



DevConnect Program

Application Notes for Sestek Knovvu Virtual Translator with Avaya Aura® Session Manager 10.1 and Avaya Aura® Communication Manager 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Sestek Knovvu Virtual Translator 11.5 with Avaya Aura® Session Manager 10.1 and Avaya Aura® Communication Manager 10.1.

Sestek Knovvu Virtual Translator leverages advanced Speech Recognition (SR) technology to analyze and detect the language spoken by callers. By processing the audio input, it identifies the language being spoken, converts the speech to text (STT), translates it to the desired language for the response, and generates a text-to-speech (TTS) output. This means a significantly more efficient call center, with the ability to serve in multiple languages.

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

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	6
2.2.	Test Results	7
2.3.	Support	7
3.	Reference Configuration.....	8
4.	Equipment and Software Validated	9
5.	Configure Avaya Aura® Communication Manager.....	10
5.1.	Verify Licensed Features	10
5.2.	Dial Plan.....	11
5.3.	Node Names	12
5.4.	IP Codec Set.....	12
5.5.	IP Network Region.....	13
5.6.	SIP Trunk to Session Manager.....	14
5.6.1.	Signaling Group.....	15
5.6.2.	Trunk Group.....	16
5.7.	Route Patterns	18
5.8.	AAR Call Routing.....	19
5.9.	Call Center – Vectors, Hunt Groups and Agents	20
6.	Configure Avaya Aura® Session Manager.....	23
6.1.	System Manager Login and Navigation.....	23
6.2.	SIP Domain	24
6.3.	Locations	25
6.3.1.	Main Location.....	25
6.3.2.	CM-TG23 Location	26
6.3.3.	Knovvu Translator Location.....	26
6.4.	Adaptation	26
6.5.	SIP Entities.....	27
6.5.1.	Avaya Aura® Session Manager SIP Entity	28
6.5.2.	Avaya Aura® Communication Manager SIP Entity – Trunk Group 23	29
6.5.3.	Sestek Voice Gateway SIP Entity.....	30
6.6.	Entity Links.....	31
6.6.1.	Entity Link to Avaya Aura® Communication Manager Trunk Group.....	31
6.6.2.	Entity Link to Knovvu Translator.....	32
6.7.	Routing Policies	33
6.7.1.	Routing Policy for Calls to Knovvu Translator	33
6.7.2.	Routing Policy for Calls to Communication Manager Trunk Group	33
6.8.	Dial Patterns	34
6.8.1.	Dial Pattern for Calls to Knovvu Translator	34
6.8.2.	Dial Pattern for Calls to Avaya Aura® Communication Manager.....	36
7.	Knovvu Virtual Translator Configuration	38
8.	Verification Steps.....	42
8.1.	Avaya Aura® Communication Manager Verification	42
8.2.	Avaya Aura® Session Manager Verification.....	43
8.3.	Sestek Knovvu Virtual Translator Verifications.....	44

9.	Conclusion	45
10.	Additional References.....	45

1. Introduction

These Application Notes describe the configuration steps required to integrate Sestek Knovvu Virtual Translator with Avaya Aura® Session Manager 10.1 (Session Manager) and Avaya Aura® Communication Manager 10.1 (Communication Manager).

Sestek Knovvu Virtual Translator leverages advanced Speech Recognition (SR) technology to analyze and detect the language spoken by callers. By processing the audio input, it identifies the language being spoken, converts the speech to text (STT), translates it to the desired language for the response, and generates a text-to-speech (TTS) output. This means a significantly more efficient call center, with the ability to serve in multiple languages.

The Sestek Knovvu Virtual Translator solution tested consisted of the Sestek Voice Gateway, running on a Windows Server at the enterprise site, and a Sestek API Translator Server in the Sestek cloud. The Sestek Voice Gateway interfaces with Avaya Session Manager via SIP trunk at the enterprise site. The Sestek Voice Gateway communicates with the Sestek API Translator in the Sestek cloud via http/https through the public Internet.

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 the Sestek Voice Gateway via Avaya Communication Manager and Session Manager. The general call flow used in the reference configuration is as follows:

1. Caller places a call from the PSTN via SIP trunk to the Avaya Aura® enterprise site.
2. The call is received via Avaya SBC / Session Manager / Communication Manager.
3. Communication Manager uses a Vector Directory Number (VDN) to send the call to Session Manager.
4. Session Manager routes the call to the Sestek Voice Gateway via a SIP trunk.
5. The Sestek Voice Gateway answers the inbound call, and it generates a new call, sent via Session Manager to another Communication Manager VDN. Both the inbound and outbound Voice Gateway calls are bridged together.
6. The Communication Manager VDN sends the call to an agent queue.
7. Caller hears announcement and music if agent is not available.
8. Available agent answers the call and interacts with the caller.
9. Once the agent detects that the caller uses a different language, it presses the translation activation code on the agent's telephone to start the translations.
10. Voice is translated in both directions, to the correct language used by caller and agent.
11. Caller and agent hear music during the time intervals while the voice is being processed and translated by the Sestek servers.
12. Agent or caller terminates the call.

The serviceability test cases focused on simulating a network outage and also a restart on the Sestek Voice Gateway. Calls were verified to complete successfully after the network was restored and the Voice Gateway 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 Session Manager and the Sestek Voice Gateway did not use encryption capabilities as requested by Sestek.

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

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establish SIP trunk between Avaya Session Manager and Sestek Voice Gateway.
- Responses from Sestek Voice Gateway to SIP OPTIONS messages sent by Avaya Session Manager.
- Inbound PSTN calls routed from Communication Manager via Session Manager to the SIP trunk to the Voice Gateway.
- Verify the Voice Gateway generates a new outbound call via Session Manager to the Communication Manager VDN used to reach the agents. Inbound and outbound calls are bridged together and audio is normal in both directions.
- Inbound calls from the Voice Gateway received on agents using Avaya 96x1 Series SIP and H.323 Deskphones, as well as Avaya Workplaces and Avaya Agent for Desktop softphones.
- Verify voice is translated to the correct language of the agent and caller when translation is activated by the agent.
- During the compliance test, English was manually configured as the language on the agent side, while Spanish was dynamically detected on the caller side.
- Proper disconnect when the call is abandoned by the caller before it is answered.
- Proper disconnect via normal call termination by the caller or the called parties.
- Codecs G.711U, G.711A and G.729.
- Call hold and resume.
- Verify service is restored after a network outage on the Voice Gateway.
- Verify service is restored after a Voice Gateway server restart.

Items not supported:

- Call Transfer and Call Forward are not currently supported and were not tested.

2.2. Test Results

Interoperability testing of Sestek Knovvu Virtual Translator with the Avaya solution was completed with successful results for all test cases. The following observations are noted for the sample configuration described in these Application Notes.

- **Early Media in Communication Manager needs to be Disabled** – Calls were initially affected by a 5-6 second voice delay, locally introduced by the Sestek Voice Gateway, in the path of the agent to caller direction. This delay occurred even without the agent pressing the translation activation code on the telephone. It was determined that this was due to early media RTP packets sent by Communication Manager, filling up the Sestek Voice Gateway buffers. This issue was resolved after changes were made in the Communication Manager signaling group of the trunk used for Sestek calls, to disable transmission of early media on inbound calls to the trunk. See **Section 5.6.1**. Sestek additionally made updates to the Hummingbird software, to drop any RTP packets received from Communication Manager before the call completion.
- **Processing Delay** – There is a few seconds delay in each direction during the time in which the voice is being processed and translated by the Sestek server. Caller and agent alternatively hear music during the time intervals while the processing is occurring, which helps in making a better experience for the two parties.
- **Music on Hold** – During testing it was found that on a call that was being translated and was placed on hold, the music on hold was not being played to the caller. Additionally, content on the on-hold music containing words, was unexpectedly being translated to the caller. An update was made on the Sestek Hummingbird software, to use the “sendonly” and “senrecv” attributes sent on the re-INVITES from Communication Manager, to place the Voice Gateway on “bridge” mode while the call is on hold, and back to the previous mode when the call is taken off hold. See note on the Communication Manager trunk configuration **Section 5.6.2**. Music on Hold was tested successfully after this update.
- **Message Method Over SIP** – In addition to the translated voice, the Sestek Voice Gateway sends text messages of the translation transcripts towards Session Manager, using the MESSAGE method over SIP. The MESSAGE SIP method is not supported by Avaya Communication Manager, which rejects it with a “405 Method not Allowed”. This has no effect on the voice calls, which continue their progress normally.
- **No ACK Response to “487 Request Terminated”** – On an inbound call that is abandoned by the caller before the agent answers, the Sestek Voice Gateway sends a CANCEL and Session Manager responds with a 200 OK as expected. Session Manager then sends a “487 Request Terminated” to the Gateway, but there is no ACK response from the Gateway. Session Manager keeps sending the 487 for about 30 seconds and then it stops. There is no delay on the trunk being released and there is no noticeable impact to the user. This is just noted here as an observation.

2.3. Support

Technical support for Sestek Knovvu Virtual Translator can be obtained through the following:

Phone: +90 850 737 27 37

Web: <https://support.sestek.com/en-US/signin>

Email: support@sestek.com

3. Reference Configuration

Figure 1 illustrates the sample configuration used for the compliance testing.

