Application Notes for dvsAnalytics Encore with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Service Observing – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for dvsAnalytics Encore to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 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 the 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 to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Service Observing. dvsAnalytics Encore is a call recording solution.

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

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

When there is an active call at the monitored agent, dvsAnalytics Encore is informed of the call via event reports from the TSAPI interface. dvsAnalytics Encore starts the call recording by using the Service Observing feature from the DMCC interface to add a virtual IP softphone to the active call to obtain the media. The event reports are also used to determine when to stop the call 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 requests monitoring on skill groups and agent stations, performs device queries using TSAPI, and registers the virtual IP softphones using DMCC.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for the recordings. Necessary user actions such as hold and 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 connection to Encore.

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

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member’s solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Encore:

- Handling of TSAPI messages in areas of event notification and value queries.

- Use of DMCC registration services to register and un-register virtual IP softphones.

- Use of DMCC physical devices services and monitoring services to activate Service Observing for the virtual IP softphones and to obtain the media for call recording.

- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, multiple calls, multiple agents, conference, and transfer.

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

2.2. Test Results

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

- For the conference scenarios, the recording entry for the conference-from agent can contain multiple Service Observing confirmation tones, due to different softphones added for different portions of the conference call.

- The Consultation Call parameter associated with the recording entries applied to the attended transfer and conference scenarios.

- The number of softphones to configure need to take into account the small interval of 500ms that a softphone will not be available between recordings.

2.3. Support

Technical support on Encore can be obtained through the following:

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

3. Reference Configuration

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

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

Device Type	Extension
VDN	53050
Skill Group	53090
Supervisor	53040
Agent Station	53010, 53012
Agent ID	1000, 1001

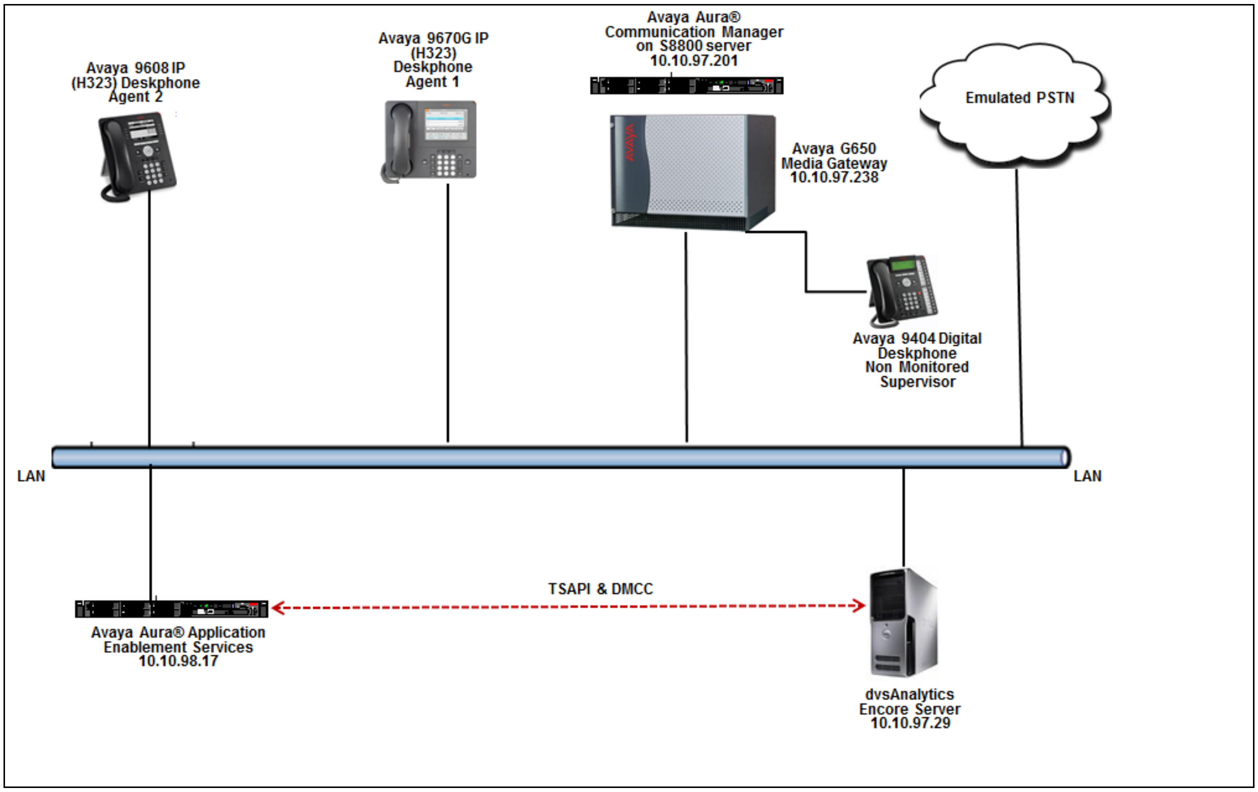

Avaya 9608 IP (H323) Deskphone Agent 2
Avaya 9670G IP (H323) Deskphone Agent 1
Avaya Aura® Communication Manager on S8800 server 10.10.97.201
Emulated PSTN
Avaya G650 Media Gateway 10.10.97.238
Avaya 9404 Digital Deskphone Non Monitored Supervisor
LAN
LAN
TSAPI & DMCC
Avaya Aura® Application Enablement Services 10.10.98.17
dvsAnalytics Encore Server 10.10.97.29

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 on Avaya S8800 Server with Avaya G650Media Gateway	6.3-03.0.124.0 (R016x.03.0.124.0-21588)
Avaya Aura® Application Enablement Services	6.3.3.1.10-0
Avaya 9670 IP Deskphone (H.323)	3.220A
Avaya 9608 IP Deskphone (H.323)	6.4014
Avaya 9404 Digital Deskphone	12
dvsAnalytics Encore on Windows Server 2008 R2 Standard • Encore Web Interface • Avaya TSAPI Windows Client (csta32.dll) • Avaya DMCC XML	6.0.1 SP1 3.0.9.6960 6.1.1.469 6.1

5. Configure Avaya Aura® Communication Manager

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

- Verify License
- Administer CTI Link
- Administer IP Codec Set
- Administer System Parameters Features
- Administer Class Of Restriction
- Administer Agent Stations
- Administer Virtual IP Softphones

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 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)? 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? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                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 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
                    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: 50001
     Type: ADJ-IP
                                                                            COR: 1
     Name: AES63
```

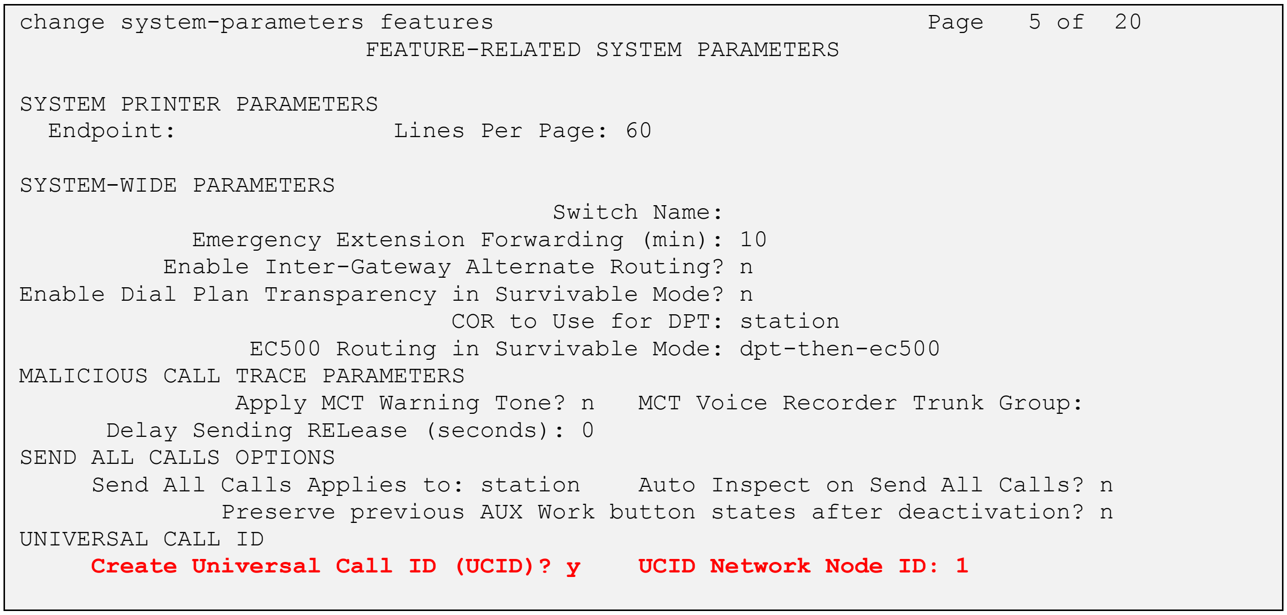
5.3. Administer IP Codec Set

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

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

                          IP Codec Set

    Codec Set: 1

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

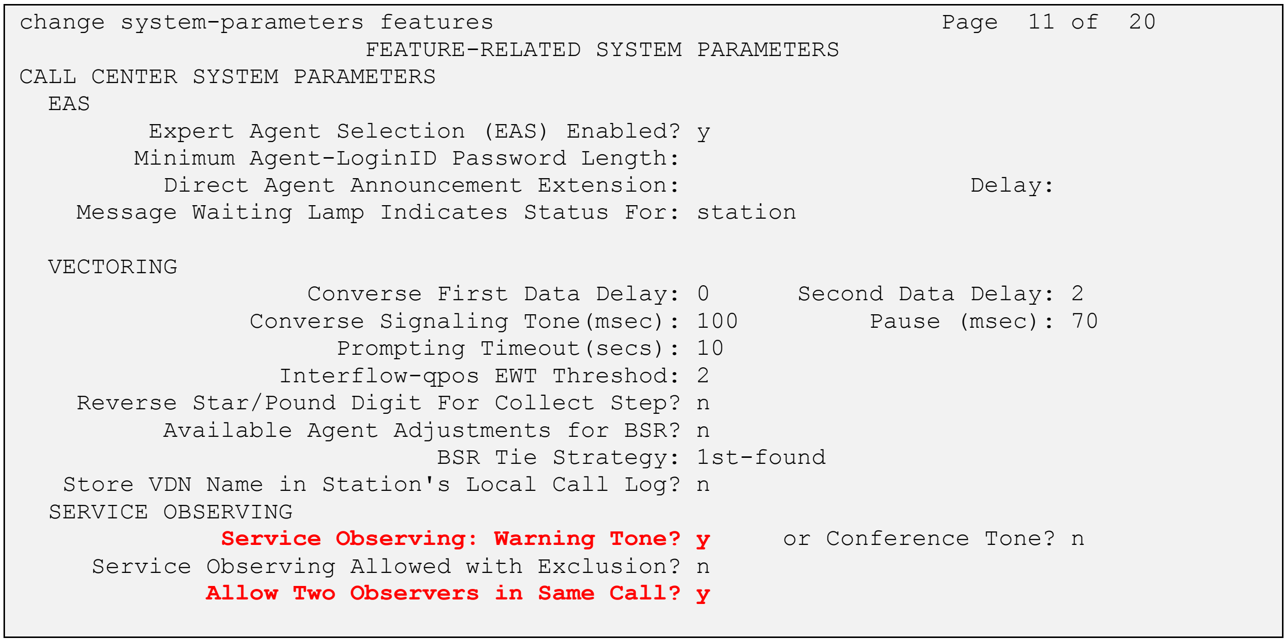
5.4. Administer System Parameters Features

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.



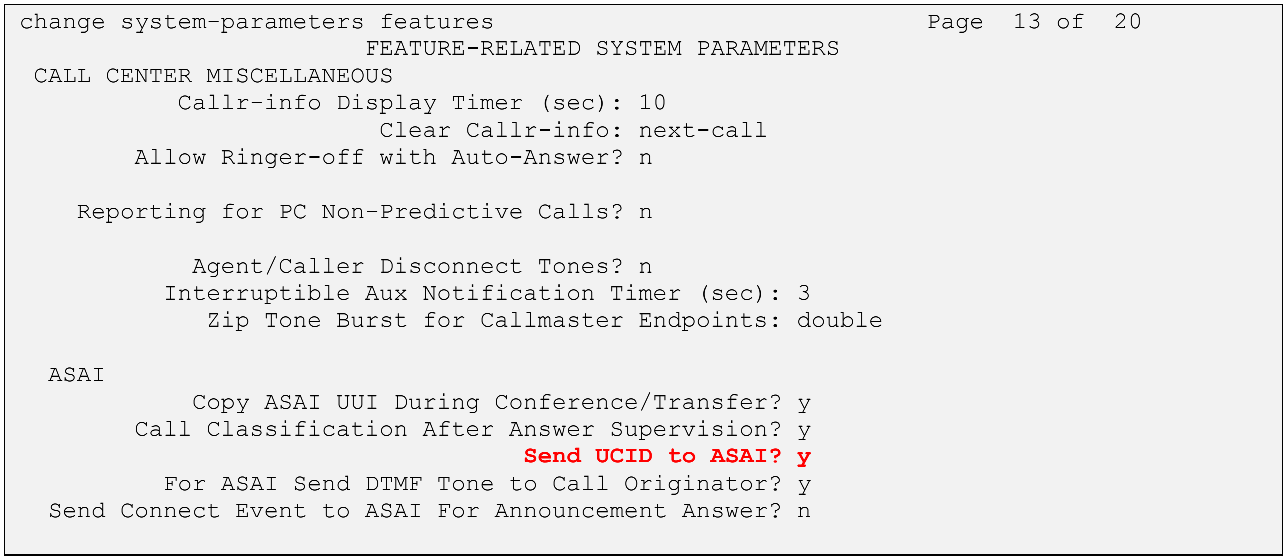
```
change system-parameters features                              Page    5 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS

