

# Oracle SBC working as Zoom Phone Local Proxy

**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.

# **Revision History**

As a best practice always follow the latest Application note available on the Oracle TechNet Website.

https://www.oracle.com/technical-resources/documentation/acme-packet.html

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC configured as Zoom Phone Local Proxy	24 Feb 2022
1.1	Added Disclaimers Section 2.1 Updated Certificates in Section 7.9	18 March 2024

# **Table of Contents**

1 INTENDED AUDIENCE	4
2. DOCUMENT OVERVIEW	4
2.1 ZOOM PHONE LOCAL PROXY	4
4 ZOOM BHONE LOCAL BROWN BEOLIDEMENTS	
4. ZOOM PHONE LOCAL PROXY REQUIREMENTS	Э
5. NETWORK ARCHITECTURES	6
5.1 INTERNAL ZOOM PHONE NATIVE CALLING PLAN USER TOPOLOGY	6 6
5.1.1 Extension to Extension thanng	
5.3 EXTERNAL ZOOM PHONE USER TOPOLOGY	
6. CONFIGURE ZOOM PHONE LOCAL PROXY	9
6.1 REGISTER TENANT DOMAIN	
6.2 VERIFY DOMAIN	
6.3 REGISTER LOCAL PROXY	
7. CONFIGURING THE SBC	
7.1 CONFIGURE SBC USING WEB GUI	
7.2. CONFIGURE SYSTEM-CONFIG	
7.5 NTP-SYNC	15 16
7.5. CONFIGURE PHYSICAL INTERFACE VALUES	
7.6. CONFIGURE NETWORK INTERFACE VALUES	
7.7. ENABLE MEDIA MANAGER	
7.8. CONFIGURE REALMS	
7.8.1 Realm ZoomEndpoints	
7.0 SIP SECURITY CONFICURATION	
7.9.1 Configuring Certificates	
7.9.1.1 End Entity Certificate	
7.9.1.2 Import Root CA Certificates.	
7.10. TLS-PROFILE	
7.10.1 TLS-Profile – TLSZoomEndpoints	
7.10.2 TLS-Profile – TLSZoomCloud	
7.11. CONFIGURE SIP INTERFACES 7.11.1 Sip_Interface for Zoom Endpoints	
7 11 2 Sip-Interface for Zoom Cloud	
7.12. CONFIGURE SESSION-AGENT	
7.13. CONFIGURE LOCAL-POLICY	
7.14. CONFIGURE STEERING-POOL	
7.14.1 Zoom Endpoints Steering Pool	
/.14.2 Zoom Cloud Steering Pool	
7.15. MEDIA SECURITY CONFIGURATION	
7 15 2 Configure Media Security Profile	
7.16. SBC Behind NAT SPL configuration	
7.17. SESSION TIMER PROFILE (OPTIONAL)	

7.18 CAVEAT -OPUS TRANSCODING
-------------------------------

## **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 Zoom Phone Service.

## 2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC as a Zoom Phone Local Proxy. The Application note focuses on the steps required to configure the Zoom Phone Local Proxy on the Zoom Admin Portal and how to create the connection between Oracle SBC and Zoom Phone Service.

Oracle Enterprise Session Border Controllers (E-SBCs) also support Zoom Phone Premise Peering which is the BYOC offering from Zoom. Please follow our Application Note "Zoom Premise Peering-(BYOC) with Oracle <u>ESBC</u>" to configure Zoom BYOC with Oracle SBC.

## 2.1 Zoom Phone Local Proxy

Oracle Enterprise Session Border Controllers (E-SBCs) are security devices that secure your critical, real-time communications for collaboration, unified communications (UC), and contact centers. Interconnect SIP trunks, on-premises enterprise telephony, UCaaS, CCaaS, and any other SIP service with reliability, quality, and scalability.

Oracle Enterprise Session Border Controller deployed as a Zoom Phone Local Proxy are Oracle SBCs hosted in the DMZ to secure the traffic originating from Zoom Phones over Public Internet. Oracle SBCs provide a perimeter defense against myriad cyber-attacks and ensures communication privacy and security. Once the Zoom Phones are enabled for the use of Local Proxy, all the traffic from the phones traverse from Oracle SBC which provides a layer of security.

#### Disclaimer -

- Zoom Phone Local Proxy is not a GA feature opened to the general public. It is only to be used in specific cases under request to Zoom.
- Zoom Phone Local Proxy is incompatible with Zoom Phone Local Survivability.

https://support.zoom.us/hc/en-us/articles/360001297663-Getting-started-with-Zoom-Phone-admin-

https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/configuration/sbcconfiguration-guide.pdf

https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/security/security-guide.pdf

https://www.oracle.com/a/ocom/docs/industries/communications/communications-session-border-controllerds.pdf

# **3. Validated Oracle Versions**

We have successfully conducted testing with the Oracle Communications SBC versions SC900p2. Minimum recommended Version – SCZ8.4 and above.

These software releases with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6350
- AP 6300
- AP 3950 (Release SCZ9.0.0 Only)
- AP 4900 (Release SCZ9.0.0 Only)
- VME

More details about different Oracle SBC Platforms can be found here.

# 4. Zoom Phone Local Proxy Requirements.

Below are the Configuration and System requirements for the Zoom Phone Local Proxy. Oracle SBC fulfils all the mentioned requirements.

- SBC must NOT have configuration that alter any SIP messages destined for Zoom Data Center that transit through it.(Regular B2BUA functionality which change signaling and media addresses is acceptable).
- SBC must have a certificate that is signed by one of Zoom's approved CA vendors.
- SBC Certificate must have the FQDN or domain name that is configured on the Zoom admin portal in the CN/SAN.
- FQDN or SRV must be resolvable within the internal corporate DNS servers. Zoom recommends that
  these entries must not be resolvable on external DNS servers and let traffic route directly to Zoom
  servers.
- FQDN is used for a single SBC.SRV records must be used if there are multiple SBCs which are not in a HA pair.
- FQDN or SRV must be operational prior to enabling it on a site. If the FQDN or SRV is not operational, the desk phone devices may fail to register and would require a manual reboot.
- Zoom Phone Local Proxy must support codecs Opus, G722, G711u/a, G729.OPUS should be set as priority codec.
- Minimum required TLS Version is TLS 1.2.
- Zoom Phone Local Proxy must support these Media ciphers- AEAD\_AES\_256\_GCM, AES\_256\_CM\_HMAC\_SHA1\_80, AES\_CM\_128\_HMAC\_SHA1\_80, AES\_CM\_128\_HMAC\_SHA1\_32,
- These ciphers should not be hardcoded and a super set of ciphers which includes the supported ciphers should be configured.

- Media Ciphers supported -TLS\_ECDHE\_RSA\_WITH\_AES256\_GCM\_SHA384,RSA\_WITH\_AES256\_CBC\_SHA256,RSA\_WITH\_ AES128\_CBC\_SHA
- Zoom recommends using Port 5091 for inbound TLS connections. Other ports are also supported.
- At present single SIP Zone per proxy server is supported.
- In case of failover, zoom clients must use SRV records to failover to a 2nd instance of the proxy server. FQDN with multiple IP addresses are NOT supported
- Zoom clients use RTCP-XR to report call statistics. This information must not be filtered by the proxy.

# 5. Network Architectures

In this section we will cover the Architectures for different Zoom Phone Local Proxy Topologies.

## 5.1 Internal Zoom Phone Native Calling Plan User Topology.

Below figure illustrates the position of Zoom Phone Local Proxy in the Customer Network. In this scenarios Zoom Phones are enabled with the <u>Zoom Native Calling Plan</u>. Oracle SBC, which is <u>certified</u> with Zoom Phone, is hosted in the Enterprise Network's premise DMZ and is used to steer the signaling, media to, and from the Zoom Phones towards the Zoom Cloud. Zoom Phones in the Corporate premise register onto the Zoom Cloud through Oracle SBC which maintains a local cache of these registrations. Oracle SBC is configured to route all outbound calls to the Registrar (Zoom Cloud) which terminates it to the PSTN Network.

