



ORACLE

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	24 th May 2024

Table of Contents

1. INTENDED AUDIENCE	4
2. DOCUMENT OVERVIEW	4
3. INTRODUCTION	4
3.1. AUDIENCE	4
3.2. REQUIREMENTS	4
3.3. ARCHITECTURE	5
3.4. CAVEATS AND LIMITATION	5
4. GOOGLE CCAI API CONFIGURATION	6
5. CONFIGURING THE SBC	6
5.1. VALIDATED ORACLE SBC VERSION	6
6. NEW SBC CONFIGURATION	7
6.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC	7
6.2. CONFIGURE SBC USING WEB GUI	11
6.3. CONFIGURE SYSTEM-CONFIG	13
6.4. CONFIGURE PHYSICAL INTERFACE VALUES	15
6.5. CONFIGURE NETWORK INTERFACE VALUES.	17
6.6. ENABLE MEDIA MANAGER	20
6.8. CONFIGURE REALMS	22
6.9. CONFIGURING A CERTIFICATE FOR SBC	25
6.10. TLS-PROFILE	30
6.11. CONFIGURE SIP INTERFACES	30
6.12. CONFIGURE SESSION-AGENT	32
6.13. CONFIGURE LOCAL-POLICY	37
6.14. CONFIGURE STEERING-POOL	38
6.15. CONFIGURE SDES PROFILE	40
6.16. CONFIGURE MEDIA SECURITY PROFILE	41
6.17. CONFIGURE TRANSLATION RULES	42
6.18. CONFIGURE SESSION TRANSLATION RULES	43
6.19. CONFIGURE CODEC POLICY	43
6.20. CONFIGURE SESSION RECORDING SERVER	44
6.21. CONFIGURE SESSION TIMER	45
6.22. CONFIGURE SIP-MANIPULATION	46
7. EXISTING SBC CONFIGURATION	49
8. ORACLE SBC DEPLOYED BEHIND NAT	50



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

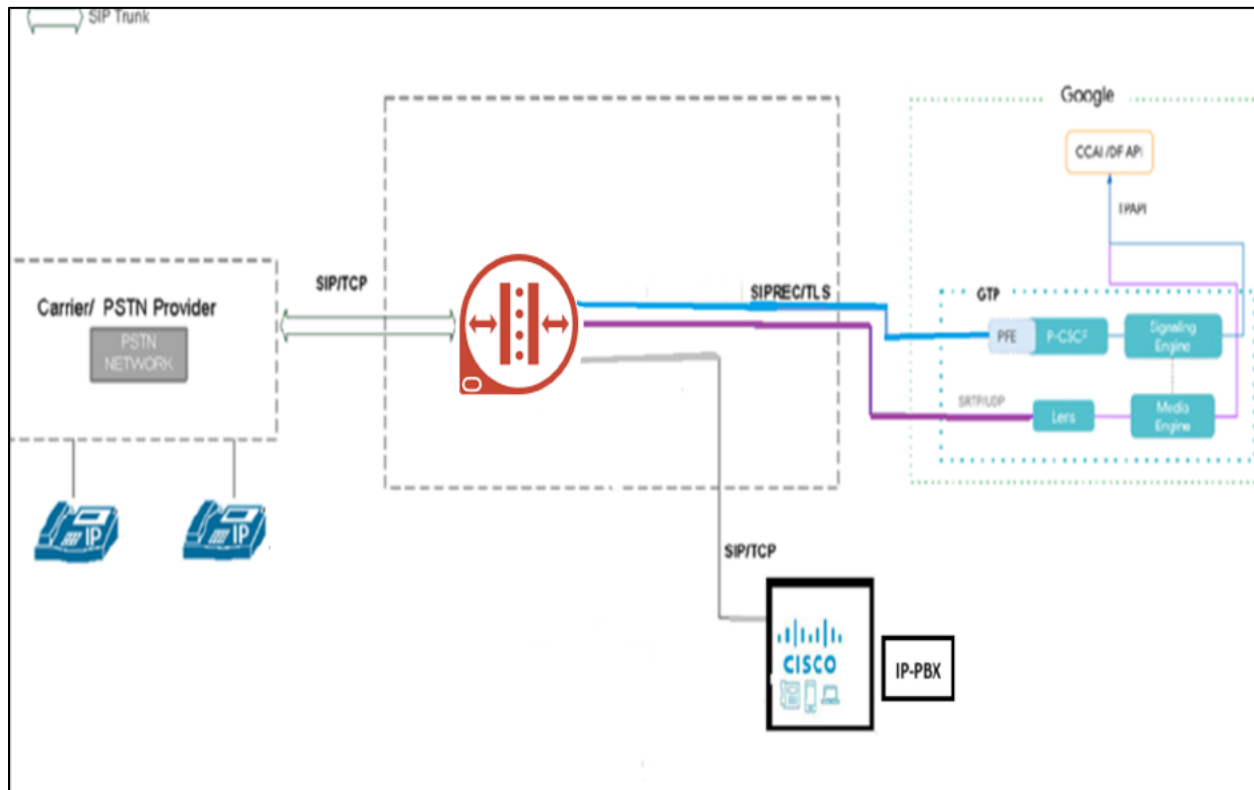
- Fully functioning Google CCAI cloud Environment.
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 9.2.0 version.
- On-prem IP PBX - **We are using Cisco Call Manager (Cisco CUCM) as on prem IP-PBX as an example for this Application note document.**

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

```
Starting tLemd...
Starting tServiceHealth...
Starting tCollect...
Starting tAtcpd...
Starting tAscpd...
Starting tMbcd...
Starting tCommMonitor...
Starting tFped...
Starting tAlgd...
Starting tRadd...
Starting tEbmd...
Starting tSipd...
Starting tH323d...
Starting tbfdd...
Starting tIPTd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tTscfd...
Starting tFcgid...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Starting tIFMIBd...
Start platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...

Starting acliMgr...
password secure mode is enabled
Admin Security is disabled
Password: █
```

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.

