



## 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 1.0

### Abstract

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

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 Endpoints (9608) and Spok MediCall applications.

Spok MediCall is a Windows-based attendant console application for Healthcare industry. 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.

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 Secure DMCC.

## 2. General Test Approach and Test Results

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

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

- Call states are consistent between MediCall 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 Spok MediCall, AES, 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 network connection from Spok MediCall is lost, the CTI service on Spok PC/PSAP needed to be manually restarted to register the DMCC station again.

## **2.3. Support**

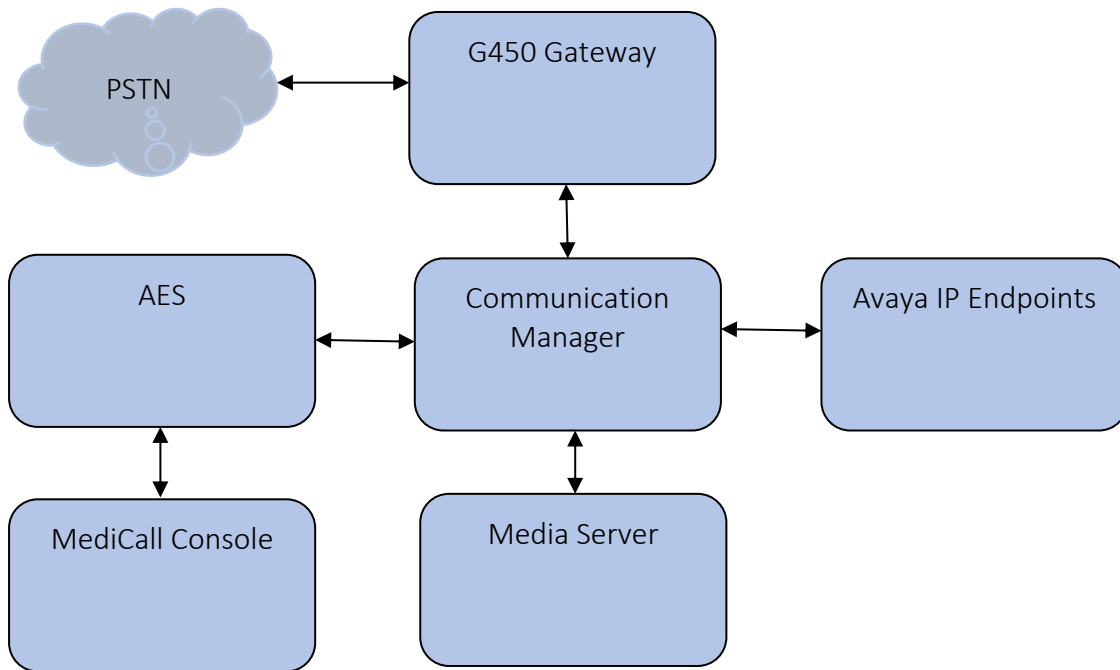
Technical support for the Spok MediCall solution can be obtained by contacting Spok:

- 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 with an Avaya G450 Media Gateway. Spok MediCall is configured to be in the same network as the enterprise. Endpoints include Avaya 9600 Series H.323 IP Telephones.

**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:

Equipment		Software/Firmware
Avaya Aura® Communication Manager		8.0.1.1.0-FP1SP1
Avaya Aura® Application Enablement Services		8.0.1.0.2.5-0
Avaya Aura® Media Server		8.0.0.183
Avaya G450 Media Gateway		40.20.0
Avaya 9600 Series IP Telephones		
	9641/9611/9608 (H.323)	6.8102
Spok CTI Layer		7.x (7.0.0.6)
Spok MediCall		11.x (11.11.28)

## 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 AES.

```
change node-names ip                                     Page 1 of 2
```

IP NODE NAMES	
Name	IP Address
aes8	10.64.110.132
ams8	10.64.110.136
cms18	10.64.110.20
default	0.0.0.0
egw1	10.64.110.200
egw2	10.64.110.201
<b>procr</b>	<b>10.64.110.131</b>
procr6	::
sm8	10.64.110.135

