

Configuration Guide for Google
CES Agent Handoff Using Oracle
E-SBC Acme Packet 4600 SCZ9.3.0
GA (Build 46)



Table of Contents

1	Audience	4
1.1	Introduction	4
1.1.1	TekVizion Labs	4
2	SIP Trunking Network Components	5
3	Hardware Components	6
4	Software Requirements	6
5	Google CES Certified Oracle E-SBC Versions	6
6	Features	6
6.1	Caveats and Limitations	6
6.2	Failed Testcase	6
7	Configuration	7
7.1	Configuration Checklist	7
7.2	IP Address Worksheet	8
7.3	Google CES API Configuration	9
7.4	Oracle E-SBC Configuration	10
7.4.1	Media Manager	10
7.4.2	Physical Interface	11
7.4.3	Network Interface	13
7.4.4	SIP Config	16
7.4.5	System-Config	19
7.4.6	SIP Monitoring	21
7.4.7	HTTP Server	21
7.4.8	Codec Policy	22
7.4.9	Translation Rules	23
7.4.10	Session Translation	24
7.4.11	Realm Config	25
7.4.12	Steering Pool	34
7.4.13	SDES Profile	35
7.4.14	Media Sec Policy	36
7.4.15	TLS – Certificate Record	38
7.4.16	TLS – TLS Profile	43
7.4.17	Session Timer	43
7.4.18	SIP Interface	44
7.4.19	Session Agent	51
7.4.20	Local Policy	57
7.4.21	SIP Manipulation	60
8	SIP INVITE To Google CES	72
8.1	SIP INVITE for SIPREC call	72
8.2	SIP INVITE for GTP call	72
9	Oracle E-SBC Running configuration file	73

1 Audience

This document is intended for the SIP Trunk customer's technical staff and Value-Added Reseller (VAR) having installation and operational responsibilities.

1.1 Introduction

This configuration guide describes configuration steps for **Google CES Agent Handoff** using **Oracle Enterprise Session Border Controller Acme Packet 4600 SCZ9.3.0 GA (Build 46)**

1.1.1 TekVizion Labs

TekVizion Labs™ is an independent testing and verification facility offered by TekVizion, Inc. TekVizion Labs offers several types of testing services including:

- Remote Testing – provides secure, remote access to certain products in TekVizion Labs for pre-Verification and ad hoc testing.
- Verification Testing – Verification of interoperability performed on-site at TekVizion Labs between two products or in a multi-vendor configuration.
- Product Assessment – independent assessment and verification of product functionality, interface usability, assessment of differentiating features as well as suggestions for added functionality, stress, and performance testing, etc.

TekVizion is a systems integrator specifically dedicated to the telecommunications industry. Our core services include consulting/solution design, interoperability/Verification testing, integration, custom software development and solution support services. Our services help service providers achieve a smooth transition to packet-voice networks, speeding delivery of integrated services. While we have expertise covering a wide range of technologies, we have extensive experience surrounding our practice areas which include SIP Trunking, Packet Voice, Service Delivery, and Integrated Services.

The TekVizion team brings together experience from the leading service providers and vendors in telecom. Our unique expertise includes legacy switching services and platforms, and unparalleled product knowledge, interoperability, and integration experience on a vast array of VoIP and other next-generation products. We rely on this combined experience to do what we do best: help our clients advance the rollout of services that excite customers and result in new revenues for the bottom line. TekVizion leverages this real-world, multi-vendor integration and test experience and proven processes to offer services to vendors, network operators, enhanced service providers, large enterprises and other professional services firms. TekVizion's headquarters, along with a state-of-the-art test lab and Executive Briefing Center, is located in Plano, Texas.

For more information on TekVizion and its practice areas, please visit [TekVizion Labs website](#).

2 SIP Trunking Network Components

The network for the SIP Trunk reference configuration is illustrated below and is representative of Google CES Agent Handoff with Oracle Enterprise Session Border Controller (E-SBC) Acme Packet 4600 SCZ9.3.0 GA (Build 46) configuration.

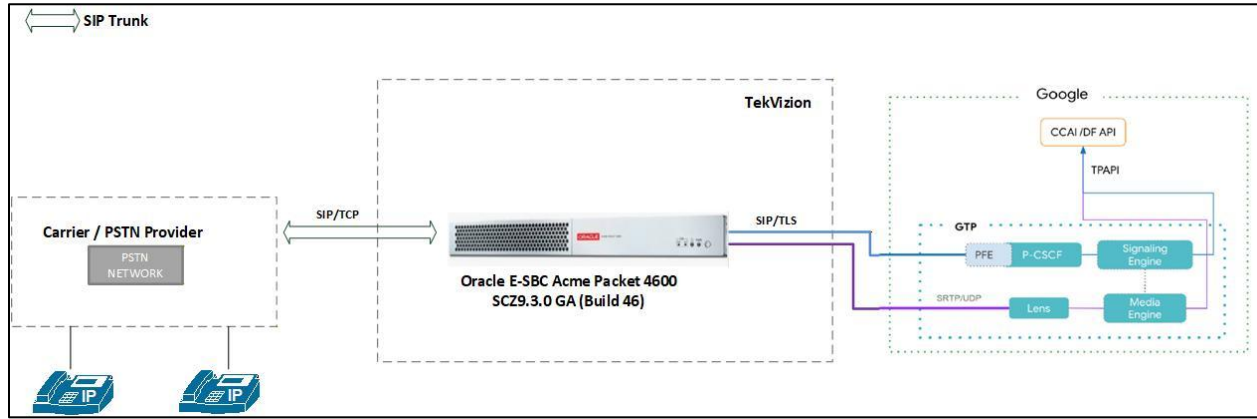


Figure 1: SIP Trunk Lab Reference Network

The lab network consists of the following components.

- Google CES cloud Environment
- Oracle E-SBC Acme Packet 4600
- PSTN Gateway

3 Hardware Components

- Oracle E-SBC Acme Packet 4600

4 Software Requirements

- Oracle E-SBC Acme Packet 4600 SCZ9.3.0 GA (Build46)

5 Google CES Certified Oracle E-SBC Versions

Table 1 – Google CES Certified Oracle E-SBC Version

Google CES Certified Oracle E-SBC Version	
Oracle E-SBC 4600	SCZ9.3.0 GA (Build46)

6 Features

6.1 Caveats and Limitations

DTLS	DTLS towards Google CES is not tested
------	---------------------------------------

6.2 Failed Testcase

- None

7 Configuration

7.1 Configuration Checklist

Below are the steps that are required to configure Oracle E-SBC.

Table 1 – Oracle E-SBC Configuration Steps

Step	Description	Reference
Step 1	Media Manager	Section 7.4.1
Step 2	Physical Interface	Section 7.4.2
Step 3	Network Interface	Section 7.4.3
Step 4	SIP Config	Section 7.4.4
Step 5	System-Config	Section 7.4.5
Step 6	SIP Monitoring	Section 7.4.6
Step 7	HTTP Server	Section 7.4.7
Step 8	Codec Policy	Section 7.4.8
Step 9	Translation Rules	Section 7.4.9
Step 10	Session Translation	Section 7.4.10
Step 11	Realm Config	Section 7.4.11
Step 12	Steering Pool	Section 7.4.12
Step 13	SDES Profile	Section 7.4.13
Step 14	Media Sec Policy	Section 7.4.14
Step 15	TLS – Certificate Record	Section 7.4.15
Step 16	TLS – TLS Profile	Section 7.4.16
Step 17	Session Timer	Section 7.4.17
Step 18	SIP Interface	Section 7.4.18
Step 19	Session Agent	Section 7.4.19
Step 20	Local Policy	Section 7.4.20
Step 21	SIP Manipulation	Section 7.4.21

7.2 IP Address Worksheet

The specific values listed in the table below and in subsequent sections are used in the lab configuration described in this document are for **illustrative purposes only**.

Table 3 - IP Address Worksheet

Component	IP Address
Google CES	
Signaling	us.telephony.goog:5672
Media	74.125.X.X
PSTN Gateway	
LAN IP Address	172.16.X.X
Oracle E-SBC	
LAN IP Address	10.80.X.X
WAN IP Address	192.65.X.X

7.3 Google CES API Configuration

Below link can be referred for troubleshooting Google CES API configuration for Agent Handoff.

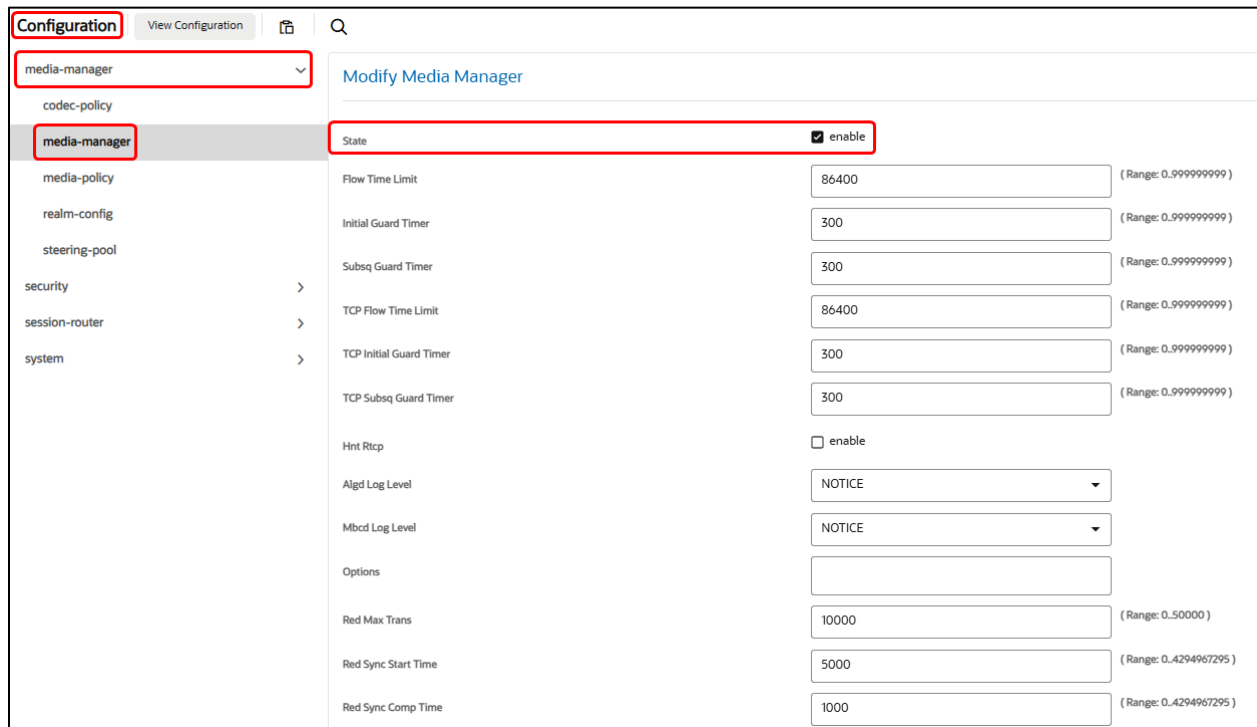
<https://docs.cloud.google.com/contact-center/insights/docs/troubleshooting>

7.4 Oracle E-SBC Configuration

The following is the example configuration of Oracle E-SBC for Google CES Agent Handoff.

7.4.1 Media Manager

- Media-Manager handles the media stack required for SIP sessions on the E-SBC. Media Manager is configured as shown below
- Navigate to **Configuration** → **media-manager** → **media-manager**

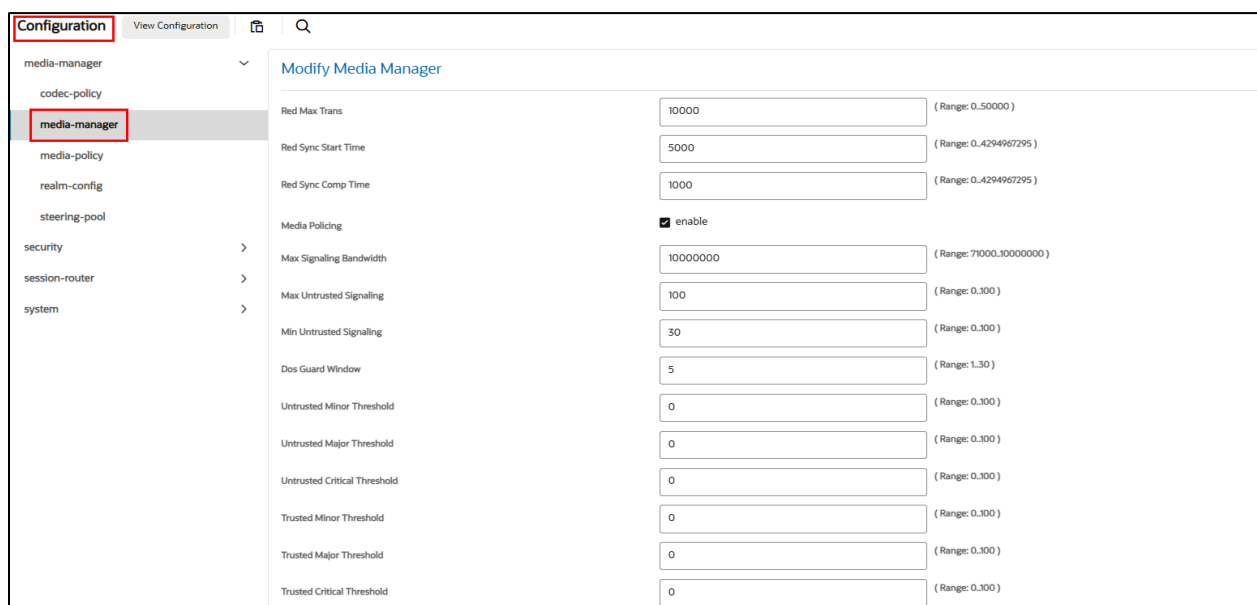


Configuration	View Configuration	Q
media-manager		
codecs-policy		
media-manager		
media-policy		
realm-config		
steering-pool		
security	>	
session-router	>	
system	>	

Modify Media Manager

State	☒ 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)
Hnt Rtcp	☐ enable
Algd Log Level	NOTICE
Mbcd Log Level	NOTICE
Options	
Red Max Trans	10000 (Range: 0.50000)
Red Sync Start Time	5000 (Range: 0.4294967295)
Red Sync Comp Time	1000 (Range: 0.4294967295)

Figure 2: Media Manager Configuration



Configuration	View Configuration	Q
media-manager		
codecs-policy		
media-manager		
media-policy		
realm-config		
steering-pool		
security	>	
session-router	>	
system	>	

Modify Media Manager

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	☒ enable
Max Signalling Bandwidth	10000000 (Range: 7000.10000000)
Max Untrusted Signalling	100 (Range: 0.300)
Min Untrusted Signalling	30 (Range: 0.300)
Dos Guard Window	5 (Range: 1.30)
Untrusted Minor Threshold	0 (Range: 0.300)
Untrusted Major Threshold	0 (Range: 0.300)
Untrusted Critical Threshold	0 (Range: 0.300)
Trusted Minor Threshold	0 (Range: 0.300)
Trusted Major Threshold	0 (Range: 0.300)
Trusted Critical Threshold	0 (Range: 0.300)

Figure 3: Media Manager Configuration (Cont.)

7.4.2 Physical Interface

- Navigate to **Configuration** → **system** → **phy-interface**.
- Configure Physical interface towards Google CES and PSTN Gateway as shown below.

