



DevConnect Program

Application Notes for Fonolo Voice Call-Backs Version 3.9 using Cloud SIP Connect with Avaya Session Border Controller Release 10.1 and Avaya Aura® 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs version 3.9 using Cloud SIP Connect to interoperate with Avaya Session Border Release 10.1 and Avaya Aura® 10.1. Fonolo Voice Call-Back is a call center solution in the cloud, that interfaces with Avaya Session Border Controller via SIP trunk.

Readers should pay attention to **Section** Error! Reference source not found., in particular the scope of testing as outlined in **Section** Error! Reference source not found. as well as the observations noted in **Section** Error! Reference source not found., 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 Avaya DevConnect Program.

1. Introduction

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs (VCB) using Cloud SIP Connect to interoperate with Avaya Session Border Controller (Avaya SBC) using SIP trunk. Fonolo VCB provides functionality to replace hold-time with a call-back and during this compliance testing was hosted on the cloud by Fonolo.

When a caller encounters a scenario where no agents are available in a call center environment and Communication Manager is part of the environment, the caller is presented with options by the call center to either continue waiting in the queue or receive a call back from the call center. If the caller chose the latter, then the call center directs the caller to Fonolo VCB via Avaya SBC SIP trunks where Fonolo VCB then provides a message to the caller to leave a call back number, so that Fonolo VCB can call back the caller when an agent becomes available. Once Fonolo VCB receives the confirmed call back number from the caller, Fonolo VCB uses SIP trunks through Avaya SBC to call back into the call center and wait in the queue until an agent becomes available. When an agent becomes available, Fonolo VCB informs the agent that there is a call waiting and if the agent would like to get connected to the caller. If the agent accepts to connect to the caller, Fonolo VCB calls the caller and connects the caller with the available agent.

In the application notes, the terms Fonolo VCB and Fonolo Cloud SIP Connect terms are interchangeably used.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on customer calls to the enterprise site, being routed to Fonolo VCB via Avaya SBC SIP trunk to Fonolo Cloud SIP Connect. Calls were placed manually from users on the PSTN to a call center Vector Directory Number (VDN).

The serviceability test cases focused on simulating a network outage and a restart on Avaya SBC. Calls to Fonolo VCB were verified to complete successfully after the network was restored and Avaya SBC came back in service.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with this Application Note, the interface between Avaya SBC and Fonolo VCB using Cloud SIP Connect used TLS encryption for SIP signaling, and SRTP encryption for the media.

TLS/SRTP encryption was also used internally on the enterprise between Avaya SBC and the Avaya Aura® servers and endpoints.

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 Fonolo VCB is hosted in a cloud environment by Fonolo. SIP trunk was used to connect the Fonolo VCB using Cloud SIP Connect with Avaya SBC. The following features and functionality were covered during compliance testing:

- Establish SIP trunk between Avaya SBC and Fonolo VCB using TLS transport.
- Responses from Fonolo VCB to SIP OPTIONS messages sent by Avaya SBC.
- Inbound PSTN calls routed from Communication Manager to Avaya SBC and to the SIP trunk to Fonolo VCB.
- Incoming PSTN to call center can be redirected to the Fonolo VCB via the SIP trunks based on vector. Outgoing calls from the Fonolo VCB to call center agent via Avaya SBC when PSTN callers decide on call back.

- Fonolo VCB places outbound calls to the PSTN caller via Avaya SBC who had selected the call back option and merge the call between the caller and available agents.
- DTMF transmission to ensure that options selected by the caller and agent is accepted correctly by Fonolo VCB.
- Telephony features such as holding and resuming call to Fonolo VCB, session refresh timer, agents transferring calls to another agent during the voice call-back and adding an agent or supervisor into a conference during the voice call-back.
- User-to-User Information (UUI) is sent from the enterprise to the Fonolo VCB and verify UUI data is sent back to agent deskphones via UUI button.
- Proper disconnect when the call is abandoned by PSTN caller.
- Proper disconnect when the call is abandoned by agent.
- SIP signaling encrypted using TLS 1.2.
- Audio encrypted using SRTP.
- Codec G.711U.
- Verify service is restored after a network outage.
- Verify service is restored after an Avaya SBC restart.

2.2. Test Results

All test cases were successfully executed and passed.

2.3. Support

Technical support on Fonolo VCB can be obtained through the following:

- **Phone:** + 1-855-366-2500 (Toll-free)
- **Web:** <https://fonolo.com/contact/>
- **Email:** support@fonolo.com.

3. Reference Configuration

A simulated enterprise site consisting of Communication Manager, Session Manager and System Manager was used during compliance testing. As shown in **Figure 1**, SIP trunks were used to connect Fonolo VCB with Avaya Session Border Controller. Avaya Session Border Controller also had a SIP trunk to connect to SIP Service Provider for external call to PSTN. A skill set queue was configured on Communication Manager with some agents belonging to this queue.

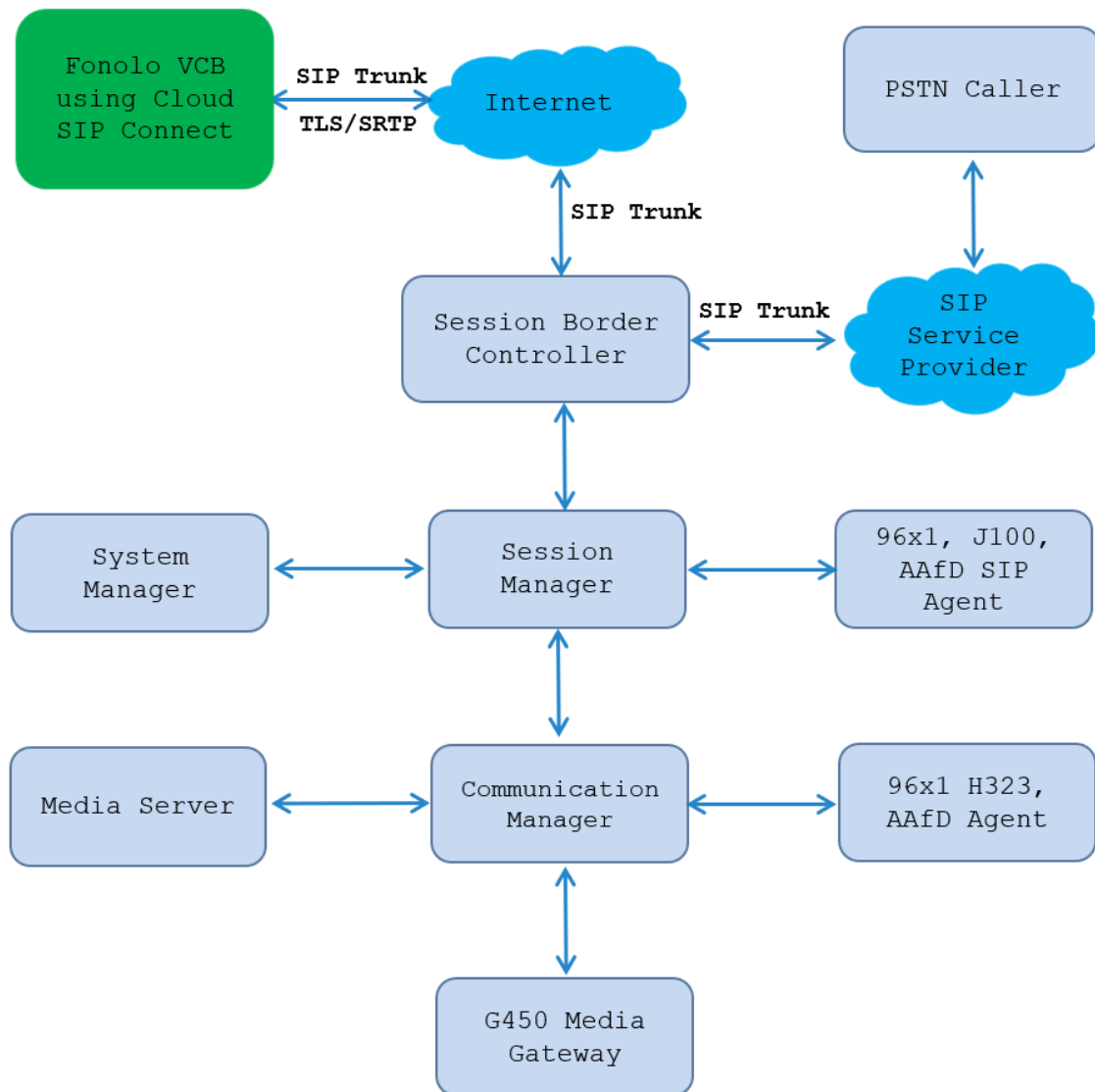


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager	10.1.3.1.0716418 Service Pack 1 Hotfix 1013116418
Avaya Aura® Session Manager	10.1.3.1.1013103
Avaya Aura® Communication Manager	10.1.3.0.1-FP3P1 Update ID 01.0.974.0-27893
Avaya Session Border Controller	10.1.2.0-64-23285 HotFix-1
Avaya Aura® Media Server	Media Server 10.1.0.154 Appliance Version 10.0.0.14
Avaya G450 Media Gateway	42.24
Avaya 96x1 Series IP Deskphone (H.323)	6.8.5.4.10
Avaya J100 SIP Deskphones (J169, J179)	4.1.2.0.11
Avaya 96x1 Series IP Deskphone (SIP)	7.1.15.2.1
Avaya Agent for Desktop Softphone (SIP)	2.0.6.25
Fonolo Voice Call-Backs using Cloud SIP Connect	V.3.9

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

Note – The initial installation, configuration, and licensing of the Avaya servers and media gateways for Communication Manager are assumed to have been previously completed and are not discussed in this document.

5.1. Verify Communication Manager License

Log in to the System Access Terminal to verify that the Communication Manager license has the appropriate 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.

If additional license is required, contact an authorized Avaya Sales or Reseller representative.

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:	12000	10	
Maximum Concurrently Registered IP Stations:	18000	7	
Maximum Administered Remote Office Trunks:	12000	0	
Max Concurrently Registered Remote Office Stations:	18000	0	
Maximum Concurrently Registered IP eCons:	414	0	
Max Concur Reg Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	41000	4	
Maximum Video Capable IP Softphones:	18000	11	
Maximum Administered SIP Trunks:	40000	30	
Max Administered Ad-hoc Video Conferencing Ports:	24000	0	
Max Number of DS1 Boards with Echo Cancellation:	999	0	

5.2. Administer IP Node Names

Use the “change node-names ip” command (not shown) and add an entry for Session Manager. In this case, **SM10** and **10.33.1.42** are entered as **Name** and **IP Address**. Note the **procr** and **10.33.1.43** entry, which is the node **Name** and **IP address** for the processor board. These values will be used later to configure the SIP signaling to Session Manager in **Section 5.5**.

```
change node-names ip!
```

IP NODE NAMES	
Name	IP Address
AMS1	10.33.1.30
default	0.0.0.0
SM10	10.33.1.42
lsp	10.33.1.7
procr	10.33.1.43

5.3. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number. Update the audio codec types in the **Audio Codec** fields as necessary. The codec shown below was used in the compliance testing.

```
change ip-codec-set 3
```

Page 1 of 2

IP MEDIA PARAMETERS				
Codec Set: 1				
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)	
1: G.711MU	n	2	20	
2: G.729	n	2	20	
3:				
Media Encryption			Encrypted SRTCP: enforce-unenc-srtcp	
1: 1-srtp-aescm128-hmac80				
2: none				

5.4. 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** Error! Reference source not found.5.

For **Authoritative Domain**, enter the applicable domain for the network. Enter a descriptive **Name**. 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 Fonolo VCB.

change ip-network-region 3

Page 1 of 20

IP NETWORK REGION

Region: 3

NR Group: 1

Location: 1

Authoritative Domain: avayalab.com

Name: Loc-1

Stub Network Region: n

MEDIA PARAMETERS

Codec Set: 3

Intra-region IP-IP Direct Audio: yes

Inter-region IP-IP Direct Audio: yes

UDP Port Min: 2048

UDP Port Max: 3329

IP Audio Hairpinning? n

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

H.323 IP ENDPOINTS

Audio RESOURCE RESERVATION PARAMETERS

H.323 Link Bounce Recovery? y

RSVP Enabled? n

Idle Traffic Interval (sec): 20

Keep-Alive Interval (sec): 5

Keep-Alive Count: 5

5.5. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “3”. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Group Type:**
 - **Transport Method:**
 - **Near-end Node Name:**
 - **Far-end Node Name:**
 - **Near-end Listen Port:**
 - **Far-end Listen Port:**
 - **Far-end Network Region:**

Set it as“sip”,

Set is as “tls”.

Enter the “procr”interface of Communication Manager.

Enter the node name for Session Manager.

Enter the TLS port for the SIP trunk to Session Manager.

The same port number as in **Near-end Listen Port**.

Enter the existing network region to use with Session Manager.

- **Far-end Domain:** The applicable SIP domain name for the network.
- **Direct IP-IP Audio Connections?:** Set is as “y”.

change signaling-group 3		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? n	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: interopASM	
Near-end Listen Port: 5063	Far-end Listen Port: 5063	
	Far-end Network Region: 3	
Far-end Domain: avayalab.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? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

5.6. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk 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:** Set is as “sip”.
- **Group Name:** Enter a descriptive name.
- **TAC:** Enter an available trunk access code.
- **Service Type:** Set is as “public-ntwrk”.
- **Signaling Group:** Enter the signaling group that has been created in **Section 5.5**.

change trunk-group 3		Page 1 of 5
TRUNK GROUP		
Group Number: 3	Group Type: sip	CDR Reports: r
Group Name: To-ServiceProvider	COR: 1	TN: 1 TAC: #03
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: public-ntwrk	Auth Code? n	
	Member Assignment Method: auto	
	Signaling Group: 3	
	Number of Members: 10	

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

change trunk-group 3	Page 3 of 4
TRUNK FEATURES	
ACA Assignment? n	Measured: both
	Maintenance Tests? y
Suppress # Outpulsing? n Numbering Format: private	
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y	

Navigate to **Page 4** and enter “y” for the **Convert 180 to 183 for Early Media?** field as shown below.

change trunk-group 3	Page 4 of 4
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? y	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? y	
Support Request History? y	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? y	
Always Use re-INVITE for Display Updates? y	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	
Request URI Contents: may-have-extra-digits	

5.7. Administer Dial Plan

This section provides a sample dial plan used for routing calls with dialed digits 78xxx to Fonolo VCB. Use the “change dialplan analysis 0” command and add an entry to specify the use of digits pattern **78**, as shown below.

