



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Frequentis AG 3020 LifeX with Avaya Aura® Communication Manager and Avaya Aura® Session Manager using Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning 3020 LifeX V3.5 from Frequentis to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 using Avaya Session Border Controller for Enterprise R8.1.2 to connect to an Oracle Session Border Controller provided by Frequentis.

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 DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps for provisioning 3020 LifeX V3.5 from Frequentis to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 using Avaya Session Border Controller for Enterprise R8.1.2 to connect to an Oracle Session Border Controller provided by Frequentis.

The Frequentis 3020 LifeX (LifeX) is an Integrated Communication Control System that is used by emergency service customers for communicating between control rooms and the front line NHS Ambulance service responders and then from the same application using radio communication (TETRA digital radio or analogue PMR) to pass details to mobile resources.

As a radio dispatch deployment with basic PTN/PSTN the LifeX acts as an end Private Branch Exchange (PBX) and performs call prioritisation and distribution to LifeX operators as defined by the profile in which they have logged in to the LifeX application. In this type of configuration, the LifeX has one primary connection to the Avaya Solution, a SIP connection to Avaya Aura® Session Manager. The LifeX supports basic call control including hold and transfer.

Some of the acronyms that will be used throughout this document are as follows.

- **UDP:** User Datagram Protocol (UDP) – a communications protocol that facilitates the exchange of messages between computing devices in a network. It's an alternative to the transmission control protocol (TCP).
- **TCP:** TCP/IP, in full Transmission Control Protocol/Internet Protocol, standard Internet communications protocols that allow digital computers to communicate over long distances.
- **TLS:** Transport Layer Security (TLS) is the successor protocol to SSL. TLS is an improved version of SSL. It works in much the same way as the SSL, using encryption to protect the transfer of data and information.
- **SIP:** Session Initiation Protocol and refers to a TCP/IP-based network protocol which can be used to establish and control communication connections of several subscribers. SIP is often used in Voice-over-IP telephony to establish the connection for telephone calls.
- **H.323:** H. 323 is an ITU Telecommunication Standardization Sector (ITU-T) recommendation that describes protocols for the provision of audio-visual (A/V) communication sessions on all packet networks. H. 323 is widely used in IP based videoconferencing, Voice over Internet Protocol (VoIP) and Internet telephony.
- **PSTN:** “Public Switched Telephone Network”, and it refers to the world's oldest collection of interconnected communication solutions – both government, and commercially-owned. Some people also refer to this communications option as the “Plain Old Telephone Service”, or POTS.
- **PBX:** Private Branch eXchange and has become a general term used to describe a business telephone system that offers multiple inbound and outbound lines, call routing, voicemail, and call management features.
- **CM:** Avaya Aura® Communication Manager.
- **SM:** Avaya Aura® Session Manager.

- **ASBCE:** Avaya Session Border Controller for Enterprise or Avaya SBCE.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of LifeX operators to make and receive calls to and from Communication Manager endpoints. Calls from a simulated PSTN were routed to Communication Manager endpoints and were then transferred to LifeX operators as well as routing PSTN calls directly to LifeX. The connection between LifeX and Session Manager is facilitated by a Session Border Controller on each side, this is outlined in **Section 3**.

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 the Avaya Session Border Controller for Enterprise and LifeX made use of a TLS connection, however the RTP between the Avaya SBCE and LifeX was not secure as requested by Frequentis.

2.1. Interoperability Compliance Testing

The compliance testing included the test scenarios shown below. Note that when applicable, all tests were performed with Avaya SIP, H.323 and Digital endpoints.

- **Basic calls between Communication Manager and LifeX** – Test calls between the Avaya platform and the LifeX platform, these are basic calls that involve no transfers.
- **Hold/Transfer/Conference calls between Communication Manager and LifeX** – Test the hold and transfer functions to/from the LifeX platform.
- **Simulated PSTN calls to and from Life X** – Calls to and from LifeX from a simulated PSTN.
- **Test calls with CM Shuffling on and off** – Calls are made using a Direct Media path between Avaya endpoints and with the initial media path on the Media Server/Gateway that then shuffles off to the IP endpoints.
- **CODEC testing** – Testing using different codecs on Communication Manager.
- **DTMF** – Testing the DTMF using a voicemail system.

- **LifeX Features** – Calls were made to specific LifeX roles that utilized features on the LifeX platform.
- **Serviceability Tests** – Observations on call flow when a LAN failure occurs.

Note: Compliance testing does not include redundancy testing as standard. Where some LAN failures were simulated, and the results observed, there were no redundancy or failover tests performed.

2.2. Test Results

Tests were performed to verify interoperability between LifeX operators and Communication Manager endpoints. All test cases passed with the following observations noted.

1. The SIP trunk on Communication Manager was configured to use the From header for the Identity for Calling Party Display, see **Section 5.5**.
2. Topology Hiding was used to ensure that all calls to LifeX were in the format ext@domain, see **Section 7.10**.
3. When calling from Avaya H.323 endpoints the display shows information from the CONTACT header received from LifeX. Initially this was set by the Oracle SBC by overwriting the Contact Header and testing was carried out using this setup. This was then changed to have LifeX send out the “role number” in the Contact header and some regression testing was carried out successfully using that setup, thus eliminating the need for the Oracle SBC to make any changes to the Contact header.
4. When Avaya transfers LifeX caller to another Avaya phone the LifeX callers display is not updated with the new CLID info. Scenario – LifeX calls to CM1 and CM1 transfers LifeX to CM2. LifeX should show CM2 number on the display but continues to show CM1. SIP Updates are not supported in LifeX release 3.5 but will be supported in future releases.
5. When an Avaya user transfers LifeX caller back to another LifeX caller, the display on both LifeX callers should be updated to show each other’s CLID on the display, however the CLID of the CM phone is displayed on both. SIP Updates are not supported in LifeX release 3.5 but will be supported in future releases.
6. There is no MOH or Announcement played to the Avaya party when the LifeX places the caller on hold. This only occurs when it is LifeX that initiates the original call. This will be configurable in future releases of LifeX.
7. G.722 or G723 codecs were not utilized between the Avaya and LifeX. G.711A, G.711U and G.729 are the only supported codecs on LifeX currently.

2.3. Support

Technical support for the Frequentis AG 3020 LifeX can be obtained as follows:

- Web: <https://www.frequentis.com/en/contact-us>

3. Reference Configuration

Figure 1 shows the setup for compliance testing Frequentis's LifeX with Communication Manager and Session Manager using SIP signalling over SIP trunks to pass calls from Communication Manager to the LifeX Operators. There are two Session Border controllers each side of the solution, these are designed as Firewalls and simply pass the SIP messages through them onto each relevant destination.

A VPN connection was established between the Session Border Controllers as they are on the edge of each platform. This VPN connection was to facilitate testing between labs in London and Galway but would not necessarily be part of a typical setup.

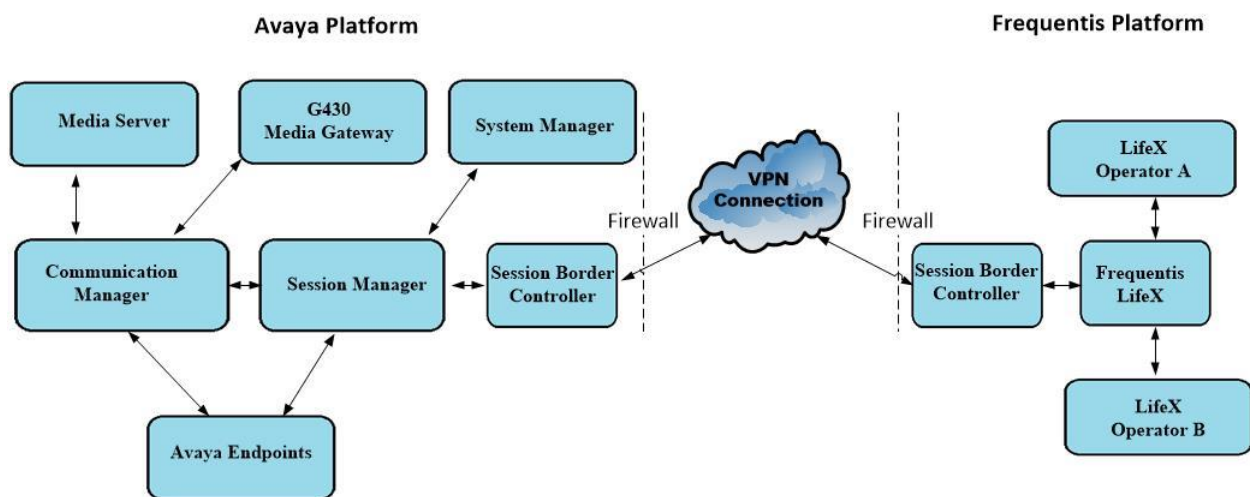


Figure 1: Connection of Frequentis LifeX with Avaya Aura® Communication Manager R8.1, Avaya Aura® Session Manager R8.1 and Avaya Session Border Controller for Enterprise R8.1.2

4. Equipment and Software Validated

The following equipment and software were used for the compliance test.

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	8.1.3.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.0.1011784 Feature Pack 3
Avaya Aura® Session Manager running on a virtual server	8.1.3 Build No. – 8.1.3.0.813014
Avaya Aura® Communication Manager running on a virtual server	8.1.3 – FP3 R018x.01.0.890.0 Update ID 01.0.890.0-26568
Avaya Session Border Controller for Enterprise	8.1.2.0-31-19809
Avaya Aura® Media Server	8.0.2.138
Avaya G450 Media Gateway	40.20.0/2
Avaya J179 H.323 Deskphone	6.8304
Avaya J189 SIP Deskphone	4.0.7.0.7
Avaya 9404 Digital Phone	2.00
Frequentis LifeX 3020 ORACLE Enterprise Session Border Controller	3.5.13.4 8.3.0

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing with SIP trunks in place to Session Manager. For further information on the configuration of Communication Manager please see **Section 11** of these Application Notes.

The configuration operations described in this section can be summarized as follows:

- Verify System Parameters Customer Options.
- System Features and Access Codes.
- Administer Dial Plan.
- Administer Route Selection for calls to LifeX.
- Configure SIP Trunk.

Note: The configuration of PSTN trunks and routes are outside the scope of these Application Notes.

5.1. Verify System Parameters Customer Options

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that **Maximum Administered SIP Trunks** has sufficient capacity. Calls that are transferred across the link between the two systems use two SIP trunks for the full duration of the call.

display system-parameters customer-options		Page	2 of 12
OPTIONAL FEATURES			
IP PORT CAPACITIES	USED		
Maximum Administered H.323 Trunks:	12000	250	
Maximum Concurrently Registered IP Stations:	18000	2	
Maximum Administered Remote Office Trunks:	12000	0	
Maximum Concurrently Registered Remote Office Stations:	18000	0	
Maximum Concurrently Registered IP eCons:	414	0	
Max Concur Registered Unauthenticated H.323 Stations:	100	0	
Maximum Video Capable Stations:	18000	0	
Maximum Video Capable IP Softphones:	18000	0	
Maximum Administered SIP Trunks:	24000	319	
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0	

On **Page 4**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

display system-parameters customer-options		Page	4 of 12
OPTIONAL FEATURES			
Abbreviated Dialing Enhanced List?	y	Audible Message Waiting?	y
Access Security Gateway (ASG)?	n	Authorization Codes?	y
Analog Trunk Incoming Call ID?	y	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01?	y	CAS Main?	n
Answer Supervision by Call Classifier?	y	Change COR by FAC?	n
	ARS? y	Computer Telephony Adjunct Links?	y
	ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net?	y
ARS/AAR Dialing without FAC?	y	DCS (Basic)?	y

On **Page 6**, ensure that **Uniform Dialing Plan** is set to **y**.

display system-parameters customer-options		Page	6 of 12
OPTIONAL FEATURES			
Multinational Locations?	n	Station and Trunk MSP?	y
Multiple Level Precedence & Preemption?	n	Station as Virtual Extension?	y
Multiple Locations?	n	System Management Data Transfer?	n
Personal Station Access (PSA)?	y	Tenant Partitioning?	y
PNC Duplication?	n	Terminal Trans. Init. (TTI)?	y
Port Network Support?	y	Time of Day Routing?	y
Posted Messages?	y	TN2501 VAL Maximum Capacity?	y
		Uniform Dialing Plan? y	
Private Networking?	y	Usage Allocation Enhancements?	y

5.2. System Features and Access Codes

For the testing, **Trunk-to Trunk Transfer** was set to **all** on **Page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction). See **Section 11** for supporting documentation.

display system-parameters features		Page	1 of 19
FEATURE-RELATED SYSTEM PARAMETERS			
Self Station Display Enabled?	n		
	Trunk-to-Trunk Transfer: all		
Automatic Callback with Called Party Queuing?	n		
Automatic Callback - No Answer Timeout Interval (rings):	3		
Call Park Timeout Interval (minutes):	10		
Off-Premises Tone Detect Timeout Interval (seconds):	20		
AAR/ARS Dial Tone Required?	y		
Music (or Silence) on Transferred Trunk Calls?	no		
DID/Tie/ISDN/SIP Intercept Treatment:	attd		
Internal Auto-Answer of Attd-Extended/Transferred Calls:	transferred		
Automatic Circuit Assurance (ACA) Enabled?	n		
Abbreviated Dial Programming by Assigned Lists?	n		
Auto Abbreviated/Delayed Transition Interval (rings):	2		
Protocol for Caller ID Analog Terminals:	Bellcore		
Display Calling Number for Room to Room Caller ID Calls?	n		

Use the **display feature-access-codes** command to verify that a FAC (feature access code) has been defined for both AAR and ARS. Note that **8** is used for AAR and **9** for ARS routing.

display feature-access-codes	Page 1 of 10
FEATURE ACCESS CODE (FAC)	
Abbreviated Dialing List1 Access Code:	
Abbreviated Dialing List2 Access Code:	
Abbreviated Dialing List3 Access Code:	
Abbreviated Dial - Prgm Group List Access Code:	
Announcement Access Code:	
Answer Back Access Code:	
Attendant Access Code:	
Auto Alternate Routing (AAR) Access Code: 8	
Auto Route Selection (ARS) - Access Code 1: 9	Access Code 2:
Automatic Callback Activation: *25	Deactivation: #25

5.3. Administer Dial Plan

It was decided for compliance testing that all calls beginning with 700x with a total length of 4 digits were to be sent across the SIP trunk to LifeX via Session Manager and ASBCE. In order to achieve this, automatic alternate routing (aar) would be used to route the calls. The dial plan and aar routing analysis need to be changed to allow this.

Type **change dialplan analysis** in order to make changes to the dial plan. Ensure that **700** is added with a **Total Length** of **4** and a **Call Type** of **udp**.

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
4	4	udp						
5	5	udp						
6	4	ext						
700	4	udp						
9	1	fac						
*	3	fac						

5.4. Administer Route Selection for calls to LifeX

As digits 7001 to 7009 (700x) were defined in the dial plan as udp (**Section 5.3**) use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **700x** that are **4** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

change uniform-dialplan 5						Page 1 of 2	
UNIFORM DIAL PLAN TABLE							
						Percent Full: 0	
Matching			Insert			Node	
Pattern	Len	Del	Digits	Net	Conv	Num	
700	4	0		aar	n		
					n		

Use the **change aar analysis x** command to further configure the routing of the dialed digits. Calls to LifeX begin with **700x** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 12**, which contains the outbound SIP Trunk Group.

change aar analysis 7						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	
700	4	4	12	aar		n	

Use the **change route-pattern n** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Pattern Number 12** is used to route calls to trunk group (**Grp No**) **12**, this is the SIP Trunk configured in **Section 5.5**. Other settings such as **FRL** and **Numbering Format** can be seen below.

change route-pattern 12										Page 1 of 4	
Pattern Number: 12										Pattern Name: SIP-Trunk-Out	
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:	12	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	unre		lev0-pvt	none
2:	y	y	y	y	y	n	n	rest			none
3:	y	y	y	y	y	n	n	rest			none
4:	y	y	y	y	y	n	n	rest			none
5:	y	y	y	y	y	n	n	rest			none
6:	y	y	y	y	y	n	n	rest			none

5.5. Configure SIP Trunk

In the Node Names IP form, note the IP Address of the **procr** and the Session Manager (**sm81vmpg**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

display node-names ip		IP NODE NAMES
Name	IP Address	
AMS80vmpg	10.10.40.61	
G450	10.10.40.14	
IPOffice	10.10.40.25	
NRS	10.10.40.101	
PGDECT	10.10.40.50	
sm81vmpg	10.10.40.32	
SM_Oceana	10.10.41.26	
aes81vmpg	10.10.40.56	
default	0.0.0.0	
procr	10.10.40.37	
(16 of 18 administered node-names were displayed)		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager in **Section 6.1**. In this configuration, the domain name is **devconnect.local**. The **IP Network Region** form also specifies the **Codec Set** to be used. This codec set will be used for calls routed over the SIP trunk to Session manager as **ip-network region 1** is specified in the SIP signaling group.

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

In the **IP Media Parameters** form, select the audio codec's supported for calls routed over the SIP trunk to Communications Portal. The form is accessed via the **display ip-codec-set n** command or if a change were needed to be made type change ip-codec-set n. Note that IP codec set 1 was specified in IP Network Region 1 shown on the previous page. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), **G.711U** (mu-law), and **G.729** which are supported by LifeX.

Media Encryption is used on the Avaya sets where possible these use **srtp-aescm128-hmac80** media encryption. **None** is also present to facilitate any devices that do not support media encryption.

display ip-codec-set 1
Page 1 of 2

IP MEDIA PARAMETERS

Codec Set: 1

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

Media Encryption
 1: **1-srtp-aescm128-hmac80**
 2: **none**
 3:
 4:
 5:

Encrypted SRTCP: enforce-unenc-srtcp

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the desired transport method, for compliance testing this was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively.
- Set the **Near-end Node Name** to **procr**.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm81vmpg**).
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured previously. This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- Leave the **Far-end Domain** field blank to allow Communication Manager to accept any domain.
- The **Direct IP-IP Audio Connections** field is set to **y**. This is to turn 'shuffling' on.
- The default values for the other fields may be used.

Note: During Compliance testing a selection of complex calls including blind transfers were carried out with the **Initial IP-IP Direct Media** field is set to **y**. This was to ensure that no issues would arise with this set for early media.

change signaling-group 12		Page 1 of 3
SIGNALING GROUP		
Group Number: 12	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? n	
Peer Detection Enabled? y	Peer Server: SM	Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
Alert Incoming SIP Crisis Calls? n		
Near-end Node Name: procr	Far-end Node Name: sm81vmpg	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain:		
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	
	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for all incoming and outgoing SIP calls to Session Manager SIP Entities including the Avaya SBCE. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie** (this may vary depending on the site in question). Specify the signaling group associated with this trunk group in the **Signaling Group** field and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

change trunk-group 12		Page 1 of 4	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: SIPTRUNK-OUT	COR: 1	TN: 1	TAC: *812
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 12	
		Number of Members: 10	

On **Page 2** of the trunk-group form the following values were used for compliance testing.

change trunk-group 12		Page 2 of 4	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
Redirect On OPTIM Failure: 5000			
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 600			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n			
Caller ID for Service Link Call to H.323 1xC: station-extension			

On **Page 3** of the trunk-group form the following values were used for compliance testing. The **Numbering Format** was set to **private**.

change trunk-group 12	Page 3 of 4
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Suppress # Outpulsing? n	Numbering Format: private
	UUI Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Hold/Unhold Notifications? y
	Modify Tandem Calling Number: no
Show ANSWERED BY on Display? y	
DSN Term? n	

Settings on **Page 4** are as follows. **Send Transferring Party Information** is set to **y** and **Identity for Calling Party Display** is set to **From**. The other settings should be set as shown below.

