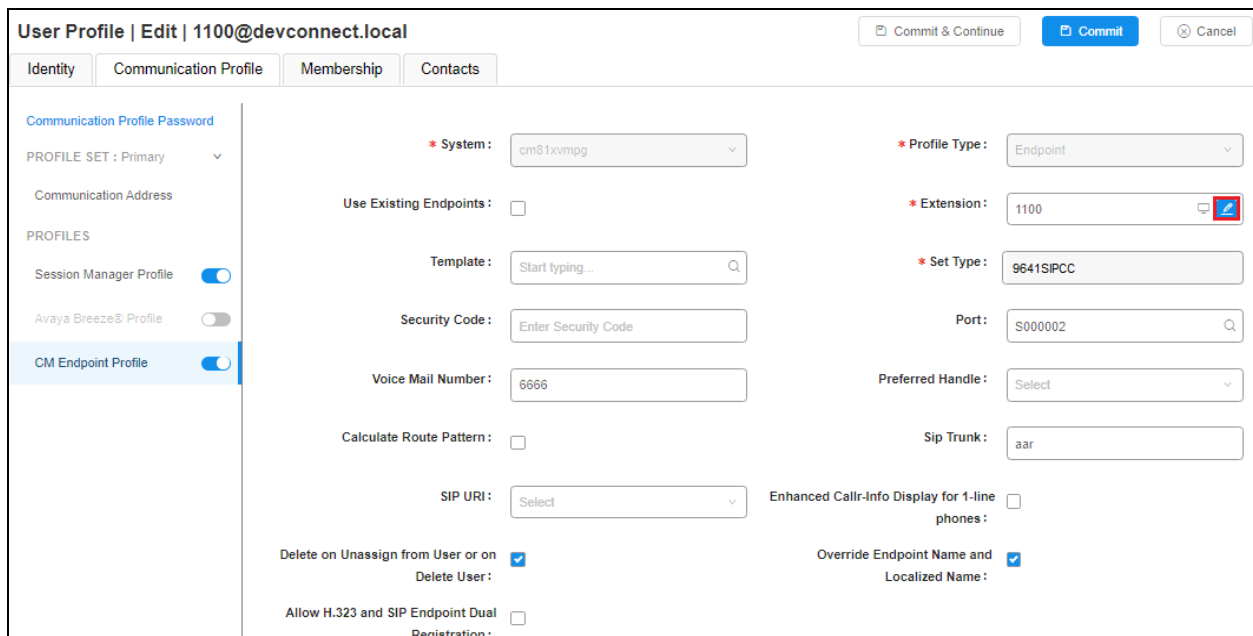


The screenshot shows the 'User Management' interface. On the left, the 'Manage Users' option is selected in the sidebar. The main area displays a table of users. The 'Edit' button in the top toolbar is highlighted with a red box. The table contains the following data:

	First Name	Surname	Display Name
<input type="checkbox"/>	H323 Ext	1000	1000, H323 Ext
<input checked="" type="checkbox"/>	SIP Ext	1100	1100, SIP Ext
<input type="checkbox"/>	J129 SIP	1101	1101, J129 SIP
<input type="checkbox"/>	Equinox Vantage	1102	1102, Equinox Vantage
<input type="checkbox"/>	Agent	Agent	Agent One
<input type="checkbox"/>	Agent	Agent	Agent Two
<input type="checkbox"/>	admin	admin	Default Administrator
<input type="checkbox"/>	SIP	Ext 1150	Ext 1150, SIP
<input type="checkbox"/>	SIP	Ext 1151	Ext 1151, SIP
<input type="checkbox"/>	SIP	Ext 1152	Ext 1152, SIP

At the bottom of the table, it says 'Select All' and 'Selected 1 items'.

Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.



The screenshot shows the 'User Profile | Edit | 1100@devconnect.local' form. The 'CM Endpoint Profile' tab is selected in the left sidebar. The form contains the following fields and options:

- System:** cm81xvmpg
- Profile Type:** Endpoint
- Extension:** 1100
- Set Type:** 9641SIPCC
- Port:** S000002
- Preferred Handle:** Select
- Sip Trunk:** aar
- Use Existing Endpoints:** ☐
- Template:** Start typing...
- Security Code:** Enter Security Code
- Voice Mail Number:** 6666
- Calculate Route Pattern:** ☐
- SIP URI:** Select
- Enhanced Callr-Info Display for 1-line phones:** ☐
- Delete on Unassign from User or on Delete User:** ☒
- Override Endpoint Name and Localized Name:** ☒
- Allow H.323 and SIP Endpoint Dual Registration:** ☐

In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below. Click on **Done**, at the bottom of the screen, once this is set.

The screenshot shows the 'General Options (G)' tab selected. The configuration fields are as follows:

- Class of Restriction (COR):** 1
- Emergency Location Ext:** 1100
- Tenant Number:** 1
- SIP Trunk:** aar
- Coverage Path 1:** (empty)
- Lock Message:** ☐
- Multibyte Language:** Not Applicable
- Class Of Service (COS):** 1
- Message Lamp Ext.:** 1100
- Type of 3PCC Enabled:** Avaya (highlighted with a red box)
- Coverage Path 2:** (empty)
- Localized Display Name:** 1100, SIP Ext
- Enable Reachability for Station Domain Control:** system
- SIP URI:** (empty)
- Primary Session Manager:**
 - IPv4:** 10.10.40.32
 - IPv6:** (empty)
- Secondary Session Manager:** (empty)

Click on **Commit** once this is done to save the changes.

The screenshot shows the 'User Profile | Edit | 1100@devconnect.local' screen. The 'Communication Profile' tab is selected. The configuration fields are as follows:

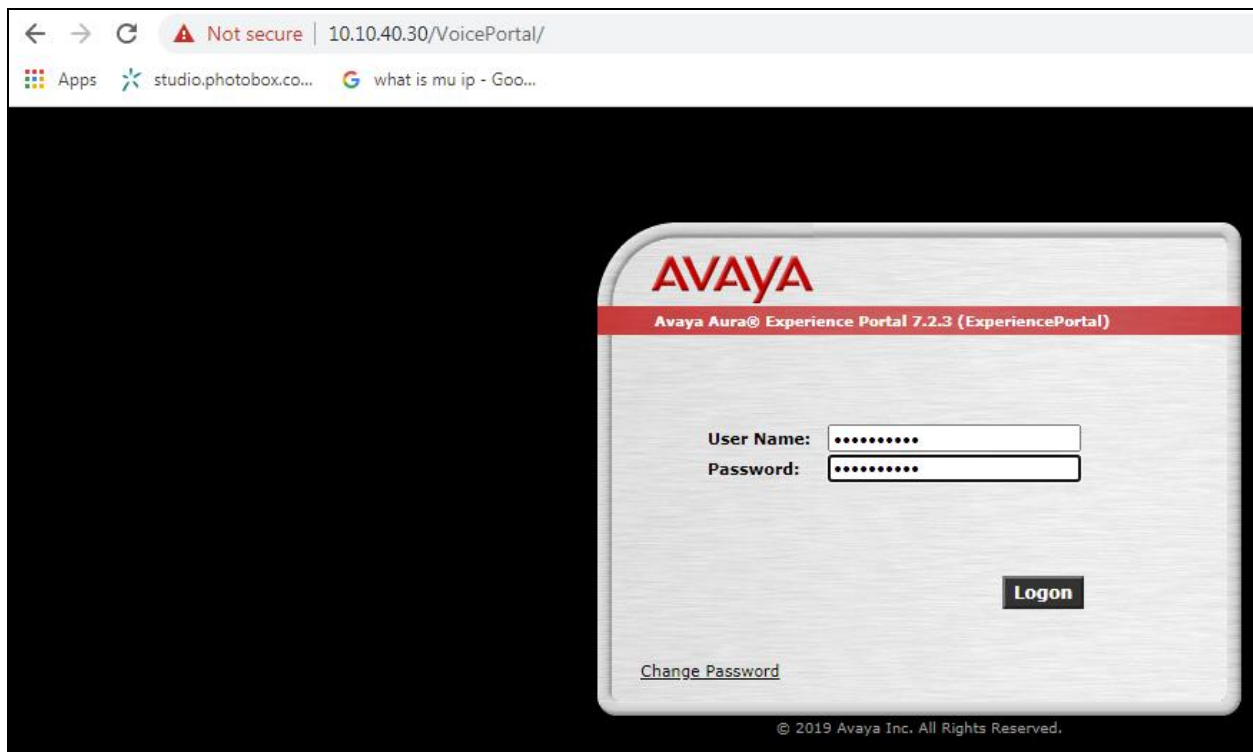
- System:** cm81xvmpg
- Profile Type:** Endpoint
- Extension:** 1100
- Set Type:** 9641SIPCC
- Port:** S000002
- Preferred Handle:** Select
- Sip Trunk:** aar
- Use Existing Endpoints:** ☐
- Template:** Start typing...
- Security Code:** Enter Security Code
- Voice Mail Number:** 6666
- Calculate Route Pattern:** ☐
- SIP URI:** Select
- Enhanced Call-Info Display for 1-line phones:** ☐
- Delete on Unassign from User or on Delete User:** ☒
- Override Endpoint Name and Localized Name:** ☒
- Allow H.323 and SIP Endpoint Dual Registration:** ☐

The 'Commit' button is highlighted with a red box.

