



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Carina Recorder R6.5 with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Application Enablement Services R8.1 using Single Step Conference – Issue 1.0

### Abstract

These Application Notes describe the configuration steps for Carina Recorder R6.5 with Avaya Aura® Communication Manager R8.1.3 and Avaya Aura® Application Enablement Services R8.1.3. Carina Recorder is a voice recording solution which can be used to record voice streams for Avaya telephony.

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

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

# 1. Introduction

The purpose of this document is to describe the compliance testing carried out using the Single Step Conference recording (SSC) method on Carina Recorder solution with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services (AES). It includes a description of the configuration of both the Avaya and the Carina solutions, a description of the tests that were performed and a summary of the results of those tests.

The compliance testing focused on the voice integration with Communication Manager via the Application Enablement Services Telephony Services Application Programming Interface (TSAPI) and Device, Media, and Call Control (DMCC) interfaces.

Carina Recorder uses the TSAPI interfaces to monitor extensions to be recorded. When the monitored extension is active, Carina Recorder controller sets up recording by using SSC to conference a dedicated virtual DMCC device into the call. The conference call is then transferred to a Carina Recorder via the DMCC device. Agent information from the TSAPI data is used to start and stop recordings and to add metadata to the recording database for recording identification and searching.

## 2. General Test Approach and Test Results

The test approach was to verify that the calls placed and recorded using the Carina solution with Avaya solution functioned correctly with good audio quality received. Functionality testing included basic telephony operations such as answer, hold/retrieve, transfer, conference, call forward and calls to/from the PSTN. Tests also include ACD Agent Recording. Serviceability testing was also included where the LAN cables were disconnected to AES, Carina server and Media Gateway.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Carina did not include use of any specific encryption features as requested by ComputerTel (subsidiary of Fournet).

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing.

The feature functionality testing focused on verifying the following on Carina:

- Handling of TSAPI messages in areas of event notification and value queries.
- Use of DMCC services to register virtual IP softphones, and to obtain the media for call recording from Single Step Conference.
- Proper recording, logging and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, resume, G.711 Alaw, call forwarding, long duration, multiple calls, multiple agents, conference, and transfer.

The serviceability testing focused on verifying the ability of Carina recorder server to recover from LAN disconnection and reconnection and also between Carina server and Avaya solutions.

## 2.2. Test Results

All functionality and serviceability test cases were completed successfully.

## 2.3. Support

Technical support on Carina Recorder can be obtained through the following:

**Phone:** +44 (0) 1474 565749

**Email:** [engineering@computertel.co.uk](mailto:engineering@computertel.co.uk)

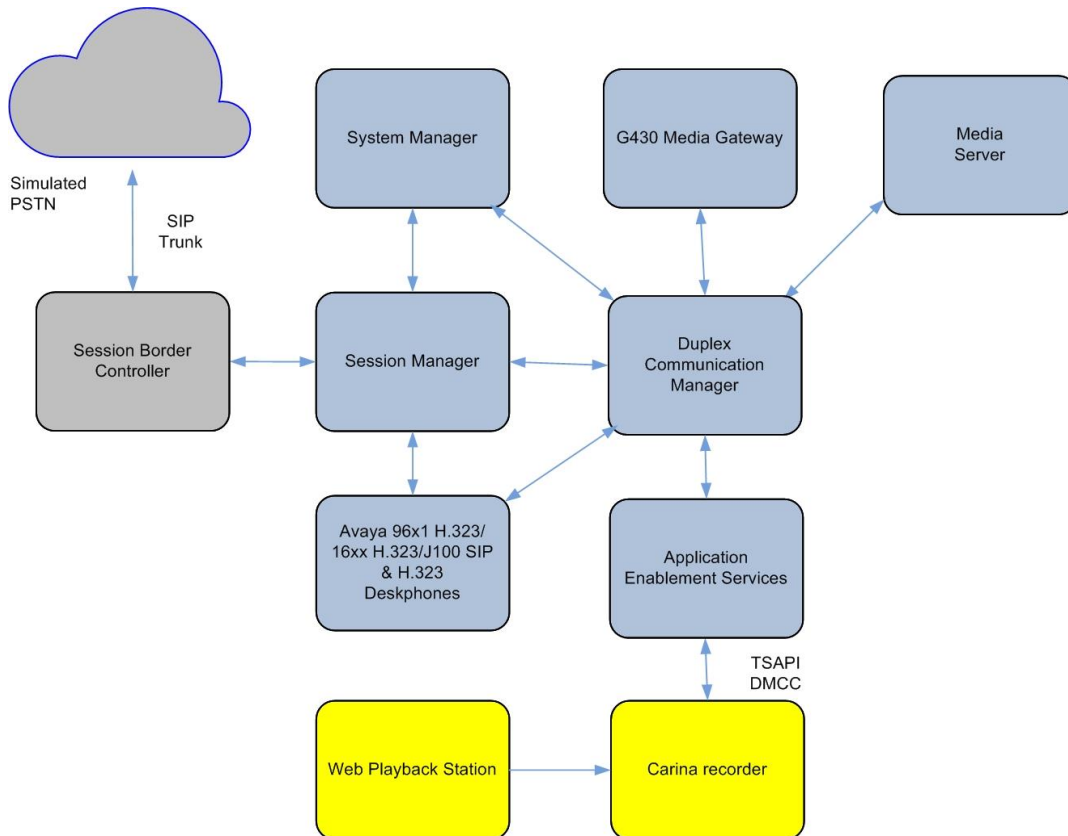
**Web :** <https://computertel.co.uk/>

### 3. Reference Configuration

**Figure 1** illustrates the network topology used during compliance testing. The Avaya solution consists of an Avaya Aura® Communication Manager with Avaya G430 Media Gateway and Avaya Aura® Application Enablement Services. Avaya 96x1 Series IP Deskphones (H.323), 1600 Series IP Deskphones (H.323), J100 Series IP Deskphones (SIP and H.323) are connected to the PBX and used in the testing. Avaya one-X® Agent (H.323) is setup as softphone. The Carina recorder server is installed on a Windows 2019 server.

