



Avaya Solution & Interoperability Test Lab

Application Notes for PCI Pal® Agent Assist with Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate PCI Pal® Agent Assist 2022 with Avaya Aura® Communication Manager 10.1, Avaya Aura® Session Manager 10.1, and Avaya Session Border Controller for Enterprise 10.1. Avaya Session Border Controller for Enterprise routes calls between a contact center on Avaya Aura® Communication Manager and a VoIP Service Provider with calls routing through PCI Pal® Agent Assist. PCI Pal® Agent Assist is a hosted solution that allows contact centers to take card payments securely using DTMF capture technology while the contact center agent remains in the conversation with the customer. PCI Pal® Agent Assist integrates with Avaya Session Border Controller for Enterprise via a SIP trunk.

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.

Table of Contents

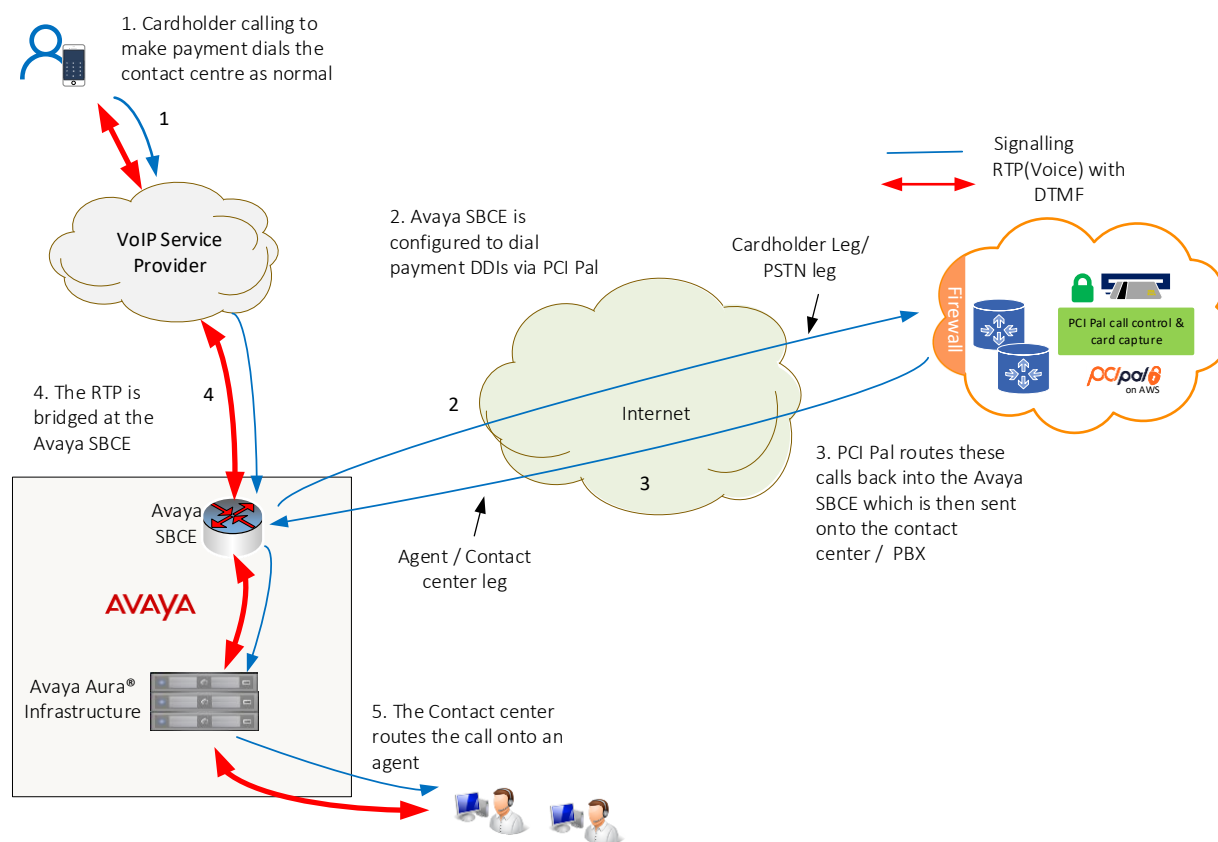
1.	Introduction.....	4
2.	General Test Approach and Test Results.....	6
2.1.	Interoperability Compliance Testing.....	6
2.2.	Test Results	7
2.3.	Support	7
3.	Reference Configuration	8
4.	Equipment and Software Validated	9
5.	Configure Avaya Aura® Communication Manager.....	10
5.1.	Verify Licenses	10
5.2.	Administer IP Node Names.....	11
5.3.	Administer IP Codec Set.....	11
5.4.	Administer IP Network Region.....	12
5.5.	Administer SIP Trunk to Session Manager.....	13
5.6.	Administer Private Numbering	15
5.7.	Administer ARS Call Routing	16
5.8.	Administer Route Pattern	17
5.9.	Administer Incoming Call Treatment	17
6.	Configure Avaya Aura® Session Manager	18
6.1.	Add Adaptation	19
6.2.	Add SIP Entities	21
6.2.1.	Avaya Aura® Communication Manager	21
6.2.2.	SIP Entity for SBCE	23
6.3.	Add Routing Policies	25
6.4.	Add Dial Patterns	27
6.5.	Add Session Manager.....	29
7.	Configure Avaya Session Border Controller for Enterprise	31
7.1.	Launch SBCE Web Interface	31
7.2.	Administer Server Interworking Profiles	33
7.2.1.	Server Interworking Profile for PCI PAL Agent Assist	33
7.2.2.	Server Interworking Profile for Session Manager	37
7.2.3.	Server Interworking Profile for VoIP Service Provider	39
7.3.	Administer SIP Servers	41
7.3.1.	SIP Server for PCI Pal Agent Assist.....	41
7.3.2.	SIP Server for Session Manager	43
7.3.3.	SIP Server for VoIP Service Provider	45
7.4.	Administer Routing Profiles.....	47
7.4.1.	Routing Profile for PCI Pal Agent Assist	47
7.4.2.	Routing Profile for Session Manager.....	50
7.4.3.	Routing Profile for VoIP Service Provider	51
7.5.	Administer Signaling Manipulation Scripts.....	52
7.6.	Administer URI Groups	54
7.7.	Administer Media Rules.....	55
7.8.	Administer End Point Policy Groups	58
7.9.	Administer TLS Management.....	60
7.10.	Administer Media Interfaces	63

7.11.	Administer Signaling Interfaces	64
7.12.	Administer End Point Flows.....	65
7.12.1.	End Point Flows for PCI Pal Agent Assist.....	66
7.12.2.	End Point Flows for Session Manager	68
7.12.3.	End Point Flows for VoIP Service Provider	70
8.	Configure PCI Pal Agent Assist	72
9.	Verification Steps.....	72
10.	Conclusion	75
11.	Additional References.....	75

1. Introduction

These Application Notes describe the configuration steps required to integrate PCI Pal® Agent Assist with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise. Avaya Session Border Controller for Enterprise routes calls between a contact center on Avaya Aura® Communication Manager and a VoIP Service Provider with calls routing through PCI Pal® Agent Assist. PCI Pal Agent Assist is a hosted solution that allows contact centers to take card payments securely using DTMF capture technology while the contact center agent remains in the conversation with the customer. PCI Pal Agent Assist integrates with Avaya Session Border Controller for Enterprise (Avaya SBCE) via a SIP trunk.

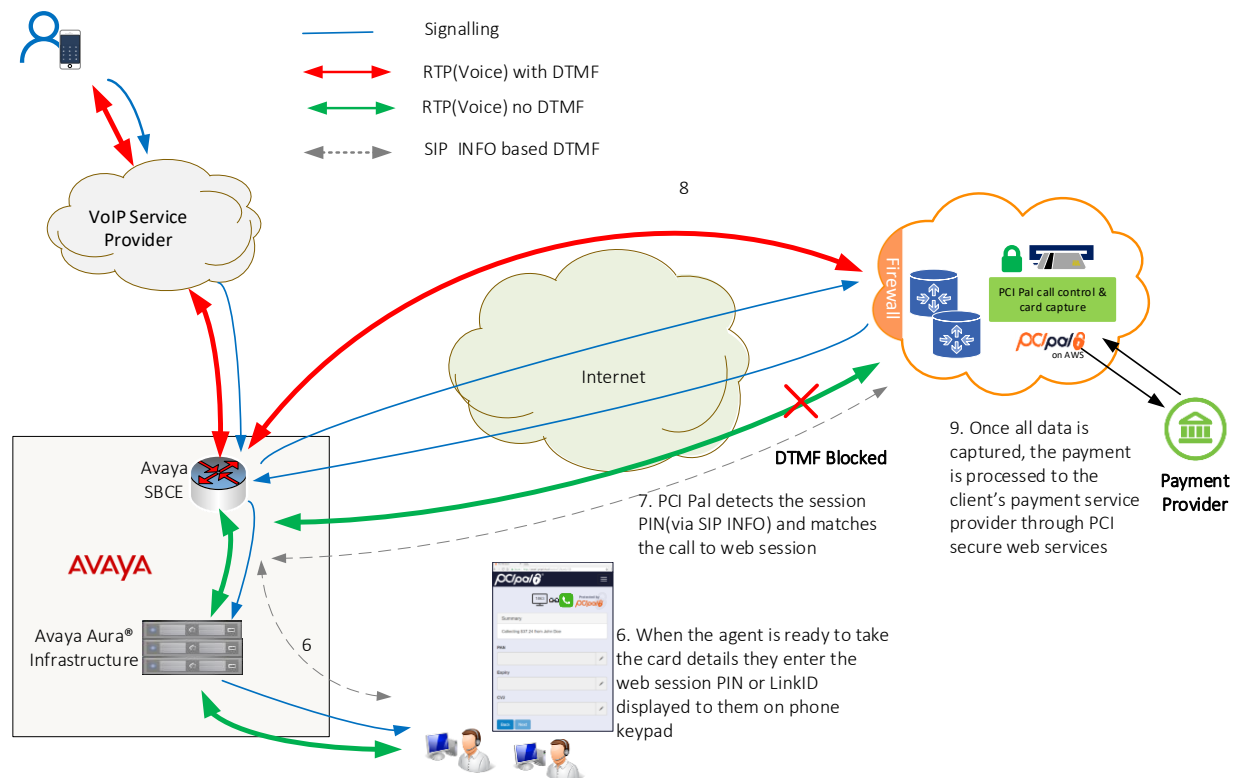
Calls between the Avaya Aura® environment and the VoIP Service Provider are generally routed via Avaya SBCE. Avaya SBCE routes such calls through PCI Pal Agent Assist. All inbound and outbound calls are routed (looped) via Avaya SBCE to PCI Pal Agent Assist. Initially, for a given call, only SIP signaling is looped via Avaya SBCE to PCI Pal Agent Assist, RTP still flows through Avaya SBCE.



Once the call is answered by a contact center agent, a 4-digit code (PIN or Link ID) provided by the PCI Pal Portal is entered by the contact center agent at the time of payment is required to secure the call. This code is sent to Avaya SBCE via DTMF using RFC2833. Avaya SBCE then converts the DTMF using RFC2833 to SIP INFO messages and sends them to PCI Pal Agent

Assist. RFC2833 tones are also sent in the RTP. Upon successful authentication, PCI Pal Agent Assist sends a re-INVITE to Avaya SBCE to redirect RTP using RFC2833 to PCI Pal Agent Assist. After the RTP has been successfully redirected, the call is considered secured. Once instructed, customer enters payment information via their telephone keypad. These DTMF digits are sent to Avaya SBCE and converted to SIP INFO. Both DTMF methods using RFC2833 and SIP INFO are sent to PCI Pal Agent Assist when the call is secured. For each DTMF digit, PCI Pal Agent Assist removes the SIP INFO, RFC2833, and in-band DTMF (if present) from the agent leg RTP, and replaces with mono tones (i.e., not the actual digits entered by customer) and sends them along with RTP. Mono tones are sent to agents for informational purposes only to inform them that the customer has entered digits.

