



Avaya Solution & Interoperability Test Lab

Application Notes for TelStrat Engage with Avaya Aura® Communication Manager Using Avaya Aura® Application Enablement Services with TSAPI and DMCC – 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 with Telephony Services Application Programming Interface (TSAPI) and Device, Media, and Call Control (DMCC).

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 telephone extensions on Avaya Aura® Communication Manager, and used DMCC 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 with TSAPI and DMCC.

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 telephone extensions on Avaya Aura® Communication Manager, and used DMCC 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 telephone 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 Single Step Conference feature from the DMCC interface to add a virtual IP softphone to the active call to obtain the media. 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 TelStrat Engage application, the application automatically registers the virtual IP softphones to Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services DMCC, and queries for the skill group and agent telephone extensions and requests monitoring using TSAPI.

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 cable to TelStrat 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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on TelStrat Engage:

- Handling of TSAPI messages in the areas of event notification and value queries.
- Use of DMCC registration services to register and un-register the virtual IP softphones.
- Use of DMCC call control services to activate Single Step Conference for the virtual IP softphones and to obtain the media for call recording.
- 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 TelStrat Engage to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to the TelStrat Engage server.

2.2. Test Results

All test cases were executed and passed. The following were observations on TelStrat 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.
- For calls established before a link outage and stayed up during and after the link outage, the recordings will contain the conversation up to the link disruption.

2.3. Support

Technical support on TelStrat Engage can be obtained through the following:

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

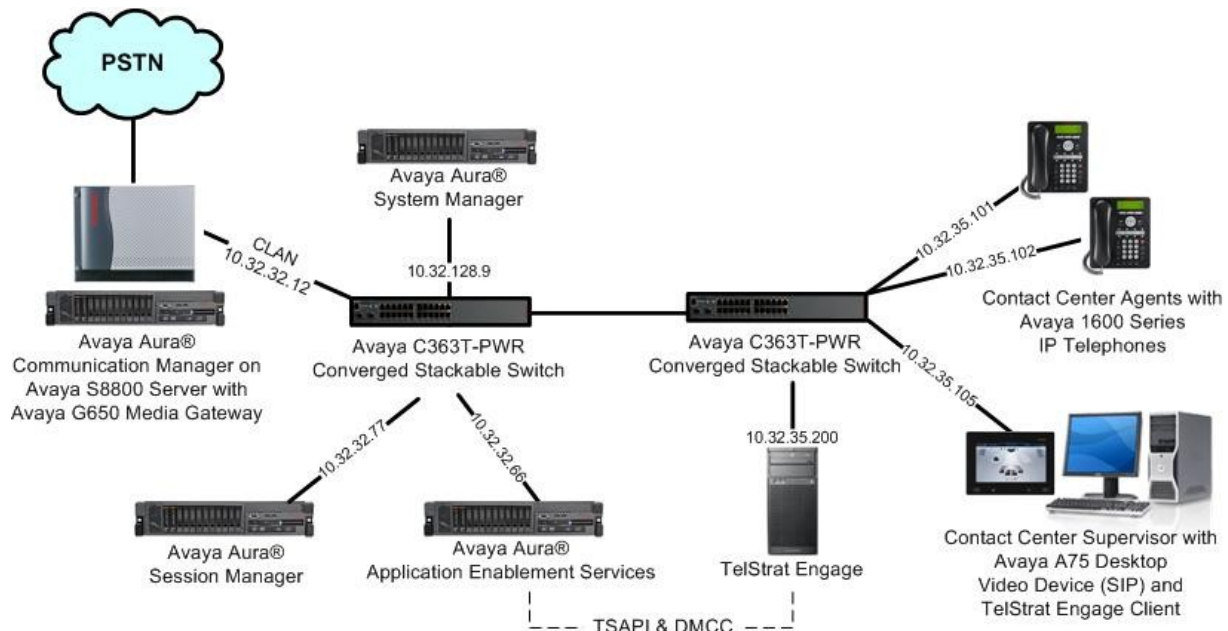
3. Reference Configuration

TelStrat 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 detailed administration of basic connectivity between Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, the contact center devices consisted of a skill group, a supervisor, and two agents shown in the table below. TelStrat Engage requested monitoring on the skill group and agent telephone extensions.

