



Avaya Solution & Interoperability Test Lab

Application Notes for configuring the Verba Collaboration Compliance Platform 8.9 to interoperate with Avaya Aura® Communication Manager R7.0.1 and Avaya Aura® Application Enablement Services R7.0.1 - Issue 1.0

Abstract

These Application Notes describe the configuration steps for Verba Collaboration Compliance Platform to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Verba Collaboration Compliance Platform integrates with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using dual registration implemented via DMCC over TSAPI.

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 compliance tested configuration of Verba Collaboration Compliance Platform (CCP) with Avaya Aura® Communication Manager (Communication Manager) R7.0 and Avaya Aura® Application Enablement Services (AES) R7.0 to record telephone conversations.

Verba CCP uses Communication Manager's Dual registration via the Device, Media, and Call Control (DMCC) service provided by the AES to capture the audio and call details for recording agent calls. Verba CCP uses the AES' DMCC service to monitor a pool of telephones that are used as present on the Communication Manager as extensions. Target devices, whose calls are to be recorded, are configured on the Verba CCP

The Verba CCP is fully integrated into a LAN (Local Area Network), and includes easy-to-use web based application that works with Java to retrieve telephone conversations from a comprehensive long-term calls database.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of Verba CCP to carry out call recording in a variety of scenarios using DMCC with AES and Communication Manager.

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 Calls
- Outbound Calls
- Call Hold
- Blind Transfer
- Consultative Transfer
- Blind Conference
- Supervised Conference
- Forwarded Calls
- EC500 and Feature Calls
- Inbound Calls to Communication Manager Call Center Agents

The serviceability testing focused on verifying the ability of Verba CCP to recover from disconnection and reconnection to the Avaya solution.

2.2. Test Results

All functionality and serviceability test cases were completed successfully with the following observations.

- For outbound calls over ISDN trunks to the PSTN, a valid connected number is required by AES. If this is not returned from the service provider, AES does not pass an “Established Event” to the Verba CCP server. This issue is a known issue and a fix is planned for AES Service Pack 4.

The above issue is with AES and is not an issue with the Verba CCP recorder.

2.3. Support

Technical support can be obtained for Verba CCP as follows:

- Email: support@verba.com
- Website: <http://support.verba.com>
- Phone: 1-888-90-83722

3. Reference Configuration

Figure 1 shows the network topology during interoperability testing. Communication Manager with an Avaya G430 Gateway was used as the hosting PBX. Verba CCP is connected to the LAN and recording is performed using the Dual Registration feature of Communication Manager using DMCC provided by AES.

