



**Application Notes for configuring Liquid Assure from
Liquid Voice to interoperate with Avaya Aura®
Communication Manager R7.0 and Avaya Aura®
Application Enablement Services R7.0 using DMCC Multi-
Registration to record calls - Issue 1.0**

Abstract

These Application Notes describe the configuration steps for Liquid Voice Liquid Assure to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0, and Avaya Aura® Application Enablement Services R7.0 using Multi-Registration.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the 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 for the Liquid Assure R7.1 from Liquid Voice to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R7.0, an Avaya Aura® Session Manager R7.0, and Avaya Aura® Application Enablement Services R7.0. Liquid Assure uses Communication Manager's Multiple Registrations feature via the Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Telephony Services API (TSAPI) to capture the audio and call details for call recording on various Communication Manager endpoints, listed in **Section 4**.

DMCC works by allowing software vendors to create soft phones on a recording server, and use them to monitor and record Avaya phonesets. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure. The DMCC API associated with the AES server monitors the digital and VoIP extensions. The application uses the AE Services DMCC service to register itself as a recording device at the target extension. When the target extension joins a call, the application automatically receives the call's aggregated RTP media stream via the recording device and records the call.

Liquid Assure is a modular based call-recorder with an easy-to-use web based interface. The modular design allows the system to be scaled to any number of extensions and sites. The web interface provides tools for searching and retrieving recording, forwarding exporting and annotating recordings, centralized system security authorization and auditing, and system status monitoring. The base solution can be amended with additional add-ons including Avaya powered speech analytics, screen-recordings and quality management. The same recording components are also available as an SME targeted product called Liquid Recording. Liquid Recording has a reduced feature-set and is limited to recording 60 concurrent calls.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of the Liquid Assure to carry out call recording in a variety of scenarios using DMCC Multi-Registration with AES and Communication Manager. A range of Avaya endpoints were used in the compliance testing all of which are listed in **Section 4**.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios with good quality audio recordings and accurate call records. The tests included:

- **Inbound/Outbound calls** – Test call recording for inbound and outbound calls to the Communication Manager to and from PSTN callers.
- **Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **Forwarded calls** - Test call recording for calls that were forwarded to various endpoints.
- **Feature calls** - Test call recording for calls that are parked or picked up using Call Park and Call Pickup.
- **Calls to Elite Agents** – Test call recording for calls to Communication Manager agents logged into one-X® Agent.
- **Serviceability testing** - The behavior of Liquid Assure under different simulated failure conditions.

2.2. Test Results

All functionality and serviceability test cases were completed successfully, except for the following feature test which had an issue as follows.

1. **Call Park.** The un-parked call is not being recorded. It appears that there are no events being sent for un-parking a call by Communication Manager. Modification Report [CM-9860] has been raised with the Communication Manager support team. A fix for this issue will be implemented for release 7.1 of Communication Manager.

2.3. Support

Technical support can be obtained for Liquid Assure from:

- Website <http://www.liquidvoice.com>
- Telephone +44 (0) 113 200 2020
- Email support@liquidvoice.com

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test Liquid Assure with the Avaya solution using DMCC Multi-Registration to record calls. The Liquid Voice server is setup for DMCC Multi-Registration mode and connects to the AES.

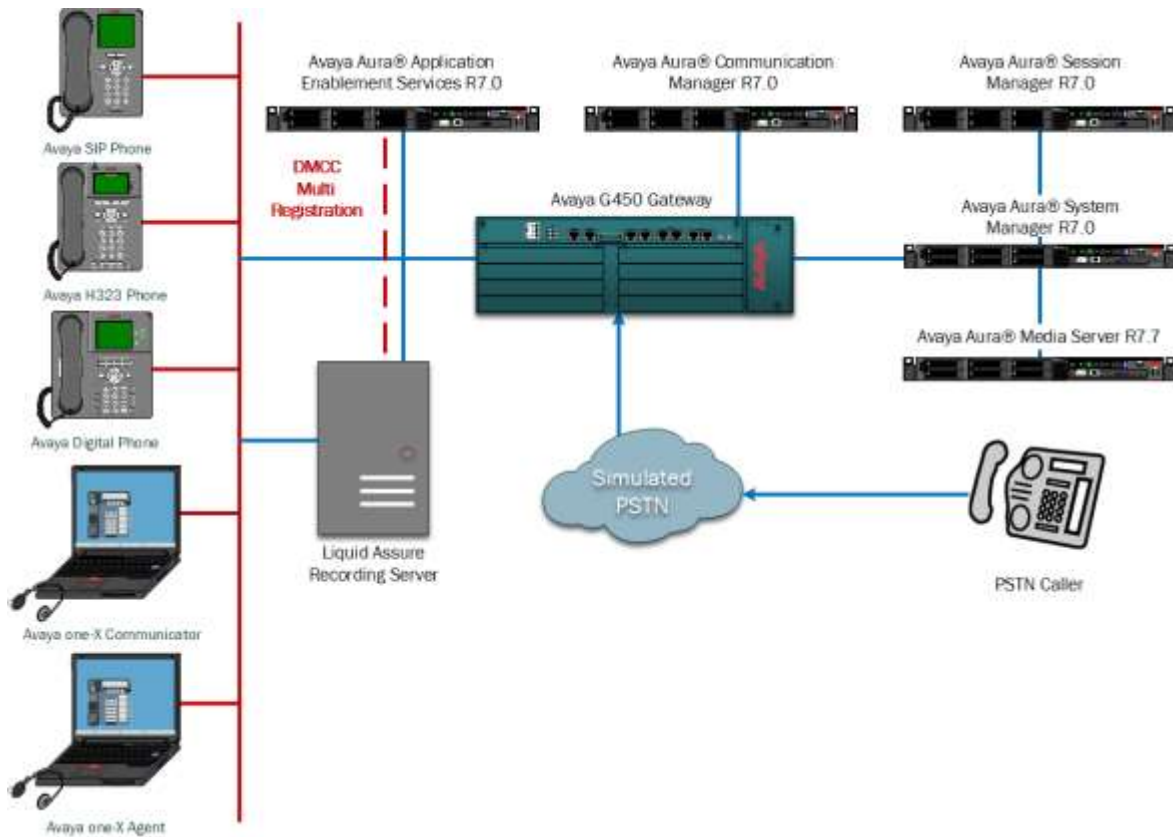


Figure 1: Connection of Liquid Assure R7.1 from Liquid Voice with Avaya Aura® Communication Manager R7.0, Avaya Aura® Session Manager R7.0 and Avaya Aura® Application Enablement Services R7.0

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.0.0.1 Build No. – 7.0.0.0.16266-7.0.9.7001011 Software Update Revision No: 7.0.0.1.4212
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.0 Build No. – 7.0.0.1.700102
Avaya Aura® Communication Manager running on a virtual server	R7.0 SP1 00.0.441.0-22684
Avaya Aura® Application Enablement Services running on a virtual server	R7.0 Build No – 7.0.0.0.1.13
Avaya G450 Gateway	37.19.0 /1
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9641 SIP Deskphone	96x1 SIP Release 7.0.0.39
Avaya 9630 SIP Deskphone	R2.6.13.1
Avaya one-X® Communicator H.323	R6.2.4.07-FP4
Avaya one-X® Agent	R 2.5.50022.0
Avaya 9408 Digital Deskphone	FW Version 2
Avaya DECT Handsets	3725 DH4 (R3.3.11) 3720 DH3 (R3.3.11)
Liquid Voice, Liquid Assure <ul style="list-style-type: none">- Liquid Assure Standalone Server- Liquid Recording Service	V7.1 Interface V7.0.0

5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

5.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

display system-parameters customer-options		Page	3 of 11
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	n	Authorization Codes?	y
Analog Trunk Incoming Call ID?	y	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n
ARS?	y	Computer Telephony Adjunct Links?	y
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y
ASAI Link Core Capabilities?	n	DCS Call Coverage?	y
ASAI Link Plus Capabilities?	n	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		

5.2. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the procr IP address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aes70vmpg**).

display node-names ip		Page	1 of 2
IP NODE NAMES			
Name	IP Address		
SM100	10.10.40.12		
aes70vmpg	10.10.40.16		
default	0.0.0.0		
G450	10.10.40.15		
procr	10.10.40.13		

5.3. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Should be set to **AESVCS**.
- **Enabled:** Set to **y**.
- **Local Node:** Set to the node name assigned for the procr in **Section 5.2**
- **Local Port:** Retain the default value of **8765**.

change ip-services					Page	1 of	4
IP SERVICES							
Service	Enabled	Local	Local	Remote	Remote		
Type		Node	Port	Node	Port		
AESVCS	y	procr	8765				

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes70vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

Note: The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** must match the administered name for the AES server; this is created as part of the AES installation, and can be obtained from the AES server by typing **uname -n** at the Linux command prompt.

change ip-services				Page	4	of	4
AE Services Administration							
Server ID	AE Services Server	Password	Enabled	Status			
1:	aes70vmpg	*****	y	idle			
2:							
3:							

