



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Tetherfi Multimedia Agent Client 4.0 with Avaya Proactive Outreach Manager 3.1.3 – Issue 1.0

### Abstract

These Application Notes describe the configuration steps to integrate Tetherfi Multimedia Agent Client 4.0 to interoperate with Avaya Proactive Outreach Manager 3.1.3.

Tetherfi Multimedia Agent Client is a web-based CTI solution. This thin client provides a single unified agent desktop capable of servicing Voice, SMS, Email, Chat, Video and Social Media Channels. Tetherfi Multimedia Agent Client communicates with Avaya Proactive Outreach Manager using the Avaya Proactive Outreach Manager Web Services and 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 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 Tetherfi Multimedia Agent Client 4.0 to interoperate with Avaya Proactive Outreach Manager (POM) 3.1.3.

Tetherfi Multimedia Agent Client (TMAC) is a thin client single unified agent desktop capable of servicing Voice, SMS, Email, Chat, Video and Social Media Channels. TMAC integrates to Avaya Application Enablement Services (AES) through Telephony Server Application Programming Interface (TSAPI) for events and call control and through System Management Service (SMS) for dynamic update of wallboard skills list and real-time skill statistics. Contact Center agents login to this desktop to handle all interactions across channels for inbound and outbound. TMAC will login to Avaya AES via TSAPI API and to Avaya POM to get notifications for Nail call /Preview/ Predictive/ Progressive calls via POM Agent Desktop API and POM Web Services. These Application Notes concentrate on the integration of TMAC with Avaya POM.

Configuration of TMAC Agent users' is done from Omni Channel Management (OCM), a web interface that shares the same database with TMAC. OCM is used to perform updates of contacts on POM through POM Web Services and also used to configure below in POM:

- 1- Campaign Start/Stop
- 2- Manual contact upload
- 3- Manual Purging
- 4- Job Linking
- 5- Reports (Extracted from POM Database to OCM)

During the compliance testing, Avaya POM was configured as CC Elite to allow communications with Avaya Aura® Communication Manager and Avaya AES. Avaya POM was installed on Avaya Aura® Experience Portal (AAEP). Outbound calls from POM were routed via a SIP trunk to Avaya Aura® Session Manager. Calls were made with agents using TMAC for control and deskphones for voice.

These Application Notes focus on the integration between TMAC and POM and assume the integration between the TMAC with Avaya AES for screen pop and call control is already in place as documented in reference [5].

## 2. General Test Approach and Test Results

The feature test cases were performed manually. As there are two distinct connections to the Avaya solution, i.e., AES and POM, both connections were tested as part of the compliance testing. The integration between the TMAC with AES is documented in reference [5].

Outbound calls were made using POM and calls handled by agents running the TMAC. For compliance testing, agents were logged in from the respective phones as CC Elite expert agents. The connection to AES was tested by placing incoming calls to various VDN's and which were routed through CC Elite skills and were handled by agents using the TMAC.

Serviceability test cases were also performed by manually disconnecting/reconnecting the ethernet cable on the client PC, POM and AES server, and restarting the POM service on the POM server.

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 the TMAC utilized enabled capabilities of HTTPS for browser.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying TMAC for the following:

AES testing:

- Agents Login and Logout.
- Agent states: Ready, Not Ready and changing Aux Reason code.
- Make/receive phone calls.
- Receive skillset calls.
- Hold/transfer/conference phone calls (incoming calls).

POM testing:

- Agent Login and Logout.
- Agent state: Ready, Not Ready and changing Aux Reason code.
- Nailing the agent and new call notifications.
- "Nail up" calls from POM to the agent were automatically answered by TMAC.
- Preview/Predictive/Progressive Campaign Calls.
- Campaign Dashboard display.
- Updating contact details.
- Callbacks.
- Adding contacts to Do Not Call (DNC) lists.
- Call features such as: Hold/Resume, Consult, Transfer and Conference.
- Redial customer.
- Search customer details for ACD call.

The serviceability testing focused on verifying the ability of TMAC to recover from adverse conditions such as disconnecting the ethernet cables on the Client PC, AES and POM server, and restarting of the POM service on the AAEP/POM server.

## **2.2. Test Results**

All feature test cases were successfully completed. The following observations were noted:

- Call Blending could not be tested as CMS interface is required with RQT connection.
- POM HA was also not tested.

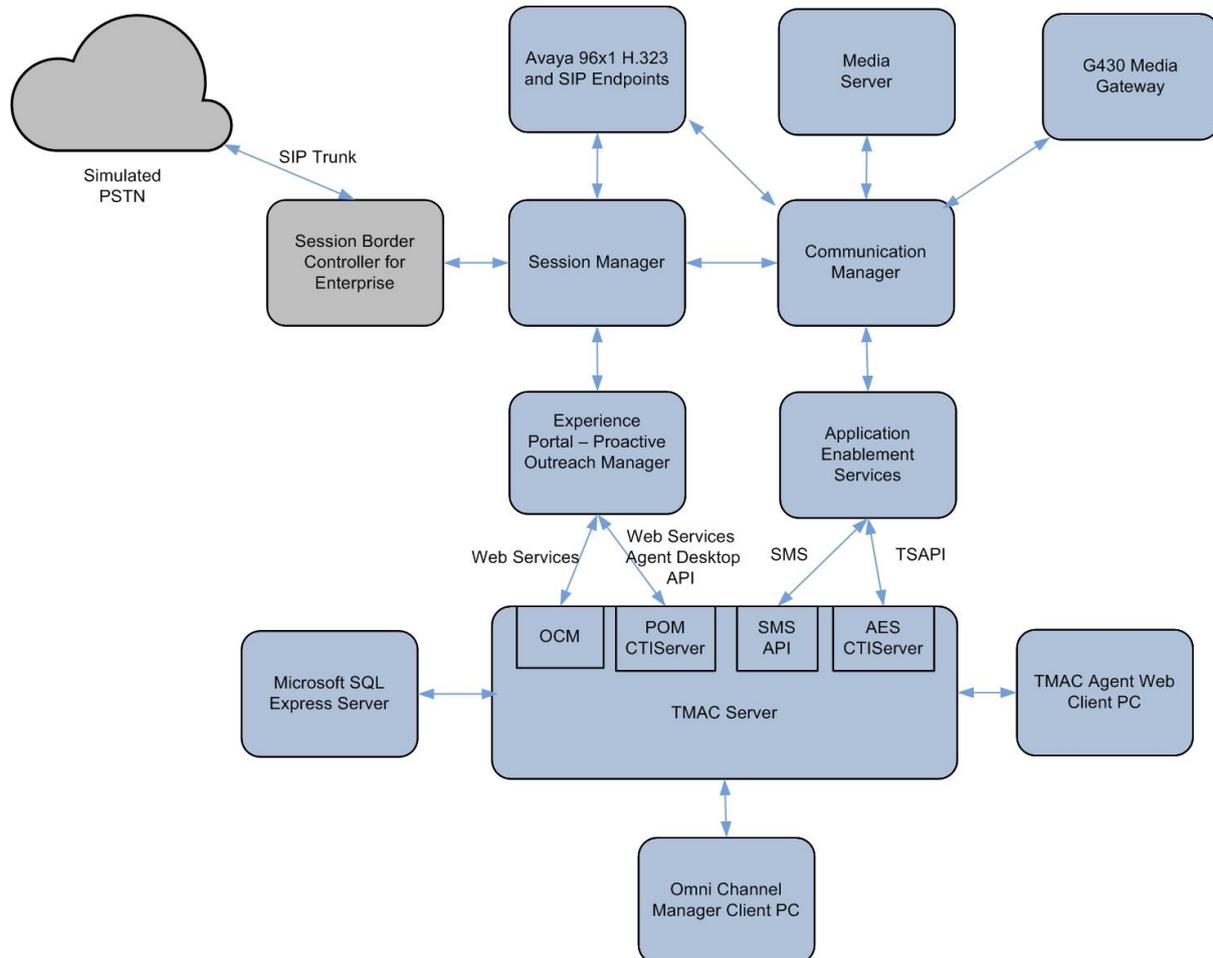
## **2.3. Support**

Technical support on Tetherfi can be obtained through the following:

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

### 3. Reference Configuration

**Figure 1** illustrates the configuration used for testing. In this configuration, outbound call is made via the SIP interface between Avaya Aura® Session Manager and Avaya Aura® Experience Portal Media Processing Platform. In this compliance testing, TMAC is hosting various components as shown below including the MS SQL Express server for its database.



