



## DevConnect Program

---

# Application Notes for Tetherfi Multimedia Agent Client R5.1 with Avaya Proactive Outreach Manager R4.0.2 – Issue 1.0

## Abstract

These Application Notes describe the configuration steps required for Tetherfi Multimedia Agent Client 5.1 to interoperate with Avaya Proactive Outreach Manager 4.0.2. Tetherfi Multimedia Agent Client is a web-based CTI solution which integrates with Avaya Proactive Outreach Manager using the Agent Desktop API.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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.

# 1. Introduction

These Application Notes describe the configuration steps required for Tetherfi Multimedia Agent Client 5.1 to interoperate with the Avaya solution consisting of Avaya Proactive Outreach Manager R4.0.2, Avaya Aura® Communication Manager R10.1, Avaya Aura® Session Manager R10.1 and Avaya Aura® Application Enablement Services R10.1 using the Agent Desktop API on Avaya Proactive Outreach Manager (POM). Tetherfi Multimedia Agent Client (TMAC) is a web-based CTI solution. This thin client provides a single unified CTI desktop capable of servicing Voice, SMS, Email, Chat, Video and Social Media Channels.

TMAC is an Agent/User desktop application that allows users to control telephony functions via their desktop PC instead of physical hard phone or softphone. It empowers agents/users to interact with customers across multiple channels. TMAC connects to POM using the Agent Desktop API to provide Computer Telephony Integration (CTI) call control and monitoring functionality. Contact Center agents log into this desktop to handle all interactions across channels for outbound calls.

**Note:** Tetherfi Multimedia Agent Client may also be referred to as ‘TMAC’, or ‘Agent Desktop’ throughout these Application Notes.

**Note:** A connection to Avaya Aura® Application Enablement Services is required in order for this solution to work. The details of this connection are contained in the *Application Notes for Tetherfi Multimedia Agent Client with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services*, please refer to these Application Notes for any information on the connection to Avaya Aura® Application Enablement Services.

## 2. General Test Approach and Test Results

The general test approach was to validate the ability of TMAC to connect to POM and handle and control various Communication Manager endpoints in a variety of outbound call scenarios. Two agents were logged into TMAC, each agent was assigned to a specific Avaya endpoint, a SIP and H.323 endpoint was used during compliance testing. Outbound POM calls were made from these endpoints using TMAC to control the calls. Two outbound campaigns were run, a progressive campaign where outbound calls are made to customers on behalf of the agent and the agent is connected automatically, and a preview campaign where the call is presented to the agent allowing the outbound call to be initiated by the agent. All calls are handled by the agent desktop. Serviceability testing was carried out to observe the response of the agent desktop when various LAN failures were simulated.

For compliance testing, POM was configured as “CCElite” to allow communications with Communication Manager and Application Enablement Services. POM was installed on Avaya Experience Portal. Calls to and from Experience Portal were routed via a SIP trunk to Avaya Aura® Session Manager.

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 Avaya systems and Tetherfi Multimedia Agent Client did not include use of any specific encryption features as requested by Tetherfi.

## 2.1. Interoperability Compliance Testing

Interoperability compliance testing consisted of using TMAC to verify successful handling and control of a variety of endpoints as follows:

- Agent Log In/Log Out using Agent Desktop.
- Set Status for ACD Agents using Agent Desktop.
- Outbound calls using POM and controlling the call using Agent Desktop.
- Scheduling Callback using Agent Desktop.
- Adding and removing contacts from Do Not Call (DNC) lists.
- Call features such as hold, consult, transfer and conference using Agent Desktop.
- Serviceability testing by simulating LAN failures.

## 2.2. Test Results

All test cases were executed successfully, with the following observations:

1. Calls must be transferred or conferenced within 40secs (approx.) or the transfer/conference consultation will fail. This is when transferring or conferencing with another agent ID, the transfer/conference will work fine when done to another extension.
2. There are some discrepancies with the precise information shown on the Agent State compared to that shown on the POM Dashboard, however they would always be referring to the same state, for example the POM dashboard may show 'idle' and TMAC shows 'ready'.
3. A connection to Avaya Aura® Application Enablement Services is required for this solution to work. The details of this connection are contained in the *Application Notes for Tetherfi Multimedia Agent Client with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services*.

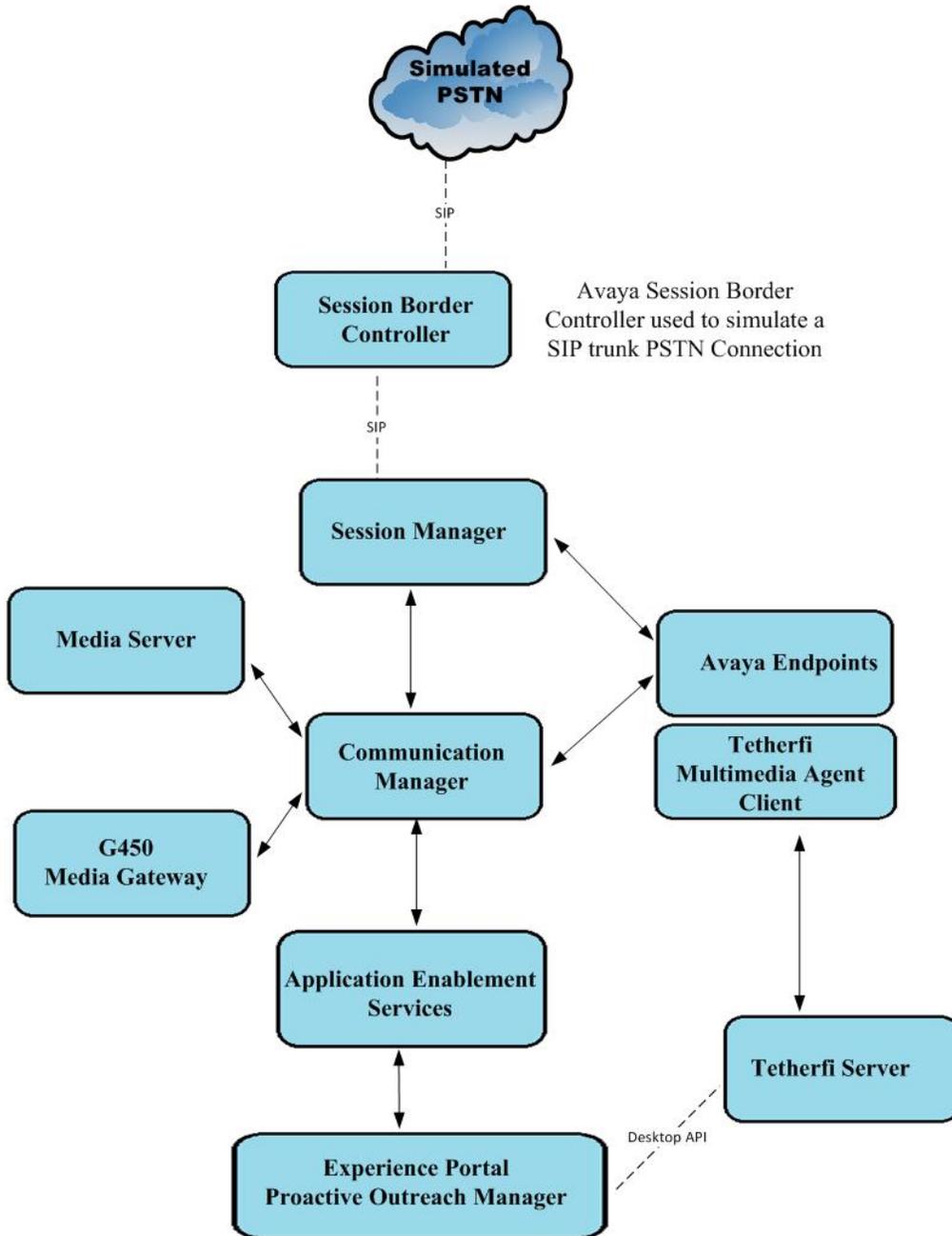
## 2.3. Support

Technical support on Tetherfi can be obtained through the following:

- Phone: +65-6715 7048 (Singapore), +1-415 9157048 (US)
- Email: [support@tetherfi.com](mailto:support@tetherfi.com)
- Web: <https://www.tetherfi.com>

### 3. Reference Configuration

**Figure 1** below shows Communication Manager serving both SIP and H.323 endpoints with Avaya Proactive Outreach Manager providing an Agent Desktop API to which the Tetherfi Multimedia Agent Client application connects to. Session Manager is used to route the outbound calls to the PSTN via Session Border Controller.



**Figure 1: Connection of Tetherfi Multimedia Agent Client with Avaya Proactive Outreach Manager R4.0.2 and Avaya Aura® Communication Manager R10.1**

## 4. Equipment and Software Validated

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

<b>Avaya Equipment/Software</b>	<b>Firmware/Version</b>
Avaya Experience Portal	8.1.2.0.0402
Avaya Proactive Outreach Manager	4.00.02.02.23116
Avaya Aura® System Manager	System Manager 10.1.3.0 Feature Pack 3 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.3.0.0715713
Avaya Aura® Session Manager	Session Manager R10.1 Build No. – 10.1.3.0.1013007
Avaya Aura® Communication Manager	R10.1.3.0 – FP3 R020x.01.0.974.0 Update ID 01.0.974.0-27893
Avaya Aura® Application Enablement Services	10.1.3 R10.1.3.0.0.11-0
Avaya Aura® Media Server	10.1.0.101
Avaya G450 Media Gateway	42.7.0 /2
Avaya J100 Series (H323) Deskphone	6.8.5.3.2
Avaya J100 Series (SIP) Deskphone	4.0.14.0.7
Avaya 9404 Digital Deskphone	17.0
Avaya Session Border Controller (To facilitate simulated PSTN)	10.1
<b>Tetherfi Equipment/Software</b>	<b>Firmware/Version</b>
Tetherfi Multimedia Agent Client Server	5.1.11.3009
Tetherfi Agent Desktop UI	5.2.7.3004
Tetherfi CTI Server	6.0.5.19
Tetherfi SMS API Server	5.1.3.1514
Windows 10 PC running a Web Browser	Windows 10/Chrome 119.0.6045.160

All equipment are virtual servers running on VMware.

## 5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using the Communication Manager System Access Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**.

**Note:** Some screens in this section have been abridged and highlighted for brevity and clarity in presentation. The general installation of the Avaya Media Servers and Media Gateways are presumed to have been previously completed and is not discussed here.

### 5.1. Configuration of the Hunt Group and Agent

For calls to be routed to agents, Hunt Groups (skills), must be configured and then assigned to Agents.

#### 5.1.1. Hunt Group

A hunt group is setup for outbound calls. The outbound hunt group is referenced in **Section 6.3** as a Skill in POM. Enter the **add hunt-group n** command where **n** in the example below is **10**. On **Page 1** of the **hunt-group** form, assign a **Group Name** and **Group Extension** valid under the provisioned dial plan. **Group Type** should be set to **ead-mia**. **ACD**, **Queue** and **Vector** set to **y**.

```
add hunt-group 10                                     Page 1 of 4
                                                    HUNT GROUP
      Group Number: 10                                ACD? y
      Group Name: Outbound                            Queue? y
      Group Extension: 3801                           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:
```

On **Page 2**, set the **Skill** field to **y** as shown below.

```
add hunt-group 10                                     Page 2 of 4
                                                    HUNT GROUP
                Skill? y      Expected Call Handling Time (sec): 180
                  AAS? n
                Measured: none
Supervisor Extension:

                Controlling Adjunct: none

                Multiple Call Handling: none

                Timed ACW Interval (sec):      After Xfer or Held Call Drops? n
```

### 5.1.2. Administer Agent Logins

Enter the **add agent-loginID n** command, where **n** is an available extension number. Enter a descriptive name for the agent in the **Name** field. . The **Auto Answer** field is set to **station**. Configure a password as required.

```
add agent-loginID 3411                               Page 1 of 2
                                                    AGENT LOGINID
                Login ID: 3411                        AAS? n
                Name: Agent1                          AUDIX? n
                TN: 1      Check skill TNs to match agent TN? n
                COR: 1
                Coverage Path:                        LWC Reception: spe
                Security Code:                        LWC Log External Calls? n
                Attribute:                            AUDIX Name for Messaging:

                                                    LoginID for ISDN/SIP Display? n
                                                    Password:
                                                    Password (enter again):
                                                    Auto Answer: station
                AUX Agent Remains in LOA Queue: system      MIA Across Skills: system
                AUX Agent Considered Idle (MIA): system      ACW Agent Considered Idle: system
                Work Mode on Login: system                    Aux Work Reason Code Type: system
                                                    Logout Reason Code Type: system
                Maximum time agent in ACW before logout (sec): system
                Forced Agent Logout Time: :

                WARNING: Agent must log in again before changes take effect
```

On **Page 2**, assign the skills to the agent by entering the relevant hunt group numbers created in

**Section 5.1.1** for **SN** and entering a skill level of **1** for **SL**. In this case, an agent able to handle outbound calls is created.

```
change agent-loginID 3411                                     Page 2 of 2
                    AGENT LOGINID
    Direct Agent Skill: 10                                     Service Objective? n
Call Handling Preference: skill-level                         Local Call Preference? n

    SN   RL  SL           SN   RL  SL
1: 10   1    1           16:
2:
3:
4:
5:
6:
7:
```

Repeat this task accordingly for any additional inbound or outbound agents required.

## 5.2. Configuration of Call Routing

The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options.
- System Features and Access Codes.
- Administer Dial Plan.
- Administer Route Selection for outgoing calls.