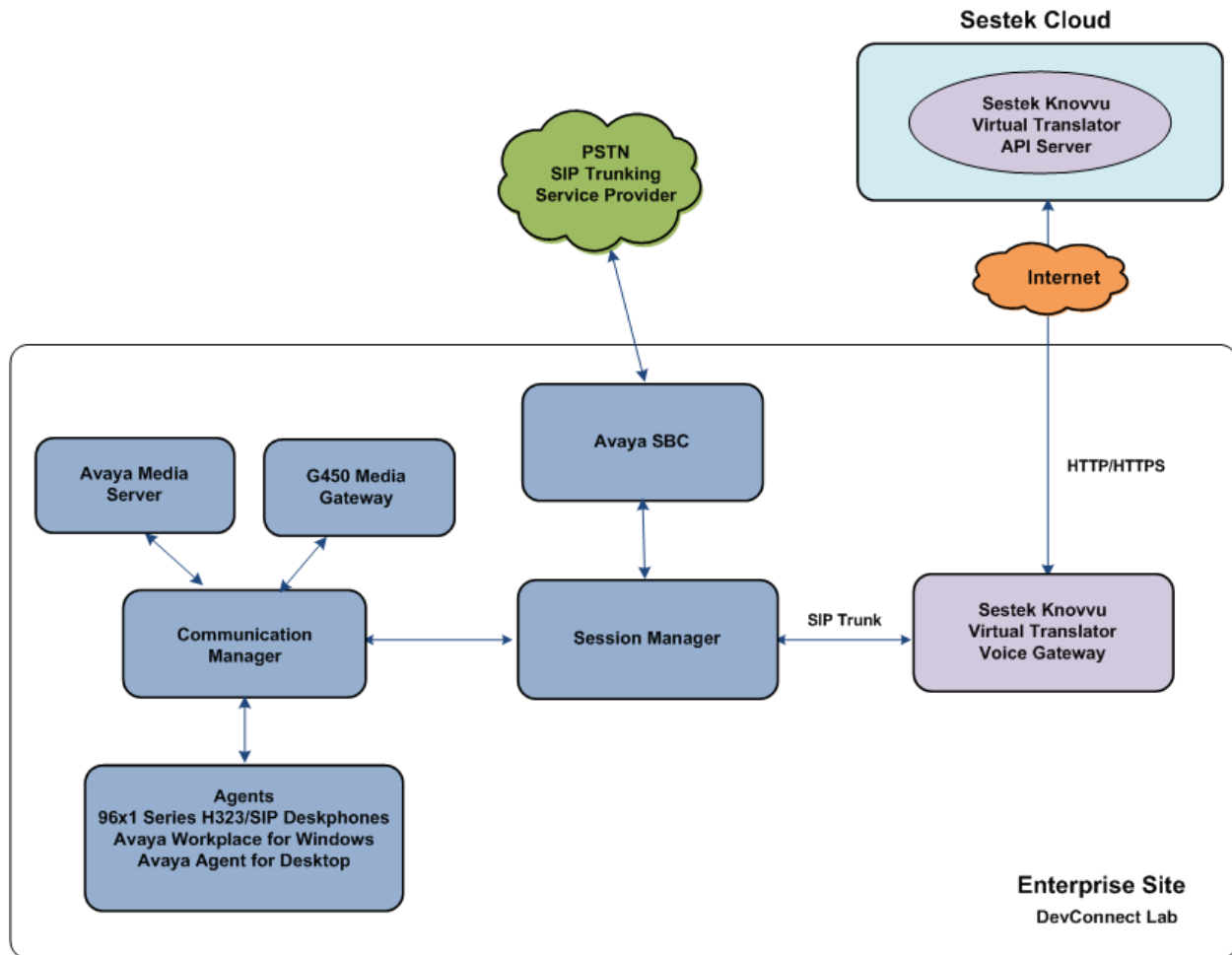


Figure 1: Test Configuration

A simulated enterprise site containing the Sestek Voice Gateway, Avaya Session Manager, Communication Manager and the rest of the Avaya Aura® infrastructure was installed at the DevConnect Lab. An Avaya SBC connected the enterprise site to a SIP trunk service provider, used to generate inbound PSTN calls to the enterprise.

The PSTN carrier in the lab provided Direct Inward Dial (DID) 10-digit numbers. One of the DID numbers was mapped by Session Manager to the corresponding Communication Manager Vector Directory Number (VDN), where a vector routed the inbound call on a dedicated trunk to the number expected by the Sestek Voice Gateway. In similar fashion, the Voice Gateway generates a new call that is sent to another VDN in Communication Manager, where a vector routes the call to an agent queue.

Note – These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning described in this document.

The following Avaya components were used in the reference configuration in the DevConnect Lab:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Session Border Controller
- Avaya G450 Media Gateway
- Avaya Media Server
- Avaya 96X1 Series IP Deskphones using the SIP and H.323 software bundle
- Avaya Workplace Client for Windows and Avaya Agent for Desktop SIP softphones

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 96x1 Series IP Deskphone (SIP)	7.1.15.2.1
Avaya Workplace Client for Windows	3.35.0.167
Avaya Agent for Desktop	2.0.6.26.3002
Sestek Knovvu Virtual Translator running on Windows Server machine	Hummingbird Version 11.5.2.2

5. Configure Avaya Aura® Communication Manager

This section covers the configuration steps required to establish a SIP trunk between Communication Manager and Session Manager. This trunk that will carry the calls to the Sestek Voice Gateway. Call routing configuration and sample VDN and vectors are also shown. Communication Manager is configured through the System Access Terminal (SAT).

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. Similarly, the configuration of the call center, including agents, skill/hunt group, etc. is outside the scope of these Application Notes.

5.1. Verify Licensed Features

This section describes steps to verify Communication Manager feature settings that are required for the reference configuration described in these Application Notes. Depending on access privileges and licensing, some or all of the following settings might only be viewed, and not modified. If any of the required features are not set, and cannot be configured, contact an authorized Avaya account representative to obtain the necessary licenses/access

Enter the **display system-parameters customer-options** command. On **Page 2** of the form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks.

display system-parameters customer-options		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	0
Maximum Concurrently Registered IP Stations:	2400	1
Maximum Administered Remote Office Trunks:	12000	0
Max Concurrently Registered Remote Office Stations:	2400	0
Maximum Concurrently Registered IP eCons:	128	0
Max Concur Reg Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	36000	0
Maximum Video Capable IP Softphones:	2400	1
Maximum Administered SIP Trunks:	12000	120
Max Administered Ad-hoc Video Conferencing Ports:	12000	0
Max Number of DS1 Boards with Echo Cancellation:	688	0

On **Page 5** of the form, verify that **IP Trunks** and **ISDN/SIP Network Call Redirection** features are enabled.

display system-parameters customer-options

Page5 of 12

OPTIONAL FEATURES

Emergency Access to Attendant? y

Enable 'dadmin' Login? y

Enhanced Conferencing? y

Enhanced EC500? y

Enterprise Survivable Server? n

Enterprise Wide Licensing? n

ESS Administration? y

Extended Cvg/Fwd Admin? y

External Device Alarm Admin? y

Five Port Networks Max Per MCC? n

Flexible Billing? n

Forced Entry of Account Codes? y

Global Call Classification? y

Hospitality (Basic)? y

Hospitality (G3V3 Enhancements)? y

IP Trunks? y

IP Attendant Consoles? y

IP Stations? y

ISDN Feature Plus? n

ISDN/SIP Network Call Redirection? y

ISDN-BRI Trunks? y

ISDN-PRI? y

Local Survivable Processor? n

Malicious Call Trace? y

Media Encryption Over IP? y

Mode Code for Centralized Voice Mail? n

Multifrequency Signaling? y

Multimedia Call Handling (Basic)? y

Multimedia Call Handling (Enhanced)? y

Multimedia IP SIP Trunking? y

5.2. Dial Plan

The dial plan defines how digit strings will be used locally by Communication Manager. The following dial plan was used in the reference configuration.

Enter the **change dialplan analysis** command to provision the following dial plan.

- 5-digit extensions with a **Call Type** of **ext** beginning with:
 - The digits **1, 2, 3, 5** and **7** for Communication Manager extensions and VDNs.
- 3-digit dial access code (indicated with a **Call Type** of **dac**), e.g., access code ***xx** for SIP Trunk Access Codes (TAC). See the trunk form in **Section 5.6.2**.

change dialplan analysis

Page1 of 12

DIAL PLAN ANALYSIS TABLE

Location: all

Percent Full: 1

Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
1	5	ext						
2	5	ext						
3	5	ext						
4	5	ext						
5	5	ext						
60	3	ext						
66	2	fac						
7	5	ext						
8	5	ext						
9	1	fac						
*	3	dac						

5.3. Node Names

Node names define IP addresses to various Avaya components in the enterprise. In the reference configuration a Processor Ethernet (procr) based Communication Manager platform is used.

