



Avaya Solution & Interoperability Test Lab

Application Notes for dvsAnalytics Encore 7.1 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for dvsAnalytics Encore 7.1 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 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 7.1 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing. Encore is a call recording solution.

In the compliance testing, Encore used the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services to monitor skill groups and agent stations on Communication Manager, and used the Service Observing feature via the 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 Encore to monitor skill groups and agent stations on Communication Manager. When there is an active call at a monitored agent station, Encore is informed of the call via event reports from the TSAPI interface to start the call recording. The event reports are also used by Encore to determine when to stop the call recordings.

The DMCC interface is used by Encore to register virtual IP softphones, and for adding softphones to active calls using the Service Observing feature to pick up the media for 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 requested monitoring of skill groups and agent stations, performed device queries on agent stations, and registered the virtual IP softphones.

For 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 resume 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.

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 interface between Application Enablement Services and Encore did not include use of any specific encryption features as requested by dvsAnalytics.

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, transfer, and conference.

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 number of softphones to configure needs 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:** +1 (800) 910-4564
- **Email:** Support@dvsAnalytics.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager, Application Enablement Services, System Manager, Session Manager, and of call 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
Agent Station	65001 (H.323), 66006 (SIP)
Agent ID	65881, 65882

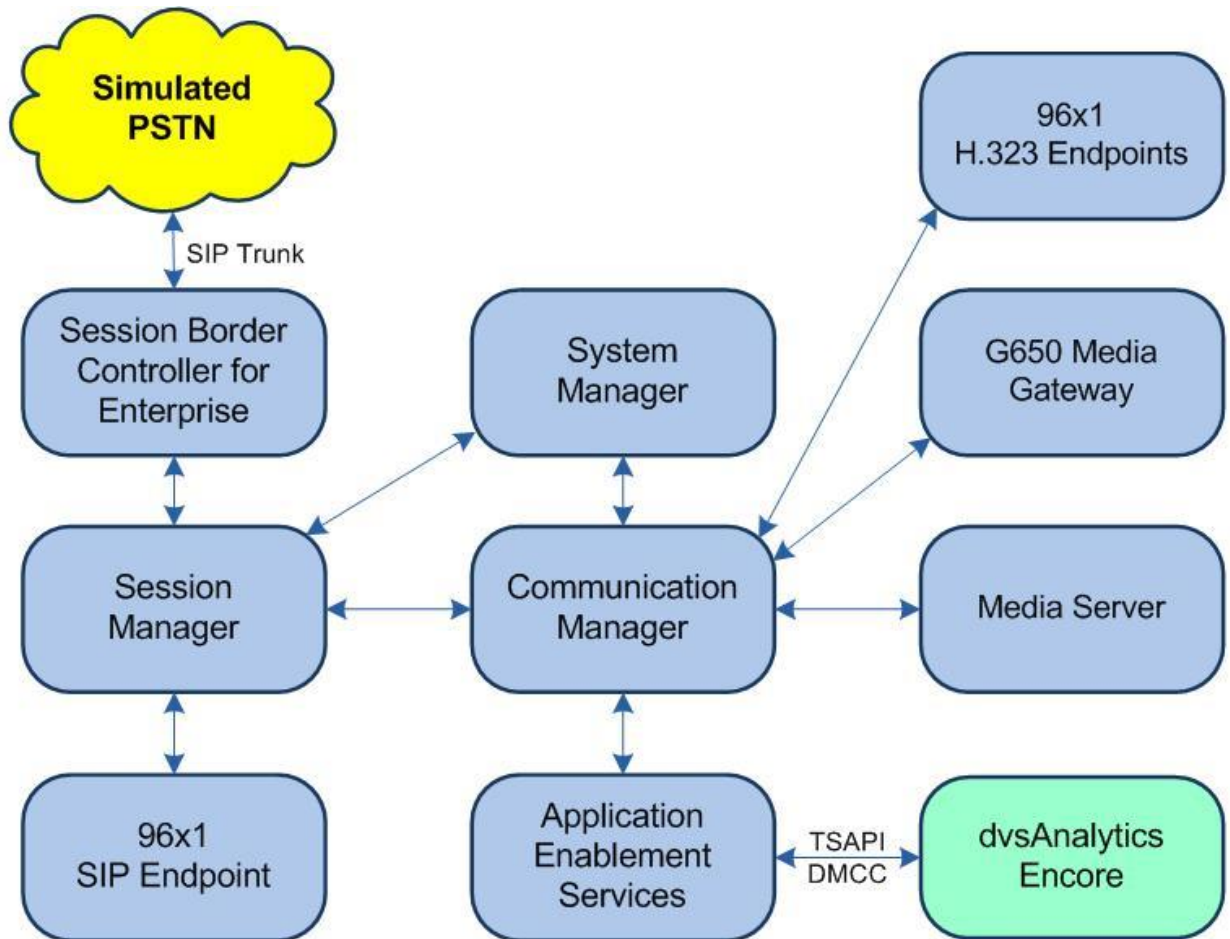


Figure 1: Compliance Testing Configuration

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	8.1 (8.1.0.1.1.890.25517)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.1.121
Avaya Aura® Application Enablement Services in Virtual Environment	8.1 (8.1.0.0.0.9-1)
Avaya Aura® Session Manager in Virtual Environment	8.1 (8.1.0.0.810007)
Avaya Aura® System Manager in Virtual Environment	8.1 (8.1.0.0.079814)
Avaya 1608-I IP Deskphone	1.3120
Avaya 9611G IP Deskphone (H.323)	6.8202
Avaya 9641G IP Deskphone (SIP)	7.1.6.1.3
dvsAnalytics Encore on Windows Server 2016 <ul style="list-style-type: none">Avaya TSAPI Windows Client (csta32.dll)Avaya DMCC XML	7.1 Standard 8.1.0.9 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 into 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 12
CALL CENTER OPTIONAL FEATURES			
Call Center Release: 8.0			
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	
Name: AES CTI Link	
Unicode Name? n	
COR: 1	

5.3. Administer 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”.

For customer network that uses encrypted media, make certain that “none” is included for **Media Encryption**, and that **Encrypted SRTP** is set to “best-effort”, these settings are needed for support of non-encrypted media from the virtual IP softphones used by Encore.

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 MEDIA PARAMETERS			
Codec Set: 1			
Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size(ms)
1: G.711MU	n	2	20
2:			
3:			
4:			
5:			
6:			
7:			
Media Encryption		Encrypted SRTP: best-effort	
1:	1-srtp-aescm128-hmac80		
2:	aes		
3:	none		
4:			

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 19
FEATURE-RELATED SYSTEM PARAMETERS	
CALL CENTER SYSTEM PARAMETERS	
EAS	
Expert Agent Selection (EAS) Enabled? y	
Minimum Agent-LoginID Password Length:	
Direct Agent Announcement Extension:	
Delay:	
Message Waiting Lamp Indicates Status For: station	
Work Mode On Login: aux	
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? n
    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 43
                                CLASS OF RESTRICTION

    COR Number: 2
    COR Description:

        FRL: 0
        APLT? y
    Can Be Service Observed? y          Calling Party Restriction: none
    Can Be A Service Observer? y       Called Party Restriction: none
        Time of Day Chart: 1          Forced Entry of Account Codes? n
        Priority Queuing? n           Direct Agent Calling? n
        Restriction Override: none     Facility Access Trunk Test? n
        Restricted Call List? 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**.

