Avaya Solution & Interoperability Test Lab

Application Notes for configuring Avaya Aura® Communication Manager R8.0 and Avaya Aura® Application Enablement Services R8.0 to interoperate with Netlogic Tec i-Listen Call Recording System 4.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps for Netlogic Tec i-Listen Call Recording system with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. i-Listen Call Recording system is a voice recording solution which can be used to record voice streams for Avaya telephony.

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

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

1. Introduction

The purpose of this document is to describe the compliance testing carried out using the Multiple Device Registration recording method on Netlogic Tec i-Listen Call Recording System with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. It includes a description of the configuration of both the Avaya and the i-Listen Call Recording System, a description of the tests that were performed and a summary of the results of those tests.

The i-Listen Call Recording System is used to record the voice stream of Avaya telephony endpoints. In this compliance test, it uses Avaya Aura® Communication Manager's Multiple Device Registration feature via the Avaya Aura® Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface to capture the audio and call details for call recording. The application uses the AES DMCC service to register the extensions that are to be recorded. When the extension receives a Telephony Services API (TSAPI) event pertaining to the start of a call, the application receives the extensions RTP media stream.

2. General Test Approach and Test Results

The test approach was to verify that the calls placed and recorded using the i-Listen Call Recording System with Avaya solution functioned correctly with good audio quality received. Functionality testing included basic telephony operations such as answer, mute/unmute, hold/retrieve, blind/attended transfer, blind/attended conference and calls to\from the PSTN. Features like call forwarding and service observing were also tested. Tests also include recordings for calls with G.711 and G.729 codec.

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 i-Listen Call Recording System did not include use of any specific encryption features as requested by Netlogic Tec.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios to ensure good quality audio recordings were received. Intra-switch calls were made on Communication Manager and inbound and outbound calls from/to the PSTN. The serviceability testing focused on verifying the ability of i-Listen to recover from disconnection and reconnection from the network and AES CTI link restart via Communication Manager.

2.2. Test Results

All functionality and serviceability test cases were completed successfully. The following observations were made:

- Initial tests revealed that calls were not recorded for the last leg of calls after transfer is completed or conference is dropped. However, these issues were fixed with an update on the software from Netlogic Tec.
- Restart of AES link from Communication Manager is not detected and hence the i-Listen Call Recording services are not restarted for the call recordings to work. Again, this was fixed with an update of the software from Netlogic Tec.

2.3. Support

Technical support can be obtained for i-Listen Call Recording solution from Netlogic Tec as follows:

- Email: support@infodyna.com
- Website: www.infodyna.com
- Phone: +202 37600212 or +202 33354159

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an Avaya Aura® Communication Manager with Avaya G430 Media Gateway and Avaya Aura® Media Server as the PBX and Avaya Aura® Application Enablement Services Server. Avaya 96x1 series IP telephones are connected to the PBX and used in the testing. The i-Listen Call Recording Server was used in the compliance test. The system is installed on a Windows 2012 R2 server.

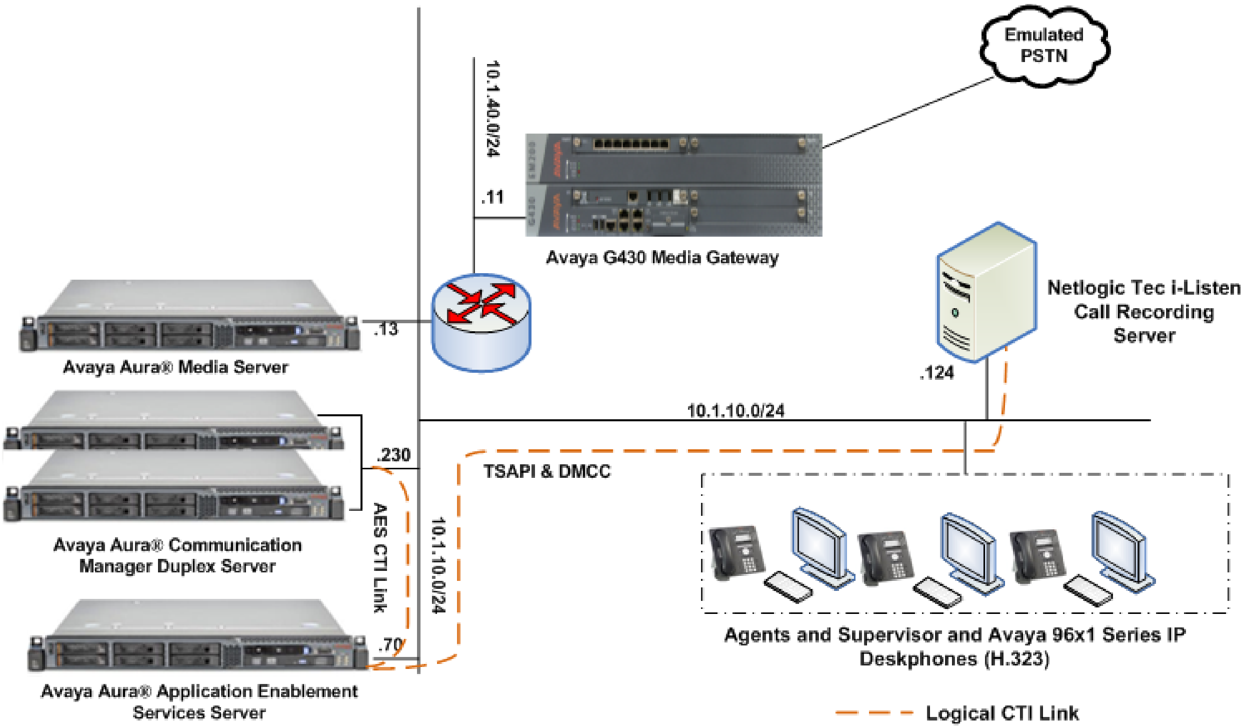

Emulated PSTN
10.1.40.0/24
.11
Avaya G430 Media Gateway
Netlogic Tec i-Listen Call Recording Server
.13
Avaya Aura® Media Server
.124
10.1.10.0/24
.230
TSAPI & DMCC
AES CTI Link
10.1.10.0/24
Avaya Aura® Communication Manager Duplex Server
.70
Agents and Supervisor and Avaya 96x1 Series IP Deskphones (H.323)
Avaya Aura® Application Enablement Services Server
Logical CTI Link

Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services Server and Netlogic Tec i-Listen Call Recording Server Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration as shown in **Figure 1.**

Equipment	**Software**
Avaya Aura® Communication Manager	R018x.00.0.822.0 - 24826
Avaya G430 Media Gateway - MGP	40.10.0
Avaya Aura® Application Enablement Services	8.0.0.0.0.6-0
Avaya Aura® Media Server	8.0.0.150
Avaya 96x1 Series H.323 IP Deskphones	6.6604
Netlogic Tec i-Listen Call Recording Server	4.0

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options
- Configure Target Stations to be Recorded
- Configure the Interface to AES

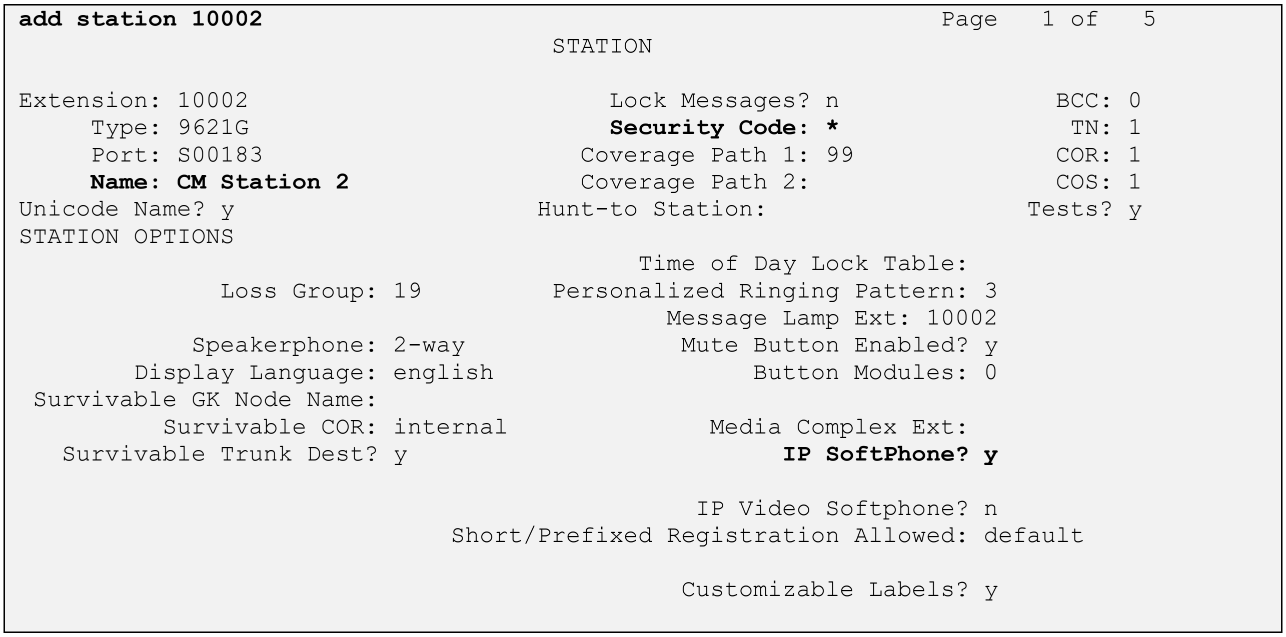
5.1. Verify System Parameters Customer Options

