# Application Notes for NextGen LA-6000 with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 for VoIP call recording – Issue 1.0

## Abstract

These Application Notes describe the configuration steps required for NextGen LA-6000 to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 for VoIP call recording.

In the compliance testing, NextGen LA-6000 uses the Avaya Aura® Application Enablement Services, Telephony Service API (TSAPI) interface to monitor calls, especially contact center agents to Avaya Aura® Communication Manager, and 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 (LA-6000) to interoperate with Avaya Aura® Communication Manager (Communication Manager) 7.1 and Avaya Aura® Application Enablement Services (AES) 7.1 for VoIP call recording.

In the compliance testing, LA-6000 used the AES' TSAPI interface to monitor calls, especially contact center agents to Communication Manager, and obtained call information such call start and end time, caller IDs, etc., and thereby extract media associated with the calls for call recording from monitored ports. The media is obtained from monitored 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 cell 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 the Communication Manager, interchange Communication Manager server and finally restarting the AES server.

The verification of tests included using the LA-6000 logs for proper message, using the 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 included feature and serviceability testing.

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

- Inbound calls, external and internal calls
- Outbound calls, external and internal calls
- 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)

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 interchange of the 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 can be obtained through the following:

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

# 3. Reference Configuration

NextGen 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, NextGen 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 | 10001,10002,10006 |
| 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 Aura® Application Enablement server and Avaya Aura® Media Server. Avaya 9600 Series H.323 IP Deskphones are used as agent stations. NextGen 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.

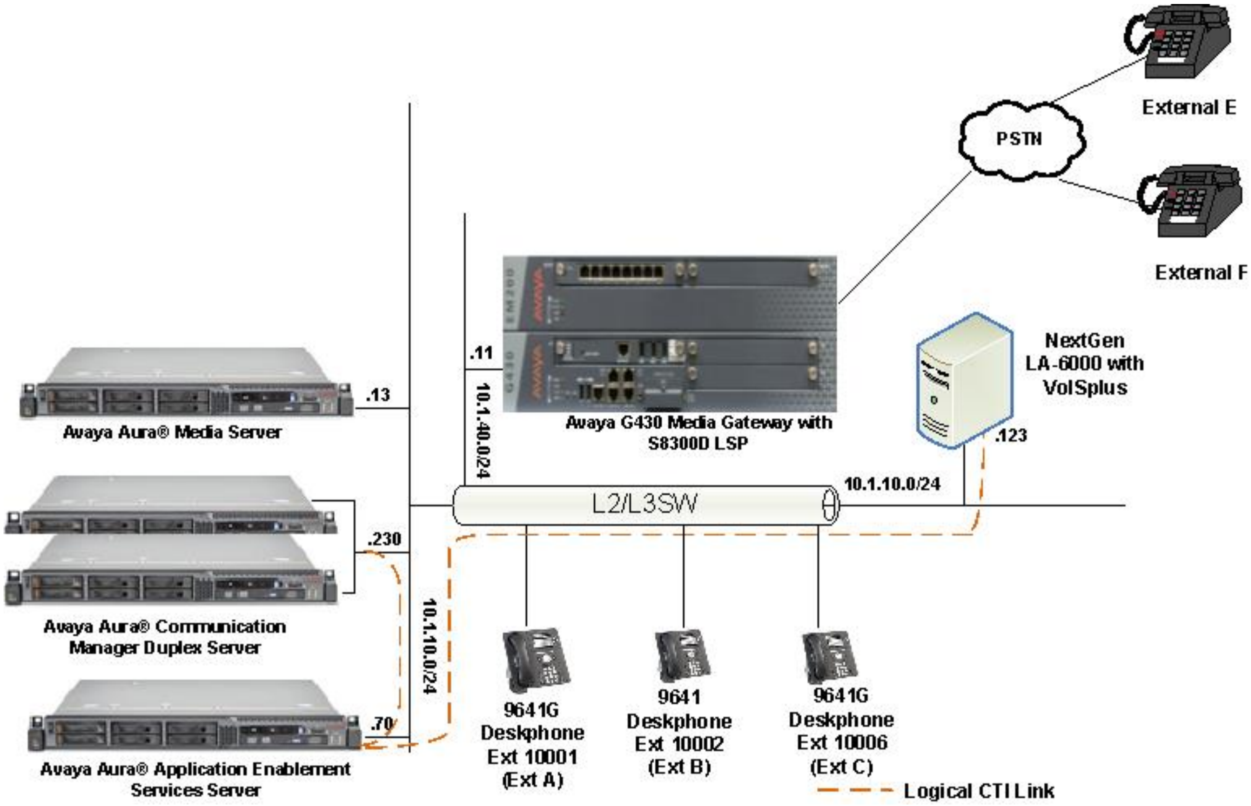


**Figure 1: Test Configuration**

# 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) | 7.1.2<br>(R017x.01.0.532.0-24184) |
| Avaya S8300D Server (w/ G430) running<br>Avaya Aura® Communication Manager | 7.1.2<br>(R017x.01.0.532.0-24184) |
| Avaya G430 Media Gateway:<br>MGP | <br>39.5.0 |
| Avaya Aura® Media Server | 7.8.0.333 |
| Avaya Aura® Application Enablement Services | 7.1.2<br>(7.1.2.0.0.3-0) |
| Avaya 9600 Series IP Deskphones:<br>• 9641G (H.323)<br>• 9641 (H.323) | <br>• 6.6506<br>• 6.6506 |
| NextGen Centos Server<br>• AESMGR6K<br>• LA-6000<br>• VoISplus | 7.4.1708<br>• 1.0.9<br>• 2.0-0b<br>• 2.0-0b |

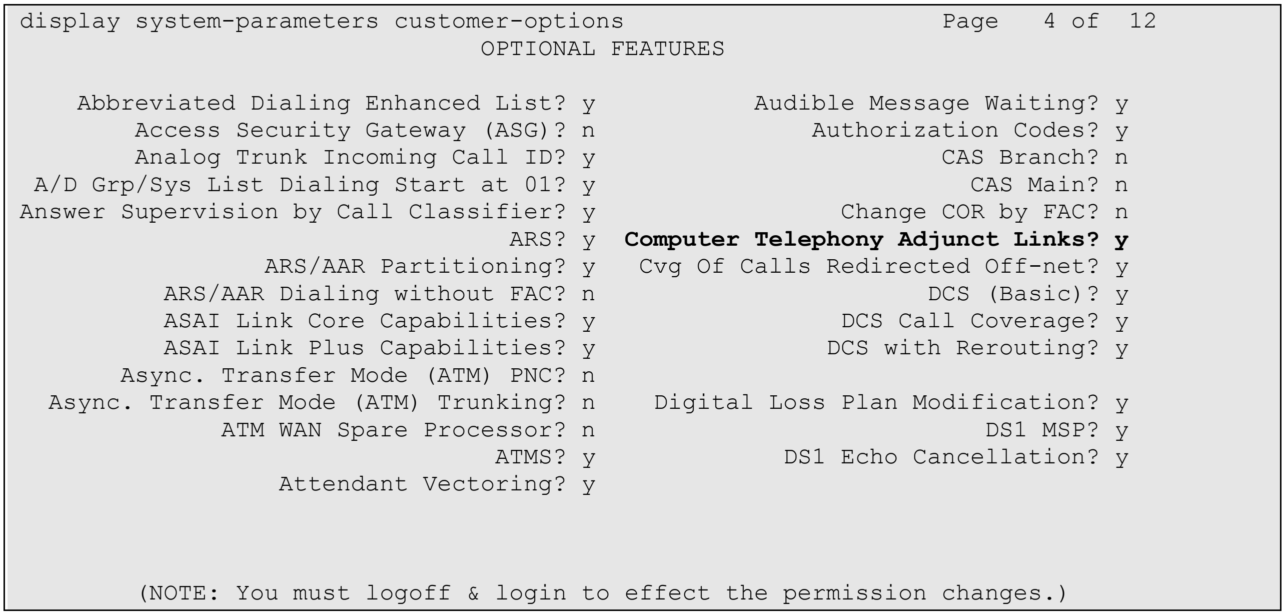
# 5. Configure Avaya Aura® Communication Manager

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

- Verify Communication Manager License
- Administer AES and CTI link
- Administer Agent Stations
- Administer Agent IDs
- 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)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                DCS with Rerouting? y
       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 AES and CTI Link

Enter the **change node-names ip procr** command. In the compliance-tested configuration, note the ip address of the Communication Manager with the node-name **procr** was utilized for connectivity to Avaya AES server.

```
change node-names ip procr                                      Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
procr               10.1.10.230
procr6              ::
```

Enter the **change ip-services** command.  On **Page 1**, configure the **Service Type** field to **AESVCS** and the **Enabled** field to **y**. The **Local Node** field should be set to the **procr**. During the compliance test, the default port was utilized in the **Local Port** field.

```
change ip-services                                              Page   1 of   4

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

On **Page 4**, enter the hostname of the Avaya AES server in the **AE Services Server** field. The server name may be obtained by logging in to the Avaya AES server using Secure Shell (SSH) and running the **uname -a** command. Enter an alphanumeric password in the **Password** field and set the **Enabled** field to y. The same password will be configured on Avaya AES server in **Section 6.3**.

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

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:
      2:      aes7x            xxxxxxxxxxxxxxxx      y
```

