



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Verion Research Veriva 3i DMCC Recorder with Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Application Enablement Services 6.1.1 - Issue 1.0**

### **Abstract**

These Application Notes describe the procedure for configuring Veriva 3i DMCC Recorder to monitor and record calls placed to and from stations and agents on Avaya Aura® Communication Manager. Veriva 3i DMCC Recorder uses the Telephony Services Application Programming Interface (TSAPI) and Device, Media and Call Control (DMCC) API to interface with Avaya Aura® Application Enablement Services.

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 a compliance-tested configuration comprised of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Veriva 3i DMCC Recorder.

Veriva 3i DMCC Recorder is a software-based IP call recording solution. Veriva 3i DMCC Recorder communicates with Application Enablement Services (AES) using the Telephony Services Application Programming Interface (TSAPI) and Device, Media and Call Control (DMCC) API. Using DMCC, it registers IP stations on Communication Manager and uses them to service-observe every extension that is configured to be recorded. When a call starts on any of those extensions, the DMCC station will also receive the audio packets which it will then record them. Detailed call information obtained using TSAPI are also stored for each call along with the recording.

## 2. General Test Approach and Test Results

The general approach was to place various types of calls to and from stations, agents, and Vector Directory Numbers (VDNs), monitor and record them using Veriva 3i DMCC Recorder, and verify the recordings.

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 feature and serviceability testing.

For feature testing, the types of calls included internal calls, inbound and outbound trunk calls, transferred calls, and conference calls. For serviceability testing, failures such as disconnecting the LAN cable to the Veriva 3i DMCC Recorder server and AES server, as well as rebooting the Veriva 3i DMCC Recorder server and of Communication Manager were applied.

### 2.2. Test Results

All test cases passed successfully. However, on demand and scheduled recordings are not available in this version.

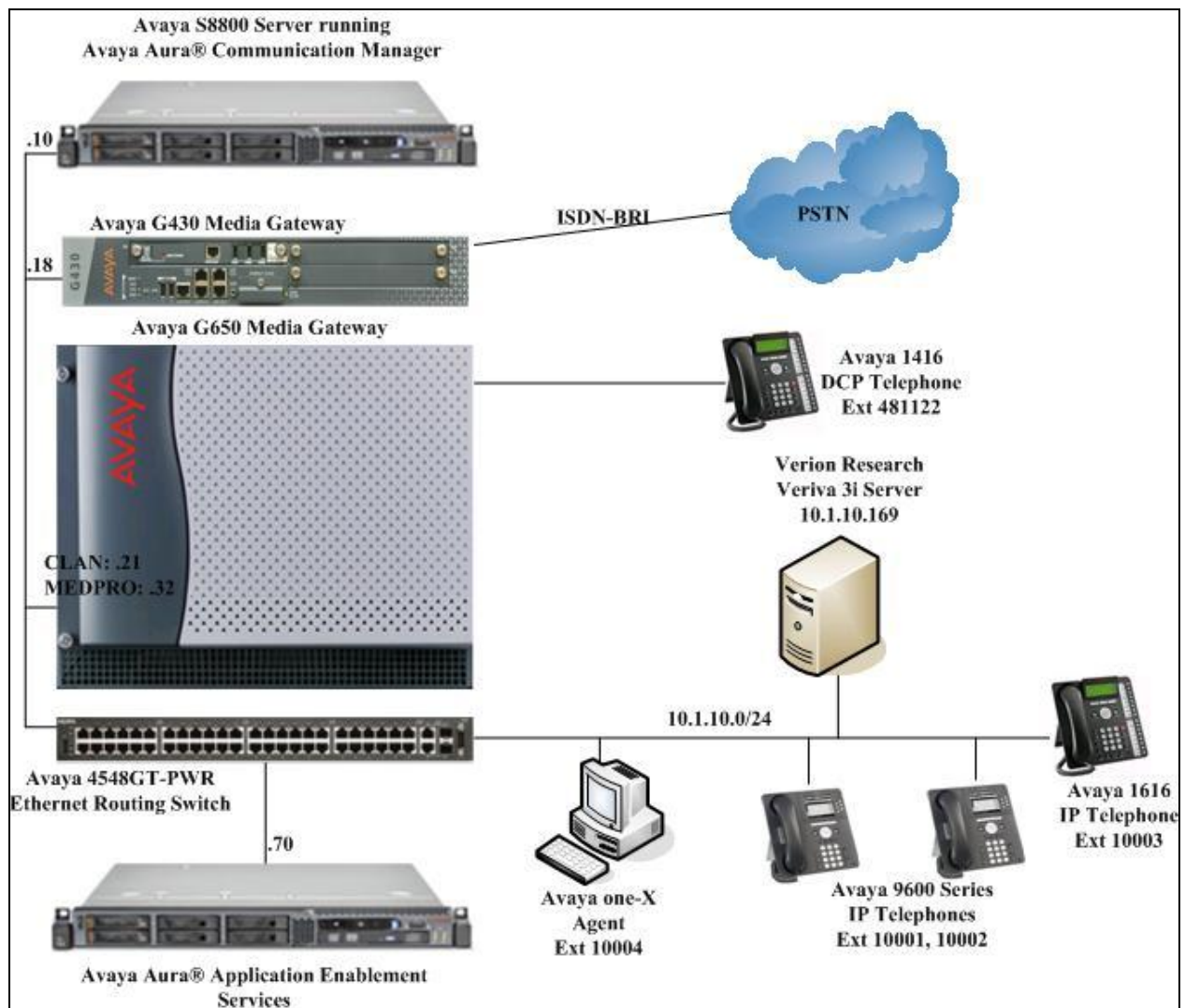
## 2.3. Support

For technical support on Veriva 3i, contact Verion Research at:

- Phone: +60-3-8996 7116
- Email: support@verionresearch.com

## 3. Reference Configuration

**Figure 1** illustrates the test configuration used to verify the Veriva 3i solution. Veriva 3i was installed on a server running Microsoft Windows 2008 R2. Calls were placed to the Vector Directory Numbers (VDNs) or directly to the agents' extensions, which were then recorded by Veriva 3i DMCC Recorder. Call related information was also captured by Veriva DMCC Recorder using the TSAPI interface.



**Figure 1: Test Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya S8800 Server	R6.0.1 SP 7
Avaya G650 Media Gateway <ul style="list-style-type: none"><li>TN2312BP IP Server Interface</li><li>TN799DP C-LAN Interface</li><li>TN2302AP IP Media Processor</li><li>TN2602AP IP Media Processor</li></ul>	HW07, FW054 HW01, FW040 HW20, FW121 HW02, FW059
Avaya Aura® Application Enablement Services	R6.1.1
Avaya 4548GT-PWR Ethernet Routing Switch	V5.4.0.008
Avaya IP Telephones <ul style="list-style-type: none"><li>9640</li><li>9612</li><li>1616</li></ul>	3.1 SP2 (H.323) 6.0 SP5 (H.323) 1.300B (H.323)
Avaya DCP Telephone <ul style="list-style-type: none"><li>1416</li></ul>	-
Veriva 3i DMCC Recorder running on Microsoft Windows Server 2008 R2 Standard	V1.0

## 5. Configure Avaya Aura® Communication Manager

This section provides the procedure for configuring Communication Manager. The procedure includes the following areas:

- Verify Communication Manager software options
- Configure CTI Link
- Configure AES Service
- Configure Service-Observing Feature Access Code
- Configure DMCC Recording Devices

The detailed administration of contact center devices such as Skilled Hunt Group, VDN, Vector, and Agents are assumed to be in place. These Application Notes will only cover the steps to administer the CTI Links and the Service-Observing feature access codes (FAC) used by AES and Veriva 3i DMCC Recorder.

## 5.1. Verify Communication Manager Software Options

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the **display system-parameters customer-options** command to verify that the **Computer Telephony Adjunct Links** field is set to **y** on Page 3, as shown below.

display system-parameters customer-options		Page	3 of	11
OPTIONAL FEATURES				
Abbreviated Dialing Enhanced List?	n	Audible Message Waiting?	n	
Access Security Gateway (ASG)?	n	Authorization Codes?	y	
Analog Trunk Incoming Call ID?	n	CAS Branch?	n	
A/D Grp/Sys List Dialing Start at 01?	n	CAS Main?	n	
Answer Supervision by Call Classifier?	n	Change COR by FAC?	n	
ARS?	y	<b>Computer Telephony Adjunct Links?</b>	<b>y</b>	
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	n	
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	n	
ASAI Link Core Capabilities?	n	DCS Call Coverage?	n	
ASAI Link Plus Capabilities?	n	DCS with Rerouting?	n	
Async. Transfer Mode (ATM) PNC?	n	Digital Loss Plan Modification?	n	
Async. Transfer Mode (ATM) Trunking?	n	DS1 MSP?	y	
ATM WAN Spare Processor?	n	DS1 Echo Cancellation?	y	
ATMS?	n			
Attendant Vectoring?	n			

## 5.2. Configure CTI Link

Enter the **add cti-link n** command, where **n** is a number between 1 and 64, inclusive. Enter a valid **Extension** under the provisioned dial plan in Communication Manager, set the **Type** field to **ADJ-IP**, and assign a descriptive **Name** to the CTI link. The CTI Link number corresponds to the **Switch CTI Link Number** in Section 6.4 Step 2.

add cti-link 3		Page	1 of	3
CTI LINK				
CTI Link:	3			
Extension:	10093			
Type:	ADJ-IP			
				COR: 1
Name:	TSAPI Service - AES6x			

### 5.3. Configure AES Service

Enter the **change ip-services** command. On Page 1, configure the **Service Type** field to **AESVCS** and the **Enabled** field to **y**. During the compliance test, the **Local Node** field is set to the processor Ethernet interface **procr** which is the IP address of the S8800 Server as shown in **Figure 1**. The default port **8765** was utilized for the **Local Port** field.

change ip-services				Page 1 of 4	
IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		
PMS		procr	0	FCSUni	5053
CDR1		procr	0	FCSUni	5052

On Page 3, enter the hostname of the Application Enablement Services server for the **AE Services Server** field. The server name may be obtained by logging in to the Application Enablement Services server using Secure Shell (SSH), and running the **uname -a** command. Enter an alpha-numeric password for the **Password** field and set the **Enabled** field to **y**. The same password will be configured on the Application Enablement Services server in **Section 6.3 Step 2**.

change ip-services				Page	4 of	4
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:	aes6x	xxxxxxxxxxxxxxxxxx	y			
2:						
3:						

## 5.4. Configure Service-Observing Feature Access Code

Enter the **change feature-access-codes** command. On Page 5, configure a feature access code (FAC) for the **Service Observing Listen Only Access Code** field valid under the provisioned dial plan. In this compliance testing, **\*68** was used.

change feature-access-codes		Page 5 of 9
FEATURE ACCESS CODE (FAC)		
Call Center Features		
AGENT WORK MODES		
After Call Work Access Code: *61		
Assist Access Code: *62		
Auto-In Access Code: *63		
Aux Work Access Code: *64		
Login Access Code: *65		
Logout Access Code: *66		
Manual-in Access Code: *67		
SERVICE OBSERVING		
Service Observing Listen Only Access Code: *68		
Service Observing Listen/Talk Access Code: *69		
Service Observing No Talk Access Code: *70		
Service Observing Next Call Listen Only Access Code:		

## 5.5. Configure DMCC Recording Devices

Enter the **add station n** command, where **n** is an available extension. Set the **Type** to a recommended value for DMCC, in this case, **4624**, and specify the **Name**. Specify the **Security Code**, which will be used to configure the DMCC Recording Devices in **Section 7**. Set **IP SoftPhone** to **y**. Repeat this section to create additional DMCC Recording Devices. For this testing, extensions 19901 to 19904 were created.

add station 19901		Page 1 of 6
STATION		
Extension: 19901	Lock Messages? n	BCC: 0
Type: 4624	Security Code: 111222	TN: 1
Port: S00006	Coverage Path 1:	COR: 1
Name: DMCC #1	Coverage Path 2:	COS: 1
Hunt-to Station:		
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 19902	
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		