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 4**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

```
display system-parameters customer-options                      Page   4 of  12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? y               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y



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

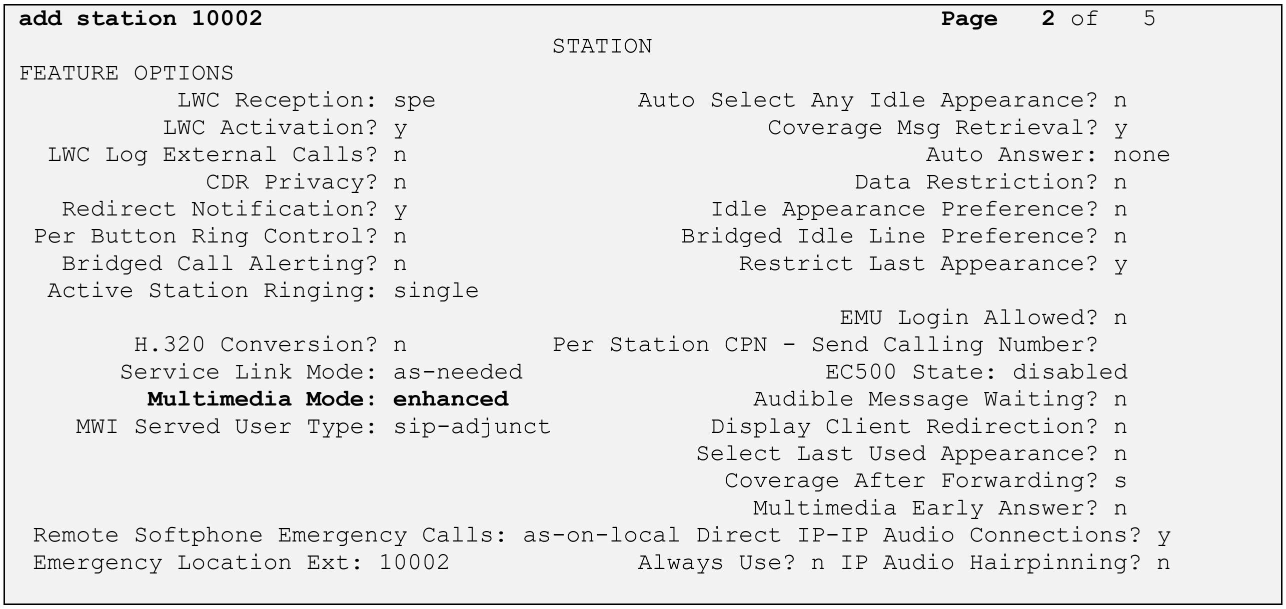
5.2. Configure Target Stations to be Recorded

Use the **add station** command to configure a station for each of the target stations to be recorded. Enter in a descriptive **Name** and **Security Code** for each one. The **Security Code** will be referenced by i-Listen when setting up the recording extensions. Set the **IP Softphone?** to **y**.



```
add station 10002                                            Page   1 of   5
                                     STATION

Extension: 10002                         Lock Messages? n               BCC: 0
     Type: 9621G                         Security Code: *                TN: 1
     Port: S00183                      Coverage Path 1: 99              COR: 1
     Name: CM Station 2                Coverage Path 2:                 COS: 1
Unicode Name? y                     Hunt-to Station:                  Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 3
                                             Message Lamp Ext: 10002
            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
```

On **Page 2**, ensure that the **Multimedia Mode** is set to **enhanced**. Repeat for all other stations to be recorded.



```
add station 10002                                            Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe             Auto Select Any Idle Appearance? n
          LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                   Auto Answer: none
            CDR Privacy? n                               Data Restriction? n
   Redirect Notification? y                    Idle Appearance Preference? n
 Per Button Ring Control? n                  Bridged Idle Line Preference? n
   Bridged Call Alerting? n                      Restrict Last Appearance? y
  Active Station Ringing: single
                                                        EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                    EC500 State: disabled
         Multimedia Mode: enhanced                Audible Message Waiting? n
    MWI Served User Type: sip-adjunct           Display Client Redirection? n
                                               Select Last Used Appearance? n
                                                 Coverage After Forwarding? s
                                                   Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
 Emergency Location Ext: 10002             Always Use? n IP Audio Hairpinning? n
```

5.3. Configure Interface to Avaya Aura® Application Enablement Services

Enter **list node-names all** and note the **procr IP Address**.

```
list node-names all                                                    Page   2

                        NODE NAMES

Type     Name                  IP Address
IP       aams1                 10.1.10.13
IP       aams2                 10.1.10.12
IP       cms1                  10.1.10.85
IP       default               0.0.0.0
IP       iptm                  10.1.10.125
IP       lsp-g430              10.1.40.18
IP       mypc                  10.3.10.8
IP       n                     10.3.10.253
IP       procr                 10.1.10.230
IP       procr6                ::
IP       s8500-clan1           10.1.10.21
IP       s8500-clan2           10.1.10.22
IP       s8500-medpro1         10.1.10.31
IP       s8500-medpro2         10.1.10.32
IP       s8500-val1            10.1.10.36
IP       site6                 10.1.60.18
```

In order for Communication Manager to establish a connection to Application Enablement Services, administer the CTI Link as shown below. Specify an available **Extension** number, set the **Type** as **ADJ-IP**, which denotes that this is a link to an IP connected adjunct, and name the link for easy identification, in this instance, the node-name is used.

```
add cti-link 3                                                  Page   1 of   3
                                    CTI LINK
 CTI Link: 3
Extension: 10093
     Type: ADJ-IP
                                                                        COR: 1
     Name: TSAPI Service – AES8x
Unicode Name? n
```

Configure IP-Services for the **AESVCS** service using **change ip-services** command. Using the proc node name as noted above and the default port and make sure it is **Enabled** to **y**.

```
change ip-services                                            Page   1 of   4

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

Navigate to **Page 4**, set the **AE Services Server** hostname **from Section 6.1** and the **Password** for the AES Server will use to authenticate with Communication Manager.

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

   Server ID    AE Services       Password         Enabled    Status
                   Server
      1:
      2:      aes               ***************      y        in use
      3:
```

6. Configuration of Avaya Aura® Application Enablement Services

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

- Obtain AES hostname
- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Verify TSAPI and DMCC Services
- Create CTI User
- Enable CTI User
- Configure DMCC and TSAPI Ports
- Disable Security Database
- Restart TSAPI and DMCC Services

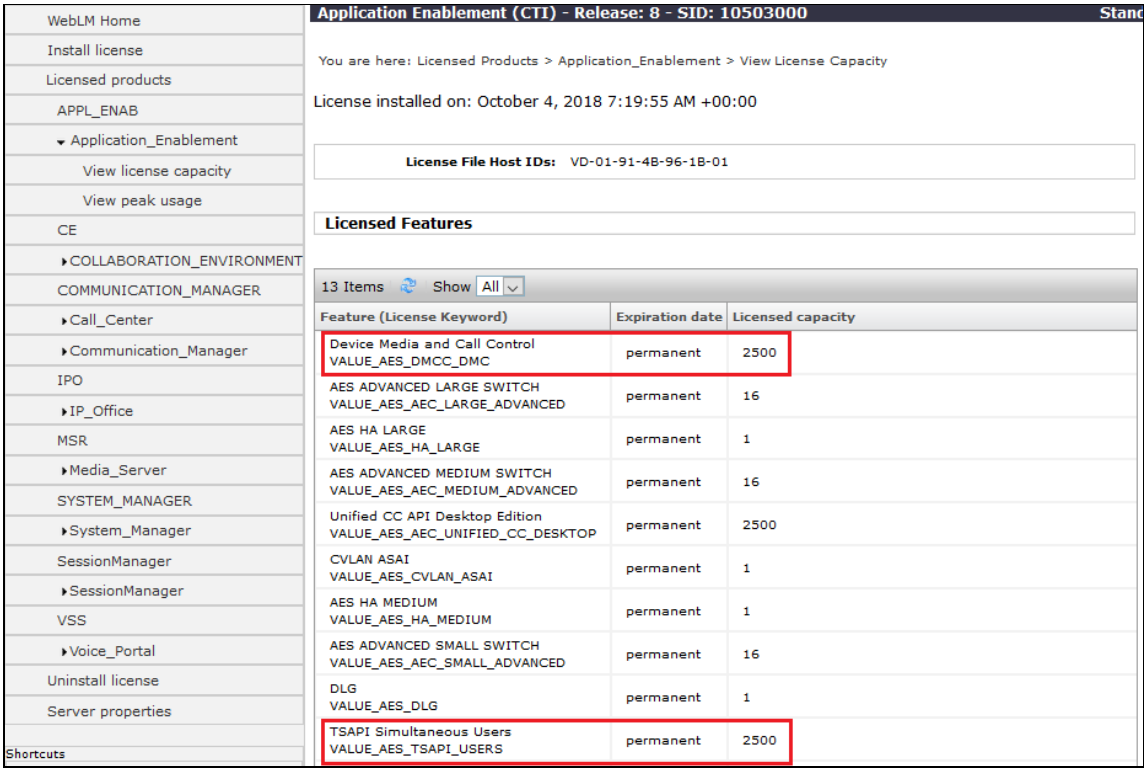
6.1. Obtain AES hostname

Login into the AES server and type **hostname** on the command prompt.

