Oracle SBC integration with Google CCAI Call Recording

Technical Application Note

ORACLE
COMMUNICATIONS

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Revision History

Version	Description of Changes	Date Revision Completed
1.0	Initial Version – Tested with Oracle SBC software version **OS920p4 and SCZ930 GA**	24th May 2024

Table of Contents

1. Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of the Oracle Enterprise Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform along with Google CCAI Call Recording and on prem IP-PBX.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between IP-PBX with Google CCAI Call Recording. The solution contained within this document has been tested using Oracle Communication SBC with software version **OS920p4 (SCZ9.2.0 Patch 4) and OS930 GA (SCZ9.3.0 GA).** Please note there is no difference in SBC GUI between 9.2.0 and 9.3.0 version from end user perspective. We have tested the solution in 9.3.0 version as it is the latest software available as of now. The configuration screenshots will be mostly covered in 9.2.0 version but there will also be some screenshots captured in 9.3.0 version too.

Please note that the IP Addresses, FQDN and configuration names and details given in this document are used for reference purposes only. These same details cannot be used in customer configurations. End users of this document can use the configuration details according to their network requirements. There are some public facing IPs (externally routable IPs) that we use for our testing are masked in this document for security reasons.
The customers can configure any publicly routable IPs for these sections as per their network architecture needs.

3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Google CCAI Call Recording feature using Oracle Enterprise SBC. There will be steps that require navigating the Oracle SBC GUI interface, understanding the basic concepts of TCP/UDP, IP/Routing, DNS server, SIP/RTP and TLS/SRTP are also necessary to complete the configuration and for troubleshooting, if necessary.

3.2. Requirements

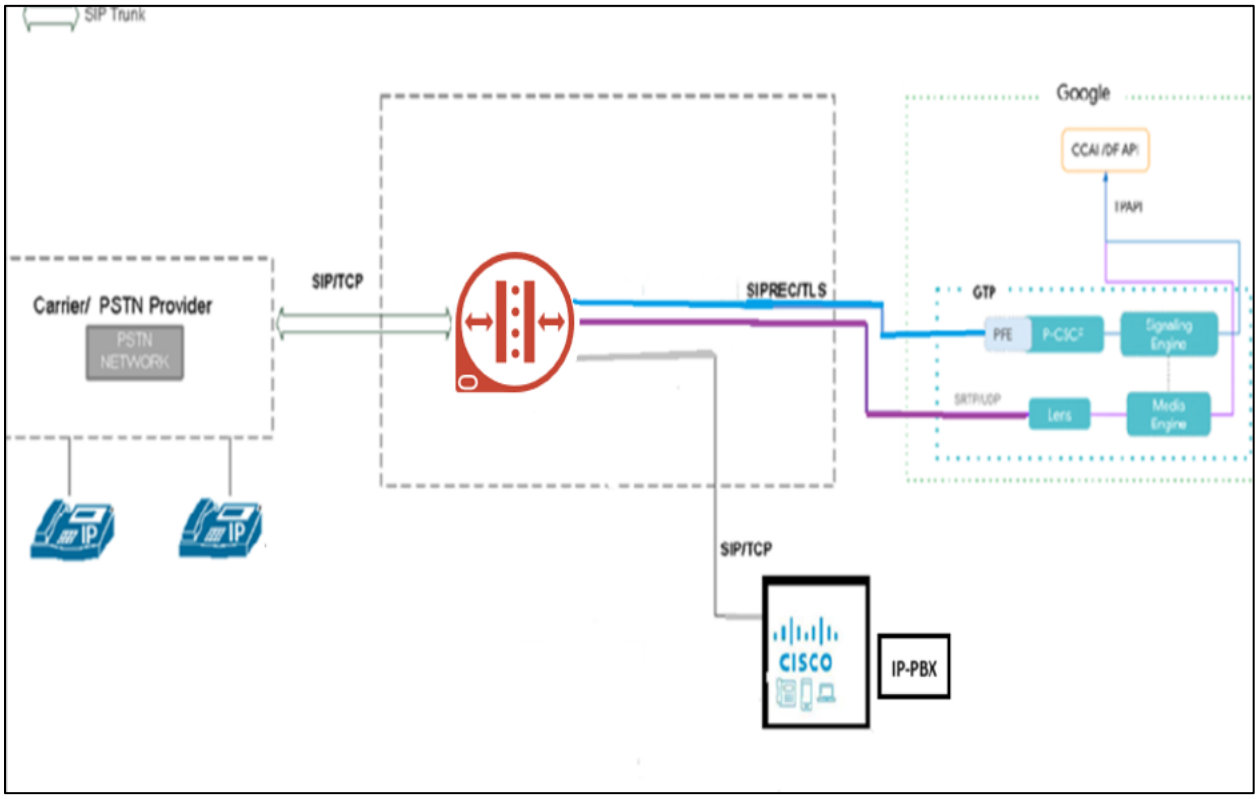
- Fully functioning Google CCAI cloud Environment.
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 9.2.0 version.
- On-prem IP PBX - **We are using Cisco Call Manager (Cisco CUCM) as on prem IP-PBX as an example for this Application note document.**

The below revision table explains the versions of the software used for each component:
This table is Revision 1 as of now:

Software Used	SBC Version	Google CCAI
Revision 1	9.2.0 / 9.3.0	3.13

3.3. Architecture

The network configuration is illustrated below for Google CCAI Call Recording with Oracle Enterprise Session Border Controller and On-prem IP PBX



The configuration, validation and troubleshooting are the focuses of this document and will be described in two phases:

- Phase 1 – About the Google CCAI cloud Environment.
- Phase 2 – About the Configuration of the Oracle SBC.

3.4. Caveats and Limitation

DTLS	DTLS towards Google CCAI is not supported

4. Google CCAI API Configuration

About CCAI Platform

CCAI Platform is an AI-driven Contact Center as a Service (CCaaS) platform that is built natively on Google Cloud and uses the other Google Cloud Contact Center AI (CCAI) products at its core.

CCAI Platform is a unified contact center platform that accelerates the organization's ability to leverage and deploy CCAI without relying on multiple technology providers.

CCAI Platform is a full-stack contact center platform for queuing and routing customer interactions across voice and digital channels. It provides easy routing of customer interactions to the appropriate resource pools. It uses the contact center AI building blocks to allow a seamless transition to human agents. CCAI Platform also allows for reporting on contact center agent performance and customer satisfaction.

CCAI Platform:

- Provides organizations with modern, embeddable APIs that are optimized for the smartphone era.
- Delivers AI-based omni-channel routing, intelligent Virtual Agent, Agent Assist, and Insights capabilities that enables organizations to streamline customer experiences.
- Provides smart device capabilities like photo and video sharing, channel blending, and convenient, on-device authentication.
- Reduces complexity and dependencies.
- Improves speed of deployment

For more information about the Google CCAI platform, please refer to the below link:

https://cloud.google.com/contact-center/ccai-platform/docs

5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Configuring the Google CCAI cloud Environment. **In this SBC config, Google CCAI side is secure (TLS/SRTP) and** PSTN along with on prem IP-PBX side is unsecure (UDP or TCP/RTP).

5.1. Validated Oracle SBC Version

Oracle conducted tests with SBC 9.2.0 and 9.3.0 software – this software with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6300
- AP 6350
- AP 3950 (Starting from SBC 9.0 version)
- AP 4900 (Starting from SBC 9.0 version)
- VME
- Oracle SBC on Public Cloud

6. New SBC configuration

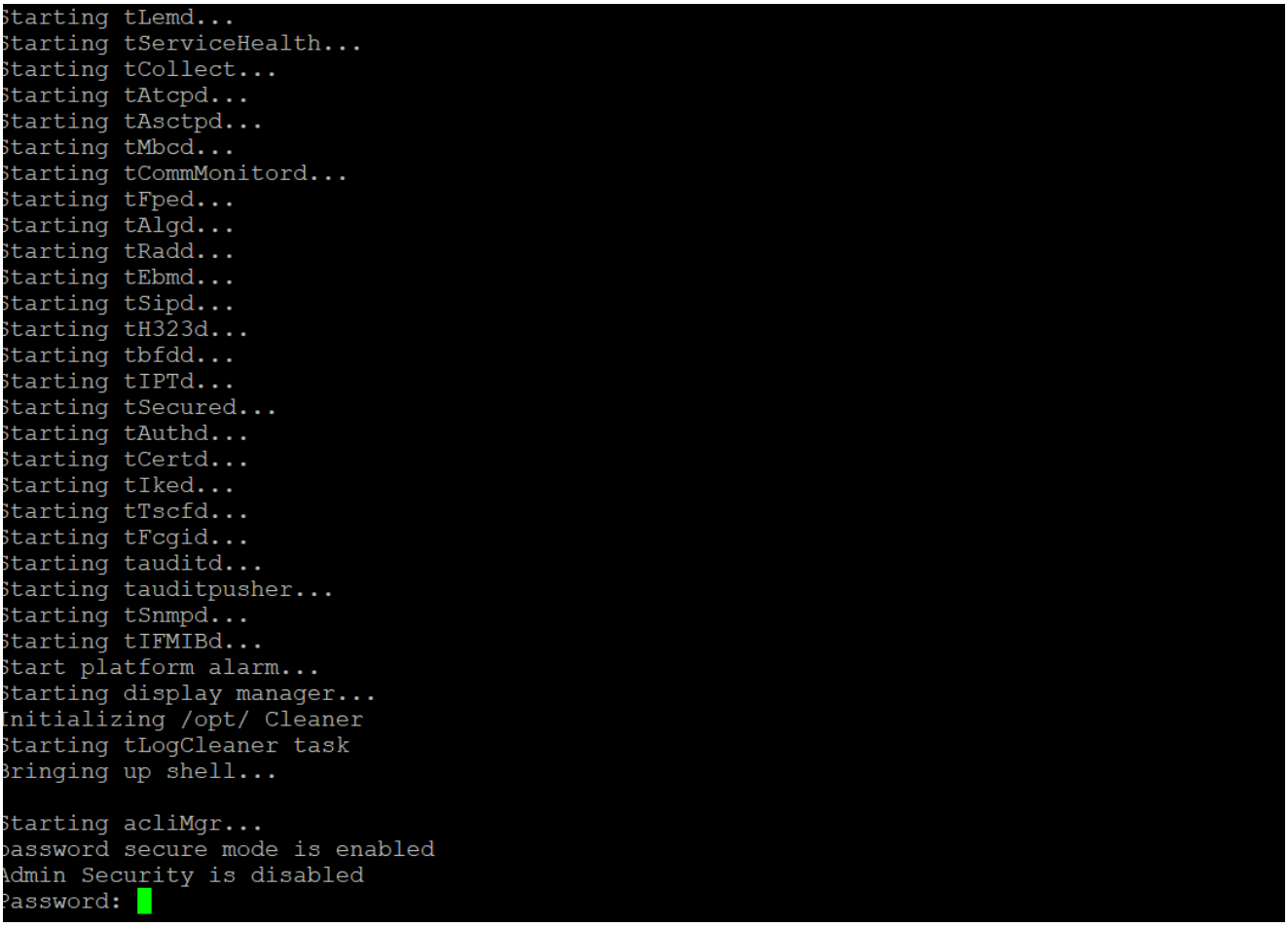
If the customer is looking to setup a new SBC from scratch, please follow the section below.

6.1. Establishing a serial connection to the SBC

Connect one end of a straight-through Ethernet cable to the front console port (which is active by default) on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB-9 adapter) to the DB-9 port on a workstation, running a terminal emulator application such as Putty. Start the terminal emulation application using the following settings:

- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

Power on the SBC and confirm that you see the following output from the boot-up sequence



Enter the default password to log in to the SBC. Note that the default SBC password is “acme” and the default super user password is “packet”.

Both passwords have to be changed according to the rules shown below.

```
Password:
%
% Only alphabetic (upper or lower case), numeric and punctuation
% characters are allowed in the password.
% Password must be 8 - 64 characters,
% and have 3 of the 4 following character classes :
%      - lower case alpha
%      - upper case alpha
%      - numerals
%      - punctuation
%
Enter New Password:
Confirm New Password:

Password is acceptable.
```

Now set the management IP of the SBC by setting the IP address in bootparam.

To access bootparam. Go to Configure terminal->bootparam.

Below is the screenshot captured for SBC 9.2.0 p4 version

```
SolutionsLab-vSBC-2#
SolutionsLab-vSBC-2# conf t
SolutionsLab-vSBC-2(configure)# bootparam

'.' = clear field;  '-' = go to previous field;  q = quit

Boot File               : /boot/nnSCZ920p4.bz
IP Address              :
VLAN                    :
Netmask                 :
Gateway                 :
IPv6 Address            :
IPv6 Gateway            :
Host IP                 :
FTP username            : vxftp
FTP password            :
Flags                   : 0x00000040
Target Name             : SolutionsLab-vSBC-2
Console Device          : COM1
Console Baudrate        : 115200
Other                   :

NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.


        ERROR   : space in /boot      (Percent Free: 1)

SolutionsLab-vSBC-2(configure)#
SolutionsLab-vSBC-2(configure)#
SolutionsLab-vSBC-2(configure)#
```

Below is the screenshot captured for SBC 9.3.0 GA version

```
SolutionsLab-vSBC-2# conf t
SolutionsLab-vSBC-2(configure)# bootparam

'.' = clear field;  '-' = go to previous field;  q = quit

Boot File               : /boot/nnSCZ930.bz
IP Address              :
VLAN                    :
Netmask                 :
Gateway                 :
IPv6 Address            :
IPv6 Gateway            :
Host IP                 :
FTP username            : vxftp
FTP password            :
Flags                   : 0x00000040
Target Name             : SolutionsLab-vSBC-2
Console Device          : COM1
Console Baudrate        : 115200
Other                   :

NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.
```

Note: There is no management IP configured by default.

To configure product type, type in setup product in the terminal

Set product type to Enterprise Session Border Controller as shown below.

```
SolutionsLab-vSBC-2# setup product

------------------------------------------------------------
WARNING:
Alteration of product alone or in conjunction with entitlement
changes will not be complete until system reboot

Last Modified 2022-10-03 07:21:29
------------------------------------------------------------
 1 : Product       : Enterprise Session Border Controller

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]:
```

Enable the features for the ESBC using the setup entitlements command as shown

Save the changes and reboot the SBC.(The below screen is just an example and not actual config)

```
-------------------------------------------------------------------
Entitlements for Enterprise Session Border Controller
Last Modified: 2022-02-23 18:18:18
-------------------------------------------------------------------
 1 : Session Capacity                          : 9999
 2 :   Advanced                                : enabled
 3 :   STIR/SHAKEN Client                      :
 4 : Admin Security                            :
 5 : Data Integrity (FIPS 140-2)               :
 6 : IPSec Trunking Sessions                   : 0
 7 : MSRP B2BUA Sessions                       : 0
 8 : SRTP Sessions                             : 0
 9 : Transcode Codec AMR                       :
 10: Transcode Codec AMR Capacity              : 0
 11: Transcode Codec AMRWB                     :
 12: Transcode Codec AMRWB Capacity            : 0
 13: Transcode Codec EVRC                      :
 14: Transcode Codec EVRC Capacity             : 0
 15: Transcode Codec EVRCB                     :
 16: Transcode Codec EVRCB Capacity            : 0
 17: Transcode Codec EVS                       :
 18: Transcode Codec EVS Capacity              : 0
 19: Transcode Codec OPUS                      : enabled
 20: Transcode Codec OPUS Capacity             : 2000
 21: Transcode Codec SILK                      : enabled
 22: Transcode Codec SILK Capacity             : 2000

Enter 1 - 22 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Session Capacity (0-10000)                   : 500

Enter 1 - 22 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10

  Transcode Codec AMR Capacity (0-10000)       : 50

Enter 1 - 22 to modify, d' to display, 's' to save, 'q' to exit. [s]: 14

  Transcode Codec EVRC Capacity (0-10000)      : 40

Enter 1 - 22 to modify, d' to display, 's' to save, 'q' to exit. [s]:
```

The SBC comes up after reboot and is now ready for configuration.

Go to configure terminal->system->http-server-config. Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

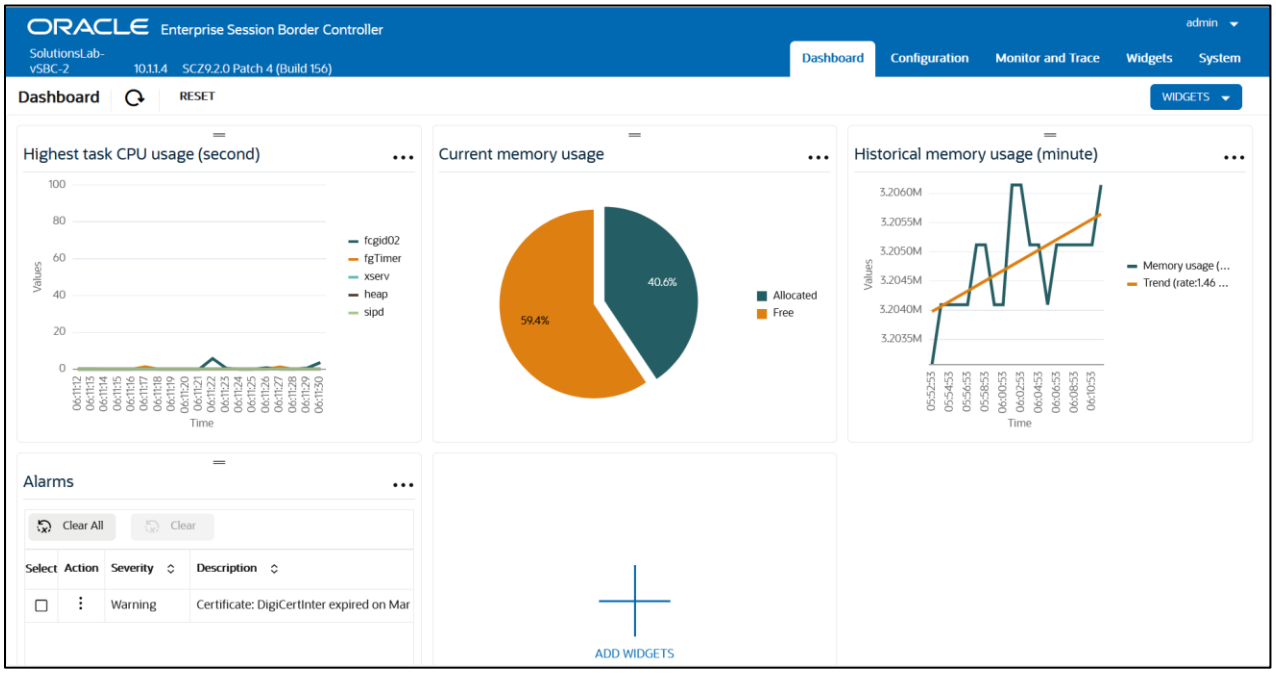
```
SolutionsLab-vSBC-2(http-server)# show
http-server
       name                                  webserver
       state                                 enabled
       realm
       ip-address
       http-state                            enabled
       http-port                             80
       HTTP-strict-transport-security-policy disabled
       https-state                           disabled
       https-port                            443
       http-interface-list                   REST,GUI
       http-file-upload-size                 0
       tls-profile
       auth-profile
       last-modified-by                      webHTTP-admin@196.15.23.12:33336
       last-modified-date                    2022-07-07 17:34:44

SolutionsLab-vSBC-2(http-server)#
SolutionsLab-vSBC-2(http-server)#
SolutionsLab-vSBC-2(http-server)#
```

6.2. Configure SBC using Web GUI

In this app note, we configure SBC using the WebGUI.

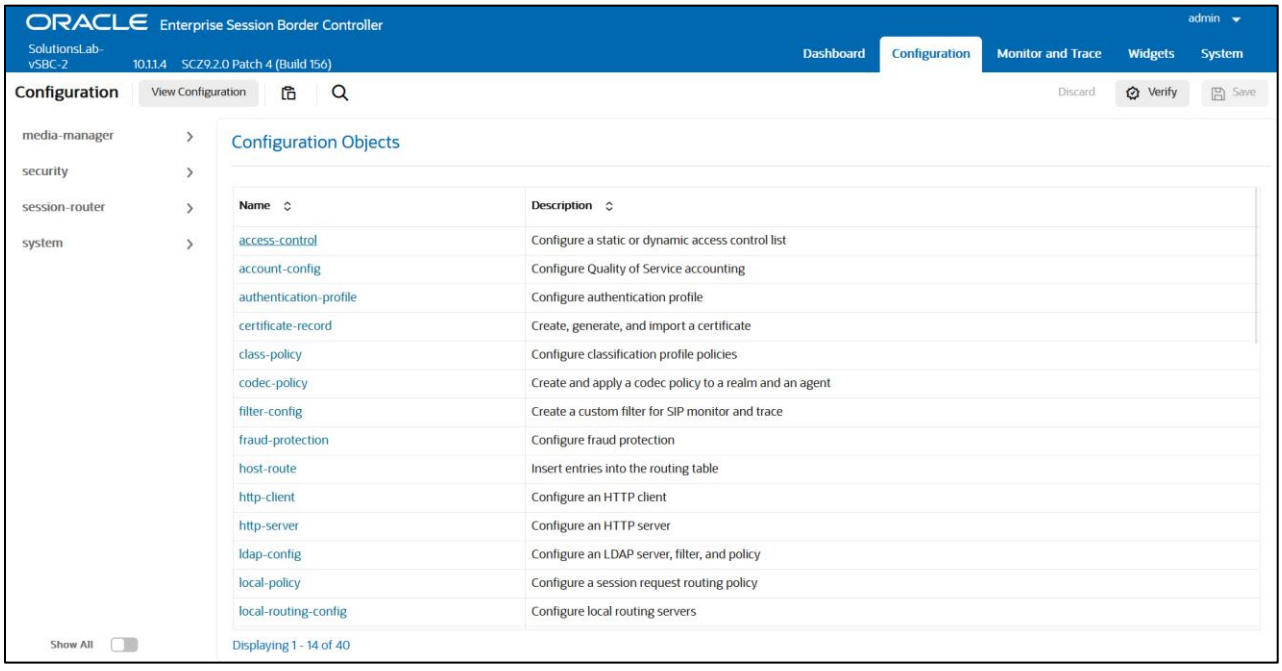
The Web GUI can be accessed through the url http://<SBC_MGMT_IP>.

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

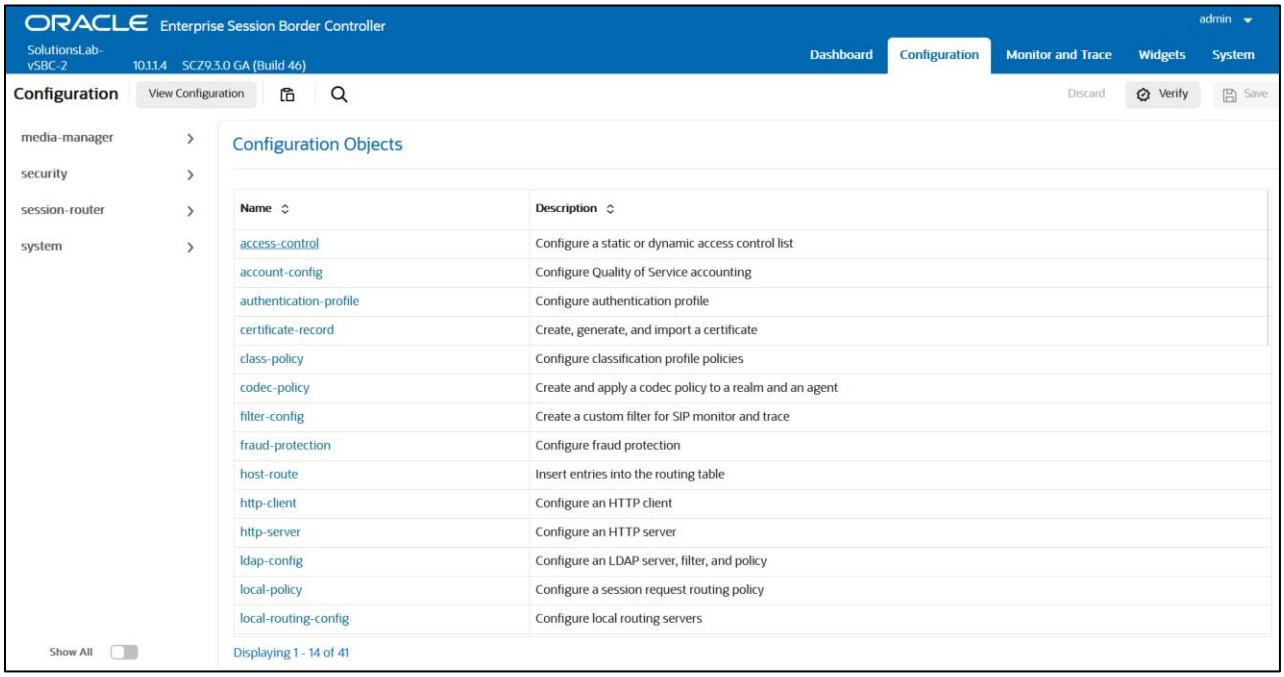


Go to Configuration as shown below, to configure the SBC

Below is the screenshot captured for SBC 9.2.0p4 version



Below is the screenshot captured for SBC 9.3.0 GA version



Kindly refer to the GUI User Guide given below for more information.

