Avaya Solution & Interoperability Test Lab

Application Notes for MiaRec On Premise Call Recording & Quality Management R7 with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the MiaRec On Premise Call Recording & Quality Management to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

MiaRec On Premise Call Recording & Quality Management uses the Avaya Aura® Application Enablement Services Device, Media and Call Control (DMCC) and Telephony Services Application Programming Interface (TSAPI) services to capture real-time CTI data and RTP streams from Avaya Aura® Communication Manager.

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

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

1. Introduction

MiaRec On Premise Call Recording & Quality Management (MiaRec) is a call recording and quality management solution that uses the DMCC and TSAPI interfaces to interoperate with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager.

The MiaRec DMCC integration works by using the DMCC Multiple Registration method to capture the media for Avaya SIP, H.323 and digital endpoints. MiaRec uses the TSAPI interface to extract call state information for Avaya SIP, H.323 and digital endpoints.

2. General Test Approach and Test Results

The compliance test focused on the ability for calls to be recorded. Calls were manually placed from the public switched telephone network (PSTN) directly to and from recorded devices, and to VDN or Skill group extensions. For each recorded station in a call, there is one recording generated. Once a call is completed, the recordings are reviewed for their quality, completeness (number of recordings beginning to end, etc.), and accuracy of tagging information (owner, calling party, called party, etc).

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 MiaRec did not include use of any specific encryption features.

2.1. Interoperability Compliance Testing

The compliance test validated the ability of MiaRec to successfully record various types of calls routed to and from Avaya digital, H.323 and SIP endpoints. The feature testing included the following:

- Handling of real-time TSAPI call events
- Use of AES DMCC registration services to register and un-register the virtual IP Softphone
- Use of AES DMCC monitoring services and media control events to obtain the media from the virtual IP Softphones
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, agent drop, customer drop, hold, reconnect, transfer and conference.

Additionally, testing confirmed the ability for MiaRec to recover from common outages such as network outages and server reboots.

2.2. Test Results

All test cases passed with the following observations.

- In a scenario where an Avaya SIP station consult transfers a call to another Avaya endpoint, call association on the MiaRec portal is not available. However, calls are recorded successfully.

2.3. Support

For technical support on MiaRec products please contact MiaRec.

- **Email:** support@miarec.com
- **Phone:** +1-866-324-6717
- **Web:** www.miarec.com

3. Reference Configuration

Figure 1 illustrates the compliance test configuration consisting of:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya Aura® Application Enablement Services
- Avaya Endpoints
- MiaRec server

Calls routed to and from Communication Manager used PRI trunks to connect to the PSTN.

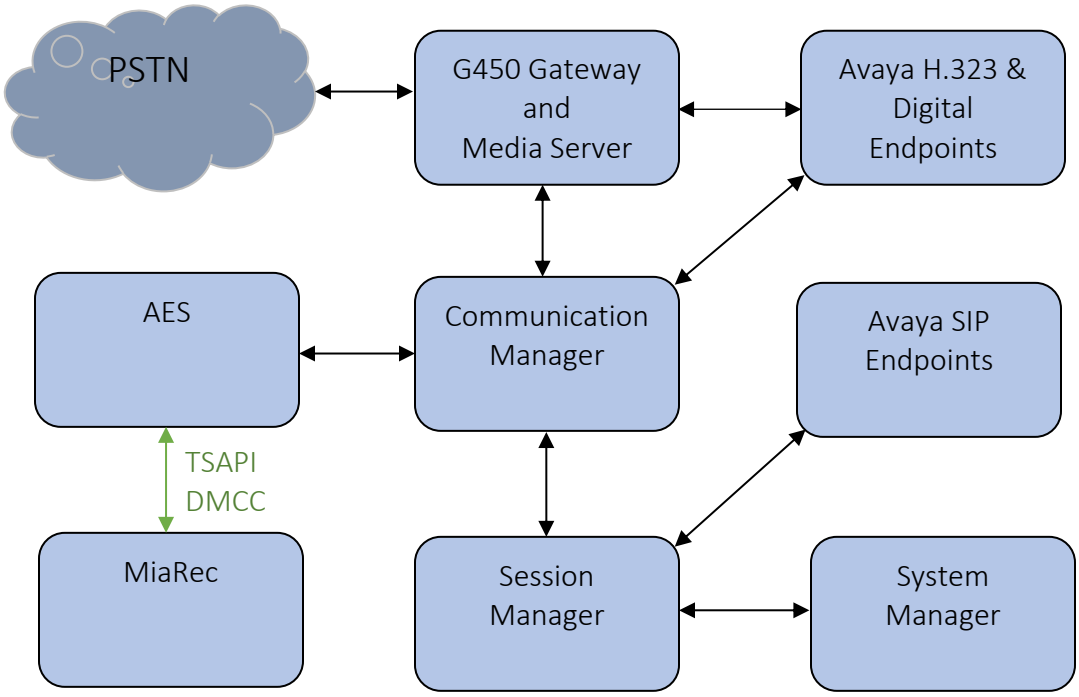


Figure 1 – MiaRec Compliance Test Configuration

4. Equipment and Software Validated

The following equipment and version were used in the reference configuration described above:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	CM 8.1.1.0.0.890.25763 (R018x.01.0.890.0)
Avaya Aura® Application Enablement Services running on virtualized environment	8.1.1.0.0.8-0
Avaya Aura® Session Manager running on virtualized environment	8.1.1.0.811021
Avaya Aura® System Manager running on virtualized environment	8.1.1.0.0310504
Avaya Aura® Media Server running on virtualized environment	8.0.2.61
Avaya G450 Media Gateway	41.9.0
Avaya IP Endpoints • 9608 (H.323) • J169 (H.323) • 9641GS (SIP) • J179 (SIP)	 6.8.3 6.8.3 7.1.7.1 4.0.3.1
Avaya 9404 Digital Telephone	17.0
Desktop PC running Avaya One-X® Communicator (H.323)	6.2.14 SP14
MiaRec On Premise Call Recording & Quality Management running on Microsoft 2016 Standard virtual machine • MiaRec Web Portal • MiaRec Recorder • Avaya TSAPI SDK • Avaya DMCC SDK	 7.0.0.327 7.0.0.19 (Build Aug 6 2019) 8.1 8.1

5. Configure Avaya Aura® Communication Manager

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

- Verify Feature and License for the integration
- Administer Communication Manager System Features
- Administer IP Services for Application Enablement Services
- Administer Computer Telephony Integration (CTI) Link
- Configure COR
- Verify Recorded Extensions

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more details on configuring Communication Manager, refer to the Avaya product documentation in **Section 10**.

5.1. Verify Feature and License

Enter the **display system-parameters customer-options** command and ensure that **Computer Telephony Adjunct Links** is set to **y.** If this option is not set to **y**, contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                      Page   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? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
             ATM WAN Spare Processor? n                            DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y



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

5.2. Administer Communication Manager System Features

Enter the **change system-parameters features** command and ensure that on page 5 **Create Universal Call ID (UCID)** is enabled and a relevant **UCID Network Node ID** (**1** was used in the test) is defined. Also ensure that on page 13 that **Send UCID to ASAI** is set to **y**. MiaRec relies on UCID to track complex calls (Transfers and Conferences).

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

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                     Switch Name:
            Emergency Extension Forwarding (min): 10
          Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                              COR to Use for DPT: station
                EC500 Routing in Survivable Mode: dpt-then-ec500
MALICIOUS CALL TRACE PARAMETERS
                Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:
      Delay Sending RELease (seconds): 0
SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
               Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
```

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

    Reporting for PC Non-Predictive Calls? n

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

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

5.3. Administer IP-Services for Application Enablement Services

Add an IP Services entry for Application Enablement Services as described below:

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

```
change ip-services                                          Page   1 of   3

                                   IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
AESVCS         y       procr            8765
```

On Page 3 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the host name of the Application Enablement Services server.
- In the **Password** field, type the same password to be administered on the Application Enablement Services server in **Section 6.1**.
- In the **Enabled** field, type **y**.

```
change ip-services                                          Page   3 of   3
                           AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:       aes81              *                    y        in use
```

5.4. Administer Computer Telephony Integration (CTI) Link

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

- In the **Extension** field, type a valid extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

