

Oracle SBC integration with Avaya Aura Session Manager for Avaya Workplace soft client in TLS/SRTP mode

**Technical Application Note** 



# Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

11/18

# **Revision History**

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with Avaya Aura Session Manager for Avaya Workplace client in TLS/SRTP mode	20 <sup>th</sup> December 2020
1.1	App Note updated with Minor changes (Caveat added)	30 <sup>th</sup> March 2021
1.1	App Note updated with Minor formatting changes	12 <sup>th</sup> November 2021



## **Table of Contents**

1. INTENDED AUDIENCE	5
2. DOCUMENT OVERVIEW	5
3. INTRODUCTION	6
3.1. AUDIENCE	6
3.2. REQUIREMENTS	6
3.3. ARCHITECTURE	7
4. CONFIGURING THE AVAYA AURA SESSION MANAGER 8.1	8
4.1. Adding SIP Domain	8
4.2. Adding Location	9
4.3. ADDING THE SBC AS A SIP ENTITY AND CONFIGURING AN ENTITY LINK	9
4.4. ALLOWING UNSECURED PPM TRAFFIC (ONLY IF TLS IS NOT USED) AND PPM RATE LIMITING	
4.5. ENABLING REMOTE UFFICE	
4.6. ADDING ROUTING POLICIES	15 15
4.7. ADDING DIAL FAI TERNS	13
5. CONFIGURING THE AVAYA WORKPLACE SOFT CLIENT FOR WINDOWS	
5.1. TURN ON THE MANUAL MODE FOR THE GUENT	20
5.2. CONFIGURE MANUAL MODE FOR THE CLIENT	
3.3. CONFIGURE THE DIRECTORT NOMBER FOR THE WORKSFACE CLIENT	
6. CONFIGURING THE SBC	
6.1. VALIDATED ORACLE SBC VERSION	24
7. NEW SBC CONFIGURATION	24
7.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC	24
7.2. CONFIGURE SBC USING WEB GUI	
7.3. CONFIGURE SYSTEM-CONFIG	
7.4. CONFIGURE PHYSICAL INTERFACE VALUES	
7.5. CUNFIGURE NET WURK INTERFACE VALUES	
7.0. ENABLE MEDIA MANAGER	
7.8. ENABLE SIP-CONFIG	
7.9. CONFIGURING A CERTIFICATE FOR SBC	
7.10. TLS-PROFILE	
7.11. CONFIGURE SIP INTERFACES.	
7.12. CONFIGURE SESSION-AGENT	45
7.13. CONFIGURE LOCAL-POLICY	46
7.14. CONFIGURE HTTP-ALG	
7.15. CONFIGURE STEERING-POOL	
7.16. CONFIGURE SDES PROFILE	
7.17. CONFIGURE MEDIA SECURITY PROFILE	
7.10. CONFIGURE DEADER MANIPULATION RULES (DMR)	
8. EXISTING SBC CONFIGURATION	61
9. REGISTRATION AND VERIFICATION OF AVAYA WORKSPACE CLIENT FOR WINDOWS	67

## 



#### 1. Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of the Oracle Enterprise Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform along with Avaya Aura System Manager GUI and Avaya Aura Session Manager.

#### 2. Document Overview

This Oracle technical application note outlines the configuration needed to set up the interworking between on premises Avaya Aura Session Manager using Oracle SBC. The solution contained within this document has been tested using Oracle Communication OS 840p3 version.

Our scope of this document is only limited to registering Avaya Workplace soft client for windows as remote worker (In Manual mode alone) to Avaya Session Manager using Oracle SBC and testing call features which are available using TLS/SRTP protocol. Testing Avaya Workspace soft client in automatic mode is out of scope of this document. The pre-requisite is also that the user should have downloaded the Avaya workspace client for windows 3.13 version (or above) from Avaya website and have installed that in the windows machine.

In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the Avaya Server associated parameters. Many SBC applications may have additional configuration requirements that are specific to individual customer requirements. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

For more information about Avaya Workplace client configuration and other things, please refer to the below link:

https://downloads.avaya.com/css/P8/documents/101071816

Please note that the IP address, FQDN and config name and its details given in this document is used as reference purpose only. The same details cannot be used in customer config and the end users can use the configuration details according to their network requirements. There are some public facing IPs (externally routable IPs) that we use for our testing are masked in this document for security reasons. The customers can configure any publicly routable IPs for these sections as per their network architecture needs.



#### 3. Introduction

#### 3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Avaya Aura System Manager GUI and Avaya Aura Session manager server in 8.1 version using Oracle Enterprise SBC. There will be steps that require navigating to Oracle SBC GUI interface, understanding the basic concepts of TCP/UDP, IP/Routing, SIP/TLS/SRTP and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary. It is also understood that the end user has already configured Avaya Aura Session Manager Configuration before referring this document.

#### 3.2. Requirements

- Avaya Workplace soft client for windows 3.13 version and above.
- Fully functioning Avaya Aura Session Manager 8.1 version.
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version

The below revision table explains the versions of the software used for each component: This table is Revision 1 as of now:

Software Used	Avaya Aura Session Manager using Avaya Aura System Manager GUI	SBC Version	Avaya Workplace soft client
Revision 1	8.1	8.4.0	3.13



#### 3.3. Architecture



The configuration, validation and troubleshooting is the focus of this document and will be described in two phases:

- Phase 1 Configuring the Avaya Aura Session Manager for Oracle SBC
- Phase 2 Configuring the Avaya Workplace soft client for windows 3.13 version
- Phase 3 Configuring the Oracle SBC.



# 4. Configuring the Avaya Aura Session Manager 8.1

Please login to Avaya Aura System Manager Web GUI with proper login credentials (Username and password). After that, perform the steps below in the given order.

Recommended access to System Manager is via FQDN.	
Go to central login for Single Sign-On	User ID: admin
If IP address access is your only option, then note that authentication will fail in the following cases:	Password:
First time login with "admin" account     Expired/Reset passwords	Log On Cancel
Use the "Change Password" hyperlink on this page to change the password manually, and then login.	Change Password
Also note that single sign-on between servers in the same security domain is	
not supported when accessing via IP address.	<b>Osupported Browsers:</b> Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.	
Unauthorized users are subject to company disciplinary procedures and or	

#### 4.1. Adding SIP Domain

Click on Routing under the Elements section On the Routing tab, select Domains and Click New

- Set domain name as aura.com (Example in this config)
- Set Type as SIP
- click "Commit" to save the configuration

Aura® Syste	m Manager 8.1	Users 🗸 🍦	🗲 Elements 🗸	Services 🗸	Widgets ~	Shortci	uts ~		Search	] ♣ ≡	adm
Home	Session Manager	Routing									
Routing	^	Domai	n Manage	ment				Commit Cancel			Help
Dom	ains										
Locat	tions	1 Item   🗟	3							Filter	r: Enable
Conc	litions	Name					Туре	Notes			
Adap	otations Y	* aura.co	m				sip 🗠				
SIP E	ntities										
Entity	y Links							Commit Cancel			
Time	Ranges										
Routi	ing Policies										
Dial I	Patterns 🗸 🗸										
Regu	Ilar Expressions										



#### 4.2. Adding Location

Click on Routing under the Elements section On the Routing tab, select Locations and Click New

- Set Name as Phonerlite
- Leave all other fields as default values and click "Commit" to save the configuration.

Avra® System Manager 8.1	Users ∨ ✓ Flements ∨ 🏟 Services ∨ │ Widge	ts v Shortcuts v		Search	📕   admi
Home Session Manager	Routing				
Routing ^	Location Details		Commit Cancel		Help ?
Domains	General				
Locations	* Name:	Phonerlite			
Conditions	Notes:				
Adaptations 🗸 🗸	Dial Plan Transparency in Survivable Mode				
SIP Entities	Enabled:				
Entity Links	Listed Directory Number:				
Time Ranges	Associated CM SIP Entity:				
Routing Policies	Overall Managed Bandwidth				
Dial Patterns 🛛 🗸	Managed Bandwidth Units:	Kbit/sec 💟			
	Total Bandwidth:				
Regular Expressions	Multimedia Bandwidth:				
×	Audio Calls Can Take Multimedia Bandwidth:				

## 4.3. Adding the SBC as a SIP Entity and Configuring an Entity Link

Click on Routing under the Elements section

On the Routing tab, select SIP Entities from the menu on the left side of the screen. Click New to add the SBC as a SIP entity as shown below.

- Set Name: SBC3900 (example in this configuration)
- Set FQDN or IP Address: This is the "inside" IP address of Oracle E-SBC, 10.50.232.75 in this example.
- Set Type: Other
- Set Location: Select Phonerlite from drop down (example in this configuration)
- Set Time Zone: America/New\_York (example in this configuration)
- Under Entity Links, Click Add
- Set SIP Entity 1: Select acme-sm which was previously configured
- Set SIP Entity 2: leave the default value SBC3900
- Set Protocol: UDP/TCP/TLS based on our testing
- Set Ports: Set both Ports to 5060/5061 for testing
- Set Connection Policy: trusted

Leave all other fields as default values and click "Commit" to save the configuration.



Aura® System Manager 8.1	🛎 Users 🗸 🌶 Elements 🗸 🏚 Services 🗸   Widgets 🗸 Shortcuts 🗸	Search 🔶 🚍 🛛 admin
Home Routing S	ession Manager	
Routing ^	SIP Entity Details	Help ?
Domains	General	
Locations	* Name: SBC3900	
	* FQDN or IP Address: 10.232.50.75	
Conditions	Type: Other	
Adaptations 🗸 🗸	Notes:	
SIP Entities	Adaptation:	
Entity Links	Location: Phonerlite 🗸	
,	Time Zone: America/New_York 🗸	
Time Ranges	* SIP Timer B/F (in seconds): 4	
Routing Policies	Minimum TLS Version: Use Global Setting 🗠	
Dial Pattorns V	Credential name:	
Regular Expressions		
<		
	and the second	

Domains									
	Entity Links								
Locations	Override Port &	Override Port & Transport with DNS SRV:							
Conditions	Add Remove								
	2 Items 🛛 👸							Filter: Enable	
Adaptations *	Name 🔺	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	
SIP Entities	acme-sm_SBC3900_	Racme-sm	UDP 🗵	* 5060	SBC3900	* 5060	trusted 🗸		
	* acme-sm_SBC3900_	Racme-sm	TLS 🗡	* 5061	SBC3900	* 5061	trusted 🗸		
Entity Links	Select : All, None								
Time Ranges	SIP Responses to an O	PTIONS Request							
Pouting Policies	Add Remove							_	
Routing Folicies	0 Items 🛛 🥲							Filter: Enable	
Dial Patterns v	Response Code & Reason Phrase					Mark Entity Notes Up/Down	5		
					Commit Cancel				



Please configure Avaya Session Manager as another SIP entity in the same way as we added SBC:

- Set Name: acme-sm (example in this configuration)
- Set FQDN or IP Address: This is the SIP IP address of Avaya SM, 10.50.232.127 in this example.
- Set Type: Session Manager
- Leave all other fields as default values and click "Commit" to save the configuration.

Aura® System Manager 8.1	Users 🗸 🌶 Elements 🗸 🏟 Services 🗸 ╞ Widg	ets × Shortcuts × Search 🔶 🚍   adm
Home User Management	t Routing	
Routing ^	SIP Entity Details	Commit Cancel
Domains	General	
	* Name:	acme-sm
Locations	* IP Address:	10.232.50.127
Conditions	SIP FQDN:	
	Туре:	Session Manager
Adaptations 🗸 🗸	Notes:	
SIP Entities	Location:	Phonerlite V
Entity Links	Outbound Proxy:	SBC3900 ×
	Time Zone:	America/New York
Time Ranges	Minimum TLS Version:	Use Global Setting V
Routing Policies	Credential name:	
Dial Patterns 🗸 🗸 🗸	Monitoring	
	SIP Link Monitoring:	Use Session Manager Configuration 👻
Regular Expressions	CRLF Keep Alive Monitoring:	Use Session Manager Configuration V
	Entity Links	

Please configure listen ports for the Avaya Session Manager as given below:

Routing					
	Failover Ports				
Domains	TCP Failover port:				
	TLS Failover port:				
Locations	Listen Ports				
Conditions	Add Remove				
Adaptations Y	2 Items 🛛 🥭				Filter: Enable
	Listen Ports	Protocol Default Domain	Endpoint	Notes	
SIP Entities	5060	UDP Y aura.com Y	$\checkmark$	1	
	5061	TLS 🗡 aura.com 🗡	$\checkmark$		
Entity Links	Select : All, None				
Time Ranges	SIP Responses to an	OPTIONS Request			
	Add Remove				
Routing Policies	0 Items 👌				Filter: Enable
Dial Patterns 🗸 🗸					Mark
	Response Code & Reas	on Phrase			Up/Down
Regular Expressions	·				
			C	Commit Cancel	
Routing Policies Dial Patterns × Regular Expressions ✓	Add Remove 0 Items 2 Response Code & Reas	ion Phrase	C	commit Cancel	Filter: Enable Entity Up/Down



#### 4.4. Allowing Unsecured PPM Traffic (only if TLS is not used) and PPM Rate Limiting

Navigate to: Elements->Session Manager->Global Settings

#### Set Allow Unsecured PPM Traffic: checked.

Note that this is only required if you're using HTTP for the PPM downloads. If you're using HTTPS as shown in the E-SBC configuration, leave this unchecked.