**Note:** The configuration of the simulated PSTN is outside the scope of these Application Notes.

### 5.2.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that the **Maximum Administered SIP Trunks** have sufficient capacity. Each call uses a minimum of one SIP trunk.

```

display system-parameters customer-options                               Page 2 of 12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
    Maximum Administered H.323 Trunks: 12000                          15
    Maximum Concurrently Registered IP Stations: 2400                  2
    Maximum Administered Remote Office Trunks: 12000                  0
Max Concurrently Registered Remote Office Stations: 2400              0
    Maximum Concurrently Registered IP eCons: 128                     0
    Max Concur Reg Unauthenticated H.323 Stations: 100                 0
    Maximum Video Capable Stations: 36000                             0
    Maximum Video Capable IP Softphones: 150                          3
    Maximum Administered SIP Trunks: 12000                            65
    Max Administered Ad-hoc Video Conferencing Ports: 12000           0
    Max Number of DS1 Boards with Echo Cancellation: 688              0
  
```

On **Page 4**, ensure that **ARS** is set to **y**.

```

display system-parameters customer-options                               Page 4 of 12
                                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                       Cvg Of Calls Redirected Off-net? y
    ARS/AAR Partitioning? y                                           DCS (Basic)? y
    ARS/AAR Dialing without FAC? n                                     DCS Call Coverage? y
    ASAI Link Core Capabilities? y                                     DCS with Rerouting? y
    ASAI Link Plus Capabilities? y
    Async. Transfer Mode (ATM) PNC? n
    Attendant Vectoring? y
  
```

On **Page 6**, ensure that **Uniform Dialing Plan** is set to **y**.

```
display system-parameters customer-options                               Page 6 of 12
                                OPTIONAL FEATURES

    Multinational Locations? n                Station and Trunk MSP? y
Multiple Level Precedence & Preemption? y    Station as Virtual Extension? y
    Multiple Locations? n
    Personal Station Access (PSA)? y          System Management Data Transfer? n
    PNC Duplication? n                       Tenant Partitioning? y
    Port Network Support? y                  Terminal Trans. Init. (TTI)? y
    Posted Messages? y                      Time of Day Routing? y
    Private Networking? y                   TN2501 VAL Maximum Capacity? y
    Processor and System MSP? y              Uniform Dialing Plan? y
    Processor Ethernet? y                   Usage Allocation Enhancements? y
    Remote Office? y                         Wideband Switching? y
Restrict Call Forward Off Net? y              Wireless? n
    Secondary Data Module? y
```

### 5.2.2. System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **Page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 10** for supporting documentation.

```
display system-parameters features                                       Page 1 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS
    Self Station Display Enabled? n
    Trunk-to-Trunk Transfer: all
    Automatic Callback with Called Party Queuing? y
Automatic Callback - No Answer Timeout Interval (rings): 3
    Call Park Timeout Interval (minutes): 10
    Off-Premises Tone Detect Timeout Interval (seconds): 20
    AAR/ARS Dial Tone Required? y

    Music (or Silence) on Transferred Trunk Calls? all
    DID/Tie/ISDN/SIP Intercept Treatment: attendant
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
    Automatic Circuit Assurance (ACA) Enabled? n
```

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. Note that **8** is used for AAR and **9** for ARS routing.

```

display feature-access-codes                                     Page 1 of 10
                                FEATURE ACCESS CODE (FAC)
    Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
    Announcement Access Code:
    Answer Back Access Code:
    Attendant Access Code:
    Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
    Automatic Callback Activation: *25      Deactivation: #25
  
```

### 5.2.3. Administer Dial Plan

It was decided for compliance testing that all calls to the “PSTN” were calls that began with **3539184xxxx** and these were to be sent across the SIP trunk via the Session Border Controller to another Communication Manager, thus simulating a PSTN call. To achieve this, automatic route selection (ARS) will be used to route the calls. The dial plan and ARS routing analysis need to be changed to allow this routing.

Type **change dialplan analysis** to make changes to the dial plan. Note that **3539184** is of call type **udp** which means any numbers beginning with 3539184 are a part of the uniform dial plan. The total length is 11 meaning that 3539184xxxx will be sent across the trunk.

```

change dialplan analysis                                     Page 1 of 12
                                DIAL PLAN ANALYSIS TABLE
                                Location: all                    Percent Full: 3

    Dialed   Total   Call   Dialed   Total   Call   Dialed   Total   Call
    String   Length Type   String   Length Type   String   Length Type
    1         4     udp     #         3     fac
    2         4     udp
    3539184   11    udp
    4         4     ext
    5         4     udp
    58        5     ext
    5999      4     ext
    6         4     udp
    6666      4     ext
    7         4     udp
    781       5     ext
    8         1     fac
    9         1     fac
    *         3     fac
    *8        4     dac
  
```

### 5.2.4. Administer Route Selection for Outgoing Calls

Use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to **3539184** will use ARS. No further digits are deleted or inserted. Calls are sent to **ars** for further processing.

```
change uniform-dialplan 3                                     Page 1 of 2
                                     UNIFORM DIAL PLAN TABLE
                                     Percent Full: 0
```

Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num
<b>3539184</b>	11	0		<b>ars</b>	n	
4	4	0		aar	n	
5				ars	n	
					n	
					n	
					n	
					n	
					n	

Use the **change ars analysis** command to further configure the routing of the dialed digits. Calls to the ‘Simulated PSTN’ are achieved by dialing **3539184xxxx** and are matched with the ARS entry shown below. Calls are sent to **Route Pattern 22**, which contains the outbound SIP Trunk Group.

```
change aar analysis 3                                     Page 1 of 2
                                     AAR DIGIT ANALYSIS TABLE
                                     Location: all
                                     Percent Full: 3
```

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
3	4	4	1	aar		n
<b>3539184</b>	11	11	<b>22</b>	lpvt		n
65	4	4	1	aar		n
7	7	7	254	aar		n
8	7	7	254	aar		n
9	7	7	254	aar		n
						n
						n
						n
						n
						n

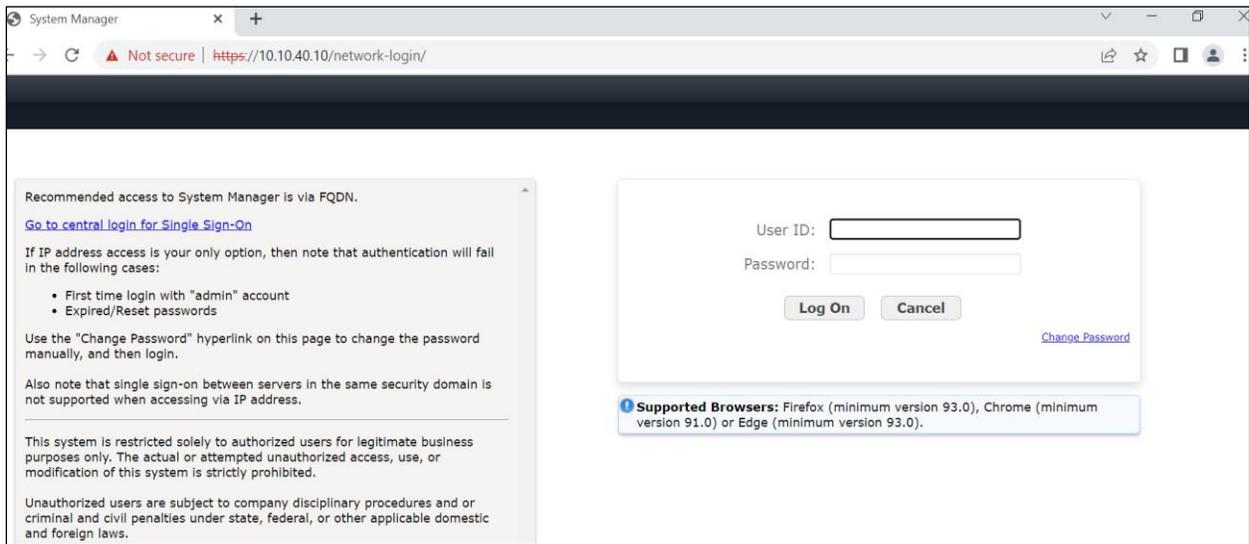
Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that ARS selects. In this configuration, Route Pattern Number **22** is used to route calls to trunk group **(Grp No) 22**. The **Numbering Format** was set to **pub-unk**. The configuration of this outgoing trunk is outside the scope of these Application Notes.

change route-pattern 22											Page 1 of 3			
Pattern Number: 1											Pattern Name: TO SIP PSTN			
SCCAN? n											Secure SIP? n		Used for SIP stations? n	
<b>Grp</b>	FRL	NPA	Pfx	Hop	Toll	No.	Inserted				DCS/	IXC		
<b>No</b>			Mrk	Lmt	List	Del	Digits				QSIG			
							Dgts				Intw			
1:	<b>22</b>	0									n	user		
2:											n	user		
3:											n	user		
4:											n	user		
5:											n	user		
6:											n	user		
	BCC	VALUE	TSC	CA-TSC		ITC	BCIE	Service/Feature	PARM	Sub	<b>Numbering</b>	LAR		
	0	1	2	M	4	W		Request		Dgts	<b>Format</b>			
1:	y	y	y	y	y	n	n				<b>pub-unk</b>	none		
2:	y	y	y	y	y	n	n					none		
3:	y	y	y	y	y	n	n					none		
4:	y	y	y	y	y	n	n					none		
5:	y	y	y	y	y	n	n					none		
6:	y	y	y	y	y	n	n					none		

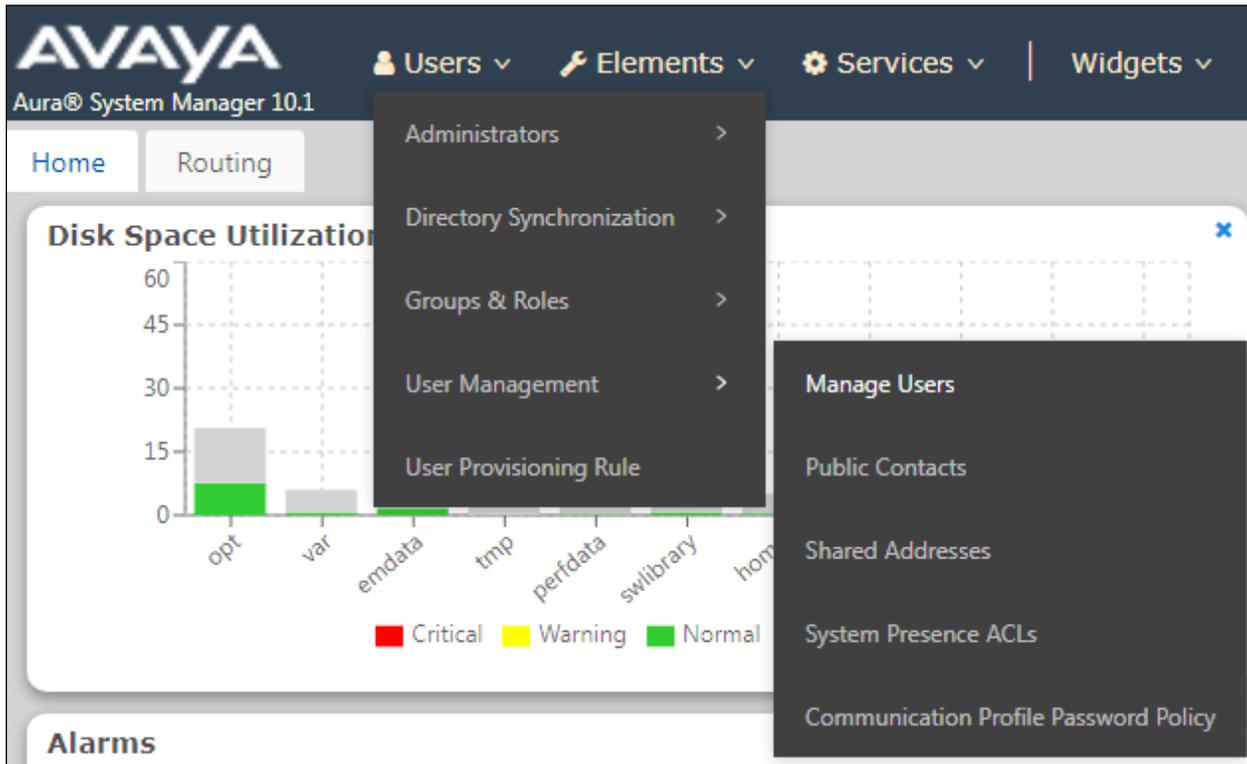
### 5.3. Configure Avaya SIP Endpoints for Third Party Call Control

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

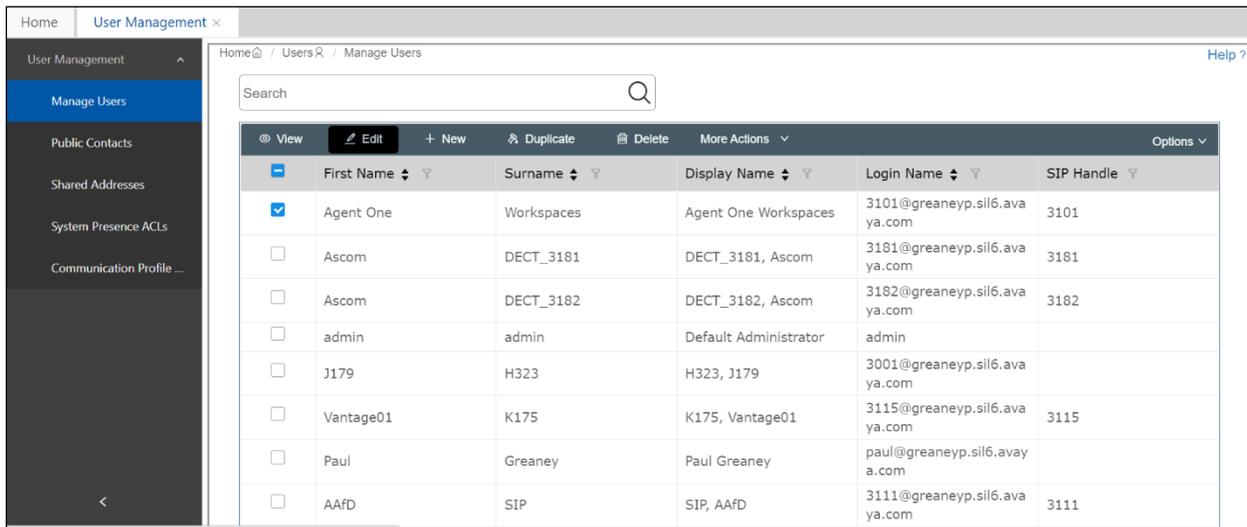
**Note:** The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



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**.



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

Home / Users / Manage Users Help ?

**User Profile | Edit | 3101@greanep.sil6.avaya.com** Commit & Continue Commit Cancel

Identity | **Communication Profile** | Membership | Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

**CM Endpoint Profile**

\* System : cm101x

\* Profile Type : Endpoint Editor

Use Existing Endpoints :

\* Extension : 3101

Template : Start typing...

\* Set Type : 9641SIPCC

Security Code : Enter Security Code

Port : S000003

Voice Mail Number : 6667

Preferred Handle : Select

Calculate Route Pattern :

Sip Trunk : aar

In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below.

<b>System</b>	cm101x	<b>Extension</b>	3101
<b>Template</b>	Select	<b>Set Type</b>	9641SIPCC
<b>Port</b>	S000003	<b>Security Code</b>	
<b>Name</b>	Agent One Workspaces		

<b>General Options (G)</b> *	<b>Feature Options (F)</b>	<b>Site Data (S)</b>	<b>Abbreviated Call Dialing (A)</b>	<b>Enhanced Call Fwd (E)</b>
<b>Button Assignment (B)</b>	<b>Profile Settings (P)</b>	<b>Group Membership (M)</b>		
* <b>Class of Restriction (COR)</b>	1	* <b>Class Of Service (COS)</b>	1	
* <b>Emergency Location Ext</b>	3101	* <b>Message Lamp Ext.</b>	3101	
* <b>Tenant Number</b>	1	<b>Type of 3PCC Enabled</b>	Avaya	
* <b>SIP Trunk</b>	aar	<b>Coverage Path 2</b>		
<b>Coverage Path 1</b>		<b>Localized Display Name</b>	Agent One Workspaces	
<b>Lock Message</b>	<input type="checkbox"/>	<b>Enable Reachability for Station Domain Control</b>	system	
<b>Multibyte Language</b>	Not Applicable			
<b>SIP URI</b>				
<b>Primary Session Manager</b>				
<b>IPv4:</b>	10.10.40.12	<b>IPv6:</b>		

The buttons were set as shown below but these are not critical to the overall operation of TMAC. Click on **Done** at the bottom of the screen (not shown).

