



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

---

# **Application Notes for Configuring ESNA Office-LinX with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager - Issue 1.0**

### **Abstract**

These Application Notes describe the procedure for configuring ESNA Office-LinX to interoperate with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager.

The Office-LinX is a voice processing system that functions with an organization's existing telephone system to enhance its overall telecommunications environment.

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 procedure for configuring ESNA Office-LinX to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

ESNA Office-LinX is a voice processing system that functions with an organization's existing telephone system to enhance its overall telecommunications environment.

ESNA Office-LinX acts as a unified messaging solution offering call and voice messaging control over the phone, web, or via client applications from the user's desktop PC or mobile smart device. System Administrative functions may be performed either by using a touchtone telephone or the Windows interface from the Voice Mail server.

However, during this compliance test, the focus was on the TSAPI CTI link (3<sup>rd</sup> party Call Control) integration between ESNA Office-LinX and Avaya Aura® Application Enablement Services server.

## 2. General Test Approach and Test Results

The general test approach was to place calls to ESNA Office-LinX, using a coverage path and hunt group. The main objectives were to verify the following:

- Successfully establish calls to ESNA Office-LinX from SIP and H.323 telephones attached to Session Manager or Communication Manager.
- Successfully transfer from ESNA Office-LinX to SIP and H.323 telephones attached to Session Manager or Communication Manager.
- Using the Office-LinX UC Client Manager, verify the call state is consistent with the physical phone.
- Using the Office-LinX UC Client Manager, calls can be answered / transferred/ Held / Resumed and Hung up.

For serviceability testing, failures such as cable pulls and resets were applied. All test cases passed.

### 2.1. Interoperability Compliance Testing

The interoperability compliance testing included features and serviceability tests. The focus of the compliance testing was primarily on verifying the interoperability between ESNA Office-LinX and Application Enablement Services.

### 2.2. Test Results

The test objectives were verified. For serviceability testing, ESNA Office-LinX operated properly after recovering from failures such as cable disconnects and resets of ESNA Office-LinX, Communication Manager, and Application Enablement Services.

### 2.3. Support

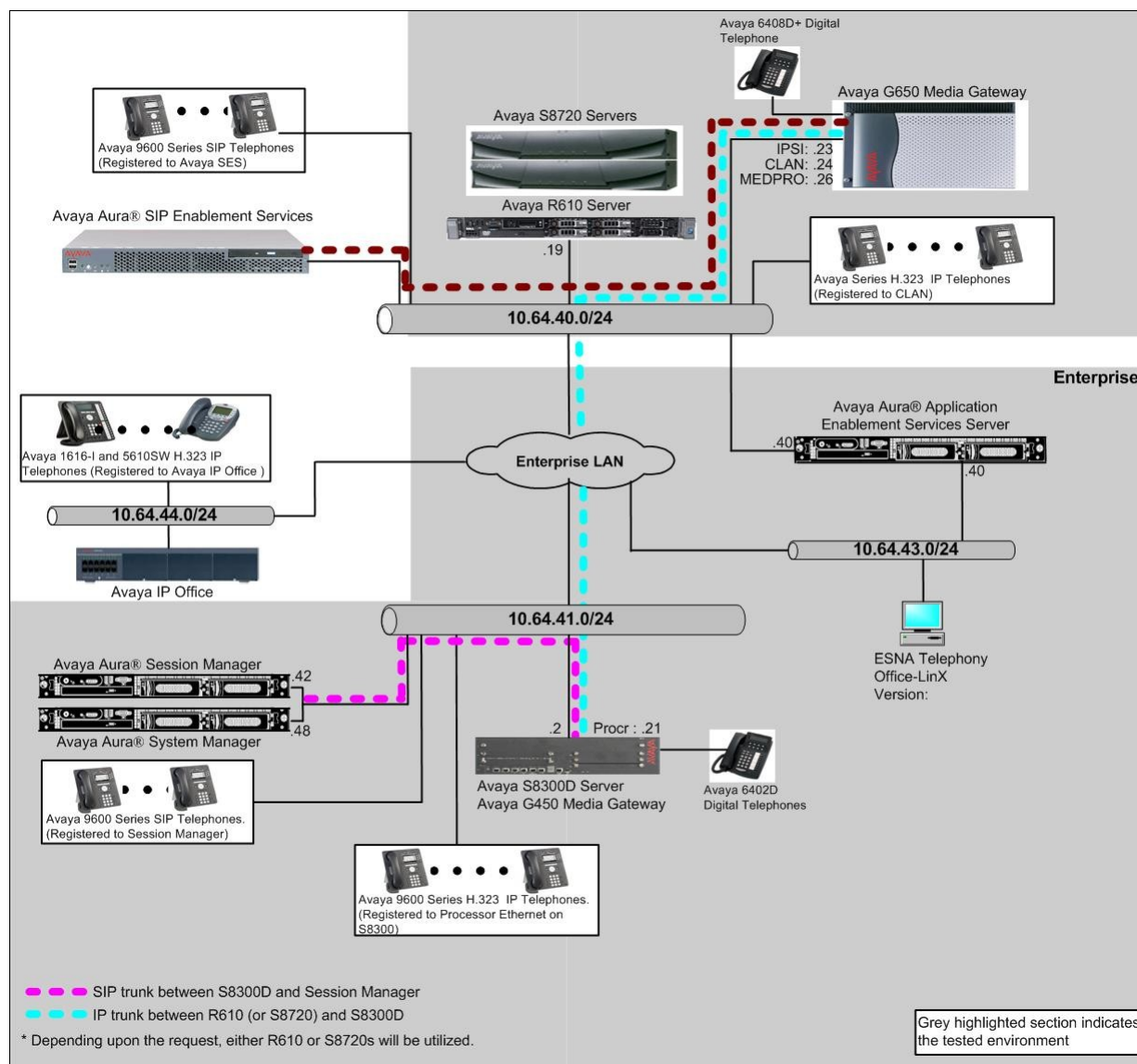
Technical support for the ESNA Office-LinX solution can be obtained by contacting ESNA:

