Application Notes for TeleSvyaz FLAT Record with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services for selective recording using Single Step Conference – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TeleSvyaz FLAT Record to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services for selective recording using Single Step Conference.

In the compliance testing, FLAT Record used the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to monitor users on 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 TeleSvyaz FLAT Record (FLAT Record) to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services for selective recording using Single Step Conference.

In the compliance testing, FLAT Record used the Avaya Aura® Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface to monitor stations on Avaya Aura® Communication Manager (Communication Manager), and obtain call information and media associated with the monitored stations for call recording.

As a voice recording system, FLAT Record provides selective voice recording capability in 2 modes, i.e. Active and Passive. Passive recording method uses the mirroring of gateway port or media server for voice recording. In this compliance testing, active recording mode was used.

2. General Test Approach and Test Results

In FLAT Record implementation architecture, a local collector server can be used. The local collector server will communicate with the centralized system server and synchronize with it for wider geographical location. In this compliance testing, a centralized server is setup without a local collector server.

The feature and serviceability test cases were performed manually. Upon start of the FLAT Record application, it uses AES' DMCC to automatically register the virtual IP softphones to Communication Manager and request monitoring on the subscriber to be recorded. The number of virtual IP softphones must correspond to the number of active channels in the recording system. "Single Step Conference" method is used for voice recording. A virtual station from which the recording system receives media data joins automatically to any session held by the station subscribed for recording.

In feature testing, each call was handled manually on the station user with generation of unique audio content for the recording. Necessary user actions such as hold and reconnect were performed from the user telephones to test the different call scenarios for softphone and hard phone. It also includes feature calls such as inbound attended/blind transfer and conference.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cable to FLAT Record server with dropping/establishing call in different scenarios and restarting of the TSAPI/DMCC service on AES.

The verification of tests included using the FLAT Record logs for proper message exchanges. FLAT Record client was used to verify proper recording 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 this DevConnect Application Note 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 this Application Note, the interface between Avaya systems and *FLAT Record* did not include use of any specific encryption features as requested by Telesvyaz.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

Feature testing focused on verifying the following on FLAT Record for proper recordings, loggings and playback of calls:

- Inbound and Outbound calls to/from PSTN
- Inbound and Outbound calls to/from internal phones
- Transfer calls
- Conference calls
- Call Hold and Resume
- Avaya 9600 Series Deskphones and Avaya one-X® Communicator

Serviceability testing focused on verifying the ability of FLAT Record to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to the server and restarting of AES services.

2.2. Test Results

All feature test cases were successfully completed with the following observations:

- In attended transfer scenario, the final call leg is recorded twice:
  e.g., A → B (transfer) → C
  A-C call recording is found in A-B call recording and B-C call recording.

2.3. Support

Technical support on FLAT Record can be obtained through the following:

- **Phone:** +7 (499) 551-77-77
- **Email:** public@teleswyz.ru
- **Web:** http://www.teleswyz.ru/

3. Reference Configuration

Figure 1 below illustrates the test configuration consisting of Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Media Server, a duplex pair of Avaya Aura® Communication Manager Servers, Avaya Aura® Application Enablement Services and Avaya G430 Media Gateway. Avaya 96x1, 96x0 and 1600 Series H.323 and SIP 96x1 IP Deskphones including 1400 Series Digital Deskphone are used as stations. FLAT Record client is installed on a PC that runs Avaya one-X® Communicator. FLAT Record server is installed on Microsoft Windows 2012 R2 which communicates with the DMCC Service on the Avaya Aura® Application Enablement Services. The Avaya 4548GT-PWR Converged Stackable Switch provided ethernet connectivity to the servers and telephones. A simulated public PSTN trunk connected to the system. The telephones were used to generate intra-switch calls (calls between telephones on the same system) and outbound/inbound calls to/from the PSTN.

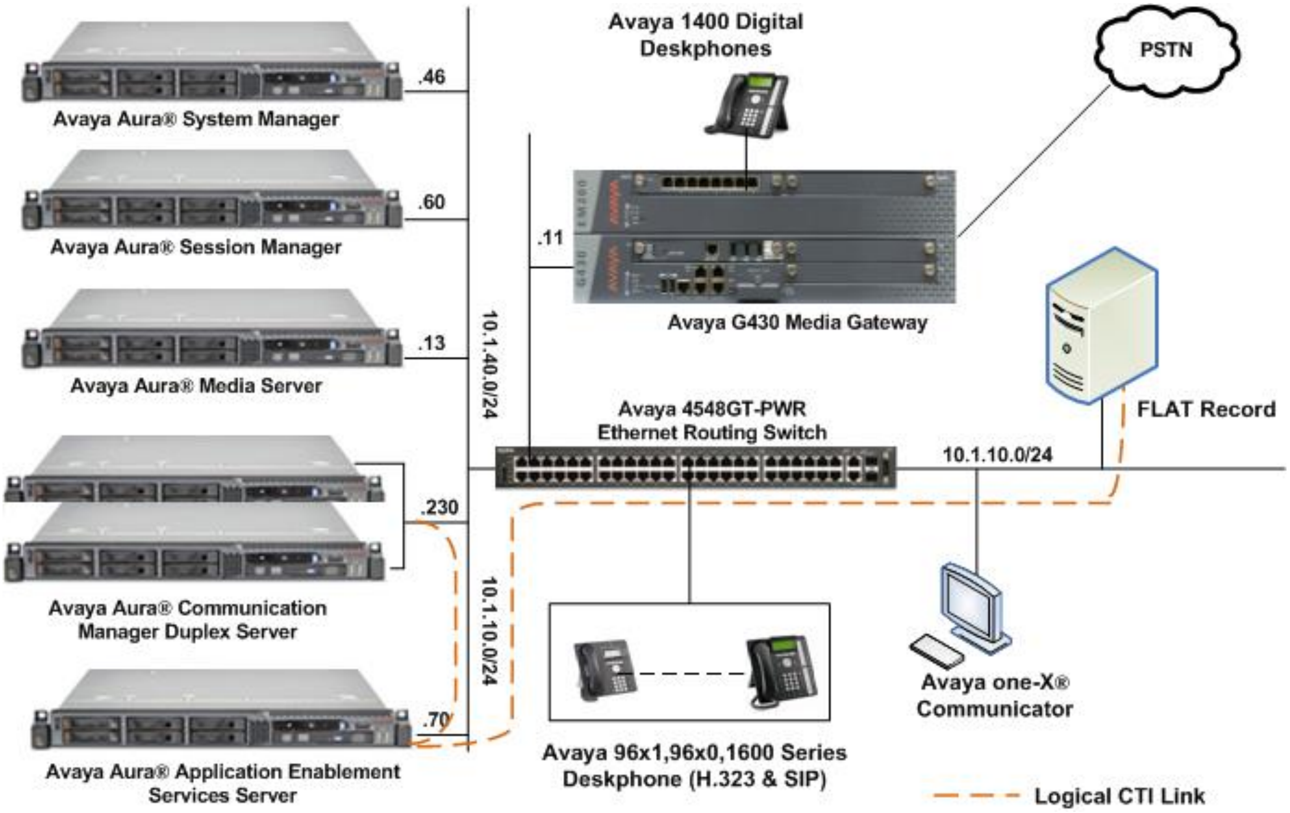

Avaya Aura® System Manager
.46
Avaya Aura® Session Manager
.60
Avaya Aura® Media Server
.13
Avaya Aura® Communication Manager Duplex Server
.230
Avaya Aura® Application Enablement Services Server
.70
10.1.40.0/24
10.1.10.0/24
Avaya 1400 Digital Deskphones
PSTN
.11
Avaya G430 Media Gateway
FLAT Record
Avaya 4548GT-PWR Ethernet Routing Switch
10.1.10.0/24
Avaya one-X® Communicator
Avaya 96x1,96x0,1600 Series Deskphone (H.323 & SIP)
Logical CTI Link

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 running on virtual platform	7.0.1.2.0.441.23523 (7.0.1.2.0-FP1 SP2)
Avaya S8300D Server (w/ G430) running on Avaya virtual platform as Local Survivable Processor (LSP)	7.0.1.2.0.441.23523 (7.0.1.2.0-FP1 SP2)
Avaya G430 Media Gateway: MM712AP (DCP)	 HW04 FW015
Avaya Application Enablement Services (AES) Server running on virtual platform	7.0 SP3 (7.0.1.0.3.15-0)
Avaya Aura® System Manager running on virtual platform	7.0.1.2.086007
Avaya Aura® Session Manager running on virtual platform	7.0.1.2.701230
Avaya Aura® Media Server running on virtual platform	7.8.0.268
Avaya 4548GT-PWR Converged Stackable Switch	5.3.0.3
Avaya 1600 Series IP Phones : 1608 (H.323)	 1.3100
Avaya 96x0 Series IP Phones: 9630 (H.323)	 3.270B
Avaya 96x1 Series IP Phones: 9611 (H.323) 9641 (H.323)	 6.6401 6.6401
Avaya 96x1 Series IP Phones: 9611 (SIP)	7.0.1.3.4
Avaya 1400 Series Digital Phones	Rel 4 SP9
Avaya one-X® Communicator (H.323) FLAT Record client running on a PC using Windows 10 Pro	6.2.12.04-SP12 3.0.1.33
FLAT Record as an application on Windows Server 2012 R2 running on virtual server	3.0.1

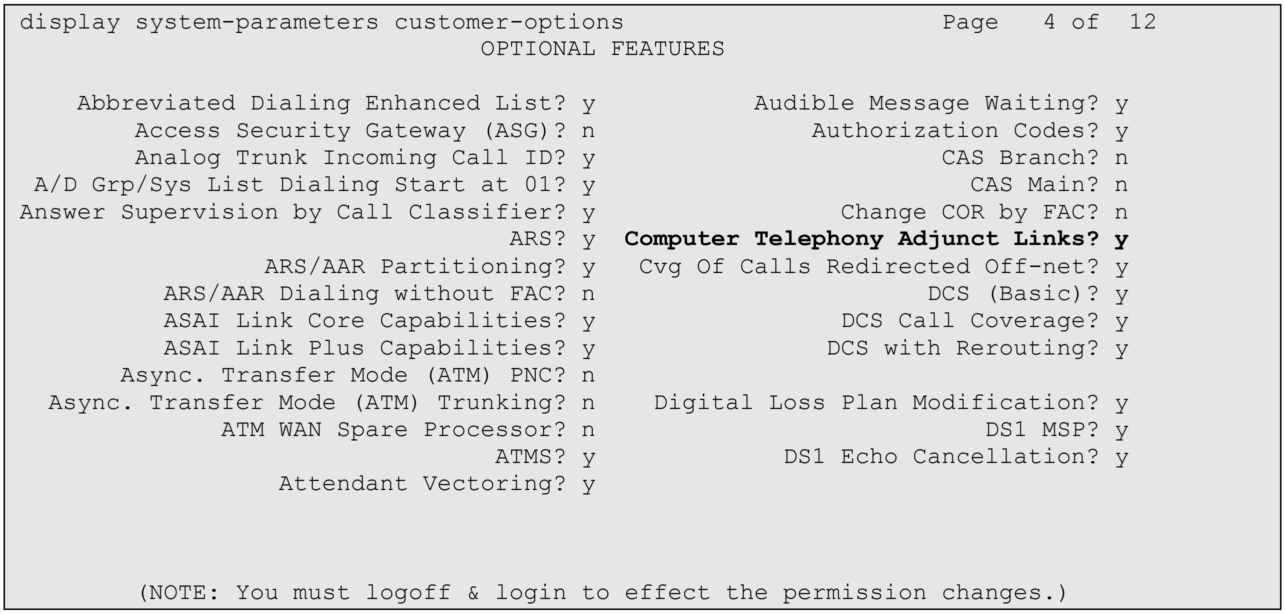
5. Configure Avaya Aura® Communication Manager

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 Virtual IP softphones
- Administer SIP Stations for recording

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 AES.

```
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 for 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 for the **AE Services Server** field. The server name may be obtained by logging in to the AES server using Secure Shell (SSH) and running the **uname -a** command. Enter an alphanumeric password for 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 Virtual IP Softphones

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

- **Type:** Any IP telephone type allowing multiple buttons, such as **4624**.
- **Name:** A descriptive name.
- **Security Code:** A desired value. Note that all stations must use the same password.
- **IP SoftPhone:** Set to **y**.

