



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

---

# **Application Notes for TelStrat Engage 5.2 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 and Avaya 9600 Series IP Deskphone for On-Demand Recording – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for TelStrat Engage 5.2 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 and Avaya 9600 Series 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 9600 Series IP Deskphones for call recording, and the Web and Push interfaces from the Avaya 9600 Series 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 5.2 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 and Avaya 9600 Series 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 9600 Series IP Deskphones for call recording, and the Web and Push interfaces from the Avaya 9600 Series 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 and Push interfaces are used by Telstrat Engage to provide activation and deactivation of call recording options via the agents' Avaya 9600 Series 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 requested monitoring on skill groups and agent stations and performed 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 web interface 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, G.711 and G.729 codec, forwarding, service observing, long duration, multiple calls, multiple agents, conference, and transfer.
- Proper display of phone 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.
- This release of Engage does not support recording of unparked calls.

## 2.3. Support

Technical support on Engage can be obtained through the following:

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

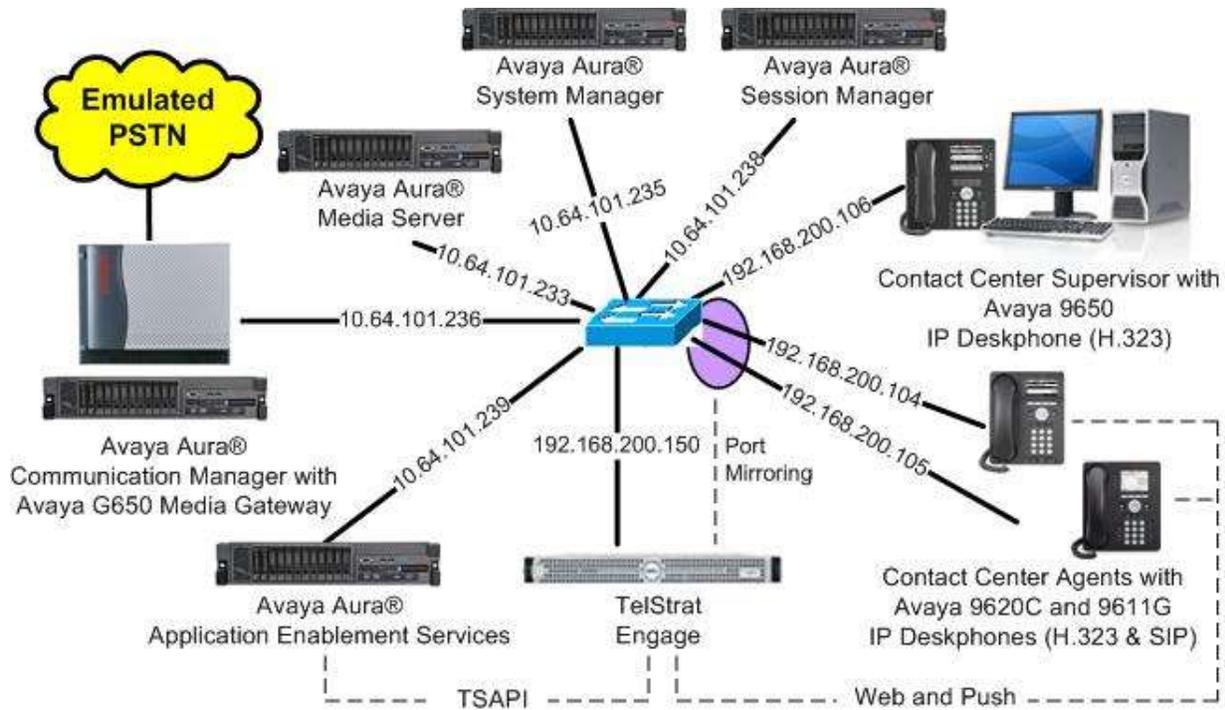
### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The RTP streams for agents with 9600 Series IP Deskphones were mirrored from the layer 2 switch, and replicated over to Engage.

The configuration of Session Manager is performed via the web interface of System Manager. 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	60001, 60002
Skill Group	61001, 61002
Supervisor	65000
Agent ID	65881, 65882
Agent Station	65001, 66002



**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 in Virtual Environment	7.0 SP1 (7.0.0.1.0.441.22477)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.236
Avaya Aura® Application Enablement Services in Virtual Environment	7.0 Patch 1 (7.0.0.0.1.13)
Avaya Aura® Session Manager in Virtual Environment	7.0 (7.0.0.0.0.700007)
Avaya Aura® System Manager in Virtual Environment	7.0 (7.0.0.0.0.4036)
Avaya 9620C & 9650 IP Deskphones (H.323)	3.250A
Avaya 9611G IP Deskphone (SIP)	7.0.0.39
TelStrat Engage on Windows Server 2008 <ul style="list-style-type: none"><li>• VOIP Engine Module</li><li>• Microsoft SQL Server 2012</li><li>• Avaya TSAPI Windows Client (csta32.dll)</li></ul>	5.2.0.14 R2 Standard 5.2.0.16 11.0.2100.60 7.0.0.131

## 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 4**. 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 4 of 12
                                OPTIONAL FEATURES

