DevConnect Program

Application Notes for CallCabinet SSC Recorder with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Single Step Conference – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate CallCabinet SSC Recorder 3.0.1.5 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1 using Single Step Conference. CallCabinet SSC Recorder is a cloud-based call recording solution.

In this compliance test, CallCabinet SSC Recorder used the Device, Media, and Call Control interface of Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager and used the Single Step Conference method to capture media associated with the monitored agent stations for stereo call recording. The solution supports both mono and stereo 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.

1. Introduction

These Application Notes describe the configuration steps required to integrate CallCabinet SSC Recorder with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Single Step Conference. CallCabinet SSC Recorder is a cloud-based call recording solution.

In this compliance test, CallCabinet SSC Recorder used the Device, Media, and Call Control (DMCC) interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager and used the Single Step Conference method to capture media associated with the monitored agent stations for stereo call recording. Stereo call recording is suited for analytics, speech recognition, and transcription applications. The solution supports both mono and stereo call recording.

CallCabinet SSC Recorder is comprised of two applications, the SSC Recorder and the RTP Recorder. When there is an active call at the monitored agent station, SSC Recorder application is informed of the call via event reports from the DMCC interface using an encrypted DMCC link. SSC Recorder starts the stereo call recording(s) by using the Single Step Conference method to add a virtual IP softphone to the active call at the agent to obtain the media. The event reports are also used to determine when to stop the call recordings. The RTP Recorder applications captures the SRTP audio and uploads it to the cloud. Per design, the audio of all active calls on a monitored agent station are captured in the same call recording. The CallCabinet SSC Recorder Portal allows play back of all call recordings logged with call details, such as time, duration, calling and called party, agent ID, queue ID, and more.

In these Application Notes, SSC Recorder refers to the complete call recording solution, not simply the SSC Recorder application mentioned above, unless otherwise specified.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on SSC Recorder using DMCC to perform device queries, monitor skill groups and agent stations, register the virtual IP softphones, and use Single Step Conference for call recordings. Each call to an agent station was recorded in stereo and stored in the cloud and the SSC Recorder Portal allowed the call recordings to be played back. Various call scenarios, such as hold/resume, call transfers, and conferences were exercised to verify proper call recording.

Test verification also included the use of Application Enablement Services and SSC Recorder logs to verify the message exchanges and the use of SSC Recorder Portal to verify the proper logging and playback of calls.

The serviceability testing focused on verifying that SSC Recorder returned to service after busying out and releasing the CTI link between Communication Manager and Application Enablement Services and restarting the DMCC and TSAPI services on Application Enablement Services.

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 Avaya systems and CallCabinet SSC Recorder utilized encrypted DMCC and SRTP.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Use of DMCC to monitor skill groups and agent stations, register virtual IP softphones, and activate Single Step Conference.

- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711, forwarding, service observing, auto answer, RONA, long duration, multiple calls, multiple agents, conference, and transfer. The solution supports both G.711 and G.729 for RTP and G.711 for SRTP.

- The use of an encrypted DMCC link between Application Enablement Services and SSC Recorder and stereo call recordings using SRTP. The solution supports both mono and stereo recording.

The serviceability testing focused on verifying the ability of SSC Recorder to recover from adverse conditions, such as restarting the CTI link and the DMCC and TSAPI services on Application Enablement Services.

2.2. Test Results

All test cases passed with the following observation:

- The association of an agent station to Agent ID persists in the SSC Recorder Portal call listing after the agent has logged out.

- The Queue ID in the SSC Recorder Portal call listing shows the hunt group ID when the agent is logged into the ACD queue and is blank when the agent is logged out. The Queue ID is also blank when a direct call (i.e., non-ACD call) is placed to an agent station without the call being routed through a VDN or hunt group or for outgoing calls from an agent station.

2.3. Support

Technical support on CallCabinet SSC Recorder may be obtained through the following:

- **Phone:** (800) 653-1389
- **Web:** https://support.callcabinet.com

3. Reference Configuration

The configuration used for the compliance test is shown in **Figure 1**. The configuration consisted of a basic call center with a skill group and agent stations being monitored by SSC Recorder in the cloud using an encrypted DMCC link and recording two-way, SRTP audio of active calls on monitored agent stations in stereo. The SSC Recorder Portal allowed the logging and play back of call recordings.

In the compliance Test, SSC Recorder monitored skill groups and agent stations shown in the table below.

Device Type	Extension
Skill Group	77500
Agent Stations	77301 (H.323), 78004 (SIP)
Agent IDs	76301, 76302

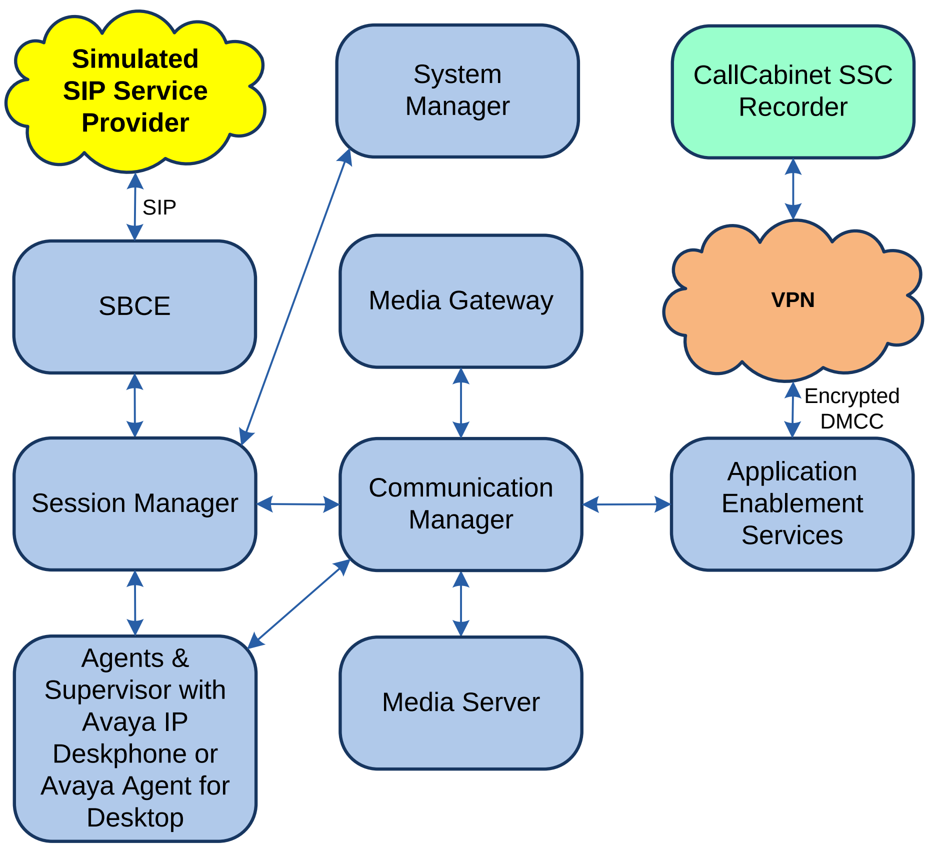


Figure 1: Avaya Aura® Call Center with CallCabinet SSC Recorder in the Cloud

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	10.1.2.0.0-FP2
Avaya G430 Media Gateway	FW 42.8.0
Avaya G450 Media Gateway	FW 42.7.0
Avaya Aura® Media Server	10.1.0.77
Avaya Aura® Application Enablement Services	10.1.0.2.0.12-0)
Avaya Aura® System Manager	10.1.2.0 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.2.0.0-071476 Feature Pack 2
Avaya Aura® Session Manager	10.1.2.0.1012016
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872
Avaya 96x1 Series Deskphones	6.8.5.4.10 (H.323)
Avaya J100 Series Telephones	4.0.13.0.6 (SIP)
Avaya Agent for Desktop	2.0.6.25.3006 (SIP)
CallCabinet SSC Recorder	3.0.1.5

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 virtual IP softphones

Note: It is assumed that the configuration of a basic call center, including VDN, skill group, agent stations, and agent login IDs, is already in place and will not be covered in these application notes.

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 enabled, contact an authorized Avaya sales representative to make appropriate changes.

```
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
```

5.2. Administer CTI Link

Add a CTI link using the **add cti-link** command. 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: 77700
     Type: ADJ-IP
                                                                       COR: 1
     Name: AES TSAPI Link
Unicode Name? n
```

5.3. Administer IP Codec Set

Use the **change ip-codec-set** command to access the **IP Codec Set** form to select the audio codec and media encryption for agents calls and call recording using virtual IP softphones. SSC Recorder supports G.711 with stereo call recording and SRTP using *1-srtp-aescm128-hmac80*. SSC Recorder also supports G.729 with RTP.

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

                          IP MEDIA PARAMETERS
    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 SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3: none
 4:
 5:
```

5.4. Administer Virtual IP Softphones

Add a virtual IP softphone using the **add station** command. Enter the following values for the specified fields and retain the default values for the remaining fields. For the compliance test, eight virtual IP softphones were created with extensions 77951 to 77958. SSC Recorder registers two device instances per virtual IP softphone for stereo call recording and uses Single Step Conference to join one virtual IP softphone to an active call for call recording.

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as "9608".
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **IP SoftPhone:** "y"

```
add station 77951                                               Page   1 of   5
                                     STATION

Extension: 77951                         Lock Messages? n             BCC: 0
     Type: 9608                          Security Code: 1234           TN: 1
     Port: IP                          Coverage Path 1:               COR: 1
     Name: SSC Recorder DMCC 1         Coverage Path 2:               COS: 1
Unicode Name? n                      Hunt-to Station:               Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                             Message Lamp Ext: 77951
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english                 Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

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

                                              Customizable Labels? Y
```

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

```
list station 77951 count 8                                          Page   1

                                  STATIONS

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

77951            S000057 SSC Recorder DMCC 1                          1
                 9608                      no                        1  1
77952            S000059 SSC Recorder DMCC 2                          1
                 9608                      no                        1  1
77953            S000060 SSC Recorder DMCC 3                          1
                 9608                      no                        1  1
77954            S000061 SSC Recorder DMCC 4                          1
                 9608                      no                        1  1
77955            S000062 SSC Recorder DMCC 5                          1
                 9608                      no                        1  1
77956            S000063 SSC Recorder DMCC 6                          1
                 9608                      no                        1  1
77957            S000064 SSC Recorder DMCC 7                          1
                 9608                      no                        1  1
77958            S000064 SSC Recorder DMCC 8                          1
                 9608                      no                        1  1
```