Note that the Communication Manager procr and Session Manager node names and IP address are entered during installation. Enter the **change node-names ip** command, and verify the node name and IP address for the following:

- Communication Manager (e.g., **procr** and **10.64.91.87**).
- Session Manager SIP signaling interface (e.g., **SM** and **10.64.91.85**).

change node-names ip		Page	1 of	2
IP NODE NAMES				
Name	IP Address			
AMS10	10.64.91.88			
SM	10.64.91.85			
aes	10.64.91.95			
default	0.0.0.0			
procr	10.64.91.87			

5.4. IP Codec Set

Use the **change ip-codec-set x** command, where **x** is the number of an IP codec set used for calls between the enterprise Sestek Voice Gateway (e.g., **3**). Note the codec set number since it will be used in the IP Network Region covered in the next section. **G.711MU**, **G.711A** and **G.729** were used, in that order. Media Encryption was not used and it was set to **none**.

change ip-codec-set 3

Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 3

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

Media Encryption

Encrypted SRTCP: enforce-unenc-srtcp

1: **none**

2:

3:

5.5. IP Network Region

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G450 Media Gateway and Avaya Media Server are in region 1 (not shown). To provide testing flexibility, network region **3** was associated with other components used specifically for the calls to Sestek Voice Gateway.

Enter **change ip-network-region x**, where **x** is the number of an unused IP network region (e.g., region **3**). Populate the form with the following values:

- Enter a descriptive name (e.g., **Knovvu Translator**).
- Enter the enterprise domain (e.g., **avayalab.com**) in the **Authoritative Domain** field.
- Enter **3** for the **Codec Set** parameter.
- **Intra-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
- **Inter-region IP-IP Audio Connections** – Set to **yes**, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.

change ip-network-region 3		Page 1 of 20
IP NETWORK REGION		
Region: 3	NR Group: 3	
Location: 1	Authoritative Domain: avayalab.com	
Name: Knovvu Translator	Stub Network Region: n	
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 3	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
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		

On **Page 4** of the form:

- Next to region **1** in the **dst rgn** column, enter **3** for the codec set (this means region 1 is permitted to talk to region 3 and it will use codec set 3 to do so). The **direct WAN** and **Units** columns will self-populate with **y** and **No Limit** respectively.
- Note that **dst rgn 3** is pre-populated with codec set **3** (from page 1 provisioning).
- Let all other values default for this form.

change ip-network-region 3										Page 4 of 20			
Source Region: 3				Inter Network Region Connection Management						I	M		
										G	A	t	
dst	codec	direct	WAN-BW-limits		Video		Intervening		Dyn	A	G	n	c
rgn	set	WAN	Units	Total	Norm	Prio	Shr	Regions	CAC	R	L	c	e
1	3	y	NoLimit							n		y	t
2													
3	3									all			
4													
5													

5.6. SIP Trunk to Session Manager

A new SIP Trunk (Trunk Group 23) was defined in the reference configuration between Communication Manager and Session Manager, to carry inbound and outbound traffic to the Sestek Voice Gateway. This trunk will use TLS port 5083. Note that this port is different to the port assigned to other trunks to Session Manager. This is necessary so Session Manager can distinguish the traffic on the trunk to Sestek Voice Gateway, from the traffic on other trunks used on the enterprise.

5.6.1. Signaling Group

SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group. Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g., **23**), and provision the following:

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**.
- The **Transport Method** field was set to **tls**.
- Verify that **Peer Detection Enabled** is set to **y**. The system will auto detect and set the **Peer Server** to **SM**.
- **Near-end Node Name** – Set to the node name of the **procr** noted in **Section 5.3**.
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 5.3** (e.g., **SM**).
- **Near-end Listen Port** and **Far-end Listen Port** – Set to **5083**.
- **Far-end Network Region** – Set the IP network region to **3**, as set in **Section 5.5**.
- **Far-end Domain** – Enter the enterprise domain, e.g., **avayalab.com**.
- **DTMF over IP** – Set to **rtp-payload** to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to **y**, indicating that the RTP paths should be optimized directly to the associated stations, to reduce the use of media resources on the Avaya Media Gateway when possible (known as shuffling).
- **Initial IP-IP Direct Media** – Set to **y**. This setting effectively disables Communication Manager early media on inbound calls on the associated trunk. See note in **Section 2.2**.

change signaling-group 23		Page 1 of 2
SIGNALING GROUP		
Group Number: 23	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: SM	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: SM	
Near-end Listen Port: 5083	Far-end Listen Port: 5083	
	Far-end Network Region: 3	
Far-end Domain: avayalab.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? y	Initial IP-IP Direct Media? y	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	
Alternate Route Timer(sec): 6		

Use the default parameters on **page 2** of the form (not shown).

5.6.2. Trunk Group

Next enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g., **23**). On **Page 1** of the **trunk-group** form, provision the following:

- **Group Type** – Set to **sip**.
- **Group Name** – Enter a descriptive name (e.g., **To SM and Knovvu Translator**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g., ***23**).
- **Direction** – Set to **two-way**.
- **Service Type** – Set to **public-ntwrk**.
- **Signaling Group** – Set to the signaling group previously administered (e.g., **23**).
- **Number of Members** – Enter the maximum number of simultaneous calls desired on this trunk group (based on licensing) (e.g., **10**).

```
add trunk-group 23                                     Page 1 of 21
TRUNK GROUP
Group Number: 23          Group Type: sip          CDR Reports: y
  Group Name: To SM and Knovvu Translator COR: 1    TN: 1      TAC: *23
  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: 23
                          Number of Members: 10
```

On **Page 3** of the **Trunk Group** form set **Numbering Format** to **public**. Accept all other defaults.

```
add trunk-group 4                                     Page 3 of 21
TRUNK FEATURES
ACA Assignment? n          Measured: none
                          Maintenance Tests? y

Suppress # Outpulsing? n  Numbering Format: public
                          UI Treatment: shared
                          Maximum Size of UI Contents: 128
                          Replace Restricted Numbers? n
                          Replace Unavailable Numbers? n

                          Modify Tandem Calling Number: no
Send UCID? n

Show ANSWERED BY on Display? y
```


On **Page 4** of the trunk group form, set **Network Call Redirection** to **y**. With this setting the “sendonly” and “senrecv” attributes are sent on re-INVITES from Communication Manager when calls are placed and retrieved from Hold. See note on **Section 2.2**. All other fields retained their default values.

add trunk-group 4	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? n	
Support Request History? y	
Telephone Event Payload Type:	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Resend Display UPDATE Once on Receipt of 481 Response? 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. Route Patterns

Route Patterns are used to direct outbound calls via the public or local CPE SIP trunks. This form defines the public SIP trunk, based on the route-pattern selected by the AAR table next in **Section 5.8**. The routing defined in this section is simply an example and not intended to be prescriptive. Other routing policies may be appropriate for different customer networks. In the reference configuration, route pattern 23 is used for calls to the Sestek Voice Gateway.

Enter the **change route-pattern x** command, where **x** is the number of an unused route pattern (e.g., **23**), to configure a route pattern for calls to the Sestek Voice Gateway and enter the following parameters:

- In the **Grp No** column, enter **23** for trunk group 23.
- In the **FRL** column enter **0** (zero).
- In the **Numbering Format** column, enter **pub-unk**.

```

change route-pattern 23
Pattern Number:23      Pattern Name: To Translator
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: 23      0
2:
3:

                                n      user
                                n      user
                                n      user

BCC VALUE  TSC CA-TSC      ITC BCIE Service/Feature PARM Sub Numbering LAR
0 1 2 M 4 W      Request      Dgts Format
1: y y y y y n      n      rest      pub-unk      none

```

5.8. AAR Call Routing

In the testing environment, **33000** was the provisioned number which needs to be dialed on the enterprise across the SIP trunk to reach the Sestek Voice Gateway. Configure the **Uniform Dial Plan** to steer these calls to AAR as shown below.

change uniform-dialplan 3					Page 1 of 2	
UNIFORM DIAL PLAN TABLE						
					Percent Full: 0	
Matching			Insert		Node	
Pattern	Len	Del	Digits	Net Conv	Num	
33000	5	0		aar n		

SIP calls to Session Manager are routed over the SIP trunk via AAR call routing. Configure the AAR analysis form and add an entry to route calls to **33000** to use **Route Pattern 23** as shown below.

change aar analysis 33000						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	
33000	5	5	23	aar		n	

5.9. Call Center – Vectors, Hunt Groups and Agents

For the compliance test, a basic call center was configured on Communication Manager, consisting of agents, hunt/skill group, VDNs, and vectors. The call center configuration is outside the scope of these Application Notes and will not be covered. The sample vectors used are shown to illustrate the call flows.