Aura® System Manager 8.1	Users 🗸 🎤 Elements 🗸 🏟 Services 🗸 📔 V	Vidgets v Shortcuts 🔻	Ś	Search	<b>) =</b>   a	ıdmi
Home Routing Ses	sion Manager					
Session Manager A	Global Settings		Commit Cancel View Defaults		Hel	p ?
Dashboard	Administer settings that apply to all Session Managers					
Session Manager Ad	Failback Policy	Auto ~	Enable IPv6			
	Allow Unauthenticated Emergency Calls		Allow Unsecured PPM Traffic	$\checkmark$		
Global Settings	ELIN SIP Entity	None 🗸	Minimum SIP Entity TLS Version	1.2 ~		
Communication Prof	Ignore SDP for Call Admission Control		Minimum Endpoint TLS Version	1.2 ~		
	Disable Call Admission Control Threshold Alarms		TLS Endpoint Certificate Validation	None	~	
Network Configur Y	Disable Loop Detection Alarms		Enable End to End Secure Call Indication			
Device and Locati 🗡	*Loop Detection Alarms Threshold (hours)	24	Enable Military Support			
	Enable Dial Plan Ranges		Enable Application Sequence for Emergency	Calls		
Application Confi *	Enable Regular Expression Adaptations		Emergency Call Resource-Priority Headers			
System Status 🛛 🗸	Enable Flexible Routing		Enable Implicit Users Applications for SIP us	sers		
System Tools 🛛 🗸	Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location	V	Enable SIP Resiliency			
Performance 🗡 🤟	Enable Load Balancer					
<						

Navigate to: Elements->Session Manager->Global Settings Session Manager Administration.

Select the proper Session Manager instance and click Edit

- Scroll down to PPM Connection Settings
- Set Limited PPM Client Connection: unchecked
- Set PPM Packet Rate Limiting: unchecked
- Leave all other fields as default and Click Commit to save Session Manager Administration page.



Aura® System Manager 8.1	∃Users ∨	🔑 Elen	nents 🗸 🔅 S	ervices ~   Widgets ~ Sh	ortcuts v	Search	📕   admii
Home Routing Ses	ssion Mana	iger					
Session Manager ^	Ses	sion M	anager Ad	dministration			Help
Dashboard	This pag global s	ge allows you ettings.	to administer Ses	sion Manager instances and configure the	ir		
Session Manager Ad	Sess	ion Mana	ger Instances	Branch Session Manager Insta	nces		
Global Settings	Sess	ion Man	ager Instan	ces			
Communication Prof	New	View	Edit Delete				
Network Configur Y	1 Iten	n   🥭	-				Filter: Enable
-		Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
Device and Locati Y	Select	: : None	Normai	4	0	4	
Application Confi 🗡							
Sustam Statur V							
System Status							
System Tools 🛛 🗸							
<							

Aura® System Manager 8.1	🛔 Users 🗸 🖌 🎤	Elements 🗸 🏟 Services 🗸   Widge	ts v Shortcuts v		Search 🔶 🗮 🛛 ad	mi
Home Routing	Session Manager					
Session Manager 🔷 🔨	Ê	Data File Format	Standard Flat File			
Dashboard		Include User to User Calls				
		Include Incomplete Calls				
Session Manager Ad	Person	al Profile Manager (PPM) - Connec	tion Settings 👻			
Global Settings		Limited PPM Client Connection				
Communication Prof		*Maximum Connection per PPM Client	0			
		PPM Packet Rate Limiting				
Network Configur *		*PPM Packet Rate Limiting Threshold	200			
Device and Locati $$	Event S	Server 👻				
Application Confi 🗡		Clear Subscription on Notification Failure	No 🕥			
System Status	Syslog	Servers -				
ojstem statas	-,	Enable Syslog Server 1				
System Tools Y		Enable Syslog Server 2				
Performance Y	~					
<	*Required	I		Commit	Cancel	



#### 4.5. Enabling Remote Office

Navigate to: Elements->Session Manager->Network Configuration->Remote Access, Click New

- Set Name: Remote\_worker for this setup.
- Click New under SIP Proxy Mapping Table. Add the Oracle SBC outside interface IP address for SIP Proxy Public Address.
- Click New under SIP Proxy Private IP Address. Add the Oracle SBC inside interface IP address for SIP Private Address, 10.232.50.75 is given in this example.
- Click Commit to save the configuration.

Aura® Syste	em Manager 8.1	Users 🗸 🥻 Elements	s ∨ 🔅 Services ∨	Widgets ~	Shortcuts v		Search		\Xi   admii
Home	Session Manager								
Session N	^ ∧	Remote Acce	ss Configuration	1		Commit	Cancel		Help ?
Dash	iboard								
Sessi	ion Manager Ad								
Glob	al Settings	*Name:	Remote_worker						
Com	munication Prof								
Netw	vork Configur 🔨	Click to open Remote	Access Reference Map 🕑						
I	Failover Groups	SIP Proxy Mapp	ing						
	 Local Host Nam	SIP Proxy Map	ping Table						
	Remote Access	O New O Delet	8						
	Remote Access	SIP Proxy Pu	blic Address (Reference A)	Sess	ion Manager (Reference	c)	IP Address Family (Refer	ence C)	
:	SIP Firewall			acr	ne-sm 🖂		IPv4 🖂		
	ce and Locati 👻 🖉	Select : All, None							
	<								





#### 4.6. Adding Routing Policies

Navigate to: Routing tab, select Routing Policies and Click New

- Set Name: 3900SBCroute (example in this configuration)
- Set Retries : Default value is 0, can be used as same value
- Select SIP Entity as Destination: Select SBC3900 which was previously configured.
- Click Commit to save the configuration

Avra® Syste	m Manager 8.1	Users 🗸 🌙	Element	ts 🗸 🏟 Se	ervices	~   w	idgets ~	Short	cuts v				Search		🔳   admi
Home	Session Manage	r Routing													
Locat	tions	Routin	g Polic	cy Detai	ls						Com	nmit Cancel			Help ?
Cond	litions 	Conoral													
Adap	otations Y	General				* Nar	ne: 390	0SBCrout	te						
SIP E	ntities					Disabl	ed: 🗌								
Entity	y Links					* Retri Not	es: 0								
Time	Ranges	SIP Entit	v as De	stination											
Routi	ing Policies	Select	·												
Dial I	Patterns ^	Name			1	QDN or IP	Address						Туре	Notes	
		SBC3900				10.232.50.7	5						Other		
l l	Dial Patterns	Time of	Day												
	Origination Dial	Add Re	move V	iew Gaps/Ove	erlaps										
		1 Item   🗟	2											Fi	lter: Enable
Regu	lar Expressions	Rank	ing	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes	
	<u> </u>	0		24/7								00:00	23:59	Time Range 24/	7
		Select : All	None												

#### 4.7. Adding Dial Patterns:

Navigate to: Routing tab, select Dial Patterns, again Dial Patterns and Click New

- Set Pattern: 1xxxxxxxx (example in this configuration)
- Set Min : 11 (example in this configuration)
- Set Max: 11 (example in this configuration)
- Select SIP Domain: aura.com which was previously configured.
- Click Commit to save the configuration.



AVAYA Aura® System Manager 8.1	🛔 Users 🗸 🌾 Elements 🗸 🌞 Services 🗸 📔 Widgets 🗸 Shortcuts 🗸		Search	🐥 🗮   adm
Home Session Manag	ger Routing			
Locations	Dial Pattern Details	mit Cancel		Help ?
Conditions	General			
Adaptations 🗸 🗸	* Pattern: 1xxxxxxxxx			
SIP Entities	* Min: 11			
Entity Links	* Max: 11 Emergency Call:			
Time Ranges	SIP Domain: aura.com V			
Routing Policies	Notes:			
Dial Patterns 🔷	Originating Locations and Routing Policies			
Dial Patterns	Add Remove			
Diarrateris	1 Item 🤯	Pouting Policy	Pouting Policy	Filter: Enable
Origination Dial	Originating Location Name Notes Name Rank	Disabled	Destination	Notes
Regular Expressions	Phonerlite 3900SBCroute 0		SBC3900	
<	Select : All, None			
	Denied Originating Locations			

After configuring the dial patterns, Please add the dial patterns to the routing policies created above.

Avra® Syste	em Manager 8.1	Jsers 🗸 🎤 Elements	; 🗸 🌣 Servio	ces ~   V	Vidgets v Shoi	tcuts ~			Searc	h 🐥	🔳   admi
Home	Session Manager	Routing									
Loca	ations	Add Remove Vie	w Gaps/Overlap	s							
6	-1747	1 Item 🍣									Filter: Enable
Conc	aitions	Ranking	Name Mo	on Tue	Wed Thu	Fri Sa	at Sun	Start Time	End Time	Notes	
Adap	ptations Y	0	24/7					00:00	23:59	Time Range 24	4/7
SIP E	Entities	Select : All, None Dial Patterns									
Entity	ty Links	Add Remove									
Time	Ranges	1 Item 🛛 🍣									Filter: Enable
	e Kanges	Pattern	🔺 Min	Max	Emergency Call		SIP Domain	Originat	ting Location		Notes
Rout	ting Policies		11	11			aura.com	Phonerli	te		
Dial	Patterns ^	Select : All, None									
		Regular Expressi	ons								
I	Dial Patterns	Add Remove									
	Origination Dial	0 Items 🛛 🍣									Filter: Enable
Regu	ular Expressions	Pattern		Rank C	Order			Deny	1	Notes	
	<						Com	nit Cancel			



#### 4.8. Adding Users to Avaya Session Manager.

Navigate to: Users tab, select User Management, select Manage Users and Click New

Under Identity Tab, please enter the following

- Set Last Name: User1(example in this configuration)
- Set First Name: Avaya (example in this configuration)
- Set Login Name: 17814437246@aura.com (example in this configuration)

Under Communication Profile tab, click Communication Profile Password

- Set Comm-Profile Password: any password (Numbers or alphabets or alphanumeric)
- Re-enter Comm-Profile Password: Type the password again for confirmation.

#### Navigate to Communication address tab, click New

- Set Type: Avaya SIP
- Set Fully Qualified Address: Type the Directory number @domain.com

17814437246@aura.com

Under Profile tab, enable Session Manager Profile and click it to open it.

- Set Primary Session Manager under SIP Registration: acme-sm (example in this configuration)
- Set Home Location Manager under Call Routing: Phonerlite (example in this configuration)
- Click Commit to save the configuration.

