ORACLE

Oracle SBC with Analog Devices and Zoom Phone

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 5
1.1 ORACLE SBC DOCUMENTATION 5
1.2 ZOOM PHONE DOCUMENTATION 5
1.3 POLY OBI302 ATA DOCUMENTATION 5

2 REVISION HISTORY 5

3 INTENDED AUDIENCE 5
3.1 VALIDATED ORACLE VERSIONS 5
3.2 SETUP REQUIREMENTS 6

4 ZOOM PHONE CONFIGURATION 6
4.1 REGISTRATION CONFIGURATION. 6
4.1.1 Create a Zoom User 6
4.2 ADD BYOC NUMBER 7
4.3 ASSIGN THE BYOC NUMBER TO A USER 8
4.4 REGISTER THE SBC INTERFACE ON ZOOM PORTAL 9
4.5 PROVISIONING 10

5 POLY OBI 302 CONFIGURATION 12

6 ORACLE SBC CONFIGURATION 14
6.1 PREREQUISITES 14
6.2 GLOBAL CONFIGURATION ELEMENTS 15
6.2.1 System-Config 15
6.2.2 Media Manager 16
6.2.3 SIP Config 17
6.2.4 NTP Config 18
6.3 NETWORK CONFIGURATION 19
6.3.1 Physical Interfaces 19
6.3.2 Network Interfaces 20
6.4 SECURITY CONFIGURATION 21
6.4.1 Certificate Records 21
6.4.2 SBC End Entity Certificate 22
6.5 ROOT CA AND INTERMEDIATE CERTIFICATES 23
6.5.1 Oracle SBC and Zoom Certificate 23
6.5.2 Generate Certificate Signing Request 23
6.5.3 Import Certificates to SBC 24
6.5.4 TLS Profile 25
6.6 MEDIA SECURITY CONFIGURATION 26
6.6.1 Sdes-profile 26
6.6.2 Media Security Policy 27
6.7 MEDIA CONFIGURATION 29
6.7.1 Realm Config 29
6.7.2 Steering Pools 30
6.8 SIP CONFIGURATION 30
6.8.1 SIP Manipulations 30
6.9 SESSION-TRANSLATION 36
6.10 SESSION TIMER PROFILE (OPTIONAL) 38

6.11 SIP INTERFACE 39
6.12 SESSION AGENTS 41
6.13 LOCAL POLICY CONFIGURATION 41
6.13.1 Route Calls from Zoom Trunk To PSTN: 42
6.13.2 Route Calls from PSTN To Zoom: 43
6.14 ACCESS CONTROLS 43

7 VERIFY CONNECTIVITY 44
7.1 ORACLE SBC OPTIONS PING 44

8 SBC BEHIND NAT SPL CONFIGURATION 45

9 CAVEAT 46
9.1 TRANSCODING OPUS CODEC 46

1 Related Documentation

1.1 Oracle SBC Documentation

- Oracle® Enterprise Session Border Controller ACLI Configuration Guide
- Oracle® Enterprise Session Border Controller Release Notes
- Oracle® Enterprise Session Border Controller Security Guide

1.2 Zoom Phone Documentation

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

1.3 Poly OBI302 ATA Documentation

- https://www.poly.com/in/en/products/phones/obi/obi302

2 Revision History

Version	Date Revised	Description of Changes
1.0	22/07/2021	Initial publication

3 Intended Audience

This document describes how to connect Analog Devices to Oracle SBC and Zoom Phone.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:

SCZ840p4a

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

3.2 Setup Requirements

Analog Telephony Adapter	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	

4 Zoom Phone Configuration

This Section covers the steps required to configure the Analog Telephony Adapter onto the Zoom Web Portal. For the purpose of Lab Testing we have used **Poly OBI302 Analog Telephone Adapter**. The steps to interwork any other brand ATA Device will remain similar, however there may be changes in the way each device is configured depending upon their make/Model.

4.1 Registration Configuration.

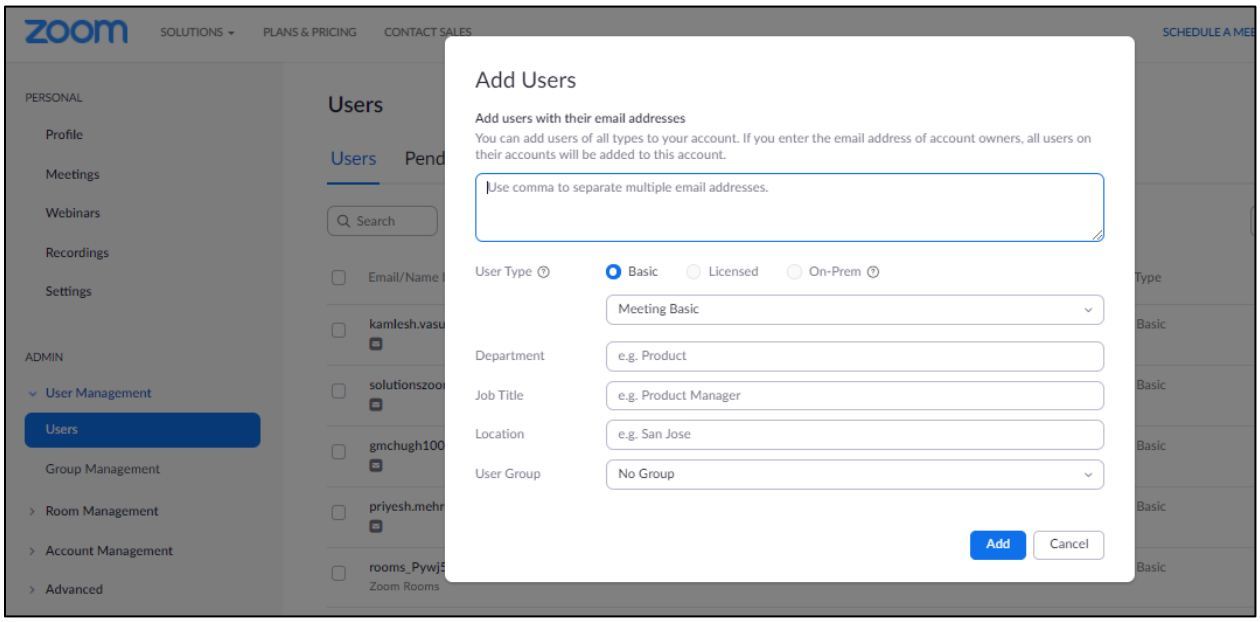
In this Section, we will talk about how to register the Poly OBI302 Device onto Zoom PBX via Oracle SBC.

4.1.1 Create a Zoom User

Navigate to **Admin>User Management > Users.**

Click **Add Users** to create a new Zoom user. Provide the necessary details about the New User and click on Add.

Note : This step can be skipped in case you want use an existing Zoom Phone User.



Once the New User is added it will start reflecting in **Admin >Users** Section on the Web portal.

4.2 Add BYOC Number

Navigate to **Phone Systems Management > Phone Numbers > BYOC**

Select **Add** to add external phone numbers provided by your carrier into the Zoom portal.

Site - Choose the relevant Site on which the Number needs to be added.

For Example, Main Site.

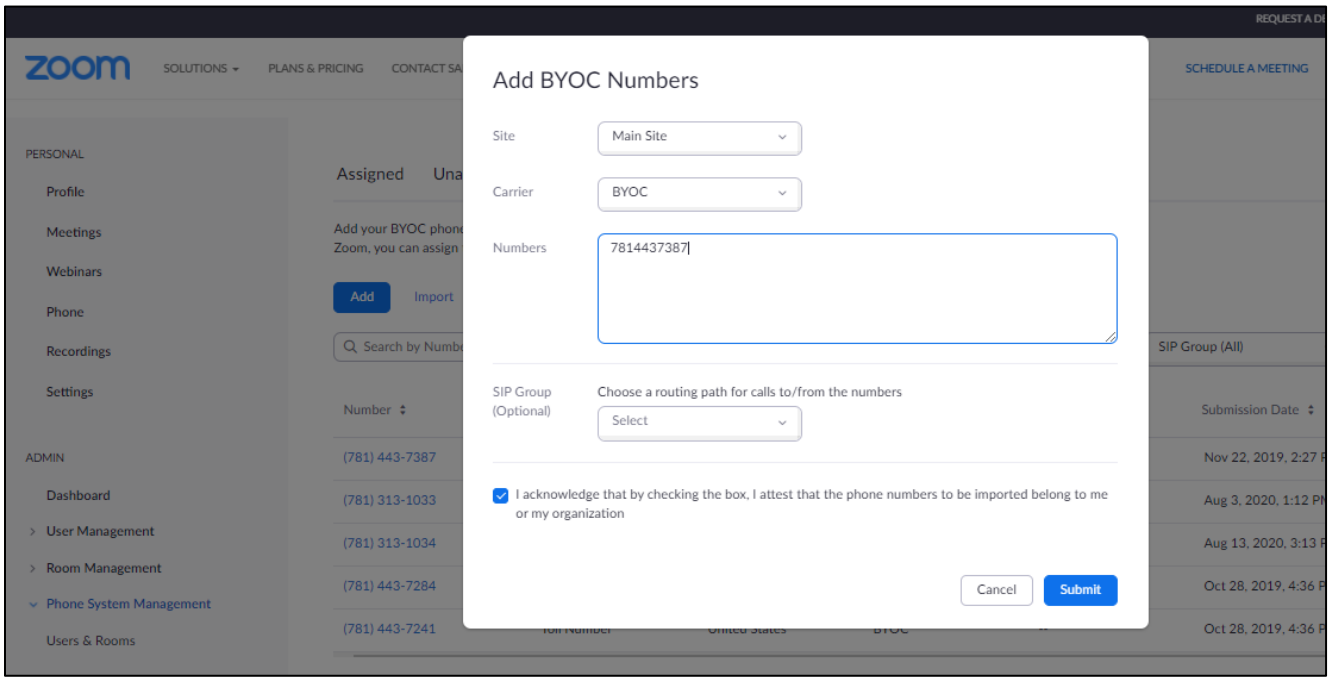
Carrier –Choose BYOC

Numbers- Put the BYOC DID Number provided by your Carrier.

SIP Group – Optional Parameter (Can be Left Blank)

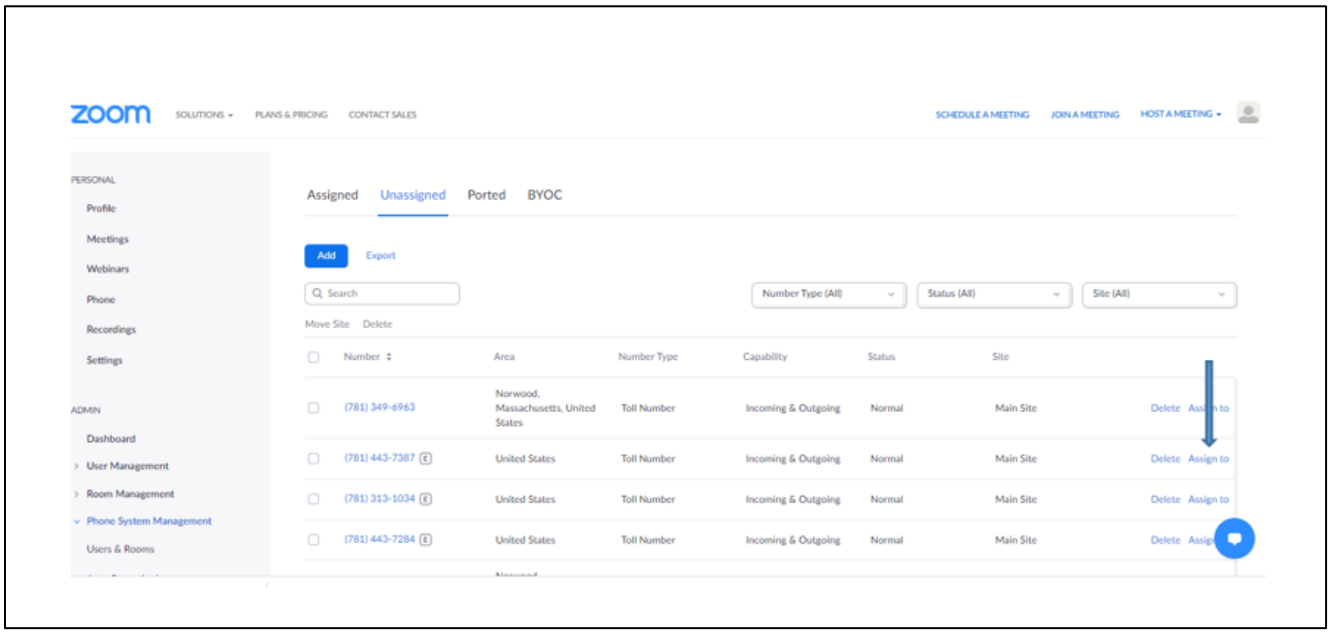
Acknowledge that the Phone Number belongs to your organization.

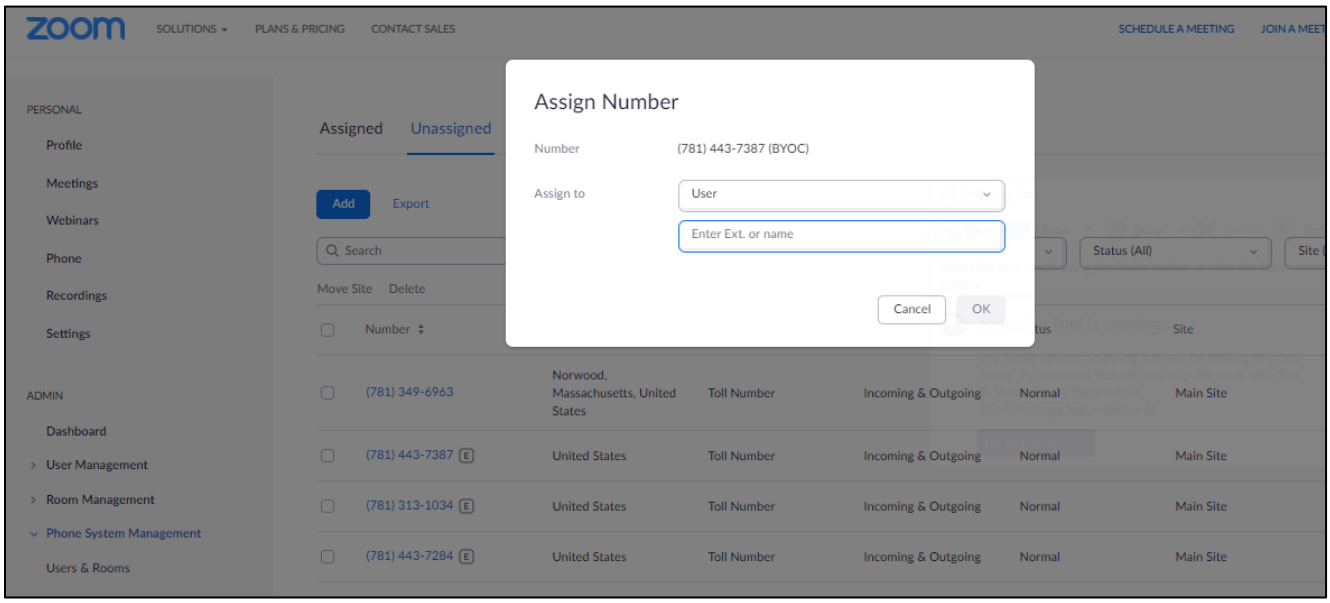
Click **Submit**.



4.3 Assign the BYOC Number to a User

The BYOC Number will now be visible in the Unassigned Tab on the portal. Click on Assign to Tab to assign the Number to This User.





4.4 Register the SBC Interface on Zoom Portal

The analog device registers on the Zoom Cloud PBX which is located at the Core Side of Oracle SBC. Oracle SBC is used as a Proxy the register from Poly ATA Device on Zoom Cloud Voice. We will add the SBC Media interface that communicates with the Zoom PBX Registrar, as a device on Zoom Web Portal.

Navigate to **Admin>Phone System Management**

Click Add to Add a New Device

Enter the MAC Address of the SBC Media Interface

Click Assign and then Add to assign this Device to the previously created User.

The SBC MAC Address can be found by running the ACLI command –

- ***Show Interfaces***

NN4600-139# show interfaces

M10 (media slot 0, port 2)

