Avaya Solution & Interoperability Test Lab

Application Notes for Mattersight Call Recording Solution with Avaya Aura® Communication Manager Using Service Observing with Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Mattersight Call Recording Solution to interoperate with Avaya Aura® Communication Manager using Avaya Aura® Application Enablement Services.

Mattersight Call Recording Solution is a call recording solution. In the compliance testing, Mattersight Call Recording Solution used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor skill group and agent station extensions on Avaya Aura® Communication Manager, and to capture the media associated with the monitored agents 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 Mattersight Call Recording Solution 4.0 to interoperate with Avaya Aura® Communication Manager 7 using Avaya Aura® Application Enablement Services 7.

Mattersight Call Recording Solution is a call recording solution. In the compliance testing, Mattersight Call Recording Solution used the Device, Media, and Call Control (DMCC) interface from Avaya Aura® Application Enablement Services to monitor skill group and agent station extensions on Avaya Aura® Communication Manager, and to capture the media associated with the monitored agents for call recording.

When there is an active call on the monitored agent, Mattersight Call Recording Solution is informed of the call via event reports from the DMCC interface. Mattersight Call Recording Solution starts the call recording by using the Service Observing Feature Access Code from the DMCC interface to add a virtual IP softphone to the active call to obtain the media. The event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Call Recording Solution application, the application automatically uses DMCC to register the virtual IP softphones to Communication Manager, and to request monitoring on the recording skill group and agent station extensions.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for the recordings. Necessary user actions such as hold and reconnect were performed from the agent telephones to test the different call scenarios. The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Call Recording Solution.

The verification of tests included using the Call Recording Solution logs for proper message exchanges, and using the Retrieval application for proper logging and playback of the calls.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Call Recording Solution:

- Use of DMCC registration services to register and un-register the virtual IP softphones.
- Use of DMCC monitoring services to monitor agent stations and virtual IP softphones.
- Use of DMCC call control services to activate Service Observing via Feature Access code for the virtual IP softphones and to obtain the media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving G711, G729, inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, simultaneous calls, simultaneous agents, conference, transfer and long call duration.

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

2.2. Test Results

All test cases were executed, and the following were observations on Call Recording Solution from the compliance testing:

- The User interface to display recordings is not part of this solution therefore the test audio files created after the call completed were played from Windows File Explorer. Call details such as DNIS, Call Type, Call Direction (Meta data) was reviewed separately.
- Agents must be a member of a specific skill group in order to be recorded.
- If the agent is reskilled without using the Avaya CMS tool the agent will need to log out and log back in for the skill changes to take effect.
- During the call if a user performs actions such as pressing the Transfer button on desk phone and then pressing the Cancel or Clear button this will trigger AES to send a Call Clear event and Mattersight will stop recording the second leg of the call. The first leg of the call will continue to be recorded.
- When an agent is active on a call that is being monitored and recorded, and the agent places another call (by using transfer, conference, or hold) to a destination that is not monitored, the call to the non-monitored destination will not be recorded. Mattersight has indicated that this is working as designed.
- For a call between 2 internal agents, only1 recording will be created.
- The voice quality of a recorded G729 call is not as clear as a G.711 call.
- The Service observe is initiated as soon as the agent logs in to ensure no portion of the call is missed. This will require one virtual station to be available for every agent phone.

2.3. Support

Technical support on Mattersight Call Recording Solution can be obtained through the following:

- **Phone:** 877.235.6925
- **Email:** support@mattersight.com

3. Reference Configuration

Call Recording Solution is a SaaS (Software as a service solution) offering. Mattersight will design an appropriately sized solution based on several factors to include concurrent calls, calls per second and concurrent agents. The compliance test used a single server configuration shown in **Figure 1**.

There is no user interface provided for Call Recording Solution to review and playback the call recordings, to verify if Call Recording Solution properly recorded the call, manually open media file locate in folder D:\AFCRecordings. Customers would leverage the Mattersight portal to access call recordings and meta data as no direct access to the file structure is provided

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, the contact center devices consisted of two VDNs, two skill groups, one supervisor, and two agents stations as shown in the table below.

Device Type	Extension
VDN	56001, 56010
Skill/Hunt Group	56300, 56303
Agent ID	1000, 1004
Agent Station	56201, 56101
Supervisor	56202

A new hunt group will need to be created so the Mattersight CRS application can keep track of the agents that need to be recorded. For testing skill group 5 with extension is 56304 was used. All agents that are in-scope for call recording would need to have this skill assigned to them. For this example agent 1000 and 1004 were added to skill group 5.

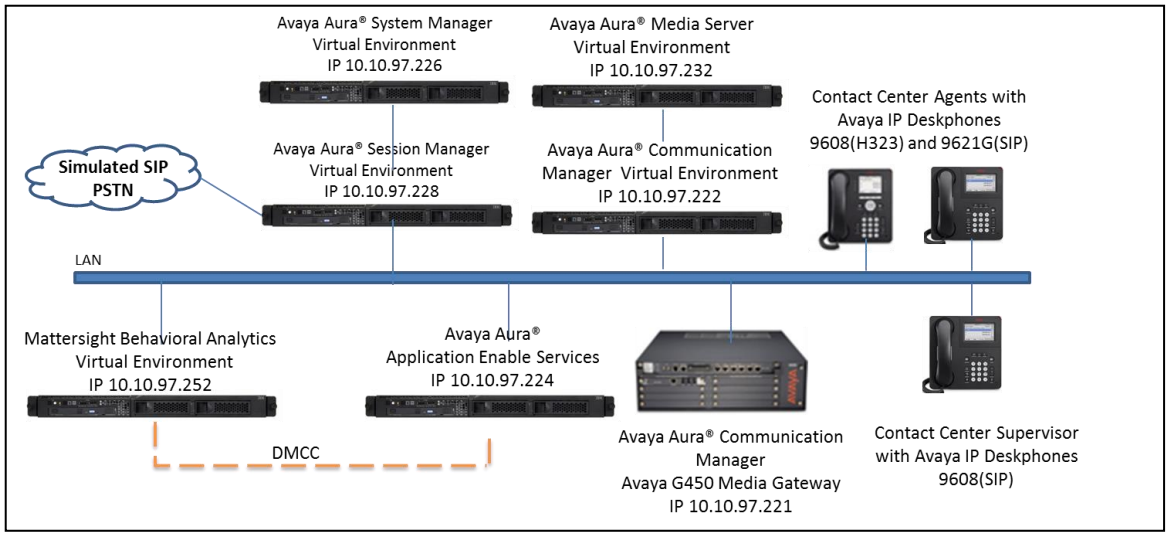


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Virtual Environment	7.0.2
Avaya G450 Media Gateway	7.0.1.1
Avaya Aura® Media Server on Virtual Environment	7.7.0.334
Avaya Aura® Application Enablement Services	7.0.1 Super Patch 3
Avaya 9608, 9621G IP Deskphone (H.323)	6.6.3
Avaya 9621G IP Deskphone (SIP)	7.0.1.4
Avaya Aura® Session Manager	7.0.1 SP2
Avaya Aura® System Manager	7.0.1.2
MatterSight Call Recording Solution on Windows 2012R2 Server • Avaya DMCC .NET (ServiceProvider.dll)	4.0 SP 2 6.2.0.29

