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

## 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

As a best practice always follow the latest Application note available on the Oracle TechNet Website.
https://www.oracle.com/technical-resources/documentation/acme-packet.html

| Version | Date Revised | Description of Changes |
|---|---|---|
| 1.0 | 04/09/2020 | • Initial publication |
| 1.1 | 14/08/2020 | • Modified version created after TekVizion Certification. |
| 1.2 | 11/01/2021 | • Update on Section 4- Added Zoom Web BYOC Configuration. |
| 1.3 | 16/08/2021 | • Update on Section 4- Added Step to assign a Calling Package. |
| 1.4 | 18/06/2021 | • Updated Zoom CA Certificates from GoDaddy to Digicert |
| 1.5 | 10/01/2022 | • Included Configuration Assistant Section. |
| 1.6 | 14/07/2022 | • Updated Section 3.1- New SBC Hardware added.<br>• Added New Section 6.5.1- Zoom Trusted CA List added |

# 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:

SCZ840p1

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
- AP 3950 (Release SCZ9.0.0 Only)
- AP 4900 (Release SCZ9.0.0 Only)

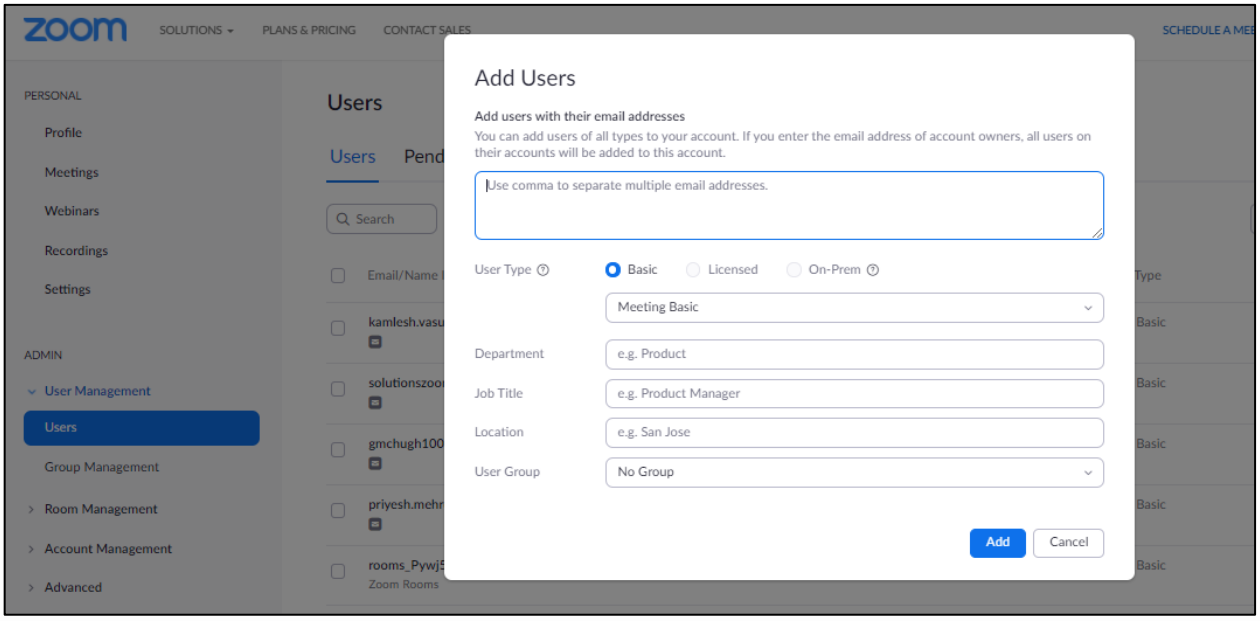
## 4 Zoom Phone Configuration

This Section describes the steps to configure BYOC Phone Numbers on the Zoom Admin Portal and assign the BYOC Number to a User. For detailed assistance with setting up and configuring your Zoom Phone System, please reach out to Zoom Sales: https://zoom.us/contactsales

### 4.1 Create a Zoom User

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

Click Add to create new Zoom users. Provide the necessary details about the New User and Click on Add to Add the 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.

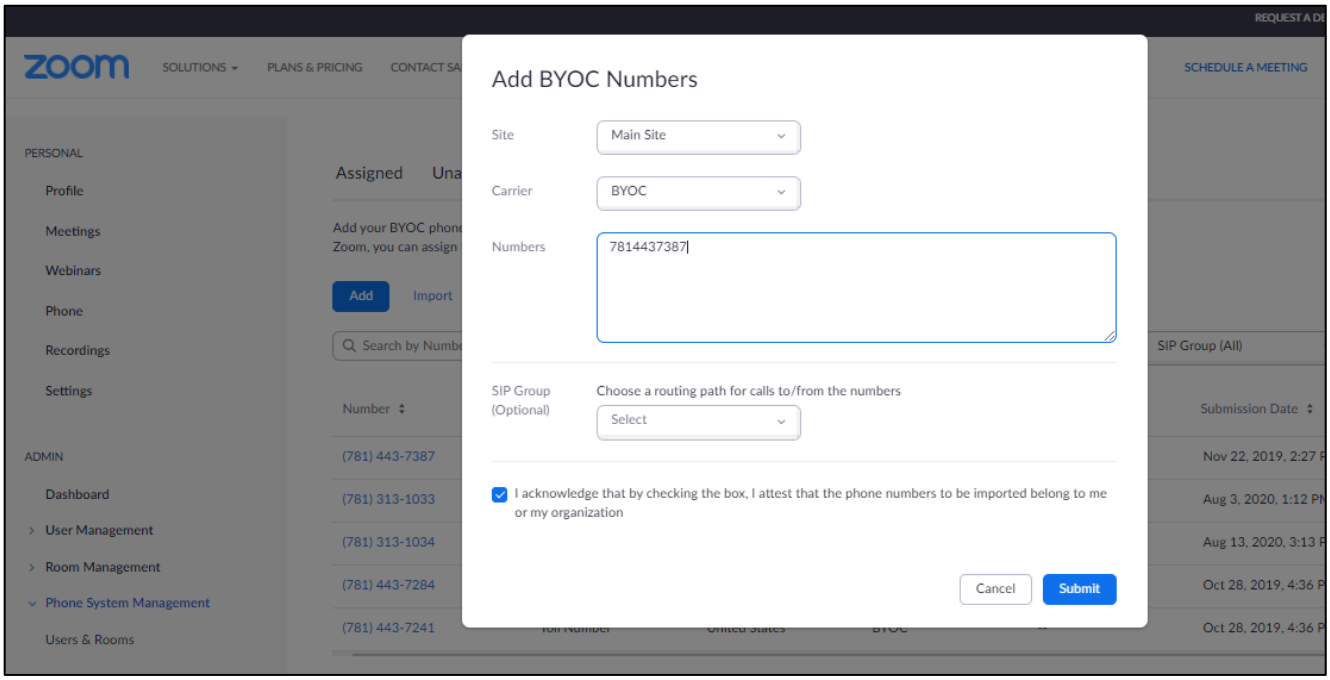
**Carrier** –Choose BYOC

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**.



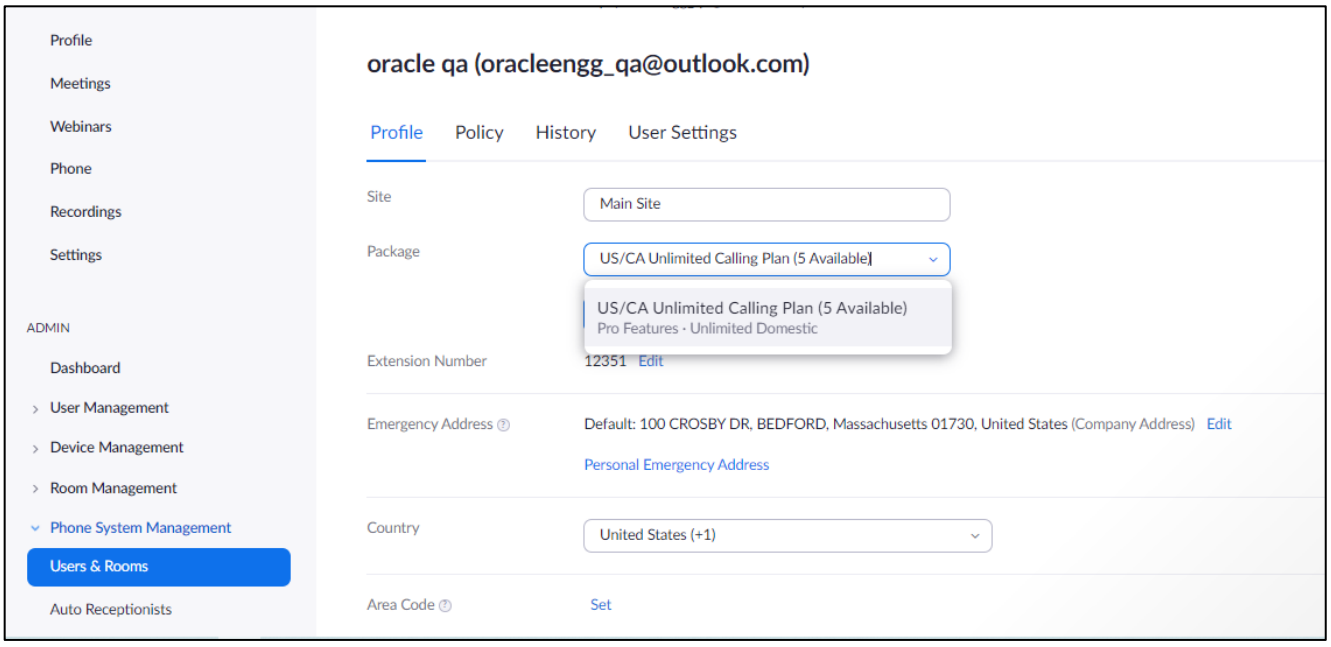

### 4.3 Assign a Calling Package to User

You may require adding a Calling package to the user before a Calling Number can be assigned to a User.

To assign a calling package

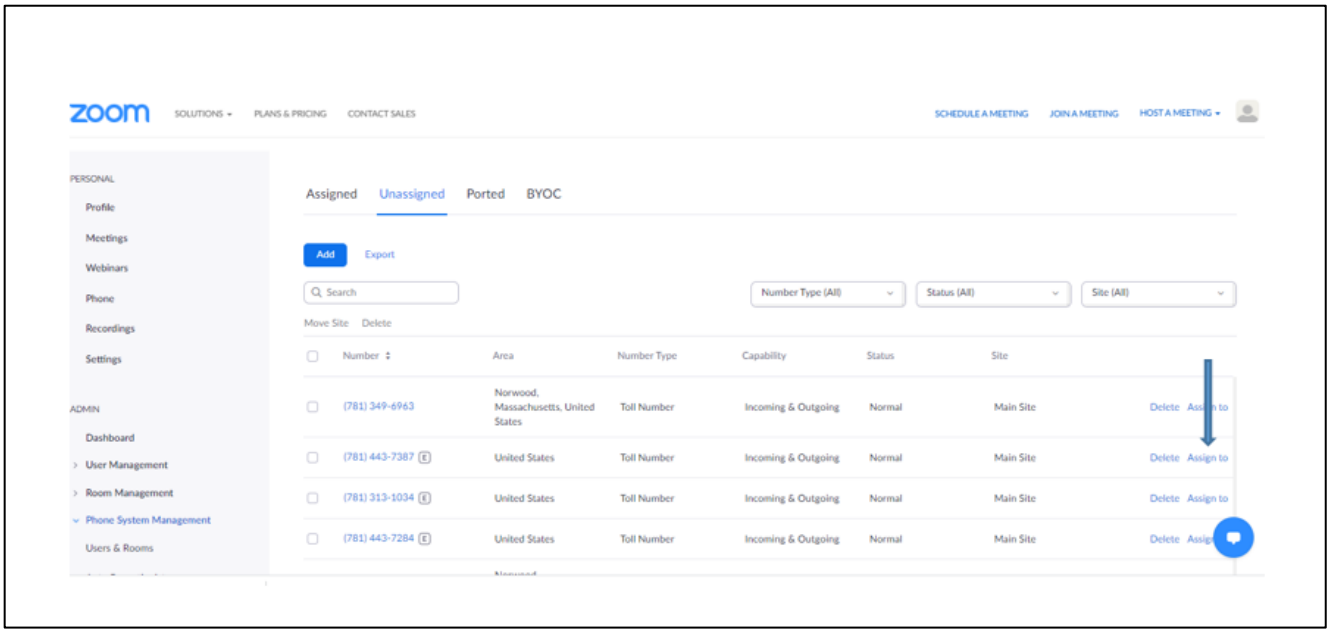
Navigate to **Users and Rooms > Package**

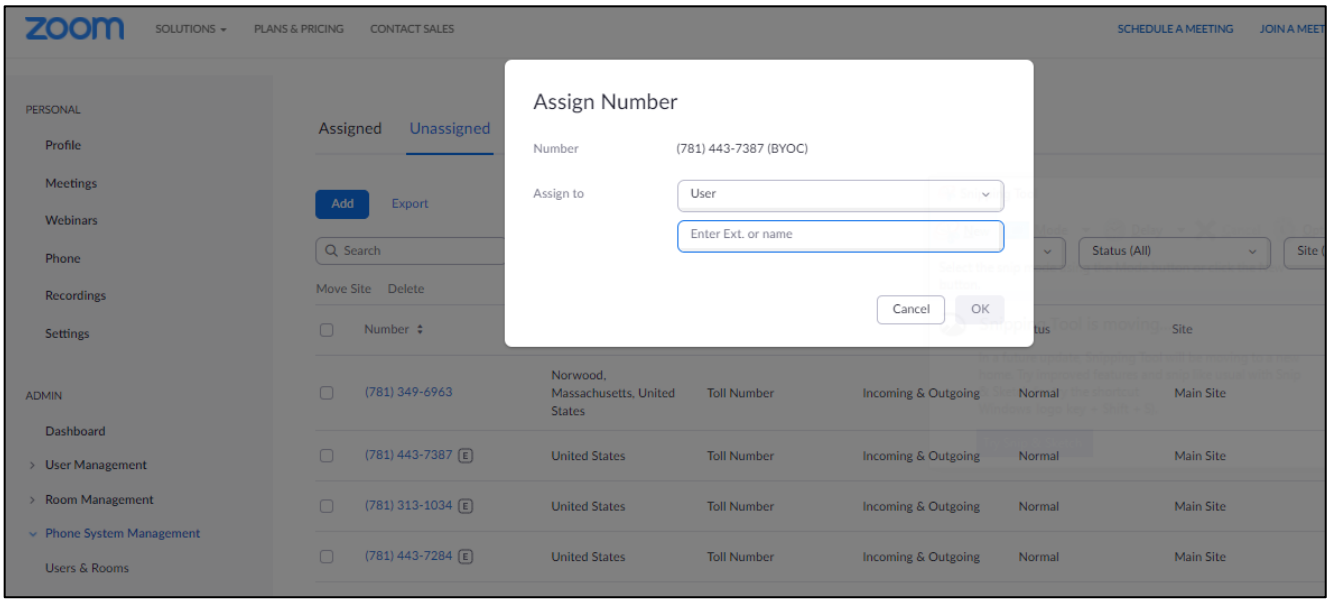
Choose the appropriate package and assign the package to the Respective User.




## 4.4 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 a User.






## 5 Infrastructure Requirements

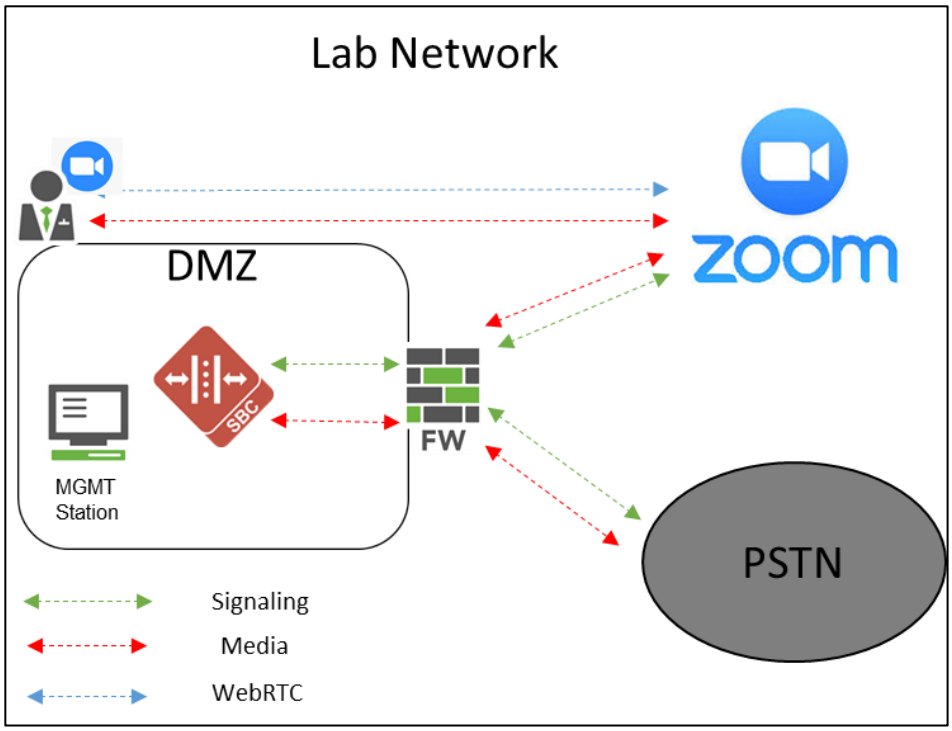
The table below shows the list of infrastructure prerequisites for deploying Zoom Premise Peering.

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




*These instructions cover configuration steps between the Oracle SBC and Zoom Phone. 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
- Zoom Public CA certificates to add to trust store of SBC

There are two methods for configuring the Oracle SBC, ACLI, or GUI. If the Oracle SBC being deployed is new, with no existing configuration, the simplest way to configure it to interface with Cisco Call Manager (Cisco CUCM) is by utilizing the Configuration Assistant feature.

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, 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.

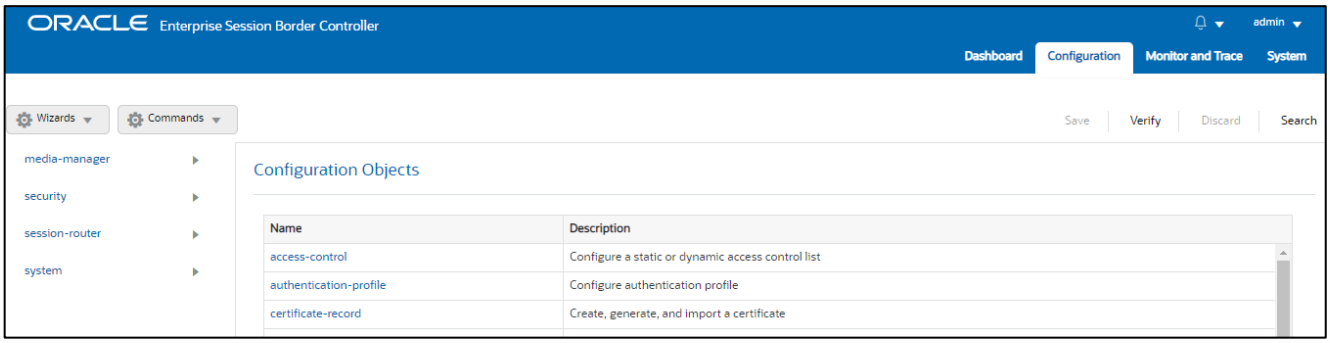
To access the Oracle SBC GUI, enter the management IP address into a web brower.
When the login screen appears, enter the username and password to access the ORACLE SBC.

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.

*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

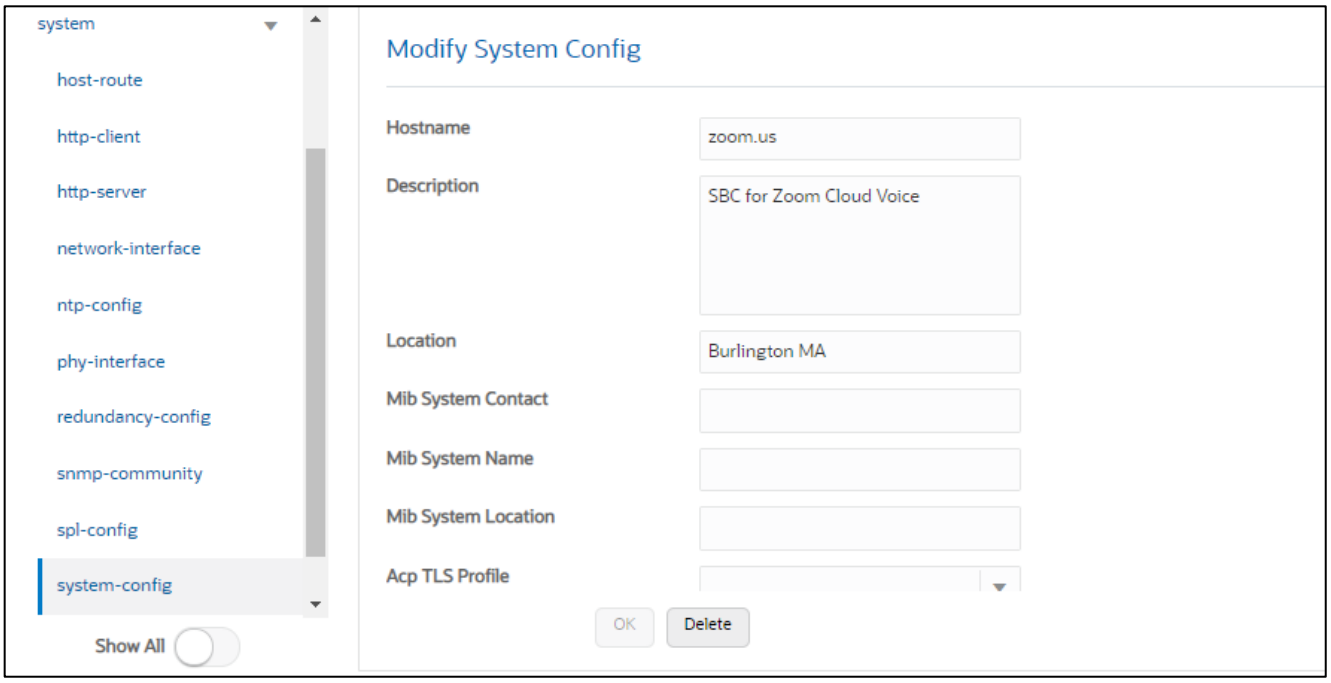
To configure system level functionality for the ORACLE SBC, you must first enable the system-config