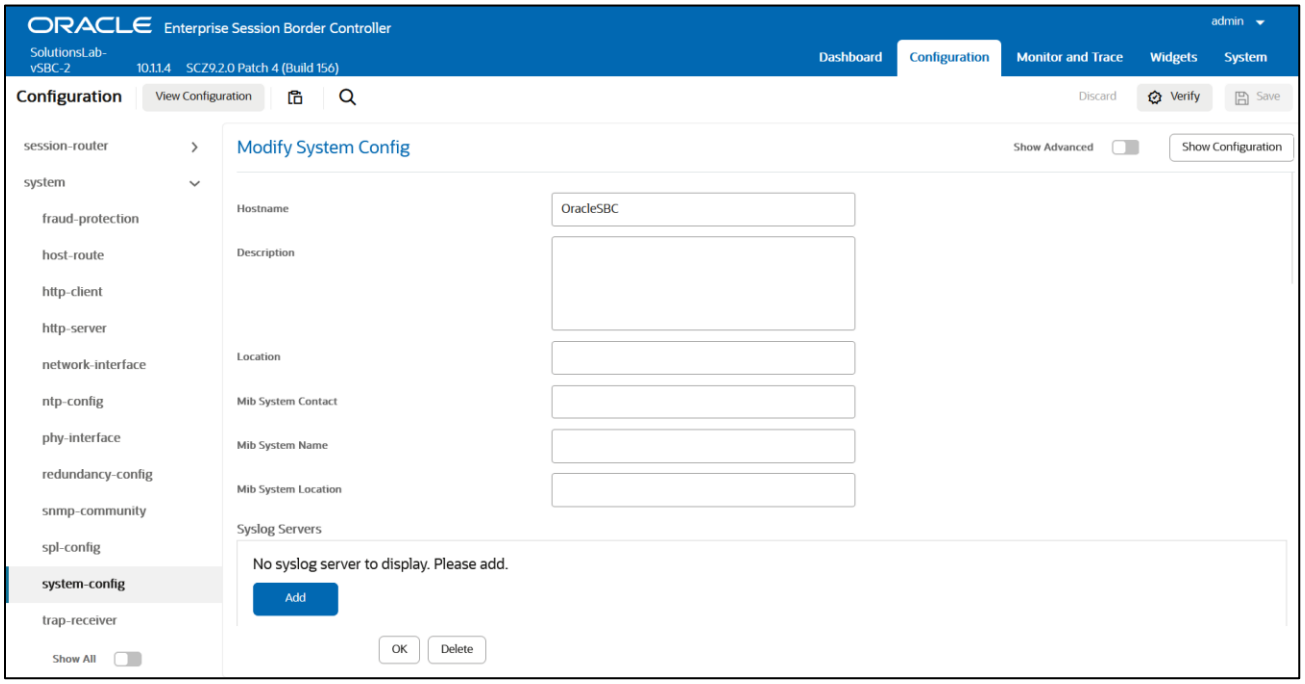
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.3.0/webgui/web-gui-guide.pdf

The expert mode is used for configuration.

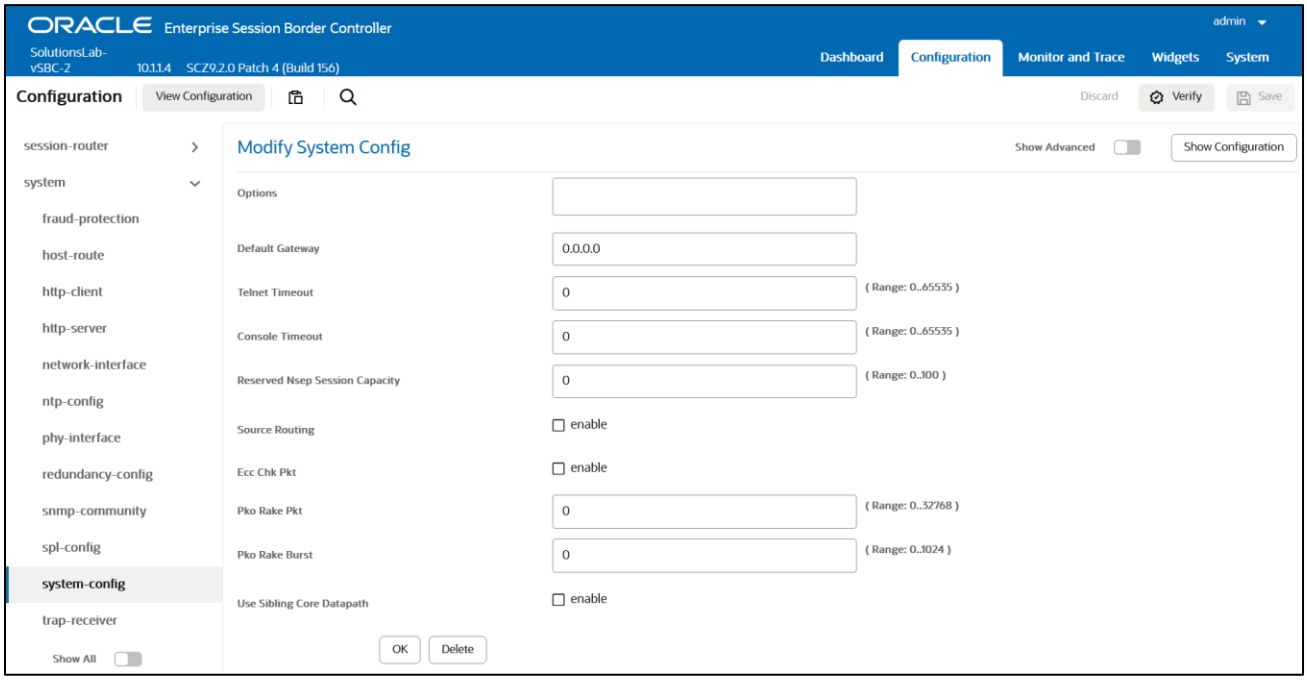
Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

6.3. Configure system-config

Go to system->system-config



Please enter the default gateway value in the system config page as below.



For VME, transcoding cores are required. Please refer the documentation here for more information

https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.2.0/releasenotes/esbc-release-notes.pdf

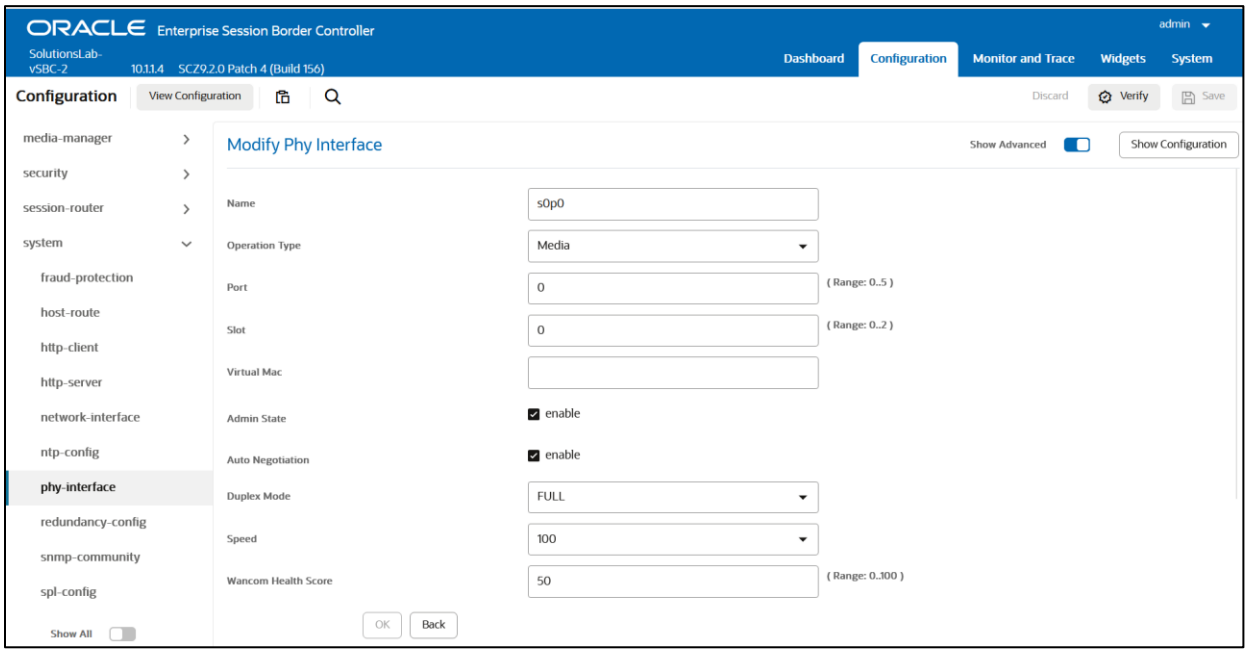
The above step is needed only if any transcoding is used in the configuration.
If there is no transcoding involved, then the above step is not needed.

6.4. Configure Physical Interface values

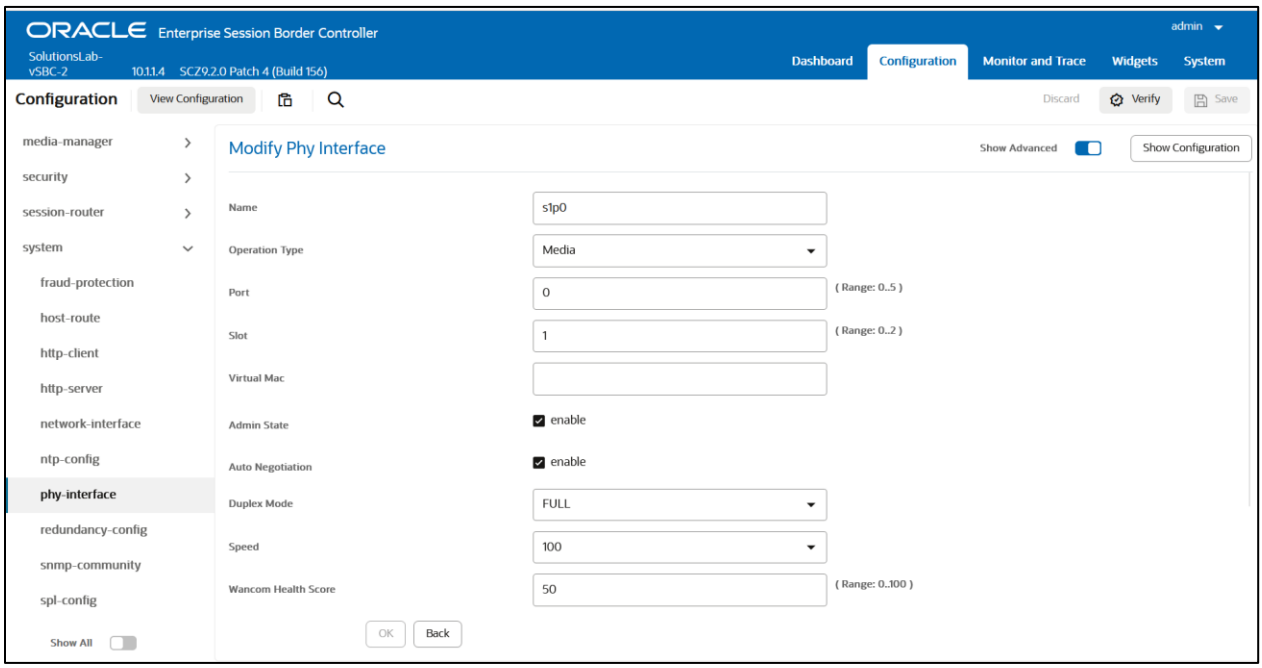
To configure physical Interface values, go to System->phy-interface.
Configure Physical interface towards Google CCAI, IP-PBX as shown below.
The interface designated towards Google CCAI is named as s0p0 (Slot 0, port 0).

Parameter Name	Google CCAI side (s0p0)	IP-PBX side (s1p0)	PSTN side (s1p1)
Slot	0	1	1
Port	0	0	1
Operation Mode	Media	Media	Media

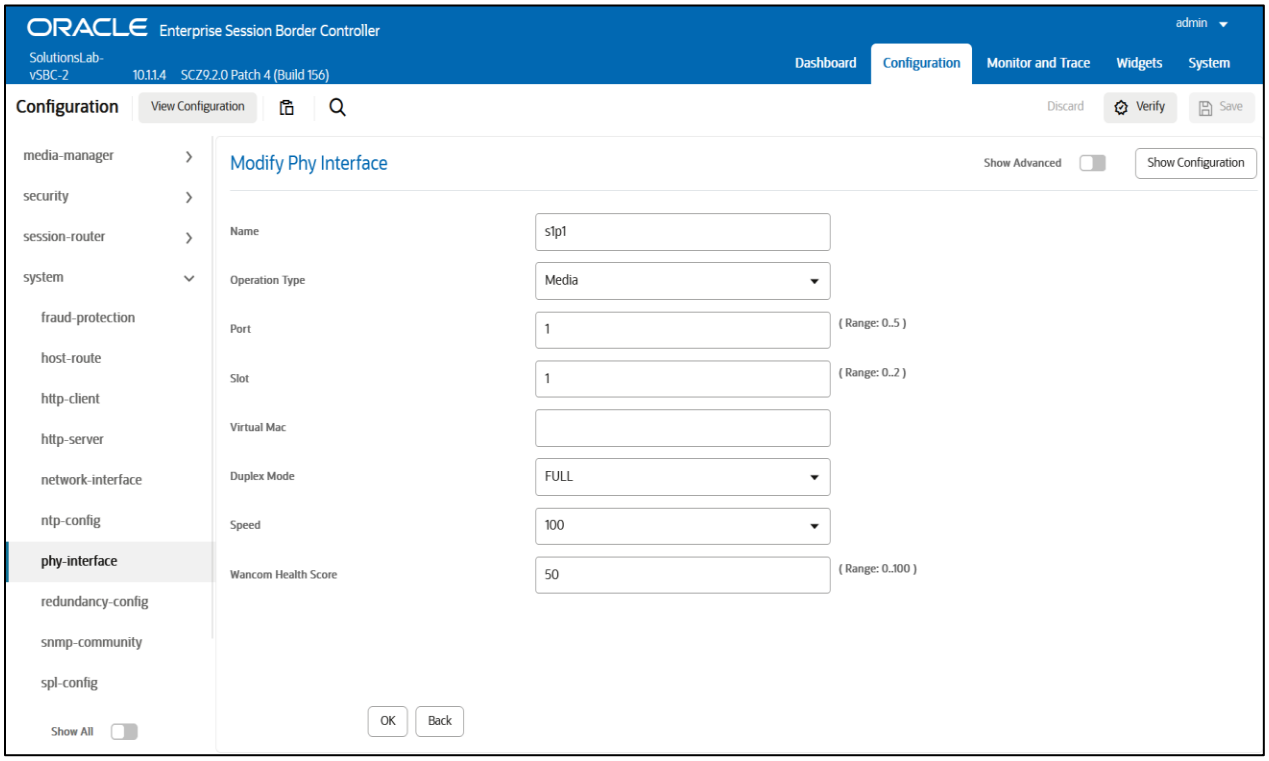
Please configure s0p0 interface as below.



Please configure s1p0 interface as below



Please configure s1p1 interface as below



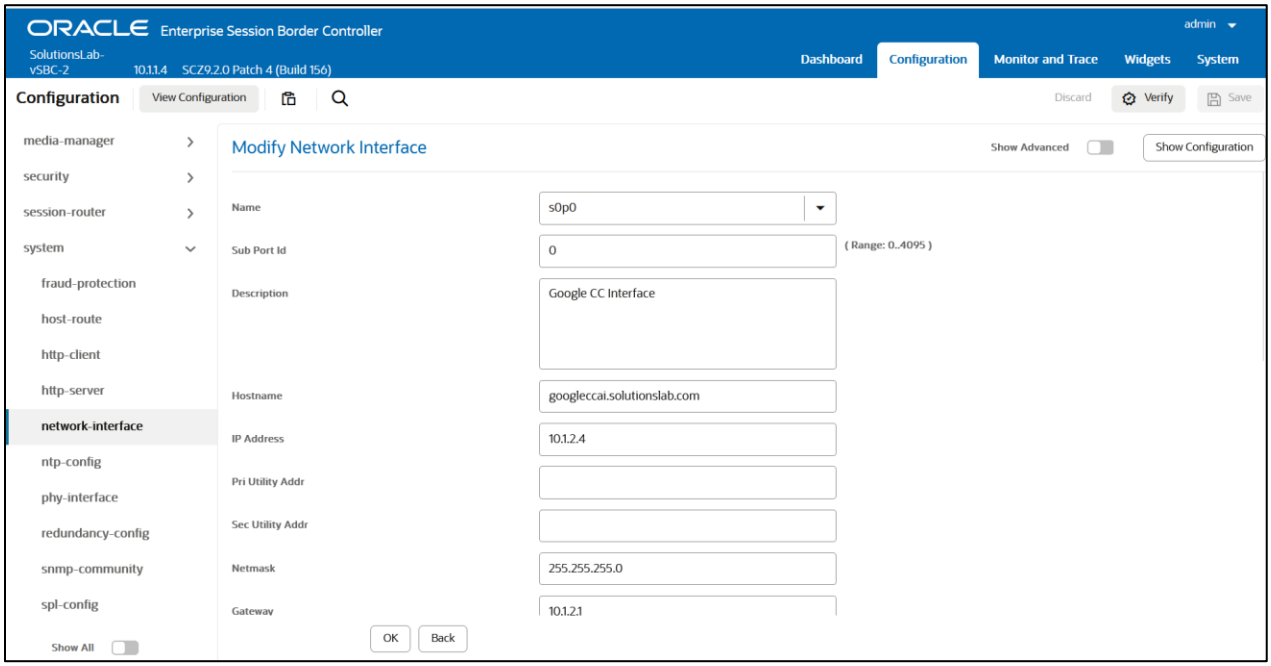
6.5. Configure Network Interface values.

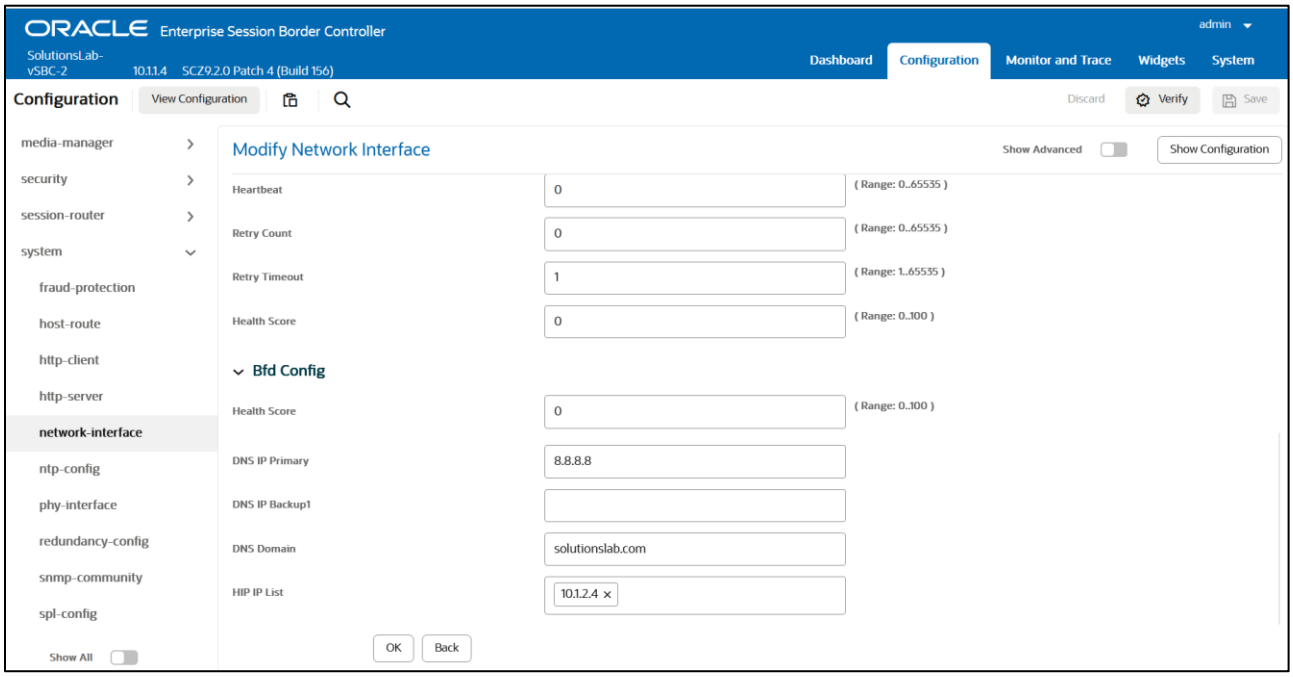
To configure network-interface, go to system->Network-Interface. Configure interface

The table below lists the parameters, to be configured for both the interfaces.

