



Avaya Solution & Interoperability Test Lab

Application Notes for AMC Connector for Avaya Aura™ Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate third-party business applications using the AMC Connector for Avaya Aura™ Application Enablement Services with a contact center environment provided by Avaya Aura™ Communication Manager. The AMC connector for Application Enablement Services provides computer telephony integration (CTI) to business applications from Microsoft, Oracle, Salesforce and SAP. The AMC Multi-Channel Integration Suite (MCIS), which includes the connector, 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. MCIS and the Application Enablement Services connector can also be used for adjunct routing. Application Enablement Services passes the adjunct route request to MCIS which leverages VB scripting to execute a data process within the business application and invokes AMC's advanced routing gateway to provide a route recommendation. For this compliance test, the AMC Connector was used to integrate SAPWeb 2007 with a contact center on Communication Manager.

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 third-party business applications using the AMC Connector for Avaya Aura™ Application Enablement Services (AES) with a contact center environment provided by Avaya Aura™ Communication Manager. The AMC connector for Application Enablement Services provides computer telephony integration (CTI) to business applications from Microsoft, Oracle, Salesforce and SAP. The AMC Multi-Channel Integration Suite (MCIS), which includes the connector, 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. MCIS and the Application Enablement Services connector can also be used for adjunct routing. Application Enablement Services passes the adjunct route request to MCIS which leverages VB scripting to execute a data process within the business application and invokes AMC's advanced routing gateway to provide a route recommendation. For this compliance test, the AMC Connector was used to integrate SAPWeb 2007 with a contact center on Communication Manager.

The Application Enablement Services connector uses a Telephony Services Application Programming Interface (TSAPI) connection and requires Basic license for standard integration or Advanced license necessary to monitor VDNs, if MCIS provides adjunct routing. AMC's MCIS is built upon component architecture using a connector / adapter pattern: connectors integrate contact channels and adapters integrate business applications, such as Salesforce. This provides a "future proof" foundation with 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.

1.1. Interoperability Compliance Testing

The interoperability compliance test verified the following features that are available to agents with the AMC Connector for Application Enablement Services.

- Logging in and out of a skill/split.
- Monitoring agent states (e.g., Ready or Not Ready).
- Agent state synchronization with agent telephones.
- 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 delivered from the PSTN with a 10-digit DID number.
- Basic telephony features such as call hold, transfer, and conference.
- Restarting the AMC Connector.

1.2. Support

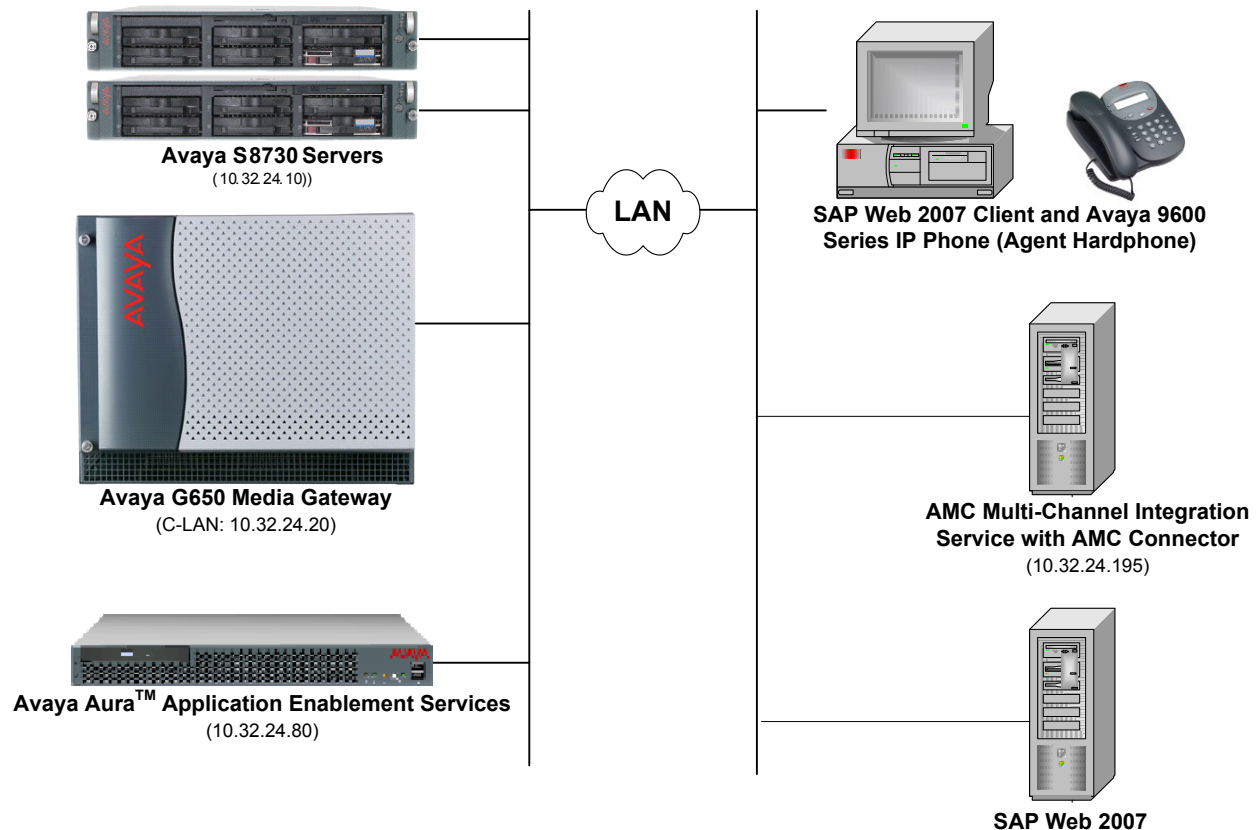
Technical support on the AMC Connector can be obtained through the following:

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

2. Reference Configuration

The following diagram illustrates a sample configuration of a contact center environment integrated with SAP Web 2007 using the AMC Connector for Application Enablement Services. The configuration includes Avaya Aura™ Application Enablement Services, a pair of Avaya S8730 Servers with a G650 Media Gateway running Avaya Aura™ Communication Manager, and Avaya IP endpoints serving as agent stations. In addition, the agent's interaction center includes SAP Web 2007 and separate servers containing the AMC Multi-Channel Integration Server with the AMC Connector and the SAP Web 2007 server.

