Avaya Solution & Interoperability Test Lab

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](http://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:

<table>
<thead>
<tr>
<th>Avaya Equipment</th>
<th>Software / Firmware Version</th>
</tr>
</thead>
</table>
| 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  
8.1.0.0.9-1 |
| 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 be set to ead-mia. ACD, Queue and Vector set to y.

```markdown
<table>
<thead>
<tr>
<th>add hunt-group 10</th>
<th>Page 1 of 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Number: 10</td>
<td>ACD? y</td>
</tr>
<tr>
<td>Group Name: Outbound</td>
<td>Queue? y</td>
</tr>
<tr>
<td>Group Extension: 1801</td>
<td>Vector? y</td>
</tr>
<tr>
<td>Group Type: ead-mia</td>
<td></td>
</tr>
<tr>
<td>TN: 1</td>
<td></td>
</tr>
<tr>
<td>COR: 1</td>
<td>MM Early Answer? n</td>
</tr>
<tr>
<td>Security Code:</td>
<td>Local Agent Preference? n</td>
</tr>
<tr>
<td>ISDN/SIP Caller Display:</td>
<td></td>
</tr>
<tr>
<td>Queue Limit: unlimited</td>
<td></td>
</tr>
<tr>
<td>Calls Warning Threshold: Port:</td>
<td></td>
</tr>
<tr>
<td>Time Warning Threshold: Port:</td>
<td></td>
</tr>
</tbody>
</table>
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Number:</td>
<td>90</td>
</tr>
<tr>
<td><strong>Group Name</strong>:</td>
<td>VoiceSales</td>
</tr>
<tr>
<td><strong>Group Extension</strong>:</td>
<td>1800</td>
</tr>
<tr>
<td><strong>Group Type</strong>:</td>
<td>ucd-mia</td>
</tr>
<tr>
<td>TN:</td>
<td>1</td>
</tr>
<tr>
<td>COR:</td>
<td>1</td>
</tr>
<tr>
<td>Security Code:</td>
<td></td>
</tr>
<tr>
<td>Queue Limit:</td>
<td>unlimited</td>
</tr>
<tr>
<td>Calls Warning Threshold:</td>
<td>Port:</td>
</tr>
<tr>
<td>Time Warning Threshold:</td>
<td>Port:</td>
</tr>
</tbody>
</table>

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

```
add hunt-group 90

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

CALL VECTOR

   Number: 19           Name: DevConnect Vector
   Multimedia? y  Attendant Vectoring? n  Meet-me Conf? n  Lock? n
   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 5.1.1.2.

```
add vdn 1900

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*: 1
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

CLASS OF RESTRICTION

COR Number: 1
COR Description: DefaultCOR_PG
FRL: 0
APLT? y
Can Be Service Observed? y
Can Be A Service Observer? y
Time of Day Chart: 1
Priority Queuing? n
Restriction Override: none
Restricted Call List? n
Access to MCT? y
Group II Category For MFC: 7
Send ANI for MFE? n
MF ANI Prefix: 
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
```

©2019 Avaya Inc. All Rights Reserved.
Syntelate_POM31
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

AGENT LOGINID
Login ID: 1400
Name: Agent1
TN: 1
COR: 1
Coverage Path: LWC Reception: spe
Security Code: LWC Log External Calls? n
Attribute: AUDIX Name for Messaging:
AAS? n
Audix? n
Check skill TNs to match agent TN? n
COR: 1
LoginID for ISDN/SIP Display? n
Password:
Password (enter again):
Auto Answer: station
AUX Agent Remains in LOA Queue: system
AUX Agent Considered Idle (MIA): 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

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

<table>
<thead>
<tr>
<th>SN</th>
<th>RL</th>
<th>SL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>90</td>
<td>17</td>
</tr>
<tr>
<td>3</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

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.

<table>
<thead>
<tr>
<th>BUTTON ASSIGNMENTS</th>
<th>List1:</th>
<th>List2:</th>
<th>List3:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: call-appr</td>
<td>5: auto-in</td>
<td>Grp:</td>
<td></td>
</tr>
<tr>
<td>2: call-appr</td>
<td>6: manual-in</td>
<td>Grp:</td>
<td></td>
</tr>
<tr>
<td>3: call-appr</td>
<td>7: release</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4: aux-work</td>
<td>RC: Grp:</td>
<td>8: after-call</td>
<td></td>
</tr>
</tbody>
</table>