5.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command, where n is the n is the cti-link number as shown in the example below this is **1**.. Enter an available extension number in the **Extension** field. 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 1		Page 1 of 3	
CTI LINK			
CTI Link: 1			
Extension: 7999			
Type: ADJ-IP			
		COR: 1	
Name: aes70vmpg			

5.5. Configure H323 Stations for Multi-Registration

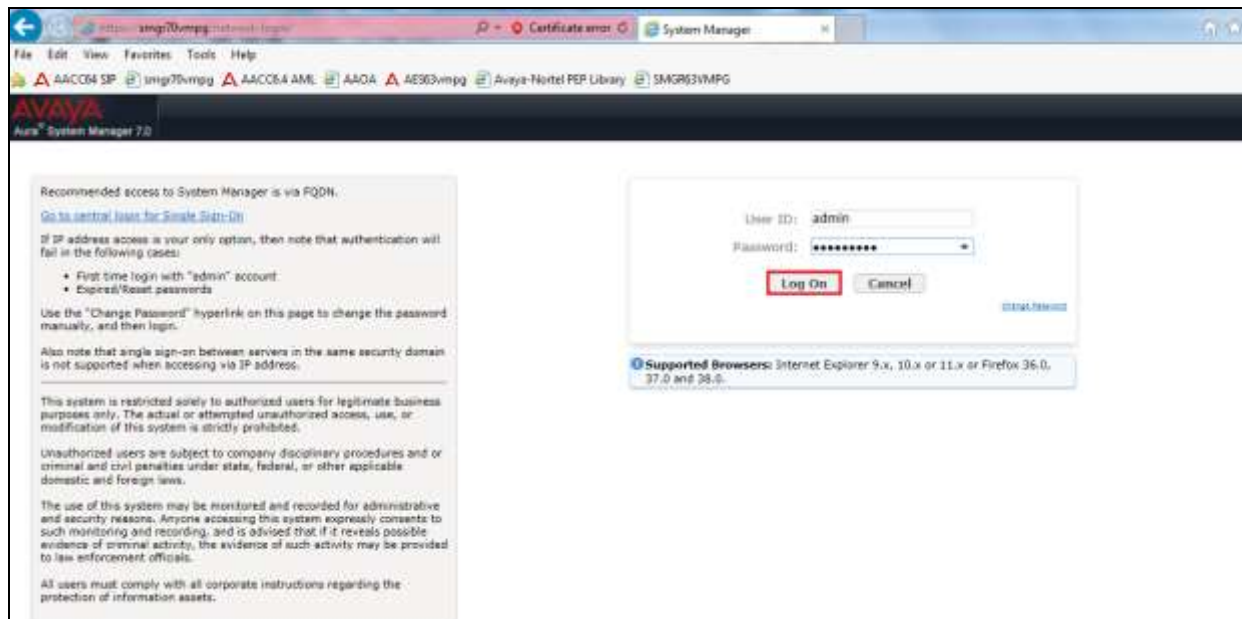
All endpoints that are to be monitored by Liquid Voice will need to have IP Softphone set to Y. IP Softphone must be enabled in order for Multi-Registration to work. Type **change station x** where x is the extension number of the station to be monitored also note this extension number for configuration required in **Section 8.1**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**.

change station x	Page 1 of 6	
STATION		
Extension: x	Lock Messages? n	BCC: 0
Type: 9608	Security Code: 1234	TN: 1
Port: S00101	Coverage Path 1:	COR: 1
Name: Extension	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext:	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	

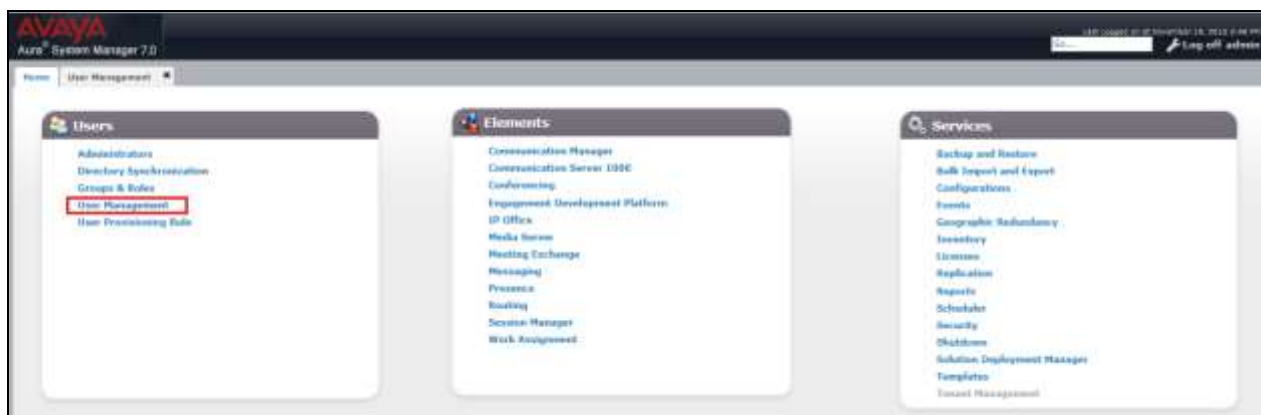
5.6. Configure SIP Stations for Multi-Registration

Any SIP extension that is to be recorded requires some configuration changes to allow call recording using multiple registration. Changes of SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a Web Browser by entering **http://<FQDN>/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager or **http://<IP Address>/SMGR**. Log in using appropriate credentials.

Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



From the home page click on **User Management** highlighted below.



Click on **Manager Users** in the left window. Select the station to be edited and click on **Edit**.

AVAYA Aura System Manager 7.0

Home / Users / User Management / Manage Users

User Management

Users

View Edit New Duplicate Delete More Actions

15 Items Show All

	Last Name	First Name	Display Name	Login Name	SIP Handle
<input checked="" type="checkbox"/>	7100	SIPEXt	7100, SIPEXt	7100@devconnect.local	7100
<input type="checkbox"/>	7101	SIPEXt	7101, SIPEXt	7101@devconnect.local	7101
<input type="checkbox"/>	7200	Ascom i62	7200, Ascom i62	7200@devconnect.local	7200
<input type="checkbox"/>	7201	Ascom i62	7201, Ascom i62	7201@devconnect.local	7201
<input type="checkbox"/>	7202	Ascom i62	7202, Ascom i62	7202@devconnect.local	7202
<input type="checkbox"/>	7203	Ascom i62	7203, Ascom i62	7203@devconnect.local	7203

Click on the **Communication Profile** tab. Ensure that the **Communication Profile Password** is known and if not click on edit to change it.

AVAYA Aura System Manager 7.0

Home / Users / User Management / Manage Users

User Profile Edit: 7100@devconnect.local

Identity Communication Profile Relationship Contacts

Communication Profile

Communication Profile Password: [Redacted]

Name: Primary

Default: ☒

Communication Address

Type	Handle	Domain
Avaya SIP	7100	devconnect.local

From the same page scroll down to **CM Endpoint Profile** click on **Endpoint Editor** to make further changes.

☒ **CM Endpoint Profile**

* System

cm70vmpg

* Profile Type

Endpoint

Use Existing Endpoints

☐

* Extension

7100

Endpoint Editor

Template

9641SIPCC DEFAULT CM 7 0

Set Type

9641SIPCC

Security Code

Port

S00003

Voice Mail Number

Preferred Handle

(None)

Calculate Route Pattern

☐

Sip Trunk

aar

Enhanced Callr-Info display for 1-line phones

☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User

☒

Override Endpoint Name and Localized Name

☒

Allow H.323 and SIP Endpoint Dual Registration

☐

In the **General Options** tab ensure that **Type of 3PCC Enabled** is set to **Avaya** as is shown below.

Edit Endpoint

System: cm70vmpp Extension: 7100
 Template: 9641SIPCC_DEFAULT_CM_7_8 Set Type: 9641SIPCC
 Port: 500003 Security Code:
 Name: 7100, SIPExt

General Options (G) * Feature Options (F) Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Feed (E) Button Assignment (B) Profile Settings (P) Group Membership (M)

* Class of Restriction (COR) 1
 * Emergency Location Ext 7100
 * Tenant Number 1
 * SIP Trunk Q aar
 Coverage Path 1
 Lock Message ☐
 Multibyte Language Not Applicable

* Class Of Service (COS) 1
 * Message Lamp Ext. 7100
Type of 3PCC Enabled Avaya
 Coverage Path 2
 Localized Display Name 7100, SIPExt
 Enable Reachability for Station Domain Control system

* Required

Click on the **Feature Options** tab and ensure that **IP Softphone** is ticked as shown. Click on **Done**, at the bottom of the screen, once this is set.

