



Avaya Solution & Interoperability Test Lab

Application Notes for Spok MediCall, utilizing Spok CTI Layer, with Avaya Aura[®] Communication Manager and Avaya Aura[®] Application Enablement Services - Issue 1.1

Abstract

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura[®] Communication Manager, Avaya Aura[®] Application Enablement Services, Avaya IP Telephones, and Spok MediCall desktop application.

Spok MediCall allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). Spok MediCall integrates with Spok CTI Layer, which is a middleware between Spok MediCall 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 (AES), Avaya IP (J169\J179) Telephones, and Spok MediCall applications.

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

The Spok CTI Layer service uses the AES Device and Media Call Control (DMCC) and Telephony Services Application Programming Interface (TSAPI) via DMCC 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 MediCall in turn uses the Spok CTI Layer service to control and monitor a physical telephone.

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. Typical call scenarios including inbound, outbound, internal, external, and various conference and transfer were performed. The main objectives were to verify that:

- The user may successfully use Spok MediCall to perform off-hook, on-hook, dial, answer, hold, retrieve, transfer, conference, and release operations on the physical telephone.
- Spok MediCall and manual telephone operations may be used interchangeably; for example, go off-hook using Spok MediCall and manually dial digits.
- Display and call information on the physical telephone is accurately reflected in the Spok MediCall GUI.
- Call states are consistent between Spok MediCall and the physical telephone.

For serviceability testing, failures such as network disconnects, and resets were applied.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Spok made use of encrypted DMCC connections.

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 MediCall, AES, and Communication Manager.

2.2. Test Results

All test cases were executed and passed. Note that the MediCall application only supports attended transfers.

2.3. Support

Technical support for the Spok MediCall 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 AES, Communication Manager, Media Server and Avaya G430 Media Gateway. Spok MediCall is configured to be in the same network as the enterprise. Endpoints include Avaya J100 Series H.323 IP Telephones and Avaya Endpoints.

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

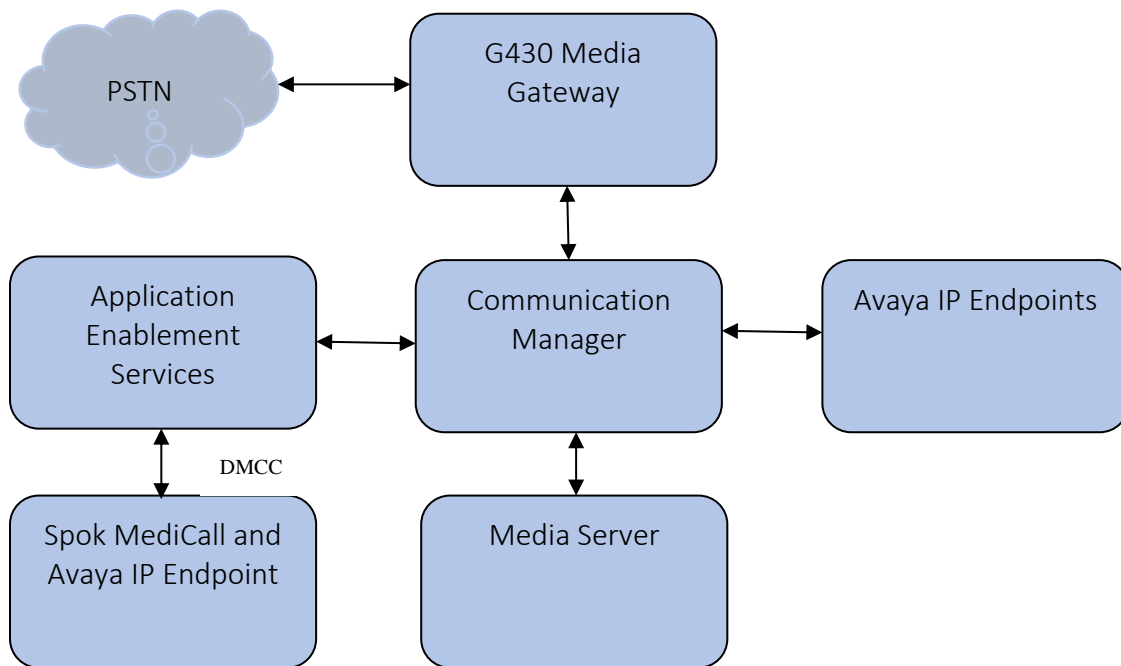


Figure 1: Spok MediCall Test Configuration

4. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided. All servers (except G430 Media Gateway) were on VM infrastructure, including the Spok components:

Equipment		Software/Firmware
Avaya Aura® Communication Manager		8.1.3.1.0-FP3SP1
Avaya Aura® Application Enablement Services		8.1.3.1.0.7-0
Avaya Aura® Media Server		8.0.2.163
Avaya G430 Media Gateway		41.34.1/1
Avaya Endpoints		
	J169\J179 (H.323)	6.8502
Spok MediCall		11.x (11.11.28) 11.13
Spok CTI Layer		7.x (7.0.0.6) 7.4

5. Configure Avaya Aura® Communication Manager

This section describes the procedures for configuring Abbreviated Dialing, and controlled telephones. Standard connectivity was in place for AES and other Avaya components and are not covered in this document. A System Access Terminal session was used to perform these steps.

5.1. Configure System Parameters Features

Enter the **change system-parameters features** command. -Verify the setting of **Auto Hold** and **Transfer Upon Hang-Up** features. Please consult with Spok to confirm which combination of these features will work best in the environment, some combinations may cause rare conflicts.

Verify the **Auto Hold** and **Transfer Upon Hang-Up** features are enabled.

```
change system-parameters features                                     Page 6 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Public Network Trunks on Conference Call: 5                  Auto Start? y
      Conference Parties with Public Network Trunks: 6             Auto Hold? y
      Conference Parties without Public Network Trunks: 6          Attendant Tone? n
      Night Service Disconnect Timer (seconds): 180                Bridging Tone? n
      Short Interdigit Timer (seconds): 3                          Conference Tone? n
      Unanswered DID Call Timer (seconds):                          Intrusion Tone? n
      Line Intercept Tone Timer (seconds): 30                      Mode

change system-parameters features                                     Page 7 of 19
      FEATURE-RELATED SYSTEM PARAMETERS

CONFERENCE/TRANSFER
      Abort Transfer? n                                           No Dial Tone Conferencing? n
      Transfer Upon Hang-Up? y                                     Select Line Appearance Conferencing? n
      Abort Conference? n                                           Unhold? n
      No Hold Conference Timeout: 60 Maximum Ports per Expanded Meet-me Conf: 7
                                           12-party Conferences? n
      External Ringing for Calls with Trunks? remote-only
```

5.2. 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. These codes will be used by Spok MediCall extensions.

add abbreviated-dialing system		Page 1 of 1
ABBREVIATED DIALING LIST SYSTEM LIST		
Size (multiple of 5): <u>5</u> Privileged? <u>n</u> Label Language: <u>english</u>		
DIAL CODE LABELS (FOR STATIONS THAT DOWNLOAD LABELS)		
01: <u>*54</u>	01: <u>Log-in</u>	
02: <u>*55</u>	02: <u>Log-out</u>	
03: _____	03: <u>*****</u>	
04: _____	04: <u>*****</u>	
05: _____	05: <u>*****</u>	

5.3. Configure Stations

During the compliance testing one extension was configured for Spok MediCall. Enter the **change station *n*** command, where ***n*** is the extension of a station.

Extension 30012 was used by Spok MediCall for controlling an Avaya Endpoint. On **Page 1** of the **station** form, enter a phone **Type**, descriptive **Name**, **Security Code**, **Button Modules** and set **IP SoftPhone** field to **y** to allow the physical station to be controlled by a softphone such as the Spok MediCall application. Note that J100 series phones use 9611 as station type for H.323 firmware configurations.

change station 30012		Page 1 of 7
STATION		
Extension: 30012	Lock Messages? <u>n</u>	BCC: 0
Type: <u>9611</u>	Security Code: <u>*</u>	TN: <u>1</u>
Port: S000007	Coverage Path 1: _____	COR: <u>1</u>
Name: <u>Spok Medical1</u>	Coverage Path 2: _____	COS: <u>1</u>
Unicode Name? <u>n</u>	Hunt-to Station: _____	Tests? <u>y</u>
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: <u>19</u>	Personalized Ringing Pattern: <u>1</u>	
Speakerphone: <u>2-way</u>	Message Lamp Ext: <u>30012</u>	
Display Language: <u>english</u>	Mute Button Enabled? <u>y</u>	
Survivable GK Node Name: _____	Button Modules: <u>2</u>	
Survivable COR: <u>internal</u>	Media Complex Ext: _____	
Survivable Trunk Dest? <u>y</u>	IP SoftPhone? <u>y</u>	
IP Video Softphone? <u>n</u>		
Short/Prefixed Registration Allowed: <u>default</u>		
Customizable Labels? <u>y</u>		

On Page 2, set **Auto Select Any Idle Appearance** to **y**.