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	Local Port	Remote Node	Remote Port
<b>AESVCS</b>	<b>y</b>	<b>procr</b>	<b>8765</b>		

On **Page 3**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES 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 AES server in **Section 6.2**.

```
change ip-services                                     Page 3 of 3
```

AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
<b>1:</b>	<b>aes8</b>	<b>*</b>	<b>y</b>	<b>idle</b>
<b>2:</b>				

## 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 MediCall extensions.

```
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: *****
```

## 5.3. Configure Stations

During the compliance testing three extensions were configured for MediCall. Two extensions were used by MediCall application for controlling Avaya Endpoints and the third one for Call Park. Enter the **change station n** command, where **n** is an available extension.

Extensions 10031 and 10032 were used by MediCall for controlling Avaya Endpoints. On **Page 1** of the **station** form, enter a phone **Type** and **Port**, 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 MediCall application. Additionally, set **Button Modules** to **2**.

```
change station 10031                                         Page 1 of 5
                    STATION

Extension: 10031      Lock Messages? n      BCC: 0
  Type: 9608          Security Code: *      TN: 1
  Port: S00081       Coverage Path 1:      COR: 1
  Name: MediCall 1   Coverage Path 2:      COS: 1
Unicode Name? n      Hunt-to Station:      Tests? y
STATION OPTIONS

                    Time of Day Lock Table:
  Loss Group: 19     Personalized Ringing Pattern: 1
                    Message Lamp Ext: 10031
  Speakerphone: 2-way      Mute Button Enabled? y
  Display Language: english      Button Modules: 2
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 2, set Auto Select Any Idle Appearance to y.

```

change station 10031                                     Page 2 of 5
                                     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: 10031                     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, 6 and 7 of the station forms, configure the following **BUTTON ASSIGNMENTS** in addition to the call-appr (call appearance) buttons as shown below

```

change station 10031                                     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
BUTTON ASSIGNMENTS
    1: call-appr                                5: call-appr
    2: call-appr                                6: q-calls   Grp: 1
    3: call-appr                                7:
    4: call-appr                                8:

change station 10031                                     Page 5 of 7
                                     STATION
BUTTON ASSIGNMENTS
    9:
    10:

```



11:  
12:  
13:  
14:  
15:  
16:  
17:  
18:  
19:  
20:  
21:  
22:  
23:  
24:

change station 10031

Page 6 of 7

STATION

BUTTON MODULE #1 ASSIGNMENTS

1: brdg-appr	B:1	E:50001	13: brdg-appr	B:1	E:50002
2: brdg-appr	B:2	E:50001	14: brdg-appr	B:2	E:50002
3: brdg-appr	B:3	E:50001	15:		
4: brdg-appr	B:4	E:50001	16:		
5: brdg-appr	B:5	E:50001	17:		
6: brdg-appr	B:6	E:50001	18:		
7:			19:		
8: abrv-dial	List: 1	DC: 01	20:		
9: auto-in		Grp:	21:		
10: aux-work	RC:	Grp:	22:		
11: after-call		Grp:	23:		
12:			24:		

change station 10031

Page 7 of 7

STATION

BUTTON MODULE #2 ASSIGNMENTS

1: brdg-appr	B:1	E:50003	13: brdg-appr	B:1	E:50004
2:			14: brdg-appr	B:2	E:50004
3:			15: brdg-appr	B:3	E:50004
4:			16: brdg-appr	B:4	E:50004
5: abrv-dial	List: 1	DC: 02	17: brdg-appr	B:5	E:50004
6:			18:		
7:			19:		
8:			20:		
9:			21:		
10:			22:		
11:			23: togle-swap		
12:			24: release		

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

## 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 an available **Group Extension** as per the dial plan. Also, set **ACD**, **Queue** and **Vector** to **y**. The Hunt group configured here will be used by contact center agents to log onto ACD.

