



Avaya Solution & Interoperability Test Lab

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 active 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the TSAPI and DMCC interfaces between Avaya Application Enablement Services system and the TelStrat Engage utilized enabled capabilities of TLS. The CCT interface between Contact Center and the TelStrat Engage does not utilize TLS.

Telstrat Engage supports schedule recording and On Demand recording. With the On Demand recording, agent/supervisor has ability to start the On Demand any time they want during conversation with customer.

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.
- Schedule recording and On Demand recording.
- Use of TLS transport for communication between TelStrat Engage and the TSAPI and DMCC interfaces of Application Enablement Services.

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.
- The On Demand recording feature can be started anytime during the call of the monitored agent, it records the call at the beginning of conversation and not at the time the On Demand recording started.

2.3. Support

Technical support on Engage can be obtained through the following:

- **Phone:** (972) 633-4548
- **Email:** support@serenova.com
- **Website:** <https://www.serenova.com/products/telstrat/>

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 ID and its extensions from Contact Center as shown in the table below.

Device Type	Extension
CDN	5000
Supervisor	3304
Agent ID	1000, 1001, 1002, 1003
Agent Station	3301, 3302, 3401, 3402

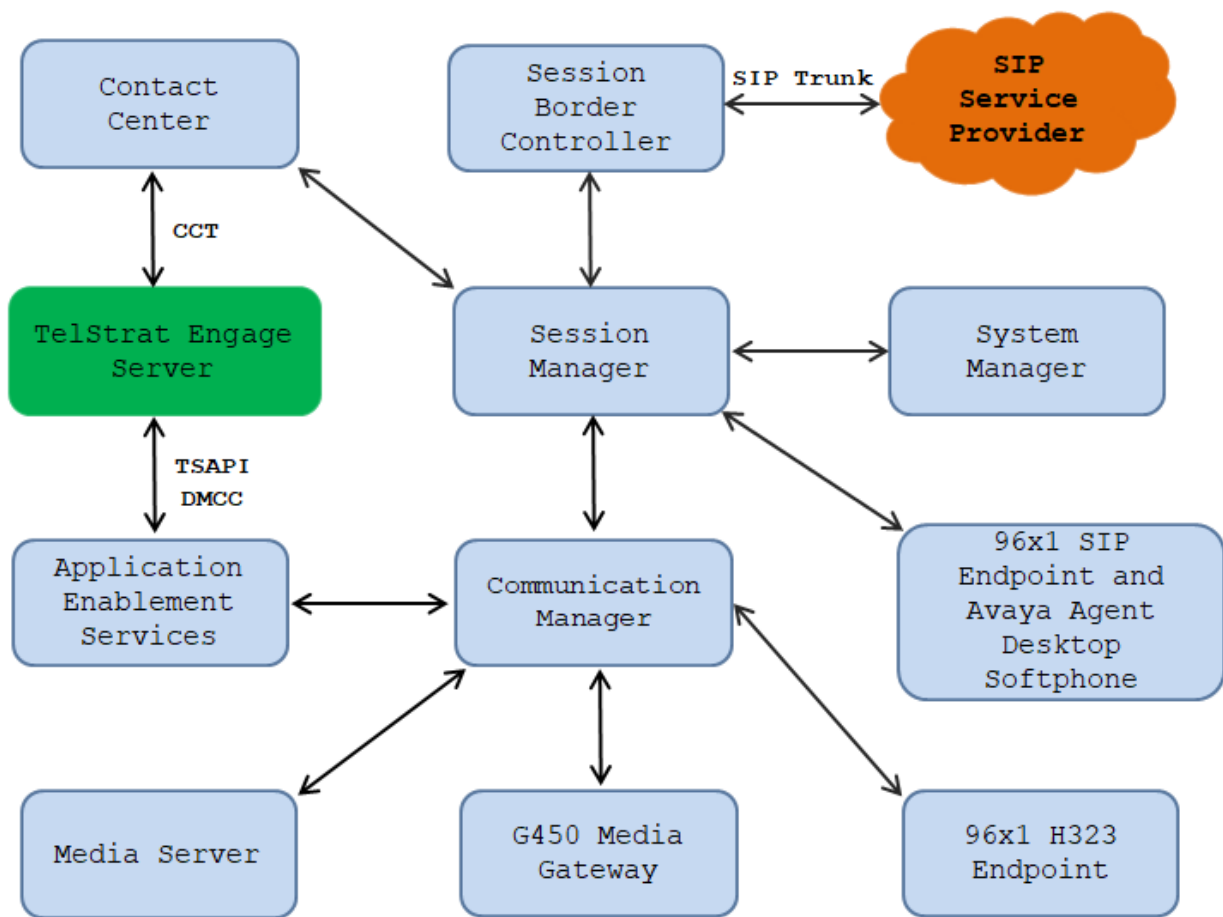


Figure 1: Test Configuration Diagram

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 running on Virtualized Environment	Release 8.1.3 R018x.01.0.890.0 CM 8.1.3.0.0.890.26568
Avaya Aura® System Manager running on Virtualized Environment	Release 8.1.3 Build No. - 8.1.0.0.733078 Software Update Revision No: 8.1.3.0.1011784 Feature Pack 3
Avaya Aura® Session Manager running on Virtualized Environment	Release 8.1.3 8.1.3.0.813014
Avaya Aura® Contact Center running on Virtualized Environment	7.1.1
Avaya Aura® Application Enablement Services	8.1.3.0.0.25
Avaya Session Border Controller for Enterprise	8.1.1
Avaya Aura® Media Server running on Virtualized Environment	8.0.0.0.25
Avaya G450 Media Gateway	41.34.0
Avaya 96x1 IP Deskphones	6.8304 (H.323) 7.1.9.0.8 (SIP))
Avaya 9408 Digital Deskphone	2.0 SP8 (R20)
Avaya Aura Agent Desktop Softphone	7.1.1
TelStrat Engage	5.7.2
TSAPI Client	8.1.3
DMCC SDK	8.1.3

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager.

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	

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:	3331			
Type:	ADJ-IP			
				COR: 1
Name:	AES8			
Unicode Name?	n			

5.3. Administer AE Services

To administer the transport link to AES, use the command “**chang ip-services**”. On Page 1, add an entry with the following values. **Service Type** should be selected as **AESVCS**, enter “y” in the **Enabled**, “procr” in the **Local Node** and 8765 in the **Local Port**.

change ip-services					Page	1 of	4
IP SERVICES							
Service	Enabled	Local	Local	Remote	Remote		
Type		Node	Port	Node	Port		
AESVCS	y	procr	8765				

Go to **Page 4**, enter the following values. **AE Services Server** should be the AES host name, enter a password in the **Password** field and select “y” in the **Enabled** field.

Note: The password entered for **Password** field must match the password on the AES server in the Switch Connection in **Section 6.3**. The **AE Services Server** should match with the host name of the AES server. To obtain the host name of AES server, use the command “**uname -n**” in the Linux command prompt.

change ip-services					Page	4 of	4
AE Services Administration							
Server ID	AE Services Server	Password	Enabled	Status			
1:	aes8	*	y	in use			

5.4. 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 “9640”.
- **Name:** A descriptive name.
- **Security Code:** Enter same value as **Extension**, as required by Engage.
- **IP SoftPhone:** “y”

add station 3371		Page 1 of 5
STATION		
Extension: 3371	Lock Messages? n	BCC: 0
Type: 9640	Security Code: 3371	TN: 1
Port: S000043	Coverage Path 1:	COR: 1
Name: Virtual DMCC IP1	Coverage Path 2:	COS: 1
Unicode Name? n	Hunt-to Station:	Tests? y
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 3371	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
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, three virtual IP softphones were administered as shown below, to allow for simultaneous recording of three monitored agents.

list station 3371 count 3									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Cable	Jack	Cv1/ Cv2	COR/ COS		
3371	S000043	Virtual DMCC IP1					1		
	9640		no				1		
3372	S000044	Virtual DMCC IP2					1		
	9640		no				1		
3373	S000000	Virtual DMCC IP3					1		
	9640		no				1		

