



Application Notes for TelStrat Engage 5.2 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 using Single Step Conference – 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 using Single Step Conference. TelStrat Engage is a call recording solution.

In the compliance testing, TelStrat Engage used the Telephony Services Application Programming Interface and Device, Media, and Call Control .NET interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and to capture the media associated with the monitored agents for call recording using the Single Step Conference method.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 using Single Step Conference. TelStrat Engage is a call recording solution.

In the compliance testing, TelStrat Engage used the Telephony Services Application Programming Interface (TSAPI) and Device, Media, and Call Control (DMCC) .NET interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and to capture the media associated with the monitored agents for call recording using the Single Step Conference method.

The TSAPI interface is used by TelStrat Engage to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and for adding virtual IP softphones to active calls using the Single Step Conference method. The DMCC interface is used by TelStrat Engage to register virtual IP softphones, and to capture the media for recording purposes.

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 Single Step Conference feature from the TSAPI interface to add a virtual IP softphone to the active call to obtain the media. The event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Engage application, the application automatically requested monitoring on skill groups and agent stations and performed device queries using TSAPI, and registered the virtual IP softphones using DMCC.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for the recordings. Necessary user actions such as hold and 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.
- Use of DMCC registration services to register and un-register the virtual IP softphones.
- Use of TSAPI call control services and DMCC monitoring services to activate Single Step Conference for the virtual IP softphones and to obtain the media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711 and G.729 codec, forwarding, service observing, long duration, multiple calls, multiple agents, conference, and transfer.

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

2.2. Test Results

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

- In the attended transfer and conference scenarios, the recording for the private conversation between the agent with the transfer-to or conference-to destination is captured in a separate recording entry for the agent by design.
- 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

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**.

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 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

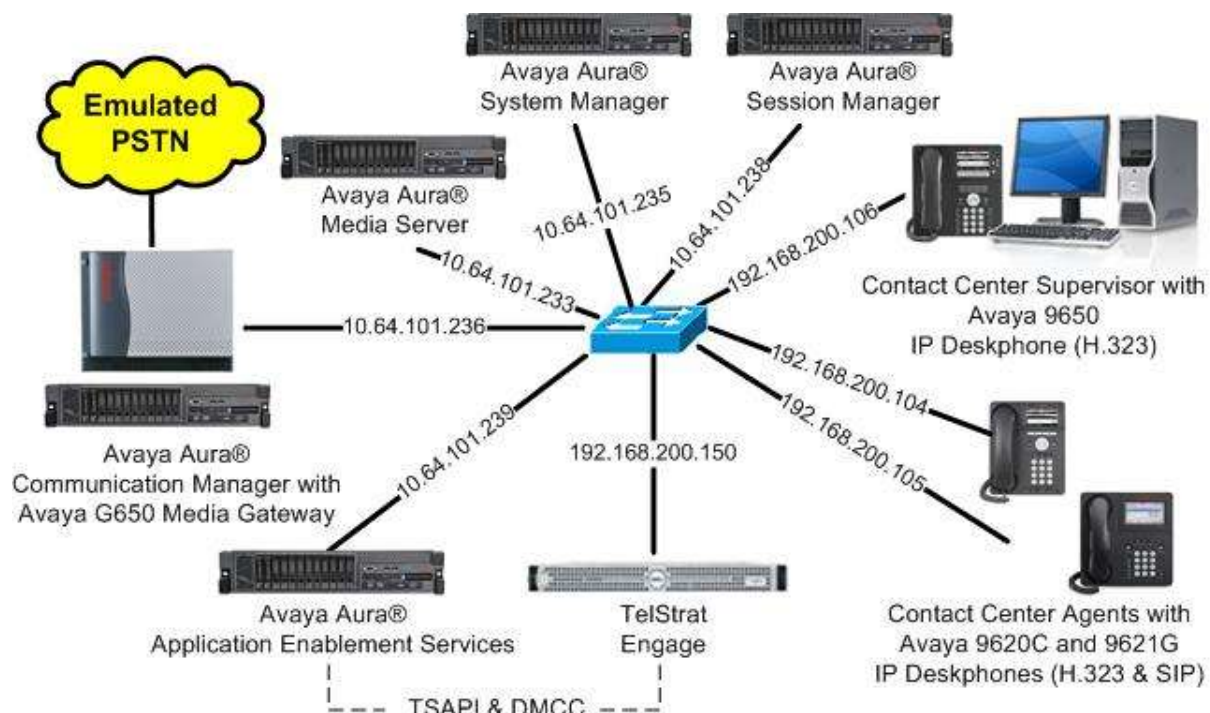


Figure 1: Compliance Testing Configuration

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 9621G IP Deskphone (SIP)	7.0.0.39
TelStrat Engage on Windows Server 2008 <ul style="list-style-type: none">• Microsoft SQL Server 2012• Avaya TSAPI Windows Client (csta32.dll)• Avaya DMCC .NET (ServiceProvider.dll)	5.2.0.14 R2 Standard 11.0.2100.60 7.0.0.131 6.3.0.229

