



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

---

# **Application Notes for TelStrat Engage with Avaya Aura® Communication Manager Using Avaya Aura® Application Enablement Services 6.2 with TSAPI – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps required for TelStrat Engage to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.2 with Telephony Services Application Programming Interface (TSAPI).

TelStrat Engage is a call recording solution. In the compliance testing, TelStrat Engage used TSAPI from Avaya Aura® Application Enablement Services to monitor skill groups and agent station extensions on Avaya Aura® Communication Manager, and used the port mirroring method to capture the media associated with the monitored agents for call recording.

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 for TelStrat Engage to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.2 with TSAPI.

TelStrat Engage is a call recording solution. In the compliance testing, TelStrat Engage used TSAPI from Avaya Aura® Application Enablement Services to monitor skill groups and agent station extensions on Avaya Aura® Communication Manager, and used the port mirroring method to capture the media associated with the monitored agents for call recording.

The TSAPI interface is used by TelStrat Engage to monitor the skill groups and agent station extensions. When there is an active call on the monitored agent, TelStrat Engage is informed of the call via event reports from the TSAPI interface. TelStrat Engage starts the call recording by using the replicated media from the port mirroring method. The TSAPI event reports are also used to determine when to stop the call recordings.

# 2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Engage application, the application automatically uses TSAPI to query on the skill group and agent station extensions and request monitoring.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for the recordings. Necessary user actions such as hold and reconnect were performed from the agent telephones to test the different call scenarios. The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Engage.

The verification of tests included using the TelStrat Engage logs for proper message exchanges, and using the Engage Client application for proper logging and playback of the calls.

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.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Engage:

- Handling of TSAPI messages in the areas of event notification and value queries.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, simultaneous, conference, and transfer.

The serviceability testing focused on verifying the ability of Engage to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the Engage server.

## 2.2. Test Results

All test cases were executed and passed. The following were observations on Engage from the compliance testing:

- In the attended conference scenarios, the first recording for the conference-from agent included silence for the period that the conference-from agent was conversing with the conference-to agent, and the second recording for the conference-from agent contained the conversation with the conference-to agent.
- After a 60 seconds link disruption, the Engage Client application may become stuck and need a manually restart.

## 2.3. Support

Technical support on Engage can be obtained through the following:

- **Phone:** (972) 633-4548
- **Email:** [support@telstrat.com](mailto:support@telstrat.com)

