



Avaya Solution & Interoperability Test Lab

Application Notes for Inisoft Syntelate XA with Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Inisoft Syntelate XA v2.6 with Avaya Aura® Application Enablement Services R8.1 and Avaya Aura® Communication Manager R8.1. Inisoft 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 v2.6 with Avaya Aura® Application Enablement Services R8.1 and Avaya Aura® Communication Manager R8.1, using the connection to Avaya Aura® Application Enablement Services Telephony Server Application Programming Interface (TSAPI) to control the Avaya endpoints when answering incoming skillset calls.

Syntelate XA is the latest omni-channel customer engagement suite from Inisoft. It allows supervisors to comprehensively control how their agents interact with customers, providing on screen guidance and prompting together with data collection. Syntelate XA allows agents to handle inbound calls, outbound calls, emails, web chats, SMS messages, and social media interactions – all from the same simple interface. For compliance testing with Application Enablement Services only the TSAPI connection was tested and so only telephony control was tested.

The agent launches Syntelate XA Unified Agent Desktop by opening a URL to the Syntelate XA server. A desktop can include things like the following.

- Call buttons (dial, hold, transfer, hang up, etc.)
- Controls for email, SMS, web chat, and social media
- A dynamic script showing the agent what to say at each point in an inbound or outbound call
- Data entry elements showing the customer's details and other information, such as special offers or objection handling tips
- A chart showing the agent's key stats, such as average handling time, and how these compare with the rest of their team
- A workload element listing things such as emails to be responded to, and upcoming callbacks

As already mentioned, the testing focused on call control and call buttons, so that module of the desktop was tested. All configuration for call control is retrieved from Syntelate XA server which has a TSAPI client installed allowing the connection to TSAPI on Application Enablement Services.

2. General Test Approach and Test Results

The connection to Application Enablement Services 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, with the following observations noted.

1. An issue appears when a Feature Access Code (call pickup *09) is used to answer a call. The call is successfully answered by dialing *09 on the agent desktop. However, once on the call, "hang up" does not work to release the call from the agent desktop. The workaround is to manually hang up the call. Inisoft are investigating this issue.
2. There was an observation with "long calls" where nothing happens on a call for over 30 mins, if the agent then attempts to hang up or make any changes via the agent desktop, there was a TSAPI error "invalid object state" and the call failed to clear on the agent's desktop, even though the actual call was hung up. The agent needed to log out and back on again to clear the issue and become useable again. As there is never an instance where an agent and a customer would be idle for more than 30 mins, this is deemed a non-issue.

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.inisoft.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 Application Enablement Services provides the Syntelate XA desktop CTI capability on Communication Manager. The Syntelate XA desktop is capable of logging agents into existing Avaya endpoints and controlling them via a web page on the agent PC.

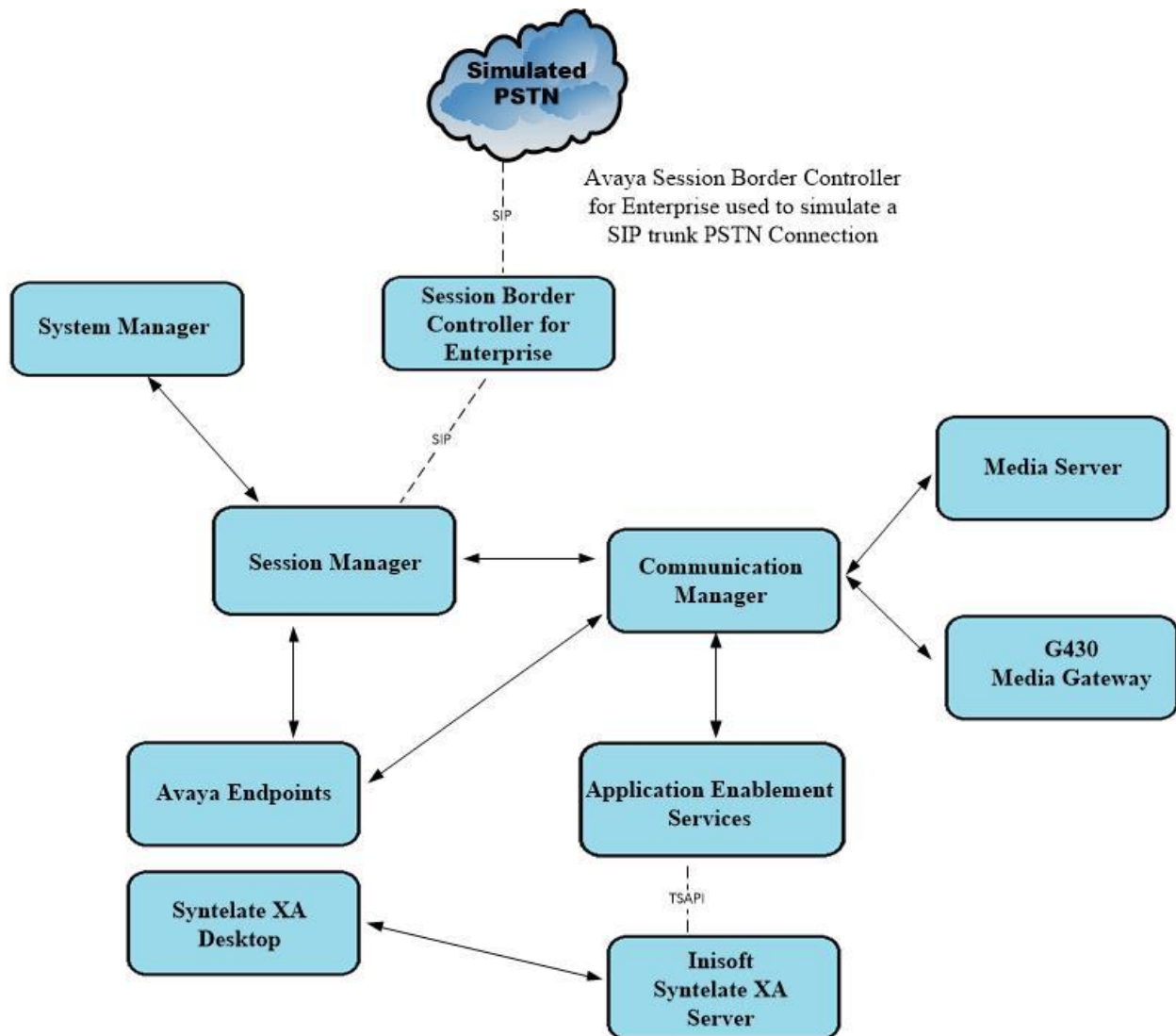


Figure 1: Network solution of Inisoft Syntelate XA v2.5 and Avaya Aura® Application Enablement Services R8.1

