



Application Notes for PCI Pal's Agent Assist with Avaya Session Border Controller for Enterprise R8.0 and Avaya Aura® R8.1 environment – Issue 1.0

Abstract

These Application Notes contain instructions for PCI Pal's Agent Assist with Avaya Session Border Controller for Enterprise R8.0 and Avaya Aura® R8.1 environment to successfully interoperate.

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

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

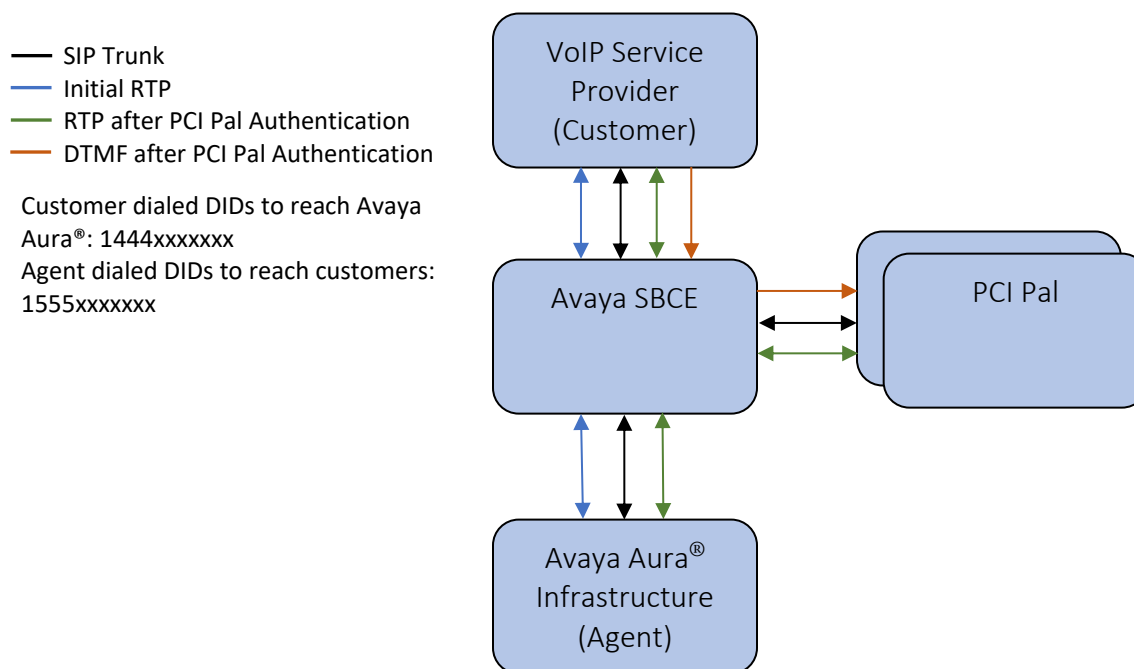
1. Introduction

These Application Notes contain instructions for PCI Pal's Agent Assist (PCI Pal) with Avaya Session Border Controller for Enterprise (Avaya SBCE) and Avaya Aura® environment to successfully interoperate.

Contact centers that use Avaya Aura® environment to accept payments over the phone face operational and technical challenges to ensure compliance when handling sensitive cardholder data. PCI Pal's Agent Assist technology allows contact centers using Avaya Aura® environment to take card payments securely, using DTMF (telephone keypad) capture technology while the contact center agent and customer remain in conversation.

Calls to and from Avaya Aura® environment to VoIP Service Provider are generally routed via Avaya SBCE. Configuration of PCI Pal involves looping such calls at Avaya SBCE. All inbound and outbound calls are routed (looped) via Avaya SBCE to PCI Pal. For a given call, initially, only SIP signalling is looped via Avaya SBCE to PCI Pal, RTP still flows through Avaya SBCE. Once the call is answered by a contact center agent, a 4-digit code provided by PCI Pal is entered by contact center agent, at the time of payment in case one is required. This code is sent to Avaya SBCE via RFC2833 DTMFs. Avaya SBCE converts RFC2833 DTMFs to SIP INFOs and sends them to PCI Pal. Upon successful authentication, PCI Pal sends a re-INVITE to Avaya SBCE to redirect RTP via PCI Pal. Once instructed, customer enters payment details via their phone. These digits are sent to Avaya SBCE via RFC2833 DTMFs, which SBCE converts to SIP INFOs and send them to PCI Pal. For each of the SIP INFOs PCI Pal generates mono tones (and not the actual digits entered by customer) and sends them along with RTP. Mono tones are sent for agents' informational purposes only, to know that customer has entered digits. The diagram below shows a logical view of calls to and from Avaya SBCE.

The PCI Pal solution consists of a third-party SBC in front of the PCI Pal Agent Assist module. The Avaya SBCE only interacts for SIP and RTP (TLS and SRTP) with the third-party SBC.



Note: During the Compliance Testing, a simulated VoIP Service Provider was used.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls from customer and agent were made manually with DTMFs sent from both customer and agent. Necessary user actions were performed from the agent telephones to test different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the network to PCI Pal. Failover tests were performed to verify if one node of PCI Pal is unavailable, calls are failed over to another node.

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.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note 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 utilized encryption capabilities of TLS/SRTP.

2.1. Interoperability Compliance Testing

The interoperability Compliance test included feature and serviceability testing. Feature testing included the validation of the following:

- Inbound calls to Avaya Aura® environment (agents and IVR)
- Outbound calls to VoIP Service Provider
- Proper transmissions of RFC2833 DTMF to Avaya SBCE
- Conversion of RFC2833 to SIP INFO by Avaya SBCE and vice-a-versa
- Proper transmissions of SIP INFOs to/from PCI Pal
- Codec negotiations between Avaya SBCE and PCI Pal
- Redirection of RTP from Avaya SBCE to PCI Pal
- Calls for scenarios involving internal, external, IVR, ACD, non-ACD, mute, hold, reconnect, conference, and transfer.

The serviceability testing focused on verifying the ability of PCI Pal to recover from adverse conditions, such as disconnecting/reconnecting the network to PCI Pal.

Failover tests were performed to verify if one node of PCI Pal is unavailable, calls are failed over to another node.

Although PCI Pal supports TCP/TLS/UDP for SIP Signalling and RTP/SRTP for voice transmission, during the Compliance Testing, SIP signalling utilized TLS transport and SRTP was voice transmission.