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page 1 of 12
			Location: all						Percent Full: 5
	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0		3	fac	33	4	ext	#	3	dac
1		4	ext	34	4	ext			
1		11	udp	45	4	aar			
78		5	udp	46	4	aar			

5.8. Administer Uniform Dial Plan

This section provides a sample AAR routing used for routing calls with dialed digits 78xxx to Fonolo VCB. Note that other routing methods may be used. Use the “change uniform-dialplan 0” command and add an entry to specify the use of AAR for routing of digits **78xxx**, as shown below.

change uniform-dialplan 0			UNIFORM DIAL PLAN TABLE						Page 1 of 2
									Percent Full: 0
	Matching Pattern	Len	Del	Insert Digits	Net	Conv	Node Num		
1		11	0		ars	n			
35		4	0		aar	n			
78		5	0		aar	n			

5.9. Administer Route Pattern

Use the “change route-pattern n” command, where “n” is an existing route pattern number to be used to reach Fonolo VCB, in this case “3”. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** The SIP trunk group number from **Section 5.6**.
- **FRL:** A level that allows access to this trunk, with 0 being least restrictive.

change route-pattern 3										Page 1 of 4	
Pattern Number: 1										Pattern Name: Public SIPTrunk	
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: 3		0								n	user
2:								n	user		
3:								n	user		
4:								n	user		
5:								n	user		
6:								n	user		

5.10. Administer AAR Analysis

Use the “change aar analysis 78” command and add an entry to specify how to route calls to 78xxx. In the example shown below, calls with digits 78xxx will be routed as an AAR call using route pattern “1” from **Section 09**

change aar analysis 78							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all							Percent Full: 1	
	Dialed	Total		Route	Call	Node	ANI	
	String	Min	Max	Pattern	Type	Num	Reqd	
78		5	5	3	aar		n	

5.11. Administer Agent Login ID

To add an **Agent LoginID**, use the command “**add agent-loginID <agent ID>**” for each agent. In the compliance test, three agent login IDs 1000, 1001 and 1002 were created.

add agent-loginID 1000

Page1 of 2

AGENT LOGINID

Login ID: 1000AAS? n

Name: Agent 1000AUDIX? n

TN: 1

COR: 1

Coverage Path:LWC Reception: spe

Security Code: 1234LWC Log External Calls? n

Attribute:AUDIX Name for Messaging:

LoginID for ISDN/SIP Display? n

Password:

Password (enter again):

Auto Answer:

station

MIA Across Skills: system

AUX Agent Considered Idle (MIA)? systemACW Agent Considered Idle: system

Aux Work Reason Code Type: system

Logout Reason Code Type: system

Maximum time agent in ACW before logout (sec): system

Forced Agent Logout Time: :

WARNING: Agent must log in again before changes take effect

On **Page 2** of the **Agent LoginID** form, set the skill number (**SN**) to hunt group 1, which is the hunt group (skill) that the agents will log into.

add agent-loginID 1000

Page2 of 2

AGENT LOGINID

Direct Agent Skill:Service Objective? n

Call Handling Preference: skill-levelLocal Call Preference? n

SNRLSL

SNRLSL

1: 1116:

2:17:

3:18:

4:19:

5:20:

6:

7:

8:

9:

10:

11:

12:

13:

14:

15:

5.12. Administer Hunt Group

This section provides the Hunt Group configuration for the call center agents. Agents will log into Hunt Group 1 configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the **Agent LoginIDs** configured in **Section 5.11**.

add hunt-group 1		Page 1 of 4
HUNT GROUP		
Group Number: 1	ACD? y	
Group Name: Skill-1	Queue? y	
Group Extension: 3320	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

5.13. Administer Vector

Use the command “change vector n” while “n” is the vector number from 1-8000. The example of the vector **12** with the basic scripting is shown below. This section provides a sample vector that was used during the compliance testing. When a call is directed to this vector it provides the caller with an option to press “1” for call-back or stay in the queue if all agents are busy. If caller presses “1”, then the call is routed to Fonolo VCB with number “78000”, in “Step 8” a line was added to send UII information to Fonolo VCB for testing purposes.

change vector 12		Page 1 of 6
CALL VECTOR		
Number: 12	Name: To-Fonolo	
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n
Basic? y	EAS? y	G3V4 Enhanced? y
Prompting? y	LAI? y	G3V4 Adv Route? y
Variables? y	3.0 Enhanced? y	CINFO? y
01 wait-time	5	secs hearing 1104
02 goto step	11	if staffed-agents in skill 1
03 goto step	7	if expected-wait for skill 1
04 queue-to	skill 1	pri m
05		
06		
07 collect	1	digits after announcement 1107
08 set	A	= digits CATR 0123456789
09 route-to	number 78000	cov n if digit
10 goto step	4	if unconditionally
11 disconnect	after announcement	none
12 stop		

5.14. Administer VDN

Use the “add vdn n” command to add a VDN number. In the **Destination** field, enter **Vector Number 12** as configured in **Section 5.13** above and keep other fields at their default values.

add vdn 3340	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 3340	
Name*: Contact Center 1	
Destination: Vector Number	12
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: both	Report Adjunct Calls as ACD*? n
Acceptable Service Level (sec): 20	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	

6. Configure Avaya Aura® Session Manager

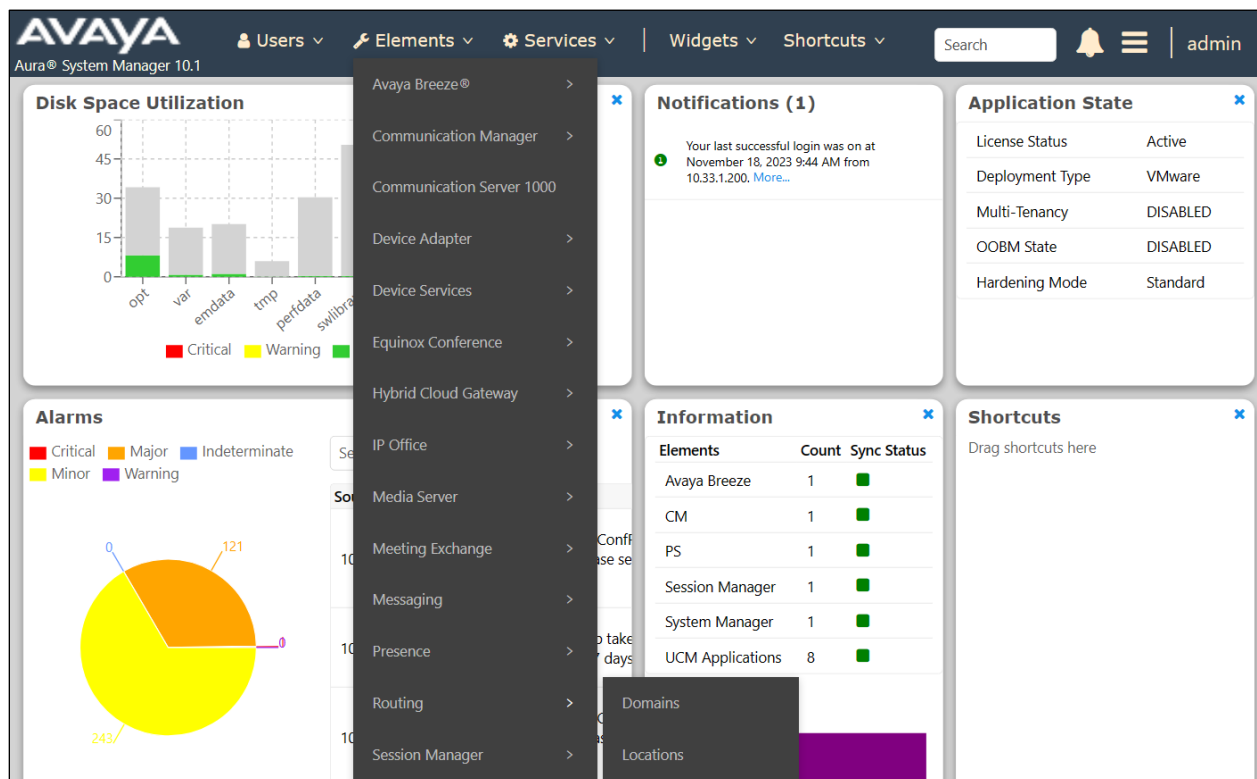
This section provides the procedures for configuring Session Manager. The procedures include the following areas:

- Launch System Manager.
- Administer Domain.
- Administer Locations.
- Administer SIP Entities.
- Administer Routing Policies.
- Administer Dial Patterns.

Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult the documentation in Additional References section for further details.

6.1. Launch System Manager

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “<https://<ip-address>/SMGR>”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). Once logged in, the **Home** screen is displayed. From the **Home** screen, under the **Elements** heading, select **Routing**.



6.2. Administer Domain

In the subsequent screen (not shown), select **Elements** → **Routing** to display the **Administration of Session Manager Routing Policies** screen below. Select **Routing** → **Domains** from the left pane and click **New** in the subsequent screen (not shown) to add a new domain.

Administration of Session Manager Routing Policies

A Routing Policy consists of routing elements such as "Domains", "Locations", "SIP Entities", etc.

The recommended order of routing element administration (that means the overall routing workflow) is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Conditions" (if Flexible Routing or Regular Expression Adaptations are in use)
- Step 4: Create "Adaptations"
- Step 5: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 6: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 7: Create "Time Ranges"
 - Align with the tariff information received from the Service Providers
- Step 8: Create "Routing Policies"
 - Assign the appropriate "Routing Destination" and "Time Of Day"

The **Domain Management** screen is displayed. In the **Name** field enter the domain name, select "sip" from the **Type** drop down menu and provide any optional **Notes**.

Domain Management

Commit Cancel

1 Item Filter: Enable

Name	Type	Notes
* avayalab.com	sip	SIP Domain name

6.3. Administer Locations

Locations identify logical and/or physical locations where SIP Entities reside, used for routing purposes. In the reference configuration, three locations are specified:

- **Main-LOC** – The enterprise site containing System Manager, Session Manager and other local servers and SIP endpoints.
- **CM-LOC** – Communication Manager, designated for Fonolo VCB.
- **SBC-LOC** – Avaya SBC.

6.3.1. Main Location

Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter a descriptive name for the Location (e.g., **Main**).
- **Notes:** Add a brief description.
- Click **Commit** to save.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The left-hand navigation pane is open, showing the 'Routing' section with 'Locations' selected. The main content area is titled 'Location Details' and contains the following sections:

- General**: Includes a required field for 'Name' (set to 'Main-LOC') and a 'Notes' field (set to 'Common Enterprise Locations').
- Dial Plan Transparency in Survivable Mode**: Features an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field.
- Overall Managed Bandwidth**: Includes a 'Managed Bandwidth Units' dropdown (set to 'Kbit/sec'), a 'Total Bandwidth' field, a 'Multimedia Bandwidth' field, and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'.

At the top right of the form, there are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

6.3.2. Avaya SBC Location

To configure Avaya SBC Location, repeat the steps in **Section 6.3.1** with the following changes:

AwayA

Aura® System Manager 10.1

Users ▾Elements ▾Services ▾Widgets ▾Shortcuts ▾Search

admin

HomeRouting

Routing

Domains

Locations

Conditions

Adaptations ▾

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns ▾

Regular Expressions

Defaults

Location Details

CommitCancel

Help ?

General

* Name: SBC-LOC

Notes: Session Border Controller Location

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec ▾


Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Scroll down to the **Location Pattern** sub-section, click **Add** and enter the private IP addresses of the SBC involved in the compliance testing in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.

Location Pattern

2 Items 
Filter: [Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.33.1.51	Private A1 IP address of SIP Trunk 1
<input type="checkbox"/>	* 10.33.1.54	Private A1 IP address of SIP Trunk 2

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

6.3.3. CM Location

To configure the Communication Manager location, repeat the steps in **Section 6.3.1** with the following changes:

AVAYA Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ admin

Home Routing

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

Location Details Commit Cancel Help ?

General

* **Name:** CM-LOC

Notes: Communication Manager Location

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec ▾

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Scroll down to the **Location Pattern** sub-section, click **Add** and enter the processor IP addresses of Communication Manager in **IP Address Pattern**, as shown below.

Location Pattern

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.33.1.43	CM Location

Select : All, None

Commit Cancel

6.4. Administer SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager, which includes Communication Manager and Avaya SBC.

6.4.1. Configure Session Manager SIP Entity

The following screen shows the previously configured Session Manager SIP Entity named **SM10**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.1.42** and select the location **Main-LOC** as defined in **Section 6.3.1** in the **Location** field.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The left navigation pane shows the 'Routing' menu expanded, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and contains two tabs: 'General' and 'Monitoring'. The 'General' tab is active, showing fields for Name (SM10), IP Address (10.33.1.42), SIP FQDN, Type (Session Manager), Notes, Location (Main-LOC), Outbound Proxy, Time Zone (America/Denver), Minimum TLS Version (Use Global Setting), and Credential name. The 'Monitoring' tab shows SIP Link Monitoring and CRLF Keep Alive Monitoring, both set to 'Use Session Manager Configuration'. The interface includes a top navigation bar with 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts' menus, a search bar, and a user profile 'admin'.

6.4.2. SIP Entity for Avaya SBC

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 SBC.

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:** Enter a descriptive name.
- **FQDN or IP Address:** The IP address of private A1 interface of Avaya SBC.
- **Type:** Set is as "SIP Trunk".
- **Notes:** Enter desired notes.
- **Location:** Select the **SBC-LOC** location as defined in **Section 6.3.2**.
- **Time Zone:** Select the applicable time zone.
- **SIP Link Monitoring:** Select "Link Monitoring Enabled" (not shown).

AVAYA
Aura® System Manager 10.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰ admin

Home Routing

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

SIP Entity Details

Commit Cancel Help ?

General

* Name: SBC-SP1

* FQDN or IP Address: 10.33.1.51

Type: SIP Trunk ▾

Notes: SIP Trunk for Fonolo VCB

Location: SBC-LOC ▾

Time Zone: America/Denver ▾

* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting ▾

Credential name:

Securable: ☐

Call Detail Recording: egress ▾

Adaptations

Add Remove

<input type="checkbox"/>	Order	Name	Module Name	State	Type	Notes
--------------------------	-------	------	-------------	-------	------	-------

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:** Enter a descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “SM10”.
- **Protocol:** Set it as “TLS”.
- **Port:** Set it as “5061”.
- **SIP Entity 2:** Avaya SBC entity name from this section.
- **Port:** Set it as “5061”.
- **Connection Policy:** Select “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"/>	* SM10-SBC-SP1-561	SM10	TLS ▾	* 5061	SBC-SP1	* 5061	trusted ▾	<input type="checkbox"/>

Select : All, None

6.4.3. 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 the screen below shows the previous configured SIP Entity of Communication Manager it is shown here for reference and display purpose.

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:** Enter a descriptive name.
- **FQDN or IP Address:** The IP address of the processor interface.
- **Type:** Select “CM”.
- **Notes:** Any desired notes.
- **Location:** Select “CM-LOC” location as defined in **Section 6.3.3**.
- **Time Zone:** Select the applicable time zone.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The left navigation pane shows the 'Routing' section expanded, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields and values:

- Name:** CM10-Public
- FQDN or IP Address:** 10.33.1.43
- Type:** CM
- Notes:** CM SIP Entity for public trunk
- Location:** CM-LOC
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty field)
- Securable:** ☐
- Call Detail Recording:** none


Buttons for 'Commit' and 'Cancel' are visible in the top right corner of the form area.

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

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “SM10”.
- **Protocol:** The signaling group transport TLS method.
- **Port:** The signaling group listen port 5063.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group listen port 5063 number.
- **Connection Policy:** Select “trusted”.

Entity Links
Override Port & Transport with DNS SRV: ☐

AddRemove

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"/>	* SM10-CM10-Public-5063	<input type="text" value="SM10"/>	TLS	* 5063	<input type="text" value="CM10-Public"/>	* 5063	trusted	<input type="checkbox"/>

Select : All, None

6.5. Administer Routing Policies

There were two routing policies used for the testing, one for Avaya SBC to reach to Fonolo VCB and one for Communication Manager.

6.5.1. Routing Policy for Avaya SBC

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 SBC.