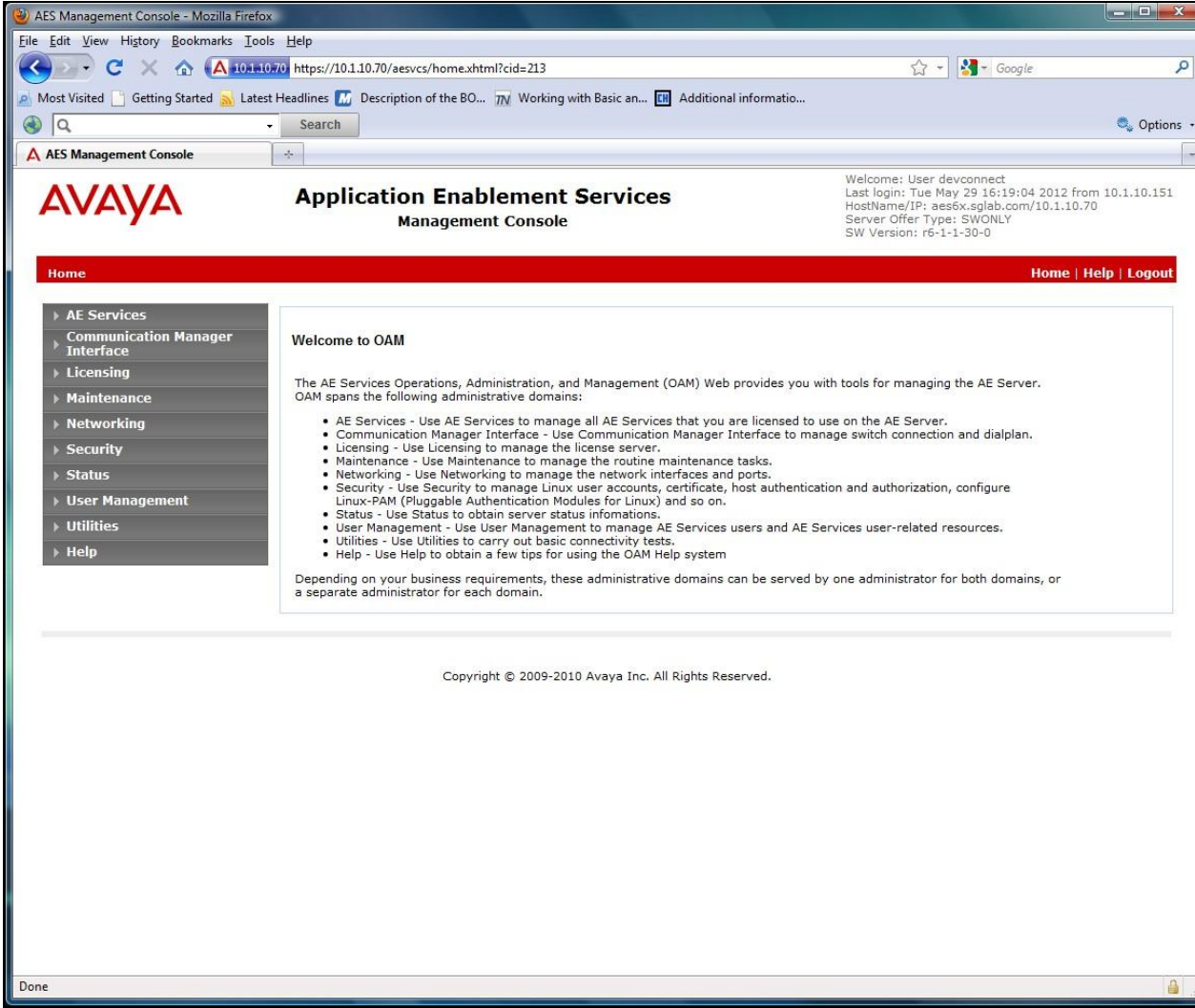
## 6. Configure Avaya Aura® Application Enablement Services

This section provides the procedure for configuring Application Enablement Services (AES).

The procedure falls into the following areas:

- Verify Application Enablement Services License
- Administer CTI User
- Administer Switch Connection
- Administer TSAPI link
- Administer CTI user permission
- Administer DMCC Ports

## 6.1. Verify Application Enablement Services License

Step	Description
1.	<p>Launch a web browser and enter <b>https://&lt;IP address of AES server&gt;</b> to access the Application Enablement Services Management Console. Log in using an administrative login and password (not shown), and the <b>Welcome To OAM</b> screen will be displayed.</p>  <p>The screenshot displays the Avaya Application Enablement Services Management Console (OAM) web interface. The browser window shows the URL <code>https://10.1.10.70/aesvcs/home.xhtml?cid=213</code>. The page features the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message. A sidebar on the left lists navigation options: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area contains a "Welcome to OAM" message and a list of administrative domains and their functions.</p> <p>Welcome: User devconnect Last login: Tue May 29 16:19:04 2012 from 10.1.10.151 HostName/IP: aes6x.sglab.com/10.1.10.70 Server Offer Type: SWONLY SW Version: r6-1-1-30-0</p> <p><b>Home</b> <a href="#">Home</a> <a href="#">Help</a> <a href="#">Logout</a></p> <p><b>AE Services</b></p> <ul style="list-style-type: none"> <li>Communication Manager Interface</li> <li>Licensing</li> <li>Maintenance</li> <li>Networking</li> <li>Security</li> <li>Status</li> <li>User Management</li> <li>Utilities</li> <li>Help</li> </ul> <p><b>Welcome to OAM</b></p> <p>The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:</p> <ul style="list-style-type: none"> <li>• AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.</li> <li>• Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.</li> <li>• Licensing - Use Licensing to manage the license server.</li> <li>• Maintenance - Use Maintenance to manage the routine maintenance tasks.</li> <li>• Networking - Use Networking to manage the network interfaces and ports.</li> <li>• Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.</li> <li>• Status - Use Status to obtain server status informations.</li> <li>• User Management - Use User Management to manage AE Services users and AE Services user-related resources.</li> <li>• Utilities - Use Utilities to carry out basic connectivity tests.</li> <li>• Help - Use Help to obtain a few tips for using the OAM Help system</li> </ul> <p>Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain.</p> <p>Copyright © 2009-2010 Avaya Inc. All Rights Reserved.</p>

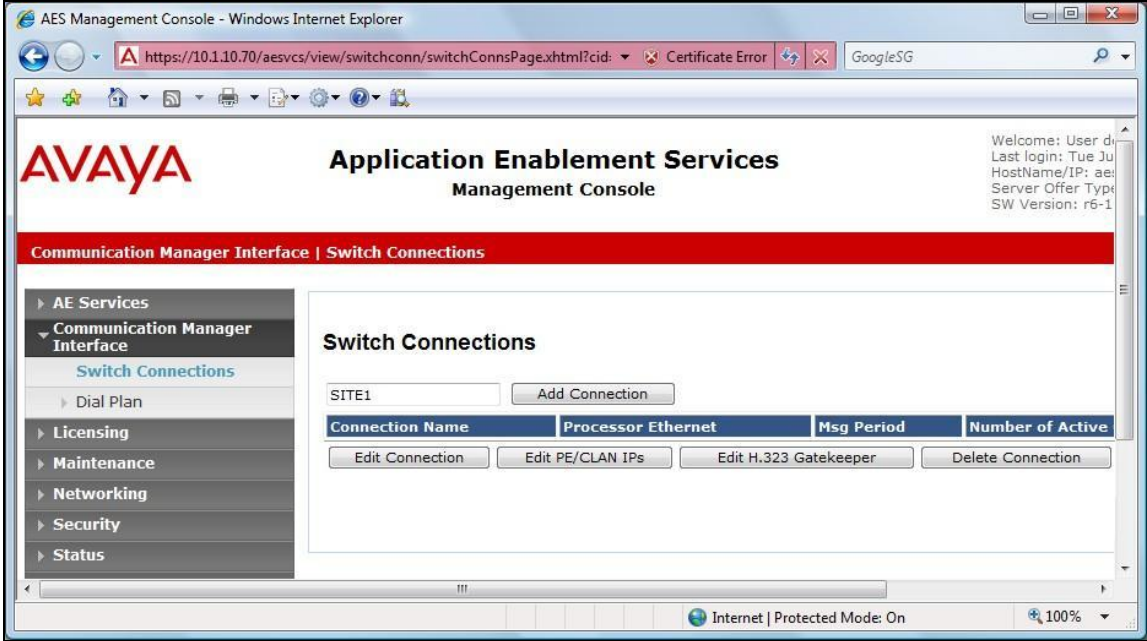
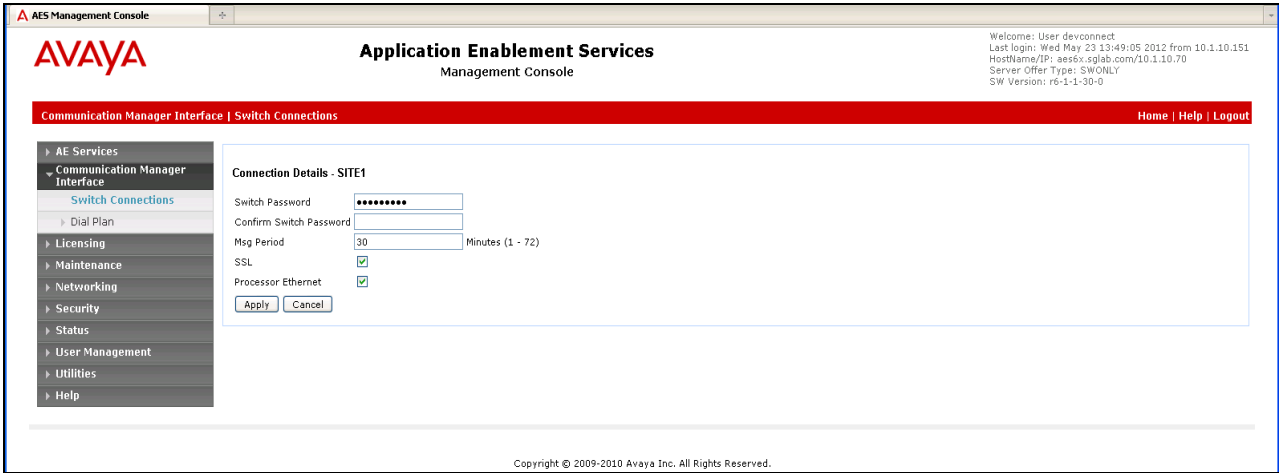
Step	Description																																			
2.	<p>Select <b>AE Services</b> from the left menu. From the AE Services page, verify that the Application Enablement Services has proper license for the feature illustrated in these Application Notes by ensuring the <b>License Mode</b> for <b>DMCC Service</b> and <b>TSAPI Service</b> are <b>NORMAL MODE</b>, as shown below. If the DMCC Service and TSAPI Service are not licensed, then contact the Avaya sales team or business partner for the proper license to install onto the WebLM Server.</p> <div><div><div>AES Management Console - Mozilla Firefox</div><div><div>File Edit View History Bookmarks Tools Help</div><div>10.1.10.70 https://10.1.10.70/aesvcs/view/welcome/ctiWelcomeWarningPage.xhtml?cid=213</div><div>Most Visited Getting Started Latest Headlines Description of the BO... Working with Basic an... Additional information...</div><div>AES Management Console</div></div></div><div><div><div>AVAYA</div><div>Application Enablement Services Management Console</div><div>Welcome: User devconnect Last login: Tue May 29 16:19:04 2012 from 10.1.10.151 HostName/IP: aes6x.sglab.com/10.1.10.70 Server Offer Type: SWONLY SW Version: r6-1-1-30-0</div></div><div><div>AE Services</div><div>Home   Help   Logout</div></div><div><div><div>▼ AE Services</div><div>▶ CVLAN</div><div>▶ DLG</div><div>▶ DMCC</div><div>▶ SMS</div><div>▶ TSAPI</div><div>▶ TWS</div><div>▶ Communication Manager Interface</div><div>▶ Licensing</div><div>▶ Maintenance</div><div>▶ Networking</div><div>▶ Security</div><div>▶ Status</div><div>▶ User Management</div><div>▶ Utilities</div><div>▶ Help</div></div><div><div>AE Services</div><div>IMPORTANT: AE Services must be restarted for administrative changes to fully take effect. Changes to the Security Database do not require a restart.</div><div><table><thead><tr><th>Service</th><th>Status</th><th>State</th><th>License Mode</th><th>Cause*</th></tr></thead><tbody><tr><td>ASAI Link Manager</td><td>N/A</td><td>Running</td><td>N/A</td><td>N/A</td></tr><tr><td>CVLAN Service</td><td>ONLINE</td><td>Running</td><td>NORMAL MODE</td><td>N/A</td></tr><tr><td>DLG Service</td><td>OFFLINE</td><td>Running</td><td>N/A</td><td>N/A</td></tr><tr><td>DMCC Service</td><td>ONLINE</td><td>Running</td><td>NORMAL MODE</td><td>N/A</td></tr><tr><td>TSAPI Service</td><td>ONLINE</td><td>Running</td><td>NORMAL MODE</td><td>N/A</td></tr><tr><td>Transport Layer Service</td><td>N/A</td><td>Running</td><td>N/A</td><td>N/A</td></tr></tbody></table></div><div><div>For status on actual services, please use <a href="#">Status and Control</a></div><div>* -- For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.</div><div><div>License Information</div><div>You are licensed to run Application Enablement (CTI) release 6.x</div></div></div></div></div></div></div>	Service	Status	State	License Mode	Cause*	ASAI Link Manager	N/A	Running	N/A	N/A	CVLAN Service	ONLINE	Running	NORMAL MODE	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
Service	Status	State	License Mode	Cause*																																
ASAI Link Manager	N/A	Running	N/A	N/A																																
CVLAN Service	ONLINE	Running	NORMAL MODE	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																																