Device Type	Value
Skill Group Number	250
Skill Group Extension	76000
VDN	75000
Agent IDs	76301 and 76302
Agent Station Extensions	77301 and 77302



3. Equipment and Software Validated

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

Equipment	Software
Avaya Aura™ Application Enablement Services	5.2.1
Avaya S8730 Servers with an Avaya G650 Media Gateway	Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3) with Service Pack 3 (Patch 17579)
Avaya 9600 Series IP Telephones	3.0 (H.323)
AMC Connector for Avaya Application Enablement Services	5.3.0.0
SAP Web 2007	6.0

4. Configure Aura™ Avaya Communication Manager

This section provides the procedures for configuring 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

4.1. 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 3**. 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 3 of 11
                                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? n    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? y           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
Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? n
ATM WAN Spare Processor? n               DS1 MSP? y
ATMS? n               DS1 Echo Cancellation? y
Attendant Vectoring? y

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

4.2. 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.

add cti-link 2	Page 1 of 3
CTI LINK	
CTI Link: 2	
Extension: 24962	
Type: ADJ-IP	
COR: 1	
Name: AMC CTI Link	

4.3. Administer Agent Hunt Group

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

add hunt-group 250	Page 1 of 3
HUNT GROUP	
Group Number: 250	ACD? y
Group Name: CC Queue 1	Queue? y
Group Extension: 76000	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:

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

add hunt-group 250		Page 2 of 3
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n	Service Level Target (% in sec): 80 in 20	
Measured: internal	Service Objective (sec): 20	
Supervisor Extension:	Service Level Supervisor? n	
Controlling Adjunct: none		
VuStats Objective:		
Timed ACW Interval (sec):	Dynamic Queue Position? n	
Multiple Call Handling: none		
Interruptible Aux Threshold: none		
Redirect on No Answer (rings):		
Redirect to VDN:		
Forced Entry of Stroke Counts or Call Work Codes? n		

4.4. 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 250.

change vector 250		Page 1 of 6
CALL VECTOR		
Number: 250		Name: IQ Vector 1
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n
Basic? y	EAS? y	G3V4 Enhanced? y
Prompting? y	LAI? y	G3V4 Adv Route? y
Variables? y	3.0 Enhanced? y	CINFO? y
01 wait-time	2 secs hearing ringback	BSR? y
02 queue-to	skill 250 pri h	Holidays? n
03 stop		
04		
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.

add vdn 75000		Page 1 of 3
VECTOR DIRECTORY NUMBER		
Extension: 75000		
Name*: Call Center		
Destination: Vector Number 250		
Attendant Vectoring? n		
Meet-me Conferencing? n		
Allow VDN Override? n		
COR: 1		
TN*: 1		
Measured: none		

4.5. Administer Agent Stations

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

add station 77301		Page 1 of 5
STATION		
Extension: 77301	Lock Messages? n	BCC: 0
Type: 9630	Security Code: ****	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: Agent 1	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 77301	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Button Modules: 0	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Customizable Labels? y	

4.6. Administer Agent IDs

Add an **Agent Login ID** for each agent in the contact 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 contact center.

add agent-loginID 76301		Page 1 of 2
AGENT LOGINID		
Login ID: 76301	AAS? n	
Name: Agent 1	AUDIX? n	
TN: 1	LWC Reception: spe	
COR: 1	LWC Log External Calls? n	
Coverage Path:	AUDIX Name for Messaging:	
Security Code: 1234	LoginID for ISDN/SIP Display? n	
	Password: 1234	
	Password (enter again): 1234	
	Auto Answer: station	
	MIA Across Skills: system	
	ACW Agent Considered Idle: system	
	Aux Work Reason Code Type: system	
	Logout Reason Code Type: system	
	Maximum time agent in ACW before logout (sec): system	
	Forced Agent Logout Time: :	
WARNING: Agent must log in again before changes take effect		

On Page 2, specify the skill number to which the agent will log in. In the example, the agent will log into skill 250.

add agent-loginID 76301										Page 2 of 2		
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:	250	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:			

5. Configure Avaya Aura™ Application Enablement Services

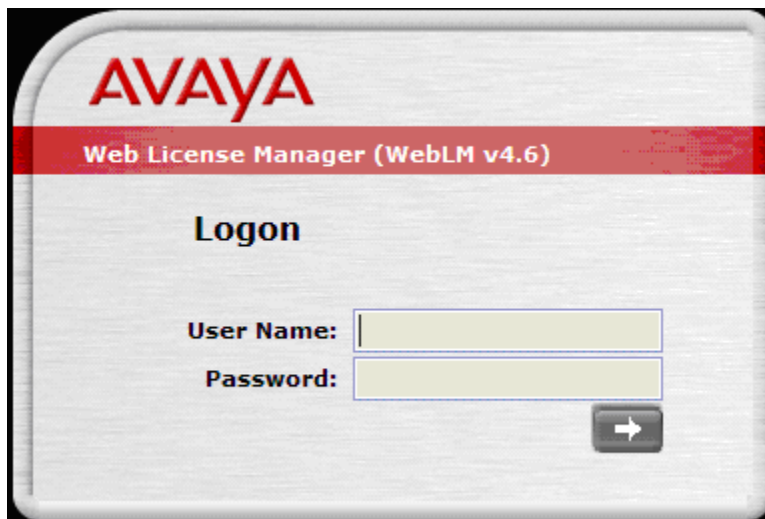
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

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

5.1. Verify TSAPI License

Access the Web 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.

