Avaya Solution & Interoperability Test Lab

Application Notes for HigherGround Calibre 9 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for HigherGround Calibre 9 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing. HigherGround Calibre is a call recording solution.

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

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

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

©2021 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the configuration steps required for HigherGround Calibre 9 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing. Calibre is a call recording solution.

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

When there is an active call at the monitored agent station, Calibre is informed of the call via event reports from the DMCC interface. Calibre starts the call recording by using media via active Service Observing from the virtual IP softphone associated with the agent station. 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 Calibre, the application used DMCC to automatically perform device queries, monitor skill groups and agent stations, register and activate Service Observing for the virtual IP softphones.

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

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

The verification of tests included use of Application Enablement Services and Calibre logs for proper message exchanges and use of Calibre web interface for proper logging and playback of calls.

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

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

©2021 Avaya Inc. All Rights Reserved.

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 this Application Note, the interface between Avaya systems and Calibre did not include use of any specific encryption features as requested by HigherGround.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Calibre:

- Use of DMCC to monitor skill groups and agent stations, register virtual IP softphones, and activate Service Observing.

- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711, G.729, forwarding, service observing, long duration, multiple calls, multiple agents, conference, and transfer.

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

2.2. Test Results

All test cases were executed, and the following were observations on Calibre:

- By design, the default Calibre setting ends an active recording upon agent placing the call on hold and starts a new recording upon agent resuming the call. This behavior is controlled by the RecordThroughHold system parameter and is configurable. The compliance testing used the default value of zero for the parameter.

- In the attended transfer scenario, the recording entry associated with the remaining conversation between the transfer-to agent and PSTN only contained values for date, duration, agent ID, agent extension, and agent name, with blank values for the remainder parameters.

- When an agent call was observed by the supervisor, the supervisor extension was reported as the answering device in the recording entry.

2.3. Support

Technical support on Calibre can be obtained through the following:

- **Phone:** (818) 456-1600
- **Email:** support@higherground.com

©2021 Avaya Inc. All Rights Reserved.

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of call center devices are not the focus of these Application Notes and will not be described.

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

Device Type	Extension
Skill Group	61001, 61002
Agent Station	65001 (H.323), 66006 (SIP)
Agent ID	65881, 65882

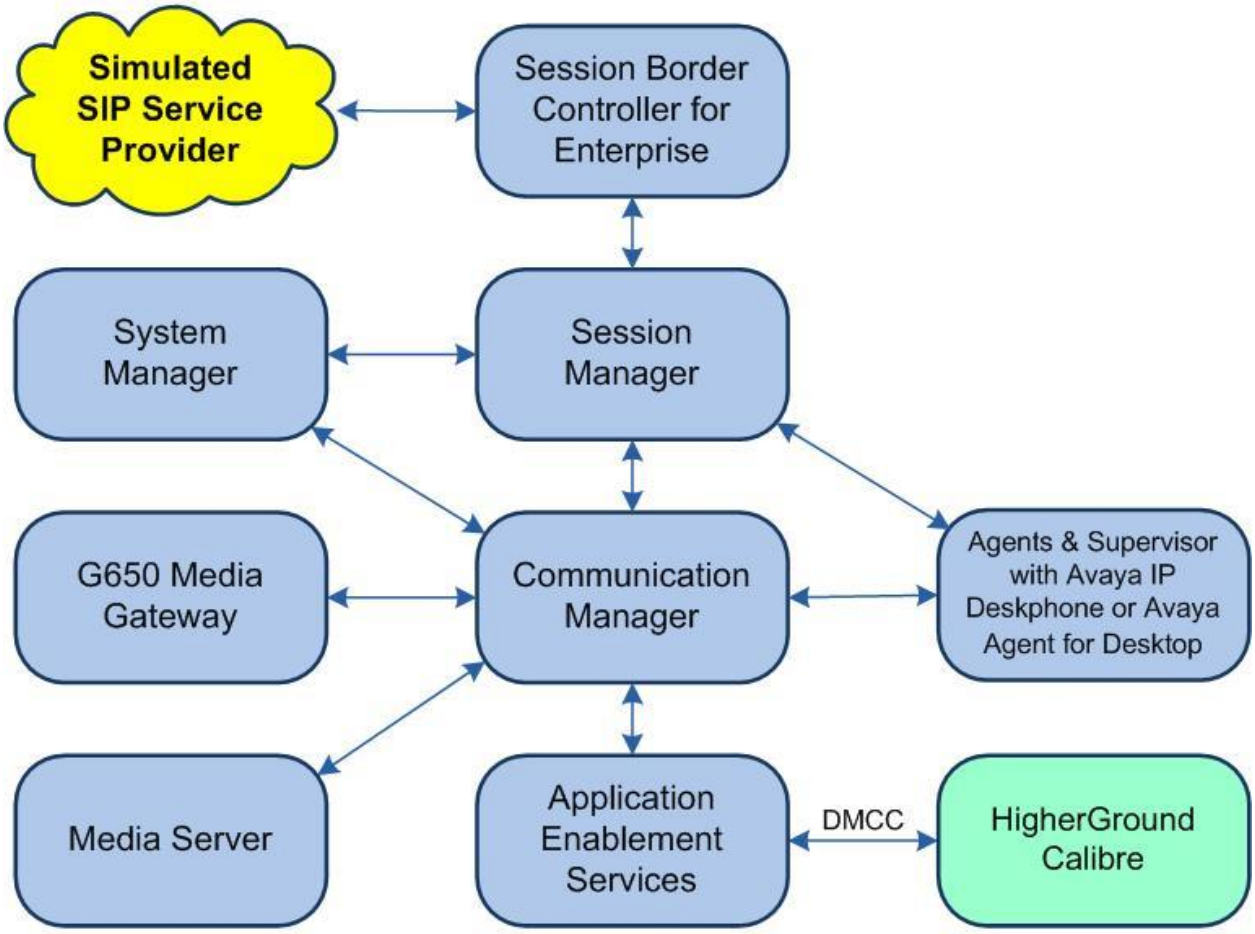


Figure 1: Compliance Testing Configuration

©2021 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.1.3 (8.1.3.0.1.890.26685)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.2.138
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3.0.0.25-0
Avaya Aura® Session Manager in Virtual Environment	8.1.3 (8.1.3.0.813014)
Avaya Aura® System Manager in Virtual Environment	8.1.3 (8.1.3.0.1012091)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.1 (8.1.1.0-19390)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.0.10
Avaya J179 & 9611G IP Deskphone (H.323)	6.8502
Avaya J169 IP Phone (SIP)	4.0.7.1.5
HigherGround Calibre on Windows 2019 Server • HgDMCC.exe • Avaya DMCC .NET (ServiceProvider.dll)	9.2021.7941 Standard 9.2021.7985.15939 7.0.0.38

©2021 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Communication Manager

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

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

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "**display system-parameters customer-options**" command to verify that the **Computer Telephony Adjunct Links** customer option is set to "**y**" on **Page 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? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                DCS with Rerouting? y
```

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

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

                          Call Center Release: 8.0

                                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
```


©2021 Avaya Inc. All Rights Reserved.

5.2. Administer CTI Link

Add a CTI link using the "**add cti-link n**" command, where "**n**" is an available CTI link number. Enter an available extension number in the **Extension** field.

Enter "**ADJ-IP**" in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

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

5.3. Administer IP Codec Set

Use the "**change ip-codec-set n**" command, where "**n**" is an existing codec set number used for integration with Calibre.

For customer network that use encrypted media, make certain that "**none**" is included for **Media Encryption**, and that **Encrypted SRTP** is set to "**best-effort**", these settings are needed for support of non-encrypted media from the virtual IPsoftphones used by Calibre.

In the compliance testing, this IP codec set was used by the agent stations and by the virtual IP softphones.

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

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.729
 3:
 4:
 5:
 6:
 7:

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


©2021 Avaya Inc. All Rights Reserved.

5.4. Administer System Parameters Features

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

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

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

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

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

```
change system-parameters features                                Page  11 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:                    Delay:
    Message Waiting Lamp Indicates Status For: station
                           Work Mode On Login: aux
  VECTORING
                    Converse First Data Delay: 0      Second Data Delay: 2
                Converse Signaling Tone(msec): 100         Pause (msec): 70
                      Prompting Timeout(secs): 10
                  Interflow-qpos EWT Threshod: 2
    Reverse Star/Pound Digit For Collect Step? n
          Available Agent Adjustments for BSR? n
                             BSR Tie Strategy: 1st-found
   Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
              Service Observing: Warning Tone? n     or Conference Tone? n
    Allowed with Exclusion: Service Observing? n                    SSC? n
             Allow Two Observers in Same Call? y
```


©2021 Avaya Inc. All Rights Reserved.

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

```
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? y
                                          Send UCID to ASAI? y
                 For ASAI Send DTMF Tone to Call Originator? y
         Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

5.5. Administer Class of Restriction

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

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

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

               COR Number: 2
          COR Description: Calibre

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


©2021 Avaya Inc. All Rights Reserved.

5.6. Administer Agent Stations

Use the "**change station n**" command, where "**n**" is the first H.323 agent station extension from **Section 3**. For **COR**, enter the COR number from **Section 5.5**.

Repeat this section to administer all H.323 agent stations from **Section 3**. In the compliance testing, one H.323 agent station was administered as shown below.

```
change station 65001                                          Page   1 of   5
                                     STATION

Extension: 65001                        Lock Messages? n               BCC: 0
     Type: 9611                         Security Code: *                TN: 1
     Port: S000106                    Coverage Path 1: 1              COR: 2
     Name: CM Station 1               Coverage Path 2:                COS: 1
Unicode Name? n                     Hunt-to Station:                 Tests? y
```

5.7. Administer Virtual IP Softphones

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

- **Extension:** The available extension number.
- **Type:** Any IP telephone type, such as "9608".
- **Name:** A descriptive name.
- **Security Code:** A desired code.
- **COR:** The COR number from **Section 5.5**.
- **IP SoftPhone:** "y"

```
add station 65991                                             Page   1 of   5
                                     STATION

Extension: 65991                        Lock Messages? n               BCC: 0
     Type: 9608                         Security Code: 123456           TN: 1
     Port: IP                         Coverage Path 1:                COR: 2
     Name: Calibre 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: 65991
            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
```


©2021 Avaya Inc. All Rights Reserved.

Navigate to **Page 4**, and add "**serv-obsrv**" to any available button as shown below.

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

ABBREVIATED DIALING
     List1:                    List2:                     List3:




BUTTON ASSIGNMENTS
 1: call-appr                            5:
 2: call-appr                            6:
 3: call-appr                            7:
 4: serv-obsrv                           8:
```

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

```
list station 65991 count 2

                                   STATIONS

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

65991            S000126 Calibre DMCC 1                                 2
               9608                          no                        1  1
65992            S000122 Calibre DMCC 2                                 2
               9608                          no                        1  1
```


©2021 Avaya Inc. All Rights Reserved.