General Options (G) * **Feature Options (F)** Site Data (S) Abbreviated Call Dialing (A) Enhanced Call Feed (E) Button Assignment (B) Profile Settings (P) Group Membership (M)

Active Station Ringing single
 MWI Served User Type signalled
 Per Station CPN - Send Calling Number None
 IP Phone Group ID
 Remote Soft Phone Emergency Calls aar-local
 LWC Reception xps
 AUDIX Name
 Short/Prefixed Registration Allowed default
 Voice Mail Number

Auto Answer none
 Coverage After Forwarding system
 Display Language english
 Hunt-to Station
 Loss Group 19
 Survivable COR internal
 Time of Day Lock Table None
 Music Source

Features

☐ Always Use
☐ IP Audio Hairpinning
☐ Bridged Call Alerting
☐ Bridged Idle Line Preference
☒ Coverage Message Retrieval
☐ Data Restriction
☒ Survivable Trunk Dest
☐ Bridged Appearance Origination Restriction
☒ Restrict Last Appearance

☐ Idle Appearance Preference
☒ **IP SoftPhone**
☒ LWC Activation
☐ CDR Privacy
☒ Direct IP-IP Audio Connections
☐ H.323 Conversion
☐ IP Video Softphone
☐ Per Button Ring Control

* Required

Done Cancel

Click on **Commit** once this is done to save the changes.

The screenshot shows the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo and the text "Aura® System Manager 7.0". The left sidebar contains a "User Management" menu with options: "Manage Users", "Public Contacts", "Shared Addresses", "System Presence ACLs", "Communication Profile", and "Password Policy". The main content area is titled "User Profile Edit: 7100@devconnect.local". It features a "Communication Profile" tab with a "Communication Profile Password" field. Below this is a "Name" field with a dropdown menu showing "Primary" selected. A "Default" checkbox is checked. At the bottom, there is a "Communication Address" field. The interface includes "Commit & Continue", "Commit", and "Cancel" buttons. The bottom status bar shows "Last updated on 01/06/2016 01:10:11 PM" and a "Log off admin" link.

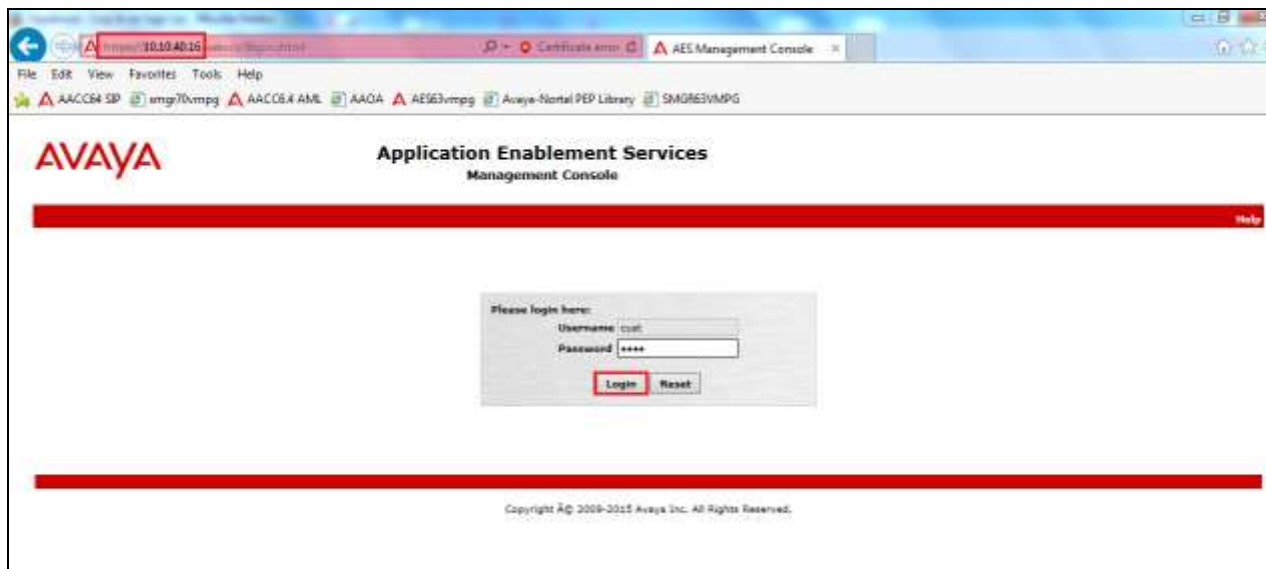
6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

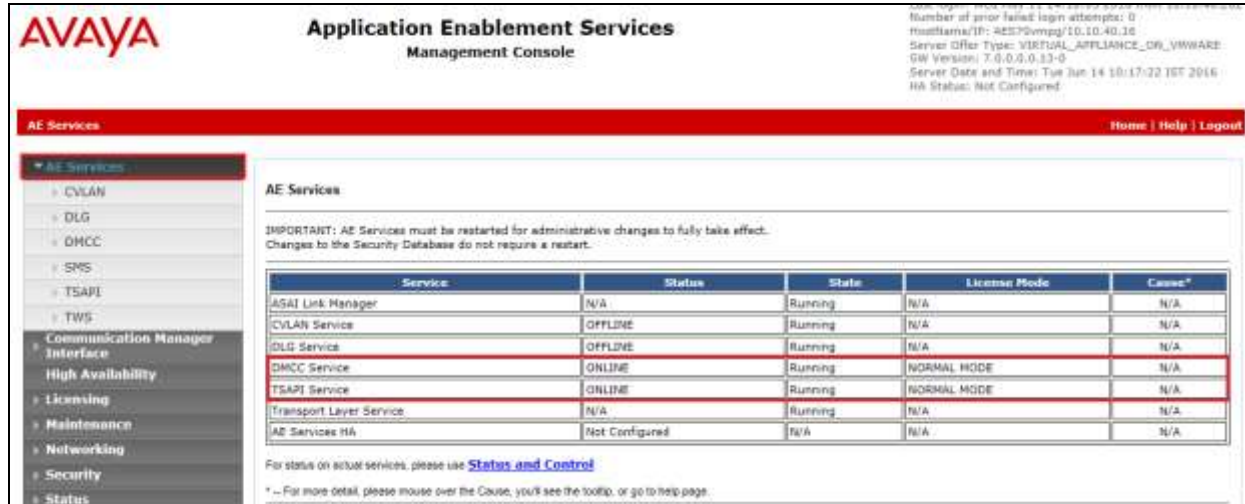
- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI and DMCC Ports
- Create CTI User
- Set Up Security Database on AES
- Associate Devices with CTI User

6.1. Verify Licensing

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.



The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that both the TSAPI and DMCC Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE** and the same for the **DMCC Service**. If not, contact an Avaya support representative to acquire the proper license for your solution.



AVAYA Application Enablement Services Management Console

Number of prior failed login attempts: 0
HostName/IP: AES70vmpg/10.10.40.10
Server Offer Type: VIRTUAL_APPLIANCE_OR_VMWARE
SW Version: 7.0.0.0.13-0
Server Date and Time: Tue Jun 14 10:17:22 IST 2016
HA Status: Not Configured

AE Services Home | Help | Logout

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

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

* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.



AVAYA Application Enablement Services Management Console

Welcome: user: cslc
Last login: Tue Nov 27 10:05:45 2015 from 10.55.46.222
Number of prior failed login attempts: 1
HostName/IP: aes70vmpg
Server Offer Type: VIRTUAL_APPLIANCE_OR_VMWARE
SW Version: 7.0.0.0.13-0
Server Date and Time: Tue Nov 24 10:08:06 CDT 2015
HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

en70vmpg Add Connection

Connection Name	Processor Ethernet	Max Period	Number of Active Connections
Edit Connection Edit FC/CVLAN 3Ps Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy			

In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3**. The remaining fields should show as below. Click **Apply** to save changes.

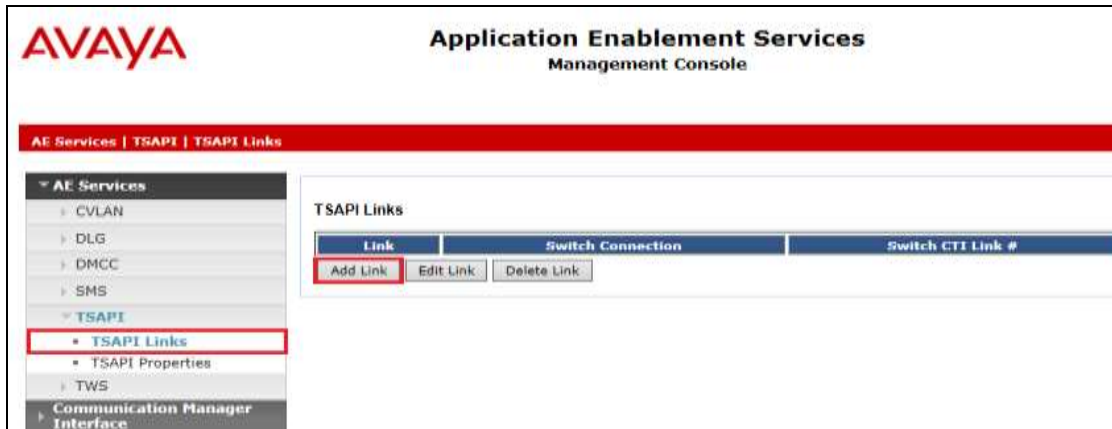
The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with the following items: AE Services, Communication Manager Interface (selected), Switch Connections (highlighted with a red box), Dial Plan, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Connection Details - cm70vmppg'. It contains the following fields: Switch Password (password field), Confirm Switch Password (password field), Msg Period (30 Minutes (1 - 72)), Provide AE Services certificate to switch (checkbox), Secure H323 Connection (checkbox), and Processor Ethernet (checked checkbox). The 'Apply' button is highlighted with a red box.

