



## **Application Notes for Fonolo Voice Call-Backs Version 3.3 with Avaya Aura® Communication Manager Release 10.1 and Avaya Aura® Session Manager Release 10.1 using SIP Trunks – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs application to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks.

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

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

# 1. Introduction

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs (Fonolo VCB) to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using SIP trunks. Fonolo VCB provides functionality to replace hold time with a call back. During this compliance testing, Fonolo VCB was hosted in the cloud by Fonolo. The solution communicates via SIP/RTP. The Fonolo VCB functionality was compliance tested utilizing SIP trunks to Session Manager. The configuration allowed Communication Manager to use SIP trunking for calls to and from the VCB application. The Fonolo VCB is a call center solution where instead of a caller staying in the queue when agents are all busy, caller can request to get a call back when an agent becomes available.

When a caller encounters a scenario where no agents are available in a call center environment, and Communication Manager is part of that 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 a Session Manager SIP trunk 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 a SIP trunk with Session Manager 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 prompts if the agent would like to get connected to the caller. If the agent accepts to connect to the caller, Fonolo VCB then calls the caller via a SIP trunk to Communication Manager and connects the caller with the available agent. When Fonolo VCB makes an outbound call to the caller and agent via Session Manager, it makes two SIP INVITE requests, one to the available agent and one to the caller, and then mixes the audio within the Fonolo VCB server.

For security purposes public and lab IP addresses have been altered in this document.

## 2. General Test Approach and Test Results

The interoperability compliance testing focused on verifying inbound and outbound call flows between Communication Manager, Session Manager and Fonolo VCB. The feature test cases were performed manually. Calls were placed manually from users on the PSTN to a call center Vector Directory Number (VDN). During compliance testing, Call Center Elite within Communication Manager was used. An assumption was made during compliance testing in the vector script to direct callers to Fonolo VCB when no agents are available. When a caller is connected with Fonolo VCB, Fonolo VCB reads the call back number of the caller or asks the caller to input a new call back number. Fonolo VCB recognized the Dual Tone Multi Frequency (DTMF) input provided by the caller confirming the call back number. For compliance testing purposes, agents were made available after the above call between the caller and Fonolo VCB is completed. Fonolo VCB then called into the call center VDN and connected with an available agent. Fonolo VCB provided a recording, informing the agent of a call in waiting, and checked if the agent wanted to get connected to the PSTN caller. The agent can accept the call by using DTMF input. Fonolo VCB then made the second outbound call to the PSTN caller via

Communication Manager and if the PSTN caller answered the call they then get connected with the agent.

The serviceability test cases were performed manually by disconnecting and reconnecting the SIP trunk connection to Fonolo VCB.

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

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and Fonolo did not include use of any specific encryption features as requested by Fonolo.

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 application is hosted in a cloud environment by Fonolo and the VCB application was installed and synchronized with the Fonolo on-premises appliances residing in customer's side. SIP trunks were used to connect the VCB application with Communication Manager via Session Manager. The following features and functionality were covered during compliance testing:

- Establishment of SIP trunk connectivity between Fonolo VCB and Session Manager including session refresh.
- Testing of G.711MU codec.
- Incoming calls to a VDN of Communication Manager call center can be redirected to the VCB application via the SIP trunk based on vector scripting. Outgoing calls from the VCB appliance to the VDN via Session Manager when callers decide on call back. During this compliance testing, Call Center of Communication Manager was used and is not the scope of these Application Notes.
- The VCB application can make an outbound call to the caller via Communication Manager who had selected the call back option and merge the call between the caller and available agent. The outbound call is made from Communication Manager via Session Manager and uses SIP INVITE.
- DTMF transmission to ensure that options selected by the caller and agent is accepted correctly by Fonolo VCB.
- User-to-User Information (UUI) is sent from Communication Manager to the VCB application and that the same information is sent back to the agent from the VCB application.

Serviceability testing focused on verifying the ability of Fonolo VCB to recover from adverse conditions, such as the SIP trunk going down (using 'busyout' command) and reboot of Session Manager.

## 2.2. Test Results

All test cases were executed and passed with the following exceptions/observations:

- Fonolo VCB only supports G.711Mu codec.
- During this compliance testing, for testing of Direct IP-IP Media (shuffling), it was ensured that Avaya Deskphones were configured such that the VCB application in the on-premises application can contact them for RTP stream.

