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 with Avaya Aura® Application Enablement Services. 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 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 Inisoft via phone, email, or internet.

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

Reference Configuration **Error! Reference source not found.** shows the n etwork 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.

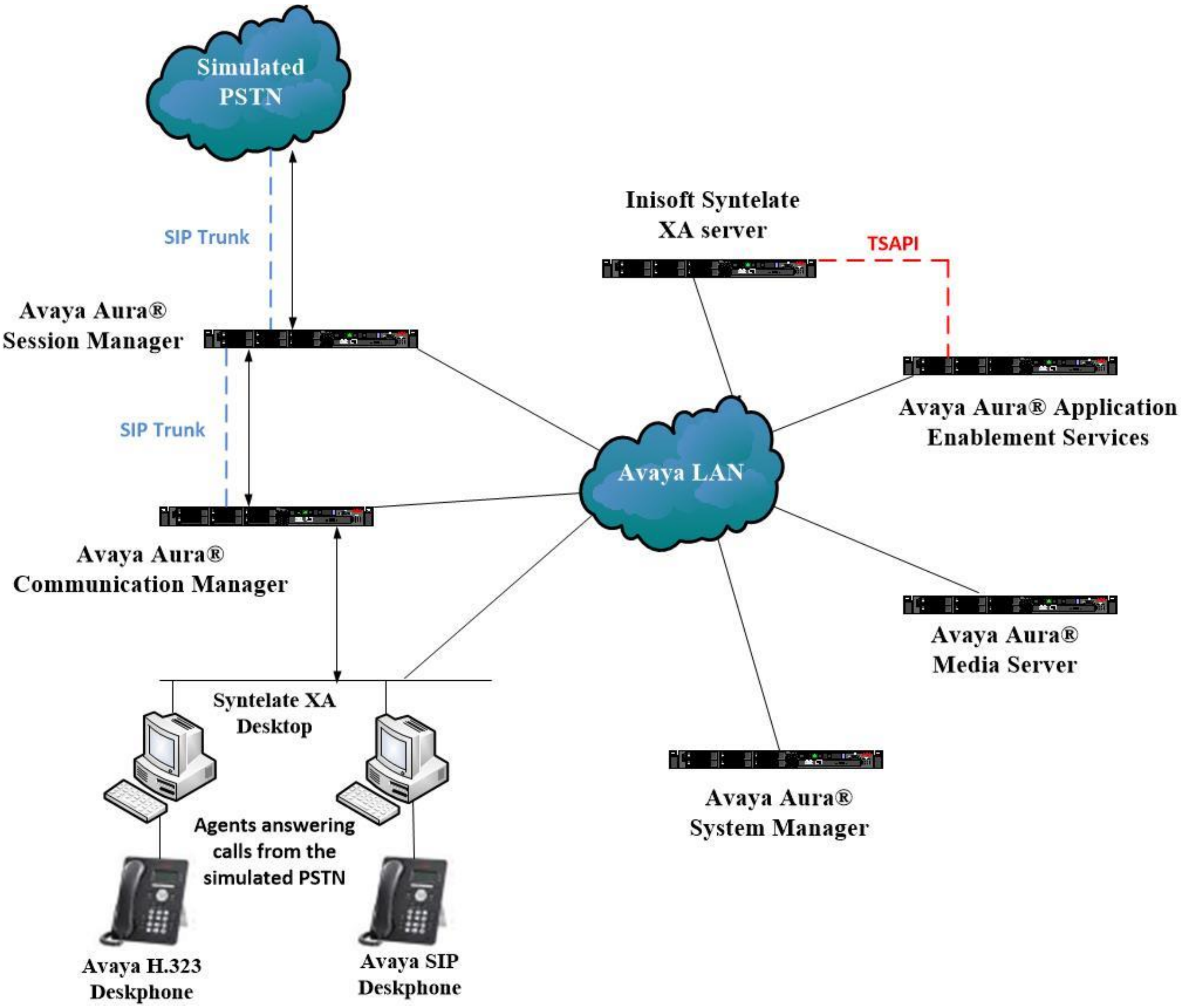

Simulated PSTN
SIP Trunk
Avaya Aura® Session Manager
SIP Trunk
Avaya Aura® Communication Manager
Inisoft Syntelate XA server
TSAPI
Avaya Aura® Application Enablement Services
Avaya LAN
Avaya Aura® Media Server
Avaya Aura® System Manager
Syntelate XA Desktop
Agents answering calls from the simulated PSTN
Avaya H.323 Deskphone
Avaya SIP Deskphone

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:

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager	System Manager 8.1.0.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.0.079880
Avaya Aura® Session Manager	Session Manager R8.1 Build No. – 8.1.0.0.810007
Avaya Aura® Communication Manager	R8.1.0.1.0 – SP1 R018x.01.0.890.0 Update ID 01.0.890.0-25393
Avaya Aura® Application Enablement Services	R8.1 8.1.0.0.0.9-1
Avaya Aura® 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.

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.

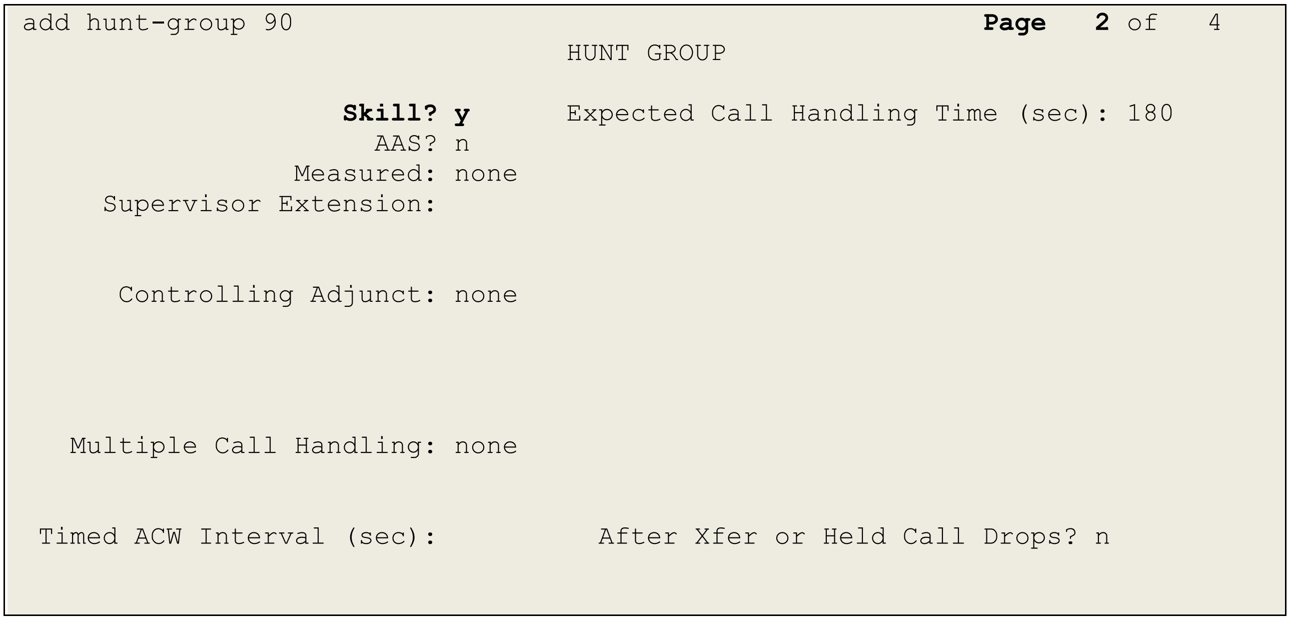
4.1.1. Hunt Group

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                                              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.

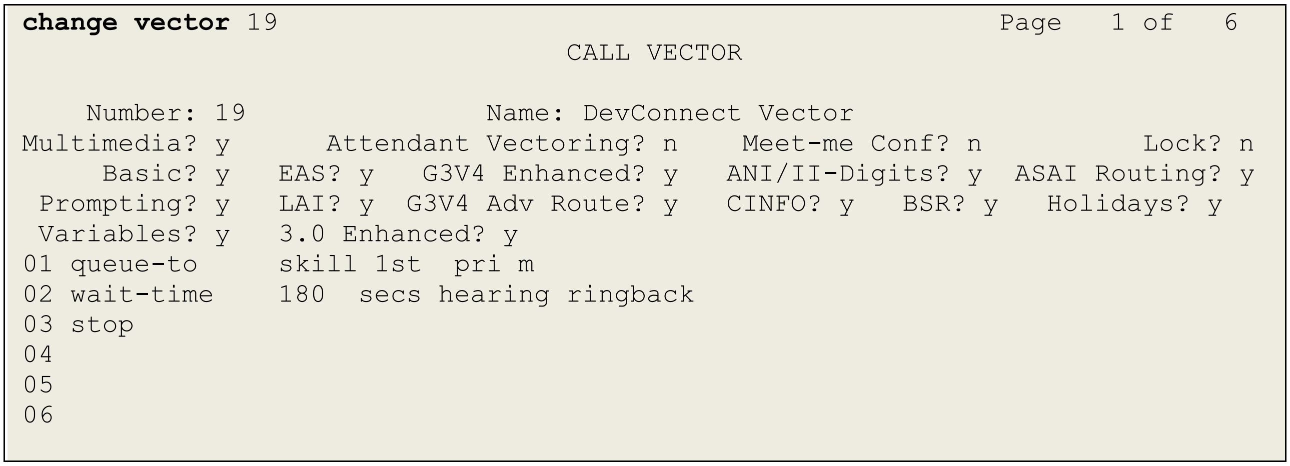


```
add hunt-group 90                                           Page   2 of    4
                                  HUNT GROUP

                    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.

4.1.2. Vectors

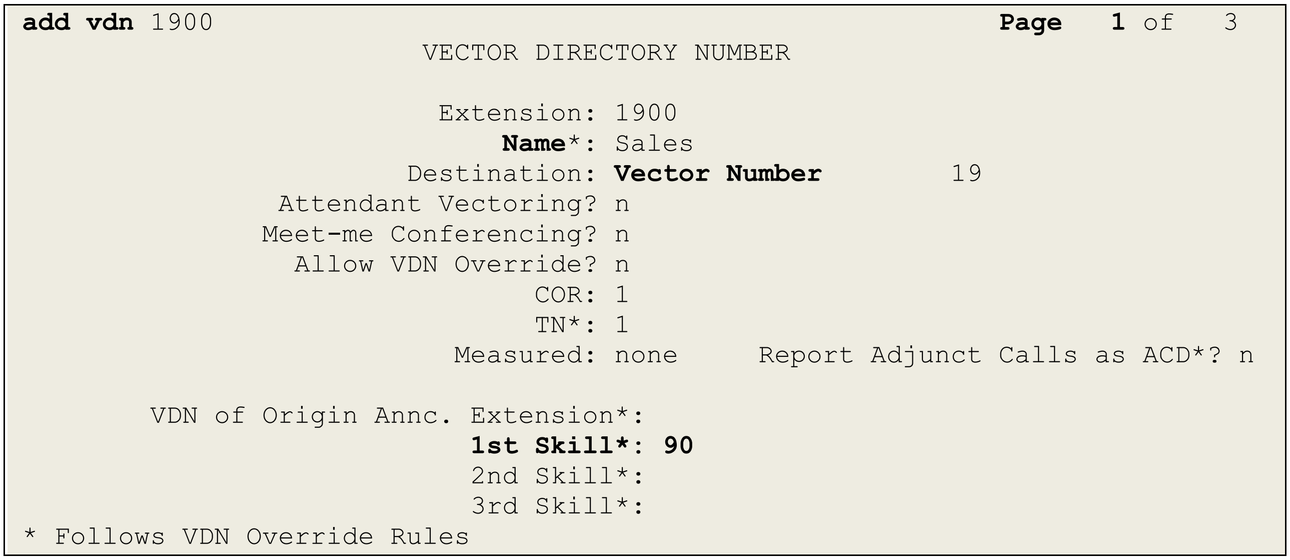
Enter the **change vector n** command, where **n** is the vector number. For this test simple routing was used to get the call to the agent. The call is queued to the skill set out on the VDN in the 1st Skill field on the next page.



