



Application Notes for TelStrat Engage with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 and Avaya IP Deskphones for On-Demand Recording – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TelStrat Engage to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 and Avaya IP Deskphones for on-demand recording. 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 stations on Avaya Aura® Communication Manager, the port mirroring method to capture the media associated with the monitored agents with Avaya 96xx IP Deskphones for call recording, and the Web Browser interface from the Avaya 96xx IP Deskphones to activate and deactivate on-demand 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 and Avaya Aura® Application Enablement Services 6.3 and Avaya IP Deskphones for on-demand recording. 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 stations on Avaya Aura® Communication Manager, the port mirroring method to capture the media associated with the monitored agents with Avaya 96xx IP Deskphones for call recording, and the Web Browser interface from the Avaya 96xx IP Deskphones to activate and deactivate on-demand call recording.

The TSAPI interface is used by TelStrat Engage to monitor skill groups and agent stations on Avaya Aura® Communication Manager. When there is an active call at 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.

The Web Browser interface is used by Telstrat Engage to provide activation and deactivation of call recording options via the agents' Avaya 96xx IP Deskphones.

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 requests monitoring on skill groups and agent stations and performs device queries 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, and with manual actions to activate/deactivate saving of conversations. Necessary user actions such as hold and resume 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 use of Engage logs for proper message exchanges, and use of the Engage Client application for proper logging and playback of 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 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, resume, multiple calls, multiple agents, conference, and transfer.
- Proper display of browser pages and begin/end/cancel of call recordings from the agent telephones.

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

2.2. Test Results

All test cases were executed, and the following were observations on Engage:

- In the blind conference scenario, there is at most one recording entry for the conference-from agent, and the agent needs to initiate the Conversation Save during the initial conversation with the customer, as the option is not provided after the conference action completes.
- In the attended transfer and conference scenarios, there are at most two recording entries for the from-agent, and the from-agent needs to select Conversation Save during the private conversation with the to-agent if that conversation is desired to be saved.
- With the phone refresh timer set to four seconds, it can take up to four seconds for the proper recording option screen to appear on the phone. Furthermore, the initial access to the Web Browser page after a link interruption may display the “Browser page cannot be rendered” message. The workaround is to press the HOME or MENU button.
- 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

3. Reference Configuration

Engage has an Engage Client application that can be used to review and playback the call recordings. In the compliance testing, Engage Client 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, Application Enablement Services, System Manager, Session Manager, 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, Engage monitored the skill groups and agent station extensions shown in the table below.

Device Type	Extension
VDN	48001, 48002
Skill Group	48101, 48102
Supervisor	45000
Agent ID	45881, 45882
Agent Station	45001, 46002

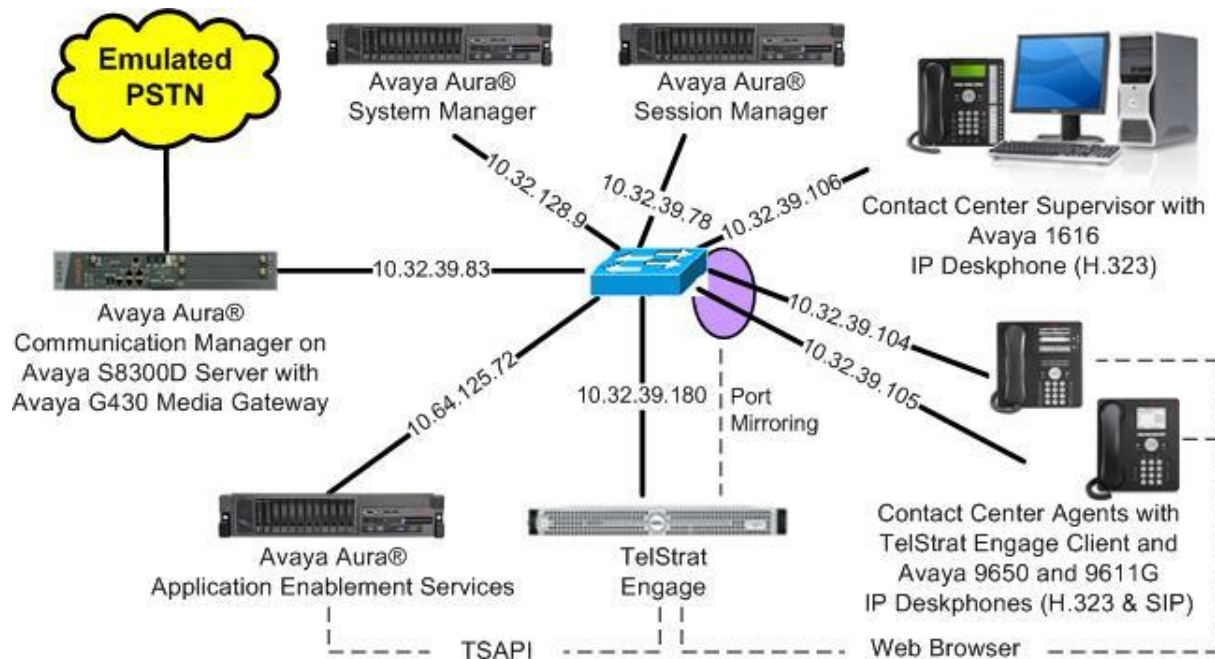


Figure 1: Compliance Testing Configuration

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	6.3.5 (R016x.03.0.124.0-21460) 6.3.5 (35.8.0)
Avaya Aura® Application Enablement Services	6.3.1 (6.3.1.0.19-0)
Avaya Aura® Session Manager	6.3.7
Avaya Aura® System Manager	6.3.7
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9621G IP Deskphone (SIP)	6.3.1.22
Avaya 9650 IP Deskphone (H.323)	3.220A
TelStrat Engage on Windows 2008 Server Standard <ul style="list-style-type: none">• Microsoft SQL Server 2008• Avaya TSAPI Windows Client (csta32.dll)	3.6.1.39 2008 SP1 R2 6.3.0.334
TelStrat Engage Client on Windows 7 Enterprise	3.6.1.39 2008 SP1