Aura® System Manager 8.1	xyxxx ▲ Users ∨ ⊁ Elements ∨ ☆ Services ∨   Widgets ∨ Shortcuts ∨ Search ▲ ☰   adr ystem Manager 8.1					
Home Session Manager	Routing User Management	User Management				
User Management ^	Identity Communication Prot	file Membership Contac	cts			
Manage Users	Basic Info					
Public Contacts	Address	User Provisioning Rule:	×			
Shared Addresses						
System Presence ACLs	Localizediname	* Last Name :	User1	Last Name (Latin Translation) :	User1	
Communication Profile		* First Name :	Avava	First Name (Latin	Avava	
				Translation) :		
		* Login Name :	17814437246@aura.com	Middle Name :	Middle Name Of User	
		Description :	Description Of User	Email Address :	Email Address Of User	
		Password :		User Type:	Basic v	
<		Confirm Password :		Localized Display Name :	User, Avaya	



Aura® System Manager 8.1				
Home User Managemen	t			
User Management ^	Home☆ / Users ႙ / Manage Users			Help ?
Manage Users	User Profile   Edit   17814437	246@aura.com	🖻 Commit & Continue	E Commit 🛞 Cancel
Public Contacts	Identity Communication Profile	Comm-Profile Password	×	
Shared Addresses	Communication Profile Password			Options ∽
System Presence ACLs	PROFILE SET : Primary V	Comm-Profile Password :	•••••	Domain 🔶 🛛
Communication Profile	Communication Address			aura.com
	PROFILES	Re-enter Comm-Profile Password :	Re-enter Comm-Profile Password	
	Session Manager Profile		Generate Comm-Profile Password	1 10 / page v Goto
	CM Endpoint Profile		Cancel	
<				

Aura® System Manager 8.1			
Home User Managemen	t		
User Management ^	Home☆ / Users		Hel;
Manage Users	User Profile   Edit   17814437	246@aura.com	Commit & Continue Commit Commit Commit
Public Contacts	Identity Communication Profile	Membership Contacts	
Charad Addrassas	Communication Profile Password	Communication Address Add/Edit	×
Silaled Addlesses			Options ~
System Presence ACLs	PROFILE SET : Primary 🗸	* Type: Avaya SIP	✓ Domain ♦ ∀
Communication Profile	Communication Address	Eully Qualified Address (	aura.com
	PROFILES	17814437246	@ aura.com v
	Session Manager Profile		1 10 / page v Goto
	CM Endpoint Drofile		
			Cancel OK
<			

	Routing User Managemen	t User Management					
User Management 🔷	User Profile   Edit   17	814437246@aura.com			D Commit & Continue	Commit	: بان : (8) Cancel
Manage Users Public Contacts	Identity Communication	Profile Membership Cor	tacts				
Shared Addresses	Communication Profile Password PROFILE SET : Primary	SIP Registration					
System Presence ACLs Communication Profile	Communication Address	Primary Session Manager	acme-sm	Q 🚺			
	PROFILES Session Manager Profile	Secondary Sessio Manager	Start typing	Q 🚺			
	CM Endpoint Profile	Survivability Server	Start typing	Q 🟮			
		Max. Simultaneous Devices	: 4	~			
<		Block New Registration Wh	en 🗌				

Aura ® System Manager 8.1	Users 🗸 🎤 Elements 🗸 🤤	Services ~   Widgets ~ Shortcuts ~		Search 💄 🗮 🛛 admi
Home Session Manage	r Routing User Managen	nent User Management		
User Management 🔹 🔨		Emergency Calling Select Origination Sequence:	v	
Manage Users Public Contacts		Emergency Calling Select Termination Sequence:	v	
Shared Addresses System Presence ACLs		Call Routing Settings  * Home Location: Phonerlite	v	
Communication Profile		Conference Factory Set: Select	v	
		Call History Settings Enable Centralized Call History?:		
<				

You can repeat the above steps to add more users to the Session Manager. With this, Avaya Session Manager Configuration is complete.



# 5. Configuring the Avaya Workplace soft client for Windows

This section provides step-by-step guidance on how to configure Avaya Workplace soft client to work with Oracle SBC. As we are configuring the client to work in Manual mode, we have to perform the following steps.

#### 5.1. Turn ON the Manual mode

As a first step, please turn on the manual mode of the client by doing following steps.

- 1) Please select the Sign in option when the client opens for the first time.
- 2) The client then gives the screen for automatic login and please select settings icon on top of the screen.
- 3) Select manually configure (Expert Mode) to enter the Manual mode option.

Avaya Workplace Sign In 🔅 — 🗙
Join Workplace Meeting
<b>8</b> O
Let's get into the meeting!
Your name
Meeting Address
Meeting ID
Use Workplace for Audio + Video
Join

AVAYA WORKPlace Enter your email address (1)
Email
NEXT

	袋 ×
Using email address is the easiest way to setup Workplace. Choose another configuration method only if instructed by support team.	
Use web address	
Manually configure (Expert mode)	
Email	
NEXT	
Can	cel



### 5.2. Configure Manual mode for the client

Once we select Manual Mode, the client opens the screen to enter the configuration.

- 1) Please select Services ---- Phone services --- ON.
- 2) Please enter SBC public interface IP, Domain given in Avaya SM and the Server port and then enable TLS as transport protocol. Click Done to save the changes made.

	Settings		$\times$
User Preferences	Services		
Accounts			
Services			>
Desktop Integration	Hide Details		
Advanced	Phone Service	OFF	>
Support	·		
Check for Services	My Meeting Room	OFF	>
	Enterprise Directory	OFF	>
	Multimedia Messaging	OFF	>
	Avaya Cloud Services	OFF	>
			-

Settings				
User Preferences	Back	Phone Service		
Accounts				
Services				
Desktop Integration	Server Address			
Advanced Support Check for Services	Server Port	5061		
	Domain	aura com		
		aura.com		
	Use TLS			
	Adhoc Conference Address			
			DONE	



#### 5.3. Configure the Directory Number for the Workspace client

Once we enable the phone services, please assign the directory number to the client (we can use one of the directory numbers that we created under users in Avaya Session Manager)

- 1) Please select Accounts ----- Extension --- Give the directory number created
- 2) Under Password ---- Enter the password for the directory number.
- 3) Enable Remember password if you want client to save the password
- 4) Click Done to save the changes.

	Settings	×
User Preferences	Accounts	
Accounts		
Services	Phone Service	
Desktop Integration	Extension	17814437248
Advanced	Password	•••••
Support	Remember Password	
Check for Services		
		DONE

With this, Avaya workplace client configuration is complete for the Manual Mode.



# 6. Configuring the SBC

This section provides step-by-step guidance on how to configure Oracle SBC for interworking with Avaya Session Manager for registering Avaya Workspace client and for making calls from Avaya Workspace client soft phones to other phones registered to the Avaya Session Manager 8.1

#### 6.1. Validated Oracle SBC version

Oracle conducted tests with Oracle SBC 8.4 software – this software with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6350
- AP 6300
- VME

# 7. New SBC configuration

If the customer is looking to setup a new SBC from scratch, please follow the section below.

#### 7.1. Establishing a serial connection to the SBC

Connect one end of a straight-through Ethernet cable to the front console port (which is active by default) on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB-9 adapter) to the DB-9 port on a workstation, running a terminal emulator application such as Putty. Start the terminal emulation application using the following settings:

- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

starting	tLema
Starting	tServiceHealth
Starting	tCollect
Starting	tAtcpd
Starting	tAsctpd
Starting	tMbcd
Starting	tCommMonitord
Starting	tFped
Starting	tAlgd
Starting	tRadd
Starting	tEbmd
Starting	tSipd
Starting	tH323d
Starting	tIPTd
ltarting	tSecured
Starting	tAuthd
Starting	tCertd
Starting	tIked
Starting	tTscfd
Starting	tAppWeb
Starting	tauditd
Starting	tauditpusher
Starting	tSnmpd
Starting	tIFMIBd
Start pla	tform alarm
Starting	display manager
Initializ	ing /opt/ Cleaner
Starting	tLogCleaner task
Bringing	up shell
password	secure mode is enabled
Admin Sec	curity is disabled
Starting	SSH
SSH Cli i	nit: allocated memory for 5 connections

Power on the SBC and confirm that you see the following output from the boot-up sequence

Enter the default password to log in to the SBC. Note that the default SBC password is "acme" and the default super user password is "packet".

Both passwords have to be changed according to the rules shown below.

Password:
<pre>% Only alphabetic (upper or lower case), numeric and punctuation % characters are allowed in the password. % Password must be 8 - 64 characters, % and have 3 of the 4 following character classes : % - lower case alpha % - upper case alpha % - numerals % - punctuation</pre>
* Enter New Password: Confirm New Password: Password is acceptable.



Now set the management IP of the SBC by setting the IP address in bootparam to access bootparam. Go to Configure terminal->bootparam.

Note: There is no management IP configured by default.

N3900-101# N3900-101# N3900-101# conf t N3900-101(configure)# }	pootparam
'.' = clear field; '-'	= go to previous field; q = quit
Boot File IP Address JLAN Netmask Bateway IPV6 Address IPV6 Gateway Host IP TTP username TTP password Flags Target Name Console Device Console Baudrate Other	: /boot/nnSC2840p3.bz : 10.138.194.136 : 0 : 255.255.192 : 10.138.194.129 : : : : vxftp : vxftp : vxftp : 0x0000010 : NN3900-101 : COM1 : 115200 :
NOTE: These changed para Also, be aware that some PHY and Network Interface NN3900-101(configure)# NN3900-101(configure)# NN3900-101	ameters will not go into effect until reboot. e boot parameters may also be changed through se Configurations. exit

Setup product type to Enterprise Session Border Controller as shown below.

To configure product type, type in setup product in the terminal





Enable the features for the ESBC using the setup entitlements command as shown

Save the changes and reboot the SBC.

Entitlements for Enterprise Session Border Controller Last Modified: Never 1 : Session Capacity 3 : Admin Security
4 : Data Integrity (FIPS 140-2) Gata Integrity (THE THE 1)
Transcode Codec AMR Capacity
Transcode Codec AMRWB Capacity
Transcode Codec EVRC Capacity
Transcode Codec EVS Capacity
Transcode Codec EVS Capacity : 0 : 0 : 0 10: Transcode Codec OPUS Capacity 11: Transcode Codec SILK Capacity : 0 Session Capacity (0-128000) : 500 CAUTION: Enabling this feature activates enhanced security functions. Once saved, security cannot be reverted without resetting the system back to factory default state. Admin Security (enabled/disabled) : 50 Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2 Advanced (enabled/disabled) : enabled Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10 Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 11 Transcode Codec SILK Capacity (0-102375)

The SBC comes up after reboot and is now ready for configuration.



Go to configure terminal->system->http-server-config.

Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

NN3900-101(Nttp-server)# NN3900-101(http-server)#	
NN3900-101(http-server)# show	
nttp-server	
name	webServerInstance
state	enabled
realm	
ip-address	
http-state	enabled
http-port	80
https-state	disabled
https-port	443
http-interface-list	REST,GUI
http-file-upload-size	0
tls-profile	
auth-profile	
last-modified-by	9
last-modified-date	2020-10-06 00:28:26
NN3900-101(http-server)#	

#### 7.2. Configure SBC using Web GUI

In this app note, we configure SBC using the WebGUI.

The Web GUI can be accessed through the url <u>http://<SBC\_MGMT\_IP</u>>.

	0		
		Sign in to E-SBC	
		Enter your details below	
ORACLE		Username	
Enterprise Session Border Controller		I	
		Password	Required
			Required
		SIGN IN	

The username and password is the same as that of CLI.



Go to Configuration as shown below, to configure the SBC

			Dashboard	Configuration	Monitor and Trace	Widgets	System
🔯 Wizards 🔻	Commands 👻				Save Verify	Discard	Search
media-manager	•	Configuration Objects					
security	•						
session-router		Name	Description				
		access-control	Configure a static or dynamic access control list				
system	•	account-config	Configure Quality of Service accounting				
		authentication-profile	Configure authentication profile				
		certificate-record	Create, generate, and import a certificate				
		class-policy	Configure classification profile policies				
		codec-policy	Create and apply a codec policy to a realm and an agent				
		filter-config	Create a custom filter for SIP monitor and trace				
		fraud-protection	Configure fraud protection				
		host-route	Insert entries into the routing table				
		http-client	Configure an HTTP client				
		http-server	Configure an HTTP server				*
		Displaying 1 - 11 of 42					
Show All							

Kindly refer to the GUI User Guide given below for more information.

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/8.4.0/webgui/esbc\_scz840\_webgui.pdf

The expert mode is used for configuration.