```
add station 19901                                              Page   1 of   6
                                     STATION

Extension: 19901                         Lock Messages? n               BCC: 0
     Type: 4624                          Security Code: 12345            TN: 1
     Port: IP                          Coverage Path 1:                 COR: 1
     Name: DMCC #1                     Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 19901
            Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal             Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? y

                                                IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default
```

Repeat this section to administer the desired number of virtual IP softphones. In the compliance test, 6 virtual IP softphones were administered as shown below for monitoring of stations.

```
list station 19901 count 6

                                  STATIONS

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

19901         S00395  DMCC #1                                      1
               4624                        no                      1   1
19902         S00006  DMCC #2                                      1
               4624                        no                      1   1
19903         S00007  DMCC #3                                      1
               4624                        no                      1   1
19904         S00008  DMCC #4                                      1
               4624                        no                      1   1
19905         S00011  DMCC #5                                      1
               4624                        no                      1   1
19906         S00042  DMCC #6                                      1
               4624                        no                      1   1
```

5.4. Administer SIP Stations for recording

The recording of SIP station requires 3rd Party Call Control. Assuming SIP station is already administered, using the **change station n** command, where **n** is the SIP extension number, on Page 6, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Type of 3PCC Enabled: Avaya**
- **SIP Trunk: aar**

```
change station 10049                                            Page   6 of   6
                                     STATION
SIP FEATURE OPTIONS