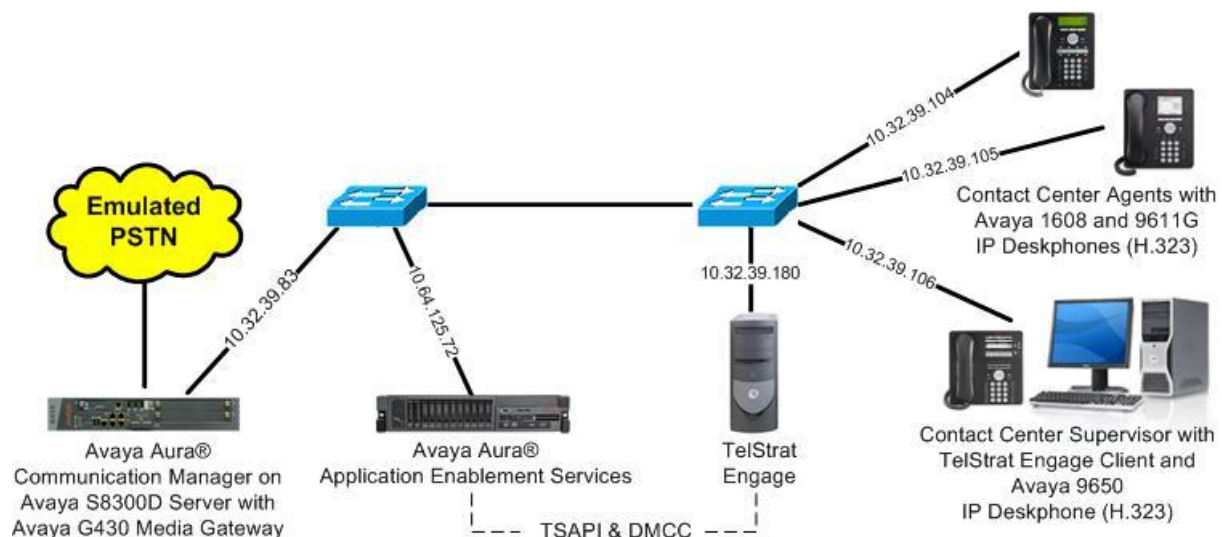
### 3. Reference Configuration

Engage has an Engage Client application that can be used to review and playback the call recordings. In the compliance testing, the Engage Client application was installed on the supervisor PC. The RTP streams for agents with Avaya IP Deskphones were mirrored from the layer 2 switch, and replicated over to Engage.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described. In addition, the port mirroring of the layer 2 switch is also outside the scope of these Application Notes and will not be described.

In the compliance testing, the contact center devices consisted of two VDNs, two skill groups, one supervisor, and two agents shown in the table below. Engage requested monitoring on the skill group and agent station extensions.

Device Type	Extension
VDN	48001, 48002
Skill Group	48101, 48102
Supervisor	45000
Agent ID	45881, 45882
Agent Station	45001, 45002



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Avaya S8300D Server with Avaya G430 Media Gateway	6.2 SP3 (R016x.02.0.823.0-20001)
Avaya Aura® Application Enablement Services	6.2 (r6-2-0-18-0)
Avaya 1608 IP Deskphone (H.323)	1.302S
Avaya 9611G IP Deskphone (H.323)	6.020S
Avaya 9650 IP Deskphone (H.323)	3.1000
TelStrat Engage on Windows 2008 Server Standard <ul style="list-style-type: none"><li>• Microsoft SQL Server 2008</li><li>• Avaya TSAPI Windows Client (csta32.dll)</li></ul>	3.6.1.11 SP 2 R2 6.2.0.257
TelStrat Engage Client on Windows XP Professional	3.6.1.11 2002 SP3

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link

### 5.1. Verify License

Log in to 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 set to “y”, 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)? y	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	<b>Computer Telephony Adjunct Links? y</b>
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	

### 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 1	Page 1 of 3
CTI LINK	
CTI Link: 1	
<b>Extension: 40001</b>	
<b>Type: ADJ-IP</b>	
	COR: 1
<b>Name: TSAPI Link</b>	

## 6. Configure Avaya Aura® Application Enablement Services

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

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

### 6.1. Launch OAM Interface


Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. Below this bar, centered, is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields labeled "Username" and "Password". Below these fields is a blue "Login" button. At the bottom of the page, another thick red horizontal bar is present, and below it, the copyright notice "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved." is displayed.

The **Welcome to OAM** screen is displayed next.

**Application Enablement Services  
Management Console**

Welcome: User  
Last login: Tue Feb 19 07:24:07 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-2-0-18-0  
Server Date and Time: Tue Feb 19 07:27:34 MST 2013

HomeHome | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

### Welcome to OAM


The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

## 6.2. Verify License

Select **Licensing → WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

**Application Enablement Services  
Management Console**

Welcome: User  
Last login: Tue Feb 19 07:24:07 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-2-0-18-0  
Server Date and Time: Tue Feb 19 07:27:34 MST 2013

LicensingHome | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▼ **Licensing**
  - WebLM Server Address
  - WebLM Server Access**
  - Reserved Licenses
- ▶ Maintenance
- ▶ Networking
- ▶ Security

### Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access


If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses



The **Web License Manager** screen below is displayed. Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane, to display the **Licensed Features** in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.


Web License Manager (WebLM v6.2)

[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

WebLM Home  
Install license  
Licensed products  
APPL\_ENAB  
▼ Application\_Enablement  
View license capacity  
View peak usage  
Uninstall license  
Server properties  
Manage users  
Shortcuts  
Help for Installed Product

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

You are here: Licensed Products > Application\_Enablement > View License Capacity  
License installed on: May 11, 2012 6:07:47 PM -05:00  
License File Host IDs: 00-16-3E-48-ED-82

Licensed Features

Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	16	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	<div> SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer  MediumServerTypes: ibmx306;ibmx306m;del11950;xen;hs20;hs20_8832_vm;CtiMediumServer  LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer  TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,, CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; </div>	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	16	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	0
DLG (VALUE_AES_DLG)	permanent	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	0

### 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 left sidebar has a tree view with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TSAPI Links', and 'TSAPI Properties'. The main content area is titled 'TSAPI Links' and contains a table with one row of data. The table has 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'.