```
login as: cust

Using keyboard-interactive authentication.
Password:
Last login: Thu Jan 31 18:14:22 +08 2019 from 10.1.10.156 on pts/0
[cust@aes ~]$ hostname
aes
[cust@aes ~]$
```

6.2. Verify Licensing

Access the Web License Manager of the Application Enablement Services Server. The **Web License Manager** screen below is displayed. Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane. Verify that there are sufficient licenses for **Device Media and Call Control** and **TSAPI Simultaneous Users**, as shown below. If not, consult with your Avaya Account Manager or Business Partner to acquire the proper license for your solution.



Application Enablement (CTI) - Release: 8 - SID: 10503000

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: October 4, 2018 7:19:55 AM +00:00

License File Host IDs: VD-01-91-4B-96-1B-01

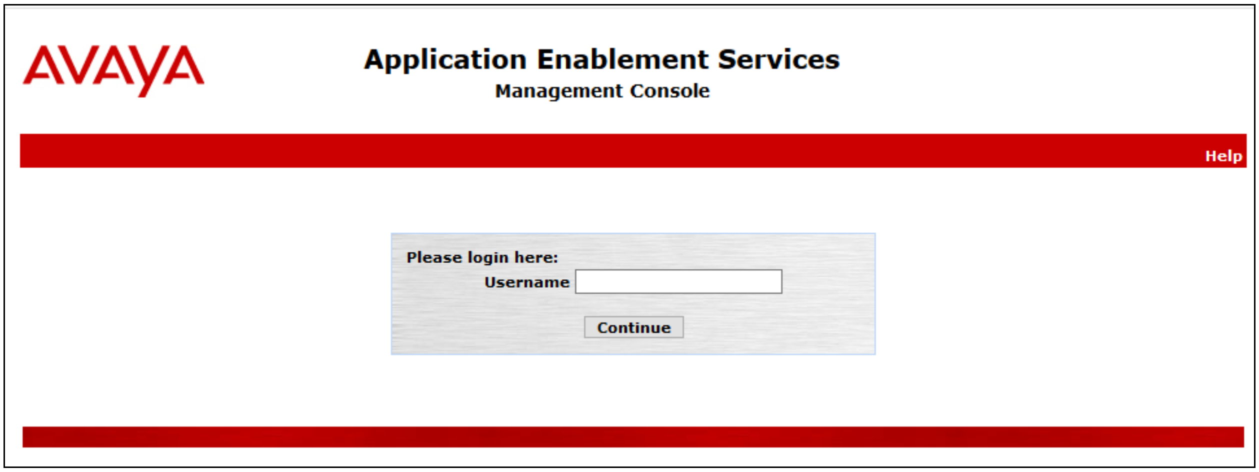
Licensed Features

13 Items Show All

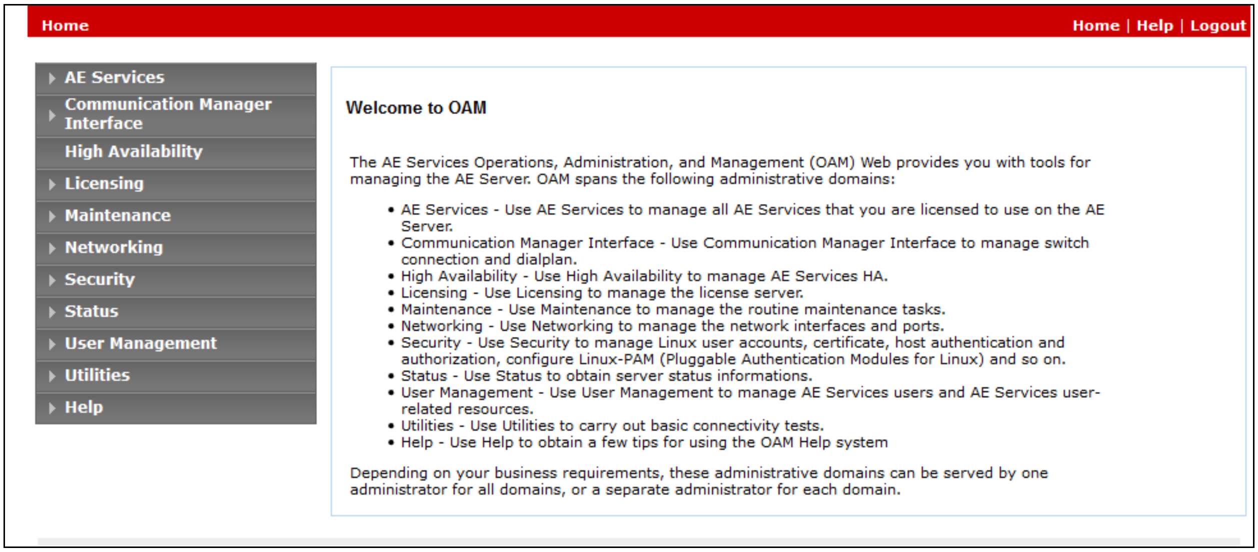
Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	2500
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	1
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	2500
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	1
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	1
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	2500

6.3. Create Switch Connection

Access the OAM web-based interface of the Application Enablement Services server, using the URL https://<Server_IP>. The Management console is displayed, log in using the appropriate credentials.



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



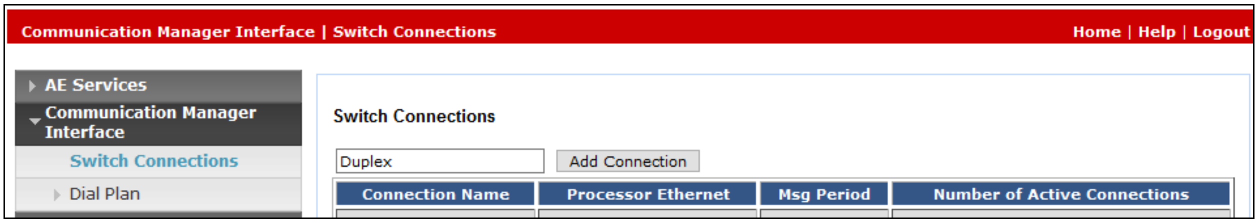
Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

