



Avaya Solution & Interoperability Test Lab

Application Notes for Spok Console, utilizing Spok 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 Spok Console desktop applications.

Spok Console allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). Spok Console integrates with Spok CTI Layer, which is a middleware between Spok Console and Avaya Aura® Application Enablement Services, to control and monitor phone states.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 Spok Console applications.

Spok Console is a Windows-based attendant console application. Spok Console allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). Spok Console integrates with Spok CTI Layer, which is a middleware between Spok Console and Application Enablement Services, to control and monitor phone states.

It is the Spok CTI Layer service that actually uses the Application Enablement Services Device and Media Call Control (DMCC) 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. Spok Console in turn uses the Spok CTI Layer service to control and monitor a physical telephone. The Smart Console applications regularly provide the Database server with call and lamp state information concerning the controlled telephones.

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 Spok desktop application. The main objectives were to verify that:

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

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

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

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

2.2. Test Results

All test cases were executed and passed with the exception of the following observation.

During a scenario where the network connection from Spok Console is lost, the CTI service on Spok Console needed to be manually restarted to register the DMCC station again.

2.3. Support

Technical support for the Spok Console solution can be obtained by contacting Spok:

- URL – <http://www.spok.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, Communication Manager, Media Server with an Avaya G450 Media Gateway. Spok Console is configured to be in the same network as the enterprise. Endpoints include Avaya 9600 Series H.323 IP and Digital Telephones.

Note: Basic administration of Communication Manager and Application Enablement Services server is assumed. For details, see [1] and [2].