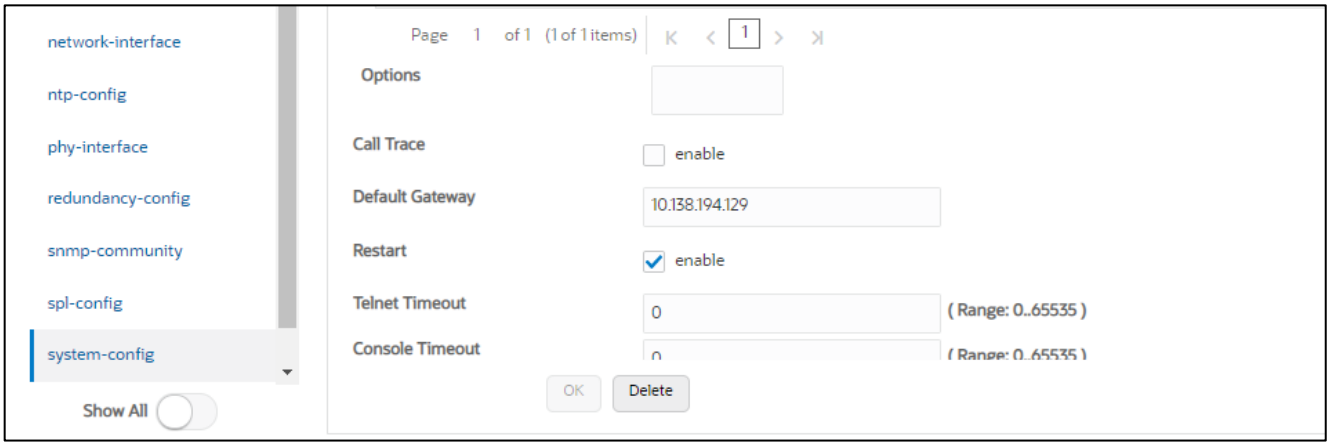
GUI Path: system/system-config

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

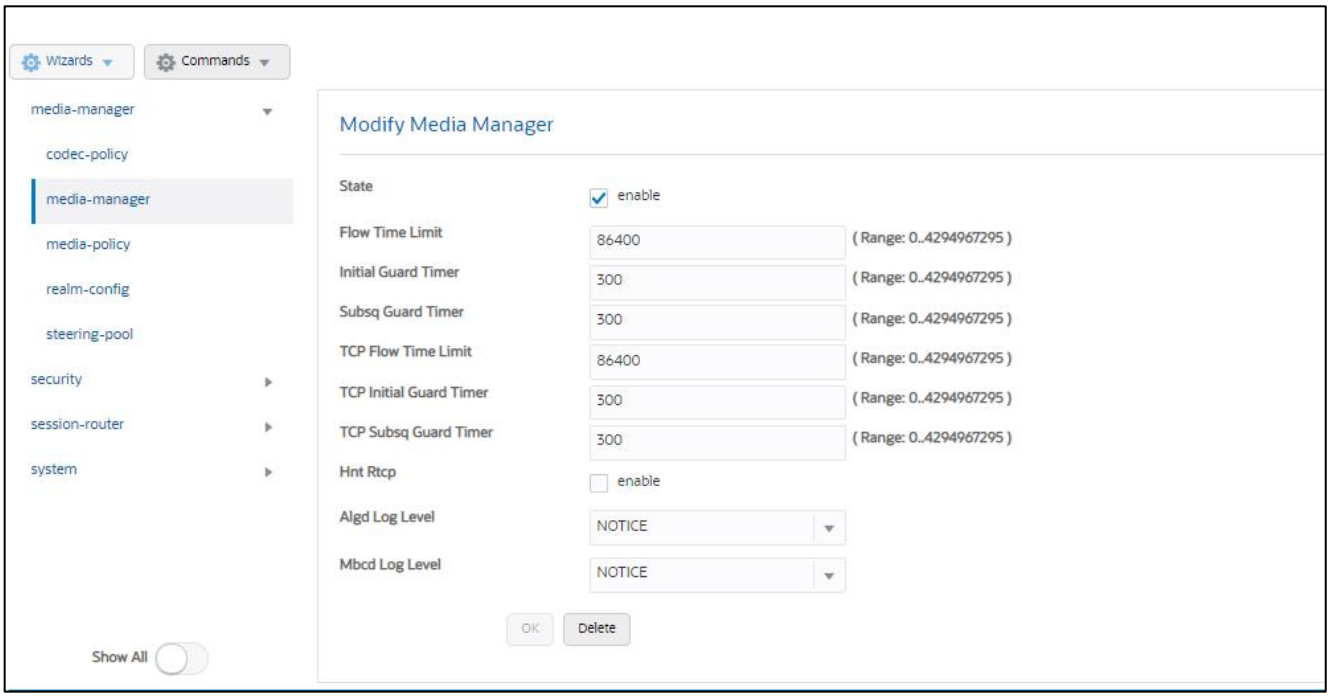
GUI Path: media-manager/media-manager

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

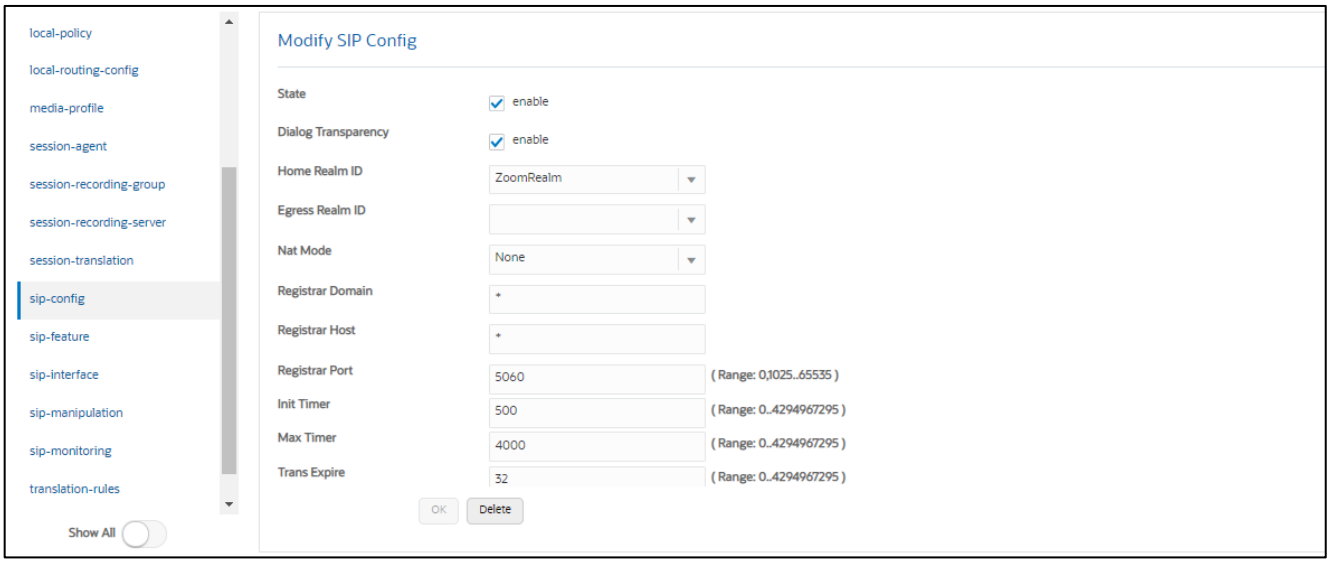
To enable SIP related objects on the ORACLE SBC, you must first configure the global SIP Config element:

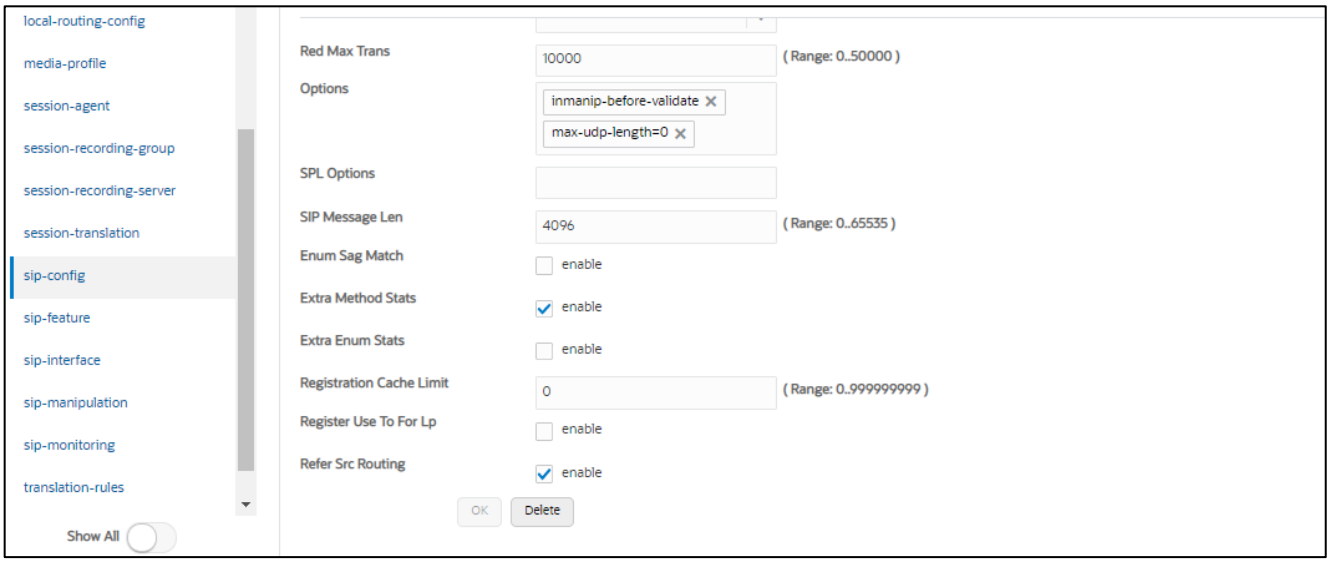
GUI Path: session-router/SIP-config

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

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

- 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)



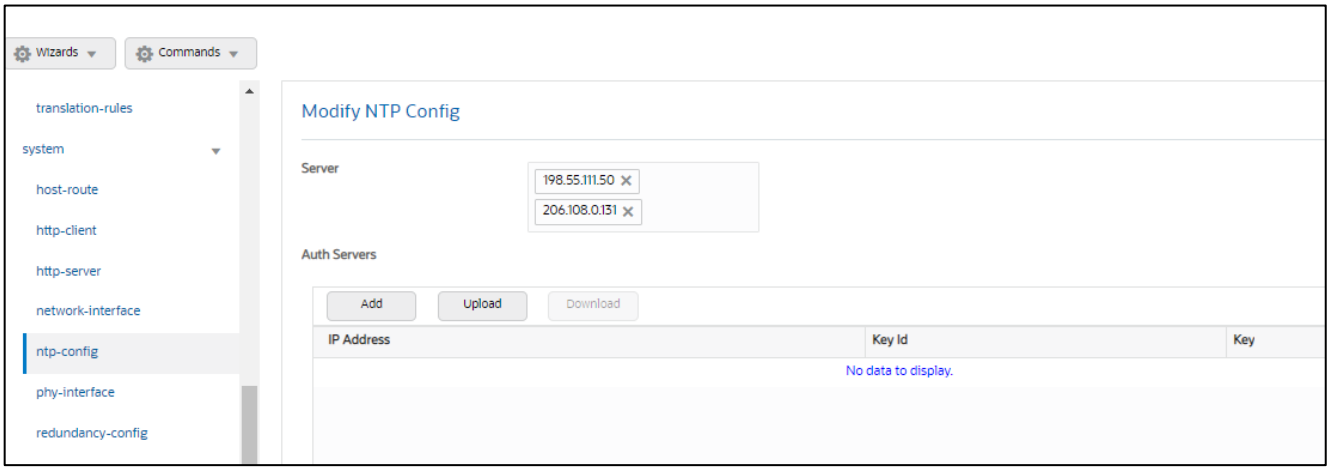



- Click OK at the bottom

### 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 Zoom Cloud Voice, the other to connect to PSTN Network.

### 6.3.1 Physical Interfaces

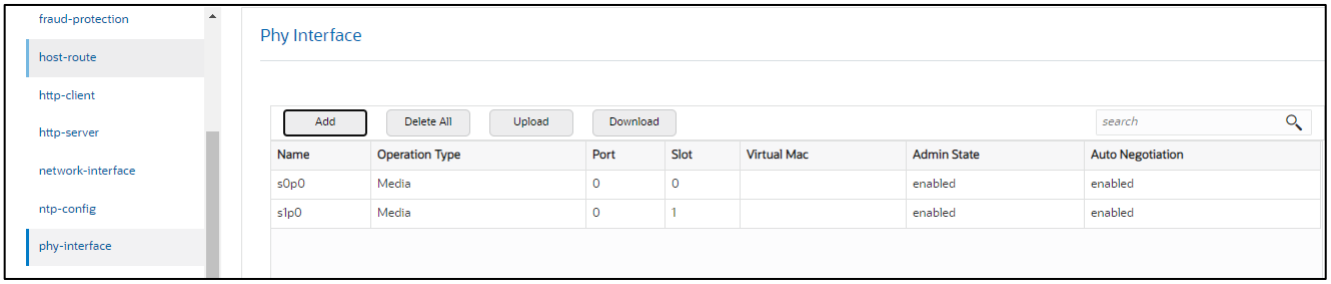
GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

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

| Config Parameter | Zoom | 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

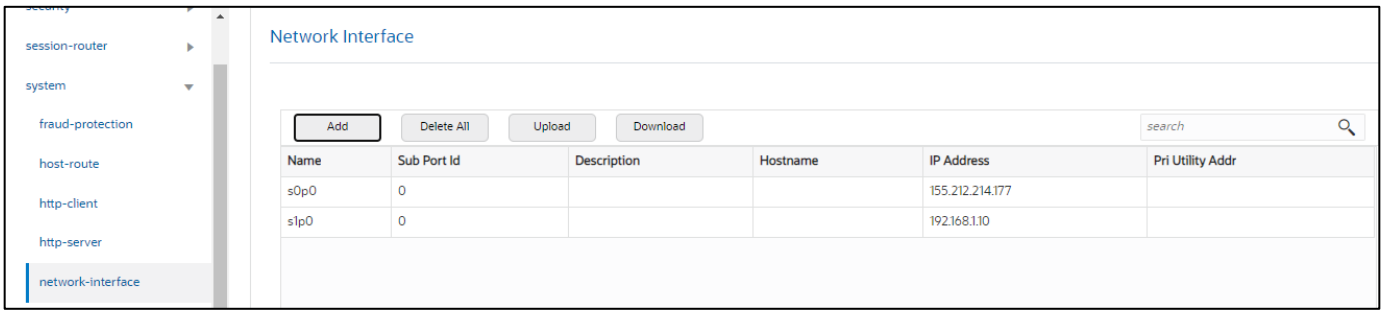
### 6.3.2 Network Interfaces

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) | |
| 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

## 6.4 Security Configuration

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

Zoom Phone allows 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.

### 6.4.1 Certificate Records

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

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

GUI Path: security/certificate-record

ACLI Path: config t→security→certificate-record

For the purposes of this application note, we'll create Five certificate records.They are as follows:

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

These Certificates can be downloaded at below links –

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

The follow certificates must be installed onto the SBC to trust the TLS Certificate provided by Zoom for TLS negotiation.DigiCert TLS Certificates can be downloaded at below Links.

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

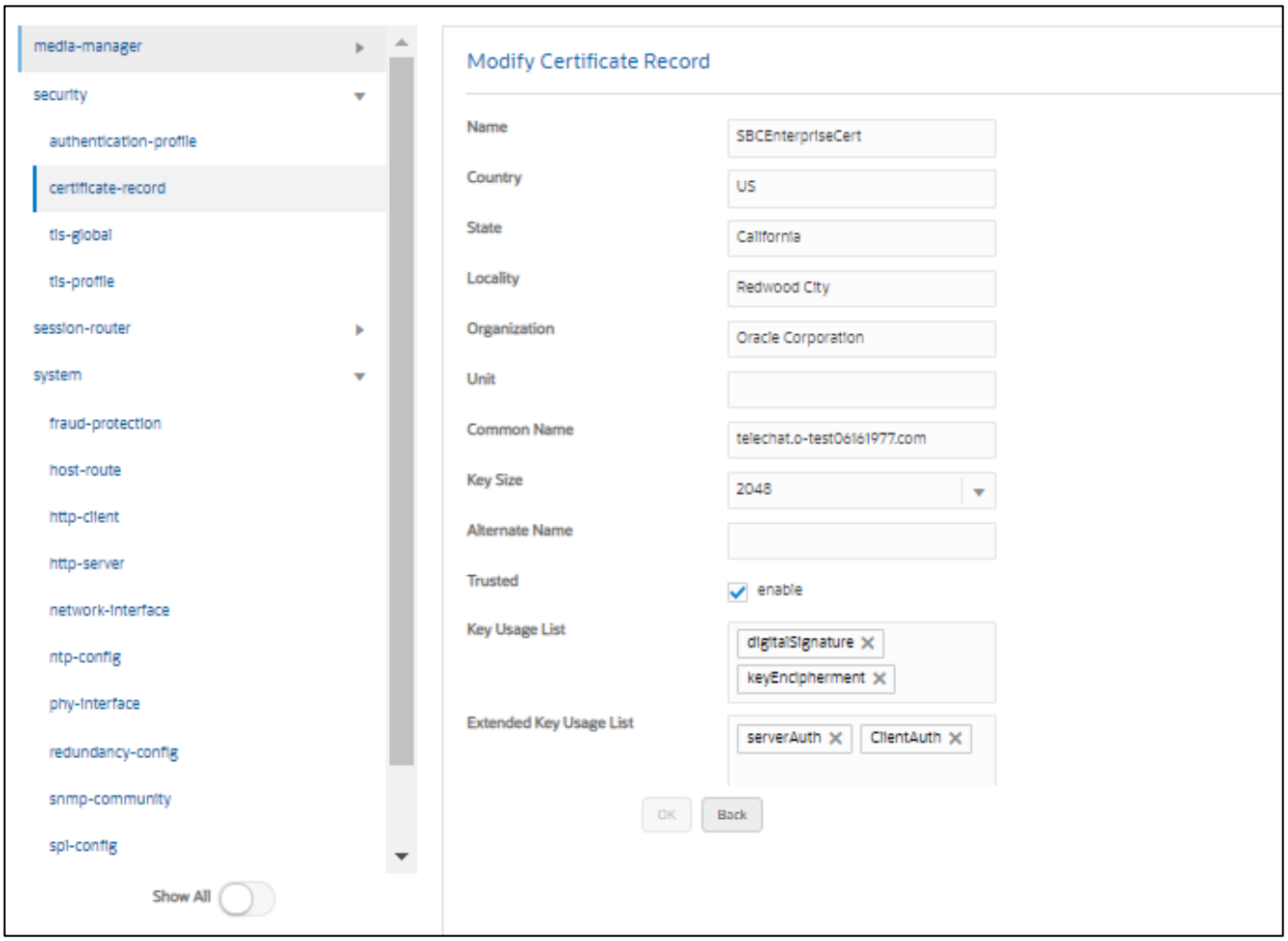
### 6.4.2 SBC End Entity Certificate

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

### 6.5 Root CA and Intermediate Certificates

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

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

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

| Config Parameter | Digicert Intermediate | DigiCertGlobalRootCA | DigiCertGlobalRootG2 | DigiCertGlobalRootG3 |
|---|---|---|---|---|
| Common Name | DigiCert SHA2 Secure Server CA | DigiCert Global Root CA | DigiCert Global Root G2 | DigiCert Global Root G3 |
| Key Size | 2048 | 2048 | 2048 | 2048 |
| Key-Usage-List | digitalSignature keyEncipherment | digitalSignature keyEncipherment | digitalSignature keyEncipherment | digitalSignature keyEncipherment |

| | | | | |
|---|---|---|---|---|
| Extended Key Usage List | serverAuth | serverAuth | serverAuth | serverAuth |
| Key algor | rsa | rsa | rsa | rsa |
| Digest-algor | Sha256 | Sha256 | Sha256 | Sha256 |

### 6.5.1 Zoom Approved CA Vendors

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

| Certificate Issuer Organization | Common Name or Certificate Name |
|---|---|
| Buypass AS-983163327 | Buypass Class 2 Root CA |
| Buypass AS-983163327 | Buypass Class 3 Root CA |
| Baltimore | Baltimore CyberTrust Root |
| Cybertrust, Inc | Cybertrust Global Root |
| DigiCert Inc | DigiCert Assured ID Root CA |
| DigiCert Inc | DigiCert Assured ID Root G2 |
| DigiCert Inc | DigiCert Assured ID Root G3 |
| DigiCert Inc | DigiCert Global Root CA |
| DigiCert Inc | DigiCert Global Root G2 |
| DigiCert Inc | DigiCert Global Root G3 |
| DigiCert Inc | DigiCert High Assurance EV Root CA |
| DigiCert Inc | DigiCert Trusted Root G4 |
| GeoTrust Inc. | GeoTrust Global CA |
| GeoTrust Inc. | GeoTrust Primary Certification Authority |
| GeoTrust Inc. | GeoTrust Primary Certification Authority - G2 |
| GeoTrust Inc. | GeoTrust Primary Certification Authority - G3 |
| GeoTrust Inc. | GeoTrust Universal CA |
| GeoTrust Inc. | GeoTrust Universal CA 2 |
| Symantec Corporation | Symantec Class 1 Public Primary Certification Authority - G4 |
| Symantec Corporation | Symantec Class 1 Public Primary Certification Authority - G6 |
| Symantec Corporation | Symantec Class 2 Public Primary Certification Authority - G4 |
| Symantec Corporation | Symantec Class 2 Public Primary Certification Authority - G6 |

| | |
|---|---|
| Thawte, Inc. | Thawte Primary Root CA |
| Thawte, Inc. | Thawte Primary Root CA - G2 |
| Thawte, Inc. | Thawte Primary Root CA - G3 |

| | |
|---|---|
| VeriSign, Inc. | VeriSign Class 1 Public Primary Certification Authority - G3 |
| VeriSign, Inc. | VeriSign Class 2 Public Primary Certification Authority - G3 |
| VeriSign, Inc. | VeriSign Class 3 Public Primary Certification Authority - G3 |
| VeriSign, Inc. | VeriSign Class 3 Public Primary Certification Authority - G4 |
| VeriSign, Inc. | VeriSign Class 3 Public Primary Certification Authority - G5 |
| VeriSign, Inc. | VeriSign Universal Root Certification Authority |
| AffirmTrust | AffirmTrust Commercial |
| AffirmTrust | AffirmTrust Networking |
| AffirmTrust | AffirmTrust Premium |
| AffirmTrust | AffirmTrust Premium ECC |
| Entrust, Inc. | Entrust Root Certification Authority |
| Entrust, Inc. | Entrust Root Certification Authority - EC1 |
| Entrust, Inc. | Entrust Root Certification Authority - G2 |
| Entrust, Inc. | Entrust Root Certification Authority - G4 |
| Entrust.net | Entrust.net Certification Authority (2048) |
| GlobalSign | GlobalSign |
| GlobalSign | GlobalSign |
| GlobalSign | GlobalSign |
| GlobalSign nv-sa | GlobalSign Root CA |
| The GoDaddy Group, Inc. | Go Daddy Class 2 CA |
| GoDaddy.com, Inc. | Go Daddy Root Certificate Authority - G2 |
| Starfield Technologies, Inc. | Starfield Class 2 CA |
| Starfield Technologies, Inc. | Starfield Root Certificate Authority - G2 |
| QuoVadis Limited | QuoVadis Root CA 1 G3 |
| QuoVadis Limited | QuoVadis Root CA 2 |
| QuoVadis Limited | QuoVadis Root CA 2 G3 |
| QuoVadis Limited | QuoVadis Root CA 3 |
| QuoVadis Limited | QuoVadis Root CA 3 G3 |
| QuoVadis Limited | QuoVadis Root Certification Authority |
| Comodo CA Limited | AAA Certificate Services |
| AddTrust AB | AddTrust Class 1 CA Root |

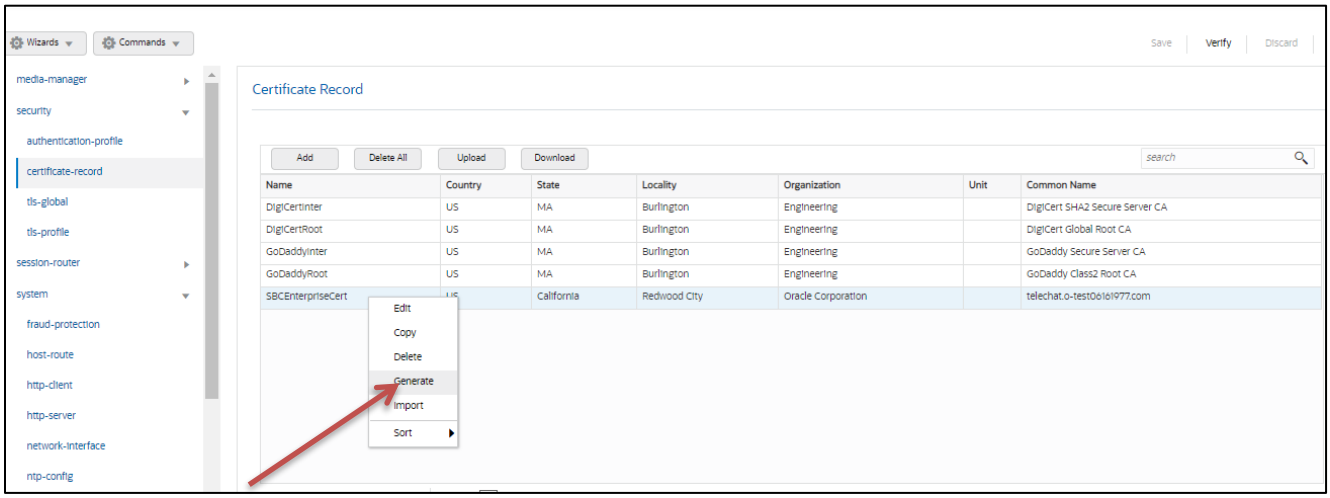
| AddTrust AB | AddTrust External CA Root |
|---|---|
| COMODO CA Limited | COMODO Certification Authority |
| COMODO CA Limited | COMODO ECC Certification Authority |
| COMODO CA Limited | COMODO RSA Certification Authority |
| The USERTRUST Network | USERTrust ECC Certification Authority |
| The USERTRUST Network | USERTrust RSA Certification Authority |
| T-Systems Enterprise Services GmbH | T-TeleSec GlobalRoot Class 2 |
| T-Systems Enterprise Services GmbH | T-TeleSec GlobalRoot Class 3 |

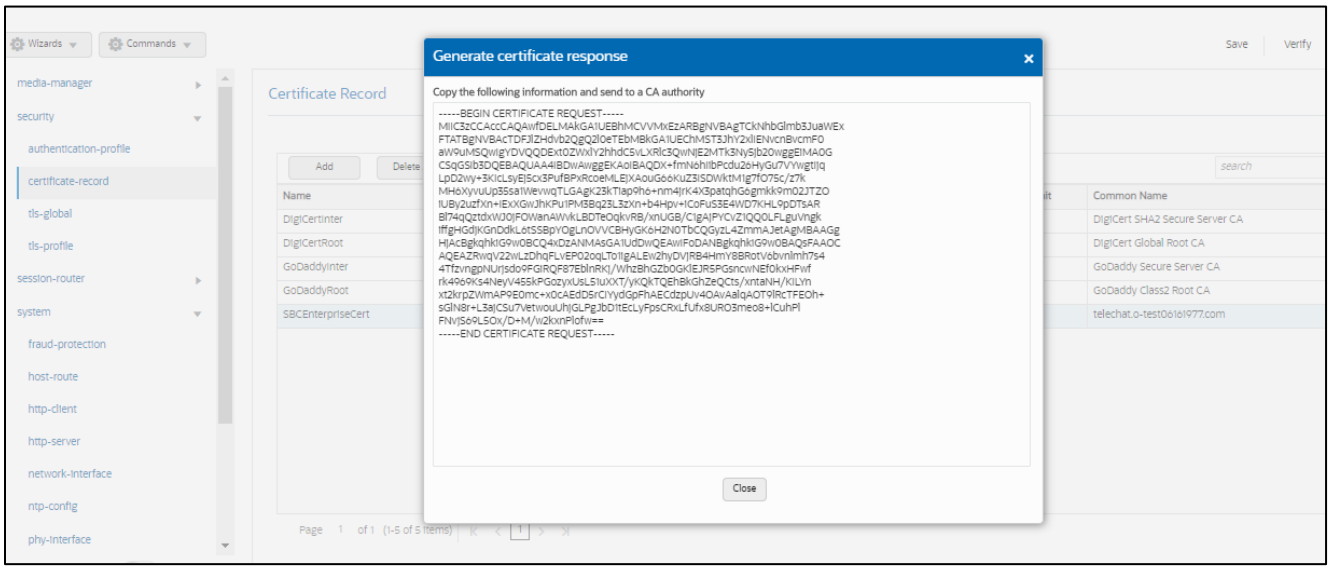
### 6.5.2 Generate Certificate Signing Request

