



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 3rd 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 AES provides CTI integration to business applications from Microsoft, Oracle, Salesforce and SAP. The AMC Contact Canvas Server (CCS), 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. CCS and the AES connector can also be used for adjunct routing. AES passes the adjunct route request to CCS which leverages VB scripting to execute a data dip 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 6 different Customer Relationship Management (CRM) adapters with a call center on 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 Connector for Avaya Aura® Application Enablement Services (AES) with a contact center environment provided by Avaya Aura® Communication Manager. The AMC connector for AES provides CTI integration to business applications from Microsoft, Oracle, Salesforce and SAP. The AMC Contact Canvas Server (CCS), 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. CCS and the AMC connector can also be used for adjunct routing. AES passes the adjunct route request to CCS which leverages VB scripting to execute a data dip 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 6 different CRM adapters with a call center on Communication Manager.

The AES connector 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 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.

2. General Test Approach and Test Results

To verify interoperability of the AMC Connector with Application Enablement Services and Communication Manager, the 6 different CRM applications were used; detail is listed in **Section 4**. SAPWeb/CRM7 is one of the business applications 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 2.1** were covered.

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 refrain from the following actions in this order: logging in via hardphone → going ready → receiving or making a call → logging into CRM during the call.

2.1. Interoperability Compliance Testing

The interoperability compliance test verified the following feature functionality available to agents with the AMC Connector 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, transfer, and conference.
- Restarting the AMC Connector.

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 refrain from the following actions in this order: logging in via hardphone → going ready → receiving or making a call → logging into CRM during the call.

2.3. Support

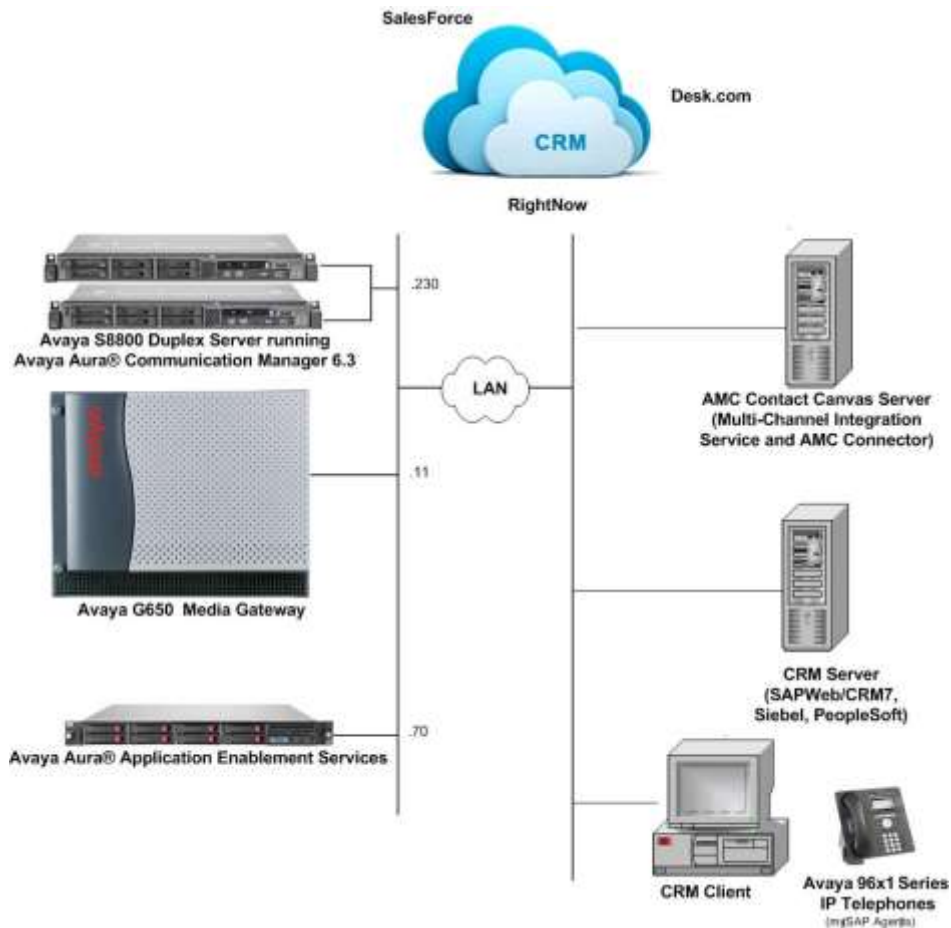
Technical support on the AMC Connector can be obtained through the following:

- **Phone:** (800) 390-4866
- **Email:** 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 Connector for Application Enablement Services. The configuration includes, including Avaya Aura® Application Enablement Services, a pair of Avaya S8800 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 included CRM Web client and separate servers containing the AMC Multi-Channel Integration Server/CCS with the AMC Connector and the CRM server.

| Device Type | Value |
|--------------------------|-----------------|
| Skill Group Number | 1 |
| Skill Group Extension | 13001 |
| VDN | 14001 |
| Agent IDs | 11001 and 11002 |
| Agent Station Extensions | 10001 and 10002 |



4. Equipment and Software Validated

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

| Equipment | Software |
|---|---|
| Avaya Aura® Communication Manager | 6.3.9.0 (Build R016x.03.0.124.0-21971) |
| Avaya Aura® Application Enablement Services | 6.3.3.1.10-0 |
| 96x1 Series H.323 IP Deskphone | 6.4014 |
| AMC Connector for Avaya Aura® Application Enablement Services | 6.5.0.0 |
| SAPCRM7EHP3 | 6.5.0.0 |
| Oracle Siebel | 6.5.0.0 |
| Salesforce.com | 6.5.0.0 |
| Oracle PeopleSoft | 6.5.0.0 |
| Oracle RightNow | 6.5.0.0 |
| SFDC Desk.com | 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 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? 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
Async. Transfer Mode (ATM) Trunking? n        Digital Loss Plan Modification? y
ATM WAN Spare Processor? n                    DS1 MSP? y
ATMS? y                                       DS1 Echo Cancellation? 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.

```
add cti-link 3                                     Page 1 of 3
                                         CTI LINK
CTI Link: 3
Extension: 10093
  Type: ADJ-IP
                                         COR: 1
Name: TSAPI Service - AES6x
COR: 1
```

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.

```
add hunt-group 1                                   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
Security Code:                                     MM Early Answer? n
Local Agent Preference? n
ISDN/SIP Caller Display: grp-name
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 1                                     Page 2 of 4
                                                    HUNT GROUP

                Skill? y      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.

```
change vector 1                                     Page 1 of 6
                                                    CALL VECTOR

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 wait-time 2 secs hearing ringback
02 queue-to  skill 1  pri m
03 wait-time 900 secs hearing music
04 disconnect after announcement none
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
```


5.5. Administer Agent Stations

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

```
add station 10001                                     Page 1 of 5
                                                    STATION
Extension: 10001                                     Lock Messages? n                BCC: 0
  Type: 9611G                                       Security Code: 111222           TN: 1
  Port: S00002                                       Coverage Path 1:                COR: 1
  Name: 10001                                       Coverage Path 2:                COS: 1
                                                    Hunt-to Station:                Tests? y

STATION OPTIONS
  Location:                                          Time of Day Lock Table:
  Loss Group: 19                                    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:                          Media Complex Ext:
  Survivable COR: internal                           IP SoftPhone? y
  Survivable Trunk Dest? 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: Alice                                       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
                                                    AUDIX Name for Messaging:

  LoginID for ISDN/SIP Display? n
  Password: 1234
  Password (enter again): 1234
  Auto Answer: none
  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 1.

```
add agent-loginID 11001                                     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   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

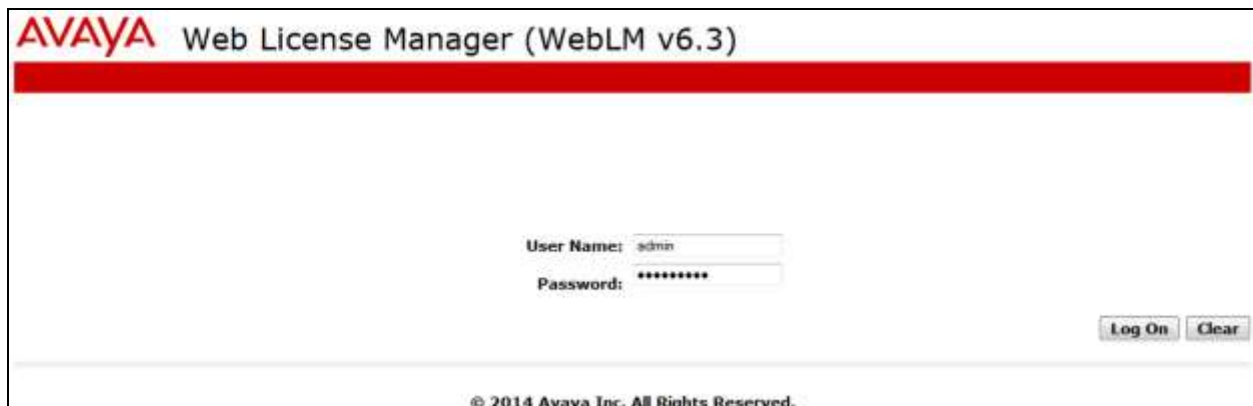
This section provides the procedures for configuring Avaya Aura® Application Enablement Services. The procedures include the following areas:

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

6.1. 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.



AVAYA Web License Manager (WebLM v6.3)

User Name: admin

Password: *****

Log On Clear

© 2014 Avaya Inc. All Rights Reserved.

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 for the switch type.

AVAYA Web License Manager (WebLM v6.3) Help | About | Change Password | Log off admin

Application Enablement (CTI) - Release: 6 - SID: 10503000 Standard License file

You are here: Licensed Products > Application Enablement > View License Capacity

License installed on: January 26, 2015 3:26:53 PM +08:00

License File Host IDs: 00-0C-29-92-EE-50, VC-01-BE-13-65-80

Licensed Features

10 Items Show ALL

| Feature (License Keyword) | Expiration date | Licensed capacity |
|--|-----------------|--|
| CVLAN ASAI VALUE_AES_CVLAN_ASAI | permanent | 1 |
| Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP | permanent | 2500 |
| AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED | permanent | 16 |
| CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS | permanent | 16 |
| Product Notes VALUE_NOTES | permanent | SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMe LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLarge TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnre DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnre DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnre DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnres DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnres DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnre DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnres DMCUnrestricted; SAMETIME_001, VALUE_AES_AEC_UNIFIED_CC_DESKTOP,; CCE_001, BasicUnrest AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicU AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicU AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUn DMCUnrestricted, AgentEvents; |
| AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED | permanent | 16 |
| TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS | permanent | 2500 |
| DLG VALUE_AES_DLG | permanent | 1 |
| Device Media and Call Control VALUE_AES_DMCC_DMC | permanent | 2500 |
| AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED | permanent | 16 |

Acquired Licenses

1 Item Show ALL

| Feature | Acquired by | Count |
|-----------------------------|---------------|-------|
| VALUE_AES_PROPRIETARY_LINKS | CVLAN (aes6x) | 1 |

6.2. 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.

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 Avaya Application Enablement Services Management Console. The top right corner displays system information: Welcome: User devconnect, Last login: Fri Feb 13 14:54:32 2015 from 192.168.100.18, Number of prior failed login attempts: 0, HostName/IP: aes6x/10.1.10.70, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 6.3.3.1.10-0, Server Date and Time: Fri Feb 13 15:37:37 SGT 2015, HA Status: Not Configured. The navigation bar includes 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'AE Services' expanded to 'TSAPI Links'. The main content area is titled 'TSAPI Links' and contains 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 “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 screenshot shows the 'Add TSAPI Links' screen in the Avaya Application Enablement Services Management Console. The top right corner displays system information: Welcome: User devconnect, Last login: Fri Feb 13 14:54:32 2015 from 192.168.100.18, Number of prior failed login attempts: 0, HostName/IP: aes6x/10.1.10.70, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 6.3.3.1.10-0, Server Date and Time: Fri Feb 13 15:33:32 SGT 2015, HA Status: Not Configured. The navigation bar includes 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'AE Services' expanded to 'TSAPI Links'. The main content area is titled 'Add TSAPI Links' and contains a form with the following fields: Link (text input with value 3), Switch Connection (dropdown menu with value Duplex), Switch CTI Link Number (dropdown menu with value 3), ASAI Link Version (dropdown menu with value 7), and Security (dropdown menu with value Unencrypted). Below the form are buttons for '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**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top right corner shows system information: Welcome: User devconnect, Last login: Fri Feb 13 14:54:32 2015 from 192.168.100.18, Number of prior failed login attempts: 0, HostName/IP: aes6x/10.1.10.70, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 6.3.3.1.10-0, Server Date and Time: Fri Feb 13 15:26:07 SGT 2015, HA Status: Not Configured.

