



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Nexidia ESI-Capture with Avaya Aura<sup>TM</sup> Communication Manager and Avaya Aura<sup>TM</sup> Application Enablement Services - Issue 1.0

### Abstract

These Application Notes describe the procedures for configuring Nexidia ESI-Capture to monitor and record calls placed to and from stations on Avaya Aura<sup>TM</sup> Communication Manager.

The ESI-Capture is an application, built upon Nexidia's Scalable Media Processing (SMP) Framework that captures calls processed by an Avaya VoIP solution and records them along with any associated metadata. The ESI-Capture is composed of the SMP, the Avaya stream control/capture extension, and the recording sink extension. The ESI-Capture interfaces with Avaya Aura<sup>TM</sup> Communication Manager through Avaya Aura<sup>TM</sup> Application Enablement Services, using TSAPI to associate recordings with important CTI information, and DMCC to acquire media. The system uses the DMCC Streaming capability to record extension, and inbound or outbound calls. Voice is recorded at the server in wav format.

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 an Avaya Aura™ Communication Manager, an Avaya Aura™ Application Enablement Services server (AES), and the ESI-Capture. The ESI-Capture is a subset of the Nexidia Enterprise Speech Intelligence (ESI) system which utilizes Speech Analytics Technology to provide a scalable, accurate, affordable and fast solution to analyze all recorded audio.

The ESI-Capture monitors, records, stores, and plays back phone calls for verification. The ESI-Capture uses TSAPI with an Application Enablement Services server to monitor stations to obtain recording triggers and call information. The ESI-Capture also uses the Device, Media and Call Control (DMCC) service with the Application Enablement Services server to register DMCC softphones that the ESI-Capture uses as recording ports.

## 1.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the compliance testing was primarily on verifying the interoperability between Nexidia ESI-Capture, SIP Enablement Services, and Communication Manager.