**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

OPTIONAL FEATURES

<table>
<thead>
<tr>
<th>IP PORT CAPACITIES</th>
<th>USED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Administered H.323 Trunks: 12000</td>
<td>250</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP Stations: 18000</td>
<td>2</td>
</tr>
<tr>
<td>Maximum Administered Remote Office Trunks: 12000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Concurrently Registered Remote Office Stations: 18000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP eCons: 414</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Video Capable Stations: 18000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Video Capable IP Softphones: 18000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Administered SIP Trunks: 24000</td>
<td>319</td>
</tr>
<tr>
<td>Maximum Administered Ad-hoc Video Conferencing Ports: 24000</td>
<td>0</td>
</tr>
</tbody>
</table>
```

On Page 3, ensure that both ARS and ARS/AAR Partitioning are set to y.
On Page 5, ensure that Uniform Dialing Plan is set to y.

<table>
<thead>
<tr>
<th>OPTIONAL FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multinational Locations? n</td>
</tr>
<tr>
<td>Multiple Level Precedence &amp; Preemption? n</td>
</tr>
<tr>
<td>Multiple Locations? n</td>
</tr>
<tr>
<td>Personal Station Access (PSA)? y</td>
</tr>
<tr>
<td>PNC Duplication? n</td>
</tr>
<tr>
<td>Posted Messages? y</td>
</tr>
<tr>
<td>Private Networking? y</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>FEATURE-RELATED SYSTEM PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Station Display Enabled? n</td>
</tr>
<tr>
<td><strong>Trunk-to-Trunk Transfer: all</strong></td>
</tr>
<tr>
<td>Automatic Callback with Called Party Queuing? n</td>
</tr>
<tr>
<td>Automatic Callback - No Answer Timeout Interval (rings): 3</td>
</tr>
<tr>
<td>Call Park Timeout Interval (minutes): 10</td>
</tr>
<tr>
<td>Off-Premises Tone Detect Timeout Interval (seconds): 20</td>
</tr>
<tr>
<td>AAR/ARS Dial Tone Required? y</td>
</tr>
<tr>
<td>Music (or Silence) on Transferred Trunk Calls? no</td>
</tr>
<tr>
<td>DID/Tie/ISDN/SIP Intercept Treatment: attd</td>
</tr>
<tr>
<td>Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred</td>
</tr>
<tr>
<td>Automatic Circuit Assurance (ACA) Enabled? n</td>
</tr>
<tr>
<td>Abbreviated Dial Programming by Assigned Lists? n</td>
</tr>
<tr>
<td>Auto Abbreviated/Delayed Transition Interval (rings): 2</td>
</tr>
<tr>
<td>Protocol for Caller ID Analog Terminals: Bellcore</td>
</tr>
<tr>
<td>Display Calling Number for Room to Room Caller ID Calls? n</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>display feature-access-codes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FEATURE ACCESS CODE (FAC)</strong></td>
</tr>
</tbody>
</table>
| 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.

<table>
<thead>
<tr>
<th>change dialplan analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DIAL PLAN ANALYSIS TABLE</strong></td>
</tr>
<tr>
<td>Location: all Percent Full: 3</td>
</tr>
<tr>
<td>Dialed Total Call Dialed Total Call Dialed Total Call</td>
</tr>
<tr>
<td>String Length Type String Length Type String Length Type</td>
</tr>
<tr>
<td>1 4 udp # 3 fac</td>
</tr>
<tr>
<td>2 4 udp</td>
</tr>
<tr>
<td><strong>351212</strong> 12 udp</td>
</tr>
<tr>
<td>4 4 ext</td>
</tr>
<tr>
<td>5 4 udp</td>
</tr>
<tr>
<td>58 5 ext</td>
</tr>
<tr>
<td>5999 4 ext</td>
</tr>
<tr>
<td>6 4 udp</td>
</tr>
<tr>
<td>6666 4 ext</td>
</tr>
<tr>
<td>7 4 udp</td>
</tr>
<tr>
<td>781 5 ext</td>
</tr>
<tr>
<td>8 1 fac</td>
</tr>
<tr>
<td>9 1 fac</td>
</tr>
<tr>
<td>* 3 fac</td>
</tr>
<tr>
<td>*8 4 dac</td>
</tr>
</tbody>
</table>
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
UNIFORM DIAL PLAN TABLE
Percent Full: 0

<table>
<thead>
<tr>
<th>Matching Pattern</th>
<th>Len Del</th>
<th>Insert Digits</th>
<th>Net Conv</th>
<th>Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>351212</td>
<td>12</td>
<td>0</td>
<td><code>ars</code></td>
<td>n</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td><code>aar</code></td>
<td>n</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td><code>ars</code></td>
<td>n</td>
</tr>
</tbody>
</table>
```

