



Application Notes for TeleSvyaz FLAT Record 3.1 with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 for selective recording using Single Step Conference – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for FLAT Record 3.1 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 for selective recording using Single Step Conference.

In the compliance testing, FLAT Record used Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to monitor agent stations on Avaya Aura® Communication Manager, and obtain call information and media associated with the monitored stations 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 3.1 to interoperate with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 for selective recording using Single Step Conference.

In the compliance testing, FLAT Record used Avaya Aura® Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface to monitor agent 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 two 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. FLAT client application is installed on a PC to administer the recording channels and monitoring stations.

The feature and serviceability test cases were performed manually. Upon start of the FLAT Record application, it uses DMCC to automatically register the virtual IP softphones to Communication Manager and request monitoring on the agent stations 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 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 utilized enabled capabilities of TLS.

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:

- Handling of DMCC messages in areas of event notification.
- Use of DMCC services to register virtual IP softphones against the agent stations, and to obtain the media for call recording.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711, long duration, multiple calls, multiple agents, conference, and transfer.

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.
- Calls that are setup during LAN disconnection to the Flat Record server does not have call information in the call recording after LAN is reconnected.

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. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of this Application Notes and will not be described.

In the compliance testing, Flat Record monitored the skill groups and agent stations shown in the table below.

Device Type	Extension
VDN	14001
Skill Group	13001
Supervisor	10001 (9641G H.323)
Agent Station	10003 (9608 H.323), 10005 (1408 DCP), 10007 (J179 H.323), 10049 (9641 SIP) 10053 (J189 SIP)
Agent ID	11001 - 11006

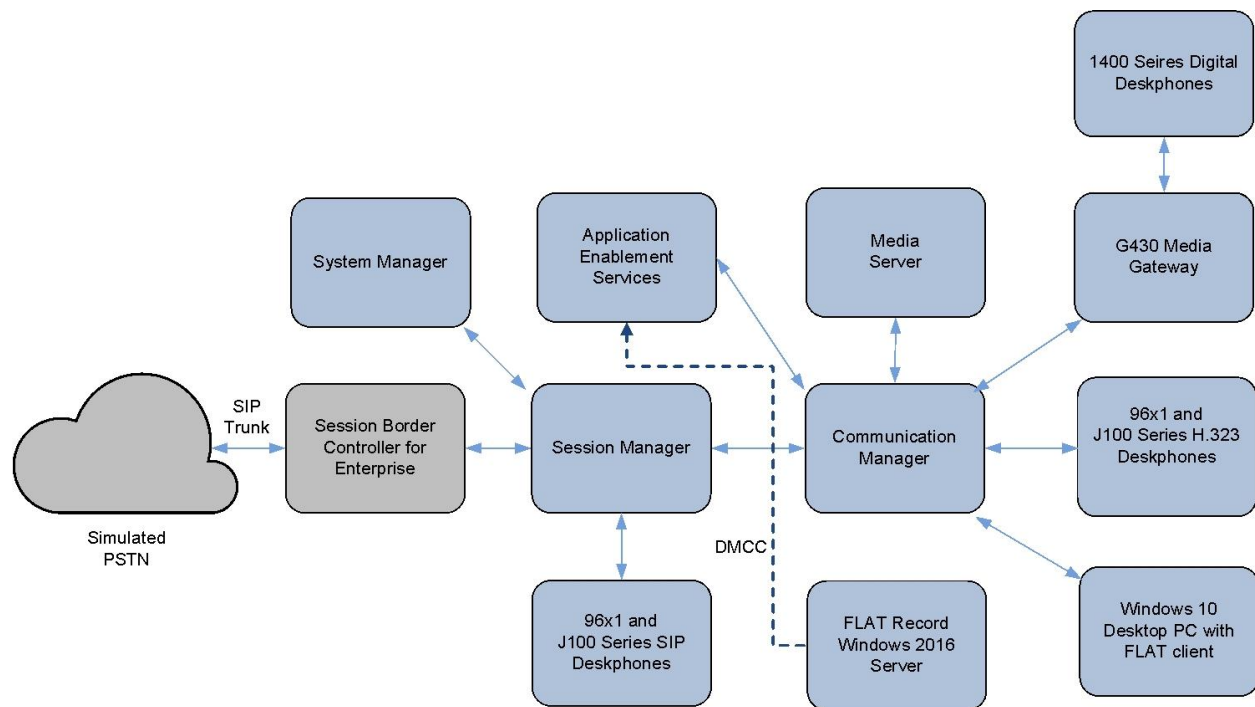


Figure 1: Test Configuration

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 in Virtual Environment	8.1.3 (8.1.3.0.0.890.26568)
Avaya G430 Media Gateway: <ul style="list-style-type: none">• MGP• MM712AP (DCP)	41.34.1 HW04 FW015
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.2 (8.1.2.1.0.6-0)
Avaya Aura® System Manager in Virtual Environment	8.1.3 (8.1.3.0.1011893)
Avaya Aura® Session Manager in Virtual Environment	8.1.3 (8.1.3.0.813014)
Avaya Aura® Media Server in Virtual Environment	8.0.2.138
Avaya 96x1 Series IP Phones: <ul style="list-style-type: none">• H.323• SIP	6.8304 7.1.9.0.8
Avaya J100 Series IP Phones: <ul style="list-style-type: none">• H.323• SIP	6.8304 4.0.7.0.7
Avaya 1400 Series Digital Phones	Release 4 SP 10
FLAT Record client running on a PC using Windows 10 Pro	3.1
FLAT Record as an application on Windows Server 2016 in Virtual Environment DMCC XML 7.1	3.1 Standard

5. Configure Avaya Aura® Communication Manager

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

- Verify Communication Manager License
- Administer CTI link
- Administer IP Codecs
- Administer Virtual IP softphones
- Administer agent 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)? y           Authorization Codes? y
Analog Trunk Incoming Call ID? y           CAS Branch? n
A/D Grp/Sys List Dialing Start at 01? y    CAS Main? n
Answer Supervision by Call Classifier? y    Change COR by FAC? n
ARS? y      Computer Telephony Adjunct Links? y
ARS/AAR Partitioning? y      Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC? n      DCS (Basic)? y
ASAI Link Core Capabilities? y      DCS Call Coverage? y
ASAI Link Plus Capabilities? y      DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n      Digital Loss Plan Modification? y
Async. Transfer Mode (ATM) Trunking? n      DS1 MSP? y
ATM WAN Spare Processor? n      DS1 Echo Cancellation? y
ATMS? y
Attendant Vectoring? y

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

5.2. Administer CTI Link

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

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

5.3. Administer IP Codecs

Use the **change ip-codec-set n** command, where **n** is an existing codec set number. For customer network that use encrypted media, make certain that **none** is included for **Media Encryption**, and that **Encrypted SRTP** is set to **best-effort**, these settings are needed for support of non-encrypted media from the virtual IP softphones used by Flat Record.