```
change vector 19                                             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
```

4.1.3. Vector Directory Numbers (VDN)

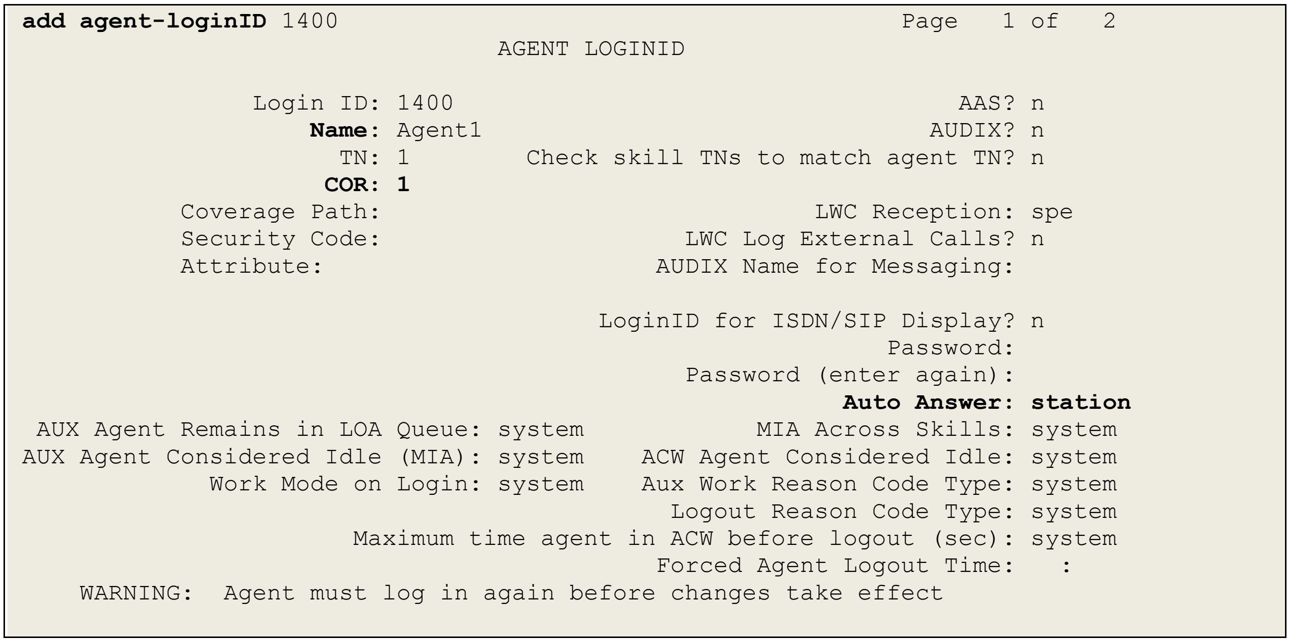
Enter the **add vdn n** command, where **n** is an available extension number. On **Page 1** assign a **Name** for the VDN and set the **Vector Number** to the relevant vector. The **1st Skill** should be set to that hunt group configured in **Section 5.1.1**.



```
add vdn 1900                                                 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
```

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                                       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.

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.

```
change station 1000                                          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    RC:    Grp:             8::after-call
```

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

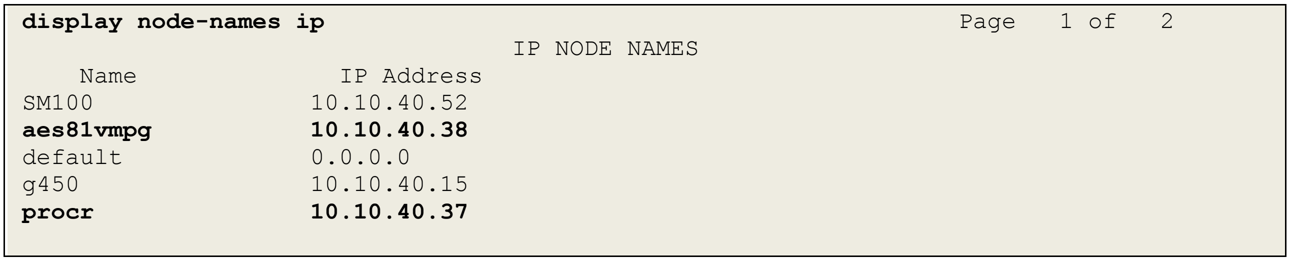
4.2. Configuration of the connection to the Avaya Aura® Application Enablement Services

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**).

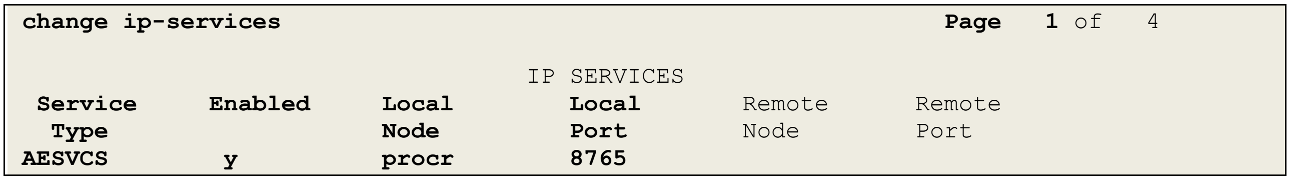


```
display node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM100               10.10.40.52
aes81vmpg           10.10.40.38
default             0.0.0.0
g450                10.10.40.15
procr               10.10.40.37
```

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**



```
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 AES server, in this case **aes81vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

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

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

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

4.2.3. Configure CTI Link for TSAPI Service

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

```
add cti-link 1                                                     Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 2002
     Type: ADJ-IP
                                                                          COR: 1
     Name: aes81vmpg
```

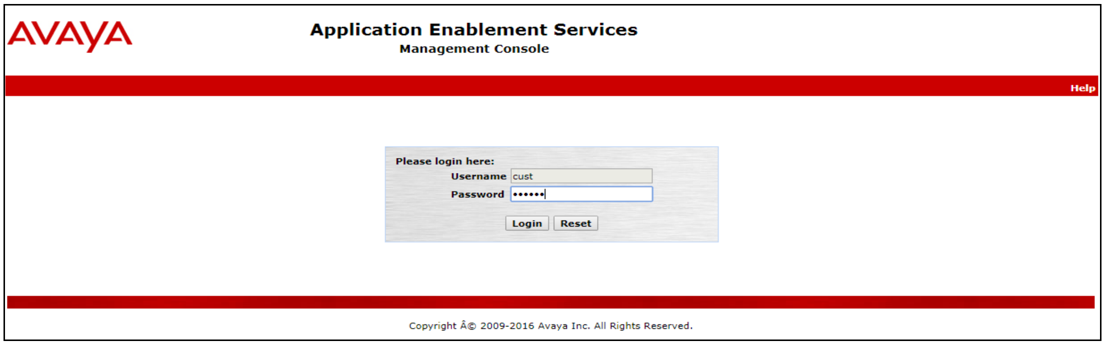
5. Configure Avaya Aura® Application Enablement Services

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.



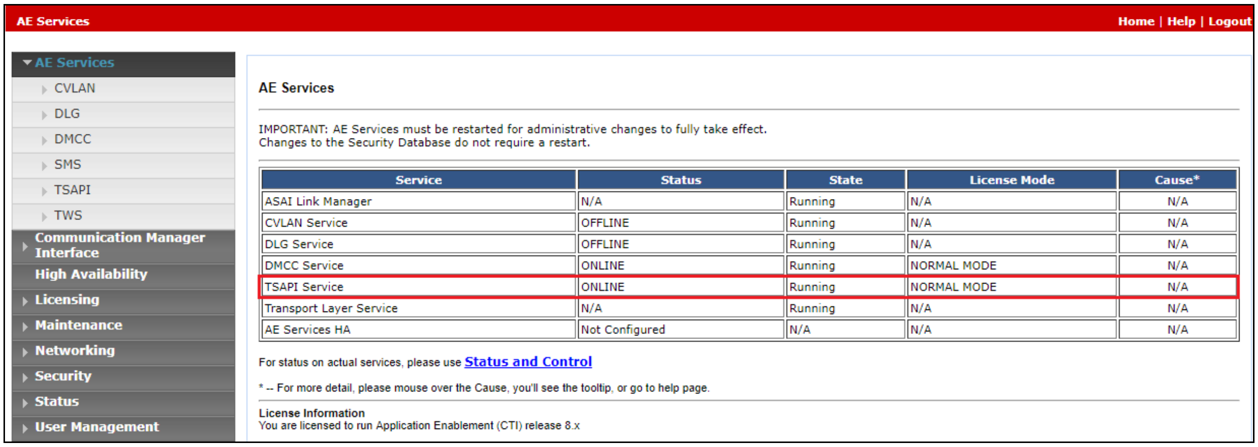
Please login here:

Username cust

Password ••••••

Copyright Â© 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**.



AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

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

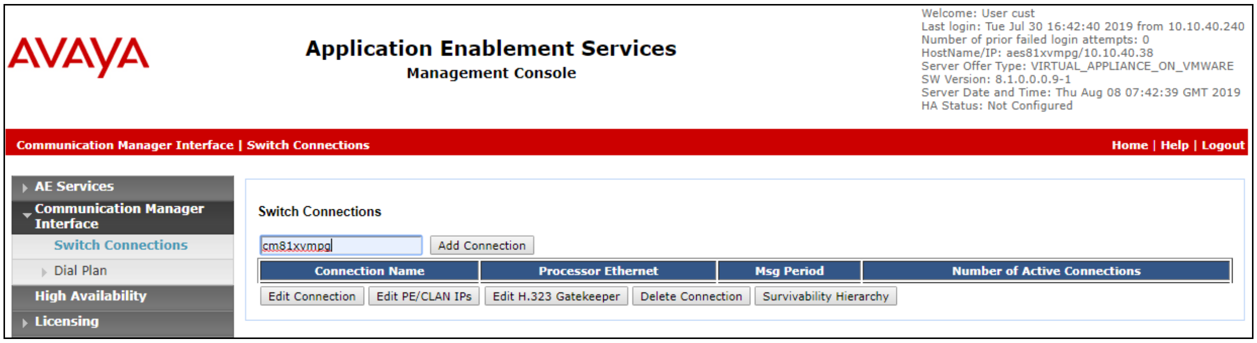
For status on actual services, please use Status and Control

* -- 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

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.



Welcome: User cust
Last login: Tue Jul 30 16:42:40 2019 from 10.10.40.240
Number of prior failed login attempts: 0
HostName/IP: aes81xvmpg/10.10.40.38
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.0.0.0.9-1
Server Date and Time: Thu Aug 08 07:42:39 GMT 2019
HA Status: Not Configured

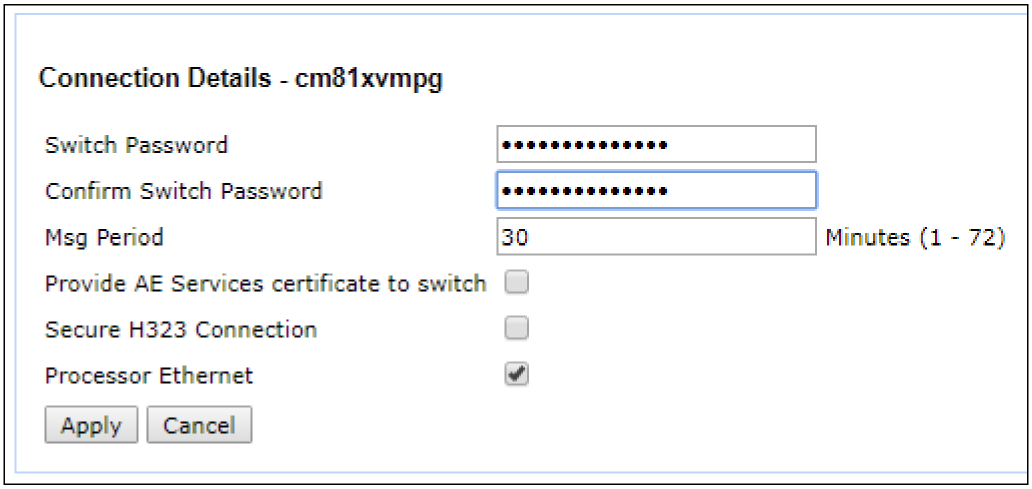
Communication Manager Interface | Switch Connections

Switch Connections

cm81xvmpg [Add Connection]

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

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.