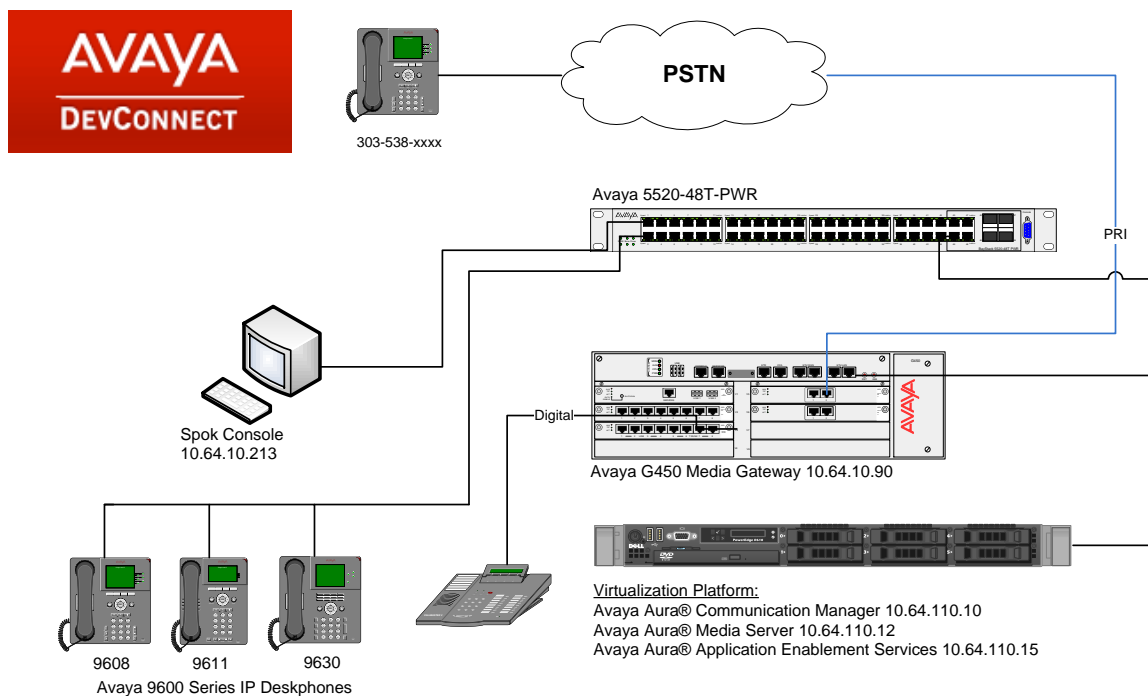


Figure 1: Spok Console Test Configuration

4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya Aura® Communication Manager		R017x.00.0.441.0 – 23012
Avaya Aura® Application Enablement Services		7.0.1.0.2.15-0
Avaya Aura® Media Server		7.7.0.334 A15
Avaya G450 Media Gateway		37.19.0
Avaya 9600 Series IP Telephones		
	9641/9611/9608 (H.323)	6.6.2
	9630 (H.323)	3.2.6
Spok CTI Layer		5.9.112.112
Spok Console		7.8.100

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 2
IP NODE NAMES		
Name	IP Address	
acms	10.64.110.18	
aes	10.64.110.15	
ams	10.64.110.16	
asm	10.64.110.13	
biscom	10.64.101.152	
cms17	10.64.10.85	
default	0.0.0.0	
egw1	10.64.110.200	
egw2	10.64.110.201	
procr	10.64.110.10	
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 3
IP SERVICES		
Service Type	Enabled	Local Node
AESVCS	y	procr

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 3 of 3
AE Services Administration		
Server ID	AE Services Server	Password
1:	aes	*
2:		

5.2. Configure Feature Access Codes (FAC)

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 11		
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: #25					
Attendant Access Code:					
Auto Alternate Routing (AAR) Access Code: 8					
Auto Route Selection (ARS) - Access Code 1: 9			Access Code 2:		
Automatic Callback Activation:			Deactivation:		
Call Forwarding Activation Busy/DA: *97 All: *99			Deactivation: *98		

5.3. 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								
Location: all						Percent Full: 1		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	3	dac						
1	4	ext						
1	5	ext						
3	10	ext						
8	1	fac						
9	1	fac						
*	3	dac						
#	3	dac						

5.4. Configure Hunt Group

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.

add hunt-group 1		Page 1 of 4	
HUNT GROUP			
Group Number: 1		ACD? y	
Group Name: Hunt Group 1		Queue? y	
Group Extension: 12001		Vector? y	
Group Type: ucd-mia			
TN: 1			
COR: 1		MM Early Answer? n	
Security Code:		Local Agent Preference? n	
ISDN/SIP Caller Display:			
Queue Limit: unlimited			
Calls Warning Threshold:	Port:		
Time Warning Threshold:	Port:		

5.5. Configure Abbreviated Dialing

Enter the **add abbreviated-dialing system** command. In the **DIAL CODE** list, enter the Feature Access Codes for ACD Login and Logout.

change abbreviated-dialing system		Page 1 of 1	
ABBREVIATED DIALING LIST			
SYSTEM LIST			
Size (multiple of 5): 5	Privileged? n	Label Language:english	
DIAL CODE	LABELS (FOR STATIONS THAT DOWNLOAD LABELS)		
01: *01		01:	Log-in
02: *06		02:	Log-out
03:		03:	*****
04:		04:	*****
05:		05:	*****

5.6. 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 Spok Console application.

change station 11054		Page 1 of 5
STATION		
Extension: 11054	Lock Messages? n	BCC: 0
Type: 9630	Security Code: 123456	TN: 1
Port: S00088	Coverage Path 1:	COR: 1
Name: Spok Console	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 11054	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
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 List 1**, enter the abbreviated dialing group configured in previous section. On **Pages 4** and **5** of the station forms, configure the following **BUTTON ASSIGNMENTS** in addition to the call-appr (call appearance) buttons as shown below:

change station 11054		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: system	List2:	List3:	
BUTTON ASSIGNMENTS			
1: call-appr	5: brdg-appr	B:1	E:11011
2:	6: brdg-appr	B:2	E:11011
3: brdg-appr B:1 E:11010	7: auto-in	Grp:	
4: brdg-appr B:2 E:11010	8: aux-work	RC:	Grp:
voice-mail			
change station 11054		Page 5 of 5	
STATION			
BUTTON ASSIGNMENTS			
9: abrv-dial List: 1 DC: 01			
10: abrv-dial List: 1 DC: 02			
11:			
12:			
13:			
14:			
15:			
16:			
17:			
18:			
19:			
20:			
21:			
22:			
23: togle-swap			
24: release			

Note: For Spok Console customers, the Toggle Swap Feature is not supported on Avaya 9621G and Avaya 9641G Deskphones.