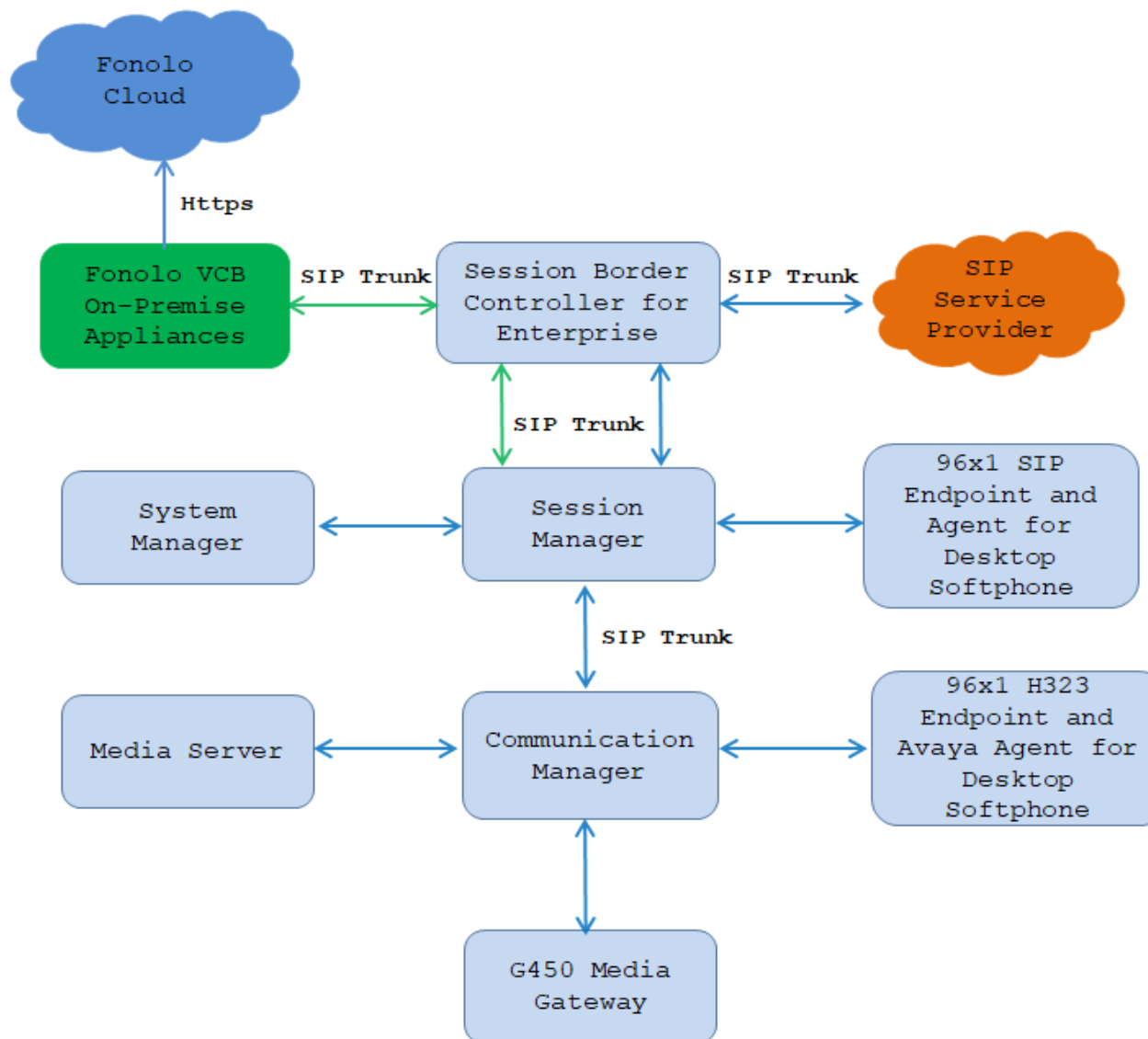
## 2.3. Support

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](mailto:support@fonolo.com).

### 3. Reference Configuration

A simulated enterprise site consisting of Communication Manager, Session Manager and System Manager were used during compliance testing. As shown in **Figure 1**, SIP trunks were used to connect two Fonolo VCB on-premises appliances with Communication Manager via Session Manager. The configuration of Fonolo VCB was done from their cloud and was synched with the Fonolo on-premises appliances via https. Avaya Session Border Controller for Enterprise was used to provide SIP connection to SIP Service Provider for external call to PSTN. A skill set queue is configured on Communication Manager with two agents belonging to this queue. The configuration allowed the enterprise site to use SIP trunking for calls to and from Fonolo VCB via the Session Manager.



**Figure 1: Reference Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtual server	R020x.01.0.974.0 (10.1.0.2.0.974.27607)
Avaya Aura® Media Server running on virtual server	8.0.2.218
Avaya G450 Media Gateway	42.08
Avaya Aura® System Manager running on virtual server	10.1.0.2 SP2 Software Update Revision No: 10.1.0.2.0715160 Hot Fix - 1010215160
Avaya Aura® Session Manager running on virtual server	10.1.0.2.1010215
Avaya IP Deskphones - 9641GS (H.323) - 9611G (SIP)	6.853 7.1.9.0.8
Avaya Digital 9408 Deskphone	R20
Fonolo Voice Call-Backs On-premises Appliance	Version 3.3

## 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.

The administration of the routing and basic connectivity between Communication Manager and Session Manager or the setting up of skill set, hunt group, vectors for a call center type environment on the Communication Manager are not the focus of these Application Notes; however, some details are provided only for informational purposes and completeness.

### 5.1. Verify Communication Manager License

Log into 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		20	
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		1	
Maximum Video Capable IP Softphones: 18000		12	
<b>Maximum Administered SIP Trunks: 40000</b>		<b>64</b>	
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 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 **10.33.1.42** 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                          10.33.1.44
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. As per the observation noted in **Section Error! Reference source not found.** only configure **G.711MU**. The codec shown below was used in the compliance testing.

```
change ip-codec-set 1
Page 1 of 2
                                IP MEDIA PARAMETERS
      Codec Set: 1
      Audio          Silence   Frames   Packet
      Codec          Suppression Per Pkt   Size (ms)
1: G.711MU          n         2         20
2:                   n         2         20
3:
      Media Encryption          Encrypted SRTCP: best-effort
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 1		Page 1 of 20
IP NETWORK REGION		
Region: 1	NR Group: 1	
Location: 1	<b>Authoritative Domain: avayalab.com</b>	
Name: Loc-1	Stub Network Region: n	
MEDIA PARAMETERS	<b>Intra-region IP-IP Direct Audio: yes</b>	
<b>Codec Set: 1</b>	<b>Inter-region IP-IP Direct Audio: yes</b>	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

## 5.5. Administer SIP Signaling Group

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

- **Group Type:** Set it as “sip”,
- **Transport Method:** Set is as “tls”.
- **Near-end Node Name:** Enter the “procr” interface of Communication Manager.
- **Far-end Node Name:** Enter the node name for Session Manager.
- **Near-end Listen Port:** Enter the TLS port for the SIP trunk to Session Manager.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** 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 1                                     Page 1 of 2
                                SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
Q-SIP? n
IP Video? n                      Enforce SIPS URI for SRTP? n
Peer Detection Enabled? 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: SM10
Near-end Listen Port: 5061                      Far-end Listen Port: 5061
                                                Far-end Network Region: 1

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 “tie”.
- **Signaling Group:** Enter the signaling group that has been created in **Section 5.5**.
- **Number of Members:** Enter a number of SIP trunk member, in this case 10 was used.

```

add trunk-group 1                                     Page 1 of 5
                                TRUNK GROUP