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

### 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: 60111
Type: ADJ-IP
                                COR: 1
Name: AES CTI Link
```

## 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
- Administer Engage user
- Disable security database
- Restart TSAPI service
- Obtain Tlink name

### 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. The title "Application Enablement Services Management Console" is centered at the top. A red horizontal bar is positioned below the title. The main content area features a login form with the text "Please login here:" above two input fields labeled "Username" and "Password". Below the fields are "Login" and "Reset" buttons. A second red horizontal bar is located below the login form. At the bottom of the page, the copyright notice "Copyright © 2009-2015 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 left features the Avaya logo and the title 'Application Enablement Services Management Console'. The top right displays system information: 'Welcome: User', 'Last login: Tue Jan 19 09:23:33 2016 from 192.168.200.20', 'Number of prior failed login attempts: 0', 'HostName/IP: aes7/10.64.101.239', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE', 'SW Version: 7.0.0.0.1.13', 'Server Date and Time: Tue Jan 19 09:24:20 EST 2016', and 'HA Status: Not Configured'. A red navigation bar contains 'Home | Help | Logout'. On the left, a sidebar menu lists: AE Services, Communication Manager Interface, High Availability, 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: '• 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 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'. Below the list, it states: '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 applicable WebLM server log in screen (not shown). Log in using the appropriate credentials, and navigate to display installed licenses (not shown).

The screenshot shows the Avaya Application Enablement Services Management Console with the 'Licensing' page selected. The top left features the Avaya logo and the title 'Application Enablement Services Management Console'. The top right displays system information: 'Welcome: User', 'Last login: Tue Jan 19 09:23:33 2016 from 192.168.200.20', 'Number of prior failed login attempts: 0', 'HostName/IP: aes7/10.64.101.239', 'Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE', 'SW Version: 7.0.0.0.1.13', 'Server Date and Time: Tue Jan 19 09:24:20 EST 2016', and 'HA Status: Not Configured'. A red navigation bar contains 'Home | Help | Logout'. On the left, a sidebar menu lists: AE Services, Communication Manager Interface, High Availability, Licensing (expanded), Maintenance, and Networking. Under 'Licensing', the sub-items are: 'WebLM Server Address', 'WebLM Server Access' (highlighted), and 'Reserved Licenses'. The main content area is titled 'Licensing' and contains the following text: 'If you are setting up and maintaining the WebLM, you need to use the following:' followed by a bulleted list: '• WebLM Server Address'. Below that, it says: 'If you are importing, setting up and maintaining the license, you need to use the following:' followed by a bulleted list: '• WebLM Server Access'. Finally, it says: 'If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:' followed by a bulleted list: '• Reserved Licenses'.

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** and **Device Media and Call Control**, as shown below. Note that the TSAPI license is used for device monitoring, and the DMCC license is used for the virtual IP softphones.

**Application Enablement (CTI) - Release: 7 - SID: 10503000** Standard

You are here: Licensed Products > Application\_Enablement > View License Capacity

License installed on: October 12, 2015 2:21:49 PM -05:00

**License File Host IDs:** V1-19-37-90-8F-BF

**Licensed Features**

10 Items