Repeat this section to administer all non-SIP agent stations from **Section 3**. In the compliance testing, one agent station was administered.

change station 65001		Page	1 of	5
		STATION		
Extension: 65001	Lock Messages? n	BCC: 0		
Type: 9611	Security Code: *	TN: 1		
Port: S00103	Coverage Path 1: 1	COR: 2		
Name: CM7 Station 1	Coverage Path 2:	COS: 1		
	Hunt-to Station:	Tests? y		

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 65991		Page	1 of	5
STATION				
Extension: 65991	Lock Messages? n	BCC: 0		
Type: 4610	Security Code: 123456	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				
	Time of Day Lock Table:			
Loss Group: 19	Personalized Ringing Pattern: 1			
	Message Lamp Ext: 65991			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english				
Survivable GK Node Name:				
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	IP SoftPhone? y			
	IP Video Softphone? n			
	Short/Prefixed Registration Allowed: default			
	Customizable Labels? y			

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

```

add station 65991
                                     Page  4 of  5

                                     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 65991 count 4

```

STATIONS									
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Cable	Room/ Jack	Cv1/ Cv2	COR/ COS	TN	
65991	S00000	Encore Virtual #1						2	
	4610		no				1	1	
65992	S00001	Encore Virtual #2						2	
	4610		no				1	1	
65993	S00003	Encore Virtual #3						2	
	4610		no				1	1	
65994	S00004	Encore Virtual #4						2	
	4610		no				1	1	

6. Configure Avaya Aura® Application Enablement Services

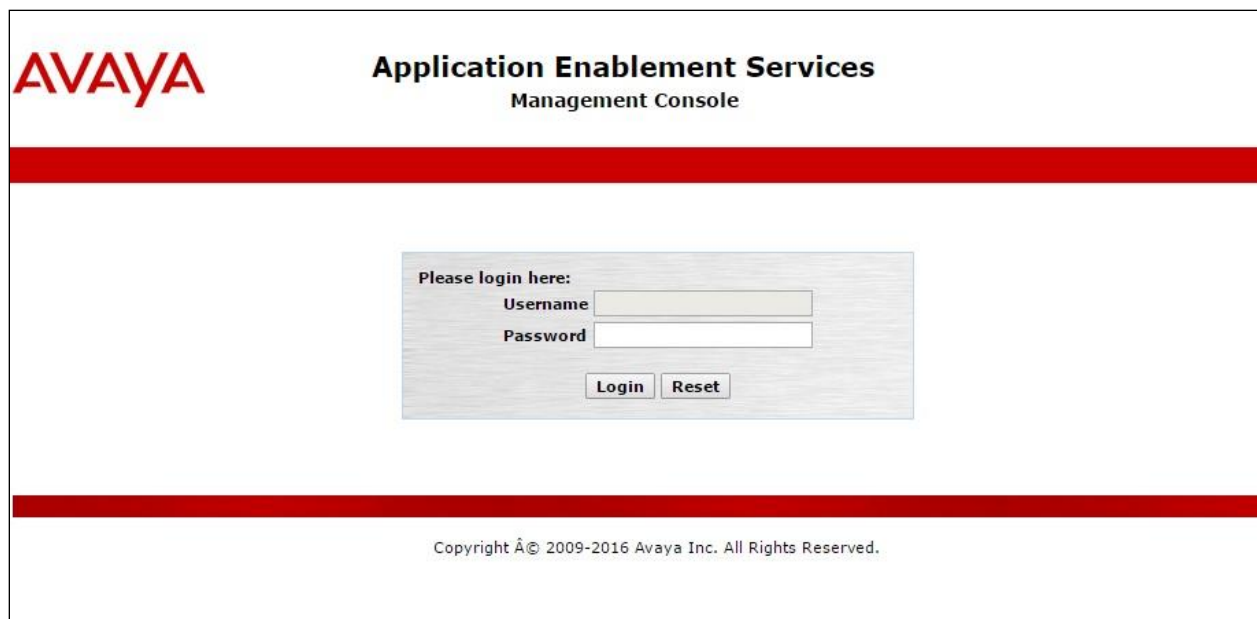
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer 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 screen below is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya Application Enablement Services Management Console login page. 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 separates the header from the main content area. In the center of the page is a login box with a light gray background. Inside the box, the text "Please login here:" is 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.

 **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jan 7 09:37:43 2020 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: 8.1.0.0.9-1
Server Date and Time: Tue Jan 07 10:07:23 EST 2020
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).

 **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jan 7 09:37:43 2020 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: 8.1.0.0.9-1
Server Date and Time: Tue Jan 07 10:07:23 EST 2020
HA Status: Not Configured

Licensing | Home | Help | Logout

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

Licensing

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

Select **Licensed products** → **APPL_ENAB** → **Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below. Note that the TSAPI license is used for device monitoring, and the DMCC license is used for the virtual IP softphones.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The left pane displays a tree view with the following structure:

- WebLM Home
- Install license
- Licensed products
 - APPL_ENAB
 - Application_Enablement
 - View by feature
 - View by local WebLM
 - Enterprise configuration
 - Local WebLM Configuration
 - Usages
 - Allocations
 - Periodic status
- ASBCE
 - Session_Border_Controller_E_AE
- CCTR
 - ContactCenter
- COMMUNICATION_MANAGER
 - Call_Center
 - Communication_Manager
- MESSAGING
 - Messaging
- MSR
 - Media_Server
- SYSTEM_MANAGER
 - System_Manager
- SessionManager

The right pane displays the **Application Enablement (CTI) - Release: 8 - SID: 10503000(Enterprise)** page. It includes the following information:

- You are here: Licensed Products > Application_Enablement > View by Feature
- License installed on: August 8, 2019 4:43:51 PM -05:00
- License File Host IDs: VE-83-02-2D-26-52-01
- Active License Mode: Standard
- License State: NA
- Pay Per Use: No
- License Available: No
- Standard License Available: Yes

Below this information is a table showing the license capacity for various features:

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

6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console** to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The screenshot shows the AVAYA Application Enablement Services Management Console. The top right corner displays user information: Welcome: User, Last login: Tue Jan 7 09:37:43 2020 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: 8.1.0.0.9-1, Server Date and Time: Tue Jan 07 10:07:23 EST 2020, HA Status: Not Configured. The left navigation pane shows the hierarchy: AE Services > TSAPI > TSAPI Links. 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 the hierarchy: AE Services > TSAPI > TSAPI Links. The main content area is titled "Add TSAPI Links" and contains form fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The Link field has a dropdown menu with the value 1. The Switch Connection field has a dropdown menu with the value cm7. The Switch CTI Link Number field has a dropdown menu with the value 1. The ASAI Link Version field has a dropdown menu with the value 10. The Security field has a dropdown menu with the value Unencrypted. Below the form 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 is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays a table of switch connections. The table has four columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. The first row shows 'cm7' with 'Yes' for Processor Ethernet, '30' for Msg Period, and '1' for Number of Active Connections. Below the table are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'. The top right corner shows user information and system status.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm7	Yes	30	1

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

The screenshot shows the 'Edit H.323 Gatekeeper - cm7' screen. The left navigation pane is the same as the previous screenshot. The main content area has a text input field containing '10.64.101.236' and an 'Add Name or IP' button. Below the input field are 'Delete IP' and 'Back' buttons. The top right corner shows user information and system status.

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 Jan 7 09:37:43 2020 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: 8.1.0.0.9-1
Server Date and Time: Tue Jan 07 10:14:06 EST 2020
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. Make certain both parameters are unchecked, as shown 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 and the title "Application Enablement Services Management Console". A welcome message and system information are shown in the top right corner. The main navigation pane on the left lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The main content area displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page, which contains two unchecked checkboxes and an "Apply Changes" button.

Welcome: User
Last login: Tue Jan 7 09:37:43 2020 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: 8.1.0.0.9-1
Server Date and Time: Tue Jan 07 10:07:23 EST 2020
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

6.8. 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**. Select **Restart Service**.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jan 7 09:37:43 2020 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: 8.1.0.0.9-1
Server Date and Time: Tue Jan 07 10:07:23 EST 2020
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 and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is shown, including login details and system status. Below the header, a red navigation bar contains links for "Security", "Security Database", and "Tlinks". The left sidebar lists various services, with "Security" expanded to show "Security Database" and "Tlinks" selected. The main content area, titled "Tlinks", shows a single Tlink named "AVAYA#CM7#CSTA#AES7" with a "Delete Tlink" button.