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown, see screen at the bottom of the previous page). In the resulting screen, enter the IP address of the procr as shown in **Section 5.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar is the same as the previous screenshot. The main content area is titled 'Edit Processor Ethernet IP - cm70vmppg'. It contains a table with the following columns: Name or IP Address. The table has one row with the value '10.10.40.13'. The 'Add/Edit Name or IP' button is highlighted with a red box. There is also a 'Back' button at the bottom left of the table.

6.3. Administer TSAPI link

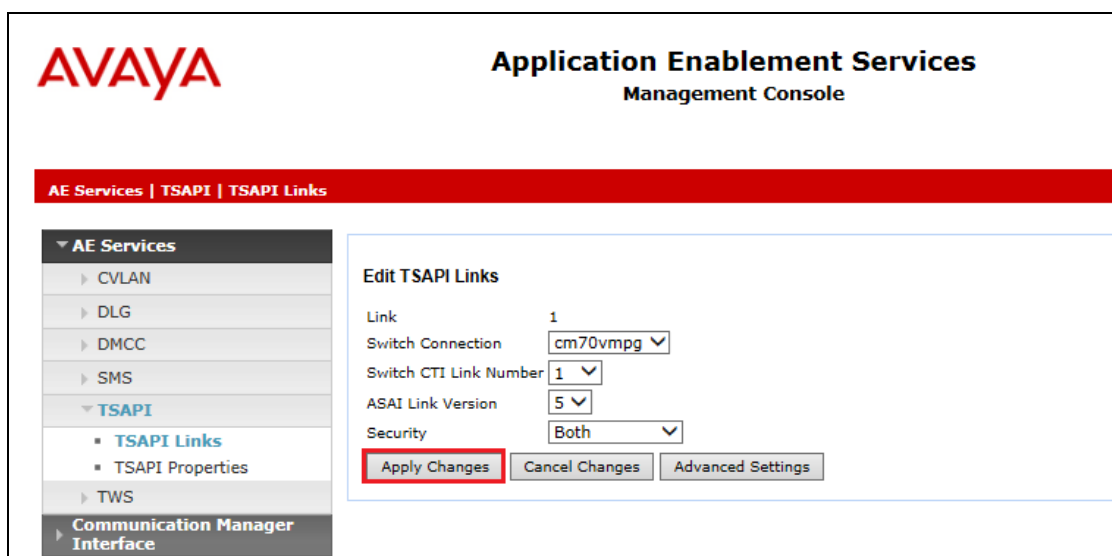
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm70vmppg**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **5**.
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.



Another screen appears for confirmation of the changes made. Choose **Apply**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (selected), and 'Communication Manager Interface'. The 'TSAPI' section is further expanded to show 'TSAPI Links' and 'TSAPI Properties'. The main content area displays a confirmation dialog titled 'Apply Changes to Link'. The dialog contains a warning message: 'Warning! Are you sure you want to apply the changes? These changes can only take effect when the TSAPI server restarts.' Below the warning is a yellow triangle icon and the text: 'Please use the Maintenance -> Service Controller page to restart the TSAPI server.' At the bottom of the dialog are two buttons: 'Apply' (highlighted with a red box) and 'Cancel'.

When the TSAPI Link is completed, it should resemble the screen below.

The screenshot shows the Avaya Application Enablement Services Management Console after the TSAPI link has been applied. The left sidebar is the same as in the previous screenshot, but the 'TSAPI Links' section is now expanded, showing a table of links. The table has five columns: 'Link', 'Switch Connection', 'Switch CTI Link #', 'ASAI Link Version', and 'Security'. There is one row in the table with the following values: '1', 'cm70vring', '1', '1', and 'Both'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'. In the top right corner, there is a status bar with the following information: 'Hostname/IP: aes70mrg', 'Server OS: Type: VIRTUAL_APPLIANCE_OPEL_UMWARE', 'SW Version: 7.0.0.0-0.12-0', 'Server Date and Time: Tue Nov 24 16:25:03 GMT 2015', and 'NA Status: Not Configured'.

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	cm70vring	1	1	Both

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance** → **Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.

AVAYA **Application Enablement Services**
Management Console

Maintenance | Service Controller

Service Controller

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

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

6.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure the Liquid Assure in **Section 7.1**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header features the Avaya logo and the title "Application Enablement Services Management Console". A red navigation bar contains the text "Security | Security Database | Tlinks". On the left, a sidebar menu lists various services, with "Security Database" and its sub-item "Tlinks" highlighted with red boxes. The main content area, titled "Tlinks", shows a "Tlink Name" section with two radio button options: "AVAYA#CM70VMPPG#CSTA#AES70VMPPG" (selected) and "AVAYA#CM70VMPPG#CSTA-S#AES70VMPPG". A "Delete Tlink" button is located below these options.

6.5. Enable TSAPI and DMCC Ports

To ensure that TSAPI ports are enabled, navigate to **Networking** → **Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below. Ensure that the **DMCC Server Ports** are also **Enabled** and take note of the **Unencrypted Port 4721** which will be used later in **Section 7.1**.

AVAYA Application Enablement Services Management Console

Networking | Ports

Ports

CVLAN Ports

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

DLG Port TCP Port 5678

TSAPI Ports

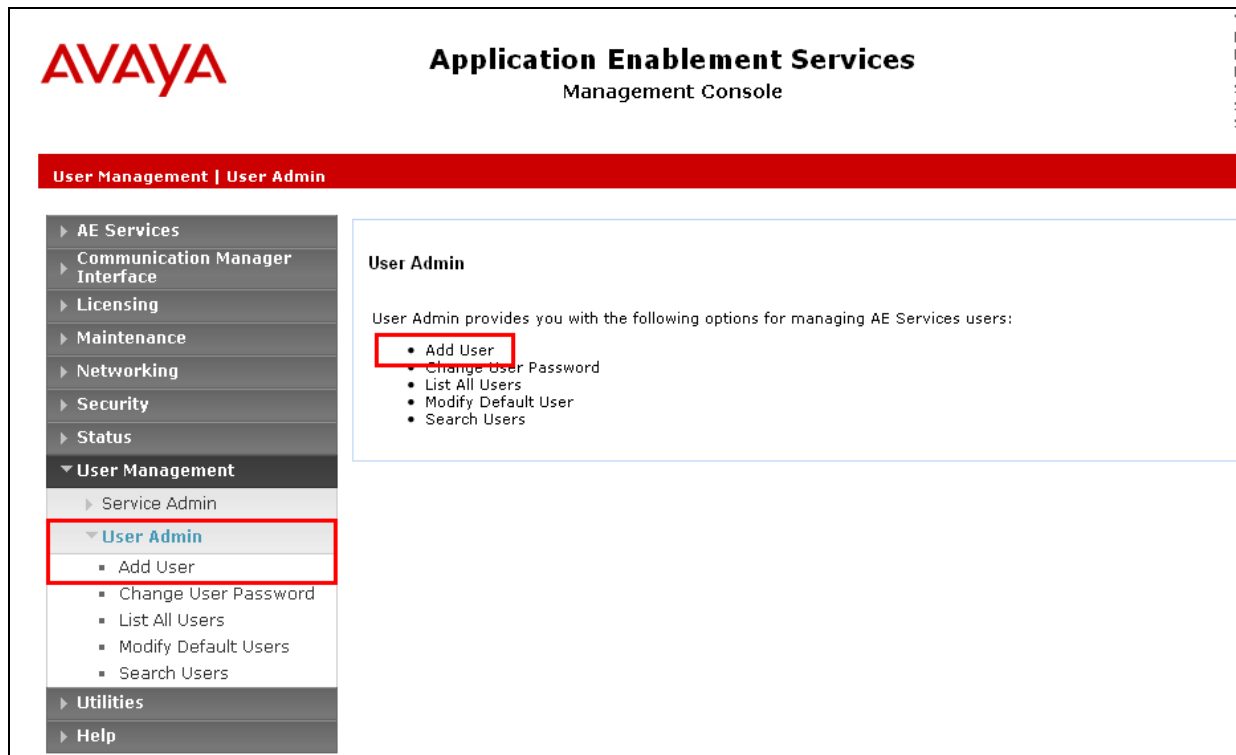
		Enabled Disabled
TSAPI Service Port	450	<input checked="" type="radio"/> <input type="radio"/>
Local TLINK Ports		
TCP Port Min	1024	
TCP Port Max	1039	
Unencrypted TLINK Ports		
TCP Port Min	<input type="text" value="1050"/>	
TCP Port Max	<input type="text" value="1065"/>	
Encrypted TLINK Ports		
TCP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

DMCC Server Ports

		Enabled Disabled
Unencrypted Port	<input type="text" value="4721"/>	<input checked="" type="radio"/> <input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>	<input checked="" type="radio"/> <input type="radio"/>
TR/87 Port	<input type="text" value="4723"/>	<input checked="" type="radio"/> <input type="radio"/>

6.6. Create CTI User

A User ID and password needs to be configured for the Liquid Assure to communicate with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.