The **Web License Manager** screen is displayed. Log in using the appropriate credentials.



The **Web License Manager** screen is displayed. 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, in this case **AES ADVANCED MEDIUM SWITCH** for the Avaya S8730 Server.

AVAYA Web License Manager (WebLM v4.6) [Logout](#)

Install License **Application Enablement (CTI) - Release: 5 - SID: 10503000 (Standard License File)**

Licensed Products
APPL_ENAB
Application_Enablement
 Uninstall License
 Change Password
 Server Properties
 Manage Users
 Logout

You are here: Licensed products > Application Enablement (CTI)

License installed on: May 17, 2010 10:55:07 AM EDT

[View Peak Usage](#)

Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	100	0
DLG (VALUE_AES_DLG)	permanent	16	0
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	1
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	0
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	3	0

SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop
 MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm
 LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown
 TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001,

5.2. Launch OAM Interface

Access the OAM web-based interface by 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.

5.3. 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 AVAYA Application Enablement Services Management Console. The top header includes the AVAYA logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with login details. A red navigation bar contains "AE Services | TSAPI | TSAPI Link" and "Home | Help | Logout". The left sidebar shows a tree view with "AE Services" expanded, containing "CVLAN", "DLG", "DMCC", "SMS", "TSAPI" (expanded), "TSAPI Links", and "TSAPI Properties". The main content area is titled "TSAPI Links" and displays a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "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 “devcon13” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 4.2**. Retain the default values in the remaining fields and click **Apply Changes**.

The screenshot shows the "Add TSAPI Links" screen in the AVAYA Application Enablement Services Management Console. The layout is similar to the previous screen, but the main content area contains a form with the following fields: "Link" (value: 1), "Switch Connection" (value: devcon13), "Switch CTI Link Number" (value: 2), "ASAI Link Version" (value: 5), and "Security" (value: Unencrypted). At the bottom of the form are buttons for "Apply Changes" and "Cancel Changes".

5.4. 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**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with login details. A red navigation bar contains "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various management categories, with "Security" expanded to show "Security Database" and "Control" selected. The main content area, titled "SDB Control for DMCC and TSAPI", contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB TSAPI Service, JTAPI and Telephony Service", along with an "Apply Changes" button.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Mon Jun 7 08:00:05 2010 from 10.32.24.251
HostName/IP: devconaes/10.32.24.80
Server Offer Type: TURNKEY
SW Version: r5-2-1-103-0

Security | Security Database | Control Home | Help | Logout

▶ AE Services
▶ Communication Manager Interface
▶ Licensing
▶ Maintenance
▶ Networking
▼ Security
 ▶ Account Management
 ▶ Audit
 ▶ Certificate Management
 Enterprise Directory
 ▶ Host AA
 ▶ PAM
 ▼ Security Database
 ▪ Control
 ▣ CTI Users
 ▪ Devices
 ▪ Device Groups
 ▪ Tlinks
 ▪ Tlink Groups
 ▪ Worktops
Standard Reserved Ports
Tripwire Properties

SDB Control for DMCC and TSAPI

☐ Enable SDB for DMCC Service
☐ Enable SDB TSAPI Service, JTAPI and Telephony Service

5.5. 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**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User craft
Last login: Fri May 21 15:03:37 2010 from 10.32.24.25
HostName/IP: devconaes/10.32.24.80
Server Offer Type: TURNKEY
SW Version: r5-2-1-103-0

Maintenance | Service ControllerHome | Help | Logou

▶ AE Services

▶ Communication Manager Interface

▶ 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

5.6. 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 Connector.

In this case, the associated Tlink name is “AVAYA#**DEVCON13**#CSTA#DEVCONAES”. Note the use of the switch connection “DEVCON13” from **Section 5.6** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with login details. A red navigation bar contains "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar shows a tree view with categories like AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, and Security Database. The "Security Database" category is expanded, showing sub-items like Control, CTI Users, Devices, Device Groups, Tlinks (highlighted), Tlink Groups, and Worktops. The main content area, titled "Tlinks", shows a single Tlink named "AVAYA#DEVCON13#CSTA#DEVCONAES" with "Edit Tlink" and "Delete Tlink" buttons.

5.7. Administer User for AMC Connector

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).

