



Avaya Solution & Interoperability Test Lab

Application Notes for Amcom CTI Layer 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 CTI Layer desktop applications.

Amcom CTI Layer is a middleware that interfaces with Avaya Aura® Communication Manager via Avaya Aura® Application Enablement Services for the following Amcom PC console applications:

- Amcom SmartConsole
- Amcom pc/PSAP
- Amcom IntelliDesk
- Amcom AnswerPro
- Amcom Medcall
- Amcom XpressDesk

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 CTI Layer applications.

Amcom CTI Layer is a software service that provides a mapping of DMCC commands and functions to a telephony API compatible with all Amcom PC Console products. Amcom PC Consoles are software applications, specialized for different vertical markets that allow a user to monitor and control a physical telephone and view call and telephone display information through a graphical user interface (GUI). The CTI Layer controls a physical telephone using first party call control, specifically the Device, Media and Control Services of Application Enablement Services.

The compliance testing will focus on the integration between Amcom CTI Layer service, Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and Avaya IP and digital telephones. Amcom provided the CTI Layer application with a special configuration file designed to fully test the CTI Layer functionality. Telephone operations such as off-hook, on-hook, dialing, answering, hold, transfer, conference, etc. will be performed from the physical telephones and from the CTI Layer application. In addition, telephone displays and call states on the physical telephones and in the CTI Layer will be verified for consistency.

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

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the compliance test was primarily on verifying the interoperability between Amcom CTI Layer, Application Enablement Services, and Communication Manager.

2.2. Support

Technical support for the Amcom CTI Layer solution can be obtained by contacting Amcom:

- URL – <http://amcomsoftware.com>
- Phone – (888) 797-7487

3. 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 an Avaya S8300D Server running Communication Manager software with an Avaya G450 Media Gateway. The CTI Layer was located in a different VLAN. Endpoints include Avaya 9600 Series H.323 IP Telephones and an Avaya 6408D Digital Telephone. Avaya S8720 Servers with an Avaya G650 Media Gateway was included in the test to provide an inter-switch scenario.