- URL – [techsupport@esna.com](mailto:techsupport@esna.com)
- Phone – (905) 707-1234

### 3. Reference Configuration

**Figure 1** illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with a Session Manager and an Avaya S8300D Server with an Avaya G450 Media Gateway. Endpoints include Avaya 9600 Series SIP telephones, Avaya 9600 Series H.323 IP telephones, and an Avaya 6408D Digital telephone. Avaya S8720 Servers with Avaya G650 Media Gateway were included in the test to provide an inter-switch scenario.

ESNA Office-LinX does not register with the Session Manager as an endpoint but instead is configured as a trusted SIP entity.



**Figure 1: Test Configuration of ESNA Office-LinX**

## 4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.0.1(R016x.00.1.510.1) w/ patch 00.1.510.1-19303
Avaya Aura® System Manager		6.1.5.0
Avaya Aura® Session Manager		6.1.5.0
Avaya S8720 Servers with Avaya G650 Media Gateway (used for inter-switch test scenarios)		Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4) w/ patch 02.1.016.4 - 18365
Avaya Aura® Application Enablement Services		6.1 (R6-1-0-20-0)
Avaya 4600 and 9600 Series SIP Telephones		
	9620 (SIP)	2.5
	9630 (SIP)	2.5
	9650 (SIP)	2.5
Avaya 4600 and 9600 Series IP Telephones		
	4625 (H.323)	2.9
	9620 (H.323)	3.1
	9630 (H.323)	3.1
	9650 (H.323)	3.1
Avaya 6408D+ Digital Telephone		-
ESNA Office-LinX		8.5 SP1

## 5. Configure Avaya Aura® Communication Manager

In the compliance test, Communication Manager was set up as an Evolution Server. This section describes the procedure for setting up a SIP trunk between Communication Manager and Session Manager. The steps include setting up an IP codec set, an IP network region, IP node names, a signaling group, a trunk group, a SIP station, and the TSAPI CTI link. Before a trunk can be configured, it is necessary to verify that there is enough capacity to setup an additional trunk. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Communication Manager System Access Terminal (SAT) interface. All SIP telephones, except ESNA Office-LinX, are configured as off-PBX telephones in Communication Manager.

## 5.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient Maximum Off-PBX Telephones – OPS licenses.

If not, contact an authorized Avaya account representative to obtain additional licenses

display system-parameters customer-options		Page 1 of 11
OPTIONAL FEATURES		
G3 Version: V16	Software Package: Standard	
Location: 2	System ID (SID): 1	
Platform: 28	Module ID (MID): 1	
		USED
Platform Maximum Ports:	6400	185
Maximum Stations:	500	19
Maximum XMOBILE Stations:	2400	0
Maximum Off-PBX Telephones - EC500:	10	0
Maximum Off-PBX Telephones - OPS:	500	9
Maximum Off-PBX Telephones - PBFMC:	10	0
Maximum Off-PBX Telephones - PVFMC:	10	0
Maximum Off-PBX Telephones - SCCAN:	0	0
Maximum Survivable Processors:	0	0

On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed.