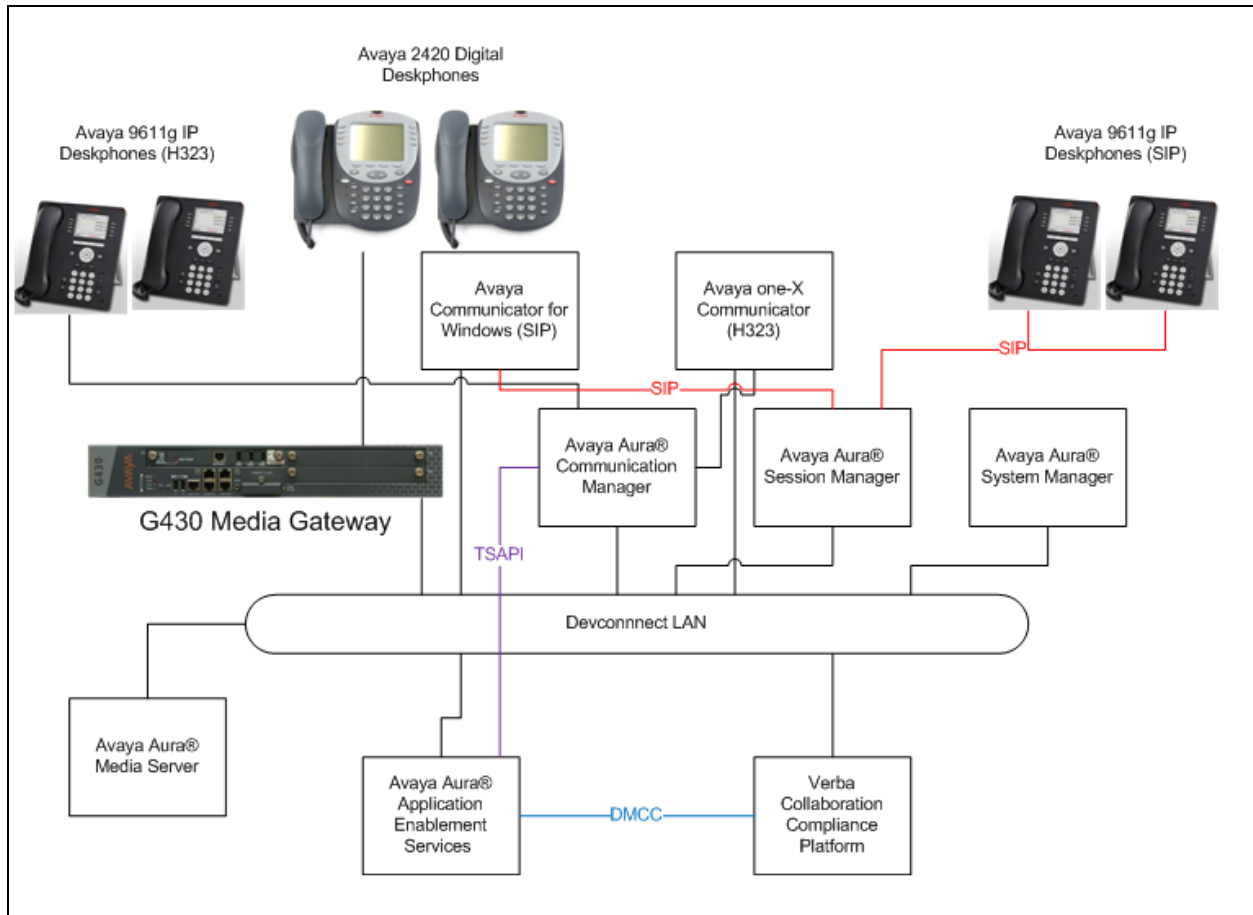


Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services, and Verba Collaboration Compliance Platform

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	7.0.1.2 Build – 7.0.0.0.16266 Software Update Revision Number: 7.0.1.2.086007 Service Pack 2
Avaya Aura® Communication Manager running on a virtual server	R17x.00.0.441.0 Version CM 7.0.1.2.0.441.23523
Avaya Aura® Session Manager running on a virtual server	7.0.1.2.701230
Avaya Aura® Application Enablement Services running on a virtual server	7.0.1.0.3.15-0
Avaya Aura® Media Server	7.7.0.200
Avaya G430 Gateway	37.11.0/1
Avaya 9641g Series Deskphone	96x1 H.323 Release 6.6229
Avaya 9611g Series Deskphone	96x1 H323 Release 6.6229
Avaya 9611g Series Deskphone	96x1 SIP Release 7.0.0-080615
Avaya 9641g Series Deskphone	96x1 SIP Release 7.0.0-080615
Avaya one-X® Agent	2.5.8.3
Avaya Equinox for Windows	3.1.0.14
Avaya 2420 Digital Deskphone	NA
Verba Collaboration Compliance Platform	V8.9.5024.0

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 **Answer Supervision by Call Classifier?** is set to **y** and **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. Display Node Names 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 (**Aes71678**).

display node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
SM100	10.10.40.34	
Aes71678	10.10.16.78	
default	0.0.0.0	
g430	10.10.40.15	
procr	10.10.16.27	

5.3. Configure AE service 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 **aes63vmppg**.
- **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** should 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:	aes71678	*****	y	idle		
2:						
3:						

5.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. 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: 2002		
Type: ADJ-IP		
COR: 1		
Name: aes71678		

5.5. Configure Monitored Stations

Verba CCP uses the Dual Registration method with the calls in order to capture the call audio. Use the command, **change station** to configure a station. To allow the station to be monitored, on **Page 1** set **IP SoftPhone** to **y**. Repeat for all extensions that need to be recorded.

change station 8270001		Page 1 of 6
STATION		
Extension: 8270001	Lock Messages? n	BCC: 0
Type: 9640	Security Code: 1234	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: Station, 8270001	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: 1591	
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	

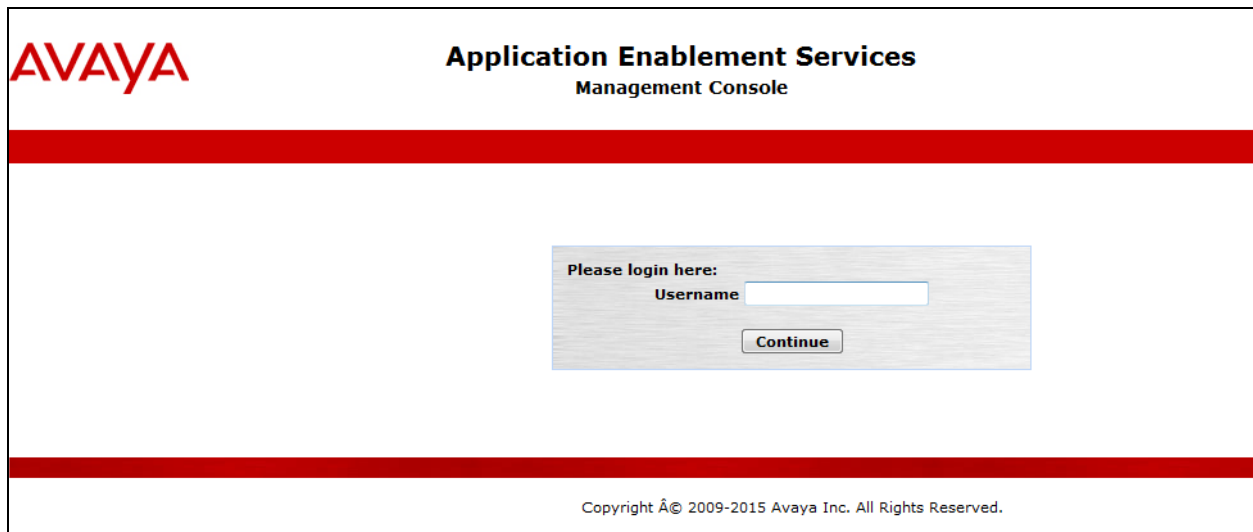
6. Configure Avaya Aura® Application Enablement Services