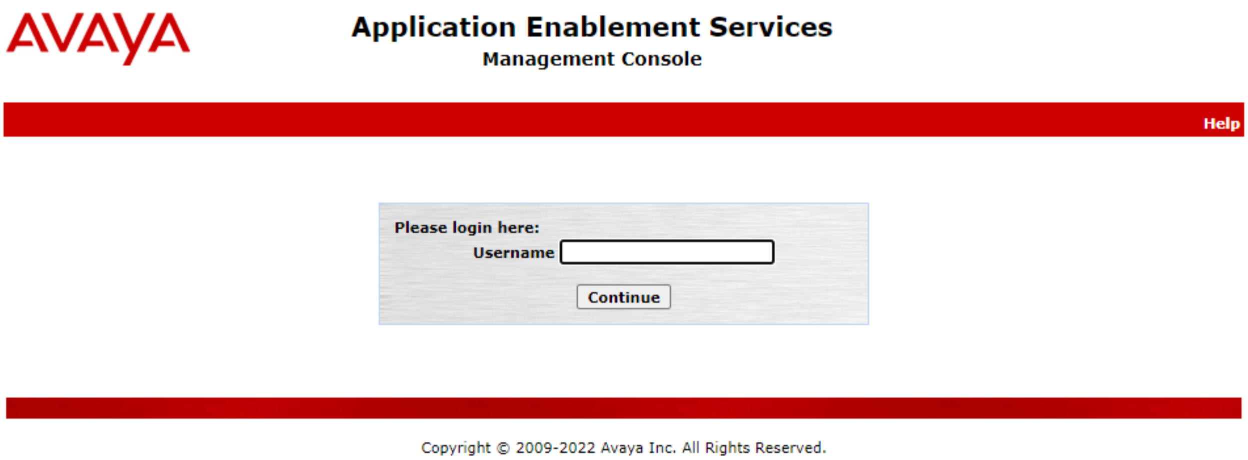
6. Configure Avaya Aura® Application Enablement Services

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

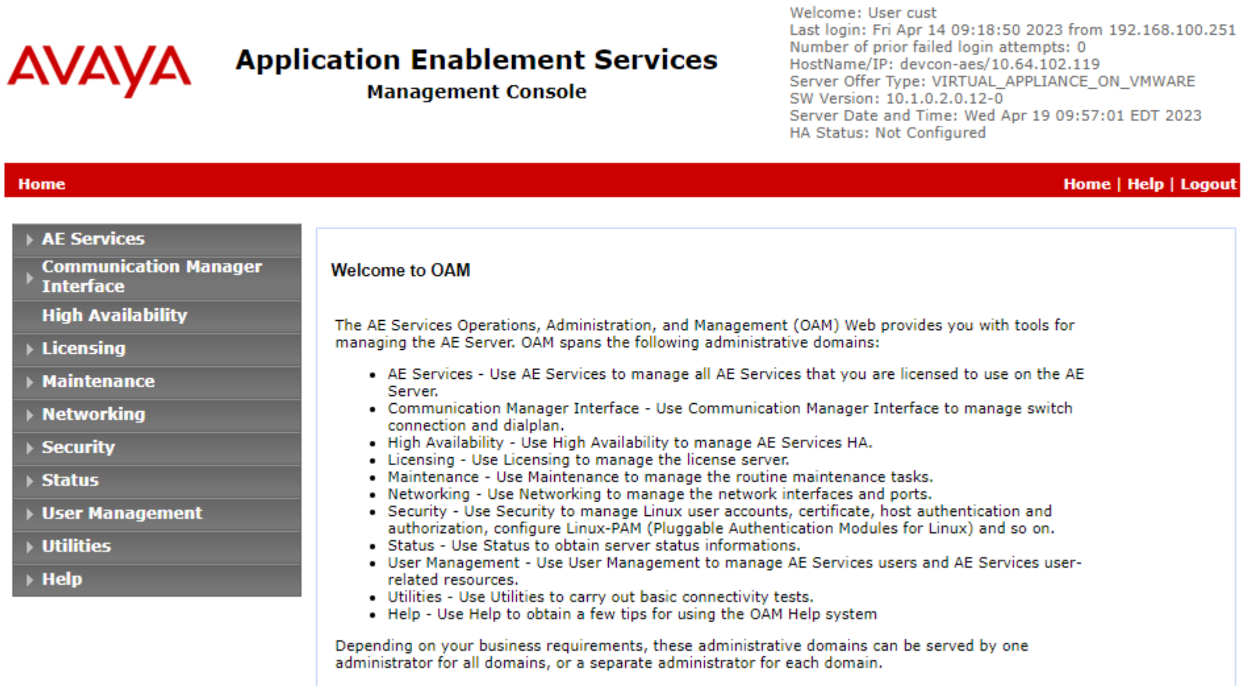
- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer Switch Connection
- Administer SSC Recorder user
- Administer security database
- Administer ports
- Restart services

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 Application Enablement Services. The login screen is displayed. Log in using the appropriate credentials.

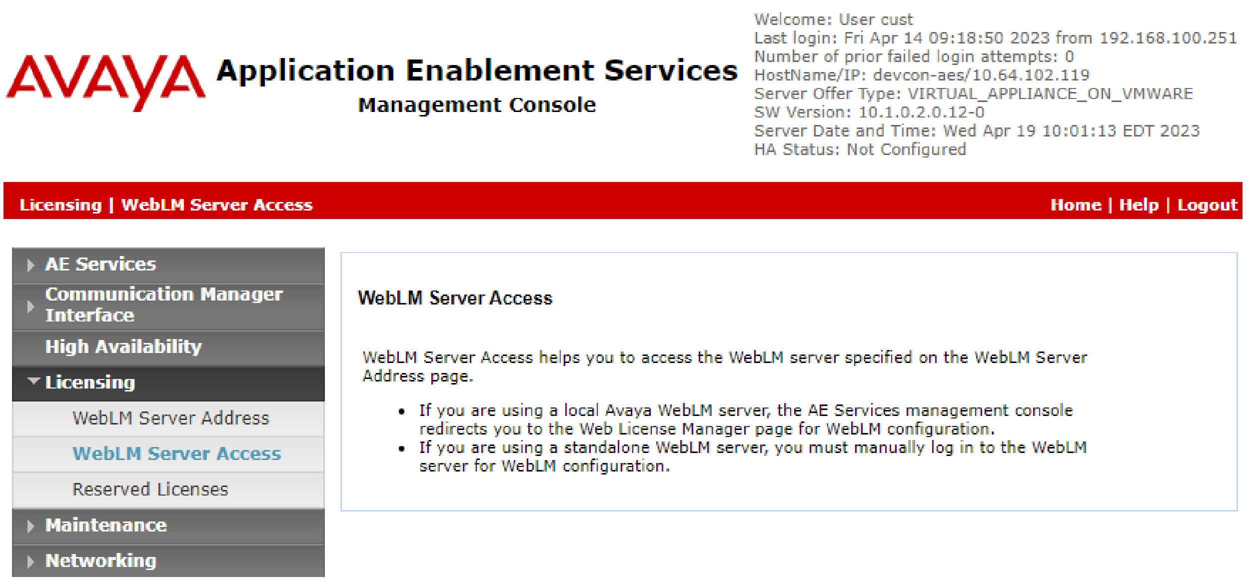


The **Welcome to OAM** screen is displayed next.



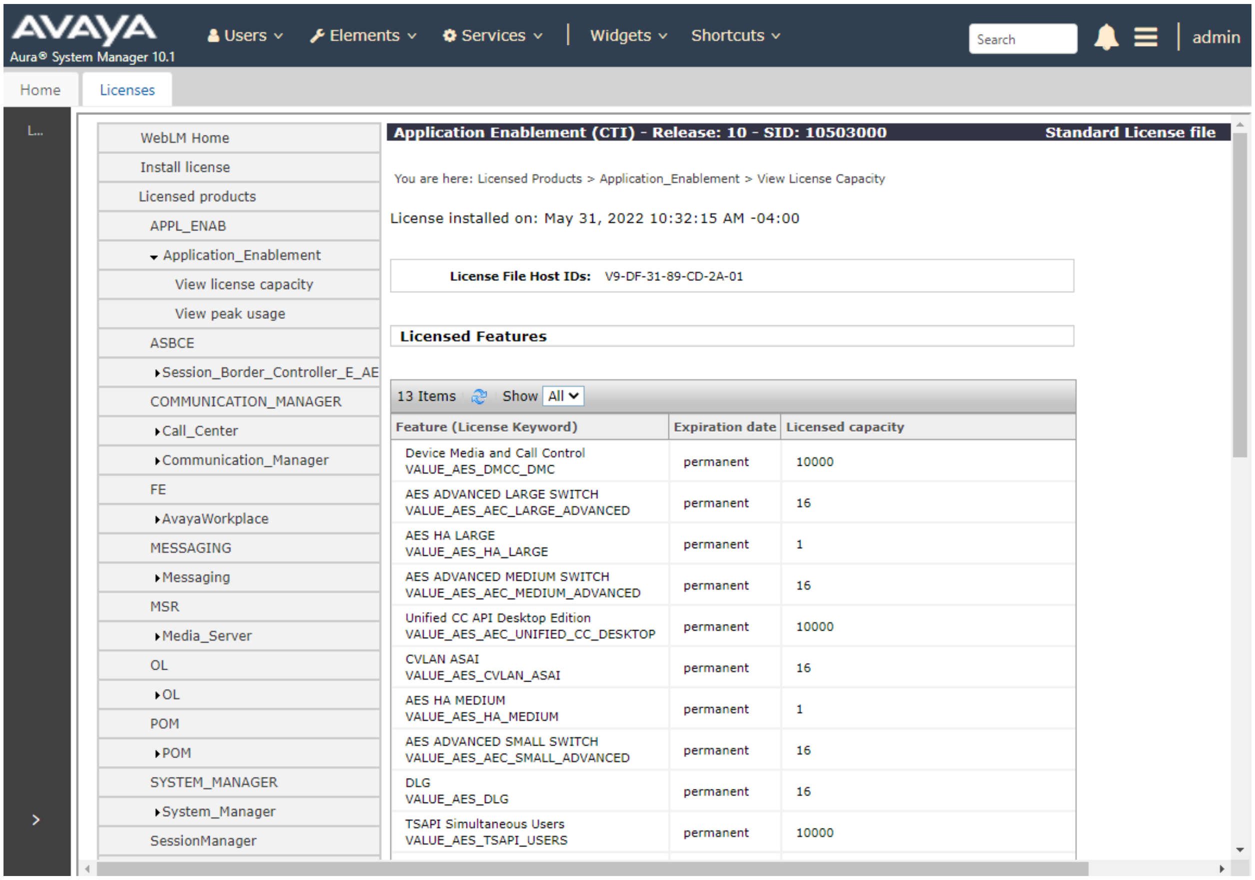
6.2. Verify License

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



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 **Device Media and Call Control** and **TSAPI Simultaneous Users** as shown below. The DMCC license is used for the virtual IP softphones and the TSAPI license is used for device monitoring.



Scrolling down to the **Acquired Licenses** section indicates that for eight virtual IP softphones used for stereo call recording, 16 DMCC licenses are used, and to monitor one skill group and two agent stations, three TSAPI licenses are used as shown below.