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 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)?	n	Authorization Codes?	y
Analog Trunk Incoming Call ID?	y	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n
ARS?	y	Computer Telephony Adjunct Links?	y
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	y
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	y
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y
ATMS?	y		
Attendant Vectoring?	y		

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			
Extension: 40001			
Type: ADJ-IP			
Name: AES CTI Link			
COR: 1			

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" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below the input fields are "Login" and "Reset" buttons. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2013 Avaya Inc. All Rights Reserved." is displayed.

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

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 sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the 'Welcome to OAM' screen, which provides an overview of the OAM Web and lists administrative domains such as AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also mentions that these domains can be served by one administrator for all domains or a separate administrator for each domain.

Welcome: User
Last login: Wed Jun 25 07:35:37 2014 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_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Wed Jun 25 07:36:10 MDT 2014
HA Status: Not Configured

Home | Help | Logout

Home

AE Services
Communication Manager Interface
High Availability
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.
- High Availability - Use High Availability to manage AE Services HA.
- 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.

The screenshot shows the Avaya Application Enablement Services Management Console with the 'Licensing' section selected in the left sidebar. The main content area displays the 'Licensing' screen, which provides instructions on how to set up and maintain the WebLM, including the need to use the following: WebLM Server Address, WebLM Server Access, and Reserved Licenses. It also mentions that if you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following: Reserved Licenses.

Welcome: User
Last login: Wed Jun 25 07:35:37 2014 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_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Wed Jun 25 07:36:10 MDT 2014
HA Status: Not Configured

Home | Help | Logout

Licensing

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking

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 **Application Enablement (CTI)** screen in the right pane.

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


Web License Manager (WebLM v6.3)
Help | About | Change Password

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 7:07:47 PM -04:00
License File Host IDs: 00-16-3E-48-ED-82

Licensed Features

10 Items Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestricted DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,, CCE_001, AdvancedUnrestricted, DMCUnrestricted; CSI_001, AdvancedUnrestricted, DMCUnrestricted; CSI_001, AdvancedUnrestricted, DMCUnrestricted; AVA_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

6.3. Administer TSAPI Link

To administer a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the Avaya Management Console interface. 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 the hierarchy: AE Services > TSAPI > TSAPI Links. The main content area displays a table of existing TSAPI Links. The table has five columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. There is one entry with Link 1, Switch Connection S8800, Switch CTI Link # 2, ASAI Link Version 6, and Security Both. 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	6	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.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Management Console. The left navigation pane is the same as the previous screenshot. The main content area has a form with the following fields: Link (set to 2), Switch Connection (set to S8300D), Switch CTI Link Number (set to 1), ASAI Link Version (set to 6), and Security (set to Unencrypted). There are "Apply Changes" and "Cancel Changes" buttons at the bottom of the form.

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.

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 "Control" selected under "Security Database". The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

Welcome: User
Last login: Wed Jun 25 07:35:37 2014 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_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Wed Jun 25 07:36:10 MDT 2014
HA Status: Not Configured

Security | Security Database | Control

Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

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

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**.



Application Enablement Services
Management Console

Welcome: User
Last login: Wed Jun 25 07:35:37 2014 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_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Wed Jun 25 07:36:10 MDT 2014
HA Status: Not Configured

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ 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

6.6. 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#AES_125_72”. 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 main navigation bar shows "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", lists three Tlink names: "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 visible below the list.

Welcome: User
Last login: Wed Jun 25 07:35:37 2014 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_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Wed Jun 25 07:36:10 MDT 2014
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Wed Jun 25 07:35:37 2014 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_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Wed Jun 25 07:36:10 MDT 2014
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

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

Enterprise Handle

Given Name

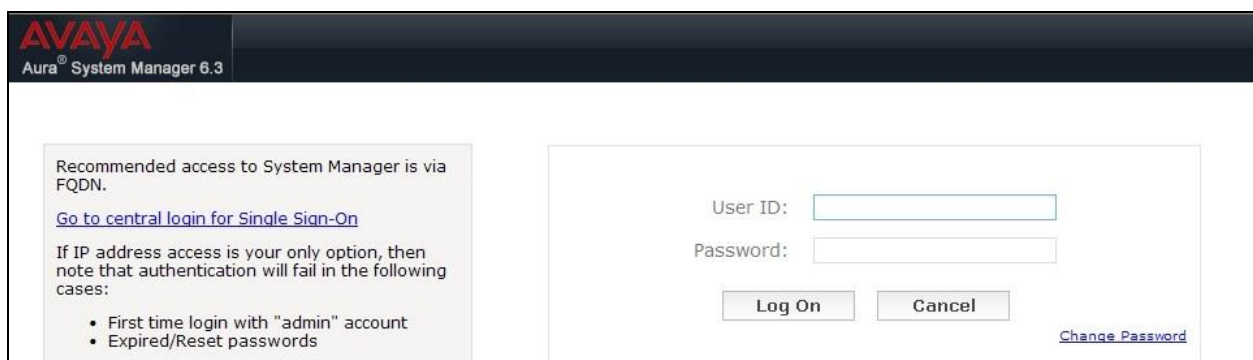
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

