



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for AMC Driver for Avaya Aura® Application Enablement Services – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required to integrate 3rd party business applications using the AMC Driver for Avaya Aura® Application Enablement Services (AES) with a contact center environment provided by Avaya Aura® Communication Manager.

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 3rd party business applications using the AMC Driver for Avaya Aura® Application Enablement Services (AES) with a contact center environment provided by Avaya Aura® Communication Manager. The AMC Driver for AES provides CTI integration to business applications from Microsoft, Oracle, Salesforce and SAP. The AMC Contact Canvas Server (CCS), which includes the Driver, provides call control, agent session control and screen pop to help make contact center agents more efficient and to realize higher levels of customer satisfaction. CCS and the AMC Driver can also be used for adjunct routing. AES passes the adjunct route request to CCS which leverages Visual Basic (VB) scripting to execute a data dip within the business application and invokes AMC's advanced routing gateway to provide a precise route. For this compliance test, the AMC Driver was used to integrate 5 different CRM adapters with Communication Manager.

The AMC Driver for AES uses a TSAPI connection and requires Basic license for standard integration or Advanced licenses necessary to monitor VDNs if CCS provides adjunct routing. AMC's CCS is built upon component architecture using a Driver/Adapter pattern; Drivers integrate contact channels and Adapters integrate business applications, such as Salesforce. This provides the flexibility to upgrade existing channels and applications or to move to or incorporate new or different channels and applications, and the scalability to integrate contact centers of all size, small, medium, large and enterprise / multi-site.

## 2. General Test Approach and Test Results

To verify interoperability of the AMC Driver with AES and Communication Manager, 5 different CRM applications were used. SAPWeb/CRM7 is one of the business applications used. This business application allowed the functionality available in the AMC Driver to be verified, including logging in and out of a skill, placing and disconnecting calls, exercising basic telephony features, agent session control, and screen pop. The features listed in **Section 2.1** were covered.

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 this DevConnect Application Note 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 this Application Note, the interface between Avaya systems and AMC Driver did not include use of any specific encryption features as requested by AMC Technology.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test verified the following feature functionality available to agents with the AMC Driver for AES.

- Logging in and out of a skill/split.
- Monitoring agent states (e.g., Ready or Not Ready).
- Agent synchronization with agent hardphones.
- Establishing calls with other agents and non-monitored devices and verifying the correct call states.
- Screen pop consisting of customer or business partner information using ANI for calls.
- Basic telephony features such as call hold/resume, blind/supervised transfer, and 3-way conference.
- Restarting the AMC Driver.

## 2.2. Test Results

All test cases were executed and passed. The following observation was noted during the compliance test:

*Best practice – in order to avoid possible synchronization issues between the hardphone and softphone, agents should perform actions in this order: logging in via hardphone → going ready → receiving or making a call → logging into CRM during the call.*

## 2.3. Support

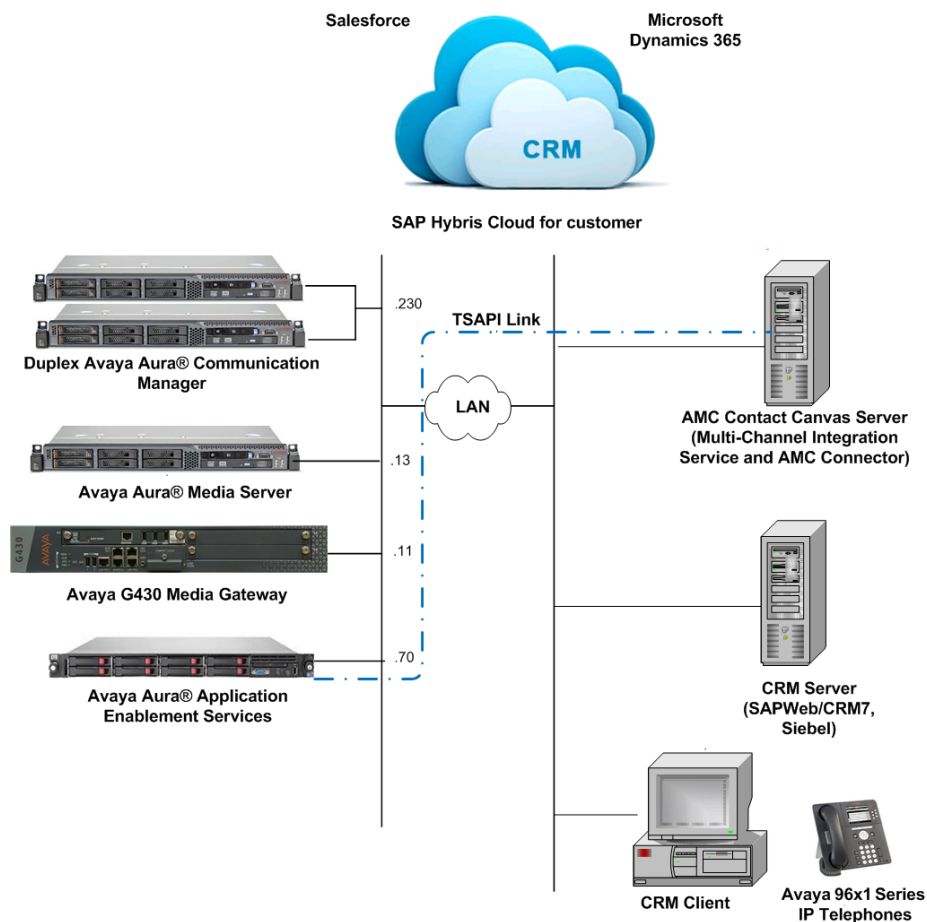
Technical support on the AMC Driver can be obtained through the following:

- **Phone:** +1 (800) 390-4866
- **Email:** [support@amctechnology.com](mailto:support@amctechnology.com)

### 3. Reference Configuration

The following diagram illustrates a sample configuration of a contact center environment integrated with CRM Servers using the AMC Driver for Application Enablement Services. The configuration includes Avaya Aura® Application Enablement Services, a pair of virtual Avaya Aura® Communication Manager Servers with a G430 Media Gateway running Avaya Aura® Communication Manager, and Avaya IP endpoints serving as agent stations. In addition, the agent's interaction center included CRM Web client and separate servers containing the AMC Multi-Channel Integration Server/CCS with the AMC Driver and the CRM server.

