Abstract

These Application Notes describe the configuration steps required to integrate Inisof Syntelate XA with Avaya Aura® Application Enablement Services. Inisof Syntelate XA integrates with Avaya Aura® Application Enablement Services using the Telephony Server Application Programming Interface (TSAPI) interface to control the Avaya endpoints.

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 Aura® Application Enablement Services R8.1.

These Application Notes describe the connection to Avaya Aura® Application Enablement Services (AES) using the 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.

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.

When Syntelate XA Desktop is launched, to connect to AES, configuration is retrieved from Syntelate server. This particular configuration is deemed as inbound type of agent where incoming skillset calls are handled by the Syntelate XA Desktop.

2. General Test Approach and Test Results

The connection to the AES was tested by placing incoming calls to various VDN’s and allowing the Syntelate XA desktop to answer and process the calls. 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.

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:

- 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.

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. All test cases passed successfully.

- Outbound calls were not tested as part of this compliance testing.

2.3. Support

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

- **Phone:** +44 (0)800 668 1290
- **Email:** support@inisof.co.uk
- **Web:** [www.Syntelate.com](http://www.Syntelate.com)
Reference Configuration Error! Reference source not found. 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.

![Network Solution Diagram](image)

Figure 1: Network solution of Inisoft Syntelate XA and Avaya Aura® Application Enablement Services R8.1
3. 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>
<tbody>
<tr>
<td>Avaya Aura® System Manager</td>
<td>System Manager 8.1.0.0</td>
</tr>
<tr>
<td></td>
<td>Build No. – 8.1.0.0.733078</td>
</tr>
<tr>
<td></td>
<td>Software Update Revision No: 8.1.0.079880</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager</td>
<td>Session Manager R8.1</td>
</tr>
<tr>
<td></td>
<td>Build No. – 8.1.0.0.810007</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager</td>
<td>R8.1.0.1.0 – SP1</td>
</tr>
<tr>
<td></td>
<td>Build No. – 8.1.0.0.810007</td>
</tr>
<tr>
<td></td>
<td>8.1.0.1.0.0.810007</td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services</td>
<td>Appliance Version R8.0.0.12</td>
</tr>
<tr>
<td></td>
<td>Media Server 8.0.0.169</td>
</tr>
<tr>
<td></td>
<td>Element Manager 8.0.0.169</td>
</tr>
<tr>
<td>Avaya 96x1 H323 Deskphone</td>
<td>6.6604</td>
</tr>
<tr>
<td>Avaya 96x1 SIP Deskphone</td>
<td>7.1.2.0.14</td>
</tr>
<tr>
<td>Inisoft Equipment</td>
<td></td>
</tr>
<tr>
<td>Inisoft Syntelate XA</td>
<td>2.0.1</td>
</tr>
<tr>
<td>Insoft Running Avaya Application Enablement</td>
<td>6.3.3</td>
</tr>
<tr>
<td>Services TSAPI Client</td>
<td></td>
</tr>
<tr>
<td>Inisoft Syntelate XA Web Application</td>
<td>Chrome</td>
</tr>
</tbody>
</table>

**Note:** Inisoft Syntelate XA Web Application was tested using Chrome but Internet Explorer, Mozilla FireFox and Microsoft Edge are also supported browsers.
4. 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 10.

4.1. 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.

4.1.1. Hunt Group

A hunt group is setup for inbound calls. 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

Group Number: 90
Group Name: VoiceSales
Group Extension: 1800
Group Type: ucd-mia

ACD? y
Queue? y
Vector? y

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 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.

### 4.1.2. 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
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
```
4.1.3. 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.

```
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*:
  1st Skill*: 90
  2nd Skill*:
  3rd Skill*:

* Follows VDN Override Rules
```

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

```
add agent-loginID 1400

AGENT LOGINID

Login ID: 1400
Name: Agent1
TN: 1
COR: 1
Coverage Path: 
Security Code: 
Attribute: 
LWC Reception: spe
LWC Log External Calls? n
AUDIX Name for Messaging: 
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
ACW Agent Considered Idle: system
Aux Work Reason Code Type: system
Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system
Forced Agent Logout Time: :

WARNING: Agent must log in again before changes take effect
```
On Page 2, assign the skills to the agent by entering the relevant hunt group numbers created in Section 5.1.1 for SN and entering a skill level of 1 for SL. In this case, an agent able to handle both inbound and outbound calls is created. Set the Direct Agent Skill to the Inbound hunt group 90.

Repeat this task accordingly for any additional inbound agents required.

4.1.5. 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.

Note: The same changes on SIP stations are made using System Manager (not shown).
4.2. 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

4.2.1. 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>

4.2.2. 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>
</tbody>
</table>

**4.2.3. Configure CTI Link for TSAPI Service**

Add a CTI link using the `add cti-link` 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.
5. 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

5.1. 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.
5.2. 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](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 - cm81xvmpg](image)

**5.3. 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.
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](image)

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

![Apply Changes to Link](image)

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](image)
5.4. 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.
5.5. 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.

5.5.1. 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)
5.5.2. 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.
### 5.5.3. Identify Tlinks

Click on **Tlinks**. Verify the value of the **Tlink Name**. This will be used by the Syntelate XA application.
5.6. 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 the AE Server. Navigate to Maintenance → Service Controller. In the main screen select Restart AE Server highlighted.
6. Configure Inisoft Syntelate XA

The configuration of the Syntelate XA server consists of amending a TSAPI client .ini file to ensure the correct IP address is given and to configure the workkzone on the Syntelate XA server.

6.1. Configure TSAPI client

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.
6.2. Configure Syntelate XA Server

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).

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**.

```
"ServerName": "AVAYA#CM81XVMPG#CSTA#AES81XVMPG",
"Username": "inisoft",
"Userpassword": "xxxxxxxxxx"
```

Optionally enter JSON to configure the selected CTI solution.
7. Verification Steps
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.

7.1.1. 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**.

![CTI User Status](image)

### 7.1.2. 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**.

![Sign in](image)
The following window appears asking to select the **workzone**. The example below shows **POMTestWZ** being selected for the AES connection.

![Syntelate XA](image)

Enter the appropriate Communication Manager credentials for **Agent ID**, **Extension** and the **Password** for this agent as per **Section 5.1**. 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.

![Answer button](image1.png)

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.

![Completion button](image2.png)
8. Conclusion
These Application Notes describe the configuration steps required to integrate Inisoft Syntelate XA with Avaya Aura® Application Enablement Services R8.1. All feature and serviceability test cases were completed successfully.

9. 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


Documentation related to Syntelate may directly be obtained from Inisoft.

©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.