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

6. Configure 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, a DMCC port.

6.1. Device and Media Call Control API Station Licenses

The Spok Console 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.

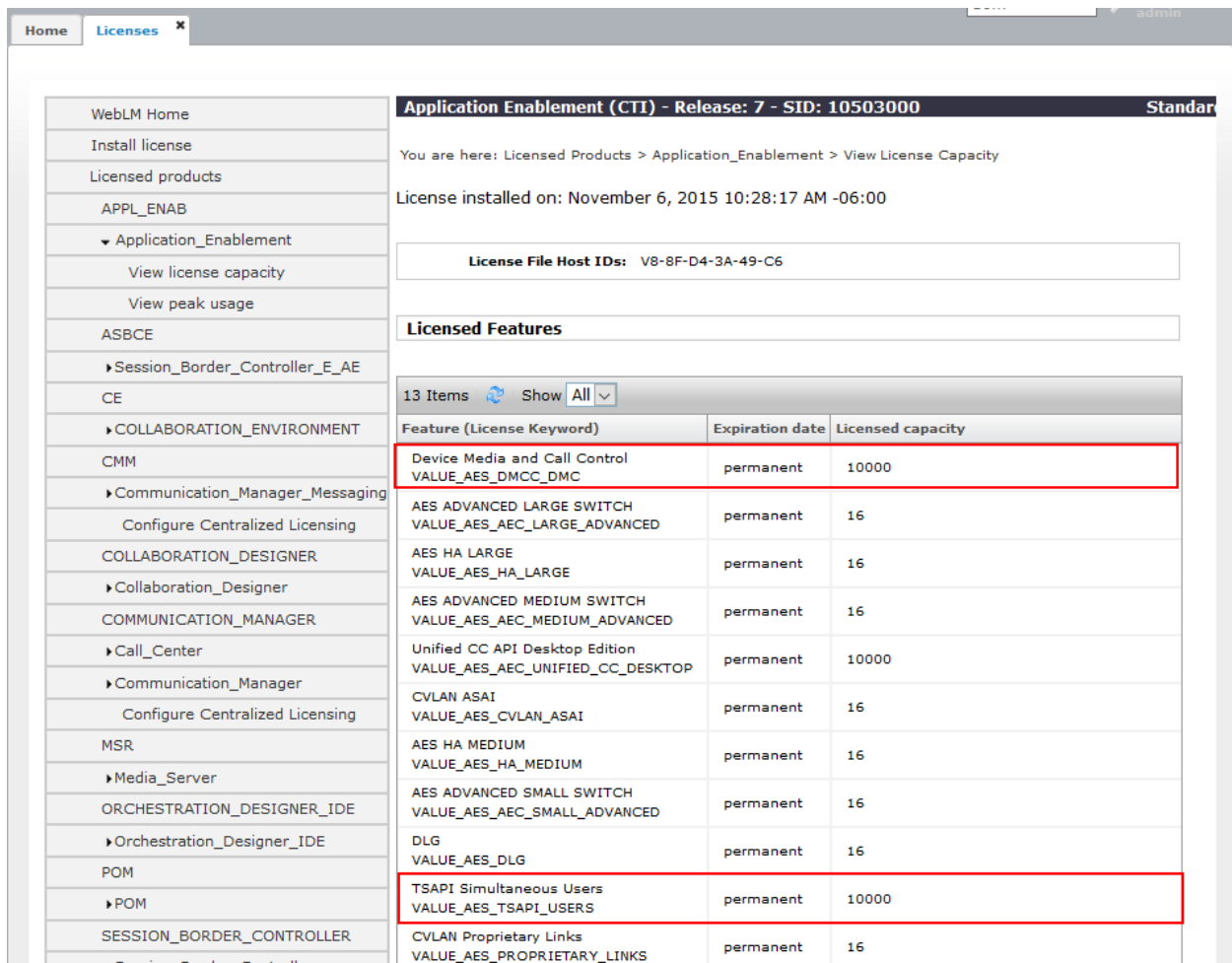
Select the **Licensing → WebLM Server Access** link from the left pane of the window (not shown). During the compliance testing, Avaya Aura System Manager was used as a license server.