Device Type	Extension
Skill Group	65555
Supervisor	65000
Agent IDs	65881, 65882
Agent Telephone Extensions	65001, 65002



4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8800 Server	6.0.1 (R016x.00.1.510.1-18621)
Avaya G650 Media Gateway <ul style="list-style-type: none">TN799DP C-LAN Circuit PackTN2302AP IP Media Processor	HW01 FW038 HW20 FW121
Avaya Aura® Application Enablement Services	5.2.2 (r5-2-2-105-0)
Avaya Aura® System Manager	6.1.0 (6.1.0.4.5072-6.1.4.113)
Avaya Aura® Session Manager	6.1.0 (6.1.0.0.610023)
Avaya 1600 Series IP Telephones (H.323)	1.3
Avaya A175 Desktop Video Device	1.0.0
TelStrat Engage on Windows 2003 Server with Service Pack 2 <ul style="list-style-type: none">Database ServerAvaya TSAPI Windows ClientAvaya DMCC .NET Service Provider	3.3.0.3 Microsoft SQL Server 2008 R2 5.2.1.483 4.2.46.0
TelStrat Engage Client	3.3.0.3

5. Configure Avaya Aura®Communication Manager

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

- Verify Communication Manager License
- Administer IP codec set
- Administer CTI link
- Administer virtual IP softphones

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 Link** 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? n
Access Security Gateway (ASG)?n            Authorization Codes? n
    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? n    Change COR by FAC? y
ARS?y Computer Telephony Adjunct Links? y
ARS/AAR Partitioning?yCvg Of Calls Redirected Off-net? n
ARS/AAR Dialing without FAC?y              DCS (Basic)? n
ASAI Link Core Capabilities?y              DCS Call Coverage? n
    ASAI Link Plus Capabilities? y          DCS with Rerouting? n
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
```

5.2. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for the agents. Enter the desired audio codec types in the **Audio Codec** fields. Note that TelStrat Engage only supports the G.711 and G.729 codec variants.

```
changeip-codec-set 1                                                    Page 1 of 2

                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
CodecSuppression PerPkt  Size(ms)
1: G.711MU          n          2          20
2:
```

5.3. 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.

```
addcti-link 1          Page 1 of 3
                        CTI LINK
CTI Link: 1
Extension: 60100
Type: ADJ-IP
Name: Engage CTI Link
COR: 1
```

5.4. Administer Virtual IP Softphones

Add a virtual softphone using the “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as “4620”.
- **Name:** A descriptive name.
- **Security Code:** Required by Engage to be the same value as **Extension**.
- **IP SoftPhone:** “y”

