



Application Notes for TelStrat Engage with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Aura® Contact Center using Single Step Conference – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TelStrat Engage to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Aura® Contact Center 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 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 Communication Control Toolkit .Net API from Avaya Aura® Contact Center is used by TelStrat Engage to obtain information such as Agent ID, Agent Name and Skill Set associated with the agent being recorded.

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 to interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Avaya Aura® Contact Center 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 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 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. The Communication Control Toolkit (CCT) .Net API from Avaya Aura® Contact Center is used to obtain information such as Agent ID, Agent Name and Skill Set associated with the agent being recorded.

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. The CCT .Net API provides the Agent ID, Agent Name and Skill Set associated with the recorded call.

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 agent stations and performed device queries using TSAPI, and registered the virtual IP softphones using DMCC. When there is an active call at the monitored agent, Engage interfaces with Contact Center CCT .Net API to receive CTI information such as Agent ID, Agent Name and Skill Set.

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, forward, 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 observation was seen 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.

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 agent station extensions and the required data from Contact Center as shown in the table below.

Device Type	Extension
CDN	57000
Supervisor	56201
Agent ID	2000, 2001, 2002
Agent Station	56104, 56201, 56204

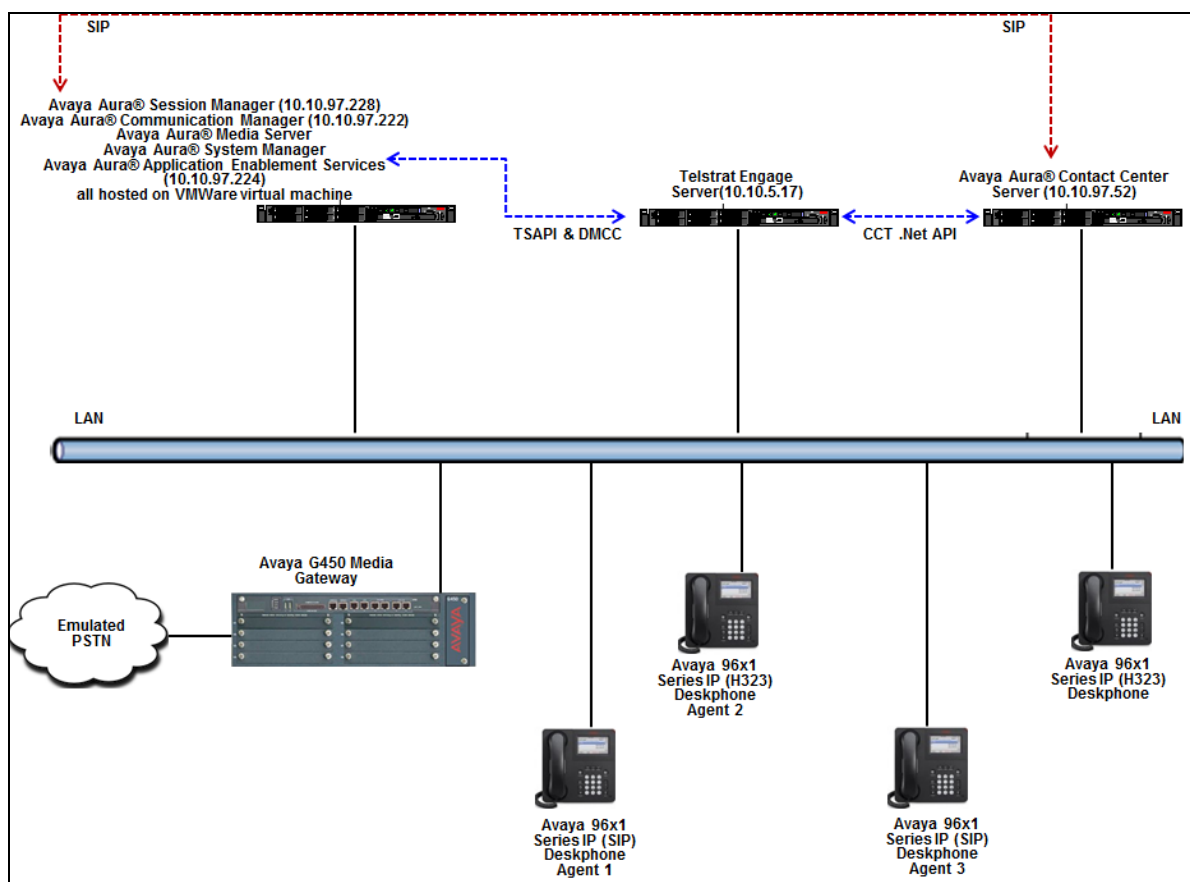


Figure 1: Compliance Testing Configuration

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	7.0.1.2.0 –FP1SP2
Avaya G450 Media Gateway	37.41.0/1
Avaya Aura® Media Server in Virtual Environment	7.7.0.375
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1.0.3.15-0
Avaya Aura® Contact Center on Windows Server 2012	7.0.1.0 Build 405 R2 Standard
Avaya Aura® Session Manager in Virtual Environment	7.0.1.2.701230
Avaya Aura® System Manager in Virtual Environment	7.0.1.2 Service Pack 2
Avaya 9611G IP Deskphones (H.323)	6.6229
Avaya 9641GS IP Deskphone (SIP)	7.0.1.1.5
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)• Avaya CCT .Net SDK (Nortel.CCT.dll & Nortel.CCT.WCF.dll)	5.3.1(web interface) 5.3.2 (VoIP Engine) R2 Standard Service Pack 1 11.0.2100.60 7.0.0.131 6.3.0.229 8.4.0.26 & 8.4.0.8

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? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	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: 56000		
Type: ADJ-IP		
		COR: 1
Name: DevvmAES		

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 56108
```

Page 1 of 5

STATION	
Extension: 56108	Lock Messages? n
Type: 9620	Security Code: *
Port: S00039	Coverage Path 1:
Name: Engage Recorder 56108	Coverage Path 2:
	Hunt-to Station:
	BCC: 0
	TN: 1
	COR: 1
	COS: 1
	Tests? y

STATION OPTIONS

Loss Group: 19	Time of Day Lock Table:
Speakerphone: 2-way	Personalized Ringing Pattern: 1
Display Language: english	Message Lamp Ext: 56108
Survivable GK Node Name:	Mute Button Enabled? y
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, three virtual IP softphones were administered as shown below, to allow for simultaneous recording of three monitored agents in **Section 3**.