Flags: UP BROADCAST MULTICAST ARP RUNNING

Type: GIGABIT_ETHERNET

Admin State: enabled

Auto Negotiation: enabled

Internet address: 10.232.50.65 Vlan: 0

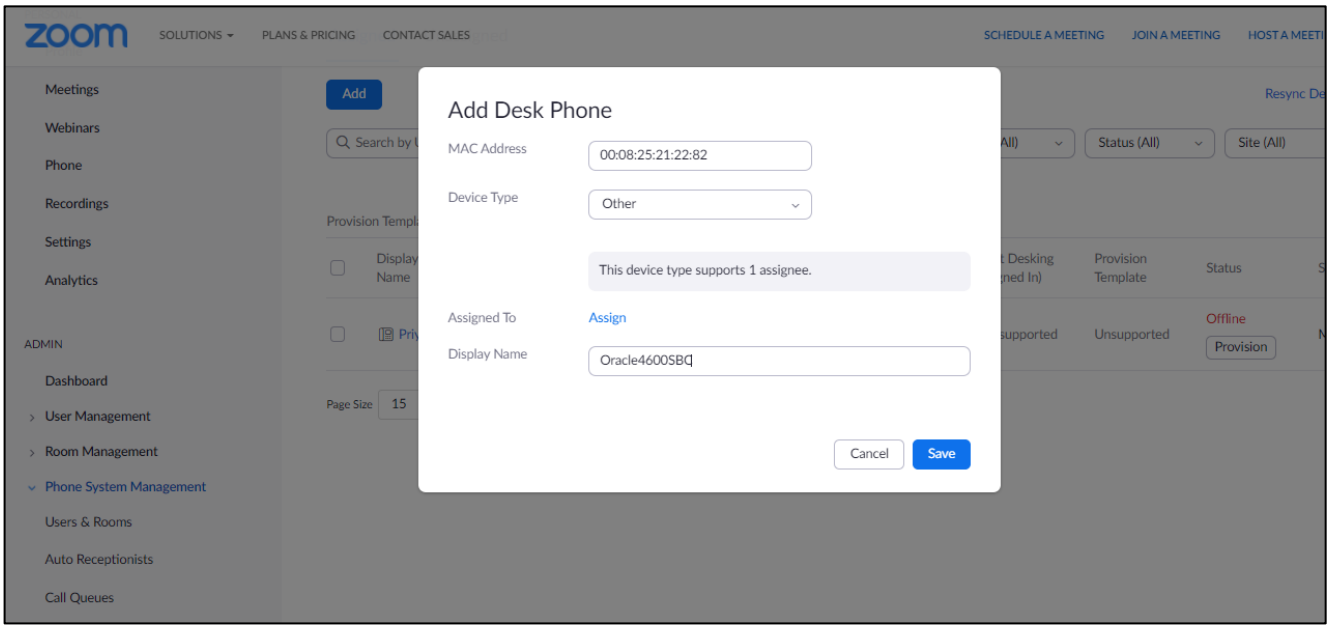
Broadcast Address: 10.232.50.255

Netmask: 255.255.255.0

Gateway: 10.232.50.1

Maximum Transfer Unit size is 1500

Ethernet address is 00:08:25:21:22:82

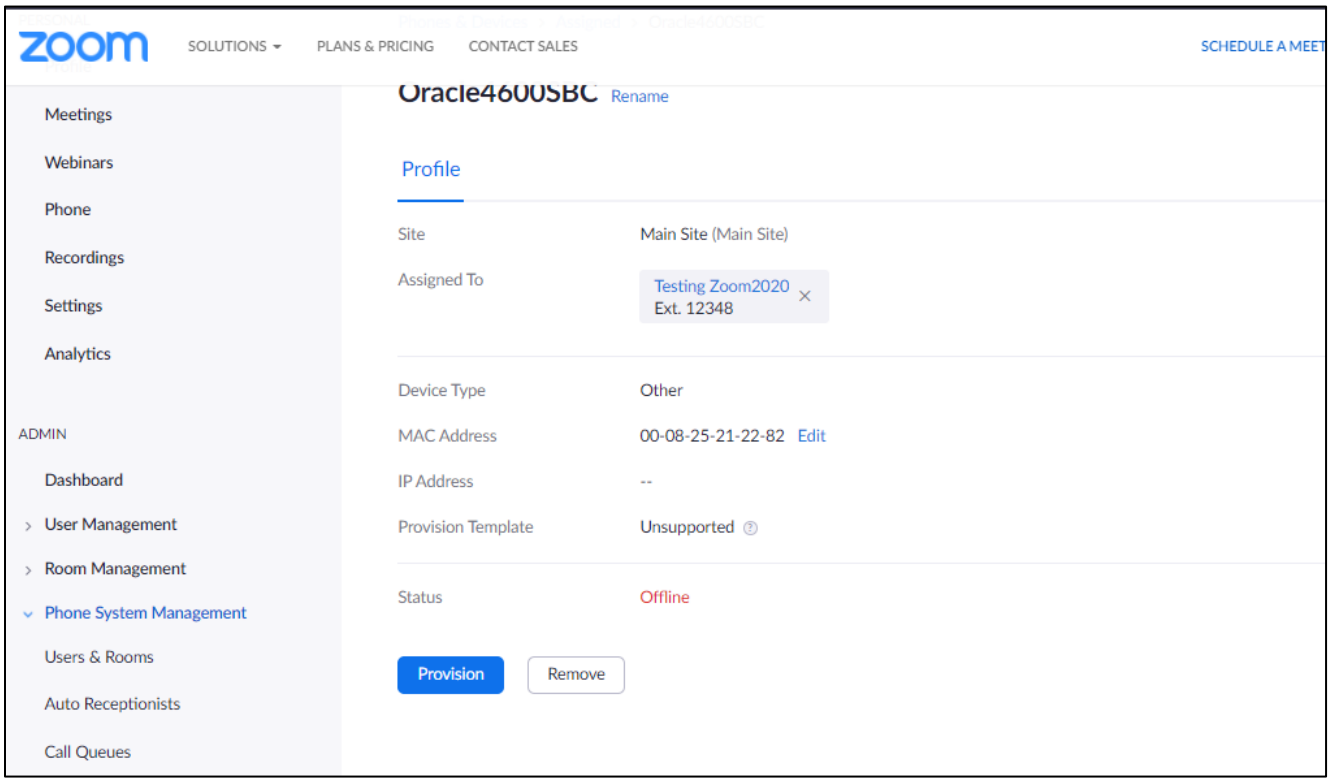


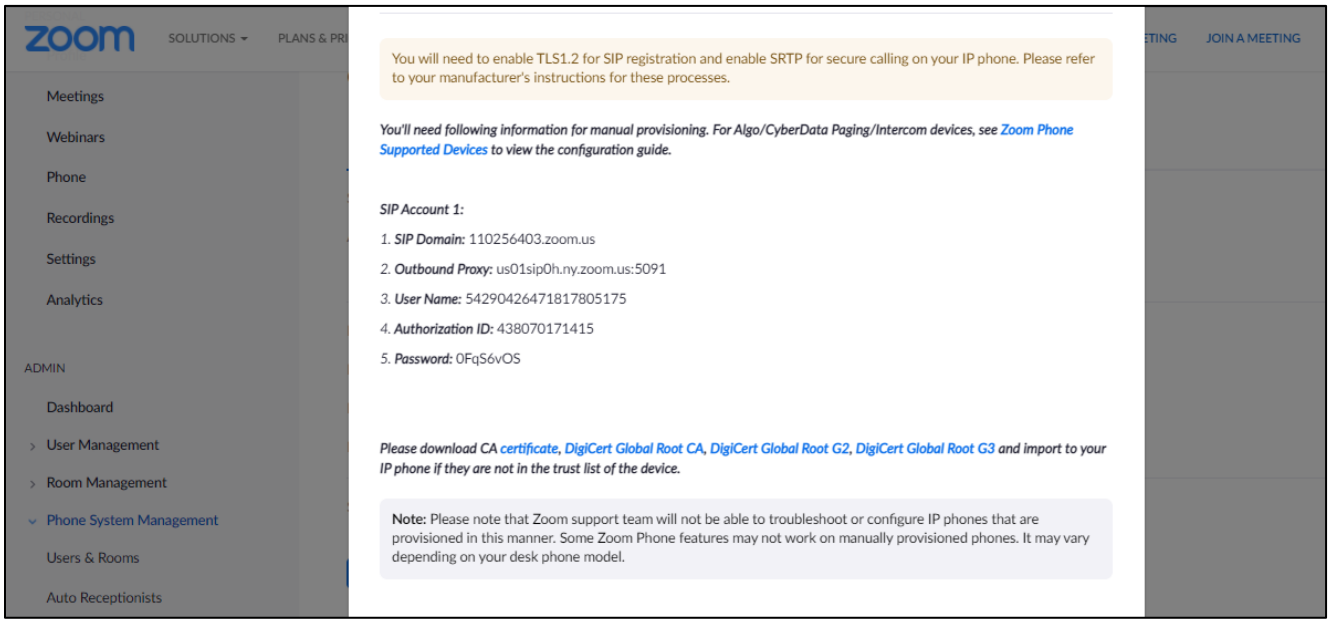
4.5 Provisioning

Once the Device is successfully added, a **Provision** Button will appear at the bottom of the screen.

Click Provision to discover the Zoom Registrar details as shown in the example below. These details will be required to configure the Poly OBI302 ATA Device.

Note these details as they will be required to configure the device for registration. Download the CA certificates as they will be required for the tls communication of Oracle SBC with Zoom Registrar as mentioned in Section 6.4 Security configuration.


zoom
SOLUTIONS
PLANS & PRICING
CONTACT SALES
SCHEDULE A MEET
Meetings
Webinars
Phone
Recordings
Settings
Analytics
ADMIN
Dashboard
User Management
Room Management
Phone System Management
Users & Rooms
Auto Receptionists
Call Queues
Oracle4600SBC
Rename
Profile
Site
Main Site (Main Site)
Assigned To
Testing Zoom2020
Ext. 12348
Device Type
Other
MAC Address
00-08-25-21-22-82
Edit
IP Address
--
Provision Template
Unsupported
Status
Offline
Provision
Remove

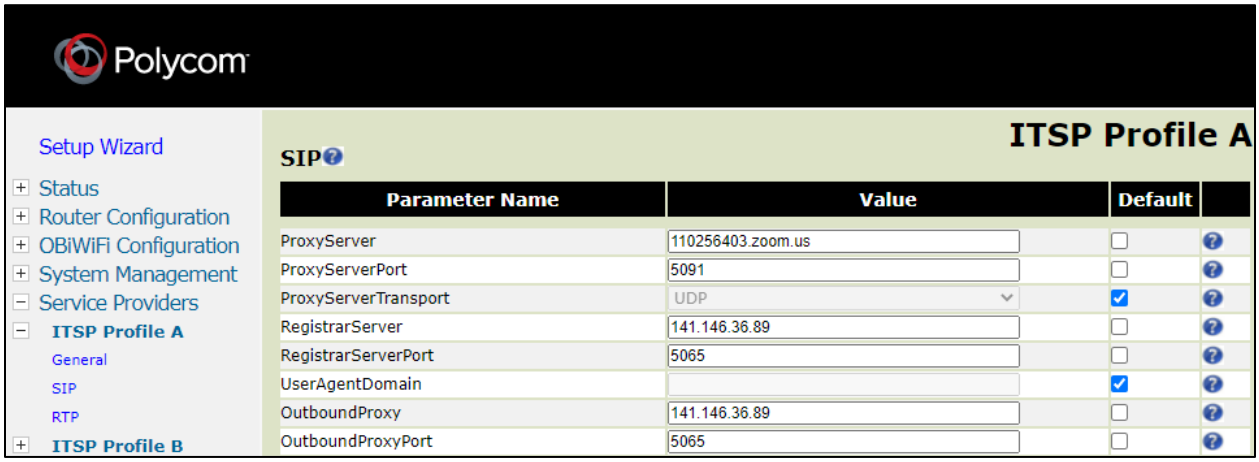

zoom
SOLUTIONS
JOIN A MEETING
Meetings
Webinars
Phone
Recordings
Settings
Analytics
ADMIN
Dashboard
User Management
Room Management
Phone System Management
Users & Rooms
Auto Receptionists
You will need to enable TLS1.2 for SIP registration and enable SRTP for secure calling on your IP phone. Please refer to your manufacturer's instructions for these processes.
You'll need following information for manual provisioning. For Algo/CyberData Paging/Intercom devices, see Zoom Phone Supported Devices to view the configuration guide.
SIP Account 1:
1. SIP Domain: 110256403.zoom.us
2. Outbound Proxy: us01sip0h.ny.zoom.us:5091
3. User Name: 54290426471817805175
4. Authorization ID: 438070171415
5. Password: 0FqS6vOS
Please download CA certificate, DigiCert Global Root CA, DigiCert Global Root G2, DigiCert Global Root G3 and import to your IP phone if they are not in the trust list of the device.
Note: Please note that Zoom support team will not be able to troubleshoot or configure IP phones that are provisioned in this manner. Some Zoom Phone features may not work on manually provisioned phones. It may vary depending on your desk phone model.

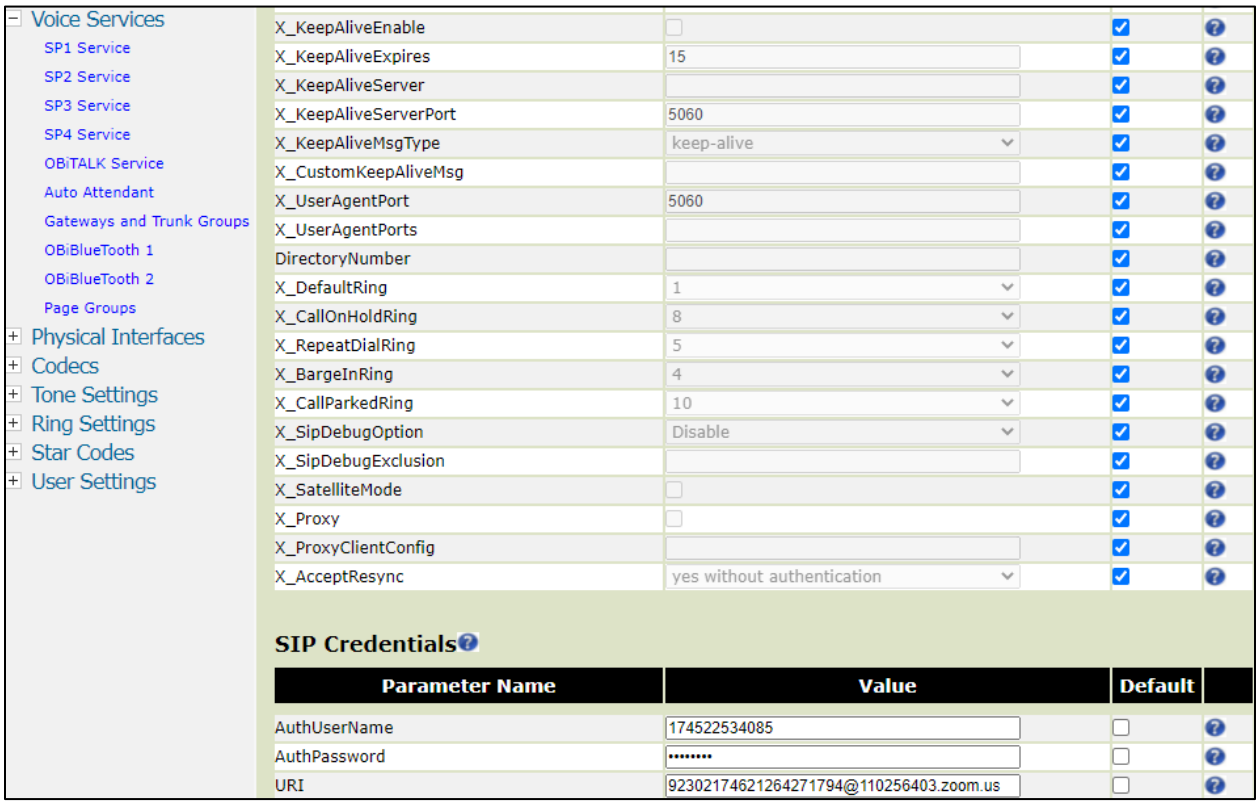
5 Poly OBI 302 Configuration

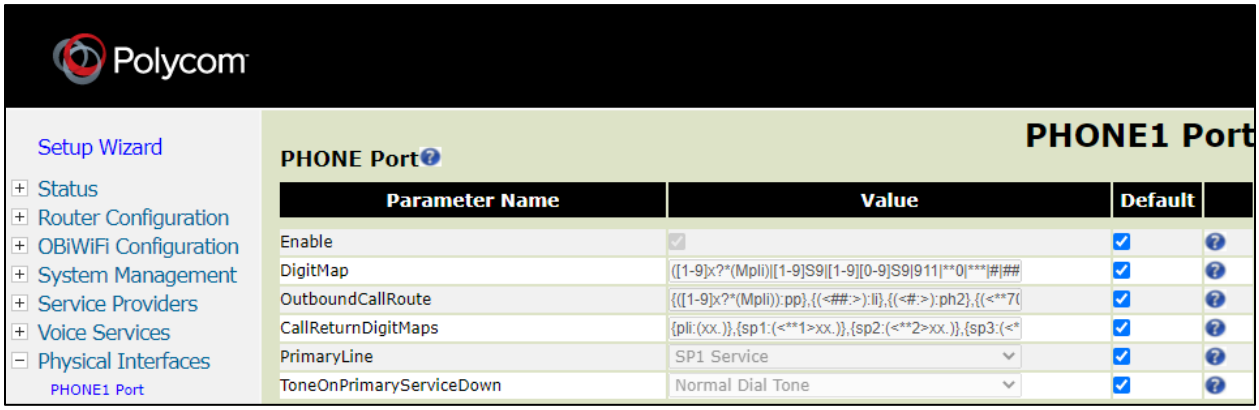
Once the ATA Device is connected and successfully powered on, we will configure it to communicate with the Zoom Cloud Voice through the Oracle SBC. The configuration parameters of the Poly OBI 302 ATA Adapter are illustrated in snippets below.

The Registrar Details discovered at the time of provisioning and the SBC configuration will be used to register the Poly OBI 302 ATA Device. Use below example as a reference for your configuration.

Discovered Configuration Element	ATA Configuration Element	Sample Value
Sip Domain	Proxy Server	110256403.zoom.us
Outbound Proxy Port	Proxy Server Port	5091
SBC Access Sip Interface IP Address	Registrar Server	141.146.36.89
SBC Access Sip Interface Port	Registrar Server Port	5065
SBC Access Sip Interface IP Address	Outbound Proxy	141.146.36.89
SBC Access Sip Interface Port	Outbound Proxy Port	5065
Authorization ID	Auth User Name	438070171415
Password	Auth Password	oFqS6vOS
Username@ProxyServer	URI	5429042647181780517 5@110256403.zoom.us




Voice Services
SP1 Service
SP2 Service
SP3 Service
SP4 Service
OBiTALK Service
Auto Attendant
Gateways and Trunk Groups
OBiBlueTooth 1
OBiBlueTooth 2
Page Groups
Physical Interfaces
Codecs
Tone Settings
Ring Settings
Star Codes
User Settings
X_KeepAliveEnable
X_KeepAliveExpires 15
X_KeepAliveServer
X_KeepAliveServerPort 5060
X_KeepAliveMsgType keep-alive
X_CustomKeepAliveMsg
X_UserAgentPort 5060
X_UserAgentPorts
DirectoryNumber
X_DefaultRing 1
X_CallOnHoldRing 8
X_RepeatDialRing 5
X_BargeInRing 4
X_CallParkedRing 10
X_SipDebugOption Disable
X_SipDebugExclusion
X_SatelliteMode
X_Proxy
X_ProxyClientConfig
X_AcceptResync yes without authentication
SIP Credentials
Parameter Name
Value
Default
AuthUserName 174522534085
AuthPassword ••••••••
URI 9230217462126427179 4@110256403.zoom.us


Polycom
Setup Wizard
Status
Router Configuration
OBiWiFi Configuration
System Management
Service Providers
Voice Services
Physical Interfaces
PHONE1 Port
PHONE1 Port
PHONE Port
Parameter Name
Value
Default
Enable
DigitMap ([1-9]x?*(Mpli)|[1-9]S9|[1-9][0-9]S9|911|**0|***|#|##
OutboundCallRoute {([1-9]x?*(Mpli)):pp},{(<##:>):li},{(<#:>):ph2},{(<**7(
CallReturnDigitMaps {pli:(xx.)},{sp1:(<**1>xx.)},{sp2:(<**2>xx.)},{sp3:(<*
PrimaryLine SP1 Service
ToneOnPrimaryServiceDown Normal Dial Tone

6 Oracle SBC Configuration

Below is an outline of the network setup used to conduct all testing between the Oracle SBC, Poly OBI 302 ATA, Zoom Phone and the SIP Trunk.

Note - 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

In this section we will provide the steps for such interworking of ATA Device with Zoom Phone via Oracle SBC. The ATA Device registers itself on the Zoom PBX through the Oracle SBC. Calls from the ATA are first forwarded to the registrar which are hair pinned back to the SBC from the Zoom BYOC Trunk IP Address. Zoom has an internal routing to send the call to their BYOC IP which connects to Oracle SBC.SBC further breaks out the call to the PSTN Network through the connected SIP Trunk.

Before you begin, make sure that you have the following per every SBC you want to pair to communicate with Zoom BYOC Trunk.

- 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

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

For the purposes of this Application note, we'll be using the Oracle SBC GUI for all configuration examples.

This guide assumes the Oracle SBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, http-server 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.

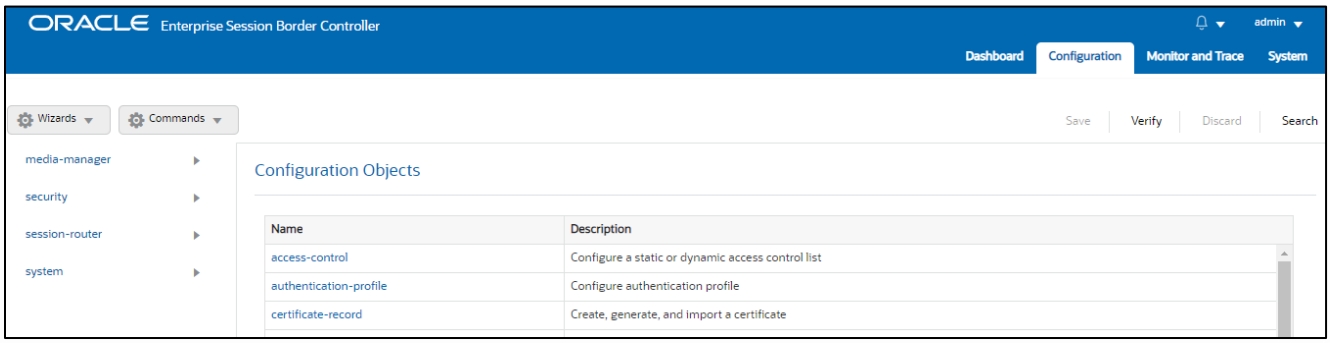
To access the Oracle SBC GUI, enter the management IP address into a web brower.
When the login screen appears, enter the username and password to access the ORACLE SBC.

