



Avaya Solution & Interoperability Test Lab

Application Notes for NextGen LA-6000 V2 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 for VoIP call recording – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for NextGen LA-6000 V2 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 for VoIP call recording.

In the compliance testing, NextGen LA-6000 uses the Avaya Aura® Application Enablement Services Telephony Services Application Programming Interface (TSAPI) to monitor call center agents with Avaya H.323 IP Deskphones, and to obtain call information and media associated with the monitored agents for call recording.

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

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

1. Introduction

These Application Notes describe the configuration steps required for NextGen LA-6000 V2 (hereafter referred to as LA-6000) to interoperate with Avaya Aura® Communication Manager (Communication Manager) 8.1 and Avaya Aura® Application Enablement Services (AES) 8.1 for VoIP call recording.

In the compliance testing, LA-6000 with AESMGR6K component used the AES' TSAPI interface to monitor call center agents with Avaya H.323 IP Deskphones, and obtained call information such as call start and end time, caller IDs, etc., and thereby extracted media associated with the calls for call recording from monitored ports. The media is obtained from mirrored network ports of Avaya Aura® Media Server (AAMS), Medpro boards and/or Media Gateway Processor (MGP) to the LA-6000 server and extracted the Real-Time Transport Protocol (RTP) packets for the voice data. Voice recording is then stored on the NextGen VoISplus server which allow searching for voice records using call data from web-browser.

2. General Test Approach and Test Results

The feature test cases were performed manually. Each call was handled manually on the station user with generation of unique audio content for the recordings. Necessary user actions such as hold and resume were performed from the user stations to test different call scenarios for Avaya 9600 Series H.323 IP Deskphones. It also included feature calls such as call park/unpark, call recovery from long hold call, call transfer and 3-way conference.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cable to LA-6000 server, restarting TSAPI service on the AES, busying and releasing CTI link on Communication Manager, restart Communication Manager server and finally restarting the AES server.

The verification of tests included using the LA-6000 logs for proper status, using the web browser to verify proper logging and playing back of the calls.

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

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 NextGen LA-6000 did not include use of any specific encryption features as requested by NextGen.

2.1. Interoperability Compliance Testing

The interoperability compliance test includes feature and serviceability testing.

Feature testing focused on verifying the following scenarios on LA-6000 for proper recordings, loggings and playback of calls:

- Inbound calls, external and internal
- Outbound calls, external and internal
- External and internal Transfer calls
- 3-Party Conference calls
- Call Hold (including Long Hold recall) and Resume
- Call Park and Unpark
- Redirection on No Answer (RONA)
- Codec G.711 Mu Law which is the only codec supported
- Long duration call

Serviceability testing focused on verifying the ability of LA-6000 to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to LA-6000 server, restarting TSAPI service, restarting the CTI link as well as AES and Communication Manager server.

2.2. Test Results

All feature test cases were successfully completed. An observation to note is that media shuffling needs to be disabled to direct all voice traffic through media processors such as AAMS, Medpro board and MGP where traffic is monitored for RTP.

2.3. Support

Technical support on NextGen LA-6000 V2 can be obtained through the following:

- **Phone:** +81-(0)50-5865-3607
- **Web:** <https://www.nextgen.co.jp/>

3. Reference Configuration

LA-6000 has a thin client web interface that can be used to review and playback the call recordings on the VoISplus server.

In the compliance testing, LA-6000 monitored the agent station extensions shown in the contact center device table below.

Device Type	Extension
VDN	14001
Skill Group	13001
Agent Station	10001,10002,10003
Agent ID	11001,11002,11003

Figure 1 below illustrates the test configuration consisting of a duplex pair of Avaya Aura® Communication Manager servers, Avaya G430 Media Gateway, Avaya G650 Media Gateway, Avaya Aura® Application Enablement Services server and Avaya Aura® Media Server. Avaya 9600 Series H.323 IP Deskphones are used as agent stations. LA-6000 server is installed on a virtualized Centos 7 server which communicates with the TSAPI service on the Avaya Aura® Application Enablement Services server. A simulated public PSTN trunk connects to the system. The 9600 Series H.323 IP Deskphones are used to generate intraswitch calls (calls between telephones on the same system) and outbound/inbound calls to/from the PSTN.

