



Application Notes for Inisoft Syntelate XA with Avaya Proactive Outreach Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Inisoft Syntelate XA with Avaya Proactive Outreach Manager. Inisoft Syntelate XA 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 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 to integrate Inisoft Syntelate XA with Avaya Proactive Outreach Manager R3.1.2 and Avaya Aura® Application Enablement Services R8.1.

These Application Notes describe two separate connections, the primary connection is to Avaya Proactive Outreach Manager (POM) which is used to control outbound calls by connecting to the Agent Desktop API of Avaya Proactive Outreach Manager. The secondary connection is to the Avaya Aura® Application Enablement Services using Telephony Server Application Programming Interface (TSAPI) to control the Avaya endpoints when answering incoming skillset calls. TSAPI also allows Syntelate agent desktop to hold, transfer and conference these skillset calls. For compliance testing the two connections were required to allow for both inbound and outbound calls.

Syntelate XA is a web client agent desktop that uses the Agent Desktop API of Avaya Proactive Outreach Manager to integrate agent functionality and management. The Syntelate XA solution consists of Syntelate XA Designer, Syntelate XA Studio and Syntelate XA Desktop all of which runs on an IIS web server. There is also a generic Database server. Syntelate XA Designer is a graphical tool used to define the call flow and custom desktop screen.

Configuration for Avaya Proactive Outreach Manager is performed in Syntelate XA Designer. When Syntelate XA Desktop is launched, to connect to Avaya POM, configuration is retrieved from Syntelate server. This particular configuration is deemed as a blended type of agent where both incoming skillset calls and outgoing POM calls are handled by the Syntelate XA Desktop.

2. General Test Approach and Test Results

As there are two distinct and connections to the Avaya solution both connections were tested as part of the compliance testing. The connection to AES was tested by placing incoming calls to various VDN's and allowing the Syntelate XA desktop to answer and process the calls. The connection to POM was tested by running two campaigns, 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 Syntelate XA desktop. Serviceability testing was carried out to observe the response of the Syntelate XA desktop when various LAN failures were simulated.

For compliance testing, POM was configured as "CCElite" to allow communications with Communication Manager and AES. POM was installed on Avaya Aura® 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 Syntelate XA did not include use of any specific encryption features as requested by Inisoft.

2.1. Interoperability Compliance Testing

Interoperability compliance testing included feature and serviceability testing. The feature testing focused on the following functionality:

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).
- Serviceability testing by simulating LAN failures.

POM testing.

- Agent states: Ready, Not Ready and changing Aux Reason code.
- Outbound calls using POM.
- Updating contact details.
- Callbacks.
- Adding and removing contacts from Do Not Call (DNC) lists.
- Call features such as hold, consult, transfer and conference (POM calls).
- Adding notes and passing them between agents.
- Serviceability testing by simulating LAN failures.

The serviceability testing focused on verifying the ability of the Syntelate XA solution to recover from adverse conditions, such as power failures and network disconnects.

2.2. Test Results

All test cases were executed and verified. The following observations were noted during compliance testing.

1. “Nail up” calls from POM to the agent were manually answered on the agent phone by the agent, this is as per design by Inisoft.
2. To allow “Nail up” calls be presented to the agent the COR must be set for Direct Agent Calling to No.

2.3. Support

For technical support on the Syntelate XA, contact Inisoft via phone, email, or internet.

- **Phone:** +44 (0)800 668 1290
- **Email:** support@inisoft.co.uk
- **Web:** www.Syntelate.com

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Syntelate XA server was placed on the Avaya Telephony LAN. The AES provides the Syntelate XA desktop CTI capability on Communication Manager. The Syntelate XA desktop is capable of logging elite agents into existing Avaya endpoints and controlling them via a web page on the agent PC. Outbound calls made from POM are also controlled using the Desktop API connection to POM.

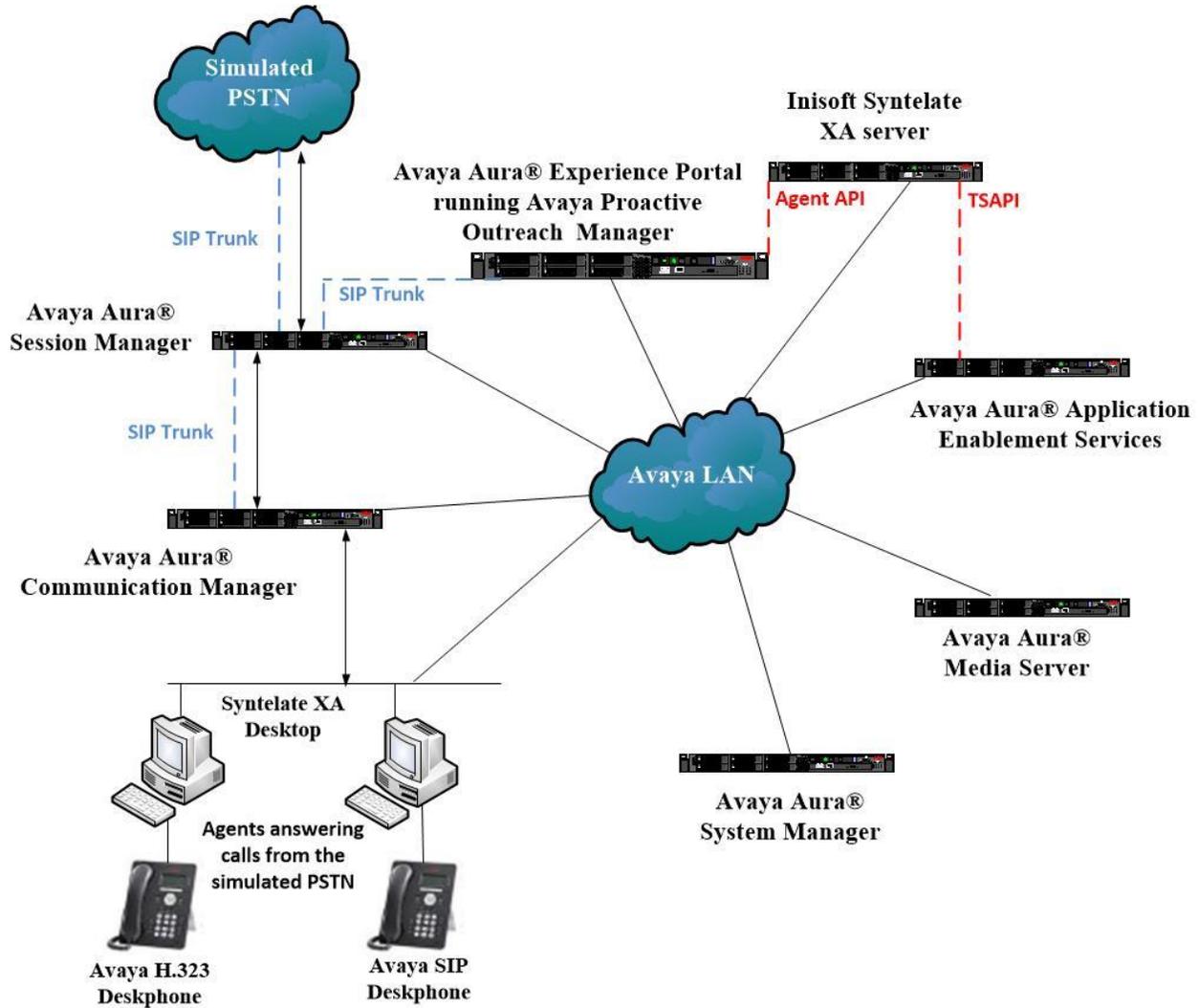


Figure 1: Network solution of Inisoft Syntelate XA and Avaya Proactive Outreach Manager R3.1.2 with Avaya Aura® Application Enablement Services R8.1

4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager	System Manager 8.1.0.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.0.079880
Avaya Aura® Session Manager	Session Manager R8.1 Build No. – 8.1.0.0.810007
Avaya Aura® Communication Manager	R8.1.0.1.0 – SP1 R018x.01.0.890.0 Update ID 01.0.890.0-25393
Avaya Aura® Application Enablement Services	R8.1 8.1.0.0.0.9-1
Avaya Aura® Experience Portal Avaya Proactive Outreach Manager	7.2.2.2.0.2065 3.1.2.0.0.31
Avaya Aura® Media Server	Appliance Version R8.0.0.12 Media Server 8.0.0.169 Element Manager 8.0.0.169
Avaya 96x1 H323 Deskphone	6.6604
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Inisoft Equipment	Software / Firmware Version
Inisoft Syntelate XA Running Avaya Application Enablement Services TSAPI Client	2.0.1 6.3.3
Inisoft Syntelate XA Web Application	Chrome

Note: Inisoft Syntelate XA Web Application was tested using Chrome but Internet Explorer, Mozilla FireFox and Microsoft Edge are also supported browsers.

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration 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 in **Section 11**.

The configuration of Communication Manager could be considered as two separate sections.

1. Configuration of the connection to POM.
2. Configuration of the connection to AES.

5.1. Configuration of the connection to Avaya Proactive Outreach Manager

The connection to POM consists of the following subsections.

- Configuration of the VDN, Vector and Agent for the incoming calls
- Configuration of the SIP trunk for call routing
- Configuration of the Communication Manager user for POM

5.1.1. Configuration of the VDN, Vector and Agent

For calls to be routed to agents, Hunt Groups (skills), Vectors, and Vector Directory Numbers (VDN) must be configured.

5.1.1.1 Hunt Groups

A hunt group is setup for inbound and another for outbound calls. The outbound hunt group is referenced in **Section 7.3** as a Skill in POM.

5.1.1.1.1 Outbound Hunt Group

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 to 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: 1801                           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
                                     HUNT GROUP
                                     Page 2 of 4

                                     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

```

5.1.1.1.2 Inbound Hunt Group

Enter the **add hunt-group n** command where **n** in the example below is **90**. On **Page 1** of the **hunt-group** form, assign a **Group Name** and **Group Extension** valid under the provisioned dial plan. Set the following options to **y** as shown below.

- **Group Type** to **ucd-mia**
- **ACD** to **y**
- **Queue** to **y**
- **Vector** to **y**

```

add hunt-group 90
                                     HUNT GROUP
                                     Page 1 of 4

Group Number: 90
Group Name: VoiceSales
Group Extension: 1800
Group Type: ucd-mia
TN: 1
COR: 1
Security Code:
ISDN/SIP Caller Display:

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

                                     ACD? y
                                     Queue? y
                                     Vector? y
                                     MM Early Answer? n
                                     Local Agent Preference? n

```

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

```
add hunt-group 90                                     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
```

Repeat the above steps to create hunt groups for other inbound services, should they be required.

5.1.1.2 Vectors

Enter the **change vector n** command, where **n** is the vector number. For this test simple routing was used to get the call to the agent. The call is queued to the skill set out on the VDN in the 1st Skill field on the next page.

```
change vector 19                                     Page 1 of 6
                                                    CALL VECTOR

                Number: 19      Name: DevConnect Vector
Multimedia? y      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
                Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
                Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
                Variables? y      3.0 Enhanced? y
01 queue-to      skill 1st pri m
02 wait-time      180 secs hearing ringback
03 stop
04
05
06
```

5.1.1.3 Vector Directory Numbers (VDN)

Enter the **add vdn n** command, where **n** is an available extension number. On **Page 1** assign a **Name** for the VDN and set the **Vector Number** to the relevant vector. The **1st Skill** should be set to that hunt group configured in **Section 5.1.1.1.2**.

```
add vdn 1900                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER
                                         Extension: 1900
                                         Name*: Sales
                                         Destination: Vector Number      19
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none      Report Adjunct Calls as ACD*? n

VDN of Origin Annc. Extension*:
1st Skill*: 90
2nd Skill*:

* Follows VDN Override Rules
```

5.1.1.4 Administer Class of Restriction

Enter the **change cor x** command where **x** corresponds to the Class of Restriction to be used for the agent login IDs in **Section 5.1.1.5**. On **Page 1**, set the **Direct Agent Calling** to **n**. This will allow agents to be called directly once they are logged in and in **Aux Work**. With **Direct Agent Calling** set to **y**, **POM** could not call the agent to **Nail Up** the call, the agent would send back a “no answer” as they were in **Aux Work**. Setting **Direct Agent Calling** to **n** solved this issue.

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

5.1.1.5 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. Ensure the **COR** field is set to **1** which relates to the COR configured in **Section 5.1.1.4**. The **Auto Answer** field is set to **station**. Configure a password as required.

```

add agent-loginID 1400                                     Page 1 of 2
                                AGENT LOGINID

Login ID: 1400                                           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 5.1.1.1** for **SN** and entering a skill level of **1** for **SL**. In this case, an agent able to handle both inbound and outbound calls is created. Set the **Direct Agent Skill** to the Inbound hunt group **90**.

```

change agent-loginID 1400                                 Page 2 of 2
                                AGENT LOGINID

Direct Agent Skill: 90                                   Service Objective? n
Call Handling Preference: skill-level                   Local Call Preference? n

  SN  RL  SL      SN  RL  SL
1: 10   1    16:
2: 90   1    17:
3:      18:
4:      19:
5:      20:
6:
7:
  
```

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

5.1.1.6 Administer Agent Stations

On **Page 4**, the following buttons were assigned for compliance testing, these may be altered depending on the customer requirements.

- **aux-work** – Agent is logged in to the ACD but is not available to take a call.
- **auto-in** - Agent is available to accept ACD calls.
- **manual-in** – Agent is available to accept ACD calls.
- **after-call** – Agent state after the ACD call is completed. The agent is not available.
- **release** – State when the call is dropped.

change station 1000		Page 4 of 5	
STATION			
SITE DATA			
Room:		Headset?	n
Jack:		Speaker?	n
Cable:		Mounting:	d
Floor:		Cord Length:	0
ABBREVIATED DIALING			
List1:	List2:	List3:	
BUTTON ASSIGNMENTS			
1: call-appr		5: auto-in	Grp:
2: call-appr		6: manual-in	Grp:
3: call-appr		7: release	
4: aux-work	RC: Grp:	8: after-call	

Note: The same changes on SIP stations are made using System Manager (not shown).

5.1.2. Configuration of the SIP Trunk and 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
- Configure SIP Trunk

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

5.1.2.1 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 11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 12000 250
      Maximum Concurrently Registered IP Stations: 18000 2
      Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
      Maximum Concurrently Registered IP eCons: 414 0
      Max Concur Registered Unauthenticated H.323 Stations: 100 0
      Maximum Video Capable Stations: 18000 0
      Maximum Video Capable IP Softphones: 18000 0
      Maximum Administered SIP Trunks: 24000 319
      Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
```

On **Page 3**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

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

Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
Access Security Gateway (ASG)? n          Authorization Codes? y
Analog Trunk Incoming Call ID? y          CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y   CAS Main? n
Answer Supervision by Call Classifier? y    Change COR by FAC? n
      ARS? y Computer Telephony Adjunct Links? y
      ARS/AAR Partitioning? y Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? y            DCS (Basic)? y
```

On **Page 5**, ensure that **Uniform Dialing Plan** is set to **y**.

```
display system-parameters customer-options                               Page 5 of 11
                                OPTIONAL FEATURES
                                Multinational Locations? n           Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n       Station as Virtual Extension? y
                                Multiple Locations? n
                                System Management Data Transfer? n
Personal Station Access (PSA)? y               Tenant Partitioning? y
                                PNC Duplication? n                 Terminal Trans. Init. (TTI)? y
Port Network Support? y                       Time of Day Routing? y
                                Posted Messages? y                TN2501 VAL Maximum Capacity? y
                                Uniform Dialing Plan? y
                                Private Networking? y              Usage Allocation Enhancements? y
```

5.1.2.2 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 11** 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? n
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? no
                                DID/Tie/ISDN/SIP Intercept Treatment: attd
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                                Automatic Circuit Assurance (ACA) Enabled? n
                                Abbreviated Dial Programming by Assigned Lists? n
Auto Abbreviated/Delayed Transition Interval (rings): 2
                                Protocol for Caller ID Analog Terminals: Bellcore
Display Calling Number for Room to Room Caller ID Calls? 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

```

5.1.2.3 Administer Dial Plan

It was decided for compliance testing that all calls to the “PSTN” were calls that began with **351212** and these were to be sent across the SIP trunk to Session Manager and then onto the Session Border Controllers and the simulated PSTN. To achieve this routing, 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 **351212** is of call type **udp** which means any numbers beginning with 351212 are a part of the uniform dial plan.

```

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
    351212    12  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

```

5.1.2.4 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 **351212** will use ARS. No further digits are deleted or inserted. Calls are sent to **ars** for further processing.