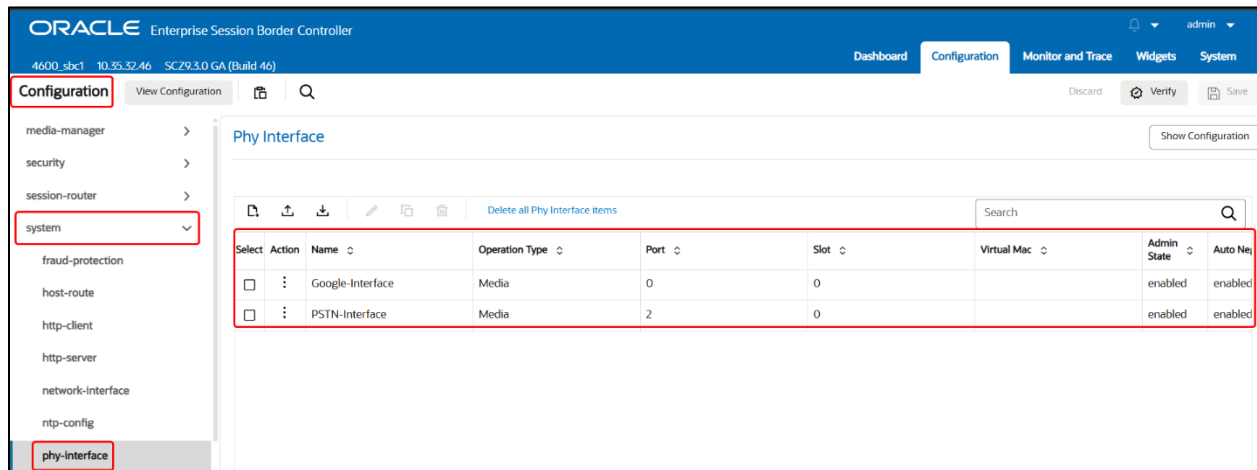


Figure 4: Physical Interfaces

- The interface designated towards Google CES is named as Google-Interface (Slot 0, Port 0).

The screenshot shows the 'Configuration' menu on the left with 'system' and 'phy-interface' highlighted. The main area is titled 'Modify Phy Interface'. A red box highlights the following fields:

- Name: Google-Interface
- Operation Type: Media
- Port: 0 (Range: 0..5)
- Slot: 0 (Range: 0)

Other visible fields include Virtual Mac, Admin State (checked), Auto Negotiation (checked), Duplex Mode (FULL), Speed (100), Wancom Health Score (50), and Network Alarm Threshold (No network alarm threshold to display).

Figure 5: Physical Interface towards Google CES

- The interface designated towards PSTN Gateway are named as PSTN-Interface (Slot 0, Port 2).

The screenshot shows the 'Configuration' menu on the left with 'system' and 'phy-interface' highlighted. The main area is titled 'Modify Phy Interface'. A red box highlights the following fields:

- Name: PSTN-Interface
- Operation Type: Media
- Port: 2 (Range: 0..5)
- Slot: 0 (Range: 0)

Other visible fields include Virtual Mac, Admin State (checked), Auto Negotiation (unchecked), Duplex Mode (FULL), Speed (100), Wancom Health Score (50), and Network Alarm Threshold.

Figure 6: Physical Interface towards PSTN Gateway

7.4.3 Network Interface

- Navigate to **Configuration** → **system** → **network-interface**.
- Configure network interface towards Google CES, and PSTN Gateway as shown below.

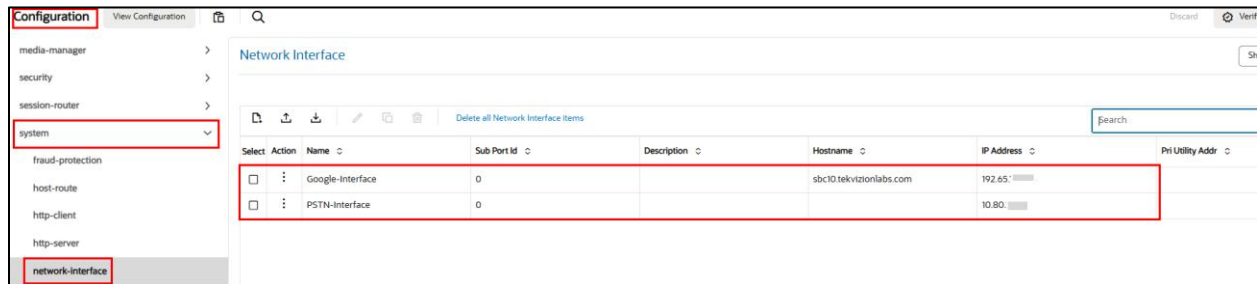


Figure 7: Network Interfaces

- Configure Network interface towards Google CES as shown below.

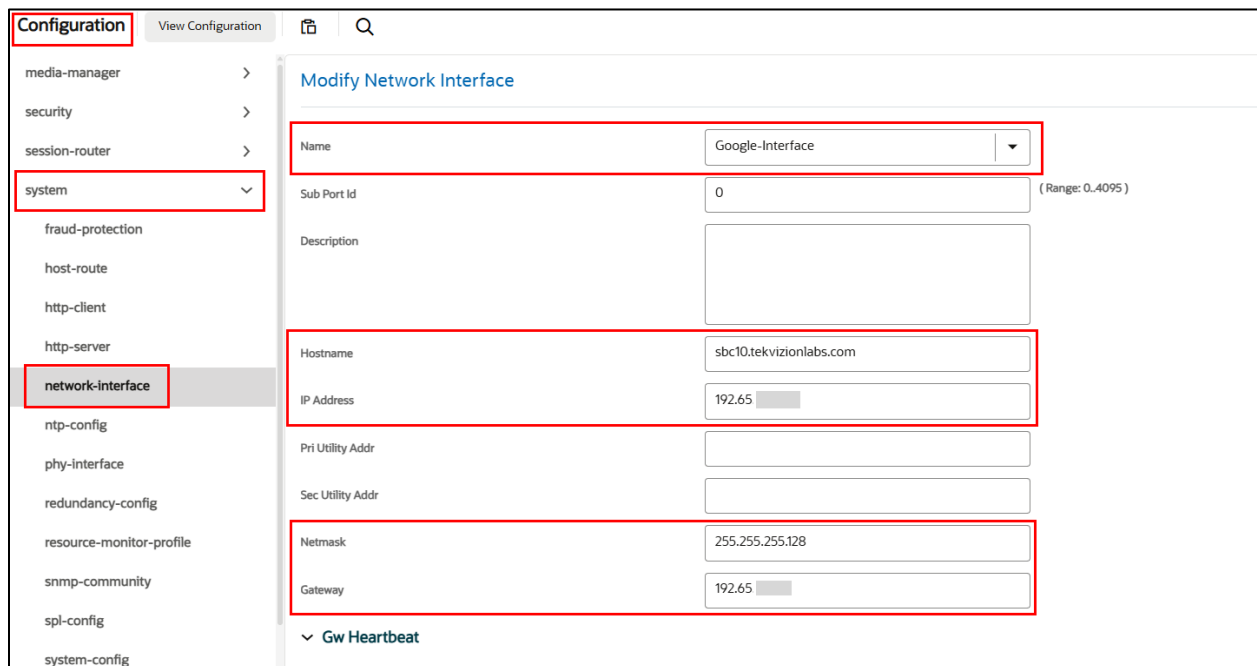


Figure 8: Network Interface towards Google CES

Configuration View Configuration

media-manager >
security >
session-router >
system >
fraud-protection
host-route
http-client
http-server
network-interface
ntp-config
phy-interface
redundancy-config
resource-monitor-profile
snmp-community

Modify Network Interface

Gw Heartbeat

State ☒ enable

Heartbeat (Range: 0..65535)
 Retry Count (Range: 0..65535)
 Retry Timeout (Range: 1..65535)
 Health Score (Range: 0..100)

Bfd Config

State ☐ enable
 Health Score (Range: 0..100)
 Options
 Bfd Session

Figure 9: Network Interface towards Google CES (Cont.)

Configuration View Configuration

security >
session-router >
system >
fraud-protection
host-route
http-client
http-server
network-interface
ntp-config
phy-interface
redundancy-config
resource-monitor-profile
snmp-community
spl-config
system-config

Modify Network Interface

DNS IP Primary
 DNS IP Backup1
 DNS IP Backup2
DNS Domain
 DNS Timeout (Range: 1..999999999)
 DNS Max Ttl (Range: 30..2073600)
 Signaling Mtu (Range: 0..576..4096)
 HIP IP List
 ICMP Address
 SSH Address
 Tunnel Config

Figure 10: Network Interface towards Google CES (Cont.)

- Configure the Network interface towards PSTN Gateway as shown below.

Configuration View Configuration

media-manager >
security >
session-router >
system >
fraud-protection
host-route
http-client
http-server
network-interface
ntp-config
phy-interface
redundancy-config
resource-monitor-profile
snmp-community
spl-config
system-config
trap-receiver

Modify Network Interface

Name PSTN-Interface
Sub Port Id 0 (Range: 0..4095)
Description
Hostname
IP Address 10.80.13.50
Pri Utility Addr
Sec Utility Addr
Netmask 255.255.255.0
Gateway 10.80.13.1
Gw Heartbeat
State ☒ enable
Heartbeat 10 (Range: 0..65535)
Retry Count 3 (Range: 0..65535)
Retry Timeout 3 (Range: 1..65535)

Figure 11: Network Interface towards PSTN Gateway

Configuration View Configuration

media-manager >
security >
session-router >
system >
fraud-protection
host-route
http-client
http-server
network-interface
ntp-config
phy-interface
redundancy-config
resource-monitor-profile
snmp-community
spl-config
system-config
trap-receiver

Modify Network Interface

BFD Session
No bfd session to display. Please add.
Add
DNS IP Primary
DNS IP Backup1
DNS IP Backup2
DNS Domain
DNS Timeout 11 (Range: 1..999999999)
DNS Max Ttl 86400 (Range: 30..2073600)
Signalling Mtu 0 (Range: 0..576..4096)
HIP IP List 10.80.13.50 x
ICMP Address 10.80.13.50 x
SSH Address

Figure 12: Network Interface towards PSTN Gateway (Cont.)

- **Note:** ICMP IP and HIP IP addresses needs to be disabled in production environment.

7.4.4 SIP Config

- Navigate to **Configuration** → **session-router** → **sip-config** for SIP configuration as shown below.

The screenshot shows the 'Configuration' menu on the left, with 'session-router' expanded and 'sip-config' selected. The main area displays the 'Modify SIP Config' form. The form includes the following fields:

Field	Value	Range
State	☒ enable	
Dialog Transparency	☒ enable	
Home Realm ID	Google	
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)
Trans Expire	32	(Range: 0.2147473)
Initial Inv Trans Expire	0	(Range: 0.2147473)
Invite Expire	180	(Range: 0.999999999)
Session Max Life Limit	0	

Figure 13: SIP-Config

The screenshot shows the continuation of the 'Modify SIP Config' form. The form includes the following fields:

Field	Value	Range
Enforcement Profile		
Emergency Dscp Profile		
Red Max Trans	10000	(Range: 0.50000)
Options	max-udp-length=0 x	
SPL Options		
SIP Message Len	65535	(Range: 0.65535)
Enum Sag Match	☐ enable	
Extra Method Stats	☒ enable	
Extra Enum Stats	☐ enable	
Registration Cache Limit	0	(Range: 0.999999999)
Register Use To For Lp	☐ enable	
Refer Src Routing	☐ enable	
Atcf Stn Sr		
Atcf Psi Dn		

Figure 14: SIP-Config (Cont.)

Configuration

View Configuration

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

session-translation

sip-config

sip-feature

sip-interface

Modify SIP Config

Atcf Route To Scas

☐ enable

Eatf Stn Sr

Sag Lookup On Redirect

☐ enable

Set Disconnect Time On Bye

☐ enable

Refer Reinvite No Sdp

☐ enable

Msrp Delayed Bye Timer

15

(Range: 0..60)

Transcoding Realm

▾

Transcoding Agents

Create Dynamic Sa

☐ enable

Node Functionality

P-CSCF

▾

Match SIP Instance

☐ enable

Sa Routes Stats

☐ enable

Sa Routes Traps

☐ enable

Rx SIP Reason Mapping

☐ enable

Figure 15: SIP-Config (Cont.)

Configuration

View Configuration

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

session-translation

sip-config

sip-feature

sip-interface

Modify SIP Config

Add Ue Location In Pani

inherit

▾

Hold Emergency Calls For Loc Info

0

(Range: 0..4294967295)

Retry After Upon Offline

0

(Range: 0..999999999)

Reg Reject Response Upon Offline

503

Hold Invite Calls For Loc Info

0

(Range: 0..4294967295)

Cache Loc Info Expire

32

(Range: 0..4294967295)

Msg Hold For Loc Info

0

(Range: 0..30)

Npli Upon Register

inherit

▾

Start Hold Timer Event

AAR

▾

Hist To Div For Cause 380

inherit

▾

Anonymize History For Untrusted

☐ enable

Asymm Preconditions Evs Swb Support

☐ enable

Sms Report Timeout

32

(Range: 1..100000)

User Agent

Figure 16: SIP-Config (Cont.)

Configuration

View Configuration

🏠

🔍

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

Modify SIP Config

Reg Reject Response Upon Offline

503

Hold Invite Calls For Loc Info

0

(Range: 0.4294967295)

Cache Loc Info Expire

32

(Range: 0.4294967295)

Msg Hold For Loc Info

0

(Range: 0.30)

NpI Upon Register

inherit

▾

Start Hold Timer Event

AAR

▾

Hist To Div For Cause 380

inherit

▾

Anonymize History For Untrusted

☐ enable

Asymm Preconditions Evs Swb Support

☐ enable

Sms Report Timeout

32

(Range: 1.100000)

User Agent

Precondition Enhancement

☐ enable

Precondition Med Enhancement

☐ enable

Internal 503 Threshold

0

(Range: 0.300)

Internal 503 Lower Threshold

40

(Range: 1.95)

503 Alarm Monitoring Time

15

(Range: 5.600)

Figure 17: SIP-Config (Cont.)

7.4.5 System-Config

- Navigate to **Configuration** → **system** → **system-config** for system configuration as shown below.

The screenshot shows the 'Modify System Config' page. The left sidebar has 'system' highlighted, and 'system-config' is selected. The main form has the following fields:

- Hostname: Oracle
- Description: SBC Connecting PSTN SIP Trunk to Google
- Location: Plano TX
- Mib System Contact: (empty)
- Mib System Name: (empty)
- Mib System Location: (empty)
- Acp TLS Profile: (empty)
- Disable Garp Out Of Subnet: ☐ enable
- SNMP Enabled: ☒ enable
- Enable SNMP Auth Traps: ☐ enable

Figure 18: System-Config

The screenshot shows the 'Modify System Config' page, specifically the 'system-config' section. The left sidebar has 'system' highlighted, and 'system-config' is selected. The main form has the following fields:

- Call Trace: ☐ enable
- Default Gateway: 10.35.32.1
- Restart: ☒ enable
- Telnet Timeout: 0 (Range: 0..65535)
- Console Timeout: 0 (Range: 0..65535)
- HTTP Timeout: 5 (Range: 0..20)
- Reserved Nsep Session Capacity: 0 (Range: 0..100)
- Alarm Threshold: No alarm threshold to display. Please add.
 [Add](#)
- Source Routing: ☐ enable
- Debug Timeout: 0 (Range: 0..65535)
- Ecc Chk Pkt: ☐ enable
- Log TLS Key: ☐ enable
- Pko Rake Pkt: 0 (Range: 0..32768)
- Pko Rake Burst: 0 (Range: 0..3024)

Figure 19: System-Config (Cont.)

Configuration

View Configuration

media-manager>

security>

session-router>

system

fraud-protection

host-route

http-client

http-server

network-interface

ntp-config

phy-interface

redundancy-config

resource-monitor-profile

snmp-community

spl-config

system-config

trap-receiver

Modify System Config

Ecc Chk Pkt☐ enable

Log TLS Key☐ enable

Pko Rake Pkt (Range: 0..32768)

Pko Rake Burst (Range: 0..3024)

Default V6 Gateway

Ipv6 Signalling Mtu (Range: 1280..4096)

Ipv4 Signalling Mtu (Range: 576..4096)

Directory Cleanup

No directory cleanup to display. Please add or upload directory cleanup.