In the **Add User** screen shown below, enter the following values:

- **User Id** - This will be used by the Liquid Assure setup in **Section 7.1**.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with Liquid Assure setup in **Section 7.1**.
- **CT User** - Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen.

AVAYA **Application Enablement Services**
Management Console

User Management | User Admin | List All Users

Edit User

* User Id: voice
* Common Name: voice
* Surname: voice
User Password:
Confirm Password:
Admin Note:
Avaya Role: None
Business Category:
Car License:
CM Home:
Cms Home:
CT User: Yes
Department Number:
Display Name:
Employee Number:
Employee Type:
Enterprise Handle:
Given Name:
Home Phone:
Home Postal Address:
Initials:
Labeled URI:
Mail:
MM Home:
Mobile:
Organization:
Pager:
Preferred Language: English
Room Number:
Telephone Number:
Apply Changes Cancel Changes

6.7. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 6.6** and click on **Edit**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with 'Security' expanded, showing 'CTI Users' and 'List All Users' (highlighted with a red box). The main content area displays a table of CTI Users with columns: User ID, Common Name, Worktop Name, and Device ID. A single user named 'voice' is listed. Below the table are 'Edit' and 'List All' buttons. The top right corner shows system information: Number of prior failed login attempts: 0, HostName/IP: AES70mrg/10.10.40.10, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 7.0.0.0.8.13.0, Server Date and Time: Wed May 11 11:31:35 IST 2016, HA Status: Not Configured.

User ID	Common Name	Worktop Name	Device ID
voice	voice	NONE	NONE

In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

The screenshot shows the 'Edit CTI User' page for the 'voice' user. The left sidebar is the same as the previous screenshot, with 'List All Users' highlighted. The main content area shows the 'Edit CTI User' form. The 'User Profile' section includes fields for User ID, Common Name, and Worktop Name, all with the value 'voice'. The 'Unrestricted Access' checkbox is checked and highlighted with a red box. Below this are sections for 'Call and Device Control', 'Call and Device Monitoring', and 'Routing Control', each with a dropdown menu set to 'None'. At the bottom are 'Apply Changes' and 'Cancel Changes' buttons, with 'Apply Changes' highlighted with a red box. The top right corner shows system information: Last login: Number of HostName, Server Off, SW Version, Server Dat, HA Status:.

User Profile:	User ID	voice
Common Name	voice	
Worktop Name	NONE	
Unrestricted Access	<input checked="" type="checkbox"/>	

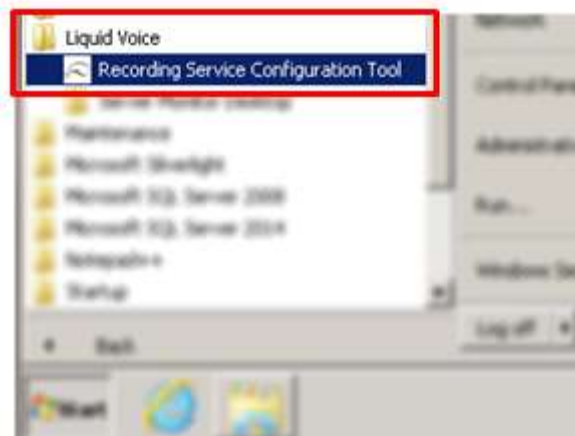
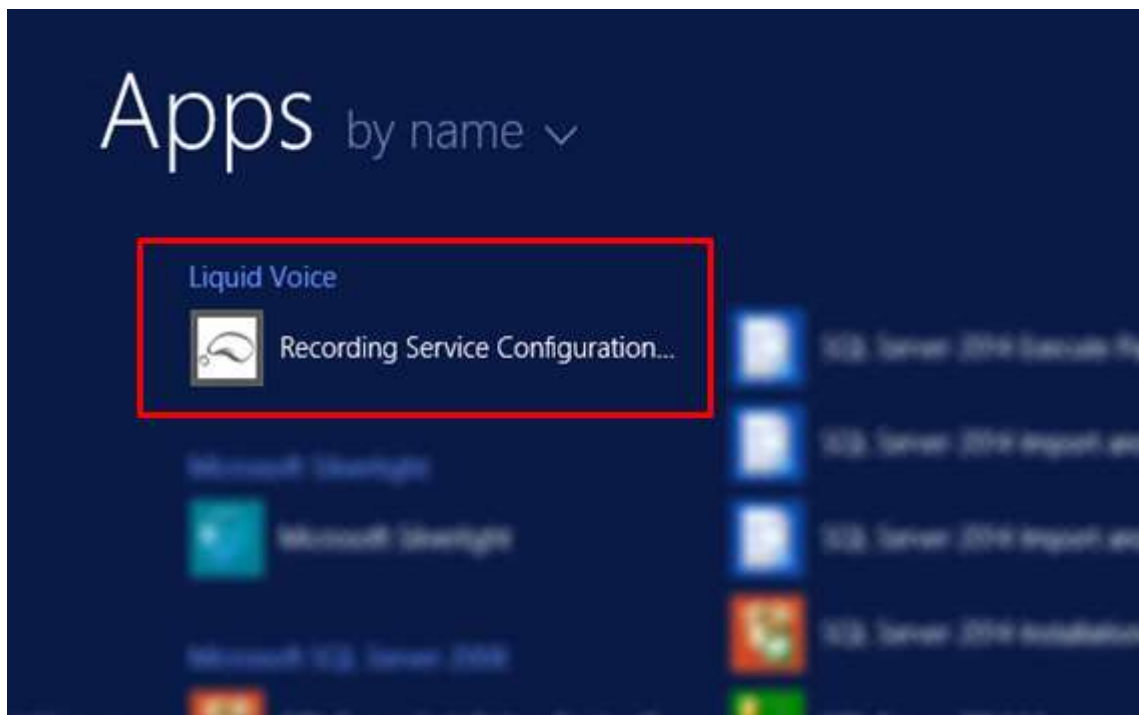
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring: <td>Device Monitoring</td> <td>None</td>	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	<input type="checkbox"/>

Routing Control:	Allow Routing on Listed Devices	None
------------------	---------------------------------	------

7. Configure Liquid Assure

The installation of Liquid Assure Recording is typically carried out by a Liquid Voice certified engineer and is outside the scope of these Application Notes. For information on the installation of Liquid Assure contact Liquid Voice as per the information provided in **Section 2.3**.

The following sections will outline the process involved in connecting the Liquid Assure to the Avaya solution. All configuration of the Liquid Assure for connection with the AES is performed from an application on the Liquid Assure server called **Recording Service Configuration Tool**, open this application as shown below depending on the Operating System of your server.



7.1. Configure connection to AES

With the Recording Service Configuration Tool opened, select the **DMCC** tab as shown, here the following information is added.

- **TLink String** This is the Tlink information from **Section 6.4**.
- **User/Password** This is the username and password configured in **Section 6.6**.
- **AES IP Address** This is the IP address of the AES server.
- **CM/CLAN IP** This is the IP address of Communication Manager as per **Section 5.2** where the procr address is displayed.
- **Recording IP** This is the IP address of the Liquid Assure server.
- **Protocol Version** Set to **7.0**.
- **Conferencing** Set to **N**.
- **Separate Calls** Set to **Y/N**** (see below for further explanation).

The remaining fields were left as default. **Save** can be pressed before moving to another tab.

The screenshot shows the 'Liquid Voice | Configuration' window with the 'DMCC' tab selected. The window contains the following fields and controls:

- Enabled:** Radio buttons for 'Yes' (selected) and 'No'.
- TLink String:** Text field containing 'AVAYA#CM70VMPPG#CSTA#AES70VMPPG'.
- User / Password:** Two text fields; the first contains 'voice' and the second contains '*****'.
- AES IP Address:** Text field containing '10.10.40.16'.
- Port *:** Text field containing '4721'.
- CM / CLAN IP:** Text field containing '10.10.40.13'.
- Switch Name *:** Text field containing 'CM70VMPPG'.
- Recording IP:** A dropdown menu.
- Protocol Version:** A dropdown menu set to '7.0'.
- Single Step Conferencing:** A dropdown menu set to 'N'.
- Separate Calls *:** A dropdown menu set to 'N'.
- DisableMultiRegMonitor *:** A dropdown menu set to 'N'.
- Silent Padding *:** A dropdown menu set to 'Y'.
- Use Jitter Buffer *:** A dropdown menu.

At the bottom of the window, there are three buttons: 'Reload', 'Save', and 'Exit'. A small note at the bottom right states '* denotes optional field'.