In the compliance testing, this IP codec set was assigned to the agent stations. G.711 is the only supported codec by FLAT Record.

```
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.711A      n         2       20
2:
3:
4:
5:
6:
7:
Media Encryption      Encrypted SRTP: best-effort
1: 1-srtp-aescm128-hmac80
2: aes
3: none
4:
5:
```


5.4. 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 **9640**.
- **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 19902                                     Page 1 of 6
                                                    STATION
Extension: 19902                                     Lock Messages? n          BCC: 0
  Type: 9640                                           Security Code: *****   TN: 1
  Port: IP                                             Coverage Path 1:          COR: 1
  Name: DMCC #2                                       Coverage Path 2:          COS: 1
                                                    Hunt-to Station:         Tests? y

STATION OPTIONS
    Loss Group: 19                                     Time of Day Lock Table:
    Speakerphone: 2-way                               Personalized Ringing Pattern: 1
    Display Language: english                         Message Lamp Ext: 19902
    Survivable GK Node Name:                          Mute Button Enabled? y
    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, five virtual IP softphones were administered as shown below.

```

list station 19902 count 5
                                                    STATIONS
Ext/      Port/   Name/      Room/      Cv1/  COR/
Hunt-to   Type     Surv GK NN  Move  Cable  Jack  Cv2  COS  TN
19902     S000006 DMCC #2                1
9640                        no                1  1
19903     S000007 DMCC #3                1
9640                        no                1  1
19904     S000008 DMCC #4                1
9640                        no                1  1
19905     S000011 DMCC #5                1
9640                        no                1  1
19906     S000042 DMCC #6                1
9640                        no                1  1
  
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

6.1. 7.1. Launch System Manager

Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using 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.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

6.2. Administer Users

In the subsequent screen (not shown), select **Users → User Management**. Select **User Management → Manage Users** from the left pane to display the screen below. Select the entry associated with the first SIP agent station from **Section 3**, in this case “10049”, and click **Edit**.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search admin

Home / User Management

User Management ▾

- Manage Users
- Public Contacts
- Shared Addresses
- System Presence ACLs

Home / Users / Manage Users

Search

	First Name ▾	Surname ▾	Display Name ▾	Login Name ▾	SIP Handle ▾