         Type of 3PCC Enabled: Avaya
                    SIP Trunk: aar

 Enable Reachability for Station Domain Control: s
```

6. Configure Avaya Aura® Application Enablement Services

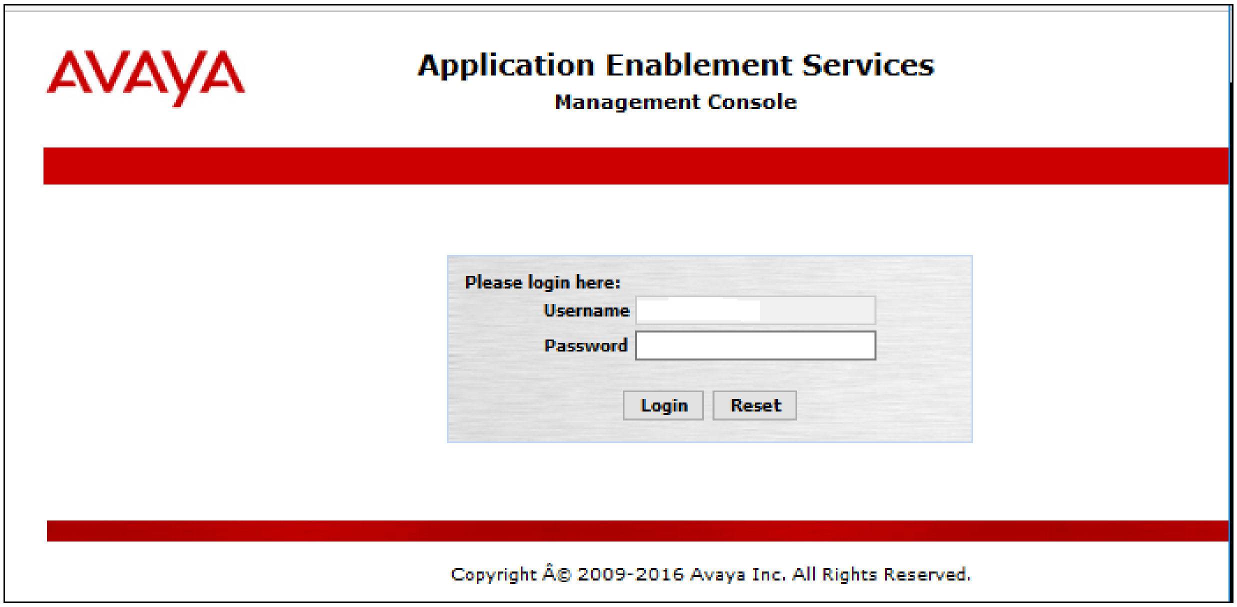
This section provides the procedures for configuring Avaya Aura® Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer Switch Connection
- Administer TSAPI link
- Administer H.323 gatekeeper
- Disable security database
- Restart TSAPI and DMCC service
- Administer Flat Record user
- Administer CTI User permissions
- Enable DMCC and TSAPI Service port

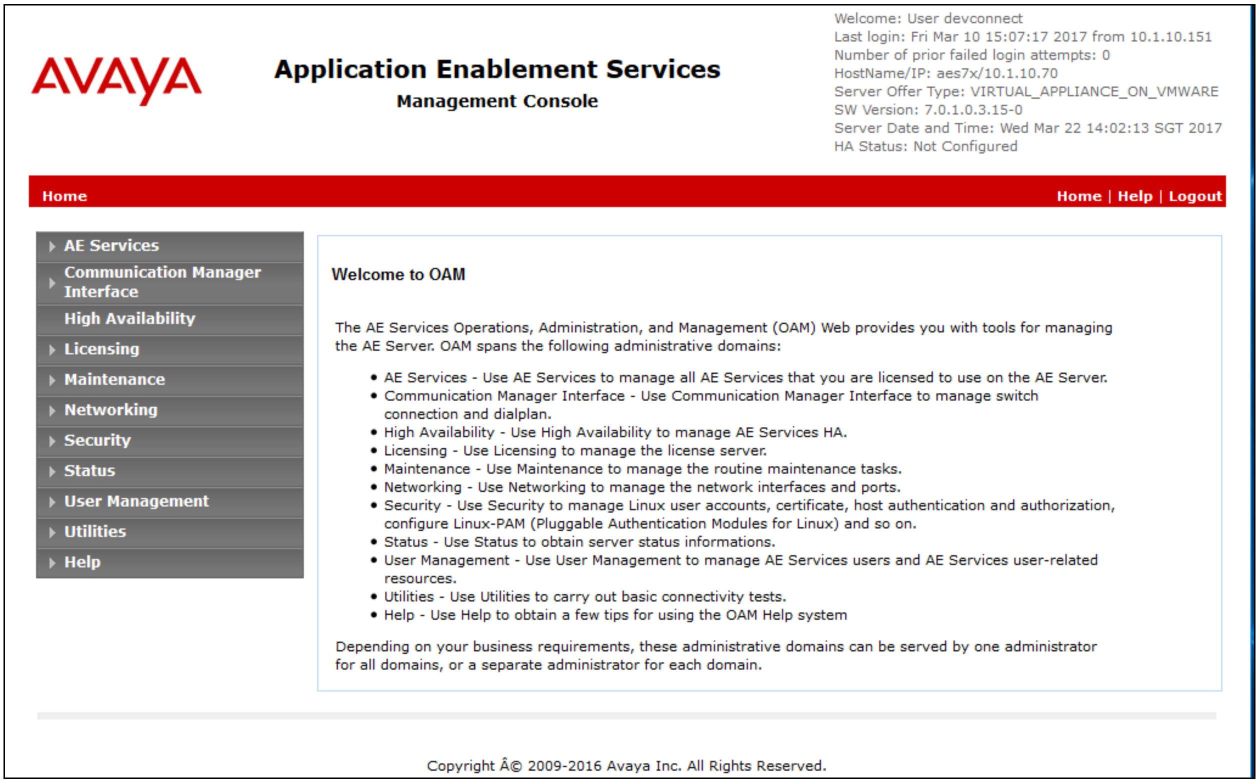
6.1. Launch OAM Interface

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 Application Enablement Services 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: Fri Mar 10 15:07:17 2017 from 10.1.10.151
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Wed Mar 22 14:02:13 SGT 2017
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:

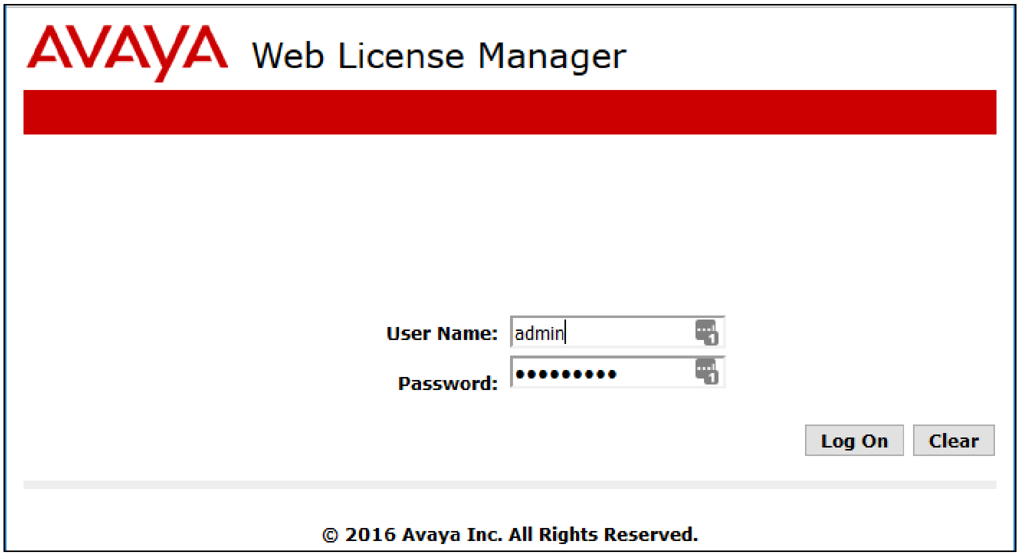
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing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

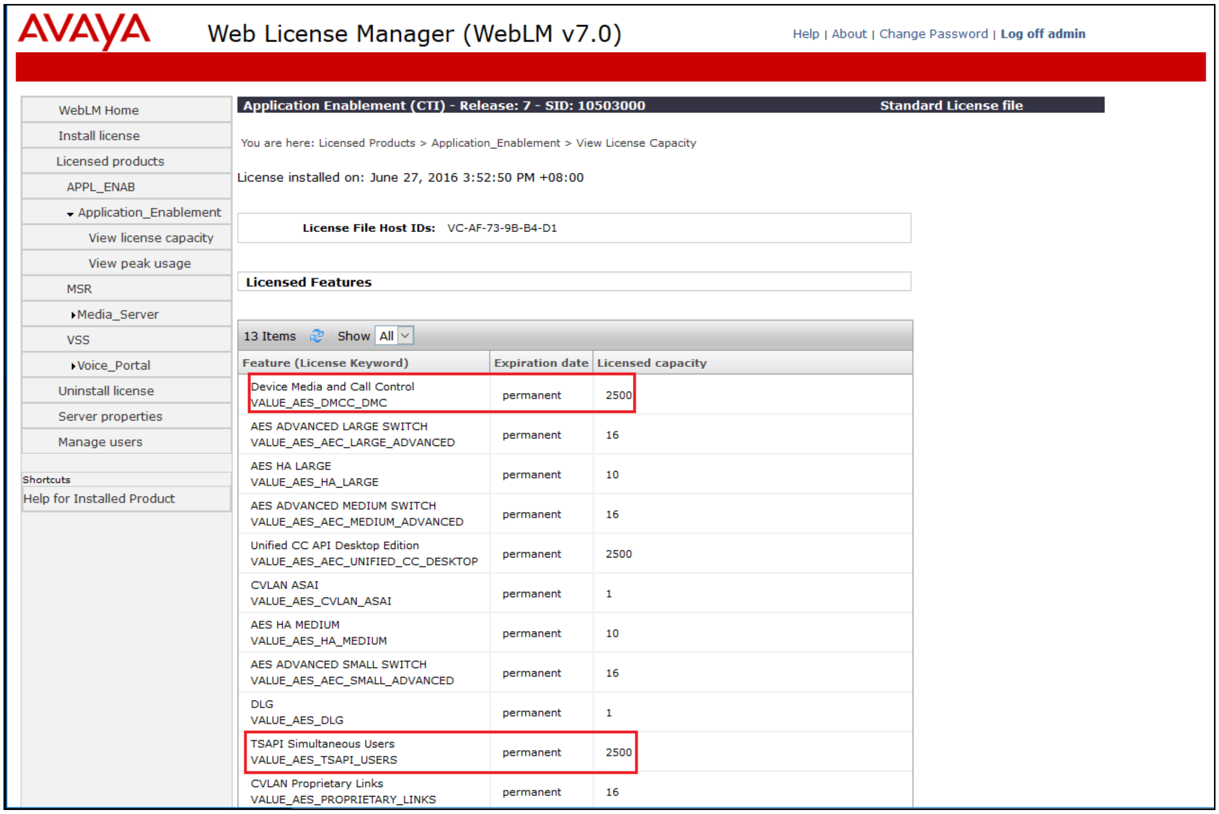
Select **Licensing → WebLM Server Access** from the left pane of the home screen and **Avaya WebLM** screen pops up (not shown). Click on the **License Administration** and the **Web License Manager** screen is displayed below. Log in with the appropriate credentials.



User Name: admin
Password: •••••••••

© 2016 Avaya Inc. All Rights Reserved.

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 for **Device Media and Call Control** and **TSAPI Simultaneous Users**, as shown below.



Application Enablement (CTI) - Release: 7 - SID: 10503000 **Standard License file**

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

License installed on: June 27, 2016 3:52:50 PM +08:00

License File Host IDs: VC-AF-73-9B-B4-D1

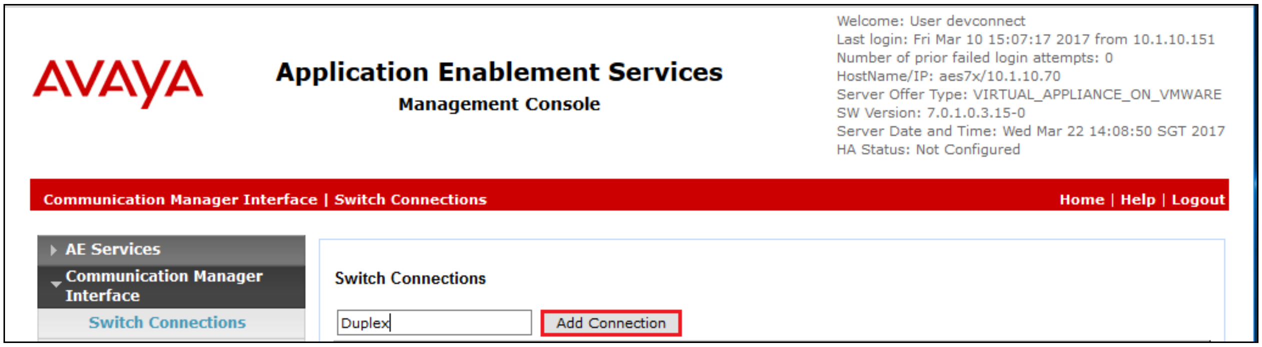
Licensed Features

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	10
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	2500
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	1
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	10
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 Switch Connection

From the Home menu, 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

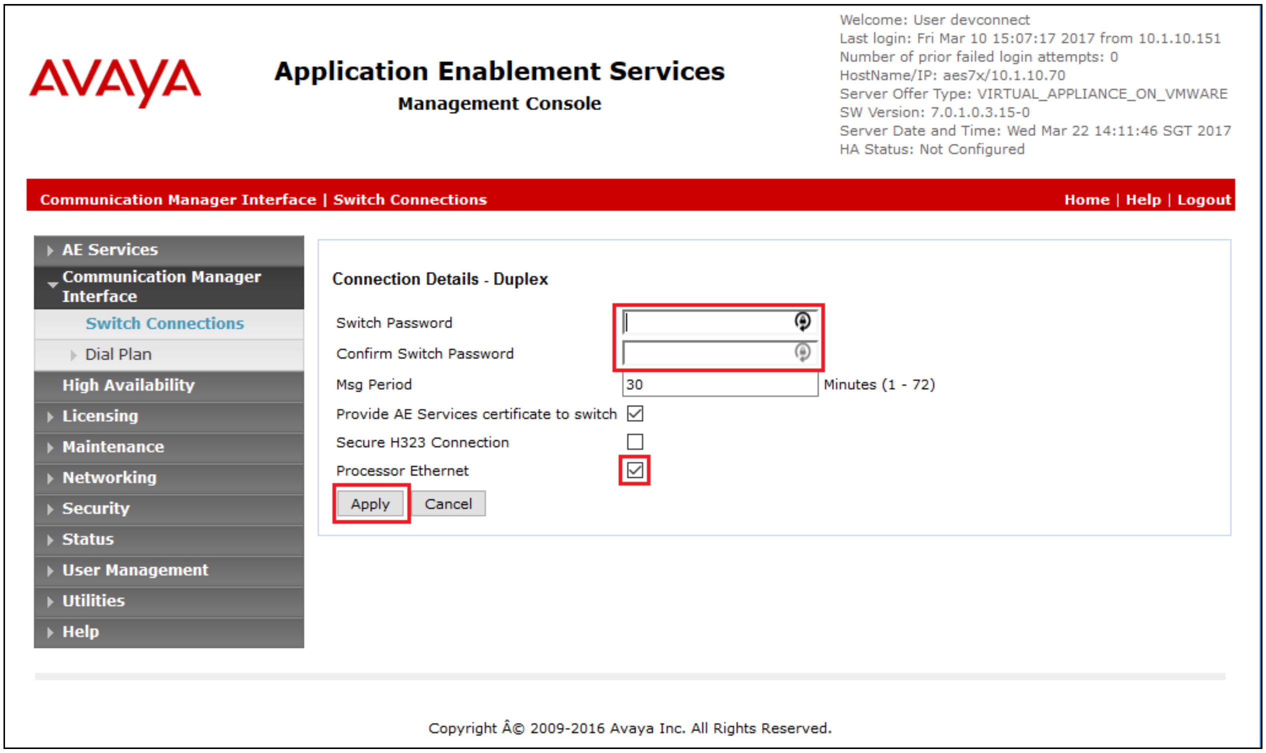
Welcome: User devconnect
Last login: Fri Mar 10 15:07:17 2017 from 10.1.10.151
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Wed Mar 22 14:08:50 SGT 2017
HA Status: Not Configured

Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections

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 effect changes.



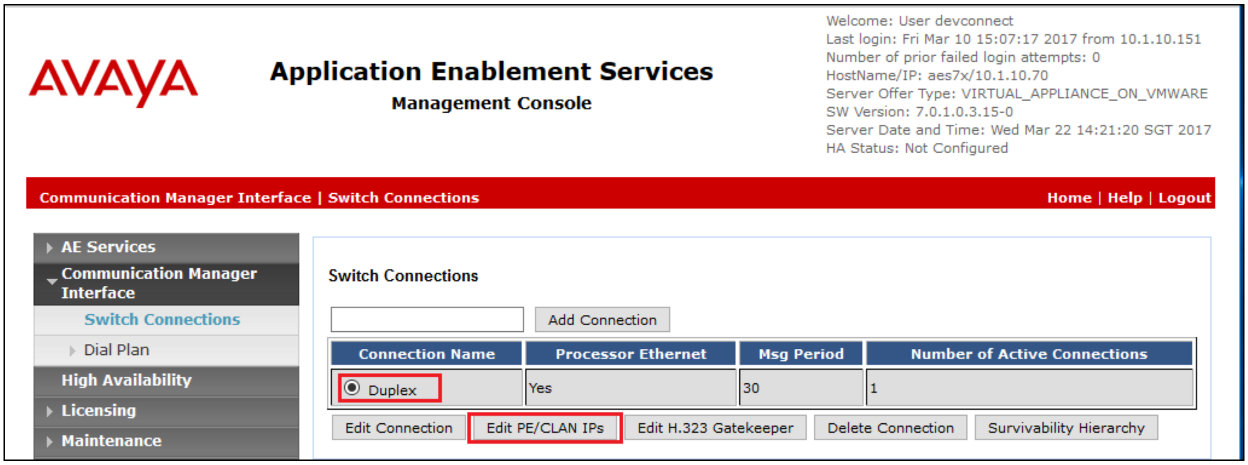
Welcome: User devconnect
Last login: Fri Mar 10 15:07:17 2017 from 10.1.10.151
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Wed Mar 22 14:11:46 SGT 2017
HA Status: Not Configured

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 ☑

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

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

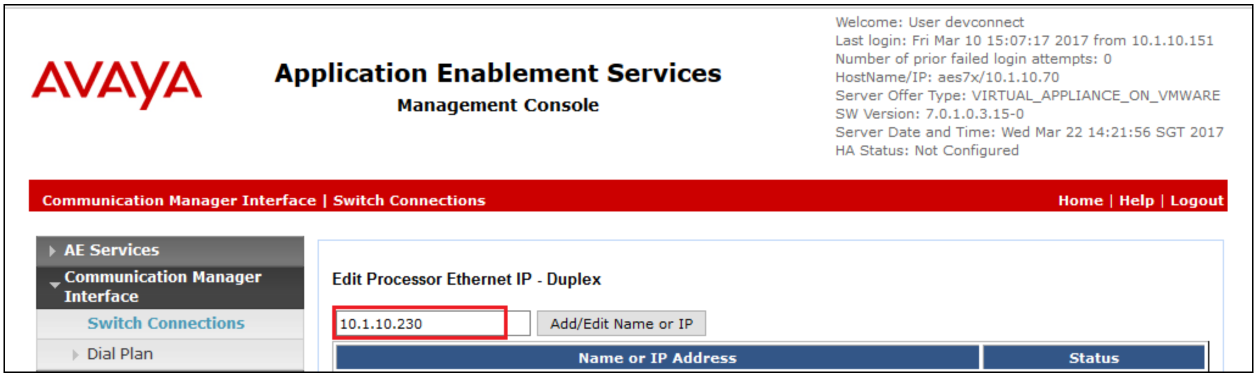


Welcome: User devconnect
Last login: Fri Mar 10 15:07:17 2017 from 10.1.10.151
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Wed Mar 22 14:21:20 SGT 2017
HA Status: Not Configured

Switch Connections

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

In the **Edit Processor Ethernet IP – Duplex** screen, enter the host name or IP address of the PE/C-LAN used for AES connectivity. 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**



Welcome: User devconnect
Last login: Fri Mar 10 15:07:17 2017 from 10.1.10.151
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Wed Mar 22 14:21:56 SGT 2017
HA Status: Not Configured

Edit Processor Ethernet IP - Duplex

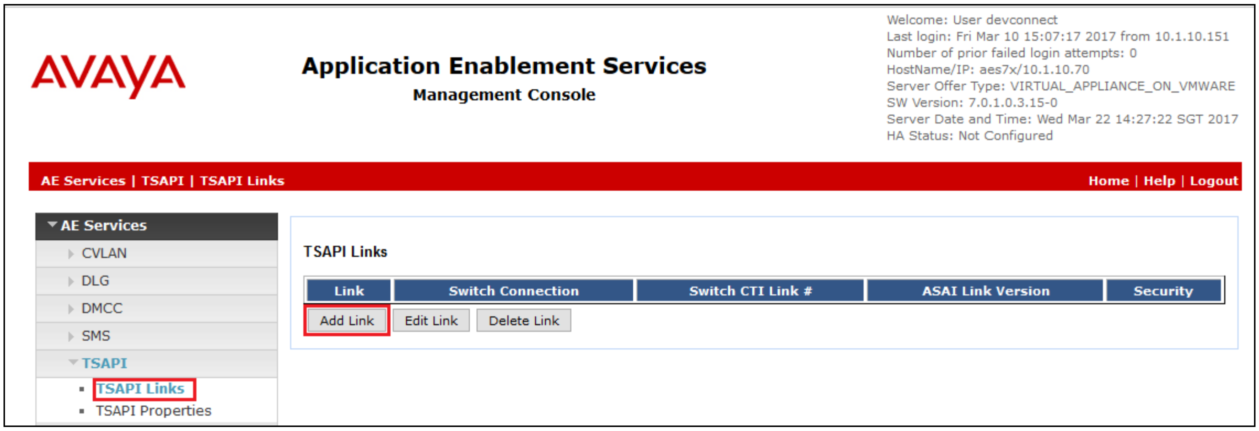
10.1.10.230

Name or IP Address	Status

AVAYA
Application Enablement Services
Management Console
Communication Manager Interface | Switch Connections
Home | Help | Logout
AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Add/Edit Name or IP

6.4. Administer TSAPI Link

To administer a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



Welcome: User devconnect
Last login: Fri Mar 10 15:07:17 2017 from 10.1.10.151
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Wed Mar 22 14:27:22 SGT 2017
HA Status: Not Configured

Application Enablement Services
Management Console

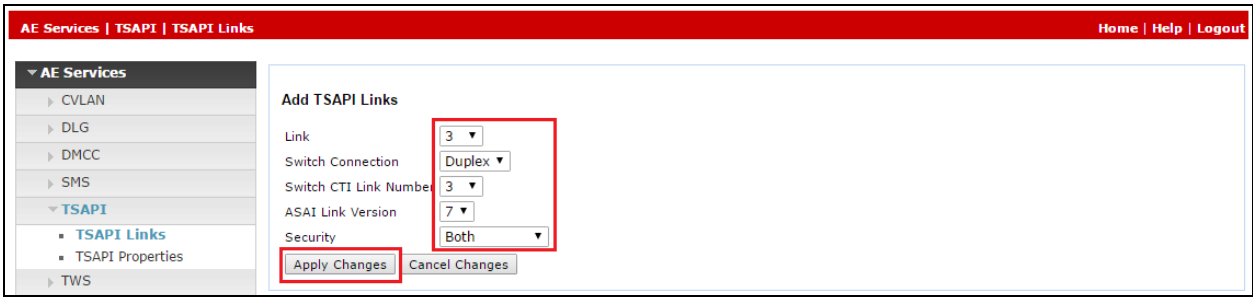
TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

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 **7** for the latest version.
- **Security:** Select **Both** to allow for encrypted or unencrypted link.

Click **Apply Changes**.



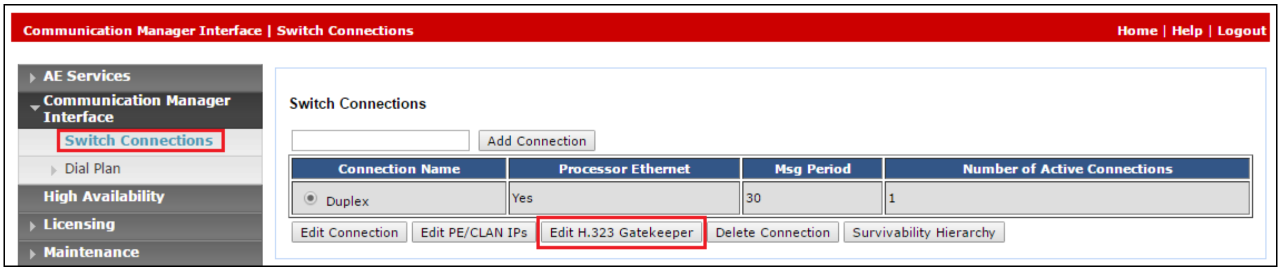
Add TSAPI Links

Link	3
Switch Connection	Duplex
Switch CTI Link Number	3
ASAI Link Version	7