**Figure 1: Test Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Version
Avaya Aura® Communication Manager	8.1.2
Avaya Aura® Media Server	8.0.2
Avaya Aura® Session Manager	8.1.2
Avaya Aura® SBCE	8.1.0
Avaya Aura® Application Enablement Services	8.1.2
Avaya Aura® Experience Portal <ul style="list-style-type: none"> <li>Experience Portal Manager (EPM)</li> <li>Media Processing Platform (MPP)</li> </ul>	7.2.3 7.2.3
Avaya Proactive Outreach Manager <ul style="list-style-type: none"> <li>POM .net Agent Desktop API</li> <li>POM Web Services</li> </ul>	3.1.3 SP2 3.1.3 3.1.3 SP2
96x1 Series IP Deskphones <ul style="list-style-type: none"> <li>H.323</li> <li>SIP</li> </ul>	• 6.8304 • 7.1.10.0
Running on Windows Server 2016 are the following: Tetherfi Omni Channel Management (OCM) Tetherfi Multimedia Agent Server <ul style="list-style-type: none"> <li>AES CTIServer</li> <li>POM CTIServer</li> </ul> Microsoft SQL Express 2016	3.3.11.6 4.0.1.13 4.0.1.13 2016
Tetherfi Multimedia Agent Client running on Windows 10 Enterprise	4.0.6.11
Tetherfi Omni Channel Manager running on Windows 10 Enterprise	3.3.11.6

**Table 1: Equipment/Software Validated**

## 5. Configure Avaya Communication Manager

The configuration of Computer Telephony Integration (CTI) links and the SMS service on Communication Manager to AES is assumed to be in place. Refer to reference [5] for more details. Setup of Agent Stations, Agent Login ID, VDNs, Hunt Groups, Trunks and Call Center features is assumed to be configured and will not be detailed here.

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

This section covers the administration of Experience Portal. Configuration for Avaya POM is also covered in the section as Avaya POM was co-resident on Experience Portal. The configuration of the SIP trunk to Communication Manager is assumed to be in place and will not be documented here.

Below are the POM configurations steps shown in subsequent pages:

- Login to the Experience Portal
- Verify POM Applications
- Configure Avaya POM
- Add POM server
- Configure POM server
- Configure CTI
- Start POM server
- Configure Contacts
- Configure Campaigns
- Configure Campaign Manager
- Add User for Web Services
- Administer POM Global Configuration

## 6.1. Login to the Experience Portal

Experience Portal 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.

*Note:* Some of the screens in this section are shown after the Experience Portal had been configured.

The screenshot displays the Avaya Aura Experience Portal Manager (EPM) web interface. At the top left is the Avaya logo. On the top right, it says "Welcome, epadmin" and "Last logged in yesterday at 6:36:01 PM PST". Below this is a red navigation bar with "Avaya Aura® Experience Portal 7.2.3 (ExperiencePortal)", "Home", "Help", and "Logoff" links. A left-hand navigation menu lists various categories like User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, and Multi-Media Configuration. The main content area is titled "Avaya Aura® Experience Portal Manager" and includes a breadcrumb "You are here: Home". It contains a description of EPM, a section for "Installed Components" with details on Media Processing Platform, Email Service, HTML Service, Proactive Outreach Manager, and SMS Service, and a "Legal Notice" section with a scrollable text area containing the "AVAYA GLOBAL SOFTWARE LICENSE TERMS" (revised May 22, 2019).

## 6.2. Verify POM Applications

Note that the applications needed for Avaya POM were configured during Avaya POM installation. To view the list of application, navigate to **System Configuration** → **Applications**.

Welcome, epadmin  
Last logged in yesterday at 6:36:01 PM PST

Avaya Aura® Experience Portal 7.2.3 (ExperiencePortal) Home Help Logoff

You are here: [Home](#) > System Configuration > Applications

### Applications

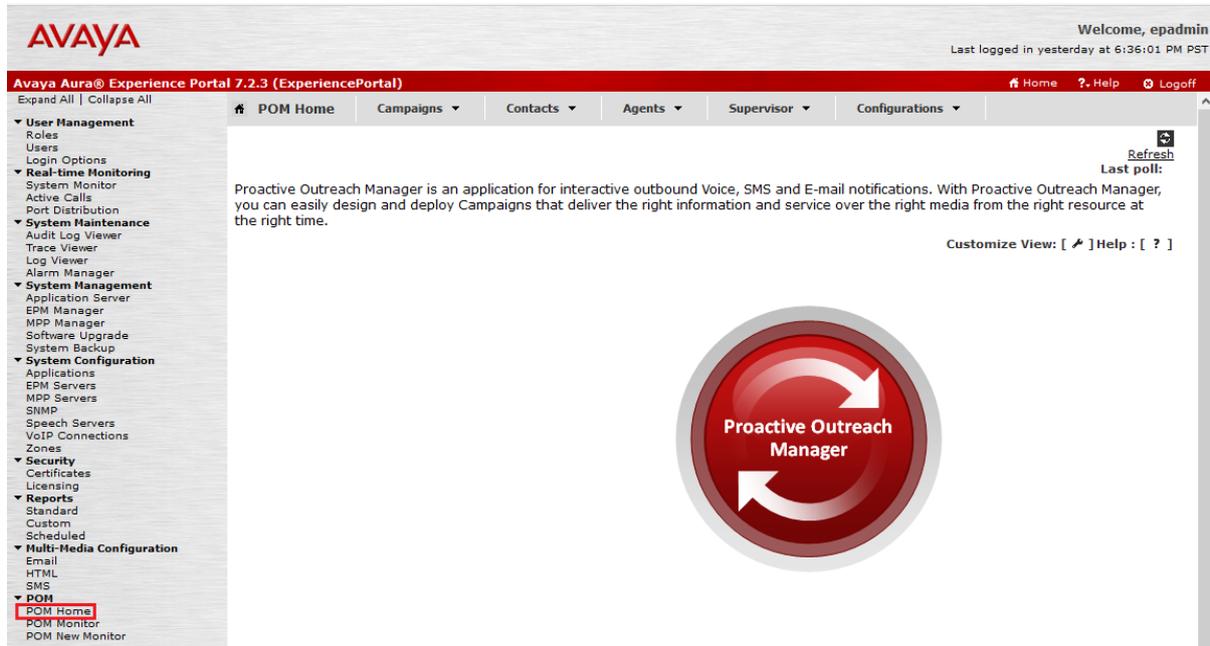
This page displays the applications that are currently deployed on the Experience Portal system.

<input type="checkbox"/>	Name	Enable	Type	URI	Launch	ASR	TTS	Request SIP Calls
<input type="checkbox"/>	<a href="#">AvayaPOMAgent</a>	Yes	POM:Application	https://10.1.10.81:7443/AvayaPOMAgent/Start	Outbound	Nuance (Acquire on call start and retain) English(USA) en-us	No TTS	None
<input type="checkbox"/>	<a href="#">AvayaPOMAnnouncement</a>	Yes	POM:Application	https://10.1.10.81:7443/AvayaPOMAnnouncement/Start	Outbound	Nuance (Acquire on call start and retain) English(USA) en-us	No TTS	None
<input type="checkbox"/>	<a href="#">AvayaPOMEmail</a>	Yes	Email	https://10.1.10.81:7443/AvayaPOMEmail/Start	Outbound	No ASR	No TTS	None
<input type="checkbox"/>	<a href="#">AvayaPOMNotifier</a>	Yes	POM:Application	https://10.1.10.81:7443/AvayaPOMNotifier/Start	Outbound	Nuance (Acquire on call start and retain) English(USA) en-us	No TTS	None
<input type="checkbox"/>	<a href="#">AvayaPOMSMS</a>	Yes	SMS	https://10.1.10.81:7443/AvayaPOMSMS/Start	Outbound	No ASR	No TTS	None
<input type="checkbox"/>	<a href="#">Nailer</a>	Yes	POM:Nailer	https://10.1.10.81:7443/Nailer/ccxml/start.jsp	Outbound	No ASR	No TTS	None
<input type="checkbox"/>	<a href="#">PomDriverApp</a>	Yes	POM:Driver	https://10.1.10.81:7443/PomDriverApp/ccxml/start.jsp	Outbound	Nuance (Acquire on call start and retain) English(USA) en-us	English(USA) en-US Jennifer F	None
<input type="checkbox"/>	<a href="#">TestApp</a>	Yes	VoiceXML	http://10.1.10.83/mpp/misc/avptestapp/intro.vxml	10390	Nuance (Acquire on call start and retain) English(USA) en-us	English(USA) en-US Jennifer F, English(USA) en-US Zoe F	None

[Add](#) [Delete](#) [Clear MPP Cache](#) [Global CAVs](#) [Help](#)

### 6.3. Configure Avaya POM

When Avaya POM is installed on Experience Portal, a sub menu is added to EPM. On the left pane, select **POM Home** under **POM**. All configurations for Avaya POM are performed from the **POM Home** page.