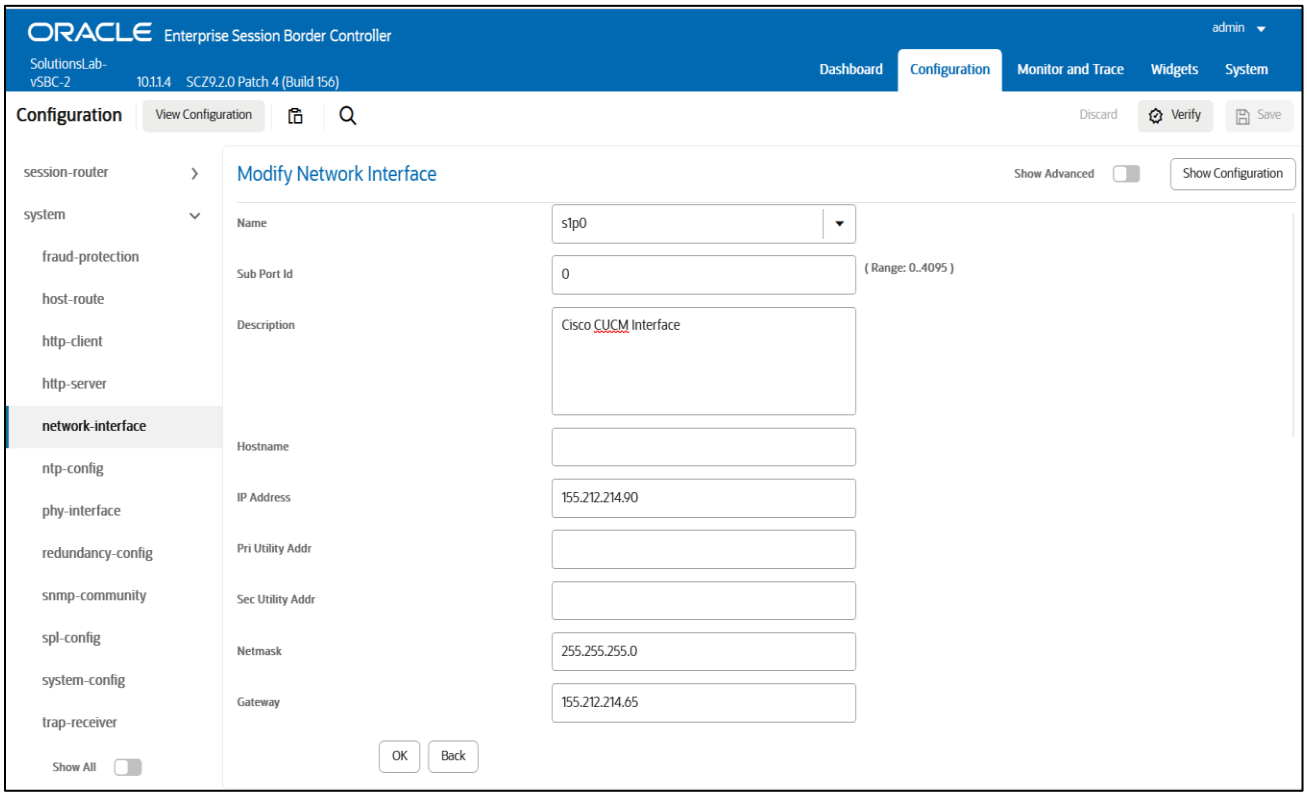
Parameter Name	Google CCAI side Network Interface(s0p0)	IP-PBX Side Network Interface(s1p0)	PSTN Side Network Interface(s1p1)
Name	s0p0	s1p0	s1p1
Host Name			
IP Address	10.1.2.4	155.212.214.90	155.212.214.100
Net Mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	10.1.2.1	155.212.214.65	155.212.214.65

Please configure network interface s0p0 as below

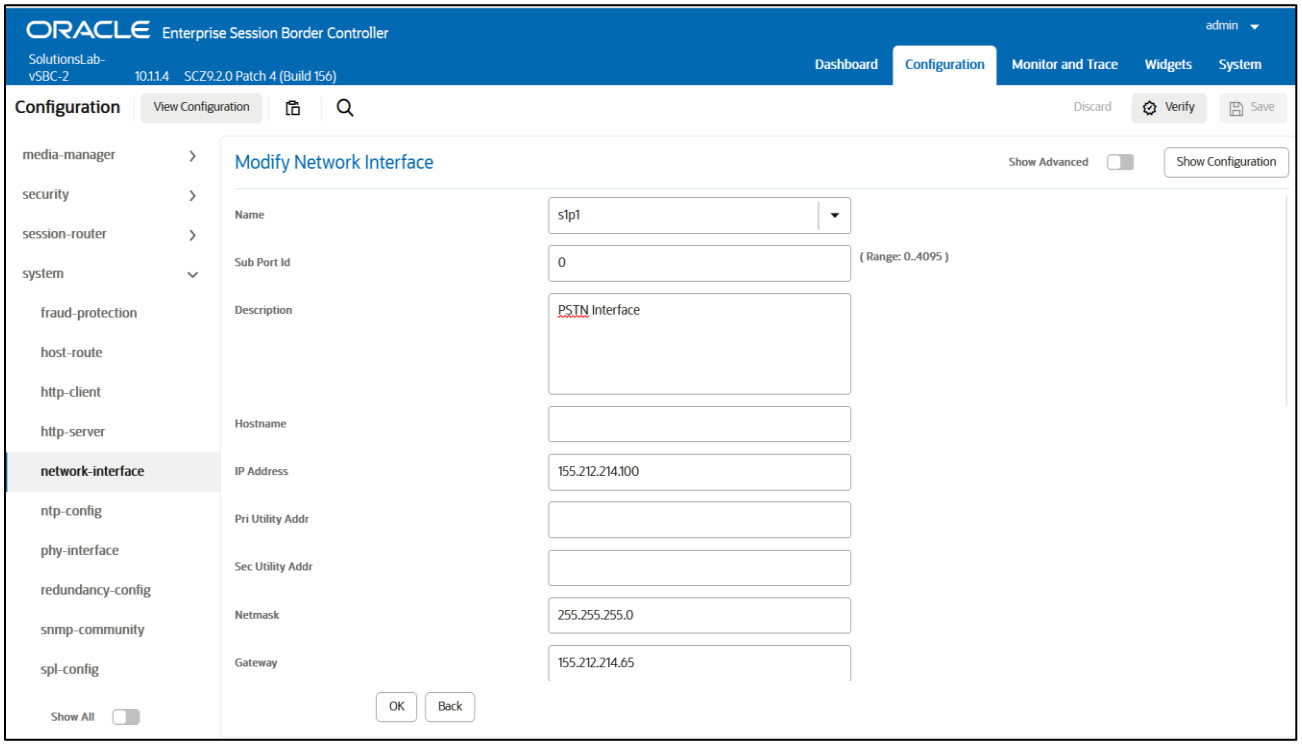




Similarly, configure network interface s1p0 as below



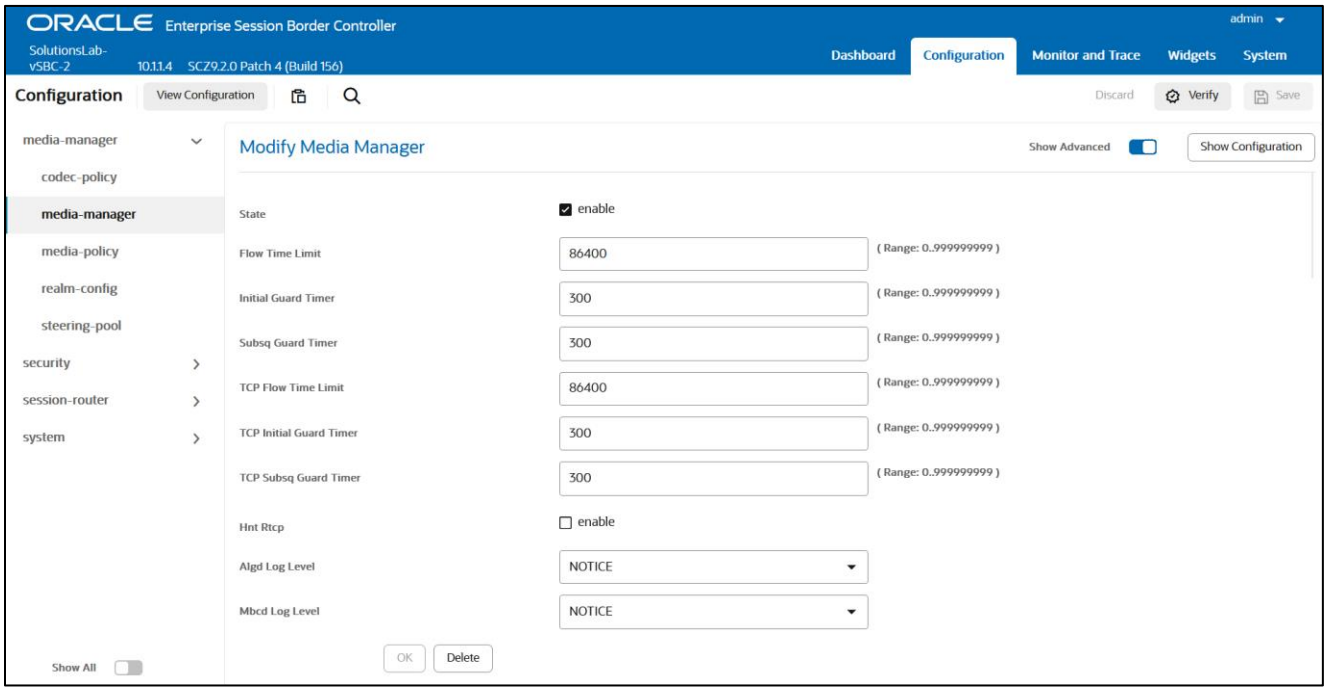
Please configure the network interface s1p0 as below

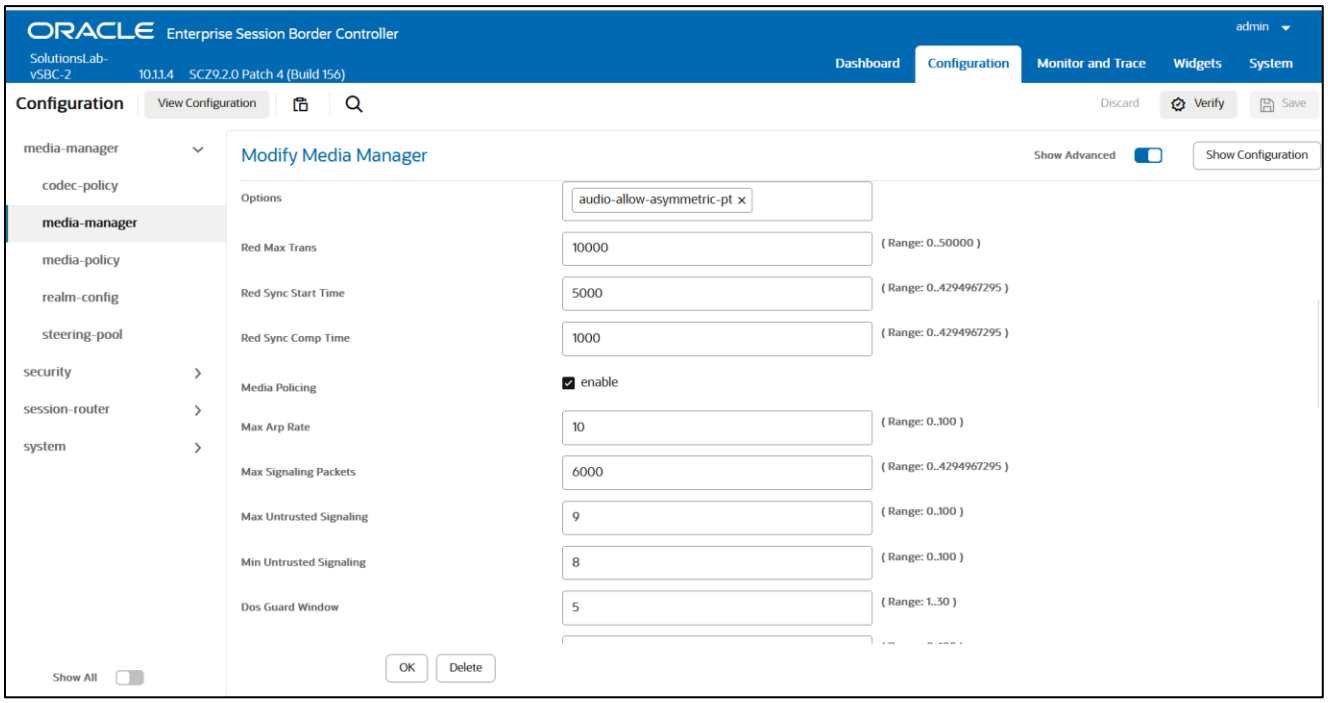


6.6. Enable media manager

Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

Go to Media-Manager->Media-Manager

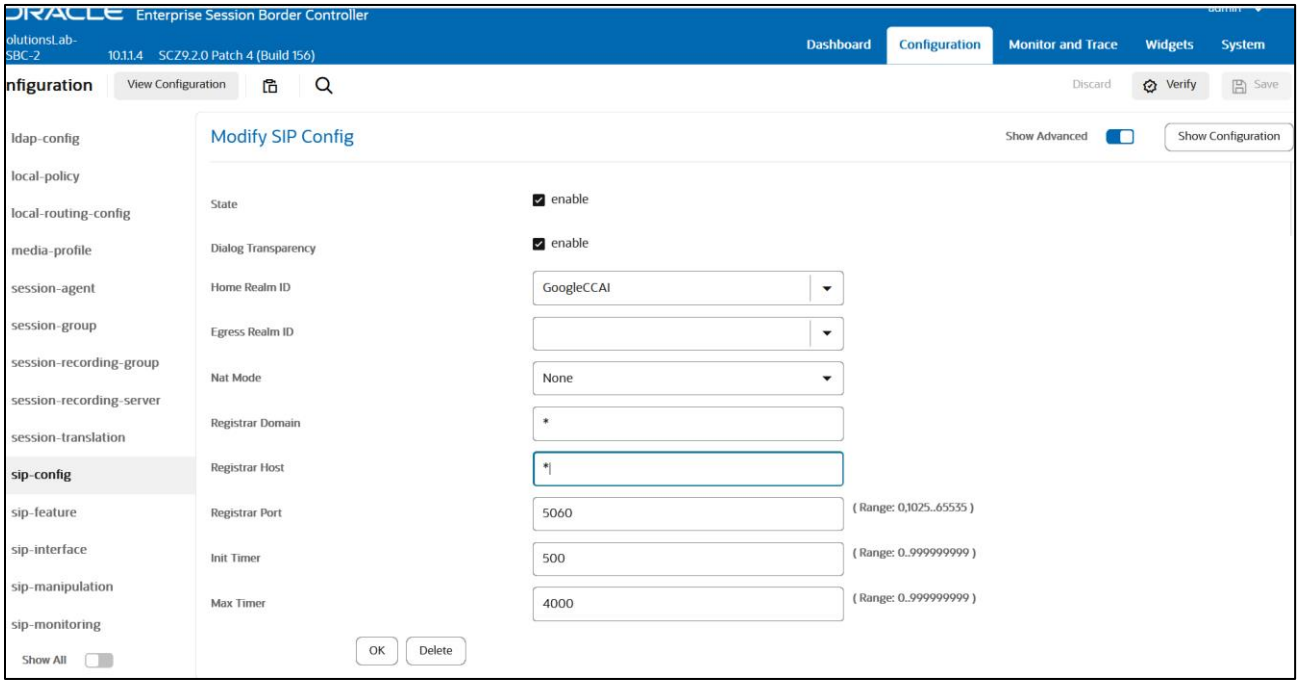


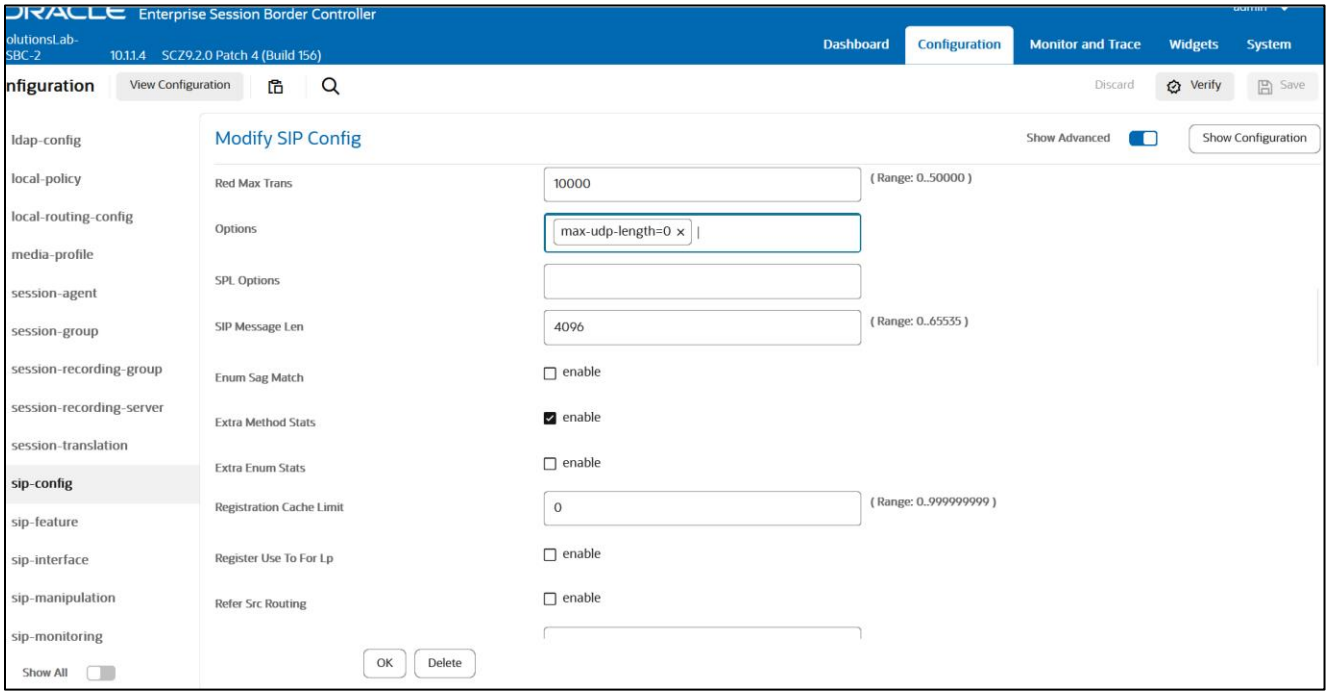


6.7. **Enable sip-config**

SIP config enables SIP handling in the SBC.
Make sure the home realm-id, registrar-domain and registrar-host are configured.
Also add the options to the sip-config as shown below.

To configure sip-config, Go to Session-Router->sip-config.
In options add max-udp-length =0.





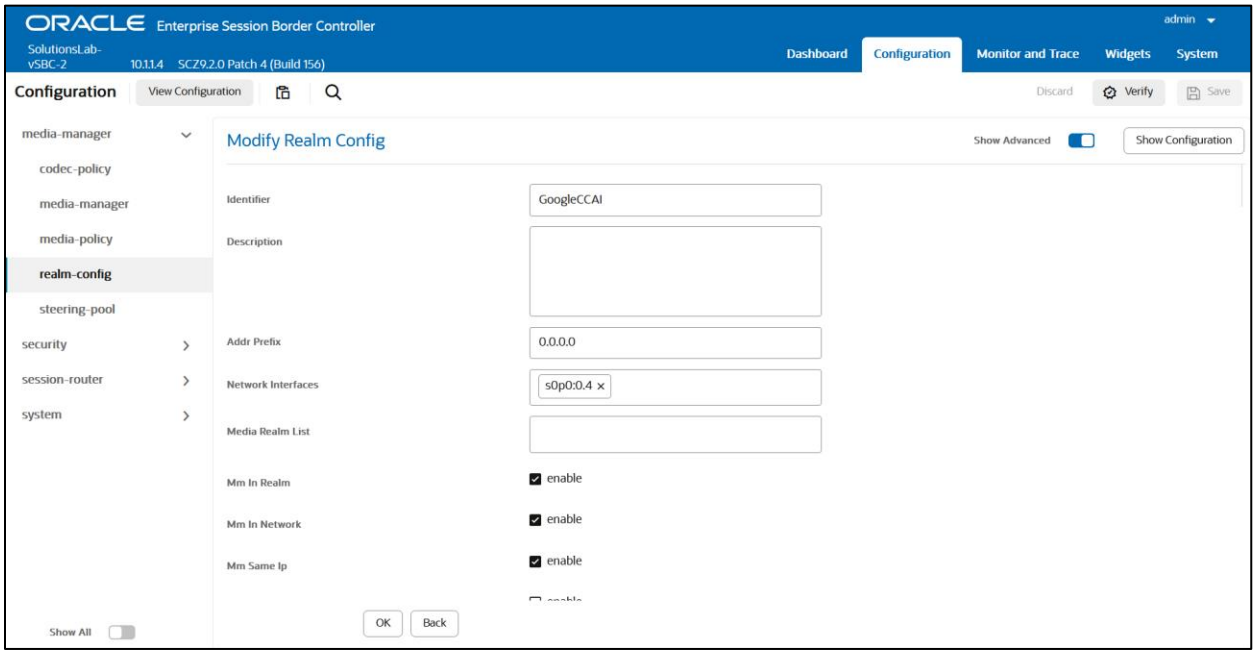
6.8. Configure Realms

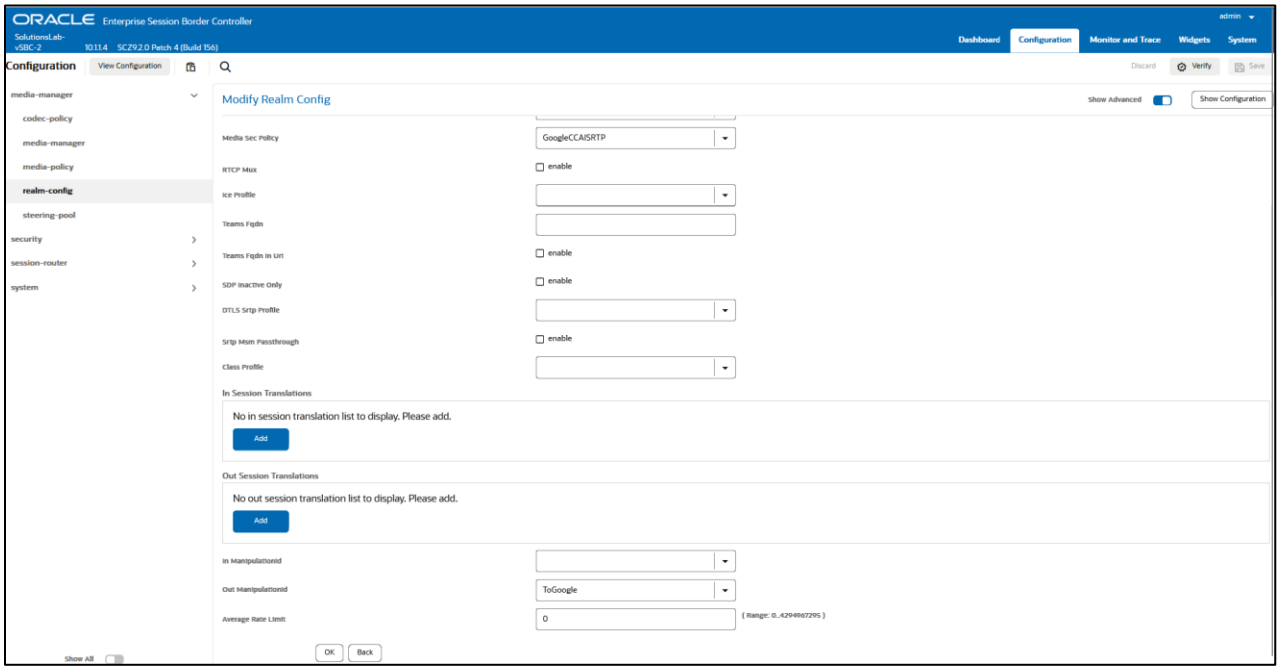
Navigate to realm-config under media-manager and configure a realm as shown below
The name of the Realm can be any relevant name according to the user convenience.

