



Application Notes for Smart Action Intelligent Virtual Assistant with Avaya Session Border Controller for Enterprise, Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Smart Action Intelligent Virtual Assistant to interoperate with Avaya Session Border Controller for Enterprise, Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks. Intelligent Virtual Assistant is a cloud-based intelligent IVR. In the compliance testing, Intelligent Virtual Assistant used SIP trunks to Avaya Session Border Controller for Enterprise to support inbound and outbound IVR applications.

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 describe the configuration steps required for Smart Action Intelligent Virtual Assistant (Intelligent Virtual Assistant) to interoperate with Avaya Session Border Controller for Enterprise (Avaya SBCE), Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Session Manager (Session Manager) using SIP trunks via UDP. Intelligent Virtual Assistant is a cloud-based IVR. In the compliance testing, Intelligent Virtual Assistant used SIP trunks to Avaya Session Border Controller for Enterprise to IVR functionality. Calls to and from Avaya Aura® Environment to Intelligent Virtual Assistant IVR were routed via Avaya SBCE.

The Intelligent Virtual Assistant used during the testing was deployed on a cloud.

2. General Test Approach and Test Results

The feature test cases were performed manually. The Intelligent Virtual IVR was tested by manually placing calls from users on the PSTN and on Communication Manager to the Intelligent Virtual Assistant IVR. The associated Intelligent Virtual IVR played greeting announcements and collected DTMF input from the caller to decide on the feature to provide, such as transfer to internal or external destinations. Intelligent Virtual Assistant outbound calling to PSTN and Communication Manager were also tested.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to Intelligent Virtual Assistant.

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.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included G.711MU, codec negotiation, media shuffling, session refresh, hold/reconnect, inbound DTMF, invalid number, busy destination, and outgoing call screening.

The serviceability testing focused on verifying the ability of Intelligent Virtual Assistant to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Intelligent Virtual Assistant.

2.2. Test Results

All test cases were executed and passed.

2.3. Support

Technical support on Intelligent Virtual Assistant can be obtained through the following:

- **Phone:** 310-776-9200 option 2
- **Email:** support@smartaction.ai
- **Web:** <https://www.smartaction.ai/support/>

3. Reference Configuration

As shown in **Figure 1**, SIP trunks were used between Intelligent Virtual Assistant and Session Manager (via Avaya SBCE), and the applicable domain name used was “avaya.com”. The configuration of Session Manager is performed via the web interface of System Manager. The detailed administration of basic connectivity between Communication Manager, System Manager, Session Manager and Avaya SBCE is not the focus of these Application Notes and will not be described.

