



Avaya Solution & Interoperability Test Lab

Application Notes for dvsAnalytics Encore 6.0.5 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 using Service Observing – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for dvsAnalytics Encore 6.0.5 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 using Service Observing. dvsAnalytics Encore is a call recording solution.

In the compliance testing, dvsAnalytics Encore used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and used the Service Observing feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture the media associated with the monitored stations for call recording.

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 dvsAnalytics Encore 6.0.5 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 using Service Observing. dvsAnalytics Encore is a call recording solution.

In the compliance testing, dvsAnalytics Encore used the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and used the Service Observing feature via the Avaya Aura® Application Enablement Services Device, Media, and Call Control (DMCC) interface to capture the media associated with the monitored stations for call recording.

The TSAPI interface is used by dvsAnalytics Encore to monitor skill groups and agent stations on Avaya Aura® Communication Manager. The DMCC interface is used by dvsAnalytics Encore to register virtual IP softphones, and for adding the softphones to active calls using the Service Observing method.

When there is an active call at a monitored agent station, dvsAnalytics Encore is informed of the call via event reports from the TSAPI interface. dvsAnalytics Encore starts the call recording by using the Service Observing feature from the DMCC 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 recording.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Encore application, the application automatically requests monitoring on skill groups and agent stations, performs device queries on agent stations, and registers the virtual IP softphones.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for recordings. Necessary user actions such as hold and reconnect were performed from the agent telephones to test various call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Encore.

The verification of tests included use of Encore logs for proper message exchanges, and use of Encore 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 Encore:

- Handling of TSAPI messages in areas of event notification and value queries.
- Use of DMCC registration services to register and un-register virtual IP softphones.
- Use of DMCC physical devices services and monitoring services to activate Service Observing for the virtual IP softphones and to obtain media for call recordings.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711, forwarding, long duration, multiple calls, multiple agents, conference, and transfer.

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

2.2. Test Results

All test cases were executed. The following were the observations on Encore from the compliance testing.

- For the conference scenarios, the recording entry for the conference-from agent can contain multiple Service Observing confirmation tones, due to different softphones added for different portions of the conference call.
- The Consultation Call parameter associated with the recording entries applied to the attended transfer and conference scenarios.
- The number of softphones to configure need to take into account the small interval of 500ms that a softphone will not be available between recordings.

2.3. Support

Technical support on Encore can be obtained through the following:

- **Phone:** (800) 910-4564
- **Email:** Support@dvsAnalytics.com

3. Reference Configuration

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, Encore monitored the skill groups and agent stations shown in the table below.

Device Type	Extension
VDN	60001, 60002
Skill Group	61001, 61002
Supervisor	65000
Agent Station	65001, 66002
Agent ID	65881, 65882

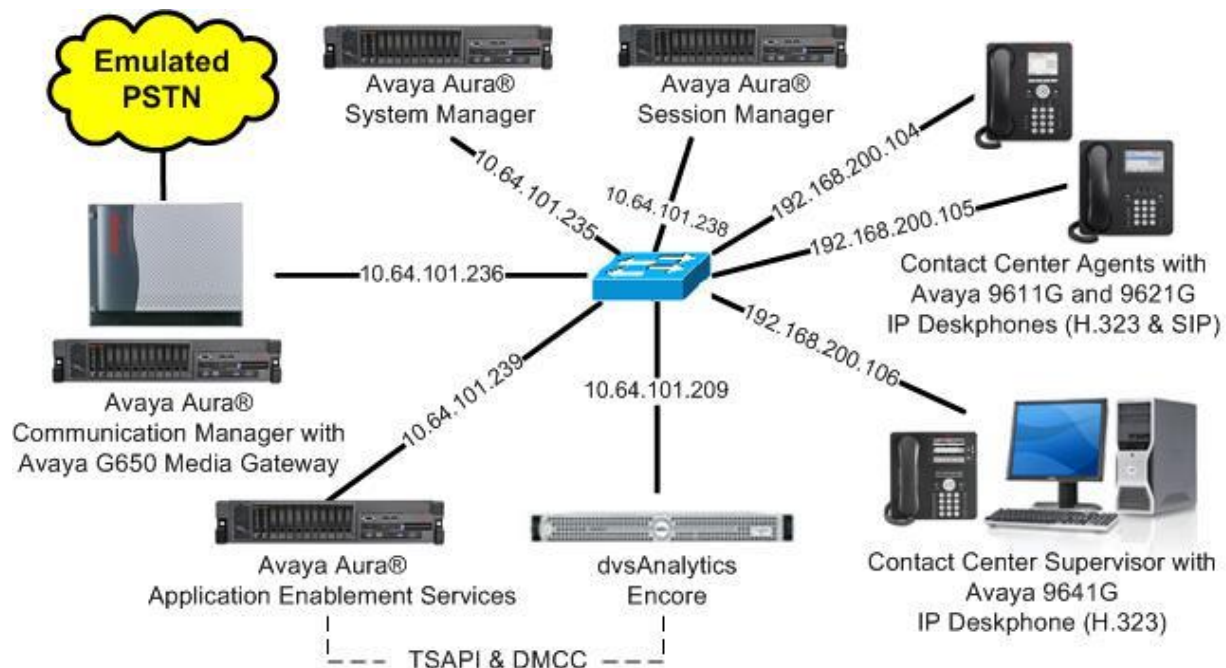


Figure 1: Compliance Testing Configuration

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	7.0.1.1 (7.0.1.1.0.441.23169)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.2.15-0)
Avaya Aura® Session Manager in Virtual Environment	7.0 .1 (7.0.1.0.701007)
Avaya Aura® System Manager in Virtual Environment	7.0 .1 (7.0.1.0.064859)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6229
Avaya 9621G IP Deskphone (SIP)	7.0.1.1.5
dvsAnalytics Encore on Windows Server 2012 R2 <ul style="list-style-type: none">Avaya TSAPI Windows Client (csta32.dll)Avaya DMCC XML	6.0.5 Standard 6.3.3.103 6.1

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 IP codec set
- Administer system parameters features
- Administer class of restriction
- Administer agent stations
- 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

Navigate to **Page 7**, and verify that the **Service Observing (Basic)** customer option is set to “y”.

display system-parameters customer-options		Page	7 of 11
CALL CENTER OPTIONAL FEATURES			
Call Center Release: 7.0			
ACD?	y	Reason Codes?	y
BCMS (Basic)?	y	Service Level Maximizer?	n
BCMS/VuStats Service Level?	y	Service Observing (Basic)?	y
BSR Local Treatment for IP & ISDN?	y	Service Observing (Remote/By FAC)?	y
Business Advocate?	n	Service Observing (VDNs)?	y
Call Work Codes?	y	Timed ACW?	y
DTMF Feedback Signals For VRU?	y	Vectoring (Basic)?	y
Dynamic Advocate?	n	Vectoring (Prompting)?	y

5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 60111		
Type: ADJ-IP		
COR: 1		
Name: AES CTI Link		

5.3. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with Encore. For **Audio Codec**, enter “G.711MU”, which is the only codec type supported by Encore along with variant “G.711A”. In the compliance testing, this IP codec set was assigned to the agents and to the virtual IP softphones used by Encore.

change ip-codec-set 1		Page 1 of 2
IP Codec Set		
Codec Set: 1		
Audio Codec	Silence Suppression	Frames Per Pkt
1: G.711MU	n	2
2:		
		Packet Size (ms)
		20