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 running on a virtual server	8.1.3.2 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.2.1012646 Service Pack 2
Avaya Aura® Session Manager running on a virtual server	8.1.3.2 Build No. – 8.1.3.2.813207
Avaya Aura® Communication Manager running on a virtual server	8.1.3.2 – FP3SP2 R018x.01.0.890.0 Update ID 01.0.890.0-26989
Avaya Aura® Application Enablement Services	8.1.3.2 Build 8.1.3.2.0.4-0
Avaya Aura® Media Server	8.0.2.184
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 H.323 IP Phone	6.8502
Avaya J189 SIP IP Phone	4.0.10.1.2
Avaya 9408 Digital Deskphone	V2.0
Inisoft Equipment	Software / Firmware Version
Inisoft Syntelate XA running on Windows 2019 server	2.6
Avaya Application Enablement Services TSAPI Client	7.1.1
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 10**.

5.1. 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. 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		Page 1 of 4	
HUNT GROUP			
Group Number: 90		ACD? y	
Group Name: VoiceSales		Queue? y	
Group Extension: 1800		Vector? y	
Group Type: ucd-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 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.

5.1.2. 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		

5.1.3. 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                                     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*:
      3rd Skill*:
* Follows VDN Override Rules
```

5.1.4. 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                           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** 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:	90		1		16:						
2:					17:						
3:					18:						
4:					19:						
5:					20:						
6:											
7:											

Repeat this task accordingly for any additional inbound agents required.

5.1.5. 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.

change station 1001										Page 4 of 5	
										STATION	
SITE DATA											
Room:						Headset? n					
Jack:						Speaker? n					
Cable:						Mounting: d					
Floor:						Cord Length: 0					
Building:						Set Color:					
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				8: after-call							
RC:				Grp:							

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

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 Application Enablement Services (**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 Application Enablement Services, 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	Enabled	Local	Local	Remote	Remote	
Type		Node	Port	Node	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 Application Enablement Services server, in this case **AES81vmppg**.
- **Password:** Enter a password to be administered on the Application Enablement Services server.
- **Enabled:** Set to **y**.

