



# ORACLE

## Oracle SBC working as Zoom Phone Local Proxy

**Technical Application Note**

**ORACLE**  

---

**COMMUNICATIONS**

## 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>

<b>Version</b>	<b>Description of Changes</b>	<b>Date Revision Completed</b>
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

<b>1 INTENDED AUDIENCE .....</b>	<b>4</b>
<b>2. DOCUMENT OVERVIEW .....</b>	<b>4</b>
2.1 ZOOM PHONE LOCAL PROXY .....	4
<b>3. VALIDATED ORACLE VERSIONS .....</b>	<b>5</b>
<b>4. ZOOM PHONE LOCAL PROXY REQUIREMENTS.....</b>	<b>5</b>
<b>5. NETWORK ARCHITECTURES .....</b>	<b>6</b>
5.1 INTERNAL ZOOM PHONE NATIVE CALLING PLAN USER TOPOLOGY. ....	6
5.1.1 Extension to Extension dialing.....	6
5.2 INTERNAL ZOOM PHONE BYOC USER TOPOLOGY.....	7
5.3 EXTERNAL ZOOM PHONE USER TOPOLOGY .....	8
<b>6. CONFIGURE ZOOM PHONE LOCAL PROXY .....</b>	<b>9</b>
6.1 REGISTER TENANT DOMAIN .....	9
6.2 VERIFY DOMAIN .....	10
6.3 REGISTER LOCAL PROXY .....	11
<b>7. CONFIGURING THE SBC .....</b>	<b>12</b>
7.1 CONFIGURE SBC USING WEB GUI .....	12
7.2. CONFIGURE SYSTEM-CONFIG.....	14
7.3 NTP-SYNC.....	15
7.4 SIP CONFIG .....	16
7.5. CONFIGURE PHYSICAL INTERFACE VALUES .....	17
7.6. CONFIGURE NETWORK INTERFACE VALUES .....	19
7.7. ENABLE MEDIA MANAGER .....	21
7.8. CONFIGURE REALMS.....	22
7.8.1 Realm ZoomEndpoints.....	23
7.8.2 Realm ZoomCloud .....	24
7.9. SIP SECURITY CONFIGURATION .....	25
7.9.1 Configuring Certificates .....	25
7.9.1.1 End Entity Certificate.....	27
7.9.1.2 Import Root CA Certificates. ....	30
7.10. TLS-PROFILE .....	31
7.10.1 TLS-Profile – TLSZoomEndpoints.....	31
7.10.2 TLS-Profile – TLSZoomCloud .....	32
7.11. CONFIGURE SIP INTERFACES.....	33
7.11.1 Sip-Interface for Zoom Endpoints.....	33
7.11.2 Sip-Interface for Zoom Cloud .....	34
7.12. CONFIGURE SESSION-AGENT.....	35
7.13. CONFIGURE LOCAL-POLICY .....	36
7.14. CONFIGURE STEERING-POOL.....	38
7.14.1 Zoom Endpoints Steering Pool.....	38
7.14.2 Zoom Cloud Steering Pool .....	39
7.15. MEDIA SECURITY CONFIGURATION.....	39
7.15.1 Configure sdes profile .....	39
7.15.2. Configure Media Security Profile .....	40
7.16. SBC BEHIND NAT SPL CONFIGURATION .....	42
7.17. SESSION TIMER PROFILE (OPTIONAL).....	43

## 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 ESBC](#)" 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/sbc-configuration-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-controller-ds.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

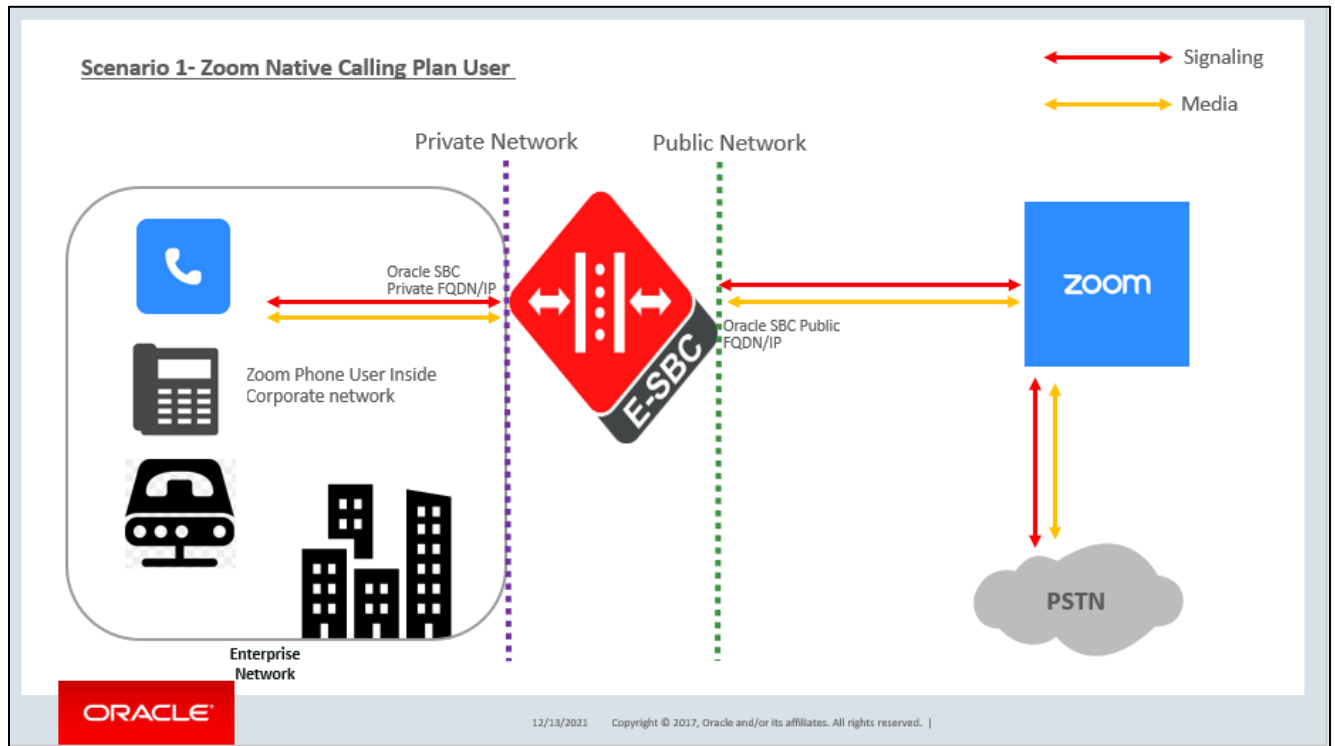
In this section we will cover the Architectures for different Zoom Phone Local Proxy Topologies.

### 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 [Zoom Native Calling Plan](#). Oracle SBC, which is [certified](#) 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

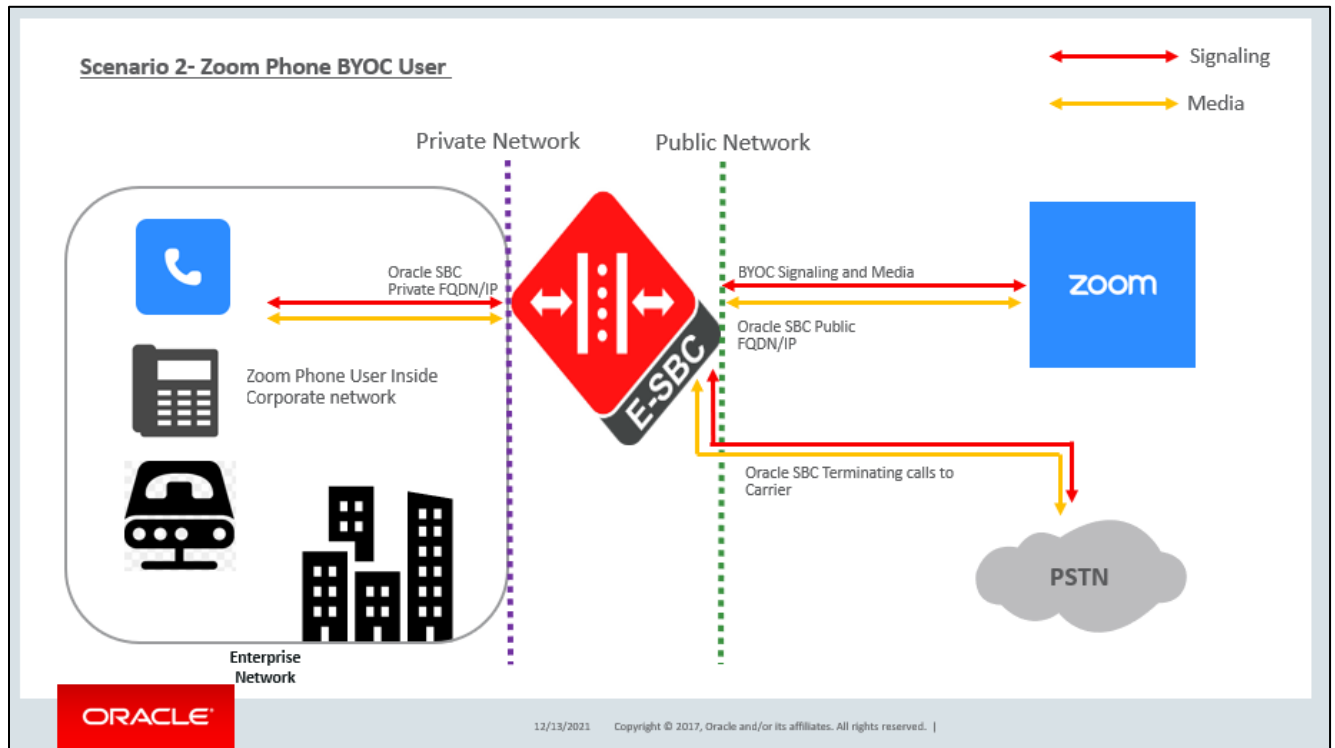
Calls between two internal users (extensions) also traverse through Oracle SBC, Caller Zoom Phone sends the call to Oracle SBC, which is forwarded to the Zoom Cloud after basic B2BUA operations ,the call is returned to the Callee registered behind Oracle SBC. Oracle SBC performs a registration cache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



## 5.2 Internal Zoom Phone BYOC User Topology.

In below scenario Zoom Phones are enabled with the [Zoom BYOC](#) Calling Plans. Oracle SBC, which is [certified](#) 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.

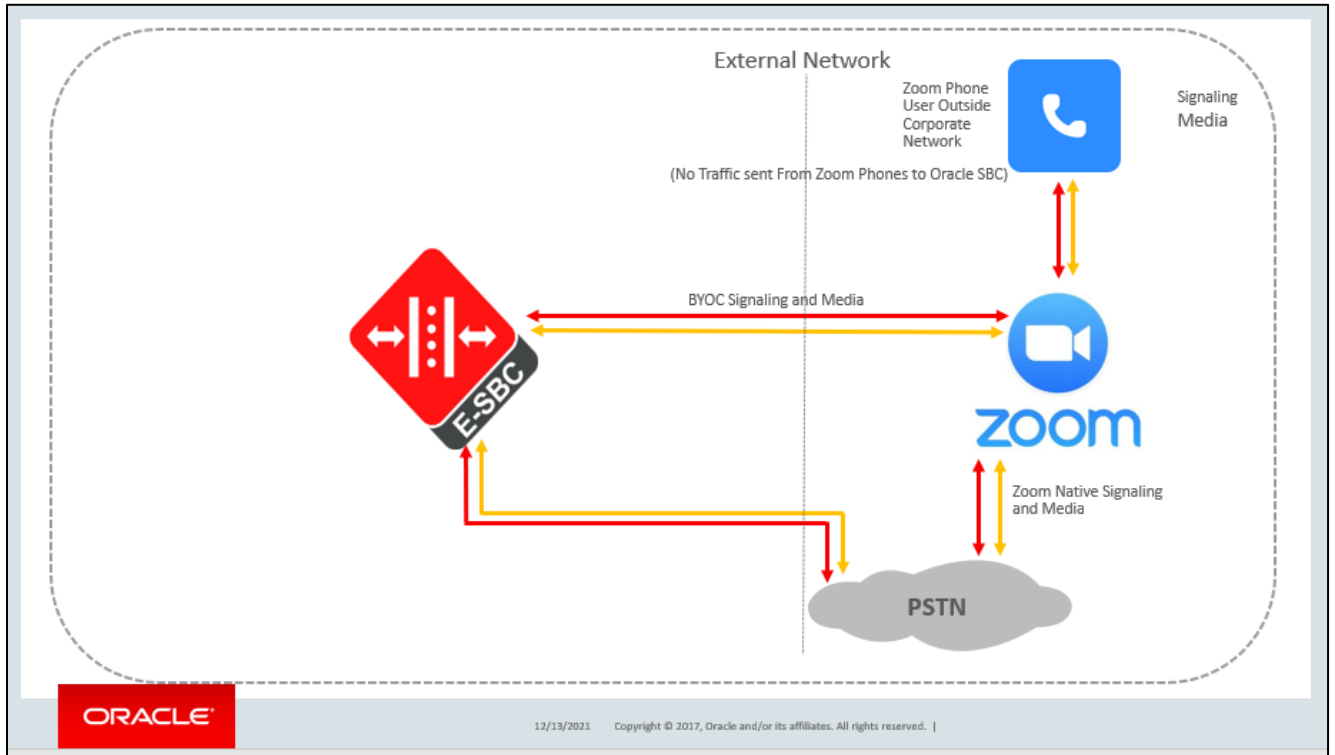
PSTN calls are hair pinned back from Zoom BYOC Endpoints to Oracle SBC which further routes to the appropriate Carrier trunk to terminate onto the PSTN Network.