6. Configure Avaya Aura® Experience Portal and Avaya Proactive Outreach Manager

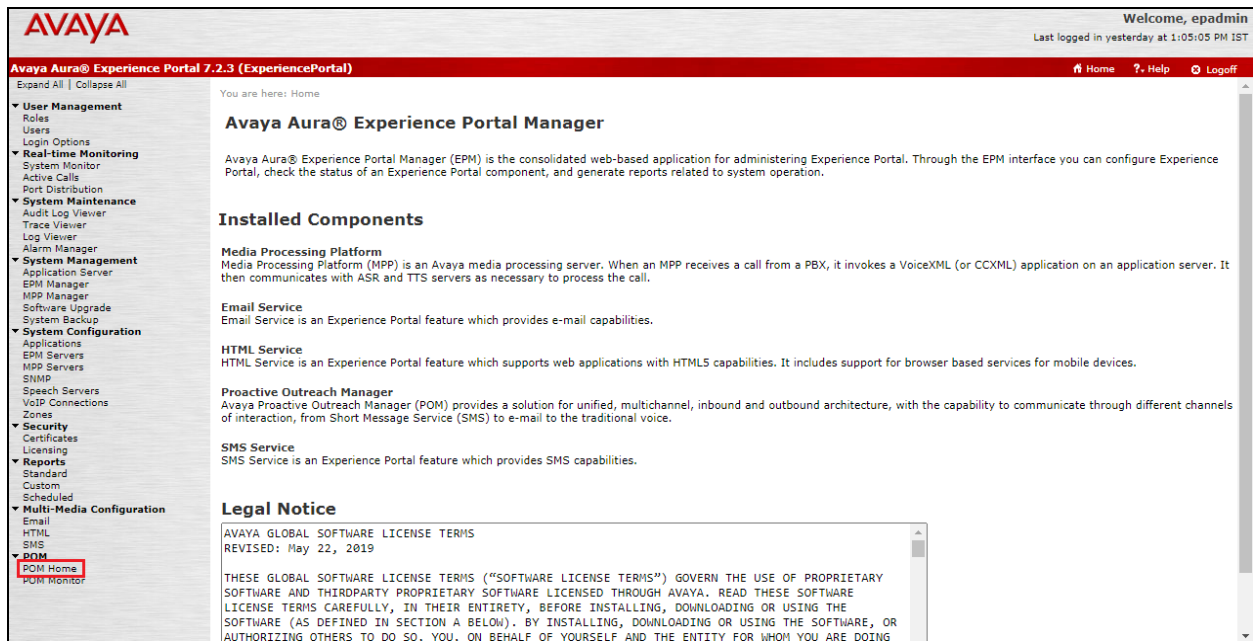
Avaya Proactive Outreach Manager is installed on top of an existing Avaya Aura® Experience Portal installation. It is assumed that both Experience Portal and POM are fully installed and configured. This section will go through the changes that are necessary to allow Behavioral Analytics for POM Outbound to connect and receive call events from the POM Call Recorder API.

Open a web browser and navigate to **https://<IPAddressofEP>/VoicePortal/** as shown below, enter the appropriate credentials and click on **Logon**.

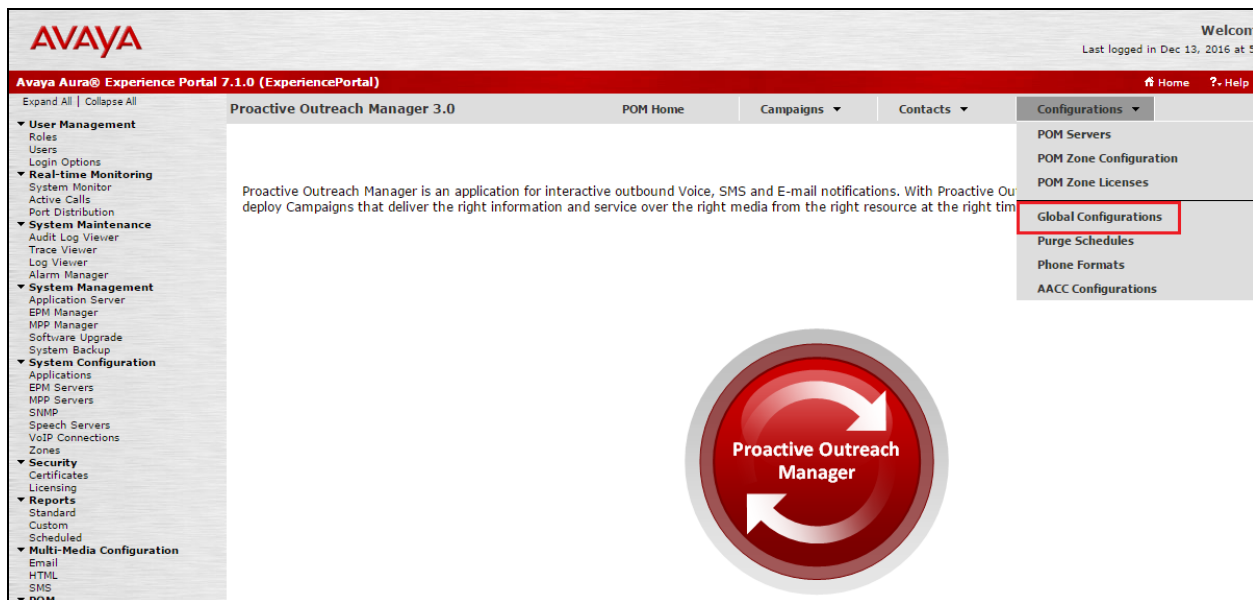


6.1. Configure Proactive Outreach Manager

Select **POM Home** from the bottom of the left window.



Select **Global Configurations** as shown below.



Scroll down to the **WFO** section and ensure that **Enable WFO** is ticked and the default port of **7999** is selected. The **Nailup call CLID** can be set at any figure and it was set as shown below. Click **Apply** at the bottom of the screen.

WFO

Enable WFO☒

WFO port * 7999

Agent settings

Maximum job waiting duration(min) * 20

Minimum job attachment period(min) * 15

Nailing retry interval(sec) * 20

Call queue ☐

Nailup call CLID * 98765

Override PAI for External Consult Calls ☐

ANI for external consult calls ☒ Nailup call CLID ☐ Agent Extension

Miscellaneous

POM poller polling interval(sec) * 5

Agent script editor auto save time(min) * 1

Advanced settings

JMS listen port * 51616

Pacer base port * 9995

Router base port * 7779

Agent manager base port * 9970

Campaign batch size * 600

Maximum concurrent jobs * 50

Maximum ports per server * 1200

Apply

Cancel

Help

6.2. Create a POM User for Behavioral Analytics for POM Outbound

A user must be created to allow Behavioral Analytics for POM Outbound access to web services for call events. This user will be configured during the Behavioral Analytics for POM Outbound setup in **Section 8.1.1**. Click on **Users** in the left window and **Add** in the main window.

Avaya Aura® Experience Portal 7.2.3 (ExperiencePortal)

You are here: [Home](#) > [User Management](#) > [Users](#)

Users

This page displays the list of EPM user accounts. Depending on your user role, you can add, modify, and delete user accounts. You can also configure the parameters under LDAP Settings to enable the EPM to access user accounts in your corporate directory.

<input type="checkbox"/>	Name	Enable	Type	Assigned Roles/Features	Last Login	Failed Attempts	Locked	Password Longevity (days)
<input checked="" type="checkbox"/>	gadmin	Yes	EP (Password)	Administration, Auditor, User Manager	Jul 17, 2020 2:02:33 PM IST			365 (System)
<input type="checkbox"/>	inisoftpom	Yes	EP (Password)	Administration, Web Services	Never			Not enforced
<input type="checkbox"/>	init	Yes	EASG	Service Account	Never			N/A
<input type="checkbox"/>	nice	Yes	EP (Password)	POM Campaign Manager, Web Services	Never			Not enforced
<input type="checkbox"/>	opentextpom	Yes	EP (Password)	POM Campaign Manager, Web Services	Never			Not enforced
<input type="checkbox"/>	pom	Yes	EP (Password)	Administration, POM Campaign Manager, POM Administration, Reporting, POM Supervisor, Web Services	Jul 2, 2019 5:20:14 PM IST			Not enforced
<input type="checkbox"/>	pomi	Yes	EP (Password)	Administration, Auditor, POM Campaign Manager, POM Contact Attributes Unmask, Maintenance, Operations, POM Administration, Privacy Manager, Reporting, POM Supervisor, User Manager, Web Services	Never			Not enforced

Add **Delete** **Help**

Ensure that **Web Services** is ticked, enter a suitable **Name** and **Password** and click on **Save**.

Change User

Use this page to modify a EPM user account. You can change the user role and password.

Name:

Enable: ☒ Yes ☐ No

Roles:

<input type="checkbox"/> Administration	<input type="checkbox"/> Auditor	<input checked="" type="checkbox"/> POM Campaign Manager
<input type="checkbox"/> POM Contact Attributes Unmask	<input type="checkbox"/> Maintenance	<input type="checkbox"/> Operations
<input type="checkbox"/> POM Administration	<input type="checkbox"/> Privacy Manager	<input type="checkbox"/> Reporting
<input type="checkbox"/> POM Supervisor	<input type="checkbox"/> User Manager	<input checked="" type="checkbox"/> Web Services

Created: 7/10/20 6:25 AM

Password:

Verify Password:

Enforce Password Longevity: ☐

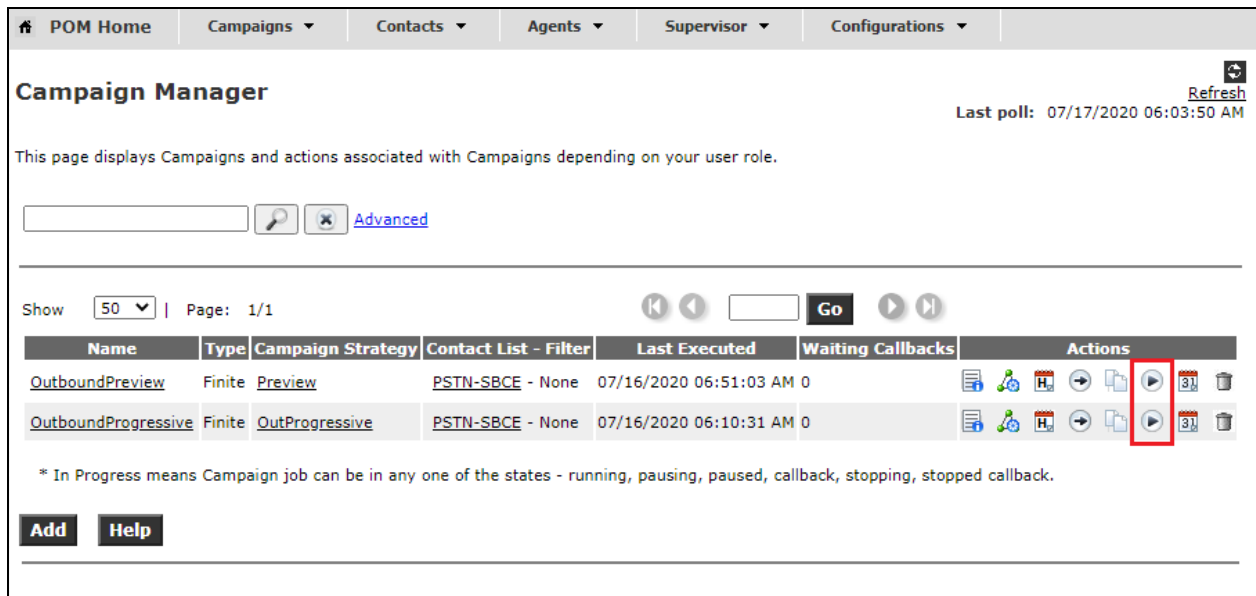
Save **Apply** **Cancel** **Help**

6.3. Starting the Outbound Campaign

Before any outbound calls can be made, the outbound campaign (configured in the **Appendix**) must be started. Open **Campaign Manager** as shown below.



All campaigns that are configured are shown. To start a campaign, click on the play icon highlighted below.



7. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- Verify Licensing
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI and DMCC Ports
- Create CTI User
- Administer Security Database

7.1. Verify Licensing

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of the AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. Below this is a red horizontal bar. The main content area contains a login box with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below the input fields are two buttons: "Login" and "Reset". At the bottom of the page, below another red horizontal bar, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license.

The screenshot shows the 'AE Services' management console. On the left is a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main area displays the 'AE Services' status. A table lists various services with their status, state, license mode, and cause. The 'TSAPI Service' is shown as 'ONLINE' with a 'Running' state and 'NORMAL MODE' license. Below the table, there is a note about restarting services for administrative changes and a link to 'Status and Control'.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

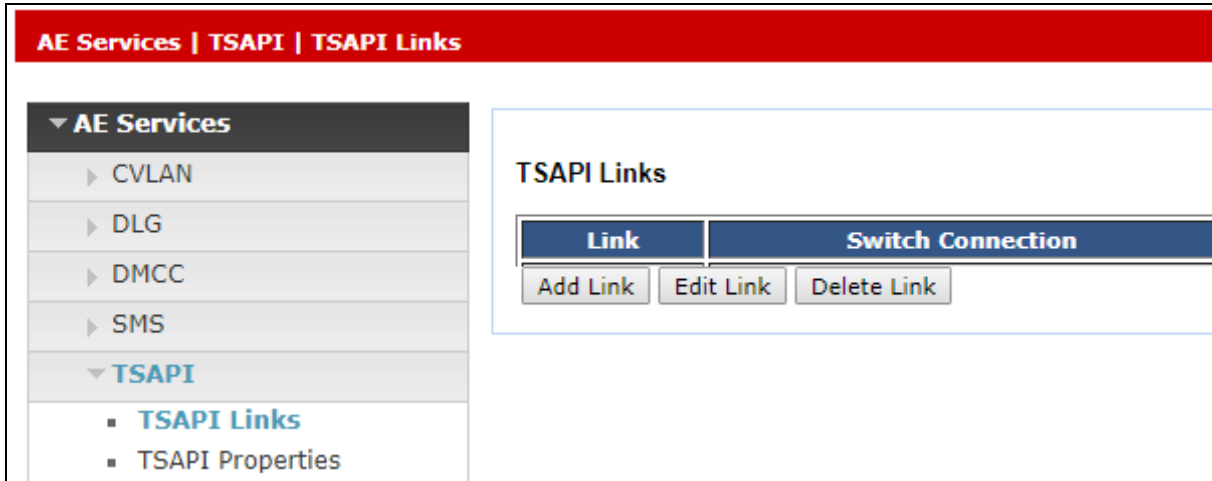
The TSAPI and DMCC licenses are user licenses issues by the Web License Manager to which the Application Enablement Services (AES) server is pointed to. The following screen shows the available licenses for both DMCC and TSAPI users.

The screenshot shows the 'Application Enablement' section of the license management console. It displays a list of licenses with columns for Feature (License Keyword), Expiration date, and Licensed capacity. Two licenses are highlighted with red boxes: 'Device Media and Call Control' (VALUE_AES_DMCC_DMC) and 'TSAPI Simultaneous Users' (VALUE_AES_TSAPI_USERS), both with a permanent expiration date and a licensed capacity of 44. The console also shows a list of server types and applications supported by the licenses.

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	44
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	44
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	44
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	4
DLG VALUE_AES_DLG	permanent	44
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	44
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	4
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	44

7.2. Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.




On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm81xvmpg**, which has already been configured from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.2** which is **1**.
- **ASAI Link Version:** This should be set to the highest version available.
- **Security:** This was set to **Both** allowing both secure and nonsecure connections.

Once completed, select **Apply Changes**.

The screenshot shows the 'Edit TSAPI Links' configuration form. It contains the following fields and values: 'Link' is set to '1'; 'Switch Connection' is set to 'cm81xvmpg' (with a dropdown arrow); 'Switch CTI Link Number' is set to '1' (with a dropdown arrow); 'ASAI Link Version' is set to '11' (with a dropdown arrow); and 'Security' is set to 'Both' (with a dropdown arrow). At the bottom of the form are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.


Another screen appears for confirmation of the changes made. Choose **Apply**.

Apply Changes to Link
Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.
 **Please use the Maintenance -> Service Controller page to restart the TSAPI server.**

When the TSAPI Link is completed, it should resemble the screen below.

TSAPI Links				
Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm81xvmpg	1	11	Both
<div><input type="button" value="Add Link"/> <input type="button" value="Edit Link"/> <input type="button" value="Delete Link"/></div>				

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance** → **Service Controller**. On the **Service Controller** screen, tick the **TSAPI Service** and select **Restart Service**.



Application Enablement Services
Management Console

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start

Stop

Restart Service

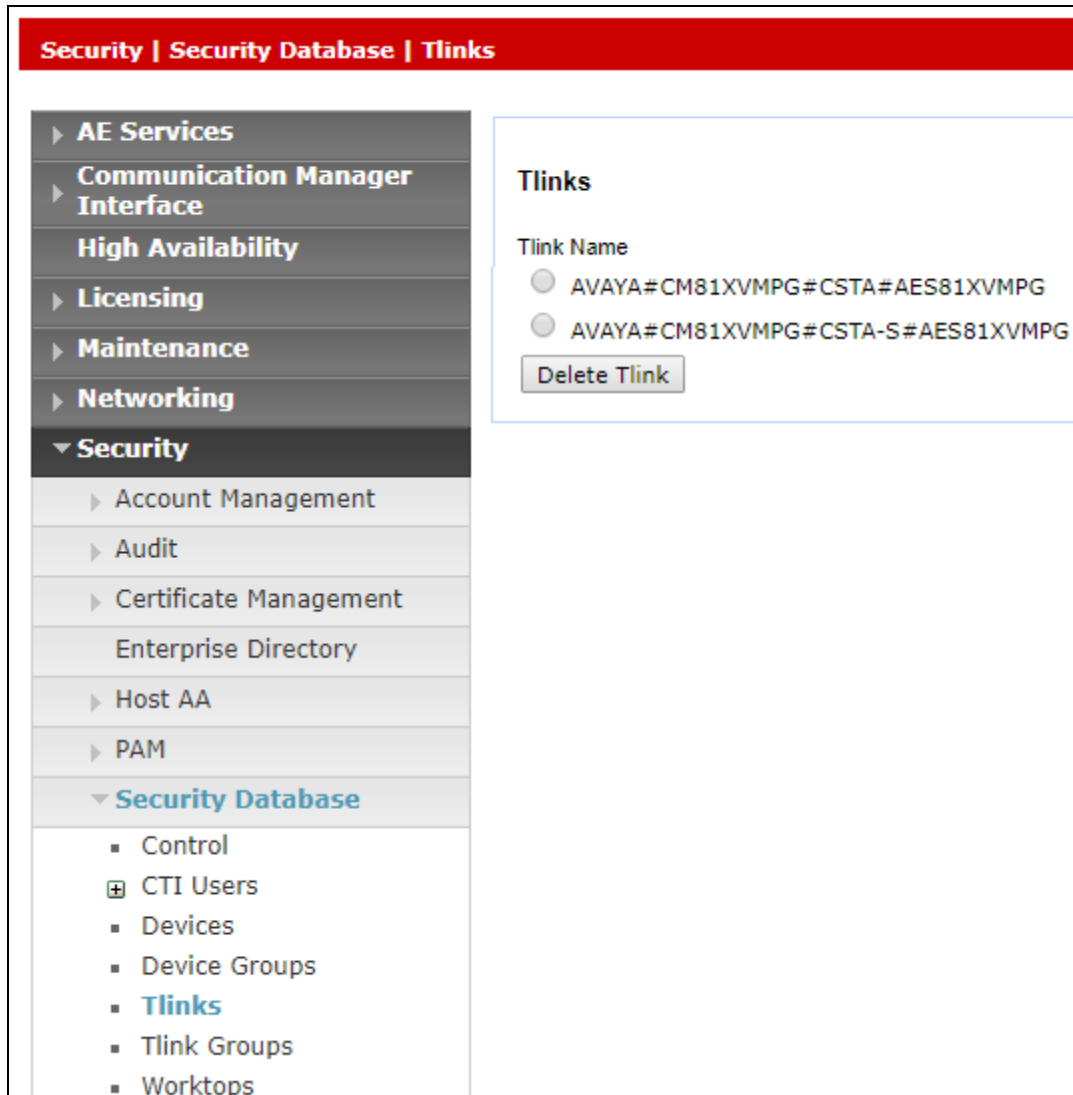
Restart AE Server

Restart Linux

Restart Web Server

7.3. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure Behavioral Analytics for POM Outbound in **Section 8.1.2**. The unsecure link (top link) was used for compliance testing.