7.1. Launch System Manager

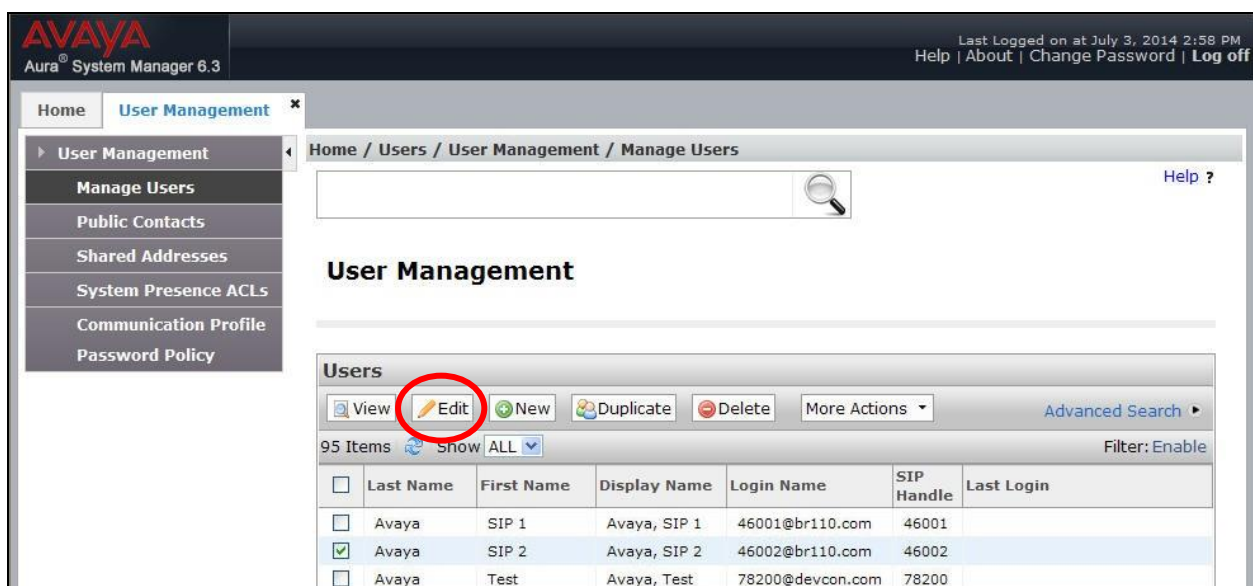
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



The screenshot shows the Avaya Aura System Manager 6.3 login interface. On the left, a text box provides instructions: "Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: First time login with 'admin' account, Expired/Reset passwords". On the right, there is a login form with fields for "User ID:" and "Password:", a "Log On" button, a "Cancel" button, and a "Change Password" link.

7.2. Administer Users

In the subsequent screen (not shown), select **Users** → **User Management** → **Manage Users** to display the **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “46002”, and click **Edit**.



The screenshot displays the Avaya Aura System Manager 6.3 User Management interface. The top navigation bar includes "Home", "User Management", and a breadcrumb trail: "Home / Users / User Management / Manage Users". A left sidebar lists various management options, with "Manage Users" selected. The main content area, titled "User Management", shows a table of users. The "Edit" button in the toolbar is circled in red. The table lists three users: Avaya SIP 1, Avaya SIP 2 (selected), and Avaya Test.

	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
<input type="checkbox"/>	Avaya	SIP 1	Avaya, SIP 1	46001@br110.com	46001	
<input checked="" type="checkbox"/>	Avaya	SIP 2	Avaya, SIP 2	46002@br110.com	46002	
<input type="checkbox"/>	Avaya	Test	Avaya, Test	78200@devcon.com	78200	

The **User Profile Edit** screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.

AVAYA
Aura® System Manager 6.3

Last Logged on at July 3, 2014 2:58 PM
Help | About | Change Password | Log off

Home User Management *
Home / Users / User Management / Manage Users

User Profile Edit: 46002@br110.com

Commit & Continue Commit Cancel

Identity * Communication Profile Membership Contacts

Communication Profile

Communication Profile Password: Edit

New Delete Done Cancel

Name

Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

New Edit Delete

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	46002	br110.com

Select : All, None

☒ Session Manager Profile

☐ Collaboration Environment Profile

☒ CM Endpoint Profile

* System BR110-G430-ES

* Profile Type Endpoint

Use Existing Endpoints ☐

* Extension 46002 Endpoint Editor

Template 9621SIPCC_DEFAULT_CM_6_3

Set Type 9621SIPCC

Security Code

The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

Repeat this section for all SIP agent users.

AVAYA
Aura® System Manager 6.3

Last Logged on at July 3, 2014 2:58 PM
Help | About | Change Password | Log off

Home User Management x

Home / Users / User Management / Manage Users

Edit Endpoint

Done Cancel

[Save As Template]

System: BR110-G430-ES Extension: 46002

Template: 9621SIPCC_DEFAULT_CM_6_3 Set Type: 9621SIPCC

Port: 500019 Security Code:

Name: Avaya, SIP 2

General Options (G) * Feature Options (F) Site Data (S)

Abbreviated Call Dialing (A) Enhanced Call Fwd (E) Button Assignment (B)

Group Membership (M)

* Class of Restriction (COR): 1 * Class Of Service (COS): 1

* Emergency Location Ext: 46002 * Message Lamp Ext.: 46002

* Tenant Number: 1

* SIP Trunk: Qaar Type of 3PCC Enabled: Avaya

Coverage Path 1: 1 Coverage Path 2:

Lock Message: ☐ Localized Display Name: Avaya, SIP 2

Multibyte Language: Not Applicable

*Required

Done Cancel

8. Configure Avaya IP Deskphones

This section provides the procedures for configuring 96xx IP Deskphones. The procedures include the following areas:

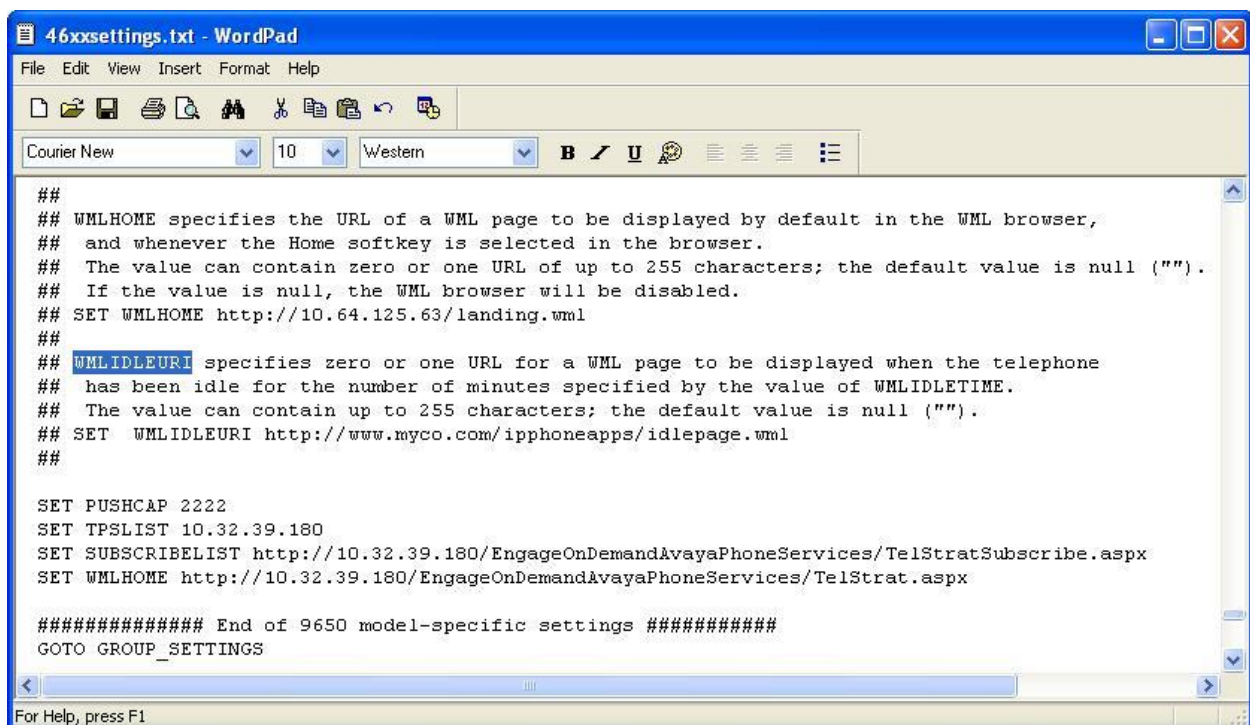
- Administer phone parameters
- Obtain MAC addresses
- Reboot telephones

8.1. Administer Phone Parameters

From the file server serving the 96xx IP Deskphones, locate the **46xxsettings.txt** file and open with the desired application such as WordPad. Navigate to the relevant phone parameters section, in this case **SETTINGS9650**.

Under the **WMLIDLEURI** subsection, set **PUSHCAP**, **TPSLIST**, **SUBSCRIBELIST**, and **WMLHOME** parameters as shown below, where “10.32.39.180” is the IP address of the Engage server running the Web Server component.

Repeat this section for all relevant 96xx IP Deskphone types. In the compliance testing, the 9650 and 9611G IP Deskphones were used for testing activation/deactivation of on-demand call recording.



```
##
## WMLHOME specifies the URL of a WML page to be displayed by default in the WML browser,
## and whenever the Home softkey is selected in the browser.
## The value can contain zero or one URL of up to 255 characters; the default value is null ("").
## If the value is null, the WML browser will be disabled.
## SET WMLHOME http://10.64.125.63/landing.wml
##
## WMLIDLEURI specifies zero or one URL for a WML page to be displayed when the telephone
## has been idle for the number of minutes specified by the value of WMLIDLETIME.
## The value can contain up to 255 characters; the default value is null ("").
## SET WMLIDLEURI http://www.myco.com/ipphoneapps/idlepage.wml
##

SET PUSHCAP 2222
SET TPSLIST 10.32.39.180
SET SUBSCRIBELIST http://10.32.39.180/EngageOnDemandAvayaPhoneServices/TelStratSubscribe.aspx
SET WMLHOME http://10.32.39.180/EngageOnDemandAvayaPhoneServices/TelStrat.aspx

##### End of 9650 model-specific settings #####
GOTO GROUP_SETTINGS
```

8.2. Obtain MAC Addresses

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 “00040DFA0FBB” and “2CF4C5F669AD”.

8.3. Reboot Telephones

After the Engage server has been configured in **Section 9**, manually reboot the 96xx IP Deskphones to pick up the new phone settings.