Welcome: User
Last login: Tue Jan 7 09:37:23 2020 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: 8.1.0.0.9-1
Server Date and Time: Tue Jan 07 09:38:04 EST 2020
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

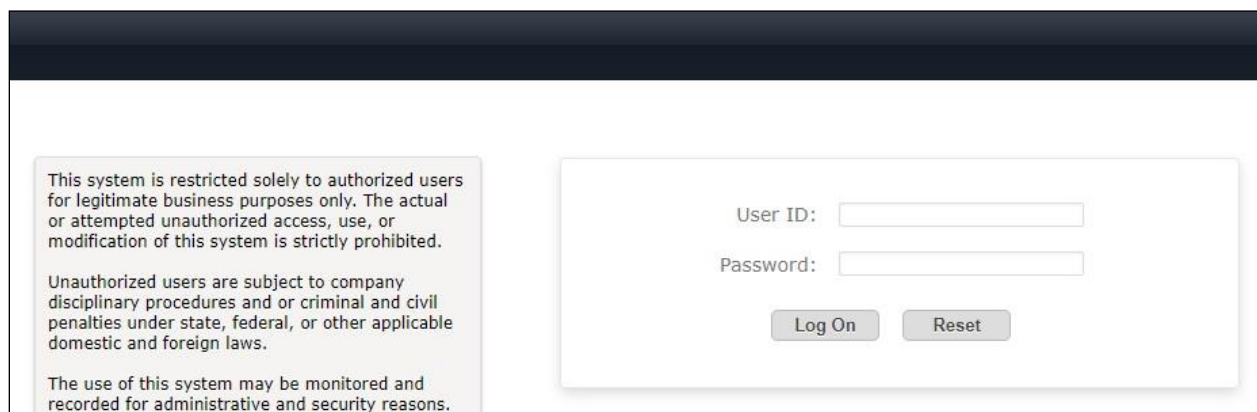
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

7.1. Launch System Manager

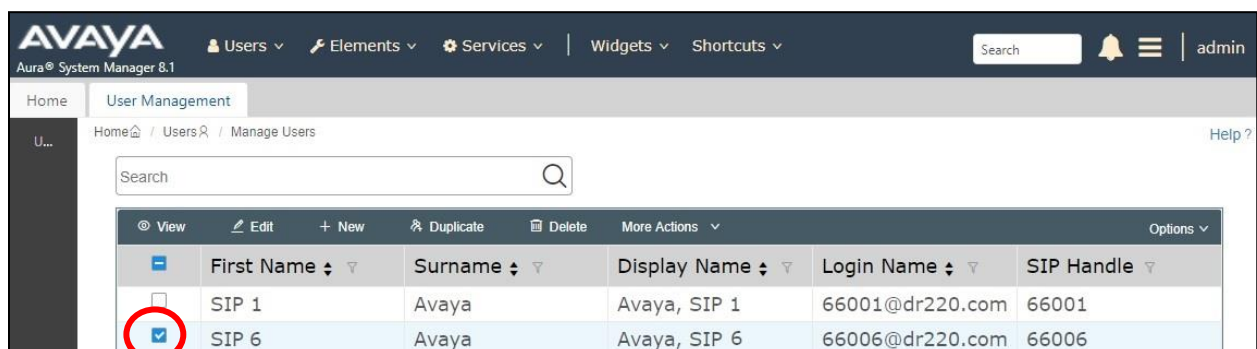
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



7.2. Administer Users

In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below.

Select the entry associated with the first SIP agent station from **Section 3**, in this case “66006”, and click **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
SIP 1		Avaya	Avaya, SIP 1	66001@dr220.com	66001
SIP 6		Avaya	Avaya, SIP 6	66006@dr220.com	66006

The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Click on the **Editor** icon shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, "Aura® System Manager 8.1", and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled "admin" are also present. The main content area is titled "User Profile | Edit | 66006@dr220.com" and features buttons for "Commit & Continue", "Commit", and "Cancel". Below the title are tabs for Identity, Communication Profile, Membership, and Contacts. The left sidebar shows a list of profiles: Communication Profile Password, PROFILE SET : Primary, Communication Address, PROFILES, Session Manager Profile, CM Endpoint Profile (highlighted), and Messaging Profile. The main form area contains fields for System (DR-CM), Profile Type (Endpoint), Extension (66006, with a red circle around the Editor icon), Set Type (9641SIPCC), Security Code, Port (S000047), Voice Mail Number, Preferred Handle (Select), and Sip Trunk (aar). There are also checkboxes for Use Existing Endpoints, Template, and Calculate Route Pattern.

In the popped-up screen, enter the following values for the specified fields and retain the default values for the remaining fields.

- **Class of Restriction (COR):** The COR number from **Section 5.5**.
- **Type of 3PCC Enabled:** “Avaya”

Repeat this section for all SIP agent users.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'User Management' and shows a 'Manage Users' page. A modal window is open for editing a user, with the 'General Options (G)' tab selected. Within this tab, the 'Profile Settings (P)' sub-tab is active. The following fields are visible and highlighted with red boxes:

- Class of Restriction (COR):** A text input field containing the value '2'.
- Type of 3PCC Enabled:** A dropdown menu with 'Avaya' selected.

Other visible fields include:

- Emergency Location Ext:** 66006
- Tenant Number:** 1
- SIP Trunk:** Qaar
- Class Of Service (COS):** 1
- Message Lamp Ext.:** 66006
- Coverage Path 1:** (empty)
- Lock Message:** (checkbox, unchecked)
- Multibyte Language:** Not Applicable
- Coverage Path 2:** (empty)
- Localized Display Name:** Avaya, SIP 6
- Enable Reachability for Station Domain Control:** system

The 'SIP URI' field is at the bottom of the modal window.

8. Configure dvsAnalytics Encore

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

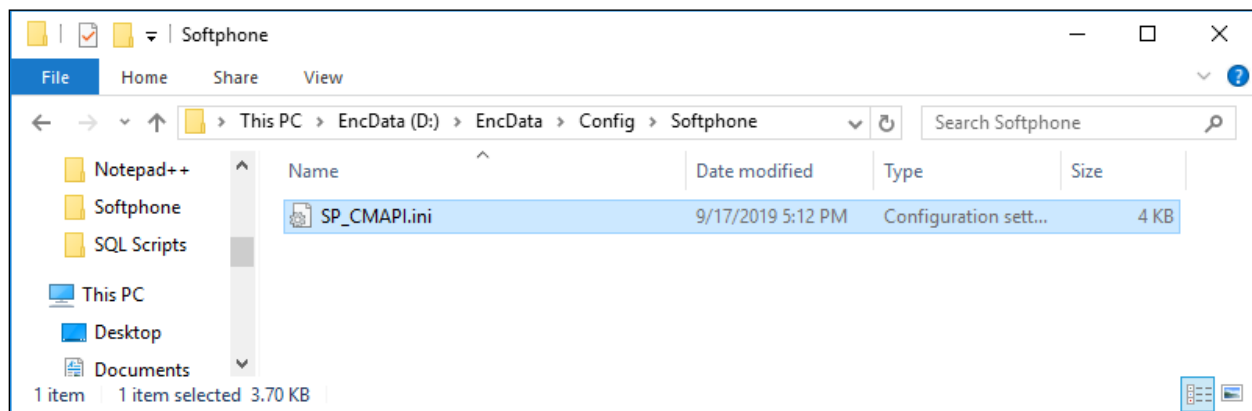
- Administer softphone
- Administer CTG settings
- Encrypt TSAPI password
- Administer recorded ID
- Administer users
- Start services
- Launch programs

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

Prior to configuration, the relevant Avaya TSAPI client is assumed to be installed on the Encore server, and that the TSAPI client has been configured with the IP address of the Application Enablement Services server as part of installation. In addition, a pertinent site and recording profile for Softphone Avaya DMCC are assumed to be pre-configured.

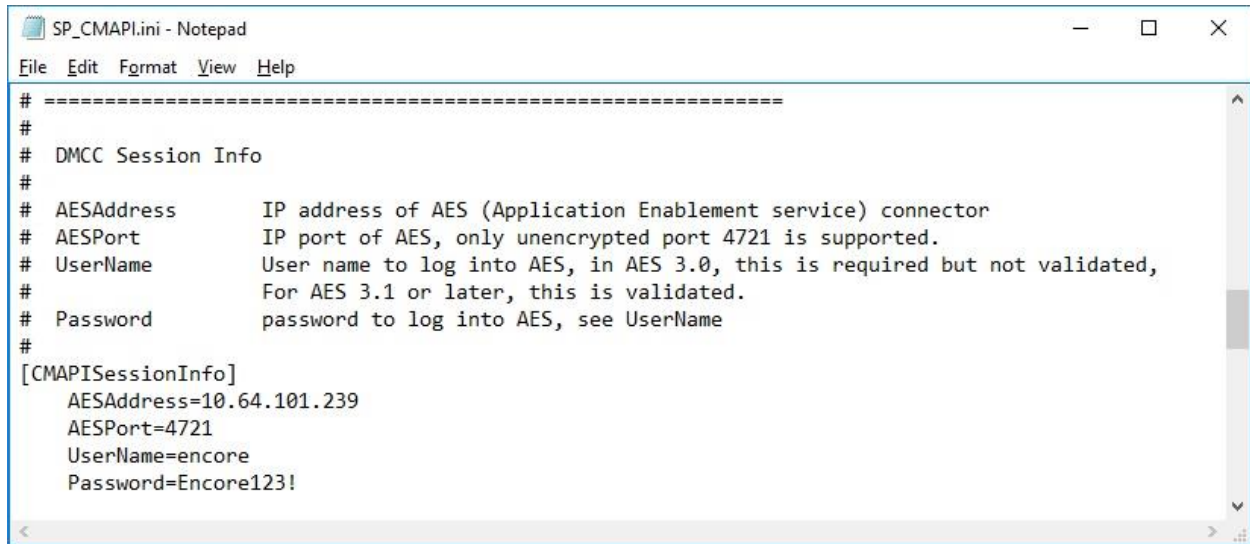
8.1. Administer Softphone

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

- **AESAddress:** IP address of Application Enablement Services server.
- **UserName:** The Encore user credentials from **Section 6.5**.
- **Password:** The Encore user credentials from **Section 6.5**.