```
add station 65991          Page 1 of 5
                        STATION
Extension: 65991          Lock Messages? n          BCC: 0
Type: 4620Security Code: 65991          TN: 1
Port: IP          Coverage Path 1:          COR: 1
Name: Engage Virtual #1          Coverage Path 2:          COS: 1
                        Hunt-to Station:
STATION OPTIONS
Loss Group: 19          Time of Day Lock Table:
Personalized Ringing Pattern: 1
Message Lamp Ext: 65991
Speakerphone: 2-way          Mute Button Enabled? y
Display Language: english          Expansion Module? n
Survivable GK Node Name:
Survivable COR: internal          Media Complex Ext:
Survivable Trunk Dest?yIP SoftPhone? y
IP Video Softphone?n
Short/Prefixed Registration Allowed: default
Customizable Labels? Y
```

Repeat this section to administer the desired number of virtual softphones, using sequential extension numbers. In the compliance testing, two virtual softphones were administered as shown below, to allow for simultaneous recording of two monitored agents in **Section 3**.

list station 65991 count 2									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack		
65991	S00020 4620	Engage Virtual #1	no		1	1			
65992	S00023 4620	Engage Virtual #2	no		1	1			

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 license
- Launch OAM interface
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer Engage user
- Enable DMCC unencrypted port

6.1. Verify License

Access the Web License Manager interface by using the URL “https://ip-address/WebLM/index.jsp” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

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

The image shows the Avaya Web License Manager (WebLM v4.6) login interface. At the top, the Avaya logo is displayed in red. Below it, a red banner contains the text "Web License Manager (WebLM v4.6)". The main heading is "Logon". There are two input fields: "User Name:" and "Password:". To the right of the password field is a dark gray button with a white right-pointing arrow.

The **Web License Manager** screen below 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 **Device Media and Call Control** and **TSAPI Simultaneous Users**, as shown below.

The screenshot shows the Avaya Web License Manager (WebLM v4.6) interface. The left sidebar contains navigation links: Install License, Licensed Products (expanded), APPL_ENAB (expanded), Application_Enablement (selected), Uninstall License, Change Password, Server Properties, Manage Users, and Logout. The main content area is titled "Application Enablement (CTI) - Release: 5 - SID: 10503000 (Standard License File)". It includes a breadcrumb "You are here: Licensed products > Application Enablement (CTI)", the license installation date "Apr 16, 2010 11:27:38 AM EDT", and a link to "View Peak Usage". Below this is a table titled "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	2
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	1000
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	3	1

6.2. 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, the Avaya logo is followed by the text "Application Enablement Services" and "Management Console". A red horizontal bar contains a "Help" link on the right. The main content area is a light gray box with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below these fields is a "Login" button. At the bottom of the page, a red horizontal bar is followed by the copyright notice "© 2009 Avaya, Inc. All Rights Reserved."

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

Application Enablement Services
Management Console

Welcome: User craft
