



Avaya Solution & Interoperability Test Lab

Application Notes for Spok MediCall Version 11, utilizing Spok CTI Layer Version 7.4, with Avaya Aura[®] Communication Manager Release 10.1 and Avaya Aura[®] Application Enablement Services Release 10.1 - Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura[®] Communication Manager Release 10.1, Avaya Aura[®] Application Enablement Services Release 10.1, Avaya IP and Digital Telephones, 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 (J189) Telephones, and Spok MediCall applications.

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

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

2. General Test Approach and Test Results

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

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

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

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya

products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the compliance test was primarily on verifying the interoperability between Spok MediCall, AES, and Communication Manager.

2.2. Test Results

All test cases were executed and passed. The following observations are noted in the compliance test.

- The MediCall application only supports attended transfers.
- During a scenario where network connection from Spok MediCall is lost, the CTI service on Spok PC needed to be manually restarted to register the DMCC station again.
- In a scenario where swap hold is performed on a bridged appearance and the call is transferred, the bridged appearance for the line on MediCall Console is not released. That is because the calling party is stilled on hold on the bridged physical phone. This is a known behavior and an internal Avaya ticket has been opened.

2.3. Support

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

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

3. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with an AES, Communication Manager, Media Server and Avaya G430 Media Gateway. Spok MediCall is configured to be in the same network as the enterprise. Endpoints include Avaya J100 Series H.323 IP Telephones and Avaya Digital Endpoints.

