



Avaya Solution & Interoperability Test Lab

Application Notes for TelStrat Engage with Avaya Aura® Communication Manager Using Avaya Aura® Application Enablement Services – 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. TelStrat Engage is a call recording solution. In the compliance testing, TelStrat Engage used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent telephone 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. TelStrat Engage is a call recording solution. In the compliance testing, TelStrat Engage used the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor skill groups and agent telephone 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 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 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 TelStrat Engage application, the application automatically queries for the skill group and agent telephone extensions and requests monitoring using Avaya 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.
- 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.
- The DMCC port is required to be configured even though the integration does not use the DMCC API.

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

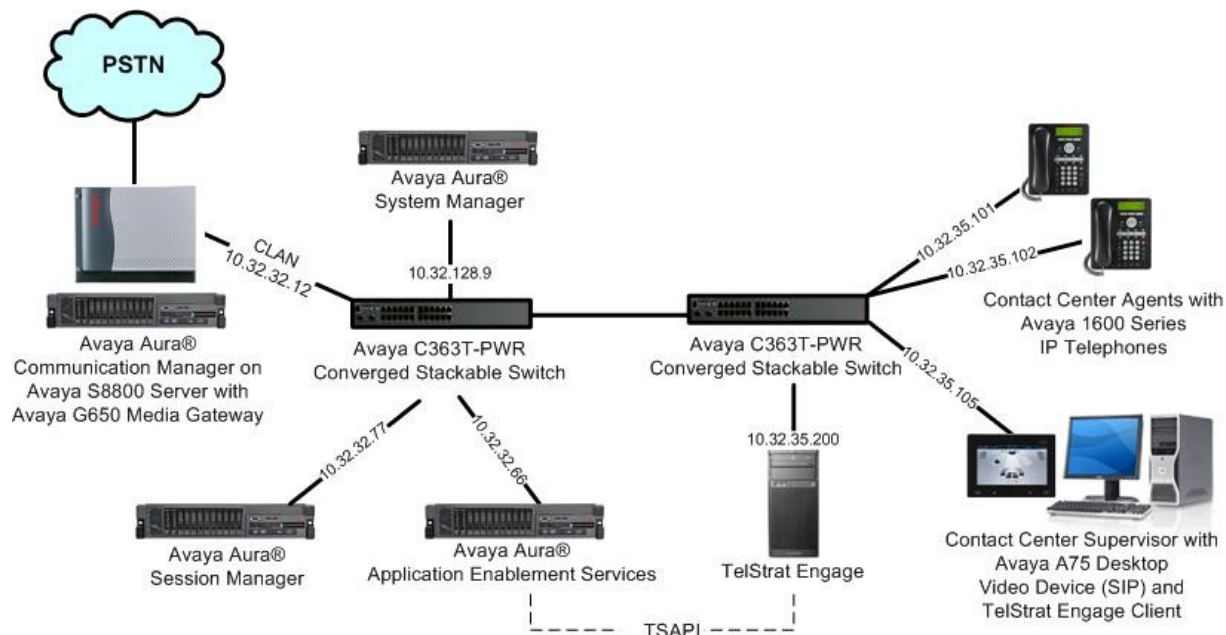
In the compliance testing, the RTP streams for agents with Avaya IP Telephones were mirrored from the layer 2 switch, and replicated over to TelStrat Engage.

TelStrat Engage also 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 addition, the port mirroring of the layer 2 switch is also outside the scope of these Application Notes and will not be described. The Avaya Aura® System Manager and Avaya Aura® Session Manager were used in the configuration to support the Avaya SIP endpoint.

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 (R016x.00.0.345.0-18246) |
| 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 |
| Avaya Aura® System Manager | 6.0 (6.0.0.0.556-3.0.6.1) |
| Avaya Aura® Session Manager | 6.0.1 (6.0.1.0.601016) |
| Avaya 1600 Series IP Telephones (H.323) | 1.3 |
| Avaya A175 Desktop Video Device (SIP) | 1.0.0 |
| TelStrat Engage on Windows 2003 Server with Service Pack 2 <ul style="list-style-type: none">Database ServerAvaya TSAPI Windows Client | 3.3.0.3 Microsoft SQL Server 2008 R2 5.2.1.483 |
| 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

5.1. Verify Communication Manager 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? 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? y      Cvg 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.

```
change ip-codec-set 1                                                  Page 1 of 2
                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt    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.