**Tip:** To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.



#### 7.3. Configure system-config

Go to system->system-config

	Session Border Controller					admi
			Dashboard	Configuration	Monitor and Trace	Widgets Sy
🔅 Wizards 💌					Save Verify	Discard
http-client	Modify System Config					Show Coungura
http-server network-interface	Hostname	OracleSBC				
ntp-config	Description					
redundancy-config	Lagation					
snmp-community	Location					
spl-config	Mib System Contact					
system-config						
tdm-config	Mib System Location					
trap-receiver	ОК	Delete				

Please enter the default gateway value in the system config page.

	e Session Border Controller						adn
				Dashboard	Configuration	Monitor and Trace	Widgets S
🔅 Wizards 💌	•					Save Verify	Discard
http-client	Modify System Config						Show Configu
http-server	Displaying U - U of U Options						
network-interface							
ntp-config	Call Trace	enable					
phy-interface	Default Gateway	10.138.194.129					
redundancy-config	Restart	🗹 enable					
snmp-community	Telnet Timeout	0	(Range: 065535)				
spl-config	Console Timeout	0	( Range: 065535 )				
system-config	Alarm Threshold	5	( Range: 020 )				
tdm-config							
trap-receiver	Add						
Show All	ОК	Delete					

For VME, transcoding cores are required. Please refer the documentation here for more information

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/8.4.0/releasenotes/esbc\_scz840\_releasenotes.pdf

The above step is needed only if any transcoding is used in the configuration. If there is no transcoding involved, then the above step is not needed.



#### 7.4. Configure Physical Interface values

To configure physical Interface values, go to System->phy-interface.

You will first configure the slot 0, port 1 interface designated with the name M10. This will be the port plugged into your (connection to the Avaya Workspace client) public interface. Avaya Core side side is configured on the slot 1 port 1.

Parameter Name	Avaya Workspace client side (M10)	Avaya Core Side (M11)
Slot	0	1
Port	1	1
Operation Mode	Media	Media

Please configure M10 interface as below.

	Session Border Controller						a
				Dashboard	Configuration	Monitor and Trace	Widgets
Wizards v nost-route http-client	Add Phy Interface					Save Verify	Discard
http-server	Name	M10					
network-interface	Operation Type	Media	v				
ntp-config	Port	0	(Range: 05)				
phy-interface	Slot	1	(Range: 02)				
redundancy-config	Virtual Mac						
snmp-community	Admin State	✓ enable					
spl-config	Auto Negotiation	✓ enable					
system-config	Duplex Mode	FULL	V				
tdm-config	Speed	100	v				
trap-receiver v Show All	ОК	Back					



Similarly, configure M11 interface as below.

	Session Border Controller					
			Dashl	board Configuration	Monitor and Trace	Widgets
🔅 Wizards 👻					Save Verify	Discard
nost-route	Add Dhy Interface					
http-client	Add Phy Interface					
http-server	Name	M11				
network-interface	Operation Type	Media 🔹				
ntp-config	Port	1	(Range: 05)			
phy-interface	Slot	1	( Range: 02 )			
redundancy-config	Virtual Mac					
snmp-community	Admin State	🖌 enable				
spl-config	Auto Negotiation	✓ enable				
system-config	Duplex Mode	FULL 🔻				
tdm-config	Speed	100 💌				
trap-receiver 🗸	ОК Е	Back				
Show All						

#### 7.5. Configure Network Interface values

To configure network-interface, go to system->Network-Interface. Configure two interfaces, one for Avaya Workspace client side and one for Avaya Core side.

The table below lists the parameters, to be configured for both the interfaces.

Parameter Name	Avaya Workspace client side Network Interface (Avaya Public Interface)	Avaya Core side Network interface (Avaya Core Interface)
Name	M10	M11
Host Name		
IP address		10.232.50.75
Netmask	255.255.255.192	255.255.255.0
Gateway		10.232.50.1



Please configure network interface M10 as below

	ise Session Border Controller					
				Dashboard Configuration	Monitor and Trace	Widgets
🔅 Wizards 🔻	v				Save Verify	Discard
fraud-protection	Add Network Interface					
http-client	Name	M10	v			
http-server	Sub Port Id	0	(Range: 04095)			
network-interface	Description					
ntp-config						
phy-interface						
redundancy-config	Hostname					
snmp-community	IP Address					
spl-config	Pri Utility Addr					
system-config	Sec Utility Addr					
tdm-config Show All	ОК	Back				

Please configure network interface M11as below

	Session Border Controller							a
					Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 🔻							Save Verify	Discard
fraud-protection	Add Network Interface							
http-client	Name	M11	•					
http-server	Sub Port Id	0	(	[Range: 04095 )				
network-interface	Description	I						
ntp-config								
phy-interface								
redundancy-config	Hostname	10.232.50.75						
snmp-community	IP Address	10.232.50.75						
spl-config	Pri Utility Addr							
system-config	Sec Utility Addr							
trlm-config ¥ Show All	ОК Е	łack						



#### 7.6. Enable media manager

Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

In addition to the above config, please set the max and min untrusted signaling values to 1. Go to Media-Manager->Media-Manager

ORACI	_E Enterprise	Session Border Controller					ā
				Dashboard	Configuration	Monitor and Trace	Widgets
🚯 Wizards 🔻	🔅 Commands 👻					Save Verify	Discard
media-manager codec-policy	•	Modify Media Manager					
media-manage	r-	State	✓ enable				
media-policy		Flow Time Limit	86400	(Range: 04294967295)			
realm.config		Initial Guard Timer	300	(Range: 04294967295)			
realiti-coning		Subsq Guard Timer	300	(Range: 04294967295)			
steering-pool		TCP Flow Time Limit	86400	(Range: 04294967295)			
security	•	TCP Initial Guard Timer	300	(Range: 04294967295)			
session-router	•	TCP Subsq Guard Timer	300	(Range: 04294967295)			
system	•	Hnt Rtcp	enable				
		Algd Log Level	NOTICE				
		Mbcd Log Level	NOTICE				
		ОК	Delete				
Show All							

ORACI	_E Enterprise	Session Border Controller				ac
				Dashboard Configuration	Monitor and Trace	Widgets
-	_					
🔅 Wizards 🔻	🔅 Commands 🔻				Save Verify	Discard
media-manager	* ^	Modify Media Manager				
codec-policy			1000	[mmberos icritorcis]		
media-manage	r	Media Policing	🖌 enable			
media-policy		Max Arp Rate	10	(Range: 0.100)		
media-policy		Max Signaling Packets	0	(Range: 04294967295)		
realm-config		Max Untrusted Signaling	1	(Range: 0100)		
steering-pool		Min Untrusted Signaling	1	(Range: 0100)		
security	•	Tolerance Window	30	(Range: 04294967295)		
session-router	•	Untrusted Drop Threshold	0	(Range: 0100)		
sustem		Trusted Drop Threshold	0	(Range: 0.100)		
system	•	Acl Monitor Window	30	(Range: 53600)		
fraud-protectio	n	Trap On Demote To Deny	enable			
host-route						
Show All	~	ОК	Delete			



### 7.7. Configure Realms

Navigate to realm-config under media-manager and configure a realm as shown below The name of the Realm can be any relevant name according to the user convenience.

In the below case, Realm name is given as AvayapublicRealm (Avaya Workplace client to SBC side). Please set the Access Control Trust Level to medium for this realm

		Session Border Controller		Dashboard	Configuration	Monitor and Trace	Widgets
🔯 Wizards 🔻	Commands 🔻					Save Verify	Discard
codec-policy	^	Add Realm Config					
media-manage media-policy	r	Identifier Description	AvayapublicRealm				
steering-pool	,						
session-router	•	Addr Prefix Network Interfaces	0.0.0.0 M10:0.4 X				
fraud-protectio	▼ n	Media Realm List					
host-route		Mm In Realm	enable				
http-client Show All	<b>`</b>	ОК	Back				

					Dashboard Configuration	Monitor and Trace	Widgets
Wizards 🔻	Commands 🔻					Save Verify	Discard
media-manager	•	Modify Realm Config					
codec-policy		In Manipulationid		w			
media-manage	r	Out Manipulationid		v			
media-policy		Average Rate Limit	0		(Range: 04294967295)		
realm-config		Access Control Trust Level	medium	Ŧ			
steering-pool		Invalid Signal Threshold	0		(Range: 04294967295)		
security	+	Maximum Signal Threshold	0		(Range: 04294967295)		
session-router	•	Untrusted Signal Threshold	0		(Range: 04294967295)		
system		Nat Trust Threshold	0		(Range: 065535)		
ojstan	,	Max Endpoints Per Nat	0		(Range: 065535)		
		Nat Invalid Message Threshold	0		(Range: 065535)		
Show All		OK	Back				



Similarly, Realm name is given as AvayaCoreRealm (SBC to Avaya Session Manager) Please set the Access Control Trust Level to high for this realm

	Session Border Controller			Ē
			Dashboard Configuration	Monitor and Trace Widgets
🔅 Wizards 🔻				Save Verify Discard
codec-policy	Add Realm Config			
media-manager	Identifier	AvayaCoreRealm		
realm-config	Description			
steering-pool				
security	Addr Prefix	0000		
session-router	Network Interfaces	M11:0.4 ×		
fraud-protection	Media Realm List			
host-route	Mm In Realm	v enable		
http-client v	ОК	Back		
Show All				
ORACLE Enterprise S	ession Border Controller			ā
			Dashboard Configuration	Monitor and Trace Widgets

				Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 🔻	🔅 Commands 🔻					Save Verify	Discard
media-manager	•	Modify Realm Config					
codec-policy		ouctransactoria		V			
media-manage	r	In Manipulationid		v			
media-policy		Out Manipulationid		v			
realm-config		Average Rate Limit	0	(Range: 04294967295)			
steering-pool		Access Control Trust Level	high	•			
security	►	Invalid Signal Threshold	0	(Range: 04294967295)			
session-router	•	Maximum Signal Threshold	0	(Range: 04294967295)			
		Untrusted Signal Threshold	0	(Range: 04294967295)			
system	•	Nat Trust Threshold	0	(Range: 065535)			
		Max Endpoints Per Nat	0	(Range: 065535)			
		Nat Invalid Message Threshold	0	(Danger 0, AEEZE )			
		ОК	Back				
Show All							No ne

For more information on Access Control Trust Level, please refer to SBC Security guide link given below:

https://docs.oracle.com/en/industries/communications/session-bordercontroller/8.4.0/security/sbc\_scz840\_security.pdf



#### 7.8. Enable sip-config

SIP config enables SIP handling in the SBC. Make sure the home realm-id, registrar-domain and registrar-host are configured.

Also add the options to the sip-config as shown below. To configure sip-config, Go to Session-Router->sip-config and in options, add the below

- add max-udp-length =0 & global-contact
- inmanip-before-validate & reg-cache-mode=from

For more info, please refer to SBC security guide given in the above section.

	rise Session Border Controller						3
				Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 🔻 🔅 Command	S 🔻					Save Verify	Discard
local-policy	Modify SIP Config						
local-routing-config media-profile session-agent	State Dialog Transparency	<ul><li>✓ enable</li><li>✓ enable</li></ul>					
session-group	Home Realm ID	AvayaCoreRealm	v				
session-recording-group	Egress Realm ID		٣				
session-recording-server	Registrar Domain	None	*				
session-translation	Registrar Host	*					
sip-config	Registrar Port	5060		(Range: 0.102565535)			
sip-feature	Init Timer	500		(Range: 04294967295)			
sip-interface	OK	Delete					

	Session Border Controller						a
				Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 💌						Save Verify	Discard
local-policy	Modify SIP Config						
local-routing-config	Enforcement Profile	•					
media-profile	Red Max Trans	10000	(Range: 050000)				
session-agent	Options	global-contact 🗙					
session-group		inmanip-before-validate 🗙					
session-recording-group		max-udp-length=0 ×					
session-recording-server		reg-cache-mode-mont X					
session-translation	SPL Options						
sip-config	SIP Message Len	4096	(Range: 065535)				
cin feature	Enum Sag Match	enable					
sip-leature	Extra Method Stats	🗸 enable					
sip-interface	ОК	Delete					
Show All							



#### 7.9. Configuring a certificate for SBC

As we need to test Avaya Workspace client configuration with TLS connections (Avaya Workspace client to SBC side which is access side), we need to have certificates for the same.