### 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.





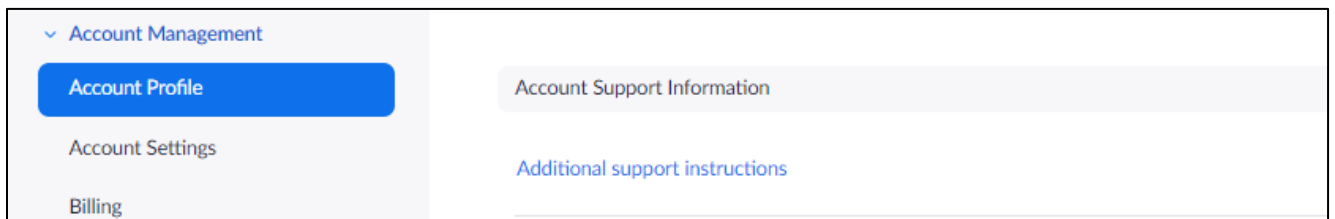
## 6. Configure Zoom Phone Local Proxy

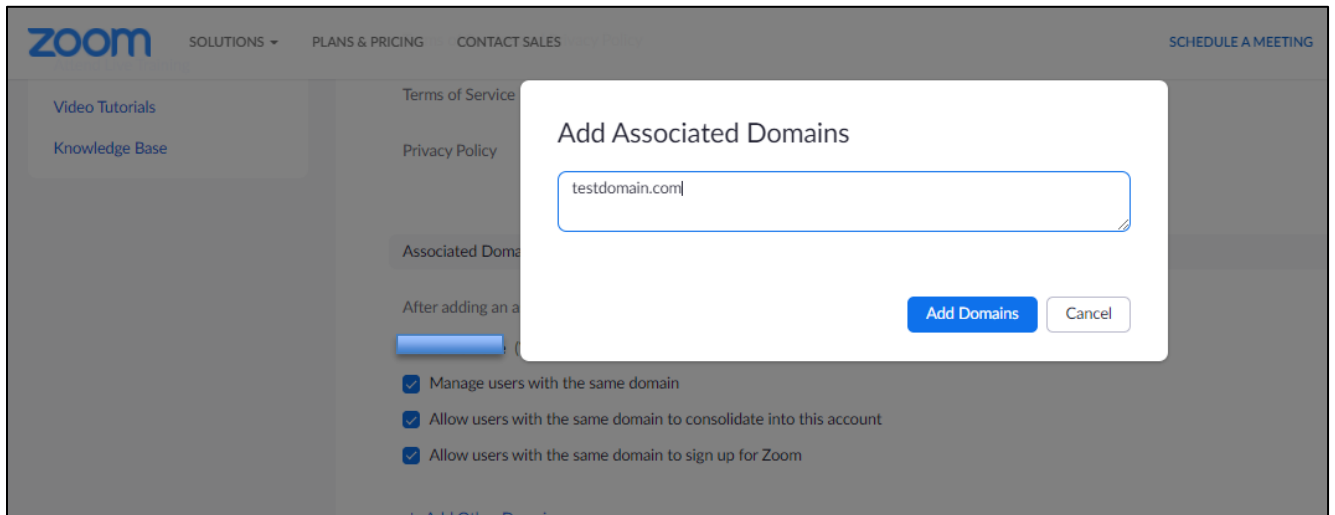
This Section describes the steps to configure the Zoom Phone Local Proxy on the on the Zoom Admin Portal. For detailed assistance with setting up and configuring your Zoom Phone System, please reach out to Zoom Sales: <https://zoom.us/contactsales>

### 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.

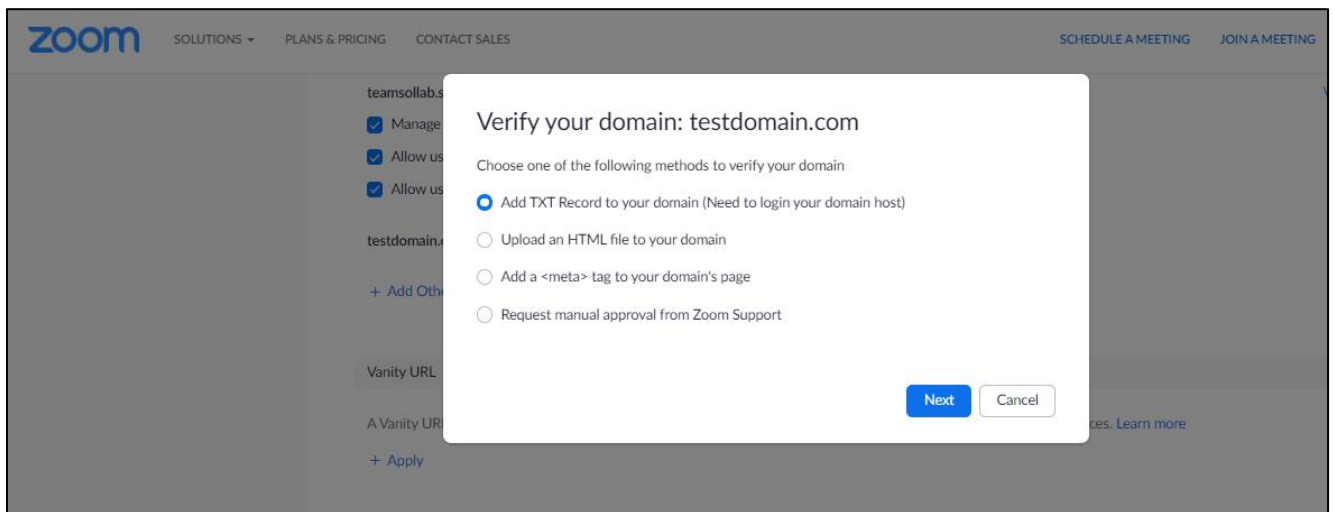
- Navigate to **Admin > Account Management > Account Profile**.
- Scroll Down to look for the Associated domain Section. If the desired domain is not registered
- Click on Add Associated Domain and add your domain.





## 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.



Associated Domains

After adding an associated domain, you can choose to consolidate all users with that domain into one account.

teamsollab.site (Verified) [View User Summary](#)

- Manage users with the same domain
- Allow users with the same domain to consolidate into this account
- Allow users with the same domain to sign up for Zoom

### 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**

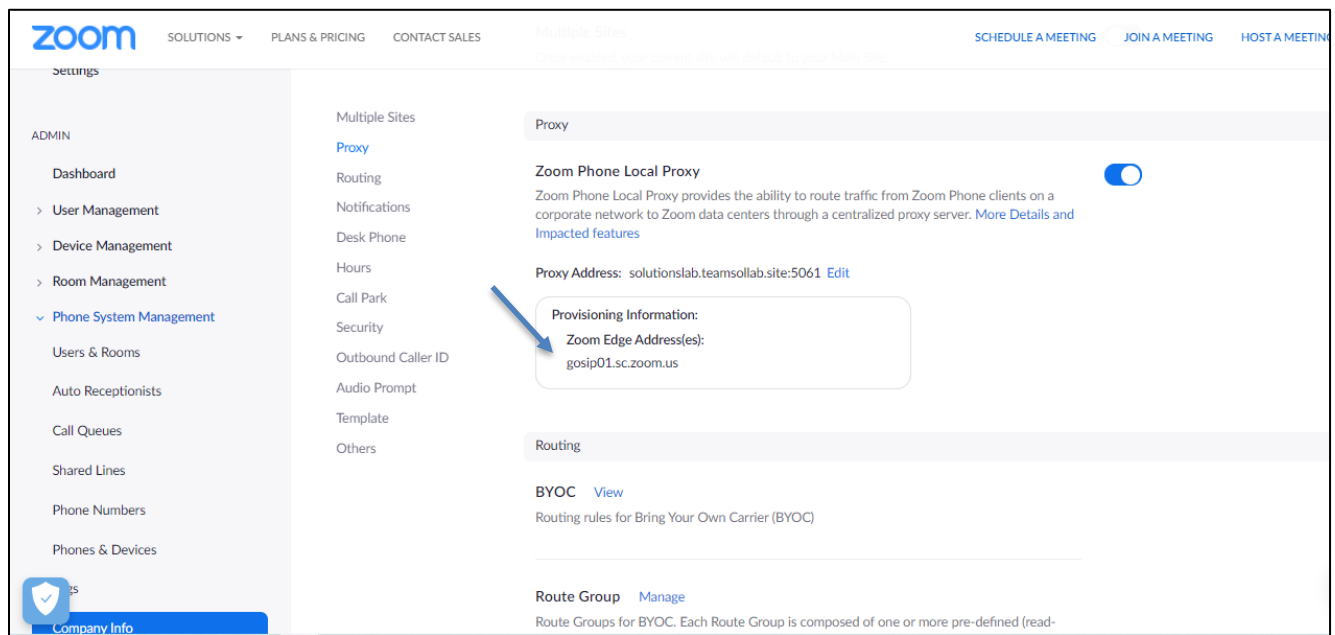
Enter the Oracle SBC FQDN and its Port. Check Mark the Acknowledgement. Click Save and Apply.

**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.

**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 [Section 7.12](#) of the document.



**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 - CLI, or GUI.

For the purposes of this note, we'll be using the OCSBC GUI for all configuration examples. We will however provide the CLI 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 CLI 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/atn/docs/zoombyocappnote-v1.5.pdf>

### 7.1 Configure SBC using Web GUI

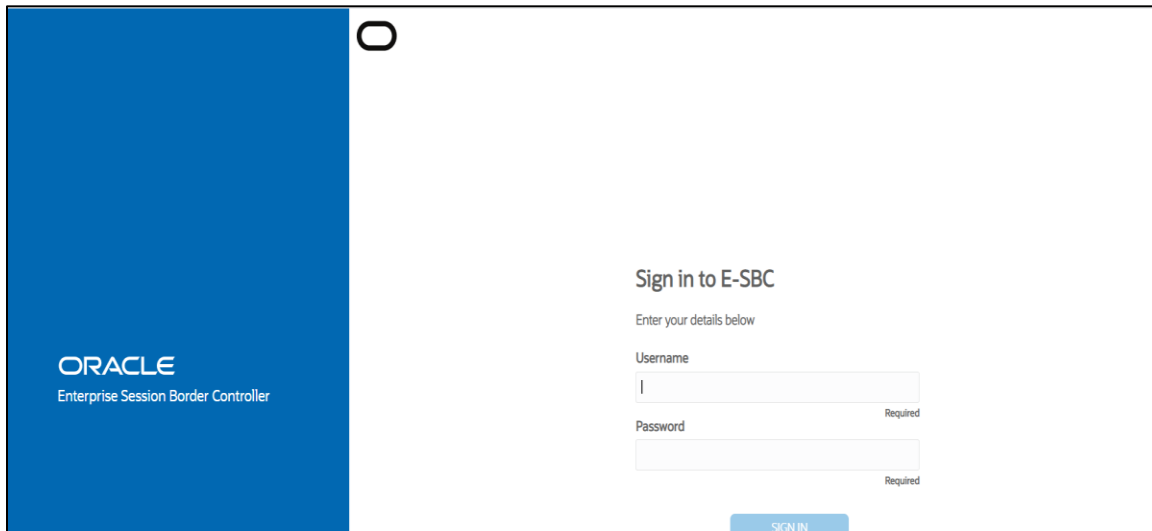
To access the OCSBC GUI, enter the management IP address into a web Browser.

[http://<SBC\\_MGMT\\_IP>](http://<SBC_MGMT_IP>).

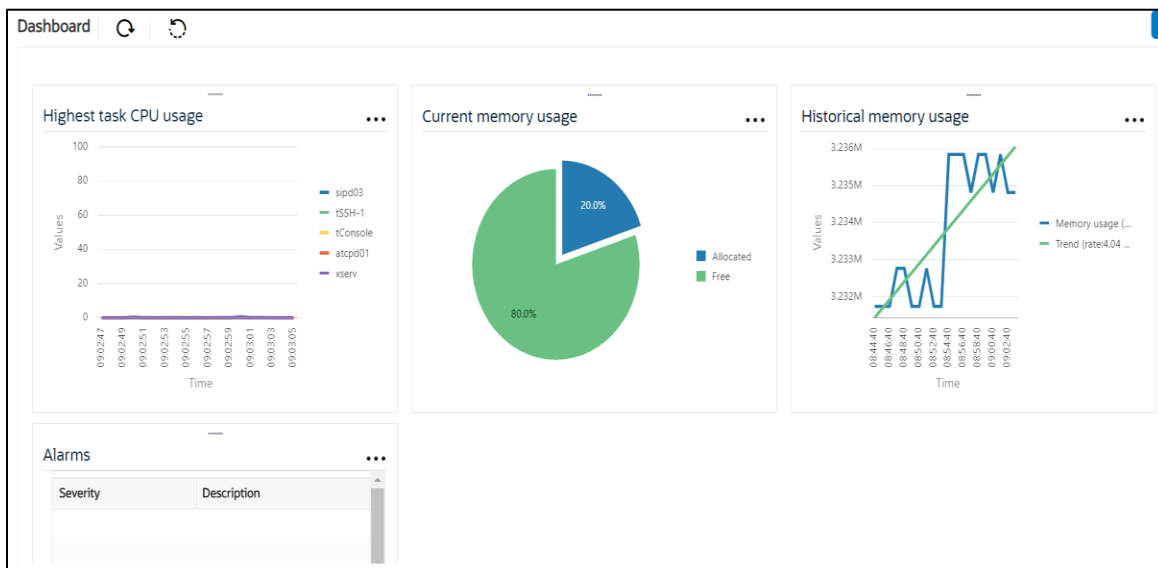
When the login screen appears, enter the username and password to access the OCSBC.