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.
- Create CTI User.
- Enable Unrestricted Access for CTI Link User.
- Enable DMCC ports.

6.1. Verify Licensing

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



The screenshot shows the login interface for the Avaya Application Enablement Services Management Console. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A thick red horizontal bar separates the header from the main content area. In the center of the page is a login box with a light gray background. Inside this box, the text "Please login here:" is followed by a label "Username" and a text input field. Below the input field is a button labeled "Continue". Another thick red horizontal bar is located below the login box. At the bottom of the page, centered, is the copyright notice: "Copyright © 2009-2015 Avaya Inc. All Rights Reserved."

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

Application Enablement Services Management Console

Welcome: User cust
Last login: Tue Feb 23 13:07:53 2016 from 10.10.16.8
Number of prior failed login attempts: 0
HostName/IP: AES71678/10.10.16.78
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.0.1315-0
Server Date and Time: Wed Feb 24 14:39:56 GMT 2016
HA Status: Not Configured

AE Services

Home | Help | Logout

AE Services

CVLAN

DLG

DMCC

SMS

TSAPI

TWS

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

User Management

Utilities

Help

AE Services

This AE Services server is using a default installed server certificate. Default installed certificates should not be used in a production environment. It is highly recommended to replace all default installed certificates.

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.

License Information
You are licensed to run Application Enablement (CTI) release 7.x

6.2. Create Switch Connection

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

AE Services

Communication Manager Interface

Switch Connections

Dial Plan

Switch Connections

CM1627

Add Connection

Connection Name

Processor Ethernet

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** Default values may be accepted for the remaining fields. Click **Apply** to save changes.

Connection Details - CM1627

Switch Password: [Masked]

Confirm Switch Password: [Masked]

Msg Period: 30 Minutes (1 - 72)

Provide AE Services certificate to switch: ☒

Secure H323 Connection: ☐

Processor Ethernet: ☒

Apply Cancel

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown). 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.

Edit Processor Ethernet IP - CM1627

10.10.16.27 Add/Edit Name or IP

Name or IP Address

Back

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.

The screenshot shows the 'AE Services' sidebar on the left with 'TSAPI' selected. The main panel is titled 'TSAPI Links' and contains a table with two columns: 'Link' and 'Switch Connection'. Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'.

On the **Add TSAPI Links** screen, enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM1627**, 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 **7**.
- **Security:** select **Both** from the drop down.

Once completed, select **Apply Changes**.

The screenshot shows the 'Edit TSAPI Links' configuration screen. The sidebar on the left shows 'TSAPI Links' selected under 'AE Services'. The main panel contains the following fields and values:

Field	Value
Link	1
Switch Connection	CM1627
Switch CTI Link Number	1
ASAI Link Version	7
Security	Both

At the bottom of the main panel are three buttons: 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

Another screen appears for confirmation of the changes. Choose **Apply** (not shown).

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**.

The screenshot shows the 'Service Controller' management console. On the left is a navigation menu with the following items: 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance' (expanded), 'Date Time/NTP Server', 'Security Database', 'Service Controller' (highlighted in blue), 'Server Data', 'Networking', and 'Security'. The main panel is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists six services: ASAI Link Manager, DMCC Service, CVLAN Service, DLG Service, Transport Layer Service, and TSAPI Service. Each service has a checkbox to its left. The 'TSAPI Service' checkbox is checked. All services show a status of 'Running'. Below the table, there is a text prompt: 'For status on actual services, please use [Status and Control](#)'. At the bottom of the panel are four buttons: 'Start', 'Stop', 'Restart Service', and 'Restart AE Server'.