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

Device Type	Extension
VDN	14001, 14002
Skill Group	13001, 13002
Supervisor	10003 (H.323)
Agent Station	10002 (H.323), 10053 (SIP)
Agent Station Security Code	111222 (same for both)
Agent ID	11002 (10002), 11004 (10053), 11003 (10003)
Virtual Station	19001 to 19010
Virtual Station Security Code	111222 (same for all)



**Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services Server and Carina Recorder Server Configuration**

## 4. Equipment and Software Validated

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

<b>Equipment</b>	<b>Software</b>
Avaya Aura® System Manager running on a Virtual Server	8.1.3.1
Avaya Aura® Session Manager running on a Virtual Server	8.1.3.1
Avaya Aura® Communication Manager running on Virtual Server	8.1 FP3 SP1
Avaya Aura® Application Enablement Services running on Virtual Server	8.1.3.1.0.7-0
Avaya G430 Media Gateway	41.34.1
Avaya Media Server running on a Virtual Server	8.0.2.138
Avaya 9608 H.323 Deskphone Avaya J179 H.323 Deskphone	6.8511
Avaya 1616-I H.323 Deskphone	1.312
Avaya J169 SIP Deskphone	4.0.10.0.3
Avaya one-X® Agent Softphone	2.5.15
Carina IP Recorder running on Windows Server 2019 Avaya TSAPI Windows Client	6.5 Standard 8.1.3 Build 7
Carina Web Playback running on Windows 10 Pro PC	3.5

## 5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration of vdn, vectors, routing, skill hunt groups etc., are not the focus of these Application Notes and will not be described.

The configuration operations described in this section can be summarized as follows:

- Verify system parameters customer options
- Configure virtual stations for the recording pool
- Configure interface to AES

### 5.1. Verify System Parameters Customer Options

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

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

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

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

## 5.2. Configure Virtual Stations for the Recording Pool

Use the **add station** command to configure a station for each of the virtual stations to be used for the recorder channels. Enter in a descriptive **Name** and **Security Code** for each one. The **Security Code** will be referenced by Carina when setting up the recording extensions. The security code must be the same for all virtual devices as the configuration on the Carina only allows for the specification of one global security code. Set **IP Softphone?** to **y**. Repeat these step for all the virtual stations to be used.

```

add station 19901                                     Page 1 of 5
                                                    STATION
Extension: 19901                                     Lock Messages? n          BCC: 0
  Type: 9640                                         Security Code: *          TN: 1
  Port: S000395                                     Coverage Path 1:          COR: 1
  Name: DMCC #1                                     Coverage Path 2:          COS: 1
Unicode Name? n                                     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                         Button Modules: 0
Survivable GK Node Name:
  Survivable COR: internal                           Media Complex Ext:
  Survivable Trunk Dest? y                           IP SoftPhone? y
                                                    IP Video Softphone? n
                                                    Short/Prefixed Registration Allowed: default
                                                    Customizable Labels? y
  
```

In the compliance testing, **19901** to **19910** are added as listed below:

```

list station ext 19901 count 10                       Page 1
                                                    STATIONS
Ext/      Port/   Name/      Room/   Cv1/   COR/
Hunt-to   Type    Surv GK NN   Move  Cable  Jack  Cv2  COS  TN
19901     S000407 DMCC #1           1
          9640
19902     S000006 DMCC #2           1 1
          9640           no
19903     S000007 DMCC #3           1 1
          9640           no
19904     S000008 DMCC #4           1 1
          9640           no
19905     S000011 DMCC #5           1 1
          9640           no
19906     S000042 DMCC #6           1
          9640           no
19907     S000088 DMCC #7           1 1
          9640           no
          press CANCEL to quit -- press NEXT PAGE to continue
  
```

```
list station ext 19901 count 10
```

STATIONS										
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Cable	Room/ Jack	Cv1/ Cv2	COS	COR/ TN		
19908	S000086 9640	DMCC #8		no				1		
19909	S000066 9640	DMCC #9		no				1	1	
19910	S000009 9640	DMCC #10		no				1	1	

### 5.3. Configure Interface to Avaya Aura® Application Enablement Services

In order for Communication Manager to establish a connection to Application Enablement Services, administer the CTI Link as shown below. Add an available cti-link number which in this case is **3**. Specify an available **Extension** number, set the **Type** as **ADJ-IP**, which denotes that this is a link to an IP connected adjunct, and name the link for easy identification.

```
add cti-link 3
```

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



## 6. Configuration of Avaya Aura® Application Enablement Services

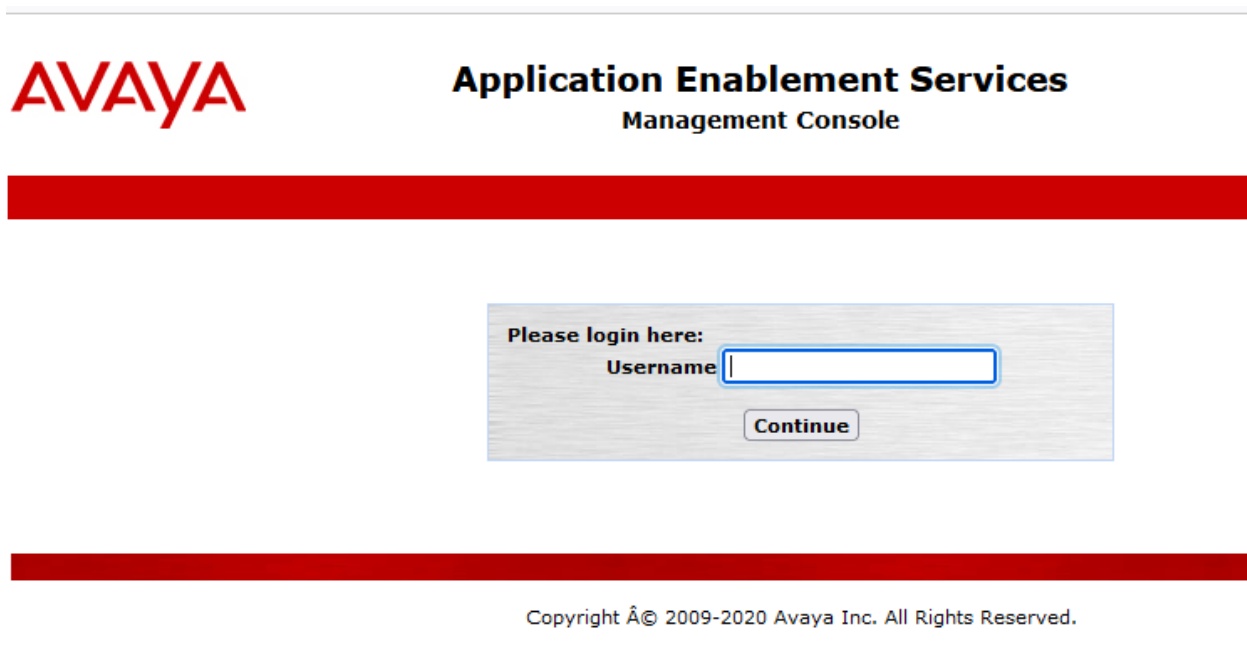
This section provides the procedures for configuring AES. The procedures fall into the following areas:

- Launch OAM interface
- Verify License
- Administer TSAPI link
- Administer H.323 Gatekeeper
- Create CTI User
- Configure DMCC Port
- Administer Security Database
- Restart Services

### 6.1. Launch OAM Interface

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

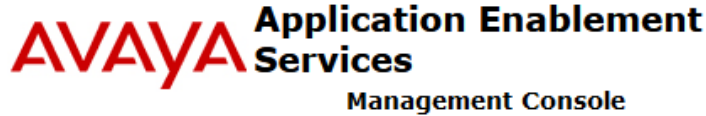
The **Please login here** screen is displayed. Log in using the appropriate credentials.



The screenshot shows the Avaya logo on the left and the text "Application Enablement Services Management Console" on the right. Below this is a red horizontal bar. In the center, there is a login form with the text "Please login here:" followed by "Username" and a text input field. Below the input field is a "Continue" button. At the bottom of the page, there is a red horizontal bar and the copyright notice "Copyright © 2009-2020 Avaya Inc. All Rights Reserved."

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

---



**AVAYA** Application Enablement  
Services  
Management Console

Welcome: User cust  
Last login: Fri Aug 13 14:50:26 2021 from dcvpnsvr01.sglab.com  
Number of prior failed login attempts: 0  
HostName/IP: aes/10.1.10.70  
Server Offer Type:  
VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.3.1.0.7-0  
Server Date and Time: Fri Aug 13 15:49:50 SGT 2021  
HA Status: Not Configured

HomeHome | 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

## 6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

The screenshot shows a web application interface. At the top, there is a red navigation bar with the word "Licensing" on the left and "Home | Help | Logout" on the right. Below this is a left-hand navigation pane with a dark grey background and white text. The menu items are: "AE Services", "Communication Manager Interface", "High Availability", "Licensing" (expanded), "WebLM Server Address", "WebLM Server Access" (highlighted in blue), "Reserved Licenses", "Maintenance", "Networking", "Security", and "Status". The main content area on the right has a white background and a blue border. It is titled "Licensing" and contains three paragraphs of text. The first paragraph says "If you are setting up and maintaining the WebLM, you need to use the following:" followed by a bullet point "WebLM Server Address". The second paragraph says "If you are importing, setting up and maintaining the license, you need to use the following:" followed by a bullet point "WebLM Server Access". The third paragraph says "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by a bullet point "Reserved Licenses". At the bottom of the main content area, there is a red note: "NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page".

Select **Licensed products** → **APPL\_ENAB** → **Application\_Enablement** in the left pane, to display the **Licensed Features** screen in the right pane.

Verify that there are sufficient licenses for **Device Media and Call Control and TSAPI Simultaneous Users**, as shown below. If not, consult with your Avaya Account Manager or Business Partner to acquire the proper license for your solution.

The screenshot shows the 'Application Enablement (CTI) - Release: 8 - SID: 10503000' interface. The left sidebar contains a navigation menu with items like 'WebLM Home', 'Install license', 'Licensed products', 'APPL\_ENAB', 'Application\_Enablement', 'View license capacity', 'View peak usage', 'CE', 'COLLABORATION\_ENVIRONMENT', 'MESSAGING', 'POM', 'SYSTEM\_MANAGER', 'SessionManager', 'VDIA', 'VSS', 'Uninstall license', 'Server properties', 'Metering Collector Configuration', 'Shortcuts', and 'Help for Licensed products'.

The main content area displays the following information:

- You are here: Licensed Products > Application\_Enablement > View License Capacity
- License installed on: May 13, 2020 2:06:31 PM +08:00
- License File Host IDs: V6-BB-8E-6F-89-B6-01
- Licensed Features**
- 13 Items Show All

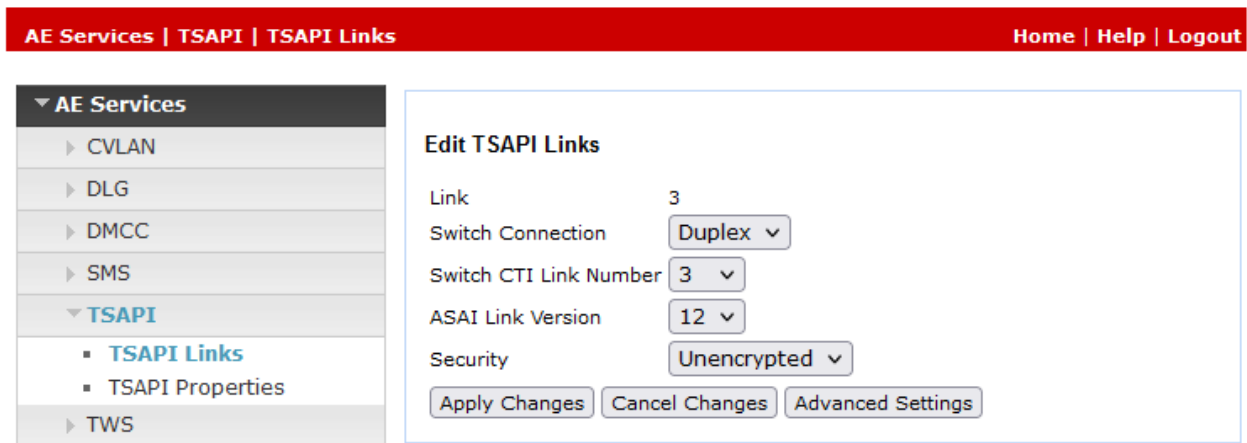
Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	2500
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	10
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	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

SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS  
MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20  
LargeServerTypes:

### 6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the Management Console, to administer a TSAPI link. Click **Add Link** (not shown). Below shows the TSAPI link configured.

