



Avaya Solution & Interoperability Test Lab

Application Notes for the Amcom PC/PSAP with Avaya Aura™ Communication Manager and Avaya Aura™ Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura™ Communication Manager, Avaya Aura™ Application Enablement Services, Avaya IP and Digital Telephones, and Amcom PC/PSAP desktop applications.

Amcom PC/PSAP is a powerful Windows-based intelligent E911 workstation solution for a campus or municipality. Using the existing PBX telephone system as an “Automatic Number Identification (ANI)/Automatic Location Information (ALI) controller”, Amcom PC/PSAP eliminates the need for external proprietary switching solutions and is able to perform all necessary telephony functions from the call taker’s PC keyboard. Amcom PC/PSAP integrates with Amcom CTI Layer, which is a middleware between Amcom PC/PSAP and Avaya Aura™ Application Enablement Services, to control and monitor phone states.

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, Avaya IP and Digital Telephones, and Amcom PC/PSAP applications.

Amcom Communications PC/PSAP is a PC and LAN based system, which allows Communication Manager to be used in a PSAP (Public Safety Answering Position – a physical location where 911 emergency telephone calls are received and then routed to the proper emergency services by the security agent or “911 operator” at the PSAP). Campuses or municipalities can set up a public or private PSAP using Amcom PC/PSAP, which has the capabilities to extract ANI (Automatic Number Identification – phone number of the caller) from Emergency 911 trunks and retrieve corresponding ALI (Automatic Location Information – information about the call based on the ANI such as name, phone number, address, nearest cross street, etc.). Amcom PC/PSAP integrates with Amcom CTI Layer, which is a middleware between Amcom PC/PSAP and Application Enablement Services, to control and monitor phone states.

It is the Amcom CTI Layer service that actually uses the Application Enablement Services Device and Media Control Application Programming Interface (API) to share control of and monitor a physical telephone and receive the same terminal and first party call information received by the physical telephone. Amcom PC/PSAP in turn uses the Amcom CTI Layer service to control and monitor a physical telephone. The PC/PSAP applications regularly provide the Database server with call and lamp state information concerning the controlled telephones.

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 Amcom PC/PSAP, Application Enablement Services, and Communication Manager.

Amcom PC/PSAP allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). During compliance testing, calls were successfully placed to and from Avaya IP and Digital Telephones that were controlled and monitored by the Amcom PC/PSAP application. Basic telephone and call operations on Avaya IP and Digital telephones were tested using the Amcom desktop application.

1.2. Support

Technical support for the Amcom PC/PSAP solution can be obtained by contacting Amcom:

- URL – <https://secure5.inet7.com/amcomsoftware-com/Support/online.aspx>
- Phone – (888) 797-7487

2. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with an Application Enablement Services server and Avaya S8720 Media Servers with G650 Media Gateway. The PC/PSAP was located in a different VLAN. Endpoints include Avaya 9600 Series H.323 IP Telephones, Avaya 4625 H.323 IP Telephone, and an Avaya 6408D Digital Telephone. An Avaya S8300 Server with an Avaya G450 Media Gateway was included in the test to provide an inter-switch scenario.

Note: Basic administration of Application Enablement Services server is assumed. For details, see [2].