After the payment has been successfully processed, PCI Pal Agent Assist redirects the RTP back to Avaya SBCE by sending re-INVITES for both call legs.



2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between a customer, via the VoIP Service Provider, and agents in an Avaya contact center, and routing calls through PCI Pal Agent Assist. Agents then enter a PIN supplied by the PCI Pal Portal to secure the call and allow cardholder/payment information to be redirected to PCI Pal Agent Assist. Compliance testing also entailed verifying DTMF transmission in both directions by navigating the menu of an IVR application or voicemail system. In addition, agents exercised various telephony features before and after calls were secured and unsecured.

The serviceability test cases focused on failover scenarios where the primary PCI Pal Agent Assist was unavailable and the call had to route to the secondary PCI Pal Agent Assist or both PCI Pal Agent Assist were unavailable and the call had to be routed directly to Session 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 these Application Notes, the interface between Avaya systems and PCI Pal Agent Assist utilized encryption capabilities of TLS/SRTP.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP trunk between SBCE and Agent Assist using TLS transport and verifying the exchange of SIP OPTIONS messages.
- Inbound and outbound PSTN call via a VoIP Service Provider routed through Agent Assist using TLS/SRTP with Direct IP Media (Shuffling) and Initial IP-IP Direct Media enabled or disabled.
- DTMF transmission using RFC2833 to SBCE.
- Conversion of RFC2833 to SIP INFO by SBCE and vice versa.
- DTMF transmission using RFC2833 and SIP INFO with Agent Assist.

- RTP redirection from SBCE to Agent Assist after call is secured and card payment info is being sent.
- Agent enters PIN using DTMF (telephone keypad) and PIN is sent to Agent Assist via SIP INFO. DTMF using RFC2833 is redirected from SBCE to Agent Assist to secure call. Payment info is sent only to Agent Assist (i.e., agent doesn't receive DTMF).
- Multiple payments processed by a single agent on one call.
- Multiple payments processed by multiple agents simultaneously.
- Inbound calls from VoIP Service Provider to IVR to verify successful navigation of menu using DTMF.
- Outbound calls that cover to voicemail to verify successful navigation of voicemail system using DTMF.
- G.711mu-law codec support.
- Telephony features, such as call hold/resume, call transfer, conference, call forwarding, call coverage, and queuing calls to split to ensure proper operation after call is secured and unsecured.
- Failover scenarios between primary and secondary Agent Assist when one is unavailable and routing calls directly to Session Manager when both Agent Assist aren't available.

2.2. Test Results

All test cases passed with the following observation:

- The call legs between (1) SBCE and Session Manager and (2) SBCE and Agent Assist must use different SRTP ciphers to trigger a change in SRTP encryption keys, which helps SBCE decrypt the DTMF signals. For example, one call leg may use srtp-aescm128-hmac80 while the other call leg may srtp-aescm128-hmac32. If the ciphers are the same for both call legs, the SIP INFO messages, which are supposed to deliver the DTMF digits (PIN) provided by the contact center agent to secure the call, may contain a blank Signal header instead of a DTMF digit. When this occurs the call cannot be secured.

2.3. Support

Technical support on PCI Pal Agent Assist can be obtained through the following:

- **Phone:** US: +1 866 645 2903 (Charlotte, NC)
UK: +44 207 030 3770 (London) or +44 330 131 0330 (Ipswich)
- **Web:** www.pcipal.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of redundant PCI Pal Agent Assist in an Avaya Aura® environment. All SIP calls between the VoIP Service Provider and the Avaya Aura® environment were routed from SBCE to PCI Pal Agent Assist, and then to Session Manager or VoIP Service Provider, depending on the call direction. The Avaya Aura® environment consisted of the following products:

- SBCE with SIP trunk connectivity to Session Manager, PCI Pal Agent Assist, and VoIP Service Provider.
- Session Manager connected to Communication Manager via a SIP trunk and acting as a Registrar/Proxy for SIP endpoints.
- Media resources in Avaya G450 Media Gateway and Avaya Aura® Media Server.
- System Manager used to configure Session Manager.
- Experience Portal to provide access to IVR applications.
- Avaya 96x1 Series H.323 Deskphones and Avaya J100 Series SIP Phones.

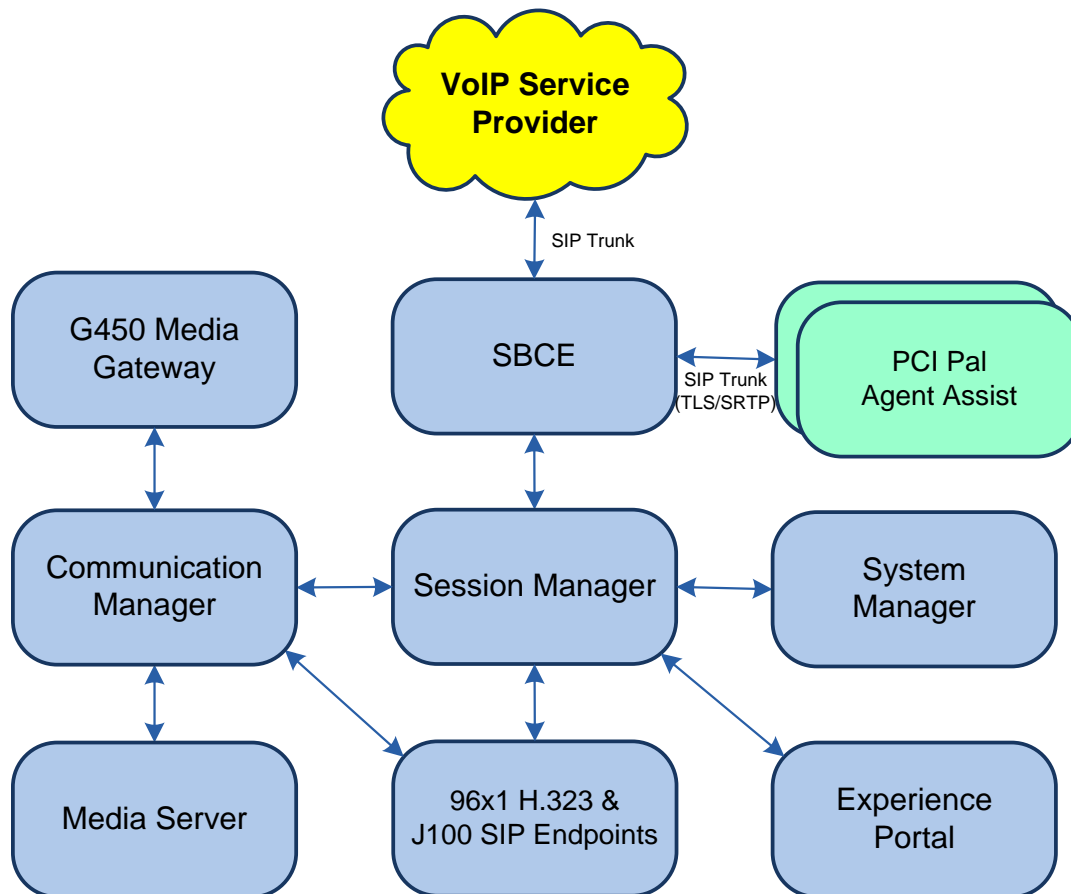


Figure 1: Avaya Aura® Environment with PCI Pal Agent Assist

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	10.1.0.1.0-SP1
Avaya G450 Media Gateway	FW 42.4.0
Avaya Aura® Media Server	v.10.1.0.77
Avaya Aura® System Manager	10.1.0.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.1.061394 Service Pack 1
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Aura® Experience Portal	8.1.1.0.0251
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872
Avaya 96x1 Series IP Deskphones	6.8511 (H.323)
Avaya J100 Series IP Phones	4.0.10.3.2 (SIP)
PCI Pal® Agent Assist	2022.707.166.8421

5. Configure Avaya Aura® Communication Manager

For this solution, Communication Manager provides a contact center whose agents communicate with customers to collect payment information using Agent Assist. The configuration of the contact center, including agents, skill/hunt group, vectors, and VDNs are outside the scope of these Application Notes, but note that customer calls were placed to a VDN, which pointed to a vector that queued the call to a split/hunt group, and eventually routed the call to an available agent or queued the call. Customer calls were routed from the VoIP Service Provider to SBCE, SBCE looped the SIP signaling through Agent Assist, and then the call was routed to Session Manager and finally to Communication Manager. Outbound agent calls followed the same call path, but in reverse order.

This section covers the configuration steps required to establish a SIP trunk between Communication Manager and Session Manager and routing calls to/from the VoIP Service Provider. Communication Manager is configured through the System Access Terminal (SAT). The procedures include the following areas:

- Verify Licenses
- Administer IP Node Names
- Administer IP Codec Set
- Administer IP Network Region
- Administer SIP Trunk Group to Session Manager
- Administer Private Numbering
- Administer AAR Call Routing
- Administer Route Pattern
- Administer Incoming Call Treatment

5.1. Verify Licenses

Using the SAT, enter the **display system-parameters customer-options** command to verify there is sufficient capacity for SIP trunks on **Page 2**. The license file installed on the system controls these options. If there is insufficient capacity of SIP trunks or a required feature is not enabled, contact an authorized Avaya sales representative.

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	0
Maximum Concurrently Registered IP Stations:		2400	2
Maximum Administered Remote Office Trunks:		12000	0
Max Concurrently Registered Remote Office Stations:		2400	0
Maximum Concurrently Registered IP eCons:		128	0
Max Concur Reg Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		36000	2
Maximum Video Capable IP Softphones:		2400	2
Maximum Administered SIP Trunks:		12000	20
Max Administered Ad-hoc Video Conferencing Ports:		12000	0
Max Number of DS1 Boards with Echo Cancellation:		688	0
(NOTE: You must logoff & login to effect the permission changes.)			

5.2. Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*devcon-sm*). The host names will be used in other configuration screens of Communication Manager.

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

IP NODE NAMES	
Name	IP Address
default	0.0.0.0
devcon-aes	10.64.102.119
devcon-ams	10.64.102.118
devcon-sm	10.64.102.117
procr	10.64.102.115
procr6	::

(6 of 6 administered node-names were displayed)
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name

5.3. Administer IP Codec Set

In the **IP Codec Set** form, specify the audio codec to be used by Agent Assist. The form is accessed via the **change ip-codec-set 2** command. Note the codec set number since it will be used in the IP Network Region covered in the next section. For the compliance test, *G.711MU* was used. In addition, configure **Media Encryption** and **Encrypted SRTCP** as shown below.

```
change ip-codec-set 2                                     Page 1 of 2
```

IP MEDIA PARAMETERS			
Codec Set: 2			
Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size(ms)
1: G.711MU	n	2	20
2:			
3:			
4:			
5:			
6:			
7:			

Media Encryption	Encrypted SRTCP: best-effort
1: 1-srtp-aescm128-hmac80	
2: none	
3:	
4:	
5:	

5.4. Administer IP Network Region

In the **IP Network Region** form, specify the codec set to be used for Agent Assist and enable **IP-IP Direct Audio** (shuffling), if desired. Shuffling allows audio traffic to be sent directly between IP endpoints and SBCE without using media resources in the Avaya G450 Media Gateway or Avaya Aura® Media Server after call establishment. For this compliance test, shuffling was enabled. The **Authoritative Domain** for this configuration is *avaya.com*.

change ip-network-region 2		Page 1 of 20
IP NETWORK REGION		
Region: 2	NR Group: 2	
Location: 1	Authoritative Domain: avaya.com	
Name: To Avaya SBCE	Stub Network Region: n	
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 2	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

5.5. Administer SIP Trunk to Session Manager

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the **Signaling Group** form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Specify Communication Manager (*procr*) and the Session Manager (*devcon-sm*) as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form.
- Ensure that the TLS port value of *5062* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.
- **Direct IP-IP Audio Connections** is enabled to allow shuffling for calls routed over the trunk group associated with this signaling group.
- **Initial IP-IP Direct Media** may be enabled or disabled.

Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

add signaling-group 11		Page 1 of 2
SIGNALING GROUP		
Group Number: 11	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? y	Priority Video? n	Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y	Peer Server: SM	Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: devcon-sm	
Near-end Listen Port: 5062	Far-end Listen Port: 5062	
	Far-end Network Region: 2	
Far-end Domain: avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? y	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to the VoIP Service Provider. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie* or *public-ntwk*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

add trunk-group 11		Page 1 of 5	
TRUNK GROUP			
Group Number: 11	Group Type: sip	CDR Reports: y	
Group Name: To SIP Service Provider	COR: 1	TN: 1	TAC: 1011
Direction: two-way	Outgoing Display? n		
Dial Access? n	Night Service:		
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group: 11		
	Number of Members: 10		

On **Page 3** of the trunk group form, set the **Numbering Format** field to *private*. This field specifies the format of the calling party number sent to the far-end.

add trunk-group 11		Page 3 of 5	
TRUNK FEATURES			
ACA Assignment? n	Measured: none		
	Maintenance Tests? y		
Suppress # Outpulsing? n	Numbering Format: private		
	UUI Treatment: shared		
	Maximum Size of UUI Contents: 128		
	Replace Restricted Numbers? n		
	Replace Unavailable Numbers? n		
	Modify Tandem Calling Number: no		
Send UCID? n			
Show ANSWERED BY on Display? y			

On **Page 5** of the trunk group form, the default settings were used as shown below.

add trunk-group 11	Page 5 of 5
<p>PROTOCOL VARIATIONS</p> <p>Mark Users as Phone? n</p> <p>Prepend '+' to Calling/Alerting/Diverting/Connected Number? n</p> <p>Send Transferring Party Information? n</p> <p>Network Call Redirection? n</p> <p>Send Diversion Header? n</p> <p>Support Request History? y</p> <p>Telephone Event Payload Type: 101</p> <p>Convert 180 to 183 for Early Media? n</p> <p>Always Use re-INVITE for Display Updates? n</p> <p>Resend Display UPDATE Once on Receipt of 481 Response? n</p> <p>Identity for Calling Party Display: P-Asserted-Identity</p> <p>Block Sending Calling Party Location in INVITE? n</p> <p>Accept Redirect to Blank User Destination? n</p> <p>Enable Q-SIP? n</p> <p>Interworking of ISDN Clearing with In-Band Tones: keep-channel-active</p> <p>Request URI Contents: may-have-extra-digits</p>	

5.6. Administer Private Numbering

Configure the **Numbering – Private Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 5-digit extension beginning with ‘7’ whose calls are routed over trunk group 11 have their extension converted to a 11-digit number.

change private-numbering 0	Page 1 of 2										
<p>NUMBERING - PRIVATE FORMAT</p> <table> <thead> <tr> <th>Ext Len</th> <th>Ext Code</th> <th>Trk Grp(s)</th> <th>Private Prefix</th> <th>Total Len</th> </tr> </thead> <tbody> <tr> <td>5</td> <td>7</td> <td>11</td> <td>173277</td> <td>11</td> </tr> </tbody> </table> <p>Total Administered: 2</p> <p>Maximum Entries: 540</p>		Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	5	7	11	173277	11
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len							
5	7	11	173277	11							

5.7. Administer ARS Call Routing

Use the **change feature access code** command to define a feature access code for **Auto Route Selection (ARS)** per the dial plan. For the compliance test, 9 was used as the ARS Access Code.

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:	*11
Answer Back Access Code:	*24
Auto Alternate Routing (AAR) Access Code:	8
Auto Route Selection (ARS) - Access Code 1:	9
Access Code 2:	
Automatic Callback Activation:	*25
Deactivation:	#25
Call Forwarding Activation Busy/DA:	*21 All: *20
Deactivation:	#20
Call Forwarding Enhanced Status:	Act:
Deactivation:	
Call Park Access Code:	*26
Call Pickup Access Code:	*27
CAS Remote Hold/Answer Hold-Unhold Access Code:	
CDR Account Code Access Code:	*39
Change COR Access Code:	
Change Coverage Access Code:	
Conditional Call Extend Activation:	Deactivation:
Contact Closure Open Code:	Close Code:

SIP calls destined for the VoIP Service Provider are routed through Session Manager over a SIP trunk via ARS call routing. Configure the ARS analysis form and add an entry that routes digits beginning with “1908” to route pattern 12 as shown below.

change ars analysis 19						Page 1 of 2	
ARS DIGIT ANALYSIS TABLE							
Location: all						Percent Full: 1	
Dialed	Total		Route	Call	Node	ANI	
String	Min	Max	Pattern	Type	Num	Reqd	
190	11	11	4	fnpa		n	
1900	11	11	deny	fnpa		n	
1900555	11	11	deny	fnpa		n	
1908	11	11	12	fnpa		n	

5.8. Administer Route Pattern

Configure a preference in **Route Pattern** 12 to route calls over SIP trunk group 11 as shown below.

change route-pattern 12										Page	1	of	4						
Pattern Number: 12										Pattern Name: Twilio									
SCCAN? n		Secure SIP? n		Used for SIP stations? n															
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC											
No			Mrk	Lmt	List	Del	Digits	QSIG											
								Intw											
1:	11	0	1							n	user								
2:									n	user									
3:									n	user									
4:									n	user									
5:									n	user									
6:									n	user									
BCC VALUE										TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	Sub	Numbering	LAR	
0 1 2 M 4 W											Request					Dgts	Format		
1:	y	y	y	y	y	n	n	rest						unk-unk	none				
2:	y	y	y	y	y	n	n	rest							none				
3:	y	y	y	y	y	n	n	rest							none				
4:	y	y	y	y	y	n	n	rest							none				
5:	y	y	y	y	y	n	n	rest							none				
6:	y	y	y	y	y	n	n	rest							none				

5.9. Administer Incoming Call Treatment

Incoming calls from the VoIP Service Provider use a DID number beginning with “+1720”. Use the **change inc-call-handling-trmt trunk-group** command to convert the DID number to the VDN that routes calls to an agent in the contact center.

change inc-call-handling-trmt trunk-group 11										Page	1	of	30
INCOMING CALL HANDLING TREATMENT													
Service/	Number	Number	Del Insert										
Feature	Len	Digits											
public-ntwrk	12	+1720	all 77550										

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedure includes adding the following items:

- Adaptation
- SIP Entities for Communication Manager and SBCE
- Entity Links, which defines the SIP trunk parameters used by Session Manager when routing calls to/from Communication Manager and SBCE
- Routing Policies and Dial Patterns
- Session Manager, corresponding to the Avaya Aura® Session Manager server to be managed by Avaya Aura® System Manager

Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL **https://<ip-address>/SMGR**, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials.

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.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

User ID:

Password:

[Change Password](#)

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

6.1. Add Adaptation

Session Manager can be configured with Adaptations that can modify SIP messages before or after routing decisions have been made; for example, replacing a domain name with a different value as shown in this section. Note that the following Adaptation replaces the domain in the To and From header to the IP address of the SBCE internal interface. This allows SBCE to identify calls that should route through Agent Assist (i.e., if domain matches SBCE internal interface, then route call through Agent Assist). Session Manager should route all other calls, which should not route through Agent Assist, to a different SBCE SIP entity without this Adaptation assigned to it.

To create an **Adaptation** that will be applied to the SBCE SIP entity in **Section 6.2.2**, navigate to **Elements → Routing → Adaptations** and click on the **New** button (not shown). In the **General** section, enter the following values. Use default values for all remaining fields.

- **Adaptation Name:** Enter a descriptive name for the Adaptation (e.g., *SBCE for PCIPal*).
- **Module Name:** Select *DigitConversionAdapter*.
- **Module Parameter Type:** Select *Name-Value Parameter*. The section will expand with an area to enter **Name** and **Value** pairs. Click **Add**. Set **fromto** to *true* to allow the From and To headers to be modified. Set **iodstd** and **iosrcd** to *avaya.com* to replace the ingress domain name with *avaya.com*. Set **odstd** and **osrcd** to *10.64.102.106* to replace the egress domain name with the IP address of the SBCE interface connected to Session Manager.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Routing' menu with 'Adaptations' selected. The main content area displays the 'Adaptation Details' form.

Adaptation Details

General

* **Adaptation Name:** SBCE for PCIPal

Notes: Used for PCIPal

* **Module Name:** DigitConversionAdapter

Type: digit

State: enabled

Module Parameter Type: Name-Value Parameter

Name	Value
fromto	true
iodstd	avaya.com
iosrcd	avaya.com

Select : All, None Page 1 of 2

6.2. Add SIP Entities

In the sample configuration, two SIP Entities were added for Communication Manager and SBCE. This section also covers the configuration of the Entity Links.

6.2.1. Avaya Aura® Communication Manager

A SIP Entity must be added for Communication Manager. To add a SIP Entity, select **Elements** → **Routing** → **SIP Entities** from the top menu, followed by **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of the signaling interface (e.g., procr) on Communication Manager.
- **Type:** Select *CM*.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

Default values can be used for the remaining fields.


The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and tabs for 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. A search bar and a user profile 'admin' are also present. The left sidebar shows a navigation menu with 'Routing' selected, and a sub-menu with 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities' (highlighted), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', and 'Regular Expressions'. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields: 'Name' (devcon-cm SBC Trk), 'FQDN or IP Address' (10.64.102.115), 'Type' (CM), 'Notes' (From SBCE), 'Adaptation' (CM SBC Adaptation), 'Location' (Thornton), 'Time Zone' (America/New_York), 'SIP Timer B/F (in seconds)' (4), 'Minimum TLS Version' (Use Global Setting), 'Credential name' (empty), 'Securable' (checkbox), and 'Call Detail Recording' (none). 'Commit' and 'Cancel' buttons are at the top right of the form.

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name (e.g., *devcon-cm SBC Trk Link*).
- **Protocol:** Set to *TLS*.
- **Port:** Set to *5062*.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** Set to *5062*.
- **Connection Policy:** Set to *trusted*.

Entity Links

Override Port & Transport with DNS SRV: ☐

<input type="button" value="Add"/> <input type="button" value="Remove"/>							
1 Item 							
Filter: Enable							
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* devcon-cm SBC Trk Link	<input type="text" value="devcon-sm"/>	TLS ▼	* 5062	<input type="text" value="devcon-cm SBC Trk"/>	* 5062	trusted ▼

Select : [All](#), [None](#)

6.2.2. SIP Entity for SBCE

A SIP Entity must be added for SBCE. To add a SIP Entity, select **Elements** → **Routing** → **SIP Entities** from the top menu, followed by **New** in the subsequent screen (not shown) to add a new SIP entity for SBCE.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the SBCE internal interface.
- **Type:** Select *SIP Trunk*.
- **Adaptation :** Select the Adaptation configured in **Section 6.1**.
- **Location:** Select the appropriate pre-existing location name.
- **Time Zone:** Time zone for this location.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, version information, and user options. The left sidebar shows a tree view with 'Routing' selected. The main panel is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows:

- Name:** devcon-sbce
- FQDN or IP Address:** 10.64.102.106
- Type:** SIP Trunk
- Notes:** (empty text area)
- Adaptation:** SBCE for PCIPal
- Location:** Thornton-SBC
- Time Zone:** America/New_York
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** egress




'Commit' and 'Cancel' buttons are located at the top right of the form area.

Scroll down to the **Entity Links** sub-section and click **Add** to add an entity link. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name (e.g., *devcon-sm*).
- **Protocol:** Set to *TLS*.
- **Port:** Set to *5061*.
- **SIP Entity 2:** The SBCE entity name from this section.
- **Port:** Set to *5061*.
- **Connection Policy:** Set to *trusted*.

Entity Links

Override Port & Transport with DNS SRV: ☐

Add Remove		1 Item  Filter: Enable					
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* devcon-sbce Link	 devcon-sm	TLS ▼	* 5061	 devcon-sbce	* 5061	trusted ▼

Select : All, None

6.3. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.2**. A routing policy was added for Communication Manager to route incoming calls from the VoIP Service Provider. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition. The following screen shows the Communication Manager Policy.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows a tree view with 'Routing' selected, and sub-items like Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, and Routing Policies. The main content area is titled 'Routing Policy Details' and contains a 'Commit' button and a 'Cancel' button. The 'General' tab is active, showing fields for 'Name' (devcon-cm SBC Trk Policy), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. Below this is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
devcon-cm SBC Trk	10.64.102.115	CM	From SBCE

The 'Time of Day' section is partially visible at the bottom.