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: 1
```

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



```
change system-parameters features                               Page  11 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:                      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? y     or Conference Tone? n
     Service Observing Allowed with Exclusion? n
             Allow Two Observers in Same Call? y
```

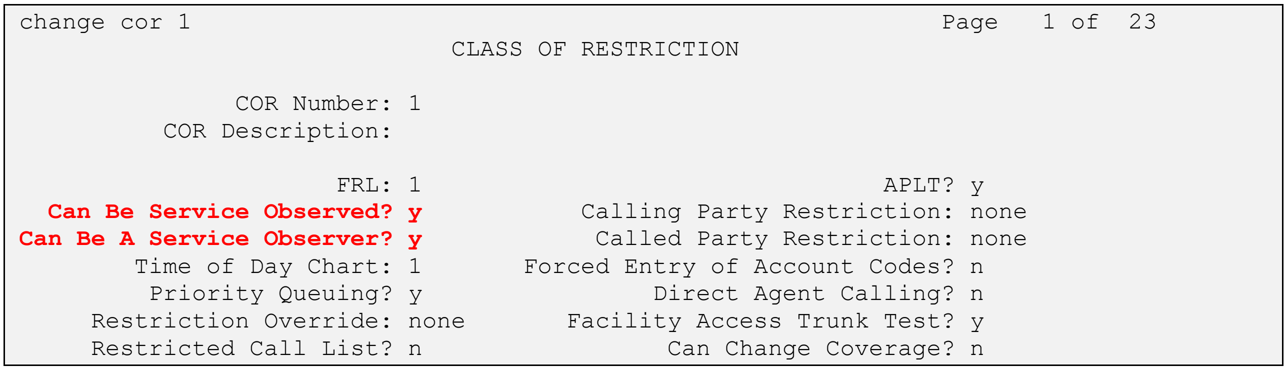
Navigate to **Page 13**, and enable **Send UCID to ASAI**. This parameter allows for the universal call ID to be sent to Encore.



```
change system-parameters features                              Page  13 of  20
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
           Callr-info Display Timer (sec): 10
                         Clear Callr-info: next-call
        Allow Ringer-off with Auto-Answer? n

    Reporting for PC Non-Predictive Calls? n

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

  ASAI
            Copy ASAI UUI During Conference/Transfer? y
        Call Classification After Answer Supervision? y
                                   Send UCID to ASAI? y
          For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
```

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.



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

               COR Number: 1
          COR Description:

                      FRL: 1                                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? y                Direct Agent Calling? n
     Restriction Override: none       Facility Access Trunk Test? y
     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**.

```
change station 53010                                           Page   1 of   5
                                     STATION

Extension: 53010                         Lock Messages? n               BCC: 0
     Type: 9608                          Security Code: *                TN: 1
     Port: S00004                      Coverage Path 1:                 COR: 1
     Name: H.323 53010                 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: 53010
            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
```

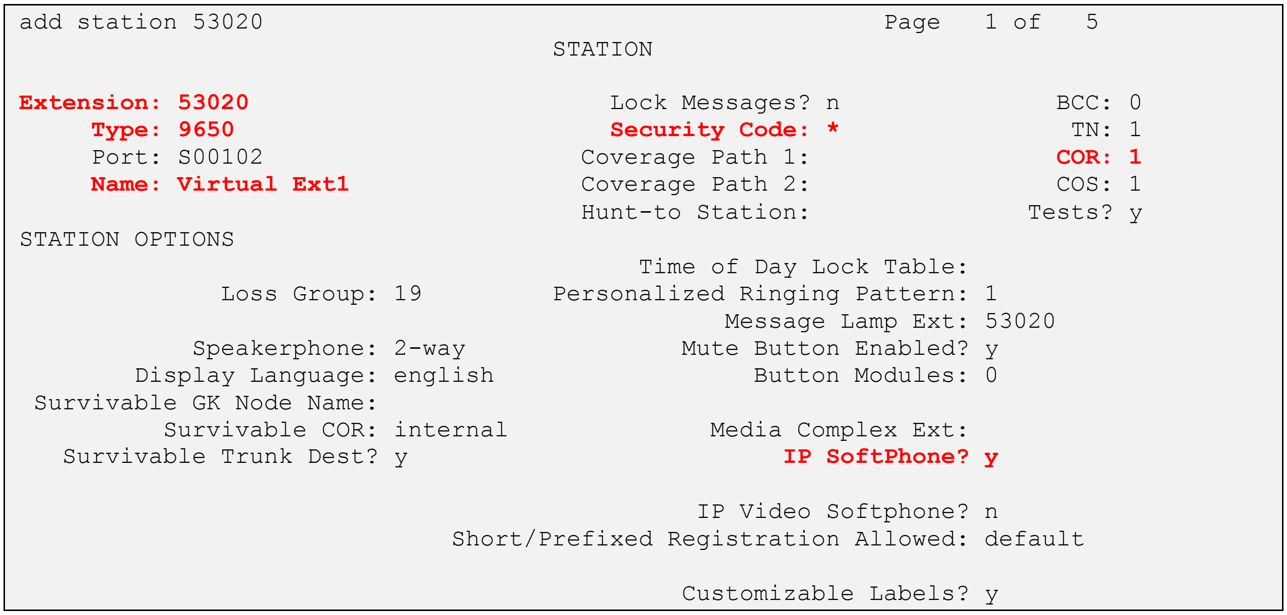
Repeat this section to administer all agent stations from **Section 3**. In the compliance testing, two agent stations were administered as shown below.

```
list station 53010 count 3

                                  STATIONS

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

53010         S00004  H.323 53010                                    1
               9608                        no                         1
53012         S00119  H.323, 53012                                   1
               9670                        no                         1
```

5.7. Administer Virtual IP Softphones

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

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as “9650 or 4620”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **COR:** The COR number from **Section 5.5**.
- **IP SoftPhone:** “y”



```
add station 53020                                           Page   1 of   5
                                     STATION

Extension: 53020                         Lock Messages? n                BCC: 0
     Type: 9650                          Security Code: *                 TN: 1
     Port: S00102                      Coverage Path 1:                 COR: 1
     Name: Virtual Ext1                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: 53020
            Speakerphone: 2-way                 Mute Button Enabled? y
        Display Language: english                    Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                            IP SoftPhone? y

                                               IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default

                                              Customizable Labels? y
```

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

```
add station 53020                                           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
 2: call-appr
 3: serv-obsrv
```

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 53020 count 4

                                  STATIONS

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

53020         S00102  Virtual Ext1                                      1
               9650                        no                            1
53021         S00105  Virtual Ext2                                      1
               4620                        no                            1
53022         S00108  Virtual Ext3                                      1
               4620                        no                            1
53023         S00111  Virtual Ext4                                      1
               4620                        no                            1
```

6. Configure Avaya Aura® Application Enablement Services

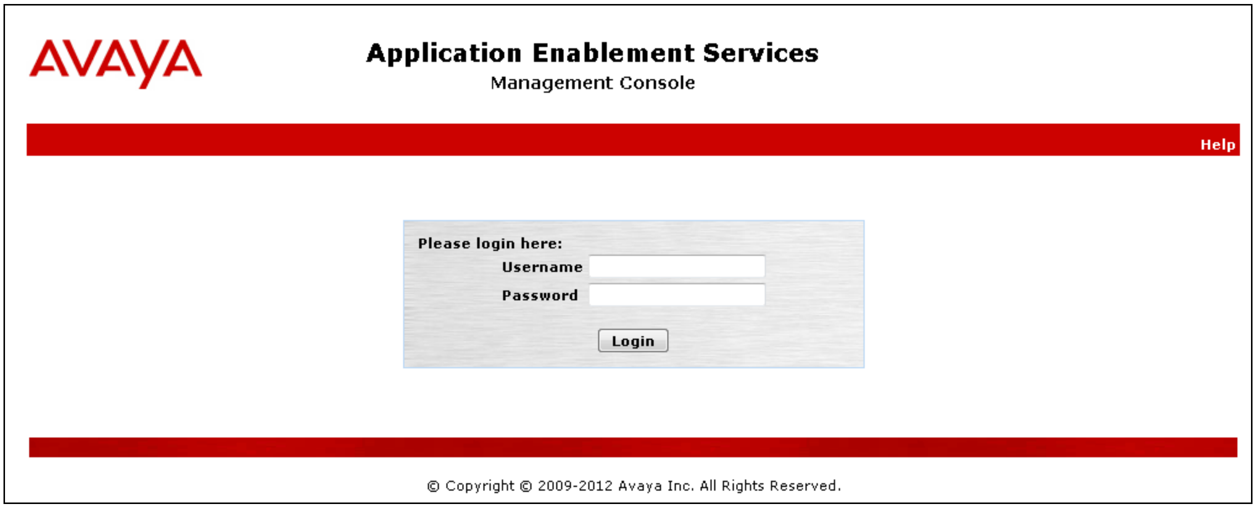
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM Interface
- Verify License
- Administer TSAPI Link
- Administer H.323 Gatekeeper
- Disable Security Database
- Restart Services
- Obtain Tlink Name
- Administer Encore User
- Enable Ports

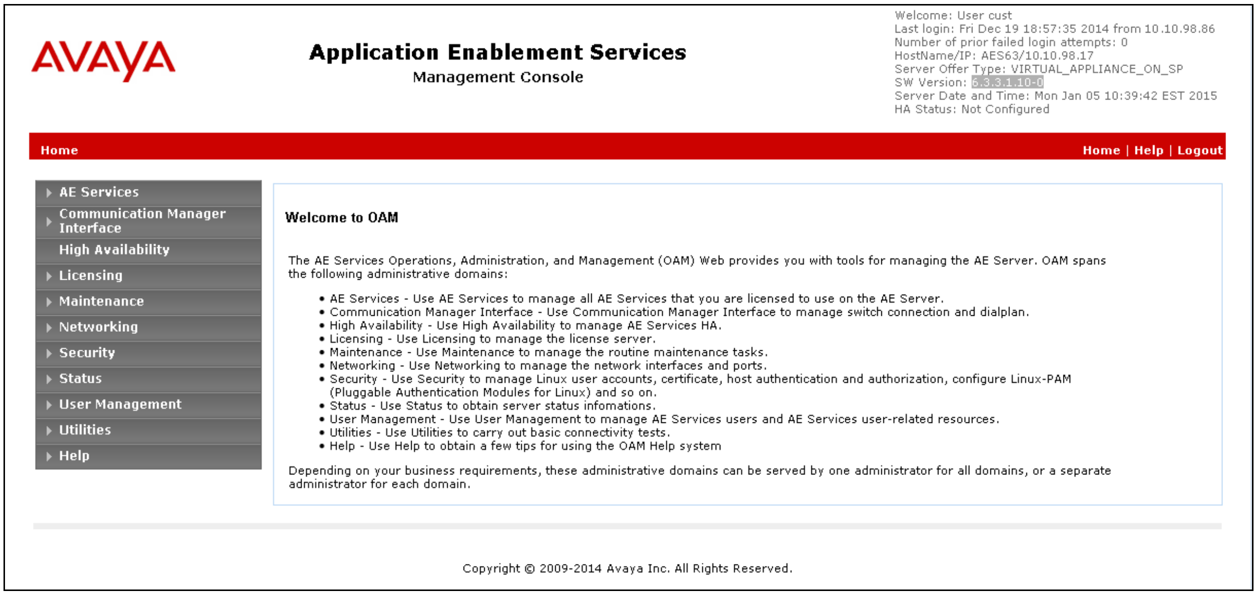
6.1. Launch OAM Interface

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
Help
Please login here:
Username
Password
Login
© Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