Use the following table as a configuration example for the two realms used in this configuration:

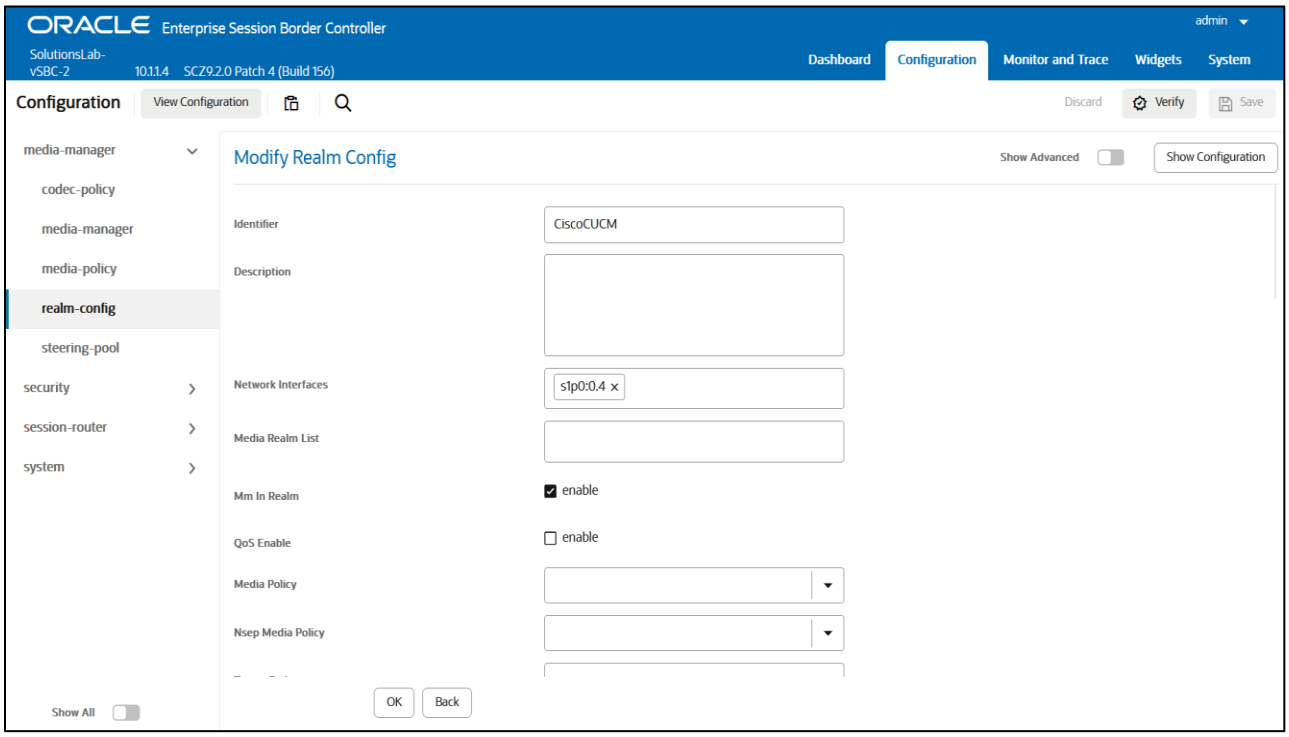
Config Parameter	GoogleCCAI Side	IP-PBX Side	PSTN Side
Identifier	GoogleCCAI	CiscoCUCM	PSTNRealm
Network Interface	S0p0	s1p0	s1p1
Mm in realm	☑	☑	☑
Codec policy	GoogleCC		
Media Sec policy	GoogleCCAISRTP	RTP	RTP
Access Control Trust Level	High	High	High
Out Manipulation id	ToGoogle		
Session Recording Server		GoogleCCAI	

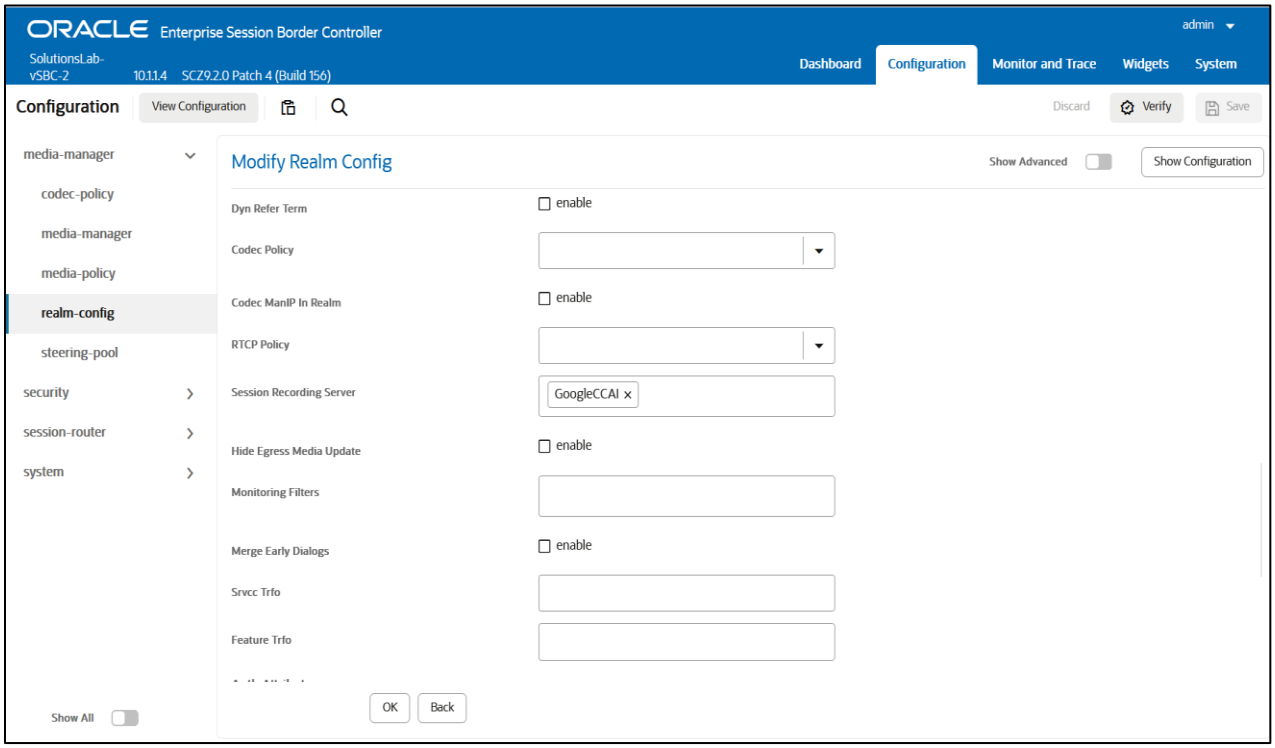
In the below case, Realm name is given as **GoogleCCAI** for Google Side
Please set the Access Control Trust Level as high for this realm



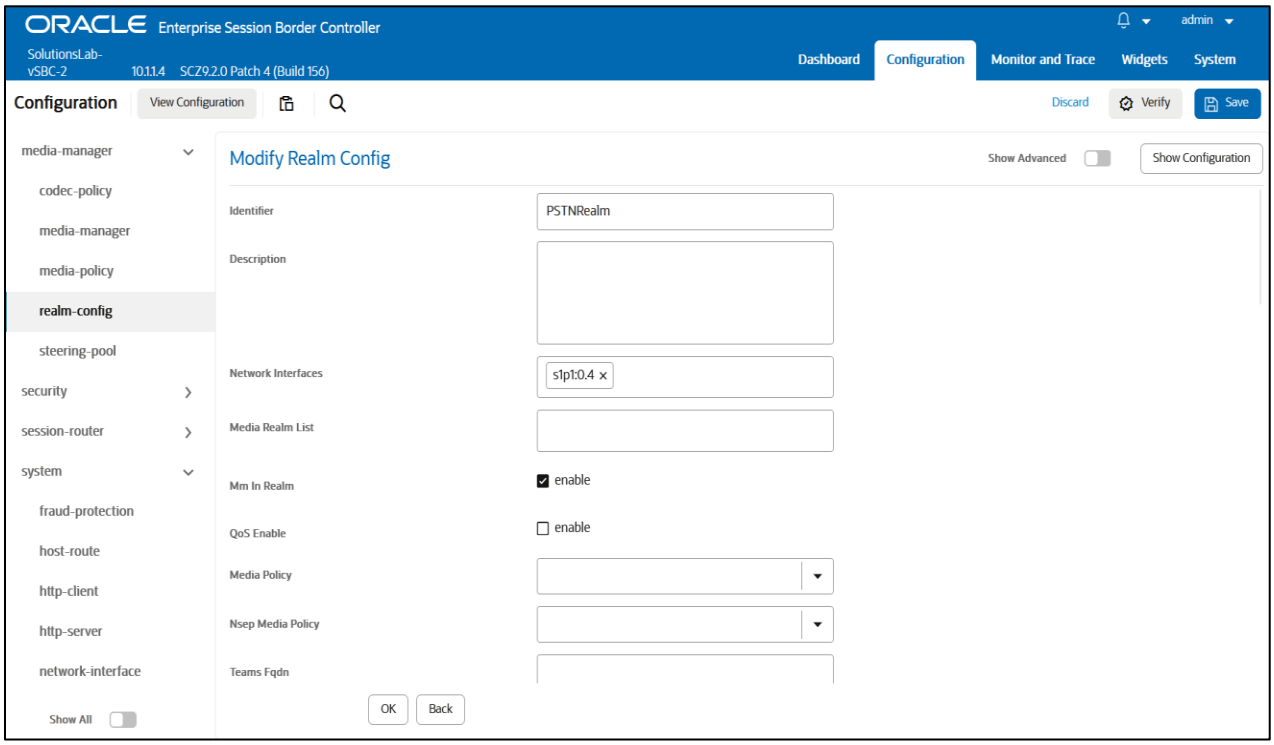


Similarly, Realm name is given as **CiscoCUCM** for IP-PBX side.
Please set the Session Recording Server as GoogleCCAI
Please set the Access Control Trust Level as high for this realm too.





Similarly, Realm name is given as **PSTNRealm** for PSTN side
Please set the Access Control Trust Level as high for this realm too.



For more information on Access Control Trust Level, please refer to SBC Security guide link given below:

https://docs.oracle.com/en/industries/communications/session-border-controller/9.3.0/security/security-guide.pdf

6.9. Configuring a certificate for SBC

This section describes how to configure the SBC for TLS and SRTP communication for Google CCAI Google CCAI side allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. The only requirement when configuring this certificate is the common name must contain the SBC's FQDN. In this example our common name will be **solutionslab.cgbuburlington.com**. You must also give it a name. All other fields are optional and can remain at default values.

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

- SBC Certificate (end-entity certificate)
- DigiCert RootCA Cert (Root CA used to sign the SBC's end entity certificate)
- Google GTS Root R1 (GTSR1) (Google Presents the SBC a certficate signed by this authority)

Note: The DigiCert RootCA is only part of this example and is the Authority we used to sign our SBC certificate. You would replace this with the root and/or intermediate certificates used to sign the CSR generated from your SBC.

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

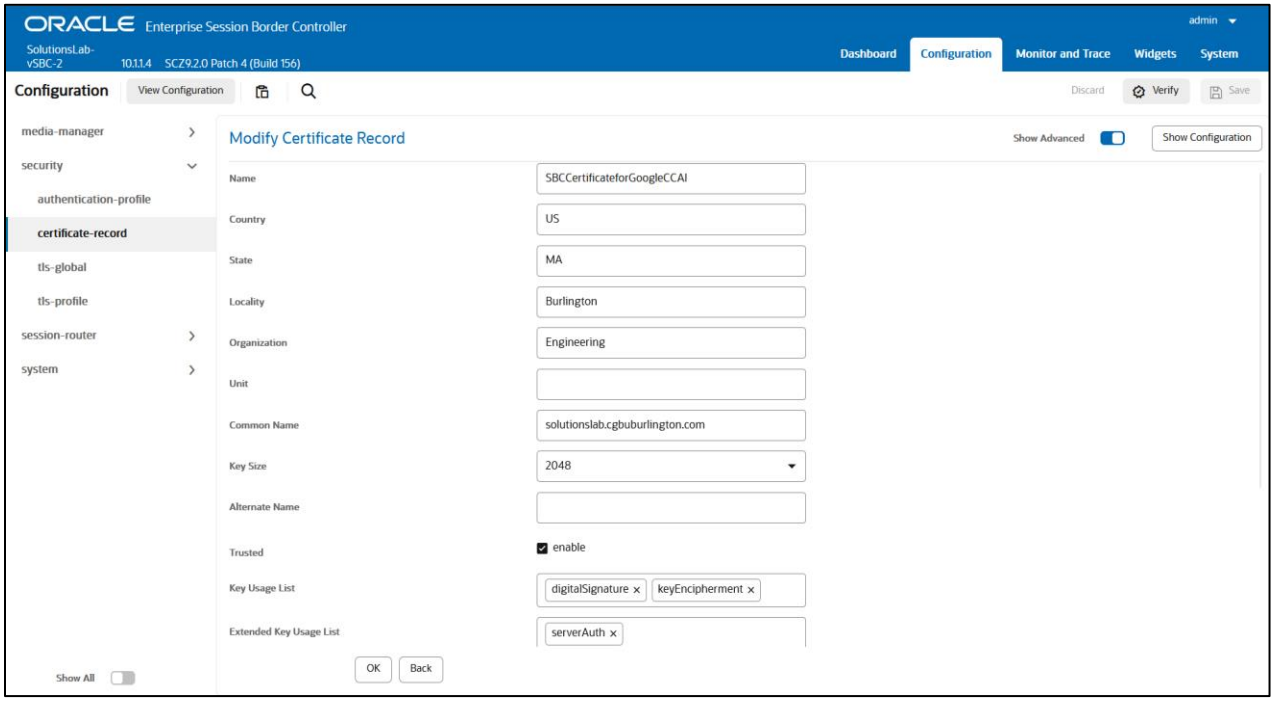
   This section walks you through how to configure certificate records, create a certificate signing request and import the necessary certificates into the SBC's configuration.

- SBC – 1 certificate-record assigned to SBC
- Root – 1 certificate-record for root cert

2) Deploy the SBC and Root certificates on the SBC

Step 1 – Creating the certificate record

Go to security->Certificate Record and configure the SBC entity certificate for SBC as shown below.



The following, DigitCertRoot, is the root CA certificate used to sign the SBC's end entity certificate. As mentioned above, your root CA and/or intermediate certificate may differ. This is for example purposes only.

Google GTS Root 1 (GTSR1) Certificate:

Google presents a certificate to the SBC which is signed by Google GTS Root 1. The TLS certificate and the trust chain from either of the public CAs must be added to the TLS profile of the SBC along with the Google Root certificate.

You can download the GTSR1 trusted root certificate here: https://pki.goog/repo/certs/gtsr1.pem
You can access the GlobalSign trusted root certificate here: GlobalSignRootCA
Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

The table below specifies the parameters required for certificate configuration. Modify the configuration according to the certificates in your environment.

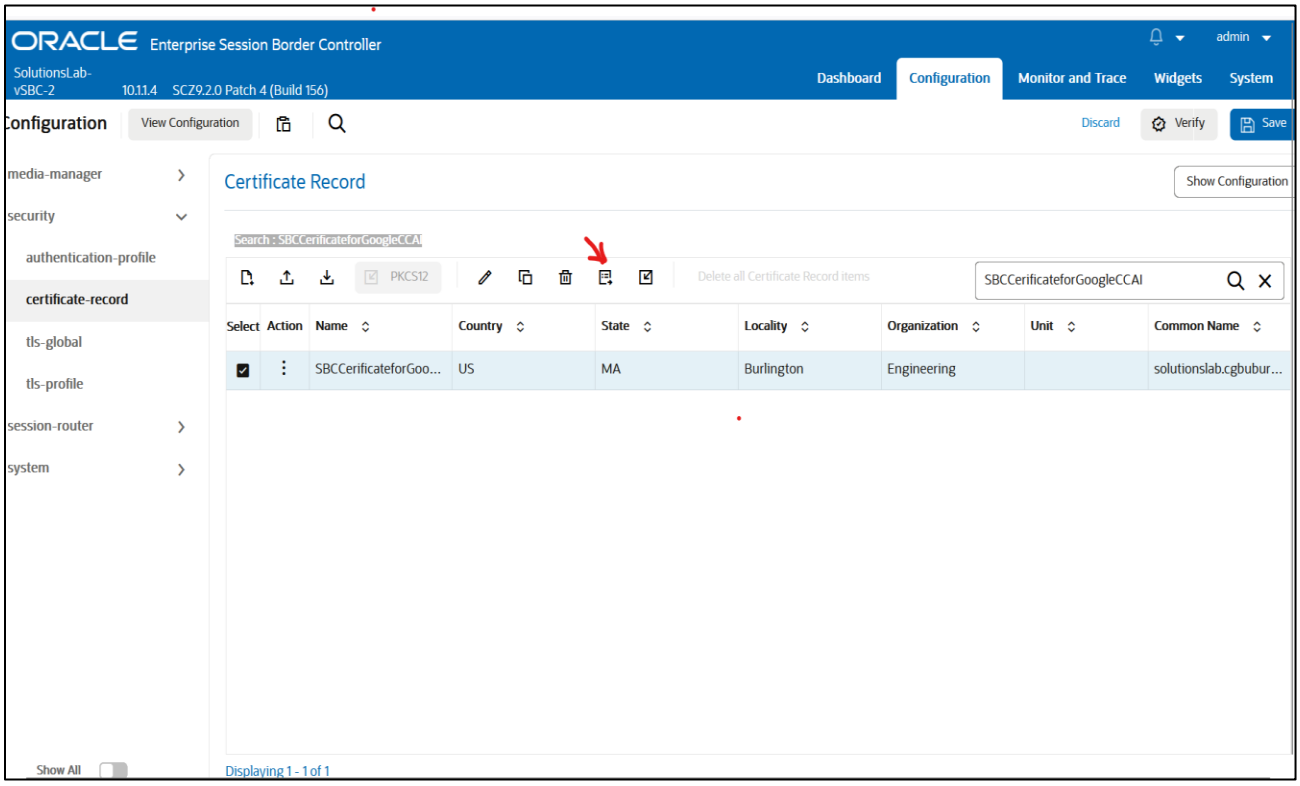
Config Parameter	GTSR1	GlobalSign Root CA	DigiCert Root CA
Common Name	GTS Root R1	GlobalSign Root CA	DigiCert Global Root CA
Key Size	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256

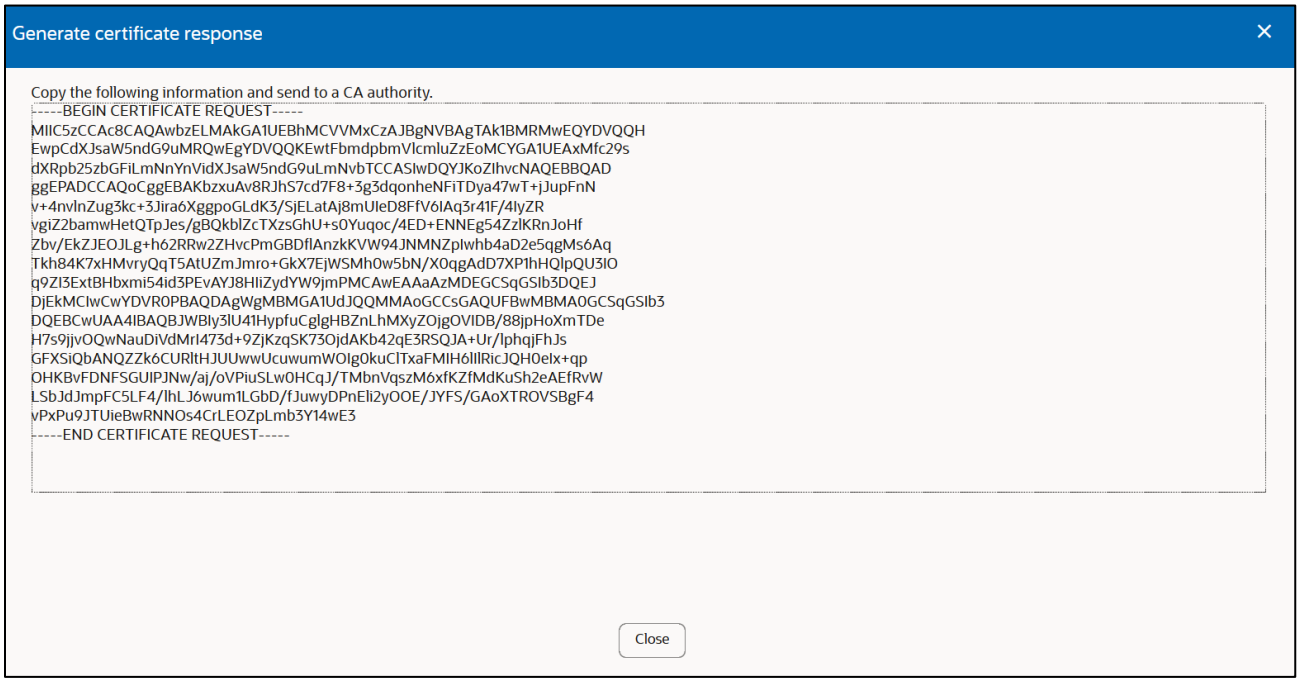
Step 2 – Generating a certificate signing request

(Only required for the SBC's end entity certificate, and not for root CA certs)

Please note – certificate signing request is only required to be executed for SBC Certificate – not for the root/intermediate certificates.

- Select the certificate and generate certificate on clicking the "Generate" command.
- Please copy/paste the text that gets printed on the screen as shown below and upload to your CA server for signature.

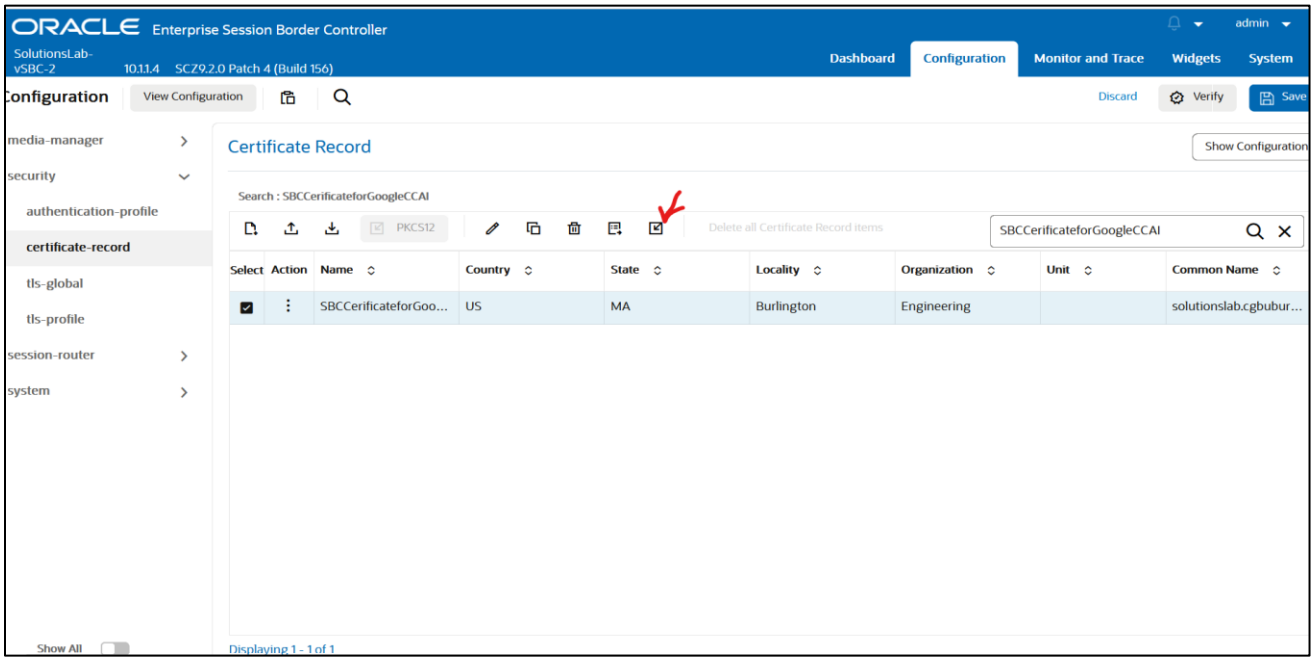


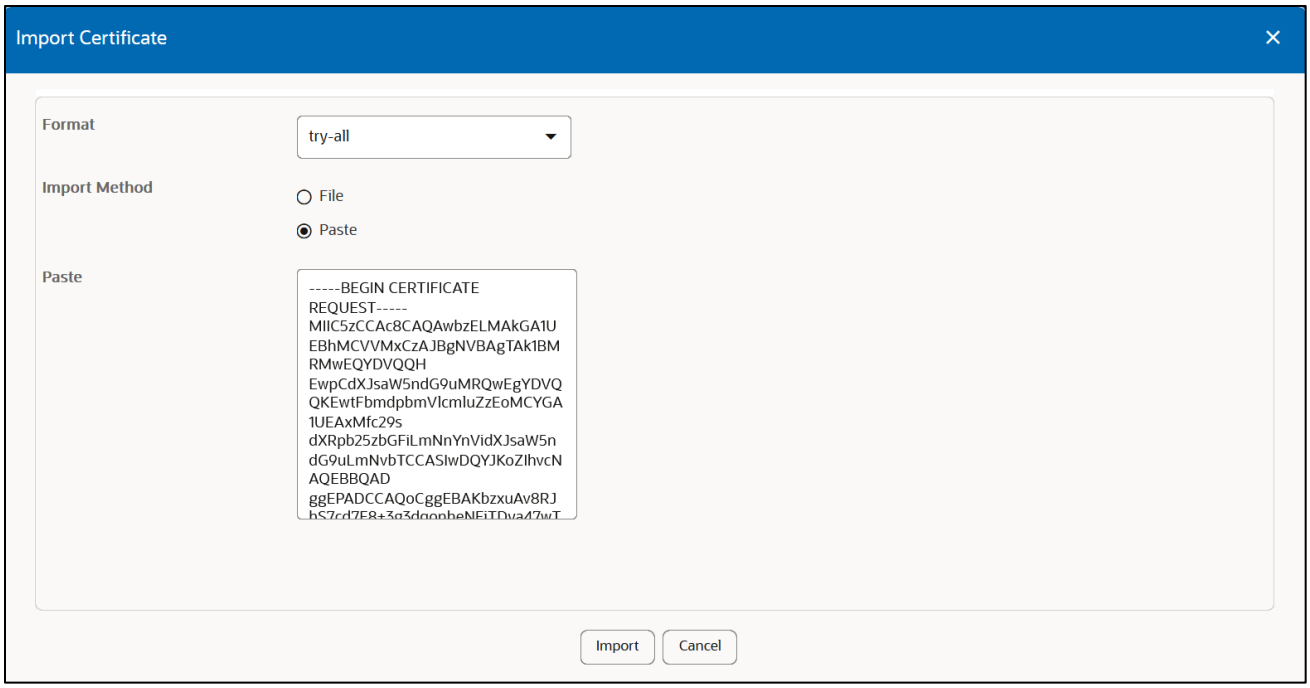


- Also, note that a **save/activate** is required

Step 3 – Deploy SBC & root certificates

Once certificate signing request have 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 done, issue **save/activate** from the WebGUI

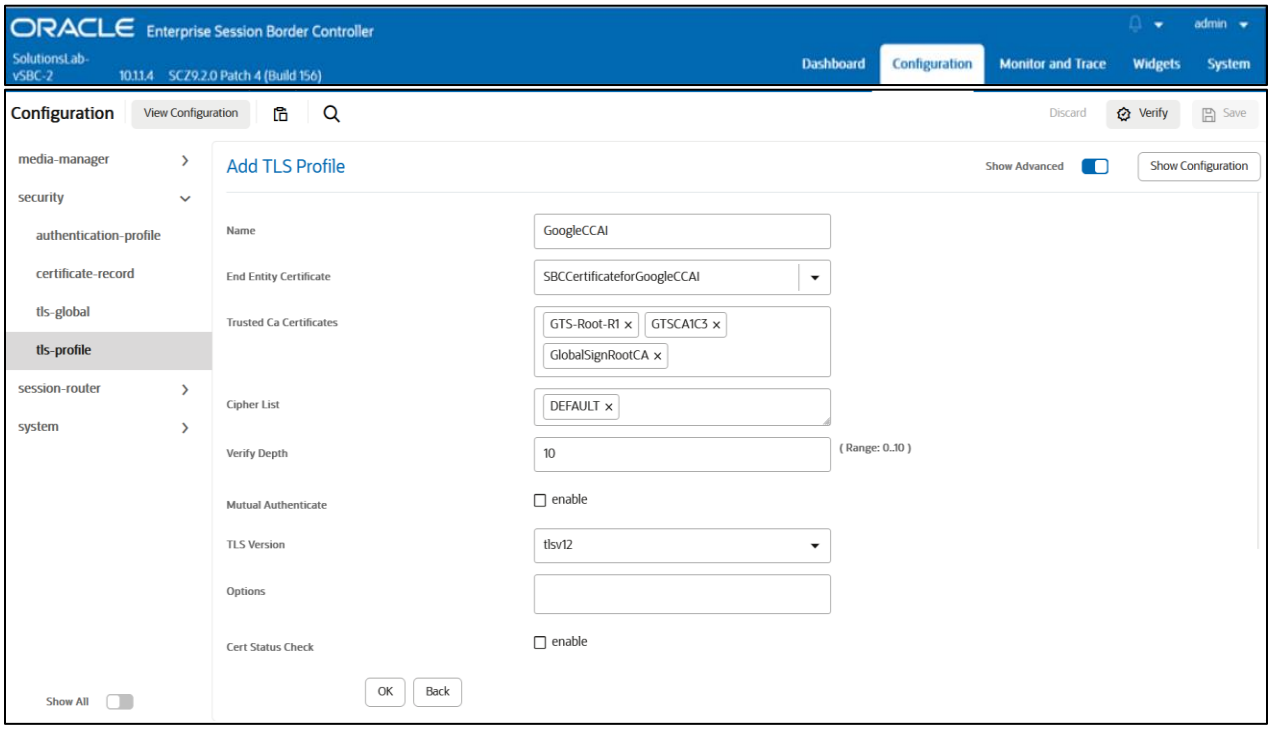




Repeat these steps to import all the root and intermediate CA certificates into the SBC:
At this stage all the required certificates have been imported to the SBC for GoogleCCAI.