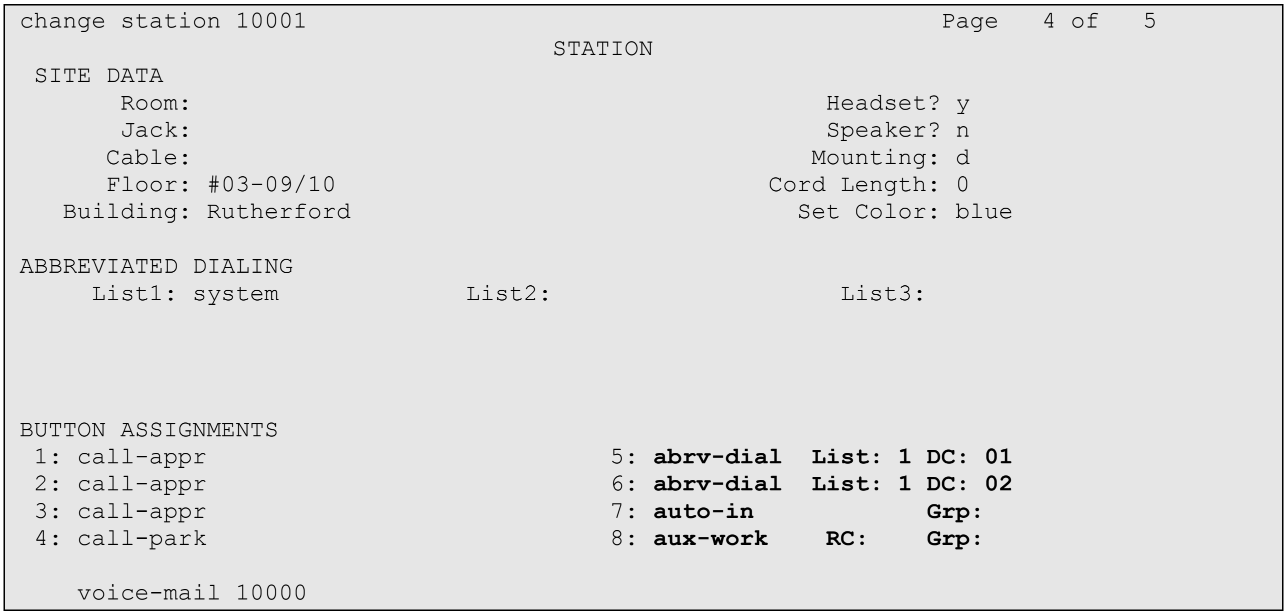
Add a CTI link using the **add cti-link n** command, where **n** is an available CTI link number. Enter an available extension number in the **Extension** field.  Note that the CTI link number and extension number may vary.  Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** 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 - AES7x
```

## 5.3. Administer Agent Stations

Modify each physical station used by the agents to allow the station to perform agent functions. Change the agent station using the **change station n** command, where **n** is the station extension number. Assigned agent login and logout buttons using abbreviated dialing for system, auto-in and aux-work etc., as required for agent stations.

Repeat this section for all agent stations in **Section 3**.

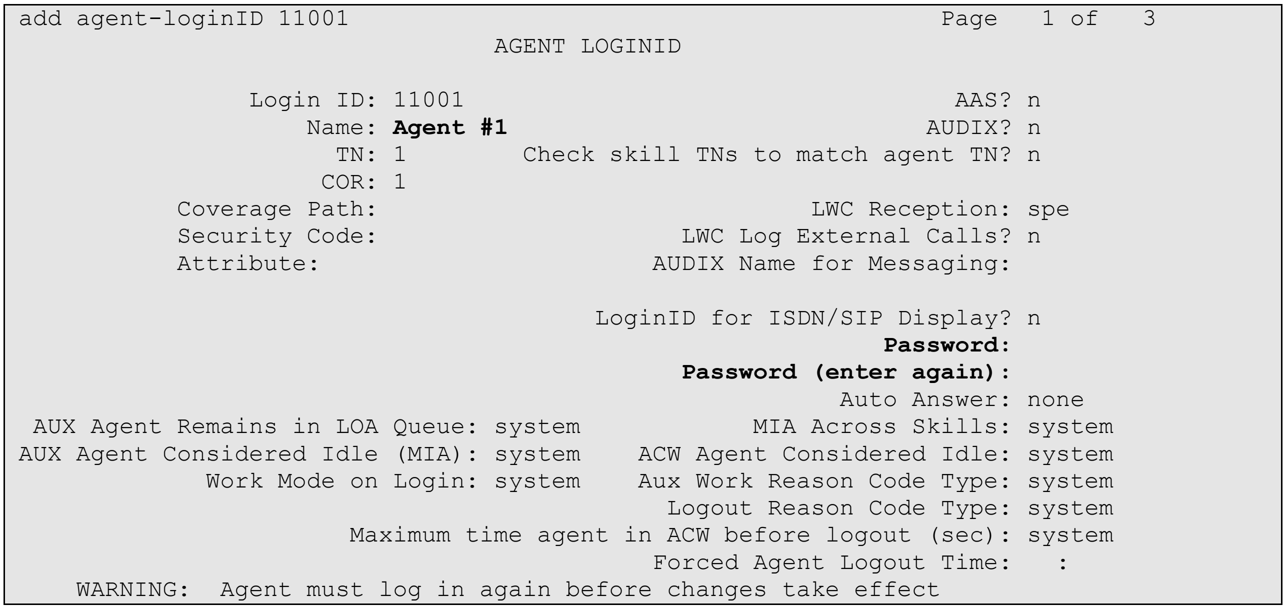


```
change station 10001                                            Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                            Headset? y
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor: #03-09/10                              Cord Length: 0
   Building: Rutherford                               Set Color: blue

ABBREVIATED DIALING
     List1: system             List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                            5: abrv-dial  List: 1 DC: 01
 2: call-appr                            6: abrv-dial  List: 1 DC: 02
 3: call-appr                            7: auto-in            Grp:
 4: call-park                            8: aux-work    RC:    Grp:

    voice-mail 10000
```

## 5.4. Administer Agent IDs

Create agent IDs using the **add agent-loginID next** command. Enter the **Name** and **Password** for the agent ID.

Repeat this section for all agent stations in **Section 3**.



```
add agent-loginID 11001                                         Page   1 of   3
                                 AGENT LOGINID

                Login ID: 11001                                  AAS? n
                    Name: Agent #1                             AUDIX? n
                      TN: 1        Check skill TNs to match agent TN? n
                     COR: 1
           Coverage Path:                              LWC Reception: spe
           Security Code:                     LWC Log External Calls? n
           Attribute:                       AUDIX Name for Messaging:

                                        LoginID for ISDN/SIP Display? n
                                                            Password:
                                              Password (enter again):
                                                         Auto Answer: none
 AUX Agent Remains in LOA Queue: system            MIA Across Skills: system
AUX Agent Considered Idle (MIA): system    ACW Agent Considered Idle: system
             Work Mode on Login: system    Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                            Forced Agent Logout Time:   :
    WARNING:  Agent must log in again before changes take effect
```

## 5.5. 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
```

