Avaya Solution & Interoperability Test Lab

Application Notes for dvsAnalytics Encore 6.0.6 with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 using Service Observing – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for dvsAnalytics Encore 6.0.6 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 using Service Observing. dvsAnalytics Encore is a call recording solution.

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

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for dvsAnalytics Encore 6.0.6 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 using Service Observing. Encore is a call recording solution.

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

The TSAPI interface was used by Encore to monitor skill groups and agent stations on Communication Manager. The DMCC interface was used by Encore to register virtual IP softphones, and for adding the softphones to active calls using the Service Observing feature.

When there was an active call at a monitored agent station, Encore was informed of the call via event reports from the TSAPI interface. Encore started the call recording by adding a virtual IP softphone to the active call to obtain the media and use of the Service Observing feature via the DMCC interface. The event reports were 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 requested monitoring of skill groups and agent stations, performed device queries on agent stations, and registered the virtual IP softphones.

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

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

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

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

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

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

For the testing associated with these Application Notes, the interface between Application Enablement Services and Encore did not include use of any specific encryption features as requested by dvsAnalytics.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Encore:

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

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

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

- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711, forwarding, long duration, multiple calls, multiple agents, 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 configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described.

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

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

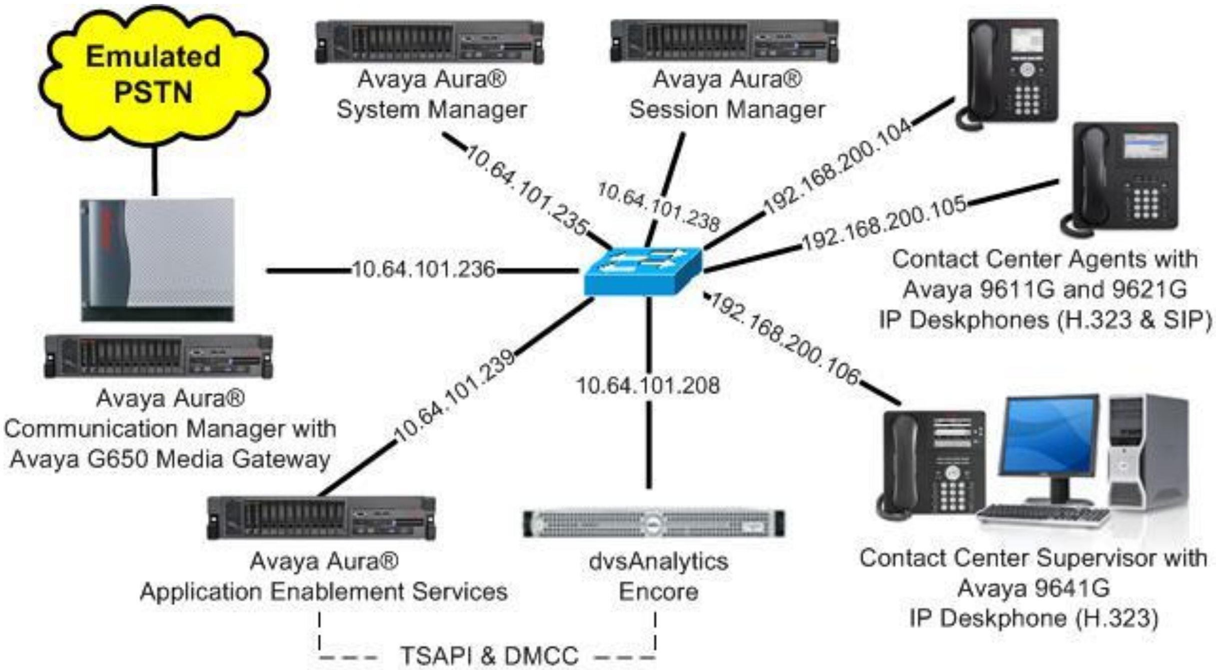

Emulated PSTN
Avaya Aura® System Manager
Avaya Aura® Session Manager
10.64.101.235
10.64.101.238
192.168.200.104
192.168.200.105
Contact Center Agents with Avaya 9611G and 9621G IP Deskphones (H.323 & SIP)
10.64.101.236
192.168.200.106
Avaya Aura® Communication Manager with Avaya G650 Media Gateway
10.64.101.239
10.64.101.208
Avaya Aura® Application Enablement Services
dvsAnalytics Encore
Contact Center Supervisor with Avaya 9641G IP Deskphone (H.323)
TSAPI & DMCC

Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	7.1.1 (7.1.1.0.0.532.23985)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.8.0.333
Avaya Aura® Application Enablement Services in Virtual Environment	7.1.1 (7.1.1.0.0.5-0)
Avaya Aura® Session Manager in Virtual Environment	7.1.1 (7.1.1.0.711008)
Avaya Aura® System Manager in Virtual Environment	7.1 .1 (7.1.1.0.046931)
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6506
Avaya 9621G IP Deskphone (SIP)	7.1.0.1.1
dvsAnalytics Encore on Windows Server 2012 R2 • Avaya TSAPI Windows Client (csta32.dll) • Avaya DMCC XML	6.0.6 Standard 6.3.3.103 6.1

5. Configure Avaya Aura® Communication Manager

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

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

5.1. Verify License

Log into the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command to verify that the **Computer Telephony Adjunct Links** customer option is set to "y" on **Page 4**. If this option is not set to "y", then contact the Avaya sales team or business partner for a proper license file.

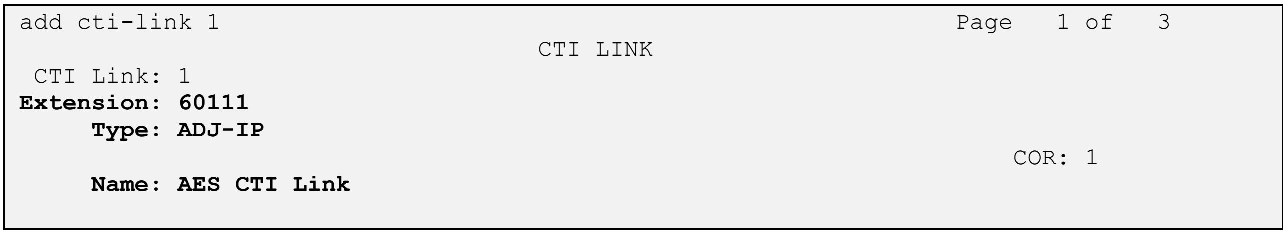
```
display system-parameters customer-options                      Page   4 of  12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y  Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
```

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

```
display system-parameters customer-options                      Page   7 of  12
                         CALL CENTER OPTIONAL FEATURES

                          Call Center Release: 7.0

                                ACD? y                        Reason Codes? y
                       BCMS (Basic)? y           Service Level Maximizer? n
         BCMS/VuStats Service Level? y        Service Observing (Basic)? y
  BSR Local Treatment for IP & ISDN? y    Service Observing (Remote/By FAC)? y
                  Business Advocate? n           Service Observing (VDNs)? y
                    Call Work Codes? y                           Timed ACW? y
      DTMF Feedback Signals For VRU? y                   Vectoring (Basic)? y
                   Dynamic Advocate? n               Vectoring (Prompting)? y
```

5.2. Administer CTI Link

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



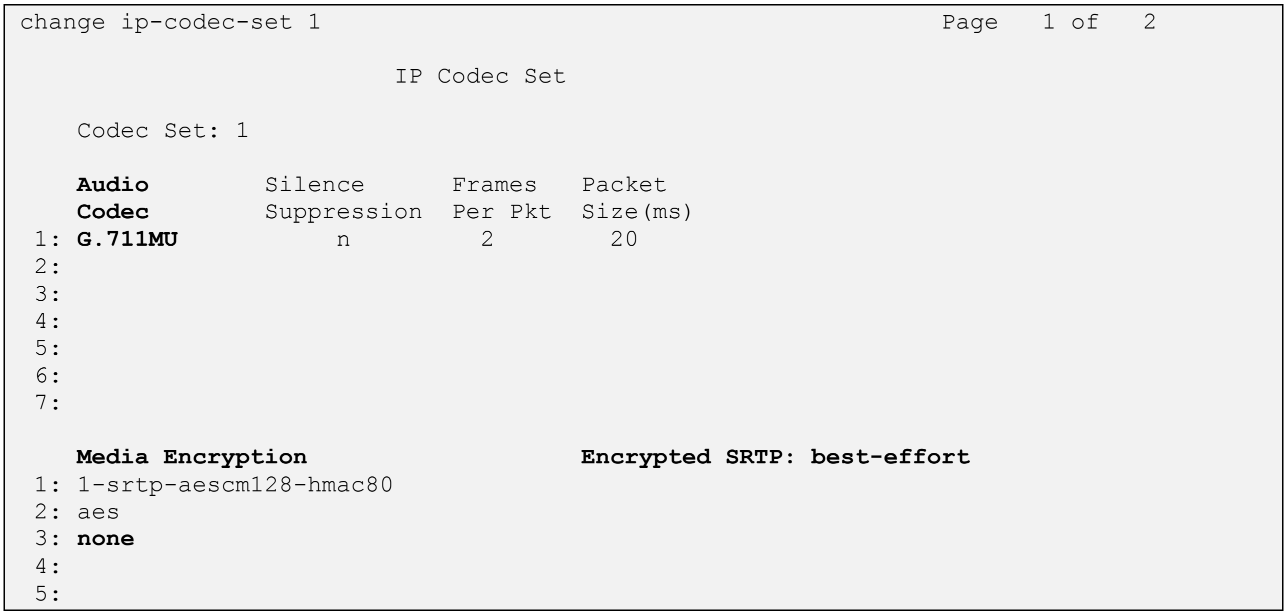
```
add cti-link 1                                                   Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 60111
     Type: ADJ-IP
                                                                     COR: 1
     Name: AES CTI Link
```

5.3. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with Encore. For **Audio Codec**, enter “G.711MU”, which is the only codec type supported by Encore along with variant “G.711A”.

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

In the compliance testing, this IP codec set was assigned to the agents and to the virtual IP softphones used by Encore.



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

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
 3:
 4:
 5:
 6:
 7:

    Media Encryption                   Encrypted SRTP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: aes
 3: none
 4:
 5:
```

5.4. Administer System Parameters Features

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

```
change system-parameters features                              Page   5 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

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

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

```
change system-parameters features                               Page  11 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:                    Delay:
    Message Waiting Lamp Indicates Status For: station

  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 Threshod: 2
    Reverse Star/Pound Digit For Collect Step? n
          Available Agent Adjustments for BSR? n
                             BSR Tie Strategy: 1st-found
   Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
              Service Observing: Warning Tone? n     or Conference Tone? n
    Allowed with Exclusion: Service Observing? n                    SSC? n
             Allow Two Observers in Same Call? y
```

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

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

    Reporting for PC Non-Predictive Calls? n

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

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

5.5. Administer Class of Restriction

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

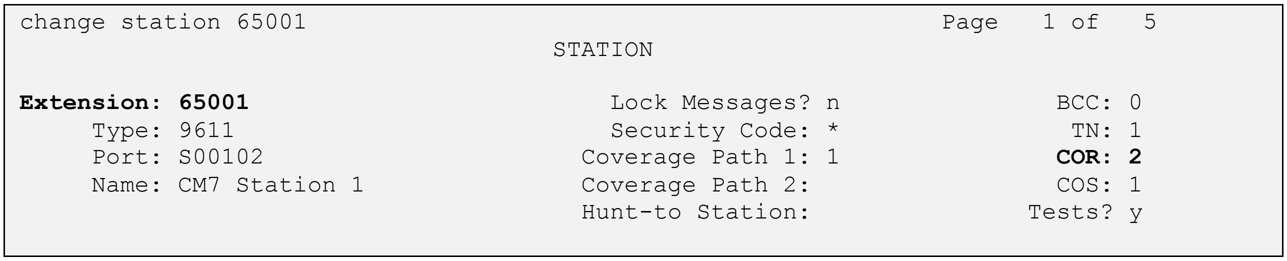
If desired, separate COR can be used for each parameter enablement. The COR with **Can Be Service Observed** enabled needs to be assigned to the agent stations, and the COR with **Can Be A Service Observer** enabled needs to be assigned to the virtual IP softphones.