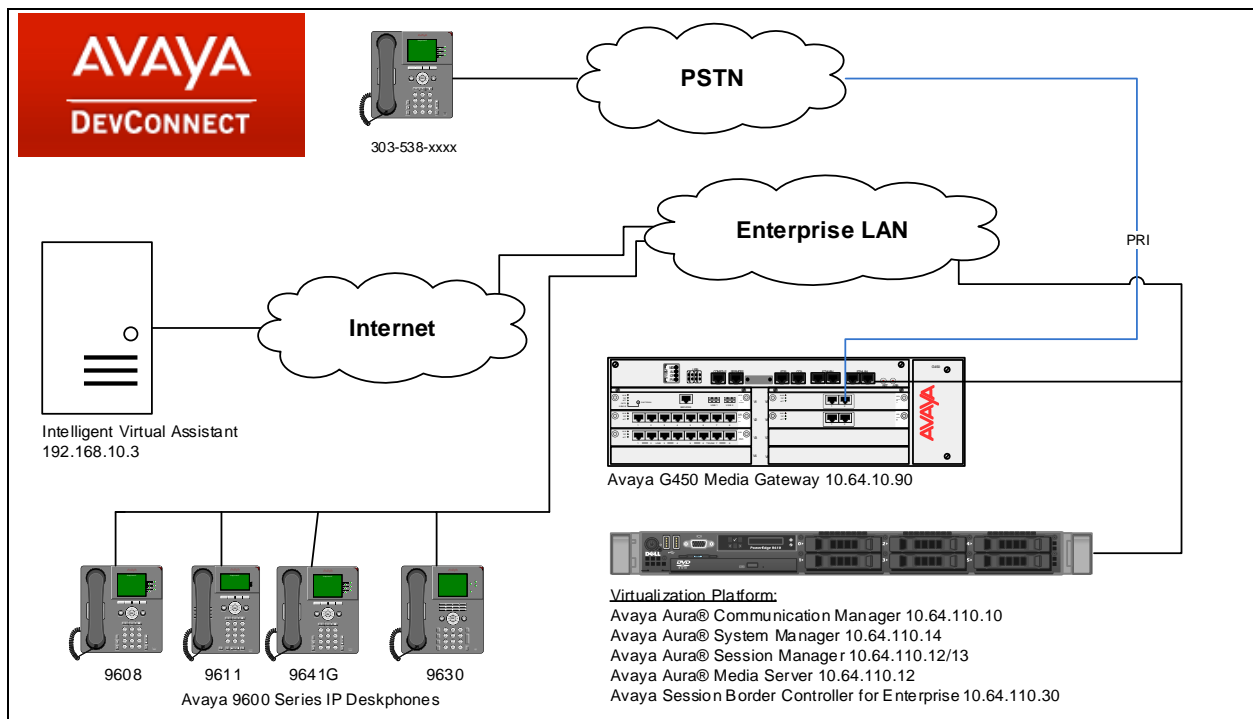


Figure 1: Intelligent Virtual Assistant with Avaya Aura® Environment

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 with Avaya G450 Media Gateway	7.1.2 37.19.0
Avaya Aura® Session Manager	7.1.2
Avaya Aura® System Manager	7.1.2
Avaya Session Border Controller for Enterprise	7.2.2.0
Avaya 96x0 IP Deskphone (H.323)	3.2.8
Avaya 96x1 IP Deskphone (H.323)	6.6.6
Avaya 96x0 IP Deskphone (SIP)	2.6.17
Avaya 96x1G IP Deskphone (SIP)	7.1.1.0
Smart Action Intelligent Virtual Assistant	10.3

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer system parameters features
- Administer SIP trunk group
- Administer SIP signaling group
- Administer SIP trunk group members
- Administer IP network region
- Administer IP codec set
- Administer route pattern
- Administer private numbering
- Administer uniform dial plan
- Administer AAR analysis
- Administer PSTN trunk group
- Administer tandem calling party number

In the compliance testing, a separate set of codec set, network region, trunk group, and signaling group were used for integration with Intelligent Virtual Assistant.

5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. 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.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales 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:	18000	3
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	128	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	36000	0
Maximum Video Capable IP Softphones:	18000	3
Maximum Administered SIP Trunks:	12000	10
Maximum Administered Ad-hoc Video Conferencing Ports:	12000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0

5.2. Administer System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers.

For ease of interoperability testing, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system wide basis. Note that this feature poses significant security risk, and must be used with caution. For alternatives, the trunk-to-trunk feature can be implemented on the Class Of Restriction or Class Of Service levels. Refer to [1] for more details.

```
change system-parameters features                               Page 1 of 19
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y

      Music (or Silence) on Transferred Trunk Calls? all
      DID/Tie/ISDN/SIP Intercept Treatment: attendant
      Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
      Automatic Circuit Assurance (ACA) Enabled? n

      Abbreviated Dial Programming by Assigned Lists? n
      Auto Abbreviated/Delayed Transition Interval (rings): 2
      Protocol for Caller ID Analog Terminals: Bellcore
      Display Calling Number for Room to Room Caller ID Calls? N
```


5.3. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “1”. This trunk group is used between Communication Manager and Session Manager. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “tie”

add trunk-group 1		Page 1 of 22	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: asm	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:		
	Number of Members:		

Navigate to **Page 3**, and enter “private” for **Numbering Format**.

add trunk-group 1		Page 3 of 22	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Suppress # Outpulsing? n	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		
Send UCID? y			

5.4. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “1”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Transport Method:** “tls”
- **Near-end Node Name:** An existing C-LAN node name or “procr” in this case.
- **Far-end Node Name:** The existing node name for Session Manager.
- **Near-end Listen Port:** An available port for integration with Communication Manager.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** An existing network region to use with Intelligent Virtual Assistant.
- **Far-end Domain:** The applicable domain name for the network.
The empty Far-end Domain indicates “any” domain.

```
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? y
Peer Detection Enabled? y Peer Server: SM
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: asm
Near-end Listen Port: 5061             Far-end Listen Port: 5061
Far-end Network Region: 1

Far-end Domain:
Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 65 IP Audio Hairpinning? n
Enable Layer 3 Test? y              Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6
```

5.5. Administer SIP Trunk Group Members

Use the “change trunk-group n” command, where “n” is the trunk group number from **Section 5.3**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Signaling Group:** The signaling group number from **Section 5.4**.
- **Number of Members:** The desired number of members, in this case “10”.

change trunk-group 1		Page 1 of 22	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: asm	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	