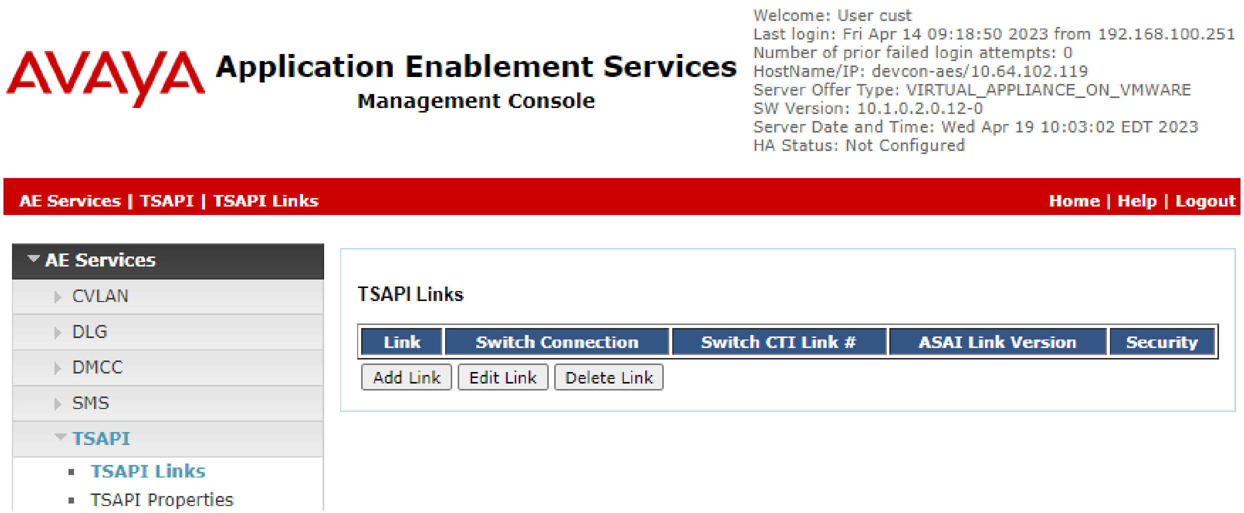
Acquired Licenses

2 Items | Show All

Feature	Acquired by	Acquirer ID	Count
VALUE_AES_DMCC_DMC	DMCC (devcon-aes)	6392456460958976	16
VALUE_AES_TSAPI_USERS	TSAPI (devcon-aes)	devcon-aes:1681483417:2006978:139820032505984:0000	3

6.3. Administer TSAPI Link

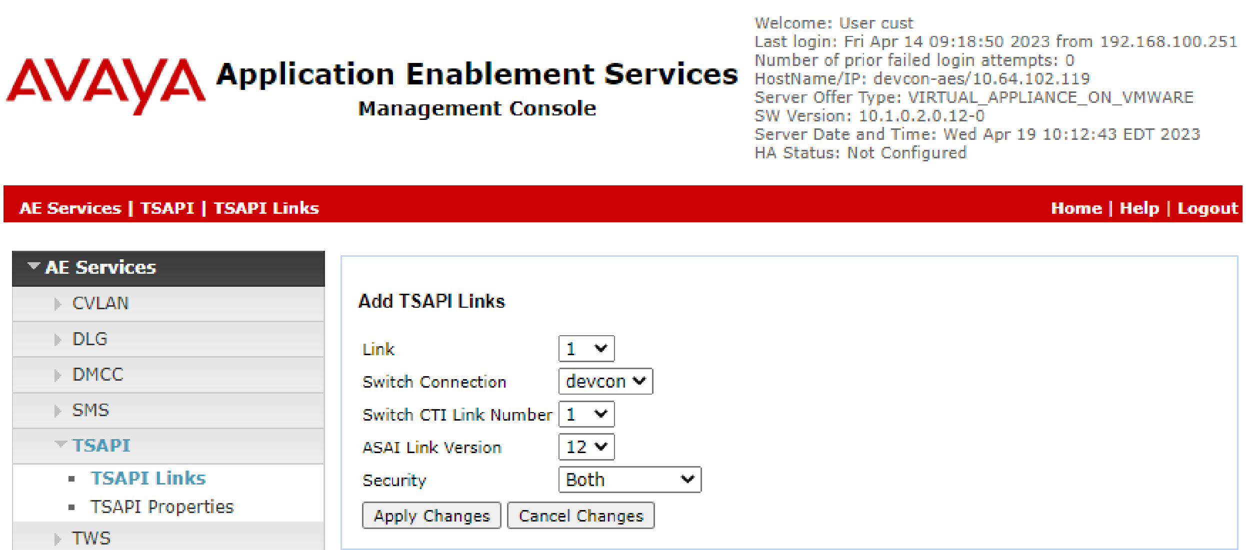
Select **AE Services → TSAPI → TSAPI Links** from the left pane of the **Management Console** to administer a TSAPI link. The **TSAPI Links** screen is displayed as shown below. Click **Add Link**.



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 *devcon* is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**.

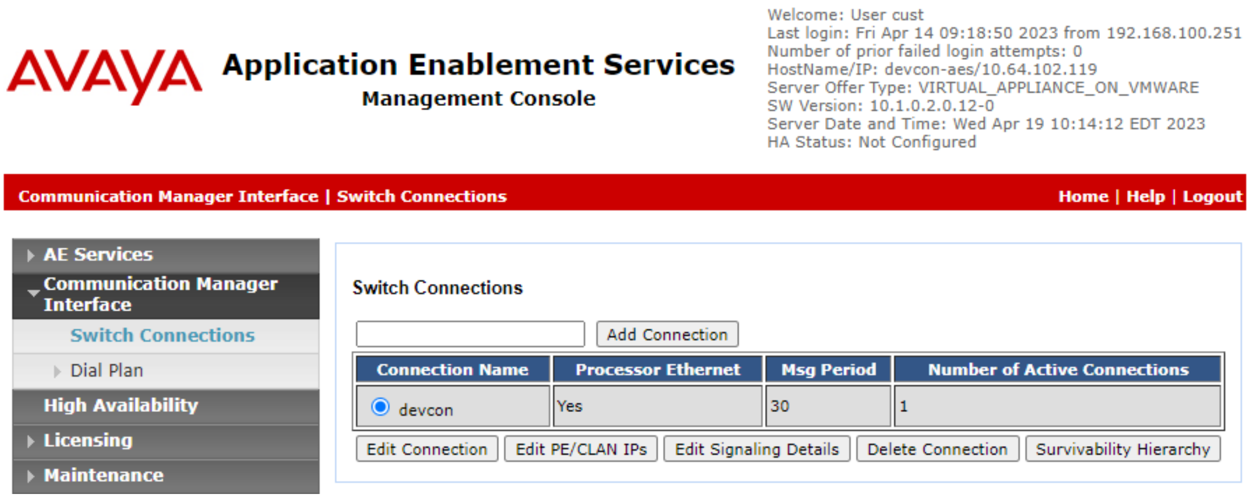
Retain the default value for **ASAI Link Version** and set **Security** to the desired value, in this case *Both* to allow for both encrypted and non-encrypted connections.



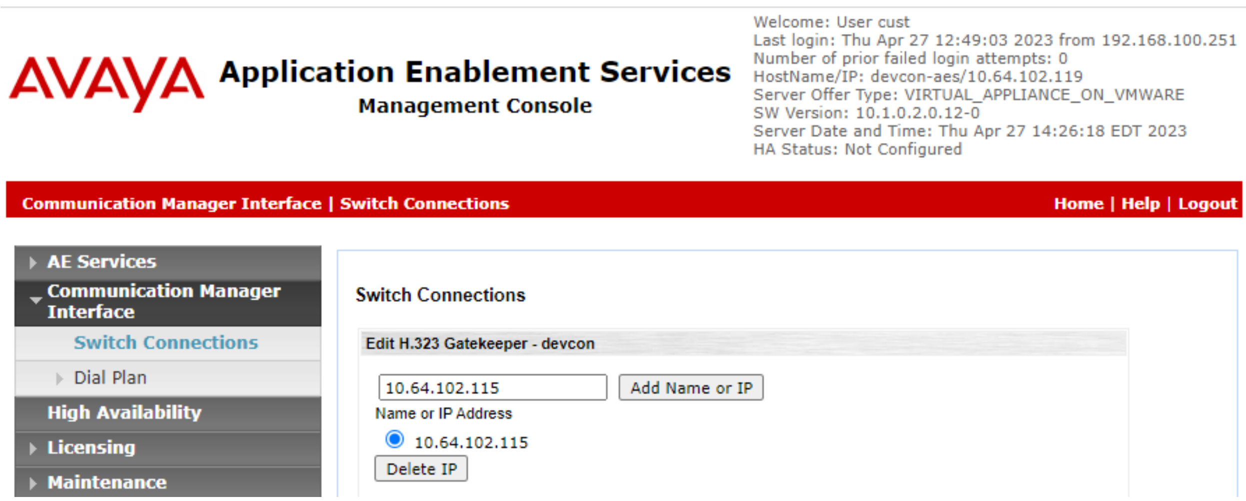
6.4. Administer H.323 Gatekeeper

Select **Communication Manager Interface → Switch Connections** from the left pane. The **Switch Connections** screen shows a list of existing switch connections.

Locate the connection name associated with relevant Communication Manager, in this case *devcon*, and select the corresponding radio button. Click **Edit Signaling Details**.



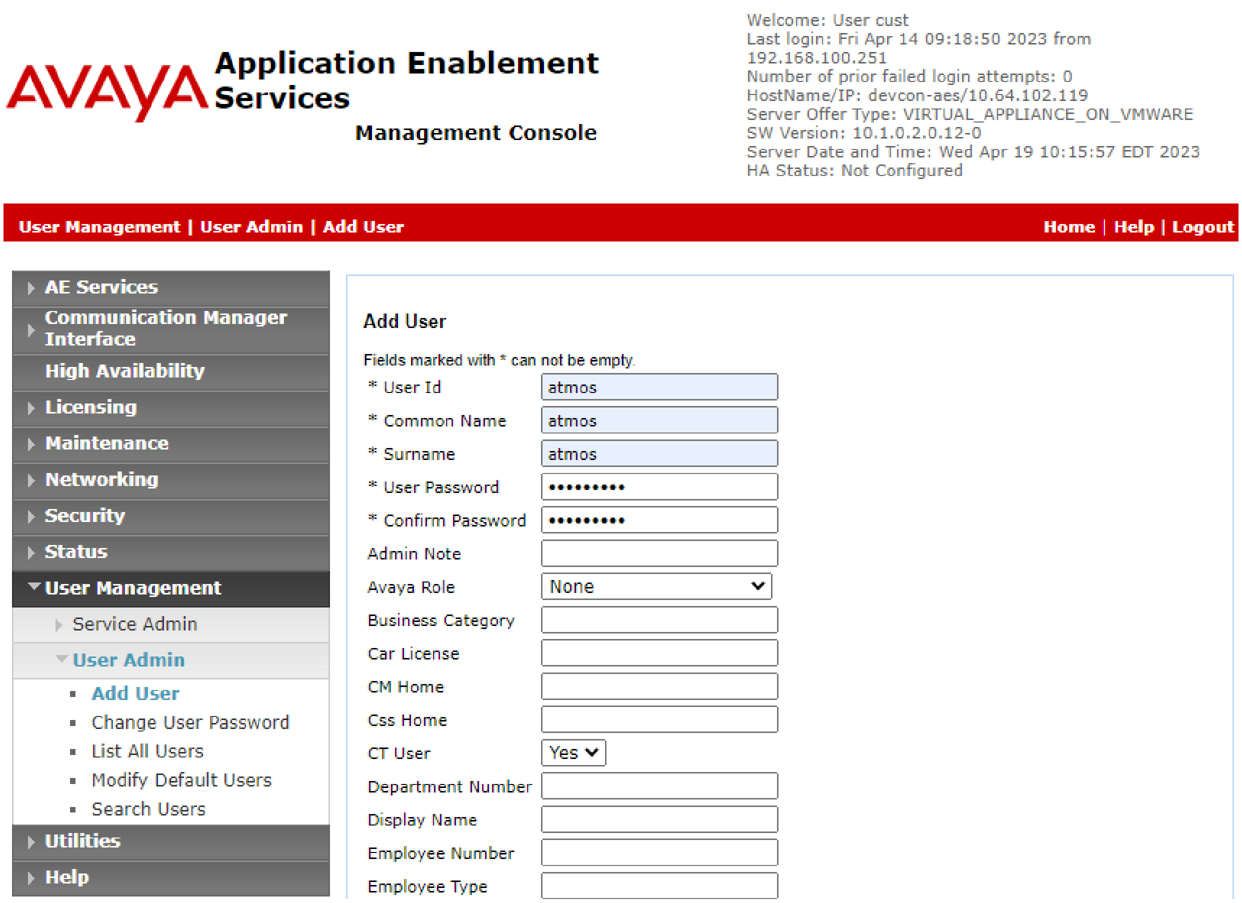
The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of Processor Ethernet on Communication Manager to use as H.323 gatekeeper for registering the virtual IP softphones, in this case *10.64.102.115* as shown below. Click **Add Name or IP**.