5.4. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Create Universal Call ID (UCID)**, which is located on **Page 5**. For **UCID Network Node ID**, enter an available node ID.

change system-parameters features	Page 5 of 19
FEATURE-RELATED SYSTEM PARAMETERS	
SYSTEM PRINTER PARAMETERS	
Endpoint:	Lines Per Page: 60
SYSTEM-WIDE PARAMETERS	
Switch Name:	
Emergency Extension Forwarding (min): 10	
Enable Inter-Gateway Alternate Routing? n	
Enable Dial Plan Transparency in Survivable Mode? n	
COR to Use for DPT: station	
EC500 Routing in Survivable Mode: dpt-then-ec500	
MALICIOUS CALL TRACE PARAMETERS	
Apply MCT Warning Tone? n MCT Voice Recorder Trunk Group:	
Delay Sending RElease (seconds): 0	
SEND ALL CALLS OPTIONS	
Send All Calls Applies to: station Auto Inspect on Send All Calls? n	
Preserve previous AUX Work button states after deactivation? n	
UNIVERSAL CALL ID	
Create Universal Call ID (UCID)? y UCID Network Node ID: 27	

Navigate to **Page 11**. Set **Service Observing: Warning Tone** to the needed setting per customer requirement, and enable **Allow Two Observers in Same Call**, as shown below.

change system-parameters features	Page 11 of 20
FEATURE-RELATED SYSTEM PARAMETERS	
CALL CENTER SYSTEM PARAMETERS	
EAS	
Expert Agent Selection (EAS) Enabled? y	
Minimum Agent-LoginID Password Length:	
Direct Agent Announcement Extension:	
Message Waiting Lamp Indicates Status For: station	
Delay:	
VECTORIZING	
Converse First Data Delay: 0	
Second Data Delay: 2	
Converse Signaling Tone(msec): 100	
Pause (msec): 70	
Prompting Timeout(secs): 10	
Interflow-qpos EWT Threshod: 2	
Reverse Star/Pound Digit For Collect Step? n	
Available Agent Adjustments for BSR? n	
BSR Tie Strategy: 1st-found	
Store VDN Name in Station's Local Call Log? n	
SERVICE OBSERVING	
Service Observing: Warning Tone? n	
or Conference Tone? n	
Allowed with Exclusion: Service Observing? n	
SSC? n	
Allow Two Observers in Same Call? y	

Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Encore.

```
change system-parameters features                                     Page 13 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER MISCELLANEOUS
    Callr-info Display Timer (sec): 10
        Clear Callr-info: next-call
    Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n

        Agent/Caller Disconnect Tones? n
        Interruptible Aux Notification Timer (sec): 3
        Zip Tone Burst for Callmaster Endpoints: double

ASAI
    Copy ASAI UUI During Conference/Transfer? y
    Call Classification After Answer Supervision? y
        Send UCID to ASAI? y
        For ASAI Send DTMF Tone to Call Originator? y
    Send Connect Event to ASAI For Announcement Answer? n
    Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.5. Administer Class of Restriction

Enter the “change cor n” command, where “n” is the class of restriction (COR) number used for integration with Encore. Set the **Can Be Service Observed** and **Can Be A Service Observer** fields to “y”, as shown below. For the compliance testing, this COR was assigned to the agent stations and virtual IP softphones.

If desired, separate COR can be used for each parameter enablement. The COR with **Can Be Service Observed** enabled needs to be assigned to the agent stations, and the COR with **Can Be A Service Observer** enabled needs to be assigned to the virtual IP softphones.

```
change cor 2                                                         Page 1 of 23
                                CLASS OF RESTRICTION

    COR Number: 2
    COR Description:

        FRL: 0
        Can Be Service Observed? y
        Can Be A Service Observer? y
        Time of Day Chart: 1
        Priority Queuing? n
        Restriction Override: none
        Restricted Call List? n