## 5.6. 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: none
 2:
 3:
 4:
 5:
```

# 6. Configure Avaya Aura® Application Enablement Services

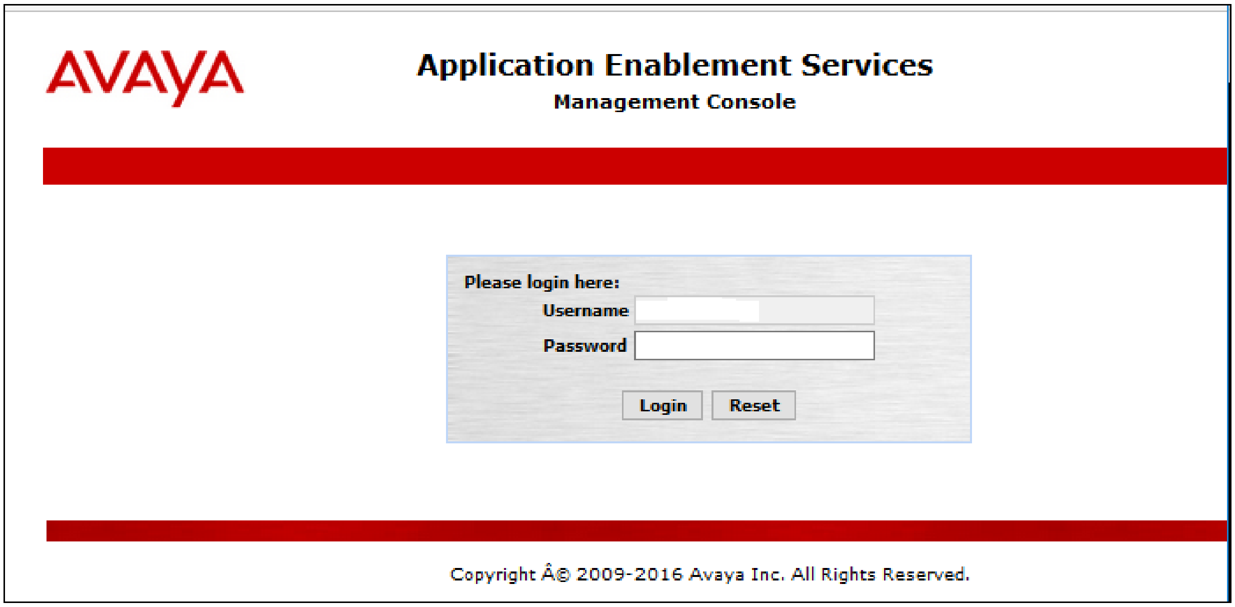
This section provides the procedures for configuring AES. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer Switch Connection
- Administer TSAPI link
- Administer H.323 gatekeeper
- 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

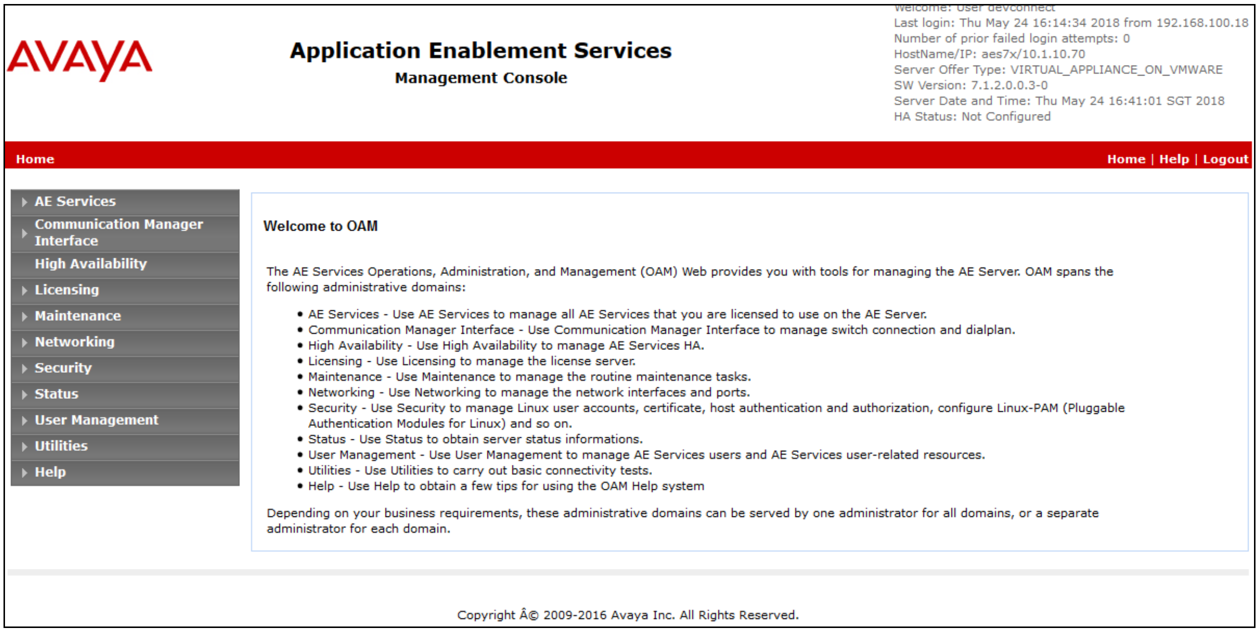
Access the OAM web-based interface by using the URL “https://ip-address” in an internet browser window, where “ip-address” is the ip address of the AES server.

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



AVAYA
Application Enablement Services
Management Console
Please login here:
Username
Password
Login
Reset
Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

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



Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 16:41:01 SGT 2018
HA Status: Not Configured

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:

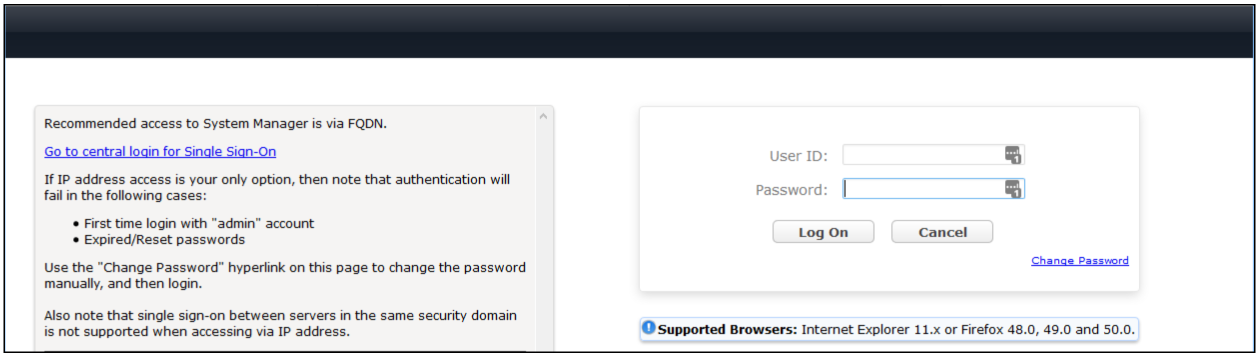
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - 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.

Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

## 6.2. Verify License

Select **Licensing → WebLM Server Access** from the left pane of the home screen and note the **WebLM Server Address**. In this setup, it is the System Manager which host the WebLM server. Access the System Manager web-based interface by using the URL “https://ip-address/SMGR” in an internet browser window, where “ip-address” is the ip address of the System Manager. Log in with the appropriate credentials.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

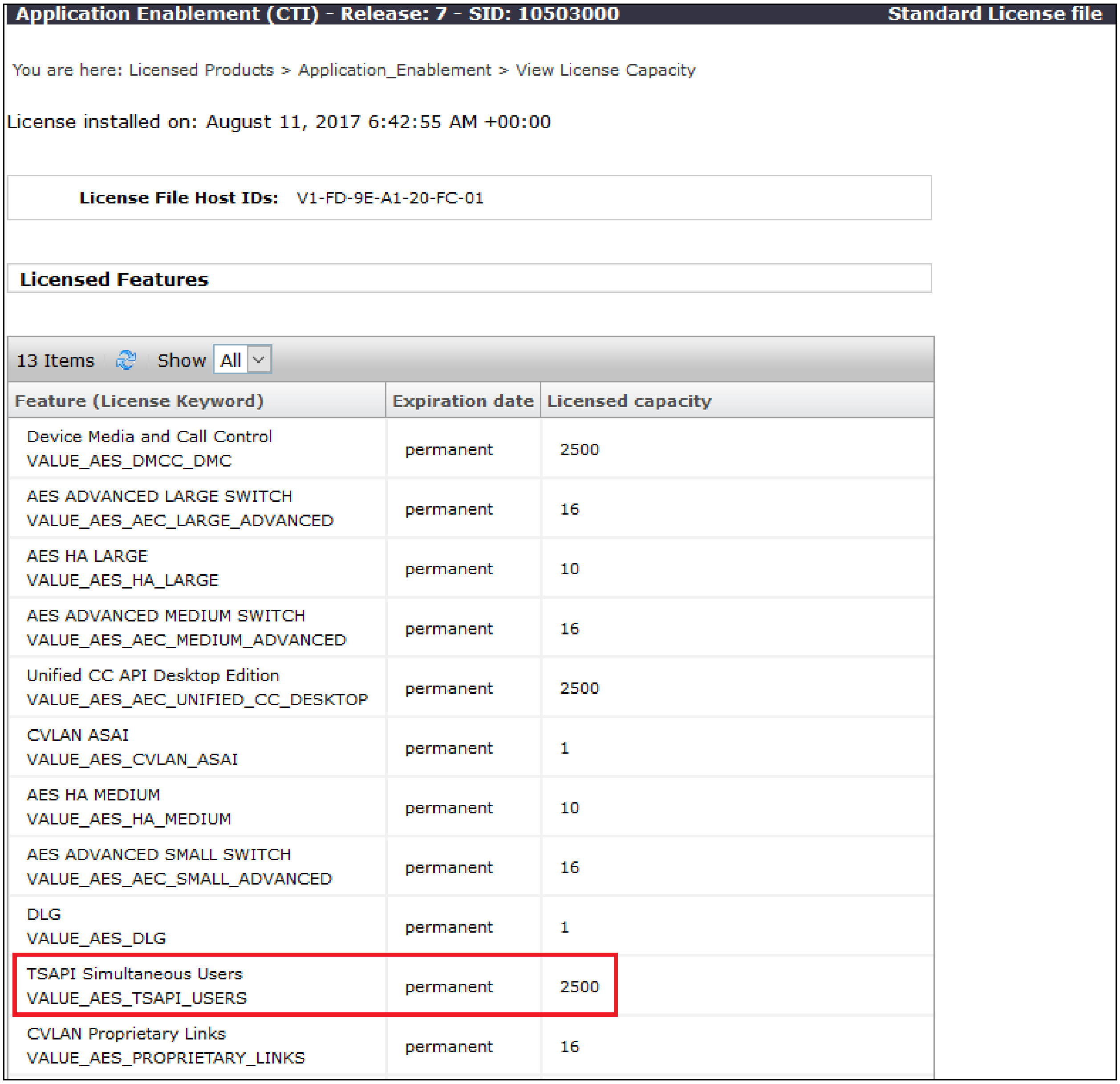
Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

**Supported Browsers:** Internet Explorer 11.x or Firefox 48.0, 49.0 and 50.0.

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: 7 - SID: 10503000 Standard License file

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

License installed on: August 11, 2017 6:42:55 AM +00:00

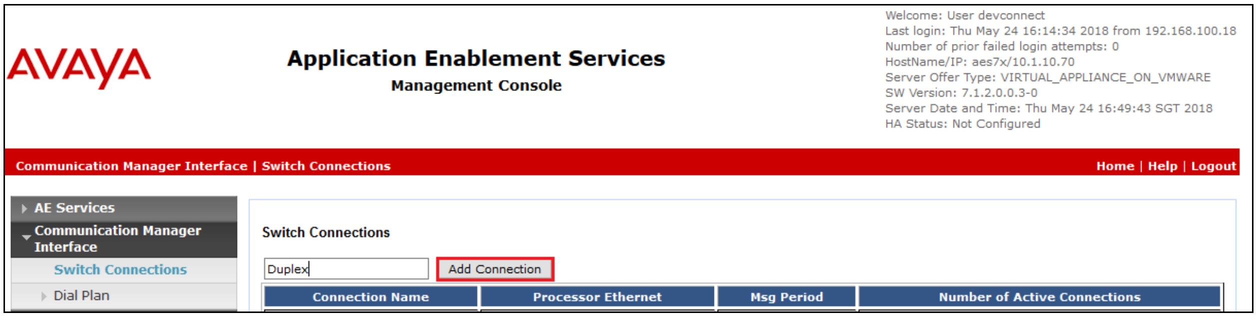
**License File Host IDs:** V1-FD-9E-A1-20-FC-01

**Licensed Features**

| Feature (License Keyword) | Expiration date | Licensed capacity |
|---|---|---|
| Device Media and Call Control<br>VALUE_AES_DMCC_DMC | permanent | 2500 |
| AES ADVANCED LARGE SWITCH<br>VALUE_AES_AEC_LARGE_ADVANCED | permanent | 16 |
| AES HA LARGE<br>VALUE_AES_HA_LARGE | permanent | 10 |
| AES ADVANCED MEDIUM SWITCH<br>VALUE_AES_AEC_MEDIUM_ADVANCED | permanent | 16 |
| Unified CC API Desktop Edition<br>VALUE_AES_AEC_UNIFIED_CC_DESKTOP | permanent | 2500 |
| CVLAN ASAI<br>VALUE_AES_CVLAN_ASAI | permanent | 1 |
| AES HA MEDIUM<br>VALUE_AES_HA_MEDIUM | permanent | 10 |
| AES ADVANCED SMALL SWITCH<br>VALUE_AES_AEC_SMALL_ADVANCED | permanent | 16 |
| DLG<br>VALUE_AES_DLG | permanent | 1 |
| TSAPI Simultaneous Users<br>VALUE_AES_TSAPI_USERS | permanent | 2500 |
| CVLAN Proprietary Links<br>VALUE_AES_PROPRIETARY_LINKS | permanent | 16 |

## 6.3. Administer Switch Connection

From the Home menu of AES, select **Communication Manager Interface → Switch Connections**. Enter a descriptive name for the switch connection and click **Add Connection**. In this configuration, **Duplex** is used.



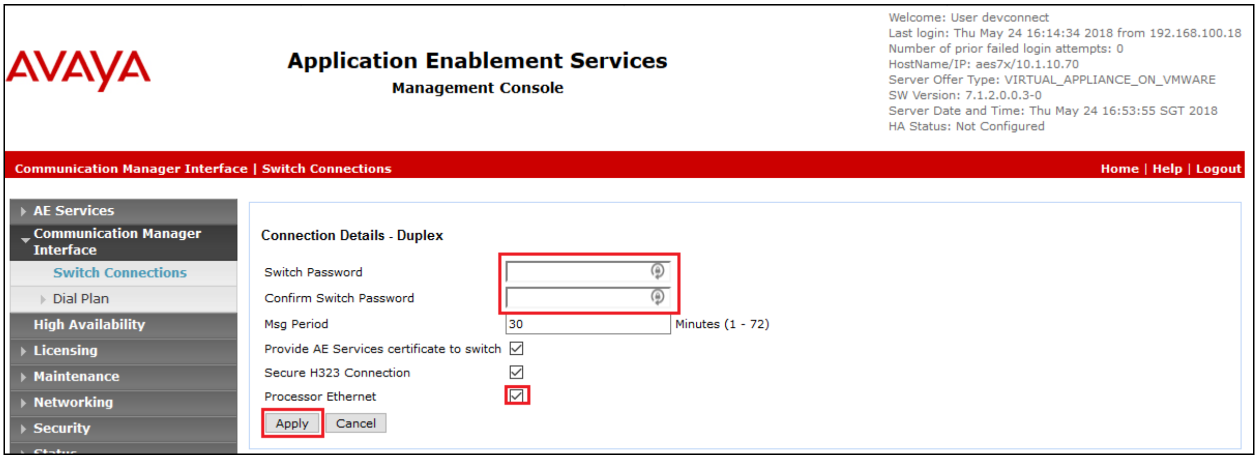
AVAYA
Application Enablement Services
Management Console
Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Add Connection
Connection Name
Processor Ethernet
Msg Period
Number of Active Connections

Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 16:49:43 SGT 2018
HA Status: Not Configured

Switch Connections

Duplex

The **Connection Details – Duplex** screen is displayed. For the **Switch Password** and **Confirm Switch Password** fields, enter the password that was administered in Communication Manager using the IP Services form in **Section 5.2**. Here we are using the **Processor Ethernet** as well for connection and the field needs to be checked. Click on **Apply** to affect changes.

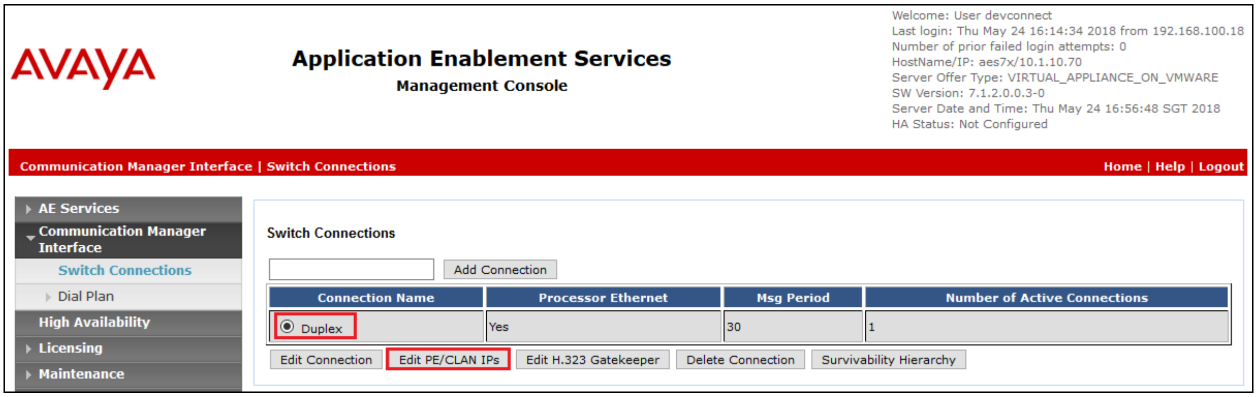


Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 16:53:55 SGT 2018
HA Status: Not Configured

Connection Details - Duplex

| | |
|---|---|
| Switch Password | |
| Confirm Switch Password | |
| Msg Period | 30 Minutes (1 - 72) |
| Provide AE Services certificate to switch | ☑ |
| Secure H323 Connection | ☑ |
| Processor Ethernet | ☑ |

The Switch Connections screen is displayed. Select the newly added switch connection name and click **Edit PE/CLAN IPs**.



Application Enablement Services
Management Console

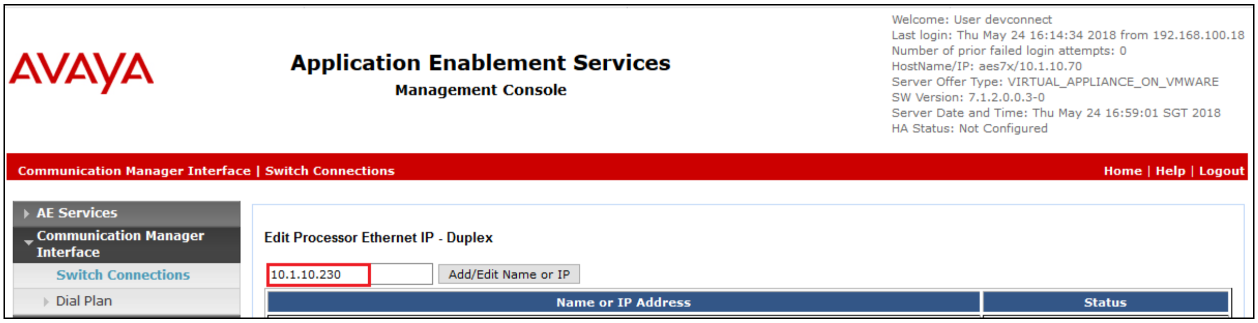
Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 16:56:48 SGT 2018
HA Status: Not Configured

Communication Manager Interface | Switch Connections

Switch Connections

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

On the **Edit Processor Ethernet IP – Duplex** screen, enter the host name or IP address of the PE/C-LAN used for AES connection. In this case, **10.1.10.230** is used, which corresponds to the **procr** address of the Communication Manager. Click **Add/Edit Name or IP**



Application Enablement Services
Management Console

Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 16:59:01 SGT 2018
HA Status: Not Configured

Communication Manager Interface | Switch Connections

Edit Processor Ethernet IP - Duplex

10.1.10.230

| Name or IP Address | Status |
|---|---|

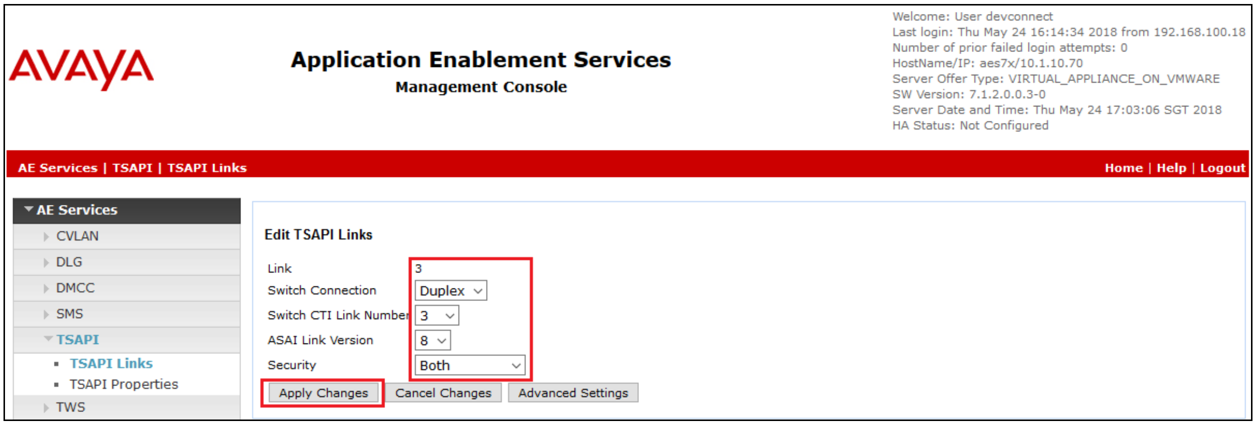
## 6.4. Administer TSAPI Link

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 5.2**.
- **ASAI Link Version:** Set to **8** for the latest version.
- **Security:** Select **Both** to allow for encrypted or unencrypted link.

Click **Apply Changes** to affect changes.



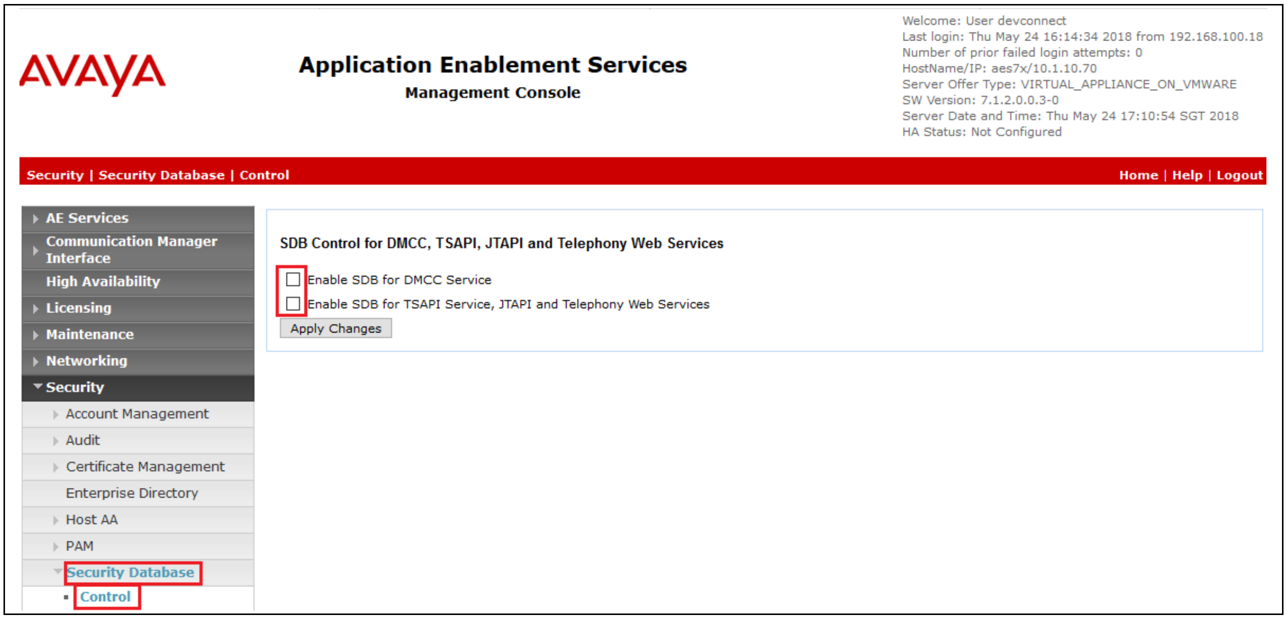
Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 17:03:06 SGT 2018
HA Status: Not Configured

Edit TSAPI Links

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

## 6.5. 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. Clear the **Enable SDB for DMCC Service** and **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** if they are checked, and click **Apply Changes**.



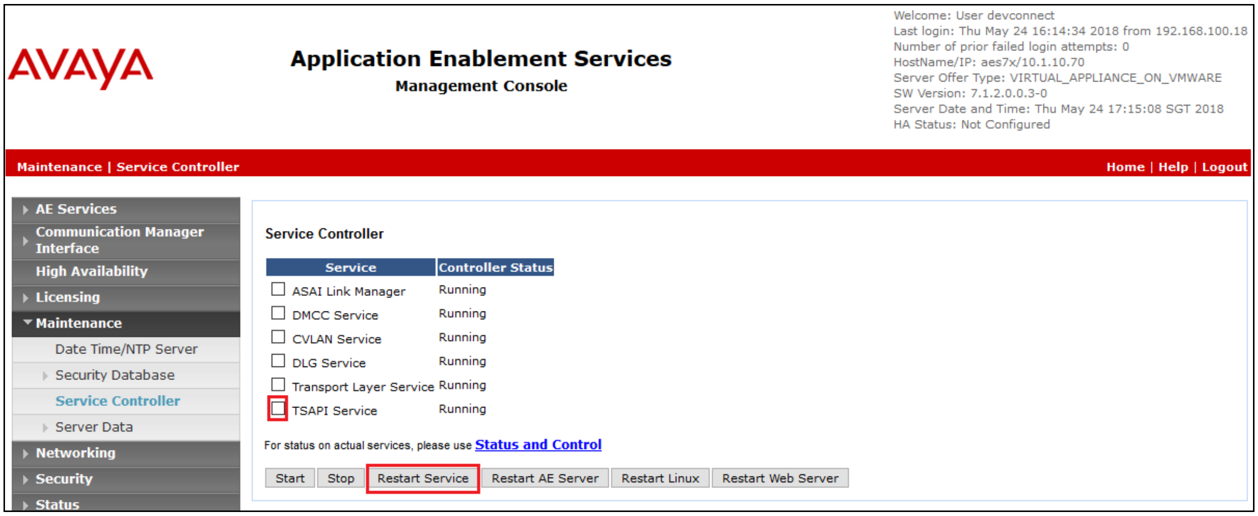
Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 17:10:54 SGT 2018
HA Status: Not Configured

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

## 6.6. 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**.



Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 17:15:08 SGT 2018
HA Status: Not Configured

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 |

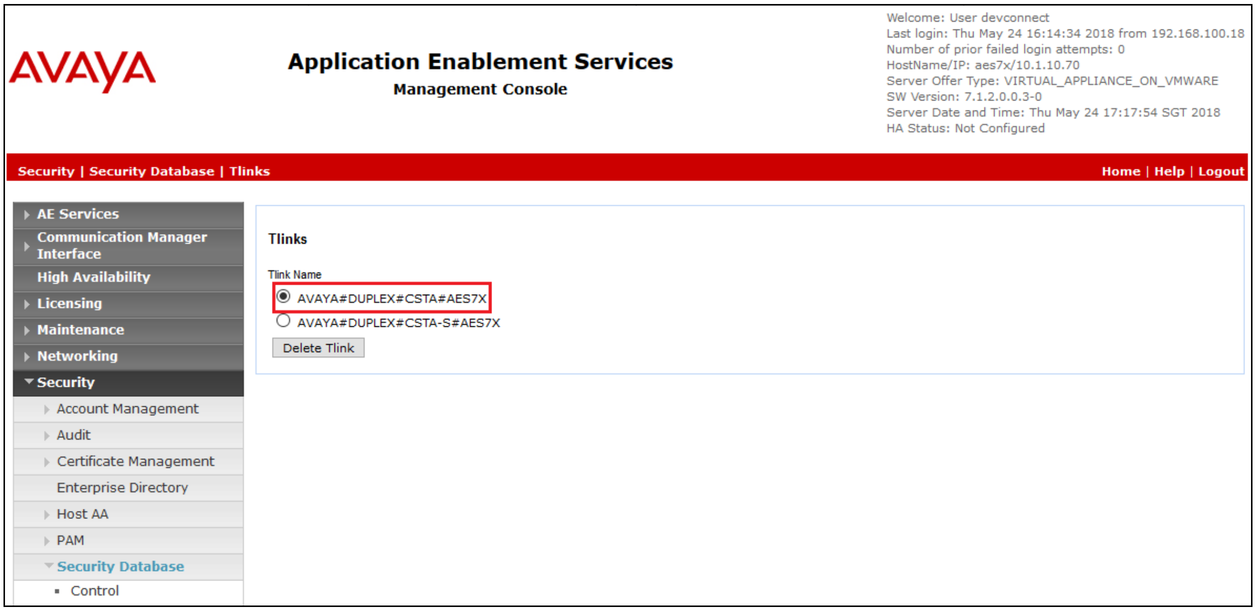
For status on actual services, please use Status and Control

## 6.7. 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 A**VAYA#DUPLEX#CSTA#AES7X,** which is automatically assigned by the Avaya AES server. Note the use of the switch connection **Duplex** of **Section 5.3** as part of the Tlink name.



Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 17:17:54 SGT 2018
HA Status: Not Configured

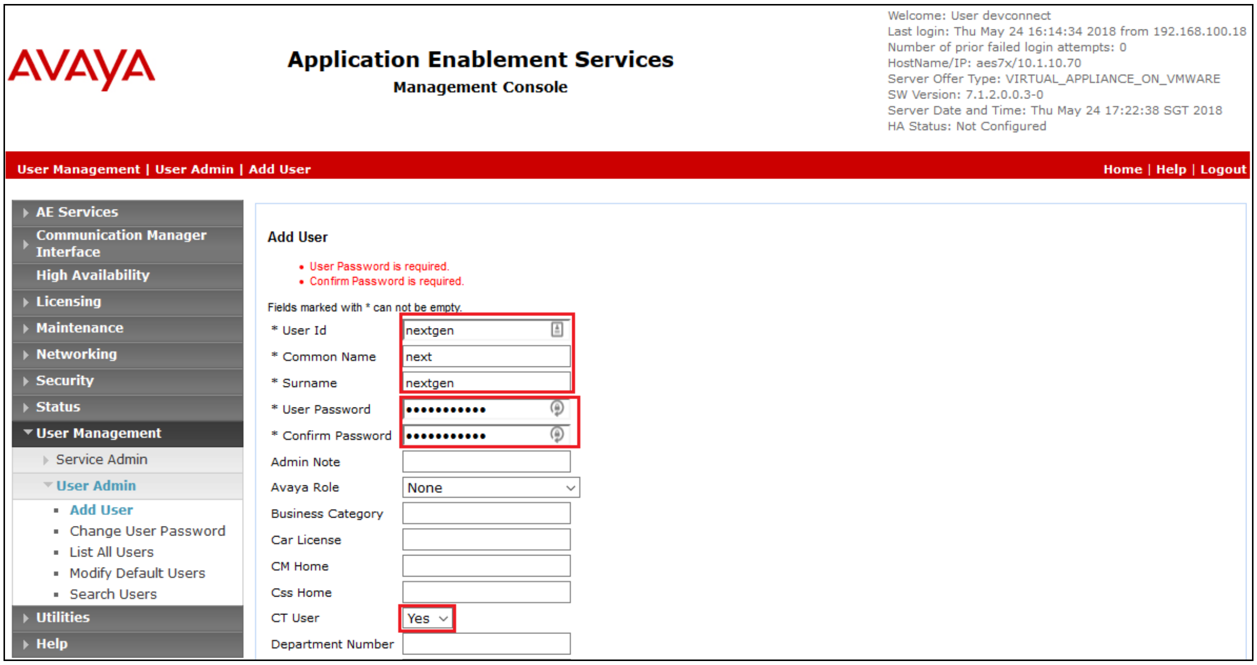
Tlinks

Tlink Name
● AVAYA#DUPLEX#CSTA#AES7X
○ AVAYA#DUPLEX#CSTA-S#AES7X

## 6.8. 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).



Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 17:22:38 SGT 2018
HA Status: Not Configured

Add User

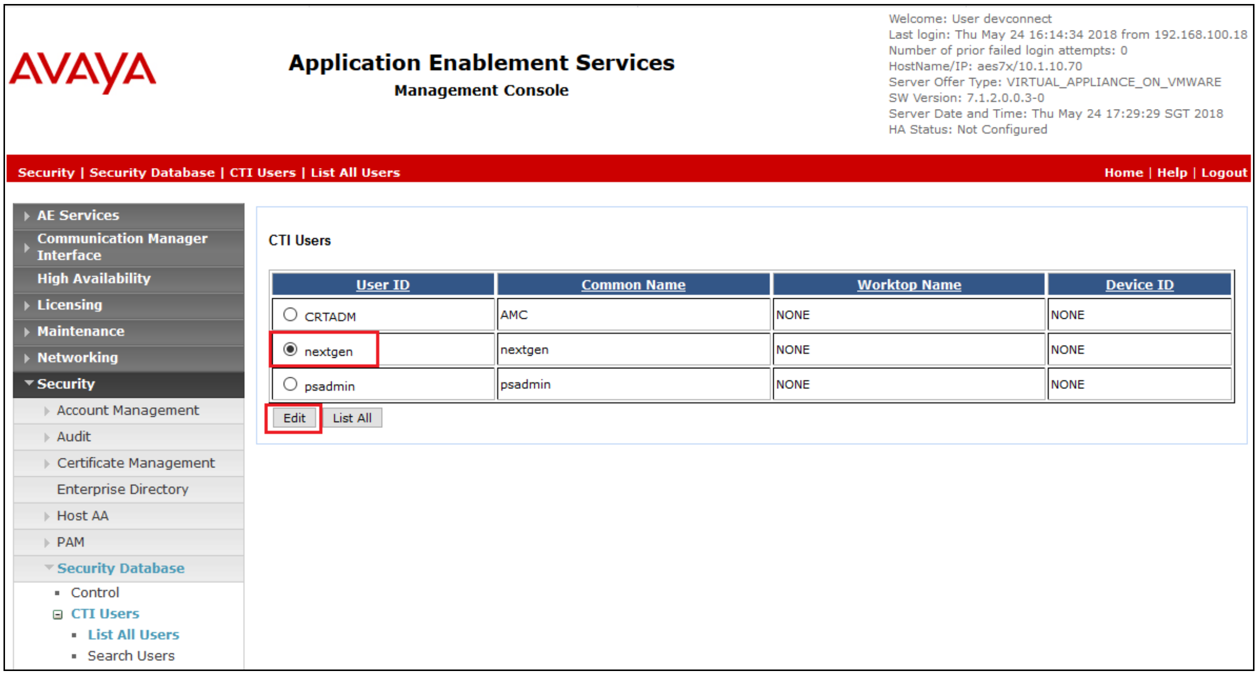
- User Password is required.
- Confirm Password is required.

Fields marked with * can not be empty.

| | |
|---|---|
| * User Id | nextgen |
| * Common Name | next |
| * Surname | nextgen |
| * User Password | ••••••••••• |
| * Confirm Password | ••••••••••• |
| Admin Note | |
| Avaya Role | None |
| Business Category | |
| Car License | |
| CM Home | |
| Css Home | |
| CT User | Yes |
| Department Number | |

## 6.9. Administer CTI User Permissions

Select **Security → Security Database → CTI Users → List All Users** from the AES Management Console Home menu. Select the User ID created in **Section 5.9** and click **Edit**.

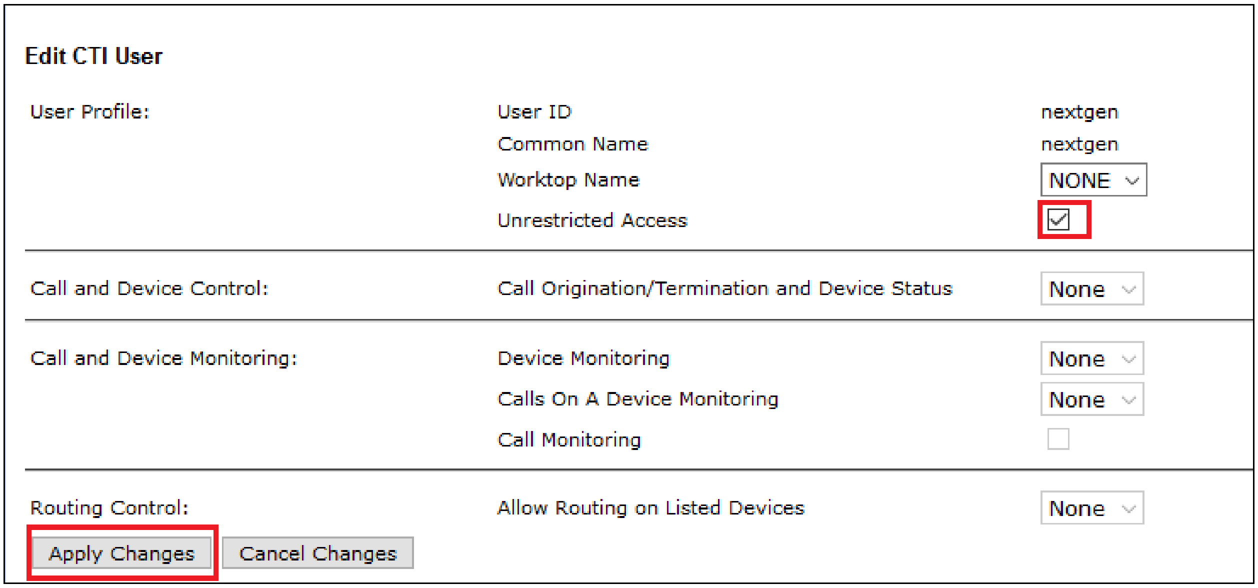


Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 17:29:29 SGT 2018
HA Status: Not Configured

CTI Users

| User ID | Common Name | Worktop Name | Device ID |
|---|---|---|---|
| ○ CRTADM | AMC | NONE | NONE |
| ● nextgen | nextgen | NONE | NONE |
| ○ psadmin | psadmin | NONE | NONE |

Check the **Unrestricted Access** box. Click **Apply Changes**.



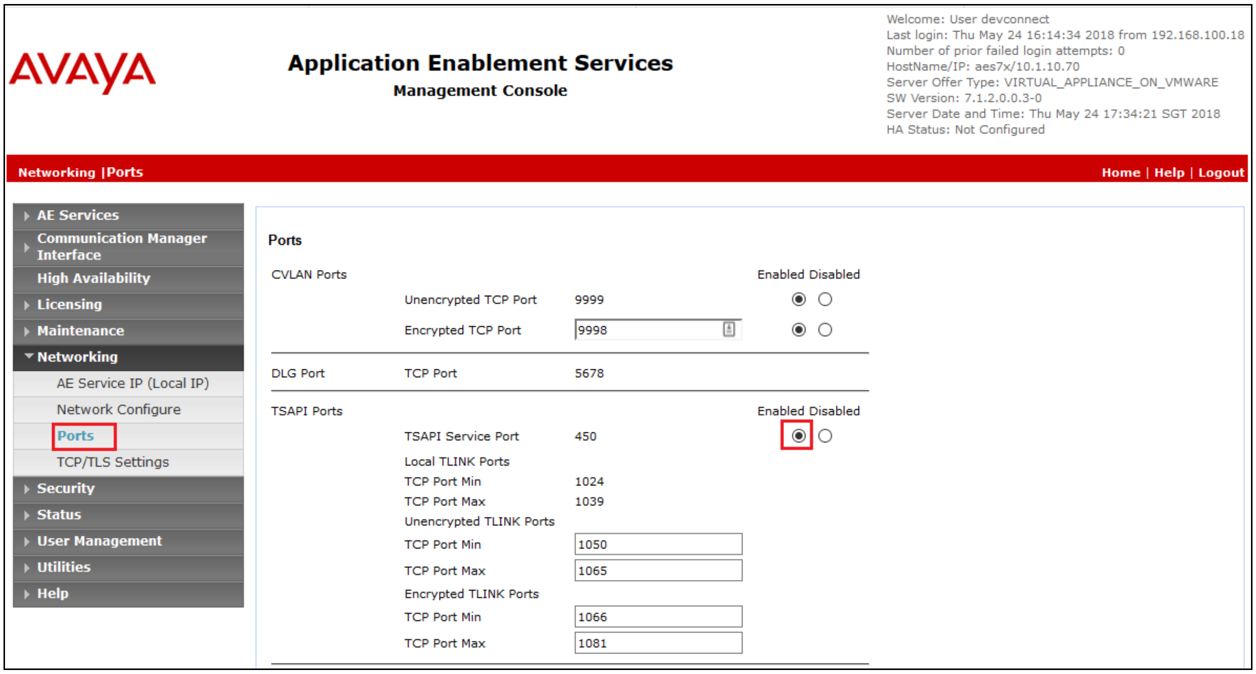
Edit CTI User

| | | |
|---|---|---|
| User Profile: | User ID | nextgen |
| | Common Name | nextgen |
| | 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 |

## 6.10. 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).



Welcome: User devconnect
Last login: Thu May 24 16:14:34 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 17:34:21 SGT 2018
HA Status: Not Configured

**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 | | |

# 7. Configure NextGen LA-6000

This section provides the procedures for configuring NextGen LA-6000. The AESMGR6K module on the LA-6000 server communicates with AES from the administrative ethernet port and the other ethernet port connects to the monitoring port of data switch, which mirror ports of Media Processors. Ensure that the monitoring ethernet ports are in promiscuous mode and all traffic is allowed on virtualized host server port. 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 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 6.7**. Verify the **LinkUserID** and **LinkPassword** is set as configured in **Section 6.8**. Check also that **AvayaEnable** is set to “1”.