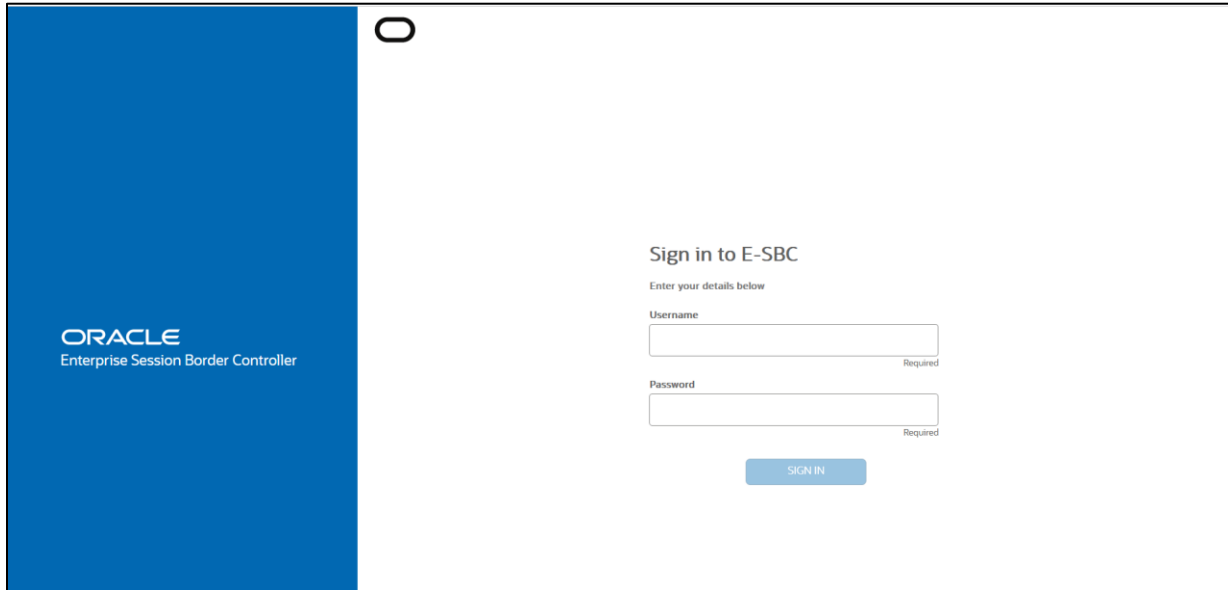
```
SolutionsLab-vSBC-2 (http-server)# show
http-server
  name                webserver
  state               enabled
  realm
  ip-address
  http-state          enabled
  http-port           80
  HTTP-strict-transport-security-policy disabled
  https-state         disabled
  https-port          443
  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.

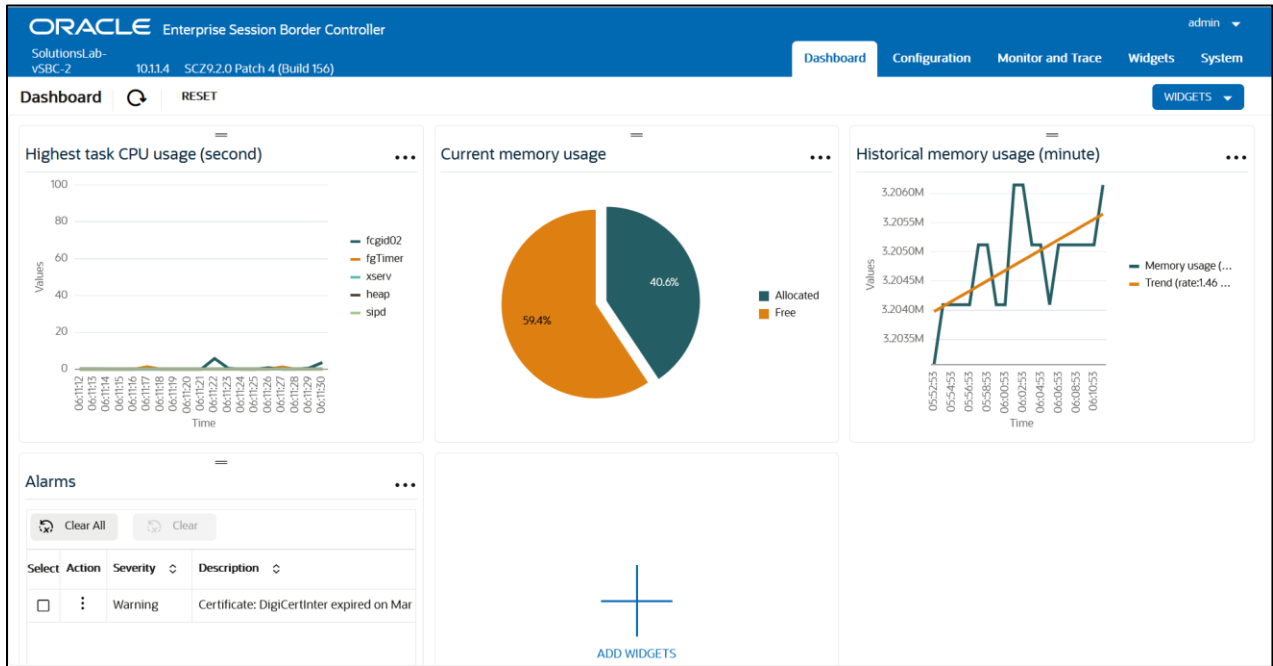
The Web GUI can be accessed through the url http://<SBC_MGMT_IP>.



The screenshot shows the Oracle E-SBC Web GUI login page. On the left, there is a blue vertical bar with the Oracle logo and the text "ORACLE Enterprise Session Border Controller". The main content area is white and contains the following elements:

- A large, faint "O" logo in the top left corner.
- The heading "Sign in to E-SBC".
- The instruction "Enter your details below".
- A "Username" label above a text input field, with "Required" written below the field.
- A "Password" label above a text input field, with "Required" written below the field.
- A blue "SIGN IN" button centered below the input fields.

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



Go to Configuration as shown below, to configure the SBC

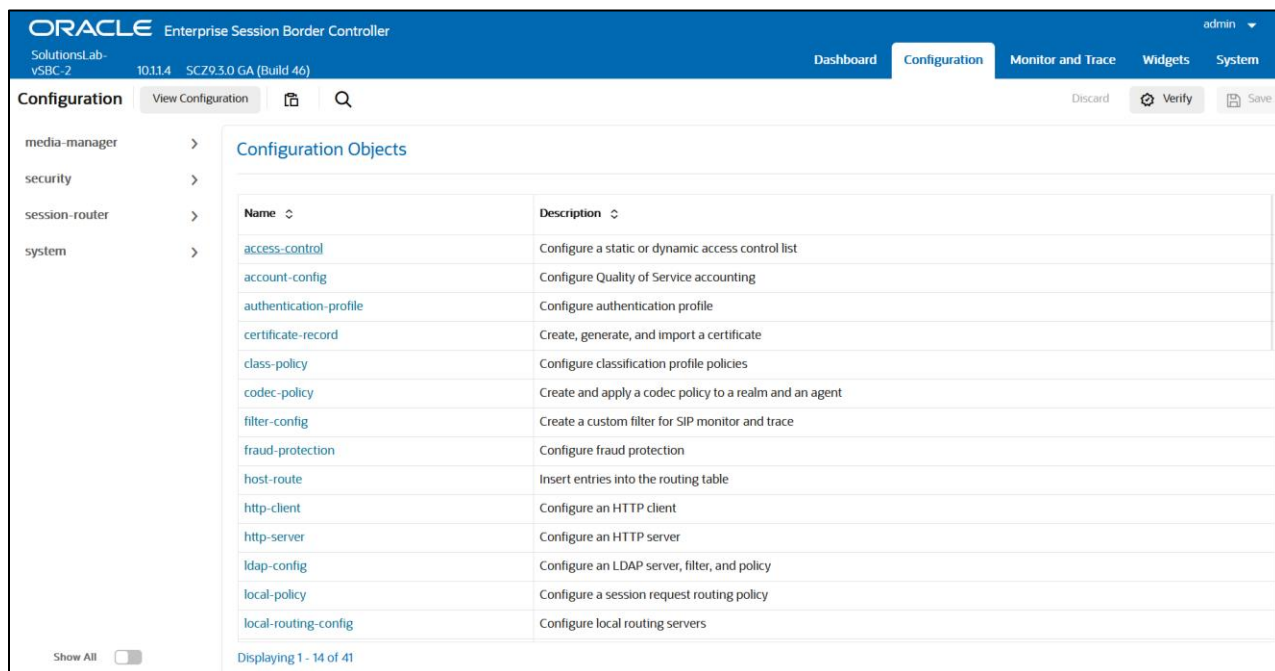
Below is the screenshot captured for SBC 9.2.0p4 version

Configuration Objects

Name	Description
access-control	Configure a static or dynamic access control list
account-config	Configure Quality of Service accounting
authentication-profile	Configure authentication profile
certificate-record	Create, generate, and import a certificate
class-policy	Configure classification profile policies
codec-policy	Create and apply a codec policy to a realm and an agent
filter-config	Create a custom filter for SIP monitor and trace
fraud-protection	Configure fraud protection
host-route	Insert entries into the routing table
http-client	Configure an HTTP client
http-server	Configure an HTTP server
ldap-config	Configure an LDAP server, filter, and policy
local-policy	Configure a session request routing policy
local-routing-config	Configure local routing servers

Showing 1 - 14 of 40

Below is the screenshot captured for SBC 9.3.0 GA version



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

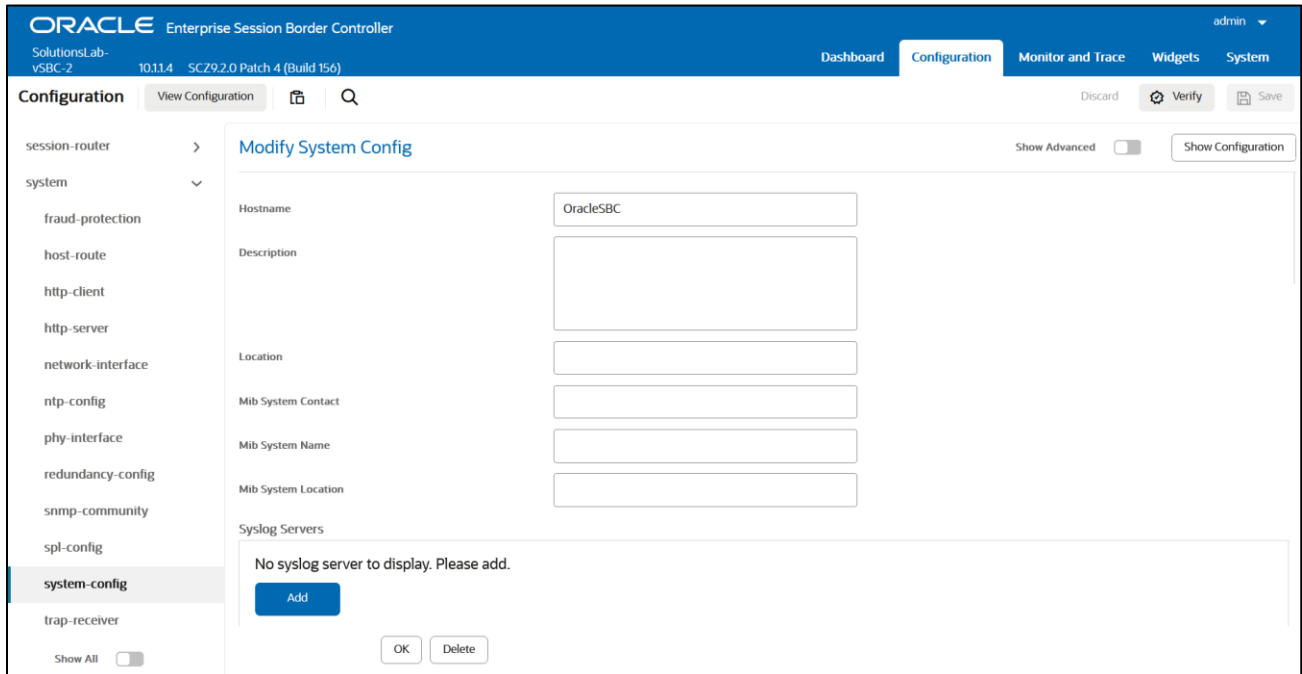
<https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.3.0/webgui/web-gui-guide.pdf>

The expert mode is used for configuration.

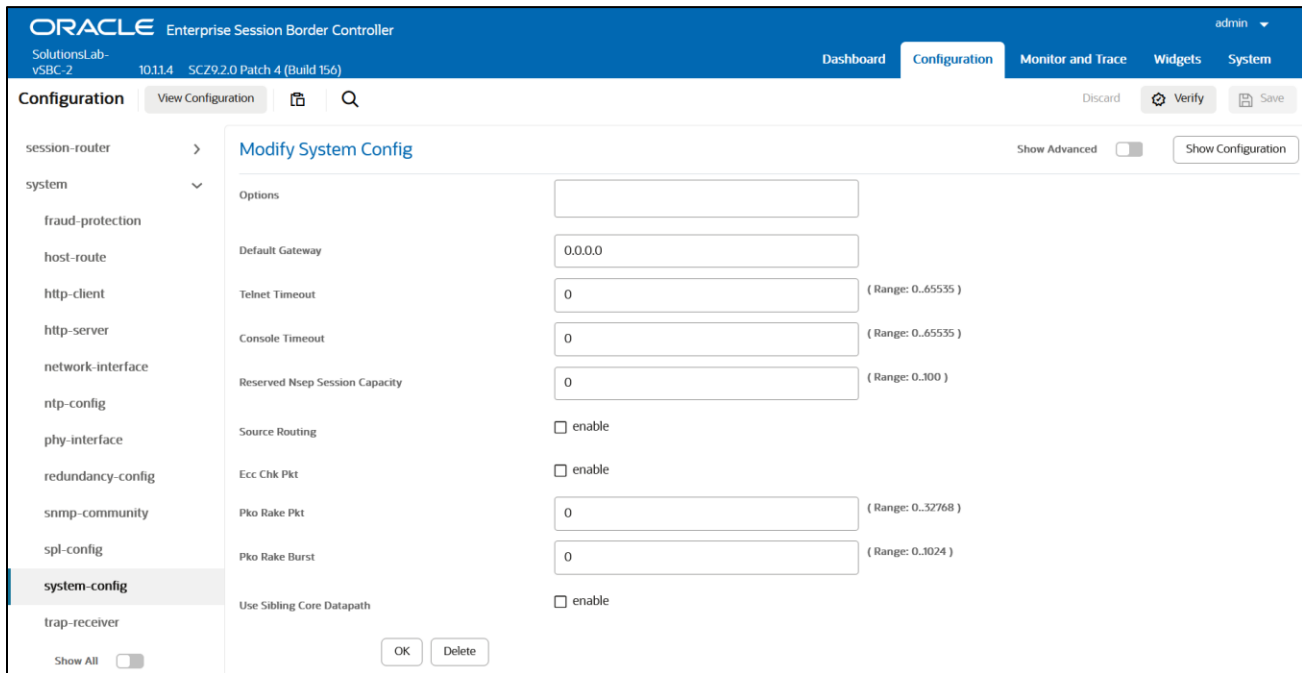
Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

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.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Phy Interface". The interface includes a navigation menu on the left with categories like media-manager, security, session-router, system, fraud-protection, host-route, http-client, http-server, network-interface, ntp-config, phy-interface (selected), redundancy-config, snmp-community, and spl-config. The main configuration area contains the following fields:

- Name: s0p0
- Operation Type: Media
- Port: 0 (Range: 0..5)
- Slot: 0 (Range: 0..2)
- Virtual Mac: (empty)
- Admin State: enable
- Auto Negotiation: enable
- Duplex Mode: FULL
- Speed: 100
- Wancom Health Score: 50 (Range: 0..300)

At the bottom of the configuration area, there are "OK" and "Back" buttons. The top right of the interface shows "Show Advanced" (checked) and "Show Configuration" buttons.

Please configure s1p0 interface as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a sidebar lists various configuration categories, with 'phy-interface' selected. The main area is titled 'Modify Phy Interface' and contains the following fields:

Name	s1p0
Operation Type	Media
Port	0 (Range: 0..5)
Slot	1 (Range: 0..2)
Virtual Mac	
Admin State	<input checked="" type="checkbox"/> enable
Auto Negotiation	<input checked="" type="checkbox"/> enable
Duplex Mode	FULL
Speed	100
Wancom Health Score	50 (Range: 0..100)

