ORACLE

Oracle Enterprise Session Border Controller with Zoom Phone (PREMISE PEERING - BYOC)

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

1 Related Documentation

1.1 Oracle SBC

- Oracle® Enterprise Session Border Controller Web GUI User Guide
- Oracle® Enterprise Session Border Controller ACLI Configuration Guide
- Oracle® Enterprise Session Border Controller Release Notes
- https://docs.oracle.com/cd/F12246_01/doc/sbc_scz830_security.pdf

1.2 Zoom Phone

- https://zoom.us/docs/doc/Zoom-Bring%20Your%20Own%20Carrier.pdf
- https://zoom.us/phonesystem
- https://zoom.us/zoom-phone-features

2 Revision History

Version	Date Revised	Description of Changes
1.0	04/09/2020	Initial publication

3 Intended Audience

This document describes how to connect the Oracle SBC to Zoom Phone- PREMISE PEERING - BYOC. 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 testing with the Oracle Communications SBC versions:

SCZ830m1p7

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
- VME

4 Zoom Phone Configuration

For Assistance with setting up and configuring your Zoom Phone System, please reach out to Zoom Sales: https://zoom.us/contactsales

5 Infrastructure Requirements

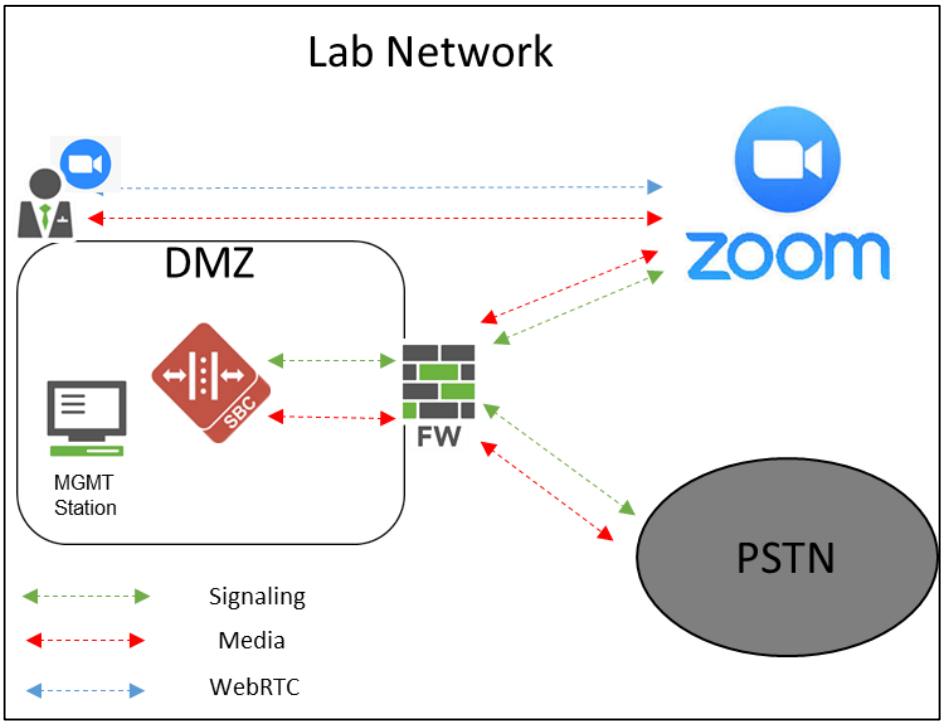
The table below shows the list of infrastructure prerequisites for deploying Direct Routing**.**

Session Border Controller (SBC)	**See Zoom Documentation for More Details**
SIP Trunks connected to the SBC	
Zoom Phone	
Public IP address for the SBC	
Public trusted certificate for the SBC	
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 was 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. 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.

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 (refer to Related Documentation for details about supported Certification Authorities).
- Zoom Public CA certificates to add to trust store of SBC

7 Oracle SBC Configuration

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

For the purposes of this note, we'll be using the Oracle SBC GUI for all configuration examples. We will however provide the ACLI path to each element.

This guide assumes the Oracle SBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, web-server-config has been enabled for GUI access. If you require more information on how to install your SBC platform, please refer to the ACLI configuration guide.

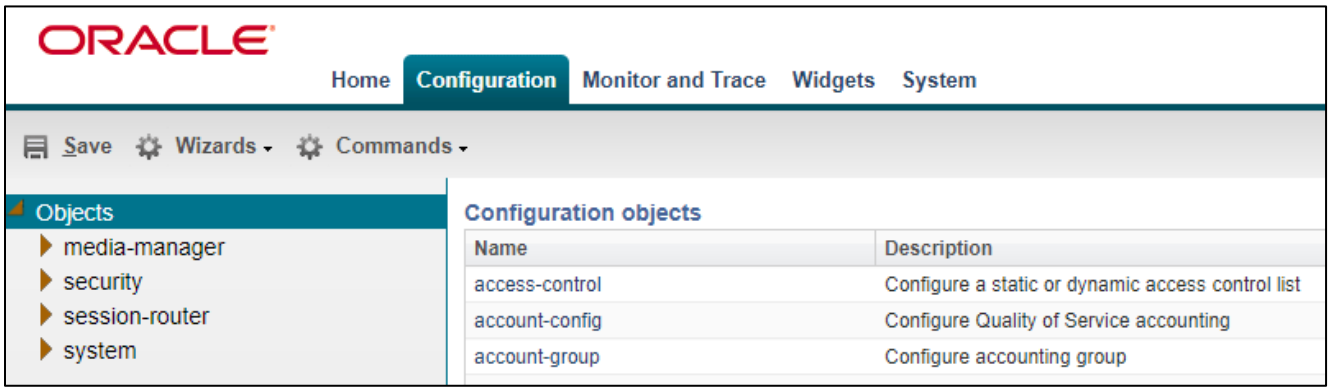
To access the Oracle SBC GUI, enter the management IP address into a web brower.
When the login screen appears, enter the username and password to access the ORACLE ESBC.

Once you have accessed the Oracle SBC, at the top, click the Configuration Tab. This will bring up the ORACLE ESBC Configuration Objects List on the left hand side of the screen.

Any configuration parameter not specifically listed below can remain at the ORACLE ESBC default value and does not require a change for connection to Zoom Phone to function properly.

The below configuration example assumes you will be using a secure connection between the Oracle SBC and Zoom Phone Platform for both signalling and media.

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



7.1 Global Configuration Elements

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

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

7.1.1 System-Config

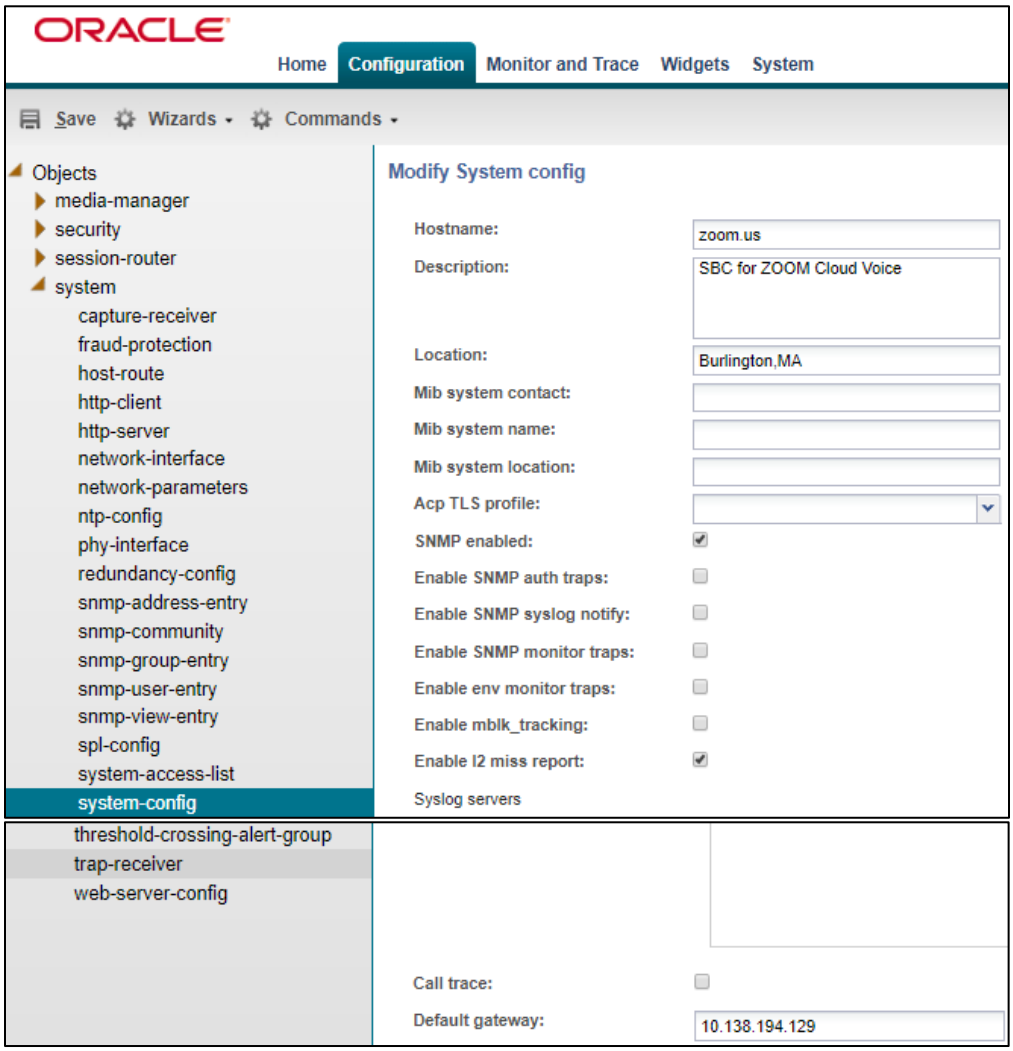
To configure system level functionality for the ORACLE ESBC, you must first enable the system-config

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)*



- Click the OK at the bottom of the screen

7.1.2 Media Manager

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

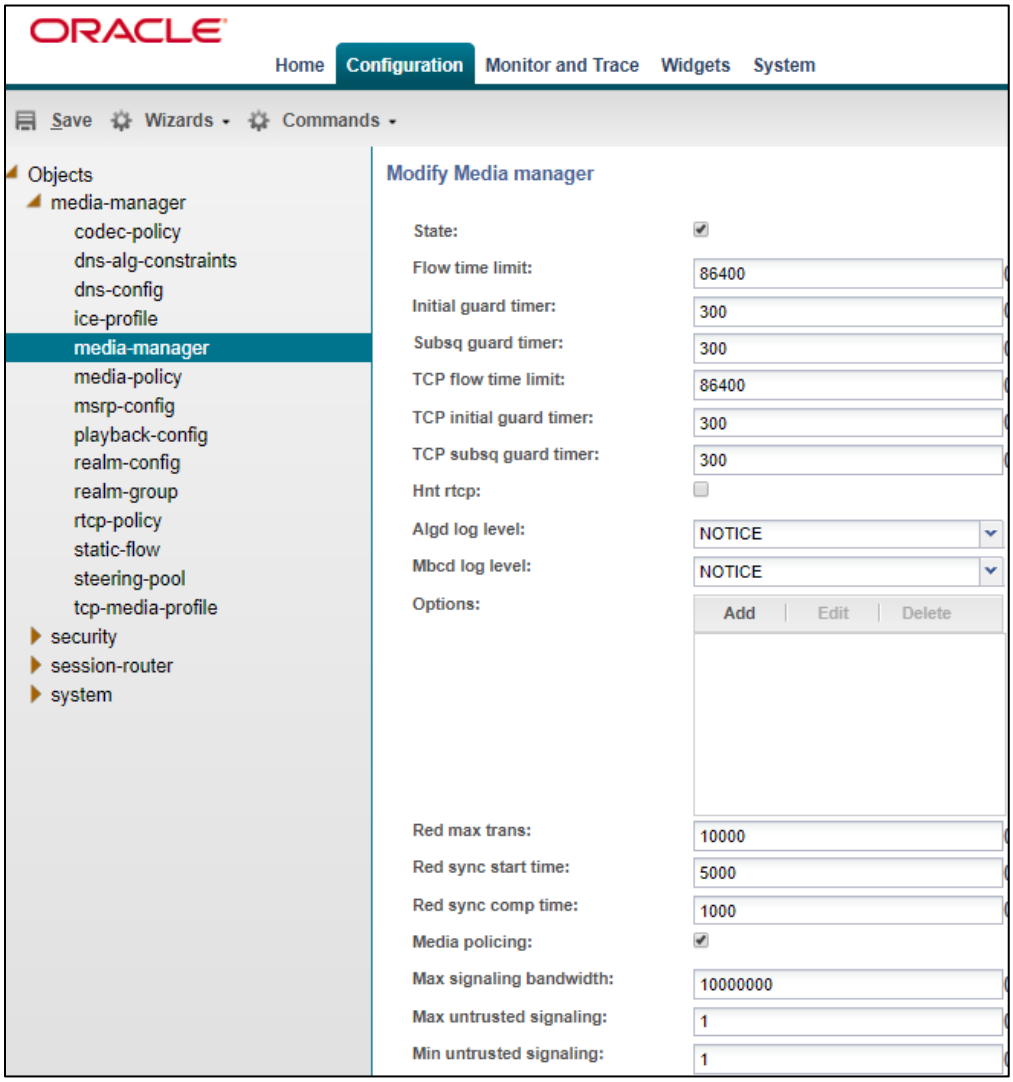
GUI Path: media-manager/media-manager

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

The following options are recommeded 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 Secuirty Guide.