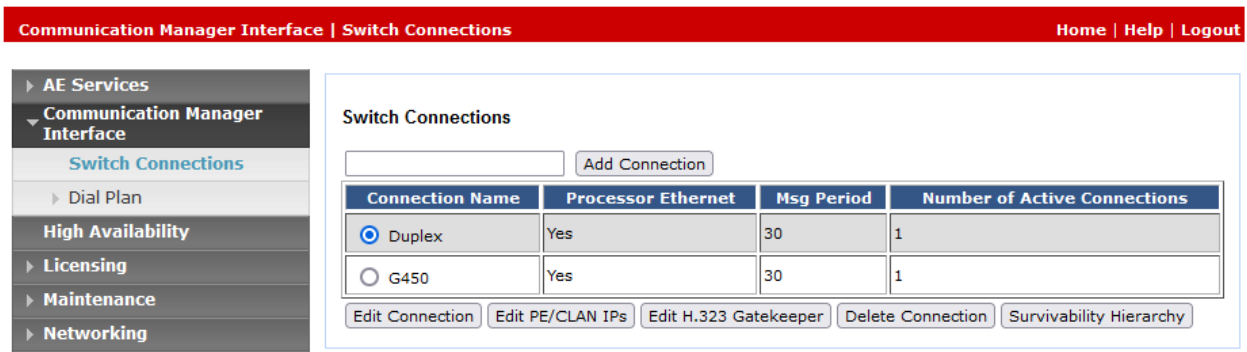
The **Link** field is only local to the Application Enablement Services server and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection “Duplex” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.3**. The **Security** is set as Unencrypted here for the testing.



## 6.4. 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**.



The screenshot shows the 'Switch Connections' page. At the top, there is a red navigation bar with 'Communication Manager Interface | Switch Connections' on the left and 'Home | Help | Logout' on the right. A left-hand navigation pane contains a tree view with 'Communication Manager Interface' expanded to 'Switch Connections'. The main content area is titled 'Switch Connections' and features a search box and an 'Add Connection' button. Below this is a table with the following data:

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> Duplex	Yes	30	1
<input type="radio"/> G450	Yes	30	1

At the bottom of the table, there are several action buttons: 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor on Communication Manager to use as the H.323 gatekeeper, in this case “10.1.10.230”. Click **Add Name or IP** and the resulting screen is as shown below.



The screenshot shows the 'Edit H.323 Gatekeeper - Duplex' page. It has the same red navigation bar and left-hand navigation pane as the previous screenshot. The main content area is titled 'Edit H.323 Gatekeeper - Duplex' and contains a search box and an 'Add Name or IP' button. Below this, the text 'Name or IP Address' is followed by a radio button selection for '10.1.10.230'. At the bottom, there are two buttons: 'Delete IP' and 'Back'.

## 6.5. Create CTI User

A user ID and password needs to be configured for the Carina recorder to communicate as a DMCC client with AES. Select **User Management** → **User Admin** → **Add User** from the left-hand menu, to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown).

**User Management | User Admin | Add User**

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▼ **User Management**
  - ▶ Service Admin
  - ▼ **User Admin**
    - **Add User**
    - Change User Password
    - List All Users
    - Modify Default Users
    - Search Users
- ▶ Utilities
- ▶ Help

### Add User

Fields marked with \* can not be empty.

* User Id	<input type="text" value="Fournet"/>
* Common Name	<input type="text" value="Fournet"/>
* Surname	<input type="text" value="Fournet"/>
* User Password	<input type="password"/>
* Confirm Password	<input type="password"/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>
Employee Type	<input type="text"/>
Enterprise Handle	<input type="text"/>

## 6.6. Configure DMCC Port

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

The screenshot shows the 'Ports' configuration page in the AES Management Console. The page has a red header with 'Networking | Ports' on the left and 'Home | Help | Logout' on the right. A left sidebar contains a navigation menu with categories like 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The 'Networking' category is expanded, showing sub-items: 'AE Service IP (Local IP)', 'Network Configure', 'Ports', and 'TCP/TLS Settings'. The main content area is titled 'Ports' and is divided into several sections:

- CVLAN Ports:** Includes 'Unencrypted TCP Port' (9999) and 'Encrypted TCP Port' (9998), each with an 'Enabled' radio button selected.
- DLG Port:** Includes 'TCP Port' (5678).
- TSAPI Ports:** Includes 'TSAPI Service Port' (450) with an 'Enabled' radio button selected, and 'Local TLINK Ports' (TCP Port Min: 1024, TCP Port Max: 1039) and 'Unencrypted TLINK Ports' (TCP Port Min: 1050, TCP Port Max: 1065).
- DMCC Server Ports:** This section is highlighted with a red box. It includes 'Unencrypted Port' (4721) with an 'Enabled' radio button selected, 'Encrypted Port' (4722), and 'TR/87 Port' (4723).