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

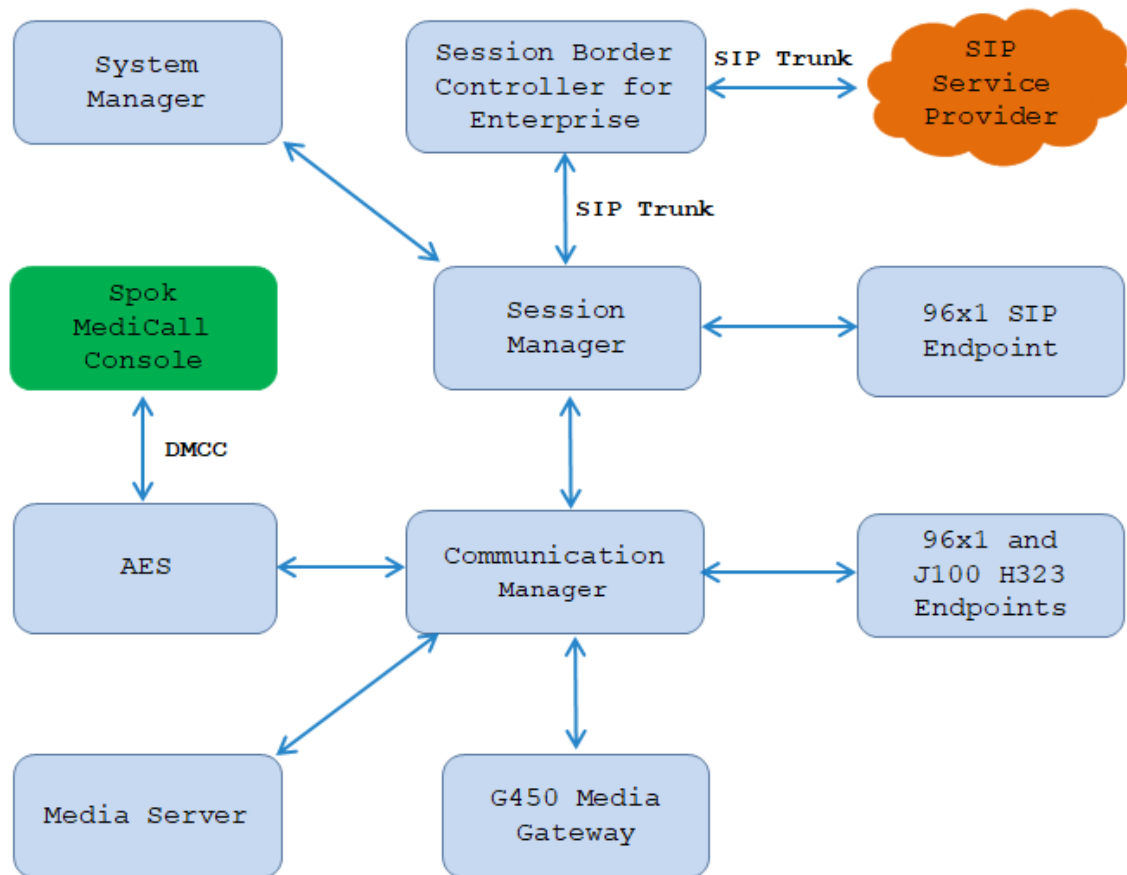


Figure 1: Spok MediCall Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtual Environment	R020x.01.0.974.0 (10.1.0.2.0.974.27607)
Avaya Aura® Session Manager running on Virtual Environment	10.1.0.2.1010215
Avaya Aura® Media Server running on Virtual Environment	8.0.2.218
Avaya G450 Media Gateway	42.08
Avaya Aura® System Manager running on Virtual Environment	10.1.0.2 SP2 Software Update Revision No: 10.1.0.2.0715160 Hot Fix - 1010215160
Avaya Session Border Controller for Enterprise running on Virtual Environment	10.1.1.0-35-21872
Avaya IP Deskphones <ul style="list-style-type: none">- J189 (H.323)- 9641GS (H.323)- 9611G (SIP)	6.8511 6.8511 7.1.9.0.8
Avaya Digital 9408 Deskphone	R20
Spok MediCall Console	11.14.99.99
Spok CTI Layer	7.4.0.93

5. Configure Avaya Aura® Communication Manager

This section describes the procedures for configuring Abbreviated Dialing, and controlled telephones. Standard connectivity was in place for AES and other Avaya components, are not covered in this document.

5.1. 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 Operator 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
      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? 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. Note: Please consult with Spok to confirm which combination of these features will work best in the environment; some combinations may cause rare conflicts.

```
change system-parameters features                               Page 6 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Public Network Trunks on Conference Call: 5               Auto Start? n
      Conference Parties with Public Network Trunks: 6          Auto Hold? y
      Conference Parties without Public Network Trunks: 6        Attendant Tone? y
      Night Service Disconnect Timer (seconds): 180             Bridging Tone? n
      Short Interdigit Timer (seconds): 3                       Conference Tone? n
      Unanswered DID Call Timer (seconds):                      Intrusion Tone? n
      Line Intercept Tone Timer (seconds): 30                   Mode Code Interface? n
      Long Hold Recall Timer (seconds): 0
      Reset Shift Timer (seconds): 0
      Station Call Transfer Recall Timer (seconds): 20          Recall from VDN? n
      Trunk Alerting Tone Interval (seconds): 15
      DID Busy Treatment: tone
      Allow AAR/ARS Access from DID/DIOD? n
      Allow ANI Restriction on AAR/ARS? n
      Use Trunk COR for Outgoing Trunk Disconnect/Alert? n
      7405ND Numeric Terminal Display? n                       7434ND? y
      DISTINCTIVE AUDIBLE ALERTING
      Internal: 1 External: 2 Priority: 3
      Attendant Originated Calls: external
      DTMF Tone Feedback Signal to VRU - Connection:           Disconnection:
```

```

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

CONFERENCE/TRANSFER
    Abort Transfer? n                                           No Dial Tone Conferencing? n
    Transfer Upon Hang-Up? y                               Select Line Appearance Conferencing? n
    Abort Conference? n                                         Unhold? n
    No Hold Conference Timeout: 60    Maximum Ports per Expanded Meet-me Conf: 7
                                         12-party Conferences? n
                                         External Ringing for Calls with Trunks? remote-only
ANALOG BUSY AUTO CALLBACK
    Without Flash? n

AUDIX ONE-STEP RECORDING
    Recording Delay Timer (msec): 500
Apply Ready Indication Tone To Which Parties In The Call? all
    Interval For Applying Periodic Alerting Tone (seconds): 15
                                         Audix Recording Display? n
POSTED MESSAGE
    Require Security Code? n

