



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Spok Console, utilizing Spok CTI Layer, with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services - Issue 1.0

### Abstract

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

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

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services (AES), Avaya IP (9608) and Digital Telephones (9408), and Spok Console applications.

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

It is the Spok CTI Layer service that uses the AES Device and Media Call Control (DMCC) Application Programming Interface (API) to share control of and monitor a physical telephone and receive the same terminal and first party call information received by the physical telephone. Spok Console in turn uses the Spok CTI Layer service to control and monitor a physical telephone. The Spok Console applications regularly provide the Database server with call and lamp state information concerning the controlled telephones.

## 2. General Test Approach and Test Results

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

- The user may successfully use Spok Console to perform off-hook, on-hook, dial, answer, hold, retrieve, transfer, conference, and release operations on the physical telephone.
- Manual operations performed on the physical telephone are correctly reflected in the Spok Console GUI.
- Spok Console and manual telephone operations may be used interchangeably; for example, go off-hook using Spok Console and manually dial digits.
- Display and call information on the physical telephone is accurately reflected in the Spok Console GUI.
- Call states are consistent between Spok Console and the physical telephone.
- Call park and retrieve from Spok 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 Secure 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 Console, 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 Console is lost, the CTI service on Spok Console needed to be manually restarted to register the DMCC station again.

## **2.3. Support**

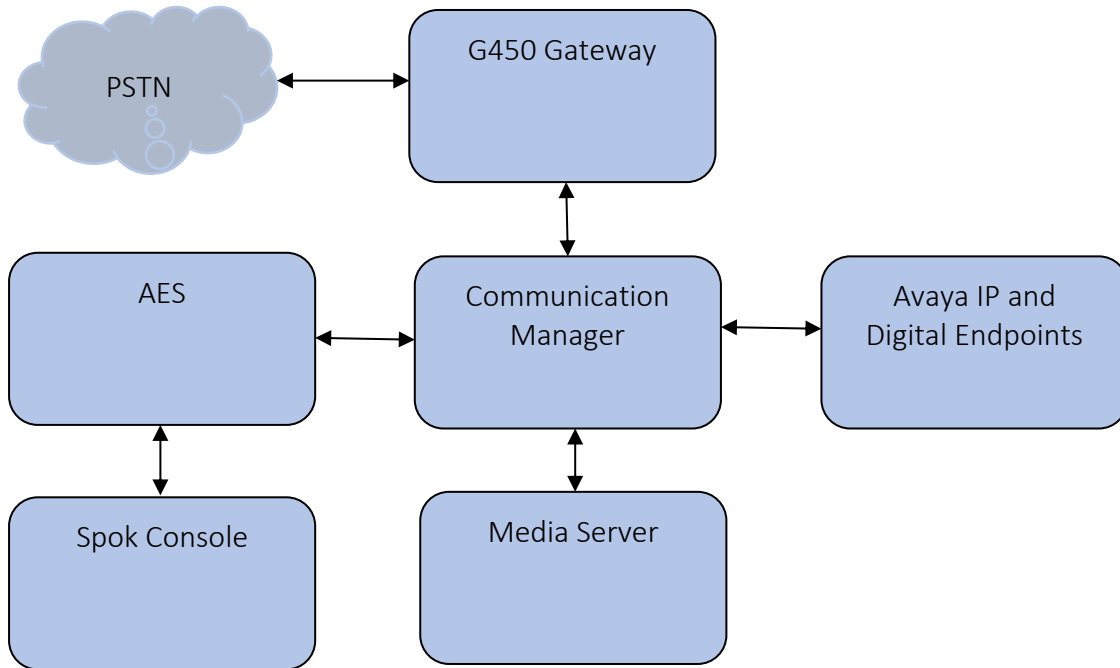
Technical support for the Spok Console solution can be obtained by contacting Spok:

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

### 3. Reference Configuration

**Figure 1** illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with an AES, Communication Manager, Media Server with an Avaya G450 Media Gateway. Spok Console is configured to be in the same network as the enterprise. Endpoints include Avaya 9600 Series H.323 IP Telephones and Avaya Digital Endpoints.