2.2. Test Results

All test cases were successfully executed with the exception of the following:

- When SIP INFO is received by Avaya SBCE with Signal value of 11 or 10, Avaya SBCE does not respond with 200 OK or convert the SIP INFO to RFC2833 DTMF. This results in dropped calls. A workaround was put in place where PCI Pal changes Signal value of 11 and 10 to # and *, respectively. When Avaya SBCE receives SIP INFO with Signal value of # and *, it converts it correctly to RFC2833 DTMF. An internal ticket was opened for Avaya SBCE development team to troubleshoot the issue.

2.3. Support

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

- **Phone:** US: +1-855-450-0560
UK: +44 (0)344 544 6858
- **Email:** support@pcipal.com
- **Web:** www.pcipal.com

3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya Products and PCI Pal's Agent Assist. All SIP traffic to and from VoIP service provider to Avaya Aura® environment was routed via PCI Pal through Avaya SBCE. Avaya Aura® environment consisted of the following:

- Avaya Aura® Communication Manager
- Avaya Aura® Media Server
- Avaya Aura® Session Manager
- Avaya Aura® System Manager
- Avaya Aura® Experience Portal
- Avaya G450 Gateway
- Avaya J100 and 9600 Series IP (SIP & H.323) Endpoints
- Avaya Digital Endpoints

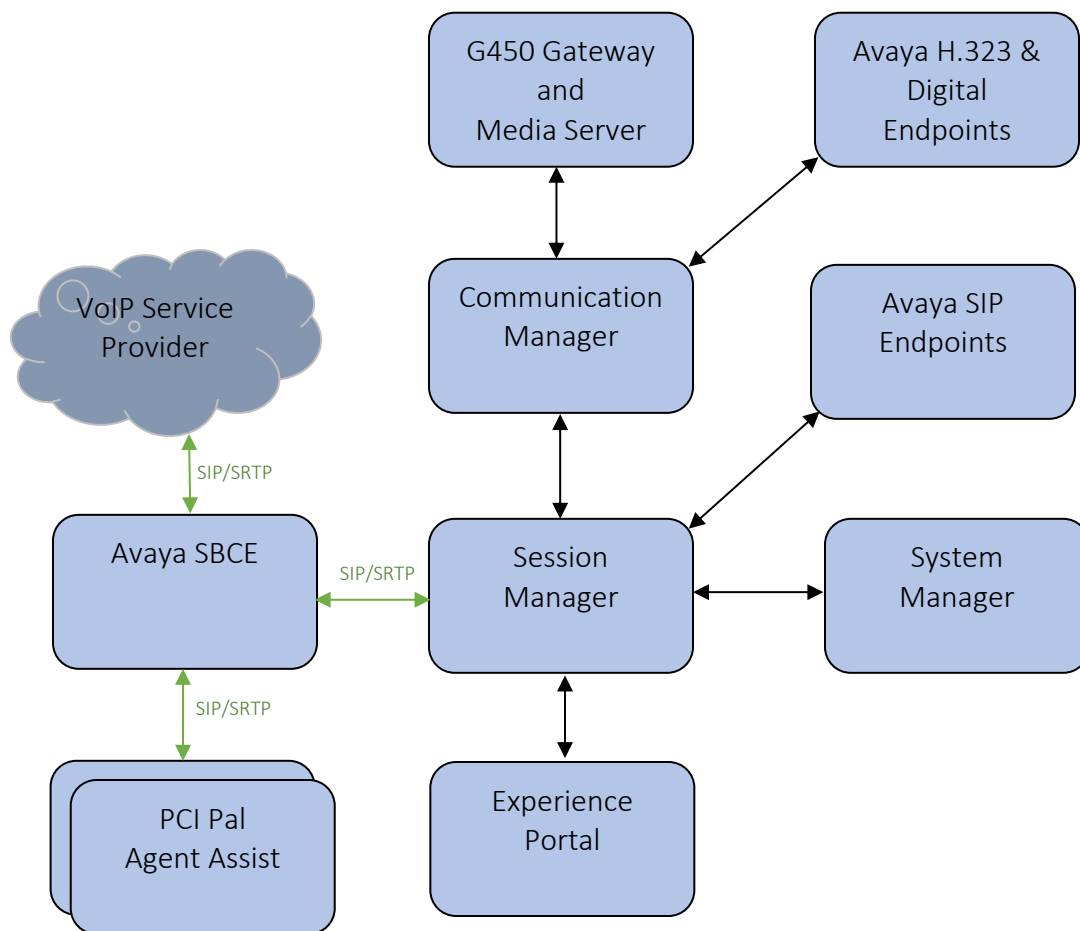


Figure 1: Test Configuration for PCI Pal's Agent Assist and Avaya Aura® Environment.

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	8.1.1
Avaya Aura® Session Manager	8.1.1
Avaya Aura® System Manager	8.1.1
Avaya 9600 Series IP Deskphones	7.1.7 (SIP)
Avaya 9600 Series IP Deskphones	6.8.3 (H.323)
Avaya J100 Series IP Deskphones	6.8.3 (H.323)
Avaya J100 Series IP Deskphones	4.0.3 (SIP)
Avaya G450 Media Gateway	41.9.0
Avaya Aura® Experience Portal	7.2.3
Avaya Aura® Media Server	8.0.2
Avaya Session Border Controller for Enterprise	8.0.1.0-10-17555
PCI Pal's Agent Assist	2020.228.55

5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure PCI Pal successfully with Communication Manager.

All configurations in Communication Manager were performed via SAT terminal.

5.1. Verify Avaya Aura® Communication Manager License

Enter the **display system-parameters customer-options** command. Navigate to **Page 2** and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. If there is insufficient capacity of SIP Trunks or a required feature is not enabled, contact an Avaya representative to make the appropriate changes.