The screenshot displays the 'Button Assignment (B)' configuration screen. At the top, there are tabs for 'General Options (G)', 'Feature Options (F)', 'Site Data (S)', 'Abbreviated Call Dialing (A)', and 'Enhanced Call Fwd (E)'. Below these are 'Button Assignment (B)', 'Profile Settings (P)', and 'Group Membership (M)'. The main content area has sub-tabs for 'Main Buttons', 'Feature Buttons', 'Button Modules', and 'Phone View'. The 'Main Buttons' tab is active, showing a table with 8 rows for button configurations. Each row includes a 'Favorite' checkbox, a 'Button Label' input field, and a 'Button Feature' dropdown menu. The 'Button Features' are: call-appr, call-appr, call-appr, agnt-login, auto-in, manual-in, aux-work, and after-call. To the right of the dropdowns are columns for 'Argument-1', 'Argument-2', and 'Argument-3', each with an input field. A 'Reason Code' dropdown is also present, with options for 'auto-in Grp', 'manual-in Grp', and 'after-call Grp'. A 'Hunt Grp' label is positioned between the 'Reason Code' and 'Argument-3' columns.

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

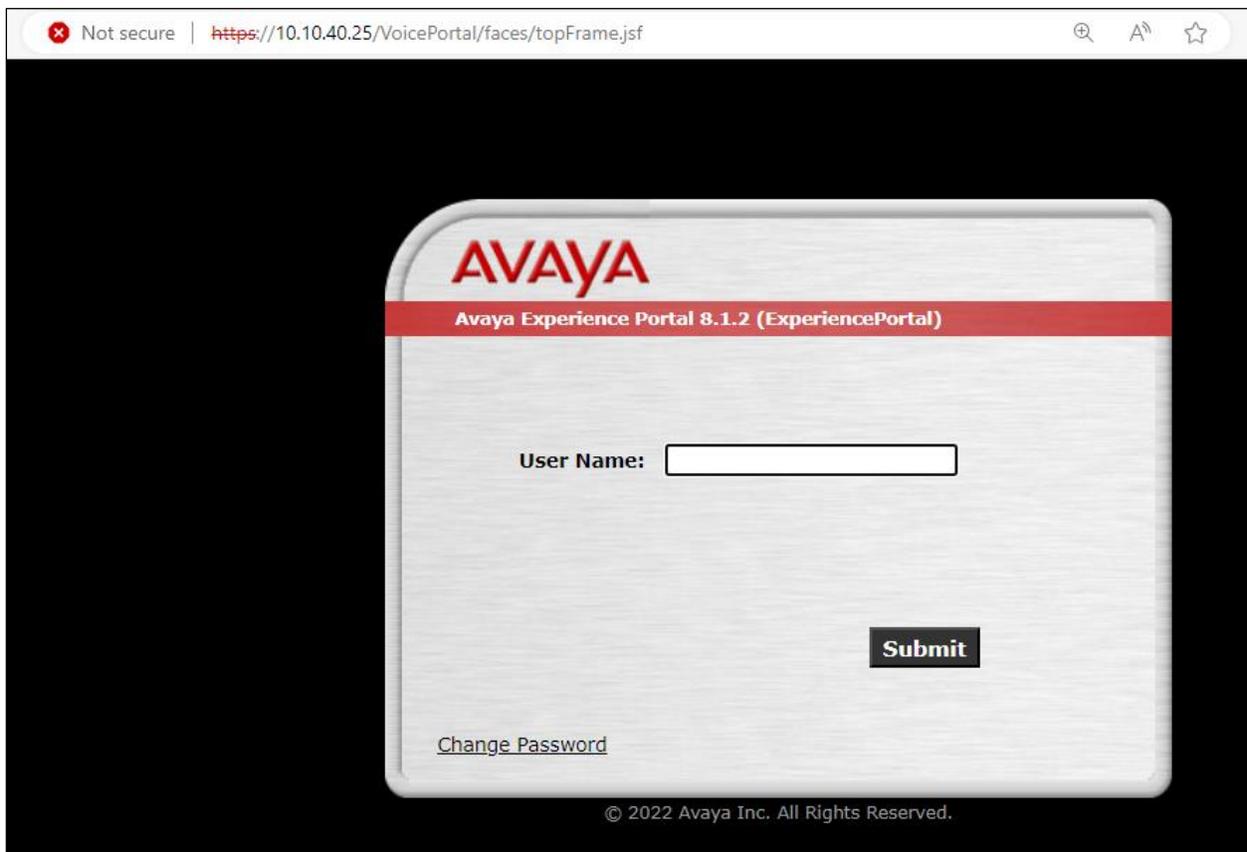
The screenshot shows the 'User Profile | Edit | 3101@greanep.sil6.avaya.com' page. At the top right, there are buttons for 'Commit & Continue', 'Commit', and 'Cancel'. Below the title are tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is selected. On the left, there is a 'Communication Profile Password' section with a 'PROFILE SET' dropdown set to 'Primary'. Below this are 'PROFILES' with toggle switches for 'Session Manager Profile', 'Avaya Breeze® Profile', and 'CM Endpoint Profile' (which is currently turned on). The main configuration area contains several fields: '\* System' (cm101x), '\* Profile Type' (Endpoint), 'Use Existing Endpoints' (checkbox), '\* Extension' (3101), 'Template' (Start typing...), '\* Set Type' (9641SIPCC), 'Security Code' (Enter Security Code), 'Port' (S000003), 'Voice Mail Number' (6667), 'Preferred Handle' (Select), 'Calculate Route Pattern' (checkbox), and 'Sip Trunk' (aar).

## 6. Configure Avaya Proactive Outreach Manager

This section describes the steps necessary to configure both POM and Experience Portal to allow TMAC to connect using the agent desktop API. Note that POM is installed on Experience Portal and that is why this section covers the administration of both Experience Portal and POM.

**Note:** It is assumed that both POM and Experience Portal are already installed with the connections made to both Session Manager and Application Enablement Services. The setup and configuration of these connections are therefore outside the scope of these Application Notes.

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



**Note:** The following sections are aimed to display the configuration on POM that was used during compliance testing and to help the reader understand the setup of POM that was used. They do not server as a setup and configuration guide for POM or Experience Portal.

## 6.1. Add a User on Avaya Aura® Experience Portal

A user is created on Experience Portal to allow the TMAC server to connect to POM. Navigate to **User Management** → **Users** in the left window. Click on **Add** in the main window.

**Avaya Experience Portal 8.1.2 (ExperiencePortal)**

Expand All | Collapse All

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 configure security options for all user logins. Configure the parameters under LDAP Settings to enable to your corporate directory.

<input type="checkbox"/>	Name	Enable	Type	Assigned Roles/Features	Last Login	Failed Attempts
<input checked="" type="checkbox"/>	<a href="#">epadmin</a>	Yes	EP (Password)	Administration, Auditor, Maintenance, Operations, Privacy Manager, User Manager, Web Services	Feb 15, 2024 3:49:30 PM GMT	
<input type="checkbox"/>	<a href="#">pom</a>	Yes	EP (Password)	Administration, POM Campaign Manager, POM Contact Attributes Unmask, Maintenance, Operations, POM Administration, POM Supervisor, User Manager, Web Services	Aug 29, 2023 4:08:00 PM IST	
<input type="checkbox"/>	<a href="#">Webservices</a>	Yes	EP (Password)	Web Services	Jan 30, 2024 4:38:17 PM GMT	

**Add** **Delete** **Help**

This user must have **Web Services** ticked as shown below. Enter a suitable password and click on **Save**.

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

Name: Webservices

Enable:  Yes  No

Roles:

<input type="checkbox"/> Administration	<input type="checkbox"/> Auditor	<input 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: 10/13/23 1:50 PM

Password:

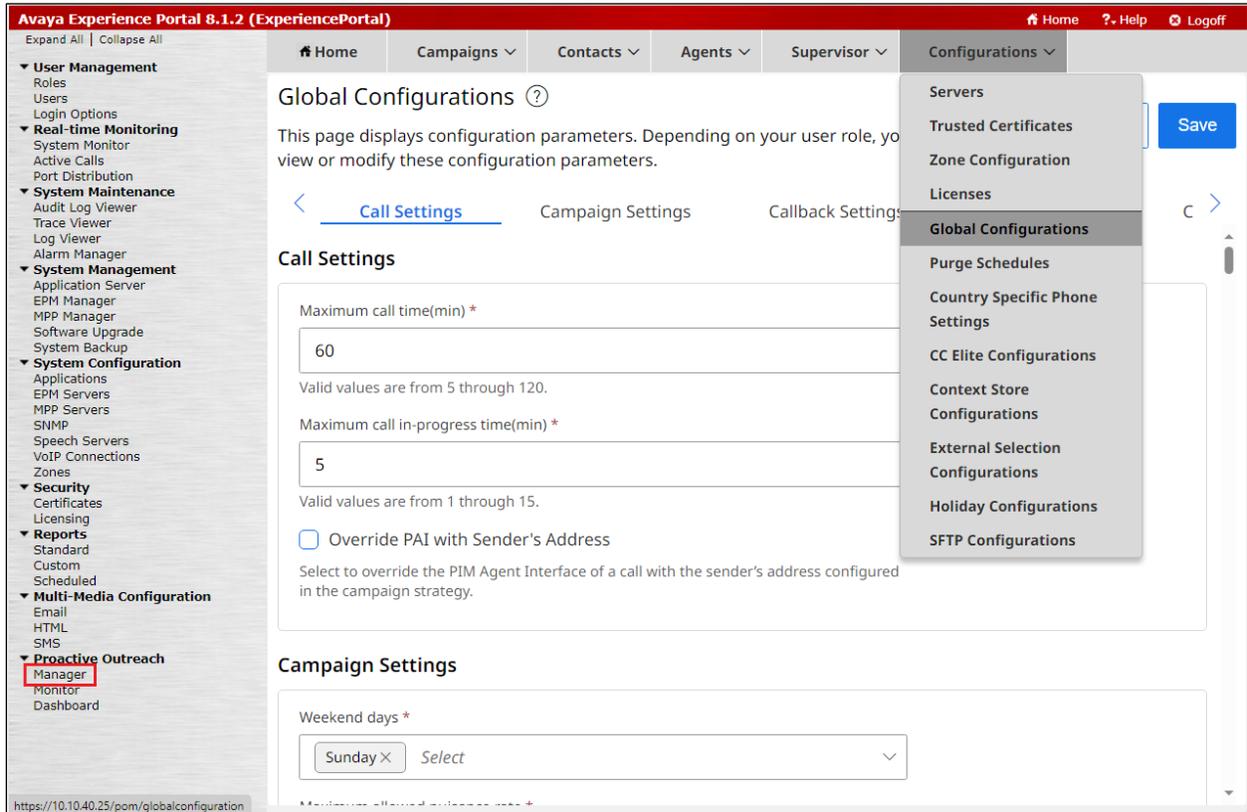
Verify Password:

Enforce Password Longevity:

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

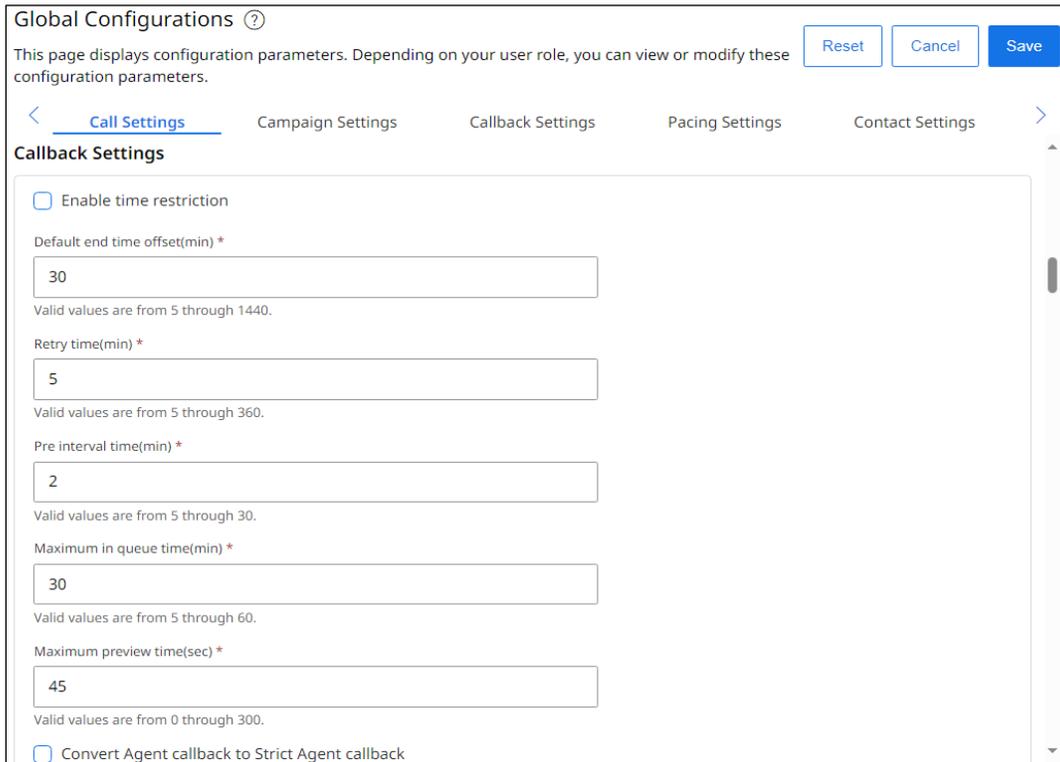
## 6.2. Display Configuration of POM Server

Navigate to **Proactive Outreach** → **Manager** in the left window and selecting **Configurations** in the main window shows the setup for the Proactive Outreach Manager. **Global Configurations** is selected below to display various settings that were used for compliance testing.



The screenshot displays the Avaya Experience Portal 8.1.2 (ExperiencePortal) interface. The left sidebar shows a navigation menu with categories like User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, Multi-Media Configuration, and Proactive Outreach. The 'Proactive Outreach' section is expanded, and 'Manager' is selected. The main content area shows the 'Global Configurations' page, which includes a 'Call Settings' section with input fields for 'Maximum call time(min) \*' (set to 60) and 'Maximum call in-progress time(min) \*' (set to 5). Below this is a checkbox for 'Override PAI with Sender's Address'. The 'Campaign Settings' section includes a 'Weekend days \*' dropdown menu currently set to 'Sunday'. A dropdown menu is open over the 'Configurations' tab, listing options such as Servers, Trusted Certificates, Zone Configuration, Licenses, Global Configurations (which is highlighted), Purge Schedules, Country Specific Phone Settings, CC Elite Configurations, Context Store Configurations, External Selection Configurations, Holiday Configurations, and SFTP Configurations. A 'Save' button is visible in the top right corner of the configuration area.