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

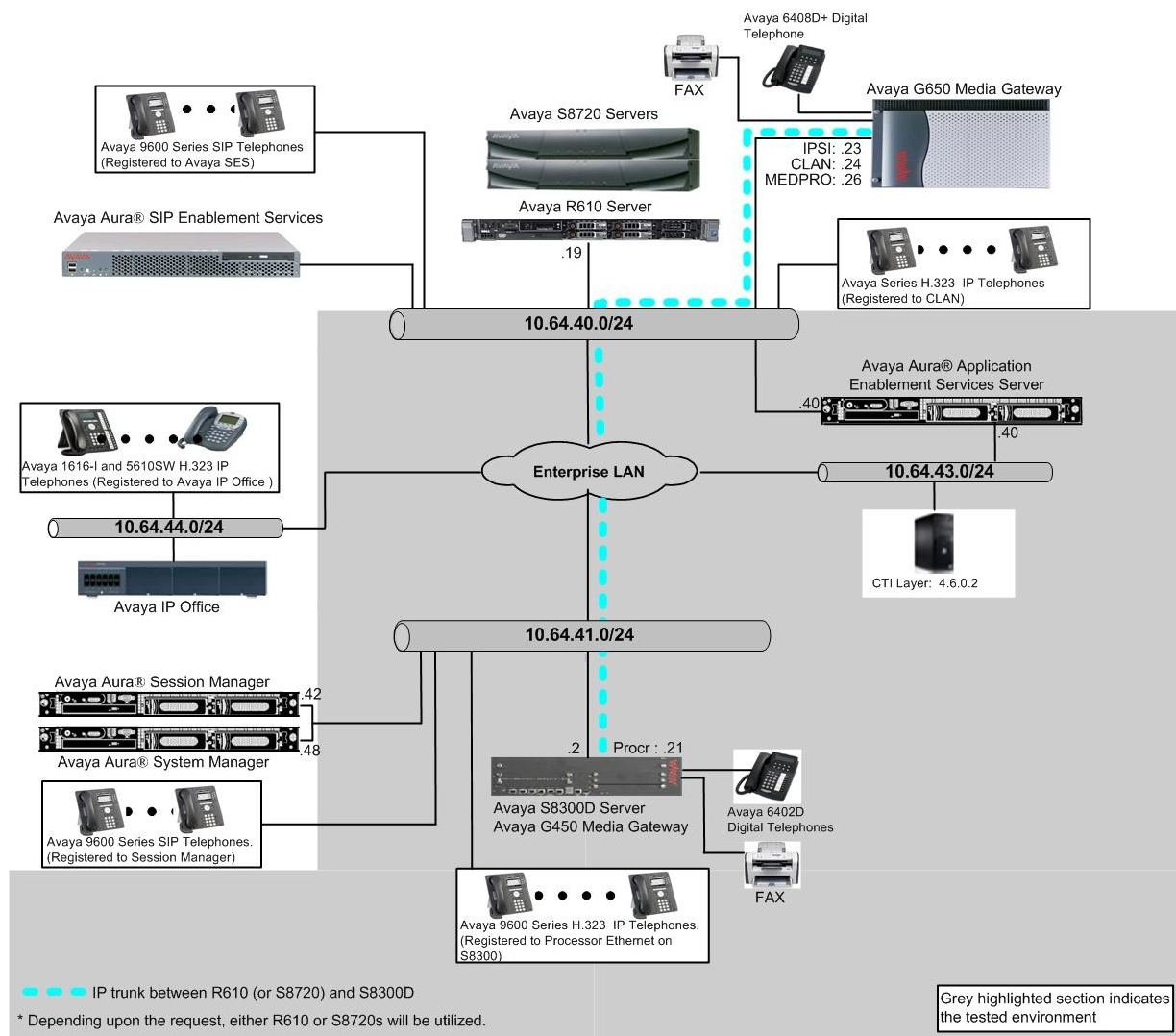


Figure 1: Amcom CTI Layer Test Configuration.

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® Application Enablement Services Server		6.1.1 (r6-1-1-30-0)
Avaya S8720 Servers with Avaya G650 Media Gateway (<i>used for inter-switch test scenarios</i>)		Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya 9600 Series IP Telephones		
	9620 (H.323)	3.1
	9630 (H.323)	3.1
	9650 (H.323)	3.1
Avaya 6408D+ Digital Telephone		-
Amcom CTI Layer		4.6.0.2

5. Configure Avaya Aura® Communication Manager

This section describes the procedures for configuring IP Services, Feature Access Codes, Abbreviated Dialing, and controlled telephones.

5.1. Configure IP Services

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

change node-names ip		Page 1 of 1
IP NODE NAMES		
Name	IP Address	
aes	10.64.43.40	
procr	10.64.41.21	
procr6	::	

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 **procr** 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	Enabled	Local	Local	Remote	Remote		
Type		Node	Port	Node	Port		
AESVCS	y	procr	8765				
CDR1		procr	0	rdtt	9002		

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 6.2**.

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

5.2. Configure Feature Access Codes (FAC)

Enter the **display feature-access-codes** command. On **Page 5** of the **feature-access-codes** 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 11
                                                                FEATURE ACCESS CODE (FAC)

                                                                Call Center Features

AGENT WORK MODES
    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
    Service Observing Listen Only Access Code: 127
    Service Observing Listen/Talk Access Code: 128
    Service Observing No Talk Access Code: 129
    Service Observing Next Call Listen Only Access Code:
```

5.3. Configure Abbreviated Dialing

Enter **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 5.2**.