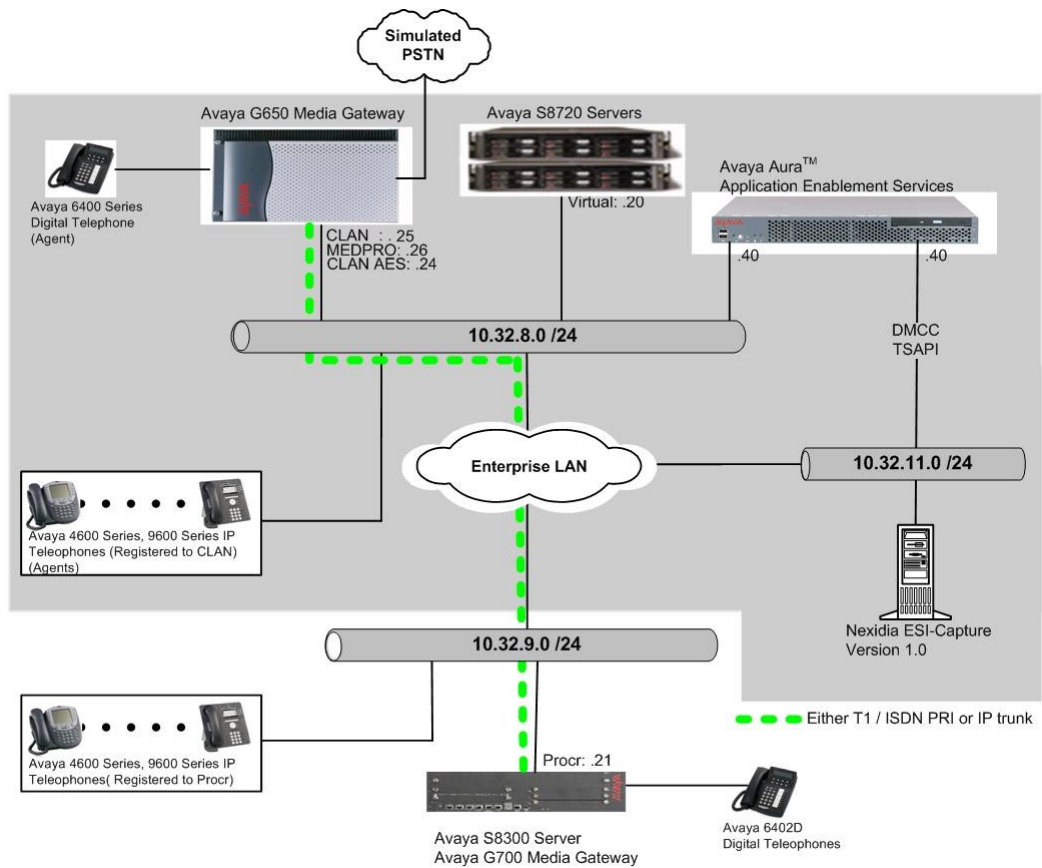
## 1.2. Support

Technical support for the Nexidia ESI-Capture solution can be obtained by contacting Nexidia:

- North/South America and Asia/PAC  
Phone: (866) 355-1241  
Email: [support@nexidia.com](mailto:support@nexidia.com)
- Europe, Middle East and Africa  
Email: [EMEAsupport@nexidia.com](mailto:EMEAsupport@nexidia.com)

# 2. Reference Configuration

**Figure 1** provides the test configuration used for the compliance test. Note that actual configurations may vary. The solution described herein is also extensible to other Avaya Servers and Media Gateways. An Avaya S8300 Server with an Avaya G450 Media Gateway was included during the test to provide an IP trunk between two Communication Manager systems.



**Figure 1: Sample Test Configuration for Nexidia ESI-Capture Solution**

### 3. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8720 Server		Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya G650 Media Gateway		-
	TN2312BP IP Server Interface TN799DP C-LAN Interface TN2302AP IP Media Processor	HW11 FW030 HW20 FW017 HW01 FW108
Avaya S8300 Server with Avaya G700 Media Gateway		Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya Aura™ Application Enablement Services Server		5.2 (r5-2-0-98-0)
Avaya 4600 Series IP Telephones		
	4620SW (H.323)	2.9
	4625SW (H.323)	2.9
Avaya 9600 Series IP Telephones		
	9620 (H.323)	3.1
	9630 (H.323)	3.1
	9650 (H.323)	3.1
Avaya 6408D+ Digital Telephone		-
Nexidia ESI-Capture on Windows Server 2003 with Service Pack 2		1.0

### 4. Configure Avaya Aura™ Communication Manager

This section provides the procedures for configuring an ip-codec-set and ip-network region, switch connection and Computer Telephony Integration (CTI) links, monitored stations, and recording stations on Communication Manager. All the configuration changes in Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

## 4.1. Codec Configuration

Enter the **change ip-codec-set t** command, where **t** is a number between 1 and 7, inclusive.

change ip-codec-set 1				Page	1 of	2
IP Codec Set						
Codec Set: 1						
	Audio	Silence	Frames	Packet		
	Codec	Suppression	Per Pkt	Size(ms)		
1:	G.711MU	n	2	20		
2:	G.729	n	2	20		

## 4.2. IP Network Regions

During compliance testing, a C-LAN board dedicated for H.323 endpoint registration was assigned to IP network region 1. The Avaya IP Telephones and IP Softphones used by the ESI-Capture, registered with the C-LAN boards and were thus also assigned to IP network region 1. One consequence of assigning the aforementioned IP telephones, IP Softphones, and MedPro boards to a common IP network region is that the RTP traffic between them is governed by the same codec set. The second C-LAN board (CLAN-AES), which is dedicated for the AES server, was assigned to network region 2. The following screen shows only network region 1.