```
LA6IP1 = "10.1.10.123"
AesServerName = "AVAYA#DUPLEX#CSTA#AES7X"
LinkUserID    = "nextgen"
LinkPassword  = "nextgen6000"
HoldSw = "1"    //* 1:Stop Recording while call-holding 0:Continue recording while
call-holding / Default:0
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 a board on the Avaya G650 Media Gateway or the AAMS or the Media Gateway Processor (MGP) of Avaya G430 and G450 Media Gateway. In this compliance testing, only the ip address of AAMS is added where RTP stream of transcoded.

```
F0_Port::31060
V0_VID::0
Operation::0
@recorder
Idx_Text1::0
Idx_Text2::0
Idx_Text3::0
Idx_Text4::0
PetName::la6k
Divsz_Type::1
BKUP_Retention::-1
NorthGWList::10.1.10.13
PowerRestart::1
BKUP_Arrange_Time::02:00
BlackNumberList::
TransAlarm::0
Idx_Number1::0
Idx_Number2::0
Idx_Agent::0
Idx_DTMF::0
Divsz_Minutes::60
Idx_Extension::0
SouthGWList::
@ipcap0
NICName::ens192
F0_Netadder::0.0.0.0
F0_Netmask::0
F0_Trans::2
F0_Network::1
V0_VID::0
Operation::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.

## 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**.**