Group Number: 1                      Group Type: sip                      CDR Reports: y
Group Name: Private Trunk                      COR: 1                      TN: 1                      TAC: #01
Direction: two-way                      Outgoing Display? n
Dial Access? n                      Night Service:
Queue Length: 0
Service Type: tie                      Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 1
                                                Number of Members: 10

```

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

add trunk-group 3	Page 3 of 4
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	<b>Numbering Format: private</b>
	UI Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	

Navigate to **Page 5** and enter “y” for the **Convert 180 to 183 for Early Media?** field as shown below.

add 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? n	
Telephone Event Payload Type: 101	
	<b>Convert 180 to 183 for Early Media? y</b>
Always Use re-INVITE for Display Updates? n	
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 Private Numbering

Use the “change private-numbering 0” command, to define the calling party number to send to Fonolo VCB. Add an entry for the trunk group defined in **Section 5.6**. In the example shown below, all calls originating from a 4-digit extension beginning with **33** and routed to trunk group **1** will result in a 4-digit calling number. The calling party number will be in the SIP “From” header.

change private-numbering 0					Page	1 of	2
NUMBERING - PRIVATE FORMAT							
Ext	Ext	Trk	Private	Total			
Len	Code	Grp(s)	Prefix	Len			
<b>4</b>	<b>33</b>	<b>1</b>		4	Total Administered: 15		
<b>4</b>	<b>34</b>	<b>1</b>		<b>4</b>	Maximum Entries: 540		

## 5.8. 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										Page	1 of	12
DIAL PLAN ANALYSIS TABLE												
Location: all												
Percent Full: 5												
	Dialed	Total	Call		Dialed	Total	Call		Dialed	Total	Call	
	String	Length	Type		String	Length	Type		String	Length	Type	
0		3	fac		33	4	ext		#		3	dac
1		4	ext		34	4	ext					
1		11	udp		45	4	aar					
<b>78</b>		<b>5</b>	<b>udp</b>		46	4	aar					

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

## 5.10. 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 “1”. 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.
- **Numbering Format:** Set to “lev0-pvt” which is private numbering plan.

change route-pattern 1

Page 1 of 4

Pattern Number: 1

Pattern Name: SIP-TLS-To-SM

SCCAN? n

Secure SIP? n

Used for SIP stations? n

Grp No	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC
			Mrk	Lmt	List	Del	Digits	QSIG
							Dgts	Intw
1:	1	0						n user
2:								n user
3:								n user
4:								n user
5:								n user
6:								n user

BCC	VALUE	TSC	CA-TSC	ITC	BCIE	Service/Feature	PARM	Sub	Numbering	LAR
0	1	2	M	4	W	Request		Dgts	Format	
1:	y	y	y	y	y	n	n		lev0-pvt	next
2:	y	y	y	y	y	n	n			none
3:	y	y	y	y	y	n	n			none
4:	y	y	y	y	y	n	n			none
5:	y	y	y	y	y	n	n			none
6:	y	y	y	y	y	n	n			none

## 5.11. 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 010**.

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

## 5.12. Administer Agent Login ID

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

add agent-loginID 1000		Page 1 of 2
AGENT LOGINID		
Login ID: 1000	AAS? n	
Name: Agent 1000	AUDIX? n	
TN: 1		
COR: 1		
Coverage Path:	LWC Reception: spe	
Security Code: 1234	LWC 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)? system	ACW Agent Considered Idle: system	
Aux Work Reason Code Type: system		
Logout Reason Code Type: system		
Maximum time agent in ACW before logout (sec): system		
Forced Agent Logout Time: :		
WARNING: Agent must log in again before changes take effect		

On **Page 2** 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		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill:	Service Objective? n	
Call Handling Preference: skill-level	Local Call Preference? n	
SN	RL	SL
1: 1		1
2:		16:
3:		17:
4:		18:
5:		19:
6:		20:
7:		
8:		
9:		
10:		
11:		
12:		
13:		
14:		
15:		

## 5.13. 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 5.12**.

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:			

## 5.14. Administer Vector

Use the command “change vector n” where “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” or stay in the queue if all agents are busy. If caller presses “1”, then the call is routed to “78000”, which is the number to dial out to VCB. Also, 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	Lock? n			
Basic? y	EAS? y	G3V4 Enhanced? y	ANI/II-Digits? y	ASAI Routing? y		
Prompting? y	LAI? y	G3V4 Adv Route? y	CINFO? y	BSR? y	Holidays? y	
Variables? y	3.0 Enhanced? y					
01 wait-time	5	secs hearing	1104	then silence		
02 goto step	11	if staffed-agents in skill 1			= 0	
03 goto step	7	if expected-wait for skill 1			pri m >= 10	
04 queue-to	skill 1	pri m				
05						
06						
07 collect	1	digits after announcement	1107	for none		
08 set	A	= digits	CATR	0123456789		
09 route-to	number 78000	cov n if digit			= 1	
10 goto step	4	if unconditionally				
11 disconnect	after announcement none					
12 stop						



## 5.15. Administer VDN

Use the “add vdn n” command to add a VDN number. In the **Destination** field, enter **Vector Number 1** as configured in **Section 5.14** above and keep other fields at their default values.

add vdn 3340	Page 1 of 3
VECTOR DIRECTORY NUMBER	
<b>Extension: 3340</b>	
Name*: Contact Center 1	
<b>Destination: Vector Number 12</b>	
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.

### 6.1. Launch System Manager

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

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

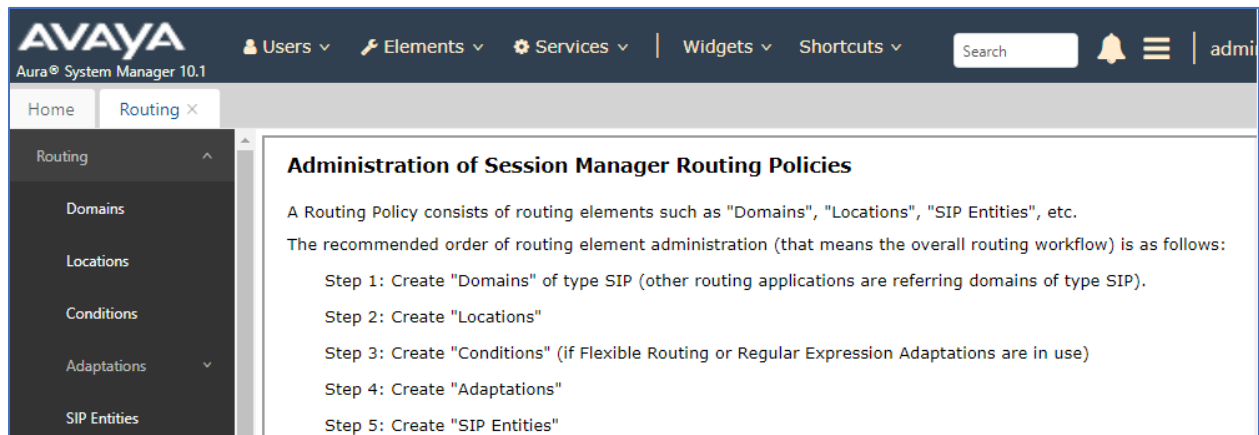
User ID:

Password:

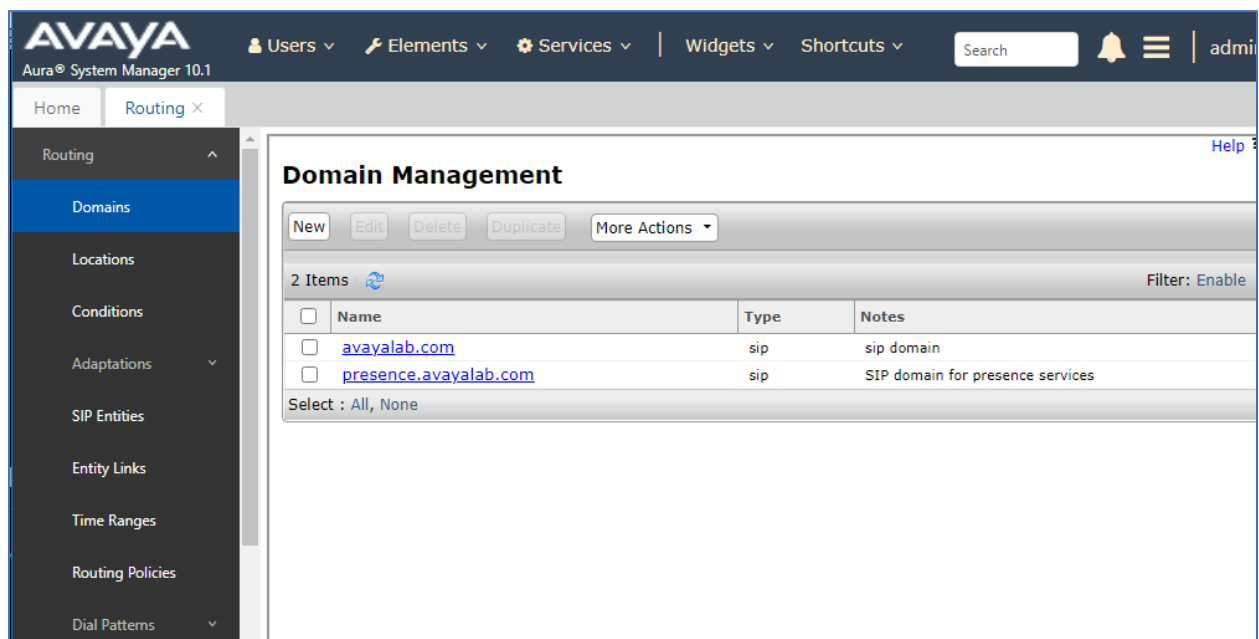
**Supported Browsers:** Internet Explorer 11.x or Firefox 58.0, 59.0 or 60.0.

## 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



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**.



### 6.3. Administer Locations

Select **Routing** → **Locations** from the left pane and click **New** in the subsequent screen (not shown) to add a new location for VCB.