The step below describes how to request a certificate for SBC External interface and configure it based on the example of DigiCert. The process includes the following steps:

- 1) Create a certificate-record "Certificate-record" are configuration elements on Oracle SBC which captures information for a TLS certificate such as common-name, key-size, key-usage etc.
- SBC 1 certificate-record assigned to SBC
- Root 1 certificate-record for root cert
- 2) Deploy the SBC and Root certificates on the SBC

#### Step 1 – Creating the certificate record

Go to security->Certificate Record and configure the SBC entity certificate for SBC as shown below.

ORACI	LE Enter	prise S	ession Border Controller						Û 🔺
					1	Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 🔻	Comman 🏟	ids 🔻						Save Verify	Discard
media-manager	•		Add Certificate Record						
security	•								
authentication-	profile		Name	AvayaCert					
certificate-reco	rd		Country	US					
tls-global			State	МА					
tls-profile			Locality	Burlington					
session-router	►		Organization	Engineering					
system	Þ		Unit						
			Common Name						
			Key Size	2048 💌					
			Alternate Name						
			ОК	Back					



ORACI	LE Ente	erprise S	ession Border Controller							a
							Dashboard	Configuration	Monitor and Trace	Widgets
🔯 Wizards 🔻	Comma	ands 🔻							Save Verify	Discard
media-manager			Modify Certificate Reco	rd						
security	v		Alternate Name							
authentication-	profile		Trusted	🖌 enable						
certificate-reco	rd		Key Usage List	digitalSignature	×					
tls-global				keyEncipherme	nt 🗙					
tls-profile			Extended Key Usage List	serverAuth 🗙	clientAuth 🗙					
session-router	)		Key Algor	rsa						
system			Digest Algor	sha256		•				
			Ecdsa Key Size	p256		•				
			Cert Status Profile List							
			OK	Back						
Show All	$\sum$									

Repeat the above steps again to create DigiCert root certificate. We need to import this root certificate to Windows machine where the Avaya Workplace client is installed. Once this certificate is imported, the soft client will work in TLS mode.

The table below specifies the parameters required for certificate configuration. Modify the configuration according to the certificates in your environment.

Parameter	DigiCertRoot
Common-name	DigiCert Global Root CA
Key-size	2048
Key-usage-list	digitalSignature keyEncipherment
Extended-key- usage-list	serverAuth
key-algor	rsa
digest-algor	sha256



## Step 2 – Generating a certificate signing request

(Only required for the SBC's end entity certificate, and not for root CA certs)

Please note – certificate signing request is only required to be executed for SBC Certificate – not for the root/intermediate certificates.

- Select the certificate and generate certificate on clicking the "Generate" command.
- Please copy/paste the text that gets printed on the screen as shown below and upload to your CA server for signature.

Copy the following information and send to a CA authority	
BEGIN CERTIFICATE REQUEST MIICvTCCAaUCAQAwRTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMR	4
MwEQYDVQQH EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzCCASIwDQY	
AQEBBQADggEPADCCAQoCggEBALzMG9rclE8r+f2nK1zIMcTJaLVdh+1WR +vWmKnn	
/nvifp7sKsUvFKX0bAjZU5SA5EpdHfYLC9G7jMz7dKJ0SUC0q6GkcFBKtvhBlf hU	
Js0vaSc3UMlc+jqy9G+2Fsd44mY/KMxPFQnMXECgT7RAyhKLj0zoxqi6dQ5zb yHg	
HGJ2dAPkXqmwBwc2zx101bawk9W/sk2o2gKWl5B6rOw2lCblVyekn7SUEPB C3IPM	
43NP43mvNQWbFffc3oCAzdqgWxvDzhQbvhu76nGJPnCGqxJoHR7dTD6GX wTVRLE1	
gNFOWdLWEh00RCktAltTNeV4KdcGeYrYZlkvJZlHHpT/7mkCAwEAAaAzMD	

• Also, note that a save/activate is required



## Step 3 – Deploy SBC & root certificates

Once certificate signing request have been completed – import the signed certificate to the SBC. Please note – all certificates including root and intermediate certificates are required to be imported to the SBC. Once done, issue save/activate from the WebGUI

Format:	try-all	<b>~ ()</b>
Import method:	File Paste	
Certificate file:		Browse

Repeat the steps for the following certificates:

- DigiCertRoot.

At this stage all the required certificates have been imported to the SBC.



### 7.10. TLS-Profile

A TLS profile configuration on the SBC allows for specific certificates to be assigned. Go to security-> TLS-profile config element and configure the tls-profile as shown below Please disable mutual authenticate option and also add options "ignore-root-ca=yes"

ORAC	LE Enterpr	ise Session Border Controller		Û 🔺	adı
			Dashboard Configuration Monitor and Trac	e Widget	5 5
🔅 Wizards 🔻	Commands	v	Save Verify	Discare	d
media-manager	•	Add TLS Profile			
security authentication certificate-reco tls-global tls-profile session-router system	▼ -profile rd ►	Name End Entity Certificate Trusted Ca Certificates Cipher List Verify Depth Mutual Authenticate TLS Version Options	TLSTeams   Enterprise   AvayaCert X   DigiCertRoot X   I   DEFAULT X		
		(	Back		

ORAC	LE Enterprise	Session Border Controller						Û 🔺 a
					Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 🔻	🔅 Commands 🔻						Save Verify	Discard
media-manager	►	Add TLS Profile						
security	•		DEFAULI X	1				
authentication	profile	Verify Depth	10	(Range: 010)				
certificate-reco	rd	Mutual Authenticate	enable					
tls-global		TLS Version	tlsv12 💌					
tls-profile		Options	ignore-root-ca=yes 🗙					
session-router	•	Cert Status Check	enable					
system	Þ	Cert Status Profile List						
		Ignore Dead Responder	enable					
		Allow Self Signed Cert	enable					
ci		ОК	Back					



### 7.11. Configure SIP Interfaces.

Navigate to sip-interface under session-router and configure the sip-interface as shown below. Please configure the below settings under the sip-interface which is configured for Avaya Workspace client.

- Tls-profile needs to match the name of the tls-profile previously created
- Set allow-anonymous to registered to ensure traffic to this sip-interface only comes from Workplace client which is registered to Avaya Session Manager via SBC.
- Set NAT traversal to always for the Avaya Workspace client to register.

ORACLE Enterprise Session Border Controller							
				Dashboard Configura	ation Monitor and Trace Widgets		
🔅 Wizards 👻	•				Save Verify Discard		
session-agent	Modify SIP Interface				Show Confi		
session-group							
session-recording-group	State	enable					
session-recording-server	Realm ID	AvayapublicRealm	Ŧ				
session-translation	Description						
sip-config							
sip-feature							
sip-interface	SIP Ports						
sip-manipulation	Add						
sip-monitoring	Address Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs		
sti-server	5061	TLS	TLSTeams	registered			
~	OK	Back					

			Dashboard	Configuration	Monitor and Trace	Widgets	Syste
Wizards Vizards Vi	Modify SIP Interface				Save Verify	Discard Show Cor	Se
session-recording-server	Nat Traversal	always 💌	)				
sip-config	TCP Nat Interval	30 90	( Range: 04294967295 ) ( Range: 04294967295 )				
sip-feature sip-interface	Registration Caching Min Reg Expire	enable	(Range: 099999999)				
sip-manipulation	Registration Interval Route To Registrar	3600 ✓ enable	(Range: 04294967295)				
sip-monitoring sti-server	Secured Network	enable					
translation-rules	OK	Back					



Similarly, Configure Internal IP under sip-port of sip-interface for Avaya Session Manager side. (Avaya Core Side). Set allow-anonymous to agents-only.

ORACLE Enterprise	Session Border Cont	troller					Û ▲ a
					Dashboard Config	uration Monitor and Trace	Widgets
🔅 Wizards 🔻						Save Verify	Discard
local-routing-config	Modify SIP Int	erface					Show Config
media-profile							
session-agent	State		✓ enable				
session-group	Realm ID		AvayaCoreRealm	•			
session-recording-group	Description						
session-recording-server							
session-translation							
sip-config	SIP Ports						
sip-feature	Add						
sip-interface	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs	
sip-manipulation	10.232.50.75	5060	UDP		agents-only		
Show All		ОК	Back				

ORACI	_E Enterprise	Session Border Con	troller						Ô 🔺
						Dashboard	Configuration	Monitor and Trace	Widgets
Wizards 💌	Commands 💌							Save Verify	Discard
local-routing-co	onfig	Modify SIP Int	erface						Show Co
media-profile session-agent session-group session-recordi session-recordi	ng-group ng-server	Realm ID Description SIP Ports		AvayaCoreRealm	V				
sip-config		Add							
sip-feature		Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	N	Iulti Home Addrs	
sin interface		10.232.50.75	5060	UDP		agents-only			
sis manipulatio		10.232.50.75	5060	ТСР		agents-only			
Show All	~		ОК	Back					

Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.



#### 7.12. Configure session-agent

Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data.

Configure the session-agent for Avaya Session Manager where SBC should route the calls. Go to session-router->Session-Agent.

- Host name and IP address to 10.232.50.127 which is the Avaya SM IP.
- Port set to 5060
- Realm ID Needs to match the realm created for Avaya SM. Transport set to "UDP+TCP

	Session Border Controller							Û 🔺 🧯
					Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 💌							Save Verify	Discard
A ldap-config	Add Session Agent							
local-policy	Hostname	10.232.50.127						
local-routing-config	IP Address	10.232.50.127						
media-profile	Port	5060		(Range: 0,102565535)				
session-agent	State	✓ enable						
session-group	App Protocol	SIP	•					
session-recording-group	Арр Туре		▼					
session-recording-server	Transport Method	UDP+TCP	•					
session-translation	Realm ID	AvayaCoreRealm						
sip-config	Egress Realm ID		•					
sip-feature v Show All	OK	Back						



### 7.13. Configure local-policy

Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

To register and make calls from Avaya Workspace client to Other Phones via sbc, The next hop here should be the Avaya SM IP which is 10.232.50.127

	Session Border Controller					Û▲ a
			Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 🔻 🔅 Commands 🔻					Save Verify	Discard
Idap-config	Add Local Policy					
local-policy	From Address	* X				
local-routing-config	To Addross					
media-profile	TO AUDIESS	*×				
session-agent	Source Realm	AvayapublicRealm 🗙				
session-group	Description					
session-recording-group						
session-recording-server						
session-translation	State	✓ enable				
sip-config	Policy Priority	none 💌				
sip-feature v	ОК	Back				

ORACL	E Enterprise	Session Border Co	ntroller								Û 🔺
							Dashbo	oard Configuration	Monitor ar	nd Trace	Widgets
🔅 Wizards 💌	🚯 Commands 👻								Save	Verify	Discard
Idap-config	^	Modify Local	Policy								
local-policy											
local-routing-cor	nfig	State		/ enable							
media-profile		Policy Priority		none	<b>v</b>						
session-agent		Doligy Attributor									
session-group		Policy Attributes									
session recording	a aroun	Add									
session-recording	R-Broop	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Ke	:y
session-recording	g-server	10.232.50.127	AvayaCoreRealm	none	disabled	0	enabled	SIP	single		
session-translatio	on										
sip-config											
sip-feature	~		OK Bac	k							
Show All											



## 7.14. Configure http-alg

The http-alg config is done for PPM support from SBC to Avaya SM. Navigate to http-alg under session-router and configure that as shown below

	Session Border Controller					Û.▲ a
			Dashboard	Configuration	Monitor and Trace	Widgets
👸 Wizards 🔻					Save Verify	Discard
enforcement-profile	Add HTTP Alg					
filter-config	Name	Avaya-SM				
h323	State	✓ enable				
http-alg	Description					
iwf-config						
ldap-config						
local-policy	Private					
local-response-map	Realm ID	CoreRealm 🔻				
local-routing-config	Address	10.232.50.75				
media-profile	Destination Address	10.232.50.127				
~	ОК Е	Back				

http-alg		Destination Address	10.232.50.127	
iwf-config		Destination Port	443	(Range: 165535)
ldap-config		TLS Profile	TLSTeams v	
local-policy		A Public		
local-response-map		Realm ID	Avayap 🔻	
local-routing-config		Address		
media-profile		Nat Address Port	10	(Deraul (FF7))
net-management-cont		TLS Profile	TLSTeams v	( Kange: L.occco )
q850-sip-map		Session Manager Mapping		
qos-constraints	,	OK Bac	k	
Show All				



## 7.15. Configure steering-pool

Steering-pool config allows configuration to assign IP address(es), ports & a realm.