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



Welcome: User cust
Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 10:39:42 EST 2015
HA Status: Not Configured

Welcome to OAM

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

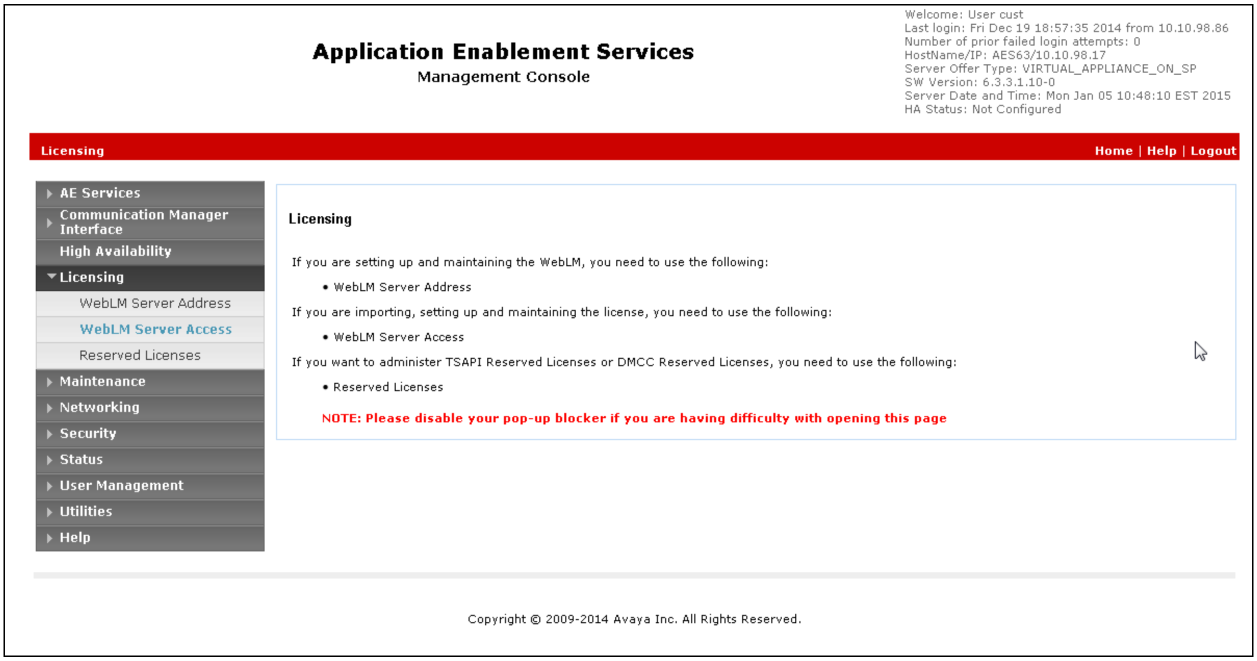
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing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

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

Copyright © 2009-2014 Avaya Inc. All Rights Reserved.

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 using the appropriate credentials.



Welcome: User cust
Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 10:48:10 EST 2015
HA Status: Not Configured

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:

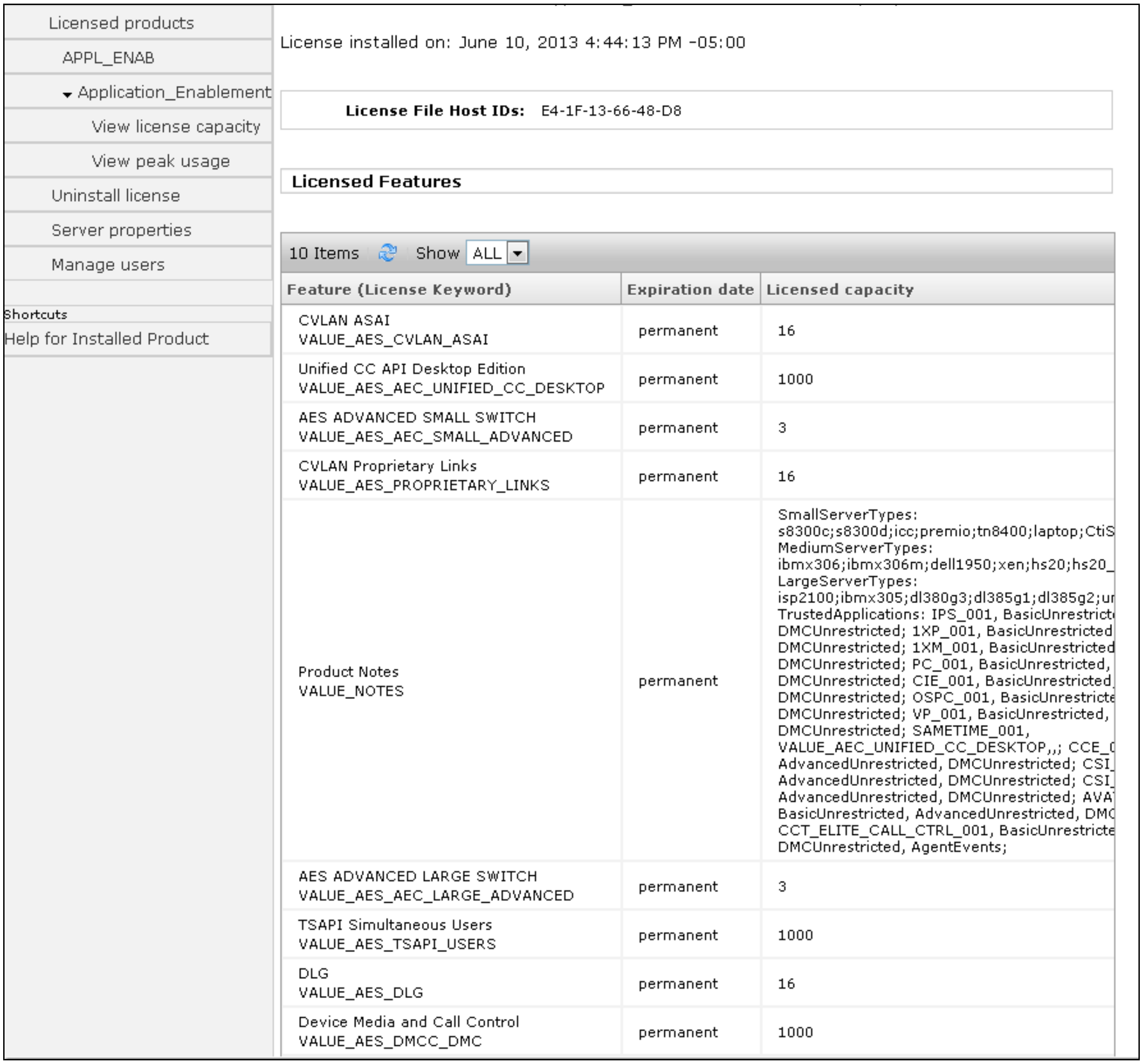
- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

Copyright © 2009-2014 Avaya Inc. All Rights Reserved.

The **Web License Manager** screen below is displayed. 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.



License installed on: June 10, 2013 4:44:13 PM -05:00

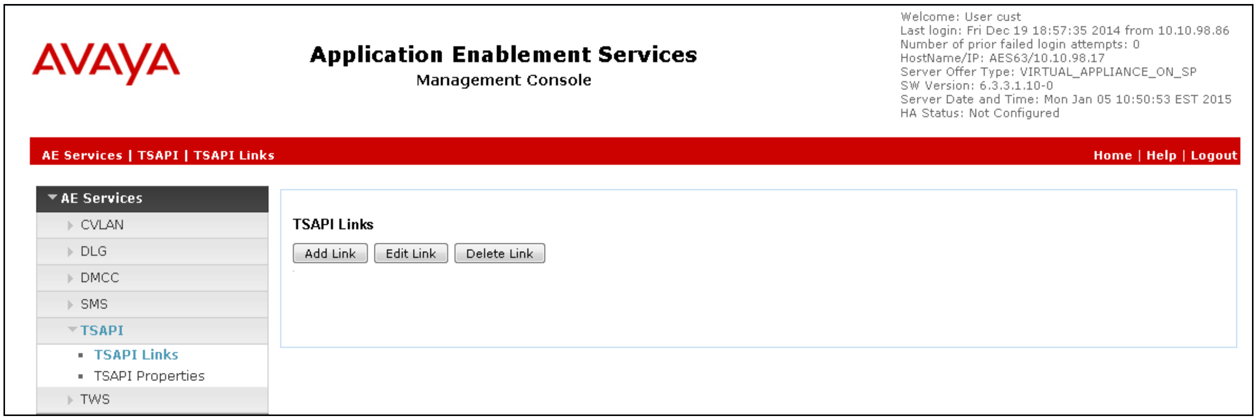
License File Host IDs: E4-1F-13-66-48-D8

Licensed Features

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;ur TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted DMCUnrestricted; OSPC_001, BasicUnrestricte DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,; CCE_ AdvancedUnrestricted, DMCUnrestricted; CSI_ AdvancedUnrestricted, DMCUnrestricted; CSI_ AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DMC CCT_ELITE_CALL_CTRL_001, BasicUnrestricte DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000

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**.

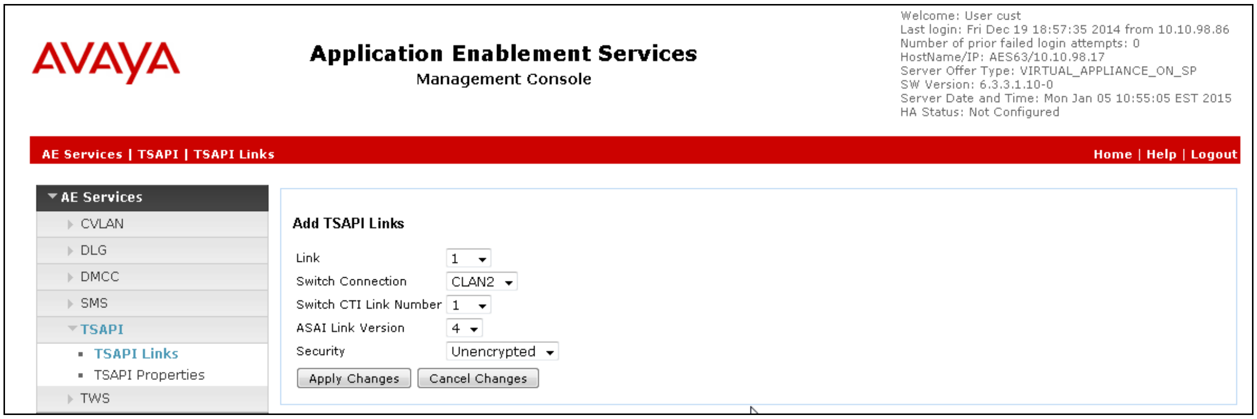


Welcome: User cust
Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 10:50:53 EST 2015
HA Status: Not Configured

TSAPI Links

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 "CLAN2" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



Welcome: User cust
Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 10:55:05 EST 2015
HA Status: Not Configured

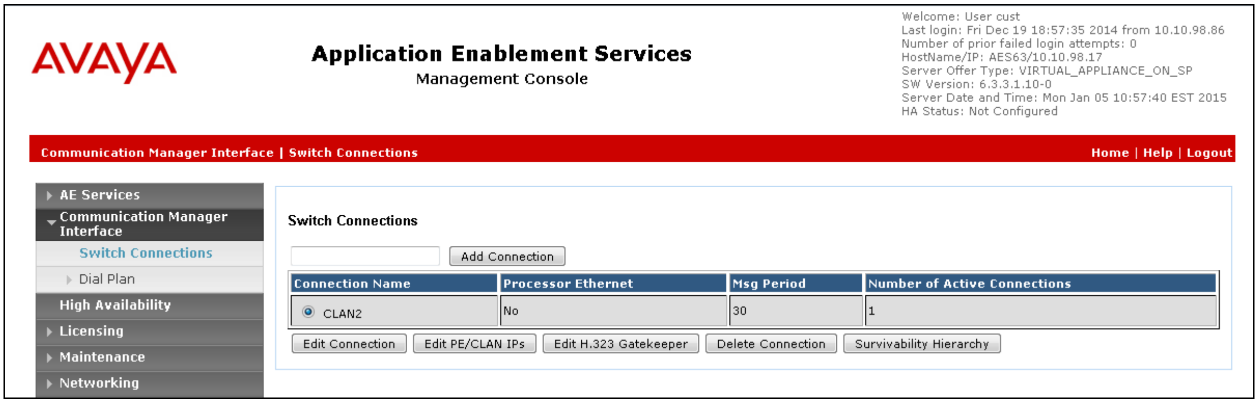
Add TSAPI Links

Link	1
Switch Connection	CLAN2
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 "**CLAN2**", and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