Provide appropriate login credentials and log in.

Navigate to **Home → Licenses**. On the WebLM Home 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.

Note: TSAPI licenses (1 per agent station) are also required if calls routed to agent stations via ACD. Without TSAPI licenses, the agents will not see the First Party Call Control (1PCC) calling party information. i.e., Calling Party Number.



The screenshot shows the 'Licenses' page in the WebLM interface. The left sidebar contains a navigation menu with options like 'WebLM Home', 'Install license', 'Licensed products', and 'Application_Enablement'. The main content area is titled 'Application Enablement (CTI) - Release: 7 - SID: 10503000'. It shows the license installed on November 6, 2015, and the license file host IDs: V8-8F-D4-3A-49-C6. Below this, there is a 'Licensed Features' section with a table of 13 items. Two items are highlighted with red boxes: 'Device Media and Call Control' and 'TSAPI Simultaneous Users'.

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	16
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	16
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16

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 Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. To its right is the text "Application Enablement Services Management Console". A red horizontal bar spans the width of the page, with a "Help" link on the right. Below this bar is a login form with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar contains the copyright notice: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya Application Enablement Services Management Console Switch Connections page. At the top left is the Avaya logo. To its right is the text "Application Enablement Services Management Console". In the top right corner, there is a welcome message: "Welcome: User: cust", "Last login: Wed Jul 27 15:20:21 2016 from 10.64.10.47", "Number of prior failed login attempts: 0", "HostName/IP: aes/10.64.110.15", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 7.0.1.0.2.15-0", "Server Date and Time: Wed Jul 27 15:28:14 MDT 2016", and "HA Status: Not Configured". Below the header is a red horizontal bar with the text "Communication Manager Interface | Switch Connections" on the left and "Home | Help | Logout" on the right. On the left side, there is a navigation pane with the following items: "AE Services", "Communication Manager Interface" (expanded), "Switch Connections" (highlighted), "Dial Plan", "High Availability", "Licensing", "Maintenance", and "Networks". The main content area is titled "Switch Connections" and contains a text input field with the value "acm" and an "Add Connection" button. Below this is a table with the following columns: "Connection Name", "Processor Ethernet", "Msg Period", and "Number of Active Connections". The table has one row with the following values: "acm", "Yes", "30", and "1". Below the table are five buttons: "Edit Connection", "Edit PE/CLAN IPs", "Edit H.323 Gatekeeper", "Delete Connection", and "Survivability Hierarchy".

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
acm	Yes	30	1

The next window that appears prompts for the **Switch Password**. Enter the same password that was administered in Communication Manager in **Section 5.1**. Check box for **Processor Ethernet**. Click on **Apply**.

Welcome! User: cust
 Last login: Wed Jul 27 15:20:21 2016 from 10.64.10.47
 Number of prior failed login attempts: 0
 HostName/IP: aes/10.64.110.15
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 7.0.1.0.2.15-0
 Server Date and Time: Wed Jul 27 15:30:02 MDT 2016
 HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 High Availability
 Licensing
 Maintenance
 Networking
 Security
 Status

Connection Details - acm

Switch Password: [password field]
 Confirm Switch Password: [password field]
 Msg Period: 30 Minutes (1 - 72)
 Provide AE Services certificate to switch: ☐
 Secure H323 Connection: ☐
 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**.