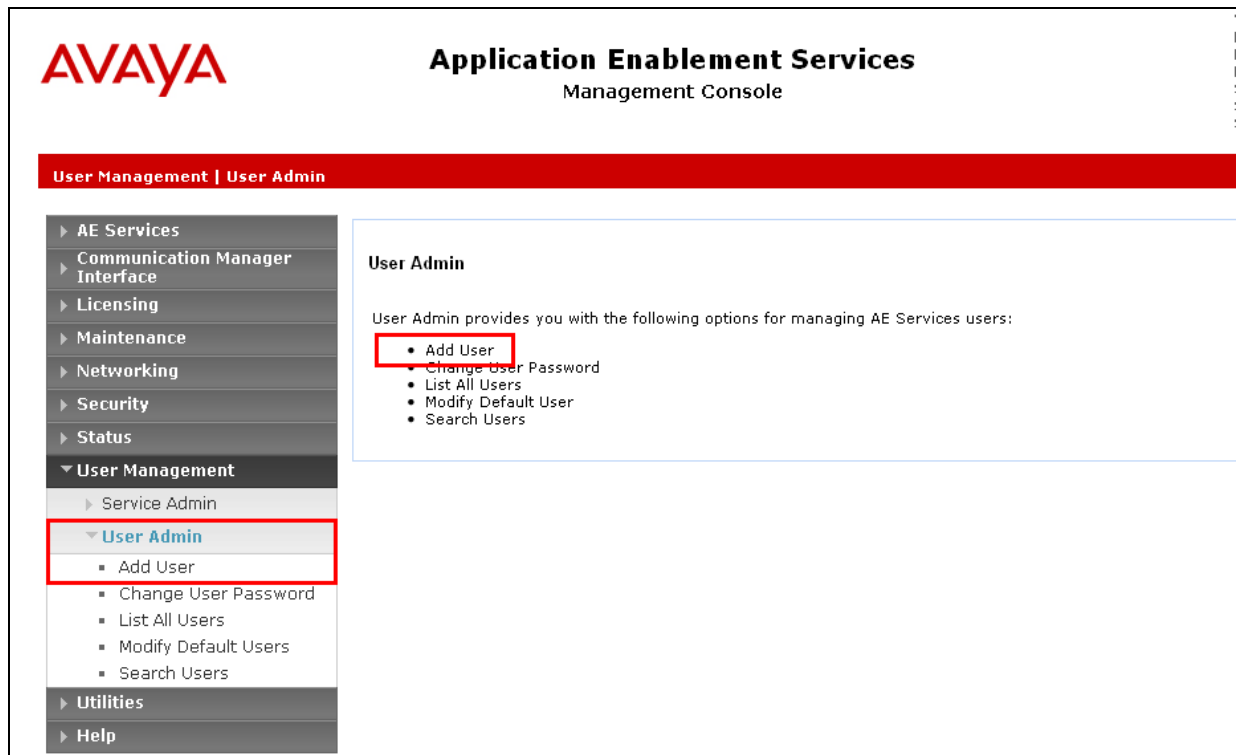
Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/>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

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

Start Stop Restart Service Restart AE Server

6.4. Create CTI User

A User ID and password needs to be configured for the Verba CCP to communicate as a TSAPI client 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 CCP Server to connect.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will be used with the **User Id** to connect.
- **CT User** - Select **Yes** from the drop-down menu.

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message for user 'cust' along with system details like last login, failed attempts, and server information. A red navigation bar contains links for 'User Management', 'User Admin', 'Add User', 'Home', 'Help', and 'Logout'. On the left, a sidebar menu lists various services, with 'User Management' expanded to show 'User Admin' and 'Add User'. The main content area is titled 'Add User' and contains a form with the following fields: 'User Id' (value: verba), 'Common Name' (value: Verba), 'Surname' (value: CCP), 'User Password' (masked with dots), 'Confirm Password' (masked with dots), 'Admin Note' (empty), 'Avaya Role' (dropdown menu showing 'None'), 'Business Category' (empty), 'Car License' (empty), 'CM Home' (empty), 'Css Home' (empty), and 'CT User' (dropdown menu showing 'Yes'). A note at the top of the form states 'Fields marked with * can not be empty.'

Complete the process by choosing **Apply** at the bottom of the screen (not shown).

The next screen will show a message indicating that the user was created successfully (not shown).

6.5. Enable Unrestricted Access for CTI User

Navigate to the **CTI Users** screen by selecting **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the user that was created in **Section 6.4** and select the **Edit** option (not shown).

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, and Security. The Security Database is expanded, showing CTI Users. The main area displays a table of CTI Users.

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> pomcti	POM	NONE	NONE
<input type="radio"/> presence	presence	NONE	NONE
<input checked="" type="radio"/> verba	Verba	NONE	NONE

The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

The screenshot shows the Avaya Application Enablement Services Management Console with the 'Edit CTI User' screen. The user profile for 'verba' is displayed, showing fields for User ID, Common Name, Worktop Name, and Unrestricted Access (checked). Below this are sections for Call and Device Control, Call and Device Monitoring, and Routing Control, each with a dropdown menu. At the bottom, there are 'Apply Changes' and 'Cancel Changes' buttons.