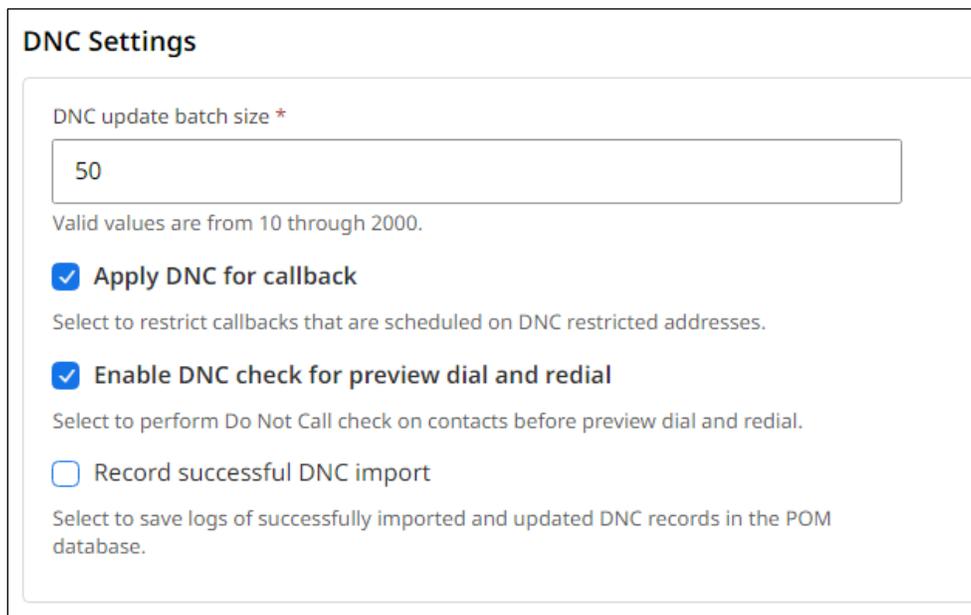
Information on various settings is shown including that of the **Callback Settings** shown below.



The screenshot shows the 'Global Configurations' page with a sub-section for 'Callback Settings'. At the top right, there are 'Reset', 'Cancel', and 'Save' buttons. Below the title, there are navigation tabs for 'Call Settings', 'Campaign Settings', 'Callback Settings', 'Pacing Settings', and 'Contact Settings'. The 'Callback Settings' section includes the following options:

- Enable time restriction
- Default end time offset(min) \*:   
Valid values are from 5 through 1440.
- Retry time(min) \*:   
Valid values are from 5 through 360.
- Pre interval time(min) \*:   
Valid values are from 5 through 30.
- Maximum in queue time(min) \*:   
Valid values are from 5 through 60.
- Maximum preview time(sec) \*:   
Valid values are from 0 through 300.
- Convert Agent callback to Strict Agent callback

The Do Not Call (**DNC**) **Settings** are shown below where the **Enable DNC check for preview dial and redial** was checked to allow the DNC to operate for both preview and progressive campaigns.



The screenshot shows the 'DNC Settings' section with the following options:

- DNC update batch size \*:   
Valid values are from 10 through 2000.
- Apply DNC for callback**  
Select to restrict callbacks that are scheduled on DNC restricted addresses.
- Enable DNC check for preview dial and redial**  
Select to perform Do Not Call check on contacts before preview dial and redial.
- Record successful DNC import  
Select to save logs of successfully imported and updated DNC records in the POM database.

The following **Agent Settings** were set for compliance testing.

**Agent Settings**

Maximum job waiting duration(min) \*

Valid values are from 10 through 60.

Minimum job attachment period(min) \*

Valid values are from 1 through 480.

Nailing retry interval(sec) \*

Valid values are from 10 through 1800.

Nailup call CLID \*

The sender's address to be displayed in the nail up call of an agent.

Maximum record waiting duration for attribute dialing(min) \*

Valid values are from 10 through 60.

ANI for external consult calls

Nailup call CLID

Agent Extension

Use campaign ANI

Free form Text

The ANI to be used for external consult calls.

The **Advanced Settings** displays the various port connections including that of the **Agent manager base port** that is used by TMAC.

**Advanced Settings**

JMS listen port \*

Valid values are from 1024 through 65535.

Pacer base port \*

Valid values are from 1024 through 65535.

Agent Initiated Pacer base port \*

Valid values are from 1024 through 65535.

Router base port \*

Valid values are from 1024 through 65535.

Agent manager base port \*

Valid values are from 1024 through 65535.

Maximum concurrent jobs \*

### 6.3. Display the Configuration of the CTI Connection

Select **Configuration** → **CC Elite Configurations** from the main window. **Aura10.1** was the CTI group already set up for compliance testing, clicking on this will open the connection to show the details.

**CC Elite Configurations**

This page allows editing of CTI server setup details, CMS server setup details and skills in POM d

**CTI Configuration**

CTI Group Name	CM IP Address	CM Login	AES IP Address	AES Secure Connection	Action
<a href="#">Aura81</a>	10.10.40.37	pomout	10.10.40.38		
<a href="#">Aura10.1</a>	10.10.40.13	pomout	10.10.40.16		

**Add CTI Detail** **Help**

**CMS Configuration**

Server IP Port	CMS Secure Connection	Server Role	Agent Thashing Interval (seconds)	Action
----------------	-----------------------	-------------	-----------------------------------	--------

**Add CMS Configuration** **Help**

Information such as the IP Address of Communication Manager and the Application Enablement Services are stored here as well as the Communication Manager user that was created for POM.

* CTI group name	<input type="text" value="Aura10.1"/>
* CM IP address	<input type="text" value="10.10.40.13"/>
* CM login	<input type="text" value="pomout"/>
* CM password	<input type="password" value="••••••••"/>
* AES IP address	<input type="text" value="10.10.40.16"/>
AES Secure Connection	<input checked="" type="checkbox"/>
CTI group role	<input type="text" value="Active"/> ▼

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

From the **CC Elite Configurations** page, the outbound skill must be added. Again, this was already in place but can be added by clicking on **Add Skill**, as shown below.

### CC Elite Configurations Refresh

This page allows editing of CTI server setup details, CMS server setup details and skills in POM database associated with CC Elite skills.

Last poll: 02/15/2024 04:01:10 PM

**CTI Configuration**

CTI Group Name	CM IP Address	CM Login	AES IP Address	AES Secure Connection	CTI Group Role	Action
<a href="#">Aura81</a>	10.10.40.37	pomout	10.10.40.38	false	Select	
<a href="#">Aura10.1</a>	10.10.40.13	pomout	10.10.40.16	true	Active	

Add CTI Detail
Help

**CMS Configuration**

Server IP Port	CMS Secure Connection	Server Role	Agent Thrashing Interval (seconds)	Action

Add CMS Configuration
Help

Skillset name All

Skillset type All Skills All

Show
Refresh Skills

CC Elite Skill Number	POM Skill Name	Skill Type	Parameter to Monitor for Blending	EWT levels	Agent Acquire Threshold	Agent Release

Add Skill
Help

The skillset number must match that of the hunt group created in **Section 5.1.1**, hunt group **10** was used for outbound calls.

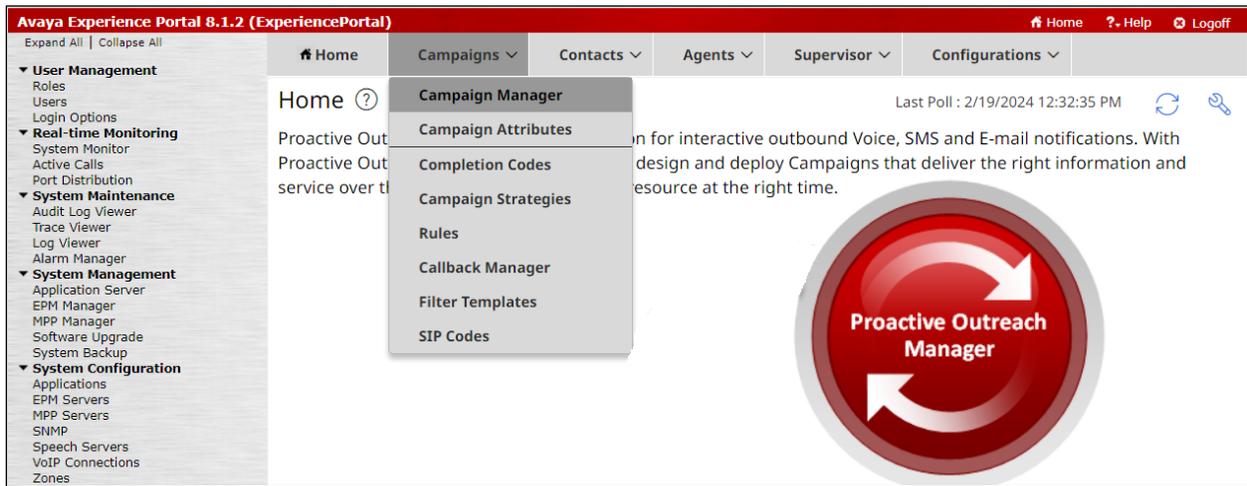
### Create POM Skills

This page allows creation of skills in POM database and associating it with CC Elite skill. For skill type "Outbound", "CC Elite Skill Number", "POM Skill Name" & "Skill Type" are mandatory.

CC Elite Skill Number	POM Skill Name	Skill Type	Parameter to Monitor for Blending	EWT levels	Agent Acq Threshold
<input style="width: 40px;" type="text" value="10"/>	<input style="width: 90%; border: 1px solid blue;" type="text" value="Outbound"/>	<span style="border: 1px solid gray; padding: 2px;">Outbound</span> ▼	<span style="border: 1px solid gray; padding: 2px;">Select only for Inbound</span> ▼	<div style="border: 1px solid gray; padding: 2px; font-size: x-small;">           Select only for EWT            Expected Wait Time(High)            Expected Wait Time(Medium)            Expected Wait Time(Low)         </div>	<input style="width: 40px;" type="text" value="0"/>

## 6.4. Display the POM Campaigns

Navigate to **Campaigns** → **Campaign Manager** from the main window, as shown.



**Note:** It is assumed that the POM campaigns are already set up and running prior to the connection from TMAC. The setup and configuration of the POM Campaign including the Strategies and Contact Lists are outside the scope of these Application Notes. However, an example of the Preview Strategy and Contact List are included in the **Appendix** of these Application Notes, **Section 11**.

The following campaigns were setup for compliance testing.

- **Preview** – this is an outbound campaign that allows the agent to make the outbound call by presenting the call information to the agent desktop and allowing the agent click on “preview dial” (see **Section 11.3**).
- **Progressive** – this is an outbound campaign that makes the call first and then presents the call information to the agent desktop this forces the call to the agent.

Name	Contact List - Filter Template	Type	Campaign Strategy	Last Executed	Waiti...
Preview	OnetoPSTN - None	Finite	Preview	2/15/2024 11:58:54 AM	0
Preview2	OnetoPSTN - None	Finite	Preview	2/15/2024 11:56:01 AM	0
Progressive	OnetoPSTN - None	Finite	Progressive	2/15/2024 10:54:11 AM	0

Each campaign can be started by clicking on the play icon highlighted below. The example below shows the **Progressive** campaign being started.

Campaign Manager ?

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

[New Campaign](#)    

Name	Contact List - Filter Template	Ty...	Campaign Stra...	Last Executed	Wait...
 <a href="#">Preview</a>	OnetoPSTN - None	Finite	<a href="#">Preview</a>	2/15/2024 11:58:54...	0
 <a href="#">Preview2</a>	OnetoPSTN - None	Finite	<a href="#">Preview</a>	2/15/2024 11:56:01...	0
 <a href="#">Progressive</a>	OnetoPSTN - None	Finite	<a href="#">Progressive</a>	2/15/2024 10:54:11...	0

- Edit
- Run Now
- Schedule
- Campaign Summary
- Rule Association
- Holiday Association
- Campaign Linking
- Save As
- Export Files
- Delete

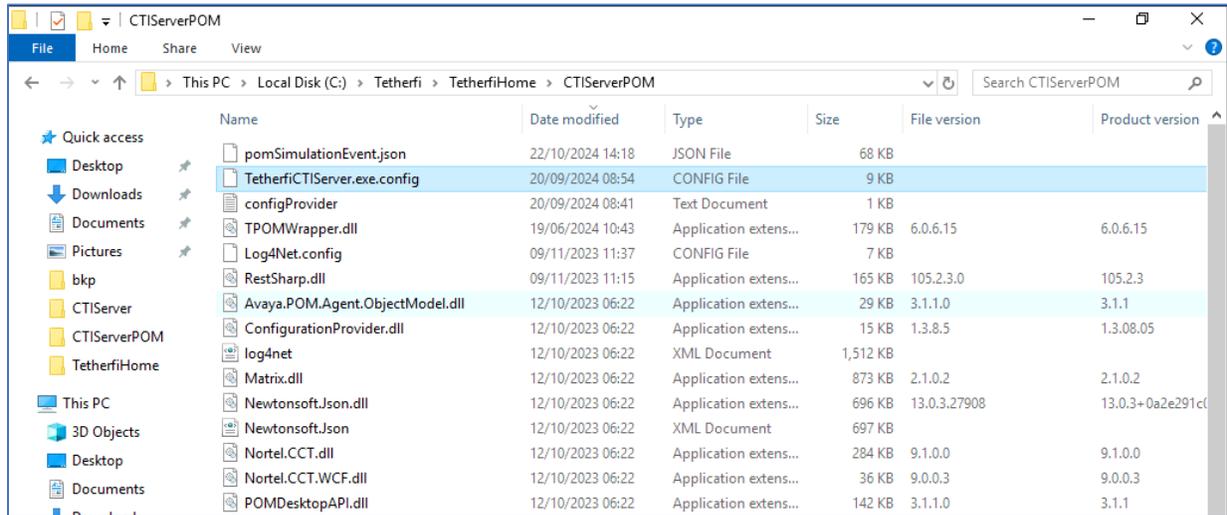
1-3    Show:  

## 7. Configure Tetherfi Multimedia Agent Client

This section provides the procedures for configuring Multimedia Agent Client. The following connections to POM must be configured on Multimedia Agent Client, as well as the Users/Agents on OCM. A connection to Avaya Aura® Application Enablement Services is required for this solution to work. The details of this connection are contained in the *Application Notes for Tetherfi Multimedia Agent Client with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services*.

### 7.1. Configure Tetherfi CTI Server to Connect to POM API

Open the **TetherfiCTIServer.exe.config** file located as shown below.



The highlighted sections below are relevant to the connection to POM API from Tetherfi CTI Server, which enables reading/sending events between the two, to manage POM outbound calls on TMAC/Agent Desktop.

```

TetherfiCTIServer.exe.config
53 <!-- POM Configuration Parameters -->
54 <add key="POMServerIP" value="10.10.40.25" />
55
56 <!--POM Auxiliary server ip means secondary-->
57 <add key="POMAuxServerIP" value="" />
58 <add key="EnablePOMHA" value="" />
59
60 <!-- POM Auxiliary server ip means secondary -->
61 <add key="POMAuxServerPort" value="" />
62 <add key="POMServerPort" value="9971" />
63 <add key="POMAgentPassword" value=
"IRzTbUyN0EszYRjSpTgVqud3eRziunA3LSYCWORv5kDWX1wX2vYbGPZ436dbonNTcxXRjrKZE
lyOpiW3abyMg==" />
64 <add key="POMLocale" value="en-US" />
65 <add key="POMTimeZone" value="GMT + 5.30" />
66 <add key="POMZoneName" value="Default" />
67 <add key="POMOrgName" value="Default" />
68 <add key="EnablePOMIntegration" value="true" />
69 <add key="EnablePOMSecureIntegration" value="true" />
70 <!--default POMVersion is v2 to use v* type v* in POMVersion-->
71 <add key="POMVersion" value="v4" />
72 <!--in minutes-->
73 <add key="CampaignStatusPollInterval" value="" />
74
75 <!--RestClient integration parameters-->
76 <add key="InterpreterSecurityProtocolType" value="tls" />
77 <add key="InterpreterCertificateFolder" value="C:\Certs\CTI\" />

```

Note the **POMServerRestUserName** and **Password** must match that configured in **Section 6.1**.