Last login: Tue Feb 1 14:02:54 2011 from 10.32.35.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r5-2-2-105-0

Home
Home | 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 infomations.
- 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 both domains, or a separate administrator for each domain.

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**.

Application Enablement Services
Management Console

Welcome: User craft
Last login: Tue Feb 1 14:02:54 2011 from 10.32.35.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r5-2-2-105-0

AE Services | TSAPI | TSAPI Link
Home | Help | Logout

- ▼ AE Services
 - ▶ CVLAN
 - ▶ DLG
 - ▶ DMCC
 - ▶ SMS
 - ▼ TSAPI
 - TSAPI Links
 - TSAPI Properties

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
Add Link Edit Link 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 “CM8800” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.3**. Retain the default values in the remaining fields, and click **Apply Changes**.

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ TSAPI

▪ TSAPI Links

▪ TSAPI Properties

▶ Communication Manager
Interface

▶ Licensing

Add TSAPI Links

Link	1 ▼
Switch Connection	CM8800 ▼
Switch CTI Link Number	1 ▼
ASAI Link Version	4 ▼
Security	Unencrypted ▼
<input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/>	

6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface > Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “CM8800”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' > 'Switch Connections'. The main content area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. There is one entry: CM8800, No, 30, 1. Below the table are four buttons: Edit Connection, Edit PE/CLAN IPs, Edit H.323 Gatekeeper, and Delete Connection. The 'Edit H.323 Gatekeeper' button is highlighted.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
CM8800	No	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor Ethernet on Communication Manager to be used as H.323 gatekeeper, in this case “10.32.32.12” is a C-LAN circuit pack. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - CM8800' screen. The left navigation pane is expanded to 'Communication Manager Interface' > 'Switch Connections'. The main content area displays a form with a text input field containing '10.32.32.12' and a button 'Add Name or IP'. Below the input field is a label 'Name or IP Address' and a button 'Delete IP'.

6.5. Disable Security Database

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Security' expanded, with 'Security Database' and 'Control' selected. The main content area is titled 'SDB Control for DMCC and TSAPI' and contains two checkboxes: 'Enable SDB for DMCC Service' (checked) and 'Enable SDB TSAPI Service, JTAPI and Telephony Service' (unchecked). An 'Apply Changes' button is at the bottom.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Tue Feb 1 14:02:54 2011 from 10.32.35.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r5-2-2-105-0

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

SDB Control for DMCC and TSAPI

☒ Enable SDB for DMCC Service
☐ Enable SDB TSAPI Service, JTAPI and Telephony Service
Apply Changes

6.6. Restart TSAPI Service

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

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Maintenance' expanded, with 'Service Controller' selected. The main content area is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'TSAPI Service' checked. 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'.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Tue Feb 1 14:02:54 2011 from 10.32.35.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r5-2-2-105-0