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.

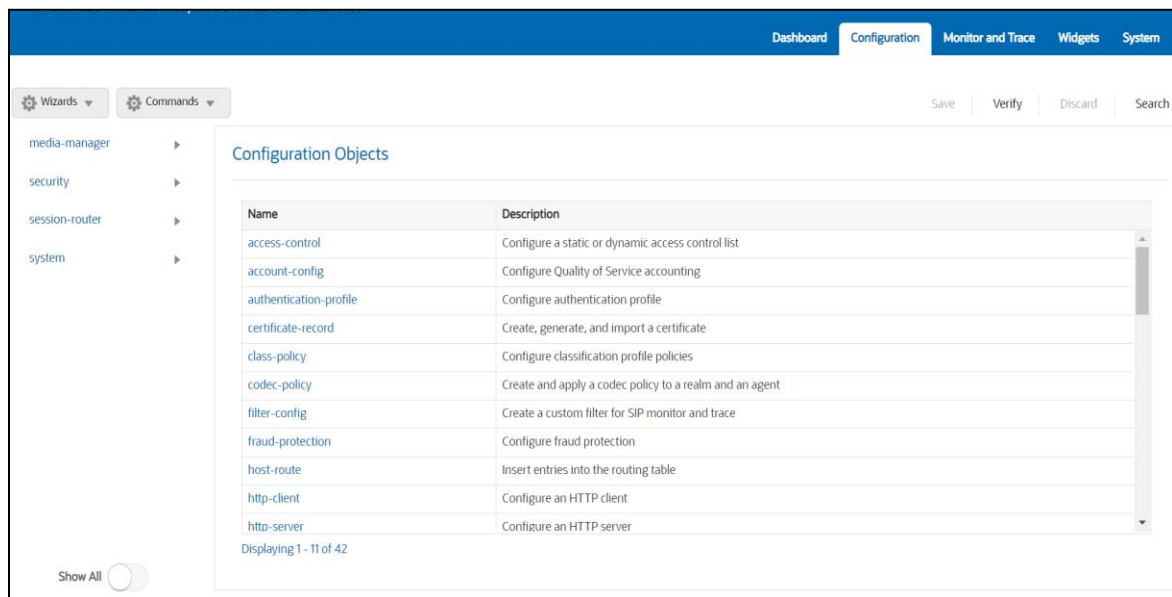
The Web GUI can be accessed through the URL



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



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



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

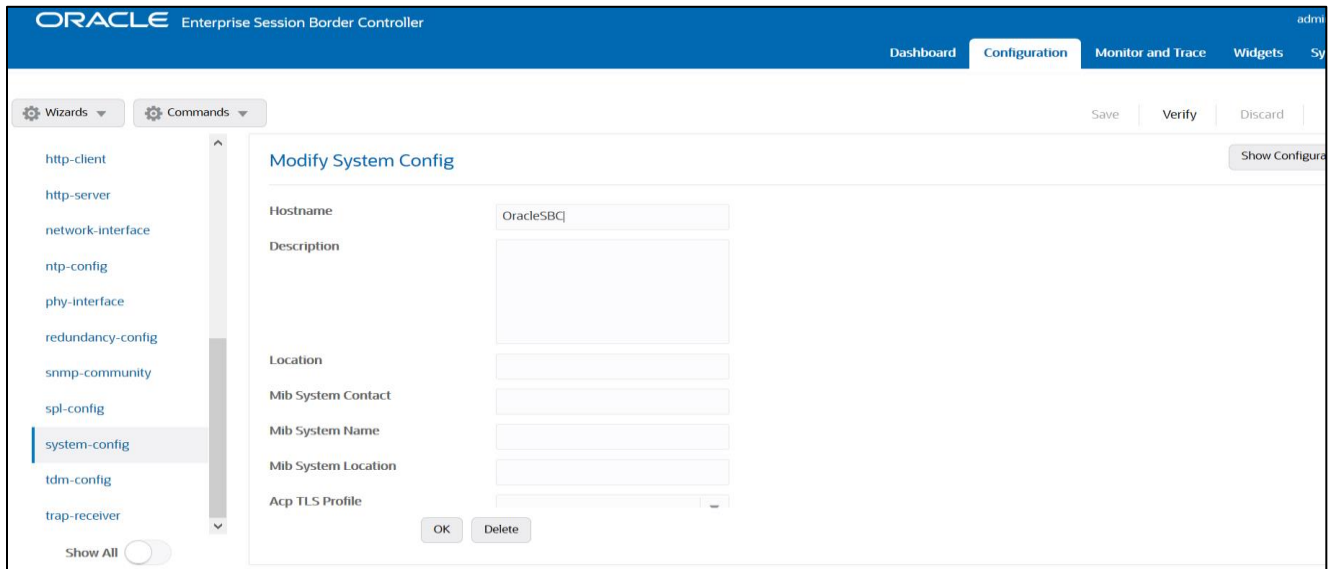
To enable system level functionality for the Oracle SBC, you must first enable the system-config

GUI Path: system/system-config

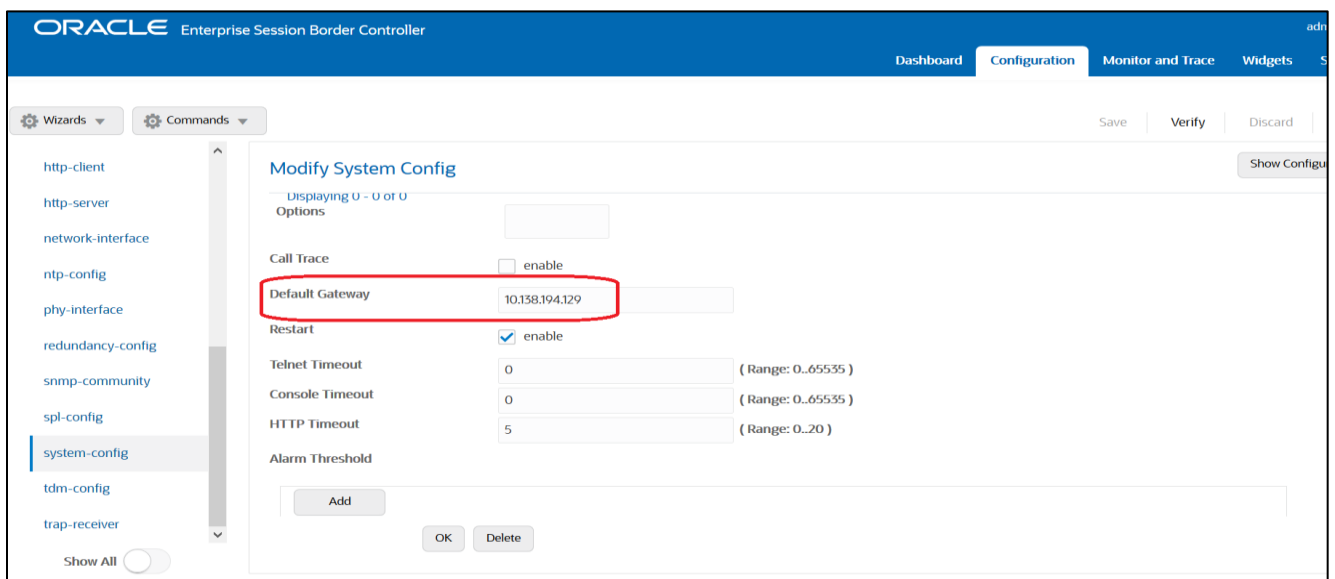
ACLI Path: config t→system→system-config

*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)



Enter the default gateway value in the system config page.

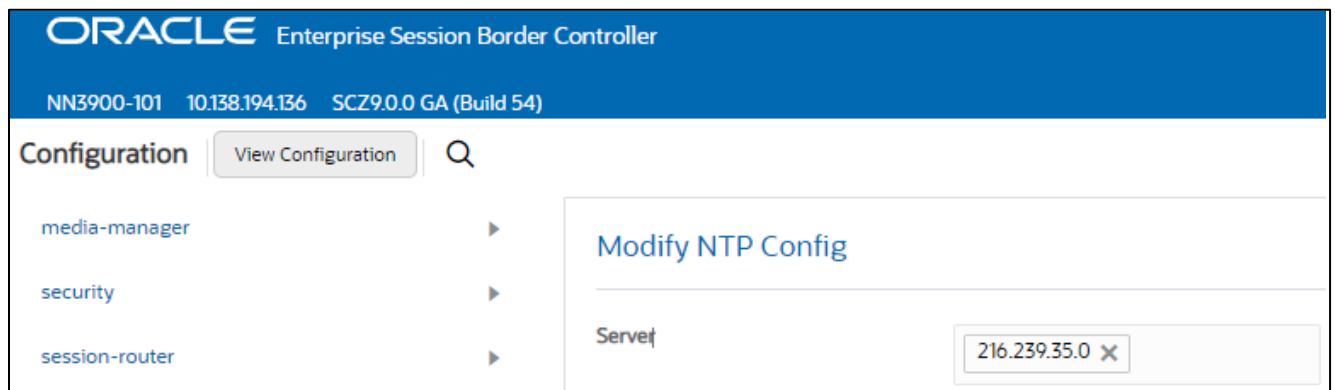


### 7.3 NTP-Sync

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



## 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                      gossip01.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-cache-mode=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 [Oracle SBC configuration guide](#) on Page 406.



**Configuration** View Configuration Q

- ldap-config
- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config**
- sip-feature

Show All

### Modify SIP Config

State  enable

Dialog Transparency  enable

Home Realm ID ZoomProxy

Egress Realm ID

Nat Mode None

Registrar Domain \*

Registrar Host gossip01.sc.zoom.us

Registrar Port 5091 (Range: 0,1025..65535)

Init Timer 500 (Range: 0..4294967295)

OK Delete

- ldap-config
- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group

### Modify SIP Config

Enforcement Profile

Red Max Trans 10000 (Range: 0..50000)

Options

- max-udp-length=0 X
- reg-cache-mode=from X

SPL Options

SIP Message Len 4096 (Range: 0..65535)

## 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

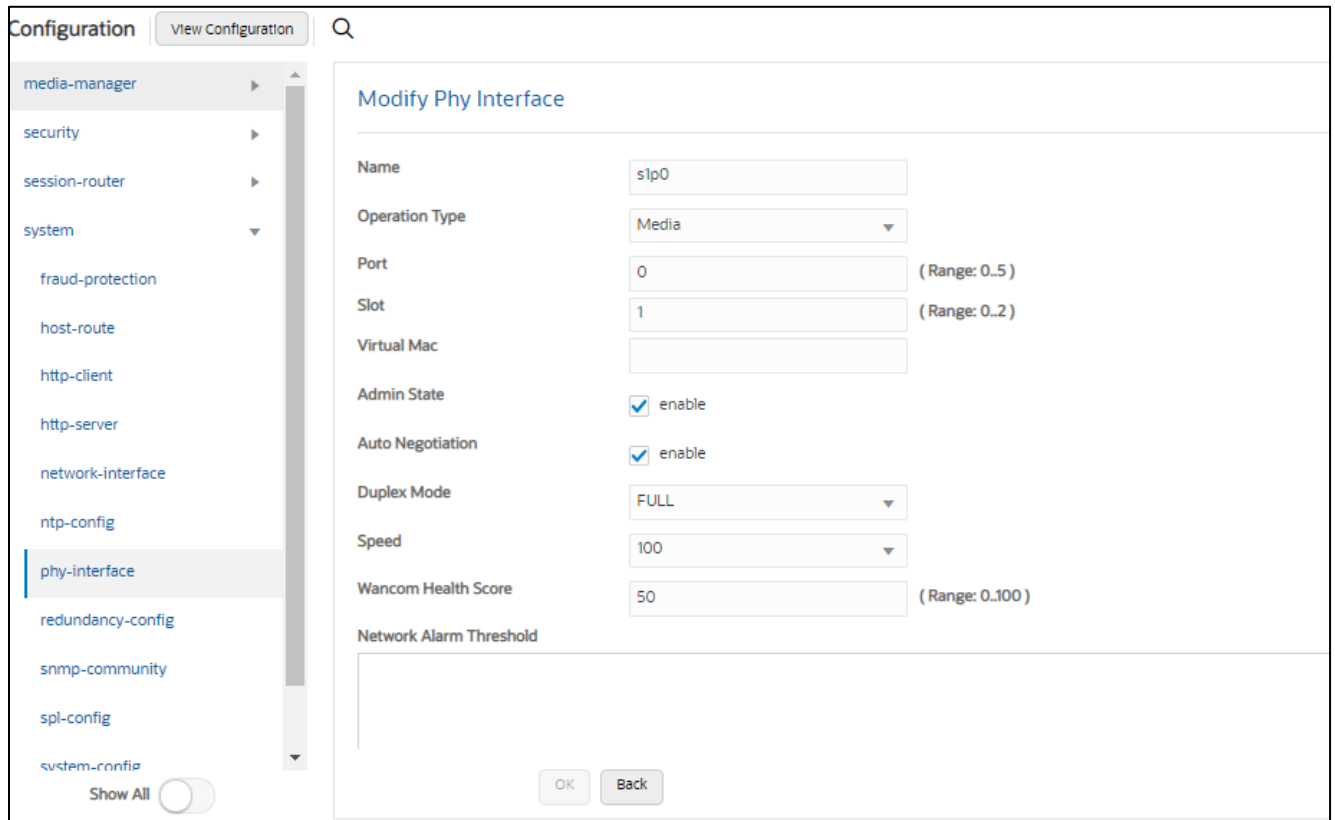
Configure **s0p1** interface as per example shared below.