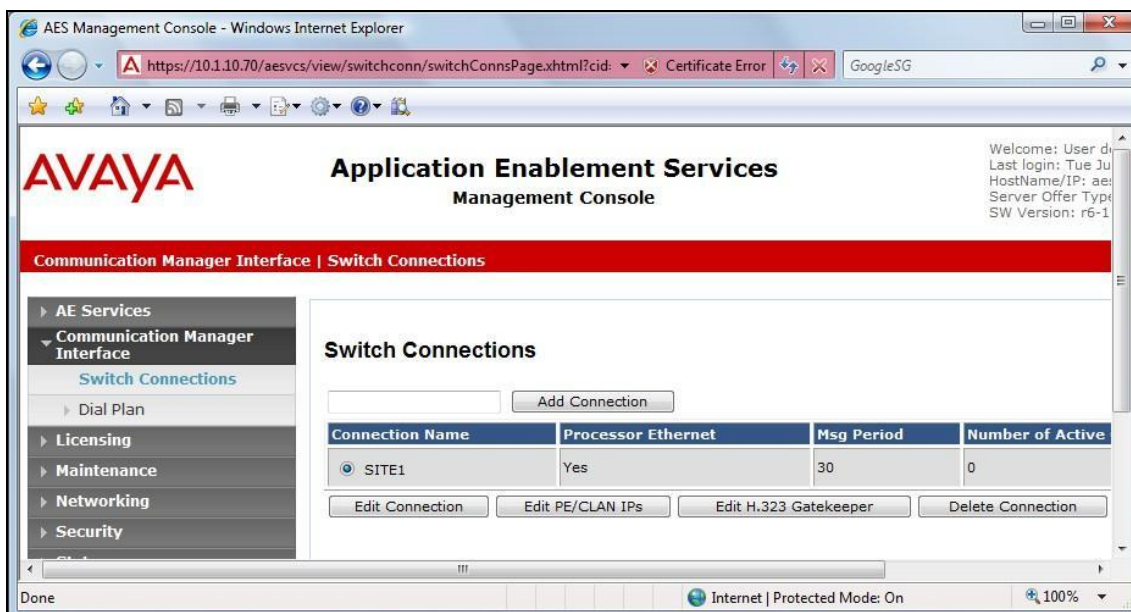
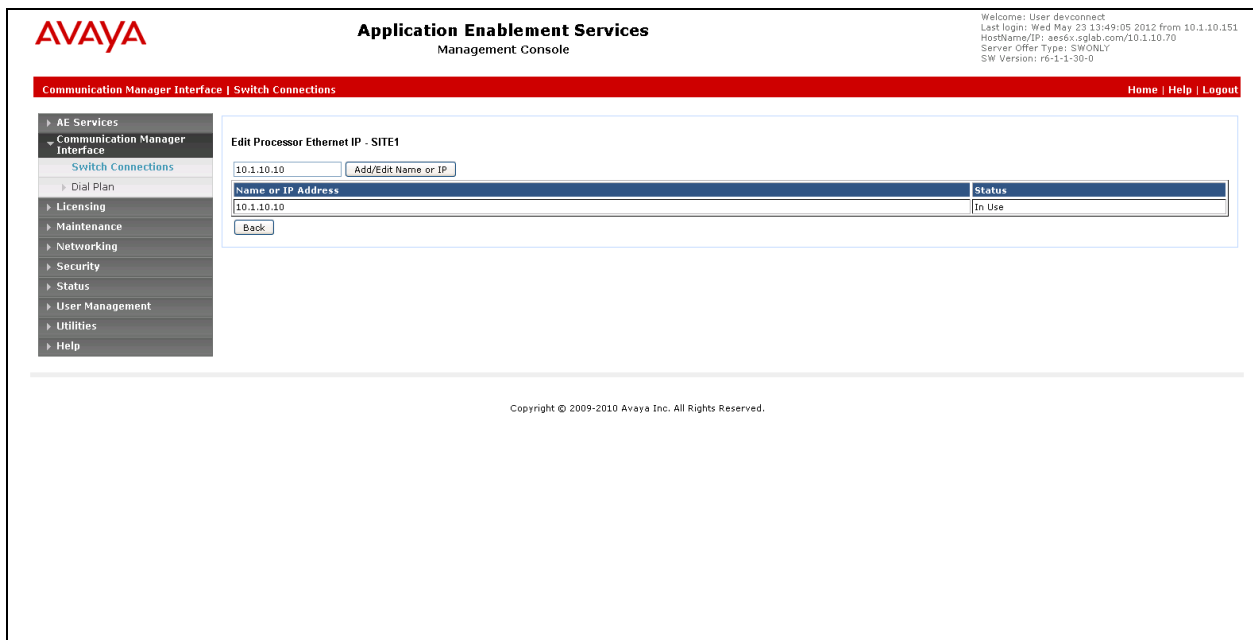
## 6.2. Administer CTI User

Click **User Management**, then **User Admin** → **Add User** in the left pane. Specify a value for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. Set **CT User** to **Yes**. Use the values for **User Id** and **User Password** to configure Veriva 3i DMCC Recorder in **Section 7** to access the DMCC Service and TSAPI Service on the Application Enablement Services. Scroll down to the bottom of the page and click **Apply** (not shown).

The screenshot displays the Avaya AES Management Console in a Mozilla Firefox browser window. The address bar shows the URL: `https://10.1.10.70/aesvcs/view/usermgmt/editUserPage.xhtml?cid=225`. The page title is "AES Management Console - Mozilla Firefox". The console interface includes a top navigation bar with the Avaya logo, "Application Enablement Services Management Console", and a welcome message for user "devconnect". Below this is a red navigation bar with links: "User Management | User Admin | List All Users" and "Home | Help | Logout". The left sidebar contains a tree view with categories: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management" (expanded), "Service Admin", "User Admin" (selected), "Utilities", and "Help". Under "User Admin", the options are "Add User", "Change User Password", "List All Users" (highlighted), "Modify Default Users", and "Search Users". The main content area is titled "Edit User" and contains a form with the following fields: "User Id" (text box with "veriva"), "Common Name" (text box with "Veriva"), "Surname" (text box with "Verion Research"), "User Password" (text box), "Confirm Password" (text box), "Admin Note" (text box), "Avaya Role" (dropdown menu with "None" selected), "Business Category" (text box), "Car License" (text box), "CM Home" (text box), "Csm Home" (text box), "CT User" (dropdown menu with "Yes" selected), "Department Number" (text box), "Display Name" (text box), "Employee Number" (text box), and "Employee Type" (text box). The bottom status bar shows "Done".

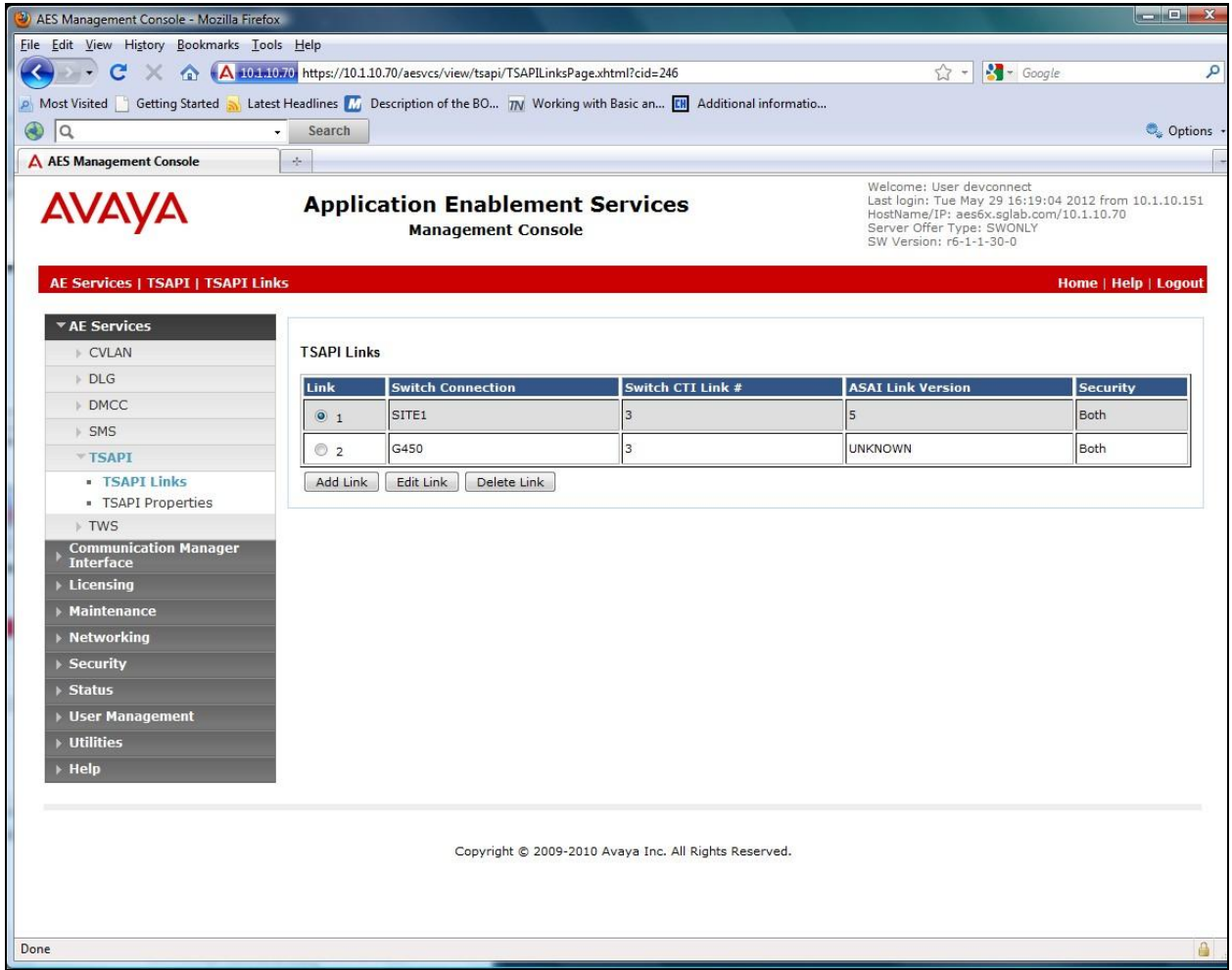
## 6.3. Administer Switch Connection

Step	Description
1.	<p>From the left menu, select <b>Communication Manager Interface</b> → <b>Switch Connections</b>. Enter a descriptive name for the switch connection and click <b>Add Connection</b>. In this configuration, <b>SITE1</b> is used.</p> 
2.	<p>The Connection Details – SITE1 screen is displayed. For the <b>Switch Password</b> and <b>Confirm Switch Password</b> fields, enter the password that was administered in Communication Manager using the IP Services form in <b>Section 5.3</b>. Both the <b>SSL</b> and <b>Processor Ethernet</b> fields need to be checked. Click on <b>Apply</b>.</p> 

Step	Description
3.	<p>The Switch Connections screen is displayed again. Select the new switch connection name <b>SITE1</b> and click <b>Edit PE/CLAN IPs</b>.</p> <div></div>
4.	<p>In the Edit Processor Ethernet IP – SITE1 screen, enter the host name or the IP address of the Communication Manager Processor Ethernet. In this case, <b>10.1.10.10</b> is used, which corresponds to the IP address of the S8800 Server as shown in <b>Figure 1</b>. Click <b>Add/Edit Name or IP</b>.</p> <div></div>