```
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:
```

5.4. 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 Amcom CTI Layer application.

change station 72001		Page 1 of 5
STATION		
Extension: 72001	Lock Messages? n	BCC: 0
Type: 9620	Security Code: *	TN: 1
Port: S00002	Coverage Path 1:	COR: 1
Name: Console-72001	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 72001	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

On **Page 4** of the station form, for ABBREVIATED DIALING List2 enter the abbreviated dialing group configured in **Section 5.2**. On **Pages 4** and **5** of the station forms, configure the following **BUTTON ASSIGNMENTS** in addition to the call-appr (call appearance) buttons:

- auto-in (on Page 4)
- aux-work (on Page 4)
- abrv-dial – configure two of these buttons, one for Login and one for Logout, along with the Dial Codes from Abbreviated Dialing List2 for ACD Login and Logout, respectively (on Page 5)
- release (On Page 5)

change station 72001		Page 4 of 5
STATION		
SITE DATA		
Room: 1001	Headset? n	
Jack:	Speaker? n	
Cable:	Mounting: d	
Floor:	Cord Length: 0	
Building: Store1	Set Color:	
ABBREVIATED DIALING		
List1: personal 1	List2: group 1	List3:
BUTTON ASSIGNMENTS		
1: call-appr	4: brdg-appr B:2 E:72002	
2: call-appr	5: auto-in Grp:	
3: brdg-appr B:1 E:72002	6: aux-work RC: Grp:	

change station 72001

Page 5 of 5

STATION

BUTTON ASSIGNMENTS

7: abrv-dial List: 2 DC: 01

HL? n 10: ec500 Timer? n

8: abrv-dial List: 2 DC: 02

HL? n 11: extnd-call

9: release

12:

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

6. Configure Avaya Aura® Application Enablement Services

The 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, and a DMCC port.

6.1. Device and Media Call Control API Station Licenses

The Amcom CTI Layer Service instances appear as “virtual” stations/softphones to Communication Manager. Each of these virtual stations, hereafter called Device and Media Call 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 Call 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.

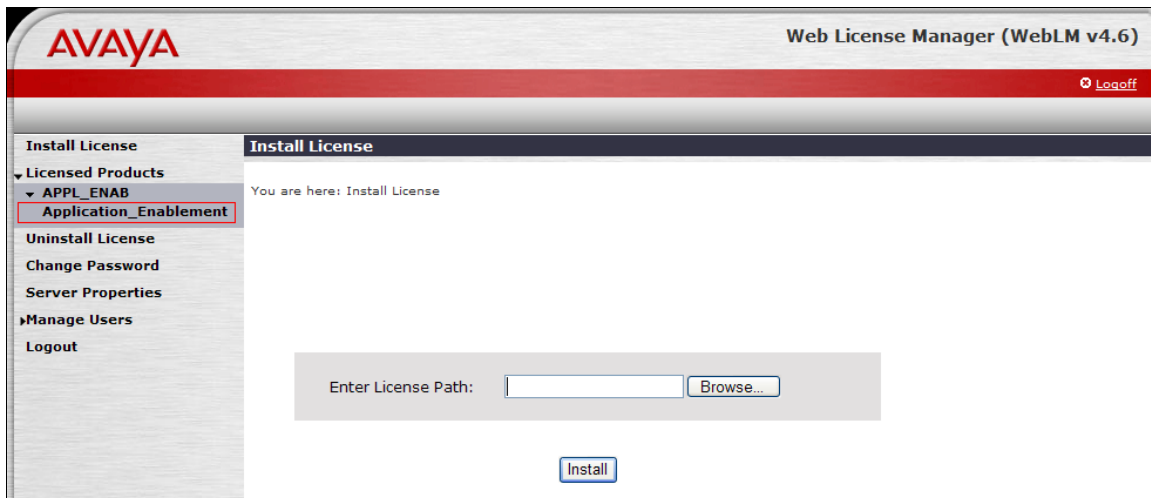
The screenshot displays the Avaya Application Enablement Services Management Console. At the top, the Avaya logo is on the left, and the title "Application Enablement Services Management Console" is in the center. On the right, a welcome message reads: "Welcome: User craft", "Last login: Thu Dec 1 14:28:33 2011 from 10.64.43.10", "HostName/IP: aes.avaya.com/10.64.43.40", "Server Offer Type: VIRTUAL_APPLIANCE", and "SW Version: r6-1-1-30-0". Below the header is a red navigation bar with "Licensing" on the left and "Home | Help | Logout" on the right. A left-hand menu contains links to "AE Services", "Communication Manager Interface", "Licensing" (expanded), "WebLM Server Address", "Reserved Licenses", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The "WebLM Server Access" link under "Licensing" is highlighted with a red box. The main content area, titled "Licensing", contains the following text: "If you are setting up and maintaining the WebLM, you need to use the following:" followed by a bullet point "WebLM Server Address"; "If you are importing, setting up and maintaining the license, you need to use the following:" followed by a bullet point "WebLM Server Access"; and "If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:" followed by a bullet point "Reserved Licenses". A red note at the bottom states: "NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page".

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



The image shows the login page of the Avaya Web License Manager (WebLM v4.6). The page has a red header with the Avaya logo and the text "Web License Manager (WebLM v4.6)". Below the header, the word "Login" is centered. There are two input fields: "User Name:" and "Password:". A gray button with a right-pointing arrow is located below the password field.

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



The image shows the "Install License" page of the Avaya Web License Manager (WebLM v4.6). The page has a red header with the Avaya logo and the text "Web License Manager (WebLM v4.6)". A "Logout" link is in the top right corner. On the left, there is a navigation pane with the following items: "Install License", "Licensed Products" (expanded), "APPL_ENAB" (expanded), "Application_Enablement" (highlighted with a red box), "Uninstall License", "Change Password", "Server Properties", "Manage Users", and "Logout". The main content area has a sub-header "Install License" and a breadcrumb "You are here: Install License". Below this, there is a form with the label "Enter License Path:" followed by a text input field and a "Browse..." button. At the bottom of the form is an "Install" button.

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

AVAYA
Web License Manager (WebLM v4.6)

[Logoff](#)

Install License

Licensed Products

APPL_ENAB

Application Enablement

Uninstall License

Change Password

Server Properties

Manage Users

Logout

Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License File)

