



Avaya Solution & Interoperability Test Lab

Application Notes for Cleric Respond-2 with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cleric Respond-2 to interoperate with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3.

The compliance testing focused on the voice integration of Cleric Respond-2 with Avaya Aura® Communication Manager via the Avaya Aura® Application Device, Media and Call Control (DMCC) Application Programming Interface.

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 the configuration steps required for Cleric Respond-2 to interoperate with Avaya Aura® Communication Manager 8.1.3 and Avaya Aura® Application Enablement Services 8.1.3

The compliance testing focused on the integration of Cleric Respond-2 with Communication Manager via the Application Enablement Services Device, Media, and Call Control (DMCC) Application Programming Interface.

Cleric Respond-2 is a highly visual Ambulance Command and Control / NHS 111 Call Centre computer aided dispatch application. Cleric Respond-2 can monitor agent states and Vector Directory Numbers (VDNs) in the emergency response centre using DMCC of Avaya Aura® Application Enablement Services.

2. General Test Approach and Test Results

Interoperability testing contained functional tests mentioned in **Section 2.1**. All test cases were performed manually. The general test approach was to validate Cleric Response-2 successfully monitoring agents' states and calls placed to Vector Directory Numbers (VDNs) from analog phones, digital phones, and IP phones (SIP and H323) on Avaya Aura® Communication Manager.

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 this Application Note, the interface between Avaya systems and Cleric Respond-2 did not include use of any specific encryption features as requested by Cleric.

2.1. Interoperability Compliance Testing

The interoperability Compliance test included feature and serviceability testing. Feature testing monitored agents and calls placed to Vector Directory Numbers (VDNs) in the following:

- **Agent State Change** – Login, Ready/Not Ready, AUX, After Call Work.
- **Inbound Calls** from Avaya SIP, H.323, and digital telephones, PSTN endpoints.
- **Hold/Transfer/Conference**
- **Serviceability** - The serviceability testing focused on verifying the ability of Cleric Respond-2 to recover from adverse conditions, such as disconnecting/reconnecting the network to Cleric Respond-2.

2.2. Test Results

The testing was successful. All test cases are passed.

2.3. Support

Technical support can be obtained for the Cleric Respond-2 solution as follows:

Tel: (+44) 01260 270433

Email: support@cleric.co.uk

Web: <https://cleric.co.uk/customers/support/>

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services is not the focus of these Application Notes and will not be described.

