Avaya Solution & Interoperability Test Lab

Application Notes for Coordinated Systems, Inc. Virtual Observer Call Recording and Quality Monitoring System 5.1with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3 – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Coordinated Systems Inc. Virtual Observer call recording solution with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Service. Virtual Observer is a software-only solution for voice call recording that offers various recording without the use of physical connections to servers other than standard network connections. The recordings can be played back for validation and voice quality evaluation purposes.

The Virtual Observer system interfaces with Communication Manager and Application Enablement Services (AES) using the Telephony Service Application Programing Interface (TSAPI) to obtain call event information and the Device, Media & Call Control Application Programing Interface (DMCC API) to obtain audio.

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 a compliance-tested configuration comprised of an Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Coordinated Systems Inc. Virtual Observer. The Virtual Observer application monitors, records, stores, and plays back phone calls for verification.

Virtual Observer uses the TSAPI interface of AES to monitor extensions to obtain call events. Virtual Observer also uses the DMCC interface to optionally register DMCC softphones with Avaya Communication Manager. The DMCC softphones are used as recording devices for either service observe or single step conference. When a call is to be recorded, Virtual Observer uses either Dual Registration or Single Step Conferencing or Service Observe to optionally add a DMCC softphone into the call and obtain the audio.

Once registration is successfully completed, Avaya Aura® Communication Manager will send call events for all calls that originate or terminate on the registered stations, and permit virtual extensions to be optionally added to these calls when requested using Service Observe or Single Step Conference. When using Dual Registration, virtual extensions are not required as media, is simply forked to the recording server.

2. General Test Approach and Test Results

The Compliance testing focused on the following areas, covered in the DevConnect Test Plan for Communication Manager, Application Enablement Services and Virtual Observer:

Phase 1 Installation & Configuration
Phase 2 Virtual Observer/Avaya Feature Functionality Verification
Phase 3 Failover and Serviceability Tests

The installation and configuration testing focused on the setup of all components and the ability to interoperate. The functionality testing focused on verifying Virtual Observer's ability to detect, record, and search calls, while recording and storing recordings appropriately with basic telephony features. The serviceability testing focused on verifying the ability of Virtual Observer to recover from adverse conditions.

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

All feature functionality test cases were performed manually to verify proper operation. The following scenarios were tested using the test configuration diagram shown in Figure 1.

The installation test cases were covered with the setup of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and Virtual Observer.

The functionality test cases were performed manually. The general test approach will be to verify that Virtual Observer can monitor analog, digital, and IP telephones (stations), IP Softphones, and agents through computer telephony integration (CTI) link and record calls using either DMCC softphones as the recording ports, or native media via multiple registrations. Virtual Observer uses Dual Registration, Single-Step Conferencing or Service Observing to conference a DMCC station into a call, thereby receiving a copy of the media stream of the call, or native media via multiple registrations. Calls will be placed from and directly to stations (telephones) and agents, and indirectly to agents via a Vector Directory Number (VDN). Calls placed to the VDN will be queued to a skill group, which in turn will deliver the calls to agents that are logged into the skill group. The recordings will be played back for validation and voice quality evaluation purposes.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to the Virtual Observer server at different intervals, powering down Avaya Aura® Communication Manager, powering down the Avaya Aura® Application Enablement Services server, and also by stopping the services on Avaya Aura® Application Enablement Services.

The verification of tests included manually listening to recordings from the web, checking the timestamps and data of the recordings.

2.2. Test Results

All test cases was executed and verified. No errors were detected.

2.3. Support

Technical support on Virtual Observer can be obtained through the following:

- **Phone:** **860-289-2151**
- **Web:** **http://www.csiworld.com**
- **Email:** **support@csiworld.com**

3. Reference Configuration

Virtual Observer can be configured on a single Windows Server, or distributed across multiple servers for larger scale deployments. The compliance test configuration used a single server configuration.

In the compliance testing, the Virtual Observer solution was configured to monitor four physical station extensions on Avaya Aura® Communication Manager.

The interoperability of Virtual Observer with Avaya Aura® Communication Manager is accomplished through Avaya Aura® Application Enablement Services. The compliance test configuration used to test Virtual Observer included the Avaya S8300D Server, the Avaya G450 Media Gateway, Avaya Aura® Application Enablement Services, Windows 2012 Server, soft clients, analog, digital and IP telephones. **Figure 1** provides a high level topology.

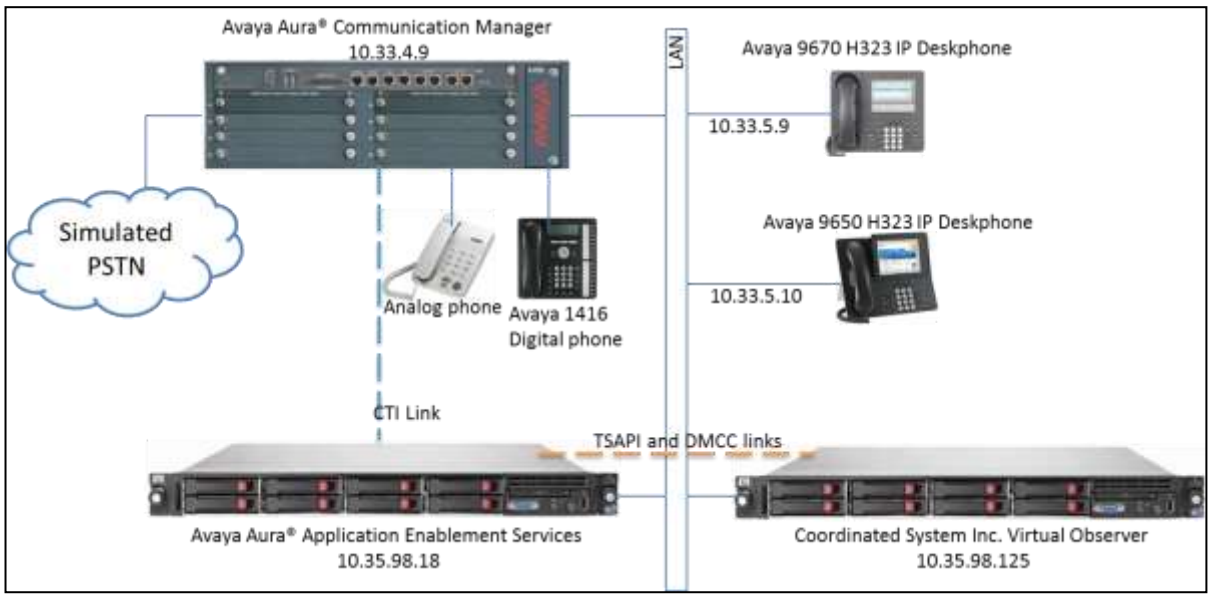


Figure 1: CSI Virtual Observer Compliance Test Sample Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya S8300 Server (w/ G450)	6.3.10
Avaya G450 Media Gateway : MM710BP (DS1) MM712AP (DCP)	 HW11, FW044 HW07, FW009
Avaya Application Enablement Services (AES) Server	6.3.3.0.10
Avaya 1416 Digital Phones :	Rel 38 SW Vintage 07
Avaya 9600 Series IP Phones: 9670 (H.323) 9650 (H323)	 3.230A 3.230A
Avaya Analog Phones	-
Virtual Observer	5.1

5. Configure Avaya Aura® Communication Manager

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

All the configuration changes in this section for Avaya Aura® Communication Manager are performed through the System Access Terminal (SAT) interface. For more information on configuring Avaya Aura® Communication Manager, refer to the Avaya product documentation, Reference [10].

This section provides the procedures for configuring Avaya Aura® Communication Manager. The procedures fall into the following areas:

- Verify Feature and License are adequate for the integration
- Administer Processor Ethernet Interface for Avaya Aura® Application Enablement Services connectivity
- Administer Avaya Aura® Communication Manager Network Regions
- Administer Computer Telephony Integration (CTI) Link
- Administer Virtual Stations

The detailed administration of contact center entities, such as VDN, Skill, Logical Agents and Station Extensions are assumed to be in place and are not covered in these Application Notes.