Device Type	Extension
VDN Inbound PSTN Call	10042
VDN Inbound Voice Gateway Call	50101
Skill Group	1
Agents	20001-20004

Inbound PSTN calls are routed to VDN 10042. This VDN is mapped to vector **42**, shown below. The vector routes the call to **33000**, sending the call via Communication Manager Trunk Group 23 to Session Manager for the Sestek Voice Gateway.

change vector 42	Page 1 of 6
CALL VECTOR	
Number: 42 Name: PSTN Inbound to Translator	
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	2 secs hearing ringback
02 route-to	number 33000 cov n if unconditionally
03	
04	

The Voice Gateway generates a new call sent to the Communication Manager agent queue. In the example of the reference configuration, this was VDN 50101. This number is provisioned in the Sestek Scenario Designer, later on **Section 7**. The following vector 9 was invoked when VDN 50101 is called. The vector queues the call to skill group **1** to route the call to an available agent. If no agent is available it plays music to the caller until one becomes available.

change vector 9	Page 1 of 6
CALL VECTOR	
Number: 15 Name: basic queue	
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	2 secs hearing ringback
02 queue-to	skill 1 pri h
03 wait-time	60 secs hearing music
04 goto step	2 if unconditionally
05 stop	

The abbreviated screens below shows the sample Hunt Group (Skill) 1 used in the reference configuration. Note that **ISDN/SIP Caller Display** was set to **mbr-name**. With this setting, the specific number and name of the agent answering the call is sent on the PAI and Contact headers of responses and re-INVITES sent by Communication Manager. If the number and name of the agent group, and not the ones for the specific agent are preferred, set this field to **grp-name**.

change hunt-group 1	HUNT GROUP	Page 1 of 4
Group Number: 1	ACD? y	
Group Name: Agent Group	Queue? y	
Group Extension: 19991	Vector? y	
Group Type: ucd-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display: mbr-name		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

On the page 2 shown below, note **Skill** is set to **y**.

change hunt-group 1	HUNT GROUP	Page 2 of 4
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n	Service Level Target (% in sec): 80 in 20	
Measured: internal		
Supervisor Extension:		

The following screen illustrates an example agent-loginID 20001. In the sample configuration, agents logged in using agent-loginID 20001 through 20004, and the configured Password to staff and take calls for skill 1.

change agent-loginID 20001		Page 1 of 2
AGENT LOGINID		
Login ID: 20001	AAS? n	
Name: Agent 1	AUDIX? n	
TN: 1	Check skill TNs to match agent TN? n	
COR: 1		
Coverage Path: 1	LWC Reception: spe	
Security Code:	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		
ACW Agent Considered Idle: system		
Aux Work Reason Code Type: system		
Logout Reason Code Type: system		

The following abridged screen shows **Page 2** for agent-loginID 20001. Note that the Skill Number (SN) has been set to 1.

change agent-loginID 20001		Page 2 of 2
AGENT LOGINID		
Direct Agent Skill:	Service Objective? n	
Call Handling Preference: skill-level	Local Call Preference? n	
SN RL SL	SN RL SL	
1: 1 1	16:	31: 46:
2:	17:	32: 47:
3:	18:	33: 48:

6. Configure Avaya Aura® Session Manager

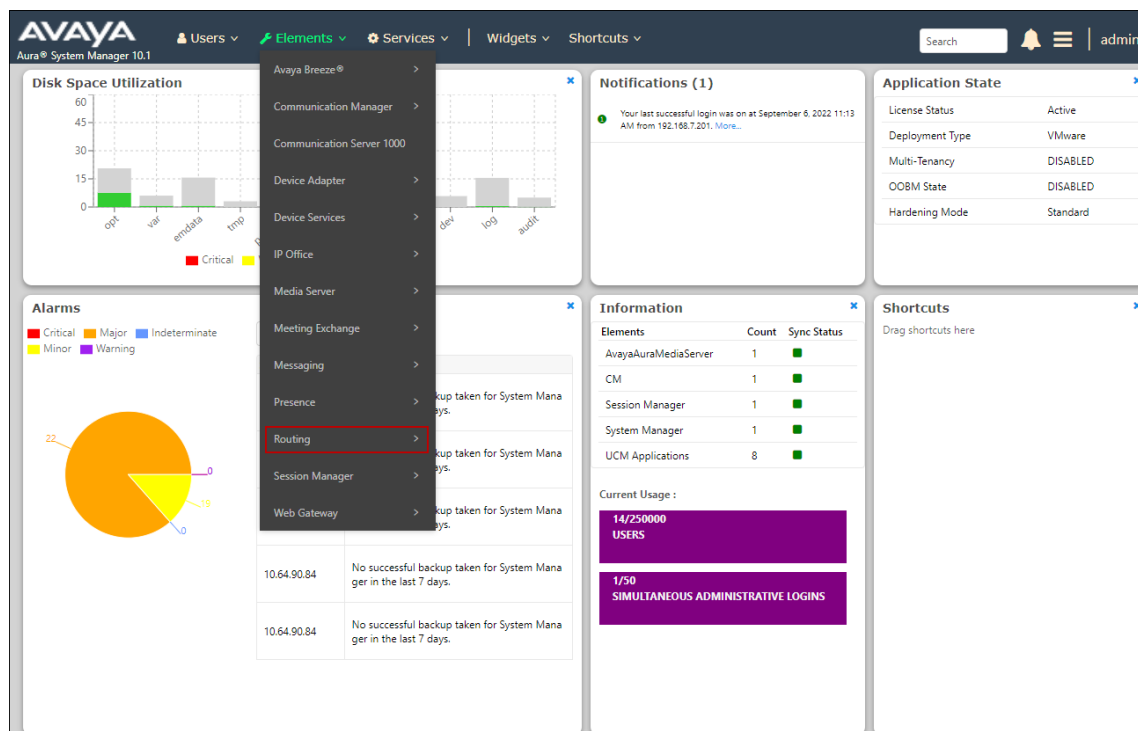
This section provides the procedures for configuring Session Manager. The procedure includes adding the following items:

- SIP Domain
- Locations
- SIP Entities for Communication Manager and Sestek Voice Gateway
- Entity Links, which defines the SIP trunk parameters used by Session Manager when routing calls to/from Communication Manager and Sestek Voice Gateway
- Routing Policies and Dial Patterns

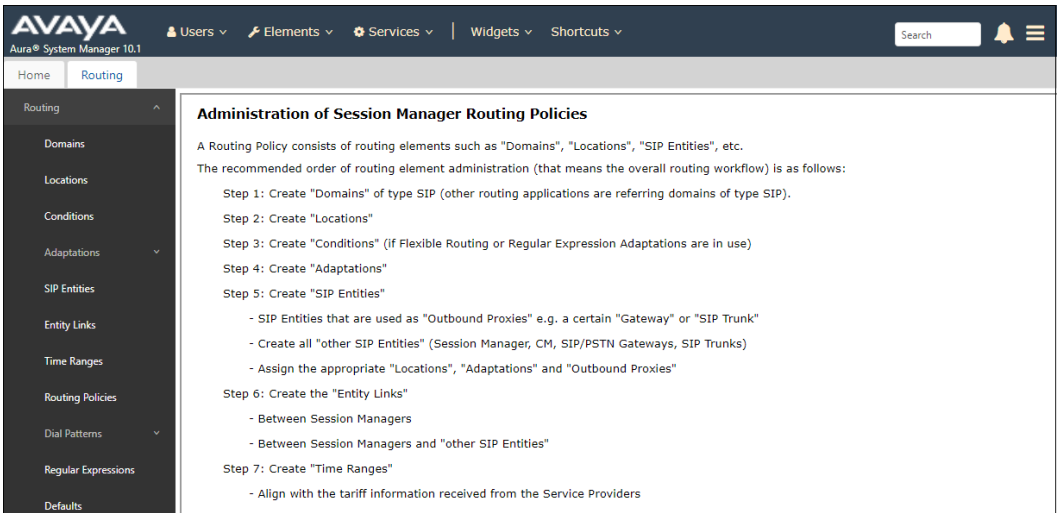
Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed. Consult the documentation in Additional References section for further details.

6.1. System Manager Login and Navigation

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**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in this section will be located under the **Routing** element shown below.



6.2. SIP Domain

Select **Domains** from the left navigation menu. In the reference configuration, domain **avayalab.com** was used. Click **New**. Enter the following values and use default values for remaining fields.

- **Name:** Enter the enterprise SIP Domain Name. In the sample screen below, **avayalab.com** is shown.
- **Type:** Verify **sip** is selected.
- **Notes:** Add a brief description.
- Click **Commit** (not shown) to save.



6.3. 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 – The customer site containing System Manager, Session Manager and other local servers and SIP endpoints.
- CM TG-23 – Communication Manager trunk group 23, designated for Sestek Voice Gateway calls.
- Knovvu Translator – Sestek Voice Gateway server location.

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 'Location Details' configuration page in the Avaya DevConnect Application. The left-hand navigation pane is expanded, showing the 'Routing' menu with 'Locations' selected. The main content area is titled 'Location Details' and includes a 'Commit' button and a 'Cancel' button. The configuration is organized into several sections:

- General:** Contains fields for 'Name' (set to 'Main') and 'Notes' (set to 'Avaya SIL').
- Dial Plan Transparency in Survivable Mode:** Includes an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field.
- Overall Managed Bandwidth:** Features a 'Managed Bandwidth Units' dropdown (set to 'Kbit/sec'), 'Total Bandwidth' and 'Multimedia Bandwidth' fields, and an 'Audio Calls Can Take Multimedia Bandwidth' checkbox (checked).
- Per-Call Bandwidth Parameters:** Includes fields for 'Maximum Multimedia Bandwidth (Intra-Location)' (2000 Kbit/Sec), 'Maximum Multimedia Bandwidth (Inter-Location)' (2000 Kbit/Sec), '* Minimum Multimedia Bandwidth' (64 Kbit/Sec), and '* Default Audio Bandwidth' (80 Kbit/sec).
- Alarm Threshold:** Includes an 'Overall Alarm Threshold' dropdown (set to 80 %).

6.3.2. CM-TG23 Location

To configure the Communication Manager Trunk Group 23 location, repeat the steps in **Section 6.3.1** with the following changes (not shown):

- **Name:** Enter a descriptive name for the Location (e.g., **CM TG-23**).

6.3.3. Knovvu Translator Location

To configure the Knovvu Translator Location, repeat the steps in **Section 6.3.1** with the following changes (not shown):

- **Name** – Enter a descriptive name (e.g., **Knovvu Translator**).