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	S8800	2	4	Both

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 “S8300D” 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 left sidebar is the same as the previous screenshot. The main content area is titled 'Add TSAPI Links' and contains a form with five fields: Link (value 2), Switch Connection (value S8300D), Switch CTI Link Number (value 1), ASAI Link Version (value 4), and Security (value Unencrypted). Below the form are buttons for 'Apply Changes' and 'Cancel Changes'.

## 6.4. Disable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below, and click **Apply Changes**.

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 the user. The left navigation pane shows a tree structure with "Security" expanded, and "Security Database" and "Control" selected. The main content area displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" screen. It contains two checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", both of which are unchecked. Below the checkboxes is an "Apply Changes" button.

## 6.5. Restart TSAPI Service

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

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 the user. The left navigation pane shows a tree structure with "Maintenance" expanded, and "Service Controller" selected. The main content area displays the "Service Controller" screen. It contains a table with two columns: "Service" and "Controller Status". The table lists several services, including ASAI Link Manager, DMCC Service, CVLAN Service, DLG Service, Transport Layer Service, and TSAPI Service. The TSAPI Service is checked, and its status is "Running". Below the table is a link "Status and Control" and a row of buttons: "Start", "Stop", "Restart Service", "Restart AE Server", "Restart Linux", and "Restart Web Server".

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

## 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, to be used later for configuring Engage.

In this case, the associated Tlink name is “AVAYA#S8300D#CSTA#AES2-S8800”. Note the use of the switch connection “S8300D” from **Section 6.3** 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 the user. The left navigation pane shows a tree structure with "Security" expanded, and "Security Database" selected, with "Tlinks" highlighted. The main content area, titled "Tlinks", lists three Tlink names with radio buttons for selection: "AVAYA#S8300D#CSTA#AES\_125\_72" (selected), "AVAYA#S8800#CSTA#AES\_125\_72", and "AVAYA#S8800#CSTA-S#AES\_125\_72". A "Delete Tlink" button is located below the list.

Welcome: User  
Last login: Tue Feb 19 07:24:07 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-2-0-18-0  
Server Date and Time: Tue Feb 19 07:27:34 MST 2013

Security | Security Database | Tlinks 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

Tlinks

Tlink Name

☒ AVAYA#S8300D#CSTA#AES\_125\_72  
☐ AVAYA#S8800#CSTA#AES\_125\_72  
☐ AVAYA#S8800#CSTA-S#AES\_125\_72

Delete Tlink

## 6.7. Administer Engage User

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

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  
Last login: Tue Feb 19 07:24:07 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-2-0-18-0  
Server Date and Time: Tue Feb 19 07:27:34 MST 2013

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 Idengage

\* Common Nameengage

\* Surnameengage

\* User Password••••••••

\* Confirm Password••••••••

Admin Note

Avaya RoleNone

Business Category

Car License

CM Home

Css Home

CT UserYes

Department Number

Display Name

Employee Number

Employee Type

## 7. Configure Avaya IP Deskphones

This section provides the procedures for obtaining the MAC addresses from the Avaya IP Deskphones.

### 7.1. Obtain MAC Address

From the Avaya IP Deskphone, press the **MENU** or **HOME** button to display the **Menu** or **Home** screen (not shown).

From the **Menu** or **Home** screen, navigate to **Network Information** → **Miscellaneous** to display the **Miscellaneous** screen (not shown).

From the **Miscellaneous** screen, page down as necessary to display the **MAC** parameter (not shown). Make a note of the **MAC** address, which will be used later to configure Engage.

Repeat this section for all Avaya IP Deskphones used by the agents in **Section 3**. In the compliance testing, the MAC addresses associated with the two agent telephones were “00073B9363F3” and “7038EEC9D518”.



