Avaya Solution & Interoperability Test Lab

Application Notes for dvsAnalytics Encore 2.3.1 with Avaya Aura® Communication Manager Using Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for dvsAnalytics Encore 2.3.1 to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services.

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.

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 2.3.1 to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services.

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 the skill groups and agent stations to be recorded. When there is an active call on the monitored station, dvsAnalytics Encore is informed of the call via event reports from the TSAPI interface. dvsAnalytics Encore starts the call recording by sending a Service Observing button press from a virtual IP softphone via the DMCC interface to observe the active call, and uses the Media Control Events from the DMCC interface to obtain the media from the virtual IP softphone. The TSAPI event reports are used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Encore application, the application automatically registers virtual IP softphones to Communication Manager using Application Enablement Services DMCC, and requests monitoring on the skill groups and agent stations using Application Enablement Services TSAPI.

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

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

The verification of tests included using the Encore logs for proper message exchanges, and using the Encore web interface for proper logging and playback of calls.

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 the areas of event notification and value queries.
- Use of DMCC registration services to register and un-register virtual IP softphones.
- Use of DMCC physical device services to activate Service Observing for virtual IP softphones.
- Use of DMCC monitoring services and media control events to obtain the media from virtual IP softphones.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, simultaneous, conference, and transfer.

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

2.2. Test Results

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

- All recordings included the confirmation tone for the Service Observing activation, and missed the first one to two seconds of the user conversation.
- In the simultaneous calls scenario for the same agent, where the agent placed an inbound call on hold and started a separate outbound call to a non-monitored supervisor without using transfer/conference, there were two recording entries generated for the agent. The first recording included the audio from the beginning of the inbound call up to the held point, plus the entire audio from the outbound call. The second recording included the audio for the inbound call after the call was taken off hold, to the end of the inbound call.
- The server provided audible alarms for unexpected events such as link interruptions and removal of monitored resources on Communication Manager.

2.3. Support

Technical support on Encore can be obtained through the following:

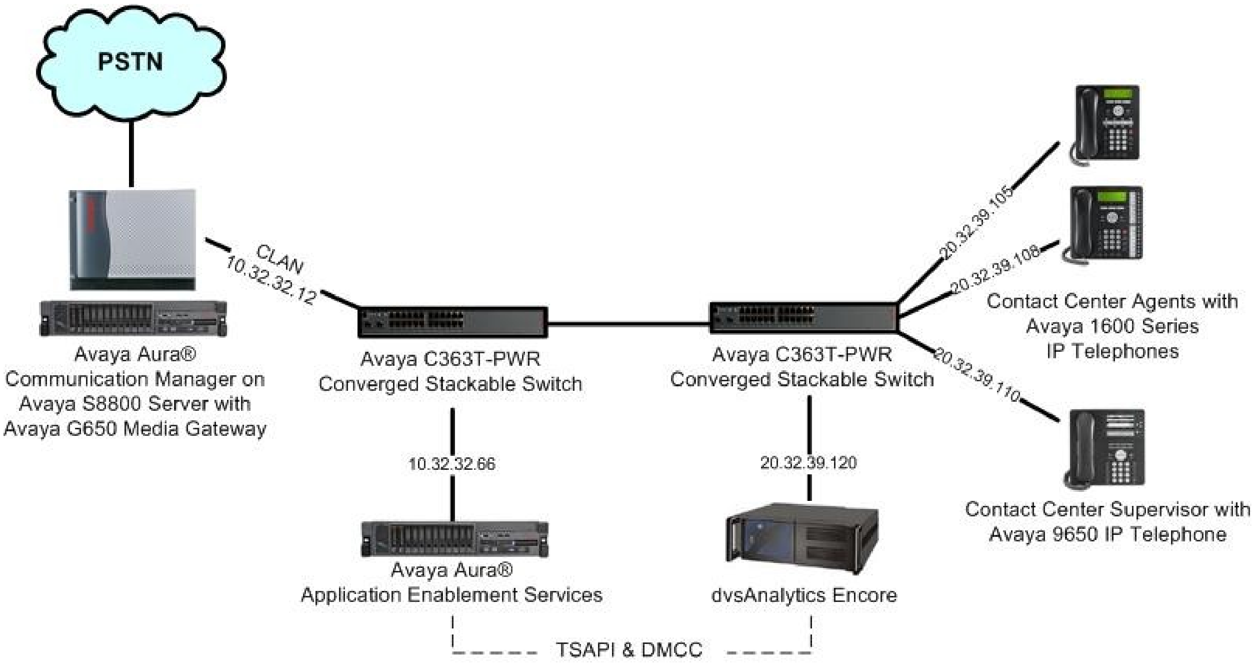
- **Phone:** (800) 910-4564
- **Email:** Support@dvsAnalytics.com

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 group and agent station extensions shown in the table below.

Contact Center Device Type	Extension
Skill Group	65555
Agent Station	65001, 65002



4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya Aura® Communication Manager on Avaya S8800 Server	6.0.1 SP 5.01 (R016x.00.1.510.1-19303)
Avaya G650 Media Gateway • TN799DP C-LAN Circuit Pack • TN2302AP IP Media Processor	 HW01 FW040 HW20 FW122
Avaya Aura® Application Enablement Services	6.1.1
Avaya 1600 Series IP Telephones (H.323)	1.3
Avaya 9650 IP Telephone (H.323)	3.1
dvsAnalytics Encore on Windows Server 2003 SP 2 • Avaya TSAPI Windows Client	2.3.1 4.2

5. Configure Avaya Aura® Communication Manager

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

- Verify License
- Administer system parameters features
- Administer CTI link
- Administer IP codec set
- Administer class of restriction
- Administer virtual IP softphones

5.1. Verify License

Log in to the System Access Terminal (SAT) 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 3**. 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   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? y              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? y                      DCS (Basic)? y
```

Navigate to **Page 6**, and verify that the **Service Observing (Basic)** customer option is set to “y”.

```
display system-parameters customer-options                      Page   6 of  11
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 6.0

                                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
```

5.2. Administer System Parameters Features

Use the “change system-parameters features” command to enable **Allow Two Observers in Same Call**, which is located on **Page 11**.

```
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: 5
          Direct Agent Announcement Extension:                   Delay:
    Message Waiting Lamp Indicates Status For: station

  VECTORING
                    Converse First Data Delay: 0      Second Data Delay: 2
               Converse Signaling Tone (msec): 100         Pause (msec): 70
                     Prompting Timeout (secs): 10
                 Interflow-qpos EWT Threshold: 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
     Service Observing Allowed with Exclusion? n
             Allow Two Observers in Same Call? Y
```

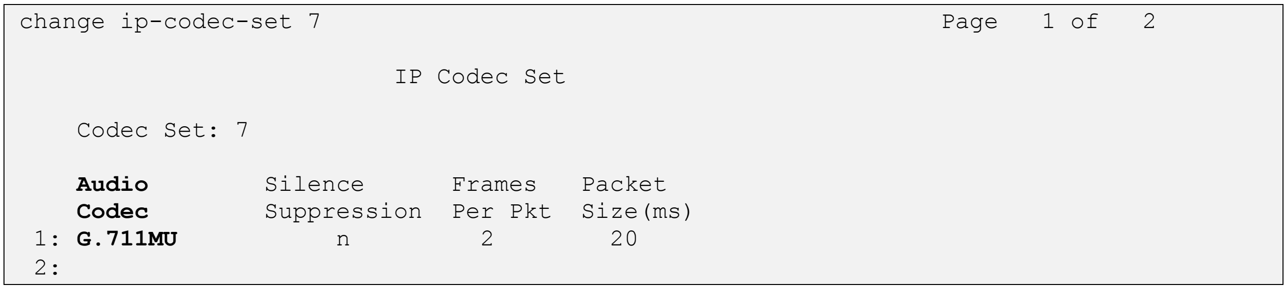
5.3. Administer CTI Link

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: 60100
     Type: ADJ-IP
                                                                        COR: 1
     Name: TSAPI Link
```

5.4. Administer IP Codec Set

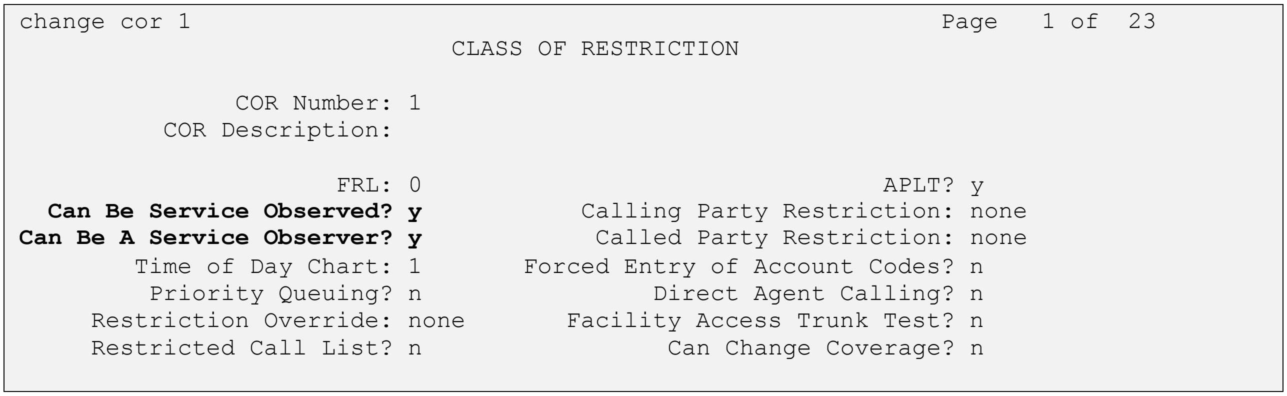
Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with Encore. For Audio Codec, enter “G.711MU”, which is the only codec type supported by Encore. In the compliance testing, this IP codec set was assigned to the agents and to the virtual IP softphones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



```
change ip-codec-set 7                                             Page   1 of   2

                          IP Codec Set

    Codec Set: 7

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2:
```

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 agents and to the virtual IP softphones used by Encore.

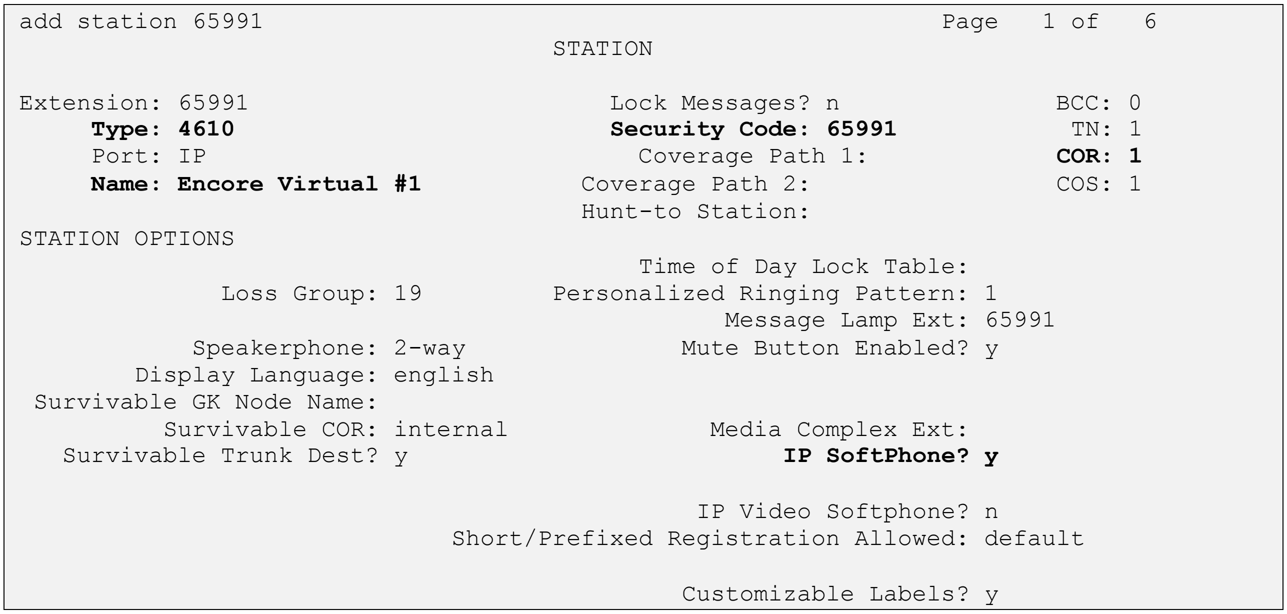


```
change cor 1                                                      Page   1 of  23
                              CLASS OF RESTRICTION

               COR Number: 1
          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 Virtual IP Softphones

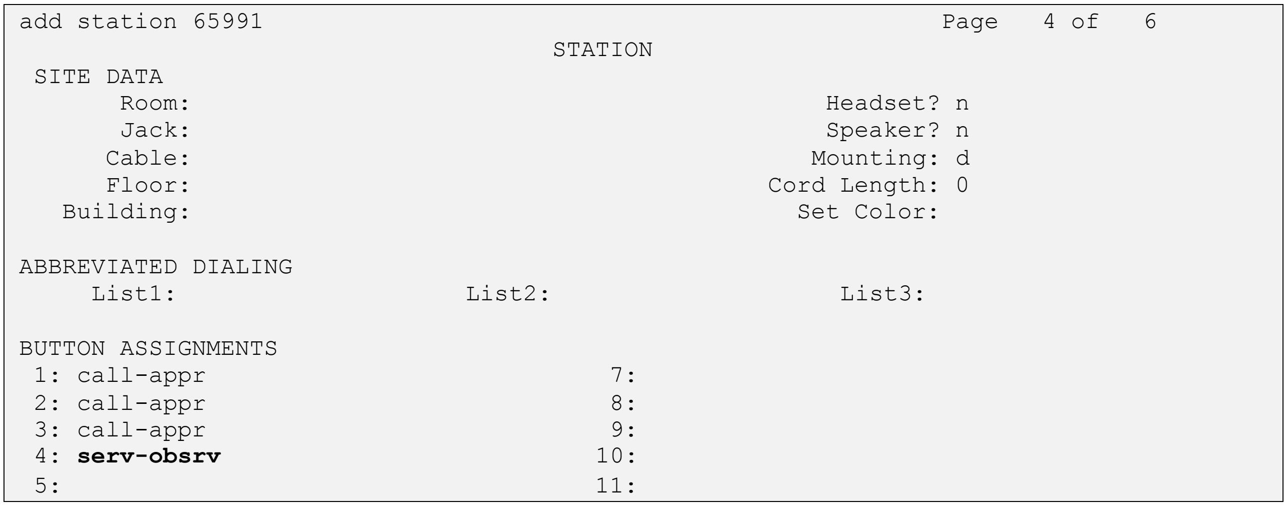
Add a virtual softphone using the “add station n” command, where “n” is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Type:** “4610”
- **Name:** A descriptive name.
- **Security Code:** A desired value.
- **COR:** The class of restriction number from **Section 5.5**.
- **IP SoftPhone:** “y”