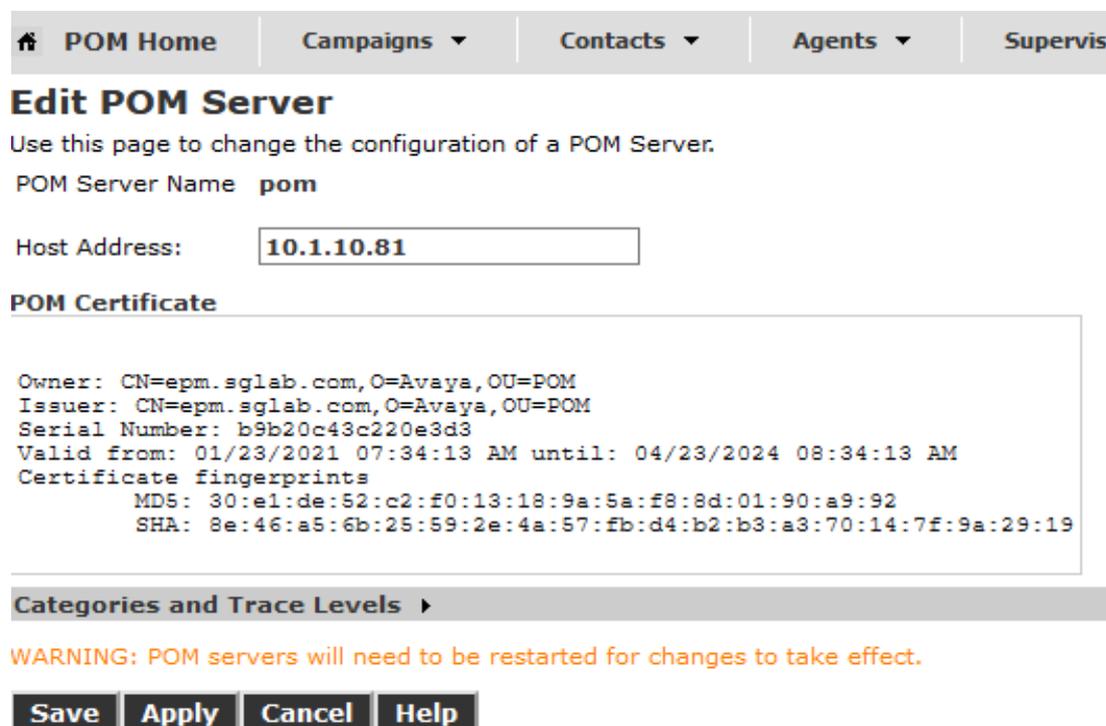


## 6.4. Add POM Server

From **POM Home**, hover over **Configurations** on the top right and select **POM Servers** from the drop-down menu (not shown); click **Add** to add Avaya POM server. On **Add POM Server** page, type in a name in **POM Server Name** and type in Avaya POM IP Address in **POM Server IP Address** and select **Continue**. Note that since Avaya POM was installed on the same server as Experience Portal, IP Address of Experience portal was used.



On the **Edit POM Server** page, **checked** the check box for **Trust this certificate** (not shown) and select **Save**. During compliance test, POM was pre-configured. The screen below displays the POM Server that was configured.



## 6.5. Configure POM Server

Outbound settings will need to be configured for Avaya POM to place outbound calls. Navigate to **Configurations** → **POM Servers** → **Outbound Settings** (not shown).

The screenshot shows the 'POM Servers' configuration page. At the top is a navigation bar with 'POM Home', 'Campaigns', 'Contacts', and 'Agents'. Below the navigation bar is the title 'POM Servers' and a description: 'This page displays the list of POM servers in the Experience Portal system. POM through Outcall web service for voice calls and communicates with SMS and E-M'. A table lists the servers with columns for 'POM Server Name', 'Host Address', 'Trace Level', and 'Certificates'. One server is listed: 'pom' with host address '10.1.10.81' and trace level 'Use POM Settings Export'. Below the table are 'Add' and 'Delete' buttons. At the bottom are four buttons: 'POM Settings', 'Outbound Settings', 'POM Manager', and 'Help'.

On the **Voice Servers** Page, click on the **Name** of Voice Server; **EPM**, in this case.

The screenshot shows the 'Voice Servers' configuration page. At the top is a navigation bar with 'POM Home', 'Campaigns', 'Contacts', 'Agents', 'Supervisor', and 'Configurations'. Below the navigation bar is the title 'Voice Servers' and a description: 'This page displays the list of voice servers. Depending on your user role, you can enter the Voice Server password for outcalling.'. A table lists the servers with columns for 'Name' and 'IP Address'. One server is listed: 'EPM' with IP address 'epm.sglab.com'. Below the table is a 'Help' button.

On the **Edit Voice Server** page, type in the **User Name** then **Password**, as configured for Experience Portal.

The screenshot shows the 'Edit Voice Server' configuration page. At the top is a navigation bar with 'POM Home', 'Campaigns', 'Contacts', 'Agents', and 'Supervisor'. Below the navigation bar is the title 'Edit Voice Server' and a description: 'This page allows you to enter Voice Server password for outbound calling.'. A form contains the following fields: 'Name' (EPM), 'IP Address' (epm.sglab.com), 'User Name' (outcall), and 'Password' (represented by dots). Below the form are three buttons: 'Save', 'Cancel', and 'Help'.

This user name and password are obtained from the **Web Service Authentication Section Outcall of System Configuration → EPM Server → EPM Settings**.

**Avaya Aura® Experience Portal 7.2.3 (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
- ▼ **POM**
  - POM Home
  - POM Monitor
  - POM New Monitor

You are here: [Home](#) > [System Configuration](#) > [EPM Servers](#) > [EPM Settings](#)

## EPM Settings

Use this page to configure system parameters that affect the Experience P

Experience Portal Name:

Number of Application Server Failover Logs:

Commands to Retain in Configuration History:

### Resource Alerting Thresholds (%) ▼

HTML Units:

Disk:  **High Water**  **Low Water**

### Web Service Authentication ▼

#### Application Reporting

User Name:

Password:

Verify Password:

#### Outcall

User Name:

Password:

Verify Password:

### Miscellaneous ▶

## 6.6. Configure CTI

From **POM Home**, navigate to **Configurations** → **CC Elite Configurations** and select **Add CTI Detail** under **CTI Configuration** (not shown). On the **Add CTI Detail** (not shown) page, configure as follows:

- **CTI group name:** Enter name of CTI group.
- **CM IP address:** Enter Communication Manager IP Address.
- **CM Login/password:** Enter username and password of Communication Manager.
- **AES IP address:** Enter in AES IP Address.
- **CTI group role:** From drop down menu, select **Active**.

Screen capture below displays the configuration that was used during the compliance test.

**Avaya Aura® Experience Portal 7.2.3 (ExperiencePortal)**  
Expand All | Collapse All

POM Home Campaigns Contacts Agents Supervisor Configurations

### Edit CTI Detail

This page allows editing of existing CTI details.