## 5.1.1 Extension to Extension dialing

Calls between two internal users (extensions) also traverse through Oracle SBC, Caller Zoom Phone sends the call to Oracle SBC, which is forwarded to the Zoom Cloud after basic B2BUA operations ,the call is returned to the Callee registered behind Oracle SBC. Oracle SBC performs a registration cache lookup and terminates the call.



1/18

# 5.2 Internal Zoom Phone BYOC User Topology.

In below scenario Zoom Phones are enabled with the <u>Zoom BYOC</u> Calling Plans. Oracle SBC, which is <u>certified</u> with Zoom Phone, hosted in the Enterprise Network's premise DMZ, is used to steer the signaling, media to, and From the Zoom Phones towards the Zoom Cloud.

PSTN calls are hair pinned back from Zoom BYOC Endpoints to Oracle SBC which further routes to the appropriate Carrier trunk to terminate onto the PSTN Network.



////

# 5.3 External Zoom Phone User Topology

When the Users are outside the corporate Network no traffic is sent from the Zoom Phones towards Oracle SBC. Users register to Zoom Cloud directly bypassing the Oracle SBC. The Oracle SBC FQDN/SRV configured as Zoom Proxy must be resolvable within the internal corporate DNS servers. These FQDN/SRV should not be resolvable from Public DNS Servers so that the traffic flows directly to Zoom Servers bypassing the Oracle SBC.



# 6. Configure Zoom Phone Local Proxy

This Section describes the steps to configure the Zoom Phone Local Proxy on the on the Zoom Admin Portal. For detailed assistance with setting up and configuring your Zoom Phone System, please reach out to Zoom Sales: <u>https://zoom.us/contactsales</u>

# 6.1 Register Tenant Domain

Before the Zoom Proxy can be added, the Tenant Domain (Oracle SBC Domain) must be registered and verified on the Zoom Portal.

- Navigate to Admin> Account Management > Account Profile.
- Scroll Down to look for the Associated domain Section. If the desired domain is not registered
- Click on Add Associated Domain and add your domain.

<ul> <li>Account Management</li> </ul>		
Account Profile	Account Support Information	
Account Settings	Additional support instructions	
Billing		

ZOOM SOLUTIONS -	PLANS & PRICING CONTACT SALES	SCHEDULE A MEETING
Video Tutorials Knowledge Base	Terms of Service Privacy Policy Add Associated Domains testdomain.com After adding an a	Add Domains Cancel
	<ul> <li>Manage users with the same domain</li> <li>Allow users with the same domain to consolidate into this accout</li> <li>Allow users with the same domain to sign up for Zoom</li> </ul>	nt

////

# 6.2 Verify Domain

The registered domain needs to be verified before it can be used. Use any of the provided methods to verify your domain. Once the domain is verified it will start reflecting as verified.





# 6.3 Register Local Proxy

#### To register the Oracle SBC as Zoom Phone Local Proxy, Navigate to Admin> Phone System Management > Company Info > Account Settings > Proxy

Enter the Oracle SBC FQDN and its Port. Check Mark the Acknowledgement. Click Save and Apply.

Note: Oracle SBC's FQDN or SRV must be resolvable within the internal corporate DNS servers only. These entries must not be resolvable on external DNS servers to let traffic route directly to Zoom servers.

	PLANS & PRICING CONTACT SALES	Enable "Zoom Phone Local Proxy"	REQUEST A DEMO 1.888.799.0125 RESOU
Recordings		Fully Qualified Domain Name (Internal)     Port	
Settings	Multiple Sites Proxy	solutionslab . teamsollab.site v : 5061	
ADMIN	Routing	The Fully Qualified Domain Name (FQDN) entered here must be resolvable in DNS and reachable within the corporate network.	
Dashboard	Desk Phone	<ul> <li>The certificate presented by the proxy server must be signed by a Zoom approved external certificate authority (CA)</li> </ul>	
> User Management	Hours	The FQDN must match the Common Name (CN) or Subject Alternate Name (SAN) of the	network to
> Device Management	Call Park	certificate installed on the proxy server.	
Room Management     Phone System Management	Security Outbound Caller ID	Service Record (Internal)	
Users & Rooms	Template		
Auto Receptionists	Others	<ul> <li>I acknowledge that Nomadic Emergency Services, or Disaster Recovery features may be affected if the proxy server modifies certain custom SIP headers used by Zoom clients. More Details and Impacted features</li> </ul>	
Call Queues Shared Lines		All devices in this SIP Zone will be reset and the new configuration will be applied. Ensure that the proxy server is reachable to avoid service disruption. Incorrect proxy server addresses may cause physical devices to go offline and may require a hard reboot.	
Group Call Pickup			
Phone Numbers		Save and Apply Cancel	
Phones & Devices			unks When
nitoring		SIP trunk status changes, admins can receive email alerts.	and, men

#### Note : Zoom recommends using Port 5091 to be used for the Oracle SBC configured as Local Proxy.

The address(s) discovered in Provisioning information will be used as a Registrar by Oracle SBC which is subjected to change based on your region. There can be more than one registrar in a region.

These Hostnames will be configured as session-agent on the Oracle SBC as shown in <u>Section 7.12</u> of the document.

	ANS & PRICING CONTACT SALES	Multiple Sites SCHEDULE A MEETING JOIN A MEETING HOST A MEET
Settings		
ADMIN	Multiple Sites Proxy	Proxy
Dashboard	Routing	Zoom Phone Local Proxy
> User Management	Notifications	Zoom Phone Local Proxy provides the ability to route traffic from Zoom Phone clients on a corporate network to Zoom data centers through a centralized proxy server. More Details and
> Device Management	Desk Phone	Impacted features
> Room Management	Hours	Proxy Address: solutionslab.teamsollab.site:5061 Edit
<ul> <li>Phone System Management</li> </ul>	Security	Provisioning Information:
Users & Rooms	Outbound Caller ID	gosip01.sc.zoom.us
Auto Receptionists	Audio Prompt	
Call Queues	Template	Routing
Shared Lines	Guidia	
Phone Numbers		BYOC View Routing rules for Bring Your Own Carrier (BYOC)
Phones & Devices		
Company Info		Route Group Manage Route Groups for BYOC. Each Route Group is composed of one or more pre-defined (read-

Note : Devices that are already operational may require a reboot to use the Oracle SBC as Proxy.

# 7. Configuring the SBC

There are two methods for configuring the Oracle SBC - ACLI, or GUI.

For the purposes of this note, we'll be using the OCSBC GUI for all configuration examples. We will however provide the ACLI path to each element. This guide assumes the Oracle SBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, web-server-config has been enabled for GUI access.

If you require more information on how to install your SBC platform, please refer to the ACLI configuration guide.

Note: The document provides instructions to configure the Zoom Proxy only. Besides Zoom Proxy, you may also have Zoom BYOC Agents and/or a Carrier Trunk for termination of PSTN Calls onto the Oracle SBC.Please follow our Application Note Oracle Enterprise Session Border Controller with Zoom Phone (Premise Peering - BYOC) which provides detailed instructions to configure Zoom BYOC.

https://www.oracle.com/a/otn/docs/zoombyocappnote-v1.5.pdf

# 7.1 Configure SBC using Web GUI

To access the OCSBC GUI, enter the management IP address into a web Brower.

#### http://<SBC\_MGMT\_IP>.

When the login screen appears, enter the username and password to access the OCSBC.

Once you have access to the OCSBC GUI, at the top, click the Configuration Tab. This will bring up the OCSBC Configuration Objects List on the left-hand side of the screen.

The Web GUI can be accessed through the URL

	0		
	2	Sign in to E-SBC	
ORACLE	E	Enter your details below Jsername	
Enterprise Session Border Controller	F	l Password	Required
	l		tequired

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



Navigate to Configuration as shown below, to configure the SBC.