5.1. Verify Feature and License are adequate for the integration

Applications that use Application Enablement Services TSAPI must have **Computer Telephony Adjunct Links** enabled on Communication Manager. This feature entitlement is provided with each TSAPI license. TSAPI entitlements must be activated in both Application Enablement Services and Communication Manager licenses. If this option is not set to "**y**", 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? n                      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
                               ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

In addition, the Virtual Observer solution requires available **Maximum Stations** licenses for each recording port/virtual station and either an **IP_API_A** registration license on Communication Manager, and/or **DMCC_DMC** licenses on Application Enablement Services, see the section**6.3** for more details.

```
display system-parameters customer-options                      Page   1 of  11
                                OPTIONAL FEATURES

     G3 Version: V16                            Software Package: Enterprise
       Location: 2                               System ID (SID): 1
       Platform: 28                              Module ID (MID): 1

                                                          USED
                                Platform Maximum Ports: 6400  115
                                      Maximum Stations: 2400  32
                             Maximum XMOBILE Stations: 2400  0
                     Maximum Off-PBX Telephones - EC500: 9600  2
                     Maximum Off-PBX Telephones -   OPS: 9600  0
                     Maximum Off-PBX Telephones - PBFMC: 9600  0
                     Maximum Off-PBX Telephones - PVFMC: 9600  0
                     Maximum Off-PBX Telephones - SCCAN: 0     0
                          Maximum Survivable Processors: 313   1




        (NOTE: You must logoff & login to effect the permission changes.)
display system-parameters customer-options                      Page  10 of  11
                      MAXIMUM IP REGISTRATIONS BY PRODUCT ID
```

```
Product ID  Rel. Limit          Used
AgentSC        : 2400           0
IP_API_A       : 2400           0
IP_Agent       : 2400           0
IP_NonAgt      : 2400           0
IP_Phone       : 2400           4
IP_ROMax       : 2400           0
IP_Soft        : 2400           0
IP_Supv        : 2400           0
IP_eCons       : 68             0
oneX_Comm      : 2400           0
               : 0              0
               : 0              0
               : 0              0
               : 0              0
               : 0              0


        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer Processor Ethernet Interface for Application Enablement Services Connectivity

Enter the change node-names ip command. The Application Enablement Services and procr node-names need to be defined here.

```
change node-names ip                                            Page   1 of   2
                                   IP NODE NAMES
    Name              IP Address
aes63               10.35.98.18
default             0.0.0.0
procr               10.33.4.9
procr6              ::
```

On most R6 or later servers, the Processor Ethernet Interface will already be administered in the ip-interface list. The **display ip-interface procr** command will display the parameters of the Processor Ethernet Interface.

```
display ip-interface procr                                      Page   1 of   2
                                   IP INTERFACES

                  Type: PROCR
                                                     Target socket load: 4800

      Enable Interface? y                          Allow H.323 Endpoints? y
                                                    Allow H.248 Gateways? y
        Network Region: 1                            Gatekeeper Priority: 5

                                  IPV4 PARAMETERS
             Node Name: procr                     IP Address: 10.33.4.9

           Subnet Mask: /24

display ip-interface procr                                      Page   2 of   2
```

```
                                IP INTERFACES

                Speed: 100Mbps
               Duplex: Full

                              IPV6 PARAMETERS
            Node Name: procr6
           IP Address: ::

          Subnet Mask: /64
     Enable Interface? n
```

Add an entry for Application Enablement Services as described below:

- Enter the **change ip-services** command.
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.
- Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration [Reference 2].

```
change ip-services                                          Page   1 of   4

                                  IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      procr            8765
CDR1                 procr            0       MTS             9000
CDR2                 procr            0       RDTT            9001
```

On Page 4 of the form, enter the following values:

- In the **AE Services Server** field, type the name obtained from the Application Enablement Services server.
- In the **Password** field, enter the password administered on the Application Enablement Services server.
- In the **Enabled** field, type **y**.

```
change ip-services                                          Page   4 of   4
                           AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      aes63               *                     y        in use
```

Note that the name and password entered for the **AE Services Server** and **Password** fields must match the name and password on the Application Enablement Services server. The administered name for the Application Enablement Services server is created as part of the Application Enablement Services installation, and can be obtained from the Application Enablement Services server by typing **uname –n** at the Linux command prompt.

5.3. Administer Communication Manager Network Regions

Common to DMCC recording solutions and standard endpoint administration, Virtual Observer requires that the H.323 registration CLAN(s) be located in a Network Region with adequate media processing resources, and that the Codec be common for all of the recording virtual stations (either G.711 or G.729).

In this configuration, procr and all endpoints, including the recorder's virtual stations were configured in a common Network Region.

5.4. Administer Computer Telephony Integration (CTI) Link

This section provides the steps required for configuring a CTI Link.

Enter the **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

- In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

```
add cti-link 5                                                  Page   1 of   3
                                    CTI LINK
 CTI Link: 5
Extension: 52997
     Type: ADJ-IP
                                                                     COR: 1
     Name: devaes63
```

```
add cti-link 5                                                  Page   2 of   3
                                    CTI LINK
FEATURE OPTIONS
      Event Minimization? n        Special Character for Restricted Number? n
      IC Adjunct Routing? n   Send Disconnect Event for Bridged Appearance? n
                                      Two-Digit Aux Work Reason Codes? n
                                          Block CMS Move Agent Events? n
```

```
add cti-link 5                                                  Page   3 of   3
                                    CTI LINK
Bridged Appearance Origination Restriction? n

            SAC/CF Override: n
```

5.5. Administer Virtual Stations

All of the stations that will be used by the recorder must be **4620** set type, **IP Softphone** and **Speakerphone** enabled, and the application needs to know the **Security Code** for each station in order to successfully register. This softphone will be used later in **Section 7.1** and called as DMCC phone.

```
add station 52158                                                Page   1 of   4
                                     STATION