To establish the connection between Communication Manager and the Application Enablement Services server, click **Communication Manager Interface → Switch Connections**. In the field next to **Add Connection**, enter appropriate name and click on **Add Connection**.

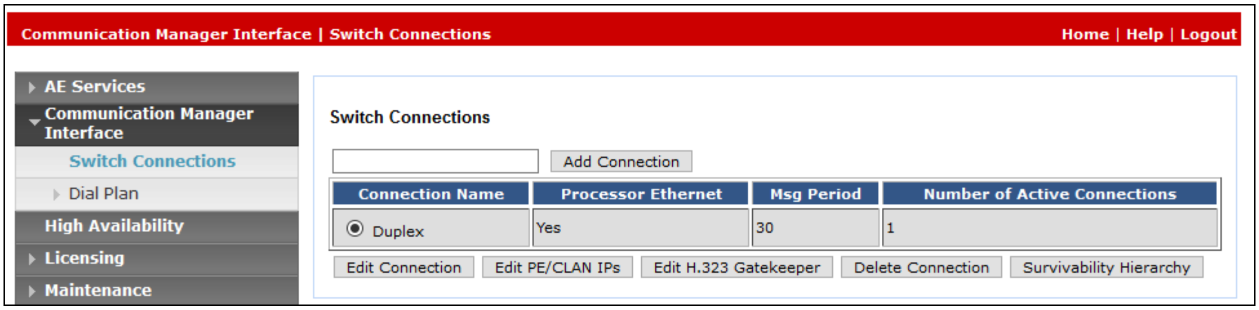

Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Add Connection

Switch Connections

Duplex

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

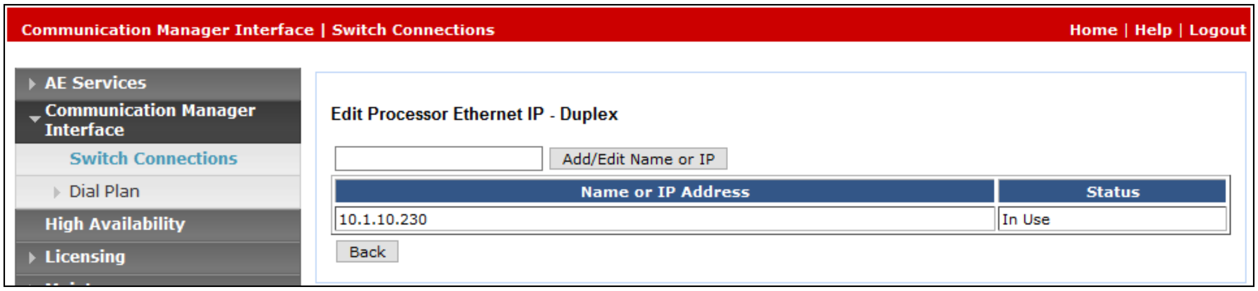
Complete the configuration as shown and enter the password specified in **Section 5.3** when configuring AESVCS in ip-services. Click on **Apply** (not shown), the screen below will be displayed.



Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● Duplex	Yes	30	1

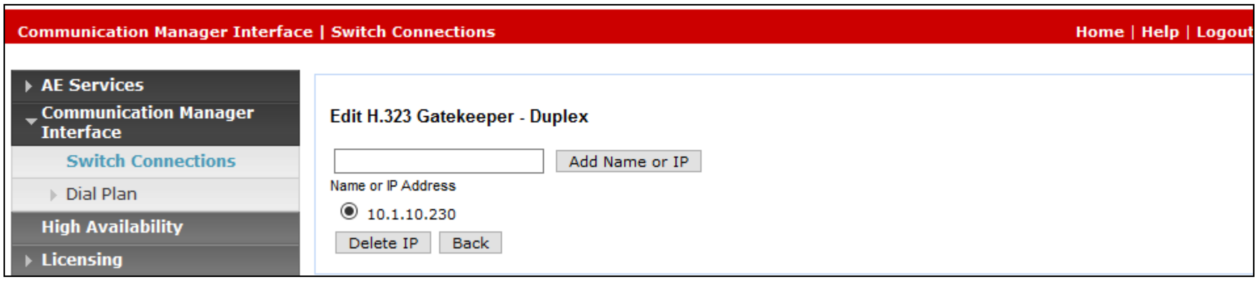
Click on **Edit PE/CLAN IPs** (at the bottom of the last screenshot) to specify the proc IP address of the Communication Manager, as noted in **Section 5.3**. Next to **Add/Edit Name or IP**, enter the proc IP address of the Communication Manager and click on **Add/Edit Name or IP**.



Edit Processor Ethernet IP - Duplex

Name or IP Address	Status
10.1.10.230	In Use

Click on **Back** and then click on **Edit H.323 Gatekeeper**. Enter the proc IP address of the Communication Manager and click on **Add Name or IP**.



Edit H.323 Gatekeeper - Duplex

Add Name or IP

Name or IP Address

● 10.1.10.230

Delete IP | Back

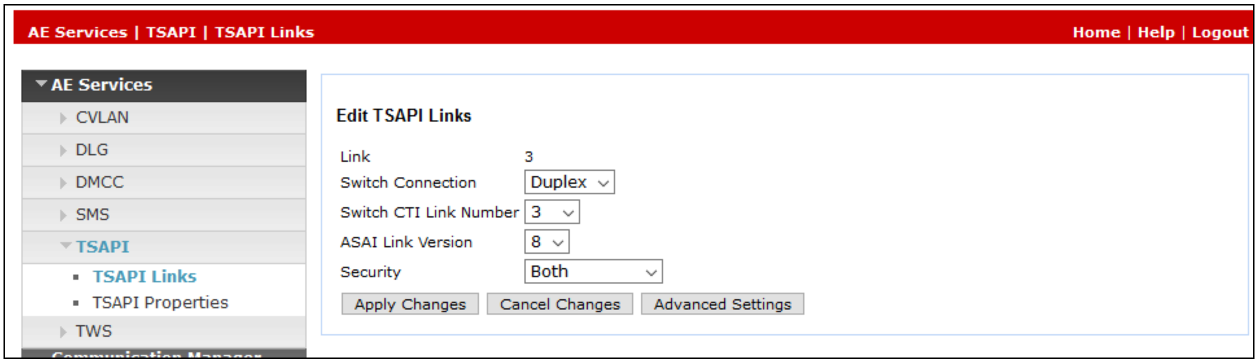
6.4. Administer TSAPI Link

To administer a TSAPI link, select **AE Services → TSAPI → TSAPI Links** from the left pane. Click **Add Link** on the right pane (not shown).

In the **Add TSAPI Links** screen, select the following values:

- **Link:** Select an available Link number from 1 to 16.