```
list station 56108 count 3
```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack		
56108	S00039	Engage Recorder 56108				1			
	9620		no			1			
56109	S00042	Engage Recorder 56109				1			
	9620		no			1			
56110	S00045	Engage Recorder 56110				1			
	9620		no			1			

6. Configure Avaya Aura® Application Enablement Services

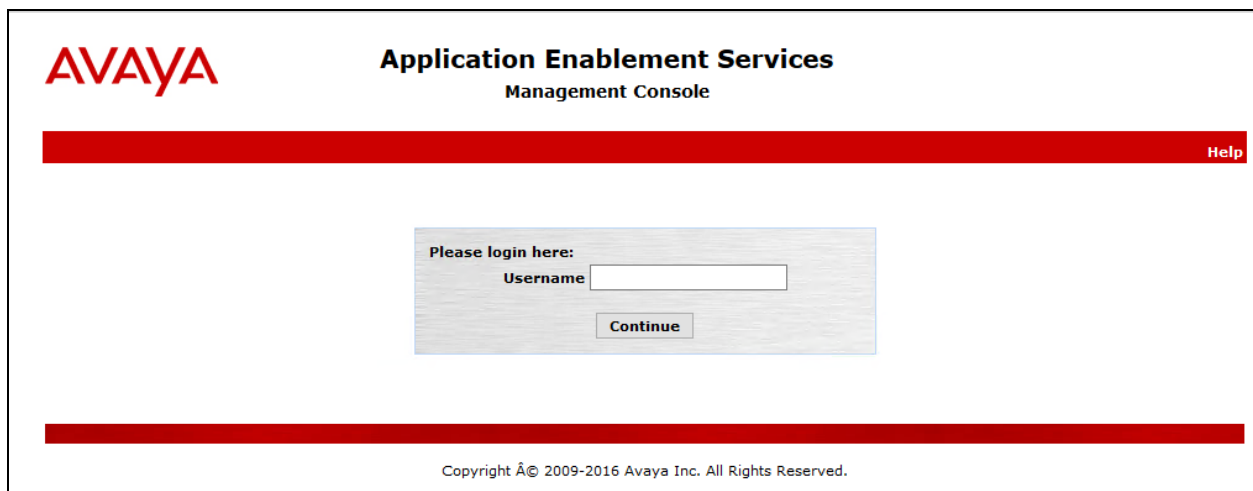
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- 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" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, another red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2016 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 right corner displays user information: "Welcome: User cust", "Last login: Thu Apr 20 15:42:32 2017 from 10.10.10.10", "Number of prior failed login attempts: 0", "HostName/IP: devvmaes/10.10.10.10", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.1.0.3.15-0", "Server Date and Time: Thu Apr 20 16:16:09 EDT 2017", and "HA Status: Not Configured". The left sidebar contains a menu with options: 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 of domains and their functions. At the bottom, it states: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain." The footer shows "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Thu Apr 20 15:42:32 2017 from 10.10.10.10
Number of prior failed login attempts: 0
HostName/IP: devvmaes/10.10.10.10
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Thu Apr 20 16:16:09 EDT 2017
HA Status: Not Configured

Home | Help | Logout

Home

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

Copyright © 2009-2016 Avaya Inc. All Rights Reserved.

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 top right corner displays the same user information as the previous screenshot. The left sidebar menu now highlights "Licensing" and includes sub-items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The main content area is titled "Licensing" and contains instructions for setting up and maintaining the WebLM, followed by a bulleted list of required items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The footer shows "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

AVAYA Application Enablement Services Management Console

Welcome: User cust
Last login: Thu Apr 20 15:42:32 2017 from 10.10.10.10
Number of prior failed login attempts: 0
HostName/IP: devvmaes/10.10.10.10
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Thu Apr 20 16:21:01 EDT 2017
HA Status: Not Configured

Home | Help | Logout

Licensing

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

Copyright © 2009-2016 Avaya Inc. All Rights Reserved.

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 License file**

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: October 13, 2015 6:25:48 AM -04:00

License File Host IDs: V1-94-05-6E-75-7F

Licensed Features

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000

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 right corner displays user information: "Welcome: User cust", "Last login: Thu Apr 20 15:42:32 2017 from [redacted]", "Number of prior failed login attempts: 0", "HostName/IP: devvmaes/10.10.10.10", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.1.0.3.15-0", "Server Date and Time: Thu Apr 20 16:27:19 EDT 2017", and "HA Status: Not Configured". The main navigation bar includes "AE Services | TSAPI | TSAPI Links" and "Home | Help | Logout". The left sidebar shows a tree view with "AE Services" expanded, containing "CVLAN", "DLG", "DMCC", "SMS", "TSAPI" (expanded), "TSAPI Links" (selected), "TSAPI Properties", and "TWS". The main content area is titled "TSAPI Links" and contains a table with columns: "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the table are buttons for "Add Link", "Edit Link", and "Delete Link".

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

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection “DevvmCM” 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 AVAYA Application Enablement Services Management Console with the "Add TSAPI Links" screen. The top right corner displays user information: "Welcome: User cust", "Last login: Thu Apr 20 15:42:32 2017 from [redacted]", "Number of prior failed login attempts: 0", "HostName/IP: devvmaes/10.10.10.10", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.1.0.3.15-0", "Server Date and Time: Thu Apr 20 16:34:48 EDT 2017", and "HA Status: Not Configured". The main navigation bar includes "AE Services | TSAPI | TSAPI Links" and "Home | Help | Logout". The left sidebar shows a tree view with "AE Services" expanded, containing "CVLAN", "DLG", "DMCC", "SMS", "TSAPI" (expanded), "TSAPI Links" (selected), "TSAPI Properties", "TWS", and "Communication Manager Interface". The main content area is titled "Add TSAPI Links" and contains form fields: "Link" (value: 1), "Switch Connection" (value: DevvmCM), "Switch CTI Link Number" (value: 1), "ASAI Link Version" (value: 7), and "Security" (value: Unencrypted). Below the fields 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 “DevvmCM”, 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 has 'Communication Manager Interface' selected, with 'Switch Connections' highlighted. The main area displays the 'Switch Connections' table with one entry, 'DevvmCM', which is selected with a radio button. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The top right shows user information and login details.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> DevvmCM	Yes	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 “10.10.97.222” as shown below. Click **Add Name or IP**.