ORACI	LE Enterprise	Session Border Controller						811	Û ▼ ak
						Dashboard	Configuration	Monitor and Trace	Widgets
🔯 Wizards 👻	🔆 Commands 👻							Save Verify	Discard
media-manager	٣	Add Steering Pool							
media-manage		IP Address							
media-policy		Start Port	30000		( Range: 165535 )				
realm-config		End Port	35000		( Range: 165535 )				
steering-pool		Realm ID	AvayapublicRealm	٣					
security	÷	Network Interface		٣					
session-router									
system	×								
		ОК	Back						
Show All									

ORACI	_E Enterprise	Session Border Controller						û ▼ a
					Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 🔻	🔅 Commands 🔻						Save Verify	Discard
media-manager	•	Add Steering Pool						
codec-policy								
media-manage	r	IP Address	10.232.50.75					
media-policy		Start Port	35001	(Range: 165535)				
realm-config		End Port	40000	(Range: 165535)				
steering-pool		Realm ID	AvayaCoreRealm	•				
security	•	Network Interface		•				
session-router	•							
system	•							
Chour All		OK	Back					



## 7.16. Configure sdes profile

Please go to  $\rightarrow$  Security  $\rightarrow$  Media Security  $\rightarrow$  sdes profile and create the policy as below.

ORACLE Ente	erprise Session Border Controller			а
			Dashboard Configuration	Monitor and Trace Widgets
🔅 Wizards 🔻	ands w			Save <b>Verify</b> Discard
certificate-record factory-accounts	Add Sdes Profile			
ike 🕨	Name	SDES		
ipsec 🕨	Crypto List	AES_CM_128_HMAC_SHA1_80 X AES_CM_128_HMAC_SHA1_32 X		
media-security <b>v</b>	Srtp Auth	enable		
dtls-srtp-profile	Srtp Encrypt	✓ enable		
media-sec-policy	SrTCP Encrypt	🗹 enable		
sdes-profile	Mki	enable		
sipura-profile	Egress Offer Format	same-as-ingress		
password-policy	Use Ingress Session Param	IS		
Show All	v	OK Back		



#### 7.17. Configure Media Security Profile

Please go to  $\rightarrow$ Security  $\rightarrow$  Media Security  $\rightarrow$ media Sec policy and create the policy as below: Create Media Sec policy with name SDES for the Avaya Public Side which will have the sdes profile created above.

Please set Mode to "any" for Inbound Media sec policy and Avaya Workplace client works in SRTP mode both ways after making this change and Assign this media policy to the AvayapublicRealm.

ORACL	Enterprise	Session Border Controller					Û.▲ ac
				Dashboard	Configuration	Monitor and Trace	Widgets
to Wizards ▼ certificate-record	Commands 🔻					Save Verify	Discard
factory-account	s	Modify Media Sec Policy					
ike	•	Name	sdesPolicy				
ipsec	•	Pass Through	enable				
local-accounts	- 1	Options					
media-security	-	⊿ Inbound					
dtls-srtp-prof	ile	Profile	SDES 🔻				
media-sec-po	olicy	Mode	any 🔻				
sdes-profile		Protocol	sdes 💌				
sipura-profile		Hide Egress Media Opdate	enable				
password-policy	,	Outbound					
security-config	~	ОК	Back				

	Session Border Controller						Û.▲ a
				Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 💌 🏠 Commands 💌						Save Verify	Discard
authentication	Add Media Sec Policy						
cert-status-profile	▲ Inbound						
certificate-record	Profile	SDES 🔻					
factory-accounts	Mode	any	•				
ike 🕨 🕨	Protocol Hide Egress Media Update	sdes enable	<b>v</b>				
ipsec	Outbound						
media-security 🔻	Profile	SDES 💌					
dtls-srtp-profile	Protocol	sdes	▼ ▼				
media-sec-policy	ОК	Back					



Similarly, Create Media Sec policy with name RTP to convert srtp to rtp for the Avaya SM side which will use only TCP/UDP as transport protocol. Assign this media policy to the AvayaCoreRealm.

ORACI	_E Enterpri	ise Session Border Controller					a
				Dashboard	Configuration	Monitor and Trace	Widgets
					-		
🔯 Wizards 💌	Commands	•				Save Verify	Discard
certificate-reco	rd ^	Add Madia Cas Daliau					
factory-accoun	ts	Add Media Sec Policy					
ike		Name	RTPI				
		Pass Through					
Ipsec	•	i ass i mough	enable				
local-accounts		Options					
media-security	v	Inbound					
dtls-srtp-pro	file	Profile	v				
media-sec-p	olicy	Mode	rtp	•			
sdes-profile		Protocol	none	-			
sipura-profile	2	Hide Egress Media Update	enable				
password-polic	y .	Outbound					
	~	ОК	Back				
Show All	$\bigcirc$						

#### 7.18. Configure Header Manipulation Rules (HMR)

As Avaya workspace client sends the requests in sips format, we need to add HMR in SBC to convert the incoming sips mode from access side to normal sip mode and send it to the core side. To achieve the same, we use the sip- manipulations as below as we need to convert URI, to, from, Contact Headers and mime rule to change rfc5939\_to\_rfc3711 from the incoming requests. The following sip-manipulation called **sips2sip** is configured with header rules and element rules for this purpose.



## To configure sip-manipulations, go to session-router->sip-manipulation

							Dashboard	Configuration	Monitor and Trace	Widgets
😳 Wizards 👻	Comman	nds 🔻							Save Verify	Discard
session-agent		^	Modify SIP Manij	oulation						Show Config
session-group			Name		sips2sip					
session-record	ing-group		Description							
session-record	ing-server									
session-transla	ition									
sip-config			Split Headers							
sip-feature										
sip-interface			Join Headers							
sip-manipulati	on		CfgRules							
sip-monitoring			Add 💌	Move Up	Move Down					
sti-server		~		ОК Ва	ick					
Show All										

	e Session Border Controller			Û ► a
		Dashboard Configuration	Monitor and Trace	Widgets
🔅 Wizards 🔻	·		Save Verify	Discard
session-agent	Modify SIP Manipulation			Show Confi
session-group	Join Headers			
session-recording-group	CfgRules			
session-translation	Add w Move Up Move Down			
sin-config	Name	Element Type		
Sip comp	modSIPStoSIP_ruri	header-rule		
sip-feature	modSIPStoSIP_Contact	header-rule		
sip-interface	modSIPStoSIP_To	header-rule		
cin manipulation	modSIPStoSIP_From	header-rule		
sip-manipulation	convert_rfc5939_to_rfc3711	mime-sdp-rule		
sip-monitoring	Displaying 1 - 5 of 5			
sti-server 🗸	OK Back			



Each Header rule and its element-rule config are given below:

Header Rule and Element Rule of Request URI header.

	Session Border Controller						Û 🔺	admin 🔻
				Dashboard	Configuration	Monitor and Trace	Widgets	System
🔅 Wizards 💌						Save Verify	Discard	Search
session-recording-group	Modify Sip manipulation ,	/ header rule						
session-recording-server	Name	modSIPStoSIP_ruri						^
sip-config	Header Name	Request-URI						
sip-feature	Action Comparison Type	manipulate case-sensitive	▼ ▼					
sip-interface	Мѕд Туре	any	*					
sip-monitoring	Methods	ACK X BYE X INVITE >	¢					
sti-server		REGISTER X						
translation-rules	Match Value							~
system V	ОК	Back						

ORACLE Enterprise	Session Border Controller					
				Dashboard	Configuration	Monitor and Trace
🚯 Wizards 👻 🚯 Commands 👻						Save Verify
session-recording-group	Modify Sip manipulation ,	/ header rule / element	rule			
session-recording-server	Name	modSIPStoSIP_ruri				
sin-config	Parameter Name					
sin-feature	Туре	header-value	•			
sip-interface	Action	find-replace-all	•			
sip-manipulation	Match Val Type	any	•			
sip-monitoring	Comparison Type	case-insensitive	•			
sti-server	Match Value	sips:				
translation-rules	New Value	sip:				
system						
Show All	ОК	Back				



Header Rule and Element Rule of Contact header.

	Session Border Controller					
				Dashboard	Configuration	Monitor and Trace
🚯 Wizards 🔻						Save Verify
session-recording-group	Modify Sip manipulation /	header rule				
session-recording-server	Name					
session-translation	Here des Marens	modSIPStoSIP_Contact				
sip-config	Header Name	Contact				
sip-feature	Action	manipulate	•			
sin_interface	Comparison Type	case-sensitive	•			
	Msg Type	any	v			
sip-manipulation	Methods	ACK × BYE × INVITE ×				
sip-monitoring		PRACK X REFER X				
sti-server		REGISTER 🗙				
translation-rules	Match Value					
system						
Show All	OK E	Sack				

	ORACLE Enterprise Session Border Controller									
				Dashboard	Configuration	Monitor and Trace				
🔅 Wizards 💌						Save Verify				
session-recording-group	Modify Sip manipulation /	' header rule / element rule	9							
session-recording-server session-translation	Name Parameter Name	modSIPStoSIP_contact								
sip-config	Туре	header-value	•							
sip-interface	Action	find-replace-all	•							
sip-manipulation	Match Val Type	any	•							
sip-monitoring	Comparison Type Match Value	case-insensitive	•							
sti-server	New Value	sip:								
translation-rules										
system	OK	Back								



Header Rule and Element Rule of To header.

	Session Border Controller					1
				Dashboard	Configuration	Monitor and Trace
🔅 Wizards 🔻 🏟 Commands 👻						Save Verify
session-recording-group	Modify Sip manipulation /	' header rule				
session-recording-server	Name					
session-translation	Nume	modSIPStoSIP_To				
sip-config	Header Name	То				
	Action	manipulate	•			
sip-reature	Comparison Type	case-sensitive	•			
sip-interface	Msg Type	201	-			
sip-manipulation	Mathada	any	•			
sip-monitoring	Metilous	ACK X BYE X INVITE X				
sti server		PRACK 🗙 REFER 🗙				
SU-SUIVEI		REGISTER 🗙				
translation-rules	Match Value					
system	ОК	Back				
Show All						

	Session Border Controller					
				Dashboard	Configuration	Monitor and Trace
🔯 Wizards 🔻						Save Verify
session-recording-group	Modify Sip manipulation /	' header rule / element ru	le			
session-recording-server session-translation	Name Parameter Name	modSIPStoSIP_to				
sip-config sip-feature	Type	header-value	•			
sip-interface	Match Val Type	find-replace-all any	▼ ▼			
sip-manipulation	Comparison Type	case-insensitive	•			
sti-server	New Value	sip:				
translation-rules system	ОК	Back				



Header Rule and Element Rule of From header.