- Click OK at the bottom

7.1.3 SIP Config

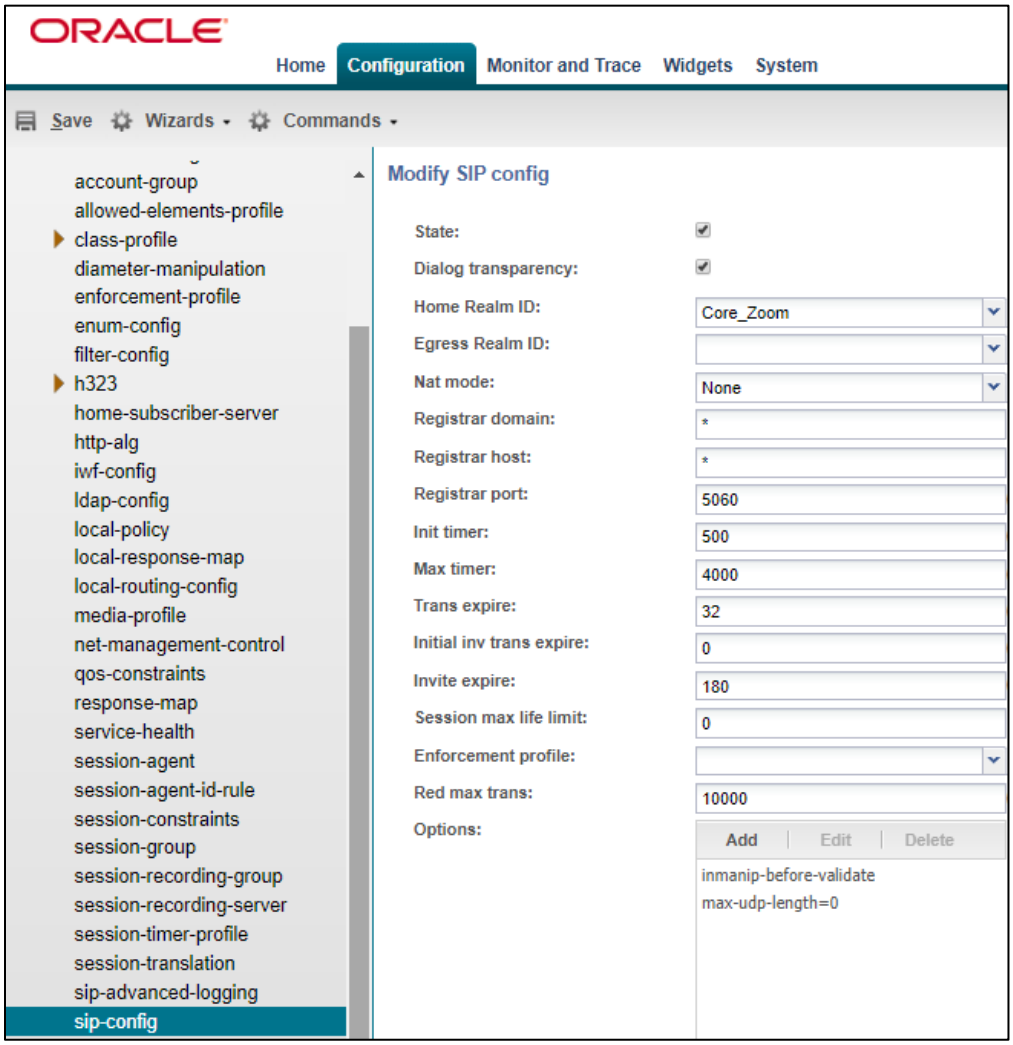
To enable SIP related objects on the ORACLE ESBC, you must first configure the global SIP Config element:

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)

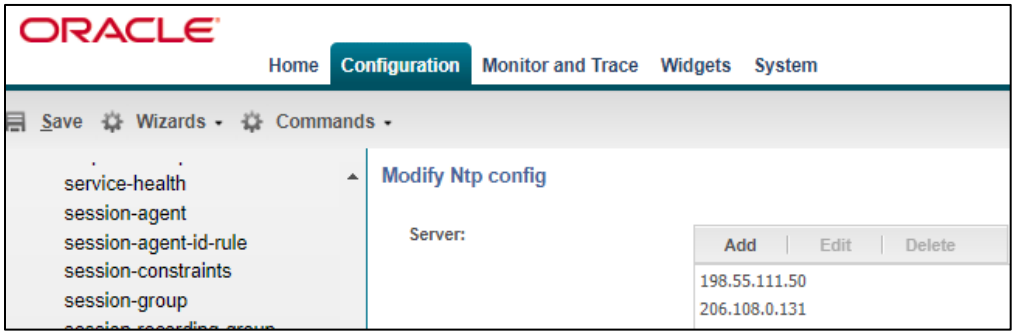


- Click OK at the bottom

7.1.4 NTP Config

GUI Path: system/ntp-config

ACLI Path: config t→system→ntp-config



- Click OK at the bottom

7.2 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.

7.2.1 Physical Interfaces

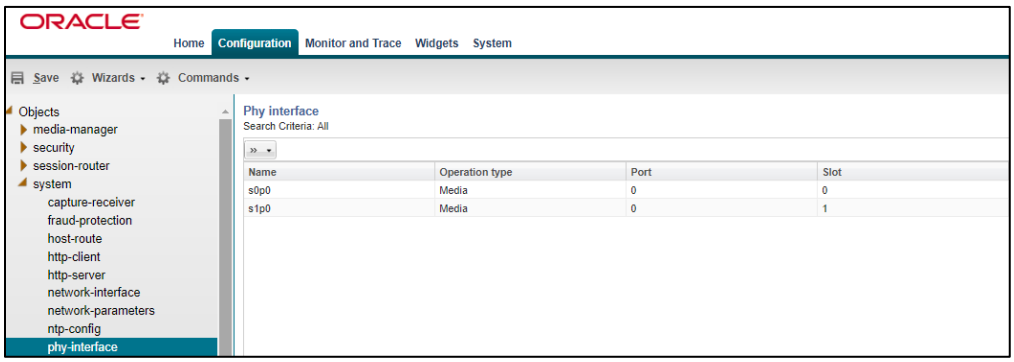
GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

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

Config Parameter	Zoom	PSTN
Name	s0p0	S1p0
Operation Type	Media	Media
Slot	0	1
Port	0	0

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



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

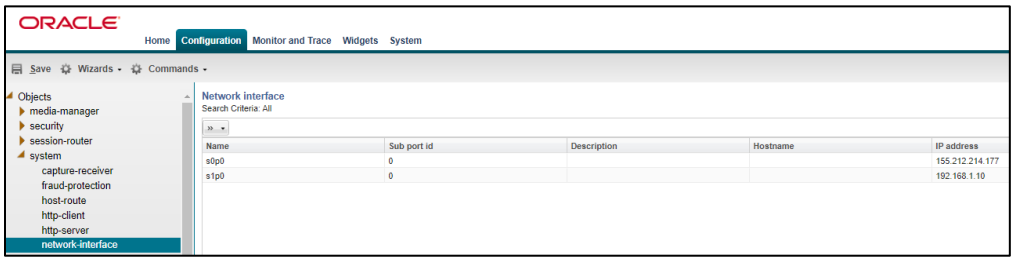
7.2.2 Network Interfaces

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	PSTN
Name	s0p0	s1p0
Hostname	Domain (if applicable)	
IP Address	155.212.214.177	192.168.1.10
Netmask	255.255.255.0	255.255.255.0
Gateway	155.212.214.1	192.168.1.1
DNS Primary IP	8.8.8.8	
DNS Domain	Domain(if applicable)	



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

7.3 Security Configuration

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

Zoom Phone allows TCP 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 Cerificate Authorities.

7.3.1 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)
- DigiCert RootCA Cert
- DigiCert Intermidiate Cert (this is optional – only required if your server certificate is signed by an intermediate)
- GoDaddy Root CA Cert (Zoom Presents the SBC a certficate signed by this authority)
- GoDaddy Intermediate Cert

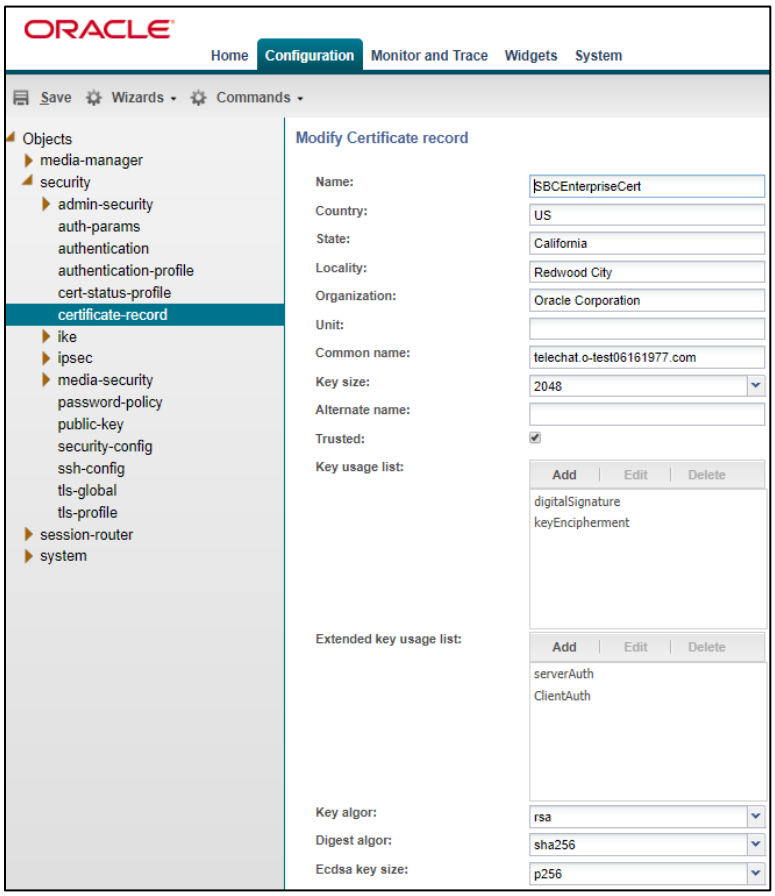
7.3.2 SBC End Entity Certificate

The SBC's end entity certificate is what is presented to Zoom Phone signed by your CA authority, 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

7.4 Root CA and Intermediate Certificates

7.4.1 Digicert Root and intermediate Certificates:

The following, DigitCertRoot and DigicertInter are the root and intermediate CA certificates used to sign the SBC's end entity certificate. As mentioned above, the intermediate certificate is optional, and only required if your server certificate is signed by an intermediate.

7.4.2 GoDaddy Root and Intermediate Certificates:

Zoom presents a certificate to the SBC which is signed by GoDaddy root/intermediate CA. To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate.