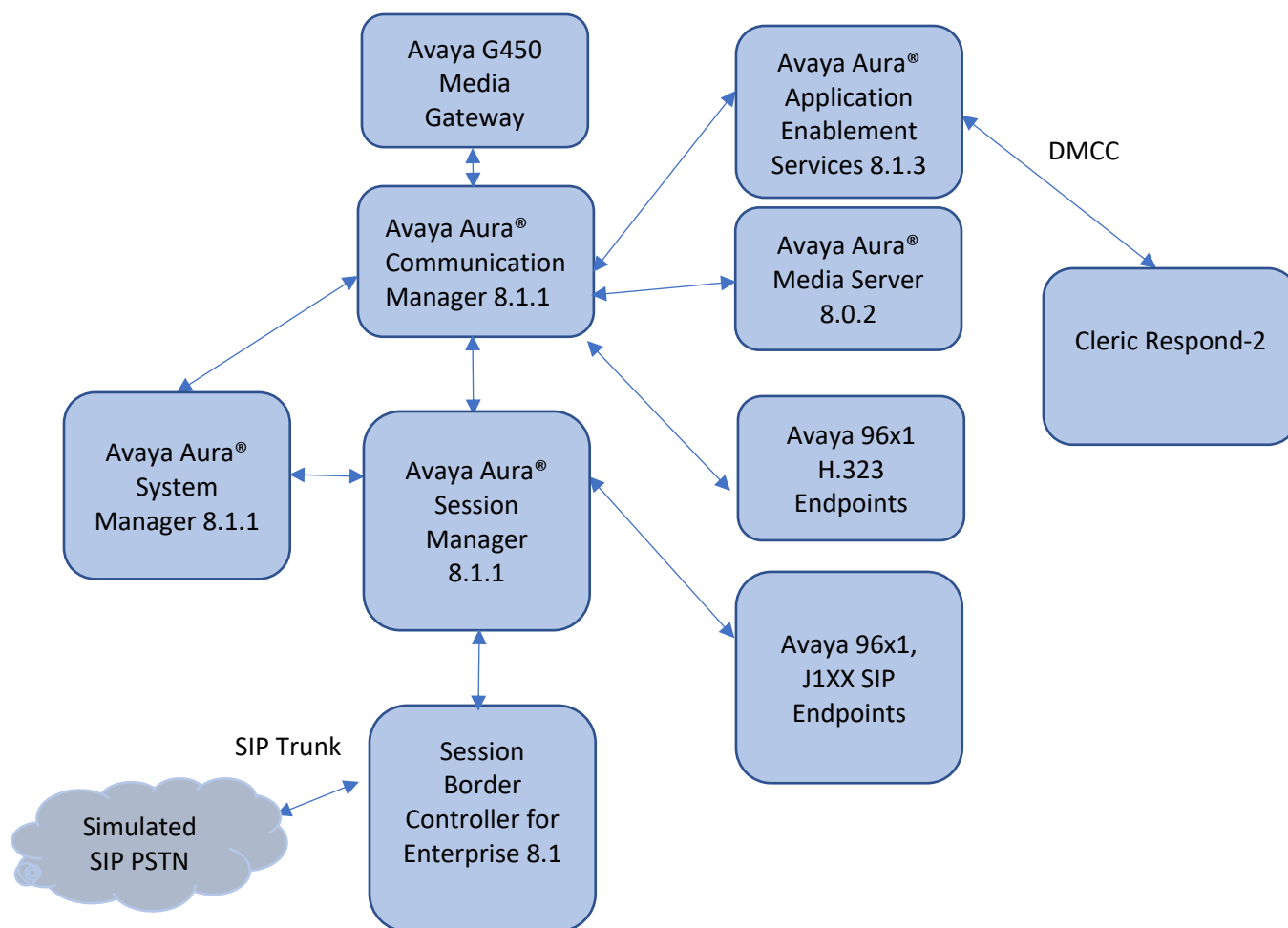


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager in Virtual Environment	8.1.3.1
Avaya Aura® Session Manager in Virtual Environment	8.1.3.1
Avaya Aura® Communication Manager in Virtual Environment	8.1.3.1
Avaya G450 Media Gateway	41.34.1
Avaya Aura® Media Server in Virtual Environment	8.0 SP2
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3.1
Avaya Session Border Controller for Enterprise	8.1.1
Avaya 9621G & 9641G IP Desk phone (SIP)	7.1.8
Avaya 9608G & 9641G IP Desk phone (H.323)	6.8.3
Avaya J159, J179 IP Desk phone (SIP)	4.0.8
Cleric Respond-2	4.7.120

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer CTI link
- Administer hunt group and agent
- Administer vectors and VDNs

5.1. Verify License

Log into the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 4**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

display system-parameters customer-options		Page	4 of 12
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	n	Authorization Codes?	y
Analog Trunk Incoming Call ID?	y	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n
ARS?	y	Computer Telephony Adjunct Links?	y
ARS/AAR Partitioning?	y	Cvg Of Calls Redirected Off-net?	y
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y
ASAI Link Core Capabilities?	y	DCS Call Coverage?	y
ASAI Link Plus Capabilities?	y	DCS with Rerouting?	y
Async. Transfer Mode (ATM) PNC?	n		
Async. Transfer Mode (ATM) Trunking?	n	Digital Loss Plan Modification?	y
ATM WAN Spare Processor?	n	DS1 MSP?	y
ATMS?	y	DS1 Echo Cancellation?	y
Attendant Vectoring?	y		
(NOTE: You must logoff & login to effect the permission changes.)			