6.10. TLS-Profile

A TLS profile configuration on the SBC allows for specific certificates to be assigned.
Go to security-> TLS-profile config element and configure the tls-profile as shown below
The below is the TLS profile configured for the Google CCAI side:

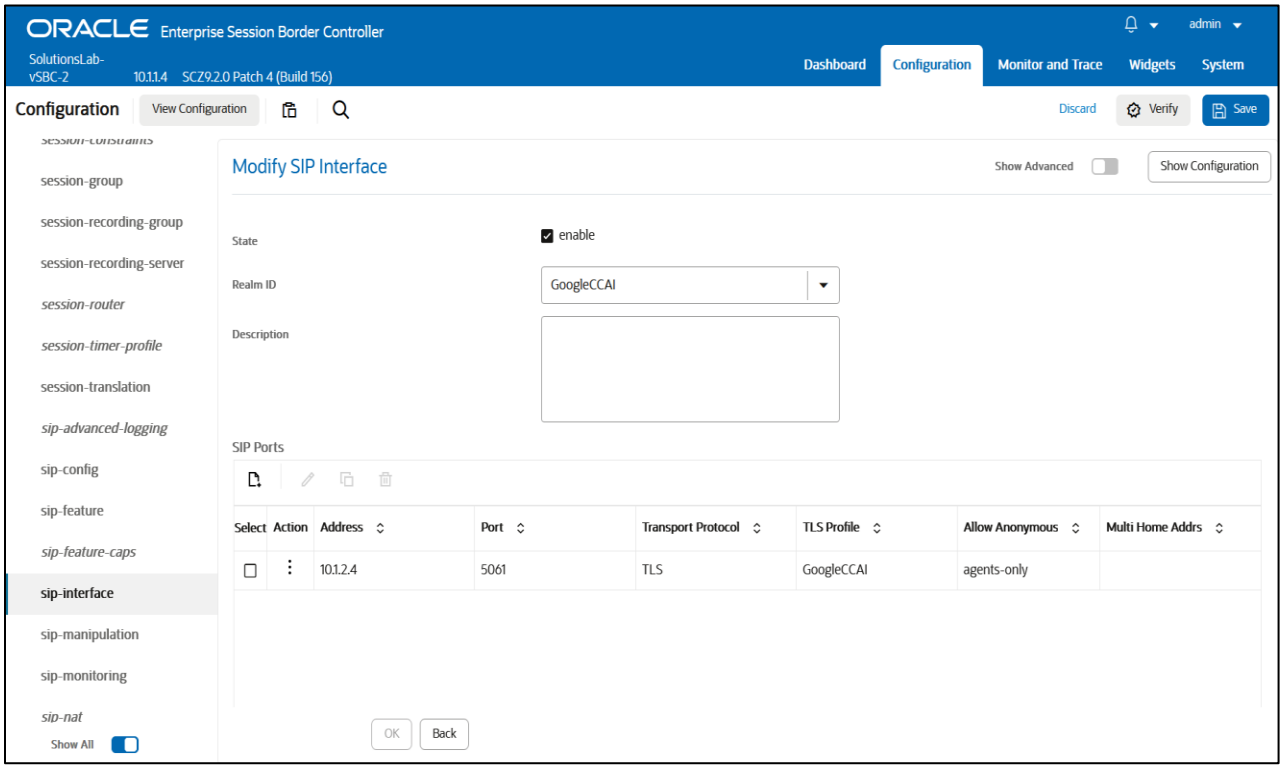


6.11. Configure SIP Interfaces

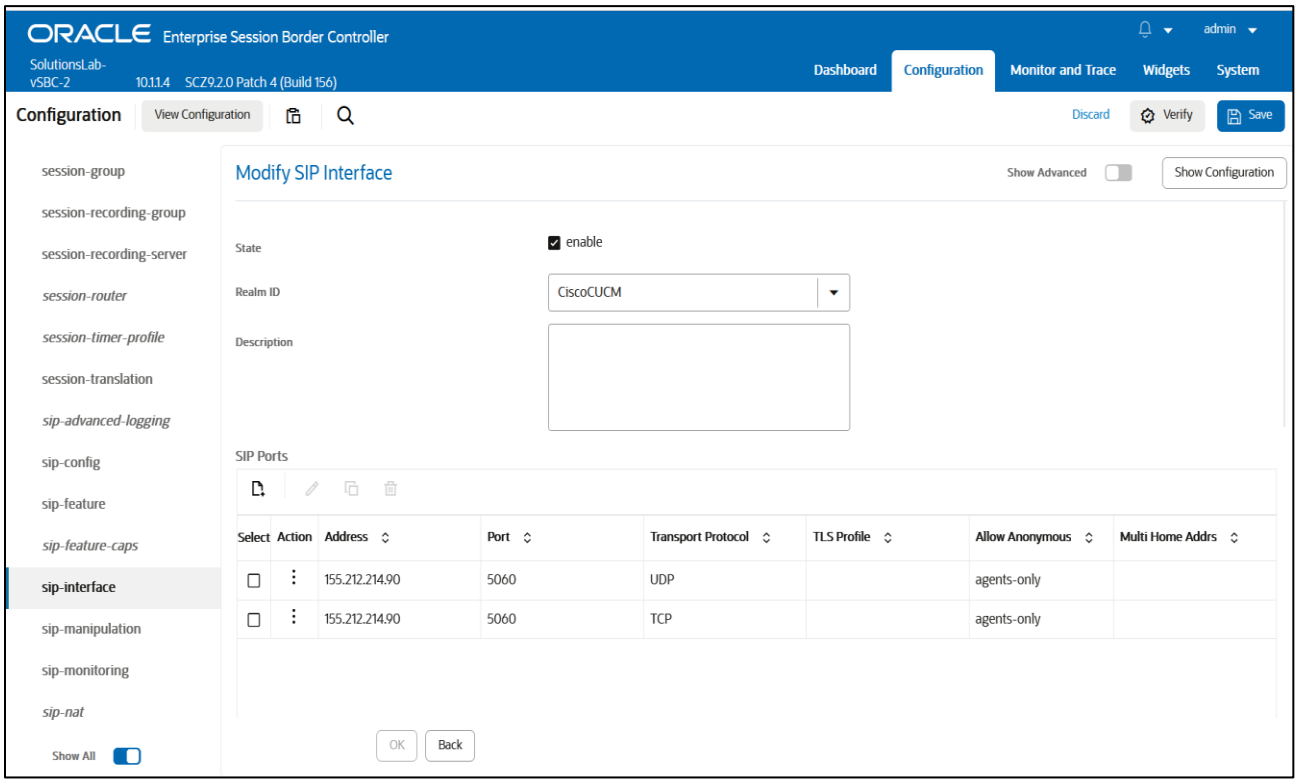
Navigate to sip-interface under session-router and configure the sip-interface as shown below.
Please configure the below settings under the sip-interface.

Please Configure sip-interface for the Google CCAI side as below:

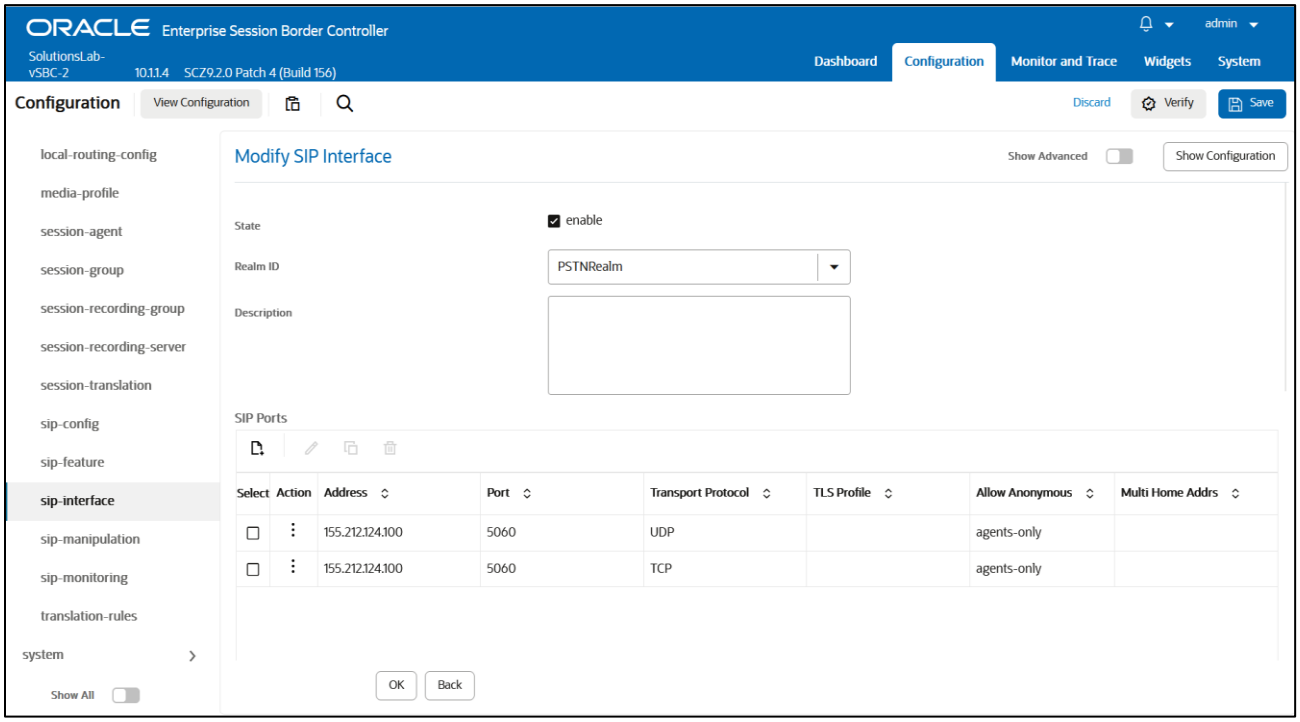
- Tls-profile needs to match the name of the tls-profile previously created
- Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from the particular Session agents added to the SBC.



Similarly, Please Configure sip-interface for the IP-PBX side as below:



Please Configure sip-interface for the PSTN side as below:



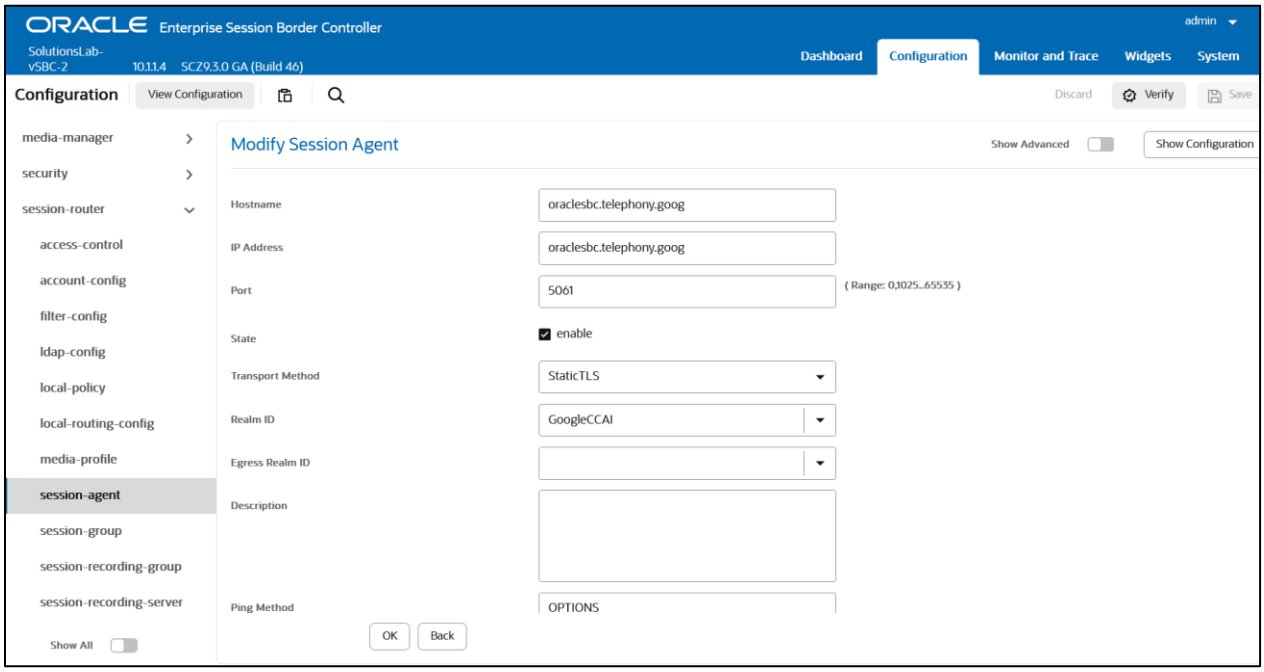
Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

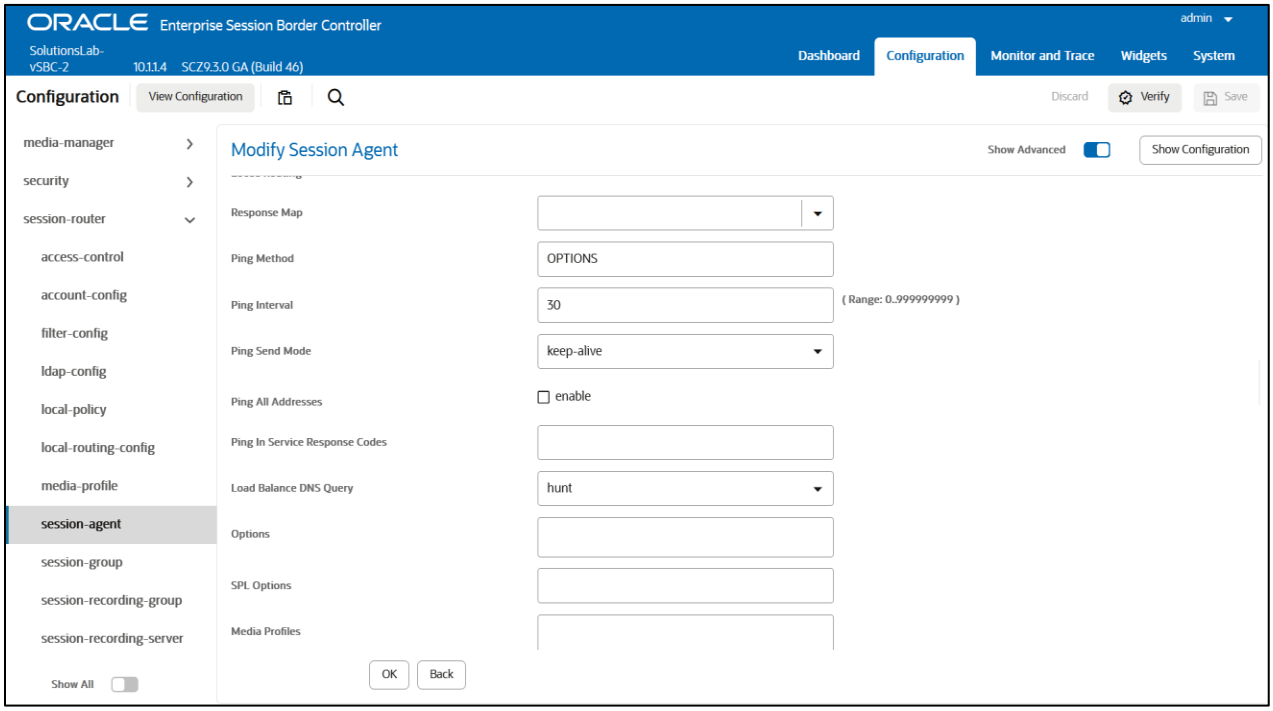
6.12. Configure session-agent

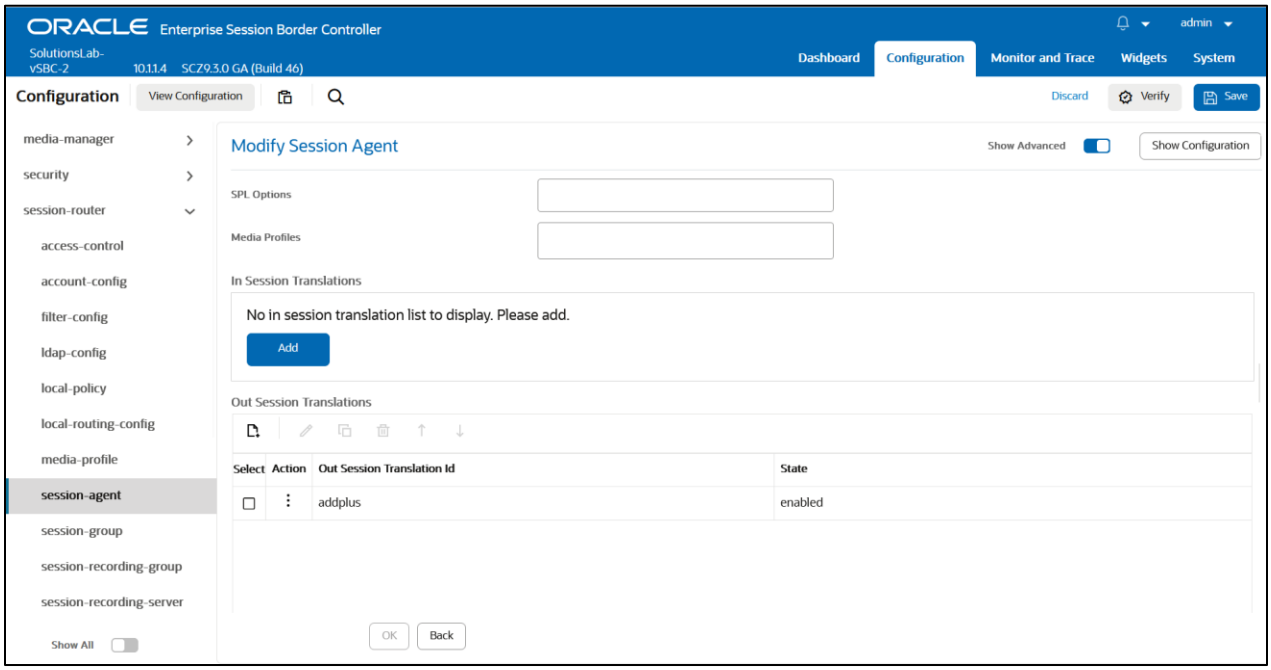
Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

Go to session-router->Session-Agent and Configure the session-agents for the Google CCAI side
.

- transport set to “staticTLS”
- Please enable the parameter **ping-response**,
- Please set ping method to OPTIONS and ping-interval duration in secs.