Device Type	Value
Skill Group Number	1
Skill Group Extension	13001
VDN	14001
Agent IDs	11001, 11002, 11003
Agent Station Extensions	10001, 10002, 10003



## 4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager	7.1.3
Avaya Aura® Application Enablement Services	7.1.3.0.1.7-0
Avaya G430 Media Gateway <ul style="list-style-type: none"><li>• MGP</li></ul>	39.5.0
Avaya Aura® Media Server	7.8.0.333
Avaya 96x1 Series H.323 IP Deskphone	6.6604
AMC Driver Avaya Aura® Application Enablement Services/Avaya Interaction Center	6.5.0.0
SAPCRM7EHP3	6.5.0.0
Oracle Siebel - On Premise	6.5.0.0
Salesforce.com	6.5.0.0
Microsoft Dynamics 365	6.5.0.0
SAP Hybris Cloud for Customer	6.5.0.0

## 5. Configure Aura® Avaya Communication Manager

This section provides the procedures for configuring Avaya Aura® Communication Manager. The procedures include the following areas:

- Verify Communication Manager license
- Administer CTI link
- Administer agent hunt group
- Administer vector and VDN
- Administer agent station
- Administer agent IDs

### 5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. If this option is not enabled, then contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                               Page 4 of 12
                                OPTIONAL FEATURES

Abbreviated Dialing Enhanced List? y      Audible Message Waiting? y
Access Security Gateway (ASG)? n           Authorization Codes? y
Analog Trunk Incoming Call ID? y           CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y    CAS Main? n
Answer Supervision by Call Classifier? y    Change COR by FAC? n
ARS? y      Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y      Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? n      DCS (Basic)? y
ASAI Link Core Capabilities? y      DCS Call Coverage? y
ASAI Link Plus Capabilities? y      DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n      Digital Loss Plan Modification? y
Async. Transfer Mode (ATM) Trunking? n      DS1 MSP? y
ATM WAN Spare Processor? n      DS1 Echo Cancellation? y
ATMS? y
Attendant Vectoring? y

(NOTE: You must logoff & login to effect the permission changes.)
```

## 5.2. Administer CTI Link

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

<b>add cti-link 3</b>	Page 1 of 3
CTI LINK	
CTI Link: 3	
<b>Extension: 10093</b>	
<b>Type: ADJ-IP</b>	
	COR: 1
<b>Name: TSAPI Service - AES7x</b>	

## 5.3. Administer Agent Hunt Group

Administer an agent hunt group. Agents will log into this split to handle calls coming into the call center. Use the “add hunt-group n” command, where “n” is an available hunt group number. Configure the hunt group as shown below.

<b>add hunt-group 1</b>	Page 1 of 4
HUNT GROUP	
Group Number: 1	ACD? y
Group Name: Sales	Queue? y
Group Extension: 13001	Vector? y
Group Type: ead-mia	
TN: 1	
COR: 1	MM Early Answer? n
Security Code:	Local Agent Preference? n
ISDN/SIP Caller Display: grp-name	
Queue Limit: unlimited	
Calls Warning Threshold: Port:	
Time Warning Threshold: Port:	
SIP URI:	

Navigate to **Page 2** and set the Skill field to 'y'.

<b>add hunt-group 1</b>	HUNT GROUP	Page 2 of 4
<b>Skill? y</b>	Expected Call Handling Time (sec): 180	
AAS? n	Service Level Target (% in sec): 80 in 20	
Measured: both		
Supervisor Extension: 11003		
Controlling Adjunct: none		
VuStats Objective:		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

## 5.4. Administer Vector and VDN

Modify an available vector using the “change vector n” command, where “n” is an existing vector number. The vector will be used to route calls to agents logged into skill 1.

<b>change vector 1</b>	CALL VECTOR	Page 1 of 6
Number: 1	Name: Sales	
Multimedia? n	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 <b>wait-time</b>	<b>2 secs hearing ringback</b>	
02 <b>queue-to</b>	<b>skill 1 pri m</b>	
03 <b>wait-time</b>	<b>900 secs hearing music</b>	
04 <b>disconnect</b>	<b>after announcement none</b>	
05		



Add a VDN using the “add vdn n” command, where “n” is an available extension number. Enter a descriptive **Name** and the vector number from above for **Vector Number**. Retain the default values for all remaining fields.

<b>add vdn 14001</b>	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 14001	
Name*: Call Center	
Destination: Vector Number 1	
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: both Report Adjunct Calls as ACD*? n	
Acceptable Service Level (sec): 20	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	
SIP URI: _____	
* Follows VDN Override Rules	

## 5.5. Administer Agent Station

Below is the configuration of the agent station. Repeat this step for each agent in the call center.

<b>add station 10001</b>	Page 1 of 5
STATION	
Extension: 10001	Lock Messages? n BCC: 0
Type: 9641G	Security Code: * TN: 1
Port: S00002	Coverage Path 1: COR: 1
Name: Agent 1	Coverage Path 2: COS: 1
	Hunt-to Station: Tests? y
STATION OPTIONS	
Loss Group: 19	Time of Day Lock Table:
	Personalized Ringing Pattern: 1
	Message Lamp Ext: 10001
Speakerphone: 2-way	Mute Button Enabled? y
Display Language: english	Button Modules: 0
Survivable GK Node Name:	
Survivable COR: internal	Media Complex Ext:
Survivable Trunk Dest? y	IP SoftPhone? y
	IP Video Softphone? n
	Short/Prefixed Registration Allowed: default
	Customizable Labels? y

## 5.6. Administer Agent IDs

Add an **Agent Login ID** for each agent in the call center using the “add agent-loginID n” command, where “n” is a valid agent ID that adheres to the dial plan. Specify the password used by the agent to log into the split. Repeat this step for each agent in the call center.

```
add agent-loginID 11001                                     Page 1 of 3
                                AGENT LOGINID

      Login ID: 11001                                         AAS? n
      Name: Agent #1                                         AUDIX? n
      TN: 1          Check skill TNs to match agent TN? n
      COR: 1
      Coverage Path:                                         LWC Reception: spe
      Security Code: 1234                                     LWC Log External Calls? n
      Attribute:      AUDIX Name for Messaging:

                                LoginID for ISDN/SIP Display? n
                                Password: 1234
                                Password (enter again): 1234
                                Auto Answer: none
      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**, specify the skill number to which the agent will log in. In the example, the agent will log into skill 1.