Navigate to **Page 7** and verify that the **Vectoring (Basic)** customer option is set to “y”.

```
change system-parameters customer-options          Page 7 of 12
CALL CENTER OPTIONAL FEATURES

Call Center Release: 8.0

ACD? y                      Reason Codes? y
BCMS (Basic)? y             Service Level Maximizer? n
BCMS/VuStats Service Level? y Service Observing (Basic)? y
BSR Local Treatment for IP & ISDN? y Service Observing (Remote/By FAC)? y
Business Advocate? n        Service Observing (VDNs)? y
Call Work Codes? y          Timed ACW? y
DTMF Feedback Signals For VRU? y Vectoring (Basic)? y
Dynamic Advocate? n         Vectoring (Prompting)? y
Expert Agent Selection (EAS)? y Vectoring (G3V4 Enhanced)? y
EAS-PHD? y                  Vectoring (3.0 Enhanced)? y
Forced ACD Calls? n         Vectoring (ANI/II-Digits Routing)? y
Least Occupied Agent? y     Vectoring (G3V4 Advanced Routing)? y
Lookahead Interflow (LAI)? y Vectoring (CINFO)? y
Multiple Call Handling (On Request)? y Vectoring (Best Service Routing)? y
Multiple Call Handling (Forced)? y Vectoring (Holidays)? y
PASTE (Display PBX Data on Phone)? y Vectoring (Variables)? y
(NOTE: You must logoff & login to effect the permission changes.)
Press 'Esc f 6' for Vector Editing
```