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
- Administer virtual IP softphones

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
Name: AES CTI Link                                                    COR: 1
```

5.3. Administer Virtual IP Softphones

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

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as “9620”.
- **Name:** A descriptive name.
- **Security Code:** Enter same value as **Extension**, as required by Engage.
- **IP SoftPhone:** “y”

```
add station 65771
```

Page 1 of 5

STATION

Extension: 65771	Lock Messages? n	BCC: 0
Type: 9620	Security Code: 65771	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: Engage Virtual 1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests: y

STATION OPTIONS

Location:	Time of Day Lock Table:
Loss Group: 19	Personalized Ringing Pattern: 1
	Message Lamp Ext: 65771
Speakerphone: 2-way	Mute Button Enabled? y
Display Language: english	
Survivable GK Node Name:	
Survivable COR: internal	Media Complex Ext:
Survivable Trunk Dest? y	IP SoftPhone? y
	IP Video Softphone? n
	Short/Prefixed Registration Allowed: default
	Customizable Labels? Y

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

```
list station 65771 count 2
```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ TN Jack		
65771	S00015	Engage Virtual 1				1			
	9620		no			1	1		
65772	S00018	Engage Virtual 2				1			
	9620		no			1	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
- Administer H.323 gatekeeper
- Administer Engage user
- Administer security database
- Administer ports
- Restart services
- 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. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. Below this bar is a central login box with a light gray background. Inside the box, the text "Please login here:" is at the top. Below it are two input fields: "Username" and "Password". At the bottom of the box are two buttons: "Login" and "Reset". Another thick red horizontal bar is at the bottom of the page. Below this bar, 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 header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message for "User" is displayed, including login details and system status. A red navigation bar at the top contains "Home", "Help", and "Logout" links. A left sidebar lists various services: 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 provides an overview of the OAM web interface, listing administrative domains and their functions. It also mentions that these domains can be managed by a single administrator or separate ones.

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

Home | Help | Logout

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 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" section selected in the left sidebar. The main content area is titled "Licensing" and 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. The top header and navigation bar are consistent with the previous screenshot.