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 ars analysis 6
AAR DIGIT ANALYSIS TABLE
Percent Full: 3

<table>
<thead>
<tr>
<th>Dialed String</th>
<th>Total Min</th>
<th>Total Max</th>
<th>Route Pattern</th>
<th>Call Type</th>
<th>Node</th>
<th>ANI</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td><code>aar</code></td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>351212</td>
<td>12</td>
<td>12</td>
<td>1</td>
<td><code>lpvt</code></td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td><code>aar</code></td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>7</td>
<td>254</td>
<td><code>aar</code></td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>7</td>
<td>254</td>
<td><code>aar</code></td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>7</td>
<td>7</td>
<td>254</td>
<td><code>aar</code></td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>
```

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.

<table>
<thead>
<tr>
<th>Grp</th>
<th>FRL NPA Pfx Hop Toll No. Inserted</th>
<th>DCS/ IXC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>1 0</td>
<td></td>
</tr>
<tr>
<td>2:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMS81vmpg</td>
<td>10.10.40.61</td>
</tr>
<tr>
<td>G450</td>
<td>10.10.40.14</td>
</tr>
<tr>
<td>IPOffice</td>
<td>10.10.40.25</td>
</tr>
<tr>
<td>SMS81vmpg</td>
<td>10.10.40.32</td>
</tr>
<tr>
<td>SM_Oceana</td>
<td>10.10.41.26</td>
</tr>
<tr>
<td>aes81vmpg</td>
<td>10.10.40.38</td>
</tr>
<tr>
<td>default</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>procr</td>
<td>10.10.40.37</td>
</tr>
</tbody>
</table>

(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

  Region: 1
  Location: 1 Authoritative Domain: devconnect.local
  Name: Default region

  MEDIA PARAMETERS
  Codec Set: 1
  UDP Port Min: 2048
  UDP Port Max: 3329

  DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26

  802.1P/Q PARAMETERS
  Call Control 801p 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
```

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` 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

  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

  Media Encryption

  1: 1-srtp-aescm128-hmac80
  2: none
  3:  
```

**PG: Reviewed:** Solution & Interoperability Test Lab Application Notes 18 of 68

**SPOC 8/31/2019** ©2019 Avaya Inc. All Rights Reserved.

**Syntelate_POM31**
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

SIGNALING GROUP

Group Number: 1
Group Type: sip
Transport Method: tls

IMS Enabled? n Q-SIP? n
Q-SIP? n
IP Video? 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
Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate
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.

<table>
<thead>
<tr>
<th>change trunk-group 1</th>
<th>Page 1 of 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUNK GROUP</td>
<td></td>
</tr>
<tr>
<td>Group Number: 1</td>
<td></td>
</tr>
<tr>
<td><strong>Group Name:</strong> SIPTRUNK</td>
<td></td>
</tr>
<tr>
<td>Direction: two-way</td>
<td></td>
</tr>
<tr>
<td>Dial Access? n</td>
<td></td>
</tr>
<tr>
<td>Queue Length: 0</td>
<td></td>
</tr>
<tr>
<td><strong>Service Type:</strong> tie</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Type: sip</td>
<td>CDR Reports: y</td>
</tr>
<tr>
<td>COR: 1</td>
<td>TN: 1</td>
</tr>
<tr>
<td>TAC: *801</td>
<td>Night Service:</td>
</tr>
<tr>
<td></td>
<td>Auth Code? n</td>
</tr>
<tr>
<td></td>
<td>Member Assignment Method: auto</td>
</tr>
<tr>
<td></td>
<td>Signaling Group: 1</td>
</tr>
<tr>
<td></td>
<td>Number of Members: 10</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>change trunk-group 1</th>
<th>Page 2 of 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUNK PARAMETERS</td>
<td></td>
</tr>
<tr>
<td>Unicode Name: auto</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Redirect On OPTIM Failure: 5000</td>
</tr>
<tr>
<td>SCCAN? n</td>
<td>Digital Loss Group: 18</td>
</tr>
<tr>
<td>Preferred Minimum Session Refresh Interval(sec): 600</td>
<td></td>
</tr>
<tr>
<td>Disconnect Supervision - In? y Out? y</td>
<td></td>
</tr>
<tr>
<td>XOIP Treatment: auto</td>
<td>Delay Call Setup When Accessed Via IGAR? n</td>
</tr>
<tr>
<td>Caller ID for Service Link Call to H.323 1xC: station-extension</td>
<td></td>
</tr>
</tbody>
</table>
Settings on Page 5 are as follows.