<code>add hunt-group 21</code>	<b>HUNT GROUP</b>	<b>Page 1 of 4</b>
Group Number: 21	ACD? y	
<b>Group Name: Hunt Group 21</b>	Queue? y	
<b>Group Extension: 12021</b>	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 VDN

Use the **add vdn *n*** command to add a new VDN, where *n* is an available extension as per the dial plan. Note that all VDNs used the same vector.

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

```
change vdn 12221                                     Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER
                                                    Extension: 12221                               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                                     Page 1 of 6
                                                    CALL VECTOR
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 ringback
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 MediCall to log onto ACD. During the compliance test, two agent extensions were added, 12031 and 12032. On **Page 1**, specify a name of the agent.

```

add agent-loginID 12031                                     Page 1 of 2
                                AGENT LOGINID

Login ID: 12031                               Unicode Name? n   AAS? n
Name: Medical1 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 12031                                     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          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 Application Enablement Services

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

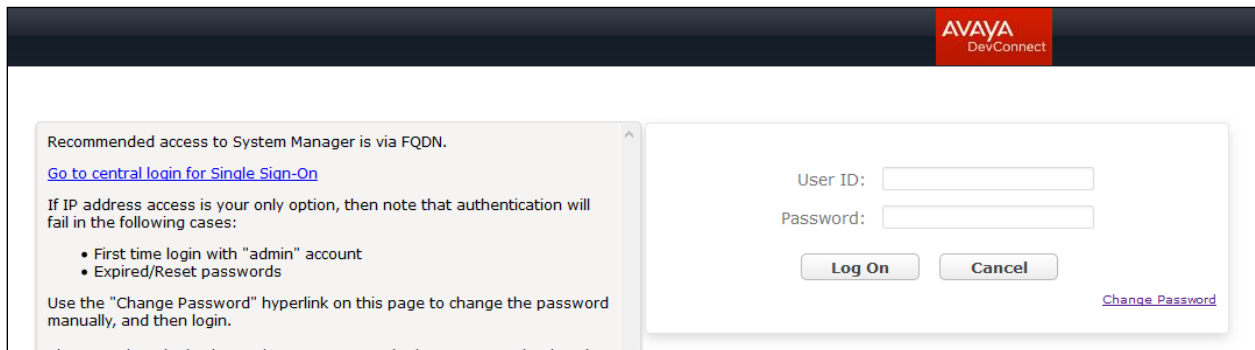
This section assumes that installation and basic administration of the AES server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, a DMCC port.

### 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 AES 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.



Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

User ID:


Password:

[Change Password](#)

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.

13 Items  Show <input type="text" value="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;jcc;premio;tn8400;laptop;CtiS

## 6.2. 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 shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: Welcome: User cust, Last login: Wed May 8 12:54:40 2019 from 10.64.10.47, Number of prior failed login attempts: 0, HostName/IP: aes8/10.64.110.132, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 8.0.1.0.2.5-0, Server Date and Time: Thu May 09 16:24:43 MDT 2019, HA Status: Not Configured. The navigation bar includes 'User Management | User Admin | List All Users' and 'Home | Help | Logout'. The left sidebar shows a tree view with 'User Management' expanded to 'User Admin', where 'Add User' is selected. The main content area is titled 'Edit User' and contains the following fields: \* User Id (spokmcs), \* Common Name (spokmcs), \* Surname (spokmcs), User Password (masked with dots), Confirm Password (masked with dots), Admin Note (empty), Avaya Role (None), Business Category (empty), Car License (empty), CM Home (empty), Css Home (empty), CT User (Yes), and Department Number (empty). A red box highlights the \* User Id, \* Common Name, \* Surname, User Password, Confirm Password, and CT User fields.

The above information (User ID and User Password) must match with the information configured in the Spok MediCall 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.

The screenshot displays the Avaya Application Enablement Services Management Console interface. At the top right, a welcome message and system information are shown: "Welcome: User cust", "Last login: Wed May 8 12:54:40 2019 from 10.64.10.47", "Number of prior failed login attempts: 0", "HostName/IP: aes8/10.64.110.132", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 8.0.1.0.2.5-0", "Server Date and Time: Thu May 09 16:26:25 MDT 2019", and "HA Status: Not Configured".