change station 30012	Page 2 of 7
STATION	
FEATURE OPTIONS	
LWC Reception: spe	Auto Select Any Idle Appearance? y
LWC Activation? y	Coverage Msg Retrieval? y
LWC Log External Calls? n	Auto Answer: none
CDR Privacy? n	Data Restriction? n
Redirect Notification? y	Idle Appearance Preference? n
Per Button Ring Control? n	Bridged Idle Line Preference? n
Bridged Call Alerting? n	Restrict Last Appearance? y
Active Station Ringing: single	
	EMU Login Allowed? n
H.320 Conversion? n	Per Station CPN - Send Calling Number?
Service Link Mode: as-needed	EC500 State: enabled
Multimedia Mode: enhanced	Audible Message Waiting? n
MWI Served User Type:	Display Client Redirection? n
AUDIX Name:	Select Last Used Appearance? n
	Coverage After Forwarding? s
	Multimedia Early Answer? n
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y
Emergency Location Ext: 30012	Always Use? n IP Audio Hairpinning? n

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 30012 <div style="text-align: center;">STATION</div> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> SITE DATA Room: _____ Jack: _____ Cable: _____ Floor: _____ Building: _____ </div> <div style="width: 45%;"> Headset? <u>n</u> Speaker? <u>n</u> Mounting: <u>d</u> Cord Length: <u>0</u> Set Color: _____ </div> </div> <div style="margin-top: 10px;"> ABBREVIATED DIALING List1: <u>system</u> List2: _____ List3: _____ </div> <div style="margin-top: 20px;"> BUTTON ASSIGNMENTS <table style="width: 100%;"> <tr> <td>1:call-appr</td> <td>5:call-appr</td> <td></td> </tr> <tr> <td>2:call-appr</td> <td>6:q-calls</td> <td>Grp: 1</td> </tr> <tr> <td>3:call-appr</td> <td>7:</td> <td></td> </tr> <tr> <td>4:call-appr</td> <td>8:</td> <td></td> </tr> </table> </div>	1:call-appr	5:call-appr		2:call-appr	6:q-calls	Grp: 1	3:call-appr	7:		4:call-appr	8:		Page 4 of 7												
1:call-appr	5:call-appr																								
2:call-appr	6:q-calls	Grp: 1																							
3:call-appr	7:																								
4:call-appr	8:																								
change station 30012 <div style="text-align: center;">STATION</div> <div style="text-align: center; margin-top: 10px;"> BUTTON MODULE #1 ASSIGNMENTS </div> <table style="width: 100%;"> <tr> <td>1:brdg-appr B:1 E:30001</td> <td>13:brdg-appr B:1 E:30002</td> </tr> <tr> <td>2:brdg-appr B:2 E:30001</td> <td>14:brdg-appr B:2 E:30002</td> </tr> <tr> <td>3:brdg-appr B:3 E:30001</td> <td>15:</td> </tr> <tr> <td>4:brdg-appr B:4 E:30001</td> <td>16:</td> </tr> <tr> <td>5:brdg-appr B:5 E:30001</td> <td>17:</td> </tr> <tr> <td>6:brdg-appr B:6 E:30001</td> <td>18:</td> </tr> <tr> <td>7:</td> <td>19:</td> </tr> <tr> <td>8:abrv-dial List: 1 DC: 01 HL? n</td> <td>20:</td> </tr> <tr> <td>9:auto-in Grp:</td> <td>21:</td> </tr> <tr> <td>10:aux-work RC: Grp:</td> <td>22:</td> </tr> <tr> <td>11:after-call Grp:</td> <td>23:</td> </tr> <tr> <td>12:</td> <td>24:</td> </tr> </table>	1:brdg-appr B:1 E:30001	13:brdg-appr B:1 E:30002	2:brdg-appr B:2 E:30001	14:brdg-appr B:2 E:30002	3:brdg-appr B:3 E:30001	15:	4:brdg-appr B:4 E:30001	16:	5:brdg-appr B:5 E:30001	17:	6:brdg-appr B:6 E:30001	18:	7:	19:	8:abrv-dial List: 1 DC: 01 HL? n	20:	9:auto-in Grp:	21:	10:aux-work RC: Grp:	22:	11:after-call Grp:	23:	12:	24:	Page 6 of 7
1:brdg-appr B:1 E:30001	13:brdg-appr B:1 E:30002																								
2:brdg-appr B:2 E:30001	14:brdg-appr B:2 E:30002																								
3:brdg-appr B:3 E:30001	15:																								
4:brdg-appr B:4 E:30001	16:																								
5:brdg-appr B:5 E:30001	17:																								
6:brdg-appr B:6 E:30001	18:																								
7:	19:																								
8:abrv-dial List: 1 DC: 01 HL? n	20:																								
9:auto-in Grp:	21:																								
10:aux-work RC: Grp:	22:																								
11:after-call Grp:	23:																								
12:	24:																								
change station 30012 <div style="text-align: center;">STATION</div> <div style="text-align: center; margin-top: 10px;"> BUTTON MODULE #2 ASSIGNMENTS </div> <table style="width: 100%;"> <tr> <td>1:brdg-appr B:1 E:30003</td> <td>13:brdg-appr B:1 E:30006</td> </tr> <tr> <td>2:</td> <td>14:brdg-appr B:2 E:30006</td> </tr> <tr> <td>3:</td> <td>15:brdg-appr B:3 E:30006</td> </tr> <tr> <td>4:</td> <td>16:brdg-appr B:4 E:30006</td> </tr> <tr> <td>5:abrv-dial List: 1 DC: 02 HL? n</td> <td>17:brdg-appr B:5 E:30006</td> </tr> <tr> <td>6:</td> <td>18:brdg-appr B:6 E:30006</td> </tr> <tr> <td>7:</td> <td>19:</td> </tr> <tr> <td>11:</td> <td>23:toggle-swap</td> </tr> <tr> <td>12:</td> <td>24:release</td> </tr> </table>	1:brdg-appr B:1 E:30003	13:brdg-appr B:1 E:30006	2:	14:brdg-appr B:2 E:30006	3:	15:brdg-appr B:3 E:30006	4:	16:brdg-appr B:4 E:30006	5:abrv-dial List: 1 DC: 02 HL? n	17:brdg-appr B:5 E:30006	6:	18:brdg-appr B:6 E:30006	7:	19:	11:	23:toggle-swap	12:	24:release	Page 7 of 7						
1:brdg-appr B:1 E:30003	13:brdg-appr B:1 E:30006																								
2:	14:brdg-appr B:2 E:30006																								
3:	15:brdg-appr B:3 E:30006																								
4:	16:brdg-appr B:4 E:30006																								
5:abrv-dial List: 1 DC: 02 HL? n	17:brdg-appr B:5 E:30006																								
6:	18:brdg-appr B:6 E:30006																								
7:	19:																								
11:	23:toggle-swap																								
12:	24:release																								