6.5. Administer SSC Recorder User

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

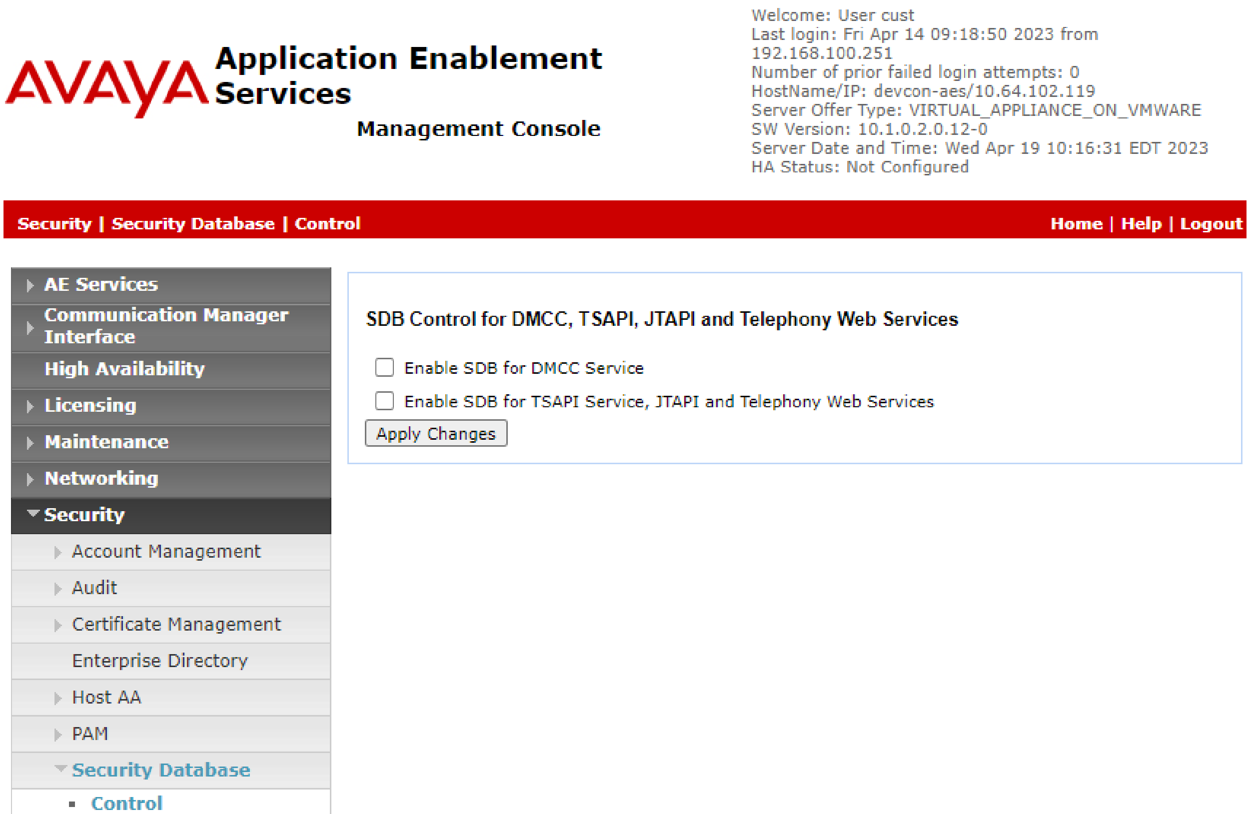
Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields.



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. Make certain that both parameters are unchecked, as shown below.

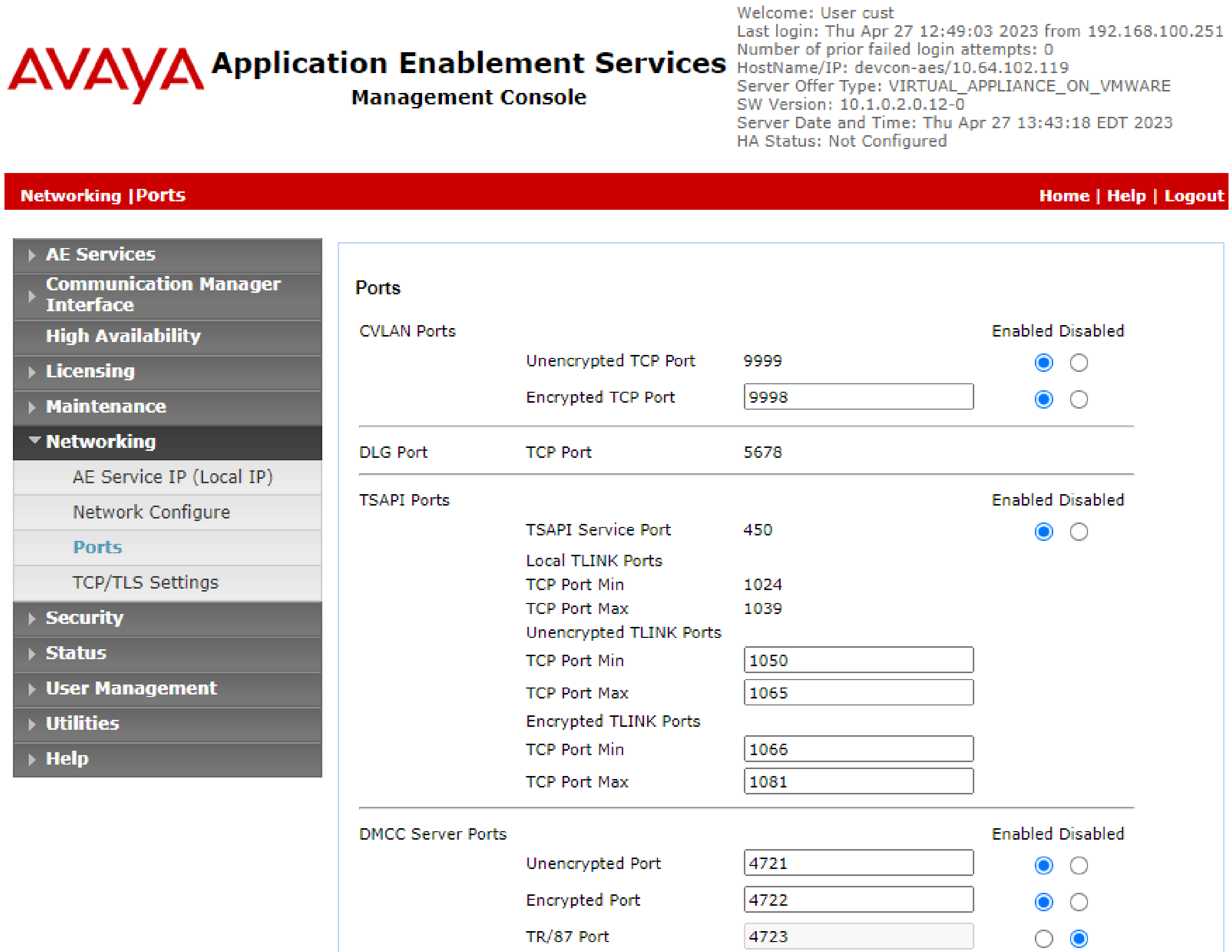
In the case that the security database is used by the customer with parameters already enabled, then follow reference **[2]** to configure access privileges for the SSC Recorder user from **Section 6.5**.



6.7. Administer Ports

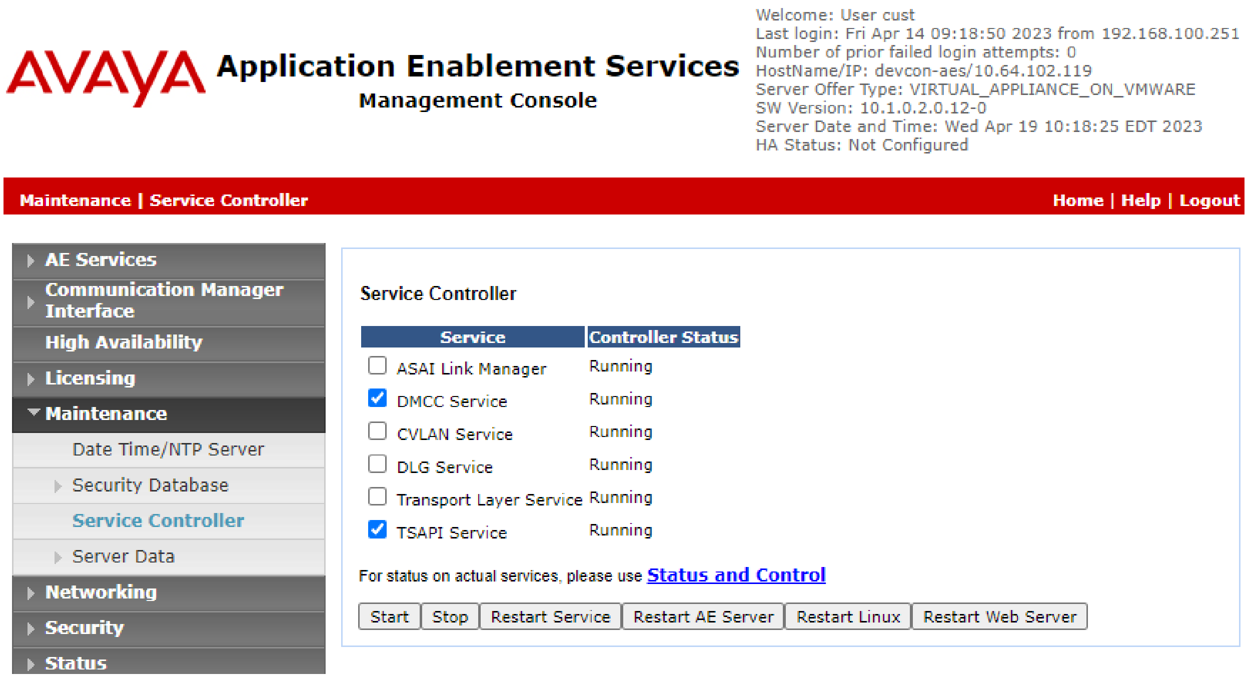
Select **Networking → Ports** from the left pane, to display the **Ports** screen in the right pane.

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



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**.