Extension: 52158                        Lock Messages? n               BCC: 0
     Type: 4620                         Security Code: 1234             TN: 1
     Port: S00147                     Coverage Path 1:                 COR: 1
     Name: VO Recording Port 1        Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                               Message Lamp Ext: 52158
            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
```

6. Configure Avaya Aura® Application Enablement Services

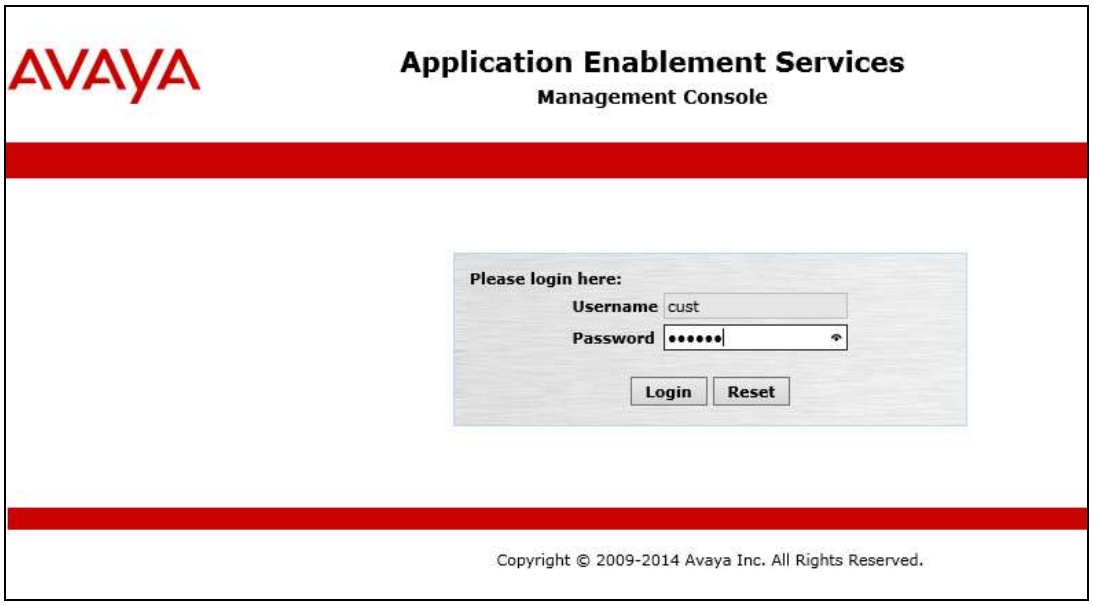
Avaya Aura® Application Enablement Services enables applications to monitor and control telephony resources on Avaya Aura® Communication Manager. The Avaya Aura® Application Enablement Services server receives requests from applications and forwards them to Avaya Aura® Communication Manager. Conversely, the Avaya Aura® Application Enablement Services server receives responses and events from Avaya Aura® Communication Manager and forwards them to the appropriate applications.

This section assumes that the installation and basic administration of the Avaya Aura® Application Enablement Services server has already been performed. For more information on administering Avaya Aura® Application Enablement Services, refer to the Avaya product documentation, Reference [10].

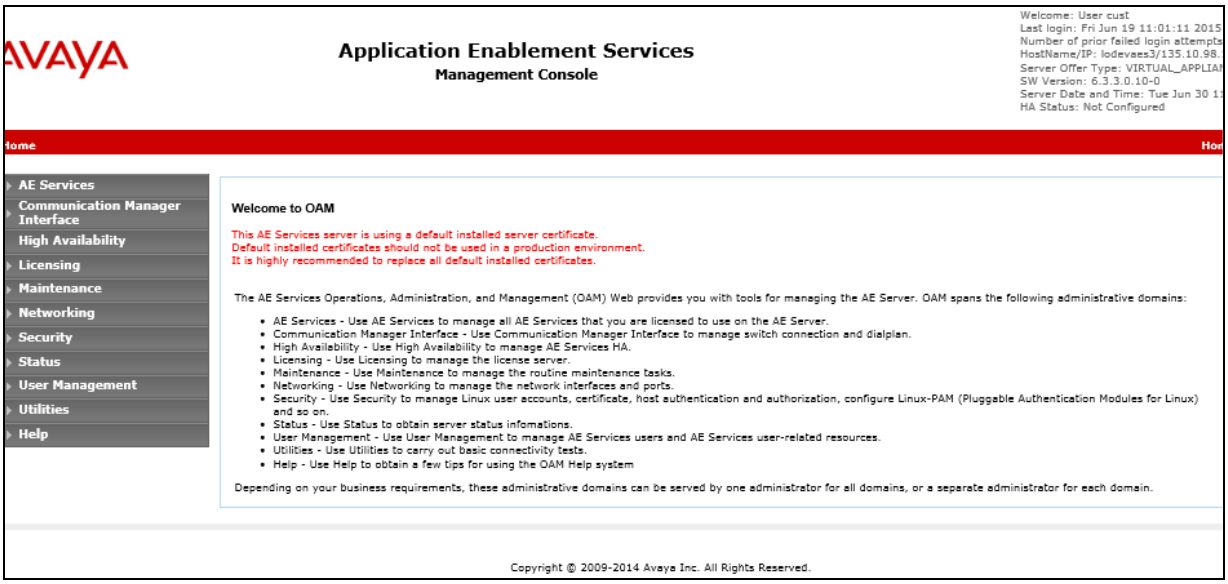
This section provides the procedures for configuring Avaya Aura® Application Enablement Services. The procedures fall into the following areas:

- Confirm Network Configuration
- Configure Avaya Aura® Communication Manager Switch Connections
- Verify TSAPI and DMCC Licensing
- Add TSAPI Links
- Add CTI User
- Enable Unrestricted Access to the Security Database

Access the web-based administration interface using **https://<ip-address>** in a browser where **<ip-address>** is the client interface address of the Avaya Aura® Application Enablement server. Click on the **Continue to Login** link, then login using appropriate credentials.

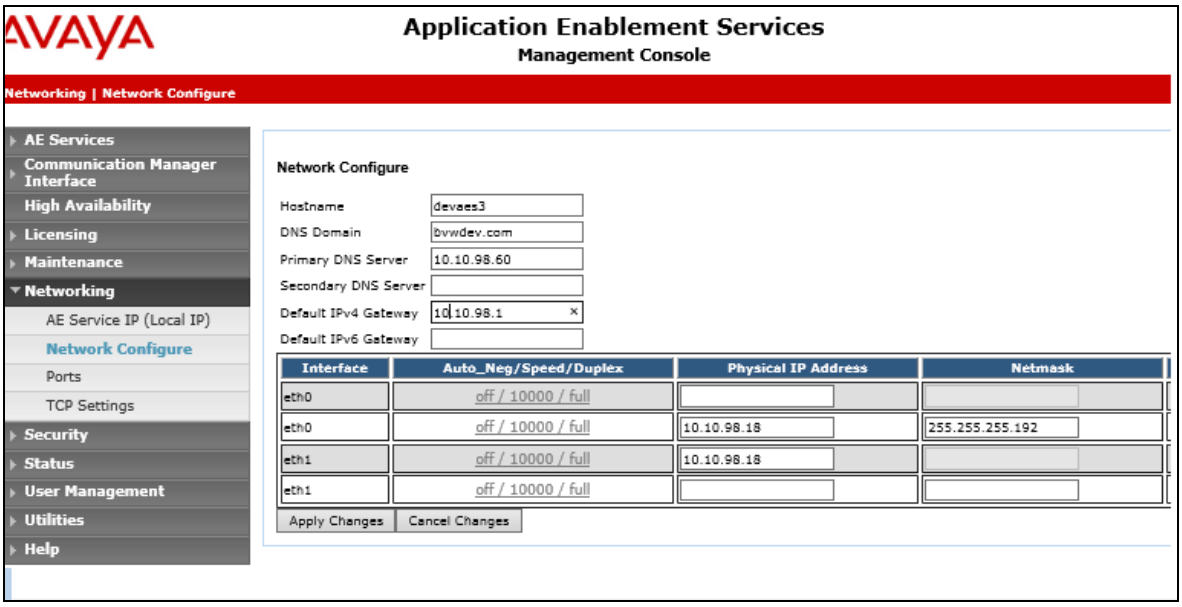


The **Welcome to OAM** screen is displayed next.



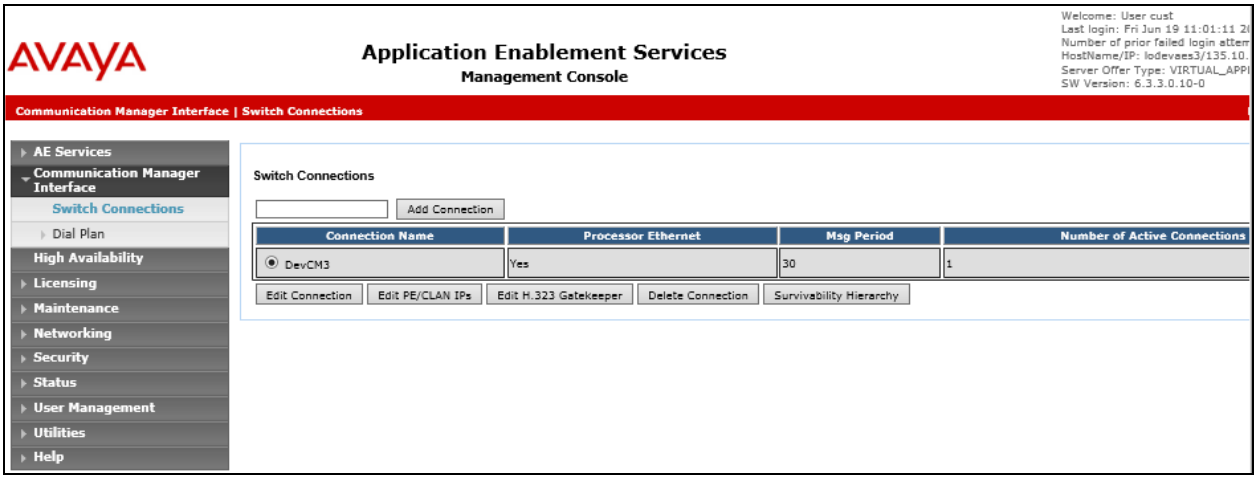
6.1. Confirm Network Configuration

Select **Networking** > **Network Configure** and note the client interface IP Address (**eth1** in this example) which will be used later in the application configuration. Application Enablement Services can be configured to use one or multiple NIC interfaces. It is preferable for security and performance reasons to use multiple interfaces and to have these on separate networks. The Communication Manager interface should always be bound to **eth0**.