AVAYA **Application Enablement Services**
Management Console

Welcome: User craft
Last login: Fri May 21 15:03:37 2010 from 10.32.24.251
HostName/IP: devconaes/10.32.24.80
Server Offer Type: TURNKEY
SW Version: r5-2-1-103-0

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User IdAMC

* Common NameAMC Connector

* SurnameAMC Connector

* User Password●●●●●●●●

* Confirm Password●●●●●●●●

Admin Note

Avaya RoleNone

Business Category

Car License

CM Home

Css Home

CT UserYes

Department Number

6. Configure AMC Connector for Application Enablement Services

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

- Verify that the Avaya Aura™ Application Enablement Services TSAPI Client MS Windows 5.2.1 has been installed on the AMC Connector 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 Application Enablement Services connector module (CTIModule) under the Avaya CT/AES comment,
 - the Application Enablement Services and MCIS license under License Manager, and
 - the CTIModule section which includes the Channel (default value of CT1 is recommended), the Server ID or Tlink name obtained in **Section 5.6**, and the user login credentials configured in **Section 5.7**.

```
#####
# MCIS Configuration file: Config.ini with ACT/AES Connector and SAPWeb2007
# MCIS Release 5.3
# File Version 1.0
#
# This file should contain all the potential keys for every module.
# Refer to the MCIS Implementation Guide, Adapter Implementation Guide,
# and Connector Implementation Guide for more information.
#
# It is recommended you create a copy of this file for Backup
#
# It is also recommended you create system specific ini files and copy
# the contents of those files to the config.ini file using the MCIS
# Administration Tool or Manually.
#
#####

...

### MCIS CORE ###
ModuleClass=AgentManagerClass,AgentManager.AMCAgentManagerModule
ModuleClass=DataStoreClass,DataStore.AMCMemoryDataStore
ModuleClass=EventManagerClass,AMCEventManagerModule.AMCEventManagerModule
ModuleClass=LicenseManagerClass,LicenseManager.AMCLicenseManagerModule
ModuleClass=WorkManagerClass,WorkManager.AMCWorkManager
ModuleClass=StandardizedClass,AMCMultiChannelInterface.AMCApplication
ModuleClass=CMGatewayClass,CMGateway.CMGatewayModule
ModuleClass=ICIAdapterClass,ICIAdapter.ICIAdapterModule

Module=AgentManager,AgentManagerClass
Module=DataStore,DataStoreClass
Module=EventManager,EventManagerClass
Module=LicenseManager,LicenseManagerClass
```

```

Module=WorkManager,WorkManagerClass
Module=StandardizedInterface,StandardizedClass
Module=CMGateway,CMGatewayClass
Module=IciAdapter,ICIAdapterClass

...

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

...

###
# License Manager
#
###
[LicenseManager]
MCIS=CWJTCQJBCBJHFCECAEHDFMCJFCEBEFDWHEHLMMRSLM
AA-DOTNET=CQJNCZJXCPJEFGCJEGDDWEFFCEBEFDQHEHLMMRSLM
CTI_CentreVu=CVJPCZJPCCJDFECIEBDFTBDFCEBEFDVHEHLMMRSLM
AA-ICWC=CWJLCRJSCCJDFECIEBDFZDCFCEBEFDWHEHLMMRSLM

...

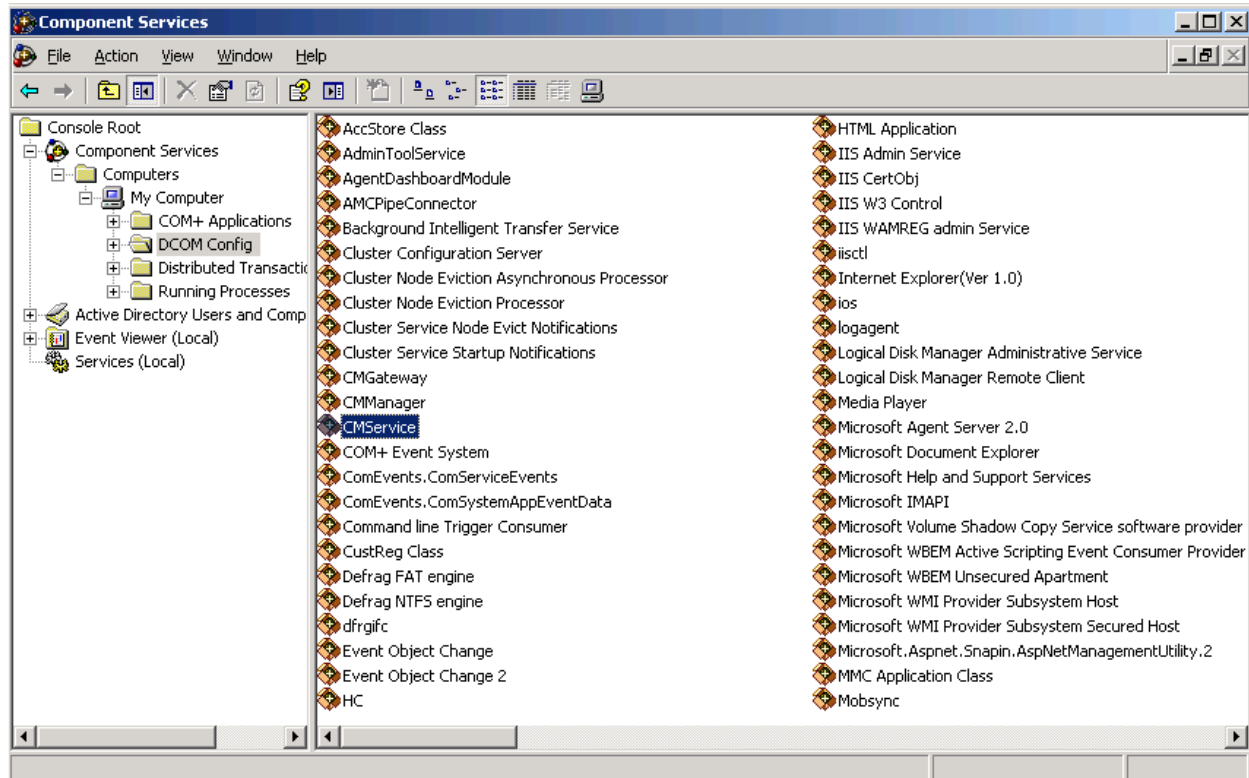
###
# CTIModule
#
###
[CTIModule]
TraceLevel=4
Channel=CTI1
ServerID=AVAYA#DEVCON13#CSTA#DEVCONAES
UserName=AMC
Password=*****
AllowDTMF=Yes
DTMFPause=5
UseAutoIn=1

...

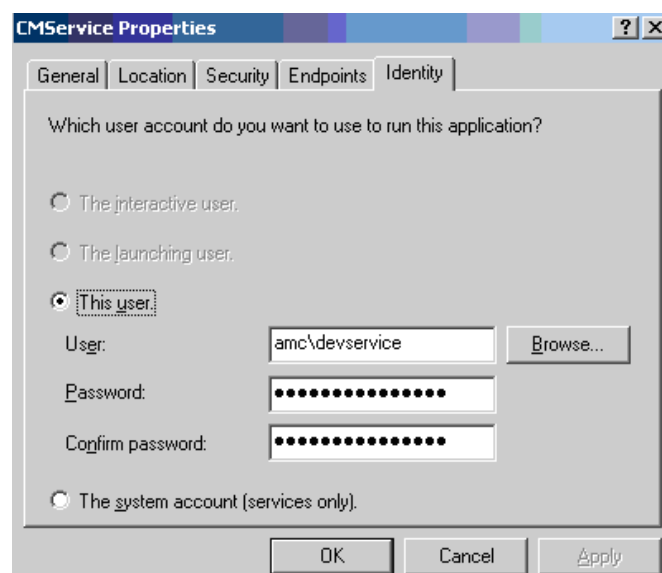
###
# IciAdapter - For SAP CRM 2007(Web client)
#
###
[IciAdapter]
TraceLevel=4
ConfigDBHost=(local)\SQLEXPRESS
ConfigServerName=AMCW23QAMCIS53
NewHandleOnWarmTransfer=False
DataStore=DataStore
ShowSelectForFailedWorkMode=True
ACWText=After Call
NotReadyReasonCode=6,Wash room
NotReadyReasonCode=7,Break
NotReadyReasonCode=8,Lunch
NotReadyReasonCode=9,Meeting
NotReadyReasonCode=9999,--Select--