```
add station 65991                                               Page   1 of   6
                                     STATION

Extension: 65991                         Lock Messages? n               BCC: 0
     Type: 4610                          Security Code: 65991            TN: 1
     Port: IP                              Coverage Path 1:             COR: 1
     Name: Encore Virtual #1           Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
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   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 softphones. In the compliance testing, two virtual softphones were administered as shown below, to allow for two simultaneous call recordings.

```
list station 65991 count 3

                                  STATIONS

Ext/          Port/   Name/                       Room/       Cv1/ COR/   Cable/
 Hunt-to       Type      Surv GK NN        Move    Data Ext    Cv2  COS TN Jack

65991         S00020  Encore Virtual #1                            1
               4610                        no                      1   1
65992         S00039  Encore Virtual #2                            1
               4610                        no                      1   1
```

6. Configure Avaya Aura® Application Enablement Services

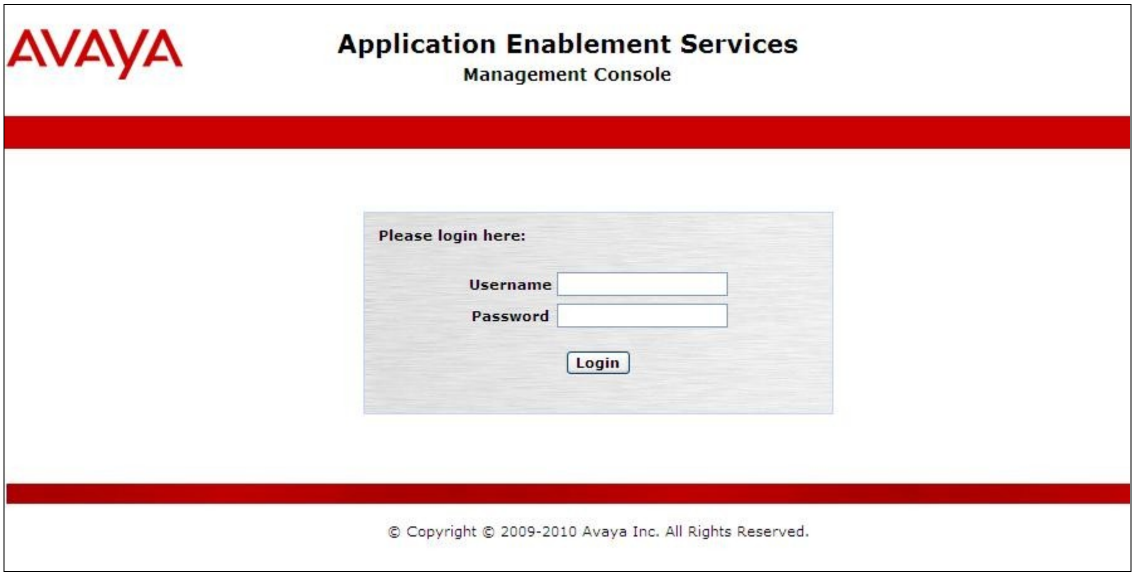
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer Encore user
- Enable DMCC unencrypted port

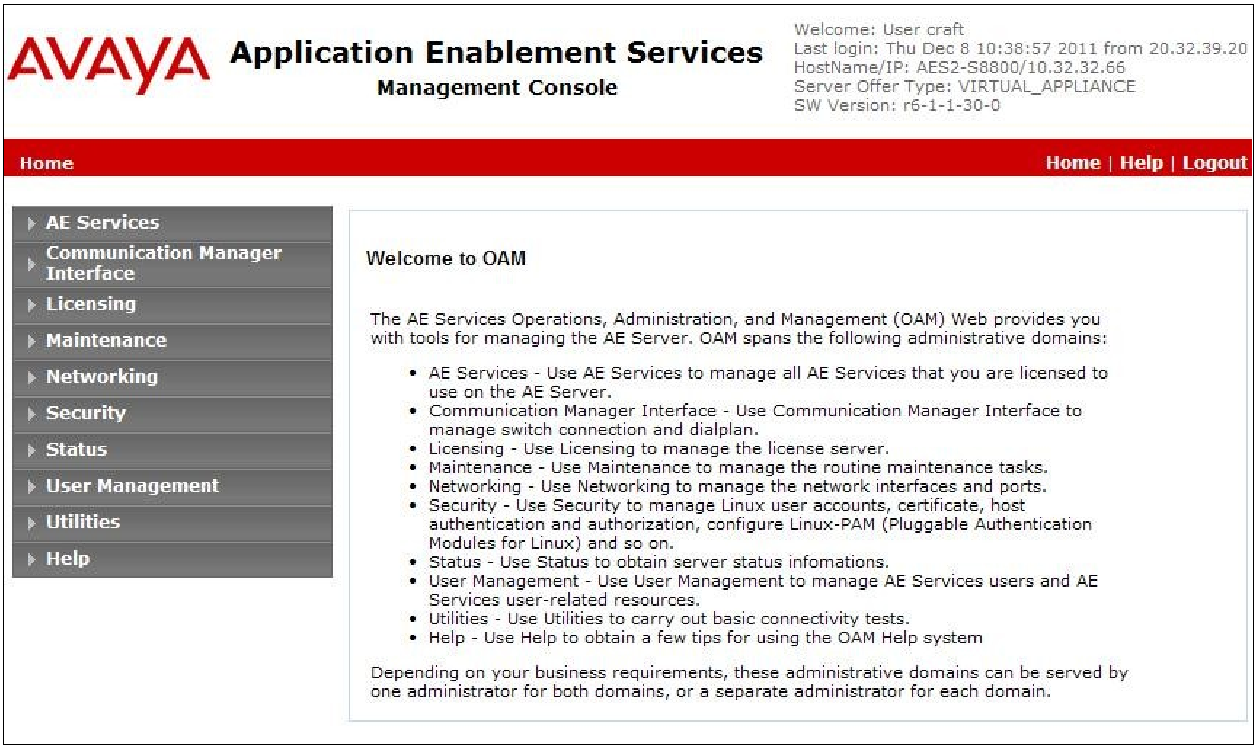
6.1. Launch OAM Interface

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.


AVAYA
Application Enablement Services
Management Console
Please login here:
Username
Password
Login
© Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

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



Welcome: User craft
Last login: Thu Dec 8 10:38:57 2011 from 20.32.39.20
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Welcome to OAM

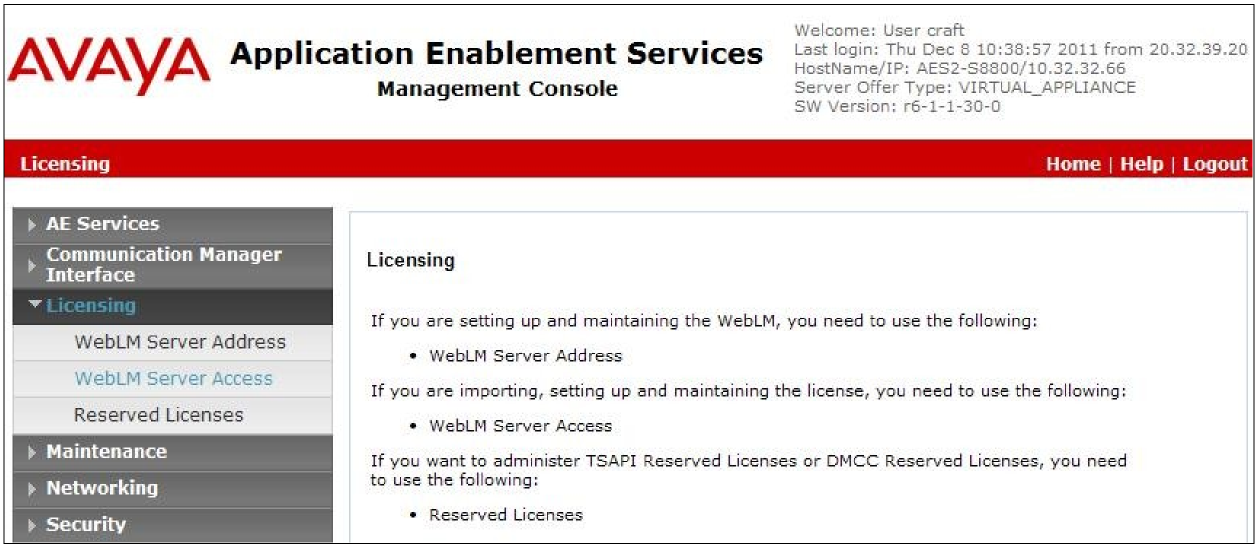
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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.
- 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 infomations.
- 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 both domains, or a separate administrator for each domain.

6.2. Verify License

Select **Licensing > WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in with the appropriate credentials.