```
change uniform-dialplan 6                                     Page 1 of 2
                                UNIFORM DIAL PLAN TABLE
                                                Percent Full: 0
```

Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num
351212	12	0		ars	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 **351212xxxxxx** and are matched with the ARS entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

```
change aar analysis 6                                       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
351212	12	12	1	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 **1** is used to route calls to trunk group (**Grp No**) **1**, this is the SIP Trunk configured in **Section 5.1.2.5**. The **Numbering Format** was set to **lev0-pvt**.

```

change route-pattern 1                               Page 1 of 3
                Pattern Number: 1           Pattern Name: SIP TRUNK
  SCCAN? n      Secure SIP? n      Used for SIP stations? n

  Grp FRL NPA Pfx Hop Toll No.  Inserted          DCS/ IXC
  No          Mrk Lmt List Del  Digits          QSIG
                                         Dgts      Intw
1: 1         0
2:
3:
4:
5:
6:

          BCC VALUE  TSC CA-TSC      ITC BCIE Service/Feature PARM Sub  Numbering LAR
          0 1 2 M 4 W      Request          Dgts  Format
1: y y y y y n  n          unre          lev0-pvt none
2: y y y y y n  n          rest          none
3: y y y y y n  n          rest          none
4: y y y y y n  n          rest          none
5: y y y y y n  n          rest          none
6: y y y y y n  n          rest          none

```

5.1.2.5 Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the **procr** and Session Manager (**SM81vmpg**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

```

display node-names ip                               IP NODE NAMES
  Name          IP Address
AMS81vmpg      10.10.40.61
G450           10.10.40.14
IPOffice       10.10.40.25
SM81vmpg     10.10.40.32
SM_Oceana     10.10.41.26
aes81vmpg     10.10.40.38
default       0.0.0.0
procr       10.10.40.37

( 16 of 18  administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

```

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **devconnect.local**. The **IP Network Region** form also specifies the **IP Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

```

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

```

In the **IP Codec Set** form, select the audio codecs supported for calls routed over the SIP trunk to the Simulated PSTN. The form is accessed via the **display ip-codec-set n** command. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), **G.711MU** (mu-law) and **G.729A** which are supported by the PSTN.

Media Encryption is used on the Avaya sets where possible these use **srtp-aescm128-hmac80** media encryption. **None** is also present to facilitate any extension not capable of handling encryption.

```

display ip-codec-set 1                                       Page 1 of 2
                                                    IP MEDIA PARAMETERS
Codec Set: 1
Audio          Silence      Frames   Packet
Codec          Suppression  Per Pkt  Size(ms)
1: G.711A      n                2        20
2: G.711MU    n                2        20
3: G.729A     n                2        20
4:
Media Encryption
1: 1-srtp-aescm128-hmac80
2: none
3:
Encrypted SRTCP: enforce-unenc-srtcp

```

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method, **tls** (Transport Layer Security) should be used for DevConnect testing.
- The **Peer Detection Enabled** field should be set to **y** allowing Communication Manager to automatically detect if the peer server is a Session Manager.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM81vmpg**), also shown above.
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above. This field logically establishes the **far-end** for calls using this signaling group as network region **1**.
- The **Far-end Domain** field can be set to the domain name specified in the IP Network Region.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- The default values for the other fields may be used.

Note: These were the settings for compliance testing, however, this trunk may be setup differently on each customer site depending on the customer's requirements for SIP routing.

```

change signaling-group 1                               Page 1 of 2
                                SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                       Transport Method: tls
  Q-SIP? n
  IP Video? n                          Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr              Far-end Node Name: SM81vmpg
Near-end Listen Port: 5061            Far-end Listen Port: 5061
                                      Far-end Network Region: 1

Far-end Domain: devconnect.local

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

```

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from the PSTN. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```

change trunk-group 1                                     Page 1 of 5
                                     TRUNK GROUP

Group Number: 1                Group Type: sip                CDR Reports: y
  Group Name: SIPTRUNK                COR: 1                TN: 1                TAC: *801
    Direction: two-way                Outgoing Display? n
Dial Access? n                Night Service:
Queue Length: 0
Service Type: tie                Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 1
                                     Number of Members: 10

```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with Inisoft to prevent unnecessary SIP messages during call setup. For the compliance test a value of **600** was used.

```

change trunk-group 1                                     Page 2 of 5
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                     Redirect On OPTIM Failure: 5000

  SCCAN? n                Digital Loss Group: 18
    Preferred Minimum Session Refresh Interval(sec): 600

Disconnect Supervision - In? y Out? y

  XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n

Caller ID for Service Link Call to H.323 1xC: station-extension

```

Settings on **Page 5** are as follows.

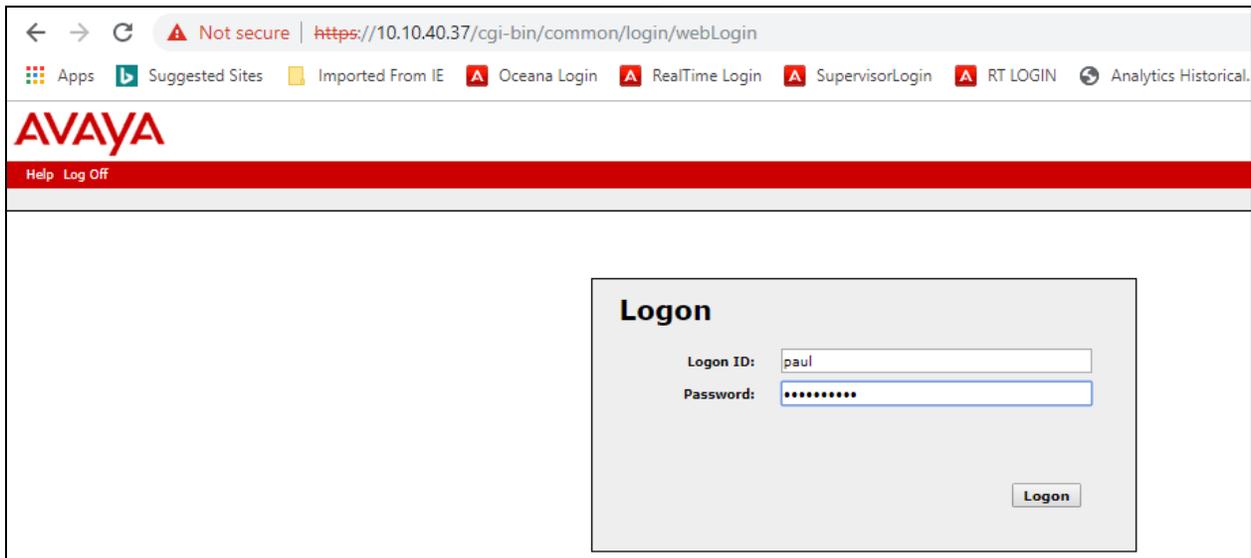
```
change trunk-group 1 Page 5 of 5
                                PROTOCOL VARIATIONS
                                Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                                Send Transferring Party Information? y
                                Network Call Redirection? y
Build Refer-To URI of REFER From Contact For NCR? n
                                Send Diversion Header? n
                                Support Request History? y
                                Telephone Event Payload Type: 101

                                Convert 180 to 183 for Early Media? n
                                Always Use re-INVITE for Display Updates? n
                                Identity for Calling Party Display: P-Asserted-Identity
Block Sending Calling Party Location in INVITE? n
                                Accept Redirect to Blank User Destination? n
                                Enable Q-SIP? n

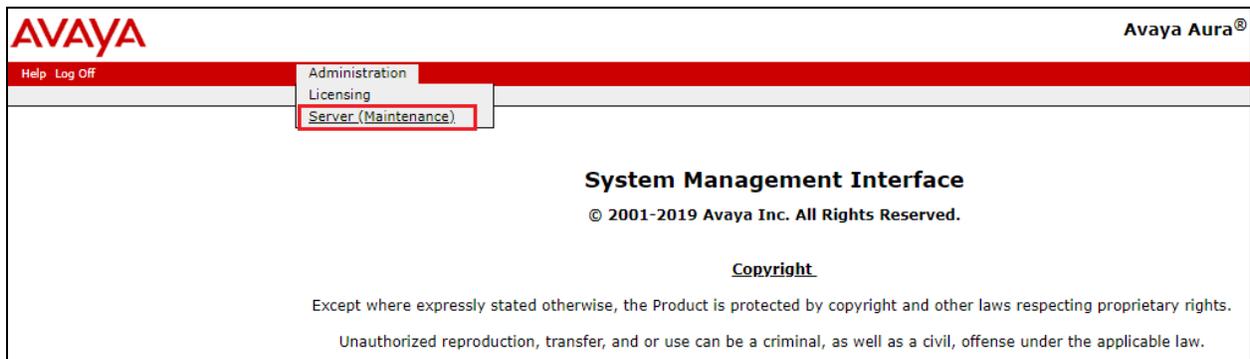
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
Request URI Contents: may-have-extra-digits
```

5.1.3. Configure Proactive Outreach Manager User

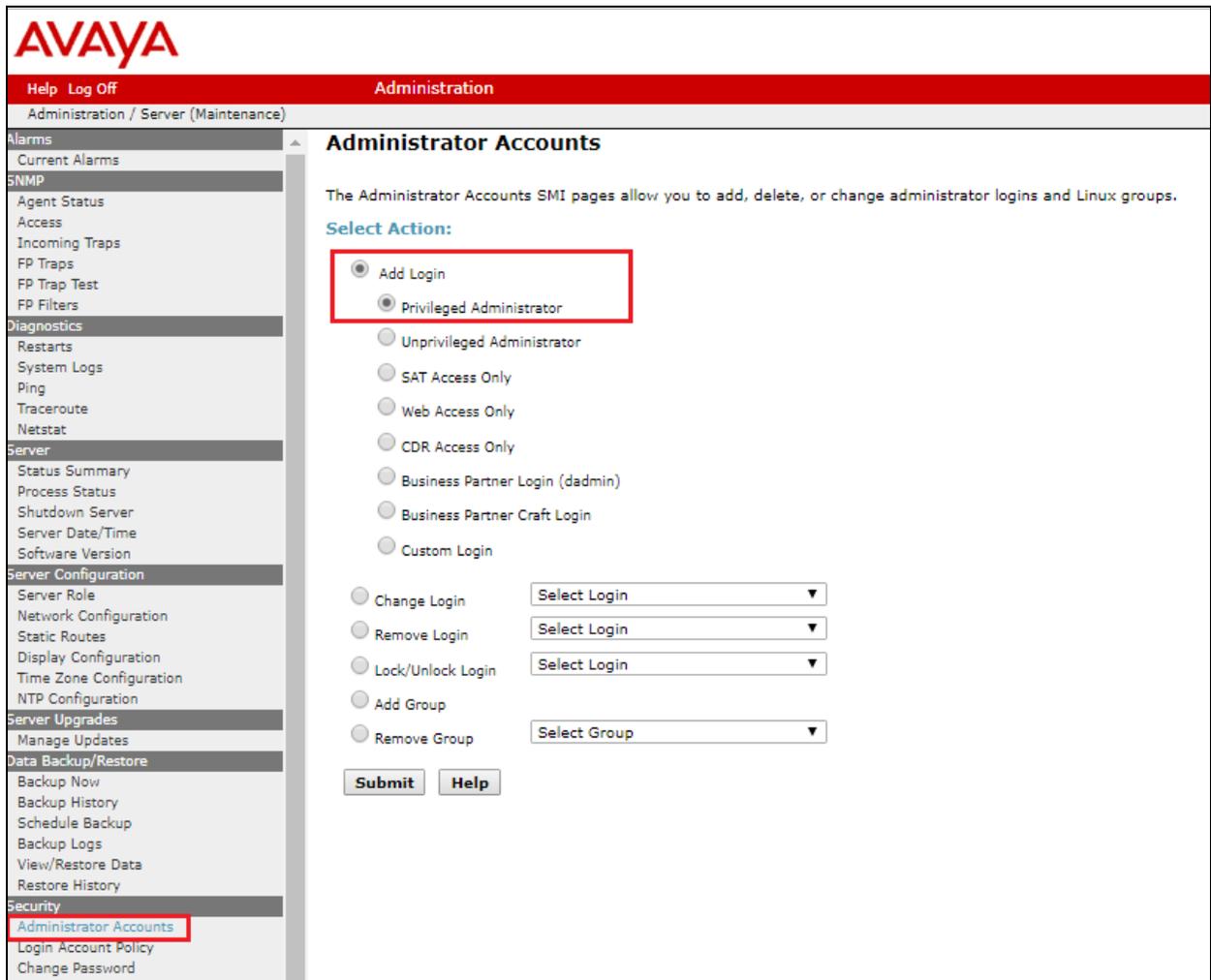
A user must be created on Communication Manager for POM to connect and nail up an outbound call using the outbound hunt group. Open a URL to the IP address of Communication Manager and use the appropriate credentials to log in as shown below.



Select **Server (Maintenance)** from the drop-down menu as shown below.



Navigate to **Security** → **Administrator Accounts** in the left window and select **Add Login** and **Privileged Administrator** in the main window.



The user **pomout** was created and this user is reference in the POM CTI configuration details as shown in **Section 7.3**.

Administrator Accounts -- Add Login: Privileged Administrator

This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest access privileges in the system next to root.

Login name	<input type="text" value="pomout"/>
Primary group	<input type="text" value="susers"/>
Additional groups (profile)	<input type="text" value="prof18"/>
Linux shell	<input type="text" value="/bin/bash"/>
Home directory	<input type="text" value="/var/home/pomout"/>
Lock this account	<input type="checkbox"/>
SAT Limit	<input type="text" value="none"/>
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	<input type="text"/>
Enter password	<input type="password" value="....."/>
Re-enter password	<input type="password" value="....."/>
Force password change on next login	<input checked="" type="radio"/> No <input type="radio"/> Yes

5.2. Configuration of the connection to the Avaya Aura® Application Enablement Services

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

- Note procr IP Address
- Configure Transport Link
- Configure CTI Link for TSAPI Service

5.2.1. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the procr IP Address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aes81vmpg**).

```
display node-names ip                                     Page 1 of 2
```

IP NODE NAMES	
Name	IP Address
SM100	10.10.40.52
aes81vmpg	10.10.40.38
default	0.0.0.0
g450	10.10.40.15
procr	10.10.40.37

5.2.2. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** should be set to **AESVCS**
- **Enabled:** set to **y**
- **Local Node:** set to the node name assigned for the **procr** in **Section 5.2.1**
- **Local Port** Retain the default value of **8765**

```
change ip-services                                     Page 1 of 4
```

IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes81vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

Note: The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server, this is created as part of the AES installation, and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

```
change ip-services                                     Page 4 of 4
                                     AE Services Administration
```

Server ID	AE Services Server	Password	Enabled	Status
1:	aes81vmpg	*****	y	idle
2:				
3:				

5.2.3. Configure CTI Link for TSAPI Service

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