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

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.

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.In this testing,The connection between Poly OBI302 Device and Oracle SBC is UDP in this setup.

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!!!



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 (ntp optional) to proceed.

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

6.2.1 System-Config

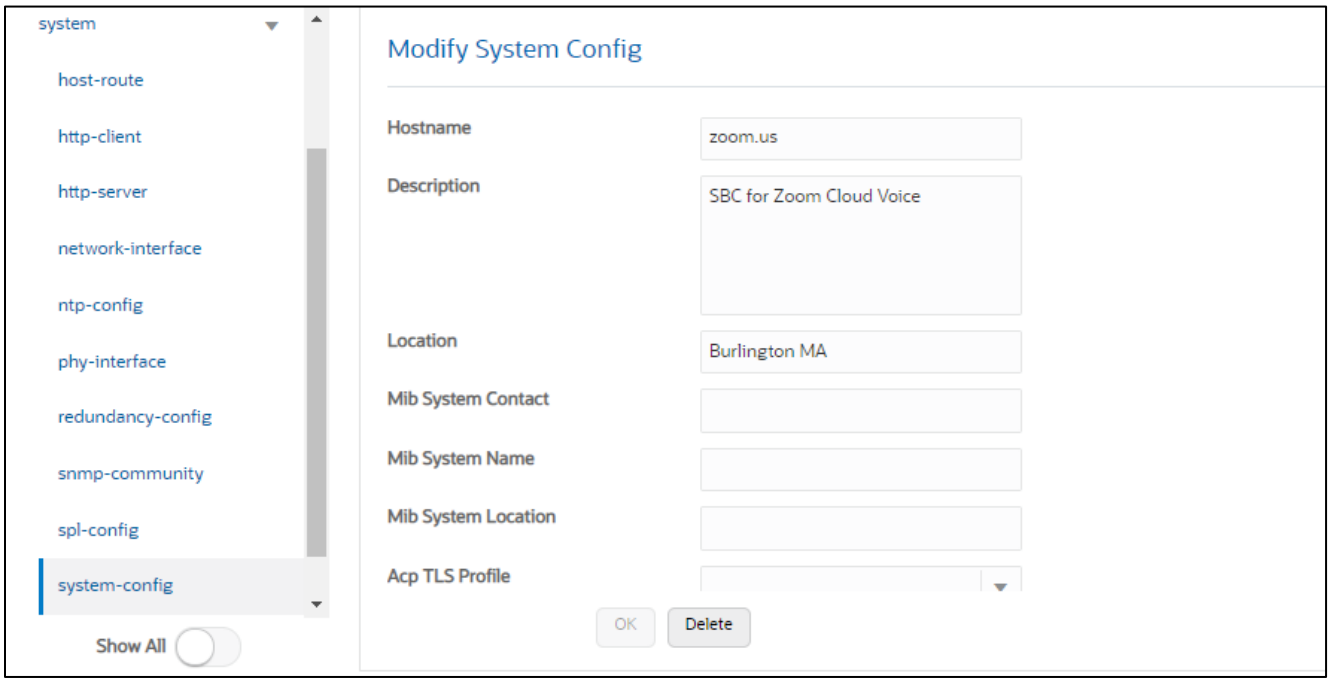
To configure system level functionality for the ORACLE SBC, you must first enable the system-config

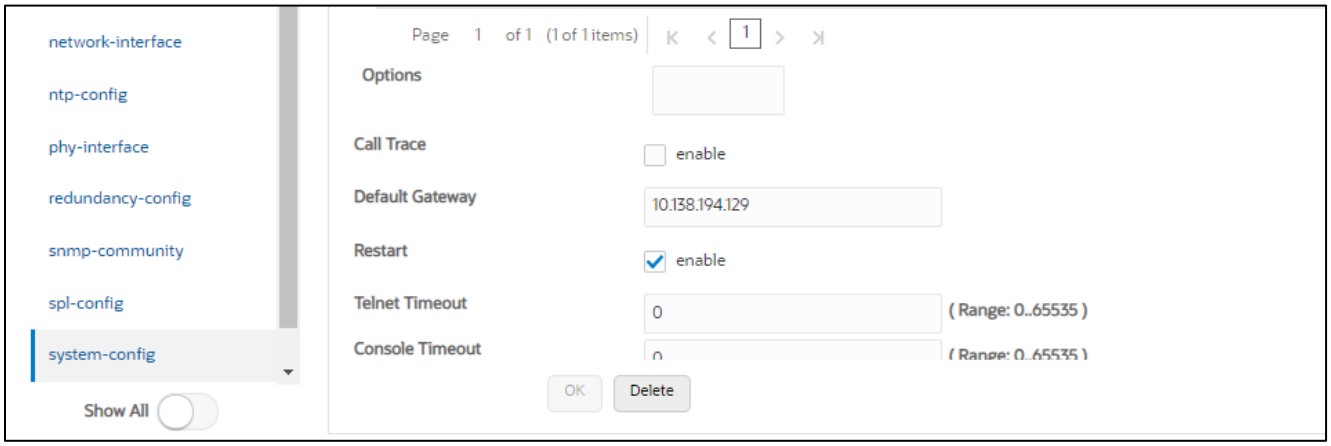
GUI Path: system/system-config

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)*





- Click the OK at the bottom of the screen

6.2.2 Media Manager

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

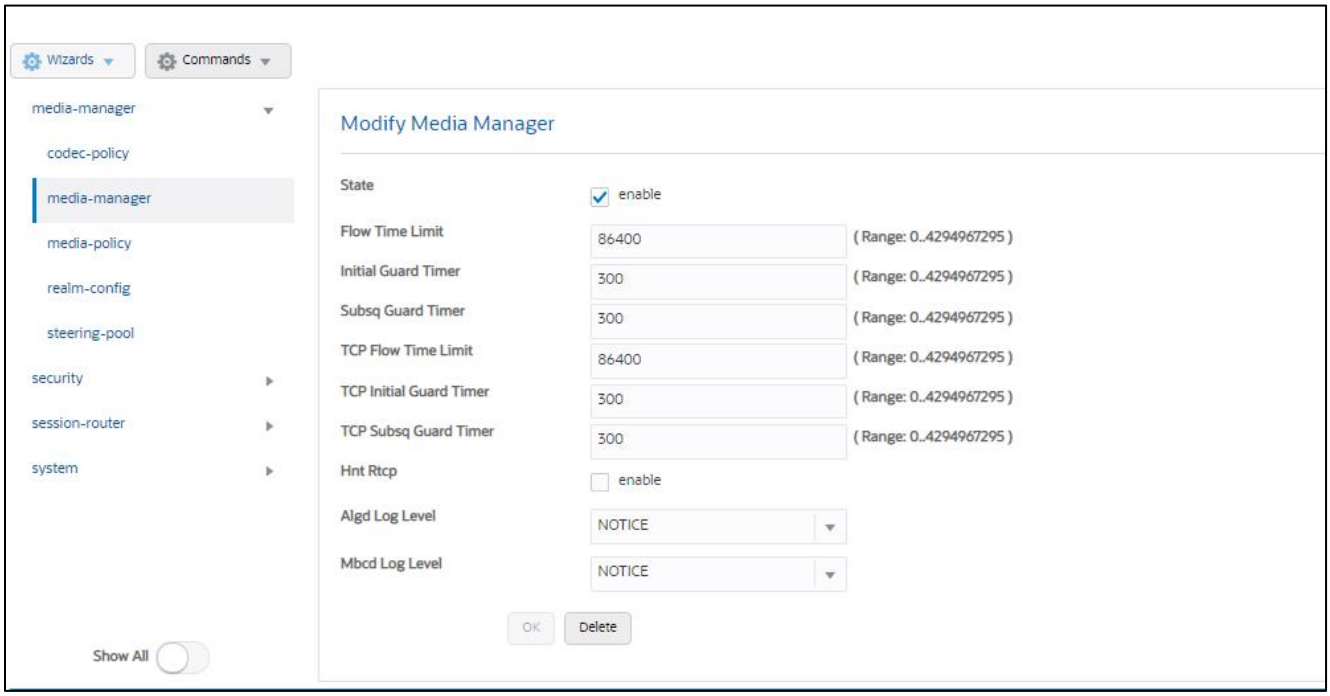
GUI Path: media-manager/media-manager

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

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

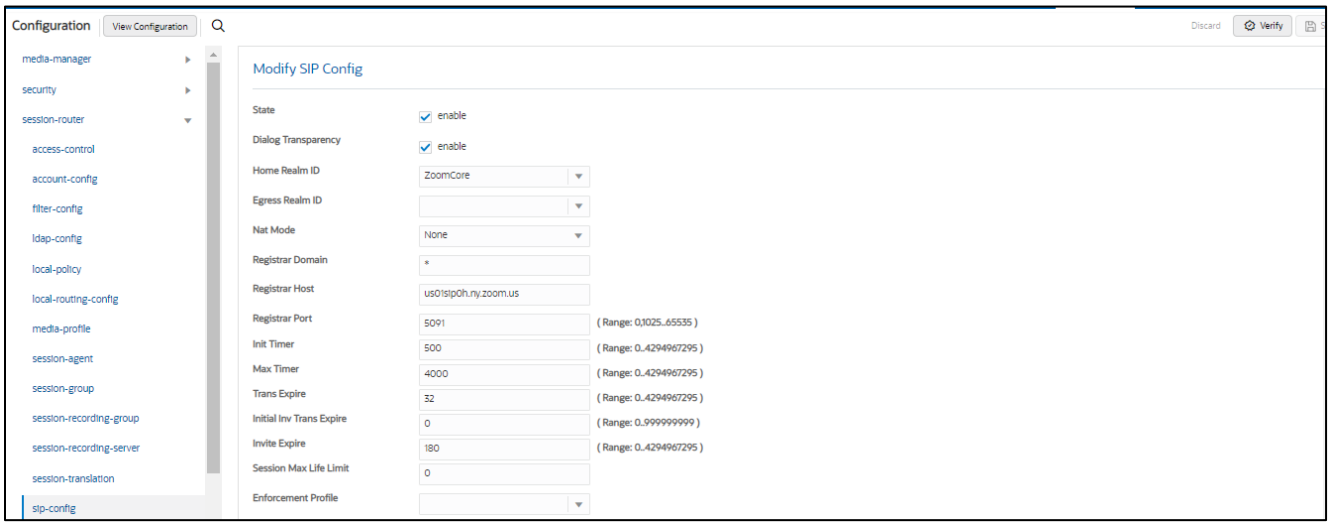
ACLI Path: config t→session-router→SIP-config

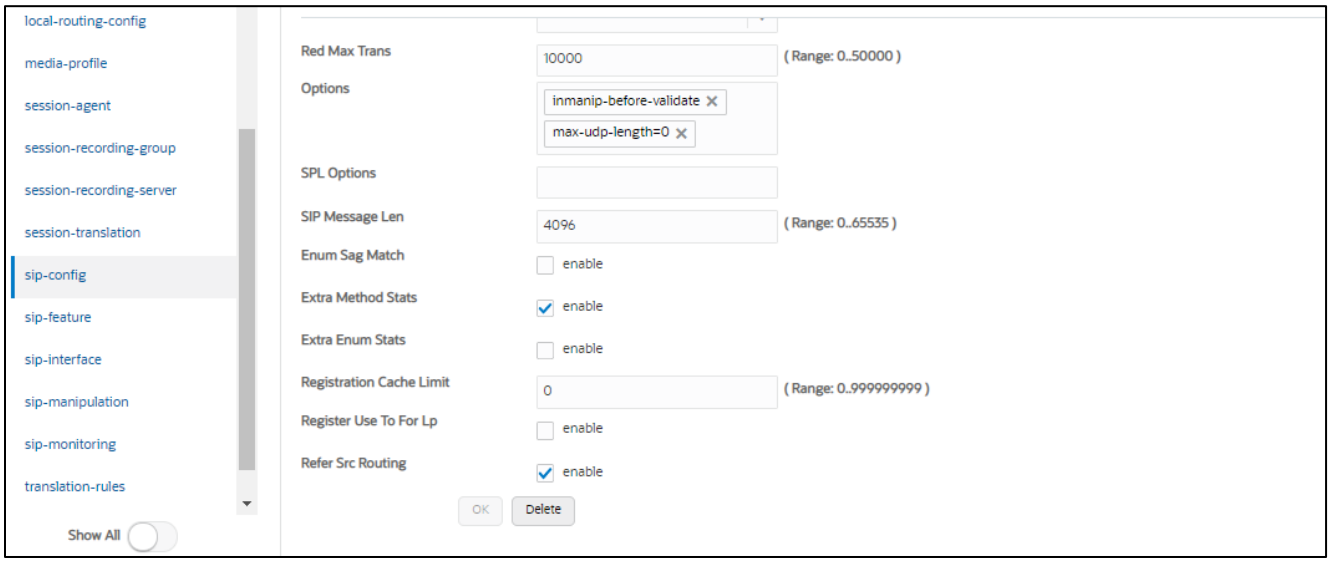
The following are recommended parameters under the global SIP-config:

- home-realm-id ZoomCore
- registrar-domain *
- registrar-host us01sip0h.ny.zoom.us
- registrar-port 5091
- Options: Click Add, in pop up box, enter the string: inmanip-before-validate
- Click Apply/Add another, then enter: max-udp-length=0
- Press OK in box

The Values for registrar Host and Port are discovered at the time of Provisioning in Step 4.4.

The home-realm-id is the Core Realm where the Zoom PBX Registrar is located.The values configured here will be used to route the incoming requests from ATA Device towards Zoom.



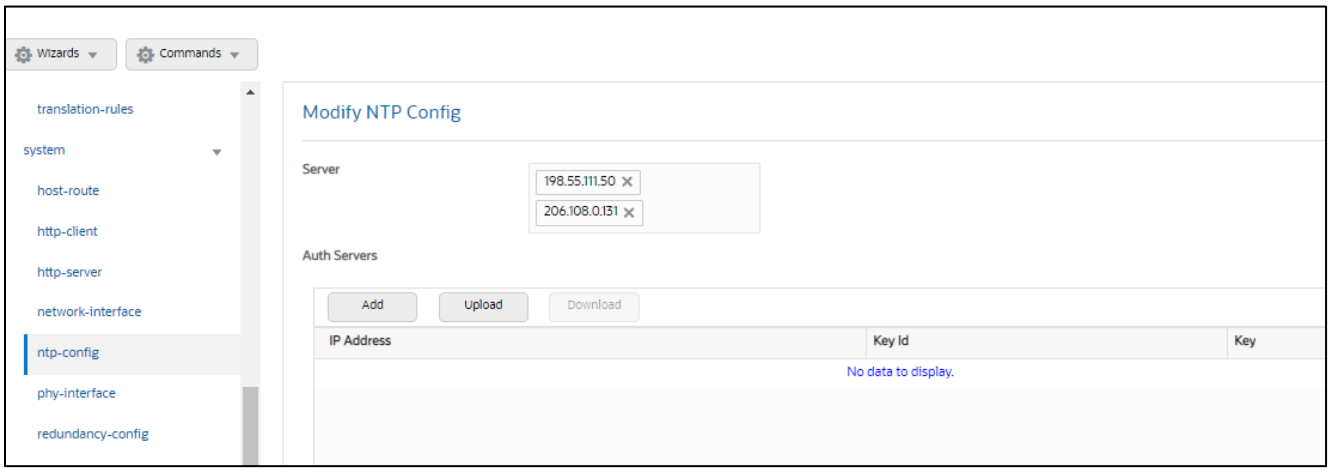


- Click OK at the bottom

6.2.4 NTP Config

GUI Path: system/ntp-config

ACLI Path: config t→system→ntp-config



- Click OK at the bottom

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 ATA Devices and Zoom PBX and BYOC Trunk,the other to connect to PSTN Network.