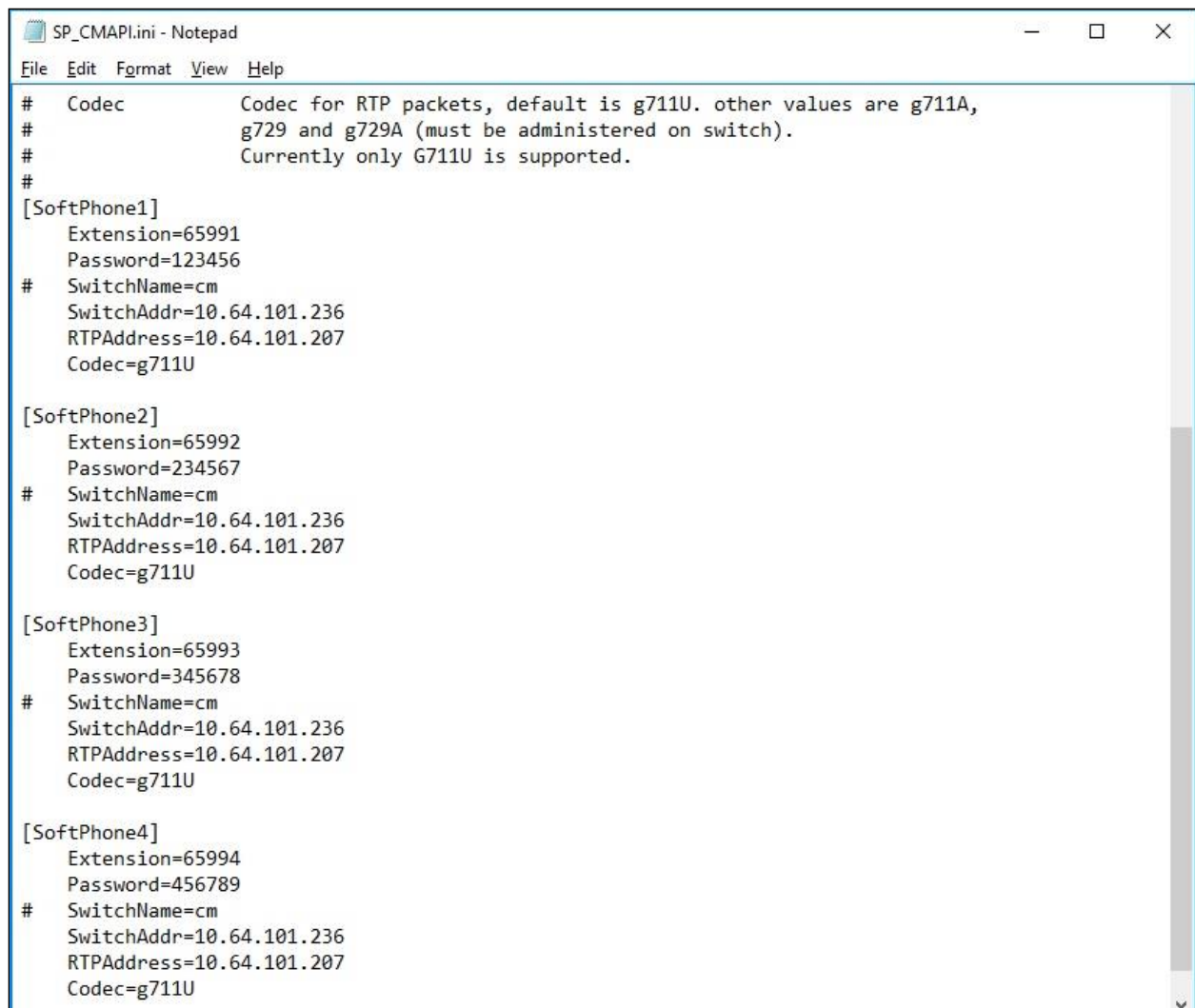
The screenshot shows a Notepad window titled "SP_CMAPI.ini - Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The text content of the file is as follows:

```
# =====  
#  
# DMCC Session Info  
#  
# AESAddress      IP address of AES (Application Enablement service) connector  
# AESPort         IP port of AES, only unencrypted port 4721 is supported.  
# UserName        User name to log into AES, in AES 3.0, this is required but not validated,  
#                 For AES 3.1 or later, this is validated.  
# Password        password to log into AES, see UserName  
#  
[CMAPISessionInfo]  
    AESAddress=10.64.101.239  
    AESPort=4721  
    UserName=encore  
    Password=Encore123!
```

Scroll down to the **DMCC softphones** sub-section (not shown). Under **SoftPhone1**, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Extension:** Extension of the first virtual IP softphone from **Section 5.7**.
- **Password:** Security code of the first virtual IP softphone from **Section 5.7**.
- **SwitchName:** Comment out this parameter.
- **SwitchAddr:** IP address of the H.323 Gatekeeper from **Section 6.4**.
- **RTPAddress:** IP address of the Encore server.

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**.



```
SP_CMAPI.ini - Notepad
File Edit Format View Help

# 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=65991
  Password=123456
#  SwitchName=cm
  SwitchAddr=10.64.101.236
  RTPAddress=10.64.101.207
  Codec=g711U

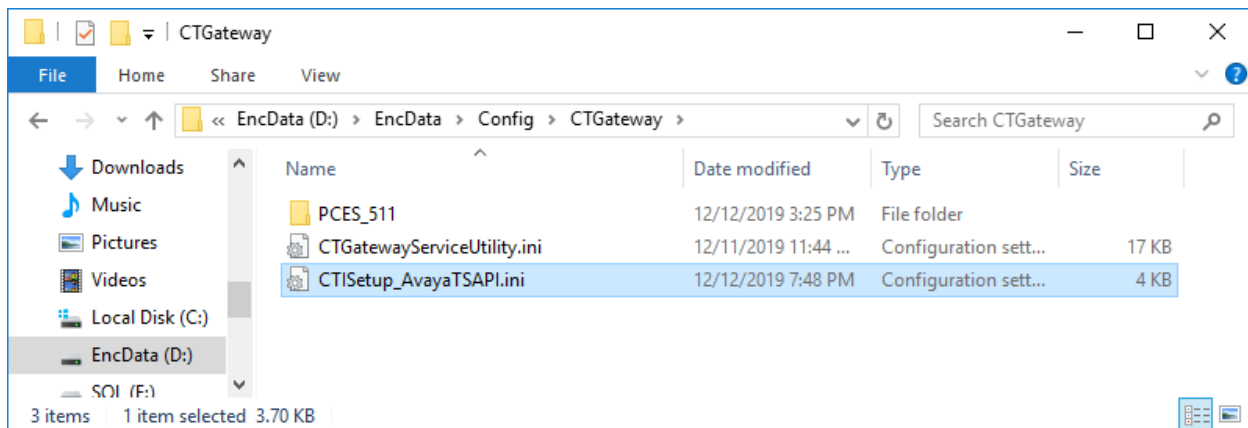
[SoftPhone2]
  Extension=65992
  Password=234567
#  SwitchName=cm
  SwitchAddr=10.64.101.236
  RTPAddress=10.64.101.207
  Codec=g711U

[SoftPhone3]
  Extension=65993
  Password=345678
#  SwitchName=cm
  SwitchAddr=10.64.101.236
  RTPAddress=10.64.101.207
  Codec=g711U

[SoftPhone4]
  Extension=65994
  Password=456789
#  SwitchName=cm
  SwitchAddr=10.64.101.236
  RTPAddress=10.64.101.207
  Codec=g711U
```