9. Configure TelStrat Engage

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

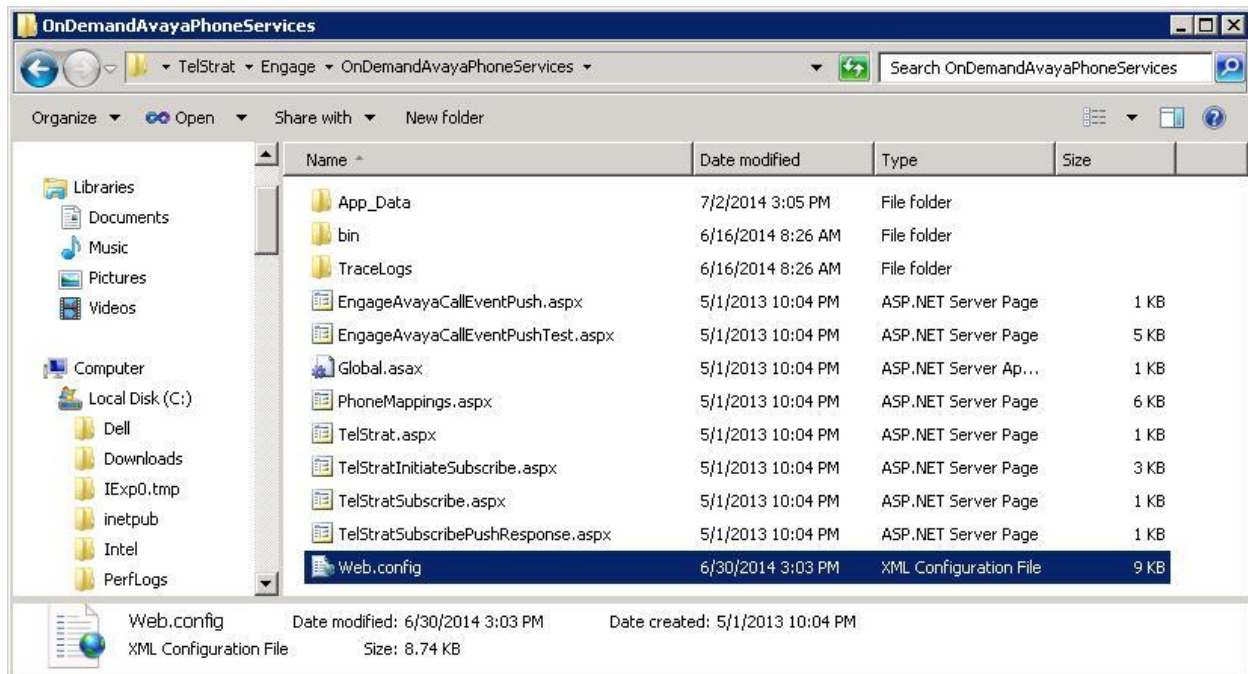
- Administer Web.config
- Launch VoIP engine
- Administer TSAPI
- Administer OnDemand
- Administer ACD groups
- Administer device port mappings

This section assumes the TSAPI client is already installed on the Engage server, along with the IP address of the Application Enablement Services server configured as part of installation.

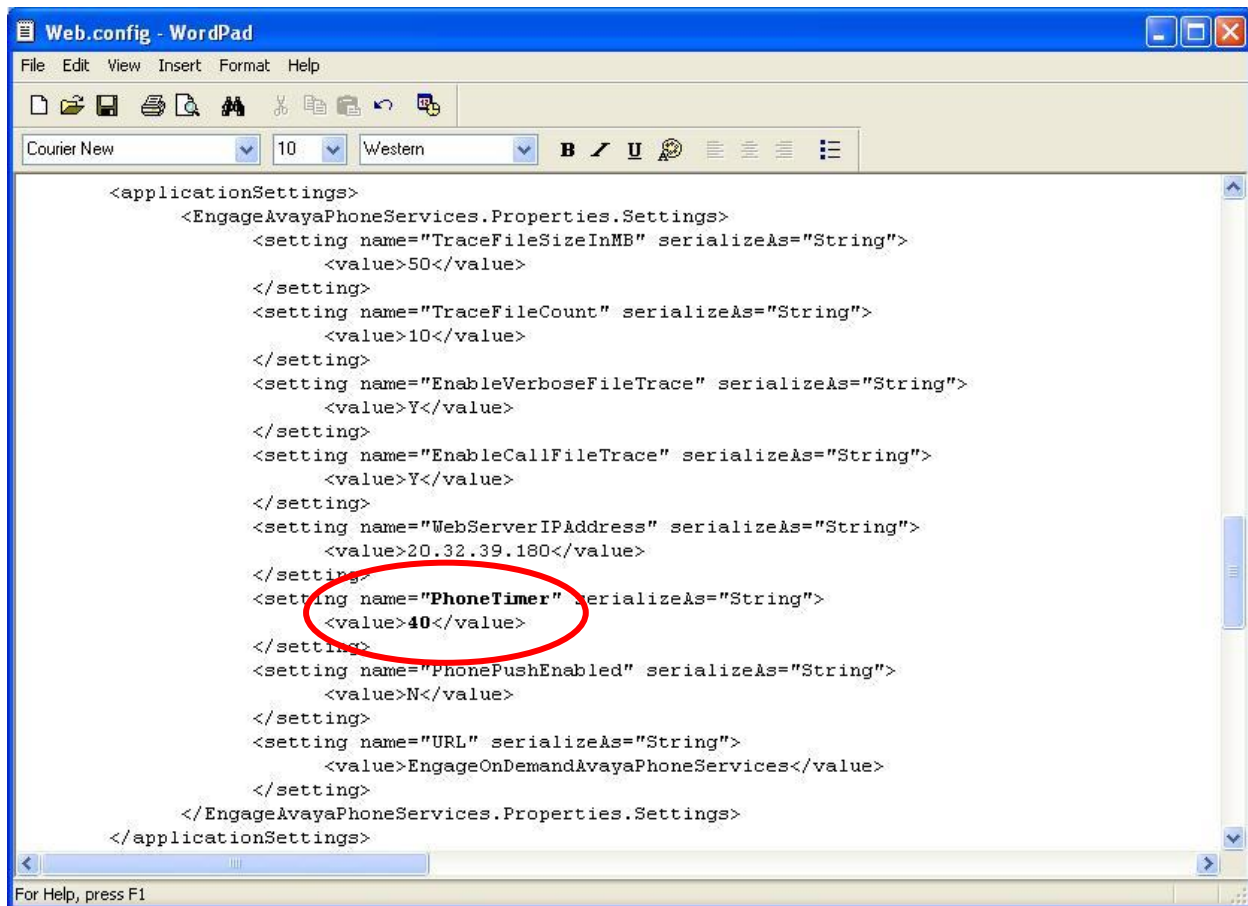
At the end of configuration, follow [4] to create the desired on-demand recording schedule for the agents.