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

Call and Device Control:	
Call Origination/Termination and Device Status	None ▼

Call and Device Monitoring:	
Device Monitoring	None ▼
Calls On A Device Monitoring	None ▼
Call Monitoring	<input type="checkbox"/>

Routing Control:	
Allow Routing on Listed Devices	None ▼

A screen (not shown) appears to confirm applied changes to CTI User, choose **Apply**. This CTI user should now be enabled.

6.6. Enable DMCC ports

In order to enable DMCC for call recording navigate to **Networking → Ports → DMCC Server Ports**.

- Enable DMCC **Unencrypted Port**
- Enable DMCC **Encrypted Port**
- Enable DMCC **TR/87 Port**

Click on **Apply Changes** at the bottom of the screen (not shown).

Networking | Ports

► AE Services
► Communication Manager Interface
► Licensing
► Maintenance
▼ **Networking**
 AE Service IP (Local IP)
 Network Configure
 Ports
 TCP Settings
► Security
► Status
► User Management
► Utilities
► Help

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"/>

Once this change is made a restart of the AE Server is required. Navigate to **Maintenance** → **Service Controller**. In the main screen select **Restart AE Server** highlighted.

AVAYA **Application Enablement Services**
Management Console

Maintenance | Service Controller

Left Sidebar:

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▼ **Maintenance**
- ▶ Date Time/NTP Server
- ▶ Security Database
- Service Controller**
- ▶ Server Data
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

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 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

7. Configure Verba Collaboration Compliance Platform

The configuration of the Verba CCP is achieved by opening a web session connecting to that servers IP address using an internet browser.

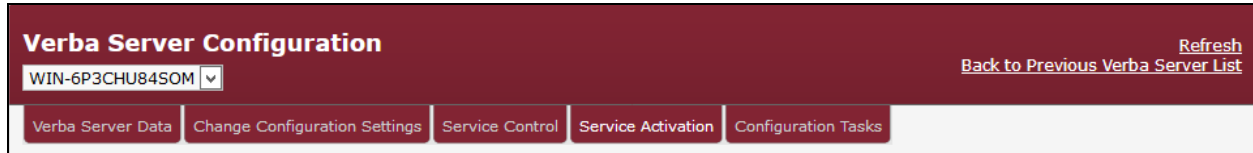
Open a web session to <https://<ServerIP>/>. Enter a valid username and password and click on **Login**.



The image shows the login interface of the Verba Collaboration Compliance Platform. The background is a dark red color. In the top left corner, the word "verba" is written in a white, lowercase, sans-serif font. In the top right corner, there is a small white square button with a question mark icon. Below the logo, there are two input fields: "Login ID:" and "Password:". The "Password:" field has a small white checkbox to its right with an asterisk symbol. Below these fields is a grey "Login" button. Below the login fields, there is a line of text: "* Click the check box to enable four eyes login!". Below that, it says "The software is licensed to: **Avaya Certification Lab**" and "Version: **8.9.5024.0**". Below that, it says "(c) Copyright Verba Technologies, LLC. 2000-2017. All rights reserved.". At the bottom, there is a paragraph of text: "The software is furnished under a license agreement and may be used or copied only in accordance with the terms of the license agreement. It is against the law to copy the software on any other medium except as specifically allowed in the license agreement. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopy, recording, or otherwise, without the prior written permission of Verba Technologies, LLC. This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately."

7.1. Configure the Avaya Recorder service

Go to the **Change Configuration Settings** tab in the Verba Server management screen (**Administration** → **Verba servers** → **Server selection**).