```
add cti-link 1                                     Page 1 of 3
                                     CTI LINK
```

CTI Link: 1
Extension: 2002
Type: ADJ-IP
Name: aes81vmpg
COR: 1

6. Configure Avaya Aura® Application Enablement Services

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

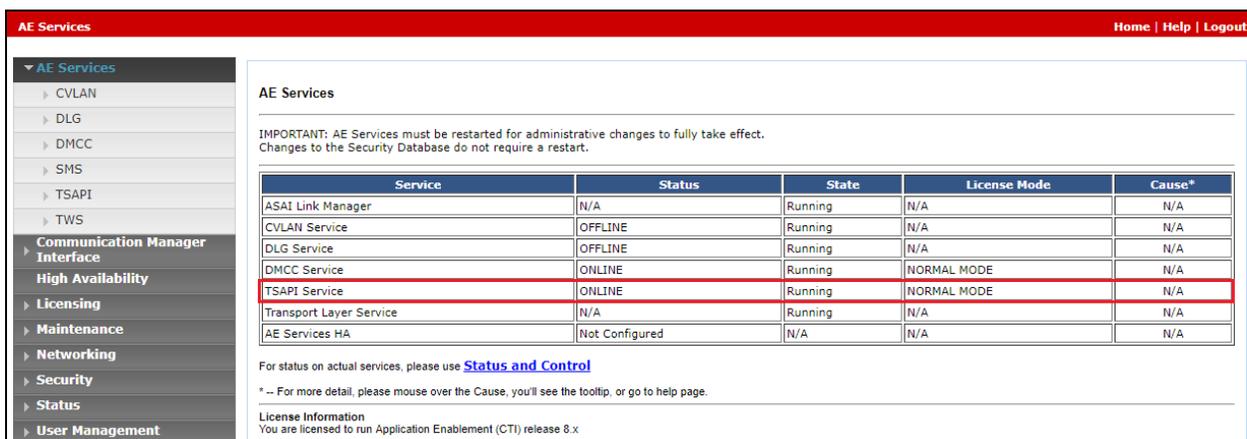
- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Create CTI User
- Configure Security Database
- Configure Networking Ports

6.1. Verify Licensing

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



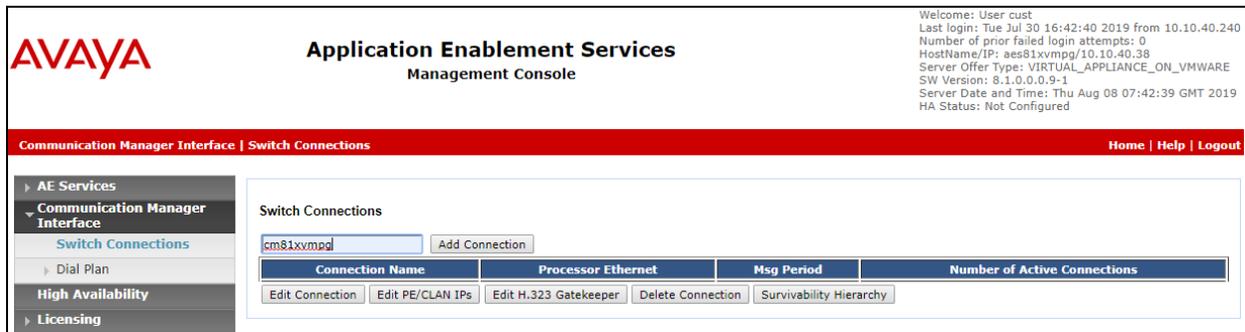
The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the **TSAPI Service** is licensed by ensuring that the **License Mode** is showing **NORMAL MODE**.



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

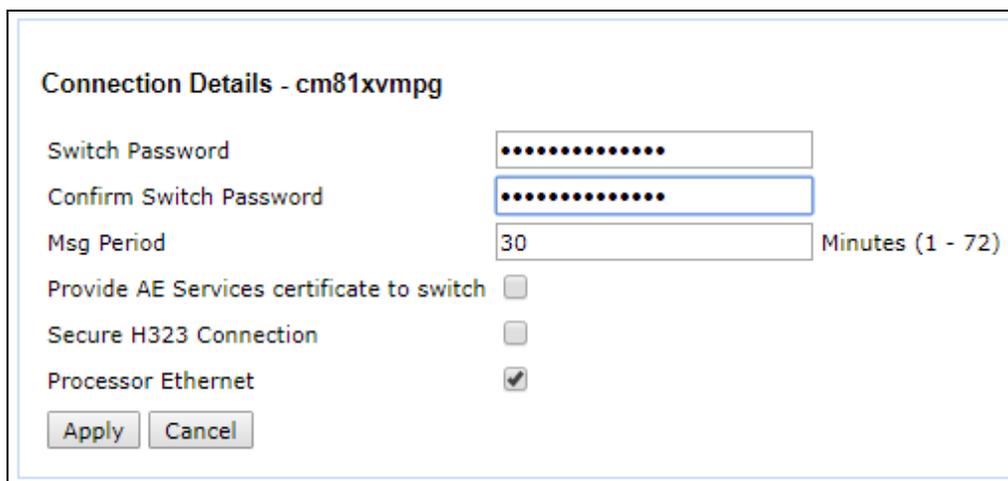
6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter in a name for the Switch Connection to be added and click the **Add Connection** button.



The screenshot shows the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title 'Application Enablement Services Management Console', and a user welcome message: 'Welcome: User cust', 'Last login: Tue Jul 30 16:42:40 2019 from 10.10.40.240', 'Number of prior failed login attempts: 0', 'HostName/IP: aes81xvmpg/10.10.40.38', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 8.1.0.0.0.9-1', 'Server Date and Time: Thu Aug 08 07:42:39 GMT 2019', and 'HA Status: Not Configured'. The main content area is titled 'Communication Manager Interface | Switch Connections' and features a sidebar with navigation options: 'AE Services', 'Communication Manager Interface', 'Switch Connections', 'Dial Plan', 'High Availability', and 'Licensing'. The main panel shows a table of 'Switch Connections' with columns for 'Connection Name', 'Processor Ethernet', 'Msg Period', and 'Number of Active Connections'. A table with one row is visible, and there are buttons for 'Add Connection', 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

In the resulting screen enter the **Switch Password**, the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.2.2**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.



The screenshot shows the 'Connection Details - cm81xvmpg' configuration form. It includes the following fields and options:

- Switch Password:** A text input field with masked characters (dots).
- Confirm Switch Password:** A text input field with masked characters (dots).
- Msg Period:** A text input field containing the value '30', with a label 'Minutes (1 - 72)' to its right.
- Provide AE Services certificate to switch:** A checkbox that is currently unchecked.
- Secure H323 Connection:** A checkbox that is currently unchecked.
- Processor Ethernet:** A checkbox that is currently checked.
- Buttons:** 'Apply' and 'Cancel' buttons are located at the bottom of the form.

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button.

Switch Connections

Connection Name	Processor Ethernet	Msg Period	
<input checked="" type="radio"/> cm81xvmpg	Yes	30	1

In the resulting screen, enter the IP address of the **procr** as shown in **Section 5.2.1** that will be used for the AES connection and select the **Add Name or IP** button.

Edit Processor Ethernet IP - cm81xvmpg

Name or IP Address
10.10.40.37

6.3. Administer TSAPI link

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

AVAYA **Application Enablement Services**
Management Console

AE Services | TSAPI | TSAPI Links

- ▼ AE Services
 - ▶ CVLAN
 - ▶ DLG
 - ▶ DMCC
 - ▶ SMS
 - ▼ TSAPI
 - **TSAPI Links**
 - TSAPI Properties
 - ▶ TWS

TSAPI Links

Link	Switch Connection	Switch CTI Link #

On the **Add TSAPI Links** screen, enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm81xvmpg**, which has already been configured in **Section 6.2**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.2.3**.
- **ASAI Link Version:** This can be left at the default value of **8**.
- **Security:** This can be left at the default value. The value **both** was used in this test.
- Once completed, select **Apply Changes**.

Edit TSAPI Links

Link: 1

Switch Connection: cm81xvmpg

Switch CTI Link Number: 1

ASAI Link Version: 8

Security: Both

Buttons: Apply Changes, Cancel Changes, Advanced Settings

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

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.

! Please use the Maintenance -> Service Controller page to restart the TSAPI server.

Buttons: Apply, Cancel

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

Service Controller

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

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

Buttons: Start, Stop, Restart Service, Restart AE Server

6.4. Create CTI User

A user ID and password need to be configured for the Syntelate XA server to communicate as a TSAPI client with the Application Enablement Services. Navigate to the **User Management** → **User Admin** and choose **Add User**. In the **Add User** screen, enter the following values:

- **User Id** – This will be used by the Syntelate XA server.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used by the Syntelate XA server.
- **CT User** - Select **Yes** from the drop-down menu.

Complete the process by choosing **Apply** at the bottom of the screen.

The screenshot shows the 'Add User' form within the 'User Management | User Admin | Add User' interface. The left sidebar contains a navigation menu with 'User Management' expanded to show 'Add User' as the selected option. The main form area is titled 'Add User' and includes a note: 'Fields marked with * can not be emotv.' The form fields are as follows:

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

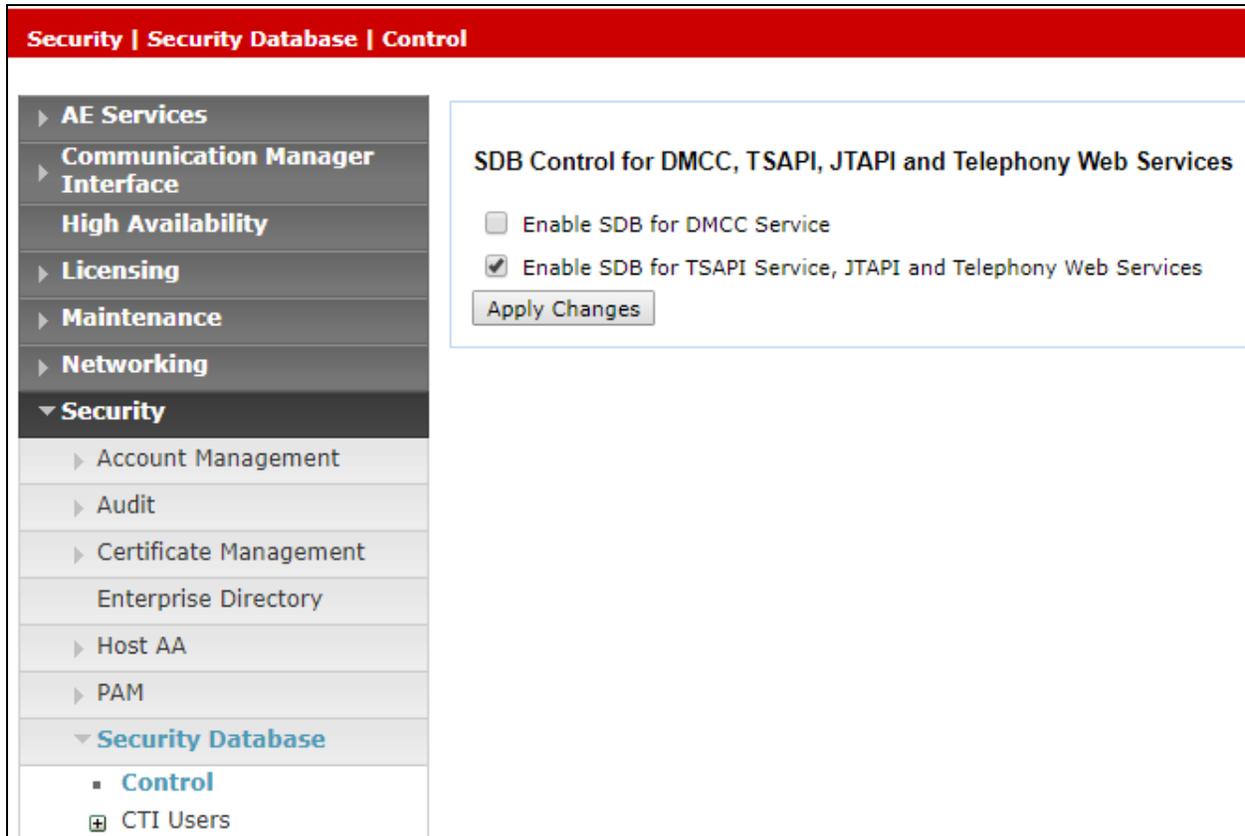
At the bottom of the form, there are 'Apply' and 'Cancel' buttons.

6.5. Configure Security Database

The security database must be configured to allow the user “inisoft” monitor and receive events from the Avaya endpoints. The following steps ensure that this will happen.

6.5.1. Configure Security Database Control for TSAPI

Navigate to selecting **Security** → **Security Database** → **Control**. By default, the **Enable SDB for TASPI Service, JTAPI and Telephony Web Services** is ticked, as shown below.



The screenshot shows a web interface for configuring the Security Database. The breadcrumb navigation at the top reads "Security | Security Database | Control". On the left is a navigation tree with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control (selected), and CTI Users. The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two checkboxes: "Enable SDB for DMCC Service" (unchecked) and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services" (checked). An "Apply Changes" button is located below the checkboxes.

6.5.2. Edit CTI User

Navigate to the **CTI Users** screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the user that was created in **Section 6.4** and select the **Edit** button.

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> inisoft	inisoft	NONE	NONE
<input type="radio"/> paul	Paul	NONE	NONE

The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

Edit CTI User

User Profile: User ID: inisoft
Common Name: inisoft
Worktop Name: NONE ▼
Unrestricted Access:

Call and Device Control: Call Origination/Termination and Device Status: None ▼

Call and Device Monitoring: Device Monitoring: None ▼
Calls On A Device Monitoring: None ▼
Call Monitoring:

Routing Control: Allow Routing on Listed Devices: None ▼

6.5.3. Identify Tlinks

Click on **Tlinks**. Verify the value of the **Tlink Name**. This will be used by the Syntelate XA application.

The screenshot displays the Syntelate XA application interface. On the left is a navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control, CTI Users, Devices, Device Groups, **Tlinks** (highlighted), Tlink Groups, and Worktops. The main content area on the right is titled "Tlinks" and contains the following elements: "Tlink Name" label, two radio button options: "AVAYA#CM81XVMPG#CSTA#AES81XVMPG" (selected) and "AVAYA#CM81XVMPG#CSTA-S#AES81XVMPG", and a "Delete Tlink" button.

6.6. Configure Networking Ports

To ensure that TSAPI ports are enabled, navigate to **Networking** → **Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.

Networking | Ports

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▼ Networking
- AE Service IP (Local IP)
- Network Configure
- Ports
- TCP/TLS Settings
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Ports

CVLAN Ports		Enabled	Disabled
Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>	<input checked="" type="radio"/>	<input type="radio"/>

DLG Port	TCP Port	5678	
----------	----------	------	--

TSAPI Ports		Enabled	Disabled
TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports			
TCP Port Min	1024		
TCP Port Max	1039		
Unencrypted TLINK Ports			
TCP Port Min	<input type="text" value="1050"/>		
TCP Port Max	<input type="text" value="1065"/>		
Encrypted TLINK Ports			
TCP Port Min	<input type="text" value="1066"/>		
TCP Port Max	<input type="text" value="1081"/>		

DMCC Server Ports		Enabled	Disabled
Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	<input type="text" value="4723"/>	<input checked="" type="radio"/>	<input type="radio"/>

H.323 Ports		Enabled	Disabled
TCP Port Min	<input type="text" value="20000"/>		
TCP Port Max	<input type="text" value="29999"/>		
Local UDP Port Min	<input type="text" value="20000"/>		
Local UDP Port Max	<input type="text" value="29999"/>		
Server Media		<input checked="" type="radio"/>	<input type="radio"/>
RTP Local UDP Port Min*	<input type="text" value="30000"/>		

PG; Reviewed:
SPOC 8/31/2019

Solution & Interoperability Test Lab Application Notes
©2019 Avaya Inc. All Rights Reserved.

34 of 68
Syntelate_POM31

Once all the necessary changes are made it is a good idea to restart of the AE Server. Navigate to **Maintenance** → **Service Controller**. In the main screen select **Restart AE Server** highlighted.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface, Licensing, Maintenance (highlighted with a red box), Date Time/NTP Server, Security Database, Service Controller (highlighted with a red box), Server Data, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Service Controller" and contains a table with the following data:

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

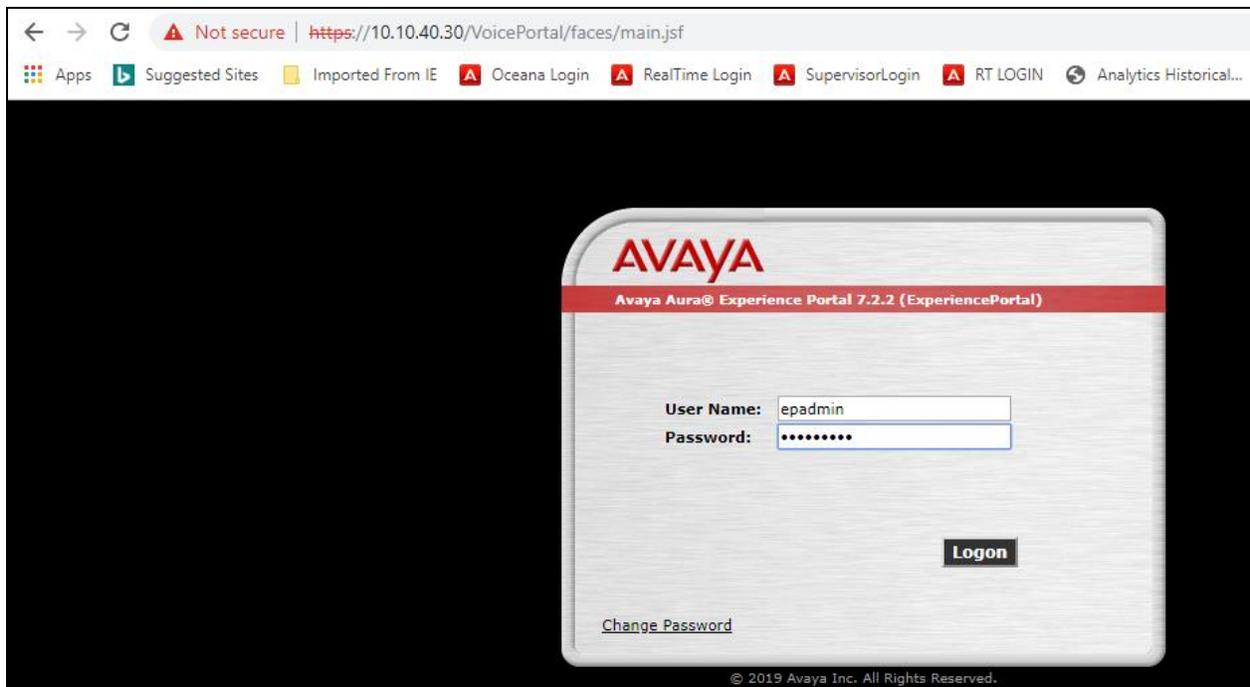
Below the table, there is a link for "Status and Control" and a row of buttons: Start, Stop, Restart Service, Restart AE Server (highlighted with a red box), Restart Linux, and Restart Web Server.

7. Configure Avaya Proactive Outreach Manager