- **Switch Connection:** Administered switch connection in **Section 6.3**.
- **Switch CTI Link Number:** Corresponding CTI link number in **Section 5.3**.
- **ASAI Link Version:** Set to the appropriate version.
- **Security:** Select **Both** to allow for encrypted or unencrypted link.

Click **Apply Changes** to affect changes.

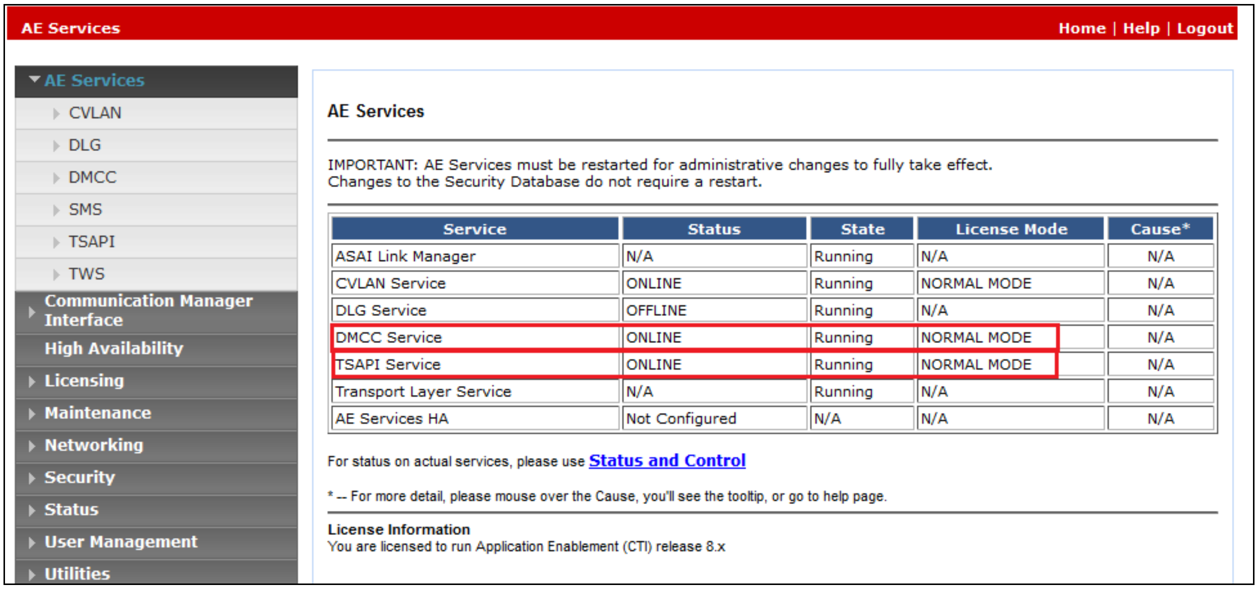


Edit TSAPI Links

Link	3
Switch Connection	Duplex
Switch CTI Link Number	3
ASAI Link Version	8
Security	Both

6.5. Verify TSAPI and DMCC Services

Select **AE Services** from the left-hand menu and select **DMCC** to verify that the **DMCC** and **TSAPI Service** are licensed by ensuring that **DMCC** and **TSAPI Service** are in the list of services and that the **License Mode** is showing **NORMAL MODE**. If not, consult with your Avaya Account Manager or Business Partner to acquire the proper license for your solution.



AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	ONLINE	Running	NORMAL MODE	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

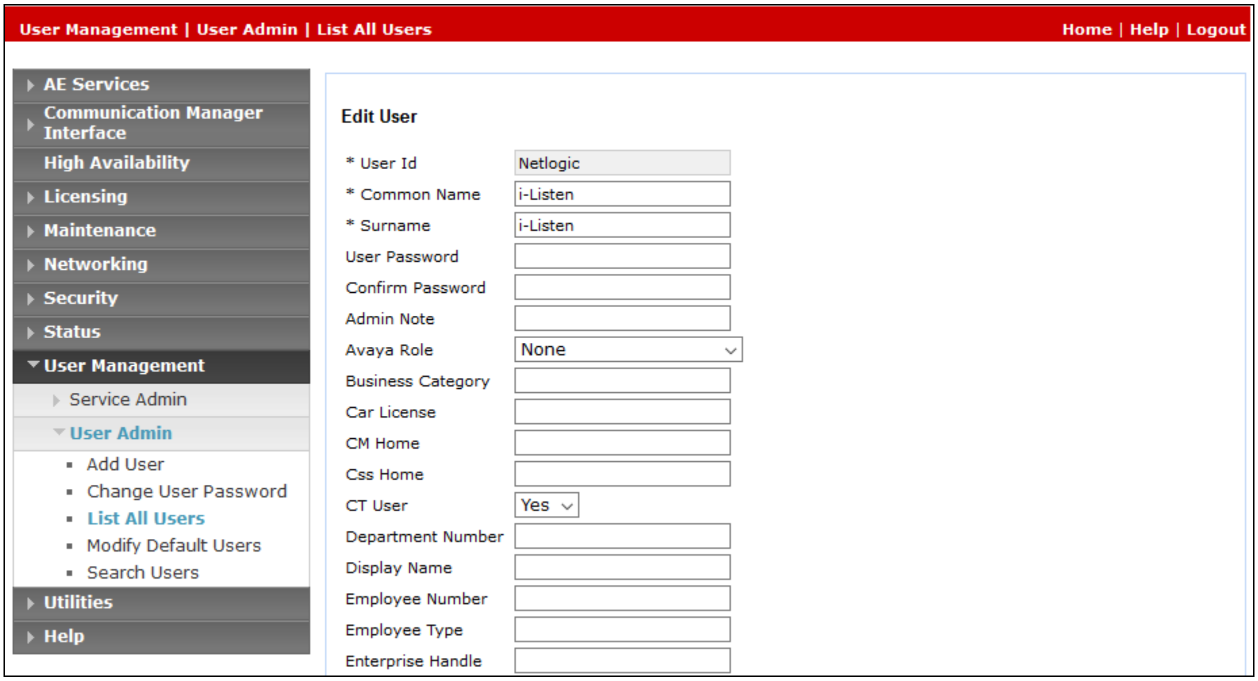
For status on actual services, please use Status and Control

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
You are licensed to run Application Enablement (CTI) release 8.x

6.6. Create CTI User

A user ID and password needs to be configured for the i-Listen Call Recording Server to communicate as a DMCC Client with the Application Enablement Services. Select **User Management → User Admin → Add User** from the left-hand menu, to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown). Below is the screenshot for the values entered.

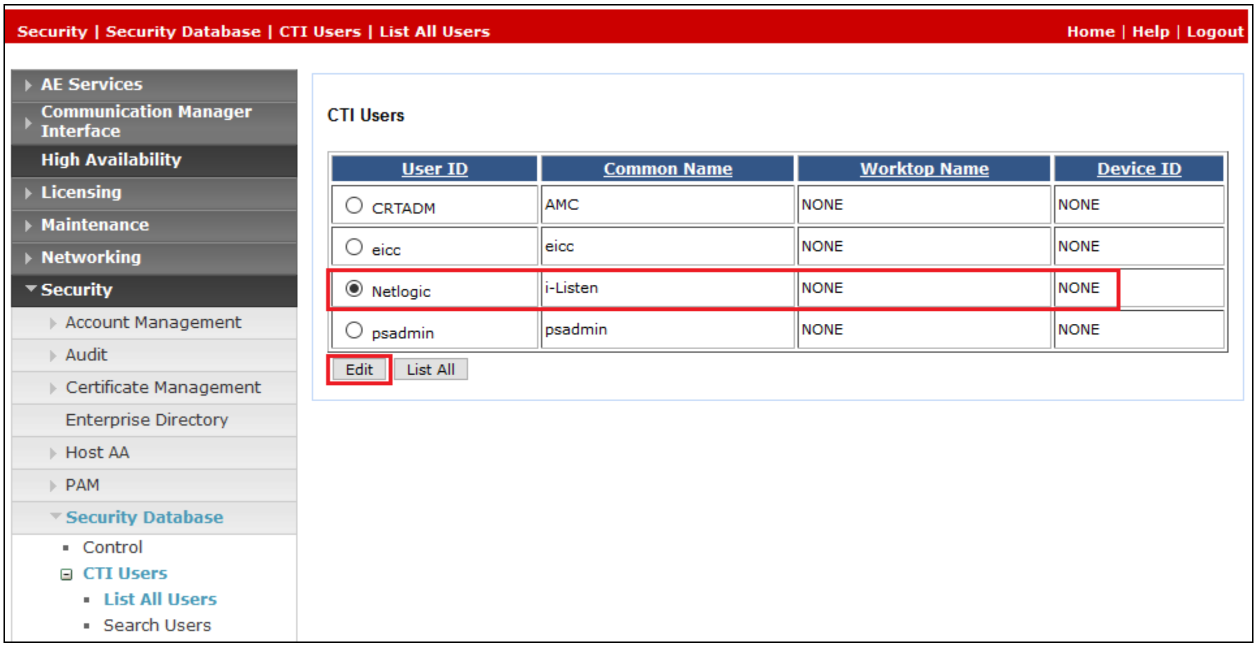


Edit User

* User Id	Netlogic
* Common Name	i-Listen
* Surname	i-Listen
User Password	
Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	

6.7. Enable CTI User

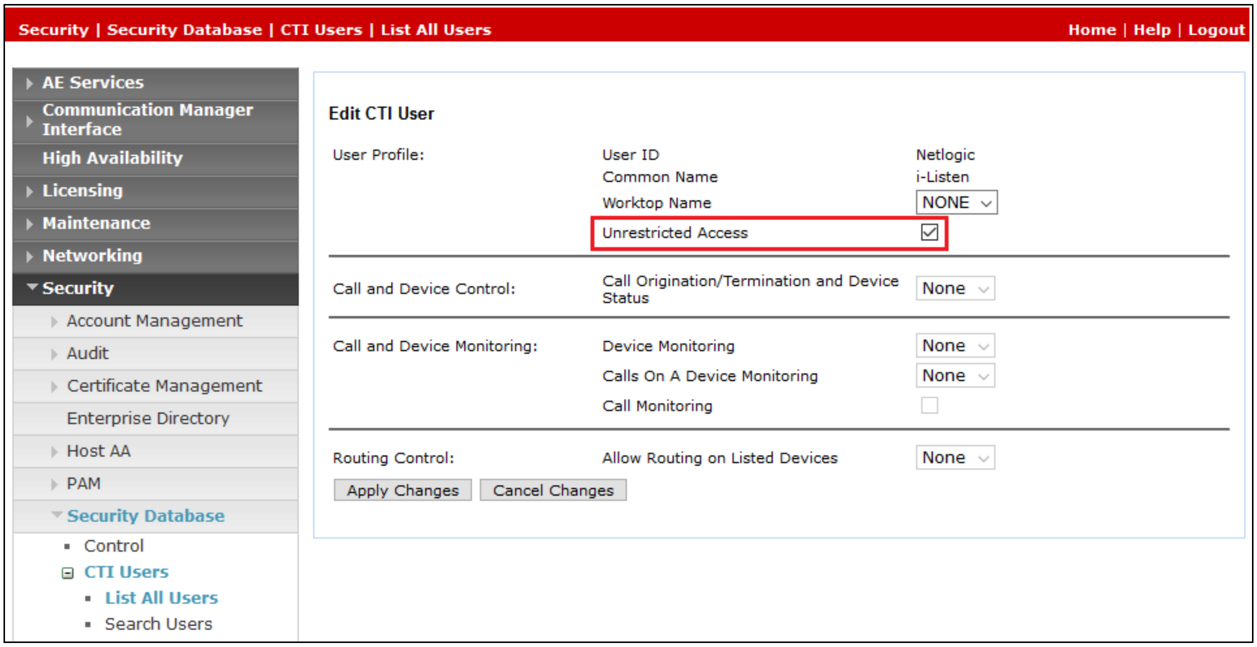
Navigate to the users' screen by selecting **Security → Security Database → CTI Users → List All Users.** In the **CTI Users** window, select the user that was set up in **Section 6.6** and select the **Edit** option.



CTI Users

User ID	Common Name	Worktop Name	Device ID
○ CRTADM	AMC	NONE	NONE
○ eicc	eicc	NONE	NONE
● Netlogic	i-Listen	NONE	NONE
○ psadmin	psadmin	NONE	NONE

The **Edit CTI User** screen appears. Tick the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

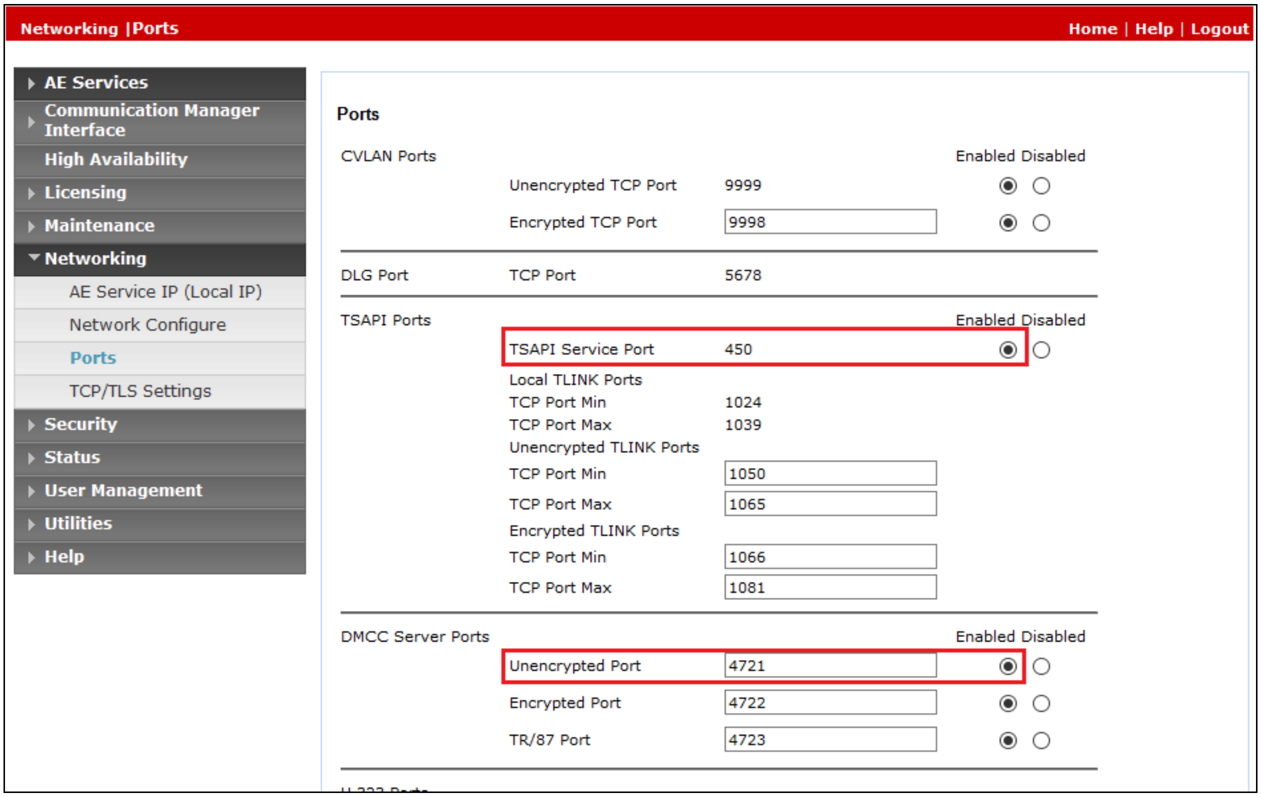


Edit CTI User

User Profile:	User ID	Netlogic
	Common Name	i-Listen
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

6.8. Configure DMCC and TSAPI Ports

On the AES Management Console navigate to **Networking → Ports** to set the TSAPI and DMCC server Ports. During the compliance test, the **Unencrypted Port** set to **4721** was **Enabled** for **DMCC Server Ports** and **TSAPI Service Port 450** was also **Enabled** as shown in the screen below. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

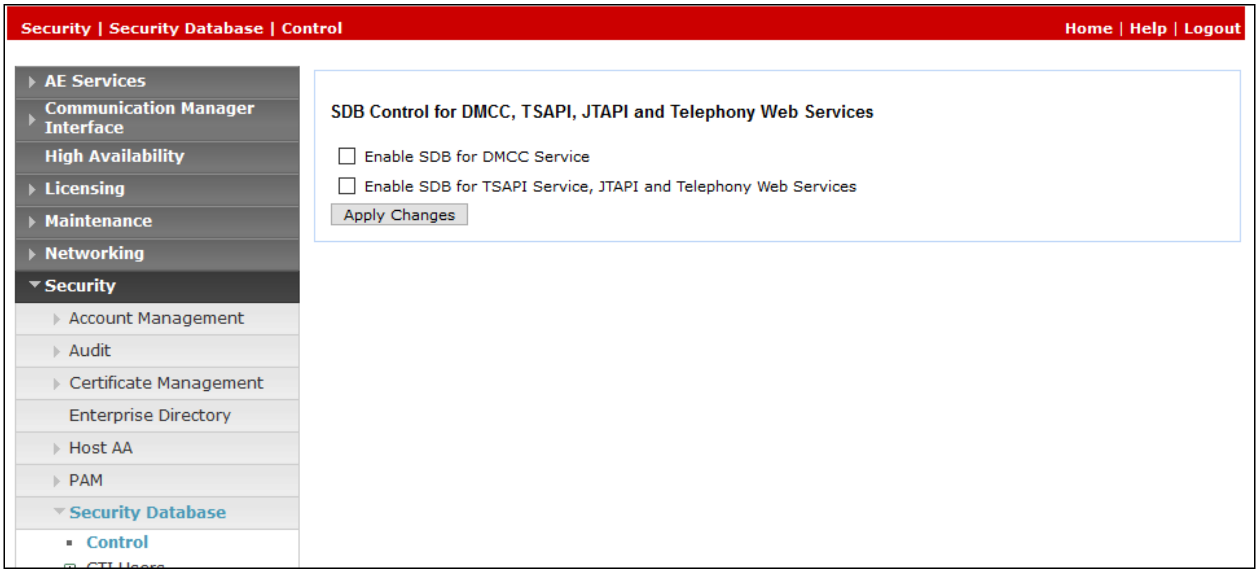


Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports				
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

6.9. Disable Security Database

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



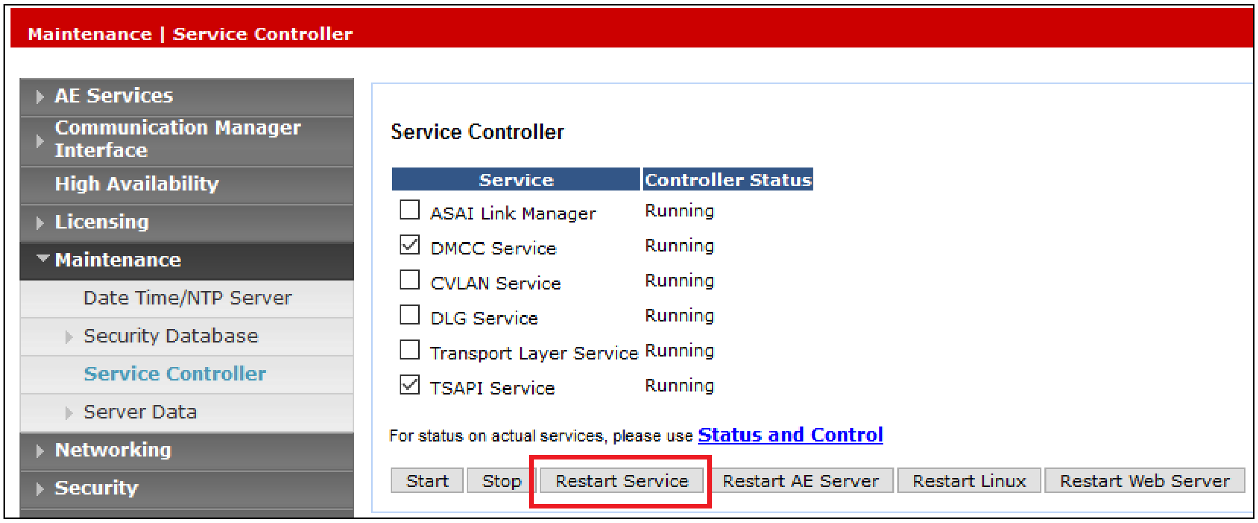
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

□ Enable SDB for DMCC Service

□ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

6.10. Restart TSAPI and DMCC Services

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



Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