## 6.7. Administer Security Database

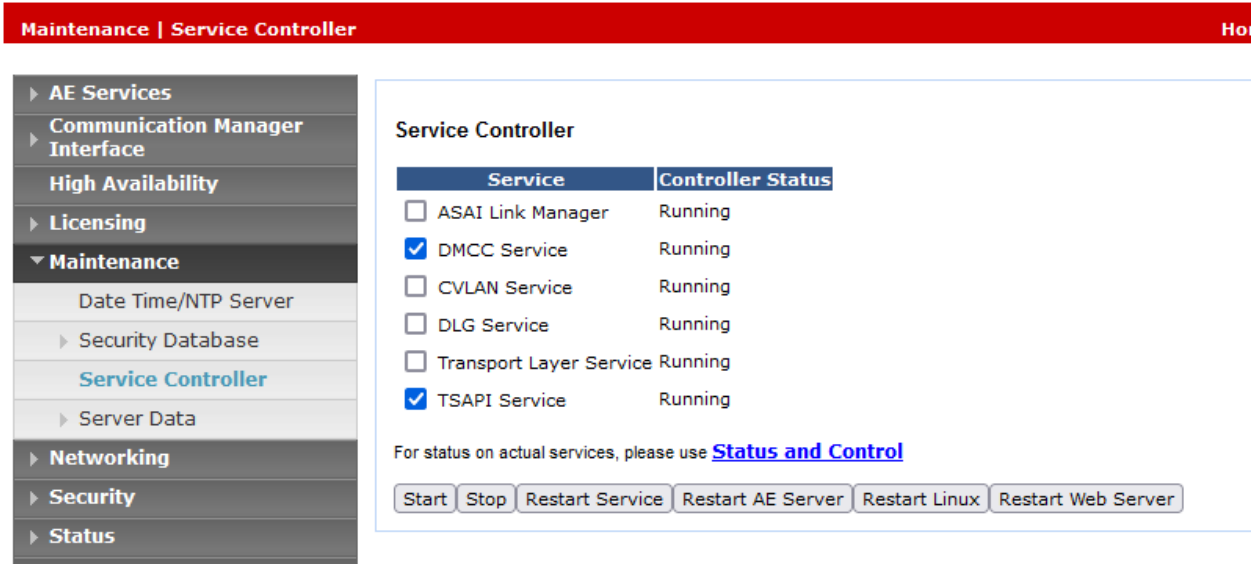
Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [1] to configure access privileges for the Fournet user from **Section 6.5**.

The screenshot shows a web interface with a red header bar containing the breadcrumb "Security | Security Database | Control". On the left is a navigation tree with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control (selected), and CTI Users. The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below the checkboxes is an "Apply Changes" button.

## 6.8. Restart Services

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



The screenshot shows a web interface with a red header bar containing "Maintenance | Service Controller" and "Ho". On the left is a navigation menu with items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance (expanded), Date Time/NTP Server, Security Database, Service Controller (highlighted), Server Data, Networking, Security, and Status. The main content area is titled "Service Controller" and contains a table with two columns: "Service" and "Controller Status".

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

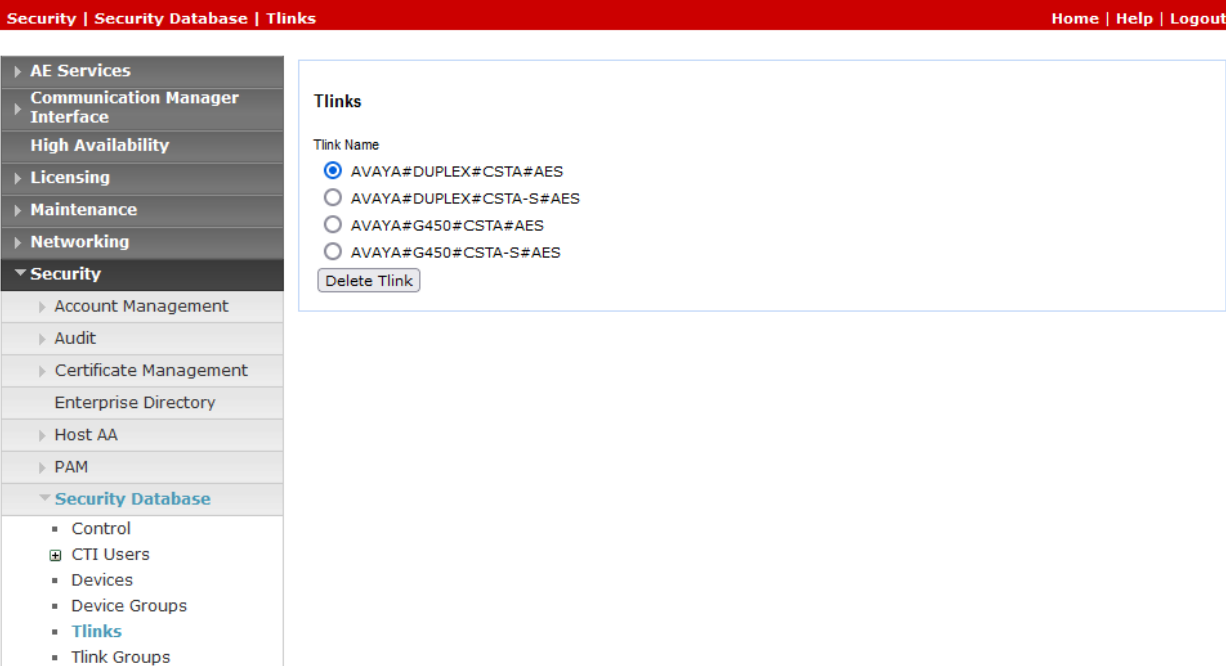
For status on actual services, please use [Status and Control](#)

Buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, Restart Web Server

## 6.9. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Carina.

In this case, the associated Tlink name is “AVAYA#**DUPLEX**#CSTA#AES”. Note the use of the switch connection “Duplex” from **Section 6.3** as part of the Tlink name.



The screenshot shows a web interface for configuring Tlinks. At the top, there is a red navigation bar with the text "Security | Security Database | Tlinks" on the left and "Home | Help | Logout" on the right. On the left side, there is a vertical navigation menu with the following items: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control, CTI Users, Devices, Device Groups, Tlinks (highlighted in blue), and Tlink Groups. The main content area is titled "Tlinks" and contains a "Tlink Name" section with four radio button options: AVAYA#DUPLEX#CSTA#AES (selected), AVAYA#DUPLEX#CSTA-S#AES, AVAYA#G450#CSTA#AES, and AVAYA#G450#CSTA-S#AES. Below the radio buttons is a "Delete Tlink" button.

