

# ORACLE

Oracle Session Border Controller with Zoom Phone (Cloud Peering)

[\*\*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.

## Contents

<b>1 DOCUMENT OVERVIEW.....</b>	<b>4</b>
1.1 ORACLE SBC.....	4
1.2 ZOOM PHONE.....	4
<b>2 REVISION HISTORY .....</b>	<b>4</b>
<b>3 INTENDED AUDIENCE.....</b>	<b>4</b>
3.1 VALIDATED ORACLE VERSIONS .....	4
<b>4 ZOOM PHONE CONFIGURATION .....</b>	<b>5</b>
<b>5 INFRASTRUCTURE REQUIREMENTS.....</b>	<b>5</b>
<b>6 CONFIGURATION .....</b>	<b>6</b>
6.1 PREREQUISITES .....	7
6.2 GLOBAL CONFIGURATION ELEMENTS .....	7
6.2.1 System-Config .....	7
6.2.2 Media Manager.....	9
6.2.3 SIP Config .....	10
6.2.4 NTP Config.....	11
6.3 NETWORK CONFIGURATION.....	11
6.3.1 Physical Interfaces.....	12
6.3.2 Network Interfaces .....	13
6.4 SECURITY CONFIGURATION.....	14
6.4.1 Certificate Records .....	14
6.4.2 SBC End Entity Certificate .....	15
6.4.3 Root CA and Intermediate Certificates .....	17
6.4.4 Zoom Approved CA Vendors.....	17
6.4.5 Generate Certificate Signing Request .....	20
6.4.6 Import Certificates to SBC .....	21
6.4.7 TLS Profile.....	23
6.5 MEDIA SECURITY CONFIGURATION .....	25
6.5.1 Sdes-profile .....	25
6.5.2 Media Security Policy.....	26
6.6 MEDIA CONFIGURATION.....	28
6.6.1 Realm Config.....	28
6.6.2 Steering Pools .....	30
6.7 SIP MODIFICATIONS .....	32
6.7.1 SIP Manipulations.....	32
6.7.2 Session-Translation .....	39
6.8 SESSION TIMER PROFILE (OPTIONAL) .....	41
6.9 SIP INTERFACE.....	42
6.10 SESSION AGENTS.....	44
6.11 ROUTING CONFIGURATION .....	46
6.11.1 Local Policy Configuration.....	47
6.12 ACCESS CONTROLS .....	49
6.13 SBC BEHIND NAT SPL CONFIGURATION .....	50
<b>7. ACLI RUNNING CONFIGURATION.....</b>	<b>52</b>

## **1 Document Overview**

Zoom Phone Cloud Peering enables service providers to leverage their existing PSTN network to provide calling service to their customers. The Service Provider can utilize Oracle SBC which supports multi-Tenant Model to establish the connectivity with Zoom Phone System and multiple Enterprises.

This document focuses how to connect Oracle SBC to Zoom Phone Cloud Peering System.

Related Documentation can be found below-

### **1.1 Oracle SBC**

- [Oracle® Session Border Controller ACLI Configuration Guide](#)
- [Oracle® Session Border Controller Release Notes](#)
- [Oracle® Session Border Controller Security Guide](#)

### **1.2 Zoom Phone**

- <https://explore.zoom.us/en/products/zoom-phone/provider-exchange/>
- <https://zoom.us/phonesystem>
- <https://zoom.us/zoom-phone-features>

## **2 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	Date Revised	Description of Changes
1.0	30/09/22	<ul style="list-style-type: none"><li>• Initial publication</li></ul>

## **3 Intended Audience**

This document describes how to connect the Oracle SBC to Zoom Phone- Cloud Peering. This paper is intended for IT or telephony professionals.

*Note: To zoom in on screenshots of Web GUI configuration examples, press Ctrl and +.*

### **3.1 Validated Oracle Versions**

We have successfully conducted call testing with the Oracle Communications SBC versions:SCZ9.0p3

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
- AP3950 (Release SCZ9.0.0 Only)
- AP4900 (Release SCZ9.0.0 Only)
- VME
- Oracle SBC on Public Cloud

Please visit <https://docs.oracle.com/en/industries/communications/session-border-controller/index.html> for further information.

#### 4 Zoom Phone Configuration

This document only covers the steps required to configure Oracle SBC with Zoom Cloud Peering. There may be other components that are part of the Zoom Cloud Peering Setup which are not included in this document. For detailed assistance with setting up and configuring your Zoom Phone System for Cloud Peering, please reach out to Zoom Sales: <https://zoom.us/contactsales>

#### 5 Infrastructure Requirements

The table below shows the list of infrastructure prerequisites for deploying Zoom Premise Peering.

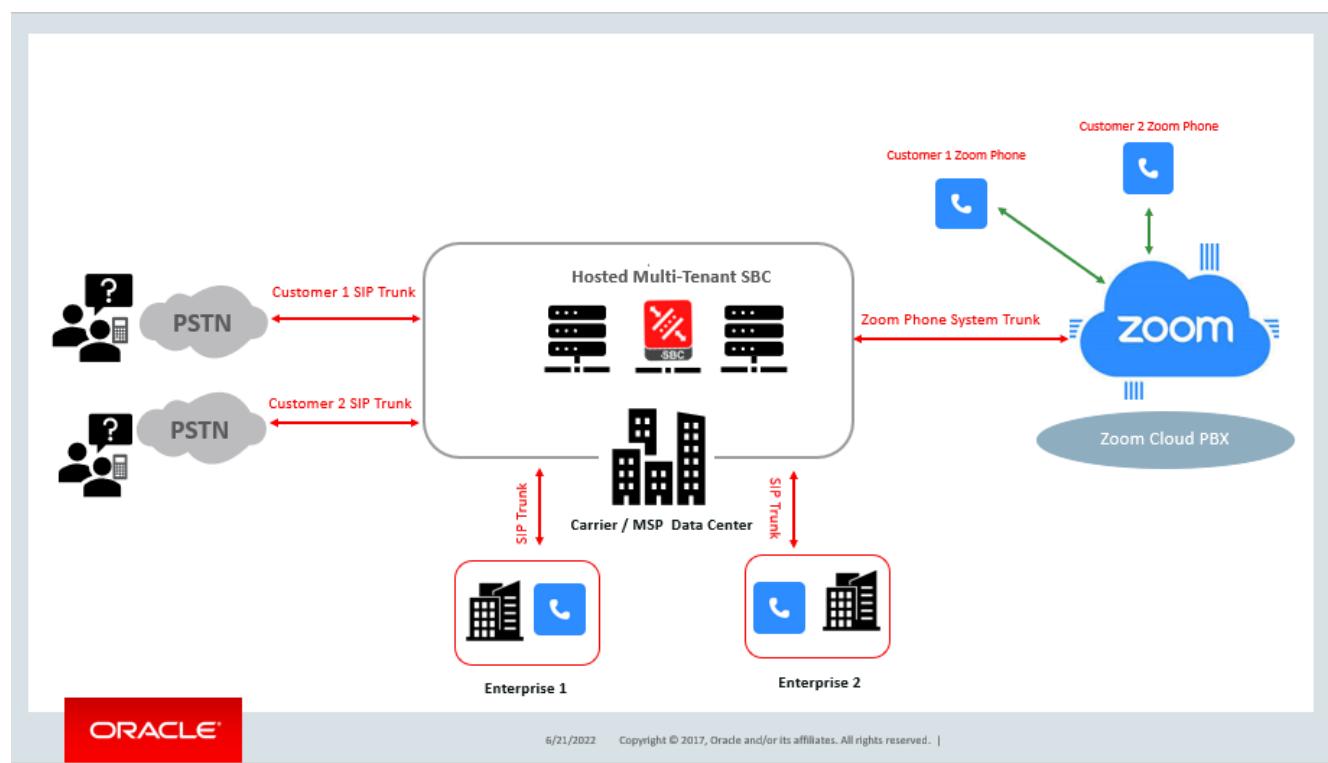
Session Border Controller (SBC)	
SIP Trunks connected to the SBC	
Zoom Phone System	
Public IP address for the SBC	
Public trusted certificate for the SBC (If TLS transport is used)	See <a href="#">Zoom Documentation</a> for More Details
Firewall ports for Zoom Voice signaling	
Firewall IP addresses and ports for Zoom Voice media	
Media Transport Profile	
Firewall ports for client media	

## 6 Configuration

This chapter provides step-by-step guidance on how to configure Oracle SBC for interworking with Zoom Phone.

All testing were performed in Oracle Labs. Below is an outline of the network setup used to conduct all testing between the Oracle SBC and Zoom Phone platform.

*These instructions cover configuration steps between the Oracle SBC and Zoom Phone Cloud Peering. The complete interconnection of other entities, such as connection of the SIP trunk, 3rd Party PBX and/or analog devices are not fully covered in this instruction. The details of such connection are available in other instructions produced by the vendors of retrospective components.*



Above Figure illustrates how a provider can utilize Oracle SBC to provide service to two Enterprise Networks. Each Customer register their Zoom Phones directly onto Zoom Cloud. These clients can be inside the corporate Network or can register from outside office premises.

PSTN Calls originating from Zoom Phone System for each customer are segregated based on DID Numbers and are routed to respective customer's PSTN Trunk from Oracle SBC.

**Note :** Having more than one PSTN trunks terminated onto the SBC is optional as service providers can leverage same carrier trunk to support multiple Enterprises.

Zoom adds custom header **X-To-Carrier** which can be used to identify each customer for billing prospective.

Inbound calls from PSTN to Zoom are terminated to appropriate customer user based on the assigned DID as Zoom does not require any specific header to identify users for each Tenant.

For the purpose of this application note the connection to Zoom Cloud PBX and Oracle SBC is TLS/SRTP.

## 6.1 Prerequisites

Before you begin, make sure that you have the following per every SBC you want to pair:

- Public IP address
- Public certificate issued by one of the supported CAs
- Zoom Public CA certificates to add to trust store of SBC

There are two methods for configuring the Oracle SBC, ACLI, or GUI. For the purposes of this note, we'll provide both ACLI and WebGUI examples.

**Note : Oracle SBC which is configured for Service provider model does not support WebGUI and configuration can only be performed through ACLI.**

This guide assumes the Oracle SBC has been installed, management interface has been configured, product selected and entitlements have been assigned. If you require more information on how to install your SBC platform, please refer to the [ACLI configuration guide](#).

Any configuration parameter not specifically listed below can remain at the ORACLE SBC default value and does not require a change for connection to Zoom Phone to function properly, however this should note should be treated as basic guidelines and there may be a need to implement additional Oracle SBC configuration parameters in your production setup.

Contact your Oracle Sales representative if you require assistance in configuring the Oracle SBC.

**Note: All network parameters, ip addresses, hostnames etc..are specific to Oracle Labs, and cannot be used outside of the Oracle Lab environment. They are for example purposes only!!!**

## 6.2 Global Configuration Elements

Before you can configuration more granular parameters on the SBC, there are four global configuration elements that must be enabled (nap optional) to proceed.

- System-Config
- Media-manager-Config
- SIP-Config
- Ntp-config

### 6.2.1 System-Config

To configure 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 (*recommend using the management interface gateway for this global setting*)

Modify System Config

Hostname	zoom.us
Description	SBC for Zoom Cloud Voice
Location	Burlington MA
Mib System Contact	
Mib System Name	
Mib System Location	
Acp TLS Profile	

OK Delete

Page 1 of 1 (1 of 1 items) 1

Options	
Call Trace	<input type="checkbox"/> enable
Default Gateway	10.138.194.129
Restart	<input checked="" type="checkbox"/> enable
Telnet Timeout	0 (Range: 0..65535)
Console Timeout	n (Range: 0..65535)

OK Delete

- Click the OK at the bottom of the screen.

To configure system-config from ACLI –

ACLI Path: config t→system→system-config

system-config	
hostname	oraclesbc.com
description	SBC for Zoom Cloud Voice
location	Burlington, MA

- Perform a save and activate configuration for changes to take effect.