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	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;Cti5 MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_1 LargeServerTypes: isp2100;ibmx305;d380g3;d385g1;d385g2;u TrustedApplications: 1P5_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CTE_001, BasicUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestrict DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES CCE_001, BasicUnrestricted, AdvancedUnrestr CSI_T1_001, BasicUnrestricted, AdvancedUnr CSI_T2_001, BasicUnrestricted, AdvancedUnr AVAYAVERINT_001, BasicUnrestricted, Advan DMCUnrestricted; CCT_ELITE_CALL_CTRL_001 AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC AgentEvents; UNIFIED_DESKTOP_001, BasicU AdvancedUnrestricted, DMCUnrestricted, Agen BasicUnrestricted, AdvancedUnrestricted, DMC
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	3

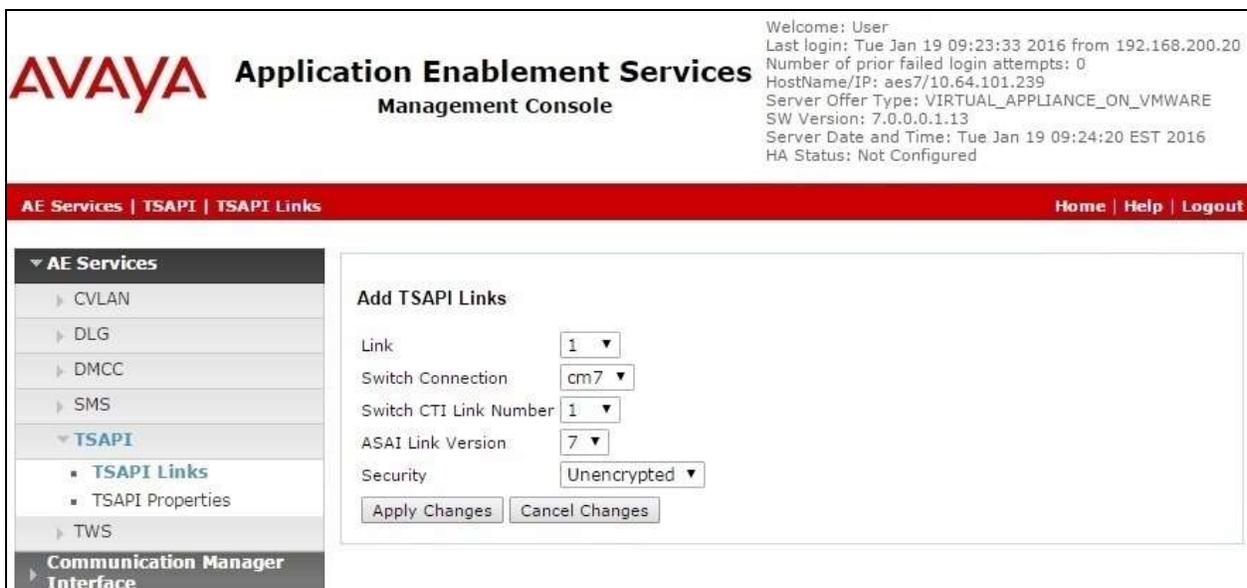
### 6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add 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 “cm7” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



## 6.4. 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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top right corner shows system information: Welcome: User, Last login: Tue Jan 19 09:23:33 2016 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes7/10.64.101.239, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 7.0.0.0.1.13, Server Date and Time: Tue Jan 19 09:27:57 EST 2016, HA Status: Not Configured.

The navigation bar includes **User Management | User Admin | Add User** and **Home | Help | Logout**.

The left sidebar menu is expanded to **User Management**, with **User Admin** selected. The **Add User** option is highlighted under **User Admin**.

The main content area shows the **Add User** form. Fields marked with \* are required. The form includes:

- \* User Id: engage
- \* Common Name: engage
- \* Surname: engage
- \* User Password: [masked]
- \* Confirm Password: [masked]
- Admin Note: [text area]
- Avaya Role: None (dropdown)
- Business Category: [text area]
- Car License: [text area]
- CM Home: [text area]
- Css Home: [text area]
- CT User: Yes (dropdown)
- Department Number: [text area]
- Display Name: [text area]
- Employee Number: [text area]
- Employee Type: [text area]
- Enterprise Handle: [text area]
- Given Name: [text area]

## 6.5. 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 **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** as shown below.

In the event that the security database is used by the customer with parameter already enabled, then follow reference [2] to configure access privileges for the Engage user from **Section 6.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". On the right side of the header, there is a welcome message and system information: "Welcome: User", "Last login: Tue Jan 19 09:23:33 2016 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 7.0.0.0.1.13", "Server Date and Time: Tue Jan 19 09:24:20 EST 2016", and "HA Status: Not Configured".

The main content area is divided into a left navigation pane and a right main pane. The left pane shows a tree view of services, with "Security Database" expanded to show "Control". The right pane displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page. This page contains two checkboxes, both of which are unchecked: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below the checkboxes is an "Apply Changes" button.

## 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 top right corner displays system information: Welcome: User, Last login: Tue Jan 19 09:23:33 2016 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes7/10.64.101.239, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 7.0.0.0.1.13, Server Date and Time: Tue Jan 19 09:24:20 EST 2016, HA Status: Not Configured.

The main interface has a red header bar with "Maintenance | Service Controller" on the left and "Home | Help | Logout" on the right. A left-hand navigation pane lists various sections: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, and Status.