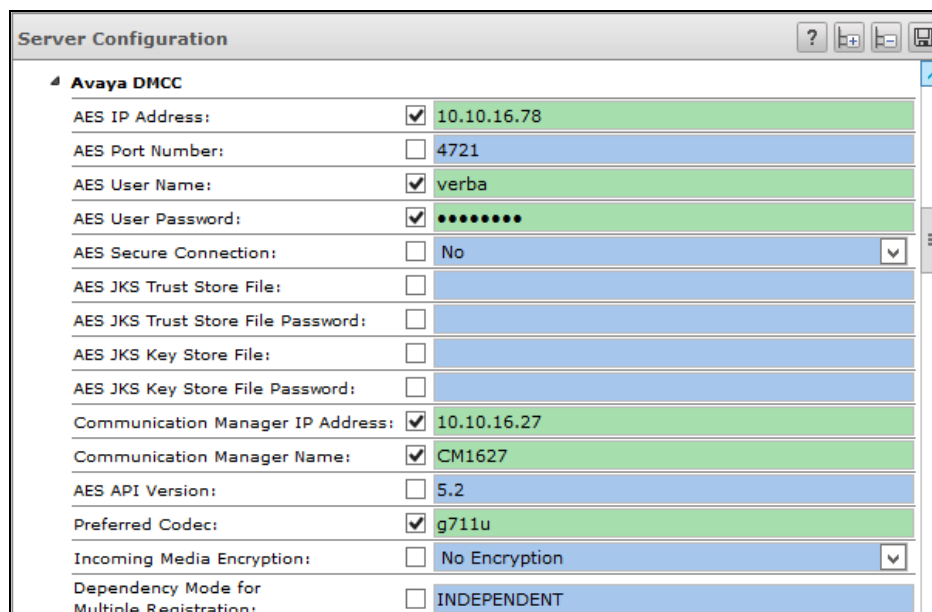


The image shows the 'Verba Server Configuration' window. At the top, there's a header bar with the title 'Verba Server Configuration' and a 'Refresh' button. Below the header, there's a dropdown menu showing 'WIN-6P3CHU84SOM'. To the right of the dropdown, there's a link 'Back to Previous Verba Server List'. Below the header bar, there are five tabs: 'Verba Server Data', 'Change Configuration Settings', 'Service Control', 'Service Activation', and 'Configuration Tasks'. The 'Change Configuration Settings' tab is currently selected.

7.1.1. Avaya DMCC section

Select **Avaya Recorder** → **Avaya DMCC**. Select the following entries and complete the Application Enablement Services and Communication manager information.

- **AES IP Address:** The IP Address of the AES server. One Recording Server can only connect to one AES server
- **AES Port Number:** Communication port of the AES server
- **AES User Name:** The user in AES that has the rights for DMCC to execute the necessary commands
- **AES User Password:** Password of the AES User
- **Communication Manager IP Address:** The IP address of Communication Manager. If there are ESS servers, then list them separated by commas (,) after the primary Communication Manager. Only one of the two entries need to be set (either the IP or the hostname)
- **Communication Manager Name:** The name of Communication Manager. If there are ESS servers, then list them separated by commas (,) after the primary Communication Manager. Only one of the two entries need to be set (either the IP or the hostname)



The image shows the 'Avaya DMCC' configuration window. It has a title bar 'Server Configuration' with standard window controls. The main area is titled 'Avaya DMCC' and contains a list of configuration items, each with a checkbox and a text field. The items are: AES IP Address (checked, 10.10.16.78), AES Port Number (unchecked, 4721), AES User Name (checked, verba), AES User Password (checked, masked with dots), AES Secure Connection (unchecked, No), AES JKS Trust Store File (unchecked), AES JKS Trust Store File Password (unchecked), AES JKS Key Store File (unchecked), AES JKS Key Store File Password (unchecked), Communication Manager IP Address (checked, 10.10.16.27), Communication Manager Name (checked, CM1627), AES API Version (unchecked, 5.2), Preferred Codec (checked, g711u), Incoming Media Encryption (unchecked, No Encryption), and Dependency Mode for Multiple Registration (unchecked, INDEPENDENT). The text fields are highlighted in green.

7.1.2. Avaya JTAPI section

Select **Avaya Recorder** → **Avaya JTAPI**. Configure as follows:

- **Avaya Tlink Name:** Tlink name for Communication Manager. This is displayed on the interface of the AES
- **JTAPI User Name:** The name of the AES user that has the necessary rights to communicate through JTAPI (This can be the same user as is used for DMCC in the previous section)
- **JTAPI User Password:** Password of the AES user
- **Disable Agent ID Handling:** The use of agent IDs can be disabled
- **Hunt Group for Monitored Agent(s):** special/"dummy" group that includes all agents. This is needed for JTAPI to gather additional information on the users
- **Agent Status Check Interval (seconds):** The system queries the agents status with a time interval that is set here

Avaya JTAPI		
Avaya Tlink Name:	<input checked="" type="checkbox"/>	AVAYA#CM1627#CSTA#AES71678
JTAPI User Name:	<input checked="" type="checkbox"/>	verba
JTAPI User Password:	<input checked="" type="checkbox"/>	••••••••
JTAPI JKS Trust Store File:	<input type="checkbox"/>	
JTAPI JKS Trust Store File Password:	<input type="checkbox"/>	
Disable Agent ID Handling:	<input type="checkbox"/>	No <input type="button" value="v"/>
Hunt Group for Monitored Agent(s):	<input checked="" type="checkbox"/>	8273060
Agent Status Check Interval (seconds):	<input type="checkbox"/>	3600

7.1.3. Media Recorders section

Select **Avaya Recorder → Media Recorders**. First, click on the add icon at the Media Recorder Server configuration, then click on the gear icon(⚙️) at the end of the line .

Complete the configuration as shown below.