The main navigation bar includes **Security | Security Database | Control** and **Home | Help | Logout**. The left sidebar menu shows the following structure:

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
 - ▶ Audit
 - ▶ Certificate Management
 - Enterprise Directory
 - ▶ Host AA
 - ▼ Security Database
 - Control
 - ▣ CTI Users
 - Devices
 - Device Groups

The main content area is titled **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** and contains the following configuration options:

- Enable SDB for DMCC Service
- Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

An **Apply Changes** button is located below the configuration options.

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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: Welcome: User devconnect, Last login: Fri Feb 13 14:54:32 2015 from 192.168.100.18, Number of prior failed login attempts: 0, HostName/IP: aes6x/10.1.10.70, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 6.3.3.1.10-0, Server Date and Time: Fri Feb 13 15:23:41 SGT 2015, HA Status: Not Configured.

The main navigation bar includes "Maintenance | Service Controller" and "Home | Help | Logout". The left sidebar lists various categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, Status, User Management, Utilities, and Help.

The main content area is titled "Service Controller" and contains a table with the following data:

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

Below the table, there is a note: "For status on actual services, please use [Status and Control](#)". At the bottom of the main content area, there are several buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and 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 Connector.

In this case, the associated Tlink name is “AVAYA#**DUPLEX**#CSTA#AES6X”. Note the use of the switch connection “**DUPLEX**” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo and the text "Application Enablement Services Management Console". At the top right, a welcome message reads: "Welcome: User devconnect", "Last login: Mon Feb 16 14:22:55 2015 from 10.1.10.99", "Number of prior failed login attempts: 0", "HostName/IP: aes6x/10.1.10.70", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 6.3.3.1.10-0", "Server Date and Time: Mon Feb 23 14:46:56 SGT 2015", and "HA Status: Not Configured". Below this is a red navigation bar with "Security | Security Database | Tlinks" on the left and "Home | Help | Logout" on the right. On the left side, a sidebar menu shows a tree structure with "Security Database" expanded to "Tlinks". The main content area is titled "Tlinks" and contains two radio button options: "AVAYA#DUPLEX#CSTA#AES6X" (which is selected) and "AVAYA#DUPLEX#CSTA-S#AES6X". A "Delete Tlink" button is located below the options.

6.7. 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).

Welcome: User devconnect
Last login: Mon Feb 16 14:22:55 2015 from 10.1.10.99
Number of prior failed login attempts: 0
HostName/IP: aes6x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Feb 23 14:49:32 SGT 2015
HA Status: Not Configured

AVAYA Application Enablement Services
Management Console

User Management | User Admin | List All Users Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ 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

Edit User

* User Id

* Common Name

* Surname

User Password

Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

Home Phone

Home Postal Address

Initials

Labeled URI

7. 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 6.2 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 pipe connector 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 Connector and SFDC -
#                               Avaya Certification lab in Singapore
# MCIS Release 6.5
#
#####

###
# 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

...

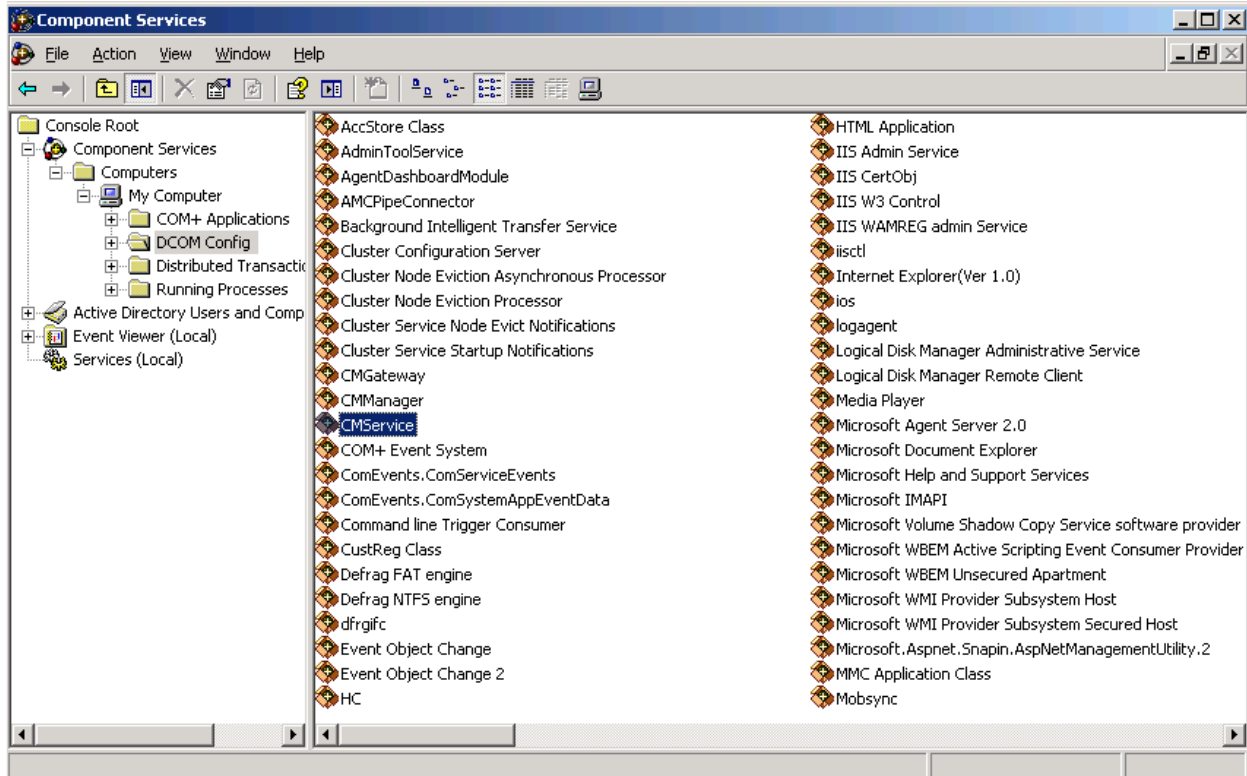
###
# License Manager
#
###
[LicenseManager]
# TraceEnabled=1
# TraceLevel=2
# TraceMaxSize=1024
```