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

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

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

In this case, the associated Tlink name is “AVAYA#CM7#CSTA#AES7”. Note the use of the switch connection “CM7” 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 and the text "Application Enablement Services Management Console". On the right side of the header, there is a welcome message: "Welcome: User", followed by system information: "Last login: Tue Jan 19 09:23:33 2016 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 7.0.0.0.1.13", "Server Date and Time: Tue Jan 19 09:24:20 EST 2016", and "HA Status: Not Configured".

The main navigation bar is red and contains the text "Security | Security Database | Tlinks" on the left and "Home | Help | Logout" on the right. The left sidebar is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), "Control", "CTI Users", "Devices", "Device Groups", and "Tlinks" (selected).

The main content area is titled "Tlinks" and contains a "Tlink Name" field with a radio button selected next to the value "AVAYA#CM7#CSTA#AES7". Below the field is a "Delete Tlink" button.

## 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

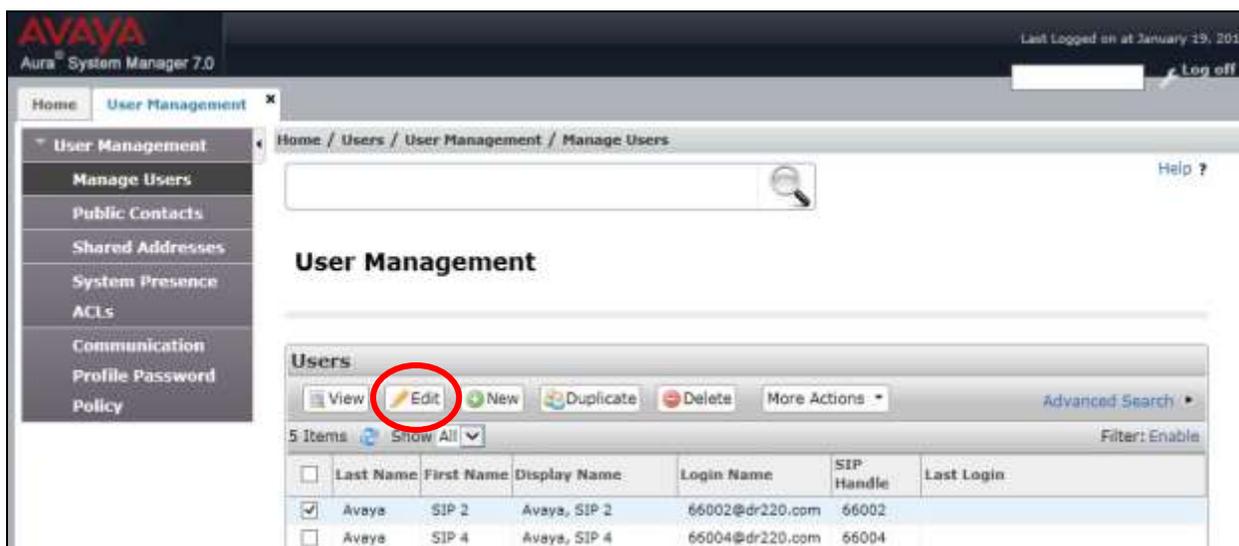
### 7.1. Launch System Manager

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.



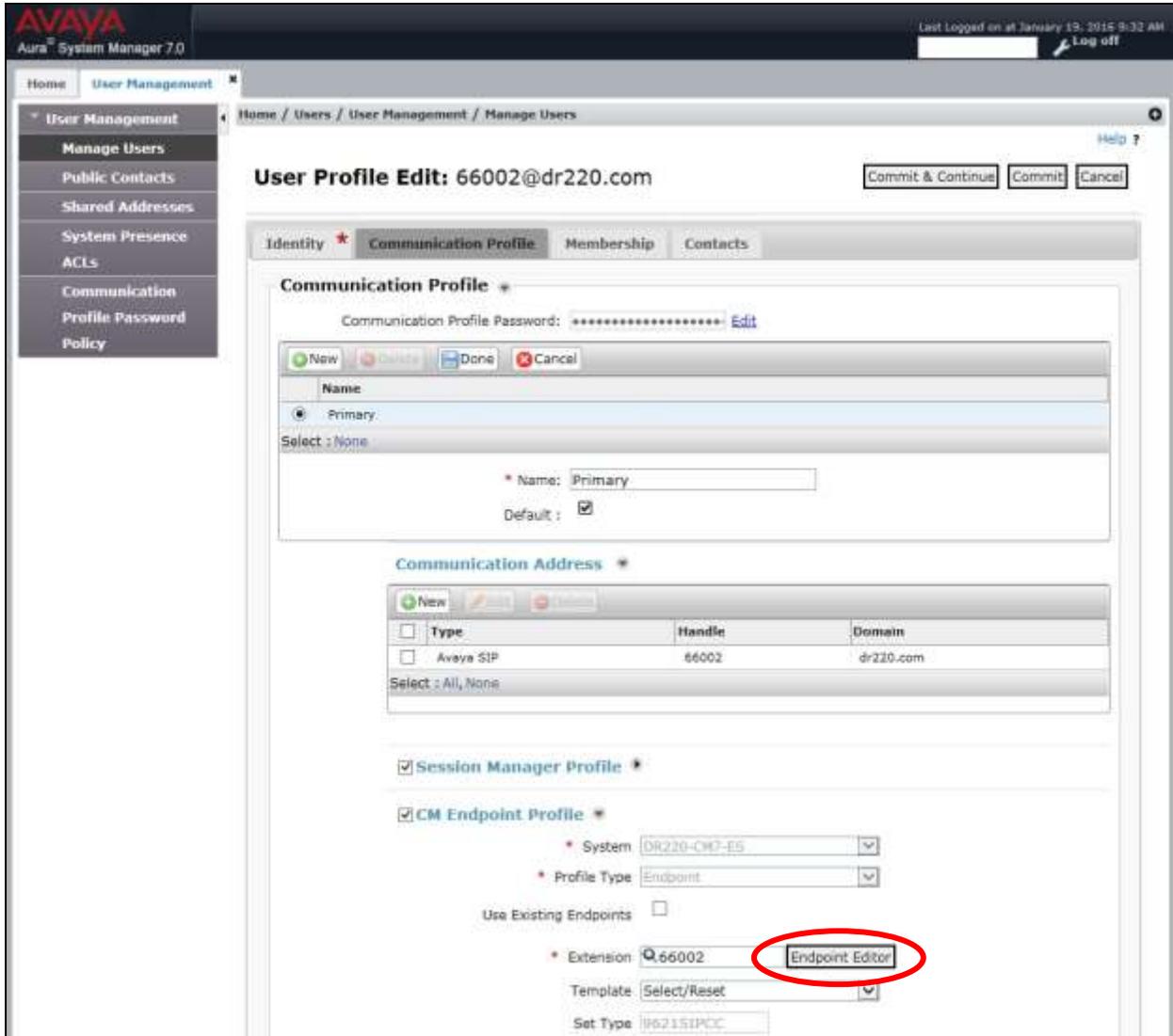
### 7.2. Administer Users

In the subsequent screen (not shown), select **Users** → **User Management**. Select **User Management** → **Manage Users** from the left pane to display the **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “66002”, and click **Edit**.



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**.



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.

The screenshot displays the Avaya Aura System Manager 7.0 interface for editing an endpoint. The main title is "Edit Endpoint". The left sidebar shows a navigation menu with "User Management" selected, and "Manage Users" as the active sub-menu. The breadcrumb trail is "Home / Users / User Management / Manage Users".

Fields for basic endpoint configuration include:

- System: DR220-CM7-ES
- Extension: 96002
- Template: Select
- Set Type: 9621SIPCC
- Port: 500004
- Security Code: (empty)
- Name: Avaya, SIP 2

The "General Options" section contains the following fields:

- Class of Restriction (COR): 1
- Emergency Location Ext: 66002
- Tenant Number: 1
- SIP Trunk: Qaar
- Coverage Path 1: 1
- Lock Message:
- Multibyte Language: First Applicable
- Class of Service (COS): 1
- Message Lamp Ext.: 66002
- Type of 3PCC Enabled: Avaya
- Coverage Path 2: (empty)
- Localized Display Name: Avaya, SIP 2
- Enable Reachability for Station Domain Control: System

Buttons for "Done", "Cancel", and "Save As Template" are visible. A note at the bottom left indicates "\*Required".

## 8. Configure Avaya 9600 Series IP Deskphones

This section provides the procedures for configuring 9600 Series IP Deskphones. The procedures include the following areas:

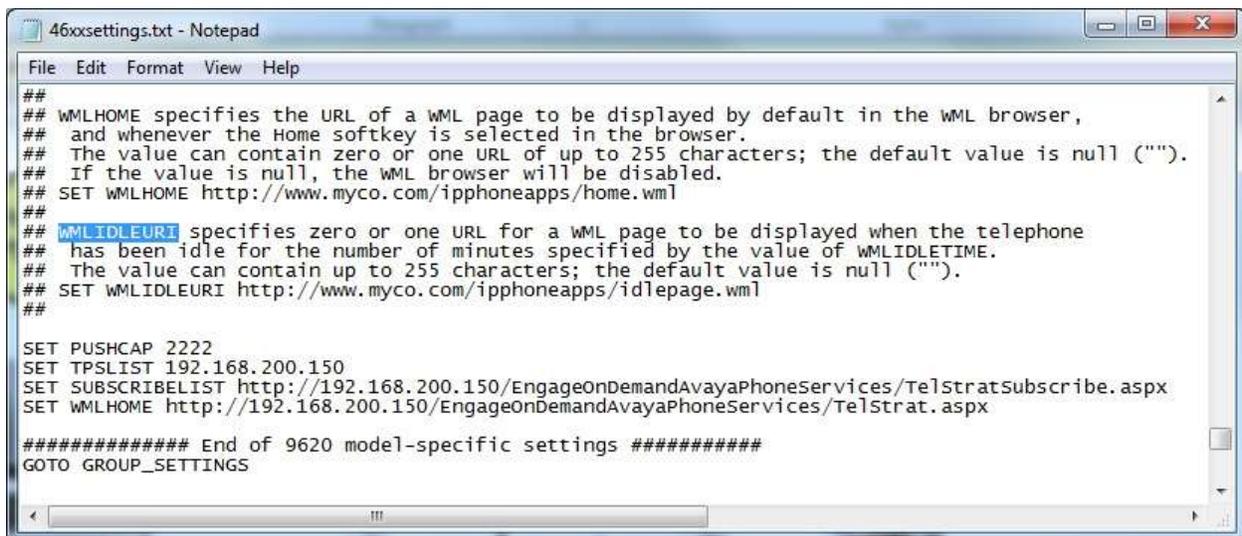
- Administer phone parameters
- Obtain MAC addresses
- Reboot telephones

### 8.1. Administer Phone Parameters

From the file server serving the 9600 Series IP Deskphones, locate the **46xxsettings.txt** file and open with the desired application such as WordPad. Navigate to the relevant phone parameters sub-section, in this case **SETTINGS9620**.

Under the **WMLIDLEURI** sub-section, set **PUSHCAP**, **TPSLIST**, **SUBSCRIBELIST**, and **WMLHOME** parameters as shown below, where “192.168.200.150” is the IP address of the Engage server running the Web Server component.

Repeat this section for all relevant 9600 Series IP Deskphone types. In the compliance testing, the **SETTINGS9620** and **SETTINGS9611** sub-sections were configured, to correspond to the 9620C and 9611G IP Deskphones used for activation/deactivation of on-demand call recording.