9.1. Administer Web.config

From the Engage server, navigate to the **C:\Program Files (x86)\TelStrat\Engage\OnDemandAvayaPhoneServices** directory to locate the **Web.config** file shown below.



Open the **Web.config** file with the desired application. Scroll down to the **applicationSettings** subsection. For **PhoneTimer**, enter the desired value. In the compliance testing, the default **30** was changed to **40**, for better interoperability with the Avaya 9611G IP Deskphone.



9.2. 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**.



9.3. Administer TSAPI

The **VoIP Configuration** screen is displayed, along with the **Avaya TSAPI** tab, as shown below. 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**.

The screenshot shows the 'VoIP Configuration' window with the 'Avaya TSAPI' tab selected. The configuration fields are as follows:

- CTI Option:** A dropdown menu set to 'Avaya TSAPI'.
- AES Server:** A text field containing '10.64.125.72'.
- DMCC Port:** A text field containing '0'.
- TSAPI APP ID:** A text field containing 'AVAYA#S8300D#C'.
- Recording Board ID:** A text field containing '2300'.
- User ID:** A text field containing 'engage'.
- Password:** A text field with masked characters (dots).

Below the fields, there are two sections:

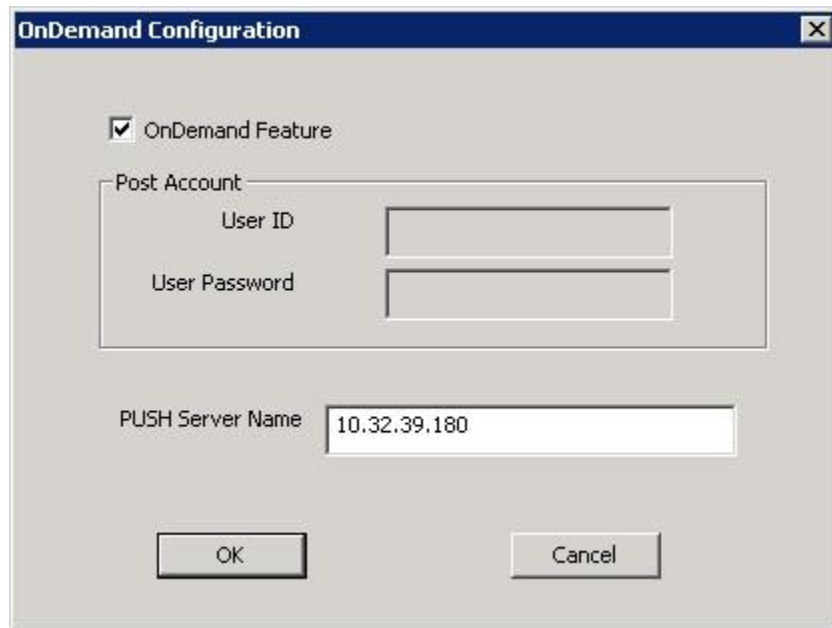
- Calls To Record:** A group box containing three radio buttons: 'All Trunk/Internal Calls' (selected), 'All Trunk Calls', and 'Calls Selected By DN'.
- Port Mapping:** A section containing four buttons: 'SoftPhone', 'OnDemand', 'SPAN Cfg', and 'ACD Groups'.

At the bottom, there is a table for 'Port Mapping' with the following headers: 'Recording Channel', 'Device ID', 'Mac Address', 'DN', 'Record With', and 'Trunk/Internal Calls'. The table body is currently empty.

9.4. Administer OnDemand

From the **VoIP Configuration** screen shown in **Section 9.3**, click on **OnDemand** to display the **OnDemand Configuration** screen below.

Check **OnDemand Feature**. For **PUSH Server Name**, enter the IP address of the Engage server, as shown below.