7.4. Enable TSAPI and DMCC Ports

To ensure that the TSAPI and DMCC ports are enabled, navigate to **Networking → Ports**. Ensure that the ports are set to **Enabled** as shown below. The ports used in compliance testing were TSAPI port **450** and DMCC port **4721**.

Networking | Ports

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

H.323 Ports

TCP Port Min20000

TCP Port Max29999

Local UDP Port Min20000

Local UDP Port Max29999

Server Media

Enabled Disabled

☒ ☐

☒ ☐

☒ ☐

Enabled Disabled

☒ ☐

Enabled Disabled

☒ ☐

☒ ☐

☒ ☐

Enabled Disabled

☒ ☐

Enabled Disabled

☒ ☐

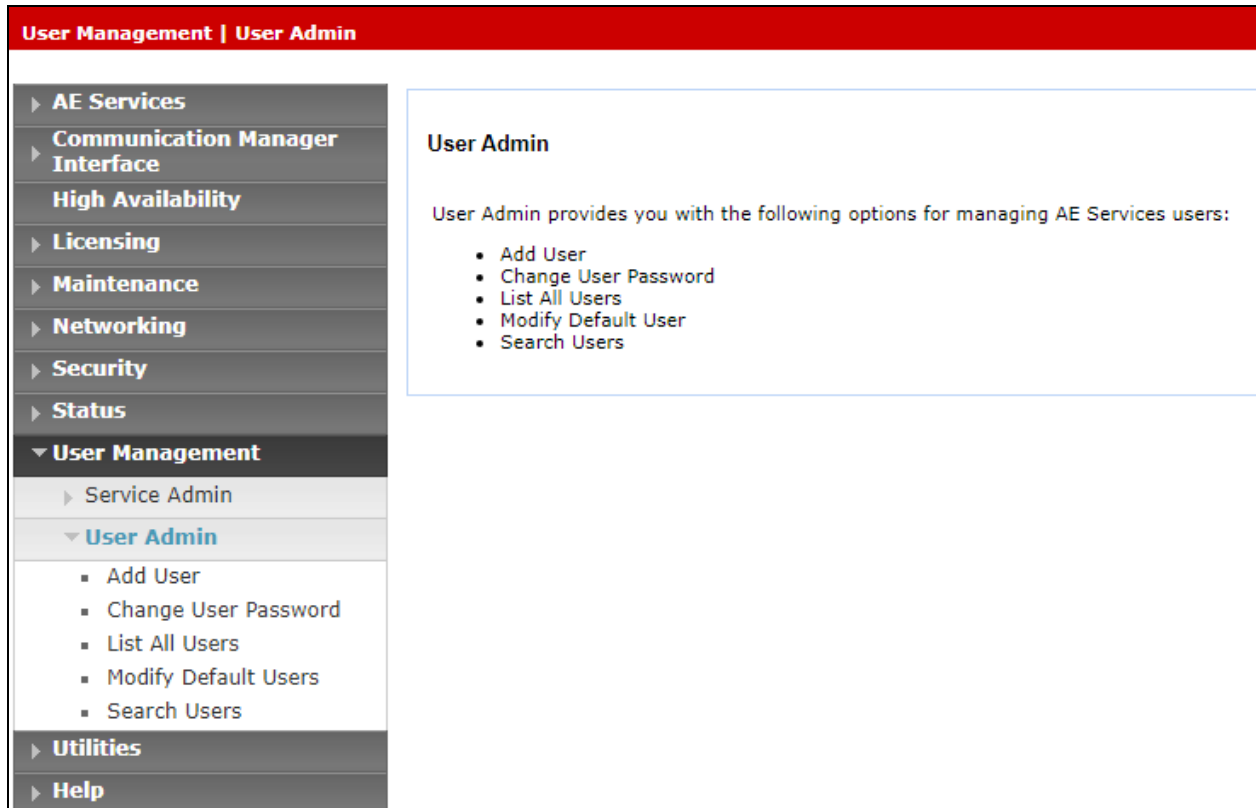
PG; Reviewed:
SPOC 10/14/2020

Solution & Interoperability Test Lab Application Notes
©2020 Avaya Inc. All Rights Reserved.

24 of 47
NICEBA-POM313

7.5. Create CTI User

A user ID and password needs to be configured for Behavioral Analytics for POM Outbound to communicate with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.



In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the Behavioral Analytics for POM Outbound setup in **Section 8.1.1** and **8.1.2**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with Behavioral Analytics for POM Outbound setup in **Section 8.1.1** and **8.1.2**.
- **CT User** - Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen.

Edit User

* User Id	nice
* Common Name	nice
* Surname	nice
User Password	*****
Confirm Password	*****
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Cms Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone	
Home Postal Address	
Initials	
Labeled URI	
Mail	
MM Home	
Mobile	
Organization	
Pager	
Preferred Language	English
Room Number	
Telephone Number	

7.6. Administer Security Database

Select **Security → Security Database → Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Make certain that both parameters are unchecked, as shown below.

In the event that the security database is used by the customer with parameters already enabled, then follow **reference [2]** to configure access privileges for the Behavioral Analytics for POM Outbound user.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Security' > 'Security Database' > 'Control'. The main content area displays 'SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services' with two unchecked checkboxes: 'Enable SDB for DMCC Service' and 'Enable SDB for TSAPI Service, JTAPI and Telephony Web Services'. An 'Apply Changes' button is at the bottom. The top right corner shows user information: 'Welcome: User cust', 'Last login: Fri Jul 17 14:32:10 2020 from 192.168.40.240', 'Number of prior failed login attempts: 0', 'HostName/IP: aes81xvmg/10.10.40.38', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 8.1.2.1.0.6-0', 'Server Date and Time: Fri Jul 17 14:56:26 IST 2020', and 'HA Status: Not Configured'.

Navigate to **Security → Security Database → CTI Users → List All Users**. Select the CTI user added in **Section 7.5** and click on **Edit**.

The screenshot shows the 'CTI Users' page in the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Security' > 'Security Database' > 'CTI Users' > 'List All Users'. The main content area displays a table with two columns: 'User ID' and 'Common Name'. The table lists several users, with 'nice' selected. Below the table are 'Edit' and 'List All' buttons.

User ID	Common Name
<input type="radio"/> Enghouse	Enghouse
<input type="radio"/> inisoft	inisoft
<input type="radio"/> mitel	mitel
<input checked="" type="radio"/> nice	nice
<input type="radio"/> Oceana	Oceana
<input type="radio"/> paul	Paul
<input type="radio"/> paul1	paul1

In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

Edit CTI User		
User Profile:	User ID	nice
	Common Name	nice
	Worktop Name	NONE ▼
	Unrestricted Access	<input checked="" type="checkbox"/>
Call and Device Control:	Call Origination/Termination and Device Status	None ▼
Call and Device Monitoring:	Device Monitoring	None ▼
	Calls On A Device Monitoring	None ▼
	Call Monitoring	<input type="checkbox"/>
Routing Control:	Allow Routing on Listed Devices	None ▼
<input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/>		

Click on **Apply** when asked again to **Apply Changes**.

8. Configure NICE Behavioral Analytics for POM Outbound

This section provides the procedures for configuring Behavioral Analytics for POM Outbound. The procedures include the configuration of the WorkerSettings.config file. The configuration of call recording solution is performed by technicians from NICE. The procedural steps are presented in these Application Notes for informational purposes.

8.1. Administer WorkerSettings

A connection to both POM and AES must be configured to allow the recording of outbound and inbound calls. These files are both located on the Behavioral Analytics for POM Outbound server.

8.1.1. Administer POM WorkerSettings

In the WorkerSettings file configure the following parameters for the call recorder to communicate with POM.

- **PomServerIP** is set to that of the Experience Portal IP address that is hosting POM.
- **PomServerport** is set to the default value of **7999** but this can be found in **Section 6.1**.
- **UserName** is set to the user configured in **Section 6.2**.
- **Password** is set to the password configured in **Section 6.2**.

```
<workerSettings>
  <add key="AcdId" value="ABC0001" />
  <add key="EndpointsToPublishTo" value="tcp://10.10.40.129:56000" />
  <add key="EndpointsToSubscribeTo" value="tcp://10.10.40.129:56001" />
  <add key="TelephonyEnterpriseId" value="ABC0002" />
  <add key="WhitelistDirectory" value=".\_config" />

  <add key="PomServerIP" value="10.10.40.30" />
  <add key="PomServerport" value="7999" />
  <add key="UserName" value="nice" />
  <add key="Password" value="xxxxxx" />

  <add key="UseAgentWhiteListAsExtensions" value="false"/>
  <add key="PomEventsOnly" value="false"/>
</workerSettings>
```

8.1.2. Administer DMCC WorkerSettings

In the WorkerSettings file configure the following parameters for the call recorder to communicate with the AES.

- **AesIpAddress** is set to that of the Application Enablement Services server IP address.
- **AesPort** is set to the default value of **4721** but this can be found in **Section 7.4**.
- **CmSwitchName** is set to that configured in **Section 7.2**.
- **CmIpAddress** is set to the IP address of Communication Manager.
- **UserName** is set to the AES user configured in **Section 7.5**.
- **Password** is set to the password configured in **Section 7.5**.