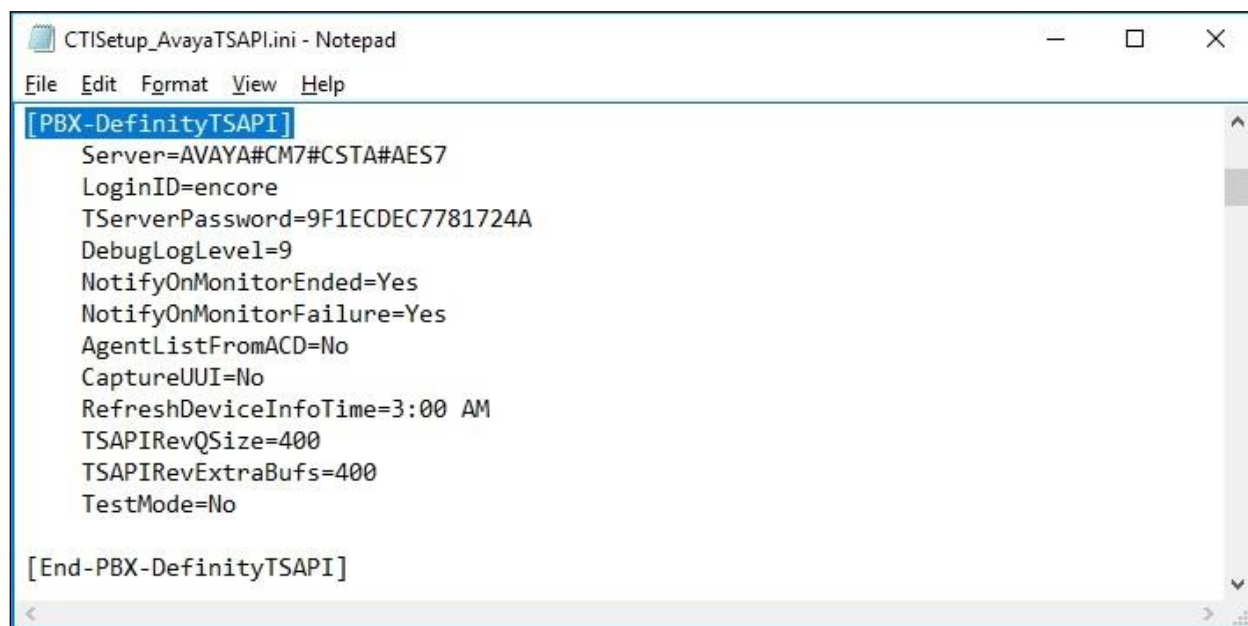
8.2. Administer CTG Settings

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

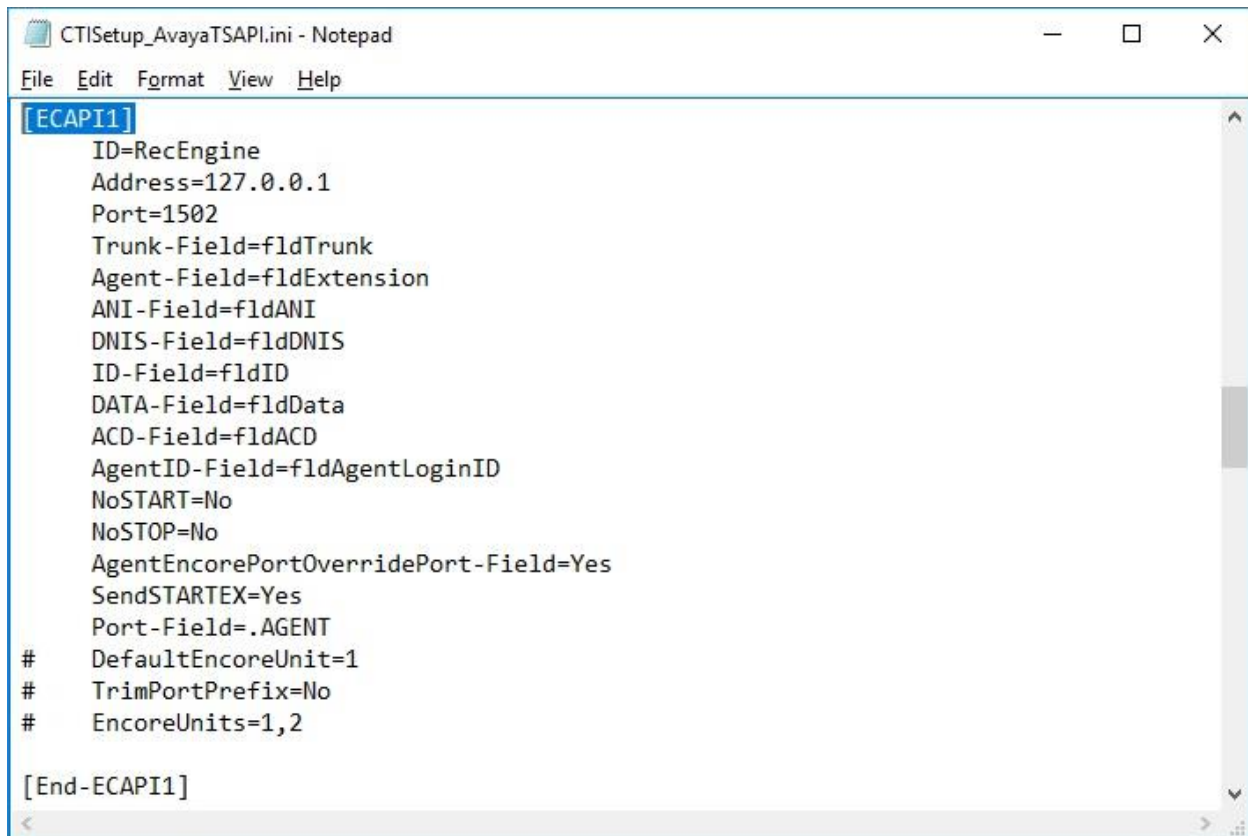


In the **PBX-DefinityTSAPI** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Server:** The Tlink name from **Section 6.9**.
- **LoginID:** The Encore user ID from **Section 6.5**.
- **DebugLogLevel:** An appropriate log level with “9” being highest and used in the testing.



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



```
CTISetup_AvayaTSAPI.ini - Notepad
File Edit Format View Help
[ECAPI1]
  ID=RecEngine
  Address=127.0.0.1
  Port=1502
  Trunk-Field=fldTrunk
  Agent-Field=fldExtension
  ANI-Field=fldANI
  DNIS-Field=fldDNIS
  ID-Field=fldID
  DATA-Field=fldData
  ACD-Field=fldACD
  AgentID-Field=fldAgentLoginID
  NoSTART=No
  NoSTOP=No
  AgentEncorePortOverridePort-Field=Yes
  SendSTARTEX=Yes
  Port-Field=.AGENT
# DefaultEncoreUnit=1
# TrimPortPrefix=No
# EncoreUnits=1,2

[End-ECAPI1]
```

Scroll further down to the **ACDs** 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. In the compliance testing, two ACD entries were created as shown below.