```
10001,10.1.10.169
10002,10.1.10.180
10006,10.1.10.153
```

## 7.4. Restart Services

On the console, navigate to the **../NXS/bin** directory. Execute the following nxs.sh command 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.

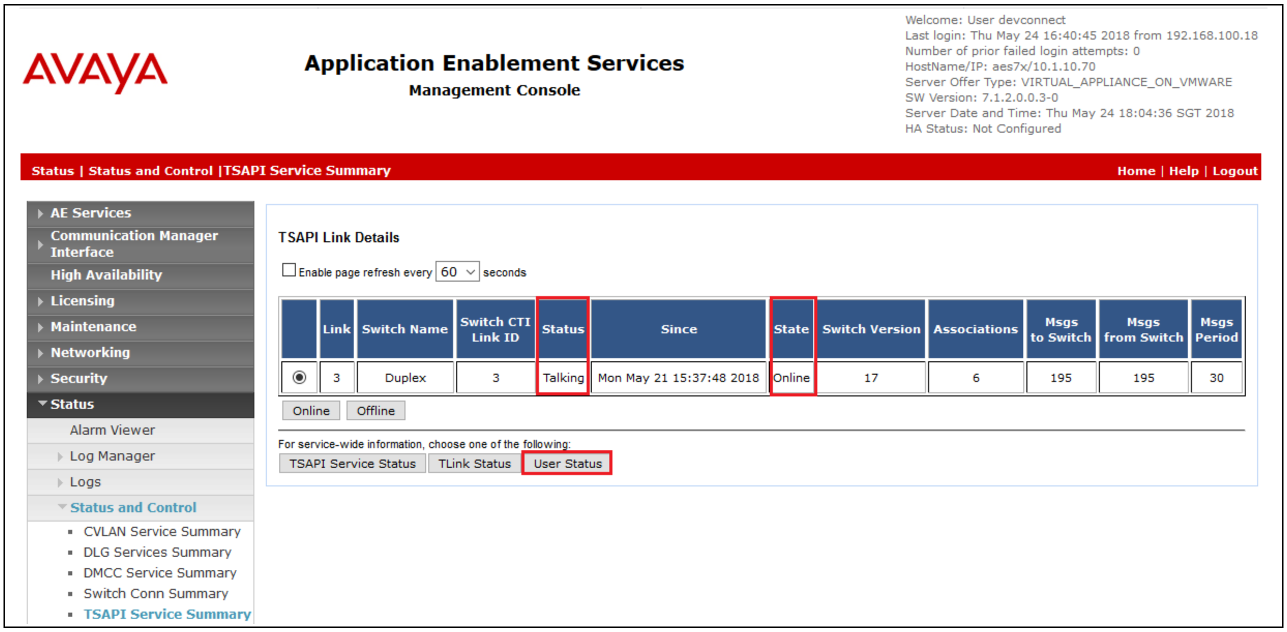
## 8.1. Verify Avaya Aura® Communication Manager

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 5.3**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

3      8        no     aes7x            established   194       194
```