ORACLE Enterprise	Session Border Controller				
			Dashboard	Configuration	Monitor and Trace
🚯 Wizards 🔻					Save Verify
session-recording-group	Modify Sip manipulation /	header rule			
session-recording-server	Name	modSIPStoSIP_From			
sip-config	Header Name Action	From			
sip-feature	Comparison Type	case-sensitive •			
sip-manipulation	Msg Type	any 💌			
sip-monitoring	Methods	ACK X BYE X INVITE X PRACK X REFER X			
sti-server		REGISTER 🗙			
translation-rules	Match Value				
system	ОК	Back			

	Session Border Controller					
				Dashboard	Configuration	Monitor and Trace
🔅 Wizards 🔻 🏟 Commands 👻						Save Verify
session-recording-group	Modify Sip manipulation /	header rule / element r	ule			
session-recording-server	Name					
session-translation	Darameter Name	modSIPStoSIP_trom				
sip-config	Parameter Name					
sip-feature	Туре	header-value	•			
sip-interface	Action	find-replace-all	•			
cin manipulation	Match Val Type	any	•			
sip-manipulation	Comparison Type	case-insensitive	•			
sip-monitoring	Match Value	sips:				
sti-server	New Value	sip:				
translation-rules						
system	OK	ack				



#### Header Rule and Element Rule of mime-sdp-rule

	Session Border Controller						Û 🗸
				Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 👻 🔅 Commands 👻						Save Verify	Discard
session-agent	Modify Sip manipulation /	mime SDP rule					
session-group	Name	convert_rfc5939_to_rfc3711					
session-recording-group	Msg Туре	request	•				
session-recording-server	Methods	INVITE X					
session-translation	Action	manipulate	•				
sip-config	Comparison Type	case-sensitive	•				
sip-feature	Match Value						
sip-interface	New Value						
sip-manipulation	CfgRules						
sip-monitoring	Add 👻 Move Up	Move Down					
sti-server 🗸	ОК	Back					
Show All							

🔣 CGBU Product and Solutions - 🤇 🗙	Enterprise Session Border Contr X     In Oracle WebCenter Sites 12c     X     +		-	o ×
← → C û 🛛 🔏 🛱 10	.138.194.139/?root=maincontent.nocache&content=config.nocache&config=s	p-manipulat 🚥 🔽 🗙 🔍 Search	III\ 🗊	≝ ⊜ ≡
	Session Border Controller		Ô 🔺	admin 👻
		Dashboard Configuration	Monitor and Trace Widgets	System
🔅 Wizards 👻			Save Verify Discard	Search
session-agent	Modify Sip manipulation / mime SDP rule / SDP media rule			
session-group	Match Value			^
session-recording-group	New Value			
session-recording-server	CfgRules			
session-translation	Add - Main Da			
sip-config	Name	Element Type		
sip-feature	modcryptoline	sdp-line-rule		
sip-interface	delattr	sdp-line-rule		
sip-manipulation	delattr1	sdp-line-rule		
sin-monitoring	modmline	sdp-line-rule		
all montaning	Displaying 1 - 4 of 4			~
sti-server	OK Back			



ORAC	LE Ente	erprise S	Session Border Controller						
							Dashboard	Configuration	Monitor and Trace
🔅 Wizards 🔻	Comma	ands 🔻							Save Verify
session-agent		^	Modify Sip manipulation /	mime SDP rule / SDP me	edia	rule / SDP line rule			
session-group			Name	modcryptoline					
session-record	ling-group		Туре	a					
session-record	ling-server		Action	replace	•				
session-transl	ation		Comparison Type	pattern-rule	•				
sip-config			Match Value	^acap:[0-9]+ (crypto:.+)\$					
sip-feature			New Value	\$1					
sip-interface									
sip-manipulati	on								
sip-monitoring	g								
sti-server		~	ОК В	ack					

ORACLE Enterprise	Session Border Controller					
				Dashboard	Configuration	Monitor and Trace
🔅 Wizards 🔻						Save Verify
session-agent	Modify Sip manipulation /	mime SDP rule / SDP m	edia rule / SDP lir	ne rule		
session-group	Name	delattr				
session-recording-group	Туре	a				
session-recording-server	Action	delete	•			
session-translation	Comparison Type	pattern-rule	•			
sip-config	Match Value	tcap:[0-9]+ RTP/SAVP				
sip-feature	New Value					
sip-interface						
sip-manipulation						
sip-monitoring						
sti-server 🗸	ОК В	lack				
Show All						



	orise Session Border Controller					
				Dashboard	Configuration	Monitor and Trace
🔅 Wizards 🔻 🔅 Command	ls 🔻					Save Verify
session-agent	Modify Sip manipulati	on / mime SDP rule / SDP me	dia rule / SDP line ru	le		
session-group	Name	delattr1				
session-recording-group	Туре	a				
session-recording-server	Action	delete	v			
session-translation	Comparison Type	pattern-rule	•			
sip-config	Match Value	^pcfg:[0-9]+ t=[0-9]+ a=[0-9]+\$				
sip-feature	New Value					
sip-interface						
sip-manipulation						
sip-monitoring						
sti-server	OK	Back				

	Session Border Controller					
				Dashboard	Configuration	Monitor and Trace
🔅 Wizards 🔻						Save Verify
session-agent	Modify Sip manipulation ,	/ mime SDP rule / SDP m	edia rule / SDP lir	ne rule		
session-group	Name	modmline				
session-recording-group	Туре	m				
session-recording-server	Action	replace	•			
session-translation	Comparison Type	pattern-rule	•			
sip-config	Match Value	(audio.+)RTP/AVP(.+)				
sip-feature	New Value	\$1+"RTP/SAVP"+\$2				
sip-interface						
sip-manipulation						
sip-monitoring						
sti-server	ОК	Back				



Assign this sip manipulation sips2sip as InManipulationID to the access side SIP Interface.

	Consider Constraller						∩ <del>–</del> ar
	Session Border Controller			Dashboard Co	onfiguration	Monitor and Trace	Widgets
🔅 Wizards 🔻						Save Verify	Discard
media-profile	Modify SIP Interface						Show Config
session-group	State	🖌 enable					
session-recording-group	Realm ID	AvayapublicRealm	•				
session-recording-server	Description						
session-translation							
sip-config							
sip-feature	SIP Ports						
sip-interface	Add						
sip-manipulation	Address Port	Transport Protocol	TLS Profile	Allow Anonymous	Ν	fulti Home Addrs	
sip-monitoring	ОК	Back					

	Session Border Controller					
			C	Dashboard	Configuration	Monitor and Trace
🔅 Wizards 👻						Save Verify
· ^						
session-agent	Modify SIP Interface					
session-group		101,107				
	Port Map Start	0	(Range: 0,102565535)			
session-recording-group	Port Map End	0	(Range: 0,102565535)			
session-recording-server	In Manipulationid	sips2sip		-		
session-translation	Out Manipulationid					
sip-config	SIP Atcf Feature	enable				
sip-feature	Rfc2833 Payload	101	(Range: 96127)			
sip-interface	Rfc2833 Mode	transparent				
sip-manipulation	Response Map	•				
sip-monitoring	Local Response Map	•				
sti-server 🗸	ОК В	ack				
Show All						

With this, the SBC configuration is complete.



# 8. Existing SBC configuration

If the SBC being used with Avaya Session Manager is an existing SBC with functional configuration, following configuration elements are required:

- New realm-config
- Configuring a certificate for SBC Interface
- TLS-Profile
- New sip-interface
- New session-agent
- <u>HTTP-ALG</u>
- New local-policy
- New steering-pools
- SDES Profile
- Media-sec-Policy
- <u>SIP-Manipulations</u>

Please follow the steps mentioned in the above sections to configure these elements.



# 9. Registration and Verification of Avaya Workspace Client for Windows Configuration

Once the SBC and Avaya Session Manager configuration is complete, we can try registering the Avaya Workplace client (17814437248 as DN) along with other remote phones and local phones and can verify whether they are successfully registered to the Avaya Session Manager.

Please Navigate to: Elements->Session Manager->System Status-> User registration. Verify whether the users are registered successfully to the Session Manager.

AV/ Aura® Syste	m Manager 8.1	Users <sup>,</sup>	v 🎤 Ele	ments 🗸 🏼 🏟 Services	~   W	idgets v	Shortcuts v				Search		≡	a	dmin
Home	Session Manager														
Devic	ce and Locati *													H	ielp ?
Appl	ication Confi	Us	er Regi	strations											
Sueta	Select rows to send notifications to devices. Click on Details column for complete registration status.														
Jyste	System status A Customize														
:	SIP Entity Monit View • Default Export Force Unregister Notifications: Reboot Reload • Failback As of 4:01 AM Advanced Search •										sh 🔹				
	Managed Band	4 Ite	ems   ಿ   S	how All ~									Filte	r: Ena	able
			Details	Address	First	Last	Actual	IP Address	Remote	Shared	Simult.	AST	Regis	tered	
:	Security Modul				Name	Name	Location		Office	Control	Devices	Device	Prim	Sec	Surv
	SIP Firewall Stat		▶ Show	17814437246@aura.com	Avaya	User	Phonerlite	10.232.50.2			1/4		◄	Ц	
			▶ Show	17814437245@aura.com	Avaya	User2	Phonerlite	172.18.0.133			1/4		◄		
l	Registration Su		▶ Show	17814437248@aura.com	Avaya	User4	Phonerlite	10.232.50.75			1/4		V		
	User Registratio		▶ Show	17814437247@aura.com	Avaya	User3	Phonerlite	10.232.50.75	V		1/4		V		
		Sele	ct : All, Non	e											

As we can see, there are couple of DNs registered as Remote office phones which has the IP address of SBC inside IP (10.232.50.75) out of which Avaya Workplace client is one phone and these phones are registered via Oracle SBC to Avaya Session Manager. There are also two phones registered to Avaya Session Manager directly



As we are specifically testing Avaya Workplace soft client in this document, we can confirm that client is successfully registered to Avaya SM through Oracle SBC as shown below.

17814437248	» – × ▲ 00
Incoming Call Features	
No Incoming Call Features available 🔹	>
	>
History is not available	
왕 Workplace Meetings	
🖧 Join Workplace Meeting	>
New Conversation +	4 <u>c</u> y

We can also see the registration flow below. We can see that REGISTER is successful and also SBC caches registration info. After that, register is directly answered by SBC instead of routing to Avaya SM till next expires time.

					🗘 🔻 adm
		Dashb	oard Configuration	Monitor and Trace	Widgets S
579-95fe-80fba8241	870 ¥				
	[+] Sessio	on Summary			
210.88		1	0.232.50.75	10	0.232.50.127
<b>→</b>	REGISTER (1)	$\rightarrow$			
	EGRE	ESS ROUTE, TYPE	=, NEXT HOP=sip:a	aura.com	
			+	REGISTER (1)	
			←	Status:401 (1)	+
	Status:401 (1)	+			
+	REGISTER (2)				
	EGRE	ESS ROUTE, TYPE	=, NEXT HOP=sip:a	ura.com	
_			+	REGISTER (2)	
	Stature 200 (2)		-	Status:200 (2)	•
· · ·	Status:200 (2)	•			
	Status: 200 (3)				
	PEGISTER (4)				
, 	Status:200 (4)	É.			
+	REGISTER (5)				
	, , , ,		→       REGISTER (4)         →       Status:200 (4)         →       REGISTER (5)	→     REGISTER (4)       ←     Status:200 (4)       →     REGISTER (5)       Refresh     Export diagram       Export session details	→       Status:200 (4)         →       REGISTER (5)

ORACLE Enterprise Se	lession Border Controller 🗘 🔻 admin 🔻										
	Dashboard Configuration Monitor and Trace Widgets System										
Sessions	Registration List bf415d8c-895f-4579-95fe-80fba8241870 🗙										
Registrations	2020-12-09 03:37:25.232 EGRESS ROUTE, TYPE=, NEXT HOP=sip:aura.com										
Subscriptions	2020-12-09 03:37:25.232       →       REGISTER (3)       →         2020-12-09 03:37:25.239       ←       Status:200 (3)       ←										
Notable Events	2020-12-09 03:37:25.240 ← Status:200 (3) ←										
	Details for REGISTER (1 2-09 03:31:24.516										
	2020-12-09 03:31:24.516										
	REGISTER sips:aura.com SIP/2.0										
	From: <sips:17814437248@aura.com>;tag=891330c5-alc1-4c3d-8e48-34ab19069fec</sips:17814437248@aura.com>										
	To: <sips:17814437248@aura.com></sips:17814437248@aura.com>										
	Call-ID: bf415d8c-895f-4579-95fe-80fba8241870										
	CSeq: 1 REGISTER										
	Max-Forwards: 70										
	Via: SIP/2.0/TLS 192.168.1.10:52639;received=122.172.210.88;branch=z9hG4bKd7465648-0d9b-4745-a7c8-110d4d9042c8;rport=52639										
	Supported: eventlist,outbound,replaces,vnd.avaya.ipo										
	Allow: INVITE, ACK, OPTIONS, BYE, CANCEL, NOTIFY, MESSAGE, REFER, INFO, FUBLISH, UPDATE										
	User-Agent: Avaya Communicator/3.0 (3.13.0.53.15; Avaya CSDK; Microsoft Windows NT 6.2.9200.0)										
	Contact: <sips:17814437248@192.168.1.10:52639>;q=1;expires=3600;+sip.instance="<urn:uuid:654b8d3c-5da4-4dc3-a46a-9043a8d698e6> 🗸</urn:uuid:654b8d3c-5da4-4dc3-a46a-9043a8d698e6></sips:17814437248@192.168.1.10:52639>										
	Refresh Export diagram Export session details										



We can also make calls from Avaya Communicator Workplace soft client and we can verify the signaling path. The above call is made from access side to core side.