```

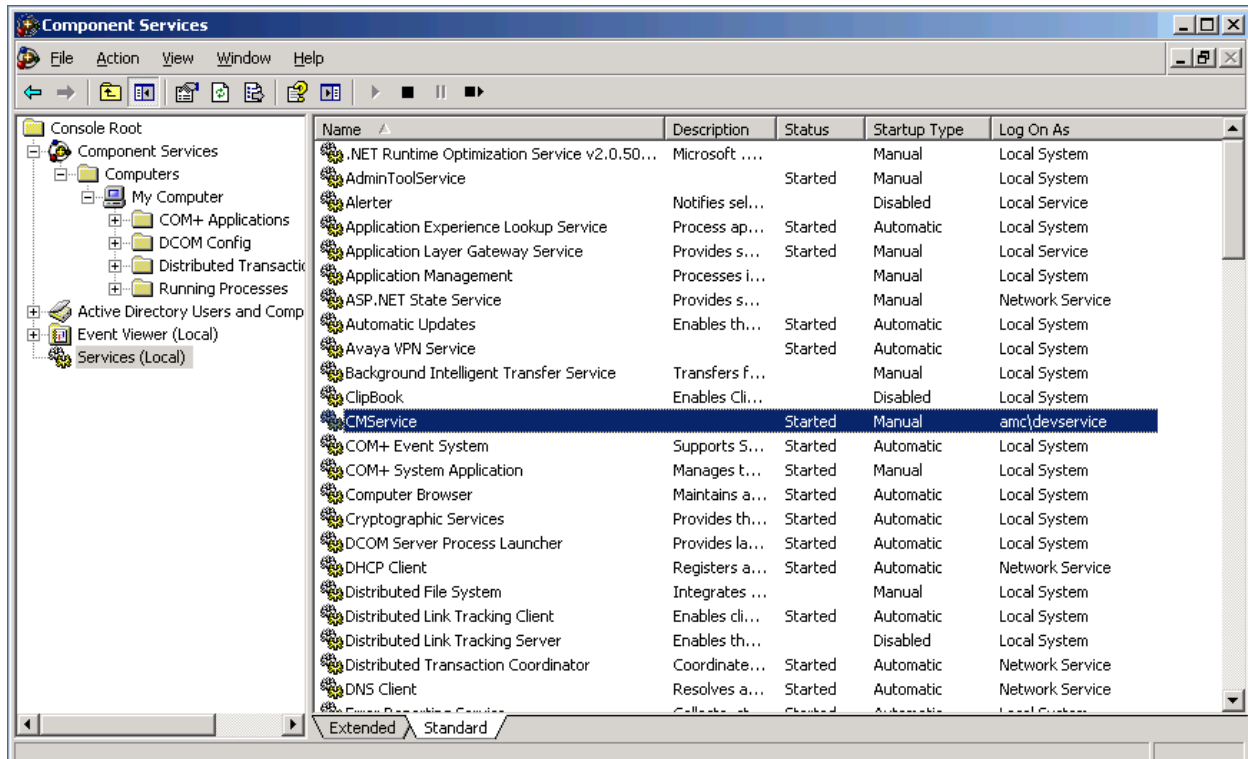
- Administer a user domain account in the Active Directory for DCOM communication between agents and CMService. In this example, the user is amc/devservice.
- Navigate to the **Component Services** in the Windows Server 2003 to access the window shown below. Double-click on CMService to open the properties window.