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

Licensing | Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
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

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.

AVAYA
Aura® System Manager 7.0

Last Logged on at January 1, 2016
Log off

Home Licenses

WebLM Home
Install license
Licensed products
APPL_ENAB
Application Enablement
View license capacity
View peak usage
COMMUNICATION_MANAGER
Communication Manager
Call Center
Configure Centralized Licensing
MSR
Media Server
SessionManager
SessionManager
Uninstall license
Server properties
Shortcuts
Help for Installed Product

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: V1-19-37-80-8F-BF

Licensed Features

10 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASA1 VALUE_AES_CVLAN_ASA1	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;leptop;Cti5 MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_1 LargeServerTypes: isp2100;ibmx305;d1380g3;d1385g1;d1385g2;u TrustedApplications: IPS_001, BasicUnrestricted; DMCUnrestricted; IXP_001, BasicUnrestricted; DMCUnrestricted; IXM_001, BasicUnrestricted; DMCUnrestricted; PC_001, BasicUnrestricted; DMCUnrestricted; CTE_001, BasicUnrestricted; DMCUnrestricted; OSPC_001, BasicUnrestricted; DMCUnrestricted; VP_001, BasicUnrestricted; DMCUnrestricted; SAMETIME_001, VALUE_AES_AEC_CCE_001, BasicUnrestricted, AdvancedUnrestricted; CS1_T1_001, BasicUnrestricted, AdvancedUnrestricted; CS1_T2_001, BasicUnrestricted, AdvancedUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted; DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, AdvancedUnrestricted, DMCUnrestricted, AgentBasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AgentEvents; UNIFIED_DESKTOP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentBasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted
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_DMCC	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 screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "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.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Application Enablement Services Management Console. The left navigation pane is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. Each field has a dropdown menu. The "Link" field is set to "1", "Switch Connection" is set to "cm7", "Switch CTI Link Number" is set to "1", "ASAI Link Version" is set to "7", and "Security" is set to "Unencrypted". Below the form are buttons for "Apply Changes" and "Cancel Changes".

6.4. Administer H.323 Gatekeeper

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

Locate the connection name associated with the relevant Communication Manager, in this case “cm7”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. The first row shows 'cm7' with 'No' for Processor Ethernet, '30' for Msg Period, and '1' for Number of Active Connections. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm7	No	30	1