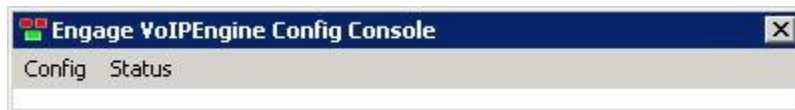
## 8. Configure TelStrat Engage

This section provides the procedures for configuring Engage. The procedures include the following areas:

- Administer VoIP engine
- Administer ACD groups
- Administer device port mappings

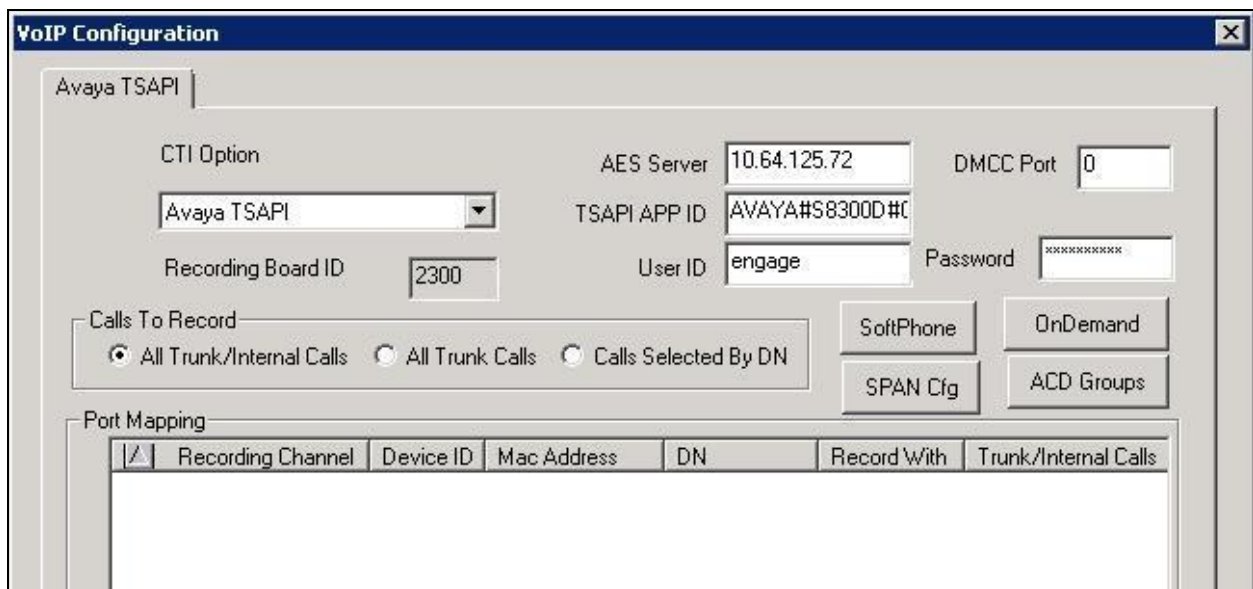
### 8.1. Launch VoIP Engine

From the Engage server, select **Start → All Programs → TelStrat Engage → VOIP Engine Configuration**, to display the **Engage VoIP Engine Config Console** screen below. Select **Config**.



The **VoIP Configuration** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

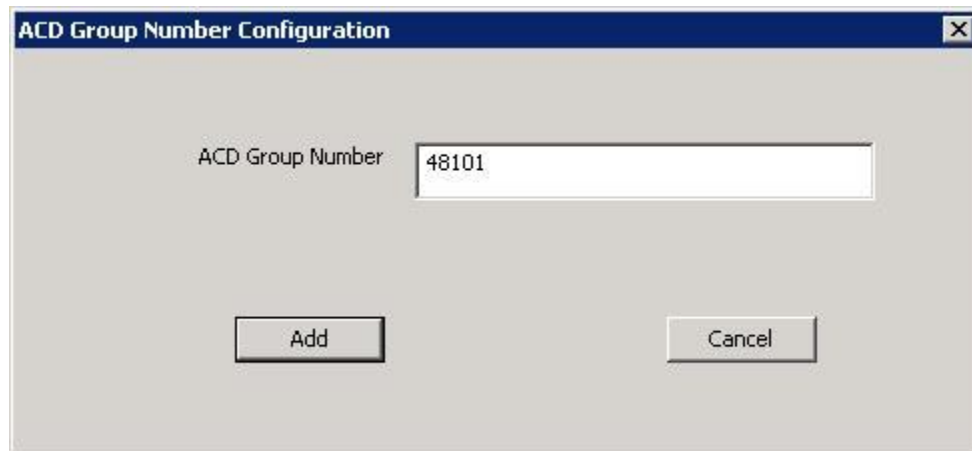
- **CTI Option:** "Avaya TSAPI"
- **AES Server:** The IP address of the Application Enablement Services server.
- **TSAPI APP ID:** The Tlink name from **Section 6.6**.
- **User ID:** The Engage user credentials from **Section 6.7**.
- **Password:** The Engage user credentials from **Section 6.7**.