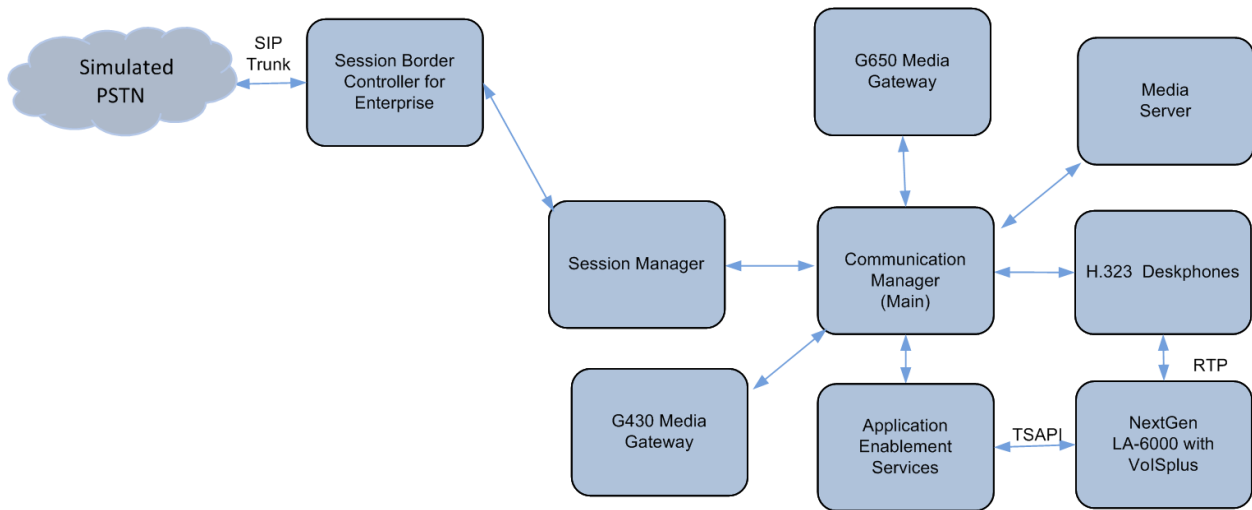


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager (Duplex)	8.1 FP1 R018x.00.0.822.0 - 25763
Avaya G650 Media Gateway <ul style="list-style-type: none"> • Medpro TN2602 	HW2 FW67
Avaya G430 Media Gateway: <ul style="list-style-type: none"> • MGP 	41.16.0
Avaya Aura® Application Enablement Services	8.1.1.0.1.8-0
Avaya Aura® System Manager	System Manager 8.1.1.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.1.0.0310912 Feature Pack 1
Avaya Aura® Session Manager	Session Manager R8.1 FP1 Build No. – 8.1.1.0.811021
Avaya Aura® Media Server	R8.0.1.121
Avaya 9600 Series IP Deskphones: <ul style="list-style-type: none"> • 9641G (H.323) • 9611G (H.323) 	<ul style="list-style-type: none"> • 6.802 • 6.802
NextGen Centos Server <ul style="list-style-type: none"> • Avaya TSAPI Linux Client • AESMGR6K • LA-6000 • VoISplus 	7.4.1708 <ul style="list-style-type: none"> • 8.1-9 • 1.5-0b • 2.3-2b • 2.3-2b

5. Configure Avaya Aura® Communication Manager

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

- Verify Communication Manager License
- Administer CTI link
- Disable Media Shuffling
- Administer IP Codec

5.1. Verify Communication Manager License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **Computer Telephony Adjunct Links** customer option is set to **y** on **Page 4**. If this option is not set to **y**, then contact the Avaya sales team or business partner for a proper license file.

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

Abbreviated Dialing Enhanced List? y                               Audible Message Waiting? y
  Access Security Gateway (ASG)? 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. Administer CTI Link

Add a CTI link using the **add cti-link n** command, where **n** is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 3                                     Page 1 of 3
                                               CTI LINK
  CTI Link: 3
  Extension: 10093
    Type: ADJ-IP
                                               COR: 1
  Name: TSAPI Service - AES 8x
  Unicode Name? n
```

5.3. Disable Media Shuffling

Media shuffling is disabled to direct all voice traffic through media processors such as MGP, AAMS and Medpro boards where traffic is monitored for RTP. In the ip-network-region form of the agents, set the IP-IP Direct Audio to **no** for both **Intra-region** and **Inter-region**. Note the **Codec Set** used for the Deskphone which is **1** in the environment setup.

Repeat this for other ip-network-region where Deskphones utilized the media resources.

```
change ip-network-region 1                         Page 1 of 20
                                               IP NETWORK REGION
  Region: 1      NR Group: 1
  Location: 1    Authoritative Domain: sglab.com
    Name: Local  Stub Network Region: n
  MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: no
    Codec Set: 1      Inter-region IP-IP Direct Audio: no
  UDP Port Min: 2048      IP Audio Hairpinning? n
  UDP Port Max: 3999
  DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46
    Audio PHB Value: 46
    Video PHB Value: 26
  802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5
  AUDIO RESOURCE RESERVATION PARAMETERS
  H.323 IP ENDPOINTS      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
```


5.4. Administer IP Codec

In the **IP Codec** form, set the first choice **Audio Codec** to **G.711MU** which is the codec supported by LA-6000.

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

                                IP MEDIA PARAMETERS

Codec Set: 1

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

Media Encryption Encrypted SRTCP: best-effort
1: 1-srtp-aescm128-hmac80
2: 2-srtp-aescm128-hmac32
3: none
4:
5:
```