			Dashboard	Configuration	Monitor and Trace	Widgets	System
🚯 Wizards 👻	Commands 👻				Save Verify	Discard	Searc
media-manager	•	Configuration Objects					
security	F						
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				*

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.

# 7.2. Configure system-config

To enable system level functionality for the Oracle SBC, you must first enable the system-config

GUI Path: system/system-config ACLI Path: config t→system→system-config

Note: The following parameters are optional but recommended for system config

- Hostname
- Description
- Location
- Default Gateway (recommended to be the same as management interface gateway)
- Transcoding Core (This field is only required if you have deployed a VME SBC)

ORACLE Enterprise	Session Border Controller					admi
			Dashboard Co	nfiguration	Monitor and Trace	Widgets Sy
Wizards 👻 🔯 Commands 👻					Save Verify	Discard
http-client	Modify System Config					Show Configura
http-server network-interface ntp-config phy-interface	Hostname Description	OracleSBC				
redundancy-config snmp-community	Location					
spl-config	Mib System Contact					
system-config	Mib System Name					
tdm-config trap-receiver	Mib System Location Acp TLS Profile	Delare				

Enter the default gateway value in the system config page.

	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 0 - 0 of 0 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	AUU	Delete					
Show All	Ŭĸ	Delete					

# 7.3 NTP-Sync

You can use the following example to connect the Oracle SBC to any network time servers you have in your network. This is an optional configuration but recommended.

GUI Path: system/nap-config ACLI Path: config t>system>ntp-sync

ORACLE Enterprise Session Border Controller							
NN3900-101 10.138.194.136 SCZ9.0.0	GA (Build 54)						
Configuration View Configuration	Q						
media-manager	•	Modify NTP Config					
security	•						
session-router	Þ	Server	216.239.35.0 🗙				

# 7.4 SIP Config

To enable SIP related objects on the Oracle SBC, you must first configure the global SIP Config element:

GUI Path: session-router/SIP-config ACLI Path: config t→session-router→SIP-config

The following are recommended parameters under the global SIP-config:

- home-realm-id
   ZoomCloud
- registrar-domain \* (To allow any domain)
- registrar-host gosip01.sc.zoom.us
- registrar-port 5091
- Options: Click Add, in pop up box, enter the string: inmanip-before-validate
- Click Apply/Add another, then enter: max-udp-length=0
- Click Apply/Add another, then enter reg-cache-mode=from
- Press OK in box

The Values for registrar Host and Port are discovered at the time of Zoom Proxy provisioning in Step 6.3

The home-realm-id is the Zoom Cloud Realm where the Zoom Registrar is located. The values configured here will be used to route the incoming requests from Zoom Endpoints towards Zoom PBX located in ZoomCloud realm.

During Normal registration scenario ,Oracle SBC inserts a Cookie in the Contact Header sent towards the registrar to uniquely identify each registration.Zoom does not want the Oracle SBC to alter any signalling messages sent from the Zoom Phones. In order to achieve this we have used a sip option reg-cachemode=from so that Oracle SBC does not alter the register message by adding the cookie.

More details about several registration handling mechanisms can be found in the <u>Oracle SBC configuration</u> <u>guide</u> on Page 406.

Configuration View Configuration	Q			
Idap-config	Modify SIP Config			
local-policy	State	enable		
local-routing-config	Dialog Transparency			
media-profile	Home Realm ID	ZoomProxy	•	
session-agent	Egress Realm ID		•	
session-group	Nat Mode	None	•	
session-recording-group	Registrar Domain	*		
session-recording-server	Registrar Host gosip01.sc.zoom.us			
session-translation	Registrar Port	5091	(Range:	0,102565535 )
sip-config	Init Timer	500	(Range:	04294967295 )
sip-feature	ОК О	elete		
Idap-config	Modify SIP Config			
local-policy	Enforcement Profile		•	
local-routing-config	Red Max Trans	10000		(Range: 050000)
media-profile	Options	max-udp-length=0 🗙		
session-agent		reg-cache-mode=from )	ĸ	
session-group	SPL Options			
session-recording-group	SIP Message Len	4096		(Range: 065535)

# 7.5. Configure Physical Interface values

To configure physical Interface values , Navigate to -

GUI Path: system/phy-interface ACLI Path: config t→system→phy-interface

Click Add, use the following table as a configuration example:

Here we have configured, Physical Interface s0p1 for Zoom Endpoints and s1p0 for ZoomCloud.

Parameter Name	Zoom Endpoints (s0p1)	Zoom Cloud (s1p0)
Slot	0	1

Port	1	0
Operation Mode	Media	Media

Configure **s0p1** interface as per example shared below.

Configuration View Configuration	Q		
system 💌 🔺	Modify Phy Interface		
host-route	Name	s0p1	
http-client	Operation Type	Media	v
http-server	Port	1	(Range: 05)
network-interface	Slot	0	(Range: 0.2)
ntp-config	Virtual Mac		
phy-interface	Admin State	✓ enable	
redundancy-config	Auto Negotiation	✓ enable	
snmp-community	Duplex Mode	FULL	Y
spl-config	Speed	100	v
system-config	Wancom Health Score	50	(Range: 0.100)
trap-receiver	Network Alarm Threshold		
Show All	OK	lack	

Configure  ${\bf s1p0}$  interface as per example shared below -

onfiguration	Configuration	Q		
media-manager	•	Modify Phy Interface		
security	•			
session-router		Name	s1p0	
ystem	-	Operation Type	Media 💌	
fraud-protection		Port	0	(Range: 05)
host-route	- 1	Slot	1	(Range: 02)
http-client	- 1	Virtual Mac		
http.server		Admin State	✓ enable	
notwork interface		Auto Negotiation	✓ enable	
network-interface		Duplex Mode	FULL 👻	
ntp-config		Speed	100 💌	
phy-interface		Wancom Health Score	50	( Range: 0.100 )
redundancy-config		Network Alarm Threshold		
snmp-community				
spl-config				
system-config	•		Back	
Show All		UK	Back	

# 7.6. Configure Network Interface values

To configure network-interface,

GUI Path: system/network-interface ACLI Path: config t→system→network-interface

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

In this Setup we are using Google Public DNS to resolve the DNS names to IP Addresses.

Parameter Name	Zoom Endpoints	Zoom Cloud
Name	s0p1	s1p0
IP address	10.1.4.4	10.1.2.4
Netmask	255.255.255.0	255.255.255.0
Gateway	10.1.4.1	10.1.2.1
dns-ip-primary	8.8.8.8	8.8.8.8
dns-ip-backup1	8.8.8.4	8.8.8.4
Dns-domain	Domain(if applicable)	Domain(if applicable

Configure network interface s0p1 as below -

Configuration View Configuration	n Q		
media-manager	Modify Network Interface		
security 🕨			
session-router	Name	s0p1 💌	
system	Sub Port Id	0	(Range: 04095)
fraud-protection	Description		
host-route			
http-client	Hostname		
http-server	IP Address	10.1.4.4	
network-interface	Pri Utility Addr		
ntp-config	Sec Utility Addr		
phy-interface	Netmask	255.255.255.0	
redundancy-config	Gateway	10.1.4.1	
snmp-community  Show All	ОК	Back	

////

Similarly, configure network interface s1p0 as below

Configuration Vie	ew Configuration	Q		
media-manager	•	Modify Phy Interface		
security	•			
session-router	•	Name	s1p0	
system	-	Operation Type	Media 💌	
fraud-protection		Port	0	(Range: 05)
		Slot	1	(Range: 02)
host-route		Virtual Mac		
http-client		Admin State	🖌 enable	
http-server		Auto Negotiation	✓ enable	
network-interface		Duplex Mode	FULL 🔻	
ntp-config		Speed	100 🔻	
phy-interface		Wancom Health Score	50	(Range: 0.100)
redundancy-config		Network Alarm Threshold		
snmp-community	-			
Show All		OK	Back	

# 7.7. Enable media manager

To configure media functionality on the SBC, you must first enable the global media manager. Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

GUI Path: media-manager/media-manager ACLI Path: config t→media-manager→media-manager-config

In addition to the above config, please set the max and min untrusted signaling values to one.