Connection Details - cm81xvmpg

Switch Password: ••••••••••••••

Confirm Switch Password: ••••••••••••••

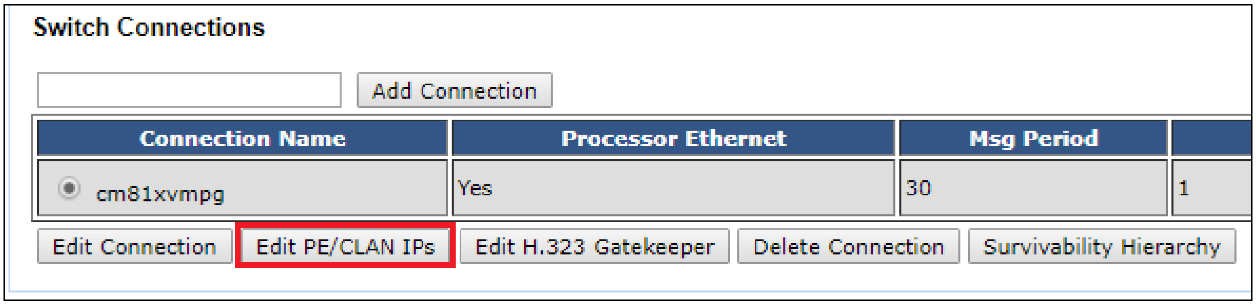
Msg Period: 30 Minutes (1 - 72)

Provide AE Services certificate to switch ☐

Secure H323 Connection ☐

Processor Ethernet ☑

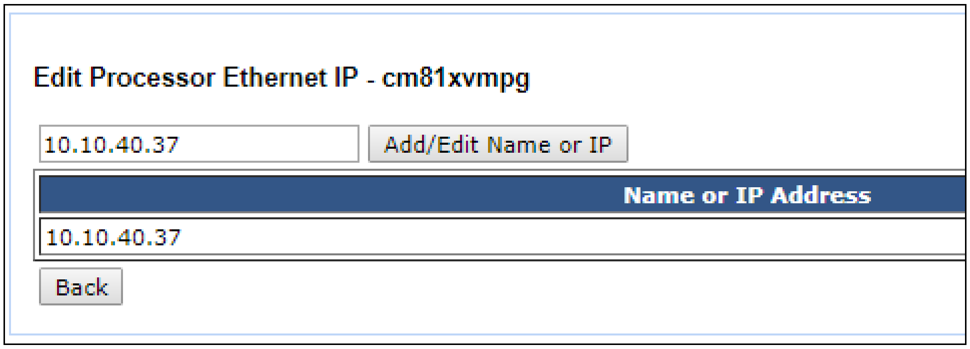
From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button.



Switch Connections

Connection Name	Processor Ethernet	Msg Period	
● cm81xvmpg	Yes	30	1

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



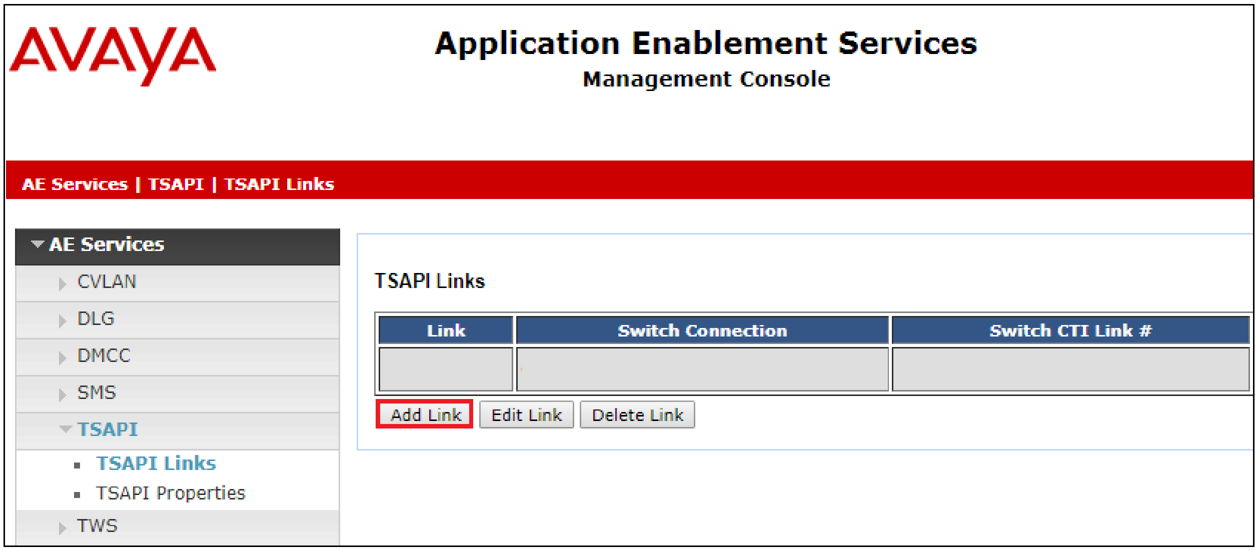
Edit Processor Ethernet IP - cm81xvmpg

10.10.40.37

Name or IP Address
10.10.40.37

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.

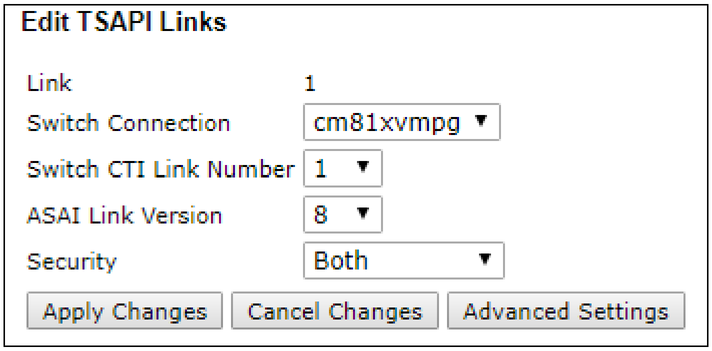


TSAPI Links

Link	Switch Connection	Switch CTI Link #

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

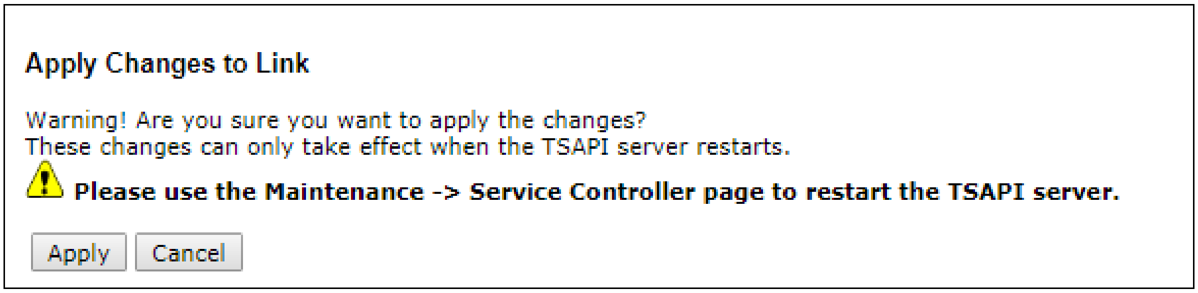
- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm81xvmpg**, which has already been configured in **Section 6.2**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.2.3**.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



Edit TSAPI Links

Link	1
Switch Connection	cm81xvmpg ▼
Switch CTI Link Number	1 ▼
ASAI Link Version	8 ▼
Security	Both ▼

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

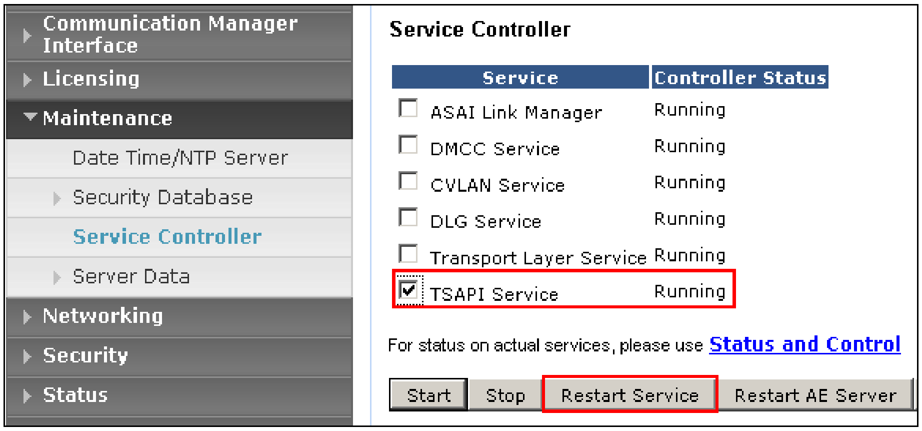


Apply Changes to Link

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

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

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



Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

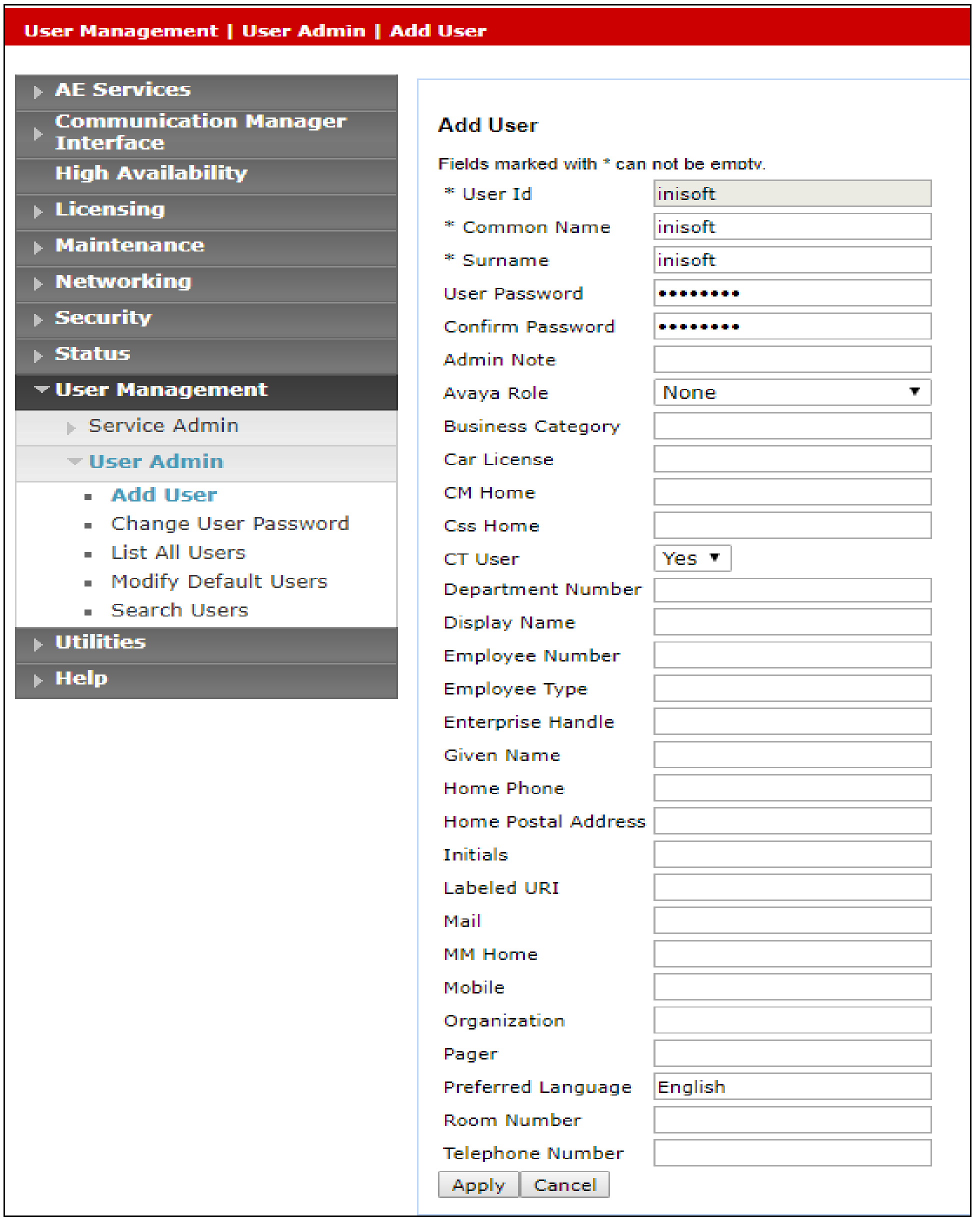
For status on actual services, please use Status and Control