6. Configure Application Enablement Services

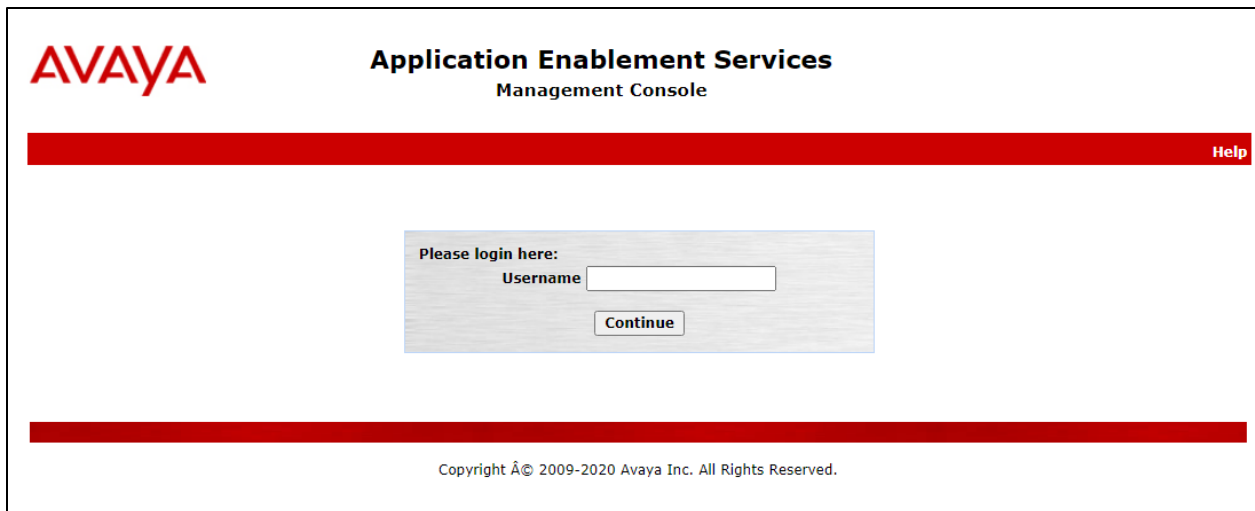
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer Switch Connection
- Administer TSAPI link
- Administer CTI 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 bold, with "Management Console" underneath it. A red horizontal bar spans the width of the page, with a "Help" link on the right side. In the center of the page is a light gray box containing 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, with the copyright notice "Copyright © 2009-2020 Avaya Inc. All Rights Reserved." centered below it.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a user status box on the right. The user status box displays: "Welcome: User cust", "Last login: Thu Jan 28 16:51:04 2021 from 10.33.1.200", "Number of prior failed login attempts: 0", "HostName/IP: aes8/10.33.1.4", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 8.1.3.0.0.25-0", "Server Date and Time: Tue Feb 02 07:41:04 IST 2021", and "HA Status: Not Configured". Below the header is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. The main content area is divided into a left sidebar and a central pane. The sidebar contains a list of menu items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The central pane is titled "Welcome to OAM" and contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:". This is followed by a bulleted list of domains and their functions: "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.", and "Help - Use Help to obtain a few tips for using the OAM Help system". At the bottom of the central pane, a note states: "Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain."


6.2. Verify License

Select **Licensing → WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials, and navigate to display installed licenses (not shown).

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" menu item selected in the left sidebar. The top header is the same as the previous screenshot. The red navigation bar now shows "Licensing" on the left and "Home | Help | Logout" on the right. The central pane is titled "Licensing" and contains three paragraphs of instructions: "If you are setting up and maintaining the WebLM, you need to use the following:", "If you are importing, setting up and maintaining the license, you need to use the following:", and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:". Each paragraph is followed by a bulleted list of items: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". At the bottom of the central pane, a red note states: "NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page".

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.

View peak usage	Licensed Features		
APS_CMS_Connectors			
▶APS_CMS_Connectors			
Configure Centralized Licensing	13 Items  Show All ▼		
ASBCE	Feature (License Keyword)	Expiration date	Licensed capacity
▶Session_Border_Controller_E_AE	Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	500
Configure Centralized Licensing	AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	500
CCTR	AES HA LARGE VALUE_AES_HA_LARGE	permanent	500
▶ContactCenter	AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	500
CE	Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	500
▶COLLABORATION_ENVIRONMENT	CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	500
CMS	AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	500
▶CMS	AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	500
Configure Centralized Licensing	DLG VALUE_AES_DLG	permanent	500
COLLABORATION_DESIGNER	TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	500
▶Collaboration_Designer			
COMMUNICATION_MANAGER			
▶Call_Center			
▶Communication_Manager			

6.3. Administer Switch Connection

Select **Communication Manager Interface** → **Switch Connection** from the left pane of the **Management Console**, enter a name in **Switch Connection** box and click **Add** button (not shown). Enter the password as configured in **Section 5.3** in the **Switch Password** and **Confirm Switch Password** and check on **Processor Ethernet** field if the Processor Ethernet is used in Communication Manager. Click **Apply** button to save the configuration.

Note that the **Enable TLS Certificate Hostname Validation** field should be unchecked if the DNS server is not used to resolve the hostname to IP address in Application Enablement Services and Communication Manager.

Communication Manager Interface | Switch Connections Home | Help | Logout

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

Connection Details - interopcm

Switch Password: [password field]
Confirm Switch Password: [password field]
Msg Period: 30 Minutes (1 - 72)
Provide AE Services certificate to switch: ☒
Secure H323 Connection: ☐
Processor Ethernet: ☒
Enable TLS Certificate Hostname Validation: ☐
Apply Cancel

Select the **interopcm** switch connection that has been added above and select **Edit PE/CLAN IPs** to add IP address of switch connection.

Communication Manager Interface | Switch Connections Home | Help | Logout

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

Switch Connections

[text field] Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> interopcm	Yes	30	1

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

Enter IP address of either CLAN interface or Processor Ethernet of Communication Manager in the box and click **Add/Edit Name of IP** button to add the IP.

Communication Manager Interface | Switch Connections Home | Help | Logout

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

Edit Processor Ethernet IP - interopcm

10.33.1.6

Name or IP Address	Status
10.33.1.6	In Use

Select **Edit H.323 Gatekeeper** button to add an IP address of gate keeper, the Gatekeeper IP address in this case is also the Processor Ethernet.

