

Configuration Guide for Google
CES Call Recording Using
Oracle E-SBC Acme Packet
4600 SCZ 9.3.0 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	Features tested for Google CES Call Recording	6
6.2	Features Not tested for Google CES Call Recording	6
6.3	Caveats and Limitations	6
6.4	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	12
7.4.3	Network Interface	13
7.4.4	SIP Config	17
7.4.5	System-Config	19
7.4.6	SIP Monitoring	21
7.4.7	HTTP Server	22
7.4.8	Codec Policy	22
7.4.9	Translation Rules	23
7.4.10	Session Translation	24
7.4.11	Session Recording Server	25
7.4.12	Realm Config	25
7.4.13	Steering Pool	31
7.4.14	SDES Profile	32
7.4.15	Media Sec Policy	33
7.4.16	TLS – Certificate Record	34
7.4.17	TLS – TLS Profile	37

7.4.18	Session Timer	38
7.4.19	SIP Interface	38
7.4.20	Session Agent	43
7.4.21	Local Policy	50
7.4.22	SIP Manipulation	52
8	SIP INVITE To Google CES	62
8.1	SIP INVITE for SIPREC call	62
8.2	SIP INVITE for GTP call	62
9	Oracle E-SBC Running configuration	63
10	Summary of Tests and Results	64

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 Call Recording** 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 Call Recording with Oracle Enterprise Session Border Controller (E-SBC) Acme Packet 4600 SCZ9.3.0 GA(Build46) configuration.

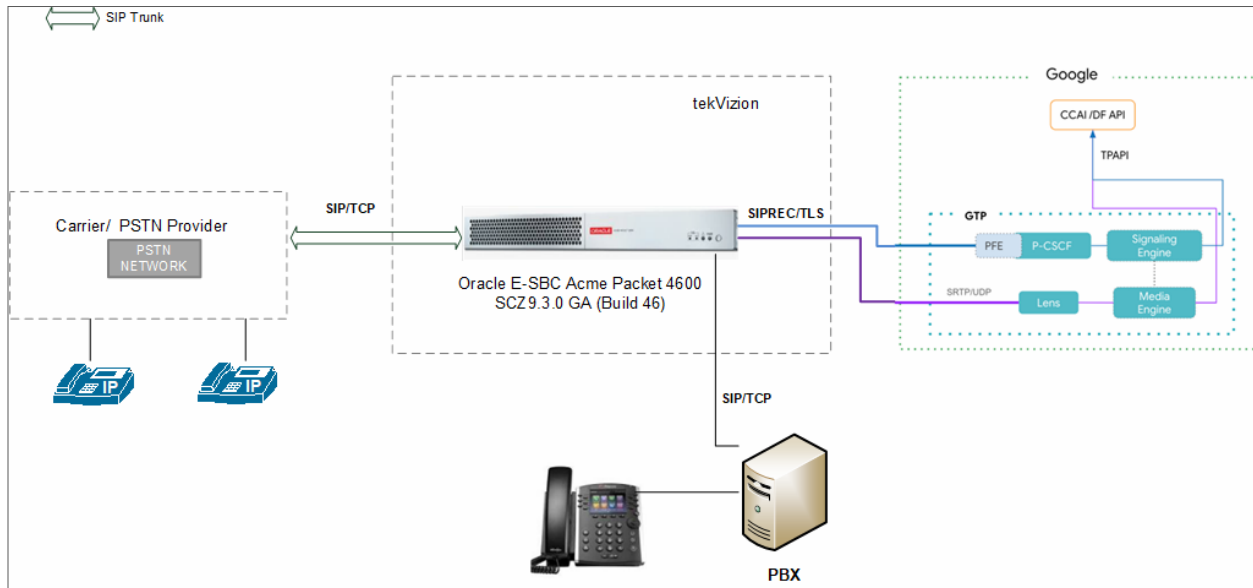


Figure 1: SIP Trunk Lab Reference Network.

The lab network consists of the following components.

