



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Spok Smart Console, utilizing Spok CTI Layer, with Avaya Aura<sup>®</sup> Communication Manager and Avaya Aura<sup>®</sup> Application Enablement Services - Issue 1.1

## Abstract

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura<sup>®</sup> Communication Manager, Avaya Aura<sup>®</sup> Application Enablement Services, Avaya IP Telephones, and Spok Smart Console desktop application.

Spok Smart Console allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). Spok Smart Console integrates with Spok CTI Layer, which is a middleware between Spok Smart Console and Avaya Aura<sup>®</sup> 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<sup>®</sup> Communication Manager, Avaya Aura<sup>®</sup> Application Enablement Services (AES), Avaya IP (J169/J179) Telephones, and Spok Smart Console applications.

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

The Spok CTI Layer service uses the AES Device and Media Call Control (DMCC) 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 Smart Console in turn uses the Spok CTI Layer service to control and monitor the physical telephone. The Spok Smart Console application regularly provides the Database server with call and lamp state information concerning the controlled 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 Smart Console to perform off-hook, on-hook, dial, answer, hold, retrieve, transfer, conference, and release operations on the physical telephone.
- Spok Smart Console and manual telephone operations may be used interchangeably; for example, go off-hook using Spok Smart Console and manually dial digits.
- Display and call information on the physical telephone is accurately reflected in the Spok Smart Console GUI.
- Call states are consistent between Spok Smart Console and the physical telephone.
- Call Park and retrieve from Spok Smart Console.

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.

## **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 Smart Console, AES, and Communication Manager.

## **2.2. Test Results**

All test cases were executed and passed.

## **2.3. Support**

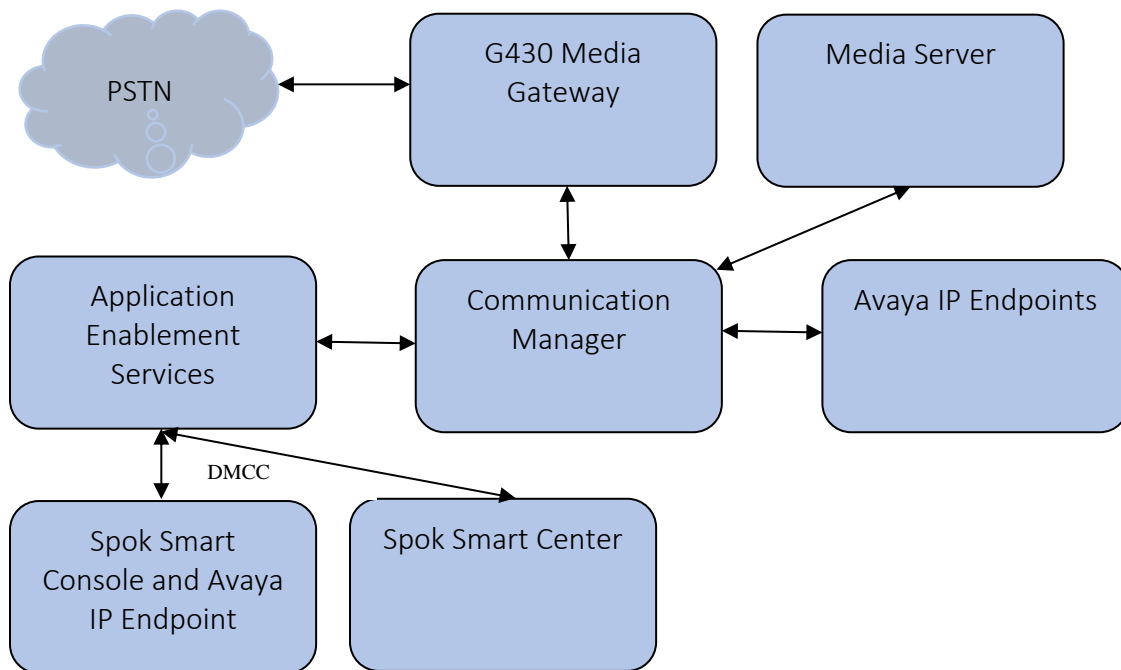
Technical support for the Spok Smart Console solution can be obtained by contacting Spok:

- 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 AES, Communication Manager, Media Server and Avaya G430 Media Gateway. Spok Smart Console 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 Smart Console 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 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 Smart Console		7.x (7.11.0179) 7.1.2
Spok CTI Layer		7.x (7.0.0.6) 7.4

## 5. Configure Avaya Aura® Communication Manager

This section describes the procedures for configuring Feature Access Codes, 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 Feature Access Codes (FAC)

Enter the **change feature-access-codes** command. On **Page 1** of the FEATURE ACCESS CODE (FAC) form, assign or verify the **Call Park Access Code** and **Answer Back Access Code** as shown below. These FACs are used by Spok Smart Console for invoking Call Park related features.