Another routing policy was added for SBCE, which routes outgoing calls to the VoIP Service Provider.

AVAYA
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search 🔍 🔔 ☰ admin

Home Routing

Routing

- Domains
- Locations
- Conditions
- Adaptations ▾
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies

Routing Policy Details Commit Cancel Help ?

General

* **Name:** devcon-sbce Policy

Disabled: ☐

* **Retries:** 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
devcon-sbce	10.64.102.106	SIP Trunk	

Time of Day

6.4. Add Dial Patterns

Dial patterns are defined to direct calls to the appropriate SIP Entity. In the sample configuration, numbers beginning with +1 are routed to Communication Manager.

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min:** Minimum length of dialed number.
- **Max:** Maximum length of dialed number.
- **SIP Domain:** SIP domain of dial pattern.
- **Notes:** Comment on purpose of dial pattern (optional).

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows the dial pattern definition for routing calls to Communication Manager.

AVAYA
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search 🔍 | admin

Home Routing

Routing

Domains

Locations

Conditions

Adaptations ▾

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Dial Pattern Details [Commit] [Cancel]

General

* Pattern: +1

* Min: 11

* Max: 12

Emergency Call: ☐

SIP Domain: -ALL-

Notes: Used for PCIPal - Incoming Calls from PSTN

Originating Locations and Routing Policies

[Add] [Remove]

1 Item

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		devcon-cm SBC Trk Policy	0	<input type="checkbox"/>	devcon-cm SBC Trk	

Select : All, None

A Dial Pattern was also created for 11-digit numbers beginning with *1908* that are routed to the SBCE as shown below.

AVAYA Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Search 🔍 🔔 ☰ | admin

Home Routing

Routing

Domains

Locations

Conditions

Adaptations ▾

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 1908

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: -ALL-

Notes: Used for PCIPal - PSTN Calls

Originating Locations and Routing Policies

Add Remove

1 Item

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		devcon-sbce Policy	0	<input type="checkbox"/>	devcon-sbce	

Select : All, None

6.5. Add Session Manager

To complete the configuration, adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

Under *General*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface

Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.

The screenshot displays the 'Edit Session Manager' configuration page in the Avaya Aura System Manager 10.1 interface. The page is organized into two main sections: 'General' and 'Security Module'. The 'General' section contains the following fields: 'SIP Entity Name' (devcon-sm), 'Description' (empty), 'Management Access Point Host Name/IP' (10.64.102.116), 'Direct Routing to Endpoints' (Enable), 'Avaya Aura Device Services Server Pairing' (dropdown), and 'Maintenance Mode' (checkbox). The 'Security Module' section contains the following fields: 'SIP Entity IP Address' (10.64.102.117), 'Network Mask' (255.255.255.0), 'Default Gateway' (10.64.102.1), 'Call Control PHB' (46), and 'SIP Firewall Configuration' (SM 6.3.8.0). The interface also features a sidebar with navigation options and a top header with user information and search bar.

The following screen shows the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to SIP Entities, including SBCE. Use default values for the remaining fields. Click **Commit** to add this Session Manager. In the following configuration, Session Manager sends a SIP Options message every *600* secs. If there is no response, Session Manager will send a SIP Options message every *120* secs.

Monitoring ▼

Enable SIP Monitoring ☒

*Proactive cycle time (secs)

600

*Reactive cycle time (secs)

120

*Number of Tries

1

*Number of Successes

1

Enable CRLF Keep Alive Monitoring ☐

*CRLF Ping Interval (secs)

0

7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya SBCE. Avaya SBCE provides SIP connectivity to Session Manager, VoIP Service Provider, and PCI Pal Agent Assist.

This section covers the following SBCE configuration:

- Launch SBCE Web Interface
- Administer Server Interworking Profiles
- Administer SIP Servers
- Administer Routing Profiles
- Administer Signaling Manipulation Scripts
- Administer URI Groups
- Administer Media Rules
- Administer End Point Policy Groups
- Administer TLS Management
- Administer Media Interfaces
- Administer Signaling Interfaces
- Administer End Point Flows

Note: For security reasons, public IP addresses will be blacked out in these Application Notes.

7.1. Launch SBCE Web Interface

Access the SBCE web interface by using the URL **https://<ip-address>/sbc** in an Internet browser window, where <ip-address> is the IP address of the SBCE management interface. The screen below is displayed. Log in using the appropriate credentials.



The image shows the login page of the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' in bold black. On the right, under the heading 'Log In', there is a 'Username:' label followed by a text input field. Below the input field is a 'Continue' button. Further down, the text 'WELCOME TO AVAYA SBC' is displayed. Below that is a warning message: 'Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.' This is followed by a consent statement: 'Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.' At the bottom, the copyright notice '© 2011 - 2020 Avaya Inc. All rights reserved.' is shown.

After logging in, the Dashboard will appear as shown below. All configuration screens of the SBCE are accessed by navigating the menu tree in the left pane. Select **Device** → **SBCE** from the top menu.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services▸ Domain Policies▸ TLS Management▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

Dashboard

Information		
System Time	11:01:28 AM EDT	Refresh
Version	10.1.1.0-35-21872	
GUI Version	10.1.1.0-21872	
Build Date	Mon Apr 18 07:57:04 UTC 2022	
License State	✔ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	07/12/2022 08:52:18 EDT	
Failed Login Attempts	0	

Active Alarms (past 24 hours)	
None found.	

Installed Devices	
EMS	
SBCE	

Incidents (past 24 hours)	
SBCE: No Server Flow Matched for Outgoing Message	
SBCE: No Server Flow Matched for Outgoing Message	
SBCE: No Server Flow Matched for Outgoing Message	
SBCE: No Server Flow Matched for Outgoing Message	
SBCE: No Server Flow Matched for Outgoing Message	

Add

Notes	
No notes found.	

JAO; Reviewed:
SPOC 8/25/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

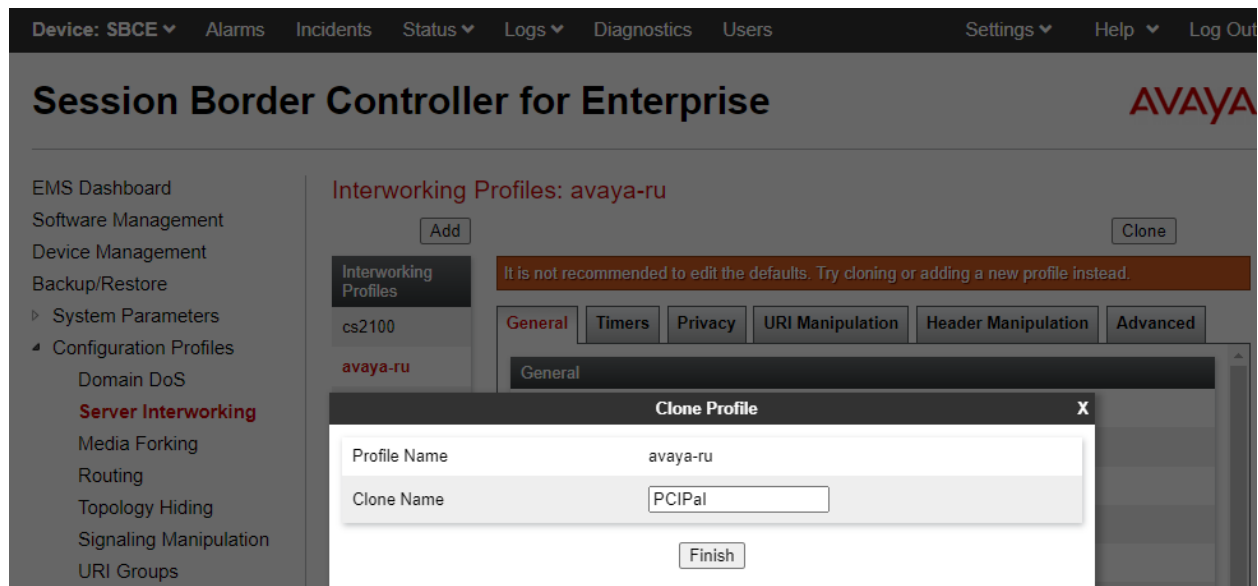
32 of 76
PCIPalAA-SBCE10

7.2. Administer Server Interworking Profiles

A server interworking profile defines a set of parameters that aid in interworking between the SBCE and a connected server. **Server Interworking** profiles were added for PCI Pal, Session Manager, and VoIP Service Provider.

7.2.1. Server Interworking Profile for PCI PAL Agent Assist

To create a new **Server Interworking** profile, select **Configuration Profiles → Server Interworking** from the left-hand menu. A new profile may be created by cloning an existing profile. Select the **avaya-ru** profile and click **Clone**. Type in a **Clone Name** for the PCI Pal profile. Select **Finish** once done.



Once added, select the PCI Pal profile and select the **General** tab to modify it. Enable **Delayed SDP Handling**. When **Delayed SDP Handling** is enabled, SBCE will include SDP in a re-INVITE sent to Agent Assist. This is required because SBCE may receive a re-INVITE without SDP from Communication Manager to shuffle a call (i.e., Direct IP Media) or un-shuffle a call when a media resource is required to send a DTMF tone.

Device: SBCE
Alarms
Incidents
Status
Logs
Diagnostics
Users
Settings
Help
Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Domain DoS

Server

Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

URN Profile

Recording Profile

H248 Profile

IP/URI Blocklist Profile

Services

SIP Servers

H248 Servers

LDAP

RADIUS

Domain Policies

TLS Management

Interworking Profiles: PCIPal

Add

Interworking Profiles

cs2100

avaya-ru

Avaya-SM

PSTN-SIP

PCIPal

VoIPSP

Click here to add a description.

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced


General

Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	Yes
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

Select the **Timers** tab. For the compliance test, the following timers were configured.

Device: sbce801 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise



▸ System Parameters

▾ Configuration Profiles

Domain DoS

Server

Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

URN Profile

Interworking Profiles: PCIPal

Add

Interworking Profiles

cs2100

avaya-ru

ServiceProvider

SessionManager

PCIPal

NICE

VoIPSP

Rename

Clone

Delete

Click here to add a description.

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

SIP Timers

Min-SE	1200 seconds
Init Timer	100 milliseconds
Max Timer	200 milliseconds
Trans Expire	3 seconds
Invite Expire	180 seconds
Retry After	2 seconds

Edit

Select the **Advanced** tab and configure the fields as the screen capture below. Note that **DTMF Support** is set to *RFC 2833 Relay & SIP INFO*. Agent Assist receives the PIN to secure the call using SIP INFO, and once the call is secured, card payment information is received using RFC2833.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▾ Configuration Profiles
 Domain DoS
 Server
 Interworking
 Media Forking
 Routing
 Topology Hiding
 Signaling Manipulation
 URI Groups
 SNMP Traps
 Time of Day Rules
 FGDN Groups
 Reverse Proxy Policy
 URN Profile
 Recording Profile

Interworking Profiles: PCIPal

Add

Interworking Profiles
cs2100
avaya-ru
Avaya-SM
PSTN-SIP
PCIPal
VoIPSP

Click here to add a description.

General Timers Privacy URI Manipulation Header Manipulation **Advanced**

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

DTMF

DTMF Support

RFC 2833 Relay & SIP INFO

Edit

JAO; Reviewed:
SPOC 8/25/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

36 of 76
PCIPalAA-SBCE10

7.2.2. Server Interworking Profile for Session Manager

Session Manager profile was cloned from the same **avaya-ru** profile. The **General** tab below shows the default settings.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

Domain DoS

Server

Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

URN Profile

Recording Profile

H248 Profile

IP/URI Blocklist Profile

▾ Services

SIP Servers

H248 Servers

LDAP

RADIUS

▸ Domain Policies

▸ TLS Management

Interworking Profiles: Avaya-SM

Add

Interworking Profiles

cs2100

avaya-ru

Avaya-SM

PSTN-SIP

PCIPal

VoIPSP

Rename

Clone

Delete

Click here to add a description.