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 SBC SIP entity name as created from **Section 6.4.2** in the **SIP Entities** window (not shown), leave the **Time of Day** sub-section as default. Click **Commit** to save.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (selected), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. It is divided into three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. The 'General' section has fields for 'Name' (To-SBC-SP1), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. The 'SIP Entity as Destination' section has a 'Select' button and a table with columns: Name, FQDN or IP Address, Type, and Notes. The table contains one row: SBC-SP1, 10.33.1.51, SIP Trunk, SIP Trunk for Fonolo VCB. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons, a 'Filter: Enable' link, and a table with columns: Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, and Notes. The table contains one row: 0, 24/7, with checkboxes for Mon through Sun all checked, and Start Time 00:00, End Time 23:59, and Notes Time Range 24/7. At the bottom of the 'Time of Day' section, it says 'Select : All, None'.

Name	FQDN or IP Address	Type	Notes
SBC-SP1	10.33.1.51	SIP Trunk	SIP Trunk for Fonolo VCB

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

6.5.2. 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 SIP entity in the **SIP Entities** window (not shown) and leave the **Time of Day** field as default. Click **Commit** to save.

Awaya
Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

admin

[Home](#)
[Routing](#)

Routing Policy Details

[Commit](#) [Cancel](#) [Help ?](#)

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select	Name	FQDN or IP Address	Type	Notes
<input checked="" type="checkbox"/>	CM10-Public	10.33.1.43	CM	CM SIP Entity for public trunk

Time of Day

[Add](#) [Remove](#) [View Gaps/Overlaps](#)
Filter: Enable

1 Item			Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	Ranking ▲												
<input type="checkbox"/>	0		24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial patterns are defined to direct calls to the appropriate SIP Entity. In the sample configuration, dial pattern 78000 was routed to the Fonolo VCB, through Avaya SBC and the dial pattern 3340 was routed to Communication Manager.

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. In the **General** section of the **Dial Pattern Details** page, provision the following:

- In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Avaya SBC. In the compliance testing, the entry allowed for call originations from all Communication Manager endpoints in locations “All”. The SBC routing policy from **Section 6.5.1** was selected as shown below.

KP; Reviewed:
SPOC 1/4/2024

6.6.2. Dial Pattern for Communication Manager

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. In the **General** section of the **Dial Pattern Details** page, provision the following:

- **Pattern** – Enter the dialed number or prefix (e.g., **3340**).
- **Min** and **Max** – Minimum and maximum length of dialed number (e.g., **4**).
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching Communication Manager. In the compliance testing, the entry allowed for call originations from all locations “All”. The CM routing policy from **Section 6.5.2** was selected as shown below.

AVAYA
Aura® System Manager 10.1

Users Elements Services Widgets Shortcuts Search admin

Home Routing

Conditions
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Dial Patterns
Origination Dial ...
Regular Expressions
Defaults

Dial Pattern Details Commit Cancel Help ?

General

* Pattern: 3340

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: avayalab.com

Notes: Fonolo VCB to call center VDN

Originating Locations and Routing Policies

Add Remove Filter: Enable

1 Item

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		To-CM10-Public	0	<input type="checkbox"/>	CM10-Public	

Select : All, None

7. Configure Avaya Session Border Controller

This section describes the required configuration of Avaya SBC to connect to Fonolo VCB using Cloud SIP Connect.

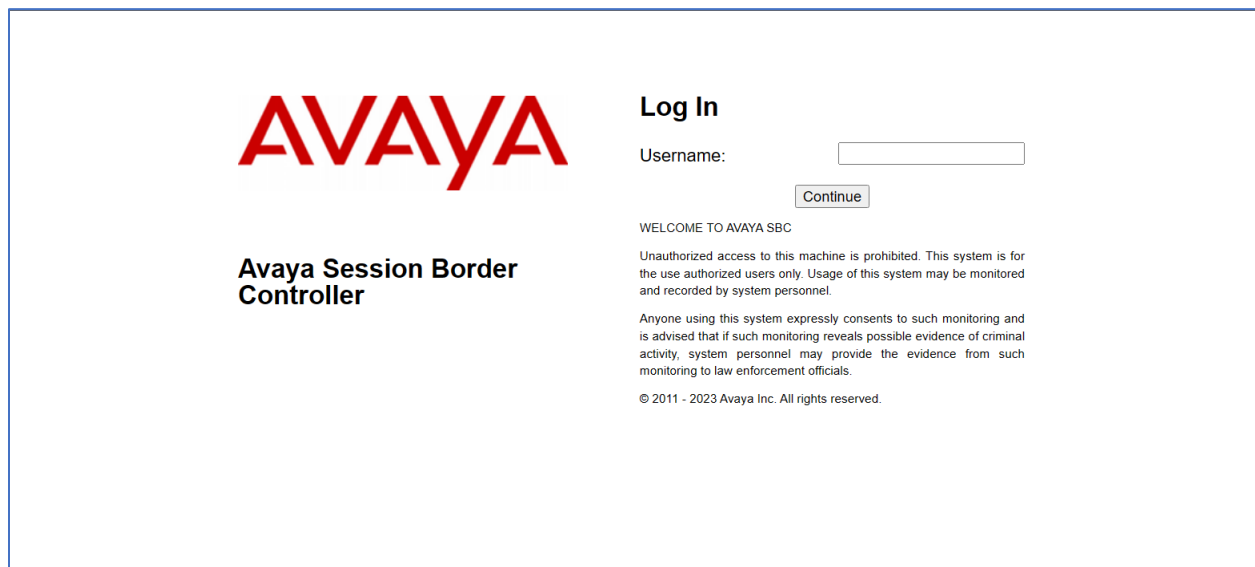
It is assumed that Avaya SBC was provisioned and is ready to be used; the configuration shown here is accomplished using the Avaya SBC web interface.

Note: In the following pages, and for brevity in these Application Notes, not every provisioning step will have a screenshot associated with it. Some of the default information in the screenshots that follow may have been cut out (not included) for brevity.

7.1. Log in Avaya Session Border Controller

Use a Web browser to access the Avaya SBC Web interface. Enter `https://<ip-addr>/sbc` in the address field of the web browser, where `<ip-addr>` is the Avaya SBC management IP address.

Enter the appropriate credentials and click **Log In**.



The screenshot displays the Avaya Session Border Controller login interface. On the left, the Avaya logo is shown in red, with the text "Avaya Session Border Controller" below it. On the right, the "Log In" section contains a "Username:" label, a text input field, and a "Continue" button. Below the login fields, there is a "WELCOME TO AVAYA SBC" message, 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." A consent statement follows: "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 - 2023 Avaya Inc. All rights reserved." is displayed.

Once logged in, on the top left of the screen, under **Device:** select the device being managed, **sbc102** in the sample configuration.

The left navigation pane contains the different available menu items used for the configuration of Avaya SBC. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.

Device: EMSAlarmsIncidentsStatusLogsDiagnosticsUsersSettingsHelpLog Out

EMS
sbc102

on Border Controller

AVAYA

EMS Dashboard

Software Management

Device Management

System Administration

Templates

Backup/Restore

Monitoring & Logging

Dashboard

Information

System Time	10:01:12 AM EST	Refresh
Version	10.1.2.0-64-23285	
GUI Version	10.1.2.0-23278	
Build Date	Tue May 16 08:55:42 IST 2023	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	11/08/2023 11:59:54 EST	
Failed Login Attempts	0	

Active Alarms (past 24 hours)

None found.

Installed Devices

EMS

sbc102

Incidents (past 24 hours)

sbc102: General Method not allowed Out-Of-Dialog

sbc102: No Subscriber Flow Matched

sbc102: General Method not allowed Out-Of-Dialog

sbc102: No Subscriber Flow Matched

7.2. Device Management

To view current system information, select **Device Management** on the left navigation pane. In the reference configuration, the device named **sbc102** is shown. The management IP address that was configured during installation is masked out for security reasons; the current software version is shown. The management IP address needs to be on a subnet separate from the ones used in all other interfaces of Avaya SBC, segmented from all VoIP traffic. Verify that the **Status** is **Commissioned**, indicating that the initial installation process of the device has been previously completed, as shown on the screen below.

Device: EMS Alarms Incidents Status Logs Diagnostics Users

Settings Help Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard
Software Management
Device Management
 System Administration
 Templates
Backup/Restore
 Monitoring & Logging

Device Management

Devices Updates Licensing Key Bundles

Device Name	Management IP	Version	Status	
sbc102	10.1.2.0-64-23285	10.1.2.0-64-23285	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

To view the network configuration assigned to the SBC, click **View** on the screen above. The **System Information** window is displayed, containing the current device configuration and network settings.

The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.

System Information: sbc102

General Configuration

Appliance Name

sbc102

Box Type

SIP

Deployment Mode

Proxy

HA Mode

No

Management IP(s)

IP #1 (IPv4)

[REDACTED]102

DNS Configuration

Primary DNS

10.33.100.60

Secondary DNS

8.8.8.8

DNS Location

DMZ

DNS Client IP

10.33.1.51

License Allocation

Standard Sessions

Requested: 0

0

Advanced Sessions

Requested: 0

0

Scopia Video Sessions

Requested: 0

0

CES Sessions

Requested: 0

0

Transcoding Sessions

Requested: 0

0

AMR

☐

Premium Sessions

Requested: 0

0

CLID

Encryption

Available: Yes

☒

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.33.1.51	10.33.1.51	255.255.255.0	10.33.1.1	A1
10.33.1.52	10.33.1.52	255.255.255.0	10.33.1.1	A1
10.33.1.53	10.33.1.53	255.255.255.0	10.33.1.1	A1
10.33.1.54	10.33.1.54	255.255.255.0	10.33.1.1	A1
10.207.80.90	10.207.80.90	255.255.255.128	10.207.80.1	B1
10.207.80.107	10.207.80.107	255.255.255.128	10.207.80.1	B1

The IP addresses in the **System Information** screen shown above are the ones used for the SIP trunk to the Fonolo VCB and are the ones relevant to these Application Notes. Other IP addresses assigned to the **SBC A1** and **B1** interfaces are used to support remote workers and other SIP trunks, and they are not discussed in this document. Also note that for security purposes, any public IP addresses used during the compliance test have been masked out in this document.

In the reference configuration, the private interface of the SBC (10.33.1.51) was used to connect to the enterprise network, while its public interface (10.207.80.107) was used to connect to the Fonolo VCB. See **Figure 1**.

7.3. TLS Management

Note –Avaya SBC in the test configuration used identity certificates signed by Avaya System Manager for the TLS internal connections to Session Manager and other Avaya systems. The procedure to create and obtain these certificates, and the creation of TLS Client and Server Profiles for these internal connections is outside the scope of these Application Notes.

The TLS connection from Avaya SBC to Fonolo Cloud SIP Connect uses a server authentication scheme. In this method of connection, the client (Avaya SBC) initiates a request to the server for a secure session. The server then sends its identity certificate to the client. The client checks the received server identity certificate against the trusted Certification Authority (CA) certificates that are saved in its trust store, to verify that the server identity certificate is signed by a CA that the client trusts. DigiCert was used as the trusted CA by Fonolo Cloud SIP Connect, so the DigiCert Global Root G2 certificate needed to be downloaded and imported into Avaya SBC trust store.

In the reference configuration, TLS transport is used for the communication between Avaya SBC and Fonolo Cloud SIP Connect. This section covers the installation of the root certificate and the configuration of the TLS client profile, used in the connection to Fonolo Cloud SIP Connect. By default, the DigiCert Global Root G2 certificate is already installed in the trusted CA of Avaya SBC as shown below.

Device: sbc102 ▾ Alarms Incidents Status ▾ Logs ▾ Diagnostics Users Settings ▾ Help ▾ Log Out

Avaya Session Border Controller

AVAYA

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

Certificates

Install Generate CSR

Certificates

Installed Certificates

sbc102.pem	View	Delete
------------	----------------------	------------------------

Installed CA Certificates

avayaitrootca2.pem	View	Delete
entrust_g2_ca.cer	View	Delete
AvayaDeviceEnrollmentCAchain.crt	View	Delete
SMGRCA10.pem	View	Delete
DigiCertGlobalRootG2.crt	View	Delete

Installed Certificate Revocation Lists

No certificate revocation lists have been installed.

Installed Certificate Signing Requests

sbc102.req	Delete
------------	------------------------

7.3.1. TLS Client Profile for Fonolo Cloud SIP Connect

Select **TLS Management** → **Client Profiles** and click on **Add**. Enter the following:

- **Profile Name:** enter descriptive name.
- **Certificate:** select the existing SBC identity certificate from the pull-down menu.
- **Peer Verification = Required.**
- **Peer Certificate Authorities:** Select the **DigiCertGlobalRootG2.pem** certificate.
- **Verification Depth:** enter **1**.
- Click **Next**.

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

Changing the certificate in a TLS Profile which has SNI enabled may cause existing Reverse Proxy entries which utilize this TLS Profile to become invalid.

TLS Profile	
Profile Name	<input type="text" value="TLS_Fonolo_Client"/>
Certificate	<input type="text" value="sbc102.pem"/>
SNI	<input type="checkbox"/> Enabled

Certificate Verification	
Peer Verification	Required
Peer Certificate Authorities	<div>entrust_g2_ca.cer AvayaDeviceEnrollmentCAchain.crt SMGRCA10.pem DigiCertGlobalRootG2.crt</div>
Peer Certificate Revocation Lists	<div></div>
Verification Depth	<input type="text" value="1"/>
Extended Hostname Verification	<input type="checkbox"/>
Server Hostname	<input type="text"/>

Next

Make sure the **TLS 1.2** is selected and click **Finish** on the next window to save configuration.

Edit Profile

Renegotiation Parameters

Renegotiation Time

0

seconds

Renegotiation Byte Count

0

Handshake Options

Version

☒ TLS 1.3

☒ TLS 1.2

Ciphers

☒ Default

☐ FIPS

☐ Custom

Value

(What's this?)

DEFAULT:!SHA

Back

Finish

The following screen shows the completed TLS **Client Profile** form:

Device: sbc102

Alarms

Incidents

Status

Logs

Diagnostics

Users

Settings

Help

Log Out

Avaya Session Border Controller

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

Domain Policies

TLS Management

Certificates

Client Profiles

Server Profiles

SNI Group

Network & Flows

DMZ Services

Monitoring & Logging

Client Profiles: TLS_Fonolo_Client

Add

Delete

Client Profiles

AvayaSBCCClient

TLS_Fonolo_Cli...

Client Profile

Click here to add a description.

TLS Profile

Profile Name

TLS_Fonolo_Client

Certificate

sbc102.pem

SNI

☐ Enabled

Certificate Verification

Peer Verification

Required

Peer Certificate Authorities

DigiCertGlobalRootG2.crt

Peer Certificate Revocation Lists

--

Verification Depth

1

Extended Hostname Verification

☐

Renegotiation Parameters

Renegotiation Time

0

KP; Reviewed:
SPOC 1/4/2024

Avaya DevConnect Application Notes
©2024 Avaya Inc. All Rights Reserved

37 of 69
FonoloVCB-SBC10

7.4. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBC, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited and modified as needed to optimize device performance and network efficiency.

Select **Networks & Flows** → **Network Management** from the menu on the left-hand side. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 and B2 are used.

The screenshot shows the Avaya Session Border Controller interface. The left sidebar contains a menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, and Network & Flows. The 'Network & Flows' section is expanded, showing 'Network Management' as the selected option. The main content area is titled 'Network Management' and has two tabs: 'Interfaces' (selected) and 'Networks'. A table displays the status of interfaces:

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Enabled

An 'Add VLAN' button is located in the top right corner of the table area.

Select the **Networks** tab to display the IP provisioning for the A1 and B2 interfaces. Some of these values are specified during installation. Addresses can be added, modified, or deleted by selecting **Edit** on each interface.