Maintenance | Service Controller

Home | Help | Logout

AE Services
Communication Manager Interface
Licensing
Maintenance
Date Time/NTP Server
Security Database
Service Controller
Server Data
Networking
Security
Status
User Management

Service Controller

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

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

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

6.7. 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 TelStrat Engage.

In this case, the associated Tlink name is “AVAYA#CM8800#CSTA#AES2-S8800”. Note the use of the switch connection “CM8800” 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 user "craft" with login details. A red navigation bar contains "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", shows a single entry: "AVAYA#CM8800#CSTA#AES2-S8800", with "Edit Tlink" and "Delete Tlink" buttons.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Tue Feb 1 14:45:14 2011 from 10.32.35.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r5-2-2-105-0

Security | Security Database | Tlinks Home | Help | Logout

Tlinks

Tlink Name
AVAYA#CM8800#CSTA#AES2-S8800
[Edit Tlink] [Delete Tlink]

6.8. 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 values in the remaining fields. Click **Apply** at the bottom of the screen (not shown).

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: 'Welcome: User craft', 'Last login: Tue Feb 1 14:02:54 2011 from 10.32.35.10', 'HostName/IP: AES2-S8800/10.32.32.66', 'Server Offer Type: VIRTUAL_APPLIANCE', and 'SW Version: r5-2-2-105-0'. Below the header is a red navigation bar with 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'. The left sidebar contains a tree view with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Utilities, and Help. Under 'User Admin', the 'Add User' option is selected. The main content area is titled 'Add User' and contains a form with the following fields: * User Id (engage), * Common Name (engage), * Surname (engage), * User Password (masked with dots), * Confirm Password (masked with dots), Admin Note (text area), Avaya Role (None), Business Category (text area), Car License (text area), CM Home (text area), Cms Home (text area), CT User (Yes), Department Number (text area), and Display Name (text area). A note at the top of the form states: 'Fields marked with * can not be empty.'

6.9. Enable DMCC Unencrypted Port

Select **Networking > Ports** from the left pane, to display the **Portss** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below.

AVAYA **Application Enablement Services**
Management Console

Welcome: User craft
Last login: Fri Feb 4 15:00:25 2011 from 10.32.35.10
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r5-2-2-105-0

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

Enabled Disabled

☒ ☐

☒ ☐

☐ ☒

☒ ☐

☒ ☐

☐ ☒

☒ ☐

☒ ☐

☐ ☒

☐ ☒

☐ ☒

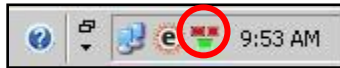
7. Configure TelStrat Engage

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

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

7.1. Administer VoIP Engine

From the Engage server, right-click on the **VoIP Engine Server** icon from the system tray shown below, and select **Config**.

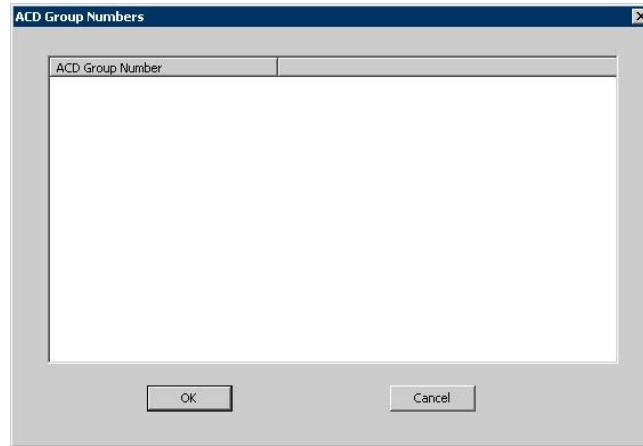


The **VoIP Configuration** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

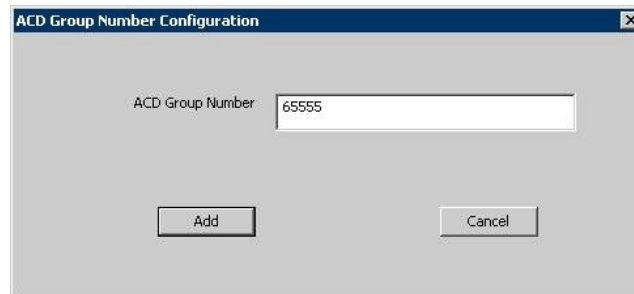
- **CTI Option:** “Avaya”
- **AES Server:** The IP address of the Application Enablement Services server.
- **TSAPI APP ID:** The Tlink name from **Section 6.7**.
- **User ID:** The Engage user credentials from **Section 6.8**.
- **DMCCPort:** The unencrypted DMCC server port from **Section 6.9**.