        APLT? y
        Calling Party Restriction: none
        Called Party Restriction: none
        Forced Entry of Account Codes? n
        Direct Agent Calling? n
        Facility Access Trunk Test? n
        Can Change Coverage? n
```

5.6. Administer Agent Stations

Use the “change station n” command, where “n” is the first agent station extension from **Section 3**. For **COR**, enter the COR number from **Section 5.5**.

change station 65001		Page 1 of 5
STATION		
Extension: 65001	Lock Messages? n	BCC: 0
Type: 9611	Security Code: *	TN: 1
Port: S00102	Coverage Path 1: 1	COR: 2
Name: CM7 Station 1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Location: 1	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 65001	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:	Media Complex Ext:	
Survivable COR: internal	IP SoftPhone? n	
Survivable Trunk Dest? y	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

Repeat this section to administer all agent stations from **Section 3**. In the compliance testing, two agent stations were administered as shown below.

list station 65001 count 2									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack		
65001	S00102	CM7 Station 1			1	2			
	9611		no			1			
66002	S00004	Avaya, SIP 2			1	2			
	9621SIPCC		no			1			

5.7. 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 “4610”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **COR:** The COR number from **Section 5.5**.
- **IP SoftPhone:** “y”

add station 65771		Page 1 of 5	
STATION			
Extension: 65771	Lock Messages? n	BCC: 0	
Type: 4610	Security Code: 65771	TN: 1	
Port: IP	Coverage Path 1:	COR: 2	
Name: Encore Virtual #1	Coverage Path 2:	COS: 1	
	Hunt-to Station:	Tests: y	
STATION OPTIONS			
Location:	Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1		
	Message Lamp Ext: 65771		
Speakerphone: 2-way	Mute Button Enabled? y		
Display Language: english	Expansion Module? n		
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		

Navigate to **Page 4**, and add a “serv-obsrv” button as shown below.

add station 65771		Page 4 of 6	
STATION			
SITE DATA			
Room:		Headset? n	
Jack:		Speaker? n	
Cable:		Mounting: d	
Floor:		Cord Length: 0	
Building:		Set Color:	
ABBREVIATED DIALING			
List1:	List2:	List3:	
BUTTON ASSIGNMENTS			
1: call-appr	7:		
2: call-appr	8:		
3: call-appr	9:		
4: serv-obsrv	10:		
5:	11:		

Repeat this section to administer the desired number of virtual IP softphones. In the compliance testing, four virtual IP softphones were administered as shown below.

list station 65771 count 4									
STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Data Ext	Cv1/ Cv2	COR/ COS	Cable/ Jack		
65771	S00003	Encore Virtual #1				2			
	4610		no			1			
65772	S00009	Encore Virtual #2				2			
	4610		no			1			
65773	S00013	Encore Virtual #3				2			
	4610		no			1			
65774	S00016	Encore Virtual #4				2			
	4610		no			1			

6. Configure Avaya Aura® Application Enablement Services

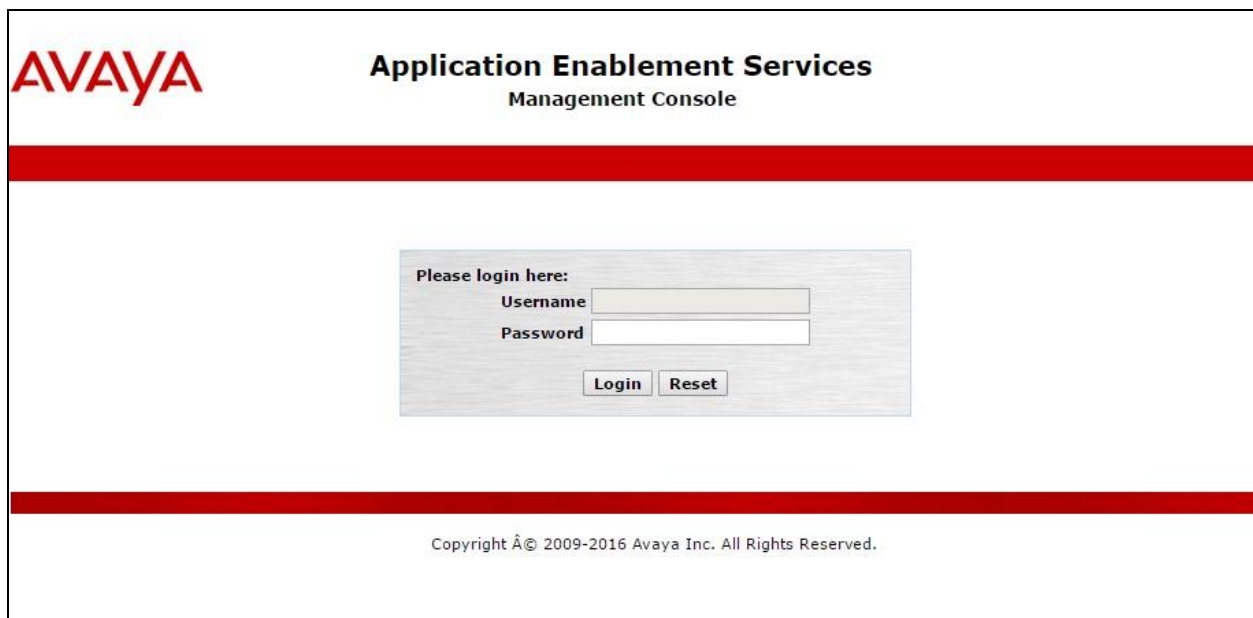
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer Encore user
- Administer security database
- Administer ports
- Restart services
- Obtain Tlink name

6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A thick red horizontal bar spans the width of the page. Below this bar is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located below the login box. At the bottom of the page, centered, is the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner provides user information: "Welcome: User", "Last login: Tue Sep 13 09:45:41 2016 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.1.0.2.15-0", "Server Date and Time: Tue Sep 13 09:48:55 EDT 2016", and "HA Status: Not Configured". The left sidebar contains a navigation menu with options: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area, titled "Welcome to OAM", explains that the OAM Web provides tools for managing the AE Server and lists administrative domains: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also notes that these domains can be served by one administrator for all or separate administrators for each.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Sep 13 09:45:41 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 13 09:48:55 EDT 2016
HA Status: Not Configured

Home | Help | Logout

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

Welcome to OAM

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

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

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

6.2. Verify License

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

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The top header and welcome message are identical to the previous screenshot. The left sidebar now highlights "Licensing" and includes sub-options: "WebLM Server Address", "WebLM Server Access", and "Reserved Licenses". The main content area, titled "Licensing", provides instructions for setting up and maintaining the WebLM, importing and setting up the license, and administering TSAPI Reserved Licenses or DMCC Reserved Licenses. It lists the following required actions: WebLM Server Address, WebLM Server Access, and Reserved Licenses.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Sep 13 09:45:41 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 13 09:48:55 EDT 2016