5.6. Administer IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section 5.4**.

For **Authoritative Domain**, enter the applicable domain for the network. Enter a descriptive **Name**, if desired. Enter “yes” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with Intelligent Virtual Assistant.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
    Region: 1          NR Group: 1
    Location: 1        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? 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
```

5.7. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from **Section 5.6**. Update the audio codec types in the **Audio Codec** fields as necessary. Note that Intelligent Virtual Assistant only supports the G.711 codec variant. The codec shown below was used in the compliance testing.

change ip-codec-set 1

Page1 of 2

IP CODEC SET

Codec Set: 1

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

5.8. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used to reach Intelligent Virtual Assistant via Session Manager, in this case “1”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name:** A descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.3**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.
- **Numbering Format:** “lev0-pvt”

change route-pattern 1												Page 1 of 3				
Pattern Number: 1												Pattern Name:				
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					
							Dgts			Intw						
1: 1		0										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							lev0-pvt	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 Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to Intelligent Virtual Assistant. Add an entry for the trunk group defined in **Section 5.3**. In the example shown below, all calls originating from a 5-digit extension beginning with 5 and routed to any trunk group will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

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: 1	
					Maximum Entries: 540	

5.10. Administer AAR Analysis

Use the “change aar analysis 48600” command, and add an entry to specify how to route calls to 48600. In the example shown below, calls with digits 48600 will be routed as an aar call type using route pattern “1” from **Section 0**.

change aar analysis 511							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all						Percent Full: 0		
Dialed		Total		Route	Call	Node	ANI	
String		Min	Max	Pattern	Type	Num	Reqd	
48600		5	5	1	aar		n	

6. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer SIP entities
- Administer routing policies
- Administer dial patterns

6.1. Launch System Manager

Access the System Manager web interface by using the URL <https://ip-address> in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.

6.2. Administer SIP Entities

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

6.2.1. SIP Entity for Avaya Session Border Controller for Enterprise

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

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 Avaya SBCE.
- **Type:** “SIP Trunk”
- **Notes:** Any desired notes.
- **Location:** Select the location name.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The top navigation bar includes 'Home', 'Licenses', and 'Routing'. The left sidebar lists various configuration options, with 'Routing' expanded and 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains a 'General' tab. The form fields are as follows:

Field	Value
Name	asbce
FQDN or IP Address	10.64.110.32
Type	SIP Trunk
Notes	
Adaptation	
Location	DevConnect
Time Zone	America/Denver
SIP Timer B/F (in seconds)	4
Minimum TLS Version	Use Global Setting
Credential name	
Securable	<input type="checkbox"/>

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.

- **SIP Entity 1:** The Session Manager entity name, in this case “asm”.
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The Avaya SBCE entity name from this section.
- **Port:** “5060”

AVAYA
Aura® System Manager 7.1

Last Logged on at August 16, 2018 12:48 PM
Go... Log off admin

Home Licenses Routing

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
<input type="checkbox"/>	*asm_asbce_5060_UDP	*Q asm	UDP	* 5060	*Q asbce	* 5060

Select : All, None

6.2.2. 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 Communication Manager. Note that this SIP entity is used for integration with Intelligent Virtual Assistant.

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 an existing CLAN or the processor interface.
- **Type:** “CM”
- **Notes:** Any desired notes.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 7.1 interface. The left navigation pane has 'Routing' selected, and 'SIP Entities' is highlighted. The main area shows the 'SIP Entity Details' form. The form has the following fields and values:

- Name:** acm
- FQDN or IP Address:** 10.64.110.10
- Type:** CM
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** DevConnect
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** none

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.

- **SIP Entity 1:** The Session Manager entity name, in this case “asm”.