Communication Manager Interface | Switch Connections Home | Help | Logout

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

Edit H.323 Gatekeeper - interopcm

Name or IP Address

☒ 10.33.1.6

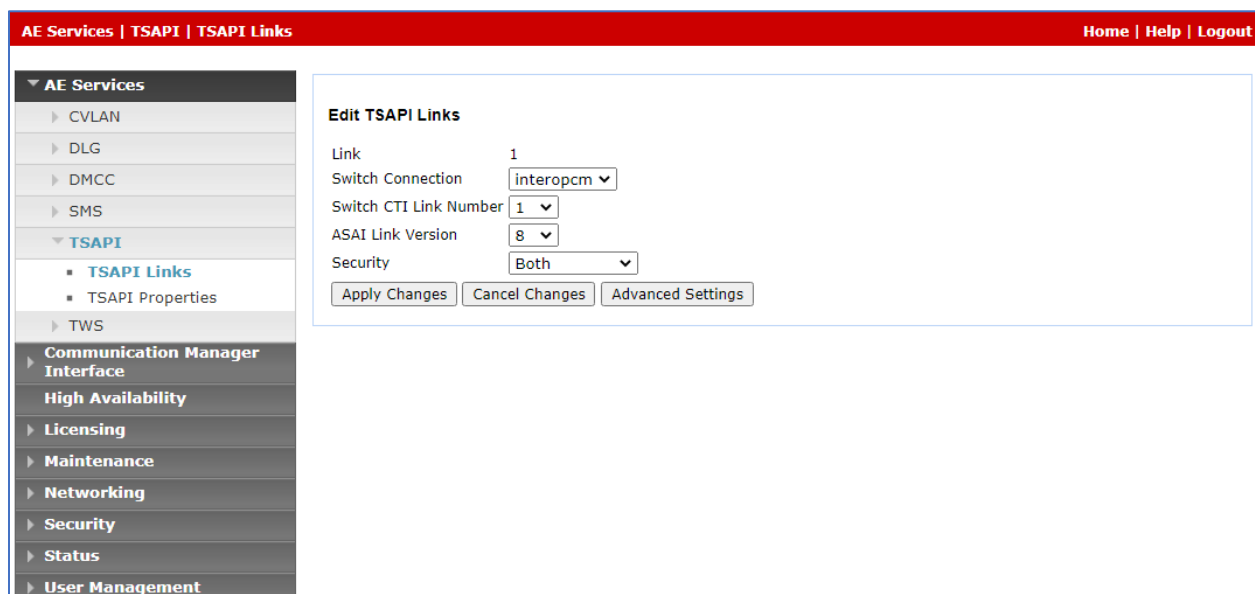
6.4. Administer TSAPI Link

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 'TSAPI Links' management console. The left sidebar contains a tree view with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'TWS', 'Communication Manager Interface', 'High Availability', and 'Licensing'. Under 'TSAPI', 'TSAPI Links' is selected. 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 three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

The **Add TSAPI Links** screen is displayed in the right side. 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 “**interopcm**” which is added in the step above. For **Switch CTI Link Number**, select the CTI link number 1 from **Section 5.2**, select the version “8” in the ASAI Link Version field and select **Both** in the **Security** dropdown menu to support both unencrypted and encrypted TSAPI link.



The screenshot shows the 'Edit TSAPI Links' screen. The left sidebar is the same as the previous screenshot. The main content area is titled 'Edit TSAPI Links' and contains a form with the following fields: 'Link' (text input with value '1'), 'Switch Connection' (dropdown menu with value 'interopcm'), 'Switch CTI Link Number' (dropdown menu with value '1'), 'ASAI Link Version' (dropdown menu with value '8'), and 'Security' (dropdown menu with value 'Both'). Below the form are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

6.5. Administer CTI 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 shows the 'Edit User' form within the Avaya User Management application. The interface has a red header bar with 'User Management | User Admin | List All Users' on the left and 'Home | Help | Logout' on the right. A left-hand navigation pane contains a tree structure with categories like 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Service Admin', 'User Admin', 'Utilities', and 'Help'. The 'User Admin' section is expanded, showing 'Add User', 'Change User Password', 'List All Users' (highlighted), 'Modify Default Users', and 'Search Users'. The main content area is titled 'Edit User' and contains a form with the following fields: 'User Id' (text box with 'test'), 'Common Name' (text box with 'Engage'), 'Surname' (text box with 'Lifesize'), 'User Password' (text box), 'Confirm Password' (text box), 'Admin Note' (text box), 'Avaya Role' (dropdown menu with 'None' selected), 'Business Category' (text box), 'Car License' (text box), 'CM Home' (text box), 'Css Home' (text box), 'CT User' (dropdown menu with 'Yes' selected), 'Department Number' (text box), 'Display Name' (text box), 'Employee Number' (text box), 'Employee Type' (text box), 'Enterprise Handle' (text box), 'Given Name' (text box), 'Home Phone' (text box), 'Home Postal Address' (text box), and 'Initials' (text box).

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 11** to configure access privileges for the Engage user from **Section 6.5**.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Feb 24 14:13:14 2021 from 10.33.1.200
Number of prior failed login attempts: 0
HostName/IP: aes8/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Feb 24 14:19:33 IST 2021
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

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.

Ports	
CVLAN Ports	
Unencrypted TCP Port	9999
Encrypted TCP Port	9998
DLG Port	
TCP Port	5678
TSAPI Ports	
TSAPI Service Port	450
Local TLINK Ports	
TCP Port Min	1024
TCP Port Max	1039
Unencrypted TLINK Ports	
TCP Port Min	1050
TCP Port Max	1065
Encrypted TLINK Ports	
TCP Port Min	1066
TCP Port Max	1081
DMCC Server Ports	
Unencrypted Port	4721
Encrypted Port	4722
TR/87 Port	4723

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: Wed Feb 24 14:13:14 2021 from 10.33.1.200
Number of prior failed login attempts: 0
HostName/IP: aes8/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Feb 24 14:27:21 IST 2021
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
▶ User Management
▶ Utilities
▶ Help

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

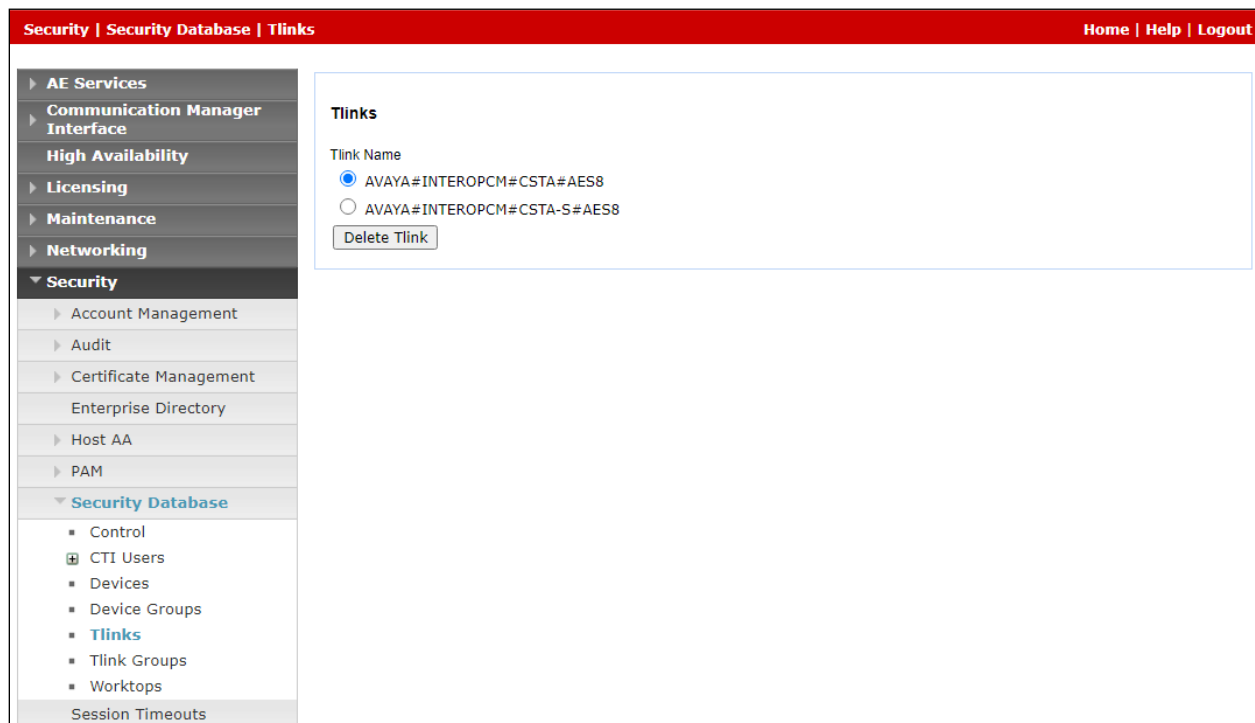
For status on actual services, please use [Status and Control](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart 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 unsecure Tlink name is “**AVAYA#INTEROPCM#CSTA#AES8**” and the secure Tlink name is “**AVAYA#INTEROPCM#CSTA-S#AES8**”. Note the use of the switch connection “**interopcm**” from **Section 6.3** as part of the Tlink name.