5. Configure Avaya Aura® Communication Manager

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

- Verify License
- Administer Service Observer Feature Access Code
- Administer Class of Restriction
- Administer CTI link
- Administer System Parameters Features
- Administer Hunt Group
- Administer Agent Station
- Administer Virtual IP softphones

5.1. Verify License

Log in to the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command to verify that the **Computer Telephony Adjunct Links** customer option is set to "y" on **Page 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
                                 ATMS? y              DS1 Echo Cancellation? y
                  Attendant Vectoring? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

Verify **Service Observing (Basic)** and **Service Observing (Remote/By FAC)** are 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
       Expert Agent Selection (EAS)? y            Vectoring (G3V4 Enhanced)? y
                           EAS-PHD? y             Vectoring (3.0 Enhanced)? y
                  Forced ACD Calls? n   Vectoring (ANI/II-Digits Routing)? y
              Least Occupied Agent? y   Vectoring (G3V4 Advanced Routing)? y
          Lookahead Interflow (LAI)? y                  Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y    Vectoring (Best Service Routing)? y
    Multiple Call Handling (Forced)? y               Vectoring (Holidays)? y
  PASTE (Display PBX Data on Phone)? y               Vectoring (Variables)? y
        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. Administer Service Observer Feature Access Code

Mattersight will need the Feature Access Code (FAC) to invoke the service observe feature. From the SAT administration tool, type **display feature-access-codes** and go to page 5. The Mattersight application uses the **Service Observing Listen Only Access Code** *43 as displayed below:

```
display feature-access-codes                                    Page   5 of  11
                             FEATURE ACCESS CODE (FAC)
                               Call Center Features
  AGENT WORK MODES
                          After Call Work Access Code: *36
                                  Assist Access Code: *37
                                Auto-In Access Code: *38
                               Aux Work Access Code: *39
                                  Login Access Code: *40
                                 Logout Access Code: *41
                              Manual-in Access Code: *42
  SERVICE OBSERVING
            Service Observing Listen Only Access Code: *43
            Service Observing Listen/Talk Access Code: *44
                Service Observing No Talk Access Code: *45
   Service Observing Next Call Listen Only Access Code:
 Service Observing by Location Listen Only Access Code:
 Service Observing by Location Listen/Talk Access Code:
  AACC CONFERENCE MODES
                    Restrict First Consult Activation:      Deactivation:
                   Restrict Second Consult Activation:      Deactivation:
```

5.3. Administer Class of Restriction

Agent stations must be part of a COR that includes the "Can be service observed" feature. Virtual stations must be part of a COR that include the "Can be a service observer" feature.

During compliance test, the same COR was used for both agent station and virtual station, use the "change cor n" command, where "n" is the class of restriction (COR) number to be assigned to the target stations, virtual IP softphones, set the **Can Be Service Observed**, **Can Be A Service Observer** and the **Calling Party Restriction** to "y" as shown below.

```
display cor 1                                                 Page   1 of  23
                              CLASS OF RESTRICTION
               COR Number: 1
          COR Description:
                      FRL: 1                                      APLT? y
  Can Be Service Observed? y            Calling Party Restriction: none
Can Be A Service Observer? y             Called Party Restriction: none
        Time of Day Chart: 1         Forced Entry of Account Codes? n
         Priority Queuing? n                  Direct Agent Calling? n
     Restriction Override: all          Facility Access Trunk Test? n
     Restricted Call List? n                  Can Change Coverage? n
           Access to MCT? y              Fully Restricted Service? n
Group II Category For MFC: 7              Hear VDN of Origin Annc.? n
         Send ANI for MFE? n               Add/Remove Agent Skills? n
            MF ANI Prefix:               Automatic Charge Display? n
Hear System Music on Hold? y    PASTE (Display PBX Data on Phone)? n
                        Can Be Picked Up By Directed Call Pickup? y
                                     Can Use Directed Call Pickup? y
                                     Group Controlled Restriction: inactive
```

5.4. 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: 56001
     Type: ADJ-IP
                                                                   COR: 1
     Name: DevvmAES
```

5.5. 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: 1
```

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

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

    Reporting for PC Non-Predictive Calls? n

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

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

5.6. Administer Hunt Group

A new hunt group will need to be created so the Mattersight CRS application can keep track of the agents that need to be recorded. All agents that are in-scope for call recording would need to have this skill assigned to them. Below is **hunt group** 5 is created.

```
display hunt-group 5                                          Page   1 of   4
                                HUNT GROUP
            Group Number: 5                                 ACD? y
              Group Name: Basic 3                         Queue? y
         Group Extension: 56304                          Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
          Security Code:                 Local Agent Preference? n
 ISDN/SIP Caller Display:
             Queue Limit: unlimited
 Calls Warning Threshold:      Port:
  Time Warning Threshold:      Port:
```

5.7. Administer Agent Station

Agent stations must be part of a COR that includes the **Can be service observed** set to yes as configured in **Section 5.3**. Repeat this section for all agent stations. In the interoperability test, two physical agent stations "56101" and "56201" were modified.

```
display station 56201                                         Page   1 of   6
                                    STATION
Extension: 56201                       Lock Messages? n              BCC: 0
     Type: 9611SIPCC                   Security Code:                 TN: 1
     Port: S00001                    Coverage Path 1: 2              COR: 1
     Name: TwoOOne, OOne             Coverage Path 2:                COS: 1
                                     Hunt-to Station:
STATION OPTIONS
                                         Time of Day Lock Table:
              Loss Group: 19
                                               Message Lamp Ext: 56201

        Display Language: english                Button Modules: 0

          Survivable COR: internal
   Survivable Trunk Dest? y                        IP SoftPhone? y

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

5.8. Administer Virtual IP Softphones

Virtual IP Softphones are used by Mattersight to service observe target stations and capture media. 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 "9620".
- **Name:** A descriptive name.
- **Security Code:** A desired code, example: 1234. Below screenshot, security code has been masked by Communication Manager for security reason.
- **COR:** Enter COR created in **Section 5.3**.
- **IP SoftPhone:** Set to "y".

```
add station 56114                                            Page   1 of   5
                                    STATION

Extension: 56114                        Lock Messages? n              BCC: 0
     Type: 9620                         Security Code: *-              TN: 1
     Port: S00067                         Coverage Path 1:            COR: 1
     Name: BA Virtual #1                Coverage Path 2:              COS: 1
                                        Hunt-to Station:             Tests: y
STATION OPTIONS
                                           Time of Day Lock Table:
             Loss Group: 19          Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 56114
           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
                                         Customizable Labels? Y
```

Repeat this section to administer the desired number of virtual IP softphones, using sequential extension numbers. In the compliance testing, two virtual IP softphones were administered as shown below, to allow for simultaneous recording of two monitored agents described in **Section 3**.