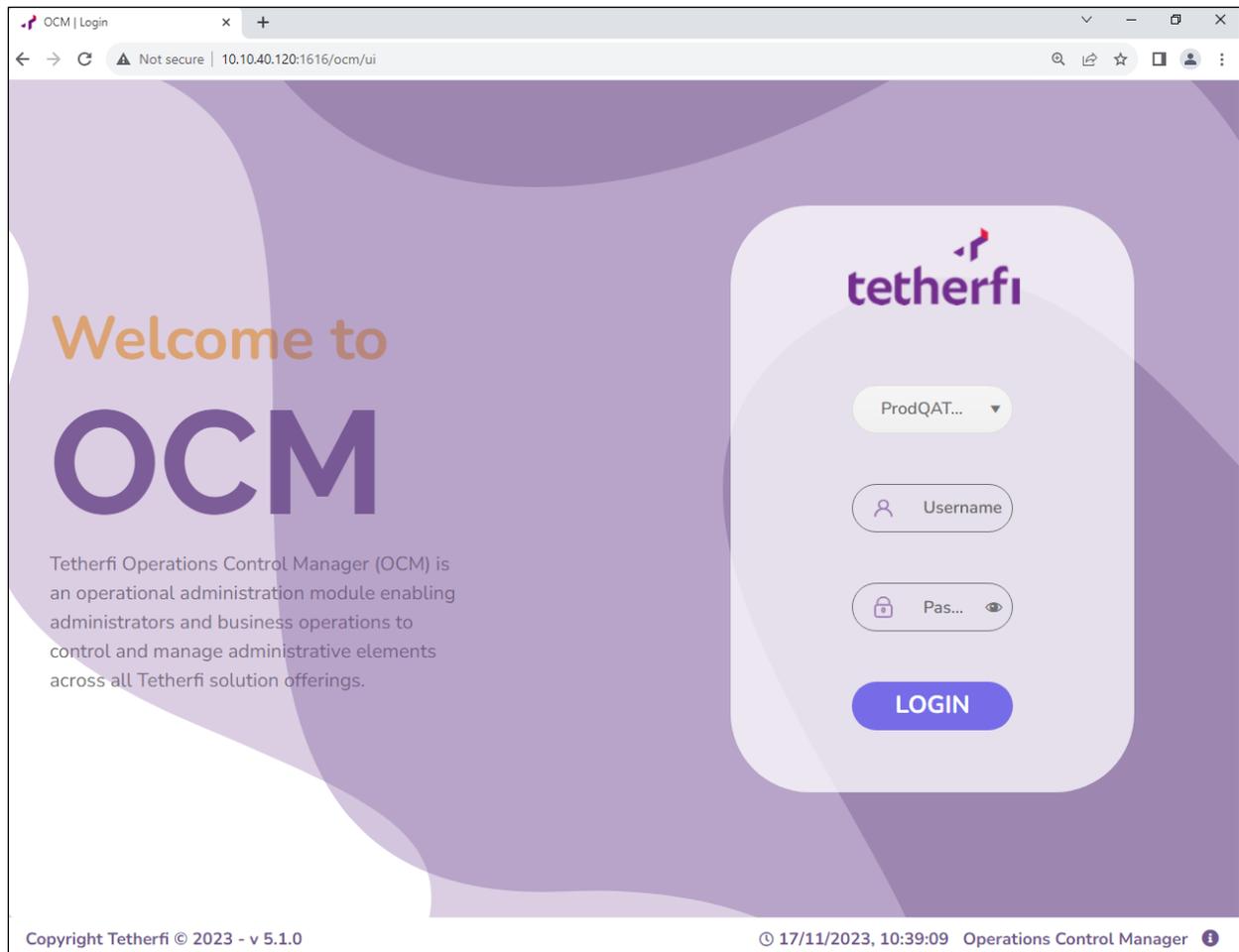
```

TetherfiCTIServer.exe.config
"IRzTbUyN0EszYRjSpTgVqud3eRziunA3LSYCWORv5kDWX1wX2vYbGPZ436dbonNTcxXRjrKZE
SlyOpiW3abyMg==" />
64 <add key="POMLocale" value="en-US" />
65 <add key="POMTimeZone" value="GMT + 5.30" />
66 <add key="POMZoneName" value="Default" />
67 <add key="POMOrgName" value="Default" />
68 <add key="EnablePOMIntegration" value="true" />
69 <add key="EnablePOMSecureIntegration" value="true" />
70 <!--default POMVersion is v2 to use v* type v* in POMVersion-->
71 <add key="POMVersion" value="v4" />
72 <!--in minutes-->
73 <add key="CampaignStatusPollInterval" value="" />
74
75 <!--RestClient integration parameters-->
76 <add key="InterpreterSecurityProtocolType" value="tls" />
77 <add key="InterpreterCertificateFolder" value="C:\Certs\CTI\" />
78 <add key="EnableRESTAPIIntegrationWithPOM" value="true" />
79 <add key="EnableRESTAPISecureIntegration" value="true" />
80 <add key="POMServerRESTURL" value="https://10.10.40.25" />
81 <add key="POMServerRESTUserName" value="WebServices" />
82 <add key="POMServerRESTPassword" value="Avaya123$" />
83 <add key="POMServerCustomRESTURL" value="https://10.10.40.25" />
84 <add key="POMCallbackDashboardURL" value=
"http://localhost:17000/TetherfiPOMCallbackDashboard" />
85
86 <add key="EnableAACCIntegration" value="" />

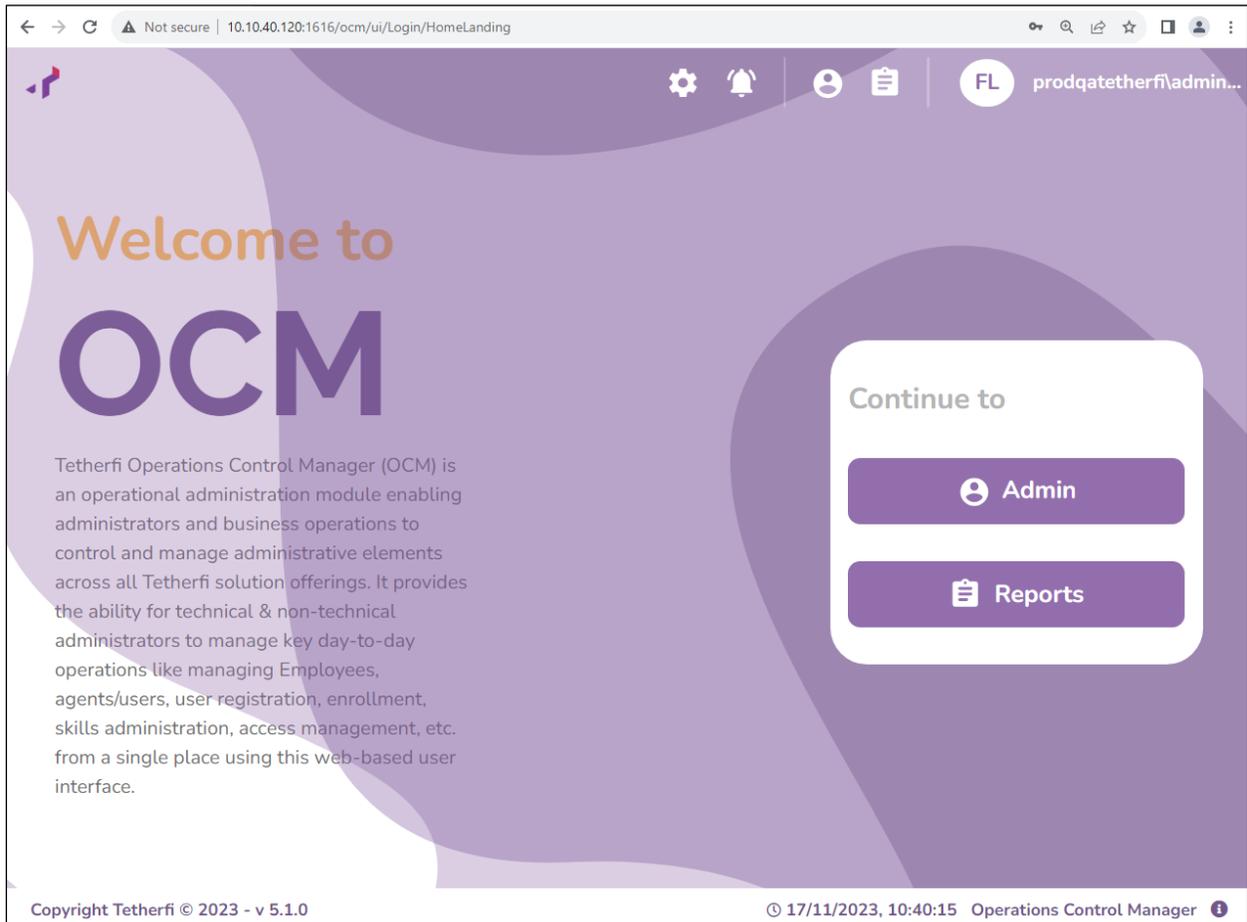
```

## 7.2. Configure the Users/Agents on Tetherfi Operations Control Manager

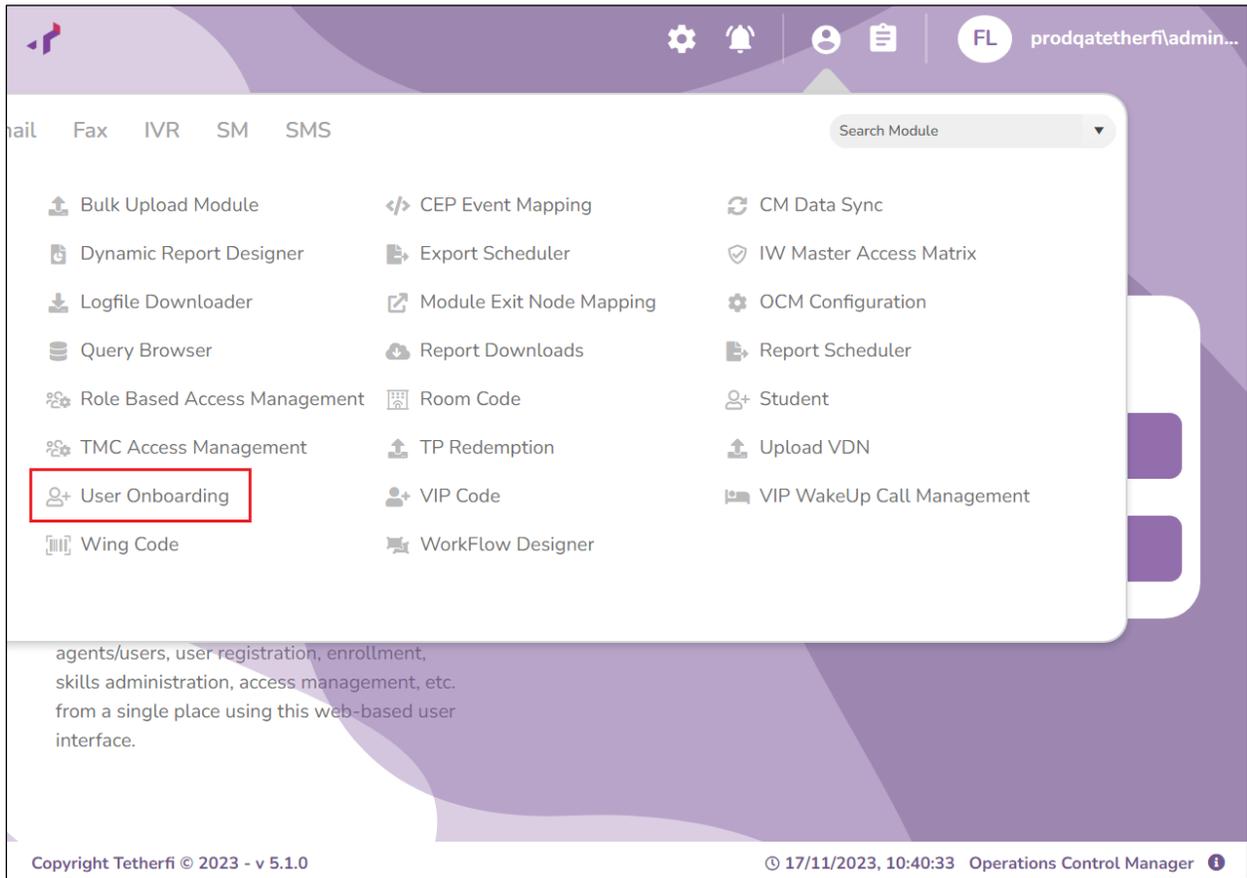
Open the Tetherfi Operations Control Manager (OCM) by opening a browser session to the <server IP address>:1616/ocm/ui, as shown.



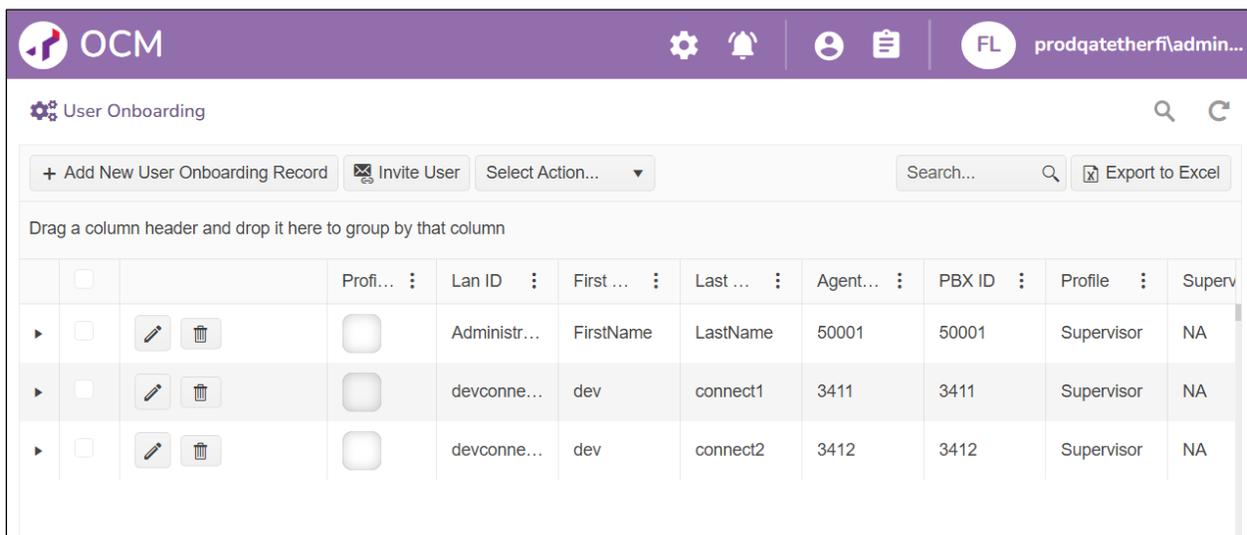
Once logged in, click on **Admin**.



Select **User Onboarding** as highlighted below.



The following users were created for DevConnect testing. However, to create a new user, click on + **Add New User Onboarding Record**.