If not, contact an authorized Avaya account representative to obtain additional licenses.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	4000	20
Maximum Concurrently Registered IP Stations:	2400	3
Maximum Administered Remote Office Trunks:	4000	0
Maximum Concurrently Registered Remote Office Stations:	2400	0
Maximum Concurrently Registered IP eCons:	68	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	2400	0
Maximum Video Capable IP Softphones:	10	0
Maximum Administered SIP Trunks:	4000	110
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0
Maximum Number of DS1 Boards with Echo Cancellation:	80	0
Maximum TN2501 VAL Boards:	10	0
Maximum Media Gateway VAL Sources:	50	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	8	0

## 5.2. IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and Session Manager. Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 5.3** for configuring the IP network region to specify which codec sets may be used within and between network regions.

**Note:** ESNA Office-LinX supports G.711MU and G.711A. During the compliance test, G711MU was utilized.

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			

### 5.3. Configure IP Network Region

This section describes the steps for administering an IP network region in Communication Manager for communication between Communication Manager and Session Manager. Enter the **change ip-network-region <n>** command, where **n** is a number between **1** and **250** inclusive, and configure the following:

- **Authoritative Domain** – Enter the appropriate name for the Authoritative Domain. During the compliance test, the authoritative domain is set to **avaya.com**. This should match the SIP Domain value used in Session Manager.
- **Codec Set** – Set the codec set number as provisioned in **Section 5.2**.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location:	Authoritative Domain: avaya.com	
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: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

## 5.4. Configure IP Node Name

This section describes the steps for setting an IP node name for Session Manager in Communication Manager. Enter the **change node-names ip** command, and add a node name for Session Manager along with its IP address.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
CLAN	10.64.40.24	
SM-1	10.64.41.42	
default	0.0.0.0	
procr	10.64.41.21	
procr6	::	
rdtt	10.64.43.10	
s8300-lsp	10.64.42.21	

## 5.5. Configure SIP Signaling

Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- **Group Type** – Set to **sip**.
- **IMS Enabled** – Verify that the field is set to **n**. Setting this field to **y** will cause Communication Manager to behave as a Feature Server.
- **Transport Method** – Set to **tls** (Transport Layer Security).
- **Near-end Node Name** – Set to **procr** as displayed in the IP Node Names **Section 5.4**.
- **Far-end Node Name** – Set to the Session Manager name configured in **Section 5.4**.
- **Far-end Network Region** – Set to the region configured in **Section 5.3**.
- **Far-end Domain** – Set to **avaya.com**. This should match the Authoritative Domain value in **Section 5.3**.
- **Direct IP-IP Audio Connections** – Set to **y**, as shuffling was enabled during the compliance test.

add signaling-group 92		SIGNALING GROUP
Group Number: 92	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		SIP Enabled LSP? n
IP Video? n		Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM-1	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? n	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

## 5.6. Configure Trunk Group

To configure the trunk group, enter the **add trunk-group <t>** command, where **t** is an available trunk group and configure the following:

- **Group Type** – Set the Group Type field to **sip**.
- **Group Name** – Enter a descriptive name.
- **TAC (Trunk Access Code)** – Set to any available trunk access code.
- **Service Type** – Set the Service Type field to **tie**.
- **Signaling Group** – Set to the Group Number field value for the signalling group configured in **Section 5.5**
- **Number of Members** – Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
add trunk-group 92                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 92                                     Group Type: sip          CDR Reports: y
Group Name: SM 41 42                                COR: 1                 TN: 1                TAC: 1092
Direction: two-way                                Outgoing Display? n
Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                                Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 92
                                                Number of Members: 20
```

On **Page 3**, during the compliance test, the Numbering Format field was set to **private**.