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 at the top:

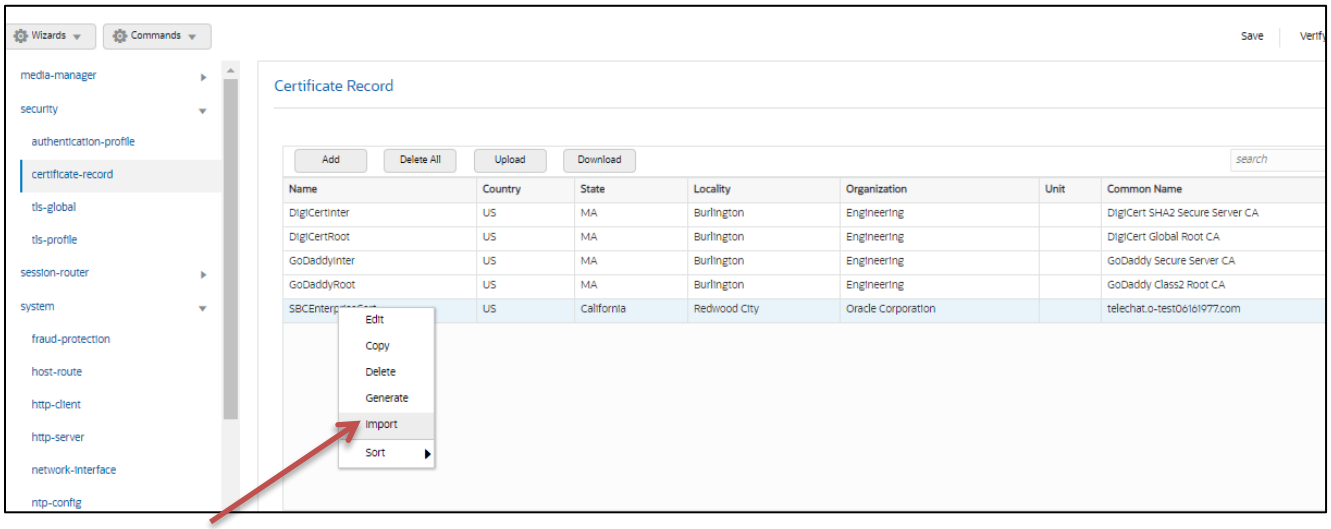


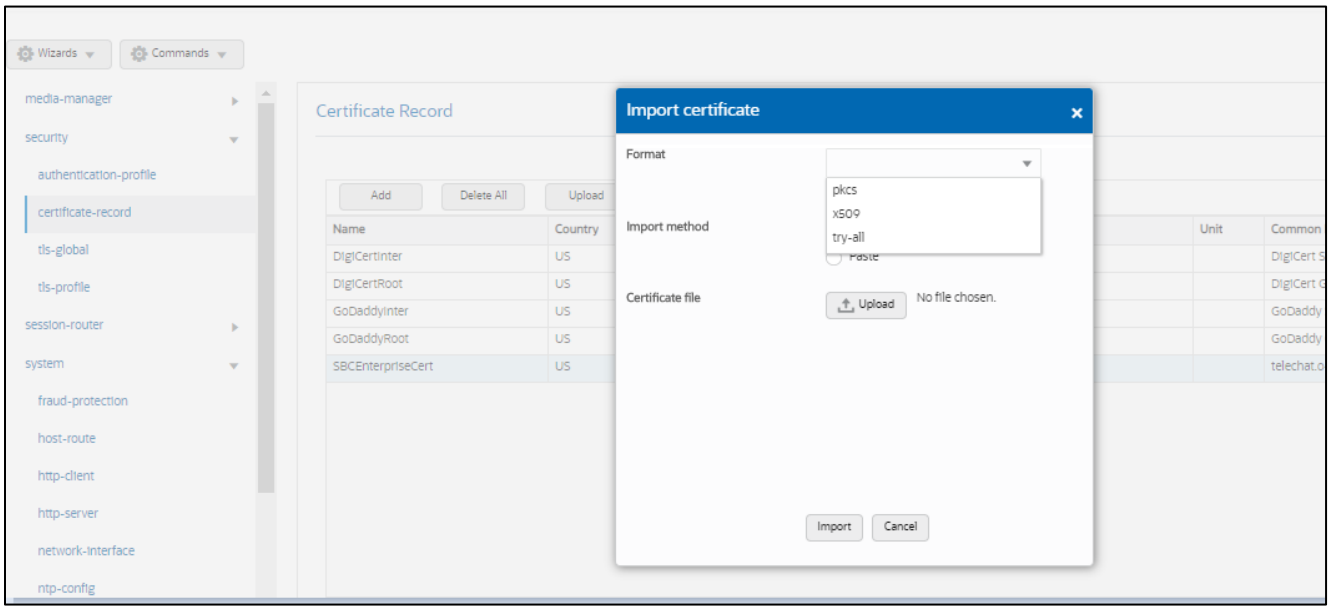



- copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, **a save and activate is required** before you can import the certificates to each certificate record created above.

### 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:

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

- DigiCertIntermediate
- DigiCertGlobalRootCA
- DigiCertGlobalRootG2
- DigiCertGlobalRootG3

At this stage, all required certificates have been imported.

### 6.5.4 TLS Profile

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

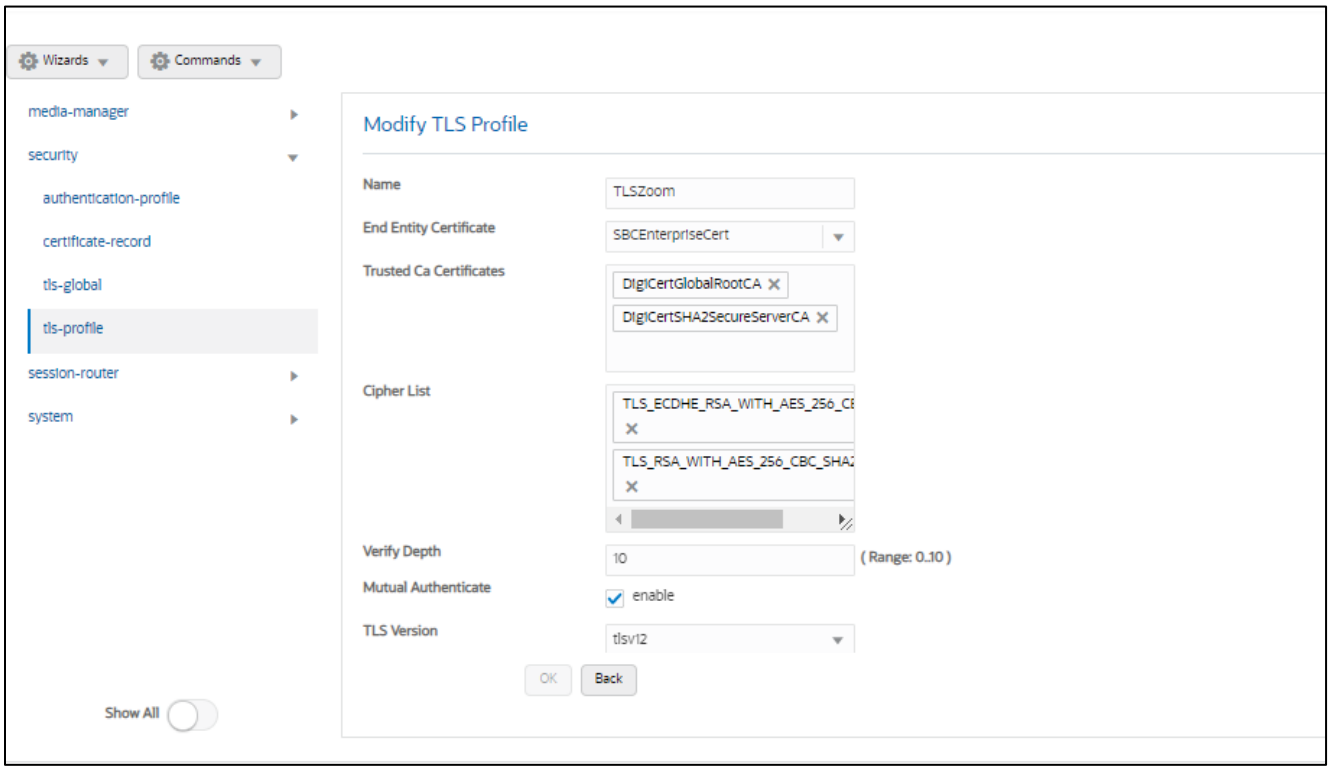
GUI Path: security/tls-profile

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.

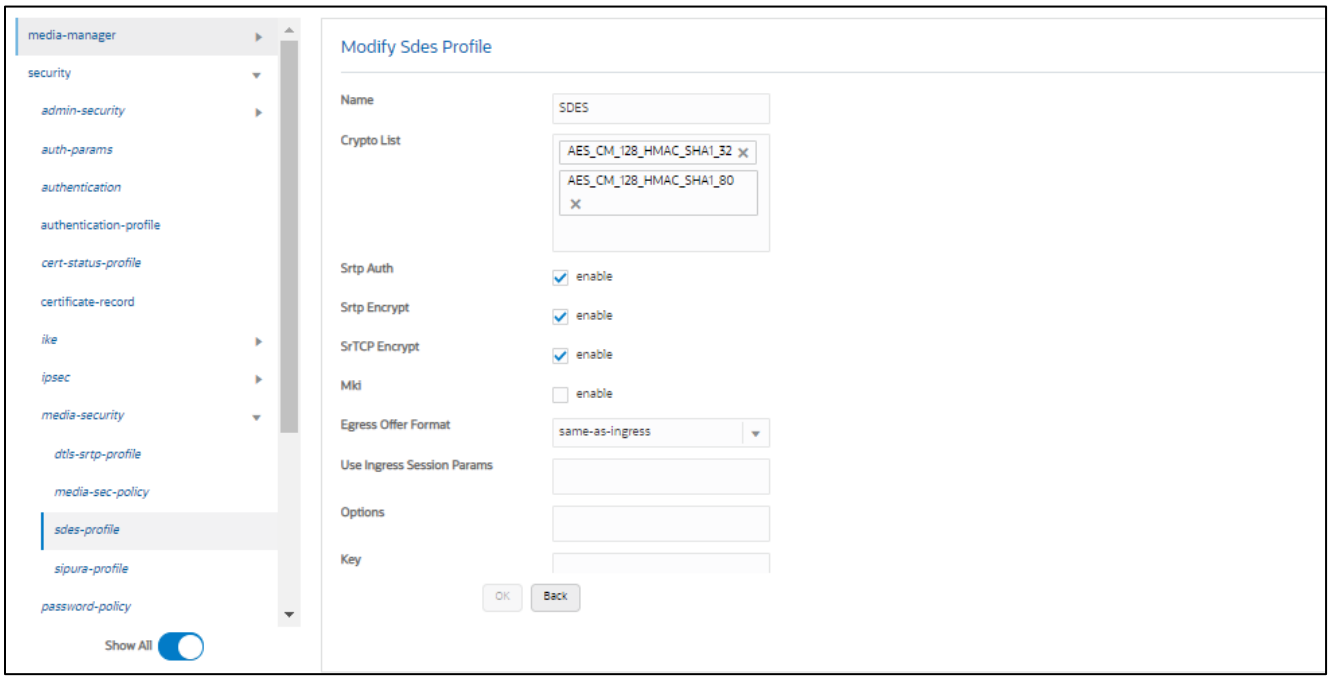
GUI Path: security/media-security/sdes-profile

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

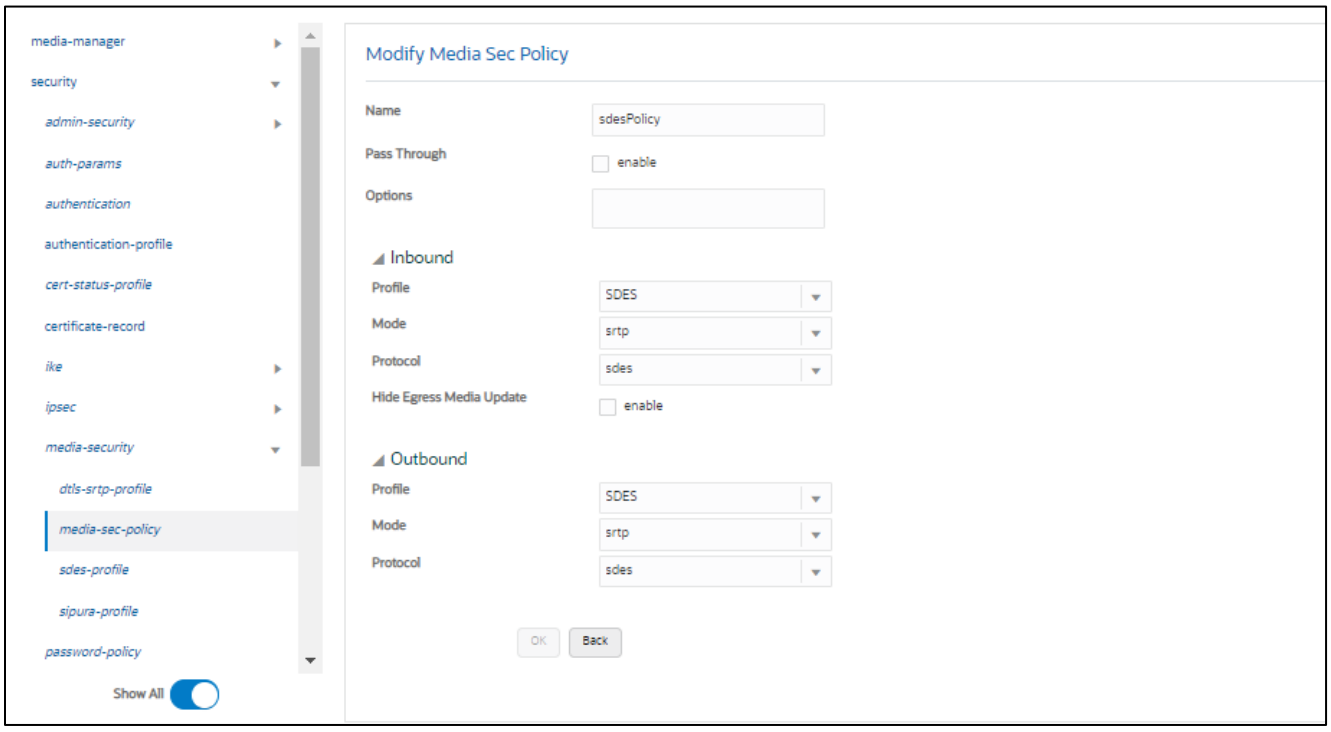
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them) and, if SRTP needs to be used, the sdes-profile that needs to be used

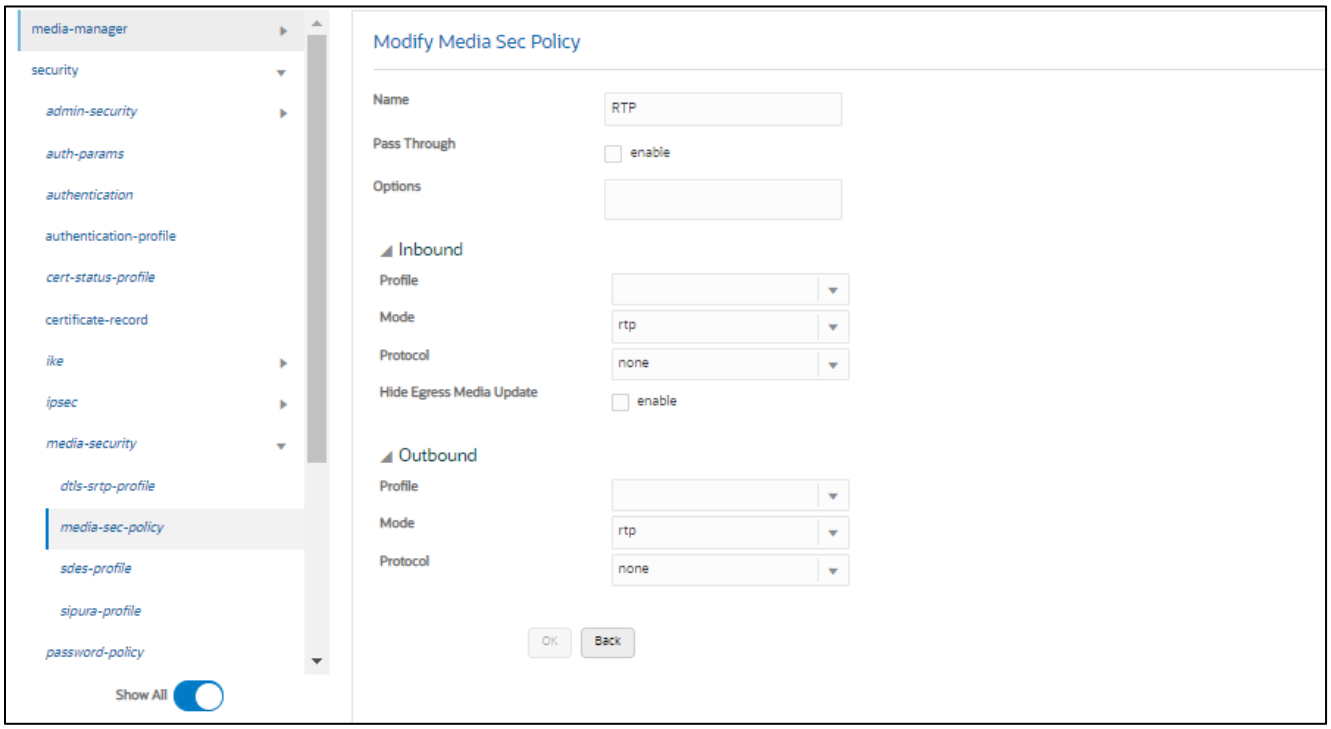
In this example, we are configuring two media security policies. One to secure and decrypt media toward Zoom, the other for non-secure media facing PSTN.

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.

**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

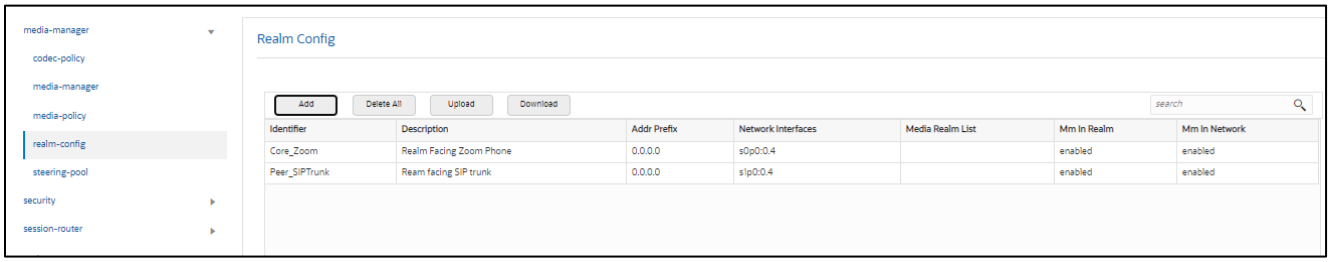
ACLI Path: config t→media-manager→realm-config

- 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, i.e.

- Network interface
- Media security policy



### 6.7.2 Steering Pools

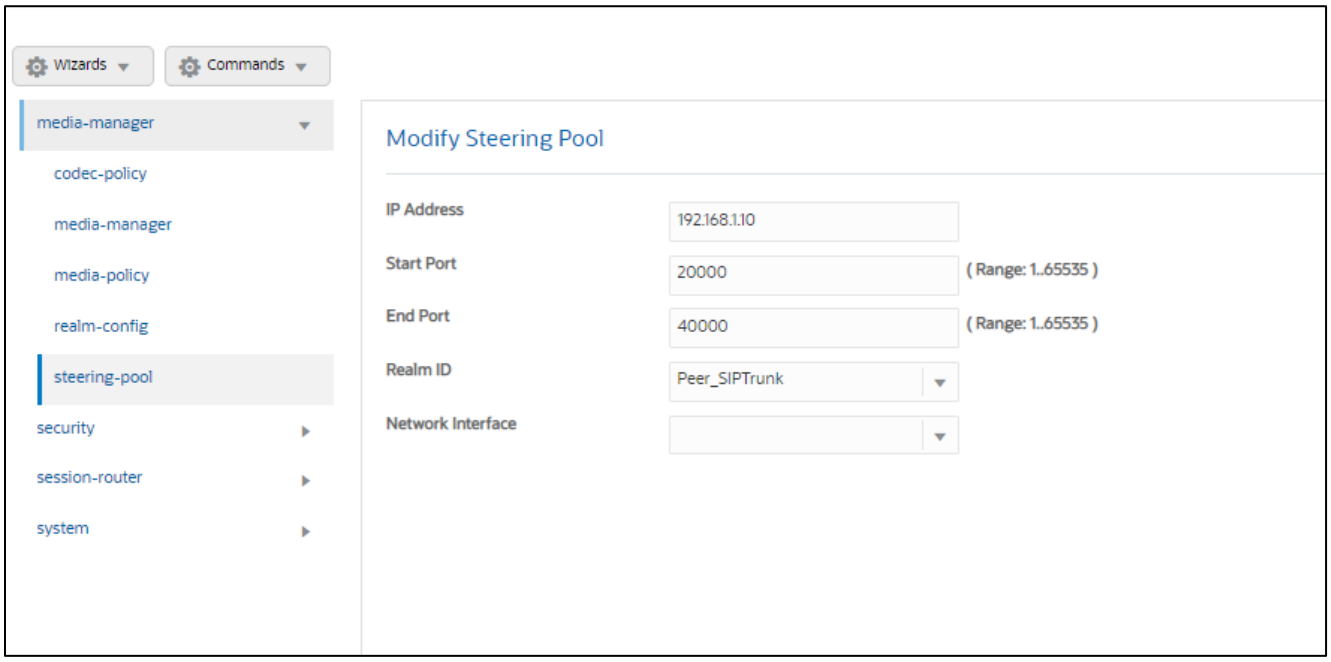
Steering pools define sets of ports that are used for steering media flows through the ORACLE SBC.
These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

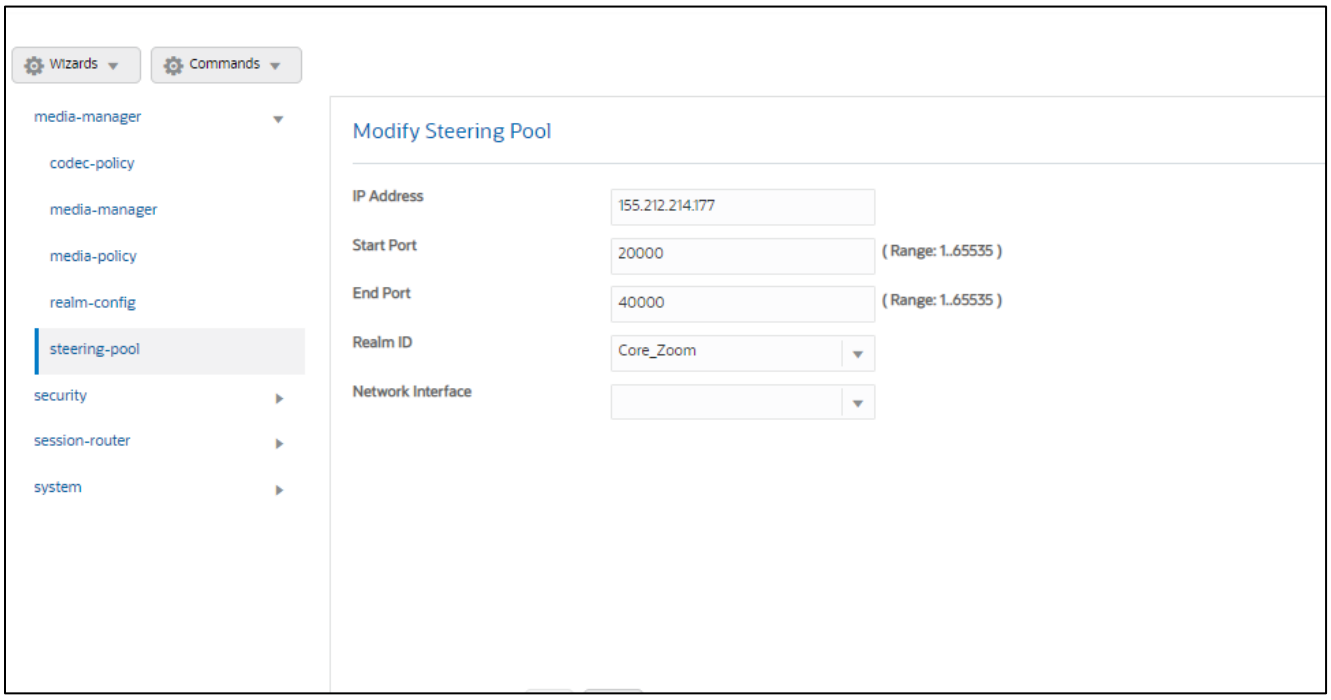
We configure one steering pool for PSTN and one steering pool for Zoom Phone