The following screen shows the information for the existing user **devconnect1** which is associated with Communication Manager Elite agent **3411**, as per **Section 5.1.2**. The same screen would be present for a new user where the information added should resemble something like shown below. The **Lan ID** may be used to match up with a local LDAP server and this is then associated with both the **Agent ID** and **PBX ID** which should be that of the Communication Manager Elite agent. Click on **Next** to continue.

The screenshot shows a 'User Onboarding' window with a sidebar on the left containing icons for: Personal Info, Profile Picture, Secondary Profil..., Channel Count, Features, Role Mapping, Access Role, and Miscellaneous. The main area contains the following fields:

<b>Lan ID*</b>	devconnect1	<b>First Name*</b>	dev
<b>Last Name*</b>	connect1	<b>Agent ID*</b>	3411
<b>PBX ID*</b>	3411	<b>Org. Unit*</b>	Tet... x ▼
<b>Profile*</b>	Superv... ▼	<b>Superviso</b>	NA ▼
<b>Is Active*</b>	<input checked="" type="checkbox"/>		

At the bottom of the window, it says 'Step 1 of 8' and has a purple 'Next' button.

Clicking **Next** until the **Channel Count** tab appears, where the types of channels are associated with the agent. For compliance testing, only **Voice** was used and so this was ticked, and two channels were associated to this agent. Click on **Next** again to move on.

**User Onboarding** [Close]

- Personal Info
- Profile Picture
- Secondary Profil...
- Channel Count**
- Features
- Role Mapping
- Access Role
- Miscellaneous

Step 4 of 8

**Voice**       **Text Chat**  
 2      0

**Audio Chat**       **Video Chat**  
 0      0

**Fax**       **SMS**  
 0      0

**Email Channel**  
 0

Previous Next

The **Features** are added here. These are the features that were ticked for compliance testing.

**User Onboarding** [Close]

- Personal Info
- Profile Picture
- Secondary Profil...
- Channel Count
- Features**
- Role Mapping
- Access Role
- Miscellaneous

Step 5 of 8

Allow Supervisor to CapturePicture       Allow Supervisor to interaction notification  
 Enter Feature Value      Enter Feature Value

Allow Supervisor to logout       Allow Supervisor to send notification  
 Enter Feature Value      Enter Feature Value

Auto Answer All ACD Calls       Go ACW After Each ACD Calls  
 Enter Feature Value      Enter Feature Value

Go ACW After Any Calls       Text Chat Auto Answer  
 Enter Feature Value      Enter Feature Value

Text Chat Auto ACW Enabled       TRS POPUP PROGRAM GAMIFICATION TRACK  
 Enter Feature Value

Previous Next

Click on Next to fill in any other information that may need to be added. Once everything is configured as required, click on **Save** at the bottom of the screen.

The screenshot shows a 'User Onboarding' configuration window with a close button (X) in the top right corner. On the left side, there is a vertical navigation menu with icons and labels for: Profile Picture, Secondary Profil..., Channel Count, Features, Role Mapping, Access Role, and Miscellaneous. The 'Miscellaneous' step is currently selected. At the top of the main content area, there are two dropdown menus: 'CRM Name' and 'Text Template', both with 'Select' as the current value. Below the navigation menu, the text 'Step 8 of 8' is displayed. A 'Previous' button is located to the right of 'Step 8 of 8'. Below that, there is a label 'Modify Reason\*' followed by an empty text input field. At the bottom right of the window, there are two buttons: a purple 'Save' button with a checkmark icon and a red 'Cancel' button with a close icon.

## 8. Verification Steps

This section verifies the configuration of Avaya Proactive Outreach Manager and Tenterfi Multimedia Agent Client.

### 8.1. Verify Avaya Proactive Outreach Manager is Running

The status of the POM server can be checked from an SSH session to the POM server using something like PuTTY. Open a connection to Experience Portal/POM server and then ensure that the user “root” is used by typing **su – root** (not shown). Type **POM status** and verify that all POM services are **RUNNING**, as shown below.

```
root@ep810:~  
Using keyboard-interactive authentication.  
Password:  
Last login: Mon Oct 21 12:37:52 2024 from 10.10.40.240  
bash: /home/cust/epm-motd.sh: No such file or directory  
[cust@ep810 ~]$ su - root  
Password:  
Last login: Mon Oct 21 12:39:58 IST 2024 on pts/0  
bash: /home/cust/epm-motd.sh: No such file or directory  
[root@ep810 ~]# POM status  
Checking POM <version POM.04.00.02.02.01.231116> Status at Thu Oct 24 14:56:54 IST 2024  
Checking individual components:  
STATE=RUNNING  
POM Cache( pid 4470 ) is running...  
  
STATE=RUNNING  
zookeeper ( pid 1842 ) is running...  
  
STATE=RUNNING  
kafka ( pid 3791 ) is running...  
  
STATE=RUNNING  
POM ActiveMQ ( pid 3452 ) is running...  
  
STATE=RUNNING  
Agent Manager ( pid 4892 ) is running...  
  
STATE=RUNNING  
Campaign Manager ( pid 4887 ) is running...  
  
STATE=RUNNING  
Campaign Director ( pid 5088 ) is running...  
  
STATE=RUNNING  
Rule Engine ( pid 4917 ) is running...  
  
STATE=RUNNING  
advance list mgmt ( pid 4404 ) is running...  
  
STATE=RUNNING  
POM agent sdk ( pid 4468 ) is running...  
  
STATE=RUNNING  
POM Dashboard ( pid 5962 ) is running...  
  
Overall Status: POM is running  
[root@ep810 ~]#
```

## 8.2. Verify Avaya Proactive Outreach Manager Campaign

Log into POM as per **Section 6**. Navigate to **Proactive Outreach → Dashboard** in the left column as shown below. Information on any campaign that is running and the agents that are logged in are shown in the main window. The example below shows that a campaign called **Preview2** has a **Status** shown as **Running** and two agents, **3411** and **3412**, logged in with 3411 **Busy** on a **Preview** call.

The screenshot shows the Avaya Experience Portal 8.1.2 (ExperiencePortal) interface. The left sidebar contains a navigation menu with categories like User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration. The 'Proactive Outreach' section is expanded, and 'Dashboard' is selected. The main content area is titled 'Proactive Outreach Dashboard' and features a breadcrumb trail: 'Active campaigns', 'Staffed agents', 'Imports', 'License summary', and 'Inbound skills'. There are two main data tables:

Active campaigns (1)			
Campaign Na...	Job Status	Percent Com...	Filtered Cont...
Preview2	Running	0.0	1

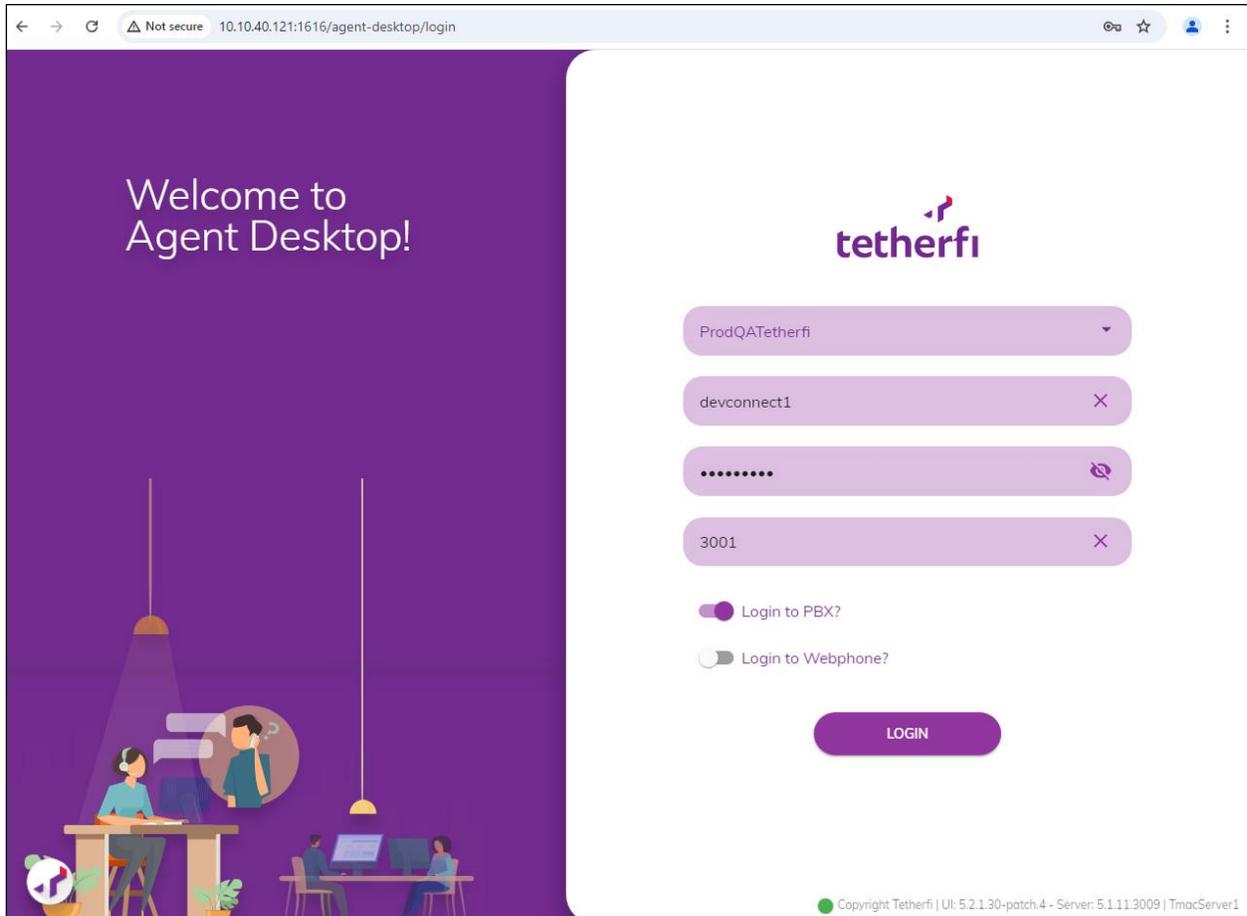
  

Staffed agents (2)			
Agent ID	Agent Name	Agent State	Call State
3411	Workspaces Agt 1	Busy	Preview
3412	Workspaces Agt 2	Not Ready - Sys...	Idle

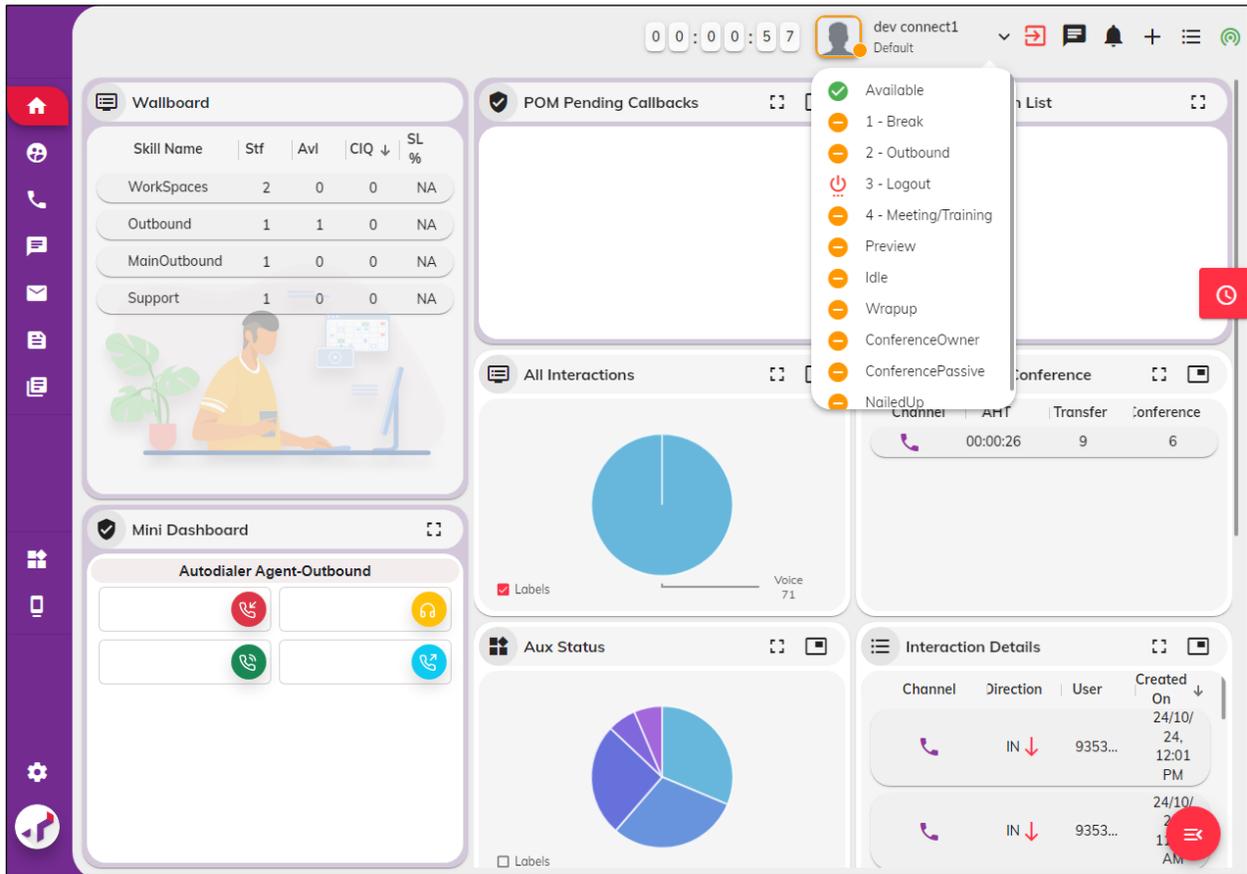
At the bottom of the dashboard, there are pagination controls for both tables, showing page 1 of 1 and 1 of 2 respectively, and a 'Show 10' dropdown menu.