change ip-network-region 1		Page	1 of	19
IP NETWORK REGION				
Region: 1				
Location: Authoritative Domain:				
Name:				
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes		
Codec Set: 1		Inter-region IP-IP Direct Audio: yes		
UDP Port Min: 2048		IP Audio Hairpinning? n		
UDP Port Max: 3929				
DIFFSERV/TOS PARAMETERS		RTCP Reporting Enabled? y		
Call Control PHB Value: 46		RTCP MONITOR SERVER PARAMETERS		
Audio PHB Value: 46		Use Default Server Parameters? y		
Video PHB Value: 46				
802.1P/Q PARAMETERS				
Call Control 802.1p Priority: 0		AUDIO RESOURCE RESERVATION PARAMETERS		
Audio 802.1p Priority: 0		RSVP Enabled? n		
Video 802.1p Priority: 5				
H.323 IP ENDPOINTS				
H.323 Link Bounce Recovery? y				
Idle Traffic Interval (sec): 20				
Keep-Alive Interval (sec): 5				
Keep-Alive Count: 5				

### 4.3. Configure Switch Connection and CTI Links between Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services

The AES server forwards CTI requests, responses, and events between the ESI-Capture and Communication Manager. The AES server communicates with Communication Manager over a switch connection link. Within the switch connection link, CTI links may be configured to provide CTI services to CTI applications such as the ESI-Capture. The following steps demonstrate the configuration of the Communication Manager side of the switch connection and CTI links. See **Section 5** for the details of configuring the AES side of the switch connection and CTI links.

Enter the **add cti-link m** command, where **m** 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.

<b>add cti-link 4</b>	Page 1 of 2
CTI LINK	
CTI Link: 4	
Extension: 20006	
Type: ADJ-IP	
Name: TSAPI	COR: 1

Enter the **change node-names ip** command. In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoints (Avaya IP Telephones, and IP Softphones, and AES Device, Media and Call Control API stations) and the CLAN-AES IP address was used for connectivity to Avaya AES.

<b>change node-names ip</b>	Page 1 of 2
IP NODE NAMES	
Name	IP Address
CLAN	10.32.8.25
CLAN-AES	10.32.8.24
MEDPRO	10.32.8.26
MEDPRO2	10.32.8.27
S8300	10.32.10.21
default	0.0.0.0

Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the **CLAN-AES** board that was configured previously in the IP NODE NAMES form in this section. During the compliance test, the default port was utilized for the Local Port field.

<b>change ip-services</b>	Page 1 of 4				
IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	CLAN-AES	8765		

On **Page 4**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES server using ssh, and running the command **uname -a**. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the AES server in **Section 5.1**.

change ip-services					Page 4 of 4
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	server2	xxxxxxxxxxxxxxxxxx	y	idle	
2:					
3:					

#### 4.4. Monitored Stations

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. During the compliance test, the following recorded stations were created.

- 22001 (Avaya 4625SW IP)
- 22002 (Avaya 9620 IP)
- 22003 (Avaya 9650 IP)
- 22004 (Avaya 9630 IP)
- 22007 (Avaya 6408D+)
- 22009 (Avaya IP Agent)

#### 4.5. Recording Stations

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the Type field to an IP telephone set type, enter a descriptive Name, specify the Security Code, and make sure that the IP Softphone field is set to **y**. For the compliance test, recording stations from 23001 to 23023 were created.

change station 23001			Page 1 of 5
STATION			
Extension: 23001	Lock Messages? n	BCC: 0	
Type: 4620	Security Code: *	TN: 1	
Port: S00046	Coverage Path 1:	COR: 1	
Name: DMCC-1	Coverage Path 2:	COS: 1	
	Hunt-to Station:		
STATION OPTIONS			
Loss Group: 19	Time of Day Lock Table:		
	Personalized Ringing Pattern: 1		
	Message Lamp Ext: 23001		
Speakerphone: 2-way	Mute Button Enabled? y		
Display Language: english	Expansion Module? n		
Survivable GK Node Name:			
Survivable COR: internal	Media Complex Ext:		
Survivable Trunk Dest? y	IP SoftPhone? y		
	IP Video Softphone? n		
	Customizable Labels? y		