5.4. Configure Hunt Group

Enter the **add hunt-group *n*** command, where *n* is an unused hunt group number. On **Page 1** assign a descriptive **Group Name** and an available **Group Extension** as per the dial plan. Also, set **ACD**, **Queue** and **Vector** to **y**. The Hunt group configured here was used by MediCall agents to log onto ACD.

add hunt-group 21		Page 1 of 4	
HUNT GROUP			
Group Number: 21		ACD? y	
Group Name: Hunt Group 21		Queue? y	
Group Extension: 31020		Vector? y	
Group Type: ucd-mia			
TN: 1			
COR: 1			
Security Code:		MM Early Answer? n	
ISDN/SIP Caller Display:		Local Agent Preference? n	
Queue Limit: unlimited			
Calls Warning Threshold:		Port:	
Time Warning Threshold:		Port:	

5.5. Configure VDNs

Use the **add vdn *n*** command to add a new VDN, where *n* is an available extension as per the dial plan.

On **Page 1**, provide a descriptive **Name** and available **Vector Number** in **Destination**.

add vdn 31501	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 31501	Unicode Name? n
Name*: Spok VDN	
Destination: Vector Number	21
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: both	Report Adjunct Calls as ACD*? n
Acceptable Service Level (sec): 20	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	
SIP URI:	

5.6. Configure Vector

To configure a vector, use the **change vector *n*** command, where *n* is the vector used during the adding the VDN. A simple vector is configured to queue calls to hunt group 21.

change vector 21				CALL VECTOR		Page 1 of 6	
Number: 21				Name: Spok Vector			
Multimedia? n	Attendant Vectoring? n		Meet-me Conf? n		Lock? n		
Basic? y	EAS? y	G3V4 Enhanced? y	ANI/II-Digits? y		ASAI Routing? y		
Prompting? y	LAI? y	G3V4 Adv Route? y	CINFO? y	BSR? y	Holidays? y		
Variables? y	3.0 Enhanced? y						
01 wait-time	2	secs hearing ringback					
02 queue-to	skill 21	pri m					
03 wait-time	30	secs hearing music					
04 goto step	2	if unconditionally					
05							