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.



Add User

Fields marked with * can not be empty.

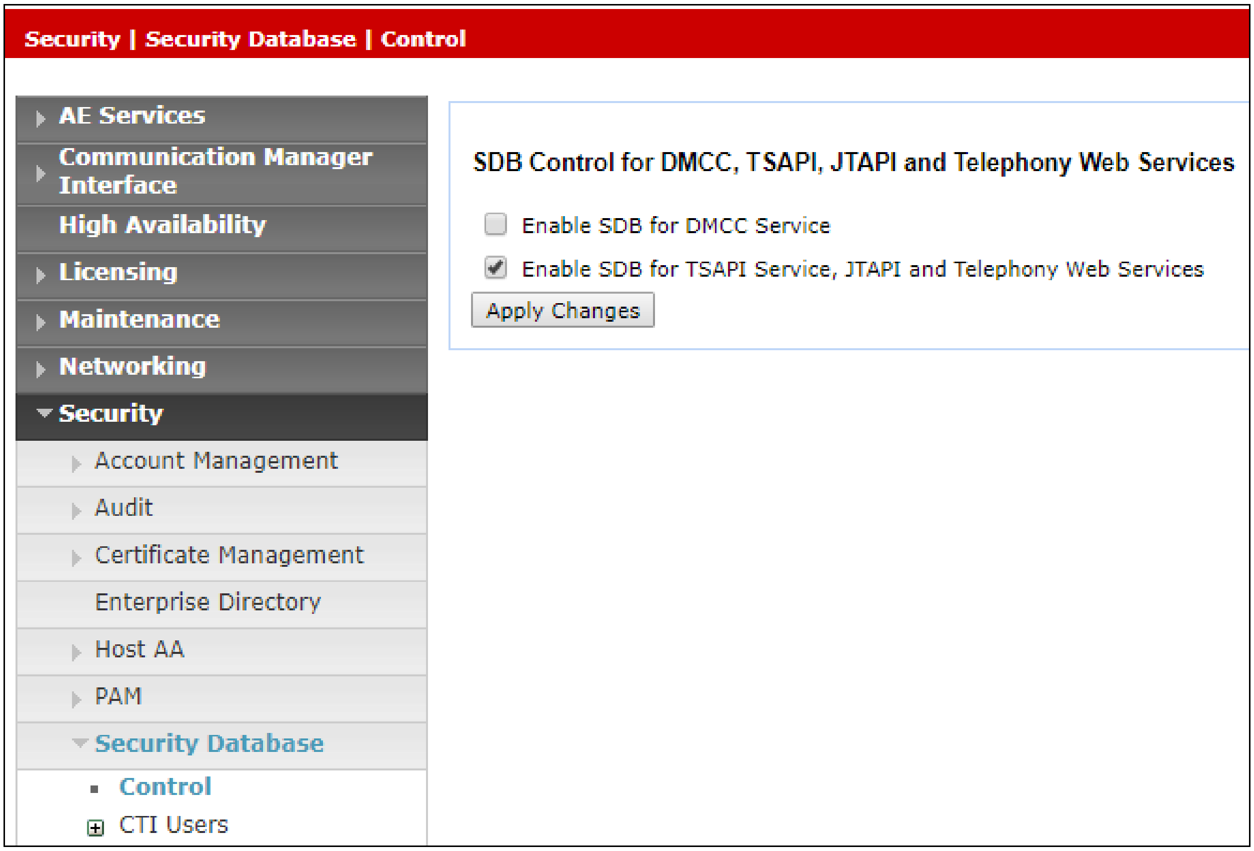
* User Id	inisoft
* Common Name	inisoft
* Surname	inisoft
User Password	••••••••
Confirm Password	••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone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

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 | Security Database | Control

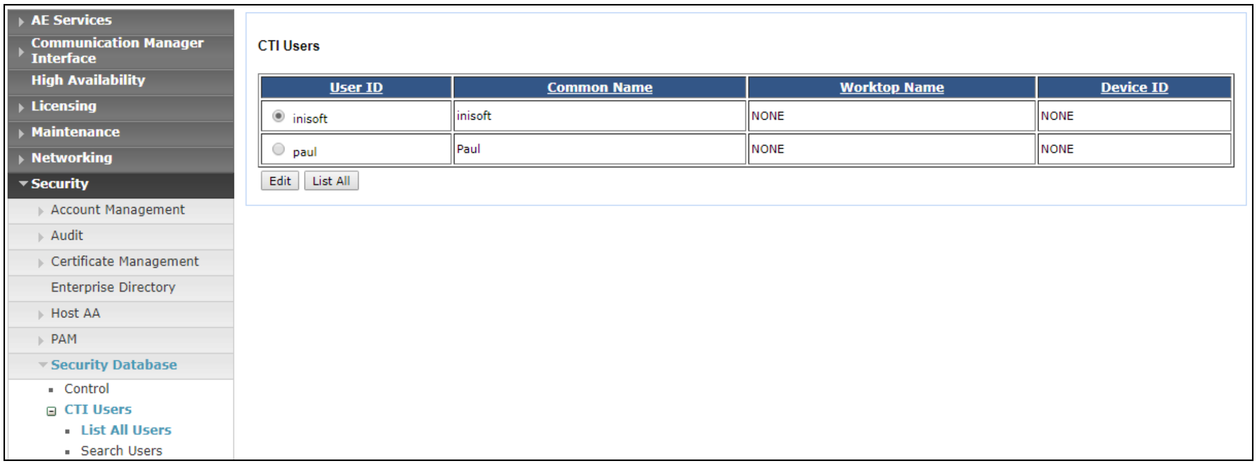
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

□ Enable SDB for DMCC Service

☑ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

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.

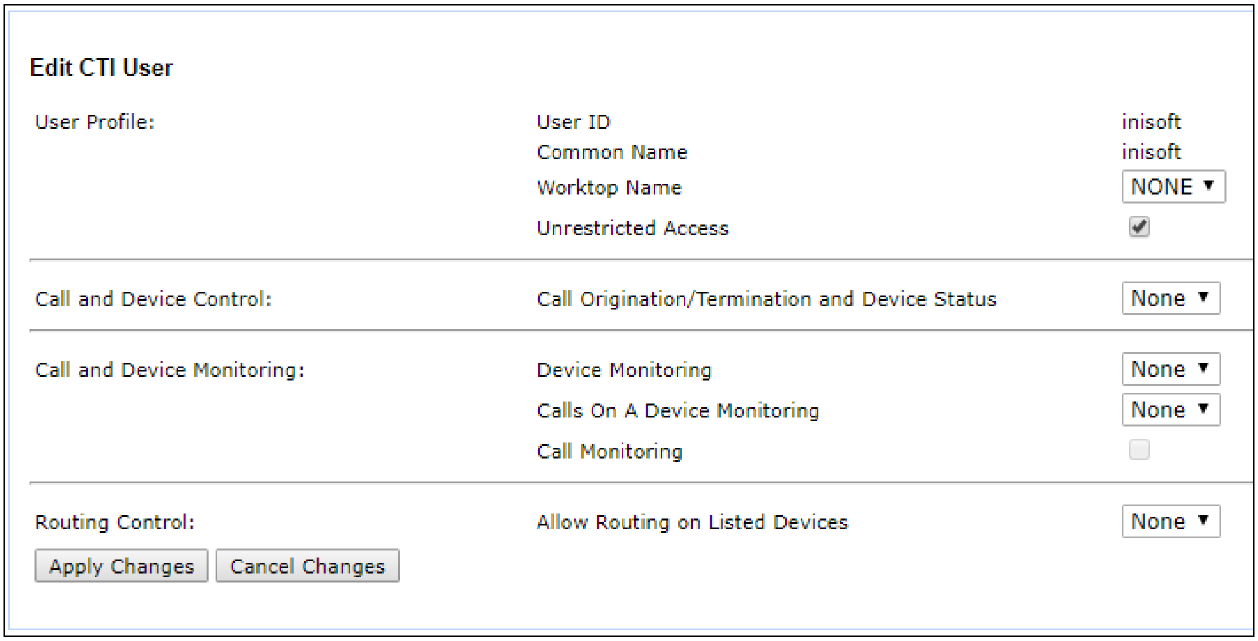


CTI Users

User ID	Common Name	Worktop Name	Device ID
● inisoft	inisoft	NONE	NONE
○ paul	Paul	NONE	NONE