Security	Both

6.5. Administer H.323 Gatekeeper

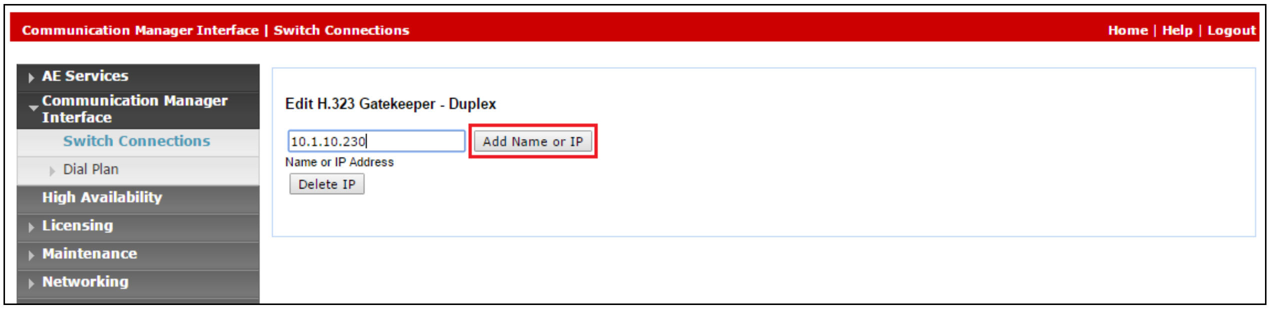
Select **Communication Manager Interface → Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

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



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

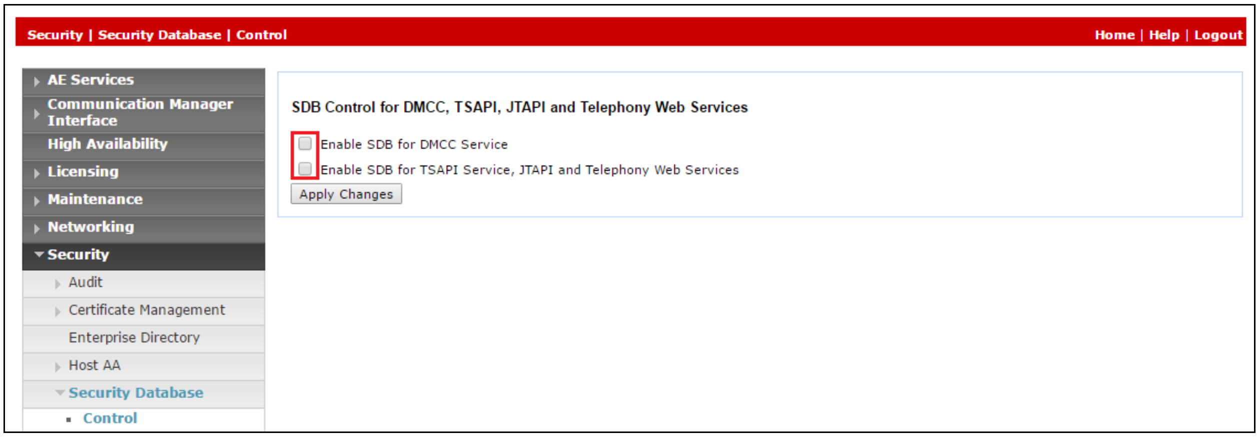
The **Edit H.323 Gatekeeper – Duplex** screen is displayed. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to be used as H.323 gatekeeper, in this case the Processor C-LAN is used as shown below. Click **Add Name or IP**.



Name or IP Address: 10.1.10.230

6.6. 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**.



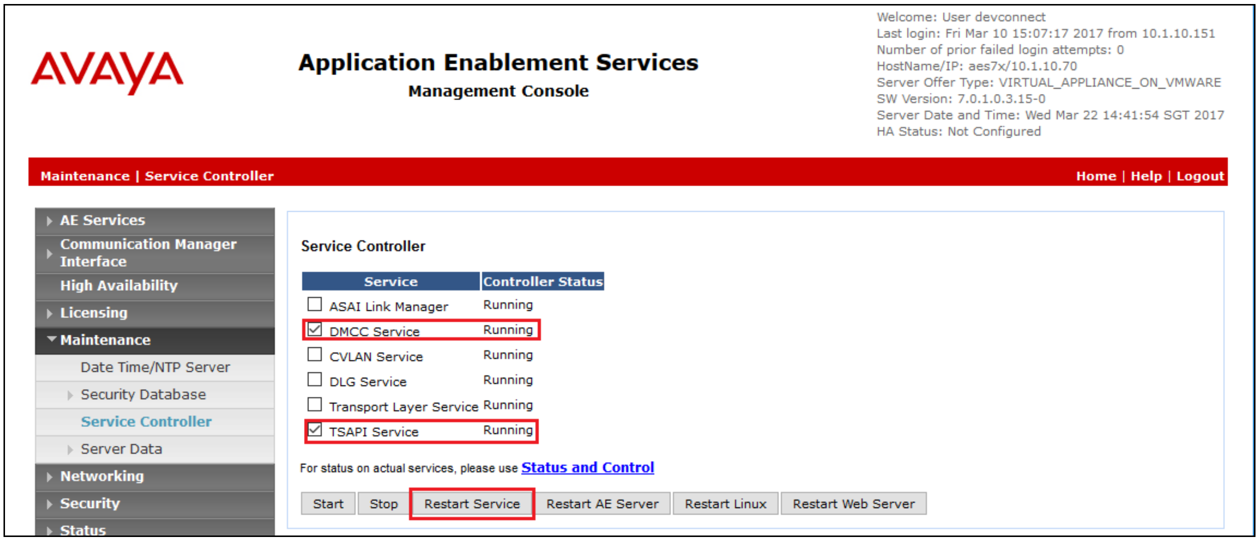
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

□ Enable SDB for DMCC Service

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

6.7. Restart TSAPI and DMCC Service

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



Welcome: User devconnect
Last login: Fri Mar 10 15:07:17 2017 from 10.1.10.151
Number of prior failed login attempts: 0
HostName/IP: aes7x/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.3.15-0
Server Date and Time: Wed Mar 22 14:41:54 SGT 2017
HA Status: Not Configured

Service Controller

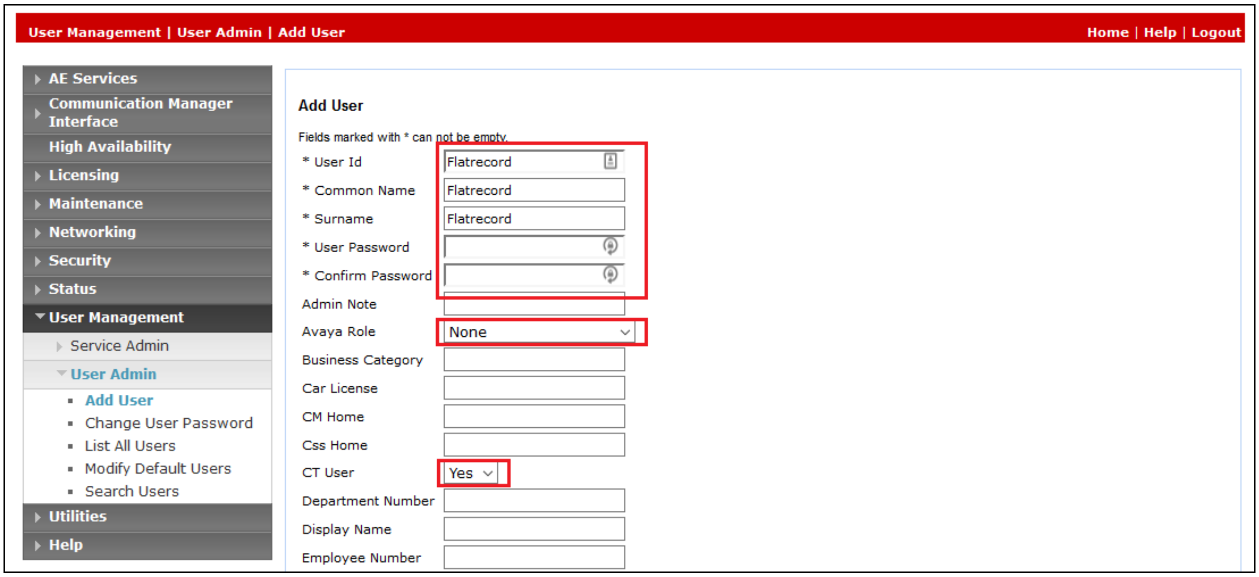
Service	Controller Status
□ ASAI Link Manager	Running
☑ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.8. Administer FLAT Record 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).



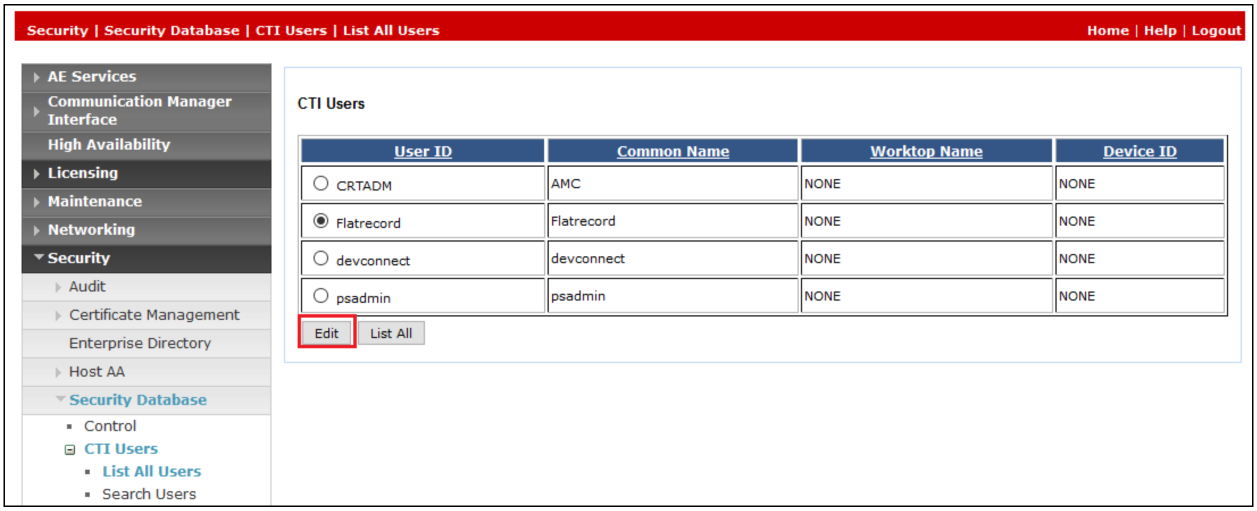
Add User

Fields marked with * can not be empty.

* User Id	Flatrecord
* Common Name	Flatrecord
* Surname	Flatrecord
* 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	

6.9. Administer CTI User Permissions

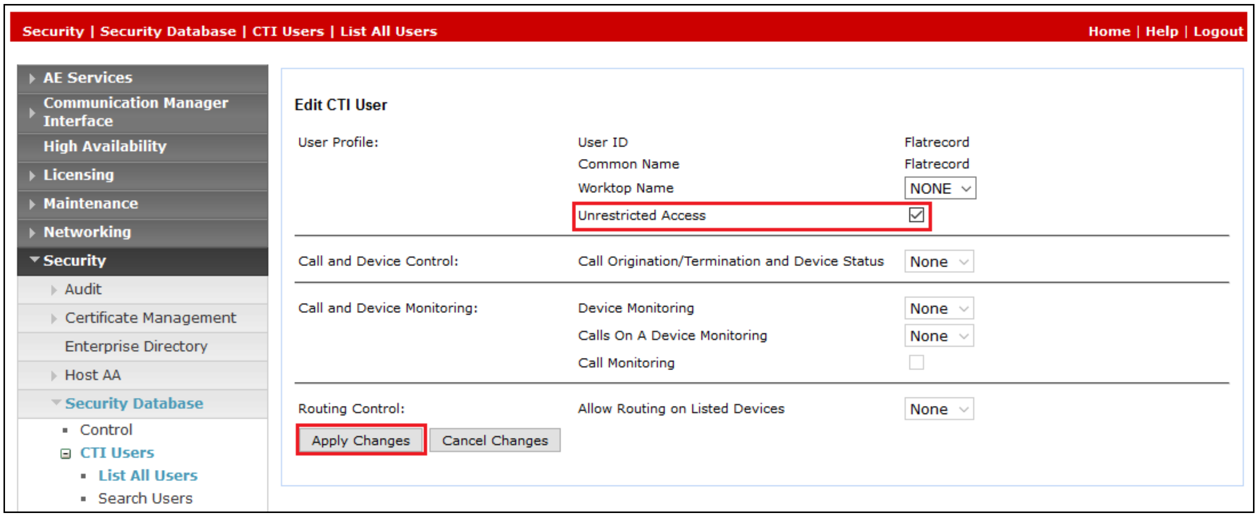
Select **Security → Security Database → CTI Users → List All Users** from the AES Management Console Home menu. Select the User ID created in **Section 6.8** and click **Edit**.



CTI Users

User ID	Common Name	Worktop Name	Device ID
○ CRTADM	AMC	NONE	NONE
● Flatrecord	Flatrecord	NONE	NONE
○ devconnect	devconnect	NONE	NONE
○ psadmin	psadmin	NONE	NONE

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



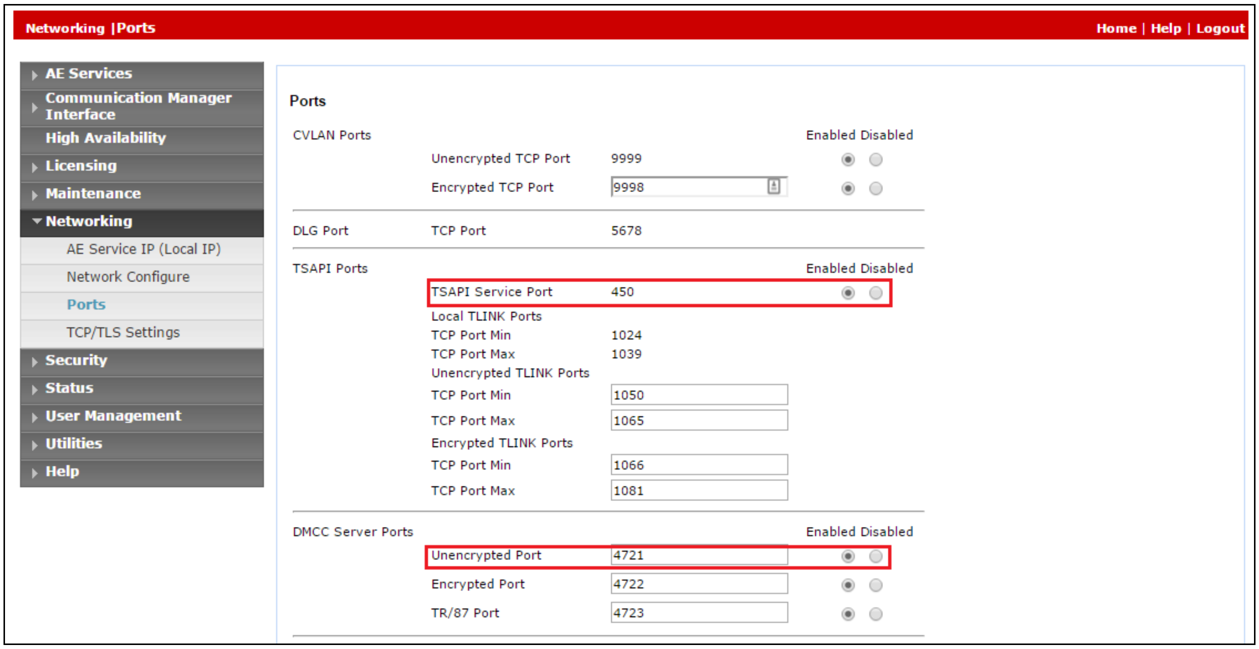
Edit CTI User

User Profile:	User ID	Flatrecord
	Common Name	Flatrecord
	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 DMCC and TSAPI Service Port

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

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Do the same for **TSAPI Ports** for **TSAPI Service Port** under the **Enabled** column.



Ports

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

7. Configure FLAT Record

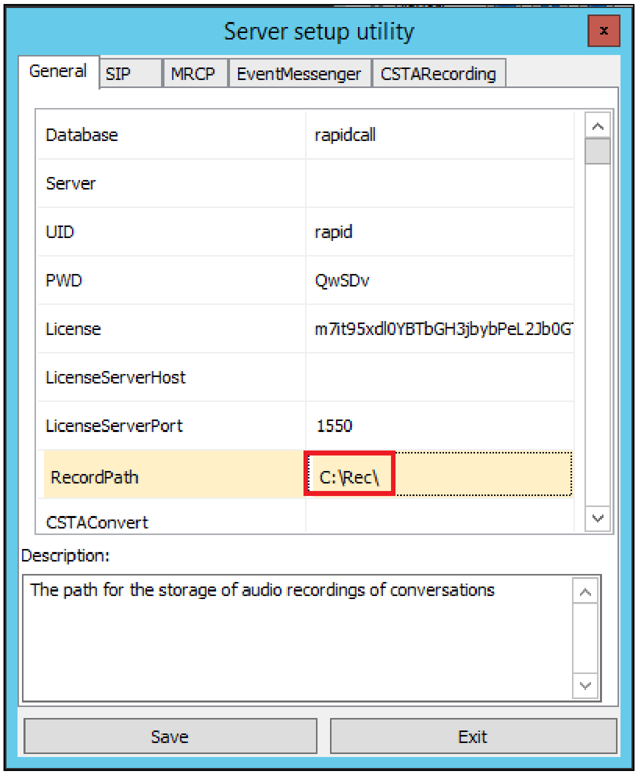
This section provides the procedures for configuring FLAT Record. The procedures include the following areas:

- Configuration of Recording Server Role
- Restart Services
- Using FLAT Client for configuration

The configuration of FLAT Record server is performed by TeleSvyaz Services engineers. The procedural steps are presented in these Application Notes for informational purposes. These Application Notes assume that the installations and basic configurations are all in place and will not be covered.

7.1. Configuration of Recording Server Role

Run the settings program at the default location "**C:\Program Files (x86)\Flat Contact\Server**". Select the **General** tab and set the recording location for the **RecordPath** parameter. In this compliance test, it is set at "**C:\Rec\**".



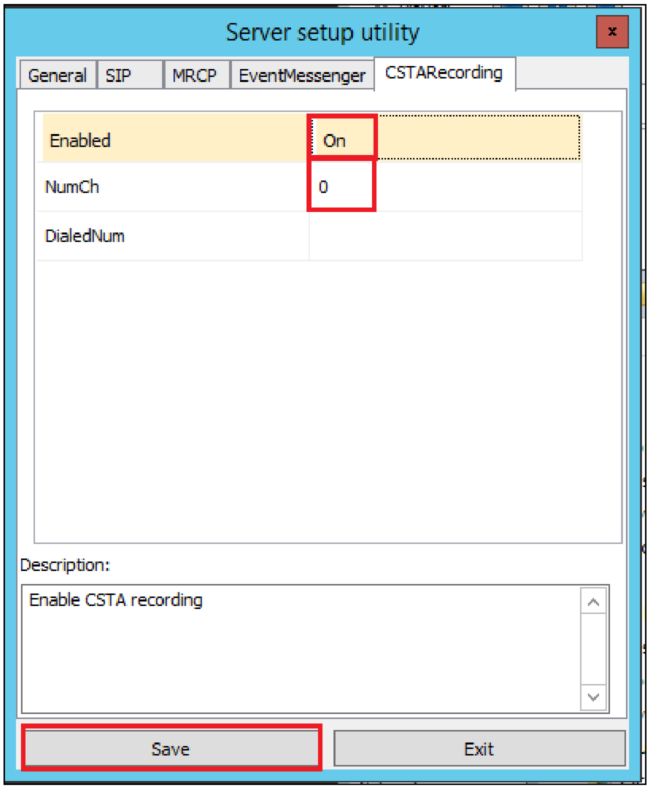
Database	rapidcall
Server	
UID	rapid
PWD	QwSDv
License	m7it95xdl0YBTbGH3jbybPeL2Jb0G
LicenseServerHost	
LicenseServerPort	1550
RecordPath	C:\Rec\
CSTAConvert	

Description:

The path for the storage of audio recordings of conversations

Next, select the **CSTARecording** tab and set the following parameters. Leave the rest as default. Click **Save** to record the settings.

- **Enabled : On**
- **NumCh : 0**



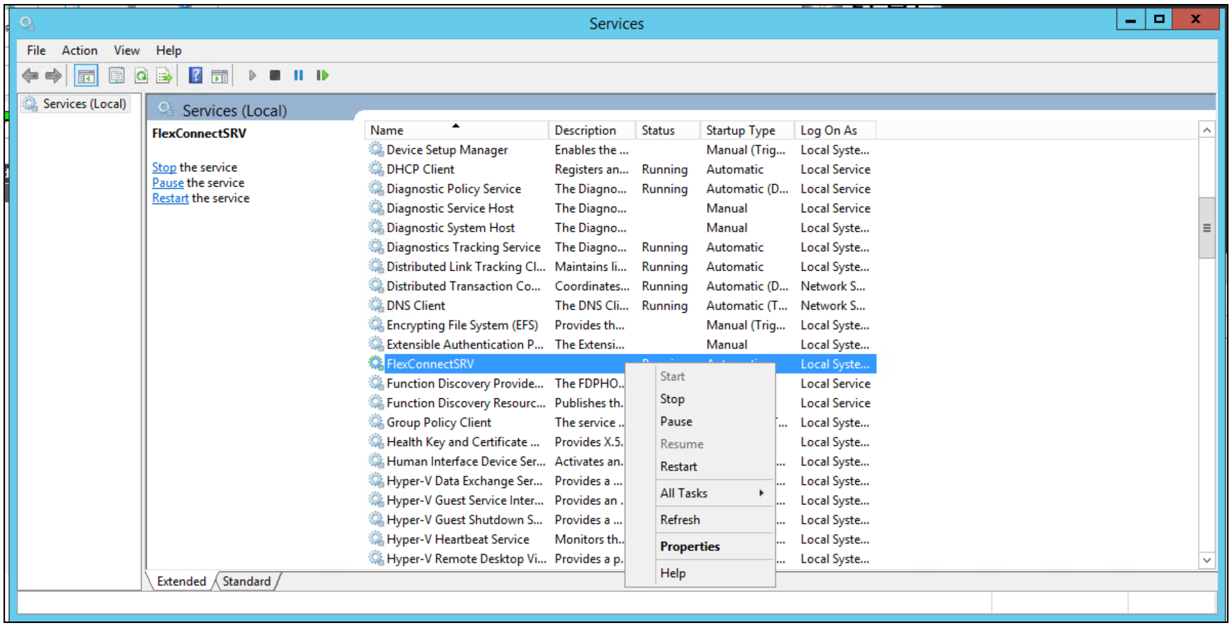
Enabled	On
NumCh	0
DialedNum	

Description:

Enable CSTA recording

7.2. Restart Services

Select **Start → Apps → Administrative Tools → Services** to display the **Services (Local)** screen. Restart the **FlexConnectSRV** shown below.



FlexConnectSRV

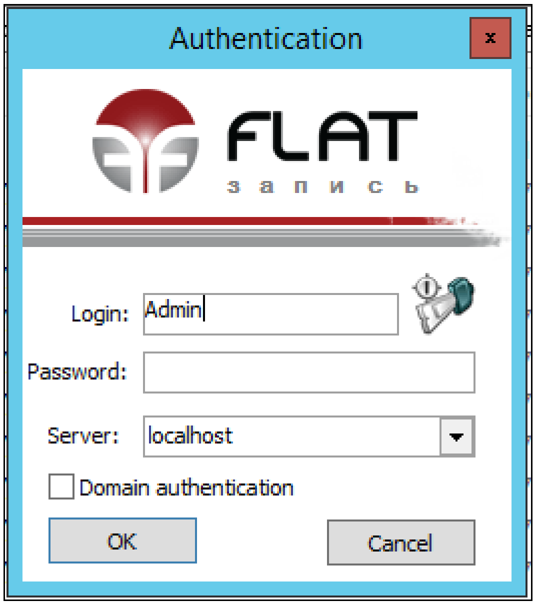
Stop the service
Pause the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Device Setup Manager	Enables the ...		Manual (Trig...	Local Syste...
DHCP Client	Registers an...	Running	Automatic	Local Service
Diagnostic Policy Service	The Diagno...	Running	Automatic (D...	Local Service
Diagnostic Service Host	The Diagno...		Manual	Local Service
Diagnostic System Host	The Diagno...		Manual	Local Syste...
Diagnostics Tracking Service	The Diagno...	Running	Automatic	Local Syste...
Distributed Link Tracking Cl...	Maintains li...	Running	Automatic	Local Syste...