5.2. Administer CTI Link

Add a CTI link using the **add cti-link n** command, where **n** is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1          Page 1 of 3
CTI LINK
CTI Link: 1
Extension: 79999
Type: ADJ-IP
COR: 1
Name: aes95
```

5.3. Administer Hunt Group and Agent

This section shows the steps required to add a new service or skill on Communication Manager. Services are accessed by calling a Vector Directory Number (VDN), which points to a vector. The vector then points to a hunt group associated with an agent. The following sections give step by step instructions on how to add the following

- Hunt Group
- Agent

5.3.1. Add Hunt Group

To add a new skillset or hunt group type, **add hunt-group x**, where **x** is the new hunt group number. For example, hunt group **2** is added for the **Voice Service** queue. Ensure that **ACD**, **Queue** and **Vector** are all set to **y**. Also, that **Group Type** is set to **ucd-mia**.

add hunt-group 1	Page 1 of 4
HUNT GROUP	
Group Number: 1	ACD? y
Group Name: Voice Service	Queue? y
Group Extension: 87000	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:	

On **Page 2** ensure that **Skill** is set to **y** as shown below.

add hunt-group 2	Page 2 of 4
HUNT GROUP	
Skill? y	Expected Call Handling Time (sec): 180
AAS? n	
Measured: none	
Supervisor Extension:	
Controlling Adjunct:	
Multiple Call Handling: none	
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n

5.3.2. Add Agent

In the compliance testing, the agents 80000 and 80001 were created.

To add a new agent, type **add agent-loginID x**, where x is the login id for the new agent.

add agent-loginID 80000		Page 1 of 3
AGENT LOGINID		
Login ID: 80000	AAS? n	
Name: Voice Agent	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	
	AUDIX Name for Messaging:	
	LoginID for ISDN/SIP Display? n	
	Password:	
	Password (enter again):	
	Auto Answer: station	
	MIA Across Skills: system	
	ACW Agent Considered Idle: 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**, add the required skills. Note that the skill **2** is added to this agent so when a call for **Voice Service** is initiated, the call is routed correctly to this agent.

add agent-loginID 80000		Page 2 of 3					
AGENT LOGINID							
Direct Agent Skill:		Service Objective? n					
Call Handling Preference: skill-level		Local Call Preference? n					
SN	RL SL	SN	RL SL	SN	RL SL	SN	RL SL
1: 2	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:	

Repeat this section to add another agent 80001.

5.4.Administer Vectors and VDNs

Add a vector using the “change vector n” command, where “n” is a vector number. Note that the vector steps may vary. Below is a sample vector used in the compliance testing.

change vector 1	CALL VECTOR	Page 1 of 6
Number: 1 Name: VoiceService		
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 silence	
02 queue-to	skill 1 pri t	
03 wait-time	2 secs hearing silence	
04 stop		
05		
06		
07		
08		
09		
10		
11		
12		
Press 'Esc f 6' for Vector Editing		

Add a VDN using the “add vdn n” command, where “n” is an available extension number. Enter a descriptive Name and the vector number from above for Destination. Retain the default values for all remaining fields.

change vdn 88000	VECTOR DIRECTORY NUMBER	Page 1 of 3
Extension: 88000 Unicode Name? n		
Name*: Voice VDN		
Destination: Vector Number 1		
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		

6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer Avaya user
- Administer security database
- Restart services
- Obtain Tlink name

6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://ip-address” in an Internet browser window, where **ip-address** is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



Application Enablement Services Management Console


[Help](#)

Please login here:

Username

Copyright © 2009-2020 Avaya Inc. All Rights Reserved.

The **Welcome to OAM** screen is displayed next.



Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri May 21 16:42:19 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.1.0.7-0
Server Date and Time: Thu Jun 03 12:09:03 ICT 2021
HA Status: Not Configured

Home

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:


- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

Copyright © 2009-2020 Avaya Inc. All Rights Reserved.