You can download these certificate here: https://ssl-ccp.godaddy.com/repository?origin=CALLISTO

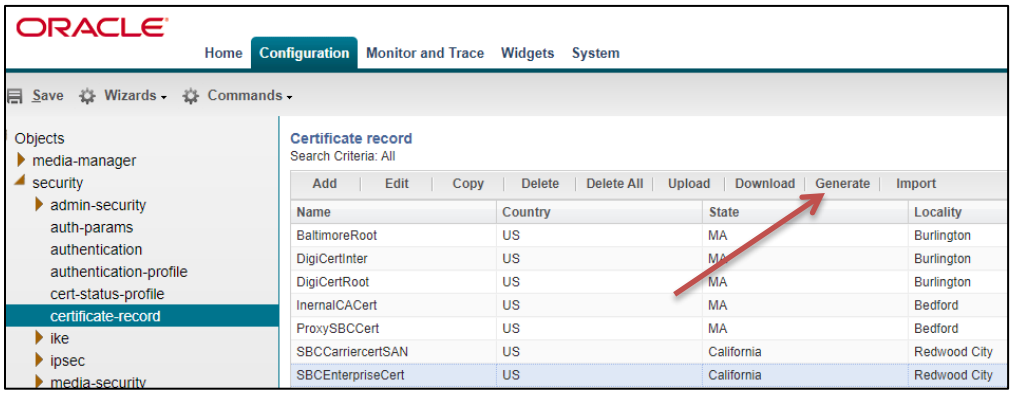
Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

Config Parameter	GoDaddy Root	GoDaddy Intermediate	Digicert Intermediate	DigiCert Root CA
Common Name	GoDaddy Class2 Root CA	GoDaddy Secure Server CA	DigiCert SHA2 Secure Server CA	DigiCert Global Root CA
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

7.4.3 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 intermidiate certificates that have been created**.

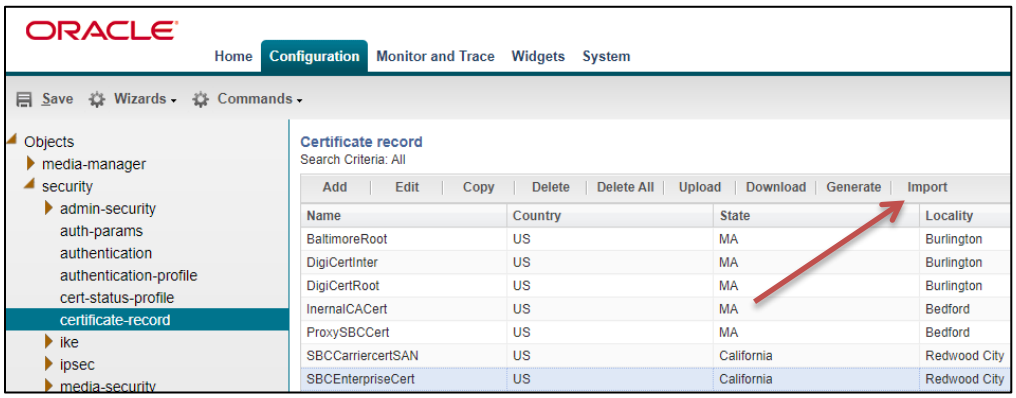
On the certificate record page in the Oracle SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:

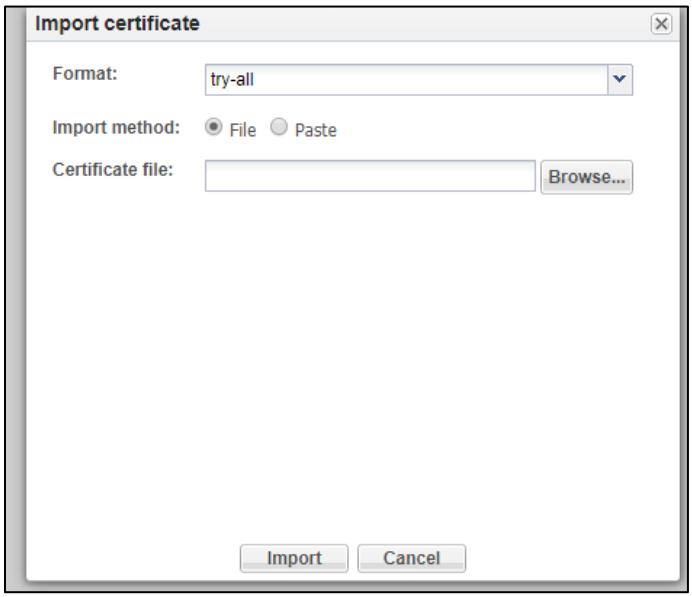


- copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, **a save and activate is required** before you can import the certificates to each certificate record created above.

7.4.4 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





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

- GoDaddyRoot
- GodaddyIntermediate
- DigiCertIntermediate
- DigiCertRoot

At this stage, all required certificates have been imported.

7.4.5 TLS Profile

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

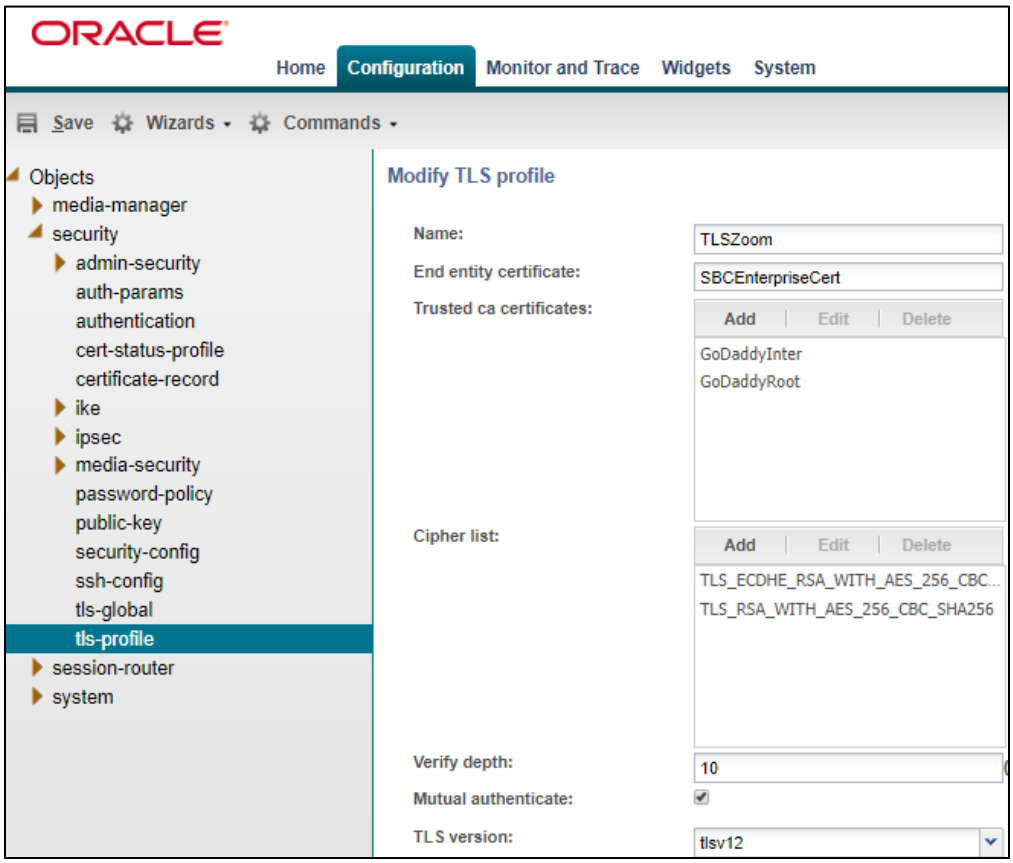
GUI Path: security/tls-profile

ACLI Path: config t→security→tls-profile

- Click Add, use the example below to configure

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

- TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA-384
- RSA-WITH-AES-256-CBC-SHA-256



Note: Only the GoDaddy Certificates need to be added to the tls-profile to authenticate the certificate presented to the SBC from Zoom Phone.

- Click OK at the bottom

7.5 Media Security Configuration

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

7.5.1 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.

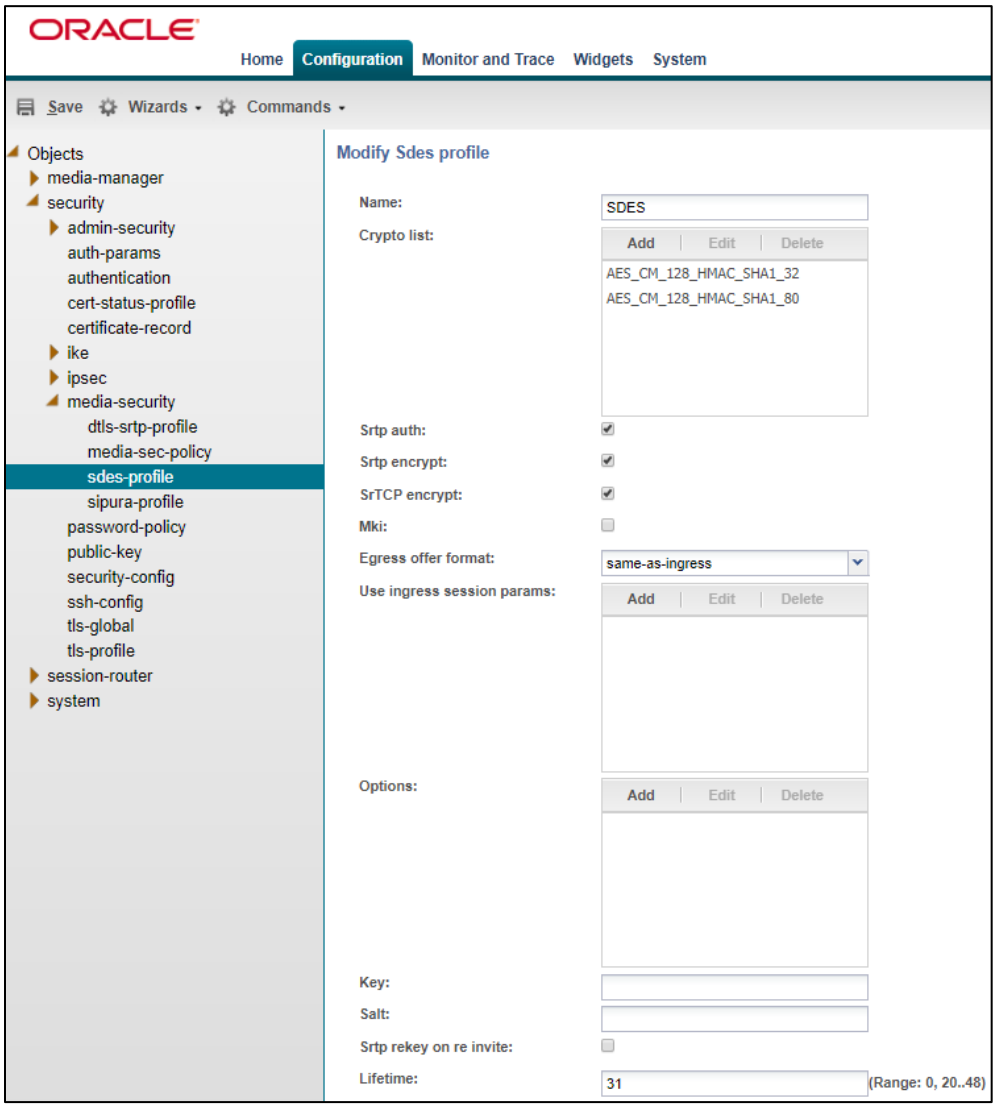
GUI Path: security/media-security/sdes-profile