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

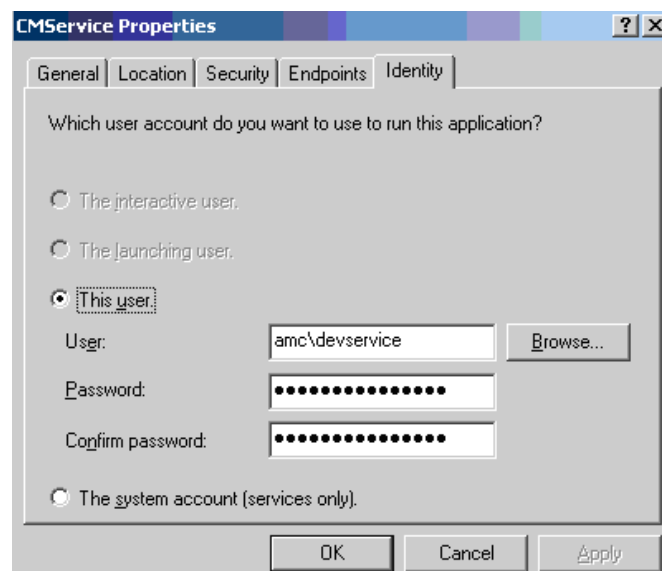
```
## For ACT
[CTIModule]
TraceLevel=4
Channel=CTI1
#ServerID=LUCENT#G3 SWITCH#CSTA#AMCW23S09
ServerID=AVAYA#DUPEX#CSTA#AES6X
UserName=CRTADM
#UserName=AMC
Password=amcamc
#Password=Connector#123
AllowDTMF=Yes
DTMFPause=5
#ForceStateRefresh=1
UseAutoIn=1
```

```
###
# 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...
```