- **Protocol:** The signaling group transport method from **Section 5.4**.
- **Port:** The signaling group far-end listen port number from **Section 5.4**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group near-end listen port number from **Section 5.4**.

Avaya Aura System Manager 7.1

Home / Elements / Routing / Entity Links

Entity Links Commit Cancel Help ?

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override
<input type="checkbox"/>	*asm_acm_5061_TLS	*asm	TLS	*5061	*acm	*5061	<input type="checkbox"/>

Select : All, None

6.3. Administer Routing Policies

Add two new routing policies, one for Avaya SBCE and another one for Communication Manager.

6.3.1. Routing Policy for Avaya Session Border Controller for Enterprise

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

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, 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 6.2.1**. The screen below shows the result of the selection.

AVAYA
Aura® System Manager 7.1

Last Logged on at August 16, 2018 12:48 PM
Go... Log off admin

Home Licenses Routing

Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular
Expressions
Defaults

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: asbce

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
asbce	10.64.110.32	SIP Trunk	

6.3.2. 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 for Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**, 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 6.2.2**. The screen below shows the result of the selection.

AVAYA
Aura® System Manager 7.1

Last Logged on at February 1, 2018 10:55 AM
Go... Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: acm

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
acm	10.64.110.10	CM	

6.4. Administer Dial Patterns

Add a new dial pattern for Intelligent Virtual Assistant, and update existing dial patterns for Communication Manager.

6.4.1. Dial Pattern for Intelligent Virtual Assistant

Select **Routing** → **Dial Patterns** from the left pane, and click **New** in the subsequent screen (not shown) to add a new dial pattern to reach Intelligent Virtual Assistant via Avaya SBCE. The **Dial Pattern Details** screen is displayed. In the **General** sub-section, enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern:** A dial pattern to match, in this case “48600”.
- **Min:** The minimum number of digits to match.
- **Max:** The maximum number of digits to match.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and select the routing policy for reaching Intelligent Virtual Assistant.

The screenshot displays the Avaya Aura System Manager 7.1 interface. The left navigation pane shows the 'Routing' menu expanded, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. The 'General' sub-section contains the following fields:

- Pattern:** 48600
- Min:** 5
- Max:** 5
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:**
- SIP Domain:** -ALL-
- Notes:**

The 'Originating Locations and Routing Policies' sub-section features an 'Add' button and a table with one item:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> DevConnect		asbce	0	<input type="checkbox"/>	asbce	

At the bottom, there is a 'Select' dropdown menu with options 'All' and 'None'.

In the compliance testing, the policy allowed for call origination from “DevConnect”, and the Avaya SBCE routing policy from **Section 6.3.1** was selected as shown below.

Avaya Aura® System Manager 7.1

Last Logged on at August 16, 2018 12:48 PM

Go... Log off admin

Home Licenses * Routing *

Home / Elements / Routing / Dial Patterns

Originating Location Select Cancel

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

1 Item Filter: Enable

<input checked="" type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	DevConnect	

Select : All, None

Routing Policies

13 Items Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	aac	<input type="checkbox"/>	aac	
<input type="checkbox"/>	aaep	<input type="checkbox"/>	aaep	
<input type="checkbox"/>	aps	<input type="checkbox"/>	aps	
<input checked="" type="checkbox"/>	asbce	<input type="checkbox"/>	asbce	
<input type="checkbox"/>	cm71	<input type="checkbox"/>	acm71	

6.4.2. Dial Pattern for Communication Manager

Similar steps were followed as previous section to add dial patterns for Communication Manager.

AVAYA
Aura® System Manager 7.1

Last Logged on at August 16, 2018 12:48 PM
Go... Log off admin

Home Licenses * Routing *

Home / Elements / Routing / Dial Patterns

Dial Pattern Details Commit Cancel

General

* Pattern: 5

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL- ▼

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		cm71	0	<input type="checkbox"/>	acm71	

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signaling to provide an interface to Intelligent Virtual Assistant.



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 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 - 2016 Avaya Inc. All rights reserved." is displayed.

7.1. Access Avaya Session Border Controller for Enterprise