This section describes the steps necessary to configure both POM and Experience Portal to allow Syntelate XA connect using the agent desktop. 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 AES. The setup and configuration of these connections are therefore outside the scope of these Application Notes.

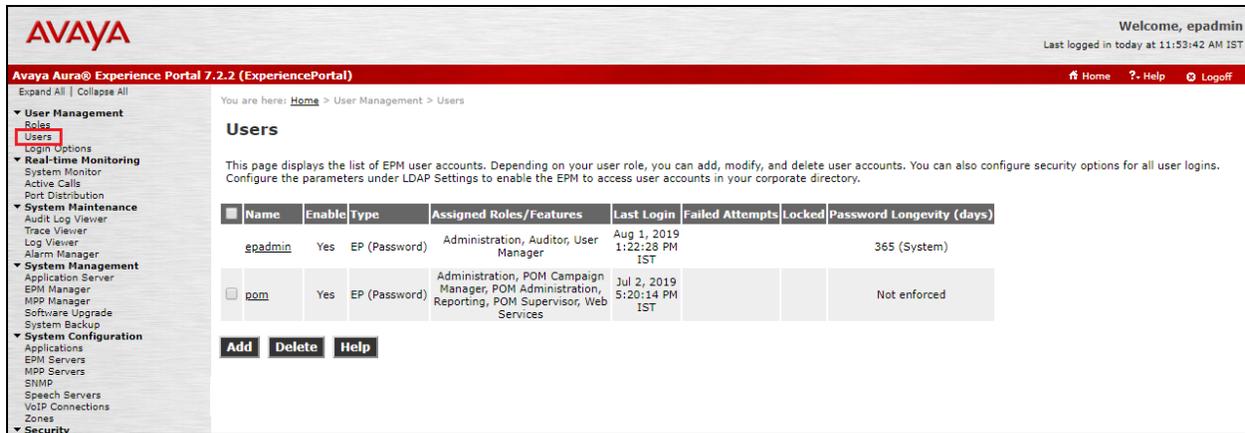
Experience Portal is configured via the Experience Portal Manager (EPM) web interface. To access the web interface, enter `http://[IP-Address]/` as the URL in an internet browser, where IP-Address is the IP address of the EPM. Log in using the Administrator user role. The screen shown below is displayed.



Note: 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.

7.1. Add a User on Avaya Aura® Experience Portal

A user is created on Experience Portal to allow the Syntelate XA server connect to POM. Navigate to **User Management** → **Users** in the left window.



AVAYA Welcome, epadmin
Last logged in today at 11:53:42 AM IST

Avaya Aura® Experience Portal 7.2.2 (ExperiencePortal) Home Help Logoff

You are here: Home > User Management > Users

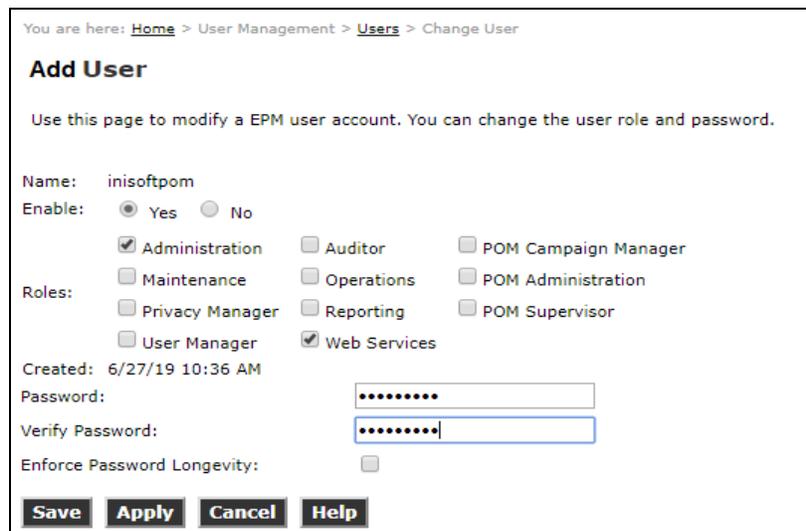
Users

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

Name	Enable	Type	Assigned Roles/Features	Last Login	Failed Attempts	Locked	Password Longevity (days)
epadmin	Yes	EP (Password)	Administration, Auditor, User Manager	Aug 1, 2019 1:22:28 PM IST			365 (System)
<input type="checkbox"/> pom	Yes	EP (Password)	Administration, POM Campaign Manager, POM Administration, Reporting, POM Supervisor, Web Services	Jul 2, 2019 5:20:14 PM IST			Not enforced

Add **Delete** **Help**

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



You are here: Home > User Management > Users > Change User

Add User

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

Name: inisoftpom

Enable: Yes No

Roles:

- Administration
- Auditor
- POM Campaign Manager
- Maintenance
- Operations
- POM Administration
- Privacy Manager
- Reporting
- POM Supervisor
- User Manager
- Web Services

Created: 6/27/19 10:36 AM

Password:

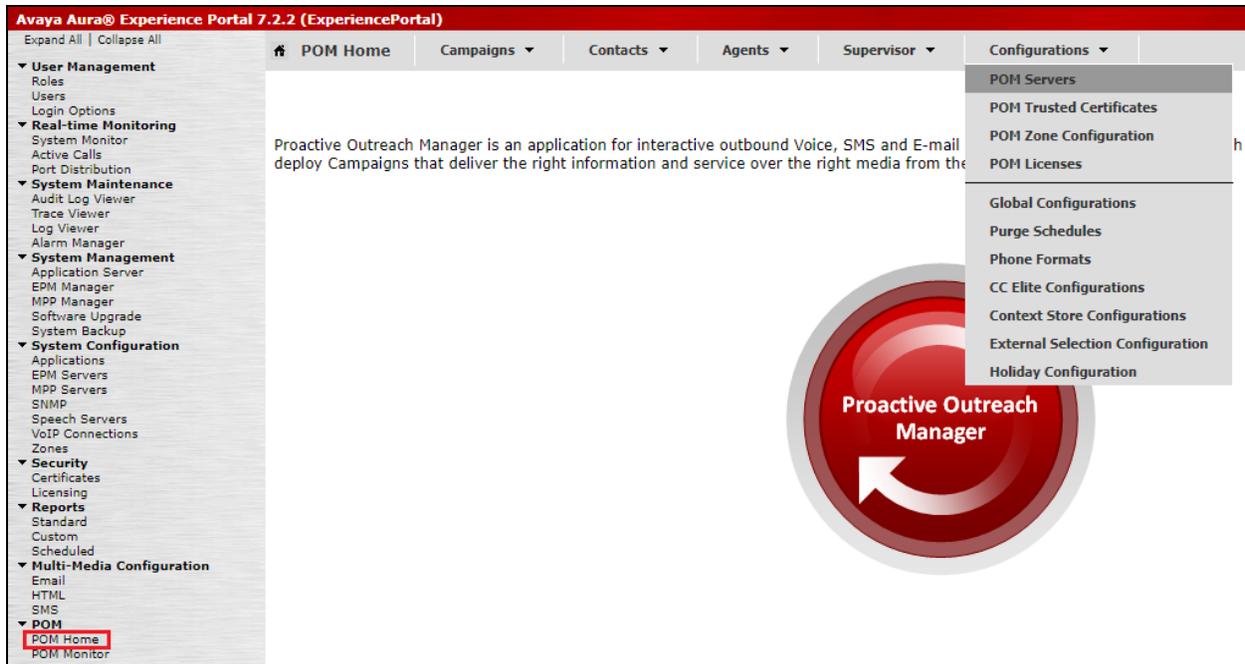
Verify Password:

Enforce Password Longevity:

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

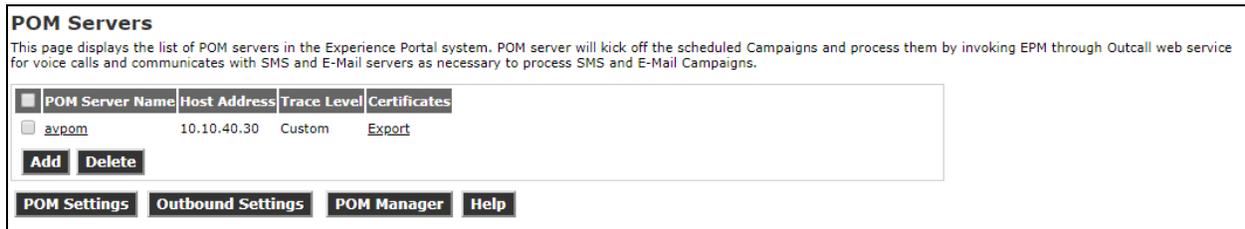
7.2. Display Configuration of POM Server

Information on the POM server can be found by navigating to **POM → POM Home** in the left window and selecting **Configurations → POM Servers** in the main window.



The screenshot shows the Avaya Aura Experience Portal 7.2.2 interface. The left sidebar contains a navigation menu with categories like User Management, Real-time Monitoring, System Maintenance, System Management, System Configuration, Security, Reports, Multi-Media Configuration, and POM. The POM category is expanded, showing POM Home and POM Monitor. The main content area displays the POM Home page with a description of Proactive Outreach Manager. A dropdown menu is open under Configurations, showing options like POM Servers, POM Trusted Certificates, POM Zone Configuration, POM Licenses, Global Configurations, Purge Schedules, Phone Formats, CC Elite Configurations, Context Store Configurations, External Selection Configuration, and Holiday Configuration. A red circular graphic with a white arrow and the text 'Proactive Outreach Manager' is overlaid on the right side of the screenshot.

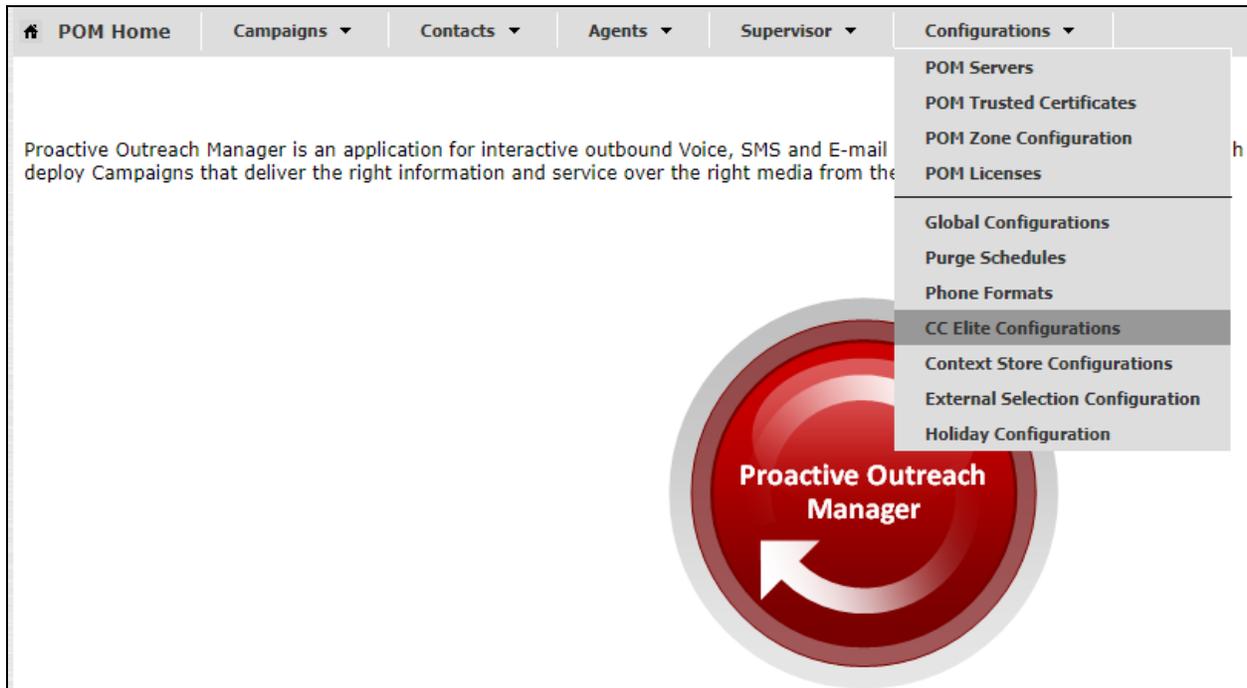
Information on the POM server can be found by either selecting the **POM Server Name** or the various buttons underneath that.



The screenshot shows the POM Servers configuration page. The page title is 'POM Servers'. Below the title is a description: 'This page displays the list of POM servers in the Experience Portal system. POM server will kick off the scheduled Campaigns and process them by invoking EPM through Outcall web service for voice calls and communicates with SMS and E-Mail servers as necessary to process SMS and E-Mail Campaigns.' Below the description is a table with columns: POM Server Name, Host Address, Trace Level, and Certificates. The table contains one row with the value 'avpom', '10.10.40.30', 'Custom', and 'Export'. Below the table are 'Add' and 'Delete' buttons. At the bottom of the page are four buttons: 'POM Settings', 'Outbound Settings', 'POM Manager', and 'Help'.

7.3. Display the Configuration of the CTI connection

Select **Configuration** → **CC Elite Configurations** from the main window.



Aura81 was the CTI group already setup for compliance testing, clicking on this will open the connection to show the details.

Configure CTI setup details, CMS setup details and POM Skills [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: 08/01/2019 01:24:58 PM

CTI Configuration

CTI Group Name	CM IP Address	CM Login	AES IP Address	AES Secure Connection	CTI Group Role	Action
OutboundCTI	10.10.40.59	pomout	10.10.40.56	false	Select	
Aura81	10.10.40.37	pomout	10.10.40.38	false	Active	

Add CTI Detail **Help**

CMS Configuration

Server IP Port	Server Role†	Agent Thrashing Interval (seconds)	Action
----------------	--------------	------------------------------------	--------

Add CMS Configuration **Help**

Information such as the IP Address of Communication Manager and the AES are stored here as well as the Communication Manager user created in **Section 5.1.3**.

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**

From the **Configure CTI setup details, CMS setup and POM Skills** 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.

Configure CTI setup details, CMS setup details and POM Skills

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

Refresh

Last poll: 08/01/2019 01:27:47 PM

CTI Configuration

CTI Group Name	CM IP Address	CM Login	AES IP Address	AES Secure Connection	CTI Group Role	Action
OutboundCTI	10.10.40.59	pomout	10.10.40.56	false	Select	
Aura81	10.10.40.37	pomout	10.10.40.38	false	Active	

Add CTI Detail **Help**

CMS Configuration

Server IP Port	Server Role	Agent Threshing Interval (seconds)	Action

Add CMS Configuration **Help**

Skillset name

Skillset type Skills

Show

CC Elite Skill Number	POM Skill Name	Skill Type	Parameter to Monitor for Blending	EWT levels	Agent Acquire Threshold	Agent Release Threshold
10	Outbound	Outbound	-	-	0	0

Add Skill **Help**

The skillset number must match that of the hunt group created in **Section 5.1.1.1.1**, this was hunt group **10** used for outbound calls.

CC Elite Skill Number	POM Skill Name	Skill Type	Parameter to Monitor for Blending	EWT levels	Agent Acq Threshold
<input type="text" value="10"/>	<input type="text" value="Outbound"/>	<input type="text" value="Outbound"/>	<input type="text" value="Select only for Inbound"/>	Select only for EWT <input type="text" value="Expected Wait Time(High)"/> <input type="text" value="Expected Wait Time(Medium)"/> <input type="text" value="Expected Wait Time(Low)"/>	<input type="text" value="0"/>

7.4. 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 setup and running prior to the connection from Syntelate XA. 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.

The following two campaigns were setup for compliance testing.

- **OutboundPreview** – this was 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 9.2.2**.
- **OutboundProgressive** – this was 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.

Campaign Manager

[Refresh](#)
Last poll: 08/01/2019 01:32:33 PM

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

[Advanced](#)

Show 50 | Page: 1/1

Name	Type	Campaign Strategy	Contact Lists	Last Executed	Waiting Callbacks	Actions
OutboundPreview	Finite	Preview	CMtoIPO	07/31/2019 03:01:00 PM 0		<input type="button" value="📄"/> <input type="button" value="🔄"/> <input type="button" value="📅"/> <input type="button" value="👉"/> <input type="button" value="📄"/> <input type="button" value="▶"/> <input type="button" value="📅"/> <input type="button" value="🗑️"/>
OutboundProgressive	Finite	OutProgressive	CMtoIPO	07/17/2019 04:20:30 PM 0		<input type="button" value="📄"/> <input type="button" value="🔄"/> <input type="button" value="📅"/> <input type="button" value="👉"/> <input type="button" value="📄"/> <input type="button" value="▶"/> <input type="button" value="📅"/> <input type="button" value="🗑️"/>

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

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

Campaign Manager

[Refresh](#)
Last poll: 08/01/2019 01:32:33 PM

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

[Advanced](#)

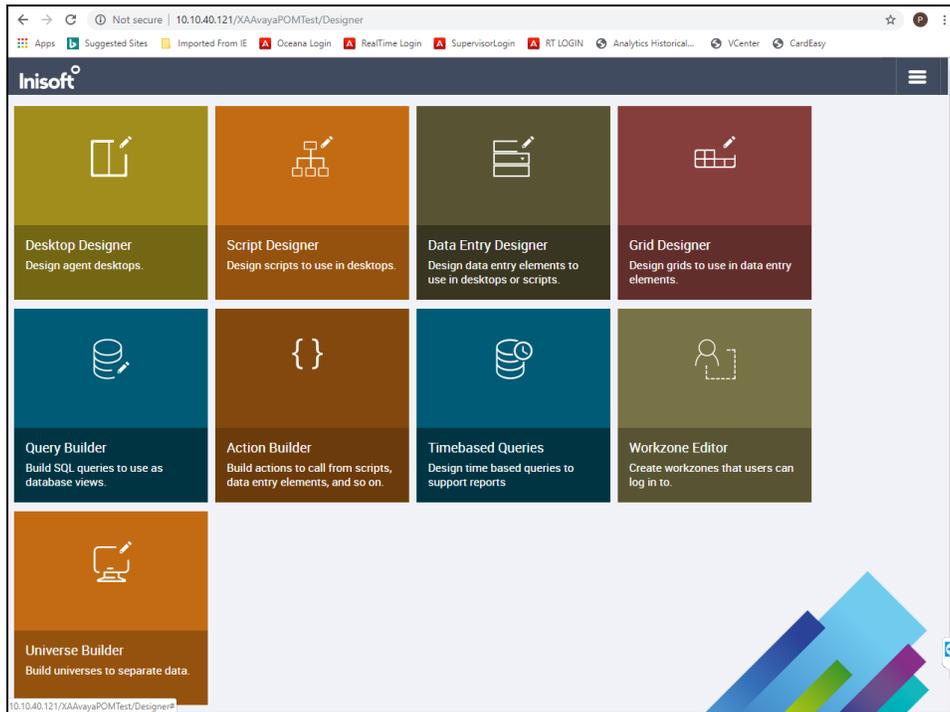
Show 50 | Page: 1/1

Name	Type	Campaign Strategy	Contact Lists	Last Executed	Waiting Callbacks	Actions
OutboundPreview	Finite	Preview	CMtoIPO	07/31/2019 03:01:00 PM 0		<input type="button" value="📄"/> <input type="button" value="🔄"/> <input type="button" value="📅"/> <input type="button" value="👉"/> <input type="button" value="📄"/> <input style="border: 2px solid red;" type="button" value="▶"/> <input type="button" value="📅"/> <input type="button" value="🗑️"/>
OutboundProgressive	Finite	OutProgressive	CMtoIPO	07/17/2019 04:20:30 PM 0		<input type="button" value="📄"/> <input type="button" value="🔄"/> <input type="button" value="📅"/> <input type="button" value="👉"/> <input type="button" value="📄"/> <input type="button" value="▶"/> <input type="button" value="📅"/> <input type="button" value="🗑️"/>

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

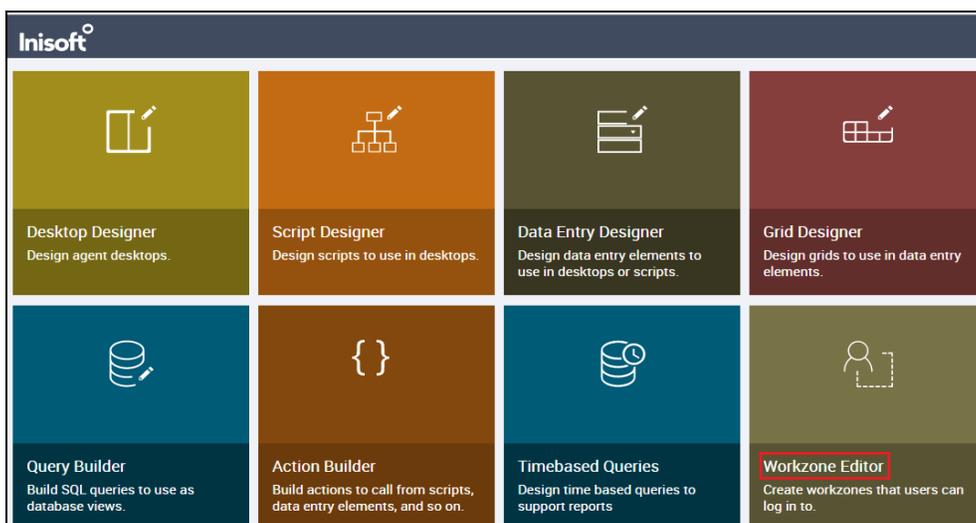
8. Configure Inisoft Syntelate XA

Configuration on the Syntelate XA server is carried out by opening a web browser to the Syntelate XA server's IP address. Open a URL to **http://<SyntelateXAServerIP>/XAAvayaPOMTest/Designer**, (note this will be different on each customer site, this was the address for the Avaya compliance testing).



8.1. Configure connection to Avaya Proactive Outreach Manager

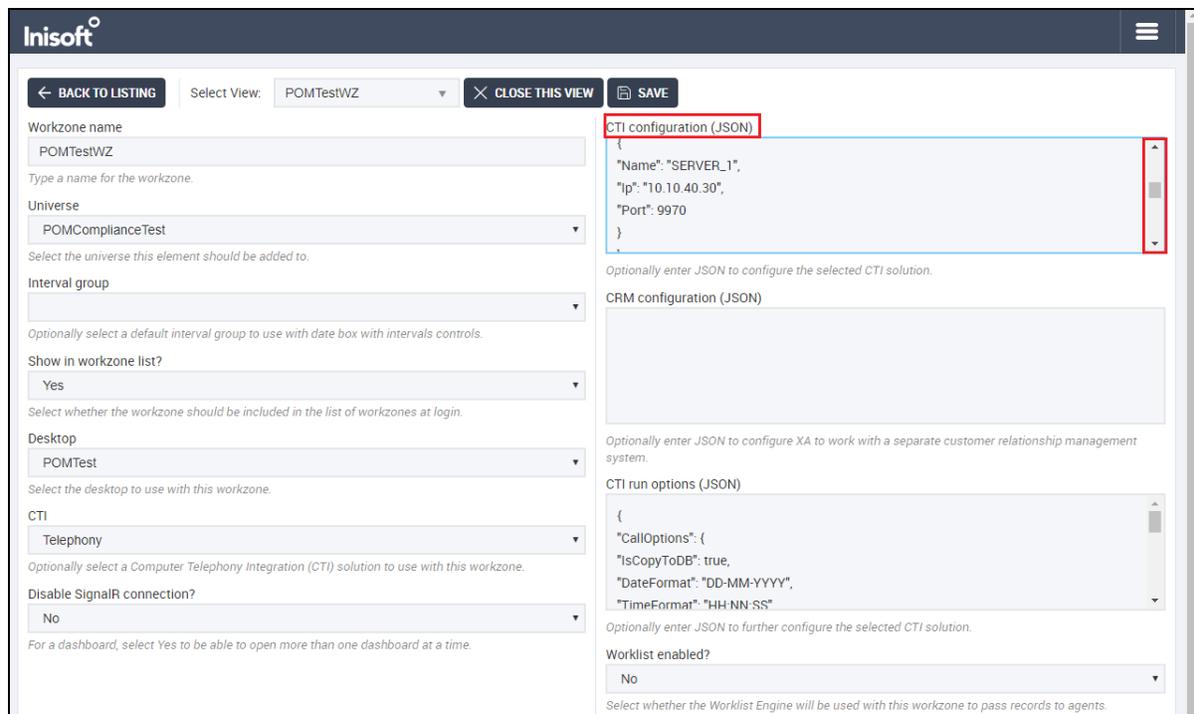
From the main page, click on **Workzone Editor**.



The following Workzones are already configured. Click on the edit icon on the appropriate Workzone to show the configuration details.

Name	Universe	Amended by	Amended at	Locked by	Locked at	
POMTestWZ - POM Only	POMComplianceTest	administrator	2019-07-10 10:39			 
POMTestWZ	POMComplianceTest	administrator	2019-07-03 09:11			 

The information on the connection to POM is located in the **CTI configuration (JSON)** window as shown below. Scroll down through this window to see the relevant information. The following displays the POM server IP address for **SERVER_1**.



Workzone name: POMTestWZ

Universe: POMComplianceTest

Interval group: [empty]

Show in workzone list: Yes

Desktop: POMTest

CTI: Telephony

Disable SignalR connection: No

CTI configuration (JSON)