The screenshot shows the 'Edit H.323 Gatekeeper - DevvmCM' screen. A text input field contains the IP address '10.10.97.222'. Below the field is the label 'Name or IP Address'. There are buttons for 'Add Name or IP', 'Delete IP', and 'Back'. The top right shows user information and login details.

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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message for 'User cust' with system details like last login time and version. A red navigation bar contains 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'. On the left, a sidebar menu lists various services, with 'User Management' expanded to show 'User Admin' and 'Add User' selected. The main area is titled 'Add User' and contains a form with fields for user details. Fields marked with an asterisk are required. The 'CT User' dropdown is set to 'Yes'.

Add User	
Fields marked with * can not be empty.	
* User Id	Test
* Common Name	Test
* Surname	Test
* User Password	*****
* Confirm Password	*****
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
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 documents in **Section 12** 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 user "cust" with login details. A red navigation bar contains "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The main content area, titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services", contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", followed by an "Apply Changes" button.

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 cust
Last login: Thu Apr 20 15:42:32 2017 from 10.10.10.10
Number of prior failed login attempts: 0
HostName/IP: devvmaes/10.10.10.10
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Thu Apr 20 16:53:05 EDT 2017
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/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999Enabled Disabled

Encrypted TCP Port9998Enabled Disabled

DLG Port

TCP Port5678

TSAPI Ports

TSAPI Service Port450Enabled Disabled

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 Port4721Enabled Disabled

Encrypted Port4722Enabled Disabled

TR/87 Port4723Enabled Disabled

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**.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Apr 20 15:42:32 2017 from [REDACTED]
Number of prior failed login attempts: 0
HostName/IP: devvmaes/[REDACTED]
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Thu Apr 20 16:54:31 EDT 2017
HA Status: Not Configured

Maintenance | Service ControllerHome | 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#DEVVMCM#CSTA#DEVVMAES”. Note the use of the switch connection “DevvmCM” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with login details. A red navigation bar contains the breadcrumb "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar shows a tree view with categories like AE Services, Communication Manager, and Security. Under Security, the "Security Database" is expanded, and "Tlinks" is selected. The main content area, titled "Tlinks", shows a single entry with the "Tlink Name" "AVAYA#DEVVMCM#CSTA#DEVVMAES" and a "Delete Tlink" button.

Welcome: User cust
Last login: Thu Apr 20 15:42:32 2017 from [REDACTED]
Number of prior failed login attempts: 0
HostName/IP: devvmaes/[REDACTED]
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Thu Apr 20 16:56:10 EDT 2017
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
Tlink Groups
Worktops

Tlinks
Tlink Name
AVAYA#DEVVMCM#CSTA#DEVVMAES
Delete Tlink

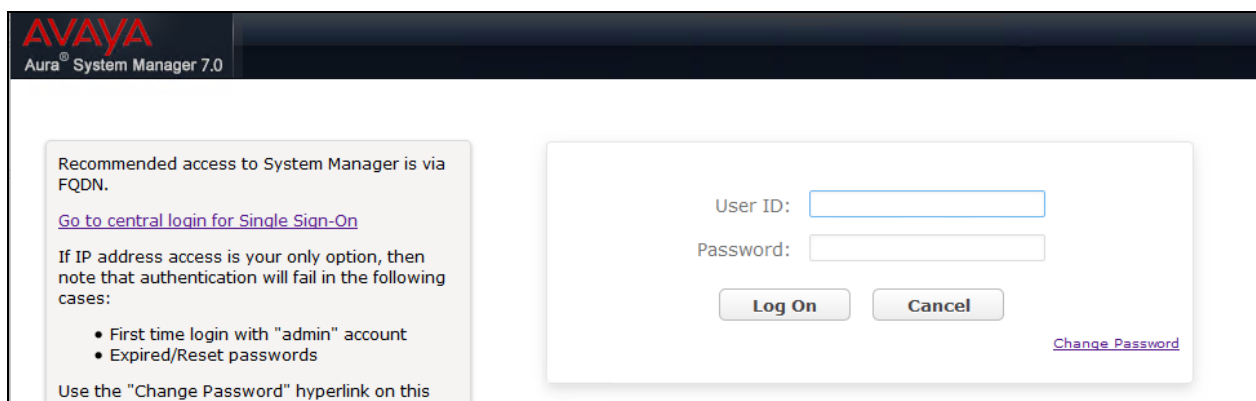
7. Configure Avaya Aura® Session Manager

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 interface. The header features the Avaya logo and the text "Aura® System Manager 7.0". The main content area is divided into two sections. On the left, a grey box contains the following text: "Recommended access to System Manager is via FQDN." followed by a blue hyperlink "Go to central login for Single Sign-On". Below this, it states "If IP address access is your only option, then note that authentication will fail in the following cases:" followed by a bulleted list: "• First time login with 'admin' account" and "• Expired/Reset passwords". At the bottom of this box, it says "Use the 'Change Password' hyperlink on this". On the right, a white box contains the login form with labels "User ID:" and "Password:" next to input fields. Below the fields are "Log On" and "Cancel" buttons. A blue hyperlink "Change Password" is located at the bottom right of the white box.

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 one of the SIP agent station from **Section 3**, in this case “56204”, and click **Edit**.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 7.0', and a search bar. The left sidebar contains a 'User Management' menu with options like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence', 'ACLs', 'Communication', 'Profile Password', and 'Policy'. The main content area is titled 'User Management' and displays a table of users. The 'Edit' button is highlighted with a red box.

	TwoOFour	OFour	TwoOFour, OFour	56204@bvwddev.com	56204
<input checked="" type="checkbox"/>	TwoOOne	OOne	TwoOOne, OOne	56201@bvwddev.com	56201
<input type="checkbox"/>	TwoOTwo	OTwo	TwoOTwo, OTwo	56202@bvwddev.com	56202