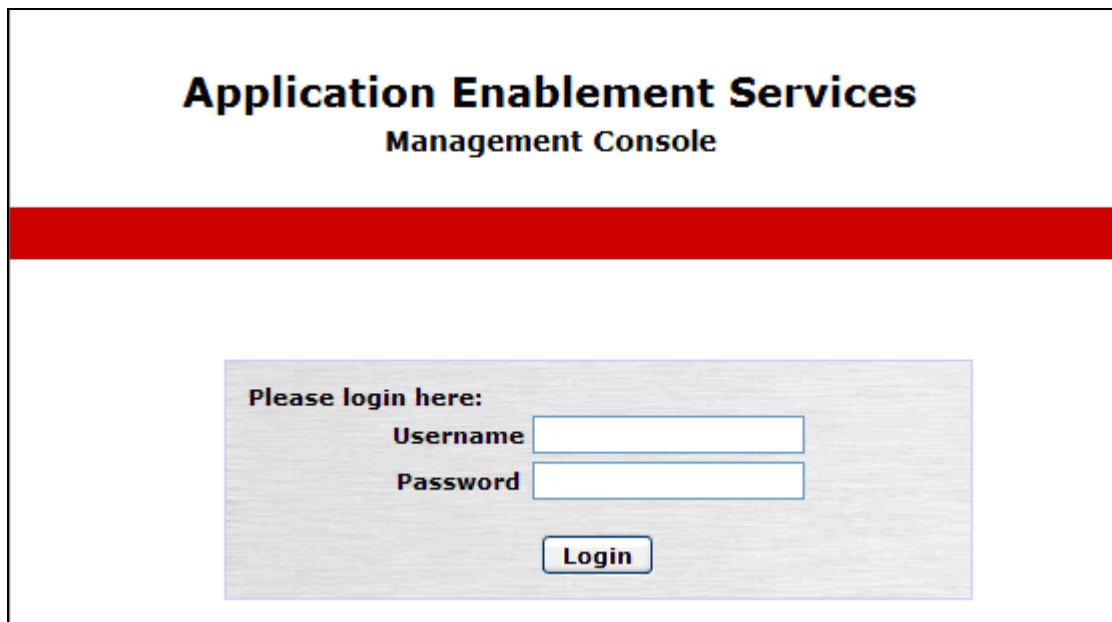
## 5. Configure Avaya Aura™ Application Enablement Services

The Avaya Aura™ Application Enablement Services server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager. The AES server receives requests from CTI applications, and forwards them to Communication Manager. Conversely, the AES server receives responses and events from Communication Manager and forwards them to the appropriate CTI applications.

This section assumes that installation and basic administration of the AES server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, a CMAPI port, and creating a CTI link for TSAPI.

### 5.1. Configure Switch Connection


Launch a web browser, enter <https://<IP address of AES server>> in the address field, and log in with the appropriate credentials for accessing the AES CTI OAM pages.



The screenshot shows the login interface for the Avaya Aura Application Enablement Services Management Console. At the top, the title "Application Enablement Services" is displayed in a large, bold, black font, with "Management Console" in a smaller, bold, black font directly below it. A thick red horizontal bar separates the header from the main content area. In the center of the page, there is a light gray rectangular box with a thin blue border. Inside this box, the text "Please login here:" is followed by two input fields: "Username" and "Password". Below these fields is a "Login" button with a blue border and a light gray background.



Click on **Communication Manager** → **Switch Connection** in the left pane to invoke the Switch Connections page.

 **Application Enablement Services**  
**Management Console**

Welcome: User craft  
Last login: Tue Jan 26 11:34:52 2010 from 10.64.43.10  
HostName/IP: server1/10.64.40.40  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

Home

Home | Help | Logout

- ▶ AE Services
- ▶ **Communication Manager Interface**
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

### Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain.

A Switch Connection defines a connection between the AESs server and Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Fri Dec 11 17:36:53 2009 from 10.32.11.10  
HostName/IP: server1/10.32.8.40  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections [Home](#) | [Help](#) | [Logout](#)

- AE Services
- Communication Manager Interface
  - Switch Connections**
  - Dial Plan
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

**Switch Connections**

S8720G650 [Add Connection](#)

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
S8300G450	No	30	1

[Edit Connection](#) [Edit PE/CLAN IPs](#) [Edit H.323 Gatekeeper](#) [Delete Connection](#)