The following IP addresses were assigned to be used by Fonolo VCB traffic:

- **A1: 10.33.1.51** – “Inside” IP address, toward Session Manager.
- **B1: 10.207.80.107** – “Outside” IP address toward the SIP trunk to Fonolo Cloud SIP Connect.

The screenshot shows the Avaya Session Border Controller interface, specifically the 'Networks' tab under 'Network Management'. The left sidebar is the same as in the previous screenshot. The main content area shows the 'Networks' tab selected. A table displays network configurations:

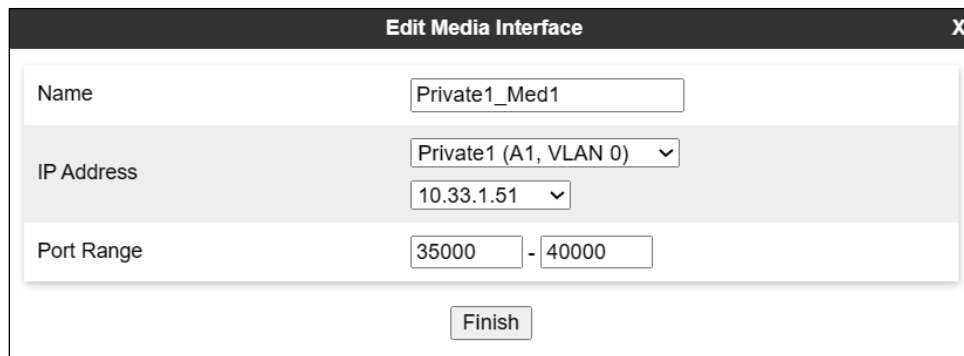
Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Inside A1	10.64.91.1	255.255.255.0	A1	10.64.91.47, 10.64.91.48, 10.64.91.49, 10.64.91.50	Edit Delete
Public B2	192.168.80.1	255.255.255.128	B2	192.168.80.77	Edit Delete

An 'Add' button is located in the top right corner of the table area.

7.5. Media Interfaces

To add to the internal media interface toward the enterprise select **Network & Flows → Media Interface** from the menu on the left-hand side. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

- **Name:** Enter an appropriate name (e.g., **Private1_Med1**).
- **IP Address:** Select **PrivateA1 (A1, VLAN0)** and the IP address used for traffic towards Communication Manager (e.g., **10.33.1.51**) from the drop-down menus.
- **Port Range:** **35000 – 40000**.
- Click **Finish**.



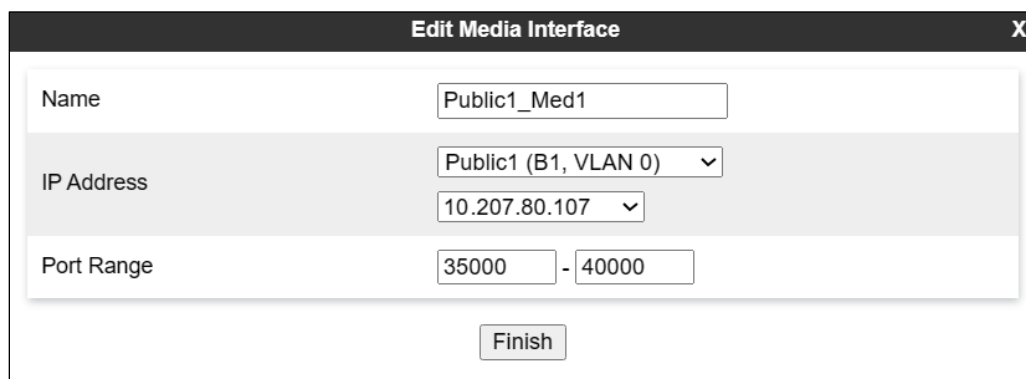
The screenshot shows the 'Edit Media Interface' window with the following configuration:

Edit Media Interface	
Name	Private1_Med1
IP Address	Private1 (A1, VLAN 0) 10.33.1.51
Port Range	35000 - 40000
Finish	

Select **Add** (not shown) to add to the external media interface toward the Fonolo VCB.

Enter the following:

- **Name:** Enter an appropriate name (e.g., **Public1_Med1**).
- **IP Address:** Select **Public1 (B1, VLAN0)** and the IP address used for the SIP trunk to Fonolo VCB (e.g., **10.207.80.107**) from the drop-down menus.
- **Port Range:** **35000 – 40000**.
- Click **Finish**.



The screenshot shows the 'Edit Media Interface' window with the following configuration:

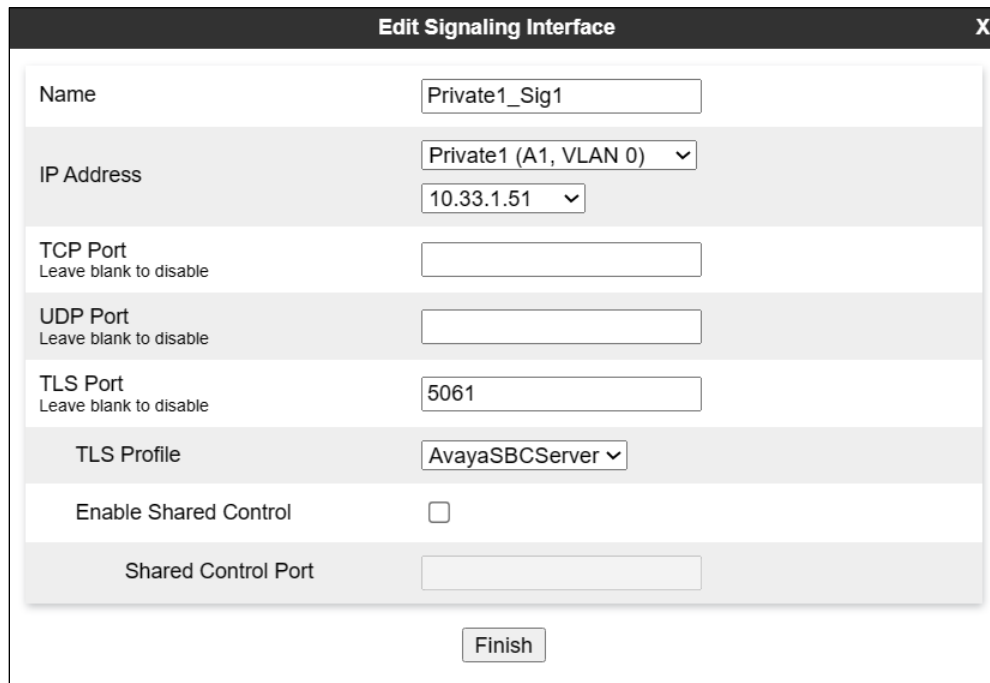
Edit Media Interface	
Name	Public1_Med1
IP Address	Public1 (B1, VLAN 0) 10.207.80.107
Port Range	35000 - 40000
Finish	

7.6. Signaling Interfaces

Select **Network & Flows** → **Signaling Interface** from the menu on the left-hand side.

Select **Add** (not shown) to add to the internal signaling interface toward the enterprise. Enter the following:

- **Name:** Enter an appropriate name (e.g., **Private1_Sig1**).
- **IP Address:** Select **Private1 (A1, VLAN0)** and **10.33.1.51**.
- **TLS Port:** **5061**.
- **TLS Profile:** Select the existing TLS server profile on the enterprise (e.g., **AvayaSBCServer**). See **Note** on **Section 7.3**.
- Click **Finish**.



The screenshot shows a web-based configuration window titled "Edit Signaling Interface" with a close button (X) in the top right corner. The window contains several input fields and a "Finish" button at the bottom. The fields are arranged in a form with alternating light and dark gray backgrounds for each row. The "Name" field contains "Private1_Sig1". The "IP Address" section has a dropdown menu showing "Private1 (A1, VLAN 0)" and a text field below it containing "10.33.1.51". The "TCP Port" field is empty, with the text "Leave blank to disable" below it. The "UDP Port" field is empty, with the text "Leave blank to disable" below it. The "TLS Port" field contains "5061", with the text "Leave blank to disable" below it. The "TLS Profile" dropdown menu shows "AvayaSBCServer". The "Enable Shared Control" checkbox is unchecked. The "Shared Control Port" field is empty. The "Finish" button is located at the bottom center of the window.

Name	Private1_Sig1
IP Address	Private1 (A1, VLAN 0) 10.33.1.51
TCP Port	 Leave blank to disable
UDP Port	 Leave blank to disable
TLS Port	5061 Leave blank to disable
TLS Profile	AvayaSBCServer
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

Select **Add** (not shown), to add to the external signaling interface toward the Fonolo VCB

- **Name:** Enter an appropriate name (e.g., **Public1_Sig1**).
- **IP Address:** Select **Public1 (B1, VLAN0)** and **10.207.80.107**.
- **TLS Port:** **5061**.
- **TLS Profile:** Select the existing TLS server profile on the enterprise (e.g., **AvayaSBCServer**). See **Note** on **Section 7.3**.

Edit Signaling Interface X

Name	Public1_Sig1
IP Address	Public1 (B1, VLAN 0) 10.207.80.107
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	5061
TLS Profile	AvayaSBCServer
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

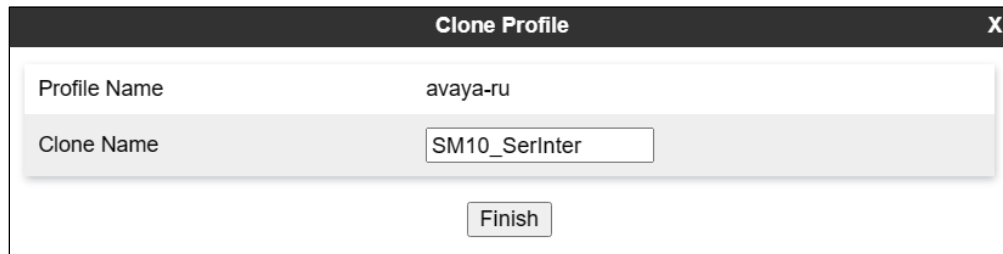
7.7. Server Interworking Profiles

A server interworking profile defines a set of parameters that aid in interworking between Avaya SBC and a connected server. The Server Interworking profiles shown were already in place and reused in the configuration to Fonolo VCB, their provisioning is covered here for completeness.

7.7.1. Server Interworking Profile for Session Manager

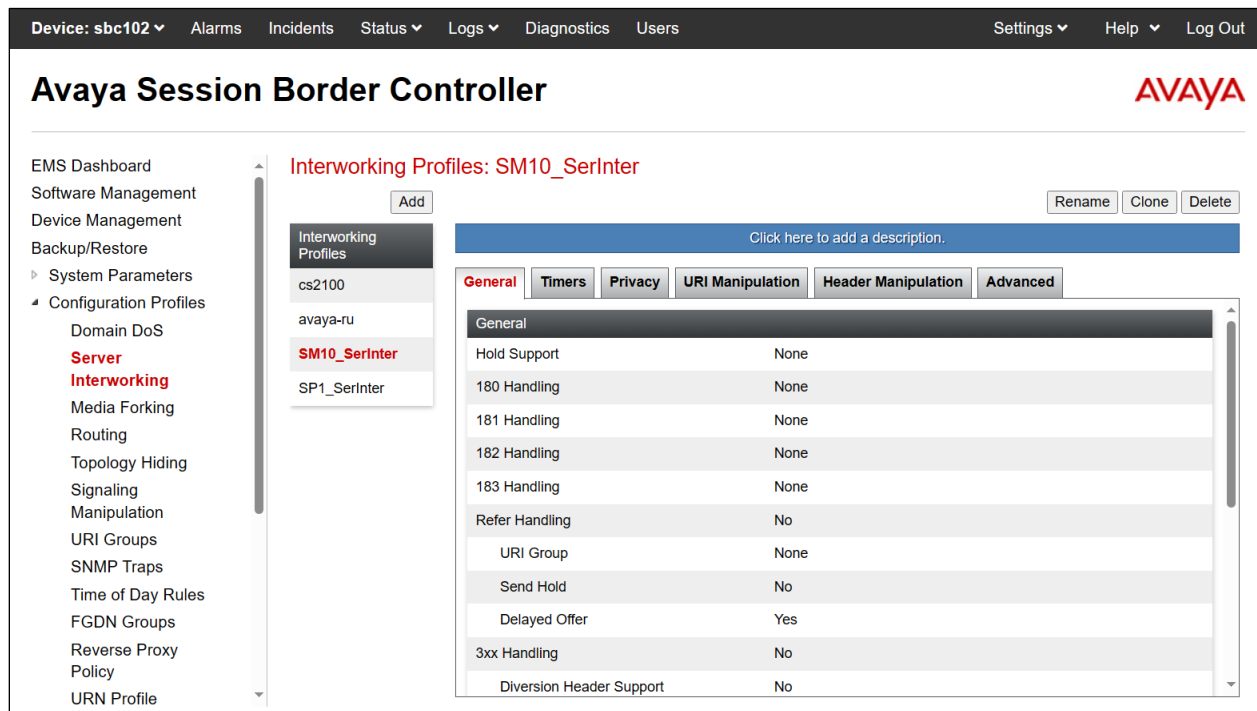
The Session Manager server interworking profile was cloned from the **avaya-ru** profile and left unmodified. Select **Configuration Profiles → Server Interworking** from the left-hand menu.

- Select the pre-defined **avaya-ru** profile and click the **Clone** button.
- Enter profile name: (e.g., **SM10_SerInter** and click **Finish** to continue.



The image shows a 'Clone Profile' dialog box. It has a title bar with 'Clone Profile' and a close button 'X'. Inside, there are two input fields: 'Profile Name' with the value 'avaya-ru' and 'Clone Name' with the value 'SM10_SerInter'. At the bottom, there is a 'Finish' button.

The **General** tab below shows the default settings used.



The image shows the Avaya Session Border Controller configuration interface. The top navigation bar includes 'Device: sbc102', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header is 'Avaya Session Border Controller' with the AVAYA logo. The left sidebar contains a tree view with 'Configuration Profiles' expanded, showing 'Domain DoS', 'Server', 'Interworking' (highlighted), 'Media Forking', 'Routing', 'Topology Hiding', 'Signaling Manipulation', 'URI Groups', 'SNMP Traps', 'Time of Day Rules', 'FGDN Groups', 'Reverse Proxy Policy', and 'URN Profile'. The main content area is titled 'Interworking Profiles: SM10_SerInter' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below this is a tabbed interface with 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced' tabs. The 'General' tab is active, showing a table of settings:

General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No

The Advanced tab below shows the default settings used.

The screenshot shows the Avaya Session Border Controller configuration interface. The top navigation bar includes 'Device: sbc102', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Avaya Session Border Controller' and the 'AVAYA' logo. The left-hand menu lists various configuration options, with 'Server Interworking' highlighted. The main content area is titled 'Interworking Profiles: SM10_SerInter' and features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. A list of profiles includes 'cs2100', 'avaya-ru', 'SM10_SerInter' (selected), and 'SP1_SerInter'. The 'Advanced' tab is active, showing settings for 'Include End Point IP for Context Lookup' (Yes), 'Extensions' (Avaya), 'Diversion Manipulation' (No), 'Has Remote SBC' (Yes), 'Route Response on Via Port' (No), 'Relay INVITE Replace for SIPREC' (No), 'MOBX Re-INVITE Handling' (No), 'NATing for 301/302 Redirection' (Yes), and 'DTMF Support' (None). An 'Edit' button is located at the bottom right of the settings table.