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



**Figure 1: Spok Console Test Configuration**

## 4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya Aura® Communication Manager		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 Endpoints		
	9600 Series (H.323)	6.8102
	9408 Digital	2.0 SP8
Spok CTI Layer		7.x (7.0.0.6)
Spok Console		7.x (7.11.0179)

## 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 Feature Access Codes (FAC)

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

```
change feature-access-codes                                     Page 1 of 11
                                                                FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code:
Abbreviated Dialing List2 Access Code:
Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
Announcement Access Code:
Answer Back Access Code: #25
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code: 8
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
Automatic Callback Activation:                    Deactivation:
Call Forwarding Activation Busy/DA: *11    All: *12    Deactivation: *13
Call Forwarding Enhanced Status:           Act:        Deactivation:
Call Park Access Code: *25
Call Pickup Access Code: #40
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:
```

## 5.3. 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: none
Automatic Callback with Called Party Queuing? n
Automatic Callback - No Answer Timeout Interval (rings): 3
Call Park Timeout Interval (minutes): 10
Off-Premises Tone Detect Timeout Interval (seconds): 20
AAR/ARS Dial Tone Required? y

Music (or Silence) on Transferred Trunk Calls? no
DID/Tie/ISDN/SIP Intercept Treatment: attendant
Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
Automatic Circuit Assurance (ACA) Enabled? n
```

## 5.4. Configure COS

**Console permissions** need to be enabled for Spok Console to have the ability to park calls on Common Shared Extensions. Use the **change cos-group 1** command to set **Console Permissions** and **Trk-to-Trk Transfer Override** to **y** for **COS Group 1**. All extensions used during the compliance testing belonged to **COS Group 1**.

```

change cos-group 1                                     Page 1 of 2
CLASS OF SERVICE          COS Group: 1   COS Name:
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Auto Callback             n y y n y n y n y n y n y n y n
Call Fwd-All Calls       n y n y y n n y y n n y y n n y
Data Privacy              n y n n n n y y y n n n n y y y
Priority Calling          n y n n n n n n n n y y y y y y
Console Permissions    n y n n n n n n n n n n n n n n n
Off-hook Alert           n n n n n n n n n n n n n n n n
Client Room               n n n n n n n n n n n n n n n n
Restrict Call Fwd-Off Net y y y y y y y y y y y y y y y
Call Forwarding Busy/DA  n n n n n n n n n n n n n n n n
Personal Station Access (PSA) n n n n n n n n n n n n n n n n
Extended Forwarding All  n n n n n n n n n n n n n n n n
Extended Forwarding B/DA n n n n n n n n n n n n n n n n
Trk-to-Trk Transfer Override n y n n n n n n n n n n n n n n n
QSIG Call Offer Originations n n n n n n n n n n n n n n n n
Contact Closure Activation n n n n n n n n n n n n n n n n
  
```

## 5.5. Configure Console Parameters

Spok 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 numbers of extensions. During the compliance testing extensions 11121-11126 were used.

```

change console-parameters                             Page 2 of 4
CONSOLE PARAMETERS

TIMING
Time Reminder on Hold (sec): 30                      Return Call Timeout (sec): 30
Time in Queue Warning (sec):                          Overflow Timer to Group Queue (sec):

INCOMING CALL REMINDERS
No Answer Timeout (sec):                              Alerting (sec):
Secondary Alert on Held Reminder Calls? y

ABBREVIATED DIALING
List1: List2: List3:
SAC Notification? n

COMMON SHARED EXTENSIONS
Starting Extension: 11121 Count: 6
Busy Indicator for Call Parked on Analog Station Without Hardware? y
  
```



## 5.6. 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 Console 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: *****
```

## 5.7. Configure Stations

During the compliance testing three extensions were configured for Spok Console. Two extensions were used by Spok Console 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 52001, 10021 and 10022 were used by Spok Console 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 Spok Console application.

```
change station 52001                                         Page 1 of 5
                    STATION

Extension: 52001      Lock Messages? n      BCC: 0
  Type: 9408          Security Code: *      TN: 1
  Port: 001V301      Coverage Path 1:      COR: 1
  Name: Digital Station 1  Coverage Path 2:      COS: 1
Unicode Name? n      Hunt-to Station:

STATION OPTIONS

          Loss Group: 2      Time of Day Lock Table:
          Speakerphone: 2-way  Personalized Ringing Pattern: 1
          Display Language: english  Message Lamp Ext: 52001
          Mute Button Enabled? y
          Button Modules: 0

          Survivable COR: internal
          Survivable Trunk Dest? y      IP SoftPhone? y
          Remote Office Phone? n
          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 52001                                     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: 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

```

change station 52001                                     Page 4 of 5
                                                    STATION