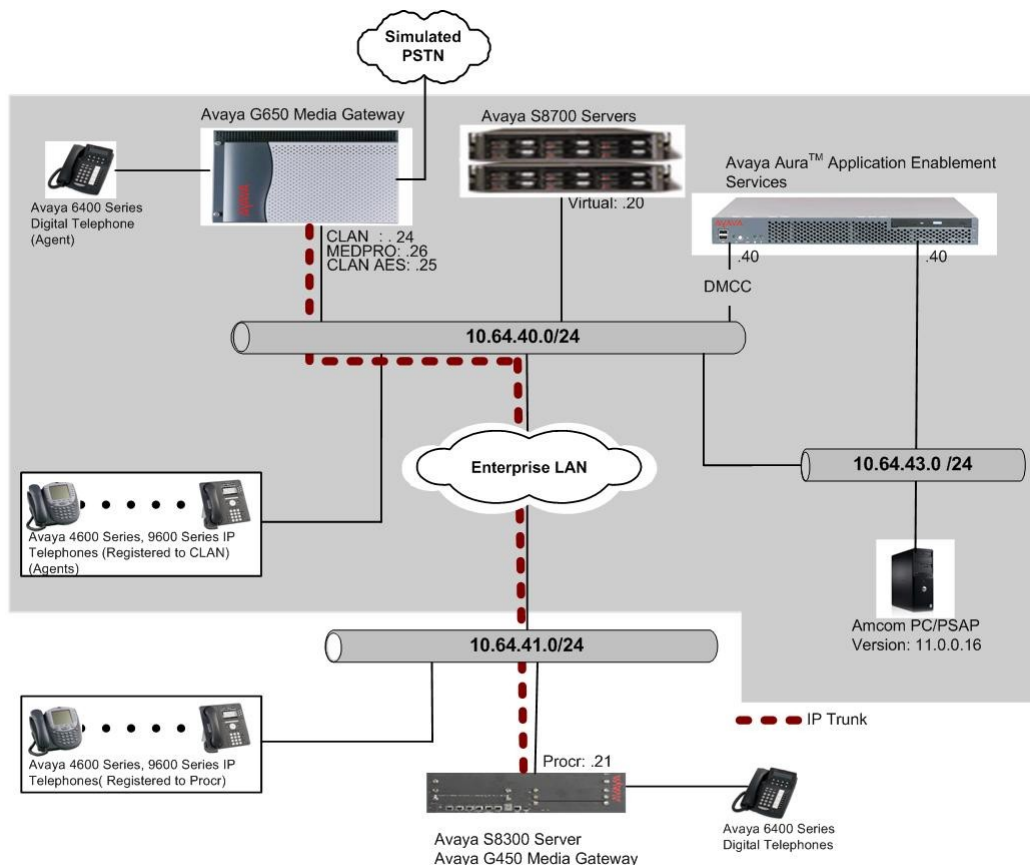


Figure 1: Sample Configuration.

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8720 Media Servers	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya G650 Media Gateway	
TN2312BP IP Server Interface	FW40
TN799DP C-LAN Interface	FW34
TN2302AP IP Media Processor	FW51
Avaya S8300C Media Server with Avaya G450 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 4625SW IP Telephone	2.5
Avaya 9600 Series IP Telephones	
9620 (H.323)	3.1
9630 (H.323)	3.1
9650 (H.323)	3.1
Avaya 6424D+ Digital Telephone	-
Amcom PC/PSAP	11.0.0.16

4. Configure Avaya Communication Manager

This section describes the procedure for administering the transport link to the AES server, setting up a Feature Access Codes. Abbreviated dialing, and controlled telephones.

Log into the System Access Terminal (SAT) to verify that Avaya Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Verify that the **ASAI Link Core Capabilities**, and **Computer Telephony Adjunct Links** customer option is set to “y” on (Page 3) and there are sufficient **IP_API_A** licenses (Page 10). If not, then contact the Avaya sales team or business partner for a proper license file.

4.1. Configure IP Services for AES

Notes: The section 4.1 was performed at the Avaya S8720 Media Server with an Avaya G650 Media Gateway side.

Enter the **change node-names ip** command. In the compliance-tested configuration, the CLAN IP address was used for registering H.323 endpoints, and the CLAN-AES IP address was used for connectivity to Application Enablement Services.

change node-names ip				Page 1 of 1		
		IP NODE NAMES				
Name	IP Address	Name	IP Address			
CDR_buffer	192.45 .80 .250		. . .			
CLAN	10.64.40.24		. . .			
CLAN-AES	10.64.40.25		. . .			
G350	10.64.42.21		. . .			
MEDPRO	10.64.40.26		. . .			
S8300	10.64.41.21		. . .			
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 used 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	CLAN-AES	8765			

On **Page 4**, 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 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 Application Enablement Services server in **Section 5.2**.

change ip-services				Page 4 of 4
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	server1	xxxxxxxxxxxxxxxxxx	y	idle
2:				
3:				
4:				
5:				

4.2. Configure feature-access-codes

Notes: The sections, 4.2, 4.3, 4.5, and 4.6, were performed at the Avaya S8300 Media Server with an Avaya G450 Media Gateway side.