Note: The password entered for **Password** field must match the password on the Application Enablement Services server in **Section 6.2**. The **AE Services Server** should match the administered name for the Application Enablement Services server, this is created as part of the Application Enablement Services installation and can be obtained from the Application Enablement Services 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:	AES81vmppg	*****	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.

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 2002		
Type: ADJ-IP		
COR: 1		
Name: AES81vmppg		

On **Page 2**, **Two-Digit Aux Work Reason Codes** needs to be set to **y**. Default values may be used in the remaining fields.

add cti-link 1		Page 2 of 3
CTI LINK		
FEATURE OPTIONS		
Event Minimization? n	Special Character for Restricted Number? n	
	Send Disconnect Event for Bridged Appearance? n	
	Two-Digit Aux Work Reason Codes? y	
	Block CMS Move Agent Events? N	

5.3. Configure SIP Agent Stations

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

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

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

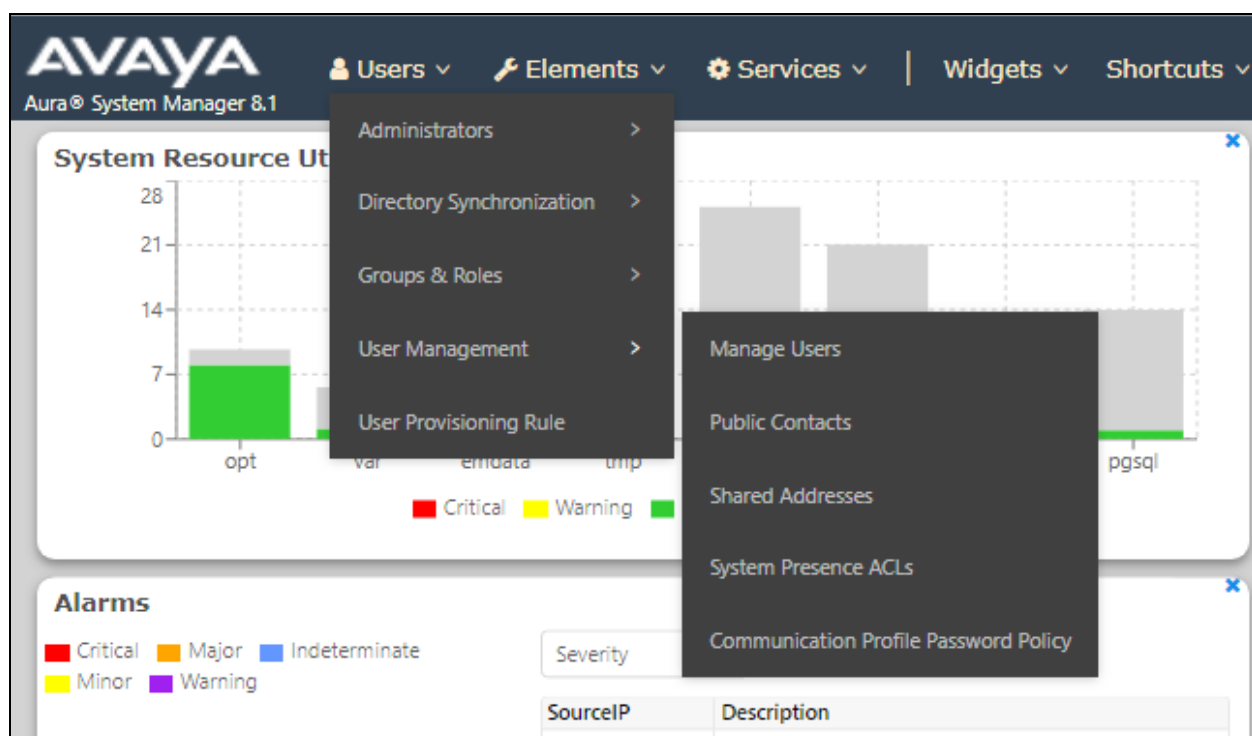
User ID:

Password:

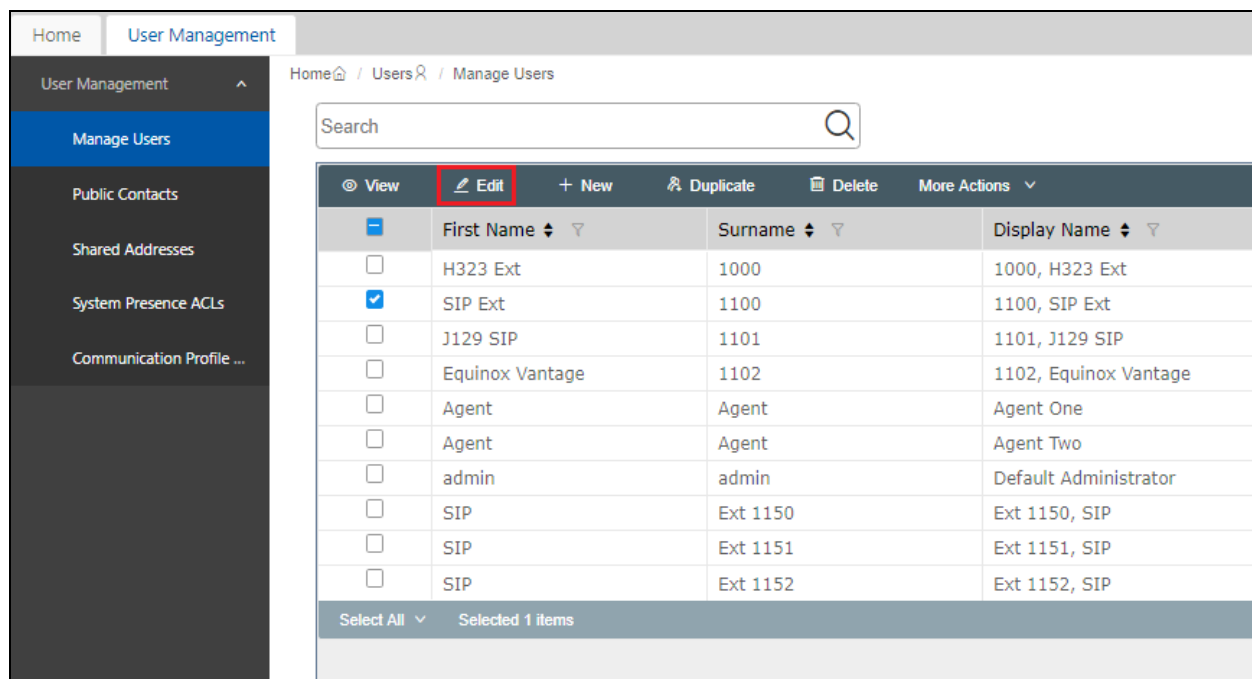
[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

From the home page, click on **Users** → **User Management** → **Manage Users**, as shown below.



Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.



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

In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below. Click on **Done**, at the bottom of the screen, once this is set, (not shown).

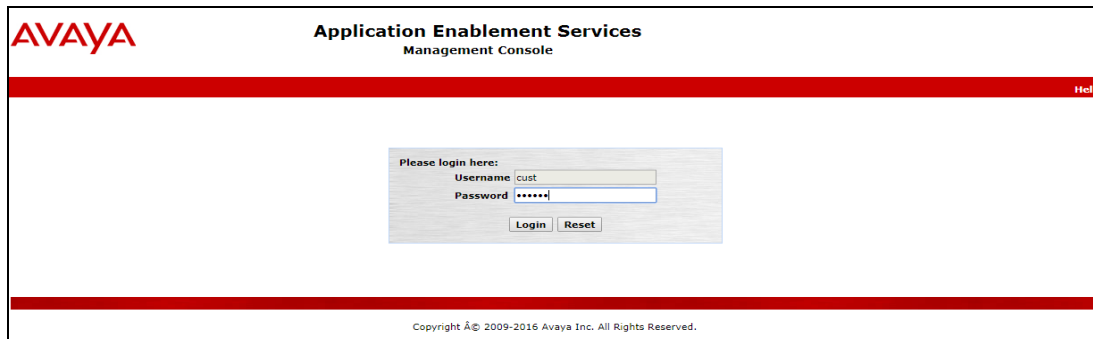
6. Configure Avaya Aura® Application Enablement Services

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

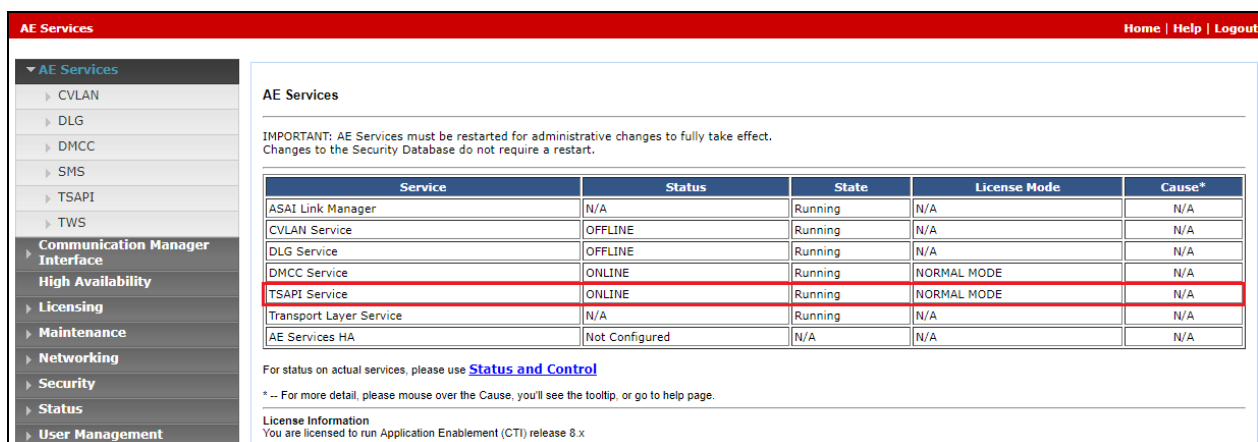
6.1. Verify Licensing

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 Application Enablement Services. The login screen is displayed, log in with the appropriate credentials and then select the **Login** button.



The screenshot shows the Avaya Application Enablement Services Management Console login page. It features the Avaya logo and the title 'Application Enablement Services Management Console'. A login form is centered on the page with fields for 'Username' (containing 'cust') and 'Password' (masked with dots). Below the fields are 'Login' and 'Reset' buttons. A 'Help' link is in the top right corner. The footer contains the copyright notice: 'Copyright © 2009-2016 Avaya Inc. All Rights Reserved.'

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**.



The screenshot displays the 'AE Services' management console. On the left is a navigation menu with options like CVLAN, DLG, DMCC, SMS, TSAPI, TWS, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, and User Management. The main content area shows the 'AE Services' status. A table lists various services and their configurations.