```
File Edit Format View Help
###
### 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://www.myco.com/ipphoneapps/home.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 192.168.200.150
SET SUBSCRIBELIST http://192.168.200.150/EngageOnDemandAvayaPhoneServices/TelStratSubscribe.aspx
SET WMLHOME http://192.168.200.150/EngageOnDemandAvayaPhoneServices/TelStrat.aspx

##### End of 9620 model-specific settings #####
GOTO GROUP_SETTINGS
```

## 8.2. Obtain MAC Addresses

From the 9600 Series IP Deskphone, press the **MENU** or **HOME** → **Settings** buttons to display the **Main Menu** screen (not shown).

From the **Main 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 Engage.

Repeat this section for all 9600 Series IP Deskphones used by the agents in **Section 3**. In the compliance testing, the MAC addresses associated with the two agent telephones were “001B4F557C69” and “7038EEC9D518”.

## 8.3. Reboot Telephones

After the Engage server has been configured in **Section 9**, manually reboot the 9600 Series IP Deskphones to pick up the new phone settings.

## 9. Configure TelStrat Engage

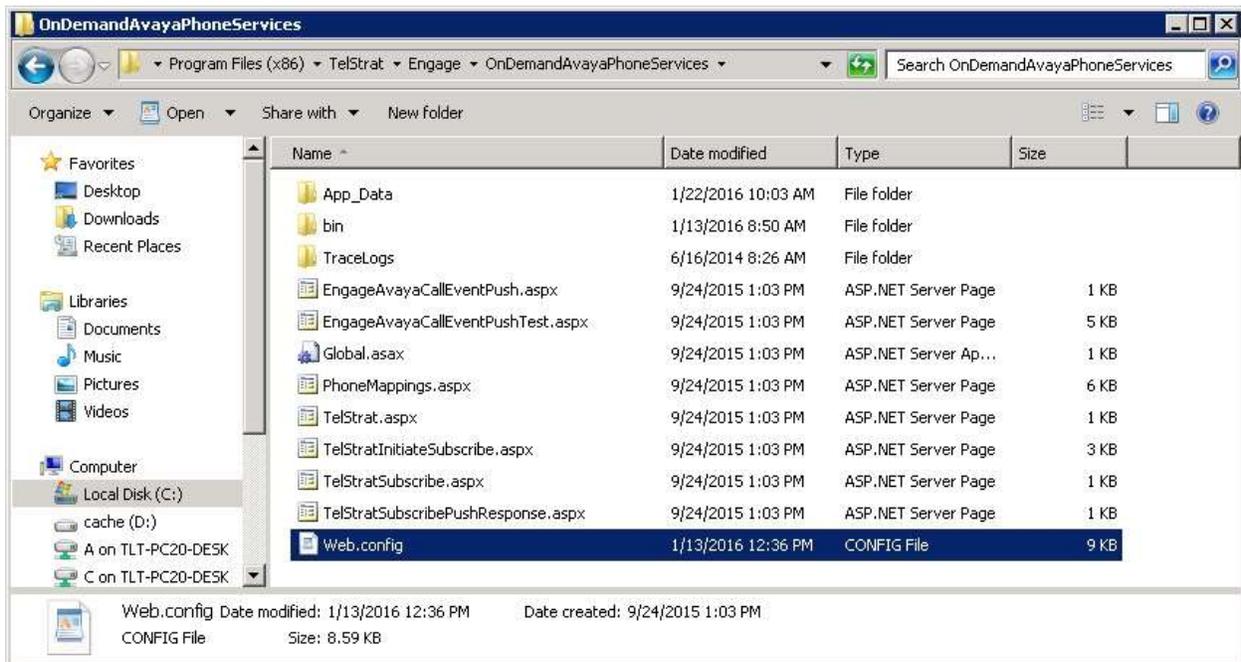
This section provides the procedures for configuring Engage. The procedures include the following areas:

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

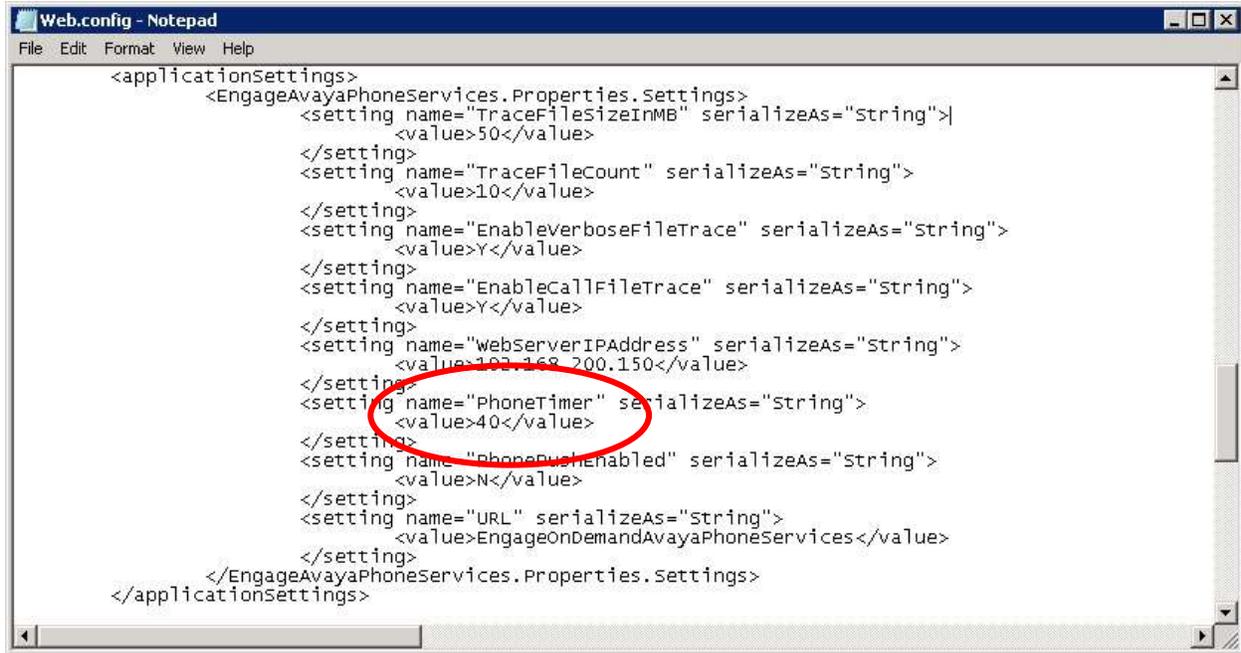
This section assumes the TSAPI client is already installed on the Engage server, along with the IP address of the Application Enablement Services server configured as part of the TSAPI client installation.

### 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** sub-section. For **PhoneTimer**, enter the desired value. In the compliance testing, the default **30** was changed to **40**, for better interoperability with the 9611G IP Deskphone.