<b>add agent-loginID 11001</b>										Page 2 of 3		
AGENT LOGINID												
Direct Agent Skill:										Service Objective? n		
Call Handling Preference: skill-level										Local Call Preference? n		
SN	RL	SL	SN	RL	SL	SN	RL	SL	SN	RL	SL	
1:	1	1	16:			31:			46:			
2:			17:			32:			47:			
3:			18:			33:			48:			
4:			19:			34:			49:			
5:			20:			35:			50:			
6:			21:			36:			51:			
7:			22:			37:			52:			
8:			23:			38:			53:			
9:			24:			39:			54:			
10:			25:			40:			55:			
11:			26:			41:			56:			
12:			27:			42:			57:			
13:			28:			43:			58:			
14:			29:			44:			59:			
15:			30:			45:			60:			

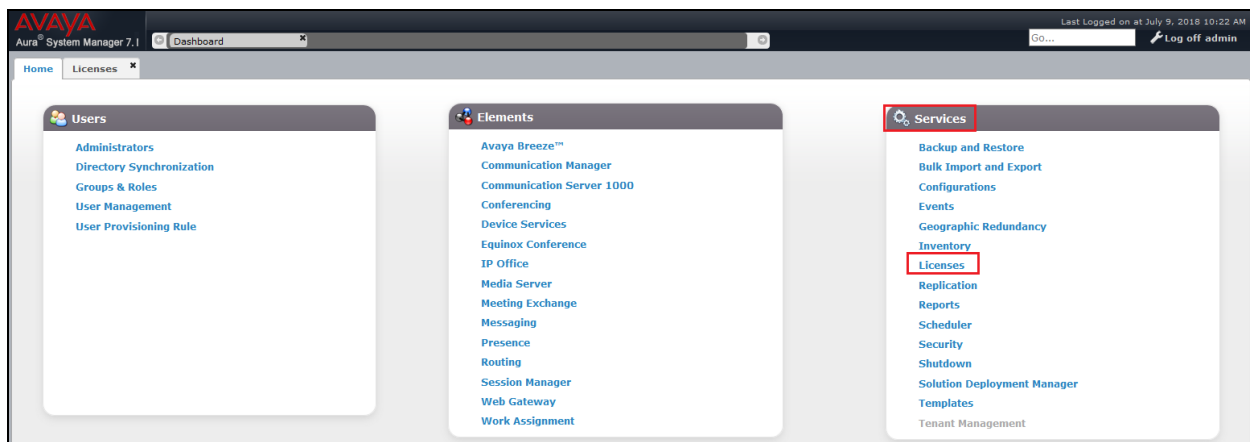
## 6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Avaya Aura® Application Enablement Services. The procedures include the following areas:

- Verify TSAPI license
- Launch OAM interface
- Administer TSAPI link
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer user for AMC Driver

### 6.1. Verify TSAPI License

Access the Web-based License Manager interface by using the URL “https://<ip-addr>/WebLM/” in an Internet browser window, where <ip-addr> is the IP address of the Application Enablement Services server. In this compliance testing, the Web-based License manager is accessed through the Avaya Aura® System Manager. From the home page, select **Services → Licenses**.



On the WebLM home page displayed below, select **Licensed Products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane to display the **Licensed Features** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** as shown below. Also verify that there is an applicable advanced switch license for the switch type.

Licensed products

APPL\_ENAB

▼ Application\_Enablement

View license capacity

View peak usage

AVP

► AVP

CE

► COLLABORATION\_ENVIRONMENT

COMMUNICATION\_MANAGER

► Call\_Center

► Communication\_Manager

Configure Centralized Licensing

MESSAGING

► Messaging

MSR

► Media\_Server

SYSTEM\_MANAGER

► System\_Manager

SessionManager

► SessionManager

VSS

► Voice\_Portal

Uninstall license

Licensed products

APPL\_ENAB

▼ Application\_Enablement

Application Enablement (CTI) - Release: 7 - SID: 10503000

You are here: Licensed Products > Application\_Enablement > View License Capacity

License installed on: August 11, 2017 6:42:55 AM +00:00

License File Host IDs: V1-FD-9E-A1-20-FC-01

Licensed Features

13 Items Show All

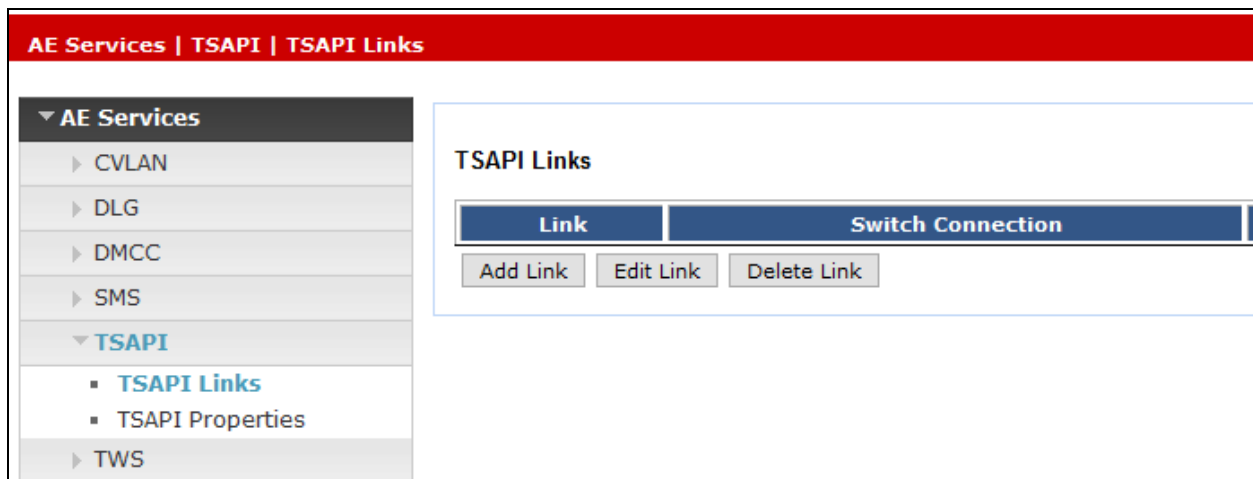
Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	2500
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	10
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	2500
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	1
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	10
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	1
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	2500

## 6.2. Launch OAM Interface

Access the OAM web-based interface y using the URL “https://<ip-addr>” in an Internet browser window, where <ip-addr> is the IP address of the Application Enablement Services server. Log in using the appropriate credentials.

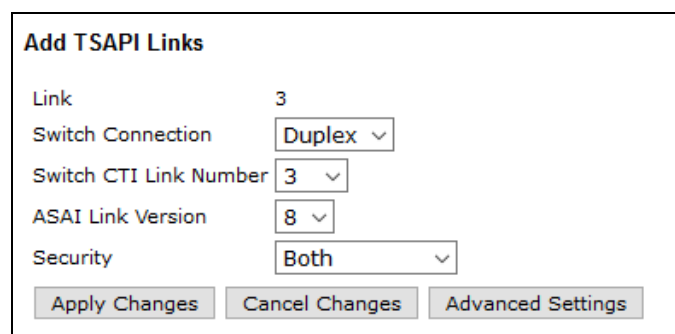
## 6.3. Administer TSAPI Link

To administer a TSAPI link, select **AE Services**→**TSAPI**→**TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed as shown below. Click **Add Link**.