<input type="checkbox"/>	SIP10048	AVAYA	AVAYA, SIP10048	10048@sglab.com	+10048
<input checked="" type="checkbox"/>	SIP10049	AVAYA	AVAYA, SIP10049	10049@sglab.com	+10049

The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Click on the **Editor** icon shown below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, "Aura® System Manager 8.1", and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and user name "admin" are also present. The left sidebar shows the "User Management" menu with options like "Manage Users", "Public Contacts", "Shared Addresses", "System Presence ACLs", and "Communication Profil...". The main content area is titled "User Profile | Edit | 10049@sglab.com" and features tabs for Identity, Communication Profile, Membership, and Contacts. The "Communication Profile" tab is active, showing a "Communication Profile Password" section and a "PROFILES" list with "CM Endpoint Profile" selected. The "CM Endpoint Profile" is highlighted in blue. The "Use Existing Endpoints" checkbox is unchecked. The "Template" field is "Start typing...". The "Security Code" field is "Enter Security Code". The "Voice Mail Number" field is "10000". The "Calculate Route Pattern" checkbox is unchecked. The "System" dropdown is "DuplexCM". The "Profile Type" dropdown is "Endpoint". The "Extension" field is "10049" with a red circle around the editor icon. The "Set Type" field is "9641SIPCC". The "Port" field is "S000138". The "Preferred Handle" field is "10049@sglab.com". The "Sip Trunk" field is "aar".

In the popped up screen, select the **General Options** tab and locate the **Type of 3PCC Enabled** parameter, and select “Avaya” from the drop-down list as shown below. Retain the existing values in the remaining fields.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows 'User Management' with options like 'Manage Users', 'Public Contacts', 'Shared Addresses', 'System Presence ACLs', and 'Communication Profil...'. The main content area is titled 'User Profile | Edit | 10049@sglab.com' and includes buttons for 'Commit & Continue', 'Commit', and 'Cancel'. Below this, the 'Edit Endpoint' section is visible, with a 'Done' button and a '[Save As Template]' link. The 'General Options (G)' sub-tab is active, showing fields for 'Class of Restriction (COR)', 'Emergency Location Ext', 'Tenant Number', 'SIP Trunk', 'Coverage Path 1', 'Lock Message', 'Multibyte Language', 'Class Of Service (COS)', 'Message Lamp Ext.', 'Type of 3PCC Enabled' (highlighted with a red box and set to 'Avaya'), 'Coverage Path 2', 'Localized Display Name', and 'Enable Reachability for Station Domain Control'.

System	DuplexCM	Extension	10049
Template	Select	Set Type	9641SIPCC
Port	S000138	Security Code	
Name	AVAYA, SIP10049		

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)		Enhanced Call Fwd (E)	
Button Assignment (B)		Profile Settings (P)		Group Membership (M)					
* Class of Restriction (COR)	1	* Class Of Service (COS)	1						
* Emergency Location Ext	10049	* Message Lamp Ext.	10049						
* Tenant Number	1								
* SIP Trunk	Qaar	Type of 3PCC Enabled	Avaya						