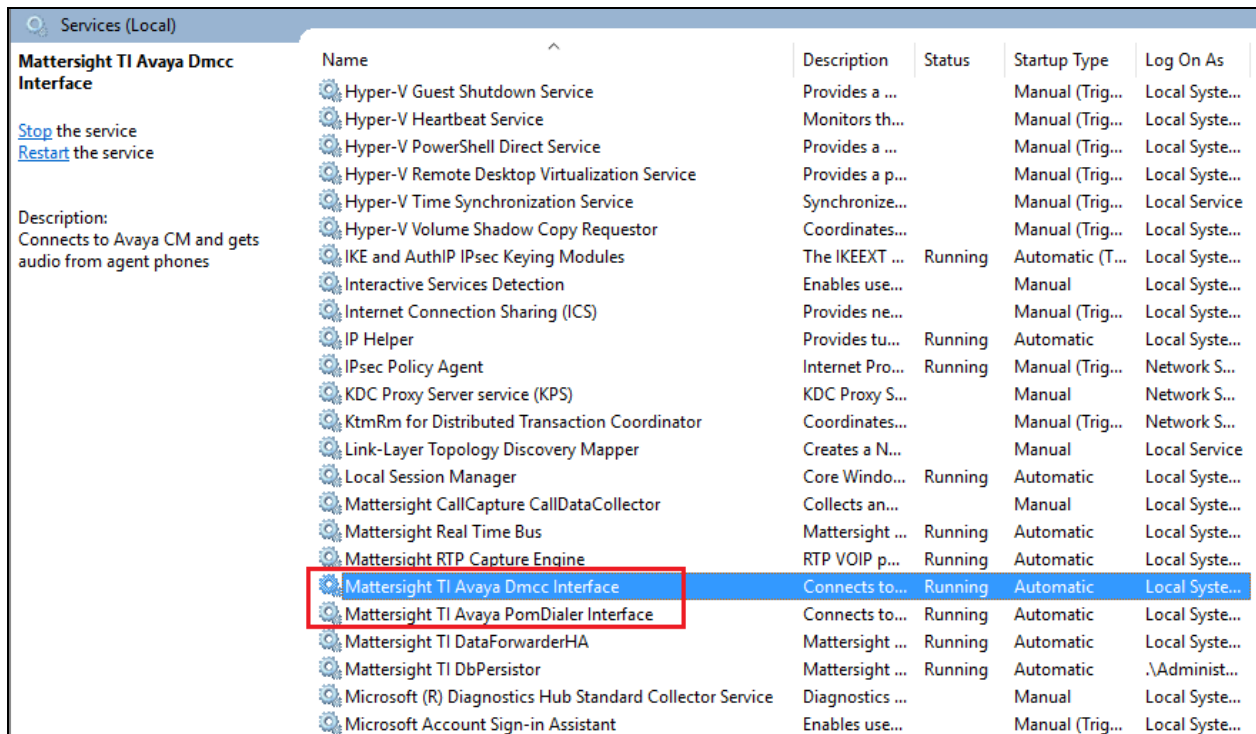
```
<workerSettings>
  <add key="AcdId" value="ABC0001" />
  <add key="EndpointsToPublishTo" value="tcp://10.10.40.129:56000" />
  <add key="EndpointsToSubscribeTo" value="tcp://10.10.40.129:56001" />
  <add key="TelephonyEnterpriseId" value="ABC0002" />
  <add key="WhitelistDirectory" value=".\_config" />

  <add key="AesIpAddress" value="10.10.40.38" />
  <add key="AesPort" value="4721" />
  <add key="CmSwitchName" value="cm81xvmpg" />
  <add key="CmIpAddress" value="10.10.40.37" />
  <add key="UserName" value="nice" />
  <add key="Password" value="xxxxxxxx;" />

  <add key="ProtocolVersion" value="http://www.ecma-international.org/standards/ecma-323/csta/ed3/privC"/>
  <add key="SessionDuration" value="7200" />
  <add key="TimeoutBe4SSC" value="300" />
  <add key="useMediaContentInRegTerm" value="true" />
  <add key="UseAgentWhiteListAsExtensions" value="true"/>
  <add key="DmccEventsOnly" value="false"/>
  <add key="RtpIpAddresses" value="10.10.40.129" />
  <add key="StartPort" value="4700" />
  <add key="EndPort" value="4800" />
  <add key="StationPassword" value="1234" />
  <add key="Codec" value="g711U" /><!--g711U, g729, g711A-->
  <add key="Mode" value="SSC" /><!--MR(multi registration), SSC(single step conf), SO(Service Observe)-->
  <add key="RegisterTerminalOnLogon" value="true"/>
</workerSettings>
```

8.2. Restart Services

From the Behavioral Analytics for POM Outbound server, select **Windows → Control Panel → Administrative Tools → Services** to display the **Services** screen. Start the services as shown below.



The screenshot shows the Windows Services console for 'Services (Local)'. The 'Mattersight TI Avaya Dmcc Interface' service is highlighted in blue. A red rectangle is drawn around the 'Mattersight TI Avaya Dmcc Interface' and 'Mattersight TI Avaya PomDialer Interface' services. The 'Mattersight TI Avaya Dmcc Interface' service is running and has an automatic startup type.

Name	Description	Status	Startup Type	Log On As
Hyper-V Guest Shutdown Service	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Heartbeat Service	Monitors th...		Manual (Trig...	Local Syste...
Hyper-V PowerShell Direct Service	Provides a ...		Manual (Trig...	Local Syste...
Hyper-V Remote Desktop Virtualization Service	Provides a p...		Manual (Trig...	Local Syste...
Hyper-V Time Synchronization Service	Synchronize...		Manual (Trig...	Local Service
Hyper-V Volume Shadow Copy Requestor	Coordinates...		Manual (Trig...	Local Syste...
IKE and AuthIP IPsec Keying Modules	The IKEEXT ...	Running	Automatic (T...	Local Syste...
Interactive Services Detection	Enables use...		Manual	Local Syste...
Internet Connection Sharing (ICS)	Provides ne...		Manual (Trig...	Local Syste...
IP Helper	Provides tu...	Running	Automatic	Local Syste...
IPsec Policy Agent	Internet Pro...	Running	Manual (Trig...	Network S...
KDC Proxy Server service (KPS)	KDC Proxy S...		Manual	Network S...
KtmRm for Distributed Transaction Coordinator	Coordinates...		Manual (Trig...	Network S...
Link-Layer Topology Discovery Mapper	Creates a N...		Manual	Local Service
Local Session Manager	Core Windo...	Running	Automatic	Local Syste...
Mattersight CallCapture CallDataCollector	Collects an...		Manual	Local Syste...
Mattersight Real Time Bus	Mattersight ...	Running	Automatic	Local Syste...
Mattersight RTP Capture Engine	RTP VOIP p...	Running	Automatic	Local Syste...
Mattersight TI Avaya Dmcc Interface	Connects to...	Running	Automatic	Local Syste...
Mattersight TI Avaya PomDialer Interface	Connects to...	Running	Automatic	Local Syste...
Mattersight TI DataForwarderHA	Mattersight ...	Running	Automatic	Local Syste...
Mattersight TI DbPersistor	Mattersight ...	Running	Automatic	.\Administ...
Microsoft (R) Diagnostics Hub Standard Collector Service	Diagnostics ...		Manual	Local Syste...
Microsoft Account Sign-in Assistant	Enables use...		Manual (Trig...	Local Syste...

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and Behavioral Analytics for POM Outbound.

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the **status aesvcs cti-link** command. Verify that the **Service State** is **established** for the CTI link number administered in **Section 5.2** as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	11	no	aes81vmpg	established	42	26

Verify that the correct phones are being monitored by using the **list monitored-station** command. For compliance testing, the three real phones are **1001**, **1050** and **1100**, as well as three virtual recorder stations **18911**, **18912** and **18913** as shown below.

```
list monitored-station
```

MONITORED STATION															
Associations:		1		2		3		4		5		6		7	
Station	Ext	CTI Lnk	CRV	CTI Lnk	CRV	CTI Lnk	CRV	CTI Lnk	CRV	CTI Lnk	CRV	CTI Lnk	CRV	CTI Lnk	CRV

1001		1	0004												
1050		1	0009												
1100		1	000F												
18911		1	0002												
18912		1	000B												
18913		1	0018												

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the DMCC link by selecting **Status** → **Status and Control** → **DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the Behavioral Analytics for POM Outbound username from **Section 7.5**, and that the **# of Associated Devices** column reflects the appropriate number of devices that are being monitored.

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Log Manager

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

TSAPI Service Summary

User Management

Utilities

Help

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Fri Sep 04 14:24:48 IST 2020

Service Uptime: 49 days, 4 hours 48 minutes

Number of Active Sessions: 4

Number of Sessions Created Since Service Boot: 23

Number of Existing Devices: 12

Number of Devices Created Since Service Boot: 157

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	74EAB2C76BA7DED5A 2C82B3DD50C0D88-18407	nice	DmccInterface	10.10.40.129	XML Unencrypted	4
<input type="checkbox"/>	8A4A9ABCF94EE0DC5 92B3F69120390A3-18411	nice	DmccInterface	10.10.40.129	XML Unencrypted	8
<input type="checkbox"/>	23F5DCEF350E941ED 1217A014FF2B58A-14	wspaces37	Khepri Call Server Connector	10.10.42.51	XML Encrypted	0
<input type="checkbox"/>	213215A173D8A4647 71685CF94C5CEF3-15	wspaces37	Khepri Call Server Connector	10.10.42.53	XML Encrypted	0

Terminate Sessions Show Terminated Sessions

Item 1-4 of 4

1Go

9.3. Verify NICE Behavioral Analytics for POM Outbound

Log an agent in to handle and complete an outbound POM call. For this compliance testing a special user interface was created to allow the viewing and playback of recorded calls. The following screen shot shows that interface where recordings can be viewed and the corresponding recording can be downloaded by clicking on **Download** highlighted on one of the recordings below.