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case “10.64.101.236” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - cm7' screen. The left navigation pane is the same as the previous screenshot. The main content area has a text input field containing '10.64.101.236' and an 'Add Name or IP' button. Below the input field are labels 'Name or IP Address', 'Delete IP', and 'Back'.

6.5. 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: 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

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

6.6. Administer 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.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the Engage user from **Section 6.5**.

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, leading to "Security Database" and then "Control". 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 these options.

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

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

6.7. Administer Ports

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

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

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

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

6.8. Restart Services

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner provides user information and system details. The left navigation pane shows a tree structure with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, and Status. The "Maintenance" category is expanded, and "Service Controller" is selected. The main content area, titled "Service Controller", contains a table listing services and their controller status. The "DMCC Service" and "TSAPI Service" are checked. Below the table, there is a link to "Status and Control" and a row of buttons: "Start", "Stop", "Restart Service", "Restart AE Server", "Restart Linux", and "Restart Web Server".

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

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

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" 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

6.9. 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, 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", shows a single Tlink named "AVAYA#CM7#CSTA#AES7" with a "Delete Tlink" button.

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

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#CM7#CSTA#AES7
Delete Tlink

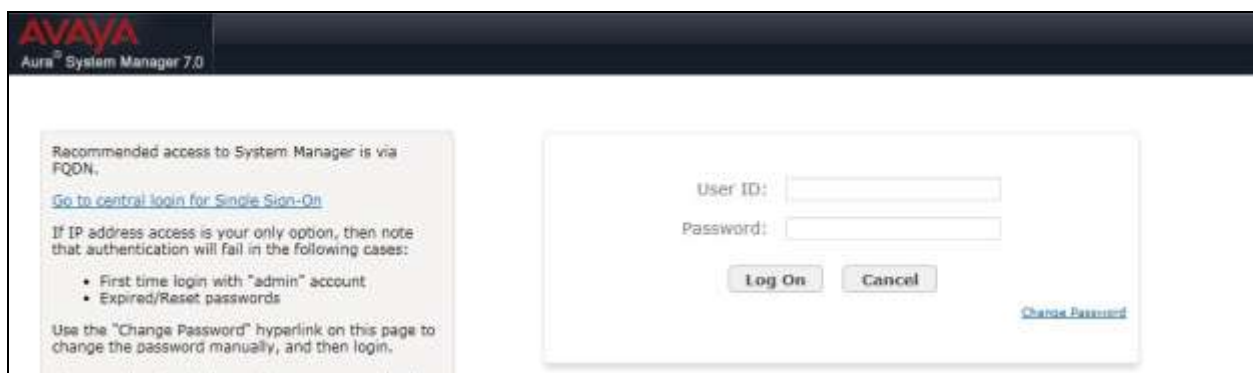
7. Configure Avaya Aura® Session Manager

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

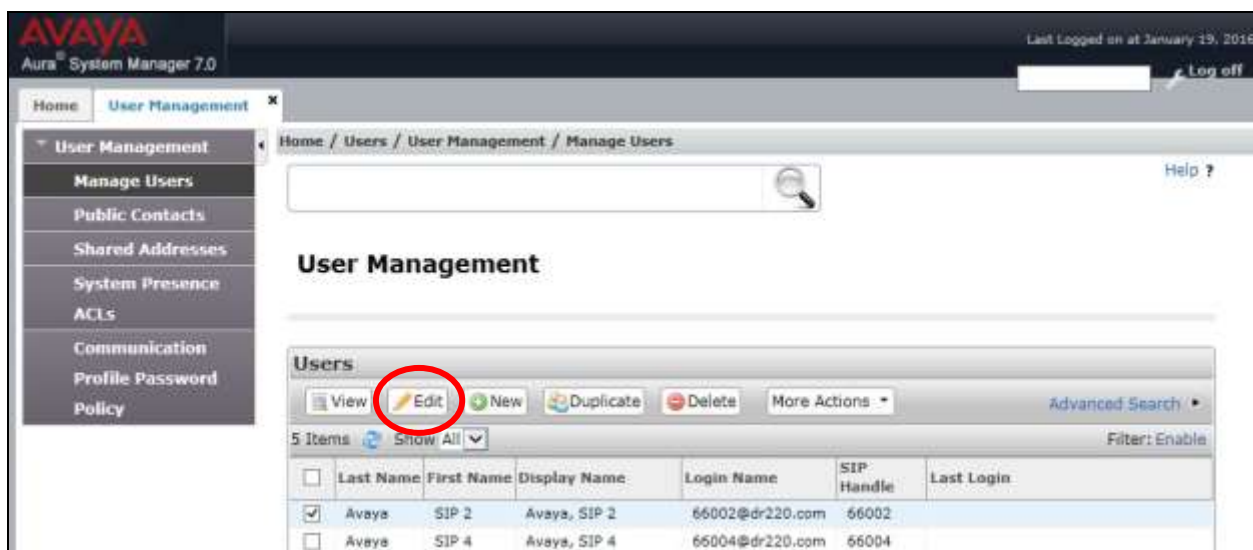
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