6.3.1 Physical Interfaces

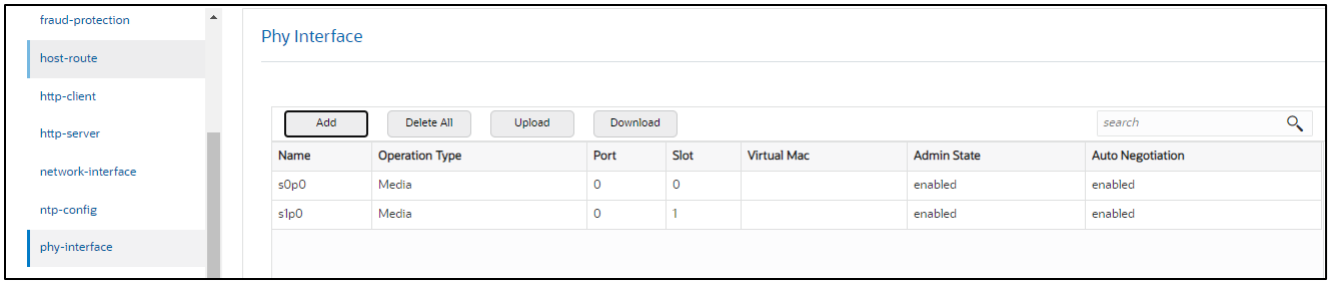
GUI Path: system → phy-interface

ACLI Path: config t→system→phy-interface

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

Config Parameter	Zoom	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

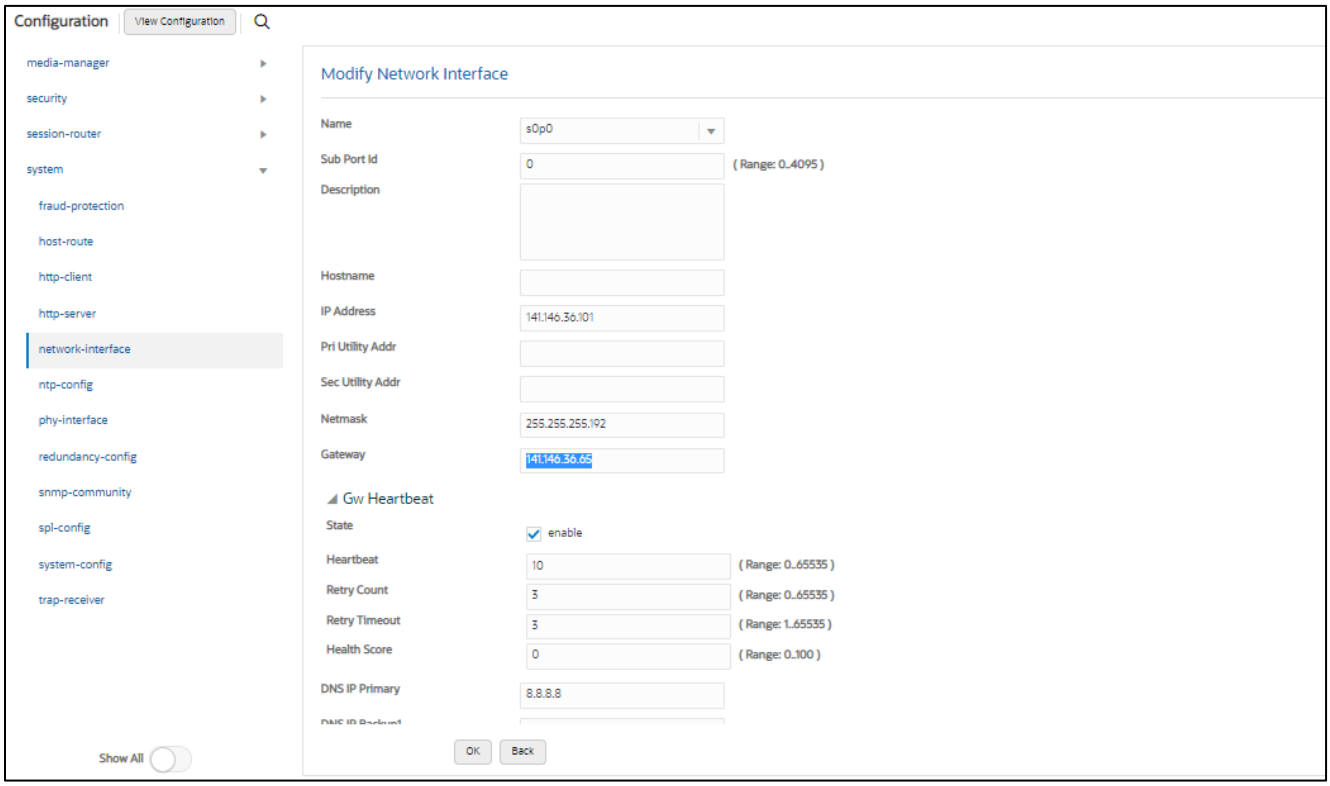
6.3.2 Network Interfaces

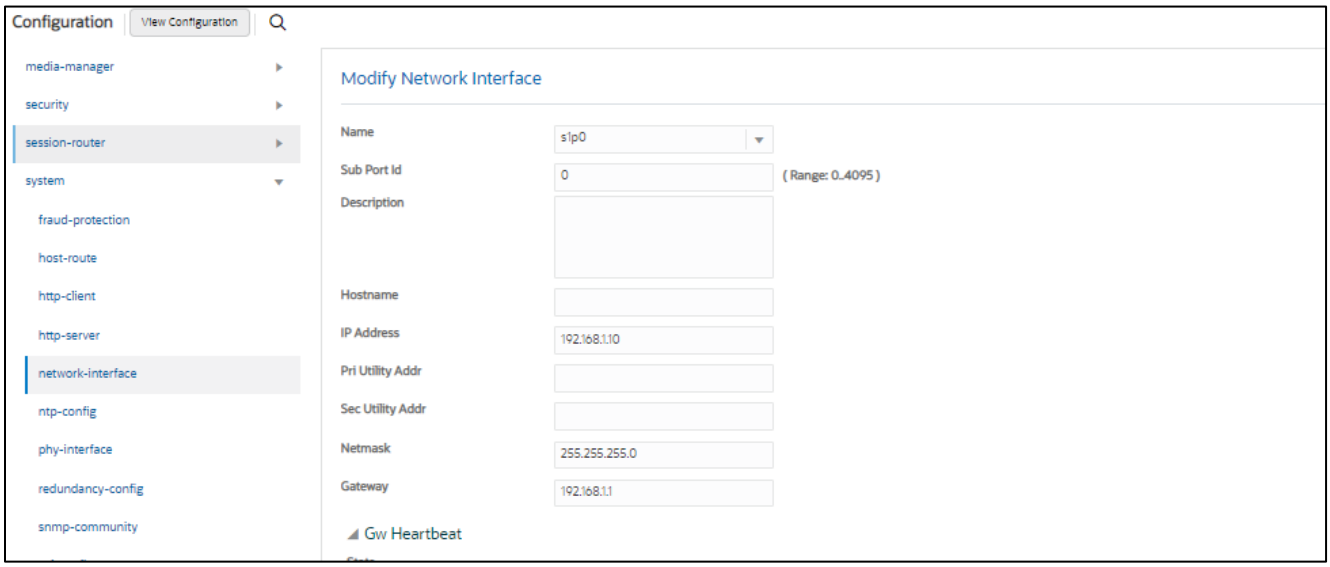
GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

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

Configuration Parameter	Zoom	PSTN
Name	s0p0	s1p0
Hostname	Domain (if applicable)	Domain (if applicable)
IP Address	141.146.36.101	192.168.1.10
Netmask	255.255.255.192	255.255.255.0
Gateway	141.146.36.65	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.

6.4 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Zoom Phone BYOC Platform. The connection between 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 Certificate Authorities. The connection between ATA Device and Sip Trunk with the SBC is UDP so this section does not apply to ATA configuration on the SBC.

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 below certificate records.

SBC Certificates

- ✓ SBCEnterpriseCert.pem
- ✓ DigiCertGlobalRootCA.crt.pem
- ✓ DigiCertInter.pem

Zoom PBX and Zoom BYOC Trunk Certificates

- ✓ sbc_ca.pem
- ✓ DigiCertGlobalRootCA.crt.pem
- ✓ DigiCertGlobalRootG2.crt.pem
- ✓ DigiCertGlobalRootG3.crt.pem

6.4.2 SBC End Entity Certificate

The SBC's end entity certificate SBCEnterpriseCert.pem is what is presented to Zoom Phone signed by your CA authority.In this example we are using Digicert as our signing authority.

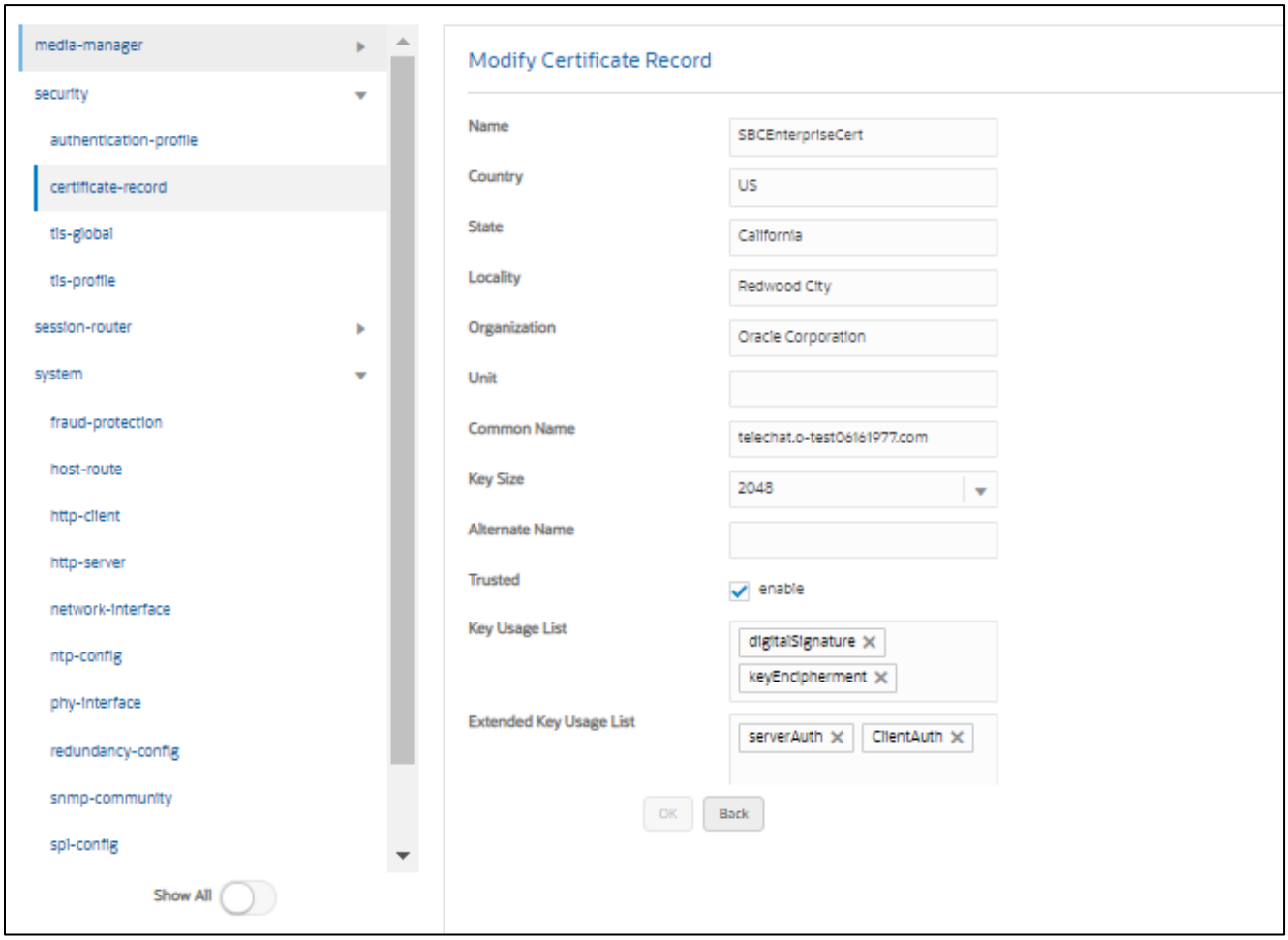
The certification must include a **common name.**

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

6.5 Root CA and Intermediate Certificates

Using this same procedure, configure certificate records for Root CA and Intermediate Certificates for SBC and Zoom.

6.5.1 Oracle SBC and Zoom Certificate

Oracle SBC certificate are signed by Digicert. Zoom also provides DigiCert certificate for the purpose of TLS connection with SBC. In this Setup the root CA for both Oracle SBC and Zoom is same so only one certificate record entry is created which covers both SBC and Zoom.DigiCertInter is the intermediate CA certificate for the SBC. We will create certificate-record entry for each certificate discovered at the time of registration configuration in Step 4.5 and the SBC CA certificate. The same certificates are required for Zoom BYOC Trunk so can be reused.

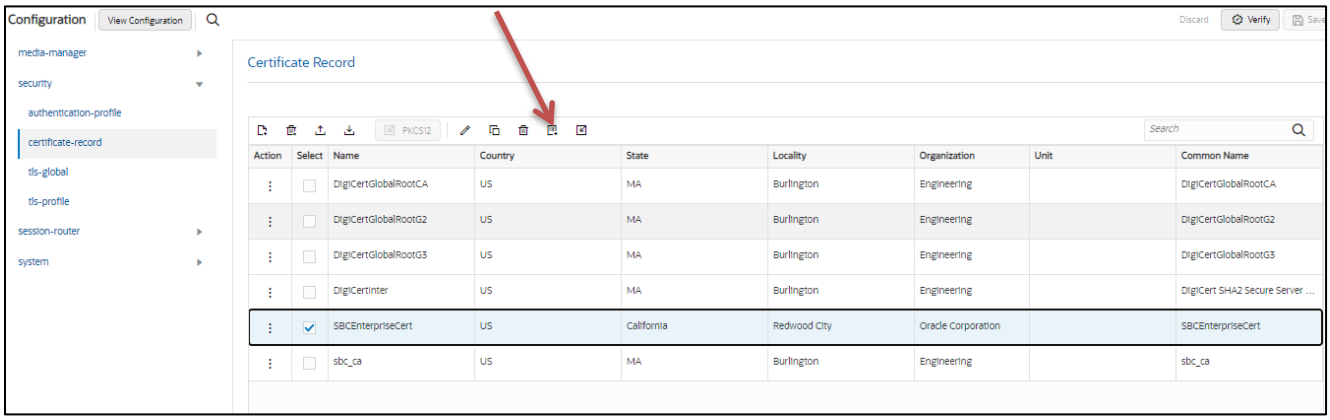
https://support.zoom.us/hc/en-us/articles/360054176992-BYOC-BYOP-Public-CA-Certificate-and-SIP-proxy-address-change

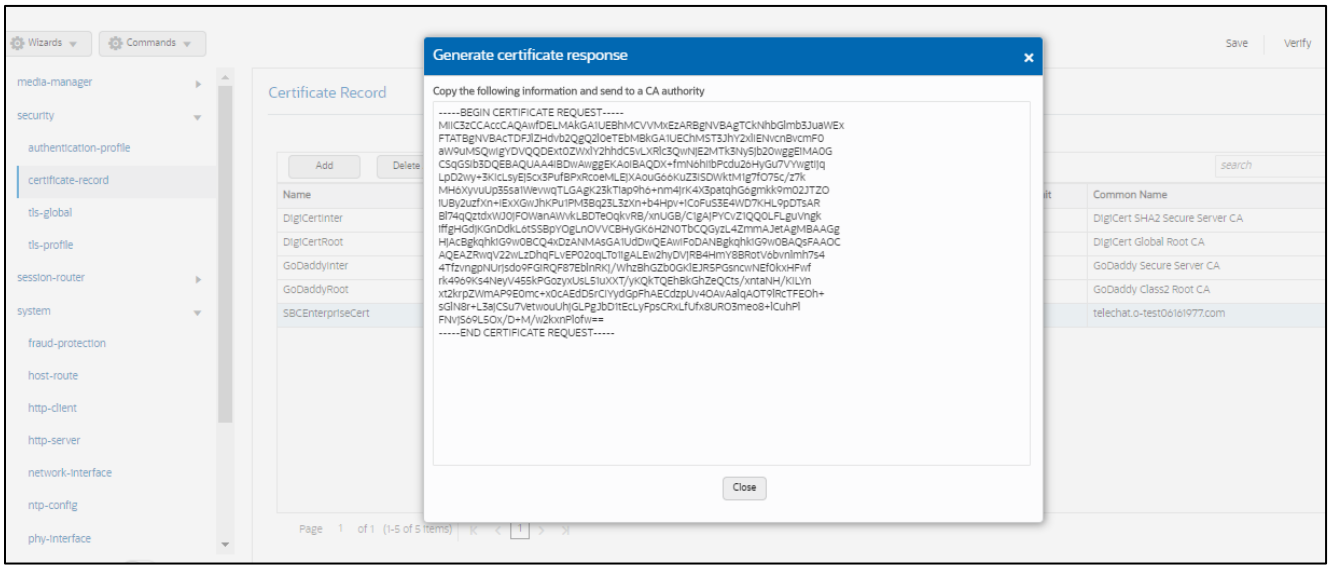
Config Parameter	sbc_ca	DigiCertGlobalRootCA	DigiCertGlobalRootG2	DigiCertGlobalRootG3	DigiCertInter
Common Name	sbc_ca	DigiCertGlobalRootCA	DigiCertGlobalRootG2	DigiCertGlobalRootG3	DigiCertInter
Key Size	2048	2048	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth	serverAuth	serverAuth
cKey algor	rsa	rsa	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256	Sha256	Sha256

6.5.2 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

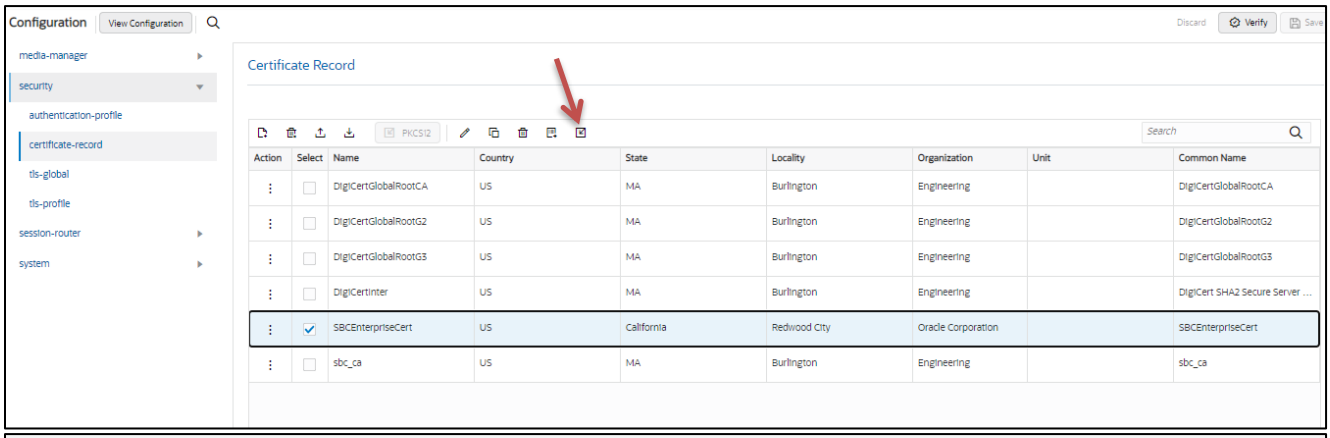


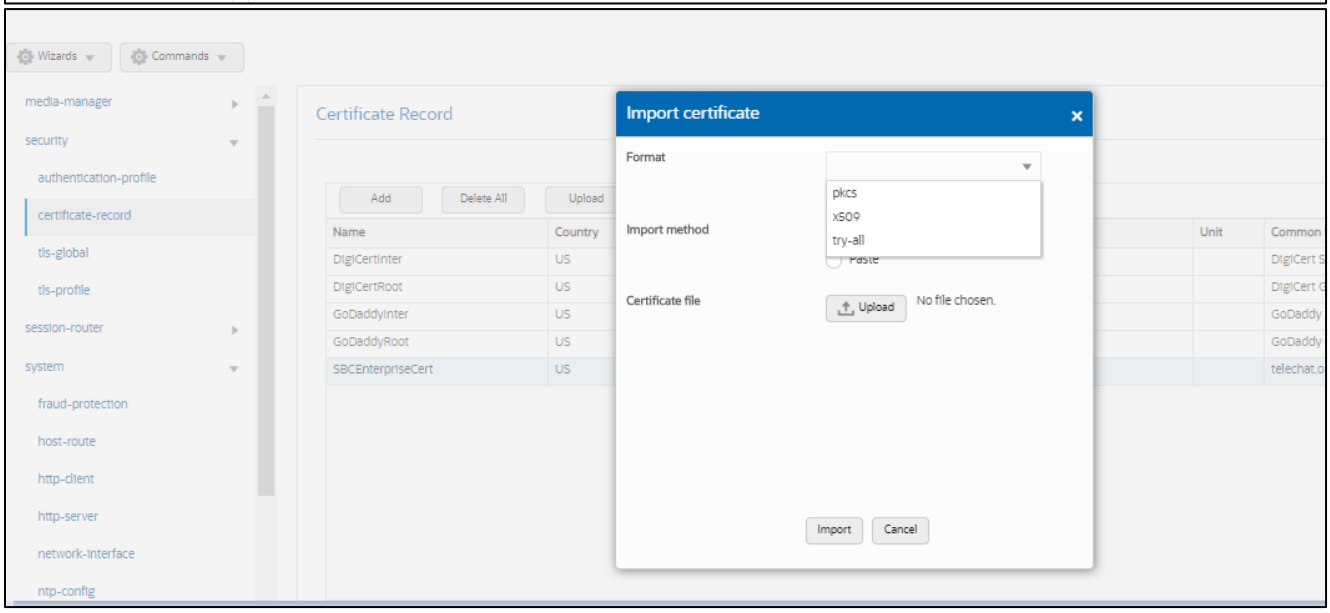


- copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, a save and activate is required before you can import the certificates to each certificate record created above.

6.5.3 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:

- ✓ sbc_ca
- ✓ DigiCertGlobalRootCA
- ✓ DigiCertGlobalRootG2
- ✓ DigiCertGlobalRootG3
- ✓ DigiCertInter

At this stage, all required certificates have been imported.