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 'User Profile Edit' interface for user '56204@bvwddev.com'. The left sidebar contains navigation links: 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence', 'ACLs', 'Communication', 'Profile Password', and 'Policy'. The main content area has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' field and an 'Edit' link. Below this is a 'Communication Address' section with a table of addresses. The table has columns for 'Type', 'Handle', and 'Domain'. Two addresses are listed: 'Avaya SIP' with handle '56204' and domain 'bvwddev.com', and 'Avaya Presence/IM' with handle '56204' and domain 'presence.bvwddev.com'. Below the table are checkboxes for 'Session Manager Profile', 'Avaya Breeze Profile', and 'CM Endpoint Profile'. The 'CM Endpoint Profile' is checked, showing fields for 'System' (DevvmCM), 'Profile Type' (Endpoint), and 'Extension' (56204). A 'Use Existing Endpoints' checkbox is also present. At the bottom, there is a 'Display Extension Ranges' link and an 'Endpoint Editor' button, which is highlighted with a red box.

User Profile Edit: 56204@bvwddev.com

Commit & Continue Commit Cancel

Identity * Communication Profile Membership Contacts

Communication Profile

Communication Profile Password: Edit

New Delete Done Cancel

Name

Primary

Select : None

* Name: Primary

Default : ☒

Communication Address

New Edit Delete

Type	Handle	Domain
<input type="checkbox"/> Avaya SIP	56204	bvwddev.com
<input type="checkbox"/> Avaya Presence/IM	56204	presence.bvwddev.com

Select : All, None

☒ Session Manager Profile

☐ Avaya Breeze Profile

☒ CM Endpoint Profile

* System DevvmCM

* Profile Type Endpoint

Use Existing Endpoints ☐

* Extension 56204

Display Extension Ranges

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. The top navigation bar includes the Avaya logo, version information, and a user session summary. The left sidebar contains a menu for 'User Management' with options like 'Manage Users', 'Public Contacts', and 'Shared Addresses'. The main content area is titled 'Edit Endpoint' and includes a breadcrumb trail: 'Home / Users / User Management / Manage Users'. Below the title are 'Done' and 'Cancel' buttons, and a '[Save As Template]' link. The configuration fields are organized into two columns: System (DevvmCM), Extension (56204), Template (Select), Port (S00016), Name (TwoOFour, OFour), Set Type (9621SIPCC), and Security Code. A tabbed interface below these fields includes 'General Options (G)', 'Feature Options (F)', 'Site Data (S)', and 'Abbreviated Call Dialing (A)'. The 'General Options' tab is active, showing fields for Class of Restriction (COR), Emergency Location Ext, Tenant Number, SIP Trunk, Coverage Path 1, Class Of Service (COS), Message Lamp Ext, Type of 3PCC Enabled (set to Avaya), and Coverage Path 2. The 'Type of 3PCC Enabled' dropdown is highlighted with a red box.

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	56204	* Message Lamp Ext.	56204				
* Tenant Number	1	Type of 3PCC Enabled		Avaya			
* SIP Trunk	Qaar	Coverage Path 1		Coverage Path 2			

8. Configure Avaya Aura® Contact Center

This section provides steps on how to configure Contact Center. This section assumes that Contact Center system is already installed and operational with the proper required licenses; the section provides steps for configuring the following configurations:

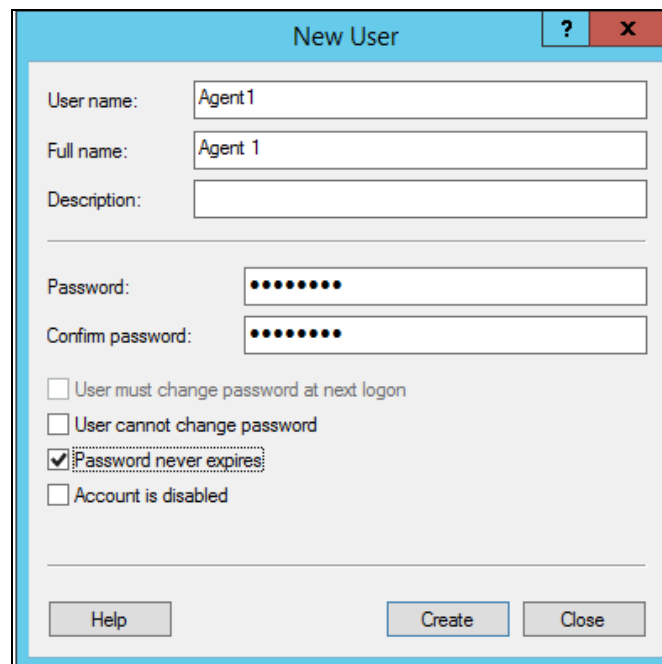
- Configure Windows users.
- Configure Agents.
- Configure Users in CCT Administration.

In the compliance test, the Contact Center system used is a co-res system which consists of Contact Center Manager Server, Contact Center Manager Administrator, Contact Center Communication Control Toolkit, Contact Center License Manager, and Avaya Media Server Applications.

8.1. Configure Windows Users

In the compliance test, the Contact Center CCT server is not joined to a Windows domain; therefore, the Windows user used for CCT user login will be created in the local CCT server. In case the CCT server joins a domain, the Windows user needs to be created in the domain controller.

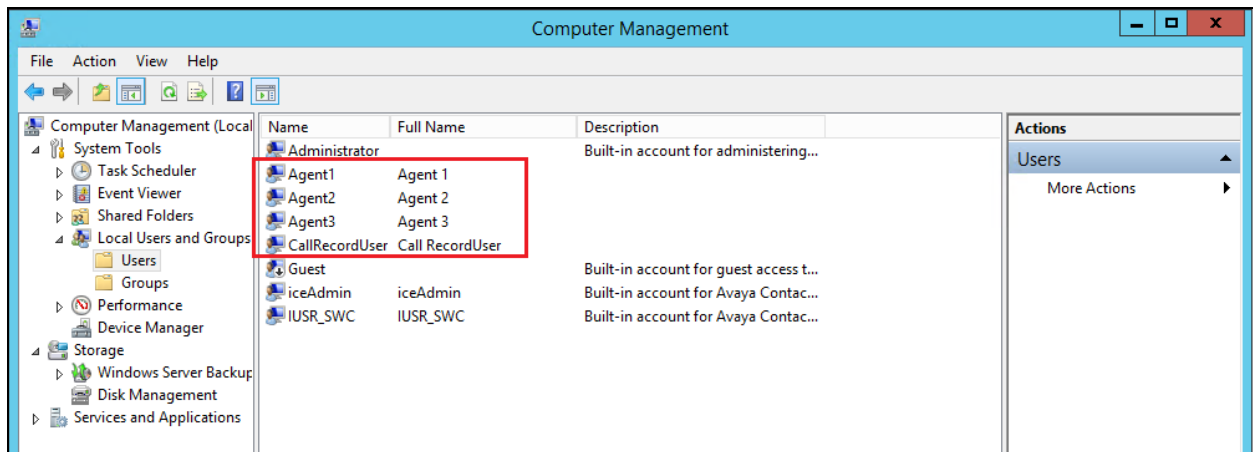
From the Contact Center CCT server, navigate to menu **Start → Administrative Tools → Computer Management → Local Users and Groups → Users** (not shown). Right click on **Users** and then select **New User....** The **New User** window is displayed; enter information for user as shown below. Click **Create** button to complete.



The screenshot shows the 'New User' dialog box. The 'User name' field is filled with 'Agent 1' and the 'Full name' field is also filled with 'Agent 1'. The 'Description' field is empty. The 'Password' and 'Confirm password' fields are both filled with masked characters (dots). Below the password fields, there are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (unchecked), 'Password never expires' (checked), and 'Account is disabled' (unchecked). At the bottom of the dialog, there are three buttons: 'Help', 'Create', and 'Close'.

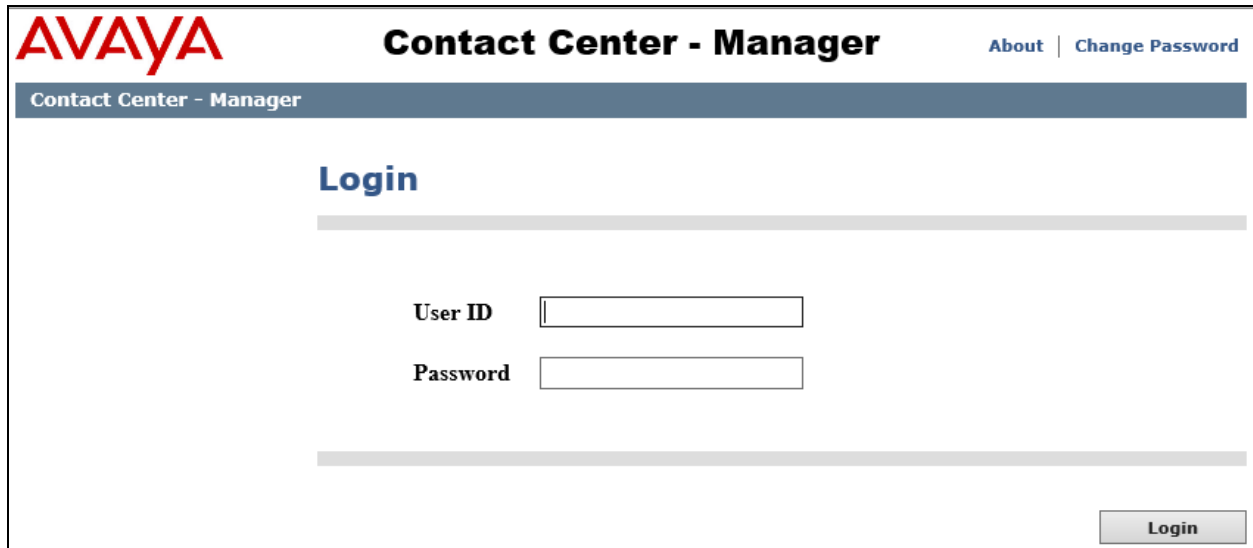
Repeat the same procedure to create “CallRecordUser” that will be used in **Section 9.3** for the Engage application.

The screen below shows the **Computer Management** window with a Window user created as **Agent1** and **CallRecordUser**. Similarly more users can be created as required.



8.2. Configure Agents

Access the Contact Center-Manager web interface by using the URL “http://server name” in an Internet browser window, where “server name” is the server name of Contact Center. Log in using the appropriate credentials.



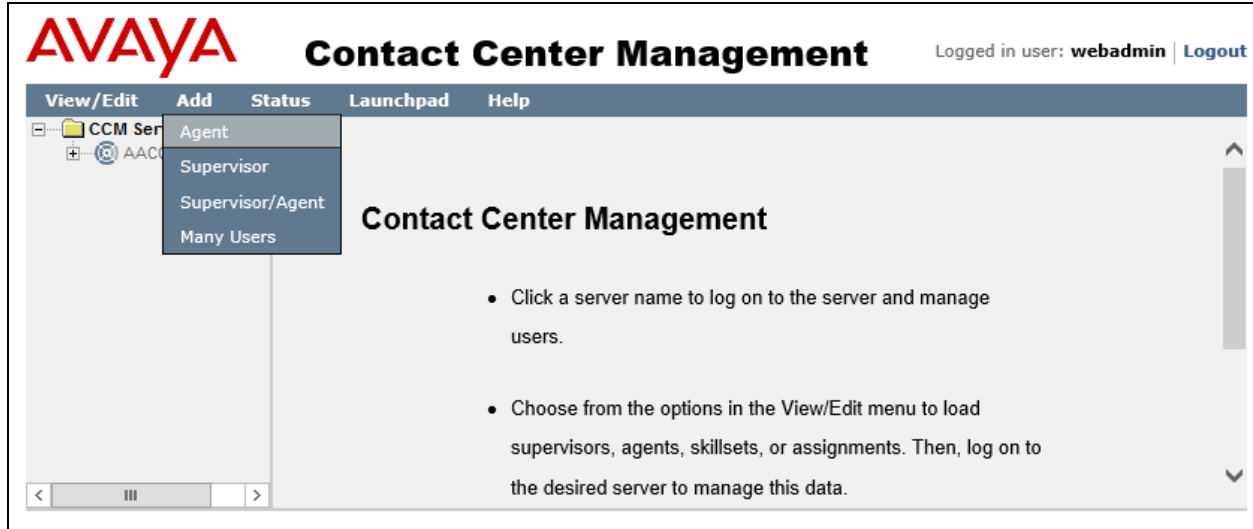
The screenshot shows the Avaya Contact Center - Manager web interface. At the top left is the Avaya logo. To its right is the title "Contact Center - Manager". Further right are links for "About" and "Change Password". Below the title bar is a dark blue header with the text "Contact Center - Manager". The main content area has a "Login" heading. Below this heading are two input fields: "User ID" and "Password". At the bottom right of the main content area is a "Login" button.