```
add trunk-group 92                                     Page 3 of 21
TRUNK FEATURES
ACA Assignment? n                                Measured: none
                                                Maintenance Tests? y
                                                Numbering Format: private
                                                UUI Treatment: service-provider
                                                Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n
                                                Modify Tandem Calling Number: no
Show ANSWERED BY on Display? Y
DSN Term? N
```



## 5.7. Configure Hunt Group

This section describes the steps for administering a hunt group in Communication Manager. Enter the **add hunt-group <h>** command, where **h** is an available hunt group number. The following fields were configured for the compliance test.

- **Group Name** – Enter a descriptive name
- **Group Extension** – Enter an available extension that is valid in the provisioned dial plan.

Add hunt-group 93		Page 1 of 60	
HUNT GROUP			
Group Number:	93	ACD?	n
Group Name:	ESNA	Queue?	n
Group Extension:	72036	Vector?	n
Group Type:	ucd-mia	Coverage Path:	
TN:	1	Night Service Destination:	
COR:	1	MM Early Answer?	n
Security Code:		Local Agent Preference?	n
ISDN/SIP Caller Display:			

On **Page 2**, provide the following information:

- **Message Center** – Enter **sip-adjunct**, indicating the type of messaging adjunct used for this hunt group. This value will also be used in the Station form.
- **Voice Mail Number** – Enter the Voice Mail Number, which is the extension of ESNA Office-LinX.
- **Voice Mail Handle** – Enter the Voice Mail Handle which is the extension of ESNA Office-LinX.
- **Routing Digit (e.g., AAR/ARS Access Code)** – Enter the AAR Access Code as defined in the Feature Access Code form.

add hunt-group 93		Page 2 of 60	
HUNT GROUP			
Message Center: sip-adjunct			
Voice Mail Number	Voice Mail Handle	Routing Digits (e.g., AAR/ARS Access Code)	
72036	72036	8	

## 5.8. Configure Coverage Path

This section describes the steps for administering a coverage path in Communication Manager. Enter the **add coverage path <s>** command, where **s** is a valid coverage path number. The **Point1** value of **h93** is used to represent the hunt group number 93 created in **Section 5.7**. Default values for the other fields may be used.

add coverage path 93		Page 1 of 1	
COVERAGE PATH			
Coverage Path Number: 93			
Cvg Enabled for VDN Route-To Party? n		Hunt after Coverage? n	
Next Path Number:		Linkage	
COVERAGE CRITERIA			
Station/Group Status	Inside Call	Outside Call	
Active?	n	n	
Busy?	y	y	
Don't Answer?	y	y	Number of Rings: 2
All?	n	n	
DND/SAC/Goto Cover?	y	y	
Holiday Coverage?	n	n	
COVERAGE POINTS			
Terminate to Coverage Pts. with Bridged Appearances? n			
Point1: h93	Rng:	Point2:	
Point3:		Point4:	
Point5:		Point6:	

## 5.9. Configure SIP Endpoint

SIP endpoints and off-pbx-telephone stations will be automatically created in Communication Manager when users (SIP endpoints) are created in Session Manager.

## 5.10. Configure Route Pattern

For the trunk group created in **Section 5.6**, define the route pattern by entering the **change route-pattern <r>** command, where **r** is an unused route pattern number. The route pattern consists of a list of trunk groups that can be used to route a call. The following screen shows that route-pattern 93 will utilize trunk group 93 to route calls. Default values for the other fields may be used.

change route-pattern 93													Page 1 of 3	
Pattern Number: 93 Pattern Name: 2ESNA-SM1														
SCCAN? n Secure SIP? n														
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC
No			Mrk	Lmt	List	Del	Digits						QSIG	