Welcome: User craft
Last login: Thu Dec 8 10:38:57 2011 from 20.32.39.20
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

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:

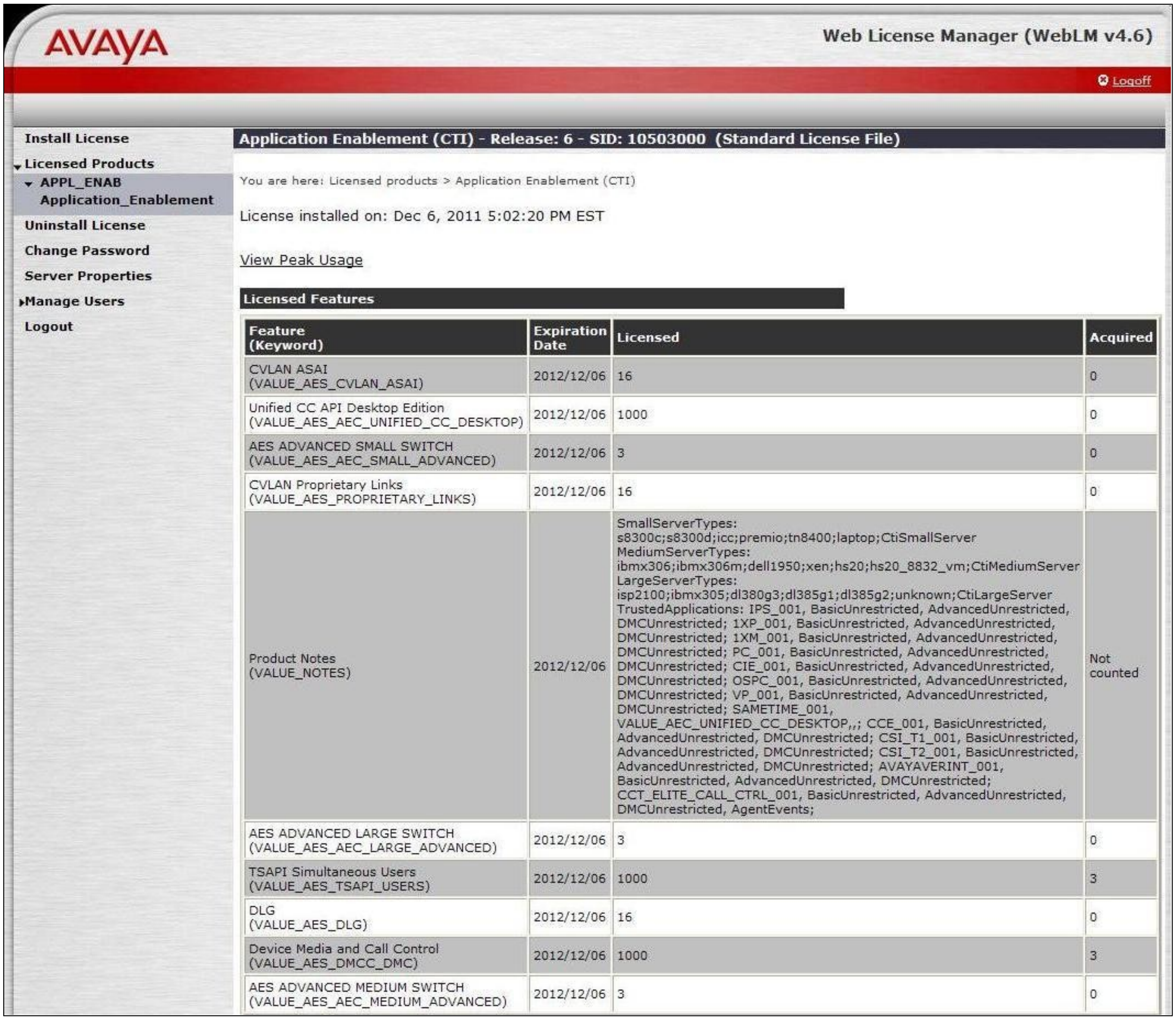
- WebLM Server Access

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

- Reserved Licenses

The **Web License Manager** screen is displayed. Select **Licensed Products > APPL_ENAB > Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users** and **Device Media and Call Control**, as shown below.



Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License File)

You are here: Licensed products > Application Enablement (CTI)

License installed on: Dec 6, 2011 5:02:20 PM EST

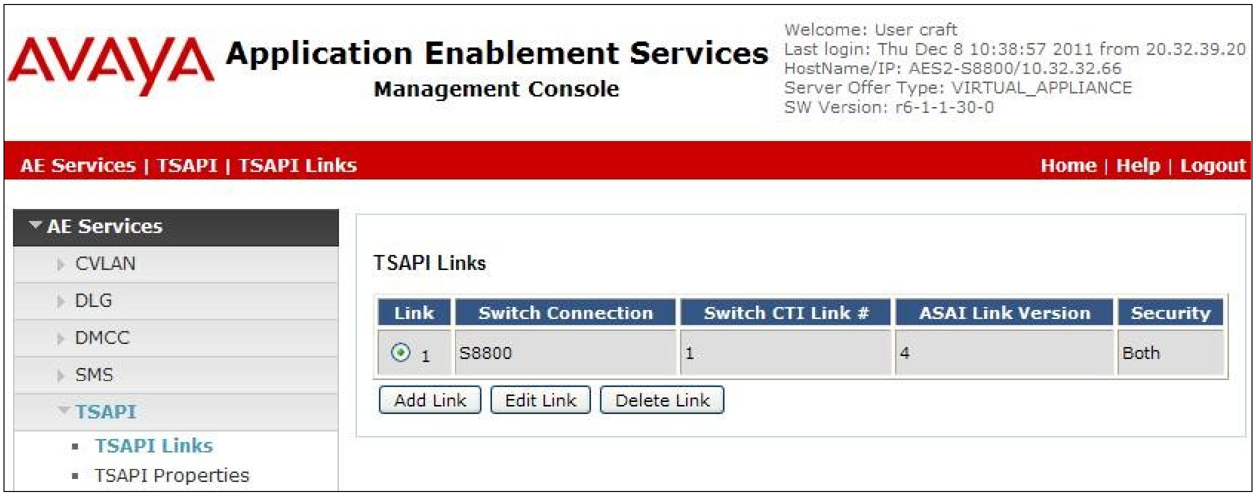
View Peak Usage

Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	2012/12/06	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	2012/12/06	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	2012/12/06	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	2012/12/06	16	0
Product Notes (VALUE_NOTES)	2012/12/06	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	2012/12/06	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	2012/12/06	1000	3
DLG (VALUE_AES_DLG)	2012/12/06	16	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	2012/12/06	1000	3
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	2012/12/06	3	0

6.3. Administer TSAPI Link

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



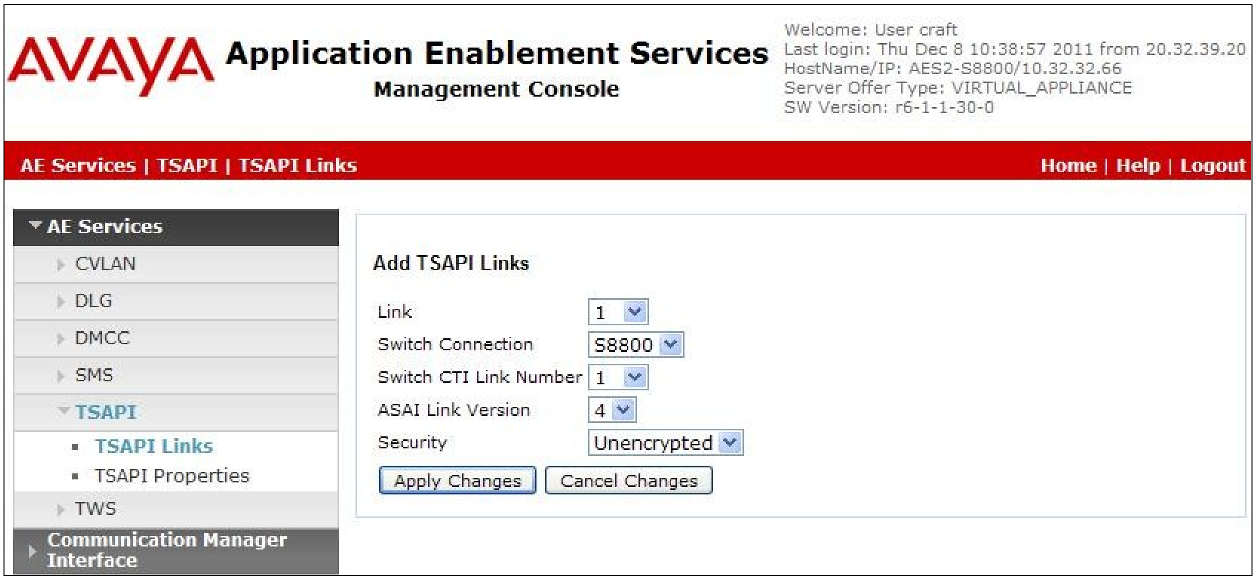
Welcome: User craft
Last login: Thu Dec 8 10:38:57 2011 from 20.32.39.20
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	S8800	1	4	Both

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 "S8800" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.3**. Retain the default values in the remaining fields, and click **Apply Changes**.



Welcome: User craft
Last login: Thu Dec 8 10:38:57 2011 from 20.32.39.20
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

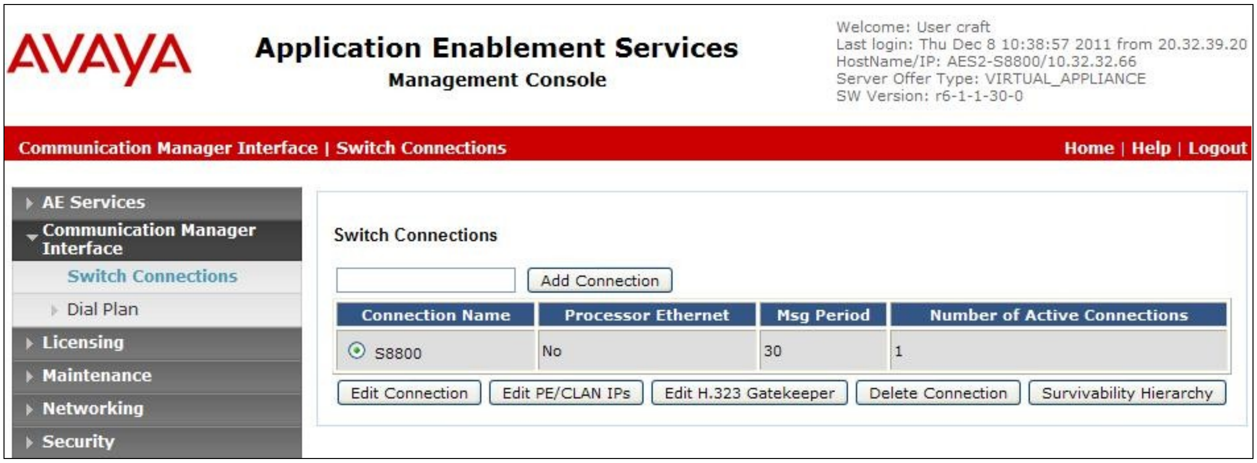
Add TSAPI Links

Link	1
Switch Connection	S8800
Switch CTI Link Number	1
ASAI Link Version	4
Security	Unencrypted

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 "S8800", and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

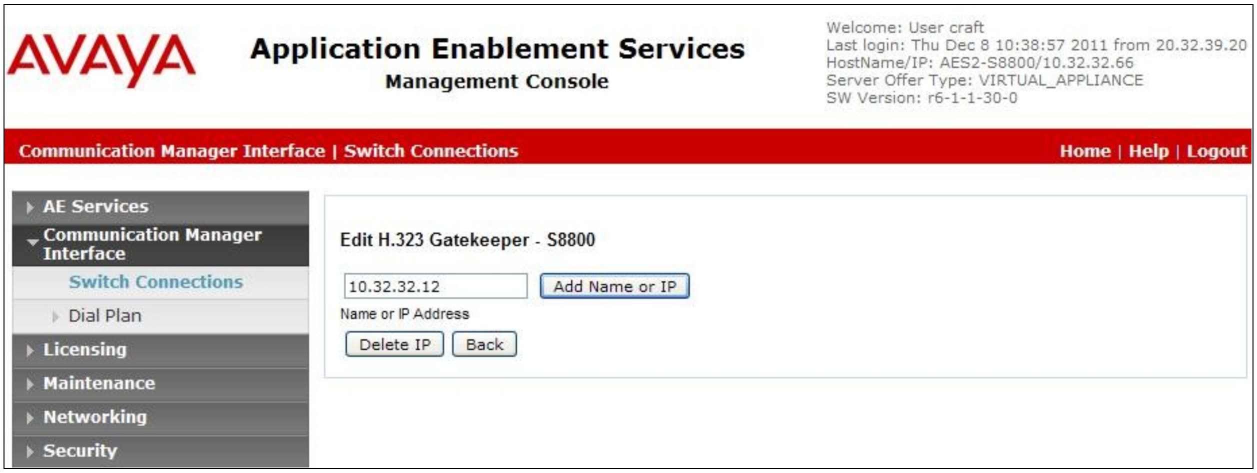


Welcome: User craft
Last login: Thu Dec 8 10:38:57 2011 from 20.32.39.20
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● S8800	No	30	1

The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as H.323 gatekeeper, in this case "10.32.32.12" as shown below. Click **Add Name or IP**.