```
add cti-link 1                                              Page   1 of   3
                                   CTI LINK
 CTI Link: 1
Extension: 77777
     Type: ADJ-IP
                                                                  COR: 1
     Name: CTI Link 1
Unicode Name? n
```

5.6. Verify Recorded Extensions – H.323 and Digital

For H.323 and digital stations that will be recorded, enable **IP Softphone** as shown below, which will be used by MiaRec to correspond to the Multiple Registration recording method.

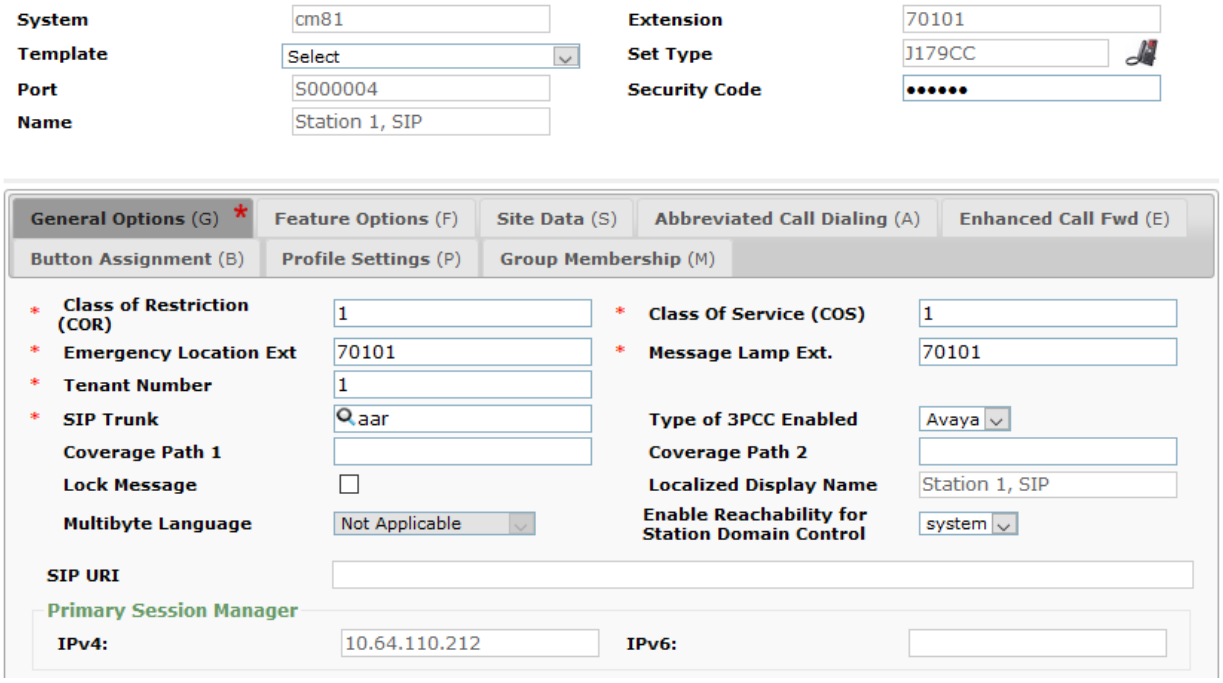
Use the **display station n** command to verify information, or **change station n** to make changes if necessary.

```
change station 70001                                          Page   1 of   5
                                    STATION