The screenshot shows a configuration page titled "Modify Phy Interface" for the interface "s0p1". The left sidebar lists various configuration categories, with "phy-interface" selected. The main area contains the following settings:

- Name: s0p1
- Operation Type: Media
- Port: 1 (Range: 0.5)
- Slot: 0 (Range: 0.2)
- Virtual Mac: (empty field)
- Admin State:  enable
- Auto Negotiation:  enable
- Duplex Mode: FULL
- Speed: 100
- Wancom Health Score: 50 (Range: 0.100)
- Network Alarm Threshold: (empty field)

At the bottom of the configuration area, there are "OK" and "Back" buttons. A "Show All" toggle is visible in the sidebar.

Configure **s1p0** interface as per example shared below -



## 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 -

The screenshot shows the 'Modify Network Interface' configuration page. On the left, a navigation menu lists various configuration categories, with 'network-interface' selected. The main area contains the following fields:

Name	s0p1
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	
IP Address	10.1.4.4
Pri Utility Addr	
Sec Utility Addr	
Netmask	255.255.255.0
Gateway	10.1.4.1

Buttons for 'OK' and 'Back' are located at the bottom right of the configuration area.

Similarly, configure network interface s1p0 as below

The screenshot shows the 'Modify Phy Interface' configuration page. On the left, the navigation menu has 'phy-interface' selected. The main area contains the following fields:

Name	s1p0
Operation Type	Media
Port	0 (Range: 0..5)
Slot	1 (Range: 0..2)
Virtual Mac	
Admin State	<input checked="" type="checkbox"/> enable
Auto Negotiation	<input checked="" type="checkbox"/> enable
Duplex Mode	FULL
Speed	100
Wancom Health Score	50 (Range: 0..100)
Network Alarm Threshold	

Buttons for 'OK' and 'Back' are located at the bottom right of the configuration area.

## 7.7. Enable media manager

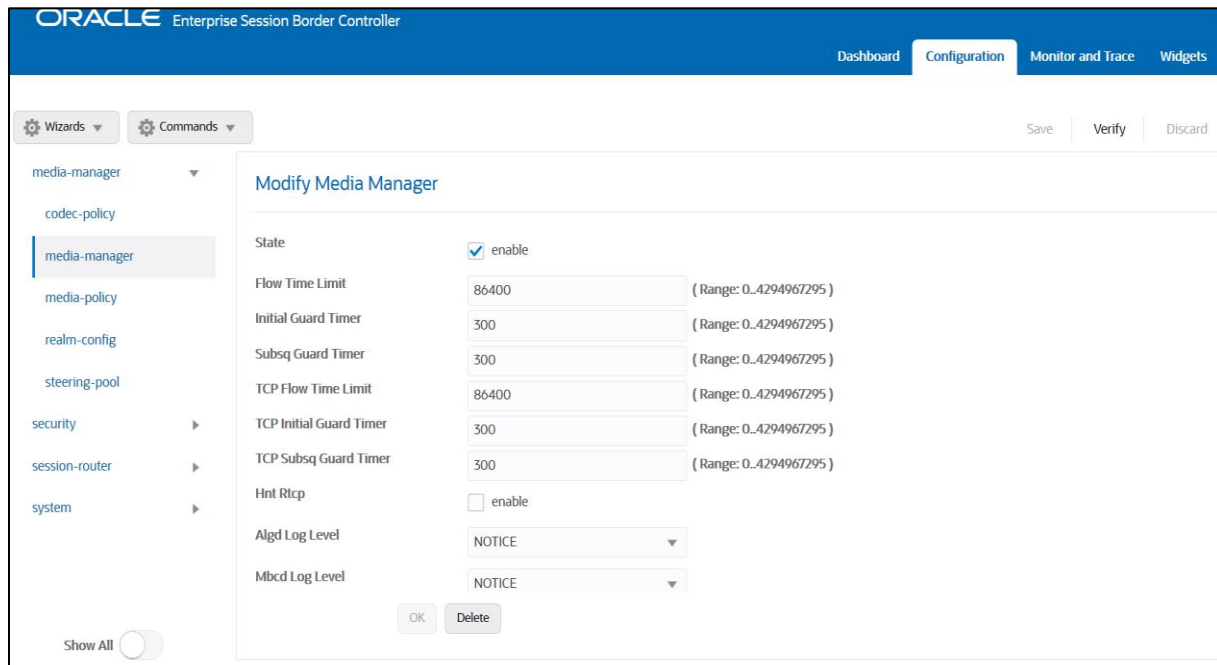
To configure media functionality on the SBC, you must first enable the global media manager. Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

GUI Path: media-manager/media-manager

ACL 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.

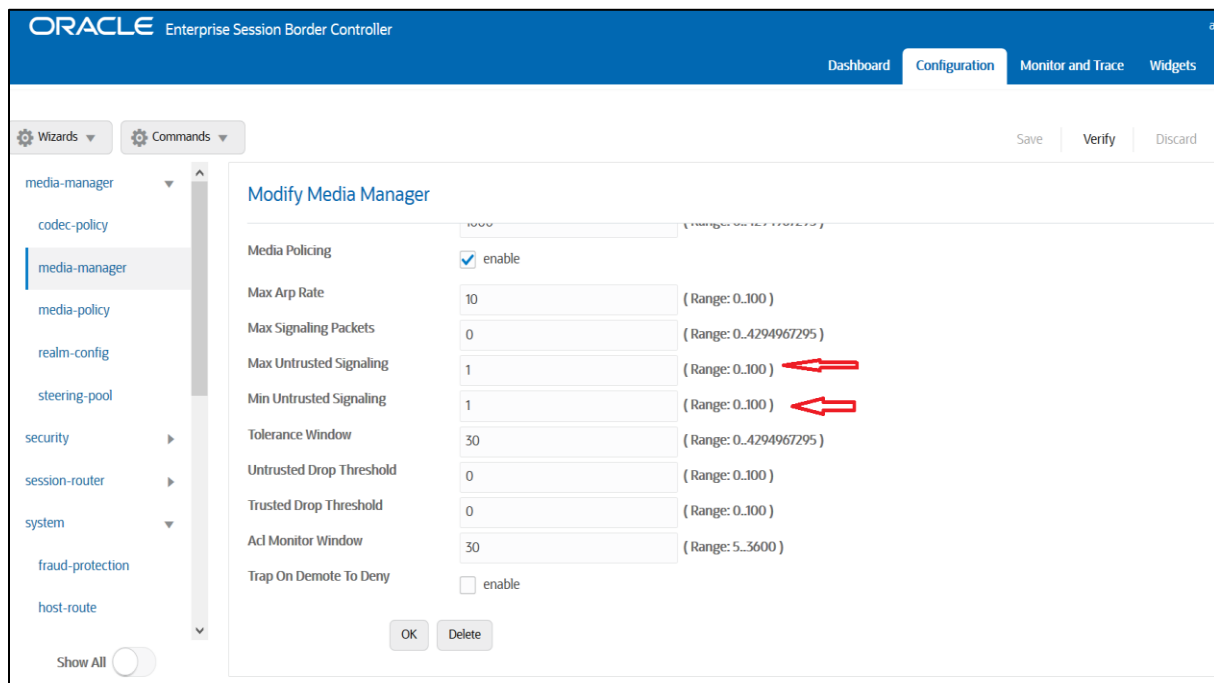
Enable Latching if required.



The screenshot displays the Oracle Enterprise Session Border Controller (ESBC) configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' tab is active. On the left, a sidebar shows a tree view of configuration categories: 'media-manager' (expanded), 'codec-policy', 'media-policy', 'realm-config', 'steering-pool', 'security', 'session-router', and 'system'. The 'media-manager' category is selected, and the 'Modify Media Manager' configuration page is displayed. The page contains the following settings:

Parameter	Value	Range
State	<input checked="" type="checkbox"/> enable	
Flow Time Limit	86400	( Range: 0..4294967295 )
Initial Guard Timer	300	( Range: 0..4294967295 )
Subsq Guard Timer	300	( Range: 0..4294967295 )
TCP Flow Time Limit	86400	( Range: 0..4294967295 )
TCP Initial Guard Timer	300	( Range: 0..4294967295 )
TCP Subsq Guard Timer	300	( Range: 0..4294967295 )
Hnt Rtcp	<input type="checkbox"/> enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	

At the bottom of the configuration area, there are 'OK' and 'Delete' buttons. A 'Show All' toggle is located at the bottom left of the sidebar.



## 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 Environment 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 [Oracle SBC configuration guide](#) on Page 291.

Here we have enabled **symmetric latching** on the ZoomEndpoints Realm which is a latching mode where a device'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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access Control Trust Level	low	High
Media Sec policy	ZoomMediaSecurity	ZoomMediaSecurity
symmetric-latching	enabled	

### 7.8.1 Realm ZoomEndpoints

The screenshot displays the 'Modify Realm Config' interface for the 'ZoomEndpoints' realm. The configuration parameters are as follows:

- Identifier:** ZoomEndpoints
- Description:** (Empty text area)
- Addr Prefix:** 0.0.0.0
- Network Interfaces:** s0p1:0.4
- Media Realm List:** (Empty list)
- Mm In Realm:**  enable
- Mm In Network:**  enable
- Mm Same Ip:**  enable
- QoS Enable:**  enable
- Max Bandwidth:** 0 (Range: 0.999999999)
- Max Priority Bandwidth:** 0 (Range: 0.999999999)
- Parent Realm:** (Dropdown menu)
- DNS Realm:** (Dropdown menu)

Navigation options in the sidebar include: media-manager, codec-policy, media-manager, media-policy, realm-config (selected), steering-pool, security, session-router, system, fraud-protection, host-route, http-client, http-server, network-interface, ntp-config, phy-interface, and redundancy-config. A 'Show All' toggle is also present.

Configuration View Configuration Q

- media-manager
  - codec-policy
  - media-manager
  - media-policy
  - realm-config
  - steering-pool
- security
- session-router
- system
  - fraud-protection
  - host-route
  - http-client
  - http-server
  - network-interface
  - ntp-config
  - phy-interface
  - redundancy-config

Show All

### Modify Realm Config

Media Sec Policy: ZoomMediaSecurity

RTCP Mux:  enable

Ice Profile:

Teams Fqdn:

Teams Fqdn In Uri:  enable

SDP Inactive Only:  enable

DTLS Srtp Profile:

Srtp Msm Passthrough:  enable

Class Profile:

In Translationid:

Out Translationid:

In Manipulationid:

Out Manipulationid:

Average Rate Limit: 0 (Range: 0..4294967295)

Access Control Trust Level: low

## 7.8.2 Realm ZoomCloud

Configuration View Configuration Q

- media-manager
  - codec-policy
  - media-manager
  - media-policy
  - realm-config
  - steering-pool
- security
- session-router
- system
  - fraud-protection
  - host-route
  - http-client
  - http-server
  - network-interface
  - ntp-config

Show All

### Modify Realm Config

Identifier: ZoomCloud

Description:

Addr Prefix: 0.0.0.0

Network Interfaces: slp0:0.4 x

Media Realm List:

Mm In Realm:  enable

Mm In Network:  enable

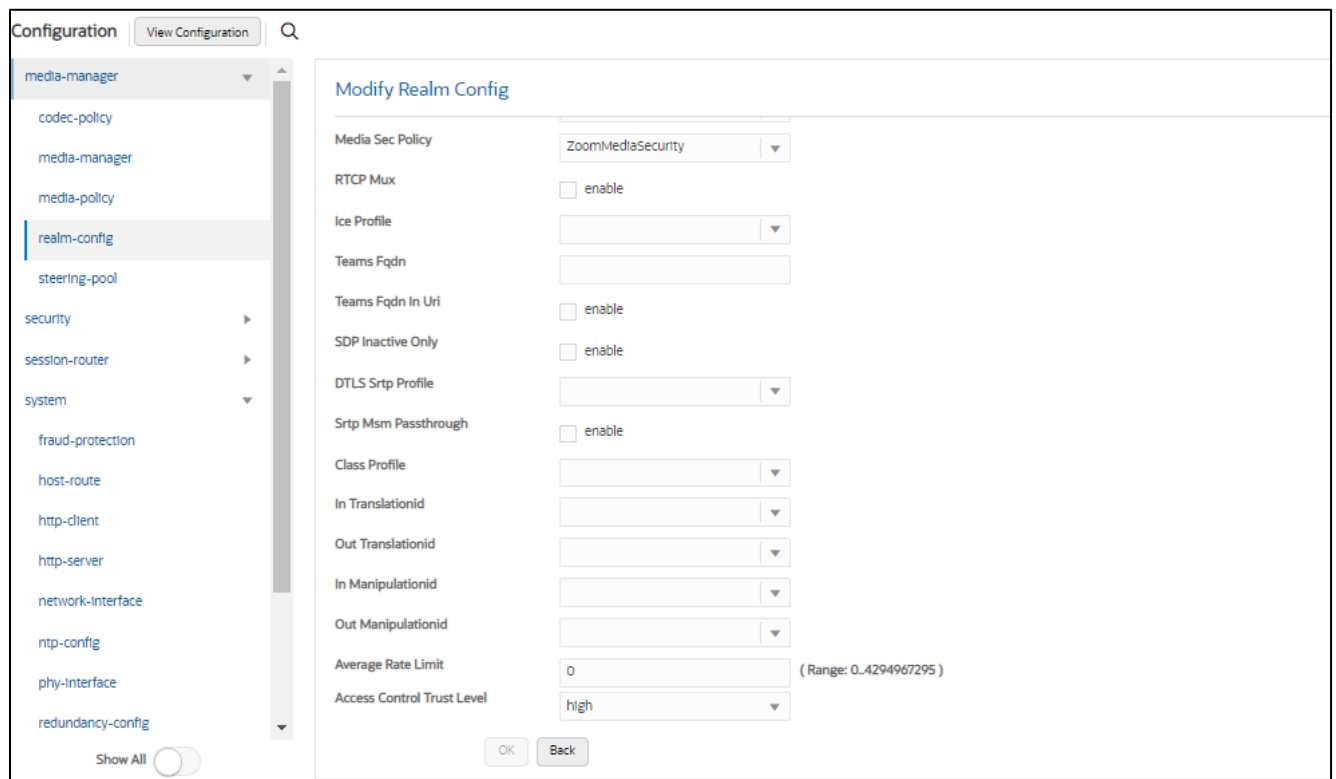
Mm Same Ip:  enable

QoS Enable:  enable

Max Bandwidth: 0 (Range: 0..999999999)

Max Priority Bandwidth:





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 Practice 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

ACL 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 Intermediate 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 be imported onto the SBC as a trusted Root CA Certificate.

The following 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	SBC Certificate for Zoom Cloud	SBC Certificate for Zoom Proxy	GoDaddy Certificate Bundle	DigiCert Root CA	DigiCert Intermediate	DigiCert Global Root G2	DigiCert Global Root G3
Name	SBC Certificate for Zoom Cloud	SBC Certificate for Zoom Proxy	GodaddyCertBundle	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA	DigiCert Global Root G2	DigiCert Global Root G3
Common Name	telechat-test06161977.com	teamsolab.site	GoDaddy Root Certificate Authority - G2 GoDaddy Secure Certificate Authority - G2	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA	DigiCert Global Root G2	DigiCert Global Root G3
Key Size	2048	2048	2048	2048	2048	2048	2048
Key-Us	digitalSignature keyEnci	digitalSignature keyEnci	digitalSignature keyEnci	digitalSignature keyEnci	digitalSignature keyEnci	digitalSignature keyEnci	digitalSignature keyEnci

age - List	phermement	phermement	phermement	phermement	phermement	phermement	phermement
Extended Key Usage List	serverAuth	serverAuth	serverAuth	serverAuth	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa	rsa	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256	Sha256	Sha256	Sha256	Sha256

### 7.9.1.1 End Entity Certificate

In this setup we have created two end entity (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 unsuccessful.

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

- media-manager ▶
- security ▼
  - authentication-profile
  - certificate-record**
  - tls-global
  - tls-profile
- session-router ▶
- system ▶

Show All

### Modify Certificate Record

Name	<input type="text" value="SBCCertificateforZoomCloud"/>
Country	<input type="text" value="US"/>
State	<input type="text" value="California"/>
Locality	<input type="text" value="Redwood City"/>
Organization	<input type="text" value="Oracle Corporation"/>
Unit	<input type="text" value="Oracle CGBU-LABS BOSTON"/>
Common Name	<input type="text" value="telechat.o-test06161977.com"/>
Key Size	<input type="text" value="2048"/>
Alternate Name	<input type="text"/>

Similarly create another certificate record for Zoom Proxy.

Configuration View Configuration

- media-manager** ▶
- security ▼
  - authentication-profile
  - certificate-record**
  - tls-global
  - tls-profile
- session-router ▶
- system ▶

Show All

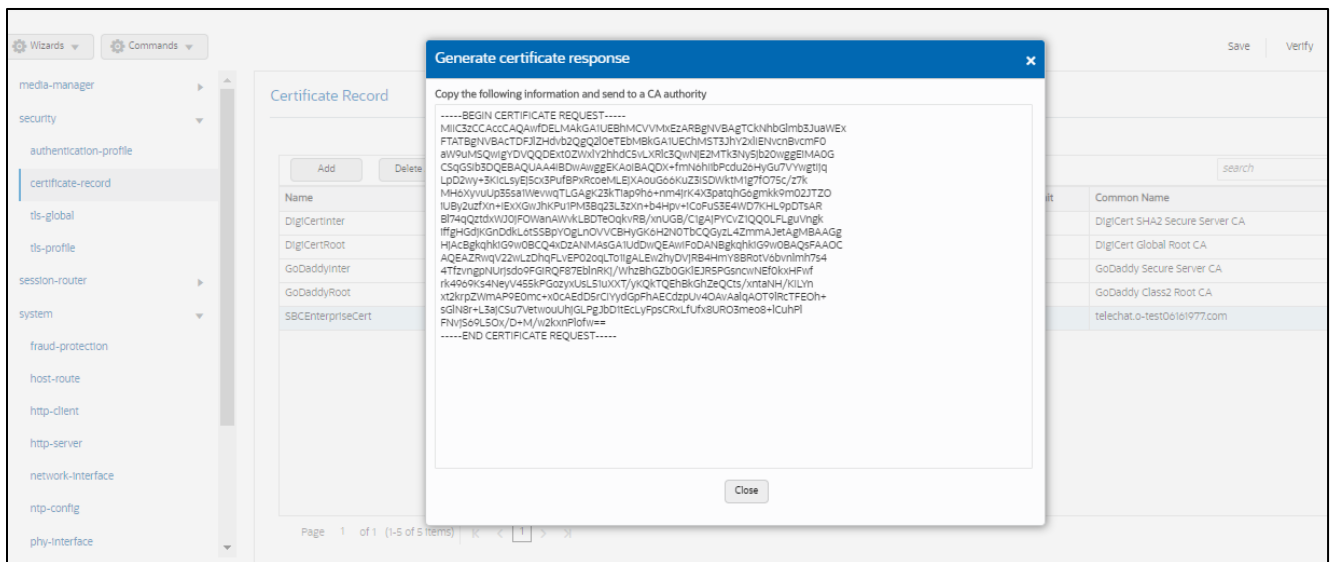
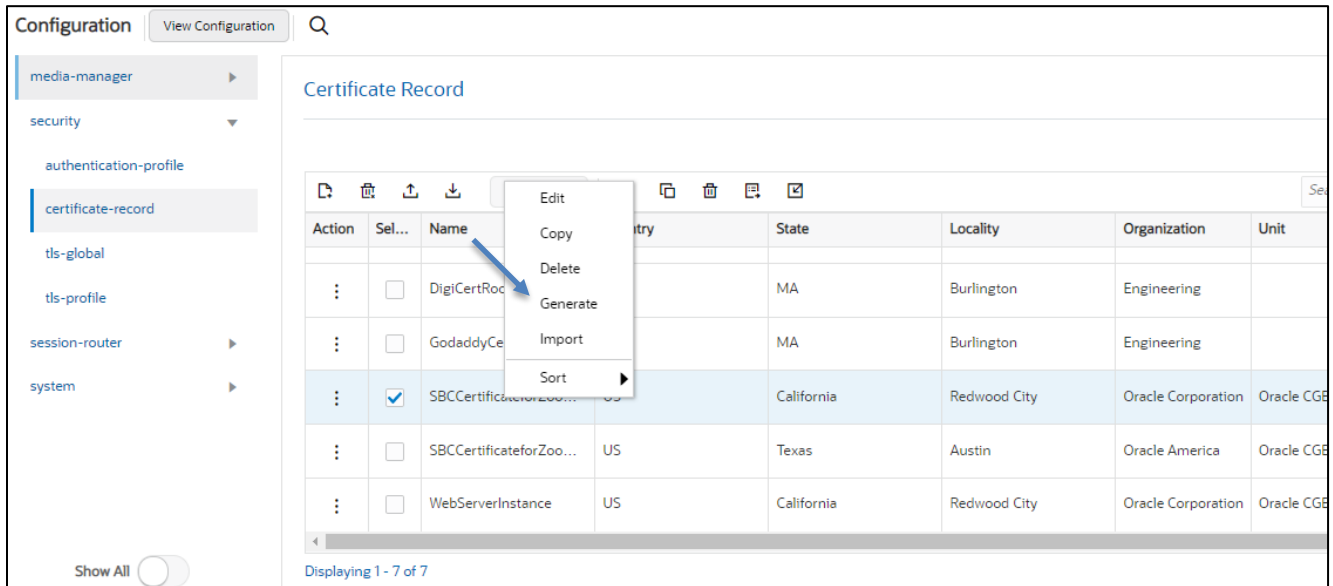
### Modify Certificate Record

Name	<input type="text" value="SBCCertificateforZoomProxy"/>
Country	<input type="text" value="US"/>
State	<input type="text" value="Texas"/>
Locality	<input type="text" value="Austin"/>
Organization	<input type="text" value="Oracle America"/>
Unit	<input type="text" value="Oracle CGBU-LABS BOSTON"/>
Common Name	<input type="text" value="teamsollab.site"/>
Key Size	<input type="text" value="2048"/>
Alternate Name	<input type="text"/>

## 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.



- 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

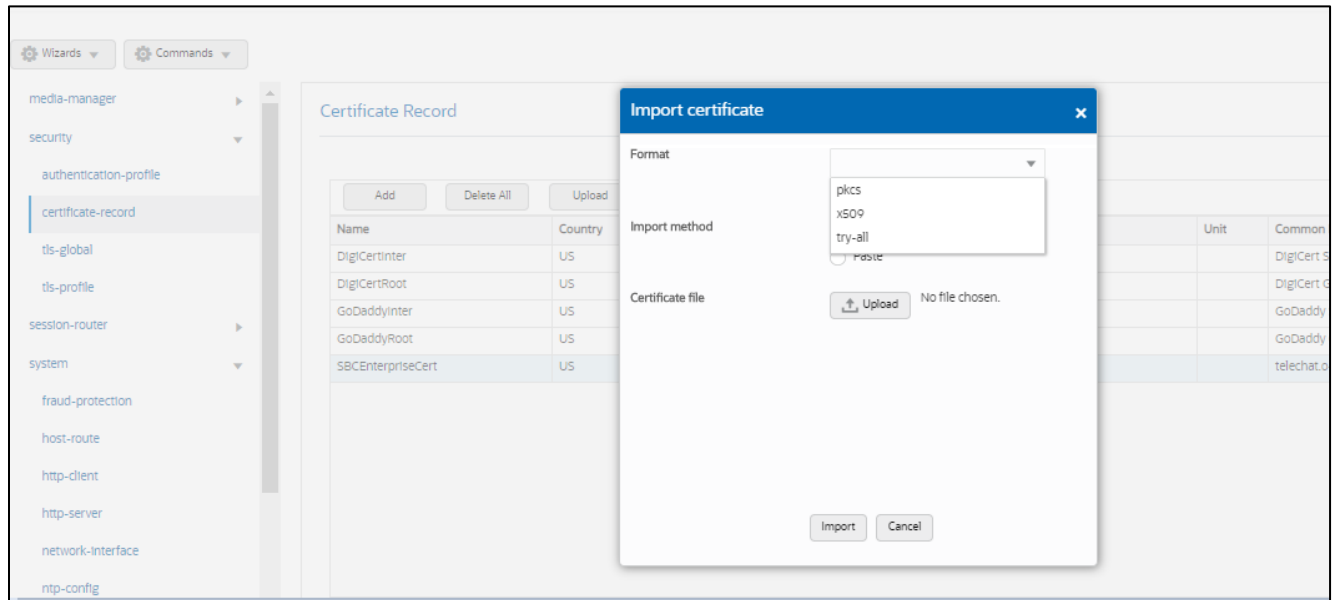
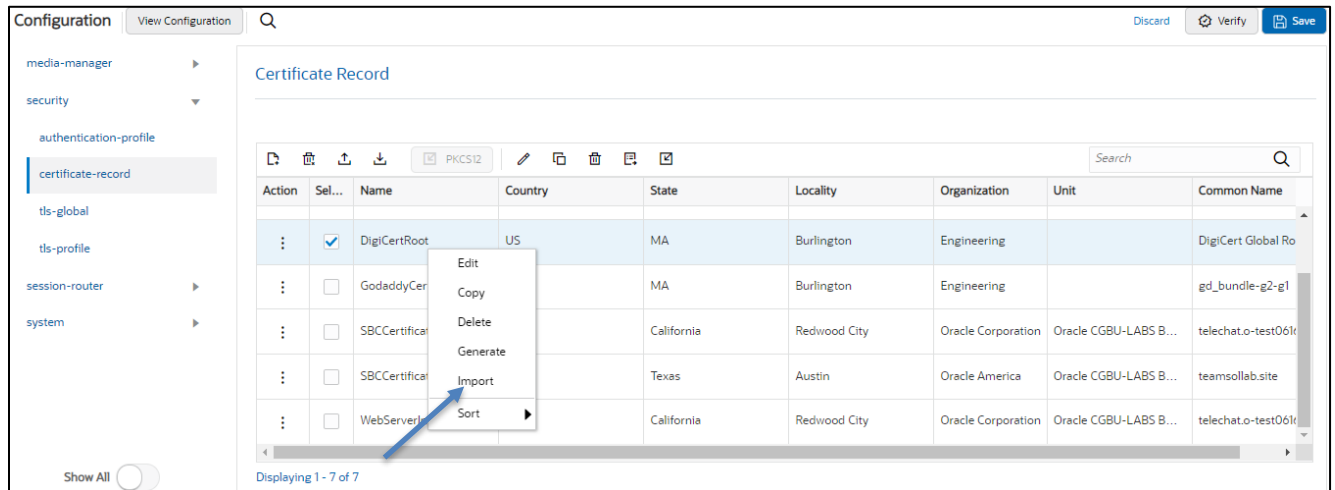
The screenshot displays the SBC WebGUI interface. The top section shows the 'Configuration' menu with 'Certificate Record' selected. Below this is a table of certificate records. A context menu is open over the 'SBCCertificateforZoomProxy' entry, with the 'Import' option highlighted. The bottom section shows the 'Import certificate' dialog box, which is currently empty, indicating that no file has been chosen for import.

Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
:	<input type="checkbox"/>	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberTrust Root
:	<input type="checkbox"/>	DigiCertInter	US	MA	Burlington	Engineering		DigiCert SHA2 Secure Ser...
:	<input type="checkbox"/>	DigiCertRoot	US	MA	Burlington	Engineering		DigiCert Global Root CA
:	<input type="checkbox"/>	GoDaddyCertBundl...	US	MA	Burlington	Engineering		gd_bundle-g2-g1
:	<input type="checkbox"/>	SBCCertificateforCl...	US	California	Redwood City	Oracle Corporation	Oracle CGBU-LABS BOST...	telechat.o-test06161977.c...
:	<input checked="" type="checkbox"/>	SBCCertificateforZoomProxy	US	Texas	Austin	Oracle America	Oracle CGBU-LABS BOST...	teamsollab.site
:	<input type="checkbox"/>	WebServerInstance	US	California	Redwood City	Oracle Corporation	Oracle CGBU-LABS BOST...	telechat.o-test06161977.c...

#### 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.



## 7.10. TLS-Profile

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

GUI Path: security/tls-profile

ACL Path: config t→security→tls-profile

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

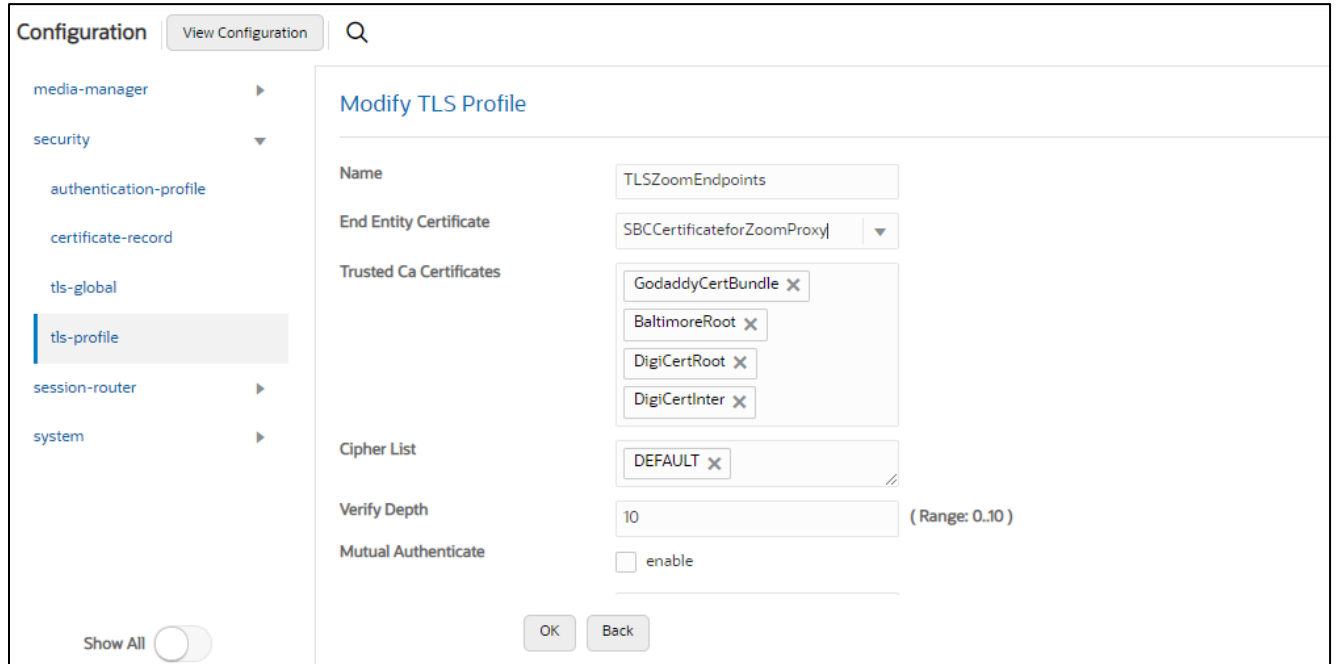
### 7.10.1 TLS-Profile – TLSZoomEndpoints

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 Negotiation Method is used.



## 7.10.2 TLS-Profile – TLSZoomCloud

End Entity Certificate-SBCCertificateforZoomCloud

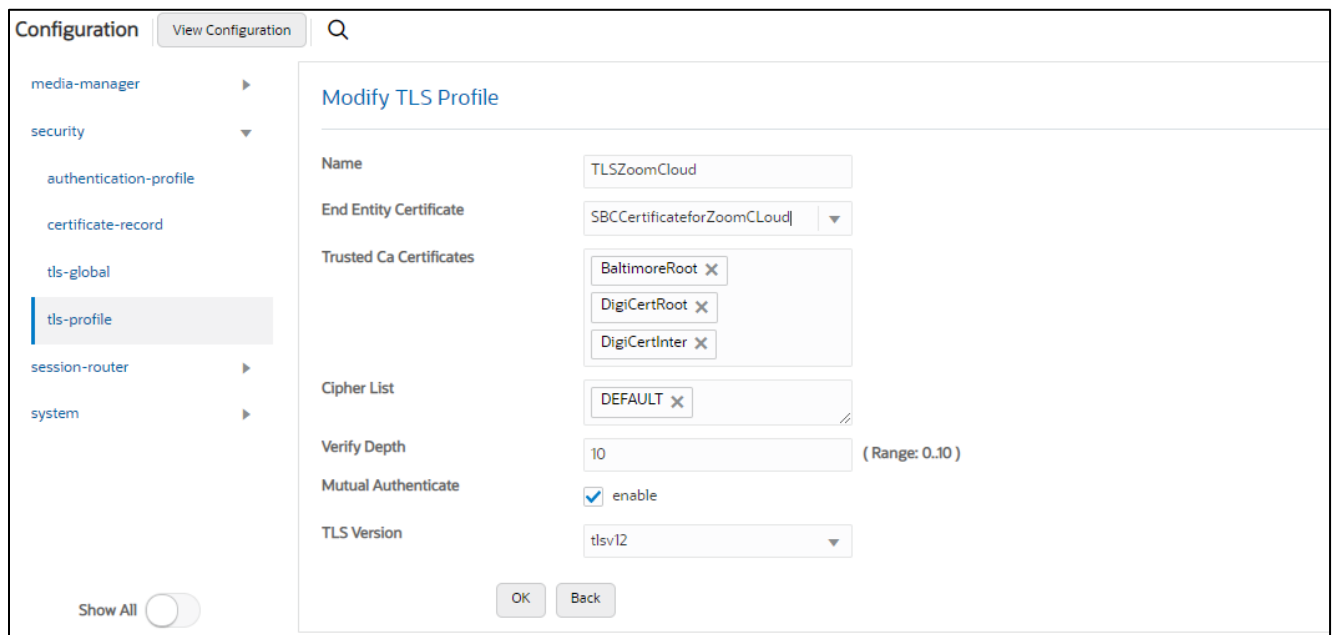
Mutual Authentication-Enabled

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 be 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>





## 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

ACL 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 [Section 7.16](#) of the document.

Configuration View Configuration Q Discard Verify Save

Modify SIP Interface Show Configuration

State  enable

Realm ID ZoomEndpoints

Description

SIP Ports

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
:	<input type="checkbox"/>	10.1.4.4	5061	TLS	TLSZoomEndpoints	registered	

Configuration View Configuration Q

Modify SIP Interface

Nat Traversal always

Nat Interval 30 (Range: 0..4294967295)

TCP Nat Interval 90 (Range: 0..4294967295)

Registration Caching  enable

Min Reg Expire 300 (Range: 0..999999999)

Registration Interval 3600 (Range: 0..4294967295)

Route To Registrar  enable

Secured Network  enable

Uri Fqdn Domain

Options

SPL Options HeaderNatPublicSipfip=20.65.42.129;}

Trust Mode all

Max Nat Interval 3600 (Range: 0..4294967295)

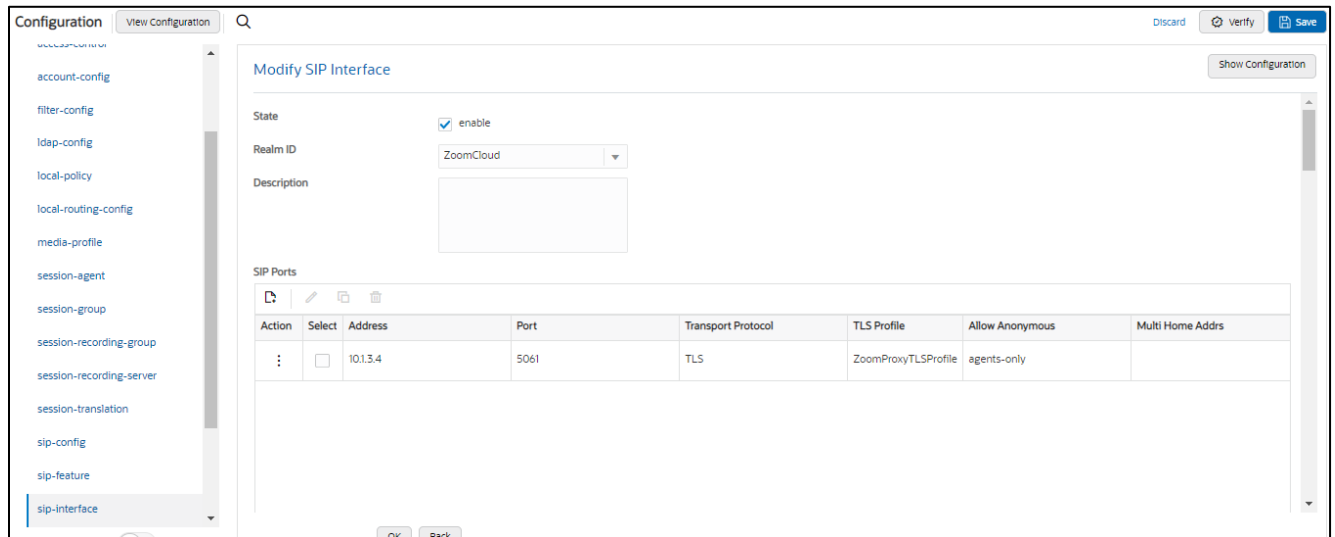
Show All

OK Back

## 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.



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.