ORACLE Enter	prise Session Border Controller							<u>∏</u> , ▼	admin 🚽	
-					Dashboard	Configuration	Monitor and Trace	Widgets	Syster	
Sessions	Corrigo List 7000b41f c7b0 43b4 b	175 01002-F1Fd0	k v							
Registrations	36551011 LIST 70000411-(700-4204-0	400-91600011100	~ ×						_	
			[+] Se	ssion Summary						
Subscriptions	122.172.210	.88			10.232	.50.75	10	.232.50.12	27	
Notable Eusete	2020-12-09 04:09:35.143	+	INVITE (1)							
NULUNE EVENIS	2020-12-09 04:09:35.143	←	Status:100 (1)	+						
	2020-12-09 04:09:35.150	) MEDIA FLOW ADD, ID=134218193, DIRECTION=CALLING								
	2020-12-09 04:09:35.151	MEDIA FLOW ADD, ID=134218194, DIRECTION=CALLED								
	2020-12-09 04:09:35.152		EGRESS R	OUTE, TYPE=,	NEXT HOP=	=sip:1781443724	16@aura.com			
	2020-12-09 04:09:35.152					Þ	INVITE (1)		•	
	2020-12-09 04:09:35.158						Status:100 (1)		+	
	2020-12-09 04:09:35.161					←	Status:407 (1)		+	
	2020-12-09 04:09:35.161					+	ACK (1)		+	
	2020-12-09 04:09:35.163	←	Status:407 (1)	+						
	2020-12-09 04:09:35.778	+	ACK (1)	$\rightarrow$						
	2020-12-09 04:09:35.793	+	INVITE (2)	$\rightarrow$						
	2020-12-09 04:09:35.794		Status:100 (2)	+						
	2020 12 00 04 00 25 000		FORFOC R	OUTE TUDE	NEVT HOD	1701440704	VA			

Here the INVITE from access side comes with TLS protocol and from SBC it is changed to TCP/UDP

Similarly, we can also make calls from core side to access side and check the SIP path. Here the call is converted to TLS after reaching SBC.

	ise Session Border Controller						Û 🔺	admin 🚽	
				Dashboard	Configuration	Monitor and Trace	Widgets	Syster	
Sessions		1 0005 FD0C3DF0D 420 040 373 F0 3							
Registrations	Session List 809F2150-0E58-EB	11-88BE-5D9C2DF0D428@10.252.50.2	×						
-		ľ	+] Session Sur	mmary					
Subscriptions	10.232.50.127	10.232.	50.75			12	2.172.210.	88	
Notable Events	2020-12-09	INIVITE (1086)							
Hotable Events	04:22:26.859	INVITE (1000)	·						
	2020-12-09	Statue:100 (1086)	4						
	04:22:26.860	Status.100 (1080)	'						
	2020-12-09	MEDIA ELOW ADD ID=50332123 DIRECTION=CALLING							
	04:22:26.866	MEDIA FLOW ADD, ID-30332123, DIRECTION=CALLING							
	2020-12-09	MEDIA ELOW ADD ID=50332124 DIRECTION=CALLED							
	04:22:26.866	MEDIATI	.0 " ADD, ID	, 50552124, DIREC	TION CALLE	0			
	2020-12-09	EGRESS ROUTE, TYPE=le	ocal-policy, NE	EXT HOP= <sip:178< td=""><td>14437248@122.</td><td>172.210.88:51125;</td><td></td><td></td></sip:178<>	14437248@122.	172.210.88:51125;			
	04:22:26.867	acme_nat=	17814437248+	122.172.210.88@19	2.168.1.6:51125	5>			
	2020-12-09			ļ	•	INVITE (1086)		<b>→</b>	
	04:22:26.867							_	
	2020-12-09				<b>←</b> !	Status:100 (1086)		+	
	04:22:27.221								
	2020-12-09				<u> </u>	Status-190 (1096)		-	
		Refresh	Export diagram	Export session details					



## Appendix A

Following are the test cases that are executed as part of Avaya workspace client config and Avaya Session Manager with Oracle SBC in between. We get limited call options in manual mode and the Test cases that has been executed are listed below.

Note: Please note that the workspace client side is configured to work in TLS/SRTP mode (Avaya Workspace client to SBC) and Core side is configured to work in TCP/UDP mode (SBC to Avaya Session Manager). Call Merge or Conference option is not working in Avaya Workplace client and we cannot check this issue with Avaya as our SBC is not tested/certified by Avaya as supported SBC as of today.

Serial	Test Cases Executed	Result
Number		
1	Register Avaya Workspace client to Avaya Session manager via Oracle SBC	Pass
2	Outbound Call from Avaya Workspace client to other users, calling party hangs up after call	Pass
3	Outbound Call from Avaya Workspace client to other users, called party hangs up after call	Pass
4	Inbound Call to Avaya Workspace client from other user, calling party hangs up	Pass
5	Inbound Call to Avaya Workspace client from other user, called party hangs up	Pass
6	Outbound call from Avaya Workspace client and client CANCEL the call before call is established	Pass
7	Outbound Call from Avaya Workspace client to other user, answers the call, caller puts call on hold, then retrieves the call to ensure speech path is returned	Pass
8	Inbound call to Avaya Workspace client, answers the call, caller puts call on hold, then retrieve the call to ensure speech path is returned	Pass
9	Outbound Call from Avaya Workspace client phone to other device; Keep the call active for more than 30 minutes	Pass
10	Inbound Call to Avaya Workspace client and keep the call active for more than 30 minutes	Pass
11	Avaya Workspace client makes outbound call User A, User A attends the call and then Avaya Workspace client transfers the call to User B	Pass
12	User A calls inbound call to Avaya Workspace client and Avaya Workspace client attends the call and transfers to User B	Pass



## 10. Caveat

#### 10.1. SRTP Call flow scenarios.

In some cases if we set **Mode to "any" for Inbound Media sec policy** as described in Section 7.17, the SRTP is not flowing towards the other side. To solve this issue, Use the given HMR **chg3711to5939** as **OutManipulationid** to the access side SIP Interface and then set the **Mode to "SRTP" for Inbound Media sec policy**. After making this change, the call works with TLS/SRTP both ways. The end user can add this HMR from the SBC GUI or through CLI according to their convenience. We have also provided the other HMR **sips2sip** config below for reference.

The configuration elements mentioned in this section maybe necessary to support SRTP exchanges between the client and the Oracle SBC (OCSBC). A protocol mismatch between the client and the OCSBC can result in unintelligible audio being experienced by both calling and called parties.

Calls from Client - SDP offers from the client may use RFC5939 to signal support for SRTP. One of the roles of HMR "**sips2sip**" (in this section) is to convert these SDP offers to RFC 3711 (i.e. a SRTP format currently supported by the OCSBC). HMR "**chg3711to5939**" presents SDP answers (from the OCSBC) as per RFC5939 to the client.

Calls to Client - SDP offers from the OCSBC are sent as RFC3711 to the client. The client responds using RFC3711.

sip-manipulation	on	
name	chg	3711to5939
mime-sdp	o-rule	
	name	modsdp
	msg-type	reply
	methods	INVITE
	action	manipulate
	comparison-type	case-sensitive
	match-value	
	new-value	
	sdp-media-rule	
	name	modmline
	media-type	audio
	action	manipulate
	comparison-type	case-sensitive
	match-value	
	new-value	
	sdp-line-rule	
	name	getacapvalue
	type	a
	action	store
	comparison	type pattern-rule
	match-value	^crypto:([0-9]+)/s[\w\s\:V]+
	new-value	
	sap-line-rule	a dalafa
	name	addcrg
	type	a
	action	
	comparison motob voluc	upe Doolean Cmododo Cmodmlino Castosopuelus
	match-value	amousup.amournine.agetacapvalue



new-value

acfg:+\$modsdp.\$modmline.\$getacapvalue.\$1 +" t=1 a="+\$modsdp.\$modmline.\$getacapvalue.\$1

sip-manipulation	
name	sips2sip
description	
split-headers	
join-headers	
header-rule	
name	modSIPStoSIP_ruri
header-name	Request-URI
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	ACK,BYE,INVITE,PRACK,REFER,REGISTER
match-value	
new-value	
element-rule	
name	modSIPStoSIP_ruri
parameter-name	
type	header-value
action	find-replace-all
match-val-type	any
comparison-type	case-insensitive
match-value	sips:
new-value	sip:
neader-rule	
name	modSIPStoSIP_Contact
neader-name	Contact
action	manipulate
comparison-type	case-sensitive
msg-type	
metrous	AUR, DIE, INVITE, PRAUR, REFER, REGISTER
element-fule	modSIDStaSID contact
name parameter-pame	
type	beader-value
action	find-replace-all
match-val-type	any
comparison-type	case-insensitive
match-value	sins:
new-value	sin
header-rule	-it.
name	modSIPStoSIP To
header-name	To
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	ACK, BYE, INVITE, PRACK, REFER, REGISTER
match-value	
new-value	



element-rule modSIPStoSIP\_to name parameter-name type header-value find-replace-all action match-val-type any comparison-type case-insensitive match-value sips: new-value sip: header-rule modSIPStoSIP\_From name From header-name action manipulate comparison-type case-sensitive msg-type any ACK, BYE, INVITE, PRACK, REFER, REGISTER methods match-value new-value element-rule modSIPStoSIP\_from name parameter-name header-value type action find-replace-all match-val-type any comparison-type case-insensitive match-value sips: new-value sip: mime-sdp-rule convert\_rfc5939\_to\_rfc3711 name msg-type request methods INVITE action manipulate comparison-type case-sensitive match-value new-value sdp-media-rule name modmline media-type audio manipulate action case-sensitive comparison-type match-value new-value sdp-line-rule modcryptoline name type а action replace comparison-type pattern-rule match-value ^acap:[0-9]+ (crypto:.+)\$ new-value \$1 sdp-line-rule name delattr type а



action comparison-type match-value new-value	delete pattern-rule tcap:[0-9]+ RTP/SAVP
sdp-line-rule	
name	delattr1
type	а
action	delete
comparison-type	pattern-rule
match-value	^pcfg:[0-9]+ t=[0-9]+ a=[0-9]+\$
new-value	
sdp-line-rule	
name	modmline
type	m
action	replace
comparison-type	pattern-rule
match-value	(audio.+)RTP/AVP(.+)
new-value	\$1+"RTP/SAVP"+\$2

The screenshot of the particular config is given below for reference.

	Session Border Controller						û <b>→</b> ac
				Dashboard	Configuration	Monitor and Trace	Widgets
🚯 Wizards 🔻 🧔 Commands 🔻						Save Verify	Discard
media-profile							
session-agent	Modify SIP Interface						Show Config
session-group	State	✓ enable					
session-recording-group	Realm ID	AvayapublicRealm	T				
session-recording-server	Description						
session-translation							
sip-config							
sip-feature	SIP Ports						
sip-interface							
sip-manipulation	Add						
sin monitoring	Address Port	Transport Protocol	TLS Profile	Allow Anonymous	Ν	fulti Home Addrs	
sip-monitoring	0	K Back					
Show All							

|--|--|--|--|

ORACLE Enterprise Session Border Controller							
				Dashboard	Configuration	Monitor and Trace	
🚯 Wizards 🔻						Save Verify	
session-agent	Modify SIP Interface						
session-group	Port Map Start	0	(Range: 0,102565535)				
session-recording-group	Port Map End	0	(Range: 0,102565535)				
session-recording-server	In Manipulationid	sips2sip 💌					
session-translation	Out Manipulationid	chg3711to5939					
sip-config	SIP Atcf Feature	enable	-				
sip-feature	Rfc2833 Payload	101	(Range: 96127)				
sip-interface	Rfc2833 Mode	transparent 🔹					
sip-manipulation	Response Map						
sip-monitoring	Local Response Map	•					
sti-server	ОК В	ack					



CONNECT WITH US



Oracle Corporation, World Headquarters 500 Oracle Parkway Redwood Shores, CA 94065, USA Worldwide Inquiries Phone: +1.650.506.7000 Fax: +1.650.506.7200

#### Integrated Cloud Applications & Platform Services

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615