Enable Latching if required.

ORACL	_E Enterprise S	Session Border Controller					ĉ
				Dashboard	Configuration	Monitor and Trace	Widgets
🔅 Wizards 💌	🔅 Commands 👻					Save Verify	Discard
media-manager	v	Modify Media Manager	r				
media-manager	r-	State	✓ enable				
media-policy		Flow Time Limit	86400	(Range: 04294967295)			
realm-config		Initial Guard Timer	300	(Range: 04294967295)			
i como		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 Ent	terprise S	Session Border Controller			a
					Dashboard Configura	ation Monitor and Trace Widgets
🔅 Wizards 🔻	🏠 Comm	nands 🔻				Save Verify Discard
media-manager	•	^	Modify Media Manager			
codec-policy media-manage	r		Media Policing	✓ enable	[1000]De on 1211101210 ]	
media-policy			Max Arp Rate Max Signaling Packets	10	(Range: 0.100)	
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: 0.100)	
system	•		Trusted Drop Threshold	0	(Range: 0.100)	
fraud-protection	n		Acl Monitor Window Trap On Demote To Deny	30 enable	( Range: 53600 )	
host-route		~	OK	Delete		
Show All			UN			

# 7.8. Configure Realms

Realms are a logical distinction representing routes (or groups of routes) reachable by the Oracle Session Border Controller and what kinds of resources and special functions apply to those routes.Realms are used as a basis for determining ingress and egress associations to network interfaces.

GUI Path; media-manger/realm-config ACLI Path: config t→media-manger→realm-config

The name of the Realm can be any relevant name according to the user convenience. Use the following table as a configuration example for the three realms used in this configuration.

In this setup we have configured two realms **ZoomEndpoints** and **ZoomCloud**.

ZoomEndpoints realm will be a collection all the Zoom Phones residing on the Access Side of the SBC which will use the Oracle SBC (Zoom Phone Local Proxy) to register onto the Zoom Cloud on the Core side via realm ZoomCloud where the Zoom Registrar is located.

In the test Enviorment Oracle SBC is behind a NAT Device, When SBC are behind NAT Device you may encounter issue of one way Audio or No Audio.

Oracle SBC supports media latching and there are many modes to choose from as mentioned in the <u>Oracle</u> <u>SBC configuration guide</u> on Page 291.

Here we have enabled **symmetric latching** on the ZoomEndpoints Realm which is a latching mode where adevice's source address/ports for the RTP/RTCP it sends to the Oracle SBC that are latched, are then used for the destination of RTP/RTCP sent to the device.

Please enable latching only it is requirement in your Environment.

Config Parameter	Zoom Endpoints Realm	Zoom Cloud Realm	
Identifier	ZoomEndpoints	ZoomCloud	
Network Interface	s0p1	s1p0	
Mm in realm	Z	N	
Access Control Trust Level	low	High	
Media Sec policy	ZoomMediaSecurity	ZoomMediaSecurity	
symmetric-latching	enabled		

# 7.8.1 Realm ZoomEndpoints

Configuration View Configuration	Q			
media-manager 🔹		Modify Realm Config		
codec-policy				
media-manager		Identifier	ZoomEndpoInts	
media-policy		Description		
realm-config				
steering-pool		Addr Prefix	0.0.0.0	
security 🕨		Network Interfaces	s0p1:0.4 🗙	
session-router		Media Realm List		
system 💌				
fraud-protection		Mm In Realm	✓ enable	
host-route		Mm In Network	✓ enable	
http-client		Mm Same Ip	✓ enable	
http-server		QoS Enable	enable	
network-Interface		Max Bandwidth	0	(Range: 0999999999)
ntp-config		Max Priority Bandwidth	0	( Range: 0.999999999 )
phy-interface		DNS Dealm	•	
redundancy-config	-	miser ceru	•	
Show All		OK	ack	

Configuration View Configuration Q			
media-manager 💌 🍝	Modify Realm Config		
codec-policy			
media-manager	Media Sec Policy	ZoomMediaSecurity	
media-policy	RTCP Mux	enable	
realm-config	Ice Profile		
steering-pool	Teams Fqdn		
security >	Teams Fqdn In Uri	enable	
session-router	SDP Inactive Only	enable	
system 💌	DTLS Srtp Profile		
fraud-protection	Srtp Msm Passthrough	enable	
host-route	Class Profile		
http-client	In Translationid		
http-server	Out Translationid		
network-Interface	In Manipulationid		
ntp-config	Out Manipulationid		
phy-Interface	Average Rate Limit	0	(Range: 04294967295)
redundancy-config	Access Control Trust Level	low	
Show All	ОК	Back	

# 7.8.2 Realm ZoomCloud

Configuration	View Configuration	Q		
media-manager	<b>▼</b> ^	Modify Realm Config		
codec-policy				
media-manager		Identifier	ZoomCloud	
media-policy		Description		
realm-config				
steering-pool		Addr Prefix	0.0.0.0	
security	<b>F</b>	Network Interfaces	s1p0:0.4 🗙	
session-router		Media Realm List		
system	-			
fraud-protection		Mm In Realm	✓ enable	
host-route		Mm In Network	✓ enable	
http-client		Mm Same Ip	✓ enable	
http-server		QoS Enable	enable	
network-interface		Max Bandwidth	0	(Range: 0999999999)
nto-config Show All	•	May Priority Randwidth	Back	í <u>-</u>
SHOW All				

Configuration View Config	uration Q			
media-manager	•	Modify Realm Config		
codec-policy				
media-manager		Media Sec Policy	ZoomMediaSecurity	
media-policy		RTCP Mux	enable	
realm-config		Ice Profile		
steering_pool		Teams Fqdn		
security		Teams Fqdn In Uri	enable	
seconcy		SDP Inactive Only	enable	
session-router		DTLS Srtp Profile		
system	•	Srtp Msm Passthrough	enable	
fraud-protection		Class Profile	Chubic	
host-route		to Translationid	•	
http-client		in Translationid		
http-server		Out Translationid		
network-Interface	- 11	In Manipulationid		
ntp-config		Out Manipulationid		
nhv-Interface		Average Rate Limit	0	(Range: 04294967295)
programmer race		Access Control Trust Level	high 👻	
redundancy-config	*	ОК	ack	
Show All				

The Access Control Trust Level is set to Low on the Access Side and set to high on the Core Side as per the Best Pratice in an Access Core Environment.

https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/security/security-guide.pdf

## 7.9. SIP Security Configuration

## 7.9.1 Configuring Certificates

This section describes how to configure the Oracle SBC for communication with Zoom Phones and Zoom Cloud. The communication between the Oracle SBC with Zoom Phones and Zoom Cloud is **TLS/SRTP**.

Using TLS requires a certificate signed by one of the trusted Certificate Authorities.

"Certificate-records" are configuration elements on Oracle SBC which captures information for a TLS certificate such as common-name, key-size, key-usage etc.

The section walks you through how to configure certificate records, create a certificate signing request, and import the necessary certificates into the SBC's configuration.

GUI Path: security/certificate-record ACLI Path: config t→security→certificate-record

For the purposes of this application note, we have created below certificate records. You may choose to create the certificates as per your Setup requirements.

#### SBC Certificate and its CA Certificates-

- SBC Certificates (end-entity certificates)
- DigiCert Root CA
- DigiCert Intermidiate Cert (this is optional only required if your server certificate is signed by an intermediate)
- GodaddyCertBundle

For communication with Zoom Cloud,Oracle SBC also validates Zoom Certificates. Zoom provides certificates signed by DigiCert that needs to imported onto the SBC as a trusted Root CA Certificate. The follow certificates must be installed onto the SBC to trust the TLS Certificate provided by Zoom for TLS negotiation. DigiCert TLS Certificates can be downloaded at below Links.

https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem https://cacerts.digicert.com/DigiCertGlobalRootG3.crt.pem

#### Supported CAs for Zoom Phone.

https://support.zoom.us/hc/en-us/articles/360056087612-Zoom-Phone-certificate-update

Below Table 1 is for reference. Modify the configuration according to the certificates in your environment.