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

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

- 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

7.5.2 Media Security Policy

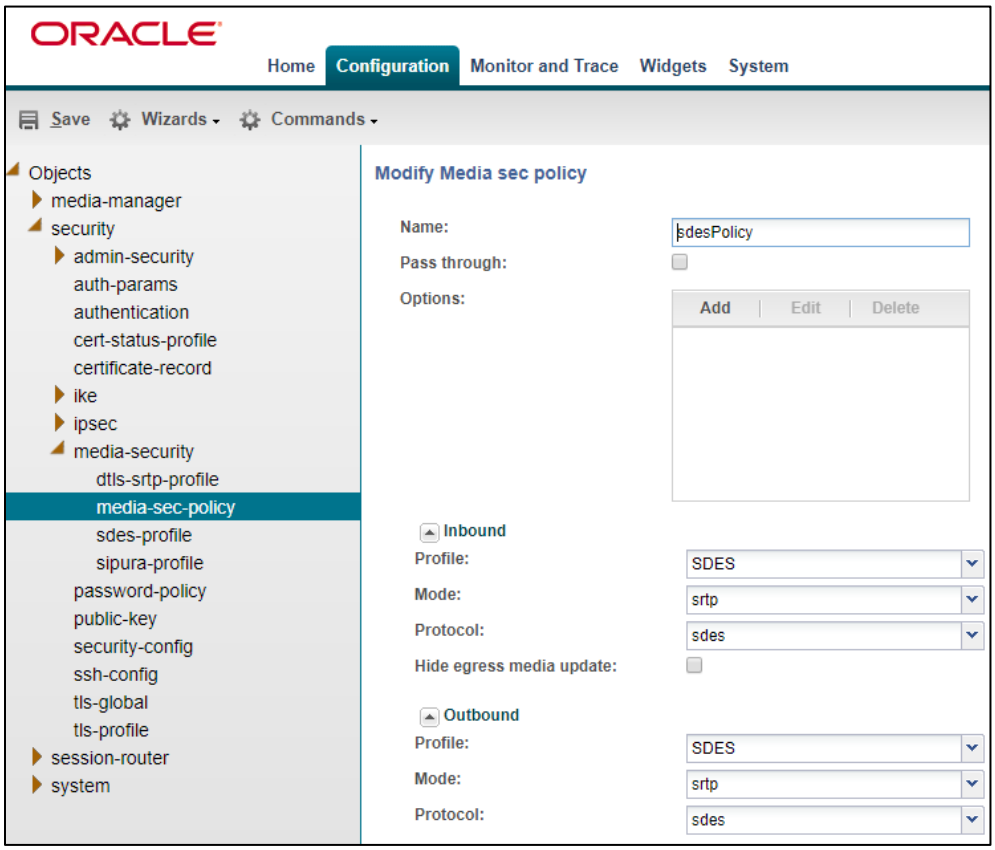
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them) and, if SRTP needs to be used, the sdes-profile that needs to be used

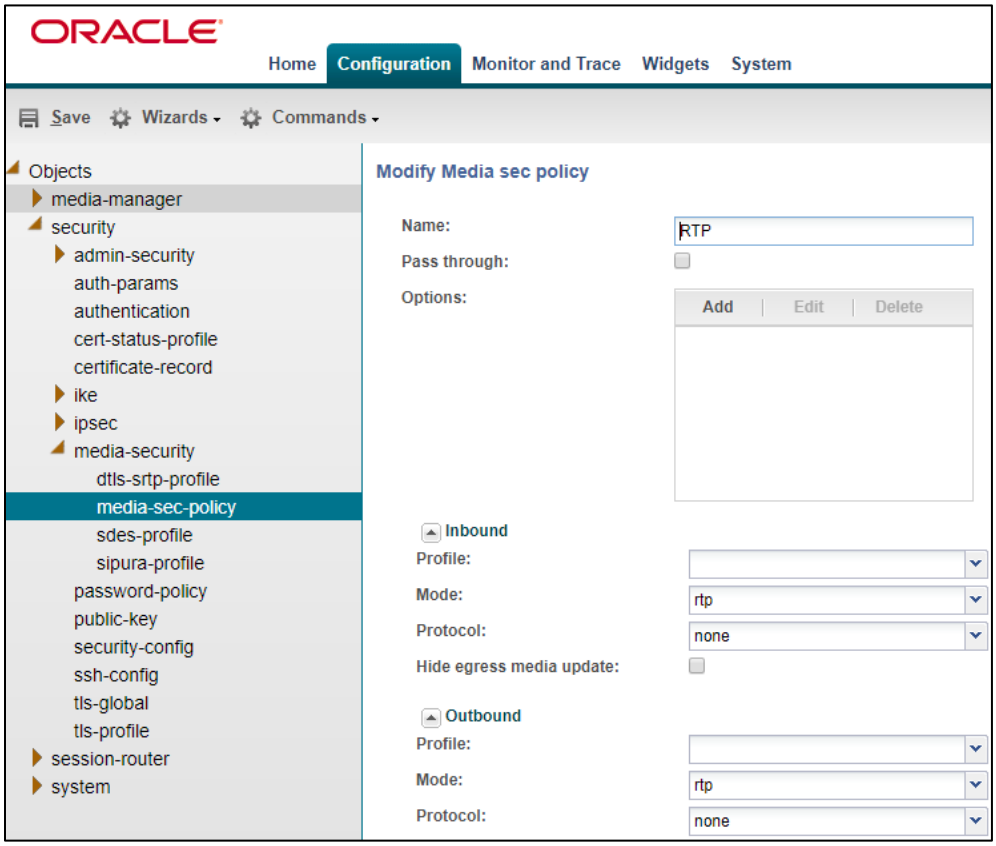
In this example, we are configuring two media security policies. One to secure and decrypt media toward Zoom, the other for non secure media facing PSTN.

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


ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Objects
media-manager
security
admin-security
auth-params
authentication
cert-status-profile
certificate-record
ike
ipsec
media-security
dtls-srtp-profile
media-sec-policy
sdes-profile
sipura-profile
password-policy
public-key
security-config
ssh-config
tls-global
tls-profile
session-router
system
Modify Media sec policy
Name:
sdesPolicy
Pass through:
Options:
Add
Edit
Delete
Inbound
Profile:
SDES
Mode:
srtp
Protocol:
sdes
Hide egress media update:
Outbound
Profile:
SDES
Mode:
srtp
Protocol:
sdes


ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Objects
media-manager
security
admin-security
auth-params
authentication
cert-status-profile
certificate-record
ike
ipsec
media-security
dtls-srtp-profile
media-sec-policy
sdes-profile
sipura-profile
password-policy
public-key
security-config
ssh-config
tls-global
tls-profile
session-router
system
Modify Media sec policy
Name:
RTP
Pass through:
Options:
Add
Edit
Delete
Inbound
Profile:
Mode:
rtp
Protocol:
none
Hide egress media update:
Outbound
Profile:
Mode:
rtp
Protocol:
none

7.6 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.

7.6.1 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 Realm

This is a standalone realm facing PSTN/SIP Trunk

GUI Path; media-manager/realm-config

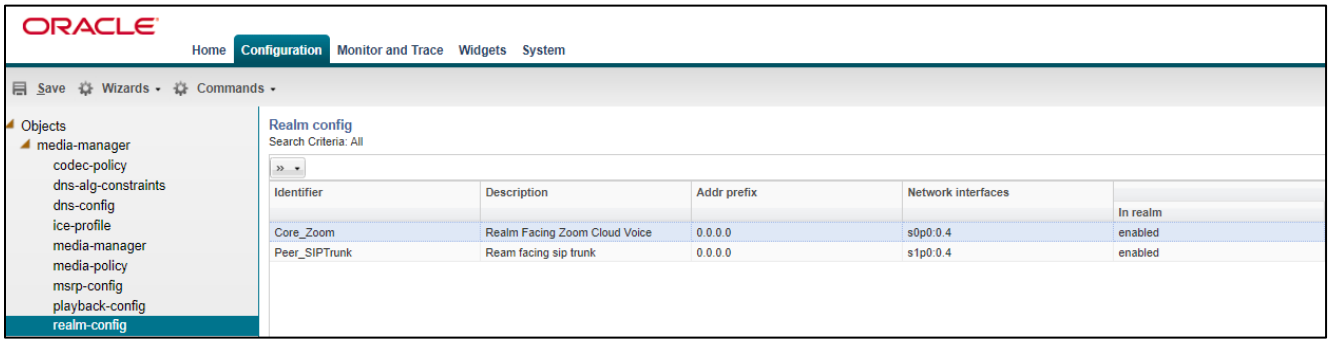
ACLI Path: config t→media-manager→realm-config

- 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 Realm
Identifier	Core_Zoom	Peer_SIPTrunk
Network Interface	s0p0:0	s1p0:0
Mm in realm	☑	☑
Access-control-trust-level	High	High
Media Sec policy	sdespolicy	RTP
RTCP mux	☑ (optional)	

Also notice, the realm configuration is where we assign some of the elements configured earlier in this document, ie…

- Network interface
- Media security policy



7.6.2 **St**eering Pools

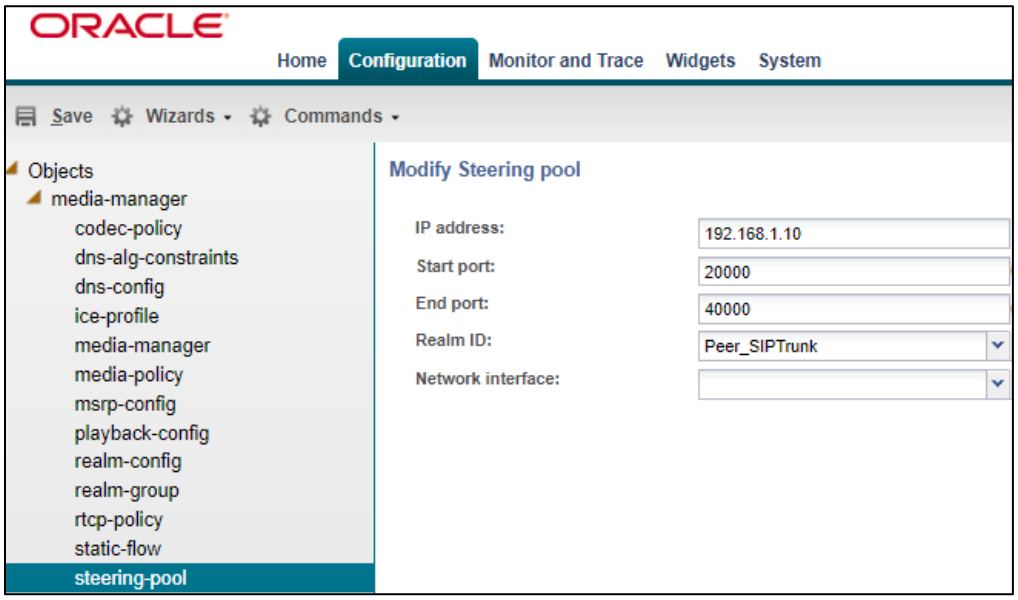
Steering pools define sets of ports that are used for steering media flows through the ORACLE ESBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

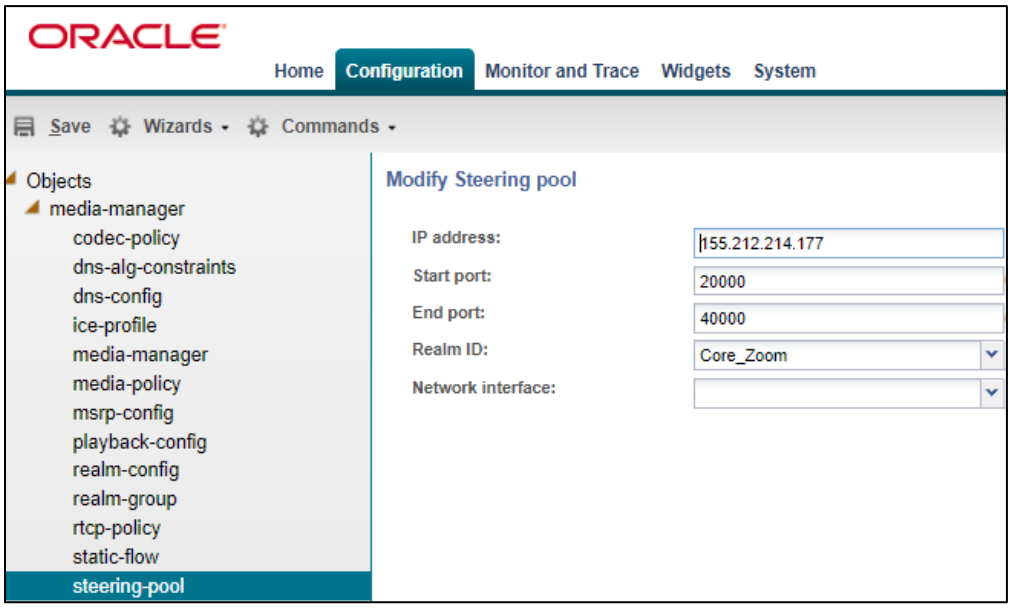
We configure one steering pool for PSTN and one steering pool for Zoom Phone

GUI Path: media-manager/steering-pool

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

- Click Add, and use the below examples to configure





7.7 SIP Configuration

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

7.7.1 SIP Manipulations

For calls to be presented to Zoom Phone from the Oracle SBC, the Oracle SBC requires alterations to the SIP signaling natively created. To do this, we must configure a SIP manipulation in order to preset signaling packets that are acceptable to Zoom Phone.