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

**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 ▾

**Location Details** Commit Cancel Help ?

**General**

\* **Name:** Others

**Notes:** For the third party application

**Dial Plan Transparency in Survivable Mode**

**Enabled:** ☐

**Listed Directory Number:**

**Associated CM SIP Entity:**

**Overall Managed Bandwidth**

**Managed Bandwidth Units:** Kbit/sec ▾

**Total Bandwidth:**

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

**Location Pattern**

Add Remove

2 Items 🔍 Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.33.1.187	Fonolo VCB Appliance 1
<input type="checkbox"/>	* 10.33.1.188	Fonolo VCB Appliance 2

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 Fonolo VCB appliances.

### 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**.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, "Aura® System Manager 10.1", and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled "admin" are also present. The left sidebar shows a menu with options: Home, Routing (selected), Domains, Locations, Conditions, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, and Regular Expressions. The main content area is titled "SIP Entity Details" and contains two sections: "General" and "Monitoring". In the "General" section, the "Name" is "SM10", the "IP Address" is "10.33.1.42", the "SIP FQDN" is empty, the "Type" is "Session Manager", and the "Notes" field is empty. The "Location" is "Session Manager", the "Outbound Proxy" is empty, the "Time Zone" is "America/Denver", the "Minimum TLS Version" is "Use Global Setting", and the "Credential name" is empty. In the "Monitoring" section, both "SIP Link Monitoring" and "CRLF Keep Alive Monitoring" are set to "Use Session Manager Configuration". "Commit" and "Cancel" buttons are located at the top right of the form.

SIP Entity Details	
<b>General</b>	
* Name:	SM10
* IP Address:	10.33.1.42
SIP FQDN:	
Type:	Session Manager
Notes:	
Location:	Session Manager
Outbound Proxy:	
Time Zone:	America/Denver
Minimum TLS Version:	Use Global Setting
Credential name:	
<b>Monitoring</b>	
SIP Link Monitoring:	Use Session Manager Configuration
CRLF Keep Alive Monitoring:	Use Session Manager Configuration

The ports need to be defined in Session Manager for other endpoints to connect to, scroll down to the **Listen Ports** section of the **SIP Entity Details** screen. Note that this section is only present for the **Session Manager** SIP Entity.

In the **Listen Ports** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which Session Manager listens for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain.

The compliance test used port **5060** for **UDP** and **5061** for **TLS** for connecting to the Fonolo appliance and Communication Manager.

**Listen Ports**

Add Remove

6 Items
Filter: Enable

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP ▼	bvwdev.com ▼	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP ▼	bvwdev.com ▼	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS ▼	bvwdev.com ▼	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5062	TLS ▼	bvwdev.com ▼	<input type="checkbox"/>	
<input type="checkbox"/>	5067	TLS ▼	bvwdev.com ▼	<input type="checkbox"/>	
<input type="checkbox"/>	5080	TCP ▼	bvwdev.com ▼	<input type="checkbox"/>	

Select : All, None

### 6.4.2. SIP Entity for Fonolo Voice Call-Backs

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

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 Fonolo VCB appliance
- **Type:** Set is as “Other”.
- **Notes:** Enter desired notes.
- **Location:** Select the VCB location name from **Section 0**.
- **Time Zone:** Select the applicable time zone.
- **SIP Link Monitoring:** Select “Link Monitoring Enabled” (not shown).

The screenshot shows the AVAYA Aura System Manager 10.1 interface. The left sidebar contains a navigation menu with the following items: Home, Routing, Domains, Locations, Conditions, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, and Dial Patterns. The main content area displays the 'SIP Entity Details' screen. The title bar of the screen shows 'SIP Entity Details' and 'General'. The form contains the following fields and values:

- Name:** Fonolo1
- FQDN or IP Address:** 10.33.1.187
- Type:** SIP Trunk
- Notes:** SIP trunk to Fonolo VCB Appliance1
- Location:** Others
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** egress

At the top right of the form, there are 'Commit' and 'Cancel' buttons. A 'Help ?' link is also 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:** Enter a descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “SM10”.
- **Protocol:** Set it as “UDP”.
- **Port:** Set it as “5060”.
- **SIP Entity 2:** The VCB entity name from this section.
- **Port:** Set it as “5060”.
- **Connection Policy:** Select “trusted”.

Note that only **UDP** protocol was tested.

**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	Connect Policy
<input type="checkbox"/>	* SM10_Fonolo1_5060_UDI	SM10	UDP	* 5060	Fonolo1	* 5060	trusted

Select : All, None

**SIP Responses to an OPTIONS Request**  

Add Remove

0 Items

Filter: Enable

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

Commit Cancel

Repeat the procedure above to add another SIP entity for VCB, during the compliance testing two Fonolo appliances were used for outgoing and incoming calls between Communication Manager and Fonolo appliances.

**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

**SIP Entity Details**  
General

Commit Cancel

\* Name: Fonolo2

\* FQDN or IP Address: 10.33.1.188

Type: SIP Trunk

Notes: SIP trunk to Fonolo VCB Appliance 2

Location: Others

Time Zone: America/Denver

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐

Call Detail Recording: egress



The screen below shows the entity link for the Fonolo VCB appliance server 2.

**Entity Links**

Override Port & Transport with DNS SRV: ☐

Add Remove

1 Item Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port
<input type="checkbox"/>	* SM10_Fonolo2_5060_UDI	SM10	UDP	* 5060	Fonolo2	* 5060

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 the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