- Google CES cloud Environment
- Oracle E-SBC Acme Packet 4600
- OnPrem PBX

3 Hardware Components

- Oracle E-SBC Acme Packet 4600

4 Software Requirements

- Oracle E-SBC Acme Packet 4600 SCZ 9.3.0 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	SCZ 9.3.0 GA (Build46)
Oracle E-SBC 3900	SCZ 9.3.0 GA (Build46)
Oracle E-SBC 3900	SCZ 8.4.0 Patch 2 (Build 151)

6 Features

6.1 Features tested for Google CES Call Recording

- Basic Inbound calls
- Call Hold and Resume
- Call Transfer
- Conference

6.2 Features Not tested for Google CES Call Recording

- None

6.3 Caveats and Limitations

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

6.4 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	Session Recording Server	Section 7.4.11
Step 12	Realm Config	Section 7.4.12
Step 13	Steering Pool	Section 7.4.13
Step 14	SDES Profile	Section 7.4.14
Step 15	Media Sec Policy	Section 7.4.15
Step 16	TLS – Certificate Record	Section 7.4.16
Step 17	TLS – TLS Profile	Section 7.4.17
Step 18	Session Timer	Section 7.4.18
Step 19	SIP Interface	Section 7.4.19
Step 20	Session Agent	Section 7.4.20
Step 21	Local Policy	Section 7.4.21
Step 22	SIP Manipulation	Section 7.4.22

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
OnPrem PBX	
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 to configure Google CES API configuration for Call recording.

-----Link provided by Google team-----

<https://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 Call Recording.

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

media-manager

media-manager

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)

Hint Rtcp ☐ enable

Algd Log Level NOTICE

Mbcd Log Level NOTICE

Options

Figure 2: Media Manager Configuration.

Configuration View Configuration

media-manager

media-manager

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 Signaling Bandwidth 10000000 (Range: 71000.100000000)

Max Untrusted Signaling 100 (Range: 0.100)

Min Untrusted Signaling 30 (Range: 0.100)

Dos Guard Window 5 (Range: 1.30)

Untrusted Minor Threshold 0 (Range: 0.100)

Untrusted Major Threshold 0 (Range: 0.100)

Untrusted Critical Threshold 0 (Range: 0.100)

Figure 2.1: Media Manager Configuration.

Configuration

View Configuration

Q

media-manager

codecc-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Media Manager

Trusted Critical Threshold

0

(Range: 0..100)

Arp Minor Threshold

0

(Range: 0..100)

Arp Major Threshold

0

(Range: 0..100)

Arp Critical Threshold

0

(Range: 0..100)

Tolerance Window

30

(Range: 0..999999999)

Untrusted Drop Threshold

0

(Range: 0..100)

Trusted Drop Threshold

0

(Range: 0..100)

Ad Monitor Window

30

(Range: 5..3600)

Trap On Demote To Deny

☐ enable

Trap On Demote To Untrusted

☐ enable

Syslog On Demote To Deny

☐ enable

Syslog On Demote To Untrusted

☐ enable

Anonymous Sdp

☐ enable

Reactive Transcoding

☐ enable

Translate Non Rfc2833 Event

☐ enable

Xcode Fax Max Rate

14400

Figure 2.2: Media Manager Configuration (Cont.)