CallId	CallStartEventTime	CallEndEventTime	AcidCallId	Extension	Ani	Dnis	AudioFileLengthInSecs	AgentId	AudioRecordingDecision	RecordingResult	RecordingDecisionInfo	CallDirection	AudioFilePathLink
1674	28/08/2020 15:34:57	28/08/2020 15:35:33	3298	1001	5201	1901	55721	1401	1	Ok	ICA Success:NICEPOMRECORDER,cap=99%;	INBOUND	Download
1673	28/08/2020 15:33:59	28/08/2020 15:34:25	3295	1001	5201	1901	25691	1401	1	Ok	ICA Success:NICEPOMRECORDER,cap=100%;	INBOUND	Download
1672	28/08/2020 15:33:26	28/08/2020 15:33:47	3292	1001	5201	1901	21176	1401	1	Ok	ICA Success:NICEPOMRECORDER,cap=100%;	INBOUND	Download
1671	28/08/2020 15:21:18	28/08/2020 15:21:33	3287	1001	5201	1901	14986	1401	1	Ok	ICA Success:NICEPOMRECORDER,cap=97%;	INBOUND	Download
1670	28/08/2020 15:20:23	28/08/2020 15:20:50	3284	1001	5201	1901	27019	1401	1	Ok	ICA Success:NICEPOMRECORDER,cap=100%;	INBOUND	Download
1669	28/08/2020 15:19:52	28/08/2020 15:20:07	3270	1001	5201	1901	14536	1401	1	Ok	ICA Success:NICEPOMRECORDER,cap=96%;	INBOUND	Download
1668	28/08/2020 15:19:24	28/08/2020 15:19:38	3269	1001	1001	5201	13680	1401	1	Ok	ICA Success:NICEPOMRECORDER,cap=96%;	OUTBOUND	Download
1667	28/08/2020 15:18:57	28/08/2020 15:19:15	3268	1001	1001	1000	18585	1401	1	Ok	ICA Success:NICEPOMRECORDER,cap=97%;	OUTBOUND	Download
1666	28/08/2020 14:47:43	28/08/2020 14:47:48	3244	1001	5201	1901		1401	-1	StopMonitoringRequested	Replay:082820 15:08;StopMonitor;NoFlowMatch;	INBOUND	
1665	28/08/2020 14:47:19	28/08/2020 14:47:30	3243	1001	1000	1901		1401	-1	NoFlowMatch	Replay:082820 15:08;NoFlowMatch;	INBOUND	
1664	28/08/2020 14:27:03	28/08/2020 14:27:15	3239	1001	1000	1901		1401	-1	NoFlowMatch	Replay:082820 15:08;NoFlowMatch;	INBOUND	
1663	28/08/2020 14:17:50	28/08/2020 14:18:23	3232	1001	5201	1901		1401	-1	NoFlowMatch	Replay:082820 15:08;NoFlowMatch;	INBOUND	
1662	28/08/2020 14:16:00	28/08/2020 14:16:46	3229	1001	5201	1901		1401	-1	NoFlowMatch	Replay:082820 15:08;NoFlowMatch;	INBOUND	
1661	14/08/2020 15:26:50	14/08/2020 15:27:27	1939	1001	35391847001	35391731901	37050	1401	1	Ok	ICA Success:NICEPOMRECORDER,cap=94%;	INBOUND	Download
1660	14/08/2020 15:24:41	14/08/2020 15:25:10	1925	1001	35391847001	35391731901	29175	1401	1	Ok	ICA Success:NICEPOMRECORDER,cap=92%;	INBOUND	Download
1659	14/08/2020 15:24:30	14/08/2020 15:24:31	1923	1100	1105	1100	1257	1400	-1	AudioDurationDeficit	ICA Failure:NICEPOMRECORDER.Invalid capture duration;	INBOUND	Download
1658	14/08/2020 15:22:00	14/08/2020 15:22:49	1906	1001	35391847001	35391731901	48988	1401	1	Ok	ICA Success:NICEPOMRECORDER,cap=96%;	INBOUND	Download

These recordings are downloaded and stored to a designated folder to be unzipped, opened and played back using any suitable Media Player.

NICE Recordings > Aug 13					Search Aug 13	
Organize Include in library Share with Burn New folder						
Favorites						
Desktop						
Downloads						
Recent Places						
Libraries						
Documents						
Music						
Pictures						
Videos						
Homegroup						
Computer						
Local Disk (C:)						
SoftwareFiles (D:)						
Name					Date modified	Type
1100_1743_2020081310.wav.zip					13/08/2020 11:52	WinRAR ZIP archive
1100_1747_2020081310.wav.zip					13/08/2020 11:52	WinRAR ZIP archive
1001_1762_2020081310.wav.zip					13/08/2020 11:52	WinRAR ZIP archive
1100_1707_2020081310.wav.zip					13/08/2020 11:28	WinRAR ZIP archive
1100_1725_2020081310.wav.zip					13/08/2020 11:28	WinRAR ZIP archive
1001_1722_2020081310.wav.zip					13/08/2020 11:28	WinRAR ZIP archive
1001_1740_2020081310.wav.zip					13/08/2020 11:28	WinRAR ZIP archive
1001_1703_2020081309.wav.zip					13/08/2020 11:04	WinRAR ZIP archive
1001_1698_2020081309.wav.zip					13/08/2020 11:04	WinRAR ZIP archive
1050_1701_2020081309.wav.zip					13/08/2020 11:04	WinRAR ZIP archive
1050_1702_2020081309.wav.zip					13/08/2020 11:04	WinRAR ZIP archive
1100_1696_2020081309.wav.zip					13/08/2020 11:04	WinRAR ZIP archive
1100_1704_2020081309.wav.zip					13/08/2020 11:04	WinRAR ZIP archive
Size						
1,109 KB						
1,917 KB						
1,253 KB						
600 KB						
1,190 KB						
579 KB						
1,003 KB						
357 KB						
514 KB						
428 KB						
417 KB						
548 KB						
388 KB						

10. Conclusion

These Application Notes describe the configuration steps required for Behavioral Analytics for POM Outbound to successfully interoperate with Avaya Proactive Outreach Manager, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Single Step Conference. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

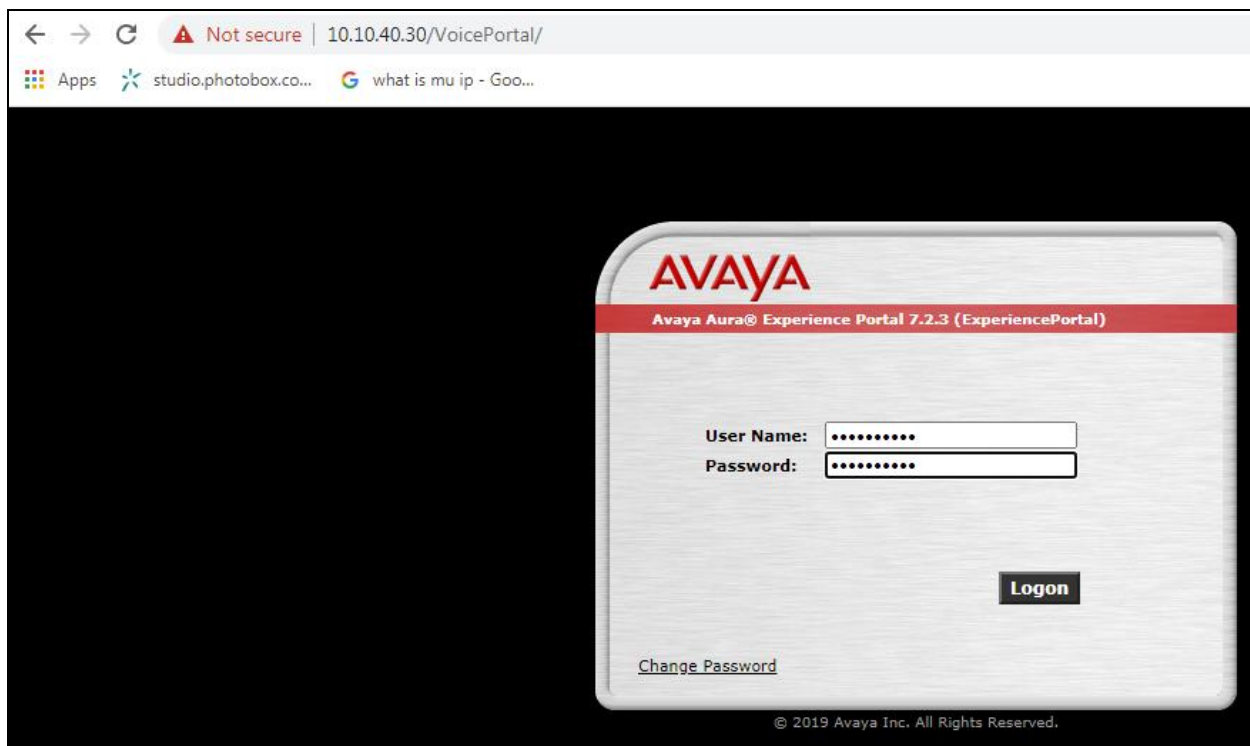
1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, March 2020, available at <http://support.avaya.com>.
2. *Administering Aura® Application Enablement Services*, Release 8.1.x, Issue 7, July 2020, available at <http://support.avaya.com>.
3. *Avaya Proactive Outreach Manager Integration*, Release 3.1.3, Issue 1, January 2020
4. *Implementing Avaya Proactive Outreach Manager*, Release 3.1.3, March 2020
5. *NICE Behavioral Analytics for POM Outbound User Guide*, see Section 2.3 for details on support documentation for NICE.
6. *Application Notes for Mattersight Call Recording Solution with Avaya Aura® Communication Manager Using Single Step Conference with Avaya Aura® Application Enablement Services*.

Appendix

This Appendix contains information on the Contact List, Completion Codes, Outbound Strategy and Outbound Campaign. The Application Notes assume that these components are already in place and a campaign is fully operational. However, it is useful to see the setup of the Preview Campaign, including the Preview Strategy and Contact List assigned to it.