The **Contact Center – Manager Launchpad** screen is shown below. Click on **Contact Center Management**.



The screenshot shows the Avaya Contact Center - Manager Launchpad web interface. At the top left is the Avaya logo. To its right is the title "Contact Center - Manager". Further right are links for "About", "Audit Trail", and "Logout". Below the title bar is a dark blue header with the text "Launchpad". The main content area has a "Launchpad" heading. Below this heading is a list of menu items, each with a circular icon containing a stylized 'C' and the text of the menu item. The menu items are arranged in two columns. The first column contains: "Contact Center Management", "Access and Partition Management", "Real-Time Reporting", "Historical Reporting", "Call Recording and Quality Monitoring", and "Prompt Management". The second column contains: "Configuration", "Scripting", "Emergency Help", "Outbound", and "Multimedia".

Navigate to **Add → Agent** as shown below.



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

- **First Name:** A descriptive name.
- **Last Name:** A descriptive name.
- **Login ID:** Enter an agent login ID. During compliance test “2001” was configured.
- **Voice URI:** Assign a station extension like “sip:56104@bvwdev.com”, where “bvwdev.com” is the domain created on Contact Center.

AVAYA Contact Center Management Logged in user: webadmin | Logout

View/Edit Add Status Launchpad Help

CCM Servers (Supervisors) AACC-CM

New Agent Details: Agent 2 Server: AACC-CM

User Details

First Name: * Agent
Last Name: * 2
Title:
Department:
Language: English
Comment:
User Type: Agent
Login ID: * 2001
Voice URI: sip:56104@bvwdev.com
IM URI: sip:
Account Type:
☐ Create CCT Agent

Continuing the configuration, check the **Create CCT Agent** box to create a CCT Agent login. List all the Windows user accounts created in the Contact Center server under the **Associate User Account** section. All Windows users created in **Section 8.1** are shown. Select an available Windows user to associate with this agent. In the example below “Agent 2” was selected. Under **Agent Information**, for **Primary Supervisor** select “Supervisor Default” from the drop down menu.

AVAYA **Contact Center Management** Logged in user: webadmin | Logout

View/Edit Add Status Launchpad Help

CCM Servers (Supervisors) AACC-CM

Comment:

☒ Create CCT Agent

CCT Agent Login Details

Domain: AACC-CM
User ID: Agent2

▼ Associate User Account

☒ Search local operating system ☐ Search local security server ☐ Search domain users

Search all user accounts where:
Full Name starts with and includes all users

User Name	Full Name (8)	Status
<input type="radio"/> Administrator		Available
<input type="radio"/> Agent1	Agent 1	Available
<input checked="" type="radio"/> Agent2	Agent 2	Available
<input type="radio"/> Agent3	Agent 3	Available
<input type="radio"/> CallRecordUser	Call RecordUser	Available
<input type="radio"/> Guest		Available
<input type="radio"/> iceAdmin	iceAdmin	Available

▼ Agent Information

Primary Supervisor: * Supervisor Default

Login Status: Logged Out:

Call Presentation: Call_Centre_Administrator

Threshold: Agent_Template

Continuing the configuration, under **Contact Types**, select “Voice” and under **Skillsets** assign a skillset to the agent. In the example below, “Default_Skillset” was given the priority as “1”.

Click on **Submit** to complete the configuration.

The screenshot displays the Avaya Contact Center Management (CCM) web interface. The top navigation bar includes the Avaya logo, the title "Contact Center Management", and the user information "Logged in user: webadmin | Logout". Below the navigation bar, there are tabs for "View/Edit", "Add", "Status", "Launchpad", and "Help".

The main content area is divided into two sections:

- Contact Types:** This section contains a table with columns "Contact Type" and "Priority". The "Voice" row is highlighted with a red box, indicating it is selected.
- Skillsets:** This section contains a table with columns "Skillset Name", "Contact Type", and "Priority". The "Default_Skillset" row is highlighted with a red box, indicating it is selected. The "Priority" for "Default_Skillset" is set to "1".

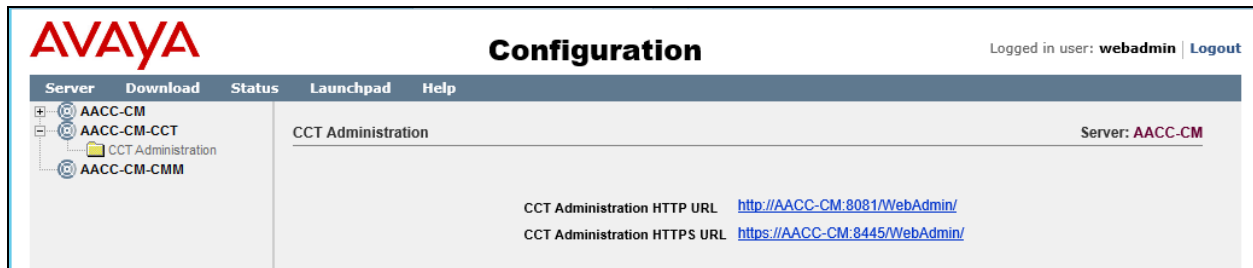
At the bottom of the interface, there are buttons for "Clear", "Submit", "Create Copy", "Create Many", and "Logout Agent". The "Submit" button is highlighted with a red box.

Contact Type	Priority
SMS	
Social_Networking	
Video	
Voice	✓
Voice_Mail	
Web_Communications	

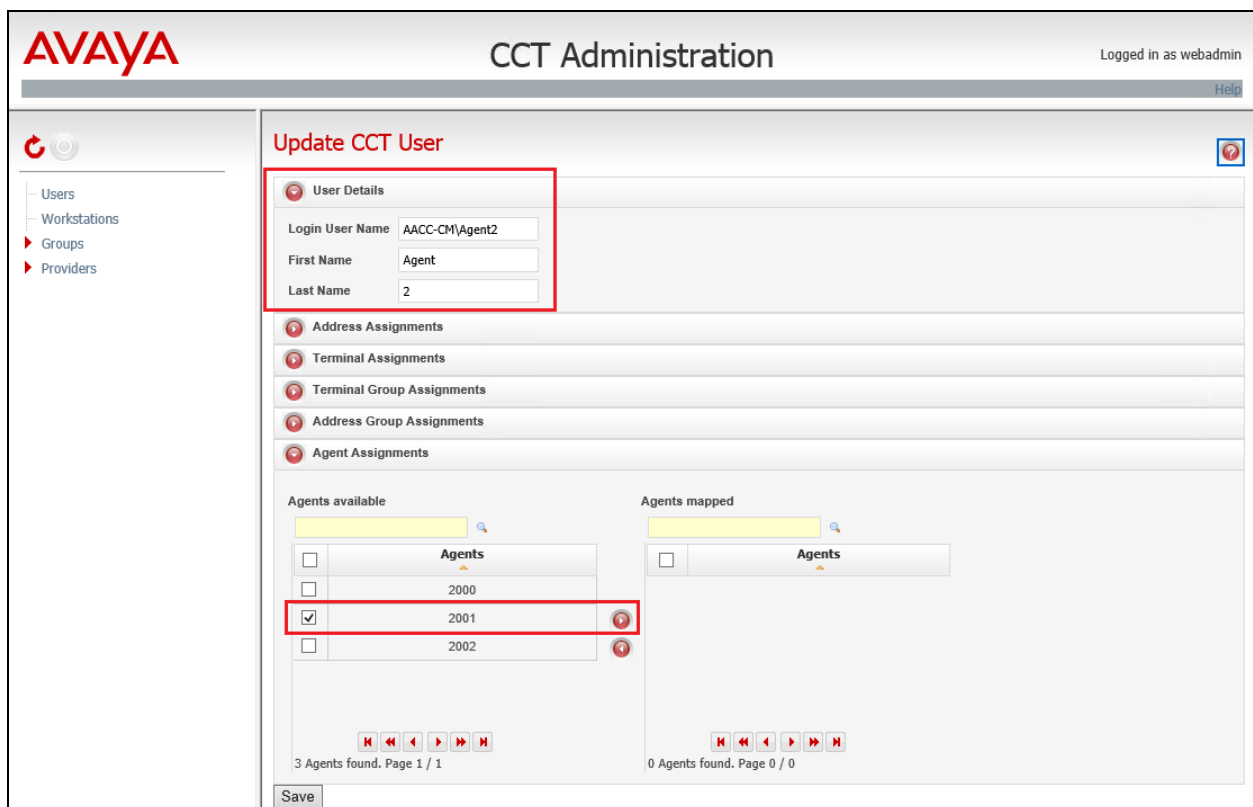
Skillset Name	Contact Type	Priority
Default_Skillset	Voice	1
EM_Default_Skillset	EMail	Unassigned
FX_Default_Skillset	Fax	Unassigned
IM_Default_Skillset	IM	Unassigned
Outbound_Default_Skillset	Outbound	Unassigned

8.3. Configure Users in CCT Administration

From the **Contact Center – Manager Launchpad** screen shown in **Section 8.2**, click on **Configuration**. Navigate to **AACC-CM-CCT → CCT Administration** where **AACC-CM-CCT** is the CCT server configured. Click on the HTTP URL of CCT Administration from the screen show below.



From the **CCT Administration** screen shown below, right click on **Users** on the left pane and click on **Add User** (not shown). On the right pane enter the **User Details** and assign an agent ID under **Agent Assignments**. In the example below, user “AACC-CM\Agent2” was assigned “2001” agent ID based on the agent configuration described in **Section 8.2**. Retain default values for all other fields and click on **Save** to complete the configuration. Note that “AACC-CM” is the Contact Center server name that was used during compliance testing.