6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer H.323 gatekeeper
- Administer Calibre user
- Administer security database
- Administer ports
- Restart services

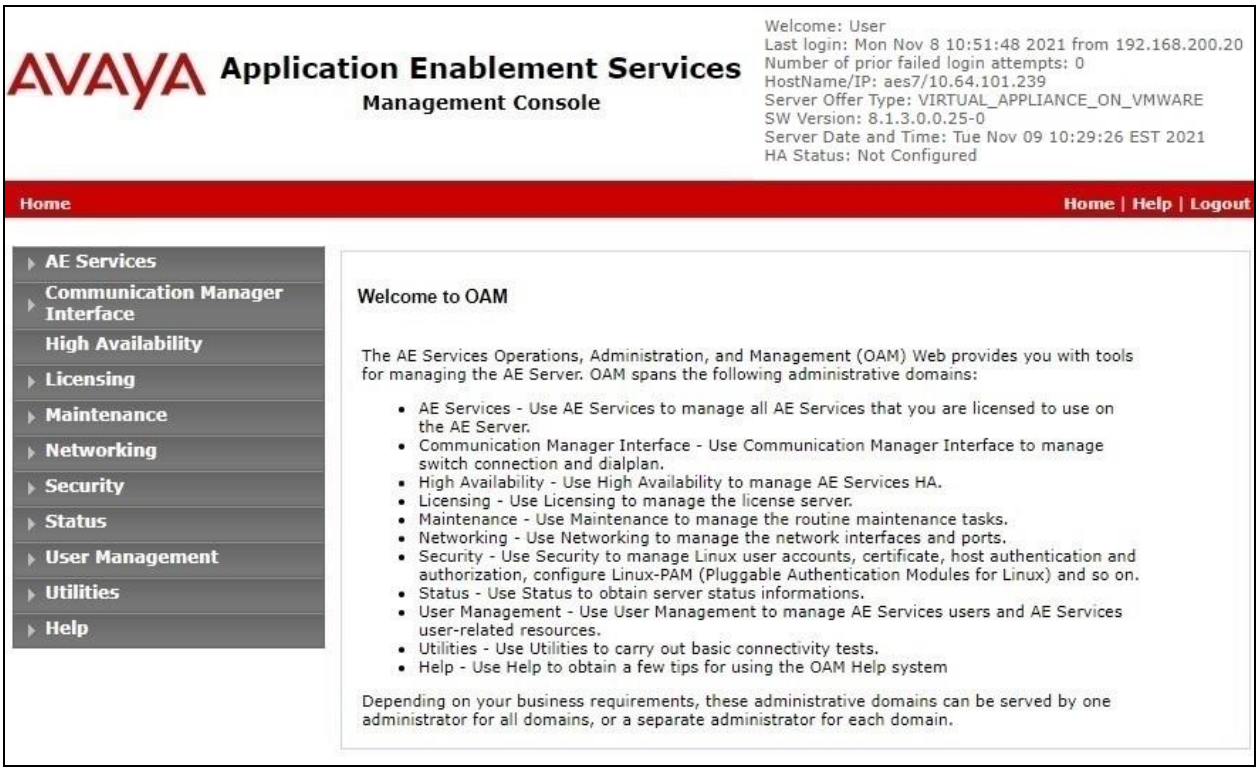
6.1. Launch OAM Interface

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 the Application Enablement Services server.

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

©2021 Avaya Inc. All Rights Reserved.

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



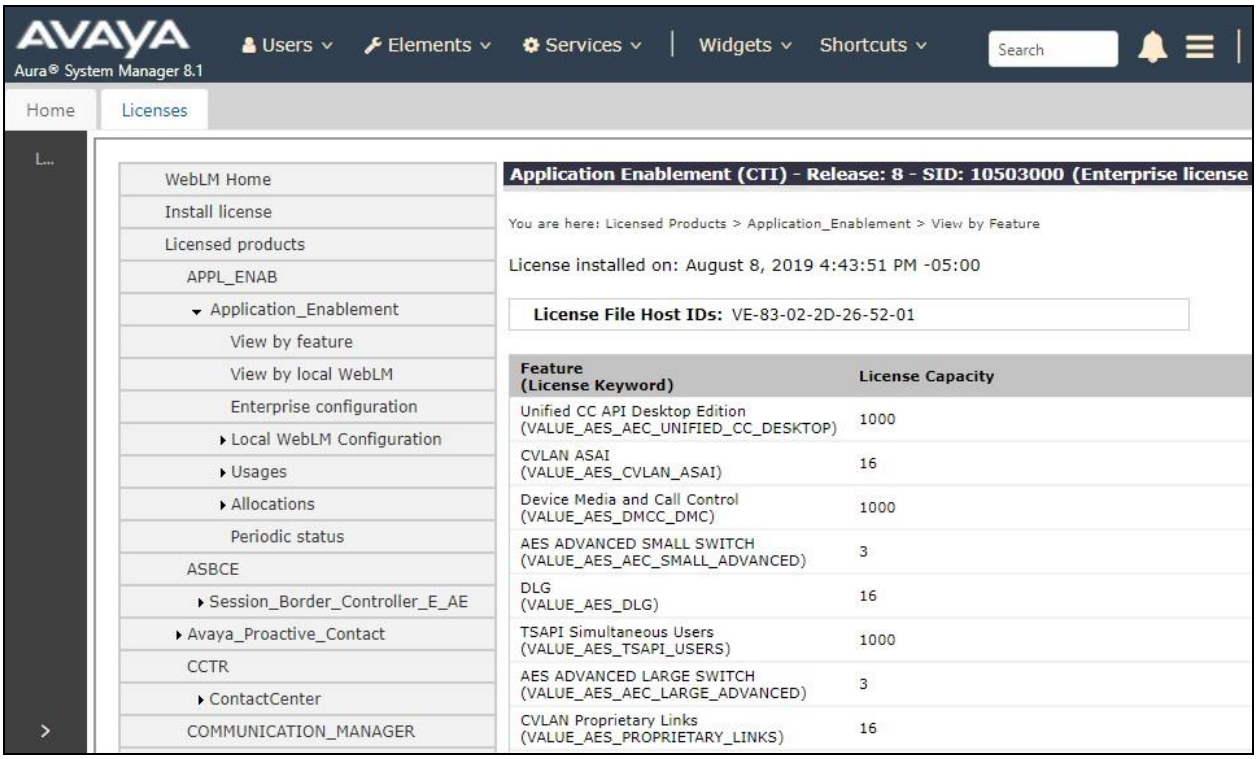
6.2. Verify License

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).

©2021 Avaya Inc. All Rights Reserved.

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

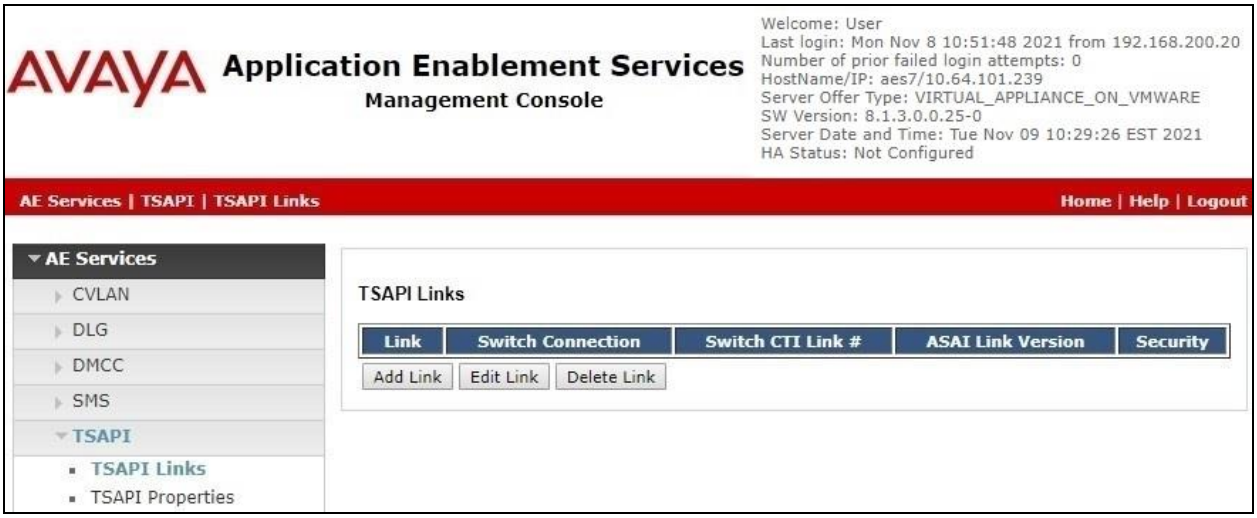
Verify that there are sufficient licenses for **Device Media and Call Control** and **TSAPI Simultaneous Users**, as shown below. The DMCC license is used for the virtual IP softphones, and the TSAPI license is used for device monitoring.



©2021 Avaya Inc. All Rights Reserved.

6.3. Administer TSAPI Link

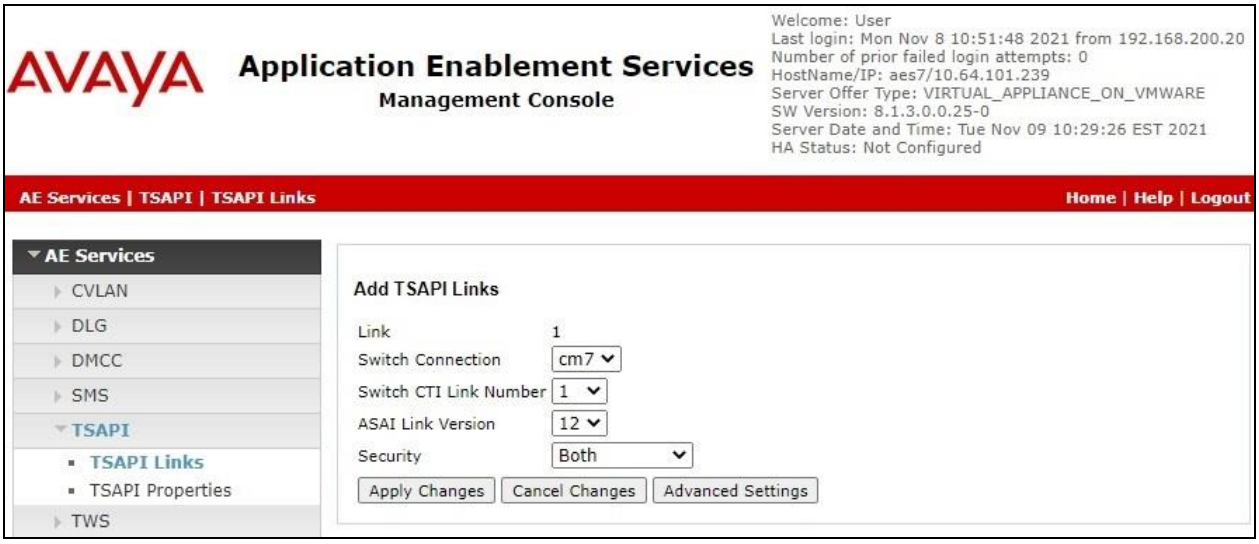
Select **AE Services → TSAPI → TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



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 "**cm7**". 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.