**Edit CTI Configuration**

\* CTI group name:

\* CM IP address:

\* CM login:

\* CM password:

\* AES IP address:

AES Secure Connection:

CTI group role:

Save Cancel Help

On the **Configure CTI setup details, CMS setup details and POM Skills** page (not shown), select **Add Skill**. Type in the skill configured in Communication Manager for **CC Elite Skill Number**, type in a name in **POM Skill Name** and select **Outbound** from the **Skill Type** drop-down menu.

POM Home Campaigns Contacts Agents Supervisor Configurations

### 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"

CC Elite Skill Number	POM Skill Name	Skill Type	Parameter to Monitor for Blending
<input type="text" value="2"/>	<input type="text" value="Support"/>	<input type="text" value="Outbound"/>	<input type="text" value="Select only for Inbound"/>

## 6.7. Start POM server

Once POM Server is completely created, start it by navigating to **Configurations → POM Servers → POM Manager** (not shown). On the POM Manager page, select the check box of Avaya POM server name and click **Start**. Note that in the picture below POM server was already started, if it is stopped the Start button is available to start POM server.

### POM Manager

Use this page to manage the POM servers connected to this EPM.

POM Servers	
Service Names	
	<input checked="" type="checkbox"/> pom
ActiveMQ	<input checked="" type="checkbox"/> MASTER
Advance List Management	<input checked="" type="checkbox"/> RUNNING
Agent SDK Service	<input checked="" type="checkbox"/> RUNNING
Agent Manager	<input checked="" type="checkbox"/> MASTER
Campaign Director	<input checked="" type="checkbox"/> MASTER
Campaign Manager	<input checked="" type="checkbox"/> RUNNING
Kafka Server	<input checked="" type="checkbox"/> RUNNING
Rule Server	<input checked="" type="checkbox"/> MASTER

**Start** **Stop** **Help**

## 6.8. Add User for Web Services

From Experience Portal home page, navigate to **User Management → Roles** (not shown) and select **Add**. Type in a name in **Name** and tick **Web Services**. This will be needed for TMAC to access POM features and functionality through its program. Creation of other POM users required will be required to administer, supervise, report or manage the Campaign but will not be documented here.

### Add User

Use this page to add a EPM user account. The roles you select for the user account determines the

Name:

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

Password:

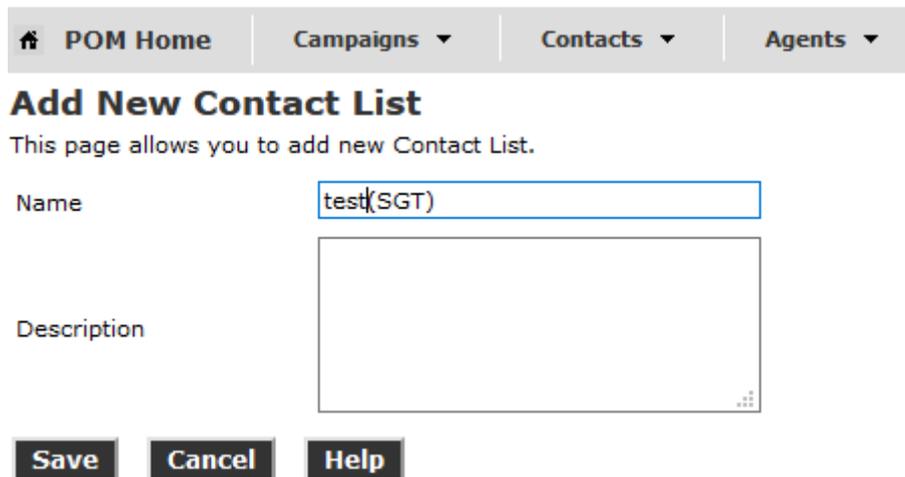
Verify Password:

Enforce Password Longevity:

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

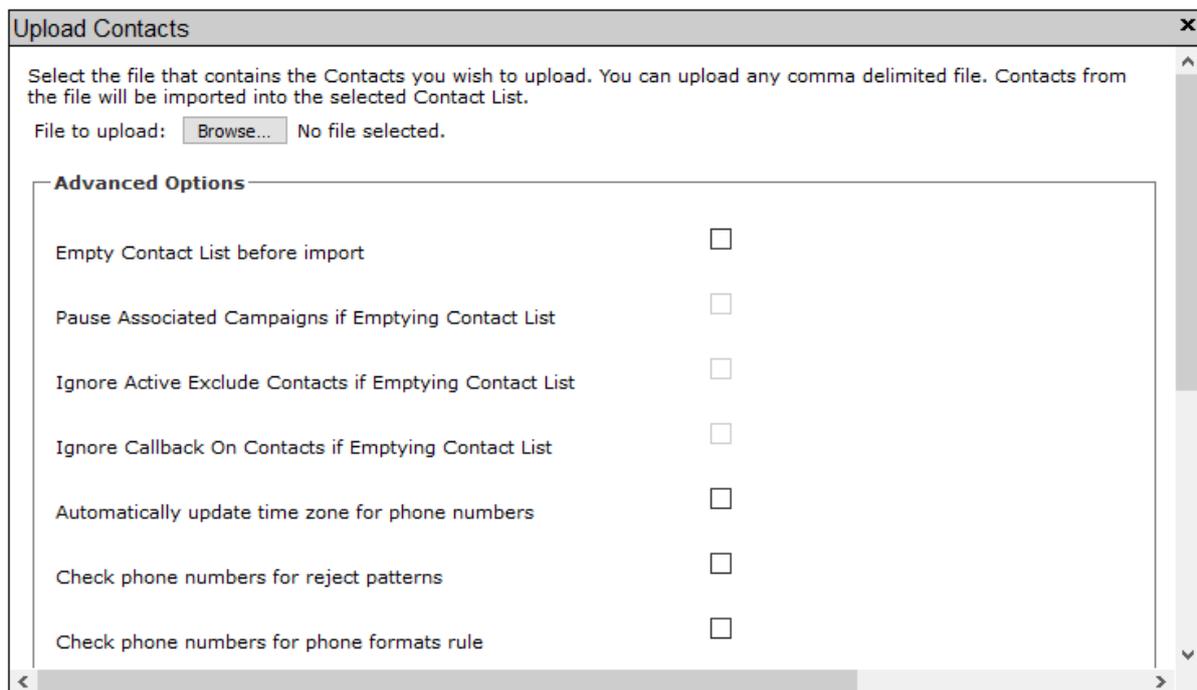
## 6.9. Configure Contacts

From **POM Home**, navigate to **Contacts** → **Contact Lists** (not shown) and select **Add**. Type in a name in **Name** and brief **Description** (if any) and select **Save**.



The screenshot shows the 'Add New Contact List' form. At the top, there is a navigation bar with 'POM Home', 'Campaigns', 'Contacts', and 'Agents'. Below the navigation bar, the title 'Add New Contact List' is displayed. A sub-header states: 'This page allows you to add new Contact List.' The form has two input fields: 'Name' with the value 'test(SGT)' and 'Description' which is currently empty. At the bottom of the form, there are three buttons: 'Save', 'Cancel', and 'Help'.

A message will indicate Contact List is created successfully. On the next page, select **Upload Contacts now** (not shown). Click on **Browse** to browse to the location of .csv for the contacts and select **Upload**.



The screenshot shows the 'Upload Contacts' dialog box. It has a title bar with 'Upload Contacts' and a close button. The main text reads: 'Select the file that contains the Contacts you wish to upload. You can upload any comma delimited file. Contacts from the file will be imported into the selected Contact List.' Below this, there is a 'File to upload:' label, a 'Browse...' button, and the text 'No file selected.'. An 'Advanced Options' section is expanded, showing several checkboxes: 'Empty Contact List before import', 'Pause Associated Campaigns if Emptying Contact List', 'Ignore Active Exclude Contacts if Emptying Contact List', 'Ignore Callback On Contacts if Emptying Contact List', 'Automatically update time zone for phone numbers', 'Check phone numbers for reject patterns', and 'Check phone numbers for phone formats rule'. All checkboxes are currently unchecked.

## 6.10. Configure Campaigns

Campaigns are created to launch calls for various programs. Below are a sample campaign creation steps.

### Configure Campaign Strategy

From **POM Home**, navigate to **Campaigns** → **Campaign Strategies** and select **Add** (not shown). Type in a **Name** as shown below and select **Continue**. A template can be used by checking the **Use template** box.