Edit | List All

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



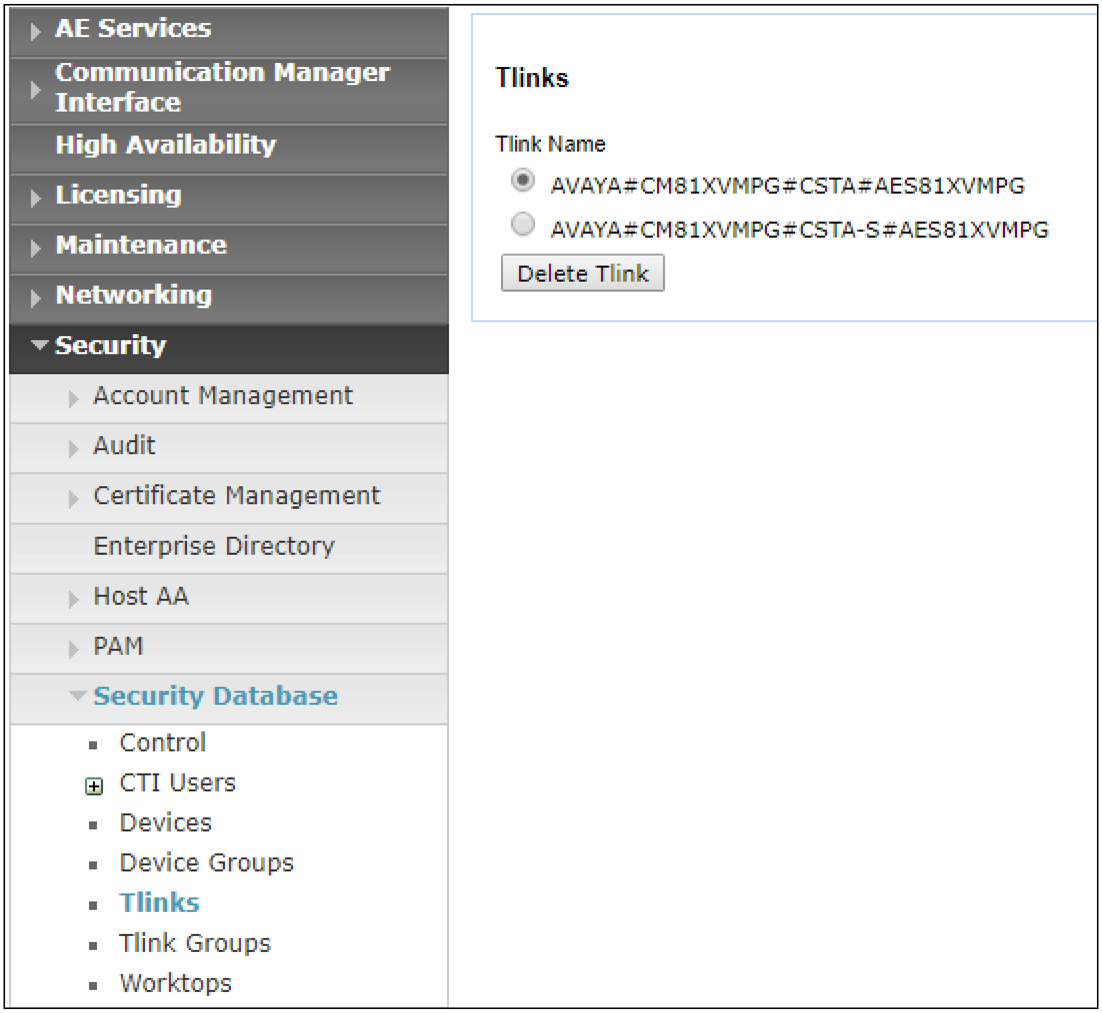
Edit CTI User

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 ▼

Apply Changes | Cancel Changes

5.5.3. Identify Tlinks

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



Tlinks

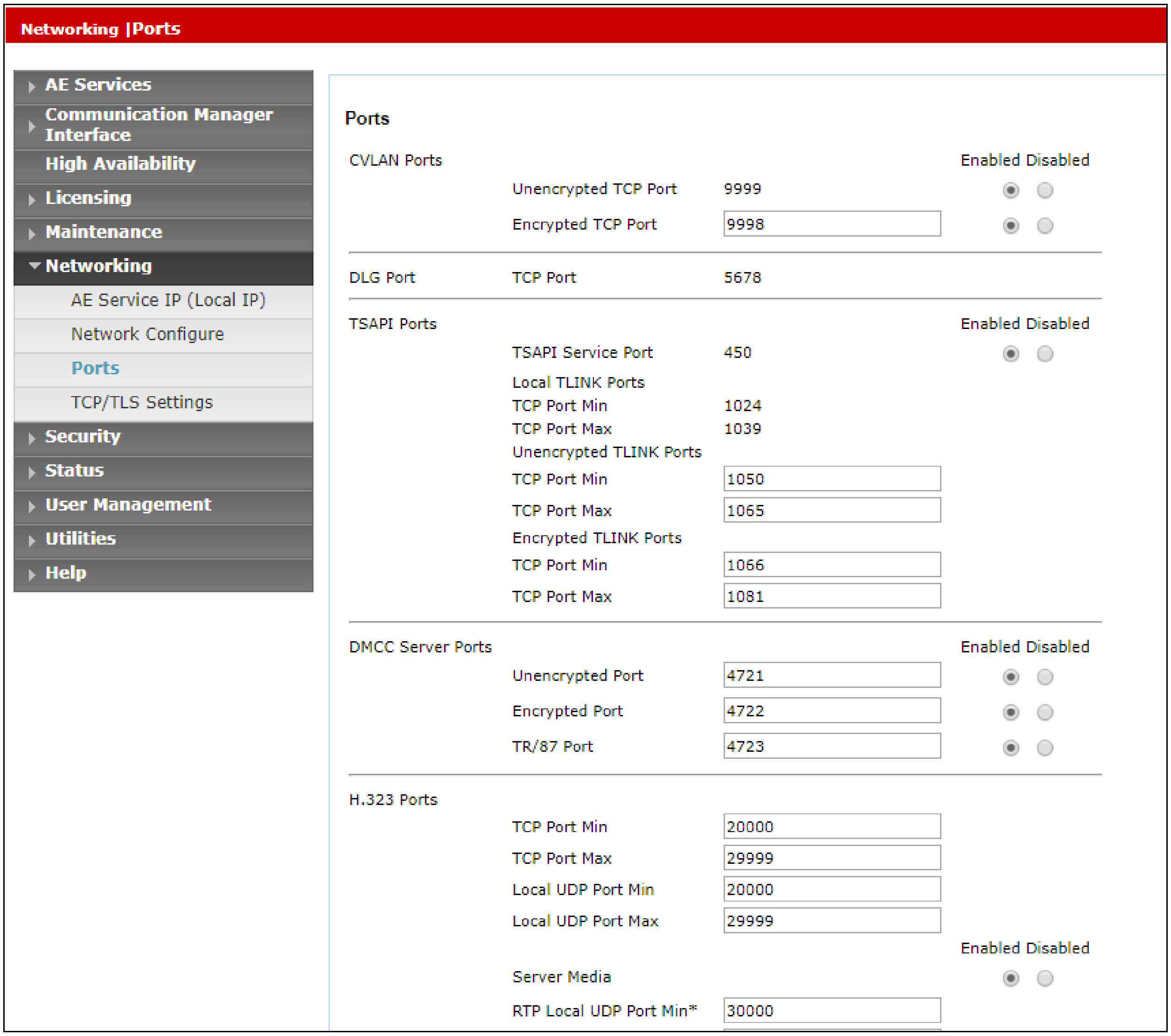
Tlink Name

● AVAYA#CM81XVMPG#CSTA#AES81XVMPG

○ AVAYA#CM81XVMPG#CSTA-S#AES81XVMPG

5.6. Configure Networking Ports

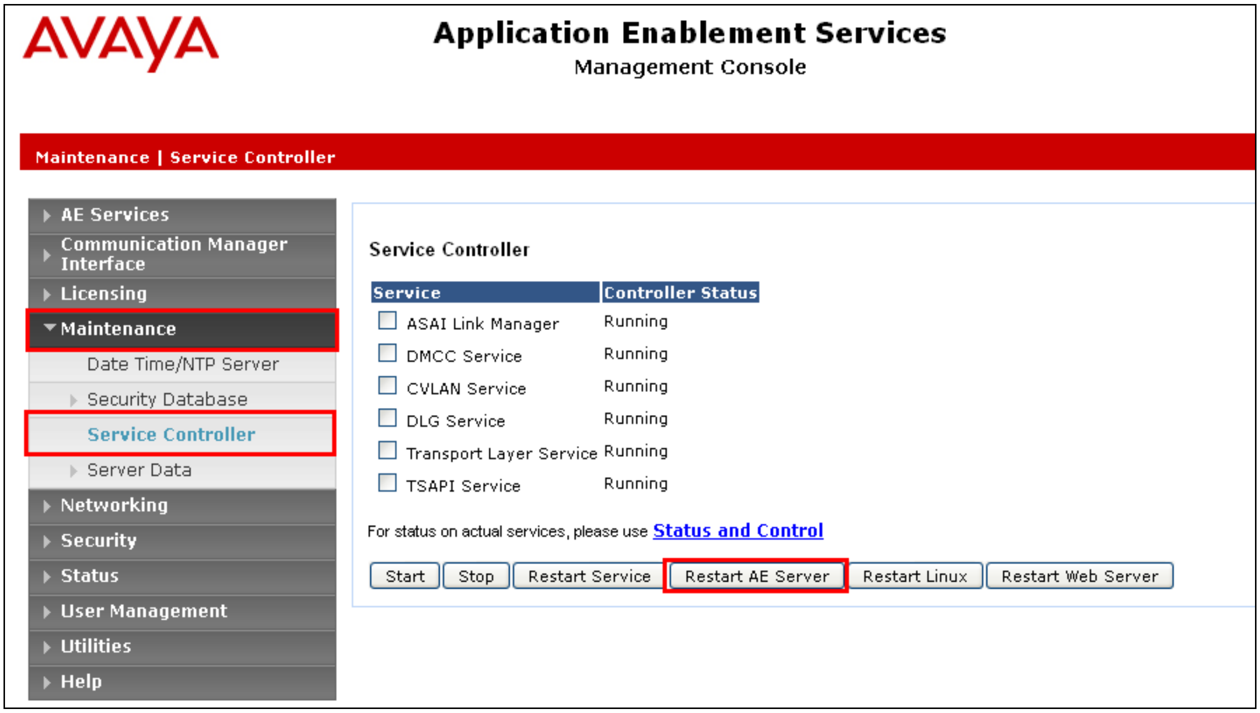
To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.



Ports

CVLAN Ports			Enabled	Disabled
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○
H.323 Ports				
	TCP Port Min	20000		
	TCP Port Max	29999		
	Local UDP Port Min	20000		
	Local UDP Port Max	29999		
			Enabled	Disabled
	Server Media		●	○
	RTP Local UDP Port Min*	30000		

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.



Application Enablement Services

Management Console

Maintenance | Service Controller

Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
□ TSAPI Service	Running

For status on actual services, please use Status and Control

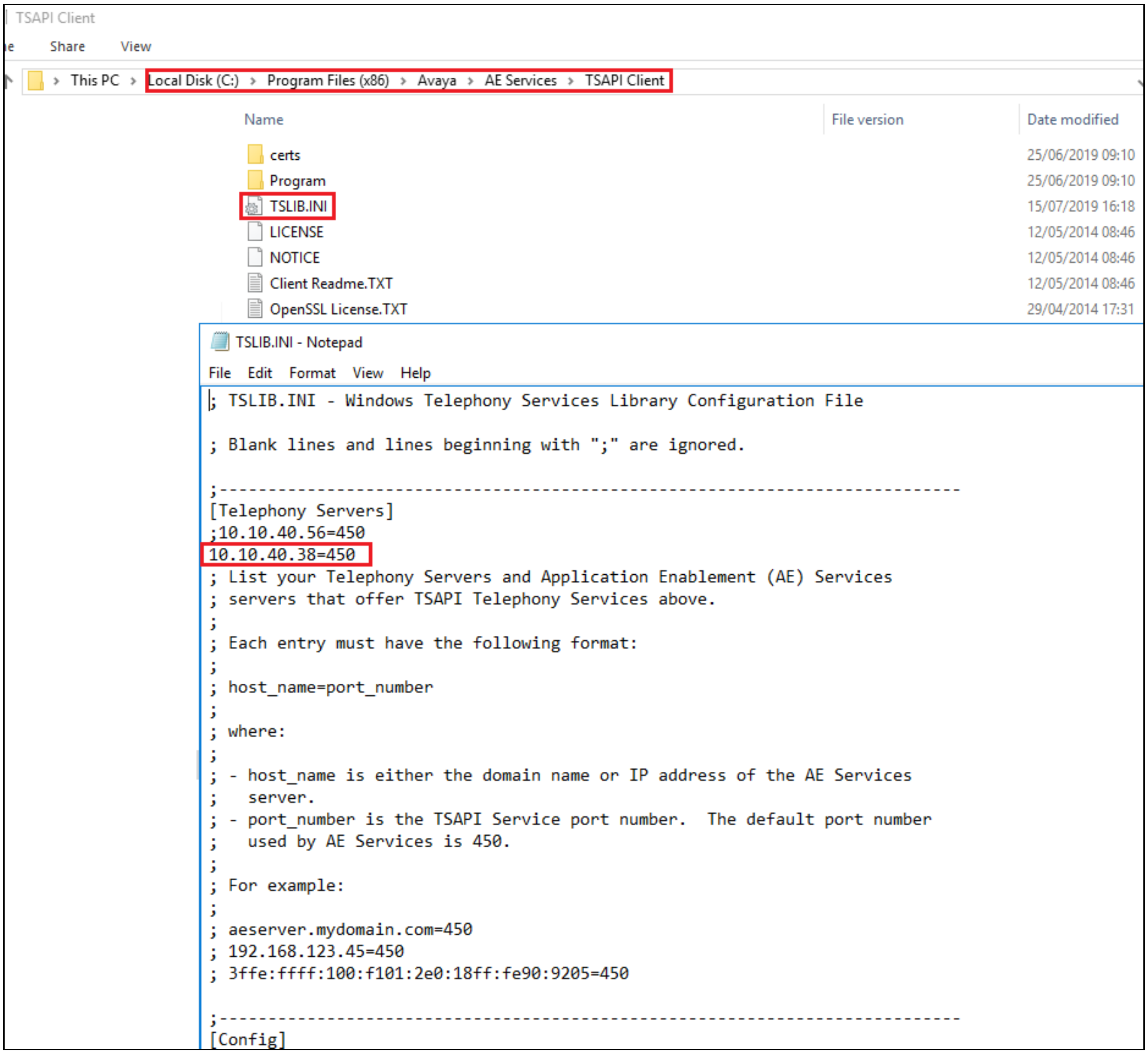
6. Configure Inisoft Syntelate XA

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 wortkzone 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.