Enter the **change feature-access-codes** command. On **Page 1** of the FEATURE ACCESS CODE (FAC) form, verify the Auto Route Selection (ARS) – Access Code 1 field is set to **9**.

change feature-access-codes			Page 1 of 7
FEATURE ACCESS CODE (FAC)			
Abbreviated Dialing List1 Access Code:			
Abbreviated Dialing List2 Access Code:			
Abbreviated Dialing List3 Access Code:			
Abbreviated Dial - Prgm Group List Access Code:			
Announcement Access Code:			
Answer Back Access Code:			
Auto Alternate Routing (AAR) Access Code:			
Auto Route Selection (ARS) – Access Code 1: 9		Access Code 2:	
Automatic Callback Activation:		Deactivation:	
Call Forwarding Activation Busy/DA:		All:	
		Deactivation:	

4.3. Configure Dialplan

Enter the **change dialplan analysis** command. Create a single digit dial string with 9 and associate it with **Feature Access Code (fac)**.

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
						Percent Full: 1		
Dialed	Total	Call	Dialed	Total	Call	Dialed	Total	Call
String	Length	Type	String	Length	Type	String	Length	Type
0	1	attd	4	5	ext			
10	4	dac	5	5	ext			
11	3	dac	6	5	ext			
12	3	fac	7	5	ext			
126	6	aar	8	1	fac			
13	3	fac	9	1	fac			
14	3	fac	*	3	fac			
15	3	fac	#	3	fac			

4.4. Configure Hunt Group

Notes: The section 4.4 was performed at the Avaya S8720 Media Server with an Avaya G650 Media Gateway side.

Enter the **add hunt-group n** command, where **n** is an unused hunt group number. On **Page 1** of the HUNT GROUP form, assign a descriptive Group Name and Group Extension valid in the provisioned dial plan at the S8720 Media Server with a G650 Media Gateway side.

```
add hunt-group 51                                     Page 1 of 60

                                HUNT GROUP

      Group Number: 51                                ACD? n
      Group Name: 911-hunt                            Queue? n
      Group Extension: 22999                          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 3**, add the 911 member extensions, which will be forwarded when a caller dials 911.

```
add hunt-group 51                                     Page 3 of 60

                                HUNT GROUP

      Group Number: 51      Group Extension: 22999      Group Type: ucd-mia
      Member Range Allowed: 1 - 1500      Administered Members (min/max): 1 /3
                                           Total Administered Members: 3

GROUP MEMBER ASSIGNMENTS

      Ext      Name (24 characters)      Ext      Name (24 characters)
      1: 22001      14:
      2: 22002      15:
      3: 22003      16:
      4:            17:
      5:            18:
```

4.5. Configure Auto Route Selection (ARS)

Enter the **change ars analysis 11** command. When a caller dials 911, the first digit (9) indicates that it is an ARS call. Therefore, the next two digits (11) are utilized in the ARS table.

```
change ars analysis 11                                     Page 1 of 2

                                ARS DIGIT ANALYSIS TABLE
                                Location: all              Percent Full: 1