AddUpload

SNMP Rate Limit (Range: 0..9999)

HttpClient Max Total Conn (Range: 0..2147483647)

HttpClient Max Cpu Load (Range: 30..90)

HttpClient Cache Size Multiplier (Range: 4..50)

HTTP ClearDead Conn Timer (Range: 0..300..86400)

Resource Monitoring☐ enable

Figure 20: System-Config (Cont.)

7.4.6 SIP Monitoring

- Navigate to **Configuration** → **session-router** → **sip-monitoring** and configure SIP monitoring for capturing trace as shown below.

Configuration View Configuration

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
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring

Modify SIP Monitoring

Match Any Filter ☒ enable

State ☒ enable

Short Session Duration (Range: 0.999999999)

Monitoring Filters

Interesting Events

No interesting event to display. Please add.

Trigger Window (Range: 0.999999999)

Figure 21: SIP Monitoring

7.4.7 HTTP Server

- Navigate to **Configuration** → **system** → **http-server** and configure HTTP Server for GUI access to Oracle E-SBC as shown below.

Configuration View Configuration

media-manager >
security >
session-router >
system >
fraud-protection
host-route
http-client
http-server
network-interface
ntp-config
phy-interface
redundancy-config
resource-monitor-profile
snmp-community

Modify HTTP Server

Name

State ☒ enable

Realm

IP Address

HTTP State ☒ enable

HTTP Port (Range: 1.65535)

HTTP Strict Transport Security Policy ☐ enable

HTTPS State ☐ enable

HTTPS Port (Range: 1.65535)

HTTP Interface List

Figure 22: HTTP Server

7.4.8 Codec Policy

- Navigate to **Configuration** → **media-manager** → **codec-policy** and configure codec policy for Google CES as shown below.

The screenshot displays the 'Configuration' interface. On the left, a sidebar lists various configuration categories: 'media-manager', 'media-policy', 'realm-config', 'steering-pool', 'security', 'session-router', and 'system'. The 'media-manager' category is selected, and within it, the 'codec-policy' sub-category is highlighted. The main area is titled 'Modify Codec Policy Entries'. A red box highlights the configuration fields for the 'Google' entry. These fields include: 'Name' (Google), 'Allow Codescs' (telephone-event, PCMU, PCMA), 'Add Codescs On Egress' (PCMU, PCMA), 'Order Codescs' (PCMU, PCMA, telephone-event), and 'Packetization Time' (20). Below these fields, there are several checkboxes and dropdown menus for additional settings: 'Force Ptime' (enable), 'Secure Dtmf Cancellation' (enable), 'Dtmf In Audio' (disabled), 'Tone Detection' (empty), 'Tone Detect Renegotiate Timer' (500), 'Reverse Fax Tone Detection Reinvite' (enable), 'Fax Single M Line' (disabled), and 'Evrc Tty Baudot Transcode' (enable).

Figure 23: Codec Policy for Google CES

7.4.9 Translation Rules

- Navigate to **Configuration** → **session-router** → **translation-rules** and configure translation rules for Google CES as shown below.
- Translation rule is created to send E.164 number format towards Google CES.
- These translation rules (adding or removing plus) are further mapped in Session Translation [Section 7.4.10](#)

Select	Action	Id	Description	Input Header Type	Input Header Value	Output Header Type	Output Header Value
☐	add	addplus1_called-header	add	called-header	^(0)(.*)\$	called-header	\$01+\$02
☐	add	addplus1_calling-header	add	calling-header	^(0)(.*)\$	calling-header	\$01+\$02
☐	add	addplus1_p-asserted-id-header	add	p-asserted-id-header	^(0)(.*)\$	p-asserted-id-header	\$01+\$02
☐	add	addplus1_request-uri	add	request-uri	^(0)(.*)\$	request-uri	\$01+\$02
☐	delete	removeplus1_called-header	delete	called-header	^(.*)\+!l(.*)\$	called-header	\$!\$2
☐	delete	removeplus1_calling-header	delete	calling-header	^(.*)\+!l(.*)\$	calling-header	\$!\$2
☐	delete	removeplus1_p-asserted-id-header	delete	p-asserted-id-header	^(.*)\+!l(.*)\$	p-asserted-id-header	\$!\$2
☐	delete	removeplus1_request-uri	delete	request-uri	^(.*)\+!l(.*)\$	request-uri	\$!\$2

Figure 24: Translation Rule to add or remove E.164 format Google CES

7.4.10 Session Translation

- Navigate to **Configuration** → **session-router** → **session-translation**. The translation rules configured in Section 7.4.9 is mapped to Google CES is shown below.

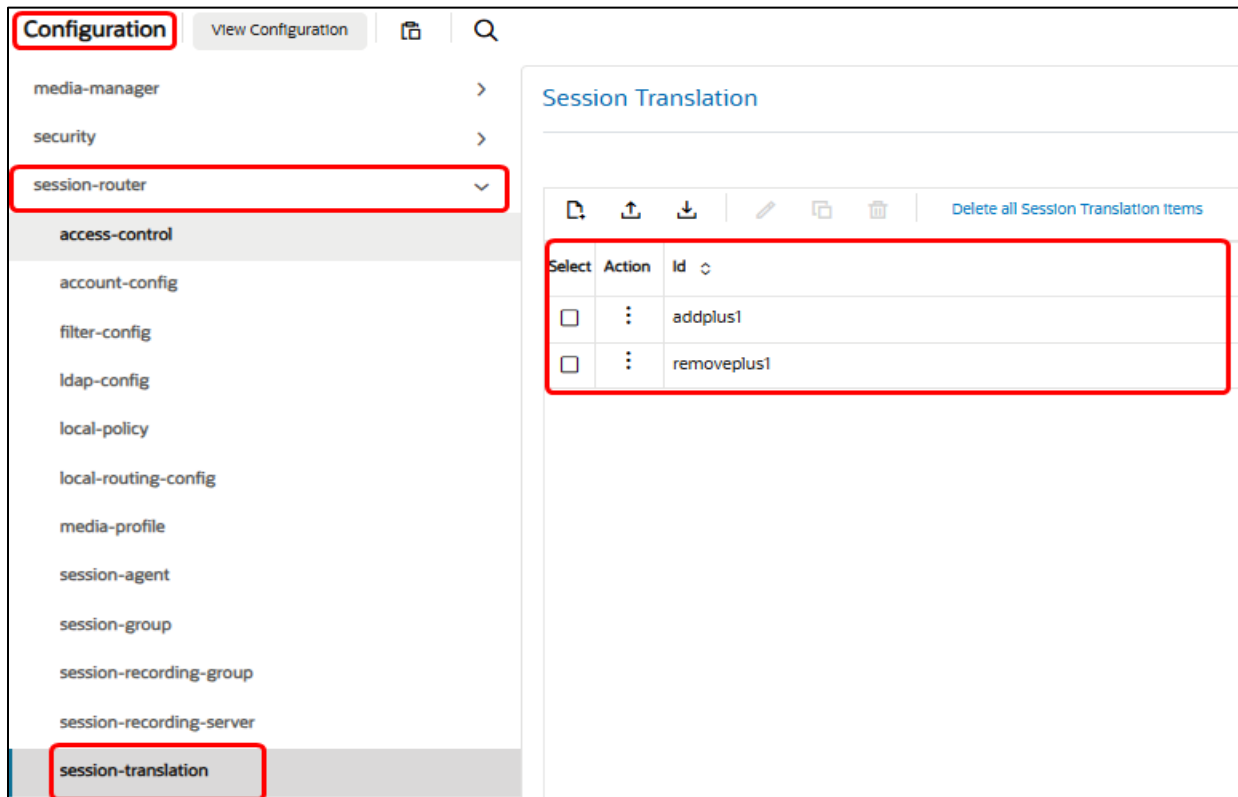


Figure 25: Session Translation towards Google CES

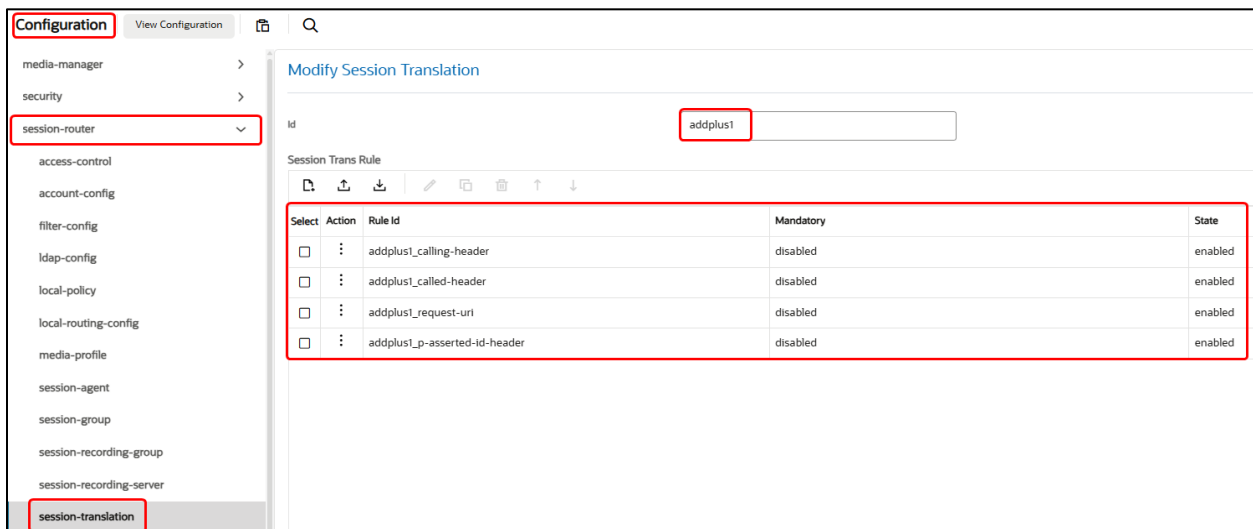


Figure 26: Session Translation for addplus1 towards Google CES (Cont.)

- Under removeplus1, we are removing the translation rules for created on [Section 7.4.9](#)

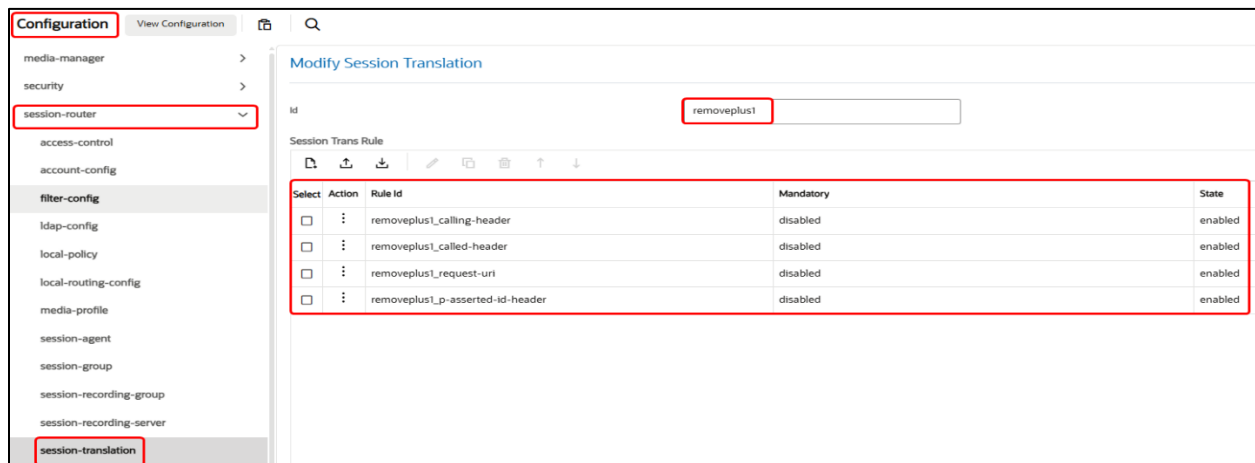


Figure 27: Session Translation for removeplus1 towards Google CES (Cont.)

7.4.11 Realm Config

- Navigate to **Configuration** → **media-manager** → **realm-config**.

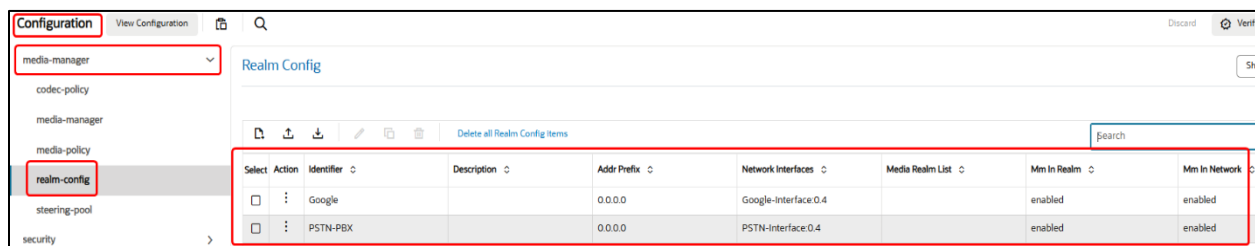


Figure 28: Realm Configuration

- Realm Config towards Google CES is shown below.

Configuration View Configuration

media-manager **realm-config**

Modify Realm Config

Identifier	Google
Description	
Addr Prefix	0.0.0.0
Network Interfaces	Google-Interface:0.4 x
Media Realm List	
Mm In Realm	☒ enable
Mm In Network	☒ enable
Mm Same Ip	☒ enable
QoS Enable	☒ enable
Max Bandwidth	0 (Range: 0.999999999)
Max Priority Bandwidth	0 (Range: 0.999999999)
Parent Realm	

Figure 29: Realm Config

Configuration View Configuration

media-manager **realm-config**

Modify Realm Config

DNS Realm	
Media Policy	
Nsep Media Policy	
Media Sec Policy	SRTP
RTCP Mux	☐ enable
Ice Profile	
Teams Fqdn	
Teams Fqdn In Uri	☐ enable
SDP Inactive Only	☐ enable
DTLS Srtip Profile	
Srtip Msm Passthrough	☐ enable
Class Profile	

Figure 30: Realm Config towards Google CES (Cont.)

Configuration

View Configuration

media-manager

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

In Session Translations

No in session translation list to display. Please add.

Add

Out Session Translations

Select	Action	Out Session Translation Id	State
☐	:	addplus1	enabled

Figure 31: Realm Config towards Google CES (Cont.)

Configuration

View Configuration

media-manager

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

In ManipulationId

Out ManipulationId

GoogleManipulation

Average Rate Limit

0

(Range: 0.4294967295)

Access Control Trust Level

high

Max Inbound Per Session Burst Rate

30

(Range: 1.999999999)

Burst Rate Window Per Session

1

(Range: 1.999999999)

Dos Action At Session

none

Invalid Signal Threshold

0

(Range: 0.4294967295)

Maximum Signal Threshold

0

(Range: 0.4294967295)

Untrusted Signal Threshold

0

(Range: 0.4294967295)

Nat Trust Threshold

0

(Range: 0.65535)

Max Endpoints Per Nat

0

(Range: 0.65535)

Nat Invalid Message Threshold

0

(Range: 0.65535)

Wait Time For Invalid Register

0

(Range: 0,4_300)

Figure 32: Realm Config towards Google CES (Cont.)

Configuration

View Configuration

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

Deny Period

30

(Range: 0..4294967295)

Session Max Life Limit

0

Untrust Cac Failure Threshold

0

(Range: 0..4294967295)

Subscription Id Type

END_USER_NONE

Trunk Context

Early Media Allow

Enforcement Profile

Additional Prefixes

Restricted Latching

none

Options

SPL Options

Delay Media Update

☐ enable

Refer Call Transfer

disabled

Hold Refer Reinvite

☐ enable

Figure 33: Realm Config towards Google CES (Cont.)