```
list station 56114 count 2

                                  STATIONS

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

56114         S00067  BA Virtual #1                             1
               9620                         no                  1
56115         S00070  BA Virtual #2                             1
               9620                         no                  1
```

6. Configure Avaya Aura® Application Enablement Services

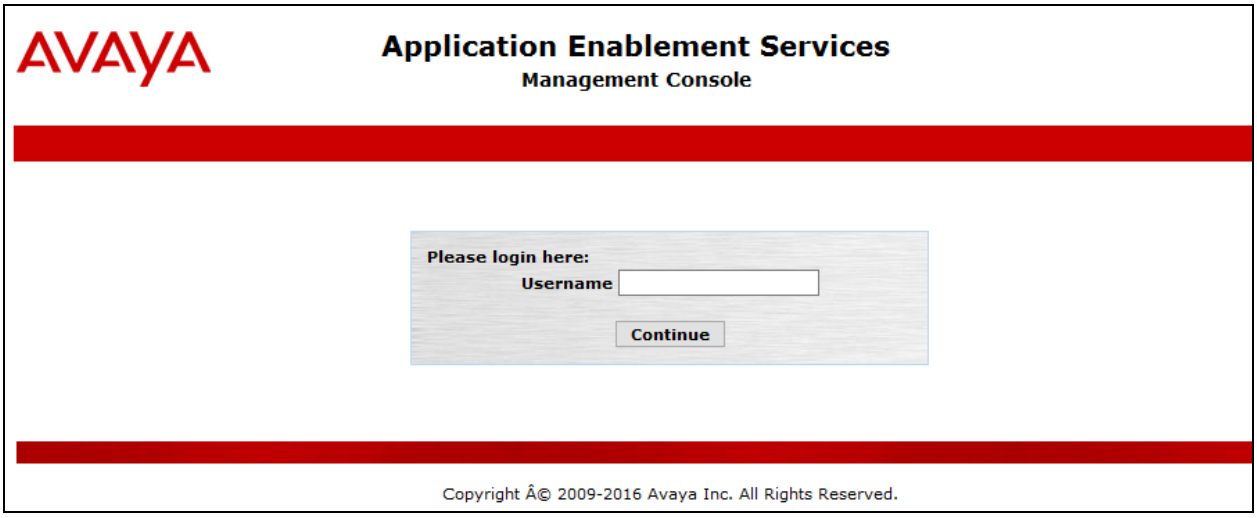
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart services
- Administer Call Recording Solution user
- Provide Call Recording Solution User unrestricted access
- Administer ports

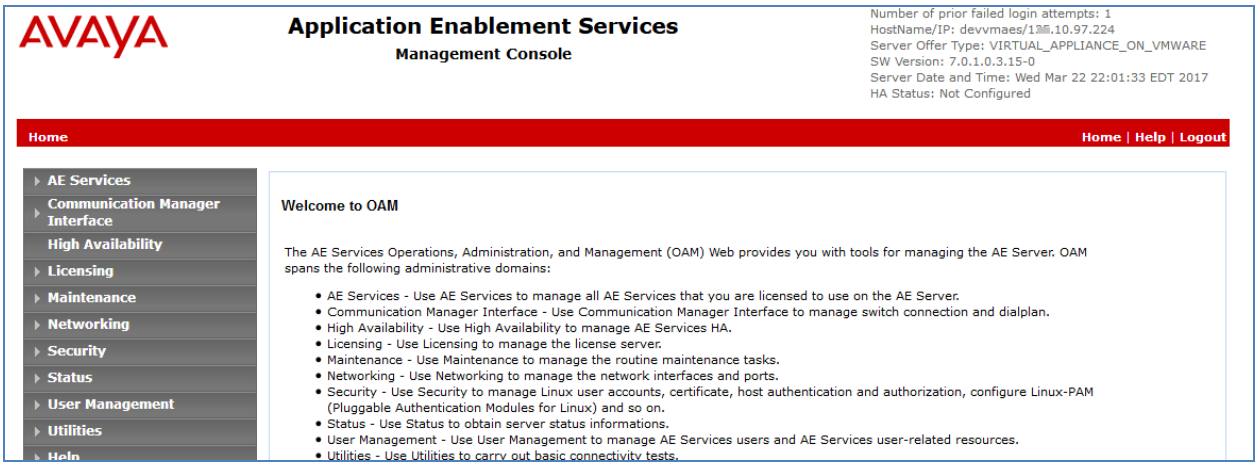
6.1. Launch OAM Interface

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

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

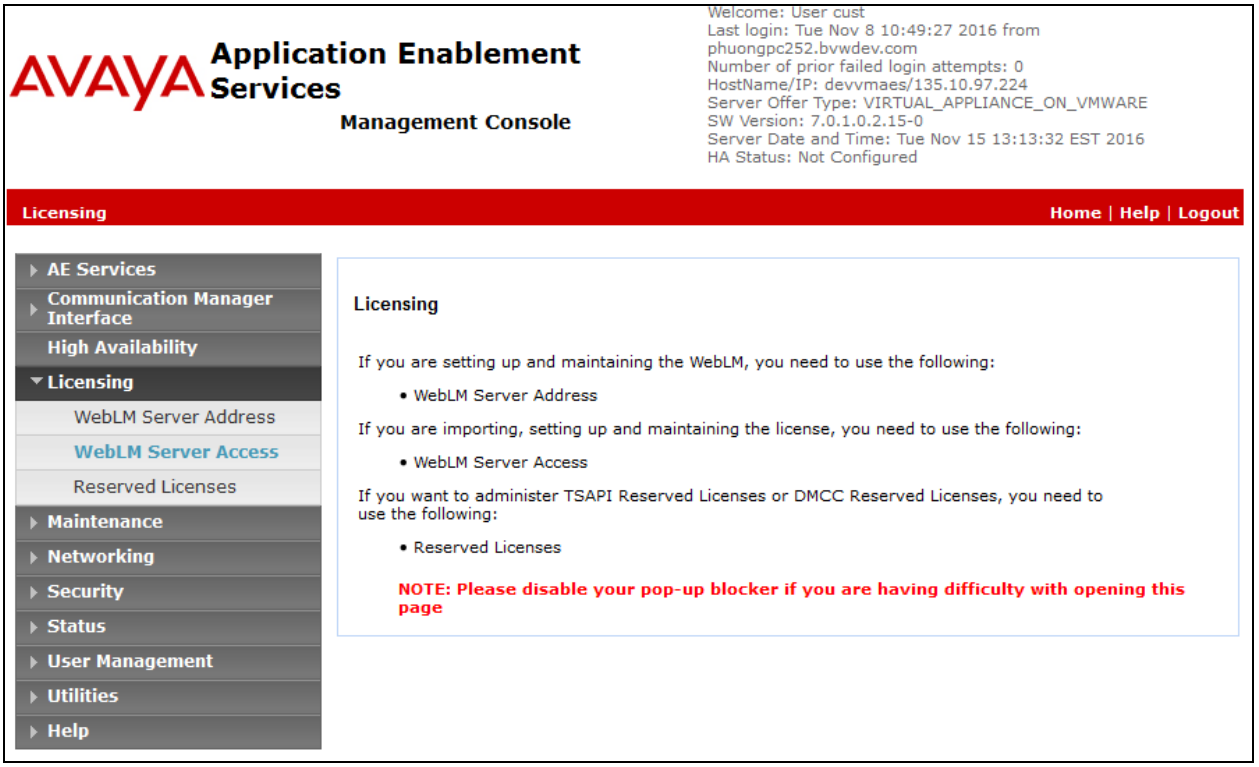


The **Welcome to OAM** screen is displayed as below.



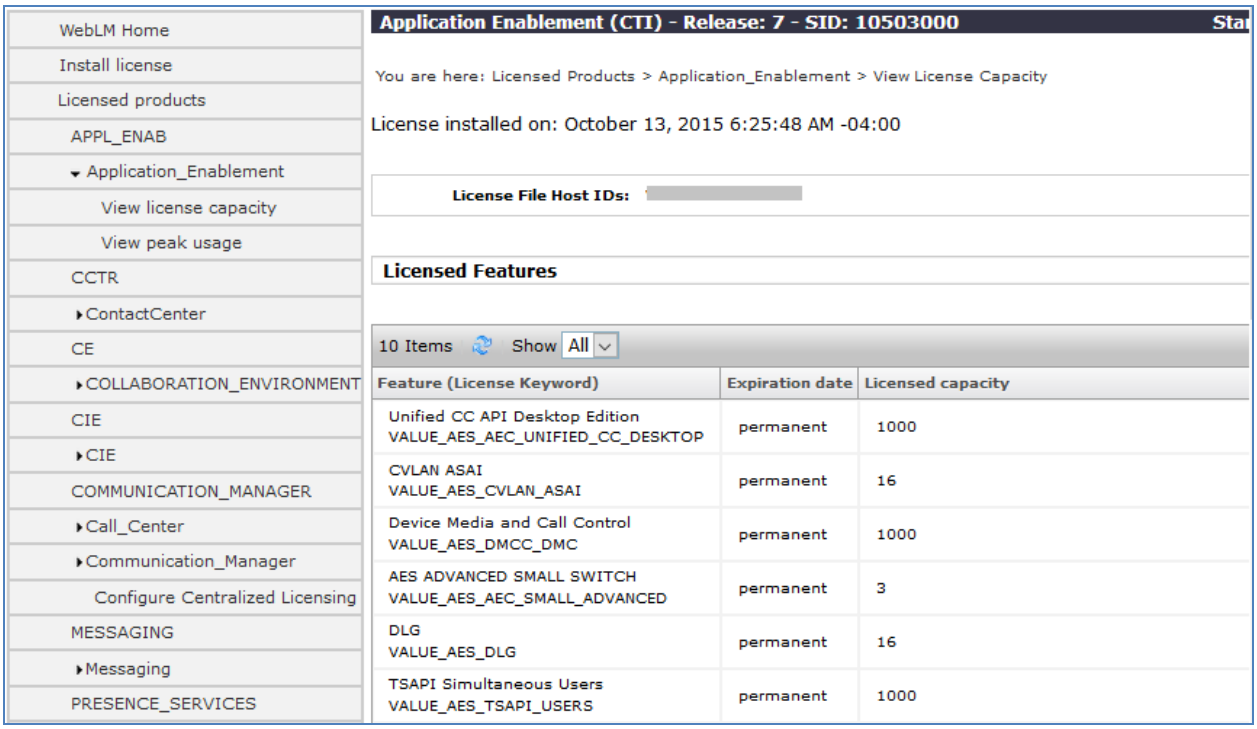
6.2. Verify License

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



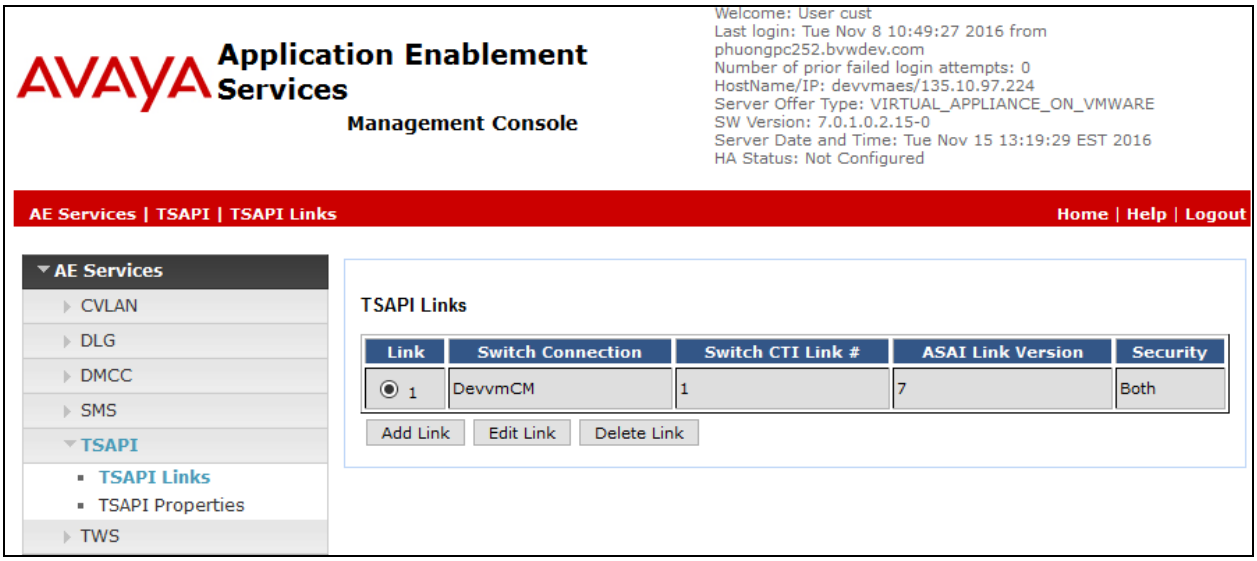
The **WebLM** screen below is displayed. Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

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



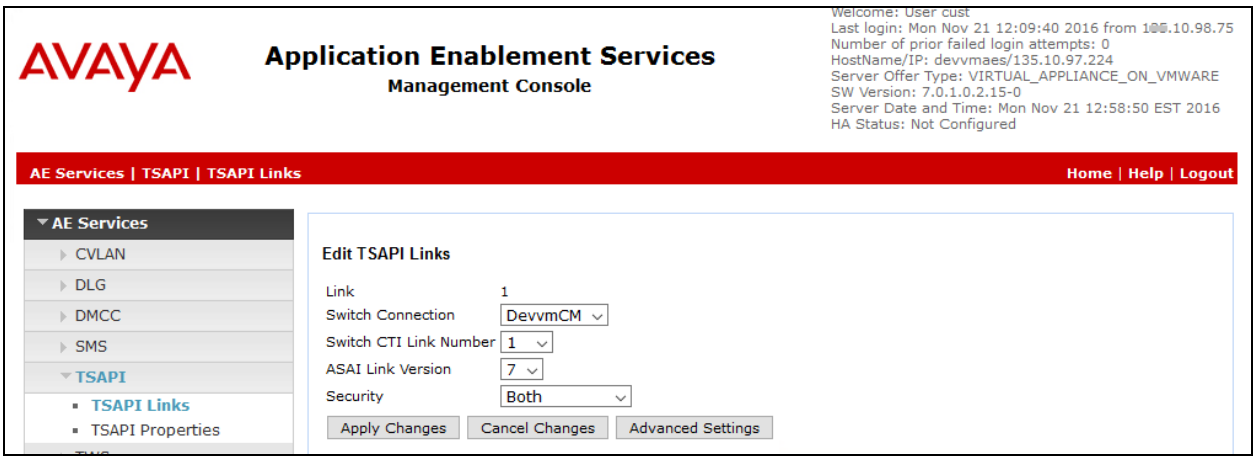
6.3. Administer TSAPI Link

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



The **Add TSAPI Links** screen is displayed next (not shown), below is example of link created during compliance test.

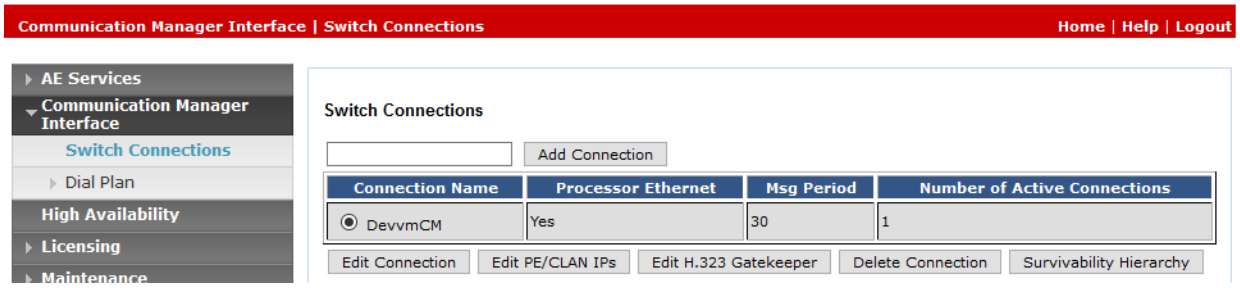