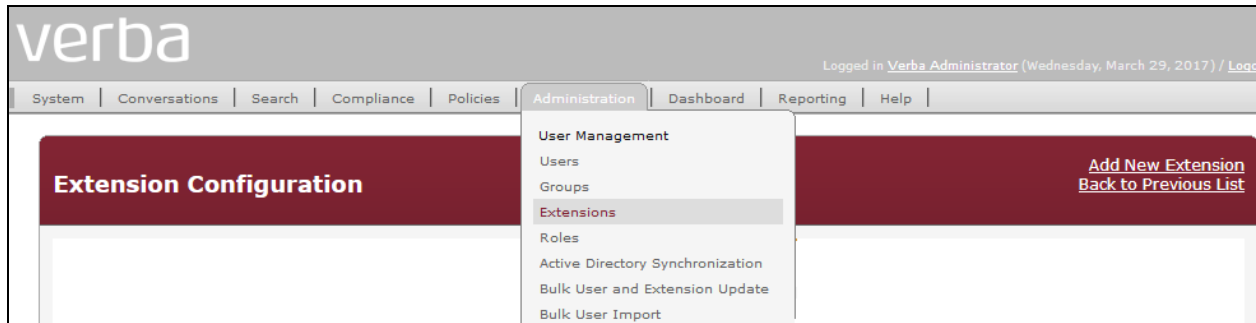
- **Protocol:** vrp
- **User:** This is the user that the service is using to connect to the Media Recorder and is configured for the Unified Call Recorder service.
- **Password:** Password of the user that connects to the Media Recorder.
- **Host:** Hostname or IP address of the machine where the Media Recorder service is running.
- **Port:** Port where the Media Recorder component is listening for incoming connections.

The screenshot displays the 'Server Configuration' window. On the left, the 'Media Recorders' section is expanded, showing a list of 'Media Recorder Servers'. One server is listed with the URL 'vrp://verba:1vcYm2yq7Fr5WuO3yi9oQQ==@V'. To the right of this list is a '+' icon for adding new servers and a gear icon (⚙️) for editing the selected server. Below the list are several configuration options with checkboxes and input fields: 'Minimum Number of Active Media Recorder Servers' (set to 1), 'Number of Connection Retry Attempts' (set to 2), 'Sleep Time Between Retries (seconds)' (set to 5), 'Connection Keepalive Interval (seconds)' (set to 5), and 'Connection Timeout (seconds)' (set to 5). On the right side of the window, the 'Remote Media Recording Servers' section is visible, showing fields for 'Protocol' (vrp), 'User' (verba), 'Password' (masked with dots), 'Host' (WIN-6P3CHU84SOM), and 'Port' (10500).

When changes are complete click on the Save button in top right corner of the configuration tree(? ⚙️ ⏮️ ⏭️).

7.2. Add Monitored Extensions

All extensions on Communication Manager that are required for monitoring by Verba CCP must be added as extensions. From the Main menu on the web interface select **Administration** → **Extensions**.



Click on **Add New Extension**.



For every Extension required add the **Extension** number on Communication Manager. **Recording Mode** is set to **Full** and **Voice** is selected.

Extension Data	
Synchronized by Active Directory	<input type="checkbox"/> Synchronization is not enabled because there are no configured Active Directory Profiles.
Extension*	<input type="text" value="8270001"/> Phone number ('1234') or address ('user@company.com')
User	<input type="text"/> If a user is missing from the list, please verify the Valid Until and Valid From fields of that user.
Type*	<input type="text" value="Number/Address"/> <input type="button" value="v"/>
Update user information on existing conversations	Apply on: <input checked="" type="radio"/> new conversations <input type="radio"/> unassigned conversations <input type="radio"/> all conversations <input type="checkbox"/> Update conversations within the user's validity period only User information can not be updated if there is no associated User to the Extension.
Description	<input type="text"/>
Recording Settings	
Recording Mode*	<input type="text" value="Full"/> <input type="button" value="v"/>
Voice	<input checked="" type="checkbox"/>

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can validate that the communication between Communication Manager and AES is functioning correctly. Check the AESVCS link status with AES 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	4	no	aes71678	established	18	18

8.2. Verify TSAPI Link and DMCC

This section will verify both the TAPI and DMCC links between the AES and Communication Manager.

8.2.1. 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**.

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

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
1	CM1627	1	Talking	Tue Jul 26 10:03:32 2016	Online	17	9	15	15	30

Online Offline

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

TSAPI Service Status TLink Status User Status

8.2.2. Verify Avaya Aura® Application Enablement Services DMCC Service

The following steps are carried out on AES to validate that the communication link between AES and the Verba CCP is functioning correctly. 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. It shows a connection to the Verba CCP server IP address **10.10.16.95**. The **Application** is shown as **cmapiApplication**, and the **Far-end Identifier** is given as the IP address **10.10.16.95** as expected.

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Log Manager

Logs

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Thu Jul 28 08:13:30 IST 2016

Service Uptime: 1 days, 22 hours 9 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 4

Number of Existing Devices: 6

Number of Devices Created Since Service Boot: 18

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	55BB86290F3297363 1BAEC2FCC9517F9-3		cmapiApplication	10.10.16.95	XML Unencrypted	6

Item 1-1 of 1

1 Go

8.3. Verify the Verba CCP Avaya Recorder Services

Navigate to the **Administration → Verba Servers** menu item and select the corresponding server from the list. **WIN-6P3CHU84SOM** was the server used during testing.