```

5.2. Configure Abbreviated Dialing

Enter the **add abbreviated-dialing system** command. In the **DIAL CODE** list, enter the Feature Access Codes for ACD Login and Logout. These codes will be used by Spok MediCall extensions.

```

add abbreviated-dialing system                                     Page 1 of 1
                        ABBREVIATED DIALING LIST
                        SYSTEM LIST

Size (multiple of 5): 5      Privileged? n      Label Language:english
DIAL CODE                  LABELS (FOR STATIONS THAT DOWNLOAD LABELS)
    01: *40                  01: Agent Log-in
    02: *41                  02: Agent Log-out
    03:                      03: *****
    04:                      04: *****
    05:                      05: *****

```

5.3. Configure Stations

Enter the **change station *n*** command, where ***n*** is the extension that the Spok MediCall Console will register to.

Extension 3305 was used by Spok MediCall for controlling Avaya Endpoints. On **Page 1** of the **station** form, enter a phone **Type**, descriptive **Name**, **Security Code**, **Button Modules** and set **IP SoftPhone** field to **y** to allow the physical station to be controlled by MediCall. Note that J100 series phones use the 9611 station type for H.323 firmware configurations.

change station 3305		Page 1 of 7
STATION		
Extension: 3305	Lock Messages? n	BCC: 0
Type: 9611	Security Code: *	TN: 1
Port: S000015	Coverage Path 1:	COR: 1
Name: Spok MediCall Console	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: 3305	
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 3305		Page 2 of 7
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? y	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced	Audible Message Waiting? n	
MWI Served User Type:	Display Client Redirection? n	
AUDIX Name:	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 3305	Always Use? n	IP Audio Hairpinning? n

change station 3305

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

2:call-appr

3:call-appr

4:call-appr

5:call-appr

6:q-calls

7:

8:

Grp: 1

change station 3305

STATION

BUTTON MODULE #1 ASSIGNMENTS

1:brdg-appr B:1 E:3301

2:brdg-appr B:2 E:3301

3:brdg-appr B:3 E:3301

4:brdg-appr B:4 E:3301

5:brdg-appr B:5 E:3301

6:brdg-appr B:6 E:3301

7:

8:abrv-dial List: 1 DC: 01

9:auto-in Grp:

10:aux-work RC: Grp:

11:after-call Grp:

12:

13:brdg-appr B:1 E:3300

14:brdg-appr B:2 E:3300

15:

16:

17:

18:

19:

20:

21:

22:

23:

24:

change station 3305

STATION

BUTTON MODULE #2 ASSIGNMENTS

1:brdg-appr B:1 E:3302

2:

3:

4:

5:abrv-dial List: 1 DC: 02

6:

7:

8:

9:

10:

11:

12:

13:brdg-appr B:1 E:3304

14:brdg-appr B:2 E:3304

15:brdg-appr B:3 E:3304

16:brdg-appr B:4 E:3304

17:brdg-appr B:5 E:3304

18:

19:

20:

21:

22:

23:toggle-swap

24:release

5.4. Configure Hunt Group

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

change hunt-group 1	Page 1 of 4
HUNT GROUP	
Group Number: 1	ACD? y
Group Name: Skill-1	Queue? y
Group Extension: 3320	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 VDNs

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

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

add vdn 3340	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 3340	Unicode Name? n
Name*: Spok VDN 3340	
Destination: Vector Number	1
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 1.

```
change vector 1                                     Page 1 of 6
                                     CALL VECTOR

  Number: 1                      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 1      pri m
03 wait-time      30      secs hearing music
04 goto step      2                      if unconditionally
05
```