General

Timers

Privacy

URI Manipulation

Header Manipulation

Advanced

General

Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

JAO; Reviewed:
SPOC 8/25/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

37 of 76
PCIPalAA-SBCE10

Select the **Advanced** tab and configure as shown in the screen capture below.

Device: SBCE ▾

Alarms

Incidents

Status ▾

Logs ▾

Diagnostics

Users

Settings ▾

Help ▾

Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

Domain DoS

Server

Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

URN Profile

Recording Profile

Interworking Profiles: Avaya-SM

Add

RenameCloneDelete

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader Manipulation**Advanced**

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

DTMF

DTMF Support	None
--------------	------

Edit

7.2.3. Server Interworking Profile for VoIP Service Provider

VoIP Service Provider profile was cloned from the same **avaya-ru** profile. The **General** tab below shows the default settings.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▾ Configuration ProfilesDomain DoS**Server****Interworking**Media ForkingRoutingTopology HidingSignalingManipulationURI GroupsSNMP TrapsTime of Day RulesFGDN GroupsReverse ProxyPolicyURN ProfileRecording ProfileH248 ProfileIP/URI BlocklistProfile▾ ServicesSIP ServersH248 ServersLDAPRADIUS▸ Domain Policies▸ TLS Management

Interworking ProfilesAddRenameCloneDelete

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
MediaSec	No

JAO; Reviewed:
SPOC 8/25/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

39 of 76
PCIPalAA-SBCE10

VoIP Service Provider profile was also cloned from the same **avaya-ru** profile. No changes were made to the cloned profile. The **Advanced** tab screen capture is shown below.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▾ Configuration Profiles

Domain DoS

Server

Interworking

Media Forking

Routing

Topology Hiding

Signaling Manipulation

URI Groups

SNMP Traps

Time of Day Rules

FGDN Groups

Reverse Proxy Policy

URN Profile

Recording Profile

Interworking Profiles: VoIPSP

Add

RenameCloneDelete

Interworking Profiles

cs2100

avaya-ru

Avaya-SM

PSTN-SIP

PCIPal

VoIPSP

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

Record RoutesBoth Sides

Include End Point IP for Context LookupYes

ExtensionsNone

Diversion ManipulationNo

Has Remote SBCYes

Route Response on Via PortNo

Relay INVITE Replace for SIPRECNo

MOBX Re-INVITE HandlingNo

NATing for 301/302 RedirectionYes

DTMF

DTMF SupportNone

Edit

7.3. Administer SIP Servers

A SIP server definition is required for each server connected to SBCE. Add a **SIP Server** for Session Manager, PCI Pal Agent Assist, and VoIP Service Provider. TLS transport was used for the SIP trunks to Session Manager and PCI Pal Agent Assist.

Note: TLS profiles were preconfigured for Session Manager and are not shown in these Application Notes. However, configuration of TLS profiles for PCI Pal Agent Assist are shown in **Section 7.9**.

7.3.1. SIP Server for PCI Pal Agent Assist

The **General** tab of the PCI Pal Agent Assist SIP Server was configured as shown below. TLS transport was used for the PCI Pal Agent Assist SIP trunk. The configuration of the **TLS Client Profile** is shown in **Section 7.9**. Note that a secondary PCI Pal Agent Assist was configured for redundancy and to test failover scenarios.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo.

The left sidebar contains a navigation menu with the following items:

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
 - SIP Servers**
 - H248 Servers
 - LDAP
 - RADIUS
 - Domain Policies
 - TLS Management
 - Network & Flows
 - DMZ Services
 - Monitoring & Logging

The main content area is titled "SIP Servers: PCIPal" and includes an "Add" button and "Rename", "Clone", and "Delete" buttons. The "General" tab is selected, showing the following configuration:

- Server Type: Trunk Server
- TLS Client Profile: PCIPalClientCert
- DNS Query Type: NONE/A

Below this, a table lists the configured SIP trunks:


IP Address / FQDN	Port	Transport
[Redacted]	3063	TLS
[Redacted]	3063	TLS

An "Edit" button is located at the bottom right of the table.

The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 7.2.1**. All other tabs were left with their default values.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise



EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

- SIP Servers**
- H248 Servers
- LDAP
- RADIUS

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

SIP Servers: PCIPal

Add

Rename Clone Delete

Server Profiles

Session Man...

PSTN-SIP

PCIPal

VoIPSP

General Authentication Heartbeat Registration Ping **Advanced**

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	PCIPal
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

Edit

7.3.2. SIP Server for Session Manager

To define a SIP server, navigate to **Services → SIP Servers** from the left pane to display the existing SIP server profiles. Click **Add** to create a new SIP Server or select a pre-configured SIP server to view its settings. The **General** tab of the Session Manager SIP Server was configured as follows. TLS transport was used for the Session Manager SIP trunk.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

SIP Servers

H248 Servers

LDAP

RADIUS

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

SIP Servers: Session Manager

Add

Rename Clone Delete

Server Profiles

Session Man...

PSTN-SIP

PCIPal

VoIPSP

General Authentication Heartbeat Registration Ping Advanced

Server Type

Call Server

TLS Client Profile

sbceInternal

DNS Query Type

NONE/A

IP Address / FQDN	Port	Transport
10.64.102.117	5061	TLS

Edit

The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 7.2.2**. All other tabs were left with their default values.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for Enterprise

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services

- SIP Servers
 - H248 Servers
 - LDAP
 - RADIUS
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

SIP Servers: Session Manager

Add

Server Profiles

Session Man...

PSTN-SIP

PCIPal

VoIPSP

RenameCloneDelete

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Enable DoS Protection☐

Enable Grooming☒

Interworking ProfileAvaya-SM

Signaling Manipulation ScriptNone

Securable☐

Enable FGDN☐

Tolerant☐

URI GroupNone

NG911 Support☐

Edit

JAO; Reviewed:
SPOC 8/25/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

44 of 76
PCIPalAA-SBCE10

7.3.3. SIP Server for VoIP Service Provider

The **General** tab of the VoIP Service Provider SIP Server was configured as shown below. UDP transport was used for the VoIP Service Provider SIP trunk. The VoIP Service Provider was accessible via any one of four IP addresses.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▾ Services

SIP Servers

H248 Servers

LDAP

RADIUS

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

SIP Servers: VoIPSP

Add

Rename

Clone

Delete

Server Profiles

Session Man...

PSTN-SIP

PCIPal

VoIPSP

General

Authentication

Heartbeat

Registration

Ping

Advanced

Server Type

Trunk Server

DNS Query Type

NONE/A

IP Address / FQDN	Port	Transport
██████████	5060	UDP
██████████	5060	UDP
██████████	5060	UDP
██████████	5060	UDP

Edit

The **Advanced** tab was configured as follows. Note that **Interworking Profile** was set to the one configured in **Section 7.2.3**. All other tabs were left with their default values.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for Enterprise

AVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services

SIP ServersH248 ServersLDAPRADIUS▸ Domain Policies▸ TLS Management▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

SIP Servers: VoIPSP

Add

RenameCloneDelete

Server ProfilesSession Man...PSTN-SIPPCIPalVoIPSP

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

Enable DoS Protection☐

Enable Grooming☒

Interworking ProfileVoIPSP

Signaling Manipulation ScriptNone

Securable☐

Enable FGDN☐

Tolerant☐

URI GroupNone

NG911 Support☐

Edit

JAO; Reviewed:
SPOC 8/25/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

46 of 76
PCIPalAA-SBCE10

7.4. Administer Routing Profiles

A routing profile is used to specify the next-hop for a SIP message. A routing profile is applied only after the traffic has matched an End Point Flow defined in **Section 7.12**. The IP addresses and ports defined here will be used as destination addresses for signaling. Create a routing profile for Session Manager, PCI Pal Agent Assist, and VoIP Service Provider.

7.4.1. Routing Profile for PCI Pal Agent Assist

Two routing profiles were added for PCI Pal Agent Assist for inbound and outbound calls. The routing profile for inbound calls from the VoIP Service Provider to Session Manager is shown below. The routing profile was named *PCIPalInbound*. This routing profile contains two routing rules. The first routing rule with **Priority** of 1 is used to route calls through Agent Assist if the incoming number matches the URI Group *PCIPAL-Bound* configured in **Section 7.6**. The second routing rule with **Priority** of 2 is used to route all other calls directly to Session Manager – bypassing Agent Assist.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▾ Configuration Profiles
 Domain DoS
 Server Interworking
 Media Forking
 Routing
 Topology Hiding
 Signaling Manipulation
 URI Groups
 SNMP Traps

Routing Profiles: PCIPalInbound

Add

Routing Profiles

default

PSTN-SIP

Session Mana...

PCIPalInbound

PCIPalOutbou...

VoIPSP

Rename Clone Delete

Click here to add a description.

Routing Profile

Update Priority Add

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	PCIPAL-Bound	default	Priority	[REDACTED]:3063 10.64.102.117:5061	TLS	Edit Delete
2	*	default	Priority	10.64.102.117:5061	TLS	Edit Delete

JAO; Reviewed:
SPOC 8/25/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

47 of 76
PCIPalAA-SBCE10

The first routing rule of Routing Profile *PCIPALInbound* is shown more detail below. It contains three routing preferences, the primary Agent Assist, the secondary Agent Assist, and Session Manager in that priority order.

Profile : PCIPalInbound - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input checked="" type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				PCIPal		None	Delete
2				PCIPal		None	Delete
3				Session	10.64.102.117:	None	Delete

Finish

The second routing rule of Routing Profile *PCIPALInbound* is shown more detail below. It contains Session Manager as the only routing preference.

Profile : PCIPalInbound - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input checked="" type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Session	10.64.102.117:	None	Delete

Finish

The routing profile for outbound calls from Session Manager to the VoIP Service Provider is shown below. The routing profile was named *PCIPalOutbound*. This routing profile contains three routing preferences, the primary Agent Assist, the secondary Agent Assist, and the VoIP Service Provider in that priority order.

Profile : PCIPalOutbound - Edit Rule

URI Group

*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				PCIPal		None	Delete
2				PCIPal		None	Delete
3				VoIPSP		None	Delete

Finish

7.4.2. Routing Profile for Session Manager

To create a new profile, navigate to **Configuration Profiles → Routing** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by series of pop-up windows in which the profile parameters can be configured. To view the settings of an existing profile, select the profile from the center pane.

The routing profile for calls to Session Manager is shown below. The routing profile was named *Session Manager*. This routing profile contains the IP address of the signaling interface of Session Manager.

Profile : Session Manager - Edit Rule

URI Group

*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight

LDAP Search Attribute

LDAP Search Regex Pattern

LDAP Search Regex Result

SIP Server Profile

Next Hop Address

Transport

1

Session

10.64.102.117

None

Delete

Finish

7.4.3. Routing Profile for VoIP Service Provider

The routing profile for calls to VoIP Service Provider is shown below. The routing profile was named *VoIPSP*. This routing profile contains the IP addresses for accessing the VoIP Service Provider.

Profile : VoIPSP - Edit Rule

URI Group

*

Time of Day

default

Load Balancing

Priority

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight

LDAP Search Attribute

LDAP Search Regex Pattern

LDAP Search Regex Result

SIP Server Profile

Next Hop Address

Transport

1

VoIPSP

None

Delete

2

VoIPSP

None

Delete

3

VoIPSP

None

Delete

4

VoIPSP

None

Delete

Finish

7.5. Administer Signaling Manipulation Scripts

Signaling manipulation scripts provide for the manipulation of SIP messages which cannot be done by another configuration within SBCE. Agent Assist required the signaling manipulation scripts in this section. It is applied to the End Point Flows in **Section 7.12**.

To create a script, navigate to **Configuration Profiles** → **Signaling Manipulation** in the left pane. In the center pane, select **Add**. A script editor window (not shown) will appear in which the script can be entered line by line. The **Title** field at the top of the editor window (not shown) is where the script name is entered. Once complete, the script is displayed. To view an existing script, select the script from the list.