The main navigation bar includes "Security | Security Database | CTI Users | List All Users" and "Home | Help | Logout". The left sidebar lists various services, with "Security" expanded to show "Security Database".

The "Edit CTI User" form is the central focus. It contains the following fields and controls:

- User Profile:**
  - User ID: spokmcs
  - Common Name: spokmcs
  - Worktop Name: NONE (dropdown)
  - Unrestricted Access**:  (checkbox, highlighted with a red box)
- Call and Device Control:**
  - Call Origination/Termination and Device Status: None (dropdown)
- Call and Device Monitoring:**
  - Device Monitoring: None (dropdown)
  - Calls On A Device Monitoring: None (dropdown)
  - Call Monitoring:  (checkbox)
- Routing Control:**
  - Allow Routing on Listed Devices: None (dropdown)

At the bottom of the form are two buttons: "Apply Changes" and "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.

Welcome: User cust  
Last login: Wed May 8 12:54:40 2019 from 10.64.10.47  
Number of prior failed login attempts: 0  
HostName/IP: aes8/10.64.110.132  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.0.1.0.2.5-0  
Server Date and Time: Thu May 09 16:27:55 MDT 2019  
HA Status: Not Configured

**AVAYA** Application Enablement Services Management Console

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

			Enabled	Disabled
Unencrypted TCP Port	9999		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>		<input checked="" type="radio"/>	<input type="radio"/>

DLG Port

TCP Port	5678			
----------	------	--	--	--

TSAPI Ports

			Enabled	Disabled
TSAPI Service Port	450		<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports				
TCP Port Min	1024			
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	<input type="text" value="1050"/>			
TCP Port Max	<input type="text" value="1065"/>			
Encrypted TLINK Ports				
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			

DMCC Server Ports

			Enabled	Disabled
Unencrypted Port	<input type="text" value="4721"/>		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>		<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	<input type="text" value="4723"/>		<input type="radio"/>	<input checked="" type="radio"/>

## 7. Configure Spok MediCall

Spok installs, configures, and customizes the MediCall applications for their end customers. Spok MediCall integrates with Spok CTI Layer, which is a middleware between Spok MediCall and AES, to control and monitor the phone states. Thus, only the Spok CTI layer will be discussed in these Application Notes.