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



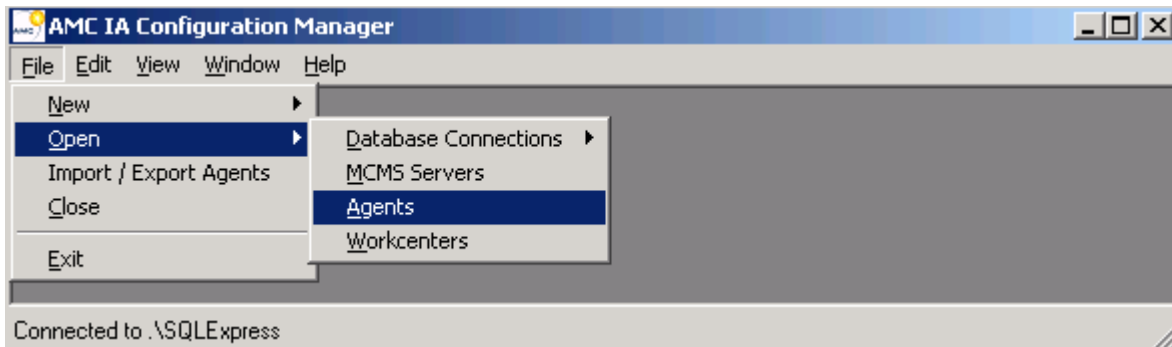
- Start the CMService from the Services management window.



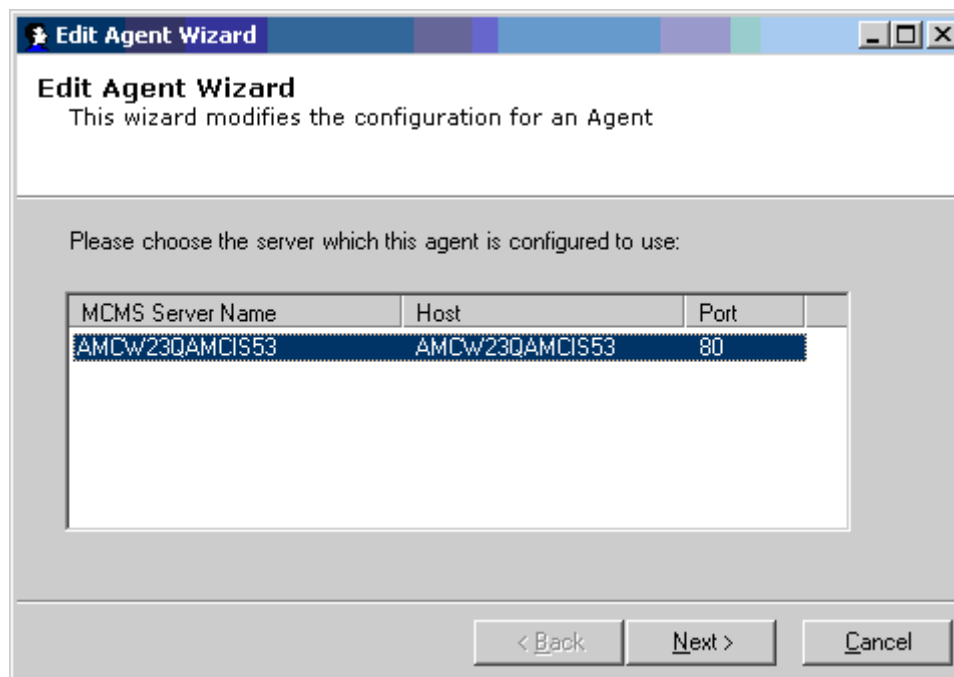
- Restart IIS by running the **iisreset** command in a command prompt window for SAP Web 2007.

7. Configure SAP Web 2007

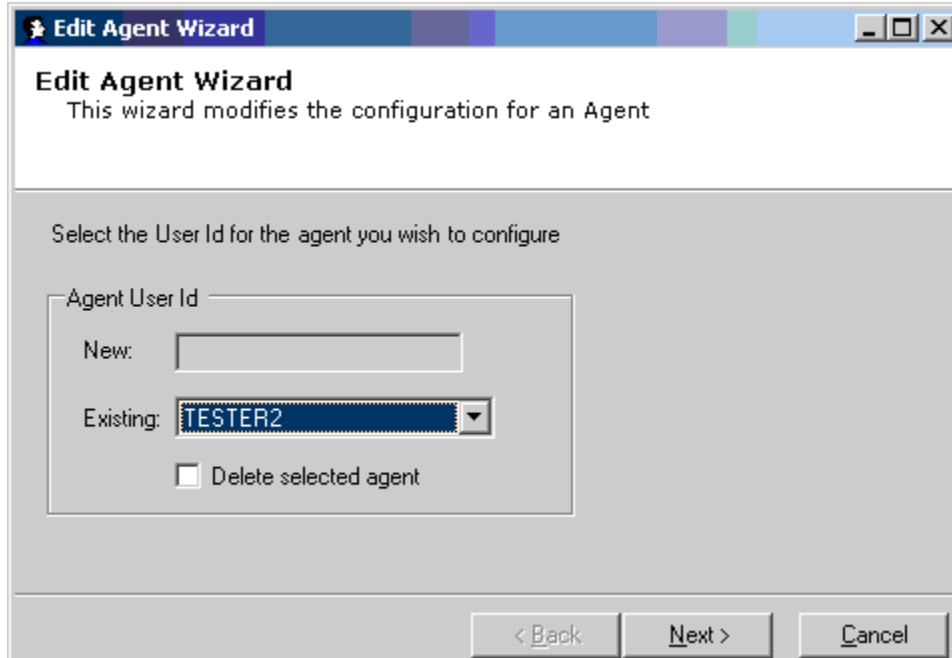
This section describes the procedure for adding agents to SAP Web 2007. From the MCIS server, start the **Agent Configuration Manager** to set up the agents. Navigate to **File→Open→Agents** as shown below.