6.4. Adaptation

The Adaptation administered in this section is used to replace the host part on the origination headers of SIP messages to Communication Manager from the Sestek Voice Gateway, with the domain “avayalab.com” used on the enterprise.

In the **left** pane under **Routing**, click on **Adaptations**. In the **Adaptations** page, click on **New** (not shown). In the **Adaptation Details** page, enter:

- A descriptive **Name**, (e.g., **CM-TG23-Sestek**).
- Select **DigitConversionAdapter** from the **Module Name** drop down.
- Select **Name-Value Parameter** from the **Module Parameter Type** drop down:
 - **Name:** **fromto** **Value:** **true**
 - **Name:** **osrcd** **Value:** **avayalab.com**

Note – Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion.

The screenshot shows the 'Adaptation Details' configuration page. On the left is a sidebar with a 'Routing' menu containing 'Domains', 'Locations', 'Conditions', 'Adaptations' (highlighted), 'Regular Expressions', 'Device Mappings', 'SIP Entities', 'Entity Links', and 'Time Ranges'. The main area is titled 'Adaptation Details' and has 'Commit' and 'Cancel' buttons. Under the 'General' tab, the following fields are visible: 'Adaptation Name' (CM-TG23 Sestek), 'Notes' (Knovvu Translator), 'Module Name' (DigitConversionAdapter), 'Type' (digit), 'State' (enabled), and 'Module Parameter Type' (Name-Value Parameter). Below these is a table with 'Add' and 'Remove' buttons. The table has columns 'Name' and 'Value' and contains two rows: 'fromto' with value 'true' and 'osrcd' with value 'avayalab.com'. A 'Select' dropdown at the bottom of the table is set to 'All'.

Name	Value
fromto	true
osrcd	avayalab.com

6.5. SIP Entities

In this section, SIP Entities are administered for the following SIP network elements:

- Session Manager (**Section 6.5.1**) – This SIP Entity should be existing in the configuration, defined during the Session Manager installation.
- Communication Manager Trunk Group 23 (**Section 6.5.2**) – This entity, and its associated Entity Link (using TLS with port 5083), is for traffic between Communication Manager and Session Manager, designated specifically for calls to/from Sestek Voice Gateway.
- Sestek Voice Gateway (**Section 6.5.3**) – This entity, and its associated Entity Link (using UDP and port 5060), is for traffic between Session Manager and the Sestek Voice Gateway.

Note – In the reference configuration, TLS is used as the transport protocol between Session Manager and Communication Manager (ports 5083). The connection between Session Manager and the Sestek Voice Gateway uses UDP port 5060 per Sestek requirements.

6.5.1. Avaya Aura® Session Manager SIP Entity

This SIP Entity should be already existing in the configuration, defined during the Session Manager installation. It is shown here for completeness.

In the left pane under **Routing**, click on **SIP Entities**. The screen below shows the Session Manager SIP Entity details in the reference configuration:

- **Name** – A descriptive name (e.g., **Session Manager**).
- **FQDN or IP Address** – This is the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **10.64.91.85**).
- **Type** – Verify **Session Manager** is selected.
- **Location** – Select location **Main** (Section 6.3.1).
- **Outbound Proxy** – Leave blank.
- **Time Zone** – Select the time zone in which Session Manager resides.
- **Minimum TLS Version** – Select the TLS version, or select **Use Global Settings** to use the default TLS version, configurable at the global level (**Elements**→**Session Manager**→**Global Settings**).
- Default values were used for the remaining parameters.

SIP Entity Details Commit Cancel

General

* **Name:**

* **IP Address:**

SIP FQDN:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Minimum TLS Version:

Credential name:

Monitoring

SIP Link Monitoring:

CRLF Keep Alive Monitoring:

6.5.2. Avaya Aura® Communication Manager SIP Entity – Trunk Group 23

In the **SIP Entities** page, click on **New** (not shown). In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name** – Enter a descriptive name (e.g., **CM-TG23**).
- **FQDN or IP Address** – Enter the IP address of Communication Manager Processor Ethernet (procr) described in **Section 5.3** (e.g., **10.64.91.87**).
- **Type** – Select **CM**.
- **Adaptation** – Select the Adaptation **CM-TG23 Sestek** administered in **Section 6.4**.
- **Location** – Select the **CM-TG23** Location administered in **Section 6.3.2**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- Use the default values for the remaining parameters.
- Click on **Commit**.

SIP Entity Details Commit Cancel Help ?

General

* **Name:**

* **FQDN or IP Address:**

Type:

Notes:

Adaptation:

Location:

Time Zone:

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

Minimum TLS Version:

Credential name:

Securable: ☐

Call Detail Recording:

Loop Detection

Loop Detection Mode:

Loop Count Threshold:

Loop Detection Interval (in msec):

Monitoring

SIP Link Monitoring:

CRLF Keep Alive Monitoring:

6.5.3. Sestek Voice Gateway SIP Entity

Repeat the steps in **Section 6.5.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **Sestek Voice Gateway**).
- **FQDN or IP Address** – Enter the IP address of the Voice Gateway server (e.g., **10.64.160.11**).
- **Type** – Select **SIP Trunk**.
- **Location** – Select the **Knovvu Translator** location administered in **Section 6.3.3**.

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

General

* **Name:**

* **FQDN or IP Address:**

Type:

Notes:

Adaptation:

Location:

Time Zone:

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

Minimum TLS Version:

Credential name:

Securable: ☐

Call Detail Recording:

Loop Detection

Loop Detection Mode:

Loop Count Threshold:

Loop Detection Interval (in msec):

Monitoring

SIP Link Monitoring:

CRLF Keep Alive Monitoring:

6.6. Entity Links

In this section, Entity Links are administered for the following connections:

- Session Manager to Communication Manager Trunk Group 23 (**Section 6.6.1**).
- Session Manager to Knovvu Translator (**Section 6.6.2**).

Note – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages configured in **Section 6.5**.

6.6.1. Entity Link to Avaya Aura® Communication Manager Trunk Group

In the left pane under **Routing**, click on **Entity Links**, then click on **New** (not shown).

Continuing in the **Entity Links** page, provision the following:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g., **SM to CM-TG23**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 6.5.1** for Session Manager (e.g., Session Manager).
- **Protocol** – Select **TLS** (see **Section 5.6.1**).
- **SIP Entity 1 Port** – Enter **5083**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.2** for the Communication Manager trunk entity (e.g., **CM-TG23**).
- **SIP Entity 2 Port** – Enter **5083** (see **Section 5.6.1**).
- **Connection Policy** – Select **trusted**.
- Leave other fields as default.
- Click on **Commit**.

The screenshot shows the 'Entity Links' configuration page. On the left is a sidebar with a menu: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, and Entity Links (which is highlighted). The main area is titled 'Entity Links' and has 'Commit' and 'Cancel' buttons. Below the title is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, and Connection Policy. The row contains: 'SM to CM-TG23', 'Session Manager', 'TLS', '5083', 'CM-TG23', '5083', an unchecked 'DNS Override' checkbox, and 'trusted'. At the bottom of the table is a 'Select : All, None' dropdown.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
* SM to CM-TG23	* Session Manager	TLS	* 5083	* CM-TG23	* 5083	<input type="checkbox"/>	trusted

6.6.2. Entity Link to Knovvu Translator

To configure this Entity Link, repeat the steps in **Section 6.6.1**, with the following changes:

- **Name** – Enter a descriptive name for this link (e.g., **SM to Knovvu Translator**).
- **Protocol** – Select **UDP**.
- **SIP Entity 1 Port** – Enter **5060**.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.5.3** for the Sestek Voice Gateway entity (e.g., **Sestek Voice Gateway**).
- **SIP Entity 2 Port** – Enter **5060**.

The screenshot shows a web interface for configuring Entity Links. On the left is a sidebar with a menu containing: Routing, Domains, Locations, Conditions, Adaptations, SIP Entities, and Entity Links (which is highlighted in blue). The main content area is titled 'Entity Links' and includes 'Commit' and 'Cancel' buttons. Below the title is a table with 10 columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, and Connection Policy. A single row is displayed with the following values: Name: 'SM to Knovvu Translator', SIP Entity 1: 'Session Manager', Protocol: 'UDP', Port: '5060', SIP Entity 2: 'Sestek Voice Gateway', Port: '5060', DNS Override: 'checked', and Connection Policy: 'trusted'. Below the table is a search bar and a 'Select : All, None' option. A 'Filter: Enable' link is in the top right corner of the table area.

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
<input type="checkbox"/>	* SM to Knovvu Translator	* Session Manager	UDP	* 5060	* Sestek Voice Gateway	* 5060	<input checked="" type="checkbox"/>	trusted

6.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. In this section, the following Routing Policies are administered:

- Inbound calls to Knovvu Translator (**Section 6.7.1**).
- Inbound calls to Communication Manager Trunk Group 23 (**Section 6.7.2**).

6.7.1. Routing Policy for Calls to Knovvu Translator

This Routing Policy is used for calls from Session Manager to Knovvu Translator via the Sestek Voice Gateway. In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** (not shown).

- In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** (e.g., **To Knovvu Translator**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
- In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the **SIP Entities** list page will open (not shown) and select the SIP Entity administered in **Section 6.5.3** for the Sestek Voice Gateway. Click on **Commit**.