- **Password:** The Engage user credentials from **Section 6.8**.

7.2. Administer ACD Groups

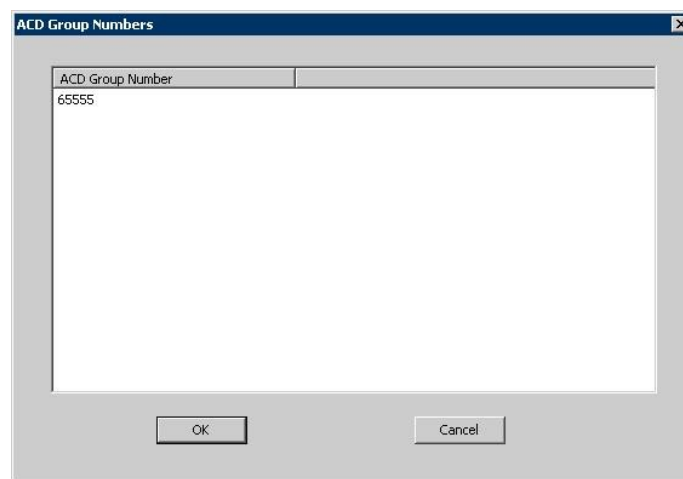
From the **VoIP Configuration** screen shown in **Section 7.1**, click on **ACD Groups** to display the **ACD Group Numbers** screen below. Right click in the empty pane and select **Add**.



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



Repeat this section to add all remaining skill groups.



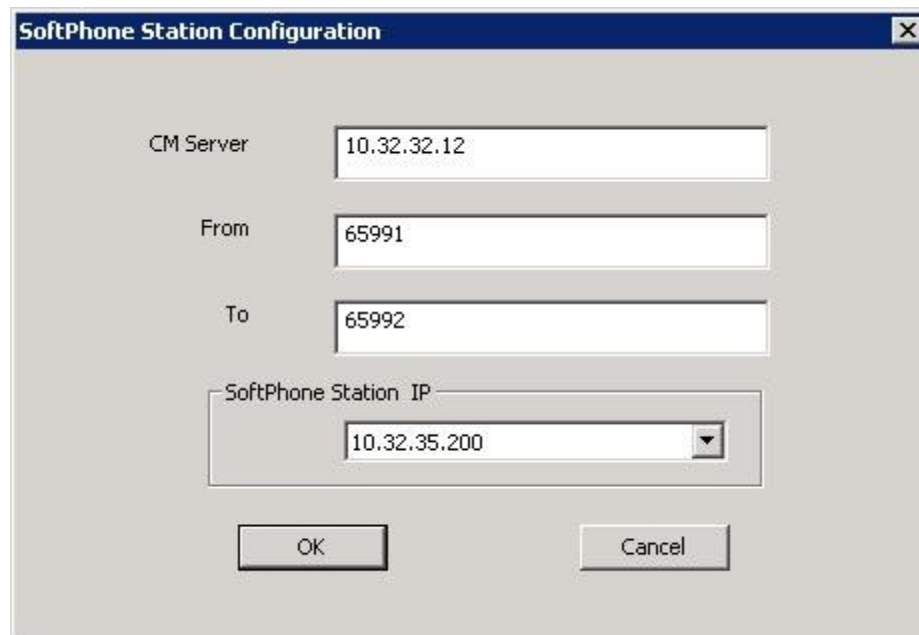
7.3. Administer SoftPhones

From the **VoIP Configuration** screen shown in **Section 7.1**, click on **SoftPhone** to display the **SoftPhone Station Configuration** screen.

For **CM Server**, enter the IP address of the H.323 gatekeeper from **Section 6.4**.

For **From** and **To**, enter the starting and ending extensions of the virtual IP softphones from **Section 5.4**.

Retain the default in the remaining fields.



The image shows a 'SoftPhone Station Configuration' dialog box with a blue title bar and a close button. It contains four input fields: 'CM Server' with the value '10.32.32.12', 'From' with '65991', 'To' with '65992', and 'SoftPhone Station IP' with a dropdown menu showing '10.32.35.200'. At the bottom are 'OK' and 'Cancel' buttons.

CM Server	10.32.32.12
From	65991
To	65992
SoftPhone Station IP	10.32.35.200

OK Cancel

7.4. Administer DevicePortMappings

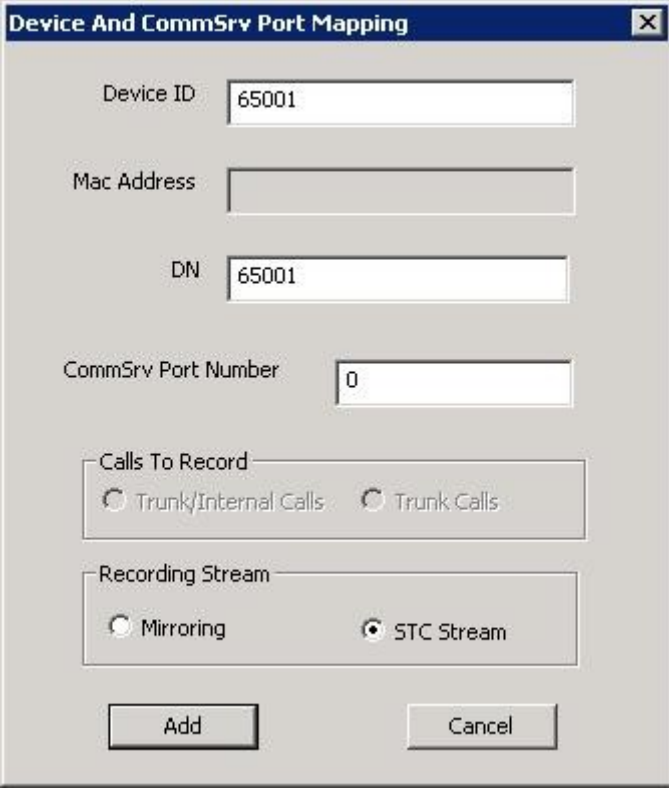
From the **VoIP Configuration** screen shown in **Section 7.1**, right-click in the empty pane and select **ADD**. The **Device AndCommSrv Port Mapping** screen is displayed.

For **Device ID**, enter the first agent telephone extension from **Section 3**.

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

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

Retain the default in the remaining fields.



The image shows a dialog box titled "Device And CommSrv Port Mapping". It contains several input fields and radio button groups. The "Device ID" field is filled with "65001". The "Mac Address" field is empty. The "DN" field is filled with "65001". The "CommSrv Port Number" field is filled with "0". There are two radio button groups: "Calls To Record" with options "Trunk/Internal Calls" and "Trunk Calls", and "Recording Stream" with options "Mirroring" and "STC Stream". At the bottom, there are "Add" and "Cancel" buttons.

Device ID	65001
Mac Address	
DN	65001
CommSrv Port Number	0
Calls To Record	<input type="radio"/> Trunk/Internal Calls <input type="radio"/> Trunk Calls
Recording Stream	<input type="radio"/> Mirroring <input checked="" type="radio"/> STC Stream
<input type="button" value="Add"/> <input type="button" value="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 trunk calls directly to the agent will have a prefix of “90884”, as shown below.

VoIP Configuration

Avaya

CTI Option: Avaya

AES Server: 10.32.32.66

DMCC Port: 4721

TSAPI APP ID: AVAYA#CM8800#

Recording Board ID: 2300

User ID: engage

Password: xxxxxxxx

Calls To Record:
☒ All Trunk/Internal Calls
☐ All Trunk Calls
☐ Calls Selected By DN

SoftPhone OnDemand
SIP/H.323 ACD Groups

Port Mapping

	Recording Channel	Device ID	Mac Address	DN	Record With	Trunk/Internal C
000		65001		65001	STC Stream	Trunk/Internal
000		65001		9088465001	STC Stream	Trunk/Internal
001		65002		9088465002	STC Stream	Trunk/Internal
001		65002		65002	STC Stream	Trunk/Internal

OK Cancel

8. 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, and TelStrat Engage.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the “status aescvscsti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.3**, as shown below.