7.7.2. Server Interworking Profile for Fonolo VCB

The server interworking profile used in the connection to the Fonolo VCB was also cloned from the **avaya-ru** profile and left unchanged. Select **Configuration Profiles → Server Interworking** from the left-hand menu.

- Select the pre-defined **avaya-ru** profile and click the **Clone** button.
- Enter profile name: (e.g., **Fonolo_SerInter**), and click **Finish**.

The screenshot shows a 'Clone Profile' dialog box with a close button (X) in the top right corner. It contains two input fields: 'Profile Name' with the value 'avaya-ru' and 'Clone Name' with the value 'Fonolo_SerInter'. A 'Finish' button is located at the bottom center of the dialog.

7.8. SIP Server Profiles

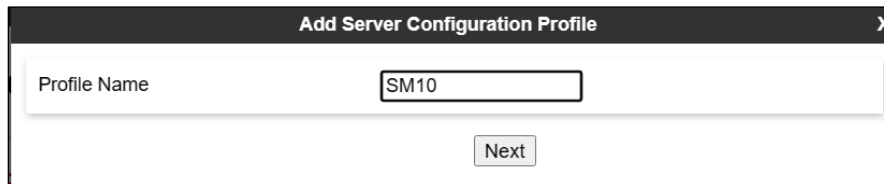
SIP Server Profiles are required for each server connected to Avaya SBC. A new server profile was created for Fonolo VCB. The SIP Server Profile for Session Manager was already in place and reused in the configuration.

Note: Avaya SBC in the test configuration used identity certificates signed by Avaya System Manager for the TLS internal connections to Session Manager. The procedure to create and obtain these certificates and the creation of TLS client and server profiles for these connections is outside the scope of these Application Notes.

7.8.1. SIP Server Profile – Session Manager

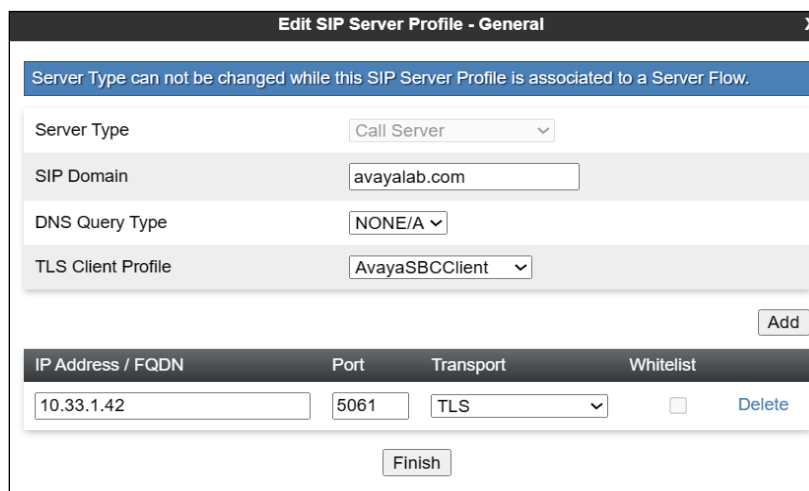
This section defines the SIP Server Profile for Avaya SBC connection to Session Manager.

- Select **Services** → **SIP Servers** from the left-hand menu.
- Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **SM10**) and click **Next**.



The **Add Server Configuration Profile** window will open.

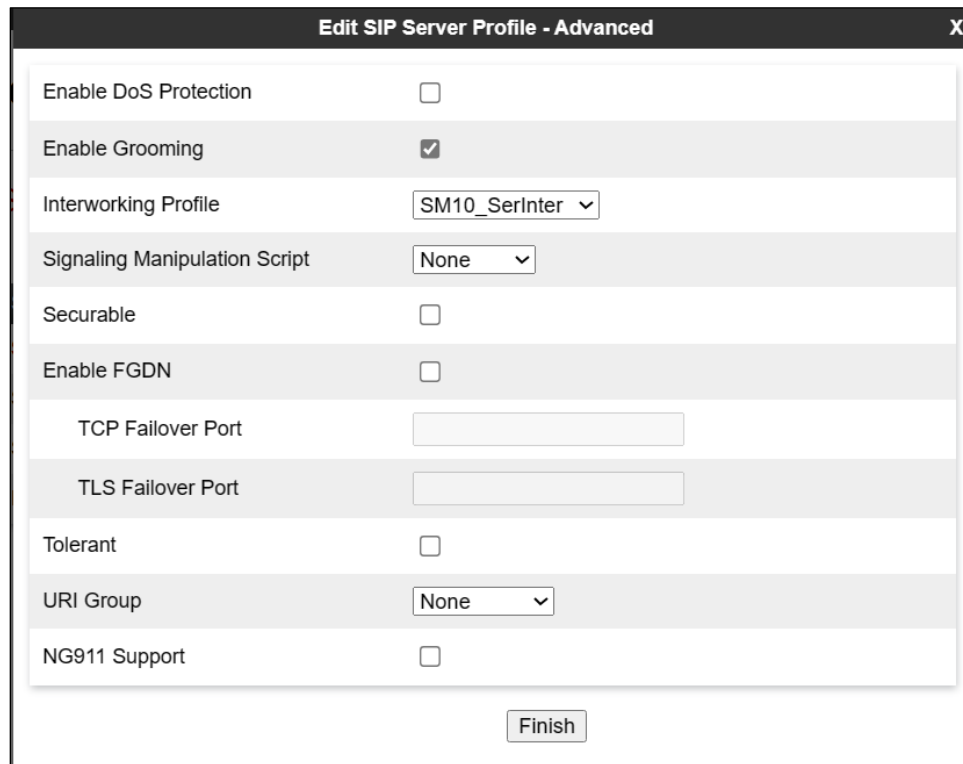
- **Server Type:** **Call Server**.
- **TLS Client Profile:** Select the existing TLS client profile on the enterprise (e.g., **AvayaSBCCClient**).
- **IP Address:** **10.33.1.42** (Session Manager Security Module IP address).
- Select **Port:** **5061**, **Transport:** **TLS**.
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish**.



Default values can be used on the **Authentication** tab.

Default values are used on the **Registration** and **Ping** tabs. On the **Advanced** tab:

- Select the **SM10_SerInter** (Section 7.7.1), for **Interworking Profile**.
- Since TLS transport is specified, then the **Enable Grooming** option should be enabled.
- In the **Signaling Manipulation Script** field select **none**.
- Select **Finish**.



The screenshot shows a configuration window titled "Edit SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains several settings, each with a label and a control element (checkbox or dropdown menu). The settings are as follows:

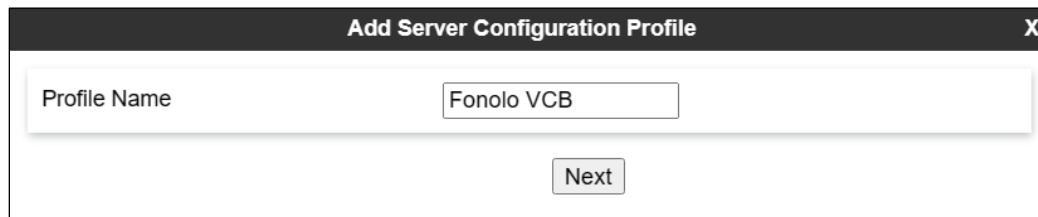
Setting	Value
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	SM10_SerInter
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

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

7.8.2. SIP Server Profile – Fonolo VCB

Repeat the steps in **Section 7.8.1**, with the following changes, to create a SIP Server Profile for Avaya SBC connection to Fonolo VCB.

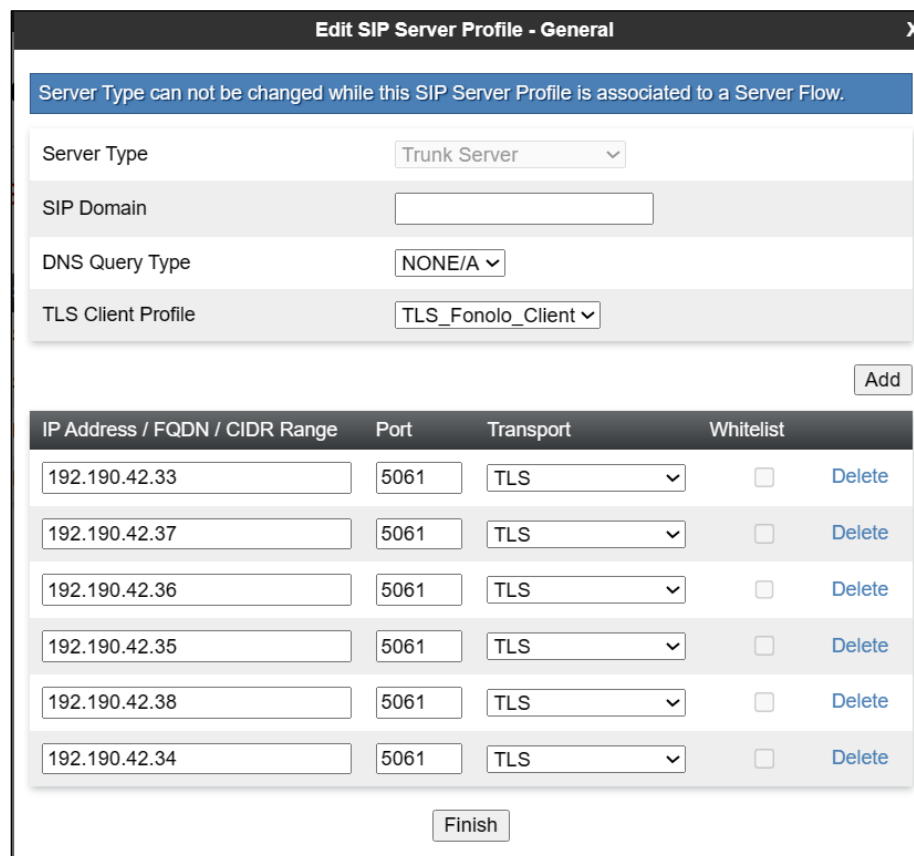
Select **Add** and enter a Profile Name (e.g., **Fonolo VCB**) and select **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". Inside, there is a text input field labeled "Profile Name" which contains the text "Fonolo VCB". Below the input field is a button labeled "Next".

On the **General** window, enter the following:

- **Server Type: Trunk Server.**
- **TLS Client Profile:** Select the client profile created in **Section 7.3.1**.
- Select **Add** and enter the IP addresses for the SIP connections to Fonolo VCB, provided by Fonolo. The service used in the reference configuration consists of 6 IP addresses.
- Select **Port: 5061, Transport: TLS.**
- If adding the profile, click **Next** (not shown) to proceed to next tab.



The screenshot shows the "Edit SIP Server Profile - General" window. At the top, a message states: "Server Type can not be changed while this SIP Server Profile is associated to a Server Flow." Below this, there are four configuration fields:

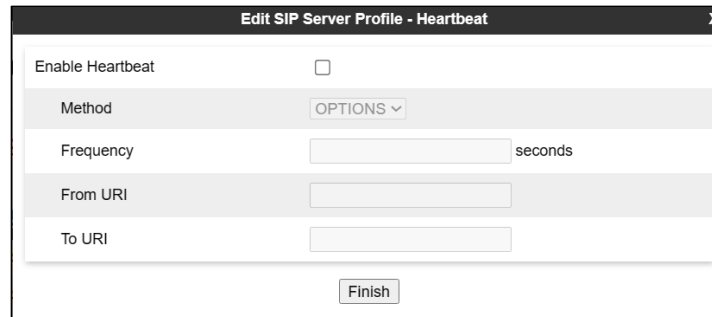
- Server Type: Trunk Server (dropdown menu)
- SIP Domain: (empty text field)
- DNS Query Type: NONE/A (dropdown menu)
- TLS Client Profile: TLS_Fonolo_Client (dropdown menu)

To the right of these fields is an "Add" button. Below the fields is a table with 6 rows of IP addresses, all with Port 5061 and Transport TLS. Each row has a "Whitelist" checkbox and a "Delete" link.

IP Address / FQDN / CIDR Range	Port	Transport	Whitelist	
192.190.42.33	5061	TLS	<input type="checkbox"/>	Delete
192.190.42.37	5061	TLS	<input type="checkbox"/>	Delete
192.190.42.36	5061	TLS	<input type="checkbox"/>	Delete
192.190.42.35	5061	TLS	<input type="checkbox"/>	Delete
192.190.42.38	5061	TLS	<input type="checkbox"/>	Delete
192.190.42.34	5061	TLS	<input type="checkbox"/>	Delete

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

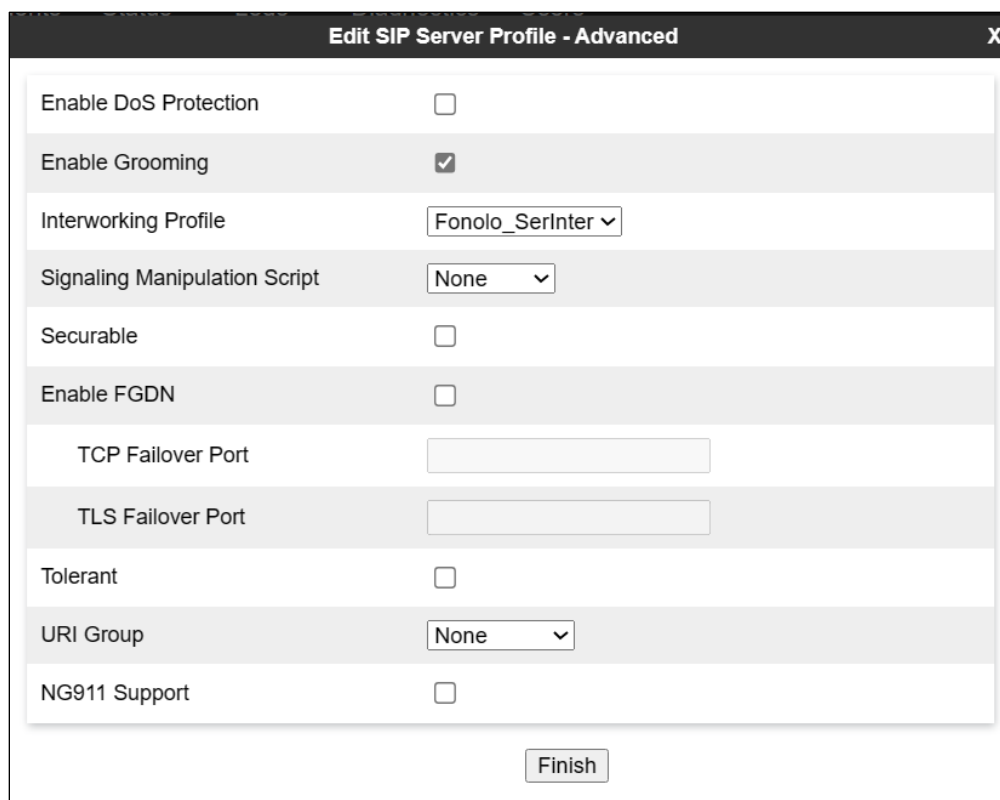
Default values are used on the **Authentication** tab. On the **Heartbeat** tab, keep it as default (uncheck the **Enable Heartbeat**) to have Avaya SBC forward OPTIONS message from Session Manager to the Fonolo Cloud SIP servers. The screen below shows the values used in the reference configuration.