The following signaling manipulation script, named *PCIPalInbound*, inserts the **X-pcipal-route** header with a value of *Avaya_Inbound* in the SIP INVITE of an inbound call from the VoIP Service Provider.

```
within session "INVITE"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    if (%INITIAL_REQUEST = "true" ) then
    {
      %HEADERS["X-pcipal-route"][1] = "Avaya_Inbound";
    }
  }
}
```

The screenshot displays the SBCE web interface. At the top, a navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left-hand navigation menu lists various management options, with "Signaling Manipulation" highlighted in red. The main content area is titled "Signaling Manipulation Scripts: PCIPalInbound" and features buttons for Upload, Add, Download, Clone, and Delete. Below these is a blue bar with the text "Click here to add a description." A list of scripts is shown, with "PCIPalInbound" selected. The script content is displayed in a text area, showing the same code as in the previous block. An "Edit" button is located at the bottom right of the script content area.

The following signaling manipulation script, named *PCIPalIOutbound*, inserts the **X-pcival-route** header with a value on *Avaya_Outbound* in the SIP INVITE of an outbound call to the VoIP Service Provider.

```
within session "INVITE"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    if (%INITIAL_REQUEST = "true" ) then
    {
      %HEADERS["X-pcival-route"][1] ="Avaya_Outbound";
    }
  }
}
```

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. At the top, a dark navigation bar contains links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. Below this, the main header reads "Session Border Controller for Enterprise" with the AVAYA logo on the right. A left-hand navigation menu lists various management options, with "Signaling Manipulation" highlighted in red. The main content area is titled "Signaling Manipulation Scripts: PCIPalOutbound" and includes buttons for Upload, Add, Download, Clone, and Delete. A blue box prompts the user to "Click here to add a description." Below this, a tab labeled "Signaling Manipulation" shows the script content:

```
within session "INVITE"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    if (%INITIAL_REQUEST = "true") then
    {
      %HEADERS["X-pcival-route"][1] = "Avaya_Outbound";
    }
  }
}
```

 An "Edit" button is located at the bottom right of the script editor.

7.6. Administer URI Groups

A **URI Group** defines any number of logical URI groups consisting of each SIP subscriber location in the particular domain or group. For this solution, a **URI Group** named *PCIPal* that is assigned to the *OutboundPCIPal* endpoint flow configured in **Section 7.12.1**. In order for the SBCE to select the *OutboundPCIPal* endpoint flow, either (1) the domain in the From header must match *10.64.102.106*, which is the SIP IP Address of Session Manager, or (2) the user part of the From header must start with *101* and the domain in the From header must be the PCI Pal Agent Assist IP address or domain.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various management options, with "URI Groups" highlighted. The main content area is titled "URI Groups: PCIPal" and features an "Add" button, "Rename", and "Delete" buttons. A description field contains the text "Click here to add a description." Below this, a "URI Group" section includes an "Add" button and a "URI Listing" table. The table lists two URIs: "101*@" and "*@10.64.102.106", each with "Edit" and "Delete" buttons.

In addition, another URI Group, *PCIPAL-Bound*, may be added to specify which calls should be routed to Agent Assist based on the number in the To header. This URI group was assigned to the *PCIPALInbound* routing profile in **Section 7.4.1**.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface, similar to the previous one but for the "PCIPAL-Bound" URI Group. The top navigation bar and main header are identical. The sidebar menu also highlights "URI Groups". The main content area is titled "URI Groups: PCIPAL-Bound" and includes "Add", "Rename", and "Delete" buttons. The description field contains "Click here to add a description." The "URI Group" section has an "Add" button and a "URI Listing" table. The table lists one URI: "*720[REDACTED]@", with "Edit" and "Delete" buttons.

7.7. Administer Media Rules

A media rule defines the processing to be applied to the selected media. A media rule is one component of the larger endpoint policy group defined in **Section 7.8**. For the compliance test, two new media rules were created, one for Session Manager and another one for Agent Assist. A pre-existing media rule, *default-low*, will be used for the VoIP Service Provider.

To view an existing rule, navigate to **Domain Policies** → **Media Rules** in the left pane. In the center pane, select the rule (e.g., *RTP-SRTP*) to be viewed. The content of the *RTP-SRTP* media rule, used for Session Manager, is described below. The **Encryption** tab was configured as shown below. It supports both SRTP and RTP. Note that the SRTP cipher is *SRTP_AES_CM_128_HMAC_SHA1_80*, which is different than the cipher used in the PCI Pal media rule. Refer to **Section 2.2** for the reason why they must be different.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▾ Domain Policies

▾ Application Rules

▾ Border Rules

Media Rules

▾ Security Rules

▾ Signaling Rules

▾ Charging Rules

▾ End Point Policy Groups

▾ Session Policies

▸ TLS Management

▸ Network & Flows

▸ DMZ Services

▸ Monitoring & Logging

Media Rules: RTP-SRTP

Add

Media Rules

default-low-med

default-low-m...

default-high

default-high-enc

avaya-low-me...

RTP-SRTP

RTP-SRTP-P...

Rename

Clone

Delete

Click here to add a description.

Encryption

Codec Prioritization

Advanced

QoS

Audio Encryption

Preferred FormatsSRTP_AES_CM_128_HMAC_SHA1_80
RTP

Encrypted RTCP☐

MKI☐

LifetimeAny

Interworking☒

Symmetric Context Reset☒

Key Change in New Offer☐

Video Encryption

Preferred FormatsRTP

Interworking☒

Symmetric Context Reset☒

Key Change in New Offer☐

Miscellaneous

Capability Negotiation☐

Edit

The content of the *RTP-SRTP-PCIPAL* media rule, used for Agent Assist, is described below. The **Encryption** tab was configured as shown below. It supports both SRTP and RTP. Note that the SRTP cipher is SRTP_AES_CM_128_HMAC_SHA1_32, which is different than the cipher used in the Session Manager media rule. Refer to **Section 2.2** for the reason why they must be different.

Device: SBCE ▾
Alarms
Incidents
Status ▾
Logs ▾
Diagnostics
Users
Settings ▾
Help ▾
Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
Charging Rules
End Point Policy Groups
Session Policies
TLS Management
Network & Flows
DMZ Services
Monitoring & Logging

Media Rules: RTP-SRTP-PCIPAL

Add
Rename
Clone
Delete

Click here to add a description.

Encryption
Codec Prioritization
Advanced
QoS

Audio Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_32 RTP
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption

Preferred Formats	RTP
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous

Capability Negotiation	<input type="checkbox"/>
------------------------	--------------------------

Edit

The **Codec Prioritization** tab for the *RTP-SRTP-PCIPAL* media rule was configured as shown below.

Device: SBCE ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardSoftware ManagementDevice ManagementBackup/Restore▸ System Parameters▸ Configuration Profiles▸ Services▾ Domain PoliciesApplication RulesBorder RulesMedia RulesSecurity RulesSignaling RulesCharging RulesEnd Point Policy GroupsSession Policies▸ TLS Management▸ Network & Flows▸ DMZ Services▸ Monitoring & Logging

Media Rules: RTP-SRTP-PCIPAL

AddRenameCloneDelete

Click here to add a description.

EncryptionCodec PrioritizationAdvancedQoS

Audio Codec

Codec Prioritization	<input checked="" type="checkbox"/>
Allow Preferred Codecs Only	<input type="checkbox"/>
Transcode When Needed	<input checked="" type="checkbox"/>
Transrating	<input type="checkbox"/>
Preferred Codecs	PCMU (0) [T], telephone-event [D]

Video Codec

Codec Prioritization	<input type="checkbox"/>
----------------------	--------------------------

Edit

JAO; Reviewed:
SPOC 8/25/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

57 of 76
PCIPalAA-SBCE10

7.8. Administer End Point Policy Groups

An endpoint policy group is a set of policies that will be applied to traffic between the SBCE and an endpoint (connected server). Two endpoint policy groups must be created for Session Manager and Agent Assist. The VoIP Service Provider will use a pre-existing endpoint policy group. The endpoint policy group is applied to the traffic as part of the endpoint flow defined in **Section 7.12**.

To create a new group, navigate to **Domain Policies → End Point Policy Groups** in the left pane. In the right pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new group, followed by the **Policy Group** window (not shown) to configure the group parameters. Once complete, the settings will be displayed. To view the settings of an existing group, select the group from the list. The settings will appear in the right pane.

The new endpoint policy group, named *RTP-SRTP*, is shown below and is assigned the *RTP-SRTP* media rule configured above. This endpoint policy group is used for Session Manager.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The left sidebar lists various management options, with 'Domain Policies' expanded to show 'End Point Policy Groups'. The main content area is titled 'Policy Groups: RTP-SRTP' and features a table with two entries: 'RTP-SRTP' and 'RTP-SRTP-P...'. An 'Edit Policy Set' modal window is open, showing configuration options for the selected group. The modal includes dropdown menus for Application Rule (default), Border Rule (default), Media Rule (RTP-SRTP), Security Rule (default-low), Signaling Rule (default), Charging Rule (None), and RTCP Monitoring Report Generation (Off). A 'Finish' button is located at the bottom of the modal.

Edit Policy Set	
Application Rule	default
Border Rule	default
Media Rule	RTP-SRTP
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

The new endpoint policy group, named *RTP-SRTP-PCIPAL*, is shown below and is assigned the *RTP-SRTP-PCIPAL* media rule configured above. This endpoint policy group is used for Agent Assist.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. The left sidebar lists various management options, with 'End Point Policy Groups' highlighted. The main content area is titled 'Policy Groups: RTP-SRTP-PCIPAL'. A modal dialog titled 'Edit Policy Set' is open, showing configuration options for the policy group. The dialog includes a 'Finish' button and a 'Summary' button. The configuration options are as follows:

Policy Group	Application Rule	Border Rule	Media Rule	Security Rule	Signaling Rule	Charging Rule	RTCP Monitoring Report Generation
RTP-SRTP-PCIPAL	default	default	RTP-SRTP-PCIPAL	default-low	default	None	Off

7.9. Administer TLS Management

This section covers installing the Agent Assist certificate, configuring the Agent Assist client profile, and configuring the server profile for the B2 public interface, which connects to Agent Assist, to set up secure communications using TLS. The TLS configuration for Session Manager is assumed to already be in place and is not shown in these Application Notes.

Navigate to **TLS Management** → **Certificates** and install the Agent Assist CA certificate. For the compliance test, the certificate was named *PCIPalCertGlobal.pem* as shown below.

The screenshot shows the 'Session Border Controller for Enterprise' interface. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. On the left, a sidebar menu lists various management options, with 'TLS Management' and 'Certificates' highlighted. The main content area is titled 'Certificates' and features 'Install' and 'Generate CSR' buttons. It contains two tables: 'Installed Certificates' and 'Installed CA Certificates'. The 'Installed Certificates' table lists 'sbceExternalB2.pem', 'sbceInternal.pem', and 'sbceExternalB1.pem'. The 'Installed CA Certificates' table lists several certificates, including 'AvayaDeviceEnrollmentCAchain.crt', 'avayaitrootca2.pem', 'entrust_g2_ca.cer', 'SystemManagerCA.pem', 'ocpSystemManagerCA.pem', 'ValcomCA.crt', 'OCP_Lab7CACert.cer', 'PCIPalCert.pem', and 'PCIPalCertGlobal.pem'. The 'PCIPalCertGlobal.pem' entry is highlighted with a red box.

Installed Certificates	
sbceExternalB2.pem	View Delete
sbceInternal.pem	View Delete
sbceExternalB1.pem	View Delete

Installed CA Certificates	
AvayaDeviceEnrollmentCAchain.crt	View Delete
avayaitrootca2.pem	View Delete
entrust_g2_ca.cer	View Delete
SystemManagerCA.pem	View Delete
ocpSystemManagerCA.pem	View Delete
ValcomCA.crt	View Delete
OCP_Lab7CACert.cer	View Delete
PCIPalCert.pem	View Delete
PCIPalCertGlobal.pem	View Delete

Next, create a client profile for Agent Assist as shown below. The **Profile Name** was set to *PCIPalClientCert* and the certificate for B2 public interface was selected. **Peer Verification** was set to *Required* and the *PCIPalCertGlobal.pem* certificate was selected for **Peer Certificate Authorities**. The **Verification Depth** was set to 2 and the **Version** was set to *TLS 1.2*. This client profile was assigned to the Agent Assist SIP server in **Section 7.3.1**.