Dgts													Intw	
1: 93 0													n	user
2:													n	user
3:													n	user
4:													n	user
5:													n	user
6:													n	user
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR														
0 1 2 M 4 W Request													Dgts Format	
													Subaddress	
1: y y y y y n n													rest none	
2: y y y y y n n													rest none	
3: y y y y y n n													rest none	
4: y y y y y n n													rest none	
5: y y y y y n n													rest none	
6: y y y y y n n													rest none	

## 5.11. Configure AAR Analysis

For the AAR Analysis Table, create the dial string that will map calls to the Office-LinX via the route pattern created in **Section 5.10**. Enter the **change aar analysis <x>** command, where **x** is the starting digit. The dialed string created in the AAR Digit Analysis table should contain a map to the Office-LinX system extension, which is configured as x72036. During the configuration of the aar table, the Call Type field was set to **unku**.

change aar analysis 720							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 3		
Dialed	Total		Route	Call	Node	ANI		
String	Min	Max	Pattern	Type	Num	Reqd		
7202	5	5	92	unku		n		
7203	5	5	92	unku		n		

## 5.12. Configure TSAPI CTI Link

This section describes the CTI link configuration between Communication Manager and Application Enablement Services. 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. Set the **Type** field to **ADJ-IP** and assign a descriptive **Name** to the CTI link. Default values may be used in the remaining fields.

<b>add cti-link 4</b>	Page 1 of 3
CTI LINK	
CTI Link: 4	
Extension: 72000	
Type: ADJ-IP	
	COR: 1
Name: TSAPI	

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 **procr** which was configured in **Section 5.4**. 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	procr	8765		
CDR1		procr	0	pcr	5852
CDR2		procr	0	rdtt-1	9004

On **Page 4**, enter the hostname of the AES server for the **AE Services Server** field. The server name may be obtained by logging into the AES server using ssh and running the **uname -a** command. 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 6.1**.

<b>change ip-services</b>	Page 4 of 4			
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aes		y	idle
2:				
3:				
4:				
5:				
6:				

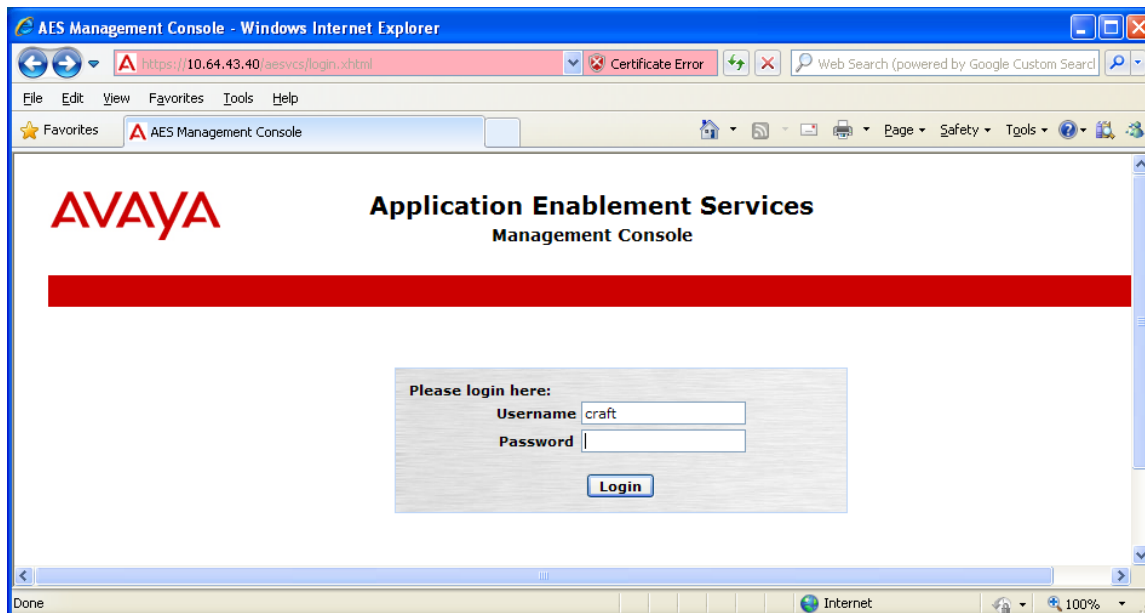
## 6. Configure Avaya Aura® Application Enablement Services

Application Enablement Services enable Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager. Application Enablement Services receives requests from CTI applications and forwards them to Communication Manager. Conversely, Application Enablement Services 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 Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, creating a CTI link for TSAPI, and a CTI user.

### 6.1. Configure Switch Connection

Launch a web browser, enter <https://<IP address of AES server>> in the URL, and log in with the appropriate credentials for accessing the Application Enablement Services Management Console page.



The Welcome to OAM screen is displayed next. Select **AE Services** from the left pane.

**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.

Verify that AES is licensed for the TSAPI service, as shown in the screen below.

**AE Services** Home | Help | Logout

AE Services

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

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	ONLINE	Running	NORMAL MODE	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 6.0

Click on **Communication Manager Interface**→ **Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Application Enablement Services server and Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.