The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "DevvmCM" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.4**. Select "7" for **ASAI Link Version** and select "Both" for **Security.**



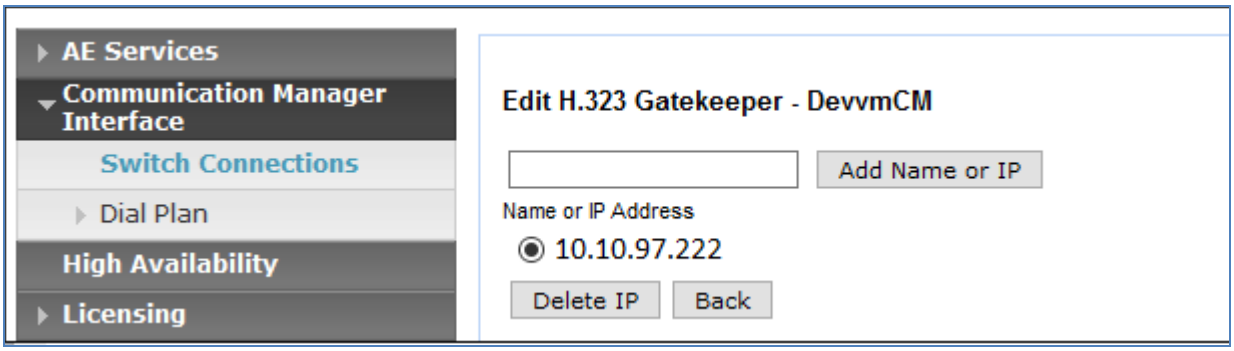
6.4. Administer H.323 Gatekeeper

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 "S8300D", and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

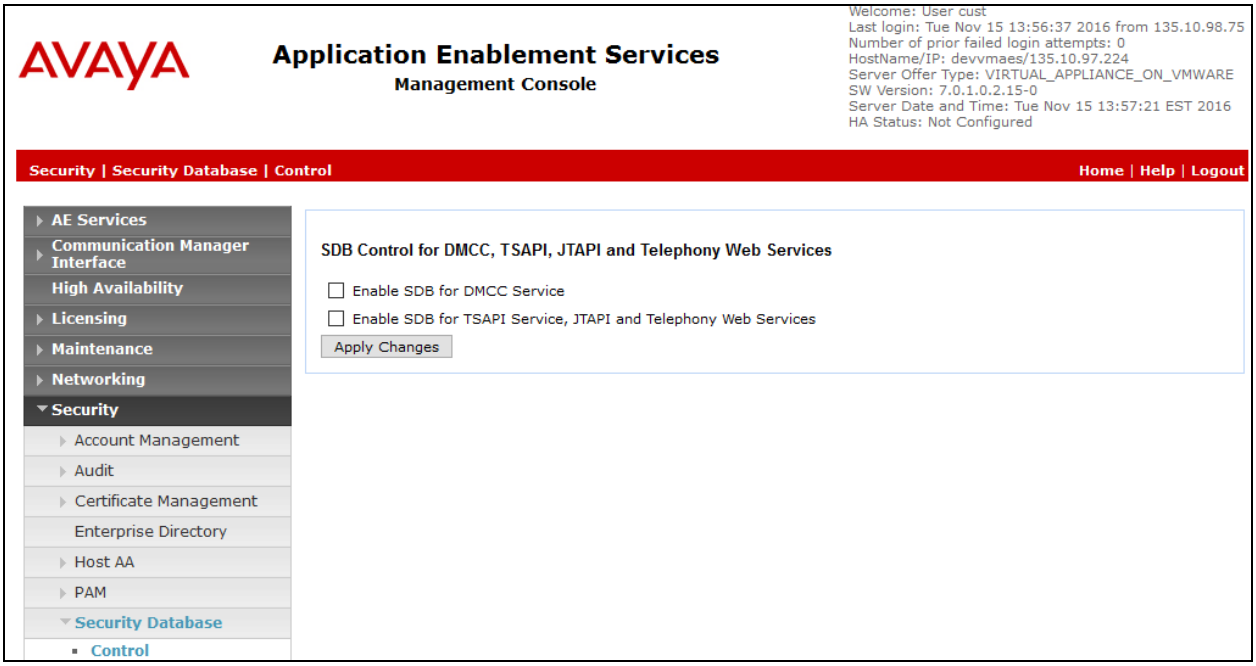


The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as H.323 gatekeeper click **Add Name or IP**. Example below is **H323 Gatekeeper** already create with IP address of Communication Manager 10.10.97.222



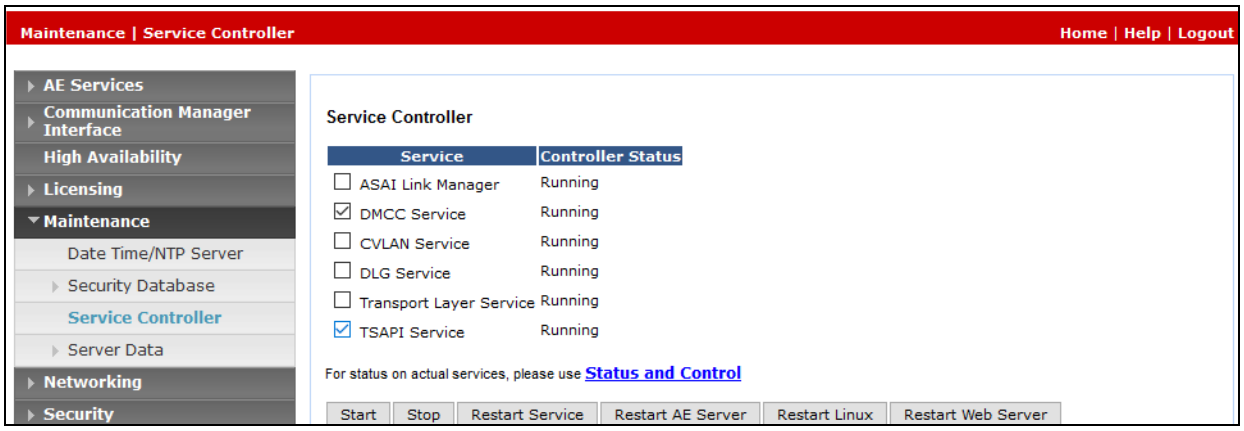
6.5. Disable Security Database

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



6.6. Restart Services

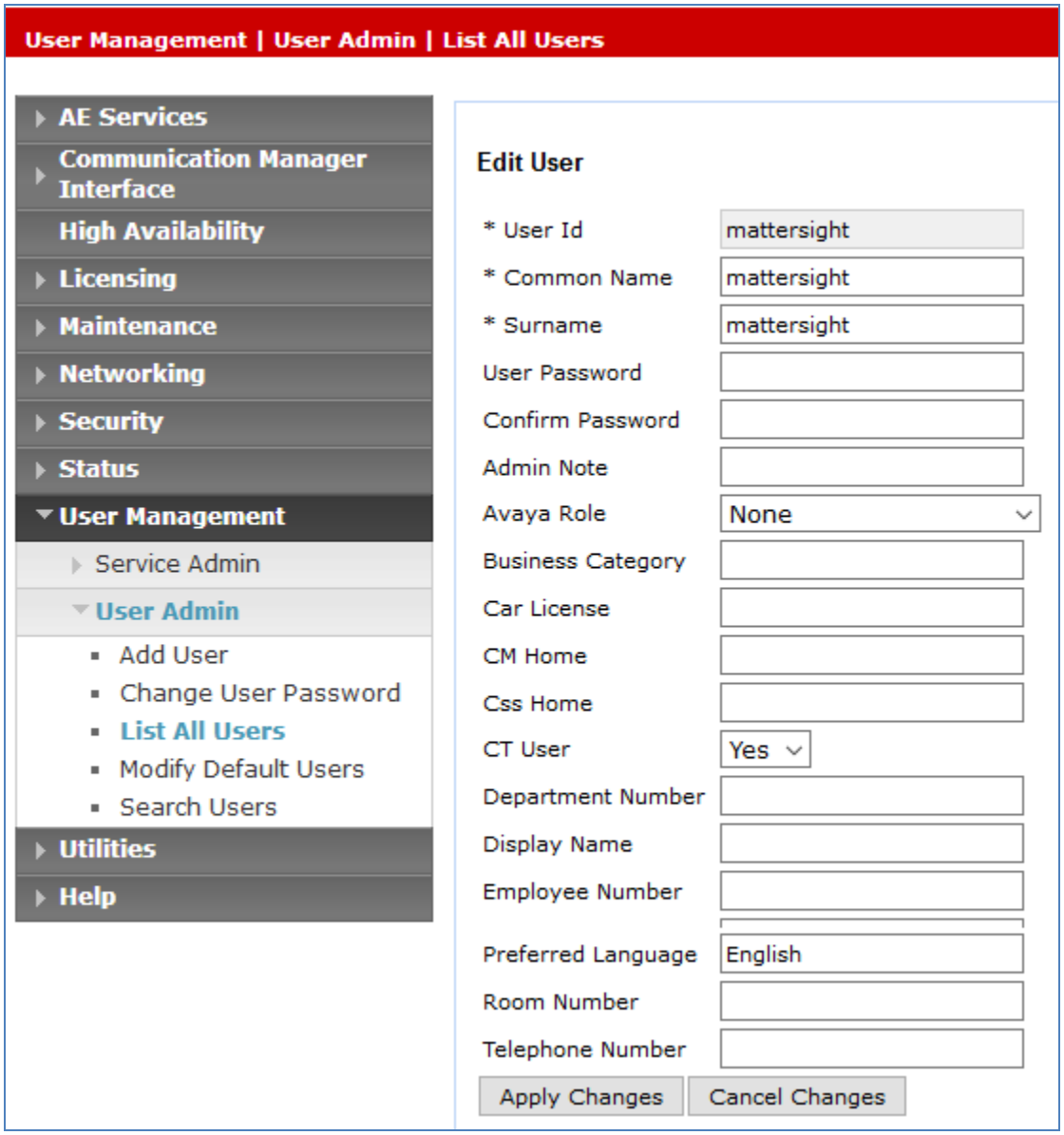
Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service**, and click **Restart Service**.



6.7. Administer Call Recording Solution User

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

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select "Yes" from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen. Below is screenshot of user mattersight created during compliance tested.



6.8. Provide Call Recording Solution User unrestricted access

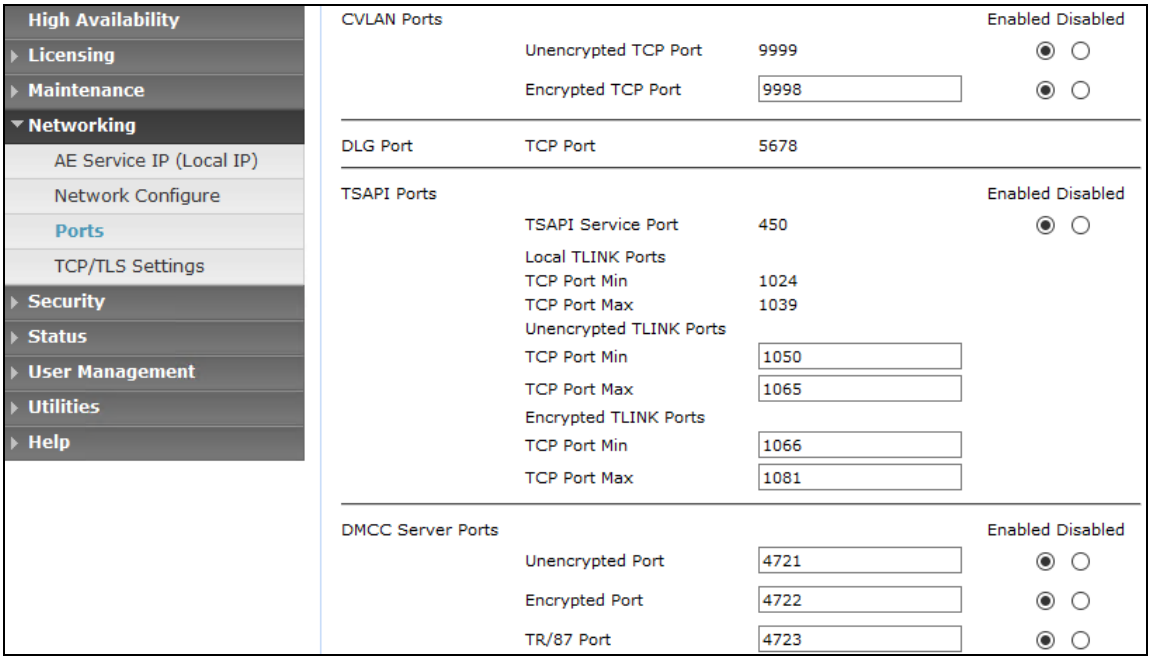
Select **Security → Security Database → CTI Users → List All Users** from the left pane to display the list of CTI users in the right pane (not shown). Under the user list select the user created in the previous step and click on Edit at the bottom of the page. In the User Profile section check the box for the Unrestricted Access.