Coverage Path 1	99	Coverage Path 2							
Lock Message	<input type="checkbox"/>	Localized Display Name	AVAYA, SIP10049						
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system						

7. Configure Avaya Aura® Application Enablement Services

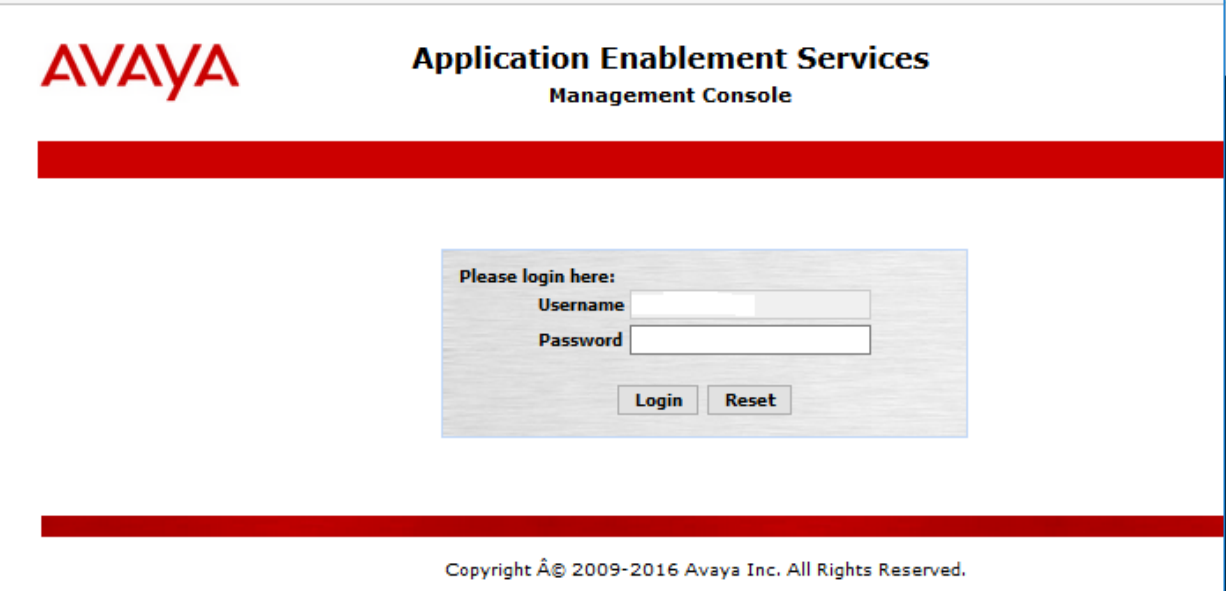
This section provides the procedures for configuring AES Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- 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

7.1. 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.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A thick red horizontal bar spans the width of the page below the header. In the center, there is a login box with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below the input fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located at the bottom of the page, above the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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



Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Dec 22 15:17:09 2020 from 10.1.10.99
Number of prior failed login attempts: 0
HostName/IP: aes/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.0.6-0
Server Date and Time: Wed Dec 23 16:12:20 SGT 2020
HA Status: Not Configured

Home

Home | Help | Logout

» AE Services

» Communication Manager Interface

» High Availability

» Licensing

» Maintenance

» Networking

» Security

» Status

» User Management

» Utilities

» Help

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.

7.2. Verify License

Select **Licensing → WebLM Server Access** from the left pane of the home screen and **Avaya WebLM** screen pops up (not shown). Depending on where the WebLM is hosted, the next screen will be similar.

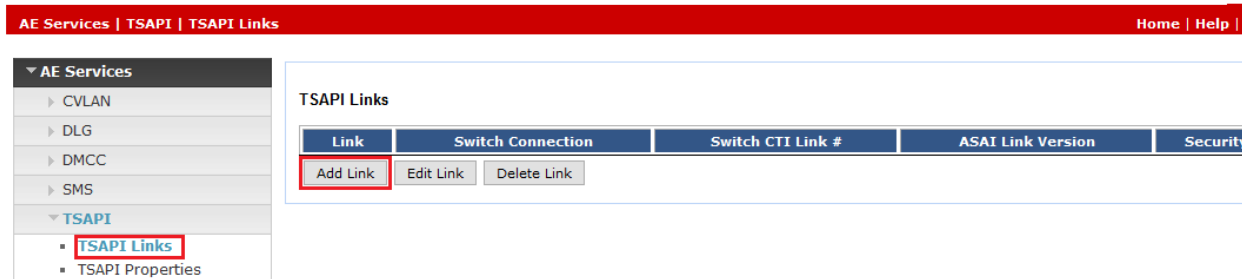
Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane to display the **Licensed Features** screen in the right pane. Scroll down the screen, and verify that there are sufficient licenses for **Device Media and Call Control** and **TSAPI Simultaneous Users**, as shown below.

WebLM Home	Application Enablement (CTI) - Release: 8 - SID: 10503000
Install license	You are here: Licensed Products > Application_Enablement > View License Capacity
Licensed products	License installed on: May 13, 2020 2:06:31 PM +08:00
APPL_ENAB	
▼ Application_Enablement	
View license capacity	License File Host IDs: V6-BB-8E-6F-89-B6-01
View peak usage	
CE	Licensed Features
►COLLABORATION_ENVIRONMENT	
MESSAGING	13 Items Show All
►Messaging	
POM	
►POM	
SYSTEM_MANAGER	
►System_Manager	
SessionManager	
►SessionManager	
VDIA	
►VDIA	
VSS	
►Voice_Portal	
Uninstall license	
Server properties	
Metering Collector Configuration	
Shortcuts	
Help for Licensed products	

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

7.3. Administer TSAPI Link

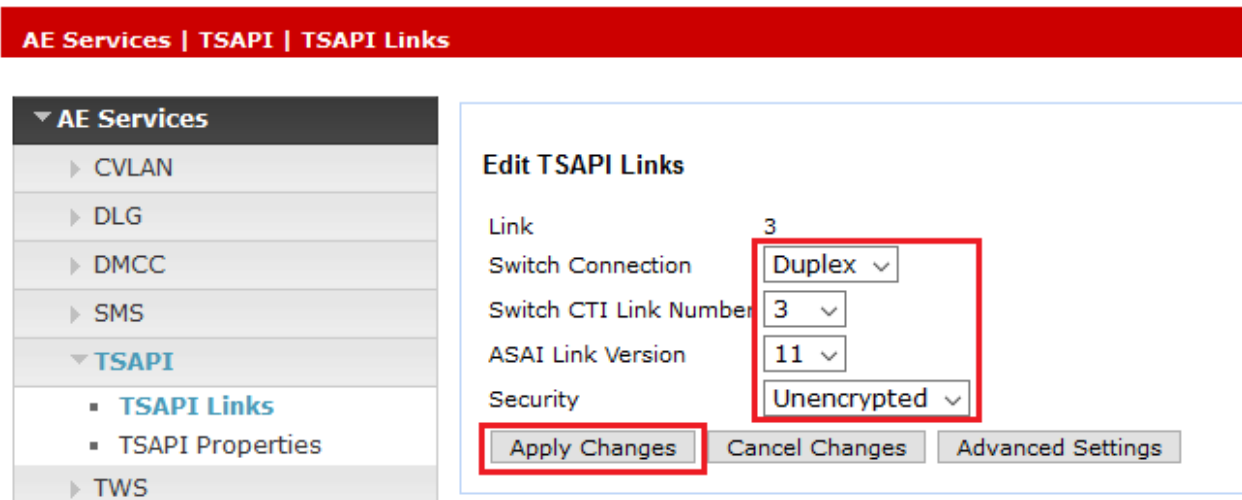
To administer a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



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

- **Link:** Select an available Link number from 1 to 16.