      Dialed      Total      Route      Call      Node      ANI
      String      Min      Max      Pattern      Type      Num      Reqd
      11          2        2        51        emer        n
      120         11       11       deny       fnpa        n
      1200        11       11       deny       fnpa        n
      121         11       11       deny       fnpa        n
```

4.6. Configure Route Pattern

Enter the **change route-pattern r** command, where r is a route-pattern number. In the following route-pattern, two digits (11) are removed and replace it with 22999 (911 hunt group extension). The extension, 22999, will be sent to the trunk group 51.

display route-pattern 51															Page 1 of 3			
Pattern Number: 51 Pattern Name: temp-911																		
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:	51	0				2	22999		n	user								
2:									n	user								
3:									n	user								
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR																		
0	1	2	3	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			

4.7. Configure Feature Access Codes (FAC)

Notes: The section 4.7 to 4.9 was performed at the Avaya S8720 Media Server with an Avaya G650 Media Gateway side.

Enter the **display feature-access-codes** command. On **Page 5** of the FEATURE ACCESS CODE (FAC) form, configure and enable the following access codes:

- After Call Work Access Code
- Auto-In Access Code
- Aux Work Access Code
- Login Access Code
- Logout Access Code

display feature-access-codes

Page 5 of 9

FEATURE ACCESS CODE (FAC)

Automatic Call Distribution Features

After Call Work Access Code: 120

Assist Access Code: 121

Auto-In Access Code: 122

Aux Work Access Code: 123

Login Access Code: 124

Logout Access Code: 125

Manual-in Access Code: 126

Service Observing Listen Only Access Code: 127

Service Observing Listen/Talk Access Code: 128

Service Observing No Talk Access Code:

Add Agent Skill Access Code: 130

Remove Agent Skill Access Code: 131

Remote Logout of Agent Access Code: 132

4.8. Configure Abbreviated Dialing

Enter the **add abbreviated-dialing group g** command, where **g** is the number of an available abbreviated dialing group. In the **DIAL CODE** list, enter the Feature Access Codes for ACD Login and Logout from **Section 4.7**.

add abbreviated-dialing group 1		Page	1 of	1
ABBREVIATED DIALING LIST				
Group List: 1	Group Name: Call Center			
Size (multiple of 5): 5	Program Ext:	Privileged? n		
DIAL CODE				
11: 124				
12: 125				
13:				

4.9. Configure Controlled Telephones

Enter the **change station r** command, where **r** is the extension of a registered, physical Avaya IP or Digital telephone. On **Page 1** of the STATION form, enter a phone Type, descriptive name, Security Code and set IP SoftPhone field to **y** to allow the physical station to be controlled by a softphone such as the CTI Layer application.

add station 22001		Page	1 of	5
STATION				
Extension: 22001	Lock Messages? n	BCC: 0		
Type: 4625	Security Code: *	TN: 1		
Port: S00416	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:		
Speakerphone: 2-way		Personalized Ringing Pattern: 1		
Display Language: english		Message Lamp Ext: 22001		
Survivable GK Node Name:		Mute Button Enabled? y		
Survivable COR: internal		Expansion Module? n		
Survivable Trunk Dest? y		Media Complex Ext:		
		IP SoftPhone? y		
IP Video Softphone? n				

On **Page 4** of the station form, for **ABBREVIATED DIALING List 1**, enter the abbreviated dialing group configured in **Section 4.8**. On **Pages 4** and **5** of the station forms, configure the following **BUTTON ASSIGNMENTS** in addition to the call-appr (call appearance) buttons:

- aux-work
- abrv-dial – configure two of these buttons, one for Login and one for Logout, along with the Dial Codes from Abbreviated Dialing **List1** for ACD Login and Logout, respectively.
- after-call
- auto-in (On Page 5)
- release (On Page 5)

add station 22001		Page 4 of 5	
STATION			
SITE DATA			
Room:		Headset?	n
Jack:		Speaker?	n
Cable:		Mounting:	d
Floor:		Cord Length:	0
Building:		Set Color:	
ABBREVIATED DIALING			
List1:	personal 1	List2:	group 1
		List3:	
BUTTON ASSIGNMENTS			
1: call-appr		5: aux-work	RC: Grp:
2: call-appr		6: abrv-dial	List: 2 DC: 11
3: brdg-appr B:1 E:22101		7: abrv-dial	List: 2 DC: 12