Buttons for 'OK' and 'Back' are located at the bottom of the configuration area. The 'Show Advanced' toggle is turned on, and the 'Show Configuration' button is visible in the top right corner of the configuration panel.

Please configure s1p1 interface as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for the s1p1 interface. The layout is identical to the previous screenshot, but with the following field values:

Name	s1p1
Operation Type	Media
Port	1 (Range: 0..5)
Slot	1 (Range: 0..2)
Virtual Mac	
Duplex Mode	FULL
Speed	100
Wancom Health Score	50 (Range: 0..100)

The 'Show Advanced' toggle is turned off in this view. The 'OK' and 'Back' buttons are present at the bottom of the configuration area.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Network Interface". The interface includes a sidebar with navigation options like "media-manager", "security", "session-router", "system", "fraud-protection", "host-route", "http-client", "http-server", "network-interface", "ntp-config", "phy-interface", "redundancy-config", "snmp-community", and "spl-config". The "network-interface" option is selected. The main configuration area contains the following fields:

- Name: s0p0
- Sub Port Id: 0 (Range: 0..4095)
- Description: Google CC Interface
- Hostname: googleccai.solutionslab.com
- IP Address: 10.1.2.4
- Pri Utility Addr: (empty)
- Sec Utility Addr: (empty)
- Netmask: 255.255.255.0
- Gateway: 10.1.2.1

At the bottom of the configuration area, there are "OK" and "Back" buttons. The top navigation bar includes "Dashboard", "Configuration", "Monitor and Trace", "Widgets", and "System".

ORACLE Enterprise Session Border Controller
 SolutionsLab-vSBC-2 10.11.4 SCZ9.2.0 Patch 4 (Build 156) Dashboard Configuration Monitor and Trace Widgets System admin

Configuration View Configuration [Search] Discard Verify Save

media-manager > Modify Network Interface Show Advanced [Toggle] Show Configuration

security > Heartbeat 0 (Range: 0..65535)

session-router > Retry Count 0 (Range: 0..65535)

system > Retry Timeout 1 (Range: 1..65535)

fraud-protection > Health Score 0 (Range: 0..100)

host-route > Health Score 0 (Range: 0..100)

http-client > Bfd Config

http-server > Health Score 0 (Range: 0..100)

network-interface

ntp-config > DNS IP Primary 8.8.8.8

phy-interface > DNS IP Backup1

redundancy-config > DNS Domain solutionslab.com

snmp-community > HIP IP List 10.1.2.4 x

spl-config >

Show All [Toggle] OK Back

Similarly, configure network interface s1p0 as below

ORACLE Enterprise Session Border Controller
 SolutionsLab-vSBC-2 10.11.4 SCZ9.2.0 Patch 4 (Build 156) Dashboard Configuration Monitor and Trace Widgets System admin

Configuration View Configuration [Search] Discard Verify Save

session-router > Modify Network Interface Show Advanced [Toggle] Show Configuration

system > Name s1p0

fraud-protection > Sub Port Id 0 (Range: 0..4095)

host-route > Description Cisco CUCM Interface

http-client > Hostname

http-server > IP Address 155.212.214.90

network-interface

ntp-config > Pri Utility Addr

phy-interface > Sec Utility Addr

redundancy-config > Netmask 255.255.255.0

snmp-community > Gateway 155.212.214.65

spl-config >

system-config >

trap-receiver >

Show All [Toggle] OK Back

Please configure the network interface s1p0 as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the 'network-interface' category is selected in the left sidebar. The main area is titled 'Modify Network Interface' and contains the following configuration fields:

Field	Value
Name	s1p1
Sub Port Id	0 (Range: 0-4095)
Description	PSTN Interface
IP Address	155.212.214.100
Netmask	255.255.255.0
Gateway	155.212.214.65

Additional controls include 'Show Advanced' (disabled), 'Show Configuration', 'OK', and 'Back' buttons.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the 'media-manager' section is selected in the left sidebar. The main content area is titled 'Modify Media Manager' and contains the following settings:

Parameter	Value	Range
State	<input checked="" type="checkbox"/> enable	
Flow Time Limit	86400	(Range: 0..999999999)
Initial Guard Timer	300	(Range: 0..999999999)