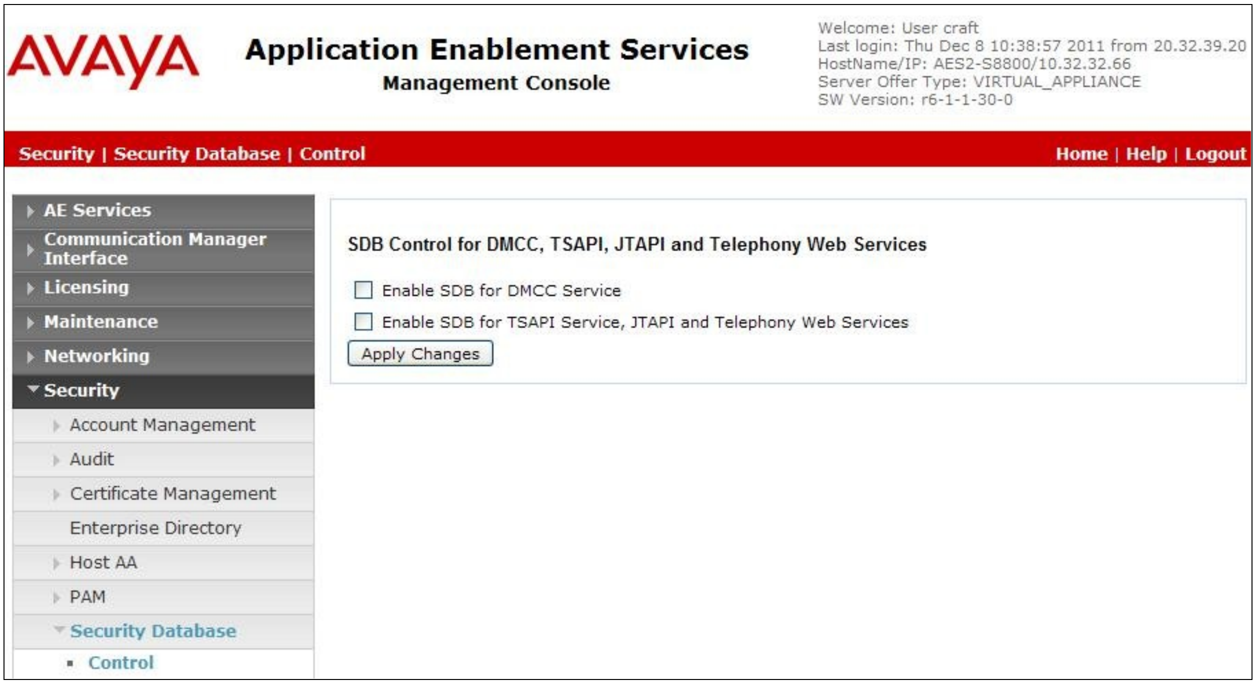
Welcome: User craft
Last login: Thu Dec 8 10:38:57 2011 from 20.32.39.20
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Edit H.323 Gatekeeper - S8800

Name or IP Address: 10.32.32.12

6.5. Disable 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, and click **Apply Changes**.



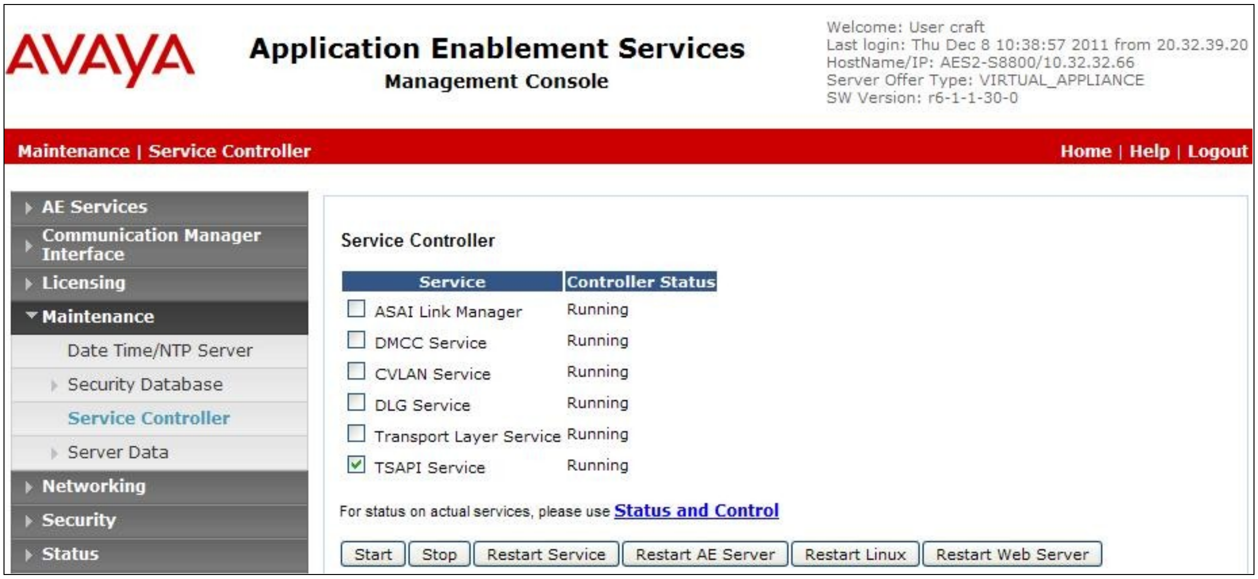
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

□ Enable SDB for DMCC Service

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

6.6. Restart TSAPI Service

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



Service Controller

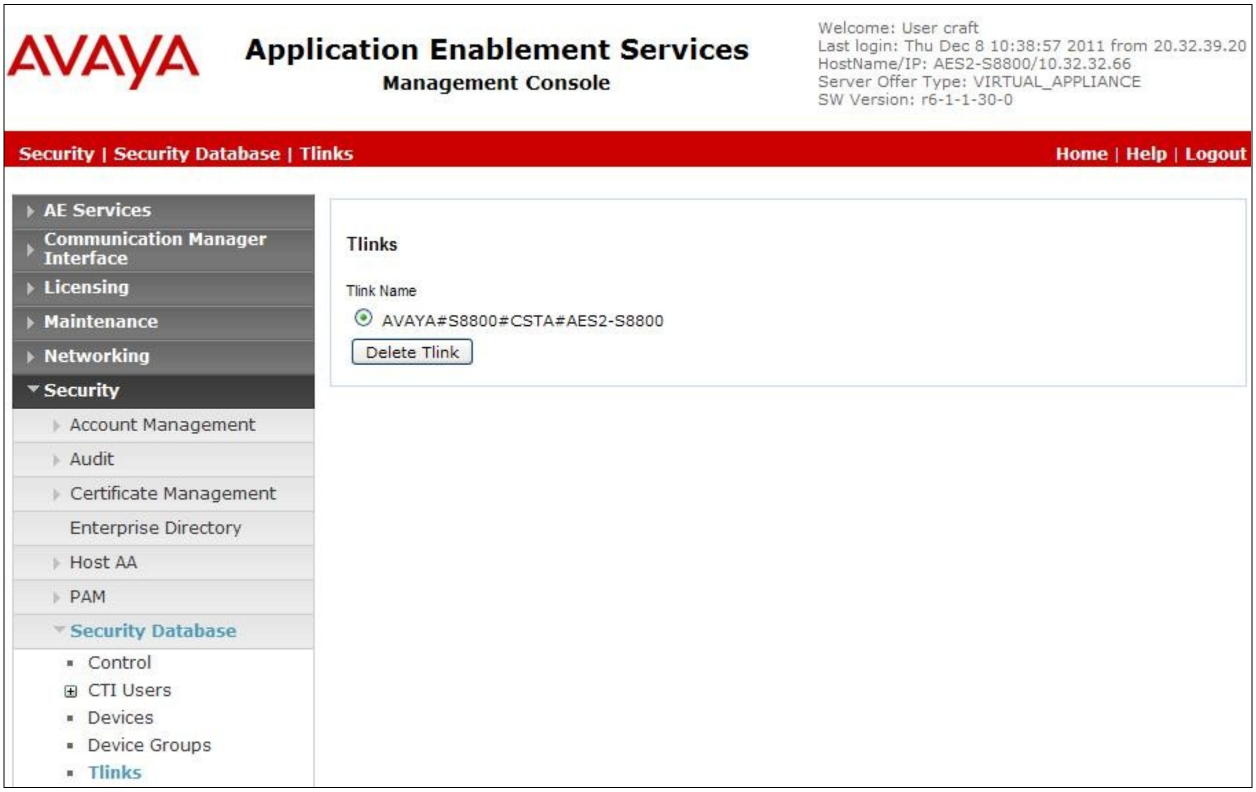
Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.7. 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#**S8800**#CSTA-S#AES2-S8800". Note the use of the switch connection "S8800" from **Section 6.3** as part of the Tlink name.



Welcome: User craft
Last login: Thu Dec 8 10:38:57 2011 from 20.32.39.20
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Tlinks

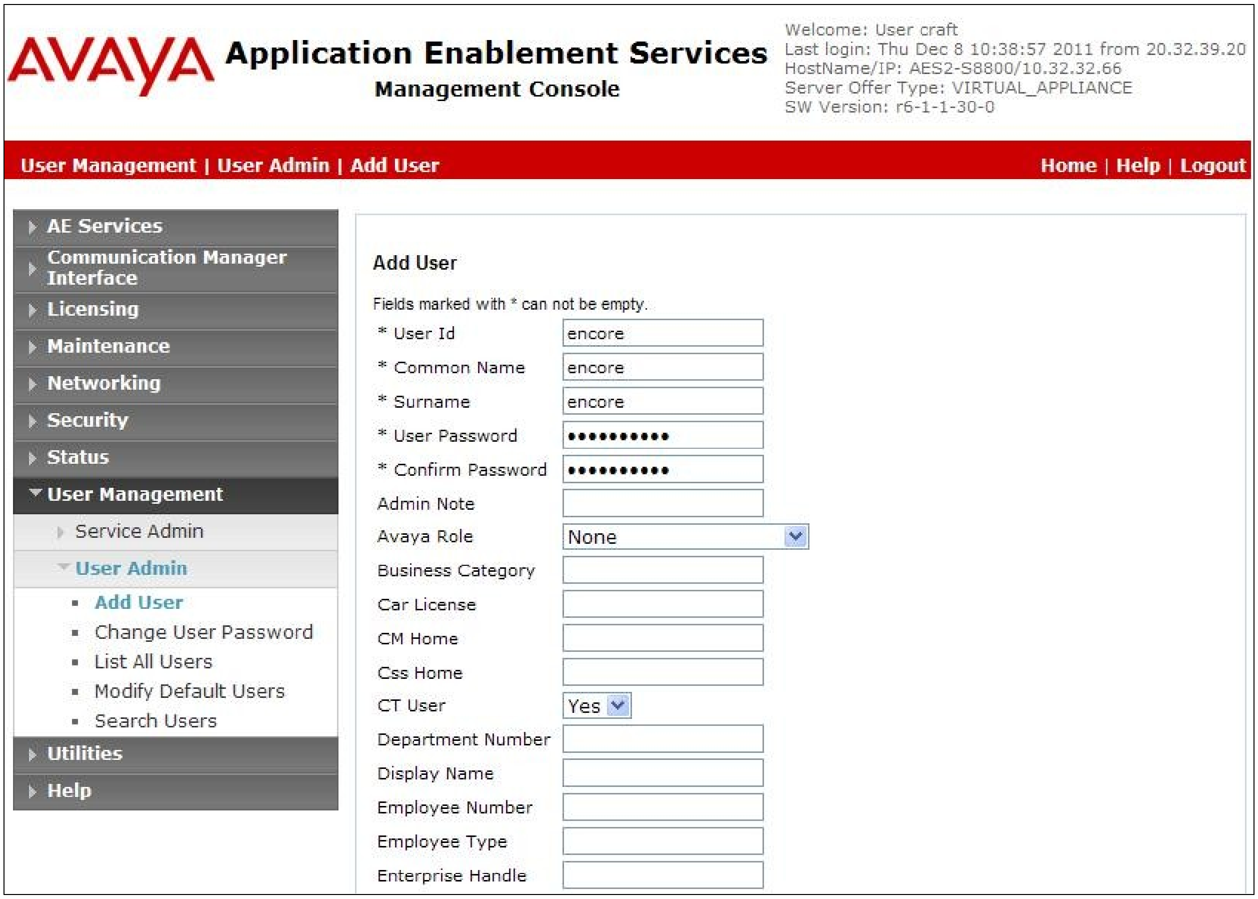
Tlink Name

● AVAYA#S8800#CSTA#AES2-S8800

6.8. 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. Click **Apply** at the bottom of the screen (not shown below).