** Setting can be **Y** or **N** with **Y** separating calls for hold/transfer/conference. This setting will change the number of recordings present for calls that were held, transferred and conferenced. Separate Calls was set to both **Y** and **N** for compliance testing and works equally well for both. Whilst this setting is configurable it is advisable to consult Liquid Voice if you are considering changing this setting.

Click on the **Extensions** tab, all the Avaya phone sets that are to be “monitored” or recorded are added to the tab. If there are passwords on the phone sets and in this case there was of **1234** which was the case for all phone sets then a **Fixed** password can be applied as shown below. Entering each **Extension No** and clicking on Save at the bottom of the screen will result in the password being populated automatically for each extension.

Liquid Voice | Configuration

LIQUIDVOICE

Use the tabs below to configure the required devices. Not all devices are required depending on the other configuration options specified.

#	Extension No	Password
1	7050	1234
2	7000	1234
3	7100	1234
4	7101	1234
5	7010	1234
6	7011	1234
7	7001	1234
8	7020	1234
9	7021	1234

Password Policy

☐ Individual ☐ Use Ext No ☒ Fixed 1234

Recording Devices Hunt Groups

Reload Save Exit

This concludes the setup of the Liquid Assure Server for DMCC Multi-Registration recording.

8. Verification Steps

This section provides the steps that can be taken to verify correct configuration of the Liquid Assure and Avaya Aura® Application Enablement Services.

8.1. Verify Avaya Aura® Communication Manager CTI Service State

Before checking the connection between the Liquid Assure and AES, check the connection between Communication Manager and AES to ensure it is functioning correctly. Check the AESVCS link status by using the command **status aesvcs cti-link**. 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	Service State	Msgs Sent	Msgs Rcvd
1	5	no	aes70vmpg	established	18	18

8.2. Verify TSAPI Link

On the AES Management Console verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, and Status. The main area displays the 'TSAPI Link Details' screen. At the top, there's a header with the Avaya logo and 'Application Enablement Services Management Console'. Below this, a red banner indicates 'Status | Status and Control | TSAPI Service Summary'. The main content area shows a table with columns: Link, Switch Name, Switch CTI Link ID, Status, State, Switch Version, Associations, Msgs to Switch, Msgs from Switch, and Msgs Period. The table contains one row with the following data: Link 1, Switch Name cm70vmpg, Switch CTI Link ID 1, Status Talking, State Online, Switch Version 17, Associations 4, Msgs to Switch 15, Msgs from Switch 15, and Msgs Period 30. Below the table, there are buttons for 'Online' and 'Offline'. At the bottom, there's a section for 'For service-side information, choose one of the following:' with buttons for 'TSAPI Service Status', 'Link Status', and 'User Status'.

8.3. Verify DMCC link on AES

Verify the status of the DMCC link by selecting **Status** → **Status and Control** → **DMCC Service Summary** to display the **DMCC Service Summary – Session Summary** screen. The screen below shows that the user **voice** is connected from the IP address **10.10.40.59** which is the Liquid Assure server.

AVAYA Application Enablement Services Management Console

Number of prior failed login attempts: 0
HostName/IP: AES70vmqg/10.10.40.18
Server Offer Type: VSR11AL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.13-0
Server Date and Time: Wed May 11 14:10:26 IST 2016
HA Status: Not Configured

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

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Wed May 11 14:10:26 IST 2016

Service Uptime: 1 days, 21 hours 37 minutes
Number of Active Sessions: 1
Number of Sessions Created Since Service Boot: 1
Number of Existing Devices: 9
Number of Devices Created Since Service Boot: 9

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
CD7F29C76AE7E109A 1E3E250FB48EAB0-0	voice	Liquid Recording	10.10.40.59	XML Unencrypted	9

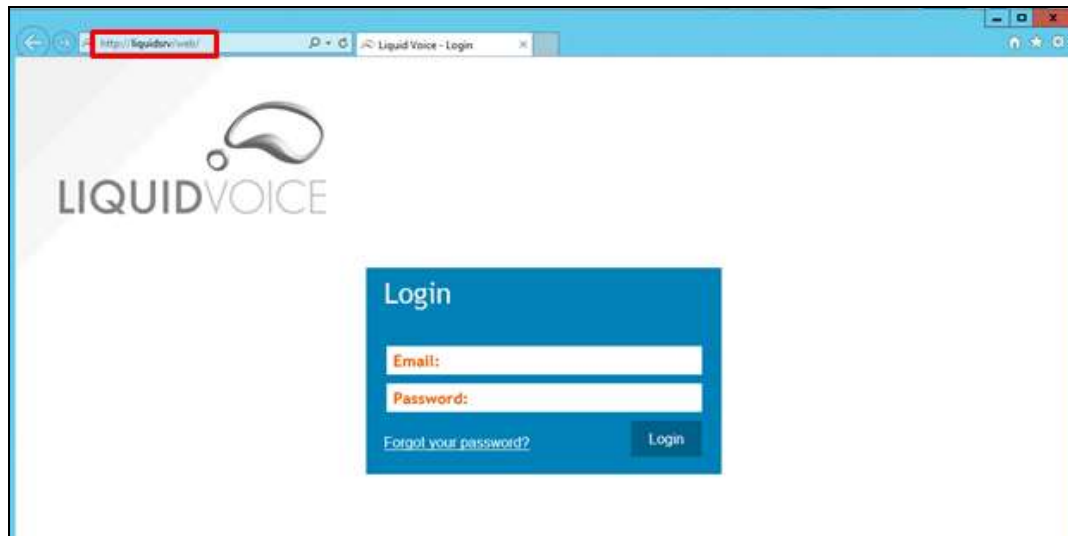
Item 1-1 of 1
1 50

Terminate Sessions Show Terminated Sessions

8.4. Verify calls are being recorded

From any of the monitored Avaya endpoints make a series of inbound and outbound calls. Once these calls are completed they should be available for playback through a web browser to the Liquid Assurance server.

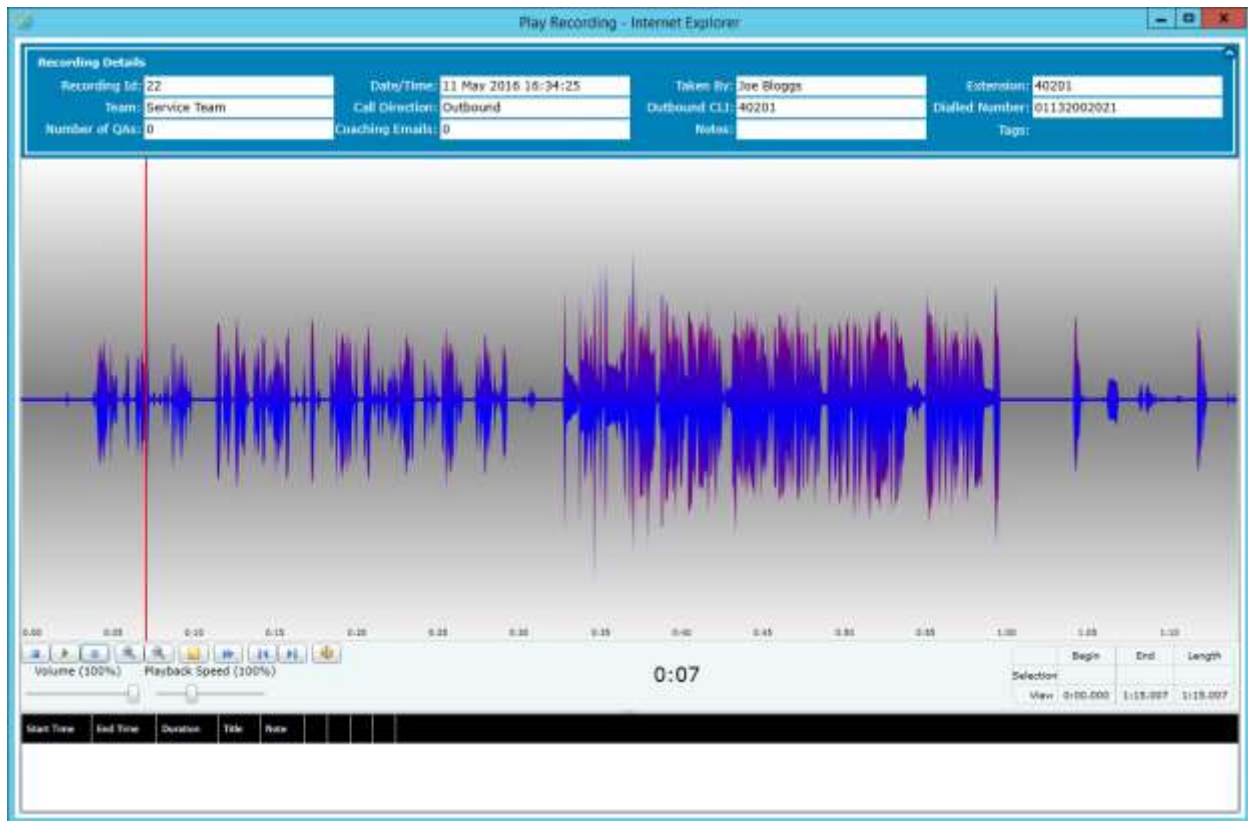
Open a browser session to the Liquid Assurance server as is shown below. If Liquid Assurance is configured for single sign-on the list of recordings will automatically appear, else enter appropriate login credentials and click on **Login**.