Subsq Guard Timer	300	(Range: 0..999999999)
TCP Flow Time Limit	86400	(Range: 0..999999999)
TCP Initial Guard Timer	300	(Range: 0..999999999)
TCP Subsq Guard Timer	300	(Range: 0..999999999)
Hint Rtcp	<input type="checkbox"/> enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	

Buttons at the bottom include 'Show All', 'OK', and 'Delete'.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, displaying advanced options for the Media Manager. The 'media-manager' section is selected in the left sidebar. The main content area is titled 'Modify Media Manager' and contains the following settings:

Parameter	Value	Range
Options	audio-allow-asymmetric-pt x	
Red Max Trans	10000	(Range: 0..50000)
Red Sync Start Time	5000	(Range: 0..4294967295)
Red Sync Comp Time	1000	(Range: 0..4294967295)
Media Policing	<input checked="" type="checkbox"/> enable	
Max Arp Rate	10	(Range: 0..300)
Max Signaling Packets	6000	(Range: 0..4294967295)
Max Untrusted Signaling	9	(Range: 0..300)
Min Untrusted Signaling	8	(Range: 0..300)
Dos Guard Window	5	(Range: 1..30)

Buttons at the bottom include 'Show All', 'OK', and 'Delete'.

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.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active, and the 'sip-config' section is selected in the left sidebar. The 'Modify SIP Config' form is displayed with the following fields:

Field	Value	Range
State	<input checked="" type="checkbox"/> enable	
Dialog Transparency	<input checked="" type="checkbox"/> enable	
Home Realm ID	GoogleCCAI	
Egress Realm ID		
Nat Mode	None	
Registrar Domain	*	
Registrar Host	*	
Registrar Port	5060	(Range: 0,1025..65535)
Init Timer	500	(Range: 0..999999999)
Max Timer	4000	(Range: 0..999999999)

Buttons: OK, Delete

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, displaying advanced options for the 'Modify SIP Config' form. The 'Show Advanced' toggle is turned on. The 'Options' field is highlighted with a red box, containing the text 'max-udp-length=0 x |'. Other fields include:

Field	Value	Range
Red Max Trans	10000	(Range: 0..50000)
Options	max-udp-length=0 x	
SIP Message Len	4096	(Range: 0..65535)
Enum Sag Match	<input type="checkbox"/> enable	
Extra Method Stats	<input checked="" type="checkbox"/> enable	
Extra Enum Stats	<input type="checkbox"/> enable	
Registration Cache Limit	0	(Range: 0..999999999)
Register Use To For Lp	<input type="checkbox"/> enable	
Refer Src Routing	<input type="checkbox"/> enable	

Buttons: OK, Delete

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:

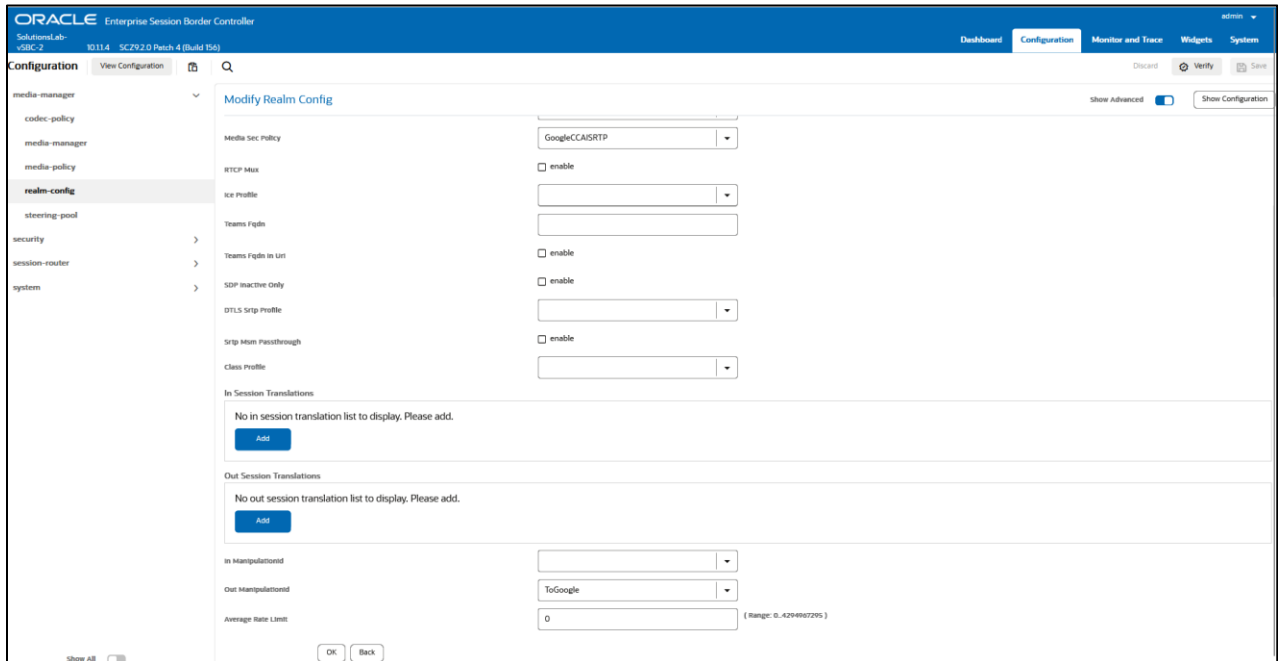
Config Parameter	GoogleCCAI Side	IP-PBX Side	PSTN Side
Identifier	GoogleCCAI	CiscoCUCM	PSTNRealm
Network Interface	S0p0	s1p0	s1p1
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Codec policy	GoogleCC		
Media Sec policy	GoogleCCAISRTP	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

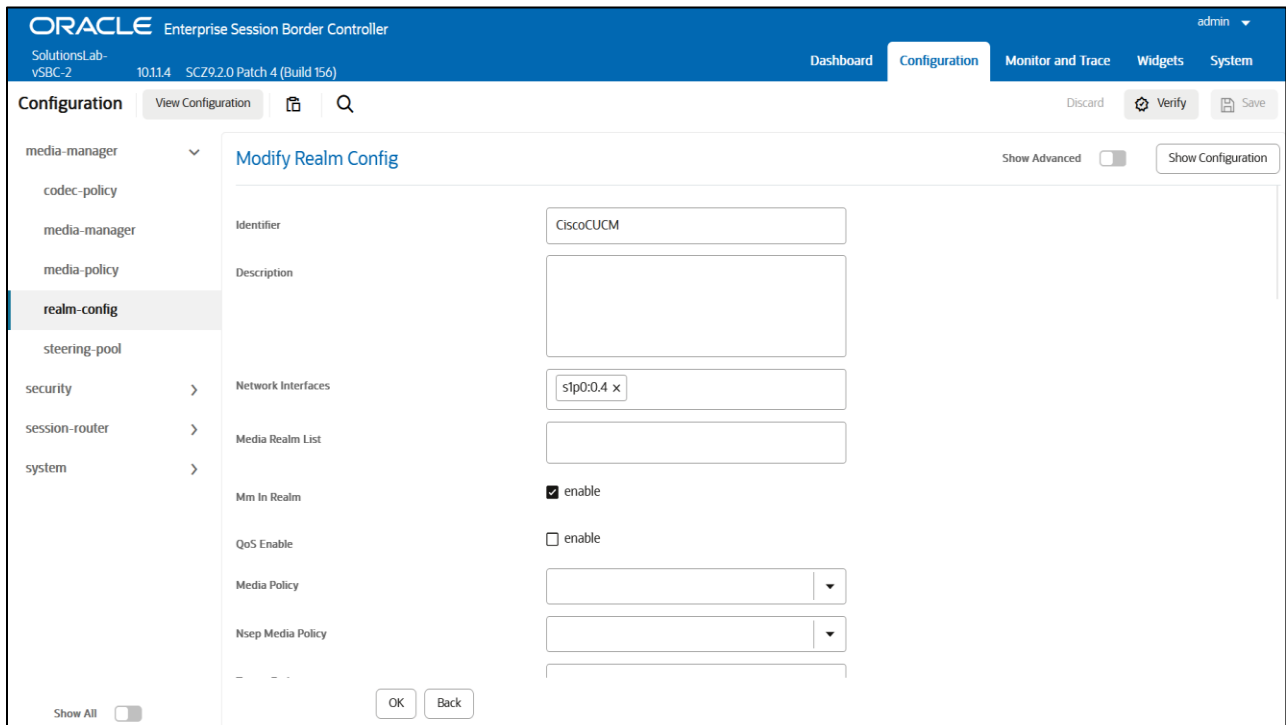
The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Realm Config" and the realm name is "GoogleCCAI". The configuration fields are as follows:

- Identifier: GoogleCCAI
- Description: (Empty text area)
- Addr Prefix: 0.0.0.0
- Network Interfaces: s0p0:0.4 x
- Media Realm List: (Empty text area)
- Mm In Realm: enable
- Mm In Network: enable
- Mm Same Ip: enable
- (Unlabeled checkbox): enable

Buttons at the bottom include "OK" and "Back". The interface also shows a navigation menu on the left with "realm-config" selected, and a top navigation bar with "Configuration" and "Monitor and Trace" tabs.



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.



ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 10.11.4 SCZ9.2.0 Patch 4 (Build 156) Dashboard Configuration Monitor and Trace Widgets System admin

Configuration View Configuration [Home] [Search] Discard Verify Save

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

Modify Realm Config Show Advanced [Toggle] Show Configuration

Dyn Refer Term	<input type="checkbox"/> enable
Codec Policy	[Dropdown]
Codec ManIP In Realm	<input type="checkbox"/> enable