Distributed Transaction Co...	Coordinates...	Running	Automatic (D...	Network S...
DNS Client	The DNS Cli...	Running	Automatic (T...	Network S...
Encrypting File System (EFS)	Provides th...		Manual (Trig...	Local Syste...
Extensible Authentication P...	The Extensi...		Manual	Local Syste...
FlexConnectSRV				Local Syste...
Function Discovery Provide...	The FDPHO...			Local Service
Function Discovery Resourc...	Publishes th...			Local Service
Group Policy Client	The service ...		T...	Local Syste...
Health Key and Certificate ...	Provides X.5...			Local Syste...
Human Interface Device Ser...	Activates an...		...	Local Syste...
Hyper-V Data Exchange Ser...	Provides a ...		...	Local Syste...
Hyper-V Guest Service Inter...	Provides an ...		...	Local Syste...
Hyper-V Guest Shutdown S...	Provides a ...		...	Local Syste...
Hyper-V Heartbeat Service	Monitors th...		...	Local Syste...
Hyper-V Remote Desktop Vi...	Provides a p...		...	Local Syste...

7.3. Using FLAT Client for Configuration

7.3.1. Connection to Avaya Aura® Application Enablement Services

Select **Start → Apps → Flat Recording → Client** to launch the FLAT client. This application can be installed on a PC or server. Log in with the appropriate credentials.



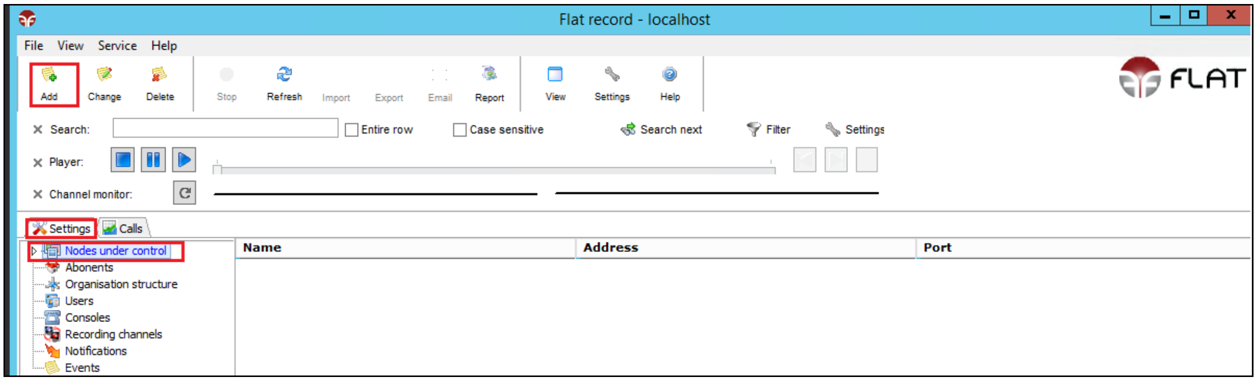
Login: Admin

Password:

Server: localhost

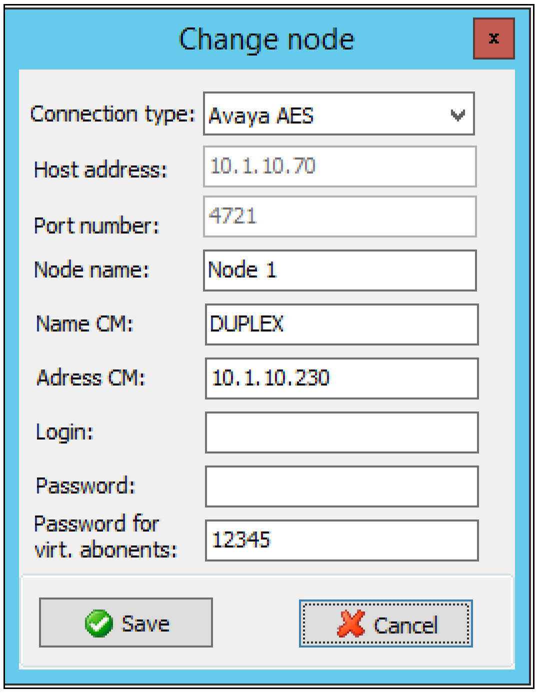
□ Domain authentication

From the home screen, select the **Settings** tab → **Nodes under control** and click **Add** icon on the top left.



Select from the **Connection type** drop down menu, **Avaya AES** and configure the parameters as below. Click **Save** after completion.

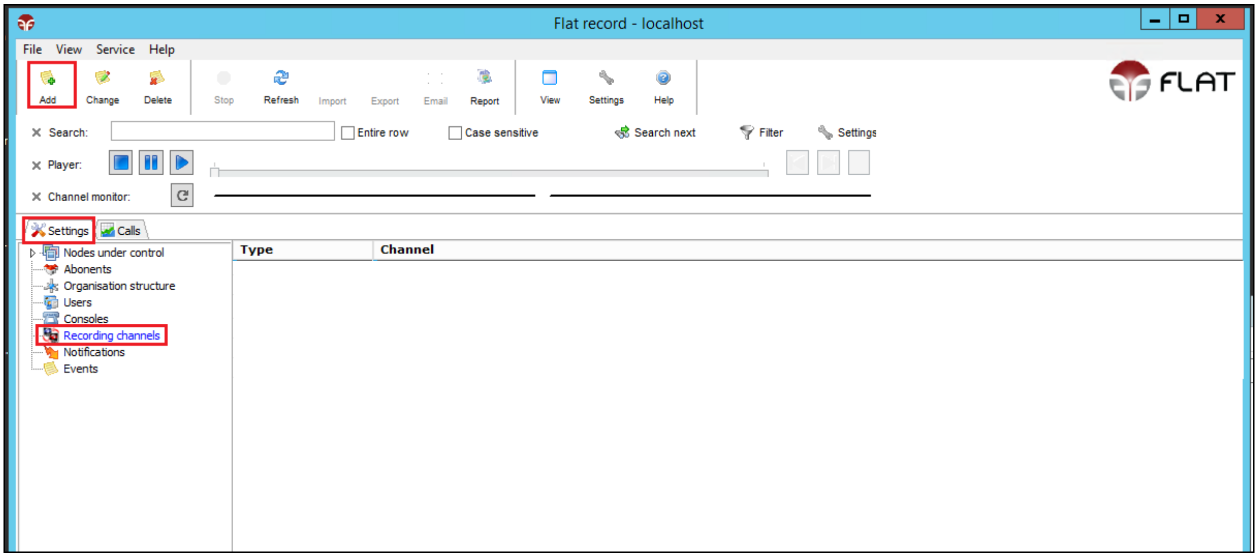
- **Host address**: AES IP address i.e., **10.1.10.70**
- **Port number**: AES DMCC unencrypted port number i.e., **4721** in **Section 6.10**
- **Node name**: Provide an appropriate name
- **Name CM**: Communication Manager switch connection name in **Section 6.3**
- **Address CM**: Communication Manager IP address i.e., **10.1.10.230**
- **Login**: AES CT User login name created in **Section 6.8**
- **Password**: AES CT User password created in **Section 6.8**
- **Password for virt. Abonents**: Virtual stations password created in **Section 5.3**


Change node

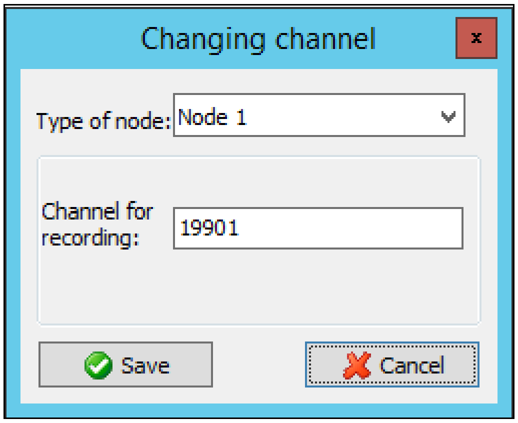
Connection type: Avaya AES
Host address: 10.1.10.70
Port number: 4721
Node name: Node 1
Name CM: DUPLEX
Adress CM: 10.1.10.230
Login:
Password:
Password for virt. abonents: 12345

7.3.2. Add Recording channels

From the home screen, select the **Settings** tab → **Recording channels** and click **Add** icon on the top left.



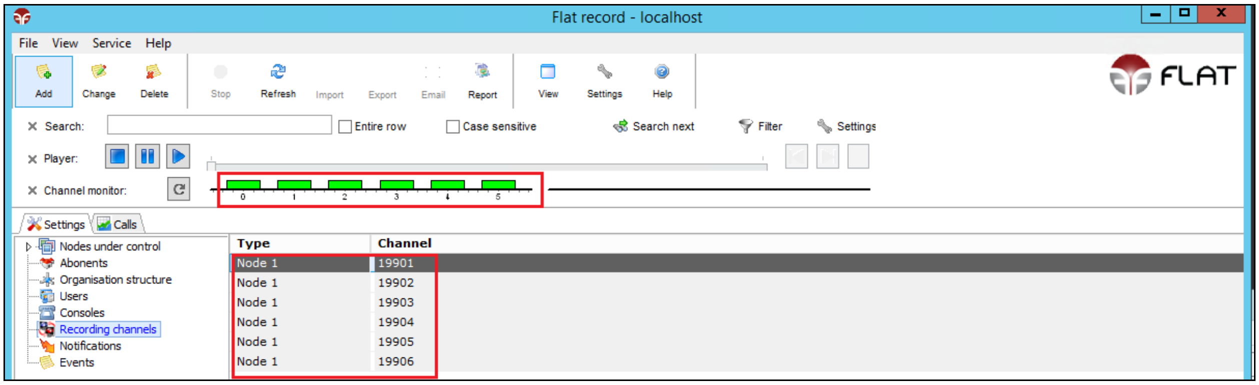
Select the node name created in **Section 7.3.1** and enter the **Channel for recording** for the first virtual stations created **in Section 5.3**. Click **Save** after completion. Repeat for the rest of the channels.



Type of node: Node 1

Channel for recording: 19901

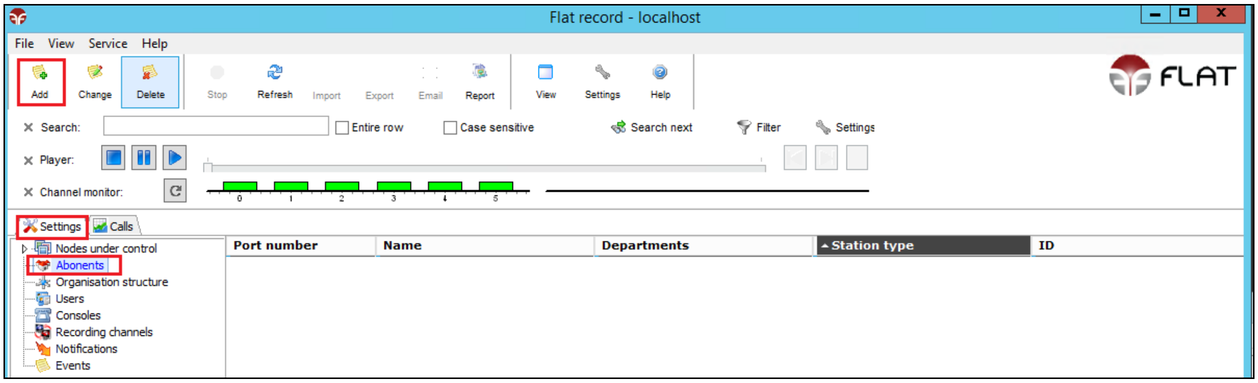
The screen below shows the list of recording channels setup for **19901 – 19906**. The green color for each channel in the **Channel monitor** indicates the connection is successfully establised.



Type	Channel
Node 1	19901
Node 1	19902
Node 1	19903
Node 1	19904
Node 1	19905
Node 1	19906

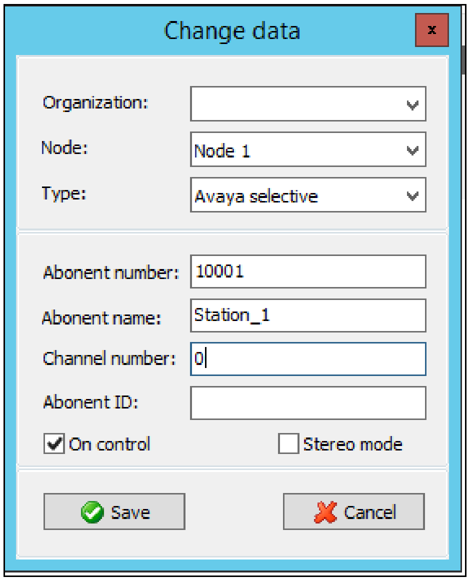
7.3.3. Enable recording for subscribers

From the home screen, select the **Settings** tab → **Abonents** and click **Add** icon on the top left.



Configure the parameters as below. Click **Save** after completion.

- **Organization**: Optional field for reference
- **Node**: Select node name created in **Section 7.3.1**
- **Type:** Select **Avaya selective**
- **Abonent number**: Enter the recorded subscriber number
- **Abonent name**: Enter the recorded subscriber name for identification
- **Channel number**: Not used in this configuration. Serves as identification for dispatcher boards
- **Abonent ID**: Optional reference parameter for sorting subscriber list
- **On Control**: Tick for recording conversation
- **Stereo mode**: Not used in this configuration


Change data

Organization:

Node: Node 1

Type: Avaya selective

Abonent number: 10001

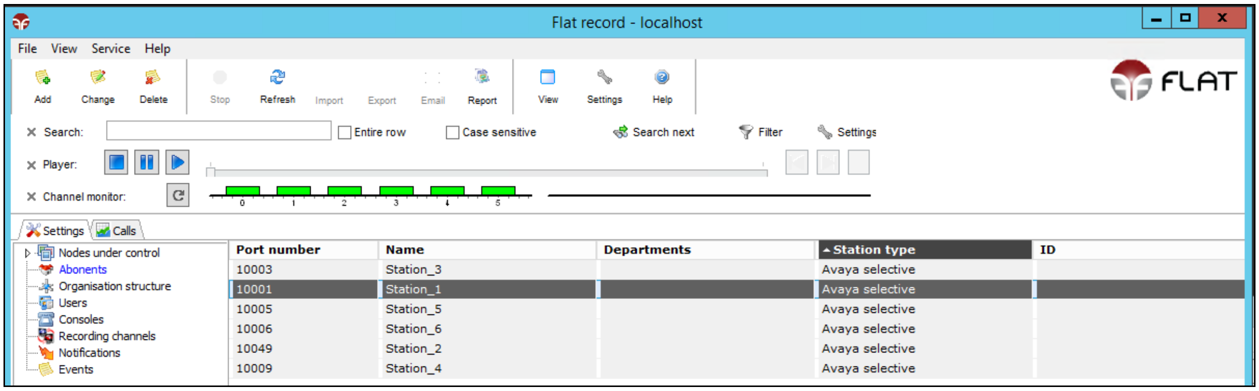
Abonent name: Station_1

Channel number: 0

Abonent ID:

☑ On control □ Stereo mode

The screen below shows the list of subscribers are setup for recording of conversation.



Port number	Name	Departments	Station type	ID
10003	Station_3		Avaya selective	
10001	Station_1		Avaya selective	
10005	Station_5		Avaya selective	
10006	Station_6		Avaya selective	
10049	Station_2		Avaya selective	
10009	Station_4		Avaya selective	

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 FLAT Record.

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

3     7        no    aes7x            established   15       15
```