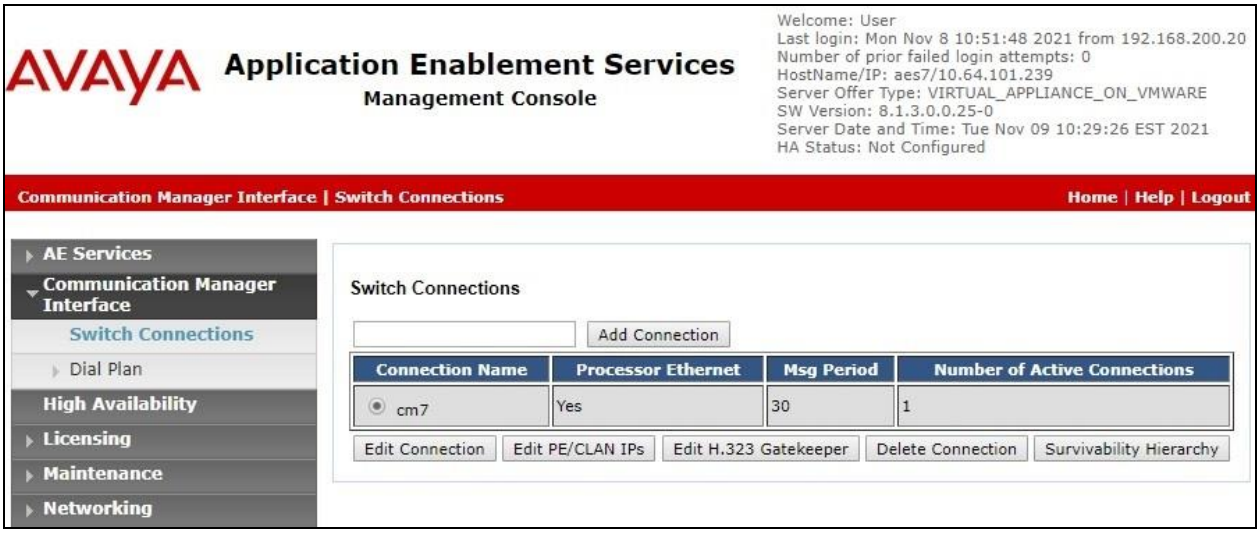


©2021 Avaya Inc. All Rights Reserved.

6.4. Administer H.323 Gatekeeper

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

Locate the connection name associated with relevant Communication Manager, in this case "**cm7**", and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.



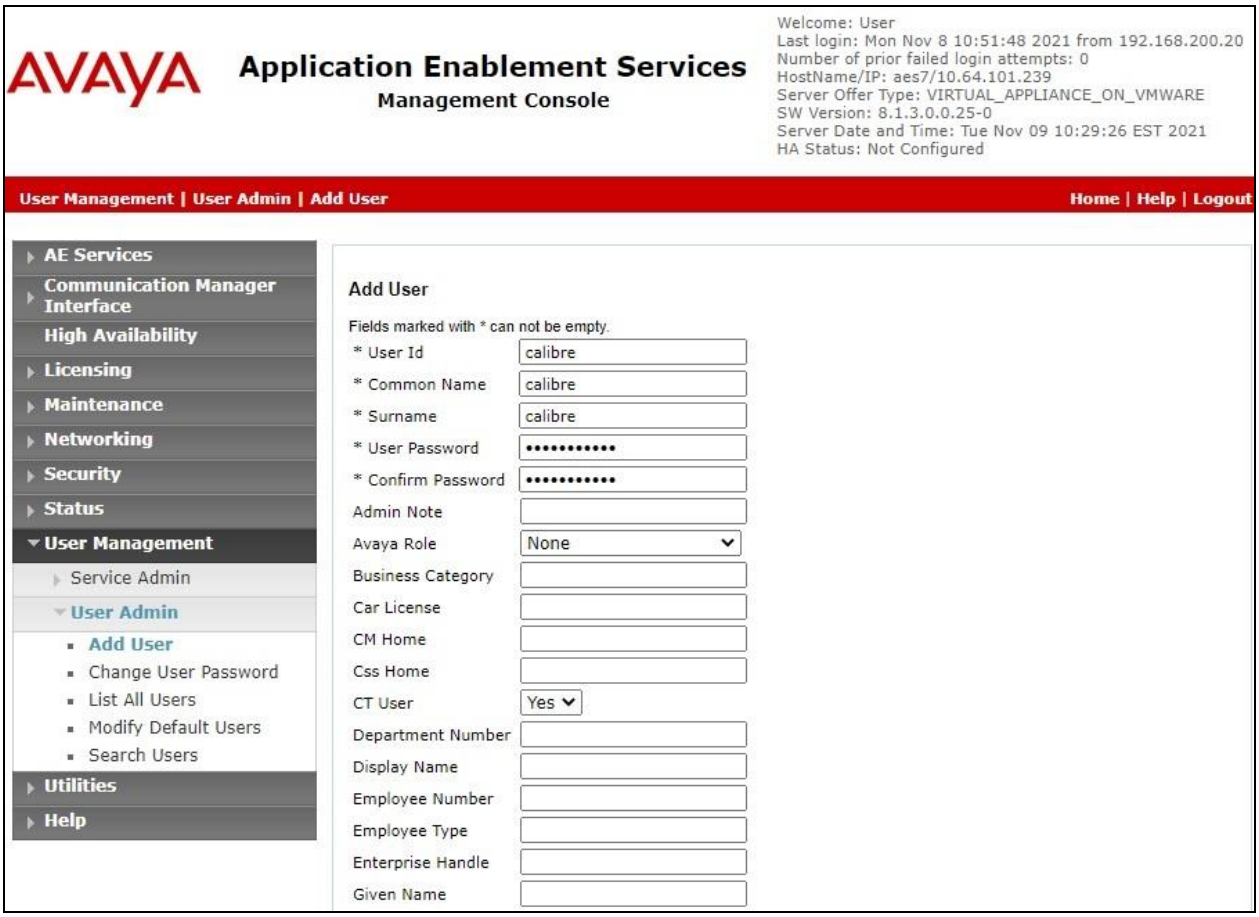
The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as H.323 gatekeeper, in this case "**10.64.101.236**" as shown below. Click **Add Name or IP**.

©2021 Avaya Inc. All Rights Reserved.

6.5. Administer Calibre 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.

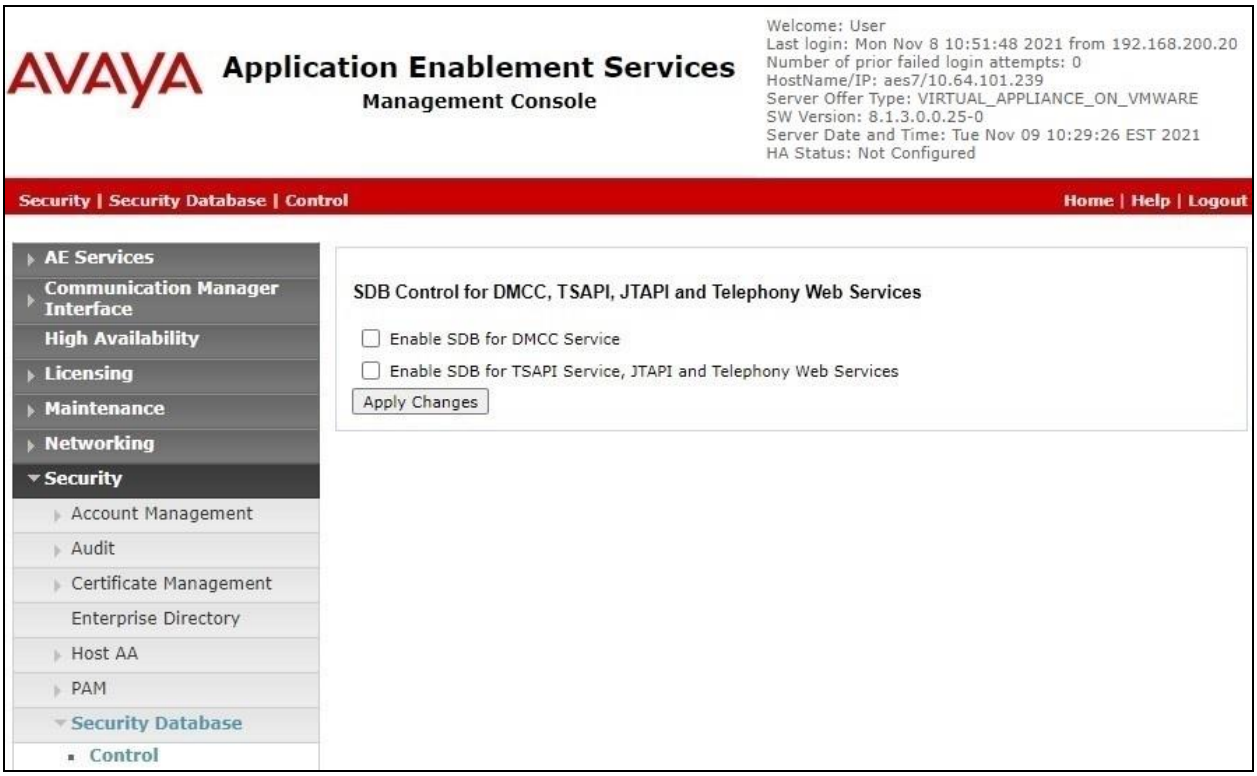


©2021 Avaya Inc. All Rights Reserved.

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 Calibre user from **Section 6.5**.