Extension: 70001                        Lock Messages? n               BCC: 0
     Type: 9641                         Security Code: *                TN: 1
     Port: S000000                    Coverage Path 1: 98             COR: 1
     Name: H.323 Station 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: 50001
            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
```

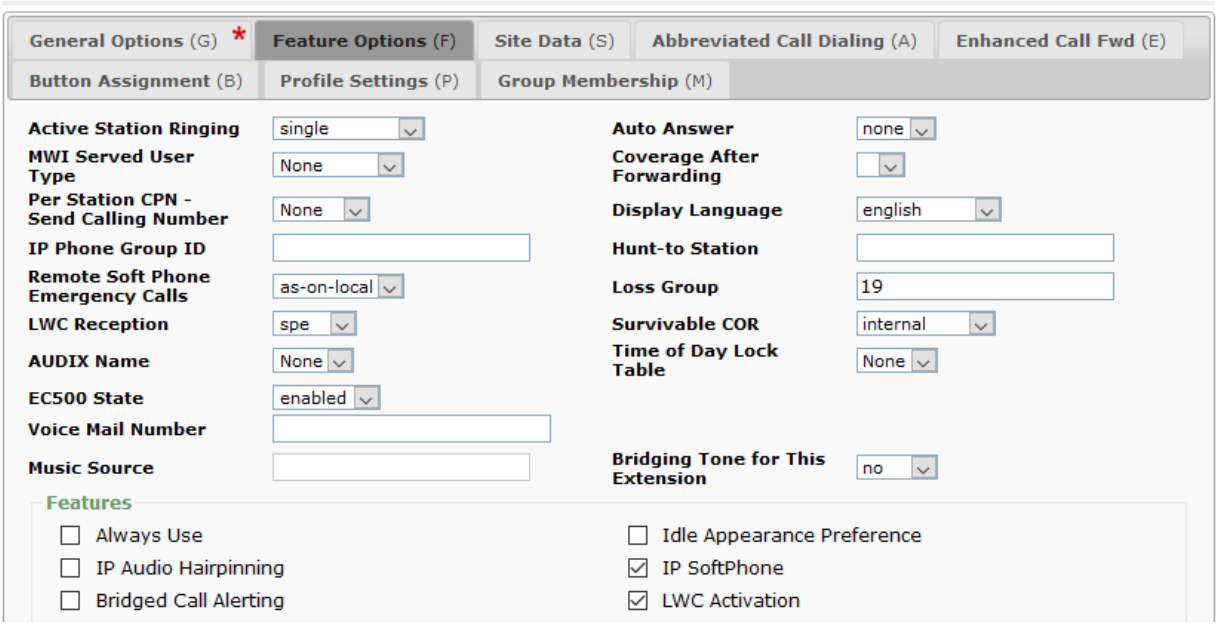
5.7. Verify Recorded Extensions – SIP

For SIP stations that will be recorded, enable **3PCC** and **IP Softphone** as shown below, which will be used by MiaRec to correspond to the Multiple Registration recording method.

Via System Manager, edit a SIP station that will be recorded and for the **CM Endpoint Profile,** select the **Endpoint Editor**. Set the **Type of 3PCC Enabled** to **Avaya.**



Under the **Feature Options** tab, check box for **IP SoftPhone.**

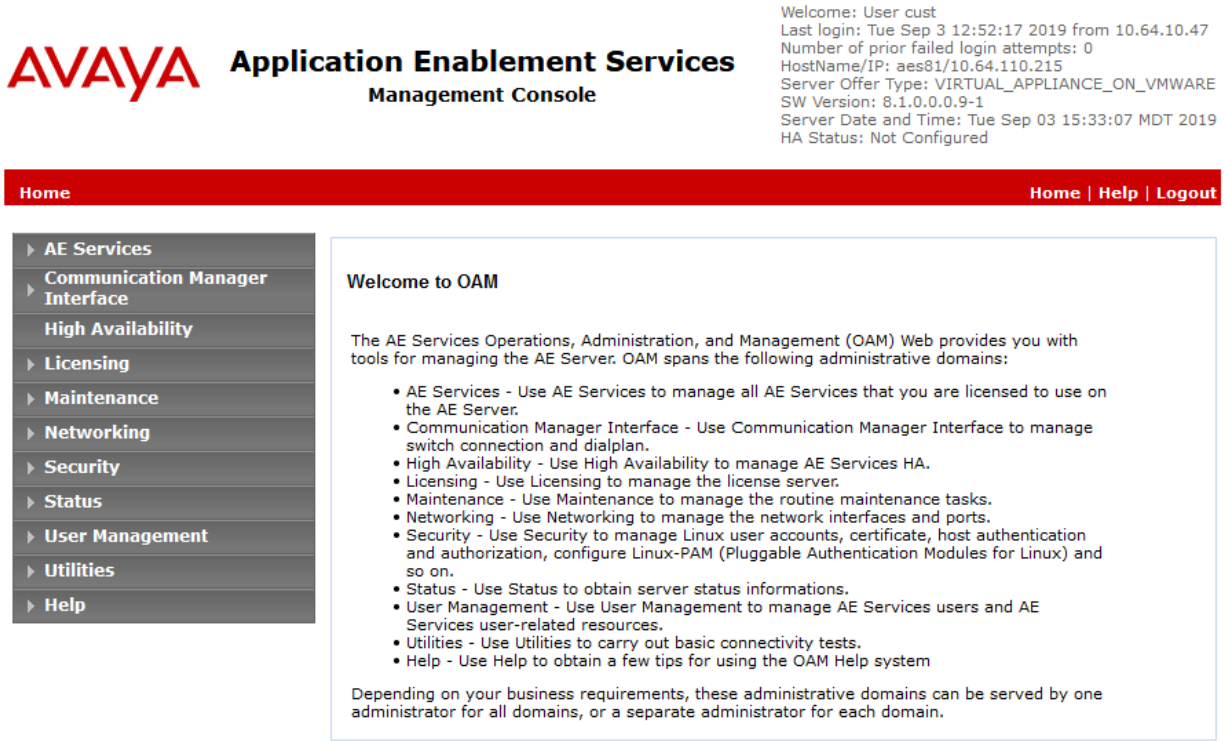


6. Configure Avaya Aura® Application Enablement Services

All administration of Application Enablement Services is performed via a web browser. Enter https://<ip-addr> in the URL field of a web browser where <ip-addr> is the IP address of the Application Enablement Services server. After a login step, the **Welcome to OAM** page is displayed. Note that all navigation is performed by clicking links in the Navigation Panel on the left side of the screen, context panels will then appear on the right side of the screen.

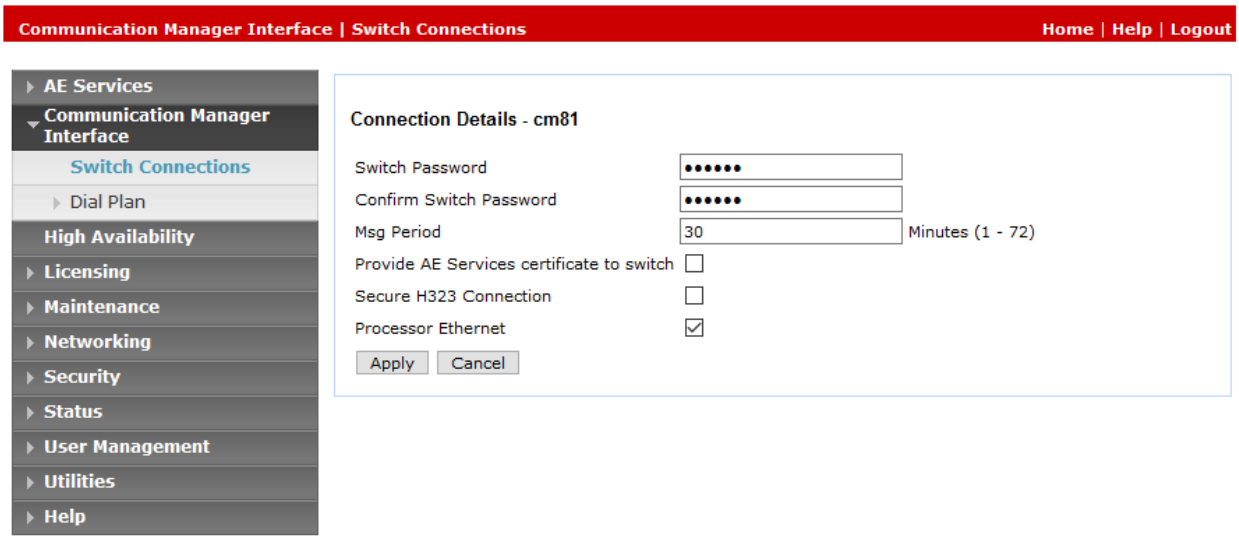
The procedures fall into the following areas:

- Configure Communication Manager Switch Connections
- Configure TSAPI Link
- Configure MiaRec User
- Enable Security Database