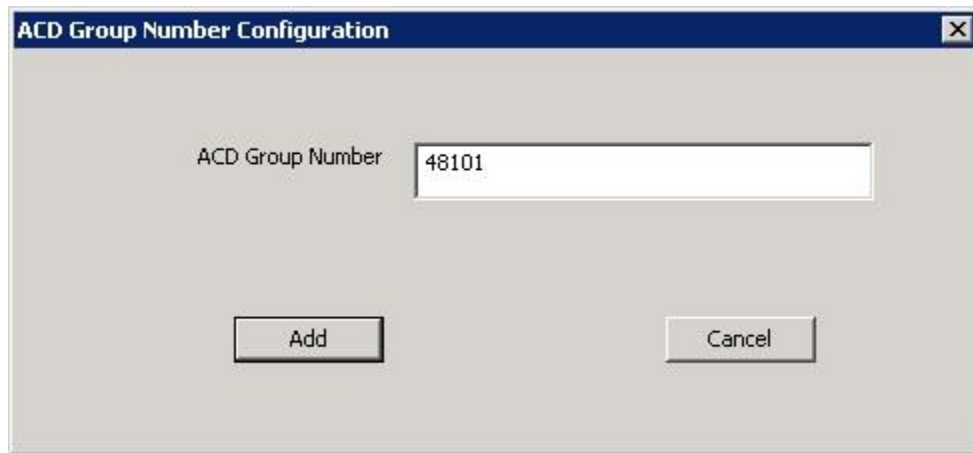


The image shows a dialog box titled "OnDemand Configuration". It has a blue title bar with a close button (X) in the top right corner. The main area is light gray. At the top, there is a checkbox labeled "OnDemand Feature" which is checked. Below this is a section titled "Post Account" enclosed in a rounded rectangle. Inside this section, there are two labels: "User ID" and "User Password", each followed by an empty text input field. Below the "Post Account" section, there is a label "PUSH Server Name" followed by a text input field containing the IP address "10.32.39.180". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

9.5. Administer ACD Groups

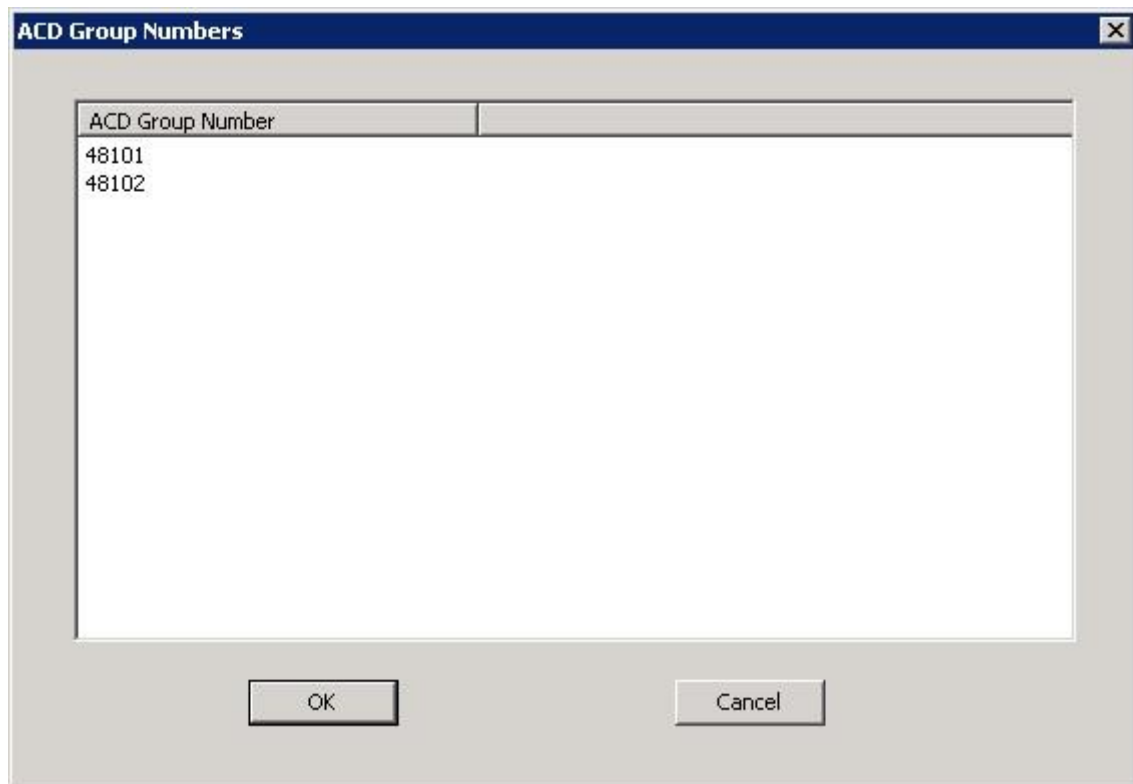
From the **VoIP Configuration** screen shown in **Section 9.3**, click on **ACD Groups** to display the **ACD Group Numbers** screen (not shown). Right click in the empty pane and select **Add**.

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



The screenshot 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 screenshot 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".

9.6. Administer Device Port Mappings

From the **VoIP Configuration** screen shown in **Section 9.3**, 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 8.2**.

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 **Recording Channel**, enter an available port, which begins with “0”.

Retain the default in the remaining fields.



Device And CommSrv Port Mapping

Device ID: 45001

MAC: 00040DFA0FBB

DN: 45001

Recording Channel: 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 “73285”, 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	00040DFA0FBB	45001	Mirroring	Trunk/Internal
000		45001	00040DFA0FBB	7328545001	Mirroring	Trunk/Internal
001		46002	2CF4C5F669AD	46002	Mirroring	Trunk/Internal
001		46002	2CF4C5F669AD	7328546002	Mirroring	Trunk/Internal

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

10. Verification Steps

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

10.1. 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	6	no	aes_125_72	established	31	26

10.2. 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 (not shown). 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 total number of monitored skill groups and agent stations from **Section 3**.