Welcome: User craft
Last login: Thu Dec 8 10:38:57 2011 from 20.32.39.20
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Add User

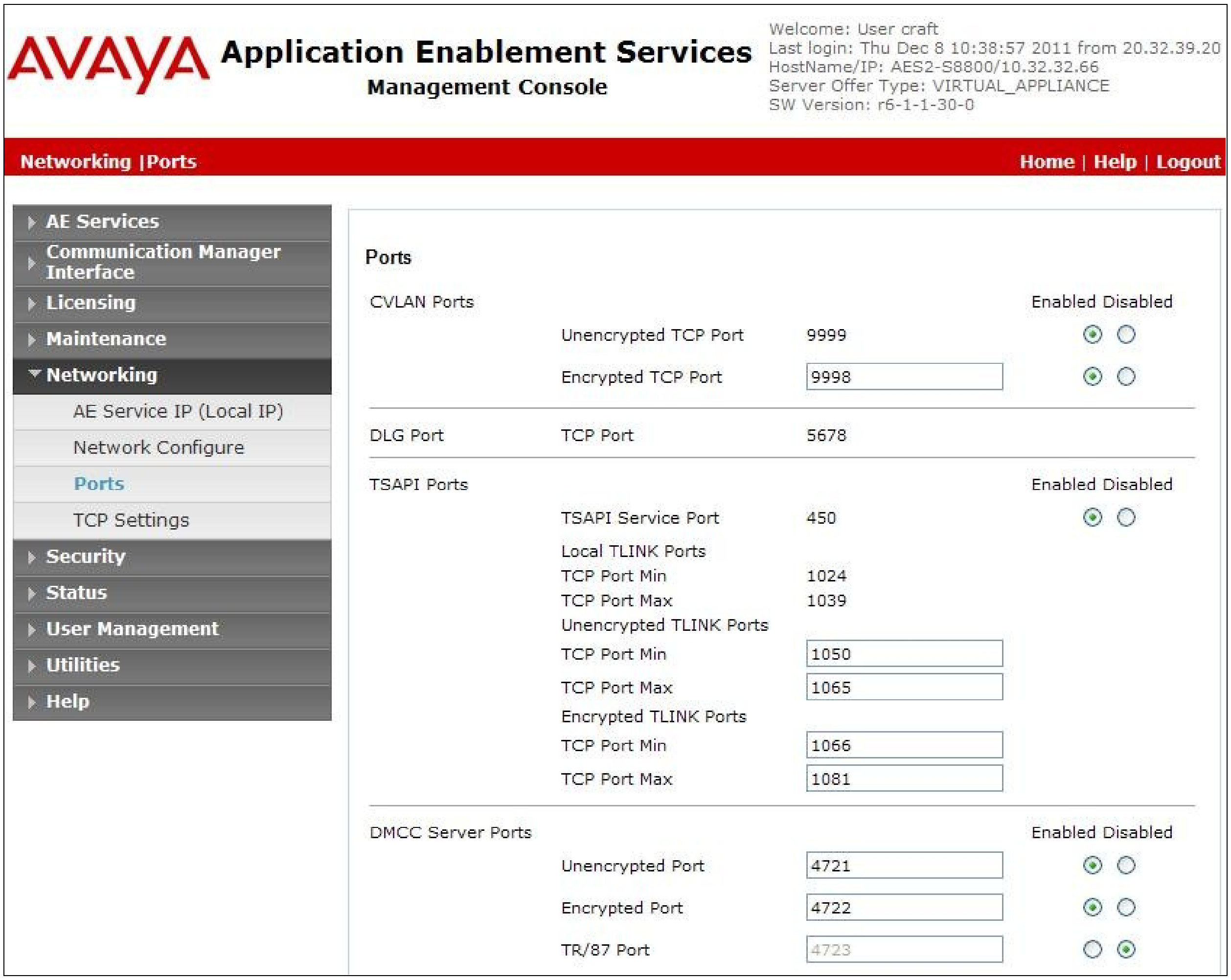
Fields marked with * can not be empty.

* User Id	encore
* Common Name	encore
* Surname	encore
* User Password	•••••••••••
* Confirm Password	•••••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	

6.9. Enable DMCC Unencrypted Port

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.



Welcome: User craft
Last login: Thu Dec 8 10:38:57 2011 from 20.32.39.20
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Ports

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

7. Configure dvsAnalytics Encore

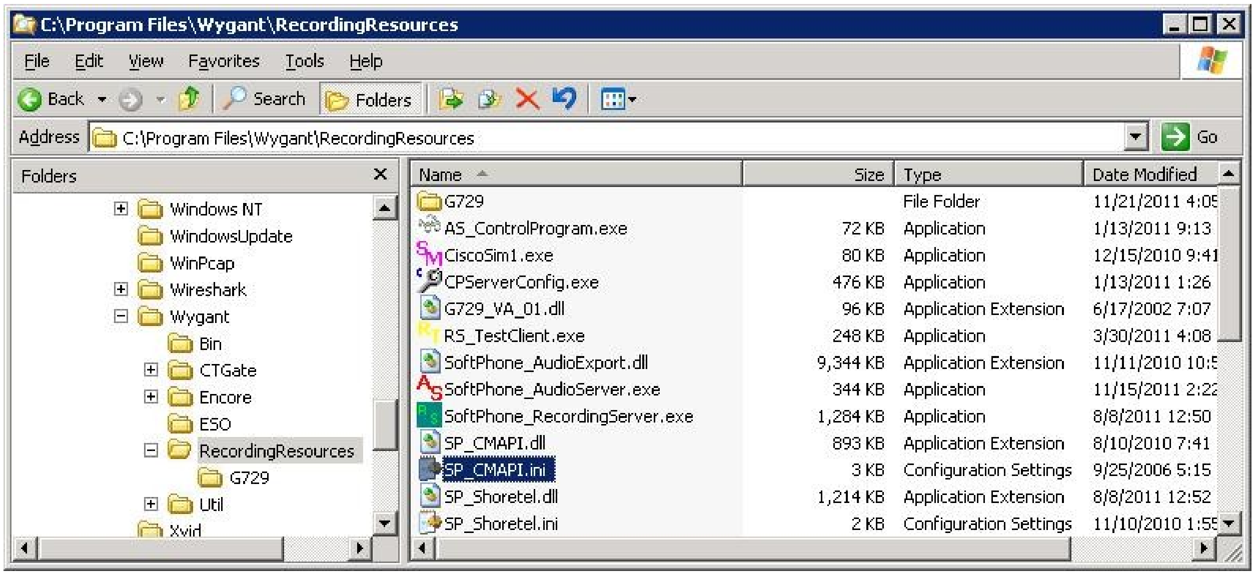
This section provides the procedures for configuring Encore. The procedures include the following areas:

- Administer softphones
- Administer CTISetup
- Administer CT Gateway
- Administer audio server

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

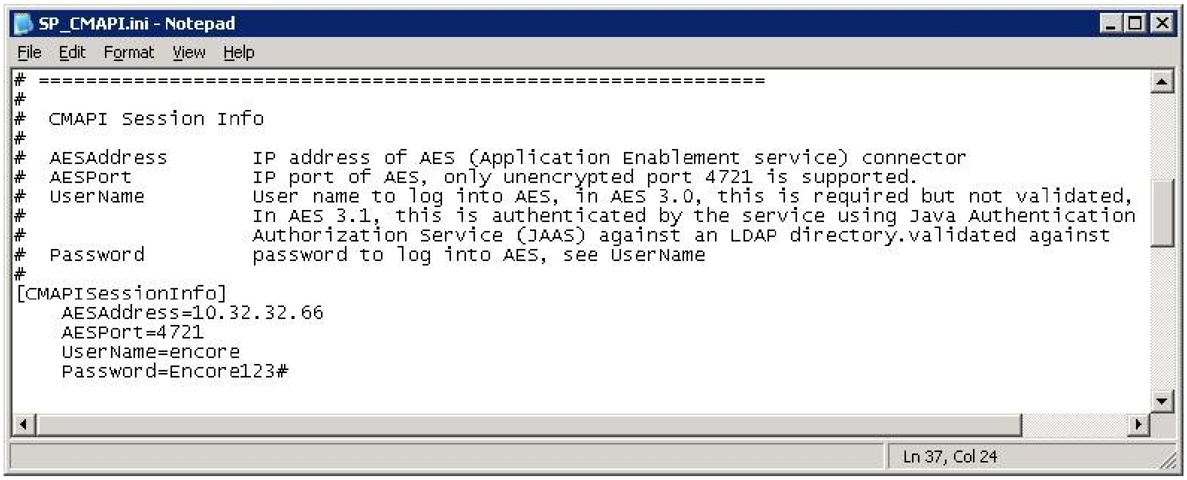
7.1. Administer Softphones

From the Encore server, navigate to the **C:\Program Files\Wygant\RecordingResources** directory to edit the **SP_CMAPI.ini** file shown below.



Name	Size	Type	Date Modified
G729		File Folder	11/21/2011 4:05
AS_ControlProgram.exe	72 KB	Application	1/13/2011 9:13
CiscoSim1.exe	80 KB	Application	12/15/2010 9:41
CPServerConfig.exe	476 KB	Application	1/13/2011 1:26
G729_VA_01.dll	96 KB	Application Extension	6/17/2002 7:07
RS_TestClient.exe	248 KB	Application	3/30/2011 4:08
SoftPhone_AudioExport.dll	9,344 KB	Application Extension	11/11/2010 10:5
SoftPhone_AudioServer.exe	344 KB	Application	11/15/2011 2:22
SoftPhone_RecordingServer.exe	1,284 KB	Application	8/8/2011 12:50
SP_CMAPI.dll	893 KB	Application Extension	8/10/2010 7:41
SP_CMAPI.ini	3 KB	Configuration Settings	9/25/2006 5:15
SP_Shoretel.dll	1,214 KB	Application Extension	8/8/2011 12:52
SP_Shoretel.ini	2 KB	Configuration Settings	11/10/2010 1:55

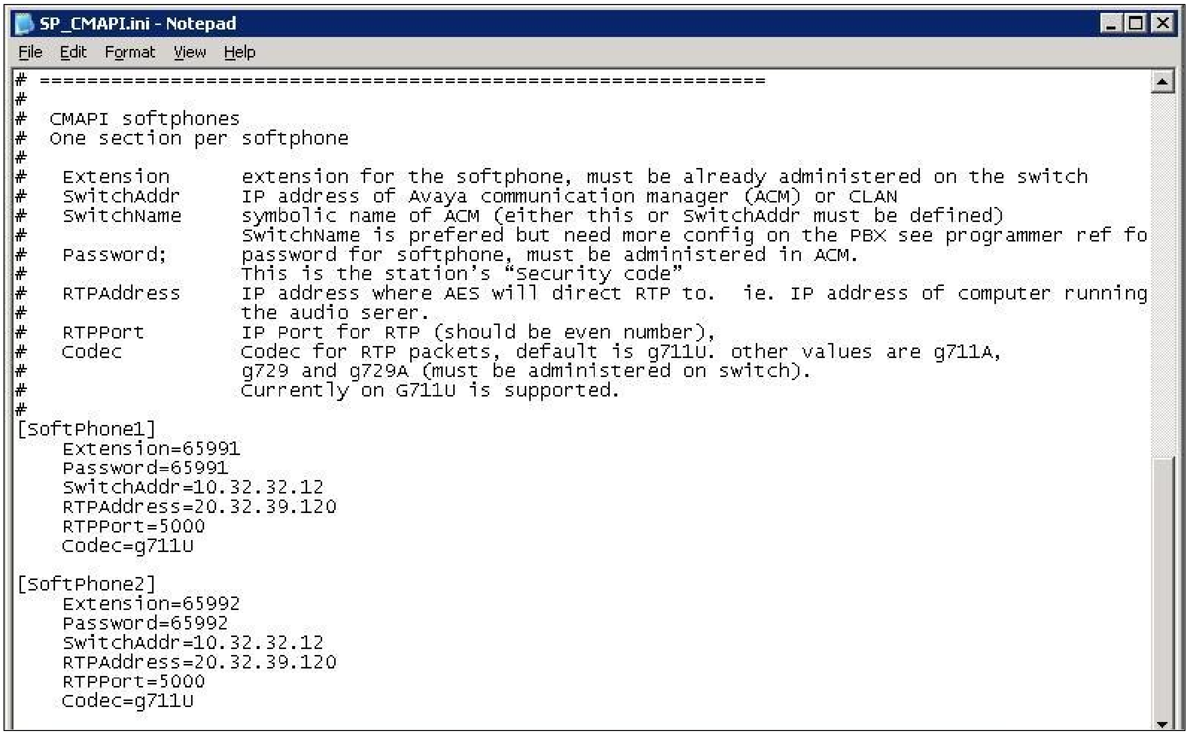
Scroll down to the **CMAPI Session Info** section. Under **CMAPISessionInfo**, set **AESAddress** to the IP address of the Application Enablement Services server. Set **UserName** and **Password** to the Encore user credentials from **Section 6.8**. Retain the default value for **AESPort**.



```
# ============================================================
#
#  CMAPI 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,
#                   In AES 3.1, this is authenticated by the service using Java Authentication
#                   Authorization Service (JAAS) against an LDAP directory.validated against
#  Password         password to log into AES, see UserName
#
[CMAPISessionInfo]
    AESAddress=10.32.32.66
    AESPort=4721
    UserName=encore
    Password=Encore123#
```

Scroll down to the **CMAPI softphones** section. Under **Softphone1**, set **Extension** and **Password** to the first virtual IP softphone extension and security code from **Section 5.6**. 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 in the remaining fields.