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

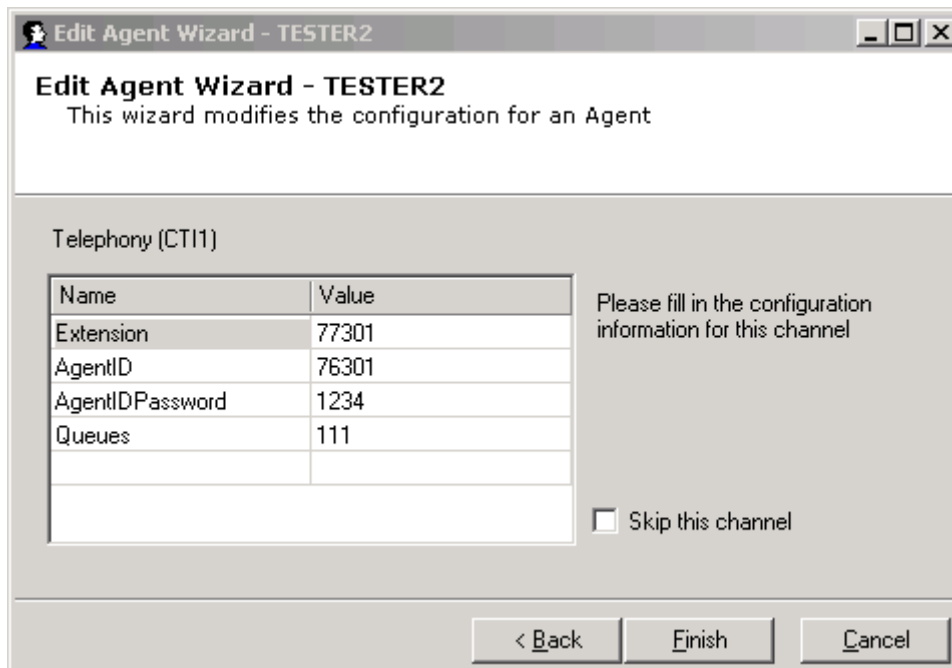


In the next window, specify the Agent User ID (e.g., TESTER2) and click **Next**.



The 'Edit Agent Wizard' dialog box is shown. It has a title bar with a small icon and the text 'Edit Agent Wizard'. Below the title bar, the text 'Edit Agent Wizard' is followed by 'This wizard modifies the configuration for an Agent'. The main area contains the instruction 'Select the User Id for the agent you wish to configure'. Below this, there is a section titled 'Agent User Id' which contains two input fields: 'New:' with an empty text box, and 'Existing:' with a dropdown menu showing 'TESTER2'. Below these fields is a checkbox labeled 'Delete selected agent'. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

In the last window, the **Extension**, **Agent ID**, and **Agent ID Password** configured in Sections 4.5 and 4.6 are specified. Click **Finish**.



The 'Edit Agent Wizard - TESTER2' dialog box is shown. It has a title bar with a small icon and the text 'Edit Agent Wizard - TESTER2'. Below the title bar, the text 'Edit Agent Wizard - TESTER2' is followed by 'This wizard modifies the configuration for an Agent'. The main area contains the section 'Telephony (CTI1)'. Below this section is a table with two columns: 'Name' and 'Value'. The table contains the following data:

Name	Value
Extension	77301
AgentID	76301
AgentIDPassword	1234
Queues	111

To the right of the table, the text 'Please fill in the configuration information for this channel' is displayed. Below the table and text is a checkbox labeled 'Skip this channel'. At the bottom of the dialog are three buttons: '< Back', 'Finish', and 'Cancel'.

8. General Test Approach and Test Results

To verify interoperability of the AMC Connector with Application Enablement Services and Communication Manager, the SAP Web 2007 application was used. This business application allowed the functionality available in the AMC Connector 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 1.1** were covered.

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

Best practice – To avoid possible synchronization issues between the agent telephone and the application softphone, agents should refrain from the following actions in this order: logging in via agent telephone → going ready → receiving or making a call → logging into CRM during the call.

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, the AMC Connector and SAP Web 2007.

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 2 administered in **Section 4.2** as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	5	no	devconaes	established	96	96
2	5	no	devconaes	established	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 5.3** as shown below.