## 7. Configuration of Carina Recorder

The configuration of Carina is typically performed by ComputerTel installation technicians. The procedural steps are presented in these Application Notes for informational purposes.

Prior to configuration, the relevant Avaya TSAPI client is assumed to be installed on the Carina server, and that the TSAPI client has been configured with the IP address of the AES server as part of installation.

This section provides procedures for the following on configuring Carina recorder server. The procedures include the following:

- Launch Carina Web Playback
- Verify the server configuration
- Verify stations, agents and hunt groups extensions administered

### 7.1. Launch Carina Web Playback

The web interface is used to configure the extensions. Use **https://<server IP>/webav3/login.html** to access the **ComputerTel Playback Sign In** screen as shown below. Log in with an appropriate credentials.



ComputerTel Playback

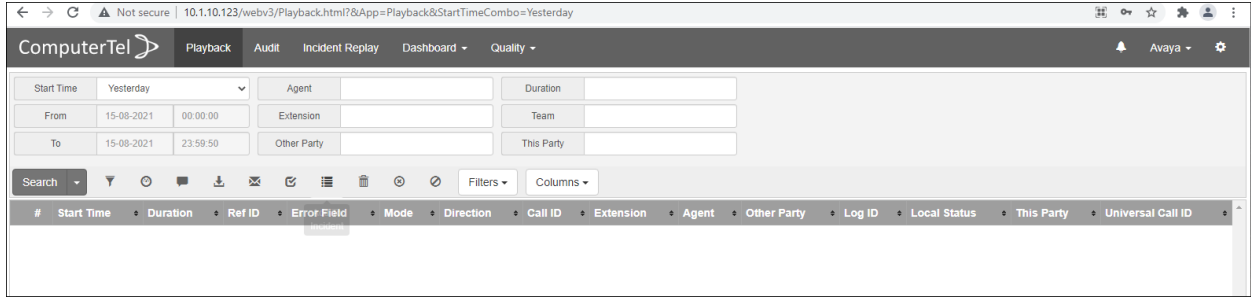
Please Sign in to use web playback.

Username

Password

Sign in

The following screen is displayed with the **Playback** tab selected as default.

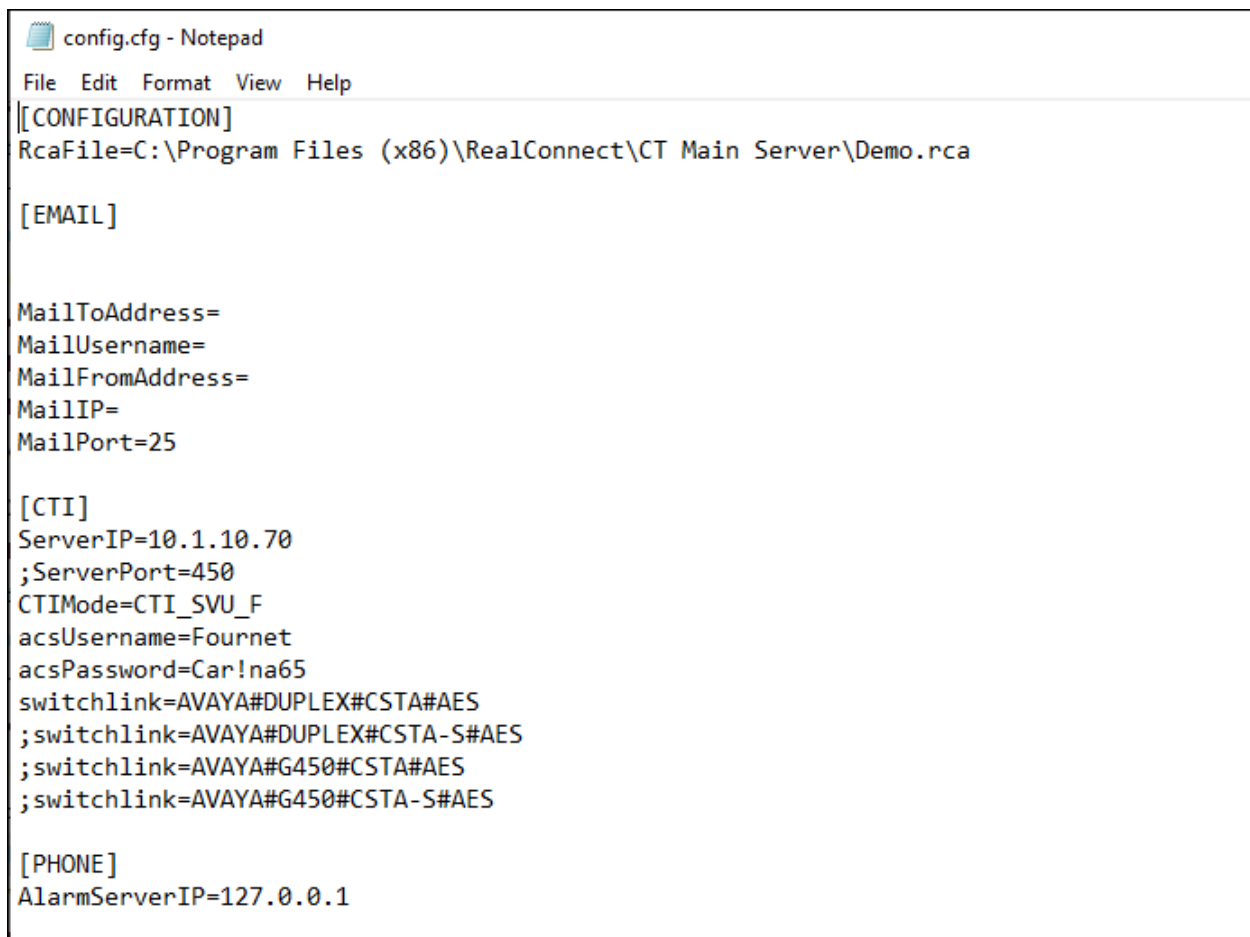


## 7.2. Verify the Server Configuration

Locate the configuration file “Config.cfg” at “C:\Program Files (x86)\RealConnect\CT Main Server\” for the **CT Main Server program** on the Windows server. Verify the parameters below:

Under **CTI**:

- **ServerIP** – AES IP address, i.e., 10.1.10.70.
- **acsUsername** – CT User ID provisioned in AES **Section 6.5**.
- **acsPassword** – CT User password provisioned in AES **Section 6.5**.
- **switchlink** – Tlink listed in **Section 6.9**. “AVAYA#DUPLEX#CSTA#AES” is used in this case.



```
config.cfg - Notepad
File Edit Format View Help
[[CONFIGURATION]
RcaFile=C:\Program Files (x86)\RealConnect\CT Main Server\Demo.rca

[EMAIL]

MailToAddress=
MailUsername=
MailFromAddress=
MailIP=
MailPort=25

[CTI]
ServerIP=10.1.10.70
;ServerPort=450
CTIMode=CTI_SVU_F
acsUsername=Fournet
acsPassword=Car!na65
switchlink=AVAYA#DUPLEX#CSTA#AES
;switchlink=AVAYA#DUPLEX#CSTA-S#AES
;switchlink=AVAYA#G450#CSTA#AES
;switchlink=AVAYA#G450#CSTA-S#AES

[PHONE]
AlarmServerIP=127.0.0.1
```

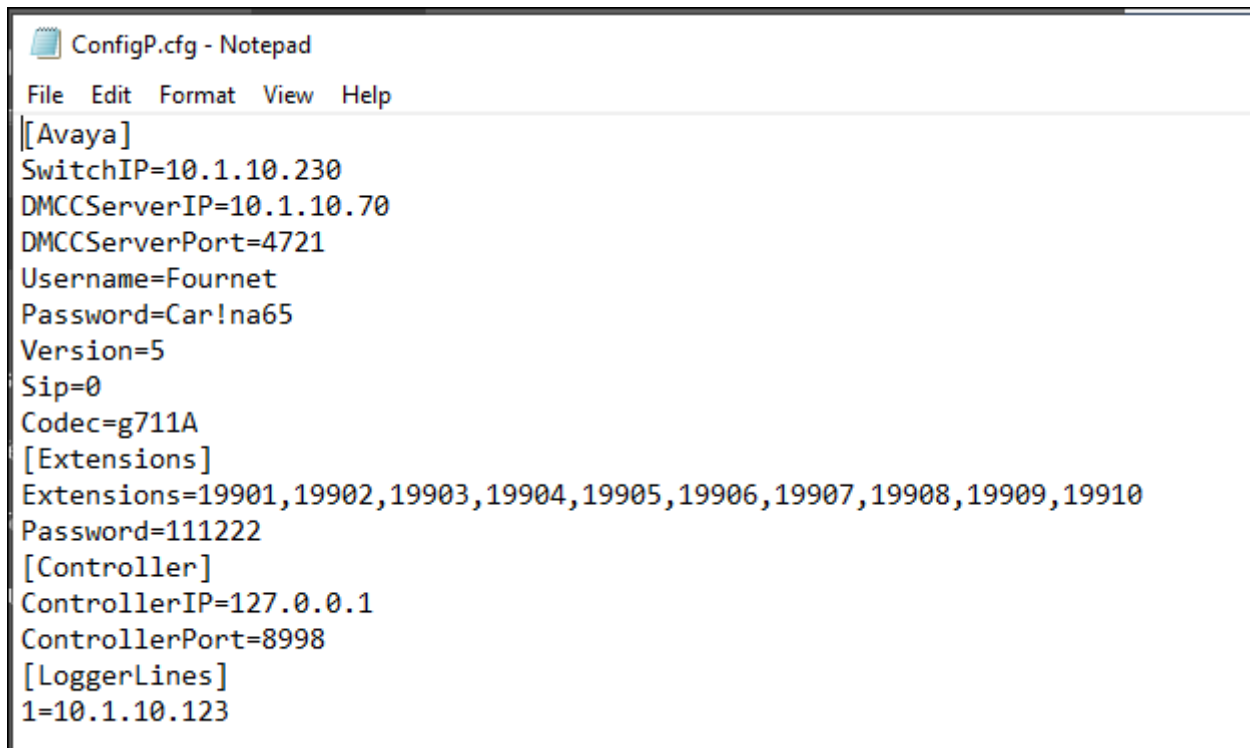
Locate the configuration file “ConfigP.cfg” at “C:\Program Files (x86)\RealConnect\CTDMCC Monitor\” for the **CT DMCC Monitor Program** on the Windows server. Verify the parameters below:

Under **Avaya**:

- **SwitchIP** – Communication Manager IP address. In this testing, processor C-LAN on Communication Manager is used, i.e., 10.1.10.230.
- **DMCCServerIP** – AES IP address, i.e., 10.1.10.70.
- **DMCCServerPort** – DMCC port in **Section 6.6**.
- **Username** – CT User ID provisioned in AES **Section 6.5**.
- **Password** – CT User password provisioned in AES **Section 6.5**.
- **Codec** – “g711A” is tested.

Under **Extensions**:

- **Extensions** – Virtual stations used for the DMCC Channels.
- **Password** – Password of virtual stations.



```
ConfigP.cfg - Notepad
File Edit Format View Help
[[Avaya]
SwitchIP=10.1.10.230
DMCCServerIP=10.1.10.70
DMCCServerPort=4721
Username=Fournet
Password=Car!na65
Version=5
Sip=0
Codec=g711A
[Extensions]
Extensions=19901,19902,19903,19904,19905,19906,19907,19908,19909,19910
Password=111222
[Controller]
ControllerIP=127.0.0.1
ControllerPort=8998
[LoggerLines]
1=10.1.10.123
```

### 7.3. Verify the Stations, Agents and Hunt Groups Extensions

From **Section 7.1** web playback screen, click on the **Settings** cog wheel on the top right corner. It shows the stations, agents and hunt groups extensions in **Section 3** that are administered for monitoring.

Configurations of these extensions on Carina recorder will not be detailed here and can be found in the reference [4].