- Confirm TSAPI and DMCC Licenses

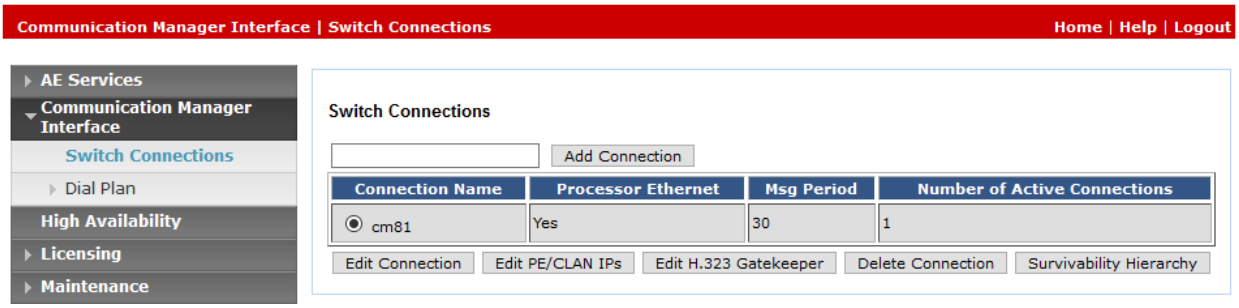


6.1. Configure Communication Manager Switch Connections

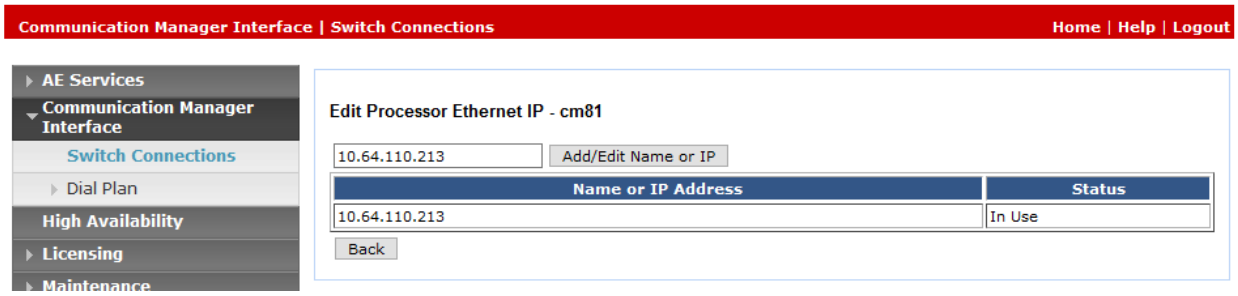
To add links to Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection (e.g. **cm81**) and click the **Add Connection** button (not shown). The **Connection Details** screen is shown. Enter the **Switch Password** configured in **Section 5.3** and check the **Processor Ethernet** box if using the **procr** interface. Click **Apply**.



The display returns to the **Switch Connections** screen which shows that the **cm81** switch connection has been added.



Click the **Edit PE/CLAN IPs** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es). The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of the **procr** interface and click the **Add/Edit Name or IP** button.

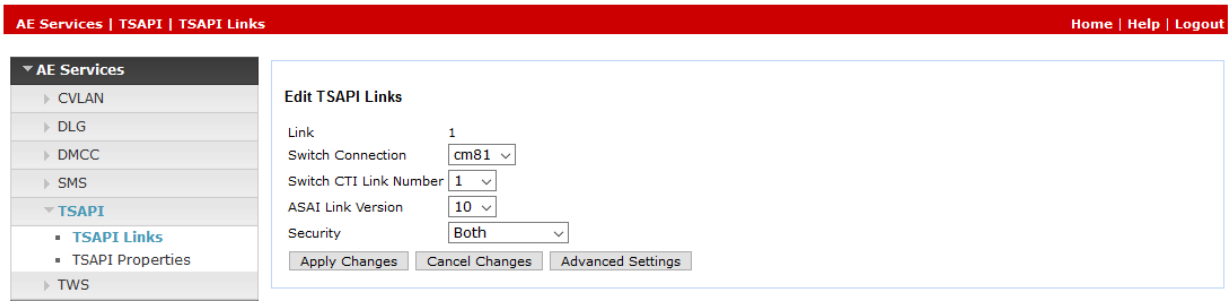


6.2. Configure TSAPI Link

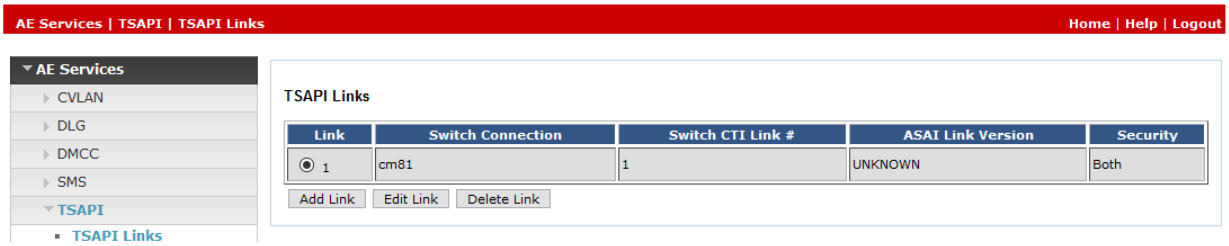
Navigate to the **AE Services →TSAPI → TSAPI Links** page to add a TSAPI CTI Link. Click **Add Link** (not shown).

Select a **Switch Connection** using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The **Switch CTI Link Number** must match the number configured in the **cti-link** form in **Section 5.3**. Select **Both** in the **Security** field.

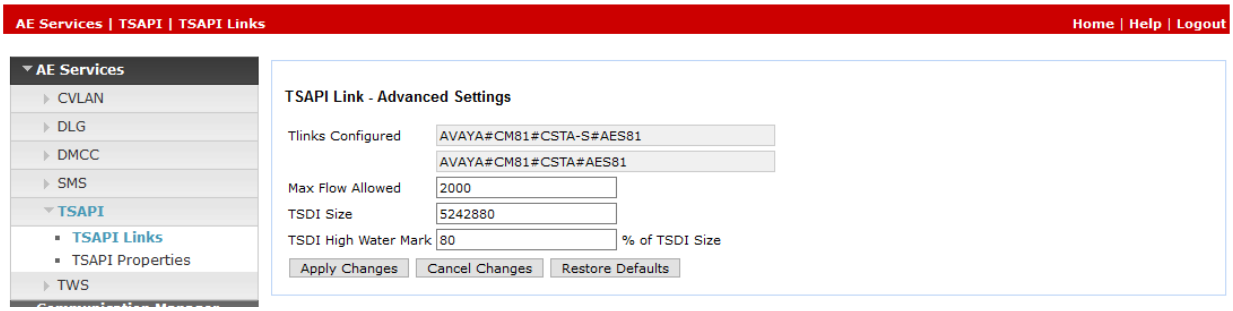
Click **Apply Changes**.



It returns to the **TSAPI Links** screen which shows that the link has been added.



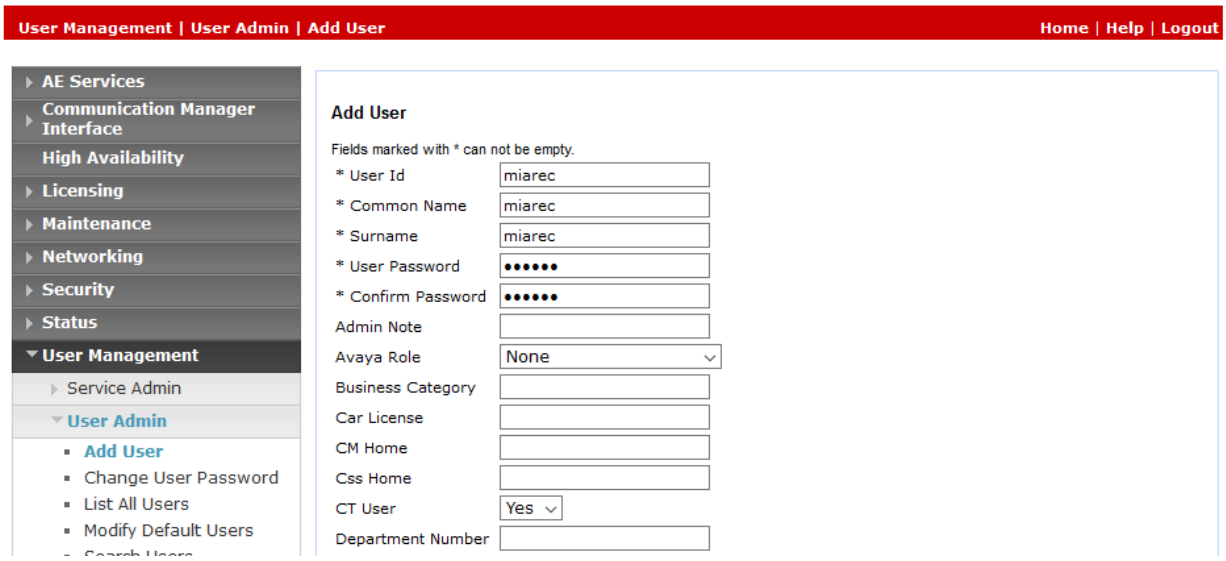
Click **Edit Link →Advanced Setting** to obtain the TSAPI Link that will be used by MiaRec.



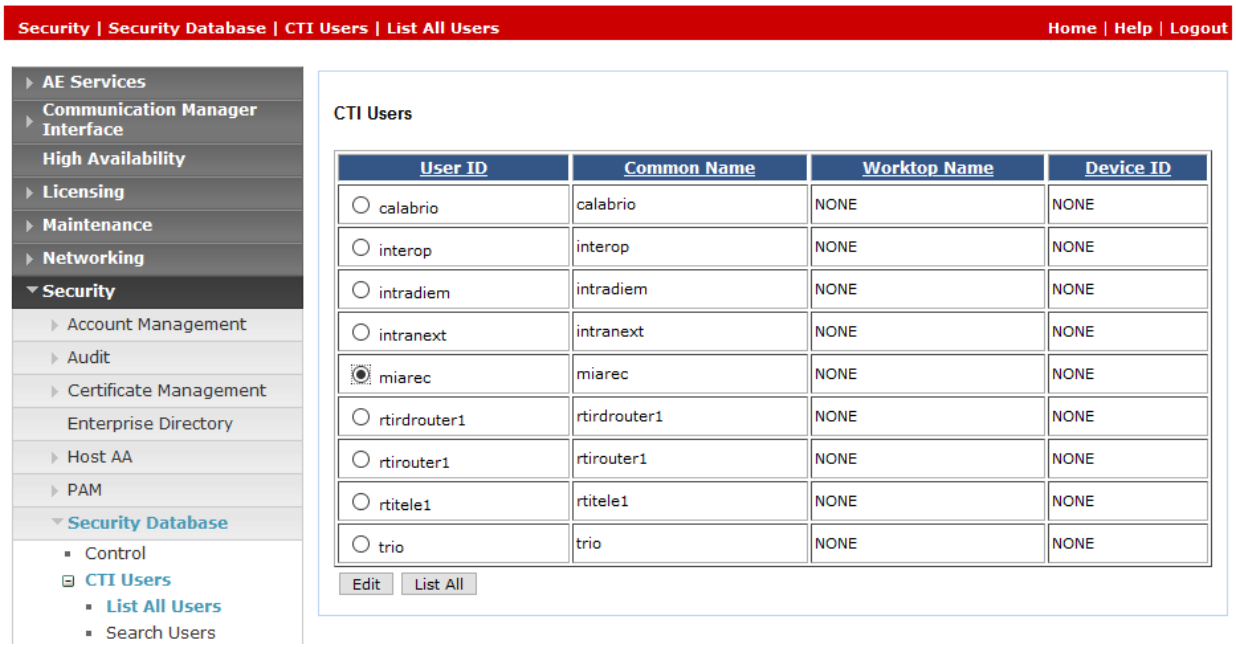
6.3. Configure MiaRec User