7.4.2 Physical Interface

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

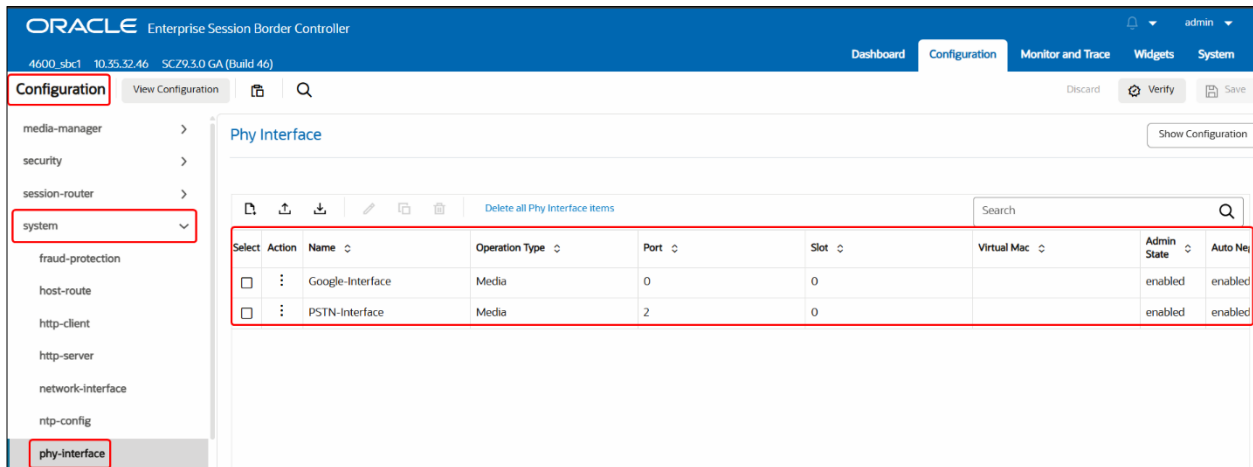


Figure 3: Physical Interfaces.

- The interface designated towards Google CES is named as s0p0 (Slot 0, port 0).

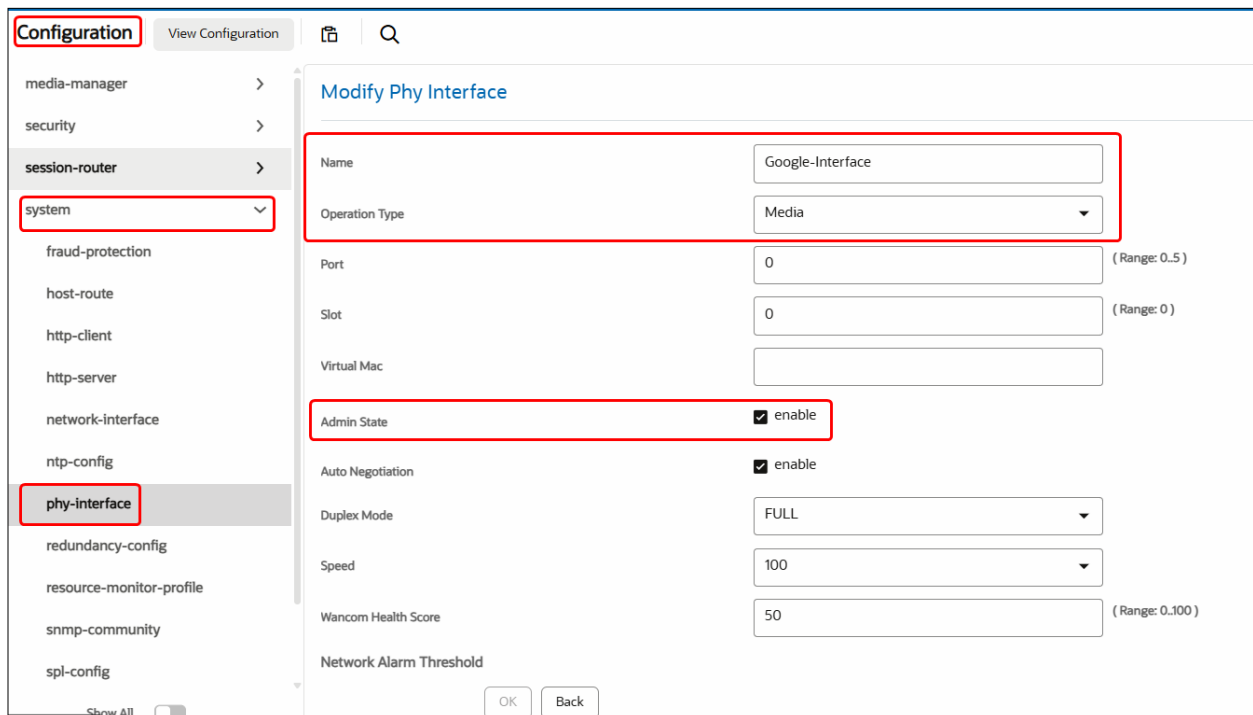


Figure 3.1: Physical Interface towards Google CES (Cont.)

- The interface designated towards PSTN Gateway and OnPrem PBX are named as s0p2 (Slot 0, port 2).