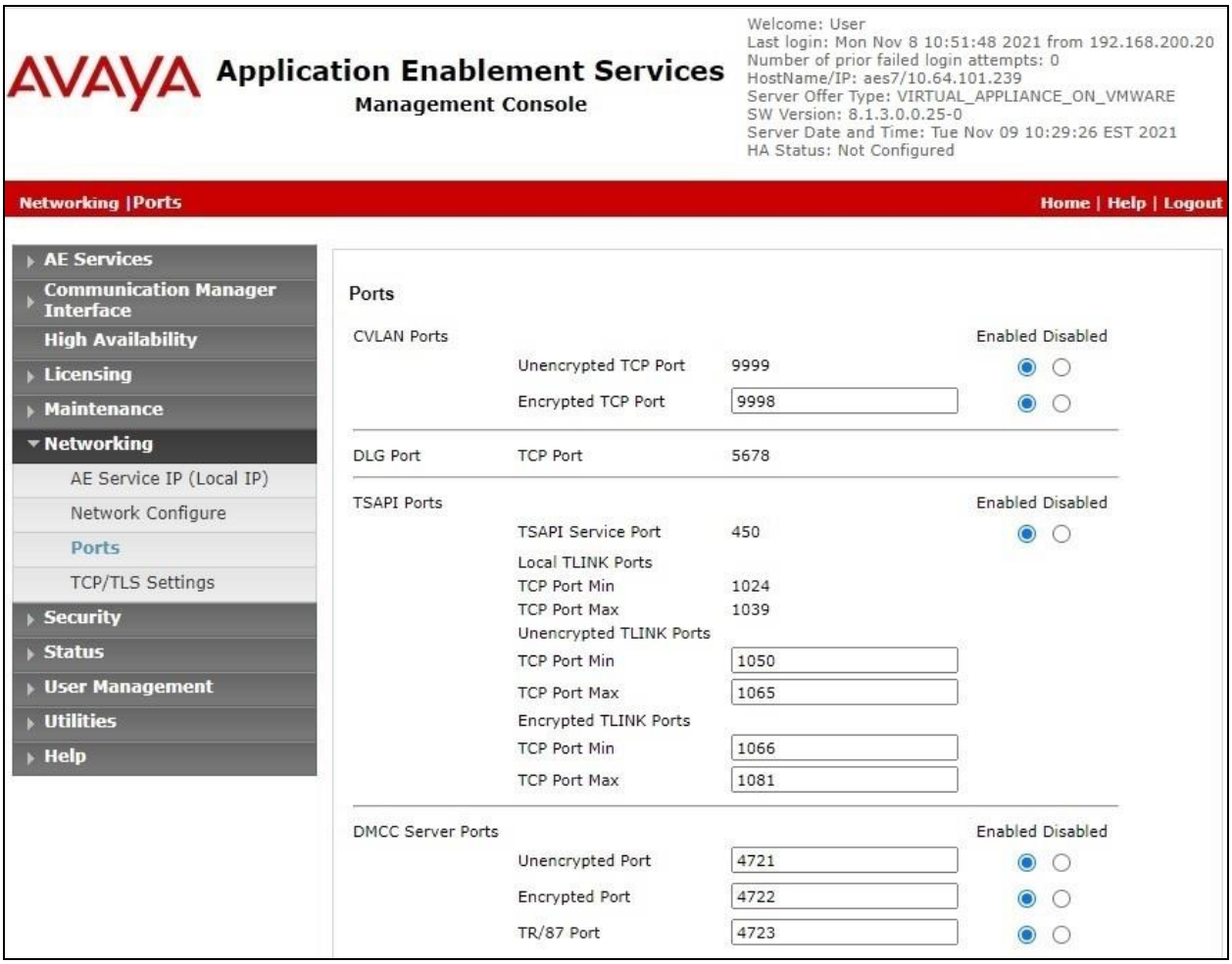


©2021 Avaya Inc. All Rights Reserved.

6.7. Administer Ports

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

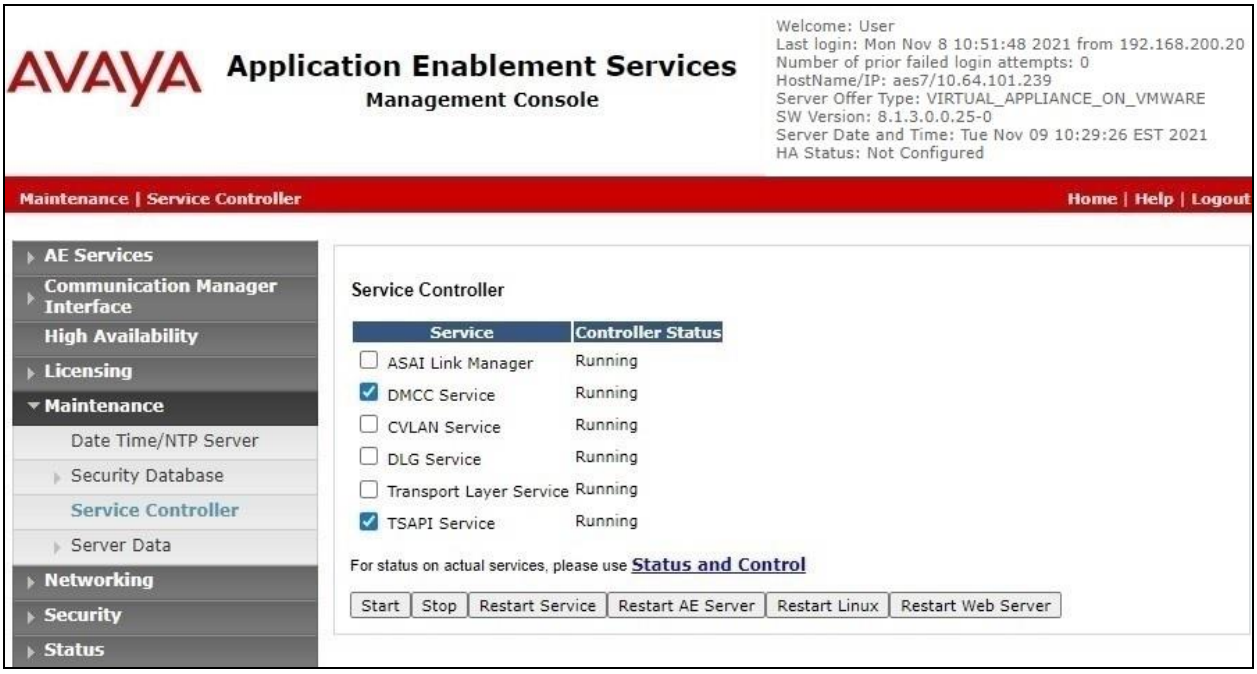
In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.



©2021 Avaya Inc. All Rights Reserved.

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**.



©2021 Avaya Inc. All Rights Reserved.

7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

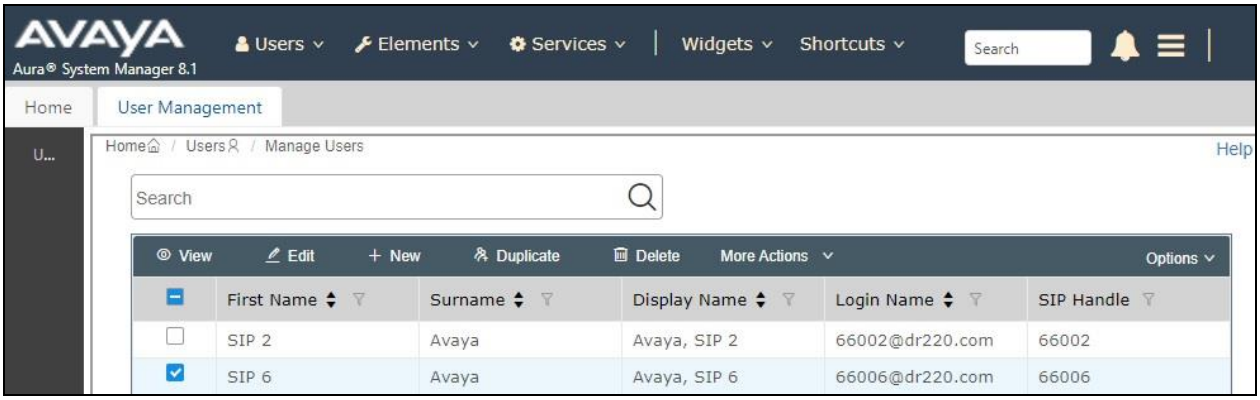
7.1. Launch System Manager

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

7.2. Administer 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.

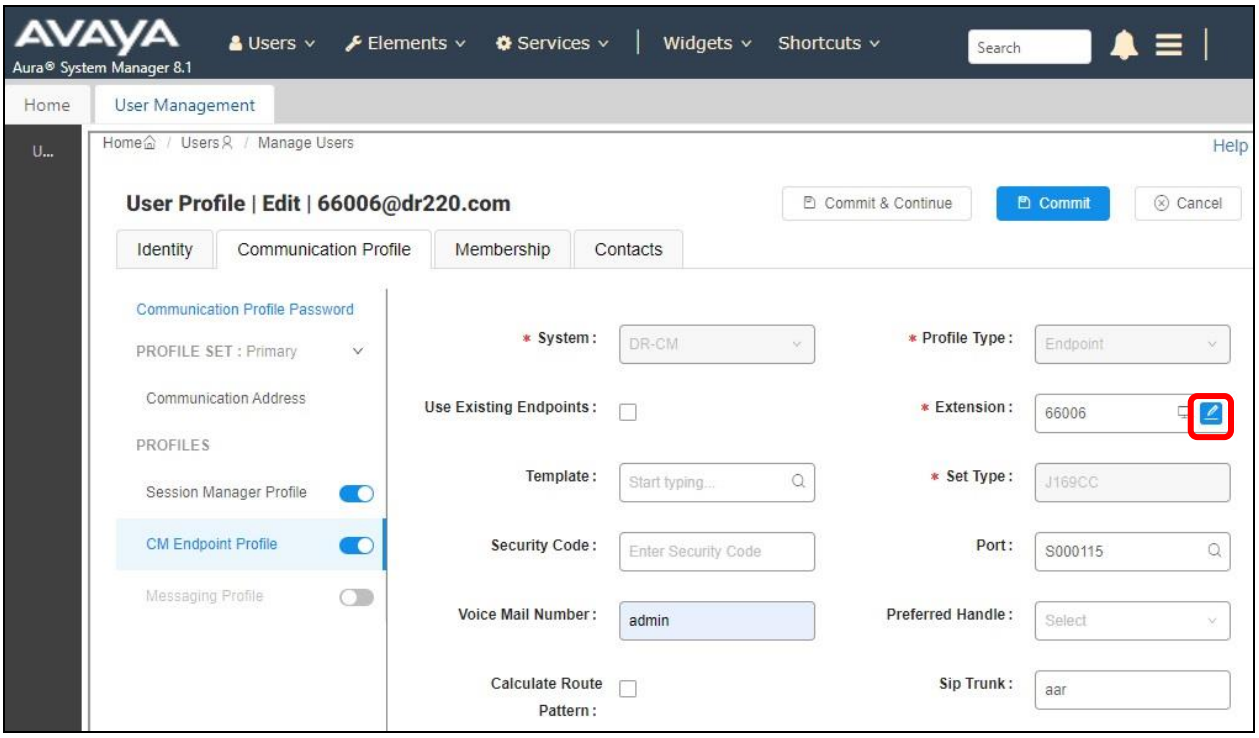
Select the entry associated with the first SIP agent station from **Section 3**, in this case "**66006**", and click **Edit**.



©2021 Avaya Inc. All Rights Reserved.

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

Click on the **Editor** icon shown below.