```
{
  "Name": "SERVER_1",
  "Ip": "10.10.40.30",
  "Port": 9970
}
```

CRM configuration (JSON): [empty]

CTI run options (JSON)

```
{
  "CallOptions": {
    "IsCopyToDB": true,
    "DateFormat": "DD-MM-YYYY",
    "TimeFormat": "HH-NN-SS"
  }
}
```

Worklist enabled?: No

Scrolling further down shows the username and password configured in **Section 7.1**.

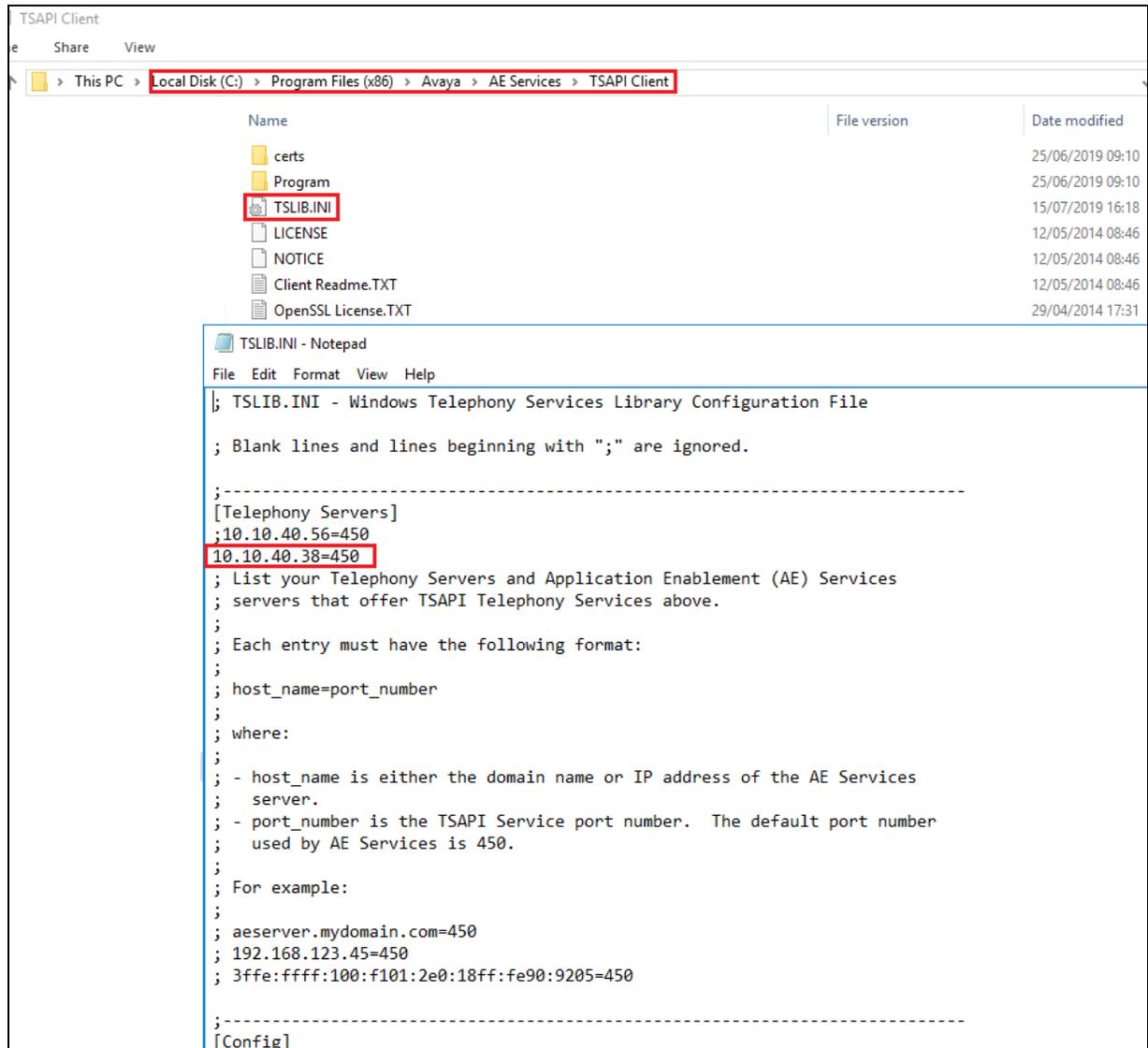
CTI configuration (JSON)

```
[,
  "WebService": {
    "Server": "https://10.10.40.30/axis2/services/VP_POMAgentAPIService",
    "Username": "inisoftpom",
    "Password": "XXXXXXXXXX"
  }
]
```

8.2. Configure connection to Avaya Aura® Application Enablement Services

It is assumed that the TSAPI Client has been installed as part of the TSAPI SDK. The IP Address for the AES is included in the TSLIB.INI file located on the Syntelate XA server.

From the Syntelate XA Server navigate to **Program Files (x86) → Avaya → AE Services → TSAPI Client**. Open the **TSLIB.INI** file in Notepad and the IP Address for the AES can be seen below or added if required.

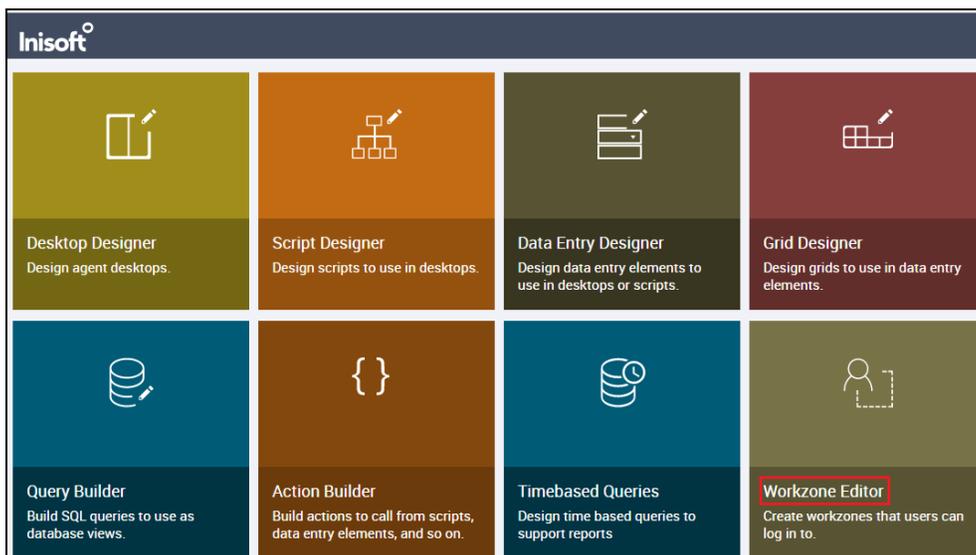


```
TSAPI Client
e  Share  View
> This PC > Local Disk (C:) > Program Files (x86) > Avaya > AE Services > TSAPI Client

Name                                     File version                               Date modified
-----
certs                                     25/06/2019 09:10
Program                                   25/06/2019 09:10
TSLIB.INI                                 15/07/2019 16:18
LICENSE                                   12/05/2014 08:46
NOTICE                                    12/05/2014 08:46
Client Readme.TXT                         12/05/2014 08:46
OpenSSL License.TXT                       29/04/2014 17:31