6.2. Verify License

Select **Licensing** → **WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Fri May 21 16:42:19 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.1.0.7-0
Server Date and Time: Thu Jun 03 12:09:44 ICT 2021
HA Status: Not Configured

LicensingHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▼ Licensing

WebLM Server Address

WebLM Server Access

Reserved Licenses

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

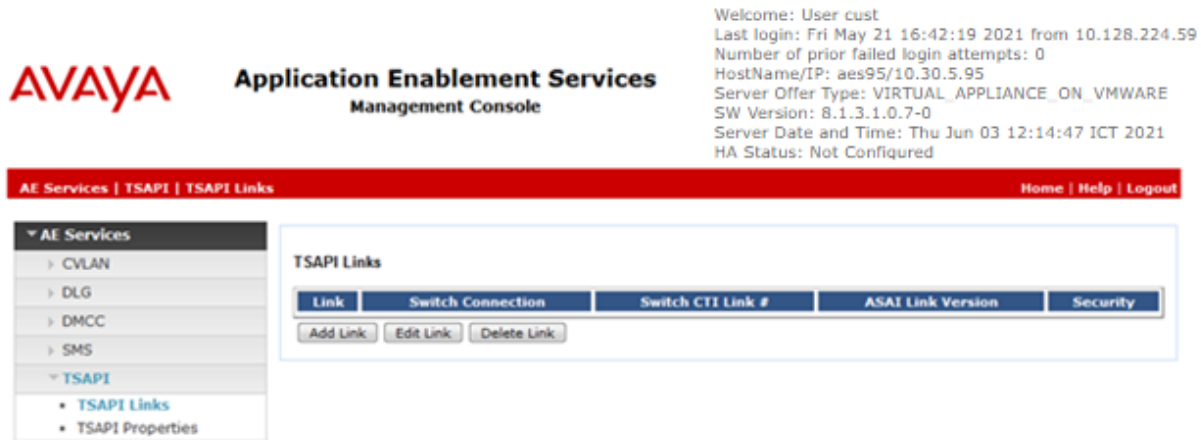
Copyright © 2009-2020 Avaya Inc. All Rights Reserved.

Verify that there are sufficient licenses for **Device Media and Call Control**, as shown below.

NAQ; Reviewed: Solution & Interoperability Test Lab Application Notes 14 of 28
SPOC 8/25/2021 ©2021 Avaya Inc. All Rights Reserved. Respond2-AES813

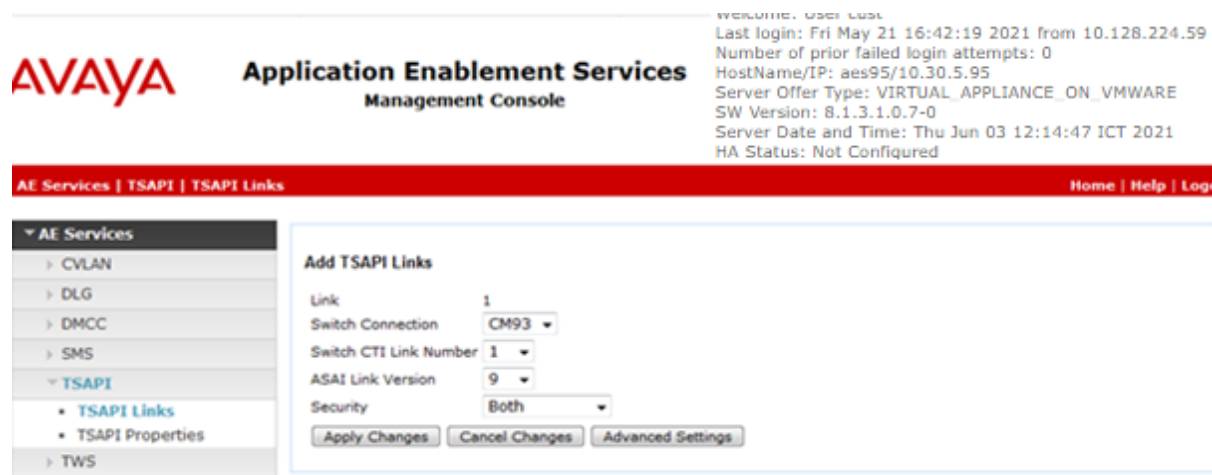
6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection **CM93** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 0**. Retain the default values in the remaining fields.



6.4. Administer Cleric User

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields.

AVAYA **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Aug 5 13:53:35 2021 from 10.128.224.163
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.2.0.4-0
Server Date and Time: Fri Aug 13 10:21:05 ICT 2021
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Idcleric

* Common Namecleric

* Surnamecleric

* User Password*****

* Confirm Password*****

Admin Note

Avaya RoleNone

Business Category

Car License

CM Home

Css Home

CT UserYes

Department Number

Display Name


Employee Number

Employee Type

6.5. Administer Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [4] to configure access privileges for the Avaya user from **Section 6.4**.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Jun 3 16:05:58 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.1.0.7-0
Server Date and Time: Thu Jun 03 16:08:17 ICT 2021
HA Status: Not Configured

Security | Security Database | Control[Home](#) | [Help](#) | [Logout](#)

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

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services
☐ Enable SDB for DMCC Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

6.6. Administer Ports

Select **Networking** → **Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Unencrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.

AVAYA

Application Enablement Services
Management Console

Welcome: User cust
Last login: Thu Jun 3 16:05:58 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.1.0.7-0
Server Date and Time: Thu Jun 03 16:09:17 ICT 2021
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 Port9999Enabled Disabled

Encrypted TCP Port9998Enabled Disabled

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450Enabled Disabled

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 Port4721Enabled Disabled

Encrypted Port4722Enabled Disabled

TR/87 Port4723Enabled Disabled

6.7. Restart Services

Select **Maintenance Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service**, and then click **Restart Service**.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Jun 3 16:05:58 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.1.0.7-0
Server Date and Time: Thu Jun 03 16:09:50 ICT 2021
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▼ Maintenance

Date Time/NTP Server

▶ Security Database

Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

Copyright © 2009-2020 Avaya Inc. All Rights Reserved.

7. Configure Cleric Respond-2 Server

This section provides the procedures for configuring Cleric Respond-2 Server. It is implied a working Cleric Respond-2 is already in place successfully with the necessary licensing. Go to CCSA folder (e.g., C:\CCSAvaya\CCSAvaya). Open the CCSAvaya.exe.config file and modify all the following settings:

AES Settings

aesServerIP_1:	Enter AES IP address, in this case 10.30.5.95
aesServerPort_1:	Enter AES DMCC port, in this case 4721 with Unencrypted Port
aesServerSecure_1:	Select 0 for Unencrypted
aesUsername_1:	Enter cleric user created in Section 6.4
aesPassword_1:	Enter password for cleric user in Section 6.4

Switch Settings

switchIP_1:	Enter Communication Manager IP address
--------------------	--