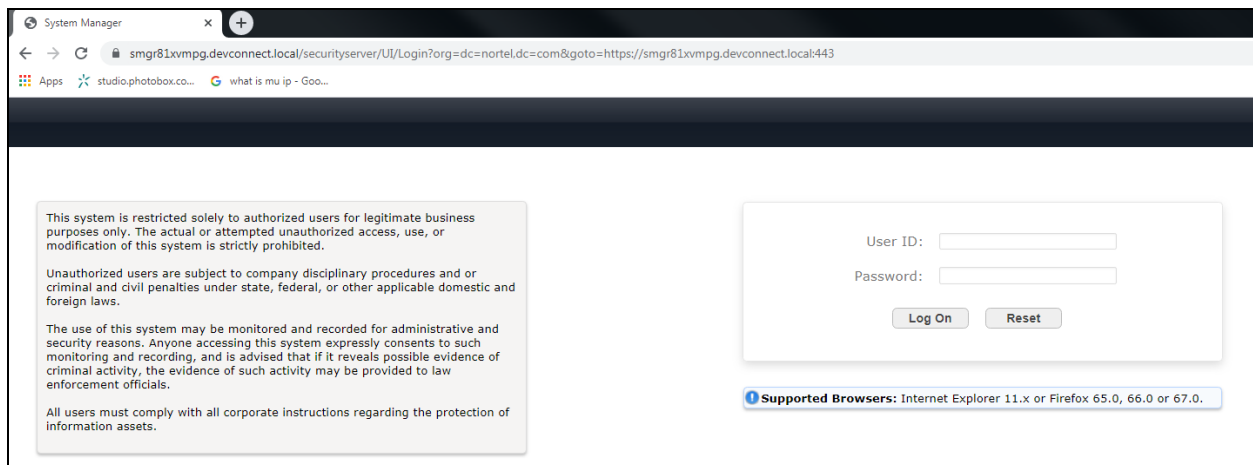
change trunk-group 12	Page 4 of 4
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? n	
Build Refer-To URI of REFER From Contact For NCR? n	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type: 101	
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: From	
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	

6. Configure Avaya Aura® Session Manager

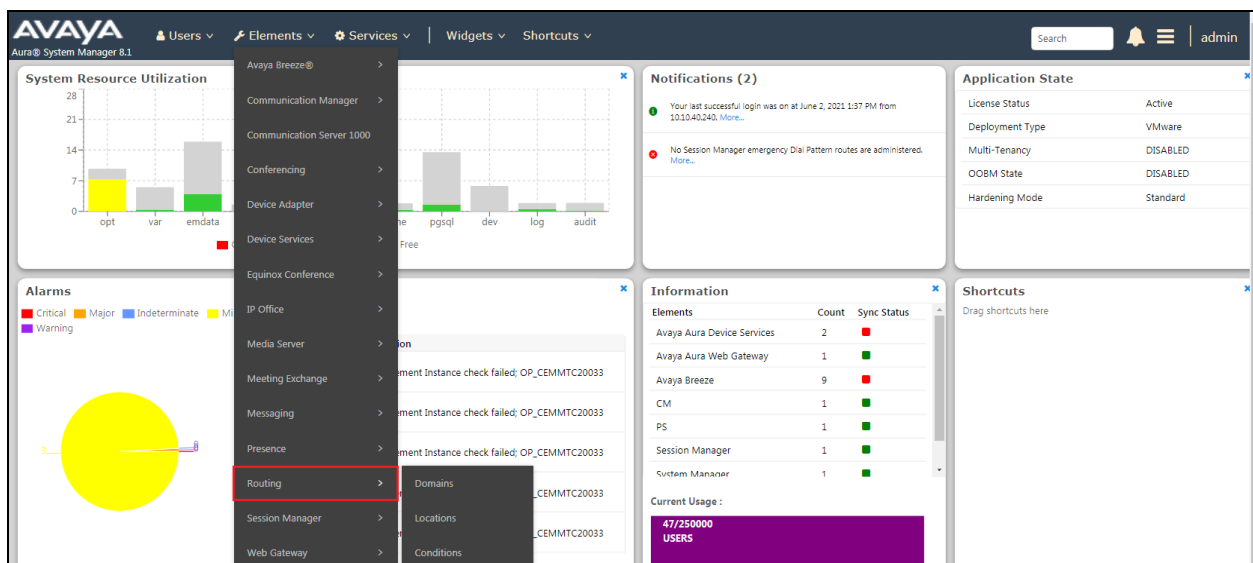
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Domains and Locations
- Adding a SIP Entity for Avaya Session Border Controller for Enterprise
- Adding a Routing Policy for Avaya Session Border Controller for Enterprise
- Adding a Dial Pattern for Avaya Session Border Controller for Enterprise

To make changes on Session Manager a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to <https://<System Manager FQDN>/SMGR>. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On**.



Once logged in navigate to **Elements** and click on **Routing**.

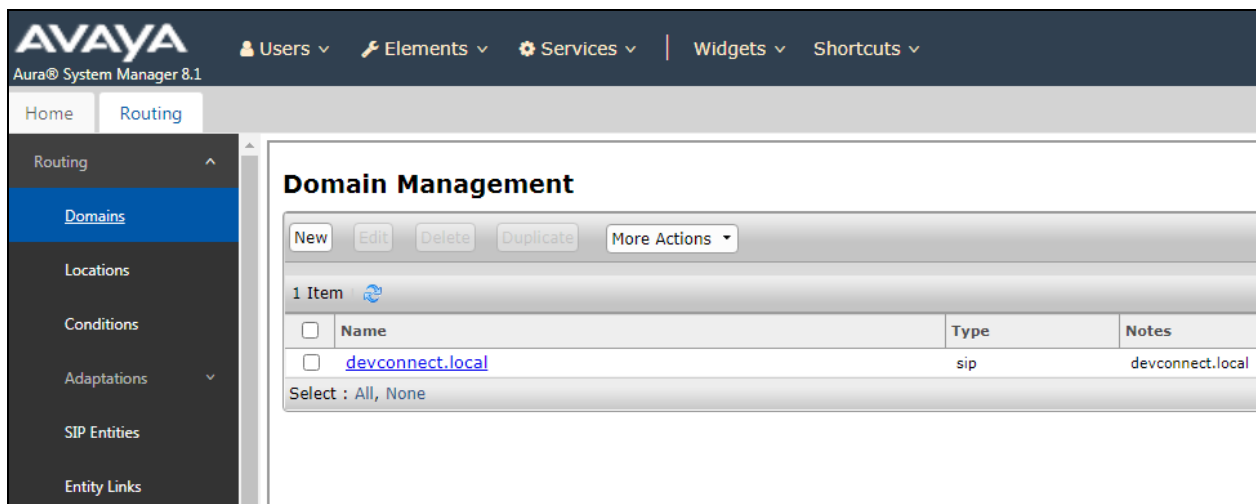


6.1. Domains and Locations

Note: It is assumed that a domain and a location have already been configured, therefore a quick overview of the domain and location that was used in compliance testing is provided here.

6.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **devconnect.local** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.

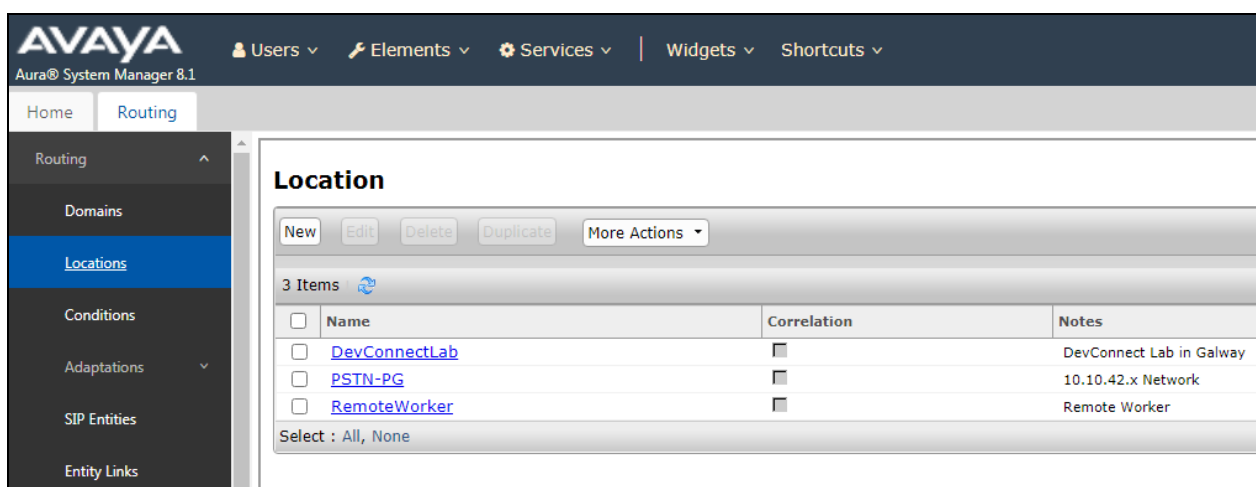


The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar has 'Routing' selected, and 'Domains' is highlighted. The main content area is titled 'Domain Management' and shows a table with one item: 'devconnect.local' of type 'sip'.

Name	Type	Notes
devconnect.local	sip	devconnect.local

6.1.2. Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **DevConnectLab** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.



The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar has 'Routing' selected, and 'Locations' is highlighted. The main content area is titled 'Location' and shows a table with three items: 'DevConnectLab', 'PSTN-PG', and 'RemoteWorker'.

Name	Correlation	Notes
DevConnectLab		DevConnect Lab in Galway
PSTN-PG		10.10.42.x Network
RemoteWorker		Remote Worker

6.2. Adding a SIP Entity for Avaya Session Border Controller for Enterprise

Because the calls are routed to the Avaya Session Border Controller and then onto LifeX there is only a requirement to have the ASBCE added as a SIP Entity, all calls to LifeX will be routed to the ASBCE and the ASBCE is then configured to route the calls to LifeX.

Click on **SIP Entities** in the left column and select **New** in the right window.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows a tree view with 'Routing' expanded, containing 'Domains', 'Locations', 'Conditions', 'Adaptations', 'SIP Entities' (highlighted), and 'Entity Links'. The main content area is titled 'SIP Entities' and features a 'New' button (highlighted with a red box), 'Edit', 'Delete', 'Duplicate', and 'More Actions' buttons. Below these buttons, it indicates '29 Items' and displays a table of existing SIP entities.

<input type="checkbox"/>	Name	FQDN or IP Address
<input type="checkbox"/>	aacc71spare	10.10.40.96
<input type="checkbox"/>	aacc71x	10.10.40.95
<input type="checkbox"/>	AAWG37x	10.10.40.67
<input type="checkbox"/>	Ascom-DECT	192.168.40.26
<input type="checkbox"/>	breeze1oc37-sm100	10.10.42.21
<input type="checkbox"/>	breeze1wspaces37-sm100	10.10.42.51

Enter a suitable **Name** for the SIP Entity, enter the **IP Address** of the ASBCE. Enter the correct **Time Zone** and **Location**. From this page, scroll down to add the appropriate Entity Link.

The screenshot shows the 'SIP Entity Details' form. The 'General' tab is selected. The form contains the following fields and values:

- Name:** SBCEforLifeX
- FQDN or IP Address:** 10.10.40.120
- Type:** SIP Trunk
- Notes:** SBCEforLifeX
- Location:** DevConnectLab
- Time Zone:** Europe/Dublin
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty field)
- Securable:** ☐
- Call Detail Recording:** egress

Buttons for 'Commit' and 'Cancel' are located at the top right of the form.

An Entity Link can be added from the SIP Entities page, as shown in the previous page, by scrolling down to **Entity Links**.

Enter a suitable **Name** for the Entity Link and select the **Session Manager** SIP Entity for **SIP Entity 1** and the newly created ASBCE SIP Entity for **SIP Entity 2**. Ensure that **TLS** is selected for the **Protocol** and that **Port 5061** is used, this is to secure communications between Session Manager and the ASBCE. Click on **Commit** once finished to save the new Entity Link and SIP Entity.

6.3. Adding a Routing Policy for Avaya Session Border Controller for Enterprise

Click on **Routing Policies** in the left window and select **New** in the main window.

Enter a suitable **Name** for the Routing Policy and click on **Select** under **SIP Entity as Destination**.

Routing Policy Details

CommitCancel

General

* Name: ToSBCEforLifeX

Disabled: ☐

* Retries: 0

Notes: ToSBCEforLifeX

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type

Time of Day

AddRemoveView Gaps/Overlaps

1 Item

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

Select : All, None

Select the ASBCE SIP Entity (**SBCEforLifeX**) as shown below and click on **Select**.

SIP Entities

SelectCancel

SIP Entities

28 Items

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	cm81Large	10.10.40.34	CM	
<input type="radio"/>	cm81vmppg - SIP PHONES 5061	10.10.40.37	CM	Used for SIP Phones on CM
<input type="radio"/>	cm81vmppg - TRUNK 5062	10.10.40.37	CM	Used for outgoing Trunk Calls
<input type="radio"/>	cm81vmppg - TRUNK 5063	10.10.40.37	CM	For Trunk calls to CM
<input type="radio"/>	EP723(MPP)	10.10.40.31	Voice Portal	EP722 and POM
<input type="radio"/>	IP Office	10.10.40.25	SIP Trunk	IP Office SE
<input type="radio"/>	IPOSE11	10.10.40.19	SIP Trunk	TO New IPO SE R11.1
<input type="radio"/>	LifeX	10.11.180.180	SIP Trunk	Frequentis LifeX
<input type="radio"/>	MessagingOn2016	10.10.40.76	Other	IX Messaging on Win 2016
<input type="radio"/>	MessagingOn2019	10.10.40.75	Other	IX Messaging on Win 2019
<input type="radio"/>	Presence	10.10.40.70	Presence Services	Presence Services
<input type="radio"/>	SBCE8	10.10.40.158	SIP Trunk	SBCE8
<input checked="" type="radio"/>	SBCEforLifeX	10.10.40.120	SIP Trunk	SBCEforLifeX

Select : None

The selected destination is now shown, click on **Commit** to save this.

Routing Policy Details

CommitCancel

General

* Name: ToSBCEforLifeX

Disabled: ☐

* Retries: 0

Notes: ToSBCEforLifeX

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SBCEforLifeX	10.10.40.120	SIP Trunk	SBCEforLifeX

6.4. Adding a Dial Pattern for Avaya Session Border Controller for Enterprise

Select **Dial Patterns** in the left window and select **New** in the main window.

AVAYA

Users Elements Services Widgets Shortcuts

Aura® System Manager 8.1

Home Routing

Routing

Domains

Locations

Conditions

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Dial Patterns

Dial Patterns

New Edit Delete Duplicate More Actions

20 Items

	Pattern	Min	Max	Emergency Call	Emergency Type
<input type="checkbox"/>	6667	4	4	<input type="checkbox"/>	
<input type="checkbox"/>	67	4	4	<input type="checkbox"/>	
<input type="checkbox"/>	68	4	4	<input type="checkbox"/>	
<input type="checkbox"/>	700	4	4	<input type="checkbox"/>	
<input type="checkbox"/>	9	5	12	<input type="checkbox"/>	

Select : All, None

Enter the required digits for the Pattern, in the example below 700 is used, which means that 7000 – 7009 will use the Routing Policy that will be selected. **700** is entered as the **Pattern** and the **Min** and **Max** digit length of **4** is used thus giving 700x. Ensure that the correct domain is entered for **SIP Domain** in this example the domain created in **Section 6.1.1** is added. Click on **Add** under **Originating Locations, Origination Dial Pattern Sets, and Routing Policies** to select the Routing Policy.

Dial Pattern Details

CommitCancel

General

* Pattern: 700

* Min: 4

* Max: 4

Emergency Call: ☐

SIP Domain: devconnect.local

Notes: To LifeX via SBC

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

AddRemove

1 Item

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank
Select : All, None						

Select the **Originating Location**, this will be the location added in **Section 6.1.2** select the newly created routing policy for the ASBCE (**ToSBCEforLifeX**).

Originating Location

Select

Cancel

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

3 Items

<input type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	DevConnectLab	DevConnect Lab in Galway
<input type="checkbox"/>	PSTN-PG	10.10.42.x Network
<input type="checkbox"/>	RemoteWorker	Remote Worker

Select : All, None

Origination Dial Pattern Sets

1 Item

<input type="radio"/>	Name
<input type="radio"/>	SA8481

Select : None

Routing Policies

13 Items

<input type="checkbox"/>	Name	Disabled	Destination
<input type="checkbox"/>	ToAACC71Spare	<input type="checkbox"/>	aacc71spare
<input type="checkbox"/>	To AACC71x	<input type="checkbox"/>	aacc71x
<input type="checkbox"/>	To CM80vmpg	<input type="checkbox"/>	cm80vmpg
<input type="checkbox"/>	To cm81xvmpg	<input type="checkbox"/>	cm81vmpg - TRUNK 5063
<input type="checkbox"/>	To CM81xvmpg - PHONES	<input type="checkbox"/>	cm81vmpg - SIP PHONES 5061
<input type="checkbox"/>	To EP722	<input type="checkbox"/>	EP723(MPP)
<input type="checkbox"/>	To IP Office	<input type="checkbox"/>	IP Office
<input type="checkbox"/>	To IPOSE11	<input type="checkbox"/>	IPOSE11
<input type="checkbox"/>	To LifeX	<input type="checkbox"/>	LifeX
<input type="checkbox"/>	To Messaging on 2016	<input type="checkbox"/>	MessagingOn2016
<input type="checkbox"/>	To Messaging on 2019	<input type="checkbox"/>	MessagingOn2019
<input type="checkbox"/>	To SBCE8	<input type="checkbox"/>	SBCE8
<input checked="" type="checkbox"/>	ToSBCEforLifeX	<input type="checkbox"/>	SBCEforLifeX

Select : All, None

With the Routing Policy selected click on **Commit** to finish adding the **Dial Pattern**.

Dial Pattern Details

CommitCancelHelp ?

General

* Pattern:700

* Min:4

* Max:4

Emergency Call:☐

SIP Domain:devconnect.local

Notes:To LifeX via SBC

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

AddRemove

1 Item

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	DevConnectLab	DevConnect Lab in Galway			To LifeX	0	<input type="checkbox"/>	LifeX	To LifeX

Select : All, None

Denied Originating Locations and Origination Dial Pattern Sets

AddRemove

0 Items

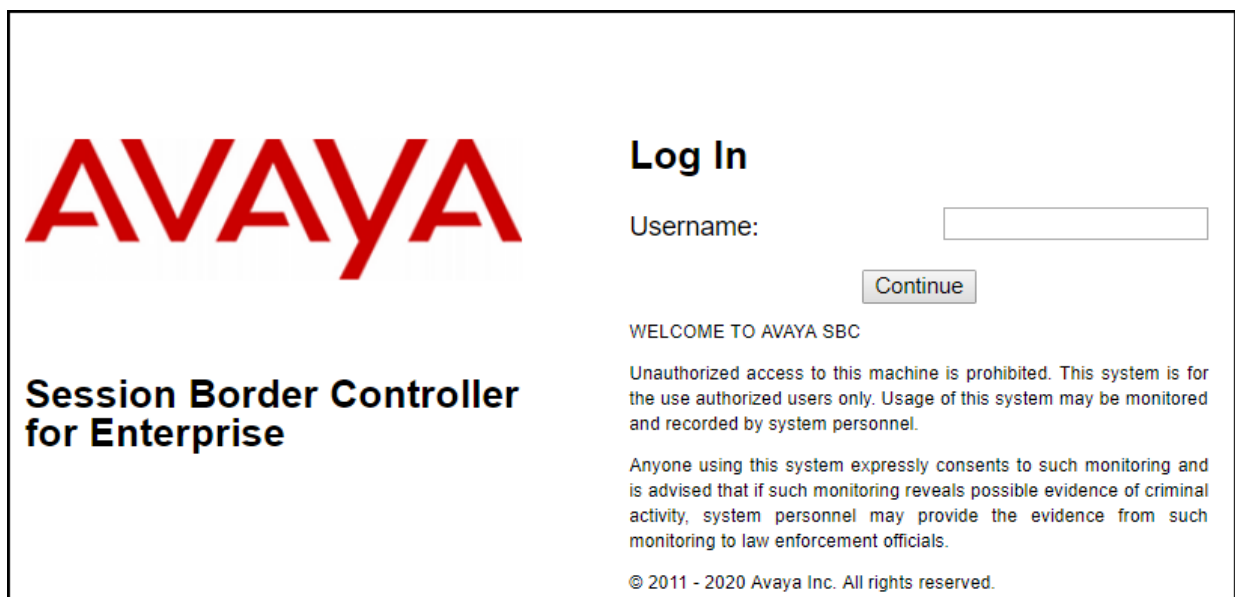
<input type="checkbox"/>	Originating Location	Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes
--------------------------	----------------------	-------	-----------------------------------	------------------------------------

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE, consult the Avaya SBCE documentation in the **Section 11**.