5.7. Configure Agent Extensions

Enter the **add agent-loginID *n*** command, where *n* is an available extension according to the dial plan. This extension will be used by Spok MediCall to log onto ACD. During the compliance test, two agent extensions were added, 12021 and 12022. On **Page 1**, specify a **Name** of the agent, **Password**, and set **Auto Answer** to **none**.

add agent-loginID 32021		Page 1 of 2	
AGENT LOGINID			
Login ID: 32021		Unicode Name? n AAS? n	
Name: Spok Agent 1		AUDIX? n	
TN: 1		Check skill TNs to match agent TN? n	
COR: 1			
Coverage Path:		LWC Reception: spe	
Security Code:		LWC Log External Calls? n	
Attribute:		AUDIX Name for Messaging:	
		LoginID for ISDN/SIP Display? n	
		Password:	
		Password (enter again):	
		Auto Answer: none	
AUX Agent Remains in LOA Queue: system		MIA Across Skills: system	
AUX Agent Considered Idle (MIA): system		ACW Agent Considered Idle: system	
Work Mode on Login: system		Aux Work Reason Code Type: system	
		Logout Reason Code Type: system	
Maximum time agent in ACW before logout (sec): system			
		Forced Agent Logout Time: :	
WARNING: Agent must log in again before changes take effect			

On **Page 2**, configure the Skill Number that was configured earlier in this document and specify a skill level.

add agent-loginID 32021		Page 2 of 2	
AGENT LOGINID			
Direct Agent Skill:		Service Objective? n	
Call Handling Preference: skill-level		Local Call Preference? n	
SN	RL SL	SN	RL SL
1: 21	1	16:	31: 46:
2:		17:	32: 47:
3:		18:	33: 48:
4:		19:	34: 49:

6. Configure Avaya Aura® Application Enablement Services

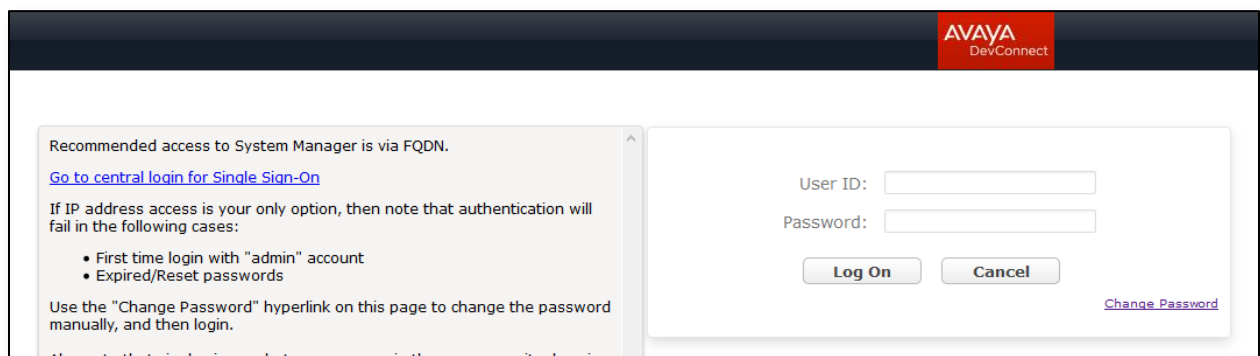
The Application Enablement Services server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager.

This section assumes that installation and basic administration of the AES server has been performed. The steps in this section describe the configuration of a CTI user, a DMCC port and TLS Version, Root Certificate, and Tlink information.

6.1. Device and Media Call Control API Station Licenses

The Spok MediCall 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 AES 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 **Services → Licenses** (not shown). On the WebLM Home page, select **License Products → Application_Enablement** (not shown) link from the left pane of the window.

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

Note on DMCC Licenses: The Spok MediCall application uses an existing station for Console Operators. Thus, the Communication Manager license requires enough station license capacity to accommodate these. The DMCC licenses can be purchased as either Basic (just the AES DMCC requirement), or Full (which bundles a Communication Manager station RTU with the AES DMCC).

Note: TSAPI licenses (one per agent station) are also required.

13 Items  Show All 		
Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	8
AES HA LARGE VALUE_AES_HA_LARGE	permanent	8
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	8
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	1000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	8
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	8
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	8
DLG VALUE_AES_DLG	permanent	8
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	1000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	8
SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS		

6.2. Configure the CTI User

Navigate to **User Management** → **User Admin** → **Add User** link from the left pane of the window. On the Add User page (not shown), 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 Edit User page below shows the configuration previously configured for this user.