☑ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

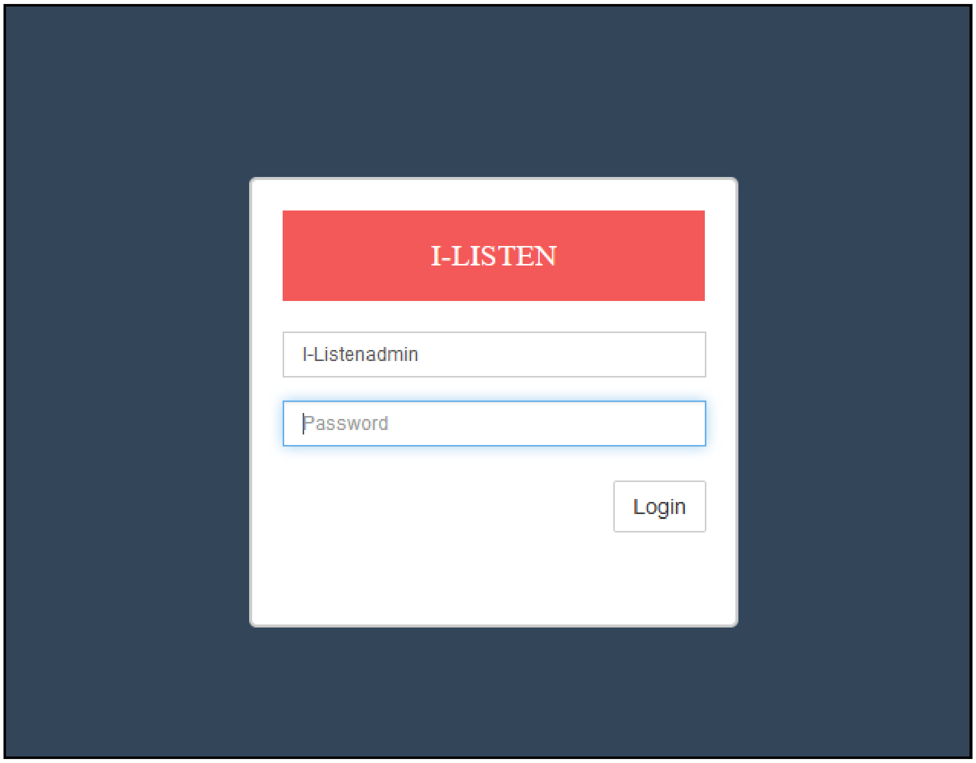
7. Configuration of Netlogic Tec i-Listen Call Recording Server

The i-Listen Call Recording Server is provided pre-installed by Netlogic engineer. Setup administration is outside of the scope of this document, but the following are demonstrated for the call recording administration.

- Login to i-Listen Call Recording server
- Register extensions to i-Listen Call Recording Service

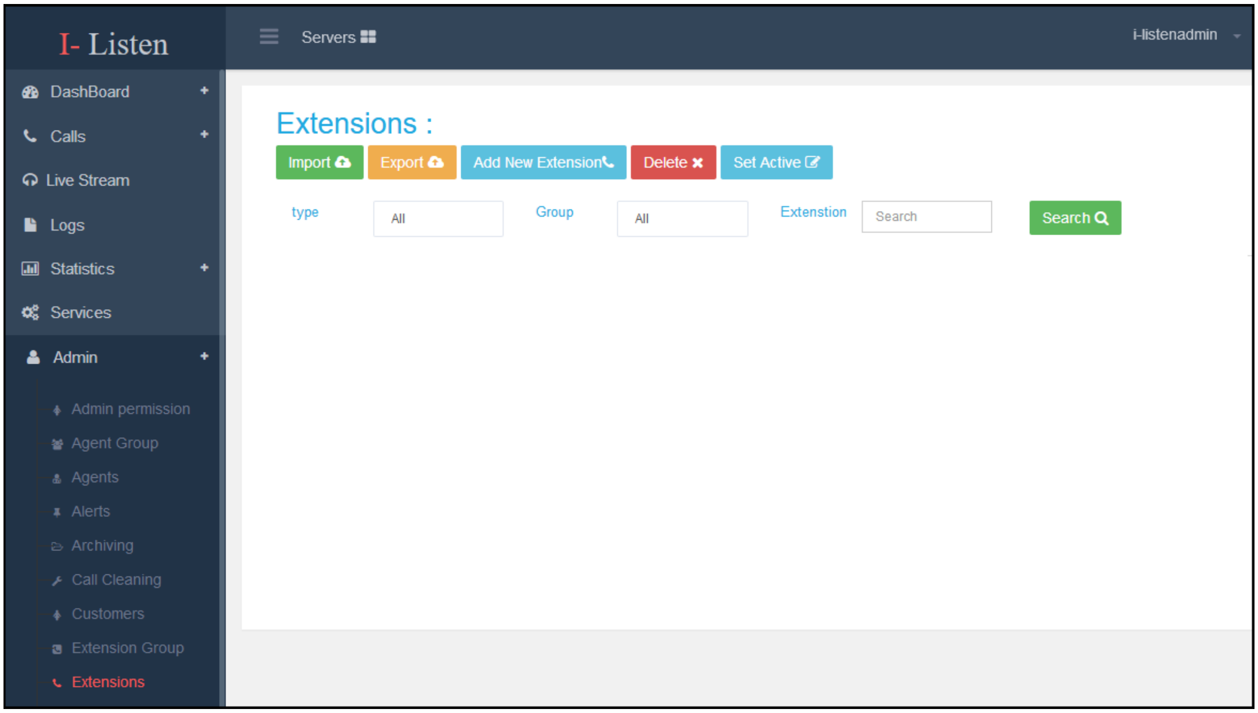
7.1. Login to i-Listen Call Recording Server

Use **http://<server IP>** to access the web administration screen of the i-Listen Call Recording Server. Log in with appropriate credentials.

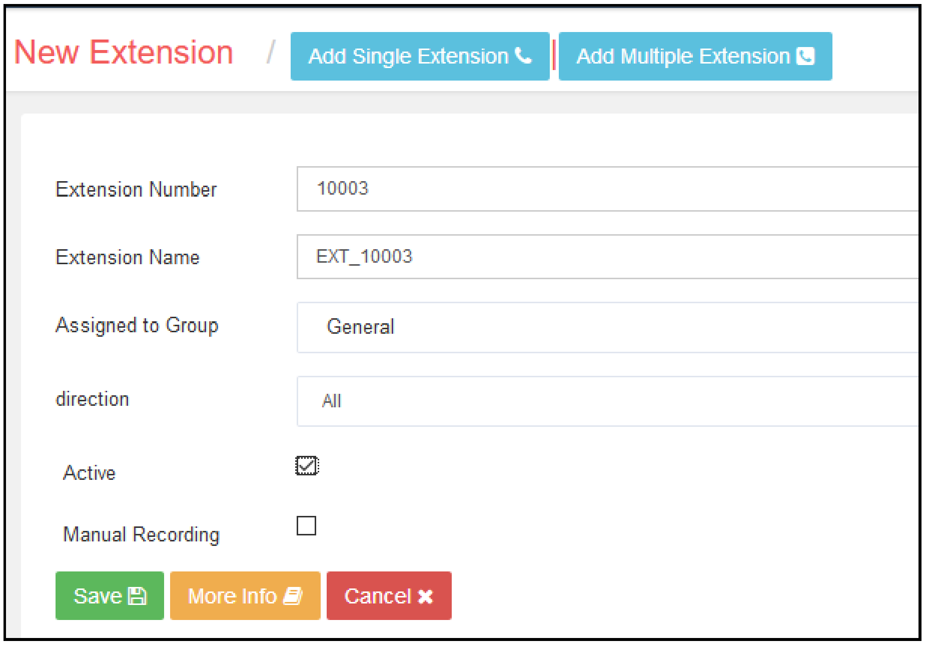


7.2. Register extensions to i-Listen Call Recording Service

The web interface is used to configure the extensions. Select **Admin → Extensions** from the home screen and click on **Add New Extension**.



Click on **Add Single Extension** and complete the details. Below is an example of extension **10003** added. Click **Save** to complete the administration.



Extension Number	10003
Extension Name	EXT_10003
Assigned to Group	General
direction	All
Active	☑
Manual Recording	□

8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Avaya and i-Listen Call Recording solution.

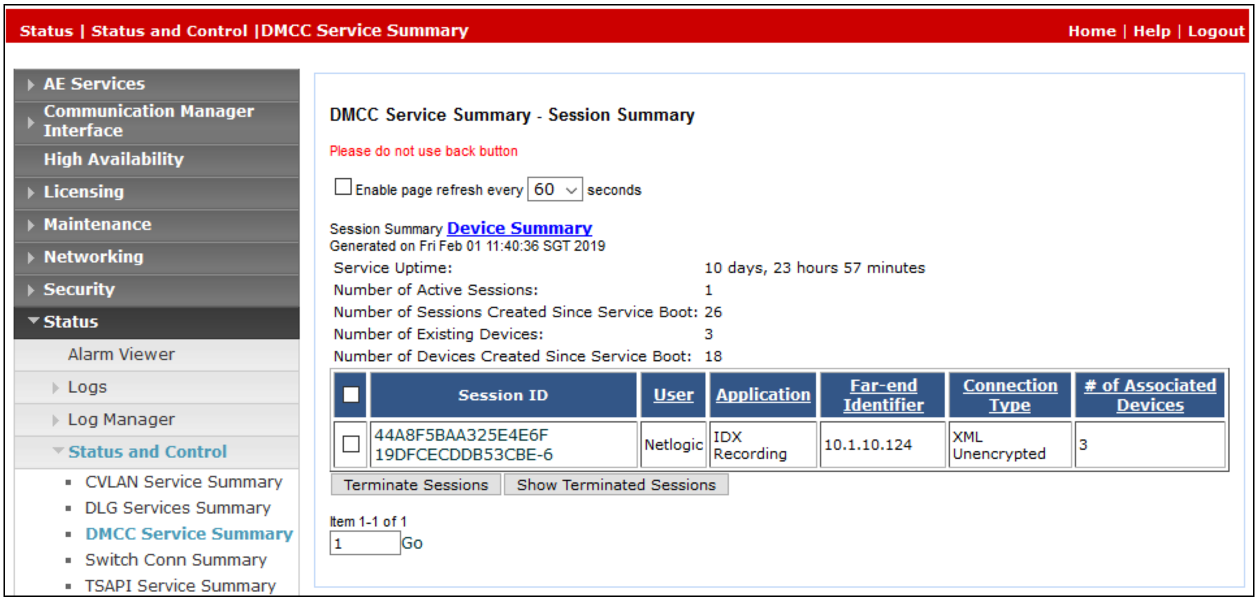
8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the AESVCS link status with Application Enablement Services by using the command **status aesvcs cti-link**. The CTI Link is 1. Verify the **Service State** of the CTI link is **established**.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

3     8        no    aes              established   14        14
```