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

               COR Number: 2
          COR Description:

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

5.6. Administer Agent Stations

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

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

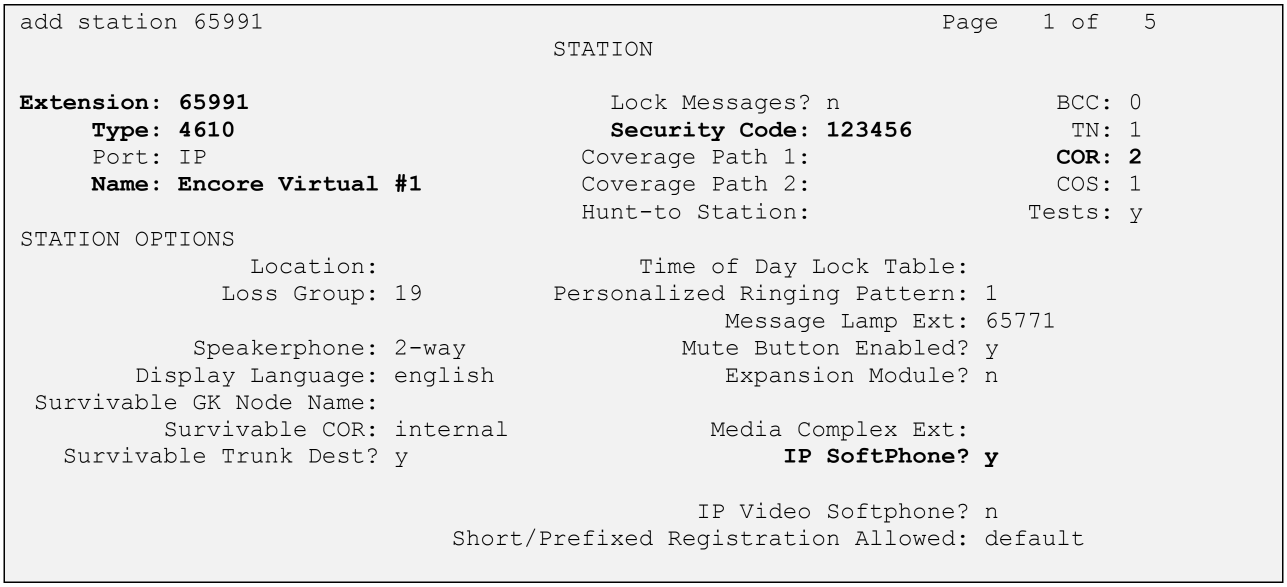


```
change station 65001                                            Page   1 of   5
                                     STATION

Extension: 65001                         Lock Messages? n               BCC: 0
     Type: 9611                          Security Code: *                TN: 1
     Port: S00102                      Coverage Path 1: 1               COR: 2
     Name: CM7 Station 1               Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
```

5.7. Administer Virtual IP Softphones

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

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as “4610”.
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **COR:** The COR number from **Section 5.5**.
- **IP SoftPhone:** “y”



```
add station 65991                                               Page   1 of   5
                                     STATION

Extension: 65991                         Lock Messages? n               BCC: 0
     Type: 4610                          Security Code: 123456           TN: 1
     Port: IP                          Coverage Path 1:                 COR: 2
     Name: Encore Virtual #1           Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests: y
STATION OPTIONS
                Location:                  Time of Day Lock Table:
              Loss Group: 19       Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 65771
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                Expansion Module? n
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

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

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

```
add station 65991                                              Page   4 of   5
                                    STATION
 SITE DATA
       Room:                                                 Headset? n
       Jack:                                                 Speaker? n
      Cable:                                                Mounting: d
      Floor:                                             Cord Length: 0
   Building:                                               Set Color:

ABBREVIATED DIALING
     List1:                   List2:                    List3:

BUTTON ASSIGNMENTS
 1: call-appr                            7:
 2: call-appr                            8:
 3: call-appr                            9:
 4: serv-obsrv                          10:
 5:                                     11:
```

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

```
list station 65991 count 4

                                 STATIONS

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

65991         S00007  Encore Virtual #1                           2
               4610                        no                     1   1
65992         S00011  Encore Virtual #2                           2
               4610                        no                     1   1
65993         S00014  Encore Virtual #3                           2
               4610                        no                     1   1
65994         S00017  Encore Virtual #4                           2
               4610                        no                     1   1
```

6. Configure Avaya Aura® Application Enablement Services

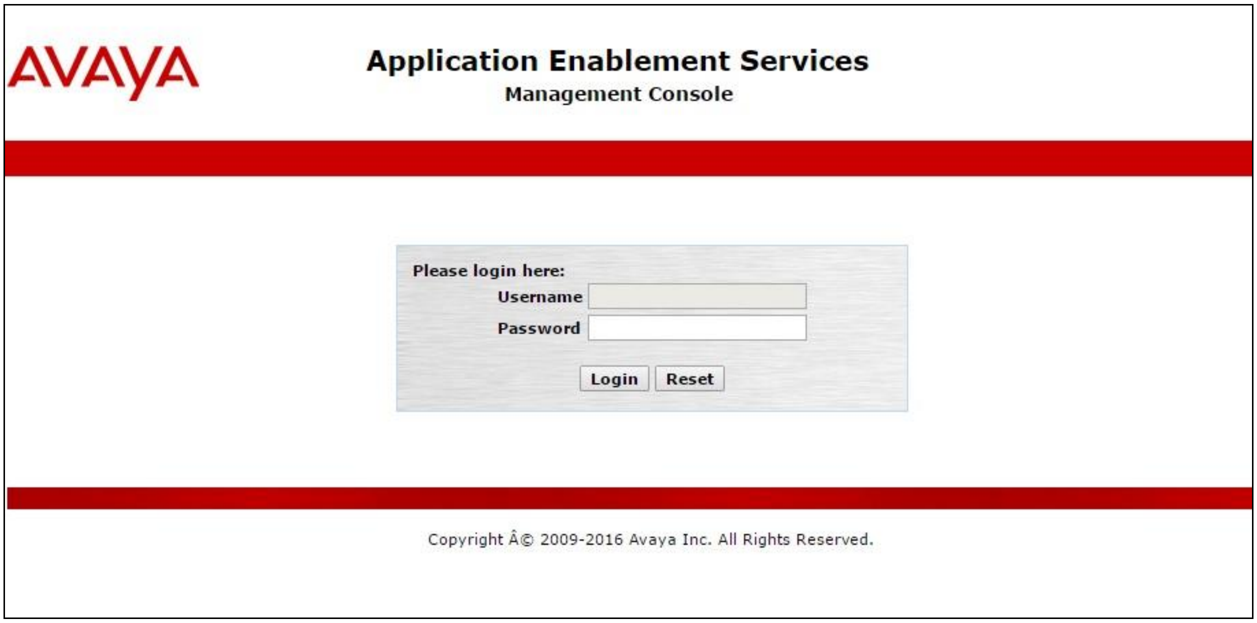
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

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

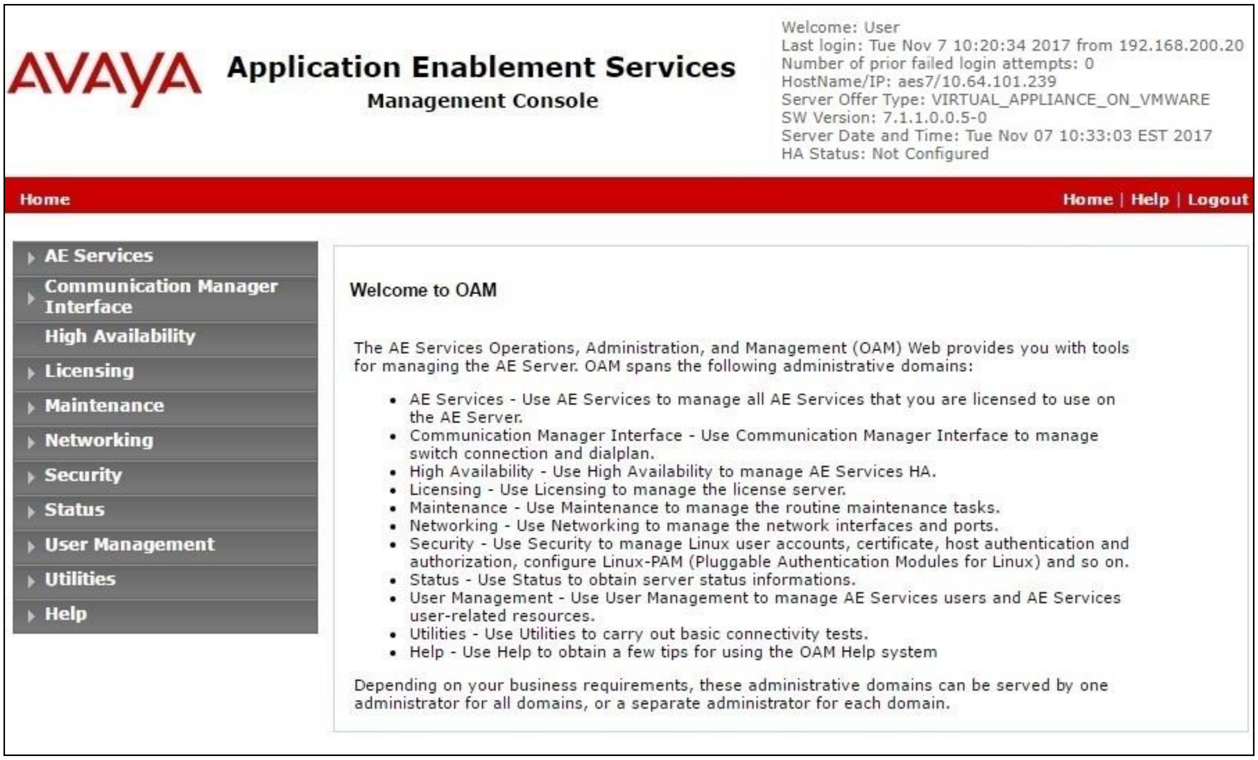
6.1. Launch OAM Interface

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

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


AVAYA
Application Enablement Services
Management Console
Please login here:
Username
Password
Login
Reset
Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

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



Welcome: User
Last login: Tue Nov 7 10:20:34 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 10:33:03 EST 2017
HA Status: Not Configured

Welcome to OAM

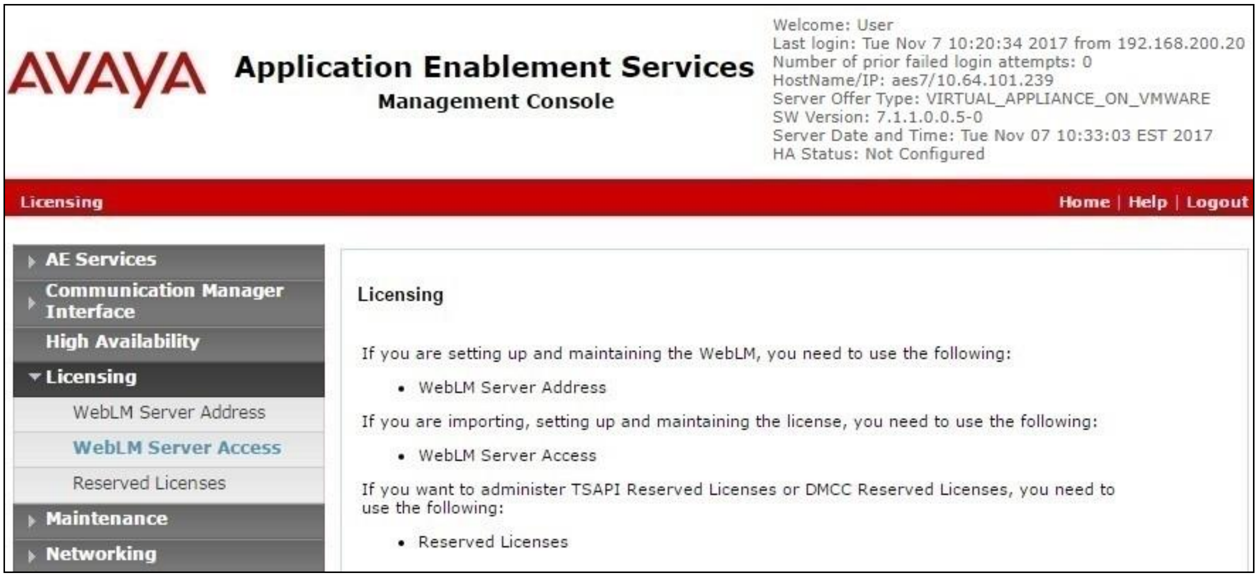
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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.

6.2. Verify License

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



Welcome: User
Last login: Tue Nov 7 10:20:34 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 10:33:03 EST 2017
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:

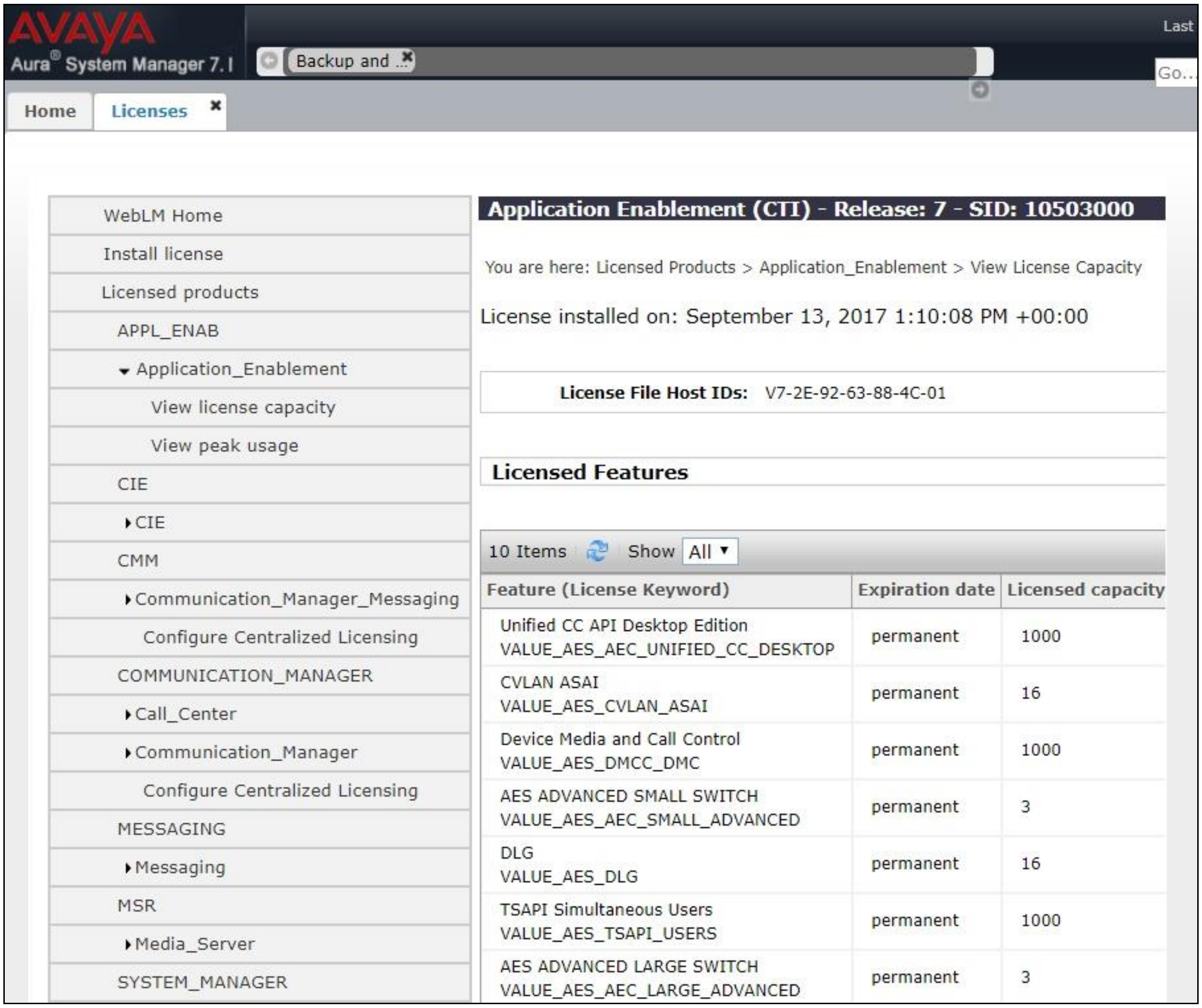
- WebLM Server Access

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

- Reserved Licenses

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.



Application Enablement (CTI) - Release: 7 - SID: 10503000

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: September 13, 2017 1:10:08 PM +00:00

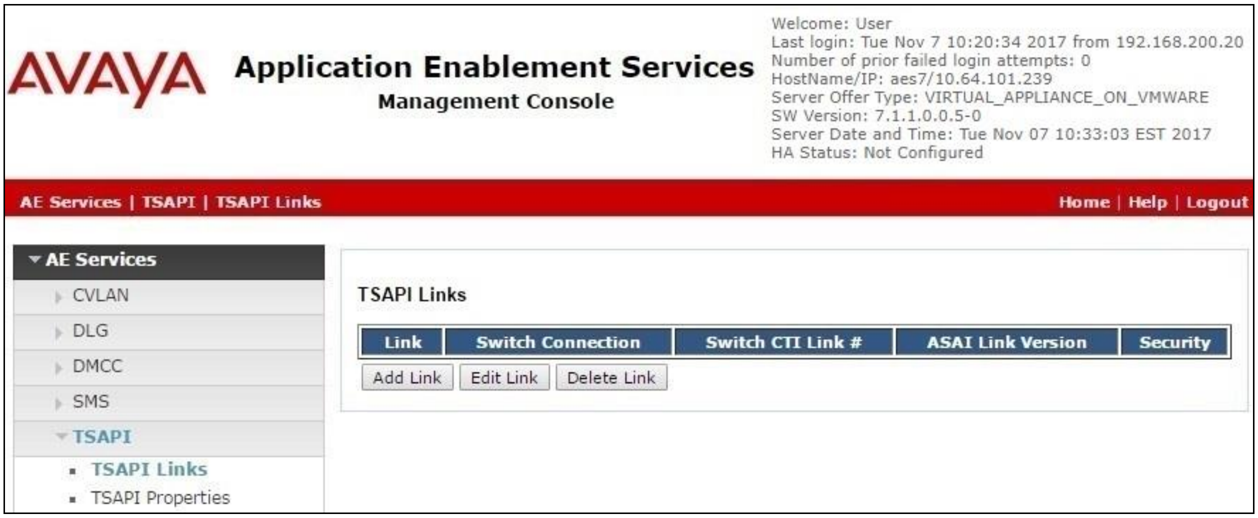
License File Host IDs: V7-2E-92-63-88-4C-01

Licensed Features

Feature (License Keyword)	Expiration date	Licensed capacity
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	3
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	3

6.3. Administer TSAPI Link

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



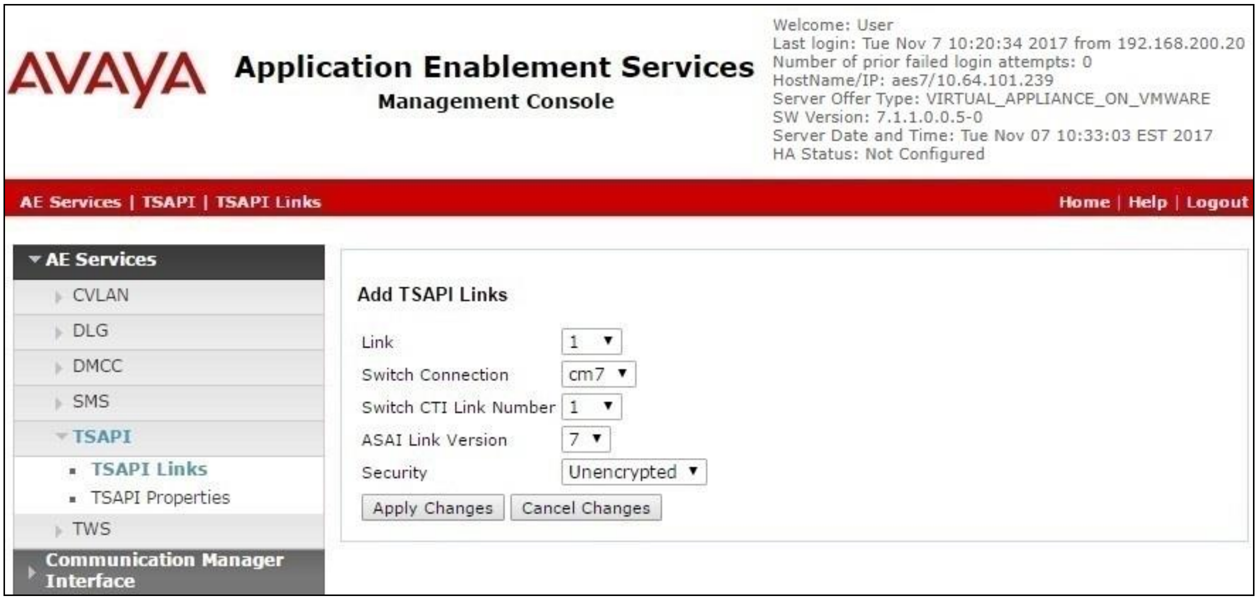
```
Welcome: User
Last login: Tue Nov 7 10:20:34 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 10:33:03 EST 2017
HA Status: Not Configured
```

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "cm7" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