SITE DATA
Room:                                         Headset? n
Jack:                                         Speaker? n
Cable:                                       Mounting: d
Floor:                                       Cord Length: 0
Building:                                    Set Color:

ABBREVIATED DIALING
List1: system                               List2:
                                           List3:

BUTTON ASSIGNMENTS
1: call-appr                                5: brdg-appr B:1 E:50002
2: call-appr                                6: brdg-appr B:2 E:50002
3: brdg-appr B:1 E:50001                    7: abrv-dial List: 1 DC: 01
4: brdg-appr B:2 E:50001                    8: auto-in      Grp:

change station 52001                                     Page 5 of 5
                                                    STATION

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

```

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

During the compliance testing, extension 10023 was used by Spok 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 Console application.

```

change station 10023                                     Page 1 of 5
                                                    STATION
Extension: 10023                                         Lock Messages? n          BCC: 0
  Type: 9608                                           Security Code: *       TN: 1
  Port: S00089                                           Coverage Path 1:         COR: 1
  Name: Spok Console Call Park                       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
    Message Lamp Ext: 10023
    Speakerphone: 2-way                                   Mute Button Enabled? y
    Display Language: english                             Button Modules: 0
Survivable GK Node Name:
  Survivable COR: internal                               Media Complex Ext:
Survivable Trunk Dest? y                                IP SoftPhone? y
                                                    IP Video Softphone? n
Short/Prefixed Registration Allowed: default
                                                    Customizable Labels? y
  
```

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

```

change station 10023                                     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: 720-977-2872                 Always Use? n IP Audio Hairpinning? N
  
```

On **Pages 4** of the station forms, 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 Call Park VDNs as configured in **Section 5.9.2**. These extensions are used for parking calls.

<b>change station 10023</b>		<b>Page 4 of 5</b>	
		STATION	
SITE DATA			
Room:		Headset?	n
Jack:		Speaker?	n
Cable:		Mounting:	d
Floor:		Cord Length:	0
Building:		Set Color:	
ABBREVIATED DIALING			
List1:	List2:	List3:	
BUTTON ASSIGNMENTS			
1: call-appr		5: busy-ind	TAC/Ext: 11113
2: call-appr		6: busy-ind	TAC/Ext: 11114
3: busy-ind	TAC/Ext: 11111	7: busy-ind	TAC/Ext: 11115
4: busy-ind	TAC/Ext: 11112	8: busy-ind	TAC/Ext: 11116
voice-mail			

## 5.8. 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:	

## 5.9. Configure VDNs

There were 3 different sets of VDNs used during the compliance test:

- VDNs for contact center agents to receive ACD calls
- VDNs for Spok Console to retrieve parked calls that are not retrieved
- VDNs for screen pop on Spok Console

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.

### 5.9.1. Contact Center VDN

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:
```

### 5.9.2. Call Park VDN

Add the same numbers of VDNs as the **Common Shared Extensions** configured in **Section 5.5**. During compliance testing 6 extensions, 11111-11116 were added. Note the name must be set to **PLM RCL: [cse]** where **cse** is the value of **Common Shared Extension**.

```
list vdn count 6
                                         VECTOR DIRECTORY NUMBERS
Name (22 characters)  Ext/Skills      VDN          Vec          Orig          Evt
Ovr COR TN          PRT Num      Meas Annc     Noti
Adj

PLM RCL: 11121       11111          n 1 1        V 21         none
PLM RCL: 11122       11112          n 1 1        V 21         none
PLM RCL: 11123       11113          n 1 1        V 21         none
PLM RCL: 11124       11114          n 1 1        V 21         none
PLM RCL: 11125       11115          n 1 1        V 21         none
PLM RCL: 11116       11116          n 1 1        V 21         none
```

### 5.9.3. Screen Pop VDN

During the compliance test one VDN was added for screen pop on Spok Console. On **Page 1**, note that the **Name** must contain the start with **MSG:** for screen pop to appear on Spok Console.

```
change vdn 11201                                     Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER
                                                    Extension: 11201                Unicode Name? n
                                                    Name*: MSG: 11201
                                                    Destination: Vector Number    21
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none          Report Adjunct Calls as ACD*? n

VDN of Origin Annc. Extension*:
1st Skill*:
2nd Skill*:
3rd Skill*:

SIP URI:

* Follows VDN Override Rules
```

### 5.10. 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
```



## 5.11. 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 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.