## 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 with the nextgen user name from **Section 6.9**, and that the **State Devices** column shows **Online**. Click on the **User Status** below.



Welcome: User devconnect
Last login: Thu May 24 16:40:45 2018 from 192.168.100.18
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.1.2.0.0.3-0
Server Date and Time: Thu May 24 18:04:36 SGT 2018
HA Status: Not Configured

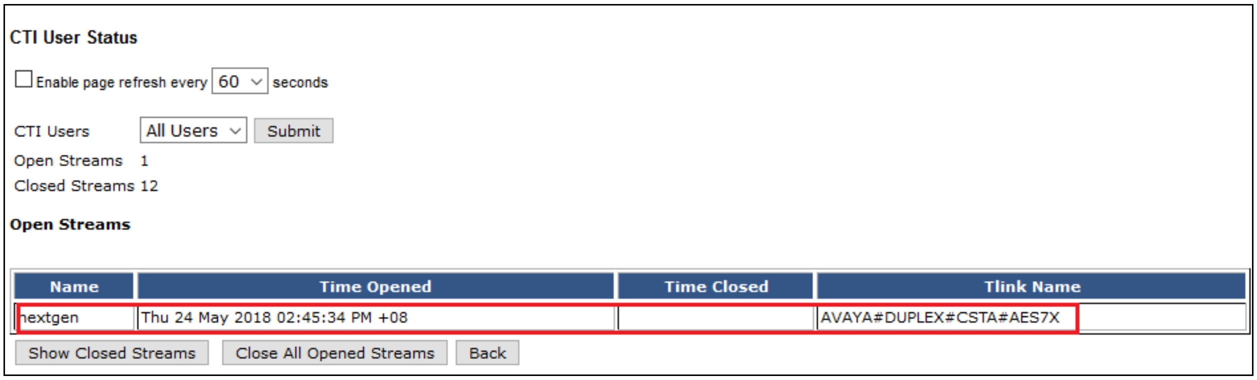
TSAPI Link Details

☐ 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ◉ | 3 | Duplex | 3 | Talking | Mon May 21 15:37:48 2018 | Online | 17 | 6 | 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 5.13**.