```
Welcome: User
Last login: Tue Nov 7 10:20:34 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 10:33:03 EST 2017
HA Status: Not Configured
```

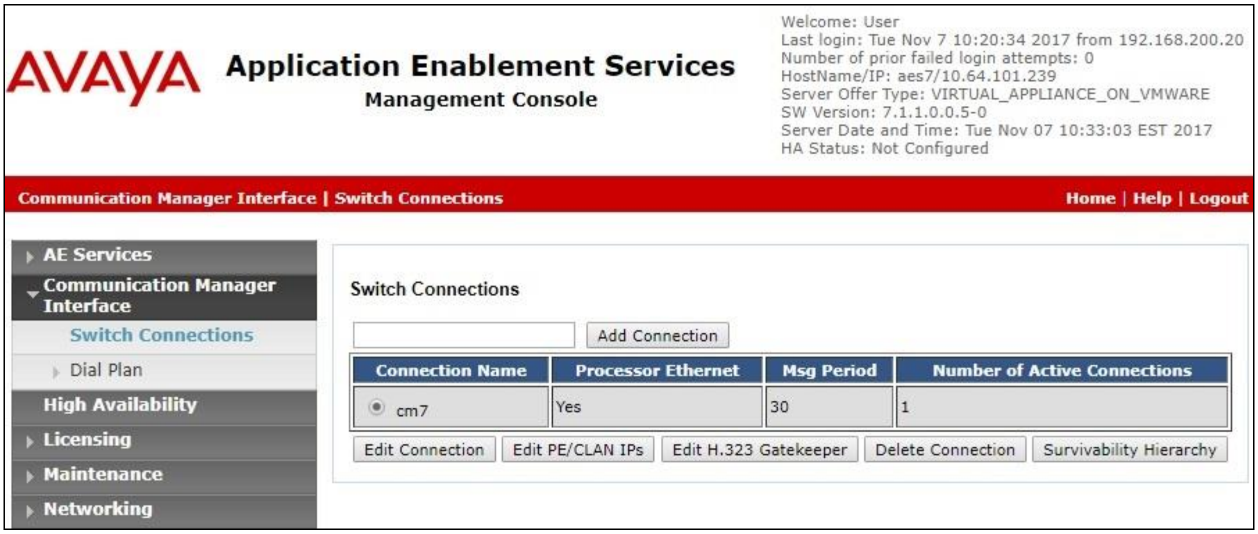
Add TSAPI Links

Link	1 ▾
Switch Connection	cm7 ▾
Switch CTI Link Number	1 ▾
ASAI Link Version	7 ▾
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 "cm7", and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

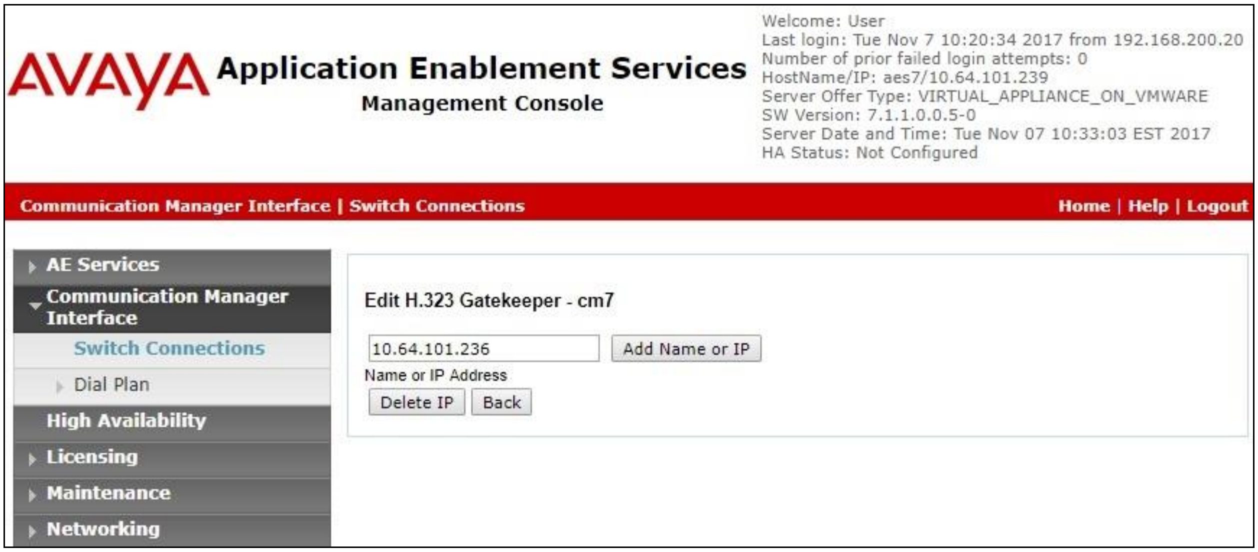


Welcome: User
Last login: Tue Nov 7 10:20:34 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 10:33:03 EST 2017
HA Status: Not Configured

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● cm7	Yes	30	1

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



Welcome: User
Last login: Tue Nov 7 10:20:34 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 10:33:03 EST 2017
HA Status: Not Configured

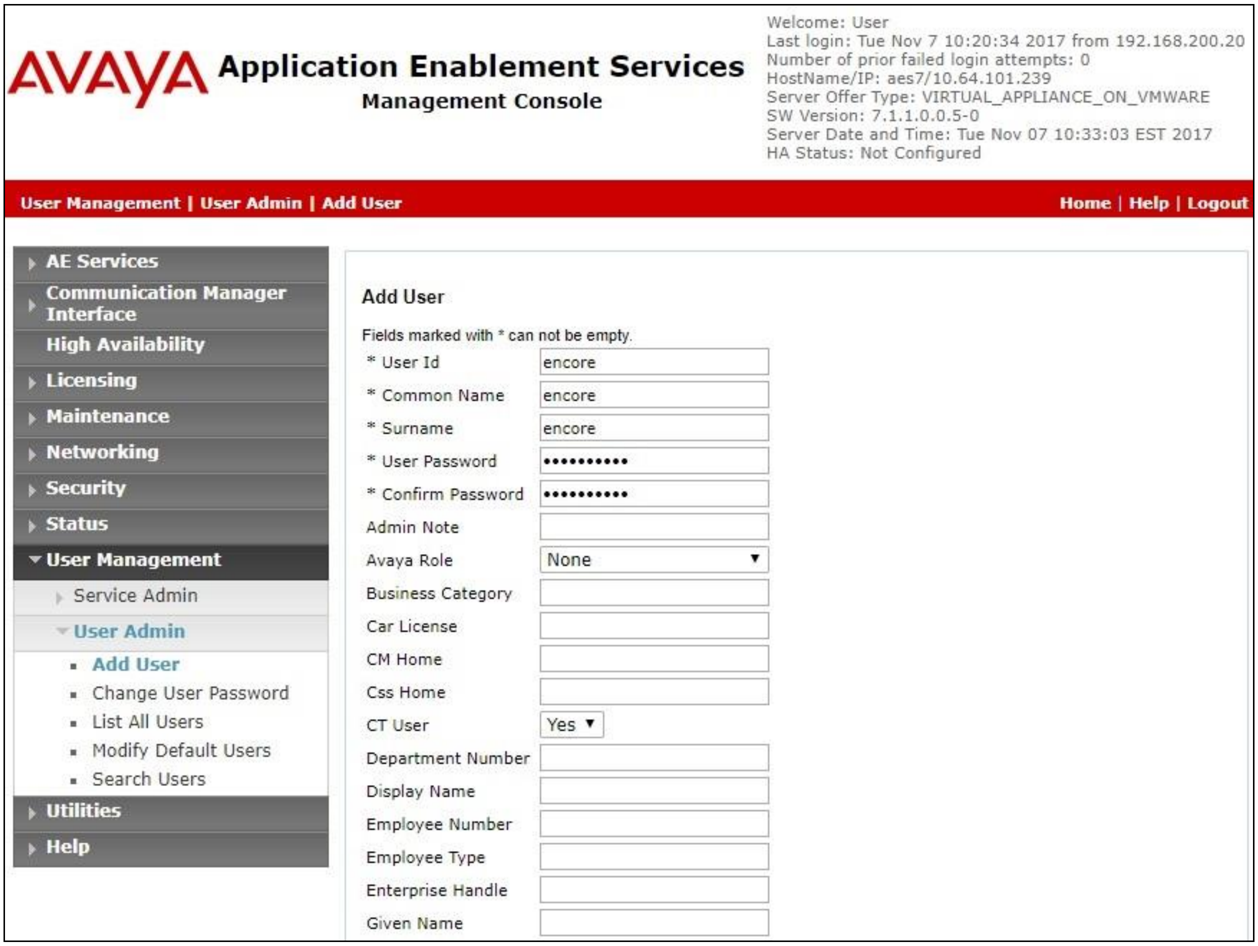
Edit H.323 Gatekeeper - cm7

Name or IP Address: 10.64.101.236

6.5. Administer Encore User

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

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



Welcome: User
Last login: Tue Nov 7 10:20:34 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 10:33:03 EST 2017
HA Status: Not Configured

Add User

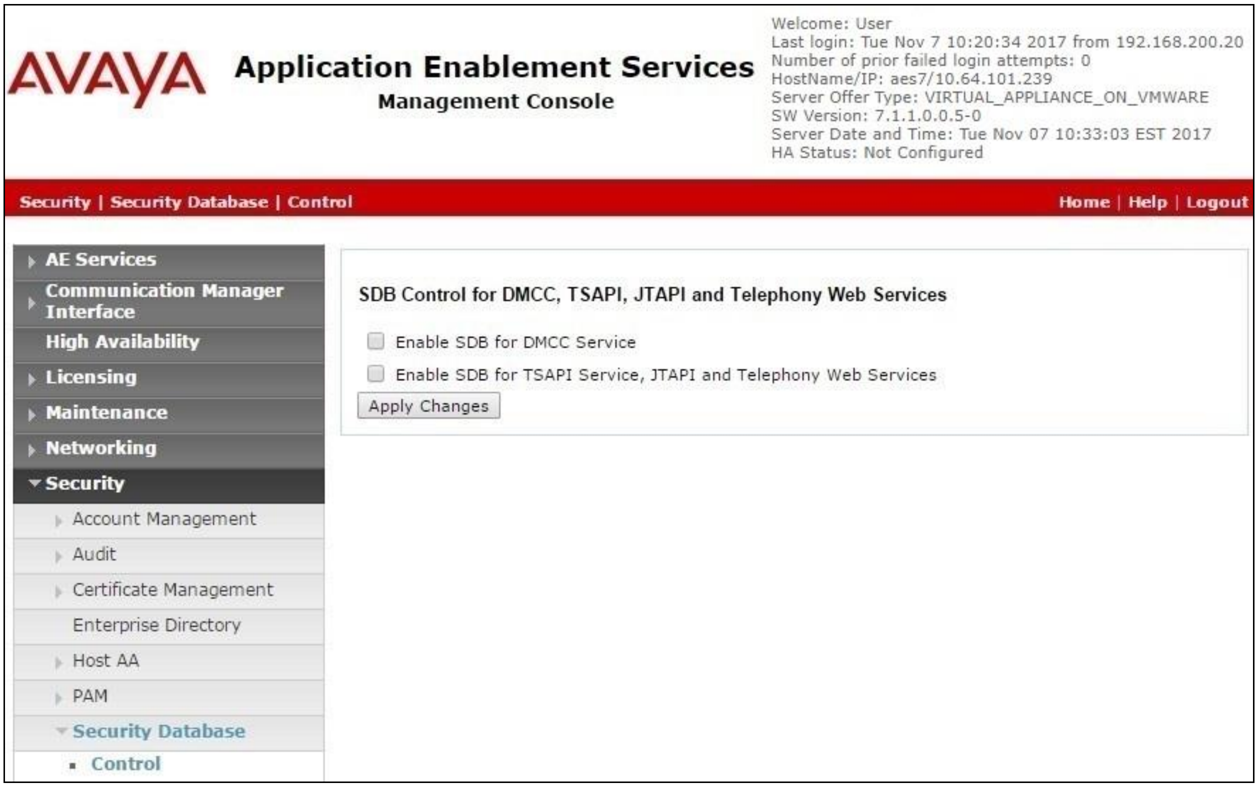
Fields marked with * can not be empty.

* 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	
Given Name	

6.6. Administer Security Database

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

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



Application Enablement Services
Management Console

Welcome: User
Last login: Tue Nov 7 10:20:34 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 10:33:03 EST 2017
HA Status: Not Configured

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

☐ Enable SDB for DMCC Service

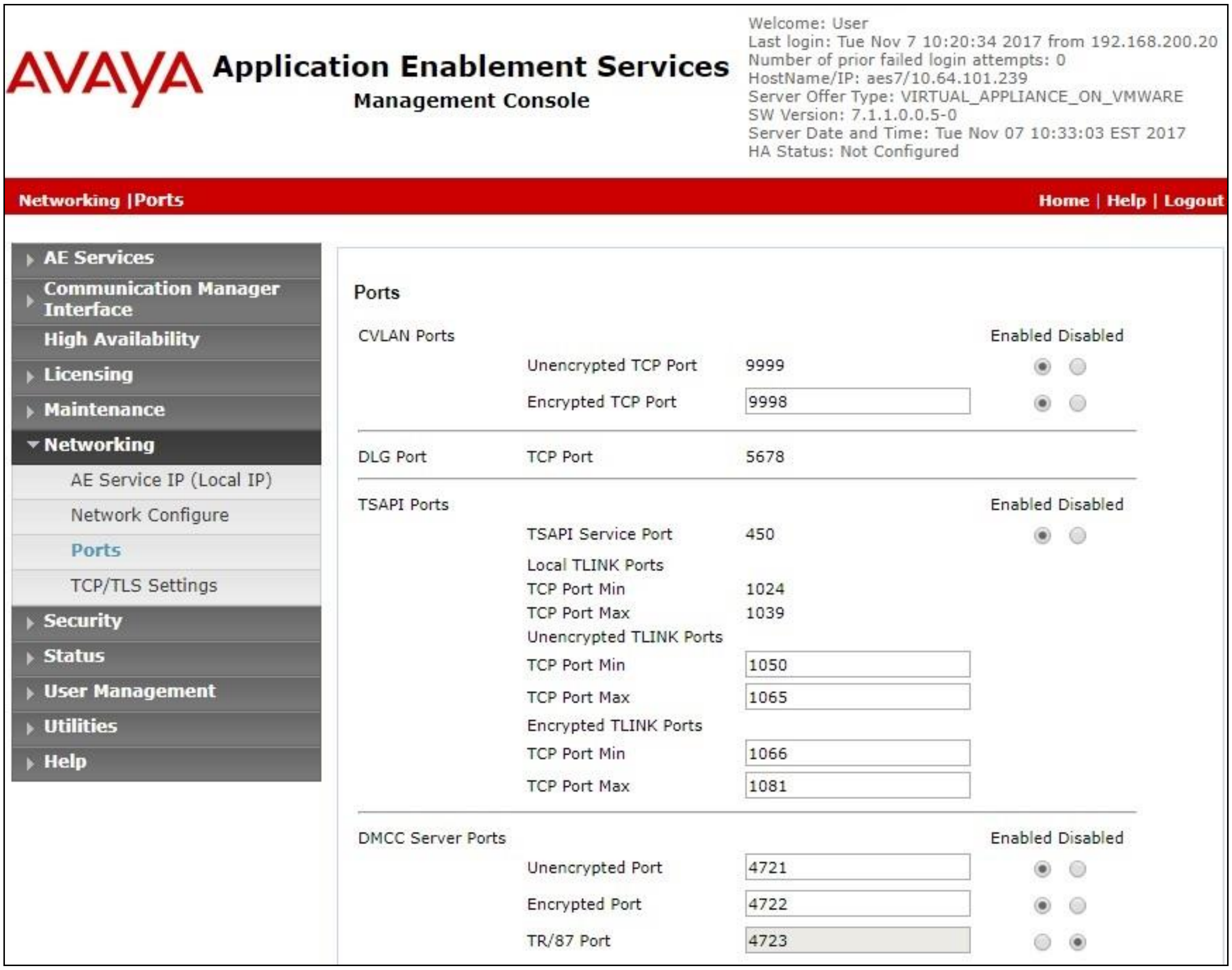
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

Apply Changes

6.7. Administer Ports

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

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