RTCP Policy	[Dropdown]
Session Recording Server	GoogleCCAI x
Hide Egress Media Update	<input type="checkbox"/> enable
Monitoring Filters	[Input Field]
Merge Early Dialogs	<input type="checkbox"/> enable
Srvcc Trfo	[Input Field]
Feature Trfo	[Input Field]

Show All [Toggle] OK Back

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

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 10.11.4 SCZ9.2.0 Patch 4 (Build 156) Dashboard Configuration Monitor and Trace Widgets System admin


Configuration View Configuration [Home] [Search] Discard Verify Save

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

Modify Realm Config Show Advanced [Toggle] Show Configuration

Identifier	PSTNRealm
Description	[Input Field]
Network Interfaces	stpt0.4 x
Media Realm List	[Input Field]
Mm In Realm	<input checked="" type="checkbox"/> enable
QoS Enable	<input type="checkbox"/> enable
Media Policy	[Dropdown]
Nsep Media Policy	[Dropdown]
Teams Fqdn	[Input Field]

Show All [Toggle] OK Back



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.cgburlington.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 certificate 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.

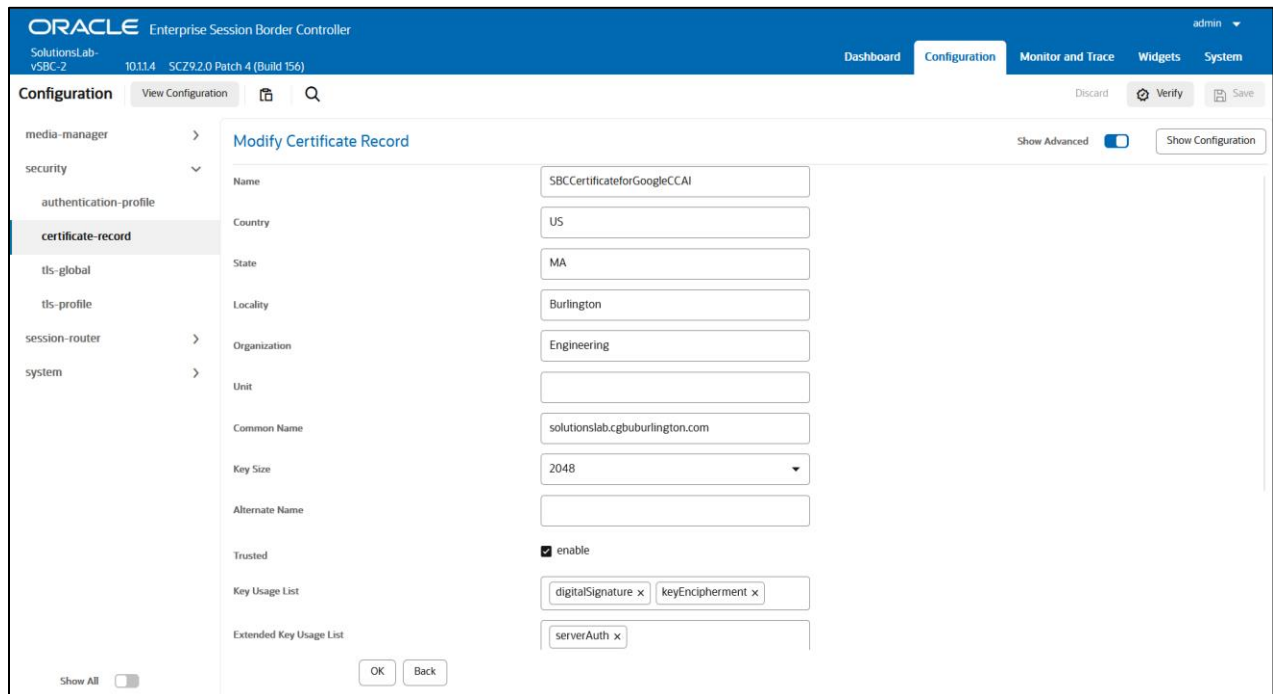
This section walks you through how to configure certificate records, create a certificate signing request and import the necessary certificates into the SBC's configuration.

- 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 screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'SolutionsLab-vSBC-2', version '10.11.4 - SCZ9.2.0 Patch 4 (Build 156)', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, showing a tree view on the left with 'security' > 'certificate-record' selected. The main area is titled 'Modify Certificate Record' and contains the following fields:

Name	SBCCertificateforGoogleCCAI
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	
Common Name	solutionslab.cgbuburlington.com
Key Size	2048
Alternate Name	
Trusted	<input checked="" type="checkbox"/> enable
Key Usage List	digitalSignature x keyEncipherment x
Extended Key Usage List	serverAuth x

Buttons for 'OK' and 'Back' are at the bottom. A 'Show All' toggle is also present.

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.

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 10.11.4 SCZ9.2.0 Patch 4 (Build 156)

Dashboard Configuration Monitor and Trace Widgets System

configuration View Configuration

media-manager security authentication-profile certificate-record

Certificate Record

Search: SBCCertificateforGoogleCCA

PKCS12 Delete all Certificate Record items SBCCertificateforGoogleCCA

Select	Action	Name	Country	State	Locality	Organization	Unit	Common Name
<input checked="" type="checkbox"/>		SBCCertificateforGoo...	US	MA	Burlington	Engineering		solutionslab.cgbubur...

Showing 1 of 1

Generate certificate response

Copy the following information and send to a CA authority.

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC5zCCA8CAQAwbzELMAkGA1UEBhMCVmxkZjBGNVBAgTAK1BMRMwEQYDVQOH
EwpCdXJsaW5ndG9uMRQwEgYDVQKEwtFbmdpbmVlcmluZzEoMUYGA1UEAxMfc29s
dXRpb25zbGFILmNnYnVidXJsaW5ndG9uLmNvbTCCASlwdQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBABkzXuAv8RjHs7cd7F8+3g3dqnheNFITDya47wT+jJupFnN
v+4nvlNzug3kc+3Jira6XggpoGLdK3/SjELatAj8mUleD8FFV6IAq3r41F/4lyZR
vgiZ2bamwHetQTPJes/gBQkblZCTXzsGhU+s0Yuqoc/4ED+ENNEg54ZlKRnJoHf
Zbv/EkZJEOJLg+h62RRw2ZhvPmGBDfIAzKkVW94JNMNZplwhb4aD2e5qgMs6Aq
Tkh84K7xHMvryQqT5AUZmJmro+GkX7EjWSMh0w5bN/X0qgAd7XP1hHqIpQU5IO
q9Z13ExtBHbxi54id3PEvAYJ8HliZydyW9jmPMCAwEAAsGAUQUFwMBMAOGCSqSIlb3
DQEBKcWUAA4IBAQBjWbly3U41HypfuCglgHBZnLhMxyZOjgOVIDB/88jpHoXmTDe
H7s9jivOQwNauDiVdMri473d+9ZjKzqSK73OjdAKb42qE3RSQJA+Ur/lphqjFhJs
GFXSiQbANQZZk6CURiHJUWwUcuwumWOlg0kuCTxaFMiH6llRiCjQH0elx+qp
OHKBvFDNFSGUIPJNw/aj/oVPiUSLw0HCqJ/TMbnVqsZM6xKZfMdKuSh2eAEFRvW
LSbJdJmpFC5LF4/lhLJ6wum1Lgbd/fJuwyDPnEli2yOEE/JYFS/GAoXTROVSBgF4
vPxPu9JTUieBwRNNos4CrLEOZpLmb3Y14wE3
-----END CERTIFICATE REQUEST-----

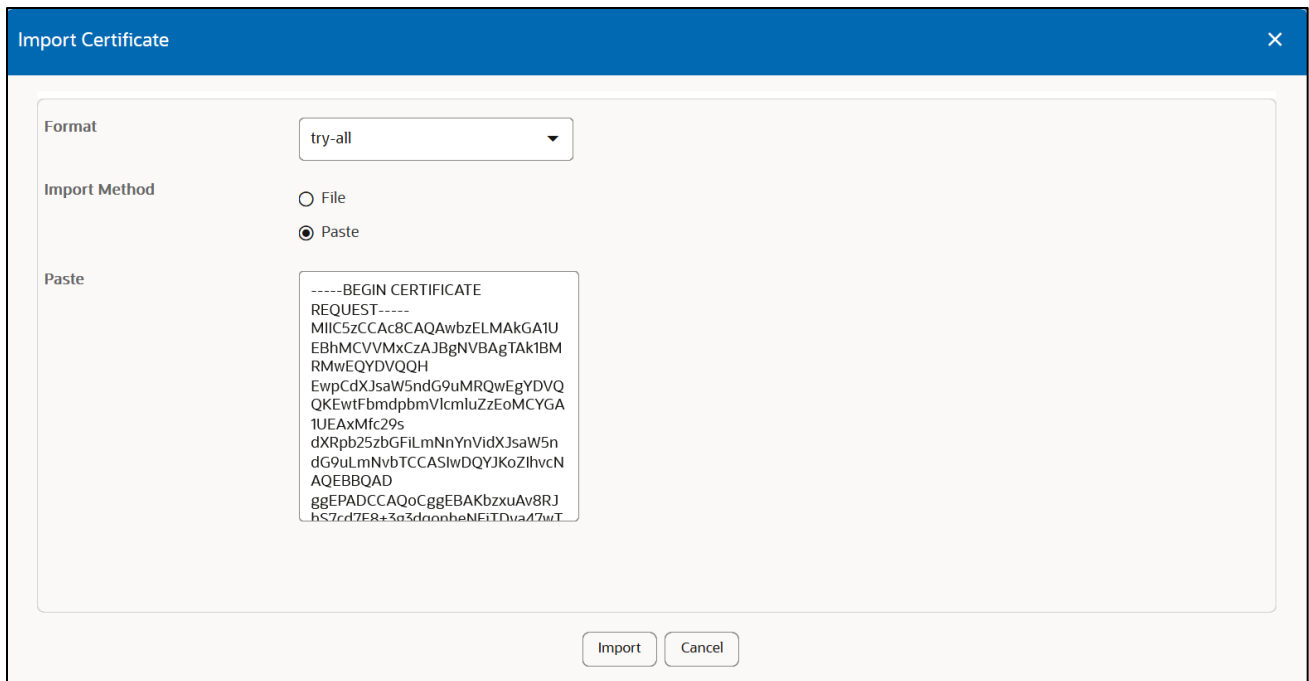
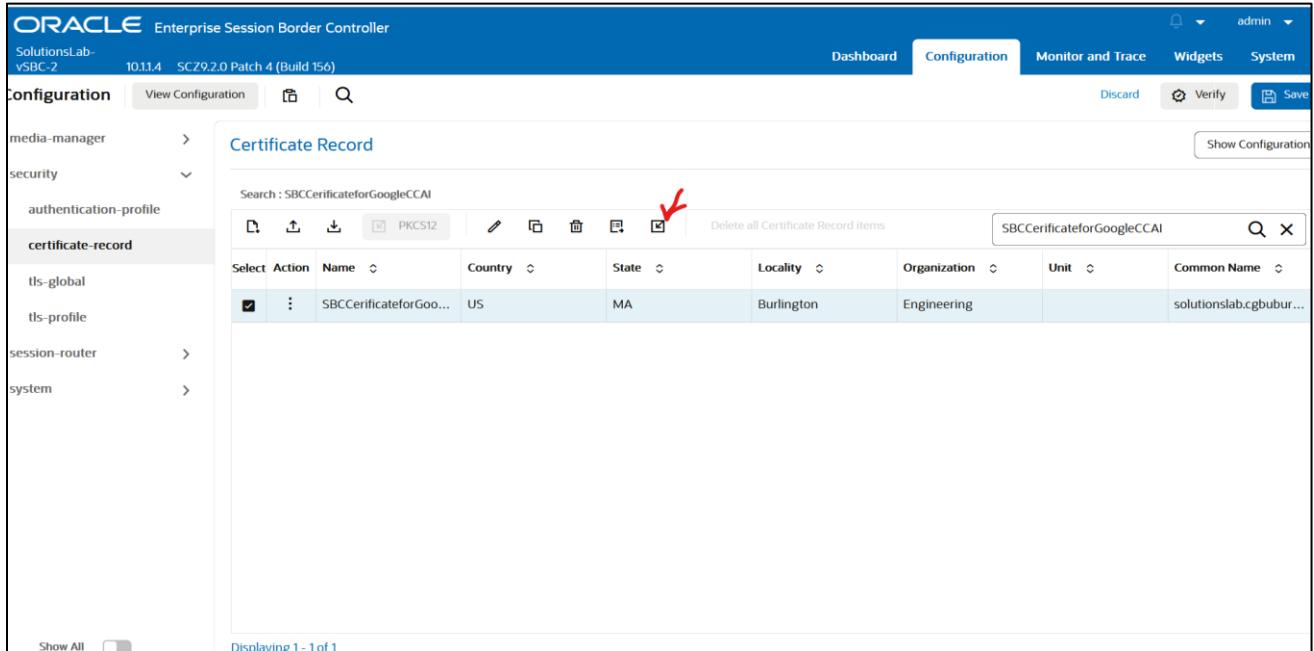
```