This will allow the CTI user access to all devices on this AES server.

6.9. Administer Ports

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

In the **DMCC Server Ports** sub-section, select the radio button for **Unencrypted Port** under the **Enabled** column, and make a note of the port value to be used later to configure Call Recording Solution. Retain the default values in the remaining fields. Click **Apply Changes** at the bottom of the screen (not shown below).



7. Configure Mattersight Call Recording Solution

This section provides the procedures for configuring Call Recording Solution. The procedures include the configuration of the WorkerSettings.config file.

The configuration of Call Recording Solution is performed by Mattersight technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Administer WorkerSettings

In the WorkerSettings file configure the following parameters in order for Mattersight to communicate with Application Enablement Service:

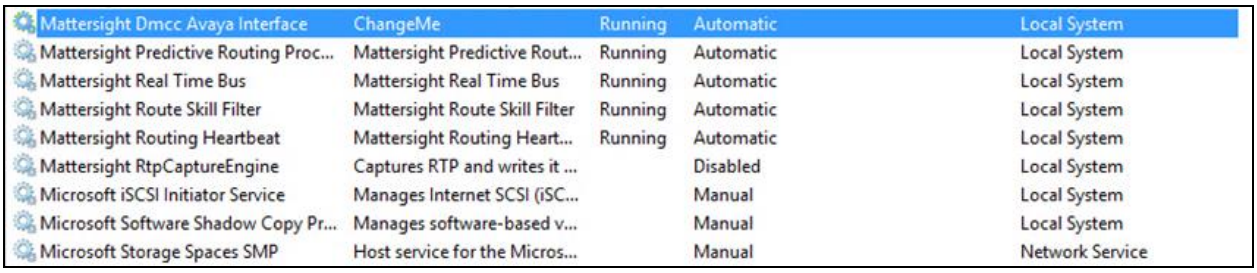
- **RecordingExtensions**: Enter virtual extension created in **Section 5.8**.
- **CmIpAddresses**: Enter IP address of Communication Manager.
- **RtpIpAddress**: Enter IP address of Mattersight server
- **AesIpAddress**: Enter IP address of Application Enablement Service.
- **AesSoketPort**: Enter port in **Section 6.9**.
- **DmccUserName**: Enter user name create in **Section 6.7**.
- **DmccPassword**: Enter password created in **Section 6.7**.
- **Codec**: Enter codec used for recording
- **Mode**: Enter the interface mode, in this case it is SO.
- **FAC**: Enter Feature Access code for Service Observer configured in **Section 5.2**.