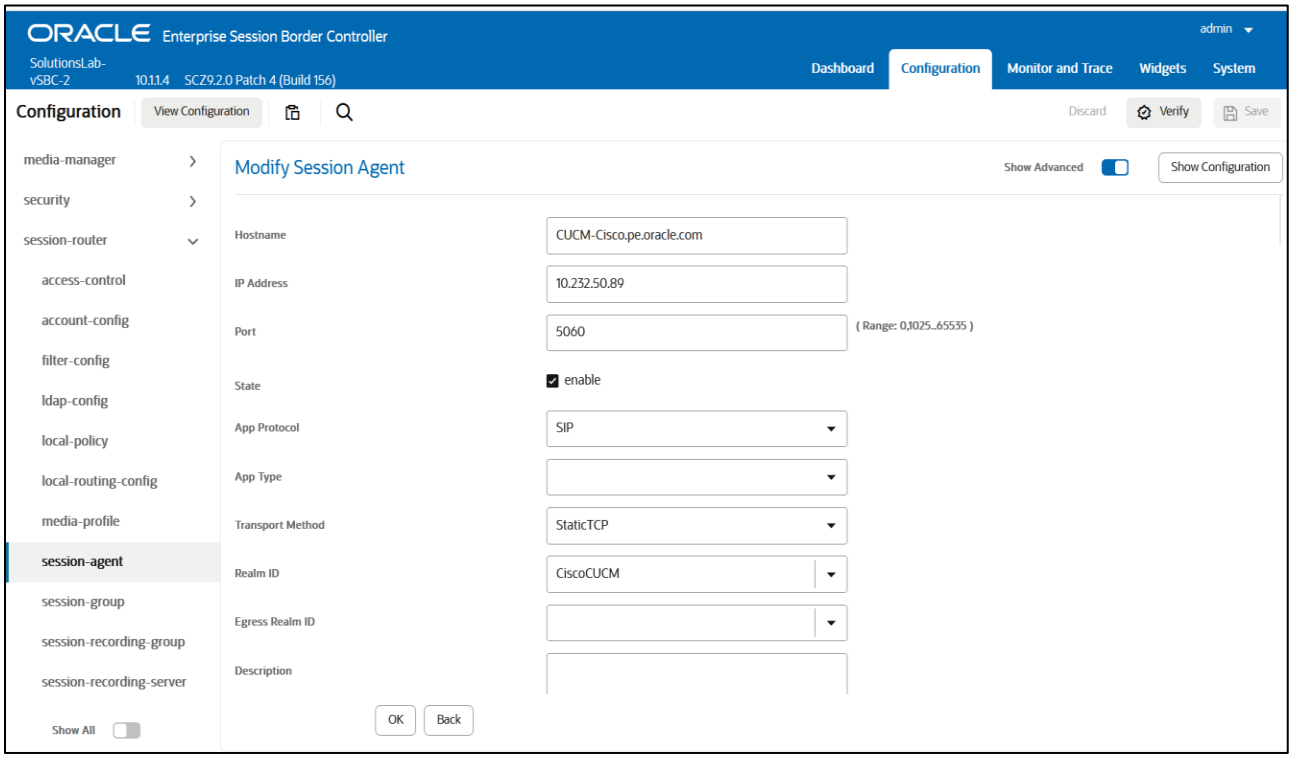

ORACLE Enterprise Session Border Controller
admin
SolutionsLab-vSBC-2 10.1.1.4 SCZ9.3.0 GA (Build 46)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
Save
media-manager
security
session-router
access-control
account-config
filter-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
Show All
Modify Session Agent
Show Advanced
Show Configuration
Hostname
oraclesbc.telephony.goog
IP Address
oraclesbc.telephony.goog
Port
5061
(Range: 0,1025..65535)
State
enable
Transport Method
StaticTLS
Realm ID
GoogleCCAI
Egress Realm ID
Description
Ping Method
OPTIONS
OK
Back

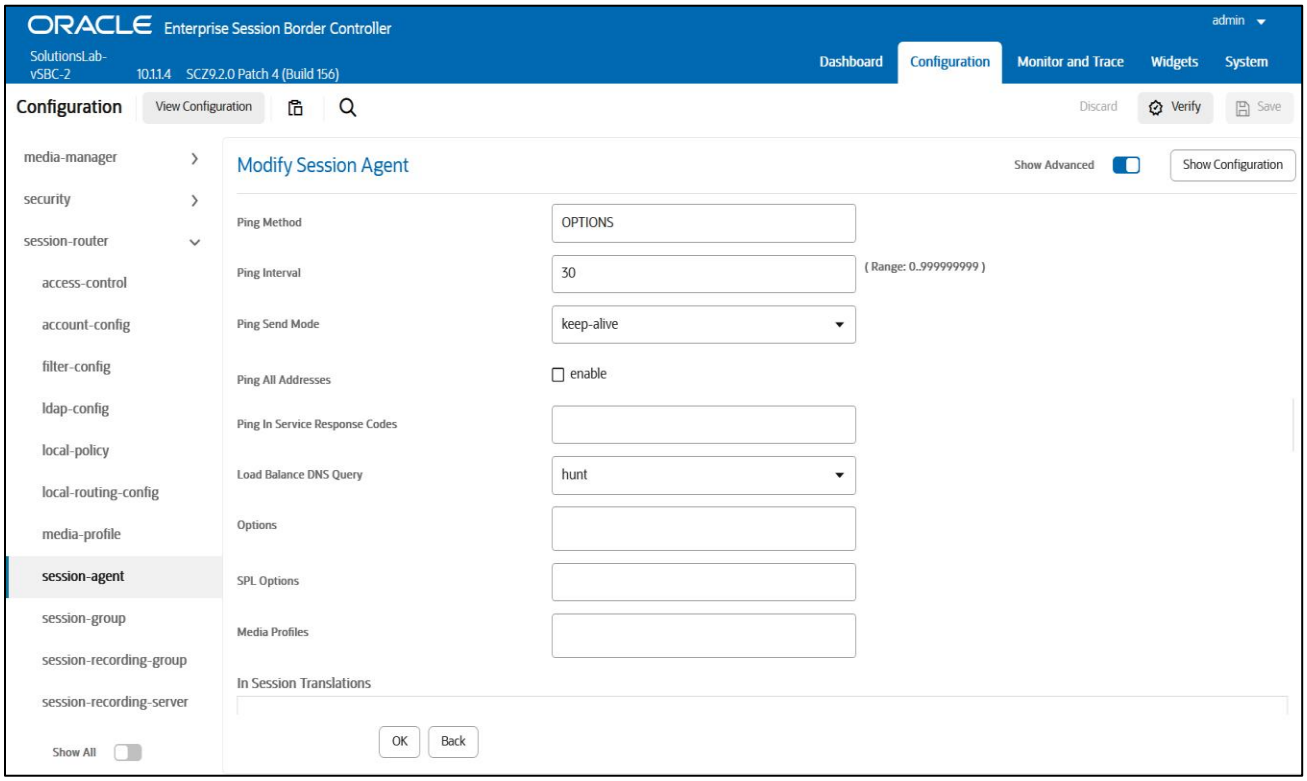

ORACLE Enterprise Session Border Controller
admin
SolutionsLab-vSBC-2 10.1.1.4 SCZ9.3.0 GA (Build 46)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
Save
media-manager
security
session-router
access-control
account-config
filter-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
Show All
Modify Session Agent
Show Advanced
Show Configuration
Response Map
Ping Method
OPTIONS
Ping Interval
30
(Range: 0..999999999)
Ping Send Mode
keep-alive
Ping All Addresses
enable
Ping In Service Response Codes
Load Balance DNS Query
hunt
Options
SPL Options
Media Profiles
OK
Back



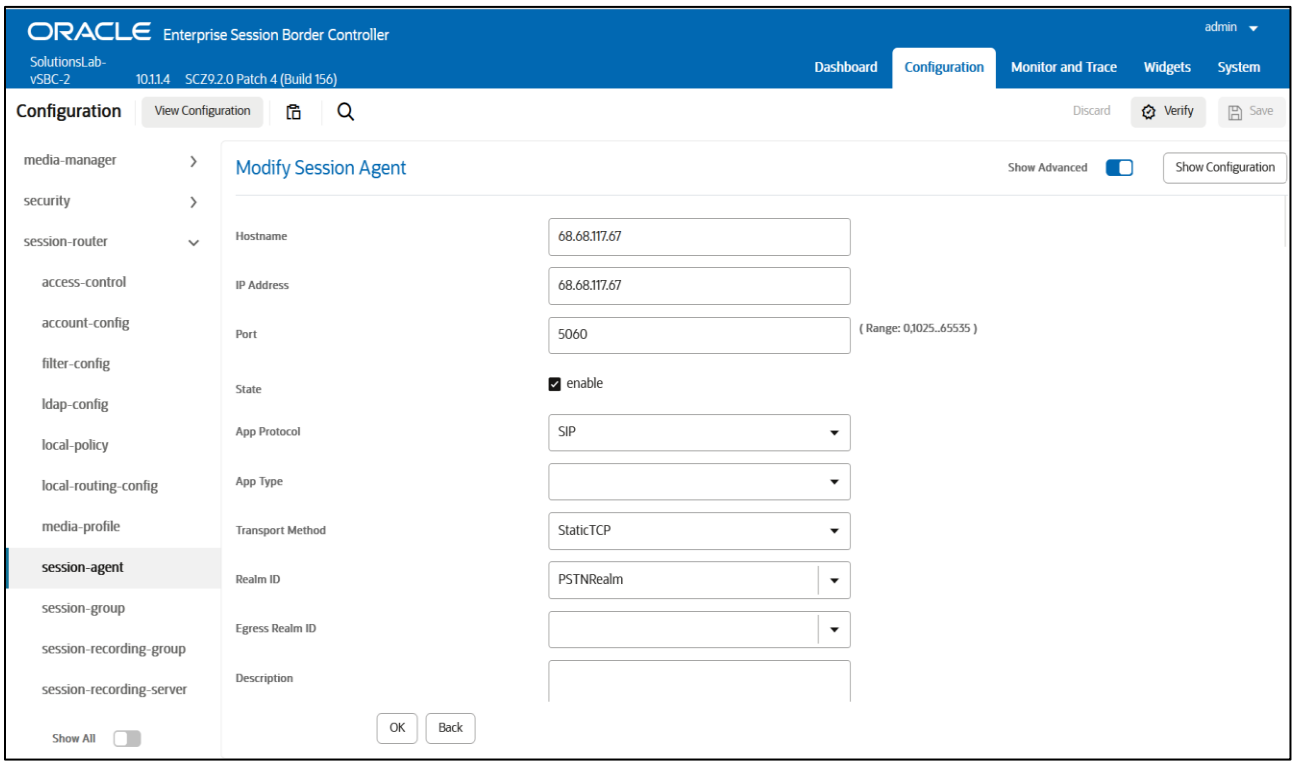
Similarly, configure the session-agents for the IP-PBX Side as below:

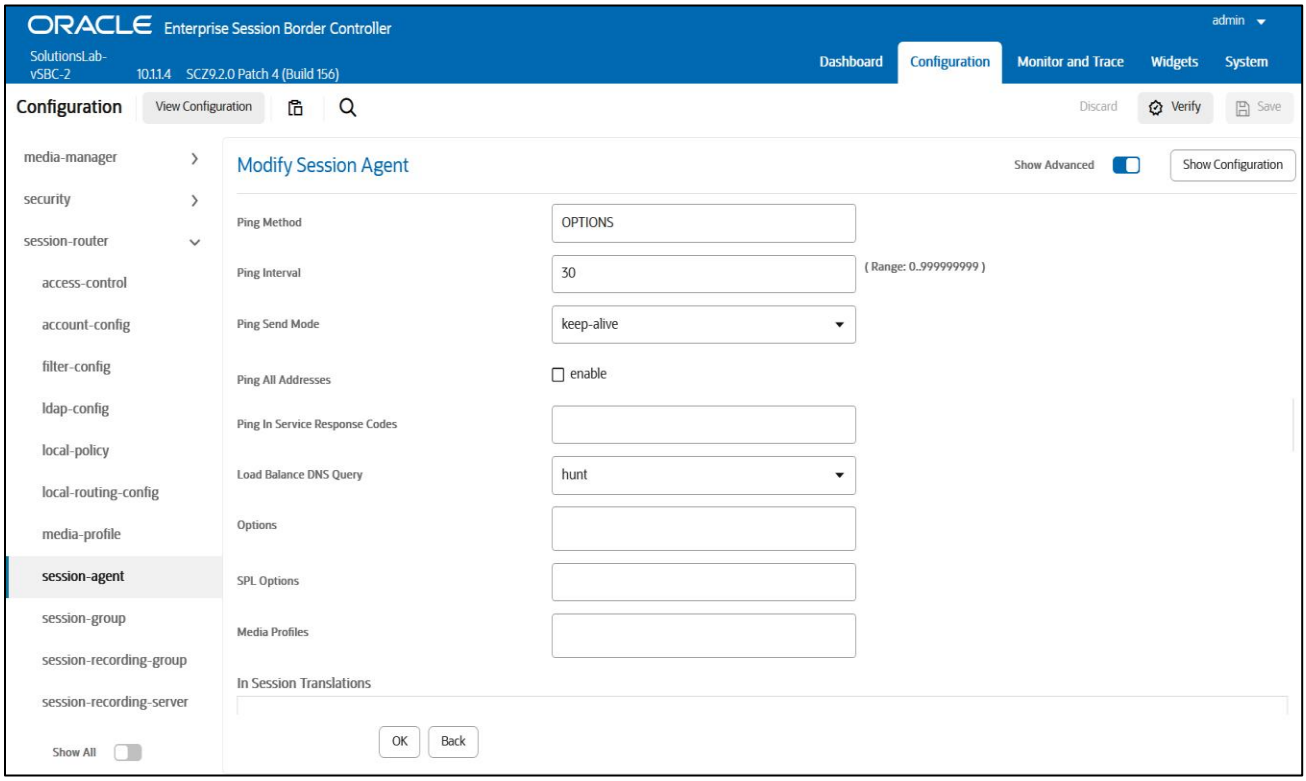
- Host name to FQDN of CUCM which is “CUCM-Cisco.pe.oracle.com” in our example. **We can also give Cisco CUCM IP address if there is no host name configured.**


ORACLE Enterprise Session Border Controller
admin
SolutionsLab-vSBC-2 10.1.1.4 SCZ9.2.0 Patch 4 (Build 156)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
Save
media-manager
security
session-router
access-control
account-config
filter-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
Show All
Modify Session Agent
Show Advanced
Show Configuration
Hostname
CUCM-Cisco.pe.oracle.com
IP Address
10.232.50.89
Port
5060
(Range: 0,1025..65535)
State
enable
App Protocol
SIP
App Type
Transport Method
StaticTCP
Realm ID
CiscoCUCM
Egress Realm ID
Description
OK
Back


ORACLE Enterprise Session Border Controller
admin
SolutionsLab-vSBC-2 10.1.1.4 SCZ9.2.0 Patch 4 (Build 156)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
Save
media-manager
security
session-router
access-control
account-config
filter-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
Show All
Modify Session Agent
Show Advanced
Show Configuration
Ping Method
OPTIONS
Ping Interval
30
(Range: 0..999999999)
Ping Send Mode
keep-alive
Ping All Addresses
enable
Ping In Service Response Codes
Load Balance DNS Query
hunt
Options
SPL Options
Media Profiles
In Session Translations
OK
Back

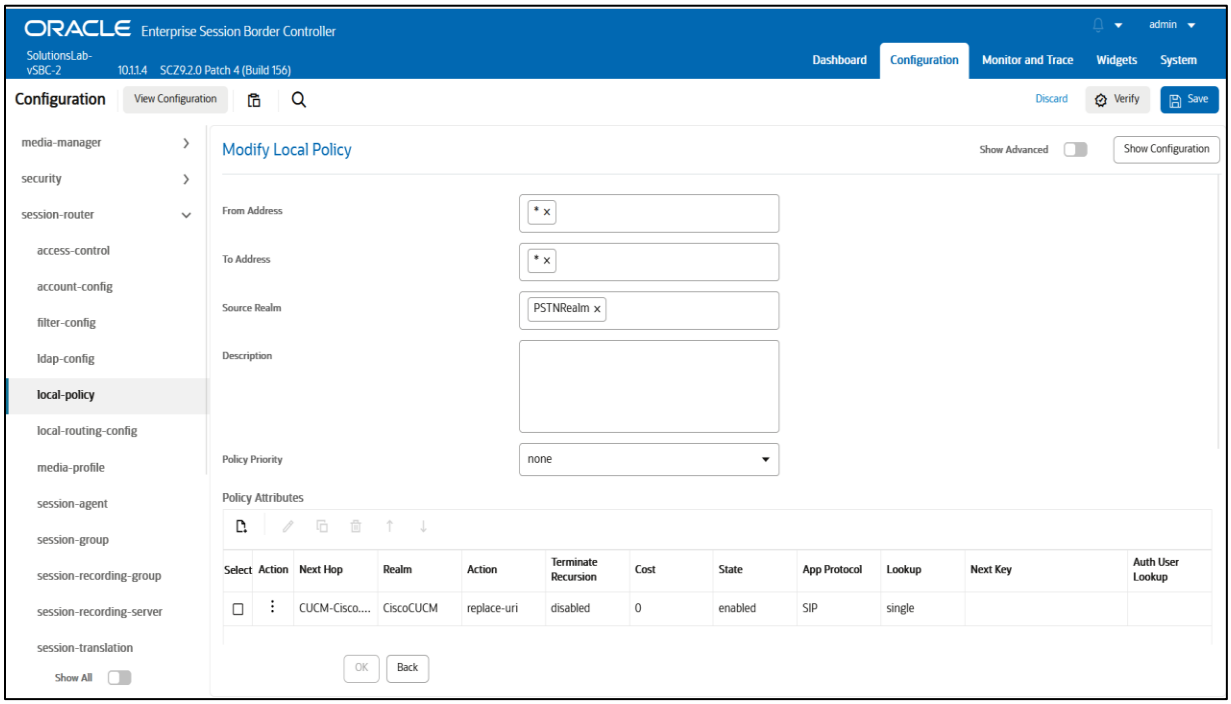
Similarly, configure the session-agents for the PSTN Side as below:



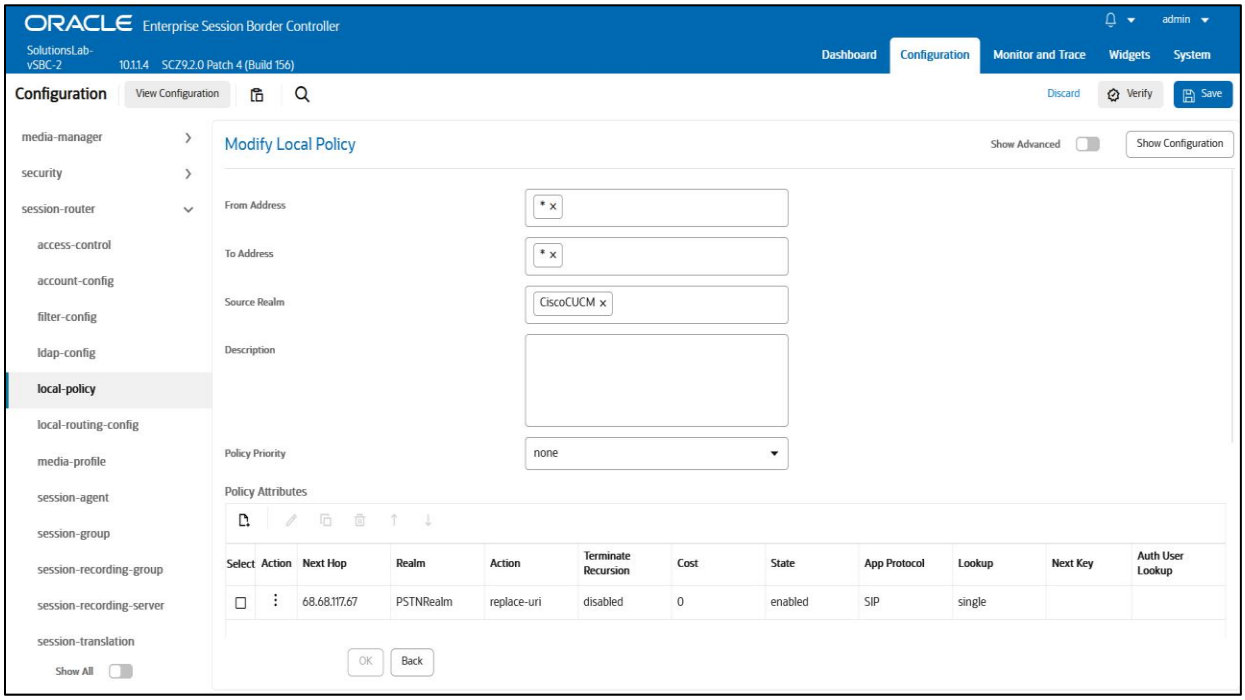


6.13. Configure local-policy

Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.
To route the calls from PSTN side to IP-PBX side, Use the below local –policy

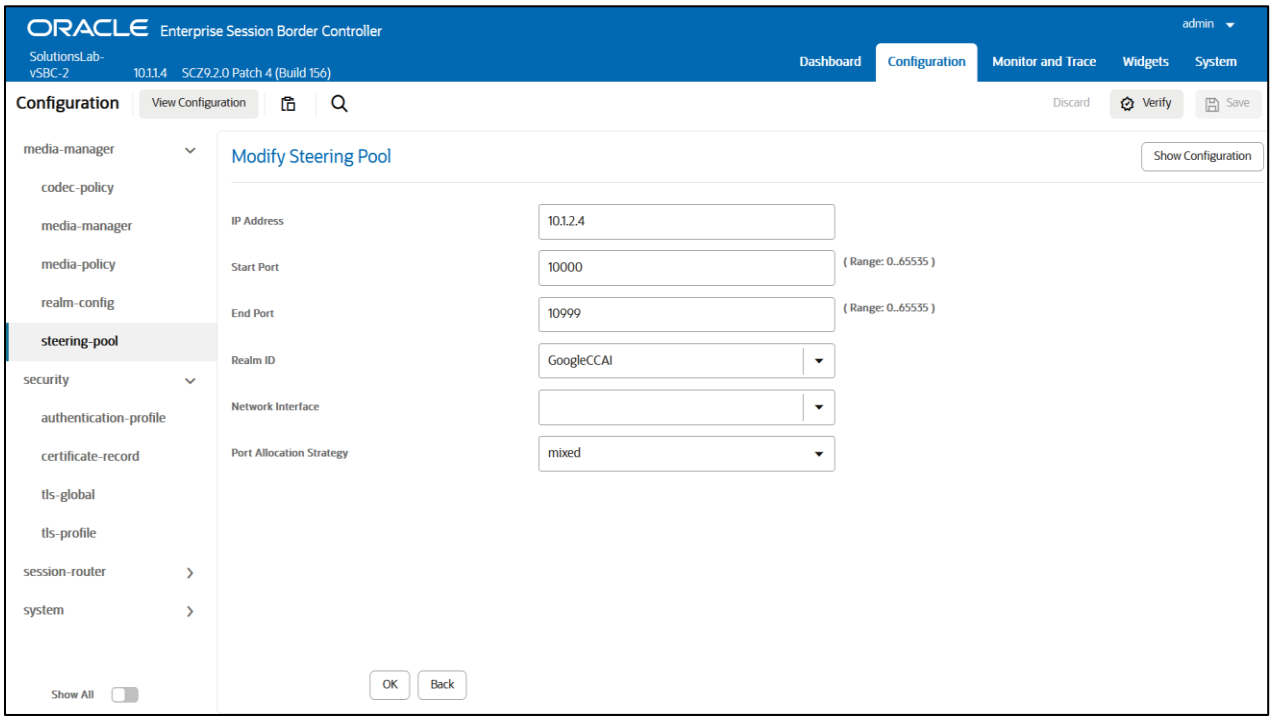


To route the calls from IP-PBX side to PSTN side, Use the below local–policy

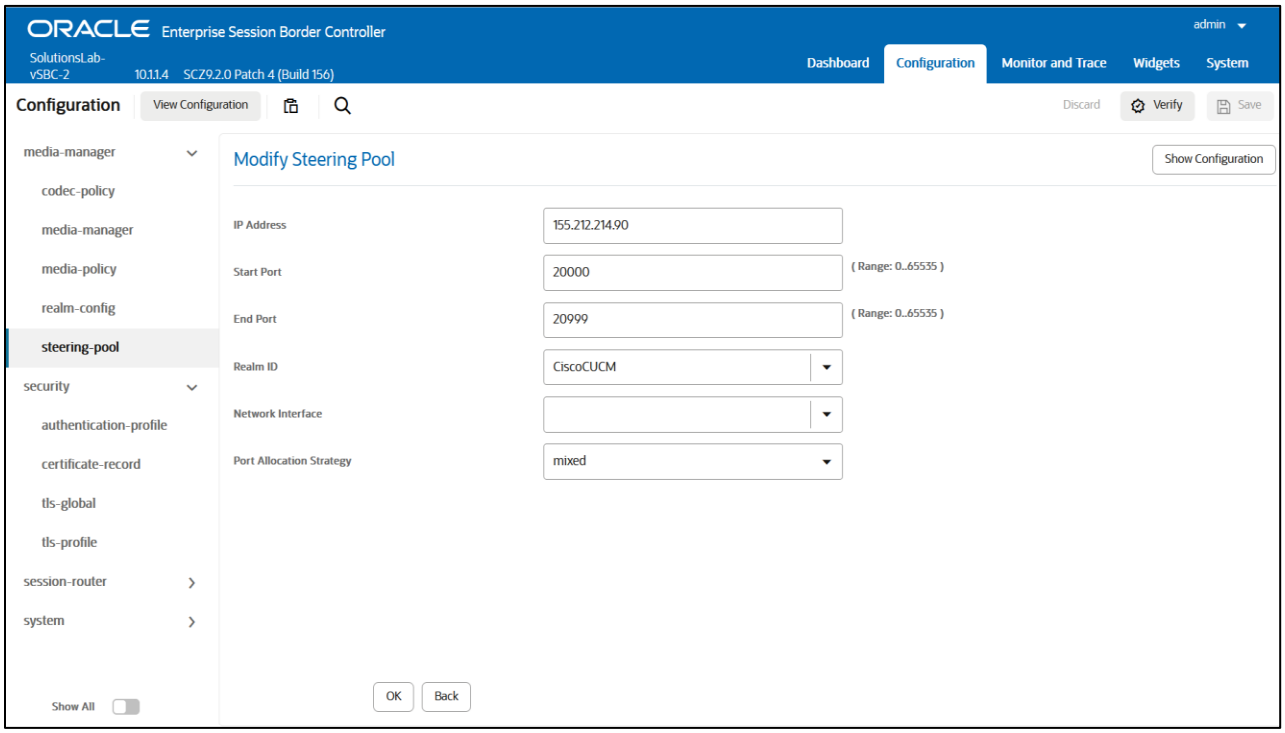


6.14. Configure steering-pool

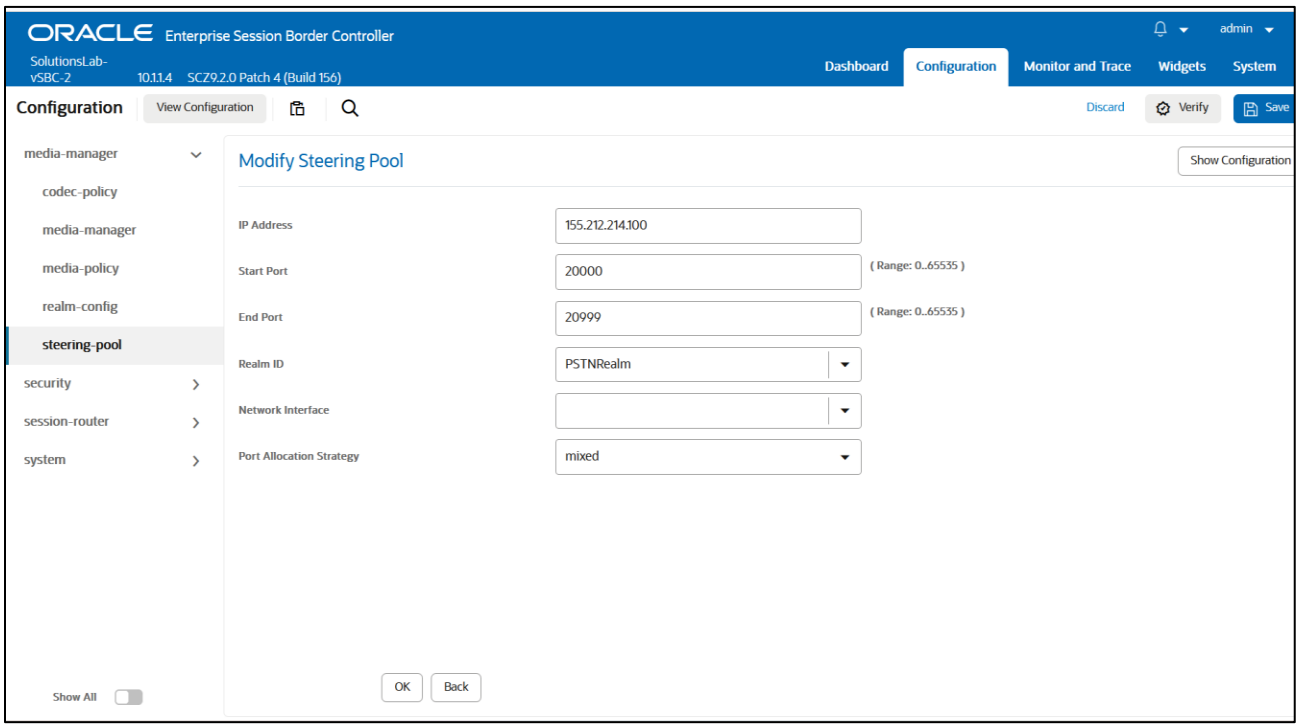
Google CCAI side steering pool.