GUI Path: media-manager/steering-pool

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

- Click Add, and use the below examples to configure






## 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.*

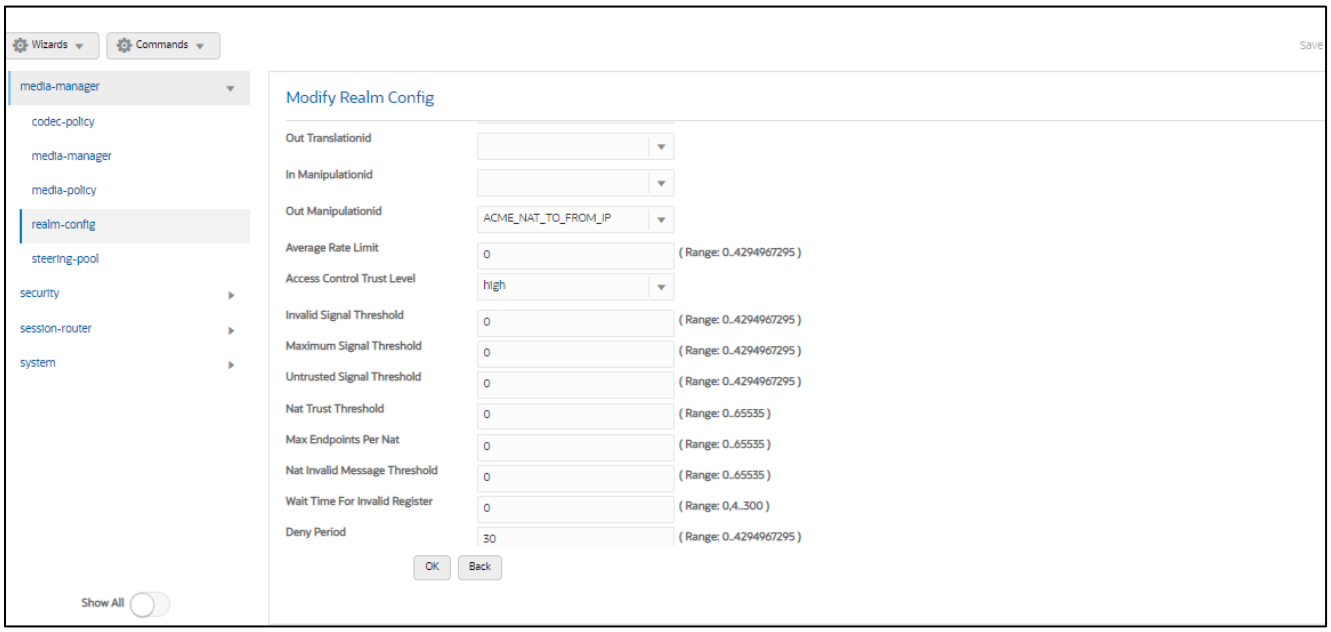
#### 6.8.1.1 Manipulation towards Zoom Side

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 and modifies packets generated by the Oracle SBC to Zoom Phone:

The manipulation performs the following modifications to SIP packets

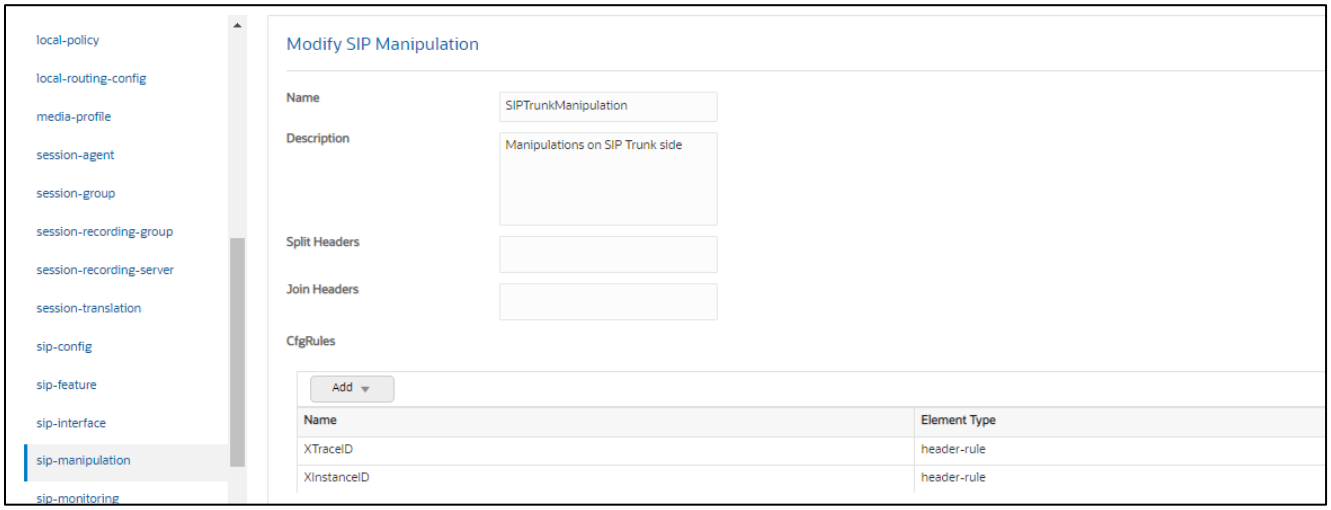
1. Changes the host portion of From address with the SBC sip-interface IP Address.
2. Changes the host portion of To Header with Zoom IP Address.




### 6.8.1.2 Manipulation towards Carrier Side.

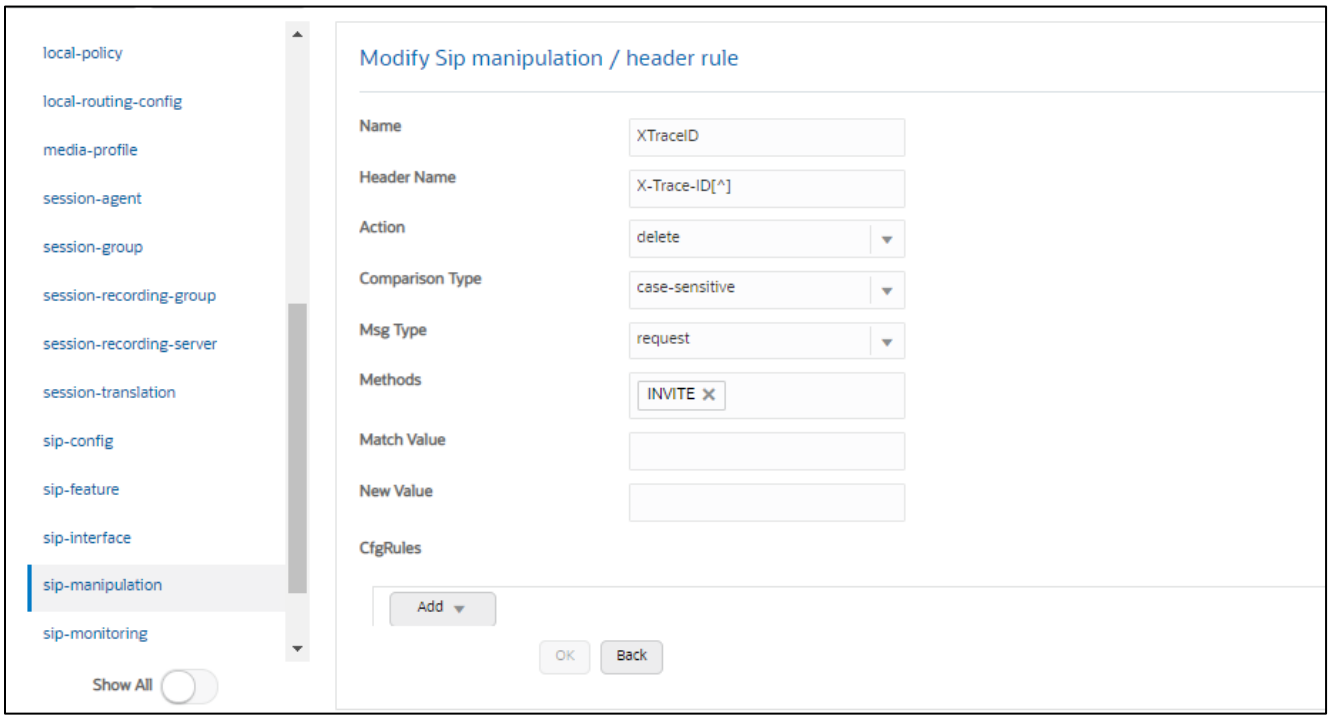
The following SIP manipulation is applied as the out-manipulationId on the Session-Agent created for the Carrier Trunk. This manipulation modifies packets generated by the Oracle SBC to Carrier Side as stated below:

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.

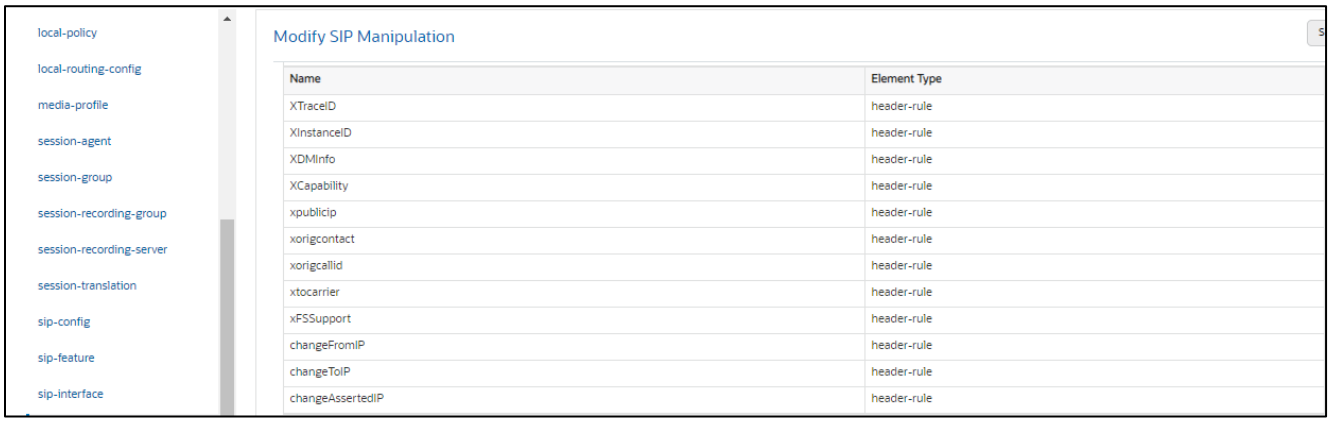



**Header-Rules**

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.



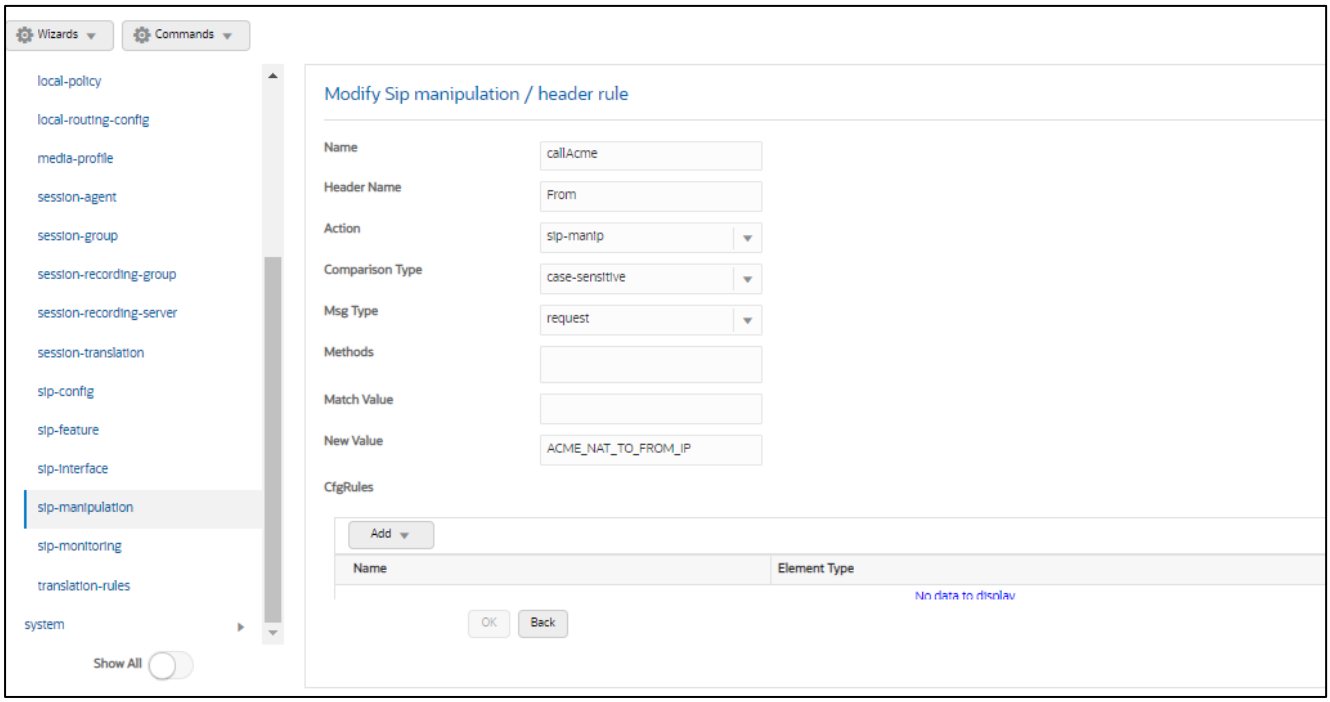

Similar Header-rules are created to remove the other X headers which are inserted by Zoom on the Sip Signaling.




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

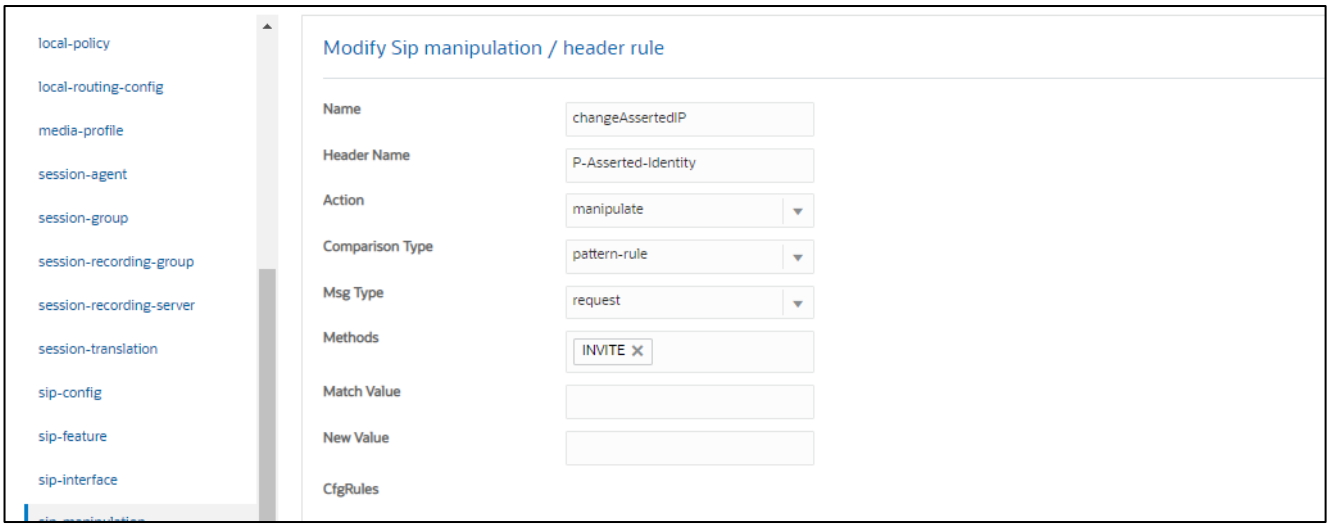
1. Changes the host portion of From Header with the Local SBC IP Address.
2. Changes the host portion of To Header with Carrier side IP Address
3. Changes the host portion of P Asserted Identity with Carrier side IP Address.

**Header-rule**

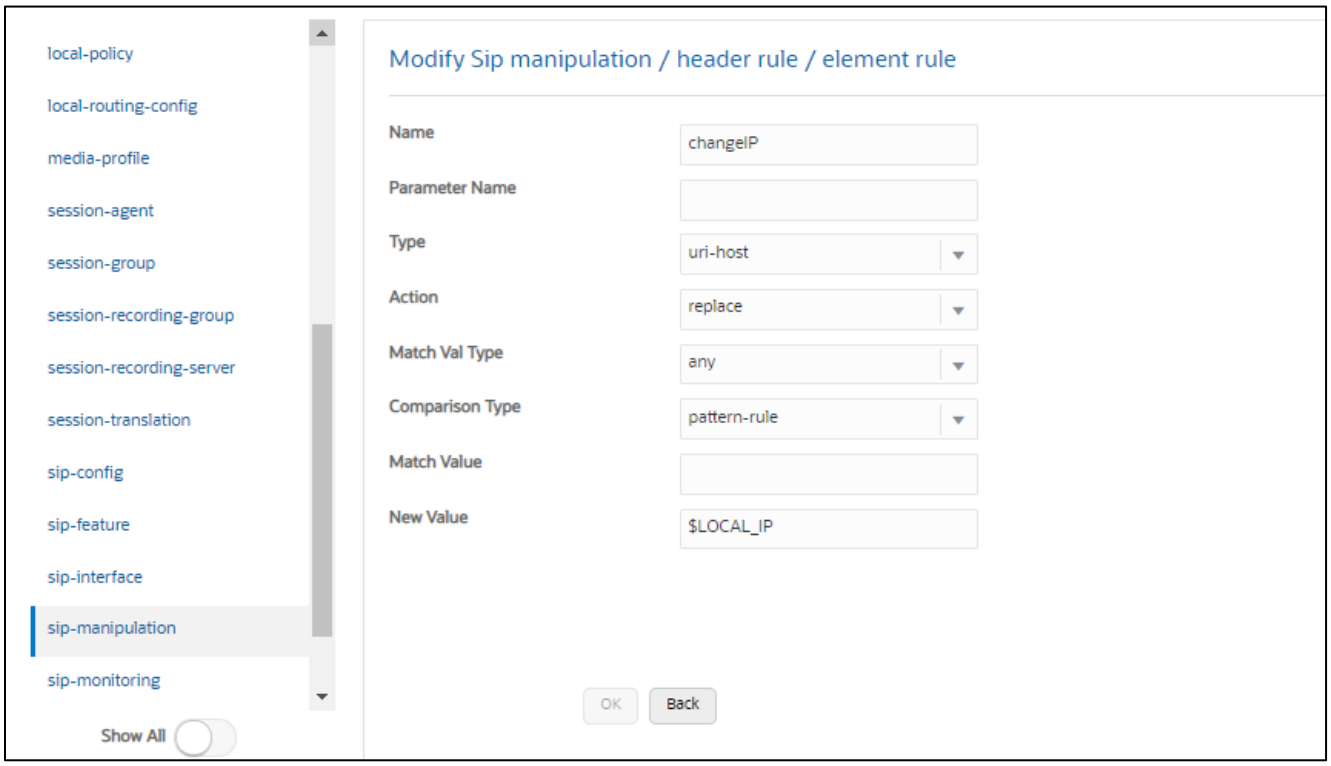



Below Portion of the HMR Changes the Host portion of P-Asserted Identity with Carrier side IP Address.

**Header-rule**

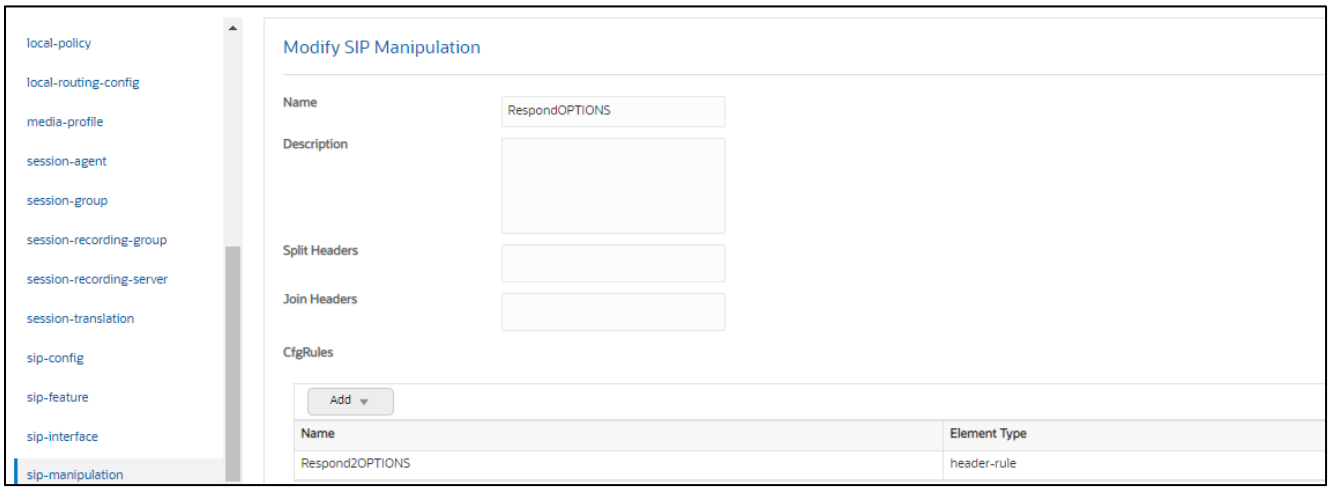



**Element Rule**

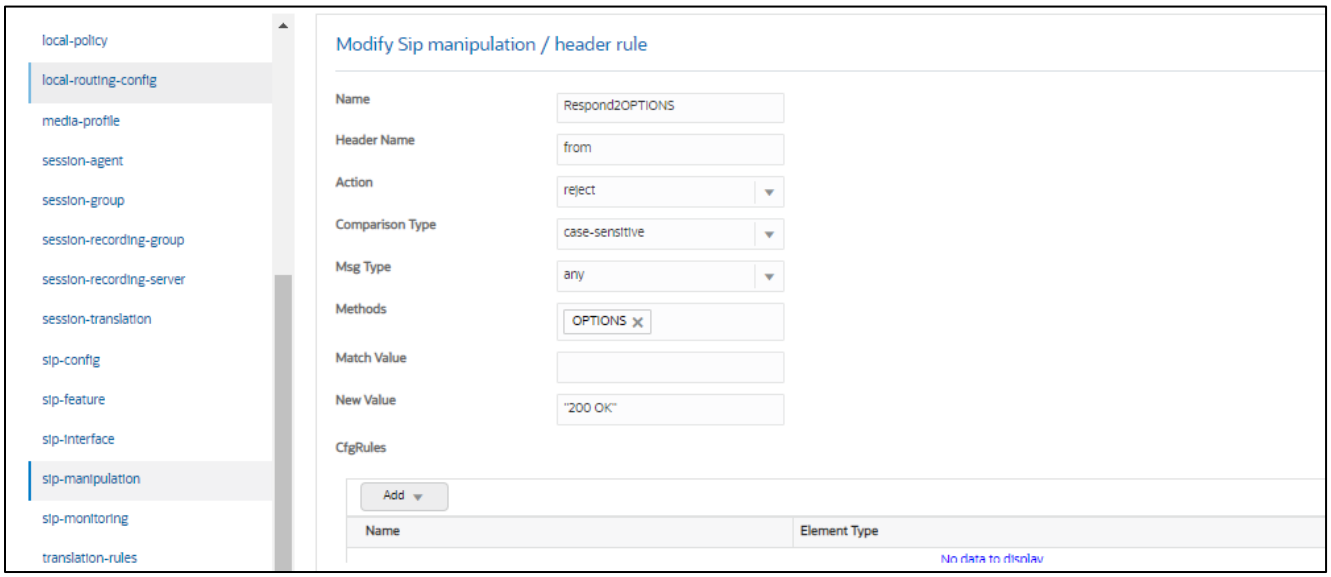



### 6.8.1.3 Manipulation for OPTIONS Ping.

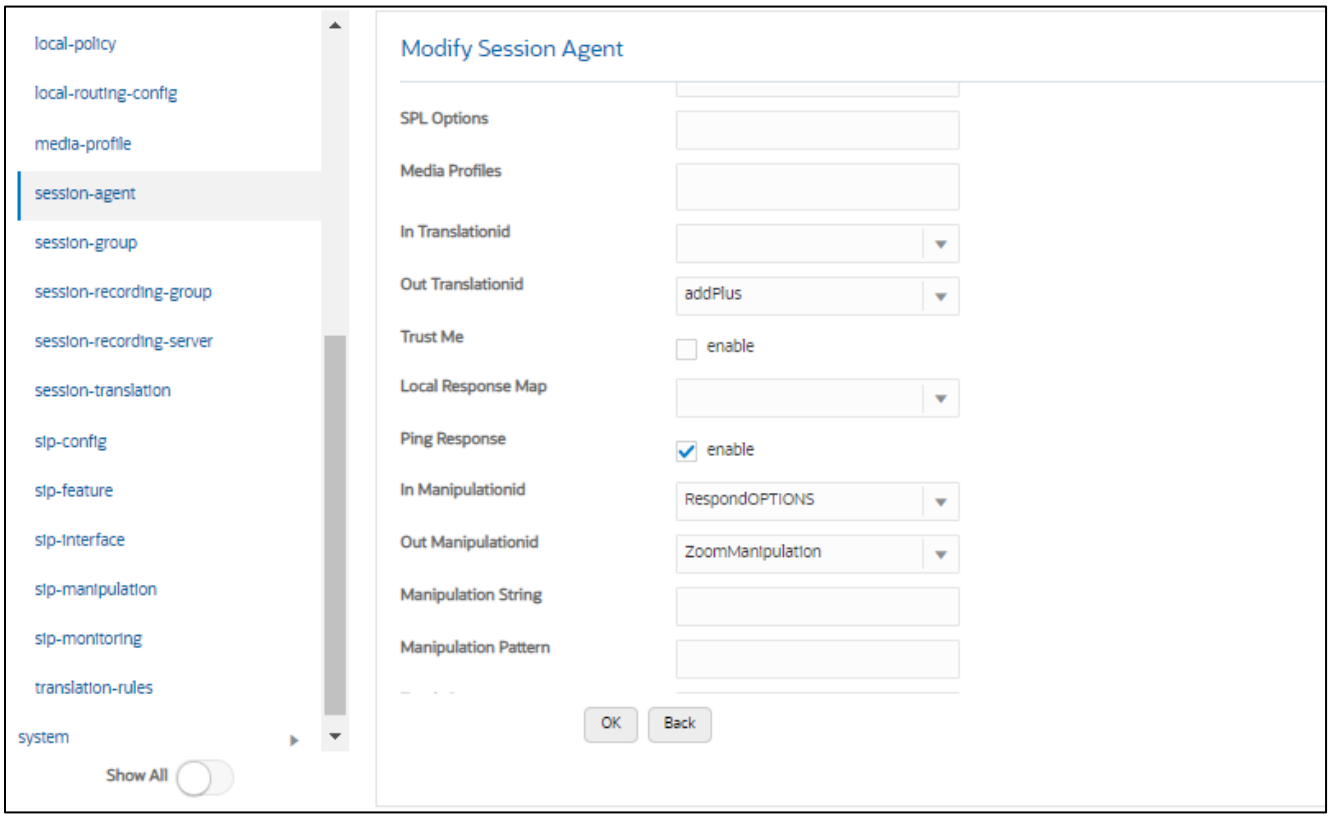
The following SIP manipulation can be applied as the in-manipulationId to be applied to Options Requests generated by Zoom to the SBC. This will allow the SBC to respond locally to Options Requests.