Device: SBCE ▾
Alarms
Incidents
Status ▾
Logs ▾
Diagnostics
Users
Settings ▾
Help ▾
Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Certificates
Client Profiles
Server Profiles
SNI Group
Network & Flows
DMZ Services
Monitoring & Logging

Client Profiles: PCIPalClientCert

Add
Delete

Client Profiles
sbceInternal
sbceExternalB2
ValcomRW
sbceExternalB1
PCIPalClient...

Click here to add a description.

Client Profile

TLS Profile

Profile Name	PCIPalClientCert
Certificate	sbceExternalB2.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	PCIPalCertGlobal.pem
Peer Certificate Revocation Lists	---
Verification Depth	2
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options

Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:IMD5:!aNULL:!eNULL:@STRENGTH

Edit

JAO; Reviewed:
SPOC 8/25/2022


Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

61 of 76
PCIPalAA-SBCE10

The following server profile is assigned to the B2 public interface covered in **Section 7.11**.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise



EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
 Certificates
 Client Profiles
 Server Profiles
 SNI Group
▸ Network & Flows
▸ DMZ Services
▸ Monitoring & Logging

Server Profiles: sbceExternalB2

Add

Delete

Server Profiles

sbceExternalB1
sbceExternal...
sbceInternal

Click here to add a description.

Server Profile

TLS Profile

Profile Name

sbceExternalB2

Certificate

sbceExternalB2.pem

SNI Options

None

Certificate Verification

Peer Verification

None

Extended Hostname Verification

☐

Renegotiation Parameters

Renegotiation Time

0

Renegotiation Byte Count

0

Handshake Options

Version

☒ TLS 1.2 ☐ TLS 1.1 ☐ TLS 1.0

Ciphers

☒ Default ☐ FIPS ☐ Custom

Value

HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

7.10. Administer Media Interfaces

A media interface defines an IP address and port range for transmitting media. Create a media interface for both the internal and external sides of the SBCE. Media Interface needs to be defined for each SIP server to send and receive media (RTP or SRTP).

Navigate to **Networks & Flows** → **Media Interface** to define a new media interface. During the compliance test, the following interfaces were defined. For security reasons, public IP addresses have been blacked out. The media interfaces used for this solution are listed below.

- **PrivateMedia:** Interface used by Session Manager to send and receive media.
- **PublicMediaB2:** Interface used by Agent Assist and VoIP Service Provider to send and receive media.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

Network Management

Media Interface

Signaling Interface

End Point Flows

Session Flows

Advanced Options

▸ DMZ Services

▸ Monitoring & Logging

Media Interface

Media Interface

Add

Name	Media IP Network	Port Range	
PrivateMedia	10.64.102.106 Private-A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
PublicMedia	10.64.101.101 Public-B1 (B1, VLAN 0)	35000 - 40000	Edit Delete
PublicMediaB2	██████████ Public-B2 (B2, VLAN 0)	35000 - 40000	Edit Delete
PrivateMediaRW	10.64.102.108 Private-A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
PublicMediaRW	10.64.101.102 Public-B1 (B1, VLAN 0)	35000 - 40000	Edit Delete

7.11. Administer Signaling Interfaces

A signaling interface defines an IP address, protocols and listen ports that the SBCE can use for signaling. Create a signaling interface for both the internal and external sides of the SBCE. Signaling interface needs to be defined for each SIP server to send and receive media (RTP or SRTP).


Navigate to **Networks & Flows** → **Signaling Interface** to define a new signaling interface. During the Compliance Testing the following interfaces were defined. For security reasons, public IP addresses have been blacked out. The signaling interfaces used for this solution are listed below.

- **PrivateSignaling:** Interface used by Session Manager to send and receive calls.
- **ServiceProvider:** Interface used by VoIP Service Provider to send and receive calls.
- **PublicSignalingB2:** Interface used by Agent Assist to send and receive calls.

Note that PCI Pal and VoIP Service Provider use the same physical interface on SBCE.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise



EMS Dashboard

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▸ Domain Policies

▸ TLS Management

▸ Network & Flows

- Network Management
- Media Interface
- Signaling Interface**
- End Point Flows
- Session Flows
- Advanced Options

▸ DMZ Services

▸ Monitoring & Logging

Signaling Interface

Signaling Interface

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
PublicSignaling	10.64.101.101 Public-B1 (B1, VLAN 0)	5060	5060	---	None	Edit Delete
PrivateSignaling	10.64.102.106 Private-A1 (A1, VLAN 0)	5060	5060	5061	sbceInternal	Edit Delete
PrivateSignalingRW	10.64.102.108 Private-A1 (A1, VLAN 0)	5060	5060	5061	sbceInternal	Edit Delete
PublicSignalingRW	10.64.101.102 Public-B1 (B1, VLAN 0)	---	---	5061	sbceExternalB1	Edit Delete
ServiceProvider	██████████ Public-B2 (B2, VLAN 0)	5060	5060	---	None	Edit Delete
PublicSignalingB2	██████████ Public-B2 (B2, VLAN 0)	---	5062	5061	sbceExternalB2	Edit Delete

JAO; Reviewed:
SPOC 8/25/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

64 of 76
PCIPalAA-SBCE10

7.12. Administer End Point Flows

Endpoint flows are used to determine the endpoints (connected servers) involved in a call in order to apply the appropriate policies. When a packet arrives at the SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to policies and profiles that control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of the compliance test, the endpoints are Session Manager, Agent Assist, and the VoIP Service Provider.

Navigate to **Network & Flows → End Point Flows → Server Flows** and select the **Server Flows** tab. The configured **Server Flows** used in the compliance test are shown below. The following subsections will review the settings for each server flow.

Device: SBCE ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Session Border Controller for Enterprise AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ Network & Flows
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 Advanced Options
▸ DMZ Services
▸ Monitoring & Logging

End Point Flows

Subscriber Flows Server Flows

Add

Modifications made to a Server Flow will only take effect on new sessions.

Click here to add a row description.

SIP Server: PCIPal

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	OutboundPCIPal	PCIPal	PrivateSignaling	PublicSignalingB2	RTP-SRTP-PCIPAL	Session Manager	View Clone Edit Delete
2	InboundPCIPal	*	ServiceProvider	PublicSignalingB2	RTP-SRTP-PCIPAL	VoIPSP	View Clone Edit Delete

SIP Server: Session Manager

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Session Manager 1	*	PublicSignalingB2	PrivateSignaling	RTP-SRTP	PCIPalOutbound	View Clone Edit Delete
2	Session Manager 2	*	ServiceProvider	PrivateSignaling	RTP-SRTP	VoIPSP	View Clone Edit Delete

SIP Server: VoIPSP

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Service Provider 1	*	PublicSignalingB2	ServiceProvider	default-low	PCIPalInbound	View Clone Edit Delete
2	Service Provider 2	*	PrivateSignaling	ServiceProvider	default-low	Session Manager	View Clone Edit Delete

JAO; Reviewed:
SPOC 8/25/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

65 of 76
PCIPalAA-SBCE10

7.12.1. End Point Flows for PCI Pal Agent Assist

For the compliance test, two endpoint flows were created for PCI Pal Agent Assist.

For inbound PSTN calls from the VoIP Service Provider, the *OutboundPCIPal* flow shown below is used as the source flow when SBCE receives a SIP INVITE from PCI Pal Agent Assist. This flow is used, because the URI Group matches the 101 prepended to the user part of the From header. The routing profile selects Session Manager as the destination endpoint.

For outbound PSTN calls from Session Manager, this flow is used as the destination flow when a SIP INVITE must be sent to PCI Pal Agent Assist. This flow is used, because URI Group matches the domain in the From header of the SIP INVITE, which contains the SBCE internal interface connected to Session Manager. The **Signaling Manipulation Script** adds a **X-pcipal-route** header with a value of *Avaya_Outbound* to the SIP INVITE sent to PCI Pal Agent Assist.

Edit Flow: OutboundPCIPal	
Flow Name	OutboundPCIPal
SIP Server Profile	PCIPal
URI Group	PCIPal
Transport	*
Remote Subnet	*
Received Interface	PrivateSignaling
Signaling Interface	PublicSignalingB2
Media Interface	PublicMediaB2
Secondary Media Interface	None
End Point Policy Group	RTP-SRTP-PCIPAL
Routing Profile	Session Manager
Topology Hiding Profile	default
Signaling Manipulation Script	PCIPalOutbound
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	

Finish

For inbound PSTN calls from the VoIP Service Provider, the *InboundPCIPal* flow shown below is used as the destination flow when a SIP INVITE must be sent to PCI Pal Agent Assist. The **Signaling Manipulation Script** adds a **X-pcipal-route** header with a value of *Avaya_Inbound* to the SIP INVITE sent to PCI Pal Agent Assist.

For outbound PSTN calls from Session Manager, this flow is used as the source flow when SBCE receives a SIP INVITE from PCI Pal Agent Assist. The routing profile selects the VoIP Service Provider as the destination endpoint.

Edit Flow: InboundPCIPal X

Flow Name	<input type="text" value="InboundPCIPal"/>
SIP Server Profile	<input type="text" value="PCIPal"/> ▼
URI Group	<input type="text" value="*"/> ▼
Transport	<input type="text" value="*"/> ▼
Remote Subnet	<input type="text" value="*"/>
Received Interface	<input type="text" value="ServiceProvider"/> ▼
Signaling Interface	<input type="text" value="PublicSignalingB2"/> ▼
Media Interface	<input type="text" value="PublicMediaB2"/> ▼
Secondary Media Interface	<input type="text" value="None"/> ▼
End Point Policy Group	<input type="text" value="RTP-SRTP-PCIPAL"/> ▼
Routing Profile	<input type="text" value="VoIPSP"/> ▼
Topology Hiding Profile	<input type="text" value="default"/> ▼
Signaling Manipulation Script	<input type="text" value="PCIPalInbound"/> ▼
Remote Branch Office	<input type="text" value="Any"/> ▼
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	<input type="text"/>

Finish

7.12.2. End Point Flows for Session Manager

For the compliance test, two endpoint flows were created for Session Manager. If PCI Pal Agent Assist is available, the destination flow will be one of the PCI Pal flows in **Section 7.12.1**; otherwise, the destination flow will be one of the VoIP Service Provider flows in **Section 7.12.3**.

The *Session Manager 1* flow shown below is used as a source flow for outbound PSTN calls from Session Manager. The routing profile selects PCI Pal Agent Assist as the destination endpoint, if available; otherwise, the VoIP Service Provider is selected as the destination endpoint.

This flow is also used as a destination flow for inbound PSTN calls from the VoIP Service Provider.

Edit Flow: Session Manager 1 X

Flow Name	<input type="text" value="Session Manager 1"/>
SIP Server Profile	<input type="text" value="Session Manager"/>
URI Group	<input type="text" value="*/"/>
Transport	<input type="text" value="*/"/>
Remote Subnet	<input type="text" value="*/"/>
Received Interface	<input type="text" value="PublicSignalingB2"/>
Signaling Interface	<input type="text" value="PrivateSignaling"/>
Media Interface	<input type="text" value="PrivateMedia"/>
Secondary Media Interface	<input type="text" value="None"/>
End Point Policy Group	<input type="text" value="RTP-SRTP"/>
Routing Profile	<input type="text" value="PCIPalOutbound"/>
Topology Hiding Profile	<input type="text" value="None"/>
Signaling Manipulation Script	<input type="text" value="None"/>
Remote Branch Office	<input type="text" value="Any"/>
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	<input type="text"/>

Finish

The *Session Manager 2* flow shown below is used as the destination flow for inbound PSTN calls from the VoIP Service Provider when PCI Pal Agent Assist is not available.