5.7. Configure Agent Extensions

Enter the **add agent-loginID *n*** command, where *n* is an available extension according to the dial plan. This extension will be used by Spok MediCall to log onto ACD. During the compliance test, two agent extensions were added, 1000 and 1001. On **Page 1**, specify a **name** of the agent, **password**, and set **Auto Answer** to **none**.

```
change agent-loginID 1000                           Page 1 of 3
                                     AGENT LOGINID

      Login ID: 1000                      Unicode Name? n      AAS? n
      Name: Agent 1000                      AUDIX? n
      TN: 1
      COR: 1
Coverage Path:                      LWC Reception: spe
Security Code: 1234                      LWC Log External Calls? n
Attribute:                      AUDIX Name for Messaging:

                                     LoginID for ISDN/SIP Display? n
                                     Password:
                                     Password (enter again):
                                     Auto Answer: none
      MWI Served User Type:                      MIA Across Skills: system
AUX Agent Remains in LOA Queue: system      ACW Agent Considered Idle: system
AUX Agent Considered Idle (MIA): system      Aux Work Reason Code Type: system
      Work Mode on Login: system      Logout Reason Code Type: forced
      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 1000										Page 2 of 3		
AGENT LOGINID												
Direct Agent Skill: 1										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: 1		1	16:			31:			46:			
2:			17:			32:			47:			
3:			18:			33:			48:			
4:			19:			34:			49:			
5:			20:			35:			50:			
6:			21:			36:			51:			
7:			22:			37:			52:			
8:			23:			38:			53:			
9:			24:			39:			54:			
10:			25:			40:			55:			
11:			26:			41:			56:			
12:			27:			42:			57:			
13:			28:			43:			58:			
14:			29:			44:			59:			
15:			30:			45:			60:			

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.

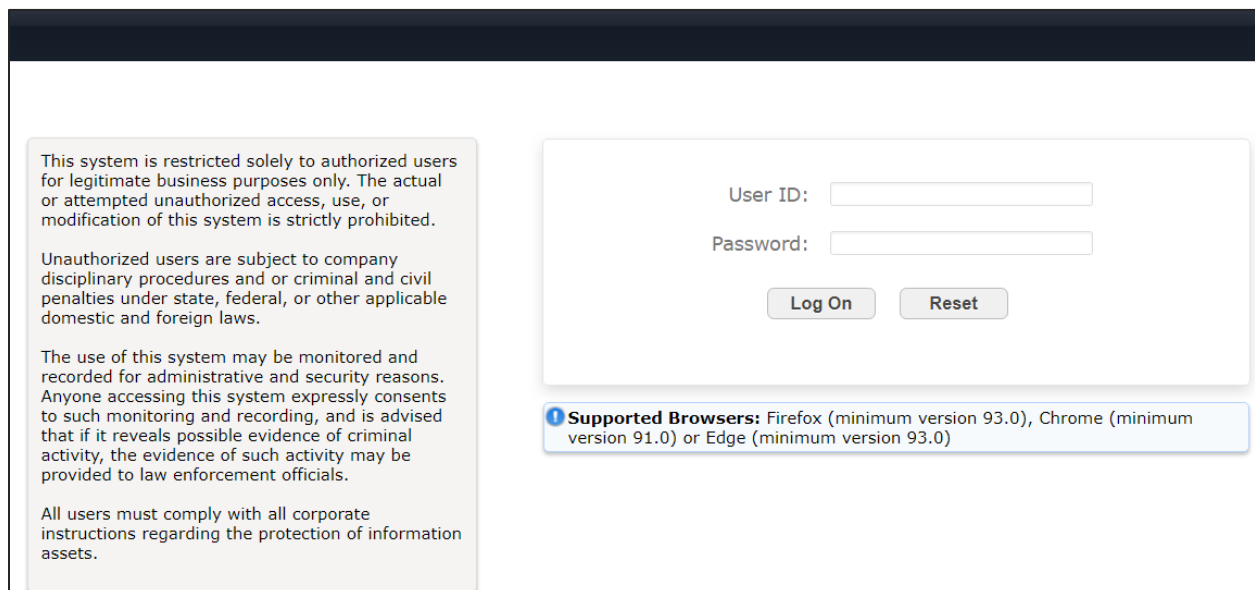
This section assumes that installation and basic administration of the AES server has been performed. The steps in this section describe the configuration of a CTI user, a DMCC port and TLS Version and Root Certificate.

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, System Manager was used as a license server.

Provide appropriate login credentials and log in.



This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:


Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0)

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

13 Items  Show All ▼		
Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	100
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	100
AES HA LARGE VALUE_AES_HA_LARGE	permanent	10
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	100
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	100
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	100
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	10