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.

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.

Session Border Controller for Enterprise **AVAYA**

Dashboard

- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - PPM Services
 - Domain Policies
 - TLS Management
 - Device Specific Settings

Information

System Time	04:37:21 PM MDT	Refresh
Version	7.2.2.0-11-15522	
Build Date	Tue May 29 11:31:10 UTC 2018	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	07/25/2018 11:17:21 MDT	
Failed Login Attempts	0	

Installed Devices

EMS
SBCE

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

None found. [Add](#)

Notes

No notes found.

7.2. Define Network Management

Network information is required on the Avaya SBCE to allocate IP addresses and subnet masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one physical interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** in the main menu on the left hand side and click on **Add**. The following interfaces were added for Session Manager and Public Internet. For security reasons the IP Address of external interface has been masked.

The screenshot shows the Avaya SBCE web interface. The top navigation bar includes Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header is "Session Border Controller for Enterprise" with the AVAYA logo. The left sidebar contains a menu with Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. Under Device Specific Settings, "Network Management" is highlighted. The main content area is titled "Network Management: SBCE" and has tabs for Devices, Interfaces, and Networks. The Networks tab is active, showing a table of network configurations. An "Add" button is in the top right of the table.

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	Edit	Delete
Internal	10.64.110.1	255.255.255.0	A1	10.64.110.32	Edit	Delete
Public	[Masked]	255.255.255.128	B1	[Masked]	Edit	Delete

Select the **Interface Configuration** tab and click on the **Status** of the physical interface to toggle it. A status of **Disabled** will be changed to **Enabled**.

The screenshot shows the Avaya SBCE web interface, specifically the "Network Management: SBCE" section. The "Interfaces" tab is active, showing a table of interface configurations. An "Add VLAN" button is in the top right of the table.

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled

Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

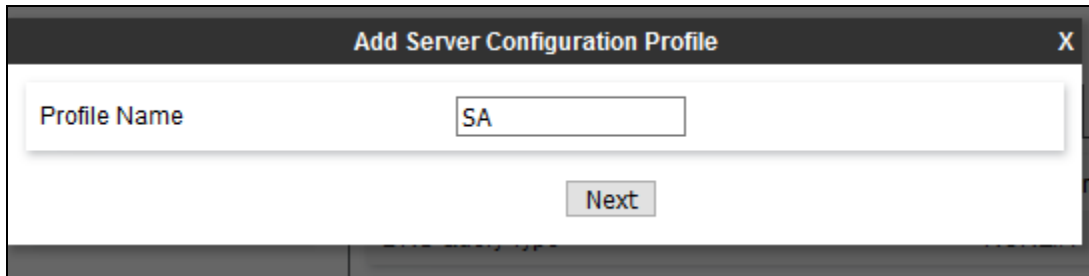
- Click on **System Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box will appear (not shown) that will indicate when the application has restarted.

7.3. Define Servers

A server definition is required for each server connected to the Avaya SBCE. In this case, the Intelligent Virtual Assistant as a Trunk Server. The server here is added with a name of **SA**.

To define the server for Intelligent Virtual Assistant, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up menu.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. The dialog contains a label "Profile Name" and a text input field with the value "SA". Below the input field is a "Next" button.

Click on **Next** and enter details in the dialogue box.

- In the **Server Type** drop down menu, select **Trunk Server**.
- Click on **Add** to enter an IP address
- In the **IP Addresses / FQDN** box, type the IP Address of Intelligent Virtual Assistant.
- In the **Port** box, enter the port to be used.
- In the **Transport** drop down menu, select **UDP**.
- Click on **Next**.

Note that the IP Address shown below is not the actual public IP Address that was used. It has been changed with a private IP Address for security reasons.

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport	
192.168.10.3	5060	UDP	Delete

Finish

Click on **Next** and configure as follows.

agnostics Users

Edit Server Configuration Profile - Heartbeat X

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS ▾
Frequency	600 seconds
From URI	sbce@10.64.110.1
To URI	sbc@19.168.10.3

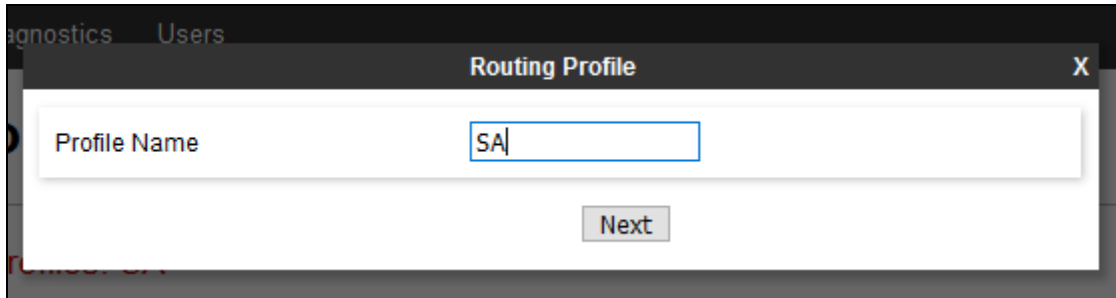
Finish

Select **Next** and then **Finish** (not shown).

7.4. Define Routing

Routing information is required for routing calls to Intelligent Virtual Assistant. The IP addresses and ports defined here will be used as the destination addresses for signaling.

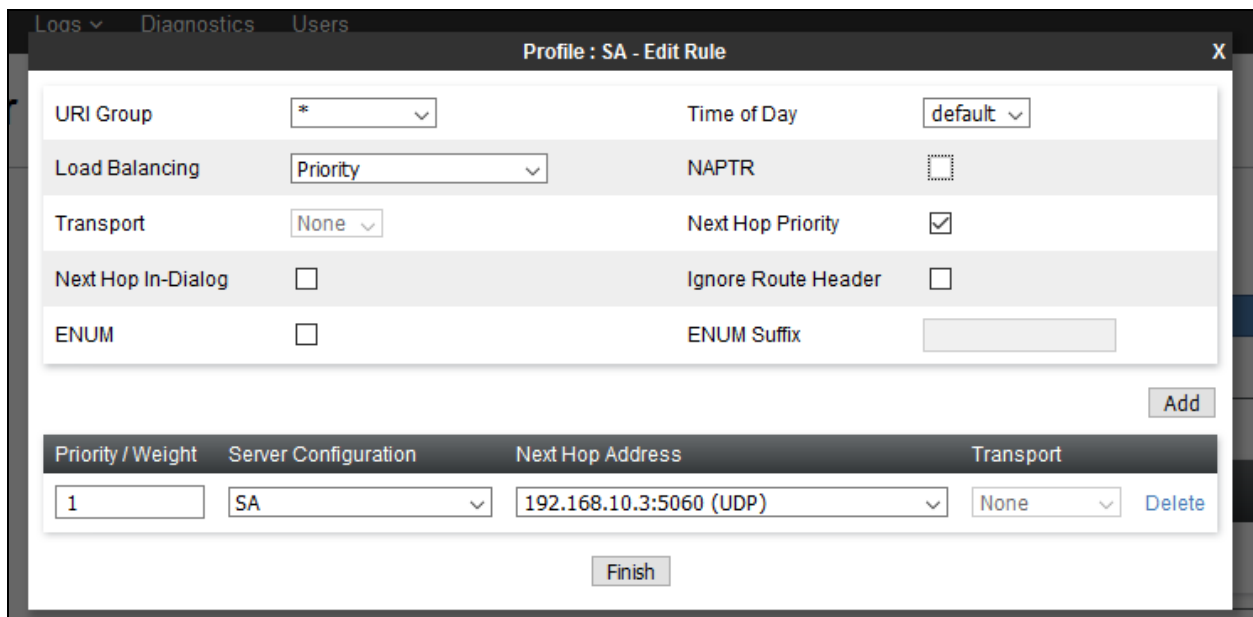
To define routing to the Intelligent Virtual Assistant SIP Trunk, navigate to **Global Profiles** → **Routing** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the dialogue box.



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "SA". Below the input field is a button labeled "Next".

Click on **Next** and enter details for the Routing Profile:

- Click on **Add** to specify the IP address for the Intelligent Virtual Assistant SIP trunk.
- Assign a priority in the **Priority / Weight** field, during testing a value of **1** was used.
- Select the Server Configuration defined in **Section 7.3** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.



The screenshot shows a dialog box titled "Profile : SA - Edit Rule" with a close button (X) in the top right corner. The dialog contains several configuration fields and a table.