Communication Manager Interface | Switch Connections Home | Help | Logout

Left Sidebar:

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

Switch Connections

S8300D Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
S8300D			

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

The next window that appears prompts for the Switch Password. Enter the same password that was administered on Communication Manager in **Section 5.12**. Default values may be used in the remaining fields. Click on **Apply**.

Communication Manager Interface | Switch Connections Home | Help | Logout

Left Sidebar:

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

Connection Details - S8300D

Switch Password: [Redacted]

Confirm Switch Password: [Redacted]

Msg Period: 30 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**.

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8300D	No	30	0

Enter the IP address of Procr used for Application Enablement Services connectivity listed in **Section 5.4**, and click on **Add Name or IP**.

Communication Manager Interface | Switch Connections Home | Help | Logout

Edit CLAN IPs - S8300D

Name or IP Address	Status



After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit H.323 Gatekeeper**.

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8300D	No	30	0

Enter the IP address of Procr used for Application Enablement Services connectivity listed in **Section 5.4**, and click on **Add Name or IP**.

Communication Manager Interface | Switch Connections Home | Help | Logout

Edit H.323 Gatekeeper - S8300D

Name or IP Address

## 6.2. Configure TSAPI CTI Link

Navigate to **AE Services → TSAPI → TSAPI Links** to configure the TSAPI CTI link. Click the **Add Link** button to start configuring the TSAPI link.

The screenshot shows the 'TSAPI Links' configuration page. On the left is a navigation tree with 'AE Services' expanded, showing 'CVLAN', 'DLG', 'DMCC', 'SMS', 'TSAPI' (expanded), 'Communication Manager Interface', 'Licensing', 'Maintenance', 'Networking', and 'Security'. Under 'TSAPI', 'TSAPI Links' is selected. The main content area is titled 'TSAPI Links' and contains a table with columns: '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 the switch connection using the drop-down menu. Select the switch connection configured in **Section 6.1**. Select the **Switch CTI Link Number** using the drop-down menu. The CTI link number should match with the number configured in the cti-link form in **Section 5.12**. Click **Apply Changes**.

The screenshot shows the 'Add TSAPI Links' configuration page. On the left is the same navigation tree as the previous screenshot. The main content area is titled 'Add TSAPI Links' and contains several form fields: 'Link' (value: 1), 'Switch Connection' (value: S8300D), 'Switch CTI Link Number' (value: 4), 'ASAI Link Version' (value: 4), and 'Security' (value: Both). Below these fields are two buttons: 'Apply Changes' and 'Cancel Changes'. The 'Apply Changes' button is highlighted with a red box.

The following screen shows the TSAPI CTI link configuration.

**AE Services | TSAPI | TSAPI Links**Home | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ TSAPI

▪ TSAPI Links

▪ TSAPI Properties

▶ TWS


▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
 1	S8300D	4	4	Both

Add Link

Edit Link

Delete Link

### 6.3. Configure CTI User

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**

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