The screenshot shows the 'TSAPI Links' screen. On the left is a navigation pane with a tree structure: 'AE Services' is expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TSAPI Links' (selected), 'TSAPI Properties', and 'TWS'. The main content area is titled 'TSAPI Links' and contains a table with two columns: 'Link' and 'Switch Connection'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection “Duplex” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields and click **Apply Changes**.



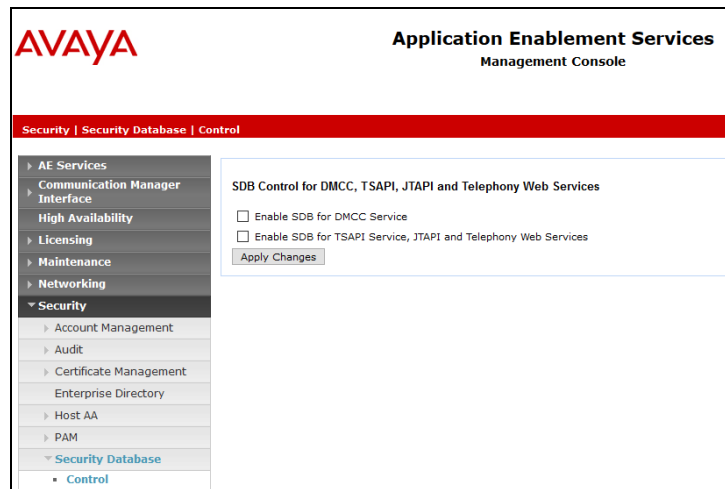
The 'Add TSAPI Links' form contains the following fields and values:

Field	Value
Link	3
Switch Connection	Duplex
Switch CTI Link Number	3
ASAI Link Version	8
Security	Both

At the bottom of the form are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

## 6.4. Disable Security Database

Select **Security**→**Security Database**→**Control** from the left pane to display the **SDB Control for DMCC and TSAPI** screen. Uncheck **Enable SDB TSAPI Service, JTAPI and Telephony Service** and click **Apply Changes**.



## 6.5. Restart TSAPI Service

Select **Maintenance**→**Service Controller** from the left pane to display the **Service Controller** screen. Check the **TSAPI Service** and click **Restart Service**.

Maintenance | Service Controller

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Service Controller

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

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

Start

Stop

Restart Service

Restart AE Server

Restart Linux

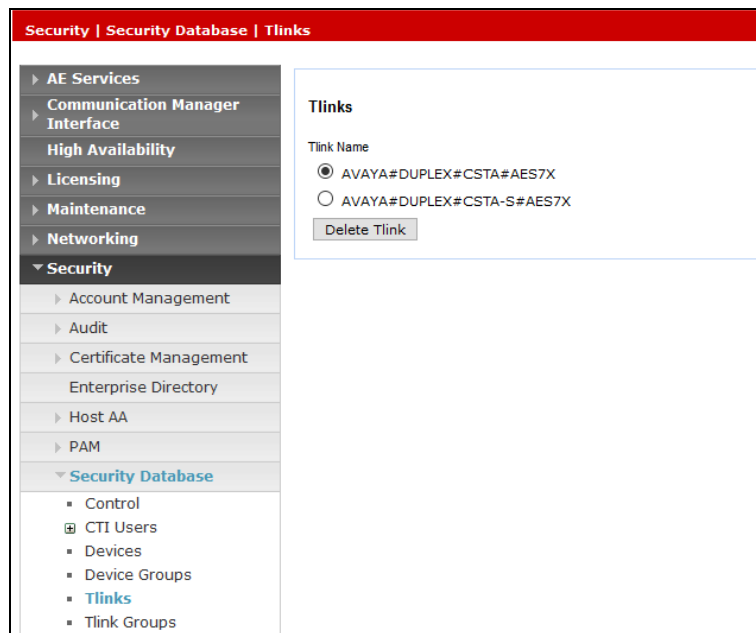
Restart Web Server



## 6.6. Obtain Tlink Name

Select **Security**→**Security Database**→**Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, which will be used later for configuring the AMC Driver.

In this case, the associated Tlink name is “AVAYA#**DUPLEX**#CSTA#AES7X”. Note the use of the switch connection “**DUPLEX**” from **Section 6.3** as part of the Tlink name.



## 6.7. Administer User for AMC Driver

Select **User Management**→**User Admin**→**Add User** from the left pane to display the **Add User** screen.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).

The screenshot shows the 'Edit User' form within the Avaya User Management application. The left sidebar contains a navigation menu with categories like AE Services, Communication Manager, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Service Admin, User Admin, Utilities, and Help. The 'User Admin' section is expanded, showing options: Add User, Change User Password, List All Users (highlighted), Modify Default Users, and Search Users. The main form area is titled 'Edit User' and contains the following fields:

- \* User Id: CRTADM
- \* Common Name: AMC
- \* Surname: AMC
- User Password: [masked with dots]
- Confirm Password: [masked with dots]
- Admin Note: [empty text box]
- Avaya Role: None (dropdown menu)
- Business Category: [empty text box]
- Car License: [empty text box]
- CM Home: [empty text box]
- Css Home: [empty text box]
- CT User: Yes (dropdown menu)
- Department Number: [empty text box]
- Display Name: [empty text box]
- Employee Number: [empty text box]
- Employee Type: [empty text box]

## 7. Configure AMC Driver for Application Enablement Services

This section covers the procedure for configuring the AMC Driver and integrating it with Application Enablement Services using a TSAPI link.