The screenshot shows the Avaya Aura System Manager 7.0 login page. It features a dark header with the Avaya logo and 'Aura System Manager 7.0'. The main content area has a light background. On the left, there is a text box with 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. Use the "Change Password" hyperlink on this page to change the password manually, and then login.' On the right, there is a login form with fields for 'User ID:' and 'Password:', 'Log On' and 'Cancel' buttons, and a 'Change Password' link.

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 screenshot shows the Avaya Aura System Manager 7.0 User Management screen. The header includes the Avaya logo, 'Aura System Manager 7.0', and a 'Log off' button. The left navigation pane has a 'User Management' section with a 'Manage Users' link. The main content area has a breadcrumb trail 'Home / Users / User Management / Manage Users' and a search bar. Below the breadcrumb, the title 'User Management' is displayed. A table titled 'Users' shows a list of users. The 'Edit' button in the table's toolbar is circled in red. The table has columns: Last Name, First Name, Display Name, Login Name, SIP Handle, and Last Login. The first row is selected and highlighted in blue.

	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
<input checked="" type="checkbox"/>	Avaya	SIP 2	Avaya, SIP 2	66002@dr220.com	66002	
<input type="checkbox"/>	Avaya	SIP 4	Avaya, SIP 4	66004@dr220.com	66004	

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 screenshot shows the Avaya Aura System Manager 7.0 interface. The top navigation bar includes 'Home' and 'User Management'. The left sidebar lists various management options. The main content area is titled 'User Profile Edit: 66002@dr220.com'. The 'Communication Profile' tab is active, showing fields for 'Name' (Primary) and 'Communication Address' (Avaya SIP, 66002, dr220.com). The 'Session Manager Profile' and 'CM Endpoint Profile' sections are expanded. The 'CM Endpoint Profile' section shows the 'Extension' as 66002, and the 'Endpoint Editor' button is circled in red.

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	66002	dr220.com

System	Profile Type
DR220-CMG-ES	Endpoint

Extension: 66002

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.

AVAYA
Aura System Manager 7.0

Last Logged in at January 19, 2016 9:32 AM
Log off

Home User Management

User Management

Manage Users
Public Contacts
Shared Addresses
System Presence
ACLs
Communication
Profile Password
Policy

Home / Users / User Management / Manage Users

Edit Endpoint

Done Cancel

[Save As Template]

System: DR220-CM7-ES Extension: 96002
Template: Select Set Type: 96215IPCC
Port: 500004 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) Profile Settings (P) Group Membership (M)

* Class of Restriction (COR): 1 * Class Of Service (COS): 1
* Emergency Location Ext: 66002 * Message Lamp Ext.: 66002
* Tenant Number: 1