Configuration fields:

- URI Group: *
- Load Balancing: Priority
- Transport: None
- Next Hop In-Dialog: ☐
- ENUM: ☐
- Time of Day: default
- NAPTR: ☐
- Next Hop Priority: ☒
- Ignore Route Header: ☐
- ENUM Suffix:

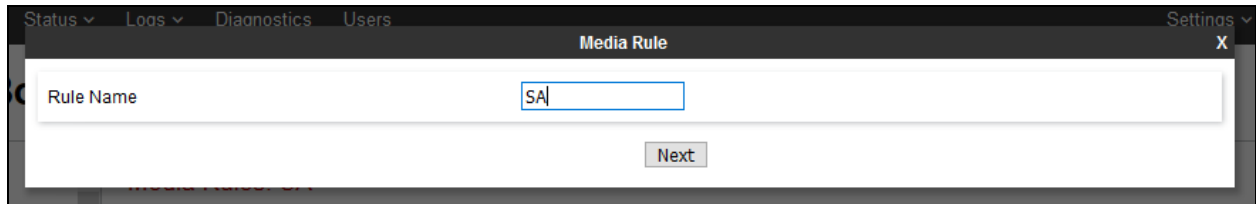
Buttons: Add, Finish

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	SA	192.168.10.3:5060 (UDP)	None

Buttons: Delete

7.5. Define Media Rules

Audio formats need to be specified for Intelligent Virtual Assistant. To create a Media Rule for Intelligent Virtual Assistant, navigate to **Domain Policies** → **Media Rules**. Click on **Add** and enter an appropriate name in the pop-up menu and select **Next**.



The screenshot shows a web application window titled "Media Rule". The window has a dark header bar with navigation links: "Status", "Logs", "Diagnostics", "Users", and "Settings". The main content area is white and contains a text input field labeled "Rule Name" with the text "SAI" entered. Below the input field is a "Next" button.

On the **Media Rule** pop-up, under **Audio Encryption**, select a **Preferred Format #1** and select **RTP**, select **Next**.

Media Encryption X

Audio Encryption

Preferred Format #1 RTP

Preferred Format #2 NONE

Preferred Format #3 NONE

Encrypted RTCP ☒

MKI ☐

Lifetime
Leave blank to match any value. 2^

Interworking ☒

Video Encryption

Preferred Format #1 RTP

Preferred Format #2 NONE

Preferred Format #3 NONE

Encrypted RTCP ☐

MKI ☐

Lifetime
Leave blank to match any value. 2^

Interworking ☒

Miscellaneous

Capability Negotiation ☐

Finish

7.6. Server Flows

Server Flows combine the previously defined profiles for Session Manager and Intelligent Virtual Assistant. These End Point Server Flows allow calls to be routed to and from Intelligent Virtual Assistant. Navigate to **Device Specific Setting → End Point Flows → Server Flows**. The screen capture below displays the configured Server Flows. Configure the fields as shown in the screen capture.

End Point Flows: SBCE

Devices
SBCE

Subscriber Flows

Server Flows

Add

Hover over a row to see its description.

Server Configuration: SA

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SA	*	InternalSig	ExternalSig	default-low	SM	View Clone Edit Delete

Server Configuration: SM

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SM	*	ExternalSig	InternalSig	default-low	SA	View Clone Edit Delete

< >

Screen captures for configuration of each Server Flow are as shown below:

The screenshot shows a configuration window titled "Edit Flow: SA" with a close button (X) in the top right corner. The window contains a list of configuration parameters, each with a label and a corresponding input field (text box or dropdown menu). The parameters are as follows:

Parameter	Value
Flow Name	SA
Server Configuration	SA
URI Group	*
Transport	UDP
Remote Subnet	*
Received Interface	InternalSig
Signaling Interface	ExternalSig
Media Interface	ExternalMedia
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	SM
Topology Hiding Profile	SM
Signaling Manipulation Script	None
Remote Branch Office	Any

At the bottom center of the window is a "Finish" button.

8. Configure Smart Action Intelligent Virtual Assistant

Configuration in this section is performed by Smart Action engineers. Configuration in this section is for informational purposes only.

8.1. Configure Adjacency

The first configuration object is to establish an adjacency with Avaya SBCE Public IP Address. It is configured to establish a SIP trunk configuration using port 5060, with the default protocol (which is UDP). The adjacency is named as "Customer: Avaya".

Configuration Objects	Values
Object name	SIP Adjacency "Customer:avaya"
Node	Unknown
Path	Connection to Session Controller "LAX-SBC" / Session Controller "LAX-SBC" / Adjacencies / Adjacencies before SIP Adjacency "S*" / SIP Adjacency "Customer:Avaya"
SNMP Index OID	3.16.67.117.115.116.111.109.101.114.37.51.6 5.97.118.97.121.97 (3.Customer:avaya)
CORBA Internal name	BOOPerimetaConnSE.3/BOOPerimetaSE/BO OPeriAdjacencyContainerSE/BOOPeriAdjace ncySipSE.Customer:avaya
Identifiers	LAX-SBC/Customer:Avaya

8.2. Adjacency Settings

Table below displays the Adjacency Settings configured during this test.

Parameter	Value
Description	Avaya test adjacency for certification testing
Adjacency Type	preset-peering
Account	None
CollectStatistics	detail
DeactivationMode	normal
NetworkHeading	Network
NetworkServiceAddress	GeneralPeering-01
NetworkServiceNetworkID	2
NetworkLocalAddress	Public IP Address of Smart Action
NetworkLocalPort	single-port
NetworkSinglePort	5060

NetworkSignalingPeer	true
NetworkSignalingPeerPort	5060
NetworkTrustSignalingPeer	True
NetworkSignalingPeerGroup	None
NetworkRemoteAddressRangeIP	Public IP Address of Avaya SBCE
NetworkRemoteAddressRangePrefixLength	32
NetworkRemoteAddressRangeTrusted	true
RoutingHeading	Routing
RoutingSimpleRouting	disabled
ConnectionHeading	Connections
ConnectionMandateTransport	allow-any-transport
ConnectionNAT	force-on