6.5.4 TLS Profile

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

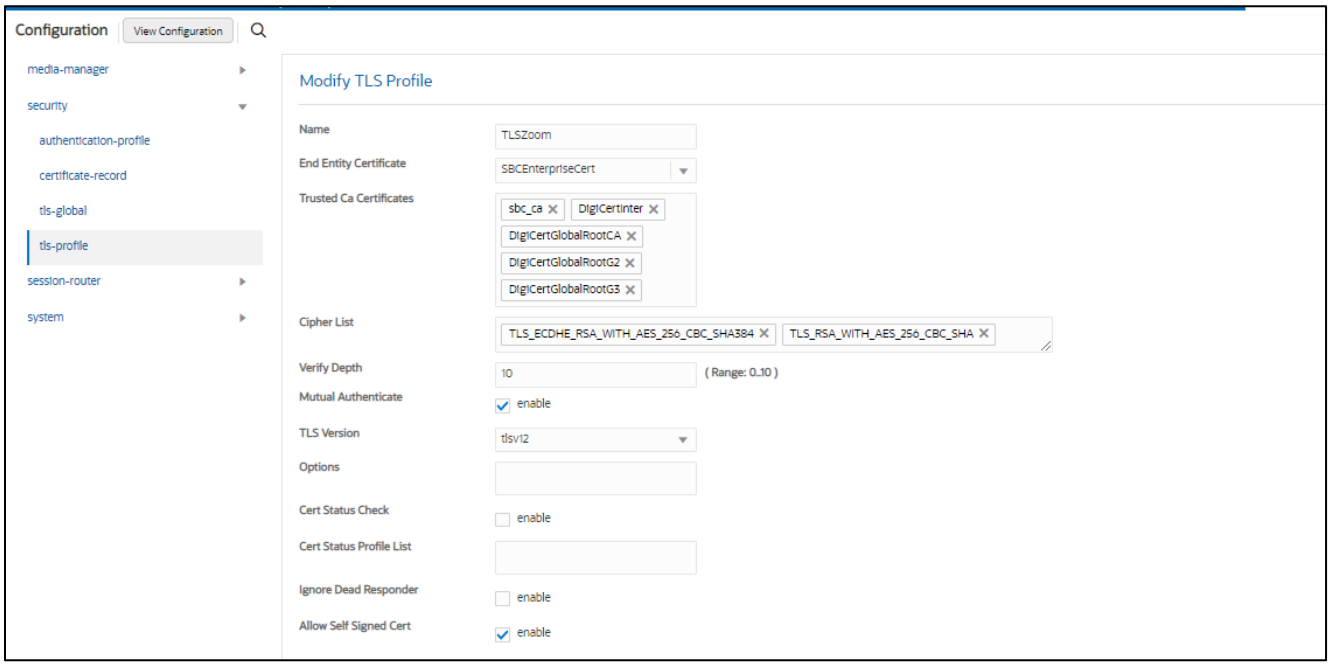
GUI Path: security/tls-profile

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 DigiCert 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

6.6 Media Security Configuration

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

6.6.1 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.

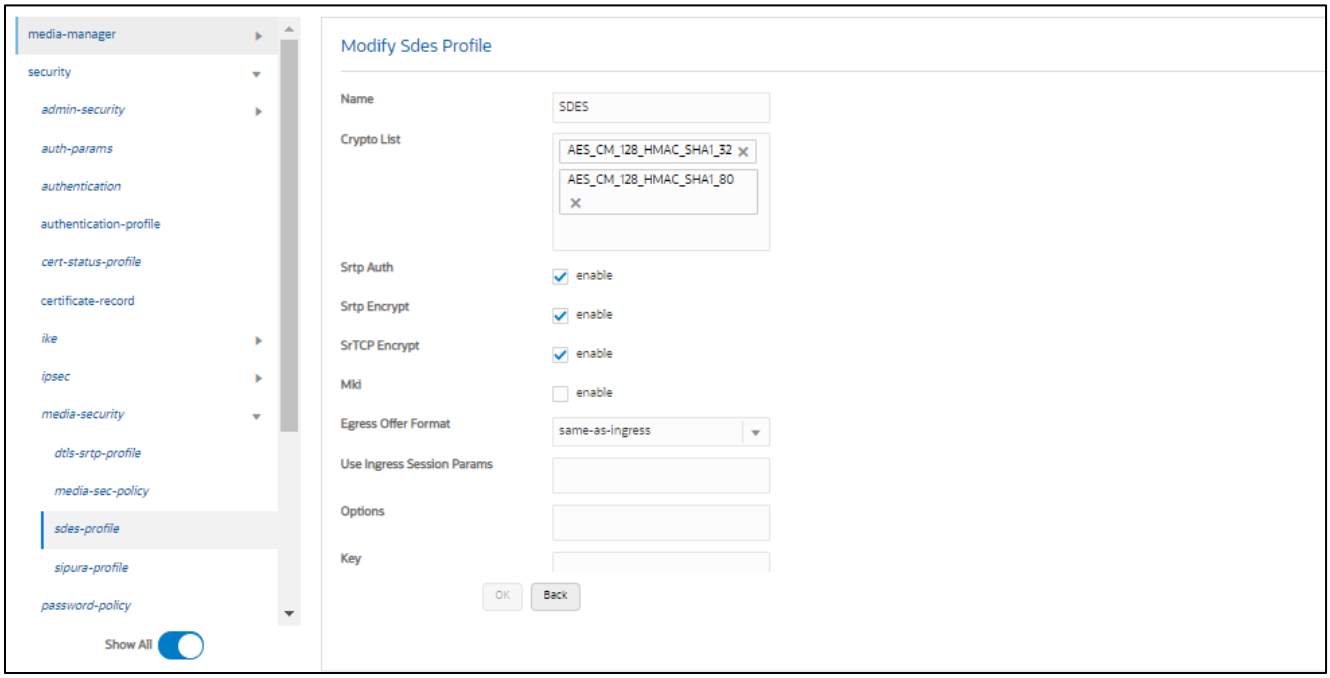
GUI Path: security/media-security/sdes-profile

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

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

- 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

6.6.2 Media Security Policy

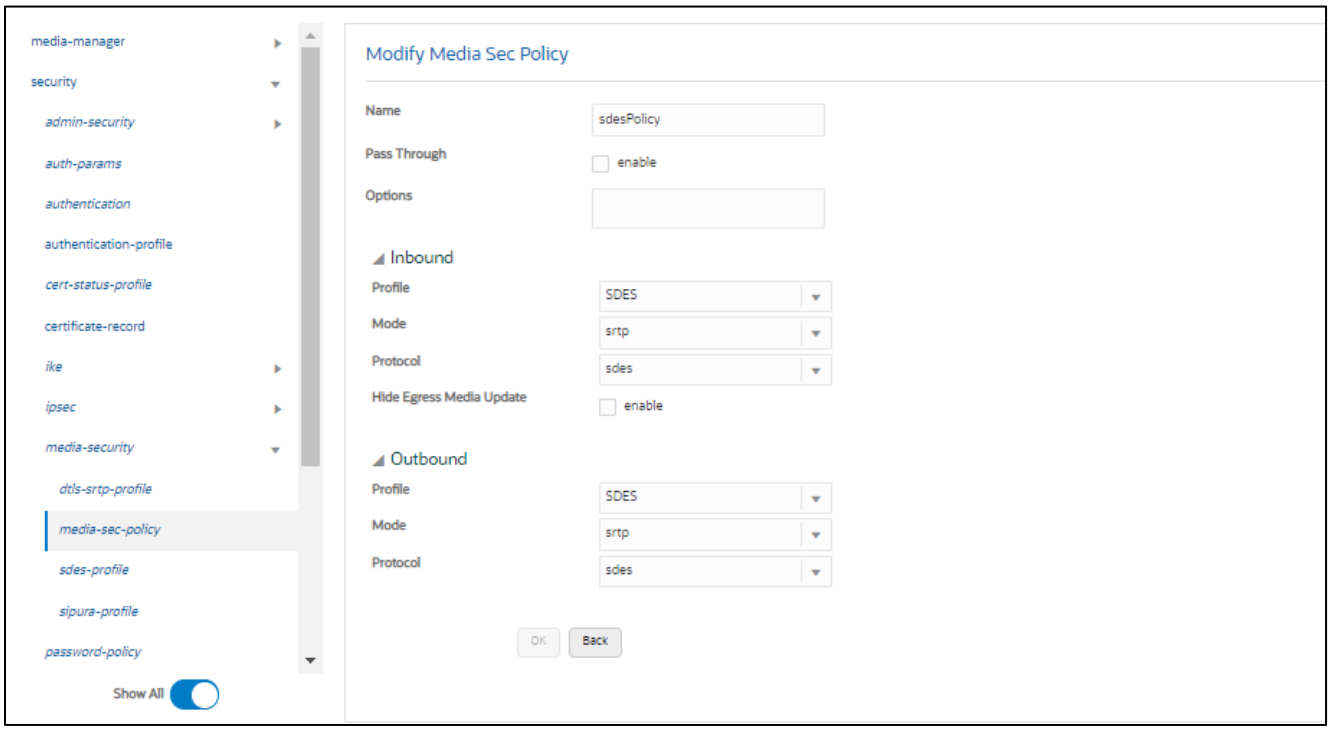
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them) and, if SRTP needs to be used, the sdes-profile that needs to be used

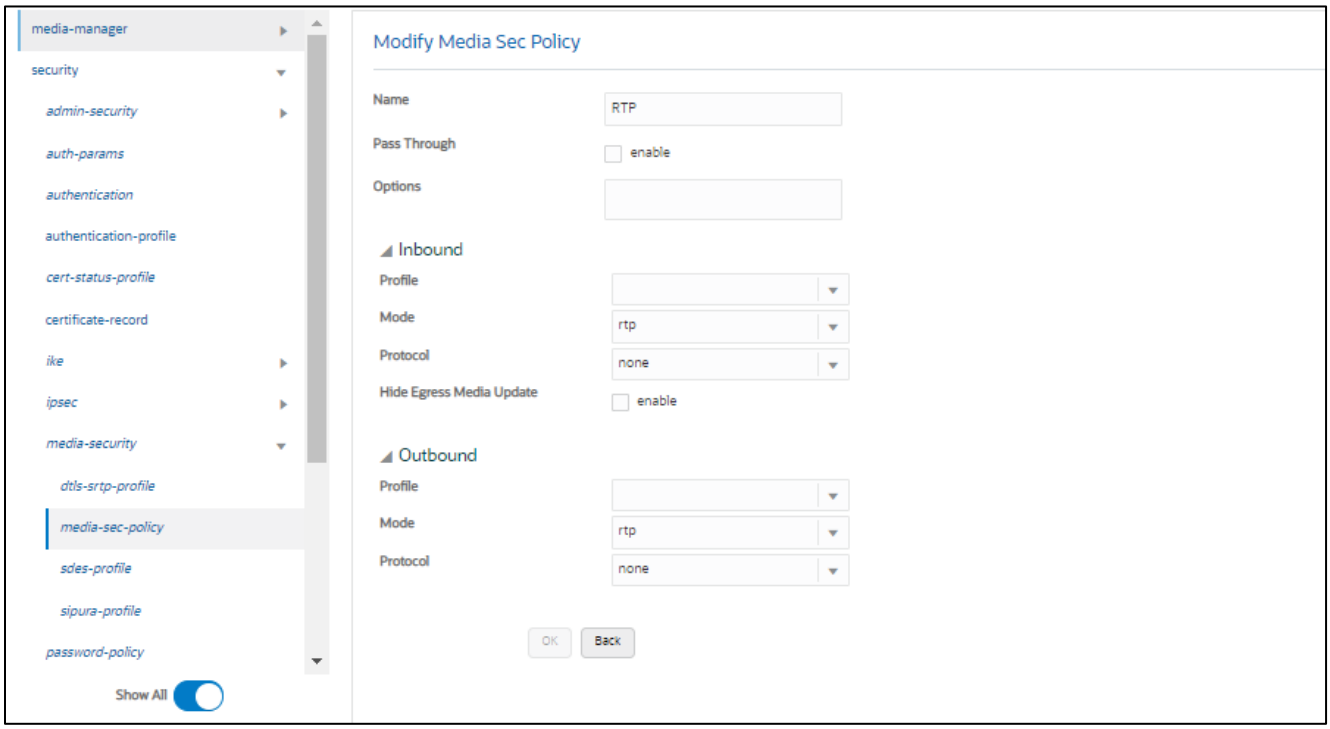
In this example, we are configuring two media security policies. One to secure and decrypt media toward Zoom, the other for non-secure media facing PSTN and the ATA Device.

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


media-manager
security
admin-security
auth-params
authentication
authentication-profile
cert-status-profile
certificate-record
ike
ipsec
media-security
dtls-srtp-profile
media-sec-policy
sdes-profile
sipura-profile
password-policy
Show All
Modify Media Sec Policy
Name
sdesPolicy
Pass Through
enable
Options
Inbound
Profile
SDES
Mode
srtp
Protocol
sdes
Hide Egress Media Update
enable
Outbound
Profile
SDES
Mode
srtp
Protocol
sdes
OK
Back


media-manager
security
admin-security
auth-params
authentication
authentication-profile
cert-status-profile
certificate-record
ike
ipsec
media-security
dtls-srtp-profile
media-sec-policy
sdes-profile
sipura-profile
password-policy
Show All
Modify Media Sec Policy
Name
RTP
Pass Through
enable
Options
Inbound
Profile
Mode
rtp
Protocol
none
Hide Egress Media Update
enable
Outbound
Profile
Mode
rtp
Protocol
none
OK
Back

6.7 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.

6.7.1 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.

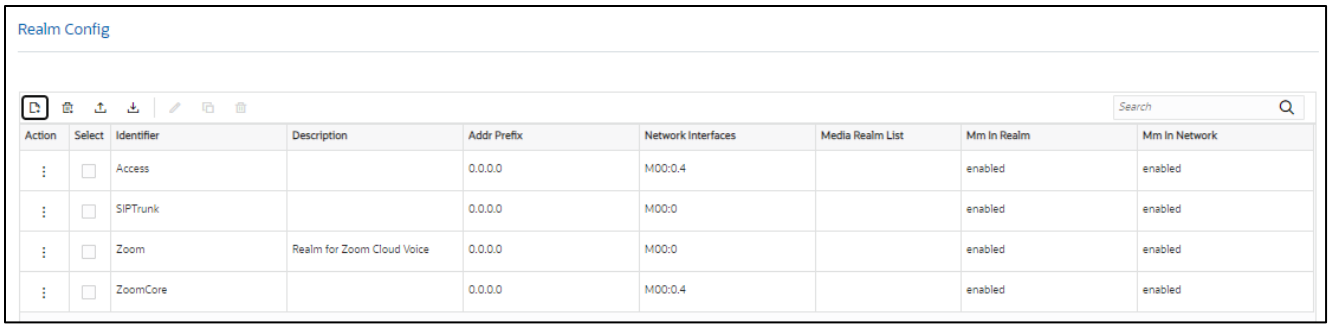
GUI Path; media-manager/realm-config

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

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

- **Access-** Realm Facing the ATA Device
- **Core -** Realm facing the Zoom Registrar
- **Zoom Realm-** Realm for the Zoom BYOC Trunk
- **PSTN Realm-** Breakout Realm for calls towards PSTN

Config Parameter	Access	Core	Zoom Trunk	PSTN
Identifier	Access	ZoomCore	Zoom	SIPTrunk
Network Interface	s0p0:0	s0p0:0	s0p0:0	s1p0:0
Mm in realm	☑	☑	☑	☑
Access-control-trust-level	Low	High	High	High
Media Sec policy	RTP	sdespolicy	sdesPolicy	RTP



6.7.2 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 steering pool for PSTN each realm configured.
GUI Path: media-manager/steering-pool

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

- Click Add, and use the below examples to configure

Steering Pool

Search

Action	Select	IP Address	Start Port	End Port	Realm ID	Network Interface
⋮	☐	141.146.36.100	10000	10999	SIPTrunk	
⋮	☐	141.146.36.68	20000	40000	Zoom	
⋮	☐	141.146.36.80	10000	10999	ZoomCore	
⋮	☐	141.146.36.89	10000	10999	Access	

6.8 SIP Configuration

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

6.8.1 SIP Manipulations

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

Note: Applying these manipulations are not compulsory is dependent upon the requirement of your Carrier. The requirement may vary from carrier to carrier so the HMRs are subjected to change.

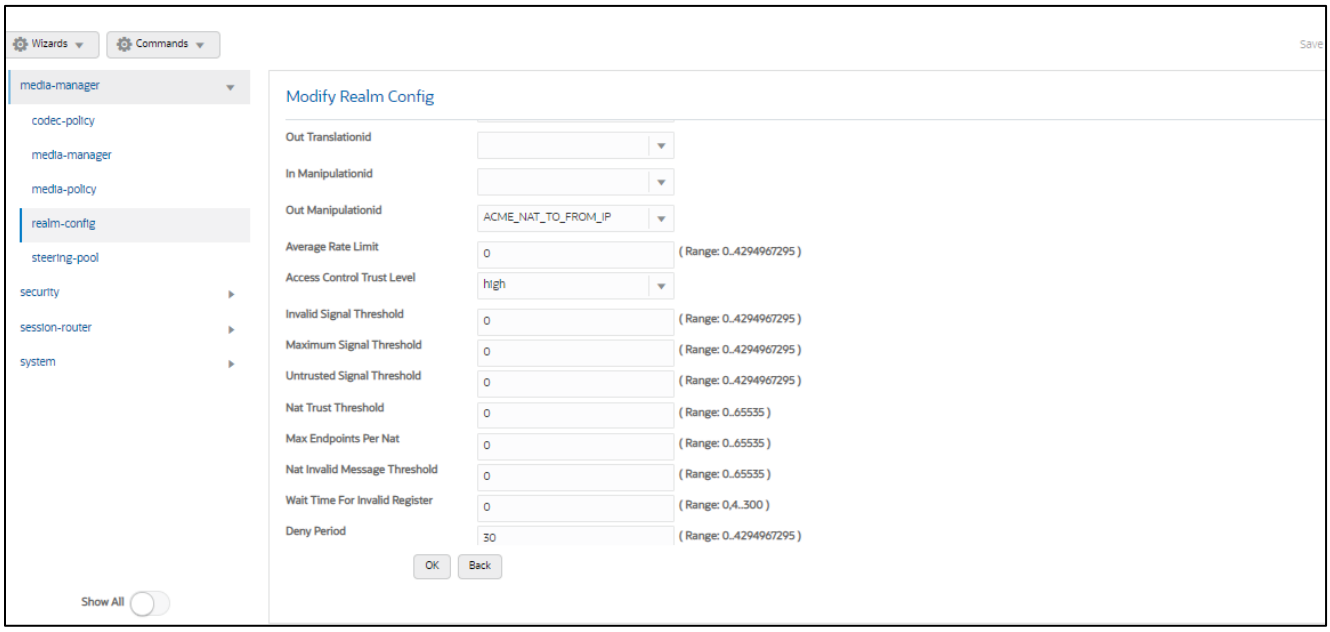
6.8.1.1 Manipulation towards Zoom Side

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 should we can use the prebuilt HMR ACME_NAT_TO_FROM_IP

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

The manipulation performs the following modifications to SIP packets

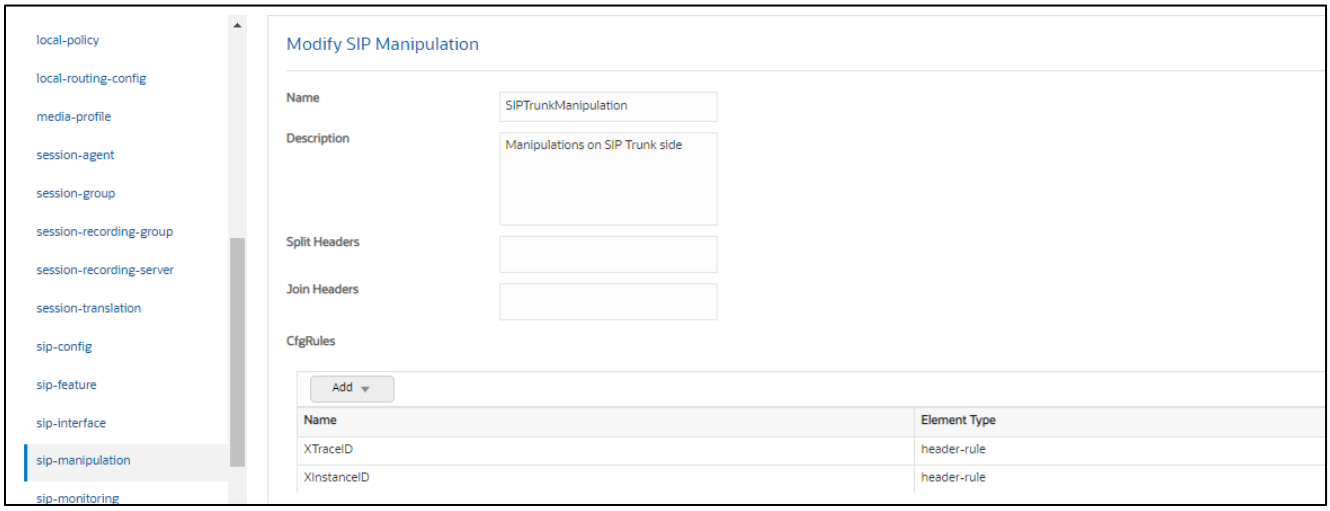
1. Changes the host portion of From address with the SBC sip-interface IP Address.
2. Changes the host portion of To Header with Zoom IP Address.