## 6.2.2 Media Manager

To configure media functionality on the SBC, you must first enable the global media manager

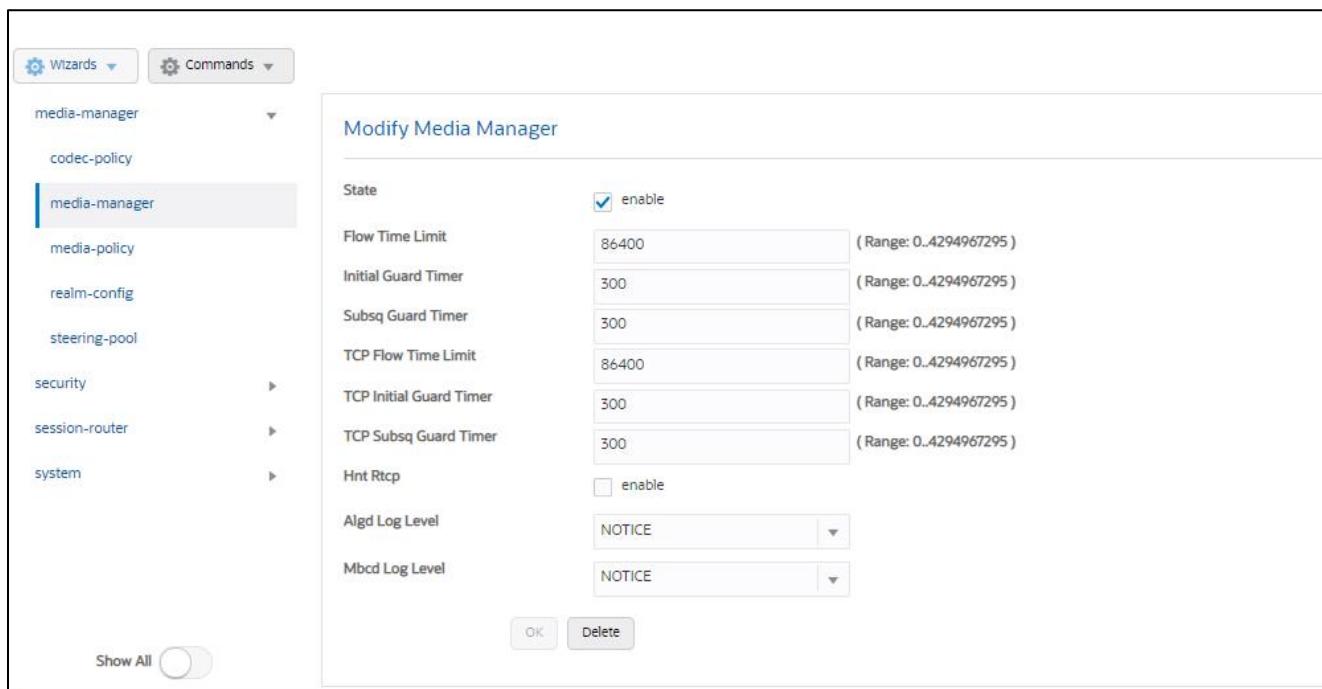
GUI Path: media-manager/media-manager

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

The following options are recommended for global media manager to help secure the SBC.

- Max-untrusted-signalling
- Min-untrusted-signalling

The values in both these fields are related to the SBC's security configuration. For more detailed security configuration options, please refer to the [SBC's Security Guide](#).



- Click OK at the bottom.

To enable media-manager from ACLI –

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

media-manager	
state	enabled

- Perform a save and activate configuration for changes to take effect.

### 6.2.3 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:

- Options: Click Add, in pop up box, enter the string: **inmanip-before-validate**
- Click Apply/Add another, then enter: **max-udp-length=0**
- Press OK in box
- Home Realm ID (Optional)

The screenshot shows the Oracle SBC configuration interface. The left sidebar lists various configuration categories like local-routing-config, media-profile, session-agent, etc., with 'sip-config' selected. The main area displays the 'Modify SIP Config' dialog with several tabs: General, Options, SPL Options, SIP Message Len, Enum Sag Match, Extra Method Stats, Extra Enum Stats, Registration Cache Limit, Register Use To For Lp, and Refer Src Routing.

**General Tab (Top Dialog):**

State	<input checked="" type="checkbox"/> enable
Dialog Transparency	<input checked="" type="checkbox"/> enable
Home Realm ID	Core_Zoom
Egress Realm ID	
Nat Mode	None
Registrar Domain	*
Registrar Host	*
Registrar Port	5060 (Range: 0;1025..65535)
Init Timer	500 (Range: 0.4294967295)
Max Timer	4000 (Range: 0.4294967295)
Trans Expire	32 (Range: 0.999999999)

**Options Tab (Bottom Dialog):**

Red Max Trans	10000 (Range: 0.50000)
Options	<input type="text"/> inmanip-before-validate <input type="button" value="X"/> <input type="text"/> max-udp-length=0 <input type="button" value="X"/>
SPL Options	
SIP Message Len	4096 (Range: 0..65535)
Enum Sag Match	<input type="checkbox"/> enable
Extra Method Stats	<input checked="" type="checkbox"/> enable
Extra Enum Stats	<input type="checkbox"/> enable
Registration Cache Limit	0 (Range: 0.999999999)
Register Use To For Lp	<input type="checkbox"/> enable
Refer Src Routing	<input checked="" type="checkbox"/> enable

- Click OK at the bottom

To configure sip config from ACLI.

ACLI Path: config t→session-router→sip-config

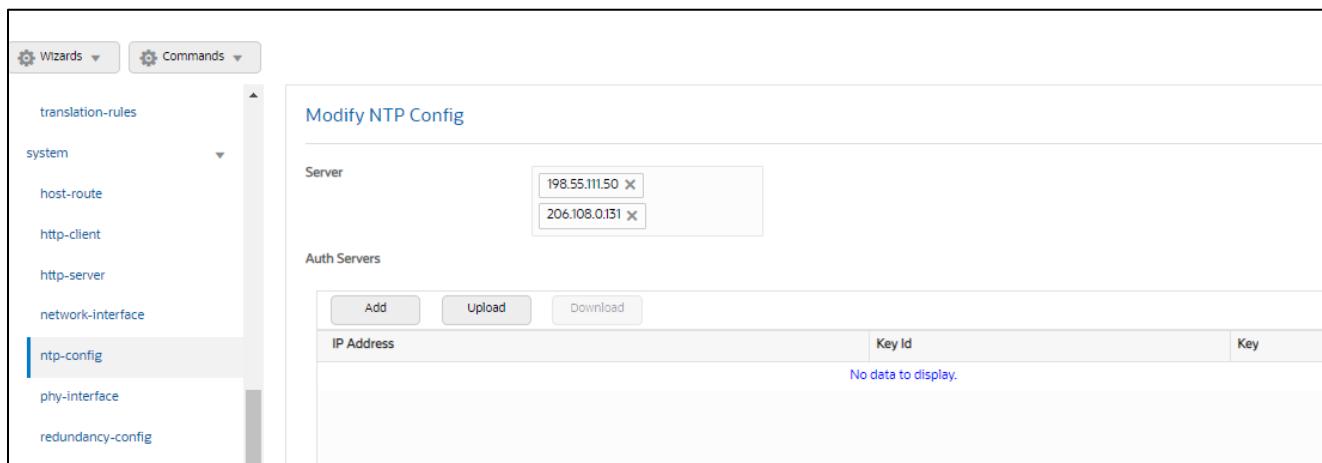
```
sip-config
  home-realm-id
  options
    Zoom
    max-udp-length=0
    inmanip-before-validate
```

- Perform a save and activate configuration for changes to take effect.

#### 6.2.4 NTP Config

GUI Path: system/ntp-config

ACLI Path: config t→system→ntp-config



- Click OK at the bottom

To configure ntp-config from ACLI –

ACLI Path: config t→system→ntp-sync

```
ntp-config
  server      216.239.35.0
```

- Perform a save and activate configuration for changes to take effect.

### 6.3 Network Configuration

To connect the SBC to network elements, we must configure both physical and network interfaces. For the purposes of this example, we will configure two physical interfaces, and two network interfaces. One to communicate with Zoom Cloud Voice, the other to connect to PSTN Network.

### 6.3.1 Physical Interfaces

GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

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

Config Parameter	Zoom	PSTN1	PSTN2
Name	s0p0	s1p0	s1p1
Operation Type	Media	Media	Media
Slot	0	1	1
Port	0	0	0

*Note: Physical interface names, slot and port may vary depending on environment*

Action	Select	Name	Operation Type	Port	Slot	Virtual Mac	Admin State	Auto Negotiation
:	<input type="checkbox"/>	s0p0	Media	0	0		enabled	enabled
:	<input type="checkbox"/>	s1p0	Media	2	0		enabled	enabled
:	<input type="checkbox"/>	s1p1	Media	3	0		enabled	enabled

- Click OK at the bottom of each after entering config information.

To configure phy-interface from ACCLI –

ACLI Path: config t→system→phy-interface

```
phy-interface
  name          s0p0
  operation-type Media
phy-interface
  name          s0p1
  operation-type Media
  port          1
phy-interface
  name          s1p0
  operation-type Media
  slot          1    slot
```

- Perform a save and activate configuration for changes to take effect.

### 6.3.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

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

Configuration Parameter	Zoom	PSTN1	PSTN2
Name	s0p0	s1p0	s1p1
Hostname	Domain (if applicable)		
IP Address	155.212.214.177	172.18.0.201	192.168.1.10
Netmask	255.255.255.0	255.255.0.0	255.255.255.0
Gateway	155.212.214.1	172.18.0.1	192.168.1.1
DNS Primary IP	8.8.8.8		
DNS Domain	Domain(if applicable)		

The screenshot shows the Zte GUI configuration interface. On the left, there is a navigation tree with items like media-manager, security, session-router, system (which is expanded), fraud-protection, host-route, http-client, http-server, network-interface (which is selected and highlighted in blue), and ntp-config. At the top right, there are buttons for Discard, Verify, and Save. The main area is titled 'Network Interface' and contains a table with the following data:

Action	Select	Name	Sub Port Id	Description	Hostname	IP Address	Pri Utility Addr
⋮	<input type="checkbox"/>	s0p0	0			155.212.214.177	
⋮	<input type="checkbox"/>	s1p0	0			172.18.0.201	
⋮	<input type="checkbox"/>	s1p1	0			192.168.1.10	

- Click OK at the bottom of each after entering config information

To configure network-interface from ACLI –

ACLI Path: config t→system→network-interface

```
network-interface
  name          s0p0
  ip-address    155.212.214.177
  netmask       255.255.255.192
  gateway       155.212.214.1
  dns-ip-primary 8.8.8.8
  dns-domain    solutionslab.cgbuburlington.com

network-interface
  name          s1p0
  ip-address    172.18.0.201
  netmask       255.255.0.0
  gateway       172.18.0.1

network-interface
  name          s1p1
  ip-address    192.168.1.10
  netmask       255.255.255.0
  gateway       192.168.1.1
```

- Perform a save and activate configuration for changes to take effect.

## 6.4 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Zoom Phone Platform

Zoom Phone allows UDP or TLS connections from SBC's for SIP traffic, and RTP or SRTP for media traffic. For our testing, the connection between the Oracle SBC and Zoom Phone platform was secured via TLS/SRTP. This setup requires a certificate signed by one of the trusted Certificate Authorities.

### 6.4.1 Certificate Records

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

This 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'll create Five certificate records. They are as follows:

- SBC Certificate (end-entity certificate)
- DigiCertGlobalRootCA- In our setup SBC certificate is signed from DigiCertGlobalRootCA
- DigiCert Intermediate Cert (this is optional – only required if your server certificate is signed by an intermediate). In our setup we have DigiCert SHA2 Secure Server CA as the Intermediate CA.

These Certificates can be downloaded at below links –

- <https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem>
- <https://www.digicert.com/kb/digicert-root-certificates.htm#intermediates>