AVAYA **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Mon May 17 10:13:35 2021 from 192.168.4.129
Number of prior failed login attempts: 0
HostName/IP: sildvaes8.sildenver.org/10.64.115.28
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.1.0.7-0
Server Date and Time: Wed Jun 02 11:32:54 MDT 2021
HA Status: Not Configured

User Management | User Admin | List All Users Home | Help | Logout

Edit User

* User Id spok
* Common Name Spok
* Surname Spok
User Password
Confirm Password
Admin Note
Avaya Role None
Business Category
Car License
CM Home
Css Home
CT User Yes

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

The Following step is only necessary if the Security Database is enabled for DMCC and TSAPI (**Security → Security Database → Control** – not shown).

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.

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 system details. A red navigation bar contains the path 'Security | Security Database | CTI Users | List All Users' and links for 'Home | Help | Logout'. On the left, a sidebar lists various services, with 'Security' expanded to show options like 'Account Management', 'Audit', 'Certificate Management', 'Enterprise Directory', 'Host AA', and 'PAM'. The main content area is titled 'Edit CTI User' and shows a form for a user named 'spok'. The 'User Profile' section includes fields for 'User ID', 'Common Name', and 'Worktop Name' (set to 'NONE'). The 'Unrestricted Access' checkbox is checked and highlighted with a red box. Below this, the 'Call and Device Control' section shows 'Call Origination/Termination and Device Status' set to 'None'. The 'Call and Device Monitoring' section shows 'Device Monitoring' and 'Calls On A Device Monitoring' set to 'None', and 'Call Monitoring' is unchecked. The 'Routing Control' section shows 'Allow Routing on Listed Devices' set to 'None'. At the bottom, there are 'Apply Changes' and 'Cancel Changes' buttons.

Edit CTI User		
User Profile:		
User ID	spok	
Common Name	Spok	
Worktop Name	NONE	
Unrestricted Access	<input checked="" type="checkbox"/>	
Call and Device Control:		
Call Origination/Termination and Device Status	None	
Call and Device Monitoring:		
Device Monitoring	None	
Calls On A Device Monitoring	None	
Call Monitoring	<input type="checkbox"/>	
Routing Control:		
Allow Routing on Listed Devices	None	
<input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/>		

6.3. 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. Both **Unencrypted** and **Encrypted Port** were used during the compliance test. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

Ports		
CVLAN Ports		
Unencrypted TCP Port	9999	Enabled <input checked="" type="radio"/> Disabled <input type="radio"/>
Encrypted TCP Port	9998	Enabled <input checked="" type="radio"/> Disabled <input type="radio"/>
DLG Port		
TCP Port	5678	
TSAPI Ports		
TSAPI Service Port	450	Enabled <input checked="" type="radio"/> Disabled <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		
Unencrypted Port	4721	Enabled <input checked="" type="radio"/> Disabled <input type="radio"/>
Encrypted Port	4722	Enabled <input checked="" type="radio"/> Disabled <input type="radio"/>
TR/87 Port	4723	Enabled <input type="radio"/> Disabled <input checked="" type="radio"/>

6.4. Configure TLS Version

Navigate to the **Networking → TCP/TLS Settings** page and verify that TLS Version 1.2 is checked. This will be used in **Section 7** when configuring Spok MediCall.

The screenshot shows the 'Networking | TCP / TLS Settings' page. On the left is a navigation menu with options like AE Services, Communication Manager, Interface, High Availability, Licensing, Maintenance, Networking (selected), AE Service IP (Local IP), Network Configure, Ports, TCP/TLS Settings (highlighted), Security, Status, User Management, Utilities, and Help. The main content area is titled 'TCP / TLS Settings'. It includes 'TLSv1 Protocol Configuration' with three checkboxes: 'Support TLSv1.0 Protocol' (unchecked), 'Support TLSv1.1 Protocol' (unchecked), and 'Support TLSv1.2 Protocol' (checked). Below this is 'TCP Retransmission Count' with two radio buttons: 'Standard Configuration (15)' (selected) and 'TSAPI Routing Application Configuration (6)' (unchecked). At the bottom of the settings area are three buttons: 'Apply Changes', 'Restore Defaults', and 'Cancel Changes'. A note states: 'Note: A smaller TCP Retransmission Count reduces the amount of time that the AE Services server waits for a TCP acknowledgement before closing the socket. Select the Standard Configuration setting unless this AE Services server is used by TSAPI routing applications.' A warning follows: 'Warning: This setting applies to all TCP and TLS sockets on the AE Services Server and so it should be used with caution.'