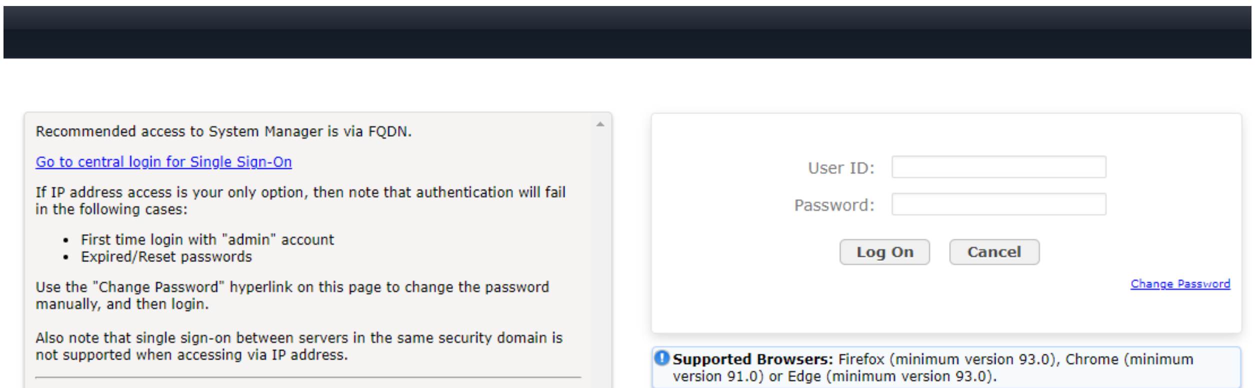
7. Configure Avaya Aura® Session Manager

This section covers the configuration of a SIP user on Session Manager so that Application Enablement Services can monitor the station. The SIP user is configured via the System Manager web interface. The procedure includes the following areas:

- Launch System Manager
- Administer SIP Users

7.1. Launch System Manager

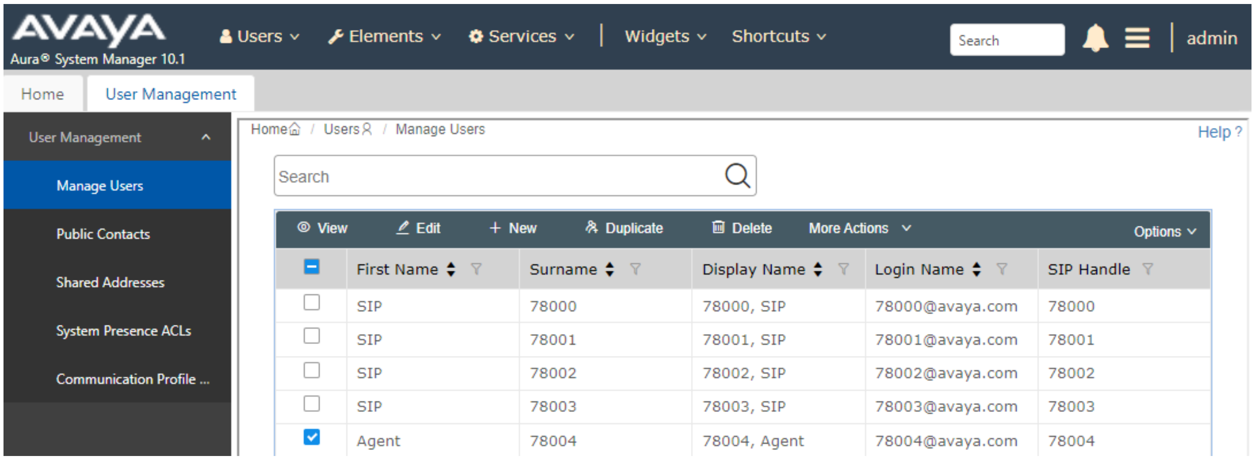
Access the System Manager web interface by using the URL "https://*<ip-address>*" in a web browser window, where *<ip-address>* is the System Manager IP address. Log in using the appropriate credentials.



7.2. Administer SIP Users

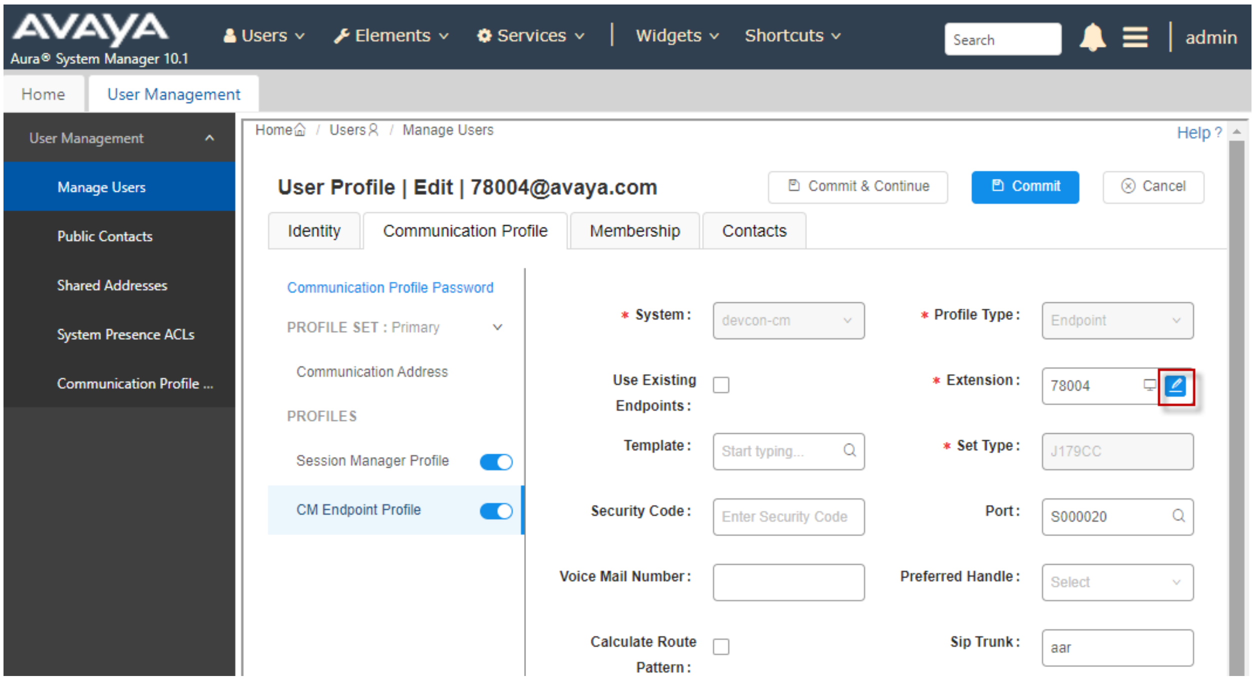
In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below.

Select the entry associated with the first SIP agent station from **Section 3**, in this case *78004*, and click **Edit**.



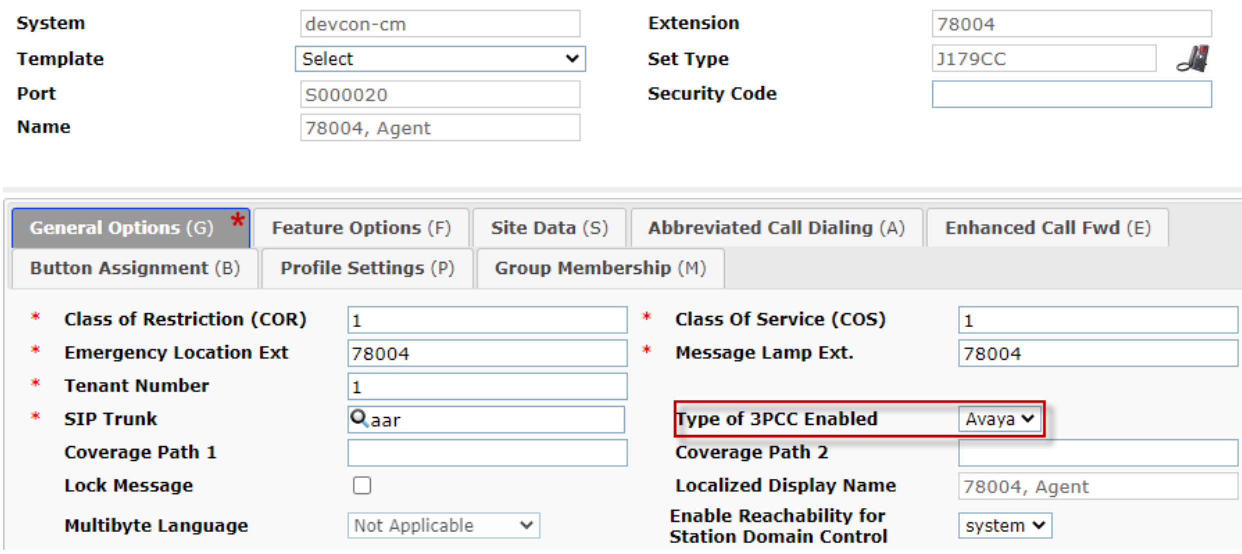
The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section and click **Editor** as shown below.



Select the **General Options** tab. For **Type of 3PCC Enabled**, select *Avaya* as shown below.

Repeat this section for all SIP agent stations from **Section 5.4**. In the compliance test, eight SIP agent stations were configured.



8. Configure CallCabinet SSC Recorder

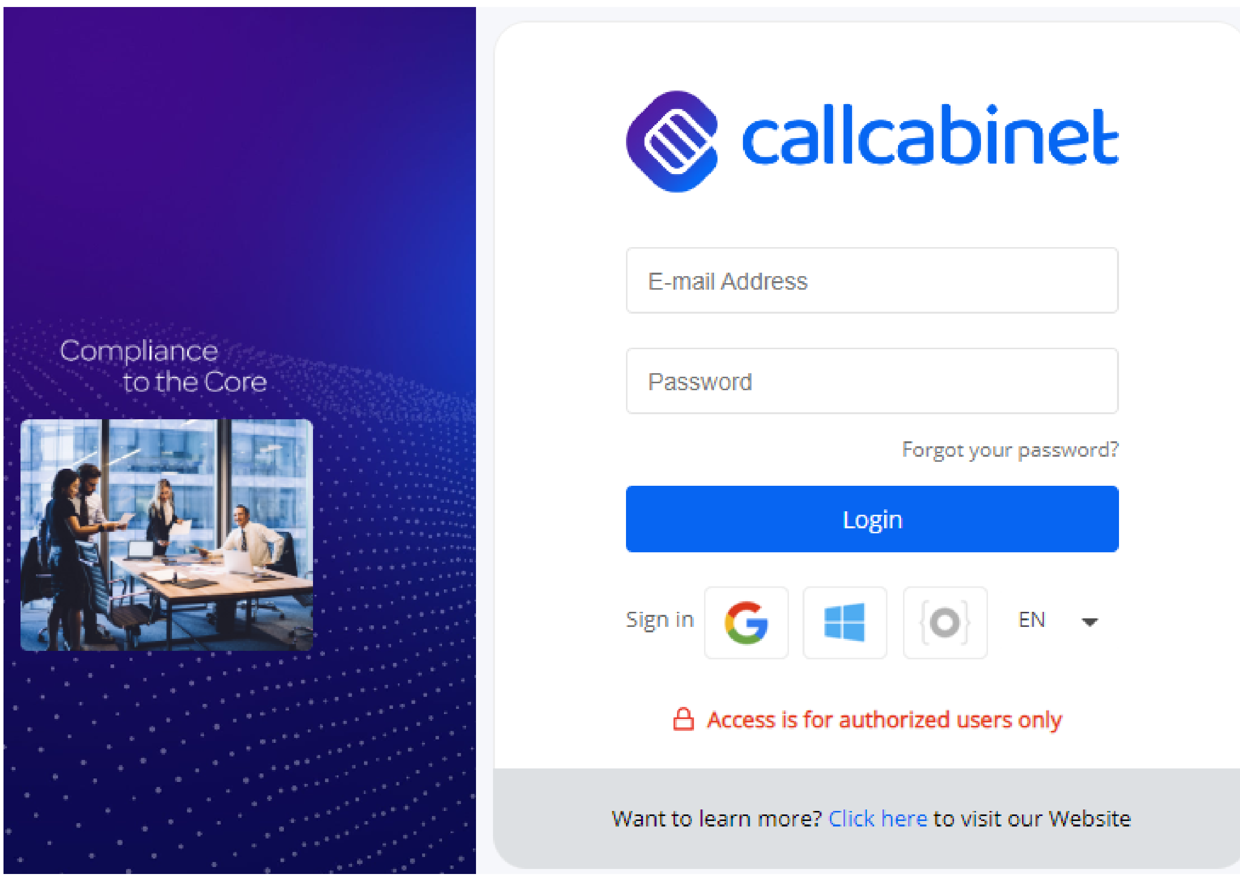
This section covers the configuration of CallCabinet SSC Recorder, which includes the SSC Recorder and RTP Recorder applications.