* SIP Trunk: Q ear Type of 3PCC Enabled: Avaya
Coverage Path 1: 1 Coverage Path 2:
Lock Message: ☐ Localized Display Name: Avaya, SIP 2
Multibyte Language: first applicable Enable Reachability for Station Domain Control: system

* Required

Done Cancel

8. Configure TelStrat Engage

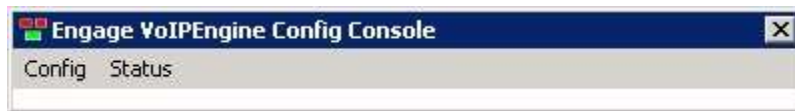
This section provides the procedures for configuring Engage. The procedures include the following areas:

- Launch VoIP engine
- Administer CTI
- Administer ACD groups
- Administer softphones
- 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.

8.1. Launch VoIP Engine

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



8.2. 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.
- **DMCC Port:** The unencrypted DMCC server port from **Section 6.7**.
- **TSAPI APP ID:** The Tlink name from **Section 6.9**.
- **User ID:** The Engage user credentials from **Section 6.5**.
- **Password:** The Engage user credentials from **Section 6.5**.

The **VoIP Configuration** window displays the **Avaya ACM** tab. The configuration fields are as follows:

- CTI Option:** Avaya ACM (selected in a dropdown menu)
- AES Server:** 10.64.101.239
- DMCC Port:** 4721
- TSAPI APP ID:** CM7#CSTA#AES7
- Recording Board ID:** 2300
- User ID:** engage
- Password:** (masked with asterisks)

Calls To Record:

- ☒ All Trunk/Internal Calls
- ☐ All Trunk Calls
- ☐ Calls Selected By DN

Port Mapping:

Recording Channel	Device ID	Mac Address	DN	Record With
-------------------	-----------	-------------	----	-------------

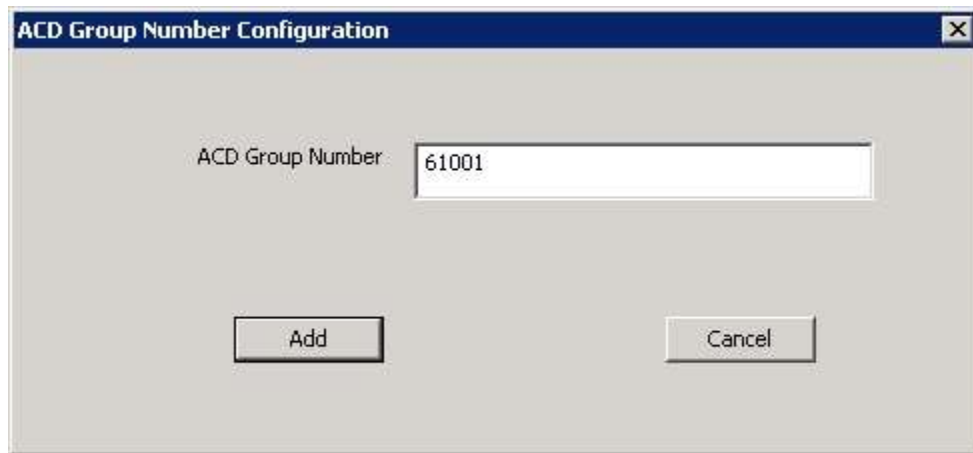
Buttons: SoftPhone, OnDemand, More, ACD Groups

Footer: No. of Log Files: 8, Config File Location, Other Parameters, OK, Cancel

8.3. Administer ACD Groups

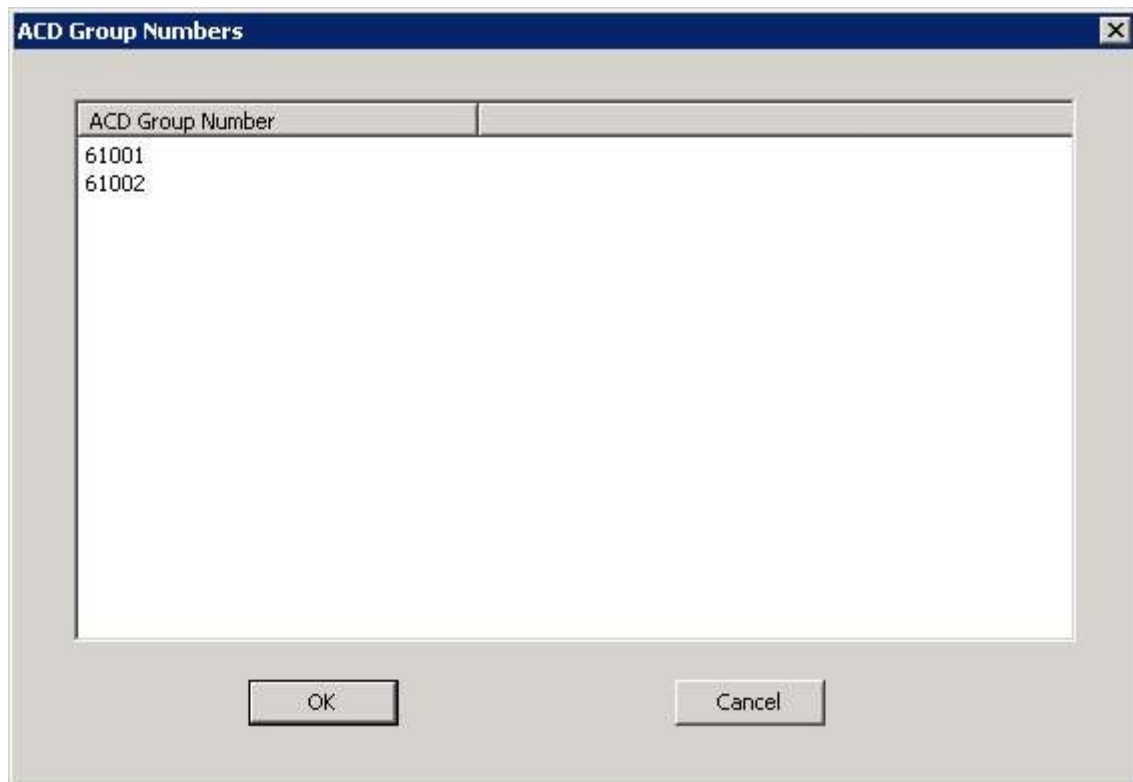
From the **VoIP Configuration** screen shown in **Section 8.2**, click on **ACD Groups** to display the **ACD Group Numbers** screen (not shown). Right click in the empty pane and select **Add**.

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



The image shows a dialog box titled "ACD Group Number Configuration". It has a text input field labeled "ACD Group Number" containing the value "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 image shows a dialog box titled "ACD Group Numbers". It contains a list box with the following items:

ACD Group Number
61001
61002

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

8.4. Administer SoftPhones

From the **VoIP Configuration** screen shown in **Section 8.2**, click on **SoftPhone** to display the **SoftPhone Station Configuration** screen below.

Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **CM Server:** IP address of the H.323 gatekeeper from **Section 6.4**.
- **From:** The extension of the first virtual IP softphone from **Section 5.3**.
- **To:** The extension of the last virtual IP softphone from **Section 5.3**.