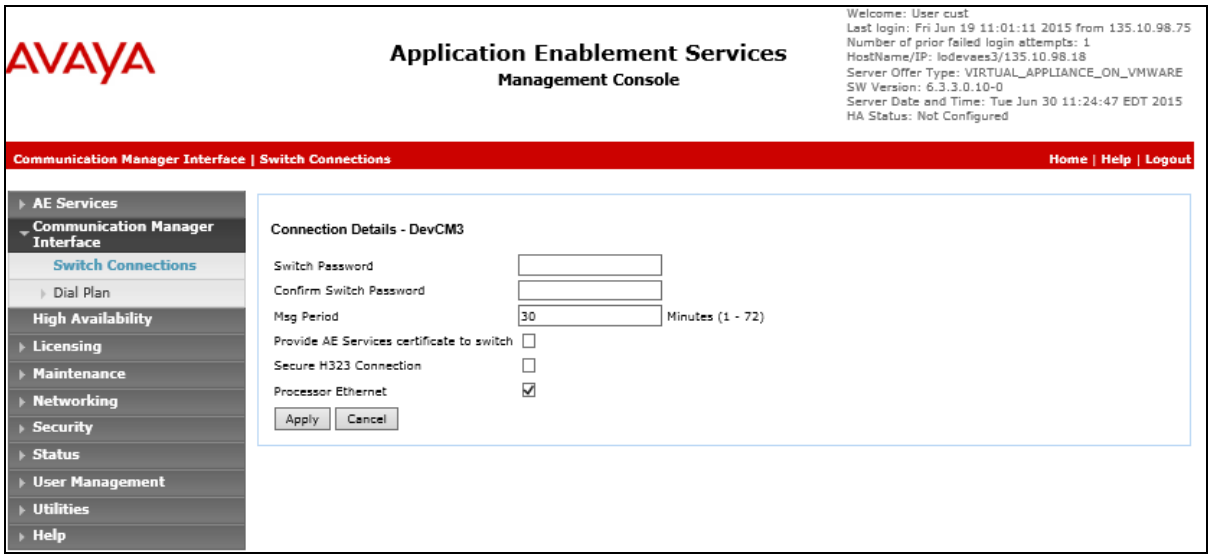


6.2. Configure Communication Manager Switch Connections

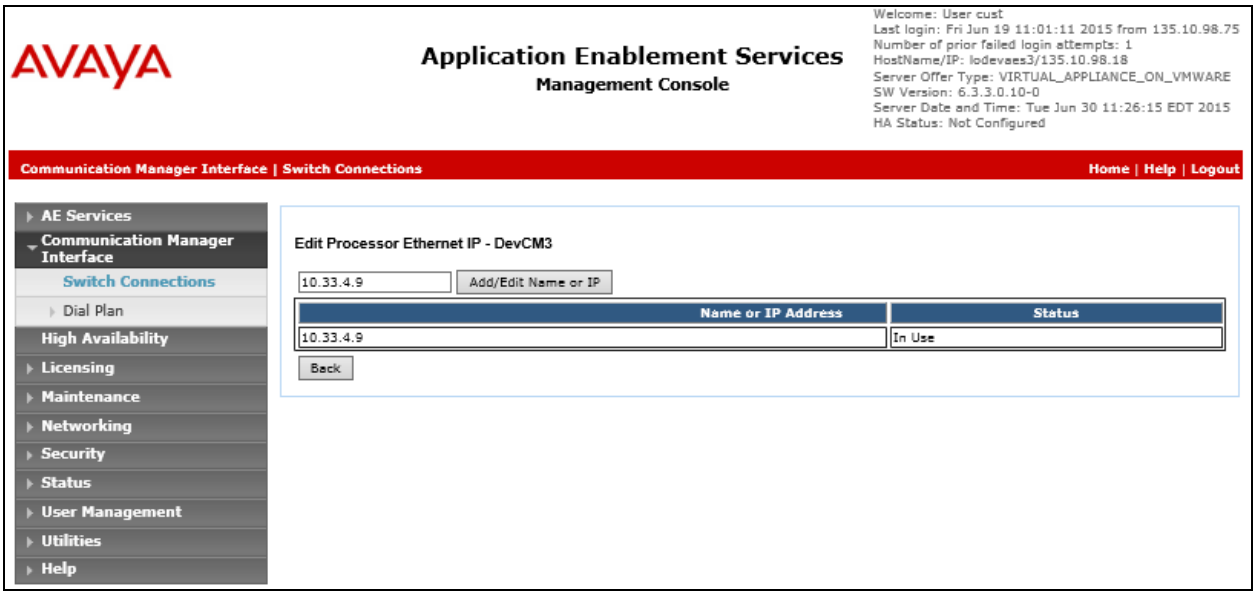
To add links to the Communication Manager, navigate to the **Communication Manager Interface > Switch Connections** page and enter a name for the new switch connection. This was previously configured as **DevCM3** for this test environment:



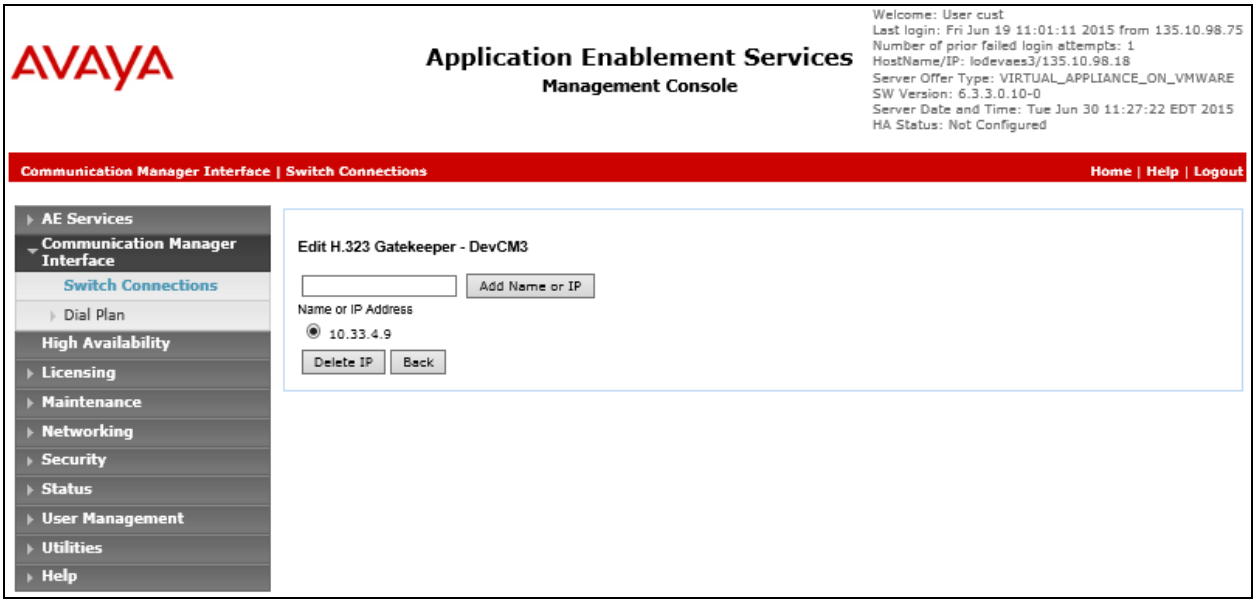
Use the **Edit Connection** button shown above to configure the **Switch Password**. This must match the password configured in section **5.2** above. Enter the **Switch Password** and check the **Processor Ethernet** box if using the **procr** interface, as shown below.



Use the **Edit PE/CLAN IPs** button (shown in this section's first screen shot above) to configure the **procr** or **CLAN** IP Address(es) for TSAPI message traffic.



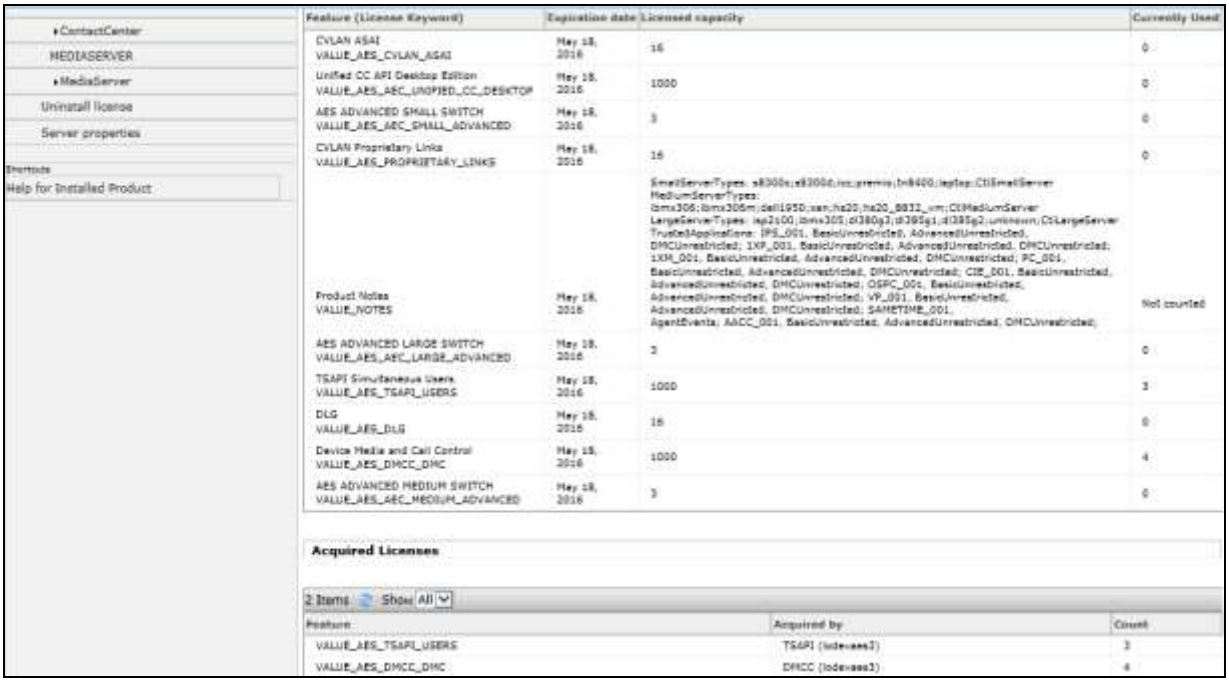
Use the **Edit H.323 Gatekeeper** button (shown in this section's first screen shot above) to configure the **procr** or **CLAN** IP Address(es) for DMCC registrations.



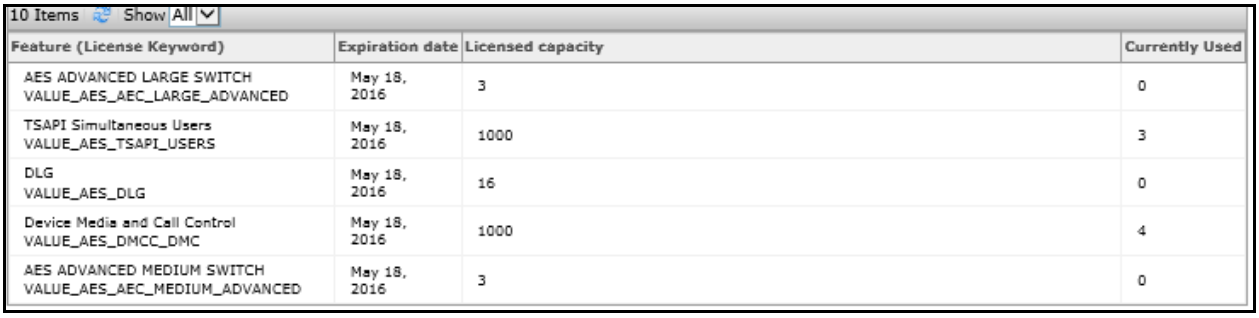
6.3. Verify TSAPI and DMCC Licensing

Virtual Observer will consume a **TSAPI** license for each station that is to be monitored for call events, and a **TSAPI** and **DMCC_DMC** license for each recording port. If the number of licenses are not adequate for the integration, contact Avaya sales or an authorized reseller.

Navigate to **Licensing > WebLM Server Access** and login using appropriate credentials. Select **Application_Enablement** under **Licensed Products > APPL_ENAB** to display entitlements and acquired licenses.



The screenshot below gives a closer look at **AES_TSAPI_USERS** and **AESDMCC_DMC** license counts.



10 Items Show All

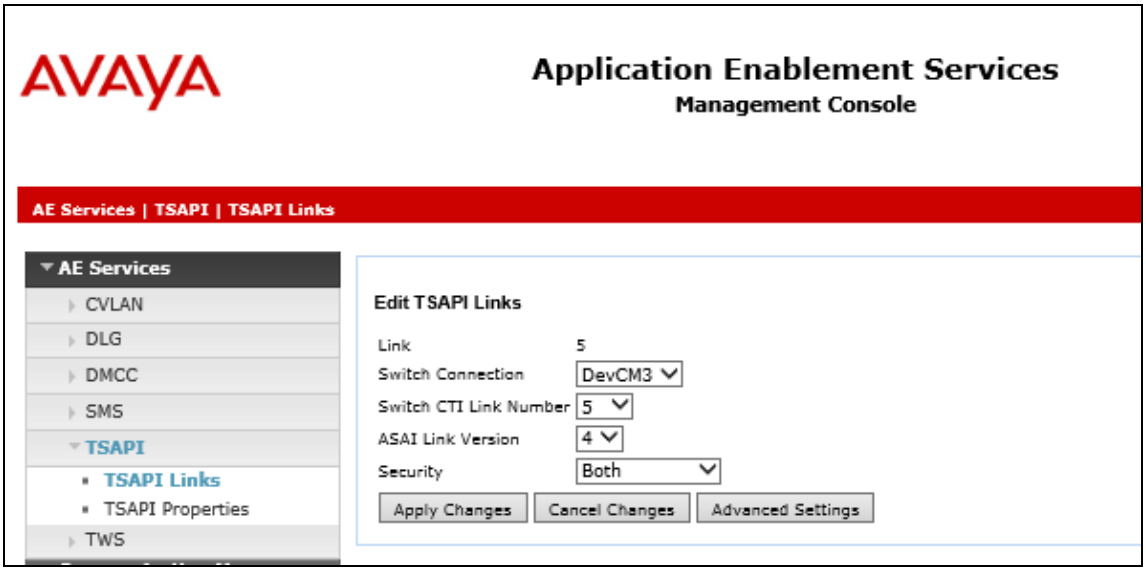
Feature (License Keyword)	Expiration date	Licensed capacity	Currently Used
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	May 18, 2016	3	0
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	May 18, 2016	1000	3
DLG VALUE_AES_DLG	May 18, 2016	16	0
Device Media and Call Control VALUE_AES_DMCC_DMC	May 18, 2016	1000	4
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	May 18, 2016	3	0

6.4. Add TSAPI Links

Navigate to the **AE Services -> TSAPI -> TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link**.

Select a **Switch Connection** using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The CTI link number must match the number configured in the **cti-link** form in **Section 5.4.** Click **Apply Changes**.

If the application will use Encrypted Links, select **Encrypted** in the **Security** selection box.