- Launch SSC Recorder Portal
- Obtain Customer ID and Site ID
- Configure SSC Recorder Application
- Configure RTP Recorder Application
- Install Trusted Certificate
- Start SSC Recorder Windows Services

The configuration of SSC Recorder is performed by CallCabinet personnel. The following configuration steps are presented for informational purposes only.

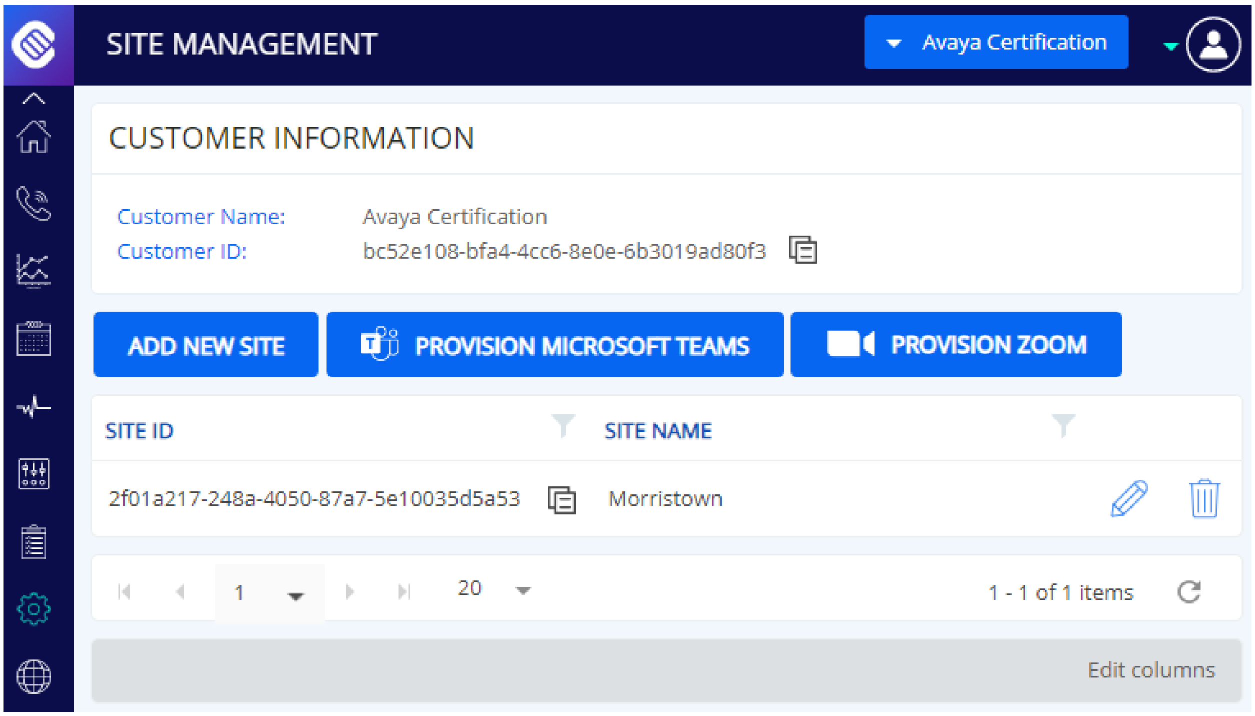
8.1. Launch SSC Recorder Portal

Access the SSC Recorder Portal by using the URL "https://<*company*>*.callcabinet.com*" in a web browser window, where <*company*> is the company URL. Log in using the appropriate credentials.



8.2. Obtain Customer ID and Site ID

Navigate to **Settings → Site Management** to retrieve the customer information, including the **Customer ID** and **Site ID** shown below. Click the icon to the right to copy the data to the clipboard. This information should be added to the RTP Recorder configuration covered in **Section 8.4**.



8.3. Configure SSC Recorder Application

The `app.xml` file for the SSC Recorder application, located in the `CallCabinet\CallCabinetSSCRecorder\bin\` directory, should be modified with the following parameter settings:

- **SwitchNameOrIP:** Set to Communication Manager **Switch Connection** name (e.g., *devcon*) from **Section 6.3.**
- **ServerID:** Set to Application Enablement Services IP address (e.g., *10.64.102.119*).
- **UserName:** Set to CT User configured in **Section 6.5**
- **Password:** Set to CT User password in **Section 6.5**.
- **DMCCPort:** Set to encrypted DMCC port (i.e., *4722*) shown in **Section 6.7**.
- **IsEncryptionEnable:** Set to *true* for encrypted DMCC.
- **AesEncryptionProtocol:** Set to *srtp-aescm128-hmac80*.
- **MediaCodec:** Set to *g711u*.
- **IP:** Set to IP address of SSC Recorder server.
- **Extensions:** Specify the agent stations and skill groups to monitor listed in **Section 3**.
- **Softphones:** Specify the virtual IP softphone extensions and passwords from **Section 5.4**. Note that there are two device instances for each virtual IP softphone to support stereo call recordings.

The SSC Recorder `app.xml` file used for the compliance test is displayed on the next page.

```xml
<CallCabinet_SSC>
  <CM_DETAILS>
    <SwitchNameOrIP>devcon</SwitchNameOrIP>
  </CM_DETAILS>
  <AES_DETAILS>
    <ServerID>10.64.102.119</ServerID>
    <UserName>atmos</UserName>
    <Password>Atmos123!</Password>
    <DMCCPort>4722</DMCCPort>
    <AesProtocol>http://www.ecma-international.org/standards/ecma-323/csta/ed3/privD</AesProtocol>
  </AES_DETAILS>
  <SRTP_ENCRYPTION>
    <IsEncryptionEnable>true</IsEncryptionEnable>
    <AesEncryptionProtocol>srtp-aescm128-hmac80</AesEncryptionProtocol>
    <MediaCodec>g711U</MediaCodec>
  </SRTP_ENCRYPTION>
  <RECORDERS>
    <CRE Index="0" Name="" IP="192.168.120.45" CREIP="127.0.0.1" Port="1701"/>
  </RECORDERS>
  <EXTENSIONS>
    <Ext>77301</Ext>
    <Ext>78004</Ext>
    <Ext>77500</Ext>
  </EXTENSIONS>
  <CRE_CHANNELS>
    <CRE_CHANNEL Channel="0" CRE="0" Port="45000"/>
    <CRE_CHANNEL Channel="1" CRE="0" Port="45002"/>
    <CRE_CHANNEL Channel="2" CRE="0" Port="45004"/>
    <CRE_CHANNEL Channel="3" CRE="0" Port="45006"/>
    <CRE_CHANNEL Channel="4" CRE="0" Port="45008"/>
    <CRE_CHANNEL Channel="5" CRE="0" Port="45010"/>
    <CRE_CHANNEL Channel="6" CRE="0" Port="45012"/>
    <CRE_CHANNEL Channel="7" CRE="0" Port="45014"/>
    <CRE_CHANNEL Channel="8" CRE="0" Port="45016"/>
    <CRE_CHANNEL Channel="9" CRE="0" Port="45018"/>
    <CRE_CHANNEL Channel="10" CRE="0" Port="45020"/>
    <CRE_CHANNEL Channel="11" CRE="0" Port="45022"/>
    <CRE_CHANNEL Channel="12" CRE="0" Port="45024"/>
    <CRE_CHANNEL Channel="13" CRE="0" Port="45026"/>
    <CRE_CHANNEL Channel="14" CRE="0" Port="45028"/>
    <CRE_CHANNEL Channel="15" CRE="0" Port="45030"/>
    <CRE_CHANNEL Channel="16" CRE="0" Port="45032"/>
    <CRE_CHANNEL Channel="17" CRE="0" Port="45034"/>
    <CRE_CHANNEL Channel="18" CRE="0" Port="45036"/>
    <CRE_CHANNEL Channel="19" CRE="0" Port="45038"/>
    <CRE_CHANNEL Channel="20" CRE="0" Port="45040"/>
    <CRE_CHANNEL Channel="21" CRE="0" Port="45042"/>
    <CRE_CHANNEL Channel="22" CRE="0" Port="45044"/>
    <CRE_CHANNEL Channel="23" CRE="0" Port="45046"/>
    <CRE_CHANNEL Channel="24" CRE="0" Port="45048"/>
    <CRE_CHANNEL Channel="25" CRE="0" Port="45050"/>
  </CRE_CHANNELS>
  <SOFTPHONES>
    <SOFTPHONE Extension="77951" Password="1234" CRE_CHANNEL="0" DeviceInstance="0"/>
    <SOFTPHONE Extension="77951" Password="1234" CRE_CHANNEL="1" DeviceInstance="1"/>
    <SOFTPHONE Extension="77952" Password="1234" CRE_CHANNEL="2" DeviceInstance="0"/>
    <SOFTPHONE Extension="77952" Password="1234" CRE_CHANNEL="3" DeviceInstance="1"/>
    <SOFTPHONE Extension="77953" Password="1234" CRE_CHANNEL="4" DeviceInstance="0"/>
    <SOFTPHONE Extension="77953" Password="1234" CRE_CHANNEL="5" DeviceInstance="1"/>
    <SOFTPHONE Extension="77954" Password="1234" CRE_CHANNEL="6" DeviceInstance="0"/>
    <SOFTPHONE Extension="77954" Password="1234" CRE_CHANNEL="7" DeviceInstance="1"/>
    <SOFTPHONE Extension="77955" Password="1234" CRE_CHANNEL="8" DeviceInstance="0"/>
    <SOFTPHONE Extension="77955" Password="1234" CRE_CHANNEL="9" DeviceInstance="1"/>
    <SOFTPHONE Extension="77956" Password="1234" CRE_CHANNEL="10" DeviceInstance="0"/>
    <SOFTPHONE Extension="77956" Password="1234" CRE_CHANNEL="11" DeviceInstance="1"/>
    <SOFTPHONE Extension="77957" Password="1234" CRE_CHANNEL="12" DeviceInstance="0"/>
    <SOFTPHONE Extension="77957" Password="1234" CRE_CHANNEL="13" DeviceInstance="1"/>
    <SOFTPHONE Extension="77958" Password="1234" CRE_CHANNEL="14" DeviceInstance="0"/>
    <SOFTPHONE Extension="77958" Password="1234" CRE_CHANNEL="15" DeviceInstance="1"/>
  </SOFTPHONES>
</CallCabinet_SSC>
```

8.4. Configure RTP Recorder Application

The `app.xml` file for the RTP Recorder application, located in the `CallCabinet\CallCabinetRTPRecorder\bin\` directory, should be modified with the following parameter settings:

AudioFileFormat:	Specify *STEREO* for stereo call recording. MONO for mono call recording is also supported.
ClientID:	Set to **Customer ID** from **Section 8.2**.
SiteID:	Set to **Site ID** from **Section 8.2**.
RecordingCallDirection:	Set to *B* for recording audio in both directions.