In the Navigation Panel, select **User Management → User Admin → Add User**. The **Add User** panel will display as shown below. Enter an appropriate **User Id**, **Common Name**, **Surname**, and **User Password**. Select **Yes** from the **CT User** dropdown list.

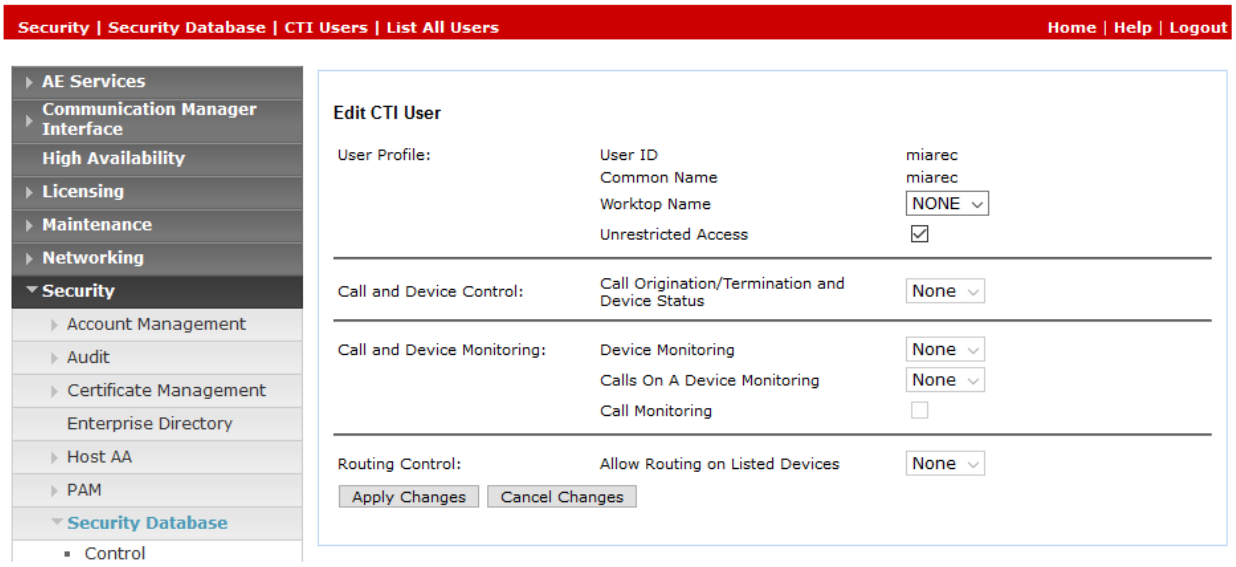
Click **Apply** (not shown) at the bottom of the pages to save the entry.



Navigate to **Security → Security Database → CTI Users → List All Users** and select the **MiaRec** user and click **Edit**.

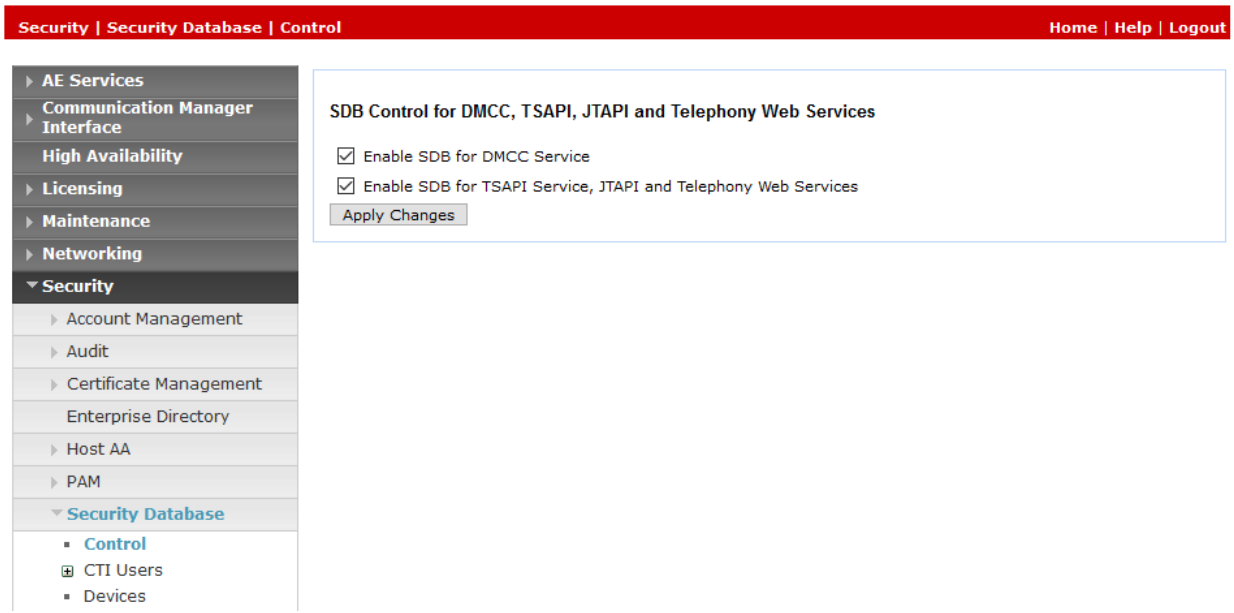


On the **Edit CTI User** panel, check the **Unrestricted Access** box and click the **Apply Changes** button. Click **Apply** when asked to confirm the change on the **Apply Changes to CTI User Properties** dialog (not shown).



6.4. Enable Security Database

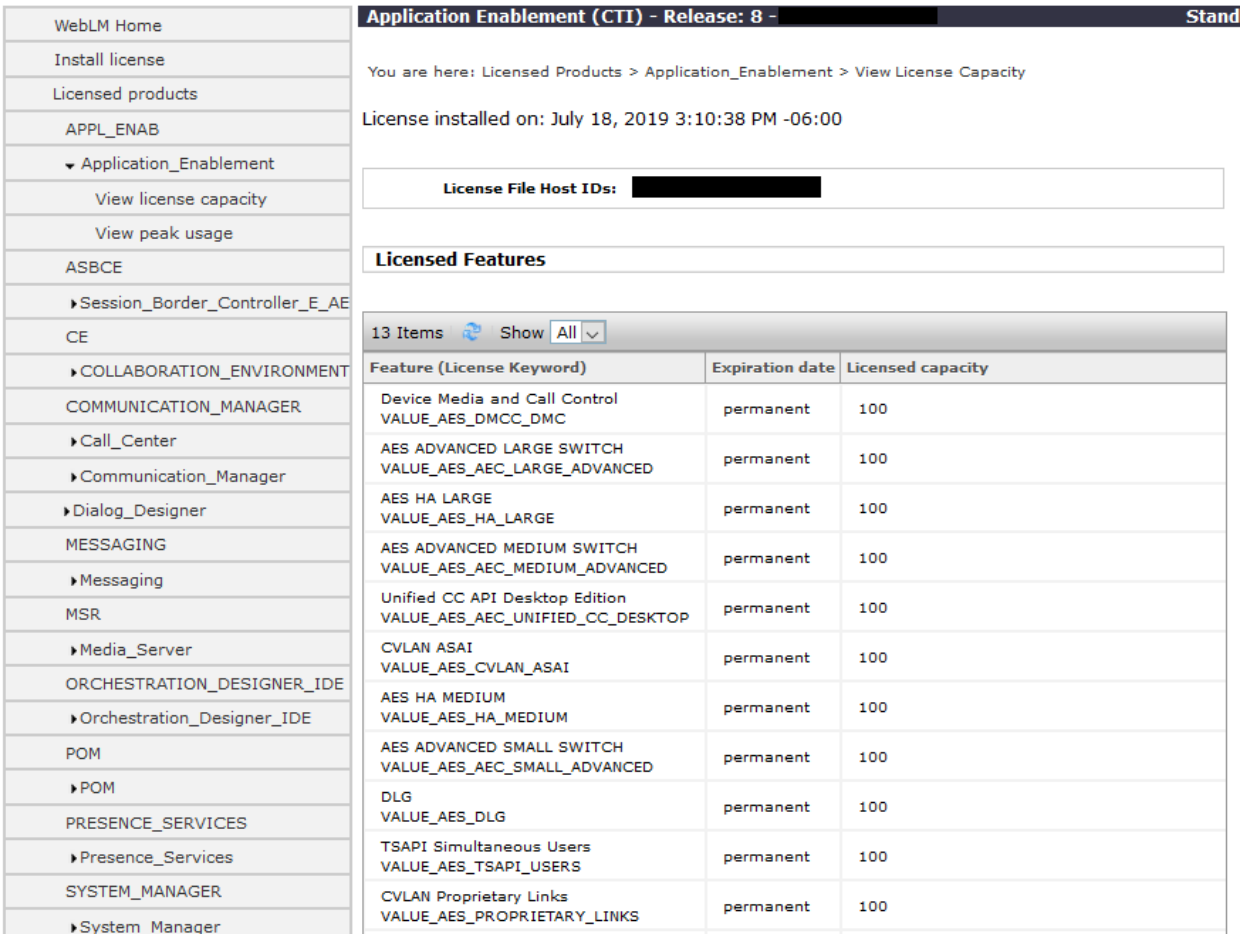
Enable the Security Database on AES by navigating to **Security → Security Database → Control.** Check box for both **Enabled SDB for DMCC Service** and **Enable SDP TSAPI Service, JTAPI and Telephone Service.**



6.5. Confirm TSAPI and DMCC Licenses

MiaRec uses a DMCC (**VALUE_AES_DMCC_DMC**) license for each recording port. Additionally, a TSAPI Basic (**VALUE_AES_TSAPI_USERS**) license is used for each agent station being monitored. If the licensed quantities are not sufficient for the implementation, contact the Avaya sales team or business partner for a proper license file.

From the left pane menu on Application Enablement Services Management Console, click **Licensing → WebLM Server Access** (not shown). A **Web License Manager** login window is displayed (not shown). Enter proper credentials to log in. Click **Licensed products → APPL_ENAB → Application_Enablement** from the left pane. The Application Enablement Services license is displayed in the right pane. Ensure that there are enough **Device Media and Call Control** and **TSAPI Simultaneous Users** licenses available.