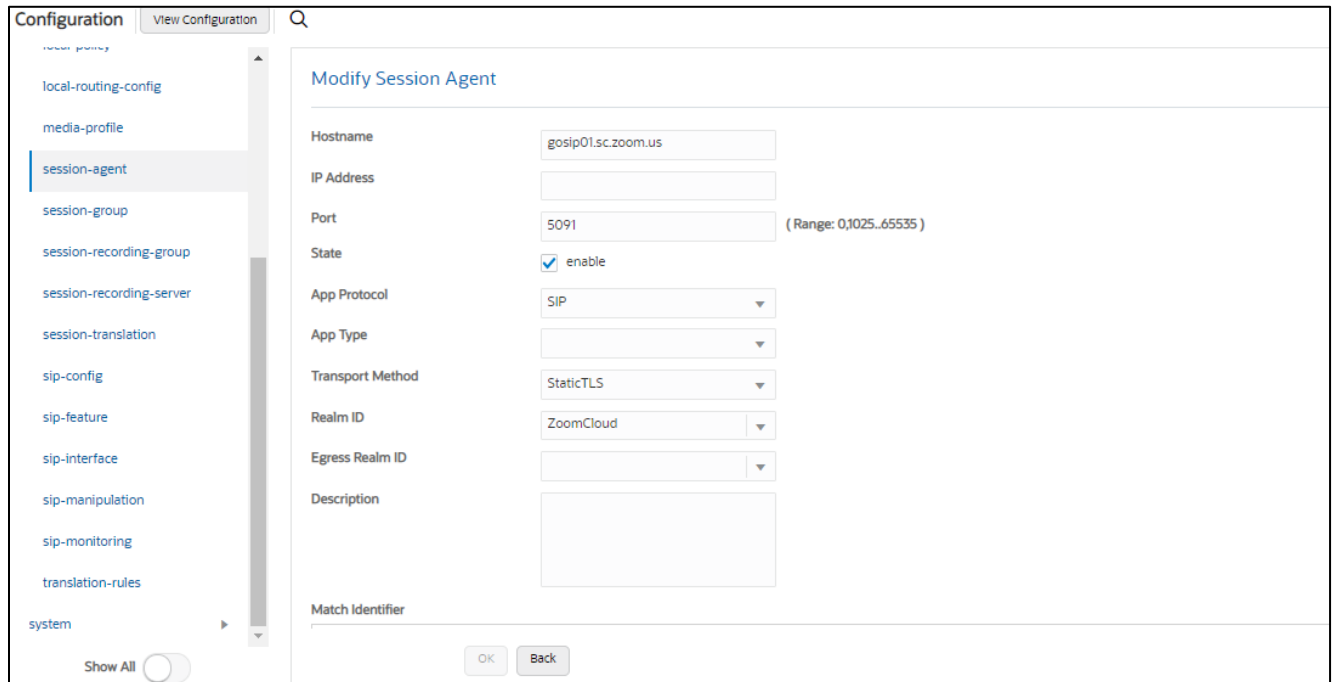
GUI Path: session-router/session-agent

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 [section 6.3](#)
- 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.



### 7.13. Configure local-policy

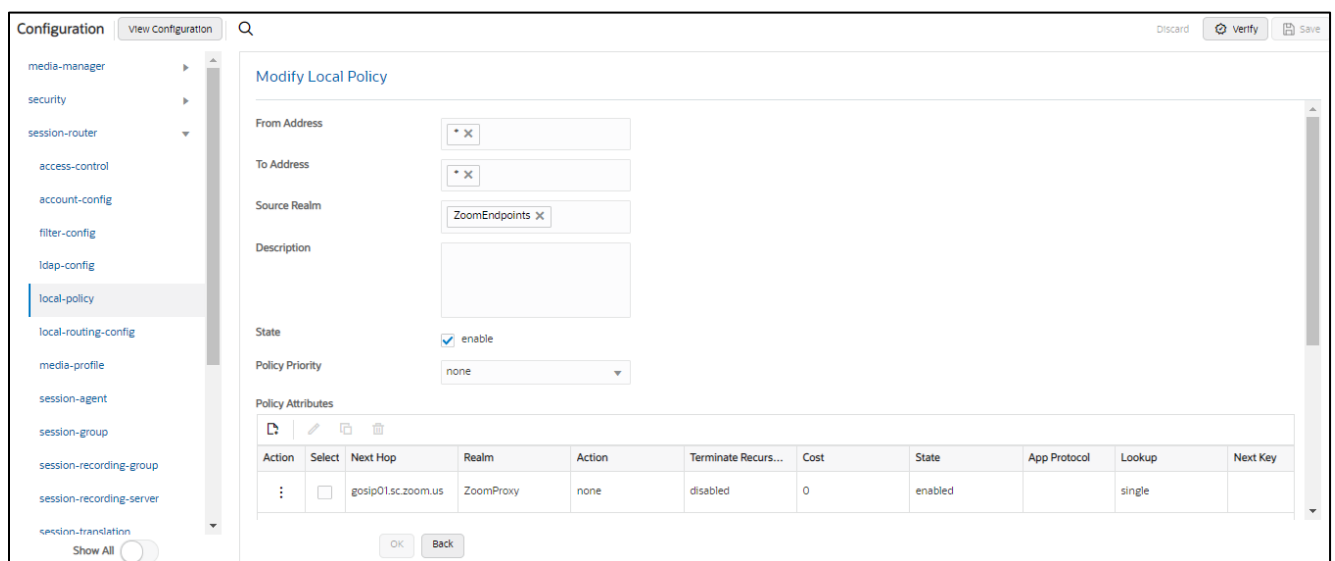
Local policy config allows the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy,

GUI Path: session-router/local-policy

CLI 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



Following local-policy routes the calls from the Carrier Trunk to Zoom BYOC Agent.

The screenshot shows the 'Modify Local Policy' configuration page. The left sidebar lists various configuration categories, with 'local-policy' selected. The main area contains the following fields:

- From Address: \* X
- To Address: \* X
- Source Realm: SipTrunk X
- Description: Route Calls from SipTrunk to Zoom BYOC
- State:  enable
- Policy Priority: none

Below these fields is a 'Policy Attributes' table:

Action	Select	Next Hop	Realm	Action	Terminate Recurs...	Cost	State	App Protocol	Lookup	Next Key
:	<input type="checkbox"/>	162.12.233.60	ZoomPhone	replace-uri	disabled	0	enabled		single	

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.

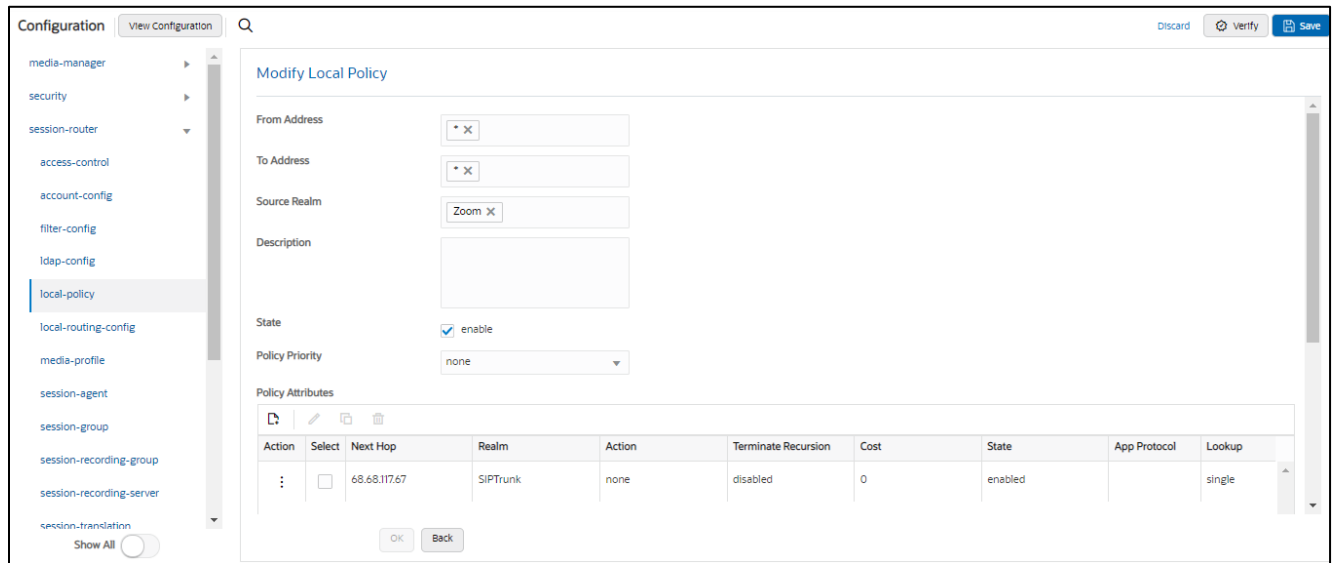
The screenshot shows the 'Modify Local Policy' configuration page. The left sidebar lists various configuration categories, with 'local-policy' selected. The main area contains the following fields:

- From Address: \* X
- To Address: \* X
- Source Realm: ZoomPhone X
- Description: Route Calls from Zoom BYOC to Sip Trunk
- State:  enable
- Policy Priority: none

Below these fields is a 'Policy Attributes' table:

Action	Select	Next Hop	Realm	Action	Terminate Recurs...	Cost	State	App Protocol	Lookup	Next Key
:	<input type="checkbox"/>	68.68.117.67	SipTrunk	none	disabled	0	enabled		single	

The screenshots are for reference. To configure Zoom BYOC with Oracle SBC please refer to this [Oracle Application Note](#).



## 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.

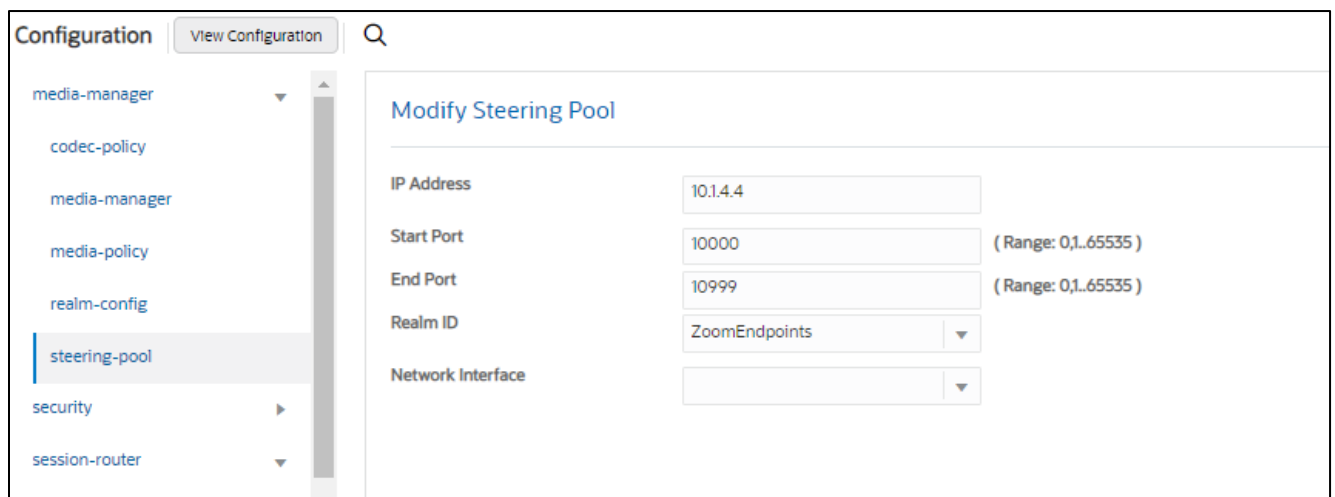
We will configure steering pool for each realm configured.

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



## 7.14.2 Zoom Cloud Steering Pool

The screenshot shows the 'Modify Steering Pool' configuration page. On the left, a navigation menu lists several categories: media-manager, codec-policy, media-manager, media-policy, realm-config, steering-pool (which is highlighted), and security. The main content area is titled 'Modify Steering Pool' and contains the following configuration fields:

IP Address	<input type="text" value="10.1.3.4"/>	
Start Port	<input type="text" value="10000"/>	( Range: 0,1..65535 )
End Port	<input type="text" value="10999"/>	( Range: 0,1..65535 )
Realm ID	<input type="text" value="ZoomCloud"/>	▼
Network Interface	<input type="text"/>	▼

## 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

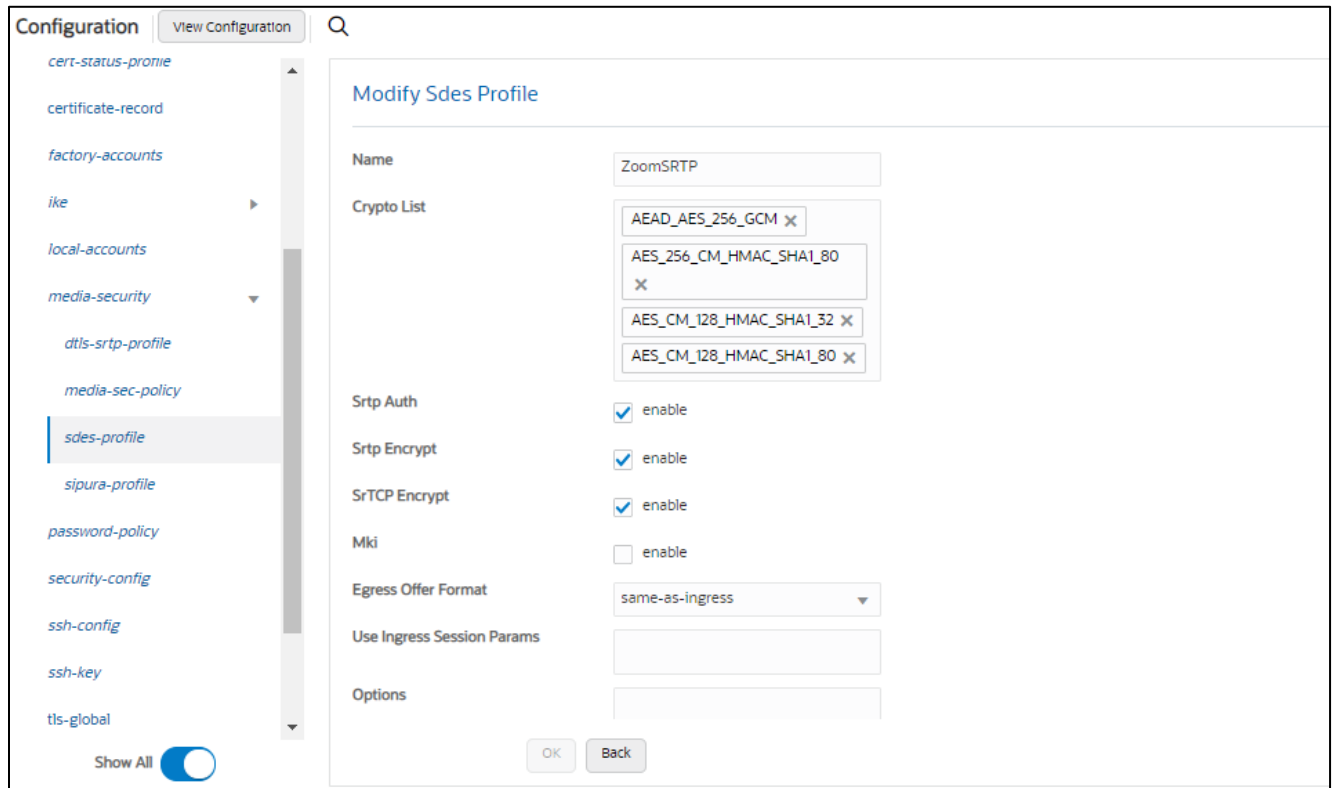
This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured.