Configuration

View Configuration

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

Refer Notify Provisional

none

Dyn Refer Term

☐ enable

Codect Policy

Google

Codect ManIP In Realm

☐ enable

Codect ManIP In Network

☒ enable

RTCP Policy

Constraint Name

Session Recording Server

Session Recording Required

☐ enable

SIP Profile

Flow Time Limit

-1

(Range: -1..2147483647)

Initial Guard Timer

-1

(Range: -1..2147483647)

Subsq Guard Timer

-1

(Range: -1..2147483647)

TCP Flow Time Limit

-1

(Range: -1..2147483647)

Figure 34: Realm Config towards Google CES (Cont.)

Configuration

View Configuration

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

TCP Initial Guard Timer

-1

(Range: -1..2147483647)

TCP Subsq Guard Timer

-1

(Range: -1..2147483647)

SIP Isup Profile

QoS Constraint

Hide Egress Media Update

☐ enable

TCP Media Profile

Monitoring Filters

Node Functionality

Default Location String

Alt Family Realm

Pref Addr Type

none

Sm Icsi Match For Invite

Sm Icsi Match For Message

Figure 35: Realm Config towards Google CES (Cont.)

Configuration

View Configuration

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

Ringback Trigger

none

Ringback File

Merge Early Dialogs

☐ enable

User Site

Srvcc Trfo

Feature Trfo

Auth Attribute

No auth attributes to display. Please add.

Add

Fqdn Hostname

Fqdn Hostname In Header

P Asserted Identity

P Asserted Identity For

Steering Pool Threshold

0

(Range: 0..100)

Figure 36: Realm Config towards Google CES (Cont.)

Configuration View Configuration

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

Modify Realm Config

Srvcc Trfo

Feature Trfo

Auth Attribute

No auth attributes to display. Please add.

Add

Fqdn Hostname

Fqdn Hostname In Header

P Asserted Identity

P Asserted Identity For

Steering Pool Threshold 0 (Range: 0..100)

Steering Pool Lower Threshold 70 (Range: 1..95)

Steering Pool Alarm Monitoring Time 15 (Range: 5..600)

Suppress Hold Resume Reinvite ☐ enable

SNMP Sipmethod Stats ☐ enable

Figure 37: Realm Config towards Google CES (Cont.)

- Realm Config towards PSTN Gateway is shown below.

Configuration View Configuration

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

Modify Realm Config

DNS Realm

Media Policy

Nsep Media Policy

Media Sec Policy RTP

RTCP Mux ☐ enable

Ice Profile

Teams Fqdn

Teams Fqdn In Uri ☐ enable

SDP Inactive Only ☐ enable

DTLS Srtp Profile

Srtp Msm Passthrough ☐ enable

Class Profile

Figure 38: Realm Config towards PSTN Gateway

Configuration

View Configuration

media-manager

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

Displaying 1 - 1 of 1

In ManipulationId		
Out ManipulationId		
Average Rate Limit	0	(Range: 0.4294967295)
Access Control Trust Level	none	
Max Inbound Per Session Burst Rate	30	(Range: 1.999999999)
Burst Rate Window Per Session	1	(Range: 1.999999999)
Dos Action At Session	none	
Invalid Signal Threshold	0	(Range: 0.4294967295)
Maximum Signal Threshold	0	(Range: 0.4294967295)
Untrusted Signal Threshold	0	(Range: 0.4294967295)
Nat Trust Threshold	0	(Range: 0.65535)
Max Endpoints Per Nat	0	(Range: 0.65535)
Nat Invalid Message Threshold	0	(Range: 0.65535)
Wait Time For Invalid Register	0	(Range: 0.4.300)

Figure 39: Realm Config towards PSTN Gateway (Cont.)

Configuration

View Configuration

media-manager

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

Displaying 1 - 1 of 1

In ManipulationId		
Out ManipulationId		
Average Rate Limit	0	(Range: 0.4294967295)
Access Control Trust Level	none	
Max Inbound Per Session Burst Rate	30	(Range: 1.999999999)
Burst Rate Window Per Session	1	(Range: 1.999999999)
Dos Action At Session	none	
Invalid Signal Threshold	0	(Range: 0.4294967295)
Maximum Signal Threshold	0	(Range: 0.4294967295)
Untrusted Signal Threshold	0	(Range: 0.4294967295)
Nat Trust Threshold	0	(Range: 0.65535)
Max Endpoints Per Nat	0	(Range: 0.65535)
Nat Invalid Message Threshold	0	(Range: 0.65535)
Wait Time For Invalid Register	0	(Range: 0.4.300)

Figure 40: Realm Config towards PSTN Gateway (Cont.)

Configuration

View Configuration

media-manager

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

Refer Notify Provisional

none

Dyn Refer Term

☐ enable

Codec Policy

Google

Codec ManIP In Realm

☐ enable

Codec ManIP In Network

☒ enable

RTCP Policy

Constraint Name

Session Recording Server

Session Recording Required

☐ enable

SIP Profile

Flow Time Limit

-1

(Range: -1_2147483647)

Initial Guard Timer

-1

(Range: -1_2147483647)

Subsq Guard Timer

-1

(Range: -1_2147483647)

TCP Flow Time Limit

-1

(Range: -1_2147483647)

Figure 41: Realm Config towards PSTN Gateway (Cont.)

Configuration

View Configuration

media-manager

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

TCP Initial Guard Timer

-1

(Range: -1_2147483647)

TCP Subsq Guard Timer

-1

(Range: -1_2147483647)

SIP Isup Profile

QoS Constraint

Hide Egress Media Update

☐ enable

TCP Media Profile

Monitoring Filters

Node Functionality

Default Location String

Alt Family Realm

Pref Addr Type

none

Sm Icsi Match For Invite

Sm Icsi Match For Message

Figure 42: Realm Config towards PSTN Gateway (Cont.)

Configuration

View Configuration

Q

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

Ringback Trigger

none

Ringback File

Merge Early Dialogs

☐ enable

User Site

Srvcc Trfo

Feature Trfo

Auth Attribute

No auth attributes to display. Please add.

Add

Fqdn Hostname

Fqdn Hostname In Header

P Asserted Identity

P Asserted Identity For

Steering Pool Threshold

0

(Range: 0..100)

Figure 43: Realm Config towards PSTN Gateway (Cont.)

Configuration

View Configuration

Q

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

Srvcc Trfo

Feature Trfo

Auth Attribute

No auth attributes to display. Please add.

Add

Fqdn Hostname

Fqdn Hostname In Header

P Asserted Identity

P Asserted Identity For

Steering Pool Threshold

0

(Range: 0..100)

Steering Pool Lower Threshold

70

(Range: 1..95)

Steering Pool Alarm Monitoring Time

15

(Range: 5..600)

Suppress Hold Resume Reinvite

☐ enable

SNMP Sipmethod Stats

☐ enable

Figure 44: Realm Config towards PSTN Gateway (Cont.)

7.4.12 Steering Pool

- Navigate to **Configuration** → **media-manager** → **steering-pool**.
- Steering pool allows configuration to assign IP address, ports, and a realm.
- Steering Pool Configuration towards PSTN Gateway are shown below.

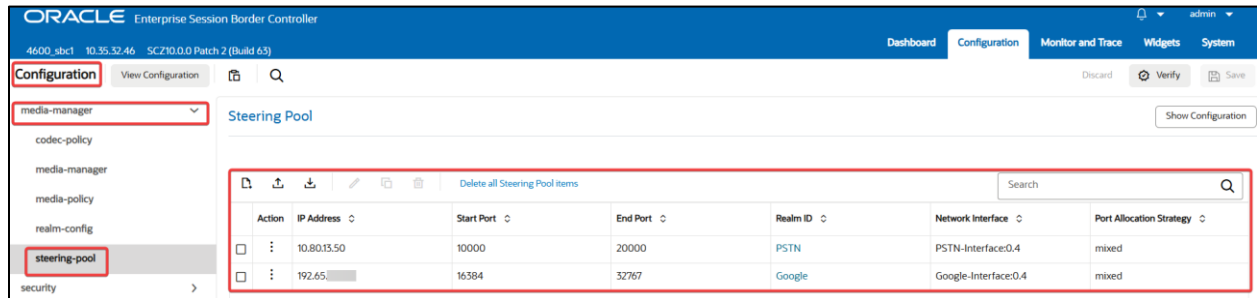


Figure 45: Steering Pool

- Steering Pool Configuration towards Google CES is shown below.

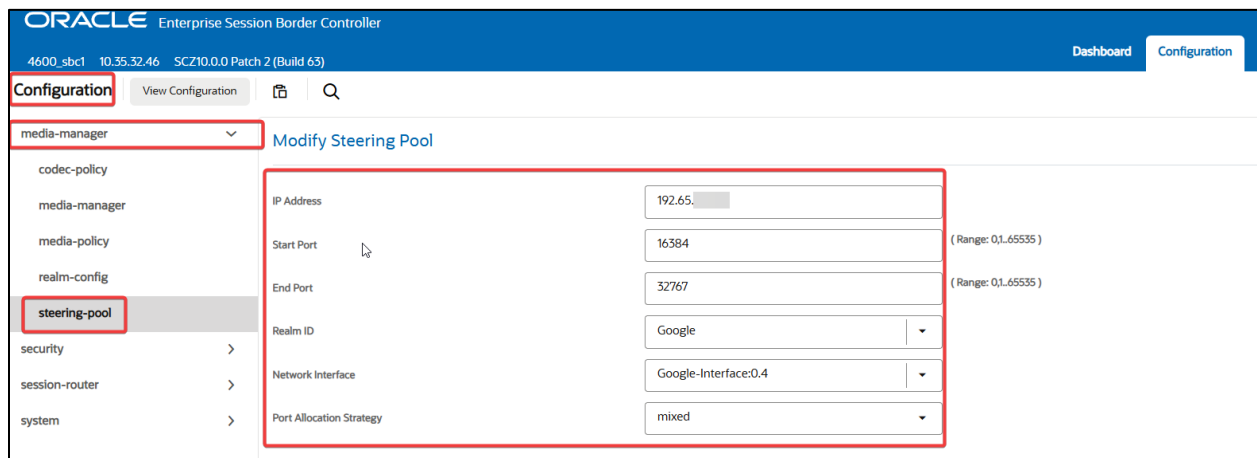


Figure 46: Steering Pool towards Google CES

- Steering Pool Configuration towards PSTN Gateway is shown below.

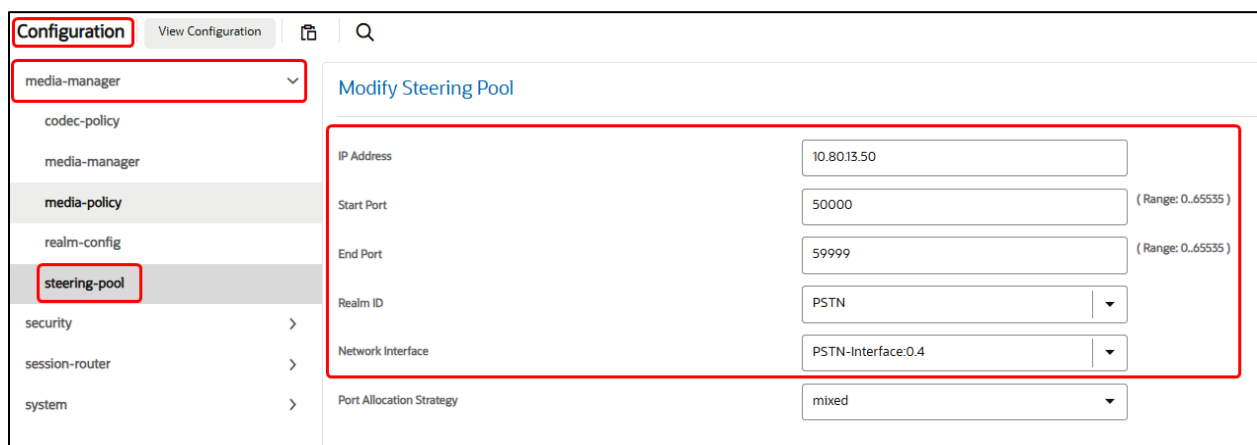


Figure 47: Steering Pool towards PSTN

7.4.13 SDES Profile

- Navigate to **Configuration** → **Security** → **media-security** → **sdes-profile** and con SDES profile as shown below.

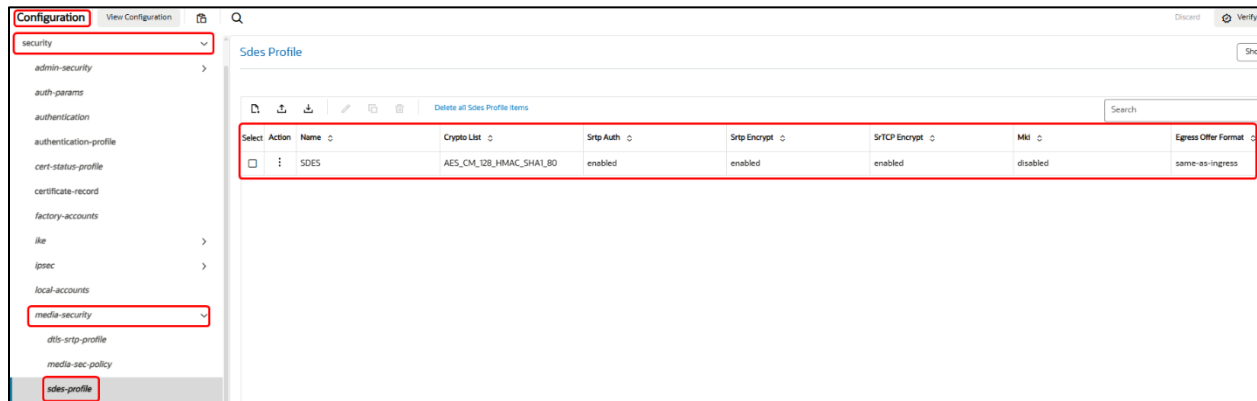


Figure 48: SDES Profile for TLS

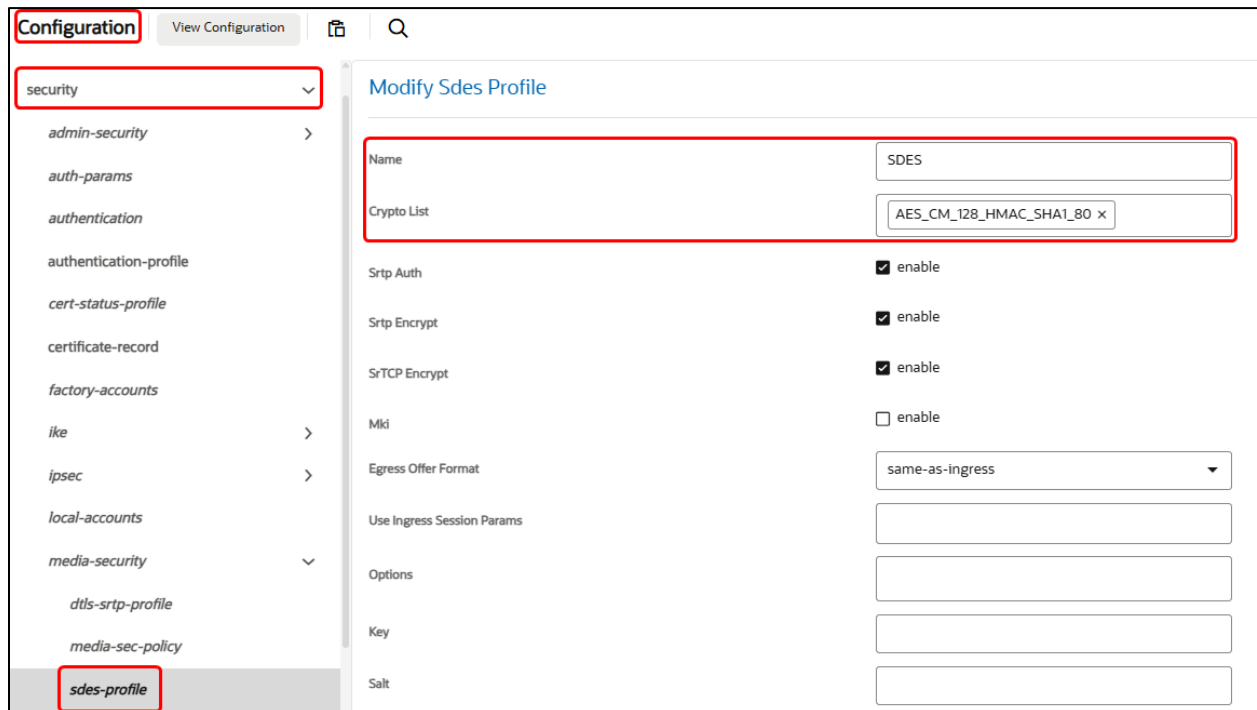


Figure 49: SDES Profile for TLS (Cont.)