Close

- 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:

The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'SolutionsLab-vSBC-2', version '1031.4 SCZ9.2.0 Patch 4 (Build 156)', and navigation tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the left sidebar shows a tree view with 'tls-profile' selected. The main content area is titled 'Add TLS Profile' and contains the following configuration fields:

- Name: GoogleCCAI
- End Entity Certificate: SBCCertificateforGoogleCCAI
- Trusted Ca Certificates: GTS-Root-R1 x, GTSCAICS x, GlobalSignRootCA x
- Cipher List: DEFAULT x
- Verify Depth: 10 (Range: 0..10)
- Mutual Authenticate: enable
- TLS Version: tlsv12
- Options: (empty field)
- Cert Status Check: enable

At the bottom of the configuration area, there are 'OK' and 'Back' buttons, and a 'Show All' toggle switch.

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.

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 10.11.4 SCZ9.2.0 Patch 4 (Build 156) Dashboard Configuration Monitor and Trace Widgets System

Configuration View Configuration Discard Verify Save

Modify SIP Interface Show Advanced Show Configuration

State enable

Realm ID GoogleCCAI

Description

SIP Ports

Select	Action	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
<input type="checkbox"/>	⋮	10.1.2.4	5061	TLS	GoogleCCAI	agents-only	

OK Back

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

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 10.11.4 SCZ9.2.0 Patch 4 (Build 156) Dashboard Configuration Monitor and Trace Widgets System

Configuration View Configuration Discard Verify Save

Modify SIP Interface Show Advanced Show Configuration

State enable

Realm ID CiscoCUCM

Description

SIP Ports

Select	Action	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
<input type="checkbox"/>	⋮	155.212.214.90	5060	UDP		agents-only	
<input type="checkbox"/>	⋮	155.212.214.90	5060	TCP		agents-only	

OK Back

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

The screenshot displays the Oracle Enterprise Session Border Controller (ESBC) configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'SolutionsLab-vSBC-2', '10.11.4 SCZ9.2.0 Patch 4 (Build 156)', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, showing a 'Configuration' sidebar on the left with options like 'local-routing-config', 'media-profile', 'session-agent', 'session-group', 'session-recording-group', 'session-recording-server', 'session-translation', 'sip-config', 'sip-feature', 'sip-interface', 'sip-manipulation', 'sip-monitoring', 'translation-rules', and 'system'. The main area is titled 'Modify SIP Interface' and contains the following configuration fields:

- State: enable
- Realm ID: PSTNRealm
- Description: (empty text box)

Below these fields is a table for 'SIP Ports' with the following data:

Select	Action	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
<input type="checkbox"/>	⋮	155.212.124.100	5060	UDP		agents-only	
<input type="checkbox"/>	⋮	155.212.124.100	5060	TCP		agents-only	

At the bottom of the interface, there are 'OK' and 'Back' buttons.

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

SolutionsLab-vSBC-2 10.11.4 SCZ9.3.0 GA (Build 46) Dashboard Configuration Monitor and Trace Widgets System admin

Configuration View Configuration [Home] [Search] 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 [Toggle]

Modify Session Agent

Show Advanced [Toggle] 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: [Dropdown]

Description: [Text Area]

Ping Method: OPTIONS

[OK] [Back]

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 10.11.4 SCZ9.3.0 GA (Build 46) Dashboard Configuration Monitor and Trace Widgets System admin

Configuration View Configuration [Home] [Search] 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 [Toggle]

Modify Session Agent

Show Advanced [Toggle] Show Configuration

Response Map: [Dropdown]

Ping Method: OPTIONS

Ping Interval: 30 (Range: 0.999999999)

Ping Send Mode: keep-alive

Ping All Addresses: enable

Ping In Service Response Codes: [Text Area]

Load Balance DNS Query: hunt

Options: [Text Area]

SPL Options: [Text Area]

Media Profiles: [Text Area]

[OK] [Back]

The screenshot displays the Oracle Enterprise Session Border Controller configuration page for 'Modify Session Agent'. The left sidebar lists various configuration categories, with 'session-agent' selected. The main area contains several sections: 'SPL Options' and 'Media Profiles' with input fields; 'In Session Translations' with a message 'No in session translation list to display. Please add.' and an 'Add' button; and 'Out Session Translations' with a table containing one entry.

Select	Action	Out Session Translation Id	State
<input type="checkbox"/>	:	addplus	enabled

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

SolutionsLab-vSBC-2 10.11.4 SCZ9.2.0 Patch 4 (Build 156) Dashboard Configuration Monitor and Trace Widgets System admin

Configuration View Configuration [Home] [Search] Discard Verify Save

media-manager > Modify Session Agent Show Advanced Show Configuration

security >

session-router >

Hostname	CUCM-Cisco.pe.oracle.com
IP Address	10.232.50.89
Port	5060 (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
App Protocol	SIP
App Type	
Transport Method	StaticTCP
Realm ID	CiscoCUCM
Egress Realm ID	
Description	

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 OK Back

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 10.11.4 SCZ9.2.0 Patch 4 (Build 156) Dashboard Configuration Monitor and Trace Widgets System admin

Configuration View Configuration [Home] [Search] Discard Verify Save

media-manager > Modify Session Agent Show Advanced Show Configuration

security >

session-router >

Ping Method	OPTIONS
Ping Interval	30 (Range: 0..999999999)
Ping Send Mode	keep-alive
Ping All Addresses	<input type="checkbox"/> enable
Ping In Service Response Codes	
Load Balance DNS Query	hunt
Options	
SPL Options	
Media Profiles	
In Session Translations	

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 OK Back

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration categories, with 'session-agent' selected. The main content area is titled 'Modify Session Agent' and contains the following fields:

- Hostname: 68.68.117.67
- IP Address: 68.68.117.67
- Port: 5060 (Range: 0,1025..65535)
- State: enable
- App Protocol: SIP
- App Type: (empty)
- Transport Method: StaticTCP
- Realm ID: PSTNRealm
- Egress Realm ID: (empty)
- Description: (empty)

Buttons for 'OK' and 'Back' are located at the bottom of the form. A 'Show Configuration' button is also present in the top right corner of the configuration area.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, similar to the previous one. The top navigation bar and left sidebar are the same. The main content area is titled 'Modify Session Agent' and contains the following fields:

- Ping Method: OPTIONS
- Ping Interval: 30 (Range: 0..999999999)
- Ping Send Mode: keep-alive
- Ping All Addresses: enable
- Ping In Service Response Codes: (empty)
- Load Balance DNS Query: hunt
- Options: (empty)
- SPL Options: (empty)
- Media Profiles: (empty)
- In Session Translations: (empty)

Buttons for 'OK' and 'Back' are located at the bottom of the form. A 'Show Configuration' button is also present in the top right corner of the configuration area.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar is expanded to 'local-policy'. The main area is titled 'Modify Local Policy' and contains the following fields:

- From Address: * x
- To Address: * x
- Source Realm: PSTNRealm x
- Description: (empty)
- Policy Priority: none

Below these fields is a table of Policy Attributes:

Select	Action	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key	Auth User Lookup
<input type="checkbox"/>	:	CUCM-Cisco...	CiscoCUCM	replace-uri	disabled	0	enabled	SIP	single		

Buttons for 'OK' and 'Back' are visible at the bottom.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar is expanded to 'local-policy'. The main area is titled 'Modify Local Policy' and contains the following fields:

- From Address: * x
- To Address: * x
- Source Realm: CiscoCUCM x
- Description: (empty)
- Policy Priority: none

Below these fields is a table of Policy Attributes:

Select	Action	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key	Auth User Lookup
<input type="checkbox"/>	:	68.68.117.67	PSTNRealm	replace-uri	disabled	0	enabled	SIP	single		

Buttons for 'OK' and 'Back' are visible at the bottom.