The screenshot shows the 'Edit SIP Server Profile - Heartbeat' window. It contains the following fields and controls:

- Enable Heartbeat:** An unchecked checkbox.
- Method:** A dropdown menu set to 'OPTIONS'.
- Frequency:** A text input field followed by the label 'seconds'.
- From URI:** A text input field.
- To URI:** A text input field.
- Finish:** A button at the bottom center.

Default values are used on the **Registration** and **Ping** tabs. On the **Advanced** window, **Enable Grooming** is selected. Select the **Fonolo_SerInter** (Section 7.7.2), for **Interworking Profile**. All other parameters retain their default values.



The screenshot shows the 'Edit SIP Server Profile - Advanced' window. It contains the following fields and controls:

- Enable DoS Protection:** An unchecked checkbox.
- Enable Grooming:** A checked checkbox.
- Interworking Profile:** A dropdown menu set to 'Fonolo_SerInter'.
- Signaling Manipulation Script:** A dropdown menu set to 'None'.
- Securable:** An unchecked checkbox.
- Enable FGDN:** An unchecked checkbox.
- TCP Failover Port:** A text input field.
- TLS Failover Port:** A text input field.
- Tolerant:** An unchecked checkbox.
- URI Group:** A dropdown menu set to 'None'.
- NG911 Support:** An unchecked checkbox.
- Finish:** A button at the bottom center.

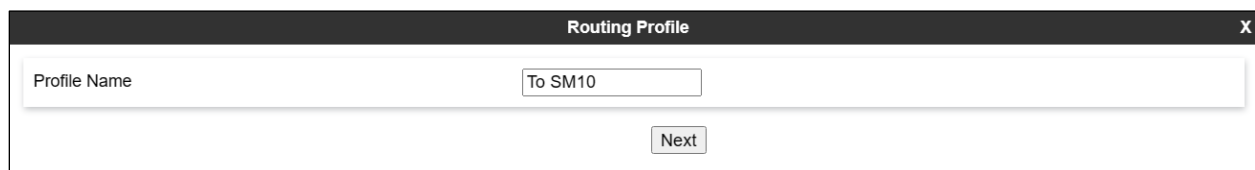
7.9. Routing Profiles

Routing Profiles are used to specify the next-hop for a SIP message. A routing profile is applied after the traffic has matched an End Point Flow defined in **Section 7.13**. The IP addresses and ports defined here will be used as destination addresses for signaling.

7.9.1. Routing Profile – Session Manager

A routing profile for inbound calls to Session Manager was already in place, and it was reused in the configuration for Fonolo VCB. Follow the steps below to create a routing profile to the Session Manager if one doesn't already exist.

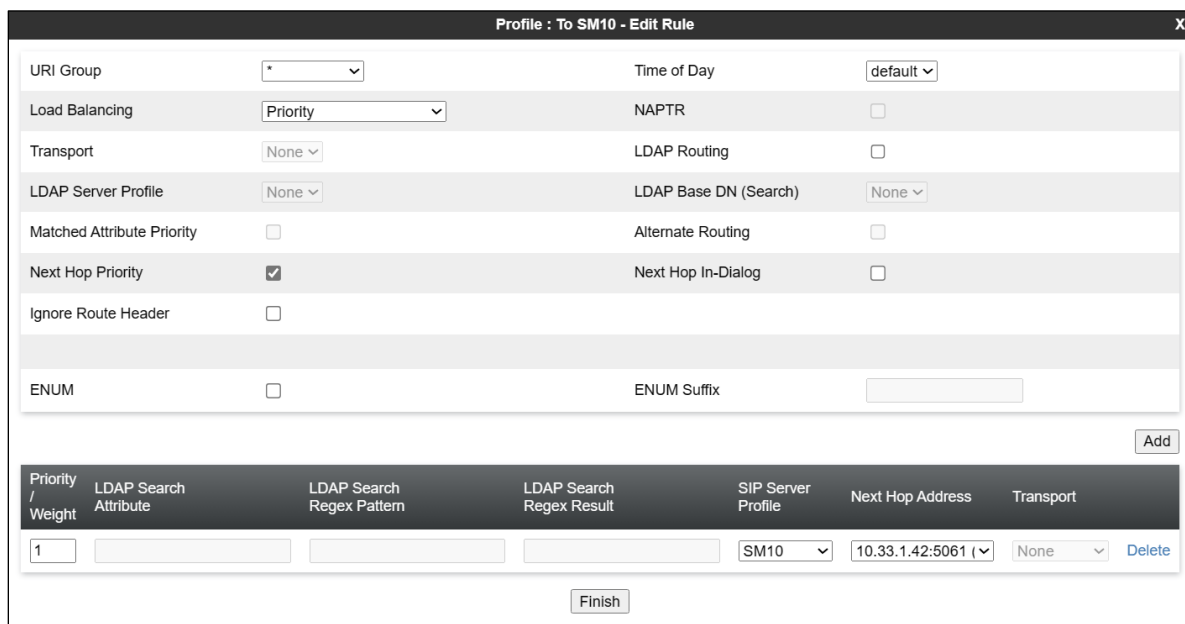
Navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** (e.g., **To SM**) and click **Next** to continue.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "To SM10". Below the input field is a button labeled "Next".

The Routing Rule window will open. The parameters in the top portion of the profile are left at their default settings. Click the **Add** button. The Next-Hop Address section will open at the bottom of the profile. Populate the following fields:

- **Priority/Weight: 1**
- **SIP Server Profile: SM10** (from **Section 7.8.1**).
- **Next Hop Address:** Verify that the **10.33.1.42:5061 (TLS)** entry from the drop-down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out. Click **Finish**.



The screenshot shows a window titled "Profile : To SM10 - Edit Rule" with a close button (X) in the top right corner. The window contains a form with various settings. At the bottom right, there is an "Add" button. Below the form, there 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. The first row of the table has the following values: 1, (empty), (empty), (empty), SM10, 10.33.1.42:5061 (v), and None. A "Delete" button is next to the last cell. At the bottom center, there is a "Finish" button.

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				SM10	10.33.1.42:5061 (v)	None

7.9.2. Routing Profile – Fonolo VCB

A routing profile for Fonolo VCB was already created during the testing, and it was shown in the configuration for reference purpose.

Navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** (e.g., **To Fonolo VCB**) and click **Next** to continue. If the profile already exists, select the profile and click **Add** on the right side of the screen to add a new routing rule to the profile.

Routing Profile

Profile Name

To Fonolo VCB

Next

On the Routing Rule window, leave **URI Group** at default and select **Round-Robin** in the **Load Balancing** field. Click the **Add** button. The **Next-Hop Address** section will open at the bottom of the profile. Populate the following fields:

- **SIP Server Profile:** Select **Fonolo VCB** server profile (from **Section 7.8.2**).
- **Next Hop Address:** Select two IP addresses **192.190.42.33** and **192.190.42.34** (from **Section 7.8.2**). Note that Fonolo Cloud SIP Connect receives voice call-backs on these two dedicated IP addresses, other 4 IP addresses are used to place outbound calls. Click **Finish**.

Profile : To Fonolo VCB - Edit Rule

URI Group

*

Time of Day

default

Load Balancing

Round-Robin

NAPTR

Transport

None

LDAP Routing

LDAP Server Profile

None

LDAP Base DN (Search)

None

Matched Attribute Priority

Alternate Routing

Next Hop Priority

Next Hop In-Dialog

Ignore Route Header

ENUM

ENUM Suffix

Add

Priority / Weight

LDAP Search Attribute

LDAP Search Regex Pattern

LDAP Search Regex Result

SIP Server Profile

Next Hop Address

Transport

0

Fonolo VC

192.190.42.33:50

None

Delete

0

Fonolo VC

192.190.42.34:50

None

Delete

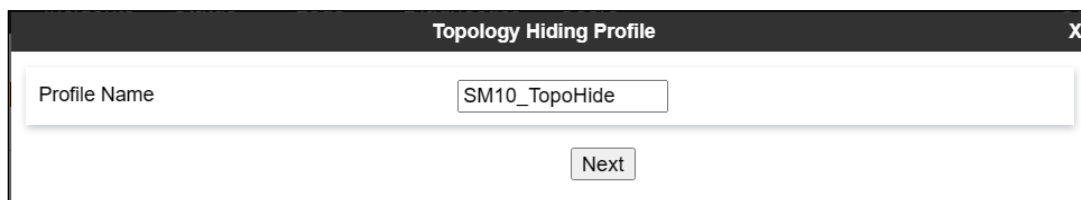
Finish

7.10. Topology Hiding Profile

The **Topology Hiding** profile manages how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

In the sample configuration, the existing enterprise Topology Hiding Profile was reused. This profile was previously cloned from the **default** profile and then modified, to adapt the host portion of the SIP headers, to the domain expected on the enterprise network. The configuration is shown here for completeness.

- Select **Configuration Profiles** → **Topology Hiding** from the left-hand menu.
- Select the pre-defined **default** profile and click the **Clone** button.
- Enter profile name: (e.g., **SM10_ToppHide**), and click **Finish** to continue.

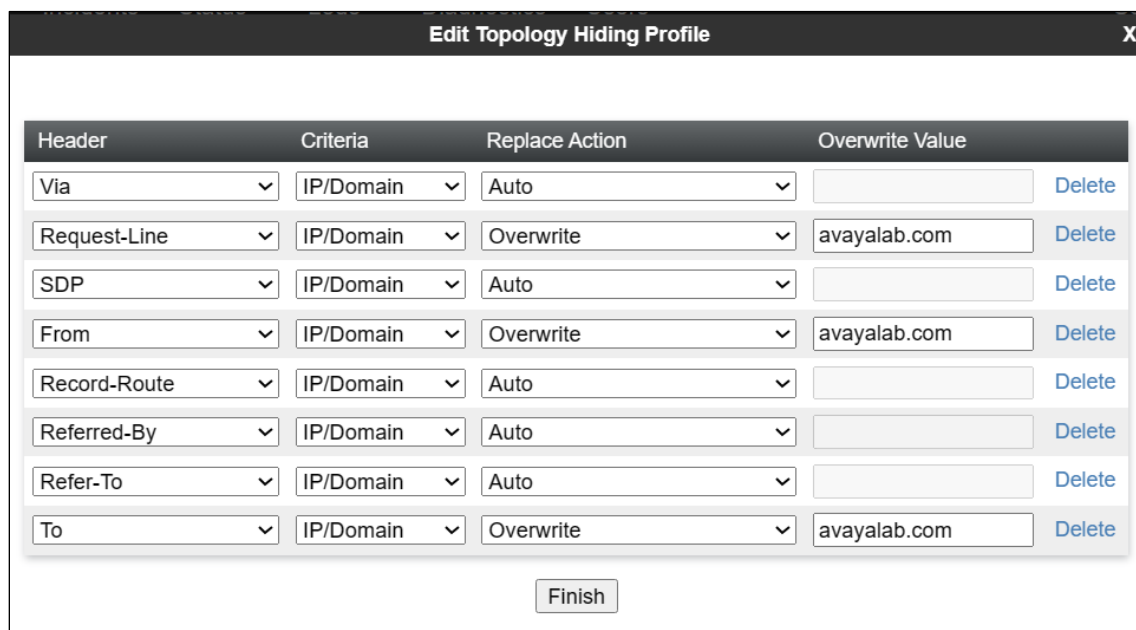


Topology Hiding Profile

Profile Name: SM10_TopoHide

Next

- Edit the newly created **SM10_TopoHide** profile.
- For the **Request-Line**, **To** and **From** headers select **Overwrite** under the **Replace Action** column. Enter the domain of the enterprise (e.g., **avayalab.com**) on the **Overwrite Value** field.
- Click **Finish**.



Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value	
Via	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	avayalab.com	Delete
SDP	IP/Domain	Auto		Delete
From	IP/Domain	Overwrite	avayalab.com	Delete
Record-Route	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	avayalab.com	Delete

Finish

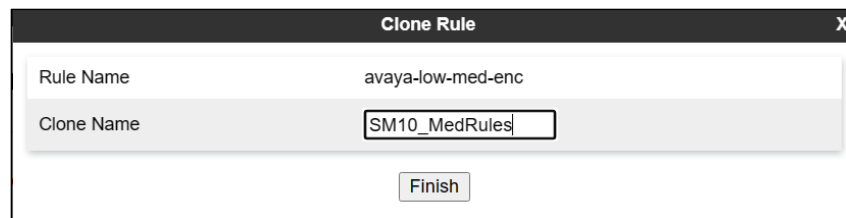
7.11. Media Rules

Media Rules define packet parameters for the RTP media, such as encryption techniques and QoS settings. A media rule for the enterprise (Session Manager) was already existing and re-used in this configuration. This configuration is show here for completeness. A new media rule was created for Fonolo VCB.

7.11.1. SM10– Media Rule

In the sample configuration, the default Media Rule **avaya-low-med-enc** was cloned to create the enterprise Media Rule, and modified as shown below:

- Select **Domain Policies → Media Rules** from the left-hand side menu (not shown).
- From the **Media Rules** menu, select the **avaya-low-med-enc** rule.
- Select **Clone** button, and the **Clone Rule** window will open.
- In the **Clone Name** field enter the new Media Rule name (e.g., **SM10_MedRules**)
- Click **Finish**. The newly created rule will be displayed.



The screenshot shows a 'Clone Rule' dialog box with a dark header bar containing the title 'Clone Rule' and a close button 'X'. The dialog has two input fields: 'Rule Name' with the value 'avaya-low-med-enc' and 'Clone Name' with the value 'SM10_MedRules'. A 'Finish' button is located at the bottom center of the dialog.

- On the **SM10_MedRules** just created, select the **Encryption** tab.
- Click the **Edit** button and the **Media Encryption** window will open.
- In the **Audio Encryption** section, select **RTP** for **Preferred Format #2**.
- In the **Video Encryption** section, select **NONE** for **Preferred Format #2**.
- In the **Miscellaneous** section, select **Capability Negotiation**.
- Click **Finish**.

Media Encryption

Audio Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

RTP

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Video Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

NONE

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2^

Leave blank to match any value.

7.11.2. Fonolo VCB – Media Rule

Repeat the steps in **Section 7.11.1**, with the following changes, to create a Media Rule for Fonolo VCB

1. Clone the **avaya-low-med-enc** profile.
2. In the **Clone Name** field enter the new Media Rule name (e.g., **Fonolo_MedRules**).

The completed **Fonolo_MedRules** media rule is shown on the screen below.

Note: Encrypted RTCP for audio encryption must be selected otherwise the secure calls are rejected by Fonolo Cloud SIP servers.

Media Encryption

Audio Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

RTP

Preferred Format #3

NONE

Encrypted RTCP

☒

MKI

☐

Lifetime

2^

Leave blank to match any value.

Interworking

☒

Symmetric Context Reset

☒

Key Change in New Offer

☐

Video Encryption

Preferred Format #1

SRTP_AES_CM_128_HMAC_SHA1_80

Preferred Format #2

NONE

Preferred Format #3

NONE

Encrypted RTCP

☐

MKI

☐

Lifetime

2^

Leave blank to match any value.

7.12. Endpoint Policy Groups

Endpoint policy groups are set of Domain Policies that will be applied to traffic between Avaya SBC and a connected server. The Endpoint Policy Group is applied to the traffic as part of the Server Flows defined later in **Section 7.13**. A new Endpoint Policy Group was defined for Fonolo VCB, while a Policy Group for the enterprise (SM10) was already existing and re-used in this configuration.

7.12.1. Endpoint Policy Group – Session Manager

The following Policy Group named **SM10_EPG** was already defined in Avaya SBC for the enterprise, using the values shown on the screen below. The Media Rule is the **SM10_MedRules** shown on **Section 7.11.1**.