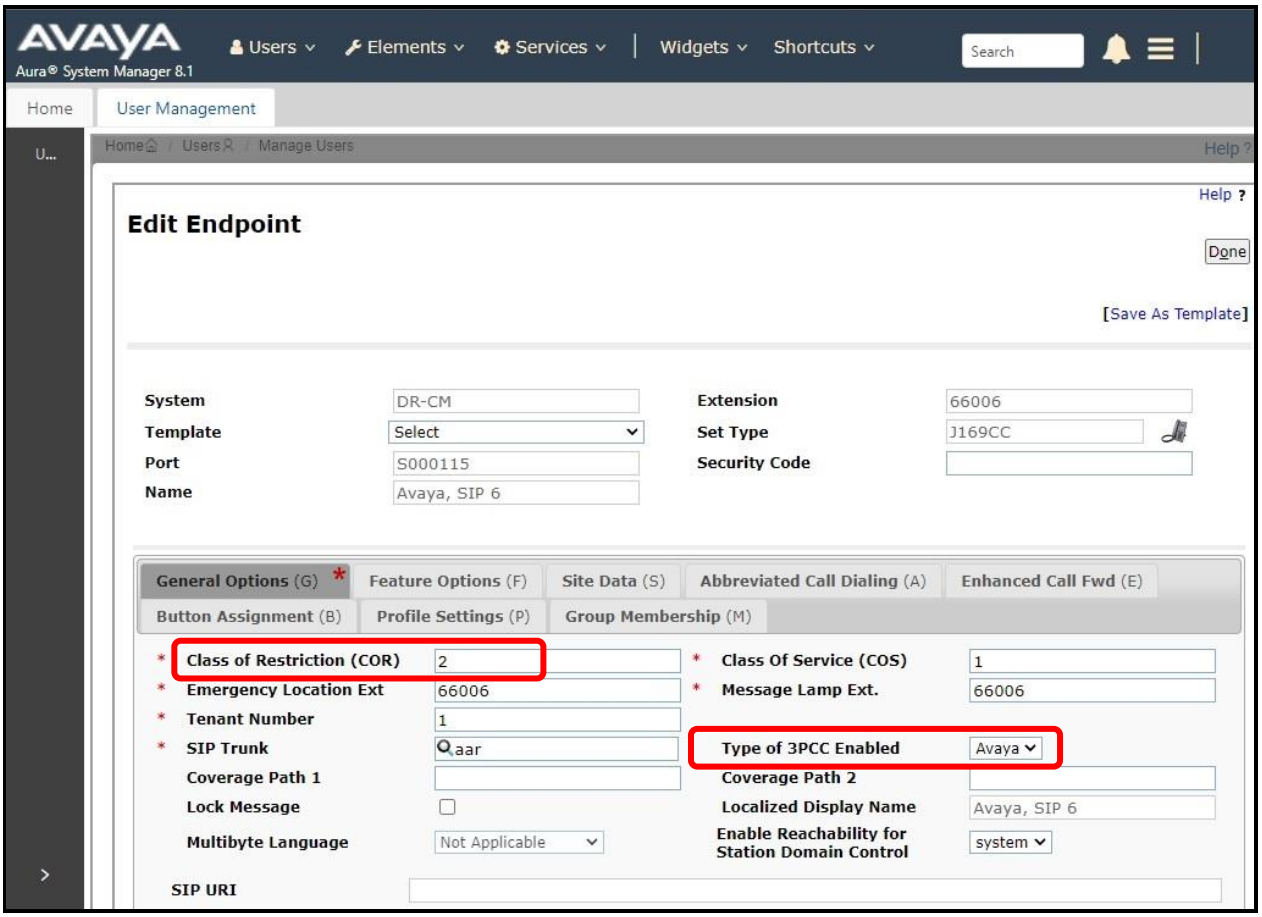


©2021 Avaya Inc. All Rights Reserved.

The **Edit Endpoint** pop-up screen is displayed. For **Class of Restriction (COR)**, enter the COR number from **Section 5.5**.

For **Type of 3PCC Enabled**, select "**Avaya**" as shown below.

Repeat this section for all SIP agent stations from **Section 3**. In the compliance testing, one SIP agent station was configured.



©2021 Avaya Inc. All Rights Reserved.

8. Configure HigherGround Calibre

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

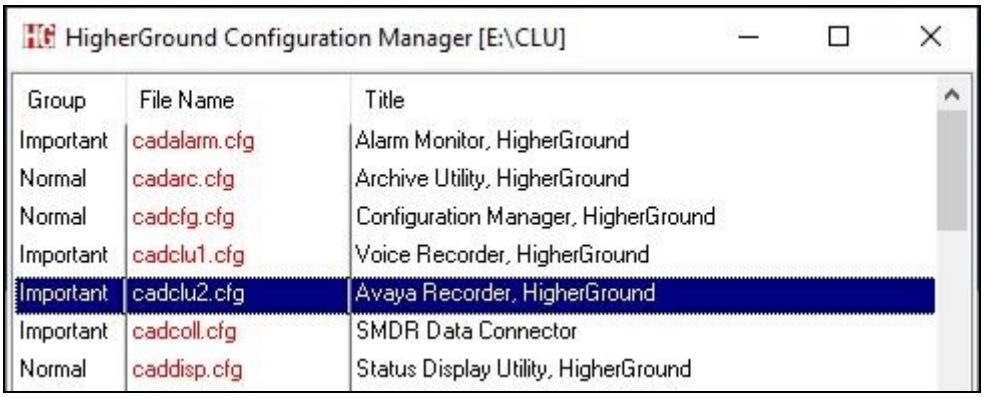
- Administer Avaya Recorder
- Restart service
- Administer station utility
- Administer VoIP channel
- Administer DMCCso.cfg

The configuration of Calibre is performed by the HigherGround technicians and the procedural steps are presented in these Application Notes for information purposes only.

8.1. Administer Avaya Recorder

From the Calibre server, double-click on the **HG4 Configuration Manager** shortcut icon shown below, which was created as part of Calibre installation. Log in using the appropriate credentials in the subsequent screen (not shown).

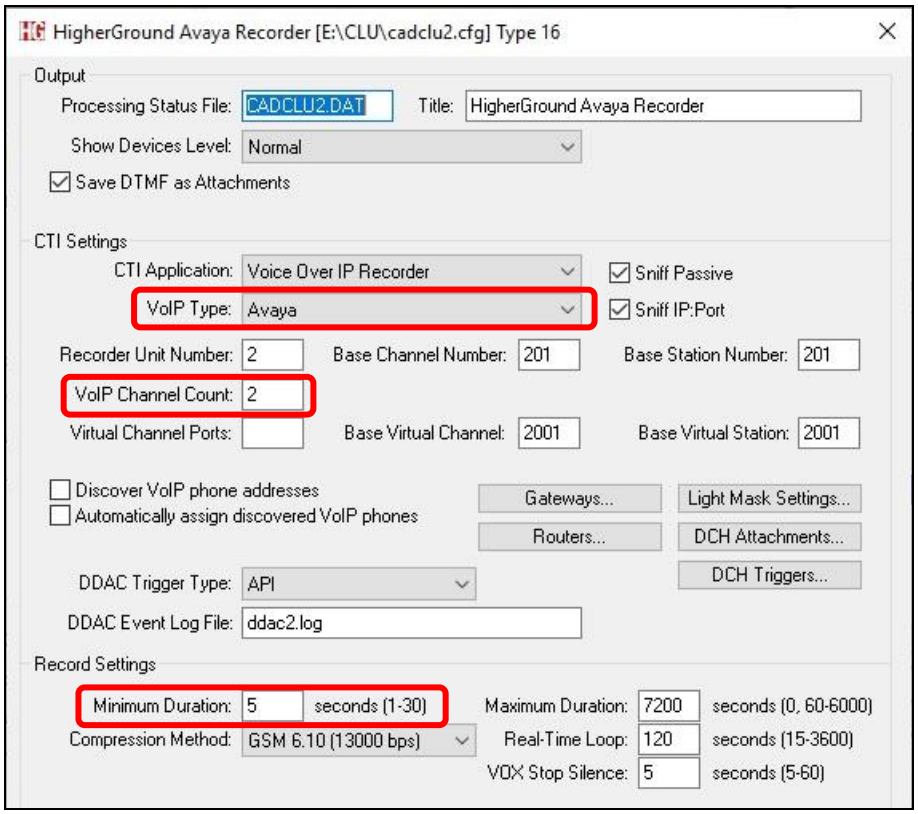
The **HigherGround Configuration Manager** screen is displayed. Double click on the **Avaya Recorder** entry shown below.



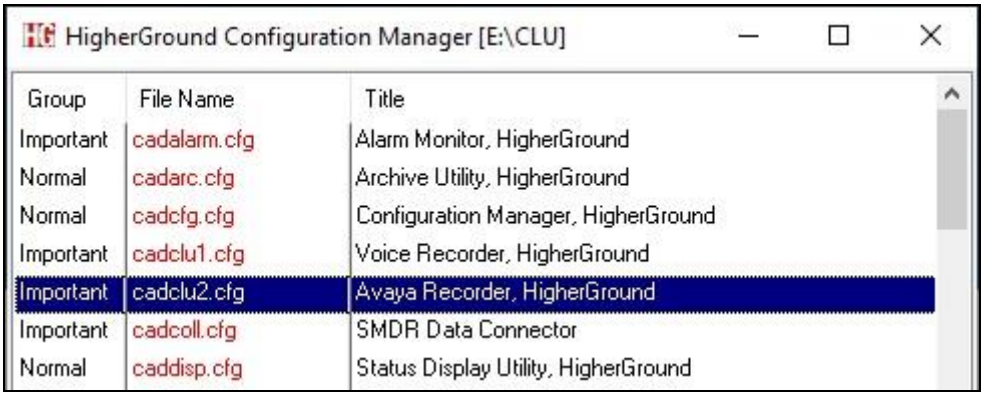
©2021 Avaya Inc. All Rights Reserved.

The **HigherGround Avaya Recorder** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **VoIP Type:** "Avaya"
- **VoIP Channel Count:** The number of virtual IP softphones from **Section 5.7**.
- **Minimum Duration:** The desired minimal duration for recordings.

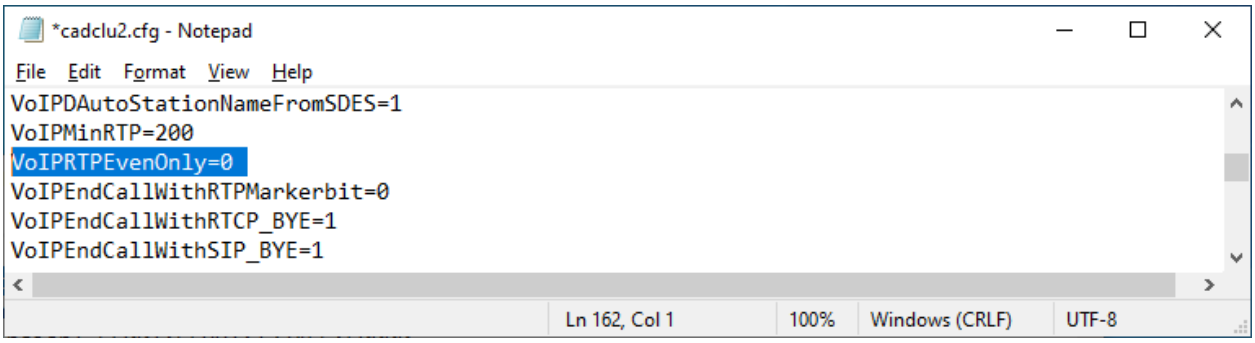


The **HigherGround Configuration Manager** screen is displayed again. Right click on the **Avaya Recorder** entry and select **Open with Notepad**.