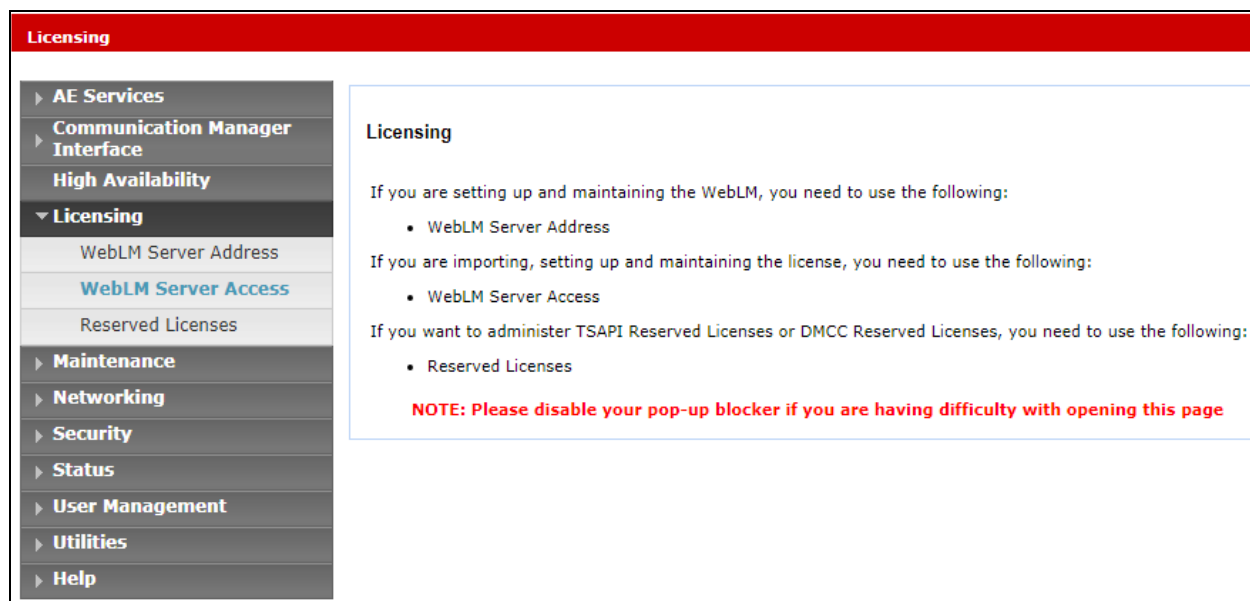
Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA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

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

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
You are licensed to run Application Enablement (CTI) release 8.x

The TSAPI licenses are user licenses issued by the Web License Manager to which the Application Enablement Services server is pointed to. From the left window open **Licensing** and click on **WebLM Server Access** as shown below.



The following screen shows the available licenses for **TSAPI** users.

▼ Application_Enablement

View license capacity

View peak usage

ASBCE

►Session_Border_Controller_E_AE

AVAYA_OCEANA

►Avaya_Oceana

CALL_CENTER_ELITE_MULTICHANNEL

►Call_Center_Elite_Multichannel

Configure Centralized Licensing

CCTR

►ContactCenter

CE

►COLLABORATION_ENVIRONMENT

COLLABORATION_DESIGNER

►Collaboration_Designer

COLLABORATIVE_BROWSING_SNAP-IN

License File Host IDs: V8-FB-29-85-BE-76-01

Licensed Features

10 Items

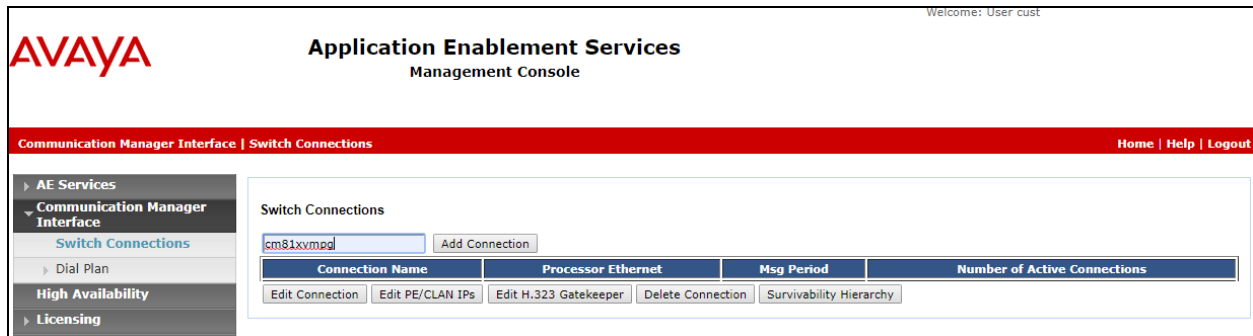
Show

All ▼

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	44
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	44
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	44
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	4
DLG VALUE_AES_DLG	permanent	44
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	44
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	4

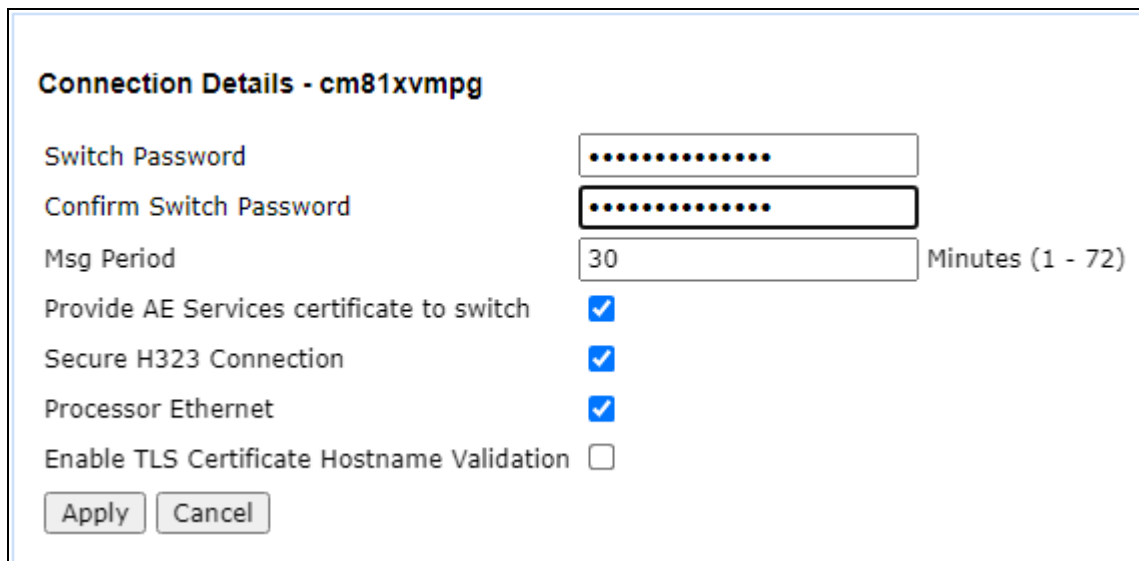
6.2. Create Switch Connection

From the Application Enablement Services 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 "Welcome: User cust" message. Below this is a red banner with "Communication Manager Interface | Switch Connections" and links for "Home | Help | Logout". On the left, a sidebar menu shows "AE Services" expanded, with "Communication Manager Interface" selected, and "Switch Connections" highlighted. The main content area is titled "Switch Connections" and features a text input field containing "cm81xvmpg" and an "Add Connection" button. Below this is a table with the following headers: "Connection Name", "Processor Ethernet", "Msg Period", and "Number of Active Connections". The table contains one row with the connection name "cm81xvmpg" and a value of "1". Below the table are several buttons: "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**. A secure connection between Application Enablement Services and Communication Manager is used by DevConnect as default. Click **Apply** to save changes.



The screenshot shows the "Connection Details - cm81xvmpg" form. It contains the following fields and options:

- Switch Password**: A text input field with a password mask (dots).