- Verify that the Avaya Aura® Application Enablement Services TSAPI Client MS Windows 7.1 has been installed on the AMC Contact Canvas server.
- Modify the **config.ini** in the C:\Program Files\AMC Technology\MCIS directory as follows. Note that the complete file is not shown below. Some of the key parameters for integration with Application Enablement Services include:
  - the **Module Class** and **Module** parameters which specify the driver under the Avaya CT/AES comment,
  - the Avaya AES license under **License Manager**, and
  - the CTIModule section which includes the Channel (default value of CT1 is recommended), the **ServerID** or Tlink name obtained in **Section 0**, and the user login credentials configured in **Section 6.7**.

```
#####
# MCIS Configuration file: Config.ini with ACT/AES Driver and SFDC -
#                               Avaya Certification lab in Singapore
# MCIS Release 6.5.2
#####

###
# Global Keys
#   Applies to every module that does not explicitly set their local value
###
[Global]
#   MessageLibrary=AMCMessages.dll
#   EventManager=EventManager
#   TraceMaxSize=1024
TraceEnabled=1
TraceLevel=4
TracePath=C:\Program Files(x86)\AMC Technology\MCIS\Server\Logs

...

### Avaya CT/AES
ModuleClass=CentreVuCTI,CentreVuCTI.CentreVuCTIModule
Module=CTIModule,CentreVuCTI

...

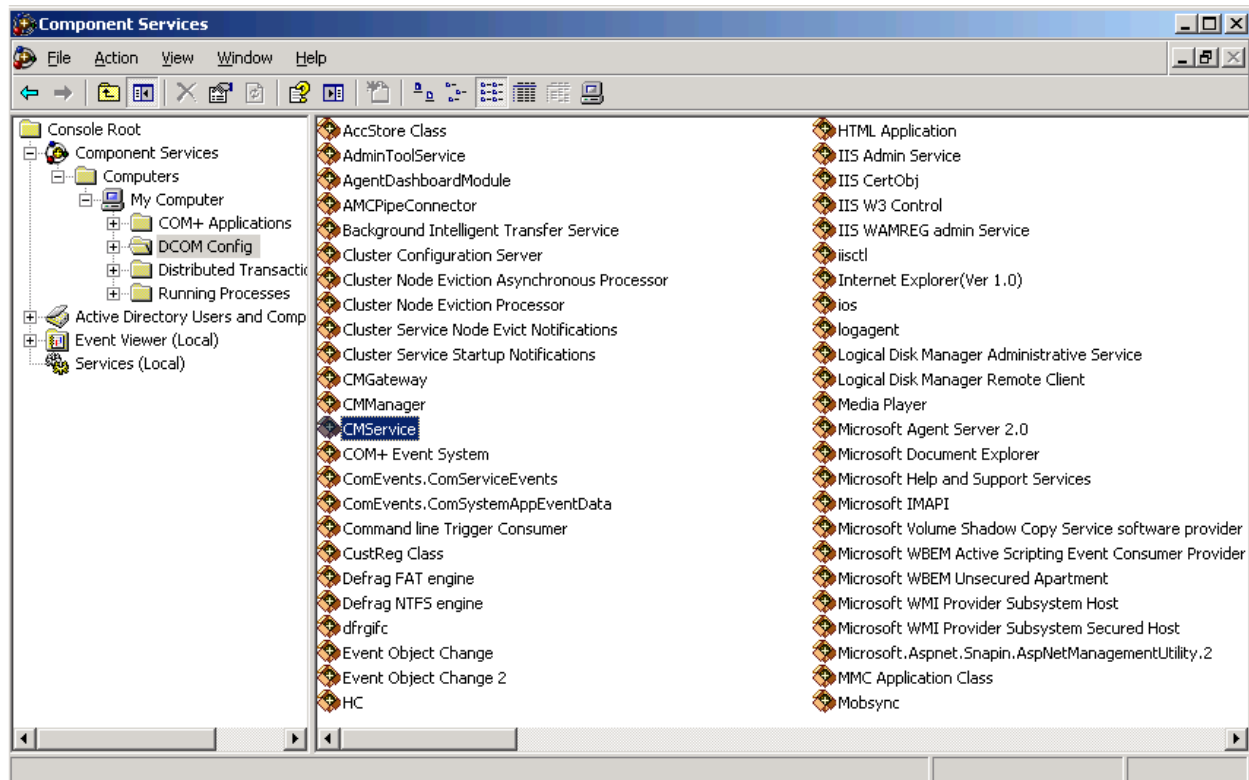
###
# License Manager
#
###
[LicenseManager]
#   TraceEnabled=1
#   TraceLevel=2
#   TraceMaxSize=1024
MCIS=DMBVHKJLDEFGEJDGFBATCJAJGBEFDMMLGOPKNTR
```

```
AA-DOTNET=DMBVHRJPDXFEEGDJFGBDVEFAJGBEFDMMLGOPKNTR
CTI_CentreVu=DZBLHUJKDCFDEEDIFBBFTBDAJGBEFDZMLGOPKNTR
```

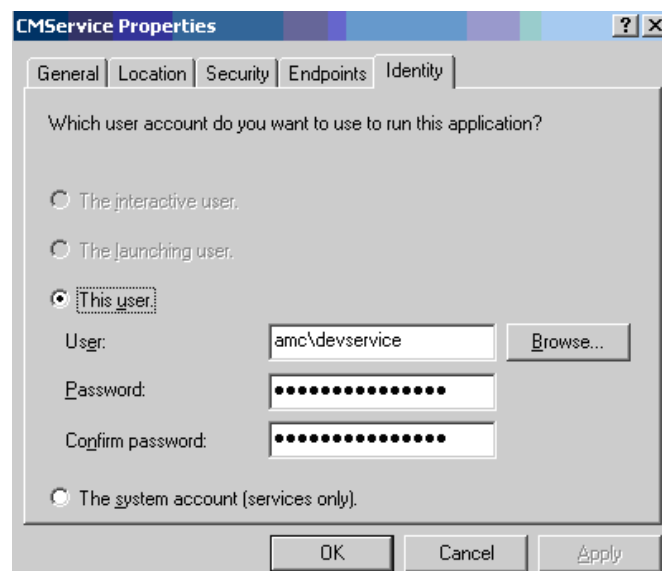
```
## For ACT
[CTIModule]
TraceLevel=4
Channel=CTI1
#ServerID=LUCENT#G3_SWITCH#CSTA#AMCW23S09
ServerID=AVAYA#DUPLEX#CSTA#AES7X
UserName=CRTADM
#UserName=AMC
Password=*****
#Password=Connector#123
AllowDTMF=Yes
DTMFPause=5
#ForceStateRefresh=1
UseAutoIn=1

###
# IciAdapter
#
###
[IciAdapter]
#ProxyForEvents=http://localhost:8080
TraceLevel=6
ConfigDBHost=(local)\SQLEXPRESS
ConfigServerName=AMCW12CCSVASU
ConfigDBUser=sa
ConfigDBPass=Amcw12ccsvasu
EventHandlingLevel=6
NEventHandlingLevel=6
NewHandleOnWarmTransfer=False
NewHandleOnConference=False
WaitForCallStateUpdateDelay=1500
DropCreatedItemAfterFailedDial=False
DropCreatedItemAfterFailedConsult=False
CheckCallStateAfterConosult=True
CheckCallStateAfterDial=True
UseExtensionForAlternate=False
DefaultNotReadyReasonCode=3
DataStore=DataStore
ContactDataKeyName=CAD
ListenForImmediateChannelArrivalEvent=True
ListenForNewWorkEvent=False
UpdateTransferHandleTelephony=False
AllowWorkCenterList=False
PostImmediateChannelArrivalDelay=0
WrapupMode=2
WaitCallStateAfterDail=3000
LetDropEventCleanItem=True
NotReadyReasonCode=6,Break
NotReadyReasonCode=7,Lunch
NotReadyReasonCode=8,Meeting
DefaultNotReadyReasonCode=0001...
```