**AVAYA** Aura® System Manager 10.1

Users Elements Services Widgets Shortcuts Search admin

Home Routing

**SIP Entity Details** Commit Cancel Help ?

**General**

\* Name: CM10

\* FQDN or IP Address: 10.33.1.43

Type: CM

Notes:

Location: Communication Manager

Time Zone: America/Denver

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: ☐


Call Detail Recording: none

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

- **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 5061.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group listen port 5061 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	Connec Poli
<input type="checkbox"/>	* SM10_CM10_5061_TLS_I	<input type="text" value="SM10"/>	TLS ▼	* <input type="text" value="5061"/>	<input type="text" value="CM10"/>	* <input type="text" value="5061"/>	trusted

Select : All, None

## 6.5. Administer Routing Policies

Add two new routing policies, one for VCB and one for the new SIP trunks with Communication Manager.

### 6.5.1. Routing Policy for Fonolo VCB

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

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 Fonolo SIP entity name from **Section 6.4.2**. In the **Time of Day** sub-section, enter “0” for **Ranking**. Ranking option is only configured for the two outgoing routing policies of VCB so that calls can be load balanced. The screen below shows the result of the selection.

**Routing Policy Details** [Commit] [Cancel] [Help ?]

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
Fonolo1	10.33.1.187	SIP Trunk	SIP trunk to Fonolo VCB Appliance 1

## 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 entity name from **Section 6.4.33**. The screen below shows the result of the selection.

**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

**Routing Policy Details** Commit Cancel Help ?

**General**

\* Name:

Disabled: ☐

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
CM10	10.33.1.43	CM	

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item 🔄 Filter: Enable

<input type="checkbox"/>	Ranking ▲	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<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

## 6.6. Administer Dial Patterns

Add a new dial pattern for Fonolo VCB and Communication Manager.

### 6.6.1. Dial Pattern for Fonolo VCB

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

- **Pattern:** A dial pattern to match, in this case “78000”
- **Min:** The minimum number of digits to match
- **Max:** The maximum number of digits to match
- **SIP Domain:** The signaling group domain name from **Section 6.2**

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create an entry for reaching the Fonolo VCB. In the compliance testing, the entry allowed for call originations from all Communication Manager endpoints in locations “All”. The VCB routing policy from **Section 6.5.1** was selected as shown below. Note that two routing policies are selected since during this compliance testing, two outgoing routing policies were configured for calls made from Communication Manager to VCB.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The left navigation pane shows the 'Routing' section expanded, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' section contains the following fields:

- Pattern:** 78000
- Min:** 5
- Max:** 5
- Emergency Call:** ☐
- SIP Domain:** -ALL-
- Notes:** (empty text area)

The 'Originating Locations and Routing Policies' section shows a table with 2 items. The table has columns for 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'. The table contains two entries:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		To-Fonolo2	0	<input type="checkbox"/>	Fonolo2	Route to Fonolo VCB Appliance
-ALL-		To-Fonolo1	0	<input type="checkbox"/>	Fonolo1	Route to Fonolo VCB Appliance

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

## 6.6.2. Dial Pattern for Communication Manager

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

- **Pattern:** A dial pattern to match, in this case “33”
- **Min:** The minimum number of digits to match
- **Max:** The maximum number of digits to match
- **SIP Domain:** The signaling group domain name from **Section 6.2**

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 VCB endpoints in all locations. The Communication Manager routing policy from **Section 6.5.2** was selected as shown below.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The left navigation pane shows the 'Routing' section expanded, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes 'Commit' and 'Cancel' buttons. The 'General' sub-section contains the following fields:

- Pattern:** 33
- Min:** 4
- Max:** 4
- Emergency Call:** ☐
- SIP Domain:** avayalab.com
- Notes:** (empty text area)

The 'Originating Locations and Routing Policies' sub-section features an 'Add' button and a table with one item. The table has columns for 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'.

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

Below the table, there is a 'Select : All, None' option.

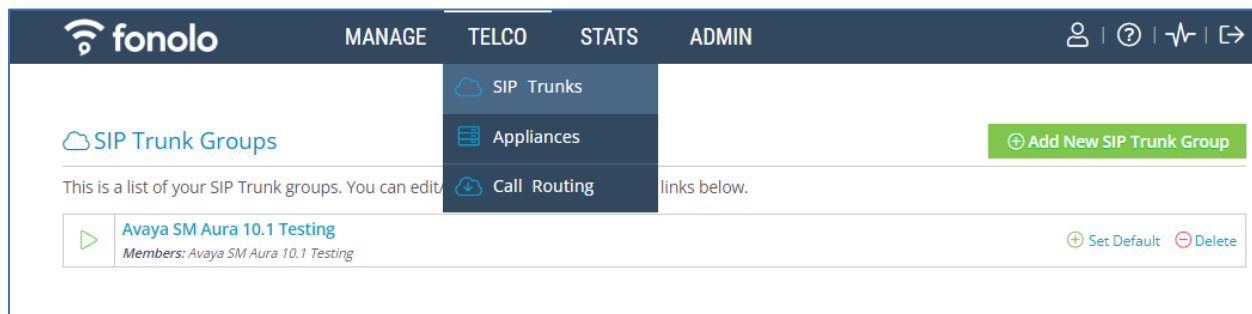
## 7. Configure Fonolo Voice Call-Backs

This section provides a “snapshot” of Fonolo VCB configuration used during compliance testing. Fonolo VCB is typically configured for customers by Fonolo. The screenshots and partial configuration shown below, supplied by Fonolo, are provided for reference only. 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.

### 7.1. Add a New SIP Trunk Group

Navigate to **Telco → SIP Trunks** and click the **Add New SIP Trunk Group** at the top of the page. Define a new label to identify this SIP trunk group. During compliance testing **Avaya SM Aura 10.1 Testing** 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:** The IP address of Session Manager formatted as a fully qualified URL, defining the protocol and SIP port.
- **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. Default is µ-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 an equal priority values are load balanced.
- **Keepalive:** This instructs the Fonolo platform to perform regular keep-alive using SIP OPTIONS requests, based on the number of seconds defined. Default is disabled.