6.14. Configure steering-pool

Google CCAI side steering pool.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Steering Pool". The configuration fields are as follows:

Field	Value	Range
IP Address	101.2.4	
Start Port	10000	(Range: 0..65535)
End Port	10999	(Range: 0..65535)
Realm ID	GoogleCCAI	
Network Interface		
Port Allocation Strategy	mixed	

Buttons: OK, Back, Show Configuration, Discard, Verify, Save.

IP-PBX side steering pool.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Steering Pool". The configuration fields are as follows:

Field	Value	Range
IP Address	155.212.214.90	
Start Port	20000	(Range: 0..65535)
End Port	20999	(Range: 0..65535)
Realm ID	CiscoCUCM	
Network Interface		
Port Allocation Strategy	mixed	

Buttons: OK, Back, Show Configuration, Discard, Verify, Save.

PSTN side steering pool.

The screenshot displays the Oracle Enterprise Session Border Controller (ESBC) configuration interface. The top navigation bar includes the Oracle logo, the product name 'Enterprise Session Border Controller', and the user 'admin'. Below this, the system information shows 'SolutionsLab-vSBC-2' and version '10.11.4 SCZ9.2.0 Patch 4 (Build 156)'. The main navigation tabs are 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the left sidebar shows a tree view with 'steering-pool' selected. The main content area is titled 'Modify Steering Pool' and contains the following configuration fields:

Field	Value	Notes
IP Address	155.212.214.100	
Start Port	20000	(Range: 0..65535)
End Port	20999	(Range: 0..65535)
Realm ID	PSTNRealm	Dropdown menu
Network Interface		Dropdown menu
Port Allocation Strategy	mixed	Dropdown menu

At the bottom of the configuration area, there are 'OK' and 'Back' buttons. A 'Show All' toggle is located at the bottom left of the sidebar area.

6.15. Configure sdes profile

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

The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'admin', 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration categories, with 'media-security' expanded to show 'sdes-profile' selected. The main content area is titled 'Modify Sdes Profile' and contains the following fields:

- Name:** SDES
- Crypto List:** AES_CM_128_HMAC_SHA1_80 x, AES_CM_128_HMAC_SHA1_32 x, AES_256_CM_HMAC_SHA1_80 x
- Srtp Auth:** enable
- Srtp Encrypt:** enable
- SrTCP Encrypt:** enable
- Mki:** enable
- Egress Offer Format:** same-as-ingress
- Use Ingress Session Params:** (empty text box)
- Options:** (empty text box)

At the bottom of the form are 'OK' and 'Back' buttons. The interface also includes a 'Show Advanced' toggle and a 'Show Configuration' button.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Media Sec Policy". The left sidebar lists various configuration categories, with "media-sec-policy" selected. The main content area contains the following fields:

- Name: GoogleCCAISRTP
- Pass Through: enable
- Options: [Empty text box]
- Inbound**
 - Profile: SDES
 - Mode: srtp
 - Protocol: sdes
 - Hide Egress Media Update: enable
- Outbound**
 - Profile: SDES
 - Mode: srtp
 - Protocol: sdes

Buttons for "OK" and "Back" are visible at the bottom of the form.

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.**

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for a different media security policy. The page title is "Modify Media Sec Policy". The left sidebar lists various configuration categories, with "media-sec-policy" selected. The main content area contains the following fields:

- Name: RTP
- Pass Through: enable
- Options: [Empty text box]
- Inbound**
 - Profile: [Empty dropdown]
 - Mode: rtp
 - Protocol: none
 - Hide Egress Media Update: enable
- Outbound**
 - Profile: [Empty dropdown]
 - Mode: rtp
 - Protocol: none

Buttons for "OK" and "Back" are visible at the bottom of the form.

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.

The screenshot displays the Oracle Enterprise Session Border Controller (ESBC) configuration interface. The top navigation bar includes the Oracle logo, the product name 'Enterprise Session Border Controller', the user 'admin', and menu items for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' menu is active, and the 'translation-rules' sub-menu is selected in the left sidebar. The main content area is titled 'Add Translation Rules' and contains the following fields:

Field	Value
Id	addplus1
Description	add plus
Input Header Type	called-address-or-number
Input Header Value	^{*}\$
Output Header Type	called-address-or-number
Output Header Value	\+\$1

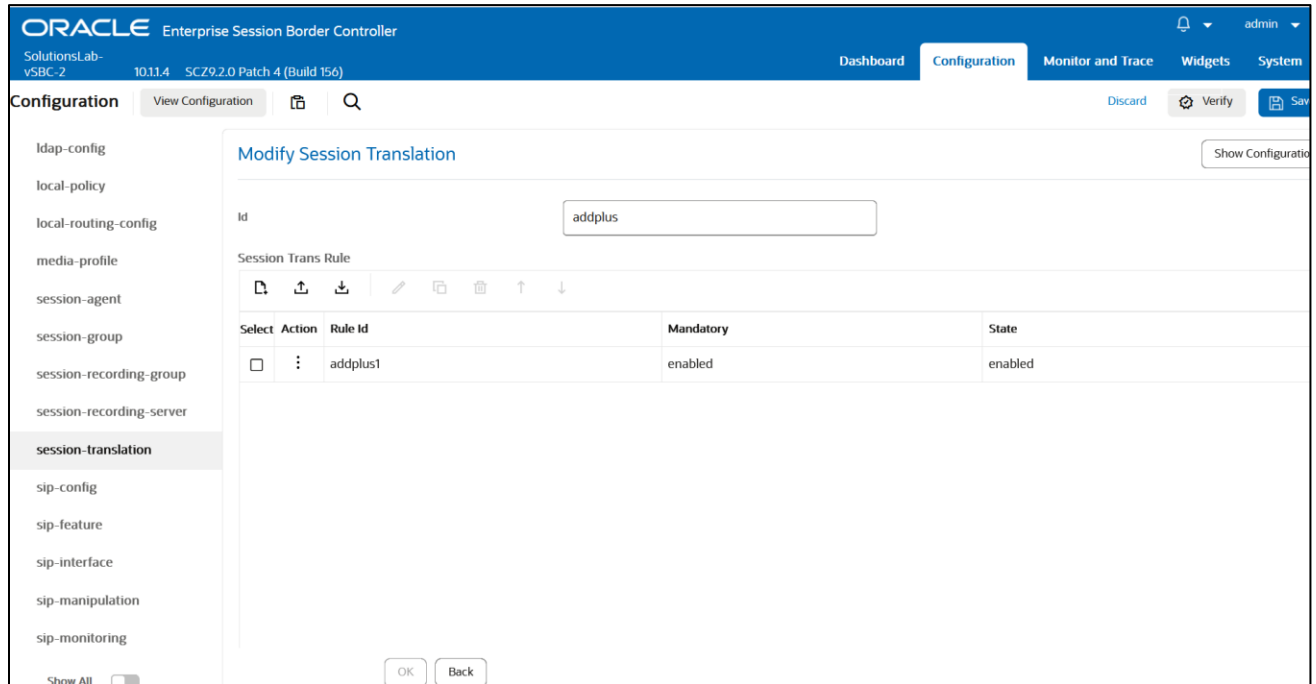
At the bottom of the form, there are 'OK' and 'Back' buttons. The interface also includes a 'Show Configuration' button in the top right and a 'Show All' toggle in the bottom left.

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.



The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The main heading is "Modify Session Translation". The "Id" field is set to "addplus". Below this, there is a table of Session Trans Rules.

Select	Action	Rule Id	Mandatory	State
<input type="checkbox"/>	:	addplus1	enabled	enabled

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.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The current page is 'Add Codec Policy' under the 'media-manager' section. The configuration form includes the following fields:

- Name: GoogleCC
- Allow Codecs: PCMU x, PCMA x
- Add Codecs On Egress: (empty)
- Order Codecs: (empty)
- Packetization Time: 20
- Force Ptime: enable
- Secure Dtmf Cancellation: enable
- Dtmf In Audio: disabled
- Tone Detect Renegotiate Timer: 500 (Range: 50..32000)
- Reverse Fax Tone Detection Reinvite: enable

Buttons for 'OK' and 'Back' are located at the bottom of the form. The left sidebar shows a tree view of configuration categories, with 'codec-policy' selected.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for 'Add Session Recording Server'. The top navigation bar is the same as the previous screenshot. The current page is 'Add Session Recording Server' under the 'session-recording-server' section. The configuration form includes the following fields:

- Name: GoogleCCAI
- Description: (empty)
- Realm: GoogleCCAI
- Mode: selective
- Destination: oraclesbc.telephony.goog
- Port: 5060 (Range: 1024..65535)
- Transport Method: StaticTLS
- Force Parity: enable
- Ping Method: OPTIONS

Buttons for 'OK' and 'Back' are located at the bottom of the form. The left sidebar shows a tree view of configuration categories, with 'session-recording-server' selected.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration page. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'SolutionsLab-vSBC-2', '10.11.4 SCZ9.2.0 Patch 4 (Build 156)', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the left sidebar shows a tree view with 'session-timer-profile' selected. The main content area is titled 'Add Session Timer Profile' and contains the following fields:

Name	<input type="text" value="SessionTimer"/>
Session Expires	<input (="")<="" 64..999999999=""]="" range:="" td="" type="text" value="900"/>
Min Se	<input (="")<="" 64..999999999=""]="" range:="" td="" type="text" value="90"/>
Force Reinvite	<input type="checkbox"/> enable
Request Refresher	<input type="text" value="uac"/>
Response Refresher	<input type="text" value="uas"/>

At the bottom of the form are 'OK' and 'Back' buttons. The top right of the configuration area includes 'Discard', 'Verify', and 'Save' buttons, along with a 'Show Configuration' button and a 'Show Advanced' toggle.