**CTI User Status**

☐ Enable page refresh every 60 seconds

CTI Users All Users Submit

Open Streams 1

Closed Streams 12

**Open Streams**

| Name | Time Opened | Time Closed | Tlink Name |
|---|---|---|---|
| nextgen | Thu 24 May 2018 02:45:34 PM +08 | | AVAYA#DUPLEX#CSTA#AES7X |

## 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.

```
2018/05/24 17:53:16.031079
2018/05/24 17:53:16.031144 *** Health Check OK! ***
2018/05/24 17:53:26.026613
2018/05/24 17:53:26.026676 *** Health Check OK! ***
2018/05/24 17:53:36.041795
2018/05/24 17:53:36.041862 *** Health Check OK! ***
2018/05/24 17:53:46.006140
2018/05/24 17:53:46.006208 *** Health Check OK! ***
2018/05/24 17:53:56.028176
2018/05/24 17:53:56.028240 *** Health Check OK! ***
```

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

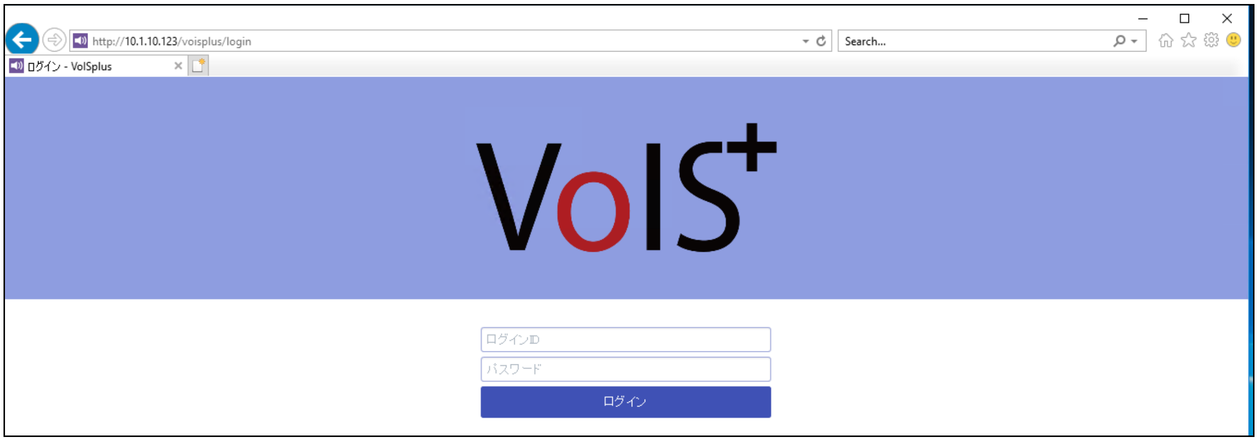
```
2018/05/18 09:16:04.054393 [CSTA_DELIVERED]
2018/05/18 09:16:04.054426 Monitor Extension: 10001
2018/05/18 09:16:04.054457 Call Status: CS_ALERTING
2018/05/18 09:16:04.054485 <<CallInfo>>
2018/05/18 09:16:04.054514 CallID: 397
2018/05/18 09:16:04.054544      CallingDevice: 10006
2018/05/18 09:16:04.054573      CalledDevice: 10001
2018/05/18 09:16:04.054602      UCID: 00001003971526606160
2018/05/18 09:16:04.054632      TrunkGroup:
2018/05/18 09:16:04.054661      TrunkMember:
2018/05/18 09:16:04.054689      Direction: 2
2018/05/18 09:16:04.054718      CallingExtensionNo:
2018/05/18 09:16:04.054747      CalledExtensionNo: 10001
2018/05/18 09:16:04.054776 calls count: 0
2018/05/18 09:16:04.054905 [Incoming in]-10001 : Dest:10006 Self:10001
TerminalIP:10.1.10.169
2018/05/18 09:16:06.000425
2018/05/18 09:16:06.000485 *** Health Check OK! ***
2018/05/18 09:16:07.801720
2018/05/18 09:16:07.801790 [CSTA_CONNECTION_CLEARED]
2018/05/18 09:16:07.801823 Monitor Extension: 10001
```

```
2018/05/18 09:16:07.801854 Call Status: CS_ALERTING
2018/05/18 09:16:07.801922 <<CallInfo>>
2018/05/18 09:16:07.801959 CallID: 397
2018/05/18 09:16:07.801990      CallingDevice: 10006
2018/05/18 09:16:07.802019      CalledDevice: 10001
2018/05/18 09:16:07.802048      UCID: 00001003971526606160
2018/05/18 09:16:07.802078      TrunkGroup:
2018/05/18 09:16:07.802107      TrunkMember:
2018/05/18 09:16:07.802135      Direction: 2
2018/05/18 09:16:07.802164      CallingExtensionNo:
2018/05/18 09:16:07.802192      CalledExtensionNo: 10001
2018/05/18 09:16:07.802221 calls count: 0
2018/05/18 09:16:07.844906
2018/05/18 09:16:07.844952 [CSTA_CONNECTION_CLEARED]
2018/05/18 09:16:07.844984 Monitor Extension: 10001
2018/05/18 09:16:07.845014 Call Status: CS_NULL
2018/05/18 09:16:07.845043 <<CallInfo>>
2018/05/18 09:16:07.845073 CallID: 397
2018/05/18 09:16:07.845102      CallingDevice: 10006
2018/05/18 09:16:07.845131      CalledDevice: 10001
2018/05/18 09:16:07.845159      UCID: 00001003971526606160
2018/05/18 09:16:07.845189      TrunkGroup:
2018/05/18 09:16:07.845218      TrunkMember:
2018/05/18 09:16:07.845246      Direction: 2
2018/05/18 09:16:07.845275      CallingExtensionNo:
2018/05/18 09:16:07.845332 calls count: 0
2018/05/18 09:16:16.014822
2018/05/18 09:16:16.014906 *** Health Check OK! ***
2018/05/18 09:16:17.438397
2018/05/18 09:16:17.438464 [CSTA_DELIVERED]
2018/05/18 09:16:17.438497 Monitor Extension: 10001
2018/05/18 09:16:17.438527 Call Status: CS_ALERTING
2018/05/18 09:16:17.438556 <<CallInfo>>
2018/05/18 09:16:17.438585 CallID: 398
2018/05/18 09:16:17.438615      CallingDevice: 10006
2018/05/18 09:16:17.438645      CalledDevice: 10001
2018/05/18 09:16:17.438674      UCID: 00001003981526606176
2018/05/18 09:16:17.438704      TrunkGroup:
2018/05/18 09:16:17.438732      TrunkMember:
2018/05/18 09:16:17.438761      Direction: 2
2018/05/18 09:16:17.438790      CallingExtensionNo:
2018/05/18 09:16:17.438819      CalledExtensionNo: 10001
2018/05/18 09:16:17.438849 calls count: 0
2018/05/18 09:16:17.438982 [Incoming in]-10001 : Dest:10006 Self:10001
TerminalIP:10.1.10.169
2018/05/18 09:16:21.331049
2018/05/18 09:16:21.331111 [CSTA_ESTABLISHED]
2018/05/18 09:16:21.331144 Monitor Extension: 10001
2018/05/18 09:16:21.331174 Call Status: CS_CONNECT
2018/05/18 09:16:21.331203 <<CallInfo>>
2018/05/18 09:16:21.331232 CallID: 398
2018/05/18 09:16:21.331262      CallingDevice: 10006
2018/05/18 09:16:21.331291      CalledDevice: 10001
2018/05/18 09:16:21.331321      UCID: 00001003981526606176
2018/05/18 09:16:21.331350      TrunkGroup:
2018/05/18 09:16:21.331379      TrunkMember:
2018/05/18 09:16:21.331407      Direction: 2
2018/05/18 09:16:21.331435      CallingExtensionNo:
2018/05/18 09:16:21.331464      CalledExtensionNo: 10001
2018/05/18 09:16:21.331502 calls count: 1
2018/05/18 09:16:21.333492 [Answer]-10001 : Rec start Dest:10006 Self:10001
TerminalIP:10.1.10.169
```

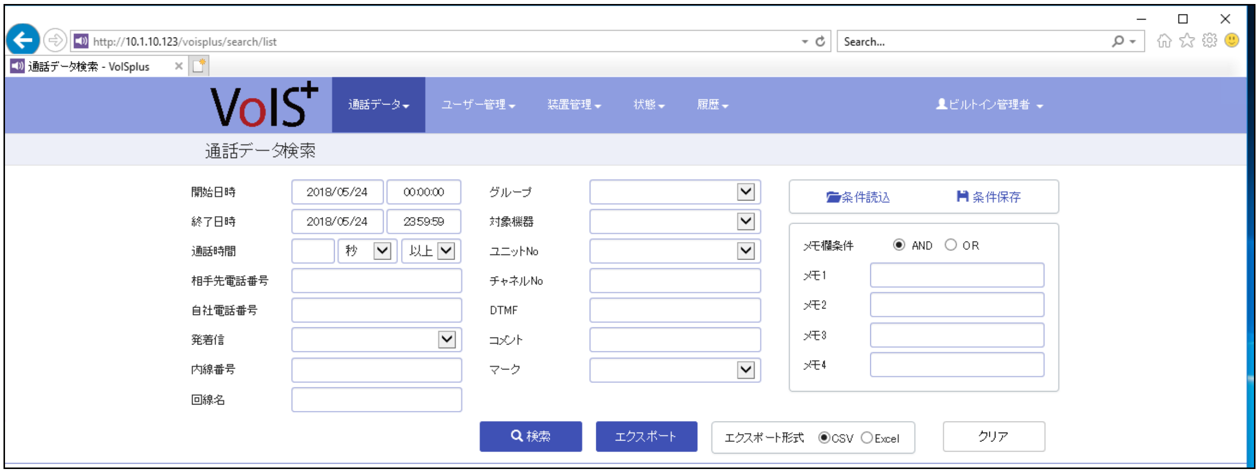
```
2018/05/18 09:16:21.333536 Rec-ID:2
2018/05/18 09:16:21.424385
2018/05/18 09:16:21.424442  QueryDeviceInfo 10001
2018/05/18 09:16:21.424483 AgentID not found : 10001
2018/05/18 09:16:26.035095
2018/05/18 09:16:26.035164 *** Health Check OK! ***
2018/05/18 09:16:33.525265
2018/05/18 09:16:33.525338 [CSTA_CONNECTION_CLEARED]
2018/05/18 09:16:33.525379 Monitor Extension: 10001
2018/05/18 09:16:33.525411 Call Status: CS_NULL
2018/05/18 09:16:33.525454 <<CallInfo>>
2018/05/18 09:16:33.525489 CallID: 398
2018/05/18 09:16:33.525522      CallingDevice: 10006
2018/05/18 09:16:33.525568      CalledDevice: 10001
2018/05/18 09:16:33.525601      UCID: 00001003981526606176
2018/05/18 09:16:33.525642      TrunkGroup:
2018/05/18 09:16:33.525681      TrunkMember:
2018/05/18 09:16:33.525712      Direction: 2
2018/05/18 09:16:33.525753      CallingExtensionNo:
2018/05/18 09:16:33.525791      CalledExtensionNo: 10001
2018/05/18 09:16:33.525822 calls count: 1
2018/05/18 09:16:33.526433 [On Hook]-10001 : Rec stop   TerminalIP:10.1.10.169
2018/05/18 09:16:33.526477 Rec-ID:2
```

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 our test environment, this storage server is residing on the same server as LA-6000.