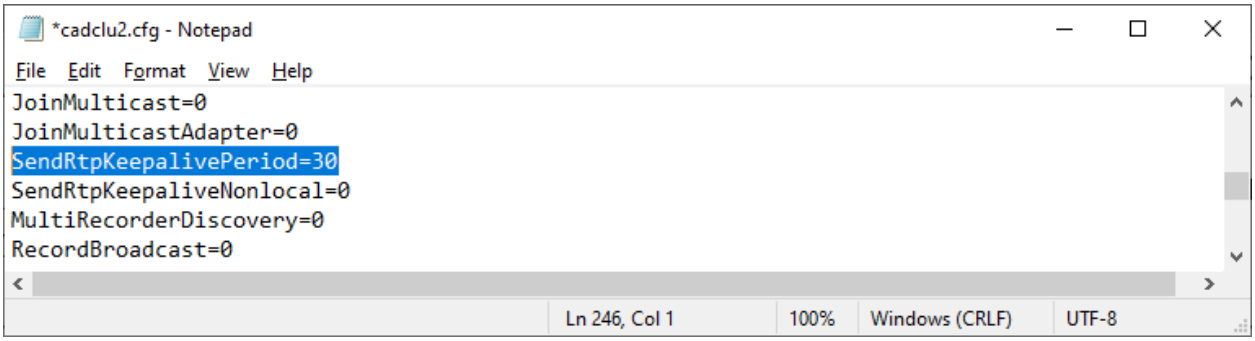


©2021 Avaya Inc. All Rights Reserved.

Locate the **VoIPRTPEvenOnly** parameter and set the value to "**0**" as shown below. This setting allows for both odd and even RTP ports.

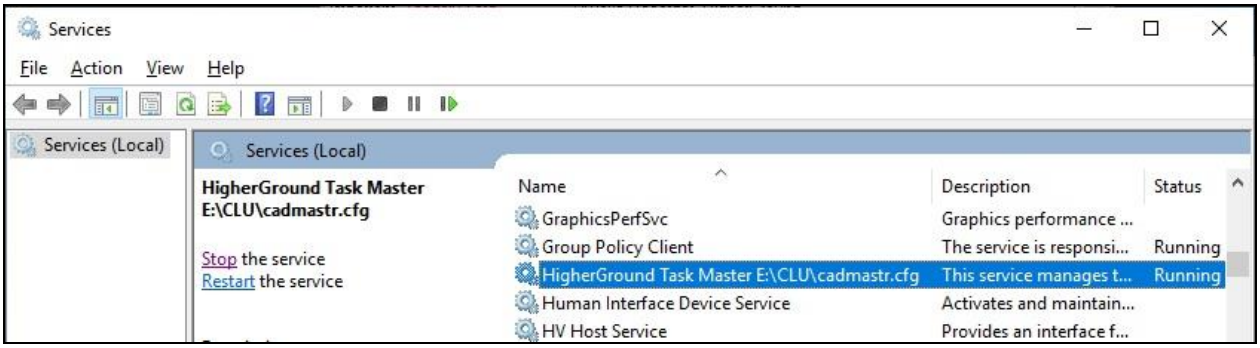


Locate the **SendRtpKeepalivePeriod** parameter and set the value to "**30**" as shown below.



8.2. Restart Service

From the Calibre server, select **Start → Control Panel → Administrative Tools → Services** to display the **Services** screen. Stop and then start the **HigherGround Task Master** service shown below.

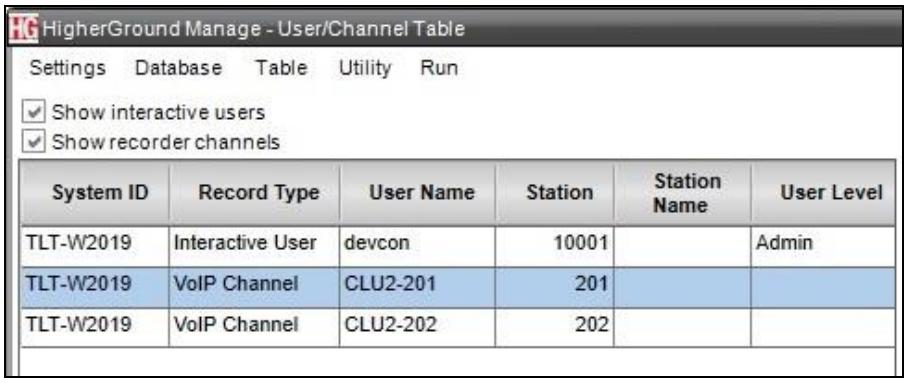


©2021 Avaya Inc. All Rights Reserved.

8.3. Administer Station Utility

From the Calibre server, double-click on the **HG4 Manage** shortcut icon shown below, which was created as part of Calibre installation. Log in using the appropriate credentials in the subsequent screen (not shown).

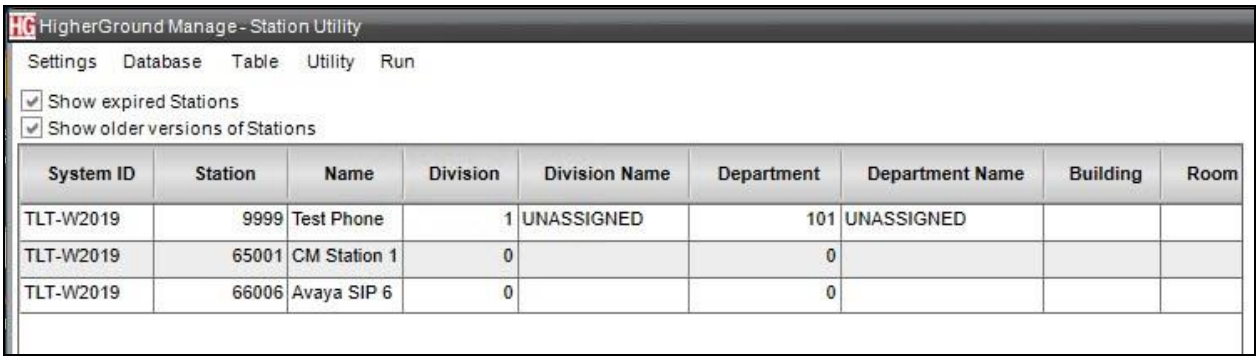
The **HigherGround Manage – User/Channel Table** screen is displayed. Select **Utility → Station Utility** from the top menu.



System ID	Record Type	User Name	Station	Station Name	User Level
TLT-W2019	Interactive User	devcon	10001		Admin
TLT-W2019	VoIP Channel	CLU2-201	201		
TLT-W2019	VoIP Channel	CLU2-202	202		

The **HigherGround Manage – Station Utility** screen is displayed next. Create an entry for each agent station extension from **Section 3** with pertinent **Station** extension and desired **Name** value.

In the compliance testing, two entries were created as shown below.

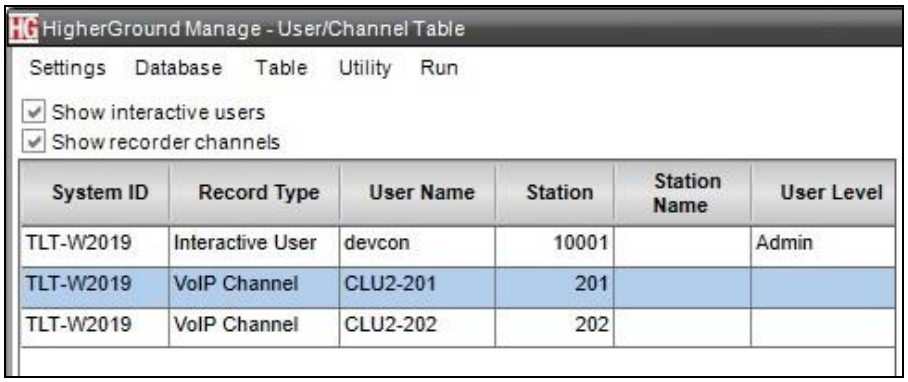


System ID	Station	Name	Division	Division Name	Department	Department Name	Building	Room
TLT-W2019	9999	Test Phone	1	UNASSIGNED	101	UNASSIGNED		
TLT-W2019	65001	CM Station 1	0		0			
TLT-W2019	66006	Avaya SIP 6	0		0			

©2021 Avaya Inc. All Rights Reserved.

8.4. Administer VoIP Channel

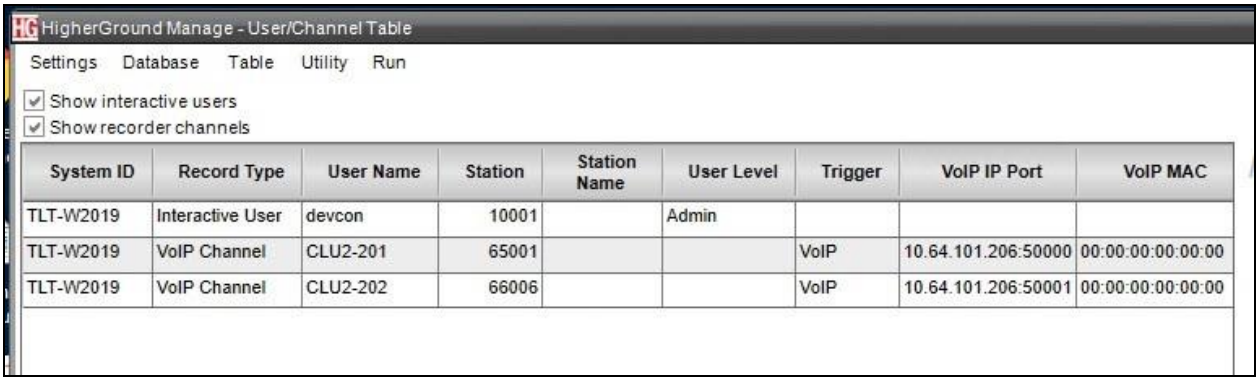
Select **Home** (not shown) from the bottom of the **HigherGround Manage – Station Utility** screen in **Section 8.3** to display the **HigherGround Manage – User/Channel Table** screen below. Note that two VoIP Channel entries were auto created as result of the VoIP channel count setting in **Section 8.1**.



System ID	Record Type	User Name	Station	Station Name	User Level
TLT-W2019	Interactive User	devcon	10001		Admin
TLT-W2019	VoIP Channel	CLU2-201	201		
TLT-W2019	VoIP Channel	CLU2-202	202		

For each **VoIP Channel** entry, assign a station utility extension from **Section 8.3**. For **VoIP IP Port**, use the IP address of the Calibre server and an available port number starting with 50000.

In the compliance testing, two **VoIP Channel** entries were updated as shown below.