7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



The image shows the login page of the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' in bold black font. On the right, under the heading 'Log In', there is a 'Username:' label followed by a text input field. Below the input field is a 'Continue' button. Further down, the text 'WELCOME TO AVAYA SBC' is displayed, followed by a disclaimer: 'Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.' Below this is a consent statement: 'Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.' At the bottom, the copyright notice '© 2011 - 2020 Avaya Inc. All rights reserved.' is shown.

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

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

The screenshot displays the Avaya SBCE web interface. At the top, a navigation bar includes 'Device: sbceforfrequentis', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. Below this, a header section shows 'EMS' and 'sbceforfrequentis' in a dropdown menu, followed by 'er Controller for Enterprise' and the 'AVAYA' logo.

The main content area is divided into two columns. The left column, titled 'EMS Dashboard', lists various management options: Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows, DMZ Services, and Monitoring & Logging. The right column, titled 'Dashboard', contains several sections:

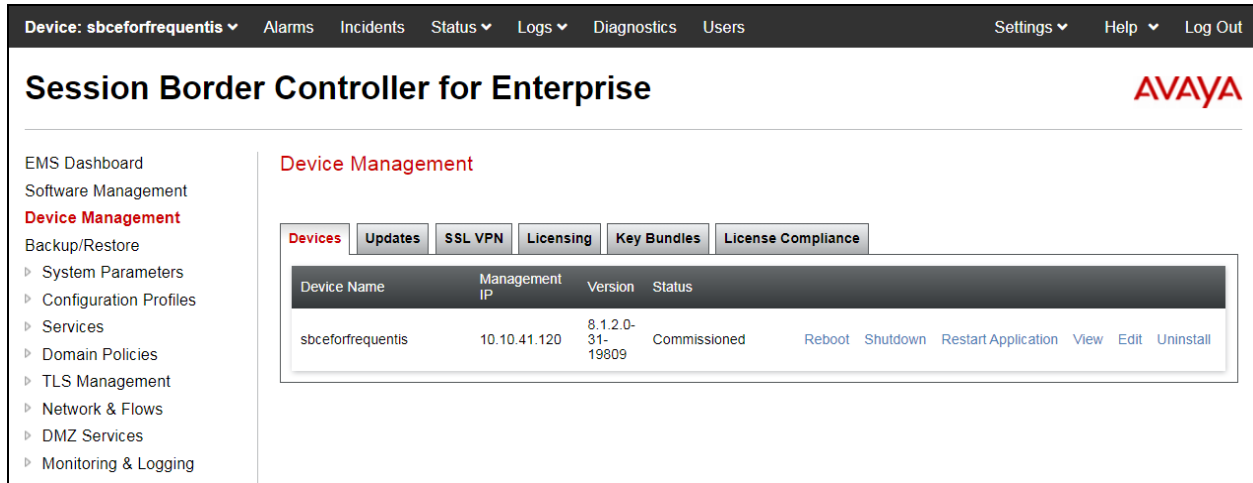
- Information**: A table with system details.

Information	
System Time	12:28:50 PM IST Refresh
Version	8.1.2.0-31-19809
GUI Version	8.1.2.0-19794
Build Date	Tue Dec 08 09:11:07 UTC 2020
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	05/26/2021 14:27:12 IST
Failed Login Attempts	0
- Installed Devices**: A list showing 'EMS' and 'sbceforfrequentis'.
- Active Alarms (past 24 hours)**: A section stating 'None found.'
- Incidents (past 24 hours)**: A section stating 'None found.'

An 'Add' button is located at the bottom right of the dashboard area.

7.2. Device Management

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



The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: sbceforfrequentis, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main heading is "Session Border Controller for Enterprise" with the AVAYA logo. The left sidebar lists various management options, with "Device Management" highlighted. The "Device Management" section shows a table of devices. The table has columns for Device Name, Management IP, Version, and Status. The device "sbceforfrequentis" is listed with a Management IP of 10.10.41.120 and a Version of 8.1.2.0-31-19809. The Status is "Commissioned". Action links for Reboot, Shutdown, Restart Application, View, Edit, and Uninstall are provided for this device.

Device Name	Management IP	Version	Status
sbceforfrequentis	10.10.41.120	8.1.2.0-31-19809	Commissioned

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

The highlighted IP addresses in the **System Information** screen shown on the next page are the ones used for the SIP trunk to LifeX and are the ones relevant to these Application Notes. Other IP addresses may be assigned to other interfaces to support remote workers and other SIP trunks, and they are not discussed in this document.

The private interface of the Avaya SBCE (10.10.40.120) was used to connect to the enterprise network, the public interface of the Avaya SBCE (10.10.40.121) was used to connect to the LAN interface of the LifeX managed SBC (10.11.180.180). A VPN connection to the network connected to LifeX was used to facilitate compliance testing, see **Figure 1**. Note that Frequentis is responsible for the configuration of the Session Border Controller that we are connecting to from this Avaya SBCE.

On the **License Allocation** area of the **System Information**, verify that the number of **Standard Sessions** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise. The number of sessions and encryption features are primarily controlled by the license file installed.

System Information: sbceforfrequentis

General Configuration

Appliance Name	sbceforfrequentis
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Dynamic License Allocation

	Min License Allocation	Max License Allocation
Standard Sessions	0	0
Advanced Sessions	0	0
Scopia Video Sessions	0	0
CES Sessions	0	0
Transcoding Sessions	0	0
Premium Sessions	0	0
CLID	---	
Encryption <small>Available: Yes</small>	<input checked="" type="checkbox"/>	

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.10.40.120	10.10.40.120	255.255.255.0	10.10.40.1	A1
10.10.40.121	10.10.40.121	255.255.255.0	10.10.40.1	A1

DNS Configuration

Primary DNS	10.10.40.1
Secondary DNS	10.10.40.5
DNS Location	DMZ
DNS Client IP	10.10.40.120

Management IP(s)

IP #1 (IPv4)	10.10.41.120
--------------	--------------

7.3. TLS Management

Transport Layer Security (TLS) is a standard protocol that is used extensively to provide a secure channel by encrypting communications over IP networks. It enables clients to authenticate servers or, optionally, servers to authenticate clients. UC-Sec security products utilize TLS primarily to facilitate secure communications with remote servers.

In the reference configuration, TLS transport is used for both the communication between Session Manager and Avaya SBCE and between the Avaya SBCE and LifeX. The following procedures show how to create the client and server profiles to support the TLS connection.

Note – Testing was done with System Manager signed identity certificates. The procedure to create and obtain these certificates is outside the scope of these Application Notes.

7.3.1. Verify TLS Certificates – Avaya Session Border Controller for Enterprise

Select **TLS Management** → **Certificates** from the left-hand menu. Verify the following:

- System Manager CA certificate is present in the **Installed CA Certificates** area.
- System Manager CA signed identity certificate is present in the **Installed Certificates** area.
- Private key associated with the identity certificate is present in the **Installed Keys** area, (not shown below but is visible after scrolling down the page).

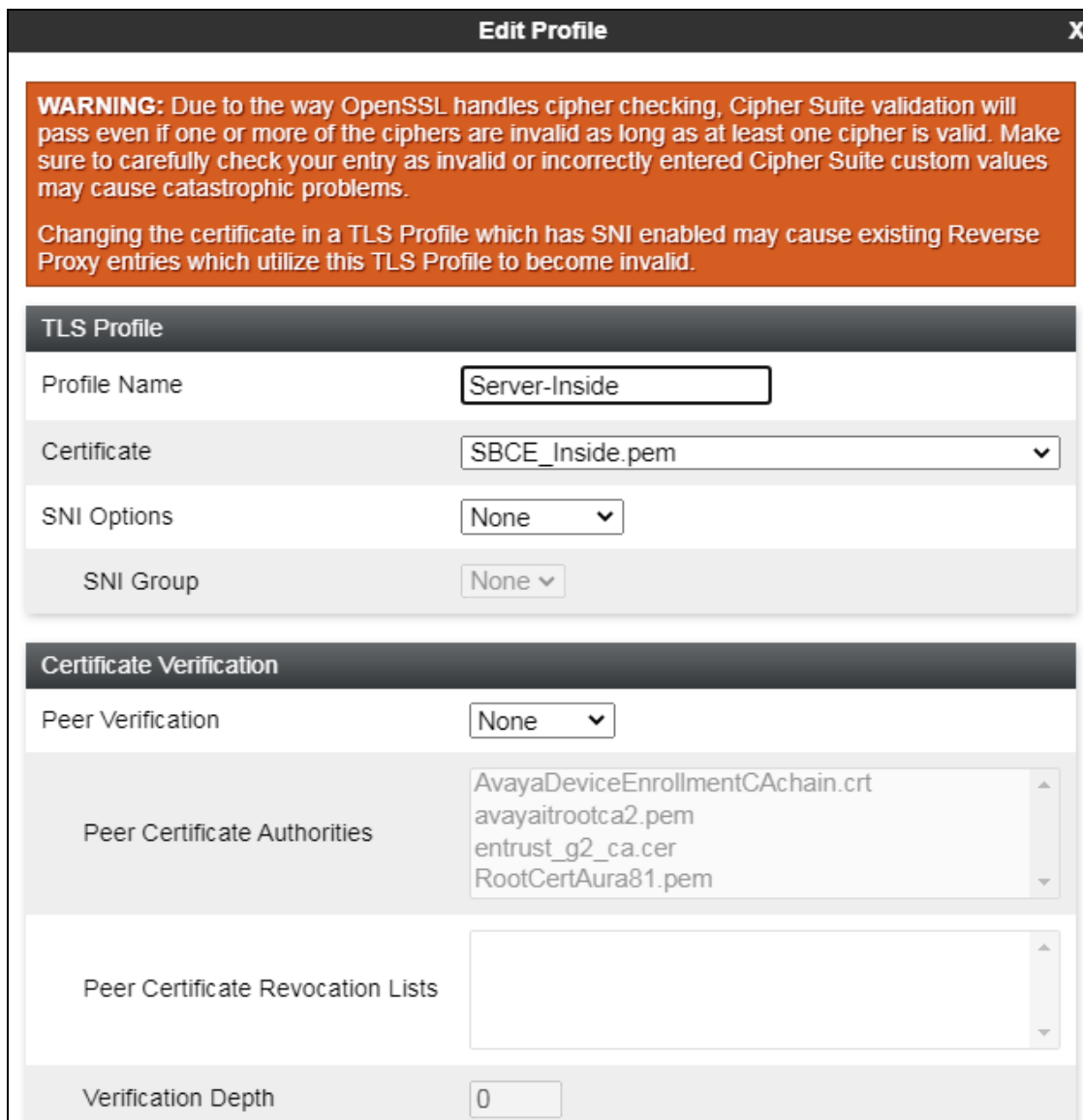
The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left is a navigation menu with options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management (selected), Certificates (highlighted), Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled "Certificates" and includes "Install" and "Generate CSR" buttons. It is divided into three sections: "Installed Certificates" (listing SBCE_Inside.pem and SBCE_Outside.pem with View/Delete links), "Installed CA Certificates" (listing AvayaDeviceEnrollmentCAchain.crt, avayaitrootca2.pem, entrust_g2_ca.cer, and RootCertAura81.pem with View/Delete links), and "Installed Certificate Revocation Lists" (stating "No certificate revocation lists have been installed.").

7.3.2. Server Profiles

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

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **SBCE_inside.pem**, from pull down menu.
- **Peer Verification = None.**
- Click **Next**.

Accept default values for the next screen (not shown) and click **Finish**.



Edit Profile X

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

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

TLS Profile

Profile Name:

Certificate:

SNI Options:

SNI Group:

Certificate Verification

Peer Verification:

Peer Certificate Authorities:

Peer Certificate Revocation Lists:

Verification Depth:

The following screen shows the completed **TLS Server Profile** form.

Click here to add a description.

Server Profile

TLS Profile

Profile Name	Server-Inside
Certificate	SBCE_Inside.pem
SNI Options	None

Certificate Verification

Peer Verification	None
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options

Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Edit

Below is the profile set for the outside server connection. It is very similar to that above just uses a different **Certificate** that contains the outside IP address instead of the inside or enterprise IP address.

Server Profile

TLS Profile

Profile Name	Server-Outside
Certificate	SBCE_Outside.pem
SNI Options	None

Certificate Verification

Peer Verification	None
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options

Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

7.3.3. Client Profiles

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

- **Profile Name:** enter descriptive name.
- **Certificate:** select the identity certificate, e.g., **SBCE_Inside.pem**, from pull down menu.
- **Peer Verification = Required.**
- **Peer Certificate Authorities:** select the CA certificate used to verify the certificate received from Session Manager, e.g., **RootCertAura81.pem**.
- **Verification Depth:** enter **1**.
- Click **Next**.

Accept default values for the next screen (not shown) and click **Finish**.

Edit Profile X

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

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

TLS Profile

Profile Name: Client-Inside

Certificate: SBCE_Inside.pem

SNI: ☐ Enabled

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities: AvayaDeviceEnrollmentCAchain.crt, avayaitrootca2.pem, entrust_g2_ca.cer, RootCertAura81.pem

Peer Certificate Revocation Lists:

Verification Depth: 1

Extended Hostname Verification: ☐

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

Click here to add a description.

Client Profile

Certificate	SBCE_Inside.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	RootCertAura81.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options

Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

[Edit](#)

Below is the profile set for the outside client connection. It is very similar to that above just uses a different **Certificate** that contains the outside IP address instead of the inside or enterprise IP address.

Client Profile

TLS Profile

Profile Name	Client-Outside
Certificate	SBCE_Outside.pem
SNI	<input type="checkbox"/> Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	RootCertAura81.pem
Peer Certificate Revocation Lists	---
Verification Depth	1
Extended Hostname Verification	<input type="checkbox"/>

Renegotiation Parameters

Renegotiation Time	0
Renegotiation Byte Count	0

Handshake Options

Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

7.4. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from the **Network & Flows** on the left-side menu. On the **Networks** tab, verify or enter the network information as needed.

The configuration used during the compliance test is displayed below, the IP addresses assigned to the private (*10.10.40.120*) and public (*10.10.40.121*) sides are as shown.

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

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Network & Flows
 Network Management
 Media Interface
 Signaling Interface

Network Management

Interfaces Networks

Add

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
A1_Network	10.10.40.1	255.255.255.0	A1	10.10.40.120, 10.10.40.121	Edit Delete

On the **Interfaces** tab, verify the **Administrative Status** is **Enabled** for the **A1** interface. Click the buttons under the **Status** column if necessary, to enable the interface.

Network Management

Interfaces Networks

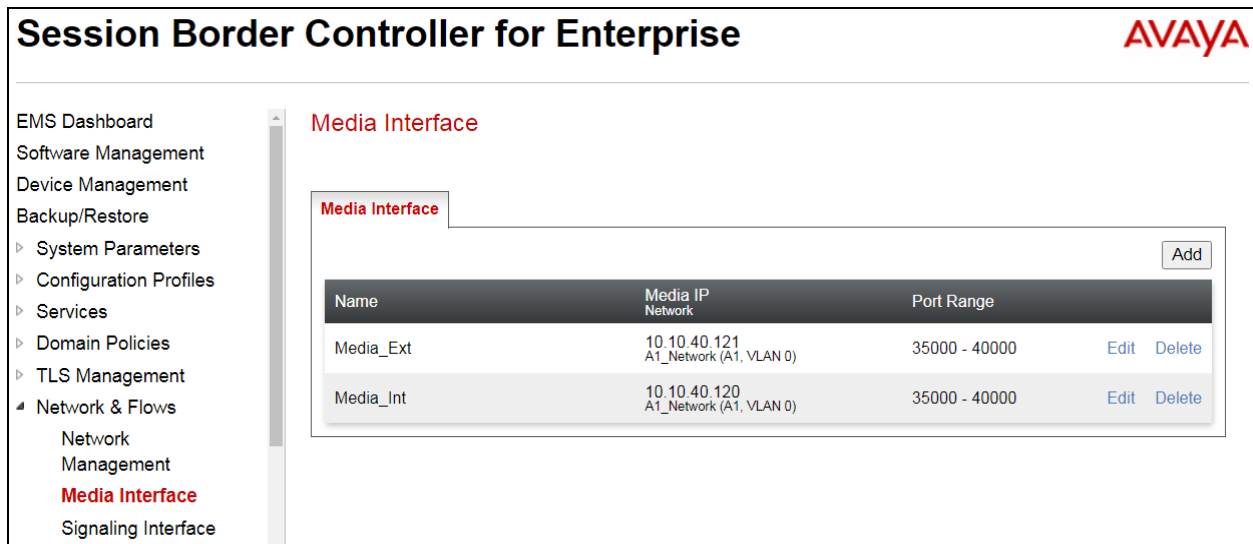
Add VLAN

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

7.5. Media Interfaces

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address, and one of the ports in this range as the listening IP address and port in which it will accept media from the Call Server or the trunk server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (the two configured Media Interfaces are already shown below).



Session Border Controller for Enterprise

EMS Dashboard
Software Management
Device Management
Backup/Restore
System Parameters
Configuration Profiles
Services
Domain Policies
TLS Management
Network & Flows
Network Management
Media Interface
Signaling Interface

Media Interface

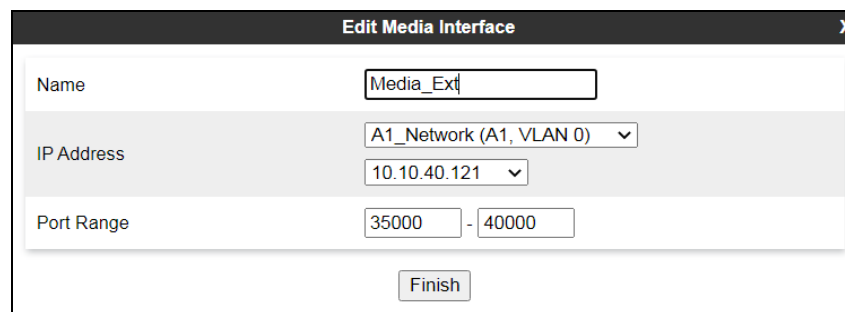
Media Interface

Name	Media IP Network	Port Range	Edit	Delete
Media_Ext	10.10.40.121 A1_Network (A1, VLAN 0)	35000 - 40000	Edit	Delete
Media_Int	10.10.40.120 A1_Network (A1, VLAN 0)	35000 - 40000	Edit	Delete

[Add](#)

The example below shows the external media interface, as shown in the screen above similar configurations are used for both internal and external interfaces. If a new media interface is to be added, these are the necessary steps to follow.

- On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface, in the example **Media_Ext** was used.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- The **Port Range** was left at the default values of **35000-40000**.
- Click **Finish**.



Edit Media Interface

Name:

IP Address:

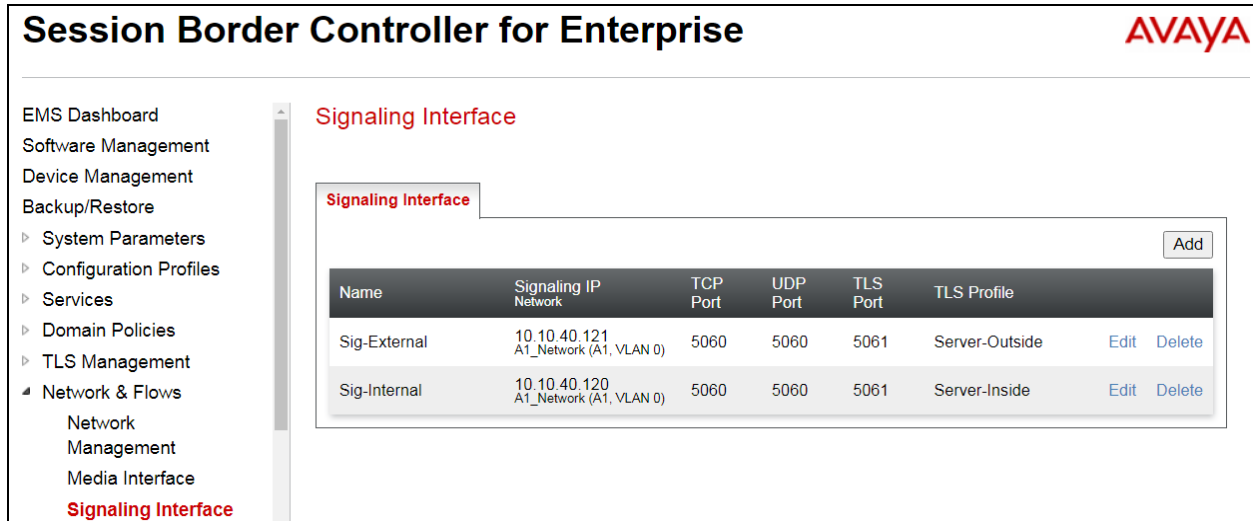
Port Range: -

[Finish](#)

7.6. Signaling Interfaces

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in the connected networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Network & Flows** menu on the left-hand side, click the **Add** button (the two configured Signaling Interfaces are already shown below).