The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Communication Manager in **Section 4.3**. Click on **Apply**.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Fri Dec 11 17:36:53 2009 from 10.32.11.10  
HostName/IP: server1/10.32.8.40  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections [Home](#) | [Help](#) | [Logout](#)

- AE Services
- Communication Manager Interface
  - Switch Connections**
  - Dial Plan
- Licensing
- Maintenance
- Networking
- Security
- Status
- User Management
- Utilities
- Help

**Connection Details - S8720G650**

Switch Password:

Confirm Switch Password:

Msg Period:  Minutes (1 - 72)

SSL: ☒

Processor Ethernet: ☐

[Apply](#) [Cancel](#)

After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit PE/CLAN IPs**.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Fri Dec 11 17:36:53 2009 from 10.32.11.10  
HostName/IP: server1/10.32.8.40  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input type="radio"/> S8300G450	No	30	1
<input checked="" type="radio"/> S8720G650	No	30	0

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

Enter the CLAN-AES IP address which was configured for AES connectivity in **Section 4.3** and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services. Click on the **Back** button after the completion.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Fri Dec 11 17:36:53 2009 from 10.32.11.10  
HostName/IP: server1/10.32.8.40  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections Home | Help | Logout

Edit CLAN IPs - S8720G650

10.32.8.25 Add Name or IP

Name or IP Address	Status

Delete IP Back

On the Switch Connections page, click on **Edit H.323 Gatekeeper** for DMCC call control and monitor.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Fri Dec 11 17:36:53 2009 from 10.32.11.10  
HostName/IP: server1/10.32.8.40  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
S8300G450	No	30	1
S8720G650	No	30	0

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

On the **Edit H.323 Gatekeeper – S8720G650** page, enter the C-LAN IP address which will be used for the DMCC service. Click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.

**AVAYA Application Enablement Services Management Console**

Welcome: User craft  
Last login: Tue Jan 26 13:40:05 2010 from 10.64.43.10  
HostName/IP: server1/10.64.40.40  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

Edit H.323 Gatekeeper - S8720G650

10.32.8.25 Add Name or IP

Name or IP Address

Delete IP

## 5.2. Configure the TSAPI CTI link

Navigate to **AE Services** → **TSAPI** → **TSAPI Links** in the left pane, and click on the **Add Link** button to create a TSAPI CTI link.

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 "craft" with login details. A red navigation bar contains "AE Services | TSAPI | TSAPI Link" and links for "Home | Help | Logout". The left sidebar shows a tree view with "AE Services" expanded, containing "CVLAN", "DLG", "DMCC", "SMS", "TSAPI" (expanded), "TSAPI Links" (selected), and "TSAPI Properties". The main content area is titled "TSAPI Links" and contains a table with headers: "Link", "Switch Connection", "Switch CTI Link #", "ASAI Link Version", and "Security". Below the table are three buttons: "Add Link", "Edit Link", and "Delete Link". The "Add Link" button is highlighted with a red box.

Select a Switch Connection using the drop-down menu. The Switch Connection is configured in **Section 5.1**. Select the Switch CTI Link Number using the drop-down menu. Switch CTI Link Number should match with the number configured in the cti-link form in **Section 4.3**. Click the **Apply Changes** button. Default values may be used in the remaining fields.

The screenshot shows the "Add TSAPI Links" form in the Avaya Application Enablement Services Management Console. The top header and navigation bar are identical to the previous screenshot. The left sidebar shows the same tree view, but "Communication Manager Interface" is now visible under "TSAPI Properties". The main content area is titled "Add TSAPI Links" and contains a form with the following fields: "Link" (dropdown menu with value "1"), "Switch Connection" (dropdown menu with value "S8720G650"), "Switch CTI Link Number" (dropdown menu with value "4"), "ASAI Link Version" (dropdown menu with value "4"), and "Security" (dropdown menu with value "Unencrypted"). Below the form are two buttons: "Apply Changes" and "Cancel Changes". The "Apply Changes" button is highlighted with a red box.

### 5.3. Configure the CTI Users

Navigate to **User Management → User Admin → Add User**. On the Add User page, provide the following information:

- User Id
- Common Name
- Surname
- User Password
- Confirm Password

The above information (User ID and User Password) must match with the information configured in the ESI-Capture Configuration page in **Section 6**.