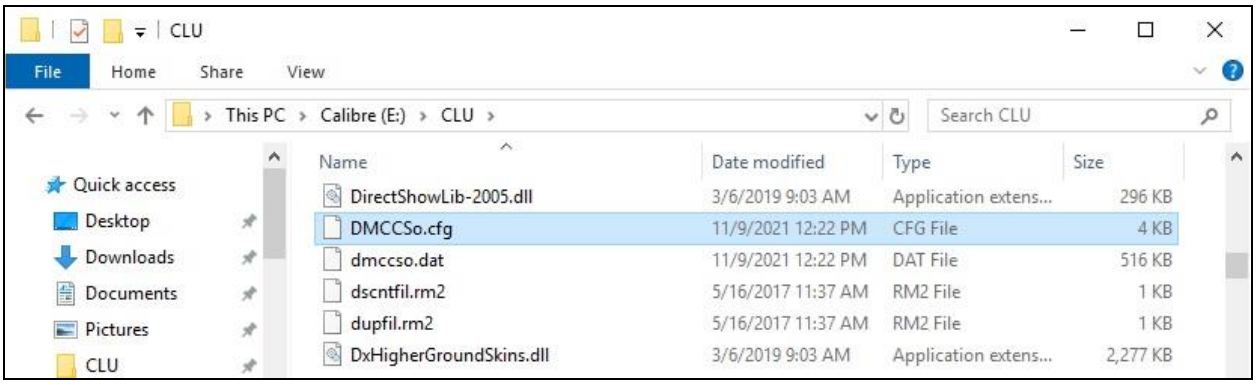


System ID	Record Type	User Name	Station	Station Name	User Level	Trigger	VoIP IP Port	VoIP MAC
TLT-W2019	Interactive User	devcon	10001		Admin			
TLT-W2019	VoIP Channel	CLU2-201	65001			VoIP	10.64.101.206:50000	00:00:00:00:00:00
TLT-W2019	VoIP Channel	CLU2-202	66006			VoIP	10.64.101.206:50001	00:00:00:00:00:00

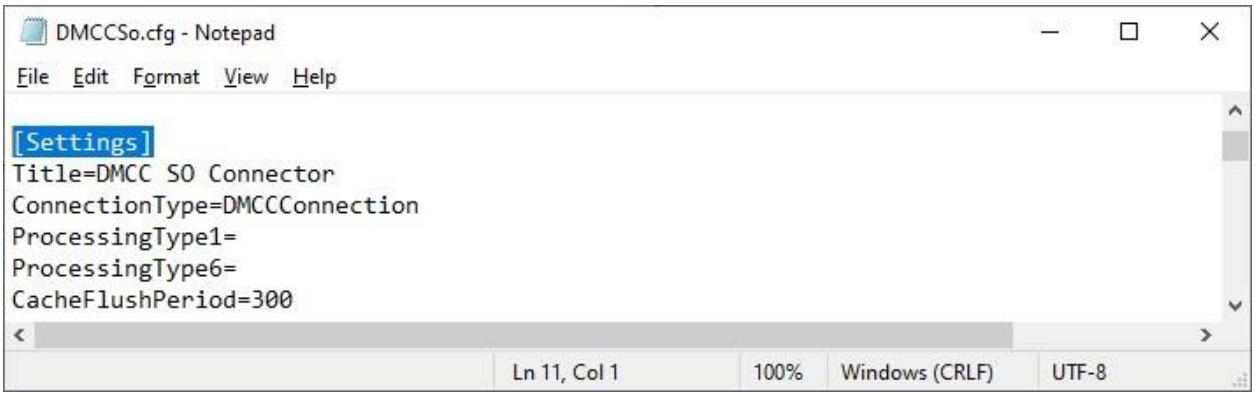
©2021 Avaya Inc. All Rights Reserved.

8.5. Administer DMCCso.cfg

From the Calibre server, navigate to the Calibre install directory and open the **DMCCSo.cfg** file with a text editor such as Notepad.



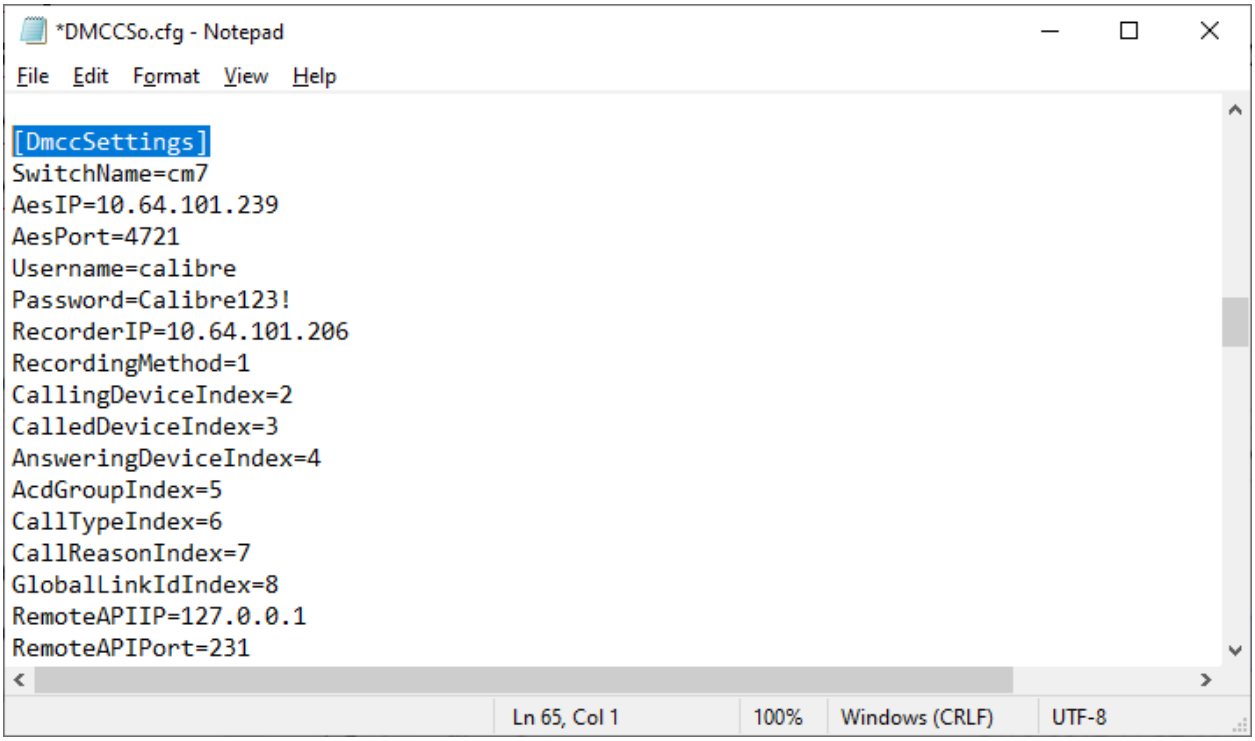
Navigate to the **Settings** sub-section and set **ConnectionType** to "**DMCCConnection**" as show below.



©2021 Avaya Inc. All Rights Reserved.

Navigate to the **DmccSettings** sub-section. Enter the following values for the specified fields and retain the default values for the remaining fields.

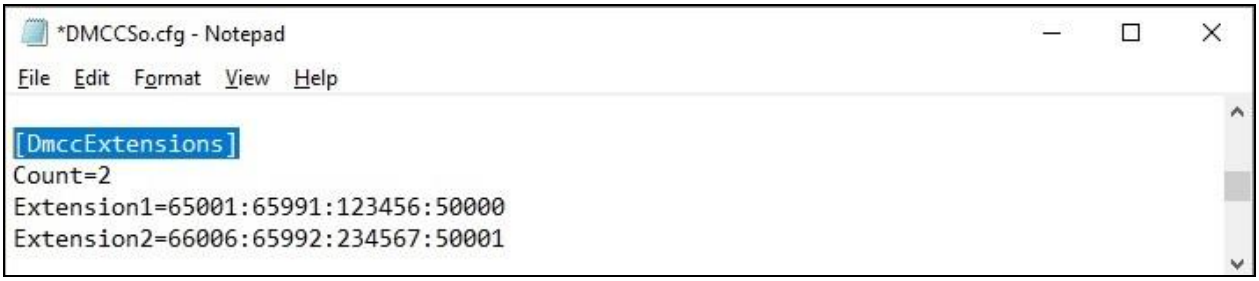
- **SwitchName:** The switch connection name from **Section 6.3**.
- **AesIP:** IP address of Application Enablement Services.
- **AesPort:** The DMCC unencrypted port from **Section 6.7**.
- **Username:** The Calibre user credentials from **Section 6.5**.
- **Password:** The Calibre user credentials from **Section 6.5**.
- **RecorderIP:** IP address of the Calibre server.
- **RecordingMethod:** "1" for Service Observing.
- **CallingDeviceIndex:** "2"
- **CalledDeviceIndex**: "3"
- **AnsweringDeviceIndex**: "4"
- **AcdGroupIndex:** "5"
- **CallTypeIndex**: "6"
- **CallReasonIndex**: "7"
- **GlobalLinkIdIndex:** "8"



©2021 Avaya Inc. All Rights Reserved.

Navigate to the **DmccExtensions** sub-section. Create an extension entry for each VoIP channel and associated station from **Section 8.4**. Set the **Count** parameter to the number of extension entries.

For each extension entry, set the value to the station extension associated with a VoIP channel from **Section 8.4** , followed by an available virtual IP softphone extension and security code from **Section 5.7**, and the VoIP channel port number from **Section 8.4**. In the compliance testing, two extension entries were created as shown below.



Navigate to the **DmccAcdGroups** sub-section. Create an ACD group entry for each skill group from **Section 3**. Set the **Count** parameter to the number of ACD group entries.

For each ACD group entry, set the value to a skill group extension from **Section 3** followed by zeroes. In the compliance testing, two ACD group entries were created as shown below.

Make certain that there is a **RecorderController** sub-section with parameters and default values shown below.

Follow the procedures in **Section 8.2** to stop and start the **HigherGround Task Master** service again.

©2021 Avaya Inc. All Rights Reserved.