| | |
|------------------------------|-------------|
| add cti-link 1 | Page 1 of 3 |
| CTI LINK | |
| CTI Link: 1 | |
| Extension: 60100 | |
| Type: ADJ-IP | |
| Name: Engage CTI Link | COR: 1 |

6. Configure Avaya Aura® Application Enablement Services

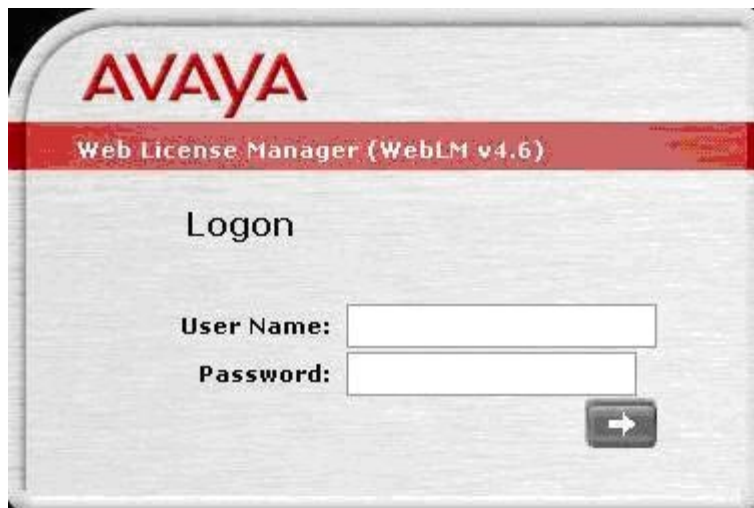
This section provides the procedures for configuring Avaya Aura® Application Enablement Services. The procedures include the following areas:

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

6.1. Verify TSAPI 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 **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 **TSAPI Simultaneous Users**, as shown below.

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

Install License

Licensed Products

▼ **APPL_ENAB**

▼ **Application_Enablement**

Uninstall License

Change Password

Server Properties

► **Manage Users**

Logout

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

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

License installed on: Apr 16, 2010 11:27:38 AM EDT

[View Peak Usage](#)

Licensed Features

| Feature (Keyword) | Expiration Date | Licensed | Acquired |
|---|-----------------|----------|----------|
| Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP) | permanent | 1000 | 0 |
| Device Media and Call Control (VALUE_AES_DMCC_DMC) | permanent | 100 | 0 |
| DLG (VALUE_AES_DLG) | permanent | 16 | 0 |
| CVLAN ASAI (VALUE_AES_CVLAN_ASAI) | permanent | 16 | 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

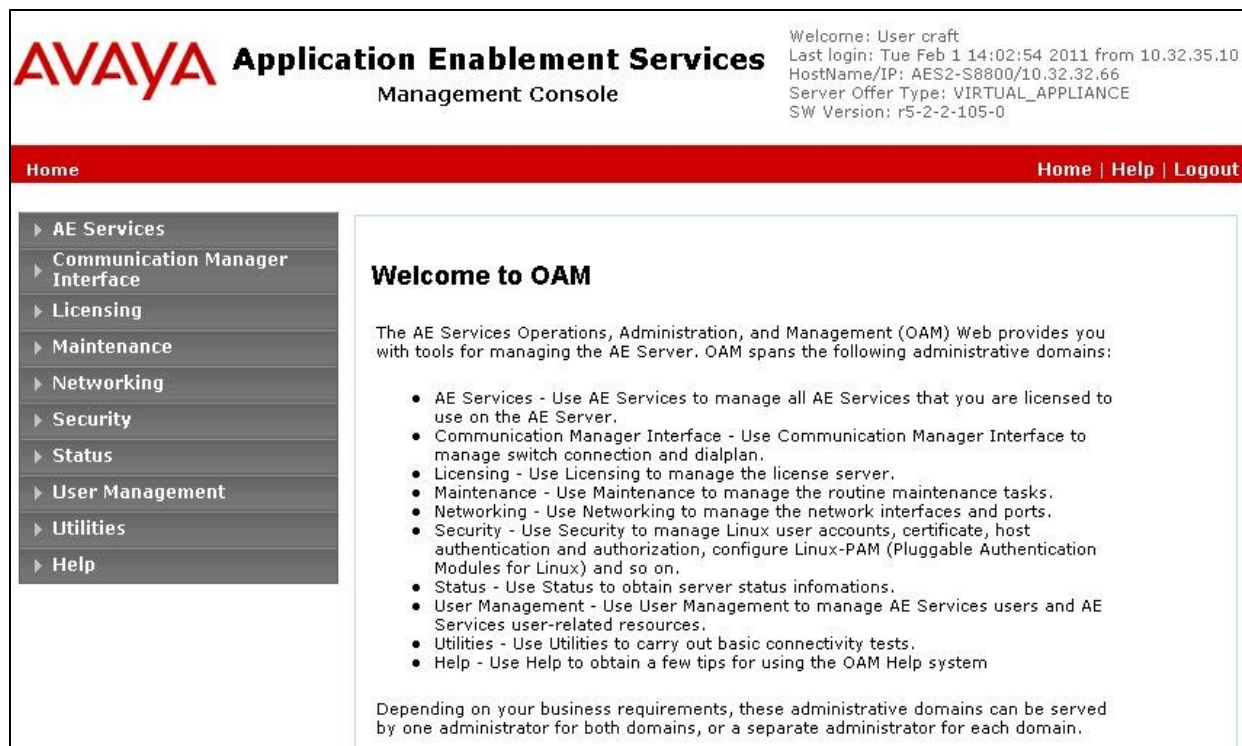
Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

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



The screenshot shows the login page of the AVAYA Application Enablement Services Management Console. At the top, the AVAYA logo is in red, followed by the text "Application Enablement Services" and "Management Console". A red horizontal bar contains a "Help" link. Below this is a gray box with the text "Please login here:". Inside the box are two input fields: "Username" and "Password", each followed by a text input field. Below the password field is a "Login" button. At the bottom of the page, a red horizontal bar contains the copyright notice "© 2009 Avaya, Inc. All Rights Reserved."