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	100
DLG VALUE_AES_DLG	permanent	100
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	100
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	100
		SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_

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 displays the Avaya Application Enablement Services Management Console. The top right corner shows system information: Welcome: User cust, Last login: Wed Sep 28 09:29:15 2022 from 10.33.1.200, Number of prior failed login attempts: 0, HostName/IP: aes10/10.33.1.47, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 10.1.0.1.0.7-0, Server Date and Time: Sat Nov 12 08:06:46 MST 2022, HA Status: Not Configured. The main navigation bar includes links for User Management, User Admin, List All Users, Home, Help, and Logout. The left sidebar lists various services and management options, with 'User Management' expanded to show 'User Admin' and 'Add User'. The 'Edit User' form is the central focus, containing fields for user identification and configuration. A red box highlights the 'User Id' (spok), 'Common Name' (spok), 'Surname' (console), 'User Password', 'Confirm Password', and 'CT User' (Yes) fields. The 'CT User' field is a dropdown menu currently set to 'Yes'.

Edit User	
* User Id	spok
* Common Name	spok
* Surname	console
User Password	
Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Cms Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	

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

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

Edit CTI User

User Profile:

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

Call and Device Control:

Call Origination/Termination and Device Status	None ▼
--	--------

Call and Device Monitoring:

Device Monitoring	None ▼
Calls On A Device Monitoring	None ▼
Call Monitoring	<input type="checkbox"/>

Routing Control:

Allow Routing on Listed Devices	None ▼
---------------------------------	--------

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. The **Encrypted Port 4722** was used during the compliance test. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Wed Sep 28 09:29:15 2022 from 10.33.1.200
Number of prior failed login attempts: 0
HostName/IP: aes10/10.33.1.47
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Sat Nov 12 08:15:49 MST 2022
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Encrypted Port4722

TR/87 Port4723

Enabled Disabled

Enabled Disabled

Enabled Disabled

Enabled Disabled

Enabled Disabled

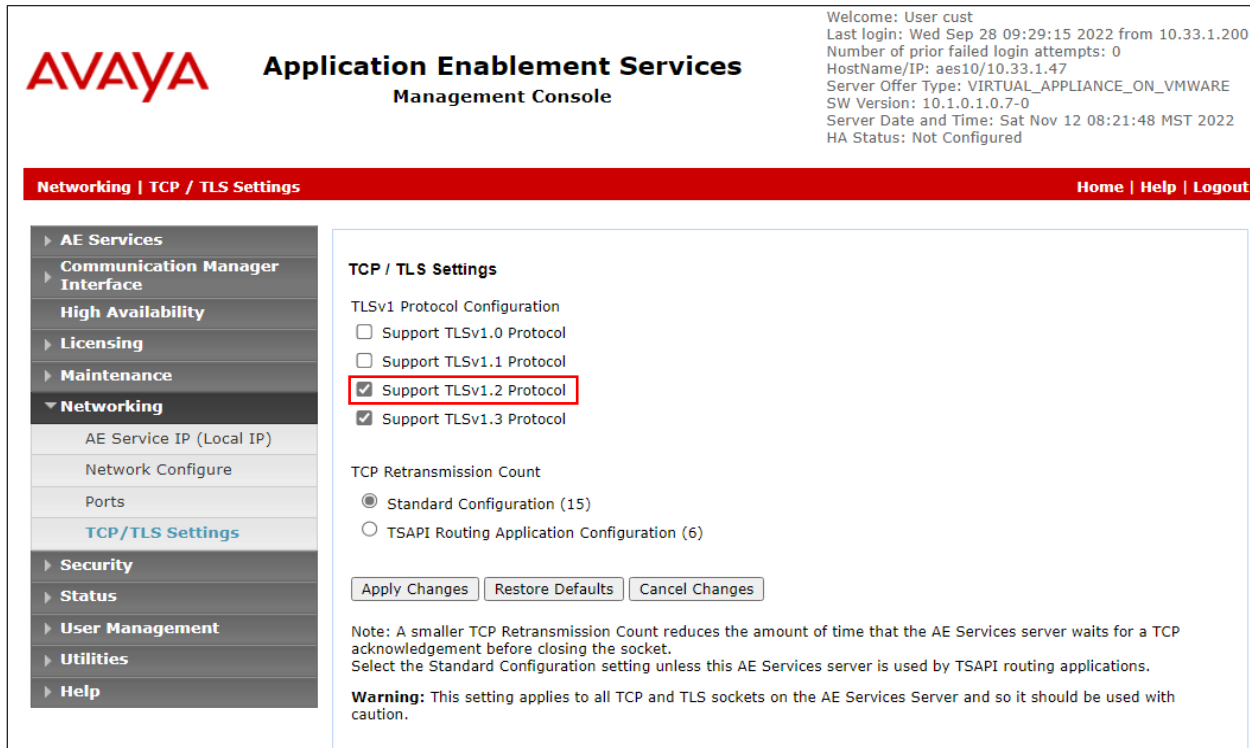
Enabled Disabled

Enabled Disabled

Enabled Disabled

6.4. Configure TLS Version

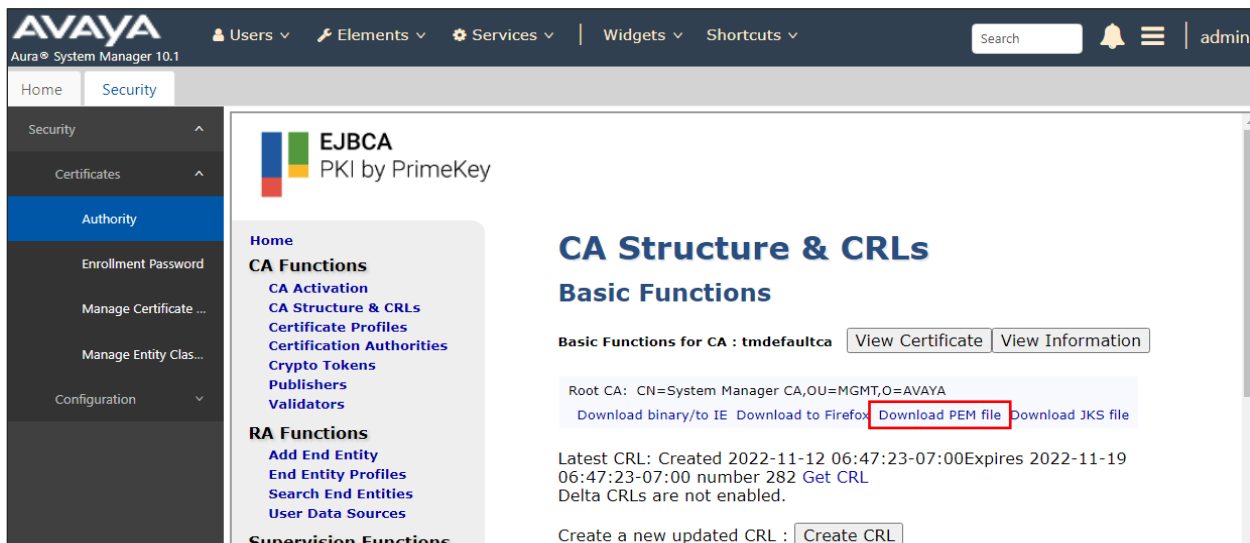
Navigate to the **Networking → TCP/TLS Settings** page and verify that TLS Version 1.2 is checked. This will be used in **Section 7** when configuring Spok Smart Console.