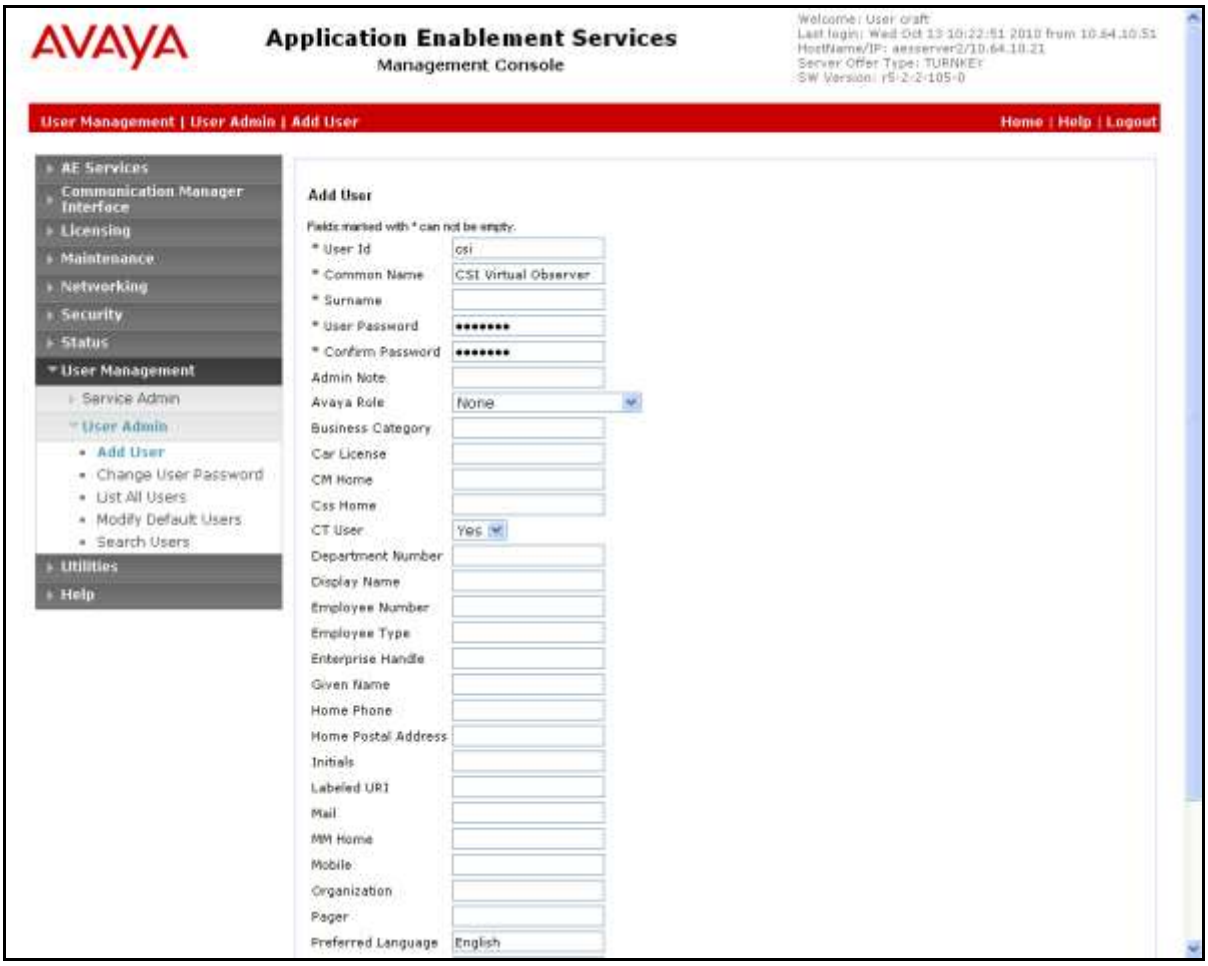


6.5. Add a CTI User

Virtual Observer requires a CTI user account to access Application Enablement Services. Select **User Management -> User Admin -> Add User** from the left pane.

In the **Add User** screen, enter the following values:

- In the **User Id** field, type a meaningful user id.
- In the **Common Name** field, type a descriptive name.
- In the **Surname** field, type a descriptive surname.
- In the **User Password** field, type a password for the user.
- In the **Confirm Password** field, re-enter the same password for the user.
- In the **Avaya Role** field, retain the default of **None**.
- In the **CT User** field, select **Yes** from the dropdown menu.
- Click **Apply** at the bottom of the screen (not shown here).



6.6. Enable Unrestricted Access to the Security Database

The Virtual Observer user account will require unrestricted SDB access in order to be able to access any of the Devices (stations) administered to be recorded in the application.

To change the security level for the CT User Select **Security -> Security Database -> CTI Users -> List All Users** from the left pane. Choose the CTI user, and click **Edit** (not shown below).

On the **Edit CTI User** form, check the **Unrestricted Access** option and click on **Apply Changes**.

7. Configure the Virtual Observer server

This section provides the procedures for configuring the Virtual Observer server. The procedures include the following areas:

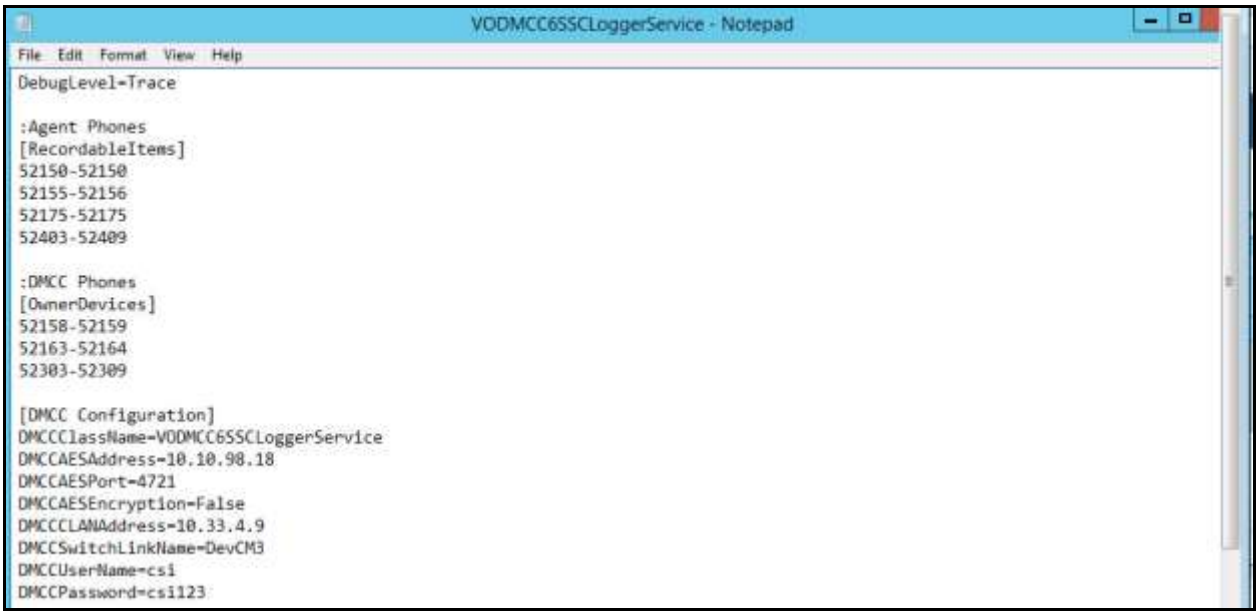
- Configuration of Extensions to Monitor and Record, Devices used for Recording, and Avaya Aura® Application Enablement Services Interface
- View Recorded Calls

The initial configuration of the Virtual Observer server is typically performed by CSI technicians or authorized installers. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Configuration of Extensions to Monitor and Record, Devices used for Recording, and Application Enablement Services Interface

Enter the following site preparation information in VODMCC6SSCLoggerService.ini file. An .ini file is saved for each interface instance and is used by the application at startup to initialize services.

- Phone Extensions to Record (Agent Phones)
- Phone Extensions used for Recording (DMCC Phones)
- Avaya Aura® Application Enablement Services Server IP
- DMCC Application Enablement Services Port
- procr IP Address
- Avaya Aura® Application Enablement Services Switch Link Name (Not the same as the server name)
- CTI User Name and Password (With “Unrestricted Access”)