```
change trunk-group 1

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.**
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).

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM100</td>
<td>10.10.40.52</td>
</tr>
<tr>
<td>aes81vmpg</td>
<td>10.10.40.38</td>
</tr>
<tr>
<td>default</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>g450</td>
<td>10.10.40.15</td>
</tr>
<tr>
<td>procr</td>
<td>10.10.40.37</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Enabled</th>
<th>Local Node</th>
<th>Local Port</th>
<th>Remote Node</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>AESVCS</td>
<td>y</td>
<td>procr</td>
<td>8765</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

```
<table>
<thead>
<tr>
<th>Server ID</th>
<th>AE Services Server</th>
<th>Password</th>
<th>Enabled</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>aes81vmpg</td>
<td>********</td>
<td>y</td>
<td>idle</td>
</tr>
<tr>
<td>2:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

### 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.

```
<table>
<thead>
<tr>
<th>CTI Link: 1</th>
<th>CTI LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension: 2002</td>
<td></td>
</tr>
<tr>
<td>Type: ADJ-IP</td>
<td></td>
</tr>
<tr>
<td>Name: aes81vmpg</td>
<td></td>
</tr>
<tr>
<td>COR: 1</td>
<td></td>
</tr>
</tbody>
</table>
```
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.
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.

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

![Switch Connections Screen](image)

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 Screen](image)

**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.

![Application Enablement Services Console](image)
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]

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

![Apply Changes to Link]

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**.
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.
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.

![Security Database Control](image)
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.

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

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

```
<table>
<thead>
<tr>
<th>AE Services</th>
<th>Tlinks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Manager Interface</td>
<td>Tlink Name</td>
</tr>
<tr>
<td>High Availability</td>
<td>Φ AVAYA=CM81XVMPG=CSTA=AES81XVMPG</td>
</tr>
<tr>
<td>Licensing</td>
<td>Φ AVAYA=CM81XVMPG=CSTA-S=AES81XVMPG</td>
</tr>
<tr>
<td>Maintenance</td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Security Database</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td></td>
</tr>
<tr>
<td>CTI Users</td>
<td></td>
</tr>
<tr>
<td>Devices</td>
<td></td>
</tr>
<tr>
<td>Device Groups</td>
<td></td>
</tr>
<tr>
<td><strong>Tlinks</strong></td>
<td></td>
</tr>
<tr>
<td>T1Link Groups</td>
<td></td>
</tr>
<tr>
<td>Worktops</td>
<td></td>
</tr>
</tbody>
</table>
```
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.
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.
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.

![Experience Portal Login](image)

**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 serve 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.

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

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

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.
The skillset number must match that of the hunt group created in Section 5.1.1.1, this was hunt group 10 used for outbound calls.

<table>
<thead>
<tr>
<th>CC Elite Skill Number</th>
<th>POM Skill Name</th>
<th>Skill Type</th>
<th>Parameter to Monitor for Blending</th>
<th>EWF Levels</th>
<th>Agent Acres Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Outbound</td>
<td>Outbound</td>
<td>Select only for Inbound</td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

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.

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

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**.

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

```
; TSLIB.INI - Windows Telephony Services Library Configuration File
;
; Blank lines and lines beginning with "#" are ignored.
;
[Telephony Servers]
10.10.40.56=450
10.10.48.38=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
; litefe:ffff:180:ff10:2e0:10ff:fe90:9205=450
;
[Conf]
```
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 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.

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

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

![Syntelate XA](image)

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](image)
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.
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.

![Waiting Screen](image)

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.

![Preview Dial Screen](image)
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.
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](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.

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](image)

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.

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

To add or view the Contact Lists, navigate to **Contacts \(\rightarrow\) 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.
The Contact List shown has three entries in it calling to 85250 then 85123 and finally to 85202.

12.3. Preview Campaign
Navigate to Campaigns → Campaign Manager as shown below.
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.
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.

<table>
<thead>
<tr>
<th>Campaign Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Preview</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Campaign type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finite □ Infinite</td>
</tr>
<tr>
<td>Do not associate any Contact List at start</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>External Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Selection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact Record Assignment to Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes □ Agent ID</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNC Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply DNC Group</td>
</tr>
<tr>
<td>From the following list select one or more DNC Group to be used with this Campaign.</td>
</tr>
<tr>
<td>PG □</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Context Store</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish Attempt Data To Context Store</td>
</tr>
</tbody>
</table>

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.

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

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

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.