## 6.4. Administer TSAPI Link

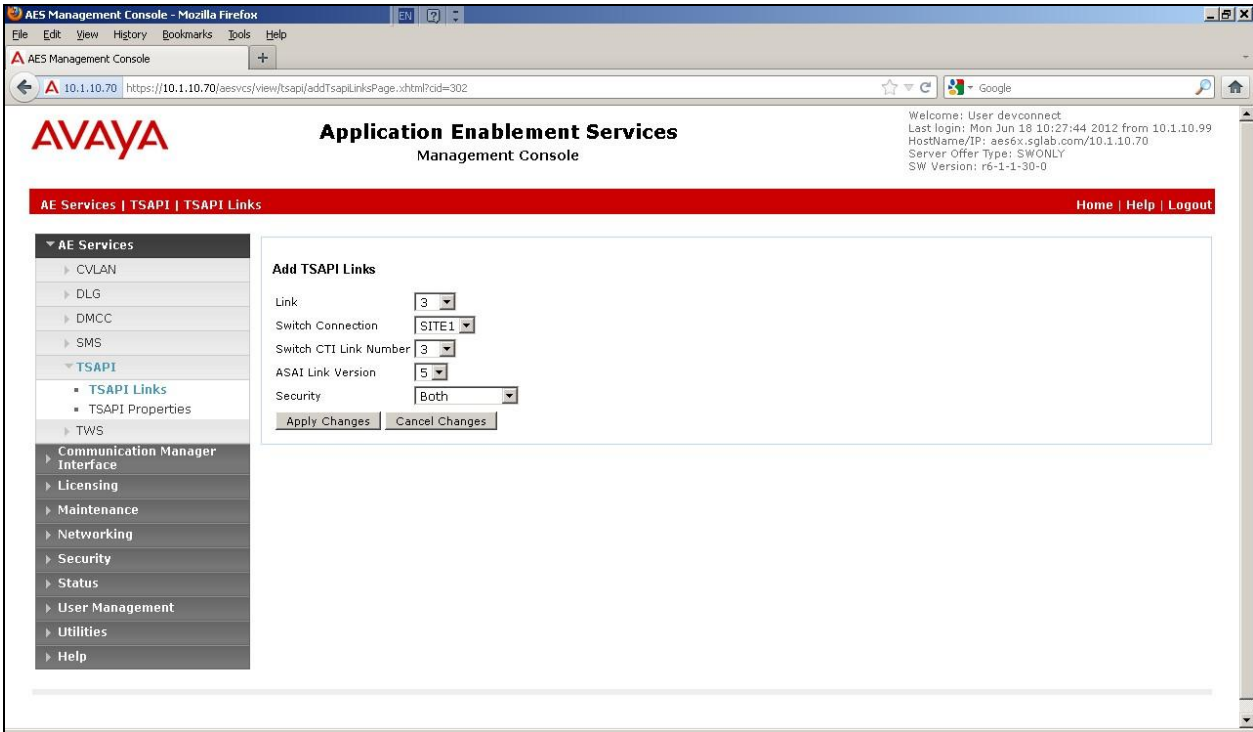
Step	Description
1.	To administer a TSAPI Link, select <b>AE Services</b> → <b>TSAPI</b> → <b>TSAPI Links</b> from the left menu. Click <b>Add Link</b> .

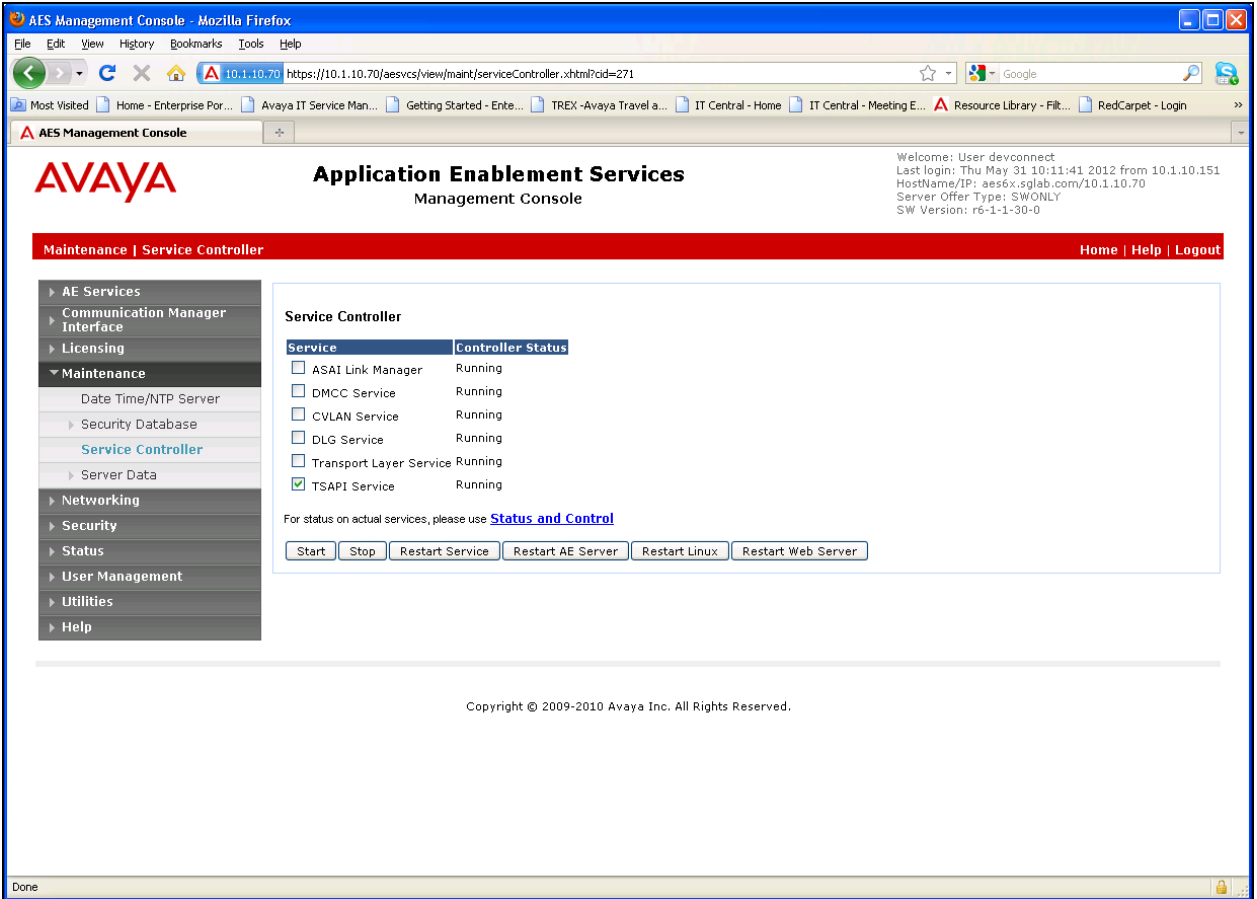


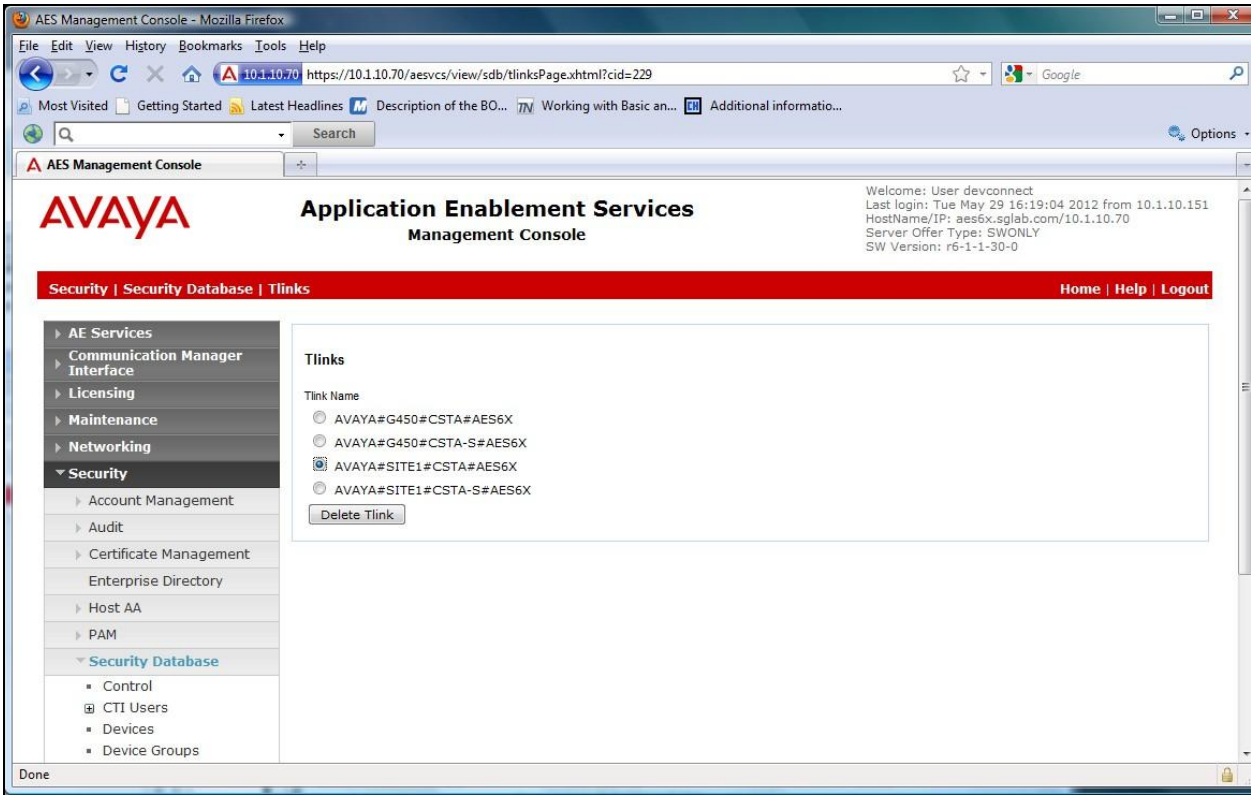
The screenshot shows the Avaya AES Management Console interface. The left sidebar contains a navigation menu with the following items: AE Services, CVLAN, DLG, DMCC, SMS, TSAPI (expanded), TSAPI Links (selected), TSAPI Properties, TWS, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'TSAPI Links' and contains a table with the following data:

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	SITE1	3	5	Both
2	G450	3	UNKNOWN	Both

Below the table are three buttons: 'Add Link', 'Edit Link', and 'Delete Link'. The bottom of the page displays the copyright notice: 'Copyright © 2009-2010 Avaya Inc. All Rights Reserved.'

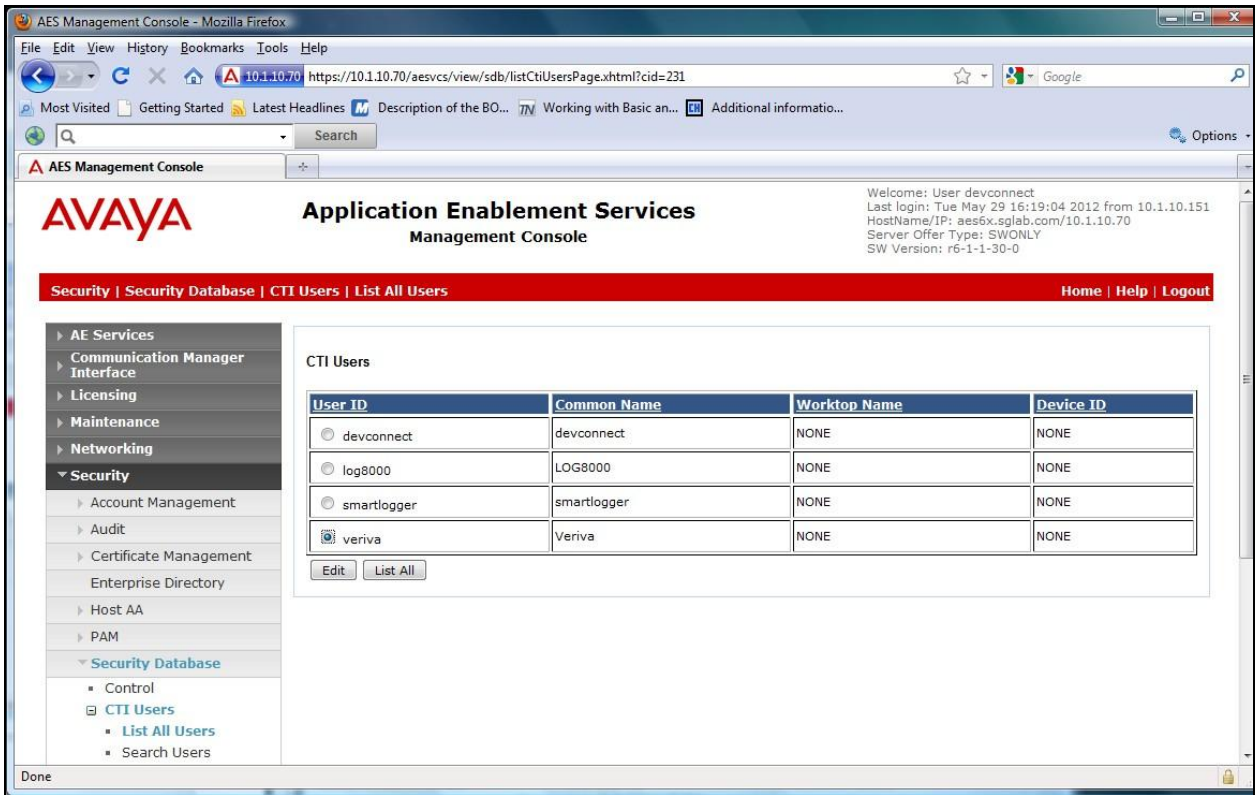
Step	Description
2.	<p>In the Add TSAPI Links screen, select the following values:</p> <ul style="list-style-type: none"> <li>• <b>Link:</b> Select an available Link number from 1 to 16.</li> <li>• <b>Switch Connection:</b> Select the switch connection in <b>Section 6.3 Step 1</b>.</li> <li>• <b>Switch CTI Link Number:</b> Corresponding CTI link number in <b>Section 5.2</b>.</li> <li>• <b>ASAI Link Version:</b> Set to <b>5</b>.</li> <li>• <b>Security:</b> Set to <b>Both</b> so that both encrypted and unencrypted TSAPI Links can be used.</li> </ul> <p>Note that the actual values may vary. Click <b>Apply Changes</b>.</p>  <p>In the next page, click <b>Apply</b> to confirm the changes (not shown).</p>