You are here: Licensed products > Application Enablement (CTI)

License installed on: Jun 2, 2011 9:55:08 AM MDT

[View Peak Usage](#)

Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;d1380g3;d1385g1;d1385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; OSCP_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	0
DLG (VALUE_AES_DLG)	permanent	16	1
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	1000	8
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	3	0

6.2. 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.

The screenshot shows the login page of the Application Enablement Services Management Console. At the top, the title "Application Enablement Services Management Console" is displayed in bold black text. Below the title is a red horizontal bar. In the center, there is a light gray box with a blue border containing the login form. The form includes the text "Please login here:" followed by two input fields labeled "Username" and "Password". Below these fields is a "Login" button.

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

The screenshot shows the home page of the Application Enablement Services Management Console. The top header features the Avaya logo and the title "Application Enablement Services Management Console". To the right of the title, there is a welcome message: "Welcome: User craft", "Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10", "HostName/IP: aes.avaya.com/10.64.43.40", "Server Offer Type: VIRTUAL_APPLIANCE", and "SW Version: r6-1-1-30-0". Below the header is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. On the left side, there is a dark gray sidebar with a list of menu items: "AE Services", "Communication Manager Interface" (highlighted with a red border), "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area on the right has a "Welcome to OAM" heading and a paragraph explaining the OAM Web's purpose. Below this is a bulleted list of administrative domains and their functions: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. At the bottom of the main content area, there is a note about administrative domains.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 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

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 infomations.
- 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: Sat Dec 3 16:26:56 2011 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

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

S8300D Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
G650	No	30	0

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 in Communication Manager in **Section 5.1**. Click on **Apply**.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 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

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 - S8300D

Switch Password
Confirm Switch Password

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 the **Edit PE/CLAN IPs** button.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 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

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
<input type="radio"/> G650	No	30	0
<input checked="" type="radio"/> S8300D	Yes	30	1

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

On the **Edit Processor Ethernet IP – S8300D** page, enter the procr IP address which will be used for the DMCC service. Click on **Add/Edit Name or IP**.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Mon Dec 12 10:51:57 2011 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

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 Processor Ethernet IP - S8300D

[Add/Edit Name or IP](#)

Name or IP Address	Status
--------------------	--------

[Back](#)

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.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 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

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

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input type="radio"/> G650	No	30	0
<input checked="" type="radio"/> S8300D	Yes	30	1

On the **Edit H.323 Gatekeeper – S8300D** page, enter the procr IP address which will be used for the DMCC service. Click on **Add Name or IP**.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 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

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

Edit H.323 Gatekeeper - S8300D

Name or IP Address


6.3. 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 Amcom CTI Layer Configuration page in **Section 7**.

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.


Application Enablement Services
Management Console

Welcome: User craft
 Last login: Sat Dec 3 16:26:56 2011 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

User Management | User Admin | Add User
 Home | Help | Logout

> AE Services
 > Communication Manager Interface
 > Licensing
 > Maintenance
 > Networking
 > Security
 > Status
 > User Management
 > Service Admin
 > User Admin
 ▪ Add User
 ▪ Change User Password
 ▪ List All Users
 ▪ Modify Default Users
 ▪ Search Users
 > Utilities
 > Help

Add User