**Header Rule:**

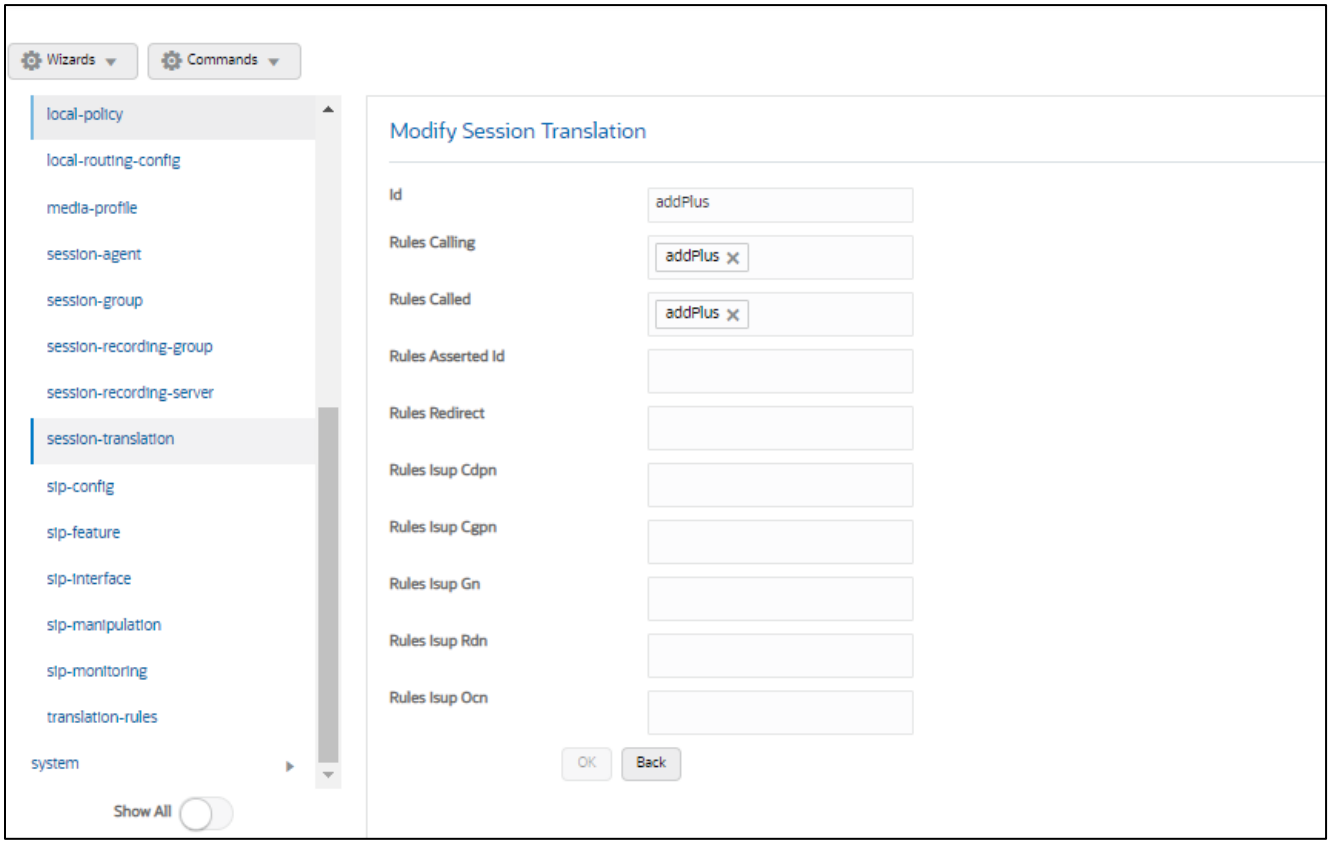


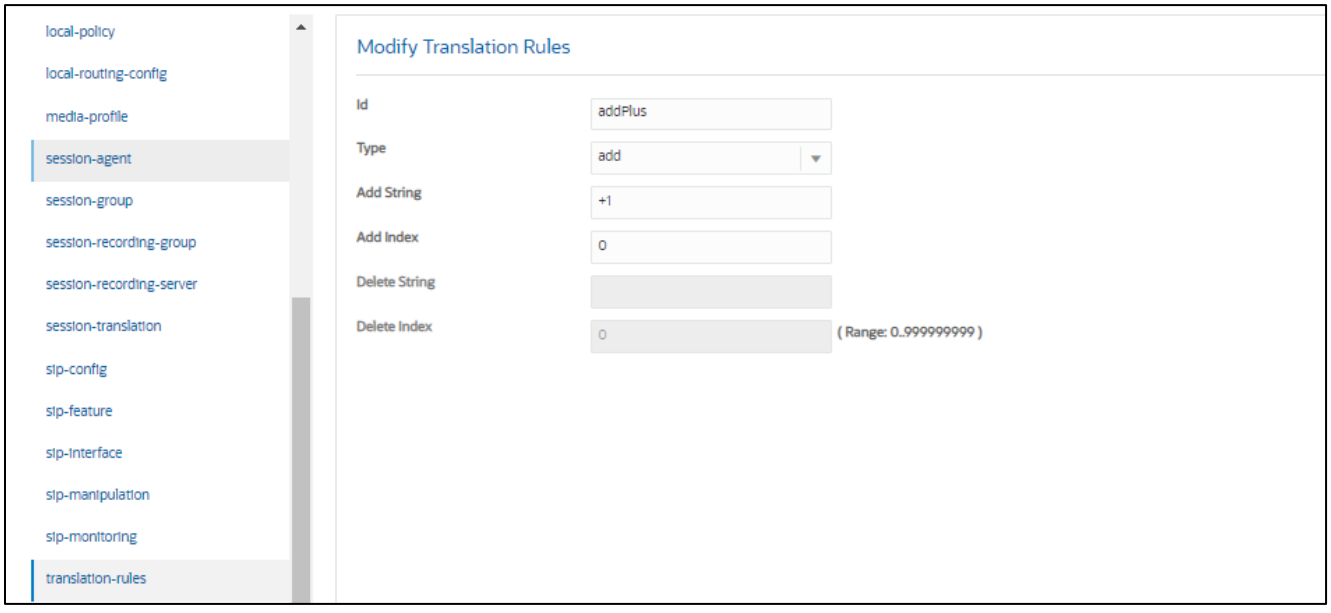

*Please note, if running release SCZ830m1p7 or later, there is a new configuration parameters on the Session Agent Config element, called ping-response. When enabled on each agent, it will take that place of the following SIP-Manipulation.*



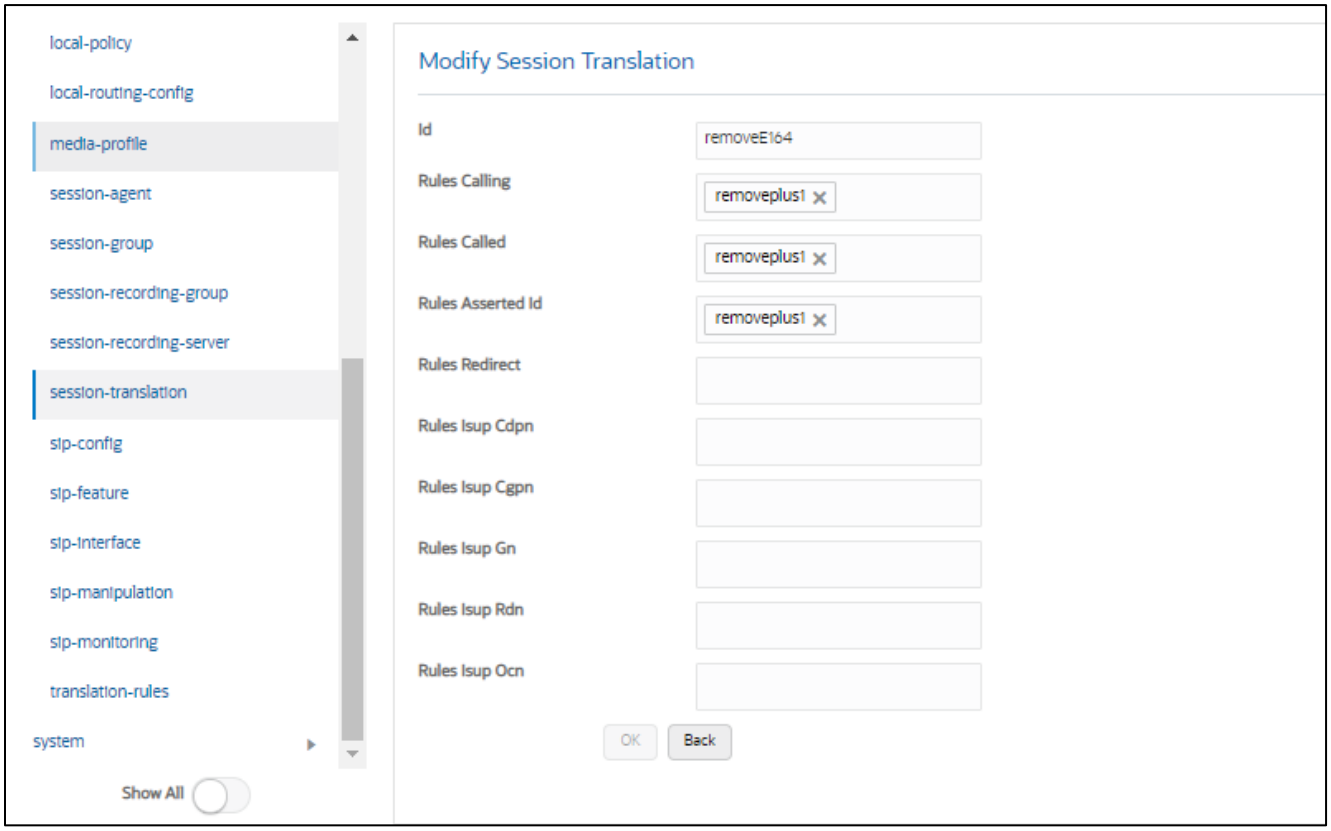

## 6.9 Session-Translation

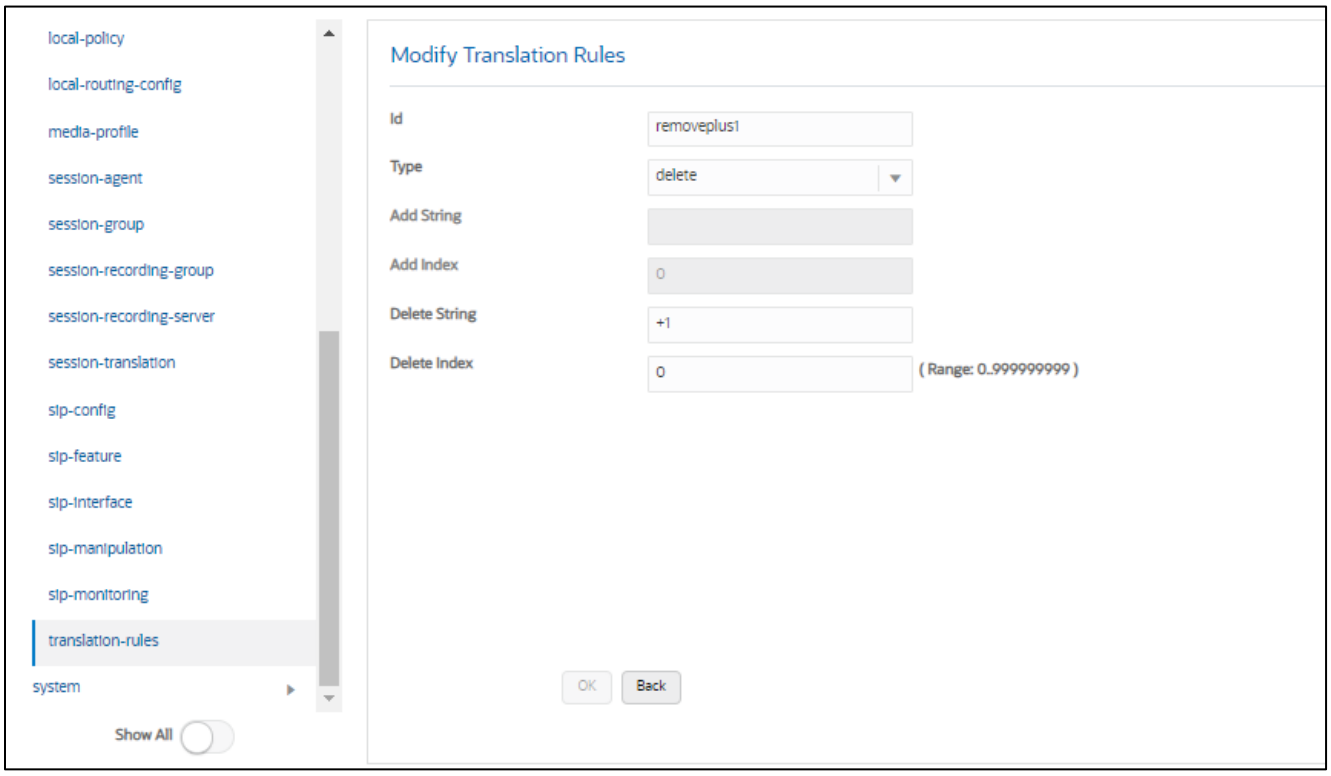
The following session-translation is created and applied as out-translationid on the Session-Agent towards Zoom. This session-translation is created to add a +1 when call is sent towards Zoom as Zoom requires calls to be presented in E.164 format.



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.






### 6.9.1 Session Timer Profile (Optional)

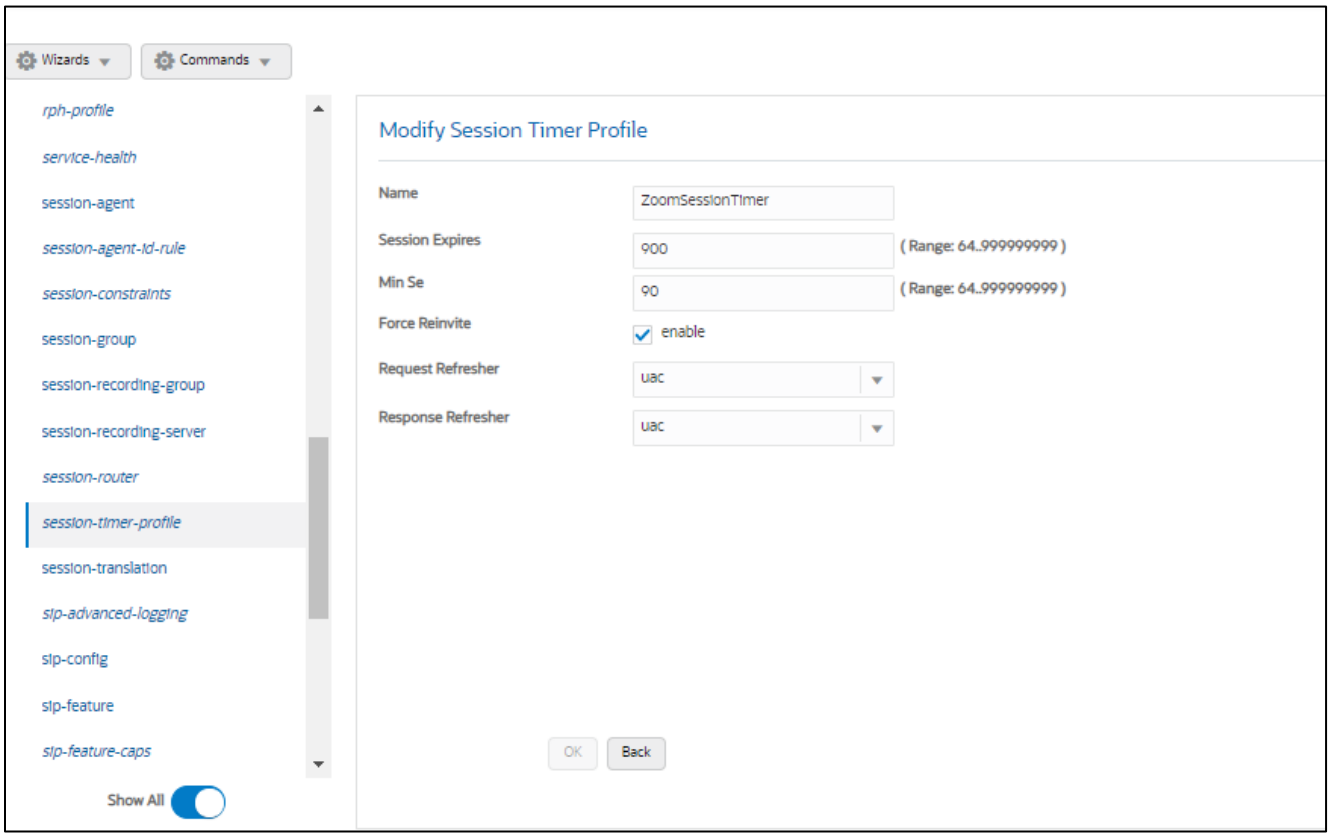
Zoom Phone does support RFC 4028 Session Timers In SIP. In many cases, RFC 4028 is not supported by carriers providing SIP trunking services to their customers. In order to accommodate this, the SBC will interwork between PSTN carrier and Zoom Phone in order to provide support for Session Timers in SIP.

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.




### 6.9.2 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:

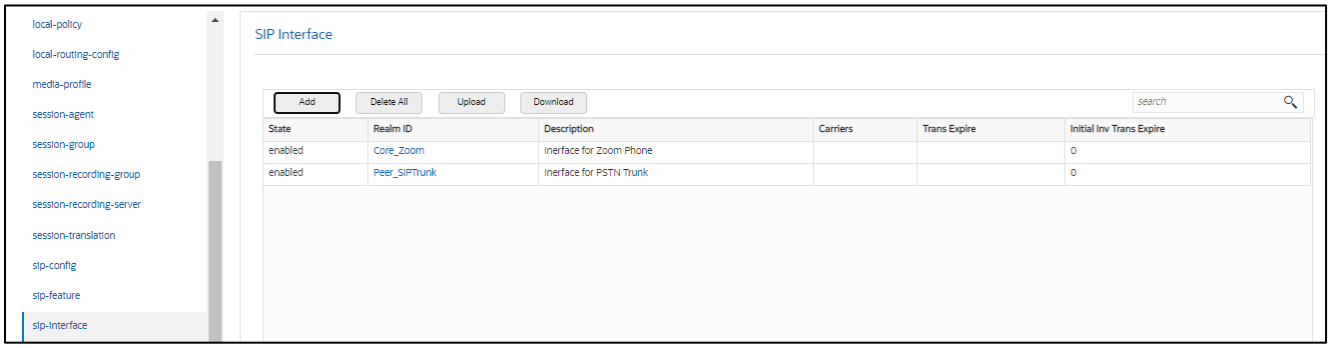
Please note, this is also where we will be assigned some of the configuration elements configured earlier in this document, ie….

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

Use the following as an example to configure SIP interfaces:

| Config Parameter | SIPTrunk | Zoom |
|---|---|---|
| Realm ID | Peer_SIPTrunk | Core_Zoom |
| Out manipulationid | | ACME_NAT_TO_FROM_IP |

| | | |
|---|---|---|
| In manipulationid | | RespondOPTIONS |
| **SIP Port Config Parmeter** | **SIP Trunk** | **Zoom** |
| 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 |




### 6.9.3 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 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

### 6.9.4 Session Agent Group

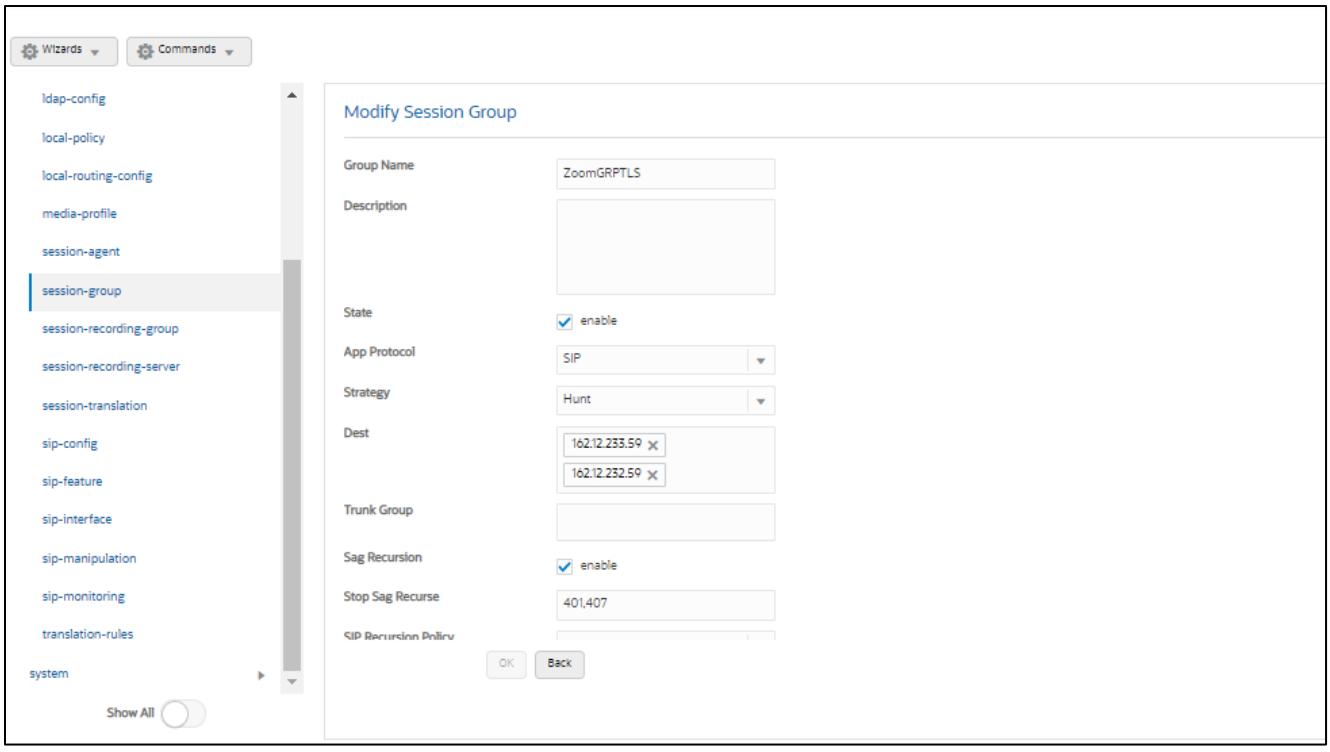
A session agent group allows the SBC to create a load balancing model:

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

### 6.9.5 Routing Configuration

This section outlines how to configure the ORACLE SBC 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.