change feature-access-codes		Page 1 of 12
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: <u>*01</u>		
<b>Answer Back Access Code: <u>#25</u></b>		
Auto Alternate Routing (AAR) Access Code: <u>8</u>		
Auto Route Selection (ARS) - Access Code 1: <u>9</u>		Access Code 2:
Automatic Callback Activation: _____		Deactivation: _____
Call Forwarding Activation Busy/DA: _____ All: <u>*69</u>		Deactivation: <u>#69</u>
Call Forwarding Enhanced Status: _____ Act: _____		Deactivation: _____
<b>Call Park Access Code: <u>*25</u></b>		
Call Pickup Access Code: <u>*70</u>		
CAS Remote Hold/Answer Hold-Unhold Access Code:		
CDR Account Code Access Code:		
Change COR Access Code:		
Change Coverage Access Code:		
Conditional Call Extend Activation: _____		Deactivation: _____
Contact Closure Open Code: _____		Close Code: _____

### 5.2. Configure System Parameters Features

Enter the **change system-parameters features** command. Verify **Call Park Timeout Interval (minutes)** is set to **10**. This parameter allows the call to be placed back into the ACD after the timeout interval is reached.

change system-parameters features		Page 1 of 19
FEATURE-RELATED SYSTEM PARAMETERS		
Self Station Display Enabled? n		
Trunk-to-Trunk Transfer: all		
Automatic Callback with Called Party Queuing? n		
Automatic Callback - No Answer Timeout Interval (rings): 3		
<b>Call Park Timeout Interval (minutes): 10</b>		
Off-Premises Tone Detect Timeout Interval (seconds): 20		
AAR/ARS Dial Tone Required? y		
Music (or Silence) on Transferred Trunk Calls? all		
DID/Tie/ISDN/SIP Intercept Treatment: attendant		
Internal Auto-Answer of Attd-Extended/Transferred Calls: none		
Automatic Circuit Assurance (ACA) Enabled? n		

~~Additionally, the **Auto Hold** and **Transfer Upon Hang-Up** features are required.~~

### 5.3. Configure COS

[illegible]

## 5.4. Configure Console Parameters

Spok Smart Console parks calls on the Common Share Extensions. Use the **change console-parameters** command to configure the **COMMON SHARED EXTENSIONS** on **Page 2**. Set the **Starting Extension** to range of the starting extension and set the **Count** to the number of extensions. During the compliance testing extensions 31121-31126 were used.

<b>change console-parameters</b>	Page 2 of 5
CONSOLE PARAMETERS	
TIMING	
Time Reminder on Hold (sec): <u>30</u>	Return Call Timeout (sec): <u>30</u>
Time in Queue Warning (sec): <u>    </u>	Overflow Timer to Group Queue (sec): <u>    </u>
INCOMING CALL REMINDERS	
No Answer Timeout (sec): <u>    </u>	Alerting (sec): <u>    </u>
Secondary Alert on Held Reminder Calls? <u>y</u>	
ABBREVIATED DIALING	
List1: <u>                    </u>	List2: <u>                    </u>
SAC Notification? <u>n</u>	
COMMON SHARED EXTENSIONS	
Starting Extension: <u>31121</u> Count: <u>6</u>	
Busy Indicator for Call Parked on Analog Station Without Hardware? <u>y</u>	

## 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. These codes will be used by Spok Smart Console extensions.

<b>add abbreviated-dialing system</b>	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>	
<b>DIAL CODE</b>	<b>LABELS (FOR STATIONS THAT DOWNLOAD LABELS)</b>
01: <u>*54</u>	01: <u>Log-in</u>
02: <u>*55</u>	02: <u>Log-out</u>
03: <u>                    </u>	03: <u>*****</u>
04: <u>                    </u>	04: <u>*****</u>
05: <u>                    </u>	05: <u>*****</u>



## 5.6. Configure Stations

During the compliance testing two extensions were configured for Spok Smart Console, 30011 for the Attendant's station, and 30015 for Call Park. Enter the **change station *n*** command, where *n* is the extension of a station.

Extensions 30011 was used by Spok Smart Console for controlling an Avaya Endpoint. 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 Smart Console application. Note that J100 series phones use 9611 as station type for H.323 firmware configurations.

change station 30011		Page 1 of 5
STATION		
Extension: 30011	Lock Messages? <u>n</u>	BCC: 0
<b>Type: 9611</b>	<b>Security Code: *</b>	TN: <u>1</u>
Port: S000004	Coverage Path 1: _____	COR: <u>1</u>
<b>Name: Spok1</b>	Coverage Path 2: _____	COS: <u>1</u>
Unicode Name? <u>n</u>	Hunt-to Station: _____	Tests? <u>y</u>
STATION OPTIONS		
Loss Group: <u>19</u>	Time of Day Lock Table:	
	Personalized Ringing Pattern: <u>1</u>	
Speakerphone: <u>2-way</u>	Message Lamp Ext: <u>30011</u>	
Display Language: <u>english</u>	Mute Button Enabled? <u>y</u>	
Survivable GK Node Name:	Button Modules: <u>0</u>	
Survivable COR: <u>internal</u>	Media Complex Ext:	
Survivable Trunk Dest? <u>y</u>	<b>IP SoftPhone? <u>y</u></b>	
	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 30011	Page 2 of 5
STATION	
FEATURE OPTIONS	
LWC Reception: spe	<b>Auto Select Any Idle Appearance? y</b>
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: 52001	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.