- Confirm Switch Password**: A text input field with a password mask (dots).
- Msg Period**: A text input field with the value "30" and a label "Minutes (1 - 72)".
- Provide AE Services certificate to switch**: A checkbox that is checked.
- Secure H323 Connection**: A checkbox that is checked.
- Processor Ethernet**: A checkbox that is checked.
- Enable TLS Certificate Hostname Validation**: A checkbox that is unchecked.

At the bottom of the form are two buttons: "Apply" and "Cancel".

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 Application Enablement Services 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:** The latest version of this can be selected.
- **Security:** This can be left at the default value. The value **both** was used in this test.
- Once completed, select **Apply Changes**.

The screenshot shows a configuration window titled "Edit TSAPI Links". It contains several fields with dropdown menus: "Link" is set to "1", "Switch Connection" is set to "cm81xvmpg", "Switch CTI Link Number" is set to "1", "ASAI Link Version" is set to "12", and "Security" is set to "Both". At the bottom of the window are three buttons: "Apply Changes", "Cancel Changes", and "Advanced Settings".

Another screen appears for confirmation of the changes. Choose **Apply** (not shown).

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**.

The screenshot shows the "Service Controller" screen in a management console. On the left is a sidebar menu with options: "Communication Manager Interface", "Licensing", "Maintenance" (expanded), "Date Time/NTP Server", "Security Database", "Service Controller" (highlighted), "Server Data", "Networking", "Security", and "Status". The main area displays a table of services and their controller status.

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

Below the table, there is a link: "For status on actual services, please use [Status and Control](#)". At the bottom, there are four buttons: "Start", "Stop", "Restart Service" (highlighted with a red box), and "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 categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Utilities, and Help. Under 'User Admin', the 'Add User' option is selected. The main form area is titled 'Add User' and includes a note: 'Fields marked with * can not be empty.' The form fields are as follows:

Field	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 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 top navigation bar is red and contains the text "Security | Security Database | Control". On the left is a sidebar menu with various categories: 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". It contains two checkboxes: "Enable SDB for DMCC Service" (unchecked) and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services" (checked). Below the checkboxes is an "Apply Changes" button.