Once logged in the following window is automatically displayed. By default the system shows the most recent recordings first. There is a search panel on the left that can be used to filter the recording list by an abundance of different criteria. Click **Play** on the desired recording and this will open the built-in audio player and play back the call.

Recording ID	Date/Time	Duration	Extension	Taken By	Group	Caller ID	Phone Number	Called ID	Call Direction	Status	% Played
1001001	10/02/15 15:18:52	48	800	James Lee	Adm	0172000113	0145120010	0145120010	Incoming		
1001002	10/02/15 15:18:52	26	311	Andrew Agnew	Tech User	0740160415	0740160415	186262	Incoming		
1001003	10/02/15 15:18:52	58	310	Donald Pounds	Contact Centre 2	0123889716	0123889716	186262	Incoming		
1001004	10/02/15 15:18:52	2	310	Donald Pounds	Contact Centre 2			186262	Incoming		
1001005	10/02/15 15:18:52	76	304	James	Adm	07163100115	07163100115	186227	Incoming		
1001006	10/02/15 15:18:52	46	302	George Cook	Adm	071666-002	0716743666	0716743666	Outgoing		
1001007	10/02/15 15:18:52	498	400	Leanne Hall	Payments	01344118115	01344118115	01344118115	Outgoing		
1001008	10/02/15 15:18:52	117	308	Alan Pigg	Contact Centre 1	0766888020	0766888020	186211	Incoming		
1001009	10/02/15 15:18:52	187	300	Christopher Hobbs	Payments	01666660115	01666660115	01666660115	Outgoing		
1001010	10/02/15 15:18:52	9	300	Christopher Hobbs	Payments	01440111003	01440111003	01440111003	Outgoing		
1001011	10/02/15 15:18:52	46	311	Andrew Agnew	Tech User	0740-043677	0740-043677	186262	Incoming		
1001012	10/02/15 15:18:52	82	700	Trish Chaplin	Contact Centre 1	01666660115	01666660115	01666660115	Outgoing		
1001013	10/02/15 15:18:52	387	310	Jeff Henderson	Contact Centre 1	0162211862	0162211862	186279	Incoming		
1001014	10/02/15 15:18:52	137	710	Vanessa Taylor	Contact Centre 1	0162211862	0162211862	186279	Incoming		
1001015	10/02/15 15:18:52	31	310	Paul Cook	Contact Centre 2	07172114333	07172114333	07172114333	Outgoing		
1001016	10/02/15 15:18:52	11	310	Paul Cook	Contact Centre 2	07172114333	07172114333	07172114333	Outgoing		
1001017	10/02/15 15:18:52	94	700	Headed Bank	Contact Centre 1	0762200010	0762200010	0762200010	Outgoing		
1001018	10/02/15 15:18:52	72	310	Donald Pounds	Contact Centre 2			186262	Incoming		
1001019	10/02/15 15:18:52	118	800	Vide Wyatt	Adm	0700011344	0700011344	0700011344	Outgoing		
1001020	10/02/15 15:18:52	440	314	Rebecca Minter	Contact Centre 1	01270000100	01270000100	186262	Incoming		
1001021	10/02/15 15:18:52	82	311	Andrew Agnew	Tech User	0717201862	0717201862	0717201862	Outgoing		
1001022	10/02/15 15:18:52	82	800	Alan Pigg	Contact Centre 1			186262	Incoming		
1001023	10/02/15 15:18:52	7	300	Alan Pigg	Contact Centre 1			186262	Incoming		
1001024	10/02/15 15:18:52	131	700	Cal Sallis	Contact Centre 2			186262	Incoming		
1001025	10/02/15 15:18:52	34	710	Vanessa Taylor	Contact Centre 1			186262	Incoming		

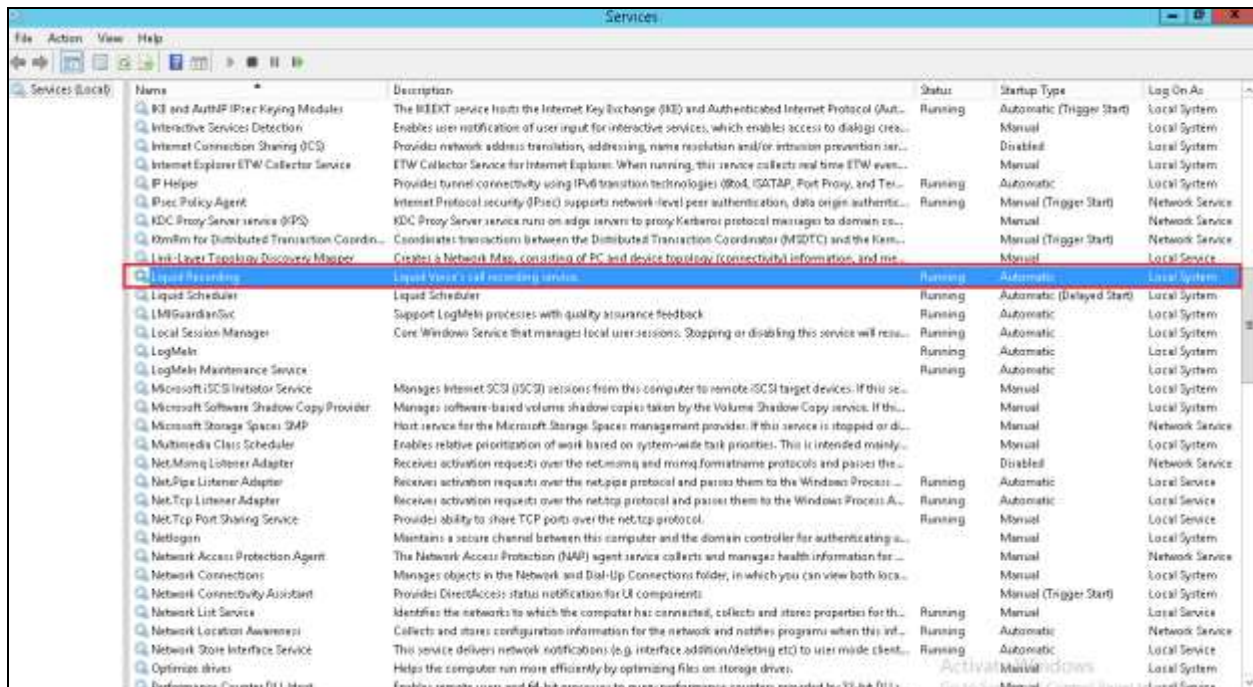
The player is opened and the recording is presented for playback. Click on the **Play/Pause** icons at the bottom of the screen to control and to play back the recording. Double clicking on the waveform will skip forward and backwards during playback as required.



8.5. Verify Liquid Voice Services

If these recordings are not present or cannot be played back the **Liquid Recording** service may not be running or may need to be restarted. The Liquid Assurance server can be logged into and checked to ensure that the **Liquid Recording** service is running.

A restart of the Recording service is required following certain configuration changes whilst others such as adding and removing Recording Devices can be changed ad-hoc. There may be a number of installed services associated with Liquid Voice, for the purposes of this document only the Recording service requires a restart.