A screenshot of the "VoIP Configuration" window. It has a blue title bar. The main area is divided into sections. The "Avaya TSAPI" section is active. It contains fields for "CTI Option" (a dropdown menu showing "Avaya TSAPI"), "AES Server" (text box with "10.64.125.72"), "DMCC Port" (text box with "0"), "TSAPI APP ID" (text box with "AVAYA#S8300D#C"), "Recording Board ID" (text box with "2300"), "User ID" (text box with "engage"), and "Password" (text box with "XXXXXXXXXX"). Below these is a "Calls To Record" section with three radio buttons: "All Trunk/Internal Calls" (selected), "All Trunk Calls", and "Calls Selected By DN". To the right of these are four buttons: "SoftPhone", "OnDemand", "SPAN Cfg", and "ACD Groups". At the bottom is a "Port Mapping" section with a table. The table has columns: "Recording Channel", "Device ID", "Mac Address", "DN", "Record With", and "Trunk/Internal Calls". The table is currently empty.

## 8.2. Administer ACD Groups

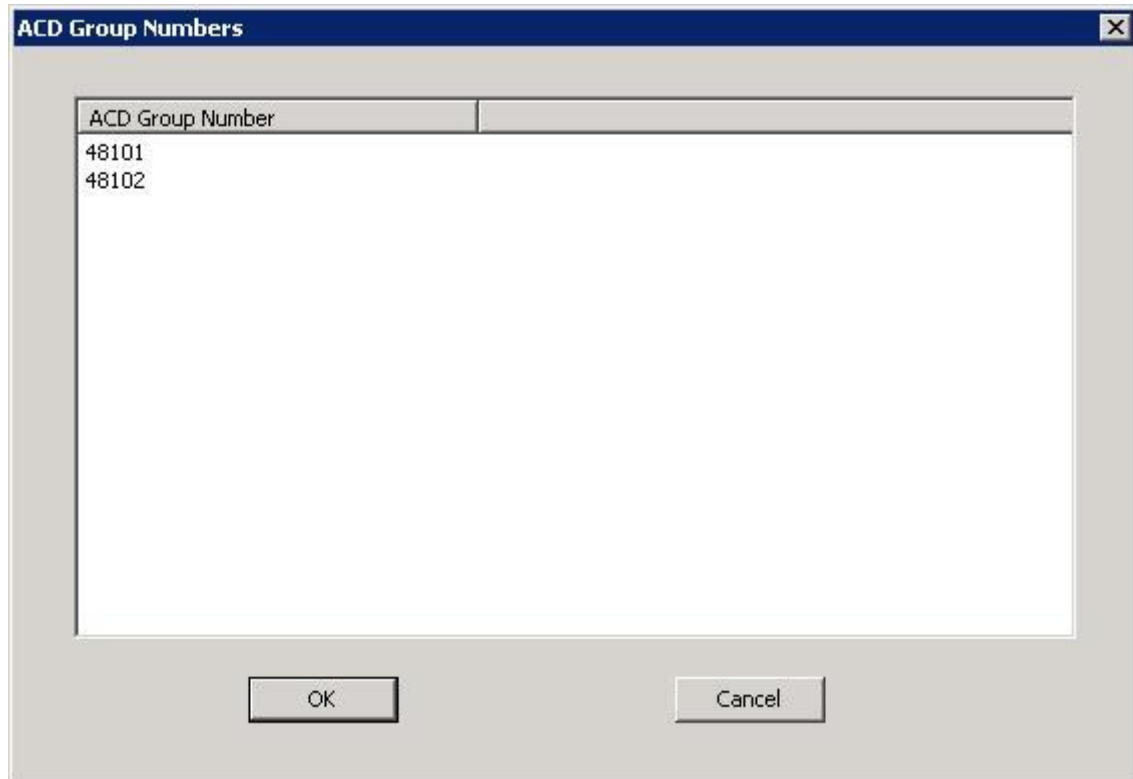
From the **VoIP Configuration** screen shown in **Section 8.1**, click on **ACD Groups** to display the **ACD Group Numbers** screen (not shown). Right click in the empty pane and select **Add**.