6. Configure Avaya Aura® Application Enablement Services

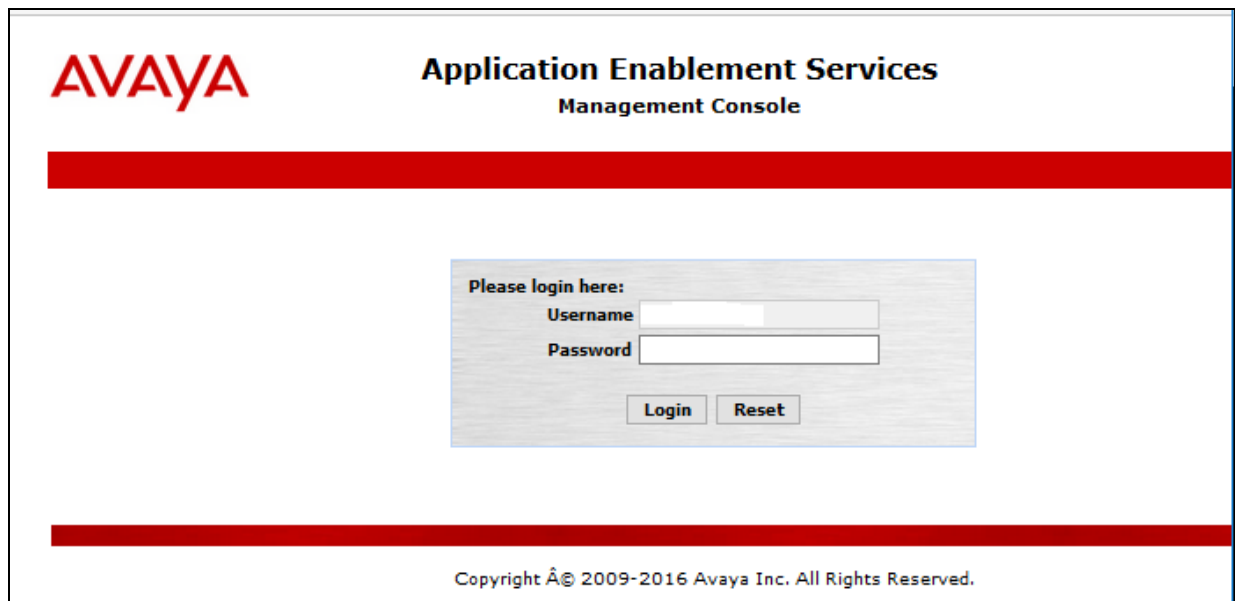
This section provides the procedures for configuring AES. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Disable security database
- Restart TSAPI service
- Obtain Tlink name
- Administer NextGen user
- Administer CTI User permissions
- Enable TSAPI Service port

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 AES server.

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



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text reads "Application Enablement Services Management Console". Below this is a thick red horizontal bar. In the center, there is a login box with the heading "Please login here:". Inside the box, there are two input fields: "Username" and "Password". Below the input fields are two buttons: "Login" and "Reset". At the bottom of the page, there is another thick red horizontal bar and a copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

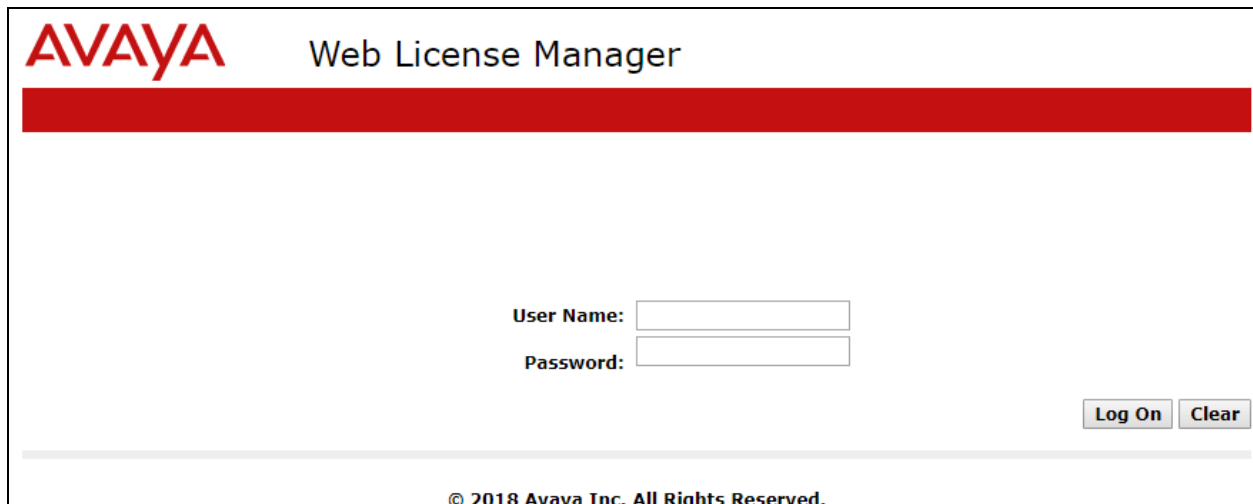
The **Welcome to OAM** screen is displayed next.

The screenshot shows the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo and the title 'Application Enablement Services Management Console'. At the top right, there is a user information block: 'Welcome: User cust', 'Last login: Wed Mar 4 14:51:35 2020 from 10.1.10.155', 'Number of prior failed login attempts: 0', 'HostName/IP: aes/10.1.10.70', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 8.1.1.0.1.8-0', 'Server Date and Time: Thu Mar 05 09:15:24 SGT 2020', and 'HA Status: Not Configured'. Below this is a red navigation bar with 'Home' on the left and 'Home | Help | Logout' on the right. On the left side of the main content area is a vertical menu with items: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The main content area is titled 'Welcome to OAM' and contains the following text: 'The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:'. This is followed by a bulleted list: '• 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'. At the bottom of the main content area, it states: 'Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.'

Note: All of the screens in subsequent sections are shown after the AES had been configured. Click Apply Changes button to save the screen parameters configured on Application Enablement Services if needed.

6.2. Verify License

Select **Licensing** → **WebLM Server Access** (not shown) from the left pane of the home screen and note the **WebLM Server Address**. Access the WebLM License Manager web-based interface by using the URL “https://ip-address:52233/WebLM” in an internet browser window, where “ip-address” is the ip address of the WebLM server. Log in with the appropriate credentials.