Security Security Database Control	
<ul style="list-style-type: none">▶ AE Services▶ Communication Manager Interface▶ High Availability▶ Licensing▶ Maintenance▶ Networking▼ Security<ul style="list-style-type: none">▶ Account Management▶ Audit▶ Certificate ManagementEnterprise Directory▶ Host AA▶ PAM▼ Security Database<ul style="list-style-type: none">▪ Control⊕ CTI Users	<h3>SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services</h3> <p><input type="checkbox"/> Enable SDB for DMCC Service</p> <p><input checked="" type="checkbox"/> Enable SDB for TSAPI Service, JTAPI and Telephony Web Services</p> <p><button>Apply Changes</button></p>

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.

CTI Users

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.

<ul style="list-style-type: none">▶ AE Services▶ Communication Manager InterfaceHigh Availability▶ Licensing▶ Maintenance▶ Networking▼ Security<ul style="list-style-type: none">▶ Account Management▶ Audit▶ Certificate ManagementEnterprise Directory▶ Host AA▶ PAM▼ Security Database<ul style="list-style-type: none">▪ Control⊕ CTI Users▪ Devices▪ Device Groups▪ Tlinks▪ Tlink Groups▪ Worktops	<h4>Tlinks</h4> <p>Tlink Name</p> <p><input checked="" type="radio"/> AVAYA#CM81XVMPG#CSTA#AES81XVMPG</p> <p><input type="radio"/> AVAYA#CM81XVMPG#CSTA-S#AES81XVMPG</p> <p><button>Delete Tlink</button></p>
--	---

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

Unencrypted TCP Port9999

Enabled Disabled

Encrypted TCP Port9998

Enabled Disabled

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port450

Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Enabled Disabled

Encrypted Port4722

Enabled Disabled

TR/87 Port4723

Enabled Disabled

H.323 Ports

TCP Port Min20000

TCP Port Max29999

Local UDP Port Min20000

Local UDP Port Max29999

Enabled Disabled

Server Media

RTP Local UDP Port Min*30000

Enabled Disabled

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 displays 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 features 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 on actual services, please use [Status and Control](#)'. At the bottom, there is a row of buttons: Start, Stop, Restart Service, Restart AE Server (highlighted with a red box), Restart Linux, and Restart Web Server.

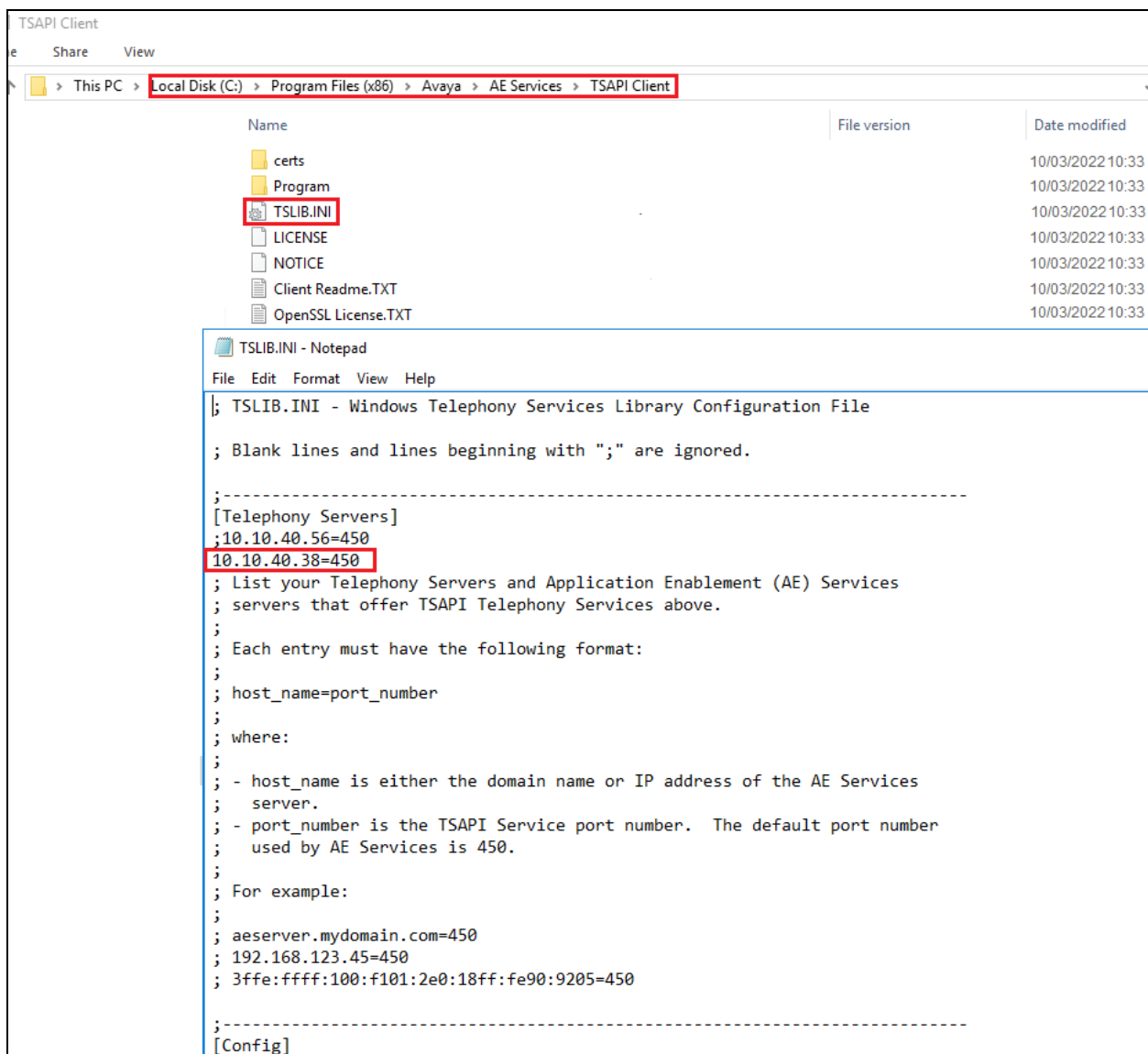
7. Configure Inisoft Syntelate XA

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 workzone on the Syntelate XA server.

7.1. Configure TSAPI client

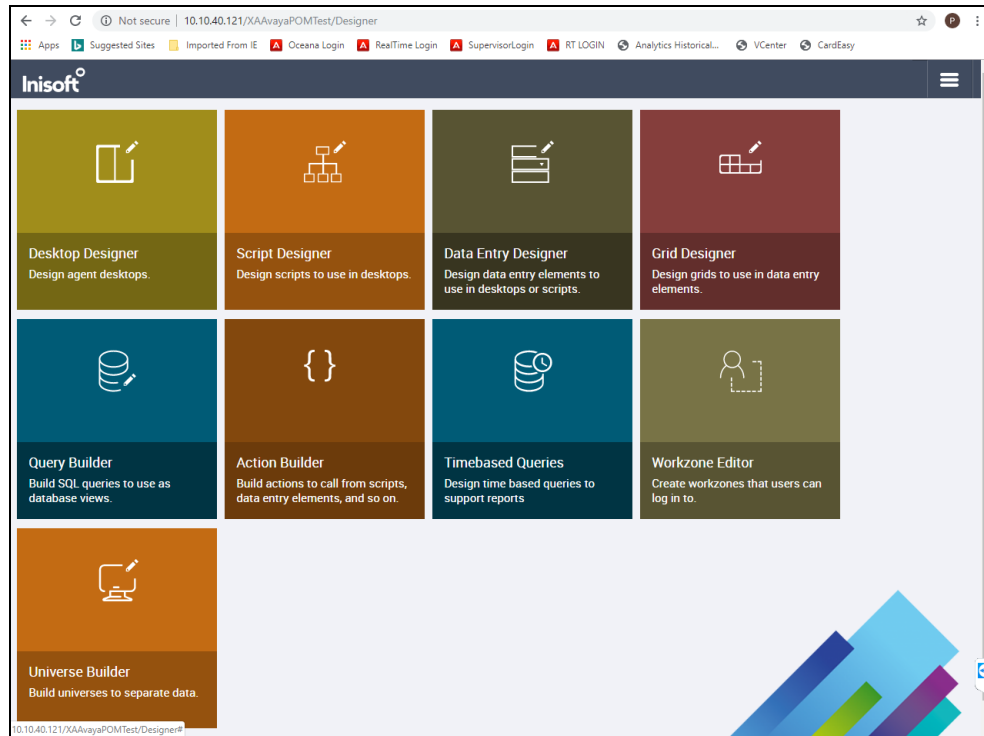
It is assumed that the TSAPI Client has been installed as part of the TSAPI SDK. The IP Address for the Application Enablement Services is included in the TSLIB.INI file located on the Syntelate XA server.

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 Application Enablement Services can be seen below or added if required.