Session Border Controller for Enterprise AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▶ System Parameters
▶ Configuration Profiles
▶ Services
▶ Domain Policies
▶ TLS Management
■ **Network & Flows**
 Network Management
 Media Interface
 Signaling Interface

Signaling Interface

Signaling Interface Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Sig-External	10.10.40.121 A1_Network (A1, VLAN 0)	5060	5060	5061	Server-Outside	Edit Delete
Sig-Internal	10.10.40.120 A1_Network (A1, VLAN 0)	5060	5060	5061	Server-Inside	Edit Delete

The example on the next page shows the Signaling Interface that was used for the external connection to LifeX, a similar interface needs to be created for the connection to Session Manager. As shown above from the configured interfaces, there are different IP addresses used as well as different TLS Profiles. If a new interface is to be created, then click on Add from the screen above.

- On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface, in the example **Sig-External** was used.
- Under **IP Address**, select from the drop-down menus the network and IP address to be associated with this interface.
- Enter **5061** for **TLS Port**, since TLS port 5061 is used to listen for signaling traffic from Session Manager in the sample configuration, as defined in **Section 6.2**.
- Select a **TLS Profile** defined in **Section 7.3.2**.
- Click **Finish**.

Edit Signaling InterfaceX

Name

Sig-External

IP Address

A1_Network (A1, VLAN 0) ▾

10.10.40.121 ▾

TCP Port

Leave blank to disable

5060

UDP Port

Leave blank to disable

5060

TLS Port

Leave blank to disable

5061

TLS Profile

Server-Outside ▾

Enable Shared Control

☐

Shared Control Port

Finish

7.7. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server).

7.7.1. Server Interworking Profile – Enterprise

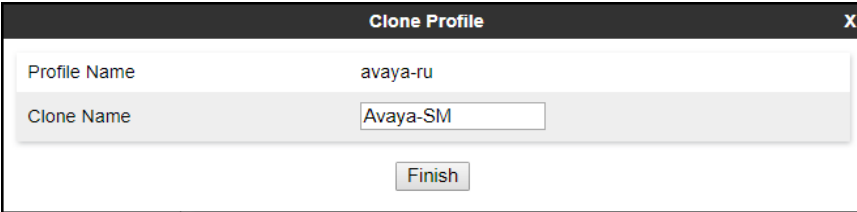
Interworking profiles can be created by cloning one of the pre-defined default profiles, or by adding a new profile. To configure the interworking profile in the enterprise direction, select **Configuration Profiles → Server Interworking** on the left navigation pane. Under **Interworking Profiles**, select *avaya-ru* from the list of pre-defined profiles. Click **Clone** (not shown).

The screenshot displays the Avaya Session Border Controller for Enterprise configuration interface. The top navigation bar includes 'Device: Avaya_SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', and 'Settings'. The main title is 'Session Border Controller for Enterprise'. The left navigation pane shows the hierarchy: EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles (expanded), and various sub-profiles. 'Server Interworking' is selected. The main content area is titled 'Interworking Profiles: avaya-ru' and includes an 'Add' button. A list of profiles is shown, with 'avaya-ru' highlighted. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this, tabs for 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced' are visible. The 'General' tab is active, showing a table of configuration parameters.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

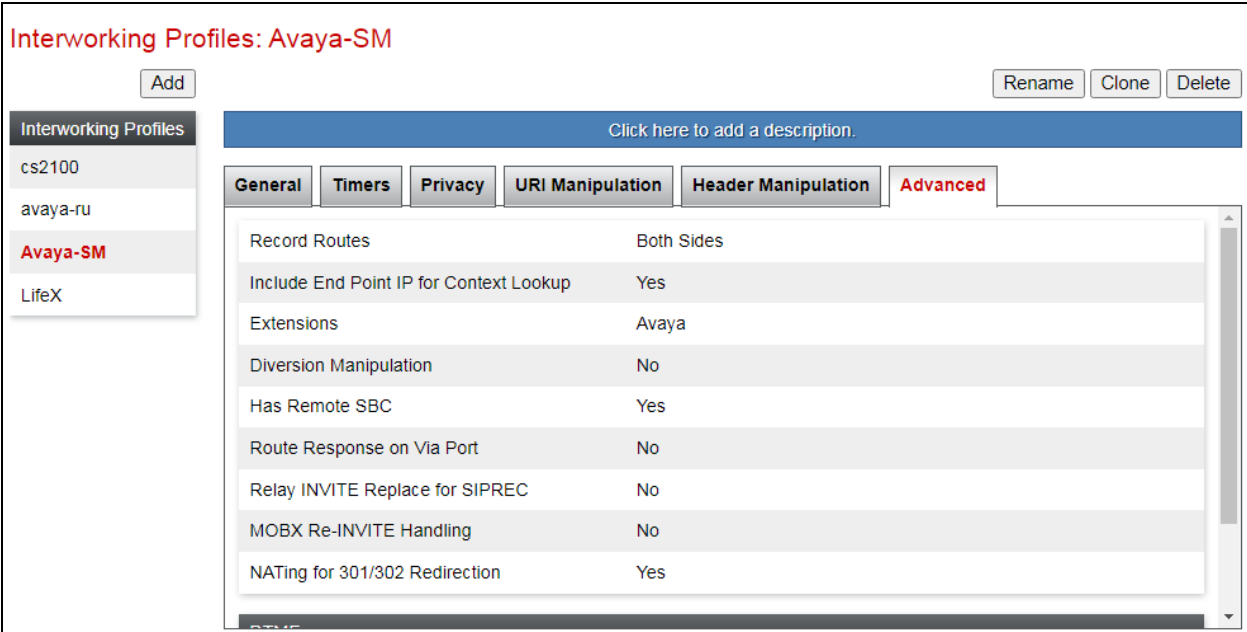
An 'Edit' button is located at the bottom right of the configuration table.

Enter a descriptive name for the cloned profile and click **Finish**.



A dialog box titled "Clone Profile" with a close button (X) in the top right corner. It contains two input fields: "Profile Name" with the value "avaya-ru" and "Clone Name" with the value "Avaya-SM". Below the fields is a "Finish" button.

The **Advanced** tab settings are shown on the screen below:

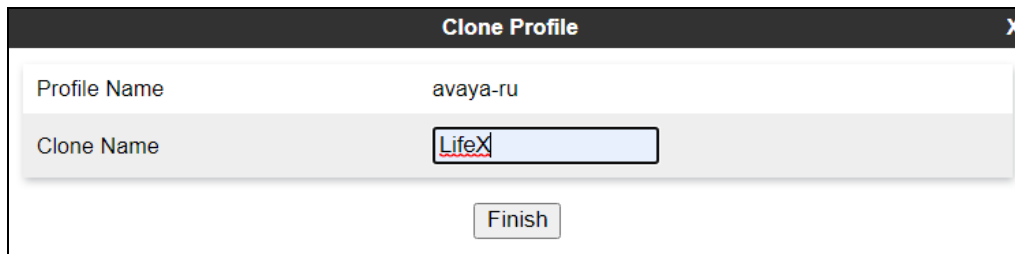


The "Interworking Profiles: Avaya-SM" configuration screen. On the left is a sidebar with "Interworking Profiles" and a list: "cs2100", "avaya-ru", "Avaya-SM" (highlighted in red), and "LifeX". Above the list are "Add", "Rename", "Clone", and "Delete" buttons. The main area has a blue header "Click here to add a description." and tabs: "General", "Timers", "Privacy", "URI Manipulation", "Header Manipulation", and "Advanced" (highlighted in red). The "Advanced" tab contains a table of settings.

Setting	Value
Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

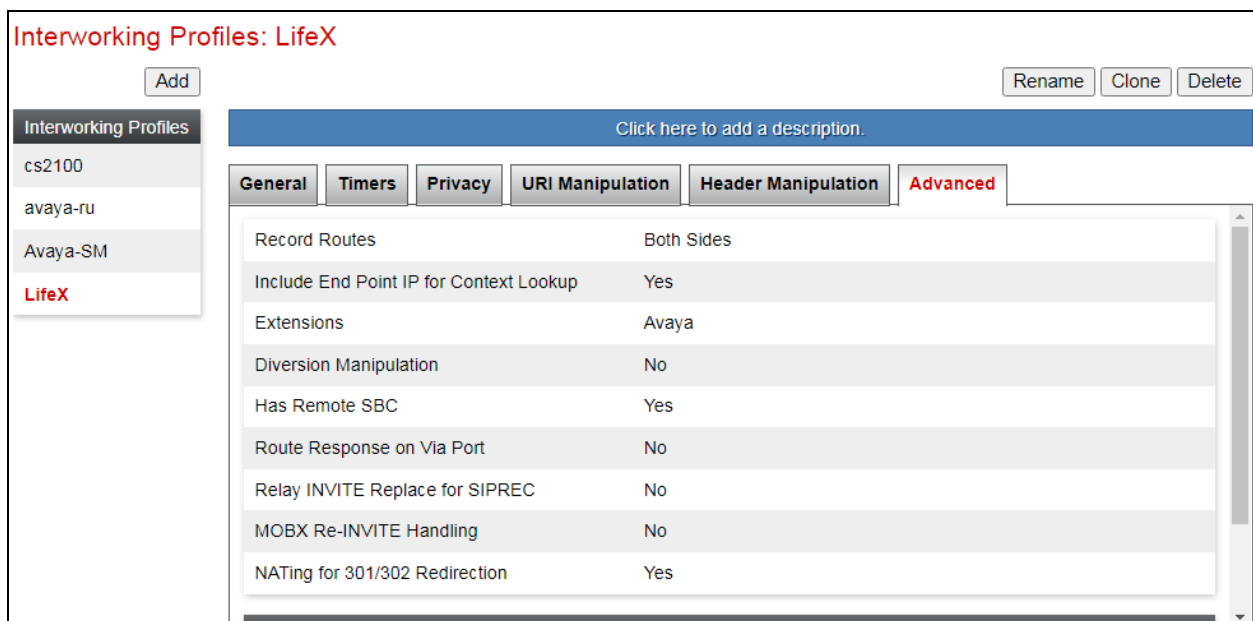
7.7.2. Server Interworking Profile – LifeX

A second interworking profile in the direction of the SIP trunk was created, by adding a new profile in this case. Select **Configuration Profiles → Server Interworking** on the left navigation pane and click **Clone** (not shown). Enter a descriptive name for the new profile and click **Finish**.



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

Again, the **Advanced** tab shows a similar setting to that of the Enterprise.



The image shows the 'Interworking Profiles: LifeX' configuration page. On the left is a sidebar with 'Interworking Profiles' and a list of profiles: 'cs2100', 'avaya-ru', 'Avaya-SM', and 'LifeX' (highlighted in red). Above the list are 'Add', 'Rename', 'Clone', and 'Delete' buttons. The main area has a blue header with 'Click here to add a description.' and a tabbed interface with 'General', 'Timers', 'Privacy', 'URI Manipulation', 'Header Manipulation', and 'Advanced' (selected). The 'Advanced' tab contains a table of settings:

Setting	Value
Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

7.8. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE peers; Session Manager (Call Server) at the enterprise and LifeX (Trunk Server). Below shows some Server Profiles that were used during compliance testing, to add a new Server Profile, from the Services menu on the left-hand navigation pane, select **SIP Servers** and click the **Add**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation pane shows the 'Services' menu expanded, with 'SIP Servers' selected. The main content area is titled 'SIP Servers: Avaya-SM-TLS' and includes an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below the title is a list of server profiles: 'Avaya-SM-TLS' (selected), 'Avaya-SM-TCP', 'LifeX-SBC-UDP', and 'LifeX-SBC-TLS'. The 'General' tab is active, showing the following configuration:

Server Type	Call Server	
SIP Domain	devconnect.local	
TLS Client Profile	Client-Inside	
DNS Query Type	NONE/A	
IP Address / FQDN	Port	Transport
10.10.40.32	5061	TLS

An 'Edit' button is located below the table.

7.8.1. Server Configuration Profile – Enterprise

The following shows the Profile used to connect to Session Manager on the Enterprise side.

- On the **Edit SIP Server Profile – General** tab select **Call Server** from the drop-down menu under the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the Session Manager Security Module (**Section 5.5**).
- Enter **5061** under **Port** and select **TLS** for **Transport**. The transport protocol and port selected here must match the values defined for the Entity Link to the Session Manager previously created in **Section 6.2**.
- Select a **TLS Client Profile** defined in **Section 7.3.3**.

Edit SIP Server Profile - General X

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type

Call Server

SIP Domain

devconnect.local

DNS Query Type

NONE/A

TLS Client Profile

Client-Inside

Add

IP Address / FQDN	Port	Transport	
10.10.40.32	5061	TLS	Delete

Finish

- Click **Next** until the **Add Server Configuration Profile – Advanced** tab is reached (not shown).
- On the **Add Server Configuration Profile – Advanced** tab:
 - Check **Enable Grooming**.
 - Select **Avaya-SM** from the **Interworking Profile** drop-down menu (**Section 7.7.1**).
- Click **Finish**.

Edit SIP Server Profile - Advanced
X

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya-SM ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼
NG911 Support	<input type="checkbox"/>

Finish

7.8.2. Server Configuration Profile – Service Provider

Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown).

- On the **Edit Server Configuration Profile - General** Tab select **Trunk Server** from the drop-down menu for the **Server Type**.
- On the **IP Addresses / FQDN** field, enter the IP address of the LAN interface of the LifeX device to connect to (**10.11.180.180**).
- Select **TLS** for **Transport** and enter **5061** under **Port**.
- Click **Next** until the **Advanced** tab is reached (not shown).

Edit SIP Server Profile - General X

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server TypeTrunk Server

SIP Domaindevconnect.local

DNS Query TypeNONE/A

TLS Client ProfileClient-Outside

Add

IP Address / FQDN	Port	Transport	
10.11.180.180	5061	TLS	Delete

Finish

On the **Add SIP Server Profile - Advanced** window:

- **Enable Grooming** (should be checked).
- Select **LifeX** from the **Interworking Profile** drop-down menu (**Section 7.7.2**).
- Click **Finish**.

Edit SIP Server Profile - Advanced X

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

Finish

7.9. Routing

Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces. Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the LifeX SIP trunk.

7.9.1. Routing Profile – LifeX

To create the outbound route, select the **Routing** tab from the **Configuration Profiles** menu on the left-hand side and select **Add**.

The screenshot shows the Avaya Session Border Controller for Enterprise configuration interface. On the left, a navigation menu lists various configuration options, with 'Routing' highlighted in red. The main area is titled 'Routing Profiles: default' and contains a list of profiles: 'default', 'ToAvayaSM-T...', 'ToLifeX-TLS', 'ToLifeX-UDP', and 'ToAvayaSM-T...'. An 'Add' button is visible above the list. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this, a 'Routing Profile' table is shown with columns: Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport. The table contains one row with the following values: Priority 1, URI Group *, Time of Day default, Load Balancing DNS/SRV, Next Hop Address Auto-Detect, and Transport Auto-Detect. There are 'Update Priority', 'Add', 'Edit', and 'Delete' buttons associated with the table.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	DNS/SRV	Auto-Detect	Auto-Detect

Enter an appropriate **Profile Name** similar to the example below and click **Next**.

The screenshot shows a 'Routing Profile' configuration dialog. It has a 'Profile Name' label and a text input field containing 'ToLifeX-TLS'. Below the input field is a 'Next' button.

- On the **Routing Profile** tab, click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **SIP Server Profile**, select the SIP Server Profile for LifeX. The **Next Hop Address** field will be populated with the IP address, port and protocol defined for the LifeX Server Configuration Profile in **Section 7.8.2**.
- Defaults were used for all other parameters.
- Click **Finish**.

Profile : ToLifeX-TLS - Edit Rule			
URI Group	<input type="text" value="*"/>	Time of Day	<input type="text" value="default"/>
Load Balancing	<input type="text" value="Priority"/>	NAPTR	<input type="checkbox"/>
Transport	<input type="text" value="None"/>	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	<input type="text" value="None"/>	LDAP Base DN (Search)	<input type="text" value="None"/>
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input checked="" type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	<input type="text"/>
<input type="button" value="Add"/>			
Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result
<input type="text" value="1"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
			<input type="text" value="LifeX-SBC"/>
			<input type="text" value="10.11.180.180:5060"/>
			<input type="text" value="None"/>
<input type="button" value="Delete"/>			
<input type="button" value="Finish"/>			

7.9.2. Routing Profile – Session Manager

Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the inbound route. Enter an appropriate **Profile Name** similar to the example below and click **Next**.

Routing Profile	
Profile Name	<input type="text" value="ToAvayaSM-TLS"/>
<input type="button" value="Next"/>	

- Click the **Add** button to enter the next-hop address.
- Under **Priority/Weight** enter **1**.
- Under **SIP Server Profile**, select the Session Manager profile. The **Next Hop Address** is populated automatically with the IP address of Session Manager along with the port number defined in **Section 7.8.1**.
- Defaults were used for all other parameters.
- Click **Finish**.

Profile : ToAvayaSM-TLS - Edit Rule							
URI Group	<input type="text" value="*"/>	Time of Day	<input type="text" value="default"/>				
Load Balancing	<input type="text" value="Priority"/>	NAPTR	<input type="checkbox"/>				
Transport	<input type="text" value="None"/>	LDAP Routing	<input type="checkbox"/>				
LDAP Server Profile	<input type="text" value="None"/>	LDAP Base DN (Search)	<input type="text" value="None"/>				
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>				
Next Hop Priority	<input checked="" type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>				
Ignore Route Header	<input type="checkbox"/>						
ENUM	<input type="checkbox"/>	ENUM Suffix	<input type="text"/>				
<input type="button" value="Add"/>							
Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
<input type="text" value="1"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Avaya-SM"/>	<input type="text" value="10.10.40.32:5061"/>	<input type="text" value="None"/>	<input type="button" value="Delete"/>
<input type="button" value="Finish"/>							

7.10. Topology Hiding

Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, the default Topology Hiding Profile was cloned and modified accordingly. Only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

7.10.1. Topology Hiding Profile – Enterprise

To add the Topology Hiding Profile in the enterprise direction, select **Topology Hiding** from the **Configuration Profiles** menu on the left-hand side, select *default* from the list of pre-defined profiles and click the **Clone** button.

The screenshot shows the 'Session Border Controller for Enterprise' configuration page. On the left is a navigation menu with 'Topology Hiding' selected. The main area is titled 'Topology Hiding Profiles: default' and contains a list of profiles: 'default', 'cisco_th_profile', 'Avaya-SM', and 'LifeX'. An 'Add' button is above the list, and a 'Clone' button is to the right. A warning message states: 'It is not recommended to edit the defaults. Try cloning or adding a new profile instead.' Below this is a table titled 'Topology Hiding' with the following data:

Header	Criteria	Replace Action	Overwrite Value
Referred-By	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
From	IP/Domain	Auto	---

Enter a **Clone Name** such as the one shown below and click **Finish**.

The 'Clone Profile' dialog box shows the 'Profile Name' as 'default' and the 'Clone Name' as 'Avaya-SM'. A 'Finish' button is at the bottom.

On the newly cloned Avaya-SM profile screen, click the **Edit** button (not shown).

- For the, **From**, **To** and **Request-Line** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain **devconnect.local**, in the **Overwrite Value** column of these headers, as shown below. This is the domain known by Session Manager, defined in **Section 6.1.1**.
- Default values were used for all other fields.
- Click **Finish**.

Edit Topology Hiding Profile X

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

Finish

There was no requirement to any other Topology Hiding Profile.

7.11. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

7.11.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect voice, video, and/or Instant Messaging (IM). In addition, Application Rules define the maximum number of concurrent voice sessions the network will process in order to prevent resource exhaustion. From the menu on the left-hand side, select **Domain Policies** → **Application Rules**, click on the **Add** button to add a new rule.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies (selected), Application Rules (highlighted in red), Border Rules, Media Rules, Security Rules, Signaling Rules, and Charging Rules. The main content area is titled "Application Rules: default" and includes an "Add" button and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." Below this, there is a table for "Application Rule" configuration. The table has columns for Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The rows show Audio (In: checked, Out: checked, Max Concurrent: 200, Max Sessions: 5) and Video (In: unchecked, Out: unchecked, Max Concurrent: 200, Max Sessions: 5). There is also a "Miscellaneous" section with a "CDR Support" option set to "Off".