- **Switch Connection:** Select switch connection administered.
- **Switch CTI Link Number:** Corresponding CTI link number in **Section 5.2**.
- **ASAI Link Version:** Set to **11** for the latest version.
- **Security:** Select *Unencrypted* for the link.

Click **Apply Changes**.



7.4. 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**.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> Duplex	Yes	30	1

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

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**.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance
Networking

Edit H.323 Gatekeeper - Duplex

10.1.10.230 Add Name or IP

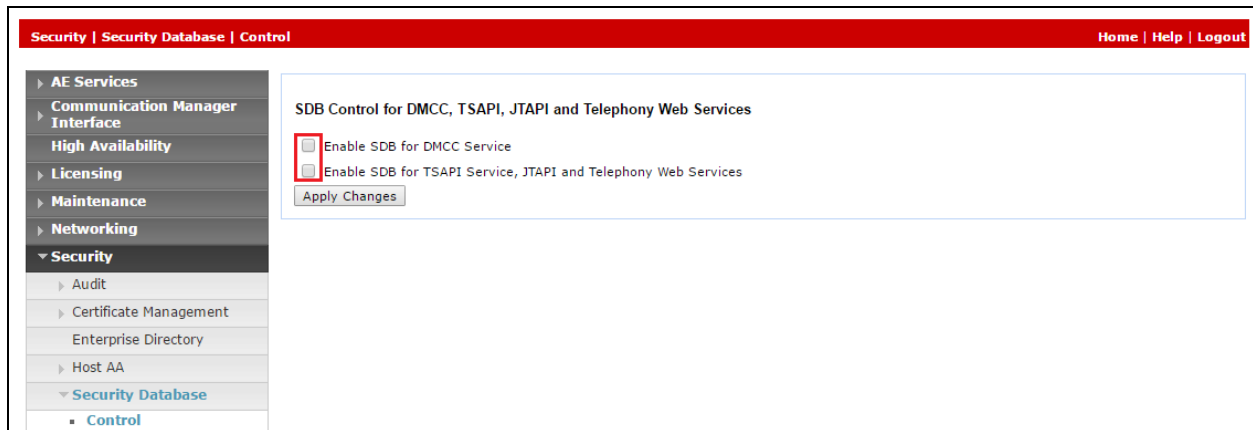
Name or IP Address

Delete IP

7.5. Disable Security Database

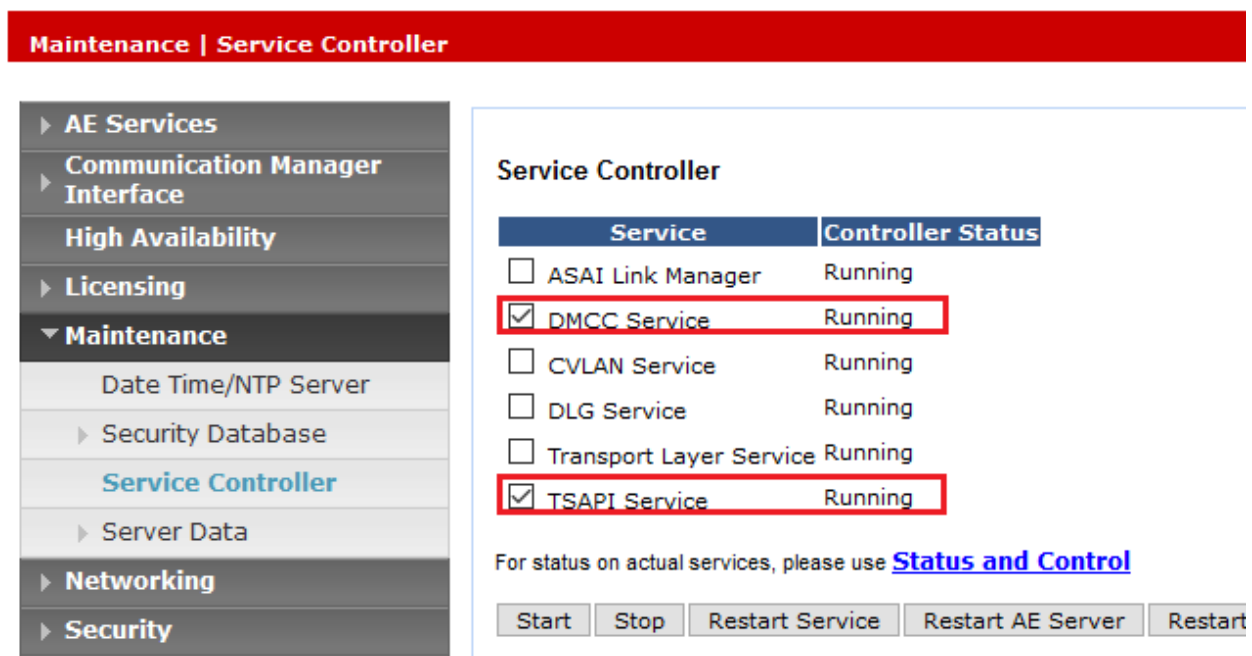
Select **Security** → **Security Database** → **Control** from the left pane to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Make certain that both parameters are unchecked, as shown below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the Flat Record user from **Section 7.7**.



7.6. 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**.



7.7. 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).

The screenshot shows the 'Add User' form within the 'User Management' application. The left sidebar contains a navigation menu with categories like 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Service Admin', 'User Admin', 'Utilities', and 'Help'. The 'User Admin' section is expanded, showing 'Add User' as the selected option. The main content area is titled 'Add User' and contains a form with the following fields: 'User Id' (text input, value: Flatrecord), 'Common Name' (text input, value: Flatrecord), 'Surname' (text input, value: Flatrecord), 'User Password' (password input), 'Confirm Password' (password input), 'Admin Note' (text area), 'Avaya Role' (dropdown menu, value: None), 'Business Category' (text input), 'Car License' (text input), 'CM Home' (text input), 'Css Home' (text input), 'CT User' (dropdown menu, value: Yes), 'Department Number' (text input), 'Display Name' (text input), and 'Employee Number' (text input). A red box highlights the 'User Id', 'Common Name', 'Surname', 'User Password', 'Confirm Password', 'Avaya Role', and 'CT User' fields. A note at the top of the form states 'Fields marked with * can not be empty'.

User Management | User Admin | Add User Home | Help | Logout

Add User

Fields marked with * can not be empty.

* User Id: Flatrecord

* Common Name: Flatrecord

* Surname: Flatrecord

* User Password: [password input]

* Confirm Password: [password input]

Admin Note: [text area]

Avaya Role: None

Business Category: [text input]

Car License: [text input]

CM Home: [text input]

Css Home: [text input]

CT User: Yes

Department Number: [text input]

Display Name: [text input]

Employee Number: [text input]

7.8. 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.

Networking | Ports

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

Enabled Disabled