Device: sbc102 ▾AlarmsIncidentsStatus ▾Logs ▾DiagnosticsUsersSettings ▾Help ▾Log Out

Avaya Session Border Controller

AVAYA

Software Management

Device Management

Backup/Restore

▸ System Parameters

▸ Configuration Profiles

▸ Services

▾ Domain Policies

Application Rules

Border Rules

Media Rules

Security Rules

Signaling Rules

Charging Rules

End Point Policy Groups

Session Policies

Policy Groups: SM10_EPG

Add

RenameCloneDelete

Policy Groups

Click here to add a description.

Click here to add a row description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
0	default-trunk	default	SM10_MedRules	default-low	default	None	Off	Edit

7.12.2. Endpoint Policy Group – Fonolo VCB

To create a new Endpoint Policy Group for Fonolo VCB, navigate to **Domain Policies** → **End Point Policy Groups** in the left pane. In the right pane, select **Add**. Enter a **Group Name** e.g., **Fonolo_EPG**, (not shown) and click **Next** to continue.

On the **Policy Group** window select the following predefined default set of rules on the SBC:

- **Application Rule:** default-trunk.
- **Border Rule:** default.
- **Media Rule:** Fonolo_MedRules as defined in **Section 7.11.2**.
- **Security Rule:** default-low.
- **Signaling Rule:** default.
- **Charging Rule:** None.
- **RTCP Monitoring Report Generation:** Off.
- Select **Finish**.

Edit Policy Set

Application Rule

default-trunk

Border Rule

default

Media Rule

Fonolo_MedRules

Security Rule

default-low

Signaling Rule

default

Charging Rule

None

RTCP Monitoring Report Generation

Off

Finish

The completed Policy Group is shown on the screen below.

Policy Groups: Fonolo_EPG

Add

RenameCloneDelete

Policy Groups

default-low

default-low-enc

default-med

default-med-enc

default-high

default-high-enc

avaya-def-low-enc

avaya-def-high-s...

Click here to add a description.

Click here to add a row description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
0	default-trunk	default	Fonolo_MedRules	default-low	default	None	Off	Edit

7.13. Endpoint Flows – Server Flows

Server Flows combine the interfaces, policies, and profiles defined in the previous sections into inbound and outbound flows. When a packet is received by Avaya SBC, the content of the packet (IP addresses, SIP URIs, etc.) is used to determine which flow it matches, so that the appropriate policies can be applied. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Two flows are involved in every call, the source endpoint flow and the destination endpoint flow.

7.13.1. Server Flows – Session Manager

Select **Network and Flows** → **Endpoint Flows** from the menu on the left-hand side, and select the **Server Flows** tab and click **Add** (not shown). Enter the following parameters:

- **Flow Name:** Enter a descriptive name, e.g., **SM10 Flow to Fonolo VCB**.
- **SIP Server Profile:** Select **SM10** as defined in **Section 7.8.1**.
- **URI Group, Transport, Remote Subnet:** Leave it at default as *.
- **Received Interface:** Select **Public1_Sig1** as defined in **Section 7.6**.
- **Signaling Interface:** Select **Private1_Sig1** as defined in **Section 7.6**.
- **Media Interface:** Select **Private1_Med1** as defined in **Section 7.6**.
- **End Point Policy Group:** Select **SM10_EPG** as defined in **Section 7.12.1**.
- **Routing Profile:** Select **To Fonolo VCB** as defined in **Section 7.9.2**.
- **Topology Hiding Profile:** Select **SM10_TopoHide** as defined in **Section 7.10**.
- Check the **Link Monitoring from Peer** box.
- Let other fields at the default values. Click **Finish**.

Edit Flow: SM10 Flow to Fonolo VCB	
Flow Name	SM10 Flow to Fonolo VCB
SIP Server Profile	SM10
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public1_Sig1
Signaling Interface	Private1_Sig1
Media Interface	Private1_Med1
Secondary Media Interface	None
End Point Policy Group	SM10_EPG
Routing Profile	To Fonolo VCB
Topology Hiding Profile	SM10_TopoHide
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input checked="" type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	
Finish	

7.13.2. Server Flow – Fonolo VCB

The screen below shows the Server Flow for Fonolo VCB created in the reference configuration, with the following parameters:

- **Flow Name:** Enter a descriptive name, e.g., **Fonolo VCB Flow To SM10**.
- **SIP Server Profile:** Select **Fonolo VCB** as defined in **Section 7.8.2**.
- **URI Group, Transport, Remote Subnet:** Leave it at default as *.
- **Received Interface:** Select **Private1_Sig1** as defined in **Section 7.6**.
- **Signaling Interface:** Select **Public1_Sig1** as defined in **Section 7.6**.
- **Media Interface:** Select **Public1_Med1** as defined in **Section 7.6**.
- **End Point Policy Group:** Select **Fonolo_EPG** as defined in **Section 7.12.2**.
- **Routing Profile:** Select **To SM10** as defined in **Section 7.9.1**.
- **Topology Hiding Profile:** Select **default**.
- Check the **Link Monitoring from Peer** box.
- Let other fields at the default values. Click **Finish**.

Edit Flow: Fonolo VCB Flow To SM10	
Flow Name	Fonolo VCB Flow To SM10
SIP Server Profile	Fonolo VCB
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private1_Sig1
Signaling Interface	Public1_Sig1
Media Interface	Public1_Med1
Secondary Media Interface	None
End Point Policy Group	Fonolo_EPG
Routing Profile	To SM10
Topology Hiding Profile	default
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input checked="" type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	
<button>Finish</button>	

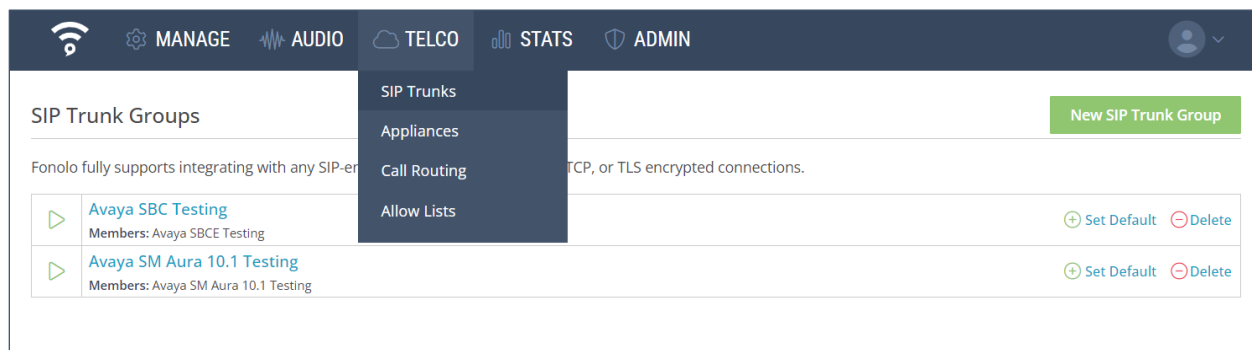
8. Configure Fonolo Voice Call-Backs

This section provides a “snapshot” of Fonolo VCB configuration used during compliance testing. Fonolo VCB is typically configured for customers by Fonolo. The screen shots and partial configuration shown below, supplied by Fonolo, are provided only for reference. These represent only an example of the configuration GUI of VCB, available through the Fonolo Customer Portal at <https://portal.fonolo.com/>. Other configurations are possible. Contact Fonolo for details on how to configure VCB. The configuration operations described in this section can be summarized as follows:

- Add a New SIP Trunk Group,
- Adding the Agent Call-Back Endpoint,
- Adding a New Call-Back Profile,

8.1. Add a New SIP Trunk Group

Navigate to **Telco** → **SIP Trunks** and click the **New SIP Trunk Group** at the top of the page. Define a new label to identify this SIP trunk group. During compliance testing a name **Avaya SBC** was used as the label. Then select **Add New SIP Trunk** (not shown).



Under the **Members** tab in this new SIP trunk group, click the **Add New Member** button (not shown), and the **Add New SIP Trunk** dialog will appear as shown below.

Under **Add New SIP Trunk**:

- **SIP URL:** Enter the public IP address of Avaya SBC formatted as a fully qualified URL, defining the protocol and SIP port. During compliance testing, the protocol **TLS** and port **5061** was used for the SIP service with Avaya SBC.
- **DTMF Mode:** The mode to use for sending DTMF tones. Default is RFC 2833.
- **Identity Header:** Whether to include an identity header (either Remote-Party-ID or P-Asserted-Identity). Default is none.
- **Codec Support:** The list of audio codecs to use. Defaults are μ -law and a-law.
- **Priority:** A numeric value that can be used to determine failover or load balance groups when more than one SIP trunk group member is defined. Members with lower priority values are used first; members with equal priority values are load balanced.

- **Keepalive:** This instructs the Fonolo VCB to perform regular keep-alive using SIP OPTIONS requests, based on the number of seconds defined.
- **Session Timers:** If Fonolo VCB should enable SIP Session Timers (RFC 4028).
- **NAT Support:** If the SIP trunk group member specified is located behind a NAT (Network Address Translation) device. Fonolo can compensate for the un-reachable RTP data specified in the SDP body of the INVITE request, using symmetric RTP.

Click **Save Trunk** button to save the changes.

Update SIP Trunk

SIP Trunk SID:

TM3b945867a5b0a8a222926da8a9906255

SIP Label:

Avaya SBC Public Interface

Only visible through this interface.

SIP URL:

tls://10.207.80.107:5061

SIP URL to connect to this SIP trunk member.

SIP URLs should use IP addresses or hostnames, and include a protocol (udp, tcp, or tls), and a port value. For example: udp://10.10.10.10:5060

DTMF Mode:

RFC 2833 (Recommended)

How we send/receive DTMF tones with this host.

Identity Header:

None

If we should add an additional SIP identity header.

From Domain:

☐

Use a custom From domain on this SIP Trunk member.

Codec Support:

☒ μ -law ☒ a-law

Priority:

10

Lower priority trunks are used first. Equal priority trunks are load balanced.

Keepalive:

☒ Enable a keepalive timer on this host. (SIP OPTIONS)

Session Timers:

☒ Enable SIP Session Timers (RFC 4028) on this host.

NAT Support:

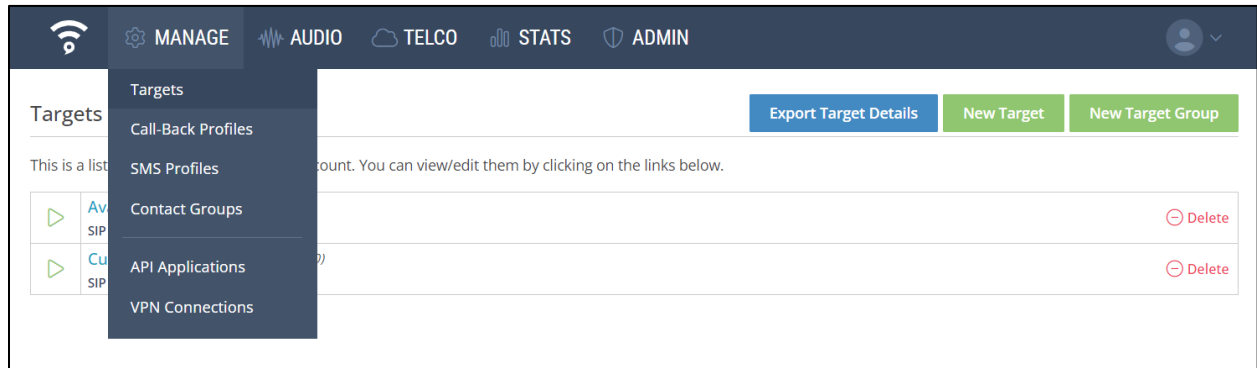
☐ This host is behind a NAT device.

Save Trunk

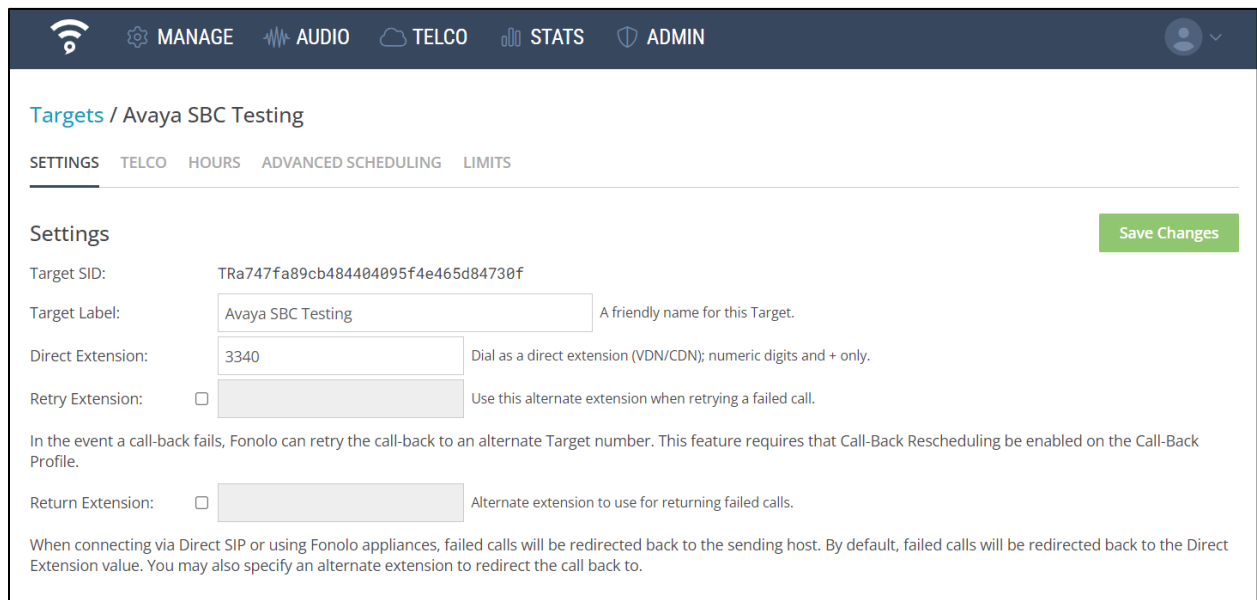
Cancel

8.2. Adding the Voice Call-Back Endpoint


Navigate to **Manage** → **Targets** and click the **New Target** button. Define a new label to identify this new Target. During compliance testing **Avaya SBC Testing** was used as the **Target Label**. Select the **Dial as SIP Extension** option (shown below) for **Dial Method** and enter a call center VDN number to reach the pertinent skillset via Session Manager in the **Extension** field.



During compliance testing, VDN **3340** was pre-configured on Communication Manager which was accessible via Session Manager. Then click on the **Save Changes** button to save the changes.



From the **Telco Settings** section of the newly added Target, select the SIP trunk to use for this Target, from the **Direct SIP** drop down menu shown below. Select the **Avaya SBC Testing** SIP trunk, added in **Section 8.1**, and then click the **Save Changes** button.



MANAGEAUDIOTELCOSTATSADMIN

Targets / Avaya SBC Testing

SETTINGSTELCOHOURSADVANCED SCHEDULINGLIMITS

Telco Settings

Save Changes

This controls how Fonolo will call in to your phone system.

Direct SIP:

Avaya SBC Testing

Use this SIP Trunk.


Dial Timeout:

60

How long to wait for the Target to answer before returning "Target Call Timeout". 10 to 120 secs.

8.3. Adding a New Call-Back Profile

Navigate to **Manage → Call-Back Profiles** and click on the **New Call-Backs Profile** button as shown below.