<b>change station 30011</b>	STATION	Page 4 of 5
SITE DATA		
Room:		Headset? n
Jack:		Speaker? n
Cable:		Mounting: d
Floor:		Cord Length: 0
Building:		Set Color:
ABBREVIATED DIALING		
List1: <u>system</u>	List2: _____	List3:
BUTTON ASSIGNMENTS		
1:call-appr	5:brdg-appr	B:1 E:30002
2:call-appr	6:brdg-appr	B:2 E:30002
3:brdg-appr B:1 E:30001	7:abrv-dial	List: 1 DC: 01 HL? n
4:brdg-appr B:2 E:30001	8:auto-in	Grp:
<b>change station 30011</b>	STATION	Page 5 of 5
BUTTON ASSIGNMENTS		
9: aux-work	RC:	Grp:
10: abrv-dial	List: 1	DC: 02
11:		
12: dn-dst		
13:		
14:		
15:		
16:		
17:		
18:		
19:		
20:		
21:		
22:		
23: togle-swap		
24: release		

During the compliance testing, extension 30015 was used by Spok Smart Console for Call Park. 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 Smart Console application. Again, this was a J169\179 H.323 set so 9611 station type was used.

change station 30015		Page 1 of 5
STATION		
Extension: 30015	Lock Messages? n	BCC: 0
<b>Type: 9611</b>	<b>Security Code: *</b>	TN: 1
Port: IP	Coverage Path 1:	COR: 1
<b>Name: Spok Smart Console Call Park</b>	Coverage Path 2:	COS: 1
Unicode Name? n	Hunt-to Station:	Tests? y
STATION OPTIONS		
Loss Group: 19	Time of Day Lock Table:	
	Personalized Ringing Pattern: 1	
Speakerphone: 2-way	Message Lamp Ext: 30015	
Display Language: english	Mute Button Enabled? y	
Survivable GK Node Name:	Button Modules: 0	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	<b>IP SoftPhone? y</b>	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

On **Page 2**, set **Auto Select Any Idle Appearance** to **y**, set **Auto Answer** to **none** and set **Restrict Last Appearance** to **y**.

change station 30015		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	<b>Auto Select Any Idle Appearance? y</b>	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	<b>Auto Answer: none</b>	
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	<b>Restrict Last Appearance? y</b>	
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: 30015	Always Use? n IP Audio Hairpinning? N	

On **Pages 4** of the station form, configure the following **BUTTON ASSIGNMENTS** in addition to the **call-appr** (call appearance) buttons as shown below. Note that buttons 3 to 8 are the Common Shared Extensions configured in **Section 5.4**. These extensions are used for parking calls. For each of these extensions, a corresponding companion extension is configured on buttons 9-14. Configuration for the companion extension is shown next in this section.

<b>change station 30015</b>	<b>STATION</b>	Page 4 of 5
SITE DATA		
Room: _____		Headset? <u>n</u>
Jack: _____		Speaker? <u>n</u>
Cable: _____		Mounting: <u>d</u>
Floor: _____		Cord Length: <u>0</u>
Building: _____		Set Color: _____
ABBREVIATED DIALING		
List1: system	List2: _____	List3: _____
<b>BUTTON ASSIGNMENTS</b>		
1:call-appr	5:busy-ind	TAC/Ext: 31123
2:call-appr	6:busy-ind	TAC/Ext: 31124
3:busy-ind      TAC/Ext: 31121	7:busy-ind	TAC/Ext: 31125
4:busy-ind      TAC/Ext: 31122	8:busy-ind	TAC/Ext: 31126
voice-mail		
<b>change station 30015</b>	<b>STATION</b>	Page 5 of 6
BUTTON ASSIGNMENTS		
9:abrdg-appr    E:31111		
10:abrdg-appr   E:31112		
11:abrdg-appr   E:31113		
12:abrdg-appr   E:31114		
13:abrdg-appr   E:31115		
14:abrdg-appr   E:31116		
15:		
24:release		

As mentioned in the previous page, extensions 31111-31116 were used as companion extensions. Configure each of these extensions as shown below. On **Page 1** of the **station** form:

- Set **Type** to **2500**
- Set **Port** to **X**
- Type in a descriptive **Name**

```

add station 31111                                     Page 1 of 4
                                     STATION
Extension: 31111                                     Lock Messages? n                                     BCC: 0
Type: 2500                                     Security Code: *                                     TN: 1
Port: X                                     Coverage Path 1:                                            COR: 1
Name: SmartPark Companion Line 1 Coverage Path 2:                                            COS: 1
Unicode Name? n                                     Hunt-to Station:                                            Tests? y
STATION OPTIONS
  XOIP Endpoint type: auto                                     Time of Day Lock Table:
  Loss Group: 1                                     Message Waiting Indicator: none
  Off Premises Station? n
                                     Survivable COR: internal
  Survivable Trunk Dest? y                                     Remote Office Phone? n