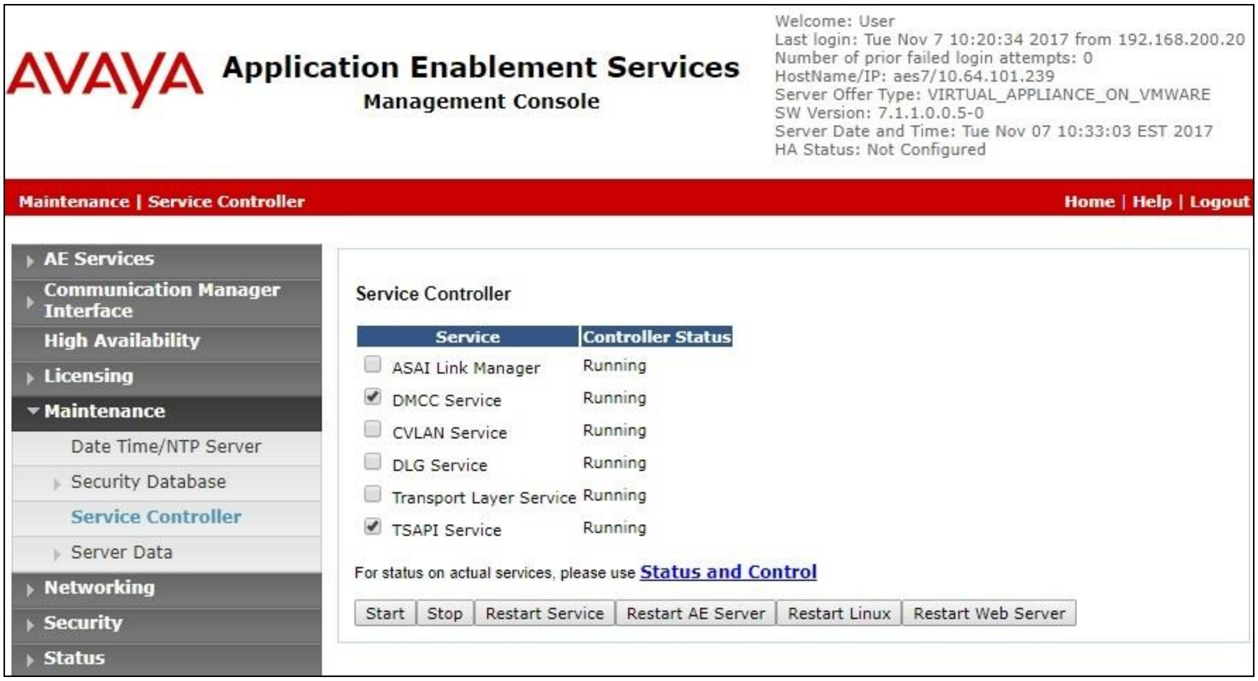
Welcome: User
Last login: Tue Nov 7 10:20:34 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 10:33:03 EST 2017
HA Status: Not Configured

Ports

			Enabled	Disabled
CVLAN Ports			Enabled	Disabled
	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	○	●

6.8. Restart Services

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



Welcome: User
Last login: Tue Nov 7 10:20:34 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 10:33:03 EST 2017
HA Status: Not Configured

Service Controller

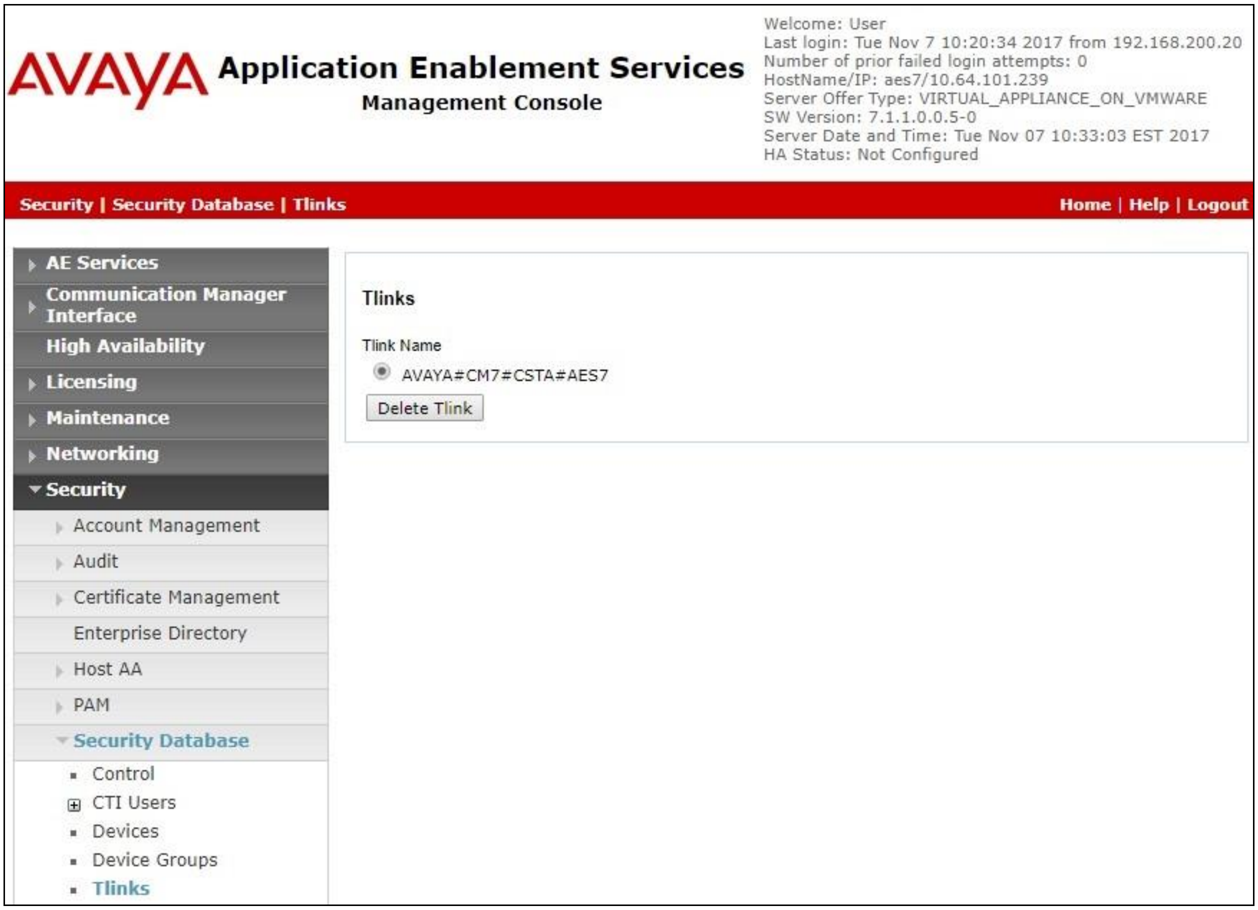
Service	Controller Status
☐ ASAI Link Manager	Running
☑ DMCC Service	Running
☐ CVLAN Service	Running
☐ DLG Service	Running
☐ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.9. Obtain Tlink Name

Select **Security → Security Database → Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Encore.

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



Welcome: User
Last login: Tue Nov 7 10:20:34 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 10:33:03 EST 2017
HA Status: Not Configured

Tlinks

Tlink Name

● AVAYA#CM7#CSTA#AES7

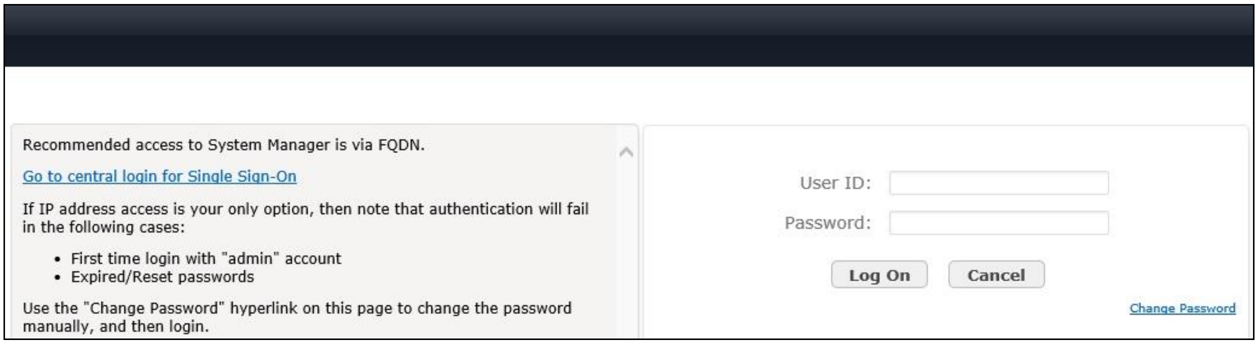
7. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer users

7.1. Launch System Manager

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



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

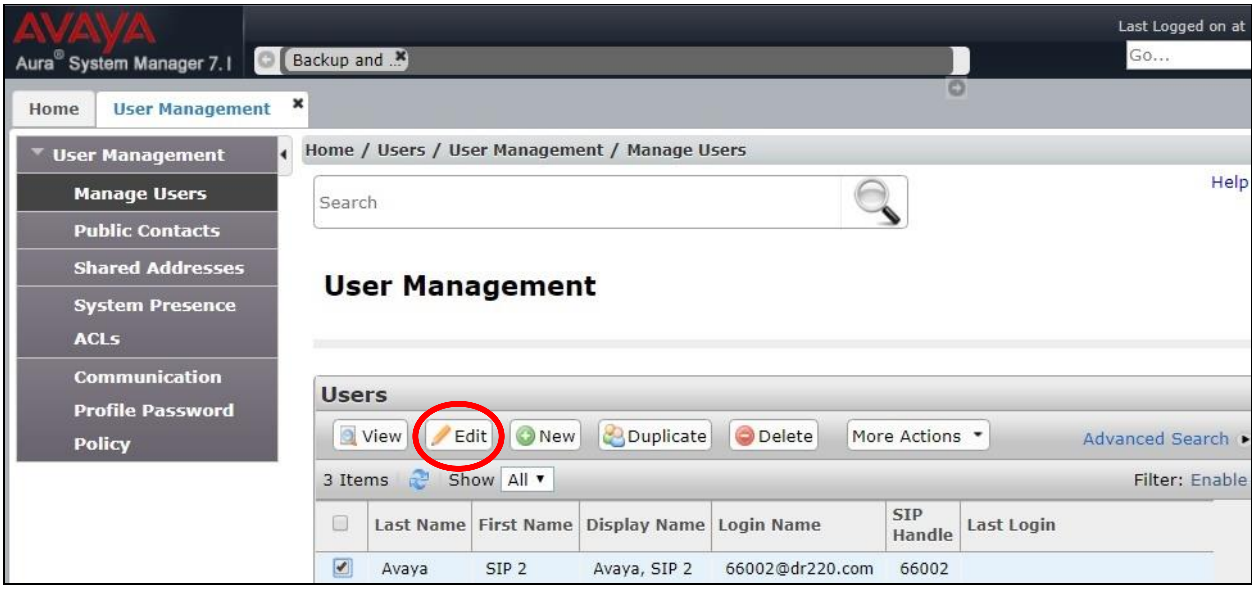
If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

7.2. Administer Users

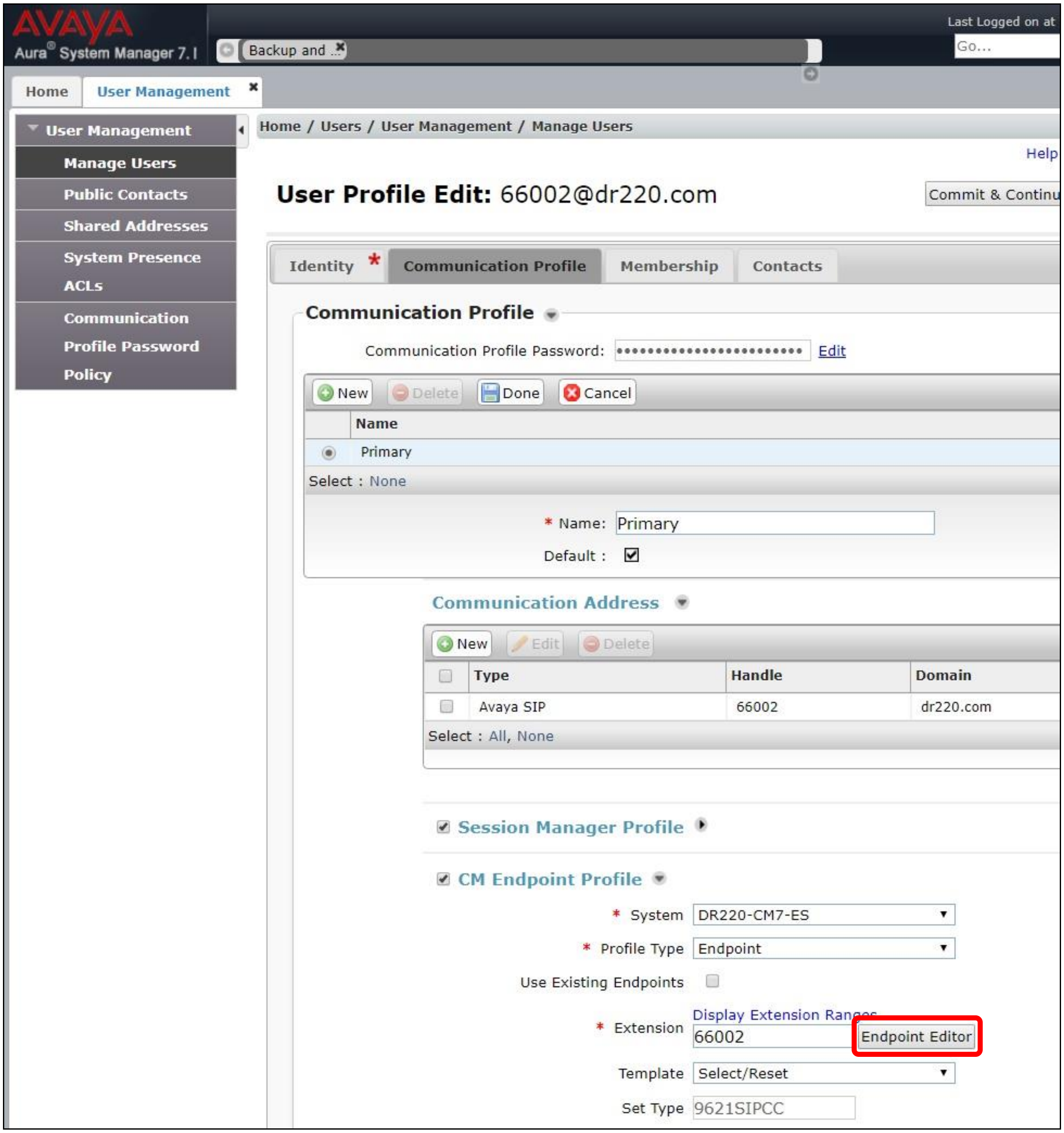
In the subsequent screen (not shown), select **Users → User Management**. Select **User Management → Manage Users** from the left pane to display the **User Management** screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case "66002", and click **Edit**.



☐	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
☑	Avaya	SIP 2	Avaya, SIP 2	66002@dr220.com	66002	

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

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



Home / Users / User Management / Manage Users

User Profile Edit: 66002@dr220.com

Communication Profile