```
<applicationSettings>
  <EngageAvayaPhoneServices.Properties.Settings>
    <setting name="TraceFileSizeInMB" serializeAs="string">
      <value>50</value>
    </setting>
    <setting name="TraceFileCount" serializeAs="string">
      <value>10</value>
    </setting>
    <setting name="EnableVerboseFileTrace" serializeAs="string">
      <value>Y</value>
    </setting>
    <setting name="EnableCallFileTrace" serializeAs="string">
      <value>Y</value>
    </setting>
    <setting name="webServerIPAddress" serializeAs="string">
      <value>192.168.200.150</value>
    </setting>
    <setting name="PhoneTimer" serializeAs="string">
      <value>40</value>
    </setting>
    <setting name="PhonePushEnabled" serializeAs="string">
      <value>N</value>
    </setting>
    <setting name="URL" serializeAs="string">
      <value>EngageOnDemandAvayaPhoneServices</value>
    </setting>
  </EngageAvayaPhoneServices.Properties.Settings>
</applicationSettings>
```

## 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 CTI

The **VoIP Configuration** screen is displayed, along with the **Avaya ACM** tab, as shown below. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **CTI Option:** “Avaya ACM”
- **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 6.4**.
- **Password:** The Engage user credentials from **Section 6.4**.

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

CTI Option	AES Server	DMCC Port
Avaya ACM	10.64.101.239	0
Recording Board ID	TSAPI APP ID	Password
2300	AVAYA#CM7#CST	*****
User ID		
engage		

Buttons: SoftPhone, OnDemand, More, ACD Groups

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

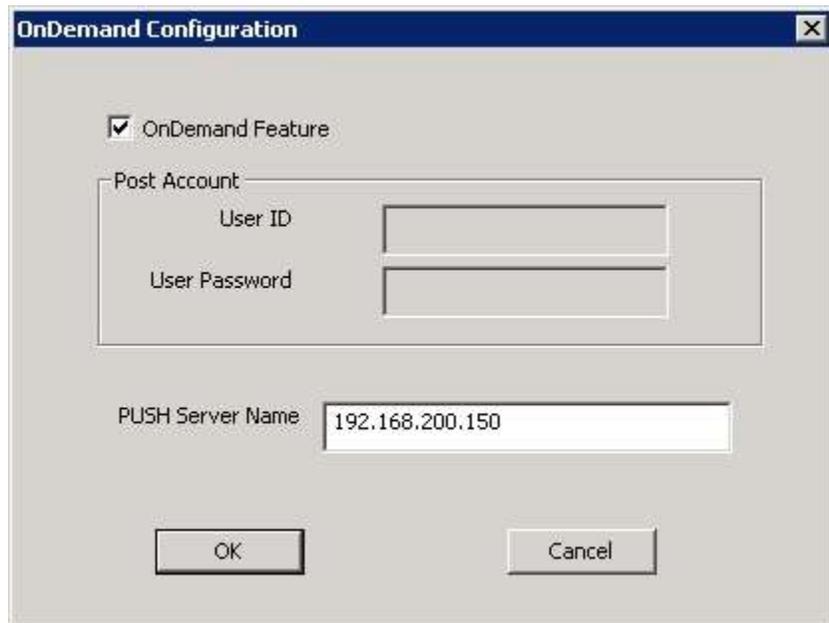
Port Mapping Table:

Recording Channel	Device...	Mac Address	DN	Record With	Trunk/Internal Calls

## 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.

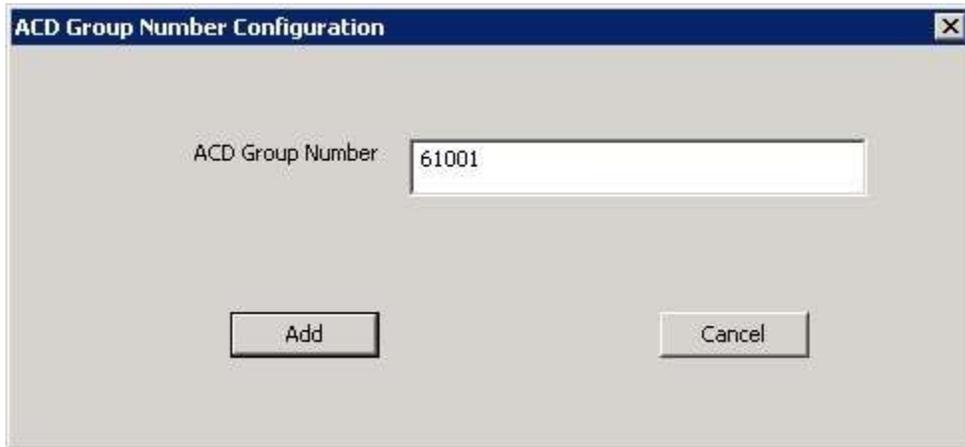


The image shows a dialog box titled "OnDemand Configuration". It contains a checked checkbox labeled "OnDemand Feature". Below this is a "Post Account" section with two input fields: "User ID" and "User Password". Below the "Post Account" section is a "PUSH Server Name" input field containing the IP address "192.168.200.150". At the bottom of the dialog are "OK" and "Cancel" buttons.

## 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 features a text input field labeled "ACD Group Number" containing the value "61001". 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 entries:

ACD Group Number