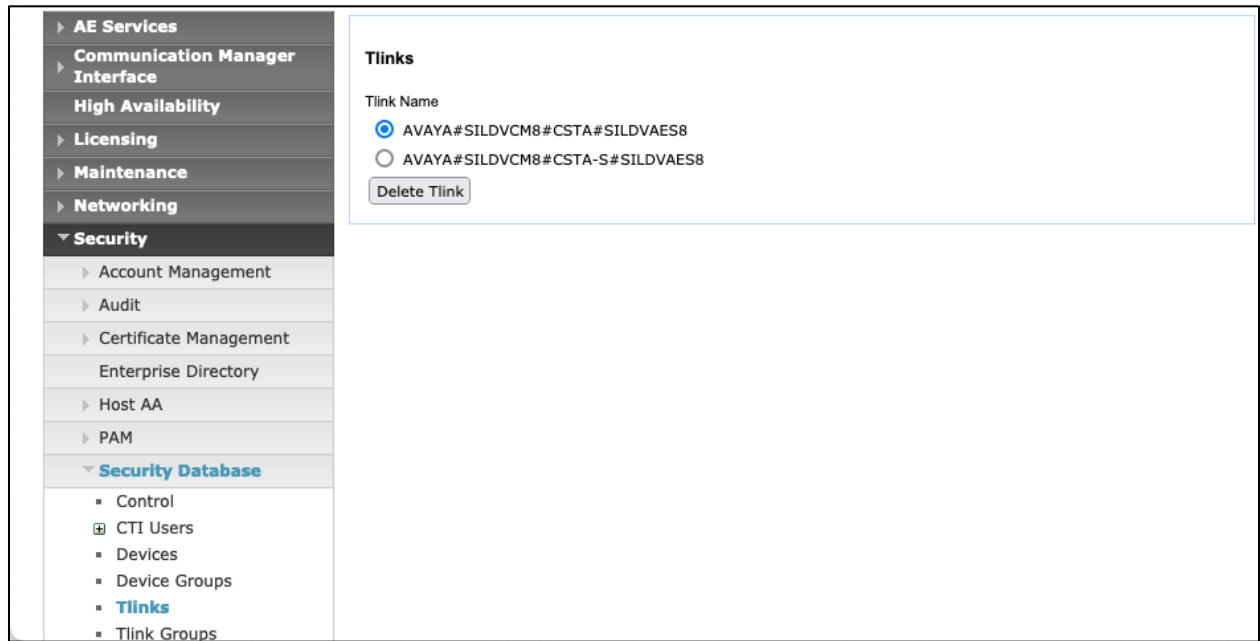
6.5. Obtain Root Certificate

In order to configure the application to use secure links, download the root certificate for the environment, in this case Avaya Aura® System Manager issued certificates to AES. The following illustrates how to download this from Avaya Aura® System Manager.

The screenshot shows the 'Avaya Aura System Manager 8.1' interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are on the right. The left sidebar shows a menu with 'Security' selected, containing 'Certificates', 'Authority' (highlighted), 'Enrollment Passw...', 'Manage Certificat...', 'Manage Entity Cl...', and 'Configuration'. The main content area is titled 'CA Structure & CRLs'. It lists 'CA Functions' (CA Activation, CA Structure & CRLs, Certificate Profiles, Certification Authorities, Crypto Tokens, Publishers) and 'RA Functions' (Add End Entity, End Entity Profiles, Search End Entities, User Data Sources). Below the functions, it shows 'Basic Functions for CA : tmdefaultca' with links for 'View Certificate' and 'View Information'. The 'Root CA' is identified as 'CN=System Manager CA,OU=MGMT,O=AVAYA'. There are three download links: 'Download binary/to IE', 'Download to Firefox', and 'Download PEM file' (which is highlighted with a red box). Below these, it shows the 'Latest CRL' details: 'Created 2021-06-15 22:37:48-06:00, Expires 2021-06-22 22:37:48-06:00, number 80' with a 'Get CRL' link. At the bottom, there is a 'Create a new updated CRL' section with a 'Create CRL' button.

6.6. Obtain the Tlink

Navigate to the **Security → Security Database → Tlinks** and note the Tlink name for use when configuring the Spok solution in the next section.



7. Configure Spok MediCall

Spok installs, configures, and customizes the Spok MediCall application for their end customers. Spok MediCall integrates with Spok CTI Layer, which is a middleware installed on the same PC that the Spok Medicall is installed on, 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 its own network connection, separate from Avaya phones.

The following shows the **Spok AES CTI Services Setup** page. This is an application installed when the Spok software is installed on the PC and is accessed for the Programs list on the PC.