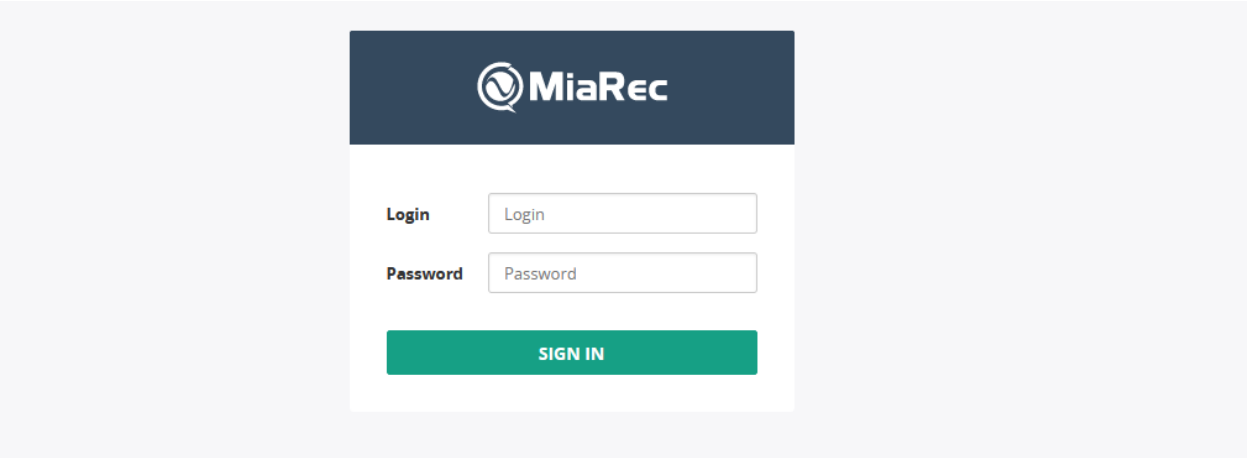


7. Configure MiaRec

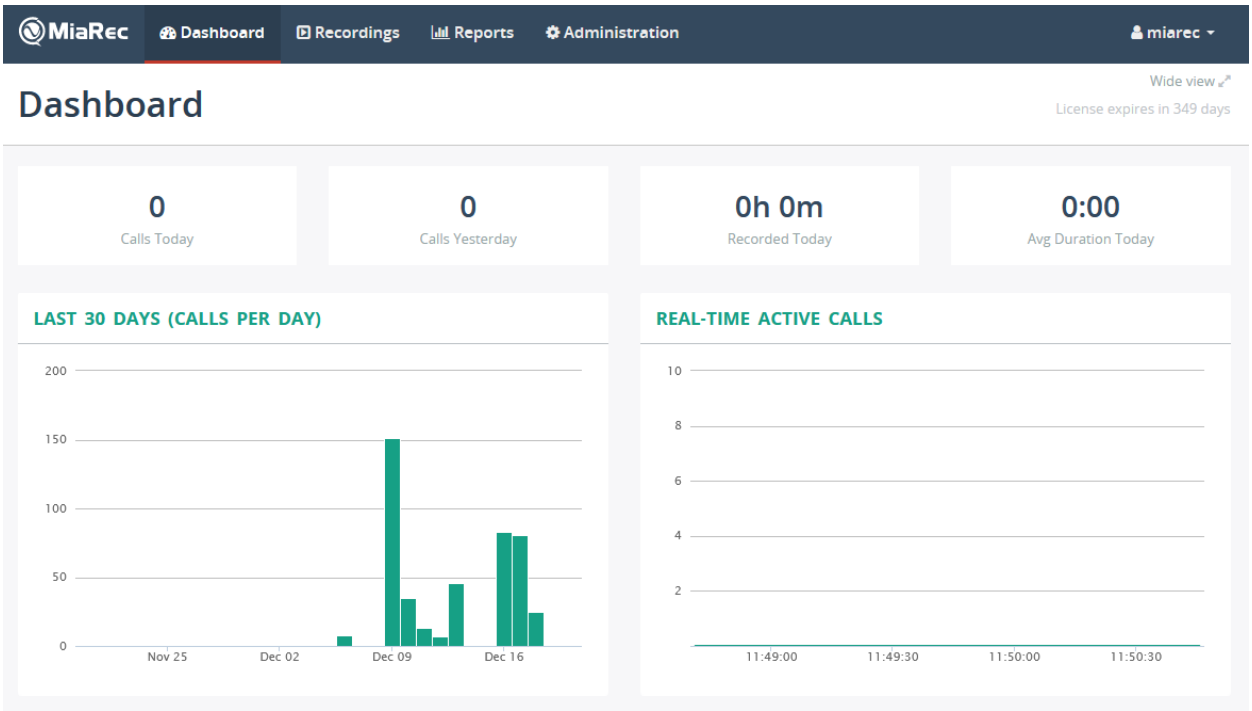
This section provides configuration steps for MiaRec. It is assumed that MiaRec and AES TSAPI client are already installed on the server. The steps include the:

- Administer DMCC Settings
- Administer TSAPI Settings

All the configuration for MiaRec is performed via MiaRec web interface. Via a web browser, open the MiaRec web interface and log on using appropriate credentials.

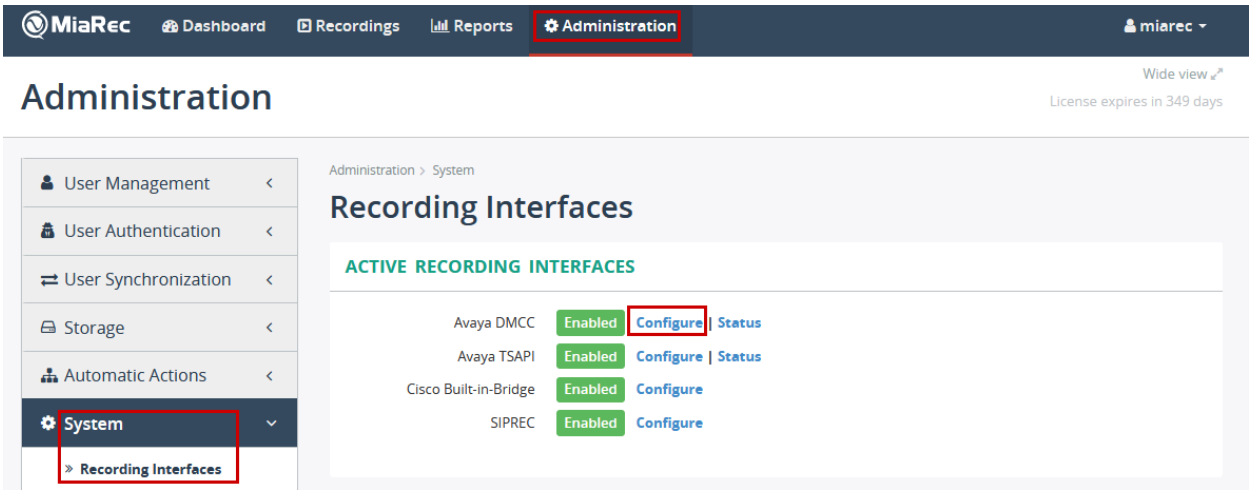


Once logged on, Menu options at top of the screen are used to navigate.



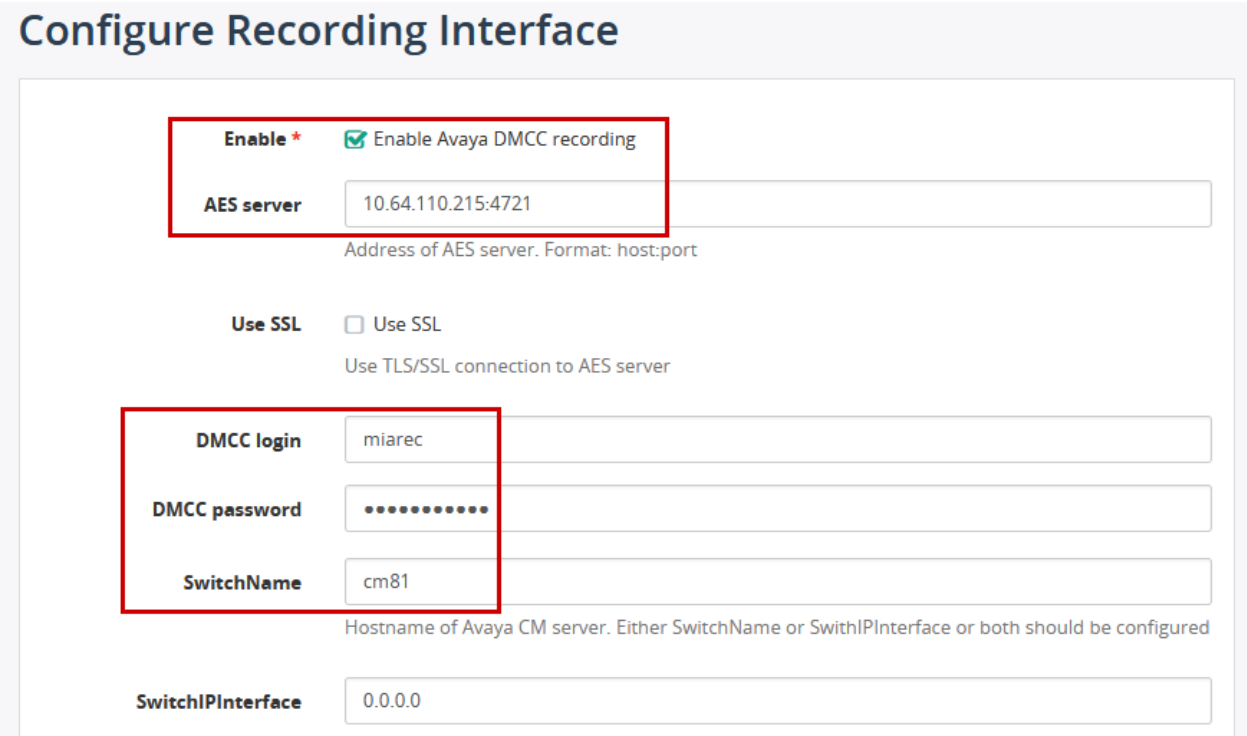
7.1. Administer DMCC Settings

To configure DMCC settings, navigate to **Administration → System → Recording Interfaces** and click **Configure** for **Avaya DMCC**.

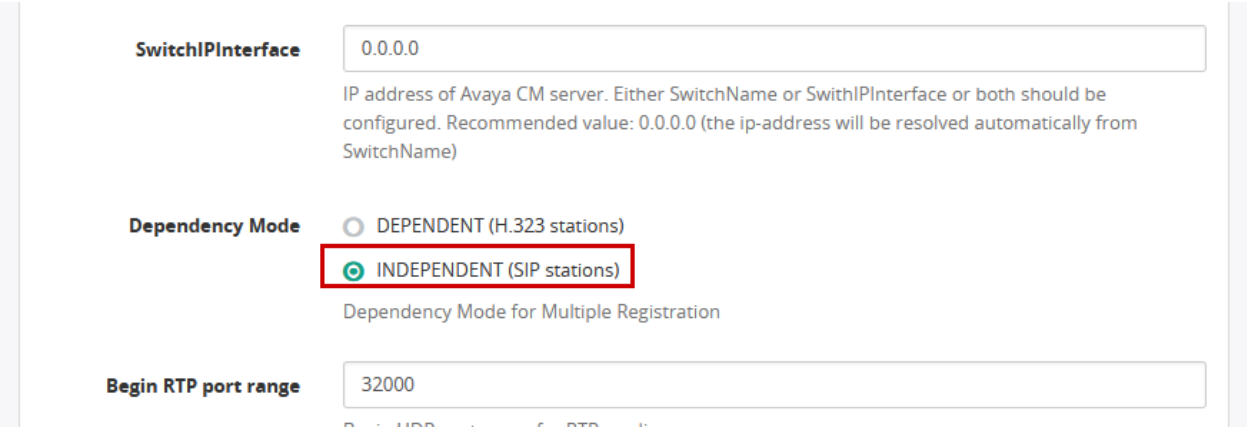


On the **Configure Recording Interface** page:

- Check box to **Enable Avaya DMCC recording**
- For **AES server**, type in the AES IP Address and Port in the format as shown below
- Type in the MiaRec credentials from **Section 6.3** for **DMCC login** and **password**
- In the **SwitchName** type in the hostname of Communication Manager

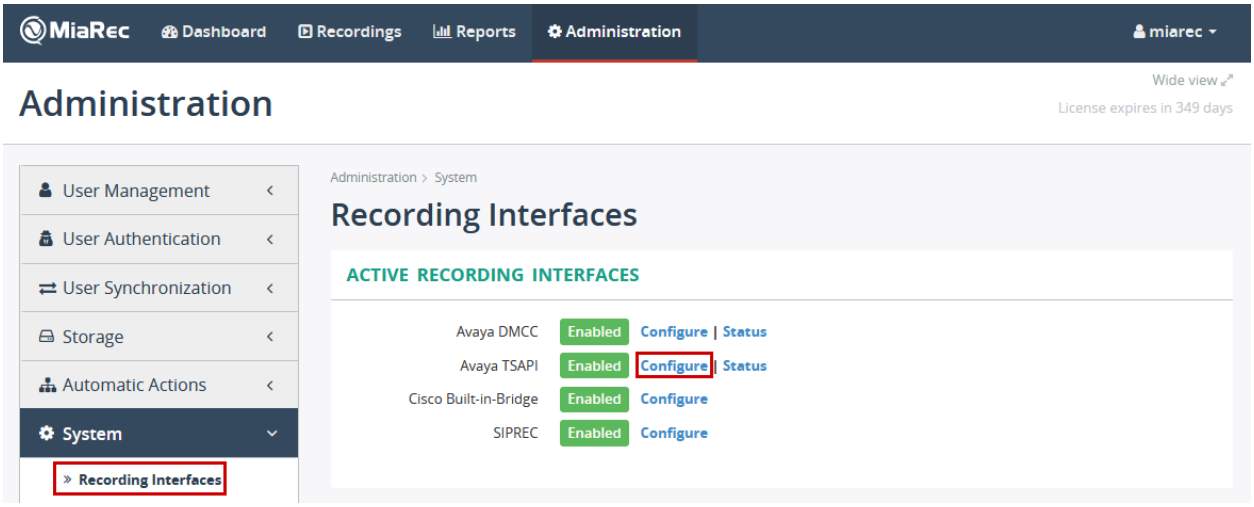


Scroll down and select the radio button for **INDEPENDENT (SIP stations).** This option enables MiaRec to register the configured DMCC stations in Independent mode for Avaya digital, H.323 and SIP stations. Retail default values for all other fields and save changes.