```
CCSAvaya.exe - Notepad
File Edit Format View Help
<add name="Connection" connectionString="Server=MYSERVER;Database=MYDATABASE;User Id=██████████;Password=██████████" />
</connectionStrings>

<appSettings>
  <add key="ClientSettingsProvider.ServiceUri" value="" />

  <!-- AES settings -->
  <add key="aesServerIP_1" value="10.30.5.95"/>
  <add key="aesServerPort_1" value="4721"/>
  <add key="aesServerSecure_1" value="0"/>
  <add key="aesUsername_1" value="cleric"/>
  <add key="aesPassword_1" value="██████████" />

  <!--
  <add key="aesServerIP_2" value="192.168.0.2" />
  <add key="aesServerPort_2" value="4722" />
  <add key="aesServerSecure_2" value="0" />
  <add key="aesUsername_2" value="username" />
  <add key="aesPassword_2" value="password" />
  -->

  <add key="aesSessionFailureMaxRetries" value="3" />
  <add key="aesSessionCleanupDelay" value="60" />
  <add key="aesSessionDuration" value="180" />

  <!-- Switch settings -->
  <add key="switchIP" value="10.30.5.93"/>

  <!-- Listener settings -->

Ln 16, Col 56 100% Windows (CRLF) UTF-8 with BOM
```

8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services and Cleric Respond-2 solution.

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established” for the CTI link number administered in **Section 5.2. as shown below.**

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	9	no	aes95	established	14	14

Enter the command **list agent-loginID** and verify that agents **80000** and **80001**, shown in **Section 5.3.2**, are logged into Skill 1 via extension **70010** and **70009**, respectively.

```
list agent-loginID
```

AGENT LOGINID									
Login ID	Name	Extension		Dir	Agt	AAS/AUD		COR	Ag Pr SO
		Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv	Skil/Lv
80000	Voice Agent	70010						1	lvl
	1/01	/	/	/	/	/	/	/	
80001	Voice Agent1	70009						1	lvl
	1/01	/	/	/	/	/	/	/	

Enter the command **status station 70010** and on **Page 7** verify that the agent is logged into the appropriate skill.