The screenshot shows the 'Routing Policy Details' page for a policy named 'To Knovvu Translator'. The left sidebar is under the 'Routing' section, with 'Routing Policies' selected. The main content area has a 'General' tab selected. In the 'General' section, the 'Name' field is 'To Knovvu Translator', 'Disabled' is unchecked, 'Retries' is '0', and 'Notes' is 'Calls to Translator'. Below this is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table. The table has columns for 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. One entry is visible: 'Sestek Voice Gateway' with FQDN '10.64.160.11' and Type 'SIP Trunk'. At the bottom, there is a 'Time of Day' section.

Name	FQDN or IP Address	Type	Notes
Sestek Voice Gateway	10.64.160.11	SIP Trunk	

6.7.2. Routing Policy for Calls to Communication Manager Trunk Group

This Routing Policy is used for calls from Session Manager to Communication Manager Trunk Group 23. Repeat the steps in **Section 6.7.1** with the following differences:

- Enter a descriptive **Name** (e.g., **To CM-TG23**).
- In the **SIP Entities** list page, select the SIP Entity administered in **Section 6.5.2** for the Communication Manager trunk (e.g., **CM-TG23**).

The screenshot shows the 'Routing Policy Details' page for a policy named 'To CM-TG23'. The left sidebar is under the 'Routing' section, with 'Routing Policies' selected. The main content area has a 'General' tab selected. In the 'General' section, the 'Name' field is 'To CM-TG23', 'Disabled' is unchecked, 'Retries' is '0', and 'Notes' is 'Calls from Translator'. Below this is the 'SIP Entity as Destination' section, which includes a 'Select' button and a table. The table has columns for 'Name', 'FQDN or IP Address', 'Type', and 'Notes'. One entry is visible: 'CM-TG23' with FQDN '10.64.91.87' and Type 'CM'. At the bottom, there is a 'Time of Day' section.

Name	FQDN or IP Address	Type	Notes
CM-TG23	10.64.91.87	CM	Knovvu Translator Calls

6.8. Dial Patterns

Dial patterns are defined to direct calls to the appropriate SIP Entity. In this section, Dial Patterns are administered matching the following calls:

- Communication Manager calls via Session Manager to Knovvu Translator (**Section 6.8.1**).
- Knovvu Translator calls via Session Manager to Communication Manager (**Section 6.8.2**).

6.8.1. Dial Pattern for Calls to Knovvu Translator

In the sample configuration, dial pattern 33000 was used to route inbound calls to the Sestek Voice Gateway.

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., **33000**).
- **Min** and **Max** – Minimum and maximum length of dialed number (e.g., **5**).
- **SIP Domain** – Select the enterprise SIP domain, e.g., **avayalab.com**.

Dial Pattern Details Commit Cancel Help ?

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

0 Items Filter: Enable

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

Denied Originating Locations

Add Remove


0 Items

Scroll down to the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page and click on **Add**.

- Under **Originating Location**, click the checkbox corresponding to the Communication Manager location for the trunk group used for Knovvu Translator calls, e.g., **CM-TG23**.
- In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to Knovvu Translator (e.g., **To Knovvu Translator**) and click on **Select** (not shown).

Originating Location


☐ Apply The Selected Routing Policies to All Originating Locations

15 Items  Filter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	Branch Location	
<input type="checkbox"/>	CM-TG1, TG11	CM trunk to Verizon
<input checked="" type="checkbox"/>	CM TG-23	CM trunk for Knovvu Translator calls
<input type="checkbox"/>	CM-TG4	CM Trunk 4 (Watson Assistant)
<input type="checkbox"/>	CM-TG5	CM Trunk to AT&T
<input type="checkbox"/>	CM TG7, TG17	CM Trunk to Simulated SIP Provider
<input type="checkbox"/>	CM-TG8	CM Trunk to UCI
<input type="checkbox"/>	Experience Portal	

Select : All, None Page 1 of 2

Routing Policies

22 Items  Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	Local calls to CM	<input type="checkbox"/>	Local Calls	Enterprise Traffic
<input type="checkbox"/>	To Aura Messaging	<input type="checkbox"/>	Aura Messaging	
<input type="checkbox"/>	To CM TG1	<input type="checkbox"/>	CM-TG1	Verizon IPT to CM via SM1
<input type="checkbox"/>	To CM-TG11	<input type="checkbox"/>	CM-TG11	Verizon IPT to CM via SM2
<input type="checkbox"/>	To CM-TG17	<input type="checkbox"/>	CM-TG17	Inbound from Sim. Provider via SM2
<input type="checkbox"/>	To CM TG2	<input type="checkbox"/>	CM-TG2	Trunk Group 2 VzIPCC to CM
<input type="checkbox"/>	To CM-TG23	<input type="checkbox"/>	CM-TG23	Calls from Translator
<input type="checkbox"/>	To CM TG5	<input type="checkbox"/>	CM-TG5	Trunk Group 5 AT&T to CM
<input type="checkbox"/>	To CM TG7	<input type="checkbox"/>	CM-TG7	Inbound from Sim Prov via SM1
<input type="checkbox"/>	To CM TG8	<input type="checkbox"/>	CM-TG8	Inbound Calls from Loopback
<input type="checkbox"/>	To Experience Portal	<input type="checkbox"/>	Experience Portal	
<input checked="" type="checkbox"/>	To Knovvu Translator	<input type="checkbox"/>	Sestek Voice Gateway	Calls to Translator
<input type="checkbox"/>	To Messaging	<input type="checkbox"/>	Avaya Messaging	

- Return to the **Dial Pattern Details** page and click on **Commit**.

6.8.2. Dial Pattern for Calls to Avaya Aura® Communication Manager

In the reference configuration, 50101 is the Communication Manager VDN number (Section 5.9) provisioned on the Sestek Scenario Designer (Section 7) to send calls from the Voice Gateway to the Communication Manager agents’ queue.

To add this 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., **50101**).
- **Min** and **Max** – Minimum and maximum length of dialed number (e.g., **5**).
- **SIP Domain** – Select **ALL**.

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Origination Dial Pat...

Dial Pattern Details

CommitCancel

Help

General

* Pattern:50101

* Min:5

* Max:5

Emergency Call:☐

SIP Domain:-ALL-

Notes:Calls from Knovvu Translator to CM

Originating Locations and Routing Policies

AddRemove

0 Items

Filter: Enable

☐

Originating Location Name

Originating Location Notes

Routing Policy Name

Rank

Routing Policy Disabled

Routing Policy Destination

Routing Policy Notes

Denied Originating Locations


AddRemove

Scroll down to the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page and click on **Add**.

- Under **Originating Location**, click the checkbox corresponding to the Sestek Voice Gateway location, e.g., **Knovvu Translator**.
- In the **Routing Policies** section, check the checkbox corresponding to the Routing Policy administered for routing calls to Communication Manager for Knovvu Translator calls (e.g., **To CM-TG23**) and click on **Select** (not shown).

Originating Location


☐ Apply The Selected Routing Policies to All Originating Locations

15 Items  Filter: Enable

<input type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	Knovvu Translator	Sestek Voice gateway
<input type="checkbox"/>	Main	Avaya SIL
<input type="checkbox"/>	Remote Access	Remote Workers Access from SBCE-90
<input type="checkbox"/>	SBC-AEC	SBC to Avaya Enterprise Cloud
<input type="checkbox"/>	SBC-AXP	SBC to MPC-AXP
<input type="checkbox"/>	SBCs	
<input type="checkbox"/>	UCSP	UCSP SIP Gateway

Select : All, None Page 2 of 2

Routing Policies

22 Items  Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	Local calls to CM	<input type="checkbox"/>	Local Calls	Enterprise Traffic
<input type="checkbox"/>	To Aura Messaging	<input type="checkbox"/>	Aura Messaging	
<input type="checkbox"/>	To CM TG1	<input type="checkbox"/>	CM-TG1	Verizon IPT to CM via SM1
<input type="checkbox"/>	To CM-TG11	<input type="checkbox"/>	CM-TG11	Verizon IPT to CM via SM2
<input type="checkbox"/>	To CM-TG17	<input type="checkbox"/>	CM-TG17	Inbound from Sim. Provider via SM2
<input type="checkbox"/>	To CM TG2	<input type="checkbox"/>	CM-TG2	Trunk Group 2 VzIPCC to CM
<input checked="" type="checkbox"/>	To CM-TG23	<input type="checkbox"/>	CM-TG23	Calls from Translator
<input type="checkbox"/>	To CM TG5	<input type="checkbox"/>	CM-TG5	Trunk Group 5 AT&T to CM
<input type="checkbox"/>	To CM TG7	<input type="checkbox"/>	CM-TG7	Inbound from Sim Prov via SM1
<input type="checkbox"/>	To CM TG8	<input type="checkbox"/>	CM-TG8	Inbound Calls from Loopback

- Return to the **Dial Pattern Details** page and click on **Commit**.

7. Knovvu Virtual Translator Configuration

The Sestek Knovvu Virtual Translator solution tested consists of the Sestek Voice Gateway, running on a Windows Server at the enterprise site, and a Sestek API Translator Server in the Sestek cloud.