Speech Servers  
VoIP Connections  
Zones  
▼ Security  
Certificates  
Licensing  
▼ Reports  
Standard  
Custom  
Scheduled  
▼ Multi-Media Configuration

Name

Use template

Template

**Continue** **Cancel**

The **Campaign Strategy Editor** page will pop up. Configure a **Campaign Strategy** as needed. Below is an example of the strategy configured during compliance testing.

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

Selected Node: Task

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

Campaign Strategy: test\_predictive

- Campaign Strategy
  - Handler (initial)
    - Call
      - Address
      - Result Processors
        - Result (Answer Human)
          - Agent

APPLICATIONS

Driver Application\* PomDriverAp

Nailer Application\* Nailer

Nuisance Call Application\* AvayaPOMA

On Hold Application\* AvayaPOMA

PACING PARAMETERS

Call Pacing Type Cruise Contr

Desired Service Level 80

Min. Agents 1

Max. Agents 10

Agent Outbound Skill Support

ACW Time (Sec) 200

Loaded: test\_predictive

## Configure Campaign Manager

From **POM Home**, navigate to **Campaigns** → **Campaign Manager** and select **Add** (not shown). Type in a name in **Name** field and select **Continue**.

The screenshot shows the Campaign Manager interface. At the top, there is a navigation bar with 'POM Home', 'Campaigns', 'Contacts', 'Agents', 'Supervisor', and 'Configurations'. The main heading is 'Campaign Manager' with a 'Refresh' button and 'Last poll: 02/03/2021 01:50:23 AM'. Below the heading, there is a search bar and an 'Advanced' link. A table lists campaigns with columns for Name, Type, Campaign Strategy, Contact List, Filter, Last Executed, and Waiting Callbacks. A modal dialog titled 'Add a Campaign' is open, showing a 'Create Campaign' form with a 'Name' field, radio buttons for 'New Campaign' (selected) and 'Copy existing Campaign', and 'Continue', 'Cancel', and 'Help' buttons.

On the **Define Campaign** page, select the strategy added in previous section for Campaign Strategy.

The screenshot shows the 'Define Campaign' page. At the top, there is a navigation bar with 'POM Home', 'Campaigns', 'Contacts', 'Agents', 'Supervisor', and 'Configurations'. The main heading is 'Define Campaign'. Below the heading, there is a paragraph of instructions: 'Give a name to Campaign, define its type, select the Campaign Strategy and one or more Contact List to be used with the Campaign. Click on the "Finish" button to complete the Campaign creation process. To change optional parameters, click the "Next" button.' The page is divided into sections: 'Name and Description' with a text input field containing 'test\_campaign'; 'Campaign Strategy' with a dropdown menu showing 'test\_preview' and three icons (refresh, add, delete).

Select the **Contact List** from **Section 6.9** and select **Finish** (not shown). **DNC Group** (Do Not Call) can also be added to the Campaign for DNC Lists before it is started.

### Contact List and Filter Selection

Select Contact List and Filter for this campaign

**Name:** test\_campaign

**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 this Campaign. Associating a Filter with the Contact List is not mandatory. Maximum 15 Contact Lists can be added to the can associated with a Contact List. Use the Apply same filter checkbox to apply filter template associated with top row of associati dialing Allocation checkbox if filtering and dialing should not be driven based on dialing allocation. No dialing Allocation checkb same filter is enabled.

Apply same filter     No Dialing Allocation

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

**Add Association**

## 6.11. Administer POM Global Configuration

From **POM Home**, navigate to **Configurations → Global Configuration**. Scroll down to **Agent settings** section. Parameters such as **Nailup call CLID** can be adjusted for display on Agent Deskphones.

The screenshot shows the Avaya Aura Experience Portal 7.2.3 configuration 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 main content area is titled "Agent settings" and contains the following configuration items:

Setting Name	Value
Maximum job waiting duration(min)	20
Minimum job attachment period(min)	15
Nailing retry interval(sec)	20
Nailup call CLID	98765
Maximum record waiting duration for attribute dialing(min)	10
ANI for external consult calls	<input type="radio"/> Nailup call CLID <input type="radio"/> Agent Extension <input checked="" type="radio"/> Use campaign ANI <input type="radio"/> Free form Text 98675
Call queue	<input type="checkbox"/>
Override PAI for External Consult Calls	<input type="checkbox"/>
Enable Time Restriction for preview dial and redial	<input type="checkbox"/>
Release agent in NOT READY state from outbound	<input type="checkbox"/>
Release agent in IDLE state from outbound	<input type="checkbox"/>
Enable RFC2833 for AGTSendDTMF API of Agent Desktop	<input type="checkbox"/>
Restrict Agent to receive out-of-band DTMF	<input type="checkbox"/>
Restrict Customer to send and receive out-of-band DTMF	<input type="checkbox"/>
Strict Nuisance Reporting	<input type="checkbox"/>
Nuisance Duration for Agent Connect(msec)	2000
External Selection	<input type="checkbox"/>

Scrolling down further to **Advance settings**, note the default port **9970** which will be used for **Agent manager base port** for the POM Web Services configured in **Section 7.1**.

### Advanced settings

JMS listen port	* 51616
Pacer base port	* 9995
Agent Initiated Pacer base port	* 10005
Router base port	* 7779
Agent manager base port	* 9970
Maximum concurrent jobs	* 50
Maximum ports per server	* 1200
Agent manager heart beat port	* 8870
Rule Engine port	* 8779
Days before certificate expiry alert	* 60

## 7. Configure Tetherfi Multimedia Agent Client

The installation of TMAC and its components is performed by Tetherfi engineers and will not be detailed here. The following steps are presented in these Application Notes for **informational** purposes. Note that configuration of TMAC for AES is also required but will not be detailed here. Refer to reference [5] for more information.

This section highlights the configuration of TMAC for POM which includes the following areas:

- Configurations setup for POM
- Configure Agents using OCM

### 7.1. Configurations setup for POM

Launch a web browser and enter **http://<IP address of TMAC Server>/TMC** to access the CTI Server configuration.

Note the following parameters are configured:

- **POMServerIP**: Enter IP address of the POM Server. This is the same as the Experience Portal Manager (EPM) IP address as POM is co-resident with EPM.
- **POMServerPort**: Enter Agent Manager Base port. The default port **9970** is used and can be viewed on the POM Global Configuration as in **Section 6.11**.
- **POMAgentPassword**: Recommended to be empty as individual agents will be configured via the Omni Channel Management.
- **POMLocale**: Locale is set to **En-US** in these Compliance Testing.
- **POMTimeZone**: Enter Time Zone.
- **POMZoneName**: Enter Zone Name.
- **POMOrgName**: Enter Organization Name (Optional).
- **POMServerRESTURL**: **https://<POM Server IP address>**.
- **POMServerRESTUserName**: Enter Web Services User Name in **Section 6.8**.
- **POMServerRESTPassword**: Enter Web Services User Password in **Section 6.8**.