The screenshot shows the Avaya Web License Manager login interface. At the top left is the Avaya logo in red. To its right is the text "Web License Manager". Below this is a thick red horizontal bar. The main content area is white and contains a login form with two input fields: "User Name:" and "Password:". To the right of the "Password:" field are two buttons: "Log On" and "Clear". At the bottom center of the page, there is a copyright notice: "© 2018 Avaya Inc. All Rights Reserved."

From Home Page (not shown), go to **Services → Licenses**. Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane to display the **Licensed Features** screen in the right pane. Scroll down the screen, and verify that there are sufficient licenses **TSAPI Simultaneous Users**, as shown below. Consult Avaya sales or business partner to obtain the license file.


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

You are here: [Licensed Products](#) > [Application_Enablement](#) > [View License Capacity](#)

License installed on: February 27, 2020 11:52:56 AM +08:00

License File Host IDs: V4-0F-01-B6-9A-9B-02

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	0
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	10
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	0
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
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16

6.3. 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.
- **Switch CTI Link Number:** Corresponding CTI link number in **Section 5.2**.
- **ASAI Link Version:** Set to the latest version.
- **Security:** Select **Both** to allow for encrypted or unencrypted link.

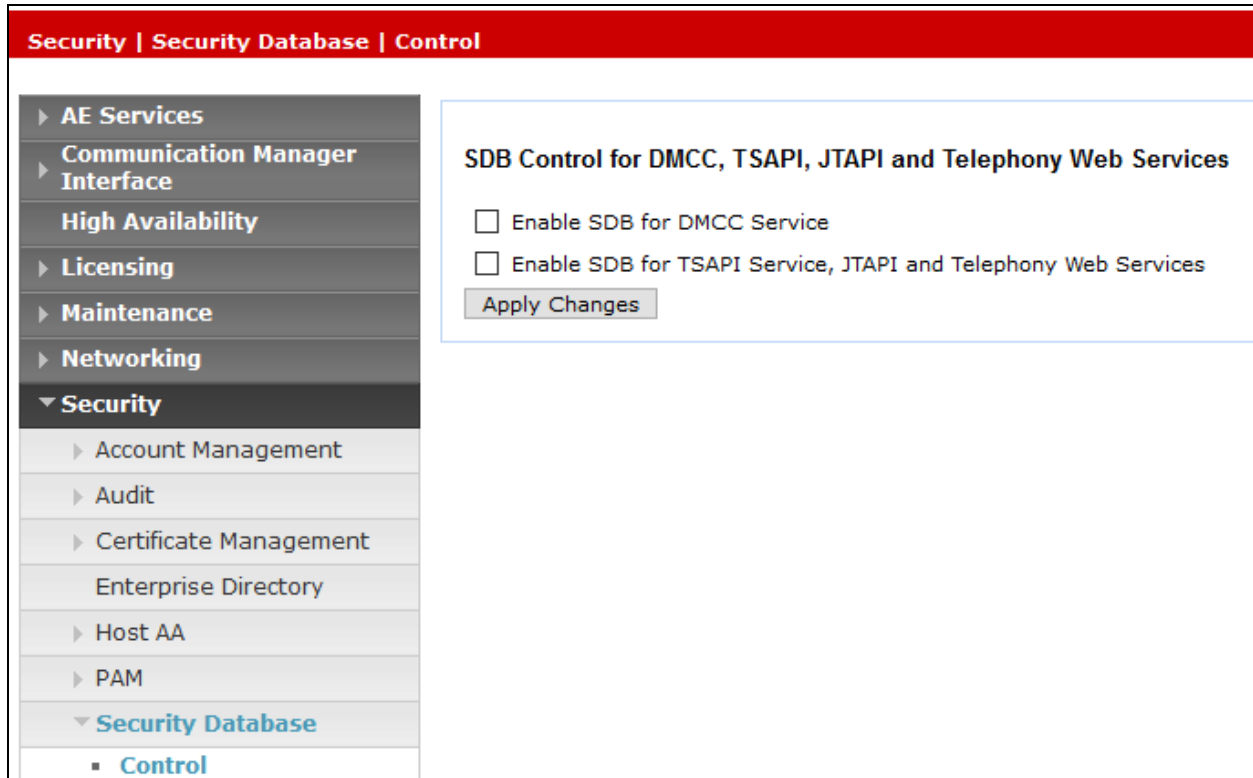
Click **Apply Changes** to affect changes.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a user welcome message: 'Welcome: User cust', 'Last login: Thu Mar 19 16:10:17 2020 from 10.1.10.156', 'Number of prior failed login attempts: 0', 'HostName/IP: aes/10.1.10.70', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 8.1.1.0.1.8-0', 'Server Date and Time: Mon Mar 23 14:23:41 SGT 2020', and 'HA Status: Not Configured'. A red navigation bar contains 'AE Services | TSAPI | TSAPI Links' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'AE Services' expanded, containing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), and 'TSAPI Properties'. The main content area is titled 'Edit TSAPI Links' and contains the following configuration fields: 'Link' (text input with value '3'), 'Switch Connection' (dropdown menu with 'Duplex' selected), 'Switch CTI Link Number' (dropdown menu with '3' selected), 'ASAI Link Version' (dropdown menu with '11' selected), and 'Security' (dropdown menu with 'Both' selected). At the bottom of the configuration area are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

6.4. Disable Security Database

Select **Security** → **Security Database** → **Control** from the left pane to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Make certain both parameters are unchecked, as shown below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the user from **Section Error!** Reference source not found.7.