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

Show All ☐

Modify Phy Interface

Name: PSTN-Interface

Operation Type: Media

Port: 2 (Range: 0-5)

Slot: 0 (Range: 0)

Virtual Mac:

Admin State: ☒ enable

Auto Negotiation: ☒ enable

Duplex Mode: FULL

Speed: 100

Wacom Health Score: 50 (Range: 0-100)

Network Alarm Threshold:

OK Back

Figure 3.2: Physical Interface towards PSTN Gateway and OnPrem PBX.

7.4.3 Network Interface

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

Configuration View Configuration

media-manager >
security >
session-router >
system ▾
fraud-protection
host-route
http-client
http-server
network-interface

Network Interface

Select Action Name Sub Port Id Description Hostname IP Address

<input type="checkbox"/>	⋮	Google-Interface	0		sbc10.tekvizionlabs.com	192.65.
<input type="checkbox"/>	⋮	PSTN-Interface	0			10.80.11.11

Figure 4: Network Interfaces.

- Configure Network interface towards Google CES as shown below.

Configuration View Configuration

media-manager >
security >
session-router >
system >
network-interface
ntp-config
phy-interface
redundancy-config
resource-monitor-profile
snmp-community

Modify Network Interface

Name: Google-Interface

Sub Port Id: 0 (Range: 0..4095)

Description:

Hostname: sbc10.

IP Address: 192.65.

Pri Utility Addr:

Sec Utility Addr:

Netmask: 255.255.255.128

Gateway: 192.65.

Figure 4.1: Network Interface towards Google CES.

Configuration View Configuration

media-manager >
security >
session-router >
system >
network-interface
ntp-config
phy-interface
redundancy-config
resource-monitor-profile
snmp-community

Modify Network Interface

▼ Gw Heartbeat

State: ☒ enable

Heartbeat: 10 (Range: 0..65535)

Retry Count: 3 (Range: 0..65535)

Retry Timeout: 3 (Range: 1..65535)

Health Score: 0 (Range: 0..100)

▼ Bfd Config

State: ☐ enable

Health Score: 0 (Range: 0..100)

Options:

Bfd Session:

Figure 4.2: Network Interface towards Google CES (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 Network Interface

Bfd Session

No bfd session to display. Please add.

Add

DNS IP Primary: 8.8.8.8

DNS IP Backup1:

DNS IP Backup2:

DNS Domain: tekvizionlabs.com

DNS Timeout: 11 (Range: 1.999999999)

DNS Max Ttl: 86400 (Range: 30..2073600)

Signaling Mtu: 0 (Range: 0.576..4096)

HIP IP List: 192.65. x

ICMP Address: 192.65. x

SSH Address:

Tunnel Config:

Figure 4.3: Network Interface towards Google CES (Cont.)

- Configure the Network interface towards OnPrem PBX and 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. (Range: 1..254)

Pri Utility Addr:

Sec Utility Addr:

Netmask: 255.255.255.0 (Range: 255..255)

Gateway: 10.80 (Range: 1..254)

Gw Heartbeat

State: ☒ enable

Heartbeat: 10 (Range: 0..65535)

Retry Count: 3 (Range: 0..65535)

Retry Timeout: 3 (Range: 1..65535)

Figure 4.4: Network Interface towards OnPrem PBX and 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 Config

State

☐ enable

Health Score

(Range: 0..100)

Options

Bfd Session

No bfd session to display. Please add.

Add

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)

HTTP IP List

×

ICMP Address

×

Figure 4.5: Network Interface towards OnPrem PBX and PSTN Gateway (Cont.)

7.4.4 SIP Config

Navigate to **Configuration** → **session-router** → **sip-config** for SIP configuration 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
translation-rules
system >

Modify SIP Config

State	<input checked="" type="checkbox"/> enable
Dialog Transparency	<input checked="" type="checkbox"/> enable
Home Realm ID	Google
Egress Realm ID	
Nat Mode	None
Registrar Domain	*
Registrar Host	*
Registrar Port	5060 (Range: 0,025..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
Enforcement Profile	
Emergency Dscp Profile	
Red Max Trans	10000 (Range: 0.50000)
Options	max-udp-length=0 x

Figure 5: SIP-Config.