Provide the following information:

Under DMCC Settings

- **AES Server** – Enter the IP address of AES.
- **Switch IP Address** – Enter the procr IP address of Communication Manager.
- **Port** – Enter the port utilized during the compliance test.
- **SSL Protocol** – Select Version 1.2 to match the AES settings in **Section 6**.
- **User** – Enter the user name created for Spok MediCall from **Section 6**.
- **Password** – Enter the password created for Spok MediCall from **Section 6**.

Under Phone Device Settings

- **Extension:** Enter the extension that will be controlled by Spok MediCall from **Section 5**.
- **Security Code:** Enter the security code for the controlled station from **Section 5**.
- **Release Button** – Enter the Release button assigned for the controlled station from **Section 5.3**.
- **Line Appearances** – Configure line appearances as per **Section 5**.

Spok AES CTI Service Setup

DMCC Settings:

AES Server: 10.64.115.28

Switch Name:

Switch IP Interface: 10.64.115.25

Port: Secure (4722) Application Id: spok

Device Instance: 0

Local Certificate File: C:\Users\Spokuser\Downloads\SystemManagerCA.crt

SSL Protocol: TLSv1.2 (Transport Layer Security version 1.2)

User (default = cmapi): spok 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: 30012 RLT Transfer Button Id:

Security Code: Release Button Id: 1341

Max SCA Timer (ms): 250 Toggle-Swap Button Id: 1340

☐ Press Release Button Upon Cancel

Park Access Code:

Unpark Access Code:

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
Line 5	Button Id = 5	Display Id = e
Line 6	Button Id = 251	Display Id = y BRIDGE
Line 7	Button Id = 252	Display Id = z BRIDGE

+ Add... X 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:

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

Debug Settings:

File Name: AvayaCTI

Number of Files: 10 File Size: 100000

Directory: C:\Program Files (x86)\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

OK Cancel Restart Service Phone Server

8. Verification Steps

The following steps may be used to verify the configuration:

- Verify Spok MediCall is successfully connected to AES via AES Management console. Navigate to **Status → Status and Control → DMCC Service Summary**. Verify the **State** of Spok MediCall user is **REGISTERED**.

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Thu Jun 03 12:39:52 MDT 2021

Service Uptime: 58 days, 18 hours 14 minutes

Number of Active Sessions: 3

Number of Sessions Created Since Service Boot: 3865

Number of Existing Devices: 3

Number of Devices Created Since Service Boot: 30

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
FD08E821D5C0B8FAD 6C0ABFF3001B31E-3866	spok	spok	10.64.115.33	XML Encrypted	1

Item 1-3 of 3

1 Go

DMCC Service Summary - Device Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Thu Jun 03 12:53:00 MDT 2021

Service Uptime: 58 days, 18 hours and 27 minutes

Number of Active Sessions: 3

Number of Sessions Created Since Service Boot: 3865

Number of Existing Devices: 3

Number of Devices Created Since Service Boot: 30

Device ID	Gatekeeper IP address	State	Associated Sessions
30012:SILDVCM8:10.64.115.25:0	10.64.115.25	REGISTERED	1

- Place and answer calls from the controlled telephones manually and use Spok MediCall and verify consistency.

MediCall™ Operator Console 11.13.31

Extension : MSG:31500

a= 1303-538-3421 to MSG: 31500

Release Auto In Aux Out AfterCall

MSG:31500 30012 30012 30012 30012 30001 30001 30001 30001

30001 30001 30002 30002 30006 30006 30006 30006 30003

Directory

PAGER: OFFICE:%O Not Found
CELL:%03 Not Found
TITLE:
Special Notes:

WAKE UP: HOME:%P Not Found
ZONE:%05 Not Found
Location:

Name	Location	Department	Dial #	Pager Id	Facility
Fletcher, Minnie					
Feuer, Davey		Development		8982607	
*Ham Department		Ham Department		8008	
Speech, Not					
Koutsavlis, Gabby				0303	
Tooth, Sweet		Chocolate Cake Departm		5018	
*Burger Department		Burger Department		5009	MASC
SUPPORT					
Parmenter, Kate			6035295737	1234	GEN
Betty, Beantown			6035295737	8877	

Associates Update Admin Profile Where... Change Status Frq Additional Take Msg Get Msg Quick List On Call LookUp Expand

9. Conclusion

These Application Notes described a compliance-tested configuration comprised of Communication Manager, AES, Avaya J169\179 IP Telephones, and the Spok MediCall application. Spok MediCall 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 Telephones that were controlled and monitored by the Spok MediCall application.

10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager, Release 8.1.x*

[2] *Administering Avaya Aura® Application Enablement Services, Release 8.1.x*

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

©2021 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.