```
DebugLevel=Trace

:Agent Phones
[RecordableItems]
52150-52150
52155-52156
52175-52175
52403-52409

:DMCC Phones
[OwnerDevices]
52158-52159
52163-52164
52303-52309

[DMCC Configuration]
DMCCClassName=VODMCC6SSCLoggerService
DMCCAESAddress=10.10.98.18
DMCCAESPort=4721
DMCCAESEncryption=False
DMCCCLANAddress=10.33.4.9
DMCCSwitchLinkName=DevCM3
DMCCUserName=csi
DMCCPassword=csi123
```

- Available Codec's
- DMCC Device Password

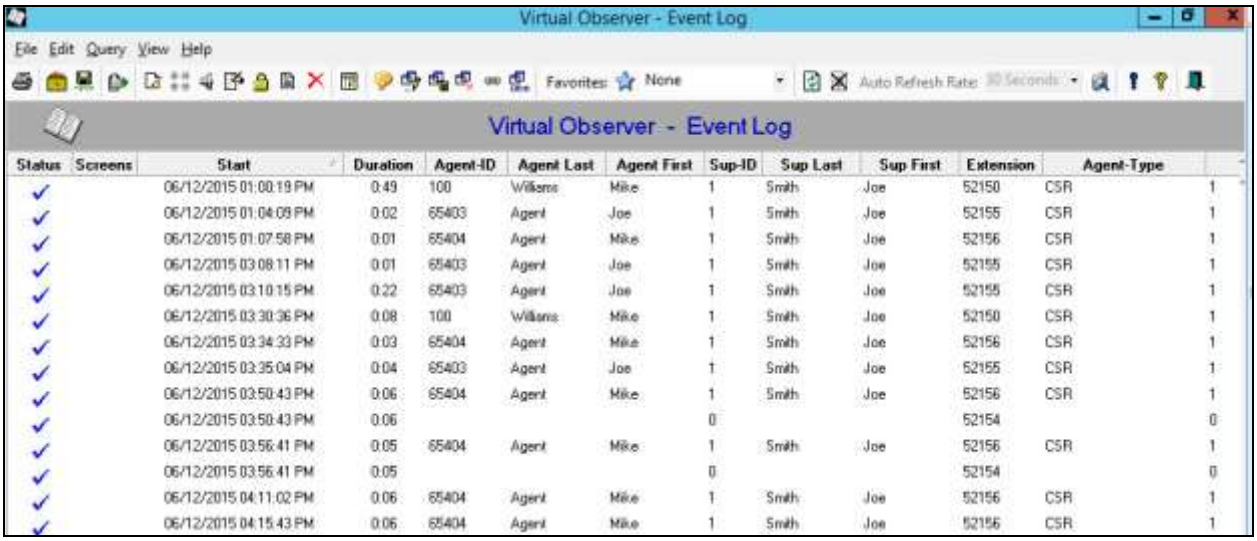
```
:Set to True  to Register the Agent Device  First. On success register the DMCC  Device. On failure DO NOT attempt the DMC
:Set to False to Register the DMCC Terminal First. On success register the Agent Device. On failure DO NOT attempt the Age
:Default in code is FALSE.