```

Following is a list of these Companion Line Stations.

```
list station type 2500
```

STATIONS								
Ext/ Hunt-to	Port/ Type	Name/ Surv GK NN	Move	Room/ Cable	Jack	Cv1/ Cv2	COR/ COS	
31111	X 2500	Spok Park Companion Line 1	no				1	
31112	X 2500	Spok Park Companion Line 2	no				1	
31113	X 2500	Spok Park Companion Line 3	no				1	
31114	X 2500	Spok Park Companion Line 4	no				1	
31115	X 2500	Spok Park Companion Line 5	no				1	
31116	X 2500	Spok Park Companion Line 6	no				1	

## 5.7. 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 Console 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:	

## 5.8. 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**.

<b>add vdn 31501</b>	<b>Page 1 of 3</b>
VECTOR DIRECTORY NUMBER	
Extension: 31501	Unicode Name? n
<b>Name*: Spok VDN</b>	
<b>Destination: Vector Number</b>	<b>21</b>
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:	



## 5.9. 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.

<b>change vector 21</b>	<b>CALL VECTOR</b>	<b>Page 1 of 6</b>
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	
<b>01 wait-time</b>	<b>2    secs hearing ringback</b>	
<b>02 queue-to</b>	<b>skill 21    pri m</b>	
<b>03 wait-time</b>	<b>30   secs hearing music</b>	
<b>04 goto step</b>	<b>2                      if unconditionally</b>	
05		

## 5.10. 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 Smart Console 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	
<b>Name: Spok Agent 1</b>		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	
		<b>Password:</b>	
		<b>Password (enter again):</b>	
		<b>Auto Answer: none</b>	
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:
2:		17:	32:
3:		18:	33:
4:		19:	34:
			46:
			47:
			48:
			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.

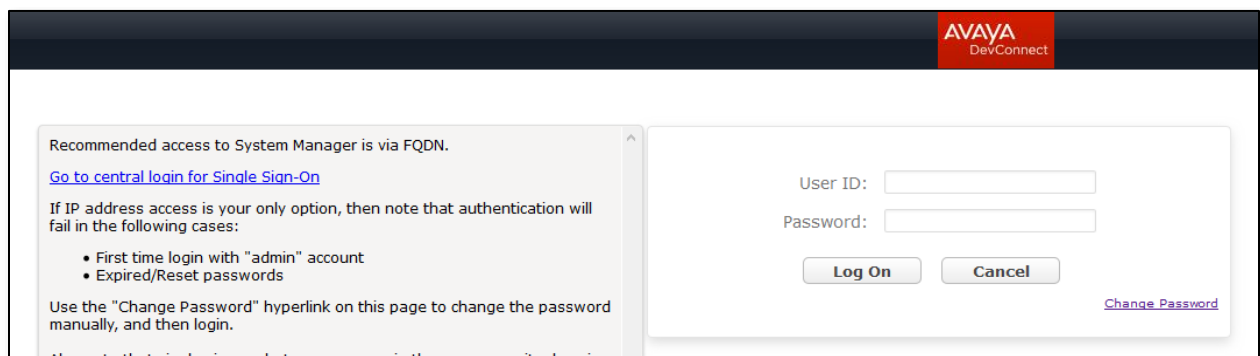
This section assumes that installation and basic administration of the AES server has been performed. The steps in this section describe the configuration of a CTI user, a DMCC port and TLS Version and Root Certificate and Tlink information.

### 6.1. Device and Media Call Control API Station Licenses

The Spok Smart 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 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 Smart Console application requires a station for the Parking Extension in addition to the stations used by 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.