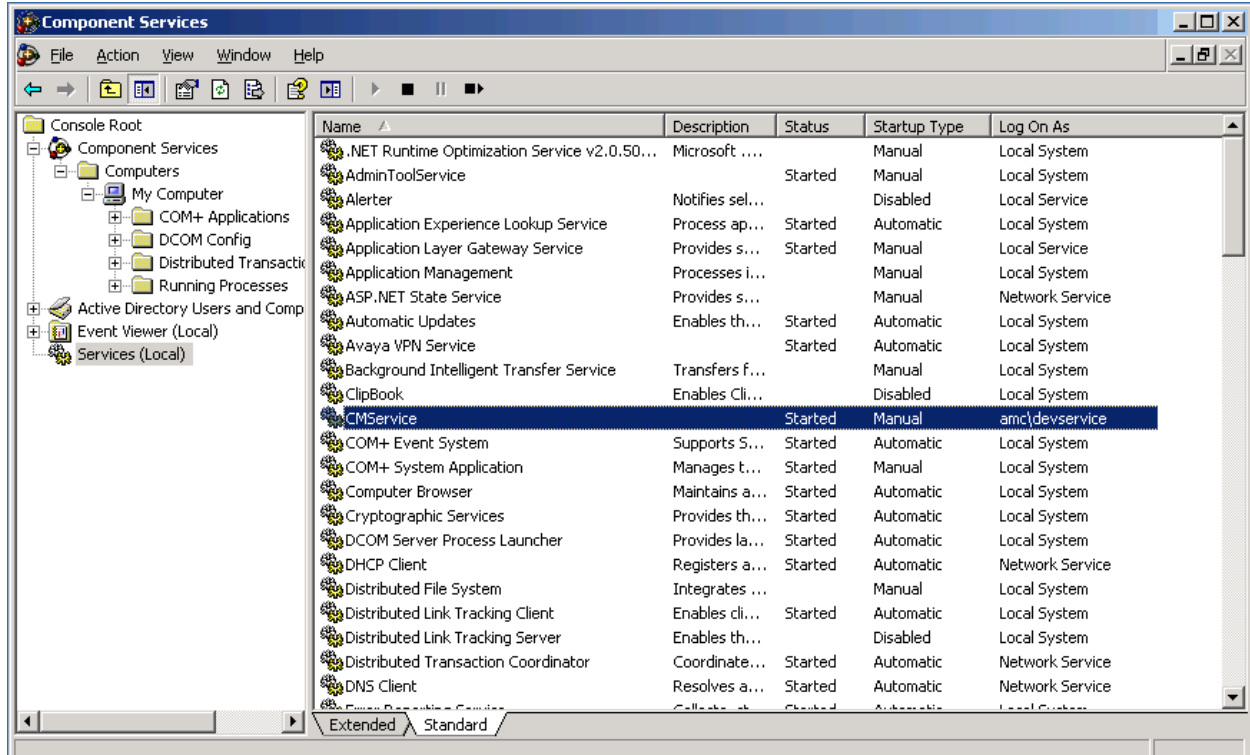
- Administer a user domain account in the Active Directory for DCOM communication between agents and CMService. In this example, the user is amc\devservice.
- Navigate to the **Component Services** in the Windows Server 2012 to access the window shown below. Double-click on CMService to open the properties window.



- In the **CMService Properties** window, navigate to the Identity tab and specify the amc\devservice user along with the password.



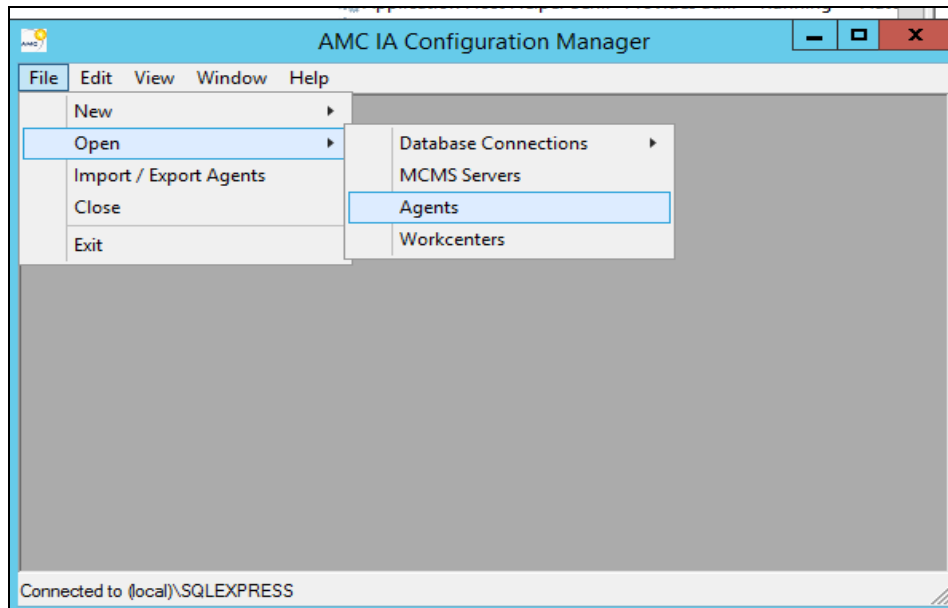
- Start the CMService from the Services management window.