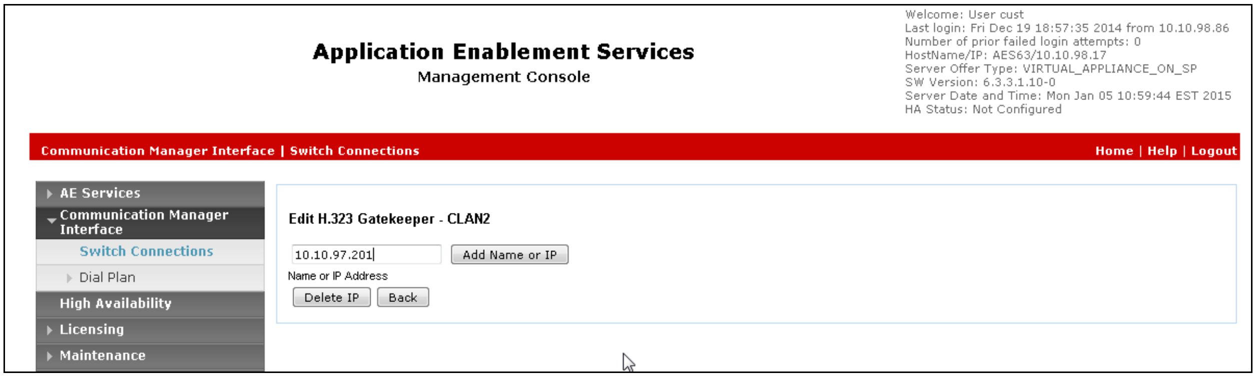


Welcome: User cust
Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 10:57:40 EST 2015
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● CLAN2	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 the H.323 gatekeeper, in this case "**10.10.97.201**" as shown below. Click **Add Name or IP**.



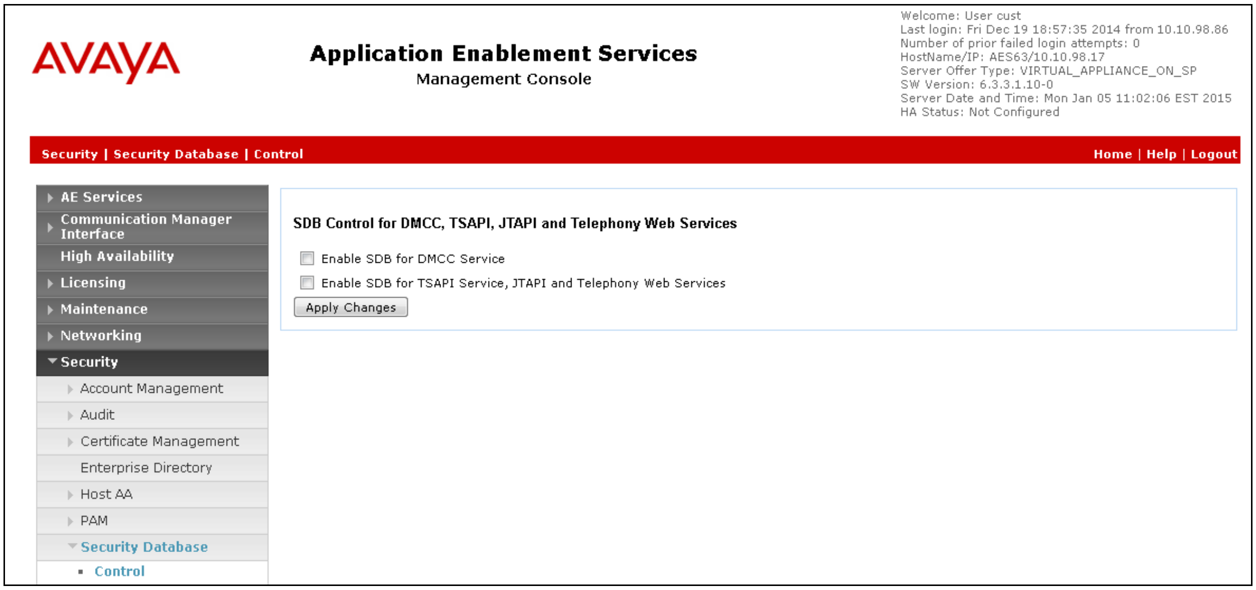
Welcome: User cust
Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 10:59:44 EST 2015
HA Status: Not Configured

Edit H.323 Gatekeeper - CLAN2

10.10.97.201
Name or IP Address

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.



Welcome: User cust
Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 11:02:06 EST 2015
HA Status: Not Configured

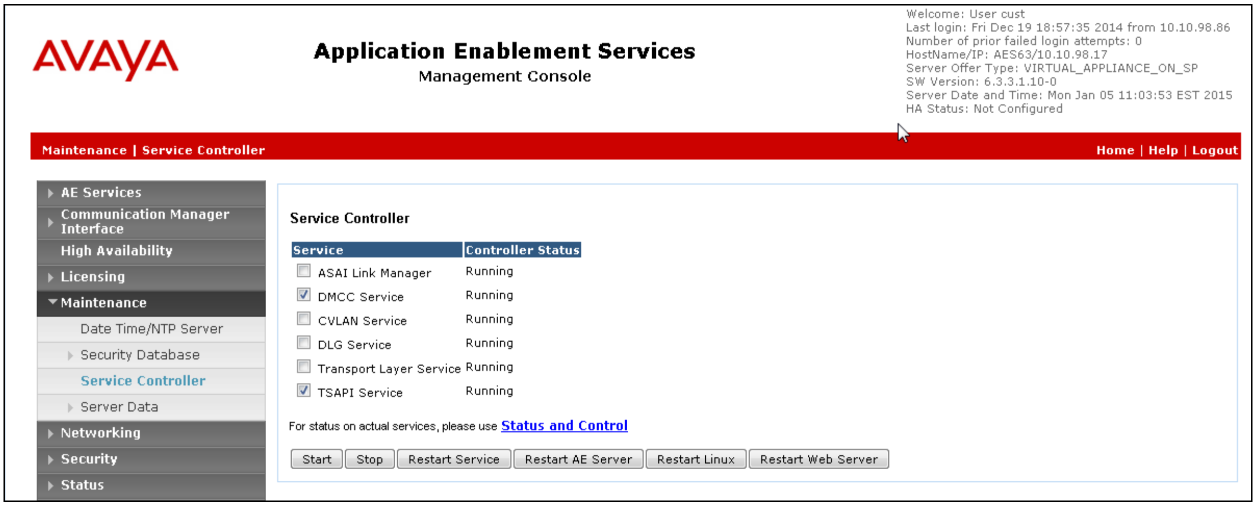
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

□ Enable SDB for DMCC Service

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

6.6. Restart Services

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



Welcome: User cust
Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 11:03:53 EST 2015
HA Status: Not Configured

Service Controller

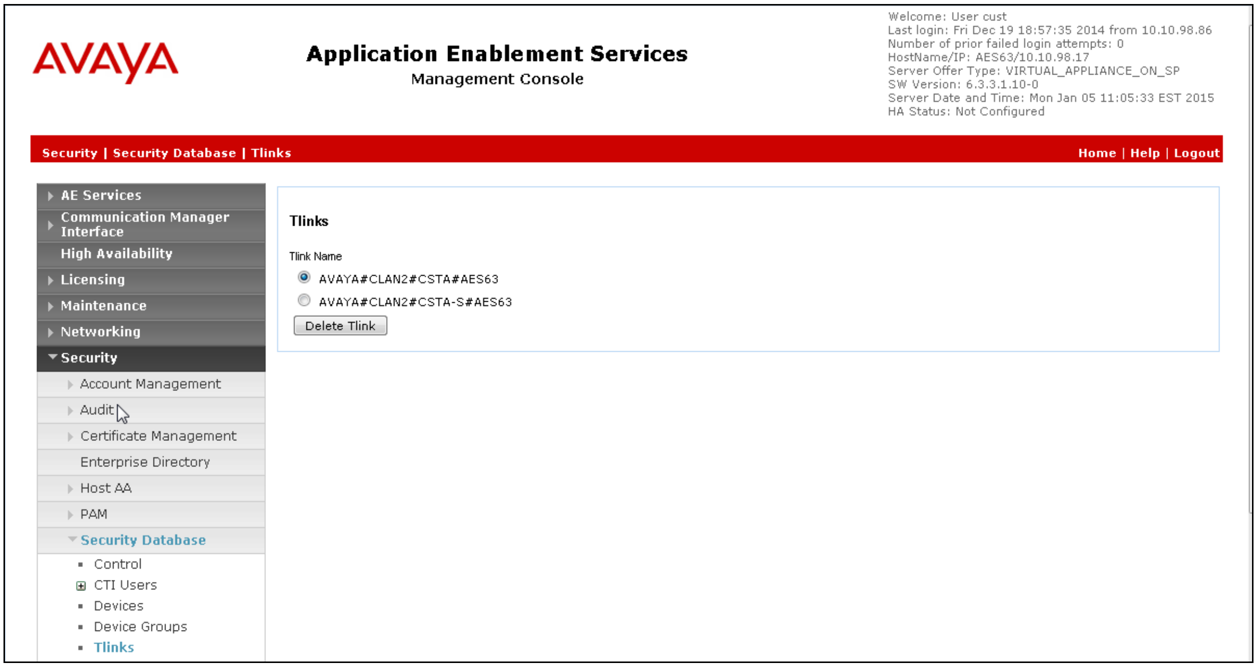
Service	Controller Status
□ ASAI Link Manager	Running
☑ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

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#**CLAN2**#CSTA#AES63". Note the use of the switch connection "CLAN2" from **Section 6.3** as part of the Tlink name.



Welcome: User cust
Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 11:05:33 EST 2015
HA Status: Not Configured

Tlinks

Tlink Name

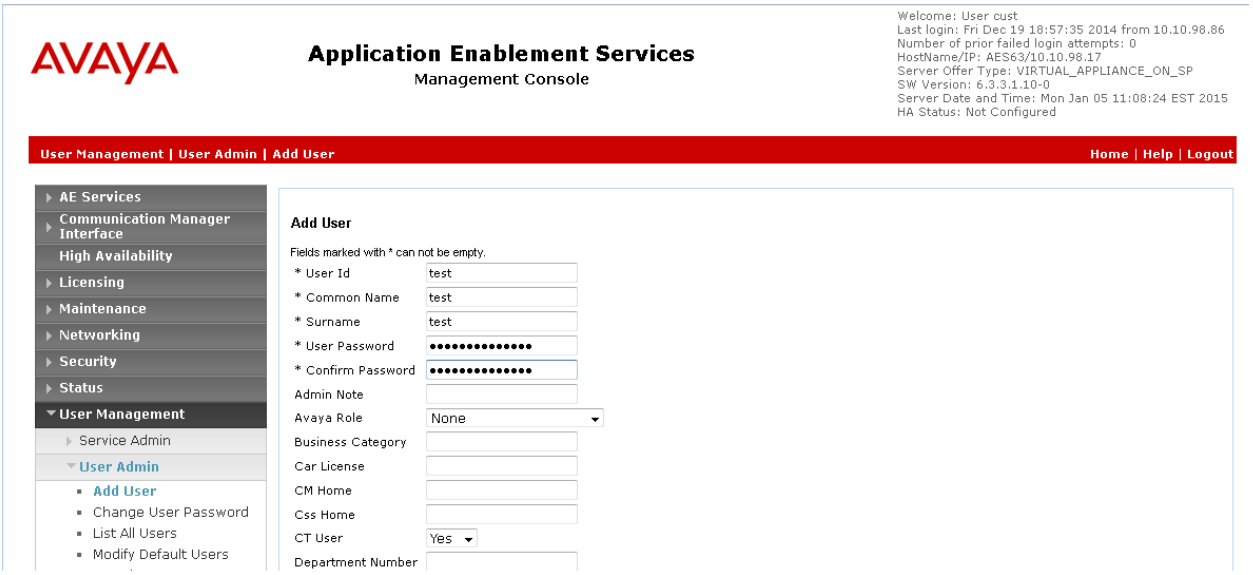
● AVAYA#CLAN2#CSTA#AES63

○ AVAYA#CLAN2#CSTA-S#AES63

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.