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 for 'User craft' with login details. A red navigation bar contains 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'. On the left, a sidebar menu lists various services, with 'User Management' expanded to show 'User Admin' and 'Add User' selected. The main content area is titled 'Add User' and contains a form. A red box highlights the required fields: '\* User Id' (ESNA), '\* Common Name' (ESNA), '\* Surname' (Esna123&), '\* User Password' (masked), and '\* Confirm Password' (masked). Below these are optional fields: 'Admin Note', 'Avaya Role' (set to 'None'), 'Business Category', 'Car License', 'CM Home', and 'Css Home'. At the bottom, the 'CT User' field is set to 'Yes' via a dropdown menu, also highlighted by a red box.

Once the user is created, navigate to the **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: Tue Feb 21 13:33:44 2012 from 10.64.40.14  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-1-30-0

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

CTI Users

User ID	Common Name	Worktop Name	Device ID
ESNA	ESNA	NONE	NONE

EditList All

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message for 'User craft' with login details. A red breadcrumb trail shows the path: 'Security | Security Database | CTI Users | List All Users'. On the right, there are links for 'Home | Help | Logout'.

The left sidebar contains a tree view of the application's features, with 'Security' expanded to show 'Security Database', which in turn has 'CTI Users' selected, leading to 'List All Users'.

The main content area is titled 'Edit CTI User'. It contains a form with the following sections:

- User Profile:** Fields for 'User ID', 'Common Name', 'Worktop Name', and 'ESNA' (set to 'NONE'). The 'Unrestricted Access' checkbox is checked and highlighted with a red box.
- Call and Device Control:** A dropdown menu set to 'None'.
- Call and Device Monitoring:** Fields for 'Device Monitoring' (set to 'None'), 'Calls On A Device Monitoring' (set to 'None'), and 'Call Monitoring' (unchecked).
- Routing Control:** A dropdown menu set to 'None'.

At the bottom of the form, there are two buttons: 'Apply Changes' (highlighted with a red box) and 'Cancel Changes'.

*Note: Since the CTI user was given **Unrestricted Access** during the compliance test, the following section becomes optional.*

Navigate to the **Security** → **Security Database** → **Tlinks** page and verify the Tlink name. The following screen shows the Tlink used during the compliance test.

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 for user 'craft' with login details. A red navigation bar contains 'Security | Security Database | Tlinks' and links for 'Home | Help | Logout'. On the left, a sidebar menu shows 'Security' expanded, with 'Security Database' and 'Tlinks' highlighted. The main content area, titled 'Tlinks', shows a list of Tlink names: 'AVAYA#S8300D#CSTA#AES' (selected with a radio button) and 'AVAYA#S8300D#CSTA-S#AES'. A 'Delete Tlink' button is also present.

## 7. Configure Avaya Aura® Session Manager

Since the focus of the compliance test was to verify the integration between Communication Manager and Application Enablement Services, this section will not discuss the configuration of Session Manager.

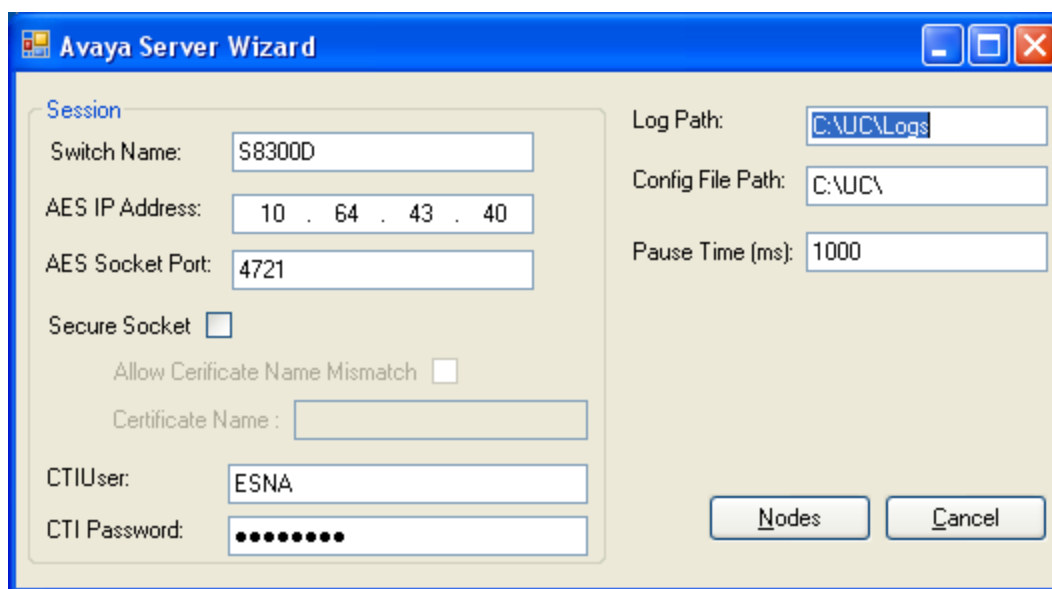
However, for configuring Session Manager, refer to [8]

## 8. Configure ESNA Office-LinX

ESNA installs, configures, and customizes the Office-LinX application for their customers. Thus, this section only describes the interface configuration so that the Office-LinX can talk to Application Enablement Services and Communication Manager. To configure ESNA Office-LinX, navigate to **Start → All Programs → Office LinX → AvayaServerWizard**. From the Avaya Server Wizard page, provide the following information:

- **Switch Name** – Enter the Switch Connection name created in **Section 6.1**.
- **AES IP Address** – Enter the IP address of the Application Enablement Services server.