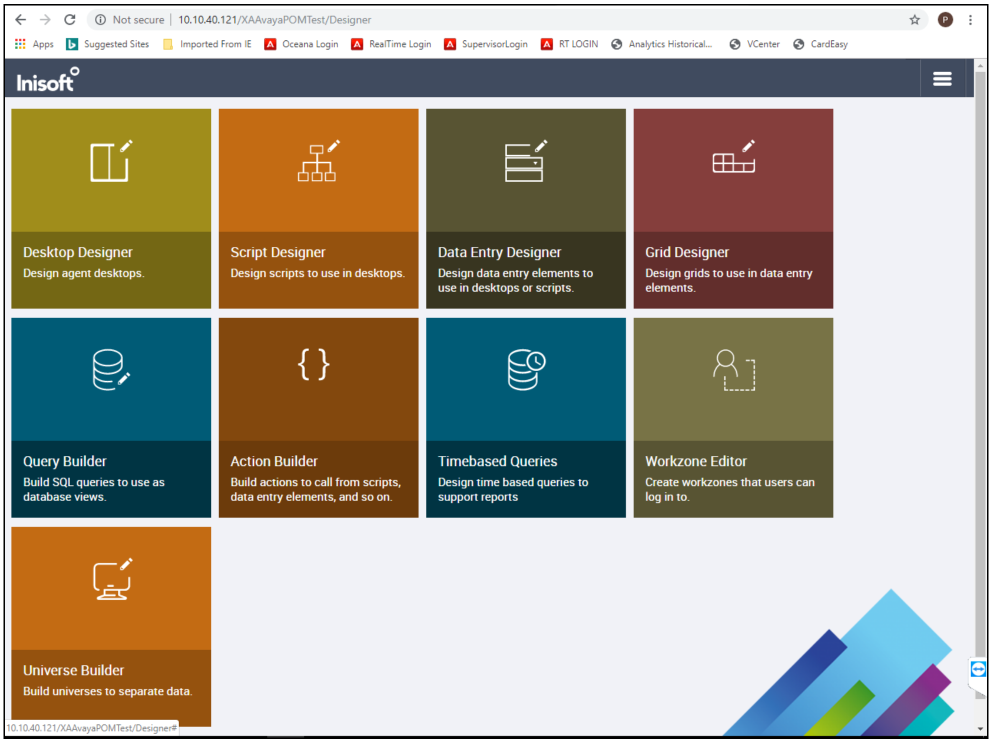

TSAPI Client
e
Share
View
This PC
Local Disk (C:) › Program Files (x86) › Avaya › AE Services › TSAPI Client
TSLIB.INI - Notepad
File
Edit
Format
View
Help

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

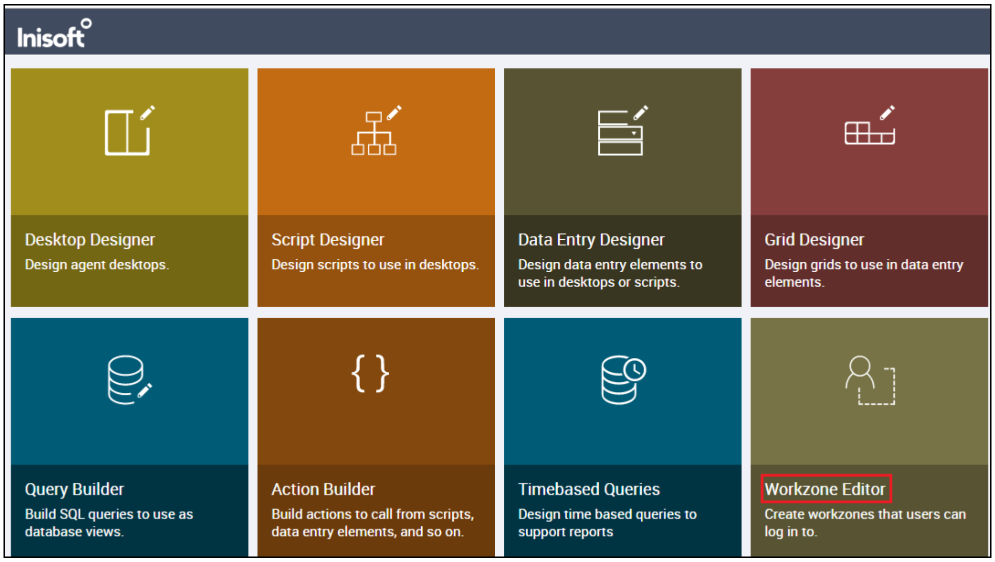
```
; TSLIB.INI - Windows Telephony Services Library Configuration File

; Blank lines and lines beginning with ";" are ignored.

;-----------------------------------------------------------------------------
[Telephony Servers]
;10.10.40.56=450
10.10.40.38=450
; List your Telephony Servers and Application Enablement (AE) Services
; servers that offer TSAPI Telephony Services above.
;
; Each entry must have the following format:
;
; host_name=port_number
;
; where:
;
; - host_name is either the domain name or IP address of the AE Services
;   server.
; - port_number is the TSAPI Service port number.  The default port number
;   used by AE Services is 450.
;
; For example:
;
; aeserver.mydomain.com=450
; 192.168.123.45=450
; 3ffe:ffff:100:f101:2e0:18ff:fe90:9205=450

;-----------------------------------------------------------------------------
[Config]
```

6.2. Configure Syntelate XA Server

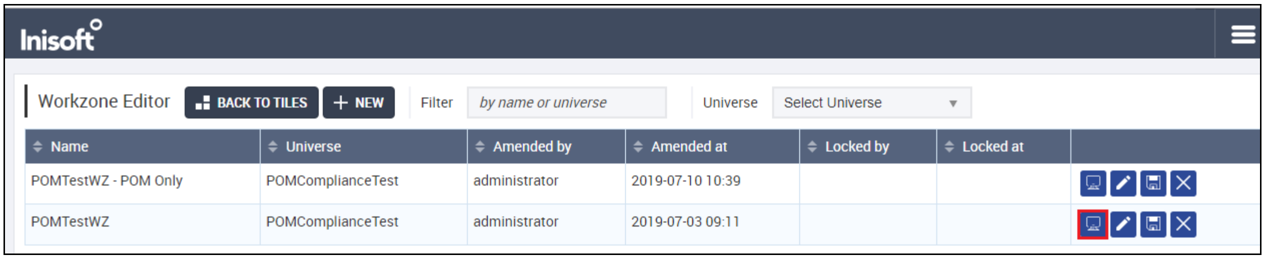
Configuration on the Syntelate XA server is carried out by opening a web browser to the Syntelate XA server's IP address. Open a URL to **http://<SyntelateXAServerIP>/XAAvayaPOMTest/Designer**, (note this will be different on each customer site, this was the address for the Avaya compliance testing).


Not secure | 10.10.40.121/XAAvayaPOMTest/Designer
Apps
Suggested Sites
Imported From IE
Oceana Login
RealTime Login
SupervisorLogin
RT LOGIN
Analytics Historical...
VCenter
CardEasy
Inisoft
Desktop Designer
Design agent desktops.
Script Designer
Design scripts to use in desktops.
Data Entry Designer
Design data entry elements to use in desktops or scripts.
Grid Designer
Design grids to use in data entry elements.
Query Builder
Build SQL queries to use as database views.
Action Builder
Build actions to call from scripts, data entry elements, and so on.
Timebased Queries
Design time based queries to support reports
Workzone Editor
Create workzones that users can log in to.
Universe Builder
Build universes to separate data.
10.10.40.121/XAAvayaPOMTest/Designer#

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

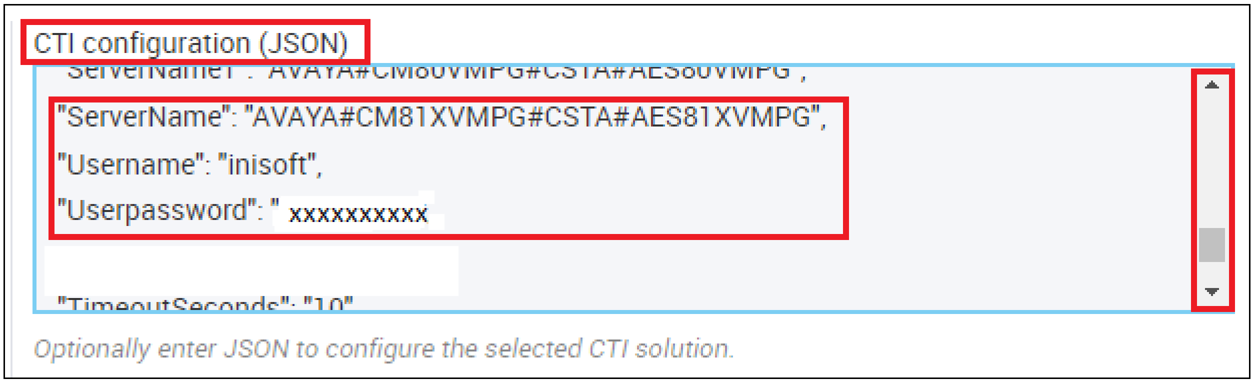

Inisoft
Desktop Designer
Design agent desktops.
Script Designer
Design scripts to use in desktops.
Data Entry Designer
Design data entry elements to use in desktops or scripts.
Grid Designer
Design grids to use in data entry elements.
Query Builder
Build SQL queries to use as database views.
Action Builder
Build actions to call from scripts, data entry elements, and so on.
Timebased Queries
Design time based queries to support reports
Workzone Editor
Create workzones that users can log in to.

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



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

The information on the connection to 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**.