7. 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:

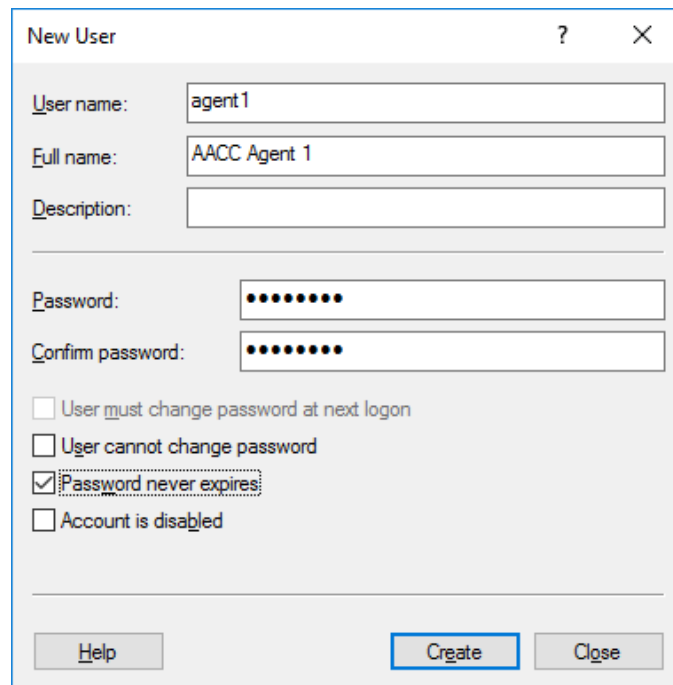
- Configure Windows users
- Configure Agents
- Configure Users in CCT Administration

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.

7.1. 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.

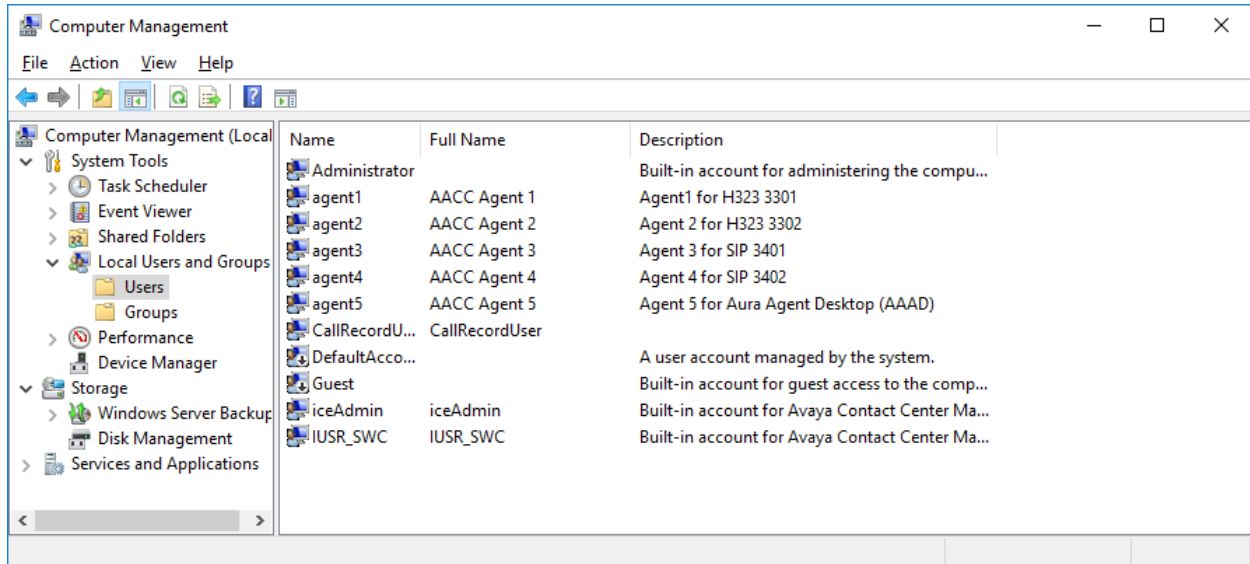


The screenshot shows the 'New User' dialog box with the following details:

- User name:** agent1
- Full name:** AACC Agent 1
- Description:** (empty)
- Password:** (masked with dots)
- Confirm password:** (masked with dots)
- ☐ User must change password at next logon
- ☐ User cannot change password
- ☒ Password never expires
- ☐ Account is disabled
- Buttons:** Help, Create, Close

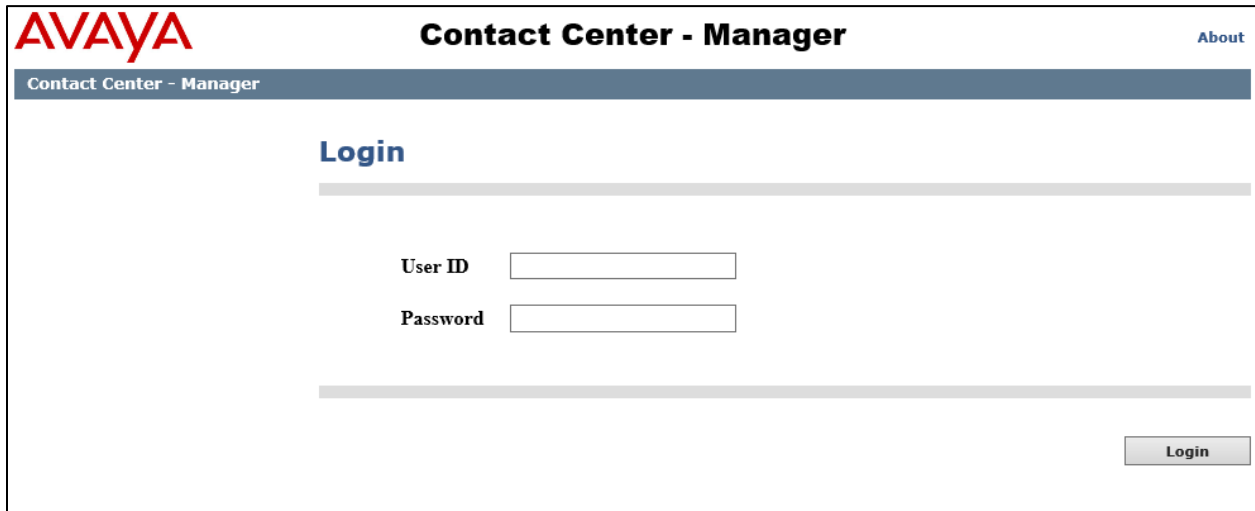
Repeat the same procedure to create three more agents and “CallRecordUser” that will be used in **Section 8.3** for the Engage application.

The screen below shows the **Computer Management** window with four Windows users created as **agent1**, **agent2**, **agent3**, **agent4** and **CallRecordUser**. Similarly more users can be created as required.



7.2. 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.



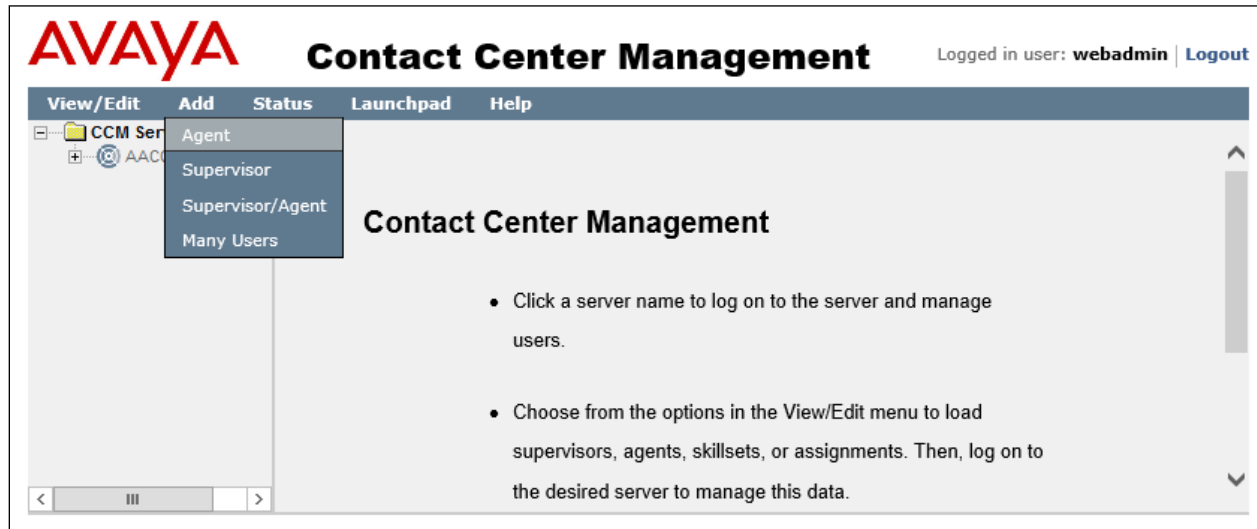
The screenshot shows the Avaya Contact Center - Manager web interface. At the top left is the Avaya logo. The title "Contact Center - Manager" is centered at the top, with an "About" link on the right. Below the title is a dark blue header bar with the text "Contact Center - Manager". The main content area has a "Login" heading. Below the heading are two input fields: "User ID" and "Password". A "Login" button is located at the bottom right of the form.