TSLIB.INI - Notepad
File Edit Format View Help
; TSLIB.INI - Windows Telephony Services Library Configuration File
; Blank lines and lines beginning with ";" are ignored.
;-----
[Telephony Servers]
;10.10.40.56=450
10.10.40.38=450
; List your Telephony Servers and Application Enablement (AE) Services
; servers that offer TSAPI Telephony Services above.
;
; Each entry must have the following format:
;
; host_name=port_number
;
; where:
;
; - host_name is either the domain name or IP address of the AE Services
; server.
; - port_number is the TSAPI Service port number. The default port number
; used by AE Services is 450.
;
; For example:
;
; aeserver.mydomain.com=450
; 192.168.123.45=450
; 3ffe:ffff:100:f101:2e0:18ff:fe90:9205=450
;-----
[Config]
```

Open a web browser to the Syntelate XA server as per **Section 8** and from the main page, click on **Workzone Editor**.

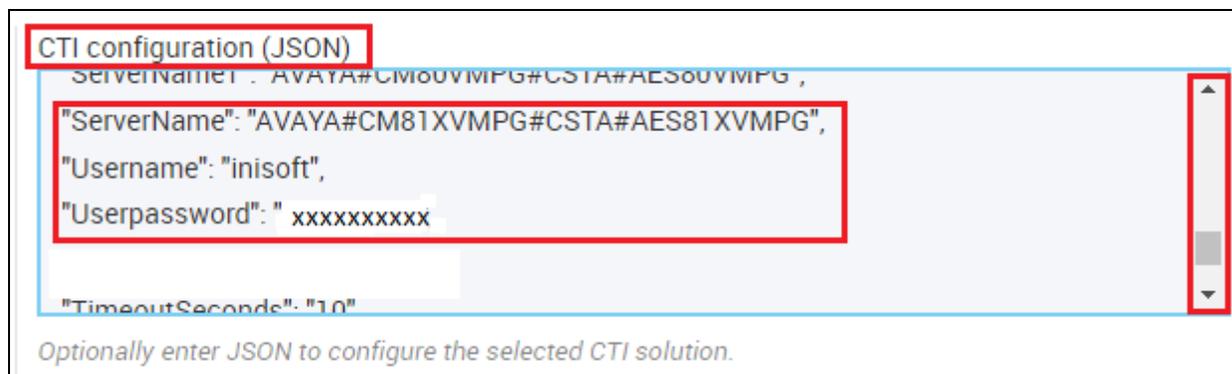


The following Workzones are already configured. Click on the edit icon on the appropriate Workzone to show the configuration details.

The screenshot shows the Workzone Editor interface. It includes a header with the Inisoft logo and a navigation bar with 'BACK TO TILES' and '+ NEW' buttons. Below the navigation bar is a table with the following data:

Name	Universe	Amended by	Amended at	Locked by	Locked at	Actions
POMTestWZ - POM Only	POMComplianceTest	administrator	2019-07-10 10:39			[Edit] [Add] [Delete]
POMTestWZ	POMComplianceTest	administrator	2019-07-03 09:11			[Edit] [Add] [Delete]

The information on the connection to AES is located in the CTI configuration (JSON) window as shown below. Scroll down through this window to see the relevant information. The following displays the AES username and password that was configured in **Section 6.4**.



9. Verification Steps

There are two connections that need to be verified one to POM and the other to AES. Each of these connections can be verified on POM and AES before any calls are made. The Syntelate XA desktop can be used to verify the connection also by making inbound VDN calls and starting the outbound campaign on POM.

9.1. Verify the Connection to Avaya Aura® Application Enablement Services

The connection to AES can be verified on the AES side and on the Syntelate XA side using the desktop to make and receive calls.

9.1.1. Verify the Connection from Avaya Aura® Application Enablement Services

Log into the AES as per **Section 6**. Once logged in, navigate to **Status** → **Status and Control** → **Switch Conn Summary** in the left window. The main window should display the connection state as **Talking** as it is shown below.

Switch Conn	Conn State	Processor Ethernet	Since	Online/Offline	Active/Standby/Admin'd AEP Conns	Num of TCI Conns	SSL	Msgs To Switch	Msgs From Switch	Msg Period
cm81xvmpg	Talking	Yes	Tue Jul 30 12:29:03 2019	Online	1 / 0 / 1	2	Enabled	645	662	30

Under **Status and Control**, navigate to **TSAPI Service Summary** and again the main window should display the **Status** as **Talking** as shown below. Click on the **User Status** button highlighted.

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	cm81xvmpg	1	Talking	Tue Jul 30 12:29:03 2019	Online	18	1	45	56	30

The **CTI User Status** should show the user created in **Section 6.4** as being connected as it shows below with the user **inisoft**.

CTI User Status

Enable page refresh every seconds

CTI Users

Open Streams 3
Closed Streams 46

Open Streams

Name	Time Opened	Time Closed	Tlink Name
inisoft	Thu 08 Aug 2019 10:39:19 AM IST		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 17 Jul 2019 11:56:54 AM IST		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Wed 17 Jul 2019 11:56:55 AM IST		AVAYA#CM81XVMPG#CSTA#AES81XVMPG

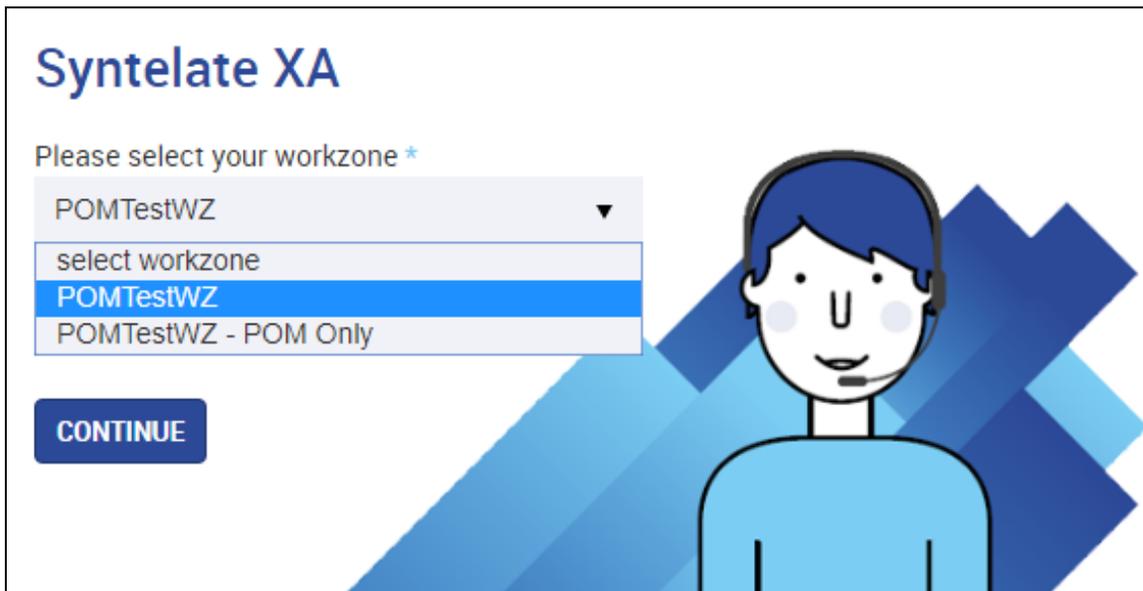
9.1.2. Verify the Connection from Syntelate XA Desktop

Open a URL to the Syntelate XA server IP address with the appropriate address. The example below is **http://<ServerIP>/XAAvayaPOMTest/**. A new window should appear looking for the username and password of the user setup on the domain or in this case the Syntelate XA server as there is no domain present. Enter the appropriate user/pass and click on **Sign in**.

The screenshot shows a web browser window with the address bar displaying `10.10.40.121/XAAvayaPOMTest/`. A "Sign in" dialog box is overlaid on the page. The dialog box contains the following text and fields:

- URL: `http://10.10.40.121`
- Warning: "Your connection to this site is not private"
- Username field: `Administrator`
- Password field: `.....`
- Buttons: `Sign in` and `Cancel`

The following window appears asking to select the **workzone**. The example below shows **POMTestWZ** being selected which is a blend of POM and AES connections.



Enter the appropriate Communication Manager credentials for **Agent ID**, **Extension** and the **Password** for this agent as per **Section 5.1.1**. Click on **LOG IN** to continue.

Telephony Login

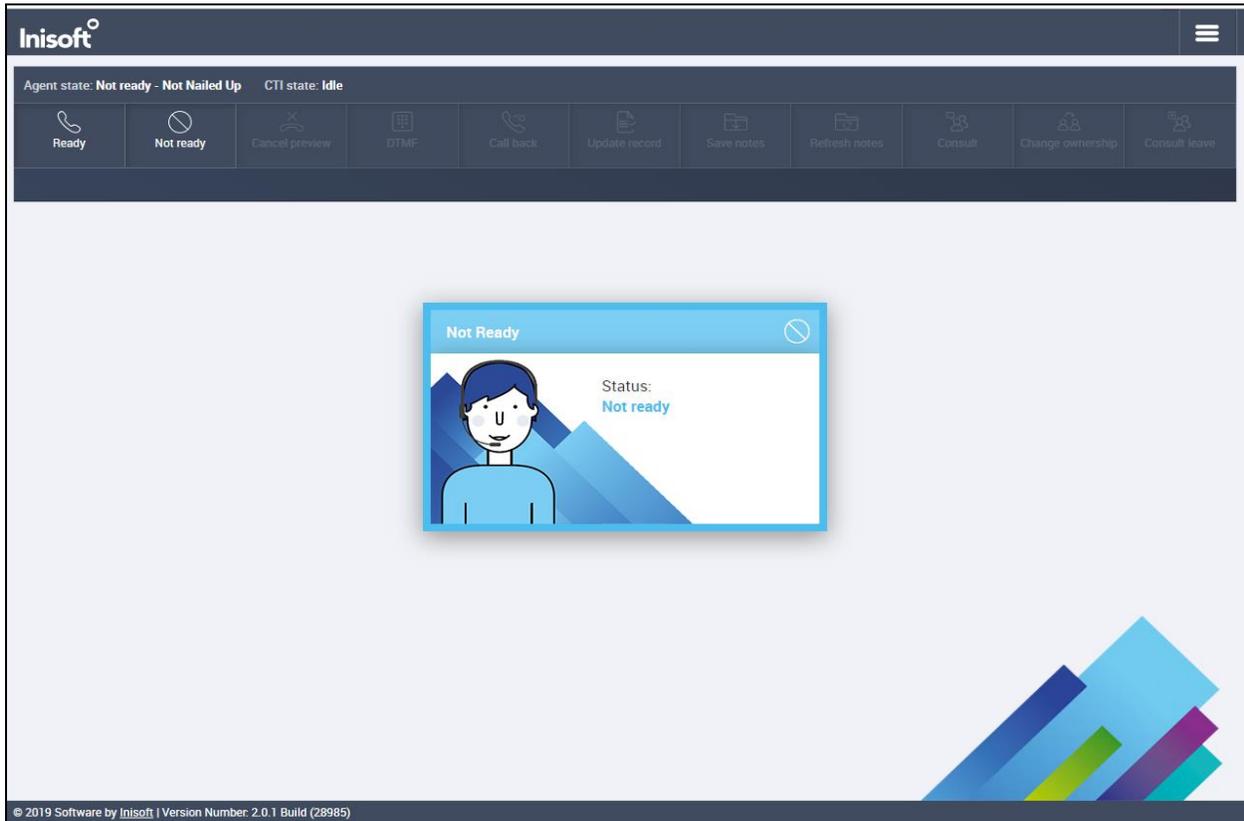
Extension *

Agent ID *

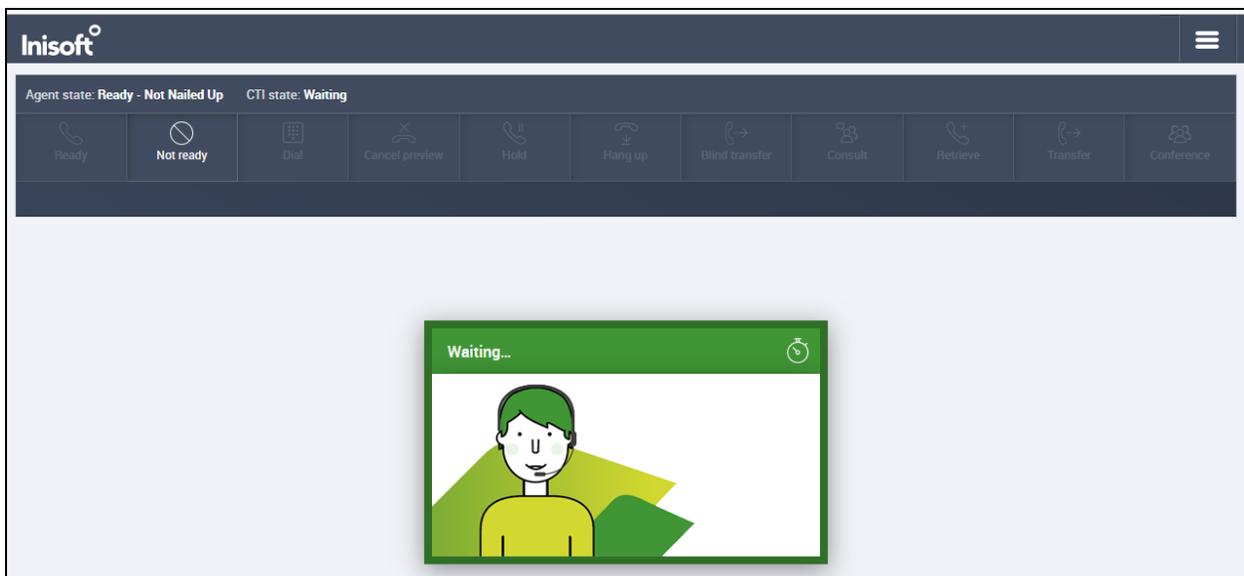
Password

Organization *

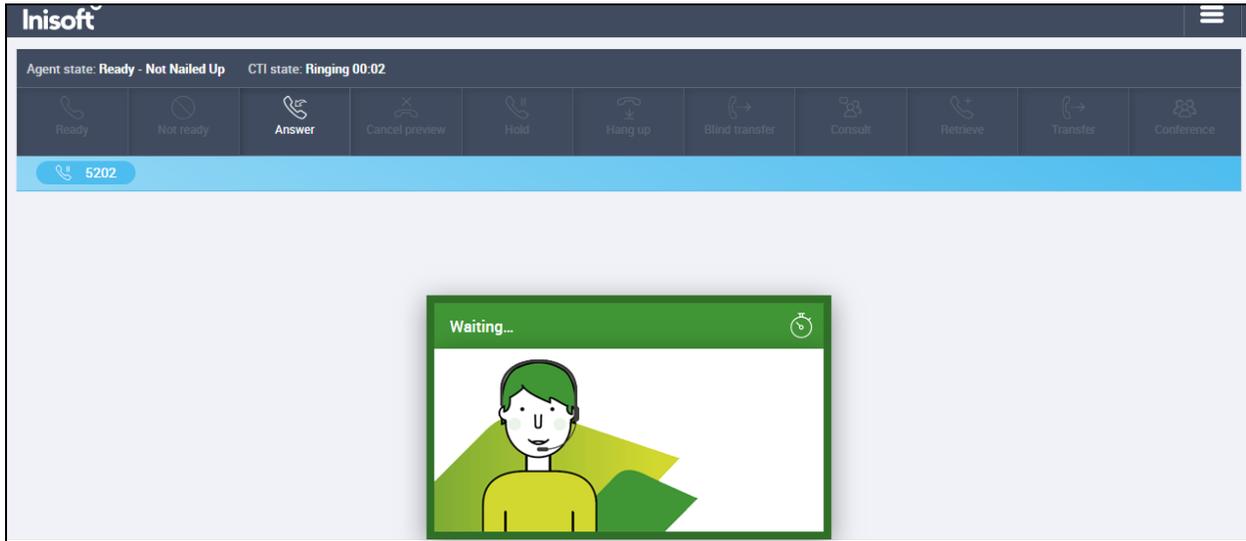
The initial screen shows the agent as being **Not Ready**. By default, agents are logged into a skill in an 'Aux Work' state which is a Not Ready state.



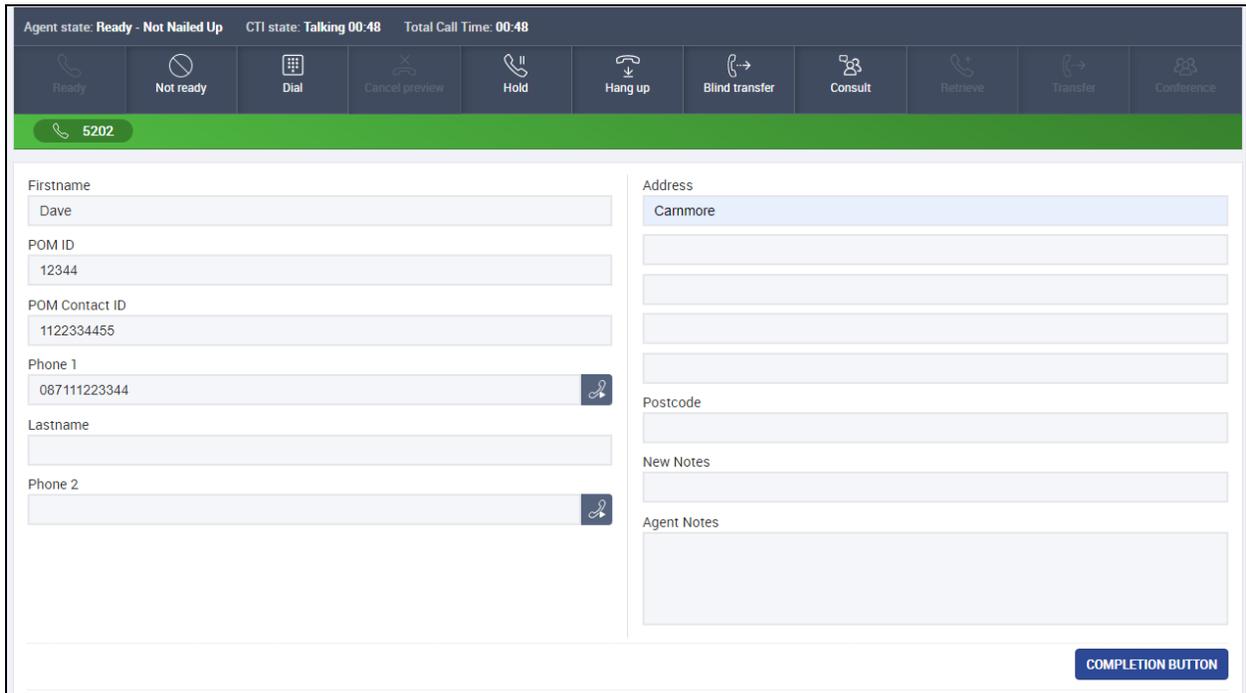
Pressing the **Ready** button on the screen above will place the agent in **Waiting** mode as shown below.



A call is then placed to the VDN 1900 (Sales) and can be answered using the **Answer** button. The caller number **5202** is displayed.