Verify the registration status of the virtual IP softphones by using the **list registered-ip-stations** command. Verify that the virtual IP softphones from **Section 5.3** are displayed, as shown below.

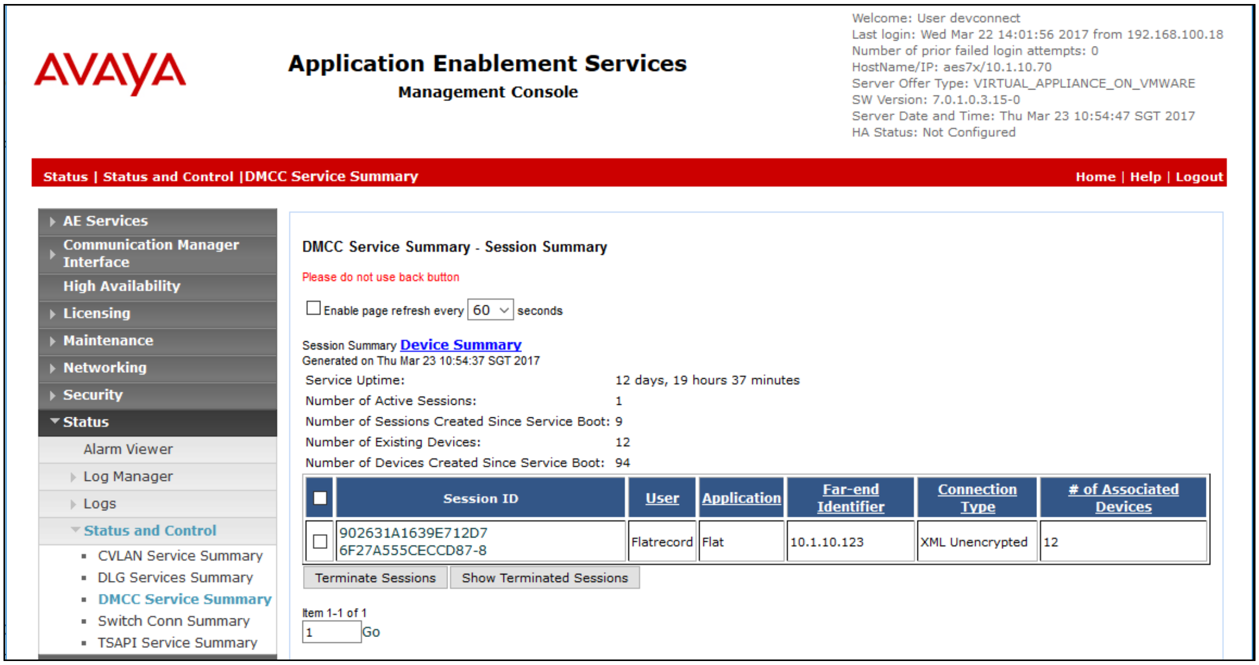
```
list registered-ip-stations ext 19901 count 5

                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/       Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ---------------------------------------
19901         4624      IP_API_A   tcp 10.1.10.70
                         1         3.2040         10.1.10.230
19902         4624      IP_API_A   tcp 10.1.10.70
              1         3.2040         10.1.10.230
19903         4624      IP_API_A   tcp 10.1.10.70
              1         3.2040         10.1.10.230
19904         4624      IP_API_A   tcp 10.1.10.70
              1         3.2040         10.1.10.230
19905         4624      IP_API_A   tcp 10.1.10.70
              1         3.2040         10.1.10.230
19906         4624      IP_API_A   tcp 10.1.10.70
              1         3.2040         10.1.10.230
```