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. The title "Contact Center - Manager" is centered at the top, with links for "About", "Audit Trail", "Change Password", and "Logout" on the right. Below the title is a dark blue header bar with the text "Launchpad". The main content area has a "Launchpad" heading. Below the heading is a grid of icons and links. The links are: "Contact Center Management", "Access and Partition Management", "Real-Time Reporting", "Historical Reporting", "Call Recording and Quality Monitoring", "Prompt Management", "Configuration", "Scripting", "Emergency Help", "Outbound", "Multimedia", and "Data Management". At the bottom of the screen, it says "Last successful login: 1/20/2021 8:31:08 AM".

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 “1001” was configured.
- **Voice URI:** Assign a station extension like “sip:3301@bvwdev.com”, where “bvwdev.com” is the domain created on Contact Center.

AVAYA Contact Center Management

Logged in user: Administrator Web | Change Password | Logout

View/Edit Add Status Launchpad Help

CCM Servers (Supervisors)

AACC-CM

Supervisor Default

New Agent Details: Agent 1

Server: AACC-CM

User Details

First Name: * Agent

Last Name: * 1

Title:

Department:

Language: English

Comment:

User Type: Agent

Login ID: * 1001

Voice URI: sip:3301@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 7.1** are shown. Select an available Windows user to associate with this agent. In the example below “Agent 1” was selected. Under **Agent Information**, for **Primary Supervisor** select “Supervisor Default” from the drop down menu.

AVAYA Contact Center Management Logged in user: Administrator Web | [Change Password](#) | [Logout](#)

View/Edit Add Status Launchpad Help

CCM Servers (Supervisors) AACC-CM Supervisor Default

Comment:

☒ Create CCT Agent

CCT Agent Login Details

Domain
User ID:

▼ **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 (11)	Status
<input type="radio"/> Administrator		Available
<input type="radio"/> agent1	AACC Agent 1	Assigned
<input type="radio"/> agent2	AACC Agent 2	Available
<input type="radio"/> agent3	AACC Agent 3	Available
<input type="radio"/> agent4	AACC Agent 4	Available
<input type="radio"/> agent5	AACC Agent 5	Available
<input type="radio"/> CallRecordUser	CallRecordUser	Available

▼ **Agent Information**

Primary Supervisor: * Supervisor Default

Call Presentation: Call_Centre_Administrator

Login Status: Logged Out

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.

AVAYA Contact Center Management Logged in user: **Administrator Web** | [Change Password](#) | [Logout](#)

View/Edit **Add** **Status** **Launchpad** **Help**

CCM Servers (Supervisors)

- AACC-CM
 - Supervisor Default

Agent Information

Primary Supervisor: * Supervisor Default ▼ Call Presentation: Call_Centre_Administrator ▼

Login Status: Logged Out Threshold: Agent_Template ▼

Contact Types

Contact Type	
IM	<input type="checkbox"/>
Voice	<input checked="" type="checkbox"/>

Skillsets

Assign Skillsets

Show all skillsets on server AACC-CM where:

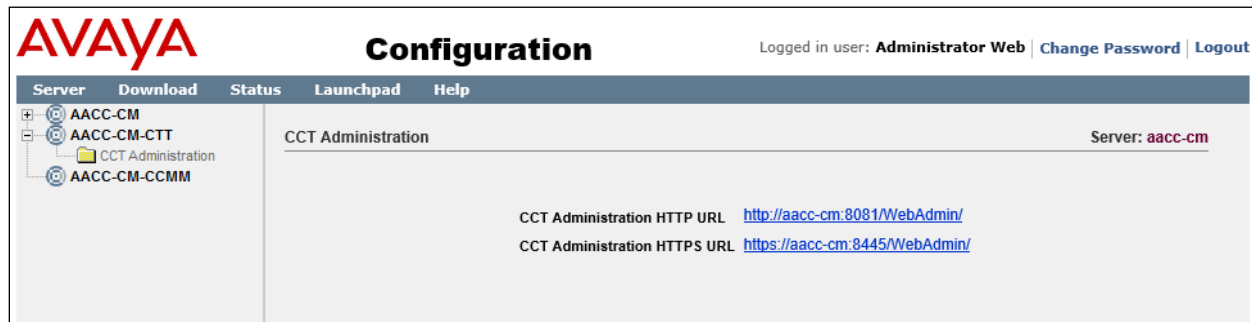
Skillset name: contains ▼

Skillset Name (2)	Contact Type	Priority
Default_Skillset	Voice	1 ▼
IM_Default_Skillset	IM	Unassigned ▼

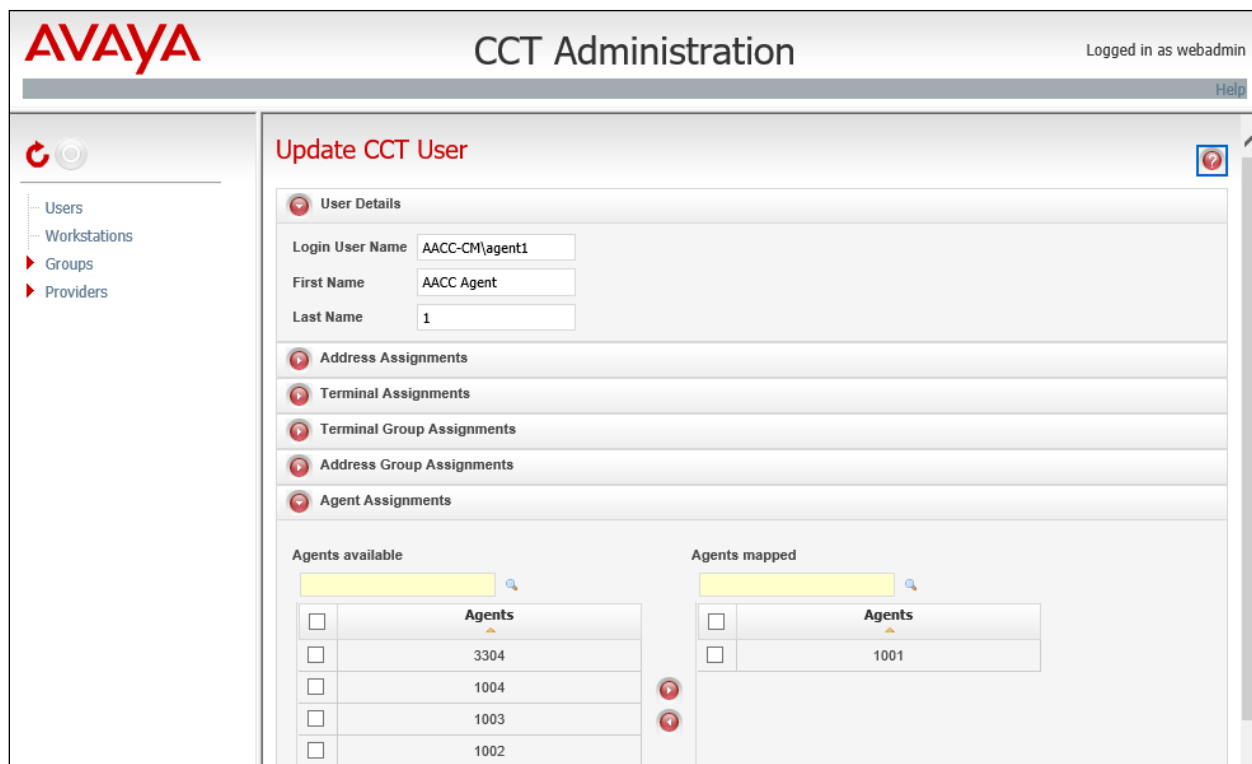
Partitions

7.3. Configure Users in CCT Administration

From the **Contact Center – Manager Launchpad** screen shown in **Section 7.2**, 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\Agent1” was assigned to the agent ID “1001”. 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”, however assign all agent IDs that are being monitored for recording to this CCT user as shown below in the **Agent Assignments** section.