Name	Description	Status	Startup Type	Log On As
Key and AuthN IPsec Keying Modules	The IKEEXT service hosts the Internet Key Exchange (IKE) and Authenticated Internet Protocol (Auth...	Running	Automatic (Trigger Start)	Local System
Interactive Services Detection	Enables user notification of user input for interactive services, which enables access to dialog crea...	Manual	Manual	Local System
Internet Connection Sharing (ICS)	Provides network address translation, addressing, name resolution and/or intrusion prevention ser...	Disabled	Disabled	Local System
Internet Explorer ETW Collector Service	ETW Collector Service for Internet Explorer: When running, this service collects real-time ETW even...	Manual	Manual	Local System
IP Helper	Provides tunnel connectivity using IPv6 transition technologies (6to4, ISATAP, Port Proxy, and Ter...	Running	Automatic	Local System
IPsec Policy Agent	Internet Protocol security (IPsec) supports network-level peer authentication, data origin authentic...	Running	Manual (Trigger Start)	Network Service
KDC Proxy Server service (KPS)	KDC Proxy Server service runs on edge servers to proxy Kerberos protocol messages to domain co...	Manual	Manual	Network Service
Krmflm for Distributed Transaction Coordi...	Coordinates transactions between the Distributed Transaction Coordinator (MSDTC) and the Rem...	Manual (Trigger Start)	Manual (Trigger Start)	Network Service
Link-Layer Topology Discovery Mapper	Creates a Network Map, consisting of PC and device topology (connectivity) information, and me...	Manual	Manual	Local Service
Liquid Recording	Liquid Voice's call recording service.	Running	Automatic	Local System
Liquid Scheduler	Liquid Scheduler	Running	Automatic (Delayed Start)	Local System
LMIGuardianSvc	Support LogMeIn processes with quality assurance feedback	Running	Automatic	Local System
Local Session Manager	Core Windows Service that manages local user sessions. Stopping or disabling this service will resu...	Running	Automatic	Local System
LogMeIn	LogMeIn	Running	Automatic	Local System
LogMeIn Maintenance Service	LogMeIn	Running	Automatic	Local System
Microsoft iSCSI Initiator Service	Manages Internet SCSI (iSCSI) sessions from this computer to remote iSCSI target devices. If this se...	Manual	Manual	Local System
Microsoft Software Shadow Copy Provider	Manages software-based volume shadow copies taken by the Volume Shadow Copy service. If this...	Manual	Manual	Local System
Microsoft Storage Spaces SMP	Host service for the Microsoft Storage Spaces management provider. If this service is stopped or di...	Manual	Manual	Network Service
Multimedia Class Scheduler	Enables relative prioritization of work based on system-wide task priorities. This is intended mainl...	Manual	Manual	Local System
Net.Monoq Listener Adapter	Receives activation requests over the net.monoq protocol and passes them to the Windows Process...	Disabled	Disabled	Network Service
Net.Pipe Listener Adapter	Receives activation requests over the net.pipe protocol and passes them to the Windows Process A...	Running	Automatic	Local Service
Net.Tcp Listener Adapter	Receives activation requests over the net.tcp protocol and passes them to the Windows Process A...	Running	Automatic	Local Service
Net.Tcp Port Sharing Service	Provides ability to share TCP ports over the net.tcp protocol.	Running	Manual	Local Service
Netlogon	Maintains a secure channel between this computer and the domain controller for authenticating a...	Manual	Manual	Local System
Network Access Protection Agent	The Network Access Protection (NAP) agent service collects and manages health information for...	Manual	Manual	Network Service
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which you can view both loca...	Manual	Manual	Local System
Network Connectivity Assistant	Provides DirectAccess status notification for UI components.	Manual (Trigger Start)	Manual (Trigger Start)	Local System
Network List Service	Identifies the networks to which the computer has connected, collects and stores properties for th...	Running	Manual	Local Service
Network Location Awareness	Collects and stores configuration information for the network and notifies programs when this inf...	Running	Automatic	Network Service
Network Store Interface Service	This service delivers network notifications (e.g. interface addition/deletion etc) to user mode client...	Running	Automatic	Local Service
Optimize drives	Helps the computer run more efficiently by optimizing files on storage drives.	Manual	Manual	Local System
Performance Counter DLL Host	Enables remote users and 64-bit processes to query performance counters provided by 32-bit DLLs...	Manual	Manual	Local Service

9. Conclusion

These Application Notes describe the configuration steps required for Liquid Assure R7.1 from Liquid Voice to successfully interoperate with Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services R7.0 to connect to using DMCC Multi-Registration to record calls. All feature functionality and serviceability test cases were completed successfully with some issues and observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and Liquid Voice product documentation that are relevant to these Application Notes.

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

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 7.0

Product documentation for Liquid Voice products may be found at:

- Website <http://www.liquidvoice.com>
- Telephone +44 (0) 113 200 2020
- Email support@liquidvoice.com

Appendix

Avaya one-X® Agent Softphone

This is a printout of the Avaya one-X® Agent softphone used during compliance testing.

display station 7011		Page 1 of 5
STATION		
Extension: 2100	Lock Messages? n	BCC: 0
Type: 9630	Security Code: *	TN: 1
Port: S00031	Coverage Path 1:	COR: 1
Name: one-X Agent1	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 7011	
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	

display station 7011		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced	Audible Message Waiting? n	
MWI Served User Type:	Display Client Redirection? n	
AUDIX Name:	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 7011	Always Use? n IP Audio Hairpinning? n	

display station 7011	STATION	Page 3 of 5
<p>Conf/Trans on Primary Appearance? n</p> <p>Bridged Appearance Origination Restriction? n</p>		
<p>Call Appearance Display Format: disp-param-default</p> <p>IP Phone Group ID:</p> <p>Enhanced Callr-Info Display for 1-Line Phones? n</p>		
<p>ENHANCED CALL FORWARDING</p>		
	Forwarded Destination	Active
Unconditional For Internal Calls To: 1000		n
External Calls To: 1000		n
Busy For Internal Calls To:		n
External Calls To:		n
No Reply For Internal Calls To:		n
External Calls To:		n
<p>SAC/CF Override: n</p>		

display station 7011	STATION	Page 4 of 5															
<p>SITE DATA</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 50%;">Room:</td> <td style="width: 50%;">Headset? n</td> </tr> <tr> <td>Jack:</td> <td>Speaker? n</td> </tr> <tr> <td>Cable:</td> <td>Mounting: d</td> </tr> <tr> <td>Floor:</td> <td>Cord Length: 0</td> </tr> <tr> <td>Building:</td> <td>Set Color:</td> </tr> </table>			Room:	Headset? n	Jack:	Speaker? n	Cable:	Mounting: d	Floor:	Cord Length: 0	Building:	Set Color:					
Room:	Headset? n																
Jack:	Speaker? n																
Cable:	Mounting: d																
Floor:	Cord Length: 0																
Building:	Set Color:																
<p>ABBREVIATED DIALING</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 33%;">List1:</td> <td style="width: 33%;">List2:</td> <td style="width: 33%;">List3:</td> </tr> </table>			List1:	List2:	List3:												
List1:	List2:	List3:															
<p>BUTTON ASSIGNMENTS</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 33%;">1: call-appr</td> <td style="width: 33%;">5: manual-in</td> <td style="width: 33%;">Grp:</td> </tr> <tr> <td>2: call-appr</td> <td>6: after-call</td> <td>Grp:</td> </tr> <tr> <td>3: call-appr</td> <td>7: aux-work</td> <td>RC: Grp:</td> </tr> <tr> <td>4: auto-in</td> <td>8:</td> <td></td> </tr> <tr> <td colspan="3"> <p>voice-mail</p> </td> </tr> </table>			1: call-appr	5: manual-in	Grp:	2: call-appr	6: after-call	Grp:	3: call-appr	7: aux-work	RC: Grp:	4: auto-in	8:		<p>voice-mail</p>		
1: call-appr	5: manual-in	Grp:															
2: call-appr	6: after-call	Grp:															
3: call-appr	7: aux-work	RC: Grp:															
4: auto-in	8:																
<p>voice-mail</p>																	

Avaya 9608 H.323 Deskphone

This is a printout of the Avaya 9608 H.323 deskphone used during compliance testing.

display station 7000	Page 1 of 5	
STATION		
Extension: 7000	Lock Messages? n	BCC: 0
Type: 9608	Security Code: *	TN: 1
Port: S00000	Coverage Path 1: 1	COR: 1
Name: Ext2000	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 7000	
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: yes	
	Customizable Labels? y	

display station 7000	Page 2 of 5
STATION	
FEATURE OPTIONS	
LWC Reception: spe	Auto Select Any Idle Appearance? n
LWC Activation? y	Coverage Msg Retrieval? y
LWC Log External Calls? n	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Redirect Notification? y	Idle Appearance Preference? n
Per Button Ring Control? n	Bridged Idle Line Preference? n
Bridged Call Alerting? n	Restrict Last Appearance? y
Active Station Ringing: single	
	EMU Login Allowed? n
H.320 Conversion? n	Per Station CPN - Send Calling Number?
Service Link Mode: as-needed	EC500 State: enabled
Multimedia Mode: enhanced	Audible Message Waiting? n
MWI Served User Type: sip-adjunct	Display Client Redirection? n
	Select Last Used Appearance? n
	Coverage After Forwarding? s
	Multimedia Early Answer? n
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y
Emergency Location Ext: 7000	Always Use? n IP Audio Hairpinning? n

display station 7000 Page 3 of 5

STATION

```

Conf/Trans on Primary Appearance? n
Bridged Appearance Origination Restriction? n    Offline Call Logging? y
Require Mutual Authentication if TLS? n

```

```

Call Appearance Display Format: disp-param-default
IP Phone Group ID:
Enhanced Callr-Info Display for 1-Line Phones? n

```

ENHANCED CALL FORWARDING

				Forwarded Destination	Active
Unconditional For		Internal Calls To:		n	
		External Calls To:		n	
Busy For		Internal Calls To:		n	
		External Calls To:		n	
No Reply For		Internal Calls To:		n	
		External Calls To:		n	

SAC/CF Override: n

display station 7000 Page 4 of 5

STATION

SITE DATA

```

Room:                               Headset? n
Jack:                               Speaker? n
Cable:                             Mounting: d
Floor:                             Cord Length: 0
Building:                           Set Color:

```

ABBREVIATED DIALING

```
List1:      List2:      List3:
```

BUTTON ASSIGNMENTS

```
1: call-appr          5: call-park
2: call-appr          6:
3: call-appr          7:
4: extnd-call         8:
```

voice-mail

©2016 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.