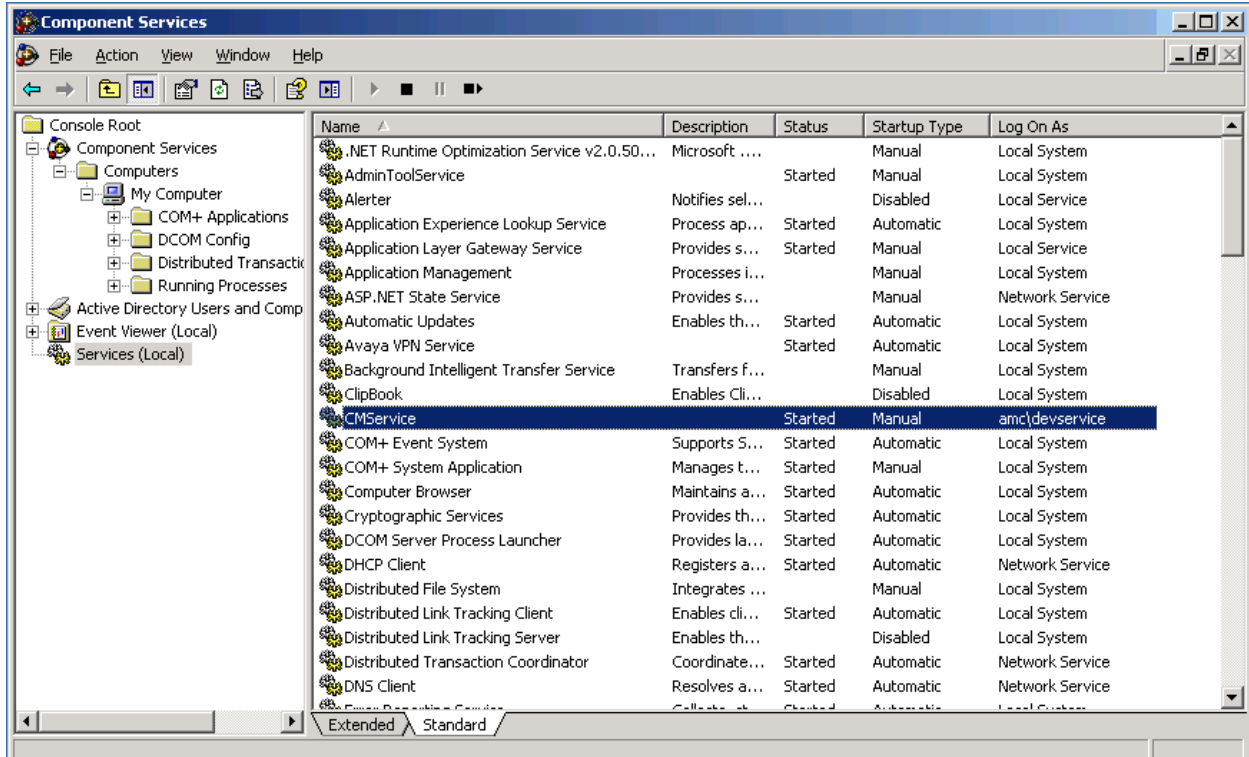
- Administer a user domain account in the Active Directory for DCOM communication between agents and CMService. In this example, the user is amc\devservice.
- Navigate to the **Component Services** in the Windows Server 2012 to access the window shown below. Double-click on CMService to open the properties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



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



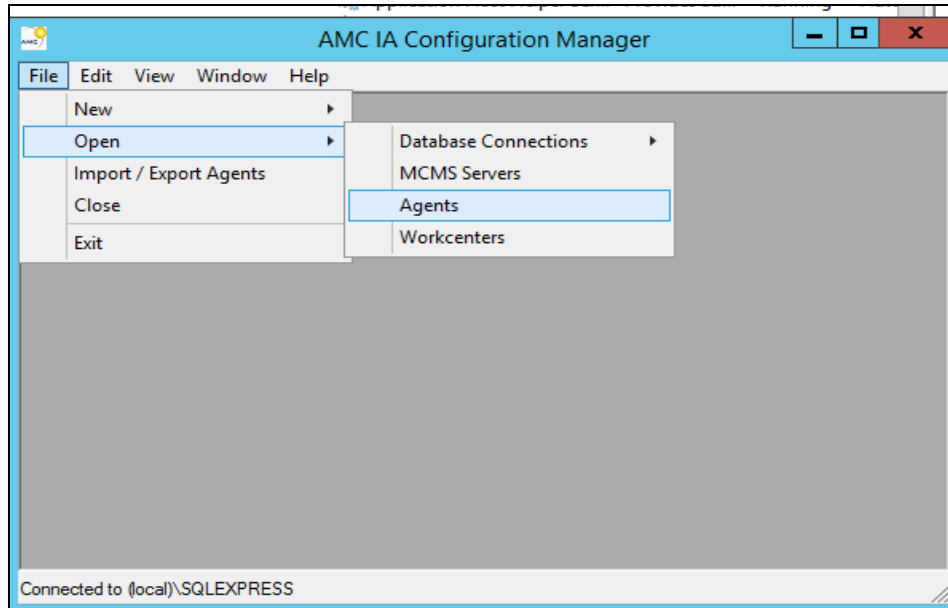
- Start the CMServices from the Services management window.