The **ACD Group Number Configuration** screen is displayed next. Enter the first skill group extension from **Section 3**.



The image shows a dialog box titled "ACD Group Number Configuration". It has a text input field labeled "ACD Group Number" containing the value "48101". Below the input field are two buttons: "Add" and "Cancel".

Repeat this section to add all remaining skill groups. In the compliance testing, two skill groups were configured as shown below.



The image shows a dialog box titled "ACD Group Numbers". It contains a list box with the following items:

ACD Group Number
48101
48102

At the bottom of the dialog box are two buttons: "OK" and "Cancel".



### 8.3. Administer Device Port Mappings

From the **VoIP Configuration** screen shown in **Section 8.1**, right-click in the empty pane and select **ADD**. The **Device And CommSrv Port Mapping** screen is displayed.

For **Device ID**, enter the first agent station extension from **Section 3**. Select the **Mirroring** radio button to enable the **MAC** field. For **MAC**, enter the MAC address of the first agent telephone from **Section 7.1**.

For **DN**, enter the dialed number to reach the agent directly for personal calls (non-ACD). For calls originated within Communication Manager, this is usually the agent station extension, depending on the switch configuration. For calls originated outside of Communication Manager, the dialed number usually contains the dial plan prefix. Note that a device port mapping needs to be created for every possible number that can be dialed to reach the agent directly.

For **CommSrv Port Number**, enter an available port, which begins with “0”.

Retain the default in the remaining fields.

Device And CommSrv Port Mapping

Device ID: 45001

MAC: 00073B9363F3

DN: 45001

CommSrv Port Number: 0

Calls To Record

☐ Trunk/Internal Calls ☐ Trunk Calls

Recording Stream

☒ Mirroring ☐ Service Observe

☐ STC Stream

Beep Tone: No

Add Cancel

Repeat this section to create device port mappings for all agents in **Section 3**.

In the compliance testing, two entries were created for each agent. The incoming non-ACD trunk calls to reach the agent directly will have a prefix of “90884”, as shown below.

The image shows a 'VoIP Configuration' dialog box with the 'Avaya TSAPI' tab selected. The settings include:

- CTI Option: Avaya TSAPI (dropdown)
- AES Server: 10.64.125.72
- DMCC Port: 0
- TSAPI APP ID: AVAYA#S8300D#C
- Recording Board ID: 2300
- User ID: engage
- Password: (masked with asterisks)

Under 'Calls To Record', the 'All Trunk/Internal Calls' radio button is selected. There are buttons for 'SoftPhone', 'OnDemand', 'SPAN Cfg', and 'ACD Groups'.

The 'Port Mapping' section contains a table with the following data:

	Recording Channel	Device ID	Mac Address	DN	Record With	Trunk/Internal Calls
000		45001	00073B9363F3	45001	Mirroring	Trunk/Internal
000		45001	00073B9363F3	9088445001	Mirroring	Trunk/Internal
001		45002	7038EEC9D518	45002	Mirroring	Trunk/Internal
001		45002	7038EEC9D518	9088445002	Mirroring	Trunk/Internal

At the bottom, there is a 'No. of Log Files' field set to 8, a 'Config File Location' button, and 'OK' and 'Cancel' buttons.

## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and Engage.

### 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 the CTI link number 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	4	no	aes_125_72	established	33	39

### 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**, and that the **Associations** column reflects the number of skill groups and agent station extensions from **Section 3**.