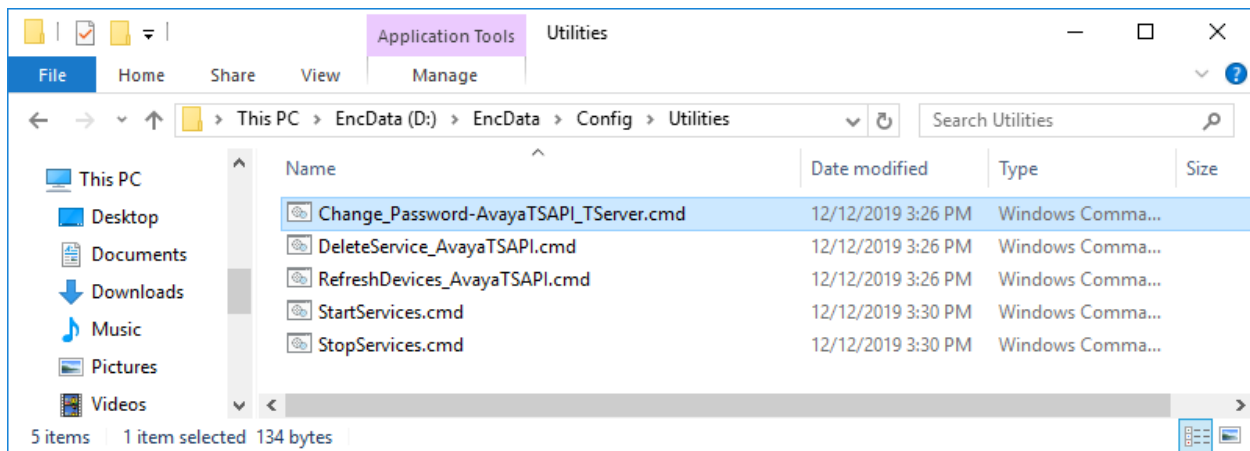
```
CTISetup_AvayaTSAPI.ini - Notepad
File Edit Format View Help
# =====
#
# ACDs
# This is required by some integrations
#
[ACD1]
ID=61001

[ACD2]
ID=61002

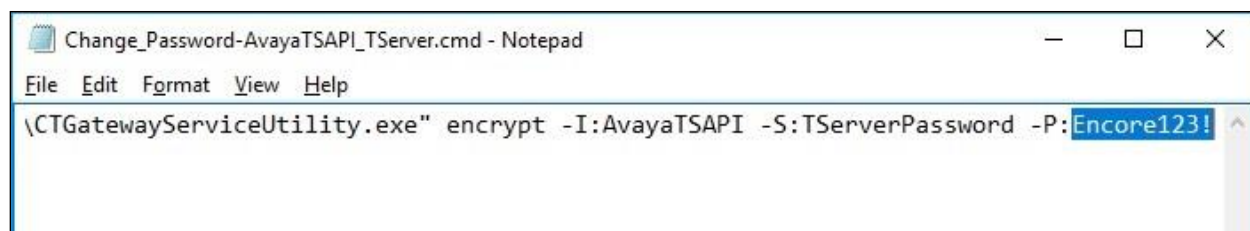
# =====
```

8.3. Encrypt TSAPI Password

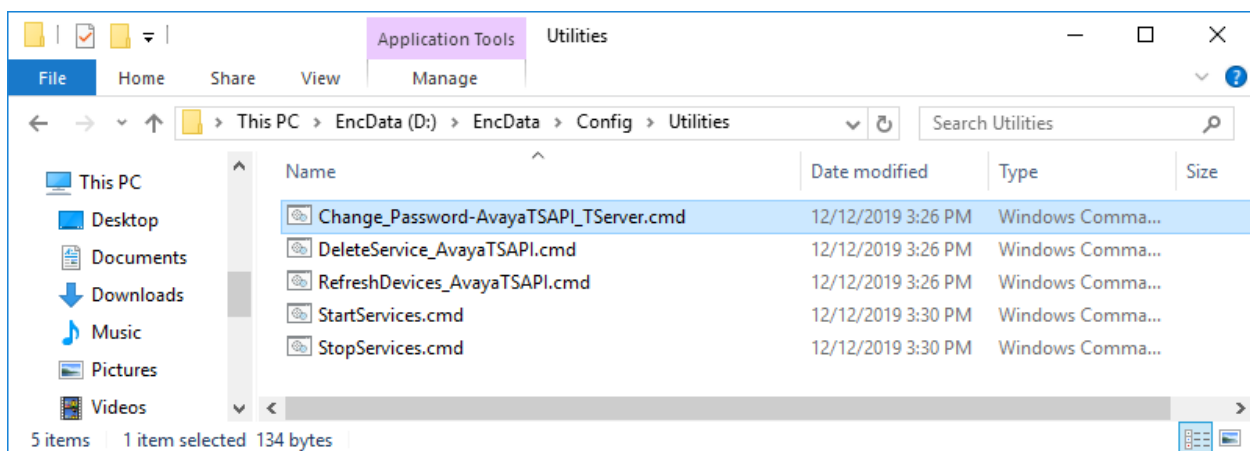
Navigate to the **D:\EncData\Config\Utilities** directory to edit the **Change_Password-AvayaTSAPI_TServer.cmd** file.



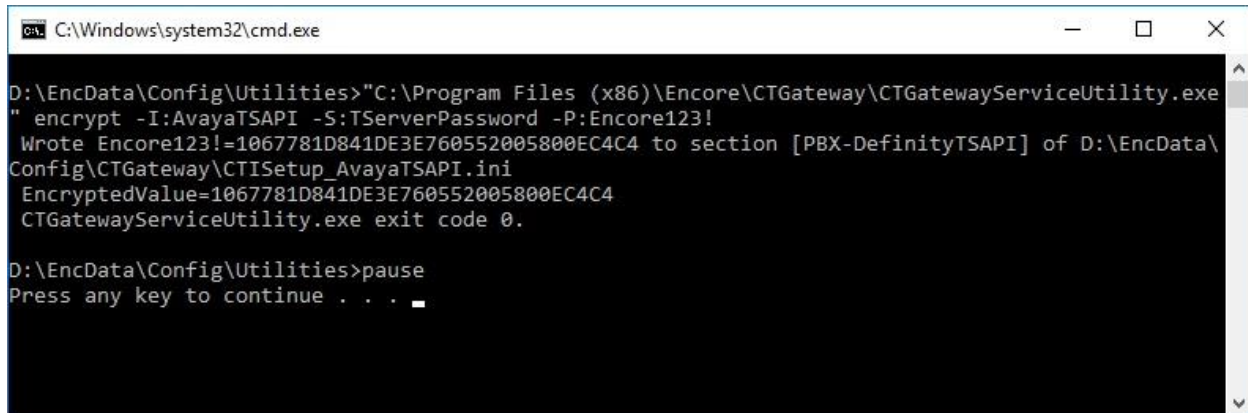
Navigate to the **-P** option toward the end of the line and replace the default value with the Encore user password from **Section 6.5** as shown below.



After updating and saving of the file, double-click on the same file to set and encrypt the TSAPI password.



A command prompt window is launched automatically and shows the result of setting and encrypting the TSAPI password as shown below.



```
C:\Windows\system32\cmd.exe

D:\EncData\Config\Utilities>"C:\Program Files (x86)\Encore\CTGateway\CTGatewayServiceUtility.exe"
 encrypt -I:AvayaTSAPI -S:TServerPassword -P:Encore123!
 Wrote Encore123!=1067781D841DE3E760552005800EC4C4 to section [PBX-DefinityTSAPI] of D:\EncData\
 Config\CTGateway\CTISetup_AvayaTSAPI.ini
 EncryptedValue=1067781D841DE3E760552005800EC4C4
 CTGatewayServiceUtility.exe exit code 0.

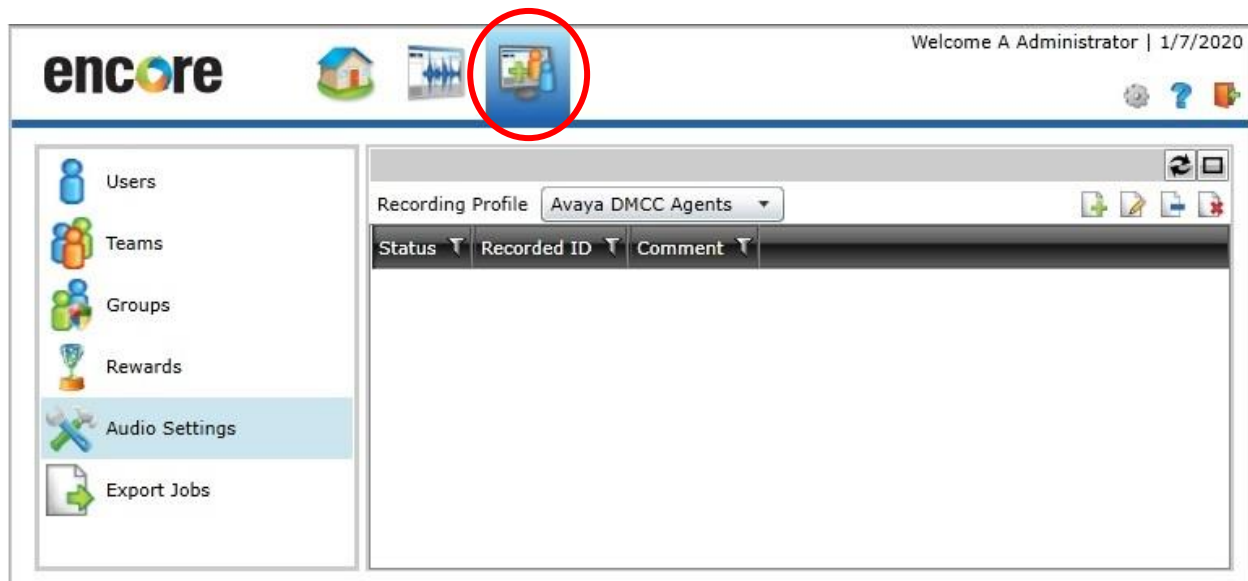
D:\EncData\Config\Utilities>pause
 Press any key to continue . . .
```

8.4. Administer Recorded ID

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 below is displayed. Click **Login** and log in using the appropriate credentials.