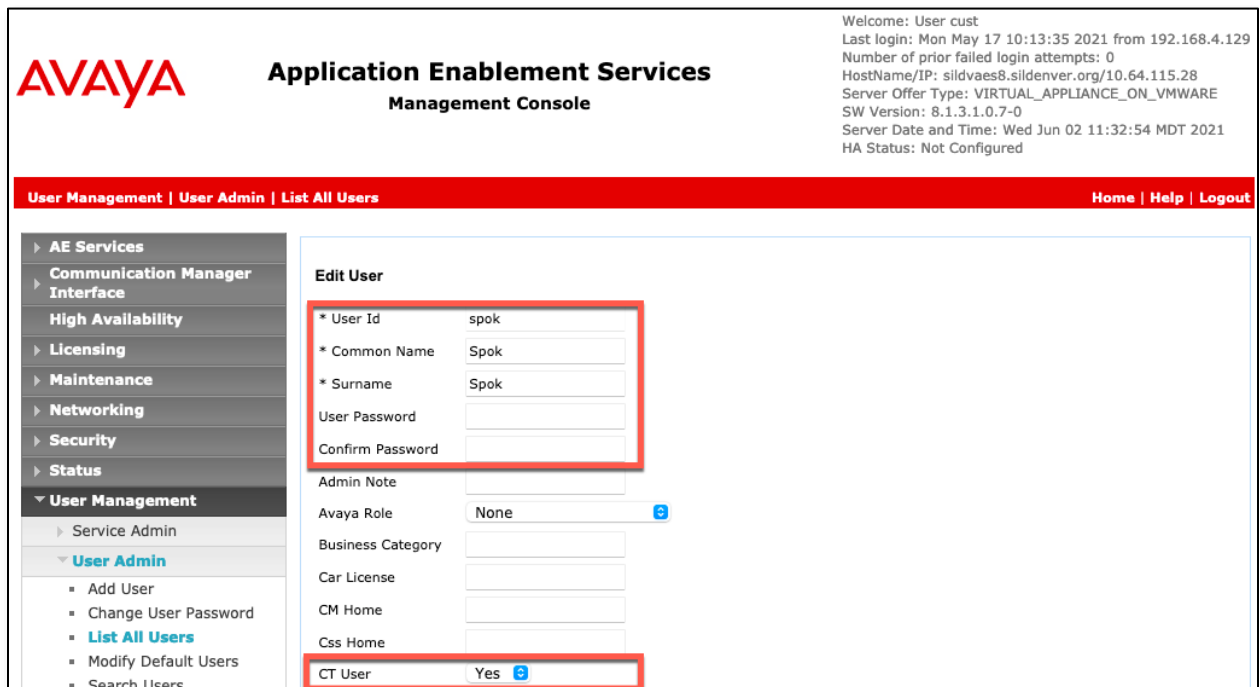
13 Items  Show <span>All</span> 		
Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	1000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	8
AES HA LARGE VALUE_AES_HA_LARGE	permanent	8
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	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 Users

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 Smart Console 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 right corner shows system information: 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 11:35:53 MDT 2021, HA Status: Not Configured.

The main navigation bar includes links for Security, Security Database, CTI Users, and List All Users. The left sidebar lists various services under the Security category, with 'Security' currently selected.

The 'Edit CTI User' form is displayed, showing the following fields and values:

User Profile:	
User ID	spok
Common Name	Spok
Worktop Name	NONE
Unrestricted Access	<input checked="" type="checkbox"/>

Below the user profile, there are sections for Call and Device Control, Call and Device Monitoring, and Routing Control, each with a dropdown menu set to 'None'.

At the bottom of the form, there are buttons for 'Apply Changes' and 'Cancel Changes'.

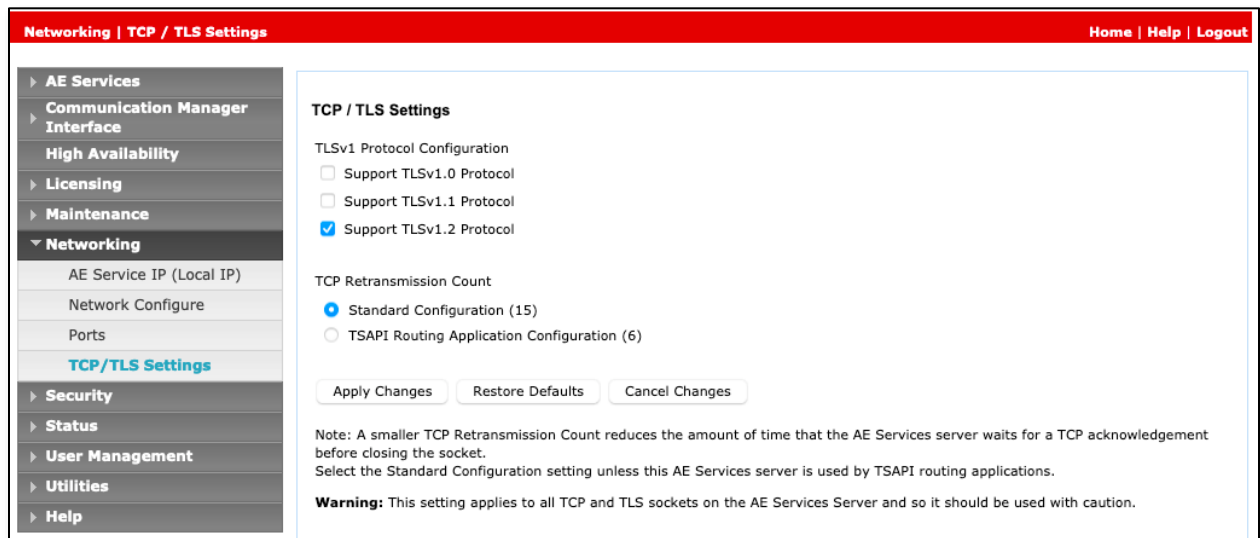
### 6.3. Configure the DMCC Port

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.