Repeat the above for user “CallRecordUser” too, however assign all agent IDs that are being monitored for recording to this CCT user as shown below.

The screenshot displays the Avaya CCT Administration web interface. The top header shows the Avaya logo, the title 'CCT Administration', and the user 'Logged in as webadmin'. A left sidebar contains navigation links for Users, Workstations, Groups, and Providers. The main content area is titled 'Update CCT User' and features several sections: 'User Details' with fields for Login User Name (AACC-CM\CallRecordUse), First Name (Call), and Last Name (RecordUser); 'Address Assignments'; 'Terminal Assignments'; 'Terminal Group Assignments'; 'Address Group Assignments'; and 'Agent Assignments'. The 'Agent Assignments' section is expanded, showing two columns: 'Agents available' (empty) and 'Agents mapped' (containing three entries: 2000, 2001, and 2002). Each entry has a checkbox. At the bottom of each column are pagination controls and status messages: '0 Agents found. Page 0 / 0' and '3 Agents found. Page 1 / 1'. A 'Save' button is located at the bottom left of the main content area.

After applying the above changes, restart all the Contact Center services from the **System Control and Monitor Utility** tool (not shown) of Contact Center server for the above changes to take effect.

9. 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.

9.1. 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**.



9.2. 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 image shows a 'VoIP Configuration' dialog box with the 'Avaya ACM' tab selected. The fields are as follows:

- CTI Option:** A dropdown menu showing 'Avaya ACM'.
- AES Server:** A text box containing '10.10.97.224'.
- DMCC Port:** A text box containing '4721'.
- TSAPI APP ID:** A text box containing 'AVAYA#DEVVMCM'.
- Recording Board ID:** A text box containing '2300'.
- User ID:** A text box containing 'Test'.
- Password:** A text box containing 'XXXXXXXX'.

Below these fields are two groups of buttons:

- Calls To Record:** Three radio buttons: 'All Trunk/Internal Calls' (selected), 'All Trunk Calls', and 'Calls Selected By DN'.
- Buttons:** 'SoftPhone', 'OnDemand', 'More', and 'ACD Groups'.

Below the buttons is a 'Port Mapping' section with a table:

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

At the bottom of the dialog box are the following fields and buttons:

- No. of Log Files:** A text box containing '8'.
- Config File Location:** A button.
- Other Parameters:** A button.
- OK:** A button.
- Cancel:** A button.

9.3. Administer Contact Center Configuration

From the **VoIP Configuration** screen shown in **Section 9.2**, click on **More** button to display the **Avaya ACM Advanced Configuration** as shown below. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Contact Center:** Select the radio button for “AACC”
- **Server:** The IP address of Contact Center.
- **Domain:** The Contact Center server name as mentioned in **Section 8.3**.
- **Port:** The port configured to connect to the CCT Services in Contact Center.
Default value of this port, that Engage uses to connect is “29373”.
- **User:** The Windows user credentials from **Section 8.1**.
- **Password:** The Windows user credentials from **Section 8.1**.

Avaya ACM Advanced Configuration

☐ Mirroring By IP

Ports

SIP Server IP Port

5060

H.323 Server IP Port

0

Trace

☐ SIP Trace
☐ H.323 Trace

Generic Value Mapping

Target Fields

Generic1

Mapped Source

UCID
SkillSet
UUI
VDN

Apply

☐ Use shared DMCC license

Multitenant

None

Default Warning Tone

Disabled

SMS Web Services

☐ Enable SMS Web Services
☐ Use TLS

SMS Port

0

SMS User ID

SMS Password

Sync Device IP via SMS

☐ Enable Device IP Sync

Sync Audit

☒ Daily
☐ Periodic

Time of Day

Period

Contact Center

☐ None
☐ CCE
☒ AACC

AACC

Server

10.10.97.52

Domain

AACC-CM

Port

29373

User

CallRecordUser

Password

OK

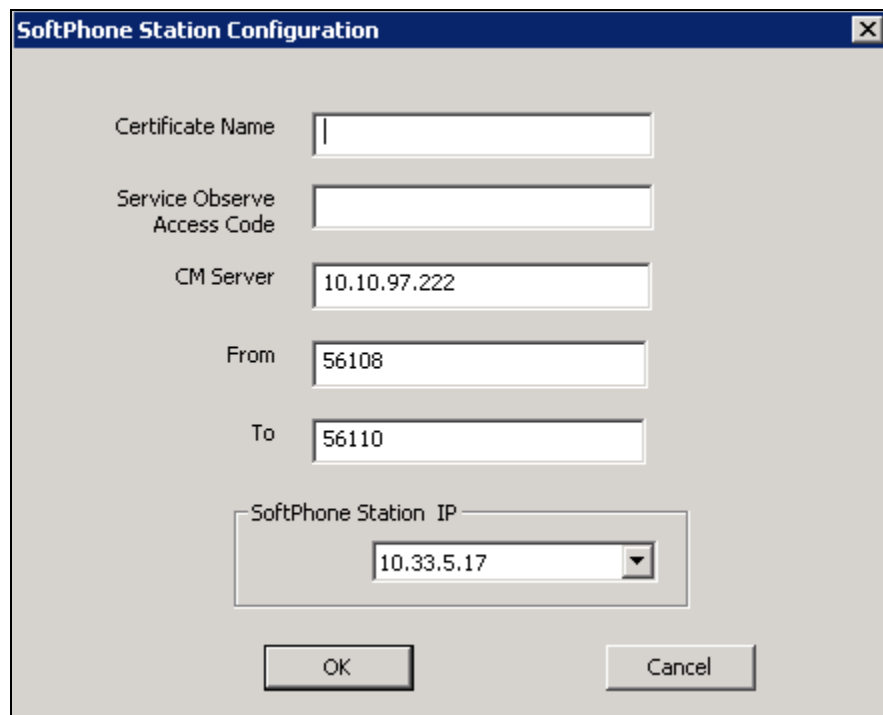
Cancel

9.4. Administer SoftPhones

From the **VoIP Configuration** screen shown in **Section 9.2**, 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	10.10.97.222
From	56108
To	56110
SoftPhone Station IP	10.33.5.17

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

9.5. Administer Device Port Mappings

From the **VoIP Configuration** screen shown in **Section 9.2**, right-click in the empty bottom pane and select **ADD** (not shown). 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: 56104

MAC:

DN: 56104

Recording Channel: 0

Calls To Record

☒ Trunk/Internal Calls ☐ Trunk Calls

Recording Stream

☐ Mirroring ☒ STC Stream

Warning Tone: Inherited

☐ HotDesk DN

Add Cancel

Repeat this section to create device port mappings for all agents in **Section 3**.

VoIP Configuration

Avaya ACM

CTI Option: Avaya ACM

AES Server: 10.10.97.224

DMCC Port: 4721

TSAPI APP ID: AVAYA#DEVVMCM

Recording Board ID: 2300

User ID: Test

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 C...	Beep To
000	56104		56104	STC Stream	Trunk/Internal	Inherited
001	56201		56201	STC Stream	Trunk/Internal	Inherited
002	56204		56204	STC Stream	Trunk/Internal	Inherited

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, 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	devvmaes	established	14	14

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
```