Codec=g711U
::Currently only support (g711U) and (g729), g711U is default

DMCCDevicePassword=1234
::Password for the DMCC Softphones

CreateRAWFile=False
::Create a RAW File with all the RTP Packets and their headers

UseTeardownSequences=True
:If True,  the device will be gracefully shutdown using a sequence of methods and onMethodResponse.
:If False, the device will have all its shutdown elements fired off in a row without waiting for response.


[LinkDown]
```

Verify the following:

- CTI User has "Unrestricted Access"
- CLAN is in a region with media processor (MedPro) resources
- Available TSAPI Licenses
- Available IP_API_A or DMCC_DMC Licenses
- Avaya Aura® Application Enablement Services "Switch Connectivity" is configured to an interface that can talk to the CLAN
- DMCC Phones have a COR with an FRL level greater than or equal to the FRL level on the agent phone's COR
- All DMCC Devices use a common Codec (either G711 or G729)

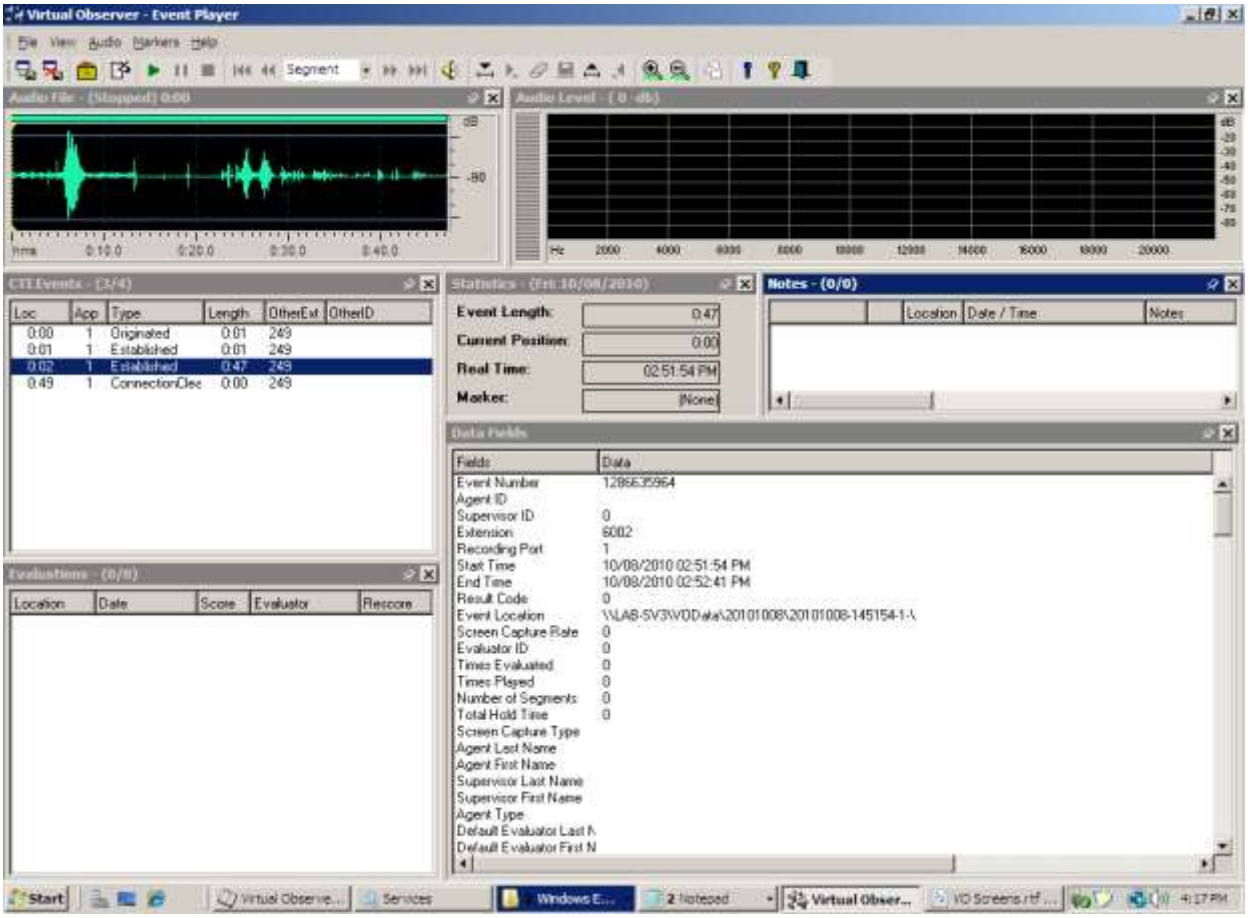
7.2. Viewing Recorded Calls

The Virtual Observer **Event Log** tool was used to search for, and playback, audio recordings. In addition to this tool, there are several administrator and user client based tools available for performing the typical user interface tasks. These application notes will not cover the other tools in detail.



Status	Screens	Start	Duration	Agent-ID	Agent Last	Agent First	Sup-ID	Sup Last	Sup First	Extension	Agent-Type	
✓		06/12/2015 01:00:19 PM	0:49	100	Williams	Mike	1	Smith	Joe	52150	CSR	1
✓		06/12/2015 01:04:09 PM	0:02	65403	Agent	Joe	1	Smith	Joe	52155	CSR	1
✓		06/12/2015 01:07:58 PM	0:01	65404	Agent	Mike	1	Smith	Joe	52156	CSR	1
✓		06/12/2015 03:08:11 PM	0:01	65403	Agent	Joe	1	Smith	Joe	52155	CSR	1
✓		06/12/2015 03:10:15 PM	0:22	65403	Agent	Joe	1	Smith	Joe	52155	CSR	1
✓		06/12/2015 03:30:36 PM	0:08	100	Williams	Mike	1	Smith	Joe	52150	CSR	1
✓		06/12/2015 03:34:33 PM	0:03	65404	Agent	Mike	1	Smith	Joe	52156	CSR	1
✓		06/12/2015 03:35:04 PM	0:04	65403	Agent	Joe	1	Smith	Joe	52155	CSR	1
✓		06/12/2015 03:50:43 PM	0:06	65404	Agent	Mike	1	Smith	Joe	52156	CSR	1
✓		06/12/2015 03:50:43 PM	0:06				0			52154		0
✓		06/12/2015 03:56:41 PM	0:05	65404	Agent	Mike	1	Smith	Joe	52156	CSR	1
✓		06/12/2015 03:56:41 PM	0:05				0			52154		0
✓		06/12/2015 04:11:02 PM	0:06	65404	Agent	Mike	1	Smith	Joe	52156	CSR	1
✓		06/12/2015 04:15:43 PM	0:06	65404	Agent	Mike	1	Smith	Joe	52156	CSR	1

By clicking on the  icon in the toolbar menu in the screen shot above, with the item of interest selected, an **Event Player** window will appear as shown below.



8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and CSI Virtual Observer.

Check the service status of your Avaya Aura® Communication Manager CTI links by entering the **status aesvcs cti-link** command. The link status should show **no** for maintenance busy (**Mnt Busy**) and the **Service State** should indicate **established**.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

5     4        no    aesserver2       established   15       15


Command successfully completed
Command:
```

The **status aesvcs interface** command should indicate the interface is listening, even before Avaya Aura® Application Enablement Services is configured.

```
                          AE SERVICES INTERFACE STATUS

Local Node        Enabled?  Number of     Status
                            Connections

procr             yes       1             listening


Command successfully completed
```

The **status aesvcs link** command will indicate the number of messages sent from, and received at the CLAN interface (or procr), to and from Avaya Aura® Application Enablement Services, including maintenance traffic.

```
status aesvcs link
                            AE SERVICES LINK STATUS

Srvr/  AE Services     Remote IP        Remote  Local Node      Msgs    Msgs
Link   Server                           Port                    Sent    Rcvd

01/01  aes63                             59815   procr           620     606
                       10.35.98.18
Command successfully completed
```