Communication Profile Password: •••••••••••••••••••••••• Edit

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address

☐	Type	Handle	Domain
☐	Avaya SIP	66002	dr220.com

Select : All, None

☑ Session Manager Profile

☑ CM Endpoint Profile

* System DR220-CM7-ES

* Profile Type Endpoint

Use Existing Endpoints ☐

* Extension 66002

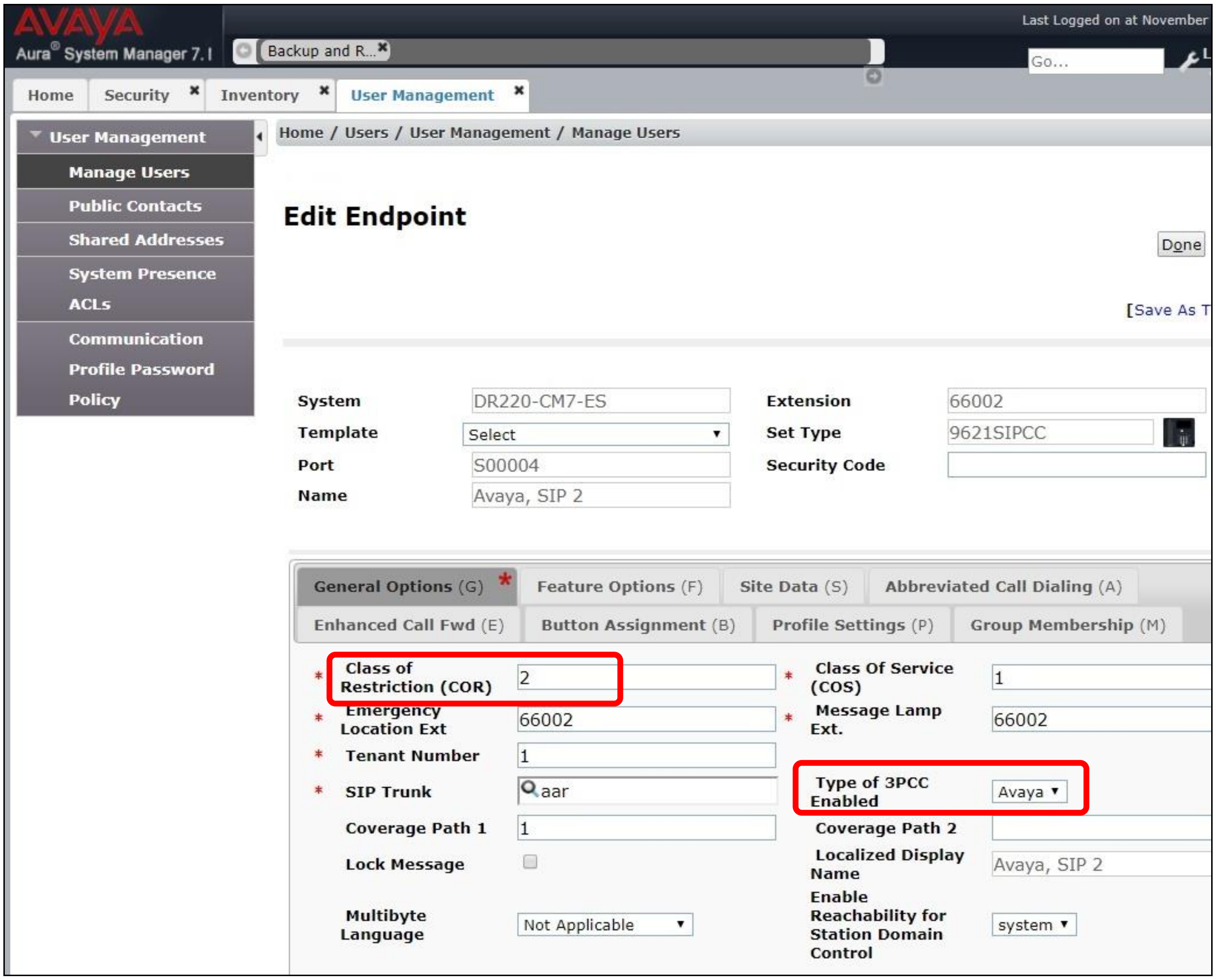
Template Select/Reset

Set Type 9621SIPCC

The **Edit Endpoint** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

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

Repeat this section for all SIP agent users.



Edit Endpoint

System	DR220-CM7-ES	Extension	66002
Template	Select	Set Type	9621SIPCC
Port	S00004	Security Code	
Name	Avaya, SIP 2		

* Class of Restriction (COR)	2	* Class Of Service (COS)	1
* Emergency Location Ext	66002	* Message Lamp Ext.	66002
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1	1	Coverage Path 2	
Lock Message	□	Localized Display Name	Avaya, SIP 2
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system

8. Configure dvsAnalytics Encore

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

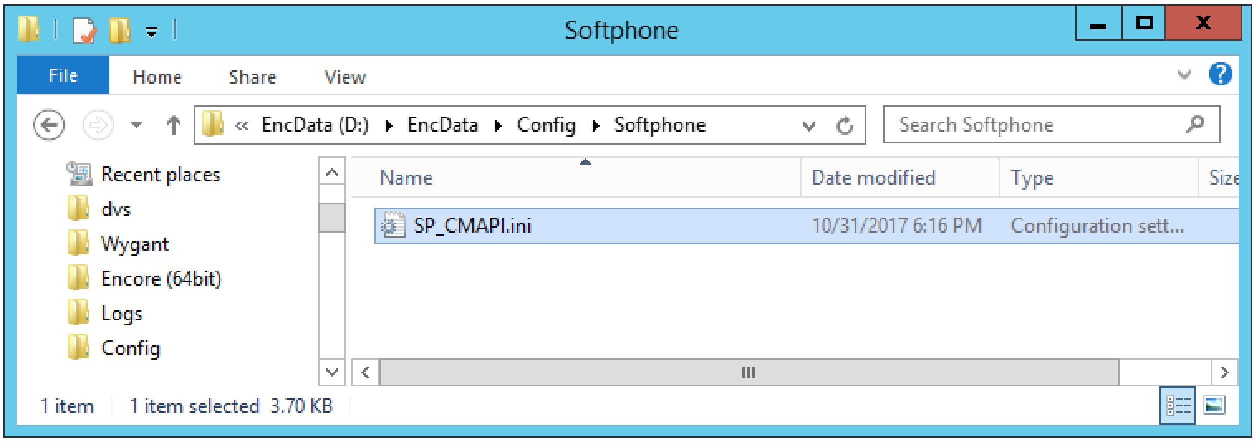
- Administer softphones
- Administer CTISetup
- Administer CT Gateway

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

Prior to configuration, the relevant Avaya TSAPI client is assumed to be installed on the Encore server, and that the TSAPI client has been configured with the IP address of the Application Enablement Services server as part of installation.

8.1. Administer Softphones

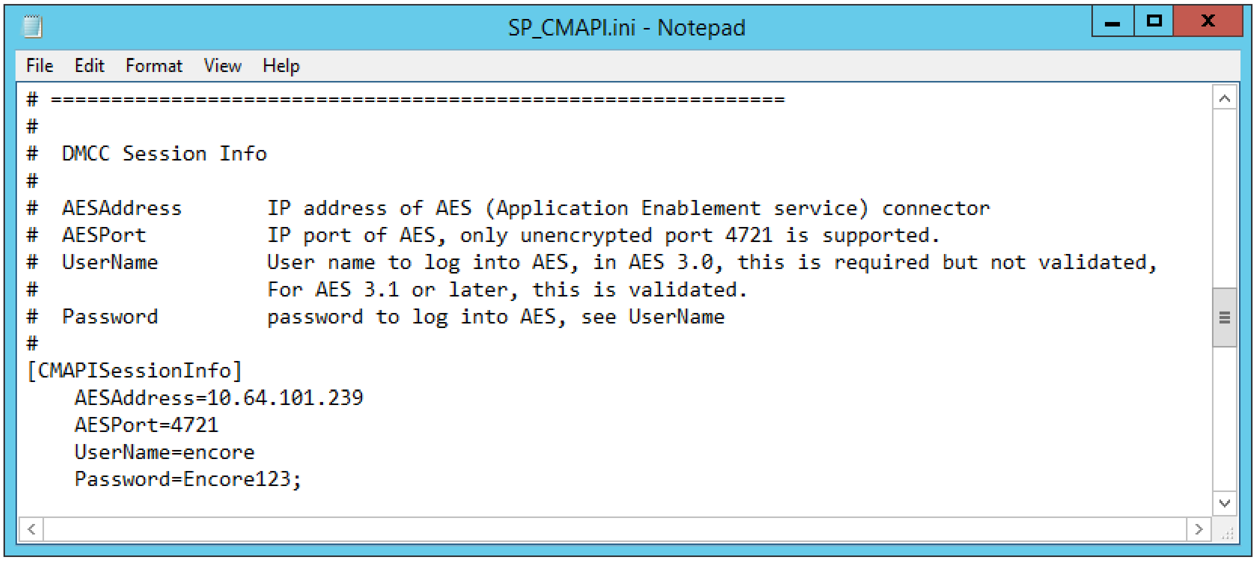
From the Encore server, navigate to the **D:\EncData\Config\Softphone** directory to edit the **SP_CMAPI.ini** file shown below.



Name	Date modified	Type	Size
SP_CMAPI.ini	10/31/2017 6:16 PM	Configuration sett...	

Scroll down to the **DMCC Session Info** sub-section. Under **CMAPISessionInfo**, enter the following values for the specified fields, and retain the default values for the remaining fields.

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

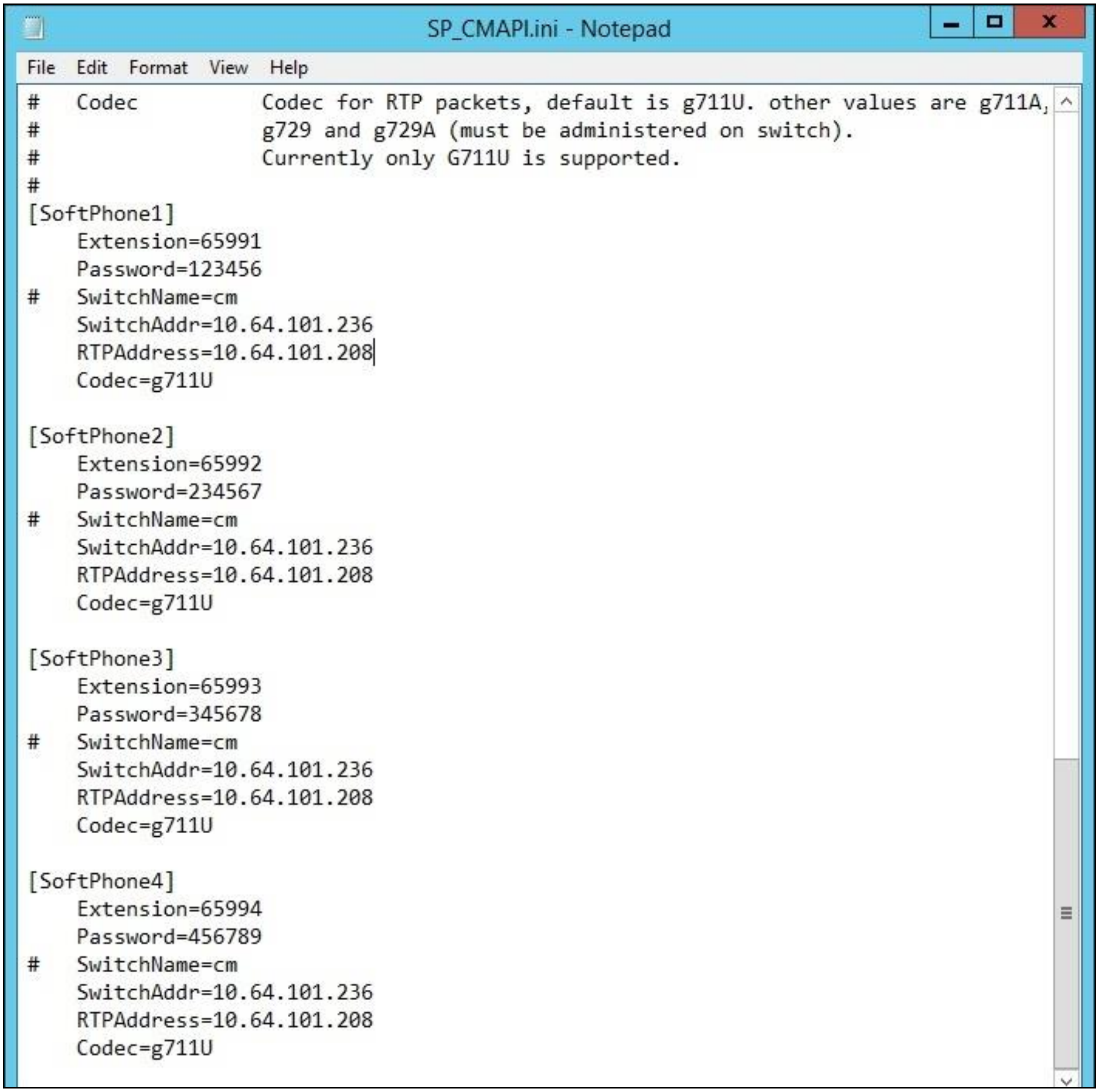