Step	Description
3.	<p>To restart the TSAPI Service, select <b>Maintenance → Service Controller</b> from the left menu. Check the <b>TSAPI Service</b> checkbox and click <b>Restart Service</b>. In the next page, click <b>Restart</b> to confirm the restart (not shown).</p>  <p>The screenshot shows the Avaya AES Management Console interface. The browser address bar indicates the URL is https://10.1.10.70/aesvcs/view/maint/serviceController.xhtml?cid=271. The page title is 'Application Enablement Services Management Console'. The left sidebar contains a menu with categories like AE Services, Communication Manager Interface, Licensing, Maintenance, Security Database, Service Controller, Server Data, Networking, Security, Status, User Management, Utilities, and Help. The 'Maintenance' category is expanded, and 'Service Controller' is selected. The main content area displays a table titled 'Service Controller' with two columns: 'Service' and 'Controller Status'. The table lists several services: ASAI Link Manager, DMCC Service, CVLAN Service, DLG Service, Transport Layer Service, and TSAPI Service. The 'TSAPI Service' row has its checkbox checked, and its status is 'Running'. Below the table, there is a note: 'For status on actual services, please use <a href="#">Status and Control</a>'. At the bottom of the main area, there are buttons: 'Start', 'Stop', 'Restart Service', 'Restart AE Server', 'Restart Linux', and 'Restart Web Server'. The footer of the page states 'Copyright © 2009-2010 Avaya Inc. All Rights Reserved.' and 'Done' is visible in the bottom left corner of the browser window.</p>

Step	Description
4.	<p>Navigate to the Tlinks screen by selecting <b>Security → Security Database → Tlinks</b> from the left menu. In this configuration, the unencrypted Tlink Name, <b>AVAYA#SITE1#CSTA#AES6X</b>, is used.</p>  <p>The screenshot displays the AVAYA Application Enablement Services Management Console in a Mozilla Firefox browser. The address bar shows the URL: https://10.1.10.70/aesvcs/view/sdb/tlinksPage.xhtml?cid=229. The page title is 'AVAYA Application Enablement Services Management Console'. The left sidebar contains a navigation menu with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security (expanded), and Security Database (selected). Under Security, the options are Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, and Security Database. Under Security Database, the options are Control, CTI Users, Devices, and Device Groups. The main content area is titled 'Tlinks' and shows a list of Tlink Names: AVAYA#G450#CSTA#AES6X, AVAYA#G450#CSTA-S#AES6X, AVAYA#SITE1#CSTA#AES6X (selected), and AVAYA#SITE1#CSTA-S#AES6X. A 'Delete Tlink' button is visible below the list. The top right corner displays user information: Welcome: User devconnect, Last login: Tue May 29 16:19:04 2012 from 10.1.10.151, HostName/IP: aes6x.sglab.com/10.1.10.70, Server Offer Type: SWONLY, and SW Version: r6-1-1-30-0. The bottom status bar shows 'Done'.</p>

## 6.5. Administer CTI User Permission

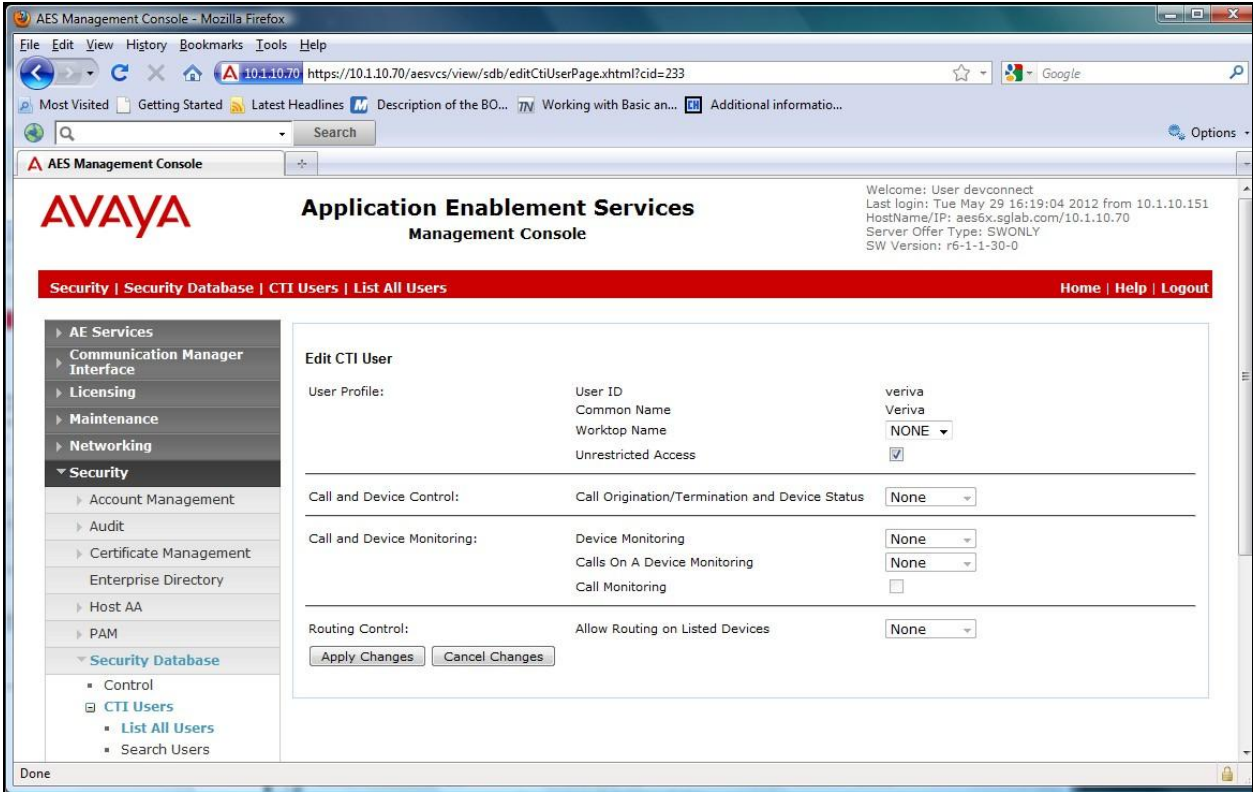
Step	Description
1.	Select <b>Security</b> → <b>Security Database</b> → <b>CTI Users</b> → <b>List All Users</b> from the left menu. Select the <b>User ID</b> created in <b>Section 6.2</b> and click <b>Edit</b> .



The screenshot shows the Avaya AES Management Console interface. The left sidebar contains a navigation menu with categories like AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, and Security Database. Under Security Database, the 'CTI Users' option is selected, and 'List All Users' is highlighted. The main content area displays a table titled 'CTI Users' with the following data:

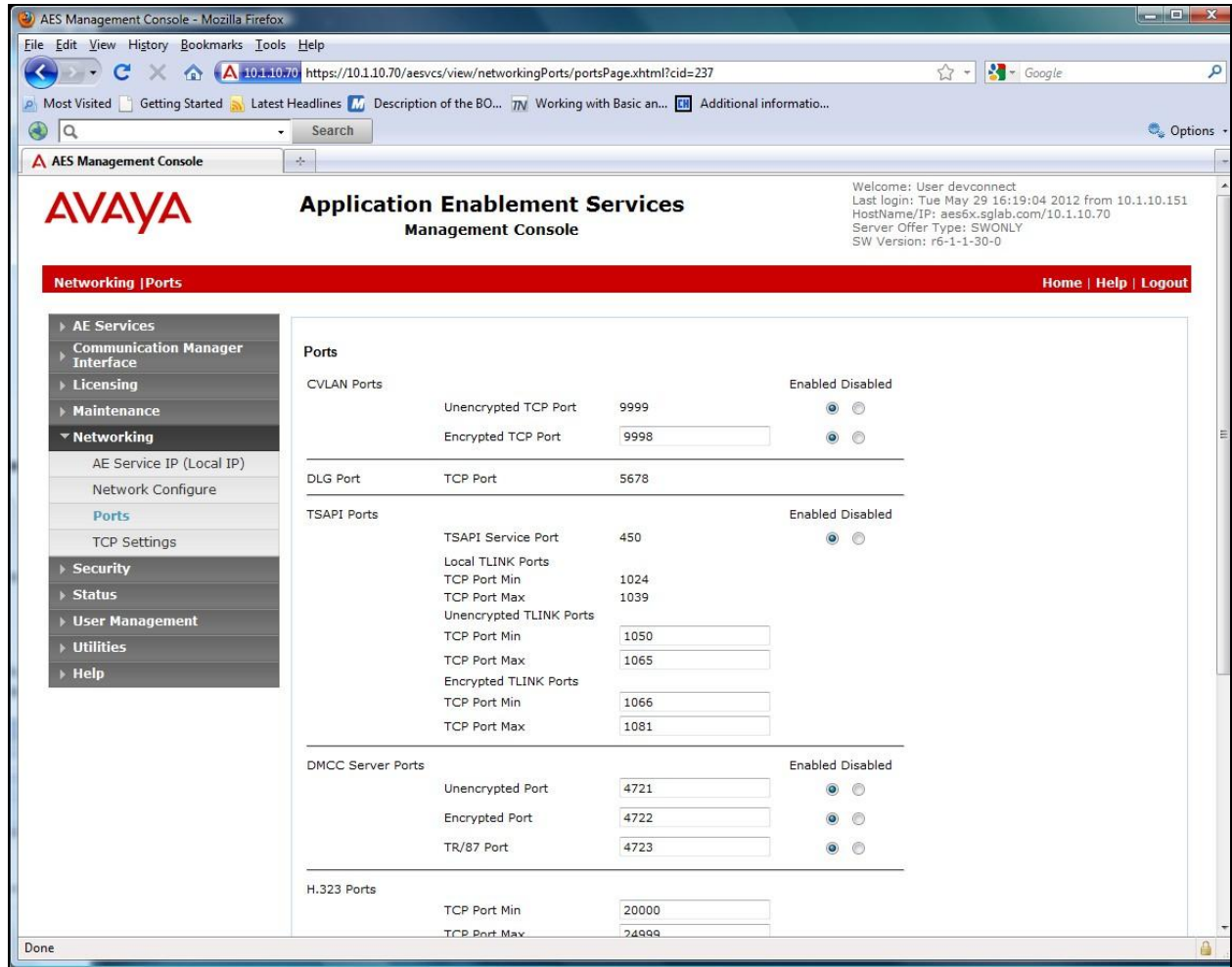
User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> devconnect	devconnect	NONE	NONE
<input type="radio"/> log8000	LOG8000	NONE	NONE
<input type="radio"/> smartlogger	smartlogger	NONE	NONE
<input checked="" type="radio"/> veriva	Veriva	NONE	NONE

Below the table are buttons for 'Edit' and 'List All'.