```
status station 70010
```

ACD STATUS							Page 7 of 7
Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	Grp/Mod	
1/AUX	/	/	/	/	/	/	On ACD Call? no

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status** → **Status and Control** → **TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify the **Status** is “Talking” for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of agents, in this case “2”.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Jun 3 12:17:21 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.1.0.7-0
Server Date and Time: Thu Jun 03 14:42:06 ICT 2021
HA Status: Not Configured

Status | Status and Control | TSAPI 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**

TSAPI Link Details

☐ Enable page refresh every seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	CM93	1	Talking	Fri May 21 16:32:15 2021	Online	18	2	15	15	30


OnlineOffline

For service-wide information, choose one of the following:

TSAPI Service StatusTLink StatusUser Status

8.3. Verify Avaya Aura® Application Enablement Services

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Communication Manager and the Application Enablement Services server is functioning correctly. Verify the status of the TSAPI service by selecting **Status** → **Status and Control** → **TSAPI Service Summary** → **User Status**. The **Open Streams** section of this page displays open stream created by the **Avaya** user with the **Tlink**.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Thu Jun 3 12:17:21 2021 from 10.128.224.59
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.1.0.7-0
Server Date and Time: Thu Jun 03 14:42:37 ICT 2021
HA Status: Not Configured

Status | Status and Control | TSAPI 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**

CTI User Status

☐ Enable page refresh every 60 seconds

CTI Users All Users Submit

Open Streams 2

Closed Streams 50


Open Streams

Name	Time Opened	Time Closed	Tlink Name
DMCCLCSUserDoNotModify	Fri 21 May 2021 03:49:23 PM +07		AVAYA#CM93#CSTA#AES95
DMCCLCSUserDoNotModify	Fri 21 May 2021 03:49:23 PM +07		AVAYA#CM93#CSTA#AES95

Show Closed StreamsClose All Opened StreamsBack

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify the **User** column shows action sessions with the **cleric** username from **Section 6.5**



Application Enablement Services
Management Console

Welcome: User cust
 Last login: Thu Jun 3 12:17:21 2021 from 10.128.224.59
 Number of prior failed login attempts: 0
 HostName/IP: aes95/10.30.5.95
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 8.1.3.1.0.7-0
 Server Date and Time: Thu Jun 03 14:45:13 ICT 2021
 HA Status: Not Configured

Status | Status and Control | **DMCC Service Summary**
Home | 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

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
 Generated on Thu Jun 03 14:44:58 ICT 2021

Service Uptime: 12 days, 22 hours 55 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 3

Number of Existing Devices: 2

Number of Devices Created Since Service Boot: 6

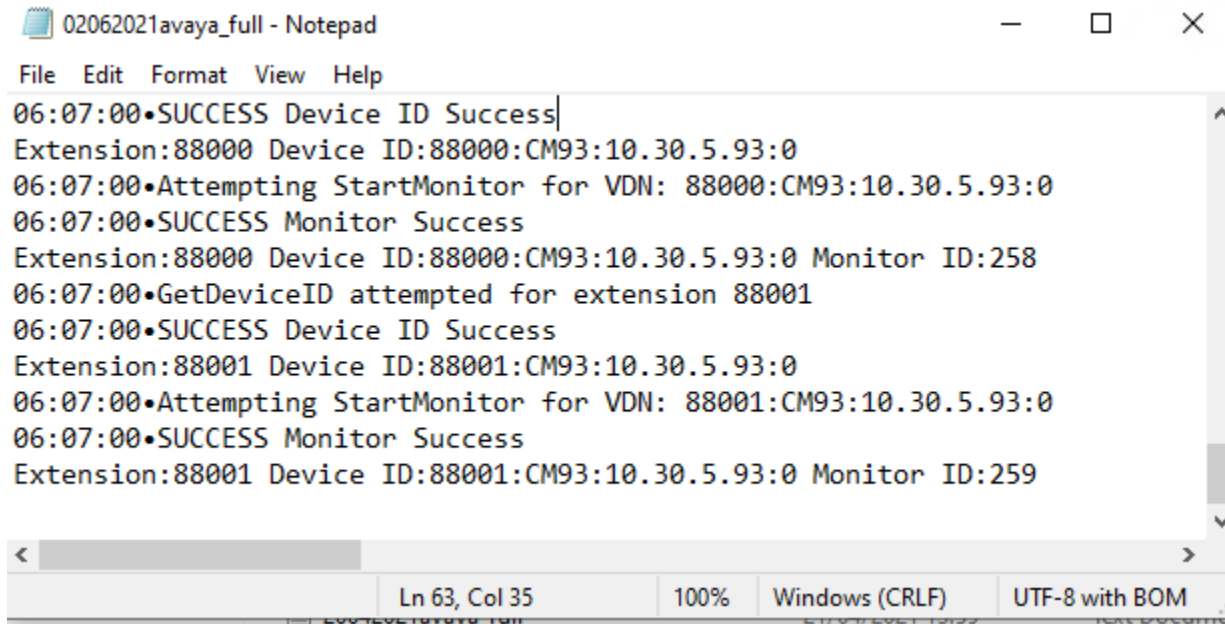
■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	A867EF7B5AABE7EE6 67B1B14410F64CC-4	cleric	CCSAvaya	10.103.3.207	XML Unencrypted	2

Terminate Sessions
Show Terminated Sessions

Item 1-1 of 1
1 Go

8.4. Verify Cleric Respond-2

On Cleric Respond-2 Server, go to CCSAvaya Logs folder (e.g., C:\CCSAvaya\Logs). Verify that all VDNs are already monitored successfully.