8.2. Verify Avaya Aura® Application Enablement Services DMCC Service

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly. Verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary.** The **DMCC Service Summary – Session Summary** screen is displayed as shown below. The **Application** is displayed as **IDX Recording** and the **Far-end Identifier** is given as the IP address as expected.



DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Fri Feb 01 11:40:36 SGT 2019

Service Uptime:	10 days, 23 hours 57 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	26
Number of Existing Devices:	3
Number of Devices Created Since Service Boot:	18

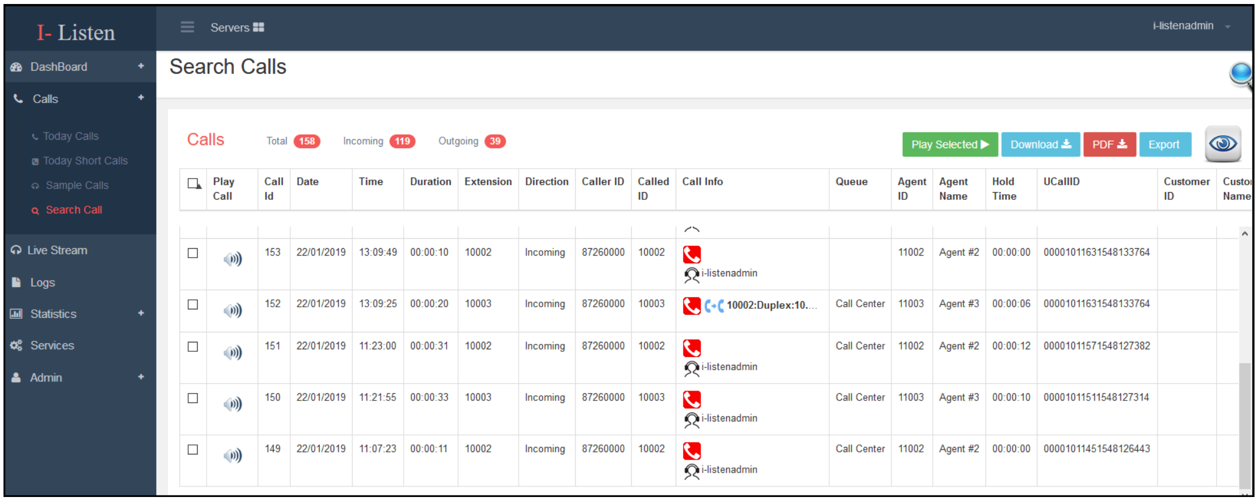
☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	44A8F5BAA325E4E6F19DFCECDDB53CBE-6	Netlogic	IDX Recording	10.1.10.124	XML Unencrypted	3

Item 1-1 of 1

1 Go

8.3. Verify Call Recording

The following steps can be performed to verify the basic operation of the system components. Click on **Calls → Search Call** (not shown) and enter the search criteria. See the result of a sample screenshot below.

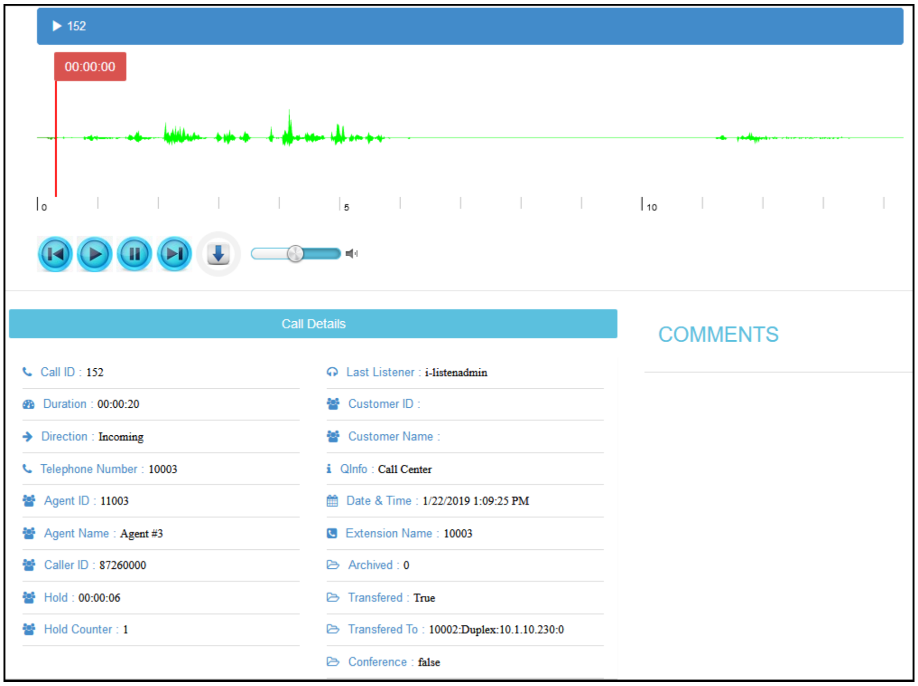


Search Calls

Calls Total 158 Incoming 119 Outgoing 39

☐	Play Call	Call Id	Date	Time	Duration	Extension	Direction	Caller ID	Called ID	Call Info	Queue	Agent ID	Agent Name	Hold Time	UCallID	Customer ID	Custo Name
☐	🔊	153	22/01/2019	13:09:49	00:00:10	10002	Incoming	87260000	10002	☎ i-listenadmin		11002	Agent #2	00:00:00	00001011631548133764		
☐	🔊	152	22/01/2019	13:09:25	00:00:20	10003	Incoming	87260000	10003	☎ 10002:Duplex:10....	Call Center	11003	Agent #3	00:00:06	00001011631548133764		
☐	🔊	151	22/01/2019	11:23:00	00:00:31	10002	Incoming	87260000	10002	☎ i-listenadmin	Call Center	11002	Agent #2	00:00:12	00001011571548127382		
☐	🔊	150	22/01/2019	11:21:55	00:00:33	10003	Incoming	87260000	10003	☎ i-listenadmin	Call Center	11003	Agent #3	00:00:10	00001011511548127314		
☐	🔊	149	22/01/2019	11:07:23	00:00:11	10002	Incoming	87260000	10002	☎ i-listenadmin	Call Center	11002	Agent #2	00:00:00	00001011451548126443		

Select any of the Play Call icon 🔊 and the following sample screen will be shown. Click on the play button to play back the recordings. Note some information regarding hold, transfer and conference will also be displayed in the details other than the essential details user number/name, duration, date and time and CallerID.



Call ID : 152	Last Listener : i-listenadmin
Duration : 00:00:20	Customer ID :
Direction : Incoming	Customer Name :
Telephone Number : 10003	QInfo : Call Center
Agent ID : 11003	Date & Time : 1/22/2019 1:09:25 PM
Agent Name : Agent #3	Extension Name : 10003
Caller ID : 87260000	Archived : 0
Hold : 00:00:06	Transfered : True
Hold Counter : 1	Transfered To : 10002:Duplex:10.1.10.230:0
	Conference : false

9. Conclusion

These Application Notes describe the configuration steps required for the Netlogic Tec i-Listen Call Recording System to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All functionality and serviceability test cases were completed successfully with observations shown in **Section 2.2**.

10. Additional References

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

[1] *Administering Avaya Aura® Application Enablement Services*, Release 8.0.1, Issue 2, December 2018

[2] *Administering Avaya Aura® Communication Manager*, Release 8.0.1, Issue 3, December 2018.

Product documentation for i-Listen Call Recording System can be obtained upon request from Netlogic Tec.

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.