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>

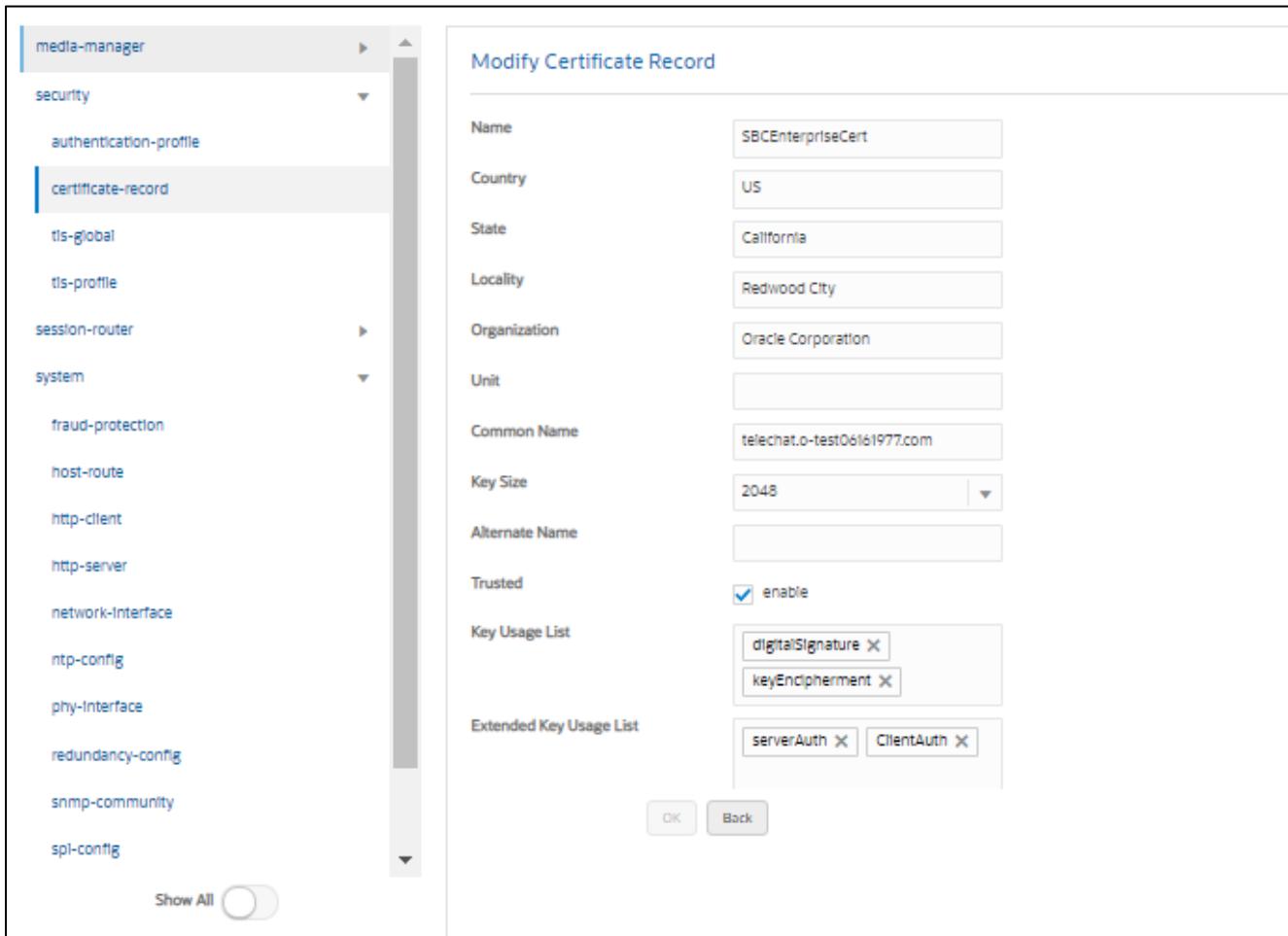
#### 6.4.2 SBC End Entity Certificate

The SBC's end entity certificate is what is presented to Zoom Phone signed by your CA authority which is trusted by Zoom (Please see section 6.5.1 for detailed Zoom Supported CA Vendors), in this example we are using Digicert as our signing authority. The certification must include a common name. For this, we are using an fqdn as the common name.

- Common name: (**telechat.o-test06161977.com**)

To Configure the certificate record:

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



- Click OK at the bottom
- Next, using this same procedure, configure certificate records for Root CA and Intermediate Certificates

To configure certificate-record from ACLI –

ACLI Path: config t→security→certificate-record

```
certificate-record
  name          SBCEnterpriseCert
  state         California
  locality      Redwood City
  organization   Oracle Corporation
  unit          Oracle CGBU
  common-name    telechat.o-test06161977.com
  extended-key-usage-list
                serverAuth
                ClientAuth
```

- Perform a save and activate configuration for changes to take effect.

- Next, using this same procedure, configure certificate records for the Root CA certificates

#### **6.4.3 Root CA and Intermediate Certificates**

The following, DigitCertRootGlobalRootCA and DigiCert SHA2 Secure Server CA are the root and intermediate CA certificates used to sign the SBC's end entity certificate.

To trust Zoom certificates, your SBC must have below DigiCert Global Root CA, DigiCert Global Root G2 and DigiCert Global Root G3 installed.

**Note : Since both Oracle SBC and Zoom use DigiCert Global Root CA only one certificate record should be created for the DigiCert Global Root CA certificate.**

Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

Config Parameter	Digicert Intermediate	DigiCertGlobalRootCA	DigiCertGlobalRootG2	DigiCertGlobalRootG3
Common Name	DigiCert SHA2 Secure Server CA	DigiCert Global Root CA	DigiCert Global Root G2	DigiCert Global Root G3
Key Size	2048	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256	Sha256

#### **6.4.4 Zoom Approved CA Vendors**

Below is the list of Zoom approved CA Vendors. Oracle SBC Certificate can be signed by any of these Certificate Authorities.

Certificate Issuer Organization	Common Name or Certificate Name
Buypass AS-983163327	Buypass Class 2 Root CA
Buypass AS-983163327	Buypass Class 3 Root CA
Baltimore	Baltimore CyberTrust Root
Cybertrust, Inc	Cybertrust Global Root
DigiCert Inc	DigiCert Assured ID Root CA

DigiCert Inc	DigiCert Assured ID Root G2
DigiCert Inc	DigiCert Assured ID Root G3
DigiCert Inc	DigiCert Global Root CA
DigiCert Inc	DigiCert Global Root G2
DigiCert Inc	DigiCert Global Root G3
DigiCert Inc	DigiCert High Assurance EV Root CA
DigiCert Inc	DigiCert Trusted Root G4
GeoTrust Inc.	GeoTrust Global CA
GeoTrust Inc.	GeoTrust Primary Certification Authority
GeoTrust Inc.	GeoTrust Primary Certification Authority - G2
GeoTrust Inc.	GeoTrust Primary Certification Authority - G3
GeoTrust Inc.	GeoTrust Universal CA
GeoTrust Inc.	GeoTrust Universal CA 2
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G6
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G6
Thawte, Inc.	Thawte Primary Root CA
Thawte, Inc.	Thawte Primary Root CA - G2
Thawte, Inc.	Thawte Primary Root CA - G3
VeriSign, Inc.	VeriSign Class 1 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 2 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G4
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign, Inc.	VeriSign Universal Root Certification Authority
AffirmTrust	AffirmTrust Commercial
AffirmTrust	AffirmTrust Networking
AffirmTrust	AffirmTrust Premium

AffirmTrust	AffirmTrust Premium ECC
Entrust, Inc.	Entrust Root Certification Authority
Entrust, Inc.	Entrust Root Certification Authority - EC1
Entrust, Inc.	Entrust Root Certification Authority - G2
Entrust, Inc.	Entrust Root Certification Authority - G4
Entrust.net	Entrust.net Certification Authority (2048)
GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign nv-sa	GlobalSign Root CA
The GoDaddy Group, Inc.	Go Daddy Class 2 CA
GoDaddy.com, Inc.	Go Daddy Root Certificate Authority - G2
Starfield Technologies, Inc.	Starfield Class 2 CA
Starfield Technologies, Inc.	Starfield Root Certificate Authority - G2
QuoVadis Limited	QuoVadis Root CA 1 G3
QuoVadis Limited	QuoVadis Root CA 2
QuoVadis Limited	QuoVadis Root CA 2 G3
QuoVadis Limited	QuoVadis Root CA 3
QuoVadis Limited	QuoVadis Root CA 3 G3
QuoVadis Limited	QuoVadis Root Certification Authority
Comodo CA Limited	AAA Certificate Services
AddTrust AB	AddTrust Class 1 CA Root
AddTrust AB	AddTrust External CA Root
COMODO CA Limited	COMODO Certification Authority
COMODO CA Limited	COMODO ECC Certification Authority
COMODO CA Limited	COMODO RSA Certification Authority
The USERTRUST Network	USERTrust ECC Certification Authority
The USERTRUST Network	USERTrust RSA Certification Authority

T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 2
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 3

#### 6.4.5 Generate Certificate Signing Request

Now that the SBC's certificate has been configured, create a certificate signing request for the SBC's end entity only.

This is not required for any of the Root CA or intermediate certificates that have been created.

On the certificate record page in the Oracle SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:

Name	Country	State	Locality	Organization	Unit	Common Name
DigiCertinter	US	MA	Burlington	Engineering		DigiCert SHA2 Secure Server CA
DigiCertRoot	US	MA	Burlington	Engineering		DigiCert Global Root CA
GoDaddyInter	US	MA	Burlington	Engineering		GoDaddy Secure Server CA
GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 Root CA
SBCEnterpriseCert	California	Redwood City	Oracle Corporation			telechat.o-test06@1977.com

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC3zCCAQCAQAwfDELMkGA1UEBhMCVVMMxEzARBgNVBAgTCKNhblGmb3JuawEx
FTATBgNVBACDFJZlhdzbzQgQ20eTEBMDkGA1UEChMS3Ihy2xElNvnbVcmFO
awWuhs5QwIyDVQQDEx0zWxly2hdC5vLXRic3QwINIE2MTK3NySjb20wggEIMAOG
CSqG5b3DQEBAQUA44BDwAwIBgEKADIBAQDX+fmNshibPcdz6-HyGU7VYwgtjII
M4t2yvUp35a1le-wxTLGAjkCB1Tsp0h-nm49k4x3p8thGz9dXf7o22T2Z0
1UBj2utfXn+ExXgJ2HKuPMEBp23L3Xn+b4hpv+ICPus584-1D7kHLq9DtsAR
Bl74qQz0tXUJOFOwanAWLKD0TeQjkiR8/vuLGB/C1gaIPVz/TQQFLpLgvngk
IffgGdjkGnddkLs53BpYQglnoVVCBhyKgH2N0TBzQGyzL42mmAjetAGmBA-Agg
HIAcBqkjhkG9BCQ4xDzANMASGA1ldDwQEAWFoDA1BqkjhkG9wD8-QsFAAO
AQEA2Rwqj22zLDhQfLVEP02oLT01tGALew2hDVfR84-ImYBrotvb/nmh754
4TfzvngolNrsd0fGRQF87ElnRK//WIBhGzB0GKIEJRSPGsrnwNEfokx+Fw
rk4969Ks4NEY45SKPGozyUSLSlUXtYkQkTQENhch2zQcTs/xtnaNH/kLYN
xt2krpZWmAPE0mc+x0CAEdDsriYdgPfAECdzpUv40A/a1qAO79RctFEDh+
sglN8r+3a(Csu7wtwouUhGLPgJbd1EcLyPpsCrxFufx8UR03meo8+IcuHP
FNV569LSO/D-M/w2kxrPlof=#
-----END CERTIFICATE REQUEST-----

```

- 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.

To Perform the Steps From ACLI use the below command –

#### **generate-certificate-request SBCEnterpriseCert**

This Step generates a text on Screen as shown below –

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC4zCCAcsCAQAwazELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQ
HEwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmIuZzEkMCIGA1UEAxMbdGVs
ZWNoYXQuby10ZXN0MDYxNjE5NzcuY29tMIIIBljANBqkqhkiG9w0BAQEFAOCAQ8A
MIIBCgKCAQEAr3AmjF15PclcWiB/kFEExUGNHQHlbkJi28MDbcprO/KLXIHQysSnw
UWz34XLBfLQ6rS4MLyEMR8Nt8GGNSIWKiR431LsX7L+yGWvRjcBFP6DIHtH0Vuqm
ixVaUJpg5luPY6SvT1shyu26iLIBsLfem43tbKq5jz/jrvaUzyhICvAQ23c1oS5a
D4UiF2mNOuSqvmkx50a3/BNYbKecLNOxvKQyyTMggfNpASbZuW+eMEUKI5iB+AB
/AAoZRP4bn4qlE3wn8pJsNm8Pjxy4hbz24ySgmaN9iXpP1FdRw0TemfCsNazZRuK
DsviWJfunZYTzRfDe5pJToMH4u1zt2fK1QIDAQABoDMwMQYJKoZlhvcNAQkOMSQw
IjALBgNVHQ8EBAMCBaAwEwYDVR0IBAwCgYIKwYBBQUHAwEwDQYJKoZlhvcNAQEL
BQADggEBADD5Y+u08LxmTMIsJ2Rjc8cgPZocTqBDXN0tp27S4FuB/01ikBBdG3YV
Ffp7/Q8ZeFHgU/rMzeF8Gpo9Cc6JUGGux3/ws8ZkgRBxsNIG276i7pFN1vCljEP
89AGxtryioRMc4kcdPpLJNQ10Qx1zKobHMTftGLDI6jN2pvn3zYHH8qA9V/1/yKa
3n0j33EuTrvTIQ5P4IgyVJqSBkdl29T1gXY6O8JVFLCQefTrF4TLc6teNzxXMdPw
PHoPu9hM3scGOWOHQnODXOFeq2AxBQzAa0/Cjf7Bw3l3POmMcIOawgDecZ8UjHpJ
IznX9/Gxg5X+S2QkHjNmPK+JuePqX4I=
-----END CERTIFICATE REQUEST-----
```

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, **another save and activate is required** before you can import the certificates to each certificate record created above.

Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

#### **6.4.6 Import Certificates to SBC**

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

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

The screenshot shows two views of the SBC Enterprise configuration interface. The top view displays a list of certificates under 'certificate-record'. A context menu is open over the 'SBCEnterpriseCert' entry, with the 'Import' option highlighted by a red arrow. The bottom view shows the 'Import certificate' dialog box, which includes fields for 'Format' (set to 'p12'), 'Import method' (set to 'try-all'), and a 'Certificate file' input field where a file can be uploaded. The background shows the same certificate list as the top view.