Config Parameter	SBCCertifi cateforZoo mCloud	SBCCertifi cateforZoo mProxy	GoDaddy Certificate Bundle	DigiCert Root CA	DigiCert Intermediat e	DigiCertGl obalRootG 2	DigiCertGI obalRootG 3
Name	SBCCe rtificatef orZoom Cloud	SBCCe rtificatef orZoom Proxy	Godadd yCertB undle	DigiCer t Global Root CA	DigiCer t SHA2 Secure Server CA	DigiCe rt Global Root G2	DigiCe rt Global Root G3
Commo n Name	telechat .o- test061 61977.c om	teamsol lab.site	Go Daddy Root Certific ate Authorit y - G2 Go Daddy Secure Certific ate Authorit y - G2	DigiCer t Global Root CA	DigiCer t SHA2 Secure Server CA	DigiCe rt Global Root G2	DigiCe rt Global Root G3
Key Size	2048	2048	2048	2048	2048	2048	2048
Key- U	digitalSi gnature	digitalSi gnature	digitalSi gnature	digitalSi gnature	digitalSi gnature	digitalSi gnature	digitalSi gnature
S	keyEnci	keyEnci	keyEnci	keyEnci	keyEnci	keyEnci	keyEnci

| a<br>g<br>e<br>-<br>Li                  | pherme<br>nt   |
|---|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| st<br>Extende<br>d Key<br>Usage<br>List | serverA<br>uth |
| Key<br>algor                            | rsa            |
| Digest-<br>algor                        | Sha256         |

# 7.9.1.1 End Entity Certificate

In this setup we have created two end entiity (SBC certificates)."SBCCertificateforZoomCloud" is used for communication with Zoom Cloud and "SBCCertificateforZoomProxy" is used for communication with Zoom Endpoints. This is not necessary and you may use single certificate for both Zoom Proxy and Zoom Cloud.

We have signed "SBCCertificateforZoomCloud" by DigiCert and "SBCCertificateforZoomProxy" by GoDaddy. You may choose any of the Zoom approved CAs to sign your TLS certificates.

As per security requirement from Zoom, The Oracle SBC certificate presented to Zoom Endpoints **must have SBCs FQDN present in the common name** otherwise TLS communication will be unsuccesful.

The certificate must be signed by any of the Zoom Approved Certificate Authorities.

In this setup we used -

Common name: (teamsollab.site) for Zoom Proxy Certificate

Common name: (telechat.o-test06161977.com) for ZoomCloud Certificate

#### Step 1 Configure SBC Certificate Record

To Configure the certificate record:

• Click Add, and configure the SBC certificate as shown below:

Configuration	View Configuration	Q		
media-manager	►	Modify Certificate Record		
security	•			
authentication-pr	ofile	Name	SBCCertificateforZoomCloud	
certificate-record		Country	US	
tls-global		State	California	
tls-profile		Locality	Redwood City	
session-router	►	Organization	Oracle Corporation	
system	►	Unit	Oracle CGBU-LABS BOSTON	
		Common Name	telechat.o-test06161977.com	
		Key Size	2048 🔻	
		Alternate Name		
Show All		ОК В	lack	

Similarly create another certificate record for Zoom Proxy.

Configuration Vie	w Configuration	Q		
media-manager	•	Modify Certificate Record		
security	•			
authentication-profile		Name	SBCCertificateforZoomProxy	
certificate-record		Country	US	
tls-global		State	Texas	
tls-profile		Locality	Austin	
session-router	•	Organization	Oracle America	
system	•	Unit	Oracle CGBU-LABS BOSTON	
		Common Name	teamsollab.site	
		Key Size	2048 💌	
		Alternate Name		
Show All		OK	Back	

# Step 2 – Generating a certificate signing request

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.
- The Step must be performed for both Certificate records SBCCertificateforZoomCloud and SBCCertificateforZoomProxy
- Please copy/paste the text that is printed on the screen as shown below and upload to your CA server for signature.

Configuration View C	Configuration	Q									
media-manager	×.	Certific	ate Re	ecord							
security	•										
authentication-profile											
certificate-record		D; t	t 1	*	Edit		6 🖞 🖽				Sei
		Action	Sel	Name	Сору		itry	State	Locality	Organization	Unit
tls-global					Delete						
tls-profile		:		DigiCertRoc	Generate			MA	Burlington	Engineering	
session-router	•	:		GodaddyCe	Import			МА	Burlington	Engineering	
system	•	:	<ul><li>✓</li></ul>	SBCCertifica	Sort	<b></b>		California	Redwood City	Oracle Corporation	Oracle CGE
		:		SBCCertifica	teforZoo	US		Texas	Austin	Oracle America	Oracle CGE
		:		WebServerIn	istance	US		California	Redwood City	Oracle Corporation	Oracle CGE
		4									
Show All		Displayin	g 1 - 7 of	7							

🚯 Wizards 👻		Concepto entificato economo		Save Verify
media-manager  security  authentication-profile certificate-record tis-global tis-profile	Certificate Record Add Delete Name DigiCertinter DigiCertRoot	Connected certificate response         X           Copy the following information and send to a CA authority	iit	Search Common Name DigiCert SHA2 Secure Server CA DigiCert Global Root CA
session-router	GoDaddyInter GoDaddyRoot	AQEAZINGV22WL2DhqTUFE020qL70fgALEUx2hyOVJR84HmY8BR0Vb0/mih754 4TzmgpNUrg069GRQF2F2BE1KRI/W1be1kg20dGREIBR5Gncn0UElSkriFHV rk490fsK4NeyV45BK50cgx/UL5LUXCT/W0kl7L2EBBK6h2QCS/rk1AbH//UL1h x2brp2VImP5Demc-K02AE0BCT(V)dGPAECEdpU-40AAA43pc170fRcFE6Dh+		GoDaddy Secure Server CA GoDaddy Class2 Root CA
system v fraud-protection host-route http-client http-server	SBCEnterpriseCert	sGH84T=L34CSU7VEtYouUHIQLPg1b0ItELyp5pCRvLfufx8UR03mee8+lCuhPI FWIS96L60UH/W20AmPH0W== END CERTIFICATE REQUEST		telechat.o-test06161777.com
network-Interface		Close		
phy-interface	Page 1 of 1 (1-5 of 5 i	items) R < 1 > X		

- copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, a save and activate is required before you can import the certificates to each certificate record created above.
- Repeat the Step for the other SBC Certificate, SBCCertificateforZoomProxy.

#### Step 3 Import Certificates to the SBC

Once certificate signing request have been completed – import the signed certificate to the SBC.