Select **Yes** using the drop down menu on the CT User field. This enables the user as a CTI user. Default values may be used in the remaining fields. Click the **Apply** button (not shown) at the bottom of the screen to complete the process.

The screenshot displays 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: 'Welcome: User craft', 'Last login: Fri Dec 11 17:36:53 2009 from 10.32.11.10', 'HostName/IP: server1/10.32.8.40', 'Server Offer Type: TURNKEY', and 'SW Version: r5-2-0-98-0'. A red navigation bar contains 'User Management | User Admin | List All Users' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'User Management' expanded, and 'User Admin' and 'Add User' highlighted. The main content area is the 'Add User' form, which includes fields for \* User Id (Nexidia), \* Common Name (Nexidia), \* Surname (Nexidia123&), User Password (masked), Confirm Password (masked), Admin Note, Avaya Role (None), Business Category, Car License, CM Home, Cms Home, CT User (Yes), Department Number, Display Name, Employee Number, and Employee Type. Red boxes highlight the \* User Id, \* Common Name, \* Surname, User Password, Confirm Password, and CT User fields.

Once the user is created, navigate to the **CTI OAM Security → Security Database → CTI Users → List All Users** page. Select the User ID created previously, and click the **Edit** button to set the permission of the user.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Fri Dec 11 17:36:53 2009 from 10.32.11.10  
HostName/IP: server1/10.32.8.40  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

Security | Security Database | CTI Users | List All UsersHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

▪ Search Users

▪ Devices

▪ Device Groups

▪ Tlinks

▪ Tlink Groups

▪ Worktops

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input checked="" type="radio"/> Nexidia	Nexidia	NONE	NONE

Edit

List All

Provide the user with unrestricted access privileges by checking the **Unrestricted Access** button. Click on the **Apply Changes** button.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Fri Dec 11 17:36:53 2009 from 10.32.11.10  
HostName/IP: server1/10.32.8.40  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

Security | Security Database | CTI Users | List All UsersHome | Help | Logout

▸ AE Services

▸ Communication Manager Interface

▸ Licensing

▸ Maintenance

▸ Networking

▼ Security

▸ Account Management

▸ Audit

▸ Certificate Management

Enterprise Directory

▸ Host AA

▸ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

▪ Search Users

▪ Devices

▪ Device Groups

▪ Tlinks

▪ Tlink Groups

▪ Worktops

Edit CTI User

User Profile:

User IDNexidia

Common NameNexidia

Worktop NameNONE ▾

Unrestricted Access☒

Call Origination and Termination / Device StatusNone ▾

Call and Device Monitoring:

DeviceNone ▾

Call / DeviceNone ▾

Call☐

Routing Control:

Allow Routing on Listed DevicesNone ▾

Apply ChangesCancel Changes



## 5.4. Configure the CTI Port

Navigate to the **Administration → Network Configuration → Ports** page to set the DMCC server port. During the compliance test, the default port values were utilized. The following screen displays the default port values. Since the unencrypted port was utilized during the compliance test, set the Unencrypted Port field to **Enabled**. Default values may be used in the remaining fields. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

**AVAYA** Application Enablement Services  
Operations Administration and Maintenance

You are here: > Administration > Network Configuration > Ports

**Ports**

CVLAN Ports

			Enabled Disabled
Unencrypted TCP Port	9999		<input checked="" type="radio"/> <input type="radio"/>
Encrypted TCP Port	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	
1050	

TCP Port Max	
1065	

Encrypted TLINK Ports

TCP Port Min	
1066	

TCP Port Max	
1081	

DMCC Server Ports

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

## 6. Configure Nexidia ESI-Capture

This section only describes the interface configuration for the ESI-Capture application to communicate with AES and Communication Manager.