Name	Country	State	Locality	Organization	Unit	Common Name
DigiCertInter	US	MA	Burlington	Engineering		DigiCert SHA2 Secure Server CA
DigiCertRoot	US	MA	Burlington	Engineering		DigiCert Global Root CA
GoDaddyInter	US	MA	Burlington	Engineering		GoDaddy Secure Server CA
GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 Root CA
SBCEnterpriseCert	US	California	Redwood City	Oracle Corporation		telechat.o-test06161977.com

Repeat these steps to import all the root and intermediate CA certificates into the SBC:

- DigiCertIntermediate
- DigiCertGlobalRootCA
- DigiCertGlobalRootG2
- DigiCertGlobalRootG3

At this stage, all required certificates have been imported.

To import the certificate from ACLI follow below procedure -

```
import-certificate try-all SBCEnterpriseCert
```

The System will show a prompt as below -

**IMPORTANT:**

Please enter the certificate in the PEM format.

Terminate the certificate with ";" to exit.....

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIC4zCCAcCAQAwazELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH  
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEkMCIGA1UEAxMbdGVs  
ZWNoYXQuby10ZXN0MDYxNjE5NzcuY29tMIIBljANBgkqhkiG9w0BAQEFAOCAQ8A  
MIIIBgKCAQEAr3AmjF15PclcWiB/kFExUGNHQHlbkJi28MDbcprO/KLXIHQysSnw  
UWz34XLBfLQ6rS4MLyEMR8Nt8GGNSIWKiR431LsX7L+yGWvRjcBFP6DIHtH0Vuqm  
ixVaUJpg5luPY6SvT1shyu26iLIBsLfem43tbKq5jz/jrvaUzyhICvAQ23c1oS5a  
D4UiF2mNOuSqxvmkx50a3/BNYbKecLNOxvKQyyTMgffNpASbZuW+eMEUKI5iB+AB  
/AAoZRP4bn4qlE3wn8pJsNm8Pjxy4hbz24ySgmaN9iXpP1FdRw0TemfCsNazZRuK  
DsViWJfunZYTzRfDe5pJToMH4u1zt2fK1QIDAQABoDMwMQYJKoZlhvcNAQkOMSQw  
IjALBgNVHQ8EBAMCBaAwEwYDVR0IBAwwCgYIKwYBBQUHAwEwDQYJKoZlhvcNAQEL  
BQADggEBADD5Y+u08LxmTMIsJ2Rjc8cgPZocTqBDXN0tp27S4FuB/01ikBBdG3YV  
Ffp7/Q8ZeFHHgU/rMzeF8Gpo9Cc6JUGGux3/ws8ZkgRBxsNIG276i7pFN1vCljEP  
89AGxtryioRMc4kcdPpLJNQ10Qx1zKobHMTftGLDI6jN2pvn3zYHH8qa9V/1/yKa  
3n0j33EuTrvTIQ5P4lgyVJqSBndl29T1gXY6O8JVFLCQefTrF4TLc6teNzxXMdPw  
PHoPu9hM3scGOWOHQnODXOFeq2AxBQzAa0/Cjf7Bw3l3POmMcIOawgDecZ8UjHpJ  
lznX9/Gxg5X+S2QkHjNmPK+JuePqX4I=
```

```
-----END CERTIFICATE REQUEST-----;
```

**save and activate** your configuration.

Repeat these steps to import all the root and intermediate CA certificates into the SBC.

#### 6.4.7 TLS Profile

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

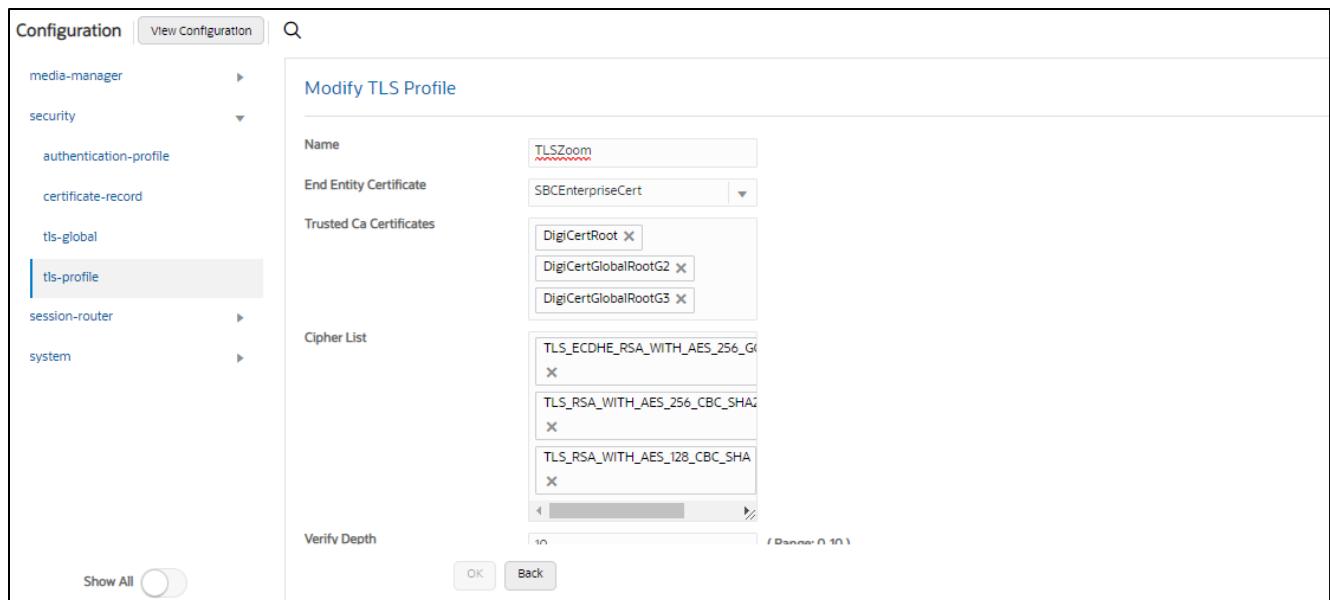
GUI Path: security/tls-profile

ACLI Path: config t→security→tls-profile

- Click Add, use the example below to configure

Zoom Cloud Peering supports the following signalling ciphers that need to be added to the TLS profile:

**TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384**  
**TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256**  
**TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA**



- Click OK at the bottom

To configure tls-profile from ACLI –

ACLI Path: config t→security→tls-profile

```
tls-profile
  name          TLSZoom
  end-entity-certificate  SBCEnterpriseCert
  trusted-ca-certificates  DigiCertRoot
                            DigiCertGlobalRootG2
                            DigiCertGlobalRootG3
  cipher-list    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
                  TLS_RSA_WITH_AES_256_CBC_SHA256
                  TLS_RSA_WITH_AES_128_CBC_SHA
  mutual-authenticate  enabled
```

- Perform a save and activate configuration for changes to take effect.
-

## 6.5 Media Security Configuration

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

### 6.5.1 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.

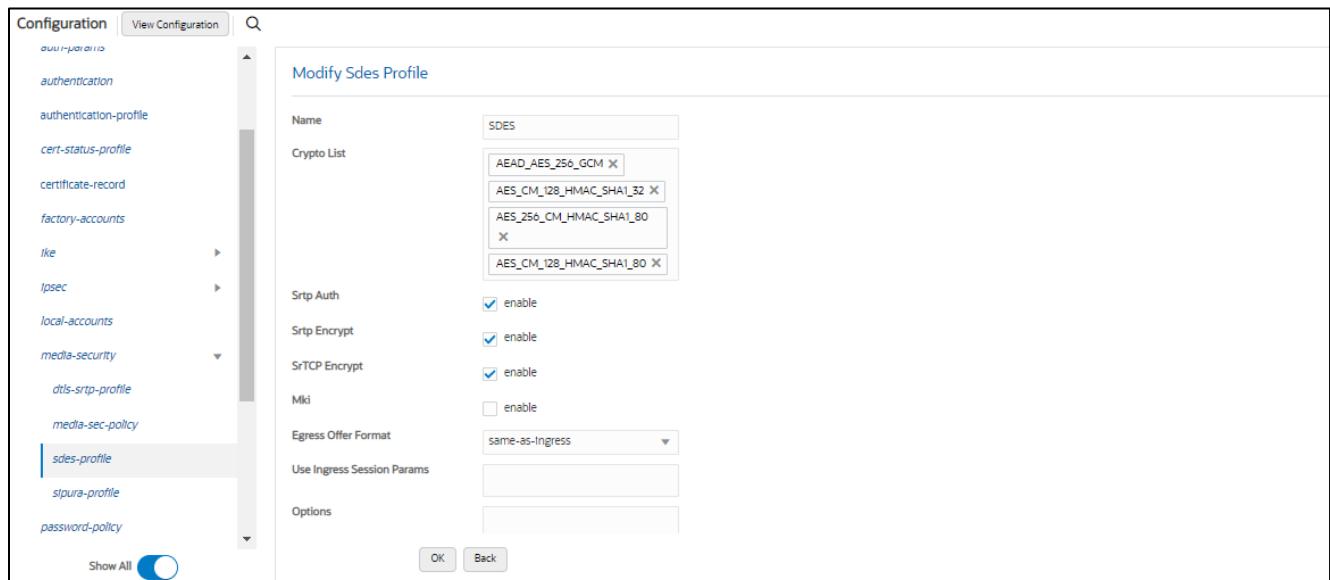
GUI Path: security/media-security/sdes-profile

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

Oracle SBC and Zoom Cloud Voice Support the following media ciphers for SRTP:

AEAD\_AES\_256\_GCM  
AES\_CM\_256\_HMAC\_SHA1\_80  
AES\_CM\_128\_HMAC\_SHA1\_80  
AES\_CM\_128\_HMAC\_SHA1\_32

Click Add, and use the example below to configure.



- Click OK at the bottom

To configure sdes-profile from ACI –

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

```

sdes-profile
  name          SDES
  crypto-list   AEAD_AES_256_GCM
                AES_CM_128_HMAC_SHA1_32
                AES_256_CM_HMAC_SHA1_80
                AES_CM_128_HMAC_SHA1_80

```

- Perform a save and activate configuration for changes to take effect.

### 6.5.2 Media Security Policy

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

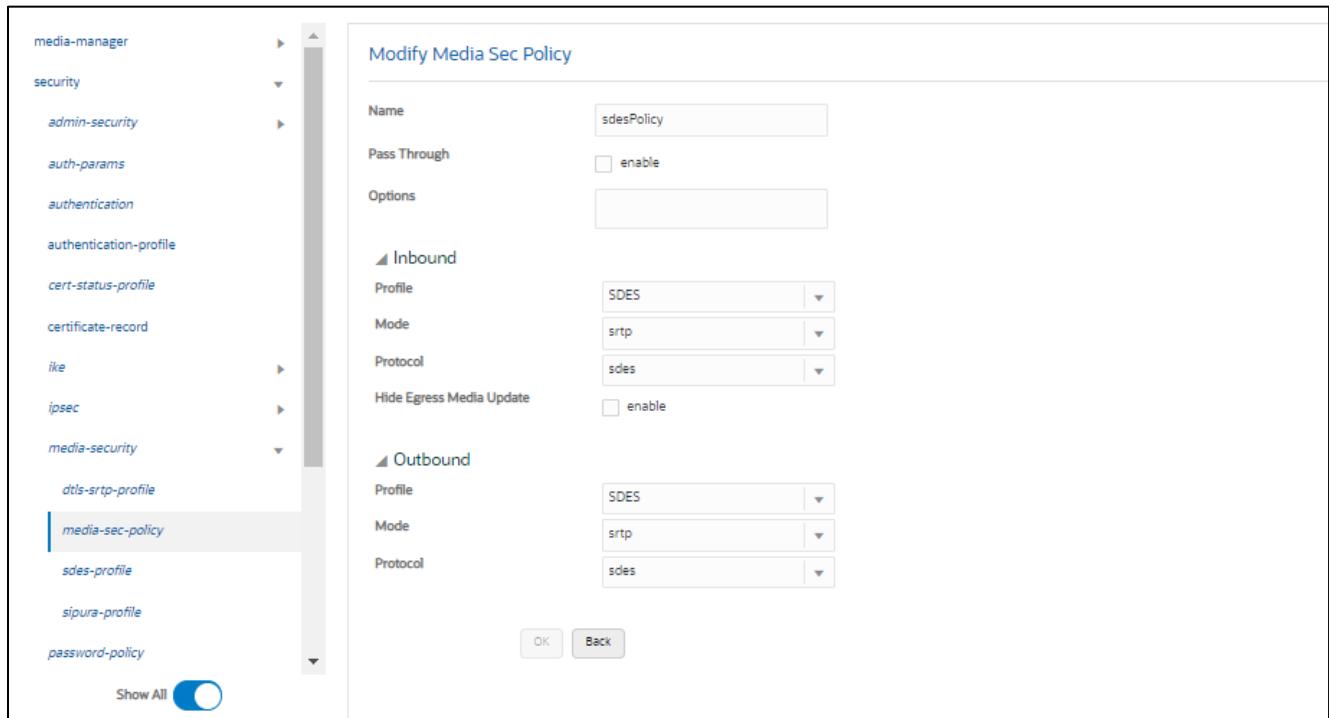
In this example, we are configuring two media security policies. One to secure and decrypt media toward Zoom, the other for non-secure media facing PSTN.

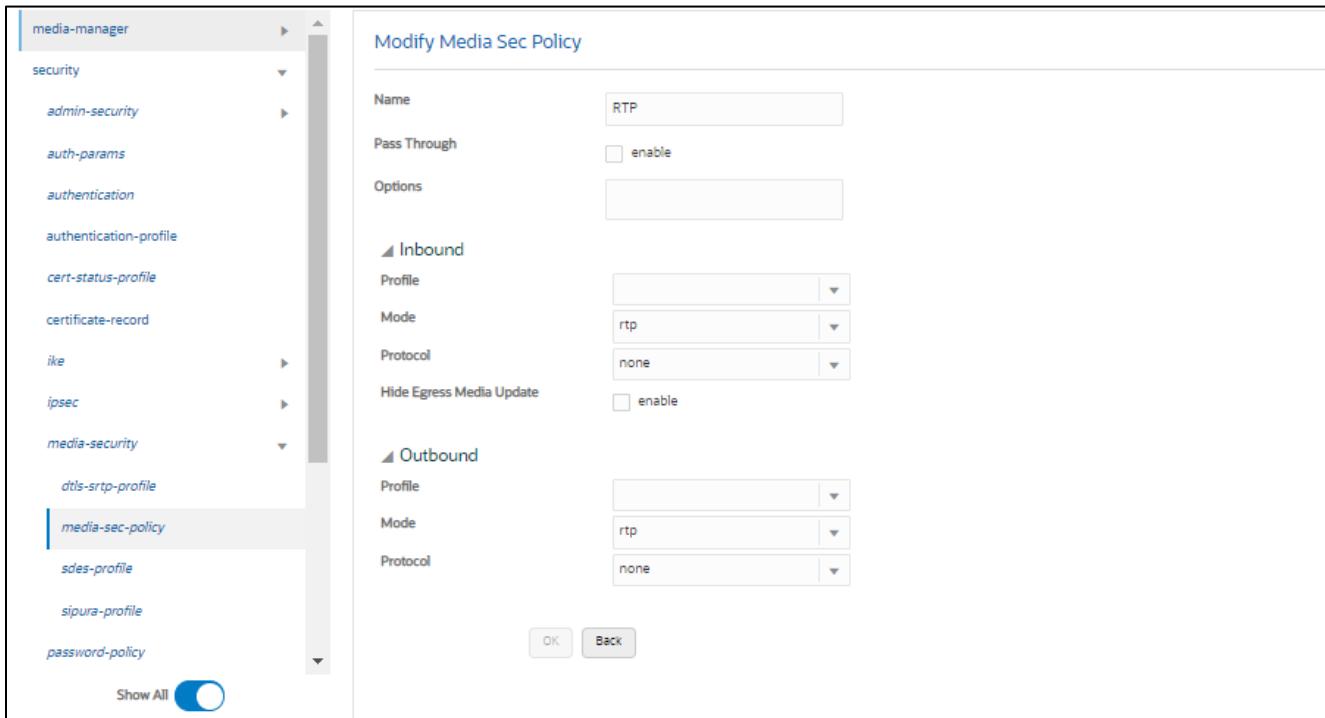
These are named as sdesPolicy and RTP.

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





To configure media security from ACLI.

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