Welcome: User cust
Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 11:08:24 EST 2015
HA Status: Not Configured

Add User

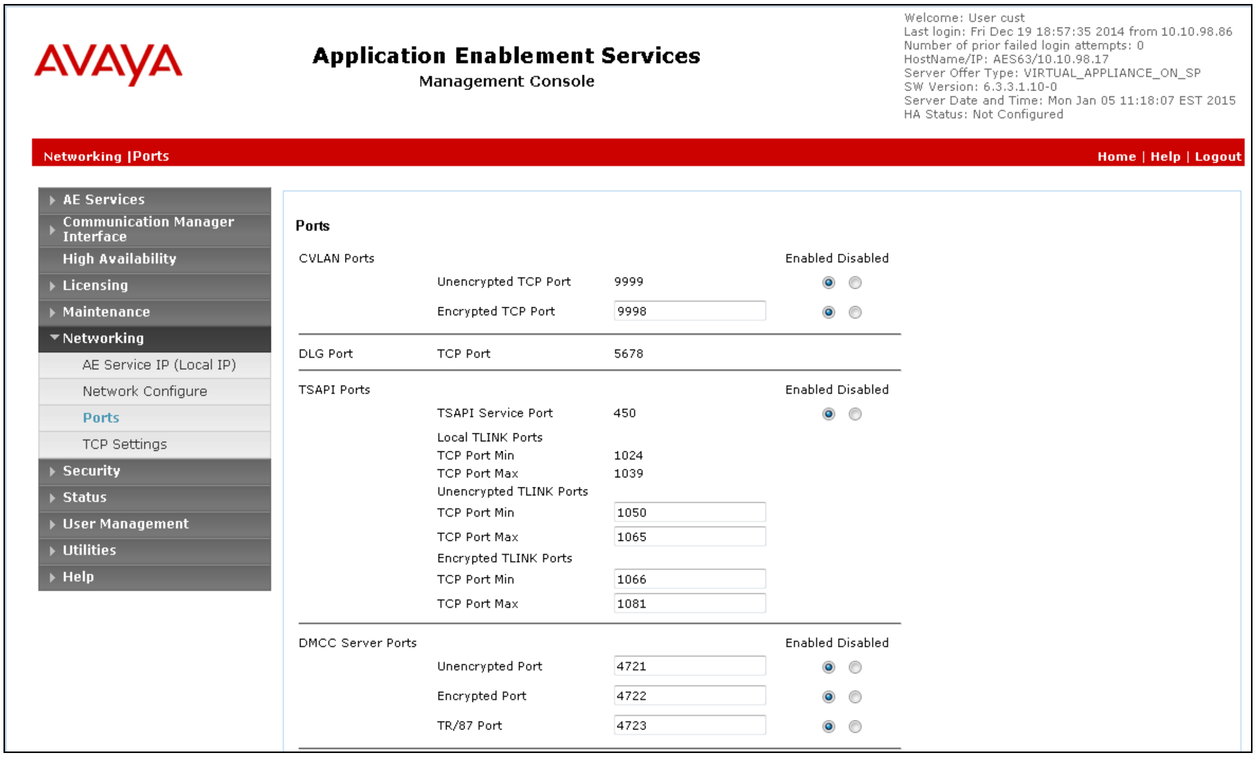
Fields marked with * can not be empty.

* User Id	test
* Common Name	test
* Surname	test
* User Password	••••••••••••••
* Confirm Password	••••••••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	

6.9. Enable Ports

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

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



Welcome: User cust
Last login: Fri Dec 19 18:57:35 2014 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 11:18:07 EST 2015
HA Status: Not Configured

Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	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			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

7. Configure dvsAnalytics Encore

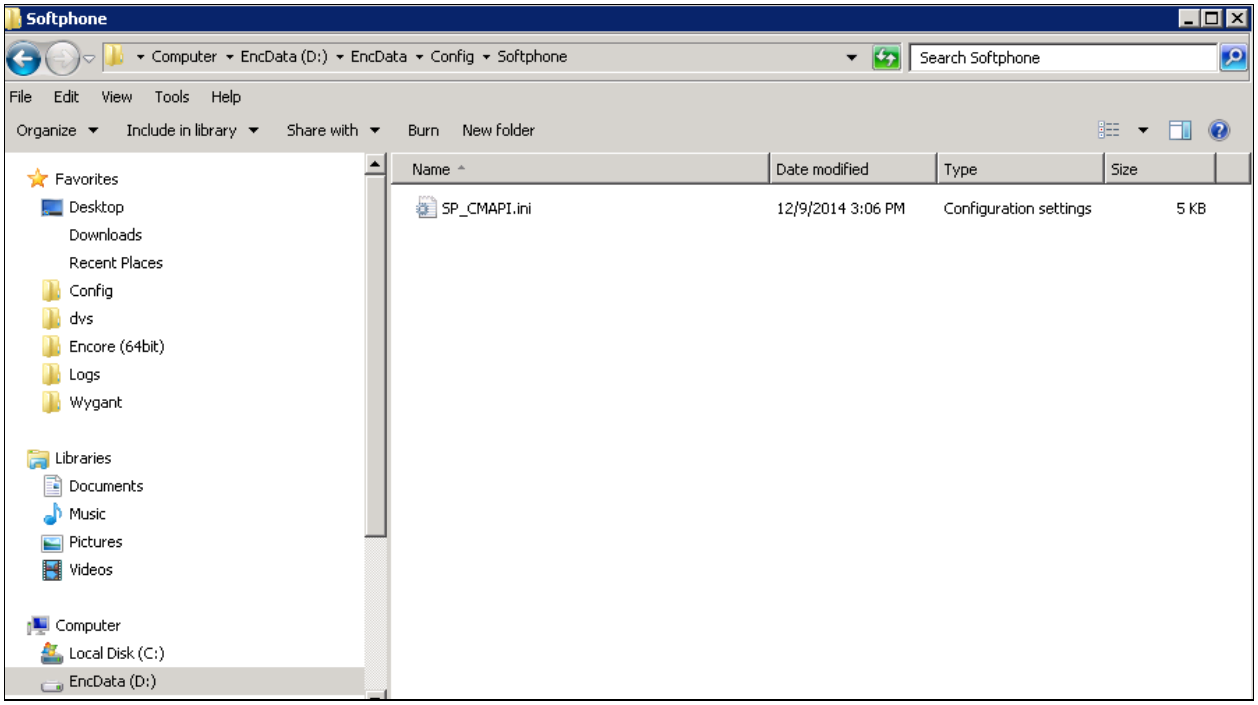
This section provides the procedures for configuring Encore. The procedures include the following areas:

- Administer Softphones
- Administer CTISetup
- Administer CT Gateway

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

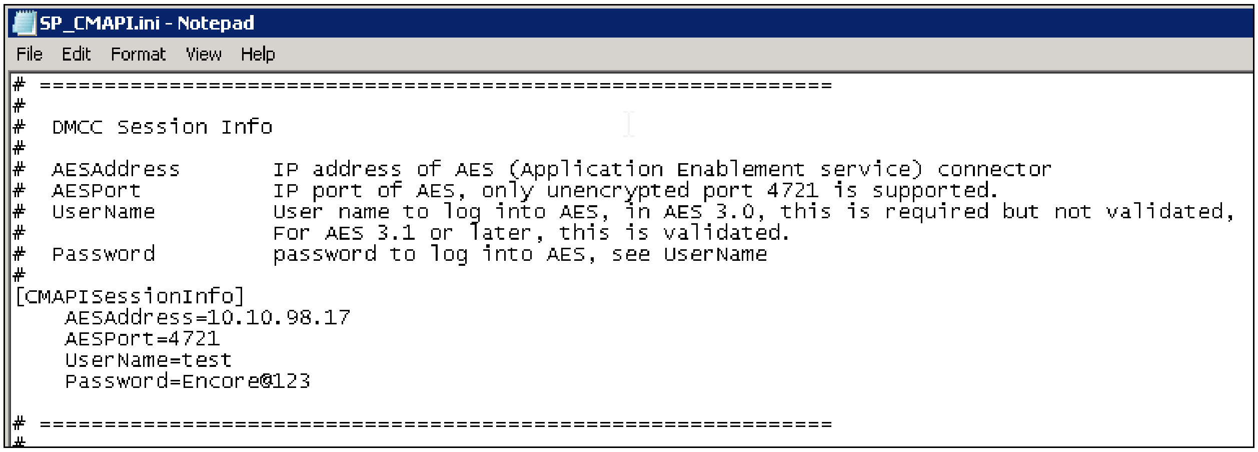
7.1. Administer Softphones

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



Name	Date modified	Type	Size
SP_CMAPI.ini	12/9/2014 3:06 PM	Configuration settings	5 KB

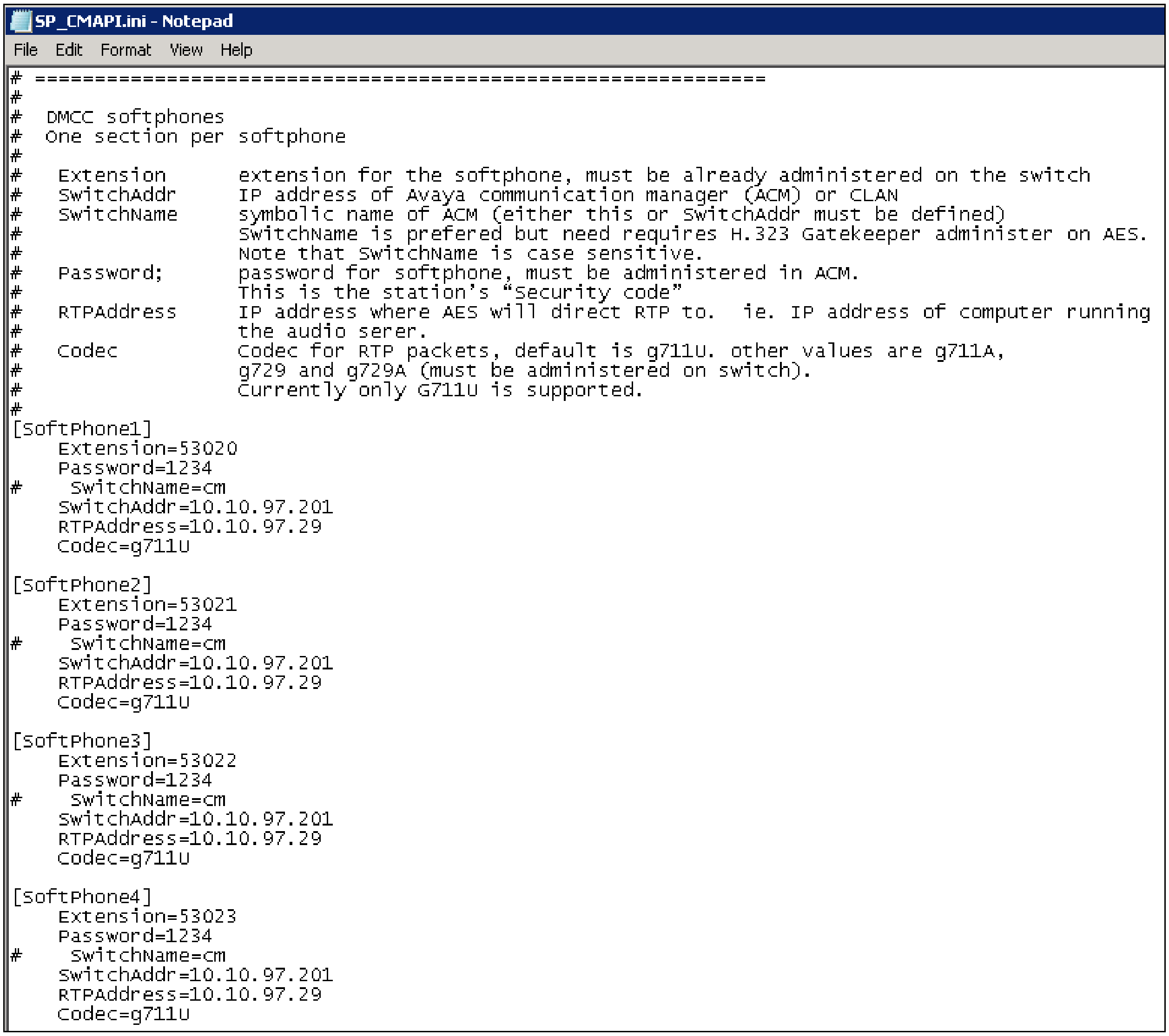
Scroll down to the **DMCC Session Info** sub-section. Under **CMAPISessionInfo**, set **AESAddress** to the IP address of the Application Enablement Services server. Set **UserName** and **Password** to the Encore user credentials from **Section 6.8**. Retain the default value for the remaining fields.



```
# ==============================================================
#
#   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=10.10.98.17
    AESPort=4721
    UserName=test
    Password=Encore@123

# ==============================================================
#
```

Scroll down to the **DMCC softphones** sub-section. Under **Softphone1**, set **Extension** and **Password** to the first virtual IP softphone extension and security code from **Section 5.7**. Set **SwitchAddr** to the IP address of the H.323 Gatekeeper from **Section 6.4**. Set **RTPAddress** to the IP address of the Encore server. Retain the default values for the remaining fields.