Step	Description
2.	<p>Assign access rights and call/device privileges according to customer requirements. For simplicity in configuration, <b>Unrestricted Access</b> was enabled during compliance testing. If <b>Unrestricted Access</b> is not desired, then consult Reference [2] for guidance on configuring the call/device privileges as well as devices and device groups. Click <b>Apply Changes</b>.</p>  <p>In the next page, click <b>Apply</b> to confirm the changes (not shown).</p>

## 6.6. Administer DMCC Ports

Step	Description
1.	<p>Select <b>Networking</b> → <b>Ports</b> from the left menu. For the DMCC Server Ports, verify that <b>Unencrypted Port</b> is <b>Enabled</b> and note the port value, as this will be needed to configure Veriva 3i DMCC Recorder in <b>Section 7</b>. During the compliance test, the default port values were utilized.</p>



The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a menu with options: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking (selected), AE Service IP (Local IP), Network Configure, Ports (selected), TCP Settings, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Ports' and shows the following configuration:

Category	Port Type	Port Value	Enabled/Disabled
CVLAN Ports	Unencrypted TCP Port	9999	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
	Encrypted TCP Port	9998	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DLG Port	TCP Port	5678	
TSAPI Ports	TSAPI Service Port	450	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
	Local TLINK Ports		
	TCP Port Min	1024	
	TCP Port Max	1039	
	Unencrypted TLINK Ports		
	TCP Port Min	1050	
DMCC Server Ports	Unencrypted Port	4721	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
	Encrypted Port	4722	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
	TR/87 Port	4723	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
	H.323 Ports		
H.323 Ports	TCP Port Min	20000	
	TCP Port Max	24999	

## 7. Configure Veriva 3i DMCC Recorder

This section provides the procedure for configuring Veriva 3i DMCC Recorder. It includes the following:

- Setup IPX configuration
- Recording configurations
- Starting DMCC service

### 7.1. Setup IPX configuration

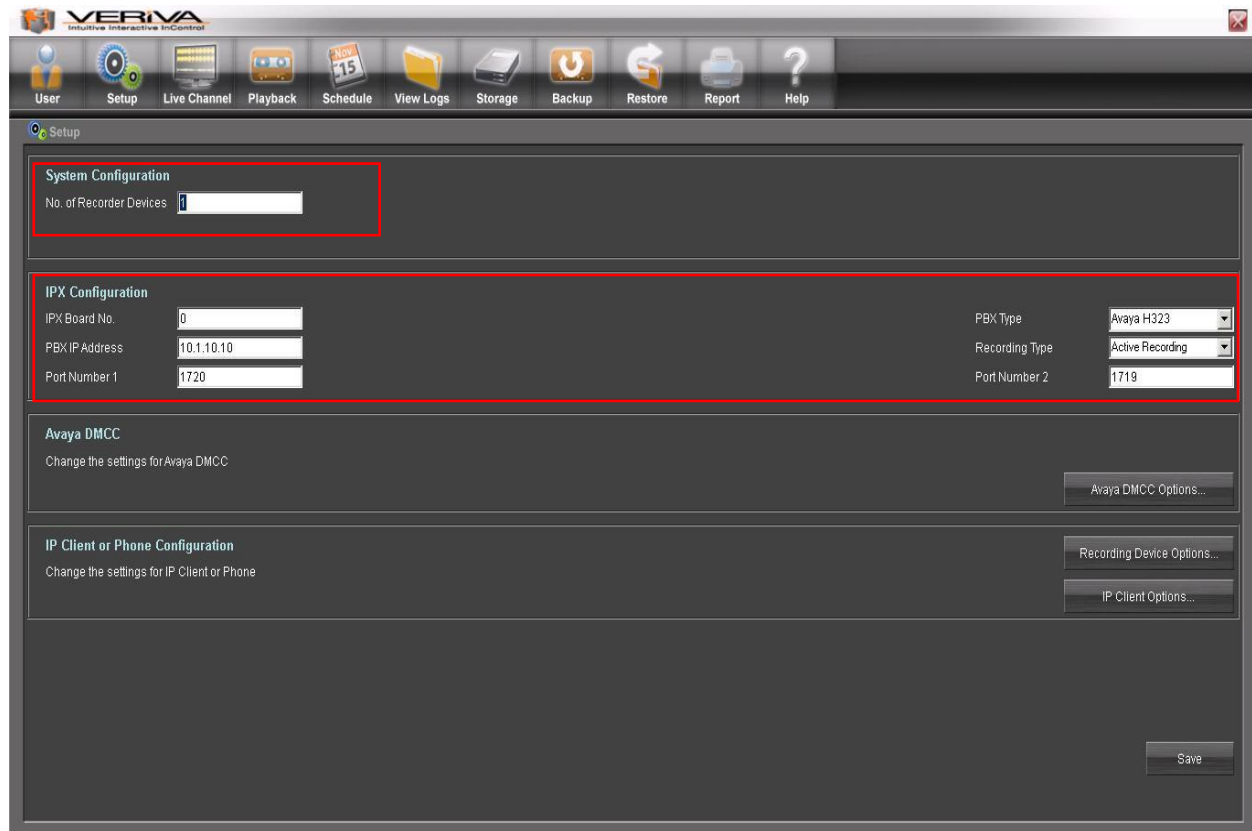
Run the program **Veriva3i.exe** from the folder “C:\Program Files\Verion\Veriva3iSetup\” and obtain the login screen below. Enter the appropriate login and password.



The following main screen will be displayed.



Select **Setup** → **IPX**.



For **System Configuration**, the **No of Recording Devices** in the Veriva 3i system is set at the default value of **1**. Click **Save** after setting the configurations below.

For **IPX Configuration**, the values are as defined below:

1. **IPX Board No.** – **0** (default value)
2. **PBX IP Address** – **10.1.10.10** (IP address of the PBX)

3. **PBX Type** – **Avaya H323** is selected

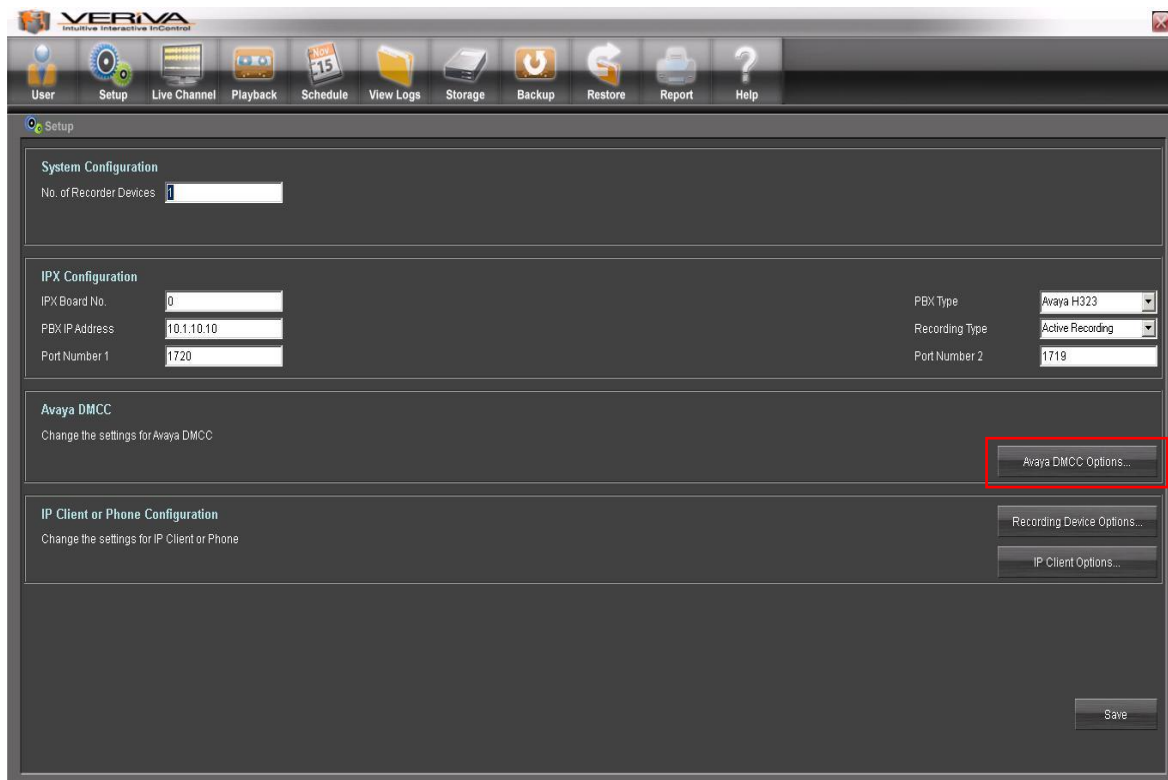


4. **Recording Type** – **Active Recording**.



5. **Port Number 1** – **1720** (Primary Mirror Port. Not used in our case as call information is obtained from TSAPI)
6. **Port Number 2** – **1719** (Secondary Mirror Port. Not used in our case as call information is obtained from TSAPI)

For **Avaya DMCC options**, select this option for configuring the DMCC settings.



For **Avaya DMCC section**, the values are as defined below which are mostly self explanatory:

1. AES IP Address: **10.1.10.70**
2. AES Port Number: **4721 (unencrypted port)**
3. AES Login and Password (as configured in **Section 6.2**)
4. RTP/RTCP IP addr: **10.1.10.169** (Veriva 3i server address)
5. RTP Port Num: **4725**
6. RTCP Port Num: **4726**
7. Session Duration: **180**
8. Session Cleanp Delay: **60**
9. Switch Name: **SITE1** (as configured in **Section 6.3**)
10. Protocol: **6.1** (AES Release)

**VERIVA**  
Intuitive Interactive InControl

### Avaya DMCC

AES IP Address	<input type="text" value="10.1.10.70"/>	RTP / RTCP IP Addr.	<input type="text" value="10.1.10.169"/>	Switch Name	<input type="text" value="SITE1"/>
AES Port Num.	<input type="text" value="4721"/>	RTP Port Num.	<input type="text" value="4725"/>	Switch IP Add.	<input type="text"/>
AES Login	<input type="text" value="veriva"/>	RTCP Port Num.	<input type="text" value="4726"/>	Protocol	<input type="text" value="6.1"/>
AES Password	<input type="password" value="....."/>	Session Duration	<input type="text" value="180"/>		
		Session Cleanup Delay	<input type="text" value="60"/>		

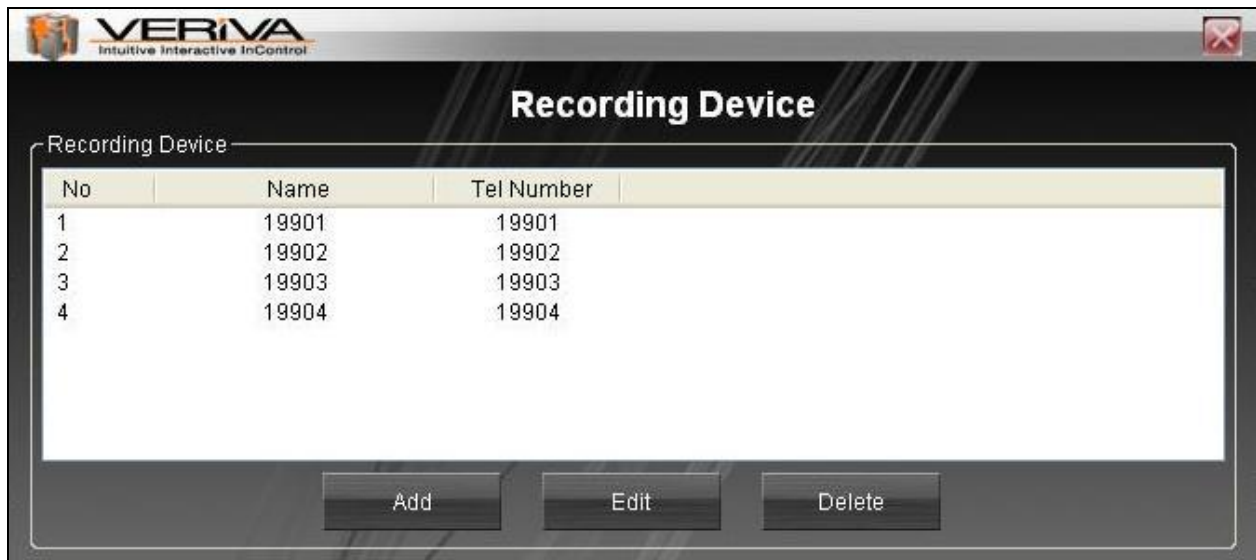
For **IP Client or Phone Configuration** → **Recording Device Options**, configure recording devices involve for active recording.

The screenshot displays the Veriva DMCC configuration window. The top menu bar includes icons for User, Setup, Live Channel, Playback, Schedule, View Logs, Storage, Backup, Restore, Report, and Help. The main configuration area is divided into several sections:

- System Configuration:** Contains a field for 'No. of Recorder Devices' with a value of 1.
- IPX Configuration:** Includes fields for 'IPX Board No.' (0), 'PBX IP Address' (10.1.10.10), 'Port Number 1' (1720), 'PBX Type' (Avaya H323), 'Recording Type' (Active Recording), and 'Port Number 2' (1719).
- Avaya DMCC:** Contains the text 'Change the settings for Avaya DMCC' and a button labeled 'Avaya DMCC Options...'.
- IP Client or Phone Configuration:** Contains the text 'Change the settings for IP Client or Phone' and two buttons: 'Recording Device Options...' (highlighted with a red rectangle) and 'IP Client Options...'.