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

☒ ☐

LYM; Reviewed:
SPOC 1/27/2021

Solution & Interoperability Test Lab Application Notes
©2021 Avaya Inc. All Rights Reserved.

20 of 34
FLATRecord_AES8

8. Configure FLAT Record

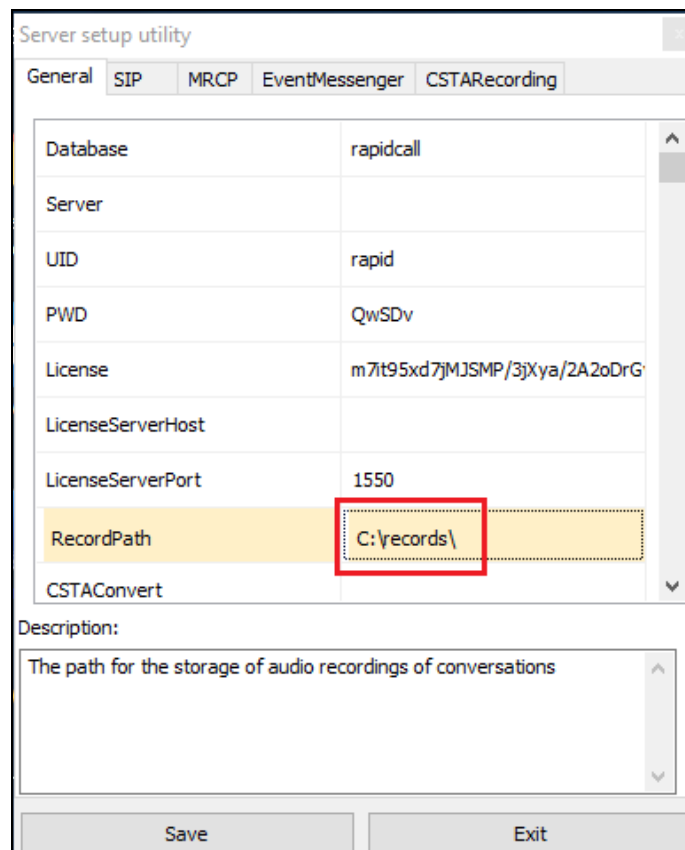
This section provides the procedures for configuring FLAT Record. The procedures include the following areas:

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

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.

8.1. 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:\records**”.



Server setup utility

General SIP MRCP EventMessenger CSTARRecording

Database	rapidcall
Server	
UID	rapid
PWD	QwSDv
License	m7it95xd7jMJSMP/3jXya/2A2oDrG
LicenseServerHost	
LicenseServerPort	1550
RecordPath	C:\records\
CSTAConvert	

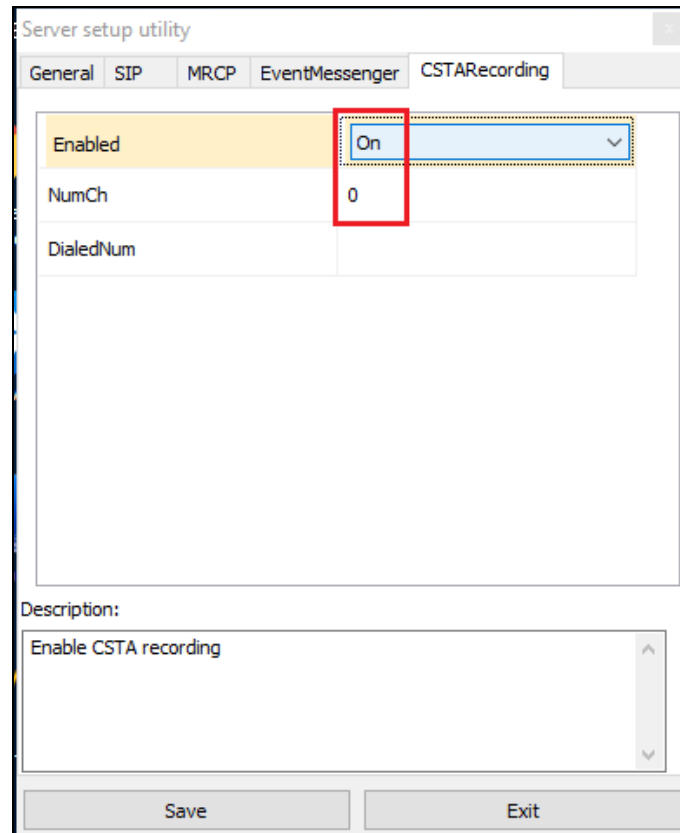
Description:

The path for the storage of audio recordings of conversations

Save Exit

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**



The screenshot shows the 'Server setup utility' window with the 'CSTARecording' tab selected. The 'Enabled' dropdown is set to 'On' and the 'NumCh' field is set to '0'. Both are highlighted with red boxes. The 'DialNum' field is empty. The 'Description' text area contains 'Enable CSTA recording'. At the bottom are 'Save' and 'Exit' buttons.

Parameter	Value
Enabled	On
NumCh	0
DialNum	

Description:
Enable CSTA recording

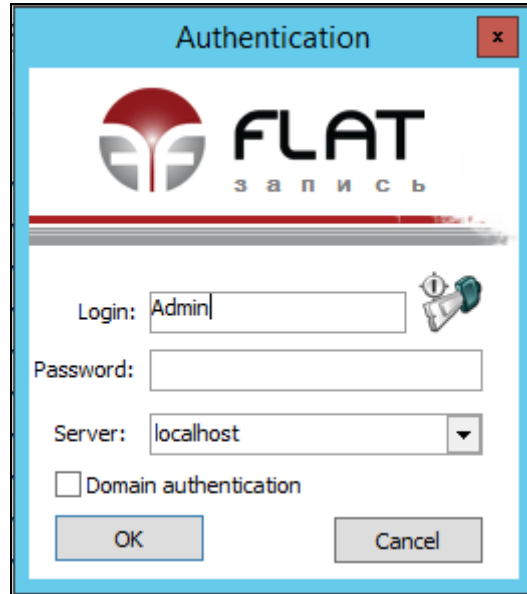
Save Exit

8.2. Using FLAT Client for Configuration

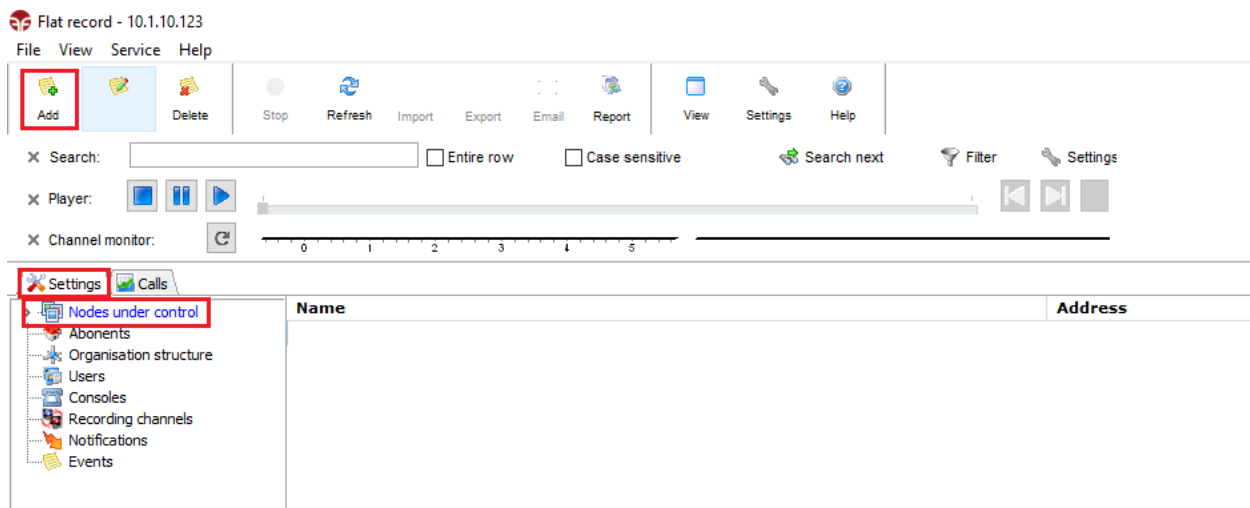
This section documents the setup of the connection to AES using the FLAT client and administering the recording channels and monitoring stations.

8.2.1. 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.

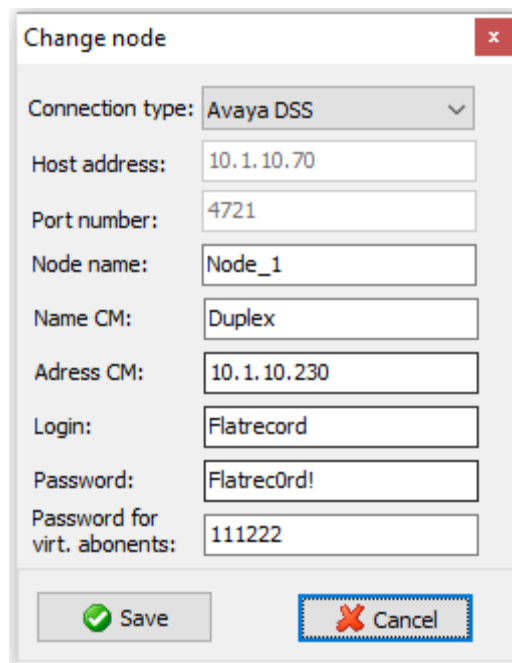


From the home screen, select **Settings → Nodes under control** and click **Add** icon on the top left.



Select from the **Connection type** drop down menu, **Avaya DSS** and configure the parameters as below. Below is a screen capture of the setup.

- **Host address:** AES IP address i.e., **10.1.10.70**.
- **Port number:** AES DMCC unencrypted port number i.e., **4721** in **Section 7.8**.
- **Node name:** Provide an appropriate name.
- **Name CM:** Communication Manager switch connection name.
- **Address CM:** Communication Manager IP address i.e., **10.1.10.230**.
- **Login:** AES CT User login name created in **Section 7.7**.
- **Password:** AES CT User password created in **Section 7.7**.
- **Password for virt. abonents:** Virtual stations password created in **Section 5.4**.



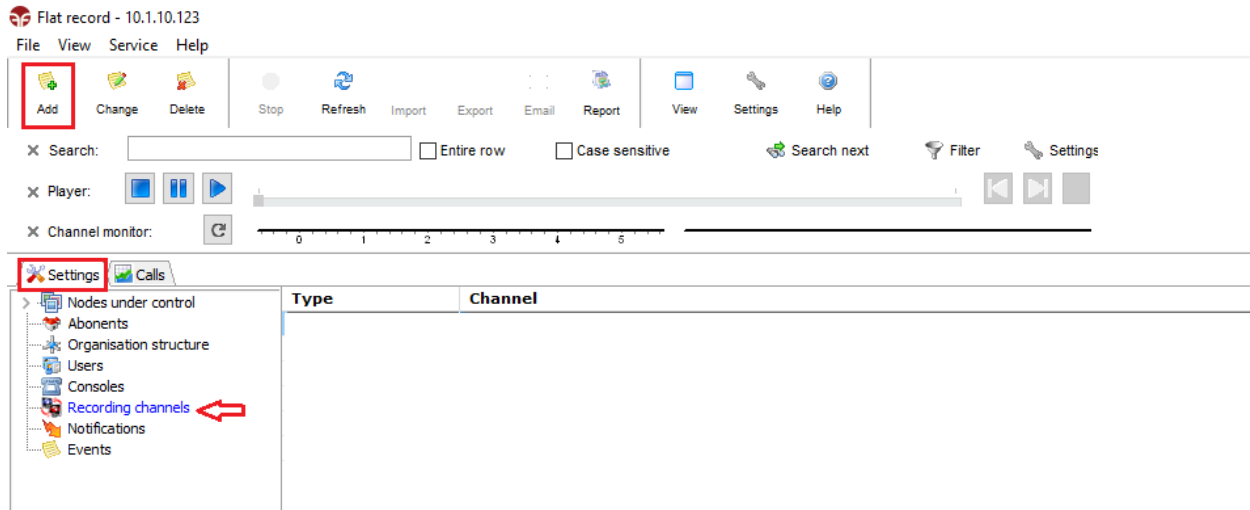
The screenshot shows a 'Change node' dialog box with the following fields and values:

Field	Value
Connection type:	Avaya DSS
Host address:	10.1.10.70
Port number:	4721
Node name:	Node_1
Name CM:	Duplex
Adress CM:	10.1.10.230
Login:	Flatrecord
Password:	Flatrec0rd!
Password for virt. abonents:	111222

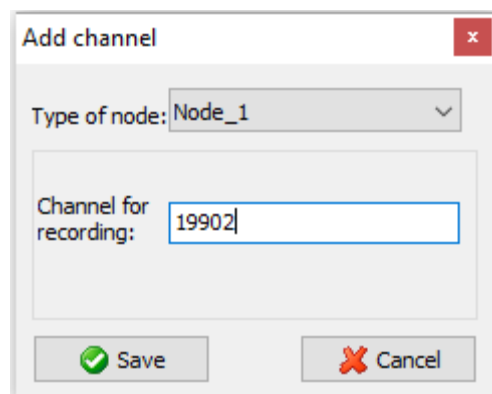