The screenshot shows a web interface with a red header bar containing the text "Security | Security Database | Control". On the left is a navigation pane with a tree view. The "Security" folder is expanded, and the "Control" item is selected. The main content area on the right is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these checkboxes is an "Apply Changes" button.

6.5. Restart TSAPI Service

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**.

The screenshot shows a web interface for the Service Controller. On the left is a navigation menu with categories: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (selected), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, and Security. The main content area is titled 'Service Controller' and contains a table with the following data:

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input type="checkbox"/> TSAPI Service	Running

Below the table, there is a note: 'For status on actual services, please use [Status and Control](#)'. At the bottom of the main area, there are several buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

6.6. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service.

Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring LA-6000.

In this case, the associated unencrypted Tlink name is **AVAYA#DUPLEX#CSTA#AES**, which is automatically assigned by the Avaya AES server.

The screenshot shows the Avaya Security Database configuration interface. The left-hand navigation pane is expanded to 'Security Database' > 'Tlinks'. The main content area, titled 'Tlinks', displays a list of Tlink names under the heading 'Tlink Name'. The first option, 'AVAYA#DUPLEX#CSTA#AES', is selected with a radio button and is highlighted with a red rectangular box. Below the list is a 'Delete Tlink' button.

Security | Security Database | Tlinks

Tlinks

Tlink Name

- AVAYA#DUPLEX#CSTA#AES
- AVAYA#DUPLEX#CSTA-S#AES
- AVAYA#G450#CSTA#AES
- AVAYA#G450#CSTA-S#AES

Delete Tlink

6.7. Administer NextGen User

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

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).

The screenshot shows the 'Add User' form within the 'User Management | User Admin | Add User' interface. The left sidebar contains a navigation menu with 'User Management' expanded to show 'User Admin' and 'Add User' selected. The main form area is titled 'Add User' and includes a note: 'Fields marked with * can not be empty.' The form fields are as follows:

Field Name	Value / Selection
* User Id	nextgen
* Common Name	nextgen
* Surname	nextgen
* 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	
Given Name	
Home Phone	
Home Postal Address	
Initials	
Labeled URI	

6.8. Enable TSAPI Service Port

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

In the **TSAPI Ports** section, select the radio button under the **Enabled** column, as shown below. Scroll down and click **Apply Changes** (not shown).

The screenshot shows the 'Networking | Ports' configuration page. The left sidebar contains a navigation menu with 'Networking' expanded to show 'Ports'. The main content area is titled 'Ports' and is divided into sections: 'CVLAN Ports', 'DLG Port', and 'TSAPI Ports'. The 'TSAPI Ports' section includes a table with columns for 'Enabled' and 'Disabled' radio buttons. The 'TSAPI Service Port' is set to 450 and is currently enabled.

CVLAN Ports			Enabled	Disabled
Unencrypted TCP Port	9999		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>		<input checked="" type="radio"/>	<input type="radio"/>

DLG Port	TCP Port	Value
		5678

TSAPI Ports			Enabled	Disabled
TSAPI Service Port	450		<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports				
TCP Port Min	1024			
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	<input type="text" value="1050"/>			
TCP Port Max	<input type="text" value="1065"/>			
Encrypted TLINK Ports				
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			

7. Configure NextGen LA-6000

This section provides the procedures for configuring LA-6000. The AESMGR6K module on the LA-6000 server communicates with AES from the administrative ethernet port and other ethernet port connects to the monitoring port of data switch, which mirror ports of Medpro, MGP and AAMS. Ensure that the monitoring ethernet ports are in promiscuous mode and all traffic is allowed on virtualized host server port. In this compliance testing, only one ethernet port is used for monitoring.

The VoISplus stores the call recording which is normally set up in a separate server. But in this compliance testing, the VoISplus function is installed on the same server with the LA-6000.

The procedures include the following areas:

- Administer Telephony TSAPI
- Administer Media Processor list and Monitor Port
- Administer Agent Station's IP address list
- Restart Services

The configuration of LA-6000 is performed by NextGen services engineers. The procedural steps are presented in these Application Notes for informational purposes. These Application Notes assume that the configurations of a site, server sizing, appropriate license and storage volumes are all in place and will not be covered. Refer to [3] in the reference section for the installation instructions.

7.1. Administer Telephony TSAPI

Log in to the LA-6000 CentOS server console with the appropriate user login. Navigate to the `../NXS/conf` directory to locate the `La6Avaya.ini` file and view the file with `vi` editor. Verify the parameter `AesServerName` is set the same as Tlink name in **Section 6.6**. Verify the `LinkUserID` and `LinkPassword` is set as configured in **Section 6.7**. Note that the `LinkPassword` is hidden here for security reason.