```
# ============================================================
#
#  DMCC Session Info
#
#  AESAddress       IP address of AES (Application Enablement service) connector
#  AESPort          IP port of AES, only unencrypted port 4721 is supported.
#  UserName         User name to log into AES, in AES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

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

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

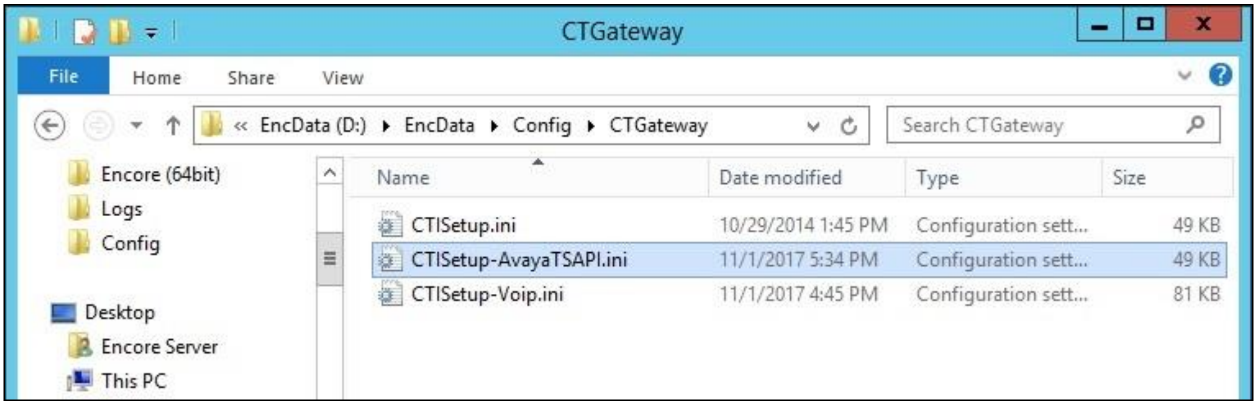
Create additional softphone entries as necessary. In the compliance testing, four softphones were configured to correspond to the four virtual IP softphones from **Section 5.7**.



```
#   Codec           Codec for RTP packets, default is g711U. other values are g711A,
#                   g729 and g729A (must be administered on switch).
#                   Currently only G711U is supported.
#
[SoftPhone1]
    Extension=65991
    Password=123456
#   SwitchName=cm
    SwitchAddr=10.64.101.236
    RTPAddress=10.64.101.208
    Codec=g711U

[SoftPhone2]
    Extension=65992
    Password=234567
#   SwitchName=cm
    SwitchAddr=10.64.101.236
    RTPAddress=10.64.101.208
    Codec=g711U

[SoftPhone3]
    Extension=65993
    Password=345678
#   SwitchName=cm
    SwitchAddr=10.64.101.236
    RTPAddress=10.64.101.208
    Codec=g711U

[SoftPhone4]
    Extension=65994
    Password=456789
#   SwitchName=cm
    SwitchAddr=10.64.101.236
    RTPAddress=10.64.101.208
    Codec=g711U
```

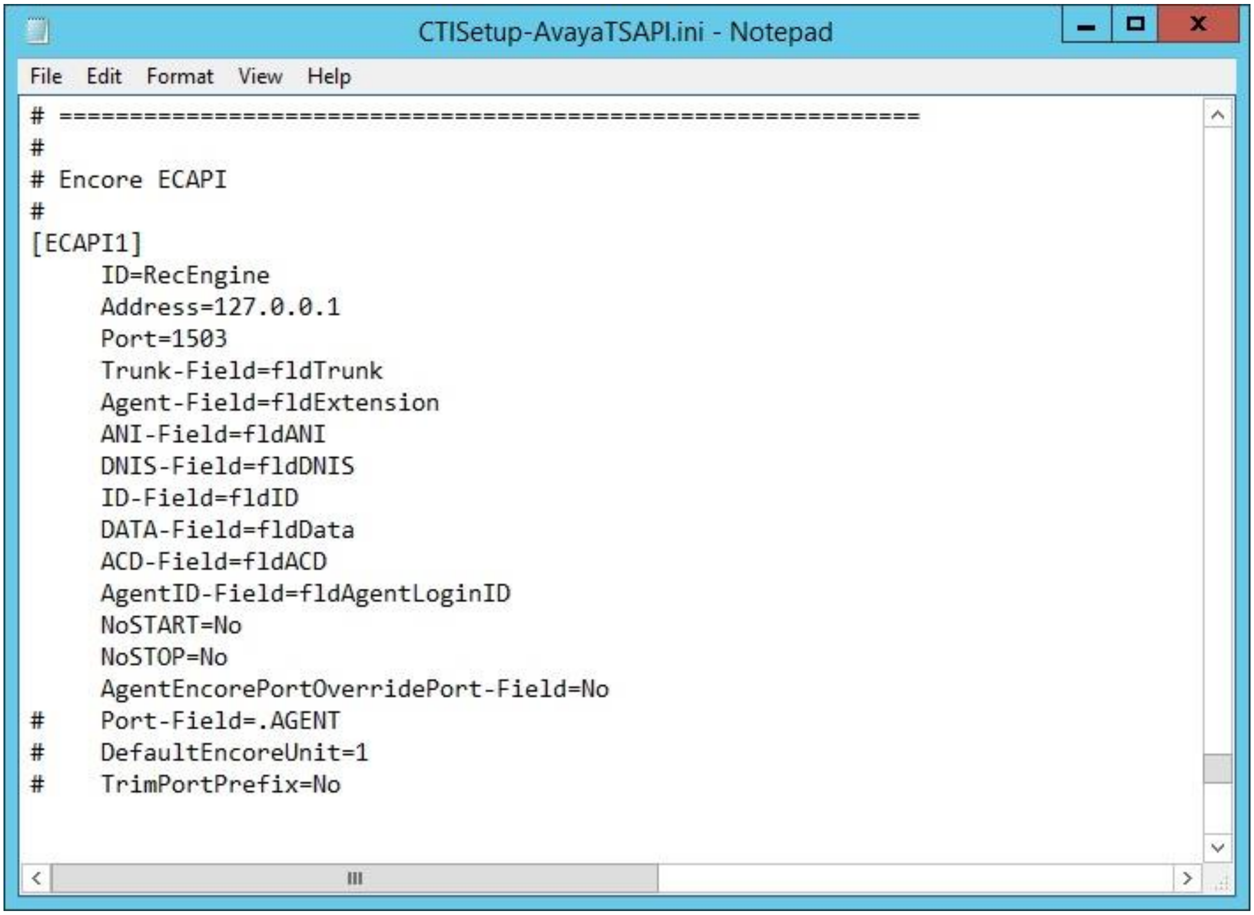
8.2. Administer CTISetup

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



Name	Date modified	Type	Size
CTISetup.ini	10/29/2014 1:45 PM	Configuration sett...	49 KB
CTISetup-AvayaTSAPI.ini	11/1/2017 5:34 PM	Configuration sett...	49 KB
CTISetup-Voip.ini	11/1/2017 4:45 PM	Configuration sett...	81 KB