9. Verification Steps

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

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    aes7             established   45       53
```

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

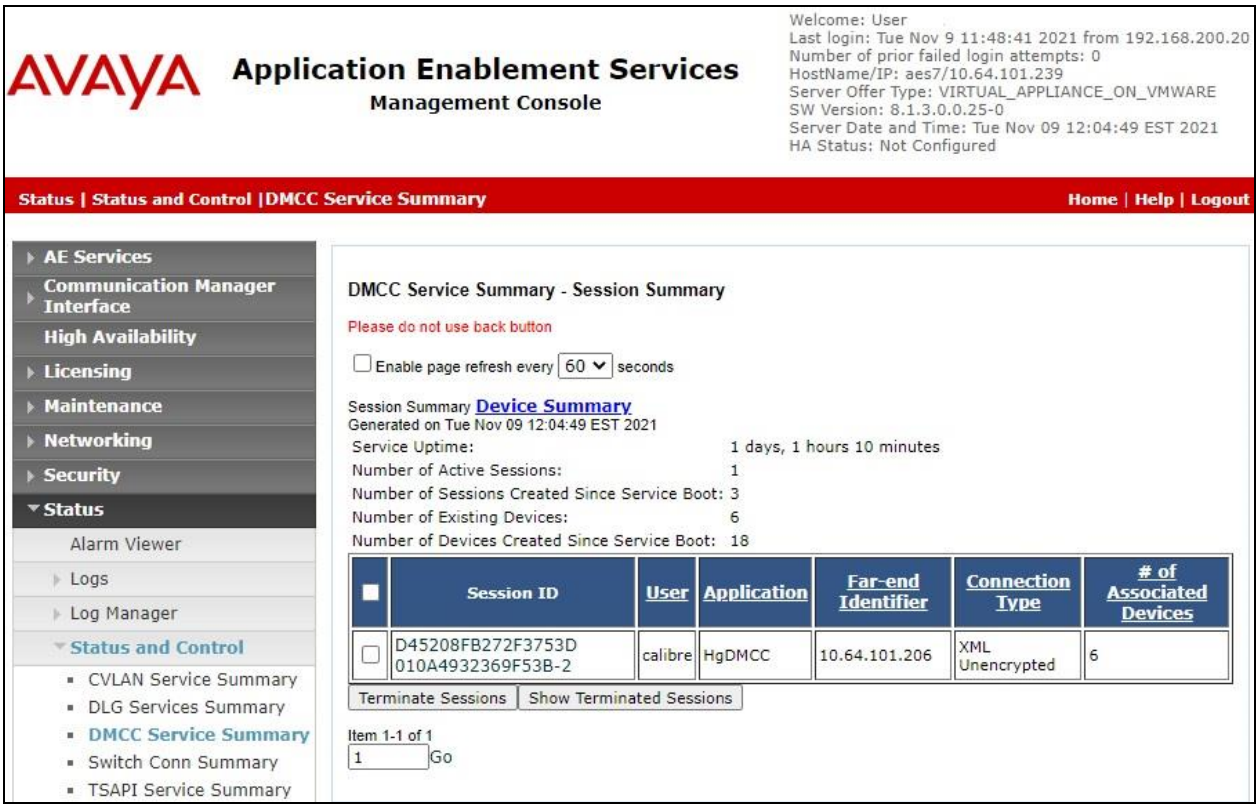
```
list registered-ip-stations

                            REGISTERED IP STATIONS

Station Ext      Set Type/ Prod ID/    Station IP Address/
or Orig Port     Net Rgn   Release     Gatekeeper IP Address
  Socket
65000            9611      IP_Phone    192.168.200.179
  tls            1         6.8502      10.64.101.236
65001            9611      IP_Phone    192.168.200.212
  tls            1         6.8502      10.64.101.236
65991            9608      IP_API_A    10.64.101.239
  tcp            1         3.2040      10.64.101.236
65992            9608      IP_API_A    10.64.101.239
  tcp            1         3.2040      10.64.101.236
```


©2021 Avaya Inc. All Rights Reserved.

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.

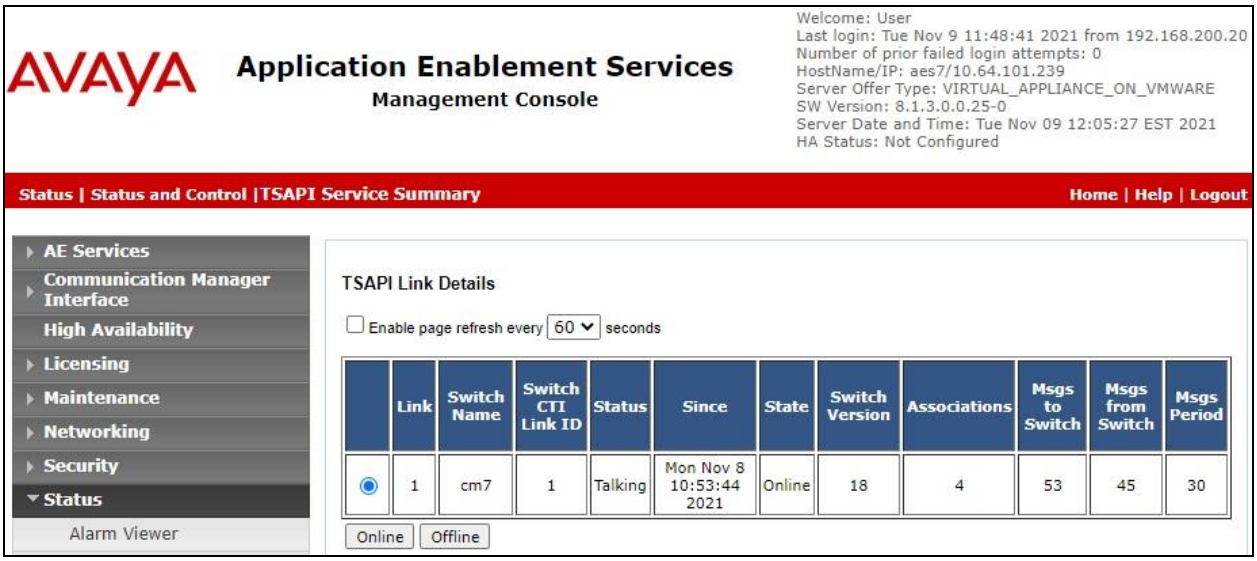
Verify the **User** column shows an active session with the Calibre user name from **Section 6.5** and that the number **# of Associated Devices** reflects the total number of monitored skill groups and agent stations from **Section 3** plus the number of virtual IP softphones from **Section 5.7**, in this case "**6**".



©2021 Avaya Inc. All Rights Reserved.

Verify status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** (not shown) 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 "**4**".

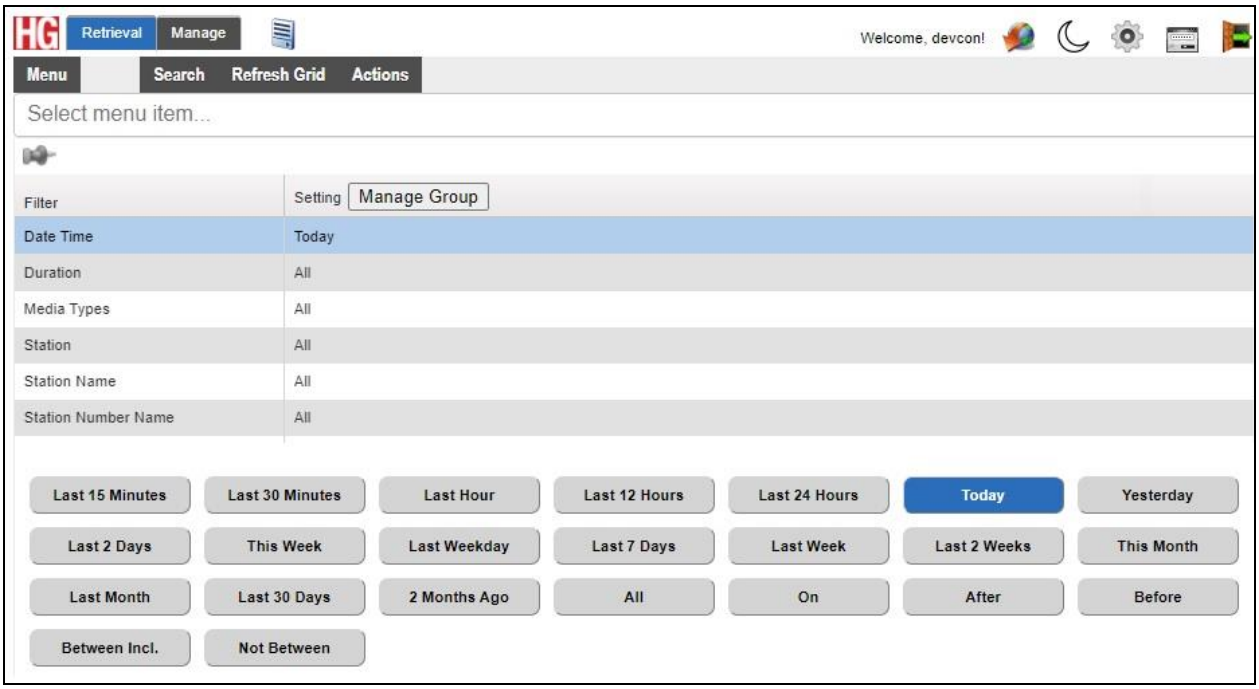


©2021 Avaya Inc. All Rights Reserved.

9.3. Verify HigherGround Calibre

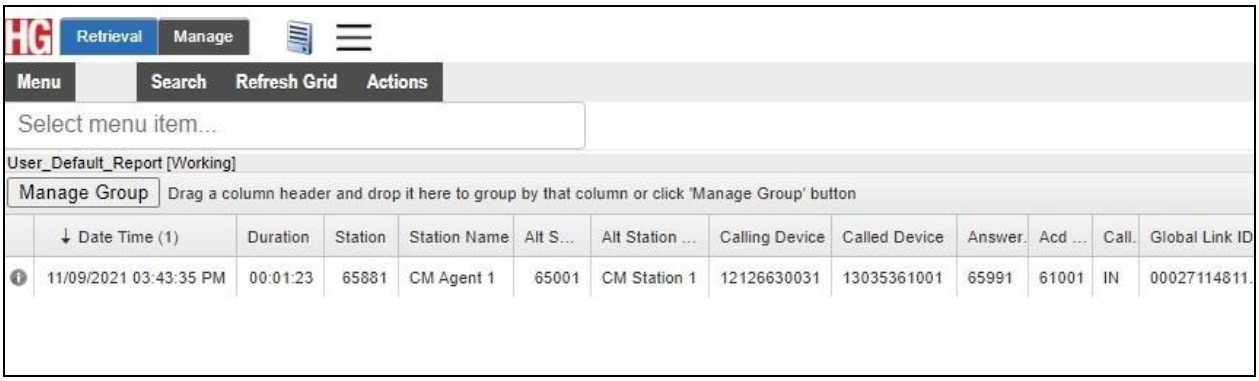
Log an agent in to handle and complete an ACD call. Access the Calibre web interface by using the URL "**http://ip-address/WBI**" where "**ip-address**" is the IP address of the Calibre server. Log in using the appropriate credentials.

The screen below is displayed. Select the **Retrieval** tab followed by **Search** then **Today**.



©2021 Avaya Inc. All Rights Reserved.

The screen is updated with a list of call recordings for today. Verify that there is an entry for the last call with proper values in the relevant fields as shown below.



Double click on the entry, and verify that the recording can be played back.

©2021 Avaya Inc. All Rights Reserved.

10. Conclusion

These Application Notes describe the configuration steps required for Calibre 9 to successfully interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 using Service Observing. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 8, November 2020, available at http://support.avaya.com.

2. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 8, December 2020, available at http://support.avaya.com.

3. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 8, February 2021, available at http://support.avaya.com.

4. *HG4 Installation Manual, v.9.2021,* available as part of Calibre installation.

5. *HG4 Admin Manual, v.9.2020,* available as part of Calibre installation.

6. *HG4 User Manual, v.9.2020,* available as part of Calibre installation.

©2021 Avaya Inc. All Rights Reserved.

©2021 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.