Ports		
<b>CVLAN Ports</b>		
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"/>
<b>DLG Port</b>		
TCP Port	5678	
<b>TSAPI Ports</b>		
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	
<b>DMCC Server Ports</b>		
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"/>

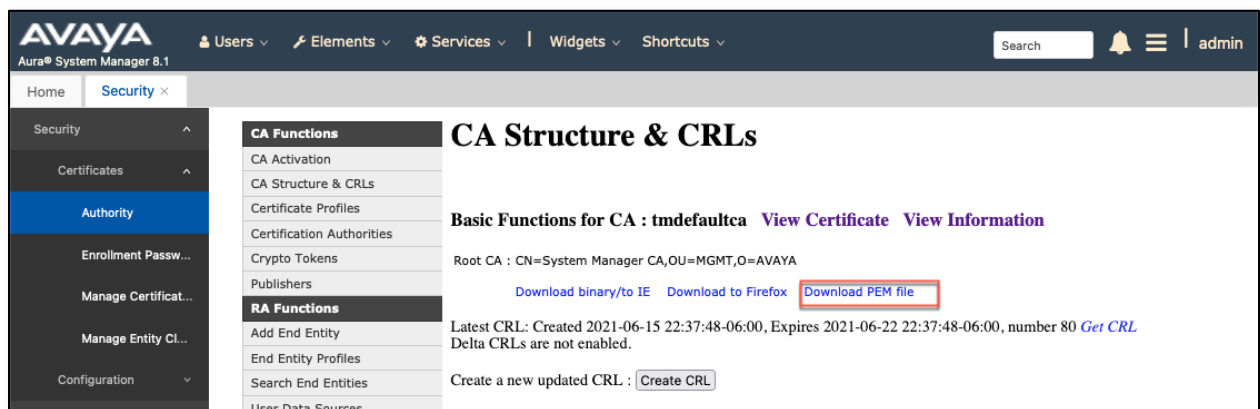
## 6.4. Configure TLS Version

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 Smart Console.



## 6.5. Obtain Root Certificate

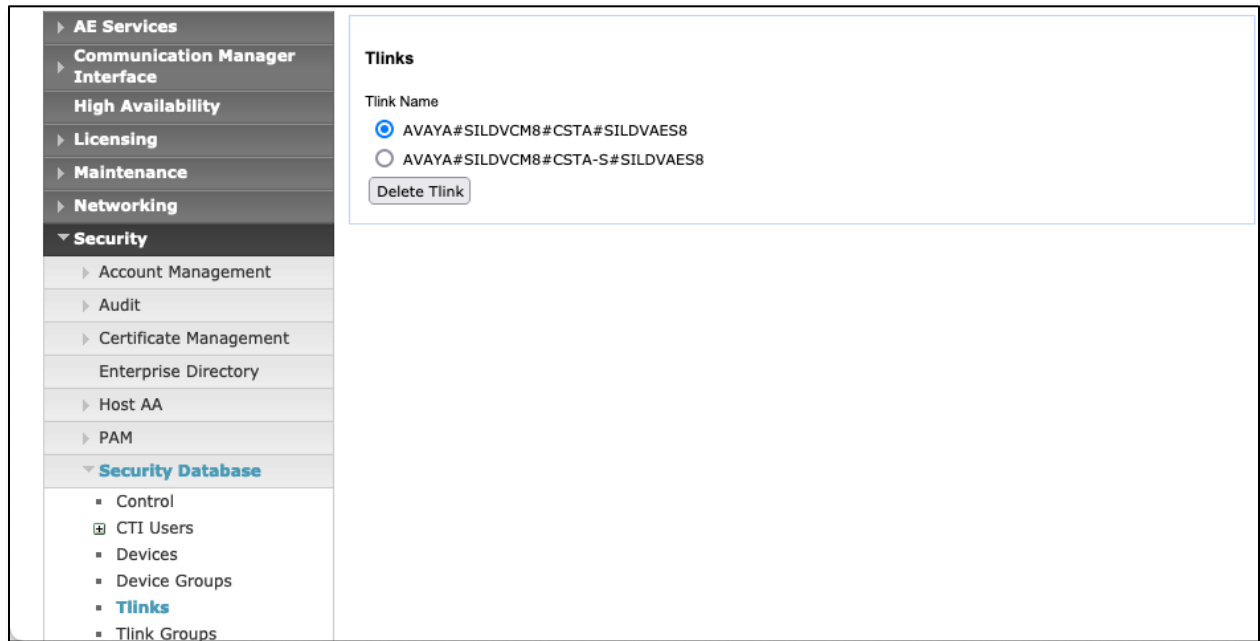
In order to configure the application to use secure links, download the root certificate for the environment, in this case Avaya Aura<sup>®</sup> System Manager issued certificates to AES. The following illustrates how to download this from Avaya Aura<sup>®</sup> System Manager.