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	5
Video	<input type="checkbox"/>	<input type="checkbox"/>	200	5

Miscellaneous

CDR Support: Off

Under **Rule Name** enter the name of the profile, e.g., **2000 Sessions** and click **Next**.

The screenshot shows a form titled "Application Rule" with a close button (X) in the top right corner. The form has a "Rule Name" label and a text input field containing the text "2000 Sessions". Below the input field is a "Next" button.

- Under **Audio** check *In* and *Out* and set the **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint** to recommended values, the value of **2000** for Audio. Repeat for video if needed, the value of **100** for Video was used for the test.
- Click **Finish**.

Editing Rule: 2000 Sessions X

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	100

Miscellaneous

CDR Support

☒ Off
☐ RADIUS
☐ CDR Adjunct

RADIUS Profile

None ▾

Media Statistics Support

☐

Call Duration

☒ Setup
☐ Connect

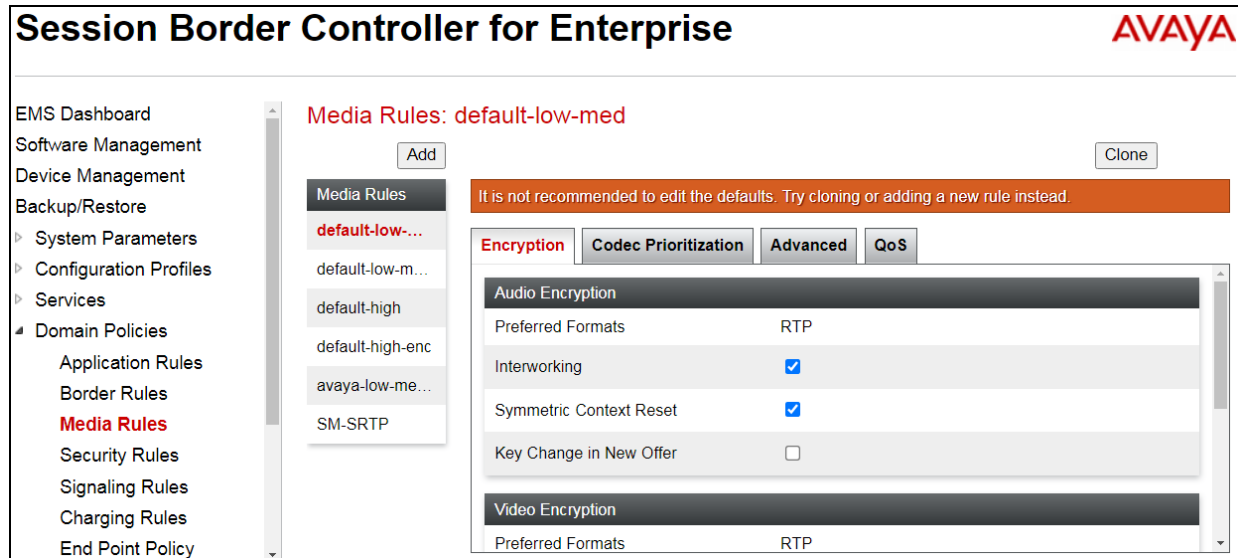
RTCP Keep-Alive

☐

7.11.2. Media Rules

Media Rules allow one to define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, one media rule (shown below) was created toward Session Manager and a default media rule was used toward LifeX.

To add a media rule in the Session Manager direction, from the menu on the left-hand side, select **Domain Policies** → **Media Rules**. Click on the **Add** button to add a new media rule.



- Under **Rule Name** enter **SM_SRTP**.
- Click **Next** (not shown).
- Under Audio Encryption, **Preferred Format #1**, select **SRTP_AES_CM_128_HMAC_SHA1_80**.
- Under Audio Encryption, **Preferred Format #2**, select **RTP**.
- Under Audio Encryption, uncheck **Encrypted RTCP**.
- Under Audio Encryption, check **Interworking**.
- Repeat the above steps under Video Encryption, if needed.
- Under Miscellaneous verify that **Capability Negotiation** is checked.
- Accept default values in the remaining sections by clicking **Next** (not shown), and then click **Finish**.

(See next page)

Media Encryption
X

Audio Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▼
Preferred Format #2	RTP ▼
Preferred Format #3	NONE ▼
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▼
Preferred Format #2	RTP ▼
Preferred Format #3	NONE ▼
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous

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

Finish

For the compliance test, the **default-low-med** Media Rule was used in the LifeX direction.

The screenshot shows a 'Media Encryption' configuration window with three main sections: Audio Encryption, Video Encryption, and Miscellaneous. Each section contains several settings, many of which are identical across sections.

Audio Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
SRTP Context Reset on SSRC Change	<input type="checkbox"/>
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

Video Encryption	
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
SRTP Context Reset on SSRC Change	<input type="checkbox"/>
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2^ <input type="text"/>
Interworking	<input checked="" type="checkbox"/>

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

Finish

7.11.3. Signaling Rules

For the compliance test, the **default** signaling rule was used.

The screenshot shows the 'Signaling Rules: default' configuration window. It includes a sidebar with 'Add' and 'Clone' buttons, and a main area with tabs for 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID'. The 'General' tab is active, showing 'Inbound' and 'Outbound' sections with a table of rules.

Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy

7.12. End Point Policy Groups

End Point Policy Groups associate the different sets of rules under Domain Policies (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. Please note that changes should not be made to any of the default rules used in these End Point Policy Groups.

7.12.1. End Point Policy Group – Enterprise

To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add**.

Enter an appropriate name in the **Group Name** field and click **Next**.

Policy Group

Group Name: SM-Internal

Next

Under the **Policy Group** tab enter the following:

- **Application Rule: 2000 Sessions (Section 7.11.1).**
- **Border Rule: default.**
- **Media Rule: SM-SRTP (Section 7.11.2).**
- **Security Rule: default-low.**
- **Signaling Rule: default (Section 7.11.3).**
- Click **Finish**.

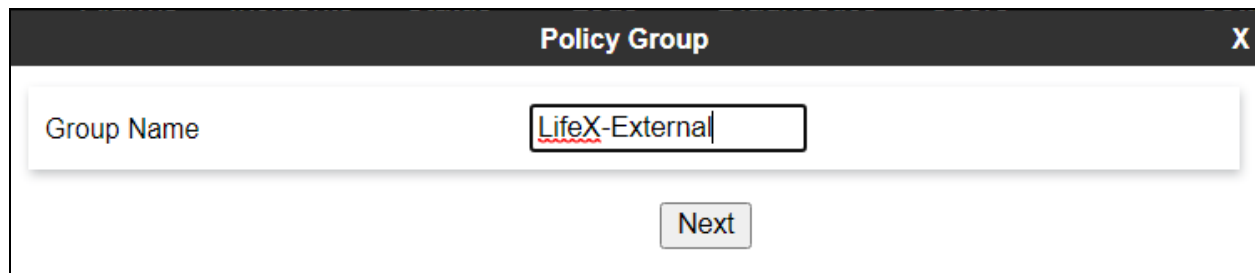
Edit Policy SetX

Application Rule	2000 Sessions ▾
Border Rule	default ▾
Media Rule	SM-SRTP ▾
Security Rule	default-low ▾
Signaling Rule	default ▾
Charging Rule	None ▾
RTCP Monitoring Report Generation	Off ▾

Finish

7.12.2. End Point Policy Group – Service Provider

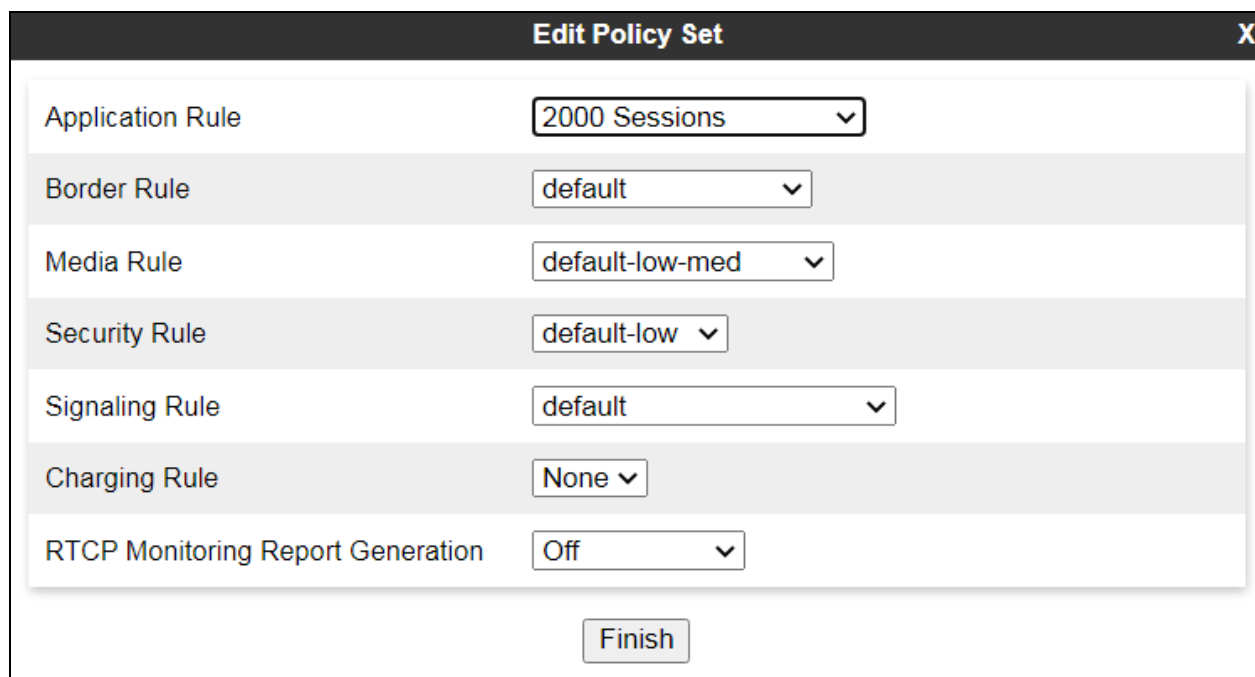
To create an End Point Policy Group for the Service Provider, select **End Point Policy Groups** under the **Domain Policies** menu and select **Add**. Enter an appropriate name in the **Group Name** field and click **Next**.



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

Under the **Policy Group** tab enter the following:

- **Application Rule: 2000 Sessions** (Section 7.11.1).
- **Border Rule: default**.
- **Media Rule: default-low-med** (Section 7.11.2).
- **Security Rule: default-low**.
- **Signaling Rule: default** (Section 7.11.3).
- Click **Finish**.



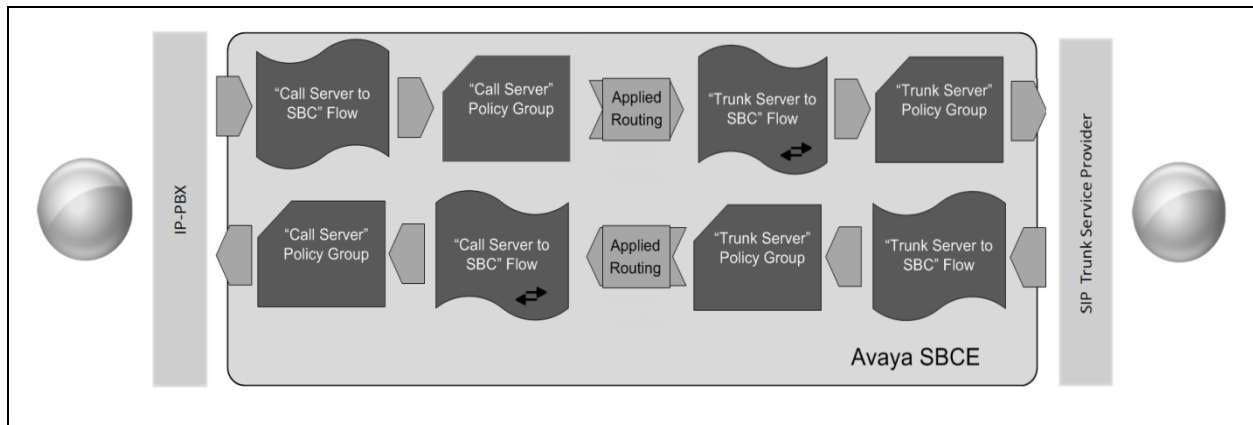
The screenshot shows a dialog box titled "Edit Policy Set" with a close button (X) in the top right corner. Inside the dialog, there are several rows, each with a label and a dropdown menu:

Label	Value
Application Rule	2000 Sessions
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

At the bottom of the dialog is a button labeled "Finish".

7.13. End Point Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy group which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP trunk call.



The **End-Point Flows** defines certain parameters that pertain to the signaling and media portions of a call, whether it originates from within the enterprise or outside of the enterprise.

7.13.1. End Point Flow – Enterprise

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown).

Session Border Controller for Enterprise AVAYA

End Point Flows

Subscriber Flows **Server Flows** Add

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

Hover over a row to see its description.

SIP Server: Avaya-SM-TLS

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	To Avaya-SM Flow	*	Sig-External	Sig-Internal	SM-Internal	ToLifeX-TLS	View Clone Edit Delete

The screen below shows the flow named **To Avaya-SM Flow** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for LifeX in **Section 7.9.1**, which is the reverse route of the flow. Click **Finish** (not shown).

Edit Flow: To Avaya-SM Flow		X
Flow Name	<input type="text" value="To Avaya-SM Flow"/>	
SIP Server Profile	Avaya-SM-TLS ▾	
URI Group	* ▾	
Transport	* ▾	
Remote Subnet	<input type="text" value="*"/>	
Received Interface	Sig-External ▾	
Signaling Interface	Sig-Internal ▾	
Media Interface	Media_Int ▾	
Secondary Media Interface	None ▾	
End Point Policy Group	SM-Internal ▾	
Routing Profile	ToLifeX-TLS ▾	
Topology Hiding Profile	default ▾	
Signaling Manipulation Script	None ▾	
Remote Branch Office	Any ▾	

7.13.2. End Point Flow – Service Provider

A second Server Flow with the name **To LifeX Flow** was similarly created in the LifeX direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note that the **Routing Profile** selection is the profile created for Session Manager in **Section 7.9.2**, which is the reverse route of the flow. Also note that there is no selection under the **Signaling Manipulation Script** field. Click **Finish** (not shown).

Edit Flow: To LifeX Flow		X
Flow Name	<input type="text" value="To LifeX Flow"/>	
SIP Server Profile	LifeX-SBC-TLS ▾	
URI Group	* ▾	
Transport	* ▾	
Remote Subnet	<input type="text" value="*"/>	
Received Interface	Sig-Internal ▾	
Signaling Interface	Sig-External ▾	
Media Interface	Media_Ext ▾	
Secondary Media Interface	None ▾	
End Point Policy Group	LifeX-External ▾	
Routing Profile	ToAvayaSM-TLS ▾	
Topology Hiding Profile	Avaya-SM ▾	
Signaling Manipulation Script	None ▾	
Remote Branch Office	Any ▾	

8. Configuration of Frequentis AG 3020 LifeX

This section describes the configuration of both the LifeX server and the Oracle Session Border Controller in order to connect to the Avaya Session Border Controller for Enterprise.

8.1. LifeX 3020

This section shows the steps necessary on the LifeX server to facilitate the connection to the Avaya Session Border Controller.

8.1.1. System Access

Access the LifeX Configurator by using a web browser and entering the URL `https://<ip-address>/lifex-configurator/?tenant=<tenant name>`, where `<ip-address>` is the IP address of web server belonging to each LX instance (DCA/DCB/RefSys...) and `<tenant name>` is shortcode of each tenant (SECAMB,NEAS...).

8.1.2. Incoming Calls Configuration

For incoming calls configuration, **SYSTEM** as `<tenant name>` was used. Navigate to section **Incoming SIP event routing** and click Create new incoming routing rule (not shown). Define to which Tenant, from all available tenants, incoming calls should be routed from specific Calling host, in this case `devconnect.local`.

The screenshot displays the Frequentis 3020 LifeX Configurator web interface. The top header shows the title 'FREQUENTIS 3020 LifeX Configurator' and the timestamp '9:00:03 AM 06/11/2021'. On the left, a sidebar menu includes 'System tenant users', 'Tenants', 'Service settings', and 'Incoming SIP event routing', with the last option being the active selection. The main content area is titled 'Incoming SIP event routing' and contains several configuration fields: 'Calling user (FROM)' with a value of '1', 'Calling host (FROM)' with 'devconnect.local', 'Called user (TO)' with '*', 'Called host (TO)' with '*', 'Source host (CONTACT)' with '*', and 'Tenant' set to 'SECAMB' via a dropdown menu. A 'Comment' field is also present but empty. At the bottom, there are 'Save', 'Cancel', and a trash icon button.

8.1.3. Outgoing Calls Configuration

For outgoing calls configuration, specific site as <tenant name> was used, in this case SECAMB tenant was used.

First navigate to **Trunking** → **Trunks** in the left window and click create new trunk (there is a + on the button). Name the new trunk and select **Telephony** as **Trunk type**. **Enable endpoint monitoring** and set **Monitoring interval** and **Response timeout**. At the end configure endpoint in the format <ip-address>:5061, where <ip-address> is IP of SBC SIP interface INT_PHONE dedicated for media flow between LifeX and the Oracle SBC. Realm INT_PHONE is described in **Section 8.2**.

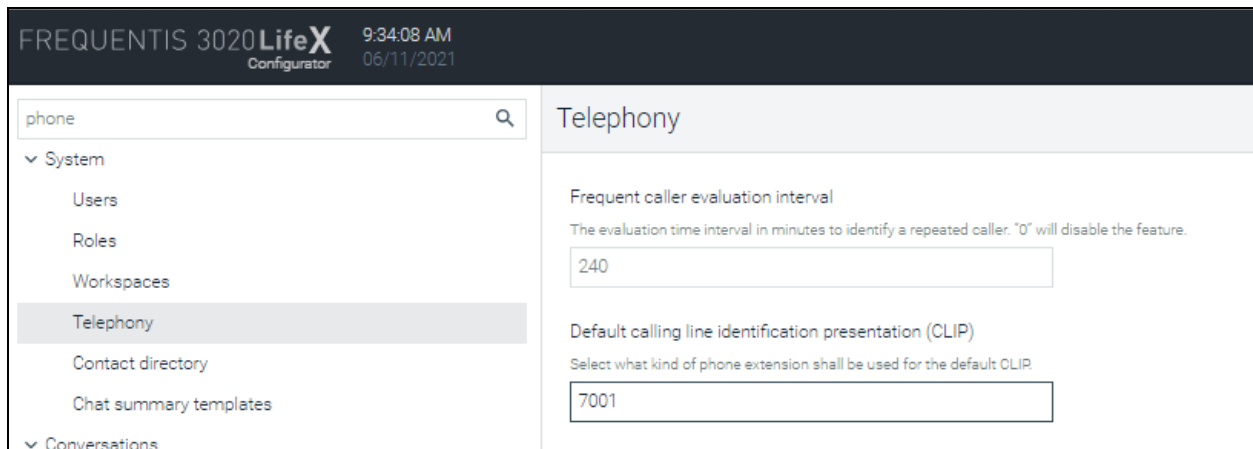
Note: Some sensitive information has been blocked out from some of the screen shots.

The screenshot shows the 'FREQUENTIS 3020 LifeX Configurator' interface. The left sidebar has a search bar and a list of options under 'Trunking', with 'Trunks' selected. The main panel is titled 'Trunks' and shows the configuration for a new trunk. The 'Trunk name' is 'SECAMB-SBC-Fourmet-Away-PBX'. The 'Trunk type' is 'Telephony'. The 'Default trunk' checkbox is unchecked. The 'Capacity' field is empty. The 'Load balancing strategy' is 'Round-robin'. The 'Enable endpoint monitoring' checkbox is checked. The 'Monitoring interval' is 6 seconds. The 'Response timeout' is 2 seconds. The 'Endpoints' table has one row with 'Endpoint' '5061' and 'Capacity' '1'. The bottom of the screen has a 'Save' button.