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	1
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	0
Maximum Video Capable IP Softphones:	2400	0
Maximum Administered SIP Trunks:	12000	10
Max Administered Ad-hoc Video Conferencing Ports:	12000	0
Max Number of DS1 Boards with Echo Cancellation:	688	0

5.2. Configure IP Node Names

All calls from and to Communication Manager are signalled over a SIP trunk to Session Manager. The signalling interface on Session Manager is provided by the SM100 security module. Use the **change node-names ip** command to add the **Name** and **IP Address** for the SIP security module of Session Manager. **sm81** and **10.64.110.212** were used in this example.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
aes81	10.64.110.215	
ams81	10.64.110.214	
cms19	10.64.110.225	
default	0.0.0.0	
procr	10.64.110.213	
procr6	::	
sm81	10.64.110.212	

5.3. Configure IP Codec Set

Use the **change ip-codec-set n** command to specify **G.711MU** and **G.729** codecs under **Audio Codec** where **n** is the codec set used in the configuration. Configure the **Media Encryption** and **Encrypted SRTCP** as shown below.

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

                                IP MEDIA PARAMETERS

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711MU      n           2          20
2: G.729      n           2          20
3:
4:
5:
6:
7:

Media Encryption                                Encrypted SRTCP: enforce-unenc-srtcp
1: 1-srtp-aescm128-hmac80
2: 2-srtp-aescm128-hmac32
3: none
4:
5:
```

5.4. Configure IP network Region

Use the **change ip-network-region n** command where **n** is the number of the network region used. Set the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** fields to **yes**. For **Codec Set**, enter the codec set configured in **Section 5.3**. Set the **Authoritative Domain** to **avaya.com**. Retain the default values for the remaining fields.

```
change ip-network-region 1                               Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location:      Authoritative Domain: avaya.com
Name:          Stub Network Region: n
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
Codec Set: 1          Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048      IP Audio Hairpinning? y
UDP Port Max: 3329
```

5.5. Configure SIP Trunk with Avaya Aura® Session Manager

To administer a SIP Trunk on Communication Manager, two intermediate steps are required, i.e., creation of a signaling group and trunk group.

5.5.1. Add Signaling Group

Use the **add signaling-group n** command, where **n** is an available signaling group number, and fill in the indicated fields. Default values can be used for the remaining fields:

- **Group Type:** **sip**
- **Transport Method:** **tls**
- **Near-end Node Name:** **procr**
- **Far-end Node Name:** Session Manager node name from **Section 5.2**
- **Near-end Listen Port:** **5061**
- **Far-end Listen Port:** **5061**
- **Far-end Network Region:** IP Network Region from **Section 5.4**
- **Far-end Domain:** **avaya.com**
- **DTMF over IP:** **rtp-payload** (RFC2833)
- **Direct IP-IP Audio Connections** **y**
- **IP Audio Hairpinning** **y**
- **Initial IP-IP Direct Media** **y**

```
add signaling-group 1                                     Page 1 of 2
                                                         SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
Q-SIP? n
IP 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: sml
Near-end Listen Port: 5061             Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Secondary Node Name:

Far-end Domain: avaya.com

Incoming Dialog Loopbacks: eliminate Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload              RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3     Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y                 IP Audio Hairpinning? y
Initial IP-IP Direct Media? y
```

5.5.2. Add SIP Trunk Group

Add the corresponding trunk group controlled by the above signaling group via the **add trunk-group n** command, where **n** is an available trunk group number and fill in the indicated fields.

- **Group Type:** **sip**
- **Group Name:** A descriptive name (e.g., **SM Trunk**)
- **TAC:** An available trunk access code (e.g., **101**)
- **Service Type:** **tie**
- **Signaling Group:** Number of the signaling group added in **Section 5.5.1** (i.e., **1**)
- **Number of Members:** The number of SIP trunks to be allocated to calls routed to **Session Manager** (must be within the limits of the total trunks available from licensed verified in **Section 5.1**)

add trunk-group 1		Page 1 of 5	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: SM Trunk	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 1	
		Number of Members: 10	

Navigate to **Page 3** and change **Numbering Format** to **private**. Use default values for all other fields.

add trunk-group 1		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: private			
		UI Treatment: shared	
		Maximum Size of UI Contents: 128	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
		Hold/Unhold Notifications? y	
Modify Tandem Calling Number: no			

5.6. Configure Route Patterns

Configure a route pattern to correspond to the newly added SIP trunk group. Use **change route pattern n** command, where **n** is an available route pattern. When changing the route pattern, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Grp No:** The trunk group number from **Section 5.5.2**
- **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

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

5.7. Configure Private Numbering

Use the **change private-numbering 0** command to assign number presented by Communication Manager for calls leaving for Session Manager. Add an entry for the extensions configured in the dialplan. Enter the following values for the specified fields, and retain default values for the remaining fields.

- **Ext Len:** Number of digits of the Extension i.e., **5**
- **Ext. Code:** Leading digits of the Extension number, i.e., **7**
- **Trk Group:** Leave it blank (meaning any trunk)
- **Private Prefix:** Enter a value a desired value or leave blank
- **Total Len** Total number of digits i.e., **11**

Note that the value entered in **Private Prefix** will replace the agent's extensions value for outbound calls.

change private-numbering 0										Page 1 of 2	
NUMBERING - PRIVATE FORMAT											
Ext	Ext			Trk			Private			Total	
Len	Code			Grp(s)			Prefix			Len	
5	5									5	Total Administered: 2
5	7					12015551212				11	Maximum Entries: 540

5.8. Configure ARS Analysis

This section shows a sample Auto Route Selection (ARS) entry used for routing calls with dialed digits beginning with **1555**. Use the **change ars analysis 1555** command to add an entry and specify routing of the calls to Session Manager. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Dialed String:** Dialed prefix digits to match on, in this case **1555**
- **Total Min:** Minimum number of digits, in this case **11**
- **Total Max:** Maximum number of digits, in this case **11**
- **Route Pattern:** The route pattern number from **Section 5.6**, i.e., **1**
- **Call Type:** **hnpa**

Note that additional entries may be added for different number destinations.

change ars analysis 1555						Page 1 of 2
ARS DIGIT ANALYSIS TABLE						
Location: all						Percent Full: 0
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd
1555	11	11	1	hnpa		n

5.9. Configure Feature Access Code

Use the **change feature access code** command to define a feature access code for **Auto Route Selection (ARS)**. In the test, **9** was used.

change feature-access-codes		Page 1 of 11
FEATURE ACCESS CODE (FAC)		
Abbreviated Dialing List1 Access Code:		
Abbreviated Dialing List2 Access Code:		
Abbreviated Dialing List3 Access Code:		
Abbreviated Dial - Prgm Group List Access Code:		
Announcement Access Code:		
Answer Back Access Code:		
Attendant Access Code:		
Auto Alternate Routing (AAR) Access Code: 8		
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:

6. Configure Avaya Aura® Session Manager

All configuration for Session Manager is performed via System Manager web interface. Open a web browser session to System Manager URL. A SIP trunk and routing needs to be configured for Communication Manager and Avaya SBCE.

6.1. Configure SIP Entities

Add two new SIP entities, one for Communication Manager and another one for Avaya SBCE

6.1.1. SIP Entity for Communication Manager

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for PCI Pal.

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 procr address of Communication Manager.
- **Type:** “CM”
- **Location:** Select a preconfigured Location.
- **Time Zone:** Select the applicable time zone.

SIP Entity Details Commit Cancel [Help ?](#)

General

* **Name:**

* **FQDN or IP Address:**

Type:

Notes:

Adaptation:

Location:

Time Zone:

* **SIP Timer B/F (in seconds):**

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, in this case “sm81”.
- **Protocol:** “TLS”
- **Port:** “5061”
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** “5061”
- **Connection Policy:** “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"/>	* sm81_cm81_5061_TLS	sm81	TLS ▼	* 5061	cm81	* 5061	trusted ▼

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items
Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit Cancel