## 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 Smart Console

Spok installs, configures, and customizes the Spok Smart Console application for their end customers. Spok Smart Console integrates with Spok CTI Layer, which is a middleware installed on the same PC that the Spok Console is installed on, to control and monitor the phone states.

### 7.1. Configure the Spok Smart Console CTI Client

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 Smart Console from **Section 6**.
- **Password** – Enter the password created for Spok Smart Console from **Section 6**.

#### Under Phone Device Settings

- **Extension**: Enter the extension that will be controlled by Spok Smart Console 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**.
- **Line Appearances** – Configure line appearances as per **Section 5**.

The screenshot displays the 'Spok AES CTI Service Setup' window, which is divided into four main sections: DMCC Settings, Phone Device Settings, Service Settings, and Debug Settings. The DMCC Settings section includes fields for 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, SSL Protocol (TLSv1.2), User (Spok), Password, Media Mode (No Media), Shared Control (False), Dependency Mode (Dependent), AES Version (7.0), and Telecommuter Extension. The Phone Device Settings section includes fields for Extension (30011), Security Code, RLT Transfer Button Id, Release Button Id (24), Max SCA Timer (ms) (250), Toggle-Swap Button Id (23), Park Access Code (\*25), and Unpark Access Code (#25). The Line Appearances section is a table with 6 lines, each having Button Id, Display Id, and a label (BRIDGE). The Service Settings section includes fields for Listener Port (973), Home Directory, Configuration File Name (cmapi.cfg), DLL File Name, LUA Agent Function File, LUA Agent State File, and LUA App Specific File. The Debug Settings section includes fields for File Name (AvayaAES), Number of Files (10), File Size (10000), and Directory (C:\Program Files (x86)\Amcom\trace). At the bottom, there are checkboxes for Monitor Call Information, Monitor Media Device, and Monitor Device Service, and buttons for OK, Cancel, Restart Service, and Phone Server.

Line	Button Id	Display Id	Label
Line 1	1	a	
Line 2	2	b	
Line 3	3	c	BRIDGE
Line 4	4	d	BRIDGE
Line 5	5	e	BRIDGE
Line 6	6	f	BRIDGE

## 7.2. Configure the Spok Smart Center Server

Spok Smart Console utilizes a Linux application server with an Oracle database for parking calls. The following steps are performed by Spok when deploying the solution.

**Smart Center:** Park Setup form below is used to configure messages that can appear with parked calls.

Oracle Fusion Middleware Forms Services

File Edit Query Setup Admin Operator Statistics Queues and Logs Reports Help Window

ORACLE

Park Setup

Site Name	COG	Timeout Destination	Error Destination
AVAYAAS	AVAYAAS	31500	31500

ID	Time	Type	Message
1	30	WARNING	This is a warning that your call is still holding
2	20	TRANSFER	Your call has timed out and will transfer to the operator

Notifications Devices

Site Name

Record: 1/1

The extensions on the Parking Extension are configured to match the phone configuration in **Section 5.6**.

Oracle Fusion Middleware Forms Services

File Edit Query Setup Admin Operator Statistics Queues and Logs Reports Help Window

ORACLE

Park Setup

Site Name	COG	Timeout Destination	Error Destination
AVAYAAES	AVAYAAES	31500	31500

Device Name

30015

Extensions

Extension	Button	Companion	Button
31121	3	31111	9
31122	4	31112	10
31123	5	31113	11
31124	6	31114	12
31125	7	31115	13

Notifications Devices

Site Name

Record: 1/1

Edit the **cmapi\_parking\_lot.ini**: located on the Linux application server to enable control of the Parking Extension.

```
SLEEP TIME = 1
MAX RESERVE TIME = 120

PARKING SITE = AVAYAAES
COMMUNICATOR TYPE = SOCKET

USER = atms
LOGIN SQL = BEGIN op.login('PARKING LOT', 'PARKING LOT-1'); END;
LOGOUT SQL = BEGIN op.logout; END;

NETWORK HOST =localhost
NETWORK PORT =972
AES SERVER NAME =10.64.115.28
AES SERVER NETWORK PORT =4721
CMAPI USER NAME =Spok
CMAPI PASSWORD =Interop123!
SWITCH NAME =SILDVCM8
SWITCH IP =10.64.115.25
APPLICATION NAME =Spok Avaya AES Parking Lot

PRIMARY DN BUTTON ID =1
OUTDIAL BUTTON ID =2
RELEASE BUTTON ID =24
PHONE SECURITY CODE =123456
HOLD PAUSE =2
ANSWER PAUSE =2
RELEASE PAUSE =2
UNPARK PAUSE =200
UNHOLD PAUSE =250
START TRANSFER PAUSE =500
COMPLETE TRANSFER PAUSE =0
START CONFERENCE PAUSE =1
COMPLETE CONFERENCE PAUSE =0
PARK ACCESS CODE =*25
UNPARK ACCESS CODE =#25
MAX PARK WAIT =120
MAX REPARK WAIT =120
```

## 8. Verification Steps

The following steps may be used to verify the configuration.