Page 1

REGISTERED IP STATIONS						
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	Skt	Station IP Address/ Gatekeeper IP Address		
56108	9620	IP_API_A	tcp	10.10.97.224		
	1	3.2040		10.10.97.222		
56109	9620	IP_API_A	tcp	10.10.97.224		
	1	3.2040		10.10.97.222		
56110	9620	IP_API_A	tcp	10.10.97.224		
	1	3.2040		10.10.97.222		

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. 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 agent stations from **Section 3**.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Apr 20 10:57:12 2017 from 10.10.10.10
Number of prior failed login attempts: 0
HostName/IP: devvmaes/10.10.10.10
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Thu Apr 20 15:44:12 EDT 2017
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	DevvmCM	1	Talking	Mon Apr 10 12:54:30 2017	Online	17	3	15	15	30


OnlineOffline

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

TSAPI Service StatusTLink StatusUser Status

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 9.4**.



Application Enablement Services

Management Console

Welcome: User cust

Last login: Thu Apr 20 15:42:32 2017 from 10.10.10.10

Number of prior failed login attempts: 0

HostName/IP: devvmaes/10.10.10.10

Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE

SW Version: 7.0.1.0.3.15-0

Server Date and Time: Thu Apr 20 16:59:29 EDT 2017

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
- ▶ User Management
- ▶ Utilities
- ▶ Help

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Thu Apr 20 16:58:49 EDT 2017

Service Uptime:	10 days, 4 hours 4 minutes
Number of Active Sessions:	4
Number of Sessions Created Since Service Boot:	15
Number of Existing Devices:	5
Number of Devices Created Since Service Boot:	30