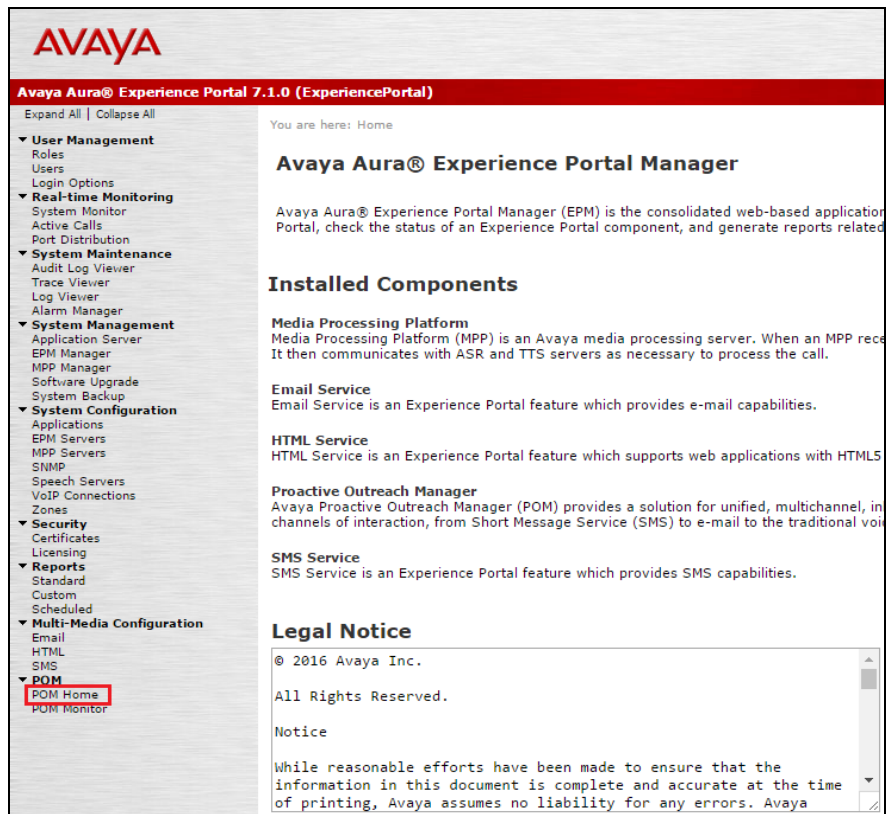
12. Avaya Proactive Outreach Manager Outbound Campaign and Components

POM is configured via the Experience Portal Manager (EPM) web interface. To access the web interface, enter `http://[IP-Address]/` as the URL in an internet browser, where IP-Address is the IP address of the EPM. Log in using the Administrator user role. The screen shown below is displayed.



12.1. Generate an Outbound Campaign

Click on **POM Home** at the bottom of the left window.



The following section shows the configuration of the Preview Campaign Strategy. Before the strategy can be created, a Completion Code must be created.

12.1.1. Completion Codes

Navigate to **Campaigns → Completion Codes** as shown below.



There are three Completion Codes already present on this POM and each of these can be assigned to the Campaign Strategy. If a new code was to be added, click on **Add** as shown below.

Completion Codes
Depending on your user role, this page allows you to create, modify, delete custom Completion Codes.

Show | Page: 1/1

	Completion Code ID↑	Completion Code	Right party connect	Success	Closure	Answer Machine by Agent	Description	Actions
<input type="checkbox"/>	72	Callback	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="button" value="Delete"/>
<input type="checkbox"/>	73	Wrong	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="button" value="Delete"/>
<input type="checkbox"/>	74	Sale	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="button" value="Delete"/>

The example below shows the **Sale** Completion Code, which is assigned to the Preview Strategy that is displayed on the next page.

Edit Completion Code

This page allows you to modify Completion Codes.

Name	Sale
Description	<div></div>
Right party connect	<input checked="" type="checkbox"/>
Success	<input checked="" type="checkbox"/>
Closure	<input checked="" type="checkbox"/>
Answer Machine by Agent	<input type="checkbox"/>

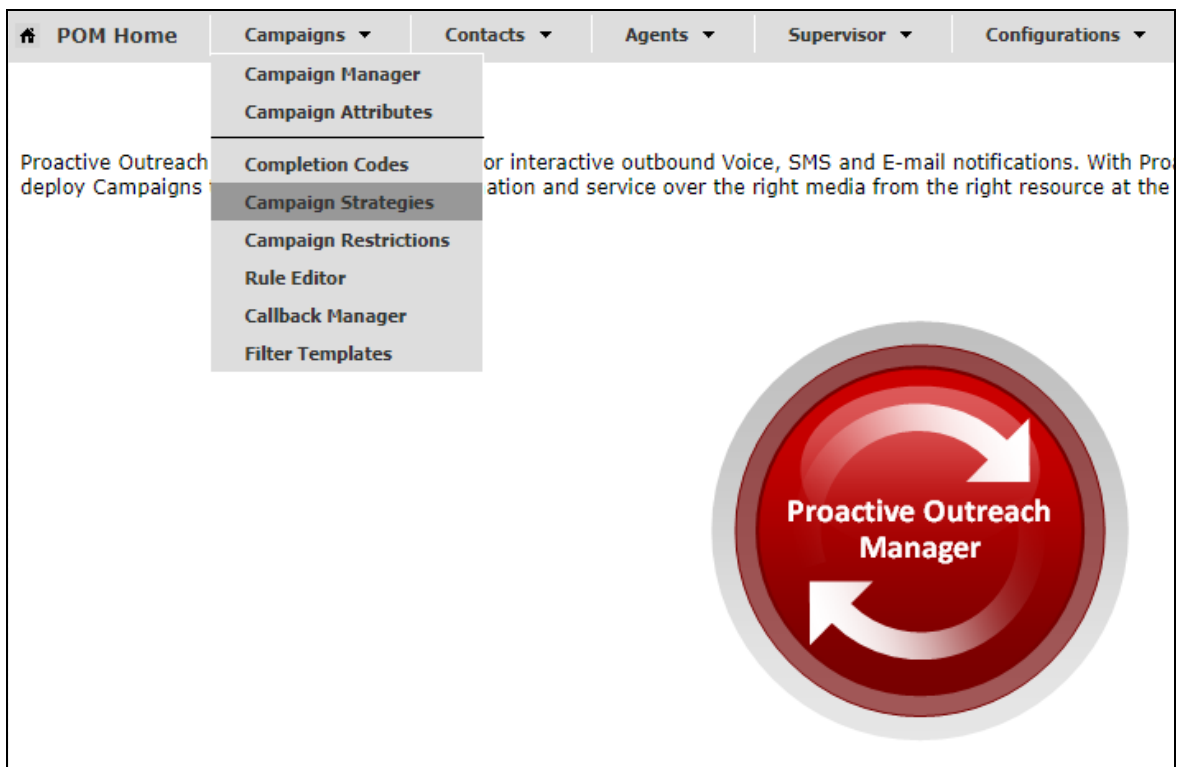
Save

Cancel

Help


12.1.2. Campaign Strategy

Navigate to **Campaigns** → **Campaign Strategies** as shown below.



The Campaign Strategies are shown below, where a new strategy can be added by clicking on **Add** or existing strategies can be viewed by clicking on the **Name** of the strategy displayed.

Campaign Strategies


[Refresh](#)

This page allows the user to manage Campaign Strategies, depending on the user role.

[Advanced](#)

Show 50 | Page: 1/1

Name	State	Task Types	Action
OutProgressive	Completed		
Preview	Completed		

Clicking on the **Preview** strategy from the screen above will show the **Campaign Strategy** called **Preview** that was created for compliance testing.

Not secure | https://10.10.40.30/VP_POM/faces/admin/ContactStrategy.xhtml

Selected Node: Task

- Restrictions
- Address
- Sender's Address
- Result Processors

Campaign Strategy: Preview

- ▼ Campaign Strategy
 - ▼ Handler (initial)
 - ▼ Preview
 - Address
 - Result Processors
 - Result (Call Answered)
 - Agent

Property	Value
Name	Preview
Description	
Sender's Display Name	DevConnect
Sender's Address	slp:9876@devconnect.local
Timeout (sec)	
Guard Times	Disable
Min Contact Time	
Max Contact Time	
Re-check Interval (min)	
On Media Server Failure	retry
Priority	5
Allocation Type	Dynamic
CCA Parameters	
Enhanced CCA	OFF
Background AMD	
Action on AMD	None
Silence Call Detection (SCD)	OFF
APPLICATIONS	
Driver Application	PomDriverApp
Nailer Application	Nailer
Nuisance Call Application	AvayaPOMAnnouncement
On Hold Application	AvayaPOMAnnouncement
PACING PARAMETERS	
Call Pacing Type	Preview
Timed Preview	No
Preview Time (Sec)	
Can Cancel Preview	Disable
Min. Agents	1

Scrolling down from the screen on the previous page shows the Default Completion code and here the Completion Code created in **Section 12.1.1** can be added. The **Applications** located on Experience Portal are also added here under **APPLICATIONS**.