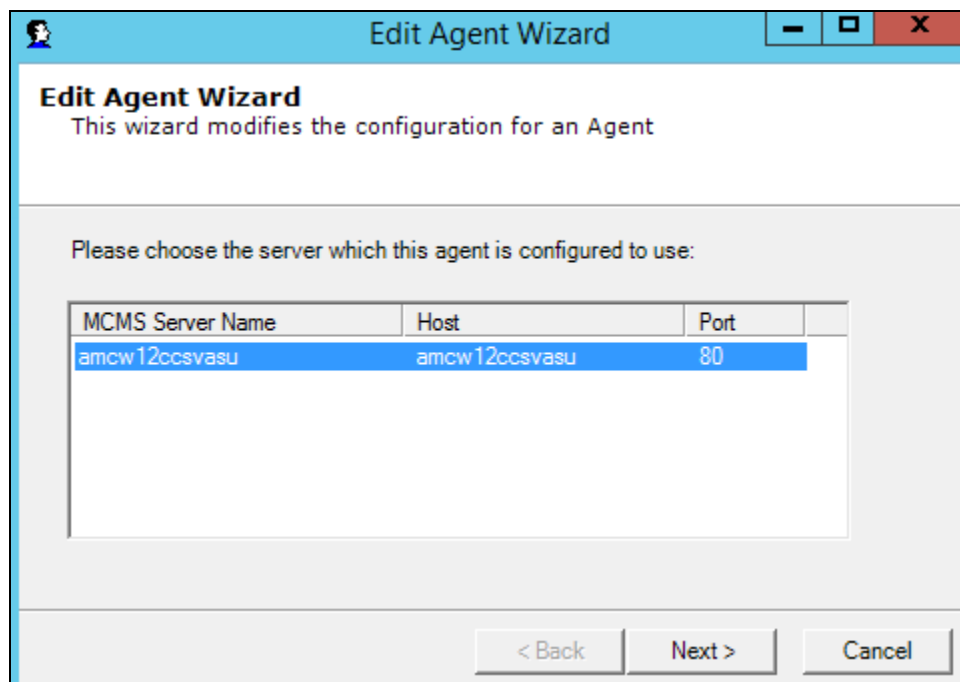
- Restart IIS by running the **iisreset** command in a command prompt window for SAPWeb/CRM7.

## 8. Configure SAPWeb/CRM7

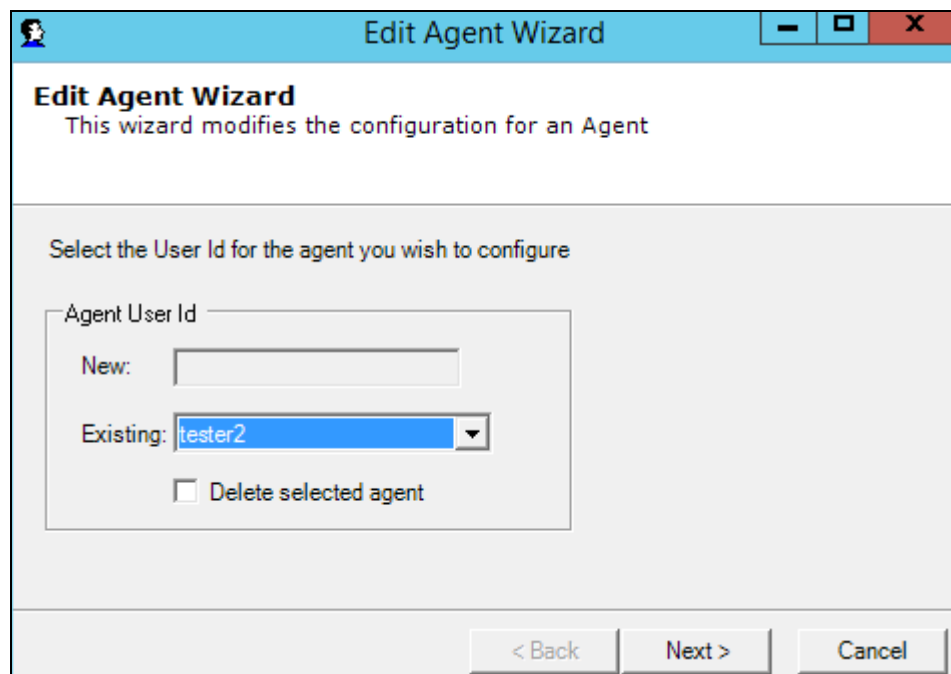
As there are 5 CRM adapters tested, this section will describe only the procedure for adding agents to SAPWeb/CRM7. From the CCS server, start the **Agent Configuration Manager** to set up the agents. Navigate to **File→Open→Agents** as shown below.



From the **Edit Agent Wizard** window, select CCS server below and click **Next**.

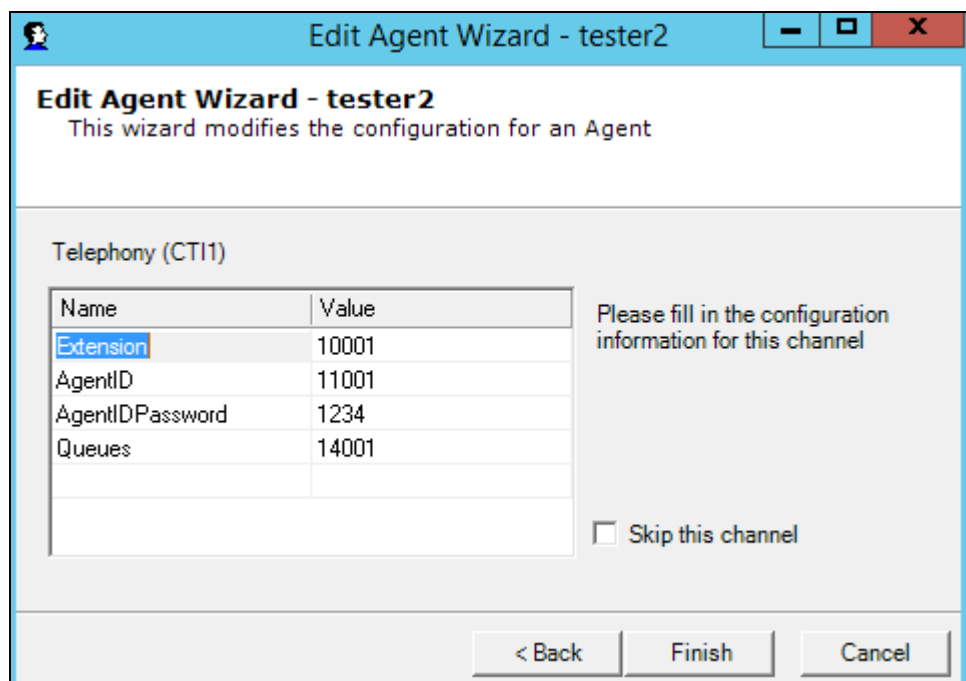


In the next window, specify the **Agent User Id** (e.g., **tester2**) and click **Next**.