Once the call is answered, information on the caller is displayed and the call can be held, transferred or conferenced. Once the call is completed the **COMPLETION BUTTON** is pressed and the call is hung up.

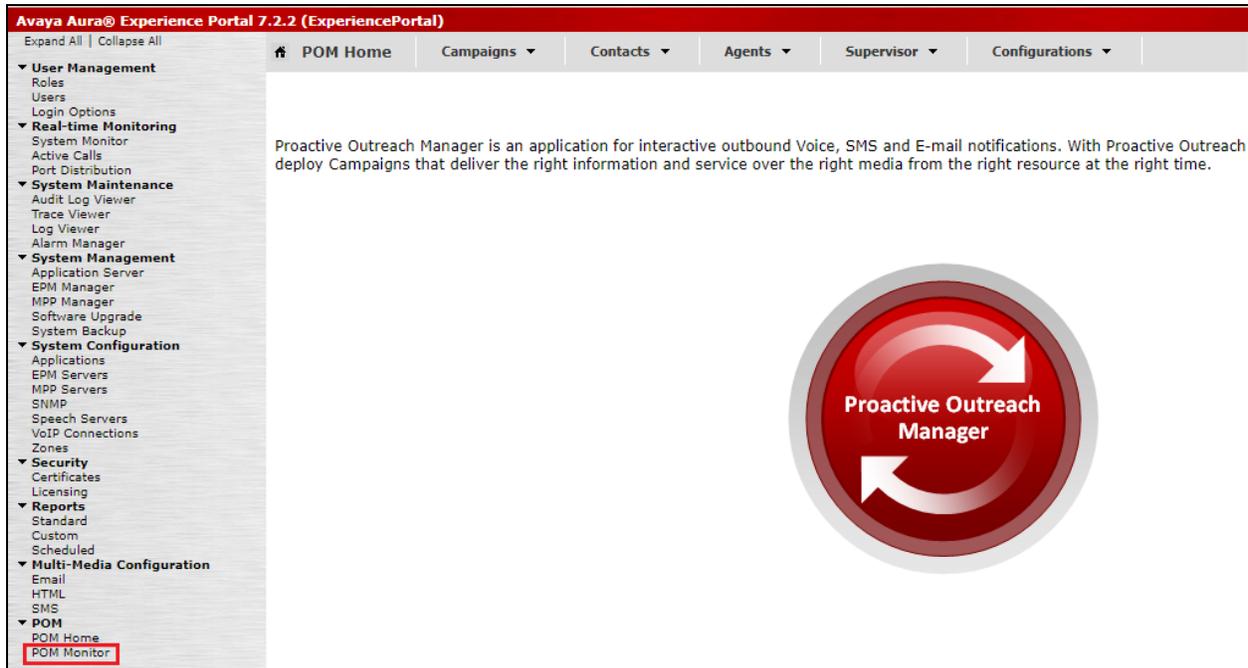


9.2. Verify the Connection to Avaya Proactive Outreach Manager

The connection to POM can be verified on the POM side and on the Syntelate XA side using the desktop to make outbound calls.

9.2.1. Verify Avaya Proactive Outreach Manager Campaign

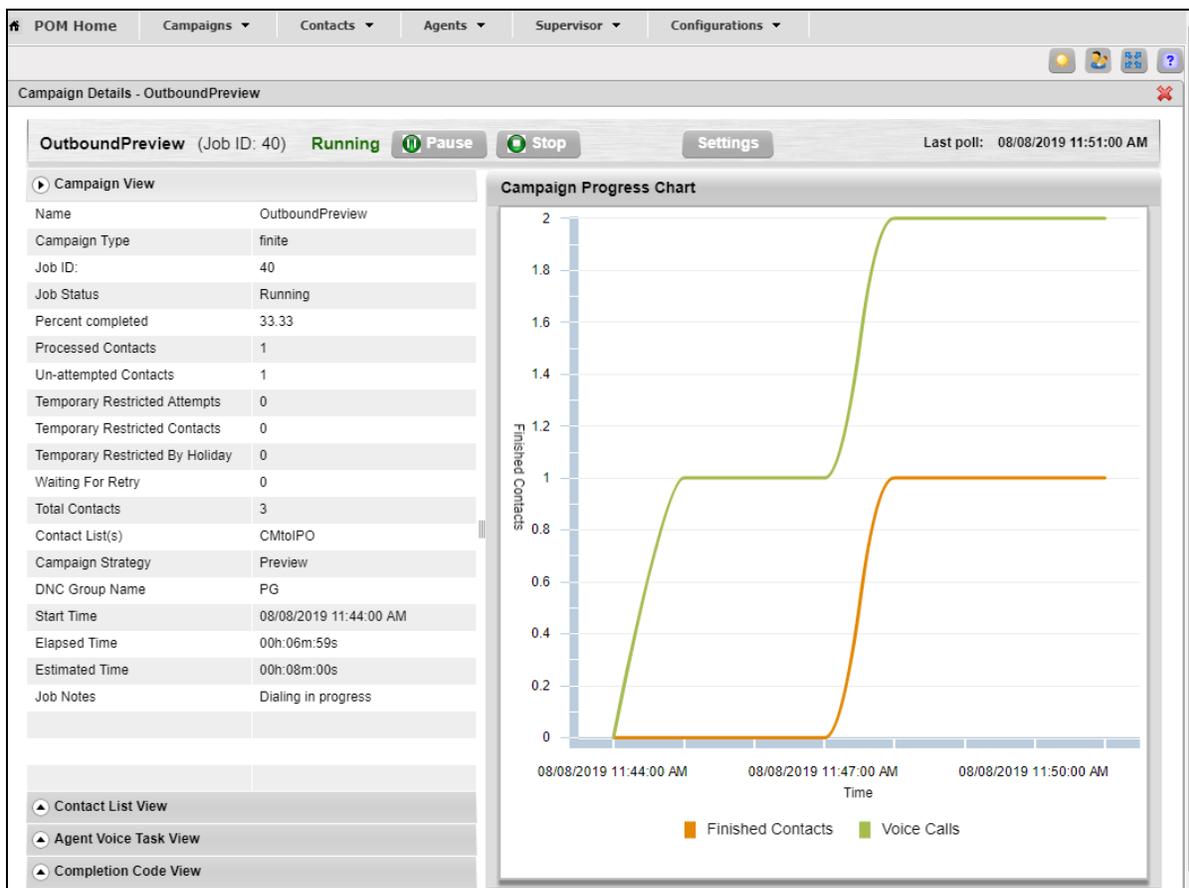
Log into POM as per **Section 7**. Navigate to **POM → POM Monitor** in the left column as shown below.



Information on any campaign that is running can be looked at by clicking on the running campaigns. The example below shows that a campaign called **OutboundPreview** has a **Status** shown as **Running** and by clicking on this row the details on the campaign will be shown.

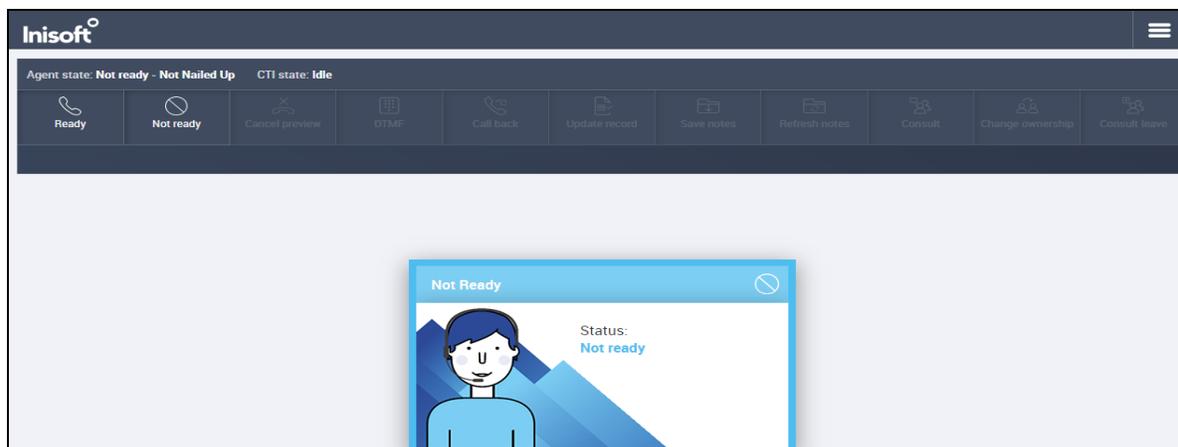
	Campaign Name	Campaign Type	Job ID	Status	Contact List(s)	Organization	Start Time	Un-attempted Contacts	Pro
	OutboundPreview	finite	40	Running	CMtoIPO		08/08/2019 11:4.	2	0

The example below shows the details of the campaign **OutboundPreview**.

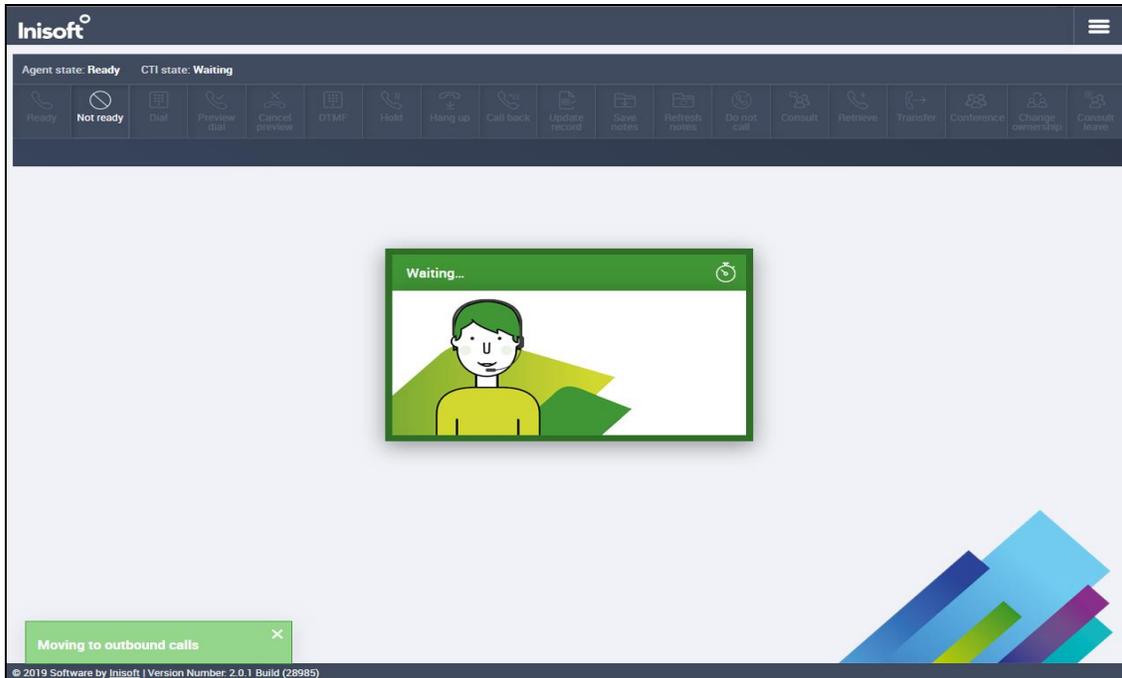


9.2.2. Verify the Connection from Syntelate XA Desktop

Log into the Syntelate XA Desktop as per **Section 9.1.2**, the same agent and station details can be used as this agent was setup with both inbound and outbound skillsets. Once logged in the agent is once again displayed as shown. Note the **Agent state is Not ready and Not Nailed Up** as the POM outbound campaign is not yet running. Start the outbound campaign as per **Section 7.4**.



The POM will make a call to the agent and this call must be answered manually on the agent's phone. This is exactly as designed, and the Syntelate XA Desktop was not designed to answer this particular call. Once the call is answered the agent will go to **Waiting**, as shown below, and the message **Moving to outbound calls** is displayed at the bottom of the screen.



Because this is a preview call it is presented to the agent allowing the agent to make the outbound call to the customer. Clicking on the **Preview dial** icon at the top of the screen will initiate the outbound call to the number **85250** displayed below.

Once the call is made, the call can then be put on hold, transferred or a call back created. Notes can be added, or the record can be updated using the buttons at the top of the screen. Once the call is completed the **COMPLETION BUTTON** can be pressed allowing the agent to wrap up the call.

The screenshot displays the Inisoft CRM interface during a call. At the top, the status bar shows 'Agent state: Ready', 'CTI state: Talking 00:02', and 'Total Call Time: 01:06'. Below this is a toolbar with various call control icons: Ready, Not ready, Dial, Preview dial, Cancel preview, DTMF, Hold, Hang up, Call back, Update record, Save notes, Refresh notes, Do not call, Consult, Retrieve, Transfer, Conference, Change ownership, and Consult leave. A green bar below the toolbar displays the phone number '85250'. The main area is divided into two columns of input fields. The left column contains fields for Firstname (Paul), POM ID (1), POM Contact ID (1), Phone 1 (85250), Lastname (Greaney), and Phone 2 (85250). The right column contains fields for Address (Carmore), Co. Galway, Ireland, Postcode, New Notes, and Agent Notes. A blue 'COMPLETION BUTTON' is located at the bottom right of the form area. The footer of the interface shows '© 2019 Software by Inisoft | Version Number: 2.0.1 Build (28985)'.

10. Conclusion

These Application Notes describe the configuration steps required to integrate Inisoft Syntelate XA with Avaya Proactive Outreach Manager. All feature and serviceability test cases were completed successfully.

11. Additional References

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

Documentation for Avaya products may be obtained via <http://support.avaya.com>

- [1] Implementing Proactive Outreach Manager, Release 3.1.2, Issue 1, June 2019
- [2] Administering Avaya Aura® Communication Manager, Release 8.1
- [3] Administering Avaya Aura® Session Manager, Release 8.1
- [4] Administering Avaya Aura® Experience Portal, Release 7.2
- [5] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 8.1

Documentation related to Syntelate may directly be obtained from Inisoft.

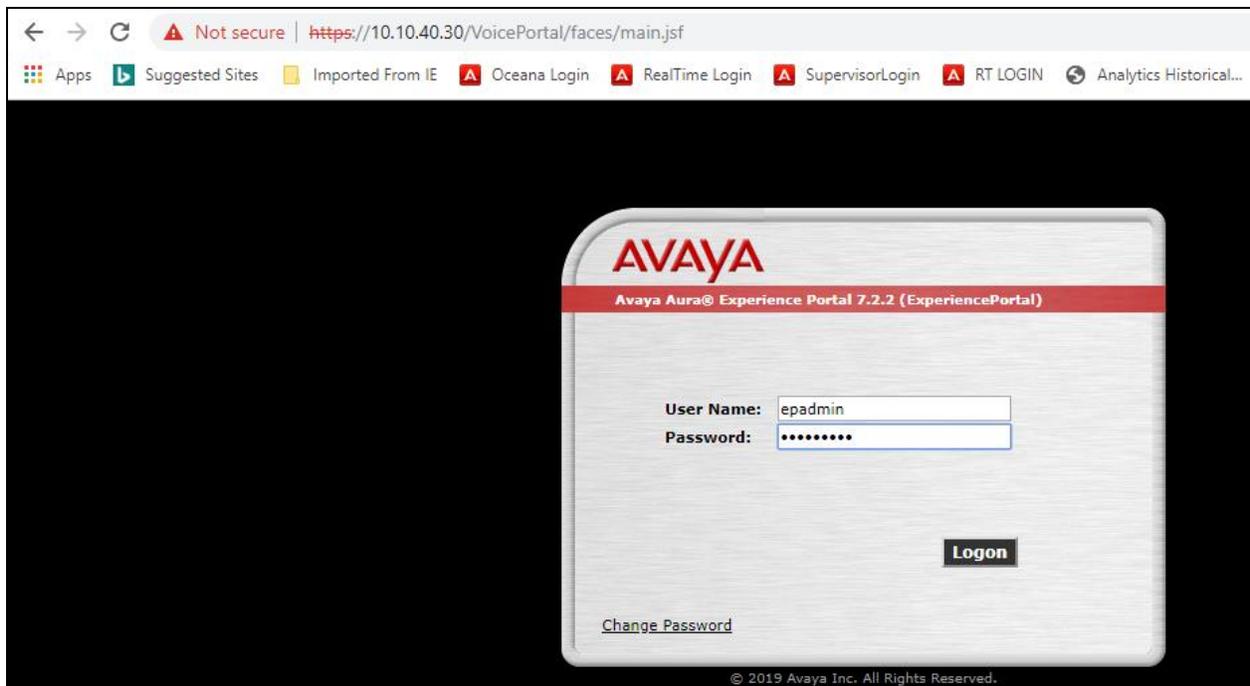
- [6] Syntelate POM – User Notes v13-3
- [7] Syntelate v4 User Document, 2014

Appendix

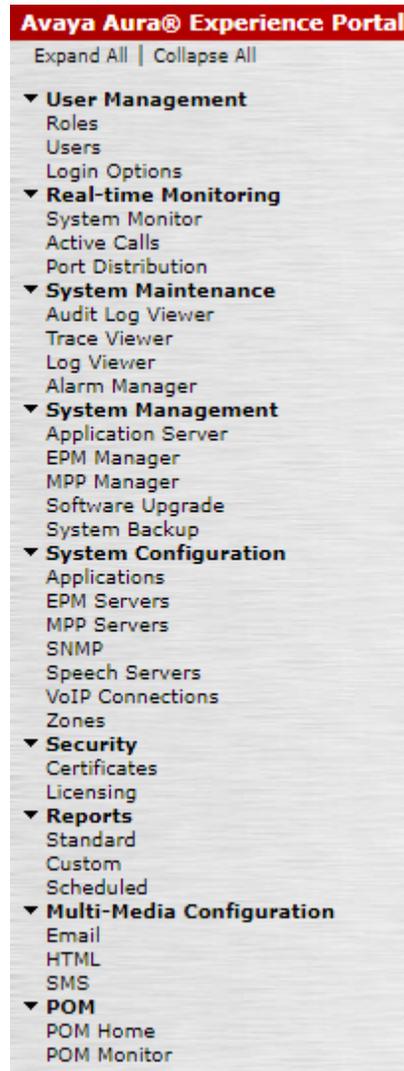
12. Avaya Proactive Outreach Manager Outbound Campaign and Components

This Appendix 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 `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.



Navigate to **POM** → **POM Home** in the left column shown below (bottom of screenshot).



12.1. Preview Campaign Strategy

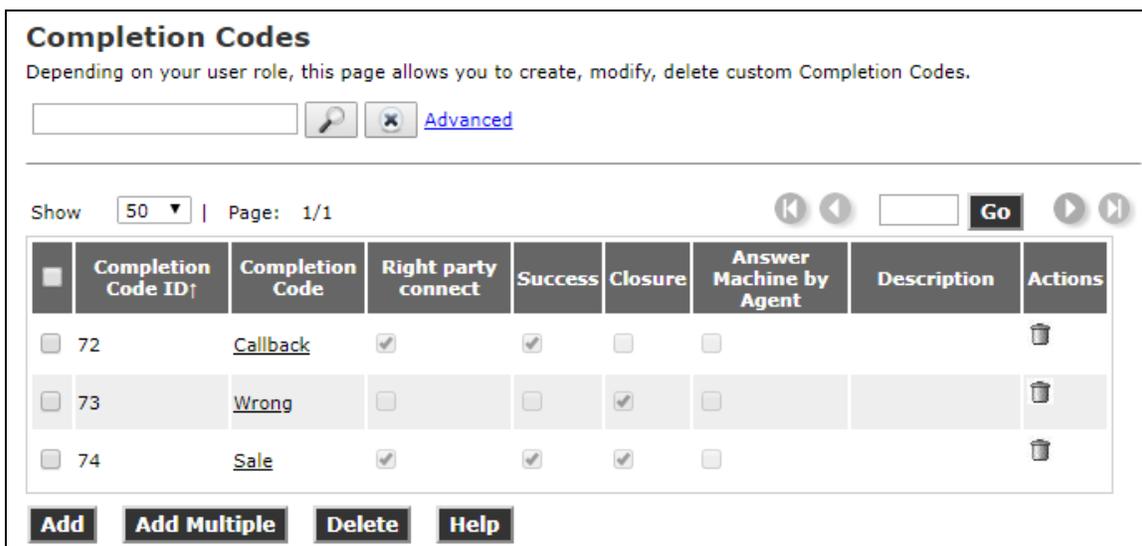
The following section shows the configuration of the Preview Campaign Strategy. Before the strategy can be created a Completion Code must be created.

12.1.1. Completion Codes

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



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



The example below shows the **Sale** Completion Code which is assigned to the Preview Strategy that is to be displayed below.

Edit Completion Code

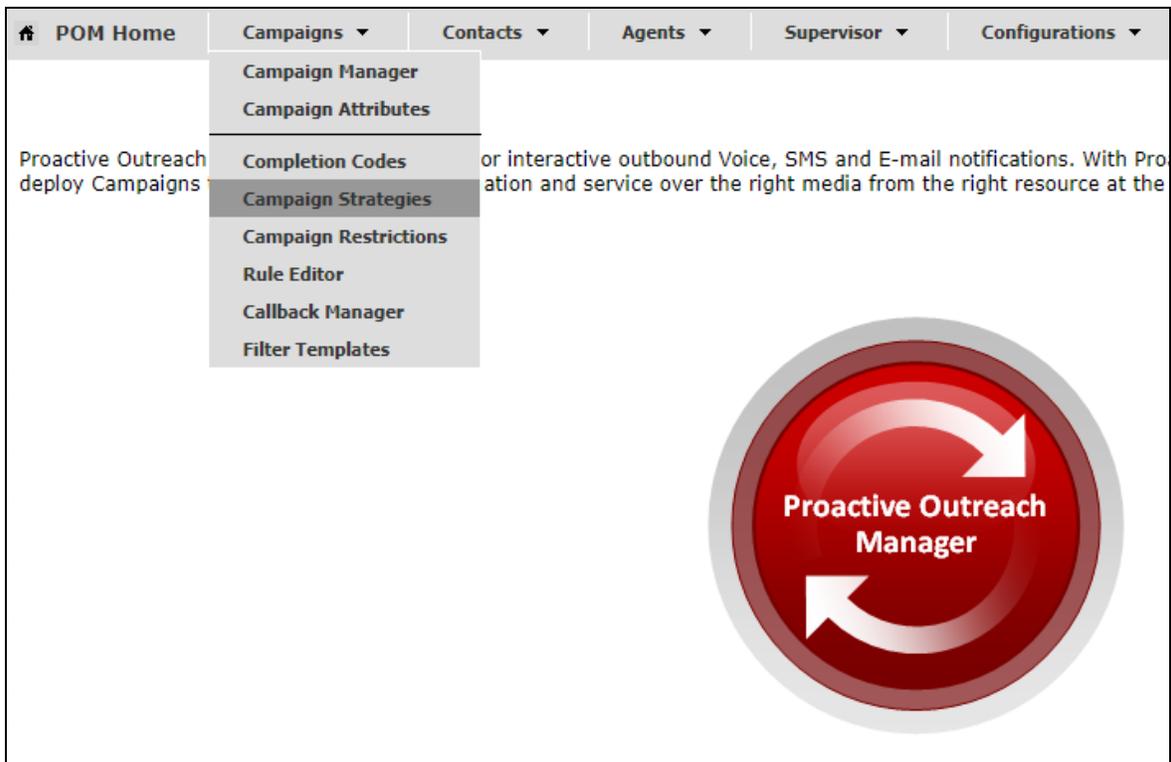
This page allows you to modify Completion Codes.

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**