### 8.3. Verify Tetherfi Multimedia Agent Client

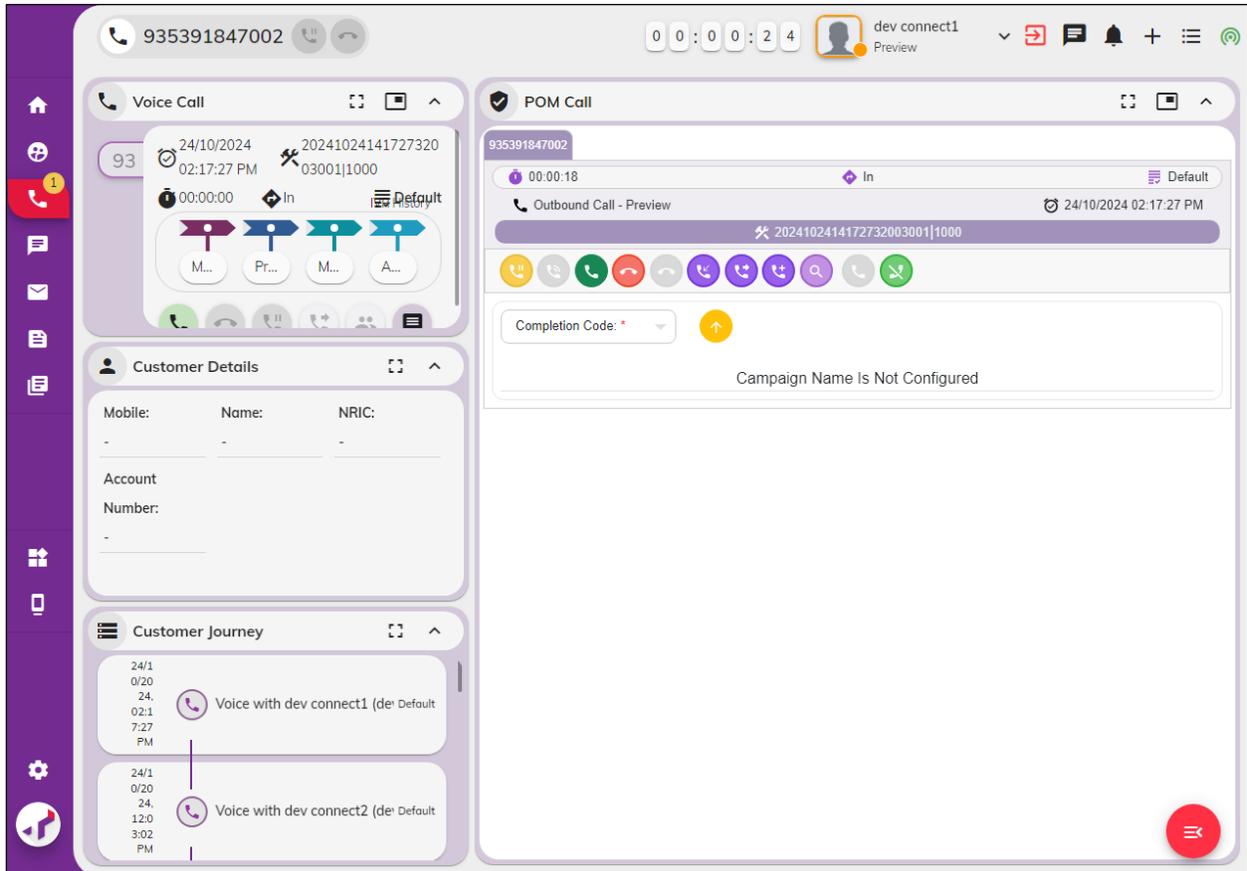
Open a browser session to **http://<serverIP:1616/agent-desktop/login** and enter the appropriate credentials. The example below shows that **devconnect1** will be logging into extension **3001**.



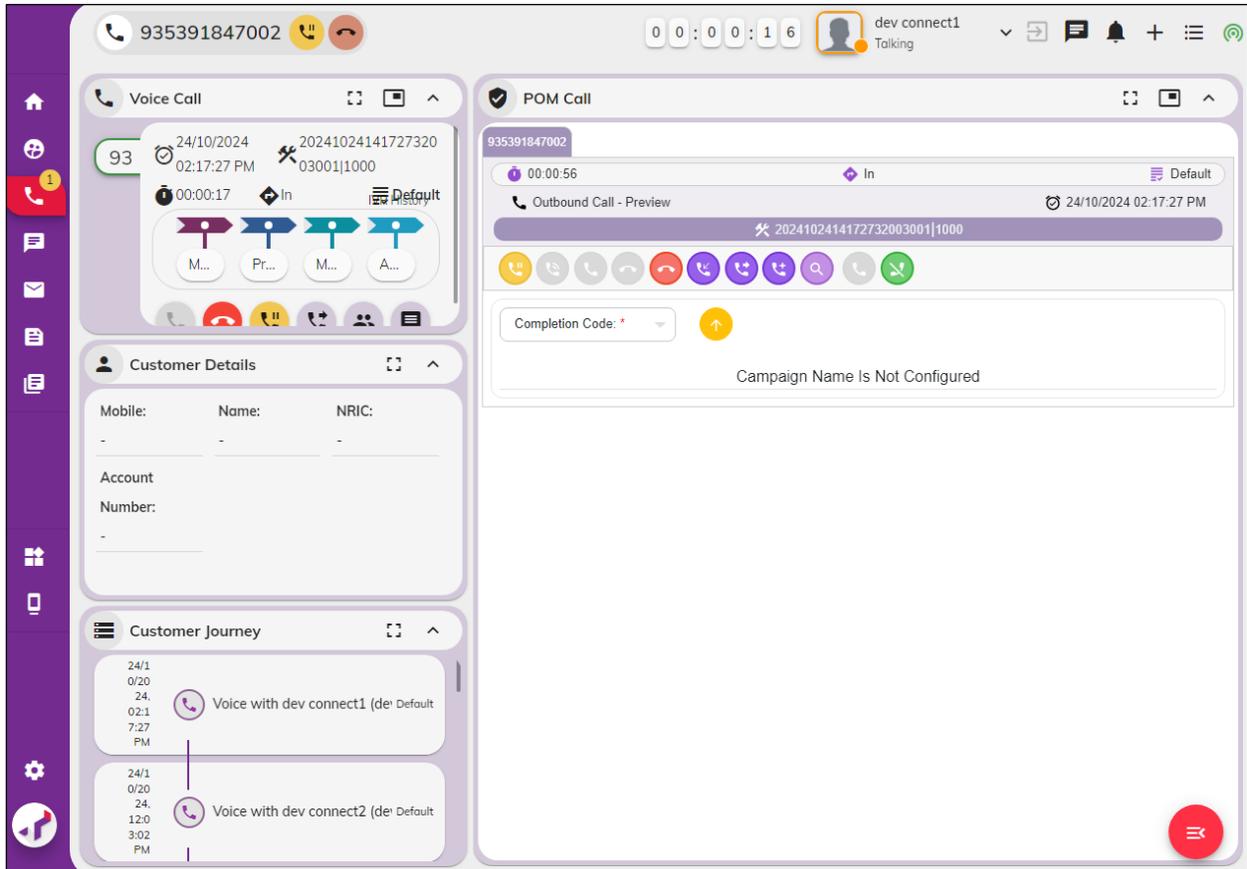
Once logged in, the agent can be made **Available**, as shown.



A **Preview** call is then presented to the agent. The **POM Call** widget is called upon and the telephony functions can be seen on the main window. At this point, the agent can dial out to the suggested number, **35391847002**.

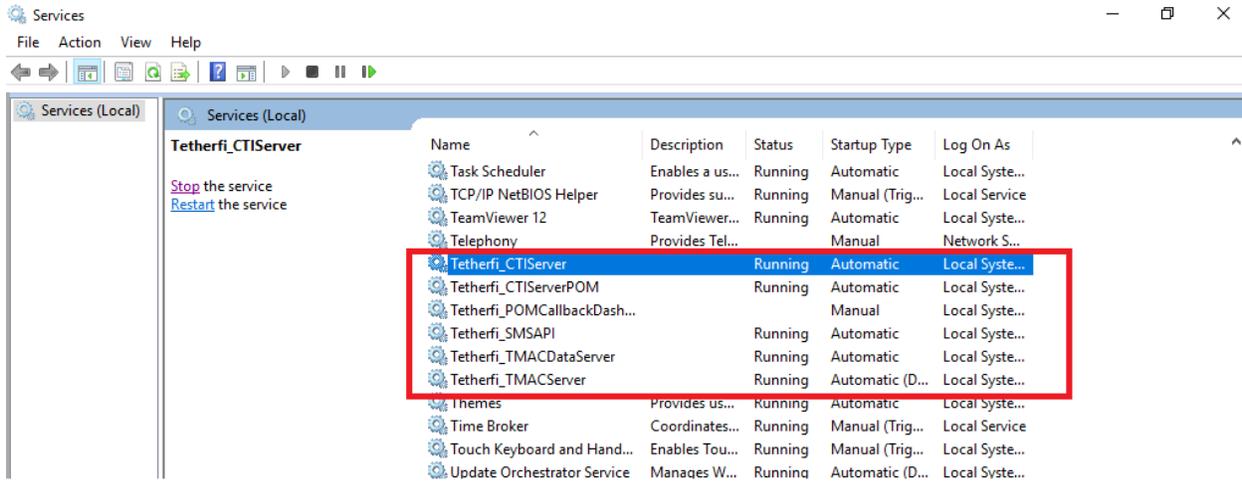


Once the outbound call has been established the agent can hold, transfer and conference the call with another agent or another extension. The telephony functions are shown on the main **POM Call Widget**.



## 8.4. Verify Tetherfi Services are Running

From the TMAC server, check on the Tetherfi\_\* services that are running. Note the following were running for compliance testing, for the connection to POM.



## 9. Conclusion

These Application Notes describe the compliance testing of Tetherfi Multimedia Agent Client to interoperate with Avaya Proactive Outreach Manager, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the Agent Desktop Application Programming Interface on Proactive Outreach Manager. All test cases were executed successfully with observations noted in **Section 2.2**.

## 10. Additional References

This section references the product documentations that are relevant to these Application Notes.

Product documentation for Avaya products may be found at <https://support.avaya.com>.

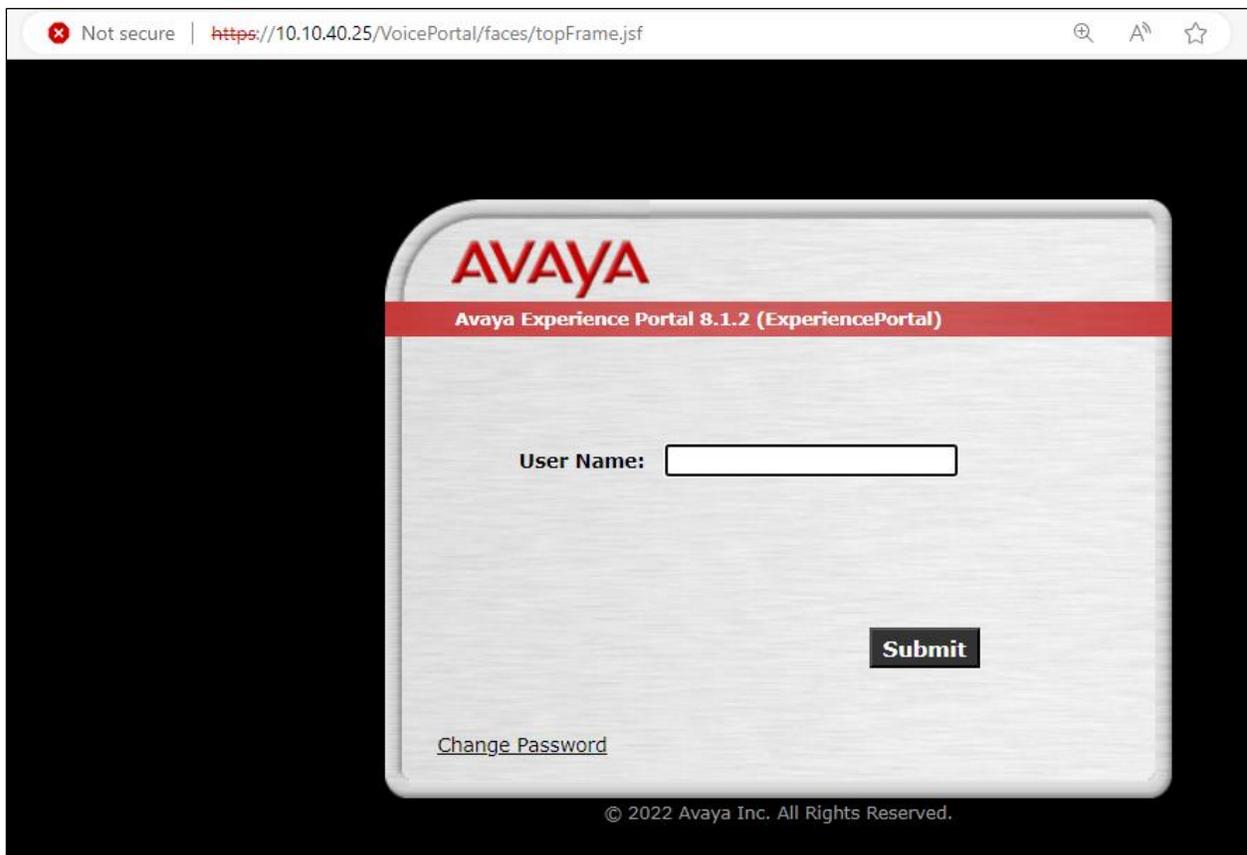
- [1] *Administering Avaya Aura® Communication Manager, Release 10.1.x, Issue 5, March 2023.*
- [2] *Administering Avaya Aura® Application Enablement Services, Release 10.1.x, Issue 6, Feb 2023.*
- [3] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 10.1.x, Issue 8, March 2023.*
- [4] *Administering Avaya Aura® Session Manager, Release 10.1.x Issue 5, Feb 2023.*
- [5] *Application Notes for Tetherfi Multimedia Agent Client with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services*

Product documentation for Multimedia Agent Client can be found by contacting Tetherfi as per **Section 2.3**.

## 11. Avaya Proactive Outreach Manager Outbound Campaign and Components

This section contains information on the Contact List, Completion data, 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.

POM is configured via the Experience Portal Manager (EPM) web interface. To access the web interface, enter **https://[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.



Navigate to **Protective Outreach** → **Manager** in the left panel shown below (bottom of screenshot).

**Avaya Experience Portal 8.1.2 (ExperiencePortal)**  
Expand All | Collapse All

- ▼ **User Management**
  - Roles
  - Users
  - Login Options
- ▼ **Real-time Monitoring**
  - System Monitor
  - Active Calls
  - Port Distribution
- ▼ **System Maintenance**
  - Audit Log Viewer
  - Trace Viewer
  - Log Viewer
  - Alarm Manager
- ▼ **System Management**
  - Application Server
  - EPM Manager
  - MPP Manager
  - Software Upgrade
  - System Backup
- ▼ **System Configuration**
  - Applications
  - EPM Servers
  - MPP Servers
  - SNMP
  - Speech Servers
  - VoIP Connections
  - Zones
- ▼ **Security**
  - Certificates
  - Licensing
- ▼ **Reports**
  - Standard
  - Custom
  - Scheduled
- ▼ **Multi-Media Configuration**
  - Email
  - HTML
  - SMS
- ▼ **Proactive Outreach**
  - Manager
  - Monitor
  - Dashboard

You are here: Home

## Avaya Experience Portal Manager

Avaya Experience Portal Manager (EPM) is the consolidated Experience Portal. Through the EPM interface you can configure Experience Portal component, and generate reports related to the component.

### Installed Components

**Media Processing Platform**  
Media Processing Platform (MPP) is an Avaya media processing (or CCXML) application on an application server. It then connects to the Avaya Experience Portal.

**Email Service**  
Email Service is an Experience Portal feature which provides email-based services for mobile devices.

**HTML Service**  
HTML Service is an Experience Portal feature which supports HTML-based services for mobile devices.

**Proactive Outreach Manager**  
Avaya Proactive Outreach Manager (POM) provides a solution for proactive outreach capability to communicate through different channels of interaction such as voice, text, and email.