ConnectionsListenForTransports	default-for-adjacency-type
ConnectionTLS	disabled
IPRoutingHeading	IP Routing
IPRoutingForceSignalingPeer	all-requests
IPRoutingRedirectMode	Use default
IPRoutingRedirectModeDefault	Pass-through
IPRoutingDynamicRoutingDomainMatch	50.207.80.111
PrivacyAndSecurityHeading	Privacy and Security
PrivacyAndSecurityPrivacy	trusted
PrivacyAndSecurityContactHeaderUsernameHandling	rewrite
PrivacyAndSecurityUseUniquePortPerUsername	false
MediaHeading	Media
MediaMSCFallback	none
MediaMSCLocationID	default
MediaRealm	GeneralPeeringMedia1
SIPHeading	SIP
SIPOutboundFloodPolicing	false
SIPDefaultInteropProfile	BOOPerimetaConnSE.3/BOOPerimetaSE/BOOPeriInteropProfilesContainerSE/BOOPeriInterop
ProfileSE_Peer	// Peer
RegistrationHeading	Registration
RegistrationRequired	false
RegistrationOutgoingTimer	0
RegistrationOutgoingNegotiateLocalExpiry	false
TrunkGroupHeading	Trunk group
TrunkGroupTrunkGroup	passthrough
MessageManipulationHeading	Message Manipulation

MessageManipulationErrorProfile	None
MessageManipulationLuaConfigSet	None
CallFlowHeading	Call Flow
CallFlowREFERToINVITETTransfer	False
IMSHeading	IMS
IMSPChargingVectorHeader	Use default
IMSPChargingVectorHeaderDefaultValue	passthrough
AlarmsHeading	Alarms
AlarmState	Clear
StatusHeading	Status
RequestedStatus	Active
ActualStatus	Active

8.3. Call Policy Settings

The second configuration object establishes a call policy in which is matched for any calls coming in via the Avaya adjacency (as defined above), and send those calls to a routing table named "DID_Maps". Table below displays the Call Policy Settings configured during this test.

Parameter	Value
Object Name	Avaya call policy
Node	Unknown
Path	Connection to Session Controller "LAX-SBC" / Session Controller "LAX-SBC" / Call Policy Sets / Call Policy Set 1 "Routing based on called number" (active) / Routing Table "Initial_Routing_Table" (Source adjacency) / Avaya call policy
SNMP Index OID	3.21.73.110.105.116.105.97.108.95.82.111.117.116.105.110.103.95.84.97.98.108.101 (3.Initial_Routing_Table)
CORBA Internal Name	BOOPerimetaConnSE.3/BOOPerimetaSE/BOOPeriCallPolicySetsContainerSE/BOOPeriCallPolicySetSE.1/BOOPeriRoutingTableSE.Initial_Routing_Table/BOOPeriRoutingEntrySE.4
Identifiers	LAX-SBC1/Initial_Routing_Table/4
MatchAdjacencyHeading	Match adjacency
MatchAdjacencyMatchAdjacency	specify
MatchAdjacencyAdjacencyToMatch	BOOPerimetaConnSE.3/BOOPerimetaSE/BOOPeriAdjacencyContainerSE/BOOPeriAdjacencySipSE.Customer%3Aavaya//Customer:avaya
NumberManipulationHeading	Number Manipulation

NumberManipulationApplyDestinationNumberManipulation	false
NumberManipulationApplySourceNumberManipulation	false
TrunkGroupIDManipulationHeading	Trunk Group ID Manipulation
TrunkGroupIDManipulationDestinationTrunkGroupIDManipulation	none
TrafficGroupHeading	Traffic Group
TrafficGroupApplyTrafficGroup	false
ActionHeading	Action
ActionAction	Next-table
ActionNextTable	BOOPerimetaConnSE.3/BOOPerimetaSE/BOOPeriCallPolicySetsContainerSE/BOOPeriCallPolicySetSE.1/BOOPeriRoutingTableSE.DID_Maps //"DID_Maps" ()
ActionDestinationAdjacency	None
AlarmsHeading	Alarms
AlarmState	Clear
RoutingTableType	source-adjacency

8.4. Routing Policy Settings

The final configuration object sets up a routing policy based on the destination phone number / extension. In the case of the testing, the number we matched on was the extension 48600 (Section 5.9). When that condition occurs, the call is forwarded to one of our QA IVR servers, named SA:PBX8. Table below displays the Routing Policy Settings configured during this test.

Parameter	Value
Object Name	Entry 16
Node	Unknown
Path	Connection to Session Controller "LAX-SBC" / Session Controller "LAX-SBC" / Call Policy Sets / Call Policy Set 1 "Routing based on called number" (active) / Routing Table "DID_Maps" (Destination ID) / Entry 16
SNMP Index OID	3.8.68.73.68.95.77.97.112.115 (3.DID_Maps)
CORBA Internal name	BOOPerimetaConnSE.3/BOOPerimetaSE/BOOPeriCallPolicySetsContainerSE/BOOPeriCallPolicySetSE.1/BOOPeriRoutingTableSE.DID_Maps/BOOPeriRoutingEntrySE.16
Identifiers	LAX-SBC1/DID_Maps

Parameter	Value
MatchIDHeading	Match ID
MatchIDMatchType	digits
MatchIDDigitsToMatch	48600
MatchIDPerformPrefixMatching	false
NumberManipulationHeading	Trunk Group ID Manipulation
TrunkGroupIDManipulationDestinationTrunkGroupIDManipulation	none
TrunkGroupIDManipulationSourceTrunkGroupIDManipulation	none
TrafficGroupHeading	Traffic Group
TrafficGroupApplyTrafficGroup	false
Action Heading	Action
ActionAction	complete
ActionDestinationAdjacency	BOOPerimetaConnSE.3/BOOPerimetaSE/BOOPeriAdjacencyContainerSE/BOOPeriAdjacencySipSE.SA%3APBX8 //SA:PBX8
AlarmsHeading	Alarms
AlarmState	Clear
RoutingTableType	Destination-id

9. Verification Steps

This section provides tests that can be performed to verify proper configuration of Communication Manager, Session Manager, and Intelligent Virtual Assistant.

9.1. Verify Avaya Aura® Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the “status trunk n” command, where “n” is the trunk group number administered in **Section 5.3**. Verify that all trunks are in the “in-service/idle” state as shown below.