A 'Save' button is located at the bottom right of the configuration area.

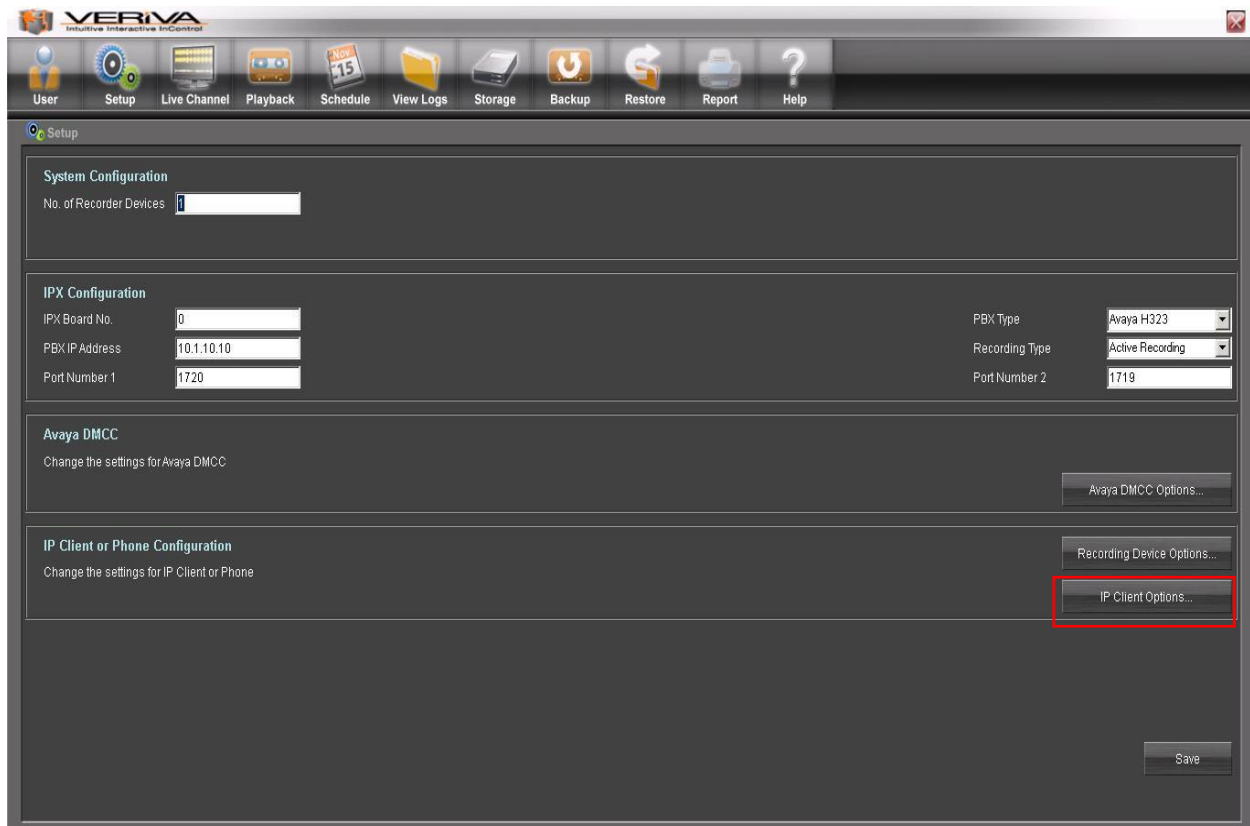
Each recording device setting will include a **Name** and **Tel Number** field (not shown) for the administrator to set for referencing. Below is list of recording devices added.



No	Name	Tel Number
1	19901	19901
2	19902	19902
3	19903	19903
4	19904	19904

Buttons: Add, Edit, Delete

For **IP Client & Phone Configuration → IP Client Options**, the administrator will need to provide each IP Phone's IP address and its allocated user details.



**System Configuration**  
No. of Recorder Devices: 1

**IPX Configuration**  
 IPX Board No.: 0  
 PBX IP Address: 10.1.10.10  
 Port Number 1: 1720  
 PBX Type: Avaya H323  
 Recording Type: Active Recording  
 Port Number 2: 1719

**Avaya DMCC**  
Change the settings for Avaya DMCC  
Avaya DMCC Options...

**IP Client or Phone Configuration**  
Change the settings for IP Client or Phone  
 Recording Device Options...  
 IP Client Options... (highlighted with a red box)  
 Save

The IP Type is set to **Static IP** for our setup. Each phone settings will include a **Name** and **Tel Number** field for the administrator to set for referencing. With each IP phone setup, the administrator can select the type of recording trigger/recording method, either by **Always Record** or **No Record**. In our setup, extensions **10001-10004** are set for **Always Record** whereas the utility digital phone at extension **481122** is set at **No Record**. Below is the list of Client Options settings used in the compliance test.

**IP Client**

IP Type

☒ Static IP ☐ Dynamic IP

☐ Record All Calls Conversation Without Filtering

☐ Record Call Conversation Using IP Client List

IP Client

No	IP Address	Name	Tel Number	Recording Method	Pin Code
1	10.1.10.153	10001	10001	Always Record	*#
2	10.1.10.161	10002	10002	Always Record	*#
3	10.1.10.155	10003	10003	Always Record	*#
4	10.1.10.152	10004	10004	Always Record	*#
5	10.1.10.50	481122	481122	No Record	*#

Add Edit Delete

Save

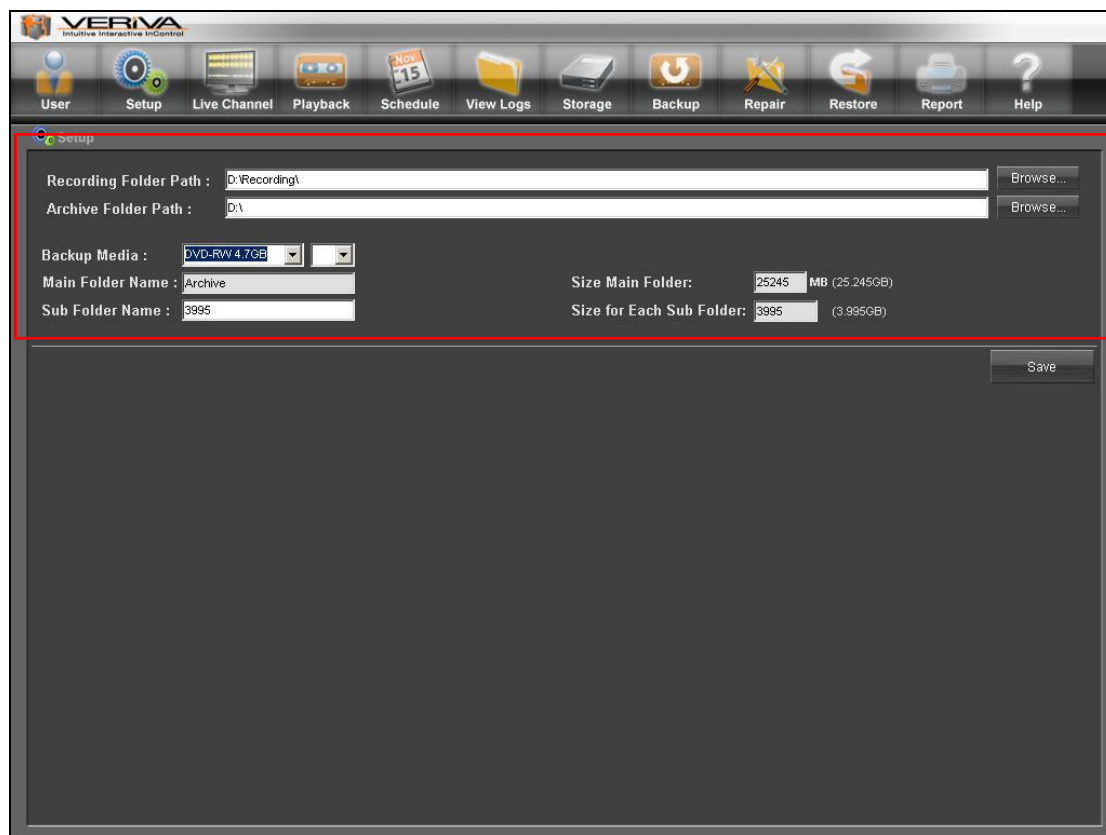
## 7.2. Recording Configurations

This section provides the details for the following for recording configurations.

1. Recording setup
2. User management
3. Playback options.

### 7.2.1. Recording Setup

Select **Setup** → **Recording** from the main screen. Users can select the preferred hard disk path and primary archive media path. Upon completing your selection, please click on the **Save** button to confirm your preference.



As default, the **Recording Folder Path** should be directed to D Directory (**D:\**) as C is reserved for System Programs. The **Archive Folder Path** is usually located in the same directory as the Recording Path for more efficient processing.

For the **Backup Media**, the DVD Media is fixed at 4.7GB (**DVD-RW 4.7GB**) and administrator is not allowed to change the size of DVD, as the recommended DVD type to use is DVD-RAM only. DVD-RAM is recommended only because of data corruption in DVD Disks are relatively high.

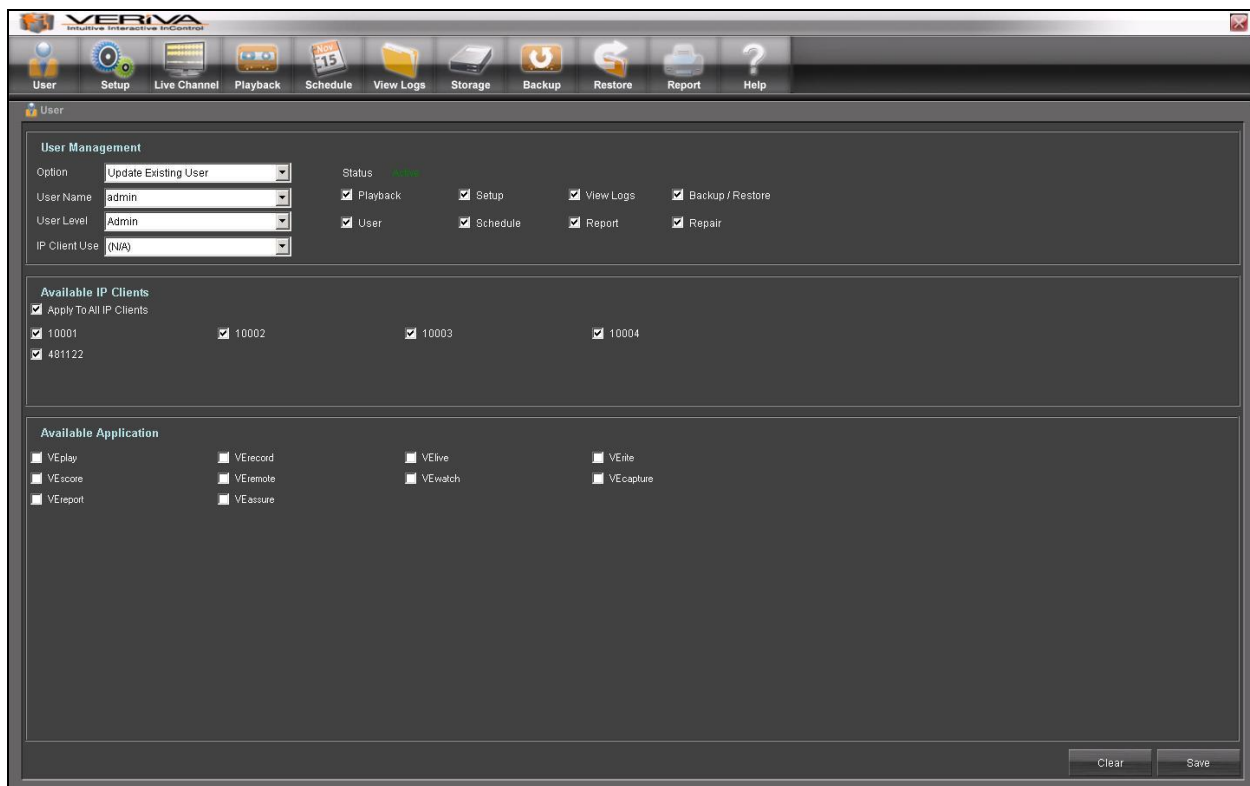
### 7.2.2. User Management

Select **User** → **User Management** for creating and administering user.