61001
61002

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 bottom 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 values in the remaining fields.

The screenshot shows the 'Device And CommSrv Port Mapping' dialog box with the following configuration:

- Device ID: 65001
- MAC: 001B4F557C69
- DN: 65001
- Recording Channel: 0
- Calls To Record:  Trunk/Internal Calls,  Trunk Calls
- Recording Stream:  Mirroring,  STC Stream
- Beep Tone: No
- HotDesk DN:

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 “30353”, as shown below.

The image shows a 'VoIP Configuration' dialog box for Avaya ACM. It contains several input fields and a table for port mapping.

**CTI Option:** Avaya ACM (dropdown)

**AES Server:** 10.64.101.239

**DMCC Port:** 0

**TSAPI APP ID:** AVAYA#CM7#CST

**Recording Board ID:** 2300

**User ID:** engage

**Password:** xxxxxxxx

**Calls To Record:**  All Trunk/Internal Calls,  All Trunk Calls,  Calls Selected By DN

**Buttons:** SoftPhone, OnDemand, More, ACD Groups

**Port Mapping Table:**

Recording Channel	Device ID	Mac Address	DN	Record With	Trunk/Internal Calls
000	65001	001B4F557C69	65001	Mirroring	Trunk/Internal
000	65001	001B4F557C69	3035365001	Mirroring	Trunk/Internal
001	66002	7038EEC9D518	66002	Mirroring	Trunk/Internal
001	66002	7038EEC9D518	3035366002	Mirroring	Trunk/Internal

**No. of Log Files:** 8

**Buttons:** Config File Location, Other Parameters, OK, Cancel

## 10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, 9600 Series IP Deskphones, 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	7	no	aes7	established	43	20

### 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**.

Welcome: User  
Last login: Sat Jan 23 14:03:34 2016 from 192.168.200.25  
Number of prior failed login attempts: 0  
HostName/IP: aes7/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 7.0.0.0.1.13  
Server Date and Time: Sat Jan 30 14:00:29 EST 2016  
HA Status: Not Configured

**AVAYA** Application Enablement Services Management Console

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

Enable page refresh every  seconds

Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
1	cm7	1	Talking	Sat Jan 23 12:53:25 2016	Online	17	4	20	39	30

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