CTI configuration (JSON)

```
 "ServerName": "AVAYA#CM80VMPG#CSTA#AES80VMPG",
"ServerName": "AVAYA#CM81XVMPG#CSTA#AES81XVMPG",
"Username": "inisoft",
"Userpassword": " xxxxxxxxxx


"TimeoutSeconds": "10"
```

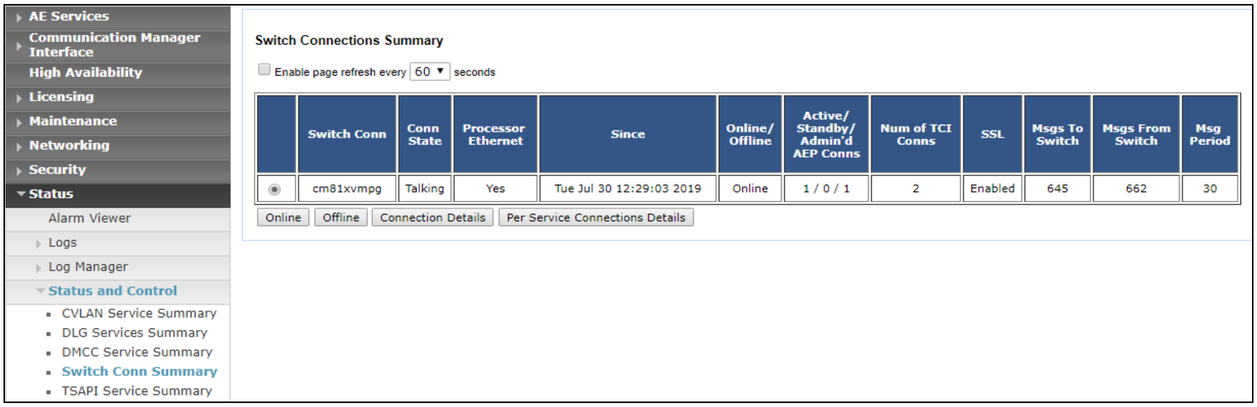
Optionally enter JSON to configure the selected CTI solution.

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.

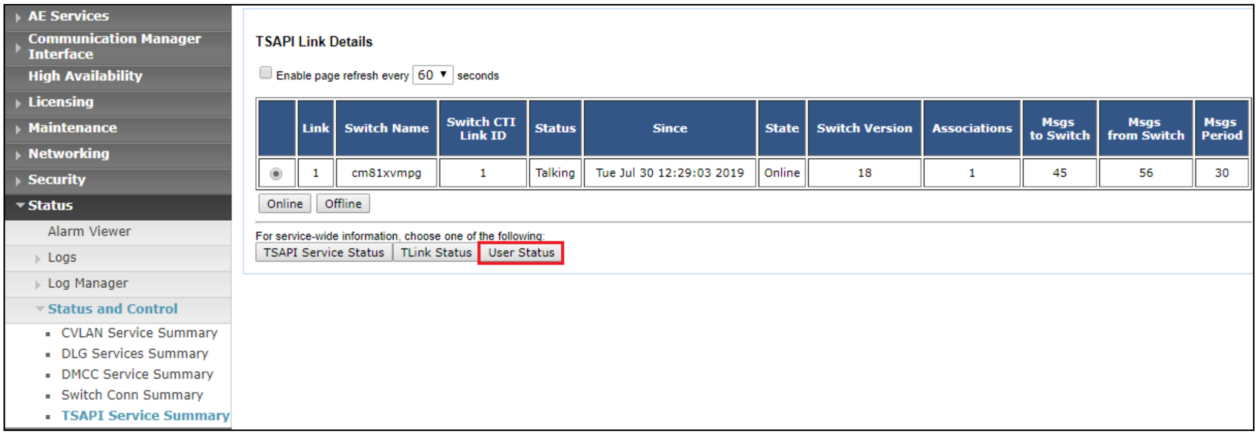


Switch Connections Summary

☐ 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
●	cm81xvmpg	Talking	Yes	Tue Jul 30 12:29:03 2019	Online	1 / 0 / 1	2	Enabled	645	662	30

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



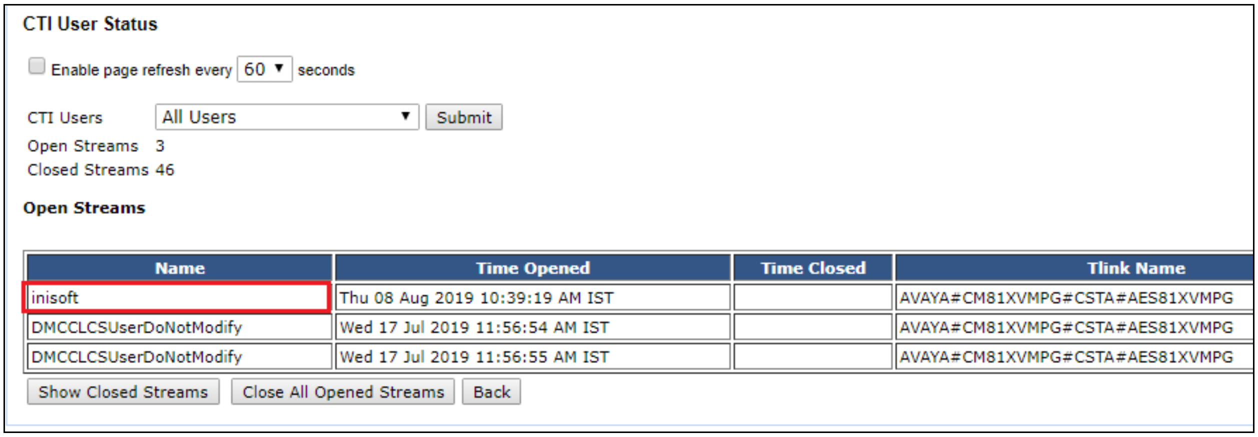
TSAPI Link Details

☐ 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
●	1	cm81xvmpg	1	Talking	Tue Jul 30 12:29:03 2019	Online	18	1	45	56	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 60 ▼ seconds

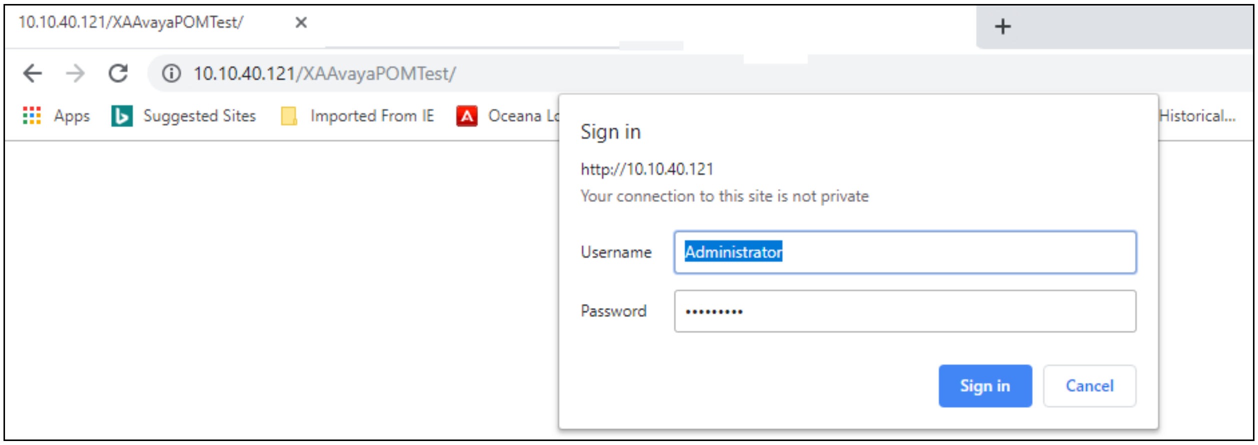
CTI Users All Users ▼ Submit
Open Streams 3
Closed Streams 46

Open Streams

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

7.1.2. Verify the connection from Syntelate XA Desktop

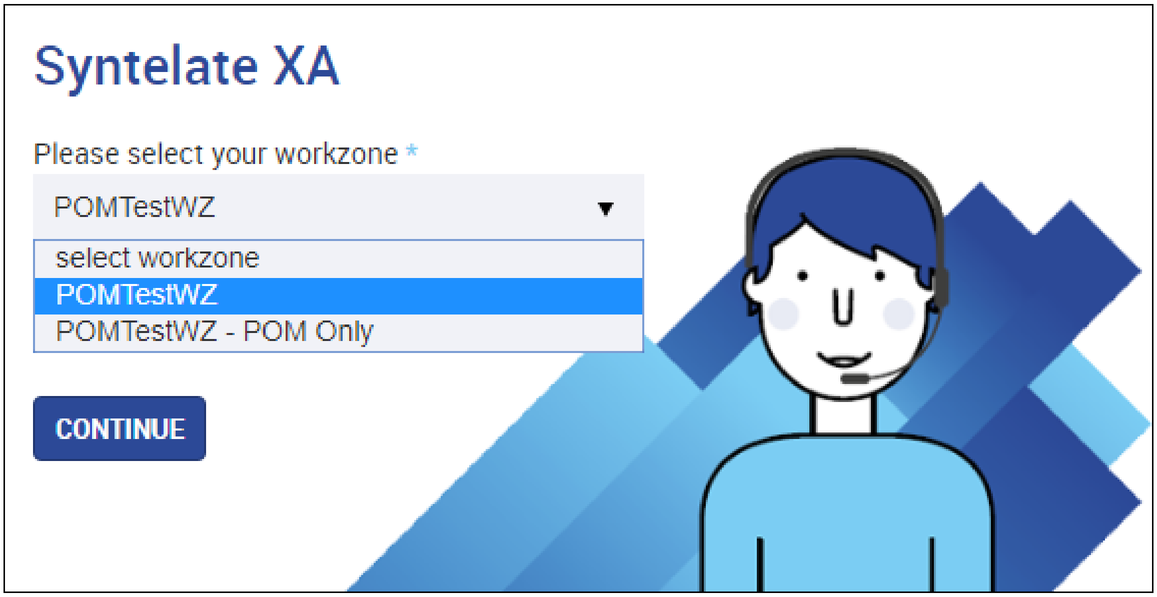
Open a URL to the Syntelate XA server IP address with the appropriate address. The example below is **http://<ServerIP>/XAAvayaPOMTest**/. A new window should appear looking for the username and password of the user setup on the domain or in this case the Syntelate XA server as there is no domain present.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



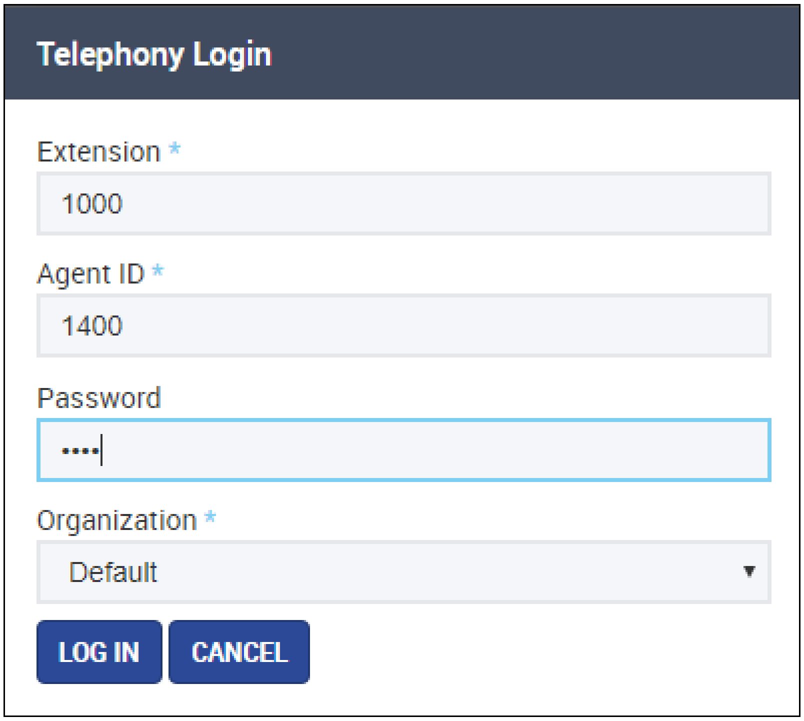
Sign in
http://10.10.40.121
Your connection to this site is not private

Username: Administrator
Password: •••••••••

The following window appears asking to select the **workzone**. The example below shows **POMTestWZ** being selected for the AES connection.