The image shows a 'SoftPhone Station Configuration' dialog box with the following fields and values:

Field	Value
Certificate Name	
Service Observe Access Code	
CM Server	10.64.101.236
From	65771
To	65772
SoftPhone Station IP	192.168.200.150

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

8.5. Administer Device Port Mappings

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

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.



Device And CommSrv Port Mapping

Device ID: 65001

MAC:

DN: 65001

Recording Channel: 0

Calls To Record:
☒ Trunk/Internal Calls ☐ Trunk Calls

Recording Stream:
☐ Mirroring
☒ STC Stream

Beep Tone: No

☐ HotDesk DN

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 “30353”, as shown below.

VoIP Configuration

Avaya ACM

CTI Option: Avaya ACM

AES Server: 10.64.101.239

DMCC Port: 4721

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

	Recording Channel	Device ID	Mac Address	DN	Record With	Trunk/Internal Calls
000		65001		65001	STC Stream	Trunk/Internal
000		65001		3035365001	STC Stream	Trunk/Internal
001		66002		66002	STC Stream	Trunk/Internal
001		66002		3035366002	STC Stream	Trunk/Internal

No. of Log Files: 8

Config File Location

Other Parameters

OK

Cancel

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	7	no	aes7	established	126	164

Verify the registration status of the virtual IP softphones by using the “list registered-ip-stations” command. Verify that all virtual IP softphone extensions from **Section 5.3** are displayed along with the IP address of the Application Enablement Services server, as shown below.


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

REGISTERED IP STATIONS					
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	TCP Skt	Station IP Address/ Gatekeeper IP Address	
65000	9650	IP_Phone	y	192.168.200.106	
	1	3.250A		10.64.101.236	
65001	9620	IP_Phone	y	192.168.200.104	
	1	3.250A		10.64.101.236	
65771	9620	IP_API_A	y	10.64.101.239	
	1	3.2040		10.64.101.236	
65772	9620	IP_API_A	y	10.64.101.239	
	1	3.2040		10.64.101.236	

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and agent stations from **Section 3**.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jan 19 12:41:56 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 13:48:08 EST 2016
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

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ **TSAPI Service Summary**

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Fri Dec 18 17:38:27 2015	Online	17	4	164	126	30

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

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the Engage user name from **Section 6.5**, and that the **# of Associated Devices** column reflects the total number of softphone extensions from **Section 8.4**.

Application Enablement Services
Management Console

Welcome: User
 Last login: Tue Jan 19 12:41:56 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 13:40:52 EST 2016