```
statusaescvscsti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	AES2-S8800	established	39	47

Verify the registration status of the virtual softphones by using the “list registered-ip-stations” command. Verify that all extensions from **Section 5.4** are displayed, as shown below.

```
list registered-ip-stations
```

REGISTERED IP STATIONS						
Station Ext	Set	Type/	Prod ID/	TCP	Station IP Address/	
orOrig Port	Net	Rgn	Release	Skt	Gatekeeper	IP Address
65001	1616	IP_Phone	10.32.35.101			
	1		1.3000		10.32.32.12	
65002	1608	IP_Phone	10.32.35.102			
	1		1.3000		10.32.32.12	
65991	4620	IP_API_A	y	10.32.32.66		
	1	3.2040		10.32.32.12		
65992	4620	IP_API_A	y	10.32.32.66		
	1	3.2040		10.32.32.12		

8.2. 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.

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. The left navigation pane shows a tree structure with "Status" expanded, leading to "Status and Control", and finally "TSAPI Service Summary". The main content area is titled "TSAPI Link Details" and includes a refresh interval setting (60 seconds). Below this is a table with columns: Link, Switch Name, Switch CTI Link ID, Status, Since, State, Switch Version, Associations, Msgs to Switch, Msgs from Switch, and Msgs Period. A single row is shown with the status "Talking". At the bottom, there are buttons for "Online" and "Offline", and a section for service-wide information with buttons for "TSAPI Service Status", "TLink Status", and "User Status".

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	CM8800	1	Talking	Thu Feb 3 10:53:58 2011	Online	16	3	47	39	30

Verify the status of the DMCC link by selecting **Status > Status and Control > DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed. In the lower portion of the screen, verify that the **User** column shows an active session with the Engage user name from **Section 6.8**, and that the **# of Associated Devices** column reflects the number of virtual softphones from **Section 5.4**.