The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "cust" with login details. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking (selected), AE Service IP, Network Configure, Ports, TCP/TLS Settings (highlighted), Security, Status, User Management, Utilities, and Help. The main content area is titled "TCP / TLS Settings". Under "TLSv1 Protocol Configuration", there are four checkboxes: "Support TLSv1.0 Protocol", "Support TLSv1.1 Protocol", "Support TLSv1.2 Protocol" (checked and highlighted with a red box), and "Support TLSv1.3 Protocol". Under "TCP Retransmission Count", there are two radio buttons: "Standard Configuration (15)" (selected) and "TSAPI Routing Application Configuration (6)". At the bottom, there are buttons for "Apply Changes", "Restore Defaults", and "Cancel Changes". A note states: "Note: A smaller TCP Retransmission Count reduces the amount of time that the AE Services server waits for a TCP acknowledgement before closing the socket. Select the Standard Configuration setting unless this AE Services server is used by TSAPI routing applications." A warning states: "Warning: This setting applies to all TCP and TLS sockets on the AE Services Server and so it should be used with caution."

6.5. Obtain Root Certificate

In order to configure the application to use secure links, download the root certificate for the environment; in this case System Manager issued certificates to AES.



The screenshot shows the Avaya Aura System Manager 10.1 Security page. The top header includes the Avaya logo, the title "Aura System Manager 10.1", and navigation links for Users, Elements, Services, Widgets, and Shortcuts. The left sidebar contains a navigation menu with options like Home, Security (selected), Certificates, Authority, Enrollment Password, Manage Certificate..., Manage Entity Clas..., and Configuration. The main content area is titled "CA Structure & CRLs" and "Basic Functions". Under "Basic Functions for CA : tmdefaultca", there are buttons for "View Certificate" and "View Information". Below these, there are links for "Download binary/to IE", "Download to Firefox", "Download PEM file" (highlighted with a red box), and "Download JKS file". The "Latest CRL" section shows: "Created 2022-11-12 06:47:23-07:00 Expires 2022-11-19 06:47:23-07:00 number 282 Get CRL". Below this, it states "Delta CRLs are not enabled." At the bottom, there is a button for "Create a new updated CRL : Create CRL".

7. Configure Spok MediCall Console

Spok installs, configures, and customizes the Spok 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.

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 encrypted DMCC 4722 port as shown in **Section 6**.
- **Local Certificate File** – Upload the root CA file as shown in **Section 6**.
- **SSL Protocol** – Select Version 1.2 to match the AES settings in **Section 6**.
- **User** – Enter the user name created for Spok MediCall from **Section 6**.
- **Password** – Enter the password created for Spok MediCall from **Section 6**.

Under Phone Device Settings

- **Extension:** Enter the extension that will be controlled by Spok MediCall from **Section 5**.