The RTP Recorder `app.xml` file used for the compliance test is displayed below.

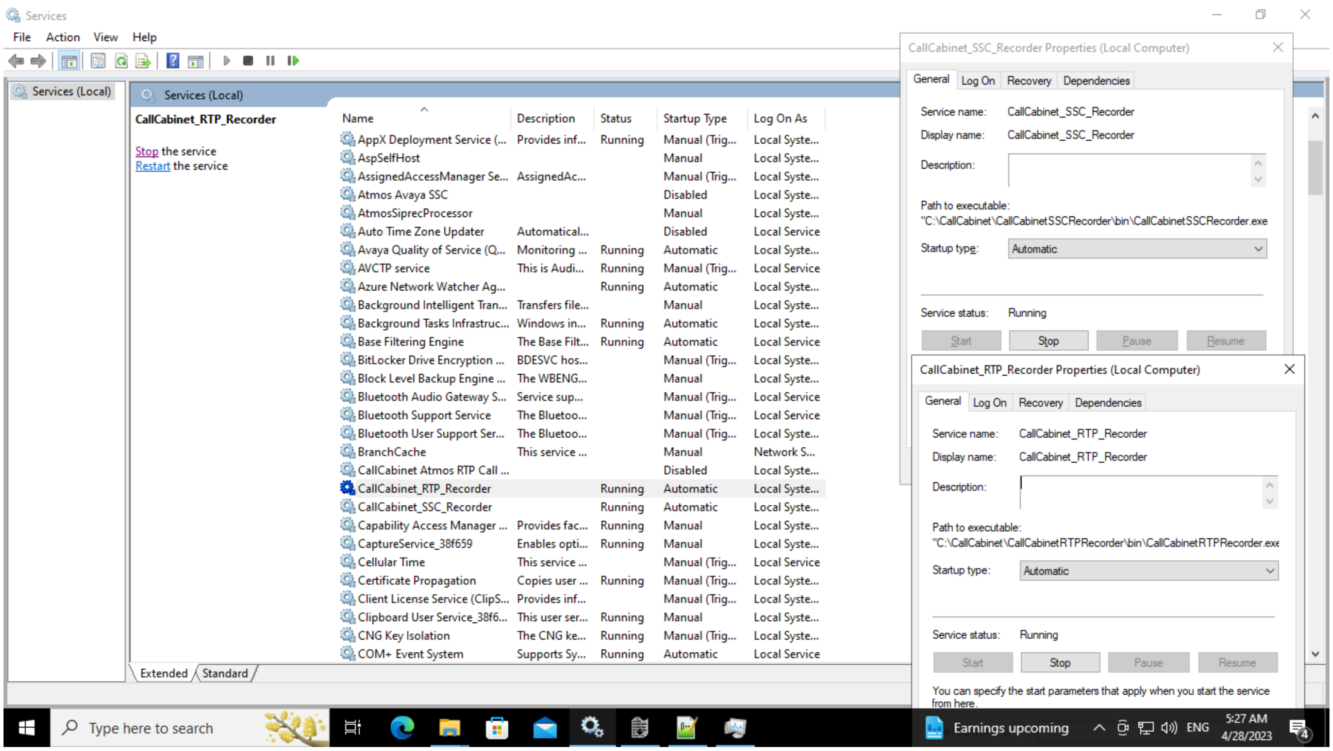
```
▼<CallCabinetConfig>
  ▼<app>
     <AudiofileFormat>STEREO</AudiofileFormat>
     <StoragePath>C:\CallCabinet\CallCabinetRTPRecorder\temp\</StoragePath>
     <NetworkAdapter>\Device\NPF_{8099E182-4C6A-4153-9CF8-8D17FBD78F49}</NetworkAdapter>
     <Port>1701</Port>
     <AudioRepository>C:\CallCabinet\CallCabinetRTPRecorder\from\</AudioRepository>
     <ReprocessDirPath>C:\CallCabinet\CallCabinetRTPRecorder\Reprocess\</ReprocessDirPath>
     <ReprocessIntervalInMinute>10</ReprocessIntervalInMinute>
     <CustomizationType>0</CustomizationType>
     <!--  For Certification  -->
     <ClientID>bc52e108-bfa4-4cc6-8e0e-6b3019ad80f3</ClientID>
     <SiteID>2f01a217-248a-4050-87a7-5e10035d5a53</SiteID>
     <RecordingCallDirection>B</RecordingCallDirection>
     <Sftp_Upload>false</Sftp_Upload>
     <Sftp_Ip>[redacted]</Sftp_Ip>
     <Sftp_Port>22</Sftp_Port>
     <Sftp_UserName>[redacted]</Sftp_UserName>
     <Sftp_Password>[redacted]</Sftp_Password>
   </app>
 </CallCabinetConfig>
```

8.5. Install Trusted Certificate

For encrypted DMCC link and SRTP support, install the trusted CA certificate used by Application Enablement Services and agent IP stations on the SSC Recorder windows server using Microsoft Management Console (MMC). Avaya Aura® System Manager was used as the certificate authority.

8.6. Start SSC Recorder Windows Services

Verify that the following SSC Recorder services, CallCabinet_SSC_Recorder and CallCabinet_RTP_Recorder, have been started in Windows Services as shown below.



9. Verification Steps

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

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     12       no    devcon-aes       established    895      370
```

Verify registration status of the virtual IP softphones by using the **list registered-ip-stations** command. Verify that all virtual IP softphones from **Section 5.4** are displayed along with the IP address of the Application Enablement Services server as shown below. Note that for stereo call recording two instances of each virtual IP softphone are registered.

```
list registered-ip-stations ext 77951 count 8                         Page   1
                            REGISTERED IP STATIONS

Station Ext      Set Type/ Prod ID/    Station IP Address/
or Orig Port     Net Rgn   Release     Gatekeeper IP Address
  Socket
77951            9608      IP_API_A    10.64.102.119
  tcp            1         3.2040      10.64.102.115
77951            9608      IP_API_A    10.64.102.119
  tcp            1         3.2040      10.64.102.115
77952            9608      IP_API_A    10.64.102.119
  tcp            1         3.2040      10.64.102.115
77952            9608      IP_API_A    10.64.102.119
  tcp            1         3.2040      10.64.102.115
77953            9608      IP_API_A    10.64.102.119
  tcp            1         3.2040      10.64.102.115
77953            9608      IP_API_A    10.64.102.119
  tcp            1         3.2040      10.64.102.115
77954            9608      IP_API_A    10.64.102.119
  tcp            1         3.2040      10.64.102.115
77954            9608      IP_API_A    10.64.102.119
  tcp            1         3.2040      10.64.102.115
```

```
list registered-ip-stations ext 77951 count 8
                            REGISTERED IP STATIONS
```

```
Station Ext       Set Type/ Prod ID/    Station IP Address/
or Orig Port      Net Rgn   Release     Gatekeeper IP Address
  Socket
77955             9608      IP_API_A    10.64.102.119
  tcp             1         3.2040      10.64.102.115
77955             9608      IP_API_A    10.64.102.119
  tcp             1         3.2040      10.64.102.115
77956             9608      IP_API_A    10.64.102.119
  tcp             1         3.2040      10.64.102.115
77956             9608      IP_API_A    10.64.102.119
  tcp             1         3.2040      10.64.102.115
77957             9608      IP_API_A    10.64.102.119
  tcp             1         3.2040      10.64.102.115
77957             9608      IP_API_A    10.64.102.119
  tcp             1         3.2040      10.64.102.115
77958             9608      IP_API_A    10.64.102.119
  tcp             1         3.2040      10.64.102.115
77958             9608      IP_API_A    10.64.102.119
  tcp             1         3.2040      10.64.102.115
```

Establish a call with a monitored station and verify the status of the virtual IP softphone using the **status station** command. Verify that the **Service State** is *in-service/off-hook* on **Page 1**.

```
status station 77955                                            Page   1 of  10
                              GENERAL STATUS
     Administered Type: 9608                Service State: in-service/off-hook
        Connected Type: N/A                 Signal Status: connected
             Extension: 77955              Network Region: 1
                  Port: S000062       Parameter Download: pending
           Call Parked? no                  SAC Activated? no
      Ring Cut Off Act? no
Active Coverage Option: 1

          EC500 Status: N/A
   Message Waiting:
   Connected Ports: S000207     S000058     T000062



 Limit Incoming Calls? no
     User Cntrl Restr: none
    Group Cntrl Restr: none
CTI Monitoring Active? Yes
```

On **Page 5**, verify that the codec used is G.711 as shown below.