Campaign Strategy: Preview

▼ Campaign Strategy

▼ Handler (initial)

▼ Preview

Address

▼ Result Processors

▼ Result (Call Answered)

Agent

CCA Parameters

Enhanced CCA	OFF
Background AMD	
Action on AMD	None
Silence Call Detection (SCD)	OFF

APPLICATIONS

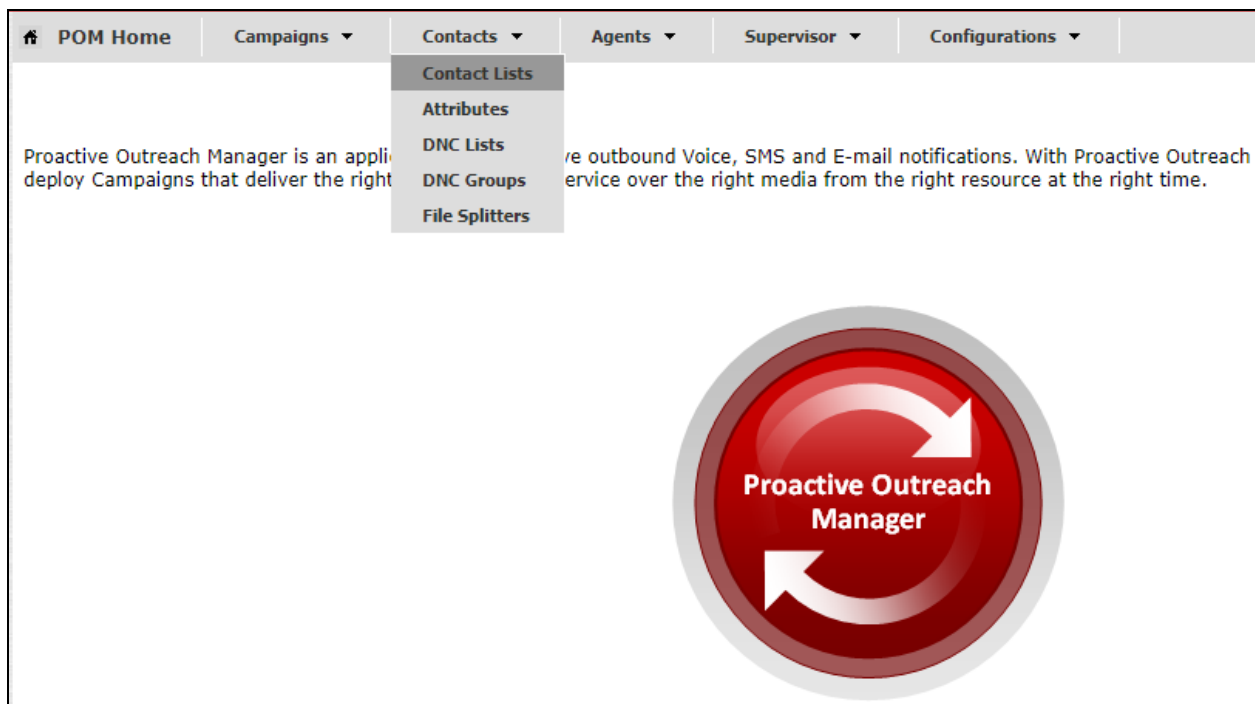
Driver Application	PomDriverApp
Nailer Application	Nailer
Nuisance Call Application	AvayaPOMAnnouncement
On Hold Application	AvayaPOMAnnouncement

PACING PARAMETERS

Call Pacing Type	Preview
Timed Preview	No
Preview Time (Sec)	
Can Cancel Preview	Disable
Min. Agents	1
Max. Agents	5
Agent Outbound Skill	Outbound
ACW Time (Sec)	10
# of ACW extensions	0
Default Completion code	Sale

12.2. Contact List

To add or view the Contact Lists, navigate to **Contacts** → **Contact Lists** as shown below.



There is a Contact List already configured for the Preview Campaign called **CMtoIPO**. Details of this Contact List can be viewed by clicking on the **Show all Contacts** icon, highlighted below. A new Contact List can be added by clicking on **Add** and uploading the contacts from a file.

Contact Lists

[Refresh](#)

This page displays all the Contact Lists. Depending on the user role, you can add, change, delete and empty Contact List. You can see Contacts in a Contact List. If organizations are enabled, you can associate Contact List with organization.

Last poll: 08/08/2019 02:26:40 PM

Contact List Name	Total Contacts	Available Contacts	Excluded Contacts	Last Updated	Actions
CMtoIPO	3	3	0	07/01/2019 01:12:28 PM	

* In Progress means Contacts are being imported into a Contact List. Total Contacts count is updated after completion of import activity.

Add Help

The Contact List shown has three entries in it calling to **85250** then **85123** and finally to **85202**.

Contact Browser
This page shows Contacts present in Contact List CMtoIPO.

Contact search and sort criteria

Search Contact where Attribute

Sort Contact using Attribute in order

Customer ID Attribute

Customer ID Attribute must be a combination of lower case letter [a-z], upper case letter [A-Z], numeric character [0-9] and special characters, _ , / , dot/period/full stop. Special character must be EMBEDDED somewhere in the middle of the Customer ID, and not in the first or the last character of the string. If CustomerID is not adhere to mentioned guidelines than that specific attempt record will not be published to Context Store.

Select Attribute that represents Customer ID

Customer ID Retrieval Mode ☐ Always ☒ Never ☐ Attribute Value is Blank

Records Per Page Page Number: 1
Total Pages: 1

System Contact ID	ID	First Name	Last Name	Phone 1	Phone 1 Country Code	Time Zone	Phone 1 State	Phone 1 Wireless	Phone 2	Phone 2 Country Code	Phone 2 Wireless
1	1	Paul	Greaney	85250	1	Europe/Dublin			85250	1	
2	2	Emma	Greaney	85123	1	Europe/Dublin			85123	1	
3	3	Dave	Greaney	85202	1	Europe/Dublin			85202	1	

12.3. Preview Campaign

Navigate to **Campaigns → Campaign Manager** as shown below.

POM Home **Campaigns** **Contacts** **Agents** **Supervisor** **Configurations**

Campaign Manager
Campaign Attributes
Completion Codes
Campaign Strategies
Campaign Restrictions
Rule Editor
Callback Manager
Filter Templates

Proactive Outreach deploy Campaigns or interactive outbound Voice, SMS and E-mail notifications. With Proactive Outreach and service over the right media from the right resource at the right time.

Proactive Outreach Manager

There are two outbound campaigns already configured for the compliance testing, a progressive campaign and a preview campaign. A new campaign can be added by clicking on the **Add** button or an existing campaign can be viewed by clicking on the **Name**.

Campaign Manager

Refresh

Last poll: 08/08/2019 02:28:23 PM

This page displays Campaigns and actions associated with Campaigns depending on your user role.

Show 50 | Page: 1/1

Name	Type	Campaign Strategy	Contact Lists	Last Executed	Waiting Callbacks	Actions
OutboundPreview	Finite	Preview	CMtoIPO	08/08/2019 11:44:02 AM 0		<input type="button" value="Details"/> <input type="button" value="Edit"/> <input type="button" value="Pause"/> <input type="button" value="Resume"/> <input type="button" value="Stop"/> <input type="button" value="Delete"/>
OutboundProgressive	Finite	OutProgressive	CMtoIPO	07/17/2019 04:20:30 PM 0		<input type="button" value="Details"/> <input type="button" value="Edit"/> <input type="button" value="Pause"/> <input type="button" value="Resume"/> <input type="button" value="Stop"/> <input type="button" value="Delete"/>




* In Progress means Campaign job can be in any one of the states - running, pausing, paused, callback, stopping, stopped callback.

The **Campaign Strategy** that was shown in **Section 12.1.2** is entered at the top of the screen below. The example below shows a Do Not Call (**DNC**) **Group** called **PG** (this was not shown in the **Appendix**) associated with this Campaign. Click on **Next** to continue.

Campaign Strategy

Select a Campaign Strategy from the following list to be used in the Campaign. Click on the icons to create a new Campaign Strategy, view details of a selected Strategy or refresh the current list.

Preview



Campaign type

☒ Finite ☐ Infinite

☐ Do not associate any Contact List at start

External Selection

☐ External Selection

Contact Record Assignment to Agent

☐ Attributes ☐ Agent ID

DNC Group

☒ Apply DNC Group

From the following list select one or more DNC Group to be used with this Campaign.

PG

From the following list select one DNC Group to be used for Agent/Web service. Agent/Web Service marked DNC contacts will be added to this DNC Group.

PG

Context Store

☐ Publish Attempt Data To Context Store

Cancel

Next

Help

The **Contact List** displayed in **Section 12.2** is associated with this campaign.

Contact List and Filter Selection
Select Contact List and Filter for this campaign

Name: OutboundPreview

If no Filter is associated for a Contact List, then all the Contacts present in that Contact List are selected

Contact List and Filter Template Association

Press the button below to add new association. Select Contact List, select an appropriate Filter for that Contact List. Repeat it for each Contact List to be used for this Campaign. Associating a Filter with the Contact List is not mandatory. Maximum 15 Contact Lists can be added to the campaign. Only one Filter can be associated with a Contact List. Use the Apply same filter checkbox to apply filter template associated with top row of association table to all other rows. Use No dialing Allocation checkbox if filtering and dialing should not be driven based on dialing allocation. No dialing Allocation checkbox will be enabled only if Apply same filter is enabled.

☐ Apply same filter ☐ No Dialing Allocation

No.	Contact List	Filter Template	Dialing Allocation Percent	Actions
1	CMtoIPO(Default) ▼	Select ▼	100	Preview

Add Association

View Records

Click on the "Show Results" button to display the Contacts selected based on the criteria entered in the above section. If no selection criteria is entered, all the records from Contact List are shown.

Show Results

Pause Dialing During Record Selection

On enabling this flag, POM will momentarily pause dialing till record selection completes. POM will pause the dialing whenever user modifies the filter condition or new import is scheduled on the associated contact list or new contact file is uploaded from web interface or a contact list is added or removed from the job. This will ensure that contacts are filtered and sorted before new attempt is made for the job. If the flag is disabled, POM will continue with dialing of records along with record selection in parallel and cannot guarantee the record ordering.

☐ Pause Dialing During Record Selection

Cancel **Previous** **Next** **Finish** **Help**

There are many other configurations that may be required for various campaigns to operate, the screen shots displayed here are to serve as to display the setup used for compliance testing. This was for the preview campaign that was used, and the contact list and strategy associated with that outbound preview campaign.

©2020 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.