Check also that `AvayaEnable` is set to "1".

```
LA6IP1 = "10.1.10.123"
AesServerName = "AVAYA#DUPLEX#CSTA#AES"
LinkUserID = "nextgen"
LinkPassword = "xxxxxxxxxxx"
AvayaEnable = "1"
```

7.2. Administer Media Processor List and Monitor Port

On the console, navigate to the `../NXS/conf` directory to locate the `vliuser.ini` file and view the file with `vi` editor. Locate the parameter `NorthGWList` and verify the Media Processors' IP address. The Media Processor IP address could be Medpro boards on the Avaya G650 Media Gateway, the AAMS or the Media Gateway Processor (MGP) of Avaya G430 and G450 Media Gateway. In this compliance testing, the IP address of AAMS and a Medpro board on the Avaya G650 Media Gateway are added where RTP stream is transcoded.

```
PetName::la6k
Divsz_Type::1
BKUP_Retention::-1
HTTPCollaboration::0
PowerRestart::1
NorthGWList::10.1.10.13,10.1.10.32
BKUP_Arrange_Time::02:00
BlackNumberList::
HTTPOri::
TransAlarm::0
Idx_Number1::1
Idx_Number2::1
Idx_Agent::0
Idx_DTMF::0
Divsz_Minutes::60
Idx_Extension::0
SouthGWList::
@ipcap0
NICName::ens192
F0_Netaddr::0.0.0.0
F0_Netmask::0
F0_Trans::2
F0_Network::1
```

On the lower portion of the vliuser.ini file on the previous page, locate the parameter **@ipcap0**. This is set to the name of the monitoring port which in this environment is **ens192**. This name can be identified through the **ifconfig** command which list the ethernet ports of the server. Up to 3 ethernet monitoring ports can be used depending also on the number of monitor ports on the data switches.

7.3. Administer Agent Station's IP address list

On the console, navigate to the **../NXS/conf** directory to locate the **LaIdTable1.csv** file and **vi** the file. Verify the IP address of the corresponding deskphones extension is correct.

```
10001,10.1.10.171
10002,10.1.10.198
10006,10.1.10.170
```

7.4. Restart Services

On the console, navigate to the **../NXS/bin** directory. Execute the following **nxs.sh** commands to restart the NXS service. Note that the user name is masked out for security reason.

```
[                ]$ ./nxs.sh stop
Stopping hamanager (PID:6915) ...
hamanager stopped.

[                ]$ ./nxs.sh start
Starting hamanager ...
[                ]$ Setting up watches.
Watches established.
Started logobserver.
start vli successfully.
AesManager6K started.
```

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and NextGen LA-6000.

8.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
3	10	no	aes	established	15	15

8.2. Verify Avaya Aura® Application Enablement Services

For AES, verify the status of the TSAPI link by selecting the **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed. On the right pane of the screen. Verify that the **Status** column shows a **Talking** session and that the **State Devices** column shows **Online**. Click on the **User Status** below.

Status | Status and Control | TSAPI Service Summary Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
▼ **Status**
Alarm Viewer
Logs
Log Manager
▼ **Status and Control**
CVLAN Service Summary
DLG Services Summary
DMCC Service Summary
Switch Conn Summary
▼ **TSAPI Service Summary**

TSAPI Link Details
 Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	G450	1	Talking	Thu Mar 19 16:01:20 2020	Online	18	0	15	15	30
<input type="radio"/>	3	Duplex	3	Talking	Mon Mar 23 14:23:29 2020	Online	18	0	195	195	30

For service-wide information, choose one of the following:

Verify the **nextgen** user is listed under the **Open Streams** with the Tlink Name in **Section 6.6**.

CTI User Status

Enable page refresh every seconds

CTI Users

Open Streams 1
Closed Streams 0

Open Streams

Name	Time Opened	Time Closed	Tlink Name
nextgen	Thu 19 Mar 2020 04:01:35 PM +08		AVAYA#DUPLEX#CSTA#AES

8.3. Verify NextGen LA-6000

Log in to the LA-6000 server with an appropriate login to verify TSAPI messages are received. Change directory to **/home/<user>/NXS/log** and type the command “tail -f La6Avaya.log”. Verify the messages “*** Health Check OK! ***” is shown and repeatedly displayed.