Edit Flow: Session Manager 2		X
Flow Name	<input type="text" value="Session Manager 2"/>	
SIP Server Profile	<input type="text" value="Session Manager"/> ▼	
URI Group	<input type="text" value="*"/> ▼	
Transport	<input type="text" value="*"/> ▼	
Remote Subnet	<input type="text" value="*"/>	
Received Interface	<input type="text" value="ServiceProvider"/> ▼	
Signaling Interface	<input type="text" value="PrivateSignaling"/> ▼	
Media Interface	<input type="text" value="PrivateMedia"/> ▼	
Secondary Media Interface	<input type="text" value="None"/> ▼	
End Point Policy Group	<input type="text" value="RTP-SRTP"/> ▼	
Routing Profile	<input type="text" value="VoIPSP"/> ▼	
Topology Hiding Profile	<input type="text" value="None"/> ▼	
Signaling Manipulation Script	<input type="text" value="None"/> ▼	
Remote Branch Office	<input type="text" value="Any"/> ▼	
Link Monitoring from Peer	<input type="checkbox"/>	
FQDN Support	<input type="checkbox"/>	
FQDN	<input type="text"/>	
<input type="button" value="Finish"/>		

7.12.3. End Point Flows for VoIP Service Provider

For the compliance test, two endpoint flows were created for VoIP Service Provider. If PCI Pal Agent Assist is available, the destination flow will be one of the PCI Pal flows in **Section 7.12.1**; otherwise, the destination flow will be one of the Session Manager flows in **Section 7.12.2**.

The *Service Provider 1* flow shown below is used as the source flow for inbound PSTN calls from the VoIP Service Provider. The routing profiles selects PCI Pal Agent Assist as the destination endpoint, if available; otherwise, Session Manager is selected as the destination endpoint.

This flow is also used as a destination flow for outbound PSTN calls from Session Manager. The Topology Hiding Profile is used for outbound PSTN calls to change the domain in the Request-URI and To header to the domain of the VoIP Service Provider.

Edit Flow: Service Provider 1		X
Flow Name	<input type="text" value="Service Provider 1"/>	
SIP Server Profile	VoIPSP ▼	
URI Group	* ▼	
Transport	* ▼	
Remote Subnet	<input type="text" value="*"/>	
Received Interface	PublicSignalingB2 ▼	
Signaling Interface	ServiceProvider ▼	
Media Interface	PublicMediaB2 ▼	
Secondary Media Interface	None ▼	
End Point Policy Group	default-low ▼	
Routing Profile	PCIPalInbound ▼	
Topology Hiding Profile	VoIPSP ▼	
Signaling Manipulation Script	None ▼	
Remote Branch Office	Any ▼	
Link Monitoring from Peer	<input type="checkbox"/>	
FQDN Support	<input type="checkbox"/>	
FQDN	<input type="text"/>	
<input type="button" value="Finish"/>		

The *Service Provider 2* flow shown below is used as the destination flow for outbound PSTN calls from Session Manager when PCI Pal Agent Assist is not available.

Edit Flow: Service Provider 2		X
Flow Name	<input type="text" value="Service Provider 2"/>	
SIP Server Profile	<input type="text" value="VoIPSP"/>	
URI Group	<input type="text" value="*/"/>	
Transport	<input type="text" value="*/"/>	
Remote Subnet	<input type="text" value="*/"/>	
Received Interface	<input type="text" value="PrivateSignaling"/>	
Signaling Interface	<input type="text" value="ServiceProvider"/>	
Media Interface	<input type="text" value="PublicMediaB2"/>	
Secondary Media Interface	<input type="text" value="None"/>	
End Point Policy Group	<input type="text" value="default-low"/>	
Routing Profile	<input type="text" value="Session Manager"/>	
Topology Hiding Profile	<input type="text" value="VoIPSP"/>	
Signaling Manipulation Script	<input type="text" value="None"/>	
Remote Branch Office	<input type="text" value="Any"/>	
Link Monitoring from Peer	<input type="checkbox"/>	
FQDN Support	<input type="checkbox"/>	
FQDN	<input type="text"/>	
<input type="button" value="Finish"/>		

8. Configure PCI Pal Agent Assist

PCI Pal is responsible for the configuration PCI Pal Agent Assist.

PCI Pal will require that the customer provide the IP addresses and ports used to reach Avaya SBCE at the edge of the enterprise. In addition, TLS certificates must be exchanged.

PCI Pal will provide the IP addresses and ports of Agent Assist. This information is used to complete the SBCE configuration in the previous section.

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, SBCE, and PCI Pal Agent Assist.

1. From the System Manager home page (not shown), select **Elements** → **Session Manager** from the top menu to display the **Session Manager Dashboard** screen (not shown).

Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the Communication Manager entity name from **Section 6.2.1**.

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn. Status** and **Link Status** are “UP”, as shown below.

The screenshot shows the Avaya System Manager 10.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows the 'Session Manager' menu with options like 'Dashboard', 'Session Manager ...', 'Global Settings', 'Communication Prof...', 'Network Configur...', 'Device and Locati...', 'Application Confi...', 'System Status', 'Load Factor', and 'SIP Entity Monit...'. The main content area is titled 'SIP Entity, Entity Link Connection Status' and contains a table of entity links.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: devcon-cm SBC Trk

Summary View

1 Item Filter: Enable

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	devcon-sm	IPv4	10.64.102.115	5062	TLS	FALSE	UP	200 OK	UP

Select : None

2. Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click on the SBCE entity name from **Section 6.2.2**.

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn. Status** and **Link Status** are “UP”, as shown below.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: devcon-sbce

Summary View

1 Item Filter: Enable

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	devcon-sm	IPv4	10.64.102.106	5061	TLS	FALSE	UP	200 OK	UP

Select : None

3. Place an incoming PSTN call from the VoIP Service Provider to an agent in the contact center. Verify the call is established with two-way audio.
4. For the compliance test, a sample PCI Pal Portal was used to obtain a 4-digit code to secure the call. The PCI Pal Portal is displayed below.

PCI Pal 6 Dev Connect

#6729

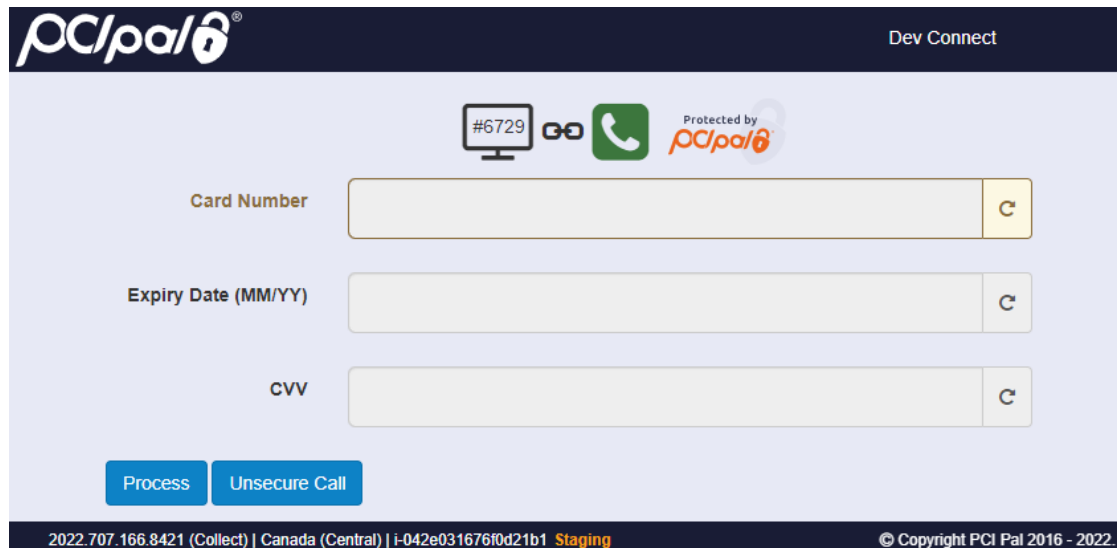
Card Number

Expiry Date (MM/YY)

CVV

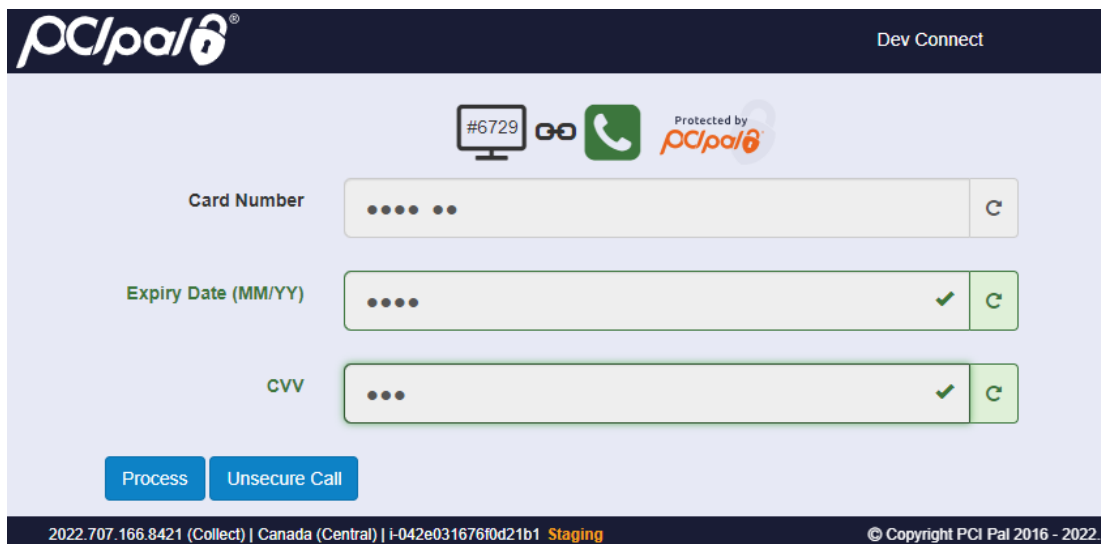
2022.707.166.8421 (Collect) | Canada (Central) | I-042e031676f0d21b1 Staging © Copyright PCI Pal 2016 - 2022.

5. Agent enters the 4-digit code via DTMF and the telephone icon in the PCI Pal Portal changes to green indicating the call is secured as shown below.



The screenshot shows the PCI Pal Portal interface. At the top, the PCI Pal logo is on the left and "Dev Connect" is on the right. Below the header, there are three icons: a monitor with "#6729", a grey telephone icon, and a "Protected by PCI Pal" logo. The main form has three input fields: "Card Number", "Expiry Date (MM/YY)", and "CVV". Each field has a "C" icon on the right. At the bottom, there are two buttons: "Process" and "Unsecure Call". The footer contains the text "2022.707.166.8421 (Collect) | Canada (Central) | i-042e031676f0d21b1 Staging" and "© Copyright PCI Pal 2016 - 2022."

6. While the call is secured, customer sends payment information via DTMF using telephone keypad to PCI Pal Agent Assist. The fields in the PCI Pal Portal are populated with the customer information. The agent hears a mono tone for each DTMF digit sent indicating that the customer is entering data.



The screenshot shows the PCI Pal Portal interface after the call is secured. The telephone icon is now green. The "Card Number" field is populated with five dots. The "Expiry Date (MM/YY)" field is populated with four dots and has a green checkmark. The "CVV" field is populated with three dots and has a green checkmark. The "Process" and "Unsecure Call" buttons are still present. The footer contains the same text as the previous screenshot: "2022.707.166.8421 (Collect) | Canada (Central) | i-042e031676f0d21b1 Staging" and "© Copyright PCI Pal 2016 - 2022."

10. Conclusion

These Application Notes have described the configuration steps required to integrate PCI Pal® Agent Assist with Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and Avaya Session Border Controller for Enterprise. Agents were able to secure customer calls so that card payment information could be sent via DTMF securely to PCI Pal Agent Assist. All test cases passed with an observation noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 1, December 2021, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2022, available at <http://support.avaya.com>.
- [3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022, available at <http://support.avaya.com>.
- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1.x, Issue 1, December 2021, available at <http://support.avaya.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.