4: brdg-appr B:2 E:22101		8: after-call	Grp:

add station 22001		Page 5 of 5	
STATION			
FEATURE BUTTON ASSIGNMENTS			
9: auto-in		Grp:	
10: release			

Repeat the instructions provided in this section for each physical station that is to be controlled / monitored by an Amcom CTI Layer.

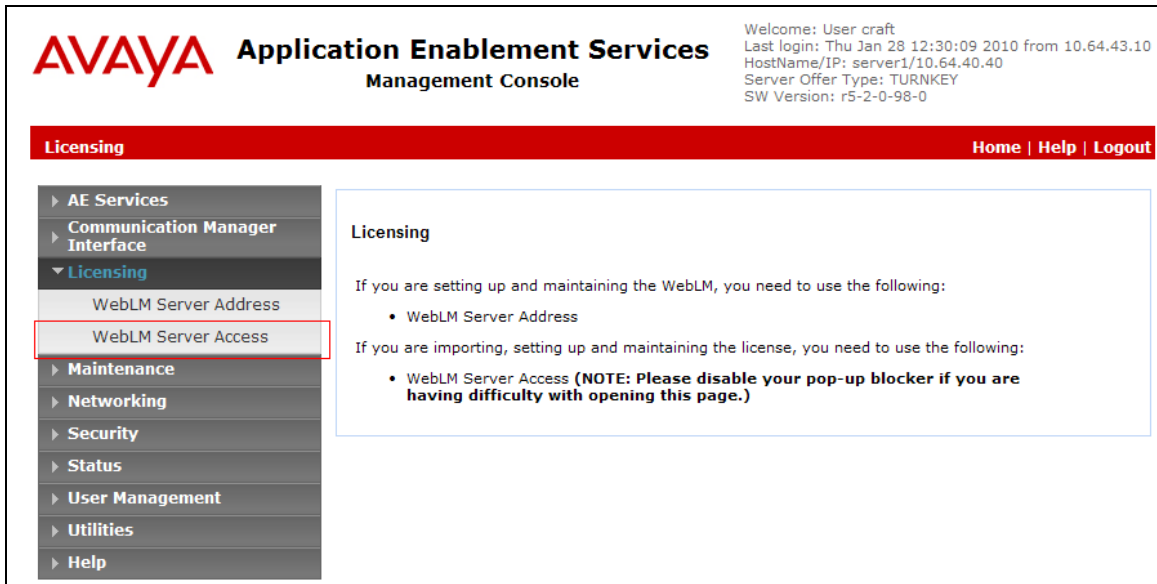
5. Configure Avaya Application Enablement Services

The Avaya Application Enablement Services server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager.

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, a CTI user, a CMAPI port.

5.1. Device and Media Control API Station Licenses

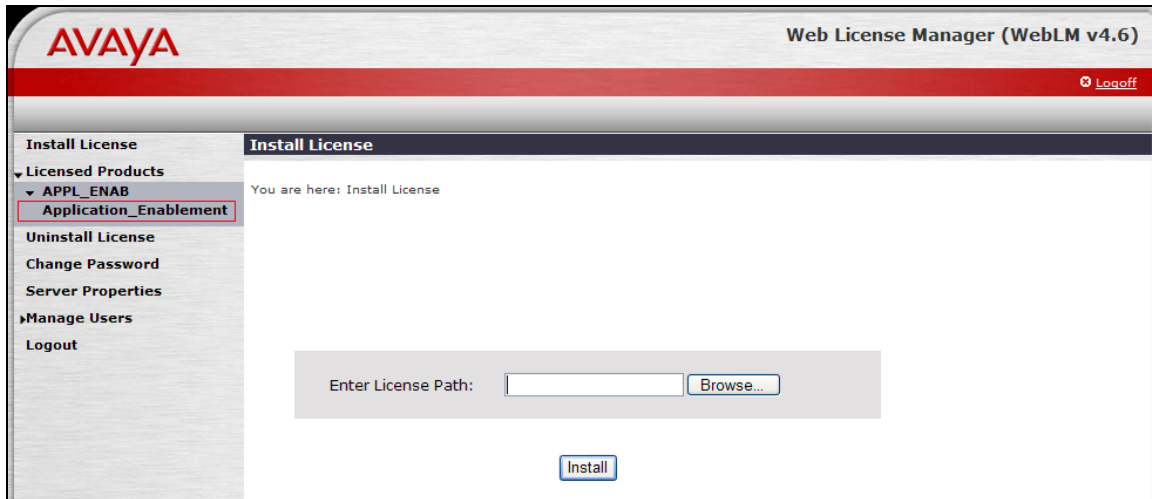
The Amcom CTI Service instances appear as “virtual” stations/softphones to Communication Manager. Each of these virtual stations, hereafter called Device and Media Control API station, requires a license. Note that this is separate and independent of Avaya IP Softphone licenses, which are required for Avaya IP Softphones but not required for Device and Media Control API stations. To check and verify that there are sufficient DMCC licenses, log in to <https://<IP address of the Application Enablement Services server>/index.jsp>, and enter appropriate login credentials to access the Application Enablement Services Management Console page. Select the **Licensing → WebLM Server Access** link from the left pane of the window.



Provide appropriate login credentials to access the Web License Manager page.



On the Install License page, select **License Products** → **Application_Enablement** link from the left pane of the window.



On the Licensed Features page, verify that there are sufficient DMCC licenses.

5.2. Configure Switch Connection

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

Application Enablement Services

Management Console

Please login here:

Username

Password

Click on **Communication Manager Interface → 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 Application Enablement Services 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

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

The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Avaya Communication Manager in **Section 4.1**. 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
☐

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

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

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

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.

Note: Avaya recommends using a CLAN board for phone registration, and another CLAN board for H.323 Gatekeeper.

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

Edit H.323 Gatekeeper - S8720G650

10.32.8.25 Add Name or IP

Name or IP Address

Delete IP

5.3. Configure the CTI Users

Navigate to **User Management** → **User Admin** → **Add User** link from the left pane of the window. 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 CTI Layer 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: Thu Jan 28 16:35:23 2010 from 10.64.43.10', 'HostName/IP: server1/10.64.40.40', 'Server Offer Type: TURNKEY', and 'SW Version: r5-2-0-98-0'. A red navigation bar contains 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'.

The left sidebar shows a tree view with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Add User (highlighted), Change User Password, List All Users, Modify Default Users, Search Users, Utilities, and Help.

The main content area is titled 'Add User'. It includes a note: 'Fields marked with * can not be empty.' Below this, a red box highlights the required fields: * User Id (Amcom), * Common Name (Amcom), * Surname (Amcom1238), * User Password (masked with dots), and * Confirm Password (masked with dots). Other fields include Admin Note, Avaya Role (set to None), Business Category, Car License, CM Home, Cms Home, CT User (set to Yes), Department Number, Display Name, and Employee Number.

Once the user is created, navigate to the **Security** → **Security Database** → **CTI Users** → **List All Users** link from the left pane of the window. 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: Thu Jan 28 16:35:23 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Security | Security Database | CTI Users | List All Users