Refer to **Section 10, [3] and [4]** for configuring the ESI-Capture application. The following screen shows the global.properties file. During the compliance test, the highlighted values were utilized:

```
#nx.switch.name=cmsim
nx.switch.name=S8720G650
nx.capture.channel0.extension=23001
nx.capture.channel0.password=1234
nx.capture.channel1.extension=23002
nx.capture.channel1.password=1234
nx.capture.channel2.extension=23003
nx.capture.channel2.password=1234
nx.capture.channel3.extension=23004
nx.capture.channel3.password=1234
nx.capture.channel4.extension=23005
nx.capture.channel4.password=1234
#nx.capture.channel5.extension=32205
#nx.capture.channel6.extension=32206
#nx.capture.channel7.extension=32207
#nx.capture.channel8.extension=32208
#nx.capture.channel9.extension=32209

nx.manager.monitor0.extension=22001
nx.manager.monitor1.extension=22002
nx.manager.monitor2.extension=22003
nx.manager.monitor3.extension=22007
nx.manager.monitor4.extension=22009
#nx.manager.monitor4.extension=32404
#nx.manager.monitor5.extension=32405
#nx.manager.monitor6.extension=32406
#nx.manager.monitor7.extension=32407
#nx.manager.monitor8.extension=32408
#nx.manager.monitor9.extension=32409

nx.capture.codecs=g711U

#cmapi.server_ip=192.168.1.224
cmapi.server_ip=10.32.11.40
cmapi.server_port=4721
#cmapi.username=craft
#cmapi.password=craft01
cmapi.username=Nexidia
cmapi.password=Nexidia123&
# It is important to set this value in production to enable session recovery
without
# reestablishing state(reregistering the stations)
cmapi.session_cleanup_delay=60
```

## 7. General Test Approach and Test Results

The general approach was to manually place calls to and from stations, monitor and record them using the ESI-Capture, and verify the recordings. The types of calls included internal calls, inbound, outbound trunk calls, transfer calls, conference calls. For serviceability testing, failures such as cable pulls, CTI link busyouts and releases, and resets were applied.

The test objectives were verified. For serviceability testing, Nexidia ESI-Capture operated properly after recovering from failures such as cable disconnects, and resets of Nexidia ESI-Capture and the SIP Enablement Services server.

## 8. Verification Steps

This section provides the steps that can be performed to verify proper configuration of Communication Manager and AES.

### 8.1. Verify Communication Manager

Verify the status of the administered AES link by using the **status aesvcs link** command.

```
status aesvcs link
```

AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	server2	10.32.8.40	60336	CLAN-AES	208	197

Verify the Service State field of the administered TSAPI CTI link is in **established** state, by using the **status aesvcs cti-link** command.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
4	4	no	server2	established	15	15

## 8.2. Verify Avaya Application Enablement Services

From the CTI OAM Admin web pages, verify the status of the TSAPI and DMCC Services are ONLINE, by selecting **AE Services** from the left pane.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Tue Jan 26 13:40:05 2010 from 10.64.43.10  
HostName/IP: server1/10.64.40.40  
Server Offer Type: TURNKEY  
SW Version: r5-2-0-98-0

**AE Services** [Home](#) | [Help](#) | [Logout](#)

**▼ AE Services**

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▶ TSAPI
- Communication Manager Interface**
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

**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	DOWN	Stopped	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

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) version 5.0

## 9. Conclusion

These Application Notes illustrate the procedures for configuring the ESI-Capture call recording solution to monitor and record calls placed to and from stations on an Communication Manager system. In the configuration described in these Application Notes, the ESI-Capture employs Device, Media and Call Control Application Programming Interface virtual stations as recording ports. During compliance testing, the ESI-Capture successfully monitored events and recorded calls placed to and from stations.

## 10. Additional References

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

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

[1] *Administering Avaya Aura™ Communication Manager*, Issue 5.0, May 2009, Document Number 03-300509

[2] *Application Enablement Services Administration and Maintenance Guide*, Release 5.2, Issue 11, November 2009, Document Number 02-300357

The following documentation was provided by Nexidia

[3] *Nexidia ESI--Capture Install and Config Guide*, Issue 1.0, October, 2009

[4] *Nexidia ESI--Capture System Requirements*, Issue 1.0

---

**©2010 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).