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



The screenshot shows the "Welcome to OAM" screen of the AVAYA Application Enablement Services Management Console. The top header includes the AVAYA logo, the text "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 horizontal bar with "Home" on the left and "Home | Help | Logout" on the right. On the left side, there is a vertical menu with the following items: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains the following text: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list of domains and their functions. At the bottom, it states: "Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain."

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

[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 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 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**.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top header includes the AVAYA logo, the title "Application Enablement Services Management Console", and a welcome message for "User craft" with login details. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected and "TSAPI Links" highlighted. 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 "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**.

The screenshot shows the "Add TSAPI Links" screen in the AVAYA Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot. The main content area is titled "Add TSAPI Links" and contains a form with the following fields: "Link" (set to 1), "Switch Connection" (set to CM8800), "Switch CTI Link Number" (set to 1), "ASAI Link Version" (set to 4), and "Security" (set to Unencrypted). At the bottom of 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 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'. It contains two checkboxes: 'Enable SDB for DMCC Service' (checked) and 'Enable SDB TSAPI Service, JTAPI and Telephony Service' (unchecked). Below these is an 'Apply Changes' button. The top right of the console displays user information: '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'.

6.5. 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'. It contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, with 'TSAPI Service' checked. Below the table is a note: 'For status on actual services, please use [Status and Control](#)'. At the bottom are buttons for 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'. The top right of the console displays the same user information as the previous screenshot.

| 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 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 user information: "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", and "SW Version: r5-2-2-105-0". A red navigation bar contains "Security | Security Database | Tlinks" and "Home | Help | Logout". The left sidebar shows a tree view with "Security" expanded, listing "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), "Control", "CTI Users", "Devices", "Device Groups", and "Tlinks" (highlighted). The main content area, titled "Tlinks", shows a "Tlink Name" field with a green status icon and the value "AVAYA#CM8800#CSTA#AES2-S8800". Below this are "Edit Tlink" and "Delete Tlink" buttons.