## Product Settings

\* Description:  \* Name:  Version:

[Configuration](#) [Prerequisites](#) [Dependencies](#) [InstallationDetails](#)

### Global Configuration

TetherfLogPath:

### Product Configuration

WebSocketServerPort:  AESKeepAliveEnabled:

DoNotProcessConnectionClearedEventForVDNMonitoring:  EnablePrivateData7:

AESAgentPassword:  EnableAgentStatusPolling:

AgentStatusPollingInterval:  AgentStatusInvokeID:

EnableDummyCTIServer:  EnableCiscoIntegration:

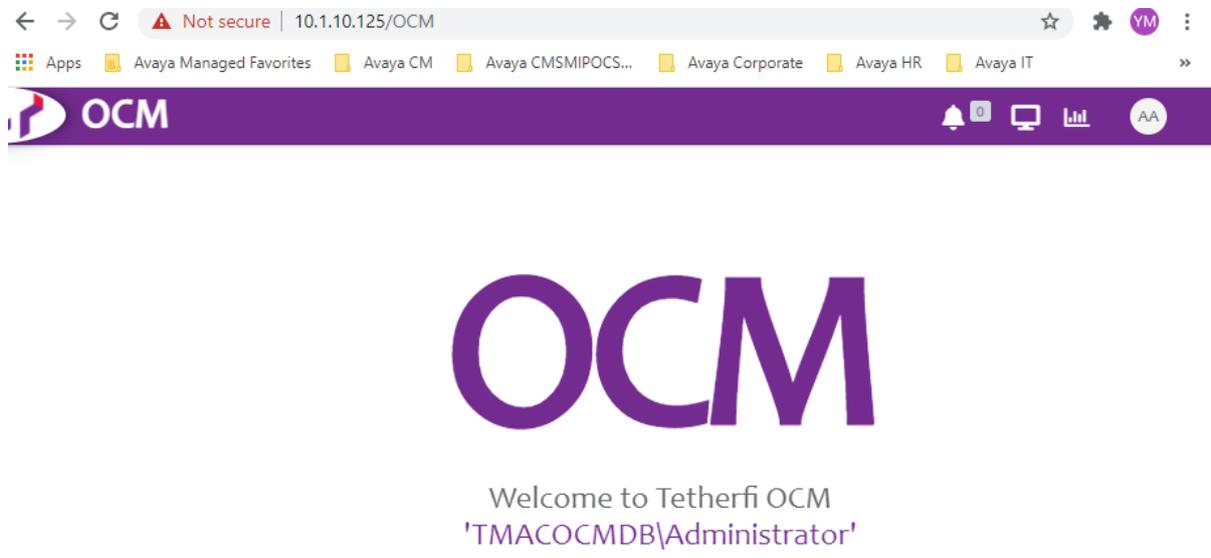
PrimaryFinesseHttpURL:  PrimaryFinesseHttpsURL:

PrimaryFinesseXmppHostName:  SecondaryFinesseHttpURL:

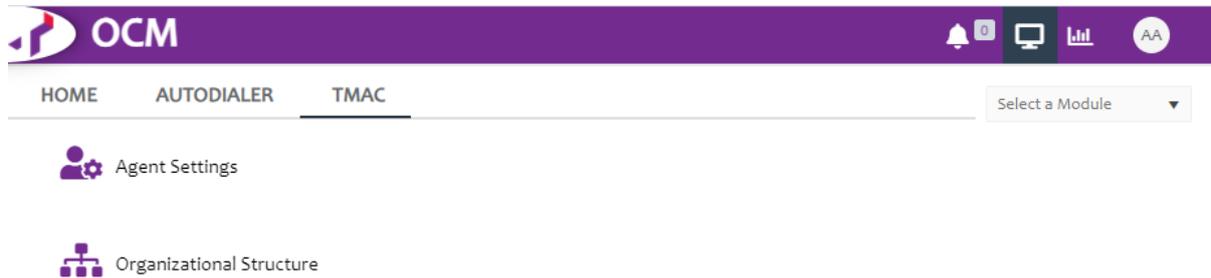
SecondaryFinesseHttpsURL:	<input type="text" value="http://localhost:8082/finesse/api/"/>	FinesseUserPassword:	<input type="text" value="password"/>
EnableSecureIntegration:	<input type="text" value="false"/>	FinesseXmppUserPassword:	<input type="text"/>
XMPPLicenseKey:	<input type="text"/>	UCCXAdminUserName:	<input type="text"/>
UCCXAdminPassword:	<input type="text"/>	POMServerIP:	<input type="text" value="10.1.10.81"/>
POMServerPort:	<input type="text" value="9970"/>	POMAgentPassword:	<input type="text" value="localhost"/>
POMLocale:	<input type="text" value="En-US"/>	POMTimeZone:	<input type="text" value="GMT-05:00"/>
POMZoneName:	<input type="text" value="SGT"/>	POMOrgName:	<input type="text" value="localhost"/>
EnablePOMIntegration:	<input type="text" value="true"/>	EnablePOMSecureIntegration:	<input type="text" value="true"/>
CampaignStatusPollInterval:	<input type="text" value="1"/>	InterpreterSecurityProtocolType:	<input type="text" value="tls12"/>
InterpreterCertificateFolder:	<input type="text" value="C:\Tetherfi\Applications\CTIServer_POM"/>	EnableRESTAPIIntegrationWithPOM:	<input type="text" value="true"/>
EnableRESTAPISecureIntegration:	<input type="text" value="true"/>	POMServerRESTURL:	<input type="text" value="https://10.1.10.81"/>
POMServerRESTUserName:	<input type="text" value="Tether"/>	POMServerRESTPassword:	<input type="text" value="Tetherfi!23"/>
POMCallbackDashboardURL:	<input type="text" value="http://localhost:50000/TetherfiPOMCallb"/>	AllowCallbacksToSetForAnyDay:	<input type="text" value="true"/>
Country:	<input type="text" value="SG"/>	AttributeFieldNameToSearch:	<input type="text" value="NRIC"/>

## 7.2. Agents configured using OCM

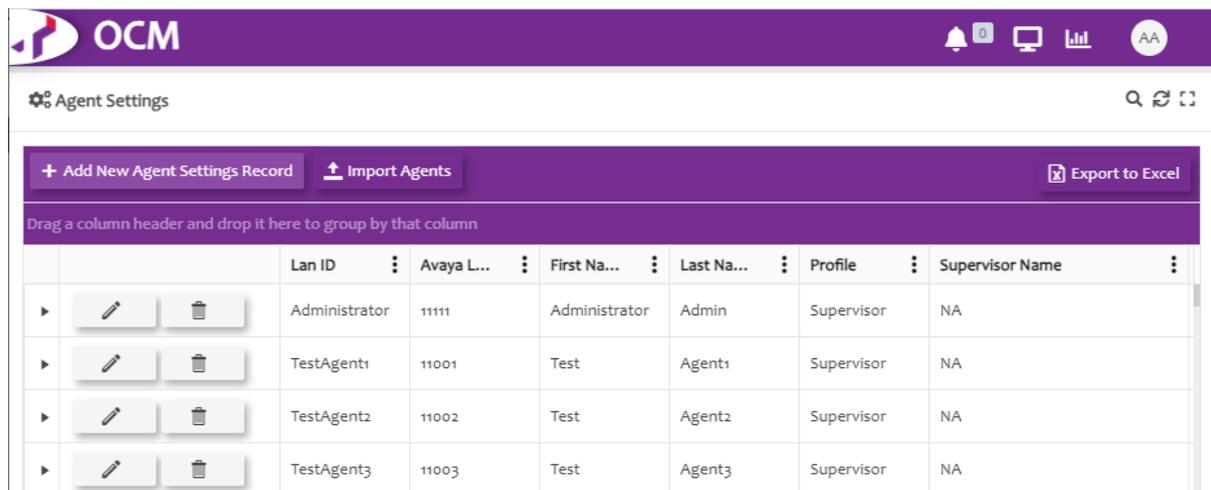
Launch a web browser and enter **http://<IP address of TMAC Server>/OCM** to access the OCM module for configuration of TMAC Agents.



Click on the monitor icon on the top right bar and select **TMAC** → **Agent Settings** below.



Below is a list of the 3 agents already created for testing. Select the pen for the first agent.



The first agent settings on the **Info** tab is shown below. Note the **Lan ID** name and **Avaya Login ID** which is the agent-ID configured on Communication Manager.