Fields marked with * can not be empty.

* User Id

Amcom

* Common Name

Amcom

* Surname

Amcom123&

* User Password

••••••••

* Confirm Password

••••••••

Admin Note

Avaya Role

None

Business Category

Car License

CM Home

Css Home

CT User


Yes

Department Number

Display Name

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.


Application Enablement Services
Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 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

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

CTI Users

User ID	Common Name	Worktop Name	Device ID
amcom	Amcom123&	NONE	NONE

Edit
List All

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

AVAYA **Application Enablement Services**
Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 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

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

Edit CTI User

User Profile:

User IDamcom

Common NameAmcom1238

Worktop NameNONE

Unrestricted Access☒

Call and Device Control:

Call Origination/Termination and Device StatusNone

Call and Device Monitoring:

Device MonitoringNone

Calls On A Device MonitoringNone

Call Monitoring☐

Routing Control:

Allow Routing on Listed DevicesNone

Apply Changes

Cancel Changes

6.4. Configure the DMCC 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: Sat Dec 3 16:26:56 2011 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

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999Enabled Disabled

Encrypted TCP Port9998Enabled Disabled

DLG Port

TCP Port5678

TSAPI Ports

TSAPI Service Port450Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721Enabled Disabled

Encrypted Port4722Enabled Disabled

TR/87 Port4723Enabled Disabled

7. Configure Amcom CTI Layer

Amcom installs, configures, and customizes the CTI Layer applications for their end customers. The Amcom Console applications integrate with the Amcom CTI Layer, which is a middleware that interfaces with Communication Manager via Application Enablement Services, to control and monitor the phone states. Thus, only the Amcom CTI layer will be discussed in these Application Notes.

The following shows the **Amcom AES CTI Services Setup** page. Provide the following information:

Under DMCC Settings

- **AES Server** – Enter the IP address of the Application Enablement Services server.
- **Switch IP Address** – Enter the procr or CLAN IP address of Avaya S8300D server.
- **Port** – Enter the DMCC port (4721) configured in **Section 6.4**.
- **User** – Enter the user name created for Amcom CTI Layer in **Section 6.3**.
- **Password** – Enter the password created for Amcom CTI Layer in **Section 6.3**.

Under Phone Device Settings

- **Extension** – Enter the extension that will be controlled by Amcom CTI Layer.
- **Security Code** – Enter the security code for the controlled station.
- **Release Button** – Enter the Release button assigned for the controlled station.
- **Line Appearances** – Enter the line appearances used for the controlled station.

Amcom AES CTI Service Setup

DMCC Settings:

- AES Server: 10.64.43.40
- Switch Name:
- Switch IP Address: 10.64.41.21
- Port (default = 4721): 4721
- Application Id: 1123
- User (default = cmapi): amcom
- Password:
- Media Mode: No Media
- Shared Control: False
- Dependency Mode: Dependent
- AES Version: 6.1
- Telecommuter Extension:
- ☐ Monitor Call Information
- ☐ Monitor Media Device
- ☐ Monitor Device Service

Phone Device Settings:

- Extension: 72001
- Security Code:
- RLT Transfer Button Id:
- Release Button Id: 9
- Toggle-Swap Button Id:
- Line Appearances:
 - Line 1 Button id = 1
 - Line 2 Button id = 2
 - Line 3 Button id = 3

Service Settings:

- Listener Port: 973
- Home Directory: c:\Program Files\Amcom
- Configuration File Name: cmapi.cfg
- DLL File Name: C:\Program Files\Amcom\bin\amcom_cmapi.dll
- LUA Agent Function File:
- LUA Agent State File:
- LUA App Specific File:

Debug Settings:

- File Name: Amcom_CTI_services
- Number of Files: 10
- File Size: 10000
- Directory: c:\program files\amcom\trace
- ☒ Level 1 ☒ Level 16 ☒ Level 256
- ☒ Level 2 ☒ Level 32 ☒ Level 512
- ☒ Level 4 ☒ Level 64 ☒ Level 1024
- ☒ Level 8 ☒ Level 128 ☒ Level 2048

Buttons: OK, Cancel, Restart Service, Phone Server, Smart Console

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 use CTI Layer to verify consistency.
- Place and answer calls from the controlled telephones manually and use CTI Layer to verify consistency.

9. Conclusion

These Application Notes described a compliance-tested configuration comprised of Communication Manager, Application Enablement Services, Avaya IP and Digital Telephones, and the Amcom CTI Layer application. Amcom CTI Layer 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 CTI Layer application.

10. Additional References

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

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

[2] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.1, Issue 2, February 2011.

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

©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.