IP-PBX side steering pool.

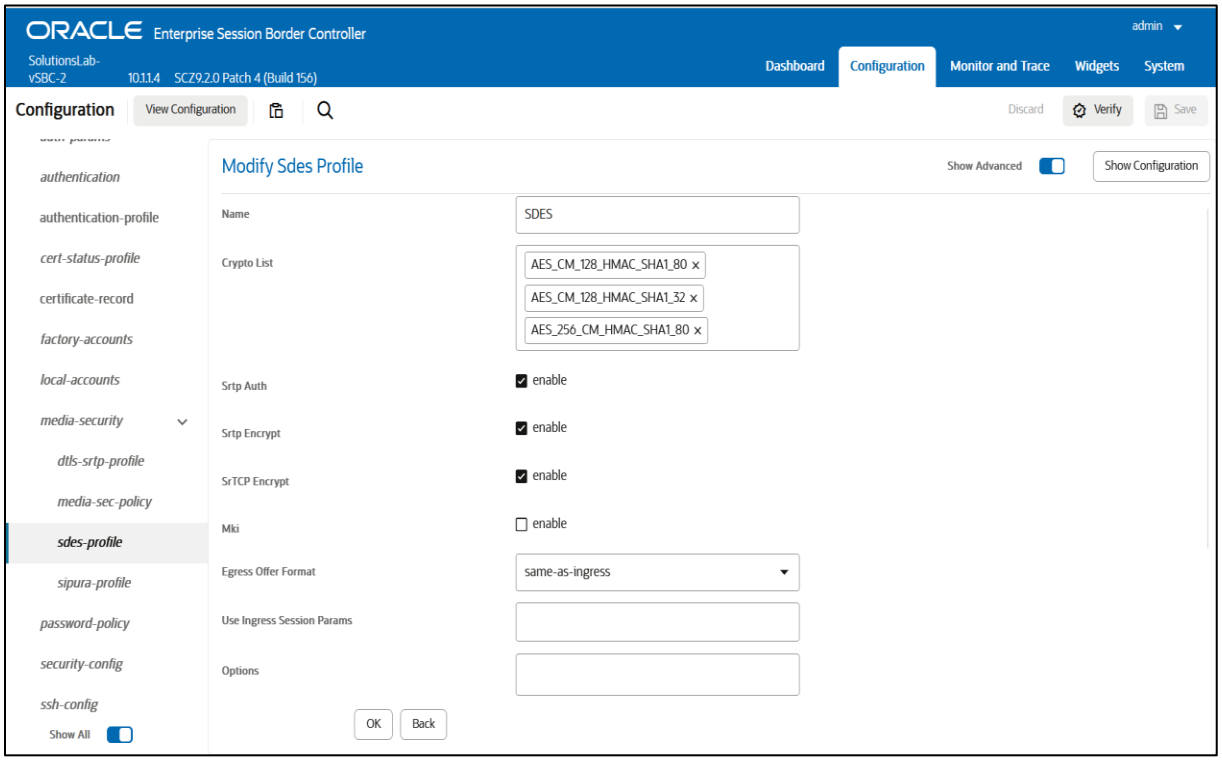


PSTN side steering pool.



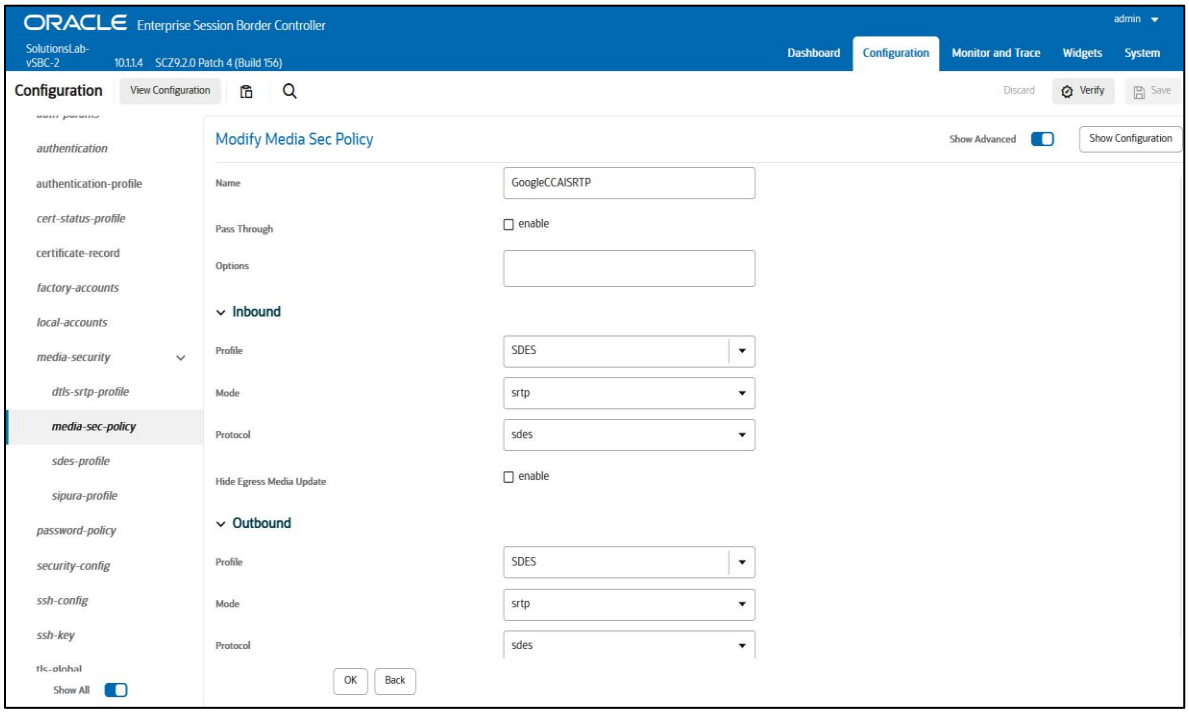
6.15. Configure sdes profile

Please go to →Security → Media Security →sdes profile and create the policy as below.

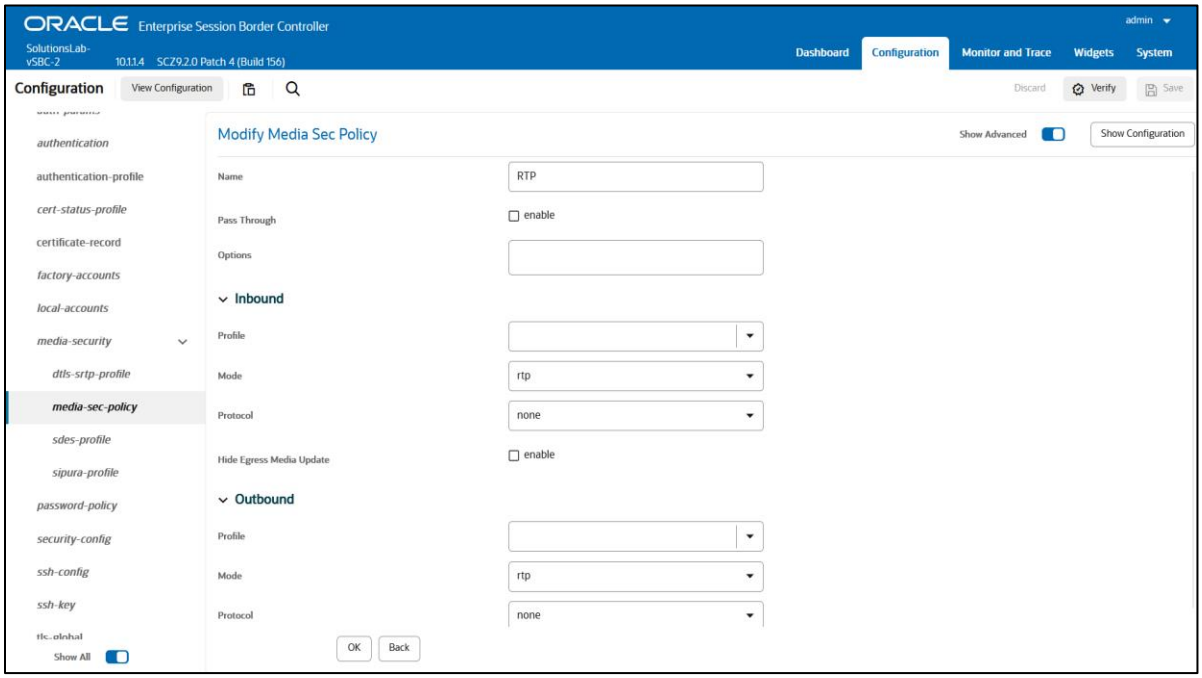


6.16. Configure Media Security Profile

Please go to →Security → Media Security →media Sec policy and create the policy as below:
Create Media Sec policy with name GoogleCCAISRTP which will have the sdes profile created above.
Assign this media policy to the GoogleCCAI Realm

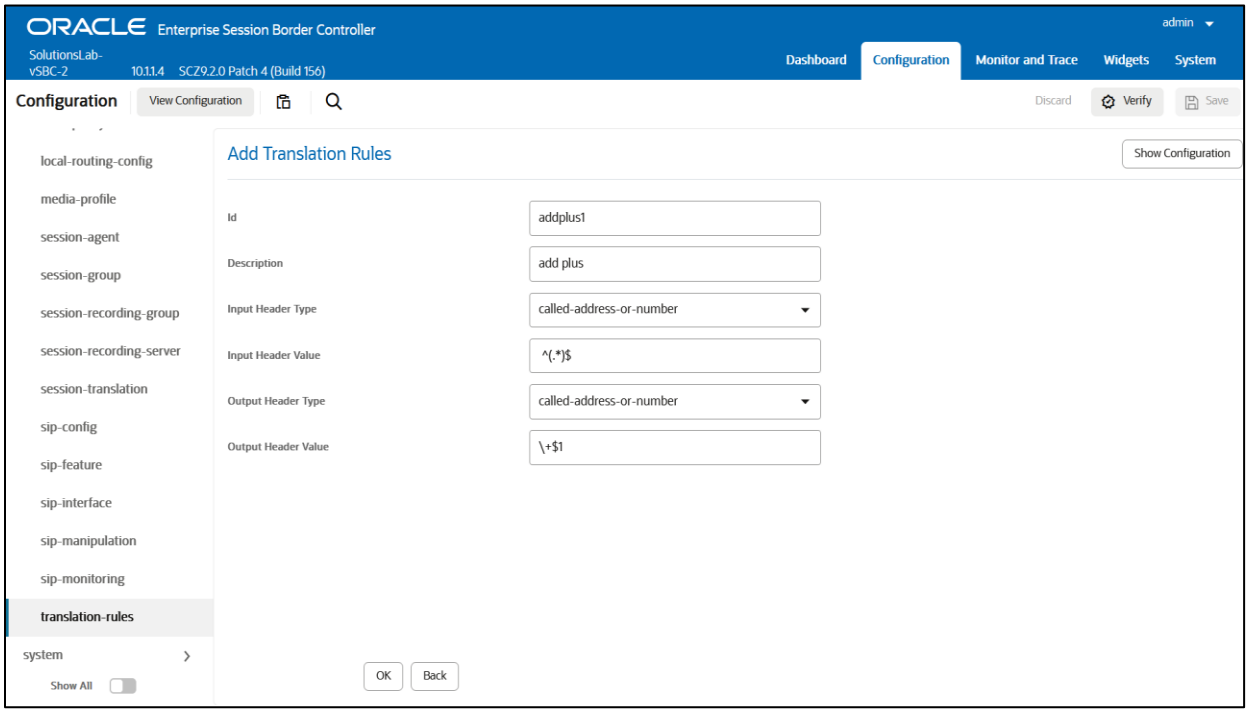


Similarly, Create Media Sec policy with name RTP to convert srtp to rtp for the IP-PBX side which will use only TCP/UDP as transport protocol. **Assign this media policy to the IP-PBX Realm.**



6.17. Configure Translation Rules

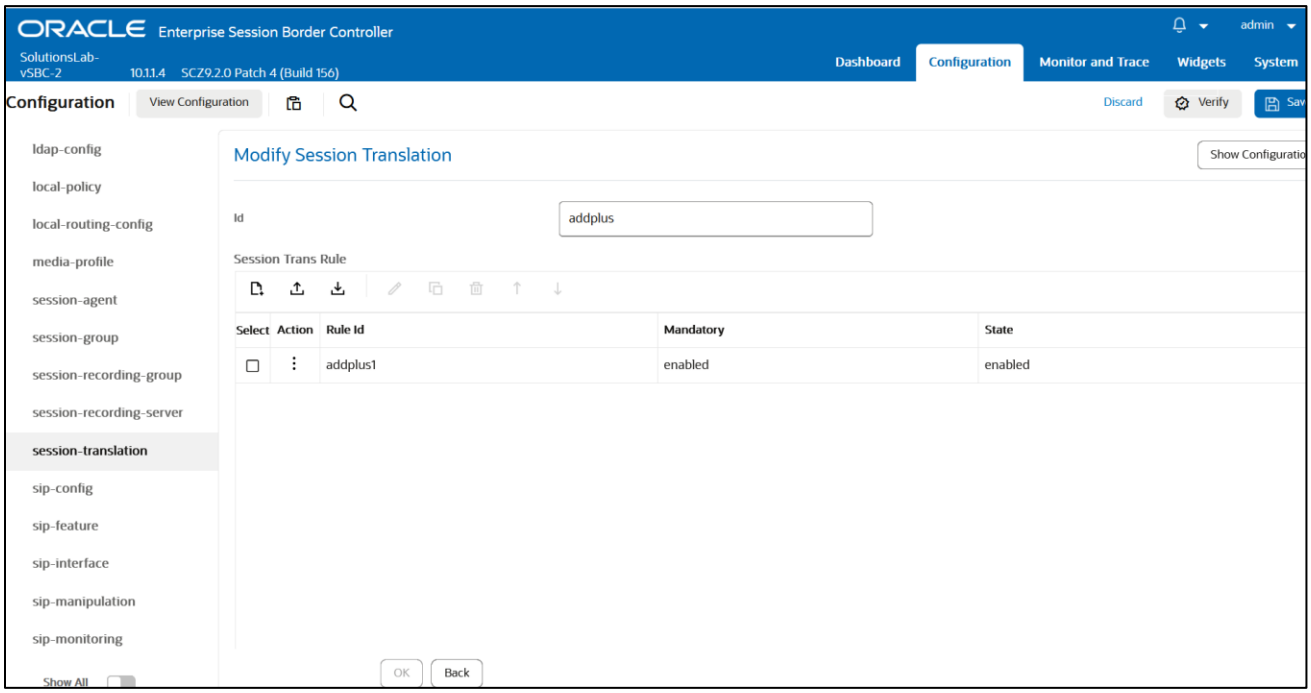
The translation rules sub-element is where the actual translation rules are created.
Go to Session router → translation-rules and create the below rule.



6.18. Configure Session Translation Rules

A session translation defines how translation rules are applied to calling and called numbers.
Go to Session Router → session-translation and configure the below translation rules.

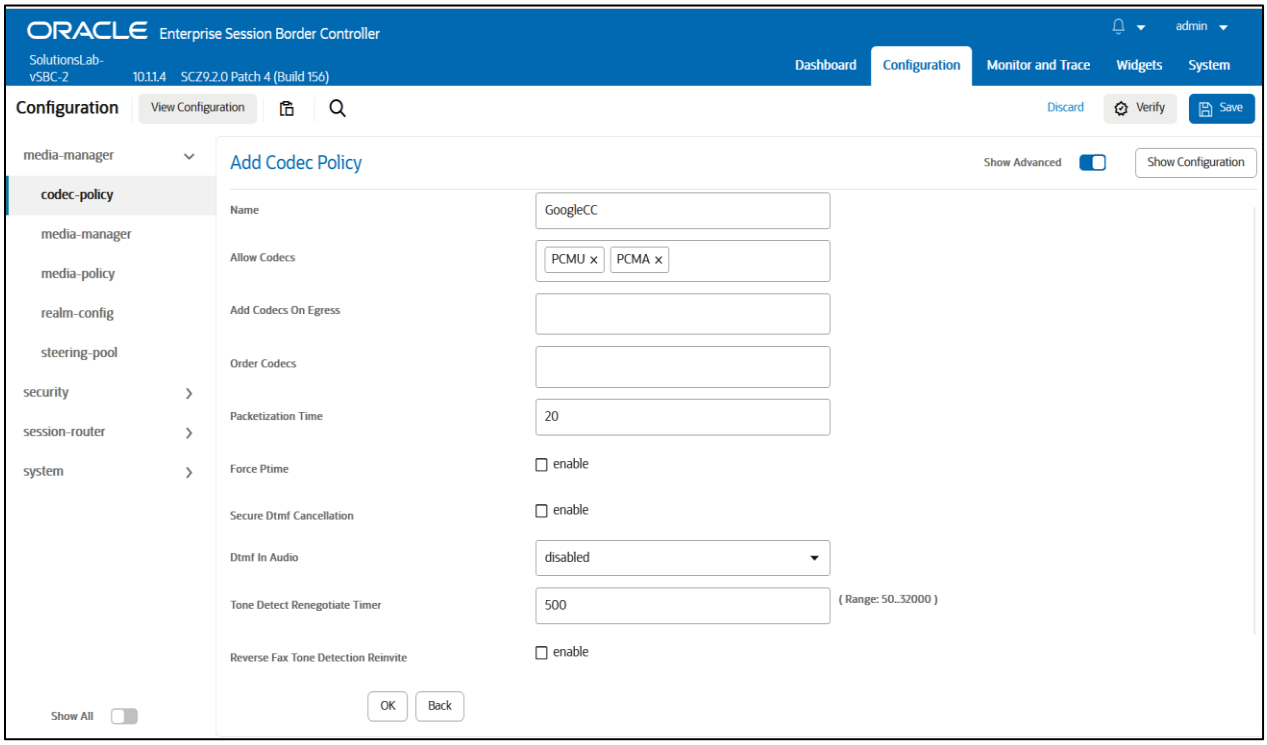
Add the below Session translation rule to Google side.
Apply this rule to the Session Agent of Google Side to take effect.



6.19. Configure Codec Policy

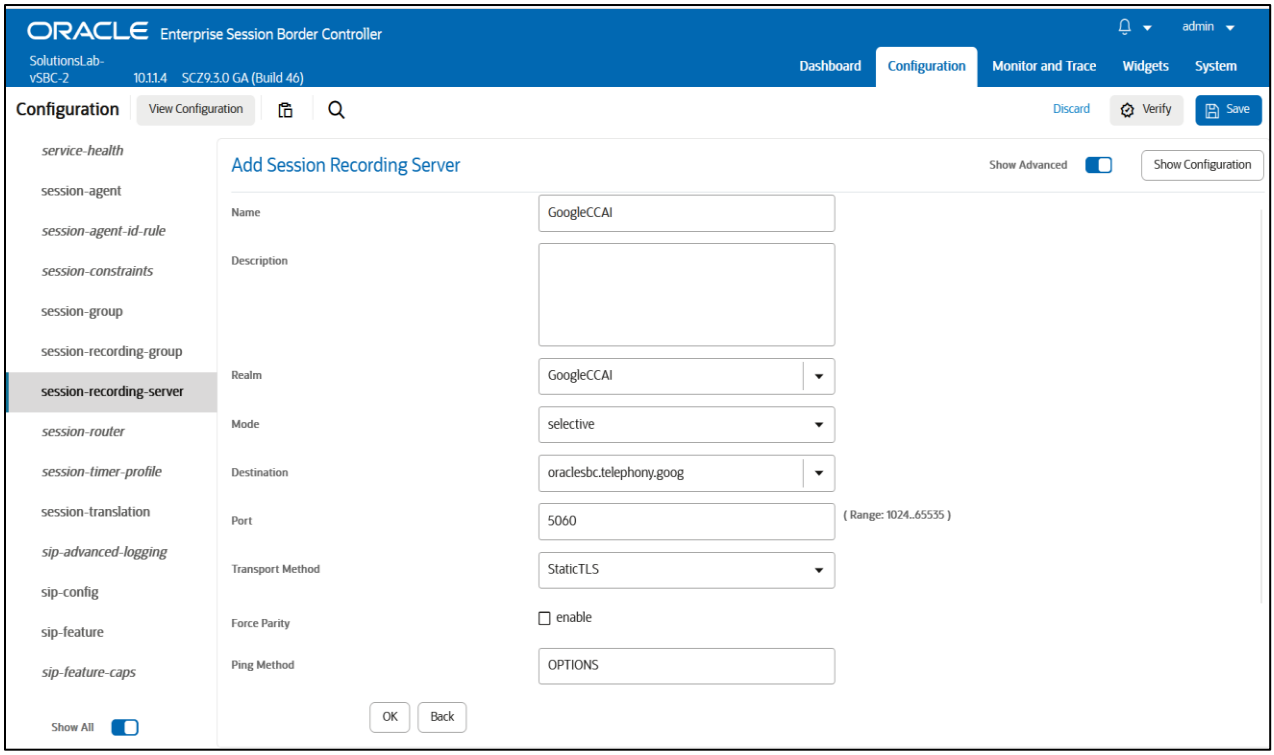
The Oracle Session Border Controller (SBC) uses codec policies to describe how to manipulate SDP messages as they cross the SBC. The SBC bases its decision to transcode a call on codec policy configuration and the SDP. Each codec policy specifies a set of rules to be used for determining what codecs are retained, removed, and how they are ordered within SDP.

Go to media manager ---- codec policy and apply this codec policy to the GoogleCCAI realm.