HA Status: Not Configured

Home | Help | Logout

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

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

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.

TLT; Reviewed: Solution & Interoperability Test Lab Application Notes 16 of 38
SPOC 10/26/2016 ©2016 Avaya Inc. All Rights Reserved. Encore-AES7-SO

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, Last login: Tue Sep 13 09:45:41 2016 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes7/10.64.101.239, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 7.0.1.0.2.15-0, Server Date and Time: Tue Sep 13 09:48:55 EDT 2016, HA Status: Not Configured. The left navigation pane shows 'AE Services' expanded, with 'TSAPI' selected, and 'TSAPI Links' highlighted. 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 “cm7” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.

The screenshot shows the AVAYA Application Enablement Services Management Console with the 'Add TSAPI Links' screen. The left navigation pane shows 'AE Services' expanded, with 'TSAPI' selected, and 'TSAPI Links' highlighted. The main content area is titled 'Add TSAPI Links' and contains form fields for: Link (dropdown with value 1), Switch Connection (dropdown with value cm7), Switch CTI Link Number (dropdown with value 1), ASAI Link Version (dropdown with value 7), and Security (dropdown with 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 “cm7”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane has 'Communication Manager Interface' expanded, with 'Switch Connections' selected. The main area displays a table of switch connections. The table has four columns: 'Connection Name', 'Processor Ethernet', 'Msg Period', and 'Number of Active Connections'. There is one entry with 'cm7' as the connection name, 'No' for processor ethernet, '30' for msg period, and '1' for the number of active connections. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The top right of the console shows user information and login details.

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

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

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

6.5. Administer Encore User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “Yes” from the drop-down list. Retain the default value in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 13 09:45:41 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 13 09:53:15 EDT 2016
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Idencore

* Common Nameencore

* Surnameencore

* User Password*****

* Confirm Password*****

Admin Note

Avaya RoleNone ▼

Business Category

Car License

CM Home

Css Home

CT UserYes ▼

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

6.6. Administer Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The right pane shows the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page, which contains two unchecked checkboxes and an "Apply Changes" button.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Sep 13 09:45:41 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 13 09:48:55 EDT 2016
HA Status: Not Configured

Security | Security Database | Control [Home](#) | [Help](#) | [Logout](#)

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

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

☐ Enable SDB for DMCC Service

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

[Apply Changes](#)

6.7. Administer Ports

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

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

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 13 09:45:41 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 13 09:48:55 EDT 2016
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

Enabled Disabled

☒ ☐

☒ ☐

Enabled Disabled

☒ ☐

Enabled 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**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 13 09:45:41 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 13 09:48:55 EDT 2016
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](#)

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 Encore.

In this case, the associated Tlink name is “AVAYA#CM7#CSTA#AES7”. Note the use of the switch connection “CM7” from **Section 6.3** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation bar shows "Security | Security Database | Tlinks" and links for "Home | Help | Logout". The left sidebar contains a tree view of the application's structure, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", shows a single Tlink named "AVAYA#CM7#CSTA#AES7" with a "Delete Tlink" button.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Tue Sep 13 09:45:41 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 13 09:48:55 EDT 2016
HA Status: Not Configured

Security | Security Database | Tlinks Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
Devices
Device Groups
Tlinks

Tlinks

Tlink Name
AVAYA#CM7#CSTA#AES7
Delete Tlink

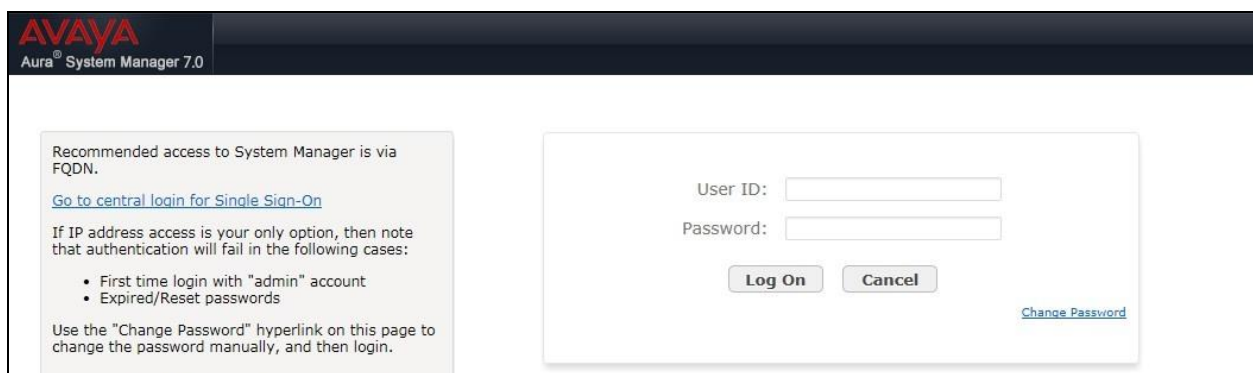