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

Modify SIP Config

SIP Message Len	65535 (Range: 0..65535)
Enum Sag Match	<input type="checkbox"/> enable
Extra Method Stats	<input 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
Atcf Sin Sr	
Atcf Psi Dn	
Atcf Route To Scas	<input type="checkbox"/> enable
Eafcf Sin Sr	
Sag Lookup On Redirect	<input type="checkbox"/> enable
Set Disconnect Time On Bye	<input type="checkbox"/> enable

Figure 5.1: 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

slip-config

system

Modify SIP Config

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

Add Ue Location In Psn

inherit

Hold Emergency Calls For Loc Info

0

(Range: 0..4294967295)

Retry After Upon Offline

0

(Range: 0..999999999)

Figure 5.2: 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

slip-config

slip-feature

slip-interface

slip-manipulation

slip-monitoring

translation-rules

system

Modify SIP Config

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)

NpII 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..100)

Internal 503 Lower Threshold

40

(Range: 1..95)

503 Alarm Monitoring Time

15

(Range: 5..600)

Figure 5.3: SIP-Config (cont.)

7.4.5 System-Config

- Navigate to **Configuration** → **system** → **system-config** for system configuration 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 System Config

Hostname: Oracle

Description: SBC Connecting PSTN SIP Trunk to Google

Location: Plano TX

Mib System Contact:

Mib System Name:

Mib System Location:

Acp TLS Profile:

Disable Garp Out Of Subnet: ☐ enable

SNMP Enabled: ☒ enable

Enable SNMP Auth Traps: ☐ enable

Enable SNMP Syslog Notify: ☐ enable

Enable SNMP Monitor Traps: ☐ enable

Figure 6: System-Config

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

Enable SNMP Syslog Notify: ☐ enable

Enable SNMP Monitor Traps: ☐ enable

Enable SNMP TLS Srtp Traps: ☐ enable

Enable Env Monitor Traps: ☐ enable

Enable Mblk_tracking: ☐ enable

Enable L2 Miss Report: ☒ enable

Syslog Servers

No syslog server to display. Please add.

Add

System Log Level: WARNING

Process Log Level: NOTICE

Collect

Sample Interval: 5 (Range: 1..120)

Push Interval: 15 (Range: 1..120)

Boot State: ☐ enable

Figure 6.1: 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

Config Backup

Admin State

☐ enable

Interval

weekly

Retry Interval

5

(Range: 5..30)

Retry Count

5

(Range: 2..10)

Push Failure Alarm

☒ enable

Push Receiver

No push receiver to display. Please add.

Add

Comm Monitor

State

☐ enable

Sbc Grp Id

0

(Range: 0..999999999)

TLS Profile

QoS Enable

☒ enable

Interim QoS Update

☐ enable

Monitor Collector

Figure 6.2: 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

Modify System Config

Interim QoS Update

☐ enable

Monitor Collector

No monitor collector to display. Please add.

Add

Options

Call Trace

☐ enable

Default Gateway

0.0.0.0

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)

Figure 6.3: 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

Source Routing ☐ enable

Debug Timeout (Range: 0..65535)

Ecc Chk Pkt ☐ enable

Log TLS Key ☐ enable

Pko Rake Pkt (Range: 0..32768)

Pko Rake Burst (Range: 0..1024)

Default V6 Gateway

Ipv6 Signaling Mtu (Range: 1280..4096)

Ipv4 Signaling Mtu (Range: 576..4096)

Directory Cleanup

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

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 6.4: 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 7: SIP Monitoring.

7.4.7 HTTP Server

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

The screenshot shows the 'Configuration' page with the 'http-server' configuration. The left sidebar has 'Configuration' at the top, followed by 'system' and 'http-server' highlighted. The main area is titled 'Modify HTTP Server'. The configuration fields are: Name (wancom0), State (checked enable), Realm (empty), IP Address (empty), HTTP State (checked enable), HTTP Port (80, range 1-65535), HTTP Strict Transport Security Policy (unchecked enable), HTTPS State (unchecked enable), HTTPS Port (443, range 1-65535), and HTTP Interface List (REST, GUI).