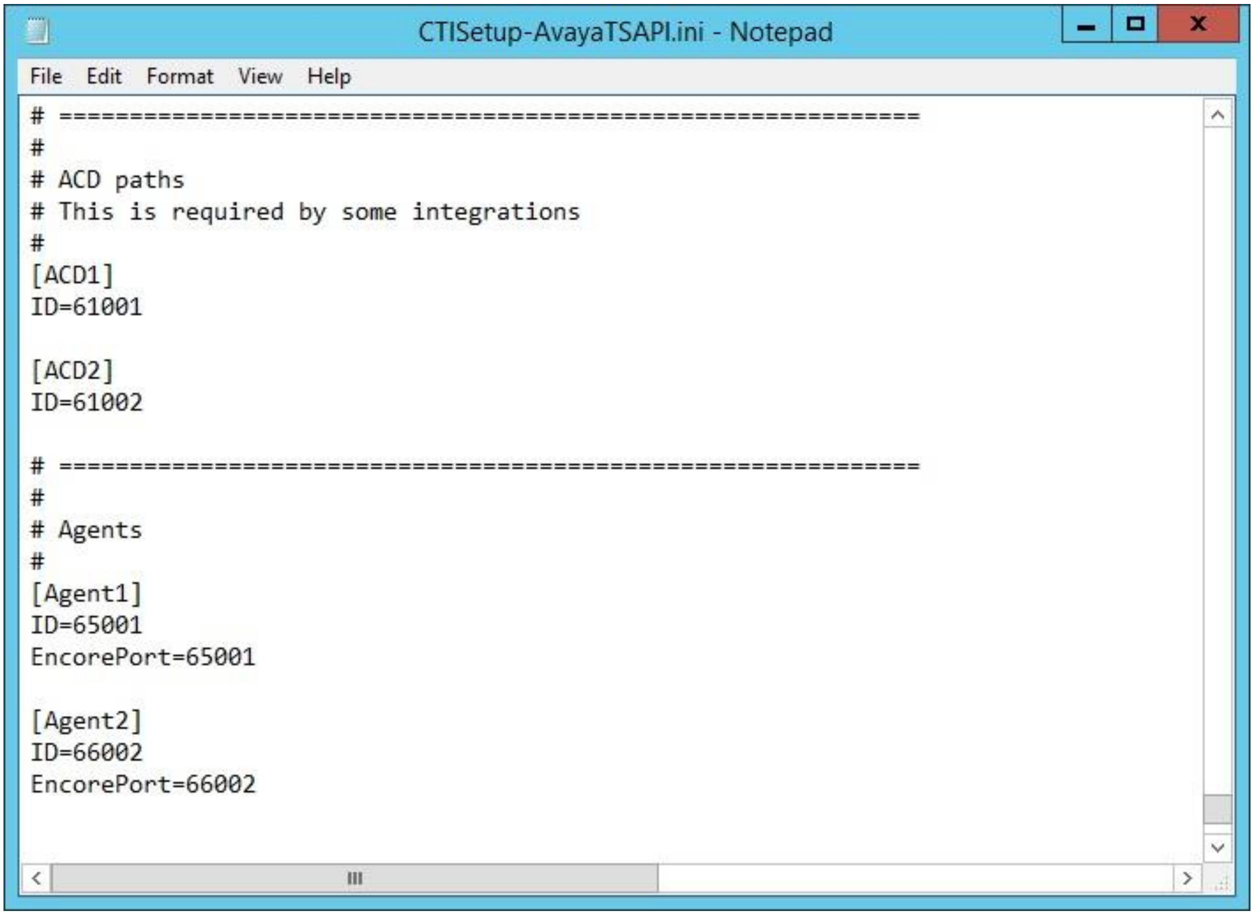
Scroll down to the **Encore ECAPI** sub-section. Under **ECAPI1**, make certain all parameters are set to the default values shown below.



```
# ============================================================
#
# 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 first skill group extension from **Section 3**. Create additional ACD entries as necessary when more than one skill group is being monitored. In the compliance testing, two ACD entries were created as shown below.

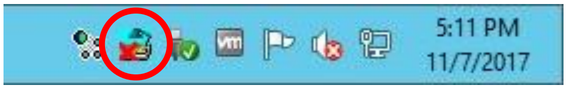
Scroll to the **Agents** sub-section. Under **Agent1**, set **ID** and **EncorePort** to the first agent station extension from **Section 3**. Create additional agent entries as necessary when more than one agent is being monitored. In the compliance testing, two agent entries were created as shown below.



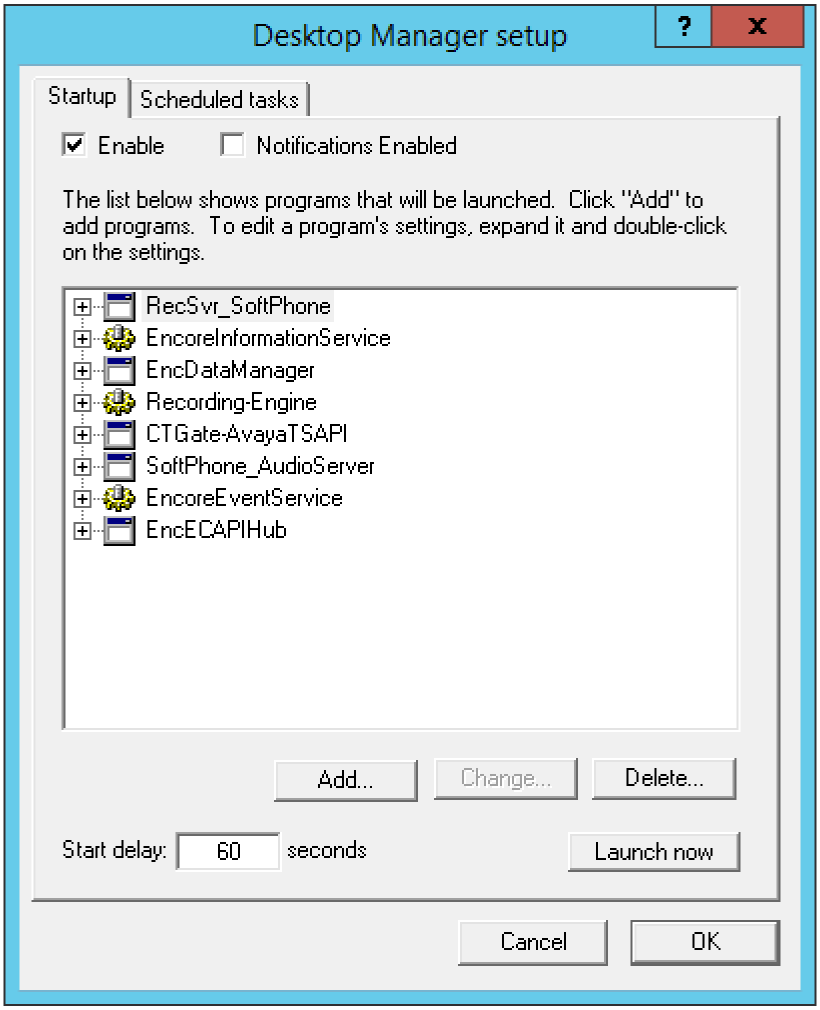
```
# =============================================================
#
# ACD paths
# This is required by some integrations
#
[ACD1]
ID=61001

[ACD2]
ID=61002

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

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

8.3. Administer CT Gateway

Right click on the **Desktop Manager** icon from the server system tray and select **Configure** (not shown).



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


Desktop Manager setup

Startup | Scheduled tasks

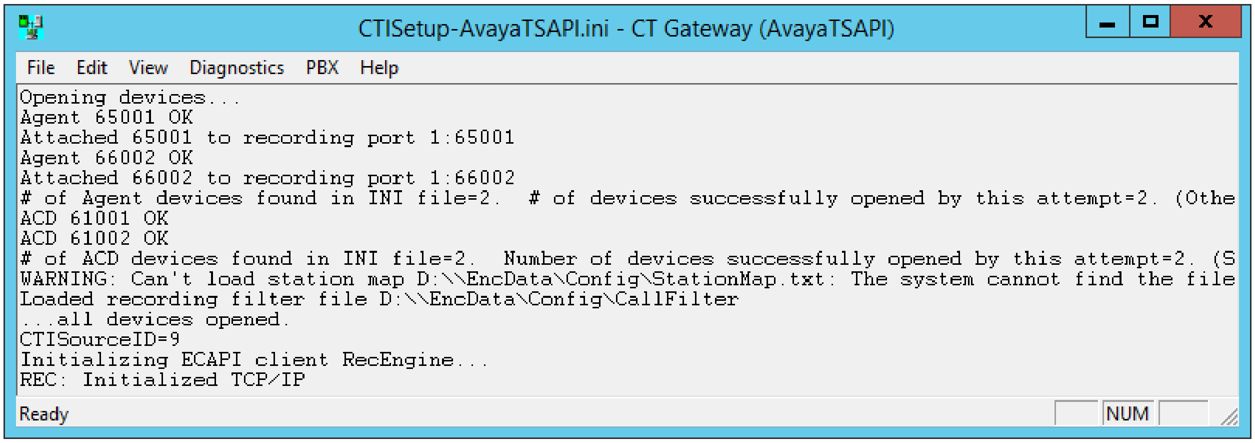
☑ Enable ☐ Notifications Enabled

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.

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

Start delay: 60 seconds

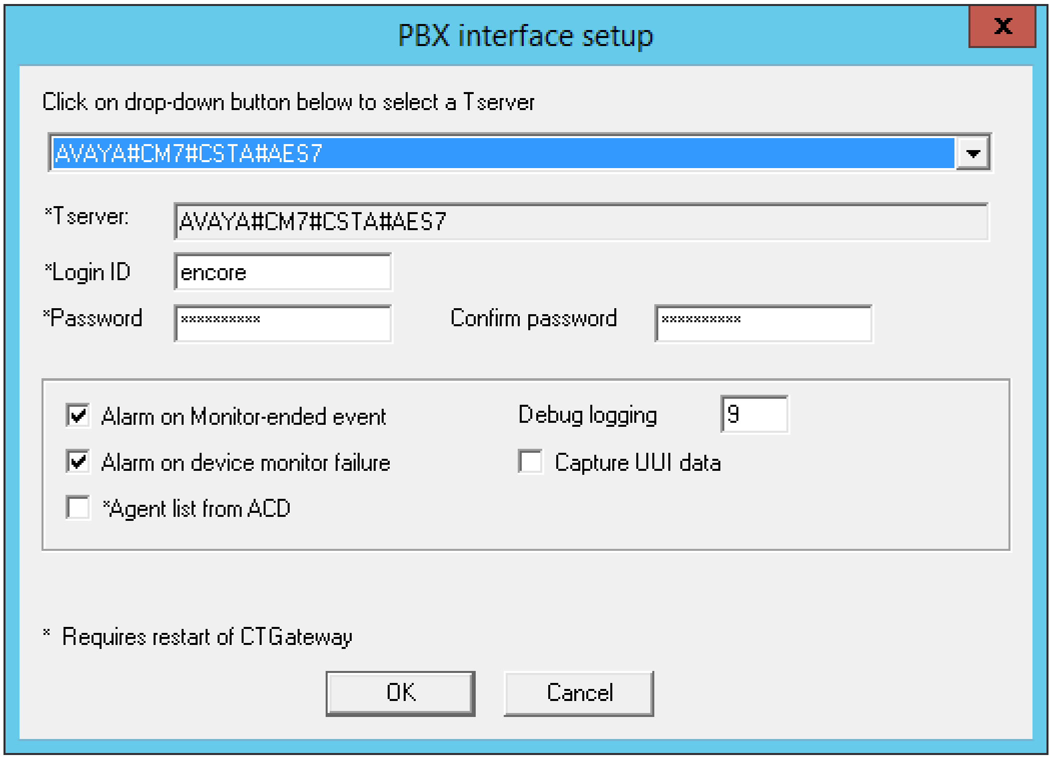
The **CTISetup-AvayaTSAPI.ini** screen is displayed. Select **PBX → Configure** from the top menu.


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

```
Opening devices...
Agent 65001 OK
Attached 65001 to recording port 1:65001
Agent 66002 OK
Attached 66002 to recording port 1:66002
# of Agent devices found in INI file=2.  # of devices successfully opened by this attempt=2. (Othe
ACD 61001 OK
ACD 61002 OK
# of ACD devices found in INI file=2.  Number of devices successfully opened by this attempt=2. (S
WARNING: Can't load station map D:\\EncData\Config\StationMap.txt: The system cannot find the file
Loaded recording filter file D:\\EncData\Config\CallFilter
...all devices opened.
CTISourceID=9
Initializing ECAPI client RecEngine...
REC: Initialized TCP/IP
```

The **PBX interface setup** screen is displayed next. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Tserver:** In the drop-down list above, select the Tlink name from **Section 6.9**.
- **Login ID:** The Encore user credentials from **Section 6.5**.
- **Password:** The Encore user credentials from **Section 6.5**.
- **Confirm Password:** The Encore user credentials from **Section 6.5**.
- **Debug logging:** Set to the desired level, in this case "9" for the highest level.