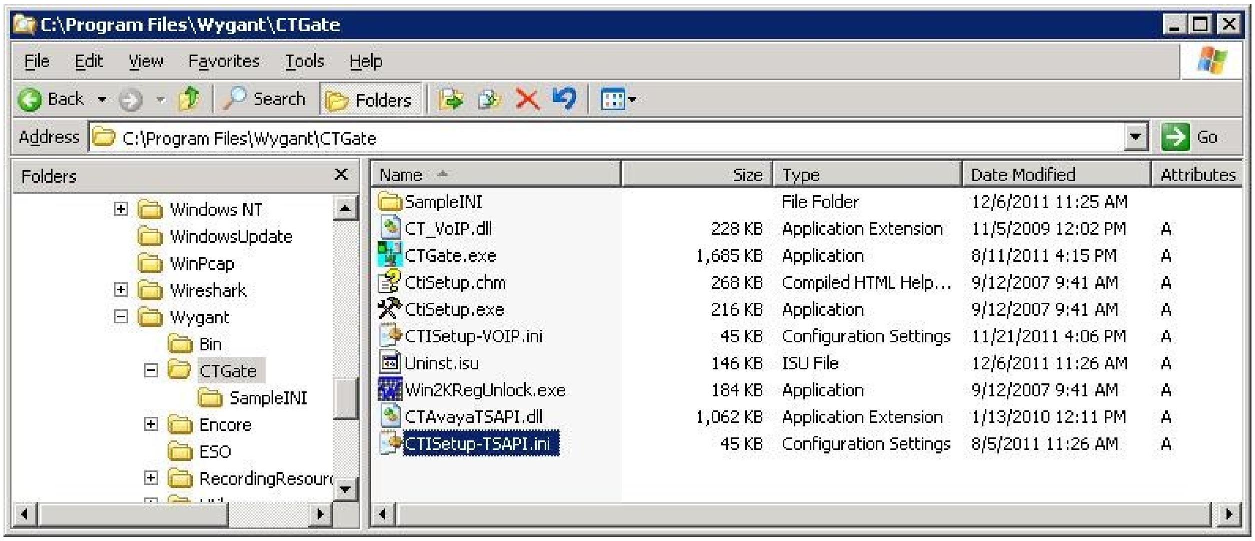
Create additional agent parameter lines as necessary. In the compliance testing, two softphones were configured to correspond to the two virtual IP softphones from **Section 5.6**.



```
# ============================================================
#
#  CMAPI 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 prefered but need more config on the PBX see programmer ref fo
#   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 serer.
#   RTPPort        IP Port for RTP (should be even number),
#   Codec          Codec for RTP packets, default is g711U. other values are g711A,
#                  g729 and g729A (must be administered on switch).
#                  Currently on G711U is supported.
#
[SoftPhone1]
    Extension=65991
    Password=65991
    SwitchAddr=10.32.32.12
    RTPAddress=20.32.39.120
    RTPPort=5000
    Codec=g711U

[SoftPhone2]
    Extension=65992
    Password=65992
    SwitchAddr=10.32.32.12
    RTPAddress=20.32.39.120
    RTPPort=5000
    Codec=g711U
```

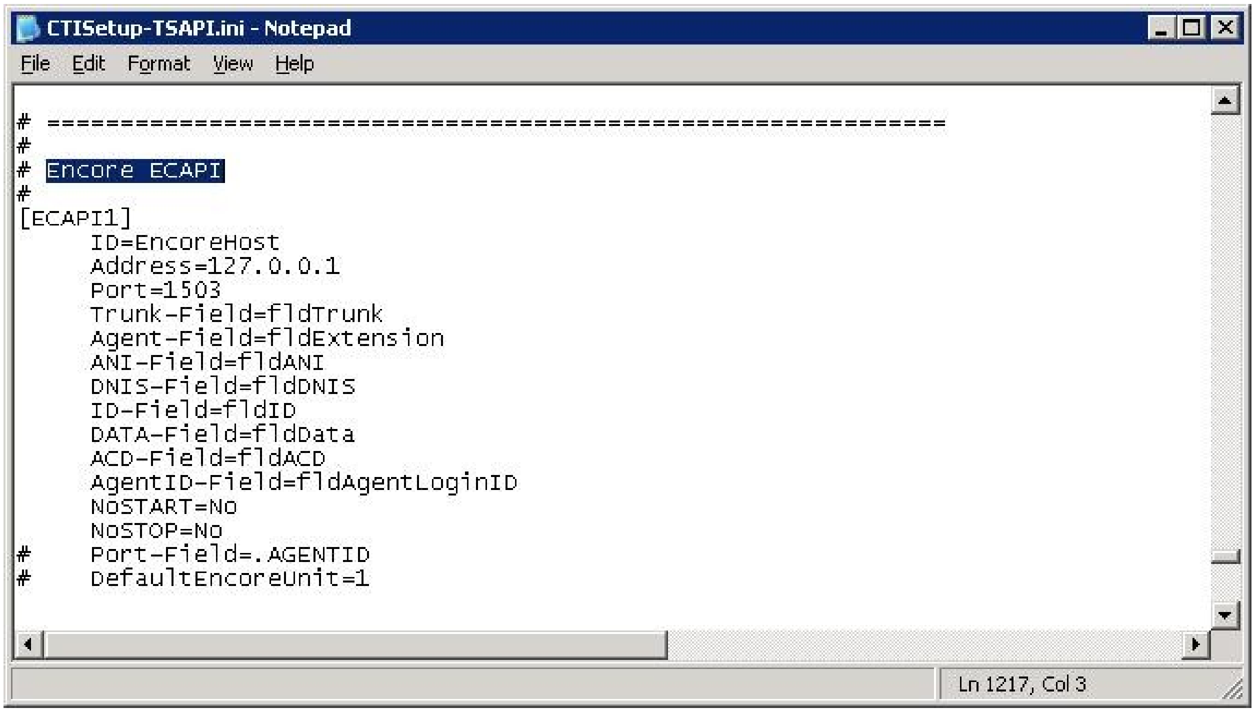
7.2. Administer CTISetup

Navigate to the **C:\Program Files\Wygant\CTGate** directory to edit the **CTISetup-TSAPI.ini** file.



Name	Size	Type	Date Modified	Attributes
SampleINI		File Folder	12/6/2011 11:25 AM	
CT_VoIP.dll	228 KB	Application Extension	11/5/2009 12:02 PM	A
CTGate.exe	1,685 KB	Application	8/11/2011 4:15 PM	A
CtiSetup.chm	268 KB	Compiled HTML Help...	9/12/2007 9:41 AM	A
CtiSetup.exe	216 KB	Application	9/12/2007 9:41 AM	A
CTISetup-VOIP.ini	45 KB	Configuration Settings	11/21/2011 4:06 PM	A
Uninst.isu	146 KB	ISU File	12/6/2011 11:26 AM	A
Win2KRegUnlock.exe	184 KB	Application	9/12/2007 9:41 AM	A
CTAvayaTSAPI.dll	1,062 KB	Application Extension	1/13/2010 12:11 PM	A
CTISetup-TSAPI.ini	45 KB	Configuration Settings	8/5/2011 11:26 AM	A

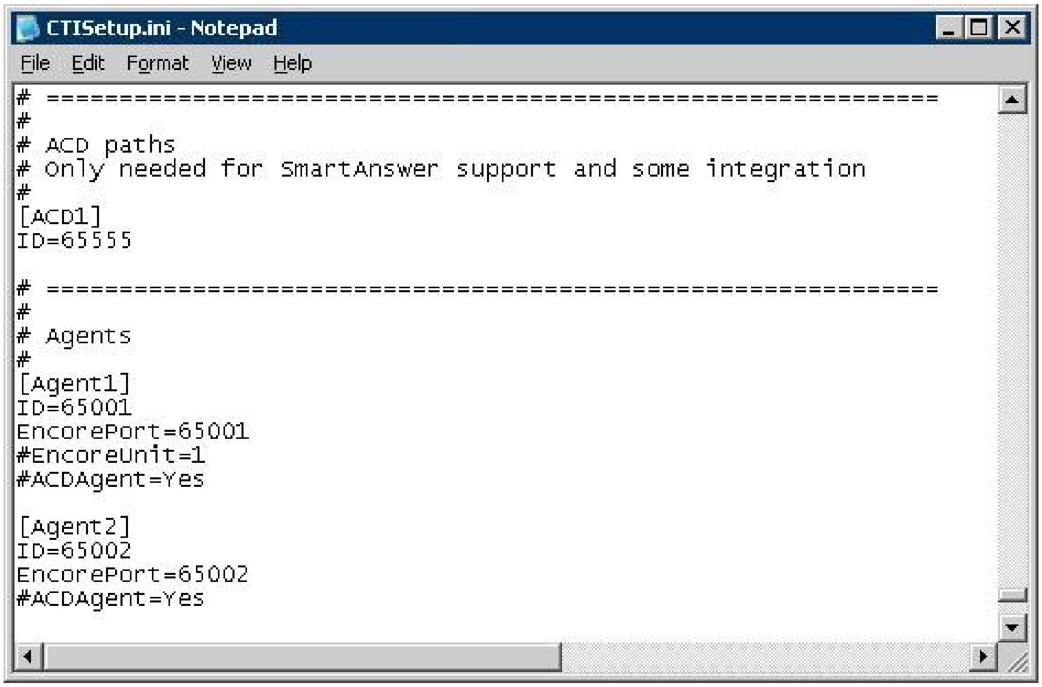
Scroll down to the **Encore ECAPI** section. Under **ECAPI1**, make sure all parameters are set to the default values shown below.



```
# ================================================================
#
# Encore ECAPI
#
[ECAPI1]
     ID=EncoreHost
     Address=127.0.0.1
     Port=1503
     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
#    Port-Field=.AGENTID
#    DefaultEncoreUnit=1
```

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

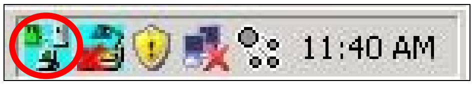
Scroll to the **Agents** section. Under **Agent1**, set **ID** and **EncorePort** to the first agent station extension from **Section 3**. Create additional agent parameter lines as necessary when more than one agent is being monitored.



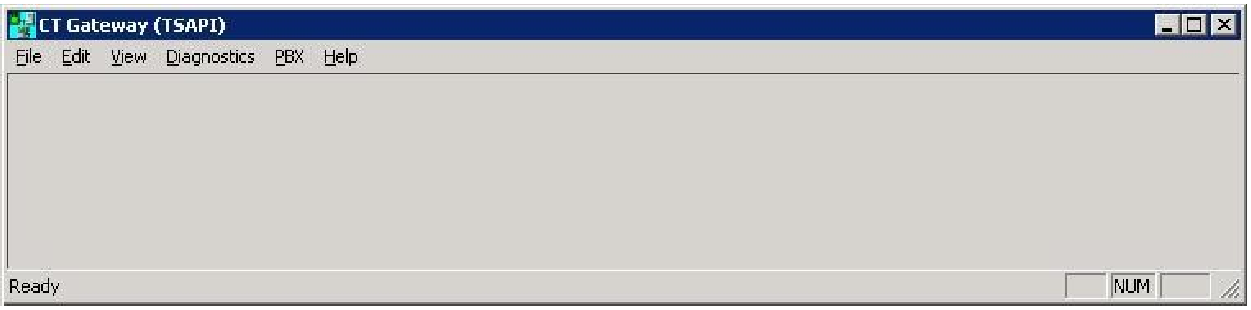
```
# ===============================================================
#
# ACD paths
# Only needed for SmartAnswer support and some integration
#
[ACD1]
ID=65555

# ===============================================================
#
# Agents
#
[Agent1]
ID=65001
EncorePort=65001
#EncoreUnit=1
#ACDAgent=Yes

[Agent2]
ID=65002
EncorePort=65002
#ACDAgent=Yes
```

7.3. Administer CT Gateway

Click on the **CT Gateway** icon from the system tray, as shown below.