7.2. Administer TSAPI Settings

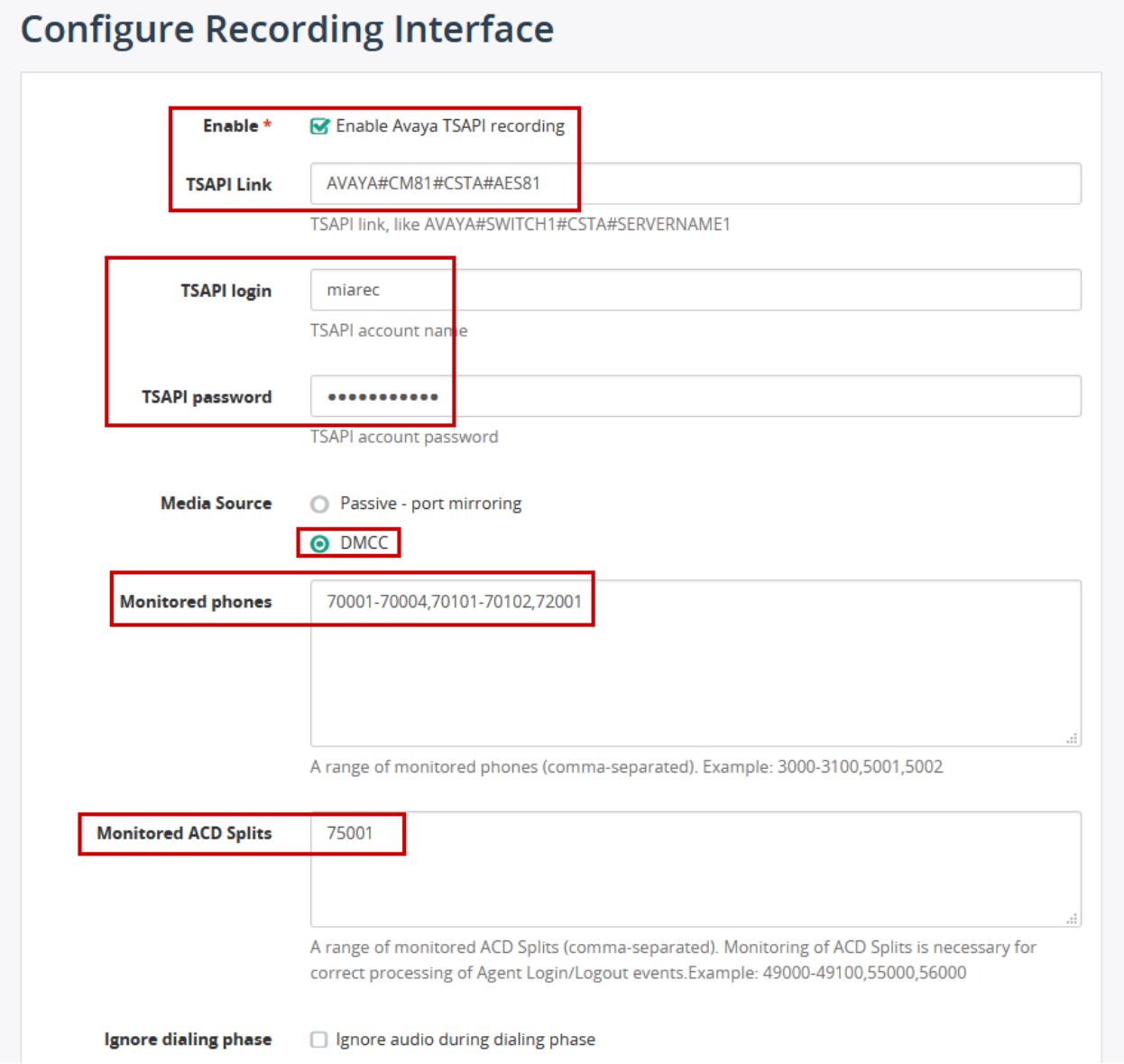
Continuing from above, from the left pane select **Recording Interfaces** and click **Configure** for **Avaya TSAPI.**



On the Configure Recording Interface (Avaya TSAPI) page:

- Check box for **Enable Avaya TSAPI recording**
- Type in **TSAPI Link** should point to the obtained TLink from **Section 6.2**.
- Type in the MiaRec credentials from **Section 6.3** for **TSAPI login** and **password**
- Select the radio button for **DMCC Media Source**
- In the **Monitored phones** field, type in the Avaya endpoints that will be monitored
- In the **Monitored ACD Splits** type in the hunt group extensions that will be monitored
- **Ignore dialing phase** could be enabled to avoid recording of initial dialing phase of the outgoing call scenario, but during the compliance test, this option was disabled

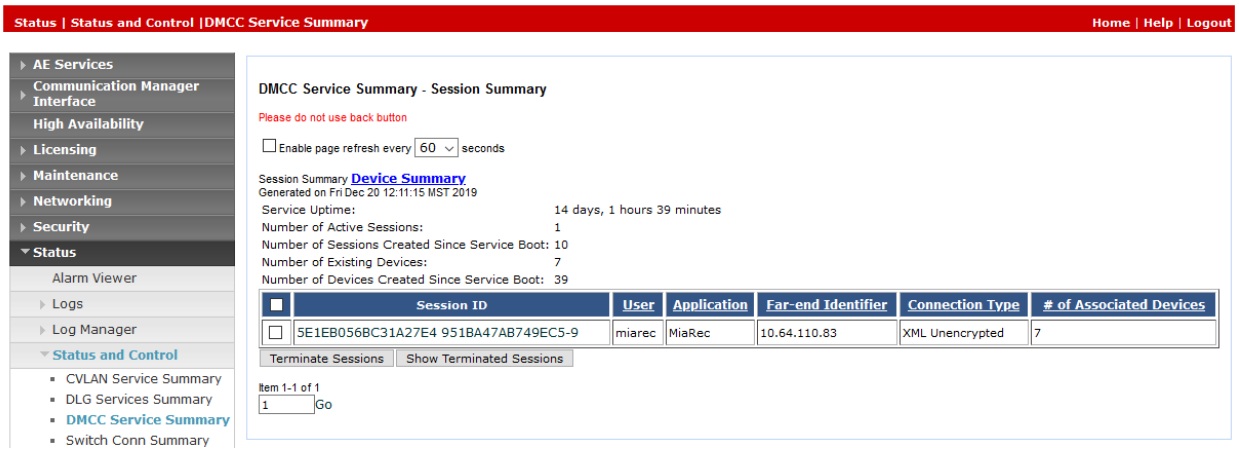
Retain default settings for other values and save changes.



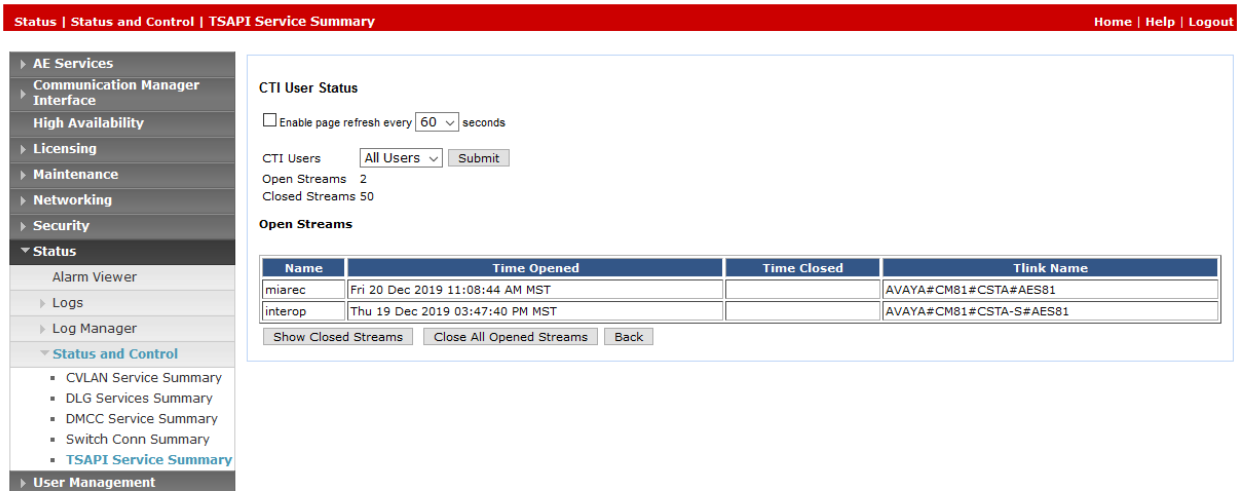
8. Verification Steps

8.1. Verify AES

From the AES OAM page, navigate to **Status → Status and Control → DMCC Service Summary.** Verify the user configured in **Section 7.1** is successfully connected to AES.



From the left pane, select **TSAPI Service Summary** followed by **User Status.** Verify the user configured in **Section 7.2** is successfully connected.



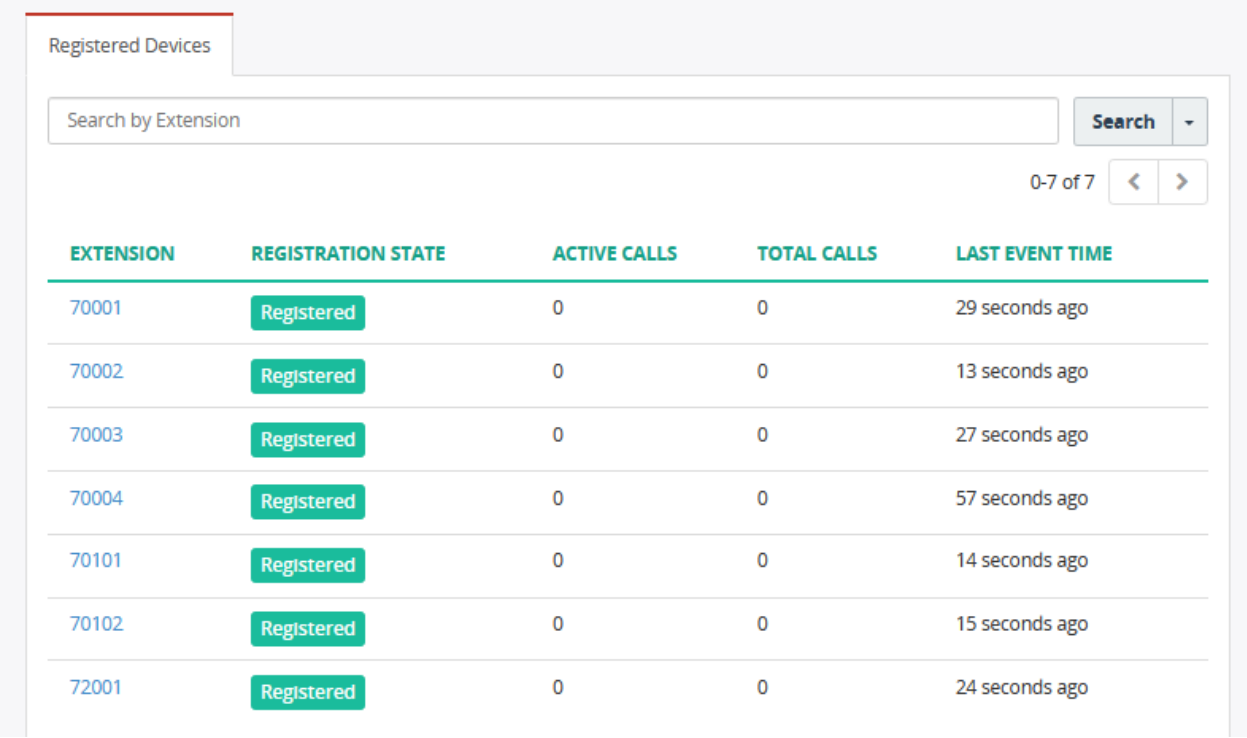
8.2. Verify Communication Manager

Via SAT, use the **list monitored-station** command to verify the MiaRec is successfully monitoring the configured station as configured in **Section 7.2.**