- **Session Timers:** If Fonolo should enable SIP Session Timers (RFC 4028). Default is disabled.
- **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.

Add the IP address of Session Manager, formatted as a fully qualified URL, defining the protocol and SIP port, then click the **Save Trunk** button. During compliance testing, the protocol **UDP** and port **5060** is used for the SIP service with Session Manager, and the default values for the remaining SIP trunk group member settings.

### Update SIP Trunk

SIP Trunk SID:

TM9ce0431733d25cbcef46285d7f0392bb

SIP Label:

Avaya SM Aura 10.1 Testing

Only visible through this interface.

SIP URL:

udp://10.33.1.42:5060

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:

☒ avayalab.com

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.

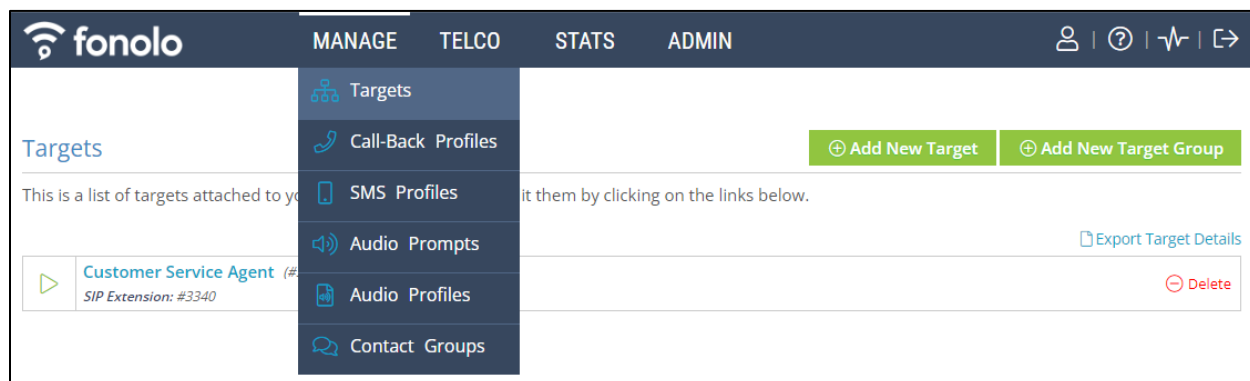
Save Trunk

Cancel

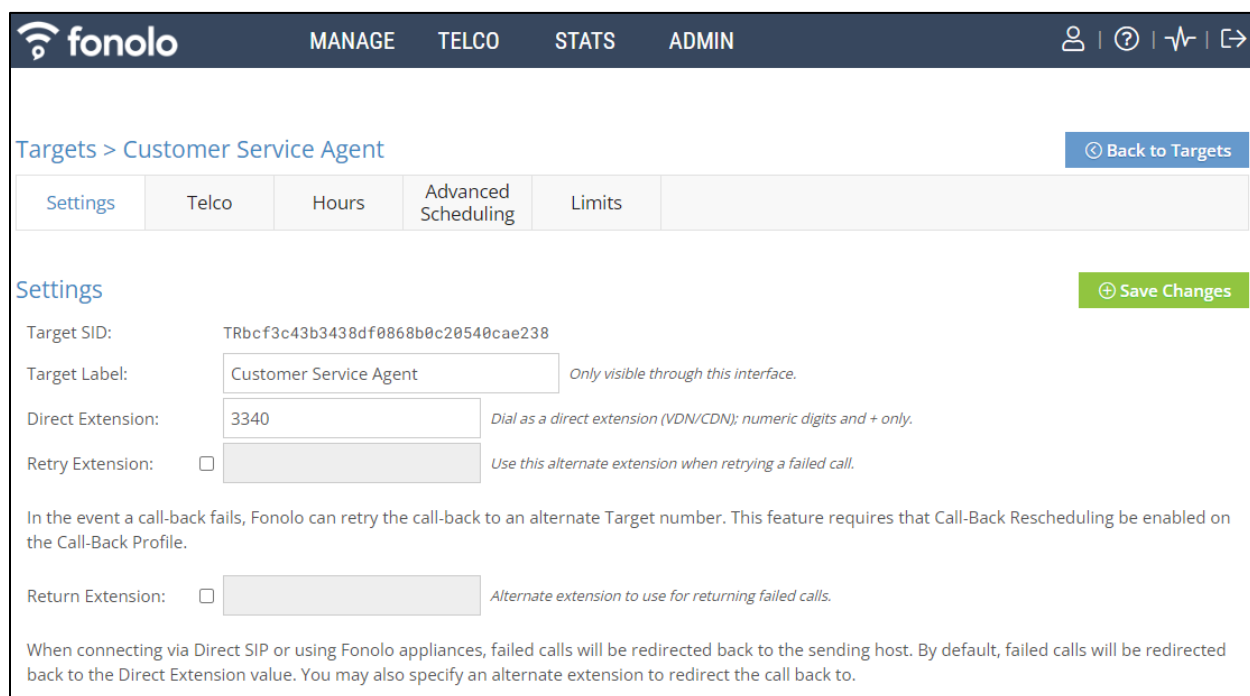


## 7.2. Adding the Voice Call-Back Endpoint

Navigate to **Manage** → **Targets** and click the **Add New Target** button. Define a new label to identify this new Target. During compliance testing, **Customer Service Agent** was used as the **Target Label**. Select the **Dial as SIP Extension** option (shown below) for **Dial Method** and enter the VDN 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 **Add New Target** button to save this Target.



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 Session Manger** SIP trunk, added in **Section Error! Reference source not found.**, and then click the **Save Changes** button.

The screenshot shows the Fonolo web interface. At the top is a dark blue header with the Fonolo logo and navigation tabs: MANAGE, TELCO, STATS, and ADMIN. On the right of the header are icons for user, help, status, and refresh. Below the header, the breadcrumb 'Targets > Customer Service Agent' is shown on the left, and a 'Back to Targets' button is on the right. A horizontal menu contains tabs for Settings, Telco (which is selected), Hours, Advanced Scheduling, and Limits. Below this menu, the 'Telco Settings' section is displayed. It includes a description: 'This controls how Fonolo will call in to your phone system.' There are two configuration fields: 'Direct SIP:' with a dropdown menu showing 'Avaya SM Aura 10.1 Testing' and a link 'Use this SIP Trunk.', and 'Dial Timeout:' with a text input '60' and a note 'How long to wait for the Target to answer before returning "Target Call Timeout". 10 to 120 secs.' A green 'Save Changes' button is located in the top right corner of the settings area.

### 7.3. Adding a New Call-Back Profile

Navigate to **Manage → Call-Back Profiles** and click on the **Add New Profile** button (not shown), and configure the new profile:

- **Profile Label:** A label to identify this new profile
- **Geo Whitelist:** A geographic whitelist to use for this new profile
- **Channel:** Select “In-Call Rescue”
- **Language:** Select the appropriate language for this skill set queue
- **Client CID Number:** The Caller-ID number the customer will see
- **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 New Call-Back Profile** button to add this new profile.

**fonolo** MANAGE TELCO STATS ADMIN

Call-Back Profiles > Voice CallBack Profile [Back to Call-Back Profiles](#)

Settings Call Options Telco Settings Features Rescheduling Scheduled Call-Backs Pre-Call Questions

**Settings** [Save Changes](#)

Profile SID: CP54a44cea0d2b25f35e23965a0034e897

Profile Label:  Only visible through this interface.

Geo. Whitelist:  This is the geographic white list to use with this call-back profile.

Channel: In-Call Rescue

Language: English

**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 **Call Options** section of the new **Call-Back Profile**, select the Target added in **Section Error! Reference source not found.** (from the drop-down menu highlighted below), and click the **Add Option** link to add the VDN value to the section on the left, as shown below, then click the **Save Changes** (not shown) button.

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.

**fonolo** MANAGE TELCO STATS ADMIN

Call-Back Profiles > Voice CallBack Profile [Back to Call-Back Profiles](#)

Settings **Call Options** Telco Settings Features Rescheduling Scheduled Call-Backs Pre-Call Questions

**Call Options**

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

[Add Option](#)

	<b>Customer Service Agent</b> <small>Target Extension: 3340, Fonolo Extension: 78000, Dialing Area: 1</small>	<a href="#">Edit</a> <a href="#">Delete</a>
--	--	---

From the **Telco Settings** section of the new **Call-Back Profile**, select the **Avaya Session Manager** SIP trunk group created in **Section Error! Reference source not found.** as the **Direct SIP** value under both the **Client Call-Back Method** and the **In-Call Rescue Call Transfers** section, as shown below, then click the **Save Changes** button.

**fonolo** MANAGE TELCO STATS ADMIN

Call-Back Profiles > Voice CallBack Profile [Back to Call-Back Profiles](#)

Settings Call Options **Telco Settings** Features Rescheduling Scheduled Call-Backs Pre-Call 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 SM Aura 10.1 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.*

**In-Call Rescue Call 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 SM Aura 10.1 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.*

Dialing Area: (+1) United States, Canada, & Island N *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 VCB system, when a call opts-in for a call-back. During compliance testing, the extension **78000** was configured on the Fonolo system.

**fonolo** ICR Settings

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

[Customer Service Agent](#) 78000

[Close](#)

[Add New Call-Back Profile](#)

[Export Call Options](#)

[Call Options](#) [Archive](#)

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

## 8. Verification Steps

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

### 8.1. 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
0001/0007 T000007 in-service/idle no
0001/0008 T000008 in-service/idle no
```