**SMS Service**  
SMS Service is an Experience Portal feature which provides SMS-based services for mobile devices.

### Legal Notice

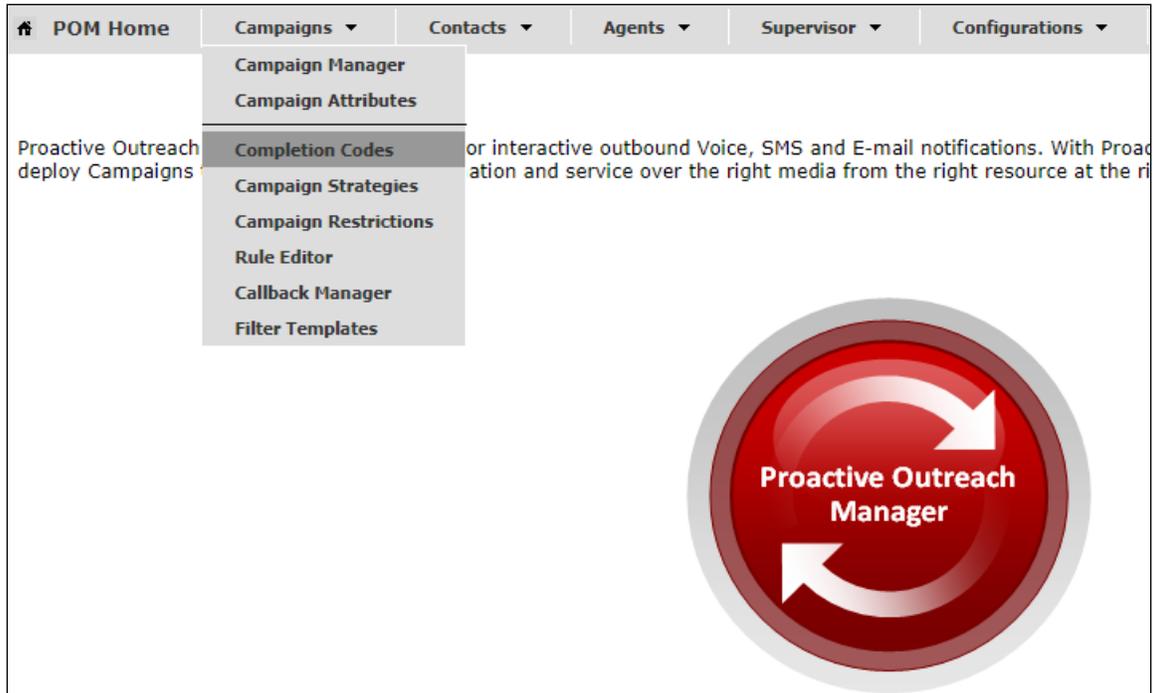
AVAYA GLOBAL SOFTWARE LICENSE TERMS

## 11.1. Preview Campaign Strategy

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

### 11.1.1. 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** shown below.

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

[Advanced](#)

Show  | Page: 1/1

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

### Edit Completion Code

This page allows you to modify Completion Codes.

Name	Sale
Description	<input type="text"/>
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**

### 11.1.2. Campaign Strategy

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



The Campaign Strategies are shown 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    Go  

Name	State	Task Types	Action
<a href="#">Preview</a>	Completed	 	   
<a href="#">Progressive</a>	Completed	 	   

Add
Import
Help

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](https://10.10.40.30/VP_POM/faces/admin/ContactStrategy.xhtml)

HIDE TOOL BOX SHOW SOURCE SAVE SAVE DRAFT COPY PASTE DELETE HELP

<p style="font-size: x-small;">Selected Node: Task</p> <ul style="list-style-type: none"> <li> Restrictions</li> <li> Address</li> <li> Sender's Address</li> <li> Result Processors</li> </ul>	<p style="font-size: x-small;">Campaign Strategy: Preview</p> <ul style="list-style-type: none"> <li> Campaign Strategy <ul style="list-style-type: none"> <li> Handler (initial) <ul style="list-style-type: none"> <li style="background-color: #add8e6;"> Preview <ul style="list-style-type: none"> <li> Address</li> <li> Result Processors <ul style="list-style-type: none"> <li> Result (Call Answered) <ul style="list-style-type: none"> <li> Agent</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>	<table border="1" style="width: 100%; border-collapse: collapse; font-size: x-small;"> <thead> <tr> <th style="text-align: left;">Property</th> <th style="text-align: left;">Value</th> </tr> </thead> <tbody> <tr><td>Name</td><td>Preview</td></tr> <tr><td>Description</td><td></td></tr> <tr><td>Sender's Display Name</td><td>DevConnect</td></tr> <tr><td>Sender's Address</td><td>sip:9876@devconnect.local</td></tr> <tr><td>Timeout (sec)</td><td></td></tr> <tr><td>Guard Times</td><td>Disable</td></tr> <tr><td>Min Contact Time</td><td></td></tr> <tr><td>Max Contact Time</td><td></td></tr> <tr><td>Re-check Interval (min)</td><td></td></tr> <tr><td>On Media Server Failure</td><td>retry</td></tr> <tr><td>Priority</td><td>5</td></tr> <tr><td>Allocation Type</td><td>Dynamic</td></tr> <tr style="background-color: #add8e6;"><td colspan="2"><b>CCA Parameters</b></td></tr> <tr><td>Enhanced CCA</td><td>OFF</td></tr> <tr><td>Background AMD</td><td></td></tr> <tr><td>Action on AMD</td><td>None</td></tr> <tr><td>Silence Call Detection (SCD)</td><td>OFF</td></tr> <tr style="background-color: #add8e6;"><td colspan="2"><b>APPLICATIONS</b></td></tr> <tr><td><b>Driver Application</b></td><td>PomDriverApp</td></tr> <tr><td>Nailer Application</td><td>Nailer</td></tr> <tr><td>Nuisance Call Application</td><td>AvayaPOMAnnouncement</td></tr> <tr><td>On Hold Application</td><td>AvayaPOMAnnouncement</td></tr> <tr style="background-color: #add8e6;"><td colspan="2"><b>PACING PARAMETERS</b></td></tr> <tr><td>Call Pacing Type</td><td>Preview</td></tr> <tr><td><b>Timed Preview</b></td><td>No</td></tr> <tr><td>Preview Time (Sec)</td><td></td></tr> <tr><td>Can Cancel Preview</td><td>Disable</td></tr> <tr><td><b>Min. Agents</b></td><td>1</td></tr> </tbody> </table>	Property	Value	Name	Preview	Description		Sender's Display Name	DevConnect	Sender's Address	sip: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	<b>CCA Parameters</b>		Enhanced CCA	OFF	Background AMD		Action on AMD	None	Silence Call Detection (SCD)	OFF	<b>APPLICATIONS</b>		<b>Driver Application</b>	PomDriverApp	Nailer Application	Nailer	Nuisance Call Application	AvayaPOMAnnouncement	On Hold Application	AvayaPOMAnnouncement	<b>PACING PARAMETERS</b>		Call Pacing Type	Preview	<b>Timed Preview</b>	No	Preview Time (Sec)		Can Cancel Preview	Disable	<b>Min. Agents</b>	1
Property	Value																																																											
Name	Preview																																																											
Description																																																												
Sender's Display Name	DevConnect																																																											
Sender's Address	sip: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																																																											
<b>CCA Parameters</b>																																																												
Enhanced CCA	OFF																																																											
Background AMD																																																												
Action on AMD	None																																																											
Silence Call Detection (SCD)	OFF																																																											
<b>APPLICATIONS</b>																																																												
<b>Driver Application</b>	PomDriverApp																																																											
Nailer Application	Nailer																																																											
Nuisance Call Application	AvayaPOMAnnouncement																																																											
On Hold Application	AvayaPOMAnnouncement																																																											
<b>PACING PARAMETERS</b>																																																												
Call Pacing Type	Preview																																																											
<b>Timed Preview</b>	No																																																											
Preview Time (Sec)																																																												
Can Cancel Preview	Disable																																																											
<b>Min. Agents</b>	1																																																											

Scrolling down from the screen on the previous page shows the **Default Completion code** and here the Completion Code created in **Section 11.1.1** can be added. The **Applications** located on Experience Portal are also added here under **APPLICATIONS**.

The screenshot displays the 'Campaign Strategy: Preview' configuration interface. On the left, a tree view shows the hierarchy: Campaign Strategy > Handler (initial) > Preview > Address > Result Processors > Result (Call Answered) > Agent. On the right, a table lists various parameters and their values.

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

## 11.2. 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 **OnetoPSTN**. Details of this Contact List can be viewed by clicking on the Contact List Name. A new Contact List can be added by clicking on **New Contact List** and uploading the contacts from a file.

Contact List Na...	Zone ...	Total ...	Availa...	Exclude...	Last Updated
⋮ OnetoPSTN	Default	1	1	0	3/2/2023 2:56:1...

The **Contact List** consists of a number of modules or sections which are arranged in the form of tabs across the top. These being **Details**, **Data Source**, **Attributes**, **Contacts** and **Excluded Contacts**. The **Contacts** tab was selected and the contact list can be amended or viewed by right-clicking on the three dots to the left of the **System Contact ID** and selecting **Edit**.

System Con...	ID	First Name	Last Name	Phone 1	Phone 1 Co...
⋮ 1	1	Paul	Greaney	935391847001	1

The **Contact List** shown has one entry in it calling to **935391847001**.

Contact List / Contacts / 1 ?

OnetoPSTN

Predefined Attributes

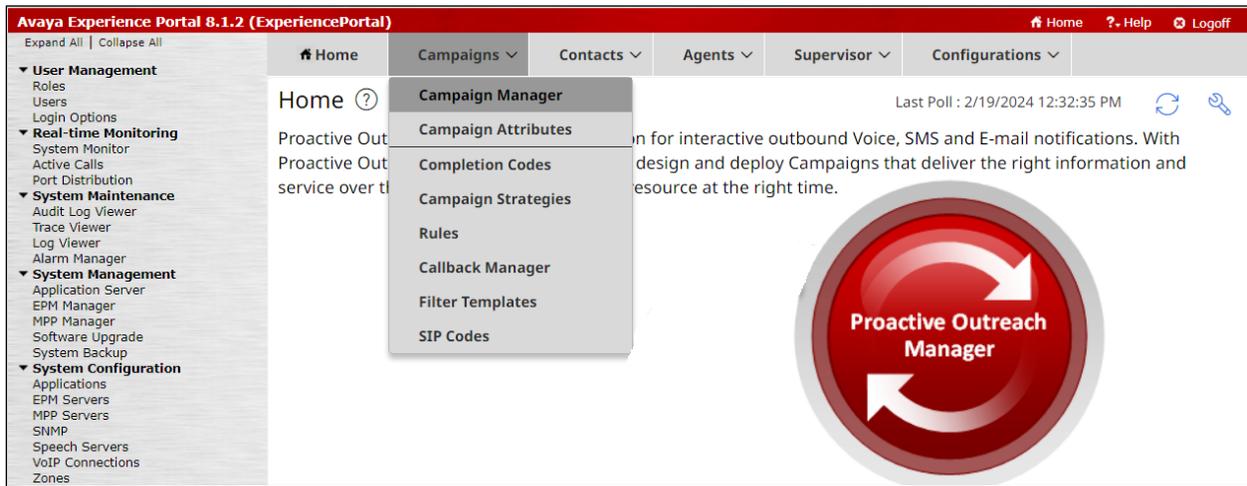
ID	First Name	Last Name
1	Paul	Greaney
E-Mail	Country Predefined	Zipcode Predefined
paul@gmail.com	Ireland	H91 XXXX
Zipcode Time Zone Predefined	Zipcode State Predefined	Address Line 5 Predefined
		Galway
Address Line 4 Predefined	Title Predefined	
Oranmore	Mr.	

Phone Attributes

Phone 1	Phone 1 Country Code	Time Zone
935391847001	1	Europe/Dublin
Phone 1 State	Phone 1 Wireless	Phone 2
		935391847001

### 11.3. Preview Campaign

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



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

Campaign Manager ?

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

[New Campaign](#)  Filter Refresh Dropdown

Name	Contact List - Filter Template	Type	Campaign Strategy	Last Executed	Waiti...
<a href="#">Preview</a>	OnetoPSTN - None	Finite	<a href="#">Preview</a>	2/15/2024 11:58:54 AM	0
<a href="#">Preview2</a>	OnetoPSTN - None	Finite	<a href="#">Preview</a>	2/15/2024 11:56:01 AM	0
<a href="#">Progressive</a>	OnetoPSTN - None	Finite	<a href="#">Progressive</a>	2/15/2024 10:54:11 AM	0

Clicking on the **Preview Campaign** (from the previous page), opens the campaign as shown. The campaign can be viewed by scrolling down through the various configurations or by selecting the various tabs at the top of the screen shown below.

The screenshot displays the 'Campaign Manager / Preview' interface. At the top, there are 'Cancel' and 'Save' buttons. Below them is a horizontal tab bar with the following tabs: 'Details' (selected), 'Campaign', 'Contacts', 'Completion Codes', 'Completion Processing', 'Media', and 'Add'. The 'Details' tab is active, showing a 'Campaign Information' section with three input fields: 'Name \*' (containing 'Preview'), 'Campaign Name', and 'Description' (containing 'Campaign Description'). A vertical scrollbar is visible on the right side of the form area.

The **Campaign Strategy** that was shown in **Section 11.1.2** is entered at the top of the screen below. The **Skill Configuration** is set here, as well as the **DNC Configuration**. Scrolling down or clicking on the tabs at the top of the screen will show further configuration of this campaign.

Campaign Manager / Preview ? Cancel Save

Details **Campaign** Contacts Completion Codes Completion Processing Media Additional Parameter

Campaign Strategy Configuration

Select Campaign Strategy \*

Preview Refresh View Strategy

Select a Campaign Strategy from the list to be used in the Campaign

---

Campaign Type Configuration

Campaign Type \*

Finite  Infinite

---

ANI Configuration

Sender's Display Name Sender's Address

Provide Sender's Display Name which will be used for this campaign Provide Sender's Address which will be used for this campaign

---

Skill Configuration

Select Skill

Outbound ?

Select a skill from the list to assign to this campaign

---

DNC Configuration

Apply DNC Group

The **Contact List** displayed in **Section 11.2** is associated with this campaign.

The screenshot displays the 'Campaign Manager / Preview' interface. At the top, there are tabs for 'Details', 'Campaign', 'Contacts' (which is selected), 'Completion Codes', 'Completion Processing', 'Media', and 'Add'. Below the tabs, the 'Contacts' section is titled 'Contact List Configuration'. Under this title, there is a section for 'Contact List and Filter Template Association \*'. This section contains three input fields: 'Contact List \*' with a dropdown menu showing 'OnetoPSTN', 'Filter Template' with a dropdown menu showing 'Select', and 'Dialing Allocation Percentage' with a text input field containing '100'. To the right of these fields are three icons: an eye, a pencil, and a trash can. Below these fields are two buttons: '+ Add New' and 'Save All'. There are also two checkboxes: 'Apply same filter' and 'No Dialing Allocation'. A 'View Contacts' button is located below the checkboxes. At the bottom of this section is a toggle switch labeled 'Pause Dialing During Contact Selection'. Below this section is another section titled 'Contact Assignment to Agent' with two checkboxes: 'Attributes' and 'Agent ID'. At the very bottom of the interface, there is a section titled 'Dialing Order Configuration'.

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.

---

**©2025 Avaya LLC. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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](mailto:devconnect@avaya.com).