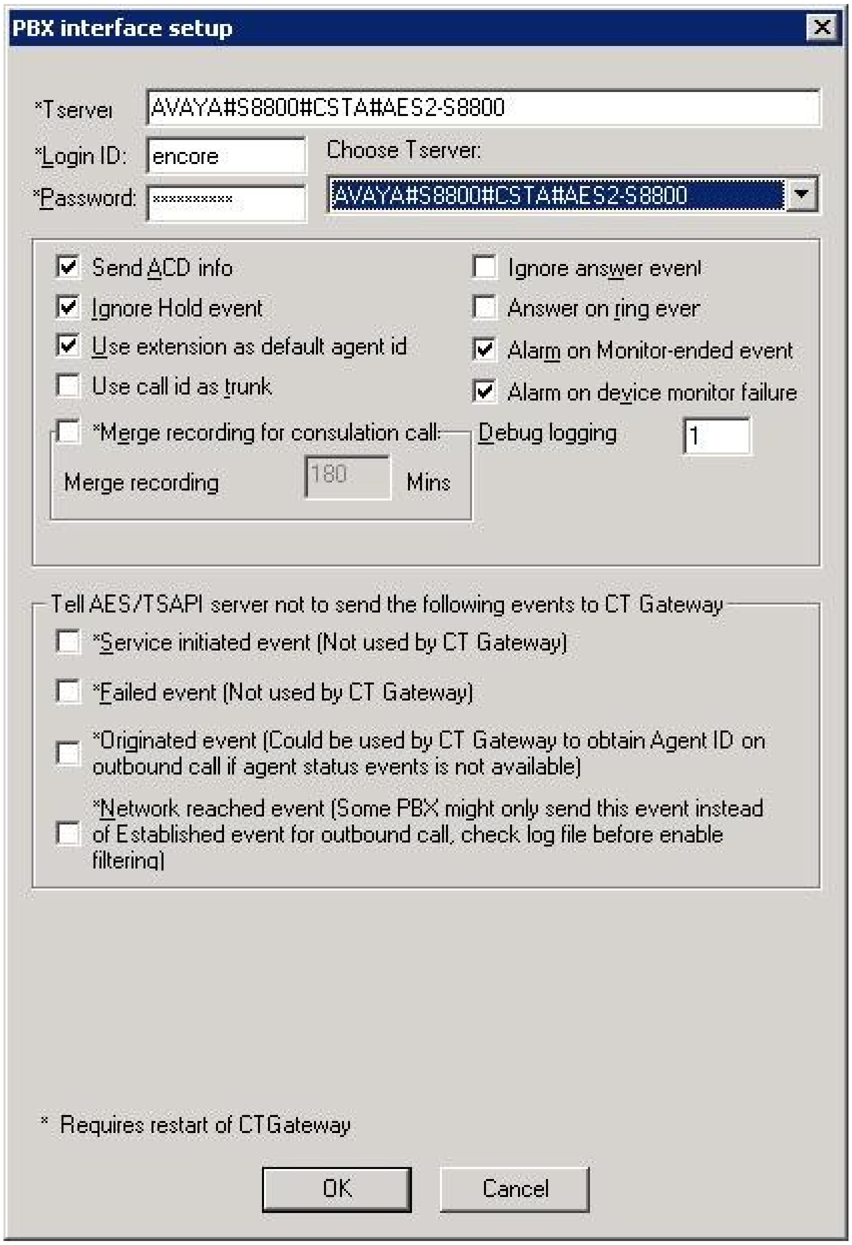


The **CT Gateway (TSAPI)** screen is displayed. Select **PBX > Configure** from the top menu.



The **PBX interface setup** screen is displayed. In **Choose Tserver**, select the Tlink name from **Section 6.7** and the **Tserver** field will be populated automatically. For **Login ID** and **Password**, enter the Encore user credentials from **Section 6.8**.

Make certain that the **Merge recording for consultation call** field is unchecked, and set the remaining fields as desired. The setting used in the compliance testing is shown in the screen shot below.



PBX interface setup

*Tserver: AVAYA#S8800#CSTA#AES2-S8800

*Login ID: encore

*Password: ***********

Choose Tserver: AVAYA#S8800#CSTA#AES2-S8800

☑ Send ACD info

☑ Ignore Hold event

☑ Use extension as default agent id

□ Use call id as trunk

□ *Merge recording for consulation call:

Merge recording 180 Mins

□ Ignore answer event

□ Answer on ring ever

☑ Alarm on Monitor-ended event

☑ Alarm on device monitor failure

Debug logging 1

Tell AES/TSAPI server not to send the following events to CT Gateway

□ *Service initiated event (Not used by CT Gateway)

□ *Failed event (Not used by CT Gateway)

□ *Originated event (Could be used by CT Gateway to obtain Agent ID on outbound call if agent status events is not available)

□ *Network reached event (Some PBX might only send this event instead of Established event for outbound call, check log file before enable filtering)

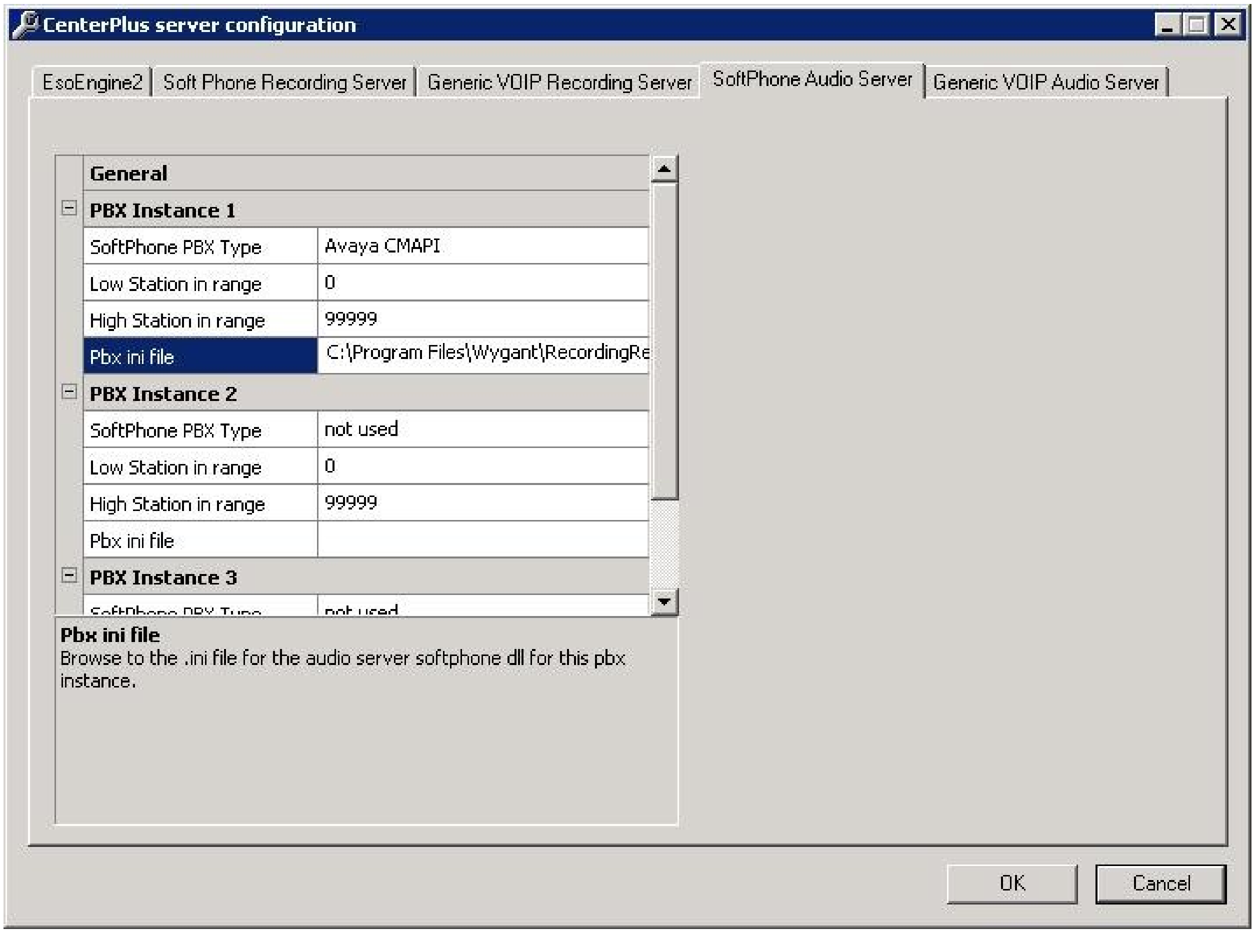
* Requires restart of CTGateway

7.4. Administer Audio Server

From the Encore server, double-click on the **CenterPlus Server Configuration** icon shown below, which is created as part of installation.

The **CenterPlus server configuration** screen is displayed. Select the **SoftPhone Audio Server** tab.

Under **PBX Instance 1**, select "Avaya CMAPI" from the drop-down list for **SoftPhone PBX Type**. Select **Pbx ini file**, and open the **C:\Program Files\Wygant\RecordingResources\ SP_CMAPI.ini** file in the pop-up window (not shown).


CenterPlus server configuration
EsoEngine2
Soft Phone Recording Server
Generic VOIP Recording Server
SoftPhone Audio Server
Generic VOIP Audio Server
OK
Cancel

General	
PBX Instance 1	
SoftPhone PBX Type	Avaya CMAPI
Low Station in range	0
High Station in range	99999
Pbx ini file	C:\Program Files\Wygant\RecordingRe
PBX Instance 2	
SoftPhone PBX Type	not used
Low Station in range	0
High Station in range	99999
Pbx ini file	
PBX Instance 3	
SoftPhone PBX Type	not used

Pbx ini file
Browse to the .ini file for the audio server softphone dll for this pbx instance.

8. Verification Steps

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

8.1. 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 **Service State** is "established" for the CTI link number administered in **Section 5.3**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

1     4        no    AES2-S8800       established   15       15
```

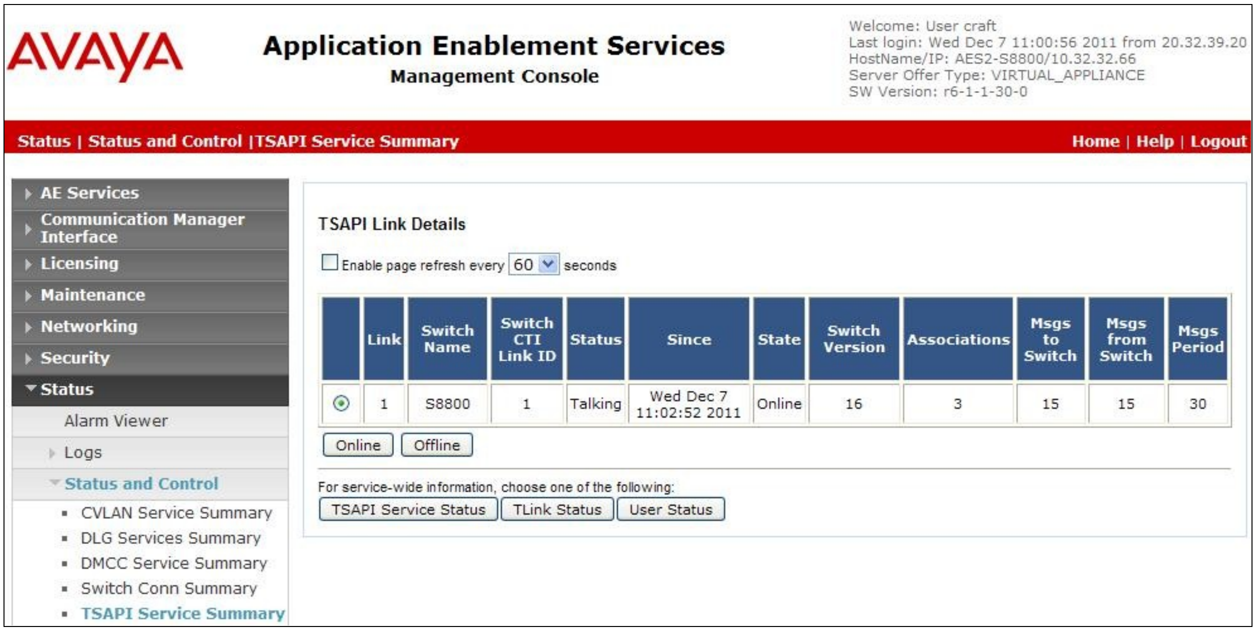
Verify registration status of the virtual softphones by using the "list registered-ip-stations" command. Verify that all extensions from **Section 5.6** are displayed, as shown below.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- -------------------------------------
65000         9650      IP_Phone    y  20.32.39.114
              1         3.1000         10.32.32.12
65001         1616      IP_Phone    y  20.32.39.113
              1         1.3000         10.32.32.12
65002         1608      IP_Phone    y  20.32.39.105
              1         1.3000         10.32.32.12
65991         4610      IP_API_A    y  10.32.32.66
              1         3.2040         10.32.32.12
65992         4610      IP_API_A    y  10.32.32.66
              1         3.2040         10.32.32.12
```

8.2. 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 that **Status** is "Talking", and that **Associations** reflect the total number of skill groups and agent station extensions from **Section 7.2**.