6.1.2. SIP Entity for Avaya SBCE

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Avaya 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 internal SIP IP address of Avaya SBCE.
- **Type:** “SIP Trunk”
- **Notes:** Any desired notes.
- **Location:** Select the applicable location.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the 'SIP Entity Details' screen. The left sidebar has 'Routing' selected, with 'SIP Entities' highlighted. The main area is titled 'SIP Entity Details' and has a 'General' tab. The fields are as follows:

Field	Value
Name	sbce81
FQDN or IP Address	10.64.110.222
Type	SIP Trunk
Notes	
Adaptation	sbce81
Location	DevConnect
Time Zone	America/Denver
SIP Timer B/F (in seconds)	4

Buttons: Commit, Cancel, Help ?

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, in this case “sm81”.
- **Protocol:** “TLS”
- **Port:** “5061”
- **SIP Entity 2:** The Avaya SBCE entity name from this section.
- **Port:** “5061”
- **Connection Policy:** “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	Deny New Service
<input type="checkbox"/>	* sm81_sbce81_5061_TLS	sm81	TLS	* 5061	sbce81	* 5061	trusted	<input type="checkbox"/>

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit Cancel

6.2. Configure Routing Policies

Add a new routing policy for routing calls to Communication Manager and Avaya SBCE.

6.2.1. Routing Policy for Communication Manager

Select **Routing** → **Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy to Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.1.1**.

Routing Policy Details

[Help ?](#)

CommitCancel

General

* Name:cm81

Disabled:☐

* Retries:0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
cm81	10.64.110.213	CM	

6.2.2. Routing Policy for Avaya SBCE

Select **Routing** → **Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy to Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Avaya SBCE entity name from **Section 6.1.2**.

Routing Policy DetailsCommitCancelHelp ?

General

* Name:

sbce81

Disabled: ☐

* Retries:

0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
sbce81	10.64.110.222	SIP Trunk	

6.3. Configure Dial Patterns

Dial patterns needs to be configured for Session Manager to know where to route the calls.

6.3.1. Dial Pattern for Communication Manager

Select **Routing → Dial Patterns** from the left pane, and add a new Dial Pattern by select **Add** (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add**. Select a preconfigured **Originating Location Name** and select the **Routing Policies** created in previous **Section 6.2.1** (not shown). The configuration below shows calls to **1444xxxxxxx** were routed to Communication Manager.

Dial Pattern Details

[Help ?](#)

CommitCancel

General

* Pattern:1444

* Min:11

* Max:11

Emergency Call:☐

SIP Domain:-ALL-

Notes:

Originating Locations and Routing Policies

AddRemove

1 Item

Filter: Enable

<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-		cm81	0	<input type="checkbox"/>	cm81	

Select : All, None

6.3.2. Dial Pattern for Avaya SBCE

Select **Routing** → **Dial Patterns** from the left pane, and add a new Dial Pattern by select **Add** (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add**. Select a preconfigured **Originating Location Name** and select the **Routing Policies** created in previous **Section 6.2.2** (not shown). The configuration below shows calls to **1555xxxxxxx** were routed to Avaya SBCE.

Dial Pattern DetailsCommitCancelHelp ?

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<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"/>	DevConnect		sbce81	2	<input type="checkbox"/>	sbce81	

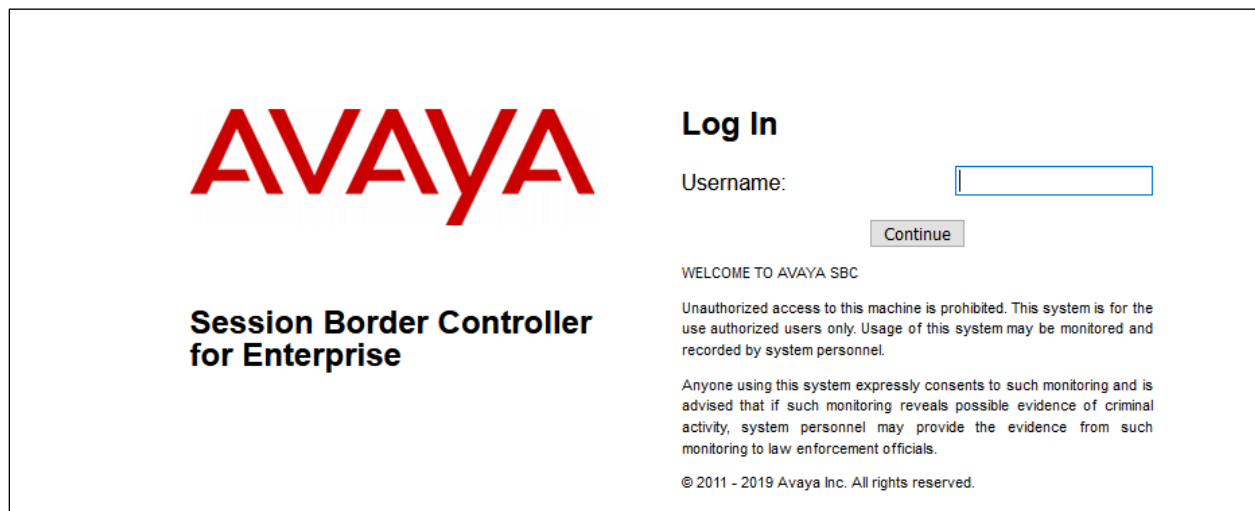
Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

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

Note: The Staging and Production PCI Pal IP Addresses and ports for the relevant region will be shared with the Avaya customer during the integration phase. Capacity numbers used for the inbound and outbound routes will also be defined at the same time.

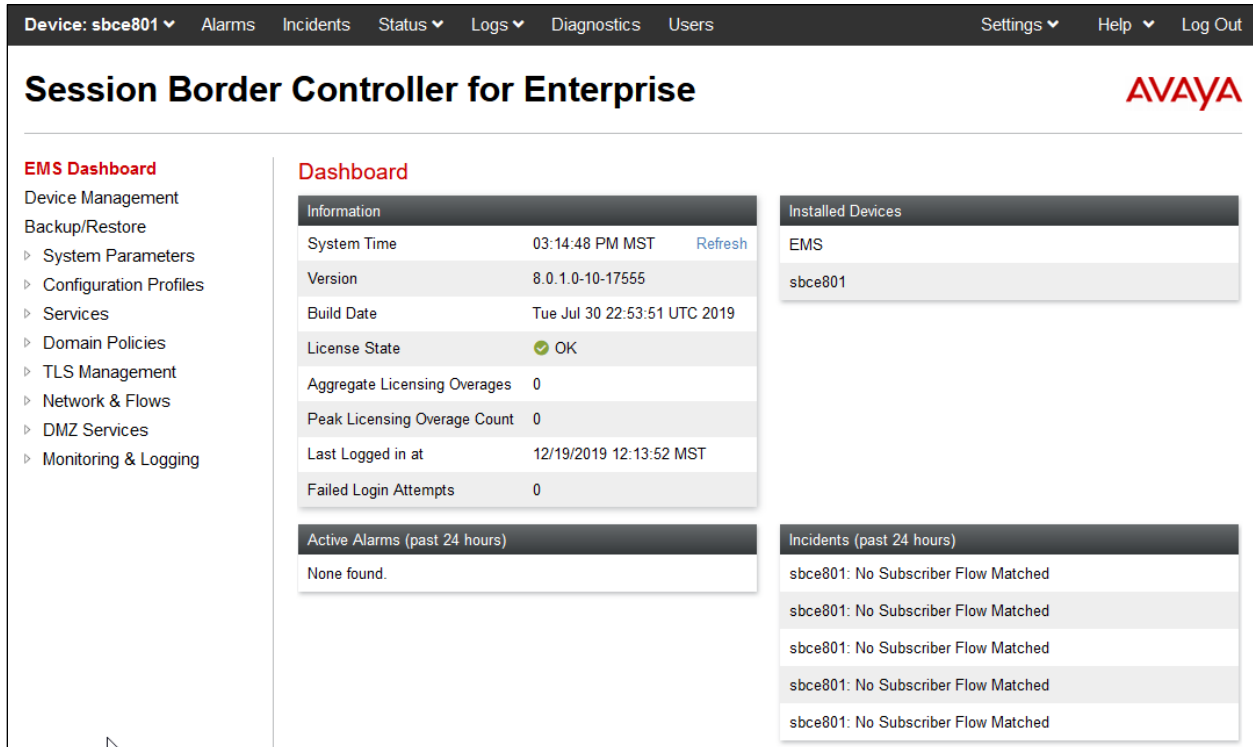
Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using the appropriate username and password.



The image shows the login interface for the Avaya Session Border Controller for Enterprise. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. 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, a "WELCOME TO AVAYA SBC" message is shown, followed by a disclaimer: "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." Below this is 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 - 2019 Avaya Inc. All rights reserved." is displayed.

7.1. Access Avaya Session Border Controller for Enterprise

Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



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

Session Border Controller for Enterprise

EMS Dashboard

- Device Management
- Backup/Restore
 - System Parameters
 - Configuration Profiles
- Services
 - Domain Policies
 - TLS Management
 - Network & Flows
 - DMZ Services
- Monitoring & Logging

Dashboard

Information	
System Time	03:14:48 PM MST Refresh
Version	8.0.1.0-10-17555
Build Date	Tue Jul 30 22:53:51 UTC 2019
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	12/19/2019 12:13:52 MST
Failed Login Attempts	0

Active Alarms (past 24 hours)

None found.

Installed Devices

EMS

sbce801

Incidents (past 24 hours)

sbce801: No Subscriber Flow Matched

sbce801: No Subscriber Flow Matched

sbce801: No Subscriber Flow Matched

sbce801: No Subscriber Flow Matched

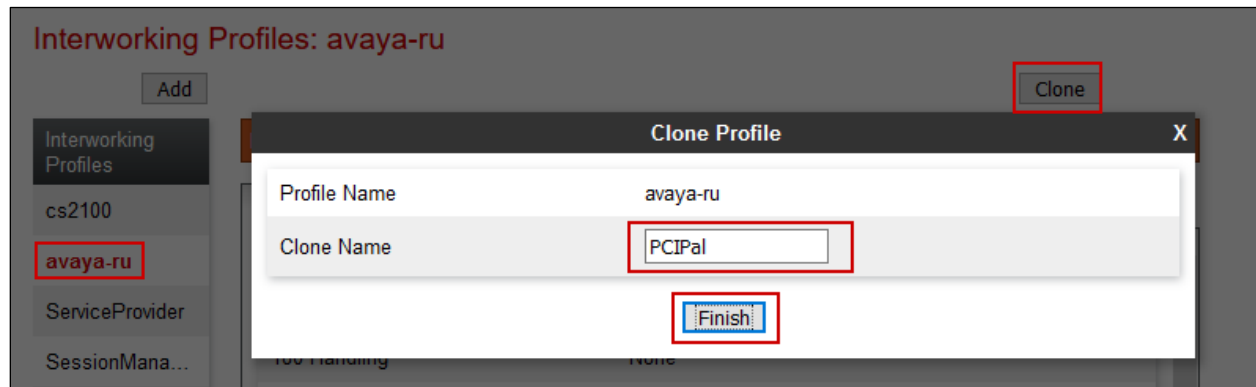
sbce801: No Subscriber Flow Matched

7.2. Define Server Interworking

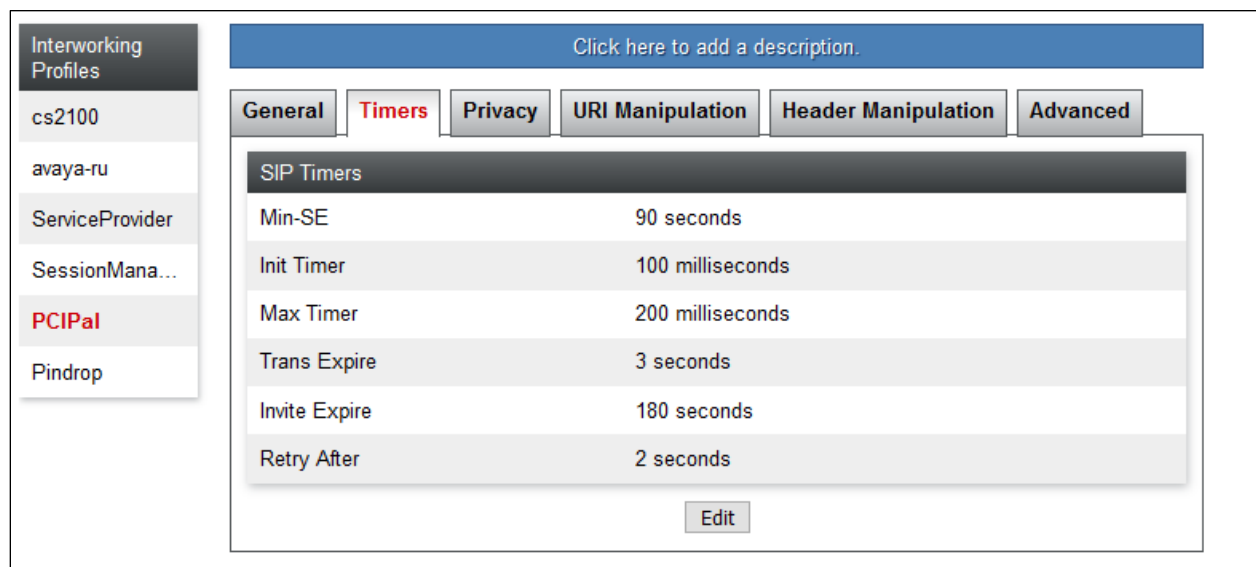
An interworking profile is needed for supported SIP functionality for a SIP server. During Compliance Testing, a pre-configured profile was used for Session Manager and VoIP Service Provider, but the screen captures for those are shown in this section. Add Interworking profile for VoIP Service Provider, PCI Pal and Session Manager.