```
<workerSettings>
  <add key="EndpointsToPublishTo" value="tcp://127.0.0.1:56000" />
  <add key="EndpointsToSubscribeTo" value="tcp://127.0.0.1:56001" />
  <add key="ExtensionsWhitelist" value="" />
  <add key="RecordingExtensions" value="56114-56115" />
  <add key="CmIpAddress" value="1[illegible].10.97.222" />
  <add key="StartPort" value="4800" />
  <add key="RtpIpAddresses" value="1[illegible].10.97.252" />
  <add key="AesIpAddress" value="1[illegible].10.97.224" />
  <add key="AesSocketPort" value="4721" />
  <add key="DmccUserName" value="mattersight" />
  <add key="DmccPassword" value="mattersight" />
  <add key="ProtocolVersion" value="http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv6"/>
  <add key="RecordOnlyAgentToAgent" value="false" />
  <add key="Codec" value="g711U" /><!--g711U, g729, g711A-->
  <add key="Mode" value="SO"/><!--MR (multi registration), SSC (single step conf), SO (Service Observe)  -
  <add key="StationPassword" value="1234" />
  <add key="FAC" value="*43" /><!--feature access code for service observe-->
  <add key="ServerPingIntervalInSecs" value="10" />
  <add key="ReconnectDelayInMins" value="2" />
</workerSettings>
```

Close the file and save all of the configuration changes.

7.2. Administer Service

In Services window, verify Mattersight Dmcc Avaya Interface is running as shown below (this is performed by the Mattersight team):



Mattersight Dmcc Avaya Interface	ChangeMe	Running	Automatic	Local System
Mattersight Predictive Routing Proc...	Mattersight Predictive Rout...	Running	Automatic	Local System
Mattersight Real Time Bus	Mattersight Real Time Bus	Running	Automatic	Local System
Mattersight Route Skill Filter	Mattersight Route Skill Filter	Running	Automatic	Local System
Mattersight Routing Heartbeat	Mattersight Routing Heart...	Running	Automatic	Local System
Mattersight RtpCaptureEngine	Captures RTP and writes it ...		Disabled	Local System
Microsoft iSCSI Initiator Service	Manages Internet SCSI (iSC...		Manual	Local System
Microsoft Software Shadow Copy Pr...	Manages software-based v...		Manual	Local System
Microsoft Storage Spaces SMP	Host service for the Micros...		Manual	Network Service

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1      7        no     devaes       established       26       20
```