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

ACL I Path: config t→security→media-security→sdes-profile

- Click Add, and use the example below to configure



### 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

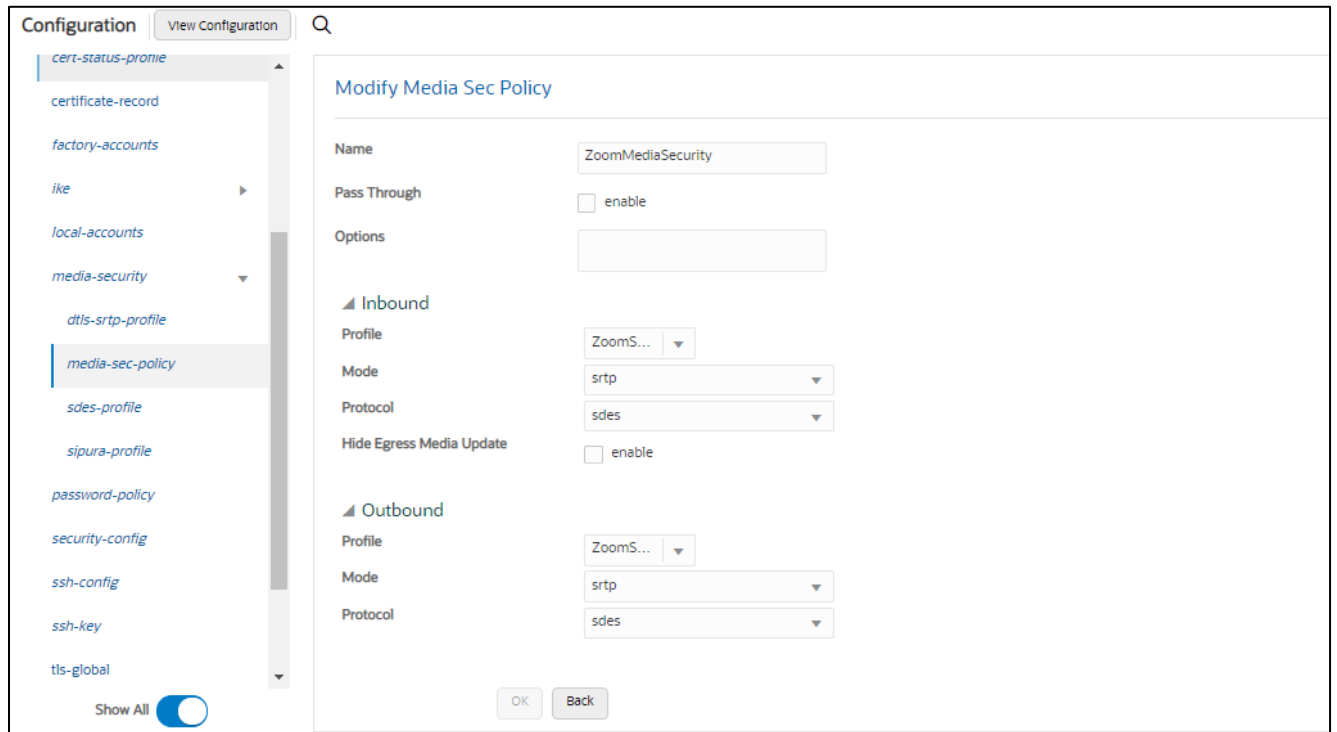
ACLI Path: config t→security→media-security→media-sec-policy

- Click Add, use the examples below to configure

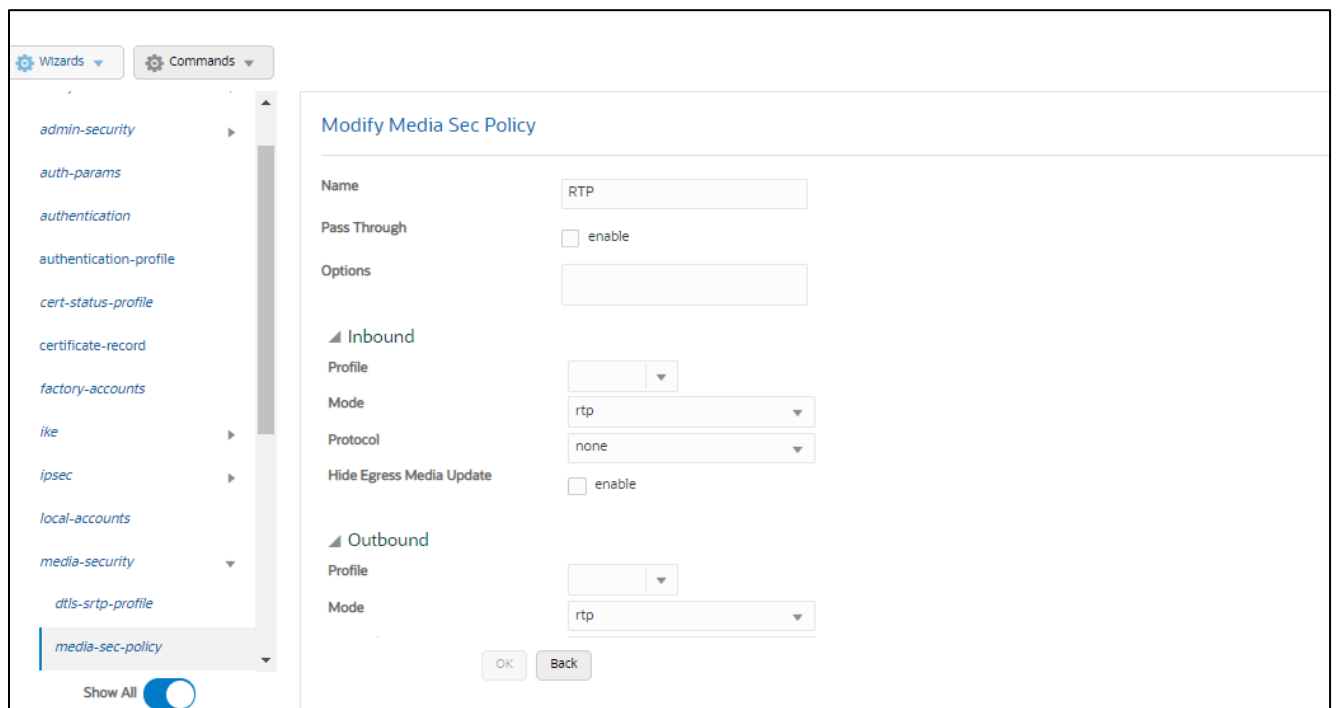
Create Media Sec policy with name ZoomMediaSecurity, which will have the sdes profile, created above.

The same media policy can be assigned to both [ZoomEndpoints](#) and [ZoomCloud Realm](#).





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.



## 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

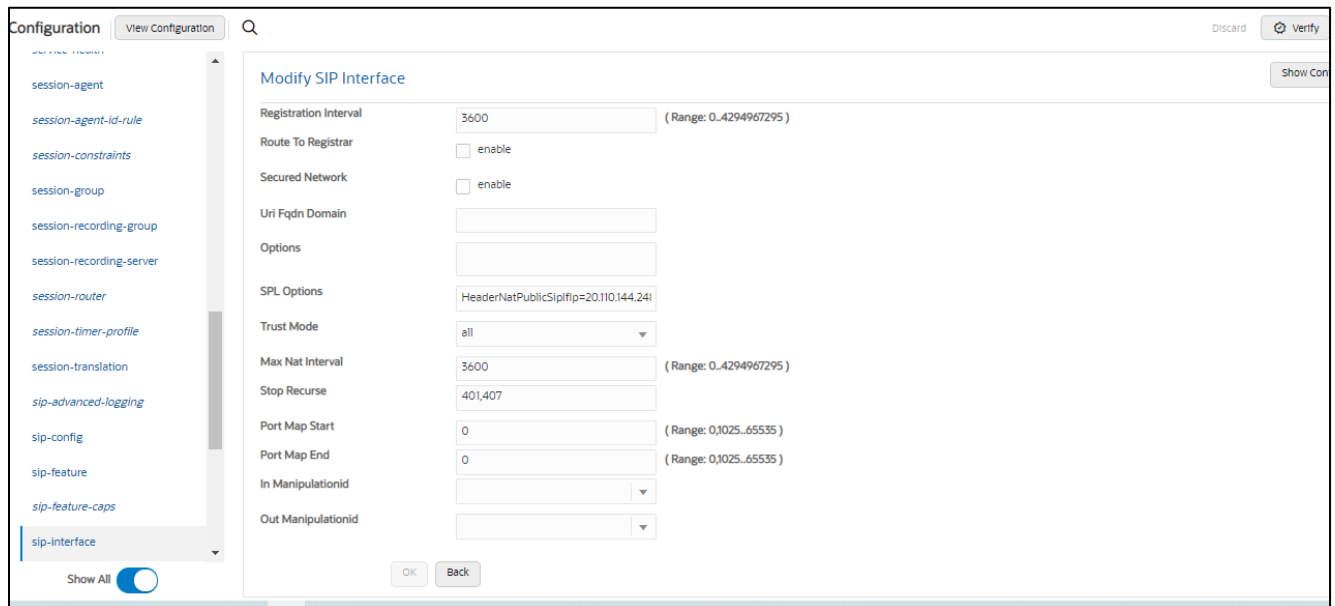
CLI Path: config t→session-router→sip-interface

**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

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



The screenshot shows the Oracle SBC Configuration GUI. The left sidebar lists various configuration categories, with 'sip-interface' selected. The main area is titled 'Modify SIP Interface' and contains several configuration fields:

- Registration Interval: 3600 (Range: 0..4294967295)
- Route To Registrar:  enable
- Secured Network:  enable
- Uri Fqdn Domain: [Empty]
- Options: [Empty]
- SPL Options: HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4
- Trust Mode: all
- Max Nat Interval: 3600 (Range: 0..4294967295)
- Stop Recurse: 401,407
- Port Map Start: 0 (Range: 0,1025..65535)
- Port Map End: 0 (Range: 0,1025..65535)
- In Manipulationid: [Empty]
- Out Manipulationid: [Empty]

At the bottom of the form are 'OK' and 'Back' buttons. The top right corner has 'Discard' and 'Verify' buttons, and the bottom right has a 'Show Con' button.

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 [Configuration Guide](#) on page 389

GUI Path: session-router/session-timer-profile

ACL 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.


The screenshot displays the Oracle SBC GUI configuration page for a Session Timer Profile. The interface includes a left-hand navigation menu with categories like 'rph-profile', 'service-health', 'session-agent', and 'session-timer-profile' (which is currently selected). The main content area is titled 'Modify Session Timer Profile' and contains the following configuration fields:

- Name:** ZoomSessionTimer
- Session Expires:** 900 (Range: 64,999999999)
- Min Se:** 90 (Range: 64,999999999)
- Force Reinvite:**  enable
- Request Refresher:** uac
- Response Refresher:** uac

At the bottom of the configuration panel, there are 'OK' and 'Back' buttons. A 'Show All' toggle is visible at the bottom left of the sidebar.

## 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.



CONNECT WITH US

 [blogs.oracle.com/oracle](https://blogs.oracle.com/oracle)

 [facebook.com/Oracle/](https://facebook.com/Oracle/)

 [twitter.com/Oracle](https://twitter.com/Oracle)

 [oracle.com](https://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