The 'Edit Agent Wizard' window has a title bar with a user icon, the text 'Edit Agent Wizard', and standard window controls. The main area has a title 'Edit Agent Wizard' and a subtitle 'This wizard modifies the configuration for an Agent'. Below this is the instruction 'Select the User Id for the agent you wish to configure'. A group box labeled 'Agent User Id' contains a 'New:' text box, an 'Existing:' dropdown menu with 'tester2' selected, and a checkbox labeled 'Delete selected agent'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

In the last window, the **Extension**, **AgentID**, and **AgentIDPassword** configured in **Sections Error! Reference source not found. and 5.6** are specified. Click **Finish**.



The 'Edit Agent Wizard - tester2' window has a title bar with a user icon, the text 'Edit Agent Wizard - tester2', and standard window controls. The main area has a title 'Edit Agent Wizard - tester2' and a subtitle 'This wizard modifies the configuration for an Agent'. Below this is the section 'Telephony (CT11)'. It contains a table with configuration details and a checkbox 'Skip this channel'.

Name	Value
Extension	10001
AgentID	11001
AgentIDPassword	1234
Queues	14001

Please fill in the configuration information for this channel

☐ Skip this channel

At the bottom are three buttons: '< Back', 'Finish', and 'Cancel'.



## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, the AMC Driver and SAPWeb/CRM7.

### 9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for CTI link 3 administered in **Section 5.2** as shown below.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Rcvd
3	8	no	aes7x	<b>established</b>	15	15

## 9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed. Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3** as shown below.

Status | Status and Control | TSAPI Service Summary

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ TSAPI Service Summary

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version
<input checked="" type="radio"/>	3	Duplex	3	Talking	Wed Jul 4 16:54:21 2018	Online	17

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

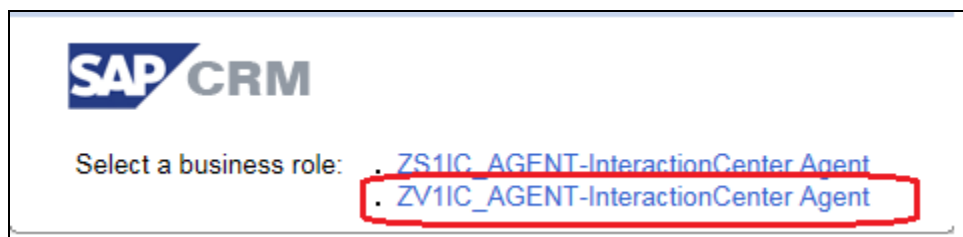
### 9.3. Verify AMC Driver and SAPWeb/CRM7

To verify that AMC Driver and SAPWeb/CRM7 are operational, log into the SAP Web client and change the agent state from “Not Ready” to “Ready”. Place a call to the VDN that routes the call to the agent and verify that the SAPWeb client receives the call and that the call can be answered. Prior to performing these steps, check that the AMC Driver has established a connection for the Application Enablement services by reviewing the **CTIModule.log** file.

Enter the appropriate URL in an internet browser to access the SAP Web client login screen shown below. Log on using the appropriate credentials. Click **Log On**.



The image shows the SAP NetWeaver login interface. On the left is a photograph of a man in a dark suit leaning over a desk, writing on a document. To the right of the photo is the login form. At the top right, the text "SAP NetWeaver" is displayed in orange. Below this is a warning message: "No switch to HTTPS occurred, so it is not secure to send a password". The login fields are: "System:" with a dropdown menu showing "C13"; "Client:" with a dropdown menu showing "010"; "User:" with a text input field containing "tester2"; "Password:" with a masked input field (dots) and a small icon to the right; and "Language:" with a dropdown menu showing "English". Below these fields is a yellow "Log On" button. A blue link "Change Password" is located below the "Log On" button. At the bottom right is the SAP logo. At the bottom center, the text "Copyright © 2015 SAP AG. All rights reserved." is displayed.



The image shows the SAP CRM business role selection screen. At the top left is the SAP CRM logo. Below the logo is the text "Select a business role:". To the right of this text are two radio button options. The first option is "ZS1IC\_AGENT-InteractionCenter Agent". The second option is "ZV1IC\_AGENT-InteractionCenter Agent", which is highlighted with a red rectangular box.

Verify that the agent is logged in and the default state is “Not Ready”.

The screenshot shows the Avaya Action Center interface. At the top, there is a header bar with 'action Center' on the left and 'Personalize System News Log Off' on the right. Below the header is a toolbar with various call control buttons: Reject, Hold, Retrieve, Hang Up, Transfer, Warm Transfer, Consult, Conference, Toggle, End, Dial Pad, Reset CTI, Clear Interaction, DTMF Pad, and Log Off. To the right of these buttons is a status indicator showing 'Ready' and 'Not Ready' with radio buttons. The 'Not Ready' option is selected and highlighted with a red box. Below the toolbar is a 'Saved Searches' dropdown menu with 'Go', 'Advanced', and 'Back' buttons. The main content area is titled 'Identify Account' and contains two sections: 'Account' and 'Installed Base | Object'. The 'Account' section has fields for First Name/Last Name, Account, Account ID, Street/House Number, City, Postal Code/Region, Country, Transaction ID, Contact Type (set to 'All'), Telephone, E-Mail Address, Fax, and Relationship (set to 'Has Contact Person'). The 'Installed Base | Object' section has fields for Component ID, Product ID, and Identification, with 'Search' and 'Clear' buttons. A yellow notification banner at the top right states 'You are logged on to the communication mgmt software system'.

Change the state to “Ready” as shown below.

This screenshot is identical to the one above, but the 'Ready' radio button in the status indicator is now selected and highlighted with a red box, indicating the agent's state has been changed.

Place a call to the VDN that routes the call to the agent. Verify that the call is delivered to the agent and the call can be answered and disconnected.

## 10. Conclusion

These Application Notes describe the configuration steps required to integrate 3rd party business applications in a call center environment consisting of Avaya Aura® Communication Manager using the AMC Driver for Avaya Aura® Application Enablement Services (AES). The AMC Driver used a TSAPI link to provide CTI integration to CCS and all the CRM adapters used, including call control, agent session control and screen pop. All test cases were completed with an observation noted in **Section 2.2**.

## 11. Additional References

This section references the Avaya documentation relevant to these Application Notes. The following Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 7.1.3, May 2018, Issue 7.
- [2] *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.1.3, May 2018, Issue 5.

The following AMC Technology is available upon request from member.

- [3] *AMC Voice Driver for Avaya Aura® Application Enablement Services (AES) Implementation Guide Contact Canvas™ 6.5*.
- [4] *AMC Application Adapter for mySAP™ CRM Interaction Center WebClient Implementation Guide Version 6.5*.
- [5] *AMC Contact Canvas Server Implementation Guide Contact Canvas 6.5*.

---

**©2018 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](mailto:devconnect@avaya.com).