```
status trunk 1

                                TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                                Busy

0001/001 T00001    in-service/idle    no
0001/002 T00002    in-service/idle    no
0001/003 T00003    in-service/idle    no
0001/004 T00004    in-service/idle    no
0001/005 T00005    in-service/idle    no
0001/006 T00006    in-service/idle    no
0001/007 T00007    in-service/idle    no
```

Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.4**. Verify that the **Group State** is “in-service”, as shown below.

```
status signaling-group 1

                                STATUS SIGNALING GROUP

      Group ID: 1
      Group Type: sip

      Group State: in-service
```

9.2. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Elements** → **Session Manager** 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 the Avaya SBCE 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”.

AVAYA
Aura® System Manager 7.1

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

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.

All Entity Links to SIP Entity: eOne

Summary View

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
asm	IPv4	192.168.10.134	5060	UDP	FALSE	UP	200 OK	UP

9.3. Verify Avaya Session Border Controller for Enterprise

Log onto Avaya SBCE via a shell console and run **tracesbc** command. Verify the **OPTIONS** from SBC to Session Manager and Intelligent Virtual Assistant are getting responded with 200 OK. This verifies SIP connectivity to and from Avaya SBCE.

192.131.21.73		192.168.10.3
	SBC	
13:29:16.136	←OPTIONS→	SIP: sip:192.131.21.73:5060
13:29:16.136	→200 OK←	SIP: 200 OK (OPTIONS)
13:30:44.264	→OPTIONS←	SIP: sip:10.64.110.12:5060
13:30:44.264	←200 OK→	SIP: 200 OK (OPTIONS)
13:32:43.433	→OPTIONS←	SIP: sip:10.64.110.12:5060
13:32:43.434	←200 OK→	SIP: 200 OK (OPTIONS)

10. Conclusion

These Application Notes describe the configuration steps required for Intelligent Virtual Assistant to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks. All feature and serviceability test cases were completed.

11. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 7.1, August 2017, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Session Manager*, Release 7.1, Issue 7, September 2017, available at <http://support.avaya.com>.
3. *Installing Intelligent Virtual Assistant*, available from <http://www.instruments.com>.
4. *Intelligent Virtual Assistant Application Server*, available from <http://www.instruments.com>.

©2018 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.