### 6.9.6 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.

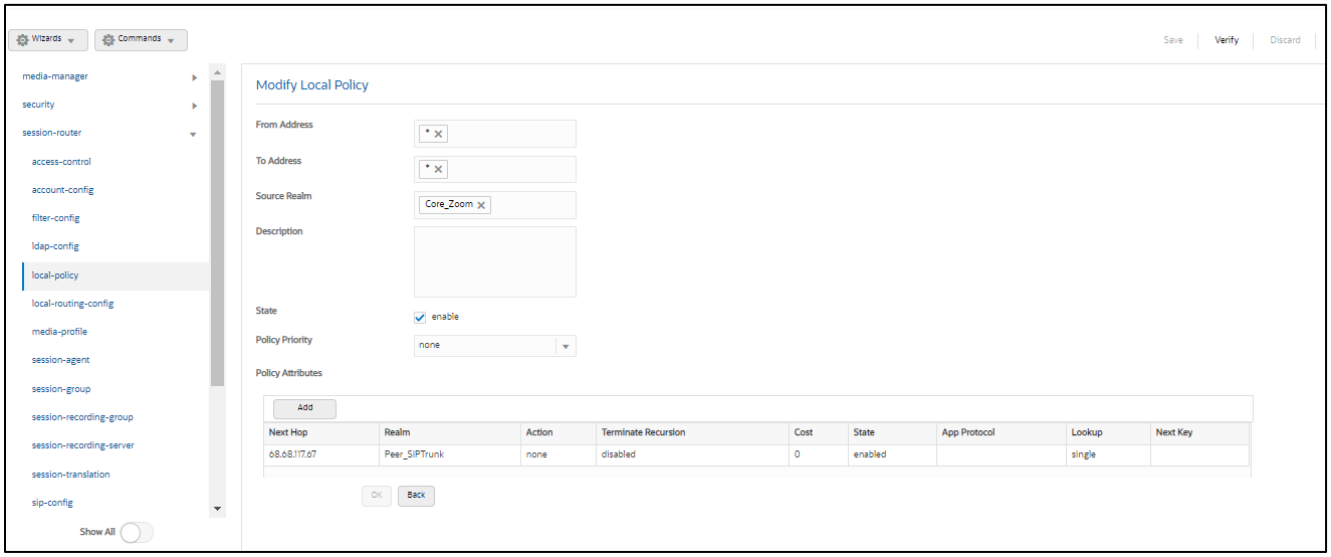
GUI Path: session-router/local-policy

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

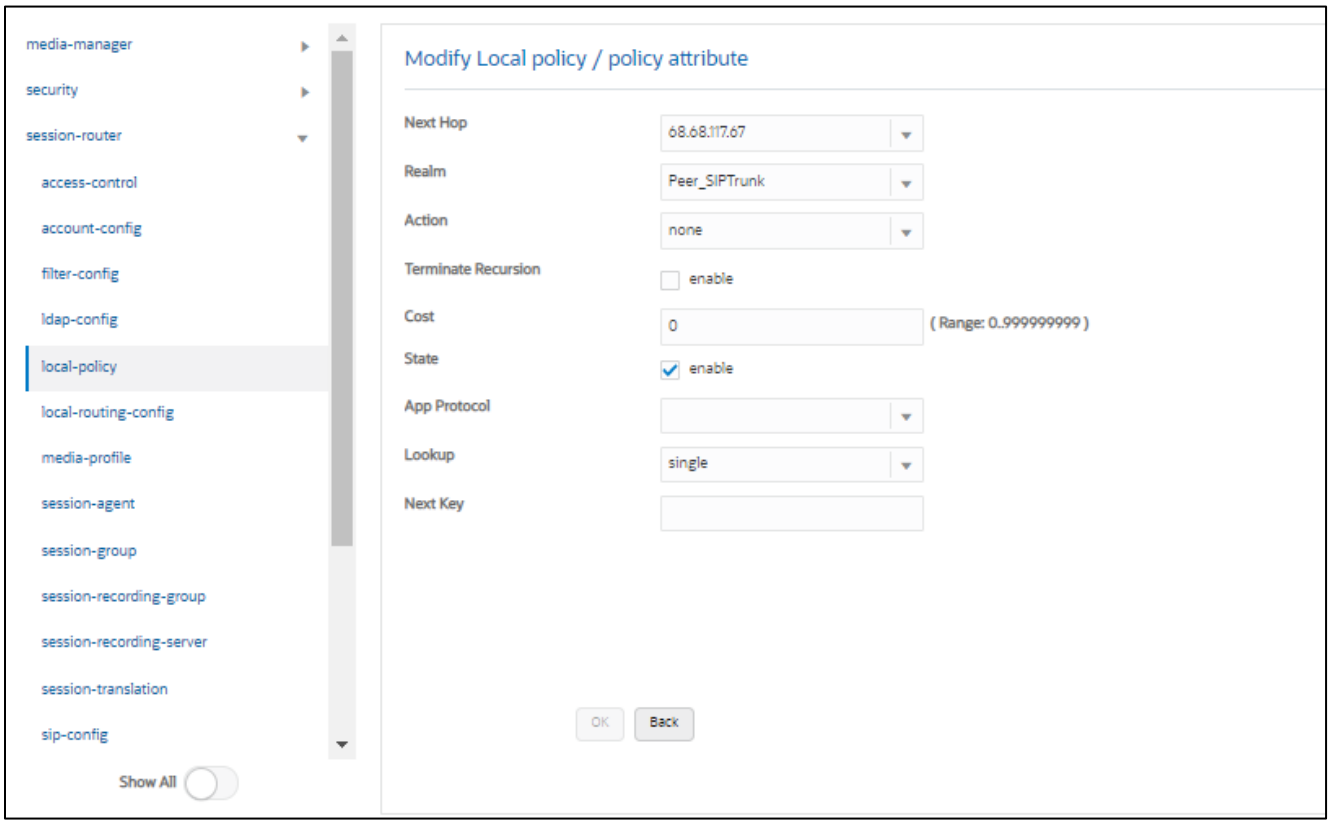
In order to route SIP traffic to and from Zoom Phone Platform, the following local-policies will need to be configured.

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

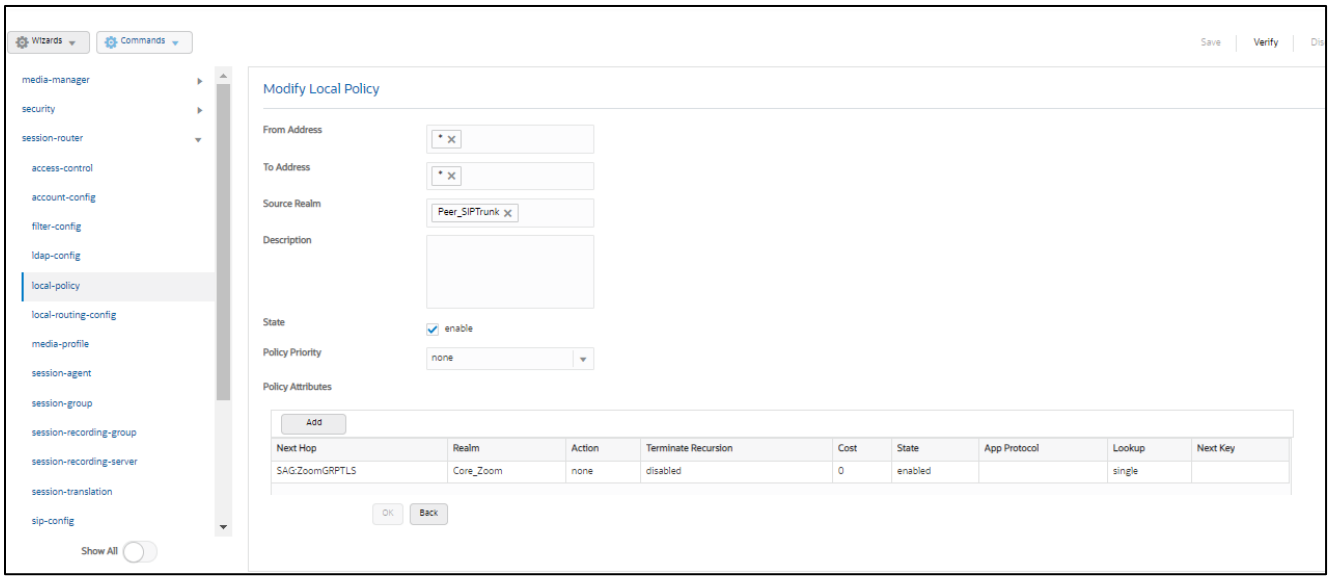
**Route Calls from Zoom To PSTN:**



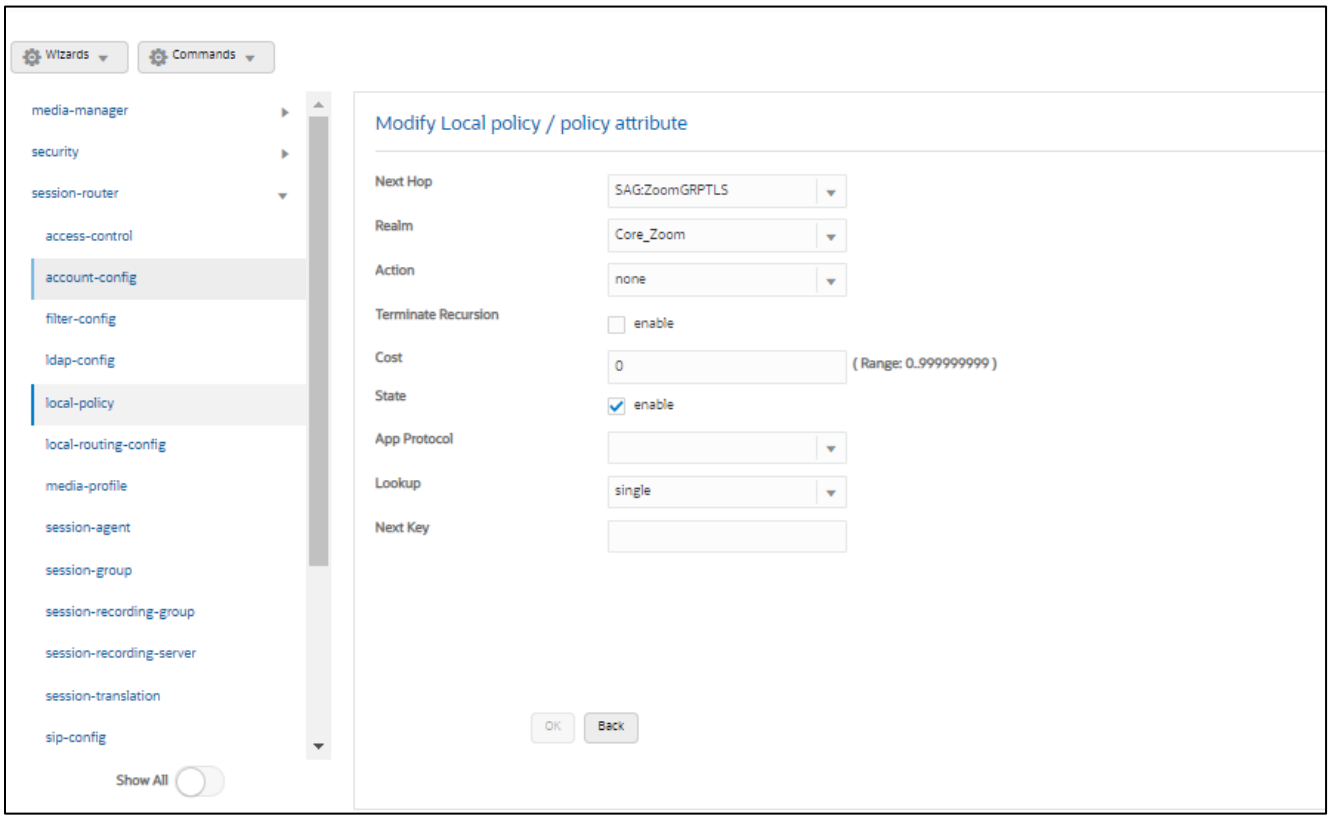

**Policy Attribute:**




**Calls from PSTN To Zoom:**




**Policy Attribute:**




- Click OK at the bottom of each when applicable.

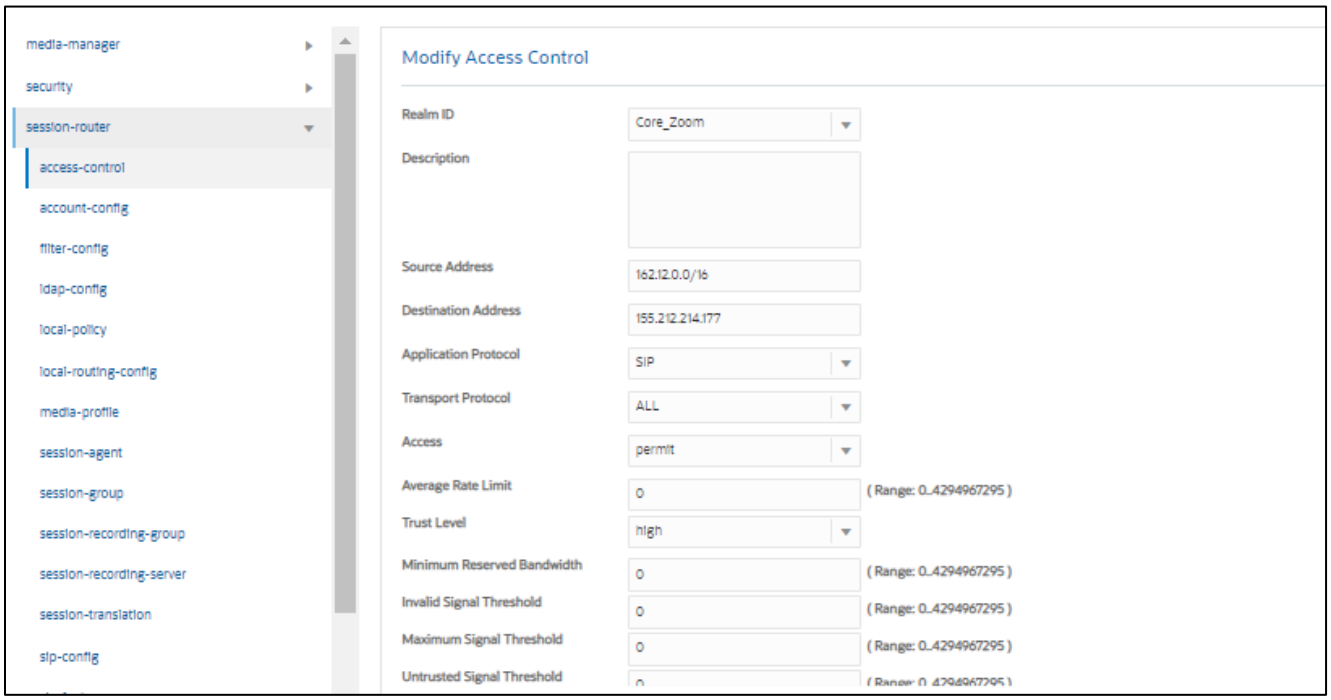
### 6.9.7 Access Controls

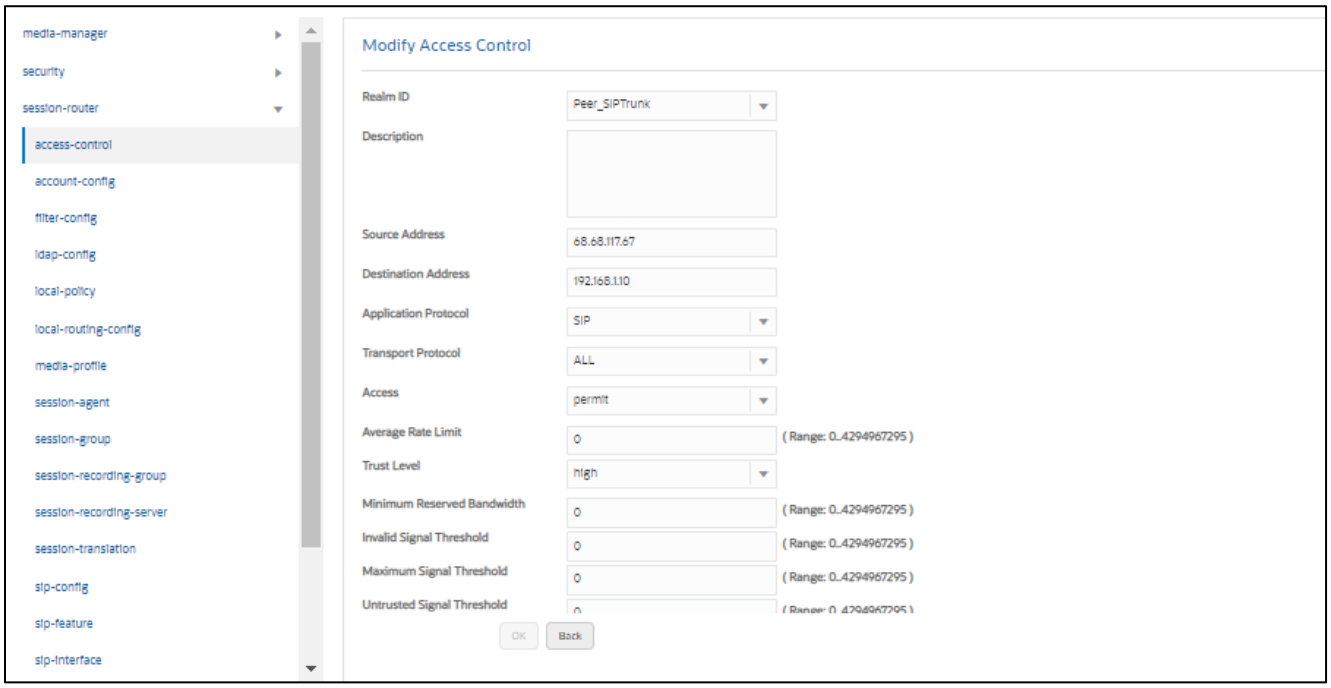
To enhance the security of your Oracle Session Border Controller, we recommend configuration access controls to limit traffic to only trusted IP addresses on all public facing interfaces

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

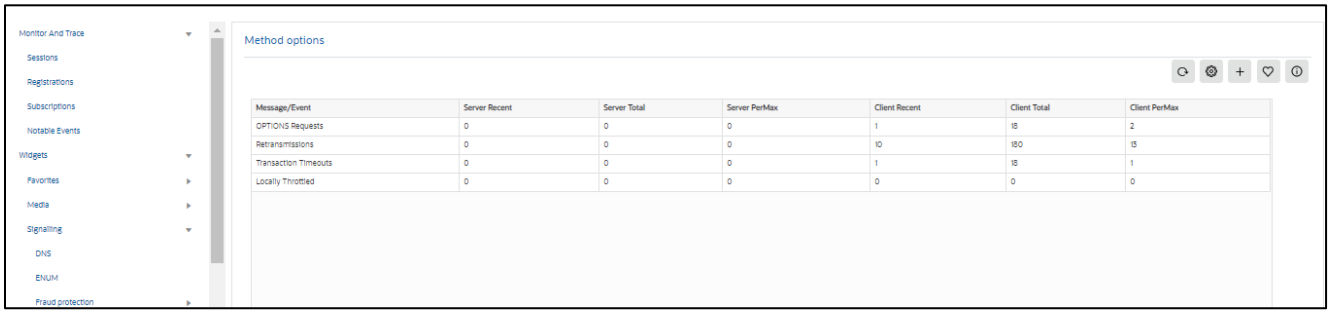
After you've paired the ORACLE SBC with Zoom, validate that the SBC can successfully exchange SIP Options with Zoom Cloud Voice.

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 Appendix A

## 8.1 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.

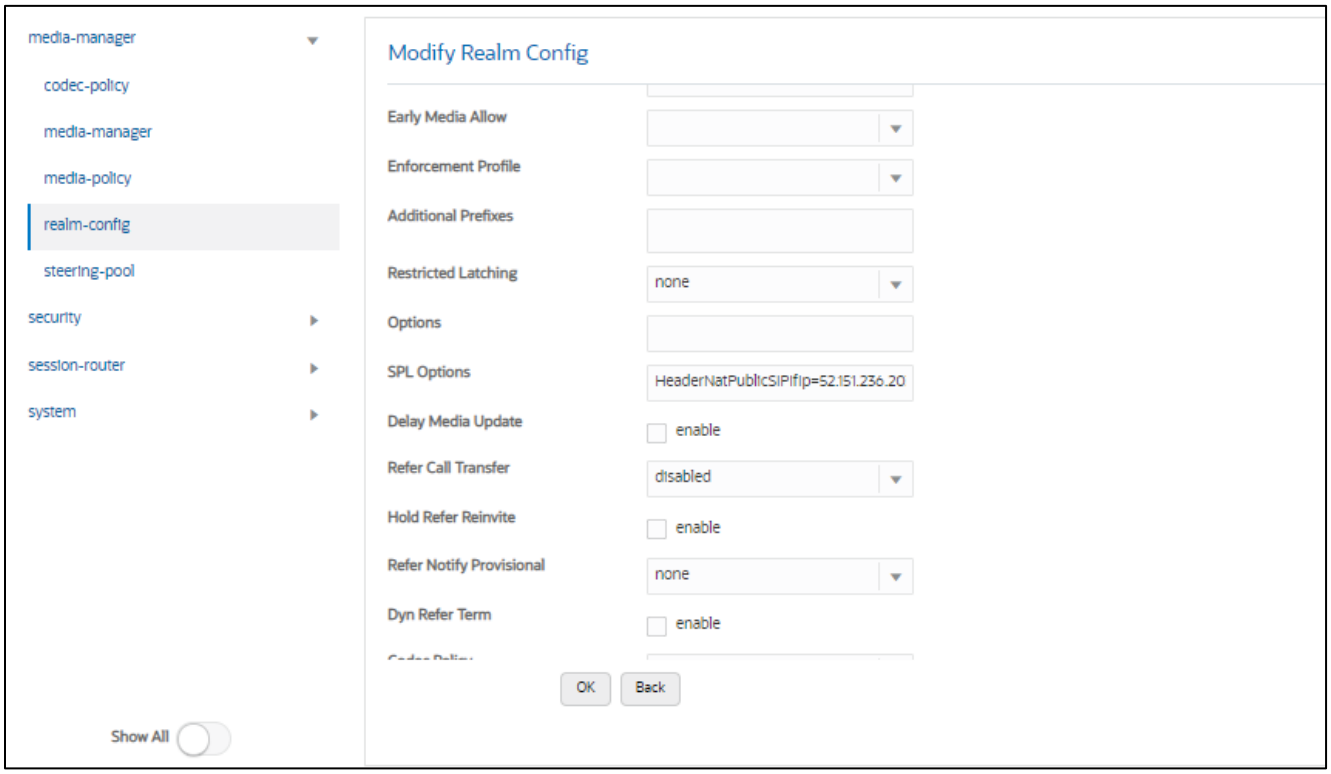
- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

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 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.

# 10 Configuring the Oracle SBC through Config Assistant.

When you first log on to the Oracle SBC, the system requires you to set the configuration parameters necessary for basic operation. To help you set the initial configuration with minimal effort, the SBC provides the Configuration Assistant.
The Configuration Assistant, which you can run from the Web GUI or the Acme Command Line Interface (ACLI), asks you questions and uses your answers to set parameters for managing and securing call traffic. You can use the Configuration Assistant for the initial set up to make to the basic configuration. Please check "Configuration Assistant Operations" in the Web GUI User Guide and "Configuration Assistant Workflow and Checklist" in the ACLI Configuration Guide

Please note, applying a configuration to the SBC via the Configuration Assistant will overwrite any existing configuration currently applied to the SBC. **We highly recommend this only be used for initial setup of the SBC. This feature is not recommended to be used to make changes to existing configurations.**

Configuration package is available starting in release nnSCZ840p7 and nnSCZ900p2.

## 10.1 Section Overview and Requirements

This section describes how to use our Configuration Assistant feature as a quick and simple way to configure the Oracle SBC for integration with Zoom BYOC and a generic PSTN Trunk.

The pre-requisites are given below.

- SBC running release SCZ840p7 or later which will have this template package by default added to the SBC code.
- TLS certificate for the SBC preferably in PKCS format, or access to Zoom supported CA to sign certificate once CSR is generated by the SBC.

The following outline assumes you have established initial access to the SBC via console and completed the following steps:

- Configured boot parameters for management access
- Setup Product
- Set Entitlements
- Configured HTTP-Server to establish access to SBC GUI

## 10.2 Initial GUI Access

The Oracle SBC WebGui can be accessed by entering the following in your web browser.

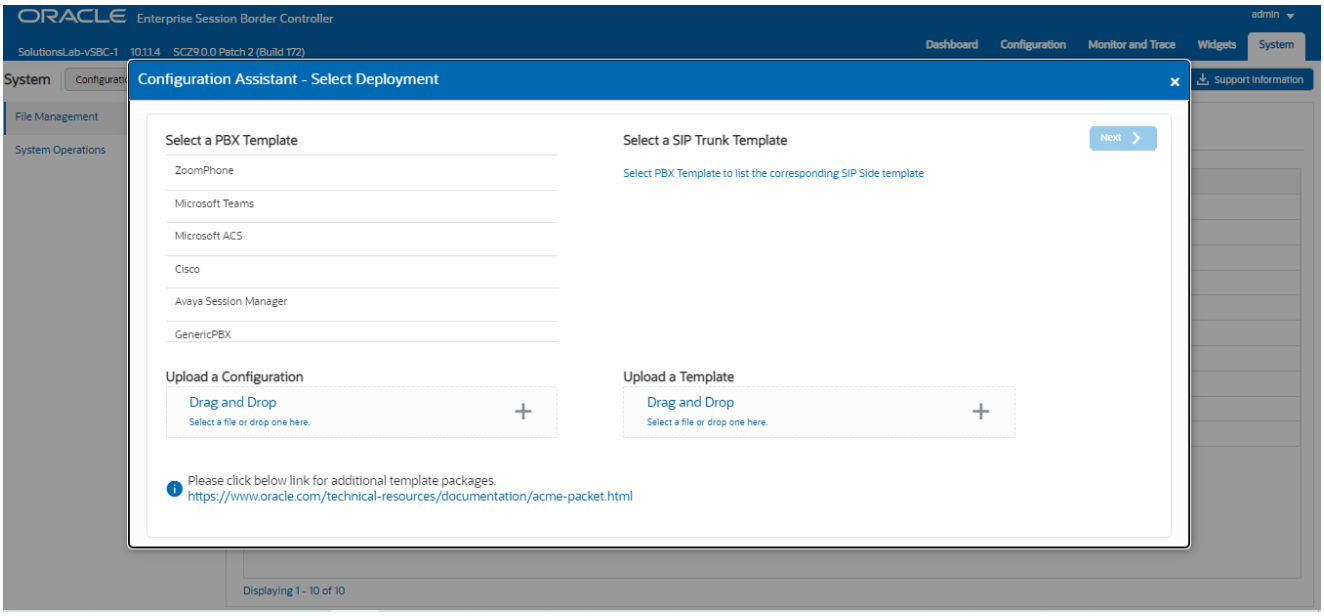
http(s)://<SBC Management IP>.