Application Enablement Services Management Console

Welcome: User
Last login: Tue Jul 1 07:52:55 2014 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_ON_SP
SW Version: 6.3.1.0.19-0
Server Date and Time: Tue Jul 1 07:54:19 MDT 2014
HA Status: Not Configured

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

Log Manager

▶ Logs

▼ Status and Control

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	Switch Down	Thu Jun 26 07:28:24 2014	Online	16	0	0	0	30
●	2	S8300D	1	Talking	Tue Jul 1 07:05:43 2014	Online	16	4	27	48	30

OnlineOffline

10.3. Verify Avaya 96xx IP Deskphones

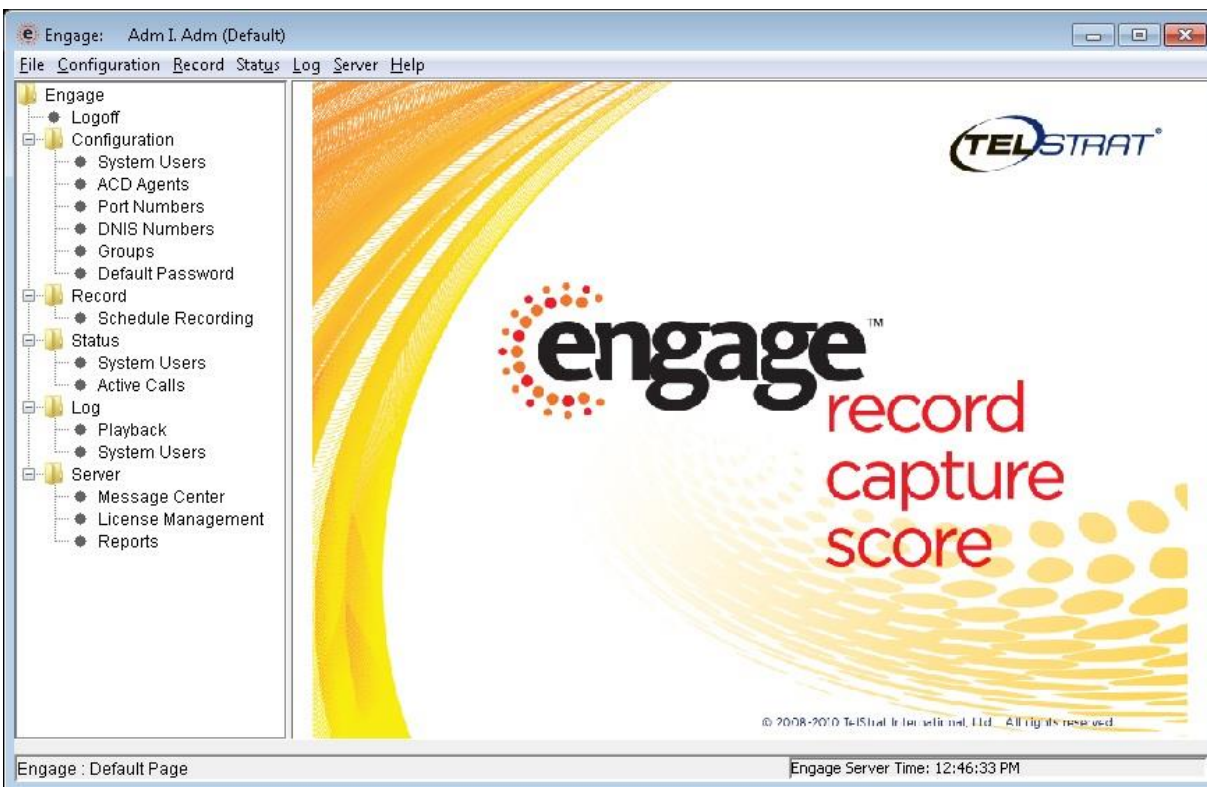
Log an agent into the skill group to answer an ACD call. From the agent's 96xx IP Deskphone, press the **MENU** or **HOME** button to display the **MENU** or **HOME** screen (not shown). Verify that the **Browser** option is included in the listing.

Select the **Browser** option, and verify that a list of recording options is displayed (not shown). Press the **Conversation Save Off** option, and verify that the display is updated to show **Conversation Save On** (not shown), which indicates the current conversation will be saved.

Complete the ACD call.

10.4. 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, 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.

The screenshot shows the Engage Admin interface. The sidebar on the left contains a tree view with the following items: Engage, Logoff, Configuration (System Users, ACD Agents, Port Numbers, DNIS Numbers, Groups, Default Password), Record (Schedule Recording), Status (System Users, Active Calls), Log (Playback, System Users), and Server (Message Center, License Management, Reports). The 'Playback' item under 'Log' is selected. The main window title is 'Engage: Adm I. Adm (Default)'. The menu bar includes File, Configuration, Record, Status, Log, Server, and Help. The main content area is titled 'Playback Log' and shows a table of cached calls. The table has the following columns: ACD Agent, Full Name, Screen Capture, Call Start Date, Call Start Time, .WAV Duration (min:sec), Call End Time, CLID, DNIS, and DN. A single call entry is listed with the following values: ACD Agent 45882, Full Name (empty), Screen Capture (checkbox), Call Start Date 7/1/2014, Call Start Time 12:28:10 PM, .WAV Duration 1:00, Call End Time 12:29:11 PM, CLID 9088485601, DNIS 7328548001, and DN 45002. Above the table, it says 'Cached Calls' and 'Number of Calls: 1'. To the right of the table, it says 'Security: Disabled'.

ACD Agent	Full Name	Screen Capture	Call Start Date	Call Start Time	.WAV Duration (min:sec)	Call End Time	CLID	DNIS	DN
45882		<input type="checkbox"/>	7/1/2014	12:28:10 PM	1:00	12:29:11 PM	9088485601	7328548001	45002

11. Conclusion

These Application Notes describe the configuration steps required for TelStrat Engage to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using VoIP recording. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

12. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3, June 2014, available at <http://support.avaya.com>.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, 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.

©2014 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.