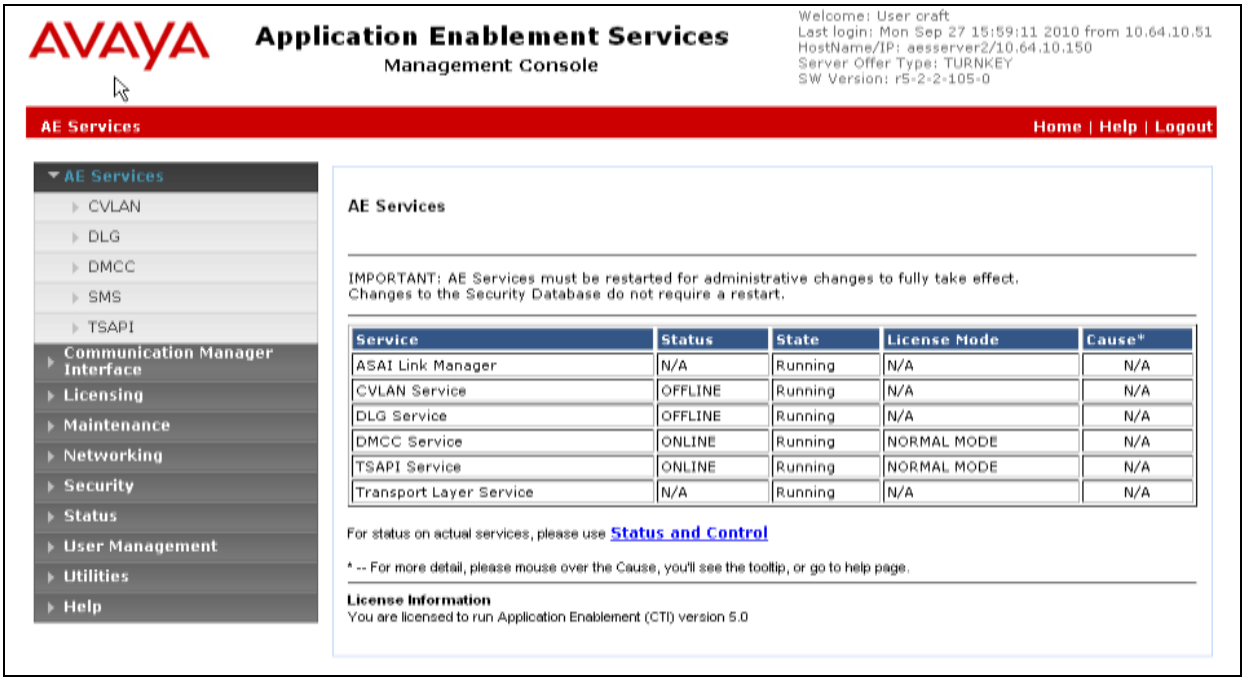
Once the Virtual Observer server is running, the **list registered-ip-stations** command will show not only active phone registrations, but also an entry for each virtual station to be used by the recorder that is associated with the Avaya Aura® Application Enablement client link Address (**10.35.98.18**).

```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/   TCP Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ---------------------------------------
52151         9630      IP_Phone    y  10.33.5.41
              1         3.220A         10.33.4.9
52155         9650      IP_Phone    y  10.33.5.24
              1         3.230A         10.33.4.9
52156         9650      IP_Phone    y  10.33.5.64
              1         3.230A         10.33.4.9
52158         4620      IP_API_A    y  10.10.98.18
              1         3.2040         10.33.4.9
52159         4620      IP_API_A    y  10.10.98.18
              1         3.2040         10.33.4.9
52163         4620      IP_API_A    y  10.10.98.18
              1         3.2040         10.33.4.9
52164         4620      IP_API_A    y  10.10.98.18
              1         3.2040         10.33.4.9
```

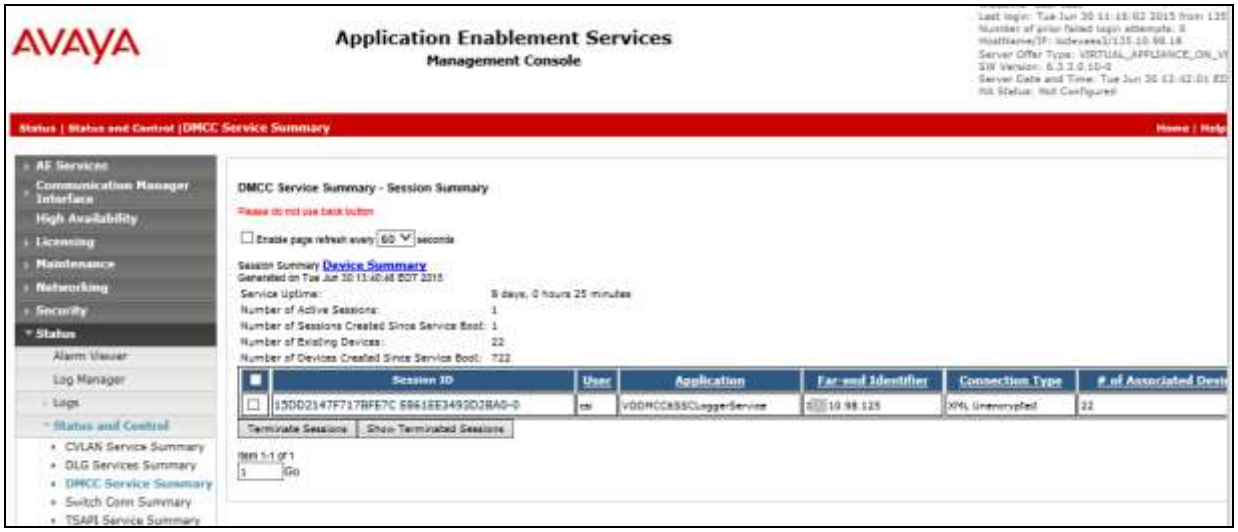
In addition, each station to be recorded will show an ASAI monitor association by using the **list monitored-station** command.

```
list monitored-station
                            MONITORED STATION

  Station     Association 1    Association 2    Association 3    Association 4
  Ext         CTI Link  CRV    CTI Link  CRV    CTI Link  CRV    CTI Link  CRV
  -------     -------------    -------------    -------------    -------------
52150          5           1
52155          5           4
52156          5           5
```

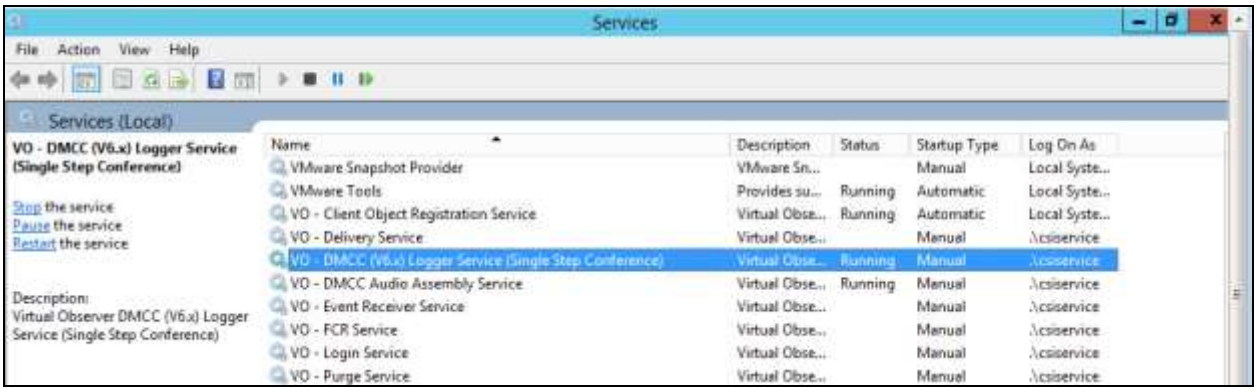
Navigate to **AE Services** on the Avaya Aura® Application Enablement Services server to verify that services are **ONLINE** and **NORMAL MODE** for the TSAPI and DMCC Services, as shown in the screen below.



Once the application has successfully started, the **DMCC Service Summary** will show a list of active session, **VODMCC6SSCLoggerService** of Virtual Observer server is listed.



On the Virtual Observer server, confirm that **VO-DMCC Audio Assembly service** and **VO-DMCC (V6x) Logger Service (Single Step Conference)** services are started.



9. Conclusion

These Application Notes describe the configuration steps required for CSI Virtual Observer 5.1 to successfully interoperate with Avaya Aura® Communication Manager 6.3 and Avaya Aura® Application Enablement Services 6.3. All feature and serviceability test cases were completed with observations noted in **Section** Error! Reference source not found..

10. Additional References

This section references the Avaya and CSI product documentation that are relevant to these Application Notes.

Avaya product documentation can be found at http://support.avaya.com:

Administering Avaya Aura® Communication Manager, Doc ID: 03-300509, Issue 10, Release 6.3, June 2015

Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Doc ID: 02-300357, Release 6.3, June 2014

CSI Virtual Observer Audio Recording White Paper, Avaya DMCC Rev. F – July 19, 2010

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.