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

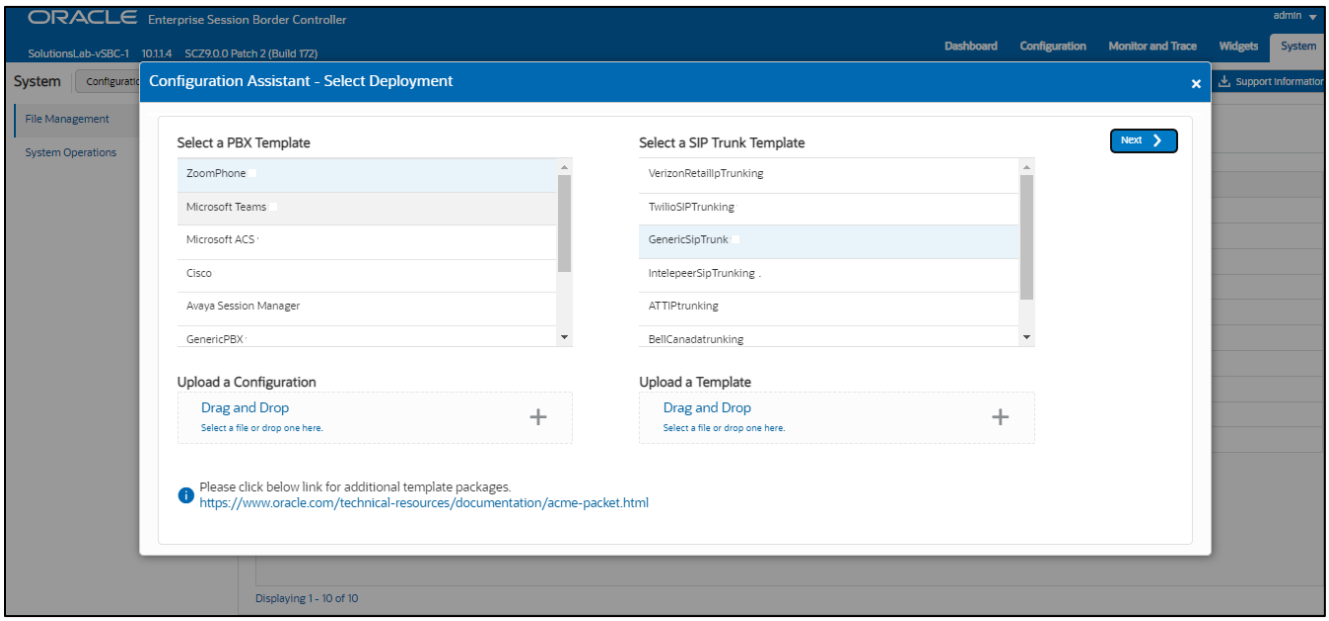
If there is no configuration on the SBC, the configuration assistant will show immediately upon login to the SBC GUI as shown below

## 10.3 Zoom Phone Configuration Assistant

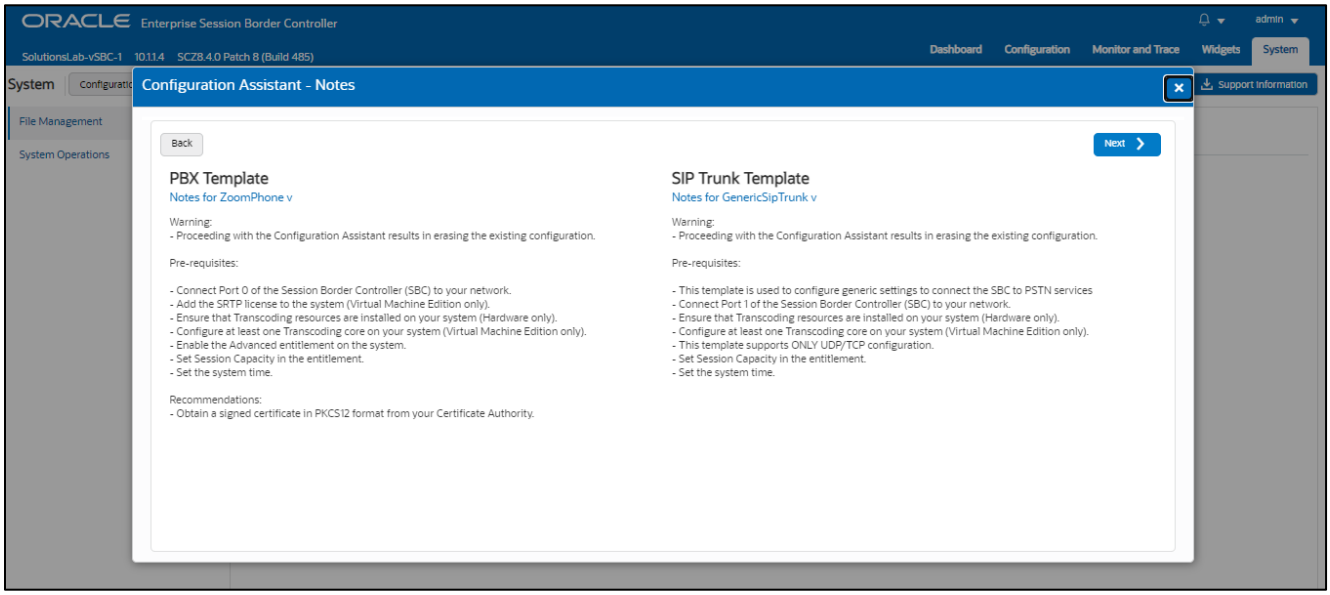
For a new SBC deployment, once access to the GUI is configured, you will see the following when logging in for the first time:




Under PBX template, we'll select ZoomPhone template. This brings up a list of available sip trunk templates.



Select a sip trunk template and click Next at the top to access the Notes page.Pay close attention to the information here, as this is a list of warnings, pre-requisites, and recommendations:



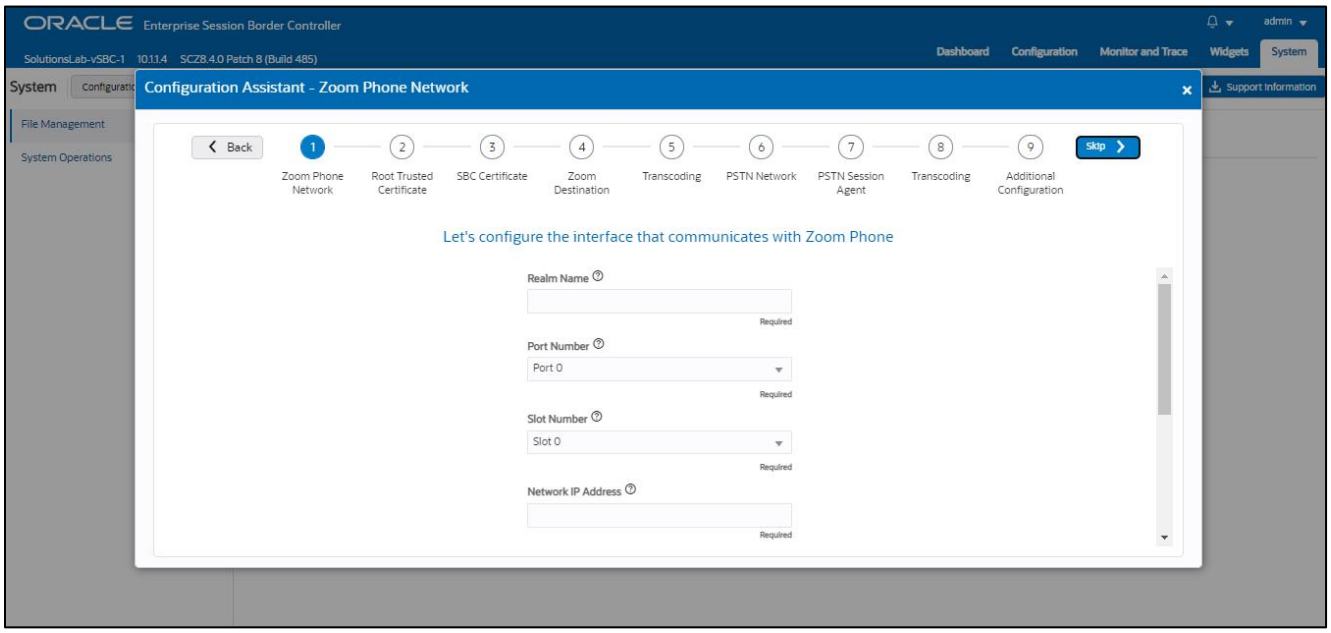

Clicking “Next” on the Notes page triggers the configuration assistant to do a system check. This ensures that all of the system requirements for the platform and sip trunk you have selected have been met before proceeding to configuration pages. If they have not been met, you will be greeted by a page providing the opportunity to setup entitlements, add license keys, etc. before moving on to the configuration.

Once all requirements for your selected templates have been satisfied, you can proceed to the configuration pages.

### 10.4 Page 1- Zoom Phone Network

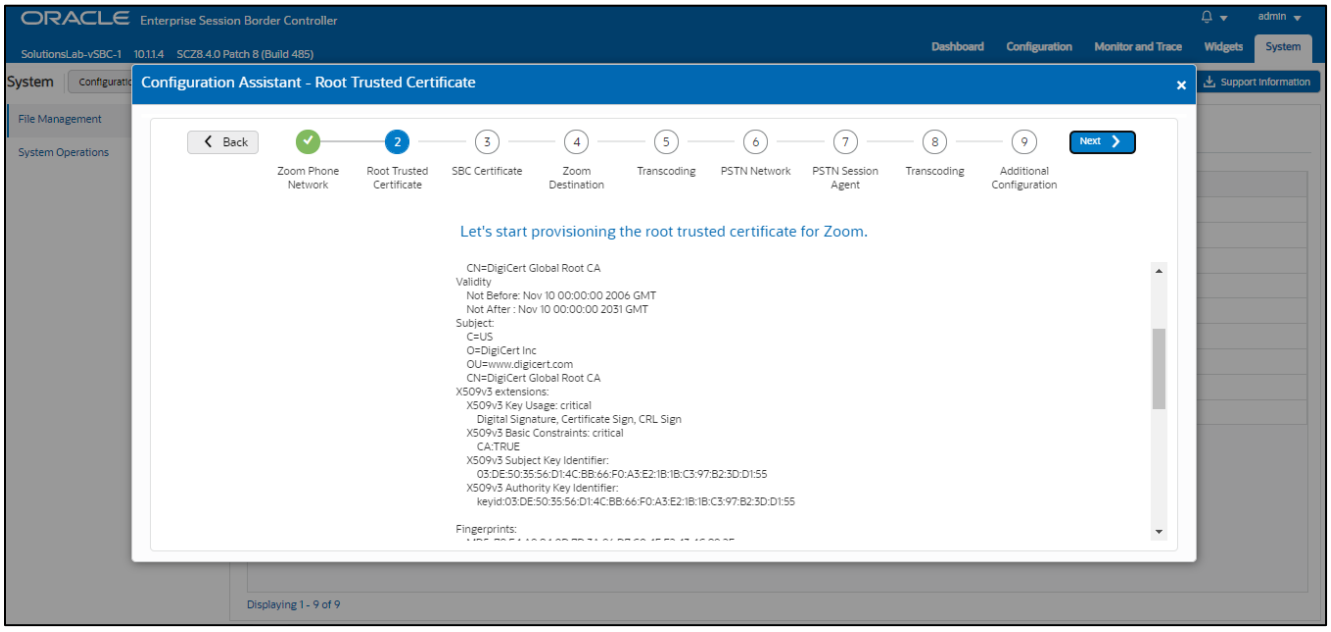
Page 1 of the template is where you will configure the network information to connect to Zoom Network.

Next to each field is a help icon. If you hover over the icon, you will be provided with a description or definition of each filed. Also, pay close attention to which fields are listed as “required”.



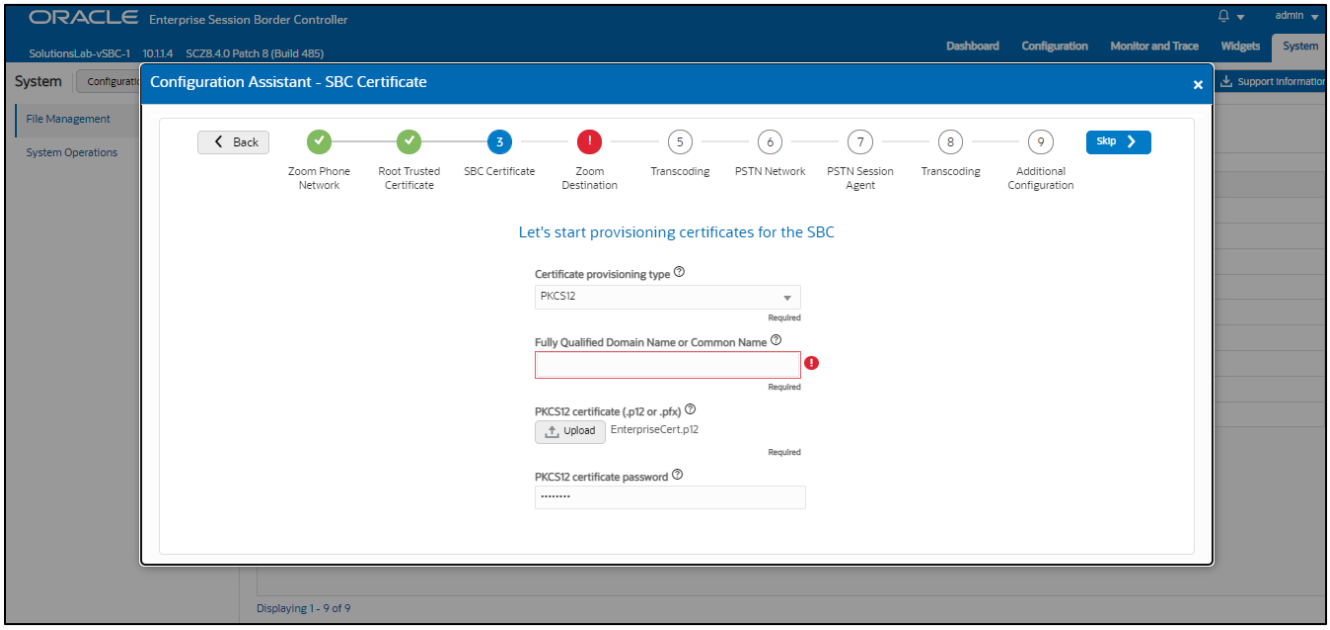

## 10.5 Page 2 - Import DigiCert Trusted CA Certificate for Zoom

Page 2 of this template is where the SBC will import the **DigiCertRoot CA** certificate, which Zoom uses to sign the certificates it presents to the SBC during the TLS handshake. Importing the Zoom Root CA certs is enabled by default.



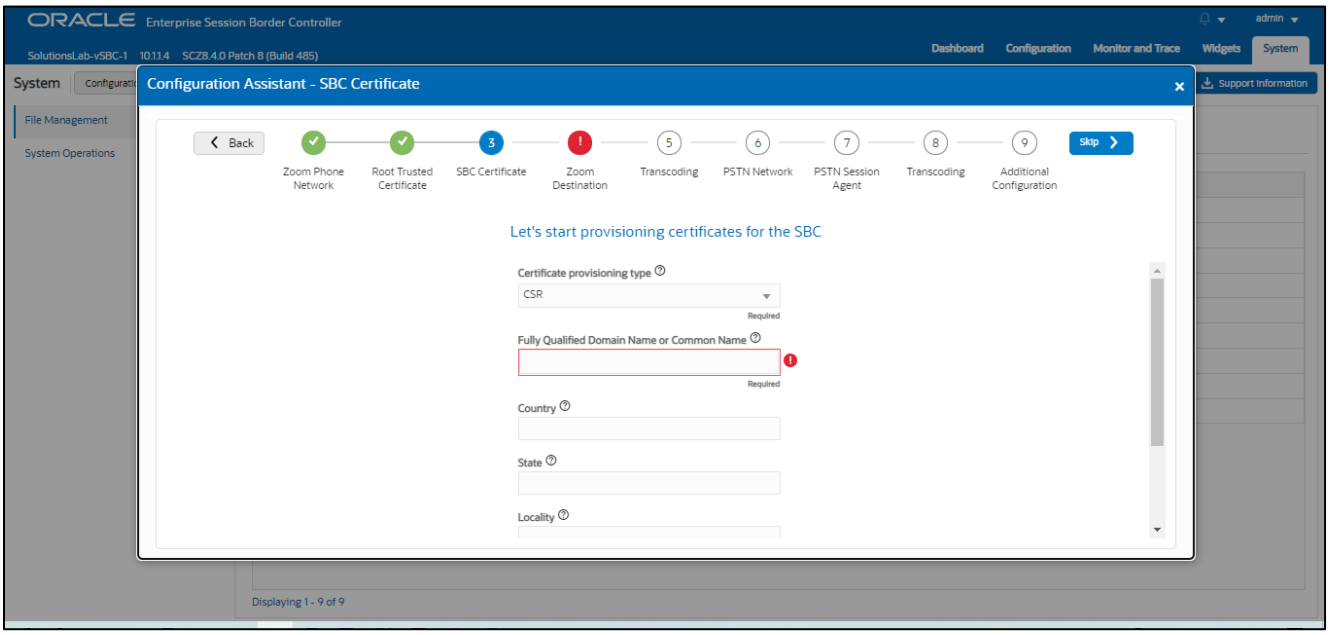

## 10.6 Page 3 - SBC Certificates for Zoom side

By default, the SBC is set to import a certificate in PKCS12 format. This is the simplest and recommended way to add a certificate to the Oracle SBC. Using this method, you will add the SBC's hostname under "FQDN or Common Name" field, upload a certificate signed from one of the Zoom Supported CA Vendors, and enter the certificates password.



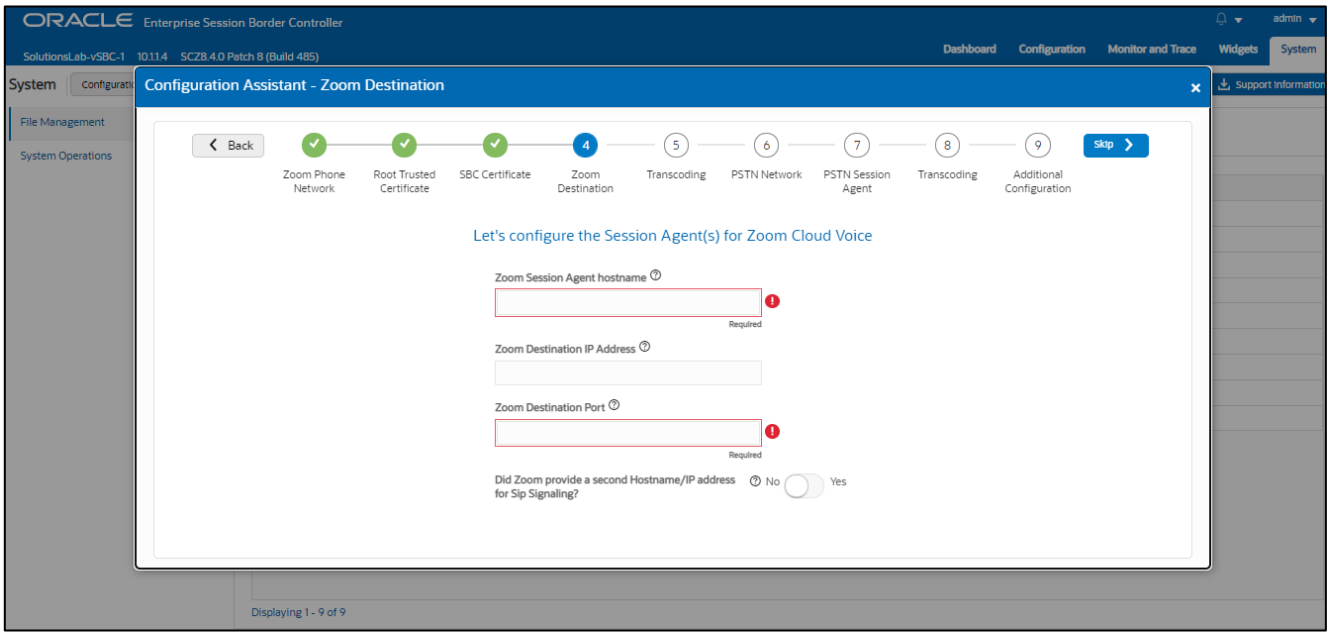

### 10.6.1.1 Certificate Signing Request (CSR)

The alternative to importing a PKCS12 certificate to the SBC is to configure a certificate and generate a certificate signing request that you will have signed by a Zoom supported CA. Same as PKCS12, you will enter the SBC's hostname under "FQDN or Common Name" and "Country" field (required) and answer the remaining question presented on this page (optional).




## 10.7 Page 4 - Zoom Destination

Page 4 of the template is where you will configure the Zoom Session Agent details where you will enter the next hop IP address and port for sip signaling to and from your Zoom Phone Network. Please fill the required fields and click Next.

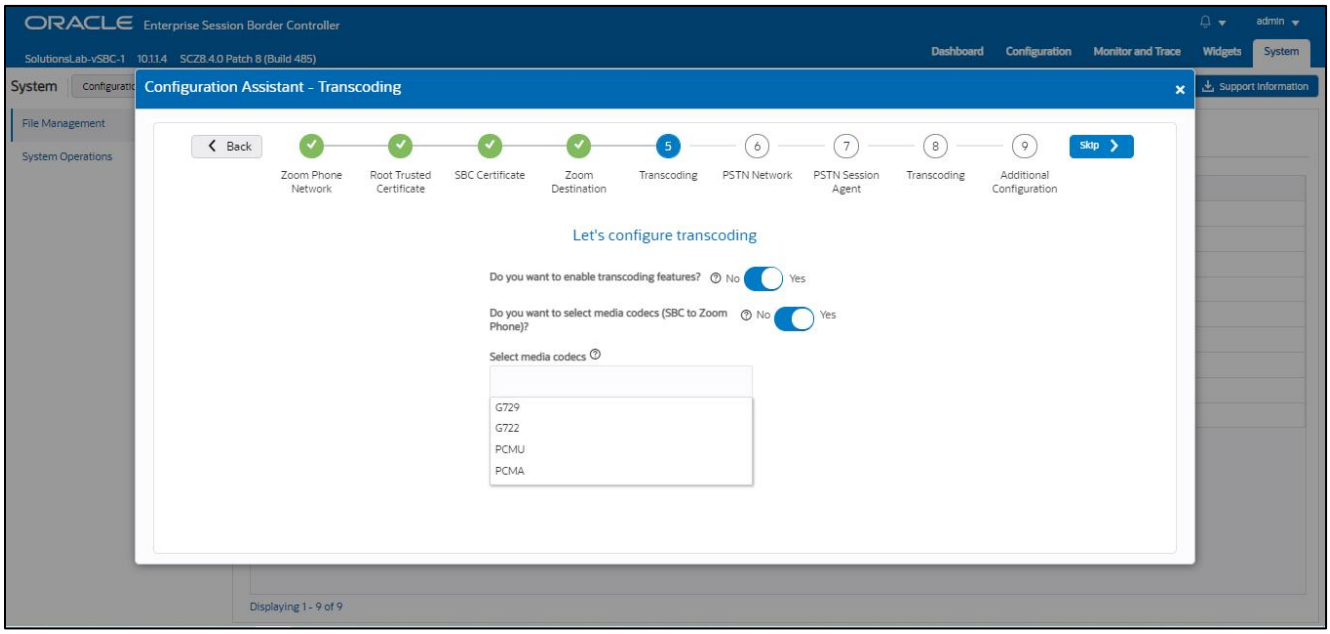



## 10.8 Page 5 - Zoom side Transcoding

Page 5 is where you will be able to configure transcoding between the SBC and Zoom.

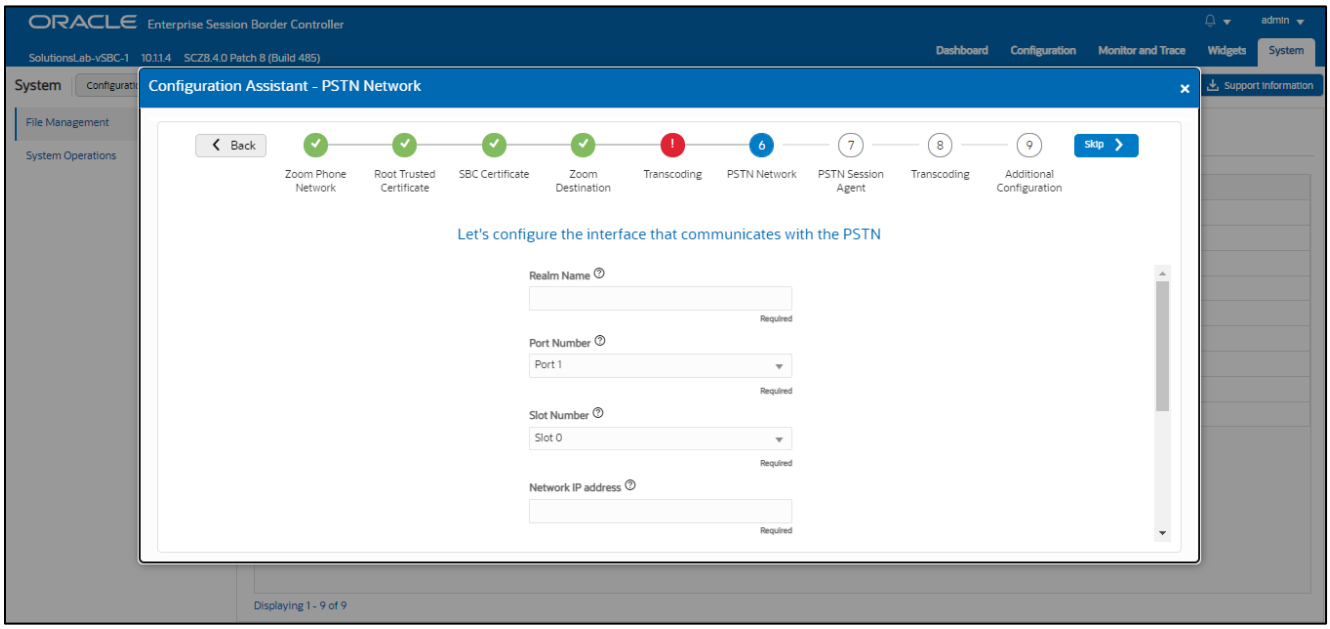
Once transcoding features is set to “yes”, you will then have an option to select additional media codecs you want included in offers/answers toward Zoom. If you select yes to either question regarding media codecs, you will be presented with a required drop down.