MANAGEAUDIOTELCOSTATSADMIN

Call-Back

Export Call OptionsNew Call-Back Profile

This is a list of Call-Back Profiles. You can edit/view them by clicking on the links below.

▶ Avaya SBC Testing

Channel Voice Call-Backs, Language English

Call OptionsArchive

▶ Avaya SBC Testing

Channel Voice Call-Backs, Language English

PreviewJavaScript CodeArchive

▶ Avaya SBC Testing

Channel Voice Call-Backs, Language English

PreviewJavaScript CodeArchive

▶ Avaya SBC Testing

Channel Voice Call-Backs, Language English

Call OptionsArchive

Archived Profiles

Archived Profiles are kept for statistical purposes. Once deleted, all data for these Profiles will be permanently removed.

Enter values for the new profile:

- **Profile Label:**
- **Geo Allow List:**
- **Channel:**
- **Language:**
- **Client CID Number:**

Enter a profile name, e.g., Avaya SBC Testing.

The Default Allow List is selected.

Select Voice Call-Backs.

Select the appropriate language for this profile.

The Caller-ID number the customer will see.

KP; Reviewed:
SPOC 1/4/2024

Avaya DevConnect Application Notes
©2024 Avaya Inc. All Rights Reserved

62 of 69
FonoloVCB-SBC10

- **Client CID Name:** The Caller-ID name the customer will see.
- **Agent CID Number:** The Caller-ID number the agent will see.
- **Agent CID Name:** The Caller-ID name the agent will see.

Click the **Add Call-Back Profile** button to save this new profile.

Call-Back Profiles / Avaya SBC Testing Cancel Add Call-Back Profile

Settings

Profile Label: A friendly name for this profile.

Geo. Allow List: This is the geographic allow list to use with this call-back profile.

Channel: This is the channel type (Voice, Web, or Programmable)

Language: The language used for this channel.

Caller ID Settings

You can adjust the caller ID name and number, seen by both your clients and agents.

Client CID Number: Caller ID number seen by clients.

Client CID Name: Caller ID name seen by clients (only supported by some systems).

Agent CID Number: Caller ID number seen by your agents.

Agent CID Name: Caller ID name seen by your agents (only supported by some systems).

From the **Options** section of the new **Call-Back Profile**, select the Target added in **Section Error! Reference source not found.**, and click the **Add Option** button to add the call options to this profile, as shown below, then click the **Save Changes** (not shown). This associates the Target VDN with this new **Call-Back Profile**. Multiple call options can be associated with a single **Call-Back Profile**, one for each skill call-backs are being offered on.

Call-Back Profiles / Avaya SBC Testing

SETTINGS **OPTIONS** TELCO FEATURES RETRIES SCHEDULED QUESTIONS

Call Options

Add Call-Back options to your Call-Back Profile with the Add Option button below.

Add Option

☐ **Avaya SBCE Testing**
Target Extension: 3340, Fonolo Extension: 78000 Move Edit Delete

From the **Telco Settings** section of the new **Call-Back Profile**, select the **Avaya SBC SIP** trunk group created in **Section 8.1** as the **Direct SIP** value under both the **Client Call-Back Method** and the **Voice Call-Backs Transfers** section, as shown below, then click the **Save Changes** button.

Call-Back Profiles / Avaya SBC Testing

SETTINGS OPTIONS TELCO FEATURES RETRIES SCHEDULED QUESTIONS

Client Call-Back Method

Test Phone Number Save Changes

This controls how Fonolo will call your clients back.

Direct PSTN:

☐ No PSTN Groups defined. Please contact Fonolo Support.

Direct SIP:

☒ Avaya SBC Testing

▼

Using this SIP Trunk Group.

Call Routing:

Avaya SM

▼

Select how calls for this SIP trunk group are routed for this profile.

Dial Timeout:

90

How long to wait for the Client to answer before returning "Client Call Timeout". 10 to 120 secs.

Voice Call-Back Transfers

This controls how calls will be transferred from your system to Fonolo.

Direct PSTN:

☐ You will transfer calls to Fonolo assigned DIDs over the PSTN.

Direct SIP:

☒ Avaya SBC Testing

▼

Calls will be transferred to Fonolo from this SIP Trunk Group.

Failed Transfers:

☒ Redirect calls (SIP REFER) back to the sender host in the event of a failure.

Validation:

Validate as a Phone Number

▼

Select how to validate client call-back numbers.

Default Dialing Area:

(+1) United States, Canada, & Island Nations

▼

Call-back numbers are limited to this country code.

Regex:

PERL Compatible Regular Expression (PCRE), e.g: ^{0-9}{3,5}\$

Navigate to **Manage → Call-Back Profiles** and click on the **Call Options** link on the newly created **Call-Back Profile** (not shown). The **ICR Settings** dialog will appear (shown below) and include the inbound extensions to use for VDN. These are the extensions to transfer calls to, on the Fonolo VCB, when a call opts-in for a call-back. During compliance testing, the extension **78000** is configured for the Fonolo VCB.

MAN

Call-Back Profiles

This is a list of your Call-Back Profiles

▶ Avaya SBCE Te

Channel Web Call-Back

▶ Avaya SBC Tes

Channel Voice Call-Back

▶ Test VIVR Widg

Channel Web Call-Back

▶ Voice CallBack

Channel Voice Call-Backs, Language English

ICR Settings

For each call option, transfer calls to the given extension:

Avaya SBC Testing

78000

Close

New Call-Back Profile

Script Code

Archive

Call Options

Archive

Script Code

Archive

Call Options

Archive

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, Avaya SBC and Fonolo VCB.

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the SIP signaling group by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section Error! Reference source not found.5**. Verify that the signaling group is **in-service** as indicated in the **Group State** field shown below.

```
status signaling-group 1

                                STATUS SIGNALING GROUP

Group ID: 1
Group Type: sip

Group State: in-service
```

Verify the status of the local SIP trunk group by using the “status trunk n” command, where “n” is the trunk group number administered in **Section 5.6**. 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
0001/0001 T000001 in-service/idle no
0001/0002 T000002 in-service/idle no
0001/0003 T000003 in-service/idle no
0001/0004 T000004 in-service/idle no
0001/0005 T000005 in-service/idle no
0001/0006 T000006 in-service/idle no
```

The following tests were also performed to verify proper configuration of Fonolo VCB:

1. PSTN user places a call to ACD queue of call center in Communication Manager.
2. If there is no available agent, PSTN caller is given options whether continue staying in the queue or pressing number #1 to have a call-back.
3. PSTN user decides to have a call-back and press #1. The call is now routed to Fonolo VCB through Avaya SBC. The Fonolo VCB confirms a call-back number with PSTN user and schedule a voice call-back for PSTN user.
4. Fonolo VCB calls the ACD queue to connect to an available agent, as soon as the agent answers the ACD call, it asks the agent to press #1 to connect to the PSTN user.
5. If the agent is ready to connect to PSTN user, they press #1. Fonolo VCB is calling to PSTN user and connect the agent to PSTN user.

9.2. Verify Avaya Aura® Session Manager

Navigate to **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring** and select the Communication Manager SIP Entity. Verify the **Link Status** is **Up**.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with options: Session Manager, Dashboard, Session Manager A..., Global Settings, Communication Profi..., Network Configura..., Device and Locatio..., Application Config..., System Status, Load Factor, and SIP Entity Monit... (highlighted in blue). The main content area is titled "SIP Entity, Entity Link Connection Status" and includes a sub-header "All Entity Links to SIP Entity: CM10-Public". Below this, there is a "Summary View" button and a table with 10 columns: Session Manager Name, Session Manager IP Address Family, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The table contains one row for "SM10" with values: IPv4, 10.33.1.43, 5063, TLS, FALSE, UP, 200 OK, and UP. A "Filter: Enable" button is visible in the top right of the table area.

Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
SM10	IPv4	10.33.1.43	5063	TLS	FALSE	UP	200 OK	UP



Repeat the same procedure selecting Avaya SBC SIP Entity and verify the **Link Status** is **Up**.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with options: Session Manager, Dashboard, Session Manager A..., Global Settings, Communication Profi..., Network Configura..., Device and Locatio..., Application Config..., System Status, Load Factor, and SIP Entity Monit... (highlighted in blue). The main content area is titled "SIP Entity, Entity Link Connection Status" and includes a sub-header "All Entity Links to SIP Entity: SBC-SP1". Below this, there is a "Summary View" button and a table with 10 columns: Session Manager Name, Session Manager IP Address Family, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The table contains one row for "SM10" with values: IPv4, 10.33.1.51, 5061, TLS, FALSE, UP, 200 OK, and UP. A "Filter: Enable" button is visible in the top right of the table area.


Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
SM10	IPv4	10.33.1.51	5061	TLS	FALSE	UP	200 OK	UP

9.3. Verify Fonolo Voice Call Back


To verify the voice call-backs, log in to the Fonolo portal with appropriate credential and navigate to **STATS → Call Details**. The **Call-Back Details** window displays list of the call-back with detail information as shown below.




MANAGE




AUDIO




TELCO



STATS




ADMIN



Call-Back Details

From: Nov 7th, 2023 to Nov 21st, 2023For: All Call-Back Profiles

Export Results



Total of 18 Calls

Date	Time	Option	Client	Deep Dial	Hold Time	CC Time	Talk Time	Duration	Debug Recording	Status	Clearing	Ended By	Retry
2023-11-20	12:56:42	Avaya SBC Testing	16139674305	00:00	01:43	00:09	04:12	06:04	--	Success	Normal Clearing	Client	--
2023-11-18	04:09:55	Avaya SBC Testing	16139674305	00:00	01:52	00:06	77:34	79:32	--	Success	Normal Clearing	Company	--
2023-11-15	13:00:54	Avaya SBC Testing	16139674305	00:00	00:21	00:03	31:20	31:44	--	Success	Normal Clearing	Client	--
2023-11-14	13:13:23	Avaya SBC Testing	16139674305	00:00	01:40	00:09	06:24	08:13	--	Success	Normal Clearing	Company	--
2023-11-14	13:05:53	Avaya SBC Testing	16139674305	00:00	02:19	00:07	04:51	07:21	--	Success	Normal Clearing	Client	Agent
2023-11-14	11:27:08	Avaya SBC Testing	16139674305	00:00	02:07	00:08	01:09	03:24	--	Success	Normal Clearing	Company	--
2023-11-10	12:05:50	Avaya SBCE Testing	16139674305	00:00	00:45	00:07	00:26	01:18	--	Success	Normal Clearing	Company	--
2023-11-10	12:04:35	Avaya SBCE Testing	16139674305	00:00	01:09	00:00	00:00	01:09	--	Failed	Agent Did Not Accept	Company	Auto
2023-11-10	12:03:20	Avaya SBCE Testing	16139674305	00:00	01:08	00:00	00:00	01:08	--	Failed	Agent Did Not Accept	Company	Auto
2023-11-09	10:50:34	Avaya SBCE Testing	16139674300	00:00	00:29	00:34	30:17	31:19	--	Success	Normal Clearing	Company	--
2023-11-09	10:49:34	Avaya SBCE Testing	16139674300	00:00	00:38	00:00	00:00	00:38	--	Failed	Agent Did Not Accept	Company	Client
2023-11-09	10:48:37	Avaya SBCE Testing	16139674300	00:00	00:46	00:00	00:00	00:46	--	Failed	Agent Did Not Accept	Company	Auto
2023-11-09	10:48:04	Avaya SBCE Testing	16139674300	00:00	00:28	00:00	00:00	00:28	--	Failed	Agent Did Not Accept	Company	Auto
2023-11-09	10:09:19	Avaya SBCE Testing	16139674305	00:00	00:46	00:04	01:59	02:48	--	Success	Normal Clearing	Company	--
2023-11-09	09:36:34	Avaya SBCE Testing	16139674305	00:00	01:08	00:05	31:29	32:47	--	Success	Normal Clearing	Client	Agent

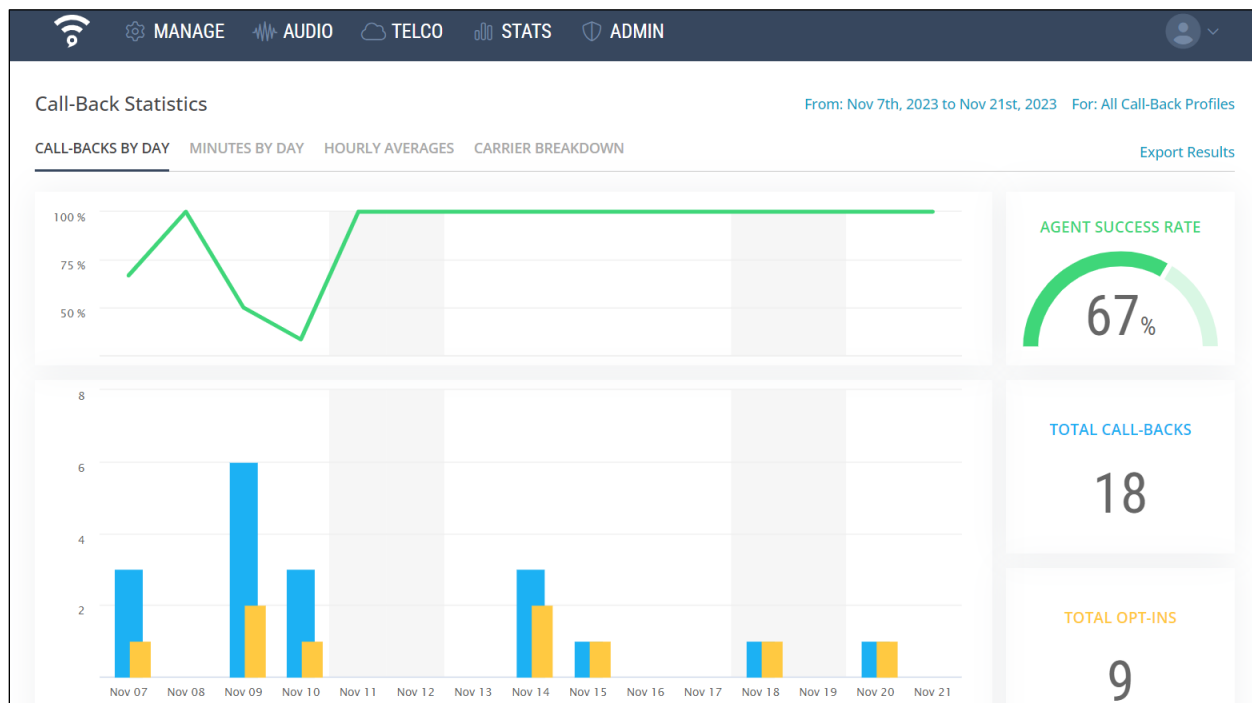
Search...

Showing 1 to 18 of 18

20 Per Page

< 1 >

The **Call-Back Statistics** is also provided in the **Graph** section of the **STATS** menu.



10. Conclusion

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs Version 3.9 using Fonolo Cloud SIP Connect to successfully interoperate with Avaya Session Border Controller Release 10.1 and Avaya Aura® Release 10.1. All feature and serviceability test cases were completed and passed.

11. Additional References

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

Avaya product documentation, including the following, is available at <http://support.avaya.com>

1. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, June 2023.
2. *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 12, September 2023.
3. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023
4. *Administering Avaya Session Border Controller*, Release 10.1.x, Issue 5, October 2023.

Fonolo provides their documentation upon delivery of their products/services.

©2024 Avaya LLC. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.