Note : All certificates including root and intermediate certificates are required to be imported to the SBC. Once all certificates have been imported, issue **save/activate** from the WebGUI

Configuration	View Configurat	tion	L							DI	scard 😟 Verify	🖹 Save
media-manager		►	Contific	ata Da	read							
security		•	Certific	ale Re	cora							
authentication-p	profile											
certificate-record	rd		D t	<u>t</u> 1	🛃 🗵 PKCS12 🖉 🔓	i 🗇 🖪	Ľ			Search		Q
tis-global			Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name	
tis profile			:		BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberT	rust Root
session-router		•	:		DigiCertInter	US	МА	Burlington	Engineering		DigiCert SHA2 Se	cure Ser
system		•	:		DigiCertRoot Copy	US	МА	Burlington	Engineering		DigiCert Global R	oot CA
			:		GodaddyCertBurdle Generate	US	МА	Burlington	Engineering		gd_bundle-g2-g1	
			:		SBCCertificateforClc	US	California	Redwood City	Oracle Corporation	Oracle CGBU-LABS BOST	telechat.o-test06	161977.c
			:	~	SBCCertificateforZoumProxy	US	Texas	Austin	Oracle America	Oracle CGBU-LABS BOST	teamsollab.site	
			:		WebServerInstance	US	California	Redwood City	Oracle Corporation	Oracle CGBU-LABS BOST	telechat.o-test06	161977.c
media-manager	r	Þ	<b>^</b>	Ce	rtificate Record		Import certil	icate		×		
security		~		Ce	runcate Record		import certi	Cate		*		
authenticatio	n-profile						Format			v.		
					Add Delete All	Upload		pkcs				
certificate-rec	cord			1	Name	Country	Import method	x509 trv-all			Unit	Common
tls-global				0	DiglCertInter	US		Paste				DigiCert S
tls-profile				C	DigiCertRoot	US	Certificate file	A Haland	No file chosen.			DigiCert G
session-router		►		(	GoDaddyInter	US						GoDaddy
system		-		(	GoDaddyRoot	US						GoDaddy
					Joe Chier prisedent	05						tercenter.o
traud-protect	tion											
host-route												
http-client												
http-server								Import Car	ncel			
network-Inter	rface											
ntp-config												

## 7.9.1.2 Import Root CA Certificates.

Repeat the steps provided Step 3 to import all the root and intermediate CA certificates into the SBC as mentioned in Table 1.

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

Configuration	View Configuration	Q									Discard	😧 Verify  🖺 Sa
media-manager	•	Certific	ate Re	ecord								
security	•											
authentication-pr	rofile			T	IN DKCS12	ß	6 8 9				Search	0
certificate-record		Li	یل <u>با</u>	News	PRC512	6		E.	L = == <sup>10</sup> te -	Orregiantian	Search	Common Name
tls-global		Action	Sel	Name		Coun	ry	State	Locality	Organization	Unit	Common Name
tls-profile		:	~	DigiCertR	oot	US		MA	Burlington	Engineering		DigiCert Global Ro
session-router	•	:		Godaddy	Edit <sup>Cer</sup> Copy			МА	Burlington	Engineering		gd_bundle-g2-g1
system	•	:		SBCCertif	ical Delete			California	Redwood City	Oracle Corporation	Oracle CGBU-LABS B	telechat.o-test0610
		:		SBCCertif	ical Import	te		Texas	Austin	Oracle America	Oracle CGBU-LABS B	teamsollab.site
		:		WebServe	Sort	•		California	Redwood City	Oracle Corporation	Oracle CGBU-LABS B	telechat.o-test061
		4	1									Þ

🚯 Wizards 👻	nds 💌						
media-manager	•	Certificate Record		Import certificate	×		
security				Format			
authentication-profile					▼ pkcs		
certificate-record		Add Delete All	Upioad		x509		
the clobal		Name	Country	Import method	try-all	Unit	Commo
riz-Biopai		DigiCertinter	US		Paste		DigiCert
tls-profile		DigiCertRoot	US	Certificate file	No file chosen.		DigiCert
session-router		GoDaddyInter	US				GoDadd
		GoDaddyRoot	US				GoDadd
system		SBCEnterpriseCert	US				telechat
fraud-protection							
host-route							
http-client							
http-server					Import Cancel		
network-Interface							
ntp-config							

# 7.10. TLS-Profile

A TLS profile configuration on the SBC allows specific certificates to be assigned.

GUI Path: security/tls-profile ACLI Path: config t→security→tls-profile

In this setup we created two tls profiles TLSZoomEndpoints for Zoom Endpoints and TLSZoomCloud for Zoom Cloud.

# 7.10.1 TLS-Profile - TLSZoomEndpoints

Configure the TLSZoomEndPoints TLS Profile as per below details.

End Entity Certificate-SBCCertificateforZoomProxy

Mutual Authentication-Disabled.

Mutual Authentication is set to disabled as this TLS Profile is for Access Endpoints and Server Auth TLS Negotiaton Method is used.

Configuration View Co	onfiguration	Q		
media-manager	•	Modify TLS Profile		
security	•			
authentication-profile		Name	TLSZoomEndpoints	
certificate-record		End Entity Certificate	SBCCertificateforZoomProxy 🔹	
tls-global		Trusted Ca Certificates	GodaddyCertBundle 🗙	
tls-profile			BaltimoreRoot 🗙	
			DigiCertRoot 🗙	
session-router	•		DigiCertInter 🗙	
system	•	Cipher List	DEFAULT X	
		Verify Depth	10	(Range: 010)
		Mutual Authenticate	enable	
Show All		ОК Е	Back	

# 7.10.2 TLS-Profile - TLSZoomCloud

End Entity Certificate-SBCCertificateforZoomCloud

Mutual Authentication-Enabled

Trusted Ca Certificates- Zoom CA Certificates

As mentioned above For communication with Zoom Cloud,Oracle SBC also validates Zoom Certificates. Zoom provides certificates signed by DigiCert that needs to imported onto the SBC as a trusted Root CA Certificate onto the Zoom Cloud TLS Profile.

https://support.zoom.us/hc/en-us/articles/360056087612-Zoom-Phone-certificate-update

Configuration View C	Configuration	Q		
media-manager	•	Modify TLS Profile		
security authentication-profile	•	Name	TLSZoomCloud	
certificate-record		End Entity Certificate	SBCCertificateforZoomCLoud	
tls-global		Trusted Ca Certificates	BaltimoreRoot 🗙	
tls-profile			DigiCertRoot X	
session-router system	•	Cipher List	DEFAULT X	
		Verify Depth	10	(Range: 010)
		TLS Version	✓ enable tlsv12 ▼	
Show All		ОК	Back	

# 7.11. Configure SIP Interfaces

The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages

GUI Path: session-router/SIP-interface ACLI Path: config t→session-router→SIP-interface

## 7.11.1 Sip-Interface for Zoom Endpoints

Since the ZoomEndPoints realm is configured to handle registrations the following parameter should be enabled on this realm to allow SBC to cache the registrations on this sip-interface.

```
nat-traversal - always registration-caching – enabled
```

route-to-registrar – enabled (Optional) allow-anonymous -registered (To allow traffic from registered endpoints only) HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4

route-to-registrar forwards the requests from Zoom Phones towards the registrar IP Address and Port configured in the sip-config Section of the document. Alternatively, a local-policy configuration can also be used in case route-to-registrar is not configured.

Allow anonymous field on the Zoom Endpoints facing sip-interface should be set to registered to allow traffic only from registered endpoints.

Since this SBC is behind a NAT Device the header NAT SPL Plugin is configured on the sip-interfaces. The functionality of header NAT SPL is mentioned in <u>Section 7.16</u> of the document.

Configuration	0									Discord	A startly D care
Configuration View Configuration	Q									Discard	O Verity 🔡 Save
account-config	Modify	/ SIP In	nterface								Show Configuration
filter-config	State			🗸 enable							A
Idap-config	Realm ID			ZoomEndpoin	its v						
local-policy	Descriptio	'n									
local-routing-config											
media-profile											
session-agent	SIP Ports										
session-group	D	/	ā ā								
session-recording-group	Action	Select	Address		Port	Transport	Protocol	TLS Profile	Allow Anonymous	Multi Home Add	drs
session-recording-server	:		10.1.4.4		5061	TLS		TLSZoomEndpoints	registered		
session-translation											
sip-config											
sip-feature											
sip-interface											•
	tion O										
filter-config											
Idap-config	-	Modi	ify SIP Interf	ace							
local-policy		Nat Tra	iversal		always	•					
local-routing-config		Nat Int	erval		30		(Range: 042949	067295)			
local-locality-comp		TCP Na	ut Interval		90		(Range: 042949	067295)			
media-profile		Registr	ation Caching		enable			,			
session-agent		Min Re	g Expire		700		( Panger 0, 00000	00000			
session-group		Registr	ration Interval		300		(Range: 0. 42040	(7777)			
session-recording-group		Route 1	To Registrar		3600		( Kguße: 0"45A4A	07295)			
session-recording-server		Secure	d Network								
session translation			- Di-		enable						
session-translation		Uri Fqd	in Domain								
sip-config		Option	S								
sip-feature		SPL Op	utions		HeaderNatPublicSipIfIp=	20.65.42.129,1					
sip-interface		Trust N	fode		all						
sip-manipulation		Max Na	at Interval		3600		(Range: 0, 42949	067205 )			
sip-monitoring	-				5500		( 1001 Ber 0142 343				
Show All				ОК	Back						

1/11

# 7.11.2 Sip-Interface for Zoom Cloud

Similarly configure the sip interface for Zoom Cloud as shown below.