7.2.1. Server Interworking profile for PCI Pal

To add a Server Interworking profile, select **Configuration Profiles → Server Interworking** from the left-hand menu. Screen captures for the profile are shown below. Select the **avaya-ru** profile and select **Clone**. Type in a **Clone Name** for PCI Pal profile. Select **Finish** once done.



Once added, select the PCI Pal profile and select the **Timers** tab. During the Compliance testing, the following timers were configured.



Select the **Advanced** tab and configure the fields as the screen capture below. Note that the **DTMF Support** is set to **SIP Info**.

Interworking Profiles: PCIPal

Add Rename Clone Delete

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	No
Extensions	None
Diversion Manipulation	No
Has Remote SBC	No
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No

DTMF

DTMF Support	SIP Info
--------------	----------

Edit

7.2.2. Server Interworking profile for Session Manager

Session Manager profile was cloned from the same **avaya-ru** profile. No changes were made to the cloned profile. The **Advanced** tab screen capture is shown below:

Interworking Profiles: avaya-ru

Add Clone

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

General Timers Privacy URI Manipulation Header 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

DTMF

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

Edit

7.2.3. Server Interworking profile for VoIP Service Provider

VoIP Service Provider profile was also cloned from the same **avaya-ru** profile. Select the **Advanced** tab and configure as shown in the screen capture below:

Interworking Profiles: ServiceProvider

Add

RenameCloneDelete

Interworking Profiles

cs2100

avaya-ru

ServiceProvi...

SessionMana...

PCIPal

Pindrop

Click here to add a description.

GeneralTimersPrivacyURI ManipulationHeader ManipulationAdvanced

Record Routes	Both Sides
Include End Point IP for Context Lookup	No
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

DTMF

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

Edit

7.3. Define SIP Servers

A SIP server definition is required for each server connected to the Avaya SBCE. Add SIP Servers for VoIP Service Provider, PCI Pal and Session Manager.

7.3.1. SIP Server for PCI Pal

To define a server, navigate to **Services → SIP Servers** in the main menu on the left-hand side. Click on **Add** and enter an appropriate name in the pop-up screen (not shown) and select **Next**. Note that for security purposes, Public IP Addresses have been changed to Private.

- **Server Type:** **Trunk Server**
- **TLS Client Profile:** Select a TLS profile for authentication
- **IP Address / FQDN** SIP IP Address of PCI Pal node
- **Port:** SIP Port of PCI Pal node
- **Transport:** **TLS**

The additional entry was added for failover purposes.

Note that TLS profiles were preconfigured and are not shown in this document. All TLS certificates used during the test were signed by System Manager.

Edit SIP Server Profile - General

Server Type:

SIP Domain:

DNS Query Type:

TLS Client Profile:

IP Address / FQDN	Port	Transport	
<input type="text" value="192.168.1.2"/>	<input type="text" value="3063"/>	<input type="text" value="TLS"/>	<input type="button" value="Delete"/>
<input type="text" value="192.168.1.3"/>	<input type="text" value="3063"/>	<input type="text" value="TLS"/>	<input type="button" value="Delete"/>

Select **Next** until **Add SIP Server Profile – Advanced** page. Select the **Interworking Profile** for PCI Pal from **Section 7.2.1** and select **Finish**.

52.48.192.179 3062 TCP

Add SIP Server Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile **PCIPal**

Signaling Manipulation Script **None**

Securable ☐

Enable FGDN ☐

TCP Failover Port 5060

TLS Failover Port 5061

Tolerant ☐

URI Group **None**

Back **Finish**

7.3.2. SIP Server for Session Manager

Session Manager SIP Server was preconfigured. The screen capture below shows the **General** tab:

SIP Servers: SessionManager

Add **Rename** **Clone** **Delete**

Server Profiles

- PCIPal
- ServiceProvider
- Pindrop
- SessionManager**
- PP

General **Authentication** **Heartbeat** **Registration** **Ping** **Advanced**

Server Type Call Server

SIP Domain avaya.com

TLS Client Profile ClientTLS

DNS Query Type NONE/A

IP Address / FQDN	Port	Transport
10.64.110.212	5061	TLS

Edit

All the other tabs were of default value except for the **Advanced** tab. Note the Server Interworking profile was configured from **Section 7.2.2**.

SIP Servers: SessionManager

Buttons: Add, Rename, Clone, Delete

Server Profiles: PCIPal, ServiceProvider, Pindrop, **SessionManager**, PP

Tabs: General, Authentication, Heartbeat, Registration, Ping, **Advanced**

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

Edit

7.3.3. SIP Server for VoIP Service Provider

VoIP Service Provider SIP Server was preconfigured. The screen capture below shows the **General** tab:

SIP Servers: ServiceProvider

Buttons: Add, Rename, Clone, Delete

Server Profiles: PCIPal, **ServiceProvider**, Pindrop, SessionManager, PP

Tabs: **General**, Authentication, Heartbeat, Registration, Ping, Advanced

Server Type	Trunk Server	
SIP Domain	avaya.com	
DNS Query Type	NONE/A	

IP Address / FQDN	Port	Transport
10.64.110.65	5060	UDP

Edit

All the other tabs were of default value except for the **Advanced** tab. Note the Server Interworking profile was configured from **Section 7.2.3**.

SIP Servers: ServiceProvider

Add

RenameCloneDelete

Server Profiles

PCIPal

ServiceProvider

Pindrop

SessionManager

PP

GeneralAuthenticationHeartbeatRegistrationPingAdvanced

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