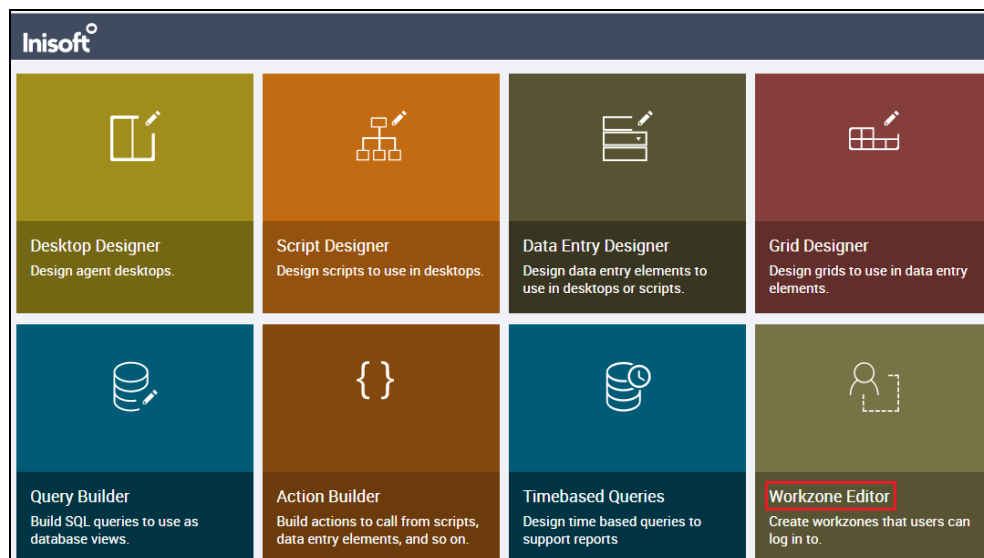


7.2. Configure Syntelate XA Server





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.

Inisoft						
Workzone Editor BACK TO TILES + NEW Filter <i>by name or universe</i> Universe Select Universe						
Name	Universe	Amended by	Amended at	Locked by	Locked at	
POMTestWZ - POM Only	POMComplianceTest	administrator	2022-03-10 10:39			 
POMTestWZ	POMComplianceTest	administrator	2022-03-10 10:39			 

The information on the connection to Application Enablement Services 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 Application Enablement Services username and password that was configured in **Section 6.4**.

CTI configuration (JSON)

SERVERNAME: AVAYA#CM80VMPG#CSTA#AES80VMPG ,

"ServerName": "AVAYA#CM81XVMPG#CSTA#AES81XVMPG",

"Username": "inisoft",

"Userpassword": "xxxxxxxxxx"

"TimeoutSeconds": "10"

Optionally enter JSON to configure the selected CTI solution.

8. Verification Steps

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

8.1.1. Verify the connection from Avaya Aura® Application Enablement Services

Log into the Application Enablement Services 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 Connections Summary

☐ Enable page refresh every 60 seconds

	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
<input checked="" type="radio"/>	cm81xvmpeg	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.

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm81xvmpeg	1	Talking	Wed Feb 23 10:47:12 2022	Online	18	2	51	78	30

For service-wide information, choose one of the following:

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 6
 Closed Streams 50

Open Streams

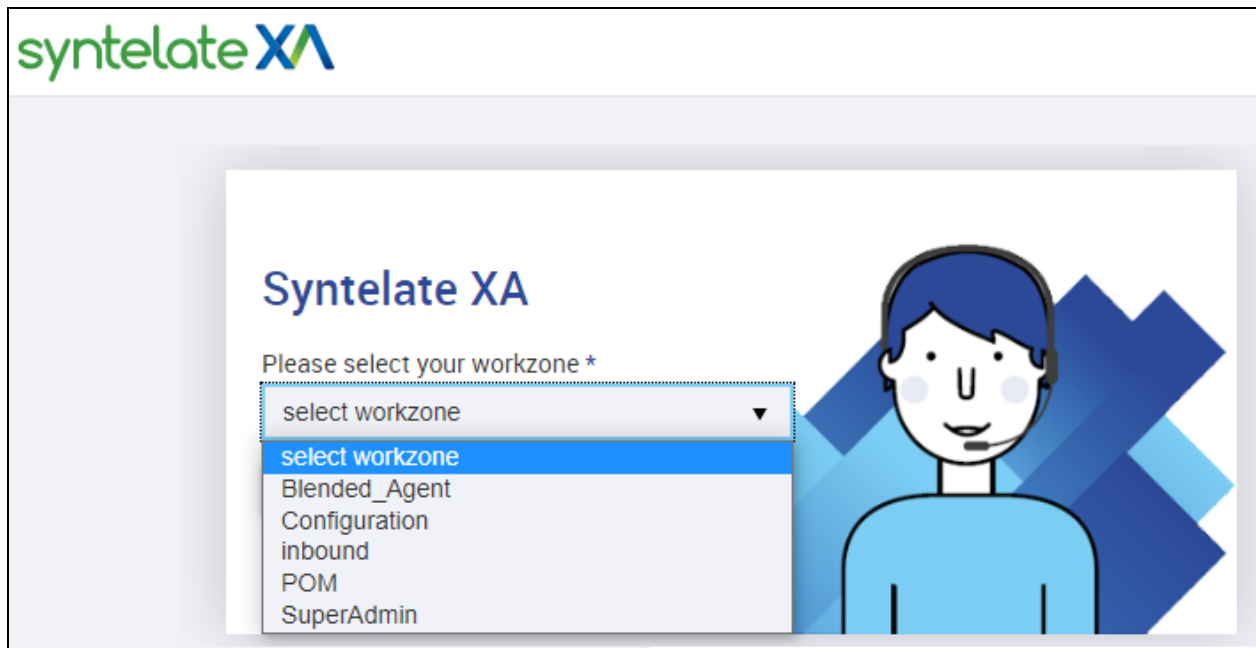
Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Fri 11 Feb 2022 02:25:57 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Fri 11 Feb 2022 02:25:57 PM GMT		AVAYA#CM81LARGE#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Fri 11 Feb 2022 02:25:58 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
DMCCLCSUserDoNotModify	Fri 11 Feb 2022 02:25:58 PM GMT		AVAYA#CM81LARGE#CSTA#AES81XVMPG
inisoft	Thu 03 Mar 2022 01:52:31 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG
inisoft	Thu 03 Mar 2022 01:54:25 PM GMT		AVAYA#CM81XVMPG#CSTA#AES81XVMPG

8.1.2. 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 Administrator was used. Enter the appropriate password and click on **Sign in**.

The screenshot shows a web browser window with the address bar displaying `http://10.10.40.121/XAAvayaPOMTest/`. A sign-in dialog box is overlaid on the page. The dialog has a title bar that says "Sign in". Below the title bar, it shows the URL `http://10.10.40.121` and a warning message: "Your connection to this site is not private". There are two input fields: "Username" with the text "Administrator" entered, and "Password" with masked characters ".....". At the bottom right of the dialog are two buttons: "Sign in" (highlighted in blue) and "Cancel".