The **encore** screen is displayed. Select the **User and System Configuration** icon from the top menu, followed by **Audio Settings** in the subsequent screen to display the screen below.

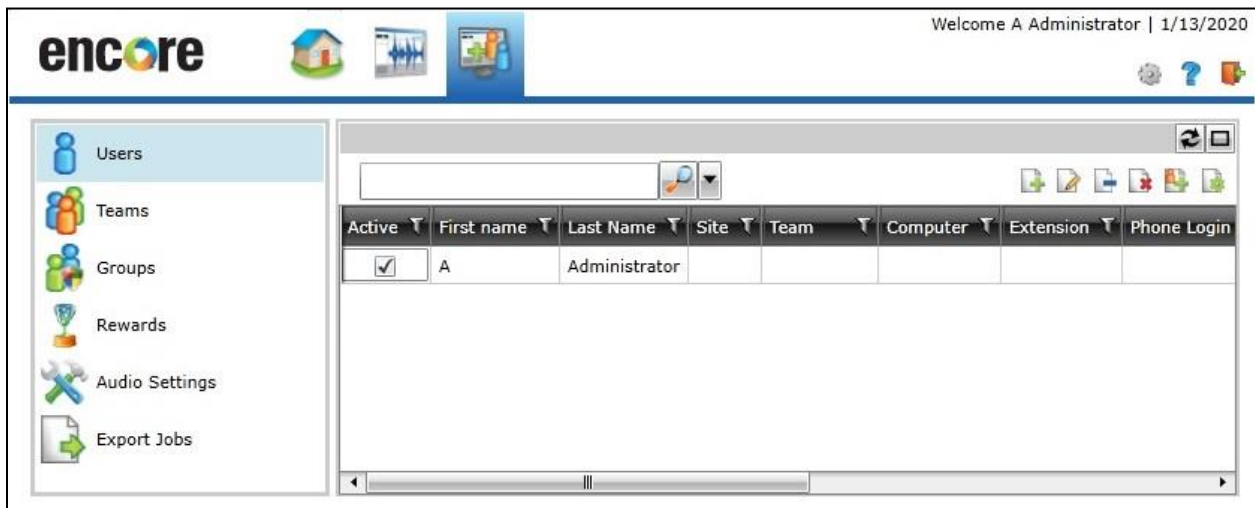


Follow reference [4] to create an entry for each agent station from **Section 3**. In the compliance testing, two recorded IDs were created as shown below.



8.5. Administer Users

Select **Users** from the left pane to display the screen below.



encore

Welcome A Administrator | 1/13/2020

Users

Teams

Groups

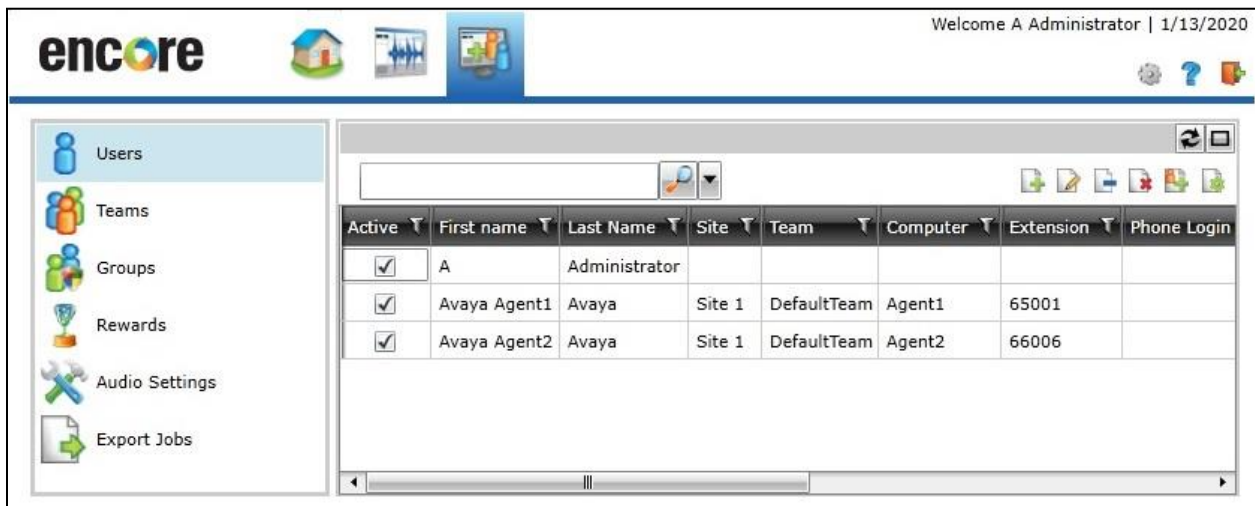
Rewards

Audio Settings

Export Jobs

Active	First name	Last Name	Site	Team	Computer	Extension	Phone Login
<input checked="" type="checkbox"/>	A	Administrator					

Follow reference [4] to create an entry for each agent station from **Section 3**. In the compliance testing, two users were created as shown below.



encore

Welcome A Administrator | 1/13/2020

Users

Teams

Groups

Rewards

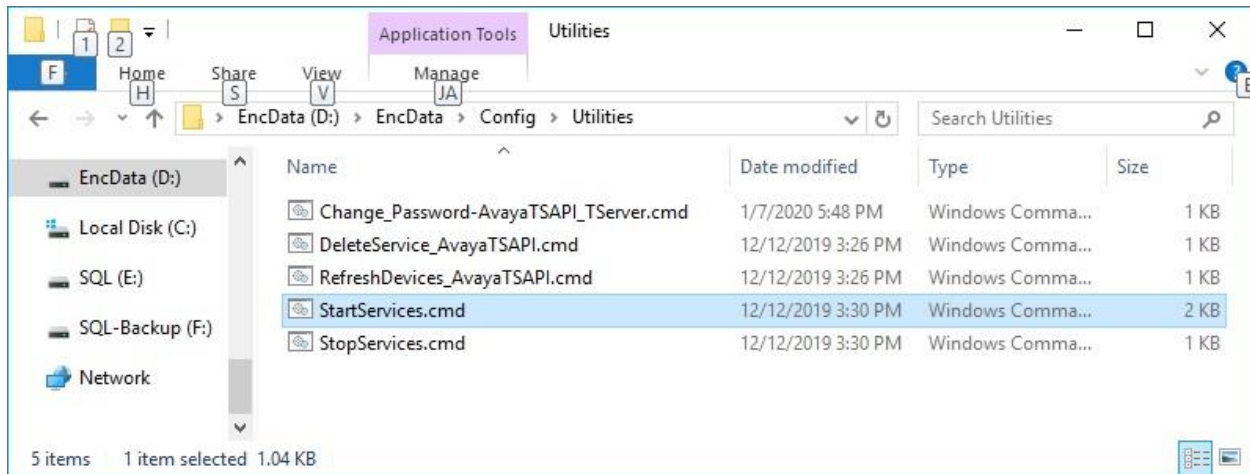
Audio Settings

Export Jobs

Active	First name	Last Name	Site	Team	Computer	Extension	Phone Login
<input checked="" type="checkbox"/>	A	Administrator					
<input checked="" type="checkbox"/>	Avaya Agent1	Avaya	Site 1	DefaultTeam	Agent1	65001	
<input checked="" type="checkbox"/>	Avaya Agent2	Avaya	Site 1	DefaultTeam	Agent2	66006	

8.6. Start Services

Navigate to the **D:\EncData\Config\Utilities** directory and double-click on **StartServices.cmd** to start services.