```
media-sec-policy
  name RTP
media-sec-policy
  name sdesPolicy
  inbound
    profile SDES
    mode srtp
    protocol sdes
  outbound
    profile SDES
    mode srtp
    protocol sdes
```

- Perform a save and activate configuration for changes to take effect.

## 6.6 Media Configuration

This section will guide you through the configuration of realms and steering pools, both of which are required for the SBC to handle signaling and media flows toward Zoom and PSTN.

### 6.6.1 Realm Config

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.

#### Zoom Realm

This is a standalone realm facing Zoom Phone Platform

#### PSTN Realms

In the below example 1, Peer\_SIPTrunk1 represents the Sip realm for customer 1. Similarly another realm is created for Peer\_SIPTrunk2 which represents the Sip Trunk for customer 2. These realms are bound to different network interfaces (subnets) in this example.

GUI Path: media-manager/realm-config

ACLI Path: config t→media-manager→realm-config

- Click Add, and use the following table as a configuration example for the three realms used in this configuration example

Config Parameter	Zoom Phone	PSTN Realm1	PSTN Realm2
Identifier	Core_Zoom	Peer_SIPTrunk1	Peer_SIPTrunk2
Network Interface	s0p0:0	s1p0:0	s1p1:0
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access-control-trust-level	High	High	High
Media Sec policy	sdespolicy	RTP	RTP

Also notice, the realm configuration is where we assign some of the elements configured earlier in this document, i.e.

- Network interface
- Media security policy

The screenshot shows the Configuration interface with the left sidebar expanded to show categories like media-manager, codec-policy, media-manager, media-policy, realm-config, steering-pool, security, session-router, and system. The 'realm-config' section is selected. The main area displays a table titled 'Realm Config' with the following data:

Action	Select	Identifier	Description	Addr Prefix	Network Interfaces	Media Realm List	Mm In Realm	Mm In Network
⋮	<input type="checkbox"/>	Core_Zoom		0.0.0.0	s0p0:0.4		enabled	enabled
⋮	<input type="checkbox"/>	Peer_SIPTrunk1		0.0.0.0	s1p0:0.4		enabled	enabled
⋮	<input type="checkbox"/>	Peer_SIPTrunk2		0.0.0.0	s1p1:0.4		enabled	enabled

At the bottom of the table, it says 'Displaying 1 - 3 of 3'.

To configure realm-config from ACLI –

ACLI Path - config t→media-manger→realm-config

```

realm-config
  identifier          Core_Zoom
  network-interfaces s0p0:0.4
  mm-in-realm        enabled
  media-sec-policy   sdesPolicy
  out-manipulationid ZoomOutManip
  access-control-trust-level high

realm-config
  identifier          Peer_SIPTrunk1
  network-interfaces s1p0:0.4
  mm-in-realm        enabled
  media-sec-policy   RTP
  access-control-trust-level high

realm-config
  identifier          Peer_SIPTrunk2
  network-interfaces s1p1:0.4
  mm-in-realm        enabled
  media-sec-policy   sdesPolicy
  access-control-trust-level high

```

- Perform a save and activate configuration for changes to take effect.

## 6.6.2 Steering Pools

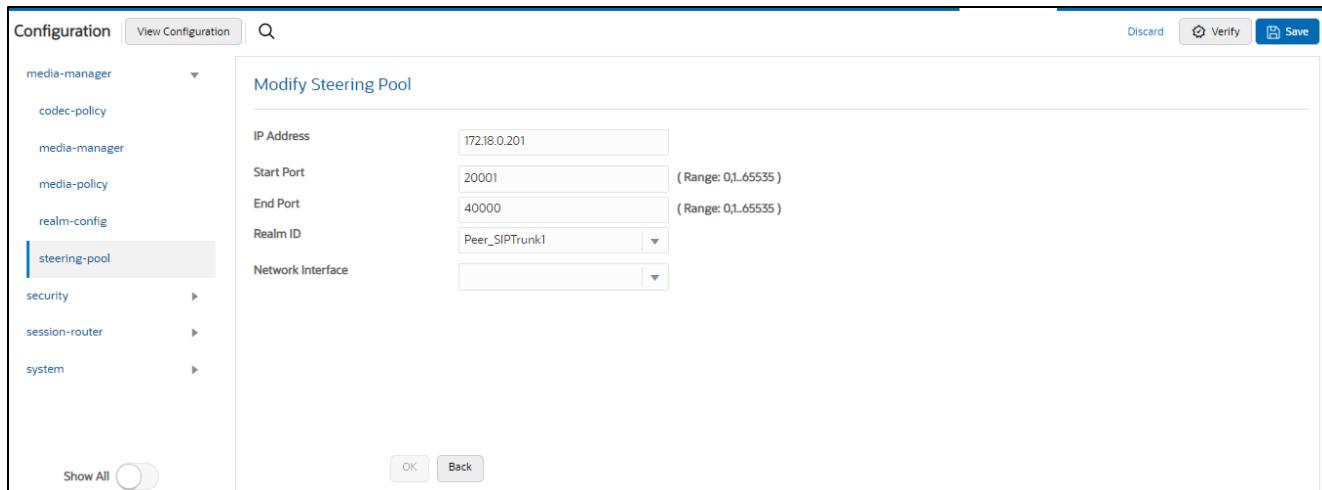
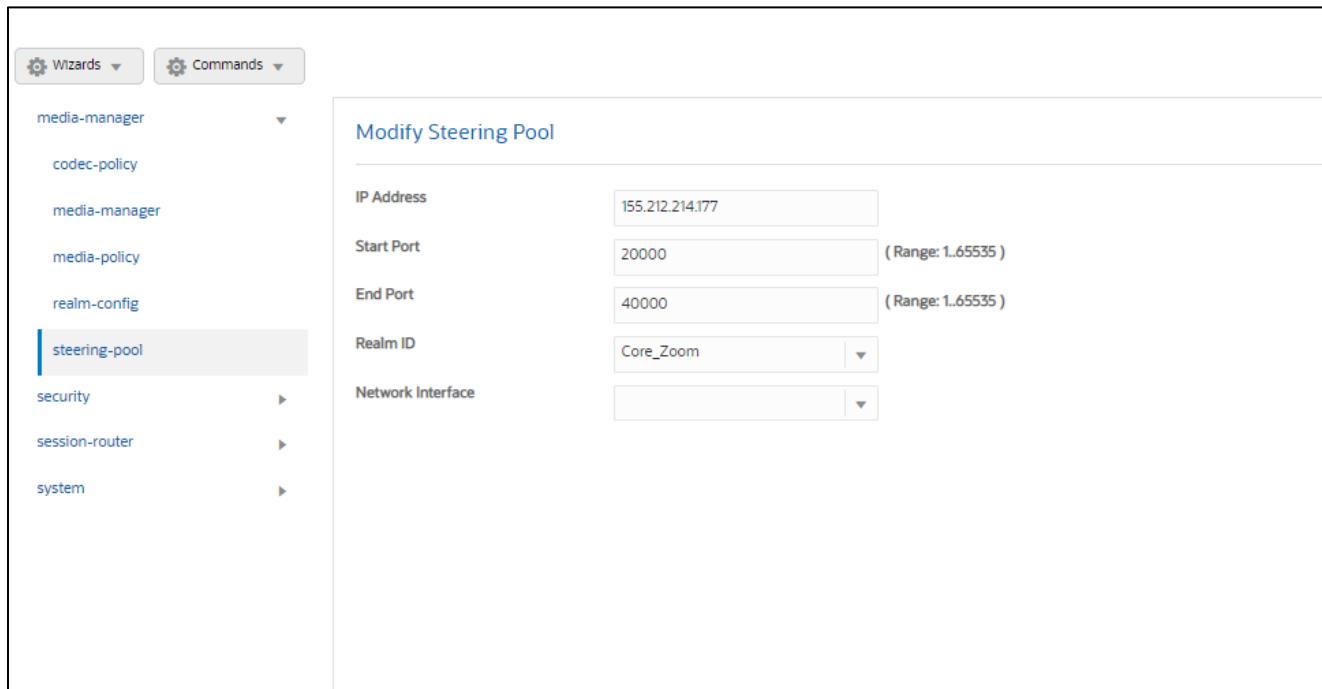
Steering pools define sets of ports that are used for steering media flows through the Oracle SBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We will configure one steering pool for both PSTN Trunks and one steering pool for Zoom Phone

GUI Path: media-manager/steering-pool

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

- Click Add, and use the below examples to configure



Configuration View Configuration Q

Discard Verify Save

media-manager  
codec-policy  
media-manager  
media-policy  
realm-config  
**steering-pool**  
security  
session-router  
system

**Modify Steering Pool**

IP Address	192.168.1.10
Start Port	40001 (Range: 0..65535)
End Port	60000 (Range: 0..65535)
Realm ID	Peer_SIPTrunk2
Network Interface	

To configure steering-pool from ACLI

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