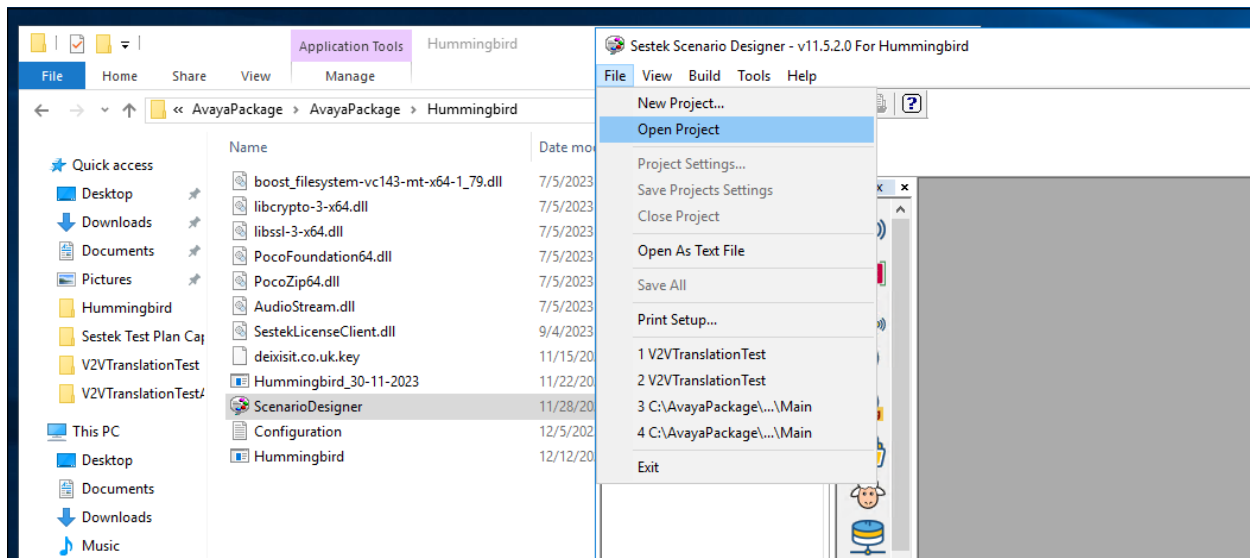
Configuration of the Sestek solution, including installation and provisioning of the Sestek Voice Gateway on a Windows server at the customer's enterprise is performed by Sestek support personnel, and it is not described in these Application Notes.

For illustration purposes, the following settings are noted, as they were provisioned on the Hummingbird configuration file (<root directory>/ Hummingbird/ Configuration.txt) in the reference configuration used for the tests:

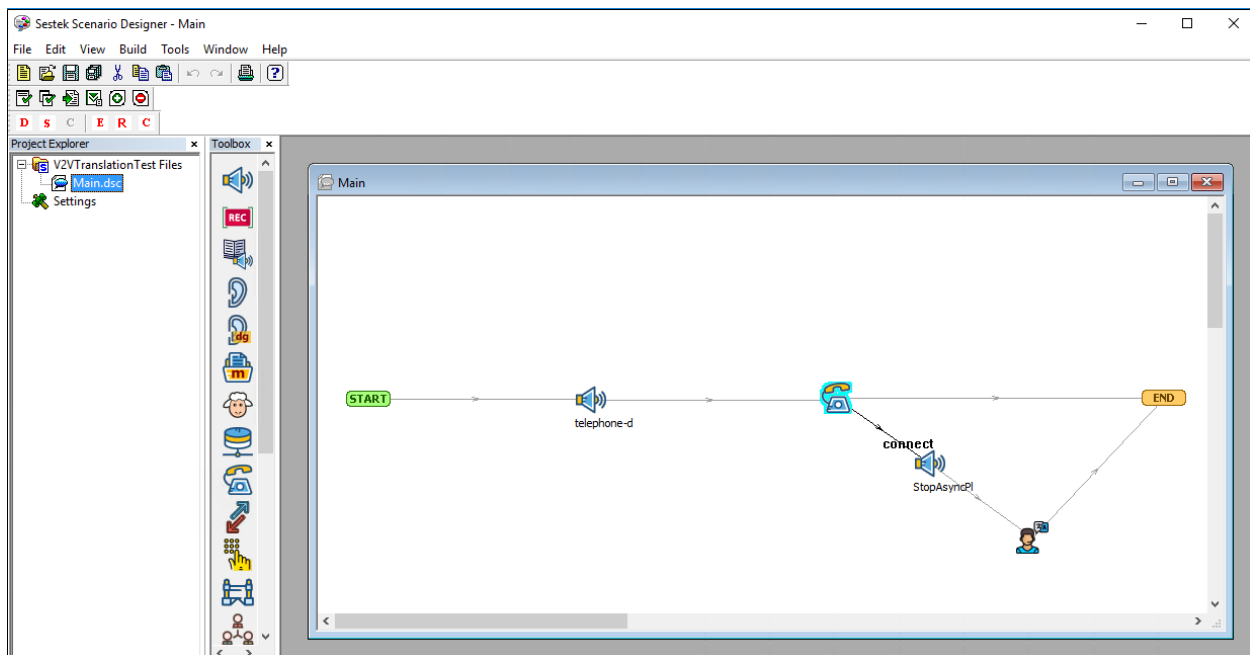
- **SipBindAddress=10.64.160.11** (IP address of the Windows server)
- **CallRequestIp=10.64.160.11**
- **SipBindPort=5060** (left at default value)
- **LocalRtpPortRange=24000-26000** (left at default value)
- **Extension=Number=;Count=10;Scenario="C:\AvayaPackage\AvayaPackage\V2VTranslationTest\V2VTranslationTest.ddp"**
 - On this line removed the default text after "Extension=Number=" to allow inbound calls from any number
 - Changed the "Count" value from 1 to 10 to allow 10 concurrent calls.
 - Changed the "Scenario" path from the default to the correct path to the V2VTranslationTest.ddp file:
"C:\AvayaPackage\AvayaPackage\V2VTranslationTest\V2VTranslationTest.ddp"
- The following line was added:
SendReplyToContactHeaderEndpoint=false
This was necessary to prevent the Voice Gateway from sending responses directly to the IP address present on the Contact header of the incoming INVITE. With this change the responses are sent to Session Manager as expected..

The Sestek Scenario Designer was used to set the number used to reach the Communication Manager agent/skill extension, as well as the translation Activation Sequence used by the agents to start translation on an active call.

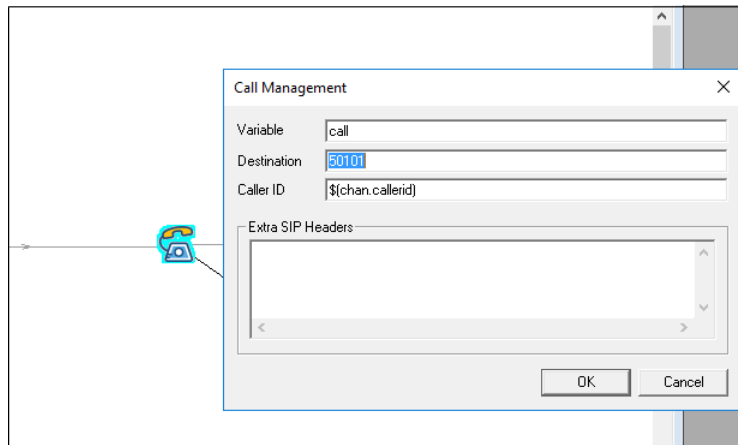
Double click **ScenarioDesigner** on the Hummingbird folder. Select **File → Open Project**.



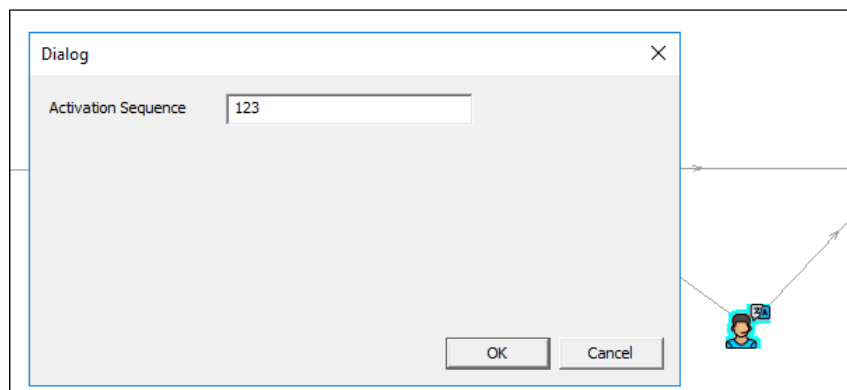
Select the **V2VTranslationTest** project and expand it. Double click **Main.dsc**



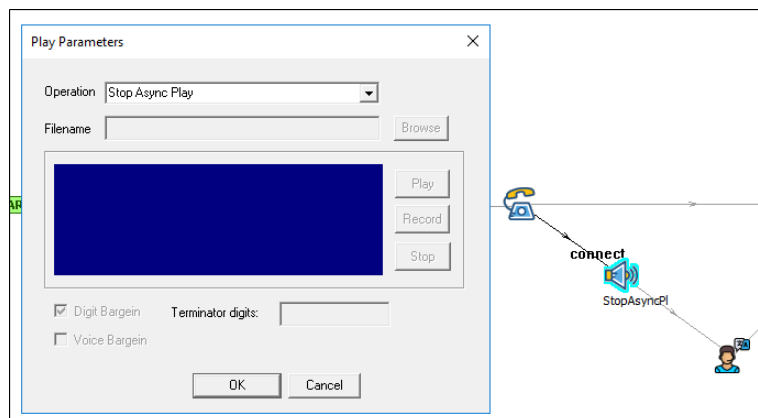
Double click the telephone icon and enter the Communication Manager extension on the Destination field, e.g., **50101**.