AVAYA CCT Administration Logged in as webadmin [Help](#)

Update CCT User

User Details

Login User Name: AACC-CM\CallRecordUse
First Name: CallRecordUser
Last Name: none

Address Assignments

Terminal Assignments

Terminal Group Assignments

Address Group Assignments

Agent Assignments

Agents available

	Agents
<input type="checkbox"/>	3304

Agents mapped

	Agents
<input type="checkbox"/>	1001
<input type="checkbox"/>	1002
<input type="checkbox"/>	1003
<input type="checkbox"/>	1004

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.

8. Configure TelStrat Engage

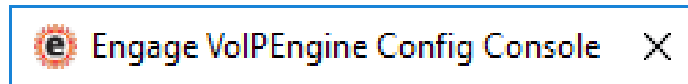
This section provides the procedures for configuring Engage. The procedures include the following areas:

- Launch VoIP engine
- Administer CTI
- Administer ACD groups
- Administer softphones
- Administer device port mappings
- Administer OnDemand Recording

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 → TelStrat Engage → VOIP Engine Configuration**, to display the **Engage VoIP Engine Config Console** window below. From the keyboard, press **Alt** key and then **Enter** key, and 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 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 settings are as follows:

- CTI Option:** Avaya ACM (dropdown)
- AES Server:** 10.33.1.4
- DMCC Port:** 4721
- TSAPI APP ID:** AVAYA#INTEROPC
- Recording Board ID:** 2300
- User ID:** test
- Password:** ****

Calls To Record:

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

Buttons: SoftPhone, OnDemand, More, ACD Groups

Port Mapping:

<input checked="" type="checkbox"/> Recording Chan...	Device ID	Mac Address	DN	Record With	Trunk/Internal C...	Beep Tone
---	-----------	-------------	----	-------------	---------------------	-----------

Footer:

- No. of Log Files:** 8
- Config File Location:** [empty]
- Other Parameters:** [empty]
- OK** button
- Cancel** button

8.3. Administer Contact Center Configuration

From the **VoIP Configuration** screen shown in **Section 8.2**, 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 “aacc-cm” in this case.
- **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 “CallRecordUser” user from **Section 7.1**.
- **Password:** The Windows password of the “CallRecordUser” user from **Section 7.1**.

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

☐ 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

Generic Value Mapping

Target Fields

Generic1

Mapped Source

UCID

SkillSet

UIT

VDN

Apply

Contact Center

☐ None
 ☐ CCE
 ☒ AACC

AACC

Server

10.33.1.55

Domain

aacc-cm

Port

29373

User

CallRecordUser

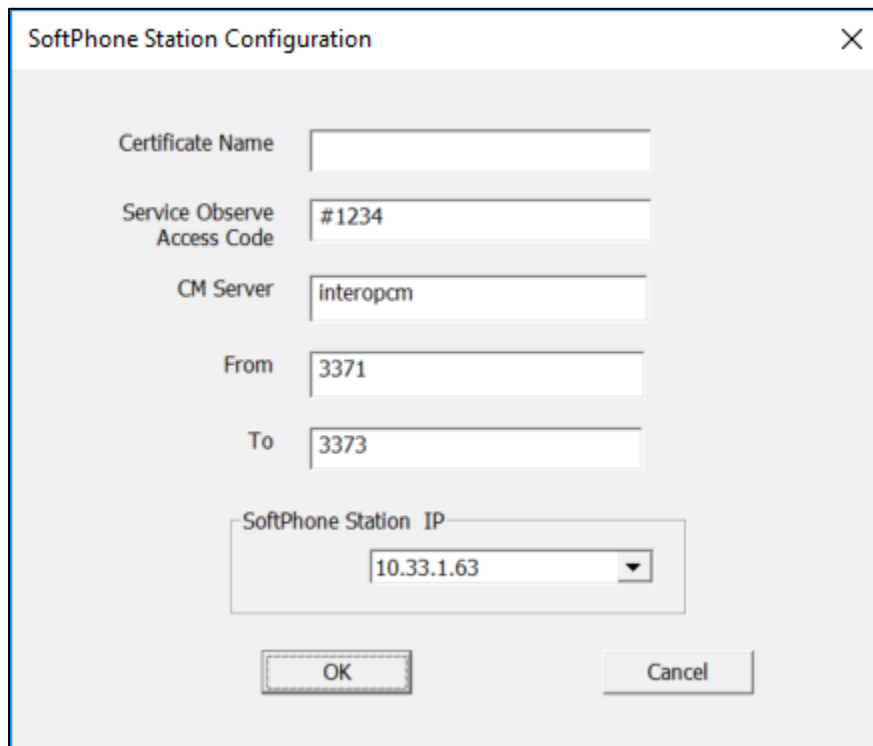
Password

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:** Server name of the H.323 gatekeeper from **Section 6.3**.
- **From:** The extension of the first virtual IP softphone from **Section 5.8**.
- **To:** The extension of the last virtual IP softphone from **Section 5.8**.



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

Field	Value
Certificate Name	
Service Observe Access Code	#1234
CM Server	interopcm
From	3371
To	3373
SoftPhone Station IP	10.33.1.63

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

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** (not shown). The **Device And CommSrv Port Mapping** screen is displayed.

For **Device ID**, enter the first agent station extension. 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

MAC

DN

Recording Channel

Calls To Record

☒ Trunk/Internal Calls ☐ Trunk Calls

Recording Stream

☐ Mirroring

☒ STC Stream Warning Tone

☐ HotDesk DN

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

VoIP Configuration [X]

Avaya ACM |

CTI Option: Avaya ACM (dropdown)

AES Server: 10.33.1.4

DMCC Port: 4721

TSAPI APP ID: AVAYA#INTEROPC

Recording Board ID: 2300

User ID: test

Password: [masked]

Calls To Record:

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

Buttons: SoftPhone, OnDemand, More, ACD Groups

Port Mapping:

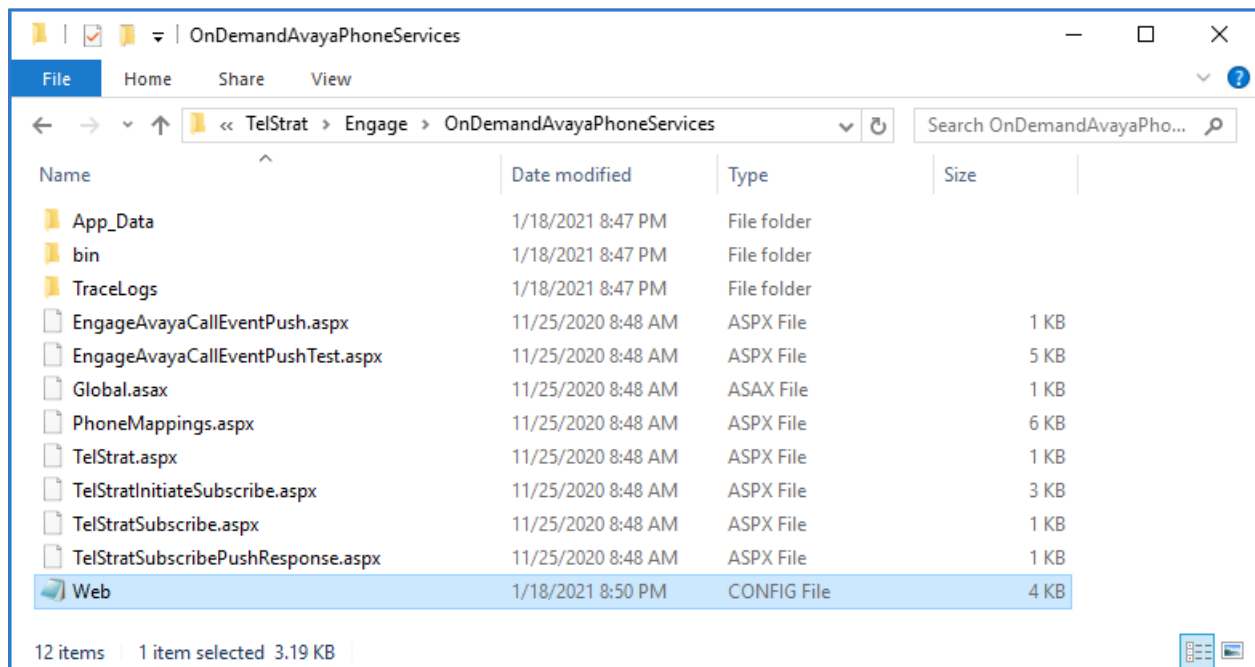
Recording Chan...	Device ID	Mac Address	DN	Record With	Trunk/Internal C...	Beep Tone
000	3301		3301	STC Stream	Trunk/Internal	Inherited
001	3302		3302	STC Stream	Trunk/Internal	Inherited
002	3402		3402	STC Stream	Trunk/Internal	Inherited
003	3401		3401	STC Stream	Trunk/Internal	Inherited

No. of Log Files: 8

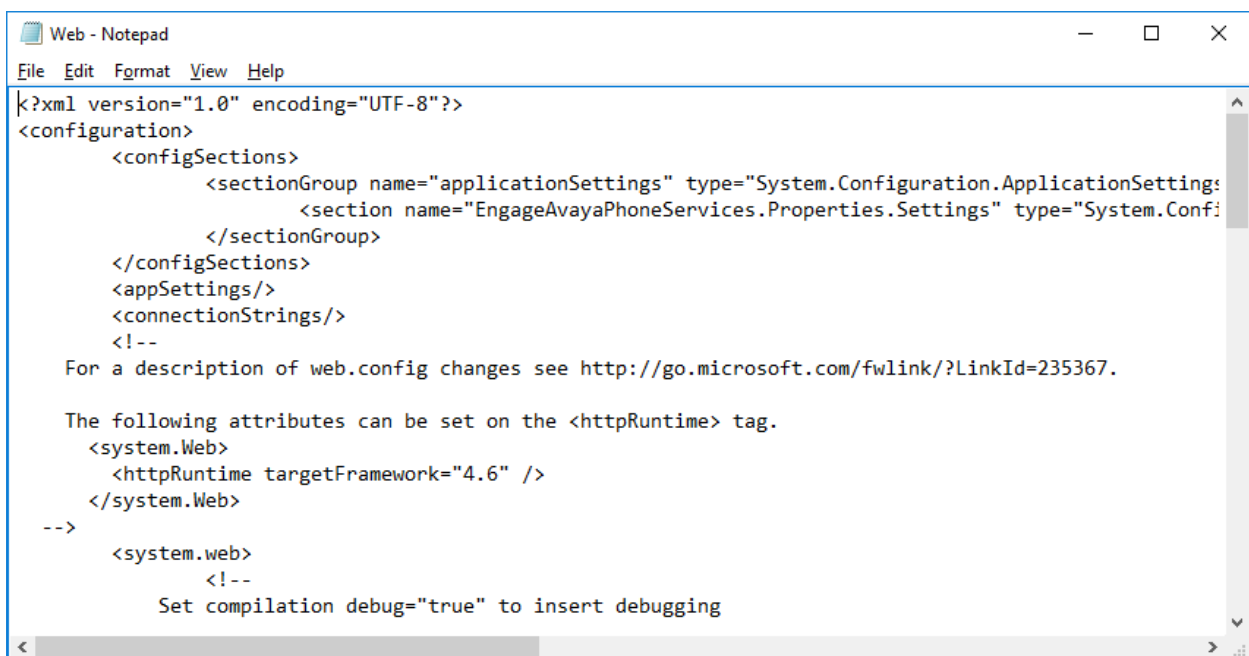
Buttons: Config File Location, Other Parameters, OK, Cancel

8.6. Administer OnDemand Recording

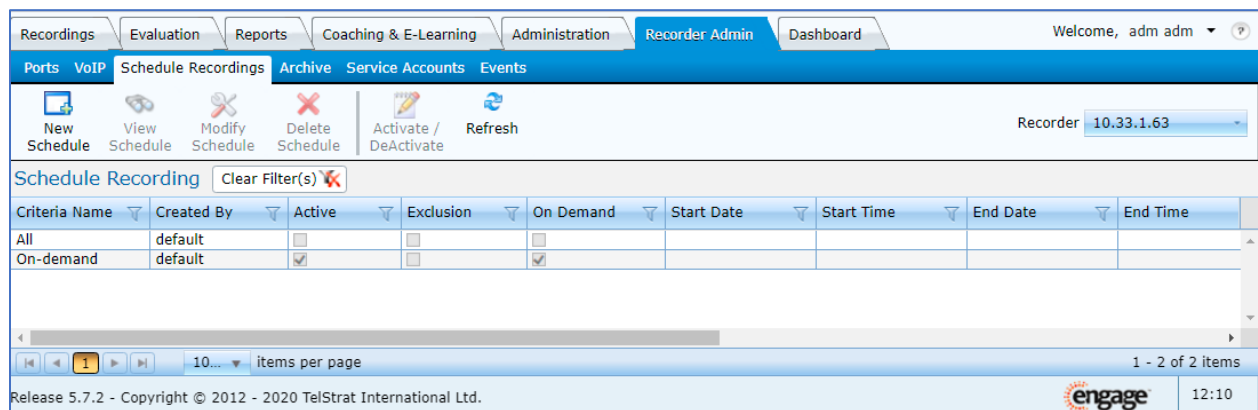
From the Engage server, navigate to the **C:\Program Files\TelStrat\Engage\OnDemandAvayaPhoneServices** directory to locate the **Web.config** file shown below.



Open the **Web.config** file with the Windows WordPad application. Scroll down to the bottom of the file. For **WebServerIPAddress** (not shown), enter the IP address of the Engage server running the Web Server component.



Open internet browser and access to the Web Portal by entering the IP address of the Engage server. Navigate to **Recorder Admin → Schedule Recordings**, create **OnDemand Schedule Recording** criteria and activate the criteria.



From the **VoIP Configuration** screen shown in **Section 8.2**, click on **OnDemand** to display the **OnDemand Configuration** screen. The **OnDemand Configuration** screen is displayed. Check **OnDemand Feature**. For **PUSH Server Name**, enter the IP address of the Engage server running the Web Server component.

OnDemand Configuration

☒ OnDemand Feature

Post Account

User ID

User Password

PUSH Server Name

10.33.1.63

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	8	no	aes8	established	15	15

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 8.4** 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 Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address
3371	9640	IP_API_A	10.33.1.4
tcp	1	3.2040	10.33.1.6
3372	9640	IP_API_A	10.33.1.4
tcp	1	3.2040	10.33.1.6
3373	9640	IP_API_A	10.33.1.4
tcp	1	3.2040	10.33.1.6

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 6.4** and that the **Associations** column reflects the total number of monitored agent stations.