7.4.14 Media Sec Policy

- Navigate to **Configuration** → **security** → **media-security** → **media-sec-policy** and configure media security policy as shown below.

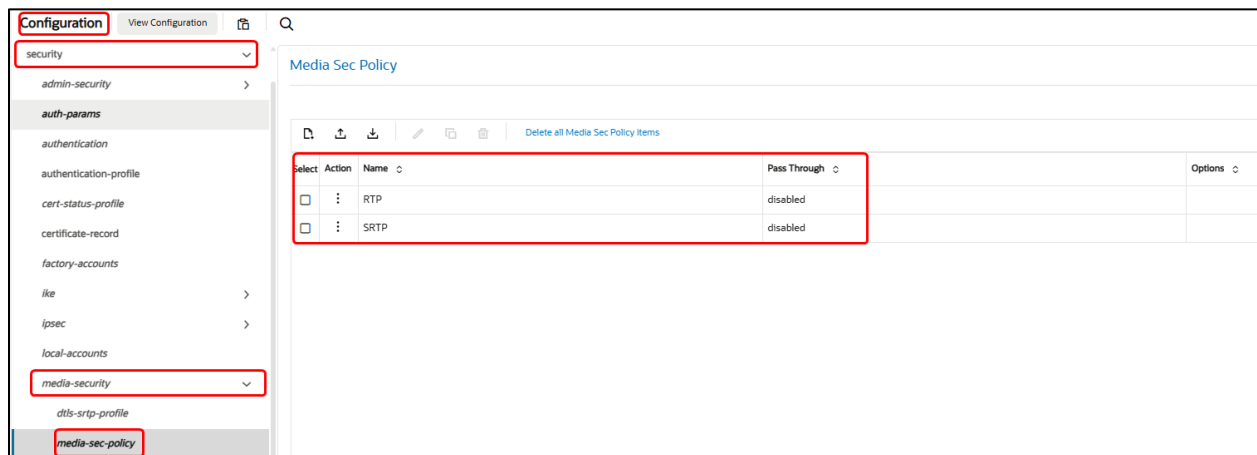


Figure 50: Media Security Policy

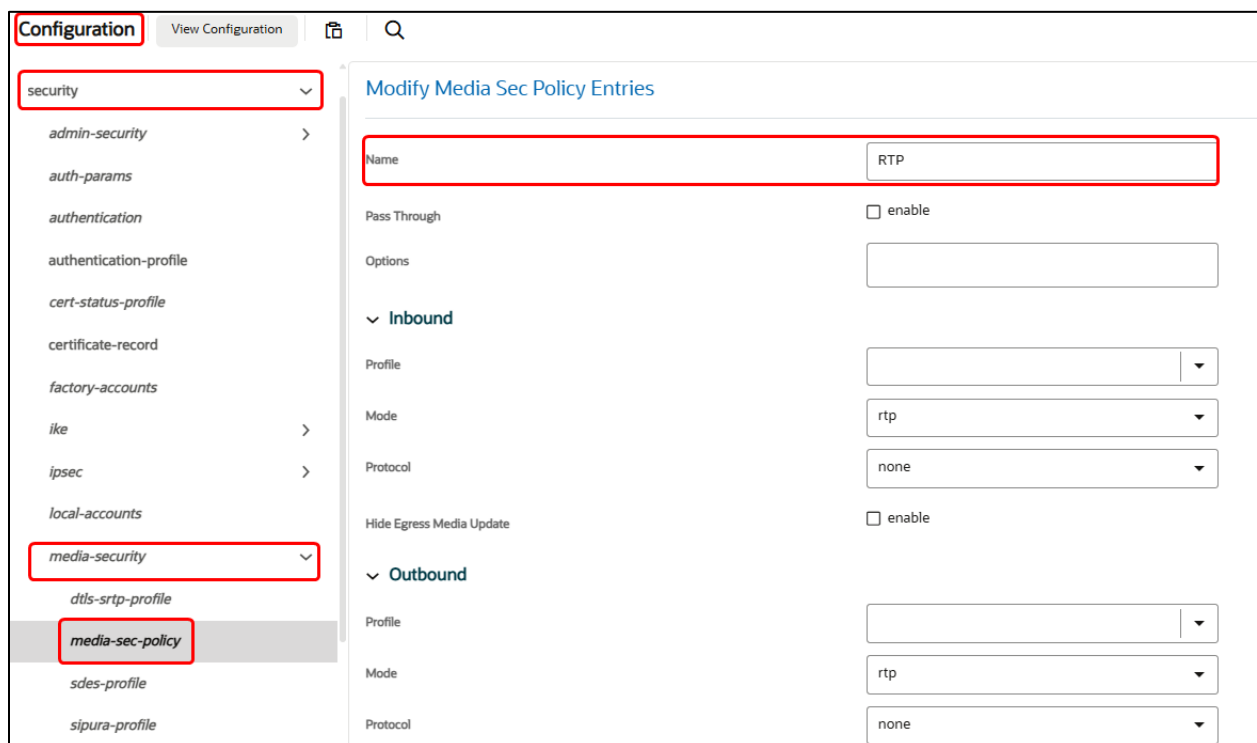


Figure 51: Media Security Policy for RTP

- SDES profile created in [Section 7.4.14](#) is associated with Media Security Policy for SRTP below.

The screenshot displays the 'Configuration' page in a network device's web interface. The left sidebar shows a tree view of configuration categories: 'media-manager', 'security', 'admin-security', 'auth-params', 'authentication', 'authentication-profile', 'cert-status-profile', 'certificate-record', 'factory-accounts', 'ike', 'ipsec', 'local-accounts', 'media-security', 'dtls-srtp-profile', 'media-sec-policy', 'sdes-profile', and 'sipura-profile'. The 'media-sec-policy' item is highlighted. The main content area is titled 'Modify Media Sec Policy Entries'. It contains two sections: 'Inbound' and 'Outbound'. Each section has a 'Name' field (set to 'SRTP'), a 'Pass Through' checkbox (unchecked), an 'Options' field, and a 'Hide Egress Media Update' checkbox (unchecked). The 'Inbound' section has three dropdown menus: 'Profile' (set to 'SDES'), 'Mode' (set to 'srtp'), and 'Protocol' (set to 'sdes'). The 'Outbound' section has three dropdown menus: 'Profile' (set to 'SDES'), 'Mode' (set to 'srtp'), and 'Protocol' (set to 'sdes'). Red boxes highlight the 'Name' field, the 'Inbound' section, and the 'Outbound' section.

Configuration View Configuration

media-manager >

security >

admin-security >

auth-params

authentication

authentication-profile

cert-status-profile

certificate-record

factory-accounts

ike >

ipsec >

local-accounts

media-security >

dtls-srtp-profile

media-sec-policy

sdes-profile

sipura-profile

Modify Media Sec Policy Entries

Name: SRTP

Pass Through: ☐ enable

Options:

▼ Inbound

Profile: SDES

Mode: srtp

Protocol: sdes

Hide Egress Media Update: ☐ enable

▼ Outbound

Profile: SDES

Mode: srtp

Protocol: sdes

Figure 52: Media Security Policy for SRTP

7.4.15 TLS – Certificate Record

- Certificate Record are configuration elements on Oracle E-SBC which captures information for a TLS certificate such as common-name, key-size etc.
- Navigate to **Configuration** → **security** → **certificate-record**.

Certificate record for Oracle E-SBC:

- Create a certificate record for Oracle E-SBC as shown below.

The screenshot displays the Oracle E-SBC Configuration interface. On the left, a navigation sidebar shows the hierarchy: Configuration (highlighted), security (expanded), and certificate-record (selected). The main content area is titled 'Modify Certificate Record'. It contains a form with the following fields and values:

Field	Value
Name	sbc10
Country	US
State	Texas
Locality	Plano
Organization	tekvisionlabs
Unit	tekvision
Common Name	sbc10.tekvisionlabs.com
Key Size	2048
Alternate Name	
Trusted	☒ enable
Key Usage List	digitalSignature x keyEncipherment x
Extended Key Usage List	serverAuth x clientAuth x
Key Algor	rsa

Figure 53: Create Certificate Record for Oracle E-SBC

- Select the Certificate record and Click Generate icon to generate CSR.

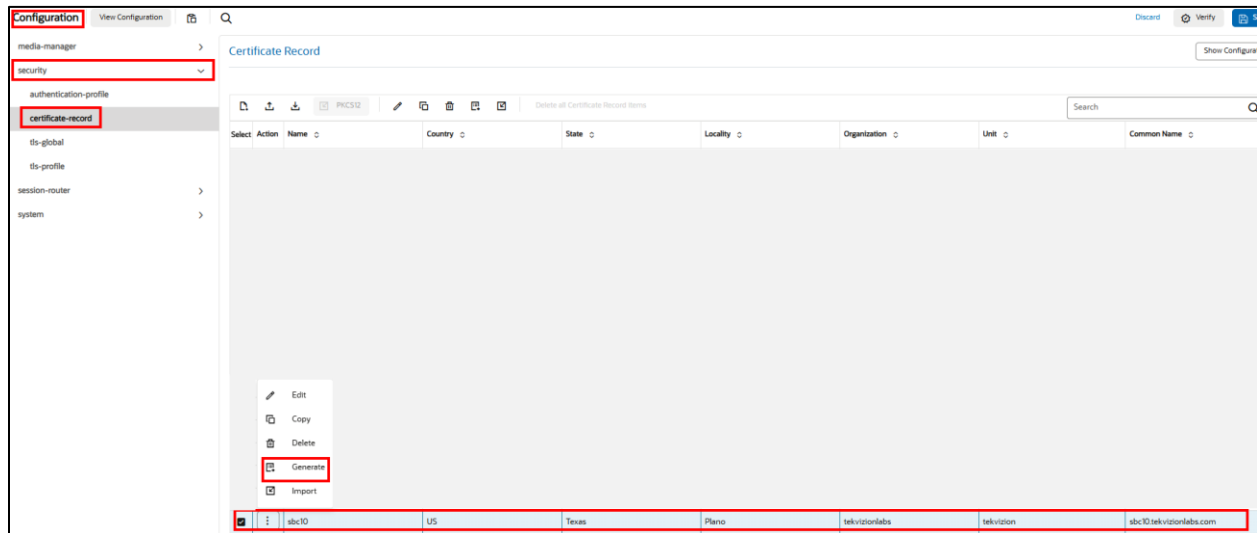


Figure 54: Generate Certificate Record for Oracle E-SBC

- Get the CSR signed by respective approved CAs and further uploaded by clicking Import to import the signed certificate.

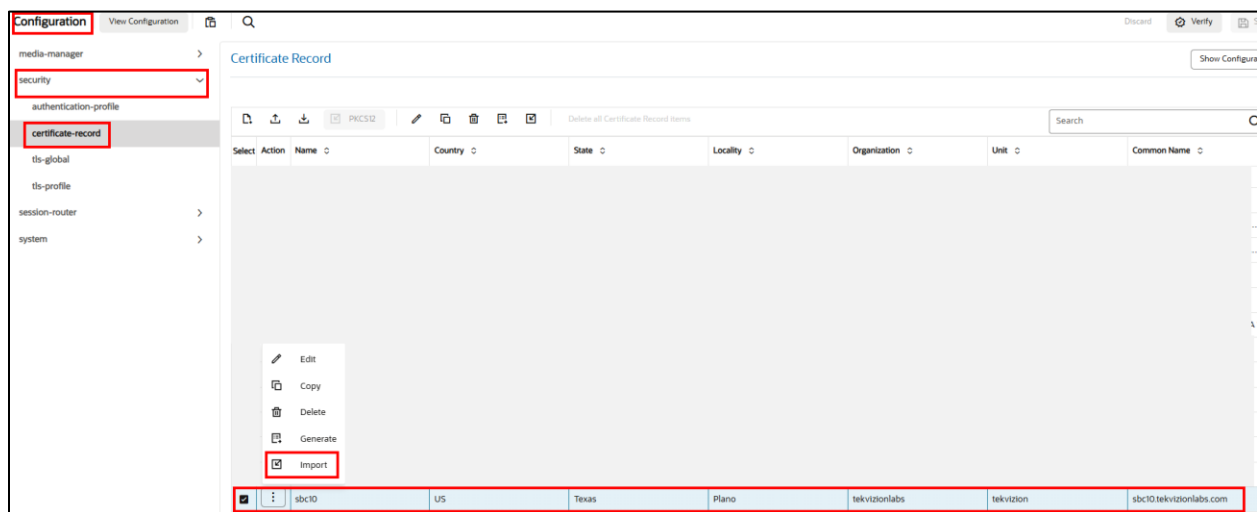


Figure 55: Import Certificate Record for Oracle E-SBC

- Import the root certificate stored in the local machine and click Import as shown below.

Import Certificate

Format: try-all

Import Method: ☒ File ☐ Paste

Certificate File: Upload 9c: 7.pem

Import Cancel

Figure 56: Import Certificate Record for Oracle E-SBC

Certificate record for Google Root CA:

- Visit Google certificate link via <https://pki.goog/roots.pem> and download the roots PEM file.
- Open the PEM file using notepad and copy the certificate under label “GTS Root R1”
- Create a certificate record GTS Root R1 for Google CES.

Configuration View Configuration

media-manager >
security >
authentication-profile
certificate-record
tls-global
tls-profile
session-router >
system >

Modify Certificate Record

Name: GTS_Root_R1
Country: US
State: MA
Locality: Burlington
Organization: Engineering
Unit:
Common Name:
Key Size: 2048
Alternate Name:
Trusted: ☒ enable
Key Usage List: digitalSignature x keyEncipherment x
Extended Key Usage List: serverAuth x
Key Algor: rsa
Digest Algor: sha256

Figure 57: Create Certificate Record for Google GTS Root R1 certificate

- Right click on the Certificate Record and Click Import.

Configuration View Configuration

media-manager >
security >
authentication-profile
certificate-record
tls-global
tls-profile
session-router >
system >

Certificate Record

Select Action Name Country State Locality Organization Unit Common Name

☒	⋮	GTS_Root_R1	US	MA	Burlington	Engineering		
☐	Edit	potCAGOOGL	us	Texas	Plano	tekvisionlabs	Tekvision	
☐	Copy	IoT_CA_G2	US	TX	Plano	Tekvisionlabs		Go Daddy Root Certificate Authori...
☐	Delete	cure_CA_G2	US	TX	Plano	Tekvisionlabs		Go Daddy Secure Certificate Auth...
☐	Generate	ICA	US	Texas	Plano	tekvisionLabs	tekvision	
☐	Import		US	MA	Burlington	Engineering		
☐			US	TX	Plano	Tekvisionlabs		IdenTrust Commercial Root CA 1

Figure 58: Import Google GTS Root R1 certificate

- Import the root certificate stored in the local machine and click Import as shown below.

Import Certificate

Format: try-all

Import Method: ☒ File ☐ Paste

Certificate File: GTS_Root_R1.pem

Figure 59: Import Google GTS Root R1 certificate (Cont.)

- Similarly create other certificate records for the Oracle E-SBC leaf certificate and the Certificate Authority Root certificate, ensuring the entire certificate chain from leaf to root is present as shown below. The following certificate-records are required on the Oracle E-SBC to connect with Google CES.