```

add agent-loginID 12021                                     Page 1 of 2
                                AGENT LOGINID

Login ID: 12021                               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 12021                                     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:       1              17:     32:     47:
3:       1              18:     33:     48:
4:       1              19:     34:     49:

```

## 6. Configure Application Enablement Services

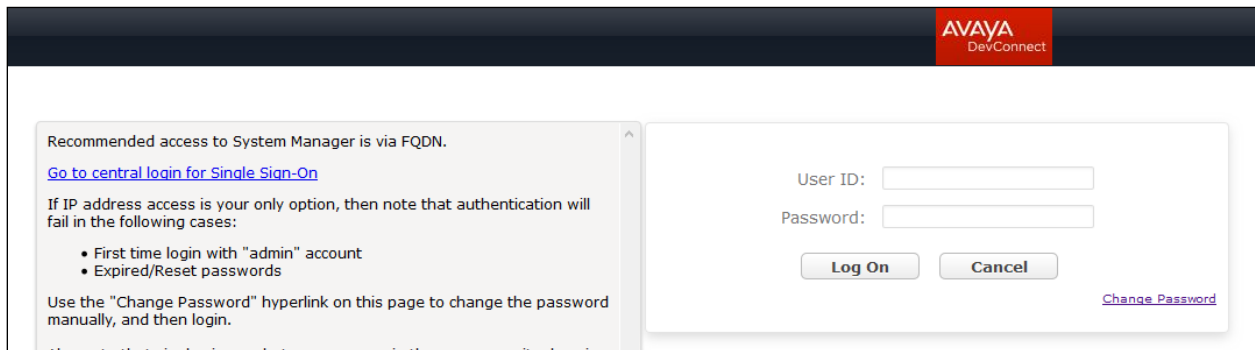
The Application Enablement Services server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager.

This section assumes that installation and basic administration of the 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 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.



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 **Services → 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;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, 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 16:24:02 MDT 2019, HA Status: Not Configured. The navigation bar shows 'User Management | User Admin | List All Users' and 'Home | Help | Logout'. The left sidebar lists various services, with 'User Management' expanded to show 'User Admin' and 'Add User'. The main content area is titled 'Edit User' and contains the following fields: \* User Id (spokscs), \* Common Name (spokscs), \* Surname (spokscs), User Password, Confirm Password, Admin Note, Avaya Role (None), Business Category, Car License, CM Home, and CSS Home. The 'CT User' field is a dropdown menu set to 'Yes'. The 'User Id', 'Common Name', 'Surname', and 'CT User' fields are highlighted with red boxes.

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

Once the user is created, navigate to the **Security** → **Security Database** → **CTI Users** → **List All Users** link from the left pane of the window. Select the User ID created previously, and click the **Edit** button to set the permission of the user (not shown).

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

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 16:26:01 MDT 2019  
HA Status: Not Configured

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

**AVAYA** **Application Enablement Services**  
Management Console

▶ AE Services  
▶ Communication Manager Interface  
▶ High Availability  
▶ Licensing  
▶ Maintenance  
▶ Networking  
▼ Security  
▶ Account Management  
▶ Audit  
▶ Certificate Management  
Enterprise Directory  
▶ Host AA  
▶ PAM  
▼ Security Database  
▶ Control

**Edit CTI User**

User Profile: User ID spokscs  
Common Name spokscs  
Worktop Name NONE ▾  
**Unrestricted Access**

---

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

---

Routing Control: Allow Routing on Listed Devices None ▾

Apply Changes 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.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Networking' > 'Ports'. The main content area displays the 'Ports' configuration page. The 'DMCC Server Ports' section is highlighted with a red box. The configuration includes:

Ports		Enabled	Disabled
<b>CVLAN Ports</b>			
Unencrypted TCP Port	9999	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	9998	<input checked="" type="radio"/>	<input type="radio"/>
<b>DLG Port</b>			
TCP Port	5678		
<b>TSAPI Ports</b>			
TSAPI Service Port	450	<input checked="" type="radio"/>	<input type="radio"/>
<b>Local TLINK Ports</b>			
TCP Port Min	1024		
TCP Port Max	1039		
<b>Unencrypted TLINK Ports</b>			
TCP Port Min	1050		
TCP Port Max	1065		
<b>Encrypted TLINK Ports</b>			
TCP Port Min	1066		
TCP Port Max	1081		
<b>DMCC Server Ports</b>			
Unencrypted Port	4721	<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	4722	<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	4723	<input type="radio"/>	<input checked="" type="radio"/>

## 7. Configure Spok Console

Spok installs, configures, and customizes the Spok Console applications for their end customers. Spok Console integrates with Spok CTI Layer, which is a middleware between Spok Console and AES, 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. 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 Spok Console from **Section 6.2**.