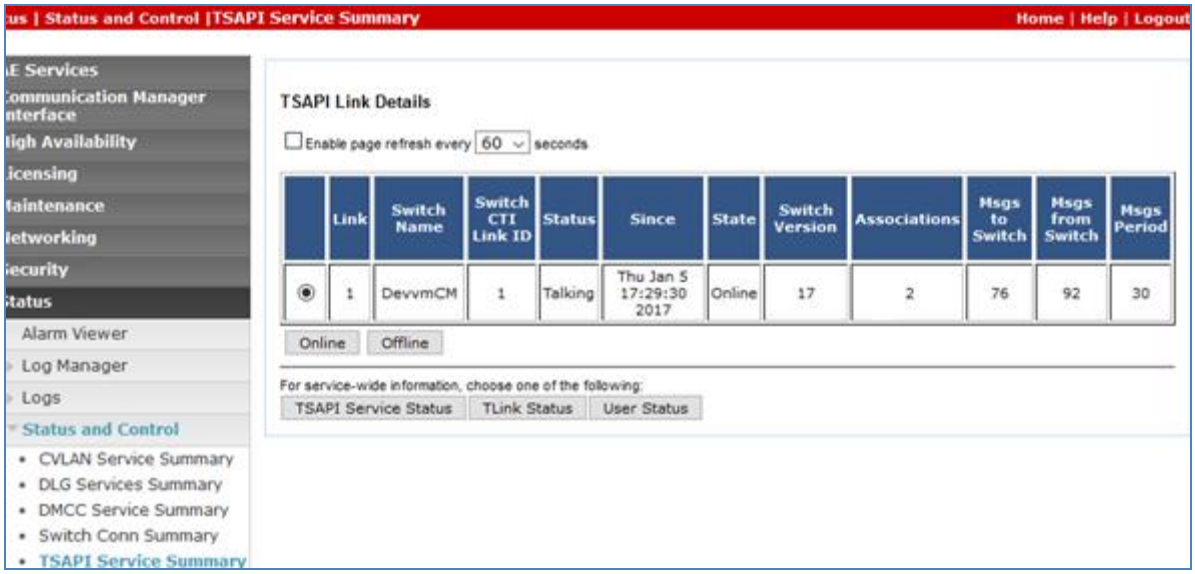
Verify the registration status of the virtual softphones by using the "list registered-ip-stations" command. Verify that all virtual extensions from **Section 5.8** are displayed, as shown below.

```
list registered-ip-stations                                          Page   1

                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/       Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ---------------------------------------
56101         9608      IP_Phone   tcp 10.33.5.29
              1         6.6229         10.10.97.222
56114         9620      IP_API_A   tcp 10.10.97.224
              1         3.2040         10.10.97.222
56115         9620      IP_API_A   tcp 10.10.97.224
              1         3.2040         10.10.97.222
```