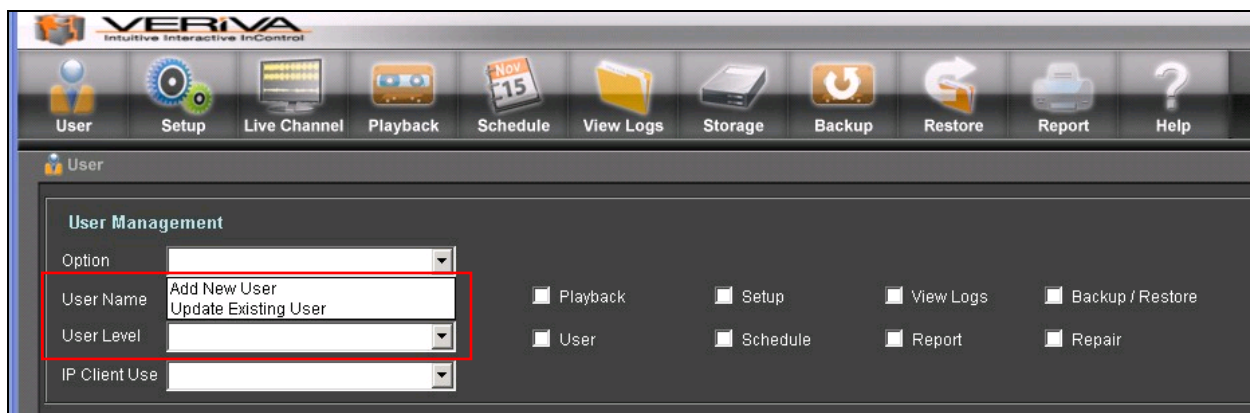
Administrators can allocate unlimited users to have access to specific pages as follows in the User Management Section.

Veriva 3i provides administrators with the capabilities of user management. In the user management page, administrators can add or modify the user's privileges.



To create new user, select the “**Add New User**” field and key in the **User Name**, and the default temporary password is **0000**. The new user will log in with the User Name and temporary password field. Users are recommended to change their passwords upon log in.

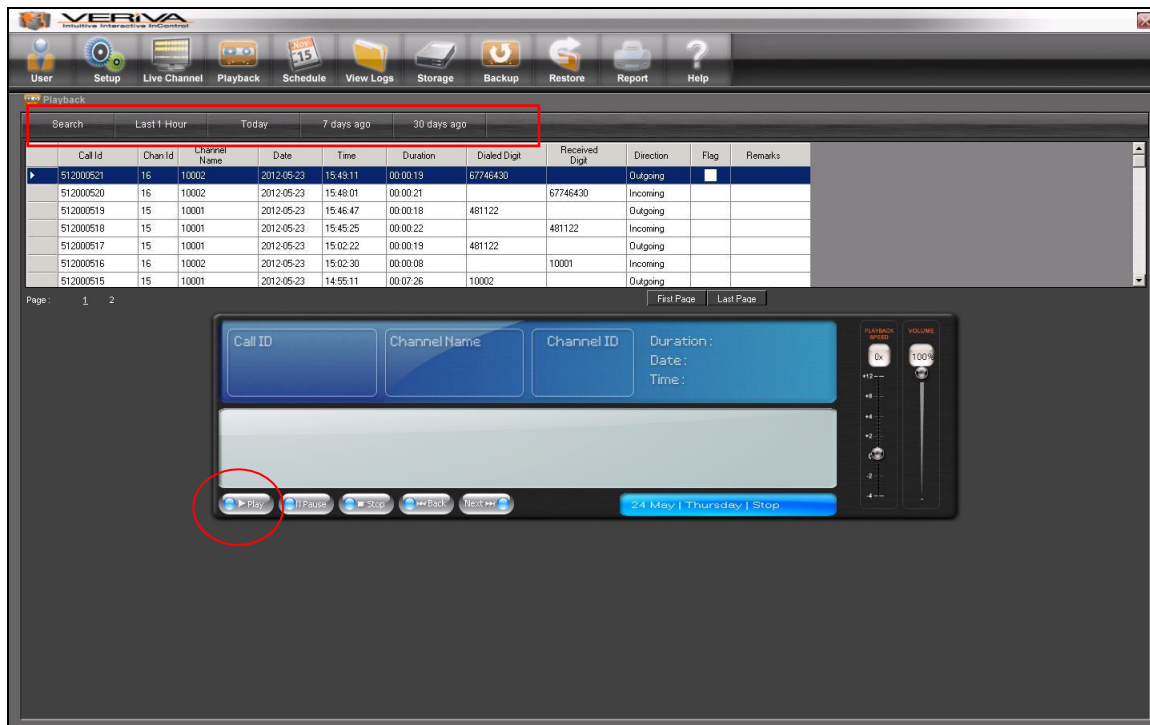
With the newly created user accounts, the administrator can proceed to allocate the **User Level** by selecting either admin or user, and which IP clients the user has access rights to.



### 7.2.3. Playback Options

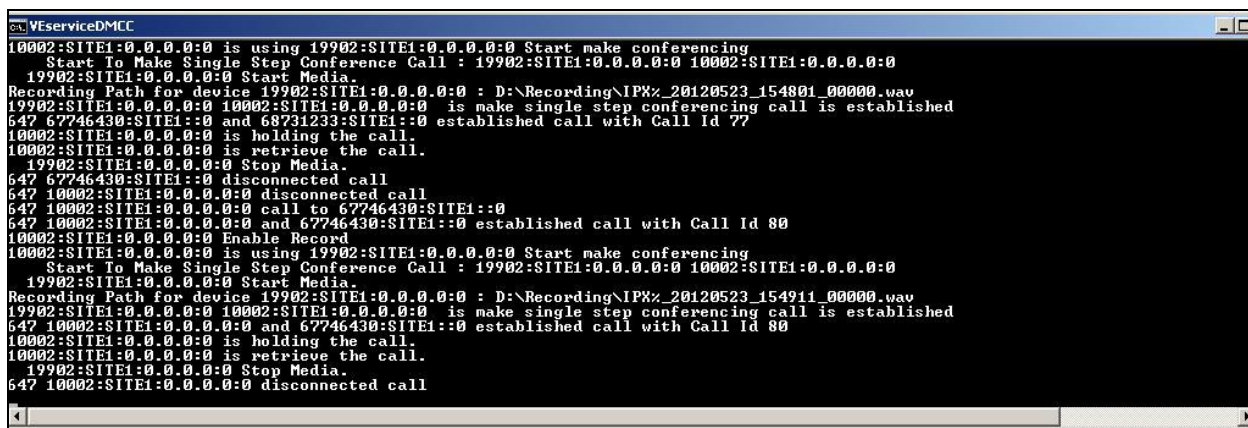
Select **Playback** in the main screen. To playback, user may select by “**Last 1 Hour**”, “**Today**”, “**7 days ago**” and “**30 days ago**”. Select calls in the list and click the **Play** button on the player

located at the bottom panel. Veriva 3i also provides a **Search** function using certain criteria or filters such as channel, date, time range, direction, or dialed/received number.




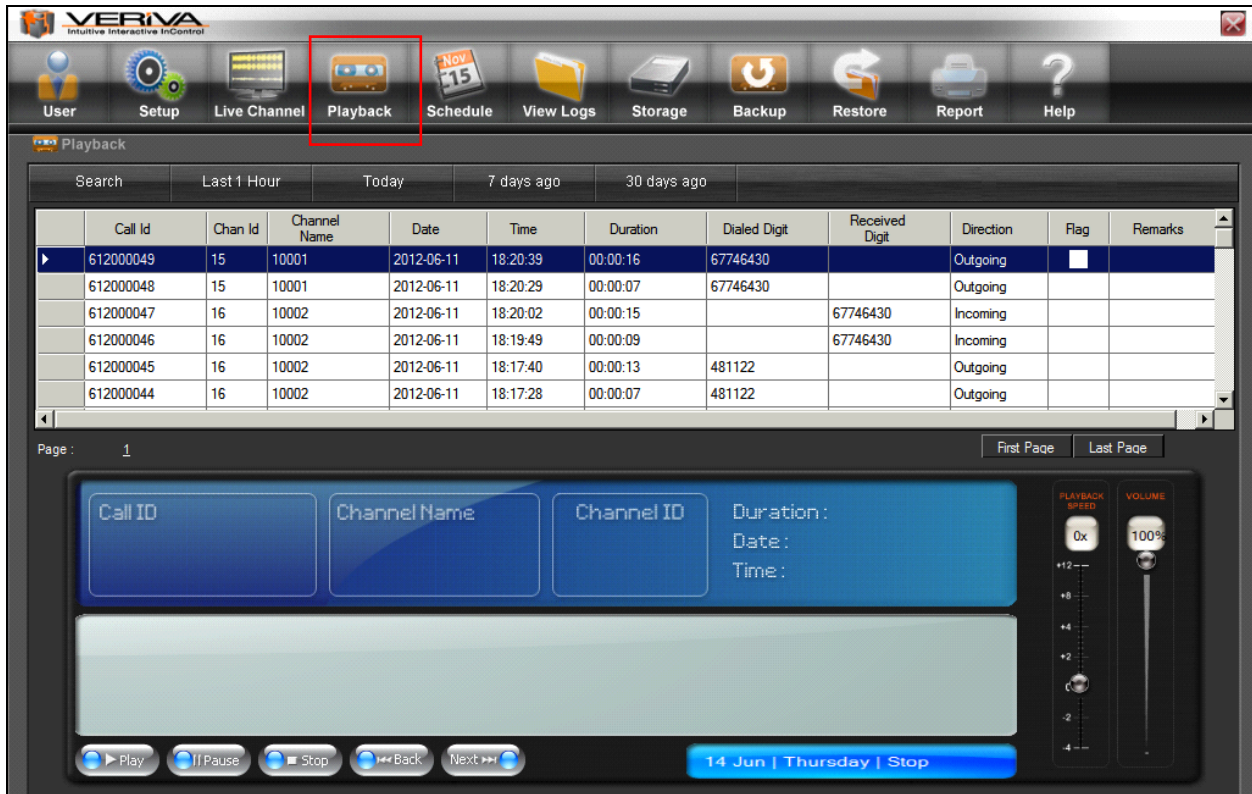
### 7.3. Starting DMCC service

In order for calls to be recorded, **VEserviceDMCC.exe** which is located at the folder “C:\Program Files\Verion\Veriva3iSetup\DMCC” need to be executed after a user has configured Setup Tab in Veriva 3i application. By default, VEServiceDMCC service is set to start automatically upon server start up.



## 8. Verification Steps

Place a call to the agent extension that is being recorded. From the **PlayBack**, verify that the call is successfully recorded. Select the recording and click on the  icon and verify that the recording can be played back successfully.



The screenshot shows the Veriva 3i DMCC Recorder interface. The top navigation bar includes icons for User, Setup, Live Channel, Playback (highlighted with a red box), Schedule, View Logs, Storage, Backup, Restore, Report, and Help. Below the navigation bar, the Playback section is active, displaying a table of recordings. The table has columns for Call Id, Chan Id, Channel Name, Date, Time, Duration, Dialed Digit, Received Digit, Direction, Flag, and Remarks. The first row is selected, showing Call Id 612000049, Chan Id 15, Channel Name 10001, Date 2012-06-11, Time 18:20:39, Duration 00:00:16, Dialed Digit 67746430, Received Digit 67746430, Direction Outgoing, and Flag [X]. Below the table, there are buttons for Play, Pause, Stop, Back, and Next. The bottom status bar shows the date and time: 14 Jun | Thursday | Stop.

Call Id	Chan Id	Channel Name	Date	Time	Duration	Dialed Digit	Received Digit	Direction	Flag	Remarks
612000049	15	10001	2012-06-11	18:20:39	00:00:16	67746430	67746430	Outgoing	[X]	
612000048	15	10001	2012-06-11	18:20:29	00:00:07	67746430		Outgoing		
612000047	16	10002	2012-06-11	18:20:02	00:00:15		67746430	Incoming		
612000046	16	10002	2012-06-11	18:19:49	00:00:09		67746430	Incoming		
612000045	16	10002	2012-06-11	18:17:40	00:00:13	481122		Outgoing		
612000044	16	10002	2012-06-11	18:17:28	00:00:07	481122		Outgoing		

## 9. Conclusion

These Application Notes describe the configuration steps required for Veriva 3i DMCC Recorder to successfully interoperate with Avaya Aura® Communication Manager 6.0.1 and Avaya Aura® Application Enablement Services 6.1.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 10. Additional References

This section references documentation relevant to these Application Notes. Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.0, Doc ID 03-300509, June 2010.
- [2] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.1, Issue 2, February 2011.
- [3] *Veriva 3i 1.0.3 User Administration Manual*, Version 1.00, October 2010.

---

**©2012 Avaya Inc. All Rights Reserved.**

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

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