You can select as many codecs from the list presented.




## 10.9 Page 6 – PSTN Sip Trunk Network

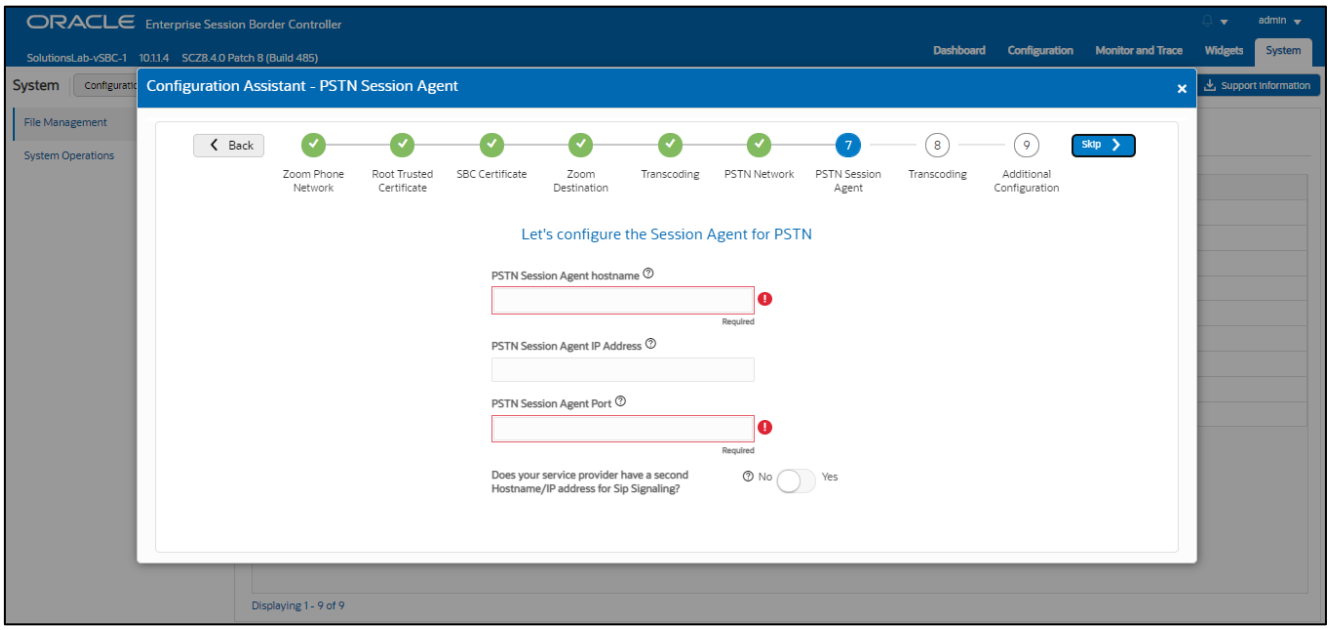
Page 6 of the template is where you will configure the network information to connect to PSTN SIP trunk Network. Please fill the required fields and Press Next.



## 10.10 Page 7 – PSTN Session Agent

Page 7 of the template is where you will configure the PSTN Session Agent details where you will enter the next hop IP address and port for sip signaling to and from your PSTN SIP trunk.

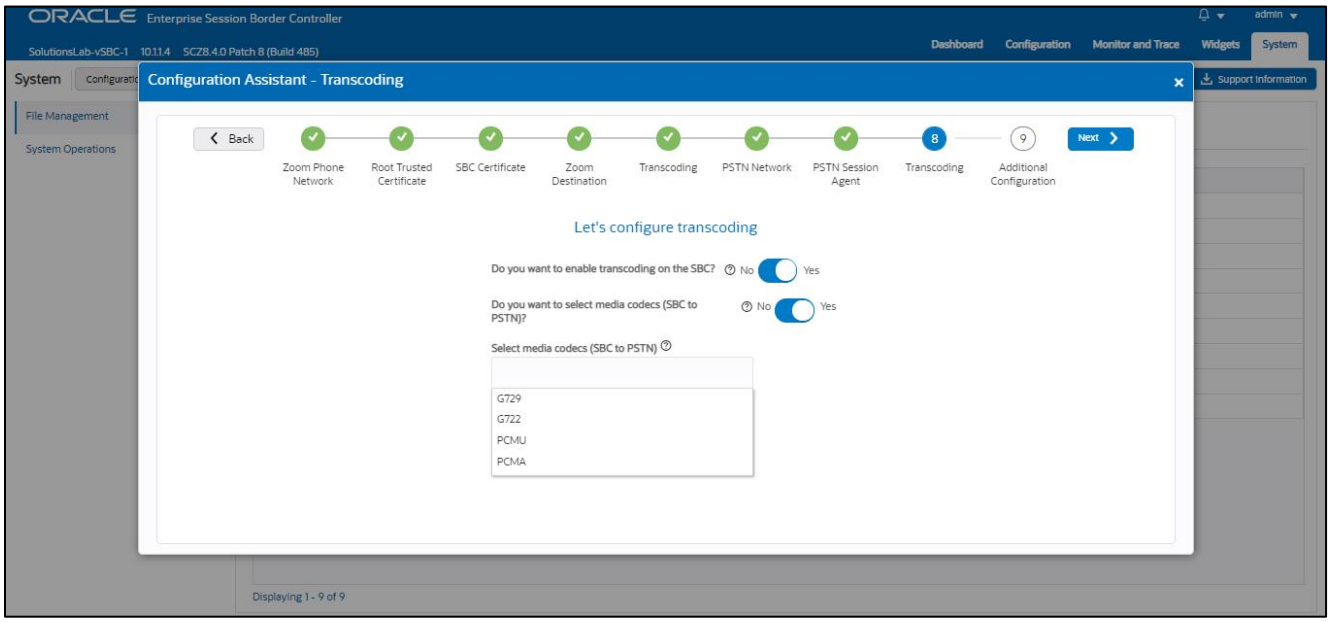
Please fill the required fields and click Next.




## 10.11 Page 8 - PSTN side Transcoding

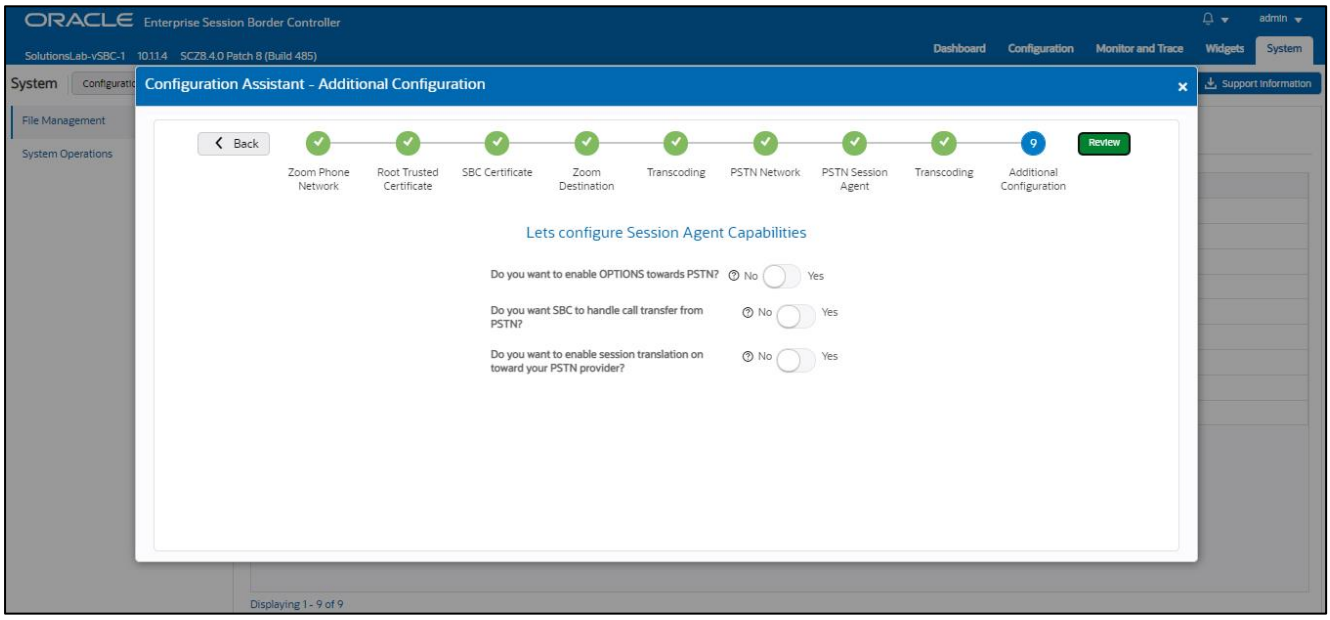
Page 8 is where you will be able to configure transcoding between the SBC and PSTN Trunk.

Once transcoding features is set to “yes”, you will then have an option to select additional media codecs you want included in offers/answers towards PSTN trunk. If you select yes to either question regarding media codecs, you will be presented with a required drop down. You can select as many codecs from the list presented.



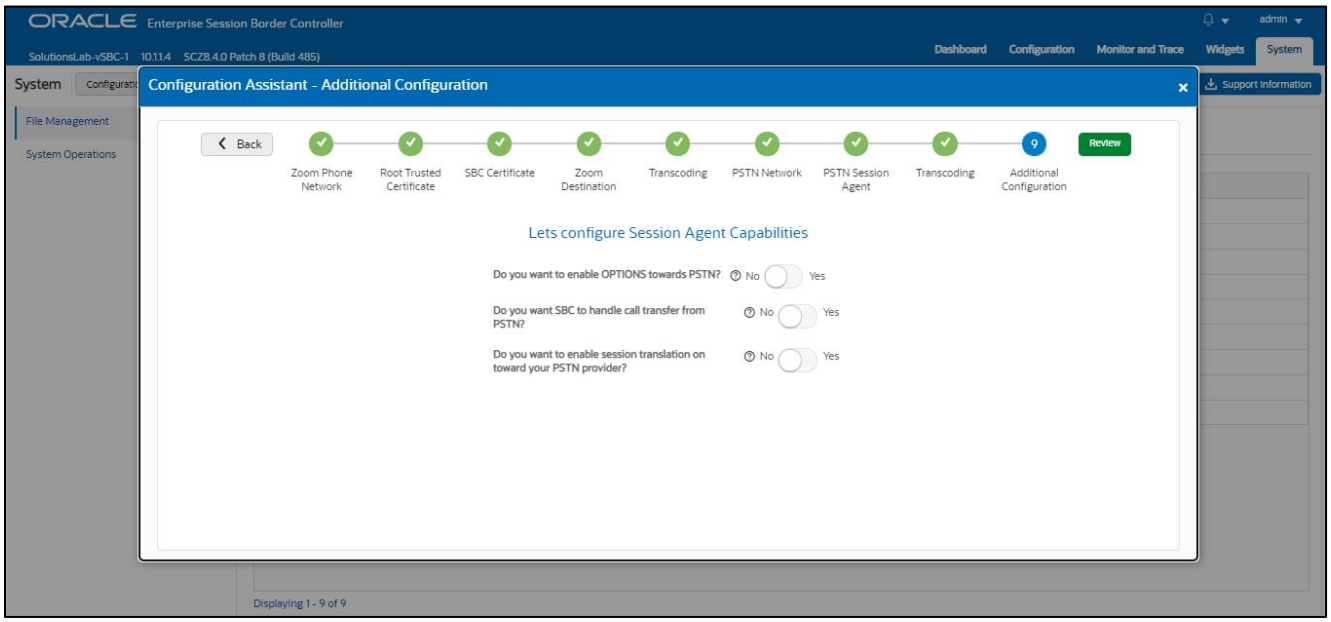

## 10.12 Page 9 – Additional Configuration

Page 9 of this template is where you perform additional optional configuration. Hover over to the **?** to know more about each Option.



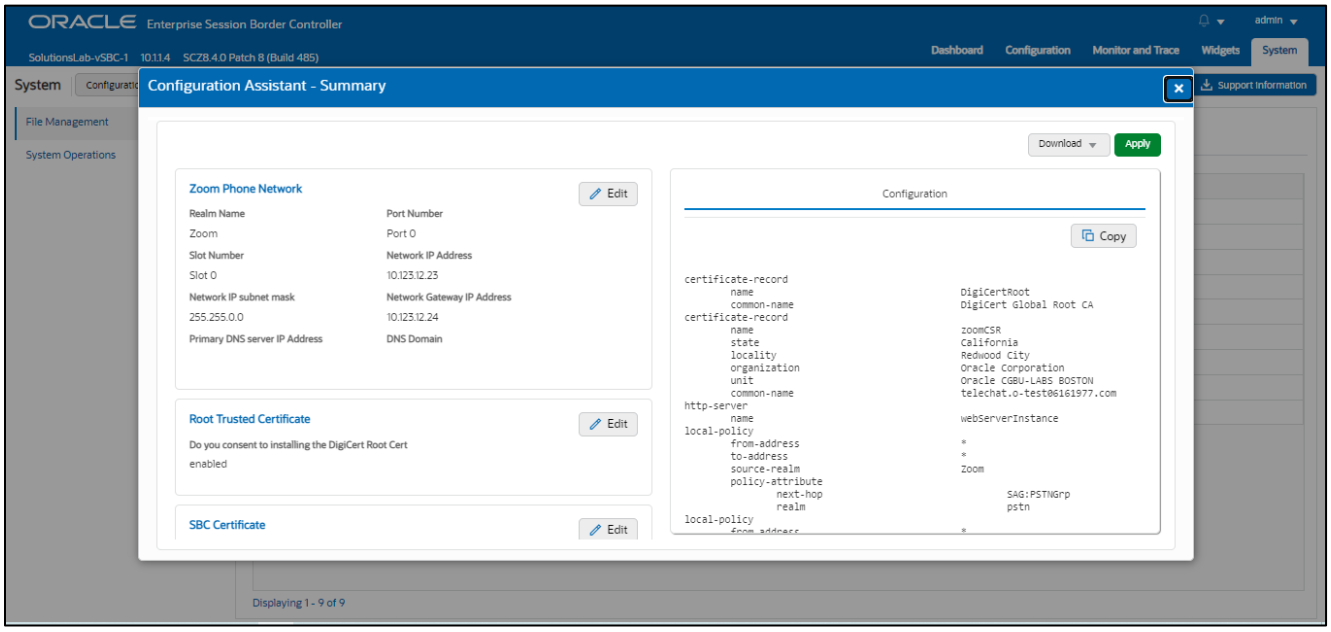

## 10.13 Review

At the end of the template, you will notice in the top right, a "*Review*" tab. If all 9 pages presented across the top are showing green, indicting there are no errors with the information entered, click on the "Review" tab.




The screen looks like below after clicking the Review Tab. The left side of the review page contains all of the entries added on each page and allows for editing each page individually if necessary.

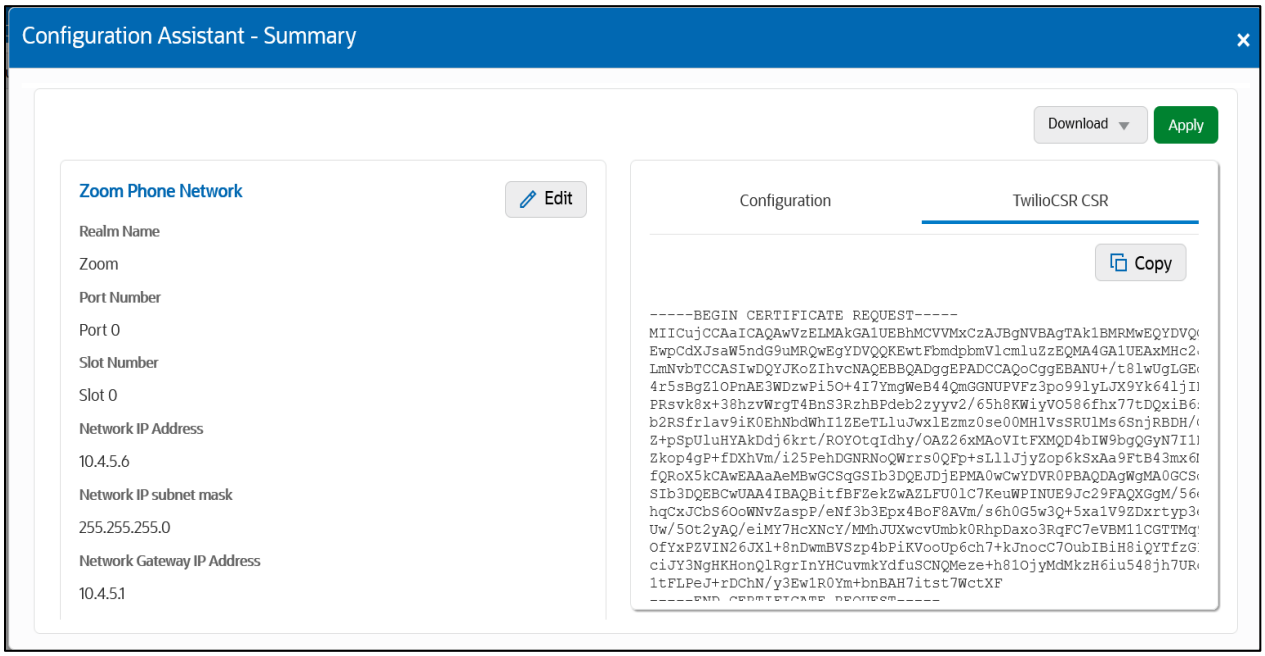
The right side displays the entire configuration created and when applicable, will also have a CSR tab that contains a certificate that can be signed by a CA authority.




On the left side of the review contains the entries for each page. Each page has an "*Edit*" tab that can be used to make changes to the information entered on that specific page without having to go through the entire template again.

On the right side of the review page, under the "*Configuration*" tab is the ACLI output from the SBC. This is the complete configuration of the SBC based on the information entered throughout the template. Also on the right side of the review page you may see another tab, "*CSR*".

On Page 3 of the template, if you chose CSR from the drop-down menu instead of PKCS, the SBC configures a certificate record and generates a certificate signing request for you.




Click the copy button under the CSR and paste the output into a text file. Next, provide the txt file to your CA for signature. Once the certificate is signed by the CA, you will need to import that certificate into the SBC manually, either via ACLI or through the GUI.

*Note: if you chose to import a certificate in PKCS12 format on page 3, the CSR tab will not be present under review.*

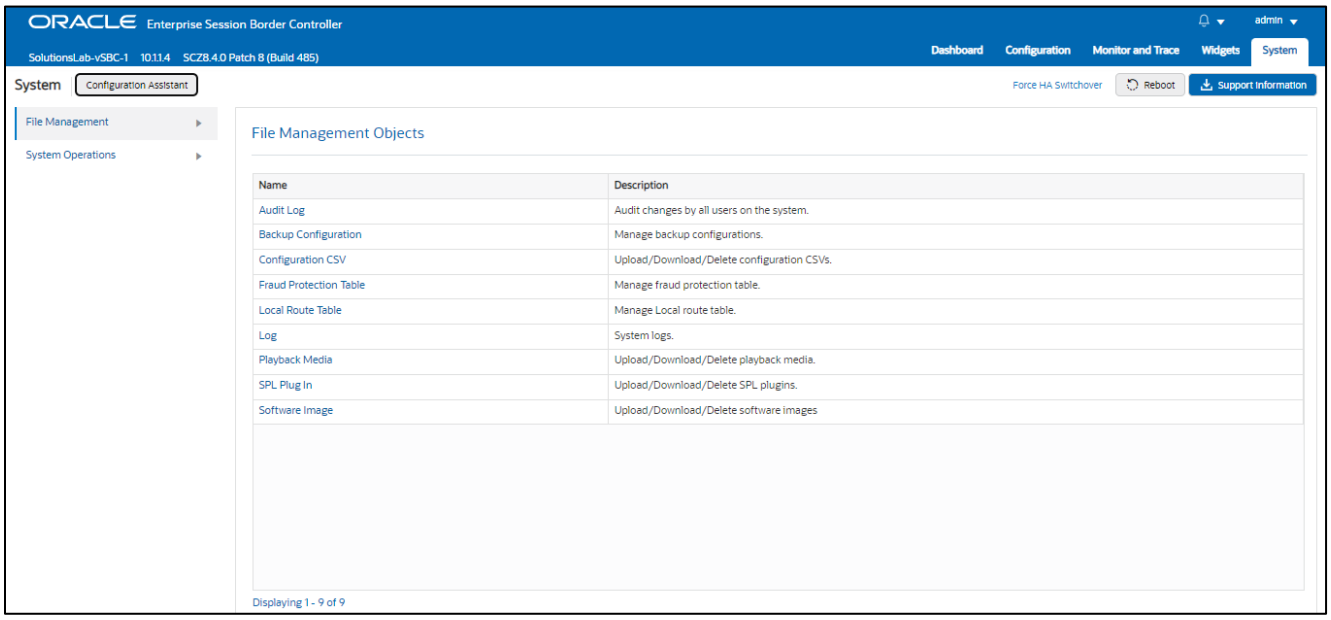
## 10.14 Download and/or Apply

The template provides you with the ability to "Download" the config by clicking the "*Download*" tab on the top right. Next, click the "*Apply*" button on the top right, and you will see the following pop-up box appear.

Now you can click "*Confirm*" to confirm you want to apply the configuration to the SBC. The SBC will reboot. When it comes back up, the SBC will have a basic configuration in place for ZoomPhone with Generic PSTN Sip Trunk.

## 10.15 Configuration Assistant Access

Upon initial login, if the Configuration Assistant Template does not immediately appear on the screen, you can access by clicking on the "*SYSTEM*" tab, top right of your screen. After that, click on the "*Configuration Assistant*" tab, top left. This allows end users to access the Configuration Assistance at any time through the SBC GUI.




## 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                    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            ZoomManipulation
                        out-translationid             addPlus
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            ZoomManipulation
                        out-translationid             addPlus
session-agent
        hostname                    68.68.117.67
        ip-address                  68.68.117.67
        realm-id                    Peer_SIPTrunk
        ping-method                   OPTIONS
        ping-interval               60
                        out-manipulationid            SIPTrunkManipulation
                        out-translationid             removeE164
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
session-translation
        id                        addPlus
        rules-calling               addPlus
        rules-called                addPlus
session-translation
        id                        removeE164
        rules-calling               removeplus1
        rules-called                removeplus1
        rules-asserted-id             removeplus1
SIP-config
        home-realm-id                 Core_Zoom
        registrar-domain              *
        registrar-host              *
        registrar-port              5060
        options                     inmanip-before-validate
                                    max-udp-length=0
        extra-method-stats            enabled
sip-interface
        realm-id                    Core_Zoom
        description                 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            ACME_NAT_TO_FROM_IP
        sip-profile                 forreplaces
        session-timer-profile           ZoomSessionTimerSIP-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                    SIPTrunkManipulation
    description              Manipulations on SIP Trunk side
    header-rule
        name                    XTraceID
        header-name                 X-Trace-ID[^]
        action                  delete
        msg-type                  request
        methods                   INVITE
    header-rule
        name                    XInstanceID
        header-name                 X-Instance-ID[^]
        action                  delete
        msg-type                  request
        methods                   INVITE
    header-rule
        name                    XDMInfo
        header-name                 X-DM-Info[^]
        action                  delete
        msg-type                  request
        methods                   INVITE
    header-rule
        name                    XCapability
        header-name                 X-Capability[^]
        action                  delete
        msg-type                  request
```

```
        methods                 INVITE
    header-rule
        name                    xpublicip
        header-name             X-PUBLIC-IP[^]
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    xorigcontact
        header-name             X-ORIGINAL-CONTACT[^]
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    xorigcallid
        header-name             X-ORIGINAL-CALLID[^]
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    xtocarrier
        header-name             X-TO-CARRIER[^]
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    xFSSupport
        header-name             X-FS-Support[^]
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    callAcme
        header-name             From
        action                  sip-manip
        msg-type                request
        new-value               ACME_NAT_TO_FROM_IP
```

```
        header-rule
            name                        changeAssertedIP
            header-name                 P-Asserted-Identity
            action                      manipulate
            comparison-type             pattern-rule
            msg-type                    request
            methods                     INVITE
            element-rule
                name                    changeIP
                type                    uri-host
                action                  replace
                comparison-type         pattern-rule
                new-value               $LOCAL_IP
SIP-monitoring
        match-any-filter            enabled
        monitoring-filters          *
SIP-profile
        name                        forreplaces
        replace-dialogs             enabled
steering-pool
        ip-address                  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         DigiCertGlobalRootCA
                                    DigiCertSHA2SecureServerCA
        cipher-list                 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
                                    TLS_RSA_WITH_AES_256_CBC_SHA256
        mutual-authenticate             enabled
translation-rules
        id                      addPlus
        type                    add
        add-string                  +1
translation-rules
        id                      removeplus1
        type                    delete
        delete-string               +1
web-server-config
        http-interface-list             GUI
```


**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