8.2. Verify Avaya Aura® Application Enablement Services

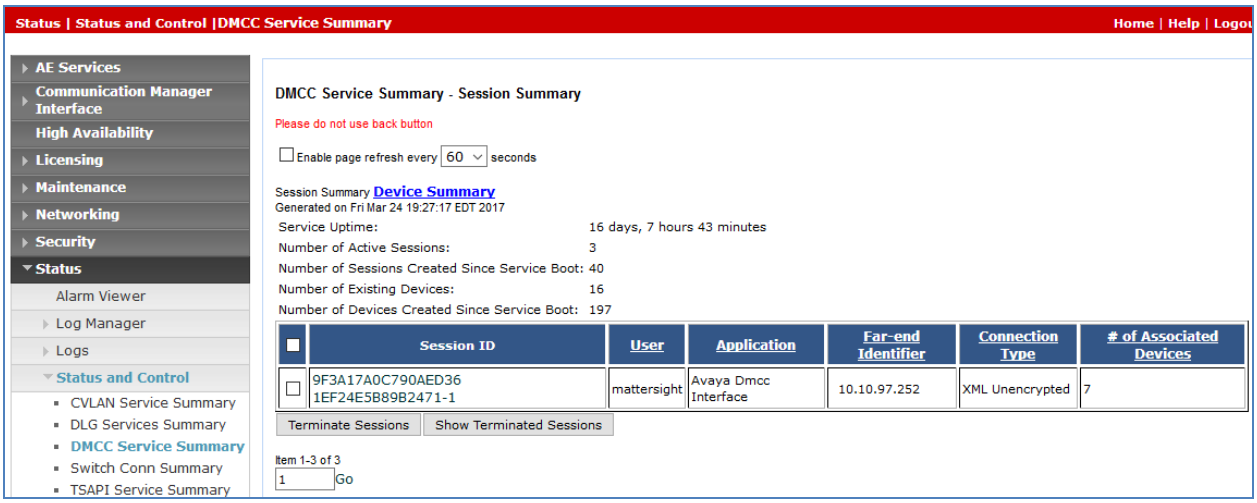
On Application Enablement Services, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is "Talking" for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the number of monitored skill group and agent station extensions from **Section 3**.



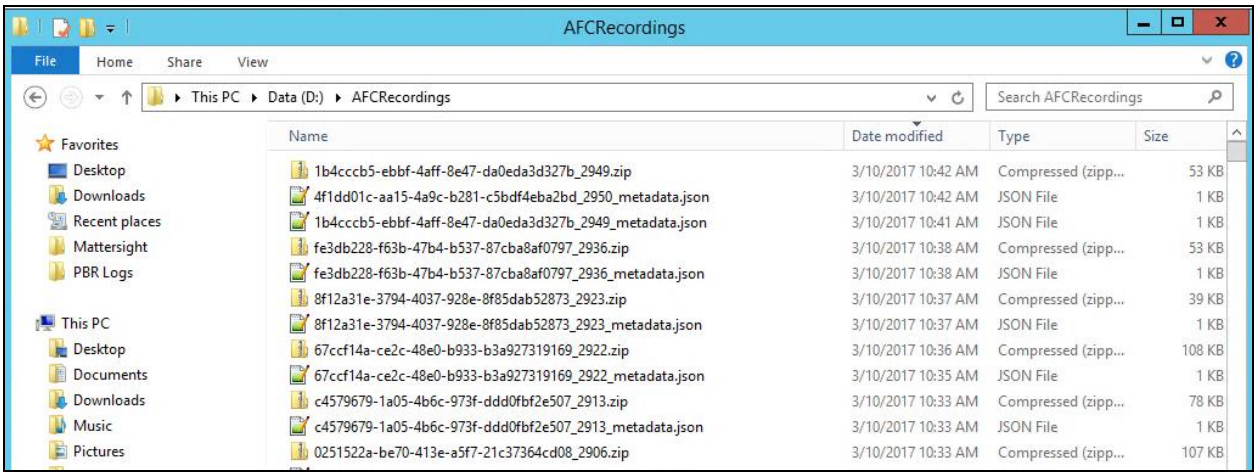
Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows an active session with the Call Recording Solution user name from **Section 6.7**, and that the **# of Associated Devices** column reflects the number of monitored skill group, agent station extensions, and virtual IP softphone extensions.



8.3. Verify Mattersight Call Recording Solution

In the AFCRecordings folder, select the entry and verify that the call recording can be played back and play the correct media.



9. Conclusion

These Application Notes describe the configuration steps required for Mattersight Call Recording Solution 4.0 to successfully interoperate with Avaya Aura® Communication Manager 7.0.2 using Avaya Aura® Application Enablement Services 7.0.1 SP3. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

10. Additional References

This section references the product documentation relevant to these Application Notes can be found on support.avaya.com:

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1 555-245-205 Issue 3 October 2016.

2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 7.0.1 Issue 2 August 2016.

Mattersight document is available upon request.

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.