Edit

7.4. Define Routing

Routing information is required for routing calls to all configured SIP Servers. The IP addresses and ports defined here will be used as the destination addresses for signalling.

7.4.1. Routing Profile for PCI Pal

To define Routing profile for PCI Pal, navigate to **Configuration Profiles → Routing** in the main menu on the left-hand side. Click on **Add** and enter an appropriate name in the dialogue box (not shown). Add two entries for PCI Pal **SIP Server Profile**. Note the **Priority / Weight** value; lower the value, higher the priority. If calls to higher priority SIP Server fail, calls are routed to the next highest priority SIP Server. Select **Finish** once done.

The screenshot shows the 'Routing Profile' configuration window. It includes fields for URI Group, Time of Day, Load Balancing, Transport, LDAP Server Profile, LDAP Base DN (Search), Matched Attribute Priority, Next Hop Priority, Ignore Route Header, ENUM, and ENUM Suffix. Below these fields is a table with columns: Priority / Weight, LDAP Search Attribute, LDAP Search Regex Pattern, LDAP Search Regex Result, SIP Server Profile, Next Hop Address, and Transport. Two entries are listed in the table.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				PCIPal	192.168.1.2:3063 (TLS)	None
2				PCIPal	192.168.1.3:3063 (TLS)	None

7.4.2. Routing Profile for Session Manager

Routing Profile for Session Manager was preconfigured. Screen capture below shows the configured Routing Profile for Session Manager.

The screenshot shows the 'Routing Profiles: SessionManager' window. It includes a list of routing profiles on the left: default, ServiceProvider, SessionManager (selected), Pindrop, and PCIPal. The main area shows the 'Routing Profile' configuration for SessionManager. It includes a table with columns: Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport. One entry is listed in the table.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	10.64.110.212:5061	TLS

7.4.3. Routing Profile for VoIP Service Provider

Routing Profile for VoIP Service Provider was preconfigured. Screen capture below shows the configured Routing Profile for VoIP Service Provider.

Routing Profiles: ServiceProvider

Add

RenameCloneDelete

Routing Profiles

default

ServiceProvider

SessionManager

Pindrop

PCIPal

Click here to add a description.

Routing Profile

Update PriorityAdd

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	*	default	Priority	10.64.110.65:5060	UDP	EditDelete

7.5. Define URI Groups

URI Groups are used in conjunction with Session Flows to route calls based of the URIs for incoming calls. During the Compliance testing, calls to 1444NPANXXX received from 1513NPANXXXXX were to Avaya Aura® environment. Calls to 1555NPANXXX received from 12015551212 were routed to VoIP Service Provider.

URI Groups: fromSP

Add

RenameDelete

URI Groups

Emergency

fromSM

fromSP

Click here to add a description.

URI Group

Add

URI Listing

*@10.64.110.223	EditDelete
1444XXXXXX@.*	EditDelete
1513XXXXXX@.*	EditDelete

URI Groups: fromSM

Add

RenameDelete

URI Groups

Emergency

fromSM

fromSP

Click here to add a description.

URI Group

Add

URI Listing

12015551212@.*	EditDelete
1555XXXXXX@.*	EditDelete

7.6. Define Media Rules

Media rules are used to define RTP media packet parameters, such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies. Note that during Compliance Testing calls to all the SIP Servers used the same Media Rules.

To define a new Media Rule, navigate to **Domain Policies → Media Rules**. Clone **default-low-med** rule and provide a **Clone Name** for the new Media Rule (not shown). Once added, select the newly added **Media Rule** and Edit the **Encryption** tab, configure as shown in the screen capture below:

Media Rules: RTP-SRTP

Buttons: Add, Rename, Clone, Delete

Media Rules List:

- Media Rules
- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- Pindrop
- RTP-SRTP**

Click here to add a description.

Tabs: Encryption, Codec Prioritization, Advanced, QoS

Audio Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_32 SRTP_AES_CM_128_HMAC_SHA1_80 RTP
SRTP Context Reset on SSRC Change	<input type="checkbox"/>
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

Video Encryption

Preferred Formats	RTP
Interworking	<input checked="" type="checkbox"/>

Miscellaneous

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

Edit

Select the **Codec Prioritization** tab and **Edit**. Configure as shown in the screen capture below:

Media Rules: RTP-SRTP

Media Rules

- default-low-med
- default-low-med-enc
- default-high
- default-high-enc
- avaya-low-med-enc
- Pindrop
- RTP-SRTP**

Click here to add a description.

Encryption **Codec Prioritization** Advanced QoS

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], G729 (18) [T]

Video Codec

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

Edit

7.7. Define Endpoint Policy Groups

Endpoint policy groups comprise a group of endpoint policy sets, all of which are specifically configured using a number of relevant parameters. Recently added Media Rule is associated with an Endpoint Policy Group.

To add an Endpoint Policy Group, navigate to **Domain Policies → Endpoint Policy Groups**. Clone **default-low** profile and provide a **Clone Name** for the new Endpoint Policy Group (not shown). Once added, **Edit** the newly cloned group and set the **Media Rule** to the Media Rule added in **Section 7.5**. Select **Finish** once done.

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

Finish

7.8. Signaling Interface

Signaling Interface needs to be defined for each SIP Server and SIP Remote Workers for SIP signaling. 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.

- SP: Signaling interface used by Service Provider to send and receive calls.