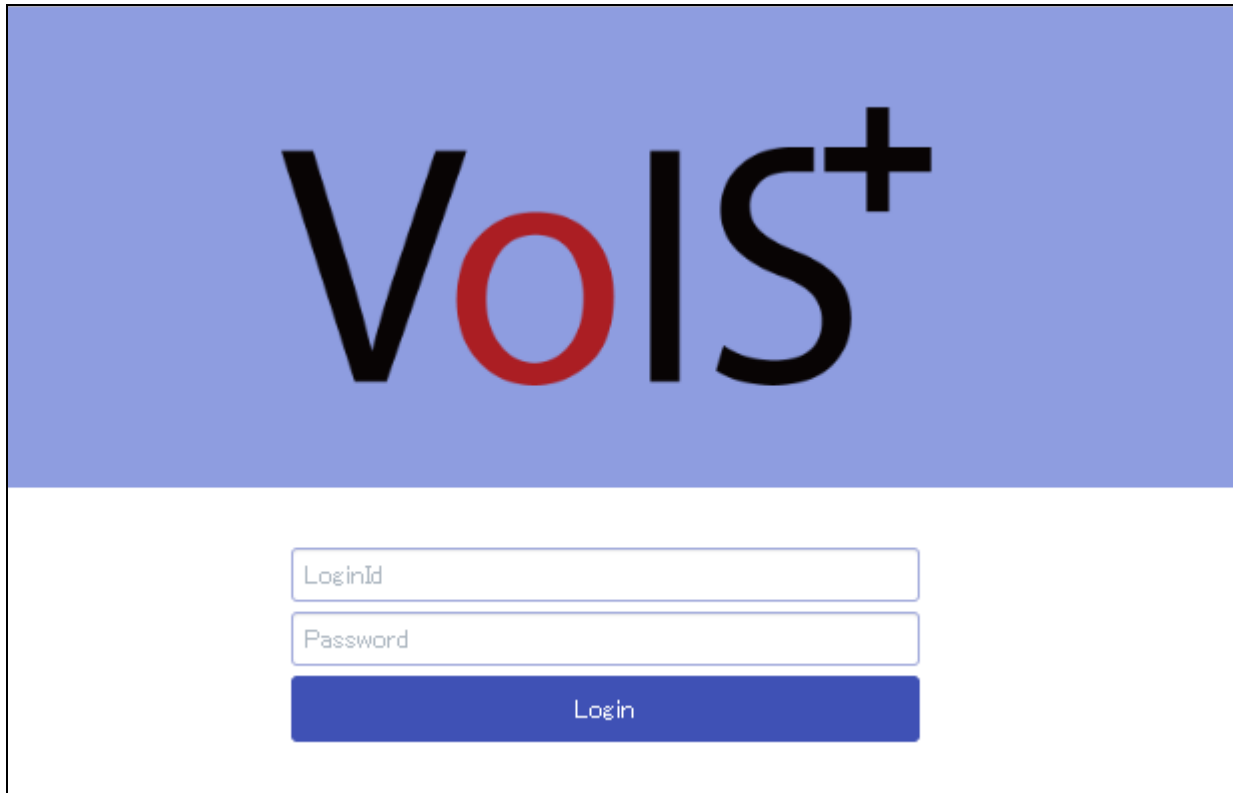
```
AES Manager for LA-6000 Ver. 1.5-0b
[2020/03/23 02:00:08.046] INF
[2020/03/23 02:00:08.046] INF *** Health Check OK! ***
[2020/03/23 02:00:18.009] INF
[2020/03/23 02:00:18.009] INF *** Health Check OK! ***
[2020/03/23 02:00:28.023] INF
[2020/03/23 02:00:28.023] INF *** Health Check OK! ***
[2020/03/23 02:00:38.036] INF
[2020/03/23 02:00:38.036] INF *** Health Check OK! ***
[2020/03/23 02:00:48.000] INF
[2020/03/23 02:00:48.000] INF *** Health Check OK! ***
[2020/03/23 02:00:58.013] INF
[2020/03/23 02:00:58.013] INF *** Health Check OK! ***
[2020/03/23 02:01:08.027] INF
[2020/03/23 02:01:08.027] INF *** Health Check OK! ***
[2020/03/23 02:01:18.040] INF
[2020/03/23 02:01:18.040] INF *** Health Check OK! ***
[2020/03/23 02:01:28.003] INF
[2020/03/23 02:01:28.004] INF *** Health Check OK! ***
[2020/03/23 02:01:38.017] INF
```


Make an inbound call to any of the agent. Verify the TSAPI monitoring messages are received from the logs.

```
[2020/03/17 15:03:15.408] INF [CSTA_DELIVERED]
[2020/03/17 15:03:15.408] INF Monitor Extension: 10001
[2020/03/17 15:03:15.408] INF Call Status: CS_ALERTING
[2020/03/17 15:03:15.408] INF <<CallInfo>>
[2020/03/17 15:03:15.408] INF CallID: 5760
[2020/03/17 15:03:15.408] INF CallingDevice: 602
[2020/03/17 15:03:15.408] INF CalledDevice: 14001
[2020/03/17 15:03:15.408] INF UCID: 00001057601584428593
[2020/03/17 15:03:15.408] INF TrunkGroup: 7
[2020/03/17 15:03:15.408] INF TrunkMember: 1
[2020/03/17 15:03:15.408] INF Direction: 2
[2020/03/17 15:03:15.409] INF CallingExtensionNo:
[2020/03/17 15:03:15.409] INF CalledExtensionNo: 10001
[2020/03/17 15:03:15.409] INF calls count: 0
[2020/03/17 15:03:15.409] INF [Incoming in]-10001 : Dest:602 Self:14001
TerminalIP:10.1.10.171
[2020/03/17 15:03:16.716] INF [Answer]-10001 : Rec start Dest:602 Self:14001
TerminalIP:10.1.10.171
[2020/03/17 15:03:16.716] INF Rec-ID:4
[2020/03/17 15:03:16.719] INF
[2020/03/17 15:03:16.719] INF [CSTA_ESTABLISHED]
[2020/03/17 15:03:16.719] INF Monitor Extension: 10001
[2020/03/17 15:03:16.719] INF Call Status: CS_CONNECT
[2020/03/17 15:03:16.719] INF <<CallInfo>>
[2020/03/17 15:03:16.719] INF CallID: 5760
[2020/03/17 15:03:16.719] INF CallingDevice: 602
[2020/03/17 15:03:16.719] INF CalledDevice: 14001
[2020/03/17 15:03:16.719] INF UCID: 00001057601584428593
[2020/03/17 15:03:16.719] INF TrunkGroup: 7
[2020/03/17 15:03:16.719] INF TrunkMember: 1
[2020/03/17 15:03:16.719] INF Direction: 2
[2020/03/17 15:03:16.719] INF CallingExtensionNo:
[2020/03/17 15:03:16.719] INF CalledExtensionNo: 10001
[2020/03/17 15:03:16.719] INF calls count: 1
[2020/03/17 15:03:16.764] INF
[2020/03/17 15:03:16.764] INF QueryDeviceInfo 10001
[2020/03/17 15:03:16.764] INF [Regist]-10001 : AgentID:11011 TerminalIP:10.1.10.171
[2020/03/17 15:03:23.042] INF
[2020/03/17 15:03:23.042] INF *** Health Check OK! ***
[2020/03/17 15:03:31.670] INF
[2020/03/17 15:03:31.670] INF [CSTA_CONNECTION_CLEARED]
[2020/03/17 15:03:31.670] INF Monitor Extension: 10001
[2020/03/17 15:03:31.670] INF Call Status: CS_NULL
[2020/03/17 15:03:31.670] INF <<CallInfo>>
[2020/03/17 15:03:31.670] INF CallID: 5760
[2020/03/17 15:03:31.670] INF CallingDevice: 602
[2020/03/17 15:03:31.670] INF CalledDevice: 14001
[2020/03/17 15:03:31.670] INF UCID: 00001057601584428593
[2020/03/17 15:03:31.671] INF TrunkGroup: 7
[2020/03/17 15:03:31.671] INF TrunkMember: 1
[2020/03/17 15:03:31.671] INF Direction: 2
[2020/03/17 15:03:31.671] INF CallingExtensionNo:
[2020/03/17 15:03:31.671] INF CalledExtensionNo: 10001
[2020/03/17 15:03:31.671] INF calls count: 1
[2020/03/17 15:03:31.671] INF [On Hook]-10001 : Rec stop TerminalIP:10.1.10.171
[2020/03/17 15:03:31.671] INF Rec-ID:4
[2020/03/17 15:03:33.006] INF
```