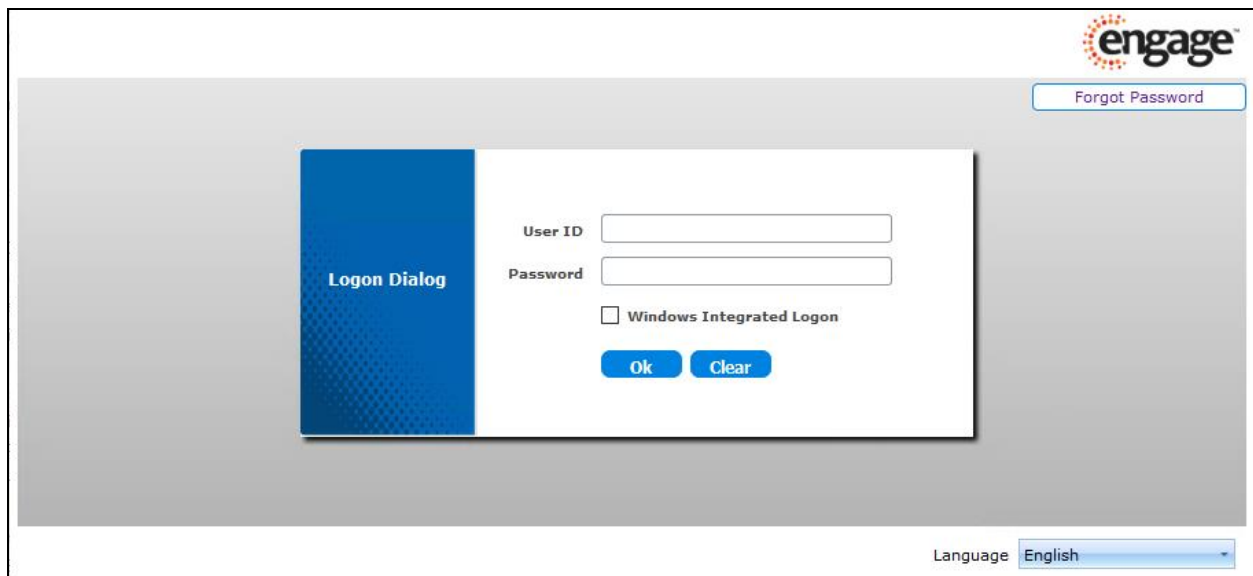
	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	26AF940471EBF98DF03E8CCC8AA14965-13	Test	Engage	10.10.5.17	XML Unencrypted	3
<input type="checkbox"/>	688763F6A1ECC91BC0B234A454006823-14	sip:56103@bvwddev.com	AACC	10.10.97.52:10.10.97.52	TR-87 Encrypted	1
<input type="checkbox"/>	29B82DBA47BF8FF6762A124118E5A423-7	sip:56104@bvwddev.com	AACC	10.10.97.52:10.10.97.52	TR-87 Encrypted	1
<input type="checkbox"/>	FB2B91A53FEB8254B3DF2D4208F17182-4	sip:56204@bvwddev.com	AACC	10.10.97.52:10.10.97.52	TR-87 Encrypted	1

Item 1-4 of 4
1 Go

10.3. Verify TelStrat Engage

Log an agent into a skillset 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. In the top right corner, the Engage logo is visible next to a "Forgot Password" link. The main content area features a "Logon Dialog" window. This dialog has a blue header with the text "Logon Dialog". Below the header, there are two input fields: "User ID" and "Password". Underneath these fields is a checkbox labeled "Windows Integrated Logon". At the bottom of the dialog are two buttons: "Ok" and "Clear". The background of the page is a light gray gradient. In the bottom right corner, there 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 calls made, with proper values in the relevant fields of the Playback Log.

Recordings Evaluation Reports Coaching & E-Learning Administration Recorder Admin Dashboard Welcome, adm adm												
Playback Active Calls												
Recent Calls Custom Search Manage Remarks Play Email Calls Download Calls Combine & Download Download Movie Evaluate Call Coaching Session Clear Filter(s)												
Playback Log Results: 200 No of Records: 200 Go												
	Date	Start Time	End Time	Rec Duration	Hold Duration	Agent ID	Extension	CLID	Dialed Number	Direction	Generic 2	
My Saved Calls	4/18/2017	2:52:43 PM	2:52:52 PM	00:07		2002	56204	56204	56104	Out		
	4/18/2017	2:52:43 PM	2:52:52 PM	00:07		2001	56104	56204	56104	In		
	4/18/2017	2:52:28 PM	2:52:51 PM	00:22	00:00:16	2002	56204	15149626003	57000	In	Default_Skillset	
	4/18/2017	2:49:49 PM	2:49:55 PM	00:06		2002	56204	15149626003	57000	In		
	4/18/2017	2:49:45 PM	2:49:49 PM	00:03		2001	56104	56104	56204	Out		
	4/18/2017	2:49:45 PM	2:49:50 PM	00:03		2002	56204	56104	56204	In		

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

Recordings Evaluation Reports Coaching & E-Learning Administration Recorder Admin Dashboard Welcome, adm adm												
Playback Active Calls												
Recent Calls Custom Search Manage Remarks Play Email Calls Download Calls Combine & Download Download Movie Evaluate Call Coaching Session Clear Filter(s)												
Playback Log Results: 200 No of Records: 200 Go												
	Date	Start Time	End Time	Rec Duration	Hold Duration	Agent ID	Extension	CLID	Dialed Number	Direction	Generic 2	
My Saved Calls	4/18/2017	2:52:43 PM	2:52:52 PM	00:07		2002	56204	56204	56104	Out		
	4/18/2017	2:52:43 PM	2:52:52 PM	00:07		2001	56104	56204	56104	In		
	4/18/2017	2:52:28 PM	2:52:51 PM	00:22	00:00:16	2002	56204	15149626003	57000	In	Default_Skillset	
	4/18/2017	2:49:49 PM	2:49:55 PM	00:06		2002	56204	15149626003	57000	In		
	4/18/2017	2:49:45 PM	2:49:49 PM	00:03		2001	56104	56104	56204	Out		
	4/18/2017	2:49:45 PM	2:49:50 PM	00:03		2002	56204	56104	56204	In		
My Saved Searches	4/18/2017	2:49:31 PM	2:49:50 PM	00:17	00:00:08	2001	56104	15149626003	57000	In	Default_Skillset	
	4/18/2017	2:04:31 PM	2:04:37 PM	00:05		2002	56204	15149626108	57000	In	Default_Skillset	
	4/18/2017	2:04:25 PM	2:04:39 PM	00:13		2001	56104	15149626003	57000	In	Default_Skillset	
	4/18/2017	10:44:14 AM	10:44:21 AM	00:07		2001	56104	56104	56204	Out		
	4/18/2017	10:44:13 AM	10:44:44 AM	00:30		2002	56204	56104	56204	In		
1000 items per page 1 - 200 of 200 items												
Media Player												
Call Started at 2:52:43 PM												
0:00 2:52:43 PM 2:52:52 PM												
Call ID: 1704181452432300006												
Release 5.3.1 - Copyright © 2012 - 2016 TelStrat International Ltd. engage 16:09												

11. Conclusion

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

12. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>.

1. *Administering Avaya Aura® Session Manager*, Release 7.0.1 Issue 2, May 2016.
2. *Deploying Avaya Aura® System Manager*, Release 7.0.1 Issue 2, August 2016.
3. *Administering Avaya Aura® System Manager for Release 7.0.1*, Release 7.0.1 Issue 3, January 2017.
4. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, 03-300509, Issue 2.1, August 2016.
5. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0.1, 555-245-205, Issue 3, October 2016.
6. *Deploying Avaya Aura® Application Enablement Services in Virtualized Environment*, Release 7.0.1 November 2016.
7. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.0.1 Issue 2, August 2016.
8. *Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications*, Release 7.0.1 Issue 01.02, December 2016.
9. *Avaya Aura® Contact Center commissioning for Avaya Aura® Unified Communications*, Release 7.0.1 Issue 01.04, February 2017.

Product documentation for Telstrat may be found at <http://esupport.telstrat.com>.

1. *Install – Setup Engage Server*, Release 5.3, Issue 1.1, December 2016.
2. *Config Guide – Avaya ACM*, Release 5.3, Issue 1.0, December 2016.
3. *Recorder Administration Guide*, Release 5.3, Issue 1.1, December 2016.

©2017 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.