```
steering-pool
  ip-address      155.212.214.177
  start-port     10000
  end-port       20000
  realm-id       Core_Zoom
steering-pool
  ip-address      172.18.0.201
  start-port     20001
  end-port       40000
  realm-id       Peer_SIPTrunk1
steering-pool
  ip-address      192.168.1.10
  start-port     40001
  end-port       60000
  realm-id       Peer_SIPTrunk2
```

- Perform a save and activate configuration for changes to take effect.

## 6.7 SIP Modifications

This section outlines the configuration parameters required for processing, modifying, and securing SIP signaling traffic.

### 6.7.1 SIP Manipulations

In order to comply with the signaling message requirements of Carrier and Zoom we have applied following sip-manipulations towards Zoom Side.

**Note:** You may have to build sip-manipulations to cover the signaling requirement from Carrier Trunk.

#### 6.7.1.1 Manipulation towards Zoom Side

For calls to be presented to Zoom Phone from the Oracle SBC Zoom expects providers to deliver E.164 formatting in all headers which contain a PSTN routable number.

Besides, Options ping from carrier peering SBC to Zoom must be formatted as follows. The same formatting is to be followed for calls.

- The “**From**” header must have the IP address/FQDN of the Oracle SBC  
From: <sip:IPaddress/FQDN>
- The “**To**” header must contain the Zoom Phone IP address/FQDN  
To: <sip:IPaddressofZoomSBC>
- The “**Request URI**” header must contain the Zoom Phone IP address/FQDN
- The “**Contact**” header must have the IP address/FQDN of the Oracle SBC  
Contact: <sip:IPaddress/FQDN:PortNumber>
- P-Preferred-Identity headers should be converted to P-Asserted-Identity by the provider before sending to Zoom
- Remote-Party-ID headers are considered deprecated, and providers should convert RPID headers to P-Asserted-Identity headers before sending messages to Zoom.
- SIP REFER is not currently supported by Zoom for transferring or forwarding calls. Zoom uses Re-Invite mechanism for call transfers/forwarding.

To achieve this we have created following Header manipulation rule on Oracle SBC.

## Sip-manipulation :

Configuration View Configuration Q

Modify SIP Manipulation

Name: ZoomCP

Description:

Split Headers:

Join Headers:

CfgRules

Action	Select	Name	Element Type
:	<input type="checkbox"/>	addPlus	header-rule
:	<input type="checkbox"/>	ChangeTO	header-rule
:	<input type="checkbox"/>	ChangeFrom	header-rule

Discard Verify Save Show Configuration

### Header-rule #1

Configuration View Configuration Q

Modify Sip manipulation / header rule

Name: addPlus

Header Name: Request-URI

Action: manipulate

Comparison Type: pattern-rule

Msg Type: request

Methods: invite

Match Value:

New Value:

CfgRules

Action	Select	Name	Element Type
:	<input type="checkbox"/>	TenDigits	element-rule
:	<input type="checkbox"/>	ElevenDigits	element-rule

Discard Verify Save

### Element-rule # 1.1

Configuration | View Configuration |

local-routing

local-routing-config

local-policy

local-routing-config

media-profile

session-agent

session-group

session-recording-group

session-recording-server

session-translation

sip-config

Modify Sip manipulation / header rule / element rule

Name	TenDigits
Parameter Name	
Type	url-user
Action	replace
Match Val Type	any
Comparison Type	pattern-rule
Match Value	^[0-9]{10}\$
New Value	\+1+\$ORIGINAL

### Element-rule #1.2

Configuration | View Configuration |

local-routing

local-routing-config

local-policy

local-routing-config

media-profile

session-agent

session-group

session-recording-group

session-recording-server

session-translation

sip-config

Modify Sip manipulation / header rule / element rule

Name	ElevenDigits
Parameter Name	
Type	url-user
Action	replace
Match Val Type	any
Comparison Type	pattern-rule
Match Value	^[0-9]{11}\$
New Value	\+1+\$ORIGINAL

### Header-rule #2

Configuration | View Configuration |  | Discard | Verify | Save

**Modify Sip manipulation / header rule**

Name	ChangeTO
Header Name	TO
Action	manipulate
Comparison Type	case-sensitive
Msg Type	request
Methods	invite X
Match Value	
New Value	

CfgRules

Action	Select	Name	Element Type
⋮	<input type="checkbox"/>	changetohost	element-rule
⋮	<input type="checkbox"/>	ChangeToPort	element-rule

### Element-rule #2.1

Configuration | View Configuration |  | Discard | Verify | Save

**Modify Sip manipulation / header rule / element rule**

Name	changetohost
Parameter Name	
Type	url-host
Action	replace
Match Val Type	any
Comparison Type	case-sensitive
Match Value	
New Value	\$REMOTE_IP

### Element-rule #2.2

**Configuration** | [View Configuration](#) |

- [inter-luring](#)
- [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](#)

**Modify Sip manipulation / header rule / element rule**

Name	ChangeToPort
Parameter Name	
Type	uri-port
Action	replace
Match Val Type	any
Comparison Type	case-sensitive
Match Value	
New Value	5061

### Header-rule #3

**Configuration** | [View Configuration](#) |  | Discard | Verify

- [inter-luring](#)
- [ldap-config](#)
- [local-policy](#)
- [local-routing-config](#)
- [media-profile](#)
- [session-agent](#)
- [session-group](#)
- [session-recording-group](#)
- [session-recording-server](#)
- [session-translation](#)
- [sip-config](#)
- [sip-feature](#)
- [sip-Interface](#)
- [sip-manipulation](#)
- [sip-monitoring](#)
- [translation-rules](#)

**Modify Sip manipulation / header rule**

Name	ChangeFromHost
Header Name	From
Action	manipulate
Comparison Type	case-sensitive
Msg Type	request
Methods	invite X   OPTIONS X
Match Value	
New Value	

**CfgRules**

Action	Select	Name	Element Type
:	<input type="checkbox"/>	ChangeFromHost	element-rule
:	<input type="checkbox"/>	ChangeFromPort	element-rule

### Element-rule #3.1

Configuration | View Configuration | Q

Modify Sip manipulation / header rule / element rule

Name	ChangeFromHost
Parameter Name	
Type	url-host
Action	replace
Match Val Type	any
Comparison Type	case-sensitive
Match Value	
New Value	20.96.25.165

incoming

- 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

### Element-rule #3.2

Configuration | View Configuration | Q

Modify Sip manipulation / header rule / element rule

Name	ChangeFromPort
Parameter Name	
Type	url-port
Action	replace
Match Val Type	any
Comparison Type	case-sensitive
Match Value	
New Value	5061

incoming

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

To configure the sip-manipulation from ACLI,

Navigate to config t→session-router→sip-manipulation

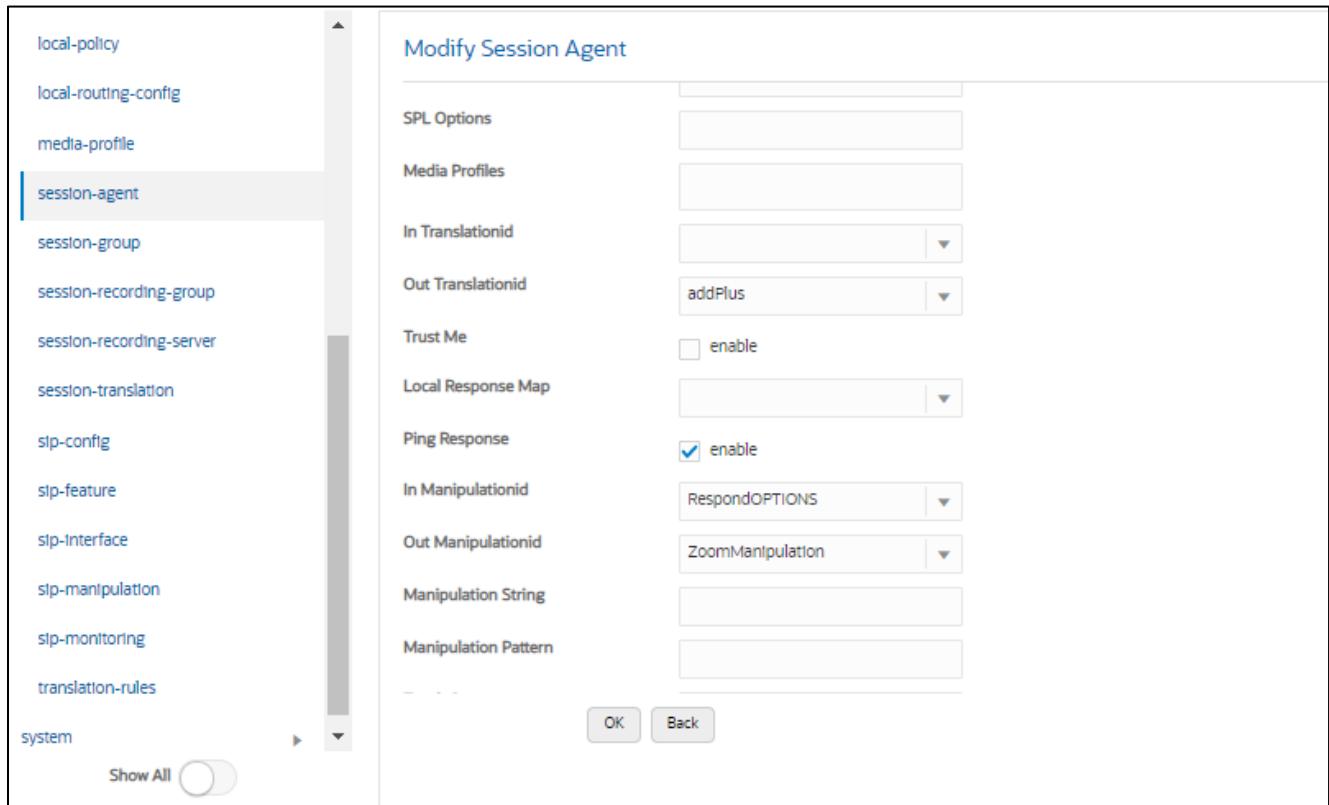
```

sip-manipulation
  name ZoomCP
  header-rule
    name addPlus
    header-name Request-URI
    action manipulate
    comparison-type pattern-rule
    msg-type request
    methods Invite
    element-rule
      name TenDigits
      type uri-user
      action replace
      comparison-type pattern-rule
      match-value ^[0-9]{10}$
      new-value \+1+$ORIGINAL
    element-rule
      name ElevenDigits
      type uri-user
      action replace
      comparison-type pattern-rule
      match-value ^[0-9]{11}$
      new-value \+$ORIGINAL
  header-rule
    name ChangeTO
    header-name TO
    action manipulate
    msg-type request
    methods Invite
    element-rule
      name changetohost
      type uri-host
      action replace
      new-value $REMOTE_IP
    element-rule
      name ChangeToPort
      type uri-port
      action replace
      new-value 5061
  header-rule
    name ChangeFrom
    header-name From
    action manipulate
    msg-type request
    methods Invite
    element-rule
      name ChangeFromHost
      type uri-host
      action replace
      new-value 20.96.25.165
    element-rule
      name ChangeFromPort
      type uri-port
      action replace
      new-value 5061

```

### 6.7.1.2 Responding to Options Ping

If running release SCZ830m1p7 or later, there is a new configuration parameters on the Session Agent Config element, called [ping-response](#). When enabled on each agent, it will take that place of the following SIP-Manipulation.



To enable ping-response from ACLI-

```
SolutionsLab-vSBC-2(session-agent)# ping-response enabled
```

- Perform a save and activate configuration for changes to take effect.

### 6.7.2 Session-Translation

The following session-translation is created and applied as out-translationid on the Session-Agent towards Carriers. This session-translation is created to remove +1 when call is sent towards Carrier as Carrier in this case requires calls to be presented in 10 digit dial format.

GUI Path: session-router/session-translation

ACLI Path: config t → session-router → session-translation

Modify Session Translation

Id	removeE164
Rules Calling	removeplus1 <input type="button" value="X"/>
Rules Called	removeplus1 <input type="button" value="X"/>
Rules Asserted Id	removeplus1 <input type="button" value="X"/>
Rules Redirect	
Rules Isup Cdpn	
Rules Isup Cgpn	
Rules Isup Gn	
Rules Isup Rdn	
Rules Isup Ocn	

OK Back

Modify Translation Rules

Id	removeplus1
Type	delete <input type="button" value="▼"/>
Add String	
Add Index	0
Delete String	+1
Delete Index	0 ( Range: 0..999999999 )

OK Back

To configure session-translation from ACI