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

7.1. Launch System Manager

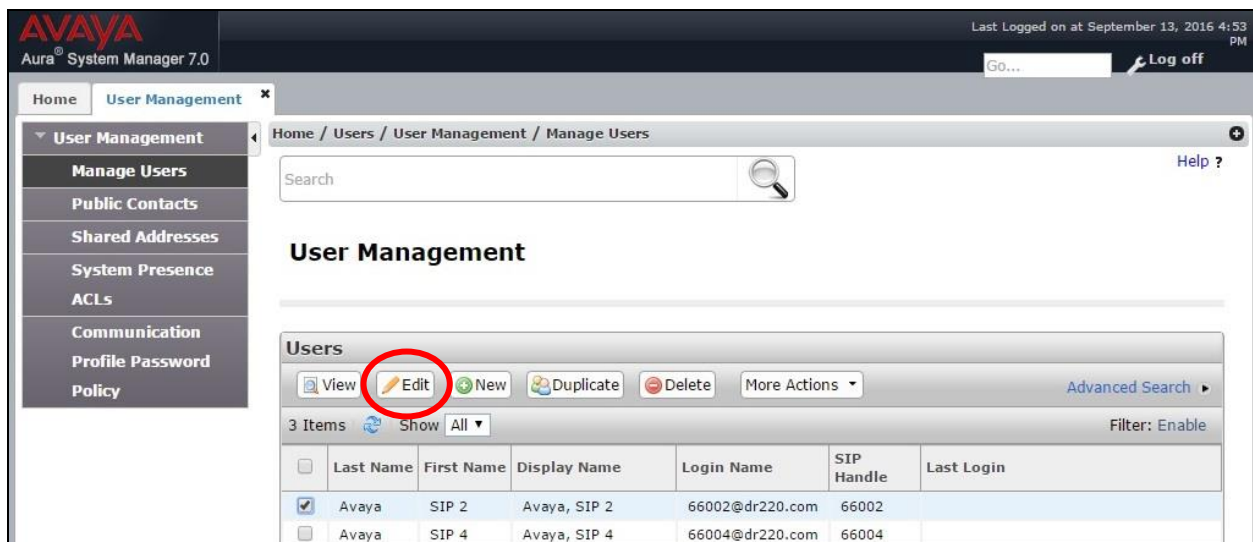
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



The screenshot shows the Avaya Aura System Manager 7.0 login page. It features a dark header with the Avaya logo and 'Aura® System Manager 7.0'. The main content area has a light gray background. On the left, there is a box with text: 'Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: • First time login with "admin" account • Expired/Reset passwords. Use the "Change Password" hyperlink on this page to change the password manually, and then login.' On the right, there is a login form with fields for 'User ID:' and 'Password:', 'Log On' and 'Cancel' buttons, and a 'Change Password' link.

7.2. Administer Users

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



The screenshot shows the Avaya Aura System Manager 7.0 User Management screen. The header includes the Avaya logo, 'Aura® System Manager 7.0', and a 'Log off' button. The left navigation pane has a 'User Management' section with a 'Manage Users' link highlighted. The main content area shows the 'User Management' title and a search bar. Below the title, there is a 'Users' section with a table of users. The 'Edit' button in the 'Users' section is circled in red. The table has columns: Last Name, First Name, Display Name, Login Name, SIP Handle, and Last Login. There are 3 items shown, with the first item selected.

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

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

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

AVAYA
Aura® System Manager 7.0

Last Logged on at September 13, 2016 4:53 PM
Go... Log off

Home User Management x

Home / Users / User Management / Manage Users

Help ?

User Profile Edit: 66002@dr220.com Commit & Conf

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
Avaya SIP	66002	dr220.com

Select : All, None

☒ **Session Manager Profile**

☒ **CM Endpoint Profile**

* System DR220-CM7-ES

* Profile Type Endpoint

Use Existing Endpoints ☐

* Extension 66002 **Endpoint Editor**

Template Select/Reset

Set Type 9621SIPCC

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 shows the Avaya Aura System Manager 7.0 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 7.0', and a 'Log off' button. 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 'Edit Endpoint' and contains several input fields for user configuration. A red circle highlights the 'Type of 3PCC Enabled' dropdown menu, which is currently set to 'Avaya'. Below the main form is a section for 'General Options (G)' with various settings like 'Class of Restriction (COR)', 'Emergency Location Ext', 'Tenant Number', 'SIP Trunk', 'Coverage Path 1', 'Lock Message', 'Multibyte Language', 'Class Of Service (COS)', 'Message Lamp Ext.', 'Coverage Path 2', 'Localized Display Name', and 'Enable Reachability for Station Domain Control'. The 'Done' and 'Cancel' buttons are visible at the bottom right.

System	Extension
DR220-CM7-ES	66002

Template	Set Type
Select	9621SIPCC

Port	Security Code
S00004	

Name
Avaya, SIP 2

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)
Enhanced Call Fwd (E)	Button Assignment (B)	Profile Settings (P)	Group Membership (M)
* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	66002	* Message Lamp Ext.	66002
* Tenant Number	1	Type of 3PCC Enabled	Avaya
* SIP Trunk	Qaar	Coverage Path 2	
Coverage Path 1	1	Localized Display Name	Avaya, SIP 2
Lock Message	<input type="checkbox"/>	Enable Reachability for Station Domain Control	system
Multibyte Language	Not Applicable		

8. Configure dvsAnalytics Encore

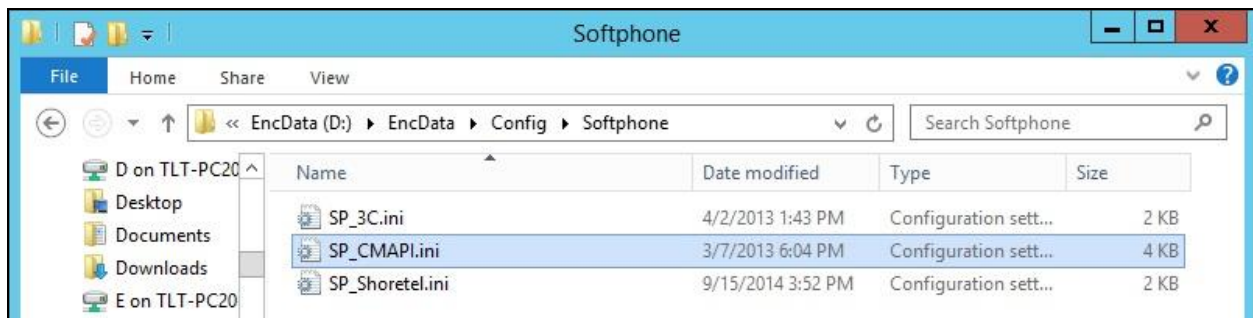
This section provides the procedures for configuring Encore. The procedures include the following areas:

- Administer softphones
- Administer CTISetup
- Administer CT Gateway

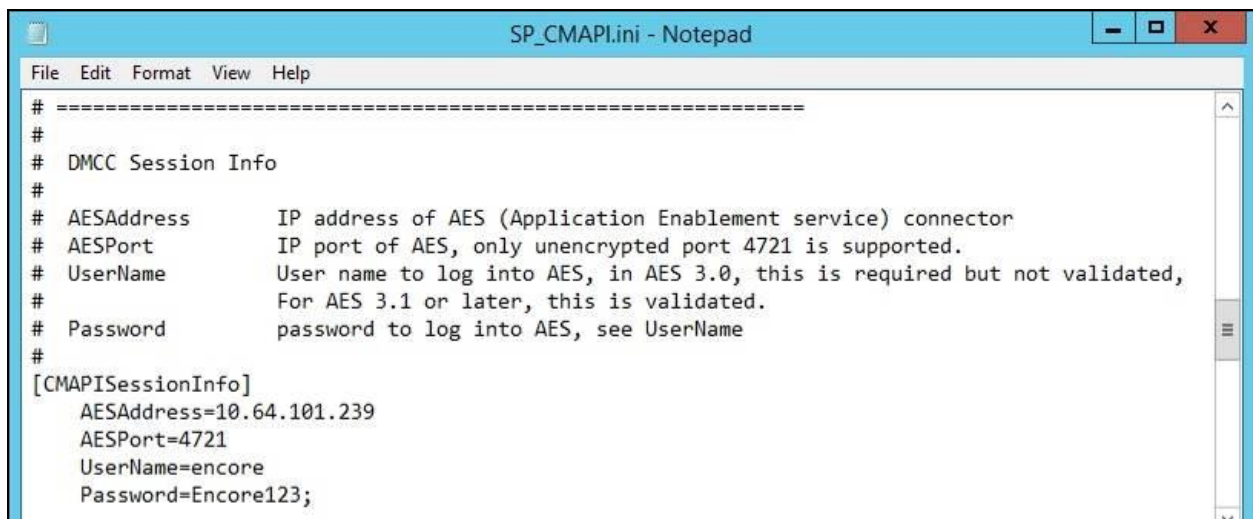
The configuration of Encore is performed by dvsAnalytics installers and dealers. The procedural steps are presented in these Application Notes for informational purposes.

8.1. Administer Softphones

From the Encore server, navigate to the **D:\EncData\Config\Softphone** directory to edit the **SP_CMAPI.ini** file shown below.

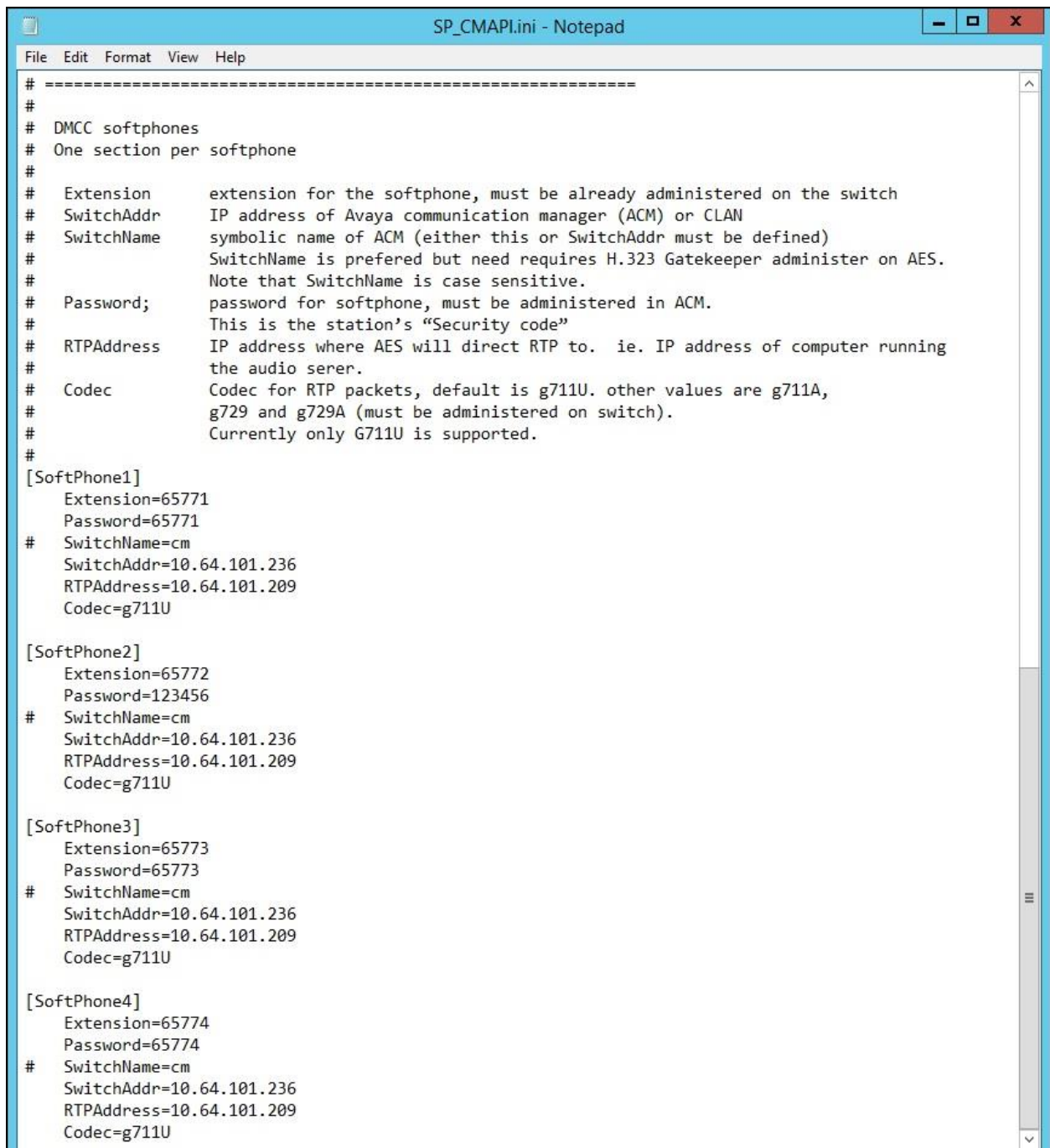


Scroll down to the **DMCC Session Info** sub-section. Under **CMAPISessionInfo**, set **AESAddress** to the IP address of the Application Enablement Services server. Set **UserName** and **Password** to the Encore user credentials from **Section 6.5**. Retain the default value for the remaining fields.



Scroll down to the **DMCC softphones** sub-section. Under **SoftPhone1**, set **Extension** and **Password** to the first virtual IP softphone extension and security code from **Section 5.7**. Set **SwitchAddr** to the IP address of the H.323 Gatekeeper from **Section 6.4**. Set **RTPAddress** to the IP address of the Encore server. Retain the default values for the remaining fields.

Create additional softphone entries as necessary. In the compliance testing, four softphones were configured to correspond to the four virtual IP softphones from **Section 5.7**.