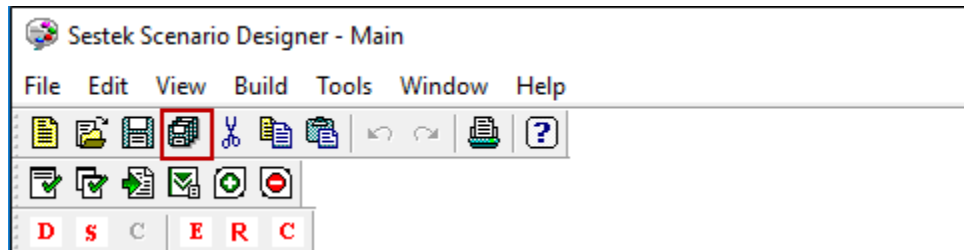
Double click the agent icon to set the translation **Activation Sequence**.



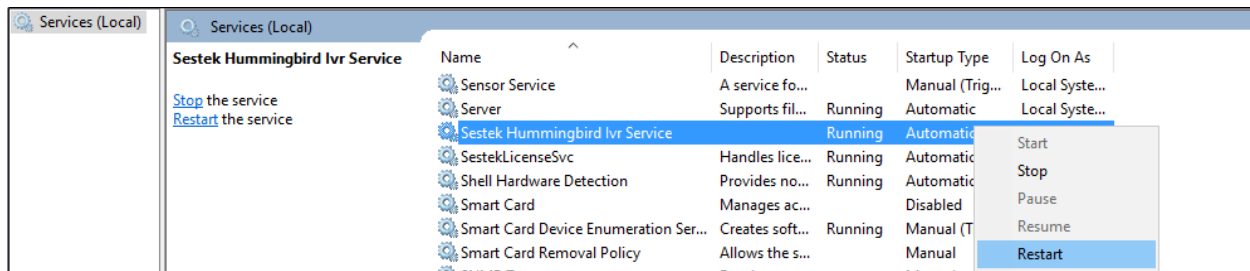
A Toolbox Play function was added with **Operation** set to **Stop Async Play** on the line between the telephone and agent icons. With this setting, if the activation code has not been pressed by the agent, the audio is bridged between the inbound and outbound calls without any delay.



Save the configuration once done making the changes.



Restart the Sestek Hummingbird Service.



8. Verification Steps

Complete the following general steps to verify correct functionality of the Avaya configuration with the Sestek Knovvu Virtual Translator.

- Place a call from the PSTN or from an enterprise extension to the number assigned to the translator.
- Session Manager routes the call to the Sestek Voice Gateway via a SIP trunk.
- The Sestek Voice Gateway answers the inbound call, and it generates a new call, sent via Session Manager to the Communication Manager VDN and vector associated with the agents.
- Caller hears announcement and music if agent is not available.
- An agent answers the call and interacts with the caller.
- Caller speaks on a different language
- Agent presses the translation activation sequence on the agent's telephone to start the translations.
- Voice is translated in both directions, to the correct language used by caller and agent.
- Caller and agent hear music during the time intervals while the voice is being processed and translated by the Sestek servers.
- Agent or caller terminates the call.

8.1. Avaya Aura® Communication Manager Verification

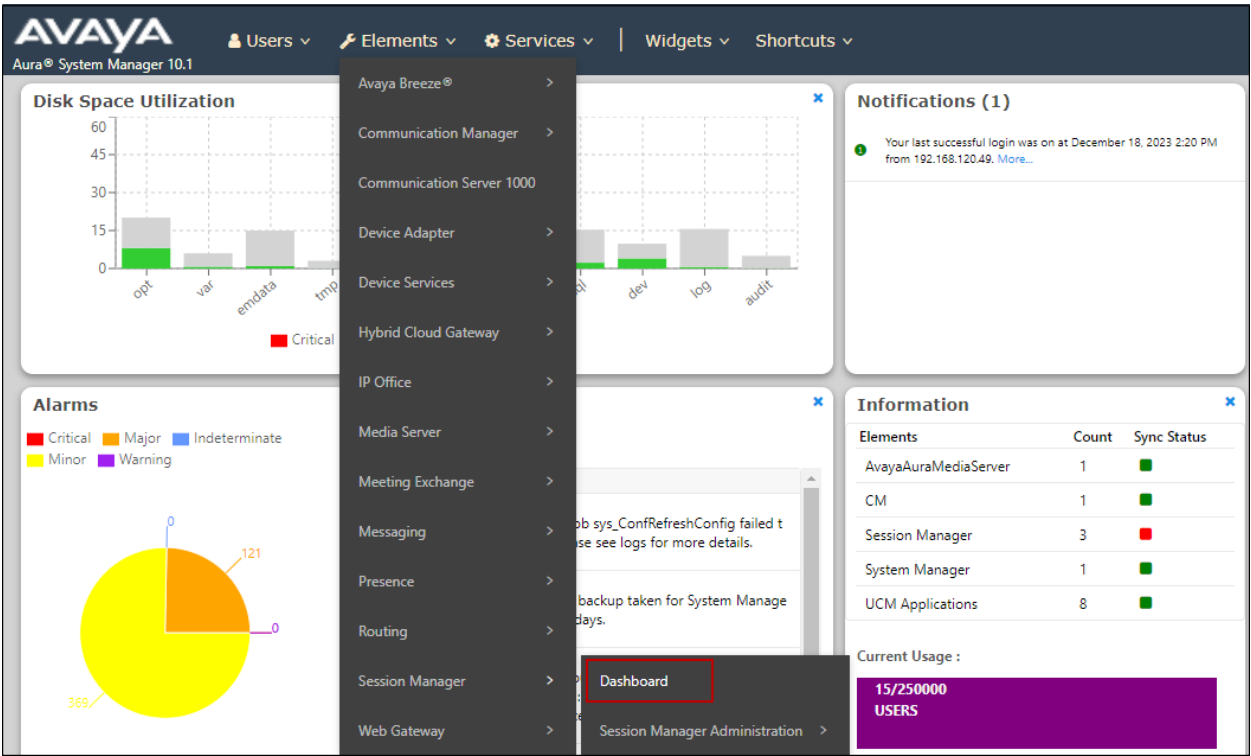
The following commands can be entered in the Communication Manager SAT terminal to verify and troubleshoot the solution functionality:

- **list trace station** <extension number>
Traces calls to and from a specific station.
- **list trace tac** <trunk access code number>
Trace calls over a specific trunk group.
- **list trace vdn** <vdn number>
Trace call processing over a specific vdn.
- **list trace vector** <vector number>
Trace call processing over a specific vector.
- **status signaling-group** <signaling group number>
Displays signaling group service state.
- **status trunk** <trunk group number>
Displays trunk group service state.
- **status station** <extension number>
Displays signaling and media information for an active call on a specific station.

8.2. Avaya Aura® Session Manager Verification

The Session Manager configuration may be verified via System Manager.

Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, select **Elements → Session Manager → Dashboard**.



The **Session Manager Dashboard** is displayed. Note that the **Test Pass**, **Alarms**, **Service State** and **Data Replication** columns all show good status.

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Service State Shutdown System EASG Clear Logs As of 1:37 PM

3 Items Show All Filter: Enable

	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Load Factor	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	EASG	Profile	Version
<input type="checkbox"/>	Session Manager	Core	✓	0/0/0	Up	Accept New Service	0/-- -/---	2/23	0	2/0	✓	✓	Normal	Enabled	1	10.1.3.1.1013103

Select : All, None

Clicking the entry under the **Entity Monitoring** column brings up the **Session Manager Entity Link Connection Status** page. Verify that the state of the Session Manager links of interest, to Communication Manager and the Sestek Voice Gateway under the **Conn. Status** and **Link Status** columns is **UP**, like shown on the screen below.

Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

Status Details for the selected Session Manager:

All Entity Links for Session Manager: Session Manager

Summary View

23 Items Filter: Enable

	SIP Entity Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	CM-TG6	IPv4	10.64.91.87	5066	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG5	IPv4	10.64.91.87	5065	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Avaya Messaging	IPv4	10.64.19.90	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG1	IPv4	10.64.91.87	5081	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	SBC-AEC	IPv4	10.64.160.31	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG8	IPv4	10.64.91.87	5068	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	SBC-1	IPv4	10.64.91.50	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	CM-TG23	IPv4	10.64.91.87	5083	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Local Calls	IPv4	10.64.91.87	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	Sestek Voice Gateway	IPv4	10.64.160.11	5060	UDP	FALSE	UP	200 OK	UP

Select : None Page 1 of 2

Other Session Manager useful verification and troubleshooting tools include:

- **traceSM** – Session Manager command line tool for traffic analysis. Log in to the Session Manager command line management interface to run this command.

8.3. Sestek Knovvu Virtual Translator Verifications

The following tools can be used on the Sestek Voice Gateway to verify and troubleshoot the solution functionality:

- Activity log files, stored on the “logs” folder in the Sestek root directory.
- Packet capture tool (e.g. Wireshark) can be installed on the Windows server to capture the calls.

9. Conclusion

These Application Notes describe the configuration steps required to integrate Sestek Knovvu Virtual Translator 11.5 with Avaya Aura® Session Manager 10.1 and Avaya Aura® Communication Manager 10.1. All test cases passed with the observation notes on **Section 2.2**.

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] *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

©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.