Configuration

media-manager >

security >

authentication-profile

certificate-record

tls-global

tls-profile

session-router >

system >

Certificate Record

Select	Action	Name	Country	State	Locality	Organization	Unit	Common Name
☐	⋮	GTS_Root_R1	US	MA	Burlington	Engineering		
☐	⋮	GoDaddy_Root_CA_G2	US	TX	Plano	Tekvizionlabs		Go Daddy Root Certificate Aut...
☐	⋮	GoDaddy_Secure_CA_G2	US	TX	Plano	Tekvizionlabs		Go Daddy Secure Certificate A...

Figure 60: Certificate Records

7.4.16 TLS – TLS Profile

- A TLS profile configuration on the Orace E-SBC allows for specific certificates to be assigned.
- Navigate to **Configuration → security → tls-profile**
- Create a TLS profile for Google CES as shown below.

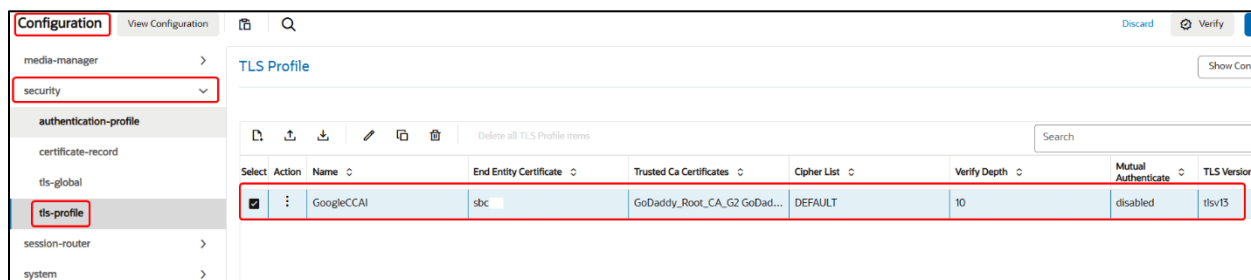


Figure 61: TLS Profile for Google CES

- Intermediate Certificates and Google GTS Root R1 certificate is added for TLS exchange.

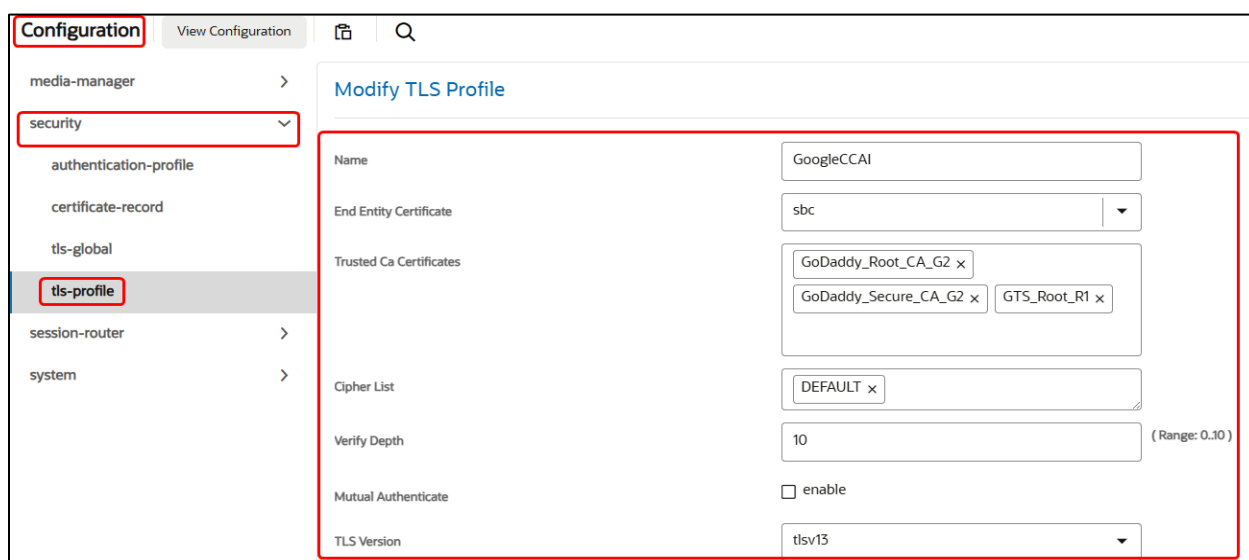


Figure 62: TLS Profile for Google CES (Cont.)

7.4.17 Session Timer

- Navigate to **Configuration → session-router → session-timer-profile**.
- Configure session timer for Google CES as shown below.

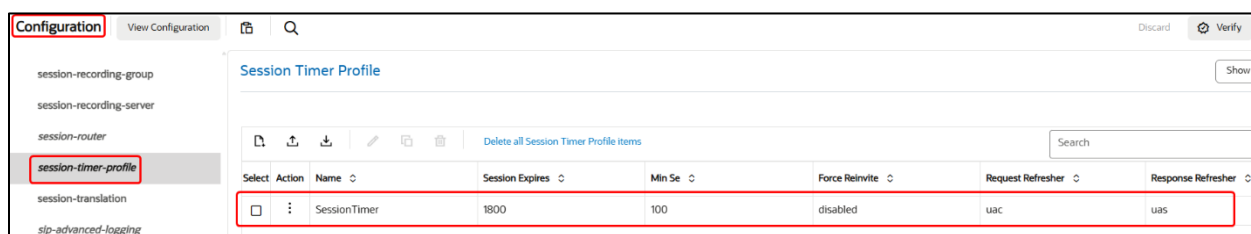


Figure 63: Session Timer

7.4.18 SIP Interface

- Navigate to **Configuration** → **session-router** → **sip-interface**.

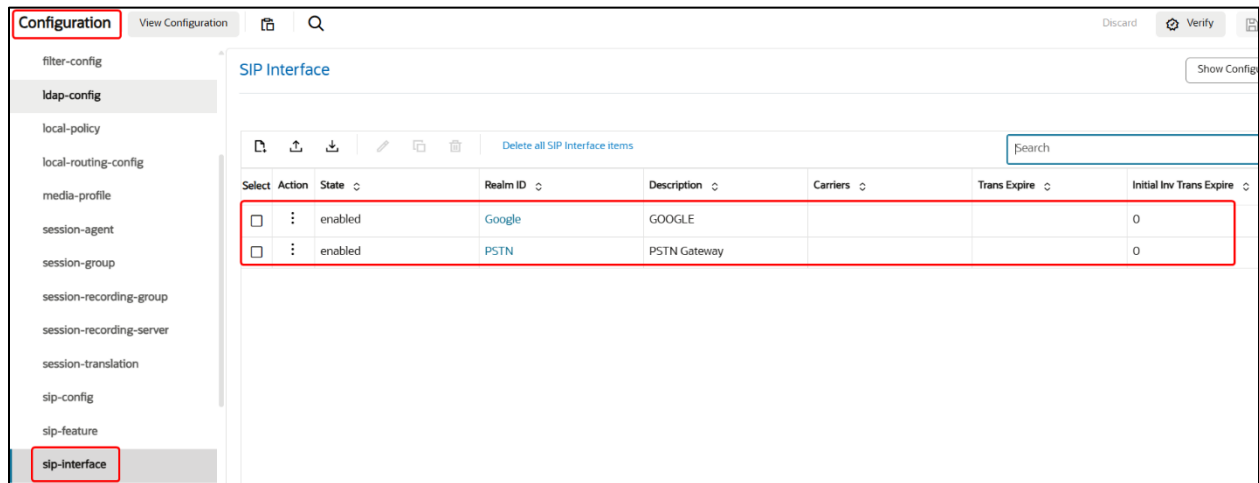


Figure 64: SIP Interface

- Create SIP interface towards PSTN Gateway by adding SIP Ports as shown below.

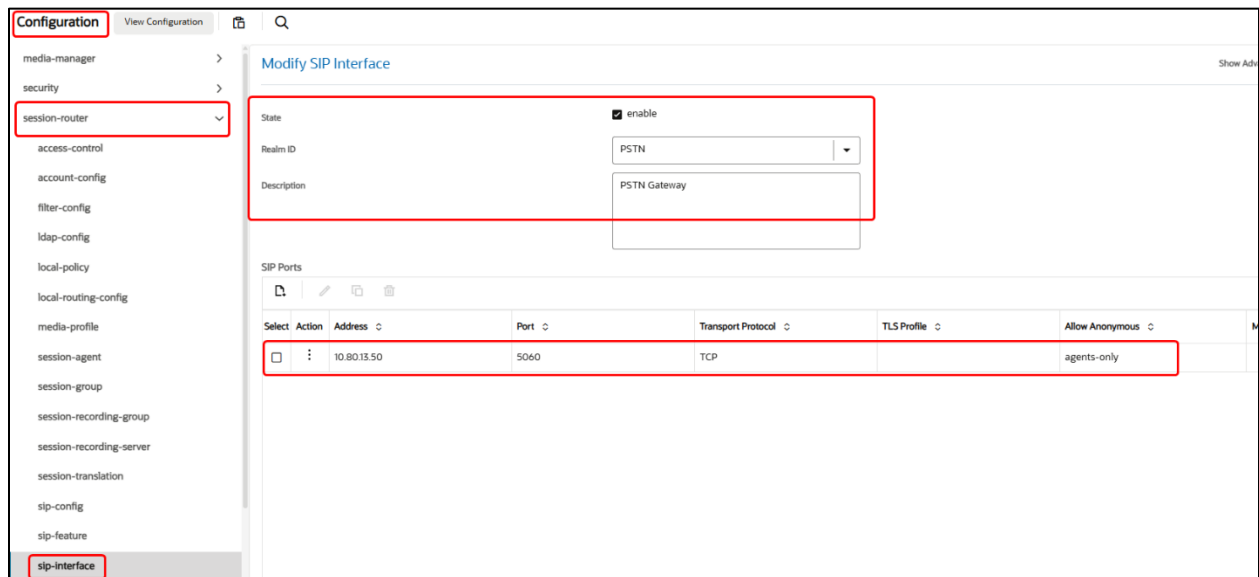


Figure 65: SIP Interface for PSTN Gateway

Configuration

View Configuration

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

session-translation

sip-config

sip-feature

sip-interface

Modify SIP Interface

Initial Inv Trans Expire

0

(Range: 0..2147473)

Session Max Life Limit

0

Proxy Mode

Redirect Action

Nat Traversal

none

Nat Interval

30

(Range: 1..99999999)

TCP Nat Interval

90

(Range: 0..99999999)

Registration Caching

☒ enable

Min Reg Expire

300

(Range: 0..99999999)

Registration Interval

3600

(Range: 1..99999999)

Route To Registrar

☒ enable

Secured Network

☐ enable

Uri Fqdn Domain

Options

Figure 66: SIP Interface for PSTN Gateway (Cont.)

Configuration

View Configuration

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

system >

Modify SIP Interface

SPL Options

Trust Mode

all

Max Nat Interval

3600

(Range: 0..99999999)

Nat Int Increment

10

(Range: 0..99999999)

Nat Test Increment

30

(Range: 0..99999999)

SIP Dynamic Hint

☐ enable

TCP Max Nat Interval

3600

(Range: 0..99999999)

TCP Nat Int Increment

10

(Range: 0..99999999)

TCP Nat Test Increment

30

(Range: 0..99999999)

TCP SIP Dynamic Hint

☐ enable

Stop Recurse

401,407

Port Map Start

0

(Range: 0,1025..65535)

Port Map End

0

(Range: 0,1025..65535)

In ManipulationId

Figure 67: SIP Interface for PSTN Gateway (Cont.)

Configuration

View Configuration

Q

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

session-translation

sip-config

sip-feature

sip-interface

Modify SIP Interface

Out ManipulationId

PSTNOUTBOUND ▾

SIP Atcf Feature

☐ enable

Rfc2833 Payload

101 (Range: 96..127)

Rfc2833 Mode

transparent ▾

Response Map

▾

Local Response Map

▾

Sec Agree Feature

☐ enable

Enforcement Profile

▾

Emergency Dscp Profile

▾

TCP Keepalive

none ▾

Add SDP Invite

both ▾

Add SDP In Msg

P Early Media Header

disabled ▾

P Early Media Direction

Figure 68: SIP Interface for PSTN Gateway (Cont.)

Configuration

View Configuration

Q

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

Modify SIP Interface

Add SDP Profiles

Add SDP Profiles In Msg

SIP Profile

▾

SIP Isup Profile

▾

TCP Conn Dereg

0 (Range: 0..999999999)

Kpml Interworking

☐ enable

Kpml2833 lwf On Hairpin

☐ enable

Msrp Delay Egress Bye

☐ enable

Send 380 Response

Pscf Restoration

Session Timer Profile

▾

Session Recording Server

Session Recording Required

☐ enable

Figure 69: SIP Interface for PSTN Gateway (Cont.)

Configuration

View Configuration

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

system

Modify SIP Interface

Session Recording Required

enable

Service Tag

Reg Cache Route

enable

Diversion Info Mapping Mode

none

Atcf Icsi Match

SIP Recursion Policy

Asymmetric Preconditions

enable

Asymmetric Preconditions Mode

send-with-nodelay

Sm Icsi Match For Invite

Sm Icsi Match For Message

S8hr Profile

Ringback Trigger

none

Ringback File

Fax Continue Session

none

Figure 70: SIP Interface for PSTN Gateway (Cont.)

Configuration

View Configuration

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

system

Modify SIP Interface

SIP Recursion Policy

Asymmetric Preconditions

enable

Asymmetric Preconditions Mode

send-with-nodelay

Sm Icsi Match For Invite

Sm Icsi Match For Message

S8hr Profile

Ringback Trigger

none

Ringback File

Fax Continue Session

none

Npl Profile

Hist To Div For Cause 380

inherit

User Agent

Allow Diff2833 Clock Rate Mode

disabled

Figure 71: SIP Interface for PSTN Gateway (Cont.)

- Create SIP interface towards Google CES by adding SIP Ports as shown below.

Configuration View Configuration

Modify SIP Interface Show Advanced

State ☒ enable

Realm ID Google

Description GOOGLE

SIP Ports

Select	Action	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
☐		192.65	5061	TLS	GoogleCCAI	agents-only	

Configuration View Configuration

media-manager >

security >

session-router v

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

session-translation

sip-config

sip-feature

sip-interface

Modify SIP Interface

Initial Inv Trans Expire 0 (Range: 0..2147473)

Session Max Life Limit 0

Proxy Mode

Redirect Action

Nat Traversal none

Nat Interval 30 (Range: 1.999999999)

TCP Nat Interval 90 (Range: 0.999999999)

Registration Caching ☐ enable

Min Reg Expire 300 (Range: 0.999999999)

Registration Interval 3600 (Range: 1.999999999)

Route To Registrar ☐ enable

Secured Network ☐ enable

Uri Fqdn Domain

Options

Figure 72: SIP Interface for Google CES

Configuration View Configuration

Modify SIP Interface

Initial Inv Trans Expire 0 (Range: 0..2147473)

Session Max Life Limit 0

Proxy Mode

Redirect Action

Nat Traversal none

Nat Interval 30 (Range: 1.999999999)

TCP Nat Interval 90 (Range: 0.999999999)

Registration Caching ☐ enable

Min Reg Expire 300 (Range: 0.999999999)

Registration Interval 3600 (Range: 1.999999999)

Route To Registrar ☐ enable

Secured Network ☐ enable

Uri Fqdn Domain

Options

Configuration View Configuration

media-manager >

security >

session-router v

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

session-translation

sip-config

sip-feature

sip-interface

Modify SIP Interface

Initial Inv Trans Expire 0 (Range: 0..2147473)

Session Max Life Limit 0

Proxy Mode

Redirect Action

Nat Traversal none

Nat Interval 30 (Range: 1.999999999)

TCP Nat Interval 90 (Range: 0.999999999)

Registration Caching ☐ enable

Min Reg Expire 300 (Range: 0.999999999)

Registration Interval 3600 (Range: 1.999999999)

Route To Registrar ☐ enable

Secured Network ☐ enable

Uri Fqdn Domain

Options

Figure 73: SIP Interface for Google CES (Cont.)