```
# =====
#
# DMCC softphones
# One section per softphone
#
# Extension      extension for the softphone, must be already administered on the switch
# SwitchAddr     IP address of Avaya communication manager (ACM) or CLAN
# SwitchName     symbolic name of ACM (either this or SwitchAddr must be defined)
#               SwitchName is preferred but need requires H.323 Gatekeeper administer on AES.
#               Note that SwitchName is case sensitive.
# Password;      password for softphone, must be administered in ACM.
#               This is the station's "Security code"
# RTPAddress     IP address where AES will direct RTP to.  ie. IP address of computer running
#               the audio server.
# Codec          Codec for RTP packets, default is g711U. other values are g711A,
#               g729 and g729A (must be administered on switch).
#               Currently only G711U is supported.
#
[SoftPhone1]
  Extension=65771
  Password=65771
#  SwitchName=cm
  SwitchAddr=10.64.101.236
  RTPAddress=10.64.101.209
  Codec=g711U

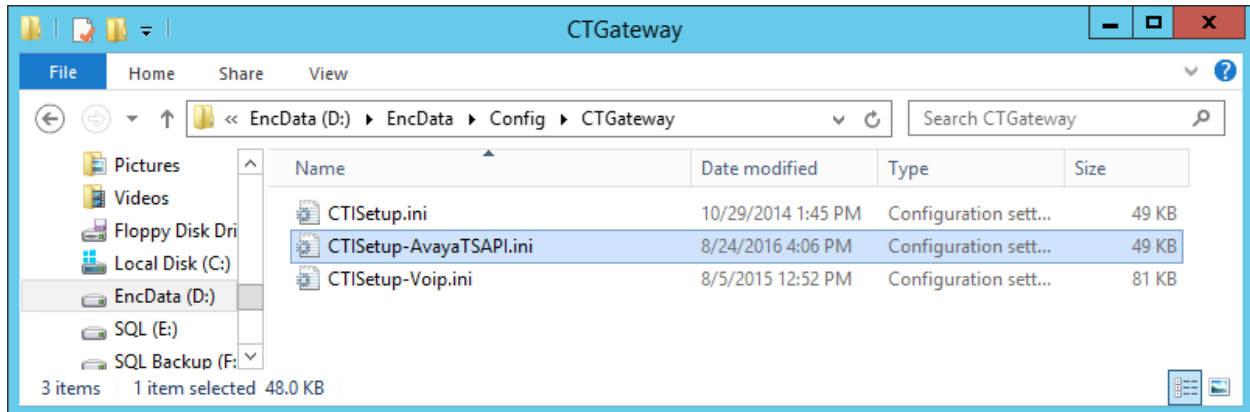
[SoftPhone2]
  Extension=65772
  Password=123456
#  SwitchName=cm
  SwitchAddr=10.64.101.236
  RTPAddress=10.64.101.209
  Codec=g711U