Application Enablement Services

Management Console

Welcome: user: root
Last login: Tue Feb 2 07:37:14 2021 from 10.33.1.200
Number of prior failed login attempts: 0
HostName/IP: aes8/10.33.1.4
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Wed Feb 03 16:36:44 IST 2021
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

▶ Logs

▶ Log Manager

▼ 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 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	interopcm	1	Talking	Sat Jan 16 16:47:03 2021	Online	18	4	15	15	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 *test* user name from **Section 6.5**, and that the **# of Associated Devices** column reflects the total number of softphone extensions from **Section 8.4**.

Status | Status and Control | DMCC Service Summary

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

Log Manager

▼ 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 seconds

Session Summary [Device Summary](#)

Generated on Wed Feb 03 16:39:06 IST 2021

Service Uptime: 7 days, 0 hours 1 minutes

Number of Active Sessions: 5

Number of Sessions Created Since Service Boot: 12

Number of Existing Devices: 3

Number of Devices Created Since Service Boot: 6

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	BE873903CE26DBF91D7EC01C548420C1-9	sip:3301@bvwddev.com	AACC	10.33.1.55:10.33.1.55	TR-87 Encrypted	1
<input type="checkbox"/>	F3F498A8C95AB4FE348495C19F90B622-10	sip:3302@bvwddev.com	AACC	10.33.1.55:10.33.1.55	TR-87 Encrypted	1
<input type="checkbox"/>	8AC8F8144D38EE29B5A8C876D04672C2-8	sip:3401@bvwddev.com	AACC	10.33.1.55:10.33.1.55	TR-87 Encrypted	1
<input type="checkbox"/>	7E6DE07F97F7C77FC4309CA91E475A94-11	sip:3402@bvwddev.com	AACC	10.33.1.55:10.33.1.55	TR-87 Encrypted	1
<input type="checkbox"/>	5154C88E53E316F5F19BD8BC7EF06BC4-6	test	Engage	10.33.1.63	XML Unencrypted	3

Terminate Sessions

Show Terminated Sessions

KP; Reviewed:
SPOC 3/21/2021

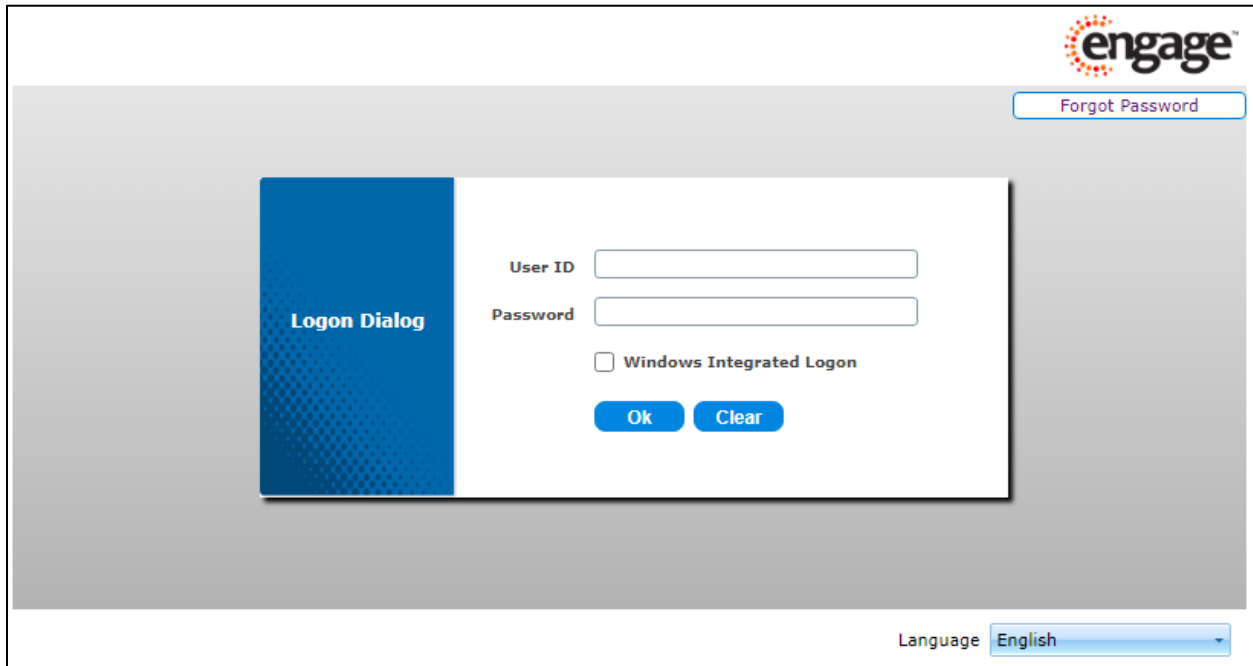
Solution & Interoperability Test Lab Application Notes
©2021 Avaya Inc. All Rights Reserved.

40 of 44
Engage-AACC71

9.3. 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's logon dialog. The dialog box is titled "Logon Dialog" and features a blue header. It contains two input fields: "User ID" and "Password". Below 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 web page shows the Engage logo in the top right corner, a "Forgot Password" link, and a "Language" dropdown menu set to "English" at the bottom right.

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.

The screenshot shows the Engage dashboard with the 'Recordings' tab selected. The 'Playback Log' table is displayed, showing a list of call recordings. The table has columns for Date, Start Time, End Time, Status, Rec Duration, Hold Duration, User First, User Last, Agent ID, and Extension. The table is filtered to show 100 results out of 200 records.

Date	Start Time	End Time	Status	Rec Duration	Hold Duration	User First	User Last	Agent ID	Extension
2/1/2021	11:23:58 AM	11:24:06 AM		00:00:08				1001	3301
1/29/2021	10:15:45 AM	10:16:30 AM		00:00:45	00:00:11	AACC Agent	3	1003	3401
1/29/2021	10:15:44 AM	10:16:30 AM		00:00:45	00:00:06	AACC Agent	4	1004	3402
1/29/2021	10:14:06 AM	10:14:58 AM		00:00:52				1001	3301
1/29/2021	10:14:06 AM	10:14:58 AM		00:00:52				1001	3301
1/29/2021	10:00:20 AM	10:01:04 AM		00:00:44				1001	3301
1/29/2021	8:49:54 AM	8:50:21 AM		00:00:27				1001	3301
1/29/2021	8:38:11 AM	8:38:40 AM		00:00:29				1001	3301
1/29/2021	8:36:07 AM	8:36:27 AM		00:00:19				1001	3301
1/29/2021	8:06:36 AM	8:06:44 AM		00:00:07		AACC Agent	3	1003	3401
1/29/2021	8:06:03 AM	8:06:44 AM		00:00:40				1001	3301

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

The screenshot shows the Engage dashboard with the 'Recordings' tab selected. The 'Playback Log' table is displayed, showing a list of call recordings. The table is filtered to show 100 results out of 200 records. The entry for 1/29/2021, 10:15:45 AM is highlighted. Below the table, the 'Media Player' is shown, displaying the call recording for the selected entry. The media player shows the call start time as 1/29/2021, 10:15:45 AM and the call ID as 210129101545QX02300003.

To start the On Demand recording, from the Engage dashboard select **Recordings** → **Active Calls** tab, select an active call in the list and select **Save** button.

10. 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**.

11. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] Administering Avaya Aura® Application Enablement Services, Release 8.1, December 2020
- [2] Deploying Avaya Aura® Communication Manager, Release 8.1, December 2020
- [3] Administering Avaya Aura® Communication Manager, Release 8.1, October 2020
- [4] Deploying Avaya Aura® Session Manager, Release 8.1 October 2020
- [5] Upgrading Avaya Aura® Session Manager, Release 8.1, October 2020
- [6] Administering Avaya Aura® Session Manager, Release 8.1, October 2020
- [7] Avaya Aura® Contact Center Server Administration, Release 7.1, October 2020

Product documentation for TelStrat may be found at <https://www.serenova.com/products/telstrat/>.

- [1] Install – Setup Engage Server, Release 5.7, Issue 2.24, December 2020.
- [2] Config Guide – Avaya ACM, Release 5.7, Issue 2.24, December 2020.
- [3] Recorder Administration Guide, Release 5.7, Issue 2.24, December 2020.

©2021 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.