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

AVAYA **Application Enablement Services**
Management Console

Welcome: User craft
Last login: 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

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 Id | <input type="text" value="engage"/> |
| * Common Name | <input type="text" value="engage"/> |
| * Surname | <input type="text" value="engage"/> |
| * User Password | <input type="password" value="....."/> |
| * Confirm Password | <input type="password" value="....."/> |
| Admin Note | <input type="text"/> |
| Avaya Role | <input type="text" value="None"/> |
| Business Category | <input type="text"/> |
| Car License | <input type="text"/> |
| CM Home | <input type="text"/> |
| Css Home | <input type="text"/> |
| CT User | <input type="text" value="Yes"/> |
| Department Number | <input type="text"/> |
| Display Name | <input type="text"/> |

6.8. Enable DMCC Unencrypted Port

Select **Networking > Ports** from the left pane, to display the **Ports** 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

| | | | Enabled | Disabled |
|----------------------|-----------------------------------|--|----------------------------------|-----------------------|
| Unencrypted TCP Port | 9999 | | <input checked="" type="radio"/> | <input type="radio"/> |
| Encrypted TCP Port | <input type="text" value="9998"/> | | <input checked="" type="radio"/> | <input type="radio"/> |

DLG Port

| | TCP Port | |
|--|----------|--|
| | 5678 | |

TSAPI Ports

| | | | Enabled | Disabled |
|-------------------------|-----------------------------------|--|----------------------------------|-----------------------|
| TSAPI Service Port | 450 | | <input checked="" type="radio"/> | <input type="radio"/> |
| Local TLINK Ports | | | | |
| TCP Port Min | 1024 | | | |
| TCP Port Max | 1039 | | | |
| Unencrypted TLINK Ports | | | | |
| TCP Port Min | <input type="text" value="1050"/> | | | |
| TCP Port Max | <input type="text" value="1065"/> | | | |
| Encrypted TLINK Ports | | | | |
| TCP Port Min | <input type="text" value="1066"/> | | | |
| TCP Port Max | <input type="text" value="1081"/> | | | |

DMCC Server Ports

| | | | Enabled | Disabled |
|------------------|-----------------------------------|--|----------------------------------|----------------------------------|
| Unencrypted Port | <input type="text" value="4721"/> | | <input checked="" type="radio"/> | <input type="radio"/> |
| Encrypted Port | <input type="text" value="4722"/> | | <input checked="" type="radio"/> | <input type="radio"/> |
| TR/87 Port | <input type="text" value="4723"/> | | <input type="radio"/> | <input checked="" type="radio"/> |

7. Configure Avaya IP Telephones

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

7.1. Obtain MAC Address

From the Avaya IP Telephone, press the **MENU** button to display the **Menu** screen (not shown).

From the **Menu** 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 TelStrat Engage. Repeat this section for all Avaya IP Telephones used by the agents in **Section 3**. In the compliance testing, the MAC addresses associated with the two agent telephones were “001B4F086158” and “00040DEC9384”.

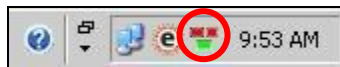
8. Configure TelStrat Engage

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

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

8.1. Administer VoIP Engine

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



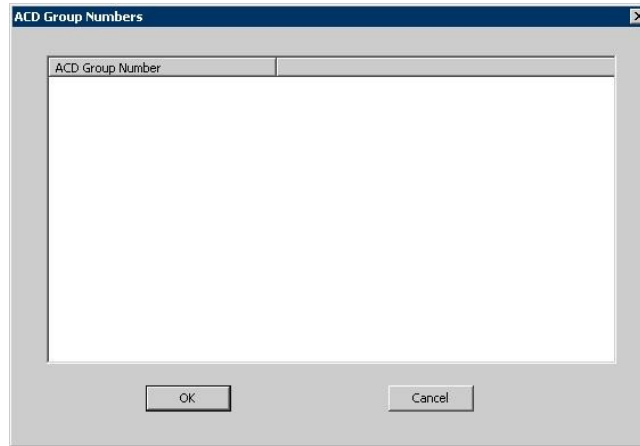
The **VoIP Configuration** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **CTI Option:** “Avaya”
- **AES Server:** The IP address of the Application Enablement Services server.
- **TSAPI APP ID:** The Tlink name from **Section 6.6**.
- **User ID:** The Engage user credentials from **Section 6.7**.
- **DMCC Port:** The unencrypted DMCC server port from **Section 6.8**.
- **Password:** The Engage user credentials from **Section 6.7**.

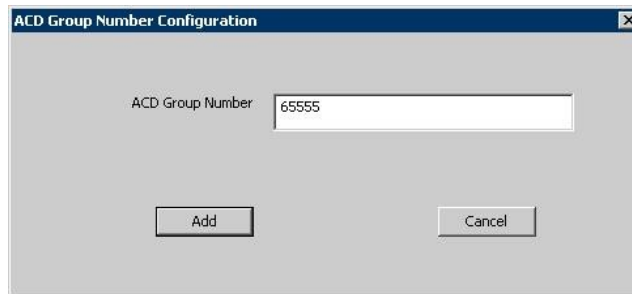
A screenshot of the 'VoIP Configuration' dialog box. The title bar says 'VoIP Configuration'. The 'Avaya' tab is selected. The 'CTI Option' is a dropdown menu showing 'Avaya'. The 'AES Server' is a text box with '10.32.32.66'. The 'DMCC Port' is a text box with '4721'. The 'TSAPI APP ID' is a text box with 'AVAYA#CM8800#'. The 'Recording Board ID' is a text box with '2300'. The 'User ID' is a text box with 'engage'. The 'Password' is a text box with masked characters. Below these fields are three radio buttons for 'Calls To Record': 'All Trunk/Internal Calls' (selected), 'All Trunk Calls', and 'Calls Selected By DN'. To the right of these are four buttons: 'SoftPhone', 'OnDemand', 'SIP/H.323', and 'ACD Groups'. At the bottom is a 'Port Mapping' section with a table header: 'Recording Channel', 'Device ID', 'Mac Address', 'DN', 'Record With', and 'Trunk/Internal C'. The table body is empty.