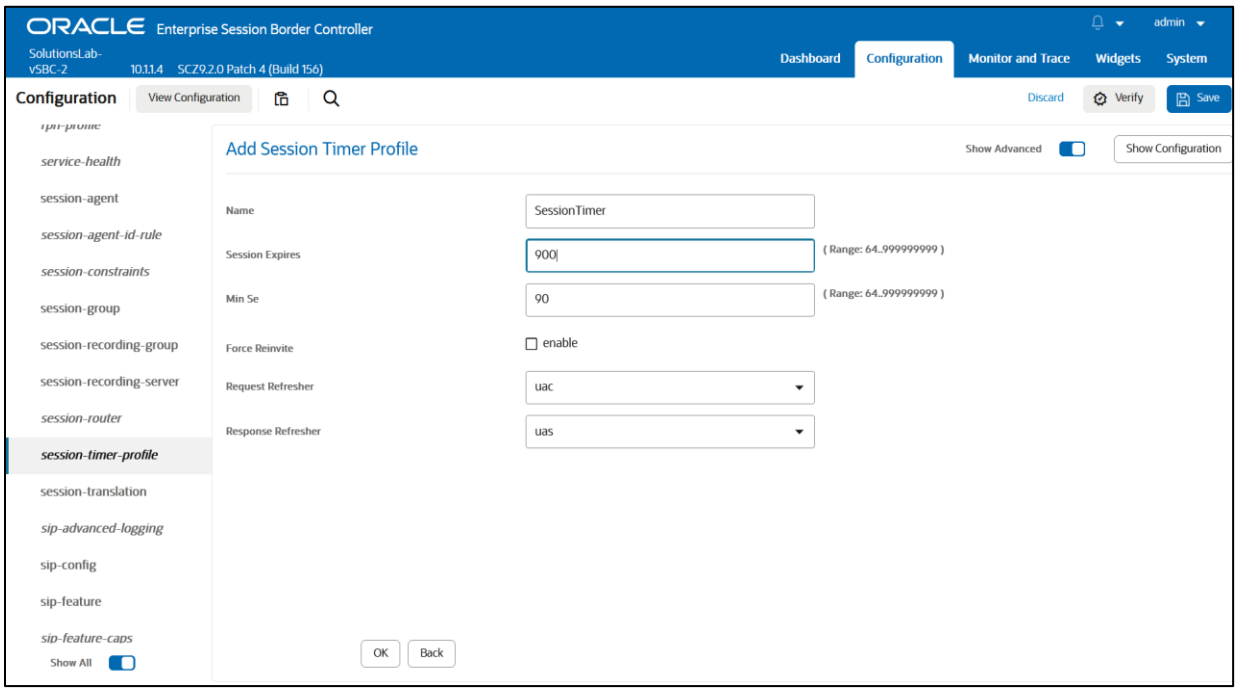
6.20. Configure Session Recording Server

SIPREC profile for Google CCAI is created using the Session Recording Server
Assign this profile to the IP-PBX Realm



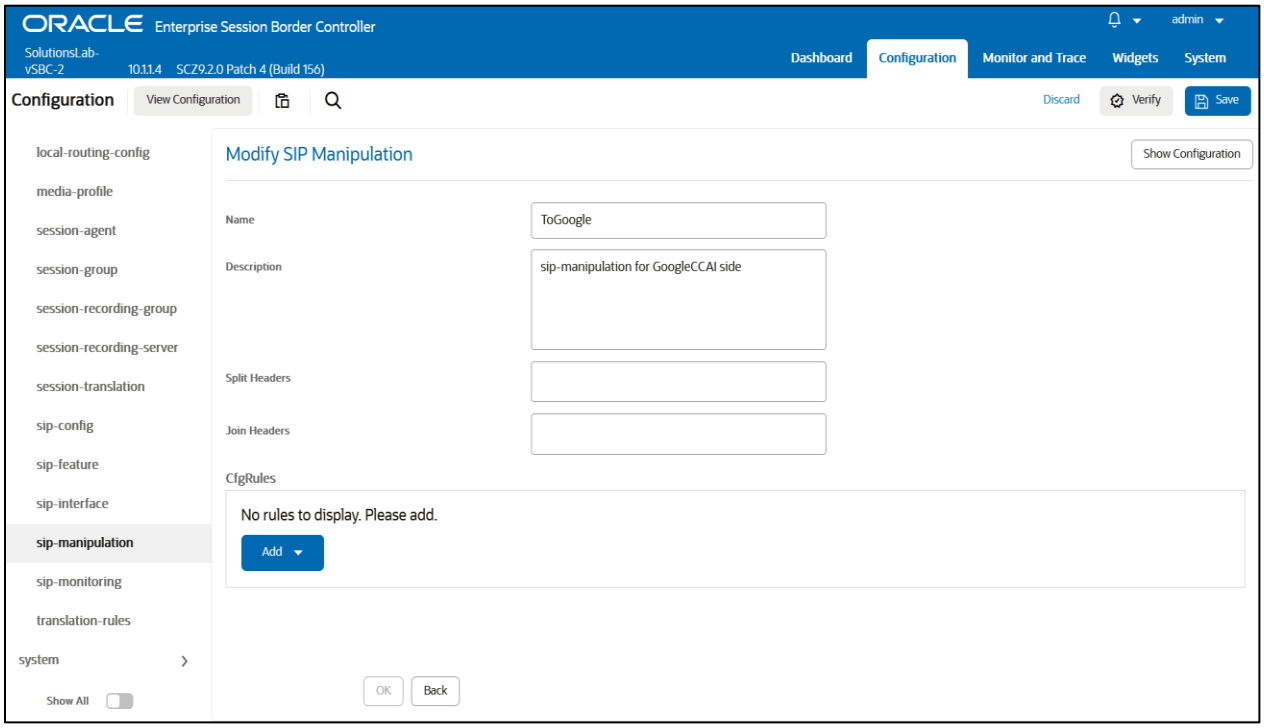
6.21. Configure Session Timer

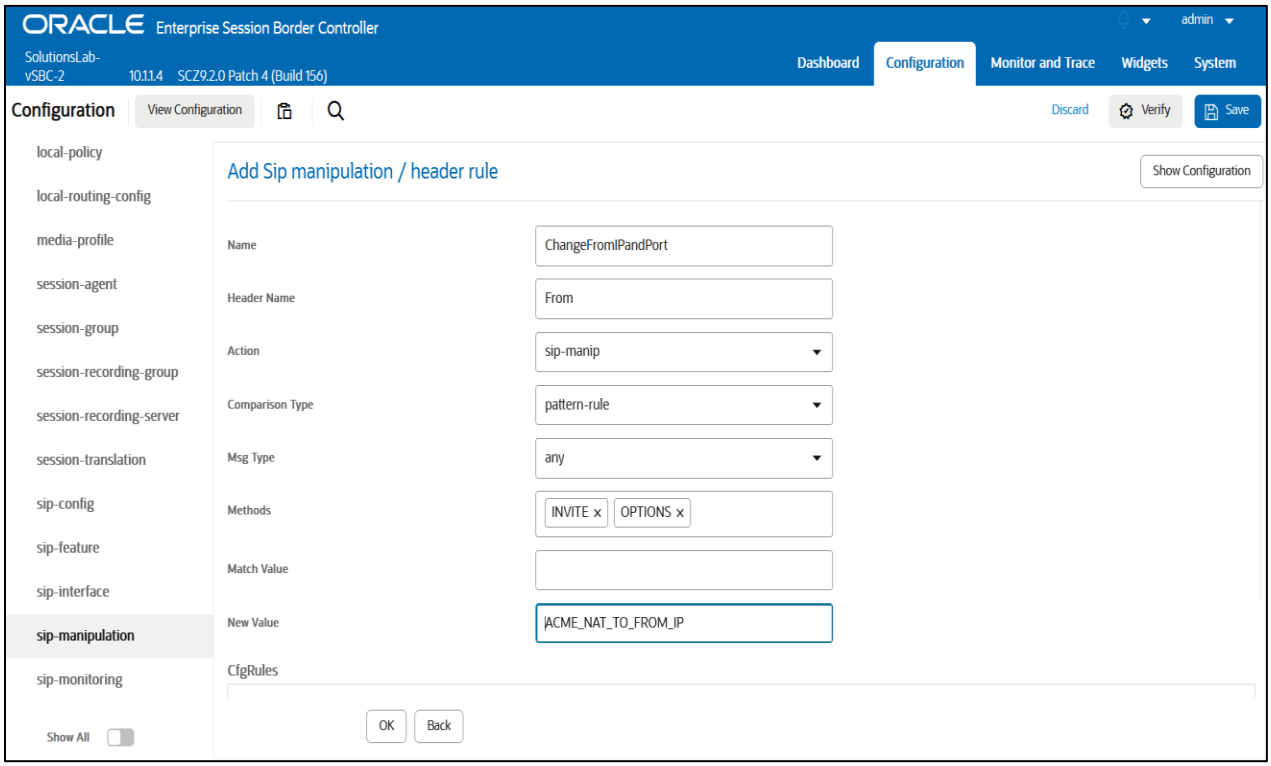
Navigate to Configuration > session-router > session-timer-profile.
Configure session timer for Google CCAI as shown below.
Assign this profile to the GogleCCAI Realm



6.22. Configure SIP-Manipulation

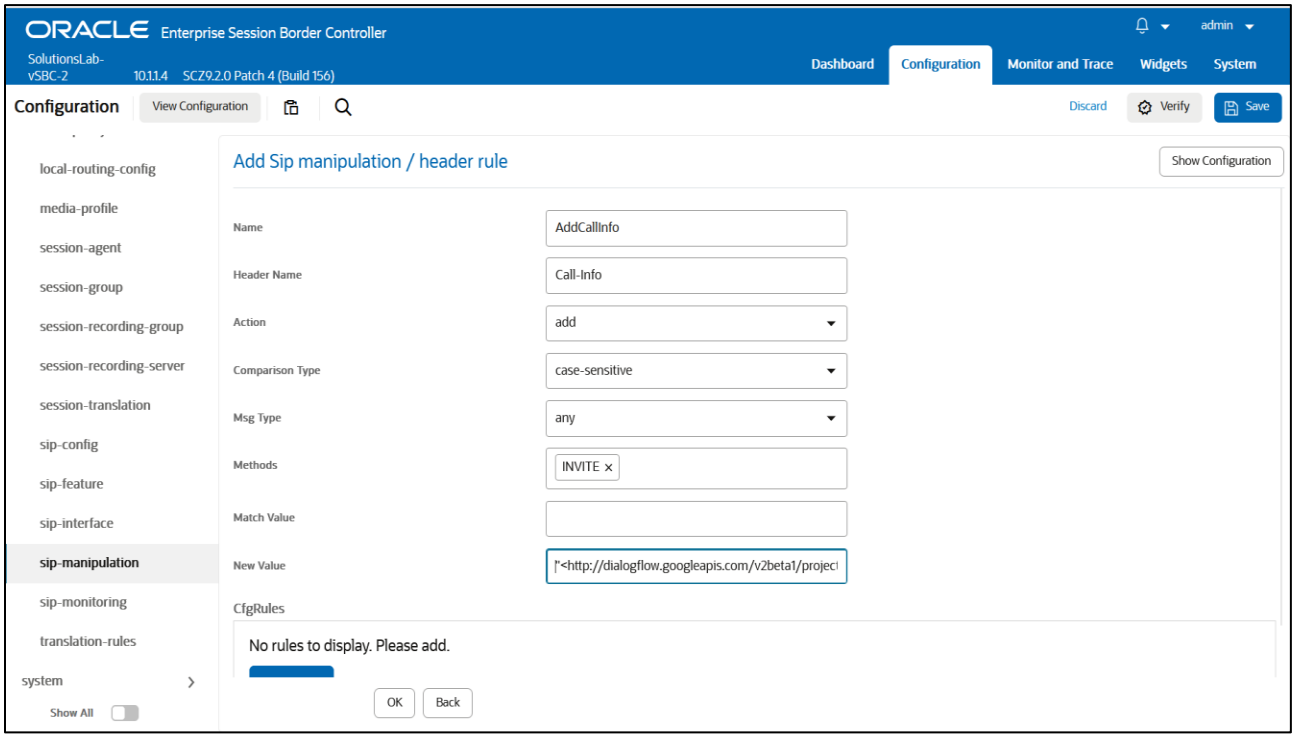
Navigate to Configuration > session-router > sip-manipulation
Configure SIP manipulation towards Google CCAI as shown below
Assign this ip-manipulation to the GoogleCCAI Realm.



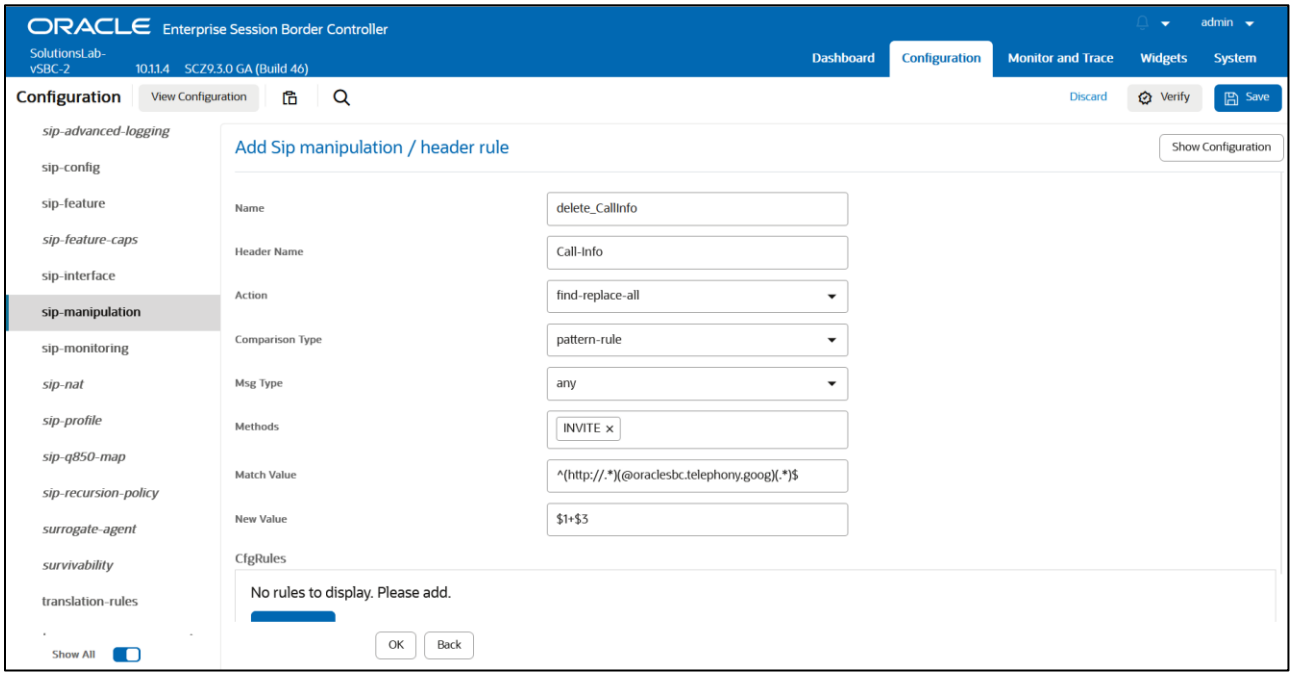


Below header rule is created to add Call-Info header towards Google CCAI with the Dialog Flow API request along with the Conversation ID. “Conversation on the Fly” is set to True in Google CCAI using REST API. Conversation ID is randomly generated by Oracle SBC for each call.

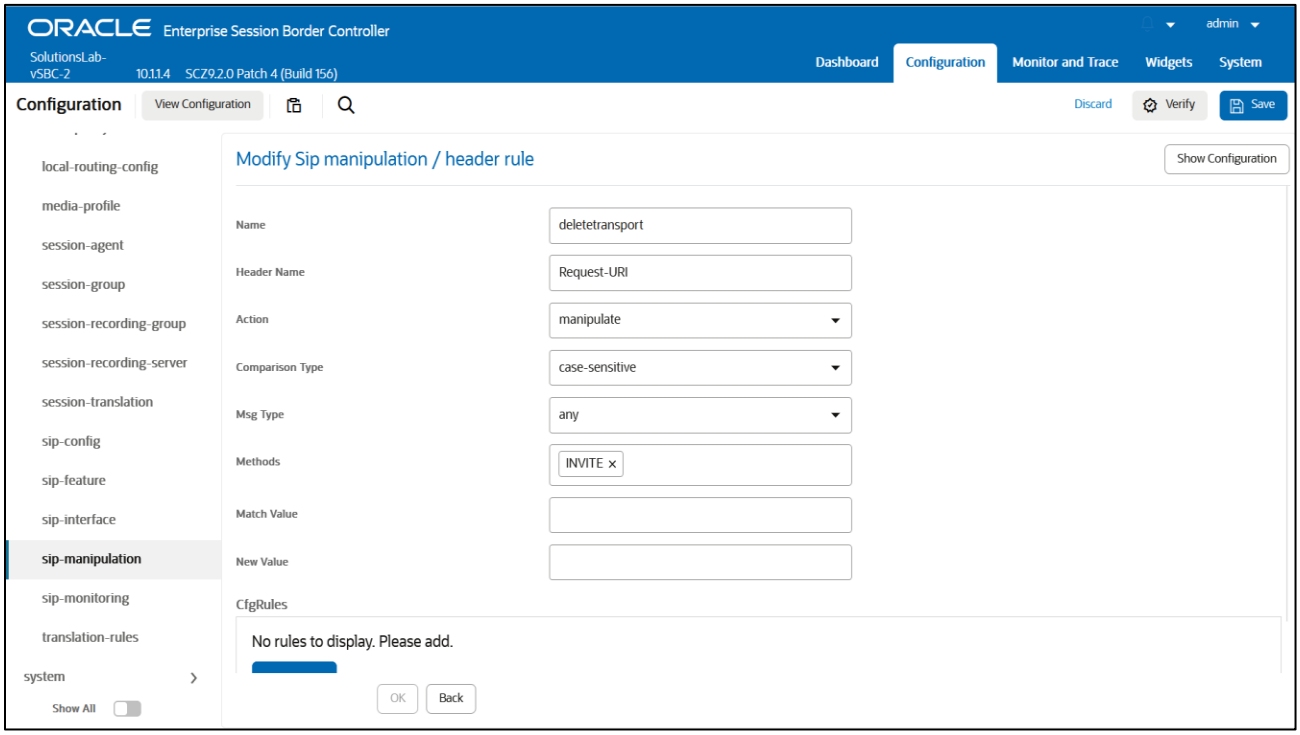
New Value is set to "<http://dialogflow.googleapis.com/v2beta1/projects/ccai-389811/conversations/Re_"+$CALL_ID.$0+">;purpose=Goog-ContactCenter-Conversation"



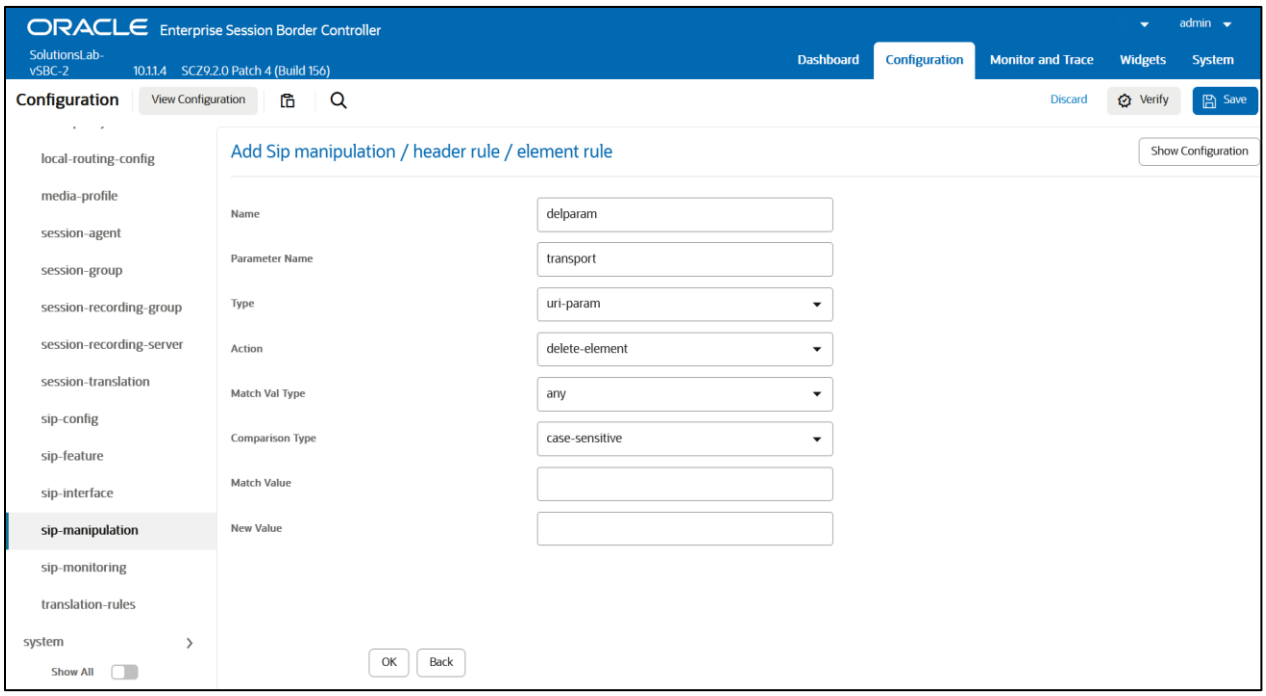
Below header rule is created to delete the Google CCAI FQDN generated by Oracle SBC during the creation of Conversation ID (this rule is applied only when Conversation on the Fly is set to True in Google CCAI).



Below header rule is created to delete the transport parameter in the Request URI towards Google CCAI



Create an element-rule delparam to delete the transport parameter.



With this, SBC configuration is complete.

7. Existing SBC configuration

If the SBC being used is an existing SBC with functional configuration, following configuration elements are required:

- New realm-config
- Configuring a certificate for SBC Interface
- TLS-Profile
- New sip-interface
- New session-agent
- New steering-pools
- New local-policy
- SDES Profile
- Media-sec-Policy
- Translation Rules
- Session Translation Rules
- Session Recording Server
- Session Timer Profile
- SIP-Manipulations

Please follow the steps mentioned in the above chapters to configure these elements.

8. Oracle SBC deployed behind NAT

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 IP as configured on both the SIP Interface and Steering Pool
• 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 Google side SIP interface.

HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4

HeaderNatPublicSipIfIp is the public interface IP.
HeaderNatPrivateSipIfIp is the private IP.

To configure header NAT SPL from ACLI

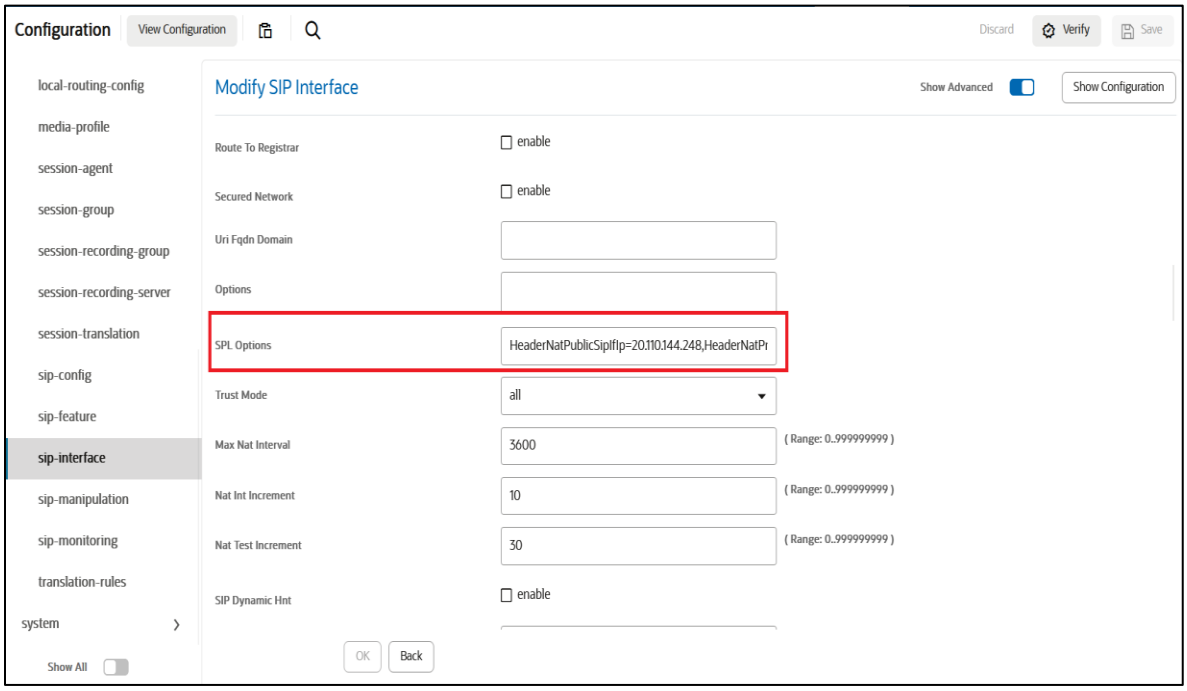
ACLI Path: config t→session-router→sip-interface

Choose the sip interface on which the header NAT SPL needs to be applied under spl-options.
Add the entry as per example shared below.

```
spl-options

HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4
```

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

To configure **header NAT SPL** from **SBC GUI,** please go to below path.
Go to Session-Router->sip-interface and configure the SPL Options as shown below. Please select "Show Advanced" tag to view the SPL Options.



You will need to apply these options to every sip interface on the SBC that is connected through a NAT.

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