Application Enablement Services
Management Console

Welcome: User craft
 Last login: Fri Feb 4 10:04:42 2011 from 10.32.35.10
 HostName/IP: AES2-S8800/10.32.32.66
 Server Offer Type: VIRTUAL_APPLIANCE
 SW Version: r5-2-2-105-0

Status | Status and Control | DMCC 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

DMCC Service Summary - Session Summary

☐ Enable page refresh every seconds

Session Summary [Device Summary](#)
 Generated on Fri Feb 04 12:19:03 EST 2011
 Service Uptime: 1 days, 1 hours 24 minutes
 Number of Active Sessions: 1
 Number of Sessions Created Since Service Boot: 12
 Number of Existing Devices: 2
 Number of Devices Created Since Service Boot: 4

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	8F74A58E3C4CB3EB6 B8E41E98850031B-11	engage	Engage	10.32.35.200	XML Unencrypted	2

8.3. Verify TelStrat Engage

Log an agent into 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.

The **Engage: Logon Dialog** screen is displayed. Enter the appropriate credentials.

Engage: Logon Dialog

TelStrat Engage

UserID

Password

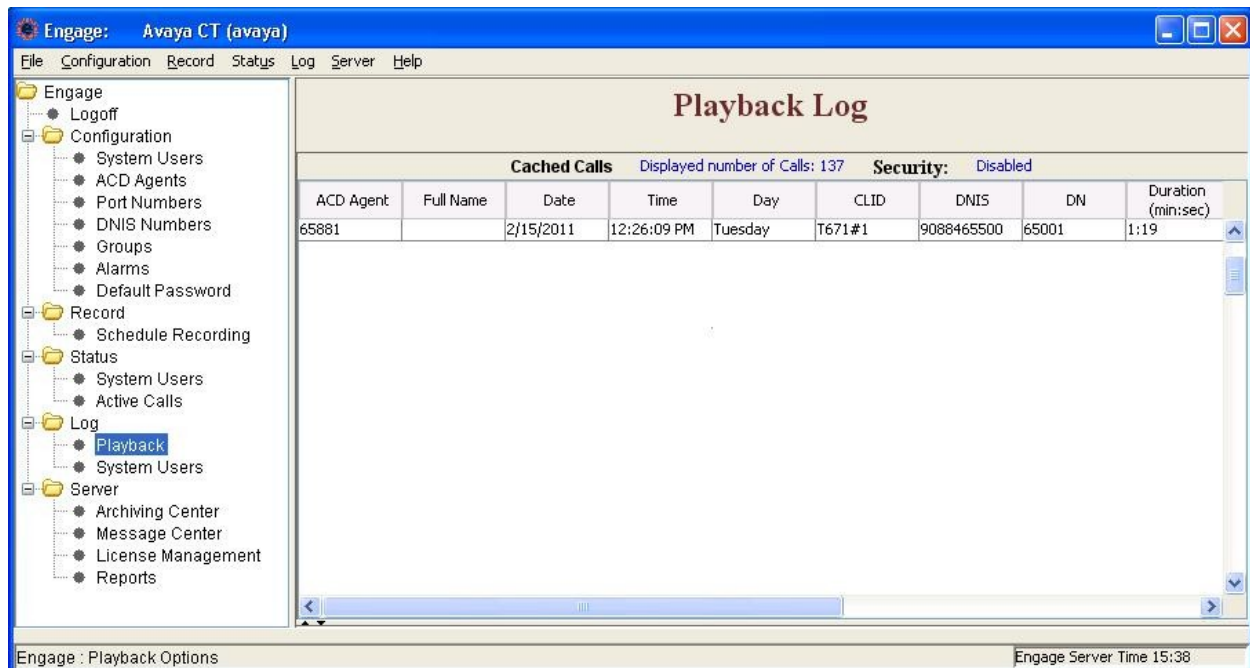
Server Name

☐ Windows Integrated Logon

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 is played back.



9. 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 with TSAPI and DMCC. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at <http://support.avaya.com>.
2. *Avaya Aura™ Application Enablement Services Administration and Maintenance Guide*, Release 5.2, Document ID 02-300357, Issue 11, November 2009, available at <http://support.avaya.com>.
3. *Engage Contact Center Suite Installation Guide*, Product Release 3.3, January 2011, available on the installation CD.
4. *Engage Contact Center System Administration Guide*, Product Release 3.3, January 2011, available on the installation CD.

©2011 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.