- **Security Code:** Enter the security code for the controlled station from **Section 5**.
- **Release Button** – Enter the Release button assigned for the controlled station from **Section 5.7**.
- **Line Appearances** – Configure line appearances as per **Section 5**.

Spok AES CTI Service Setup

DMCC Settings

AES Server: 10.33.1.47

Switch Name:

Switch IP Interface: 10.33.1.43

Port: Secure (4722) Application Id: spok

Device Instance: 2

Local Certificate File: C:\Program Files (x86)\Amcom\CTI_Service\SMGRCA10 ...

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

User (default = cmaps): spok Password:

Media Mode: No Media Shared Control: False

Dependency Mode: Dependent AES Version: 7.0

Telecomuter Extension:

☐ Monitor Call Information

☐ Monitor Media Device

☐ Monitor Device Service

Phone Device Settings

Extension: 3305 RLT Transfer Button Id:

Security Code: Release Button Id: 1063

Max SCA Timer (ms): 250 Toggle-Swap Button Id: 1062

☒ Press Release Button Upon Cancel

Park Access Code: *25

Unpark Access Code: #25

Line Appearances:

Line 1	Button Id = 1	Display Id = a
Line 2	Button Id = 2	Display Id = b
Line 3	Button Id = 3	Display Id = c
Line 4	Button Id = 4	Display Id = d
Line 5	Button Id = 5	Display Id = e
Line 6	Button Id = 251	Display Id = y BRIDGE
Line 7	Button Id = 252	Display Id = z BRIDGE

+ Add... X Delete Edit...

Service Settings

Listener Port: 973

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

Configuration File Name: cmapi.cfg ...

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

LUA Agent Function File: ...

LUA Agent State File: ...

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

☐ 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

OK Cancel Restart Service Phone Server


Activate Win Go to Settings to

8. Verification Steps

The following steps may be used to verify the configuration:

8.1. Verify Application Enablement Services

Verify Spok MediCall is successfully connected to AES via AES Management console. Navigate to **Status** → **Status and Control** → **DMCC Service Summary**. Verify the **Connection Type** and **State** of Spok MediCall user as **XML Encrypted** and **IDLE**.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Wed Sep 28 09:29:15 2022 from 10.33.1.200
Number of prior failed login attempts: 0
HostName/IP: aes10/10.33.1.47
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Sun Nov 13 09:47:44 MST 2022
HA Status: Not Configured

Status | Status and Control | DMCC Service SummaryHome | Help | Logout

▶ 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 Sun Nov 13 09:47:19 MST 2022

Service Uptime: 6 days, 10 hours 37 minutes

Number of Active Sessions: 2

Number of Sessions Created Since Service Boot: 8

Number of Existing Devices: 2

Number of Devices Created Since Service Boot: 8

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	5516D5A276A437E6A A1E74D1E31F10C5-1	spok	spok	10.33.1.116	XML Encrypted	1

Terminate SessionsShow Terminated Sessions