Welcome: User craft
Last login: Wed Dec 7 11:00:56 2011 from 20.32.39.20
HostName/IP: AES2-S8800/10.32.32.66
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

TSAPI Link Details

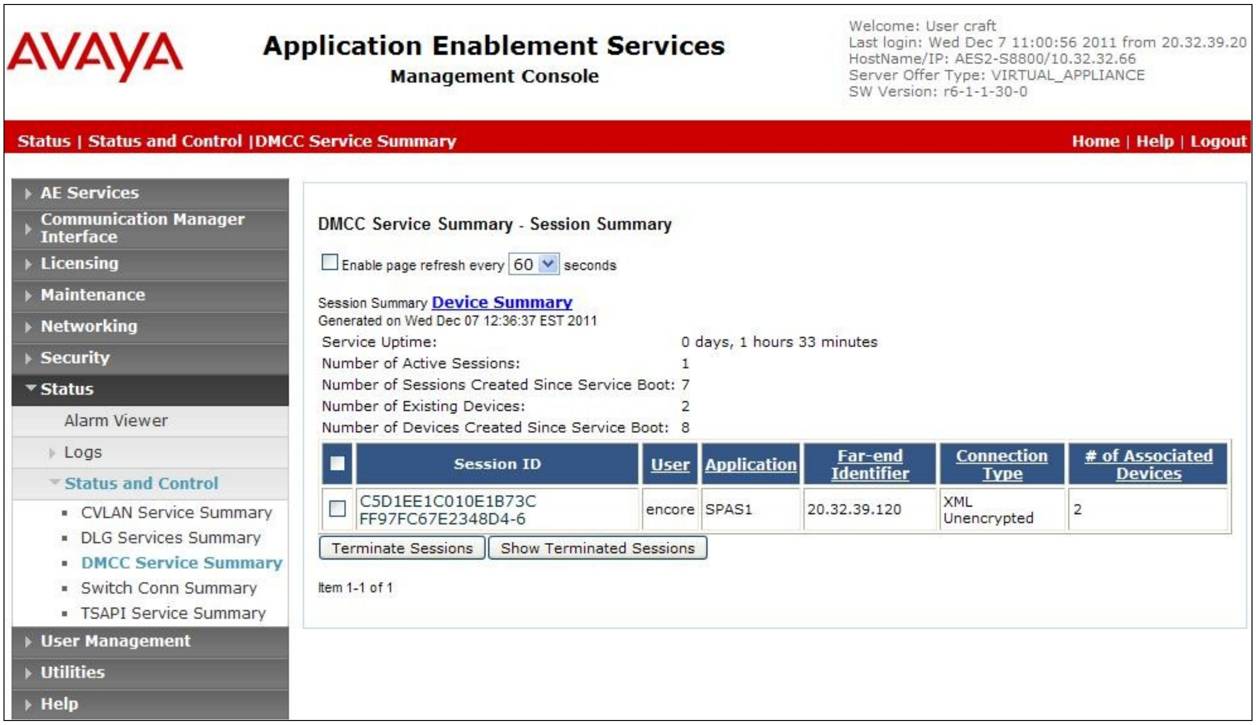
□ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	S8800	1	Talking	Wed Dec 7 11:02:52 2011	Online	16	3	15	15	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.

In the lower portion of the screen, verify that there is an active session with the Encore user name from **Section 6.8**, and that **# of Associated Devices** reflects the number of softphones from **Section 7.1**.



DMCC Service Summary - Session Summary

□ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Wed Dec 07 12:36:37 EST 2011

Service Uptime:	0 days, 1 hours 33 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	7
Number of Existing Devices:	2
Number of Devices Created Since Service Boot:	8

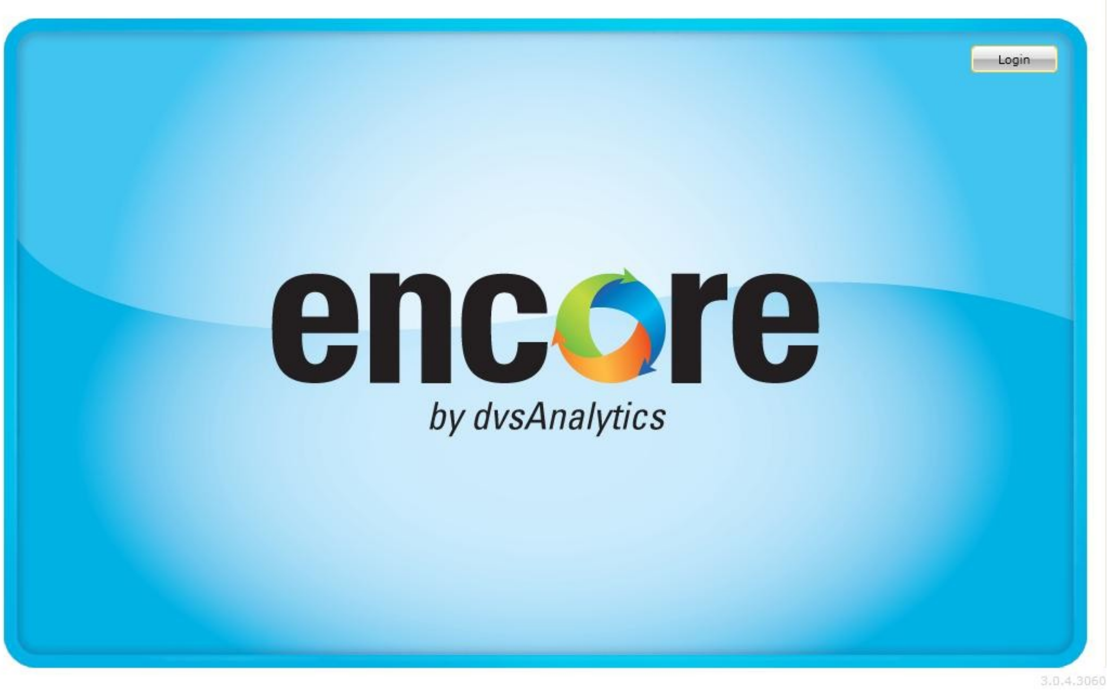
■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	C5D1EE1C010E1B73C FF97FC67E2348D4-6	encore	SPAS1	20.32.39.120	XML Unencrypted	2

Terminate Sessions | Show Terminated Sessions

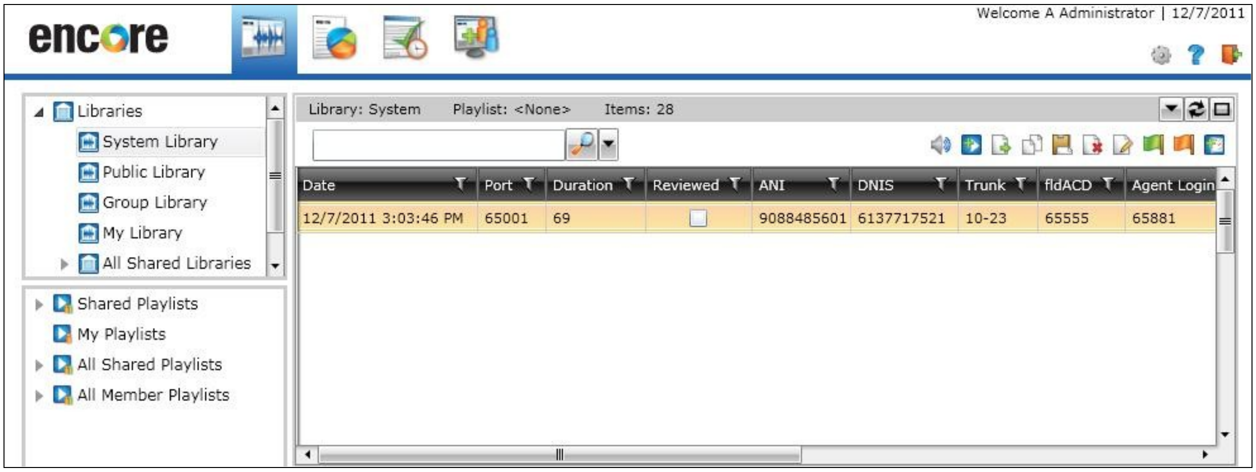
Item 1-1 of 1

8.3. Verify dvsAnalytics Encore

Log an agent in to 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 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.



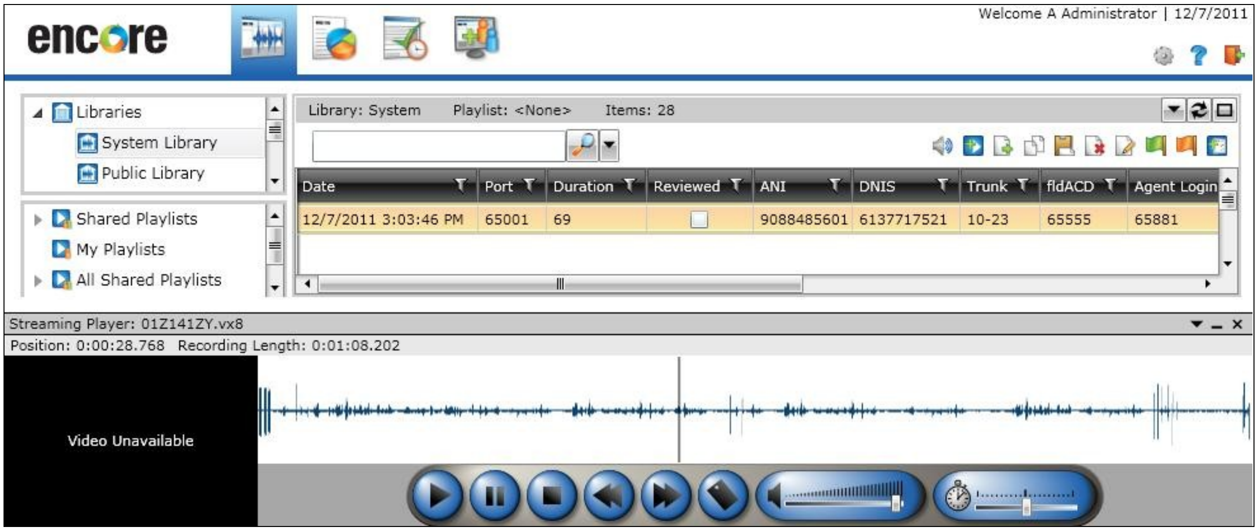
The **encore** screen is updated with a list of call recordings. Verify that there is an entry in the right pane reflecting the last call, with proper values in the relevant fields.



Library: System Playlist: <None> Items: 28

Date	Port	Duration	Reviewed	ANI	DNIS	Trunk	fldACD	Agent Login
12/7/2011 3:03:46 PM	65001	69	□	9088485601	6137717521	10-23	65555	65881

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.



Library: System Playlist: <None> Items: 28

Date	Port	Duration	Reviewed	ANI	DNIS	Trunk	fldACD	Agent Login
12/7/2011 3:03:46 PM	65001	69	□	9088485601	6137717521	10-23	65555	65881

Streaming Player: 01Z141ZY.vx8

Position: 0:00:28.768 Recording Length: 0:01:08.202

9. Conclusion

These Application Notes describe the configuration steps required for dvsAnaltyics Encore 2.3.1 to successfully interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura^{TM} Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at http://support.avaya.com.

2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.1, Issue 2, February 2011, available at http://support.avaya.com.

3. *Encore Administrator's Guide*, Release 2.3.1, September 20, 2011, available from dvsAnalytics Support.

4. *Avaya using TSAPI Switch Integration Guide*, Release 2.2.7, July 21, 2010, available from dvsAnalytics Support.

5. *Avaya DMCC Switch Integration Guide*, Release 2.2.7, July 22, 2010, available from dvsAnalytics Support.

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.