6.8.1.2 Manipulation towards Carrier Side.

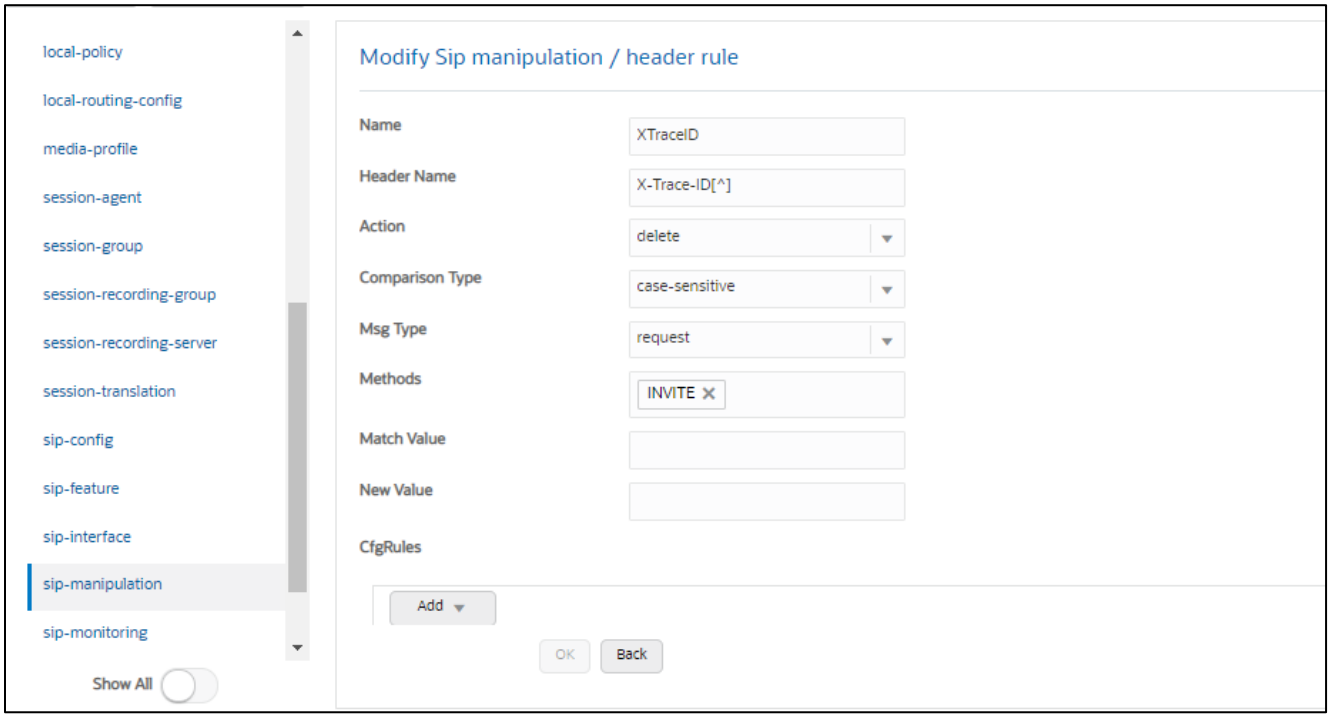
The following SIP manipulation is applied as the out-manipulationId on the Session-Agent created for the Carrier Trunk. This manipulation modifies packets generated by the Oracle SBC to Carrier Side as stated below:

1. Removes the unwanted headers inserted by Zoom in the signaling when forwarding the message to Carrier.
2. Changes the Host portion of From Header with the Local SBC IP Address.
3. Changes the Host portion of To Header with Carrier side IP Address
4. Changes the Host portion of P-Asserted Identity with Carrier side IP Address.

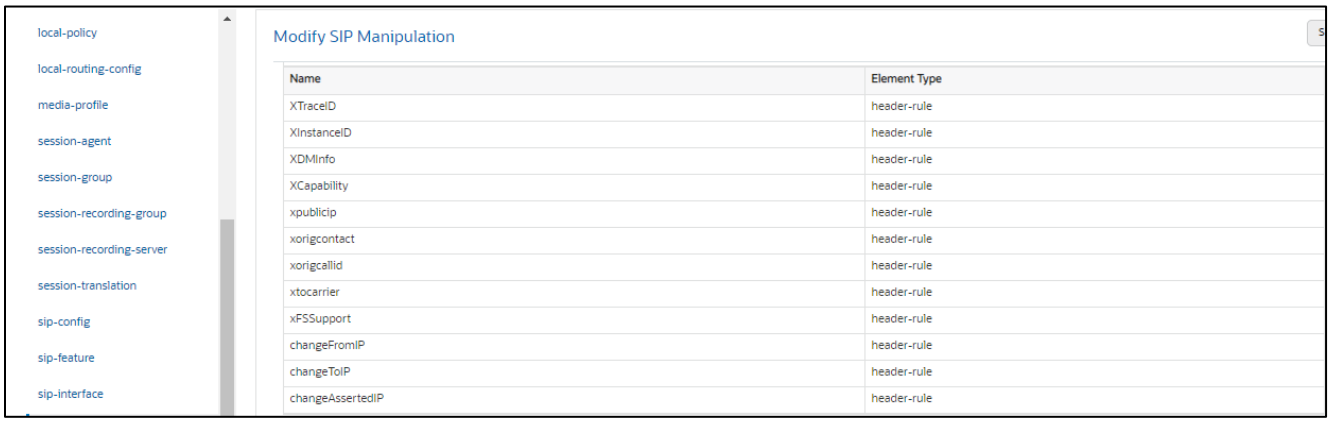


Header-Rules

Below is an example to remove the X-TraceID header towards Carrier. In similar fashion other header-rules can be created to remove other headers such as XInstanceID, XDInfo etc.



Similar Header-rules are created to remove the other X headers which are inserted by Zoom on the Sip Signaling.

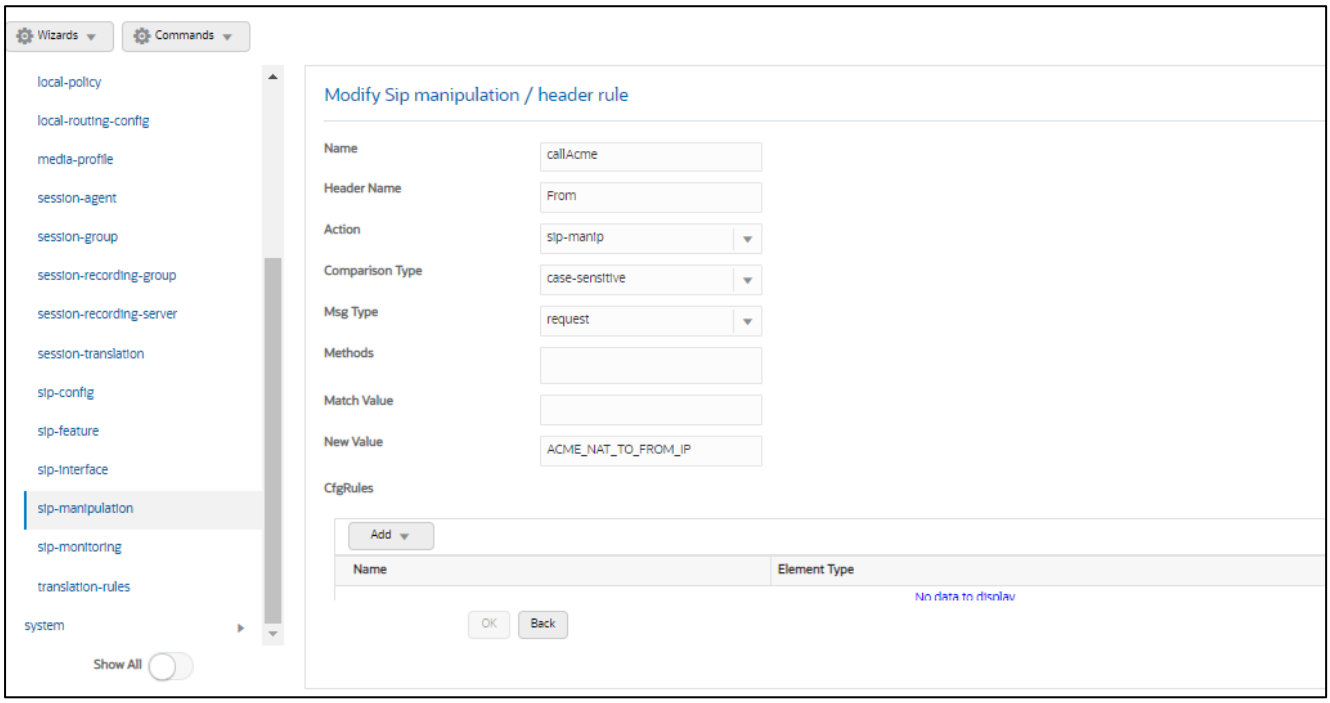


Name	Element Type
XTraceID	header-rule
XInstanceID	header-rule
XDMInfo	header-rule
XCapability	header-rule
xpublicip	header-rule
xorigcontact	header-rule
xorigcallid	header-rule
xtocarrier	header-rule
xFSSupport	header-rule
changeFromIP	header-rule
changeToIP	header-rule
changeAssertedIP	header-rule

On the same Sip-manipulation we have called the ACME_NAT_TO_FROM_IP Manipulation which performs the topology hiding as below -

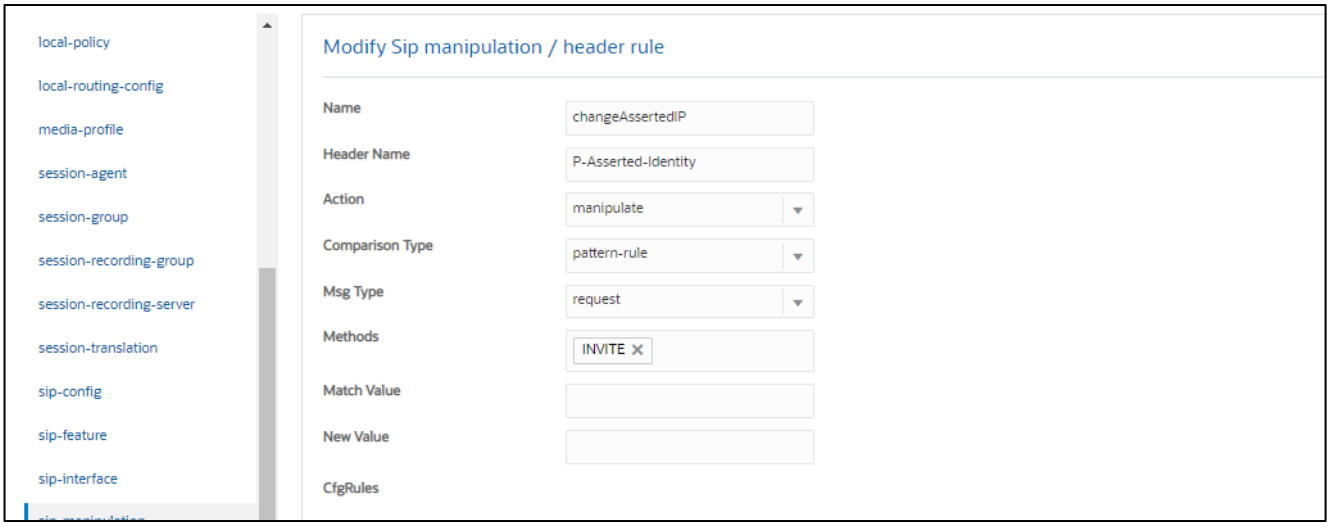
1. Changes the host portion of From Header with the Local SBC IP Address.
2. Changes the host portion of To Header with Carrier side IP Address

3. Changes the host portion of P Asserted Identity with Carrier side IP Address.
Header-rule

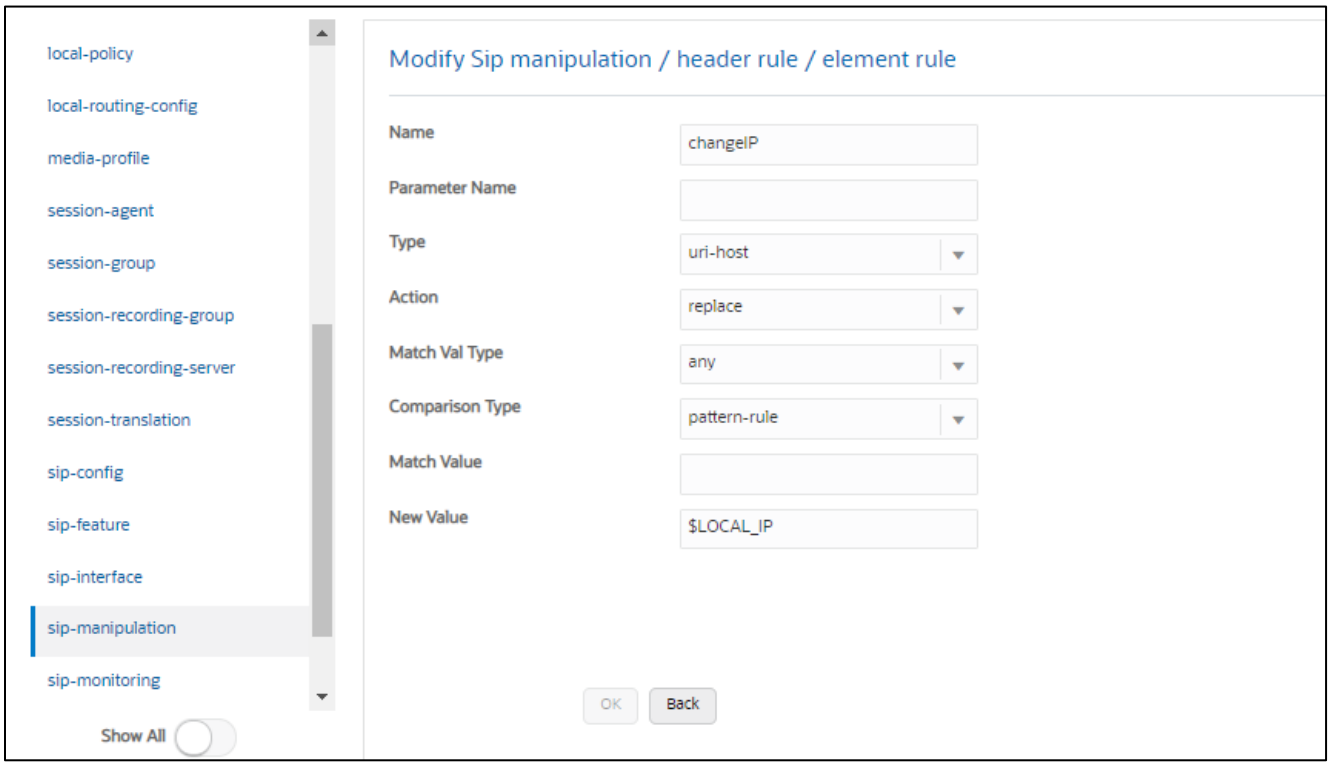


Below Portion of the HMR Changes the Host portion of P-Asserted Identity with Carrier side IP Address.

Header-rule



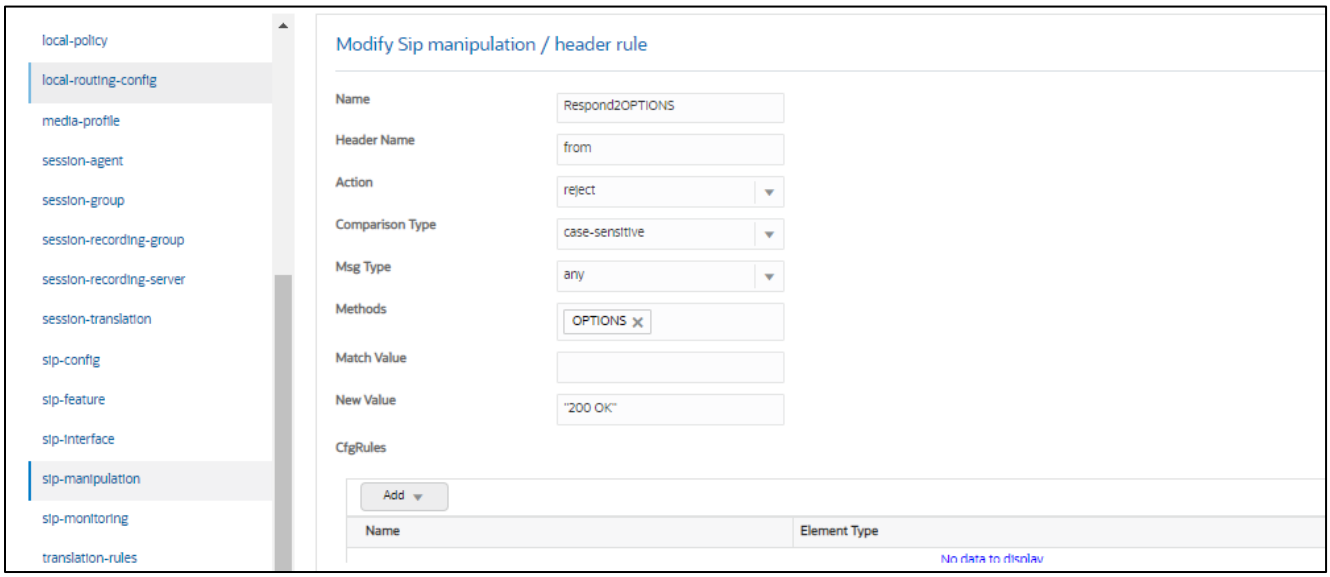
Element Rule



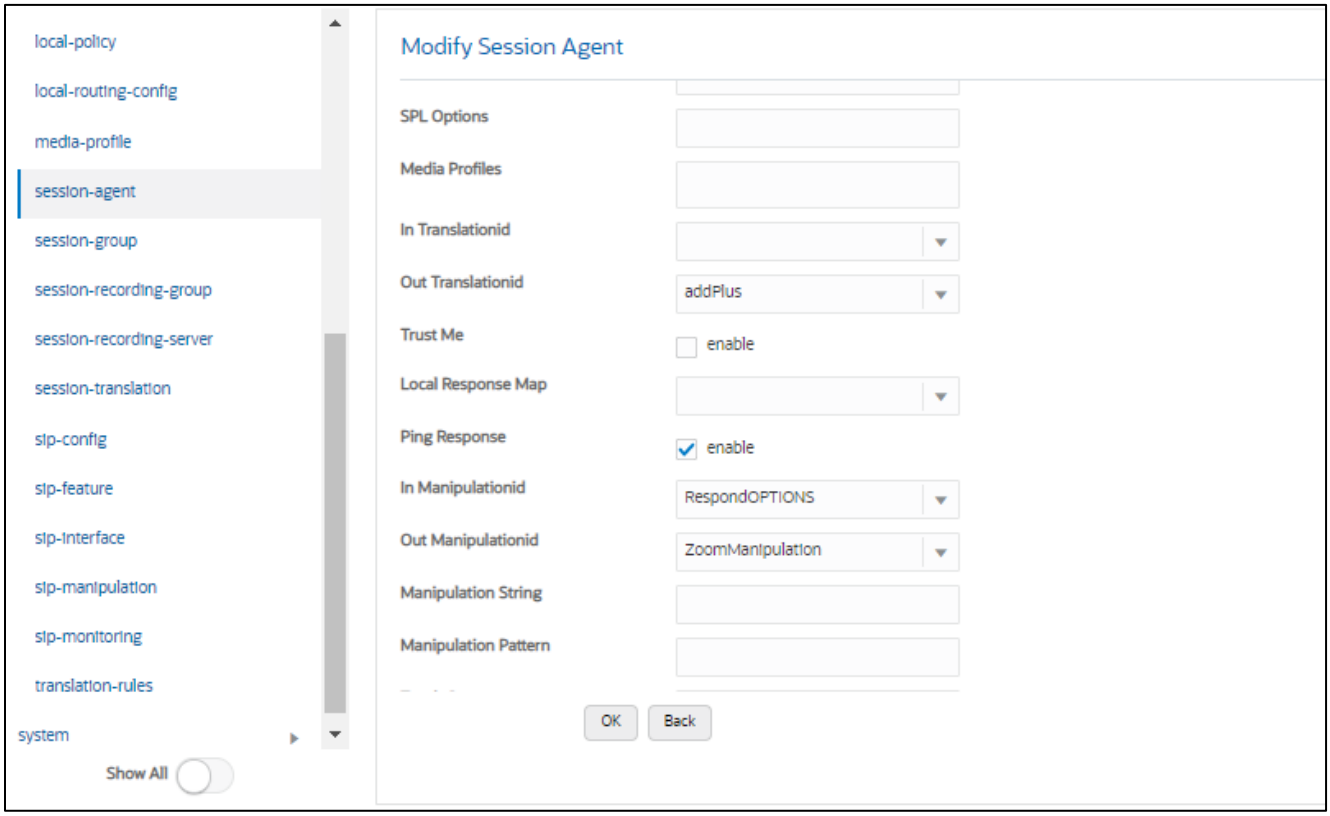
6.8.1.3 Manipulation for OPTIONS Ping.