After trunk is created navigate to **Outgoing phone call trunk assignment** and click create new rule. **Name** the new rule and select to which LifeX Roles should be **Assigned**.

Scroll down to the bottom and select the telephony trunk that was created in the previous step from the **Trunk** drop down. A range of allowed phone numbers for outgoing phone calls is also defined. To have the possibility of calling any number, leave **Number range from** and **Number range to** empty.

Default CLIP configuration is under the **System** → **Telephony** in the left window. Typically this would be the “main number” associated with the system.



The screenshot shows the Frequentis 3020 LifeX Configurator web interface. The top header displays the product name, time (9:34:08 AM), and date (06/11/2021). On the left, a navigation menu lists various system components, with 'Telephony' selected under the 'System' category. The main content area is titled 'Telephony' and contains two configuration sections. The first section, 'Frequent caller evaluation interval', includes a description and a text input field containing '240'. The second section, 'Default calling line identification presentation (CLIP)', includes a description and a text input field containing '7001'.

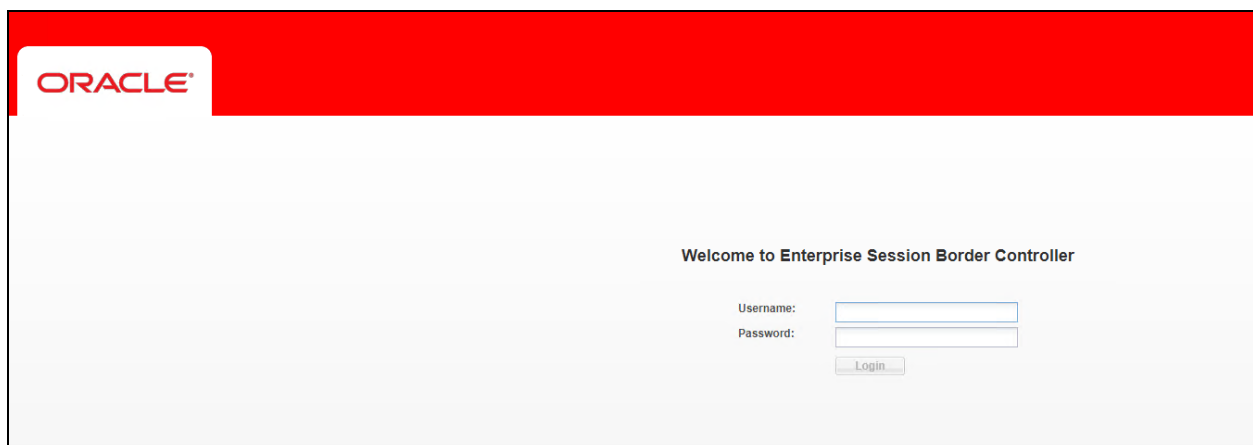
8.2. Oracle SBC-E

Frequentis use an SBC-E from Oracle as a SIP trunk between LifeX system and 3rd party sites. The reason is that Frequentis systems are more and more connected to customer equipment via IP (SIP trunks) instead of traditional legacy lines.

A **session border controller** (SBC) is a device regularly deployed in Voice over Internet Protocol (VoIP) networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications.

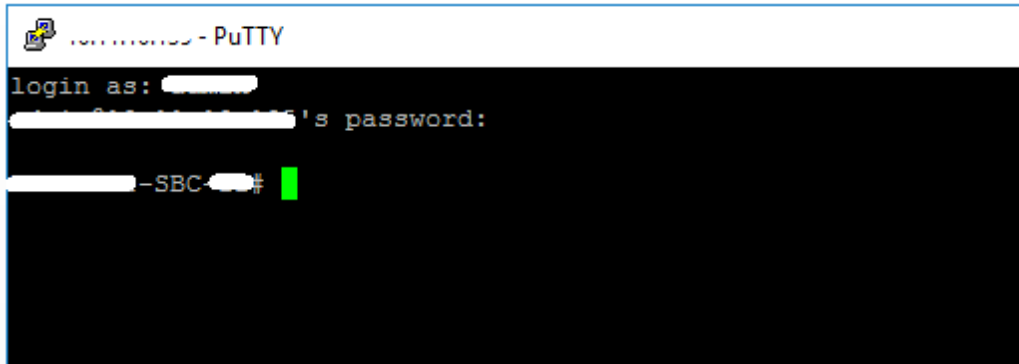
8.2.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL <https://<ip-address>>, where <ip-address> is the management IP address configured at installation. Also, the command line interface can be accessed using a ssh client i.e., “PuTTY”. Log in using the appropriate credentials.

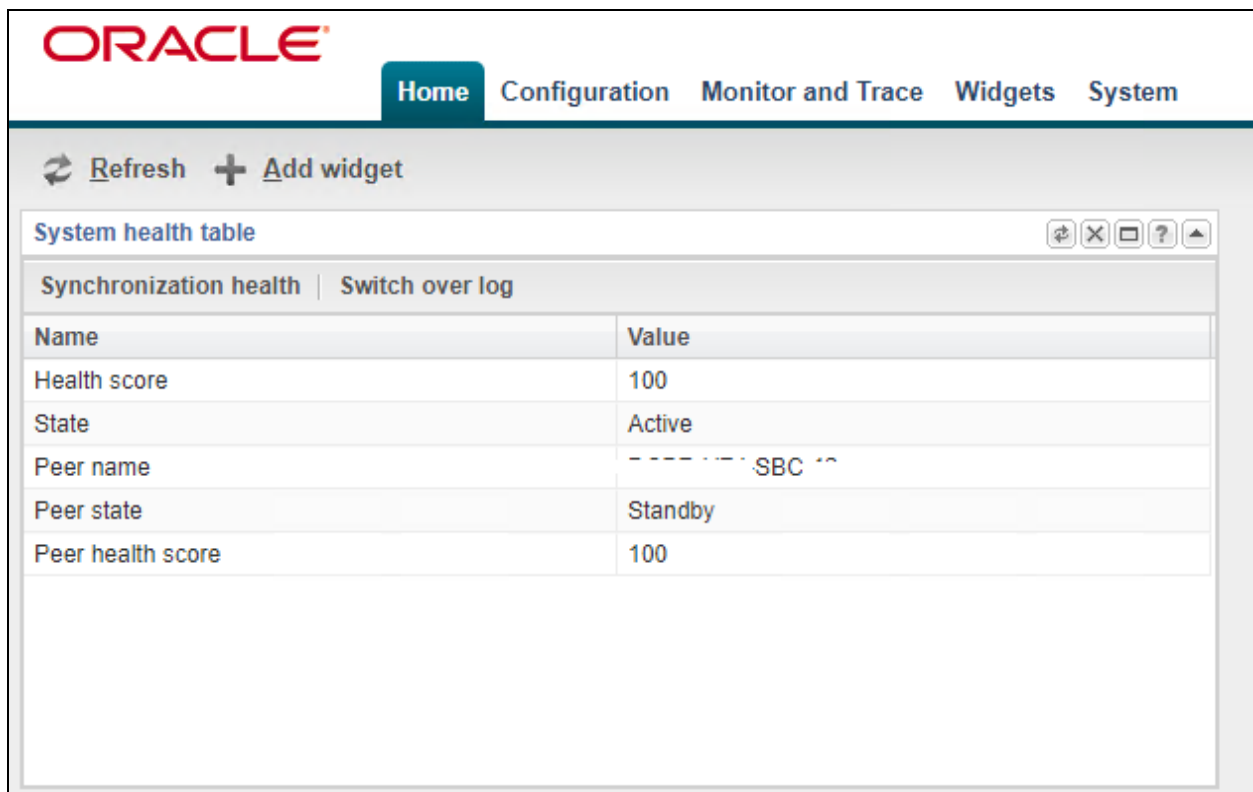


The screenshot shows the Oracle Enterprise Session Border Controller login page. It features a red header with the Oracle logo. The main content area is white and contains the text 'Welcome to Enterprise Session Border Controller'. Below this, there are two input fields labeled 'Username:' and 'Password:', followed by a 'Login' button.

The screen shot below shows the interface using **PuTTY**.



Once logged in, on the top of the screen, 5 tabs should be visible. The **Home** tab is a dashboard where widgets can be added from **Widgets** tab.



The **Configuration** tab provides a graphical display of the same objects and elements that can be accessed by CLI. Also, it provides some configuration Wizards and Commands.

Name	Description
access-control	Configure a static or dynamic access control list
account-config	Configure Quality of Service accounting
certificate-record	Create, generate, and import a certificate

The **Monitor and Trace** tab displays the results of filtered SIP session data from the SBC. It supports the summary reports.

- Sessions
- Registrations
- Subscriptions
- Notable Events

Double-click on a line entry opens the Ladder Diagram window with session details, not shown here but described in the verification steps in **Section 9.4.2**.

Start Time	State	Call ID	Request URI	From URI	To URI	Ingress Realm	Egress Realm	Duration	Notable Event
2021-06-02 14:54:03.233	TERMINATED...	fd5729fec3a941eb944e0...	sip:7004@devconnect.local	"PSTN-Caller-ONE" <sip...	<sip:7004@devconnect.lo...	EXT_PHONE	EXT_PHONE	7	

The **Widgets** tab contains a list of all available widgets that can be used to view system data and statistics. A **license** can be added here under **System** → **Licenses**.

Name	Description
Alarms table	Displays existing alarms and allows the user to clear them
Current memory usage pie graph	Pie graph displays current percentage of free and allocated memory.
Editing configuration short	<i>show configuration short</i> - Displays the modified attributes only in the editing configuration
MBCD realms	<i>show mbcd realms</i> - Displays statistics of all MB CD Realms
Sessions	<i>show sessions</i> - Displays session capacity for license and session use
System health table	System health table

The **System** tab provides the following ways to manage files on the system.

- **File Management**
- **Force HA switchover**
- **Reboot**
- **Support Information**
- **Upgrade software**

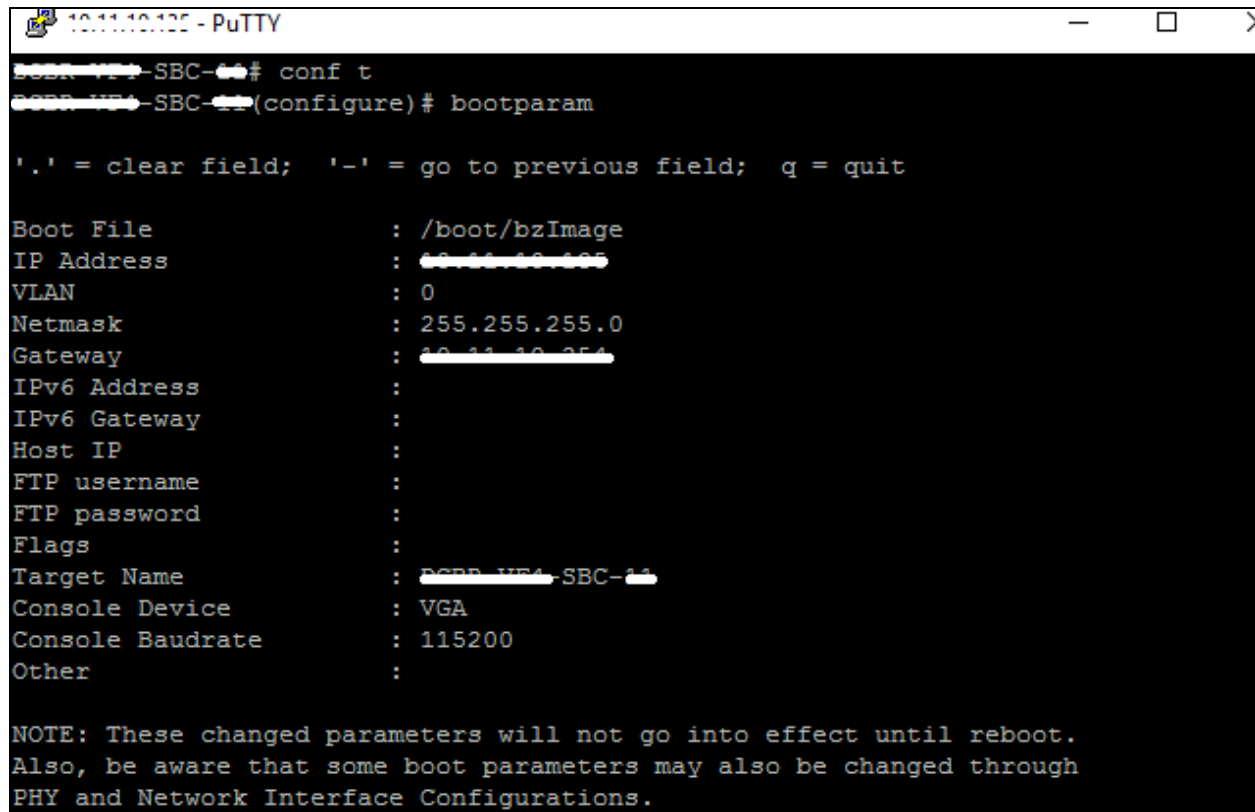
The screenshot shows the Oracle System tab interface. The top navigation bar includes Home, Configuration, Monitor and Trace, Widgets, and System. The System tab is active. On the left, a sidebar lists options: File management, Force HA switchover, Reboot, Support information, and Upgrade software. The main area is titled 'File Management' and features a 'File type:' dropdown menu set to 'Backup configuration'. Below this are buttons for Refresh, Upload, Download, Backup, Restore, and Delete. A table with a 'Name' header is partially visible at the bottom.

8.2.2. System configuration

The basic system configuration is configured under **Configuration→Objects→System**.

The screenshot shows the Oracle Configuration tab interface. The top navigation bar includes Home, Configuration, Monitor and Trace, Widgets, and System. The Configuration tab is active. On the left, a sidebar lists various system objects, with 'system-config' selected. The main area is titled 'Modify System config' and contains several input fields and checkboxes. The 'Hostname' field is pre-filled with 'ACORN-WF4-SBC-44'. The 'Description' field is empty. The 'Location' field is empty. The 'Mib system contact' field is empty. The 'Mib system name' field is empty. The 'Mib system location' field is empty. The 'Acp TLS profile' field is empty. The 'SNMP enabled' checkbox is checked. The 'Enable SNMP auth traps' checkbox is unchecked. The 'Enable SNMP syslog notify' checkbox is unchecked. The 'Enable SNMP monitor traps' checkbox is unchecked. The 'Enable env monitor traps' checkbox is unchecked. The 'Enable mblk_tracking' checkbox is unchecked. The 'Enable I2 miss report' checkbox is checked. Below these fields is a section for 'Syslog servers' with buttons for Add, Edit, Copy, and Delete. A table with columns for Address, Port, and Facility is partially visible at the bottom.

The management IP is set during the OVF deployment. This can be changed using the CLI command **bootparam**. It is interface **wancom0**.



```
10.11.10.125 - PuTTY
PCPB-INT4-SBC-111# conf t
PCPB-INT4-SBC-111(configure)# bootparam

'.' = clear field; '-' = go to previous field; q = quit

Boot File           : /boot/bzImage
IP Address          : 10.11.10.180
VLAN                : 0
Netmask             : 255.255.255.0
Gateway             : 10.11.10.254
IPv6 Address        :
IPv6 Gateway        :
Host IP             :
FTP username        :
FTP password        :
Flags               :
Target Name         : PCPB-INT4-SBC-111
Console Device      : VGA
Console Baudrate    : 115200
Other               :

NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.
```

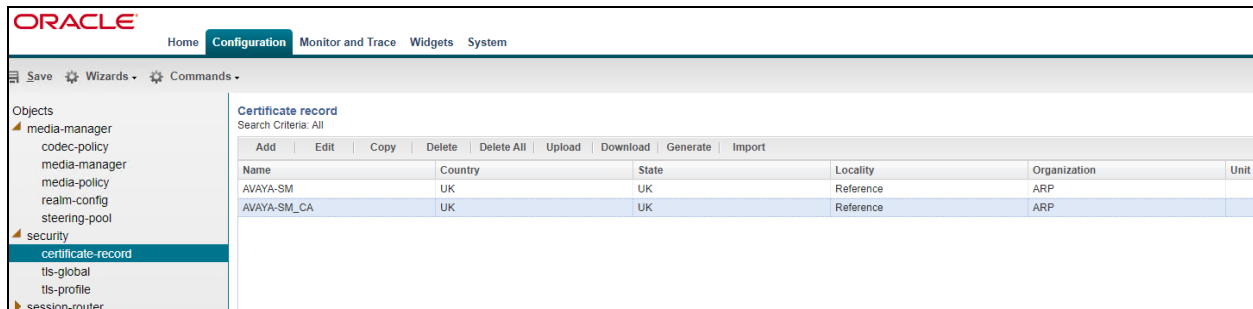
These commands can be run from the CLI command or, as displayed on the screen from the previous page, can be run from the GUI.

- **system-config**: set hostname and default gateway to be used.
- **snmp-community**: configure SNMP communities and IPs of monitoring servers (Zabbix).
- **redundancy-config**: a routing policy for SIP failover – primary and secondary node of HA cluster.
- **phy-interface**: add or edit interfaces for management and media.
 - wancom1** is dedicated for HA failover - operational type Control
 - INT** is dedicated for internal media flow - operational type Media
 - EXT** is dedicated for external media flow - operational type Media
- **ntp-config**: clock sync.
- **network interface**: set IP for physical interface, public IP (EXT) 10.11.180.180 - 3rd party, private IP (INT) X.X.X.X – LifeX
- **host-route**: routing table; 3rd party route: destination networks → 10.13.2.0/24; 10.13.4.0/24, Gateway 10.11.180.254

8.2.3. Security – TLS configuration

Frequentis use secured communications between LifeX and 3rd party vendors (PBX, VR) as standard practice. For this to happen, it is required to have configured a certificate record and imported a certificate issued by 3rd party.

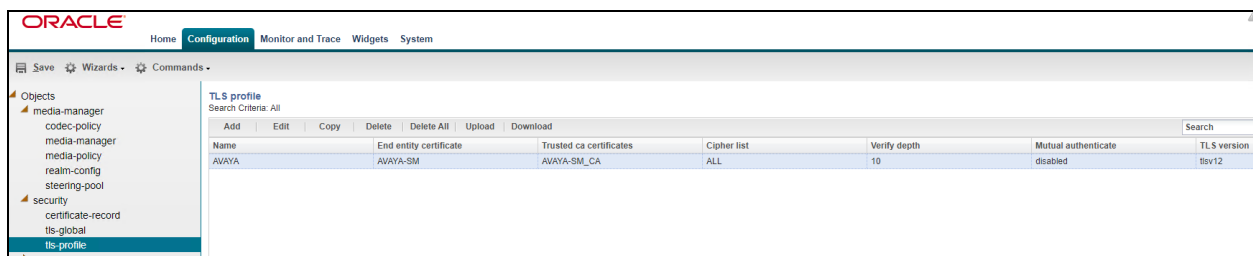
To create a certificate record, navigate to **Configuration→Objects→security→certificate-records** in the left window. There are two records present, one for private certificate (signed a generated CSR of SBC-E by CA) and root certificate of Certification Authority (in this case it is the Avaya System Manager).



The screenshot shows the Oracle Configuration interface. The left sidebar has a tree view with 'security' expanded and 'certificate-record' selected. The main panel displays a table of certificate records.

Certificate record						
Search Criteria: All						
Add	Edit	Copy	Delete	Delete All	Upload	Download
Name	Country	State	Locality	Organization	Unit	
AVAYA-SM	UK	UK	Reference	ARP		
AVAYA-SM_CA	UK	UK	Reference	ARP		

Create a TLS profile where both certificate records are used by clicking on **tls-profile** in the left window. How to apply this TLS profile is described in **Section 8.2.5**.



The screenshot shows the Oracle Configuration interface with 'tls-profile' selected in the left sidebar. The main panel displays a table of TLS profiles.