Allow anonymous field on the Zoom Cloud facing sip-interface should be set to agent-only to allow traffic only from the network entities defined as agents for security purpose.

Configuration View Configuration	ς							Discard 🖉 Verify	🖹 Save
account-config	Modify	SIP In	iterface					Show Conft	guration
filter-config	State		🗸 enable						-
ldap-config	Realm ID		ZoomCloud	<b>.</b>					
local-policy	Descriptio	n							- 1
local-routing-config									
media-profile									
session-agent	SIP Ports	1	<b>7</b> 页						
session-group	L.	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs	
session-recording-group	:		10.1.3.4	5061	TLS	ZoomProxyTLSProfile	agents-only		
session-recording-server									
session-translation									
sip-config									
sip-feature									
sip-interface									*

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 path.

GUI Path: session-router/session-agent ACLI Path: config t→session-router→session-agent

Configure the session-agents for the Zoom Cloud as below.

- Host name should match the registrar address discovered at the time of setting up proxy in <u>section 6.3</u>
- port to 5091
- realm-id needs to match the realm created for the Zoom Cloud
- transport set to "statists"
- ping-method send OPTIONS message to Zoom for check health
- ping-interval to 30 secs

Repeat the Step above to create other session-agents if you have more than One Registrars discovered at the time of Proxy configuration.

	-		
Configuration View Configuration	2		
local-routing-config	Modify Session Agent		
media-profile	Hostname	gosip01.sc.zoom.us	
session-agent	IP Address		
session-group	Port	5091	(Range: 0,102565535)
session-recording-group	State	✓ enable	
session-recording-server	App Protocol	SIP	v
session-translation	Арр Туре		v
sip-config	Transport Method	StaticTLS	v
sip-feature	Realm ID	ZoomCloud	•
sip-interface	Egress Realm ID		·
sip-manipulation	Description		
sip-monitoring			
translation-rules	Match Identifier		
system		÷	
Show All	OK	Back	

# 7.13. Configure local-policy

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

GUI Path: session-router/local-policy

ACLI Path: config t→session-router→local-policy

The following local-policy routes the traffic from Zoom Endpoints to Zoom Cloud.

Alternatively, route-to-registrar parameter can be enabled on the sip-interface associated with the Zoom Endpoints

Configuration	View Configurat	ton	2									Discard	Ø Verify	🖁 Save
media-manager	►	<b>^</b>	Modify	Local	Policy									
security	•													*
session-router	•		From Add	ress		* ×								- 1
access-control			To Addres	S		• ×								
account-config			Source Re	alm		ZoomEndpoints 🗙								
filter-config			Descriptio	n										
Idap-config														
local-policy														
local-routing-co	onfig		State		~	enable								
media-profile			Policy Price	rity	n	one								
session-agent			Policy Attr	ibutes										
session-group			D	/	ā ā									
session-recordin	ng-group		Action	Select	Next Hop	Realm	Action	Terminate Recurs	Cost	State	App Protocol	Lookup	Next Key	(
session-recordin	ng-server				gosip01.sc.zoom.us	ZoomProxy	none	disabled	0	enabled		single		
session-translat Show All	tion	•			ОК Вас	:								·



Configuration View Configuration	Q									Discard	Ø Verify	Save
media-manager	Modify	Local	Policy									
security >												<b>A</b>
session-router 👻	From Add	ress		• *								
access-control	To Addres	is		* ×								
account-config	Source Re	alm										
filter-config	Descriptio	'n		SipTrunk X								
Idap-config	Description			Route Calls from Sip Irun BYOC	ik to Zoom							
local-policy												
local-routing-config	State			🗸 enable								
media-profile	Policy Price	ority		none	•							
session-agent	Policy Attr	ibutes										
session-group	D	1	ā 🖞									
session-recording-group	Action	Select	Next Hop	Realm	Action	Terminate Recurs	Cost	State	App Protocol	Lookup	Next Key	
session-recording-server	:		162.12.233.60	ZoomPhone	replace-uri	disabled	0	enabled		single		-
session-translation  Show All			ОК Ва	ck								

For Zoom Phones enabled with the BYOC Plan, following local-policy routes the calls from the Zoom BYOC Phone to Carrier and then the calls are routed from Carrier to PSTN.

Configuration	View Configura	ation	Q									Discard	🕲 Vertfy	Save
media-manager	Þ	<b>^</b>	Modify	Local	Policy									
security	►													
session-router			From Add	From Address * ×										
access-control			To Addres	is		* x								
account-config			Source Re	alm		ZoomPhone X								
filter-config			Descriptio	n		Deute Celle from Zener D	NOC to Siz							
Idap-config						Trunk	stoc to sip							
local-policy														
local-routing-co	onfig		State			🖌 enable								
media-profile			Policy Price	ority		none	•							
session-agent			Policy Attr	ibutes										
session-group			D	1	ā ā									
session-recordin	ng-group		Action	Select	Next Hop	Realm	Action	Terminate Recurs	Cost	State	App Protocol	Lookup	Next Key	
session-recordin	ng-server		:		68.68.117.67	SipTrunk	none	disabled	0	enabled		single		
session-translat Show All	tion I	*			ОКВ	ack								

The screenshots are for reference. To configure Zoom BYOC with Oracle SBC please refer to this <u>Oracle</u> <u>Application Note</u>.

Configuration View Configuration	Q						Discard	😟 Verify	🕆 Save
media-manager	Modify Local Policy								
security 🕨									
session-router 🗸	From Address	* x							- 1
access-control	To Address	* ×							- 1
account-config	Source Realm	Zoom 🗙							- 1
filter-config	Description								
Idap-config									- 1
local-policy									- 1
local-routing-config	State	🗸 enable							- 1
media-profile	Policy Priority	none	•						
session-agent	Policy Attributes								
session-group	D: 🖉 🗇 🖬								
and a second and a second	Action Select Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	
session-recording-server	: 68.68.117.67	SIPTrunk	none	disabled	0	enabled		single	*
session-translation  Show All	ОК	Back							Ţ

# 7.14. Configure steering-pool

Steering pools define sets of ports that are used for steering media flows through the Oracle SBC.

These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We will configure steering pool for each realm configured.

GUI Path: media-manager/steering-pool

ACLI Path: config t→media-manager→steering-pool

• Click Add, and use the below examples to configure

# 7.14.1 Zoom Endpoints Steering Pool

Configuration	View Configuration	Q			
media-manager	<b>•</b>	Modify Steering Pool			
codec-policy					
media-manager		IP Address	10.1.4.4		
media-policy		Start Port	10000		(Range: 0,165535)
realm-config		End Port	10999		(Range: 0,165535)
		Realm ID	ZoomEndpoints	•	
steering-pool	_	Network Interface		_	
security				•	
session-router					

# 7.14.2 Zoom Cloud Steering Pool

media-manager	<b>•</b>	Modify Steering Pool	Modify Steering Pool							
codec-policy										
media-manager		IP Address	10.1.3.4							
media-policy		Start Port	10000	(Range: 0,165535)						
realm-config		End Port	10999	(Range: 0,165535)						
steering_pool	- 1	Realm ID	ZoomCloud 👻							
Steering-poor		Network Interface	▼							
security										

# 7.15. Media Security Configuration.

This section outlines how to configure support for media security between the ORACLE SBC and Zoom Phone.

# 7.15.1 Configure sdes profile

This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured.

In the SBC's GUI, on the bottom left, you will need to enable the switch "Show All" to access the media security configuration elements.