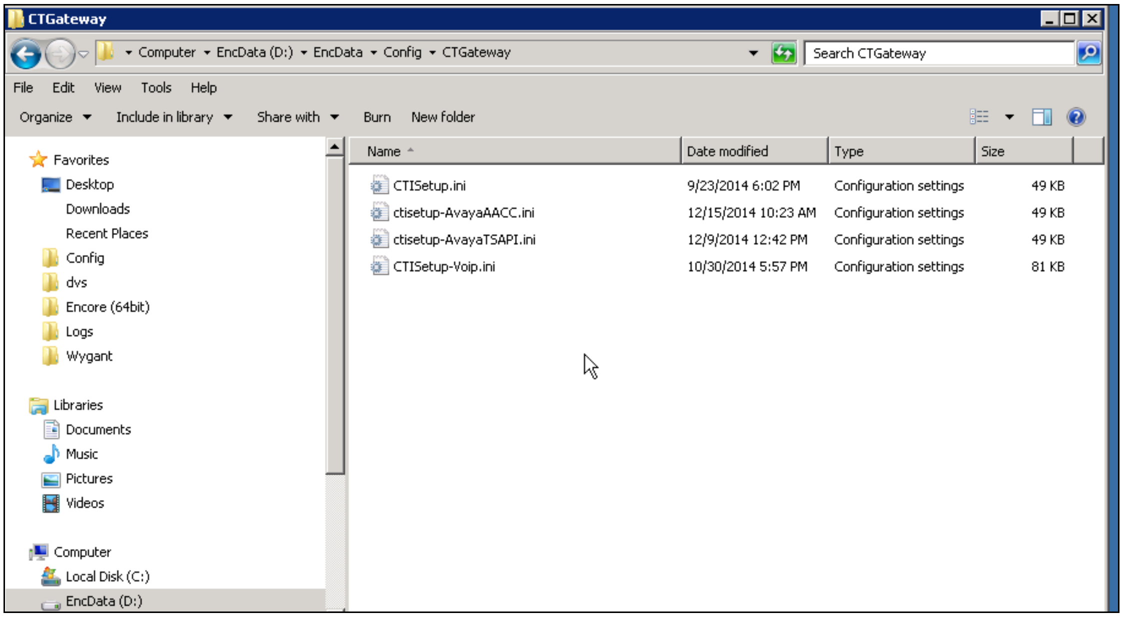
Create additional softphone entries as necessary. In the compliance testing, four softphones were configured to correspond to the four virtual IP softphones from **Section 5.7**.



```
# ==============================================================
#
#  DMCC softphones
#  One section per softphone
#
#   Extension      extension for the softphone, must be already administered on the switch
#   SwitchAddr     IP address of Avaya communication manager (ACM) or CLAN
#   SwitchName     symbolic name of ACM (either this or SwitchAddr must be defined)
#                  SwitchName is prefered but need requires H.323 Gatekeeper administer on AES.
#                  Note that SwitchName is case sensitive.
#   Password;      password for softphone, must be administered in ACM.
#                  This is the station's "Security code"
#   RTPAddress     IP address where AES will direct RTP to.  ie. IP address of computer running
#                  the audio serer.
#   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=53020
    Password=1234
#     SwitchName=cm
    SwitchAddr=10.10.97.201
    RTPAddress=10.10.97.29
    Codec=g711U

[SoftPhone2]
    Extension=53021
    Password=1234
#     SwitchName=cm
    SwitchAddr=10.10.97.201
    RTPAddress=10.10.97.29
    Codec=g711U

[SoftPhone3]
    Extension=53022
    Password=1234
#     SwitchName=cm
    SwitchAddr=10.10.97.201
    RTPAddress=10.10.97.29
    Codec=g711U

[SoftPhone4]
    Extension=53023
    Password=1234
#     SwitchName=cm
    SwitchAddr=10.10.97.201
    RTPAddress=10.10.97.29
    Codec=g711U
```

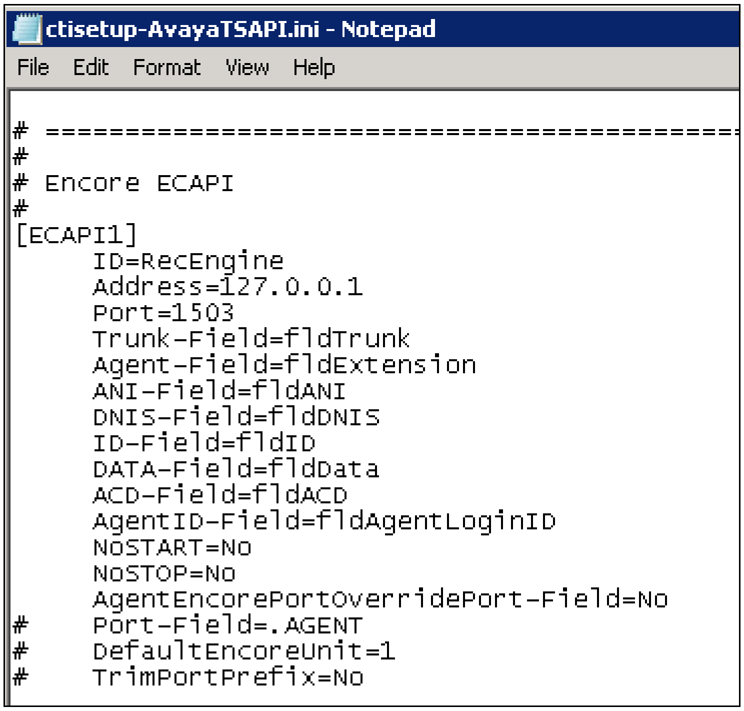
7.2. Administer CTISetup

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



Name	Date modified	Type	Size
CTISetup.ini	9/23/2014 6:02 PM	Configuration settings	49 KB
ctisetup-AvayaAACC.ini	12/15/2014 10:23 AM	Configuration settings	49 KB
ctisetup-AvayaTSAPI.ini	12/9/2014 12:42 PM	Configuration settings	49 KB
CTISetup-Voip.ini	10/30/2014 5:57 PM	Configuration settings	81 KB

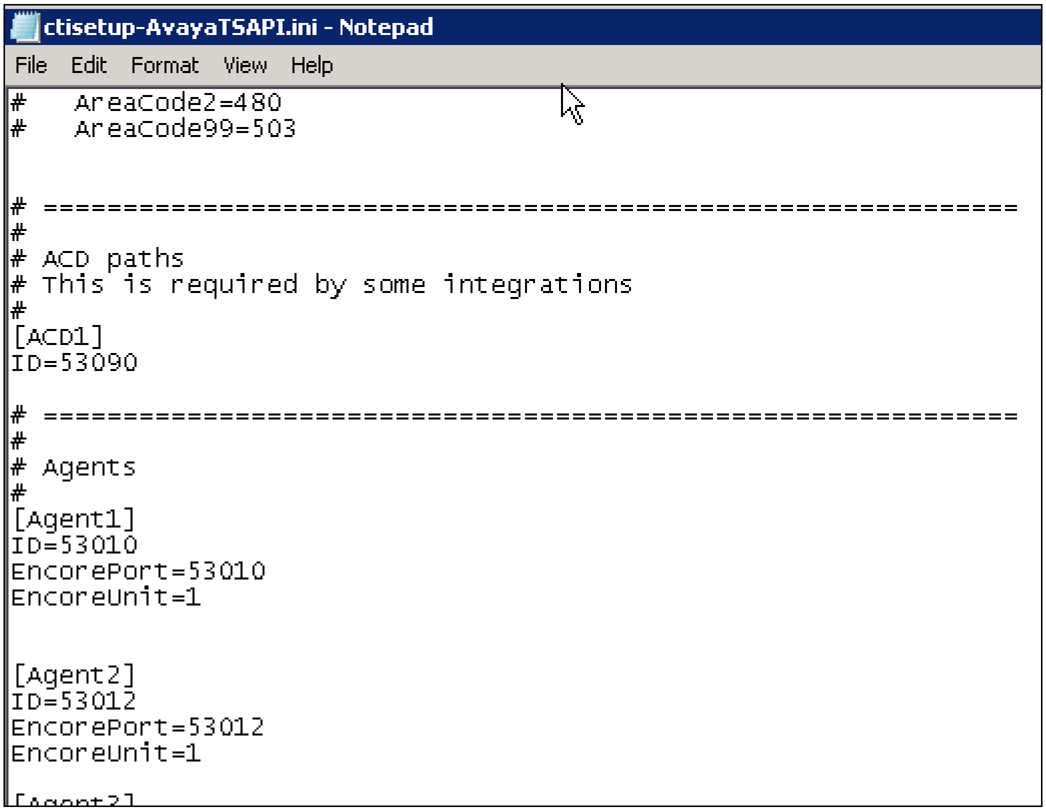
Scroll down to the **Encore ECAPI** sub-section. Under **ECAPI1**, make sure all parameters are set to the default values shown below.



```
# ============================================
#
# Encore ECAPI
#
[ECAPI1]
      ID=RecEngine
      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
      AgentEncorePortOverridePort-Field=No
#     Port-Field=.AGENT
#     DefaultEncoreUnit=1
#     TrimPortPrefix=No
```

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

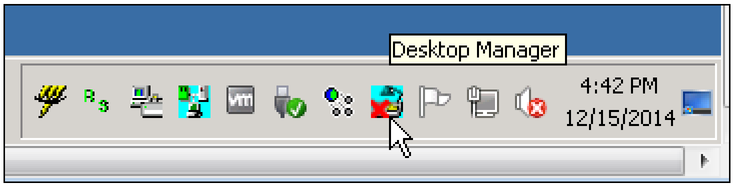
Scroll to the **Agents** sub-section. Under **Agent1**, set **ID** and **EncorePort** to the first agent station extension from **Section 3**. Create additional agent entries as necessary when more than one agent is being monitored.