The screenshot shows the 'Users' management page in the ComputerTel interface. The page includes a search bar and a table with columns for User Name, User TSRID, User ID, User Level, Level Name, Default Group, Extension, PinCode, Auto Record, Auto Stop, Allow Mute, PABX Name, Link ID, Default Email To, and Workstat. The table lists various user types including Agents, Managers, Technicians, and an Unknown user.

UserName	User TSRID	User ID	User Level	Level Name	Default Group	Extension	PinCode	Auto Record	Auto Stop	Allow Mute	PABX Name	Link ID	Default Email To	Workstat
Agent 11002	Agent 11002	7	2	Agent			11002	✓	✓	✓				
Agent 11003	Agent 11003	6	2	Agent			11003	✓	✓	✓				
Agent 11004	Agent 11004	8	2	Agent			11004	✓	✓	✓				
Avaya	Avaya	2	8	Manager				✓	✓	✓				
Ext 10002	Ext 10002	4	2	Agent		10002		✓	✓	✓				
Ext 10003	Ext 10003	3	2	Agent		10003		✓	✓	✓				
Ext 10053	Ext 10053	5	2	Agent		10053		✓	✓	✓				
Skillset HG	Skillset HG	10	2	Agent		13001		✓	✓	✓				
Skillset HG1	Skillset HG1	11	2	Agent		13002		✓	✓	✓				
Tech	Tech	0	100	Technician				✓	✓	✓			Default	
Unknown	Unknown	1	2	Agent				✓	✓	✗			Default	



## 8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Avaya and Carina recorder solution.

### 8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the AESVCS link status with AES by using the command **status aesvcs cti-link**. The CTI Link is 3. Verify the **Service State** of the CTI link is **established**.


```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	<b>Service State</b>	Msgs Sent	Msgs Rcvd
3	12	no	aes	<b>established</b>	15	15

## 8.2. Verify Avaya Aura® Application Enablement Services

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly.

Verify the status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary**. Verify that the TSAPI Link **Status** shows “Talking” and that the **Associations** column reflects the total number of agents (3) and hunt groups extensions (2) from **Section 3** plus the number of virtual stations (10) in **Section 5.2**, in this case “15”.



**Application Enablement Services**  
Management Console

Welcome: User cust  
 Last login: Fri Aug 13 18:43:03 2021 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: 8.1.3.1.0.7-0  
 Server Date and Time: Mon Aug 16 14:18:24 SGT 2021  
 HA Status: Not Configured

---

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

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

### TSAPI Link Details

Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input type="radio"/>	1	G450	1	Talking	Thu Aug 12 14:02:56 2021	Online	18	0	15	15	30
<input checked="" type="radio"/>	3	Duplex	3	Talking	Thu Aug 12 14:02:51 2021	Online	18	15	15	15	30

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

Verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary**. The **DMCC Service Summary – Session Summary** screen is displayed as shown below. Verify the **User** is “Fournet” from **Section 6.5** and the **Far-end Identifier** is given as the IP address of the Carina recorder server. Note that the **# of Associated Devices** show “10” which is the number of virtual DMCC stations registered.



**Application Enablement Services**  
Management Console

Welcome: User cust  
Last login: Fri Aug 13 16:37:13 2021 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: 8.1.3.1.0.7-0  
Server Date and Time: Fri Aug 13 18:43:41 SGT 2021  
HA Status: Not Configured

- ▶ 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
- ▶ Utilities
- ▶ Help

**DMCC Service Summary - Session Summary**

Please do not use back button

Enable page refresh every  seconds

Session Summary [Device Summary](#)  
Generated on Fri Aug 13 18:43:36 SGT 2021

Service Uptime: 102 days, 1 hours 31 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 35

Number of Existing Devices: 10

Number of Devices Created Since Service Boot: 302

<input type="checkbox"/>	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	9C39E6EB60323AF01 25497C06A0E0A98-47	Fournet	RealConnect CTSwitch + CTLogger	10.1.10.123	XML Unencrypted	10

Item 1-1 of 1  
 Go

### 8.3. Verify Carina Configuration

The following steps can be performed to verify the basic operation of the system components. Make an inbound call to one of the recorded stations.

Click on **Playback** tab on the top menu. Select the appropriate **Start Time** and click **Search** below. Verify a record is shown of the call. Click on the line and the bottom shows the audio wave image. Click on the playback icon on the left bottom and verify the recorded voice is played.

The screenshot displays the ComputerTel interface. At the top, there are navigation tabs: Playback, Audit, Incident Replay, Dashboard, and Quality. Below the tabs is a search and filter section with fields for Start Time (set to Custom), Agent, Duration, From (10-08-2021 15:08:00), Extension, Team, To (10-08-2021 23:59:50), Other Party, and This Party. A search button is located below these fields. Below the search section is a table with the following columns: #, Start Time, Duration, Ref ID, Error Field, Mode, Direction, Call ID, Extension, Agent, Other Party, Log ID, Local Status, This Party, and Universal Call ID. The table contains one row of data: # 1, Start Time 10-08-2021 15:08:44, Duration 00:00:10, Ref ID r1\_c10\_100821\_150844.rcc, Error Field, Mode 0, Direction inbound, Call ID 235142162, Extension 10053, Agent Ext 10053, Other Party 031110000, Log ID 21, Local Status Saved, This Party 31110053, and Universal Call ID 1062121628578765. Below the table is a large empty area. At the bottom of the interface is an audio playback player. A red arrow points to the play button on the left side of the player. The player shows a volume icon, a play button, a progress bar with the text 'X1 00:00:10/00:00:10', and an audio waveform.

## 9. Conclusion

These Application Notes describe the configuration steps required for the Carina recorder R6.5 to successfully interoperate with Avaya Aura® Communication Manager R8.1.3 and Avaya Aura® Application Enablement Services R8.1.3. All functionality and serviceability test cases were completed successfully.

## 10. Additional References

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

- [1] *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 11, dated June 2021.
- [2] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 12, dated July 2021.
- [3] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 10, dated October 2021.

Product documentation for Carina recorder can be obtained from ComputerTel from information provide in **Section 2.3**.

- [4] *Carina User Manual for version 6.5.0.3*.

---

**©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](mailto:devconnect@avaya.com).