**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. Provide the following information:

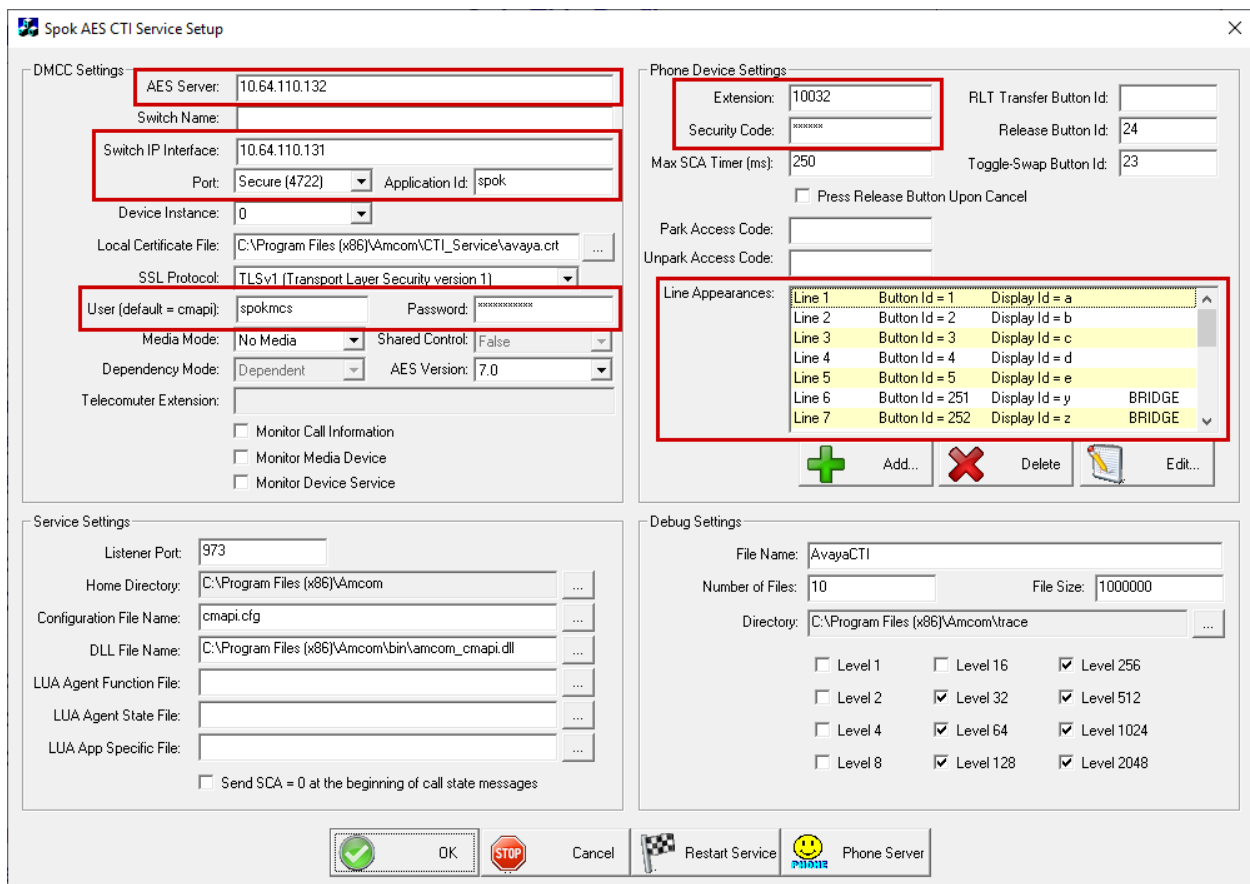
Under DMCC Settings

- **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.
- **User** – Enter the user name created for MediCall from **Section 6.2**.
- **Password** – Enter the password created for MediCall from **Section 6.2**.

Under Phone Device Settings

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

**Note:** There were two MediCall consoles used during the compliance tests. Though, the screen capture below shows DMCC Port as Secure for this MediCall console, another Medical console was configured as Unsecure.



## 8. Verification Steps

The following steps may be used to verify the configuration:

- From the Spok client computers, ping IP interfaces, in particular the AES 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.
- Verify MediCall is successfully connected to AES via AES Management console. Navigate to **Status → Status and Control → DMCC Service Summary**. Verify the State of MediCall user is **REGISTERED**.

**DMCC Service Summary - Session Detail**

Enable page refresh every  seconds

**Detailed Session View**  
Generated on Mon May 13 12:42:25 MDT 2019

Session ID: 2CE891DCBAA33E07767BD11EDD08E950-2  
State: Active  
Time Established: Tue, May 7, 2019 10:01:44 AM GMT-07:00  
Uptime: 6 days, 2 hours, 40 minutes, and 41 seconds  
Cleanup Delay Timer: 60 seconds  
Session Duration Timer: 180 seconds  
Time of Most Recent Timer Reset: Mon, May 13, 2019 12:41:53 PM MDT  
Reconnect Counter: 0

**Devices Associated with Session**

<input type="checkbox"/>	Device ID	State
<input type="checkbox"/>	10031:cm8:10.64.110.131:0	REGISTERED

Item 1-1 of 1

- Place and answer calls from the controlled telephones manually and using MediCall to verify consistency.

MediCall™ Operator Console 11.11.28

Extension: 55001

a=CC Agent 1 55001  
F01112031

55001	10031	10031	10031
50001	50001	50002	50002

**Lookup**

**MediCall™ Directory**

## 9. Conclusion

These Application Notes described a compliance-tested configuration comprised of Communication Manager, AES, Avaya IP endpoints, 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 endpoints 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 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>.

---

**©2019 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).