 HA Status: Not Configured

Status | Status and Control | DMCC Service Summary
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ Status
- Alarm Viewer
- Log Manager
- ▶ Logs
- ▼ Status and Control
- CVLAN Service Summary
- DLG Services Summary
- **DMCC Service Summary**
- Switch Conn Summary
- TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Tue Jan 19 13:40:52 EST 2016

Service Uptime: 31 days, 23 hours 23 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 12

Number of Existing Devices: 2

Number of Devices Created Since Service Boot: 19

■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
■	F18C38EC697B498A5 A504D4FFD3F9D3A-11	engage	Engage	192.168.200.150	XML Unencrypted	2

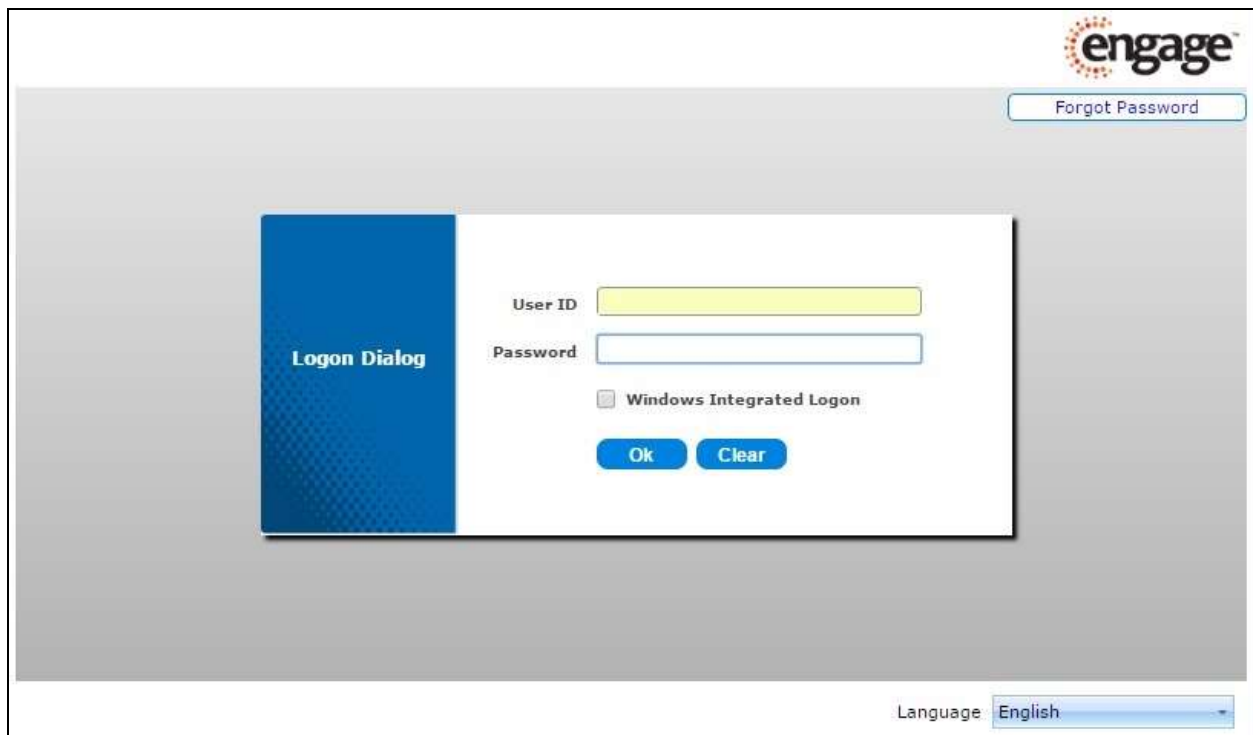
Terminate Sessions
Show Terminated Sessions

Item 1-1 of 1
1 Go

9.3. Verify TelStrat Engage

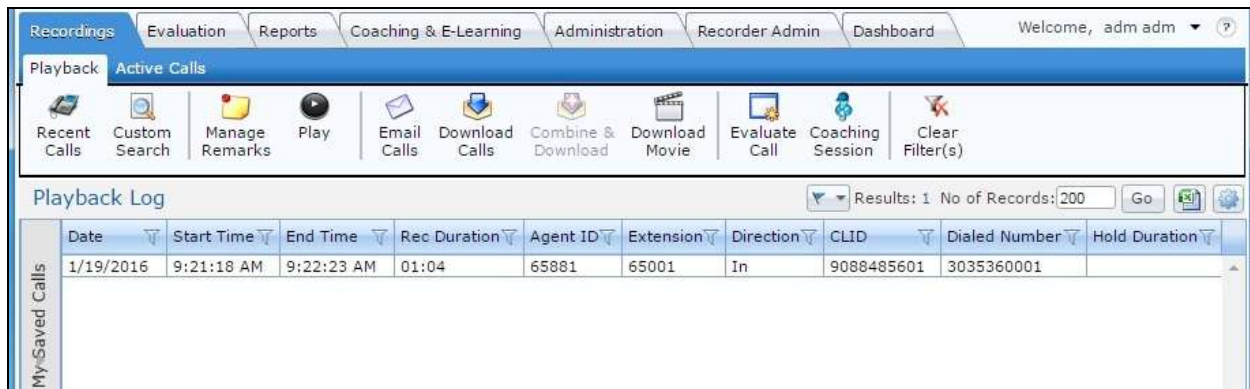
Log an agent into the skill group to handle and complete an ACD call. Access the Engage web-based interface by using the URL “http://ip-address/engage” in an Internet browser window, where “ip-address” is the IP address of the Engage server.

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



The screenshot displays the Engage web-based interface. At the top right is the Engage logo. Below it is a "Forgot Password" link. The central focus is the "Logon Dialog" window, which has a blue header with the text "Logon Dialog". Inside the dialog, there are two input fields: "User ID" (highlighted in yellow) and "Password". Below these fields is a checkbox labeled "Windows Integrated Logon". At the bottom of the dialog are two buttons: "Ok" and "Clear". At the bottom right of the main interface is a "Language" dropdown menu currently set to "English".

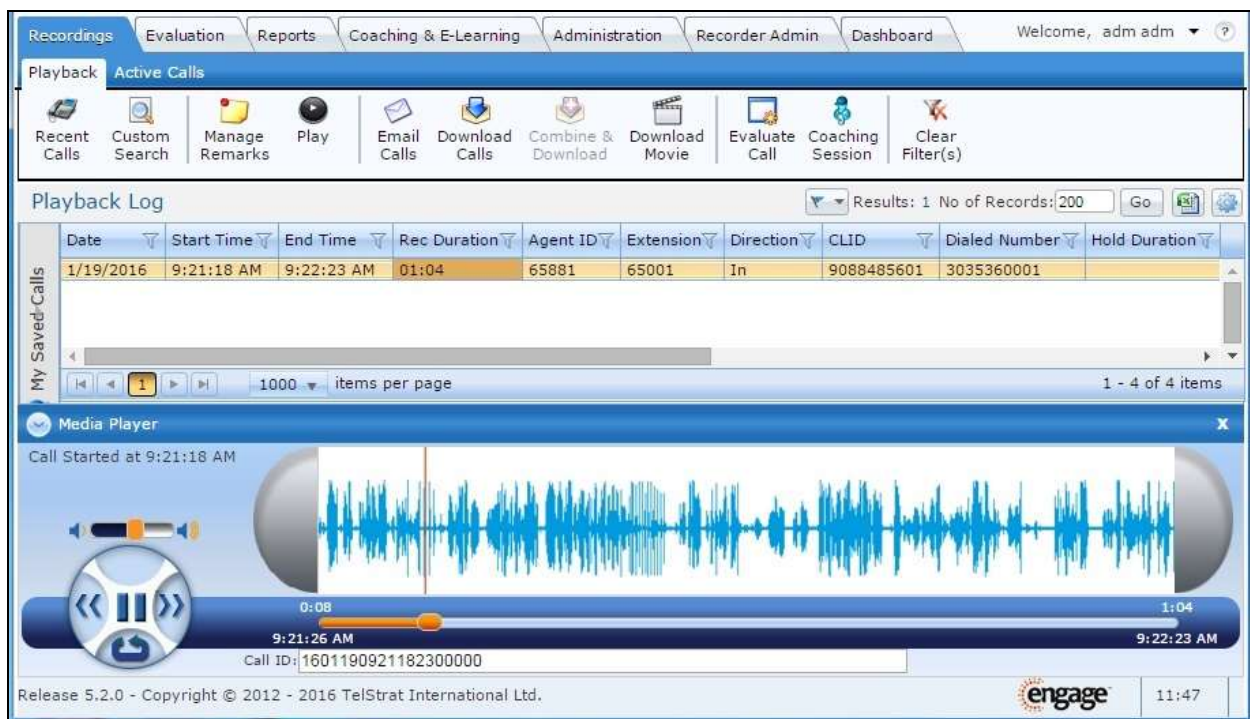
The screen is updated with a list of call recordings. Verify that there is an entry reflecting the last call, with proper values in the relevant fields.



The screenshot shows the 'Playback Log' table with the following data:

Date	Start Time	End Time	Rec Duration	Agent ID	Extension	Direction	CLID	Dialed Number	Hold Duration
1/19/2016	9:21:18 AM	9:22:23 AM	01:04	65881	65001	In	9088485601	3035360001	

Double click on the entry and verify that the call recording can be played back.



The screenshot shows the 'Media Player' window with a call recording waveform. The call started at 9:21:18 AM and ended at 9:22:23 AM. The call ID is 1601190921182300000. The waveform shows a continuous audio signal. The player controls include a play button, a progress bar, and a volume control. The call ID is displayed as 1601190921182300000.

10. Conclusion

These Application Notes describe the configuration steps required for TelStrat Engage 5.2 to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 using Single Step Conference. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, 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.