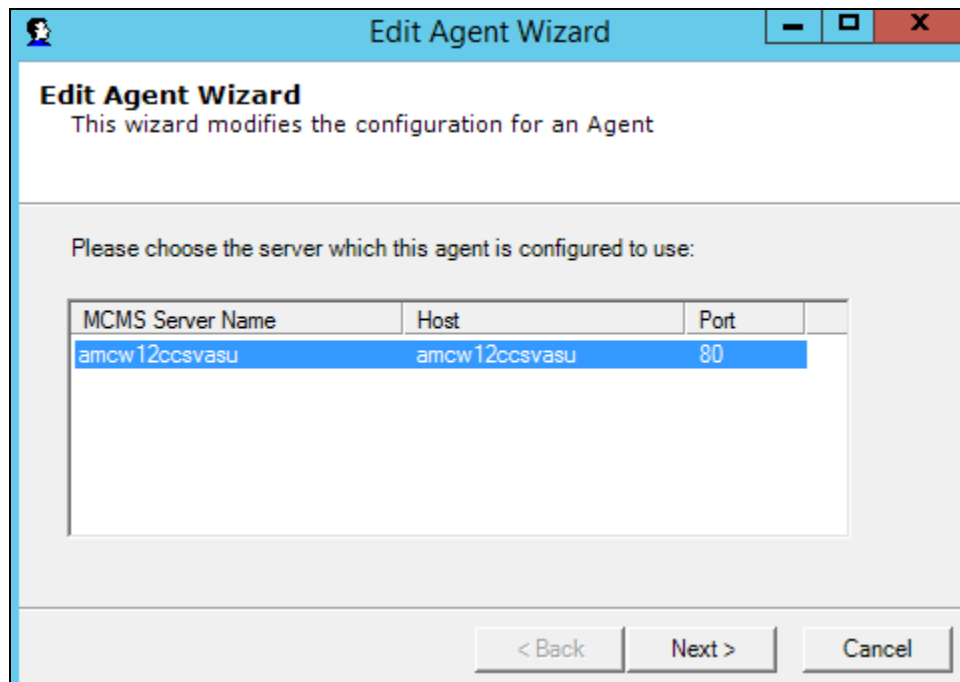
- Restart IIS by running the `iisreset` command in a command prompt window for SAPWeb/CRM7.

8. Configure SAPWeb/CRM7

As there are 6 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**.

Edit Agent Wizard
This wizard modifies the configuration for an Agent

Select the User Id for the agent you wish to configure

Agent User Id

New:

Existing:

Delete selected agent

< Back Next > Cancel

In the last window, the **Extension**, **AgentID**, and **AgentIDPassword** configured in **Sections 5.5** and **5.6** are specified. Click **Finish**.

Edit Agent Wizard - tester2
This wizard modifies the configuration for an Agent

Telephony (CT1)

| Name | Value |
|-----------------|-------|
| Extension | 10001 |
| AgentID | 11001 |
| AgentIDPassword | 1234 |
| Queues | 14001 |

Please fill in the configuration information for this channel

Skip this channel

< Back Finish 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 Connector 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 2 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 | Msgs Rcvd |
| 1 | | no | | down | 0 | 0 |
| 2 | | no | | down | 0 | 0 |
| 3 | 7 | no | aes6x | established | 15 | 15 |
| 4 | 7 | no | aes6x | 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 6.3** as shown below.

Application Enablement Services

Management Console

Welcome: user development

Last login: Thu Feb 12 21:53:14 2015 from 10.1.10.153

Number of prior failed login attempts: 0

HostName/IP: aes6x/10.1.10.70

Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE

SW Version: 6.3.3.1.10-0

Server Date and Time: Fri Feb 13 14:55:11 SGT 2015

HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ Status
 - Alarm Viewer
 - Log Manager
 - ▶ 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 seconds

| | Link | Switch Name | Switch CTI Link ID | Status | Since | State | Switch Version | Associations | Msgs to Switch | Msgs from Switch | Msgs Period |
|----------------------------------|------|-------------|--------------------|---------|-------------------------|--------|----------------|--------------|----------------|------------------|-------------|
| <input checked="" type="radio"/> | 3 | Duplex | 3 | Talking | Wed Feb 4 11:29:08 2015 | Online | 16 | 0 | 15 | 15 | 30 |

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

9.3. Verify AMC Connector and SAPWeb/CRM7

To verify that AMC Connector 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 Connector 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. Click **Log On**.



Log on using the appropriate credentials.



SAP NetWeaver

 No switch to HTTPS occurred, so it is not secure to send a password

System:

Client: *

User: *

Password: *

Language:

[Change Password](#)