GUI Path: session-router/SIP-manipulation

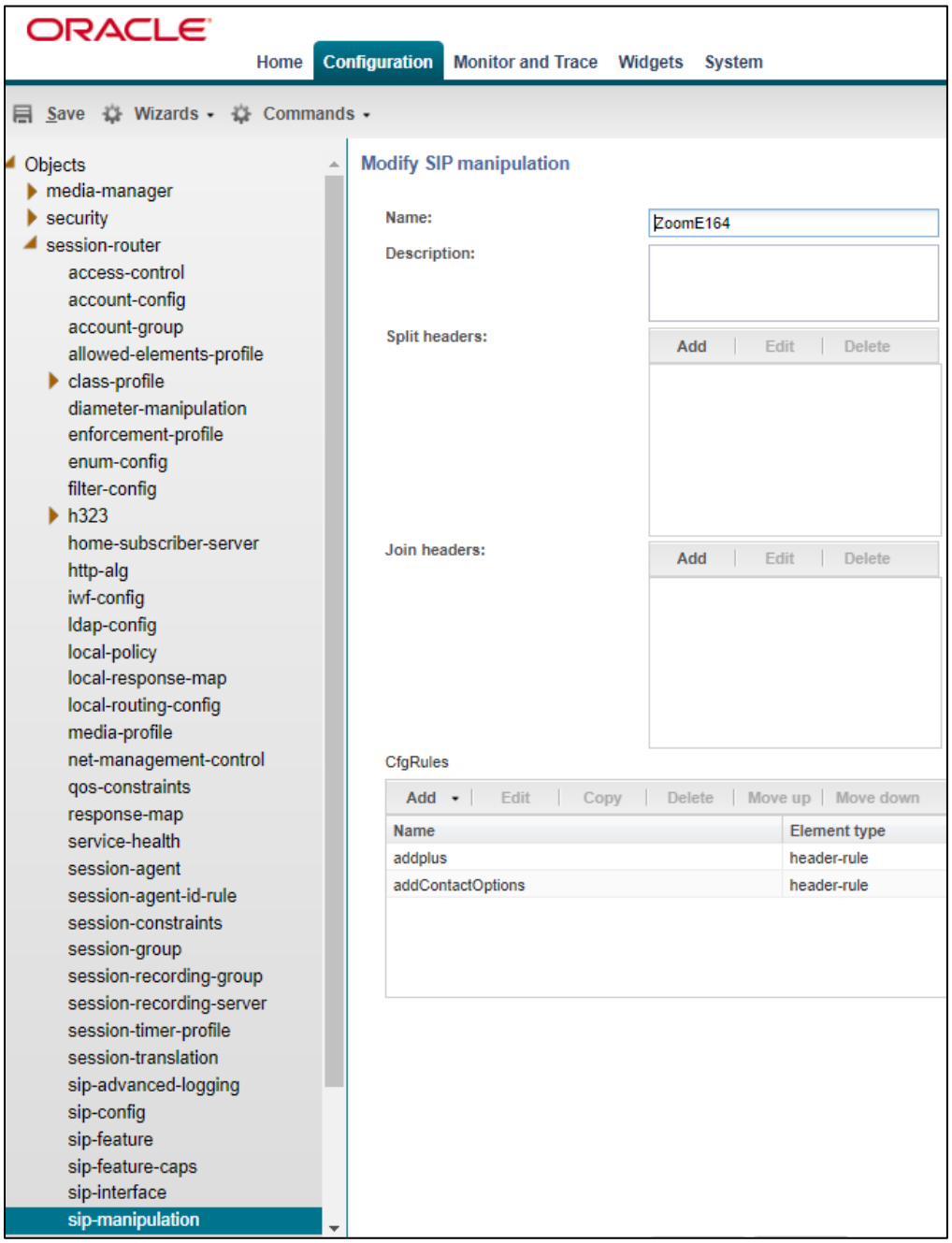
ACLI Path: config t→session-router→SIP-manipulation

The following SIP manipulation is applied as the out-manipulationId and modifies packets generated by the Oracle SBC to Zoom Phone:

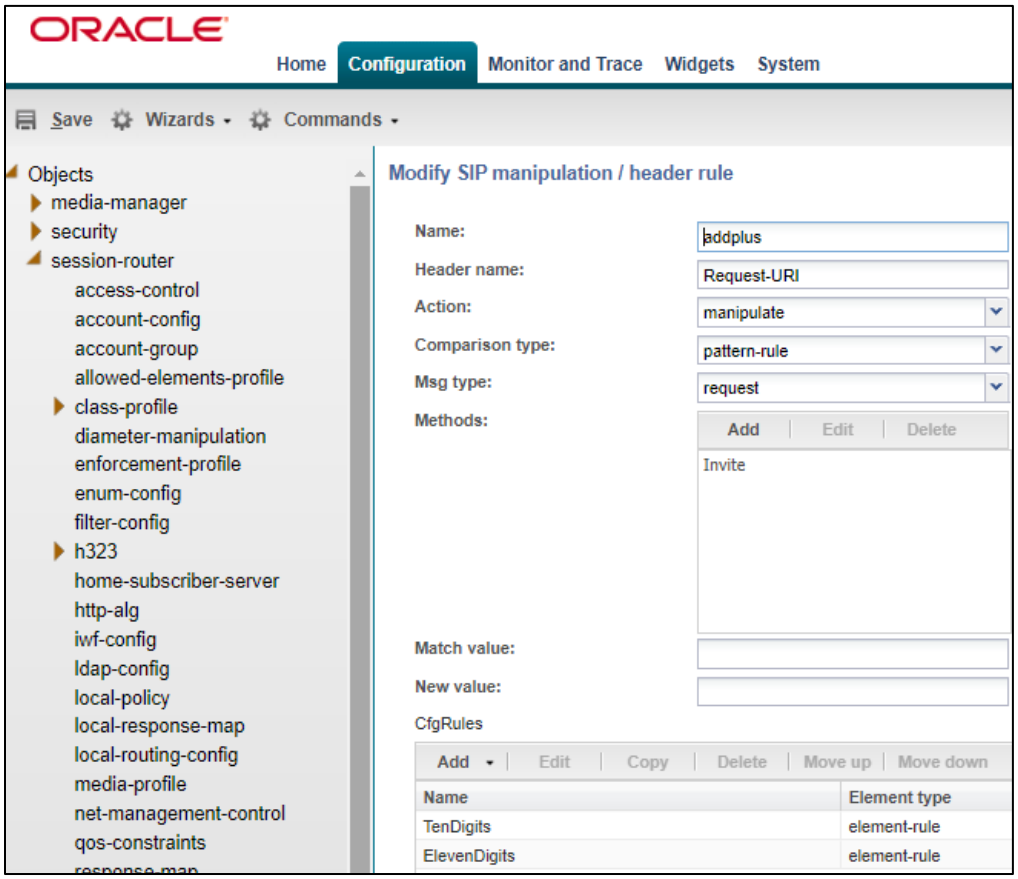
The manipulation performs the following modifications to SIP packets:

Addplus: changes the user uri of the Request Uri to E.164 format

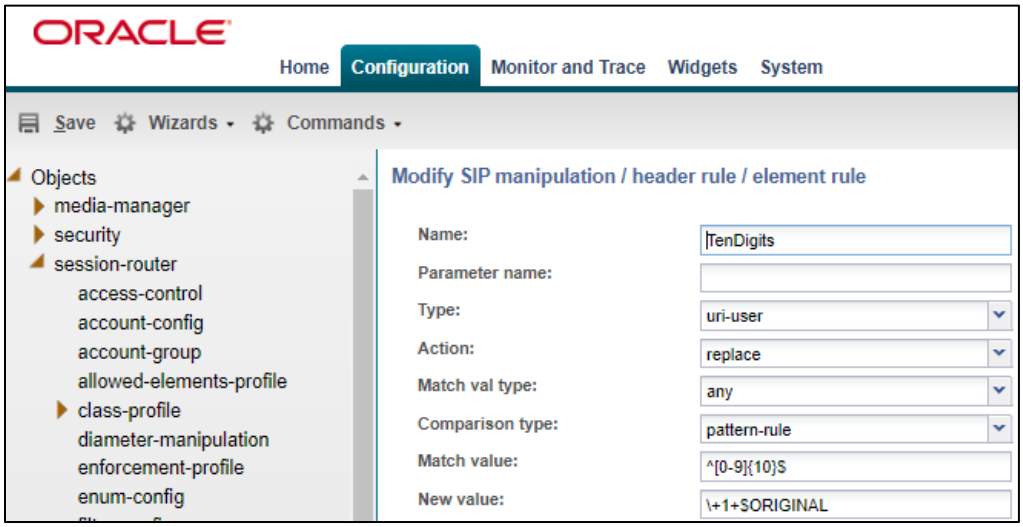
AddContactOptions: Adds a contact header to OPTIONS Requests generated by the SBC towards Zoom with the Oracle SBC's IP address.

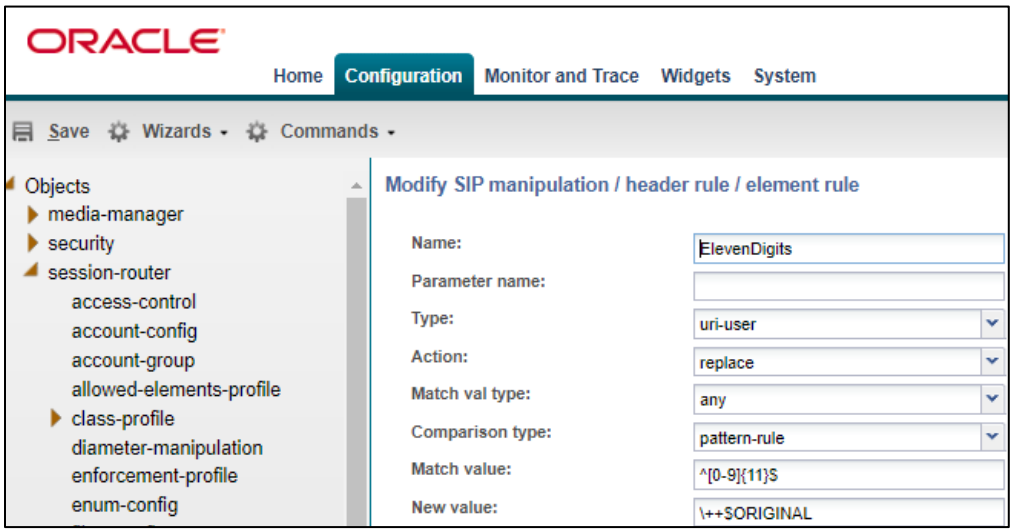

ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Objects
media-manager
security
session-router
access-control
account-config
account-group
allowed-elements-profile
class-profile
diameter-manipulation
enforcement-profile
enum-config
filter-config
h323
home-subscriber-server
http-alg
iwf-config
ldap-config
local-policy
local-response-map
local-routing-config
media-profile
net-management-control
qos-constraints
response-map
service-health
session-agent
session-agent-id-rule
session-constraints
session-group
session-recording-group
session-recording-server
session-timer-profile
session-translation
sip-advanced-logging
sip-config
sip-feature
sip-feature-caps
sip-interface
sip-manipulation
Modify SIP manipulation
Name:
ZoomE164
Description:
Split headers:
Add
Edit
Delete
Join headers:
Add
Edit
Delete
CfgRules
Add
Edit
Copy
Delete
Move up
Move down
Name
Element type
addplus
header-rule
addContactOptions
header-rule

Header Rules:



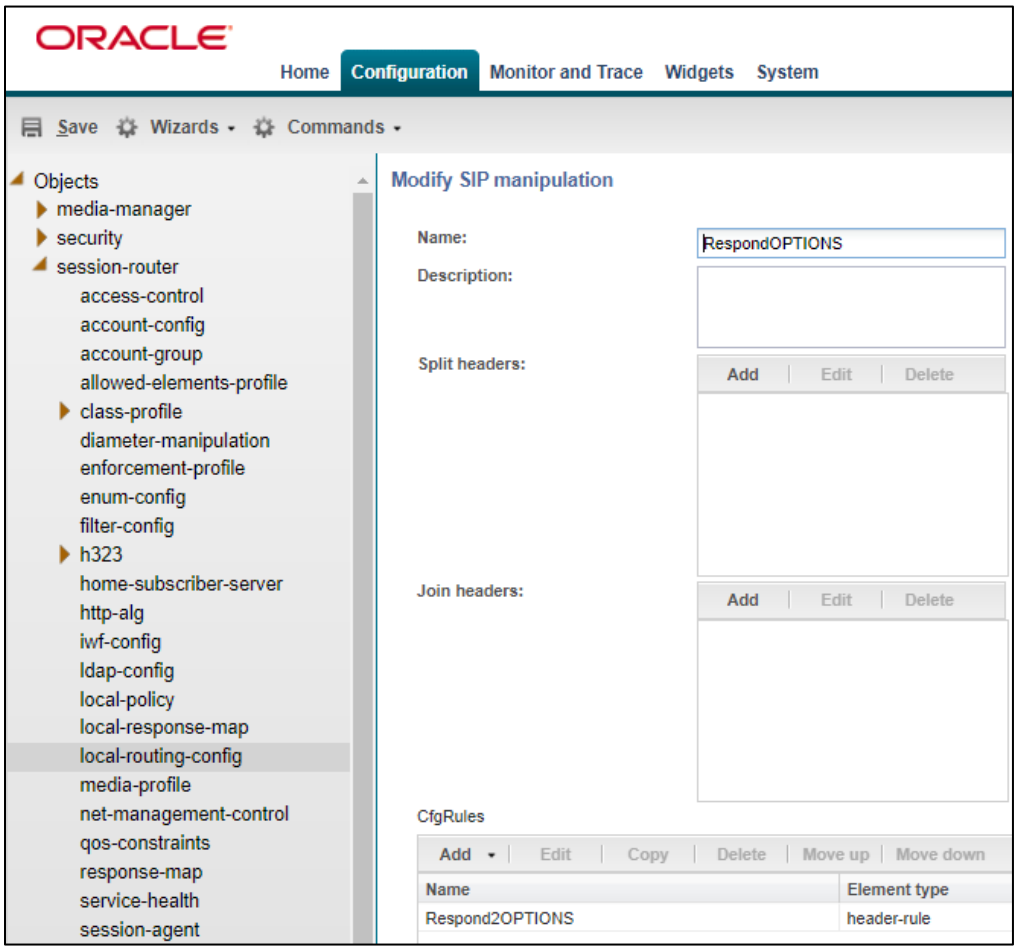
Element Rules:



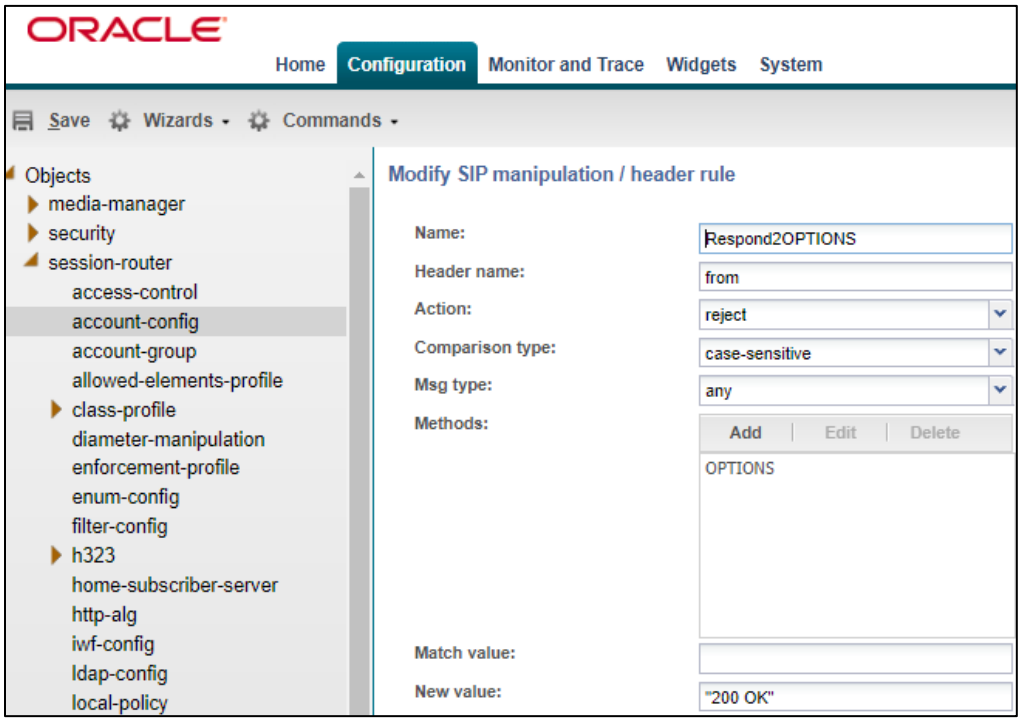


The following SIP manipulation will be applied as the in-manipulationId to be applied to Options Requests generated by Zoom to the SBC. This will allow the SBC to respond locally to Options Requests.

Please note, 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.



Header Rule:



7.7.2 Session Timer Profile (Optional)

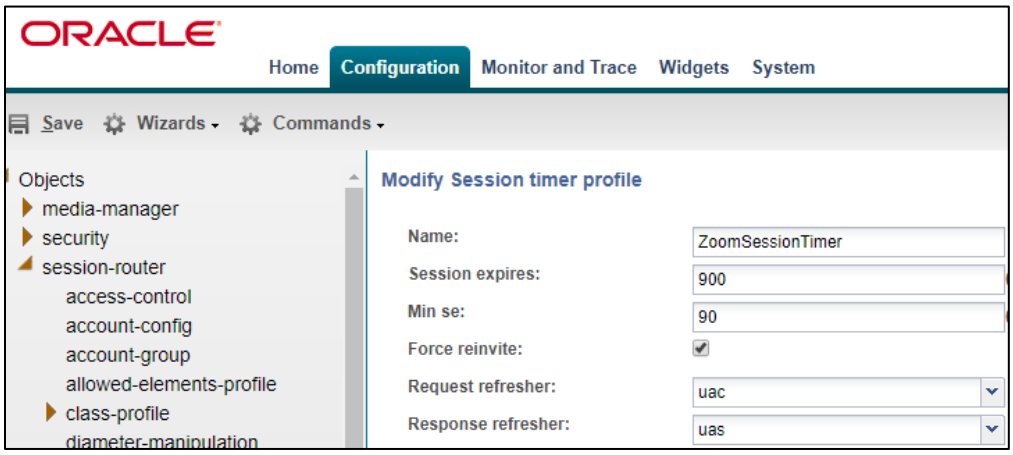
Zoom Phone does support RFC 4028 Session Timers In SIP. In many cases, RFC 4028 is not supported by carriers providing SIP trunking services to their customers. In order to accommodate this, the SBC will interwork between PSTN carrier and Zoom Phone in order to provide support for Session Timers in SIP.

For more information about the Oracle SBC's support for RFC4028, please see the 830 Configuration Guide, page 4-300

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

ACLI Path: config t→session-rouer→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.



7.7.3 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

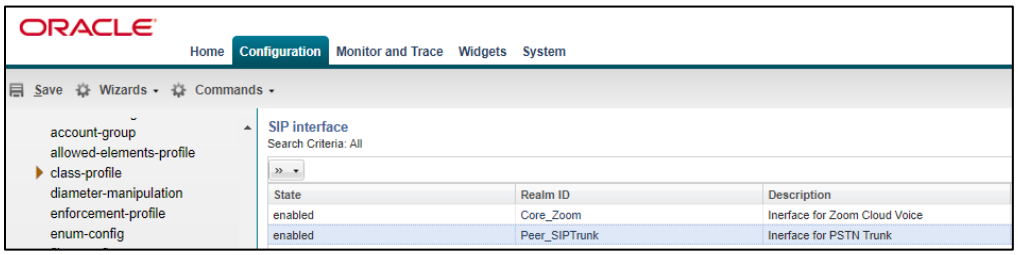
Click Add, and use the table below as an example to Configure:

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

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

Use the following as an example to configure SIP interaces:

Config Parameter	SIPTrunk	Zoom
Realm ID	Peer_SIPTrunk	Core_Zoom
Out manipulationid		RespondOPTIONS
In manipulationid		ZoomE164
SIP Port Config Parmeter	**SIP Trunk**	**Teams**
Address	192.168.1.10	155.212.214.177
Port	5060	5061
Transport protocol	UDP	TLS
TLS profile		TLSZoom
Allow anonymous	agents-only	agents-only
Session Timer Profile		ZoomSessionTimer



7.7.4 Session Agents

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

GUI Path: session-router/session-agent

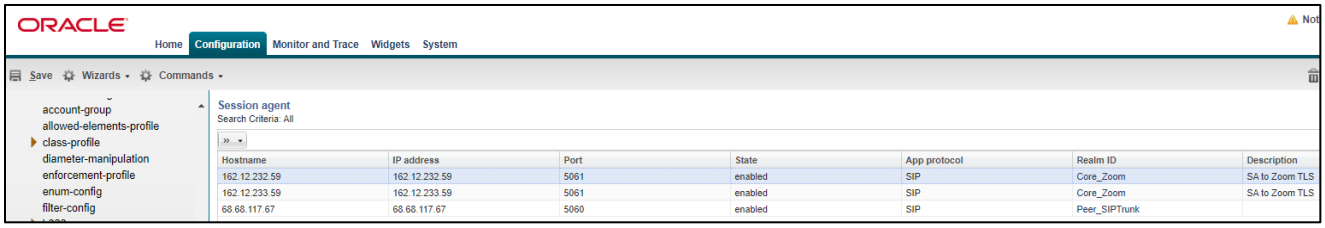
ACLI Path: config t→session-router→session-agent

You will need to configure two session agents for Zoom Phone, and in our example, one for SIPTrunk.

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

Config parameter	Zoom 1	Zoom 2	SIPTrunk
Hostname	162.12.232.59	162.12.233.59	68.68.117.67
IP Address	162.12.232.59	162.12.233.59	68.68.117.67
Port	5061	5061	5060
Transport method	StaticTLS	StaticTLS	UDP+TCP
Realm ID	Core_Zoom	Core_Zoom	Peer_SIPTrunk
Ping Method	OPTIONS	OPTIONS	OPTIONS
Ping Interval	30	30	30
Ping Response	Enabled	Enabled	Enabled

Note: Ping Response enabled takes the place of the [Respond Options Sip Manipulation Rule]



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

7.7.5 Session Agent Group

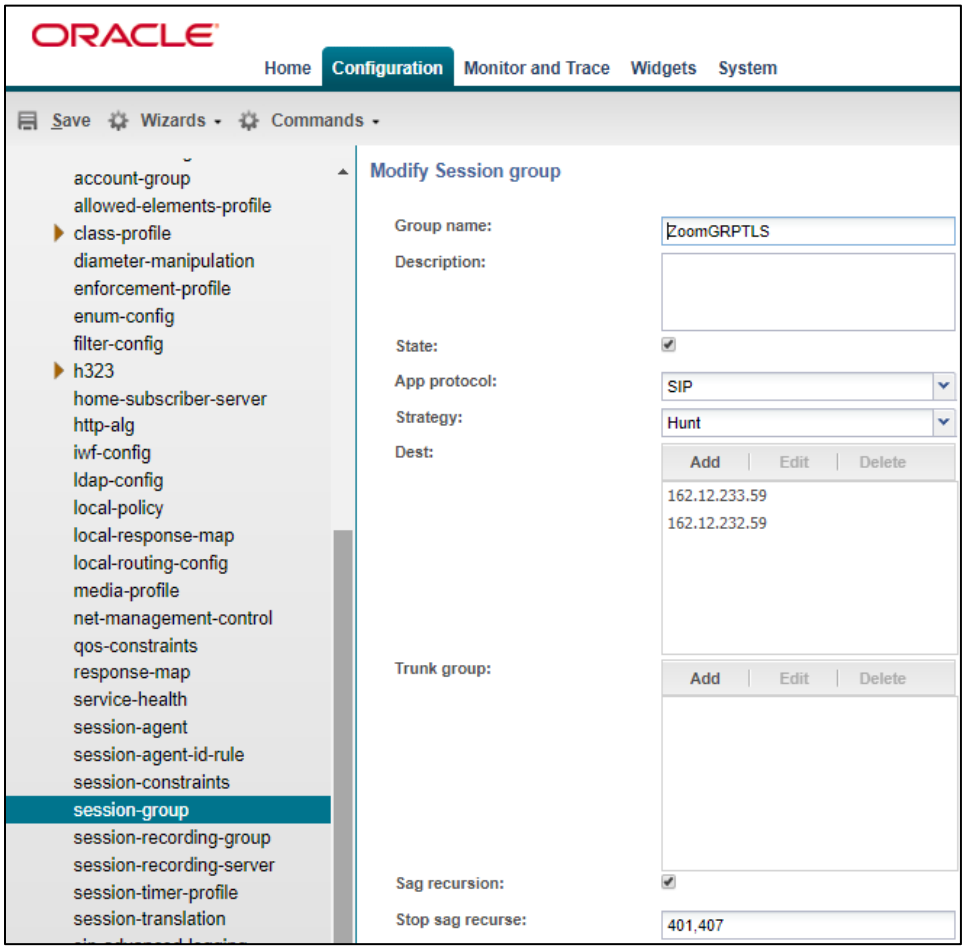
A session agent group allows the SBC to create a load balancing model:

Both session agents configured for Zoom above will be added to the group.