Figure 8: 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 shows the 'Configuration' page with the 'codec-policy' configuration. The left sidebar has 'Configuration' at the top, followed by 'media-manager' and 'codec-policy' highlighted. The main area is titled 'Modify Codec Policy Entries'. The configuration fields are: Name (Google), Allow Codecs (PCMU, PCMA), Add Codecs On Egress (PCMU, PCMA), Order Codecs (PCMU, PCMA), Packetization Time (20), Force Ptime (unchecked enable), Secure Dtmf Cancellation (unchecked enable), Dtmf In Audio (disabled), Tone Detection (empty), and Tone Detect Renegotiate Timer (500, range 50-32000).

Figure 9: 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.

Select	Action	Id	Description	Input Header Type	Input Header Value	Output Header Type	Output Header Value
<input type="checkbox"/>	+	addplus1_called-header	add	called-header	"(0)X.*"	called-header	\$01+\$02
<input type="checkbox"/>	+	addplus1_request-uri	add	request-uri	"(0)X.*"	request-uri	\$01+\$02
<input type="checkbox"/>	+	mapping_none	replace	none	"(.*)(3502).*(.*)"	none	\$02\$1\$42598\$02
<input type="checkbox"/>	+	removeplus1_called-header	delete	called-header	"(.*)(.*)"	called-header	\$1\$2
<input type="checkbox"/>	+	removeplus1_p-asserted-id-header	delete	p-asserted-id-header	"(.*)(.*)"	p-asserted-id-header	\$1\$2
<input type="checkbox"/>	+	removeplus1_request-uri	delete	request-uri	"(.*)(.*)"	request-uri	\$1\$2

Figure 10: Translation Rule to add send E.164 towards 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.