Configuration

View Configuration

Q

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

Modify SIP Interface

Trust Mode

all

Max Nat Interval

3600

(Range: 0.999999999)

Nat Int Increment

10

(Range: 0.999999999)

Nat Test Increment

30

(Range: 0.999999999)

SIP Dynamic Hnt

☐ enable

TCP Max Nat Interval

3600

(Range: 0.999999999)

TCP Nat Int Increment

10

(Range: 0.999999999)

TCP Nat Test Increment

30

(Range: 0.999999999)

TCP SIP Dynamic Hnt

☐ enable

Stop Recurse

401,407

Port Map Start

0

(Range: 0,025..65535)

Port Map End

0

(Range: 0,025..65535)

In Manipulationid

Out Manipulationid

SIP Atcf Feature

☐ enable

Rfc2833 Payload

101

(Range: 96..127)

Figure 74: SIP Interface for Google CES (Cont.)

Configuration

View Configuration

Q

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

Modify SIP Interface

Rfc2833 Mode

transparent

Response Map

Local Response Map

Sec Agree Feature

☐ enable

Enforcement Profile

Emergency Dscp Profile

TCP Keepalive

enabled

Add SDP Invite

disabled

Add SDP In Msg

P Early Media Header

disabled

P Early Media Direction

Add SDP Profiles

Add SDP Profiles In Msg

Figure 75: SIP Interface for Google CES (Cont.)

Configuration View Configuration  

- 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
- session-translation
- sip-config
- sip-feature
- sip-interface**
- sip-manipulation
- sip-monitoring
- translation-rules

Modify SIP Interface

TCP Conn Dereg	0 (Range: 0.999999999)
Kpml Interworking	☐ enable
Kpml2833 lwf On Hairpin	☐ enable
Msrp Delay Egress Bye	☐ enable
Send 380 Response	
Pcscf Restoration	
Session Timer Profile	SessionTimer ▾
Session Recording Server	
Session Recording Required	☐ enable
Service Tag	
Reg Cache Route	☐ enable
Diversion Info Mapping Mode	none ▾
Atcf Icsi Match	
SIP Recursion Policy	▾
Asymmetric Preconditions	☐ enable
Asymmetric Preconditions Mode	send-with-nodelay ▾

Figure 76: SIP Interface for Google CES (Cont.)

Configuration View Configuration  

- tls-profile
- 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
- session-translation
- sip-config
- sip-feature
- sip-interface**
- sip-manipulation
- sip-monitoring
- translation-rules

Modify SIP Interface

Reg Cache Route	☐ enable
Diversion Info Mapping Mode	none ▾
Atcf Icsi Match	
SIP Recursion Policy	▾
Asymmetric Preconditions	☐ enable
Asymmetric Preconditions Mode	send-with-nodelay ▾
Sm Icsi Match For Invite	
Sm Icsi Match For Message	
S8hr Profile	▾
Ringback Trigger	none ▾
Ringback File	
Fax Continue Session	none ▾
Npli Profile	▾
Hist To Div For Cause 380	inherit ▾
User Agent	
Allow Diff2833 Clock Rate Mode	disabled ▾

Figure 77: SIP Interface for Google CES (Cont.)

7.4.19 Session Agent

- Session-agents are config elements which are trusted agents which can send/receive traffic from the Oracle E-SBC with direct access to trusted data path.
- Navigate to **Configuration** → **session-router** → **session-agent**.
- Configure Session Agent for PSTN Gateway Google CES.

Configure the Session Agent for Google CES as shown below.

Select	Action	Hostname	IP Address	Port	State	App Protocol	Realm ID	Description
☐		172.16...	172.16...	5060	enabled	SIP	PSTN	IP peer to PSTN GW
☐		us.telephony.goog		5672	enabled	SIP	Google	

Figure 78: Session Agent

Modify Session Agent

Hostname: us.telephony.goog

IP Address:

Port: 5672 (Range: 0,1025..65535)

State: ☒ enable

App Protocol: SIP

App Type:

Transport Method: StaticTLS

Realm ID: Google

Egress Realm ID:

Description:

Figure 79: Session Agent for Google CES

Configuration

View Configuration

Q

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

Modify Session Agent

Associated Agents

☐ enable

Max Sessions

0

(Range: 0.999999999)

Max Inbound Sessions

0

(Range: 0.999999999)

Max Outbound Sessions

0

(Range: 0.999999999)

Max Burst Rate

0

(Range: 0.999999999)

Max Inbound Burst Rate

0

(Range: 0.999999999)

Max Outbound Burst Rate

0

(Range: 0.999999999)

Max Sustain Rate

0

(Range: 0.999999999)

Max Inbound Sustain Rate

0

(Range: 0.999999999)

Max Outbound Sustain Rate

0

(Range: 0.999999999)

Min Asr

0

(Range: 0.100)

Cac Trap Threshold

0

(Range: 0.99)

Session Max Life Limit

0

Time To Resume

0

(Range: 0.999999999)

Figure 80: Session Agent for Google CES (Cont.)

Configuration

View Configuration

Q

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

Modify Session Agent

In Service Period

0

(Range: 0.999999999)

Burst Rate Window

0

(Range: 0.999999999)

Sustain Rate Window

0

(Range: 0.999999999)

Max Inbound Per Session Burst Rate

30

(Range: 1.999999999)

Burst Rate Window Per Session

1

(Range: 1.999999999)

Dos Action At Session

inherit

Proxy Mode

Redirect Action

Loose Routing

☒ enable

Response Map

Ping Method

OPTIONS

Ping Interval

60

(Range: 0.999999999)

Ping Send Mode

keep-alive

Ping All Addresses

☐ enable

Ping In Service Response Codes

Load Balance DNS Query

hunt

Figure 81: Session Agent for Google CES (Cont.)

Configuration

View Configuration

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

Modify Session Agent

Options

SPL Options

Media Profiles

In Session Translations

No in session translation list to display. Please add.

Add

Out Session Translations

Select	Action	Out Session Translation Id	State
☐	:	addplus1	enabled

Figure 82: Session Agent for Google CES (Cont.)

Configuration

View Configuration

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

Modify Session Agent

☐ enable

Trust Me

Stop Recurse

Local Response Map

Ping Response

☒ enable

In ManipulationId

Out ManipulationId

Manipulation String

Manipulation Pattern

Trunk Group

Max Register Sustain Rate

0

(Range: 0.9999999999)

Invalidate Registrations

☐ enable

Rfc2833 Mode

none

Rfc2833 Payload

0

(Range: 0.96..127)

Codec Policy

Emergency Dscp Profile

Refer Call Transfer

disabled

Figure 83: Session Agent for Google CES (Cont.)

Configuration

View Configuration

Q

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

Modify Session Agent

Refer Notify Provisional

none ▾

Reuse Connections

NONE ▾

TCP Keepalive

enabled ▾

TCP Reconn Interval

60

(Range: 0,2..300)

Max Register Burst Rate

0

(Range: 0.999999999)

Rate Constraints

No rate constraints to display. Please add.

Add

SIP Profile

▾

SIP Isup Profile

▾

Kpml Interworking

inherit ▾

Kpml2853 Iwf On Hairpin

inherit ▾

Precedence

0

(Range: 0.4294967295)

Monitoring Filters

Figure 84: Session Agent for Google CES (Cont.)

Configuration

View Configuration

Q

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

system >

Modify Session Agent

Auth Attribute

No auth attributes to display. Please add.

Add

Session Recording Server

Session Recording Required

☐ enable

Hold Refer Reinvite

☐ enable

Send TCP Fin

☐ enable

SIP Recursion Policy

▾

Sm Icsi Match For Invite

Sm Icsi Match For Message

Ringback Trigger

none ▾

Ringback File

Fax Servers

Trigger Oos Alarm

☐ enable

Static TCP Source Port

0

(Range: 0,025..65535)

Figure 85: Session Agent for Google CES (Cont.)

- Configure the Session agent for PSTN Gateway as shown below.

Configuration View Configuration

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

Modify Session Agent

Hostname: 172.16.

IP Address: 172.16.

Port: 5060 (Range: 0,3025..65535)

State: ☒ enable

Transport Method: StaticTCP

Realm ID: PSTN

Egress Realm ID:

Description: IP peer to PSTN GW

Ping Method: OPTIONS

Ping Interval: 30 (Range: 0.999999999)

Load Balance DNS Query: hunt

SPL Options:

Media Profiles:

Figure 86: Session Agent for PSTN Gateway

Configuration View Configuration

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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

Modify Session Agent

Associated Agents:

Constraints: ☐ enable

Max Sessions: 0 (Range: 0.999999999)

Max Inbound Sessions: 0 (Range: 0.999999999)

Max Outbound Sessions: 0 (Range: 0.999999999)

Max Burst Rate: 0 (Range: 0.999999999)

Max Inbound Burst Rate: 0 (Range: 0.999999999)

Max Outbound Burst Rate: 0 (Range: 0.999999999)

Max Sustain Rate: 0 (Range: 0.999999999)

Max Inbound Sustain Rate: 0 (Range: 0.999999999)

Max Outbound Sustain Rate: 0 (Range: 0.999999999)

Min Asr: 0 (Range: 0.300)

Cac Trap Threshold: 0 (Range: 0.99)

Session Max Life Limit: 0

Time To Resume: 0 (Range: 0.999999999)

Figure 87: Session Agent for PSTN Gateway (Cont.)

Configuration View Configuration  

- 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
 - session-translation
 - sip-config
 - sip-feature
 - sip-interface
 - sip-manipulation
 - sip-monitoring
 - translation-rules

Modify Session Agent

Trust Me	☐ enable
Stop Recurse	
Local Response Map	
Ping Response	☒ enable
In Manipulationid	
Out Manipulationid	
Manipulation String	
Manipulation Pattern	
Trunk Group	
Max Register Sustain Rate	0 (Range: 0.999999999)
Invalidate Registrations	☐ enable
Rfc2833 Mode	none
Rfc2833 Payload	0 (Range: 0,96.127)
Codec Policy	
Emergency Dscp Profile	
Refer Call Transfer	disabled

Figure 88: Session Agent for PSTN Gateway (Cont.)

Configuration View Configuration  

- 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
 - session-translation
 - sip-config
 - sip-feature
 - sip-interface
 - sip-manipulation

Modify Session Agent

Reuse Connections	NONE
TCP Keepalive	disabled
TCP Reconn Interval	0 (Range: 0,2..300)
Max Register Burst Rate	0 (Range: 0.999999999)
Rate Constraints No rate constraints to display. Please add. Add	
SIP Profile	
SIP Isup Profile	
Kpml Interworking	inherit
Kpml2833 lwf On Hairpin	inherit
Precedence	0 (Range: 0.4294967295)
Monitoring Filters	
Auth Attribute	

Figure 89: Session Agent for PSTN Gateway (Cont.)

Configuration View Configuration

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
 session-translation
 sip-config
 sip-feature
 sip-interface
 sip-manipulation
 sip-monitoring
 translation-rules
 system >

Modify Session Agent

Auth Attribute
 No auth attributes to display. Please add.
 Add

Session Recording Server

Session Recording Required ☐ enable

Hold Refer Reinvite ☐ enable

Send TCP Fin ☐ enable

SIP Recursion Policy

Sm Icsi Match For Invite

Sm Icsi Match For Message

Ringback Trigger none

Ringback File

Fax Servers

Trigger Oos Alarm ☐ enable

Static TCP Source Port 0 (Range: 0,1025..65535)

Figure 90: Session Agent for PSTN Gateway (Cont.)

7.4.20 Local Policy

- Local policy config allows for the Oracle E-SBC to route calls from one end of the network to the other based on routing criteria.
- Navigate to **Configuration** → **session-router** → **local-policy**.
- Configure local policy for Google CES and PSTN Gateway as shown below.

Configuration View Configuration

access-control
 account-config
 filter-config
 ldap-config
local-policy
 local-routing-config
 media-profile
 session-agent

Local Policy

Delete all Local Policy Items

Select	Action	From Address	To Address	Source Realm	Description	Activate Time	Deactivate Time	State
☐	:	*	*	Google	Google to PSTN			enabled
☐	:	*	*	PSTN	PSTN To Google			enabled

Figure 91: Local Policy

- Below Local Policy is used to route calls from PSTN Gateway to Google CES.

Configuration View Configuration

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

Modify Local Policy Entries Show Advanced

From Address * x
To Address * x
Source Realm PSTN x
Description GOOGLE TO PSTN
Policy Priority none

Policy Attributes

Select	Action	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
☐	:	us.telephony.goog	Google	none	disabled	0	enabled	SIP	single	

Figure 92: Local Policy routing from PSTN Gateway to Google CES

Configuration View Configuration

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

Modify Local policy / policy attribute

Next Hop us.telephony.goog
Realm Google
Action none
Terminate Recursion ☐ enable
Cost 0 (Range: 0..999999999)
State ☒ enable
App Protocol SIP
Lookup single
Next Key
Auth User Lookup

Figure 93: Local Policy routing from PSTN Gateway to Google CES (Cont.)

- Below Local Policy is used to route calls from Google CES towards PSTN Gateway

configuration View Configuration

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
session-translation
slp-config

Modify Local Policy Entries

From Address * x
To Address * x
Source Realm Google x

Description
Google to PSTN

State ☒ enable
Parallel Forking ☐ enable
Policy Priority none

Policy Attributes

Select	Action	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
☐		172.16.	PSTN	none	disabled	0	enabled	SIP	single	

Figure 94: Local Policy routing from Google CES to PSTN Gateway

Configuration View Configuration

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

Modify Local policy / policy attribute

Next Hop 172.16.
Realm PSTN

Action none

Terminate Recursion ☐ enable

Cost 0 (Range: 0.999999999)

State ☒ enable

App Protocol SIP

Lookup single

Next Key

Auth User Lookup

Figure 95: Local Policy routing from Google CES to PSTN Gateway

7.4.21 SIP Manipulation

- Navigate to **Configuration** → **session-router** → **sip-manipulation**.
- Configure SIP manipulation towards Google CES as shown below.

Configuration View Configuration

Modify SIP Manipulation

Name: GoogleManipulation

Description: Manipulation on google side

Split Headers:

Join Headers:

CfgRules

Action	Name	Element Type
⋮	changeRequiri	header-rule
⋮	changeTo	header-rule
⋮	AddCallInfoHeader	header-rule
⋮	changelocalport	header-rule
⋮	deltransport	header-rule
⋮	delete_callInfo	header-rule

Figure 96: SIP Manipulation towards Google CES

- Adds a header-rule for Google CES.

Configuration View Configuration

Modify SIP Manipulation

Name: GoogleManipulation

Description: Manipulation on google side

Split Headers:

Join Headers:

CfgRules

Add

header-rule

Action	Name	Element Type
⋮	changeRequiri	header-rule
⋮	changeTo	header-rule
⋮	AddCallInfoHeader	header-rule
⋮	changelocalport	header-rule
⋮	deltransport	header-rule
⋮	delete_callInfo	header-rule

Figure 97: Header rule addition for SIP Manipulation towards Google CES

- Below header rule is created to change Request-URI host and user parts towards Google CES to us.telephony.goog:5672 and +1314944XXXX.

Configuration View Configuration

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
session-translation
sip-config

Modify Sip manipulation / header rule

Name: changeRequiri
Header Name: Request-URI
Action: manipulate
Comparison Type: pattern-rule
Msg Type: any
Methods: INVITE x OPTIONS x
Match Value:
New Value:

CfgRules

Action	Name	Element Type
:	ReqURI	element-rule
:	AddURI	element-rule

Figure 98: SIP Manipulation towards Google CES Request URI

Configuration View Configuration

media-manager >
security >
session-router ▾
access-control
account-config
filter-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group

Modify Sip manipulation / header rule / element rule

Name: ReqURI
Parameter Name:
Type: uri-host
Action: replace
Match Val Type: any
Comparison Type: case-insensitive
Match Value:
New Value: "us.telephony.goog:5672"

Figure 99: SIP Manipulation towards Google CES change Request URI-host

Configuration View Configuration

Modify Sip manipulation / header rule / element rule

Name: AddURI

Parameter Name: Request-URI

Type: uri-user

Action: replace

Match Val Type: any

Comparison Type: pattern-rule

Match Value:

New Value: "+13149"

Configuration menu: account-config, filter-config, ldap-config, local-policy, 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

Figure 100: SIP Manipulation towards Google CES change Request URI-user

- Below header rule is created to change TO header host part towards Google CES to IP address of Google CES and user part with Google CES DID.