### 10.3. Verify Avaya 9600 Series IP Deskphones

Log an agent into the skill group to answer an ACD call. From the agent's 9600 Series 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.

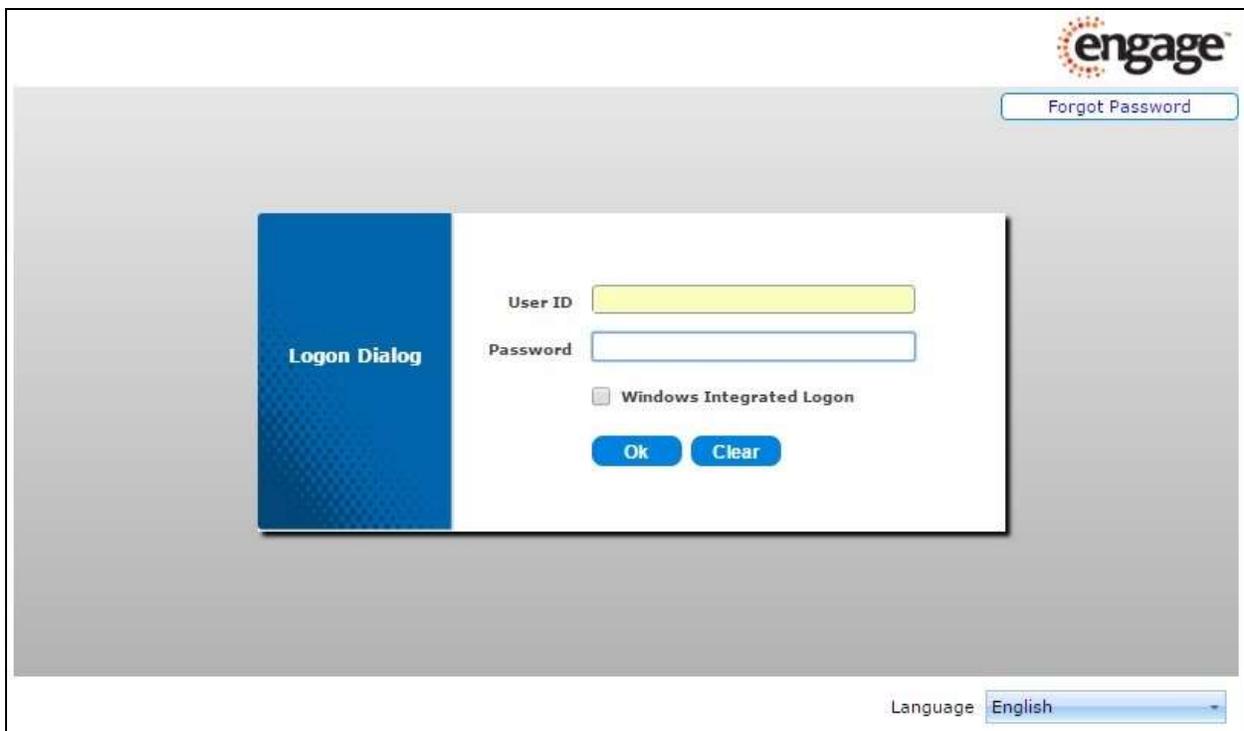
Select the **Browser** option, and verify that a list of recording options is displayed (not shown). Press the **Conversation Save Off** option, and verify that the display is updated to show **Conversation Save On** (not shown), which indicates the current conversation will be saved.

Complete the ACD call.

### 10.4. Verify TelStrat Engage

Log an agent into the skill group to handle and complete an ACD call. Access the Engage web-based interface by using the URL "http://ip-address/engage" in an Internet browser window, where "ip-address" is the IP address of the Engage server.

The **Logon Dialog** screen below is displayed. Log in using the appropriate credentials.

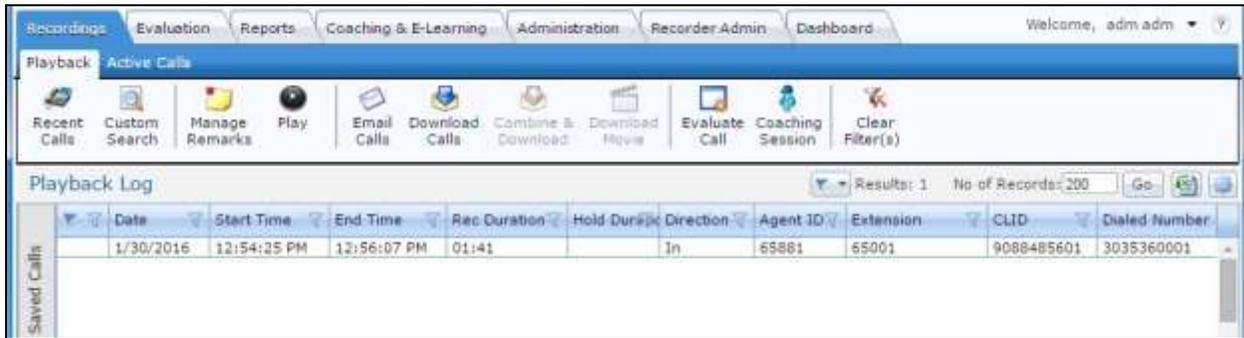


The screenshot displays the Engage web interface's logon dialog. The dialog box is titled "Logon Dialog" and features a blue header. It contains the following elements:

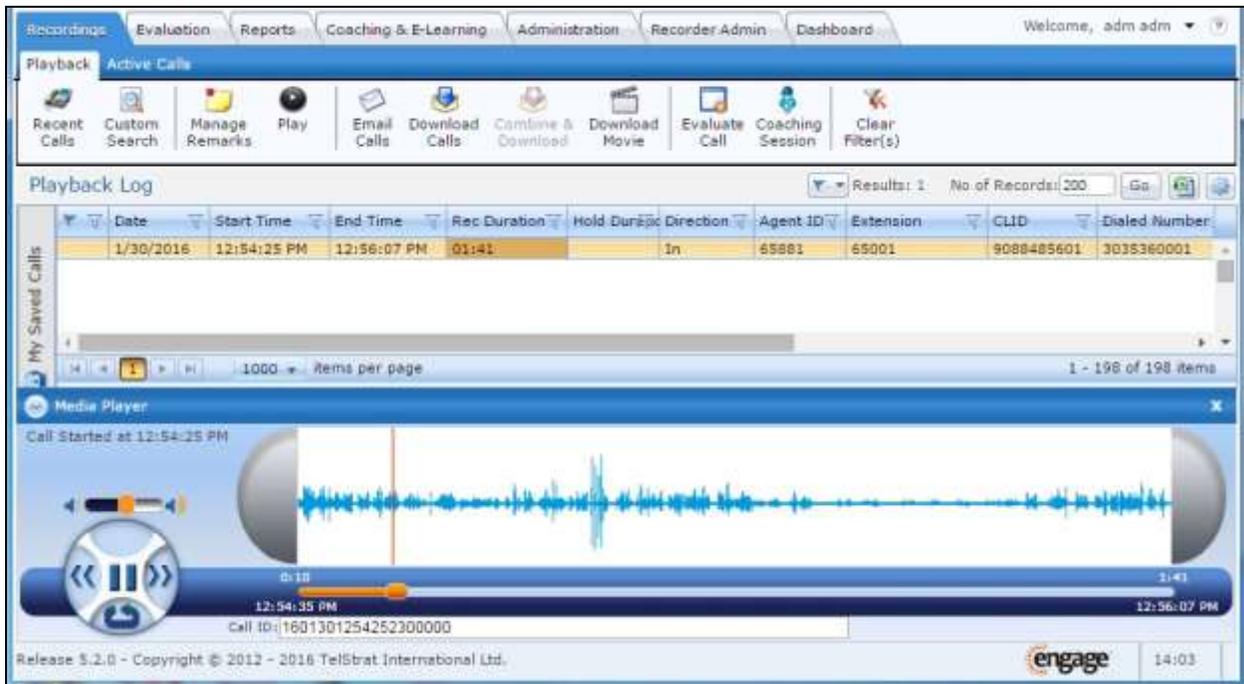
- User ID**: A text input field with a yellow highlight.
- Password**: A text input field.
- Windows Integrated Logon**: A checkbox option.
- Ok** and **Clear**: Two blue buttons for navigation.

The background of the page includes the Engage logo in the top right corner, a "Forgot Password" link, and a "Language" dropdown menu at the bottom right, currently set to "English".

The screen is updated with a list of 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.



## 11. Conclusion

These Application Notes describe the configuration steps required for TelStrat Engage 5.2 to successfully interoperate with Avaya Aura® Communication Manager 7.0, Avaya Aura® Application Enablement Services 7.0, and Avaya 9600 Series IP Deskphones for on-demand 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*, Release 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
4. *Install – Setup Engage Server*, Release 5.2, Issue 1.0, January 2016, available at <http://esupport.telstrat.com>.
5. *Config Guide – Avaya CM*, Release 5.2, Issue 1.0, January 2016, available at <http://esupport.telstrat.com>.
6. *Recorder Administration Guide*, Release 5.2, Issue 1.0, January 2016, available at <http://esupport.telstrat.com>.

---

**©2016 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).