[SoftPhone3]
  Extension=65773
  Password=65773
#  SwitchName=cm
  SwitchAddr=10.64.101.236
  RTPAddress=10.64.101.209
  Codec=g711U

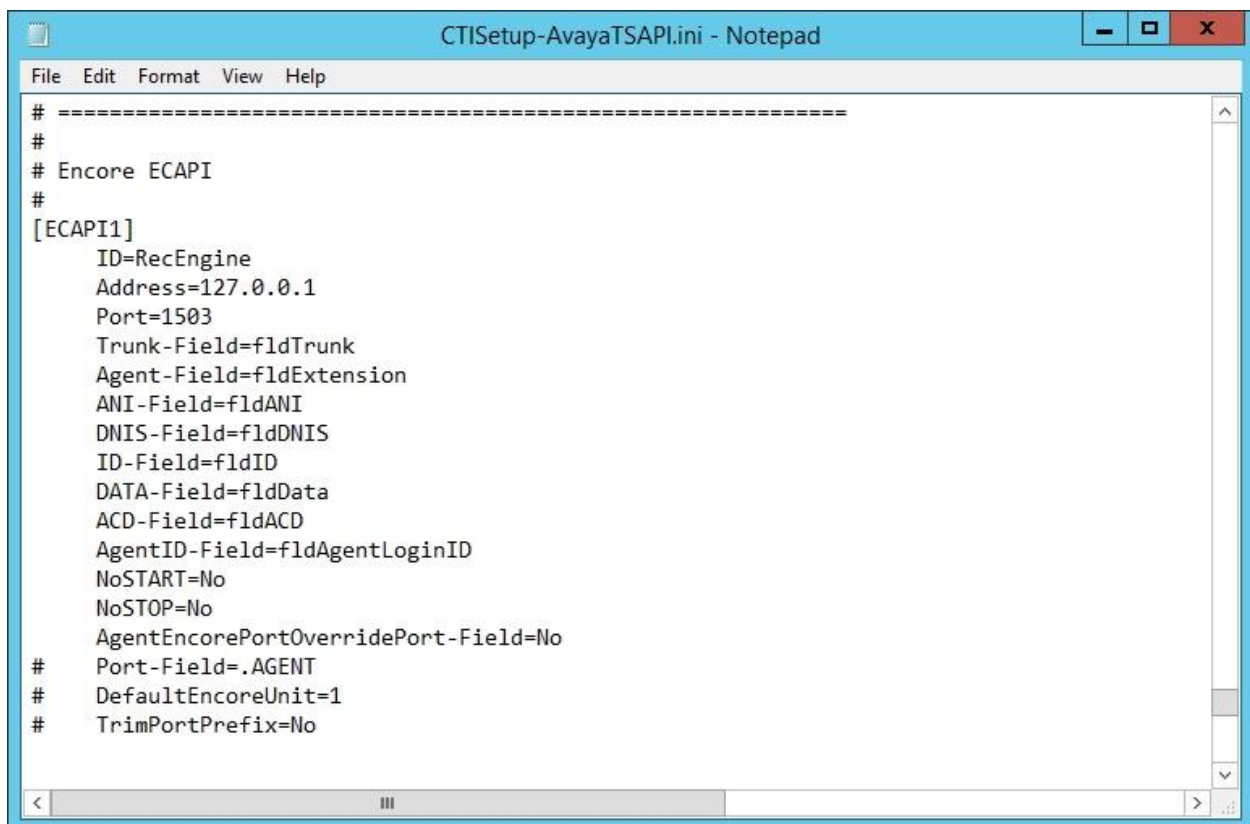
[SoftPhone4]
  Extension=65774
  Password=65774
#  SwitchName=cm
  SwitchAddr=10.64.101.236
  RTPAddress=10.64.101.209
  Codec=g711U
```

8.2. Administer CTISetup

Navigate to the **D:\EncData\Config\CTGateway** directory to edit the **CTISetup-AvayaTSAPI.ini** file.

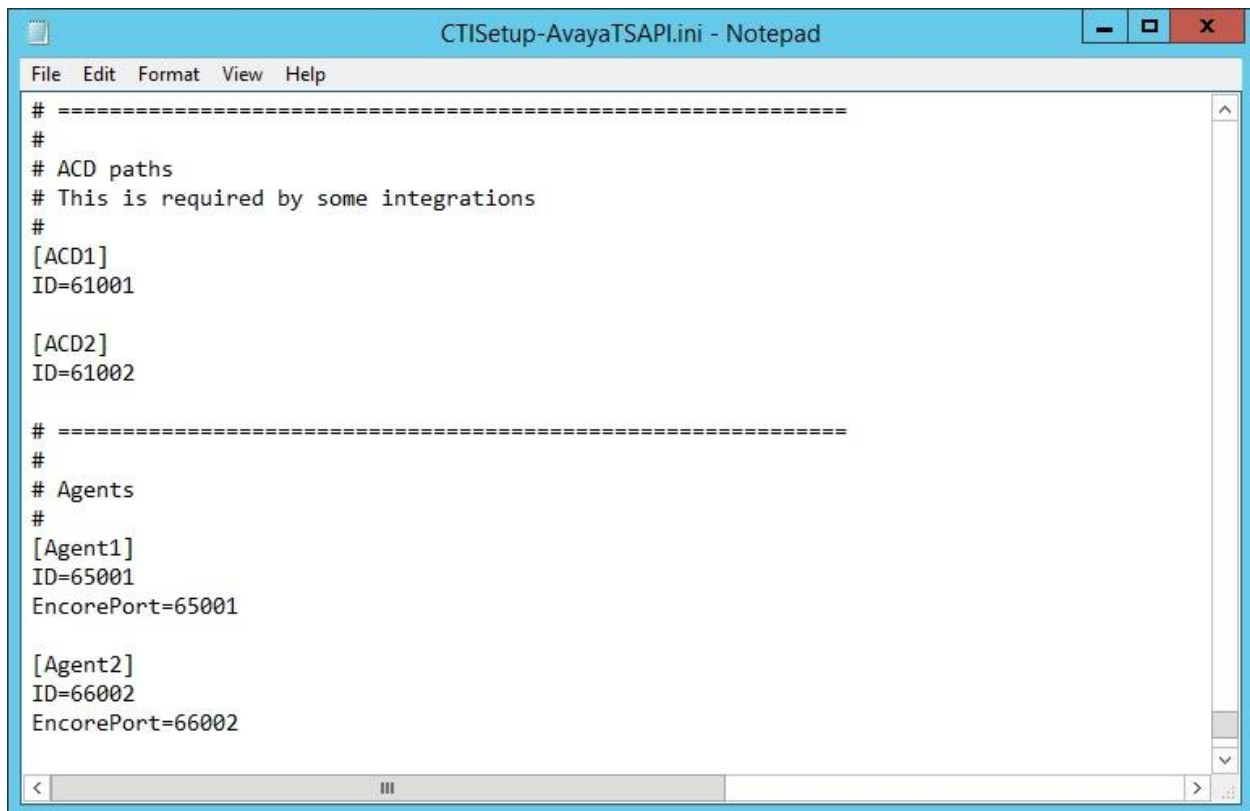


Scroll down to the **Encore ECAPI** sub-section. Under **ECAPI1**, make certain all parameters are set to the default values shown below.



Scroll to the **ACD paths** sub-section. Under **ACD1**, set **ID** to the first skill group extension from **Section 3**. Create additional ACD entries as necessary when more than one skill group is being monitored.

Scroll to the **Agents** sub-section. Under **Agent1**, set **ID** and **EncorePort** to the first agent station extension from **Section 3**. Create additional agent entries as necessary when more than one agent is being monitored.