Welcome! User: cust
 Last login: Wed Jul 27 15:20:21 2016 from 10.64.10.47
 Number of prior failed login attempts: 0
 HostName/IP: aes/10.64.110.15
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 7.0.1.0.2.15-0
 Server Date and Time: Wed Jul 27 15:30:59 MDT 2016
 HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 High Availability
 Licensing
 Maintenance
 Networking
 Security
 Status

Switch Connections

[text field] Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> acm	Yes	30	1

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

Enter the IP address of Procr used for Application Enablement Services connectivity from **Section 5.1**, and click on **Add Name or IP**.



AVAYA Application Enablement Services Management Console

Welcome! User: cust
Last login: Wed Jul 27 15:20:21 2016 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.110.15
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Wed Jul 27 15:33:53 MDT 2016
HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance

Edit Processor Ethernet IP - acm

10.64.110.10 Add/Edit Name or IP

Name or IP Address	Status
10.64.110.10	In Use

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.



AVAYA Application Enablement Services Management Console

Welcome! User: cust
Last login: Wed Jul 27 15:20:21 2016 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.110.15
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Wed Jul 27 15:34:51 MDT 2016
HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
High Availability
Licensing
Maintenance


Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> acm	Yes	30	1

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

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

**Application Enablement Services**
Management Console

Welcome! User: cust
Last login: Wed Jul 27 15:20:21 2016 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.110.15
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Wed Jul 27 15:35:44 MDT 2016
HA Status: Not Configured

Communication Manager Interface | Switch Connections

Home | Help | Logout

» AE Services
» Communication Manager Interface
» Switch Connections
» Dial Plan
» High Availability
» Licensing
» Maintenance

Edit H.323 Gatekeeper - acm

Name or IP Address

☒ 10.64.110.10

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


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 for user 'cust' with login details. A red navigation bar contains links for 'User Management | User Admin | Add User' and 'Home | Help | Logout'. On the left, a sidebar menu shows 'User Management' expanded with 'User Admin' selected, and 'Add User' highlighted. The main content area is titled 'Add User' and contains a form. A red box highlights the required fields: 'User Id', 'Common Name', 'Surname', 'User Password', and 'Confirm Password', all of which have 'interop' or '*****' entered. Below these, the 'CT User' dropdown menu is set to 'Yes' and is also highlighted with a red box. Other fields like 'Admin Note', 'Avaya Role', 'Business Category', 'Car License', 'CM Home', 'Cm Home', and 'Department Number' are present but empty.

The above information (User ID and User Password) must match with the information configured in the Spok Console Configuration page in **Section 7**.

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 (not shown).

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

**Application Enablement Services**
Management Console

Welcome! User: cust
Last login: Wed Jul 27 15:20:21 2016 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: asr/10.64.110.15
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.13-0
Server Date and Time: Wed Jul 27 15:37:40 MDT 2016
HA Status: Not Configured

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

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Account Management

Audit

Certificate Management

Enterprise Directory

Host AA

PAM

Security Database

Control

Edit CTI User

User Profile:

User IDinterrop

Common Nameinterrop

Worktop NameNONE

Unrestricted Access☒

Call and Device Controls:

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 cust
Last login: Wed Jul 27 15:20:21 2016 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aee/10.64.110.15
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.2.15-0
Server Date and Time: Wed Jul 27 15:41:18 MDT 2016
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

AE Services

Communication Manager

Interface

High Availability

Licensing

Maintenance

Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP/TLS Settings

Security

Status

User Management

Utilities

Help

Ports

CVLAN Ports

Unencrypted TCP Port 9999

Enabled Disabled

Encrypted TCP Port 9998

DLG Port

TCP Port 5678

TSAPI Ports

TSAPI Service Port 450

Enabled Disabled

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

Unencrypted Port 4721

Enabled Disabled

Encrypted Port 4722

TR/87 Port 4723

7. Configure Spok Console

Spok installs, configures, and customizes the Smart Console applications for their end customers. Spok Console integrates with Spok CTI Layer, which is a middleware between Spok Console and Application Enablement Services, to control and monitor the phone states.