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed. On the lower portion of the screen, verify that the **User** column shows an active session with the FLAT Record user name from **Section 6.8**, and that the **# of Associated Devices** column reflects the number of subscribers from **Section 7.3.3** plus the number of virtual softphones from **Section 5.3**.



Welcome: User devconnect
Last login: Wed Mar 22 14:01:56 2017 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: 7.0.1.0.3.15-0
Server Date and Time: Thu Mar 23 10:54:47 SGT 2017
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

□ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Thu Mar 23 10:54:37 SGT 2017

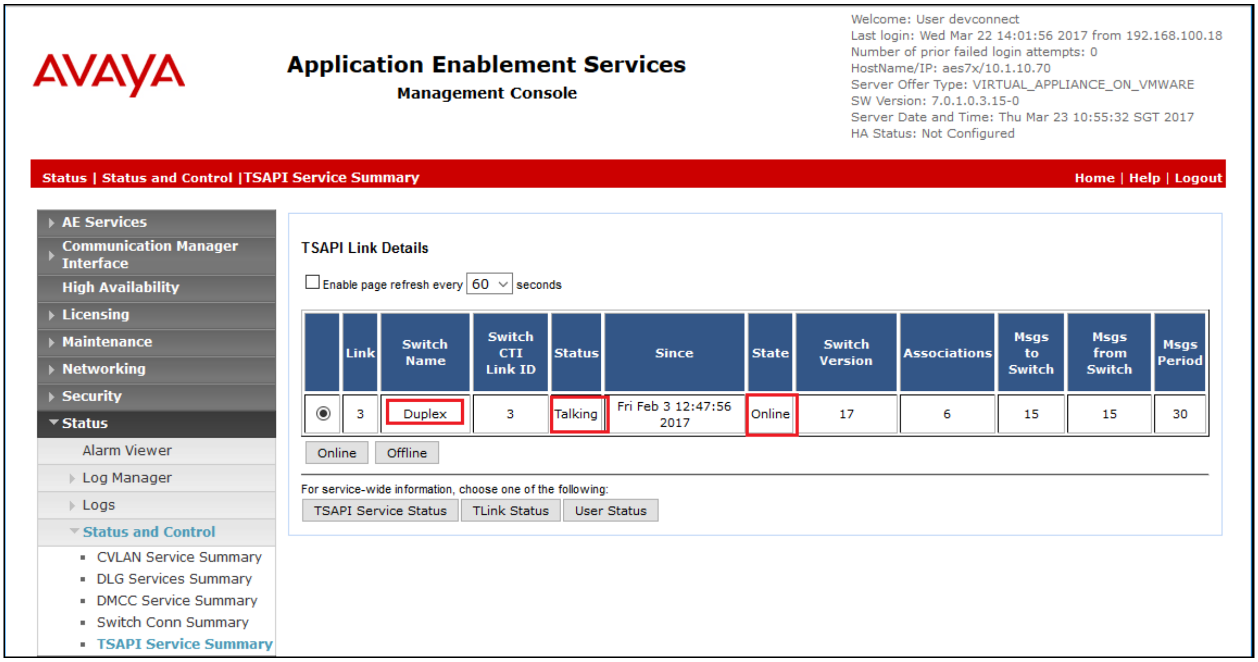
Service Uptime:	12 days, 19 hours 37 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	9
Number of Existing Devices:	12
Number of Devices Created Since Service Boot:	94

□	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	902631A1639E712D7 6F27A555CECCD87-8	Flatrecord	Flat	10.1.10.123	XML Unencrypted	12

Terminate Sessions | Show Terminated Sessions

Item 1-1 of 1
1 Go

Verify also the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed. On the lower portion of the screen, verify for the **Switch Name Duplex** that the **Status** column shows **Talking** state and the **State** column show that it is **Online**.