```

session-translation
  id          removeE164
  rules-calling    removeplus1
  rules-called      removeplus1
  rules-asserted-id  removeplus1
translation-rules
  id          removeplus1
  type        delete
  delete-string +1

```

- Perform a save and activate configuration for changes to take effect.

## 6.8 Session Timer Profile (Optional)

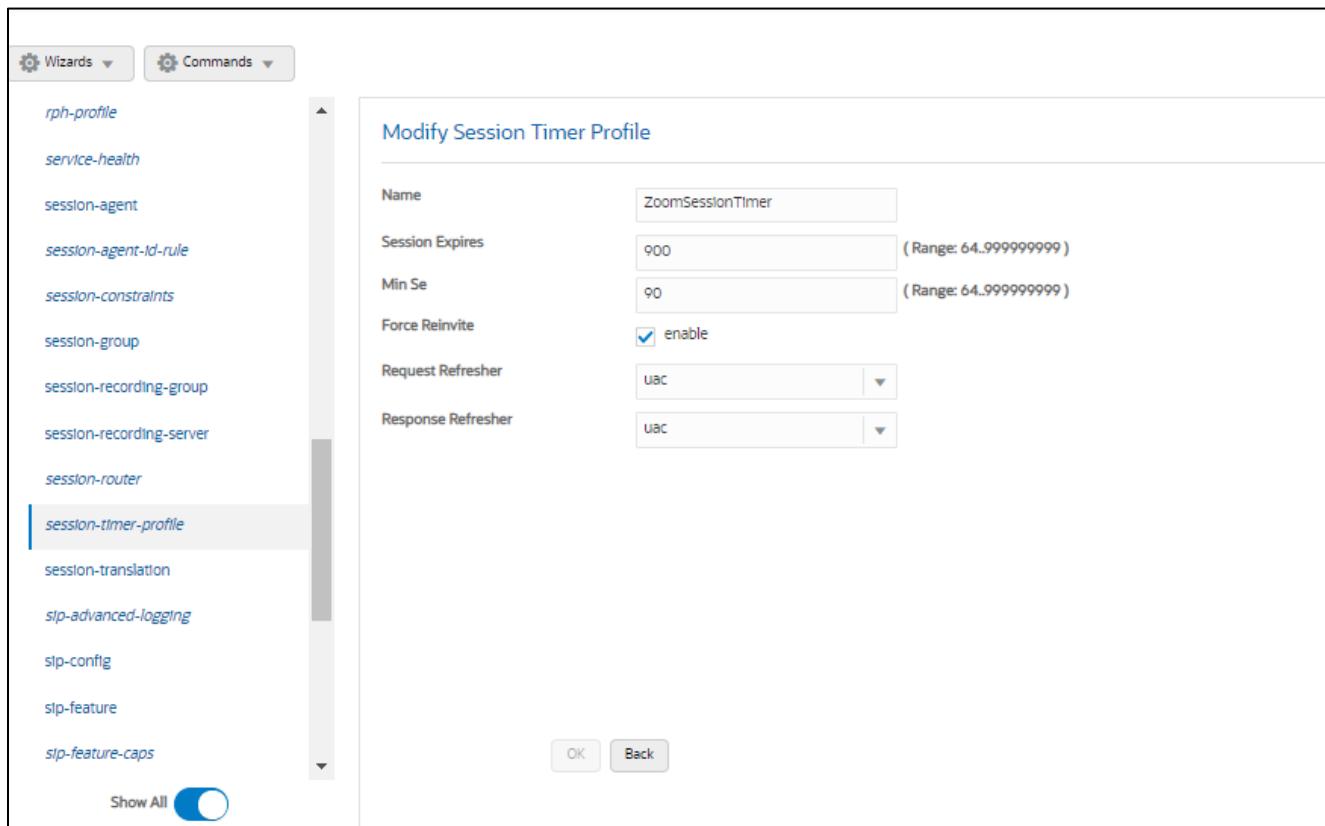
Zoom Phone does support RFC 4028 Session Timers In SIP. In many cases, RFC 4028 is not supported by carriers providing SIP trunking services to their customers. In order to accommodate this, the SBC will interwork between PSTN carrier and Zoom Phone in order to provide support for Session Timers in SIP.

For more information about the Oracle SBC's support for RFC4028, please see the [SCZ9.0 Configuration Guide, page 726](#)

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.



```
session-timer-profile
  name           ZoomSessionTimer
  session-expires 900
  force-reinvite   enabled
  response-refresher uac
```

- Perform a save and activate configuration for changes to take effect.

## 6.9 SIP Interface

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

Configure two SIP interfaces, one associated with PSTN Realm, and the other for Zoom Phone.

GUI Path: session-router/SIP-interface

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

Click Add, and use the table below as an example to Configure:

Please note, this is also where we will be assigned some of the configuration elements configured earlier in this document, i.e.

- TLS Profile
- Session-timer-profile
- SIP-Manipulations

Use the following as an example to configure SIP interfaces:

Config Parameter	Zoom	SIPTrunk	SIPTrunk
Realm ID	Core_Zoom	Peer_SIPTrunk1	Peer_SIPTrunk2
Out manipulationid	ZoomCP		
SIP Port Config Parameter	Zoom	SIP Trunk	SIP Trunk
Address	155.212.214.177	172.18.0.201	192.168.1.10
Port	5061	5060	5060
Transport protocol	TLS	UDP	UDP
TLS profile	TLSZoom		
Allow anonymous	agents-only	agents-only	agents-only
Session Timer Profile	ZoomSessionTimer		

Action	Select	State	Realm ID	Description	Carriers	Trans Expire	Initial Inv Trans Expire
⋮	<input type="checkbox"/>	enabled	Core_Zoom				0
⋮	<input type="checkbox"/>	enabled	Peer_SIPTrunk1				0
⋮	<input type="checkbox"/>	enabled	Peer_SIPTrunk2				0

```

sip-interface
realm-id Core_Zoom
description Interface for Zoom Phone
sip-port
address 155.212.214.177
port 5061
transport-protocol TLS
tls-profile TLSZoom
allow-anonymous agents-only
out-manipulationid ACME_NAT_TO_FROM_IP
sip-profile fireplaces
session-timer-profile ZoomSessionTimer

sip-interface
realm-id Peer_SIPTrunk1
sip-port
address 172.18.0.201
allow-anonymous agents-only

sip-interface
realm-id Peer_SIPTrunk2
sip-port
address 192.168.1.10
allow-anonymous agents-only

```

## 6.10 Session Agents

Session Agents are configuration elements which are trusted agents that can both send and receive traffic from the ORACLE SBC with direct access to the trusted data path.

GUI Path: session-router/session-agent

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

You will need to configure session agents for Zoom Phone and both Carrier SIP Trunks.

**Note:** In this configuration example we have used Zoom Cloud Peering Session Agents for North America Region. You will be required to configure Zoom Cloud Peering Session Agents as per your specific region. Contact your Zoom representative for detailed list of Zoom IP Addresses.

- Click Add, and use the table below to configure:

Config parameter	Zoom	SIPTrunk1	SIPTrunk2
------------------	------	-----------	-----------

Hostname	69.174.108.135	172.18.0.210	192.168.1.20
IP Address	69.174.108.135	172.18.0.210	192.168.1.20
Port	5061	5060	5060
Transport method	StaticTLS	UDP+TCP	UDP+TCP
Realm ID	Core_Zoom	Peer_SIPTTrunk1	Peer_SIPTTrunk2
Ping Method	OPTIONS	OPTIONS	OPTIONS
Ping Interval	30	30	30
Ping Response	Enabled	Enabled	Enabled

The screenshot shows the configuration interface with the 'Session Agent' tab selected. The left sidebar lists various configuration categories, and the main area displays a table of session agents.

Action	Select	Hostname	IP Address	Port	State	App Protocol	Realm ID	Description
:	<input type="checkbox"/>	172.18.0.210	172.18.0.210	5060	enabled	SIP	Peer_SIPTTrunk1	
:	<input type="checkbox"/>	192.168.1.20	192.168.1.20	5060	enabled	SIP	Peer_SIPTTrunk2	
:	<input type="checkbox"/>	69.174.108.135	69.174.108.135	5061	enabled	SIP	Core_Zoom	

- Hit the OK tab at the bottom of each when applicable

```

session-agent
  hostname          69.174.108.135
  ip-address        69.174.108.135
  port              5061
  transport-method  StaticTLS
  realm-id          Core_Zoom
  ping-method       OPTIONS
  ping-interval     30
  ping-response     enabled

session-agent
  hostname          172.18.0.210
  ip-address        172.18.0.210
  transport-method  UDP+TCP
  realm-id          Peer_SIPTrunk1
  ping-method       OPTIONS
  ping-interval     30
  ping-response     enabled
  rfc2833-mode     preferred
  rfc2833-payload   101

session-agent
  hostname          192.168.1.20
  ip-address        192.168.1.20
  transport-method  UDP+TCP
  realm-id          Peer_SIPTrunk2
  ping-method       OPTIONS
  ping-interval     30
  ping-response     enabled

```

- Perform a save and activate configuration for changes to take effect.

## 6.11 Routing Configuration

This section outlines how to configure the Oracle SBC to route SIP traffic to and from PSTN Trunks and Zoom Phone Platform.

The Oracle SBC has multiple routing options that can be configured based on environment. For the purpose of this example configuration, we are utilizing the Oracle SBC's Local Policy Routing for all traffic to and from Zoom.

### 6.11.1 Local Policy Configuration

Local Policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria.

GUI Path: session-router/local-policy

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

Note : Having more than one PSTN Carrier terminated onto the SBC is optional as service providers can leverage same carrier trunk to support multiple Enterprises. It depends upon the requirement and Network Setup.

#### 6.12.1.1 Route Calls from Zoom To Customer 1:

Calls originating from Zoom Phone System to Different customer's Carrier Trunk are segregated based on DID Range. Here in this example we DID 7692105055 belongs to Customer1 hence all calls originating from Zoom Phone System from DID 7692105055 are routed to Customer 1 Sip Trunk i.e. 172.18.0.210 through realm Peer\_SIPTrunk1

Action	Select	Next Hop	Realm	Action	Terminate Re...	Cost	State	App Protocol	Lookup	Next Key	Auth User Lo...
:	<input type="checkbox"/>	I72.18.0.210	Peer_SIPTrunk1	replace-uri	disabled	0	enabled		single		

#### 6.12.1.2 Route Calls from Zoom To Customer 2:

Similarly, in below example DID 7814437247 belongs to Customer2 hence all calls originating from Zoom Phone System from DID 7814437247 are routed to Customer 2 Sip Trunk i.e. 192.168.1.20 through realm Peer\_SIPTrunk2

Configuration View Configuration Q

**Modify Local Policy**

From Address: 7814457247, +7814457247

To Address: \*

Source Realm: ZoomRealm

Description:

State:  enable

Policy Priority: none

Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Rec...	Cost	State	App Protocol	Lookup	Next Key	Auth User Lo...
:	<input type="checkbox"/>	192.168.1.20	Peer_SIPTrunk2	replace-uri	disabled	0	enabled		single		

OK Back

### 6.12.1.3 Route Calls from Sip Trunks to Zoom:

Below local policies route all the Calls from Peer\_SIPTrunk1 and Peer\_SIPTrunk2 to Zoom Phone System.

Configuration View Configuration Q

**Modify Local Policy**

From Address: \*

To Address: \*

Source Realm: Peer\_SIPTrunk1, Peer\_SIPTrunk2

Description:

State:  enable

Policy Priority: none

Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Re...	Cost	State	App Protocol	Lookup	Next Key	Auth User Lo...
:	<input type="checkbox"/>	69.74.108.135	ZoomRealm	replace-uri	disabled	0	enabled		single		

OK Back

To configure local-policy from ACLI

```

local-policy
  from-address          7692105055
                        +17692105055
  to-address            *
  source-realm          Core_Zoom
  policy-attribute
    next-hop             172.18.0.210
    realm                Peer_SIPTrunk1
    action               replace-uri

local-policy
  from-address          7814437247
                        +17814437247
  to-address            *
  source-realm          Core_Zoom
  policy-attribute
    next-hop             192.168.1.20
    realm                Peer_SIPTrunk2
    action               replace-uri

local-policy
  from-address          *
  to-address            *
  source-realm          Peer_SIPTrunk1 Peer_SIPTrunk2

  policy-attribute
    next-hop             162.12.233.60
    realm                Core_Zoom
    action               replace-uri

```

## 6.12 Access Controls

To enhance the security of your Oracle Session Border Controller, we recommend configuration access controls to limit traffic to only trusted IP addresses on all public facing interfaces.

GUI Path: session-router/access-control

ACLI Path: config t→session-router→access-control

Please use the example below to configure access controls in your environment for rest of the Zoom IP's, as well as SIPTrunk IP's (if applicable).

- Click OK at the bottom

Save and activate your configuration.

To configure access-control from ACLI, Navigate to -

config t→session-router→access-control