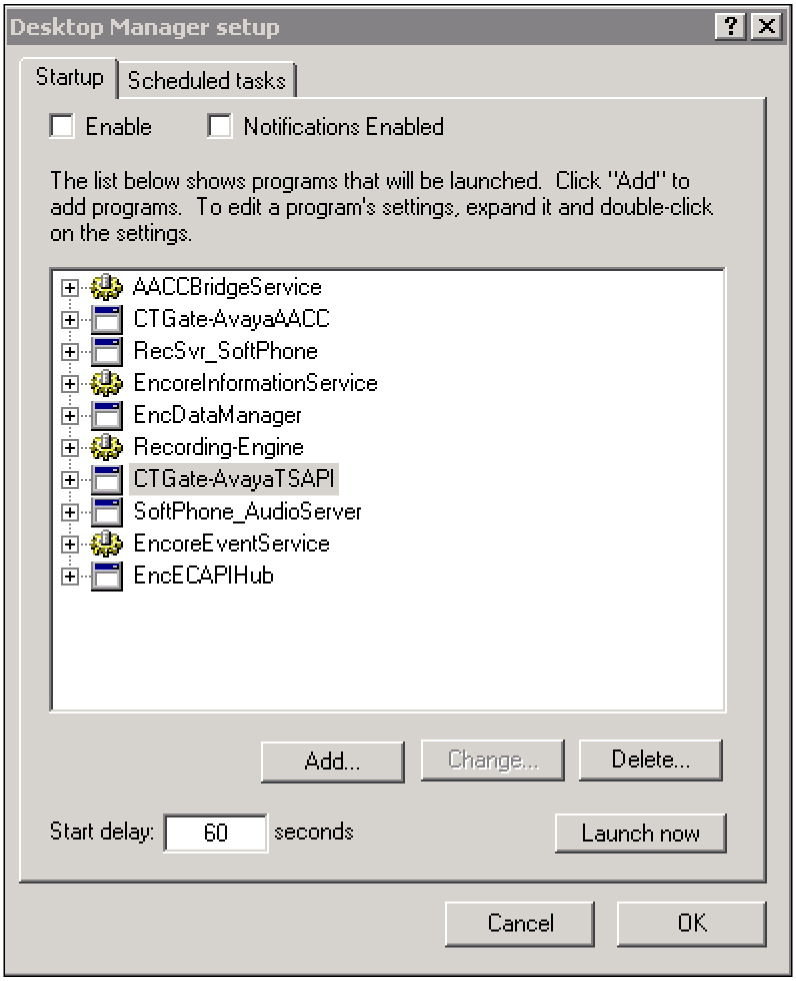
```
#   AreaCode2=480
#   AreaCode99=503


# ==============================================================
#
# ACD paths
# This is required by some integrations
#
[ACD1]
ID=53090

# ==============================================================
#
# Agents
#
[Agent1]
ID=53010
EncorePort=53010
EncoreUnit=1


[Agent2]
ID=53012
EncorePort=53012
EncoreUnit=1

[Agent3]
```

7.3. Administer CT Gateway

Right click on the **Desktop Manager** icon from the system tray, as shown below and choose **Configure** (not shown).



The **Desktop Manager setup** window is displayed as shown below. Select **CTGate-AvayaTSAPI** program from the **Startup** tab and click on the **Launch now** button.



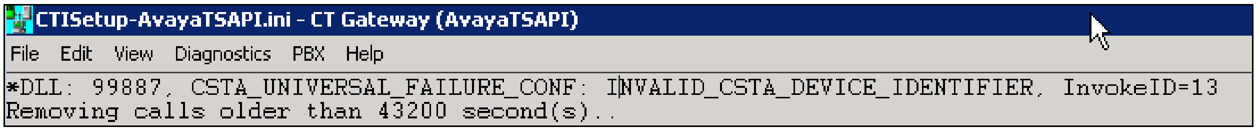
□ Enable □ Notifications Enabled

The list below shows programs that will be launched. Click "Add" to add programs. To edit a program's settings, expand it and double-click on the settings.

- AACCBridgeService
- CTGate-AvayaAACC
- RecSvr_SoftPhone
- EncoreInformationService
- EncDataManager
- Recording-Engine
- CTGate-AvayaTSAPI
- SoftPhone_AudioServer
- EncoreEventService
- EncECAPIHub

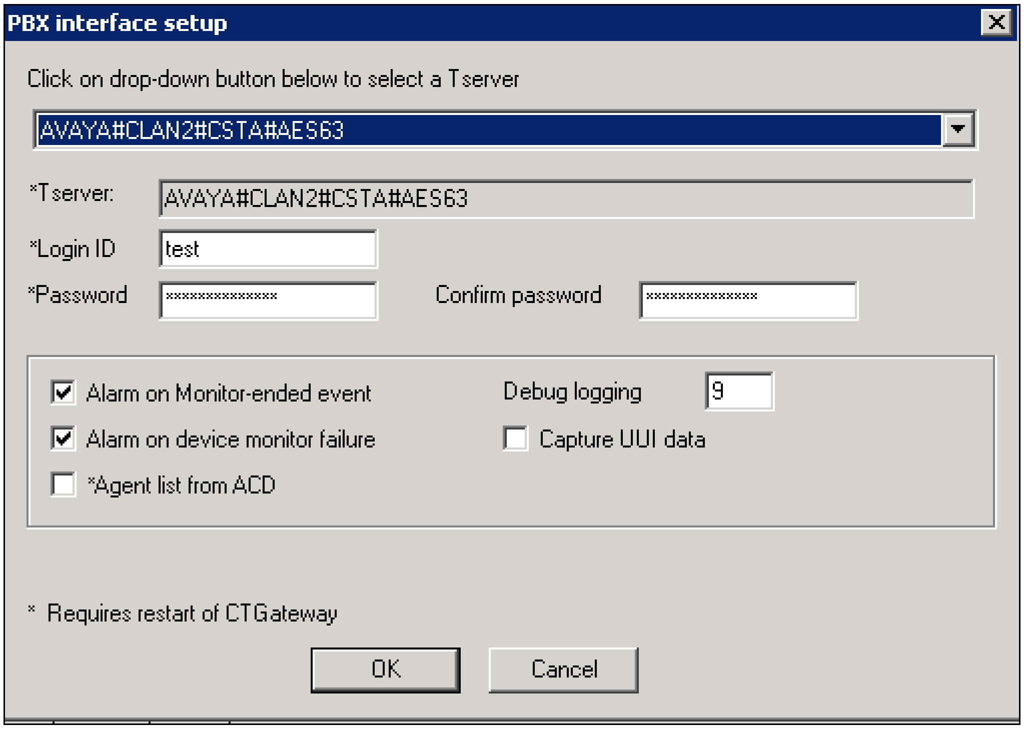
Start delay: 60 seconds

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


CTISetup-AvayaTSAPI.ini - CT Gateway (AvayaTSAPI)
File Edit View Diagnostics PBX Help

```
*DLL: 99887, CSTA_UNIVERSAL_FAILURE_CONF: INVALID_CSTA_DEVICE_IDENTIFIER, InvokeID=13
Removing calls older than 43200 second(s)..
```

The **PBX interface setup** screen is displayed. Select the Tlink name from **Section 6.7** from the drop-down list, and enter the Encore user credentials from **Section 6.8** for **Login ID**, **Password**, and **Confirm Password**. Retain the default values in the remaining fields, as shown below.



Click on drop-down button below to select a Tserver

AVAYA#CLAN2#CSTA#AES63

*Tserver: AVAYA#CLAN2#CSTA#AES63

*Login ID test

*Password ************** Confirm password **************

☑ Alarm on Monitor-ended event Debug logging 9

☑ Alarm on device monitor failure ☐ Capture UUI data

☐ *Agent list from ACD

* Requires restart of CTGateway

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

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     4        no    AES63            established   21       21
```

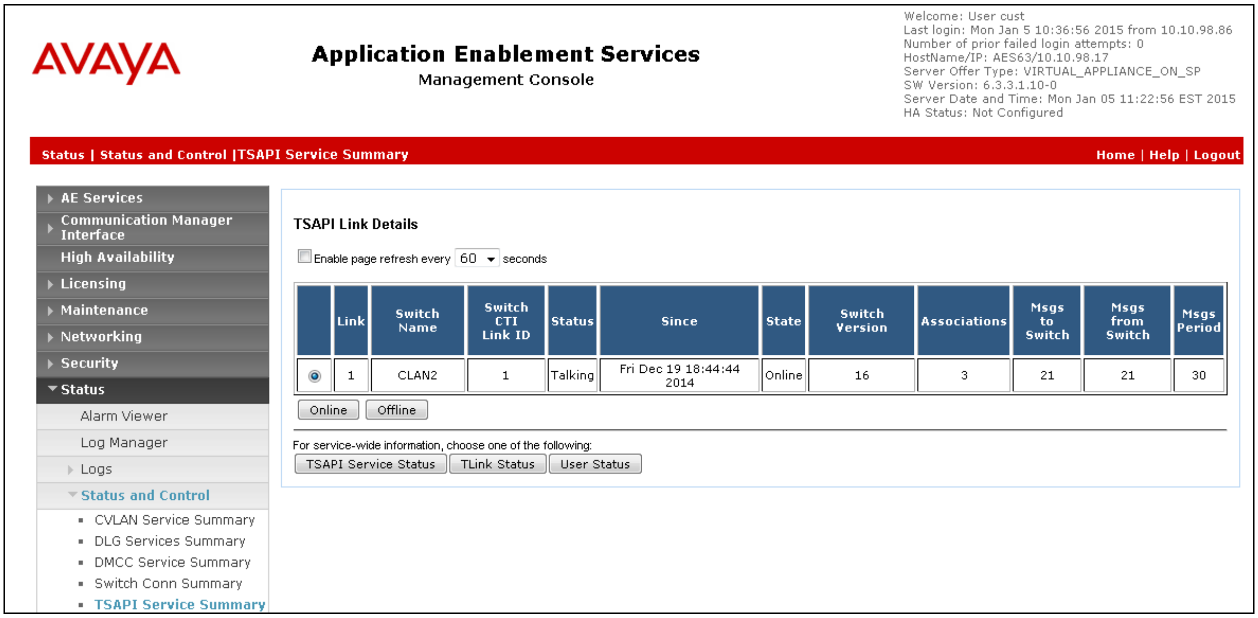
Verify the registration status of the virtual IP softphones by using the "list registered-ip-stations" command. Verify that all virtual IP softphone extensions from **Section 5.7** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations                                          Page   2

                            REGISTERED IP STATIONS

Station Ext    Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port   Net Rgn   Release    Skt Gatekeeper IP Address
-------------- --------- ---------- --- ---------------------------------------
53015          4620      IP_Phone    y  10.10.5.12
               1         2.300          10.10.97.201
53016          9620      IP_Phone    y  10.10.5.3
               1         6.3116         10.10.97.201
53018          4620      IP_Phone    y  10.10.5.61
               1         6.4014         135.10.97.201
53020          9650      IP_API_A    y  10.10.98.17
               1         3.2040         10.10.97.201
53021          4620      IP_API_A    y  10.10.98.17
               1         3.2040         10.10.97.201
53022          4620      IP_API_A    y  10.10.98.17
               1         3.2040         10.10.97.201
53023          4620      IP_API_A    y  10.10.98.17
               1         3.2040         10.10.97.201
```

8.2. Verify Avaya Aura® Application Enablement Services

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

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



Welcome: User cust
Last login: Mon Jan 5 10:36:56 2015 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 11:22:56 EST 2015
HA Status: Not Configured

TSAPI Link Details

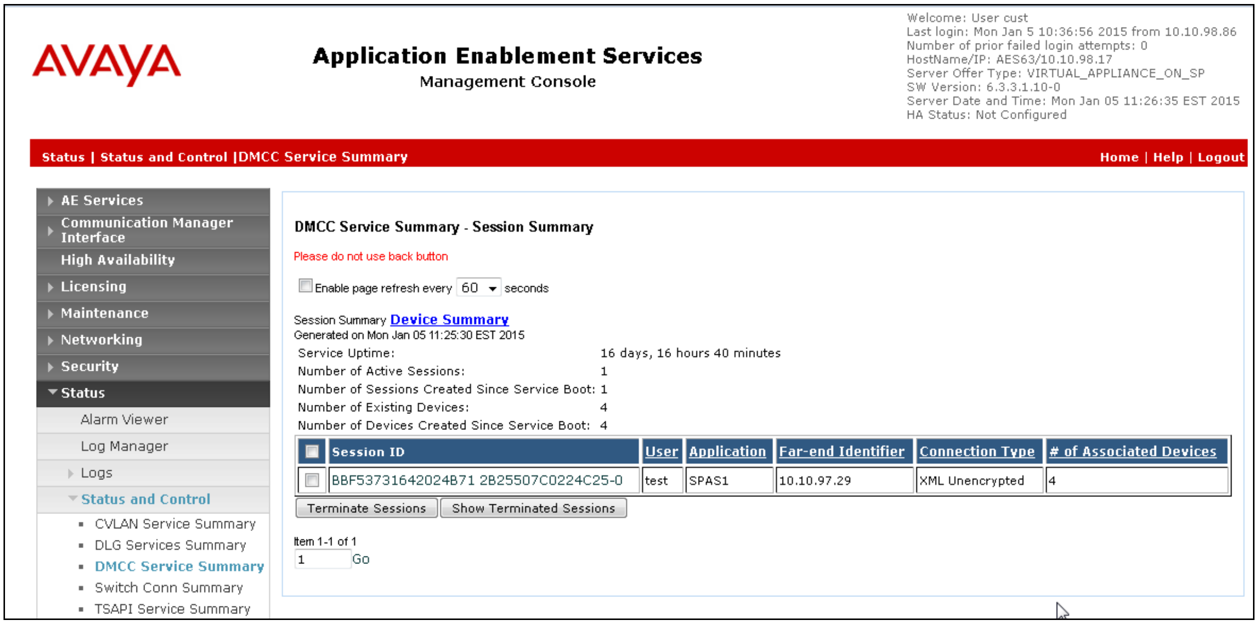
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	CLAN2	1	Talking	Fri Dec 19 18:44:44 2014	Online	16	3	21	21	30

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

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the Encore user name from **Section 6.8**, and that the **# of Associated Devices** column reflects the number of configured softphones from **Section 7.1**.