**Application Enablement Services**  
Management Console

Welcome: User  
Last login: Thu Feb 21 12:35:06 2013 from 10.32.39.20  
Number of prior failed login attempts: 0  
HostName/IP: aes\_125\_72/10.64.125.72  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-2-0-18-0  
Server Date and Time: Thu Feb 21 13:17:37 MST 2013

Status | Status and Control | TSAPI Service Summary

Home | Help | Logout

▶ 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

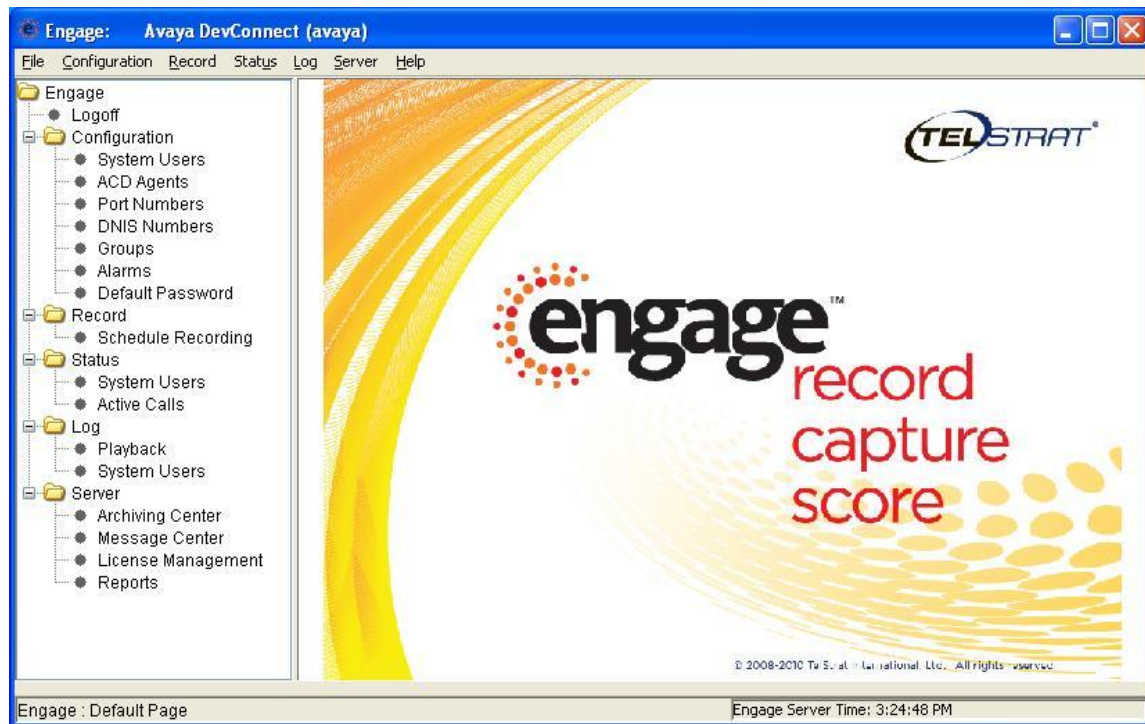
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
⊖	1	S8800	2	Talking	Wed Feb 13 11:51:18 2013	Online	16	0	15	15	30
⊕	2	S8300D	1	Talking	Thu Feb 21 07:25:08 2013	Online	16	4	39	33	30

Online Offline

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

### 9.3. Verify TelStrat Engage

Log an agent in to the skill group to handle and complete an ACD call. From the PC running the Engage Client application, select **Start** → **All Programs** → **TelStrat Engage** → **Engage Client** to launch the application, and log in using the appropriate credentials. The **Engage** screen below is displayed. Select **Engage** → **Log** → **Playback** from the left pane.



The **Engage** screen is updated with a list of the call recordings. Verify that there is an entry reflecting the last call, with proper values in the relevant fields. Double click on the entry and verify that the call recording can be played back.



## 10. Conclusion

These Application Notes describe the configuration steps required for TelStrat Engage to successfully interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services 6.2 with TSAPI. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 7.0, Release 6.2, July 2012, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.2, Issue 1, July 2012, available at <http://support.avaya.com>.
3. *Engage Server Installation and Administration Guide*, Product Release 3.6, Standard 1.2, June 2012, available on the installation CD.
4. *Engage Contact Center Suite System Administration Guide*, Product Release 3.6, Standard 3.4, June 2012, available on the installation CD.
5. *Engage Contact Center Suite Configuring Engage with Avaya Aura Communication Manager*, Product Release 3.6.1, Standard 1.3, October 2012, available on the installation CD.

---

**©2013 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).