Find and List Verba Servers			
Add New Verba Ser Discover Verba Serv View Last Conversations by Verba Serv Apply Extension Configur Refresh			
1 item found, displaying all items. Page(s): 1			
Hostname	Role	Configuration Profile	Shared
WIN-6P3CHU84SOM	Media Repository & Recording Server	Default Media Repository and Recording Server Configuration Profile (2)	No
1 item found, displaying all items. Page(s): 1			

Click on the **Service Activation** tab. Check the following services are **Running**.

- **Verba Avaya DMCC/JTAPI Service**
- **Verba Unified Call Recorder Service**

Verba Server Configuration				
WIN-6P3CHU84SOM				
Refresh Back to Previous Verba Server List				
Verba Server Data Change Configuration Settings Service Control Service Activation Configuration Tasks				
Name	Status	Startup Type	Executable Version	Activation
Microsoft SQL Server Agent Service	Stopped	Disabled	2011.110.3000.0	
Microsoft SQL Server Browser Service	Stopped	Disabled	2011.110.2100.60	
Microsoft SQL Server Service	Running	Automatic	2011.110.3000.0	
Verba Analogue and Radio Recorder Service	Stopped	Disabled	8.9.5024.0	
Verba Announcement Service	Stopped	Disabled	8.9.5024.0	
Verba Avaya DMCC/JTAPI Service	Running	Automatic	unknown	
Verba Media Utility Service	Running	Automatic	8.9.5024.0	
Verba Node Manager Agent	Running	Automatic	8.9.5024.0	
Verba Passive Recorder Service	Stopped	Disabled	8.9.5024.0	
Verba Screen Capture Multiplexer Service	Stopped	Disabled	8.9.5024.0	
Verba SfB/Lync IM Recorder Service	Stopped	Disabled	8.9.5024.0	
Verba Speech Analytics Service	Stopped	Disabled	8.9.5024.0	








8.4. Verify Verba Collaboration Compliance Platform Recordings

The playback of Verba CCP recordings is achieved by opening a web session connecting to that servers IP address.

Using an internet browser open a web session to <https://<ServerIP>/verba>. Enter a valid username and password and click on Login. **Select Conversations → My Conversations** (not shown) from the main menu. Select a date and time range that calls were made and to show all calls leave the **Phone Number** and **User** blank. Click on **Search** to find calls.

The screenshot shows the search interface with two date pickers. The left picker is set to March 29, 2017, at 11:00. The right picker is set to March 29, 2017, at 23:59. Below the date pickers are input fields for 'Phone Number (From or To Party)', 'User', and 'Label'. There is a checkbox for 'Search conference participants'. At the bottom, there are expandable sections for 'Advanced Search Options', 'Metadata and Markers', and 'Instant Messaging'. A 'Reset Search' link and a 'Search...' button are also present.

Select a call from the list.

Conversations									
108 items found, displaying 1 to 20. Page(s): < 1 2 3 4 5 6 > > Results per page 20									
Labels	Start Date	Start Time	Duration	From	From Info	To	To Info	Direction	
      	Mar 29, 2017	9:57:25 AM	00:00:32	8270005	H323 Station 8270005	8270003	H323 Station 8270003	Internal	

The call can be saved as a .wav file by clicking on the **File format WAVE** and saving the file. This can be played back in any windows media player that supports this format.

▼ Conversation Details Data ?			
Start Time	Mar 29, 2017 9:57:25 AM		End Time Mar 29, 2017 9:57:58 AM
Duration	00:00:32		Direction Internal
From	8270005	To	8270003
From Info	H323 Station 8270005		To Info H323 Station 8270003
Verba From Party Name		Verba To Party Name	
Conversation Identifier	bafd0e70-145d-11e7-811e-14feb5d77692		Recording Server WIN-6P3CHU84SOM
From IP	10.10.16.32		To IP
From Proxy IP			To Proxy IP
Audio codec	G.711 u-law 64k		Video Codec
Archived	No		Source Platform 12
Conversation Type	Voice		Forward Reason
End Cause	Normal		File format WAVE XML
Storage Target			Data Retention Events Calculate
End of Retention			Delete after End of Retention No

9. Conclusion

These Application Notes describe the configuration steps required for Verba collaboration Compliance Platform to successfully interoperate with Avaya Aura® Communication Manager R7.0.1 using Avaya Aura® Application Enablement Services R7.0.1. All feature functionality and serviceability test cases were completed successfully as outlined in **Section 2.2**.

10. Additional References

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

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

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

Product documentation for Verba CCP can be obtained as follows:

- Email: support@verba.com
- Website: <http://support.verba.com>
- Phone: 1-888-90-83722

©2017 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.