At the bottom, there are two buttons: 'Save' (with a green checkmark icon) and 'Cancel' (with a red X icon).

8.2.2. Add Recording Channels

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



Select the node name created in **Section 8.2.1** and enter the **Channel for recording** for the first virtual stations created in **Section 5.4**. Click **Save** after completion. Repeat for the rest of the channels.



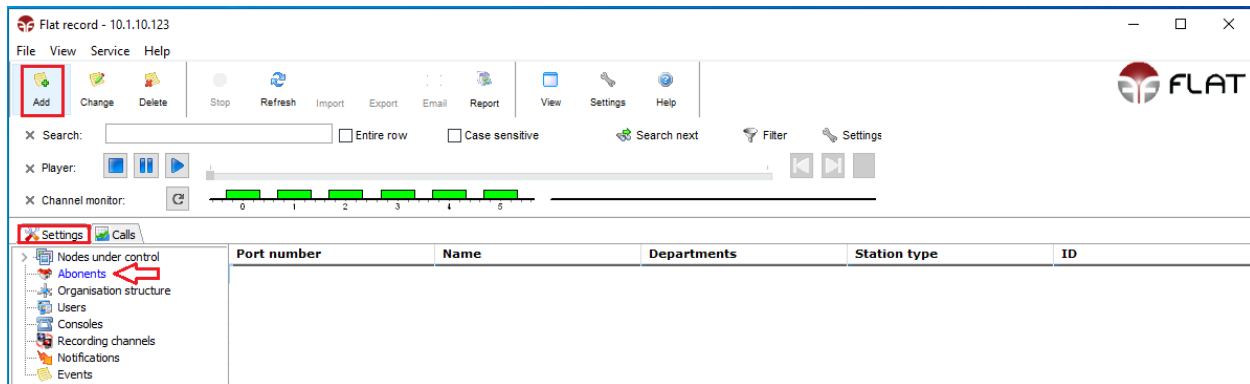
The screen below shows the list of recording channels setup for **19902 – 19907**. The green color for each channel in the **Channel monitor** indicates that each channel is able to successfully register. These channel turns yellow when it is recording.

The screenshot displays the Channel Monitor interface. At the top, there is a toolbar with icons for Add, Change, Delete, Stop, Refresh, Import, Export, Email, Report, View, Settings, and Help. Below the toolbar, there is a search bar with a search icon and a search next icon. The search bar contains the text "X Search:". To the right of the search bar are checkboxes for "Entire row" and "Case sensitive". Below the search bar, there is a "Player" section with a play button and a volume slider. To the right of the player is a "Channel monitor" section with a refresh icon and a bar chart showing six green bars, indicating that all channels are successfully registered. Below the channel monitor, there is a table with two columns: "Type" and "Channel". The table lists six channels, all of which are of type "Node_1". The channels are 19902, 19903, 19904, 19905, 19907, and 19906. The first row (Node_1, 19902) is highlighted with a red border.

Type	Channel
Node_1	19902
Node_1	19903
Node_1	19904
Node_1	19905
Node_1	19907
Node_1	19906

8.2.3. Enable Recording for Stations

From the home screen, select **Settings** → **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 8.3.1**.
- **Type:** Select **Avaya selective**.
- **Abonent number:** Enter the first agent station in **Section 3**.
- **Abonent name:** Enter the first agent station number or 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.

Adding port

Organization:

Node:

Type:

Abonent number:

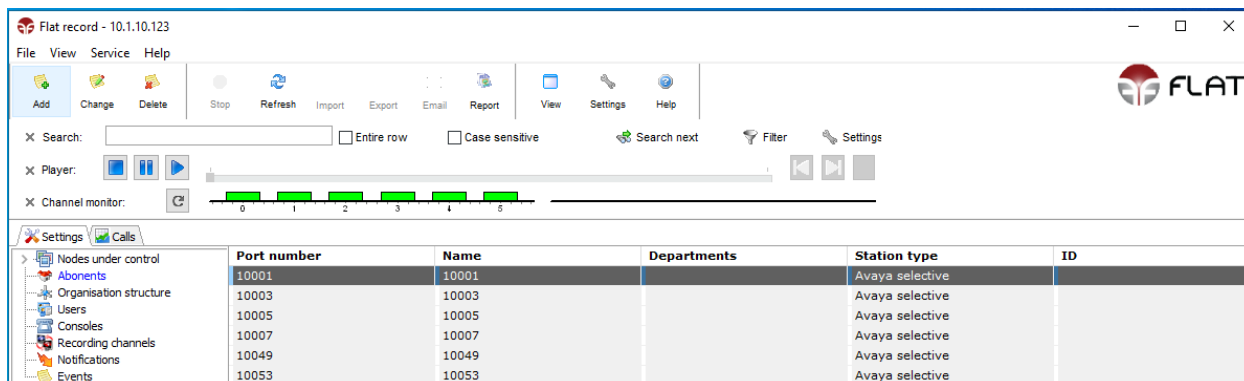
Abonent name:

Channel number:

Abonent ID:

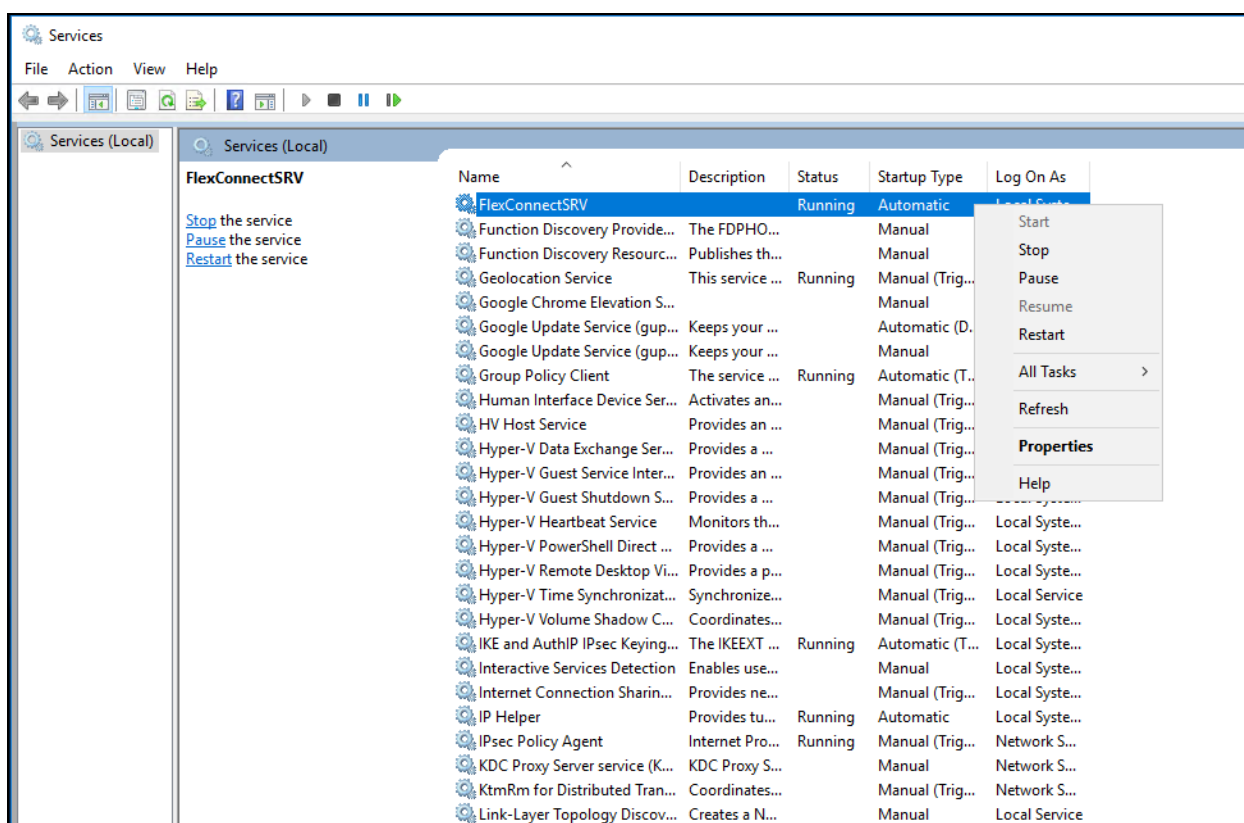
☒ On control ☐ Stereo mode

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



8.3. Restart Services

After configuring the recording channels and stations with FLAT client application in **Section 8.2**, restart the **FlexConnectSRV** service by selecting **Start → Apps → Administrative Tools → Services** to display the **Services (Local)** screen. Right-click on the service and select **Restart**.



9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and FLAT Record.

9.1. Verify Avaya Aura® Communication Manager

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

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
3	11	no	aes	established	1797	1797

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 5.4** are displayed, as shown below.