The following SIP manipulation can 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.

Header Rule:

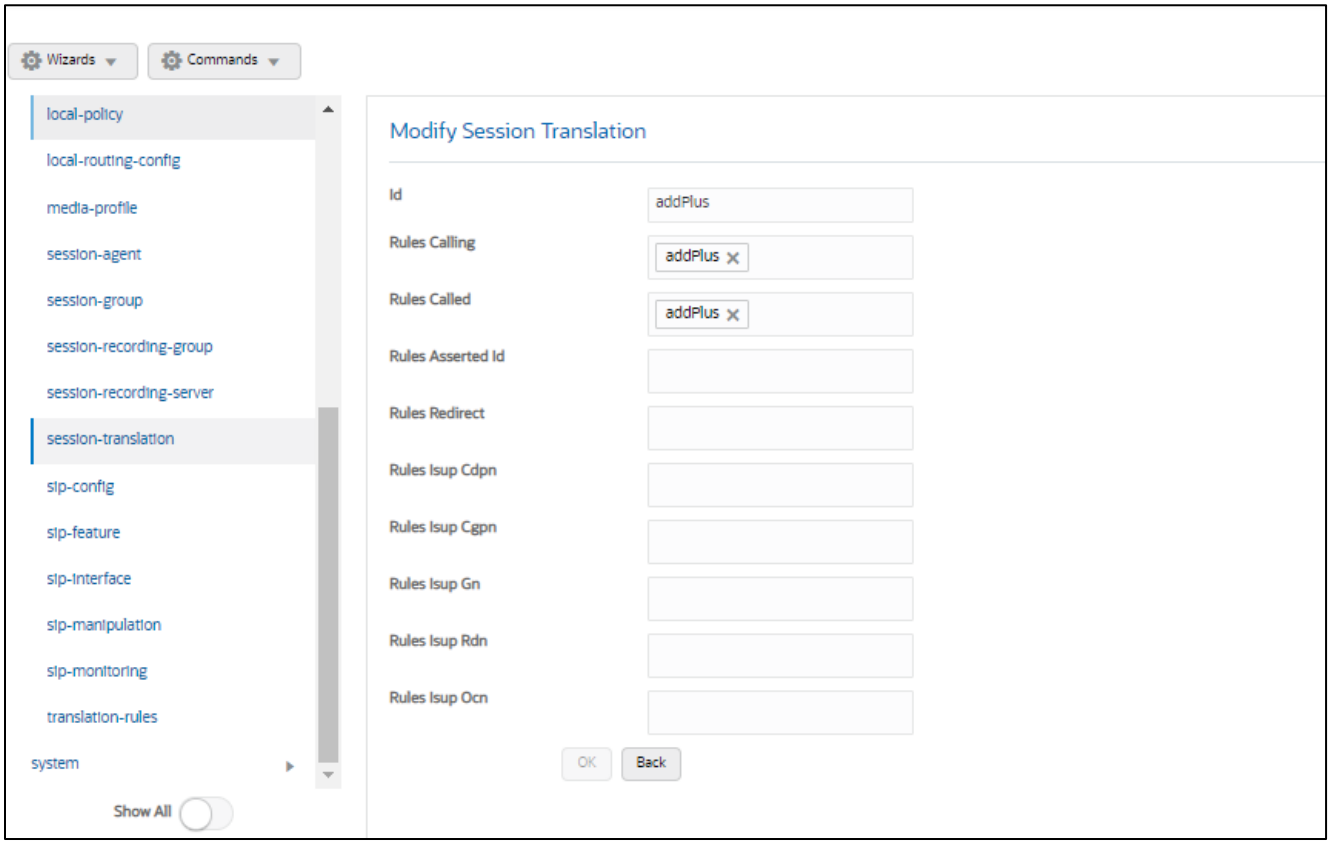


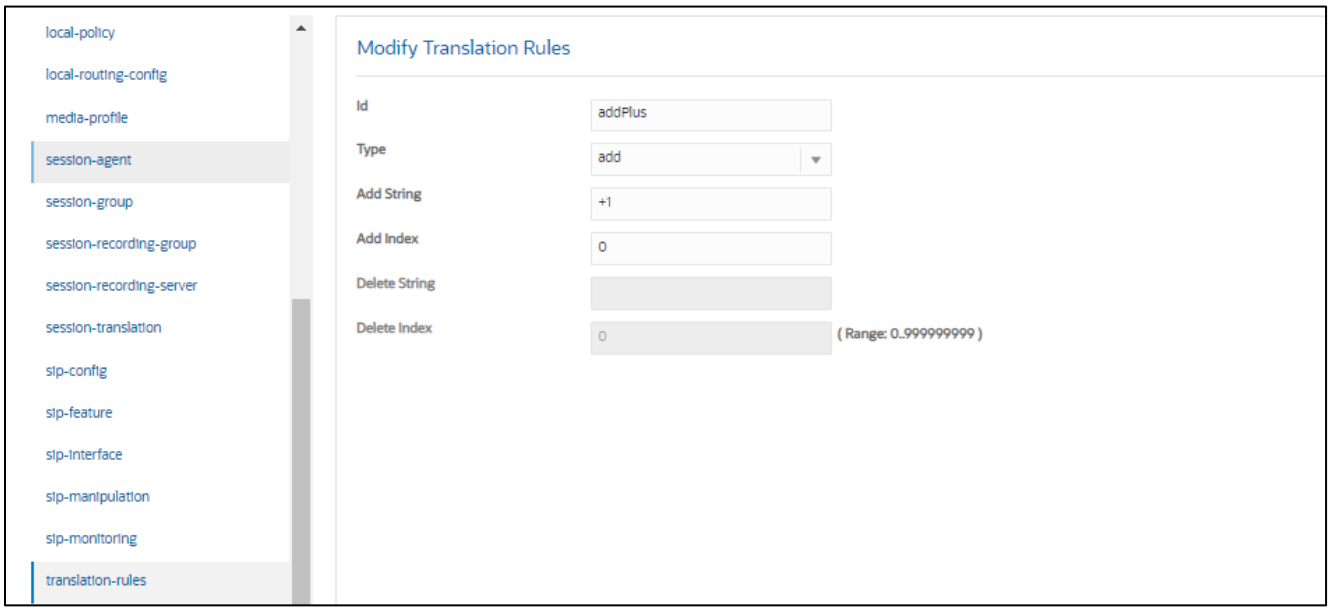
Please note, If running release SCZ830m1p7 or later, there is a new configuration parameters on the Session Agent Config element, called [ping-response](). When enabled on each agent, it will take that place of the following SIP-Manipulation.



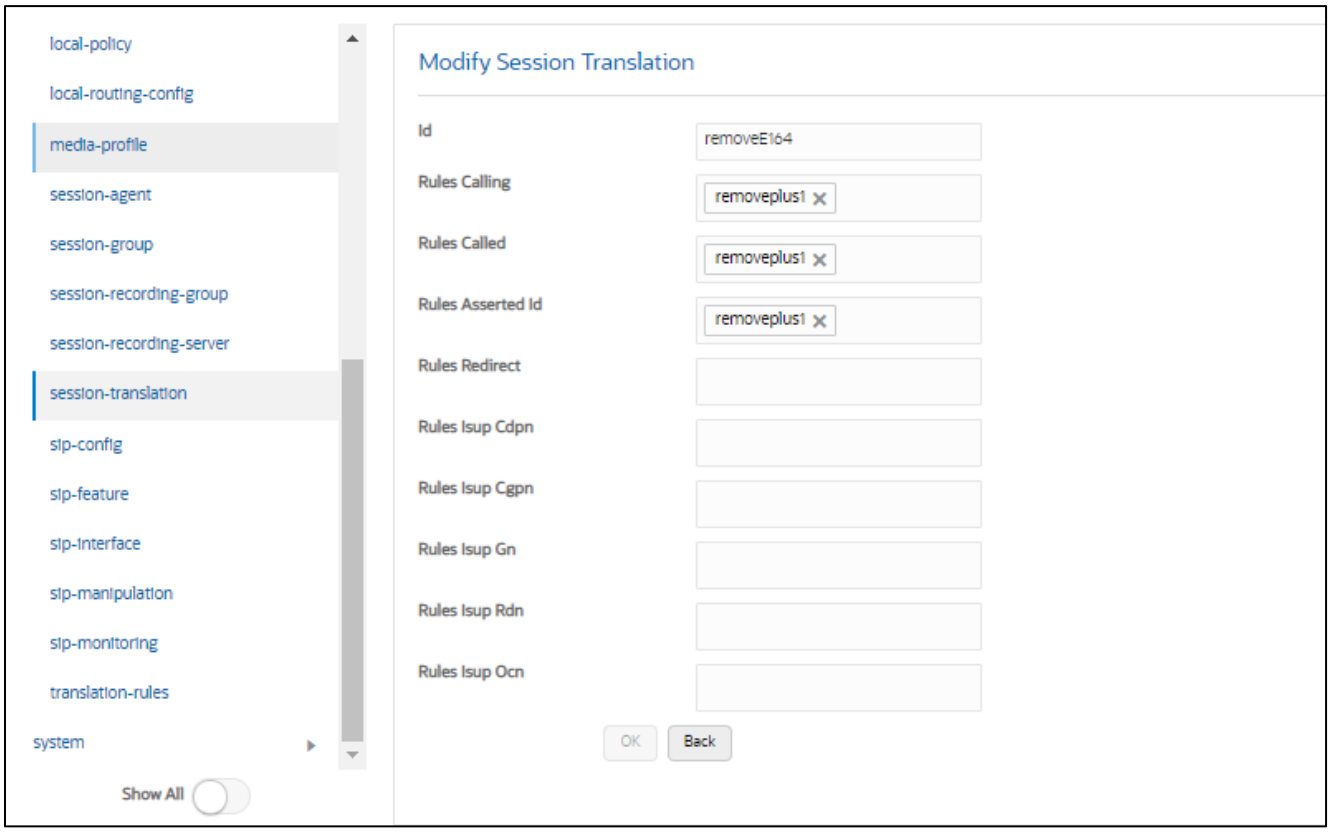
6.9 Session-Translation

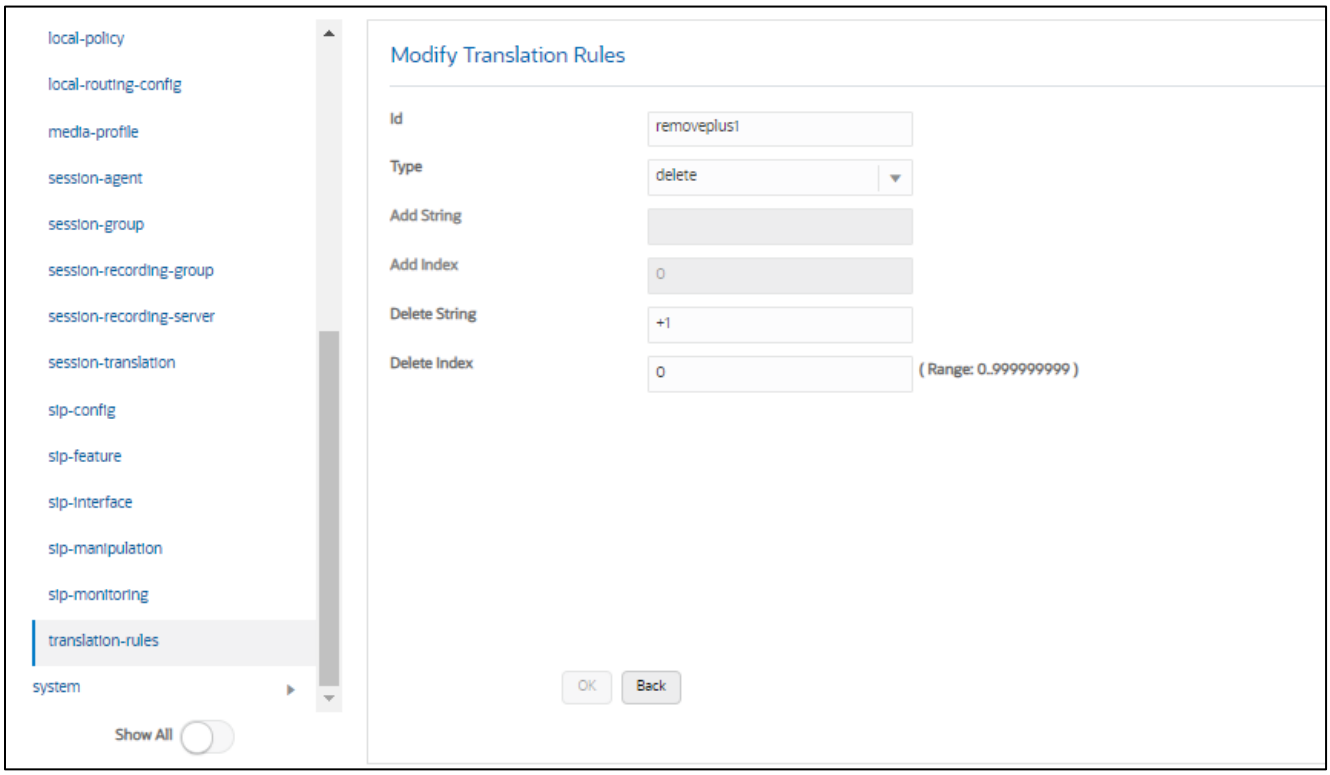
The following session-translation is created and applied as out-translationid on the Session-Agent towards Zoom. This session-translation is created to add a +1 and can be used towards as Zoom requires calls to be presented in E.164 format.





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





6.10 Session Timer Profile (Optional)

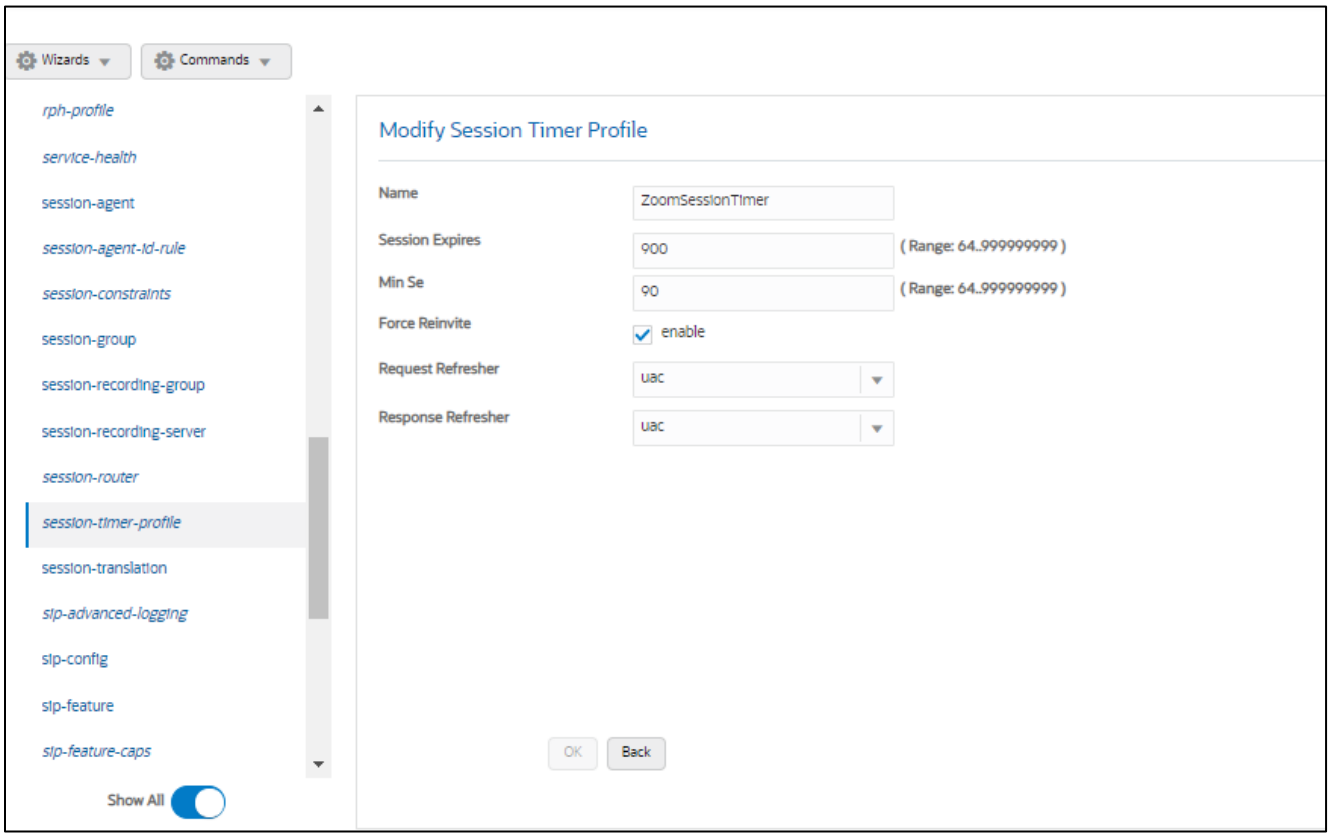
Zoom Phone does support RFC 4028 Session Timers in SIP. In many cases, RFC 4028 is not supported by carriers providing SIP trunking services to their customers. In order to accommodate this, the SBC will interwork between PSTN carrier and Zoom Phone in order to provide support for Session Timers in SIP.