The following tests were also performed to verify proper configuration of Fonolo VCB with Communication Manager.

- PSTN caller can select the call back option and get redirected to VCB via Communication Manager/Session Manager.
- PSTN caller can hear the VCB menu and make the required choices.
- VCB can recognize the choices made by the PSTN user.
- VCB can call the VDN and wait for an available agent.
- VCB can call out to the PSTN caller and connect them to an available agent.

## 8.2. 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 ..., Global Settings, Communication Prof..., Network Configur..., Device and Locati..., Application Confi..., System Status, and Load Factor. The main content area is titled "SIP Entity, Entity Link Connection Status" and includes a sub-header "All Entity Links to SIP Entity: CM10". Below this, there is a "Summary View" button and a table showing the connection status for the selected Session Manager. The table has columns: Session Manager Name, Session Manager IP Address, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The table contains one item with the following data:

Session Manager Name	Session Manager IP Address	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
SM10	IPv4	10.33.1.43	5061	TLS	FALSE	UP	200 OK	UP

The "Link Status" is "UP".

Repeat the same procedure selecting each Fonolo VCB 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 ..., Global Settings, Communication Prof..., Network Configur..., Device and Locati..., Application Confi..., System Status, and Load Factor. The main content area is titled "SIP Entity, Entity Link Connection Status" and includes a sub-header "All Entity Links to SIP Entity: Fonolo1". Below this, there is a "Summary View" button and a table showing the connection status for the selected Session Manager. The table has columns: Session Manager Name, Session Manager IP Address, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The table contains one item with the following data:

Session Manager Name	Session Manager IP Address	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
SM10	IPv4	10.33.1.187	5060	UDP	FALSE	UP	200 OK	UP

The "Link Status" is "UP".

### 8.3. Verify Fonolo Voice Call-Back

In the Fonolo customer portal, verify the link status of the SIP trunk group to Session Manager, by navigating to **Telco → Appliances** and select the appliance group (not shown) and then select the **Member** tab. All appliances should be synced successfully.

**fonolo** MANAGE TELCO STATS ADMIN

Appliances > Avaya [Back to Appliance Groups](#)