A command prompt window is launched automatically and shows the result of starting services as shown below.

The screenshot shows a Windows Command Prompt window titled 'C:\Windows\system32\cmd.exe'. The output of the command is as follows:

```
Starting Services

Successfully started - CTGatewayService_AvayaTSAPI
Successfully started - DataManagerService
Successfully started - DataManagerTransport
Successfully started - EncoreInformationService
Successfully started - EncoreSystemService
Successfully started - RecEngine
Successfully started - EncoreEventService
Successfully started - WygNetControl2

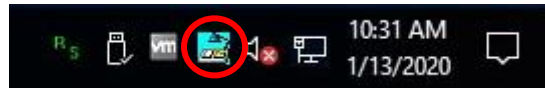
Waiting 10 seconds before starting ESGS

Successfully started - ESGS

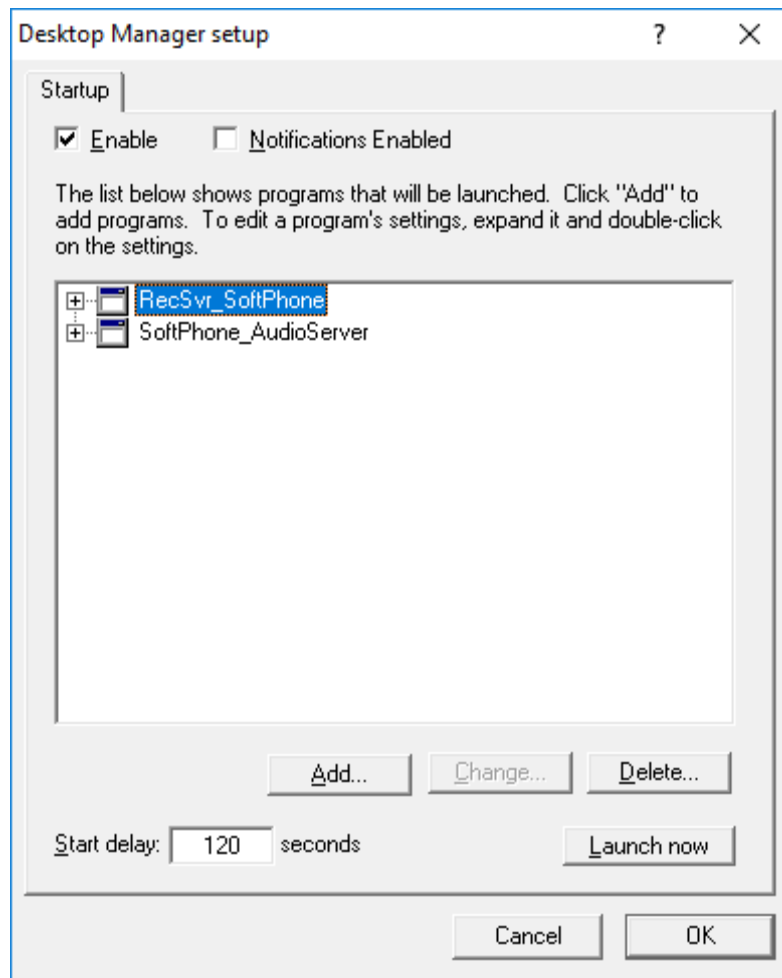
Press any key to continue . . .
```

8.7. Launch Programs

From the server system tray, right click on the **Desktop Manager** icon shown below and select **Configure**.



The **Desktop Manager setup** screen is displayed. Check **Enable** to allow automatic launch of listed programs shown below.



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	10	no	aes7	established	25	25


Verify registration status of the 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, in this case “10.64.101.239” 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
65000	1608	IP_Phone	192.168.200.142
tcp	1	1.3120	10.64.101.236
65001	9611	IP_Phone	192.168.200.217
tls	1	6.8202	10.64.101.236
65991	4610	IP_API_A	10.64.101.239
tcp	1	3.2040	10.64.101.236
65992	4610	IP_API_A	10.64.101.239
tcp	1	3.2040	10.64.101.236
65993	4610	IP_API_A	10.64.101.239
tcp	1	3.2040	10.64.101.236
65994	4610	IP_API_A	10.64.101.239
tcp	1	3.2040	10.64.101.236

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify 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**, in this case “4” as shown below.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jan 7 13:52:23 2020 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: 8.1.0.0.9-1
Server Date and Time: Tue Jan 07 14:21:06 EST 2020
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 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	Thu Jan 2 14:34:03 2020	Online	18	4	19	26	30

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

Verify 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**, in this case “4”.



Application Enablement Services

Management Console

Welcome: User
 Last login: Tue Jan 7 11:47:17 2020 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: 8.1.0.0.9-1
 Server Date and Time: Tue Jan 07 13:53:52 EST 2020
 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
 - ▶ Logs
 - ▶ Log Manager
 - ▼ **Status and Control**
 - CVLAN Service Summary
 - DLG Services Summary
 - **DMCC Service Summary**
 - Switch Conn Summary
 - TSAPI Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
 Generated on Tue Jan 07 13:53:47 EST 2020

Service Uptime:	83 days, 6 hours 20 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
☐	8A23548FBDC719A9C F99391558955E6E-0	encore	SPAS1	10.64.101.207	XML Unencrypted	4

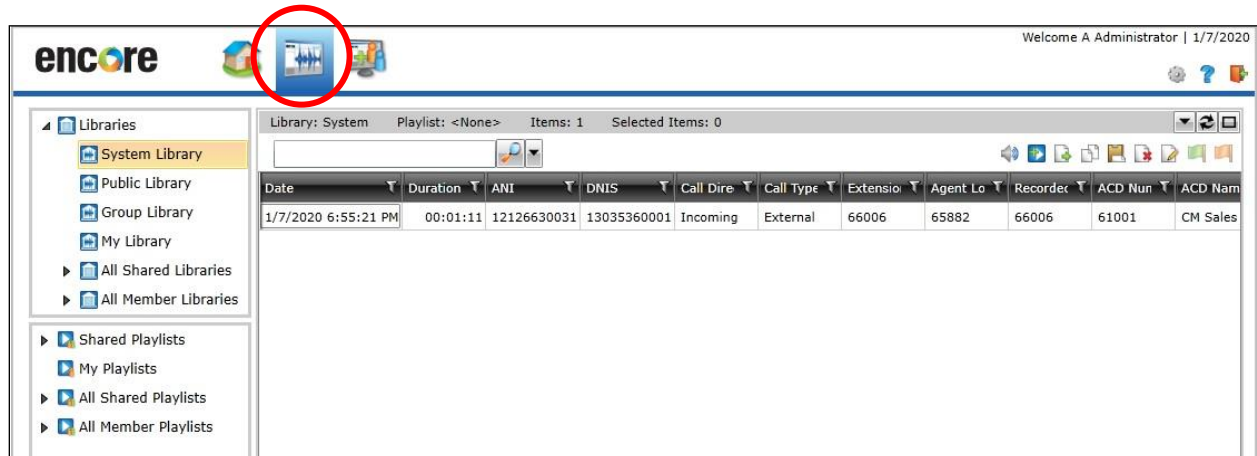
Terminate Sessions
Show Terminated Sessions

Item 1-1 of 1
1 Go

9.3. Verify dvsAnalytics Encore

Log an agent into the skill groups to handle and complete an ACD call. Access the Encore web interface using the procedures from **Section 8.5**.

From the **encore** screen, 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.



10. Conclusion

These Application Notes describe the configuration steps required for dvsAnalytics Encore 7.1 to successfully interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 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 8.1.x, Issue 3, August 2019, available at <http://support.avaya.com>.
2. *Administering Aura® Application Enablement Services*, Release 8.1.x, Issue 2, August 2019, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 8.1, Issue 1, June 2019, available at <http://support.avaya.com>.
4. *Avaya Aura™ Communication Manager TSAPI Installation Addendum*, January 7, 2020, available from dvsAnalytics Support.

©2020 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.