GUI Path: security/media-security/sdes-profile ACLI Path: config t→security→media-security→sdes-profile

• Click Add, and use the example below to configure

Configuration View C	Configuration	Q	
cert-status-prome			
certificate-record		Modify Sdes Profile	
factory-accounts		Name	ZoomSRTP
ike	•	Crypto List	AEAD_AES_256_GCM 🗙
local-accounts	- 11		AES_256_CM_HMAC_SHA1_80
media-security	•		
dtls-srtp-profile			AES_CM_120_HMAC_SHA1_52 X
media-sec-policy		Srtp Auth	✓ enable
sdes-profile		Srtp Encrypt	✓ enable
sipura-profile		SrTCP Encrypt	✓ enable
password-policy		Mki	enable
security-config		Egress Offer Format	same-as-ingress
ssh-config		Use Ingress Session Params	
ssh-key		Ontions	
tls-global	+	options	
Show All	)	ОК	Back

# 7.15.2. Configure Media Security Profile

Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any) and, if SRTP needs to be used, the sdes-profile that needs to be used

GUI Path: security/media-security/media-sec-policy ACLI Path: config t→security→media-security→media-sec-policy

• Click Add, use the examples below to configure

Create Media Sec policy with name ZoomMediaSecurity, which will have the sdes profile, created above.

The same media policy can be assigned to both <u>ZoomEndpoints and ZoomCloud Realm.</u>

Configuration View Configuration	Q	
cert-status-profile	Modify Media Sec Policy	
certificate-record		
factory-accounts	Name	ZoomMediaSecurity
ike 🕨	Pass Through	enable
local-accounts	Options	
media-security 🔻		
dtls-srtp-profile	▲ Inbound Profile	7
media-sec-policy	Mode	200m5 👻
	Mode	srtp 💌
saes-profile	Protocol	sdes 💌
sipura-profile	Hide Egress Media Update	enable
password-policy	✓ Outbound	
security-config	Profile	ZoomS 💌
ssh-config	Mode	srtp 💌
ssh-key	Protocol	sdes 💌
tis-global 🗸		
Show All	ок	Back

1111111122

2///0

Note- If any of your other network component requires RTP (for Example Carrier Trunk terminated onto the SBC), another Media Sec policy as show below and named **RTP**, to convert srtp to rtp can be created and applied to the appropriate realm as needed.

🔅 Wizards 🔻	iands 🦷	,				
admin-security	►	^	Modify Media Sec Policy			
auth-params			Name	RTP		
authentication			Pass Through	enable		
authentication-profile			Options			
cert-status-profile						
certificate-record			▲ Inbound			
factory-accounts			Profile	•		
			Mode	rtp	•	
ike	►		Protocol	none	-	
ipsec	►		Hide Egress Media Update	enable		
local-accounts						
modia cocucitu			Outbound			
media-security			Profile	-		
dtls-srtp-profile			Mode	rtp	•	
media-sec-policy		-	ок Ва	ack		
Show All						

# 7.16. SBC Behind NAT SPL configuration

This configuration is needed when your SBC is behind a NAT device. This is configured to avoid loss in voice path and SIP signaling. The Support for SBC Behind NAT SPL plug-in changes information in SIP messages to hide the end point located inside the private network. The specific information that the Support for SBC Behind NAT SPL plug-in changes depends on the direction of the call.

For example, from the NAT device to the SBC or from the SBC to the NAT device.

Configure the Support for SBC Behind NAT SPL plug-in for each SIP interface that is connected to a NAT device. One public-private address pair is required for each SIP interface that uses the SPL plug-in, as follows.

- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

Here is an example configuration with SBC Behind NAT SPL config.

To configure SBC Behind NAT SPL Plug in

GUI Path: session-router/sip-interface ACLI Path: config t→session-router→sip-interface

HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4

Here HeaderNatPublicSIPIfIp is the Public interface IP and HeaderNatPrivateSIPIfIp is the Private IP.

More Details about SBC behind NAT SPL can be found on Page 1724 <u>https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/configuration/sbc-</u> configuration-guide.pdf

Configuration View Configuration	۹			Discard Ø Vertfy
session-agent	Modify SIP Interface			Show Con
session-agent-id-rule	Registration Interval Route To Registrar	3600	(Range: 0.4294967295)	
session-constraints	Secured Network	enable		
session-recording-group	Uri Fqdn Domain			
session-recording-server	Options			
session-router	SPL Options	HeaderNatPublicSipIfIp=20.110.144.24		
session-timer-profile session-translation	Max Nat Interval	all v	(Range: 0.4294967295)	
sip-advanced-logging	Stop Recurse	401,407		
sip-config	Port Map Start Port Map End	0	(Range: 0,102565535) (Range: 0,102565535)	
sip-feature	In Manipulationid	·	(	
sip-interface	Out Manipulationid	<b>.</b>		
Show All	ОКВ	ack		

This configuration would be applied to each SIP Interface in the ORACLE SBC configuration that is deployed behind a Nat Device.

# 7.17. Session Timer Profile (Optional)

Zoom Phone does support RFC 4028 Session Timers in SIP. In many cases, RFC 4028 is not supported by carriers providing SIP Trunking services to their customers. To accommodate this, the SBC will interwork between PSTN carrier and Zoom Phone in order to provide support for Session Timers in SIP.

For more information about the Oracle SBC's support for RFC4028, please see the <u>Configuration Guide</u> on page 389

GUI Path: session-router/session-timer-profile ACLI Path: config t→session-router→session-timer-profile

Use the following as an example to configure session timer profile on your Oracle SBC. Some parameters may vary to fit your specific environment.

🔅 Wizards 🔻 🚯 Commands 👻			
rph-profile	<ul> <li>Modify Session Timer Pression</li> </ul>	rofile	
service-health			
session-agent	Name	ZoomSessionTimer	
session-agent-id-rule	Session Expires	900	(Range: 64999999999)
session-constraints	Min Se	90	(Range: 64999999999)
session-group	Force Reinvite	enable	
session-recording-group	Request Refresher	uac	•
session-recording-server	Response Refresher	uac	v
session-router			
session-timer-profile			
session-translation			
slp-advanced-logging			
sip-config			
sip-feature			
sip-feature-caps	•	Back	
Show All			

# 7.18 Caveat -OPUS Transcoding

Opus is an audio codec developed by the IETF that supports constant and variable bitrate encoding from 6 kbit/s to 510 kbit/s and sampling rates from 8 kHz (with 4 kHz bandwidth) to 48 kHz (with 20 kHz bandwidth, where the entire hearing range of the human auditory system can be reproduced). It incorporates technology from both Skype's speech-oriented SILK codec and Xiph.Org's low-latency CELT codec. This feature adds the Opus codec as well as support for transrating, transcoding, and pooled transcoding. Opus can be adjusted seamlessly between high and low bit rates, and transitions internally between linear predictive coding at lower bit rates and transform coding at higher bit rates (as well as a hybrid for a short overlap). Opus has a very low algorithmic delay (26.5 ms by default), which is a necessity for use as part of a low audio latency communication link, which can permit natural conversation, networked music performances, or lip sync at live

events. Opus permits trading-off quality or bit rate to achieve an even smaller algorithmic delay, down to 5 ms. Its delay is very low compared to well over 100 ms for popular music formats such as MP3, Ogg Vorbis, and HE-AAC; yet Opus performs very competitively with these formats in terms of quality across bit rates.

Zoom Phone fully support the use of OPUS but advertises a static value of 40000 for max average bit rate Although the range for maxaveragebitrate is 6000 to 51000, only bit rates of 6000 to 30000 bps are transcodable by the DSPs on the Oracle SBC. A media profile configured with a value for maxaveragebitrate greater than 30000 is not transcodable and cannot be added on egress in the codec-policy element.

The Oracle SBC will however support the entire range of maxaveragebitrate if negotiated between the parties of each call flow.

# ORACLE

#### CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/Oracle/

twitter.com/Oracle

oracle.com

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