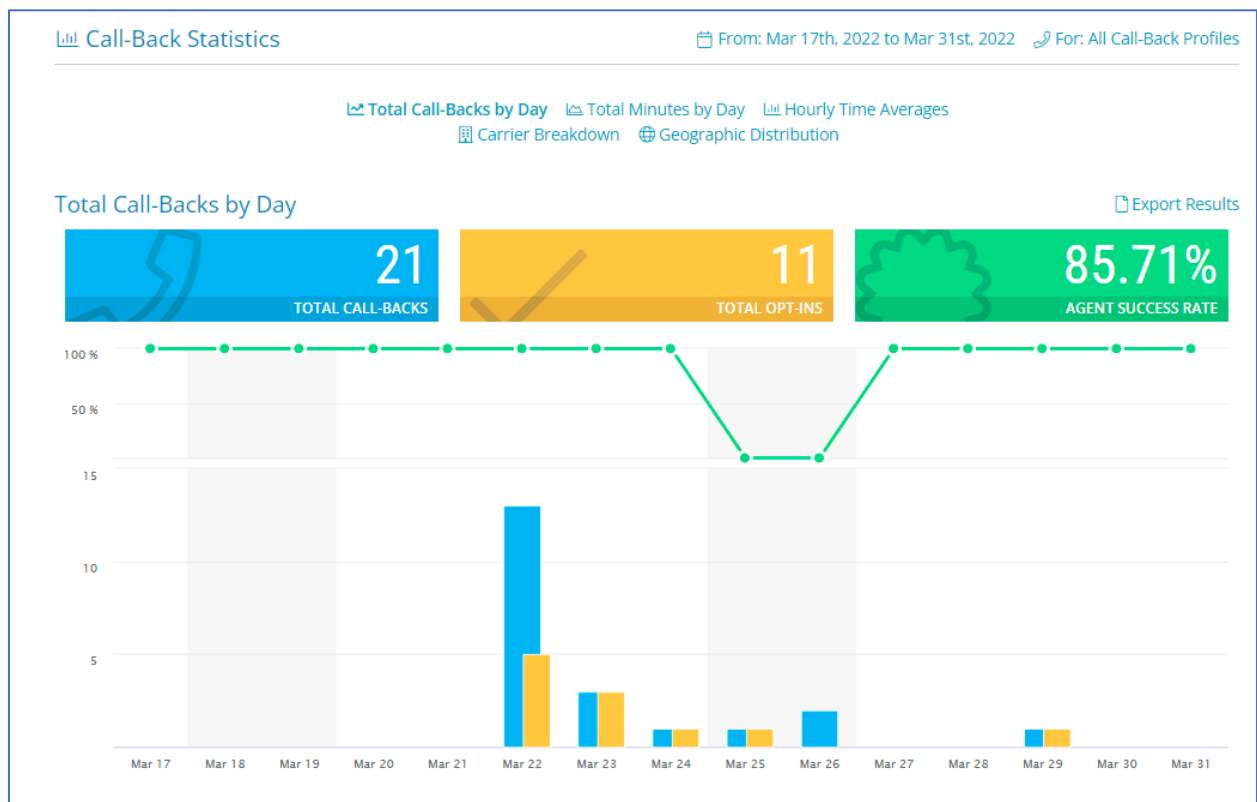
Settings Members

Appliance Group Members [Add New Member](#)

Fonolo will select an appliance from this group for each Call-Back placed.

	<b>app1.avy.icr.fonolo.net</b> (50.207.80.87) - v3.3 ✓ polled: Apr 6th, 2022 @ 16:19, priority: 10	<a href="#">Sync</a> <a href="#">Delete</a>
	<b>app2.avy.icr.fonolo.net</b> (50.207.80.88) - v3.3 ✓ polled: Apr 6th, 2022 @ 16:19, priority: 10	<a href="#">Sync</a> <a href="#">Delete</a>

Additional information is available through the **Stats → Graphs** section or **Stats → Call Details** section.



fonolo

MANAGE

TELCO

STATS

ADMIN

Call-Back Details

From: Sep 22nd, 2022 to Oct 6th, 2022

For: All Call-Back Profiles

This section lets you view and export detailed Call-Back details.

Export Results

Date	Time	Option	Client	Deep Dial	Hold Time	CC Time	Talk Time	Duration	Debug Recording	Status	Clearing	Ended By	Resch
2022-10-04	12:14:29	Customer Service Agent	16139675071	00:00	00:22	00:13	31:40	32:15	--	Success	Normal Clearing	Company	
2022-10-04	09:24:25	Customer Service Agent	16139675089	00:00	00:18	00:07	02:16	02:41	--	Success	Normal Clearing	Client	
2022-10-03	01:24:09	Customer Service Agent	16139675089	00:00	00:46	00:25	01:36	02:47	--	Success	Normal Clearing	Client	
2022-10-03	01:22:54	Customer Service Agent	16139675089	00:00	01:02	00:00	00:00	01:02	--	Failed	Agent Did Not Accept	Company	Aut
2022-10-03	01:22:09	Customer Service Agent	16139675089	00:00	00:33	00:00	00:00	00:33	--	Failed	Agent Did Not Accept	Company	Aut
2022-10-01	23:49:23	Customer Service Agent	16139675089	00:00	00:24	00:00	00:00	00:24	--	Failed	Agent Did Not Accept	Company	N
2022-10-01	23:47:49	Customer Service Agent	16139675089	00:00	01:29	00:00	00:00	01:29	--	Failed	Agent Did Not Accept	Company	Aut
2022-10-01	23:41:19	Customer Service Agent	16139675089	00:00	06:22	00:00	00:00	06:23	--	Failed	Agent Did Not Accept	Company	Aut
2022-09-30	22:37:33	Customer Service Agent	16139675085	00:00	09:06	00:07	09:54	19:08	--	Success	Normal Clearing	Client	
2022-09-30	22:34:22	Customer Service Agent	16139675071	00:00	00:26	00:07	24:14	24:47	--	Success	Normal Clearing	Company	
2022-09-30	22:26:37	Customer Service Agent	16139675085	00:00	10:42	00:00	00:00	10:42	--	Failed	Agent Did Not Accept	Company	Aut
2022-09-30	22:25:48	Customer Service Agent	16139675071	00:00	08:29	00:00	00:00	08:29	--	Failed	Agent Did Not Accept	Company	Aut
2022-09-30	11:50:48	Customer Service Agent	16139675071	00:00	00:18	00:08	03:13	03:40	--	Success	Normal Clearing	Company	
2022-09-30	11:34:52	Customer Service Agent	16139675071	00:00	15:43	00:00	00:00	15:43	--	Failed	Agent Did Not Accept	Company	Aut
2022-09-29	13:04:47	Customer Service Agent	16139675189	00:00	00:48	00:09	01:30	02:27	--	Success	Normal Clearing	Company	
2022-09-29	13:01:51	Customer Service Agent	16139675189	00:00	02:50	00:00	00:00	02:51	--	Failed	Agent Did Not Accept	Company	Aut
2022-09-29	12:48:02	Customer Service Agent	16139675189	00:00	12:02	00:00	00:00	12:02	--	Canceled	Canceled by Admin	Client	
2022-09-29	01:15:06	Customer Service Agent	16139675071	00:00	02:14	00:11	01:41	04:07	--	Success	Normal Clearing	Company	



## 9. Conclusion

These Application Notes describe the configuration steps required for Fonolo Voice Call-Backs to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. All feature and serviceability test cases were completed and passed with the exceptions/observations noted in **Section** Error! Reference source not found..

## 10. 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. *Deploying Avaya Aura® Session Manager and Branch Session Manager in Virtualized Environment*, Release 10.1, Issue 3, September 2022
2. *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 3, August 2022
3. *Deploying Avaya Aura® System Manager in Virtualized Environment*, Release 10.1, Issue 4, August 2022
4. *Administering Avaya Aura® System Manager for Release 10.1*, Release 10.1, Issue 5, September 2022
5. *Deploying Avaya Aura® Communication Manager in Virtualized Environment*, Release 10.1, Issue 4, September 2022
6. *Administering Avaya Aura® Communication Manager*, Release 10.1, September 2022
7. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.1, September 2022
8. *Administering Avaya G430 Branch Gateway*, Release 10.1, Issue 3, September 2022
9. *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0, October 2022

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

---

**©2022 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).