The screenshot displays the 'Info' tab of a user management interface. The page title is 'Channel Count & Features'. The 'Info' tab is selected, and the 'Profile Picture' section is visible. The settings are as follows:

Field	Value
Lan ID*	TestAgent1
Avaya Login ID*	11001
First Name*	Test
Last Name*	Agent1
Org. Unit*	SG
Profile*	Supervisor
Supervisor*	NA
Access Role*	Agent + Supervisor
CRM Name	Select
Text Template	Select

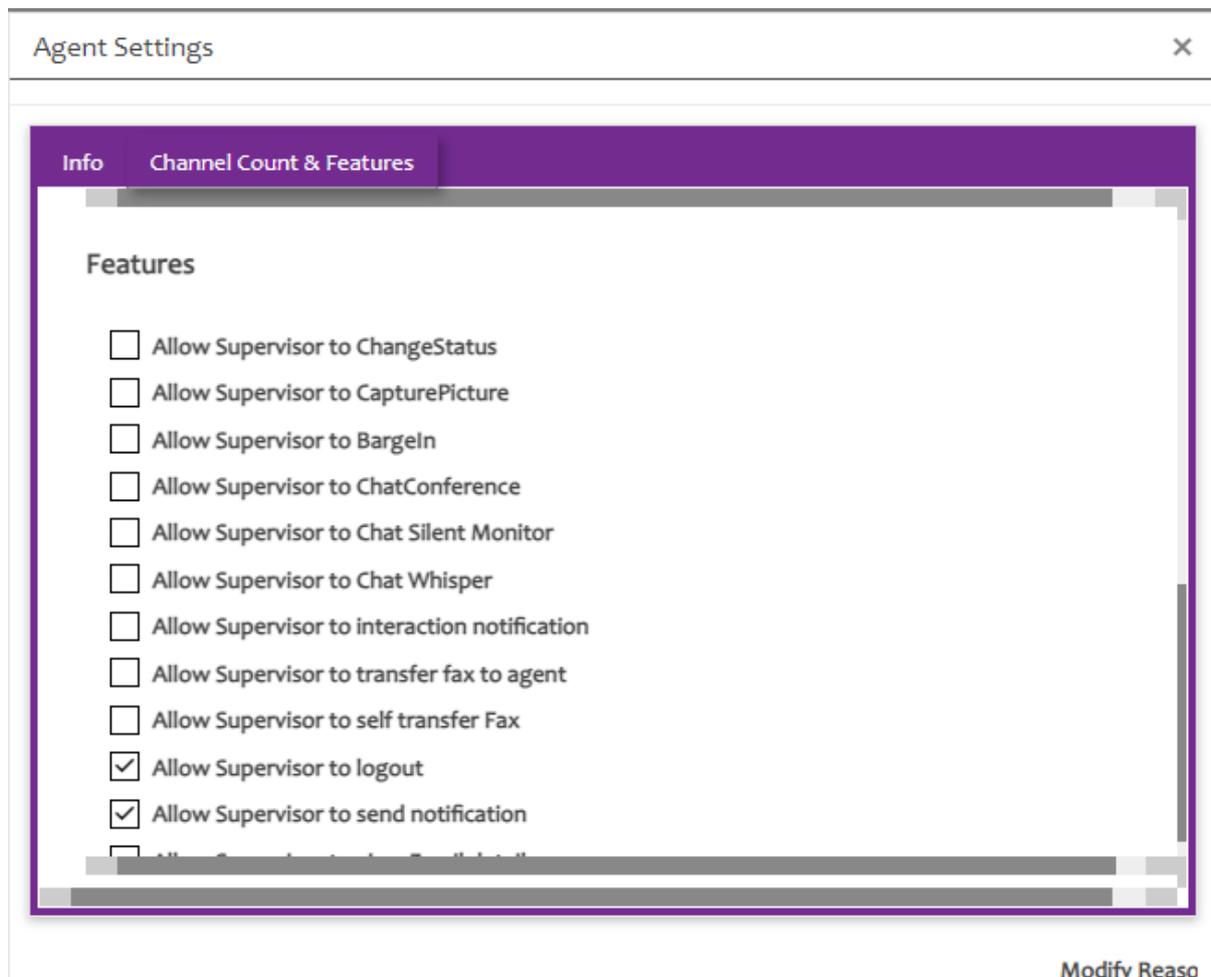
The 'Profile Picture' section shows a message: 'Existing Profile Picture Not Available'. Below this message is a button that says 'Select a new Profile Picture for Upload'. To the right of the main settings is a red button that says 'Remove Picture'.

Select the **Channel Count & Features** tab. The **Voice** channel is shown as selected.

The screenshot shows a settings window titled "Agent Settings" with a close button (X) in the top right corner. Inside the window, there are two tabs: "Info" and "Channel Count & Features". The "Channel Count & Features" tab is active. Below the tabs, the heading "Channel Count" is centered. There are six rows, each representing a channel type. Each row has a checkbox on the right and a numerical input field on the left. The "Voice" row has a checked checkbox and the number "1". The other rows ("Text Chat", "Audio Chat", "Video Chat", "Fax", and "Email") have unchecked checkboxes and the number "0".

Channel Type	Count	Selected
Voice	1	Yes
Text Chat	0	No
Audio Chat	0	No
Video Chat	0	No
Fax	0	No
Email	0	No

Scrolling down further, features selected are to **Allow Supervisor to logout and send notification.**



## 8. Verification Steps

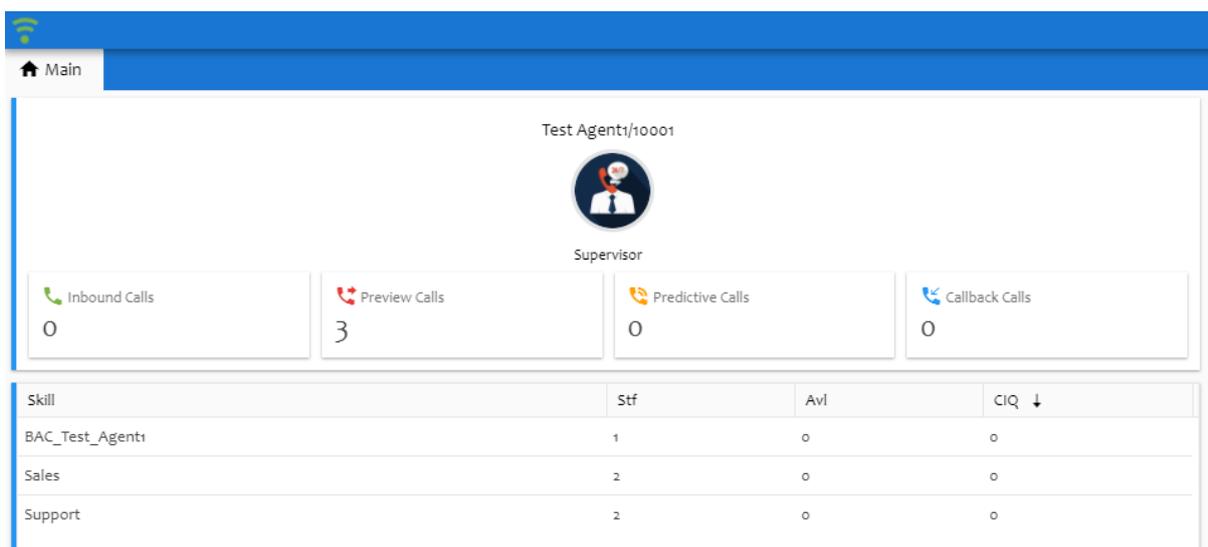
This section provides the verifications steps to verify that the TMAC agent client is able to work with Avaya POM.

### 8.1. Verify Tetherfi Multimedia Agent Client

Launch a web browser on the agent PC and enter address **http://<IP address of TMAC server>/TMAC\_UI/>** to access the TMAC. Log in to an agent **LAN ID** account in **Section 7.2** with the station extension number.