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.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the 'sip-manipulation' menu item is selected in the left sidebar. The main content area is titled 'Modify SIP Manipulation' and contains the following fields:

- Name: ToGoogle
- Description: sip-manipulation for GoogleCCAI side
- Split Headers: (empty)
- Join Headers: (empty)
- CfgRules: No rules to display. Please add. (with an 'Add' button)

Buttons for 'OK' and 'Back' are located at the bottom of the form.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for adding a SIP manipulation rule. The top navigation bar and left sidebar are consistent with the previous screenshot. The main content area is titled 'Add Sip manipulation / header rule' and contains the following fields:

- Name: ChangeFromIPandPort
- Header Name: From
- Action: sip-manip (dropdown)
- Comparison Type: pattern-rule (dropdown)
- Msg Type: any (dropdown)
- Methods: INVITE x, OPTIONS x
- Match Value: (empty)
- New Value: JACME_NAT_TO_FROM_IP

Buttons for 'OK' and 'Back' are located at the bottom of the form.

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.

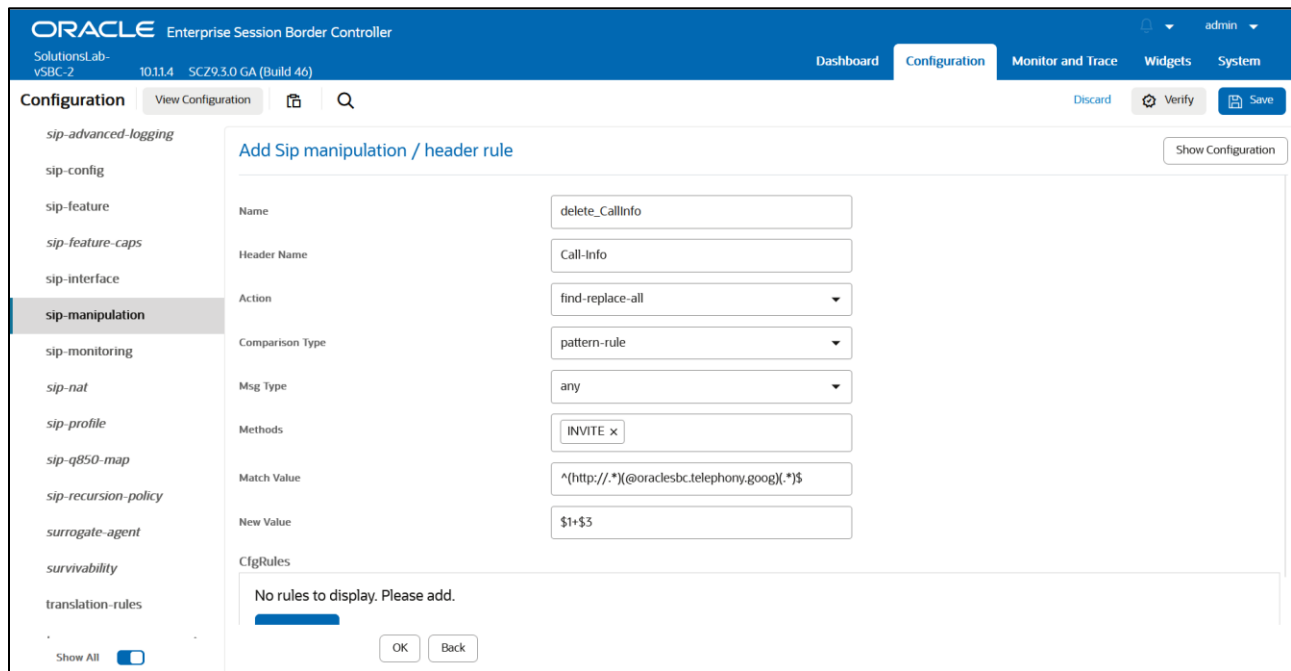
New Value is set to "<http://dialogflow.googleapis.com/v2beta1/projects/ccai-389811/conversations/Re_ "+\$CALL_ID.\$0+ ">;purpose=Goog-ContactCenter-Conversation"

The screenshot displays the Oracle Enterprise Session Border Controller (ESBC) configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'SolutionsLab-vSBC-2', version '10.11.4 SCZ92.0 Patch 4 (Build 156)', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, showing a 'Configuration' section with 'View Configuration', 'Discard', 'Verify', and 'Save' options. A sidebar on the left lists various configuration categories, with 'sip-manipulation' selected. The main area is titled 'Add Sip manipulation / header rule' and contains the following fields:

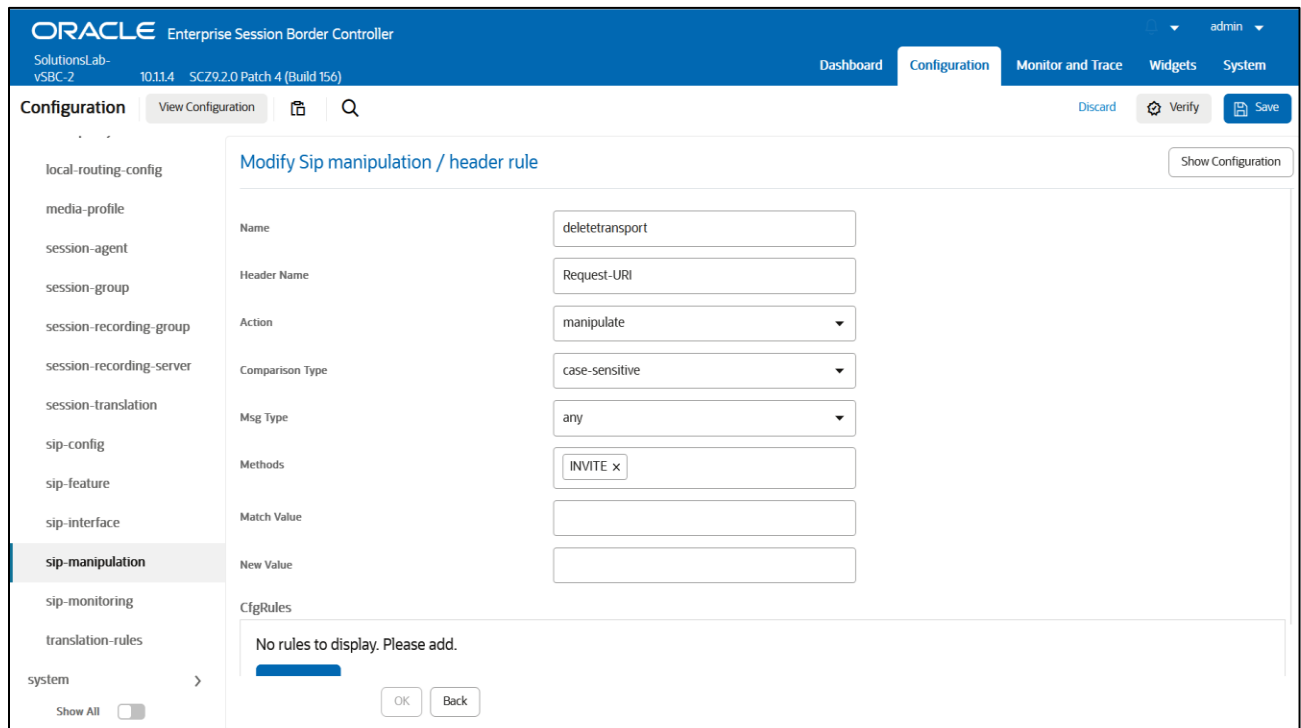
- Name: AddCallInfo
- Header Name: Call-Info
- Action: add
- Comparison Type: case-sensitive
- Msg Type: any
- Methods: INVITE x
- Match Value: (empty)
- New Value: ["<http://dialogflow.googleapis.com/v2beta1/project

Below these fields is a 'CfgRules' section with the message 'No rules to display. Please add.' and 'OK' and 'Back' buttons. A 'Show Configuration' button is located in the top right of the configuration area.

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.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'SolutionsLab-vSBC-2', '10.1.1.4', 'SCZ9.2.0 Patch 4 (Build 156)', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the 'sip-manipulation' category is selected in the left sidebar. The main area displays the 'Add Sip manipulation / header rule / element rule' form with the following fields:

Name	<input type="text" value="delparam"/>
Parameter Name	<input type="text" value="transport"/>
Type	<input type="text" value="uri-param"/>
Action	<input type="text" value="delete-element"/>
Match Val Type	<input type="text" value="any"/>
Comparison Type	<input type="text" value="case-sensitive"/>
Match Value	<input type="text"/>
New Value	<input type="text"/>

Buttons for 'OK' and 'Back' are located at the bottom of the form. A 'Show Configuration' button is also present in the top right corner of the configuration area.

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.

The screenshot shows the 'Modify SIP Interface' configuration page in the SBC GUI. The left sidebar lists various configuration categories, with 'sip-interface' selected. The main area displays several configuration options:

- Route To Registrar: enable
- Secured Network: enable
- Uri Fqdn Domain:
- Options:
- SIP Options: HeaderNatPublicSipIp=20.110.144.248,HeaderNatPr** (highlighted with a red box)
- Trust Mode: all (dropdown menu)
- Max Nat Interval: 3600 (Range: 0.999999999)
- Nat Int Increment: 10 (Range: 0.999999999)
- Nat Test Increment: 30 (Range: 0.999999999)
- SIP Dynamic Hint: enable

Buttons for 'OK' and 'Back' are visible at the bottom of the configuration area.

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



ORACLE

CONNECT WITH US

 blogs.oracle.com/oracle

 facebook.com/Oracle/

 twitter.com/Oracle

 oracle.com

Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2024, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615