Configuration View Configuration

Modify Sip manipulation / header rule

Name: changeToURIhost

Header Name: To

Action: manipulate

Comparison Type: pattern-rule

Msg Type: any

Methods: INVITE x OPTIONS x

Match Value:

New Value:

CfgRules

Action	Name	Element Type
⋮	changeURIhost	element-rule
⋮	changetouser	element-rule

Configuration menu: filter-config, ldap-config, local-policy, **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

Figure 101: SIP Manipulation towards Google CES TO header

Configuration View Configuration

filter-config
ldap-config
local-policy
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

Modify Sip manipulation / header rule / element rule

Name: changeTohost

Parameter Name:

Type: uri-host

Action: replace

Match Val Type: any

Comparison Type: pattern-rule

Match Value:

New Value: "us.telephony.goog"

Figure 102: SIP Manipulation towards Google CES – Change TO header Host

Configuration View Configuration

account-config
filter-config
ldap-config
local-policy
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

Modify Sip manipulation / header rule / element rule

Name: changeToUser

Parameter Name: To

Type: uri-user

Action: replace

Match Val Type: any

Comparison Type: case-sensitive

Match Value:

New Value: "+131494"

Figure 103: SIP Manipulation towards Google CES – Change TO header User

- Below header rule is created to add Call-Info header towards Google CES with the Dialog Flow API request along with the Conversation ID.
- Conversation on the Fly is set to True in Google CES using REST API. Conversation ID is randomly generated by Oracle E-SBC for each call.
- New Value is set to "<http://dialogflow.googleapis.com/v2beta1/projects/ccai-3898XX/conversations/OR_"+"\$CALL_ID.\$0+";purpose=Goog-ContactCenter-Conversation"

The screenshot shows the 'Configuration' page with the 'session-router' configuration selected. The 'sip-manipulation' section is highlighted. The 'Modify Sip manipulation / header rule' form is shown with the following fields:

- Name: AddCallInfoHeader
- 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/projec"

Figure 104: SIP Manipulation towards Google CES – Add Call-Info

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

The screenshot shows the 'Configuration' page with the 'session-router' configuration selected. The 'sip-manipulation' section is highlighted. The 'Modify Sip manipulation / header rule' form is shown with the following fields:

- Name: delete_callinfo
- Header Name: Call-info
- Action: find-replace-all
- Comparison Type: pattern-rule
- Msg Type: any
- Methods: INVITE x
- Match Value: ^(<http://.*)(@us.telephony.goog)(.*)\$
- New Value: \$1+\$3

Figure 105: SIP Manipulation towards Google CES – Delete Call-Info host IP address

- Below header rule is created to change the port number in the Request URI towards Google CES.

Configuration View Configuration

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
session-translation

Modify Sip manipulation / header rule

Name: changelocalport
Header Name: Request-URI
Action: manipulate ▾
Comparison Type: case-sensitive ▾
Msg Type: any ▾

Methods:
Match Value:
New Value:

CfgRules

Action	Name	Element Type
.	chnagetransportnumber	element-rule

Figure 106: SIP Manipulation towards Google CES – Change Request URI Port number

Configuration View Configuration

media-manager >
security >
session-router ▾
access-control
account-config
filter-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group

Modify Sip manipulation / header rule / element rule

Name: chnagetransportnumber
Parameter Name:

Type: uri-port ▾
Action: replace ▾
Match Val Type: any ▾
Comparison Type: case-sensitive ▾
Match Value:
New Value: \$REMOTE_PORT

Figure 107: SIP Manipulation towards Google CES – Change Request URI Port number (Cont.)

- Below header rule is created to delete the transport parameter in the Request URI towards Google CES.

The screenshot shows the 'Configuration' tab in a web interface. On the left sidebar, 'session-router' is selected under the 'sip-manipulation' category. The main area is titled 'Modify Sip manipulation / header rule'. A red box highlights the configuration fields for a header rule:

- Name: deltransport
- Header Name: Request-URI
- Action: manipulate
- Comparison Type: case-sensitive
- Msg Type: any
- Methods: INVITE x
- Match Value: (empty)
- New Value: (empty)

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

Action	Name	Element Type
:	delparam	element-rule

Figure 108: SIP Manipulation towards Google CES – Delete Transport

The screenshot shows the 'Configuration' tab in a web interface. On the left sidebar, 'sip-manipulation' is selected. The main area is titled 'Modify Sip manipulation / header rule / element rule'. A red box highlights the configuration fields for an element rule:

- Name: delparam
- Parameter Name: transport
- Type: uri-param
- Action: delete-element
- Match Val Type: any
- Comparison Type: case-sensitive
- Match Value: (empty)
- New Value: (empty)

Figure 109: SIP Manipulation towards Google CES – Delete Transport parameter (Cont.)

Manipulation for Inbound messages from Google CES

Below is the manipulation to modify Request-URI, To and REFER-To headers during call hand-off to an agent.

Action	Name	Element Type
⋮	changereqURI	header-rule
⋮	changeTo	header-rule
⋮	ReferTo	header-rule

Figure 110: SIP Manipulation towards PSTN Gateway

- Creates a Request URI sip header manipulation.

Action	Name	Element Type
⋮	Changerequiuser	element-rule

Figure 111: SIP Manipulation towards PSTN Gateway – Request URI

Configuration View Configuration

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
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation

Modify Sip manipulation / header rule / element rule

Name: Changerequiruser

Parameter Name: Request-URI

Type: uri-user

Action: replace

Match Val Type: any

Comparison Type: pattern-rule

Match Value:

New Value: "972852"

Figure 112: SIP Manipulation towards PSTN Gateway – Request URI User

- Creates a To sip header manipulation.

Configuration View Configuration

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
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation

Modify Sip manipulation / header rule

Name: changeTo

Header Name: To

Action: manipulate

Comparison Type: pattern-rule

Msg Type: any

Methods: INVITE x REFER x

Match Value:

New Value:

CfgRules

Action	Name	Element Type
⋮	changetouser	element-rule

Figure 113: SIP Manipulation towards PSTN Gateway – To Header

Configuration View Configuration

Modify Sip manipulation / header rule / element rule

Name: changetouser

Parameter Name: changetouser

Type: uri-user

Action: replace

Match Val Type: any

Comparison Type: pattern-rule

Match Value:

New Value: "972852"

Configuration menu: sip-manipulation

Figure 114: SIP Manipulation towards PSTN Gateway – To Header User

- Creates a Refer-To sip header manipulation

Configuration View Configuration

Modify Sip manipulation / header rule

Name: Referto

Header Name: Refer-To

Action: manipulate

Comparison Type: pattern-rule

Msg Type: any

Methods: REFER x

Match Value:

New Value:

CfgRules

Action	Name	Element Type
:	changereferetouser	element-rule

Configuration menu: session-router, sip-manipulation

Figure 115: SIP Manipulation towards PSTN Gateway – Refer-To Header

Configuration

View Configuration

account-coming

filter-config

ldap-config

local-policy

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

Modify Sip manipulation / header rule / element rule

Name

changereferertouser

Parameter Name

changereferertouser

Type

uri-user

Action

replace

Match Val Type

any

Comparison Type

pattern-rule

Match Value

New Value

"972852;"

Figure 116: SIP Manipulation towards PSTN Gateway – Refer-To Header User

Manipulations for Outbound messages to Google CES via UII header

- This SIP manipulation to insert a Hexa encoded User-to-User header required by Google CES to exchange session-related info to connect with Google CES Agent-Handoff.
- **The URL :** http://dialogflow.googleapis.com/v2beta1/projects/ccai-3898XX/conversations/OR_QAZ
- **Hexa Encoded:** 6XXXXXXXXXXXX;encoding=hex;Goog-ContactCenter-Conversation"

Configuration View Configuration

Modify Sip manipulation / header rule

Name	AddUUHeader
Header Name	User-to-User
Action	add
Comparison Type	case-sensitive
Msg Type	any
Methods	INVITE x
Match Value	
New Value	"68; 61

CfgRules

No rules to display. Please add.

Add

Figure 117: SIP Manipulation towards Google CES – UII Header

8 SIP INVITE To Google CES

8.1 SIP INVITE for SIPREC call

```
INVITE sip:+136188...@us.telephony.goog:5672 SIP/2.0
Via: SIP/2.0/TLS 192.65.100.100:5061;branch=z9hG4bKqtf9nq103ov0tbubt2n0
From: <sip:acmeSrc@192.65.100.100>;tag=fc4e824a0f617ddcbf1e98c90f7ead51
To: <sip:+136188...@us.telephony.goog:5672>;transport=tcp>
Call-ID: 44dd70a5480470e9f5932cb3f578484d020@us.telephony.goog
CSeq: 1080 INVITE
Contact: <sip:acmeSrc@192.65.100.100:5061;transport=tcp>;+sip.src
Max-Forwards: 70
Require: siprec
Content-Type: multipart/mixed; boundary=unique-boundary-1
Content-Length: 2237
MIME-Version: 1.0
Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/ccai-38.../conversations/OR_44d...>;purpose=Goog-ContactCenter-Conversation

--unique-boundary-1
Content-Type: application/sdp

v=0
o=- 3562256 226213 IN IP4 192.65.100.100
s=-
c=IN IP4 192.65.100.100
t=0 0
m=audio 20910 RTP/SAVP 0 101
c=IN IP4 192.65.100.100
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=label:234881075
a=sendonly
a=crypto:1 AES CM 128 HMAC SHA1_80 inline:1ZbR91HLKuYJ8T4ejRWE1rWkdq4Zket0XmrTM8Jk
m=audio 20914 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=maxptime:150
a=label:234881076
a=sendonly
a=crypto:1 AES CM 128 HMAC SHA1_80 inline:aUvfqWeUmqFDSQC65SVEu4muW9bdvNcMuqpaId
```

The INVITE Request-URI should include e.164 number obtained from Google and it should have respective regional host name with SIP Signaling port :5672

Google requires the Call-Info header, and it must contain a conversation ID. The conversation ID is unique, and the format of the conversation ID follows the regex "[a-zA-Z][a-zA-Z0-9_-]*" and is assigned for each call.

dialogflow.googleapis.com/v2beta1 - API endpoint
projects/ccai-3898XX - Google Cloud CCAI project ID
conversations/OR_xxxx - The unique conversation session ID that is assigned for that each call

The connection IP toward Google CCAI must be a public IP, not a private one.

For SIPREC, there can be multiple media lines with *a=sendonly*, for SIP there will be a single media line with *a=sendrecv*. Encrypted SRTP and the allocated port range should be used (Port: 16384-32767) else CES will not receive audio.

It must be a supported crypto suite by Google.

Figure 118: SIPREC Call

8.2 SIP INVITE for GTP call

```
INVITE sip:+13149...@us.telephony.goog:5672 SIP/2.0
Via: SIP/2.0/TLS 192.65.100.100:5061;branch=z9hG4bK1B6trn0000e10aih
From: <sip:+19728522631@192.65.100.100>;tag=d6de37c9-7561-4937-a8b9-0ca72644801a
To: <sip:+13149...@us.telephony.goog>
Contact: <sip:9728522631@192.65.100.100:5061;transport=tls>
Call-ID: 02e58ba8-b22e-41a5-aa3d-d3e88a671c0c
CSeq: 21261 INVITE
Allow: OPTIONS, INVITE, ACK, BYE, CANCEL, UPDATE, PRACK, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, REFER
Supported: 100rel, timer, replaces, norefersub, histinfo
Session-Expires: 1800; refresher=uac
Min-SE: 90
Max-Forwards: 69
User-Agent: FPBX-16.0.40.13(20.4.0)
Content-Type: application/sdp
Content-Length: 405
Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/ccai-389.../conversations/OR_02e...>;purpose=Goog-ContactCenter-Conversation

v=0
o=- 1738828058 1738828058 IN IP4 192.65.100.100
s=Asterisk
c=IN IP4 192.65.100.100
t=0 0
m=audio 21204 RTP/SAVP 0 8 101 107
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=rtpmap:107 opus/48000/2
a=fmtp:107 useinbandfec=1
a=ptime:20
a=sendrecv
a=crypto:1 AES CM 128 HMAC SHA1_80 inline:ydaFiGf4WVGacrEmG0HNx9d1V8cWoG0fdwG0x0PS
```

The INVITE Request-URI should include e.164 number obtained from Google and it should have respective regional host name with SIP Signaling port :5672

Google requires the Call-Info header, and it must contain a conversation ID. The conversation ID is unique, and the format of the conversation ID follows the regex "[a-zA-Z][a-zA-Z0-9_-]*" and is assigned for each call.

dialogflow.googleapis.com/v2beta1 - API endpoint
projects/ccai-389811 - Google Cloud CCAI project ID
conversations/OR_xxxx - The unique conversation session ID that is assigned for that each

The connection IP toward Google CCAI must be a public IP, not a private one.

For GTP, there can be single media lines with *a=sendrecv*, for SIPREC there will be a multiple media line with *a=sendonly*. Encrypted SRTP and the allocated port range should be used (Port: 16384-32767) else CES will not receive audio.

It must be a supported crypto suite by Google.

Figure 119: GTP Call

9 Oracle E-SBC Running configuration file

Attached is the Oracle E-SBC running configuration file.



Google_SIPREC_Running Config

10 Summary of Tests and Results

ID	Title	Description	Expected Results	Status (Passed or Failed etc.)	Observations
35	UUI header test	Use the UUI header as opposed to call-info header to send conversation id	Call should process as normal, and recording under conversation ID derived from UUI header as opposed to call-info	PASSED	Calls get successfully connected to Live agent when using UUI header instead of call-info header.
36	Keep_conversation_running=TRUE test	ConversationProfile needs to have SipConfig set with keepConversationRunning = TRUE. Send first call with a Call-Info header and have a call for 2 turns. End the call. Send second call with the SAME Call-Info header as above and have a call for 3 turns. End the call.	Two calls having the same call-info has both conversation details.	PASSED	Both call transcripts are present for the same conversation session id.
37	Live Agent Transfer	Call goes to virtual agent, initial live agent handoff and verify outgoing SIP INVITE, call connection and disconnection		PASSED	Call gets connected successfully to BOT and INVITE sent successfully to connect with Agent.
38	Live Agent Transfer	Call goes to virtual agent, initial live agent handoff and verify outgoing SIP INVITE, call connection and disconnection. Make calls to +1314944XXXX, "speak to an agent", +1-972-852-XXXX should then ring and get connected as the agent		PASSED	Call was connected successfully with live agent and when performing conversation "Speak to an agent", a new INVITE was sent from Google to transfer to an agent and call gets connected successfully with both-way audio.

ID	Title	Description	Expected Results	Status (Passed or Failed etc.)	Observations
39	UUI headers	Call goes to virtual agent, say "end the call", validate that the SIP BYE has a UUI header Make calls to +1314944XXXX, "end the call", check SIP BYE and ensure there is one or more (identify if there are 3 or 1) UUI headers with purpose Goog-Session-Param		PASSED	Calls get connected successfully to live agents and when performing conversation "End the call", the call gets disconnected normally with 3 UUI header.
40	SIP REFER	Call goes to virtual agent, say "send a sip refer", validate that a SIP REFER is received to 972-852-XXXX. Make calls to +1314944XXXX, "send a sip refer", SIP REFER should be received with refer to set to 972-852-XXXX		PASSED	REFER request and transfer are successful.