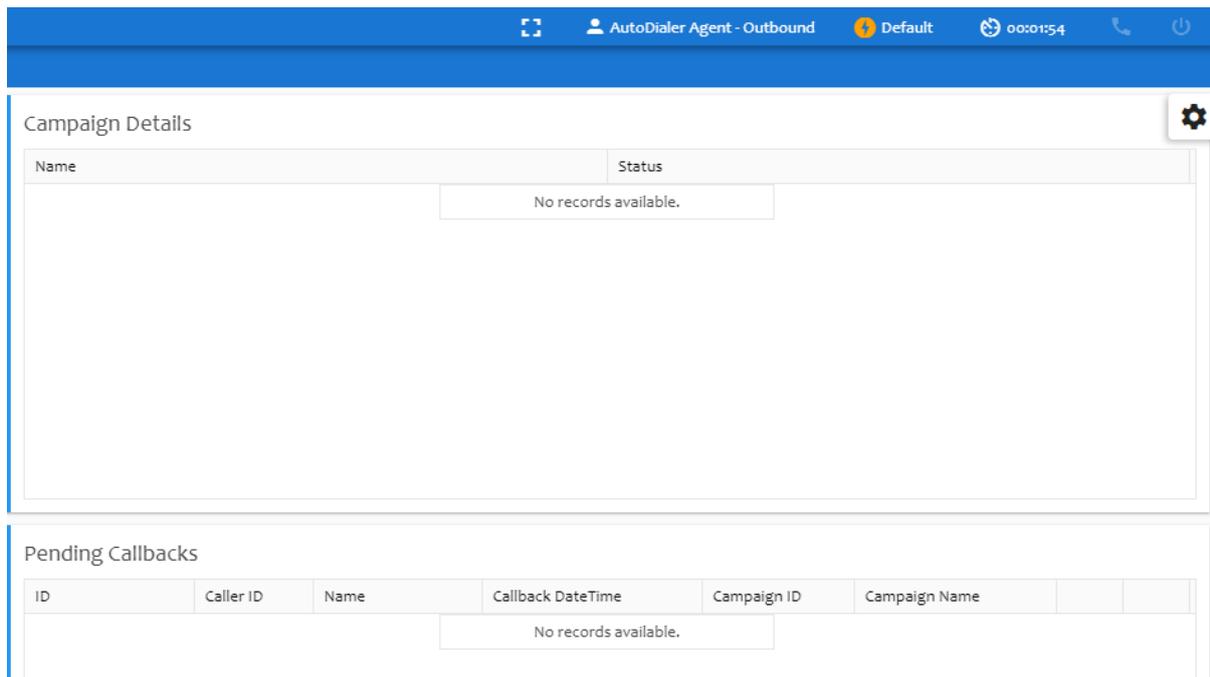


On the next screen that pops up, the login screen is displayed. For clarity, the panel below shows the left panel. The right panel is shown on the next page.

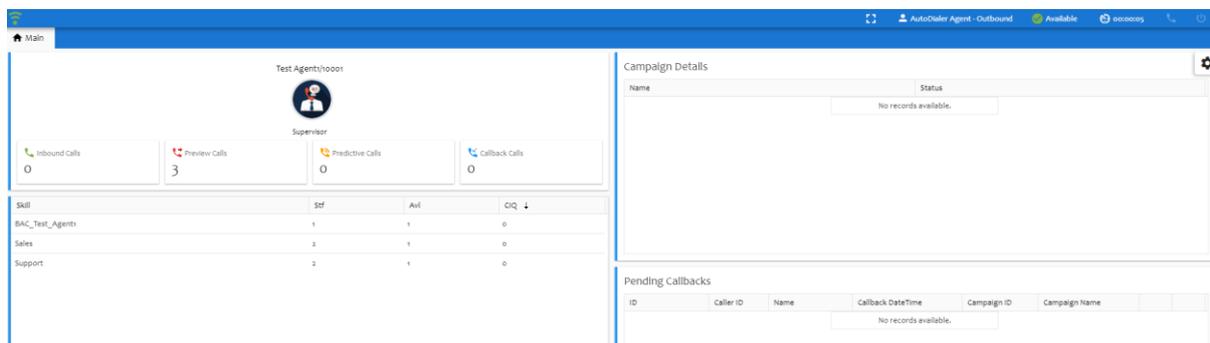


Skill	Stf	Avl	CIQ ↓
BAC_Test_Agent1	1	0	0
Sales	2	0	0
Support	2	0	0

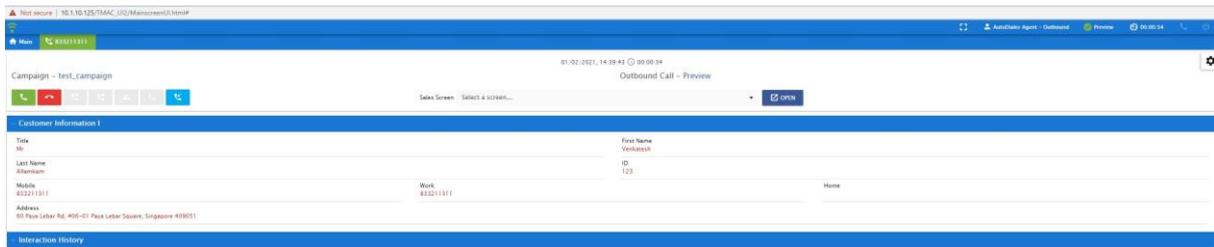
Note that the display shows **AutoDialer Agent – Outbound**.



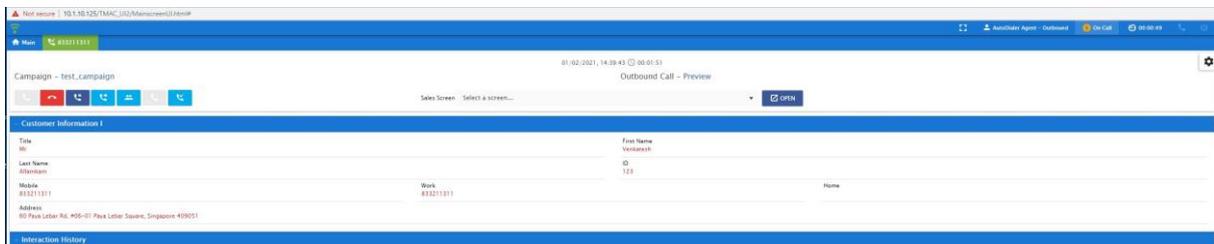
Click on the **Default** (orange) above to select **Available** on the top right bar to receive or make call.



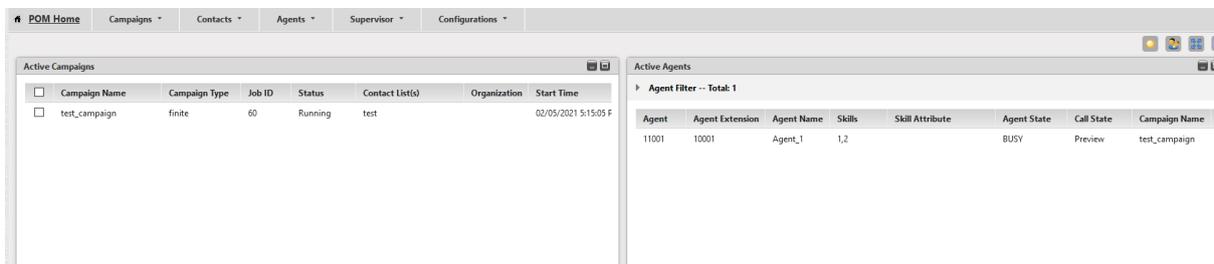
Start a POM Campaign and verify the agent receives the call. The screenshot below shows a Nailup call for Outbound Call for preview before agent launch a call. Note that customer details are also presented with the outbound calling number.



Once the agent dial call to customer using the off hook green button on top left, and customer answer the call; all the buttons including on hook, hold, transfer and conference are highlighted.



Verify from the POM monitor that a campaign is running and 11001 is an active agent in **Preview Call State** as shown below.



Verify also that the agent can hold, transfer or conference the outbound call.

## 9. Conclusion

These Application Notes describe the configuration steps required for Tetherfi Multimedia Client 4.0 to interoperate with Avaya Proactive Outreach Manager 3.1.3. All feature test cases were completed successfully with observations noted in **Section 2.2**.

## 10. Additional References

This section references the Avaya and Tetherfi documentations that are relevant to these Application Notes.

The following Avaya product documentations can be found at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 8, November 2020.
- [2] *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 8, December 2020.
- [3] *Using Avaya Proactive Outreach Manager*, Release 3.1.3, Issue 1.3, August 2020
- [4] *Administering Avaya Aura Experience Portal*, Release 7.2.3, Issue 1, September 2019.
- [5] *Application Notes for Tetherfi Omni Channel Management Multimedia Agent Client with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3*
- [6] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 6, Aug 2020.
- [7] *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 6, Apr 2020.

Tetherfi product documentations can be obtained from Tetherfi contacts in **Section 2.3**.

- [1] *Tetherfi Multimedia Agent Client Application Operations Manual*, Version 1.01, dated 5<sup>th</sup> February 2021
- [2] *Tetherfi Multimedia Agent Client Application User Guide*, Version 1.0.06.25, dated 23<sup>rd</sup> Dec 2020

---

**©2021 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](mailto:devconnect@avaya.com).