- Internal: Signaling interface used by Session Manager to send and receive calls.
- RW-Internal: Signaling interface used for SIP Remote Workers registrations and to send and receive calls towards Session Manager.
- RW-External: Signaling interface used for SIP Remote Workers registrations and to send and receive calls towards the internet.
- External: Signaling interface used by PCI Pal to send and receive calls.

Note that, though TLS was used for PCI Pal SIP connectivity during the Compliance testing, TCP and UDP are also supported by PCI Pal.

Signaling Interface						
Signaling Interface						
Add						
Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
SP	10.64.110.223 SP (A2, VLAN 0)	5060	5060	---	None	Edit Delete
Internal	10.64.110.222 Internal (A1, VLAN 0)	5060	5060	5061	ServerTLS	Edit Delete
RW-Internal	10.64.110.220 Internal (A1, VLAN 0)	5060	5060	5061	ServerTLS	Edit Delete
RW-External	██████████ External (B1, VLAN 0)	5060	5060	5061	ServerTLS	Edit Delete
External	██████████ External (B1, VLAN 0)	5060	5060	5061	ServerTLS	Edit Delete

7.9. Media Interface

Media Interface needs to be defined for each SIP Server and SIP Remote Workers to send and receive media (RTP or SRTP). Navigate to **Networks & Flows → Media Interface** to define a new Media Interface. During the Compliance Testing the following interfaces were defined. For security reasons, Public IP Addresses have been blacked out.

- Internal: Interface used by Session Manager to send and receive media.
- SP: Interface used by Service Provider to send and receive media.
- RW-Internal: Interface used for SIP Remote Workers to send and receive media towards Session Manager.
- RW-External: Interface used for SIP Remote Workers to send and receive media towards the internet.
- External: Interface used by PCI Pal to send and receive media.

Note that, though SRTP was used media transmission for PCI Pal, RTP is also supported by PCI Pal.

Media Interface			
Media Interface		Add	
Name	Media IP Network	Port Range	
Internal	10.64.110.222 Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
SP	10.64.110.223 SP (A2, VLAN 0)	35000 - 40000	Edit Delete
RW-Internal	10.64.110.220 Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
RW-External	██████████ External (B1, VLAN 0)	35000 - 40000	Edit Delete
External	██████████ External (B1, VLAN 0)	35000 - 40000	Edit Delete

7.10. Server Flows

Server Flows combine the previously defined profiles for PCI Pal/Session Manager and VoIP Service Provider. These End Point Server Flows allow calls to be routed to and from PCI Pal/Session Manager/VoIP Service Provider. Navigate to **Network & Flows → End Point Flows → Server Flows**. The screen capture below displays the configured Server Flows. The screen capture below displays the Server flows used during the Compliance test.

End Point Flows

Subscriber Flows

Server Flows

Add

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

Hover over a row to see its description.

SIP Server: PCIPal

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	PCIPal Outbound	fromSM	Internal	External	RTP-SRTP	ServiceProvider	View Clone Edit Delete
2	PCIPal Inbound	fromSP	SP	External	RTP-SRTP	SessionManager	View Clone Edit Delete

SIP Server: ServiceProvider

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SP Outbound	fromSM	External	SP	RTP-SRTP	default	View Clone Edit Delete
2	SP Inbound	fromSP	SP	SP	RTP-SRTP	PCIPal	View Clone Edit Delete

SIP Server: SessionManager

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SM Outbound	fromSM	Internal	Internal	RTP-SRTP	PCIPal	View Clone Edit Delete
2	SM Inbound	fromSP	External	Internal	RTP-SRTP	default	View Clone Edit Delete
3	RWFlow	*	RW-External	RW-Internal	RTP-SRTP	default	View Clone Edit Delete

8. Configure PCI Pal's Agent Assist

All configuration related to PCI Pal is performed by PCI Pal engineers and, thus, is not documented.

9. Verification Steps

To verify SIP connectivity to Avaya SBCE, via System Manager, navigate to **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**. Under the **All Monitored SIP Entities**, select the Avaya SBCE Entity.

All Monitored SIP Entities	
Run Monitor	
16 Items Filter: Enable	
<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	sbce81
<input type="checkbox"/>	cm81
<input type="checkbox"/>	unigy
<input type="checkbox"/>	cmm81
<input type="checkbox"/>	brz81
<input type="checkbox"/>	brzws1
<input type="checkbox"/>	brzws2
<input type="checkbox"/>	brzws3
<input type="checkbox"/>	mx62
<input type="checkbox"/>	sentry
<input type="checkbox"/>	mpp722
<input type="checkbox"/>	intranext
<input type="checkbox"/>	trio
<input type="checkbox"/>	ipo11
<input type="checkbox"/>	ps81-brz

Select : All, None Page 1 of 2

Verify **Conn. Status** is **UP**.

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: sbce81

Summary View

1 Item

Filter: Enable

	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	sm81	IPv4	10.64.110.222	5061	TLS	FALSE	UP	403 Forbidden	UP

Select : None

Additionally, calls to and from Avaya Aura® environment can be placed with VoIP Service Provider in conjunction with running **tracesbc** command on Avaya SBCE to verify correct calls routing.

10. Conclusion

PCI Pal's Agent Assist was able to successfully interoperate with Avaya Aura® environment and Avaya Session Border Controller for Enterprise with the exception of the observation in **Section 2.2**.

11. Additional References

Documentation related to Avaya can be obtained from <https://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 5, November 2019.
- [2] *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 3, October 2019.
- [3] *Administering Avaya Aura® Session Manager*, Release 8.1.1, Issue 2, October 2019.
- [4] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0.x, Issue 4, August 2019.

©2020 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.