Click on drop-down button below to select a Tserver

AVAYA#CM7#CSTA#AES7

*Tserver: AVAYA#CM7#CSTA#AES7

*Login ID encore

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

☑ Alarm on Monitor-ended event

☑ Alarm on device monitor failure

☐ *Agent list from ACD

Debug logging 9

☐ Capture UUI data

* Requires restart of CTGateway

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     7        no    aes7             established   25       25
```

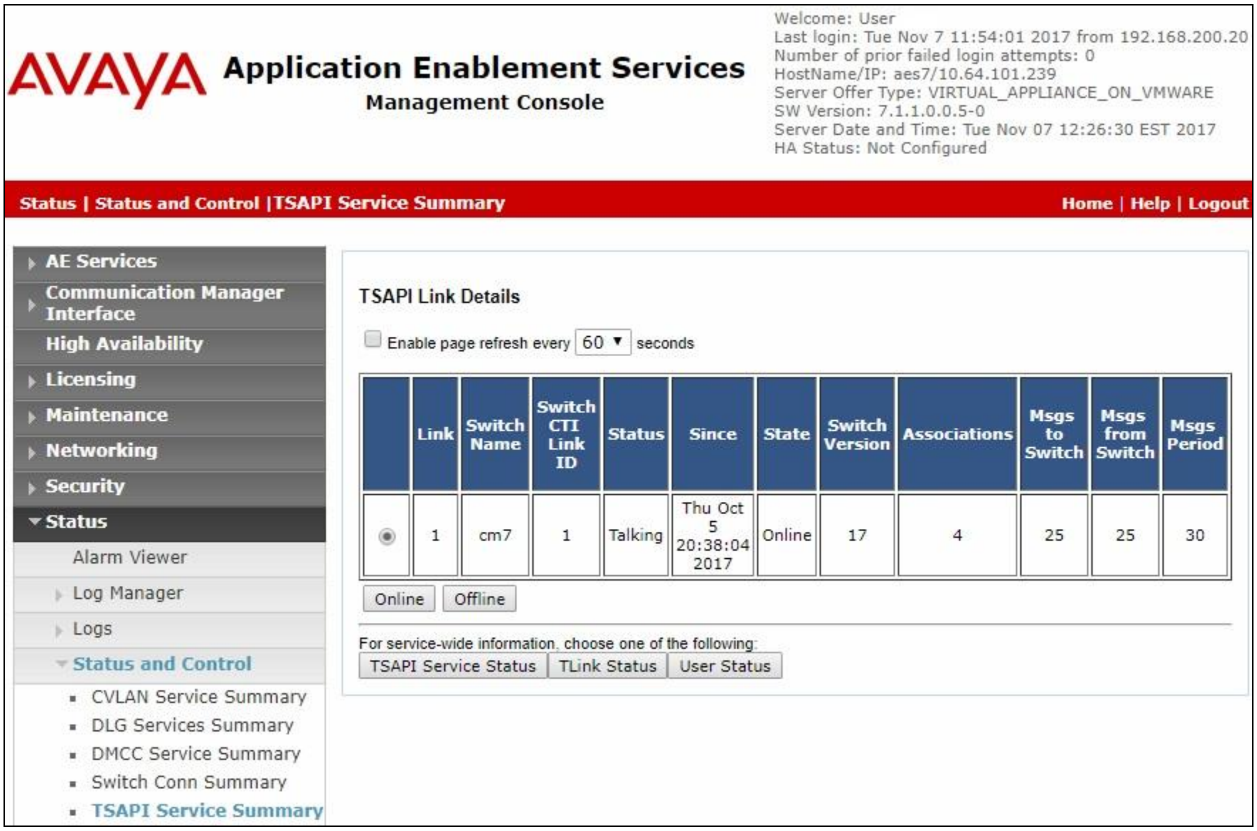
Verify registration status of the virtual IP softphones by using the "list registered-ip-stations" command. Verify that all virtual IP softphone from **Section 5.7** are displayed along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/       Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ------------------------------------
65000         9641      IP_Phone   tls 192.168.200.106
              1         6.6506         10.64.101.236
65001         9611      IP_Phone   tls 192.168.200.104
              1         6.6506         10.64.101.236
65991         4610      IP_API_A   tcp 10.64.101.239
              1         3.2040         10.64.101.236
65992         4610      IP_API_A   tcp 10.64.101.239
              1         3.2040         10.64.101.236
65993         4610      IP_API_A   tcp 10.64.101.239
              1         3.2040         10.64.101.236
65994         4610      IP_API_A   tcp 10.64.101.239
              1         3.2040         10.64.101.236
```

9.2. Verify Avaya Aura® Application Enablement Services

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

Verify the **Status** is "Talking" for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and agent stations from **Section 3**, in this case "4", as shown below.



Welcome: User
Last login: Tue Nov 7 11:54:01 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 12:26:30 EST 2017
HA Status: Not Configured

TSAPI Link Details

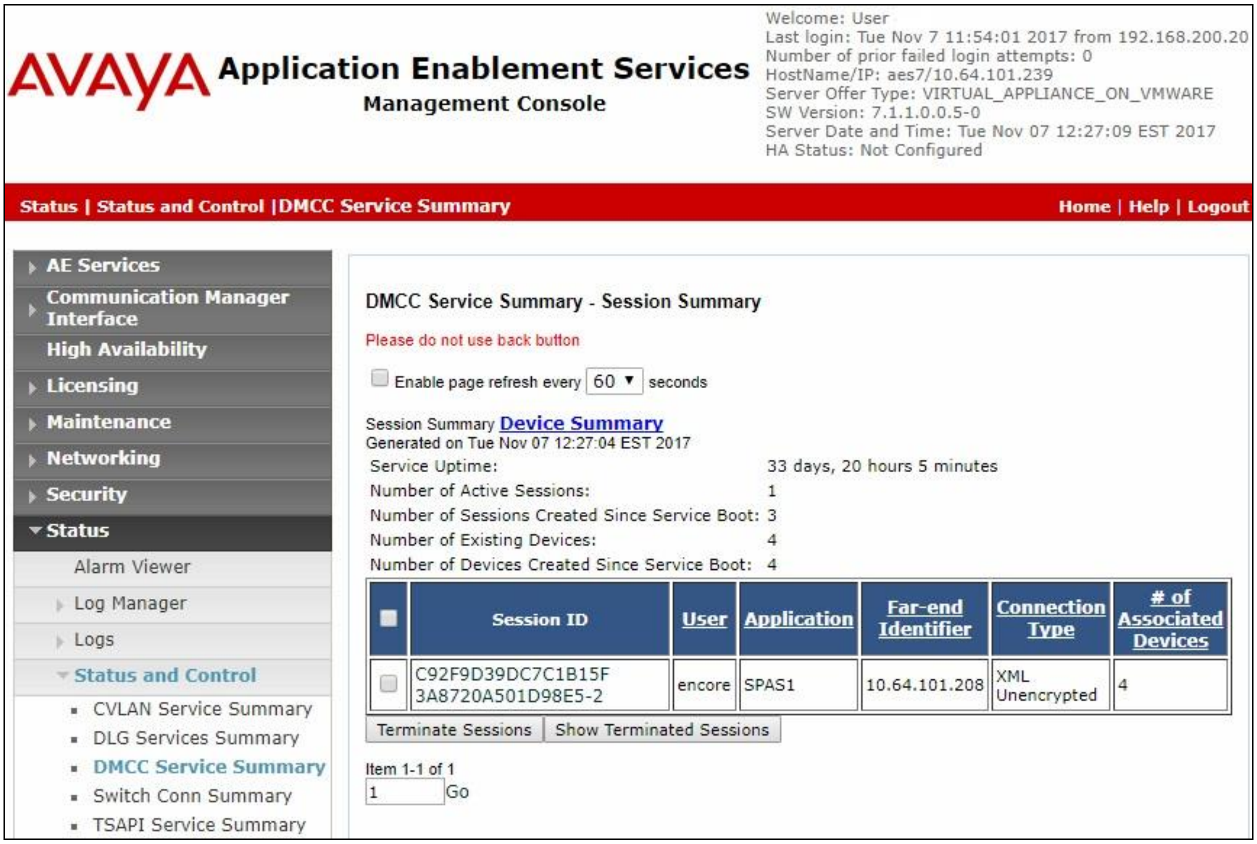
□ Enable page refresh every 60 ▾ seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm7	1	Talking	Thu Oct 5 20:38:04 2017	Online	17	4	25	25	30

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

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

Verify the **User** column shows an active session with the Encore user name from **Section 6.5**, and that the **# of Associated Devices** column reflects the number of configured softphones from **Section 8.1**, in this case "4".



Welcome: User
Last login: Tue Nov 7 11:54:01 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.1.0.0.5-0
Server Date and Time: Tue Nov 07 12:27:09 EST 2017
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 Tue Nov 07 12:27:04 EST 2017

Service Uptime:	33 days, 20 hours 5 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	3
Number of Existing Devices:	4
Number of Devices Created Since Service Boot:	4

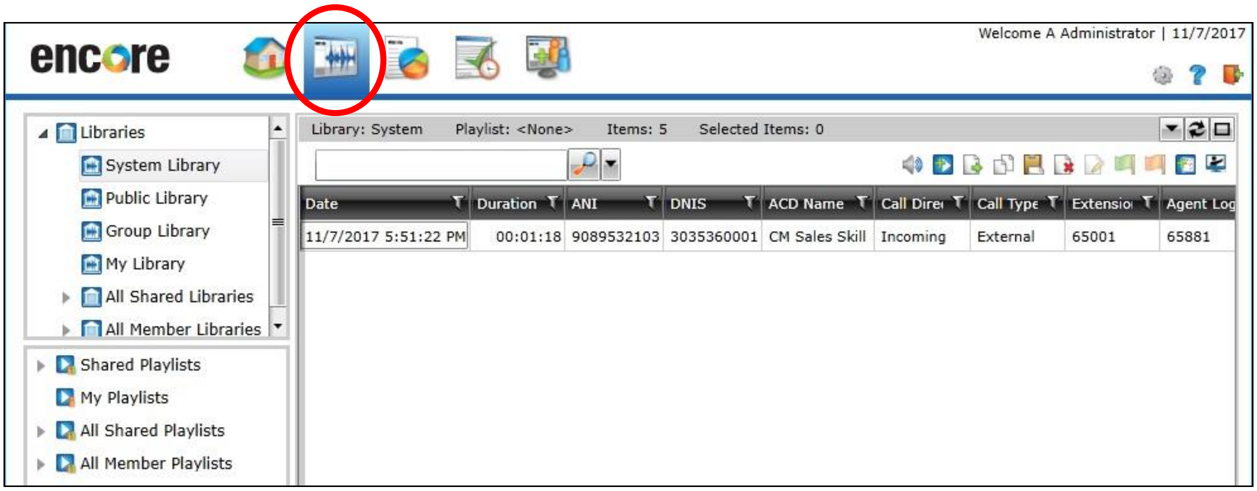
□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	C92F9D39DC7C1B15F 3A8720A501D98E5-2	encore	SPAS1	10.64.101.208	XML Unencrypted	4

Item 1-1 of 1
1 Go

9.3. Verify dvsAnalytics Encore

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

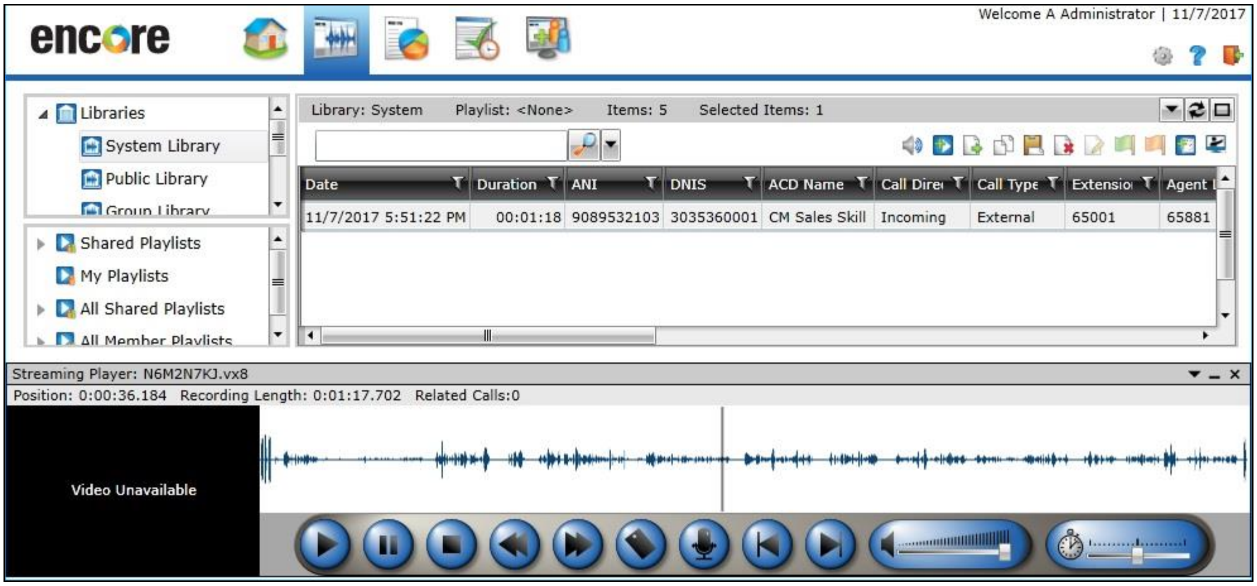
The **encore** screen is displayed. Select the **Recorded Contacts** icon from the top menu to display a list of call recordings. Verify that there is an entry in the right pane reflecting the last call, with proper values in the relevant fields.



Library: System   Playlist: <None>   Items: 5   Selected Items: 0

Date	Duration	ANI	DNIS	ACD Name	Call Dire	Call Type	Extensio	Agent Log
11/7/2017 5:51:22 PM	00:01:18	9089532103	3035360001	CM Sales Skill	Incoming	External	65001	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: 5 Selected Items: 1

Date	Duration	ANI	DNIS	ACD Name	Call Dire	Call Type	Extensio	Agent I
11/7/2017 5:51:22 PM	00:01:18	9089532103	3035360001	CM Sales Skill	Incoming	External	65001	65881

Streaming Player: N6M2N7KJ.vx8

Position: 0:00:36.184 Recording Length: 0:01:17.702 Related Calls:0

10. Conclusion

These Application Notes describe the configuration steps required for dvsAnalytics Encore 6.0.6 to successfully interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 using Service Observing. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 7.1.1, Issue 2, August 2017, available at http://support.avaya.com.

2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.1.1, Issue 3, September 2017, available at http://support.avaya.com.

3. *Avaya Aura^{TM} Communication Manager TSAPI Integration Guide*, Encore Version 6.0.6 or later, October 25, 2017, available from dvsAnalytics Support.

4. *Avaya Aura^{TM} Communication Manager TSAPI Installation Addendum*, Includes Version 6.0.6 or later, System Version 2.3.7, November 2, 2017, 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.