### 8.1. Application Enablement Verification Steps

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

AE Services

Communication Manager

Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Log Manager

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Mon Jun 07 10:37:13 MDT 2021

Service Uptime: 62 days, 16 hours 11 minutes

Number of Active Sessions: 2

Number of Sessions Created Since Service Boot: 3865

Number of Existing Devices: 2

Number of Devices Created Since Service Boot: 30

<input type="checkbox"/>	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	69DFC8A5436355AE2 11D6694F34A3127-3868	Spok	spok	10.64.115.41	XML Encrypted	1
<input type="checkbox"/>	CEE8A37FAE552399E 39E543B586BBE94-3870	Spok	Spok Avaya AES Parking Lot	10.64.115.40	XML Unencrypted	1

Terminate Sessions Show Terminated Sessions

Item 1 of 2

AE Services

Communication Manager

Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Log Manager

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

DMCC Service Summary - Device Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

[Session Summary](#) Device Summary

Generated on Mon Jun 07 10:38:23 MDT 2021

Service Uptime: 62 days, 16 hours and 13 minutes

Number of Active Sessions: 2

Number of Sessions Created Since Service Boot: 3865

Number of Existing Devices: 2

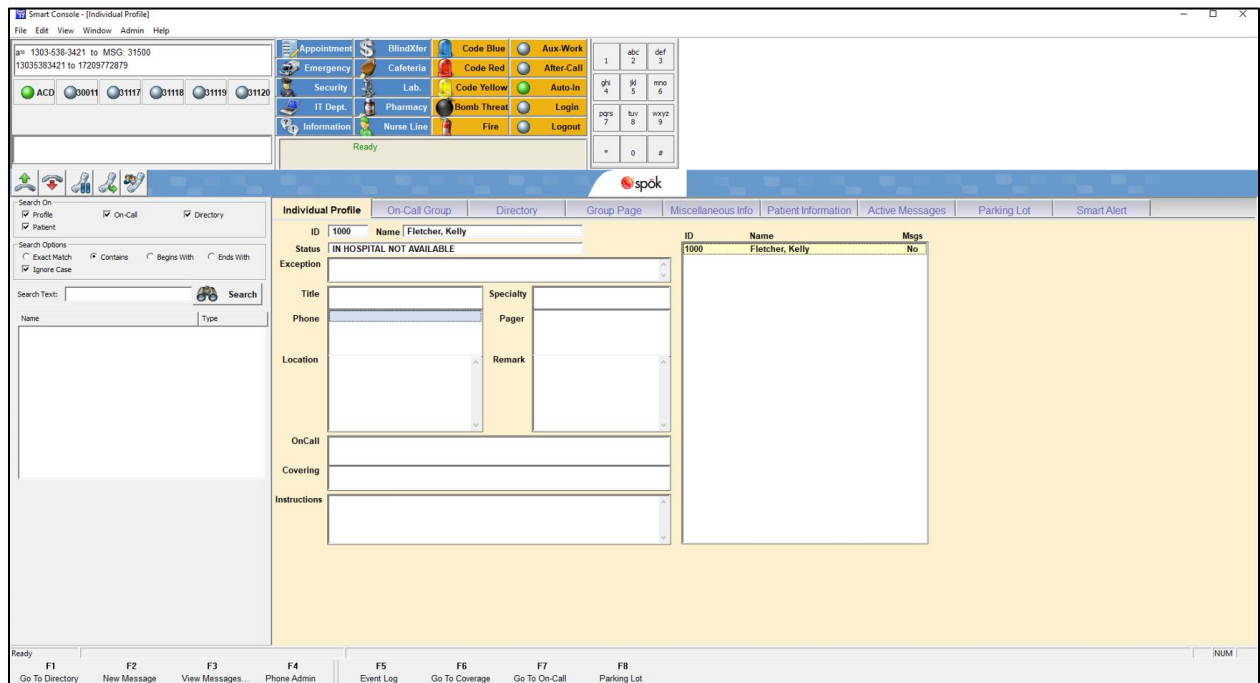
Number of Devices Created Since Service Boot: 30

<input type="checkbox"/>	Device ID	Gatekeeper IP address	State	Associated Sessions
<input type="checkbox"/>	30011:SILDVCM8:10.64.115.25:0	10.64.115.25	REGISTERED	1
<input type="checkbox"/>	30015:SILDVCM8:0.0.0.0:0	10.64.115.25	REGISTERED	1

Terminate Devices

## 8.2. Spok Smart Console Verification Steps

Place and answer calls from the controlled telephones manually and use Spok Smart Console and verify consistency.



## 9. Conclusion

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

## 10. Additional References

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

[1] *Administering Avaya Aura<sup>®</sup> Communication Manager, Release 8.1.x*

[2] *Administering Avaya Aura<sup>®</sup> 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](mailto:devconnect@avaya.com).