**Application Enablement Services**
Management Console

Welcome: User craft
Last login: Tue Jun 8 14:59:41 2010 from 10.32.24.251
HostName/IP: devconaes/10.32.24.80
Server Offer Type: TURNKEY
SW Version: r5-2-1-103-0

Status | Status and Control | TSAPI Service Summary

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▼ 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	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
	1	devcon13	2	Talking	Mon Jun 7 08:02:52 2010	Online	15	0	15	15	30

Online Offline

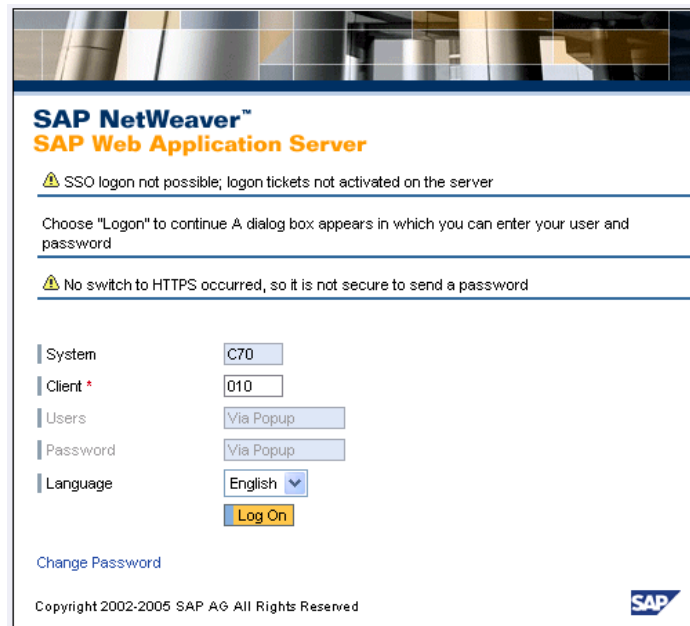
For service-wide information, choose one of the following:

TSAPI Service Status TLink Status User Status

9.3. Verify AMC Connector and SAP Web 2007

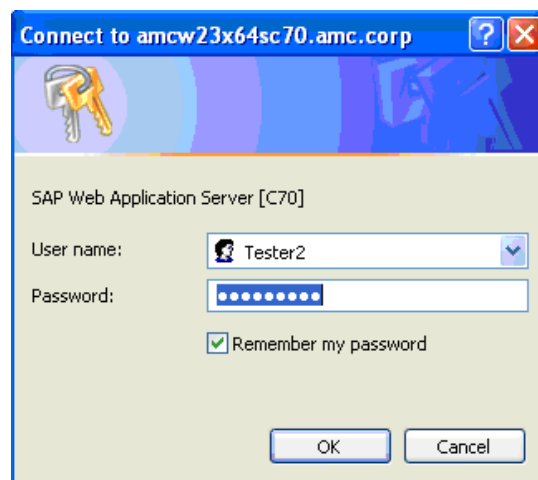
To verify that AMC Connector and SAP Web 2007 are operational, log into the SAP Web client and change the agent state from “Not Ready” to “Ready”. Place a call to the VDN that routes the call to the agent and verify that the SAP Web client receives the call and that the call can be answered. Prior to performing these steps, check that the AMC Connector has established a connection for the Application Enablement services by reviewing the **CTIModule.log** file located in the C:\Program Files\AMC Technology\MCIS\Server\Logs directory.

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



The screenshot shows the SAP NetWeaver SAP Web Application Server login interface. At the top, there is a header with the SAP logo and the text "SAP NetWeaver™ SAP Web Application Server". Below the header, there are two warning messages: "SSO logon not possible; logon tickets not activated on the server" and "No switch to HTTPS occurred, so it is not secure to send a password". The main login area contains fields for System (C70), Client (010), Users (Via Popup), Password (Via Popup), and Language (English). A "Log On" button is located at the bottom right of the login area. Below the login area, there is a "Change Password" link and a copyright notice: "Copyright 2002-2005 SAP AG All Rights Reserved".

Log on using the appropriate credentials.



The screenshot shows a dialog box titled "Connect to amcw23x64sc70.amc.corp". The dialog box contains a key icon and the text "SAP Web Application Server [C70]". Below this, there are fields for "User name:" (Tester2) and "Password:" (masked with dots). A checkbox labeled "Remember my password" is checked. At the bottom, there are "OK" and "Cancel" buttons.

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

The screenshot shows the SAP Interaction Center interface. At the top, there is a header bar with the SAP logo and the text 'Interaction Center'. Below the header, there is a navigation bar with buttons: Accept, Reject, Hold, Retrieve, Hang Up, Transfer, Warm Transfer, Consult, Conference, Toggle, End, and Dial Pad. To the right of these buttons is a state selector with two radio buttons: 'Ready' and 'Not Ready'. The 'Not Ready' radio button is selected. Below the navigation bar is a sidebar with a list of menu items: Account Identification, Account Fact Sheet, Account Overview, Interaction Record, Interaction History, Fax, Letter, Unfinished E-Mails, Case, Knowledge Search, and Script. 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, Telephone, and E-Mail Address. The 'Installed Base | Object' section has fields for Component, Product ID, and Identification. There are 'Search' and 'Clear' buttons between the two sections.

Change the state to “Ready” as shown below.

This screenshot is identical to the one above, showing the SAP Interaction Center interface. The only difference is in the state selector at the top right, where the 'Ready' radio button is now selected, and the 'Not Ready' radio button is unselected.

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 third-party business applications in a contact center environment consisting of Avaya Aura™ Communication Manager using the AMC Connector for Avaya Aura™ Application Enablement Services. The AMC connector used a TSAPI link to provide CTI integration to SAP Web 2007, including call control, agent session control and screen pop. All test cases were completed with an observation noted in **Section 8**.

11. Additional References

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

- [1] *Administering Avaya Aura™ Communication Manager*, Release 5.2, May 2009, Issue 5.0, Document Number 03-300509.
- [2] *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*, November 2009, Issue 11, Release 5.2, Document Number 02-300357.
- [3] *AMC Telephony Connector – Avaya Aura™ Application Enablement Services (AES) Implementation Guide*, Version 5.3, April 2010, available from AMC upon request.

©2010 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.