```
status station 77955                                          Page   5 of  10

                          AUDIO CHANNEL Port: S000062
G.711MU       Switch-End Audio Location: AMS1
            IP Address                              Port  Node Name       Rgn
Other-End: 10.64.102.118                            6138  devcon-ams      1
  Set-End: 192.168.120.30                           45016                 1
Audio Connection Type: ip-tdm

                          AUDIO CHANNEL Shared Port: S000207
G.711MU       Switch-End Audio Location: AMS1
            IP Address                              Port  Node Name       Rgn
Other-End: 10.64.102.118                            6140  devcon-ams      1
  Set-End: 10.64.102.119                            45018 devcon-aes      1
Audio Connection Type: ip-tdm


              Switch-End Audio Location:
```

On **Page 7** and subsequent pages (not shown), verify that SRTP is used as shown below.

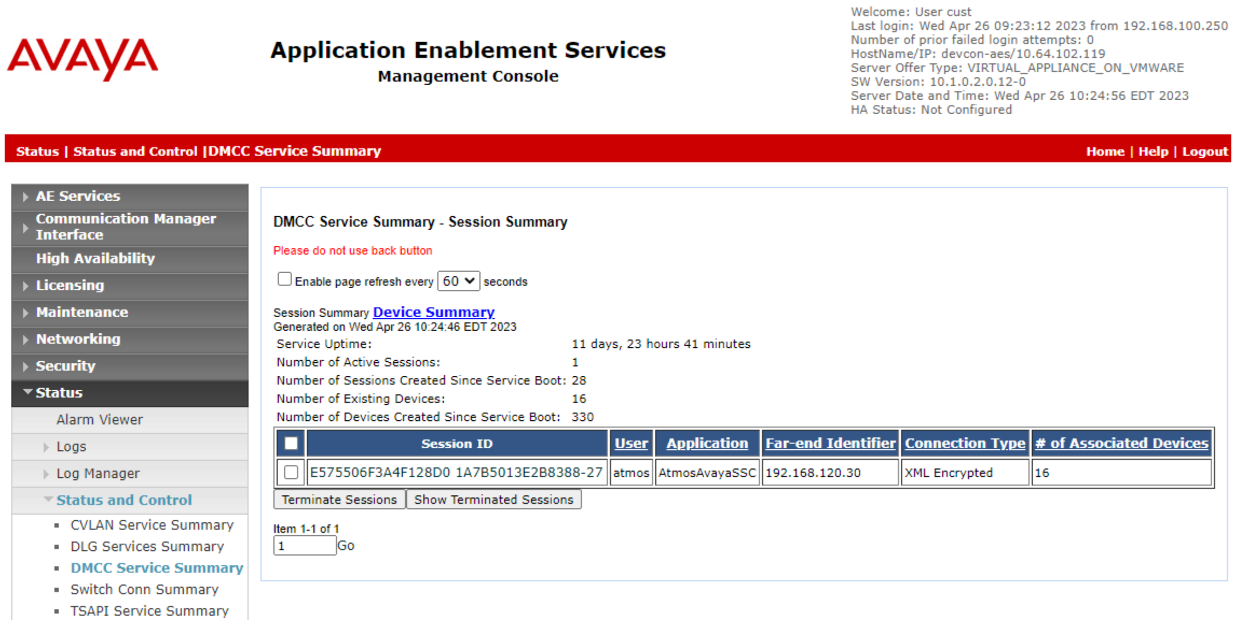
```
status station 77955                                          Page   7 of  10
                      SRC PORT TO DEST PORT TALKPATH
src port: S000062
S000062:TX:192.168.120.30:45016/g711u/20ms/1-srtp-aescm128-hmac80
AMS1:RX:10.64.102.118:6138/g711u/20ms/1-srtp-aescm128-h:TX:cnfID:1f000010000006e
AMS1:RX:cnfID:1f000010000006e:TX:10.64.102.118:6140/g711u/20ms/1-srtp-aescm128-h
S000207:RX:192.168.120.30:45018/g711u/20ms/1-srtp-aescm128-hmac80
```

Terminate the call and verify that the **Service State** of the virtual IP softphone returns to *in-service/on-hook*. Call recordings are verified in **Section 9.3**.

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify that the **User** column shows an active session with the SSC Recorder username from **Section 6.5**, that the **Connection Type** is encrypted, and that the number **# of Associated Devices** reflects the number of virtual IP softphones. For stereo call recording, two device instances per virtual IP softphone is used so the **# of Associated Devices** is *16*.



Click on the **Session ID** in the screen on previous page to display the devices associated with the session.

DMCC Service Summary - Session Detail

Enable page refresh every 60 seconds

Detailed Session View
Generated on Thu Apr 27 13:13:27 EDT 2023

Session ID:	D83D94A7FAA8D23A2AD57D802E56FD42-44
State:	Active
Time Established:	Thu, Apr 27, 2023 10:32:13 AM GMT-05:00
Uptime:	0 days, 2 hours, 41 minutes, and 13 seconds
Cleanup Delay Timer:	5 seconds
Session Duration Timer:	180 seconds
Time of Most Recent Timer Reset:	Thu, Apr 27, 2023 01:13:22 PM EDT
Reconnect Counter:	0

Terminate Sessions

Devices Associated with Session

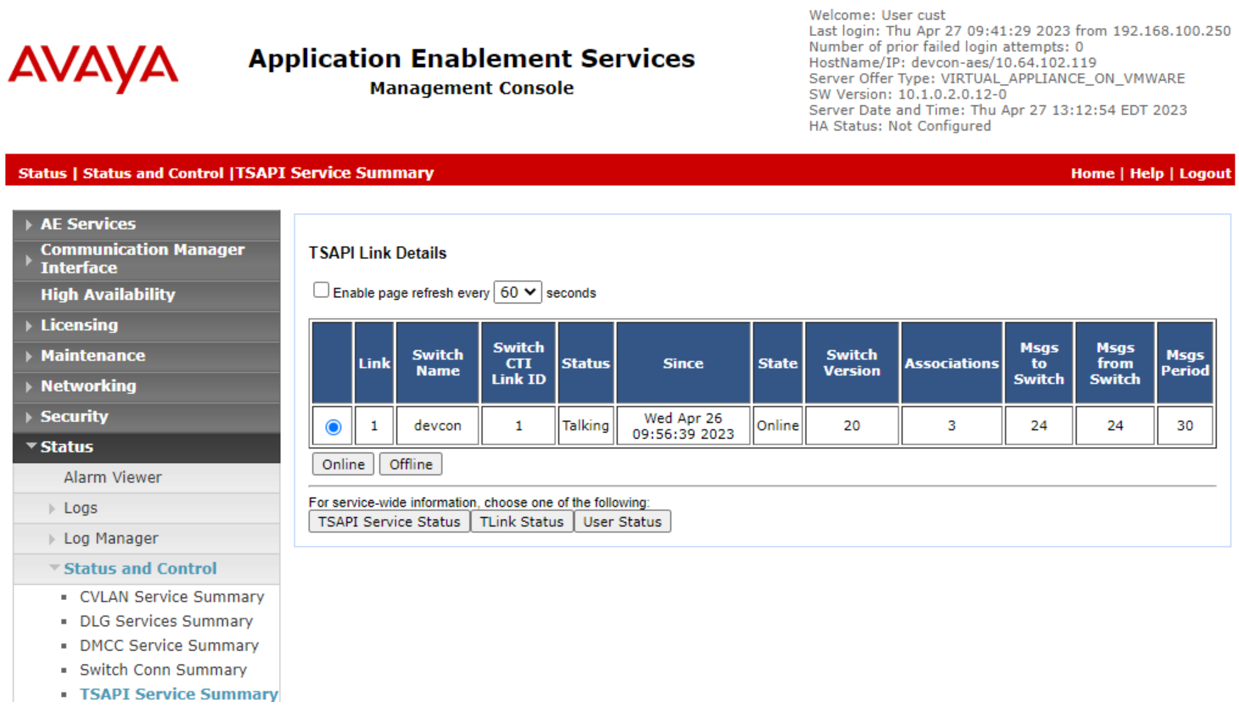
	Device ID	State
	77953:devcon:0.0.0.0:1	REGISTERED
	77953:devcon:0.0.0.0:0	REGISTERED
	77958:devcon:0.0.0.0:0	REGISTERED
	77958:devcon:0.0.0.0:1	REGISTERED
	77955:devcon:0.0.0.0:1	REGISTERED
	77955:devcon:0.0.0.0:0	REGISTERED
	77956:devcon:0.0.0.0:0	REGISTERED
	77952:devcon:0.0.0.0:0	REGISTERED
	77954:devcon:0.0.0.0:0	REGISTERED
	77957:devcon:0.0.0.0:0	REGISTERED
	77952:devcon:0.0.0.0:1	REGISTERED
	77957:devcon:0.0.0.0:1	REGISTERED
	77954:devcon:0.0.0.0:1	REGISTERED
	77956:devcon:0.0.0.0:1	REGISTERED
	77951:devcon:0.0.0.0:1	REGISTERED
	77951:devcon:0.0.0.0:0	REGISTERED

Terminate Selected Devices | Back

Item 1-16 of 16

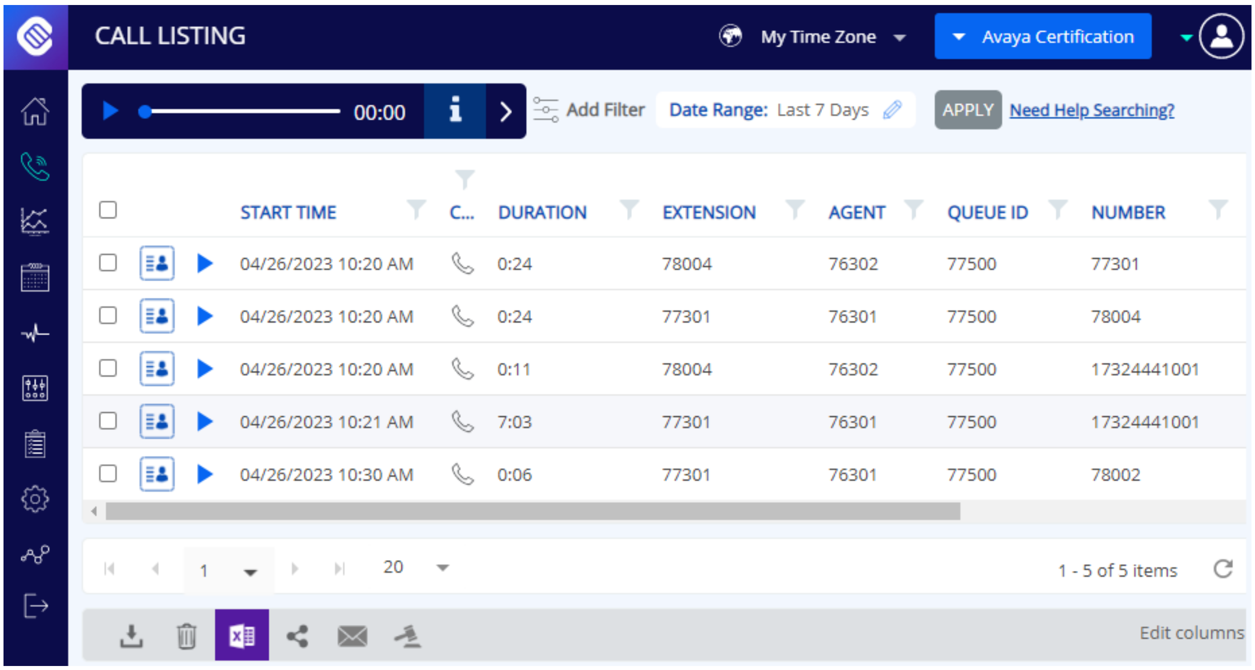
Verify status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that 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 *3*.



9.3. Verify CallCabinet SSC Recorder

Log in an agent to handle and complete an ACD call. Access the SSC Recorder Portal as described in **Section 8.1** and log in using the appropriate credentials. Navigate to **Call Listing** to view a listing of call recordings. Verify that there is an entry for the last call with proper values in the relevant fields as shown below. Verify that the recording can be played back.



10. Conclusion

These Application Notes describe the configuration steps required to integrate CallCabinet SSC Recorder with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using Single Step Conference. Stereo call recordings were logged and played back successfully. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

11. Additional References

This section references the Avaya and CallCabinet documentation relevant to these Application Notes.

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 2, September 2022, available at http://support.avaya.com.

[2] *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 5, September 2022, available at http://support.avaya.com.

[3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 4, September 2022, available at http://support.avaya.com.

[4] *Avaya Aura® AE Services Device, Media, and Call Control .NET API Programmer's Guide*, Release 8.x – 10.x, Aug 2022.

[5] *CallCabinet Atmos User Guide*, available at https://www.callcabinet.com/atmos-user-guide/.

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.