8.2. Administer ACD Groups

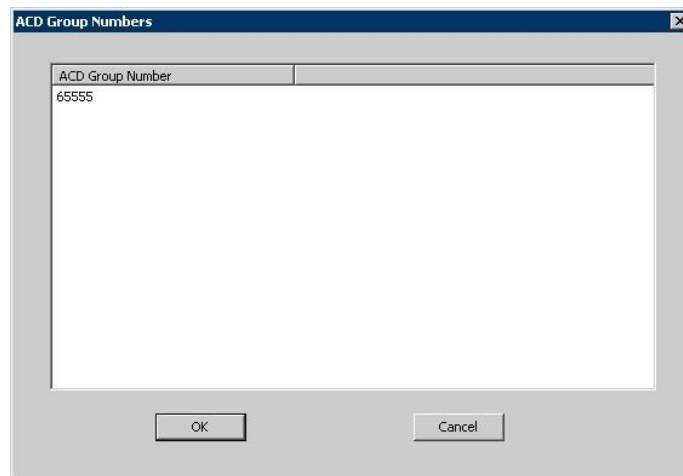
From the **VoIP Configuration** screen shown in **Section 8.1**, click on **ACD Groups** to display the **ACD Group Numbers** screen below. Right click in the empty pane and select **Add**.



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.



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 telephone extension from **Section 3**. Select the **Mirroring** radio button to enable the **Mac Address** field. For **Mac Address**, enter the MAC address of the first agent telephone from **Section 7.1**. For **CommSrv Port Number**, enter an available port, which begins with “0”.

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.



Device And CommSrv Port Mapping

Device ID: 65001

Mac Address: 001B4F086158

DN: 65001

CommSrv Port Number: 0

Calls To Record:

- ☐ Trunk/Internal Calls
- ☐ Trunk Calls

Recording Stream:

- ☒ Mirroring
- ☐ STC Stream

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 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 Calls |
|-----|-------------------|-----------|--------------|------------|-------------|----------------------|
| 001 | | 65002 | 00040DEC9384 | 65002 | Mirroring | Trunk/Internal |
| 001 | | 65002 | 00040DEC9384 | 9088465002 | Mirroring | Trunk/Internal |
| 000 | | 65001 | 001B4F086158 | 65001 | Mirroring | Trunk/Internal |
| 000 | | 65001 | 001B4F086158 | 9088465001 | Mirroring | Trunk/Internal |

OK 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, and TelStrat 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 5.3**, 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 | AES2-S8800 | established | 56 | 45 |

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 craft
Last login: Thu Feb 3 14:59:02 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 | TSAPI Service Summary

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ **TSAPI Service Summary**

TSAPI Link Details

☐ Enable page refresh every 60 seconds

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

Online Offline

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

TSAPI Service Status TLink Status User Status

9.3. 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.



The image shows a Windows-style dialog box titled "Engage: Logon Dialog". It has a blue title bar with a close button. The main area is light gray and contains the text "TelStrat Engage" in a large, dark red font. Below this, there are three input fields: "UserID", "Password", and "Server Name". Each field has a small icon to its left. Below the input fields, there is a checkbox labeled "Windows Integrated Logon". At the bottom, there are two buttons: "OK" and "Cancel".

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.

Engage: Avaya CT (avaya)

File Configuration Record Status Log Server Help

Engage

- Logoff
- Configuration
 - System Users
 - ACD Agents
 - Port Numbers
 - DNIS Numbers
 - Groups
 - Alarms
 - Default Password
- Record
 - Schedule Recording
- Status
 - System Users
 - Active Calls
- Log
 - Playback**
 - System Users
- Server
 - Archiving Center
 - Message Center
 - License Management
 - Reports

Playback Log

Cached Calls Number of Calls: 17 **Security:** Disabled

| ACD Agent | Full Name | Date | Time | Day | CLID | DNIS | DN | Duration (min:sec) |
|-----------|-----------|----------|------------|--------|--------|-------|-------|--------------------|
| 65881 | | 2/4/2011 | 8:57:06 AM | Friday | T686#1 | 65500 | 65001 | 1:03 |

Engage : Playback Options Engage Server Time 08:58

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. 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 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.