The following window appears asking to select the **workzone**. The inbound could be selected for the connection to Application Enablement Services.



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

Extension *

1001

Agent ID *

1400

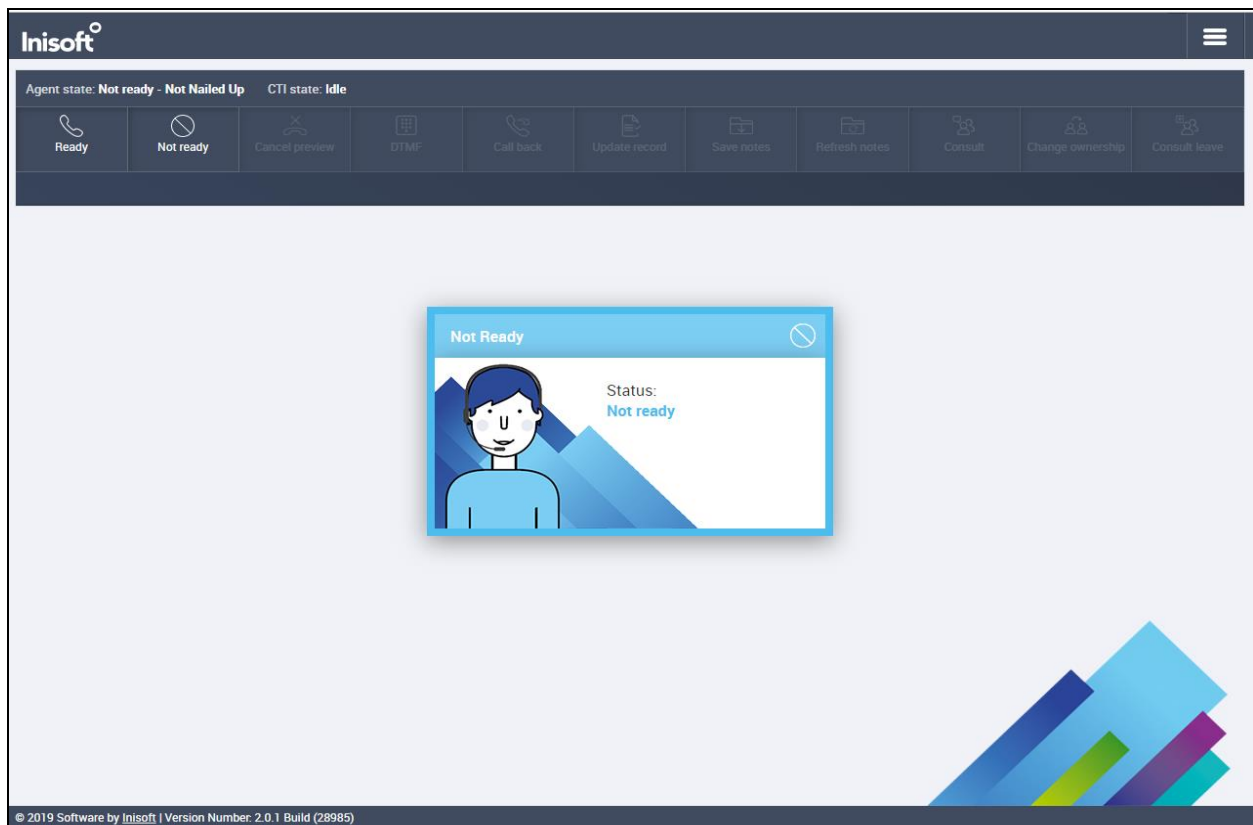
Password

....

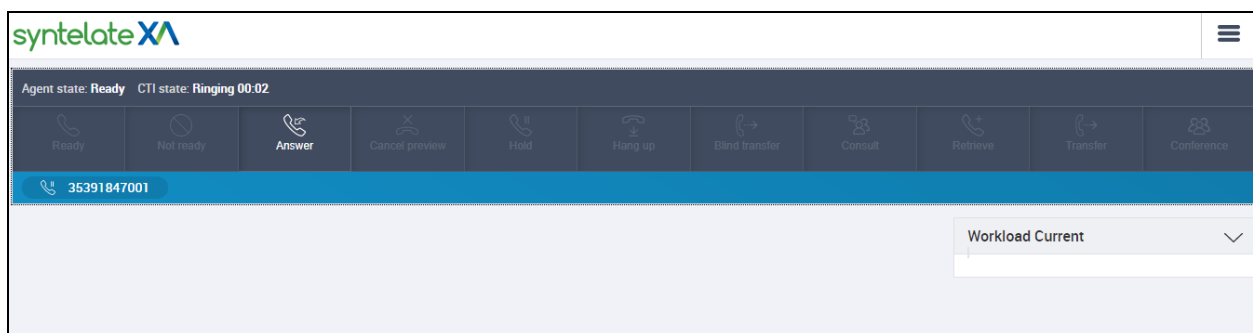
LOG IN

CANCEL

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.



A call is then placed to the VDN 1900 (Sales) and can be answered using the **Answer** button. The caller number **35391847001** 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 **COMPLETE RECORD** button is pressed and the call is hung up.

The screenshot displays the SynteloteXA agent interface. At the top, the status bar shows 'Agent state: Ready', 'CTI state: Talking 00:24', and 'Total Call Time: 00:24'. Below this is a row of call control buttons: Ready, Not ready, Dial, Cancel preview, Hold, Hang up, Blind transfer, Consult, Retrieve, Transfer, and Conference. A green bar at the top of the main workspace displays the phone number '35391847001'.

The main workspace is divided into three panels:

- Welcome:** Contains a yellow speech bubble with the text 'Hi Welcome to Inisoft Travel. How can I help you today?'. Below it are two radio buttons: 'New Customer' (selected) and 'Existing Customer'. A back arrow is visible at the bottom right of this panel.
- Customer Details:** Contains several input fields:
 - First Name: Paul
 - Last Name: Greaney
 - Email Address: paul@email.com
 - Telephone Number 1: 35391847001 (with a phone icon)
 - Timezone: (empty)
 - Client Number: 1682
- Call Log ID:** 3303
- DDI:** 35391731900
- New Notes:** (empty text area)
- Agent Notes History:** (empty text area)

On the right side, the **Workload Current** panel shows 'Inbound call: 1682' and a prominent blue button labeled **COMPLETE RECORD**. At the bottom right, there is a blue triangular graphic with the text 'Activate Windows Go to Settings to activate Windows'.

9. Conclusion

These Application Notes describe the configuration steps required to integrate Inisoft Syntelate XA v2.6 with Avaya Aura® Application Enablement Services R8.1. All feature and serviceability test cases were completed successfully with all observations listed in **Section 2.2**.

10. 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] Administering Avaya Aura® Communication Manager, Release 8.1
- [2] Administering Avaya Aura® Session Manager, Release 8.1
- [3] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 8.1

Documentation related to Syntelate may directly be obtained from Inisoft.

- [4] Syntelate XA – User Notes v13-3
- [5] Syntelate v4 User Document, 2014

©2022 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.