GUI Path: session-router/session-group

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

- Click Add, and use the following as an example to configure:



- Click OK at the bottom

7.7.6 Routing Configuration

This section outlines how to configure the ORACLE ESBC to route SIP traffic to and from PSTN 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.

7.7.7 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.

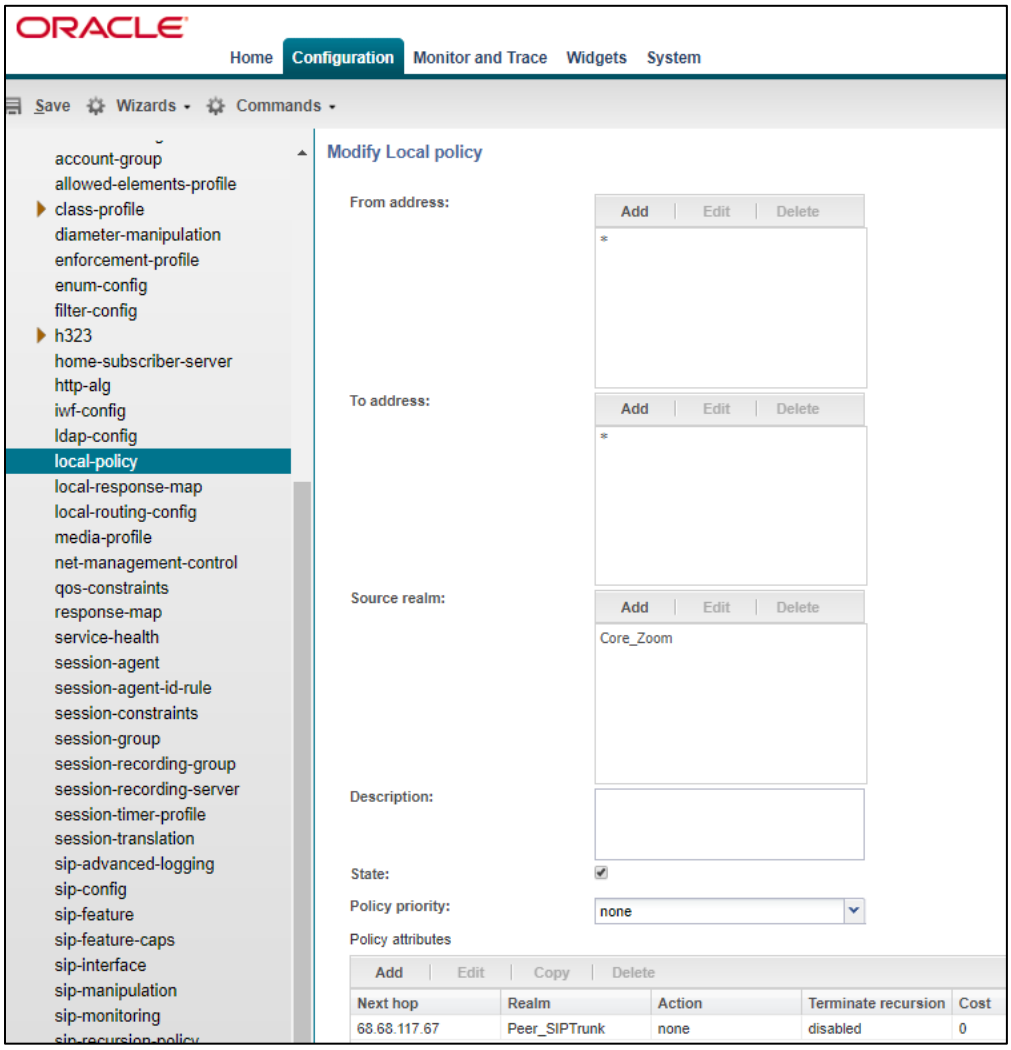
GUI Path: session-router/local-policy

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

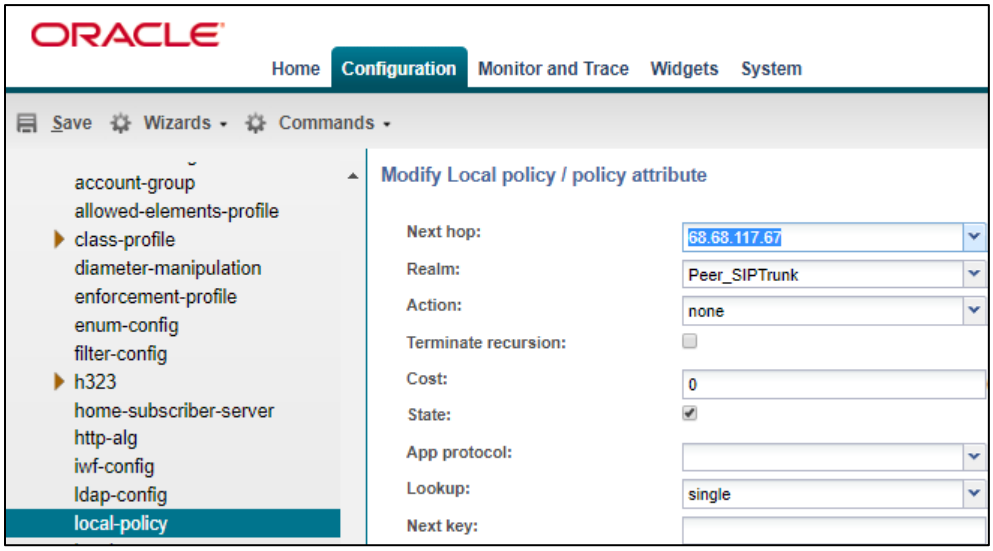
In order to route SIP traffic to and from Zoom Phone Platform, the following local-policies will need to be configured.

- Click Add and use the following and an example to configure:

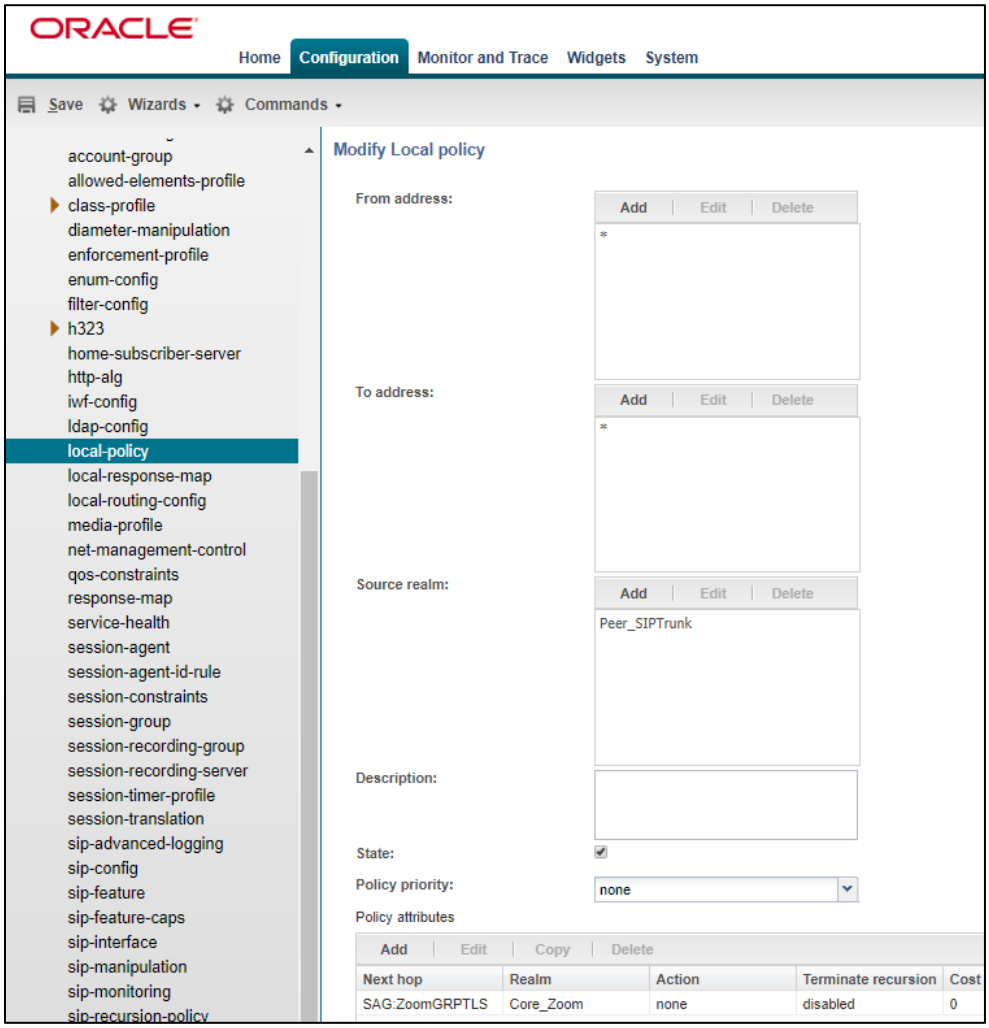
Route Calls from Zoom To PSTN:



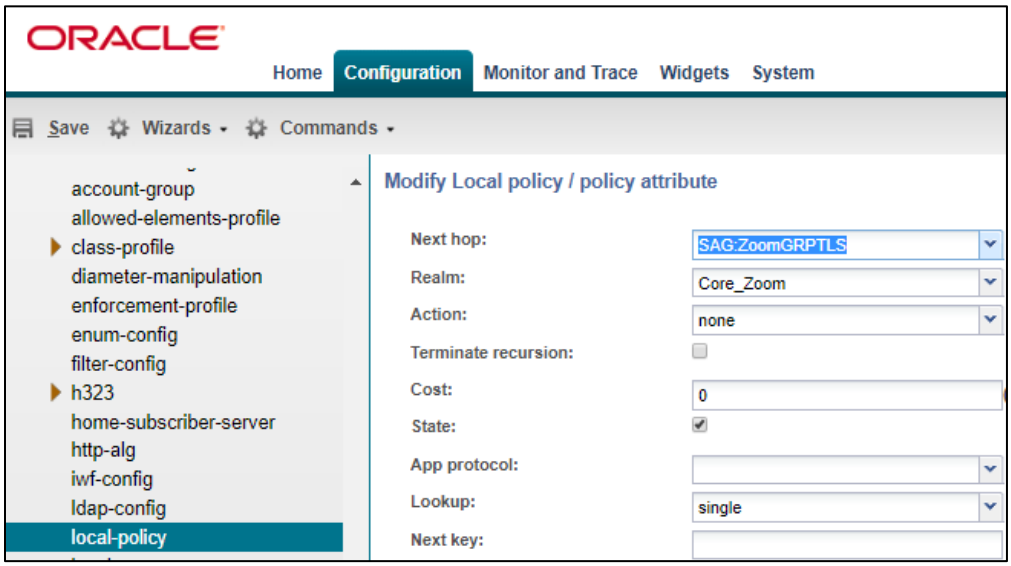
Policy Attribute:



Calls from PSTN To Zoom:



Policy Attribute:



- Click OK at the bottom of each when applicable:

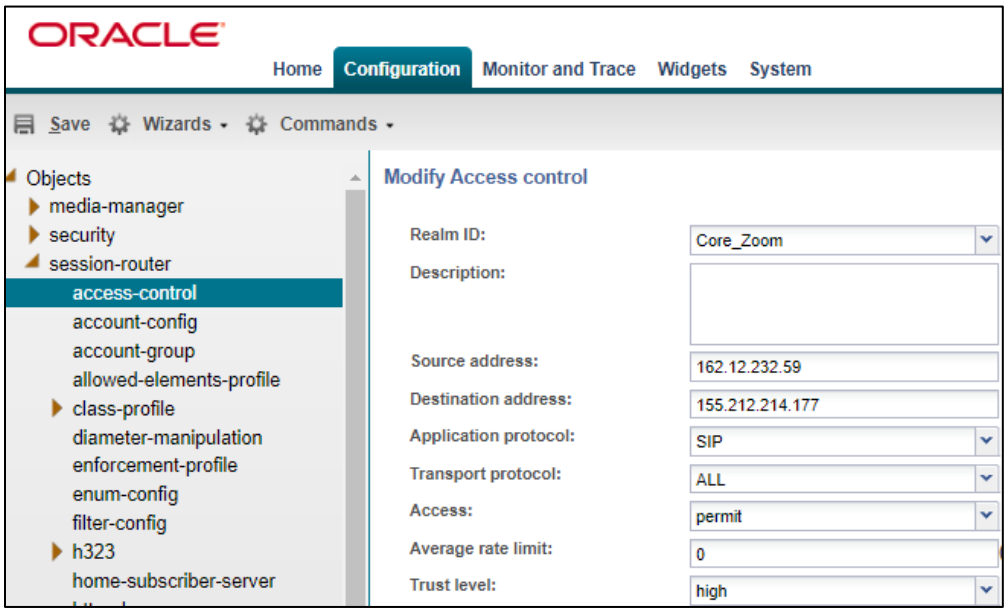
7.7.8 Access Controls

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 both Zoom IP's, as well as SIPTrunk IP's (if applicable).



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 create 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.

- Click OK at the bottom

Save and Activate your configuration!

The SBC configuration is now complete. Move to verify the connection with Zoom!

8 Verify Connectivity

8.1 ORACLE ESBC Options Ping

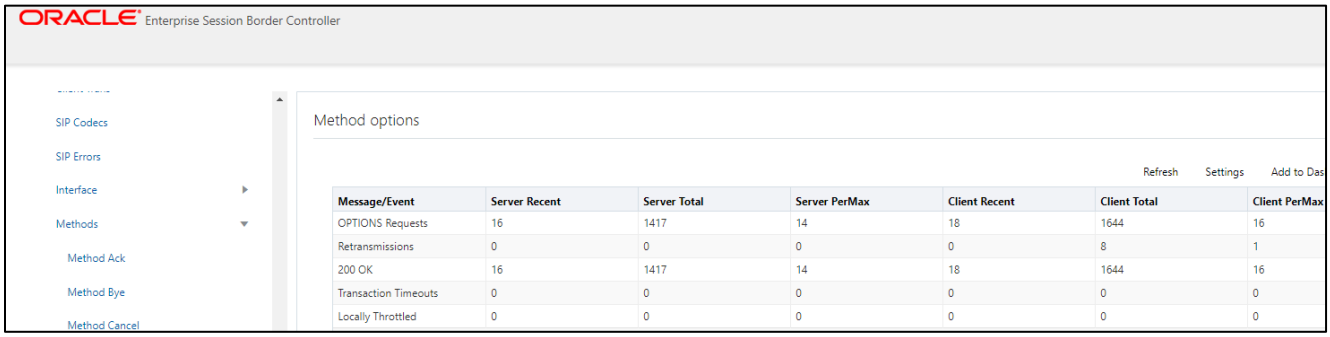
After you've paired the ORACLE ESBC with Zoom, validate that the SBC can successfully exchange SIP Options with Zoom Cloud Voice.

While in the ORACLE ESBC GUI, Utilize the “Widgets” to check for OPTIONS to and from the SBC.

- At the top, click “Widgits”

This brings up the Wigits menu on the left hand side of the screen

GUI Path: Signaling/SIP/Methods/OPTIONS



Message/Event	Server Recent	Server Total	Server PerMax	Client Recent	Client Total	Client PerMax
OPTIONS Requests	16	1417	14	18	1644	16
Retransmissions	0	0	0	0	8	1
200 OK	16	1417	14	18	1644	16
Transaction Timeouts	0	0	0	0	0	0
Locally Throttled	0	0	0	0	0	0

- Looking at both the **Server Recent** and **Client Recent**, verify the counters are showing OPTIONS Requests and 200OK responses.

9 Appendix A

9.1 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.

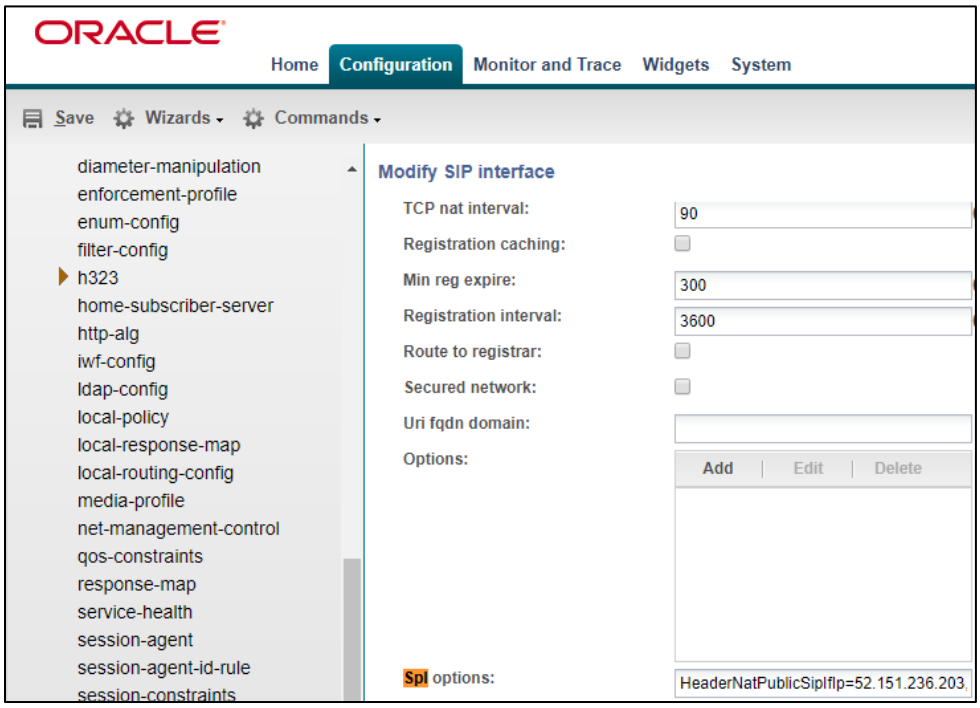
- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

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



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

10 Caveat

10.1 Transcoding Opus Codec

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 DSP's 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 of maxaveragebitrate if negotiated between the parties of each call flow.

11 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_SIPTrunk
        source-address                  68.68.117.67
        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                            DigiCertInter
        common-name                     DigiCert SHA2 Secure Server CA
certificate-record
        name                            DigiCertRoot
        common-name                     DigiCert Global Root CA
certificate-record
        name                            GoDaddyInter
        common-name                     GoDaddy Secure Server CA
certificate-record
        name                            GoDaddyRoot
        common-name                     GoDaddy Class2 Root CA
certificate-record
        name                            SBCEnterpriseCert
        state                           California
        locality                        Redwood City
        organization                    Oracle Corporation
        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
codec-policy
        name                        audiotest
        allow-codecs                  * SILK:no G729:no
filter-config
        name                        all
        user                      *
local-policy
        from-address                   *
        to-address                    *
        source-realm                   Core_Zoom
        policy-attribute
                next-hop                     68.68.117.67
                realm                       Peer_SIPTrunk
local-policy
        from-address                   *
        to-address                    *
        source-realm                   Peer_SIPTrunk
        policy-attribute
                next-hop                     SAG:ZoomGRPTLS
                realm                       Core_Zoom
media-manager
        max-untrusted-signaling              1
        min-untrusted-signaling              1
media-profile
        name                        CN
        subname                       wideband
        payload-type                   118
media-profile
        name                        SILK
        subname                       narrowband
        payload-type                   103
        clock-rate                    8000
media-profile
```

```
        name                    SILK
        subname                 wideband
        payload-type            104
        clock-rate              16000
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                 255.255.255.0
        gateway                 155.212.214.1
        dns-ip-primary          8.8.8.8
        dns-domain              customers.telechat.o-test06161977.com
        hip-ip-list             155.212.214.177
        icmp-address            155.212.214.177
network-interface
        name                    s1p0
        ip-address              192.168.1.10
        netmask                 255.255.255.0
        gateway                 192.168.1.1
        hip-ip-list             192.168.1.10
        icmp-address            192.168.1.10
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
        slot                            1
realm-config
        identifier                      Core_Zoom
        description                     Realm Facing Zoom Phone
        network-interfaces              s0p0:0.4
        mm-in-realm                     enabled
        media-sec-policy                sdesPolicy
        access-control-trust-level      high
        refer-call-transfer             enabled
        codec-policy                    audiotest
realm-config
        identifier                      Peer_SIPTrunk
        description                     Ream facing SIP trunk
        network-interfaces              s1p0:0.4
        mm-in-realm                     enabled
        qos-enable                      enabled
        media-sec-policy                RTP
        access-control-trust-level      high
        codec-policy                    OptimizeCodecs
        hide-egress-media-update        enabled
sdes-profile
        name                            SDES
        crypto-list                     AES_CM_128_HMAC_SHA1_32
                                        AES_CM_128_HMAC_SHA1_80
        lifetime                        31
session-agent
        hostname                        162.12.232.59
        ip-address                      162.12.232.59
        port                            5061
        transport-method                StaticTLS
        realm-id                        Core_Zoom
        description                     SA to Zoom TLS
        ping-method                     OPTIONS
```

```
        ping-interval                   30
        in-manipulationid               RespondOPTIONS
        out-manipulationid              ZoomE164
session-agent
        hostname                        162.12.233.59
        ip-address                      162.12.233.59
        port                            5061
        transport-method                StaticTLS
        realm-id                        Core_Zoom
        description                     SA to Zoom TLS
        ping-method                     OPTIONS
        ping-interval                   30
        in-manipulationid               RespondOPTIONS
        out-manipulationid              ZoomE164
session-agent
        hostname                        68.68.117.67
        ip-address                      68.68.117.67
        realm-id                        Peer_SIPTrunk
        ping-method                     OPTIONS
        ping-interval                   60
session-group
        group-name                      ZoomGRPTLS
        dest                            162.12.233.59
                                        162.12.232.59
        sag-recursion                   enabled
session-timer-profile
        name                            ZoomSessionTimer
        session-expires                 900
        force-reinvite                  enabled
        response-refresher              uac
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                 Inerface for Zoom Phone
    SIP-port
        address                 155.212.214.177
        port                    5061
        transport-protocol      TLS
        tls-profile             TLSZoom
        allow-anonymous         agents-only
    in-manipulationid           RespondOPTIONS
    out-manipulationid          ZoomE164
    SIP-profile                 forreplaces
    session-timer-profile       ZoomSessionTimer
SIP-interface
    realm-id                    Peer_SIPTrunk
    description                 Inerface for PSTN Trunk
    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                        ZoomE164
    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                    addContactOptions
        header-name             Contact
        action                  add
        msg-type                request
        methods                 OPTIONS
        new-value               "<SIP:ping@"+155.212.214.177+":5061>"
SIP-monitoring
    match-any-filter            enabled
    monitoring-filters          *
SIP-profile
    name                        forreplaces
    replace-dialogs             enabled
steering-pool
    ip-address                  192.168.1.10
    start-port                  20000
    end-port                    40000
    realm-id                    Peer_SIPTrunk
steering-pool
    ip-address                  155.212.214.177
    start-port                  20000
    end-port                    40000
    realm-id                    Core_Zoom
```

```
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     GoDaddyInter
                                    GoDaddyRoot
        mutual-authenticate         enabled
web-server-config
        http-interface-list         GUI
```


Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/Oracle/

twitter.com/Oracle

oracle.com

Integrated Cloud Applications & Platform Services