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

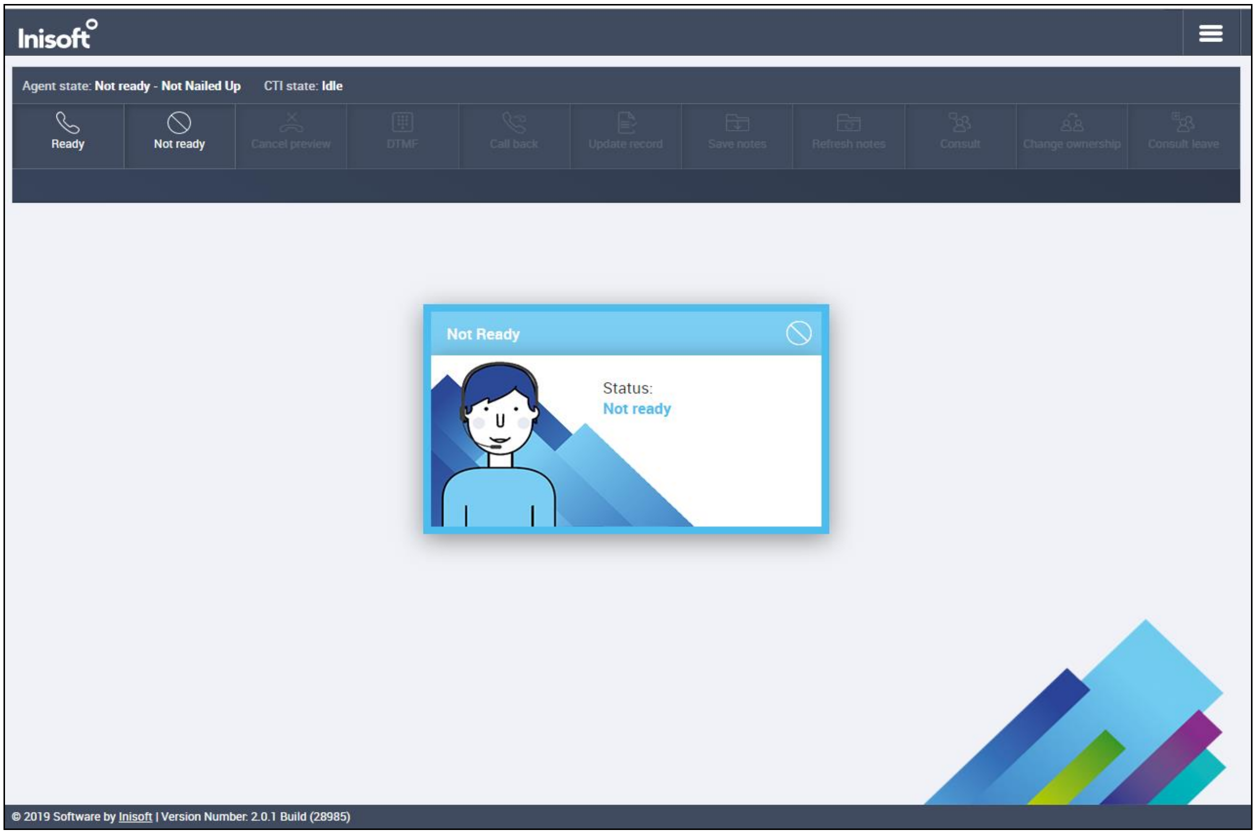
Extension * 1000

Agent ID * 1400

Password ••••

Organization * Default

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.

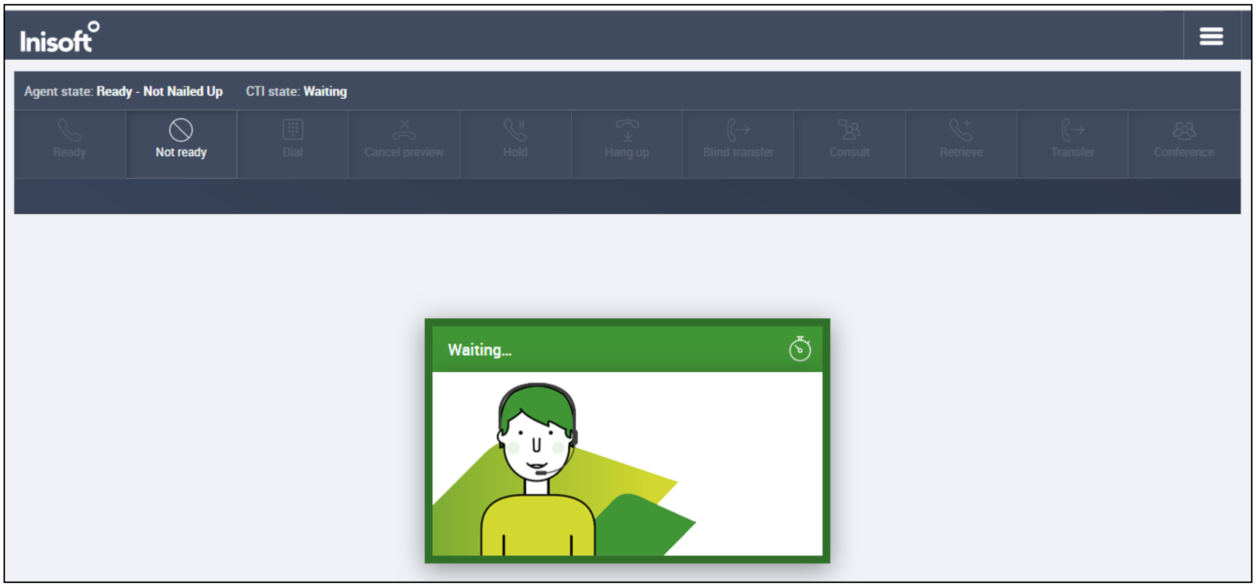


Agent state: Not ready - Not Nailed Up CTI state: Idle

Status: Not ready

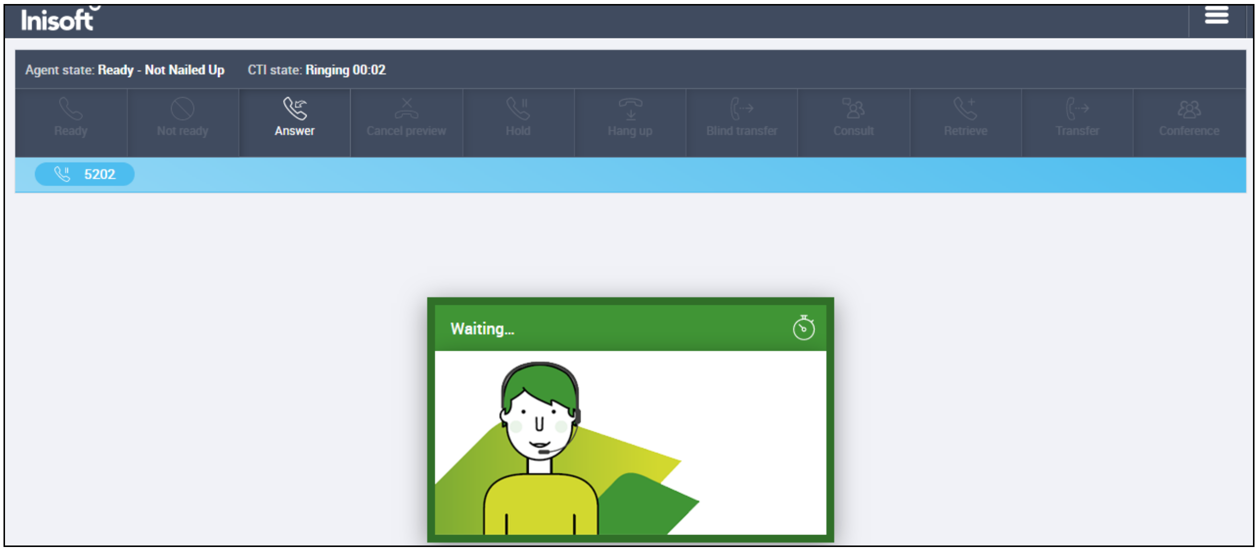
© 2019 Software by Inisoft | Version Number: 2.0.1 Build (28985)

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



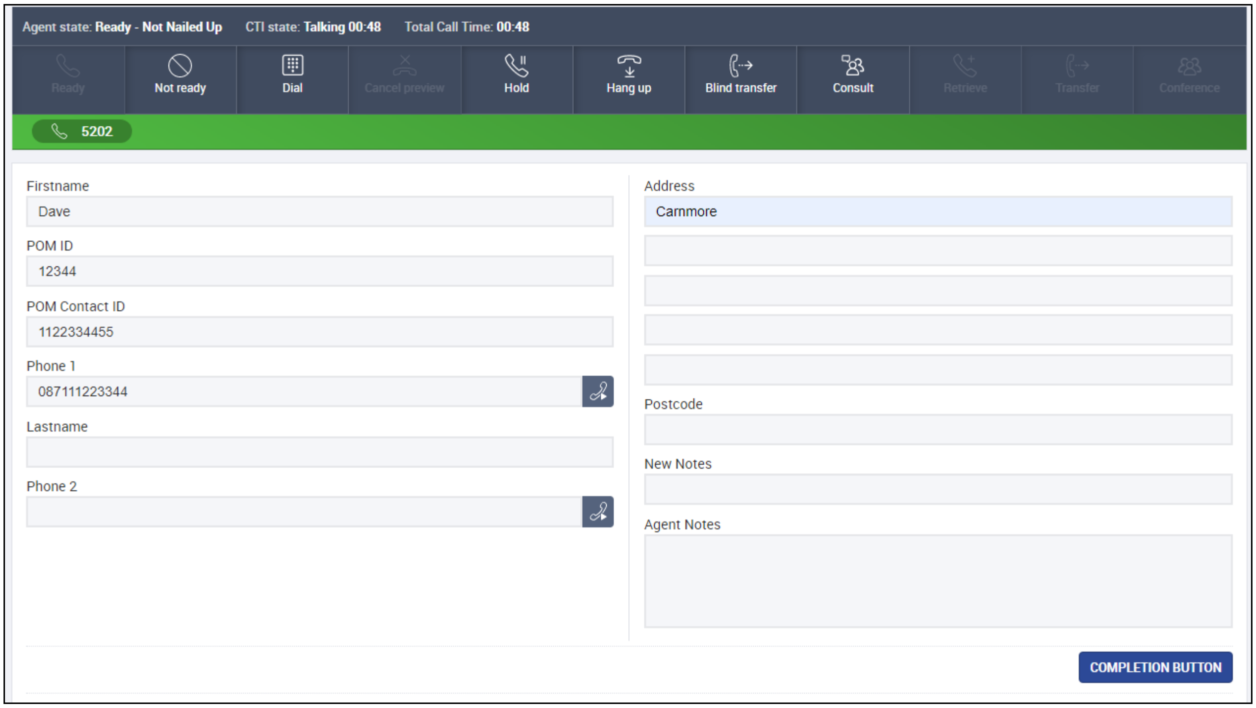
Agent state: Ready - Not Nailed Up CTI state: Waiting

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



Agent state: **Ready - Not Nailed Up** CTI state: **Ringing 00:02**

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



Agent state: **Ready - Not Nailed Up** CTI state: **Talking 00:48** Total Call Time: **00:48**

Firstname: Dave

POM ID: 12344

POM Contact ID: 1122334455

Phone 1: 087111223344

Lastname:

Phone 2:

Address: Canmore

Postcode:

New Notes:

Agent Notes:

8. *C*onclusion

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

[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

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 Dev*Connec*t Program at devconnect@avaya.com.