Home | 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"/> Amcom	Amcom	NONE	NONE
<input type="radio"/> Nexidia	Nexidia	NONE	NONE
<input type="radio"/> newfound	newfound	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: Thu Jan 28 16:35:23 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
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 ID

Common Name

Worktop Name

Amcom

Amcom

NONE ▼

Unrestricted Access

☒

Call Origination and Termination / Device Status

None ▼

Call and Device Monitoring:

Device

Call / Device

Call

None ▼

None ▼

☐

Routing Control:

Allow Routing on Listed Devices

None ▼

Apply Changes

Cancel Changes

5.4. Configure the CTI Port

Navigate to the **Networking → Ports** link, from the left pane of the window, 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 Management Console

Welcome: User craft
Last login: Fri Feb 19 16:19:59 2010 from 10.64.43.10
HostName/IP: server1/10.64.40.40
Server Offer Type: TURNKEY
SW Version: r5-2-0-98-0

Networking | Ports Home | Help | Logout

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 Amcom PC/PSAP

Amcom installs, configures, and customizes the PC/PSAP applications for their end customers.

7. General Test Approach and Test Results

The general approach was to exercise basic telephone and call operations on Avaya IP and Digital telephones using the aforementioned Amcom desktop application. The main objectives were to verify that:

- The user may successfully use PC/PSAP to perform off-hook, on-hook, dial, answer, hold, retrieve, transfer, conference, and release operations on the physical telephone.
- The agent user may successfully use PC/PSAP to log into and out of an ACD, and move between agent work modes.
- Manual operations performed on the physical telephone are correctly reflected in the PC/PSAP GUI.

- PC/PSAP and manual telephone operations may be used interchangeably; for example, go off-hook using PC/PSAP and manually dial digits.
- Display and call information on the physical telephone is accurately reflected in the PC/PSAP GUI.
- Call states are consistent between PC/PSAP and the physical telephone.

The objectives of **Section 7** were verified. For serviceability testing, the Amcom CTI Service was able to regain control of the physical telephone after restarts of the Amcom CTI Service, the computer on which it runs, and the Application Enablement Services server. In addition, after Amcom CTI Service lost network connectivity to the Application Enablement Services server, it was able to recover the existing session to the Application Enablement Services server when network connectivity was restored before the session expired, and establish a new session when network connectivity was restored after the previous session expired.

8. Verification Steps

The following steps may be used to verify the configuration:

- From the Amcom client computers, ping IP interfaces, in particular the Application Enablement Services server, and verify connectivity.
- For the physical IP telephones, verify that the physical telephones are registered by using the **list registered-ip-stations** command on the SAT. For the physical Digital telephones, verify that the telephones are attached to the correct ports.
- Go off-hook and on-hook on the controlled telephones manually and using PC/PSAP, and verify consistency.
- Place and answer calls from the controlled telephones manually and using PC/PSAP, and verify consistency.

9. Conclusion

These Application Notes described a compliance-tested configuration comprised of Avaya Aura[™] Communication Manager Release 5.2.1, Avaya Aura[™] Application Enablement Services Release 5.2, Avaya IP and Digital Telephones, and the Amcom PC/PSAP application. Amcom PC/PSAP allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). During compliance testing, calls were successfully placed to and from Avaya IP and Digital Telephones that were controlled and monitored by the Amcom PC/PSAP application.

10. Additional References

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

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

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

Product information for Amcom products may be found at <http://www.amcomsoft.com/products.cfm>.

©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.