Welcome: User devconnect
Last login: Wed Mar 22 14:01:56 2017 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: 7.0.1.0.3.15-0
Server Date and Time: Thu Mar 23 10:55:32 SGT 2017
HA Status: Not Configured

TSAPI Link Details

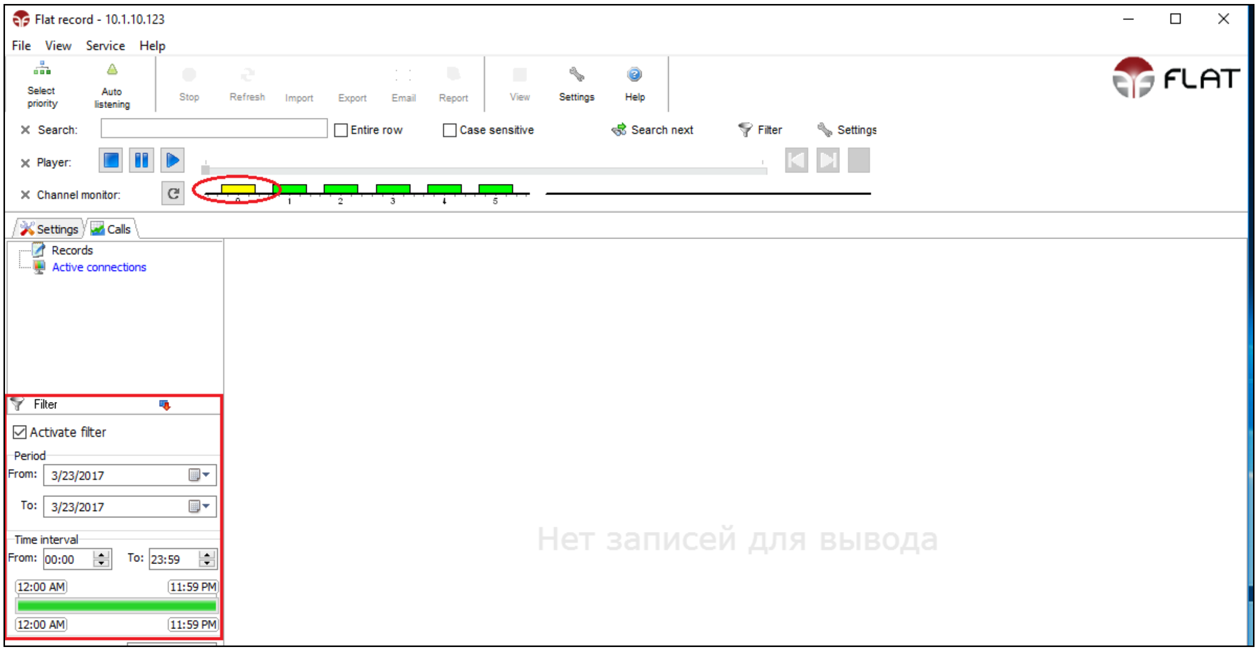
☐ Enable page refresh every 60 seconds

	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	Fri Feb 3 12:47:56 2017	Online	17	6	15	15	30

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

8.3. Verify FLAT Record

Make an inbound call to any of the subscriber. Verify the **channel monitor** shows the first channel available for recording turns yellow as below.



☐ Entire row ☐ Case sensitive

☑ Activate filter

Period

From: 3/23/2017

To: 3/23/2017

Time interval

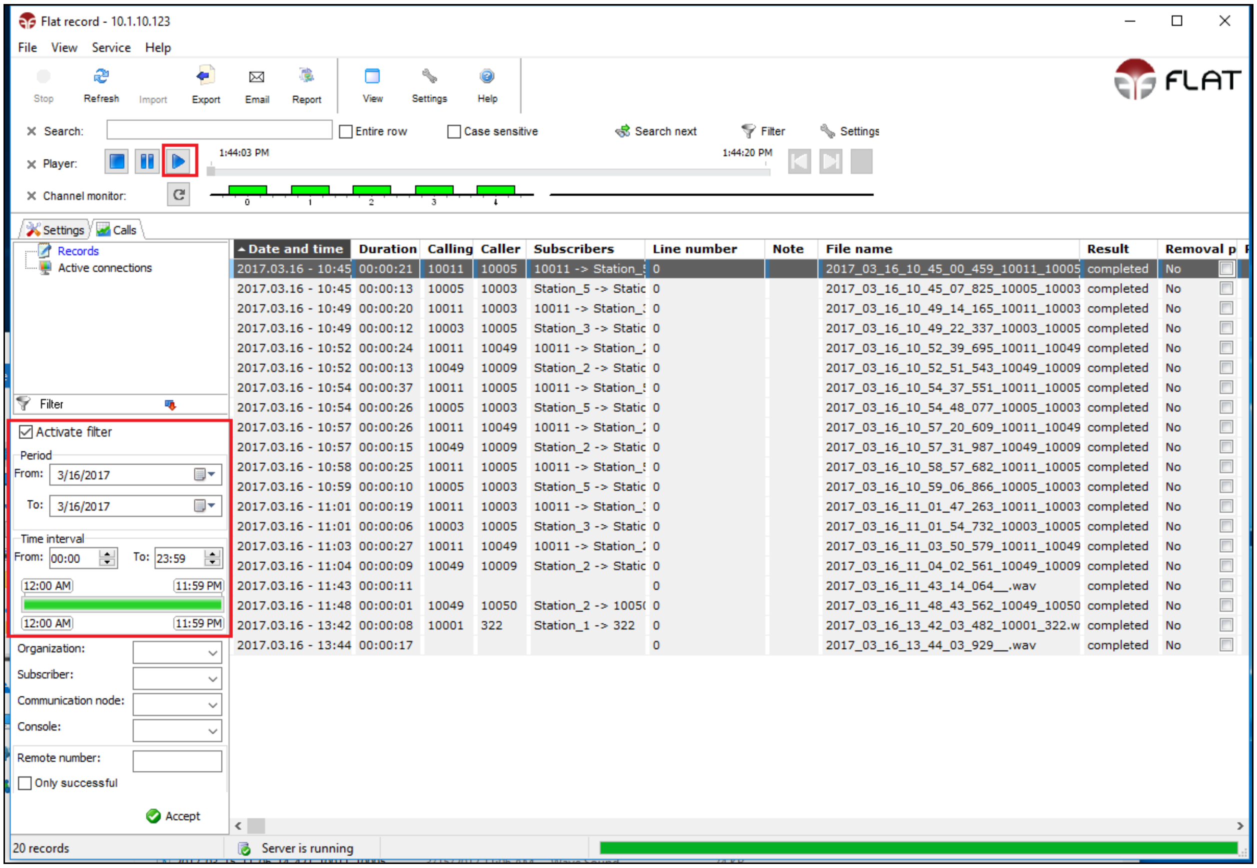
From: 00:00 To: 23:59

12:00 AM 11:59 PM

12:00 AM 11:59 PM

Нет записей для вывода

Make several more calls and check for each phone type that call recordings are collected and can be played back from the play button on the **Player**. Select **Calls** tab → **Records** and click **Activate filter** on the left pane with the appropriate **From** and **To Period/Time interval** before selecting **Accept** to see the records listed on the right pane.



☑ Activate filter

Period
From: 3/16/2017
To: 3/16/2017

Time interval
From: 00:00 To: 23:59
12:00 AM 11:59 PM
12:00 AM 11:59 PM

Organization:
Subscriber:
Communication node:
Console:
Remote number:
☐ Only successful

Accept

Date and time	Duration	Calling	Caller	Subscribers	Line number	Note	File name	Result	Removal p
2017.03.16 - 10:45	00:00:21	10011	10005	10011 -> Station_	0		2017_03_16_10_45_00_459_10011_10005	completed	No ☐
2017.03.16 - 10:45	00:00:13	10005	10003	Station_5 -> Static	0		2017_03_16_10_45_07_825_10005_10003	completed	No ☐
2017.03.16 - 10:49	00:00:20	10011	10003	10011 -> Station_	0		2017_03_16_10_49_14_165_10011_10003	completed	No ☐
2017.03.16 - 10:49	00:00:12	10003	10005	Station_3 -> Static	0		2017_03_16_10_49_22_337_10003_10005	completed	No ☐
2017.03.16 - 10:52	00:00:24	10011	10049	10011 -> Station_	0		2017_03_16_10_52_39_695_10011_10049	completed	No ☐
2017.03.16 - 10:52	00:00:13	10049	10009	Station_2 -> Static	0		2017_03_16_10_52_51_543_10049_10009	completed	No ☐
2017.03.16 - 10:54	00:00:37	10011	10005	10011 -> Station_	0		2017_03_16_10_54_37_551_10011_10005	completed	No ☐
2017.03.16 - 10:54	00:00:26	10005	10003	Station_5 -> Static	0		2017_03_16_10_54_48_077_10005_10003	completed	No ☐
2017.03.16 - 10:57	00:00:26	10011	10049	10011 -> Station_	0		2017_03_16_10_57_20_609_10011_10049	completed	No ☐
2017.03.16 - 10:57	00:00:15	10049	10009	Station_2 -> Static	0		2017_03_16_10_57_31_987_10049_10009	completed	No ☐
2017.03.16 - 10:58	00:00:25	10011	10005	10011 -> Station_	0		2017_03_16_10_58_57_682_10011_10005	completed	No ☐
2017.03.16 - 10:59	00:00:10	10005	10003	Station_5 -> Static	0		2017_03_16_10_59_06_866_10005_10003	completed	No ☐
2017.03.16 - 11:01	00:00:19	10011	10003	10011 -> Station_	0		2017_03_16_11_01_47_263_10011_10003	completed	No ☐
2017.03.16 - 11:01	00:00:06	10003	10005	Station_3 -> Static	0		2017_03_16_11_01_54_732_10003_10005	completed	No ☐
2017.03.16 - 11:03	00:00:27	10011	10049	10011 -> Station_	0		2017_03_16_11_03_50_579_10011_10049	completed	No ☐
2017.03.16 - 11:04	00:00:09	10049	10009	Station_2 -> Static	0		2017_03_16_11_04_02_561_10049_10009	completed	No ☐
2017.03.16 - 11:43	00:00:11				0		2017_03_16_11_43_14_064__.wav	completed	No ☐
2017.03.16 - 11:48	00:00:01	10049	10050	Station_2 -> 1005(	0		2017_03_16_11_48_43_562_10049_10050	completed	No ☐
2017.03.16 - 13:42	00:00:08	10001	322	Station_1 -> 322	0		2017_03_16_13_42_03_482_10001_322.w	completed	No ☐
2017.03.16 - 13:44	00:00:17				0		2017_03_16_13_44_03_929__.wav	completed	No ☐

20 records
Server is running

9. Conclusion

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

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*, Document 03-300509, Issue 2.1, Release 7.0.1, August 2016.
[2] *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016.

The following FLAT Record documentation can be obtained from member.
[3] *FLAT Record – Guidelines for establishing connection to Avaya Aura*, 2016.
[4] *FLAT Record – Installation and Configuration Manual*, 2016.

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.