- **AES Socket Port** – Enter the unsecured port
- **CTI User** – Enter the CTI user created in **Section 6.3**.
- **CTI Password** – Enter the password created in **Section 6.3**.

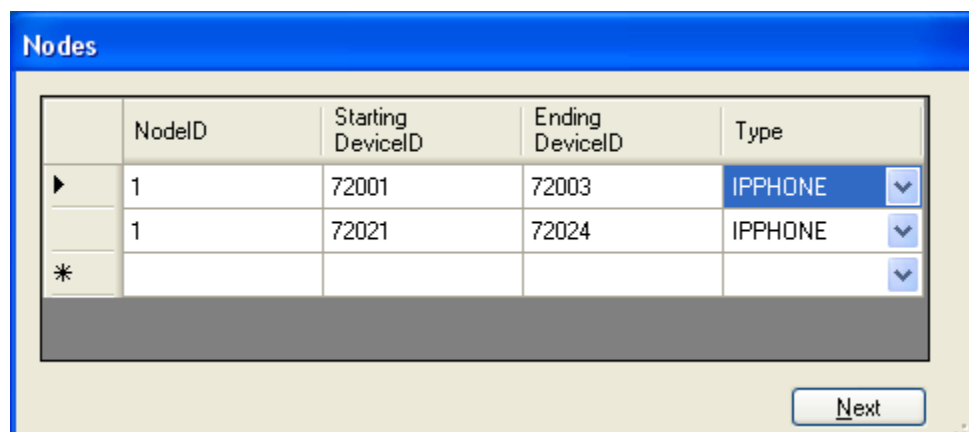
Click the **Nodes** button to configure the monitoring extension.



The Avaya Server Wizard dialog box contains the following fields and controls:

- Session** section:
  - Switch Name: S8300D
  - AES IP Address: 10 . 64 . 43 . 40
  - AES Socket Port: 4721
  - Secure Socket: ☐
  - Allow Certificate Name Mismatch: ☐
  - Certificate Name: (empty field)
  - CTI User: ESNA
  - CTI Password: (masked with dots)
- Log Path:** C:\UC\Log
- Config File Path:** C:\UC\
- Pause Time (ms):** 1000
- Buttons:** Nodes, Cancel

The following screen shows the monitoring extension



The Nodes dialog box displays a table with the following data:

	NodeID	Starting DeviceID	Ending DeviceID	Type
▶	1	72001	72003	IPPHONE ▼
	1	72021	72024	IPPHONE ▼
*				▼

Next

For configuring ESNA Office-LinX, refer to item [7] in **Section 10**.



## 9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and Application Enablement Services with ESNA Office-LinX.

### 9.1. Verify Avaya Aura® Application Enablement Services

From the Application Enablement Services Management Console web pages, select **Status** from the left pane and verify the state of the TSAPI Service is set to **NORMAL**.

**AVAYA**

**Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Fri Feb 3 15:13:19 2012 from 10.64.43.10  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-1-30-0

StatusHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Status and Control

▶ User Management

▶ Utilities

▶ Help

Services Summary

Service	State	Since	Cause
CVLAN Service	OFFLINE *	2012-01-29 17:10:35	NO_LICENSE_ACQUIRED
DLG Service	ONLINE	2012-01-29 17:10:32	NORMAL
DMCC Service	ONLINE	2012-01-29 17:10:36	NORMAL
TSAPI Service	ONLINE	2012-01-29 17:10:36	NORMAL

\* The state of the CVLAN and DLG services can either be ONLINE or OFFLINE. Also, the OFFLINE status would appear either until a link is administered or a valid license is acquired.

### 9.2. Verify Avaya Aura® Communication Manager

Verify the status of the administered CTI link by using the **status aesvcs cti-link** command. Verify the **Service State** is **established** for the CTI link number administered in **Section 5.12**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1		no		down	0	0
4	4	no	aes	established	75	75

## 10. Conclusion

These Application Notes describe the procedures required to configure ESNA Office-LinX to interoperate with Application Enablement Services and Communication Manager. ESNA Office-LinX successfully passed compliance testing.

## 11. Additional References

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

[1] *Administering Avaya Aura™ Communication Manager*, Release 6.0, June 2010, Issue 6.0, Document Number 03-300509

[2] *Administering Avaya Aura® Session Manager*, Release 6.1, November 2010, Issue 1.1, Document Number 03-603324

[3] *Administering Avaya Aura® System Manager*, Release 6.1, November 2010

The following documentation was provided by ESNA.

[4] *Configuring Avaya AES Server Properties*, February 2012, Document Version: 8.5 (1)

[5] *Office-LinX Server Configuration Guide*, March 2012, Document Version: 8.5 (3)

[6] *Office-LinX Server Installation Guide*, March 2012, Document Version: 8.5 (4)

[7] *Office-LinX Integration with Avaya Aura CM using SES and AES*, Sep 2011, Version 8.5(1)

[8] *Application Notes for Configuring ESNA Office-LinX with Avaya Aura® Session Manager and Avaya Aura® Communication Manager* - Issue 1.0

---

**©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).