```
list registered-ip-stations ext 19902 count 6
```

REGISTERED IP STATIONS			
Station Ext or Orig Port Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address
19902	9640	IP_API_A	10.1.10.70
tls	1	3.2040	10.1.10.230
19903	9640	IP_API_A	10.1.10.70
tls	1	3.2040	10.1.10.230
19904	9640	IP_API_A	10.1.10.70
tls	1	3.2040	10.1.10.230
19905	9640	IP_API_A	10.1.10.70
tls	1	3.2040	10.1.10.230
19906	9640	IP_API_A	10.1.10.70
tls	1	3.2040	10.1.10.230
19907	9640	IP_API_A	10.1.10.70
tls	1	3.2040	10.1.10.230

9.2. 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 7.7**, and that the **# of Associated Devices** column reflects the number of stations from **Section 8.2.3** plus the number of virtual softphones from **Section 5.4**.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Tue Dec 22 11:37:28 2020 from 10.1.10.152
Number of prior failed login attempts: 2
HostName/IP: aes/10.1.10.70
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.0.6-0
Server Date and Time: Tue Dec 22 15:19:08 SGT 2020
HA Status: Not Configured

Status | Status and Control | DMCC Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ **DMCC Service Summary**

■ Switch Conn Summary

■ TSAPI Service Summary

▶ User Management

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Tue Dec 22 15:19:03 SGT 2020

Service Uptime: 0 days, 0 hours 29 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 1

Number of Existing Devices: 12

Number of Devices Created Since Service Boot: 12

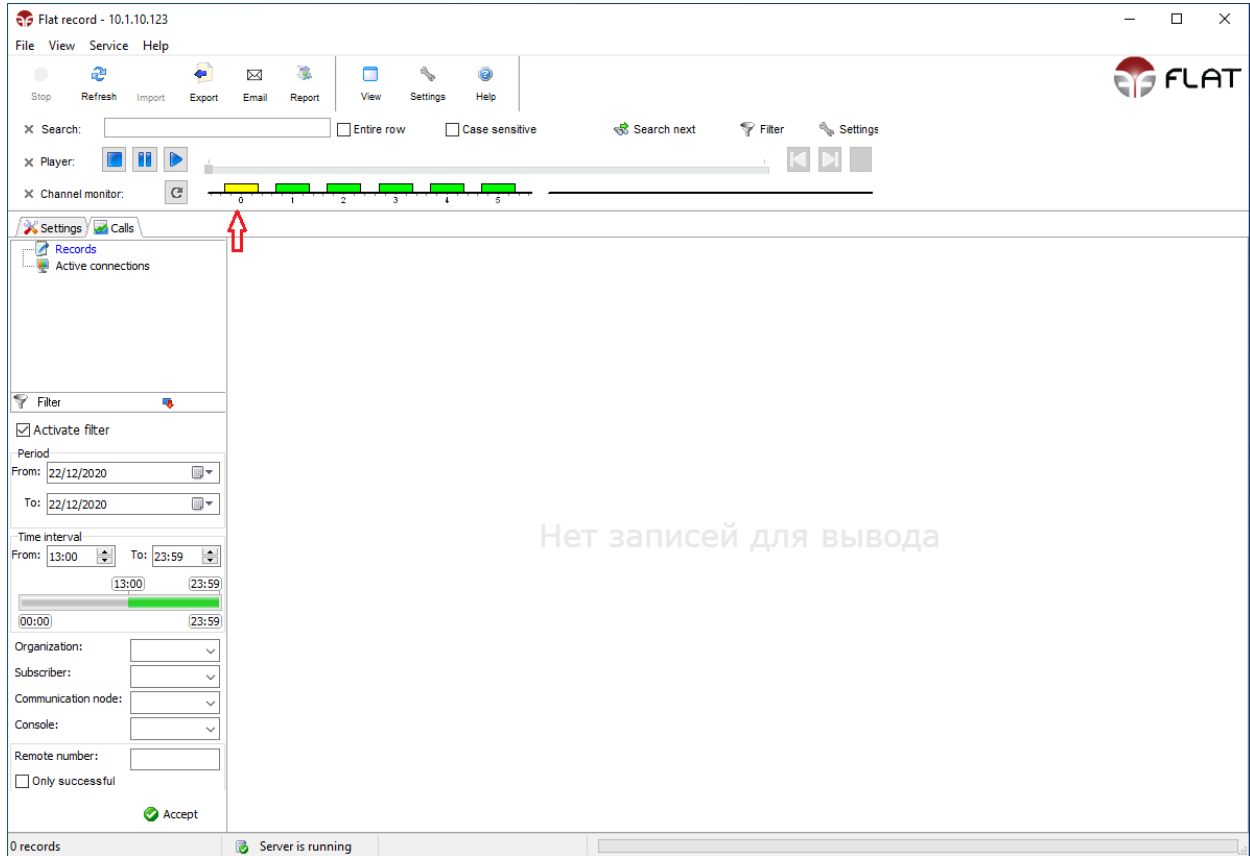
	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	46124FD08E9A73B99 691D6014E5F0D22-0	Flatrecord	Flat	10.1.10.123	XML Unencrypted	12

[Terminate Sessions](#) [Show Terminated Sessions](#)

Item 1-1 of 1
1 Go

9.3. Verify FLAT Record

Make an inbound ACD call and answer at the available agent. Verify the **Channel monitor** shows the channel that is recording turns yellow as mentioned in **Section 8.3.2**.



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** → **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.

The screenshot shows the 'Flat record - 10.1.10.123' application window. The top menu bar includes 'File', 'View', 'Service', and 'Help'. Below the menu is a toolbar with icons for 'Stop', 'Refresh', 'Import', 'Export', 'Email', 'Report', 'View', 'Settings', and 'Help'. A search bar is present with options for 'Entire row' and 'Case sensitive', along with 'Search next', 'Filter', and 'Settings' buttons. A 'Player' section features a play button icon (highlighted with a red box) and a 'Channel monitor' section with a timeline from 0 to 5. The main area is divided into two panes: 'Settings' and 'Calls'. The 'Calls' pane is active, showing a table of records. The 'Filter' pane on the left is also active, showing the 'Activate filter' checkbox (checked), 'Period' settings (From: 16/12/2020, To: 16/12/2020), 'Time interval' settings (From: 15:41, To: 23:59), and a list of filters (Organization, Subscriber, Communication node, Console, Remote number). An 'Accept' button is at the bottom of the filter pane.

Date and time	Duration	Calling	Caller	Subscribers	Line nt	Note	Catego
2020.12.16 - 15:41:06	00:00:28	311	10001	311 -> 10001	0		
2020.12.16 - 15:41:17	00:00:29	10001	10053	10001 -> 10053	0		

10. Conclusion

These Application Notes describe the configuration steps required for TeleSvyaz FLAT Record 3.1 to successfully interoperate with Avaya Aura® Communication Manager 8.1 using Avaya Aura® Application Enablement Services 8.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

11. Additional References

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

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

[1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 8, November 2020.

[2] *Administering and Maintaining Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 8, December 2020.

The following FLAT Record documentation can be obtained from member.

[3] *FLAT Record – Guidelines for establishing connection to Avaya Aura*.

[4] *FLAT Record – Installation and Configuration Manual*.

©2021 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.