- **Password** – Enter the password created for Spok Console from **Section 6.2**.

Under Phone Device Settings

- **Extension:** Enter the extension that will be controlled by Spok Console from **Section 5.7**.
- **Security Code:** Enter the security code for the controlled station from **Section 5.7**.
- **Release Button** – Enter the Release button assigned for the controlled station from **Section 5.7**.
- **Line Appearances** – Configure line appearances as per **Section 5.7**.

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

**DMCC Settings:**

- AES Server: 10.64.110.132
- Switch Name: [Empty]
- Switch IP Interface: 10.64.110.131
- Port: Secure (4722) | Application Id: spok
- Device Instance: 0
- Local Certificate File: C:\Program Files (x86)\Amcom\CTI\_Service\avaya.crt
- SSL Protocol: TLSv1 (Transport Layer Security version 1)
- User (default = cmapi): spokscs | Password: [Masked]
- Media Mode: No Media | Shared Control: False
- Dependency Mode: Dependent | AES Version: 7.0
- Telecomuter Extension: [Empty]
- Monitor Call Information
- Monitor Media Device
- Monitor Device Service

**Phone Device Settings:**

- Extension: 52001
- Security Code: [Masked]
- Max SCA Timer (ms): 250
- RLT Transfer Button Id: [Empty]
- Release Button Id: 24
- Toggle-Swap Button Id: [Empty]
- Press Release Button Upon Cancel
- Park Access Code: [Empty]
- Unpark Access Code: [Empty]

**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 = 6	Display Id = f

**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: [Empty]
- LUA Agent State File: [Empty]
- LUA App Specific File: [Empty]
- Send SCA = 0 at the beginning of call state messages

**Debug Settings:**

- File Name: AvayaAESCTI
- 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

Buttons: OK, Cancel, Restart Service, Phone Server



## 8. Verification Steps

The following steps may be used to verify the configuration:

- From the Spok client computers, ping IP interfaces, in particular the 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 Communication Manager System Access Terminal (SAT). For the physical Digital telephones, verify that the telephones are attached to the correct ports.
- Verify Spok Console is successfully connected to AES via AES Management console. Navigate to **Status → Status and Control → DMCC Service Summary**. Verify the State of Spok Console user is **REGISTERED**.

**DMCC Service Summary - Session Detail**

Enable page refresh every  seconds

**Detailed Session View**  
Generated on Thu May 09 17:58:57 MDT 2019

Session ID: E8EC13D5A2149AA2CB1E820322350040-12  
State: Active  
Time Established: Thu, May 9, 2019 05:38:05 PM GMT-07:00  
Uptime: 0 days, 0 hours, 20 minutes, and 52 seconds  
Cleanup Delay Timer: 60 seconds  
Session Duration Timer: 180 seconds  
Time of Most Recent Timer Reset: Thu, May 9, 2019 05:58:05 PM MDT  
Reconnect Counter: 0

**Devices Associated with Session**

<input type="checkbox"/>	Device ID	State
<input type="checkbox"/>	10022:cm8:10.64.110.131:0	REGISTERED

Item 1-1 of 1

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

Spok Console - AVAYA1

File Help

User: ADMIN Archive Service \* \* CI

a=Digital Station 1 52001 10022 IN USE 50003 IDLE

Search | Detail | Notes | History

CONSOLE DIREC			
F5->Last Name	F6->First Name	F8->Extension	F9
		225-1741	
		225-1730	
		288-2673	
		281-8298	
		281-8376	
		8298	
		8376	
		545-1665	
		281.8382	

**CALL INFORMATION**

Caller ID: 52001  
 Caller Name: Digital Station 1  
 Called ID:  
 Called Name:  
 Display: a=Digital Station 1 52001  
 Digital Station 1

## 9. Conclusion

These Application Notes described a compliance-tested configuration comprised of Communication Manager, AES, Avaya IP and Digital Telephones, and the Spok Console application. Spok Console allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). During compliance testing, calls were successfully placed to and from Avaya IP and Digital Telephones that were controlled and monitored by the Spok Console application.

## 10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager, Release 8.0.1*

[2] *Administering Avaya Aura® Avaya Aura® Application Enablement Services, Release 8.0.1*

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).