12.1.2. 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.

Search:

Show: | Page: 1/1 Go

Name	State	Task Types	Action
OutProgressive	Completed		
Preview	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.

Selected Node: Task

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

Campaign Strategy: Preview

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

Property	Value
Name	Preview
Description	
Sender's Display Name	DevConnect
Sender's Address	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
CCA Parameters	
Enhanced CCA	OFF
Background AMD	
Action on AMD	None
Silence Call Detection (SCD)	OFF
APPLICATIONS	
Driver Application	PomDriverApp
Nailer Application	Nailer
Nuisance Call Application	AvayaPOMAnnouncement
On Hold Application	AvayaPOMAnnouncement
PACING PARAMETERS	
Call Pacing Type	Preview
Timed Preview	No
Preview Time (Sec)	
Can Cancel Preview	Disable
Min. Agents	1

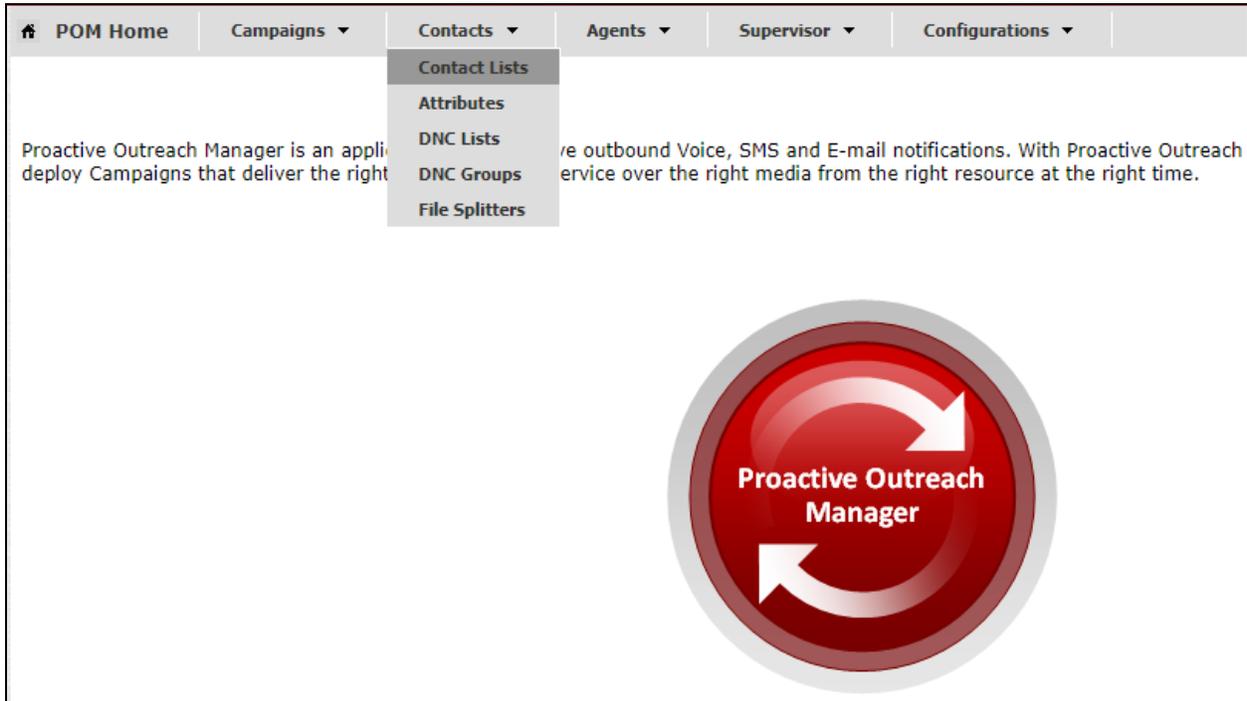
Scrolling down from the screen on the previous page shows the Default Completion code and here the Completion Code created in **Section 12.1.1** can be added. The **Applications** located on Experience Portal are also added here under **APPLICATIONS**.

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. The right pane shows configuration parameters for the selected agent.

CCA Parameters	
Enhanced CCA	OFF
Background AMD	
Action on AMD	None
Silence Call Detection (SCD)	OFF
APPLICATIONS	
Driver Application	PomDriverApp
Nailer Application	Nailer
Nuisance Call Application	AvayaPOMAnnouncement
On Hold Application	AvayaPOMAnnouncement
PACING PARAMETERS	
Call Pacing Type	Preview
Timed Preview	No
Preview Time (Sec)	
Can Cancel Preview	Disable
Min. Agents	1
Max. Agents	5
Agent Outbound Skill	Outbound
ACW Time (Sec)	10
# of ACW extensions	0
Default Completion code	Sale

12.2. Contact List

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



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

Contact Lists Refresh

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

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

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

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

Add **Help**

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

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

Contact search and sort criteria

Search Contact where Attribute

Sort Contact using Attribute in order

Customer ID Attribute

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

Select Attribute that represents Customer ID

Customer ID Retrieval Mode Always Never Attribute Value is Blank

Records Per Page Page Number: 1
 Total Pages: 1

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

12.3. Preview Campaign

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

POM Home Campaigns Contacts Agents Supervisor Configurations

Campaign Manager
 Campaign Attributes

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

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



The image shows a navigation menu for 'Campaigns' with 'Campaign Manager' selected. A large red circular button with a white arrow and the text 'Proactive Outreach Manager' is overlaid on the right side of the page.

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

Campaign Manager [Refresh](#)

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

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

[Advanced](#)

Show 50 | Page: 1/1

Name	Type	Campaign Strategy	Contact Lists	Last Executed	Waiting Callbacks	Actions
OutboundPreview	Finite	Preview	CMtoIPO	08/08/2019 11:44:02 AM 0		<input type="button" value="📄"/> <input type="button" value="🌐"/> <input type="button" value="📅"/> <input type="button" value="🔄"/> <input type="button" value="📄"/> <input type="button" value="▶"/> <input type="button" value="📅"/> <input type="button" value="🗑️"/>
OutboundProgressive	Finite	OutProgressive	CMtoIPO	07/17/2019 04:20:30 PM 0		<input type="button" value="📄"/> <input type="button" value="🌐"/> <input type="button" value="📅"/> <input type="button" value="🔄"/> <input type="button" value="📄"/> <input type="button" value="▶"/> <input type="button" value="📅"/> <input type="button" value="🗑️"/>

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

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

Campaign Strategy

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

Preview

Campaign type

Finite Infinite

Do not associate any Contact List at start

External Selection

External Selection

Contact Record Assignment to Agent

Attributes Agent ID

DNC Group

Apply DNC Group

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

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

Context Store

Publish Attempt Data To Context Store

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

Contact List and Filter Selection

Select Contact List and Filter for this campaign

Name: OutboundPreview

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

Contact List and Filter Template Association

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

Apply same filter No Dialing Allocation

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

Add Association

View Records

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

Show Results

Pause Dialing During Record Selection

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

Pause Dialing During Record Selection

Cancel
Previous
Next
Finish
Help

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

©2019 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.