```
list monitored-station

                              MONITORED STATION

   Associations:     1       2       3       4       5       6       7       8
                 CTI     CTI     CTI     CTI     CTI     CTI     CTI     CTI
Station Ext      Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV
---------------- ------- ------- ------- ------- ------- ------- ------- -------
70001            1  0001
70002            1  0013
70003            1  0014
70004            1  0015
70101            1  0004
70102            1  0009
72001            1  0016
```

8.3. Verify MiaRec

To verify the DMCC connectivity to AES, via the MiaRec web interface, navigate to **Administration → System → Recording Interface → Avaya DMCC | Status** and select View **DMCC registered devices** (not shown). Verify the configured extensions are **Registered.**



EXTENSION	REGISTRATION STATE	ACTIVE CALLS	TOTAL CALLS	LAST EVENT TIME
70001	Registered	0	0	29 seconds ago
70002	Registered	0	0	13 seconds ago
70003	Registered	0	0	27 seconds ago
70004	Registered	0	0	57 seconds ago
70101	Registered	0	0	14 seconds ago
70102	Registered	0	0	15 seconds ago
72001	Registered	0	0	24 seconds ago

To verify the DMCC connectivity to AES, via the MiaRec web interface, navigate to **Administration → System → Recording Interface → Avaya TSAPI | Status** and select View **TSAPI monitored devices** (not shown). Verify the **MONITOR STATE** for configured extensions is **active.**

Monitored Devices

Search by Extension | Search

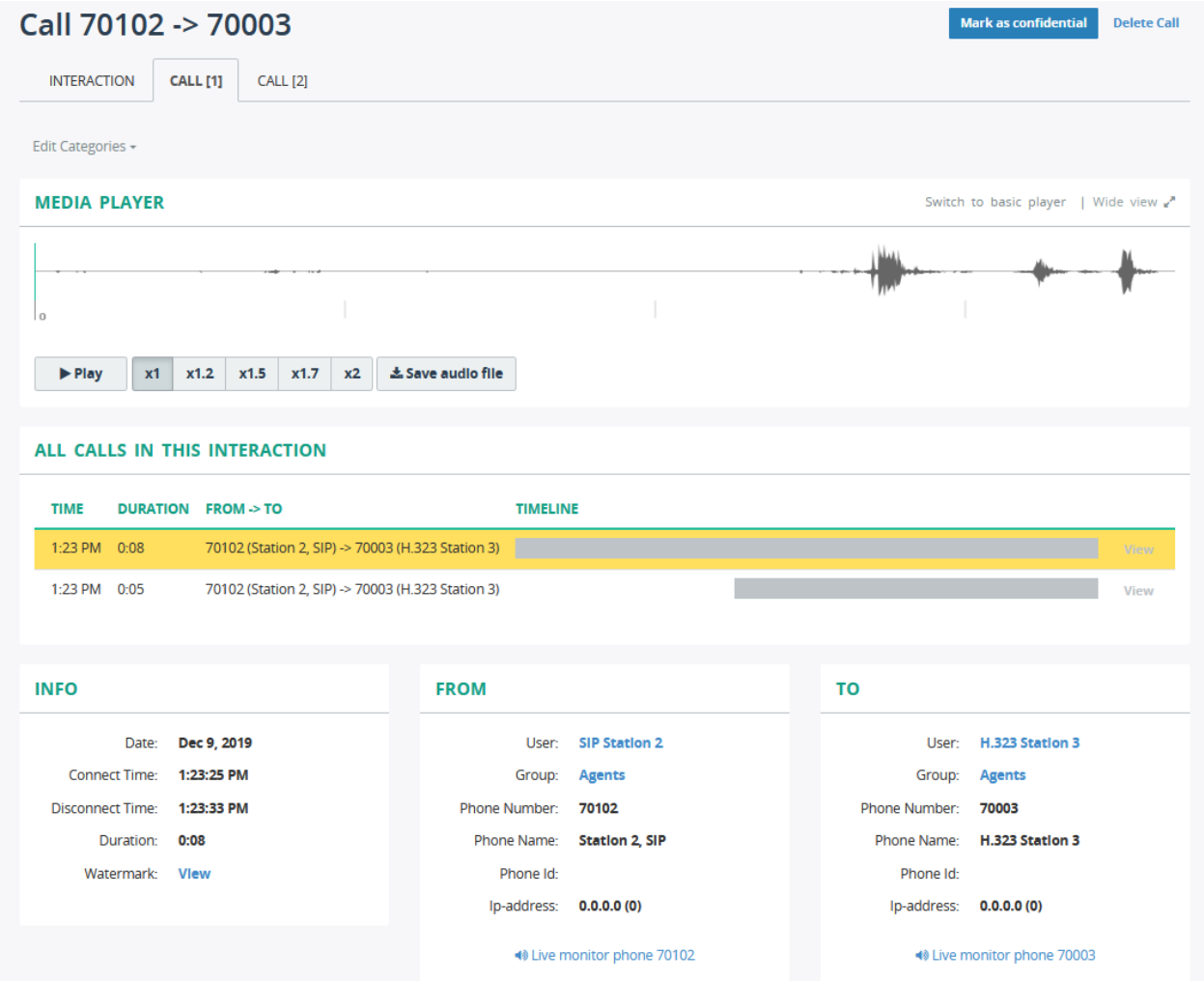
0-8 of 8

EXTENSION	DEVICE NAME	AGENT ID	AGENT NAME	MONITOR STATE	TSAPI IP	ACTIVE CALLS	TOTAL CALLS	LAST EVENT TIME
70001	Station, H323 1			active	10.64.10.200	0	0	1 hour 23 minutes ago
70002	H.323 Station 2			active		0	0	1 hour 22 minutes ago
70003	H.323 Station 3	71003	CC Agent3	active	10.64.10.202	0	0	1 hour 21 minutes ago
70004	H.323 Station 4			active		0	0	1 hour 22 minutes ago
70101	Station 1, SIP	71101	SIP Agent1	active		0	0	1 hour 23 minutes ago
70102	Station 2, SIP	71102	SIP Agent2	active	0.0.0.0	0	0	1 hour 23 minutes ago
72001	Digital Station 1	71201	Digital Agent1	active		0	0	1 hour 24 minutes ago
75001	CC Agents			active		0	0	1 hour 26 minutes ago

Place a few calls between recorded extensions. Verify the recordings are available on the MiaRec web interface.

	USER	DATE	TIME	DURATION	FROM	TO	CATEGORIES
2/2	SIP Station 1, Digital Station 1	Dec 9, 2019	1:24 PM	0:08	72001 (Digital Station 1)	70101 (Station 1, SIP)	
1/2	SIP Station 1, Digital Station 1	Dec 9, 2019	1:24 PM	0:11	72001 (Digital Station 1)	70101 (Station 1, SIP)	
1/6	Digital Station 1	Dec 9, 2019	1:24 PM	0:11	13035380121	72001 (Digital Station 1)	
2/2	H.323 Station 3, SIP Station 2	Dec 9, 2019	1:23 PM	0:05	70102 (Station 2, SIP)	70003 (H.323 Station 3)	
1/2	H.323 Station 3, SIP Station 2	Dec 9, 2019	1:23 PM	0:08	70102 (Station 2, SIP)	70003 (H.323 Station 3)	
2/2	H.323 Station 3, SIP Station 2	Dec 9, 2019	1:05 PM	0:04	70102 (Station 2, SIP)	70003 (H.323 Station 3)	

Select a call of interest to playback the audio recording.



9. Conclusion

These Application Notes describe the procedures for configuring MiaRec to monitor and record calls placed to and from agents and phones on Avaya Aura® Communication Manager. In the configuration described in these Application Notes, MiaRec uses the Device and Media Control Services and System Management Service and Telephone Services Application Programming Interface of Avaya Aura® Application Enablement Services to perform recording and monitoring. All feature and serviceability test cases were completed and passed with the observations noted in **Section 2.2**.

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.
2. *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 8.1.

Product documentation related to MiaRec can be obtained directly from MiaRec.

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.