Status | Status and Control | DMCC Service SummaryHome | Help | Logout

▶ 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

Switch Conn Summary

TSAPI Service Summary

▶ User Management

DMCC Service Summary - Session Detail

☐ Enable page refresh every 60 seconds

Detailed Session View
Generated on Sun Nov 13 09:50:10 MST 2022

Session ID: 5516D5A276A437E6AA1E74D1E31F10C5-1

State: Active

Time Established: Sun, Nov 6, 2022 11:13:15 PM GMT-07:00

Uptime: 6 days, 10 hours, 36 minutes, and 54 seconds

Cleanup Delay Timer: 60 seconds

Session Duration Timer: 180 seconds

Time of Most Recent Timer Reset: Sun, Nov 13, 2022 09:49:23 AM MST

Reconnect Counter: 0

Terminate Sessions

Devices Associated with Session

	Device ID	State
<input type="checkbox"/>	3305:cm10:10.33.1.43:2	IDLE

Terminate Selected DevicesBack

Item 1-1 of 1

8.2. Verify Spok MediCall Console

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

The screenshot displays the MediCall™ Operator Console interface. At the top, the title bar reads "MediCall™ Operator Console 11,14,34". Below the title bar, the "Extension :" section shows "a=Devconnect LAB to MSG: 3340". To the right of this section are buttons for "Auto In" (green), "Release", "Aux Out", and "AfterCall". Below the extension information is a grid of extension status buttons, including "Active" (green) and various numbers like 3305, 3301, 3300, 3304, and 3302.

The main section is titled "Lookup" and contains a "Searching by : Name" field. Below this are icons for "Dial Number", "Notes Of Day", and "Quick Page". To the right of these icons is a dropdown menu set to "ALL". Below the search area is a table titled "XTEND MultisiteTest, Kush" with columns "Key", "Description", and "Number". The table contains two rows: "F1 HOME NUMBER 5970" and "F2 OFFICE NUMBER 5971". To the right of the table is a "Refresh" button and an "OnCall Departments" section with a list of departments. On the far right is a vertical sidebar with buttons for "Add", "Advanced", "Update", "Admin", "Profile", "View Msgs", and "Tree Index". At the bottom of the interface, there is a status bar with "Searching by : Name", "Date : Sunday, Nov 13 2022 07:30:22 AM", and "Spok User".

Key	Description	Number
F1	HOME NUMBER	5970
F2	OFFICE NUMBER	5971

9. Conclusion

These Application Notes described a compliance-tested configuration comprised of Communication Manager, AES, Avaya J189 IP Telephones, and the Spok MediCall application. Spok MediCall allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). During compliance testing, calls were successfully placed to and from Avaya IP Telephones that were controlled and monitored by the Spok MediCall application with observations in **Section 2.2**.

10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1, September 2022

[2] *Administering Avaya Aura® Application Enablement Services*, Release 10.1, September 2022

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

©2022 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.