```
CTISetup-AvayaTSAPI.ini - Notepad
File Edit Format View Help
# =====
#
# ACD paths
# This is required by some integrations
#
[ACD1]
ID=61001

[ACD2]
ID=61002

# =====
#
# Agents
#
[Agent1]
ID=65001
EncorePort=65001

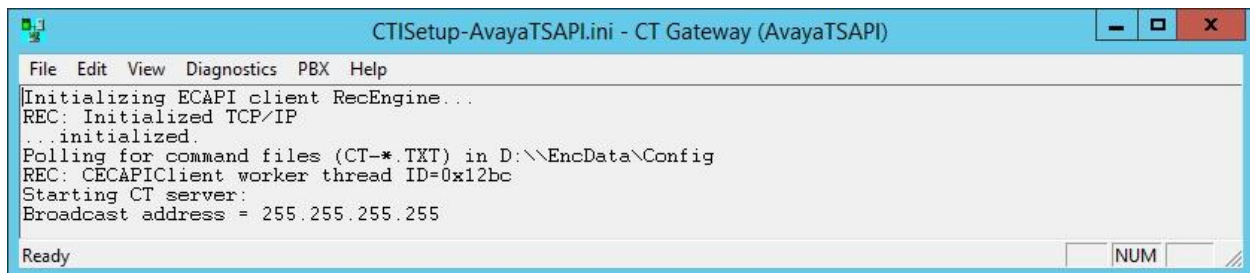
[Agent2]
ID=66002
EncorePort=66002
```


8.3. Administer CT Gateway

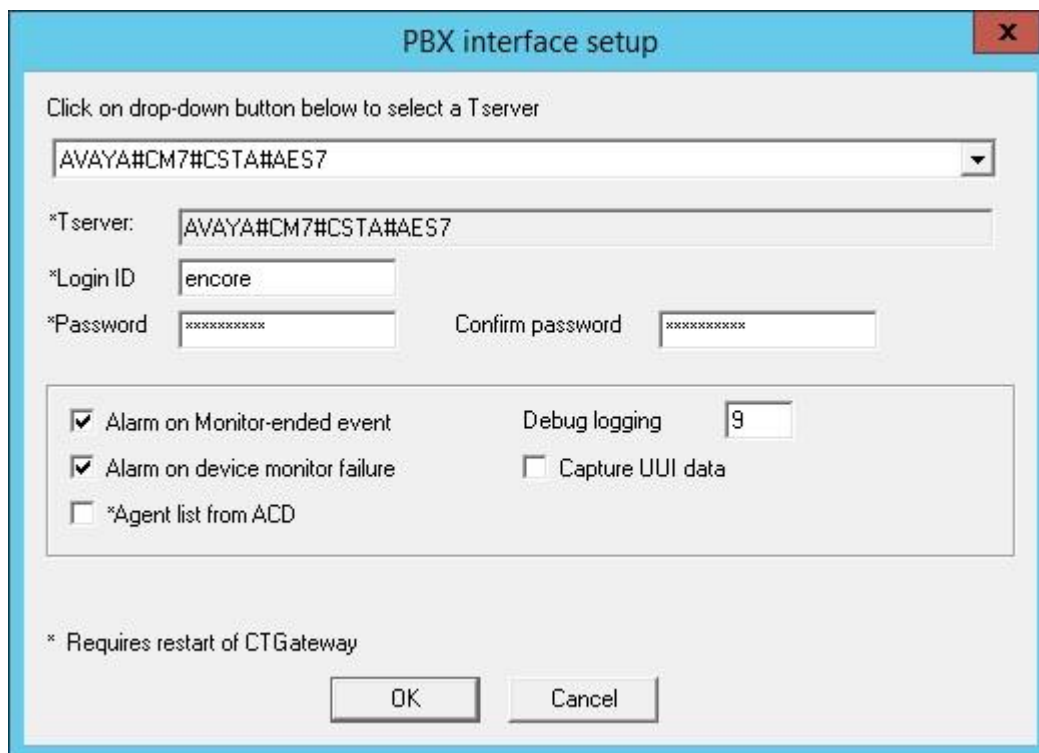
Click on the **CT Gateway** icon from the server system tray to start CT Gateway, if not running already.



The **ctiSetup-AvayaTSAPI.ini** screen is displayed. Select **PBX → Configure** from the top menu.



The **PBX interface setup** screen is displayed. Select the Tlink name from **Section 6.9** from the drop-down list, and enter the Encore user credentials from **Section 6.5** for **Login ID**, **Password**, and **Confirm Password**. Retain the default values in the remaining fields. In the compliance testing, **Debug logging** was set to the highest level of “9”.



9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	7	no	aes7	established	60	42

Verify the registration status of virtual IP softphones by using the “list registered-ip-stations” command. Verify that all virtual IP softphone from **Section 5.7** are displayed along with the IP address of the Application Enablement Services server, as shown below.


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

REGISTERED IP STATIONS						
Station Ext or Orig Port	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Skt Gatekeeper IP Address			
65000	9641	IP_Phone	tls	192.168.200.186		
	1	6.6229		10.64.101.236		
65001	9611	IP_Phone	tls	192.168.200.137		
	1	6.6229		10.64.101.236		
65771	4610	IP_API_A	tcp	10.64.101.239		
	1	3.2040		10.64.101.236		
65772	4610	IP_API_A	tcp	10.64.101.239		
	1	3.2040		10.64.101.236		
65773	4610	IP_API_A	tcp	10.64.101.239		
	1	3.2040		10.64.101.236		
65774	4610	IP_API_A	tcp	10.64.101.239		
	1	3.2040		10.64.101.236		

9.2. Verify Avaya Aura® Application Enablement Services

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

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

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 13 12:15:50 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 13 12:42:57 EDT 2016
HA Status: Not Configured

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

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Log Manager

▶ Logs

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

■ Switch Conn Summary

■ **TSAPI Service Summary**

TSAPI Link Details


☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Mon Sep 12 13:26:29 2016	Online	17	4	25	25	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 Encore user name from **Section 6.5**, and that the **# of Associated Devices** column reflects the number of configured softphones from **Section 8.1**.



Application Enablement Services
Management Console

Welcome: User
Last login: Tue Sep 13 12:15:50 2016 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Tue Sep 13 12:42:31 EDT 2016
HA Status: Not Configured

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

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status

Alarm Viewer
Log Manager
Logs
Status and Control
CVLAN Service Summary
DLG Services Summary
DMCC Service Summary
Switch Conn Summary
TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Tue Sep 13 12:42:26 EDT 2016
Service Uptime: 0 days, 23 hours 15 minutes
Number of Active Sessions: 1
Number of Sessions Created Since Service Boot: 1
Number of Existing Devices: 4
Number of Devices Created Since Service Boot: 4

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	8631E321A9BC5605F 022A5FE701BD7A4-0	encore	SPAS1	10.64.101.209	XML Unencrypted	4

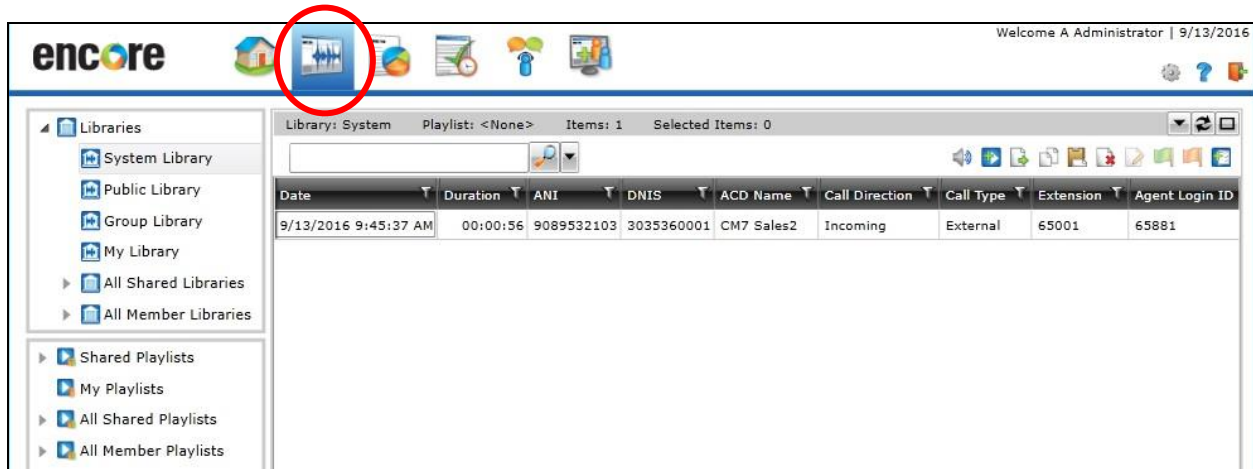
Item 1-1 of 1
1 Go

9.3. Verify dvsAnalytics Encore

Log an agent into the skill group to handle and complete an ACD call. Access the Encore web interface by using the URL “http://ip-address/encore” in an Internet Explorer browser window, where “ip-address” is the IP address of the Encore server. The **encore** screen is displayed. Click **Login** and log in using the appropriate credentials.



The **encore** screen is displayed. Select the **Recorded Contacts** icon from the top menu to display a list of call recordings. Verify that there is an entry in the right pane reflecting the last call, with proper values in the relevant fields.



Right click on the entry and select **Play** to listen to the playback. Verify that the screen is updated and that the call recording is played back.

The screenshot displays the Encore software interface. At the top, the 'encore' logo is on the left, and 'Welcome A Administrator | 9/13/2016' is on the right. Below the header is a navigation pane on the left with 'Libraries' (System Library, Public Library, Group Library) and 'Shared Playlists' (My Playlists, All Shared Playlists, All Member Playlists). The main area shows a table with call data. The table has columns: Date, Duration, ANI, DNIS, ACD Name, Call Direction, Call Type, Extension, and Agent Login ID. The first row contains the following data: 9/13/2016 9:45:37 AM, 00:00:56, 9089532103, 3035360001, CM7 Sales2, Incoming, External, 65001, 65881. Below the table is a 'Streaming Player: N6M2N7KB.vx8' section. It shows 'Position: 0:00:19.768', 'Recording Length: 0:00:56.202', and 'Related Calls:0'. A waveform visualization is present, and a 'Video Unavailable' message is shown on the left. At the bottom is a playback control bar with buttons for play, pause, stop, previous, next, and a volume slider.

Date	Duration	ANI	DNIS	ACD Name	Call Direction	Call Type	Extension	Agent Login ID
9/13/2016 9:45:37 AM	00:00:56	9089532103	3035360001	CM7 Sales2	Incoming	External	65001	65881

Streaming Player: N6M2N7KB.vx8
Position: 0:00:19.768 Recording Length: 0:00:56.202 Related Calls:0

Video Unavailable

10. Conclusion

These Application Notes describe the configuration steps required for dvsAnalytics Encore 6.0.5 to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 using Service Observing. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2.1, August 2016, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016, available at <http://support.avaya.com>.
3. *Avaya AuraTM Communication Manager TSAPI Integration Guide*, Encore Version 6.0.4, July 9, 2015, available from dvsAnalytics Support.
4. *Avaya AuraTM Communication Manager TSAPI Installation Addendum*, Includes Version 6.0.4, System Version 2.3.7, July 9, 2015, available from dvsAnalytics Support.

©2016 Avaya Inc. All Rights Reserved.

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

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