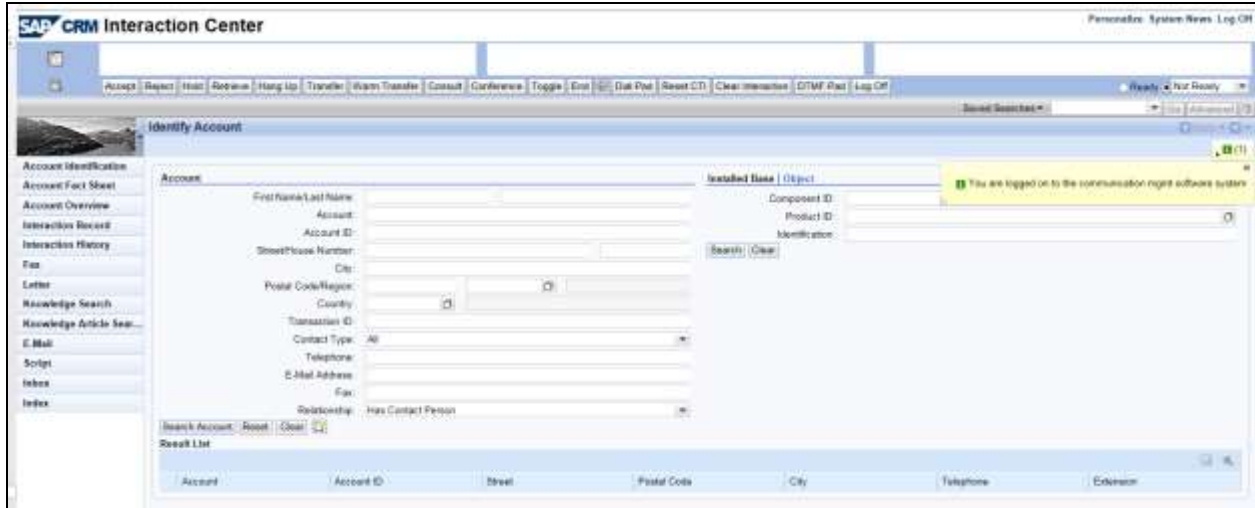
Copyright © 2015 SAP AG. All rights reserved.



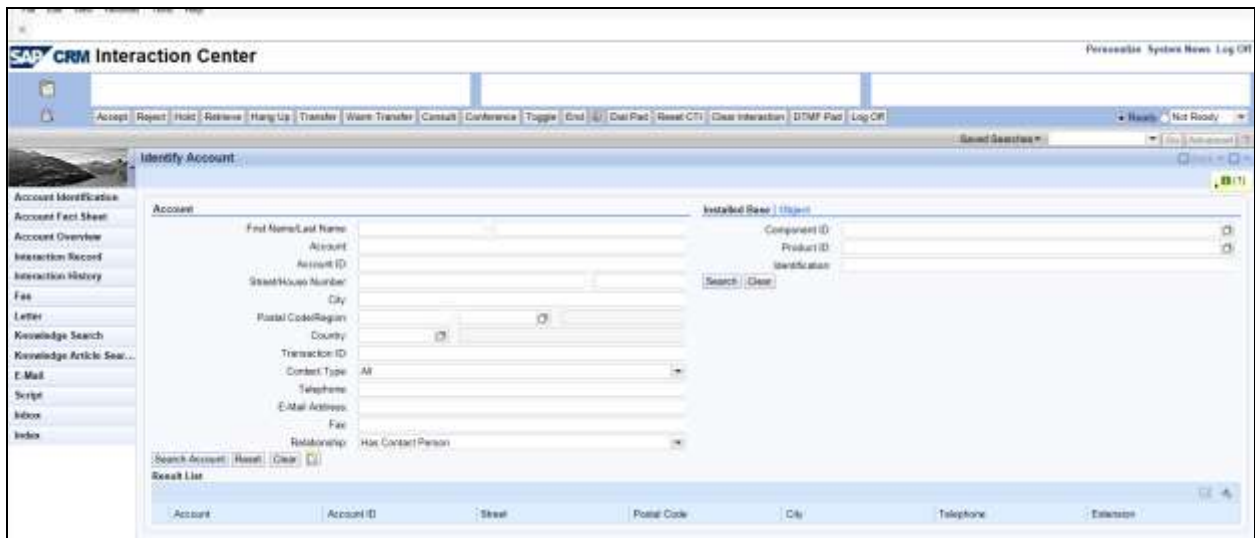
Select a business role:

- [. ZS1IC_AGENT-InteractionCenter Agent](#)
- [. ZV1IC_AGENT-InteractionCenter Agent](#)

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



Change the state to “Ready” as shown below.



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 Connector for Avaya Aura® Application Enablement Services (AES). The AMC connector 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 6.3, June 2014, Issue 10.0, Document Number 03-300509.
- [2] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, June 2014, Release 6.3, Document Number 02-300357.
- [3] *AMC Telephony Connector – Avaya Computer Telephony Implementation Guide*, Version 6.5.0.0.

©2015 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.