Note: Avaya phones as the network supplier for the agent workstations is not supported by Spok. Agent workstations should have their own network connection, separate from Avaya phones.

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

Under DMCC Settings

- **AES Server** – Enter the IP address of the Application Enablement Services.
- **Switch IP Address** – Enter the procr IP address of Communication Manager.
- **Port** – Enter the port utilized during the compliance test.
- **User** – Enter the user name created for Spok Console.
- **Password** – Enter the password created for Spok Console.

Under Phone Device Settings

- **Extension** – Enter the extension that will be controlled by Spok Console.
- **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.

Spok AES CTI Service Setup

DMCC Settings:

AES Server: 10.64.110.15

Switch Name:

Switch IP Interface: 10.64.110.10

Port: Unsecure (4721) Application Id: 12

Local Certificate File:

SSL Protocol: TLSv1 (Transport Layer Security version 1)

User (default = cmapi): interop Password:

Media Mode: No Media Shared Control: False

Dependency Mode: Dependent AES Version: 7.0

Telecomuter Extension:

☐ Monitor Call Information

☐ Monitor Media Device

☐ Monitor Device Service

Phone Device Settings:

Extension: 11054 RILT Transfer Button Id:

Security Code: Release Button Id: 24

Max SCA Timer (ms): 250 Toggle-Swap Button Id: 23

Line Appearances:

Line 1	Button Id = 1	Display Id = a	
Line 2	Button Id = 2	Display Id = b	
Line 3	Button Id = 3	Display Id = c	
Line 4	Button Id = 4	Display Id = d	BRIDGE
Line 5	Button Id = 1	Display Id = y	BRIDGE
Line 6	Button Id = 2	Display Id = z	BRIDGE
Line 7	Button Id = 3	Display Id = A	BRIDGE
Line 8	Button Id = 4	Display Id = B	BRIDGE
Line 9	Button Id = 5	Display Id = C	BRIDGE
Line 10	Button Id = 1	Display Id = R	BRIDGE
Line 11	Button Id = 2	Display Id = S	BRIDGE

+ Add... - Delete Edit...

Service Settings:

Listener Port: 973

Home Directory: C:\Program Files (x86)\Amcom\

Configuration File Name: cmapi.cfg

DLL File Name: C:\Program Files (x86)\Amcom\bin\amcom_cmapi.dll

LUA Agent Function File:

LUA Agent State File:

LUA App Specific File: C:\Program Files (x86)\Amcom\CTI_Service\app_specific_

☐ Send SCA = 0 at the beginning of call state messages

Debug Settings:

File Name: AESCTI

Number of Files: 10 File Size: 10000

Directory: C:\Program Files (x86)\Amcom\Trace

<input checked="" type="checkbox"/> Level 1	<input checked="" type="checkbox"/> Level 16	<input checked="" type="checkbox"/> Level 256
<input checked="" type="checkbox"/> Level 2	<input checked="" type="checkbox"/> Level 32	<input checked="" type="checkbox"/> Level 512
<input checked="" type="checkbox"/> Level 4	<input checked="" type="checkbox"/> Level 64	<input checked="" type="checkbox"/> Level 1024
<input checked="" type="checkbox"/> Level 8	<input checked="" type="checkbox"/> Level 128	<input checked="" type="checkbox"/> Level 2048

OK Cancel Restart Service Phone Server

8. Verification Steps

The following steps may be used to verify the configuration:

- From the Spok 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 Communication Manager System Access Terminal (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 Smart Console, and verify consistency.
- Place and answer calls from the controlled telephones manually and use Smart Console, and 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 Spok Console application. Spok Console 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 Spok Console application.

10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager, Release 7.0.1, 03-300509, Issue 2, May 2016.*

[2] *Administering Avaya Aura® Avaya Aura® Application Enablement Services, Release 7.0.1, Issue 2, May 2016.*

Product information for Spok products may be found at <http://www.spok.com>.

©2016 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.