Log on using appropriate credentials.



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



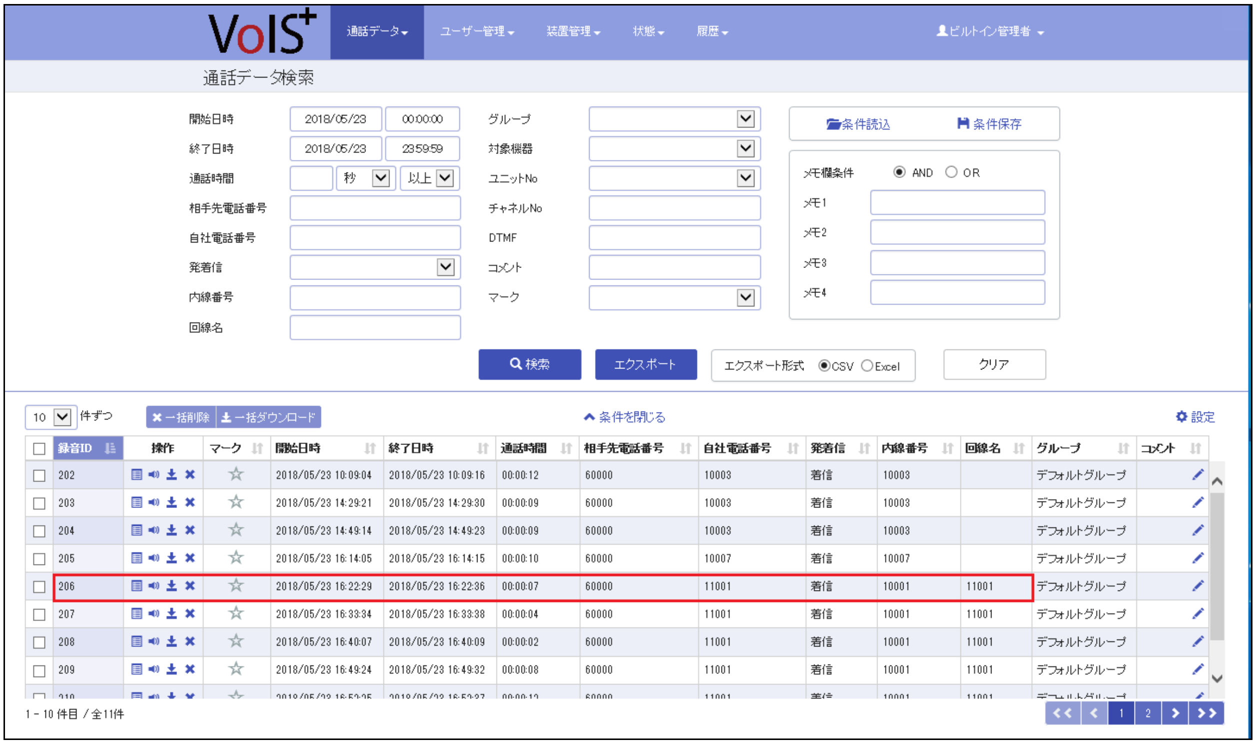
通話データ検索

| | | | |
|---|---|---|---|
| 開始日時 | 2018/05/24 00:00:00 | グループ | |
| 終了日時 | 2018/05/24 23:59:59 | 対象機器 | |
| 通話時間 | 秒 以上 | ユニットNo | |
| 相手先電話番号 | | チャネルNo | |
| 自社電話番号 | | DTMF | |
| 発着信 | | コメント | |
| 内線番号 | | マーク | |
| 回線名 | | | |

メモ欄条件 ● AND ○ OR
メモ1
メモ2
メモ3
メモ4

エクスポート形式 ● CSV ○ Excel

The following call recording was made on the Ext 10001 using Agent ID 11001. Double click on the **speaker** icon.



通話データ検索

| | | | |
|---|---|---|---|
| 開始日時 | 2018/05/23 00:00:00 | グループ | |
| 終了日時 | 2018/05/23 23:59:59 | 対象機器 | |
| 通話時間 | 秒 以上 | ユニットNo | |
| 相手先電話番号 | | チャネルNo | |
| 自社電話番号 | | DTMF | |
| 発着信 | | コメント | |
| 内線番号 | | マーク | |
| 回線名 | | | |

メモ欄条件 ● AND ○ OR
メモ1
メモ2
メモ3
メモ4

エクスポート形式 ● CSV ○ Excel

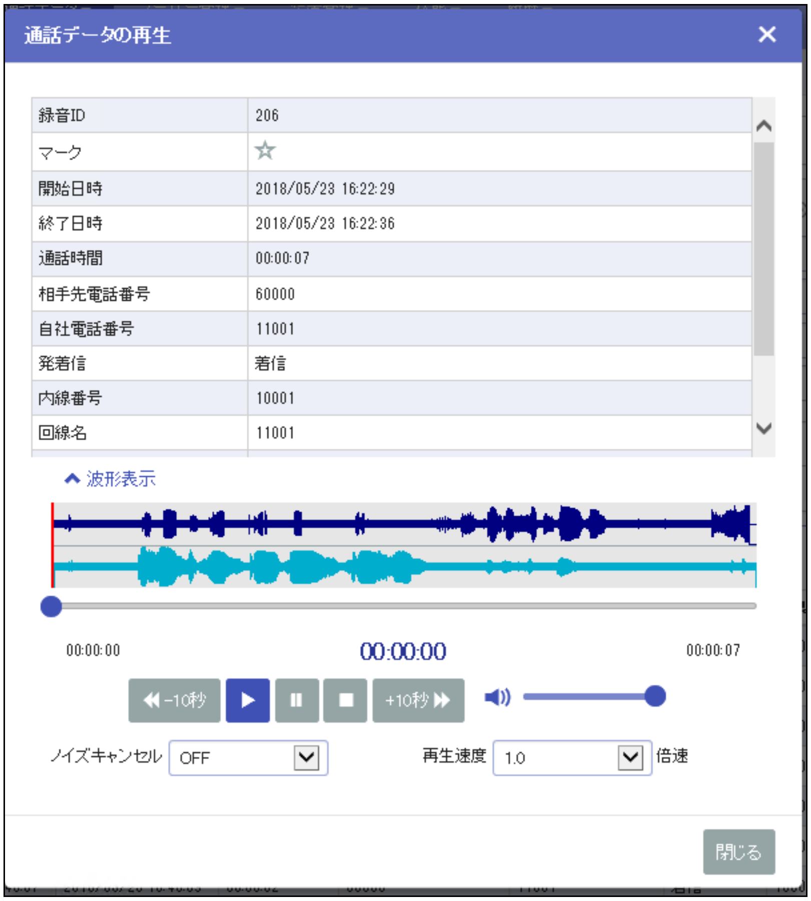
10 件ずつ

| □ | 録音ID | 操作 | マーク | 開始日時 | 終了日時 | 通話時間 | 相手先電話番号 | 自社電話番号 | 発着信 | 内線番号 | 回線名 | グループ | コメント |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 202 | | ☆ | 2018/05/23 10:09:04 | 2018/05/23 10:09:16 | 00:00:12 | 60000 | 10003 | 着信 | 10003 | | デフォルトグループ | |
| □ | 203 | | ☆ | 2018/05/23 14:29:21 | 2018/05/23 14:29:30 | 00:00:09 | 60000 | 10003 | 着信 | 10003 | | デフォルトグループ | |
| □ | 204 | | ☆ | 2018/05/23 14:49:14 | 2018/05/23 14:49:23 | 00:00:09 | 60000 | 10003 | 着信 | 10003 | | デフォルトグループ | |
| □ | 205 | | ☆ | 2018/05/23 16:14:05 | 2018/05/23 16:14:15 | 00:00:10 | 60000 | 10007 | 着信 | 10007 | | デフォルトグループ | |
| □ | 206 | | ☆ | 2018/05/23 16:22:29 | 2018/05/23 16:22:36 | 00:00:07 | 60000 | 11001 | 着信 | 10001 | 11001 | デフォルトグループ | |
| □ | 207 | | ☆ | 2018/05/23 16:33:34 | 2018/05/23 16:33:38 | 00:00:04 | 60000 | 11001 | 着信 | 10001 | 11001 | デフォルトグループ | |
| □ | 208 | | ☆ | 2018/05/23 16:40:07 | 2018/05/23 16:40:09 | 00:00:02 | 60000 | 11001 | 着信 | 10001 | 11001 | デフォルトグループ | |
| □ | 209 | | ☆ | 2018/05/23 16:49:24 | 2018/05/23 16:49:32 | 00:00:08 | 60000 | 11001 | 着信 | 10001 | 11001 | デフォルトグループ | |
| □ | 210 | | ☆ | 2018/05/23 16:52:25 | 2018/05/23 16:52:37 | 00:00:12 | 60000 | 11001 | 着信 | 10001 | 11001 | デフォルトグループ | |

1 - 10 件目 / 全11件

<< < 1 2 > >>

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



通話データの再生

| | |
|---|---|
| 録音ID | 206 |
| マーク | ☆ |
| 開始日時 | 2018/05/23 16:22:29 |
| 終了日時 | 2018/05/23 16:22:36 |
| 通話時間 | 00:00:07 |
| 相手先電話番号 | 60000 |
| 自社電話番号 | 11001 |
| 発着信 | 着信 |
| 内線番号 | 10001 |
| 回線名 | 11001 |

00:00:00 00:00:00 00:00:07

ノイズキャンセル OFF

再生速度 1.0 倍速

## 9. Conclusion

These Application Notes describe the configuration steps required for NextGen LA-6000 to successfully interoperate with Avaya Aura® Communication Manager 7.1 using Avaya Aura® Application Enablement Services 7.1 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 7.1.2, Feb 2018.
[2] *Avaya Aura® Application Enablement Services Documentation Library*, Release 7.1.2, December 2017.

The following product documentation can be obtained from NextGen.
[3] *LA-6000 Installation/Administration User's Guide*, Version 2.0

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.