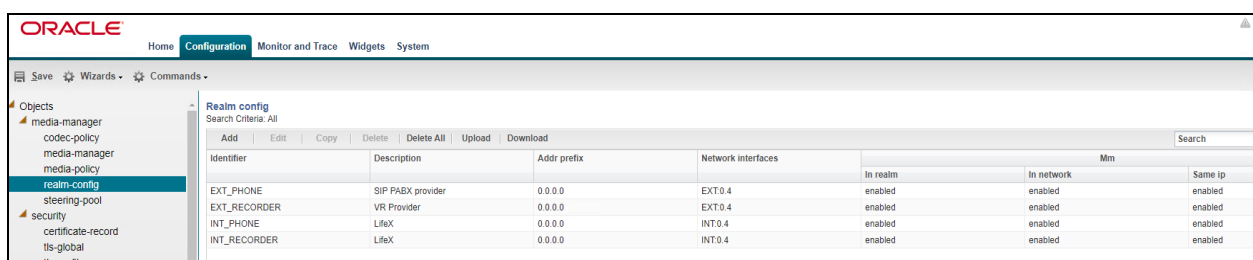
TLS profile						
Search Criteria: All						
Add	Edit	Copy	Delete	Delete All	Upload	Download
Name	End entity certificate	Trusted ca certificates	Cipher list	Verify depth	Mutual authenticate	TLS version
AVAYA	AVAYA-SM	AVAYA-SM_CA	ALL	10	disabled	tlsv12

8.2.4. Media Manager – REALM Config

Realms are a logical distinction representing routes (or groups of routes) reachable by the SBC and what kinds of resources and special functions apply to those routes. A **REALM** must be seen as an “area” / “territory” / “region”. It may include multiple session agents and / or SIP interfaces.

There are four realms created, two for LifeX (using the network interface for internal media flow described in **Section 8.2.2**) and two for 3rd Party (using the network interface for external media flow described in **Section 8.2.2**). All realms reference network interfaces on the SBC.

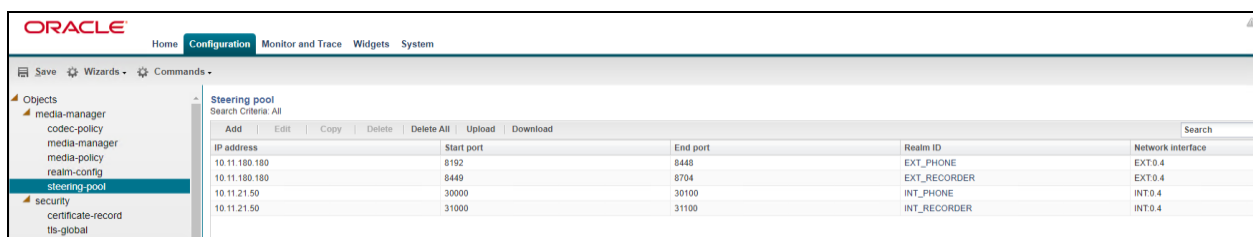
To create a new realm, navigate to **Configuration→Objects→media manager→realm-config** in the left window.



The screenshot shows the Oracle SBC configuration interface. The left sidebar lists the navigation path: Objects > media-manager > realm-config. The main area displays a table titled 'Realm config' with the following data:

Identifier	Description	Addr prefix	Network interfaces	In realm	In network	Same ip
EXT_PHONE	SIP PABX provider	0.0.0.0	EXT.0.4	enabled	enabled	enabled
EXT_RECORDER	VR Provider	0.0.0.0	EXT.0.4	enabled	enabled	enabled
INT_PHONE	LifeX	0.0.0.0	INT.0.4	enabled	enabled	enabled
INT_RECORDER	LifeX	0.0.0.0	INT.0.4	enabled	enabled	enabled

To define a set of ports that are used for steering media flows, click on **steering-pool**. A set for every realm is defined.



The screenshot shows the Oracle SBC configuration interface. The left sidebar lists the navigation path: Objects > media-manager > steering-pool. The main area displays a table titled 'Steering pool' with the following data:

IP address	Start port	End port	Realm ID	Network interface
10.11.180.180	8192	8448	EXT_PHONE	EXT.0.4
10.11.180.180	8449	8704	EXT_RECORDER	EXT.0.4
10.11.21.50	30900	30100	INT_PHONE	INT.0.4
10.11.21.50	31000	31100	INT_RECORDER	INT.0.4

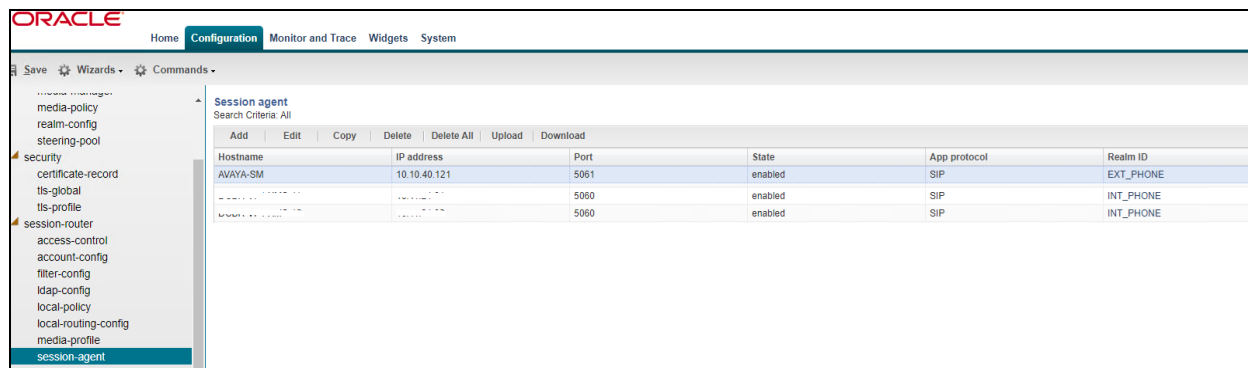
8.2.5. Session Router

Session Router provides high-performance SIP routing with scalable routing policies that increase overall network capacity and reduce cost. It plays a central role in Oracle’s open session routing architecture and helps service providers build a scalable, next-generation signaling core for SIP-based services.

SIP agents are created to specify the IP addresses and ports in which the SBC-E will listen for signalling traffic in the connected networks. SIP agent defines a signaling endpoint.

To create a new Session agent, navigate to **Configuration→Objects→session-router→session-agent** in the left window.

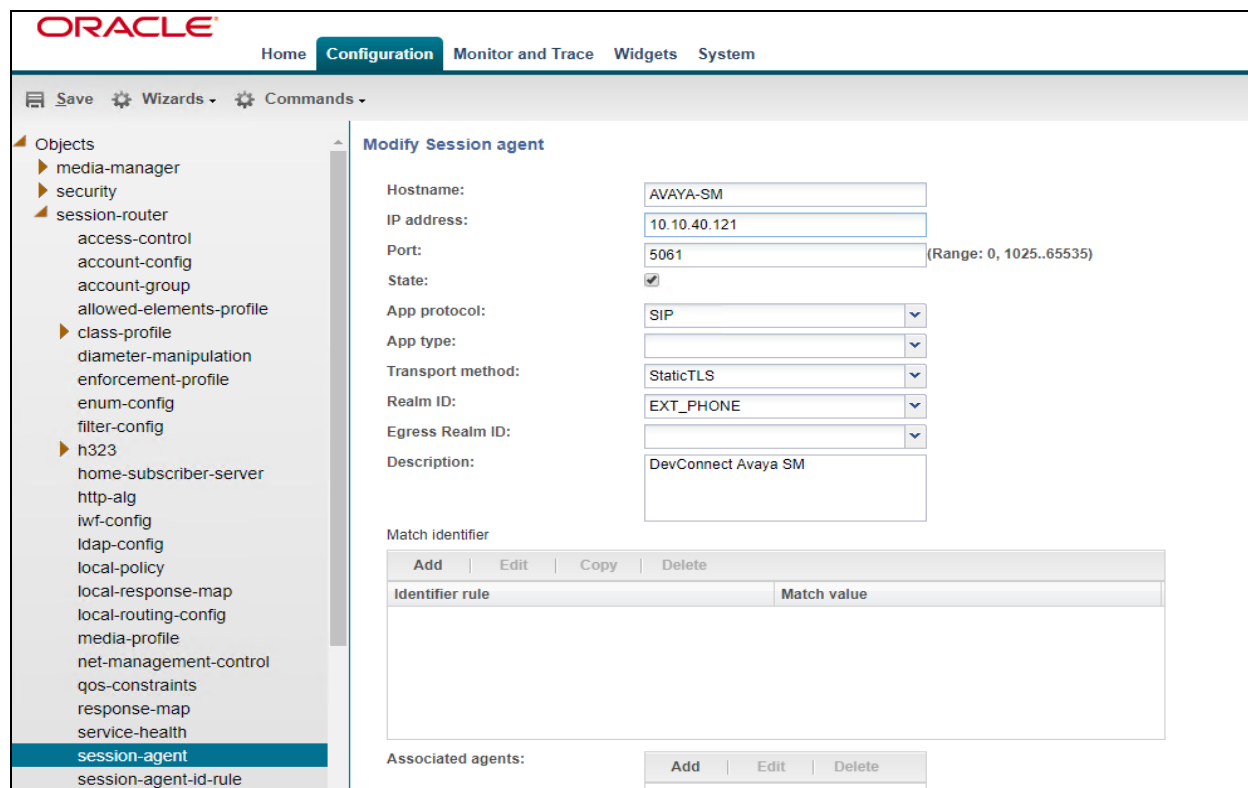
Two session agents are created for the LifeX testing environment (two media servers working as HA failover cluster) with UDP/TPC transport method. Both of these have the **Realm ID** set to **INT_PHONE**, the **Port** is set to **5060**. There is one session agent for the Avaya SBCE with the **IP address** set to that of the Avaya SBCE. Clicking on this will open the window at the bottom of the screen where some further details can be observed.



The screenshot shows the Oracle Configuration interface. The left sidebar lists various configuration objects, with 'session-agent' selected. The main panel displays a table of Session agents.

Hostname	IP address	Port	State	App protocol	Realm ID
AVAYA-SM	10.10.40.121	5061	enabled	SIP	EXT_PHONE
		5060	enabled	SIP	INT_PHONE
		5060	enabled	SIP	INT_PHONE

A suitable name is given for the Avaya SBCE with the **IP address** set to that of the Avaya SBC which is **10.10.10.121**, the **Realm ID** is set to **EXT_PHONE**, with the **Port** set to **5061**. The **Transport method** is set to **StaticTLS**.



The screenshot shows the 'Modify Session agent' form in the Oracle Configuration interface. The left sidebar lists various configuration objects, with 'session-agent' selected. The main panel displays the form fields for a session agent.

Modify Session agent

Hostname: AVAYA-SM

IP address: 10.10.40.121

Port: 5061 (Range: 0, 1025..65535)

State: ☒

App protocol: SIP

App type:

Transport method: StaticTLS

Realm ID: EXT_PHONE

Egress Realm ID:

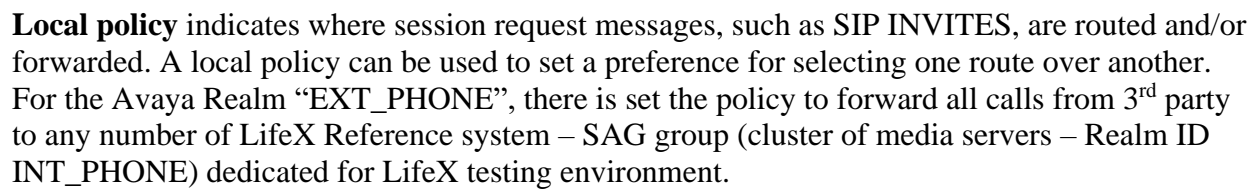
Description: DevConnect Avaya SM

Match identifier

Identifier rule	Match value

Associated agents: Add Edit Delete

To add a new session group, navigate to **session-router**→**session-group** in the left window.



SIP interface defines the transport sockets (IP address and port) upon which the SBC receives and sends SIP messages. SIP interfaces support UDP/TCP/TLS/SCTP Stream Control Transmission Protocol (SCTP) transport, as well as multiple SIP ports. A SIP interface can be defined for each network or realm to which the SBC is connected.

Every SIP interface references a **Realm ID**, as shown below. In this case one SIP interface is used for internal SIP communication with LifeX and one SIP interface for external SIP communication with Avaya SBCE. These are added as TCP and TLS as described in **Section 8.2.3**.

The **INT_PHONE** sip interface is shown below. Frequentis use port 5061 with UDP transport for communication between LifeX and the Oracle SBC.

The screenshot shows the Oracle SBC Configuration interface. The left sidebar contains a tree view of configuration categories, with 'sip-interface' selected. The main panel is titled 'Modify SIP interface' and contains the following fields and sections:

- State:** A checkbox that is checked.
- Realm ID:** A dropdown menu with 'INT_PHONE' selected.
- Description:** A text input field.
- SIP ports:** A table with columns: Address, Port, Transport protocol, TLS profile, and Allow anonymous. It contains one entry: Address: 10.11.21.50, Port: 5061, Transport protocol: UDP, TLS profile: (empty), Allow anonymous: all.
- Nat traversal:** A dropdown menu with 'none' selected.
- Registration caching:** A checkbox that is unchecked.
- Route to registrar:** A checkbox that is unchecked.
- In manipulationid:** A dropdown menu.
- Out manipulationid:** A dropdown menu.
- Service tag:** A text input field.

The **EXT_PHONE** sip interface, which shows all three transport protocols configured for use.

The screenshot shows the Oracle SIP interface configuration page. The left sidebar contains a tree view with categories like media-manager, security, session-router, and sip-interface. The main area is titled 'Modify SIP interface' and contains the following fields:

- State: ☒
- Realm ID:
- Description:

Below these fields is a table titled 'SIP ports' with columns: Address, Port, Transport protocol, TLS profile, and Allow anonymous. The table contains three rows:

Address	Port	Transport protocol	TLS profile	Allow anonymous
10.11.180.180	5060	UDP		all
10.11.180.180	5060	TCP		all
10.11.180.180	5061	TLS	AVAYA	all

Below the table are several configuration options:

- Nat traversal:
- Registration caching: ☐
- Route to registrar: ☐
- In manipulationid:
- Out manipulationid:
- Service tag:

SIP manipulation is configured, as variances among SIP networks can degrade SIP services or disrupt SIP operations. To resolve these variances, Header Manipulation Rules (HMR) are giving network administrators the ability to control SIP traffic by manipulating SIP messages. The manipulation of SIP messages is carried out because of functionality, security and 3rd party requirements. Below is an example of the SIP manipulation used for compliance testing.

ORACLE

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands

media-manager
media-policy
realm-config
steering-pool
security
certificate-record
tls-global
tls-profile
session-router
access-control
account-config
filter-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
translation-rules
system
fraud-protection
host-route
network-interface
ntp-config

Modify SIP manipulation

Name: NAT_plus_SIPREC

Description: Hide SIP traffic behind SBC. Rewrite or remove all sensitive fields.

Split headers: Add Edit Delete

Join headers: Add Edit Delete

CfgRules

Name	Element type
HR_NAT_MsgHdr_Contact_out	header-rule
HR_NAT_MsgHdr_Contact_in	header-rule
HR_NAT_ReqURI	header-rule
HR_NAT_MsgHdr_From	header-rule
HR_NAT_MsgHdr_To	header-rule

9. Verification Steps

The following steps can be taken to ensure that connections between the Avaya platform and the Frequentis platform successfully in place.

9.1. Session Manager Registration

Log into System Manager as per **Section 6**. Navigate to **Elements** and click on **Session Manager**.

The screenshot displays the Avaya Aura System Manager 8.0 web interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The 'Elements' menu is expanded, showing a list of system components. The 'Session Manager' option is highlighted with a red box. The main content area is divided into several panels: 'System Resource Utilization' (a bar chart showing utilization for 'opt', 'var', and 'emdata'), 'Alarms' (a circular gauge showing 'Critical', 'Major', 'Minor', and 'Warning' levels), 'Application State' (a table showing the status of various components), 'Notifications' (a list of alerts), 'Information' (a table showing the count and sync status of elements), and 'Shortcuts' (a list of shortcuts). The 'Session Manager' panel shows a list of instances with their status and a 'Management Instance check failed' message.

Elements	Count	Sync Status
CM	1	■
Session Manager	1	■
System Manager	1	■
UCM Applications	8	■

Current Usage:
11/250000 USERS
1/50 SIMULTANEOUS ADMINISTRATIVE LOGINS

Select the Avaya SBCE SIP Entity.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾

Home Session Manager ×

Session Manager ▾

- Dashboard
- Session Manager Ad...
- Global Settings
- Communication Prof...
- Network Configur... ▾
- Device and Locati... ▾
- Application Confi... ▾
- System Status ▾
- SIP Entity Monit...**
- Managed Band...
- Security Module...

<input type="checkbox"/>	Session Manager	Type	Monitored Entities	
			Down	Partially Up
<input type="checkbox"/>	SM81vmjpg	Core	17	0

Select : All, None

All Monitored SIP Entities

Run Monitor

26 Items

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	Presence
<input type="checkbox"/>	breeze4oc37-sm100
<input type="checkbox"/>	breeze5oc37-sm100
<input type="checkbox"/>	breeze6oc37-sm100
<input type="checkbox"/>	EP723(MPP)
<input type="checkbox"/>	breeze1wspaces37-sm100
<input type="checkbox"/>	SBCEforLifeX
<input type="checkbox"/>	aacc71x
<input type="checkbox"/>	aacc71spare
<input type="checkbox"/>	breeze2wspaces37-sm100
<input type="checkbox"/>	breeze3wspaces37-sm100

The SIP Entity should show as **UP** as it is shown below. The example below shows a connection for both TLS and TCP; however, the TLS connection was the only connection used during compliance testing.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: SBCEforLifeX

Summary View

2 Items Filter: Enable

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	SM81vmjpg	IPv4	10.10.40.120	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	SM81vmjpg	IPv4	10.10.40.120	5061	TLS	FALSE	UP	200 OK	UP

Select : None

9.2. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

Alarms: This screen provides information about the health of the SBC.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top taskbar includes the following links: Device: sbceforfrequentis, Alarms (highlighted with a red box), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various management options, with "Device Management" highlighted in red. The main content area is titled "Device Management" and contains several tabs: Devices, Updates, SSL VPN, Licensing, Key Bundles, and License Compliance. The "Devices" tab is active, showing a table with the following data:

Device Name	Management IP	Version	Status	
sbceforfrequentis	10.10.41.120	8.1.2.0-31-19809	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

The following screen shows the **Alarm Viewer** page.

The screenshot shows the Avaya Alarm Viewer web interface. The top taskbar includes the following links: Device: sbceforfrequentis, Help, and Log Out. The main header displays "Alarm Viewer" and the Avaya logo. On the left, a sidebar menu lists various management options, with "Alarms" highlighted in red. The main content area is titled "Alarms" and contains a table with the following data:

ID	Details	State	Time	Device
No alarms found for this device.				

At the bottom of the table, there are two buttons: "Clear Selected" and "Clear All".

Incidents: Provides detailed reports of anomalies, errors, policies violations, etc.

Device: sbceforfrequentis Alarms **Incidents** Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard
Software Management
Device Management
Backup/Restore
▶ System Parameters
▶ Configuration Profiles
▶ Services
▶ Domain Policies
▶ TLS Management
▶ Network & Flows
▶ DMZ Services
▶ Monitoring & Logging

Device Management

Devices Updates SSL VPN Licensing Key Bundles License Compliance

Device Name	Management IP	Version	Status	
sbceforfrequentis	10.10.41.120	8.1.2.0-31-19809	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

The following screen shows the **Incident Viewer** page. The incidents can be filtered as shown below. The example below also includes some old incidents that occurred during the setup phase.

Incident Viewer

AVAYA

Device All Category All Clear Filters Refresh Generate Report

15 out of 2000.

ID	Device	Category	Type	Cause
810932075767040	sbceforfrequentis	Policy	BYE Message Out of Dialog	General Method not allowed Out-Of-Dialog
810768124193448	sbceforfrequentis	Policy	Message Dropped	No Server Flow Matched for Outgoing Message
810768121194248	sbceforfrequentis	Policy	Message Dropped	No Server Flow Matched for Outgoing Message
810767941196221	sbceforfrequentis	Policy	Message Dropped	No Server Flow Matched for Outgoing Message
810767938196216	sbceforfrequentis	Policy	Message Dropped	No Server Flow Matched for Outgoing Message
810767935196734	sbceforfrequentis	Policy	Message Dropped	No Server Flow Matched for Outgoing Message
810767932197492	sbceforfrequentis	Policy	Message Dropped	No Server Flow Matched for Outgoing Message
810767929196227	sbceforfrequentis	Policy	Message Dropped	No Server Flow Matched for Outgoing Message

Diagnostics: This screen provides a variety of tools to test and troubleshoot the Avaya SBCE network connectivity.