From a PC, access the call recordings from the web-based interface by using the URL “http://ip-address” in an internet browser window, where “ip-address” is the IP address of the LA-6000 server. Normally, this is the IP address of the VoISplus server where call recordings are stored. But in the test environment, this storage server is residing on the same server as LA-6000.

Log on using appropriate credentials.

The image shows a web-based login interface for VoIS+. The top section has a blue background with the text "VoIS+" in large, bold, black letters, where the "O" is red. Below this, on a white background, are two input fields: "LoginId" and "Password". Below the input fields is a blue button with the text "Login" in white.

From the home screen, navigate to **Status** → **Device Status**. Verify the **Alarm Status** is green with a tick for success for both LA-6000 and VoISplus modules.

device Id	device Name	Model	IP Address	Alarm Status	Event Time
0	VoISplus	VoISplus	127.0.0.1	✔ success	
1	LA6000	LA-6000	10.1.10.123	✔ success	

Make an inbound call to the VDN and answer the call from an agent being recorded. Next click **Status** → **Collect Status** to verify the last collected date and time includes the call just made or just simply search for the call recordings in the next page.

device Id	device Name	Collect Model	Collect Target	Collect Status	Collect Final Result	Collect Date
1	LA6000	LA-6000	✔	🕒	✔ 2020/03/23 15:33	-

In the screen below, call recording for the inbound call to the agent can be found by search function using the appropriate criteria, say the date and time.

The following call recordings were shown upon a call search based on **Start Date** and **End Date**. Double click on the **speaker** icon in any one of the recordings.

Record Id	Operation	Mark	Start Date	End Date	Call Duration	Destination phone number	My phone number	Orig/Term	ext
108		☆	2020/03/19 14:32:30	2020/03/19 14:32:39	00:00:09	602	14001	Termination	
109		☆	2020/03/19 14:32:50	2020/03/19 14:33:04	00:00:14	602	14001	Termination	
110		☆	2020/03/19 14:33:11	2020/03/19 14:33:23	00:00:12	602	14001	Termination	
111		☆	2020/03/19 14:34:52	2020/03/19 14:34:59	00:00:07	10001	14001	Termination	
112		★	2020/03/19 14:34:52	2020/03/19 14:35:18	00:00:26	14001	10001	Origination	
113		☆	2020/03/19 14:35:05	2020/03/19 14:35:17	00:00:12	10001	14001	Termination	

Verify the call recording could be played back from the browser. Only IE and Chrome browsers are supported for online playback.

The screenshot displays a 'Play record' window with a table of call details and a waveform player below it.

Record Id	112
Mark	☆
Start Date	2020/03/19 14:34:52
End Date	2020/03/19 14:35:18
Call Duration	00:00:26
Destination phone number	14001
My phone number	10001
Orig/Term	Origination
extensionNo	10001
Line Name	11001

display waveform

00:00:00 00:00:00 00:00:25

-10 sec Play Pause Stop +10 sec

Noise Cancel OFF Play speed 1.0

Double speed

close

9. Conclusion

These Application Notes describe the configuration steps required for NextGen LA-6000 V2 to successfully interoperate with Avaya Aura® Communication Manager 8.1 using Avaya Aura® Application Enablement Services 8.1 for VoIP call recording. All feature and serviceability test cases were completed.

10. Additional References

This section references the Avaya documentation that is relevant to these Application Notes.

The following Avaya product documentation can be found at <http://support.avaya.com>.

[1] *Administering Avaya Aura® Communication Manager*, Issue 5, Release 8.1.2, Nov 2019.

[2] *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Mar 2020.

The following product documentation can be obtained from NextGen.

[3] *LA-6000 Installation/Administration User's Guide*, Version 2.0

©2020 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.