```
02062021avaya_full - Notepad
File Edit Format View Help
06:07:00•SUCCESS Device ID Success|
Extension:88000 Device ID:88000:CM93:10.30.5.93:0
06:07:00•Attempting StartMonitor for VDN: 88000:CM93:10.30.5.93:0
06:07:00•SUCCESS Monitor Success
Extension:88000 Device ID:88000:CM93:10.30.5.93:0 Monitor ID:258
06:07:00•GetDeviceID attempted for extension 88001
06:07:00•SUCCESS Device ID Success
Extension:88001 Device ID:88001:CM93:10.30.5.93:0
06:07:00•Attempting StartMonitor for VDN: 88001:CM93:10.30.5.93:0
06:07:00•SUCCESS Monitor Success
Extension:88001 Device ID:88001:CM93:10.30.5.93:0 Monitor ID:259
Ln 63, Col 35 100% Windows (CRLF) UTF-8 with BOM
```

Make an incoming call to VDN and verify it shows in the CCSAvaya log:

```
16:29:31•Process_OnQueuedEvent
16:29:31•<?xml version="1.0" encoding="utf-16"?>
<QueuedEvent xmlns="http://www.ecma-international.org/standards/ecma-323/csta/ed3">
  <monitorCrossRefID>258</monitorCrossRefID>
  <queuedConnection>
    <callID>356</callID>
    <deviceID typeOfNumber="other" mediaClass="notKnown" bitRate="constant">87000:CM93::0</deviceID>
  </queuedConnection>
  <queue>
    <deviceIdentifier typeOfNumber="explicitPrivate:localNumber" mediaClass="notKnown" bitRate="constant">87000:CM93::0</deviceIdentifier>
  </queue>
  <callingDevice>
    <deviceIdentifier typeOfNumber="explicitPublic:unknown" mediaClass="notKnown" bitRate="constant">T356#1:CM93::0</deviceIdentifier>
  </callingDevice>
  <calledDevice>
    <deviceIdentifier typeOfNumber="implicitPublic" mediaClass="notKnown" bitRate="constant">8900088000:CM93::0</deviceIdentifier>
  </calledDevice>
  <lastRedirectionDevice>
    <numberDialed typeOfNumber="other" mediaClass="notKnown" bitRate="constant">88000:CM93:10.30.5.93:0</numberDialed>
  </lastRedirectionDevice>
  <numberQueued>1</numberQueued>
  <localConnectionInfo>null</localConnectionInfo>
  <cause>redirected</cause>
</QueuedEvent>
```

03062021avaya_formatted - Notepad

File Edit Format View Help

16:29:31•356

03/06/2021

16:29:31

CO

Unknown

8000

16:30:16•356

03/06/2021

16:30:16

CL

Unknown

8000|

88000

16:38:48•357

03/06/2021

16:38:48

CO

Unknown

8000

16:39:13•357

03/06/2021

16:39:13

CA

Unknown

8000

70000

9. Conclusion

These Application Notes describe the configuration steps required for Cleric Respond-2 to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed successfully.

10. Additional References

This section references the Avaya and Cleric product documentation that are relevant to these Application Notes.

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 8, Nov 2020
2. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 8, Feb 2021
3. *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 9, Feb 2021
4. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 9, Feb 2021

©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.