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

Session Border Controller for Enterprise

AVAYA

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

Device Management

Devices Updates SSL VPN Licensing Key Bundles License Compliance

Device Name	Management IP	Version	Status
sbceforfrequentis	10.10.41.120	8.1.2.0-31-19809	Commissioned

Reboot Shutdown Restart Application View Edit Uninstall

The following shows a **Full Diagnostic** test being performed.

Diagnostics

AVAYA

Full Diagnostic Ping Test

Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.

Start Diagnostic

Task Description	Status
✓ EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ Ping: SBC (A1) to Gateway (10.10.40.1)	Average ping from 10.10.40.121 [A1] to 10.10.40.1 is 0.556ms.
✓ Ping: SBC (A1) to Primary DNS (10.10.40.1)	Average ping from 10.10.40.121 [A1] to 10.10.40.1 is 0.637ms.
✓ Ping: SBC (A1) to Secondary DNS (10.10.40.5)	Average ping from 10.10.40.121 [A1] to 10.10.40.5 is 0.865ms.

9.3. Observe the connection using the Avaya Session Border Controller for Enterprise tracesbc tool

By opening PuTTY and connecting to the Avaya SBCE, a **traceSBC** tool can be run by typing in `tracesbc`, the following shows the **OPTIONS** and **200 OK** messaging being passed back and forth which signals that the devices are connected and sending/receiving SIP messages. When calls are made the SIP messaging can be analysed here also.

10.10.40.32		10.11.180.180	
		SBC	
14:36:56.995	→OPTIONS→		SIP: sip:10.10.40.120;transport=tls
14:36:56.996	→OPTIONS→		SIP: sip:10.10.40.120;transport=tcp
14:36:56.996		→OPTIONS→	SIP: sip:devconnect.local;transport=tls
14:36:56.996		→OPTIONS→	SIP: sip:devconnect.local;transport=tls
14:36:57.096		←200 OK←	SIP: 200 OK (OPTIONS)
14:36:57.096	←200 OK←		SIP: 200 OK (OPTIONS)
14:36:57.097		←200 OK←	SIP: 200 OK (OPTIONS)
14:36:57.097	←200 OK←		SIP: 200 OK (OPTIONS)

Capture filter: <NO FILTER>

Display filter: <NO FILTER>

SIP

PPM

STUN

TLS

WEBRTC

AMS

LDAP

s=Stop q=Quit ENTER=Details (f=Filters

PG; Reviewed:
SPOC 6/28/2021

Solution & Interoperability Test Lab Application Notes
©2021 Avaya Inc. All Rights Reserved.

82 of 89
LifeX_SM81_SBC

9.4. Verify LifeX 3020

This section shows the steps that can be taken to verify the connection from the LifeX side.

9.4.1. Frequentis LifeX

To verify a SIP trunk (SBC), access the LifeX dashboard webpage by using https://<IP_address>:<port>/monitor/dashboard/ where IP is the business main server of LifeX reference environment and port is the monitoring service running on it.

The overall status is either Online or Degraded and the **State** below shows **ONLINE**.

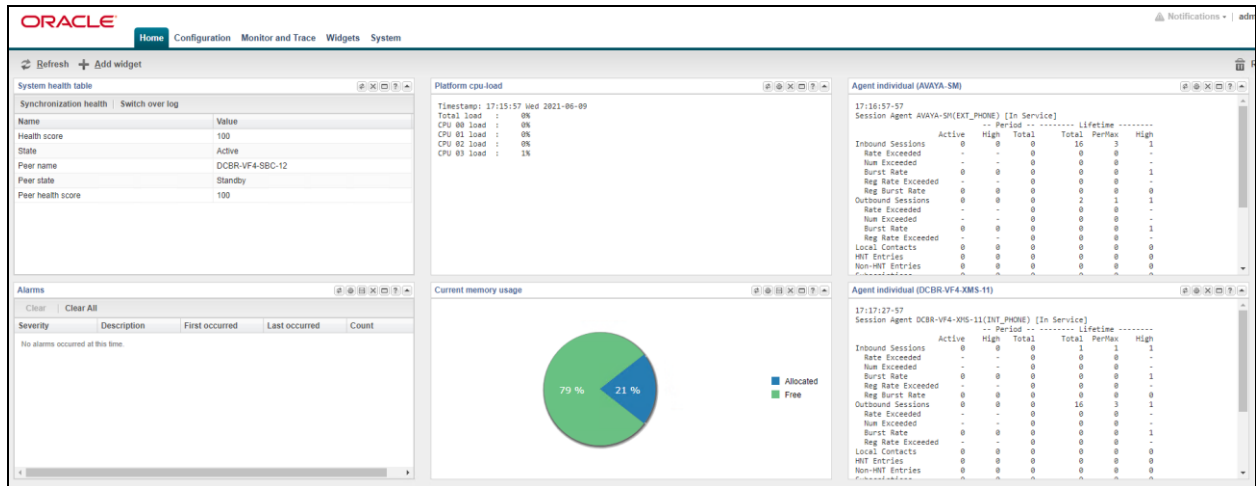
Logged In Sessions	
1	
No data available in table	

Phone Calls (Established/Total)	
0 / 0	
No data available in table	

SIP Trunk states						
Tenant	Trunk Name	Trunk Type	Strategy	Capacity	Overall State	
mess	STR playback	PLAYBACK	ROUND_ROBIN	0	ONLINE	
mess	STR recorder	RECORDING	ROUND_ROBIN	0	ONLINE	
secamb	Tetra-SECAMB	RADIO_TETRA	ROUND_ROBIN	0	ONLINE	
secamb	SECAMB-SBC-Fourmat-Avaya-PBX	TELEPHONY	ROUND_ROBIN	0	ONLINE	
Endpoint		Capacity	Active Connections	State		
sip:1061		0	0	ONLINE		
sss	Instant playback	PLAYBACK	ROUND_ROBIN	0	ONLINE	
mess	STR recorder	RECORDING	ROUND_ROBIN	0	ONLINE	

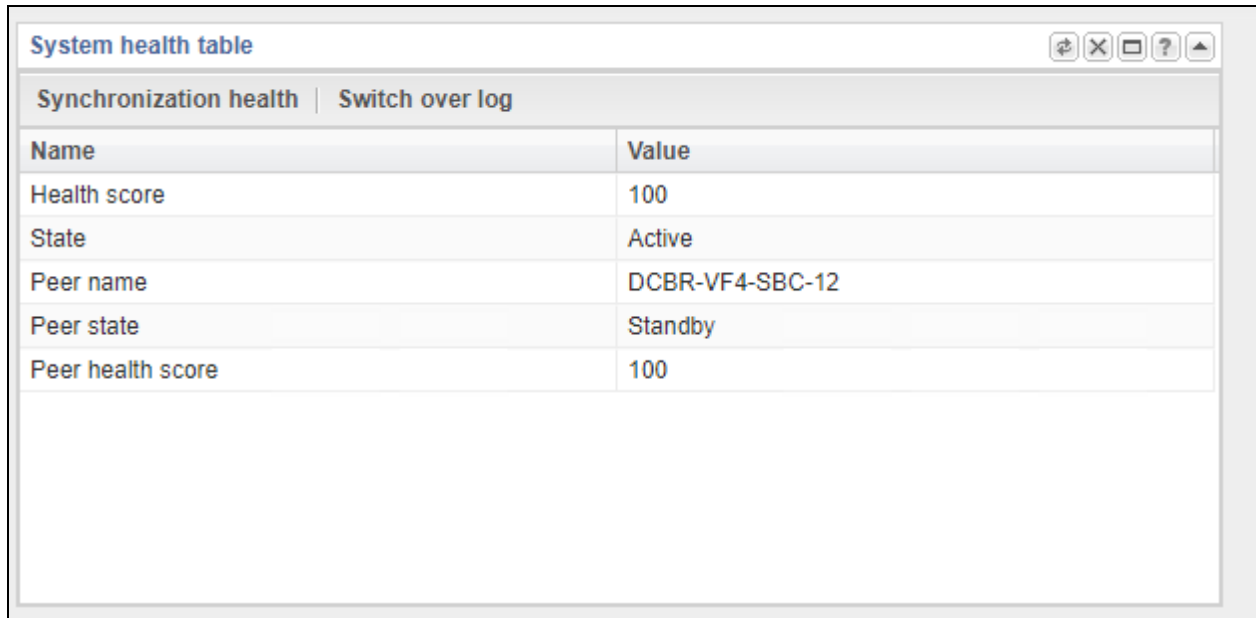
9.4.2. Frequentis Oracle SBC

From the Oracle SBC, on the **Home** tab, widgets can be added dedicated for monitoring.



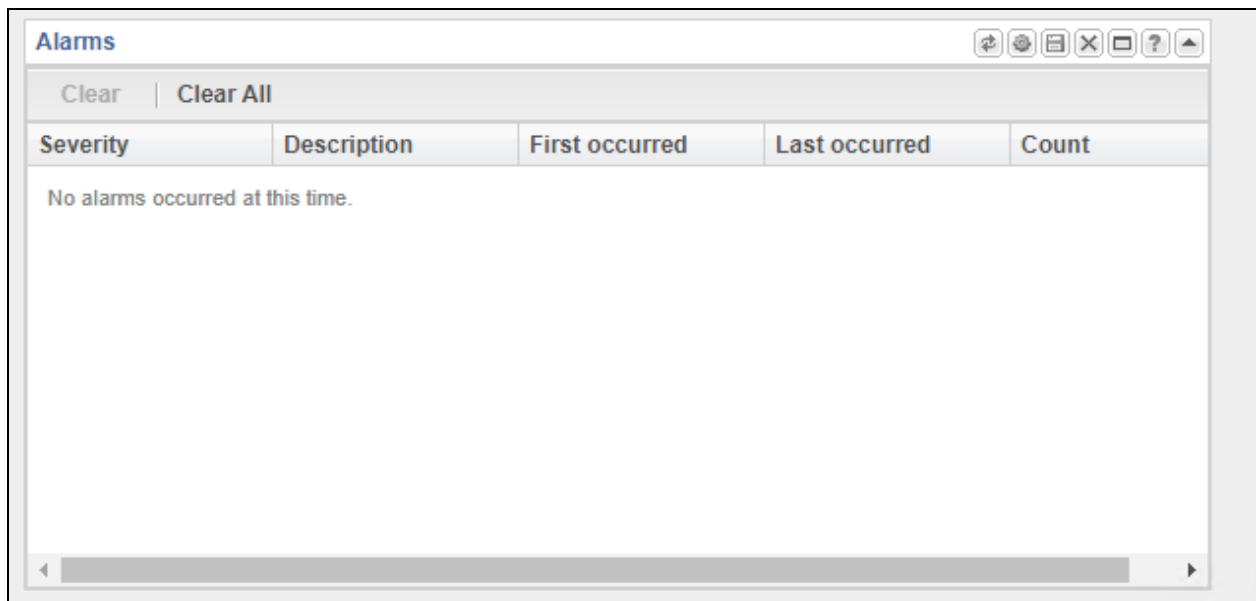
Some examples of these widgets include:

System health table – where the cluster health is observed.



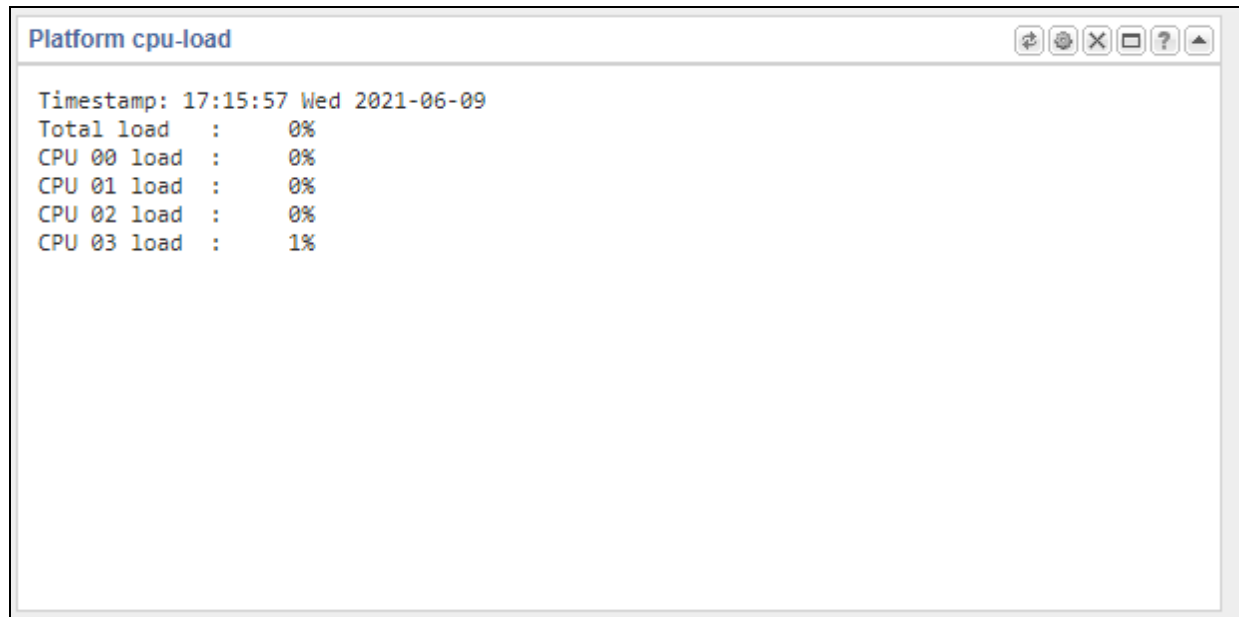
Name	Value
Health score	100
State	Active
Peer name	DCBR-VF4-SBC-12
Peer state	Standby
Peer health score	100

Alarms – describes any issue or problem.

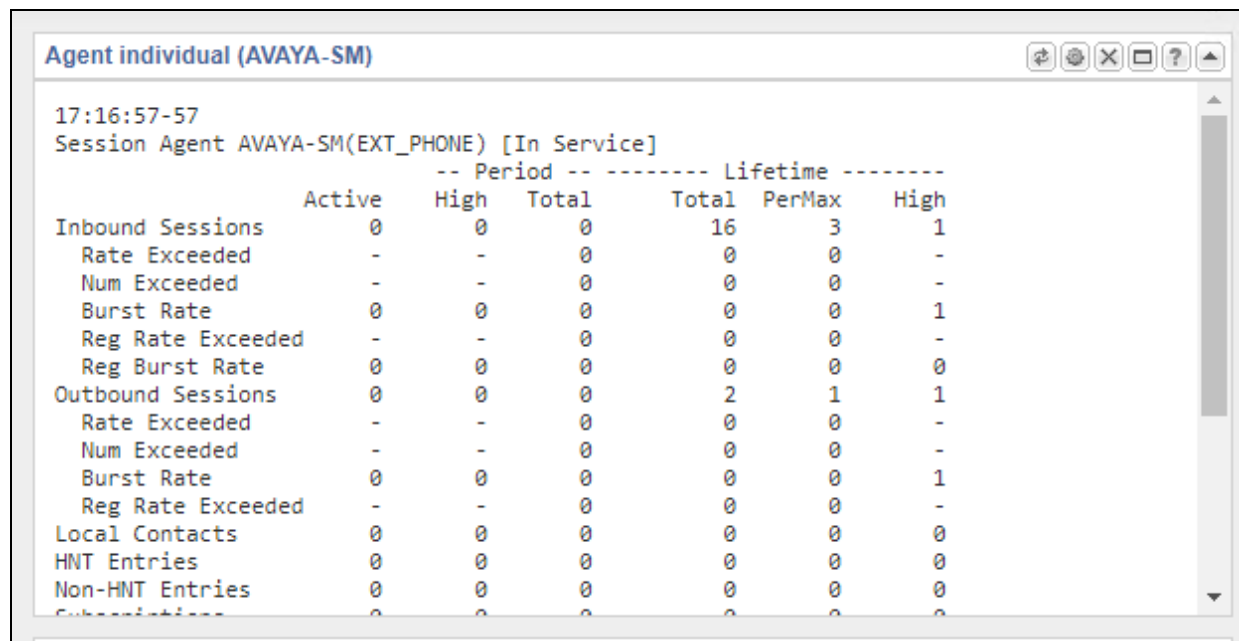


Severity	Description	First occurred	Last occurred	Count
No alarms occurred at this time.				

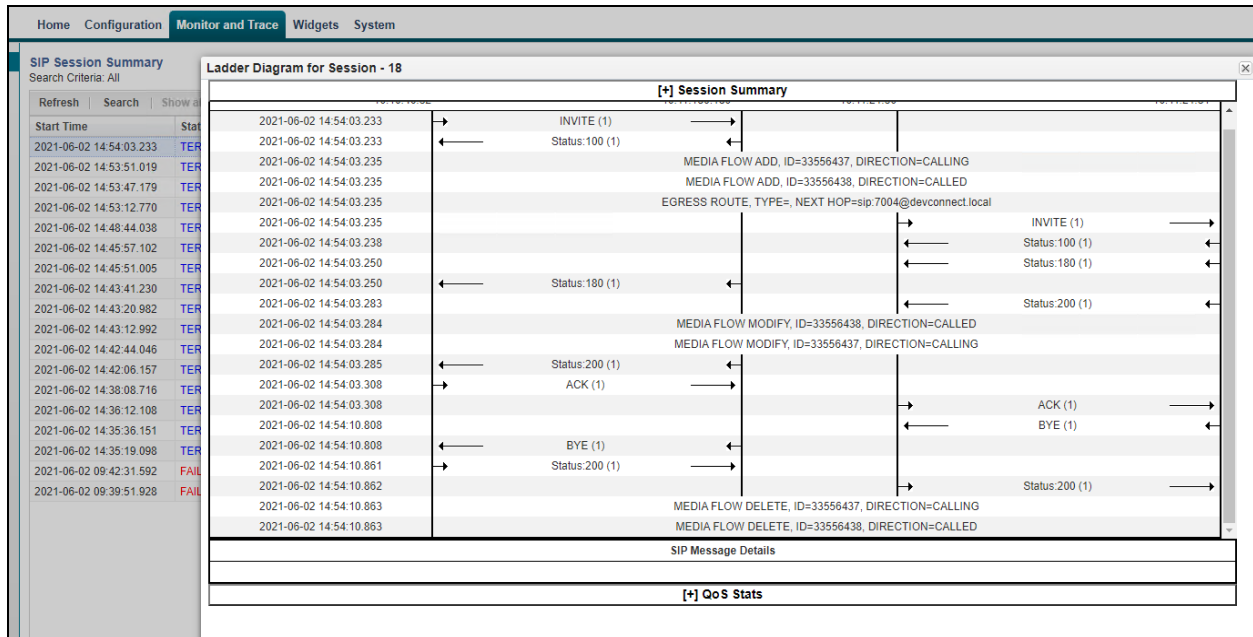
Platform cpu-load – shows the utilization of the CPU.



Agent individual – monitors the SIP connection.



For troubleshooting of a potential failed SIP session, use **SIP Session Summary** from **Monitor and Trace**. Double-click on a session to open a diagram with useful information of the SIP flow.



10. Conclusion

These Application Notes describe the configuration steps required for Frequentis AG 3020 LifeX to successfully interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 utilizing the Avaya Session Border Controller for Enterprise R8.1.2. Please refer to **Section 2.2** for test results and observations.

11. Additional References

This section references the product documentation relevant to these Application Notes. Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Deploying Avaya Aura® Communication Manager in a Virtualized Environment*, Release 8.1.x, Issue 6, October 2020.
- [2] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 7, October 2020.
- [3] *Administering Avaya Aura® System Manager* for Release 8.1.x, Issue 8, November 2020.
- [4] *Deploying Avaya Aura® System Manager in a Virtualized Environment*, Release 8.1.x, Issue 7, November 2020.
- [5] *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in a Virtualized Environment*, Release 8.1., Issue 4, October 2020.
- [6] *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 7, October 2020.
- [7] *Deploying Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 3, August 2020.
- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 3, August 2020.
- [9] *Deploying and Updating Avaya Aura® Media Server Appliance*, Release 8.0.x, Issue 11, October 2020.
- [10] *Implementing and Administering Avaya Aura® Media Server*. Release 8.0.x, Issue 11, October 2020.
- [11] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [12] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Documentation for Frequentis products can be obtained from Frequentis as follows.

- Web: <https://www.frequentis.com/en/contact-us>

©2021 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.