Welcome: User cust
Last login: Mon Jan 5 10:36:56 2015 from 10.10.98.86
Number of prior failed login attempts: 0
HostName/IP: AES63/10.10.98.17
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Jan 05 11:26:35 EST 2015
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

□ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Mon Jan 05 11:25:30 EST 2015

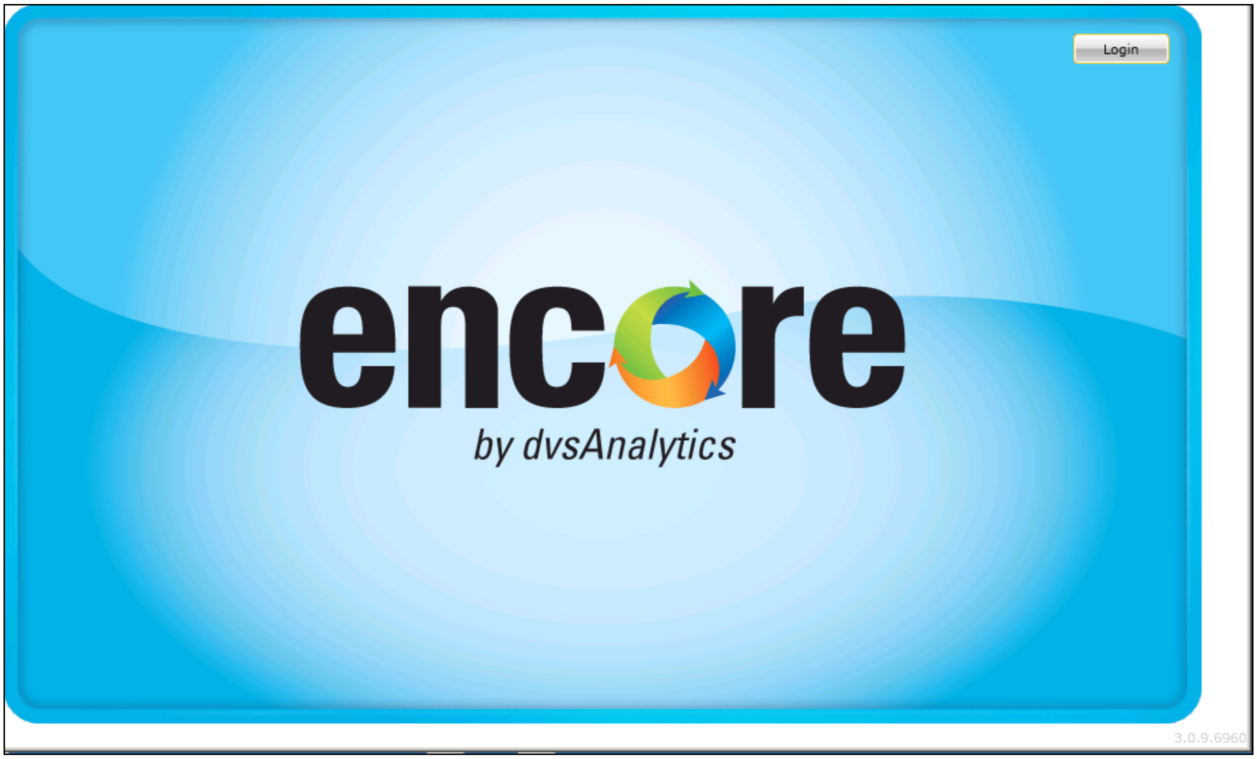
```
Service Uptime:                              16 days, 16 hours 40 minutes
Number of Active Sessions:                   1
Number of Sessions Created Since Service Boot: 1
Number of Existing Devices:                  4
Number of Devices Created Since Service Boot: 4
```

□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	BBF53731642024B71 2B25507C0224C25-0	test	SPAS1	10.10.97.29	XML Unencrypted	4

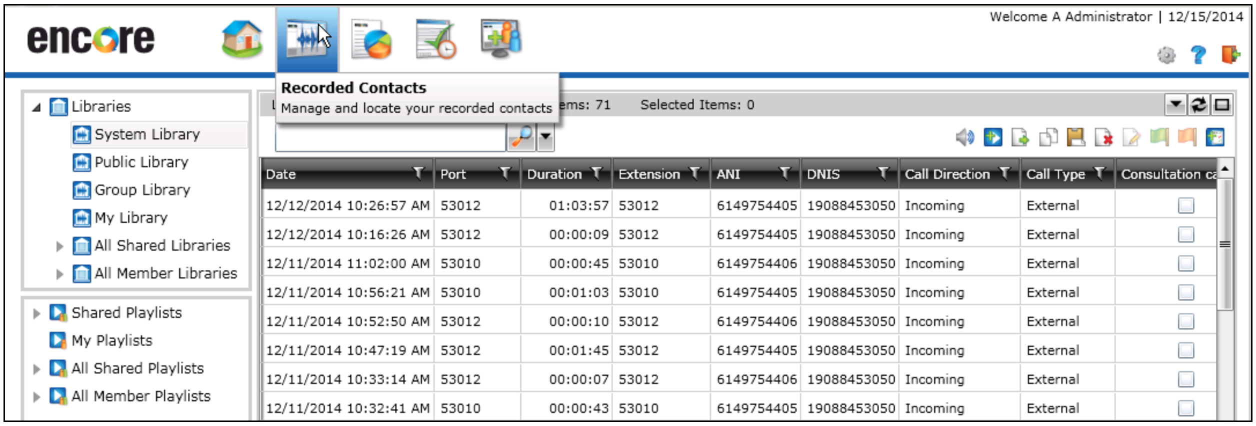
Item 1-1 of 1
1

8.3. Verify dvsAnalytics Encore

Log an agent into the skill group to handle and complete an ACD call. Access the Encore web interface by using the URL “http://ip-address/encore” in an Internet 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.



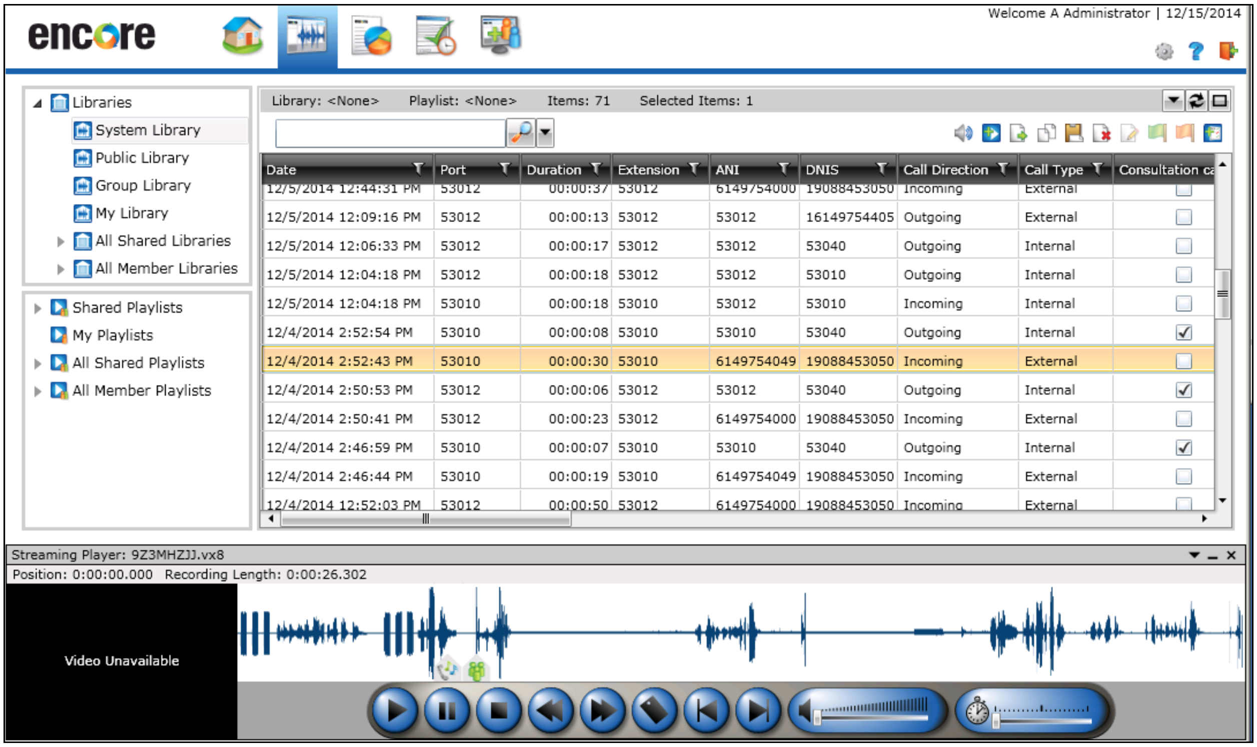
The **encore** screen is updated with a list of call recordings. Verify that there is an entry in the right pane reflecting the last call, with proper values in the relevant fields.



ems: 71 Selected Items: 0

Date	Port	Duration	Extension	ANI	DNIS	Call Direction	Call Type	Consultation ca
12/12/2014 10:26:57 AM	53012	01:03:57	53012	6149754405	19088453050	Incoming	External	□
12/12/2014 10:16:26 AM	53012	00:00:09	53012	6149754405	19088453050	Incoming	External	□
12/11/2014 11:02:00 AM	53010	00:00:45	53010	6149754406	19088453050	Incoming	External	□
12/11/2014 10:56:21 AM	53010	00:01:03	53010	6149754405	19088453050	Incoming	External	□
12/11/2014 10:52:50 AM	53012	00:00:10	53012	6149754406	19088453050	Incoming	External	□
12/11/2014 10:47:19 AM	53012	00:01:45	53012	6149754405	19088453050	Incoming	External	□
12/11/2014 10:33:14 AM	53012	00:00:07	53012	6149754406	19088453050	Incoming	External	□
12/11/2014 10:32:41 AM	53010	00:00:43	53010	6149754405	19088453050	Incoming	External	□

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.



Date	Port	Duration	Extension	ANI	DNIS	Call Direction	Call Type	Consultation ca
12/5/2014 12:44:31 PM	53012	00:00:37	53012	6149754000	19088453050	Incoming	External	□
12/5/2014 12:09:16 PM	53012	00:00:13	53012	53012	16149754405	Outgoing	External	□
12/5/2014 12:06:33 PM	53012	00:00:17	53012	53012	53040	Outgoing	Internal	□
12/5/2014 12:04:18 PM	53012	00:00:18	53012	53012	53010	Outgoing	Internal	□
12/5/2014 12:04:18 PM	53010	00:00:18	53010	53012	53010	Incoming	Internal	□
12/4/2014 2:52:54 PM	53010	00:00:08	53010	53010	53040	Outgoing	Internal	☑
12/4/2014 2:52:43 PM	53010	00:00:30	53010	6149754049	19088453050	Incoming	External	□
12/4/2014 2:50:53 PM	53012	00:00:06	53012	53012	53040	Outgoing	Internal	☑
12/4/2014 2:50:41 PM	53012	00:00:23	53012	6149754000	19088453050	Incoming	External	□
12/4/2014 2:46:59 PM	53010	00:00:07	53010	53010	53040	Outgoing	Internal	☑
12/4/2014 2:46:44 PM	53010	00:00:19	53010	6149754049	19088453050	Incoming	External	□
12/4/2014 12:52:03 PM	53012	00:00:50	53012	6149754000	19088453050	Incoming	External	□

9. Conclusion

These Application Notes describe the configuration steps required for dvsAnalytics Encore to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services 6.3 using Service Observing. All feature and serviceability test cases were completed with an observations in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3, June 2014, available at http://support.avaya.com.

2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, 02-300357, Release 6.3, June 2014, available at http://support.avaya.com.

3. *Avaya Aura^{TM} Communication Manager TSAPI Integration Guide*, Encore Version 6.0.1, October 3, 2014, available from dvsAnalytics Support.

4. *Avaya Aura^{TM} Communication Manager TSAPI Installation Addendum*, Release 2.3.5, October 20, 2014, available from dvsAnalytics Support.

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.