```
access-control
realm-id          Core_Zoom
source-address    69.174.108.135
application-protocol SIP
trust-level       high
```

Similarly create access controls for Sip Trunks if required.

Notice the trust level on this ACL is set to high. When the trust level on an ACL is set to the same value of as the access control trust level of its associated realm, this creates an implicit deny, so only traffic from IP addresses configured as ACL's with the same trust level will be allowed to send traffic to the SBC. For more information about trust level on ACL's and Realms, please see the [SBC Security Guide, Page 3-10](#).

### 6.13 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.

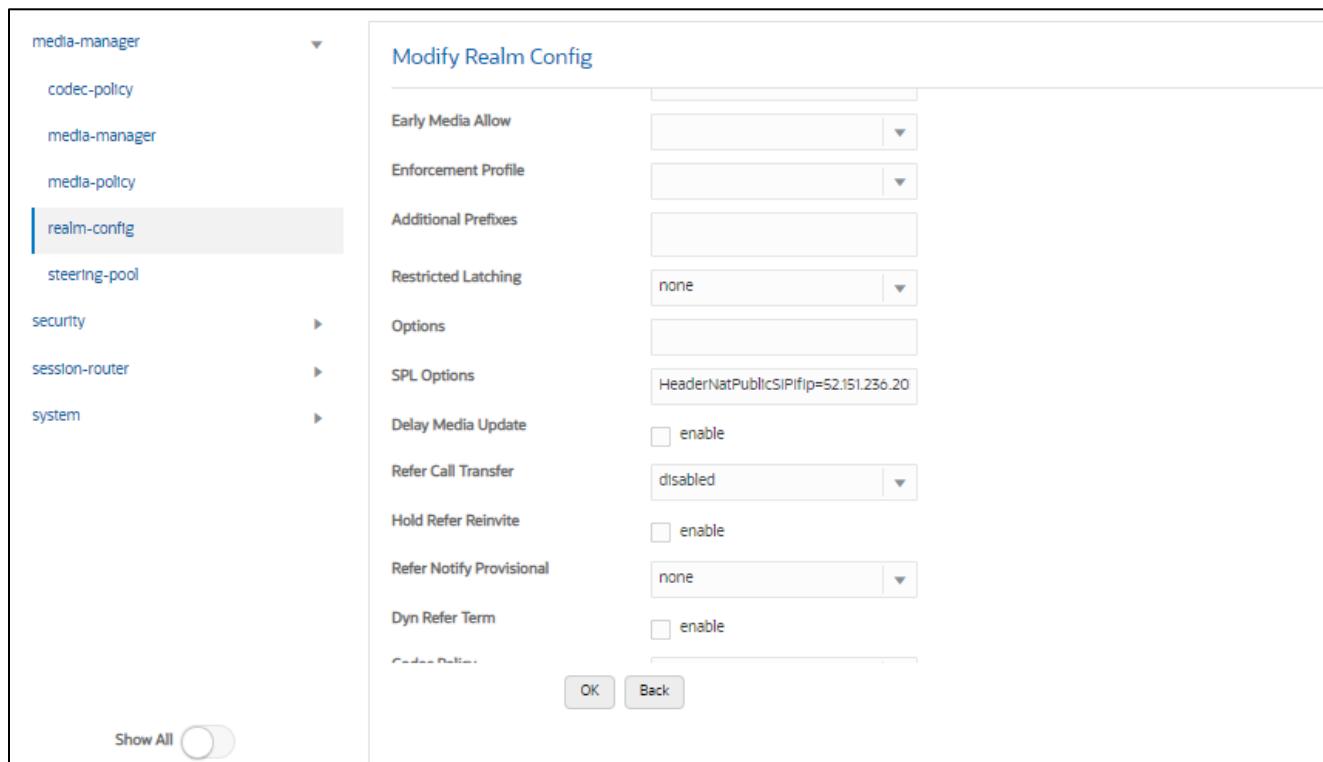
- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

Here is an example configuration with SBC Behind NAT SPL config. The SPL is applied to the Zoom side SIP interface.

To configure SBC Behind NAT SPL Plug in, Go to session-router->SIP-interface->spl-options and input the following value, save, and activate.

HeaderNatPublicSIPIfIp=52.151.236.203,HeaderNatPrivateSIPIfIp=10.0.4.4,Here 52.151.236.203 is an example value and should be your public IP address.

Here HeaderNatPublicSIPIfIp is the public interface ip and HeaderNatPrivateSIPIfIp is the private ip.



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

## 7. ACLI Running Configuration

```
access-control
realm-id          Core_Zoom
source-address     162.12.0.0/16
destination-address 155.212.214.177
application-protocol SIP
trust-level        high

access-control
realm-id          Peer_SIPTrunk1
source-address     172.18.0.210
destination-address 172.18.0.201
application-protocol SIP
trust-level        high

access-control
realm-id          Peer_SIPTrunk2
source-address     192.168.1.20
destination-address 192.168.1.10
application-protocol SIP
trust-level        high

capture-receiver
address           192.168.1.158
network-interface M10:0

certificate-record
name               DigiCertGlobalRootCA
common-name         DigiCertGlobalRootCA

certificate-record
name               DigiCertGlobalRootG2
common-name         DigiCertGlobalRootG2

certificate-record
name               DigiCertGlobalRootG3
common-name         DigiCertGlobalRootG3

certificate-record
name               DigiCertInter
common-name         DigiCert SHA2 Secure Server CA

certificate-record
name               SBCEnterpriseCert
state              California
```

```

locality           Redwood City
organization      Oracle Corporation
unit              Oracle CGBU
common-name       telechat.o-test06161977.com
extended-key-usage-list
                  serverAuth
                  ClientAuth

codec-policy
  name            OptimizeCodecs
  allow-codecs    * G722:no PCMA:no CN:no SIREN:no RED:no G729:no
  add-codecs-on-egress   PCMU

filter-config
  name          all
  user          *

local-policy
  from-address  7692105055
                 +17692105055
  to-address    *
  source-realm   Core_Zoom

policy-attribute
  next-hop      172.18.0.210
  realm         Peer_SIPTrunk1
  action        replace-uri

local-policy
  from-address  7814437247
                 +17814437247
  to-address    *
  source-realm   Core_Zoom

policy-attribute
  next-hop      192.168.1.20
  realm         Peer_SIPTrunk2
  action        replace-uri

local-policy
  from-address  *
  to-address    *
  source-realm   Peer_SIPTrunk1

policy-attribute
  next-hop      162.12.233.60

```

realm	Core_Zoom
action	replace-uri
local-policy	
from-address	*
to-address	*
source-realm	Peer_SIPTrunk2
policy-attribute	
next-hop	162.12.233.60
realm	Core_Zoom
action	replace-uri
media-manager	
max-untrusted-signaling	1
min-untrusted-signaling	1
media-profile	
name	CN
subname	wideband
payload-type	118
media-sec-policy	
name	RTP
media-sec-policy	
name	sdesPolicy
inbound	
profile	SDES
mode	srtp
protocol	sdes
outbound	
profile	SDES
mode	srtp
protocol	sdes
network-interface	
name	s0p0
ip-address	155.212.214.177
netmask	255.255.255.192
gateway	155.212.214.1
dns-ip-primary	8.8.8.8
dns-domain	solutionslab.cgbuburlington.com
network-interface	

name	s1p0
ip-address	172.18.0.201
netmask	255.255.0.0
gateway	172.18.0.1
network-interface	
name	s1p1
ip-address	192.168.1.10
netmask	255.255.255.0
gateway	192.168.1.1
ntp-config	
server	198.55.111.50
	206.108.0.131
phy-interface	
name	s0p0
operation-type	Media
phy-interface	
name	s1p0
operation-type	Media
port	2
phy-interface	
name	s1p1
operation-type	Media
port	3
realm-config	
identifier	Core_Zoom
network-interfaces	s0p0:0:4
mm-in-realm	enabled
media-sec-policy	sdesPolicy
out-manipulationid	ZoomOutManip
access-control-trust-level	high
realm-config	
identifier	Peer_SIPTrunk1
network-interfaces	s1p0:0:4
mm-in-realm	enabled
media-sec-policy	RTP
access-control-trust-level	high
realm-config	

identifier	Peer_SIPTrunk2
network-interfaces	s1p1:0.4
mm-in-realm	enabled
media-sec-policy	sdesPolicy
access-control-trust-level	high
sdes-profile	
name	SDES
crypto-list	AEAD_AES_256_GCM AES_CM_128_HMAC_SHA1_32 AES_256_CM_HMAC_SHA1_80 AES_CM_128_HMAC_SHA1_80
session-agent	
hostname	69.174.108.135
ip-address	69.174.108.135
port	5061
transport-method	StaticTLS
realm-id	Core_Zoom
ping-method	OPTIONS
ping-interval	30
ping-response	enabled
session-agent	
hostname	172.18.0.210
ip-address	172.18.0.210
transport-method	UDP+TCP
realm-id	Peer_SIPTrunk1
ping-method	OPTIONS
ping-interval	30
ping-response	enabled
rfc2833-mode	preferred
rfc2833-payload	101
session-agent	
hostname	192.168.1.20
ip-address	192.168.1.20
transport-method	UDP+TCP
realm-id	Peer_SIPTrunk2
ping-method	OPTIONS
ping-interval	30

```

ping-response           enabled
session-timer-profile
    name                ZoomSessionTimer
    session-expires      900
    force-reinvite       enabled
    response-refresher   uac
session-translation
    id                  addPlus
    rules-calling        addPlus
    rules-called         addPlus
session-translation
    id                  removeE164
    rules-calling        removeplus1
    rules-called         removeplus1
    rules-asserted-id   removeplus1
SIP-config
    home-realm-id       Core_Zoom
    registrar-domain     *
    registrar-host       *
    registrar-port       5060
    options              inmanip-before-validate
                           max-udp-length=0
    extra-method-stats   enabled
sip-interface
    realm-id             Core_Zoom
    description          Interface for Zoom Phone
    sip-port
        address           155.212.214.177
        port               5061
        transport-protocol TLS
        tls-profile         TLSZoom
        allow-anonymous    agents-only
    out-manipulationid   ACME_NAT_TO_FROM_IP
    sip-profile           forreplaces
    session-timer-profile ZoomSessionTimer
sip-interface
    realm-id             Peer_SIPTrunk1

```

```

sip-port
  address          172.18.0.201
  allow-anonymous agents-only

sip-interface
  realm-id        Peer_SIPTrunk2
  sip-port
    address          192.168.1.10
    allow-anonymous agents-only

sip-manipulation
  name             RespondOPTIONS
  header-rule
    name           Respond2OPTIONS
    header-name    from
    action         reject
    methods        OPTIONS
    new-value      "200 OK"

sip-manipulation
  name             SIPTrunkManipulation
  description     Manipulations on SIP Trunk side
  header-rule
    name           XTraceID
    header-name    X-Trace-ID[^]
    action         delete
    msg-type       request
    methods        INVITE

  header-rule
    name           XInstanceID
    header-name    X-Instance-ID[^]
    action         delete
    msg-type       request
    methods        INVITE

  header-rule
    name           XDMInfo
    header-name    X-DM-Info[^]
    action         delete
    msg-type       request
    methods        INVITE

```

```

header-rule
  name          XCapability
  header-name   X-Capability[^]
  action        delete
  msg-type     request
  methods      INVITE

header-rule
  name          xpublicip
  header-name   X-PUBLIC-IP[^]
  action        delete
  msg-type     request
  methods      INVITE

header-rule
  name          xorigcontact
  header-name   X-ORIGINAL-CONTACT[^]
  action        delete
  msg-type     request
  methods      INVITE

header-rule
  name          xorigcallid
  header-name   X-ORIGINAL-CALLID[^]
  action        delete
  msg-type     request
  methods      INVITE

header-rule
  name          xtocarrier
  header-name   X-TO-CARRIER[^]
  action        delete
  msg-type     request
  methods      INVITE

header-rule
  name          xFSSupport
  header-name   X-FS-Support[^]
  action        delete
  msg-type     request
  methods      INVITE

header-rule

```

```

name          callAcme
header-name    From
action         sip-manip
msg-type       request
new-value      ACME_NAT_TO_FROM_IP

header-rule
  name          changeAssertedIP
  header-name   P-Asserted-Identity
  action        manipulate
  comparison-type pattern-rule
  msg-type      request
  methods       INVITE

element-rule
  name          changeIP
  type          uri-host
  action        replace
  comparison-type pattern-rule
  new-value     $LOCAL_IP

SIP-monitoring
  match-any-filter enabled
  monitoring-filters *
SIP-profile
  name          forreplaces
  replace-dialogs enabled
steering-pool
  ip-address    155.212.214.177
  start-port    10000
  end-port      20000
  realm-id      Core_Zoom
steering-pool
  ip-address    172.18.0.201
  start-port    20001
  end-port      40000
  realm-id      Peer_SIPTrunk1
steering-pool
  ip-address    192.168.1.10
  start-port    40001

```

```

end-port          60000
realm-id         Peer_SIPTrunk2

system-config
  hostname        zoom.us
  description      SBC for Zoom Phone
  location         Burlington,MA
  system-log-level NOTICE
  default-gateway 10.138.194.129
  source-routing    enabled
  snmp-agent-mode v1v2

tls-global
  session-caching enabled

tls-profile
  name             TLSZoom
  end-entity-certificate SBCEnterpriseCert
  trusted-ca-certificates
    DigiCertRoot
    DigiCertGlobalRootG2
    DigiCertGlobalRootG3
  cipher-list
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    TLS_RSA_WITH_AES_256_CBC_SHA256
    TLS_RSA_WITH_AES_128_CBC_SHA
  mutual-authenticate enabled

translation-rules
  id               addPlus
  type             add
  add-string       +1

translation-rules
  id               removeplus1
  type             delete
  delete-string    +1

web-server-config
  http-interface-list GUI

```



CONNECT WITH US



- [blogs.oracle.com/oracle](http://blogs.oracle.com/oracle)
- [facebook.com/Oracle/](http://facebook.com/Oracle/)
- [twitter.com/Oracle](http://twitter.com/Oracle)
- [oracle.com](http://oracle.com)

**Oracle Corporation, World Headquarters      Worldwide Inquiries**

500 Oracle Parkway  
Redwood Shores, CA 94065, USA

Phone: +1.650.506.7000  
Fax: +1.650.506.7200

**Integrated Cloud Applications & Platform Services**

Copyright © 2020, 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