For more information about the Oracle SBC's support for RFC4028, please see the 840 Configuration Guide, page 4-300

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.



6.11 SIP Interface

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

GUI Path: session-router/SIP-interface

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

We will configure the sip-interface for each configured Realm object in this setup –

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

Config Parameter	Access	Core	Zoom Trunk	PSTN
Realm ID	Access	ZoomCore	Zoom	SIPTrunk
Out manipulationid	ACME_NAT_TO_FROM_IP	ACME_NAT_TO_FROM_IP	ACME_NAT_TO_FROM_IP	SIPTrunkManipulation
SIP Port Config Parameter				
Address	141.146.36.89	141.146.36.80	141.146.36.68	192.168.1.10
Port	5065	5061	5061	5060
Transport protocol	UDP	TLS	TLS	UDP

TLS profile		TLSZoom	TLSZoom	
Allow anonymous	registered	agents-only	agents-only	agents-only
Session Timer Profile			ZoomSessionTimer	
nat-traversal	always			
registration-caching	enabled			
route-to-registrar	enabled			

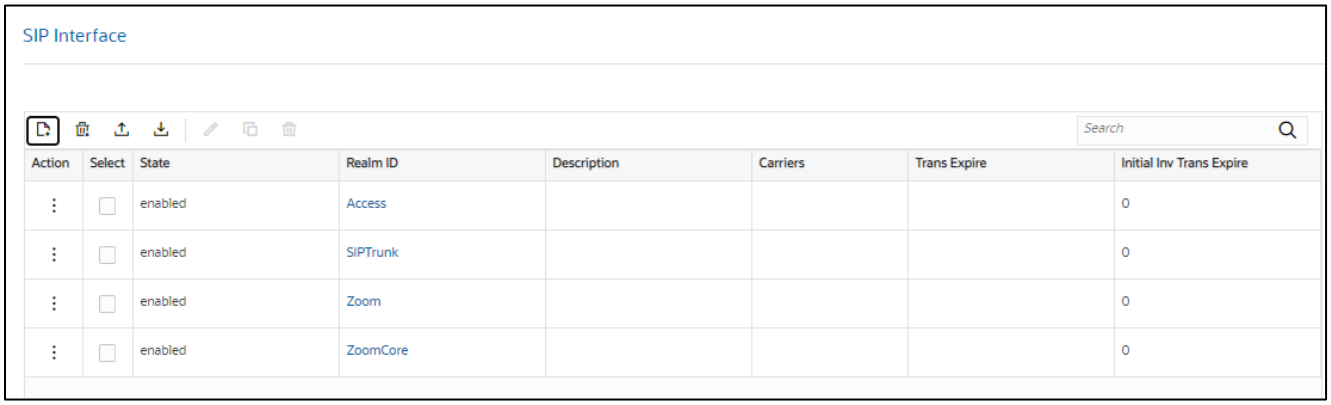
Please note, here we will assign some of the configuration elements configured earlier in this document, i.e.….

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

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

nat-traversal - always
registration-caching – enabled
route-to-registrar – enabled

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



6.12 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

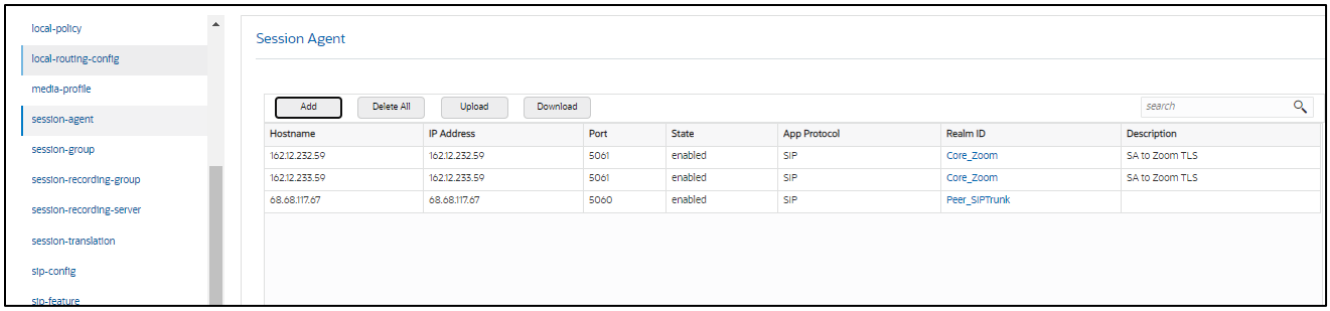
ACLI Path: config t→session-router→session-agent

You will need to configure three session agents for Zoom Trunk, Zoom Registrar and one for SIPTrunk.

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

Config parameter	Zoom Trunk	Zoom Registrar	SIPTrunk
Hostname	162.12.232.59	us01sip0h.ny.zoom.us	192.168.1.10
IP Address	162.12.232.59		192.168.1.10
Port	5061	5091	5060
Transport method	StaticTLS	StaticTLS	UDP+TCP
Realm ID	Zoom	ZoomCore	Peer_SIPTrunk
Ping Method	OPTIONS	OPTIONS	OPTIONS
Ping Interval	30	30	30
Ping Response	Enabled	Enabled	Enabled
out-manipulationid	ZoomE164		

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

  Click OK at the bottom

6.13 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.

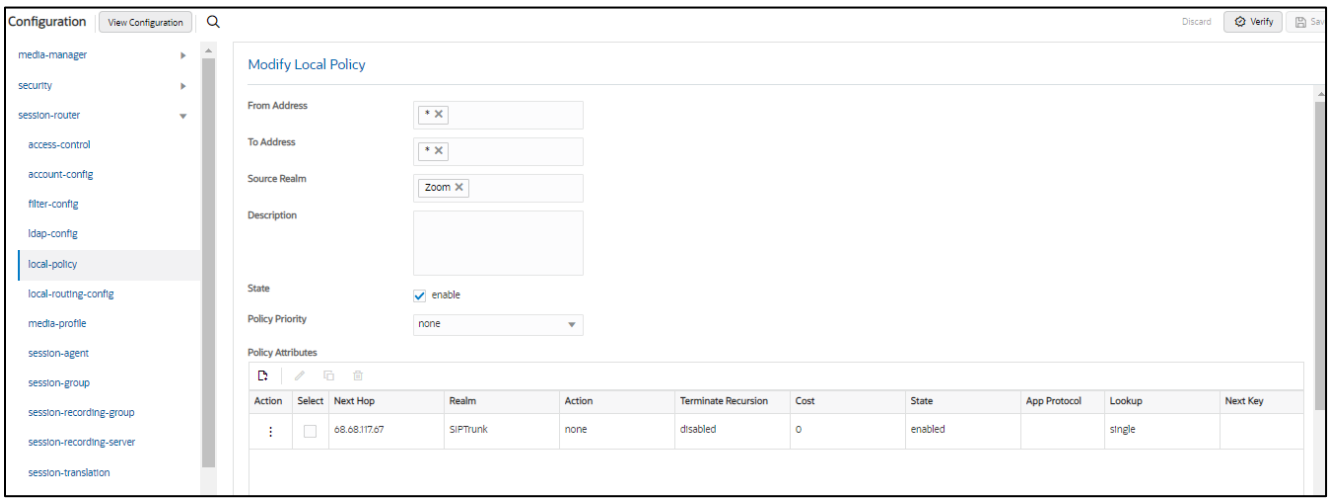
GUI Path: session-router/local-policy

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

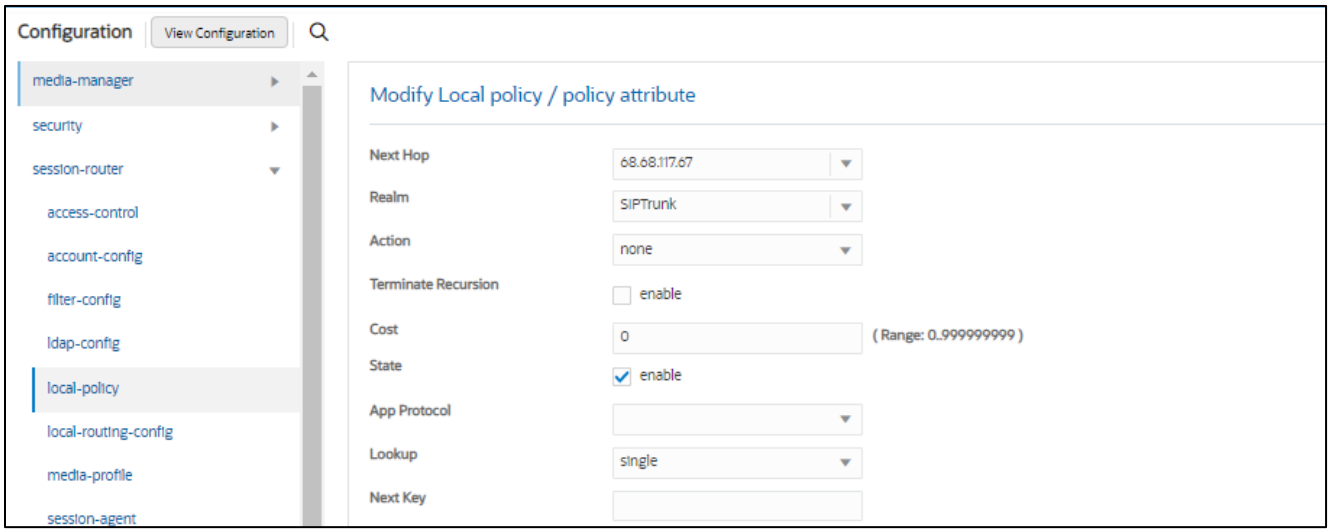
In order to route SIP traffic to and from Zoom Phone Platform, the following local-policies will need to be configured.

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

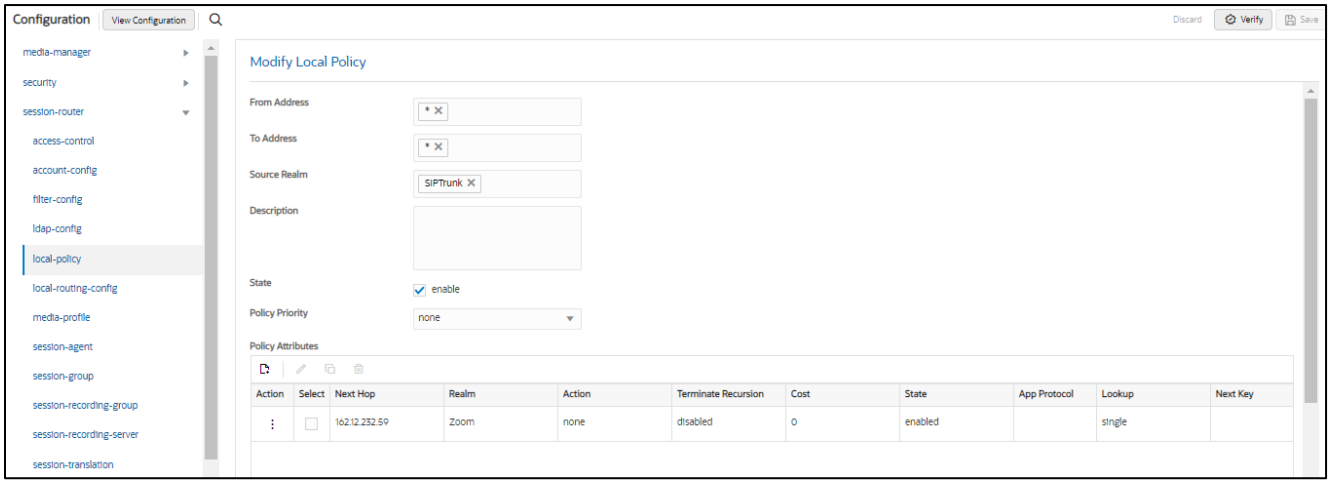
6.13.1 Route Calls from Zoom Trunk To PSTN:



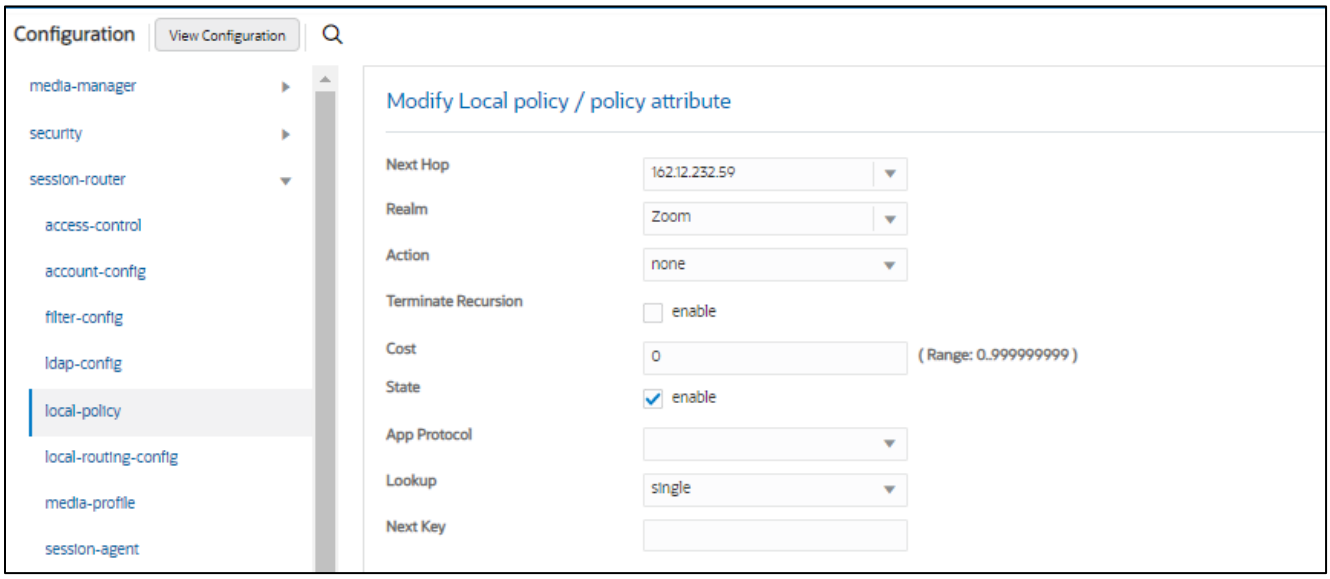
Policy Attribute:



6.13.2 Route Calls from PSTN To Zoom:



Policy Attribute:



- Click OK at the bottom of each when applicable:
-

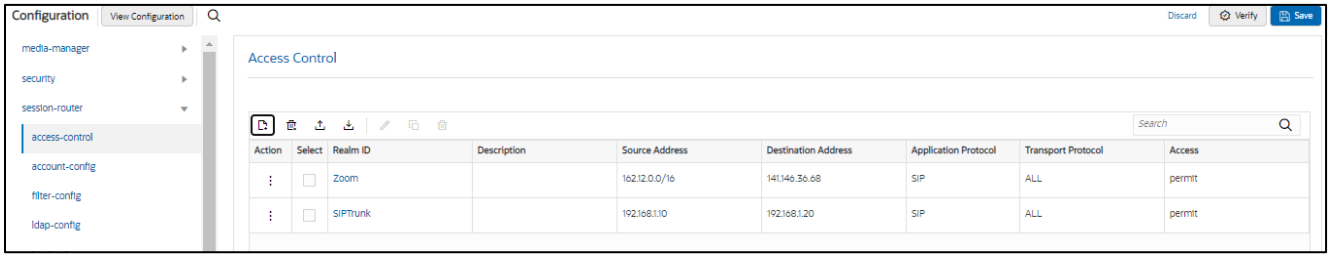
6.14 Access Controls

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.

7 Verify Connectivity

7.1 ORACLE SBC Options Ping

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

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

- At the top, click "Widgets"

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

GUI Path: Monitor and Trace/Signaling/SIP/Methods/OPTIONS

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

8 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.

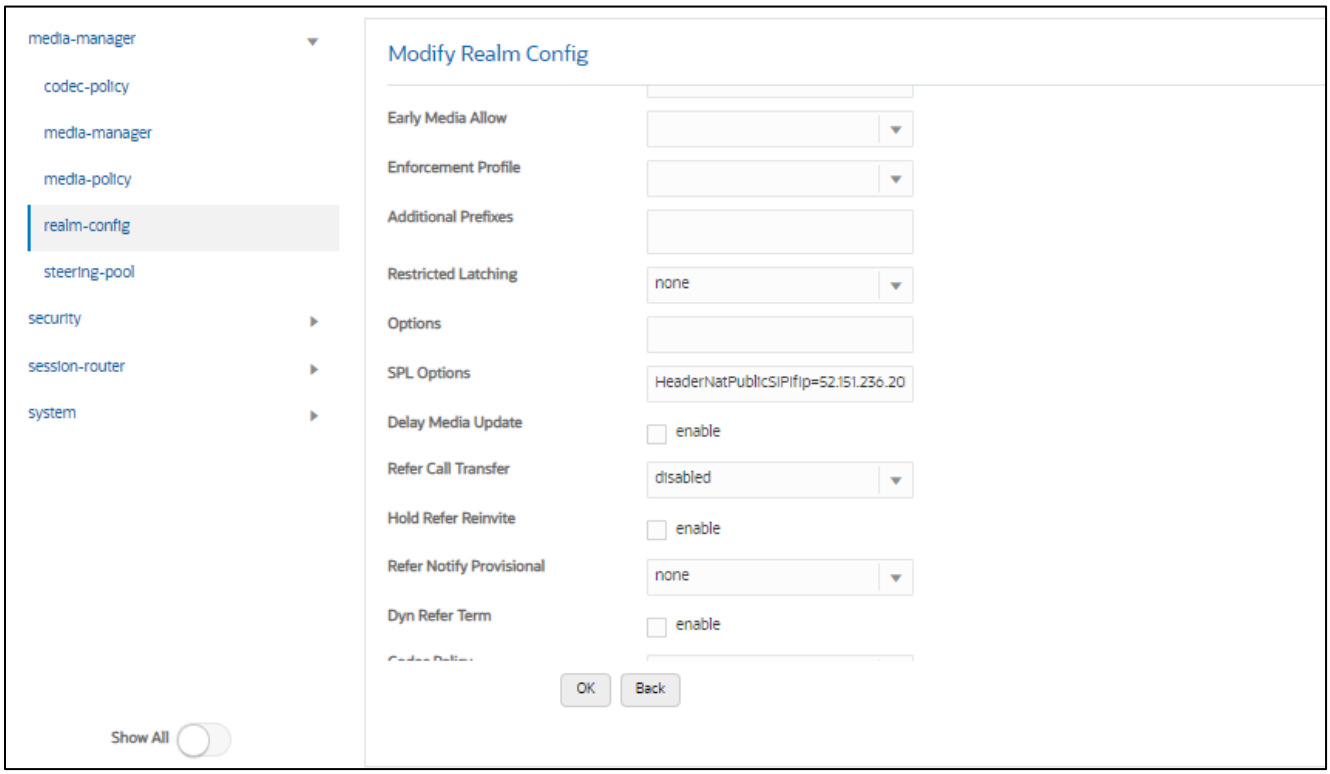
- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

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 SBC configuration that was deployed behind a Nat Device.

9 Caveat

9.1 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.

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