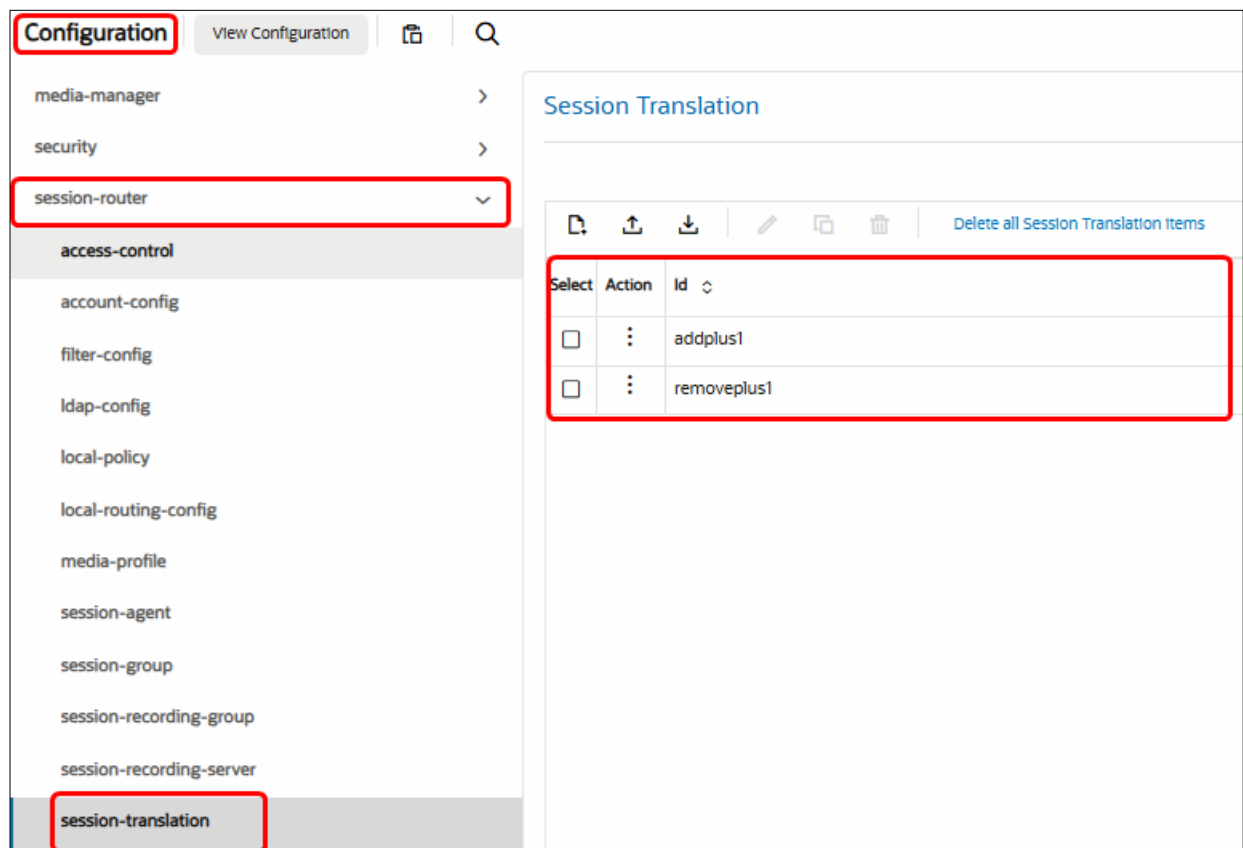


Figure 11: Session Translation towards Google CES.

7.4.11

Session Recording Server

- Navigate to **Configuration** → **session-router** → **session-recording-server** and select the destination as Google FQDN
- SIPREC profile for Google CES is created using the Session Recording Server

Configuration View Configuration

session-router **session-recording-server**

Modify Session Recording Server

Name	GoogleCCAI
Description	GoogleCCAI
Realm	Google
Mode	selective
Destination	us.telephony.goog
Port	5672 (Range: 1024..65535)
Transport Method	StaticTLS
Force Parity	<input type="checkbox"/> enable
Ping Method	OPTIONS
Ping Interval	60 (Range: 0..4294967295)
Refresh Interval	0 (Range: 0..60)

Figure 12: Session Recording Server towards Google CES.

7.4.12 Realm Config

- Navigate to **Configuration** → **media-manager** → **realm-config**.
- Realm Config towards Google CES is shown below.

Configuration View Configuration

media-manager **realm-config**

Realm Config

Delete all Realm Config items

Select	Action	Identifier	Description	Addr Prefix	Network Interfaces	Media Realm List	Min In Realm	Min In Network
<input type="checkbox"/>	:	Google		0.0.0.0	Google-Interface:0.4		enabled	enabled
<input type="checkbox"/>	:	PSTN		0.0.0.0	PSTN-Interface:0.4		enabled	enabled

Figure 13: Realm Config towards Google CES.

Configuration View Configuration

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

security >

session-router >

system >

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:

DNS Realm:

Media Policy:

Figure 13.1: 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

Media Sec Policy: SRTP

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 13.2: Realm Config towards Google CES (Cont.)

Configuration View Configuration

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

Modify Realm Config

Out Session Translations

Select	Action	Out Session Translation Id	State
<input type="checkbox"/>	addplus1		enabled

Figure 13.3: 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

Displaying 1 - 1 of 1

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)

Deny Period

30

(Range: 0.4294967295)

Figure 13.4: 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

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

Refer Notify Provisional

none

Dyn Refer Term

☐ enable

Codec Policy

Google

Figure 13.5: 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

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)

TCP Initial Guard Timer -1 (Range: -1.2147483647)

TCP Subsq Guard Timer -1 (Range: -1.2147483647)

SIP Isup Profile

QoS Constraint

Figure 13.6: Realm Config towards Google CES (Cont.)

- Realm Config towards OnPrem PBX and PSTN Gateway is shown below.

Configuration View Configuration

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

security >

session-router >

system >

Modify Realm Config

Identifier PSTN

Description

Addr Prefix 0.0.0.0

Network Interfaces PSTN-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)

Figure 14: Realm Config towards OnPrem PBX and PSTN Gateway.

Configuration View Configuration  

media-manager 

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

Modify Realm Config











Subscription Id Type	END_USER_NONE 
Trunk Context	<input type="text"/>
Early Media Allow	
Enforcement Profile	
Additional Prefixes	<input type="text"/>
Restricted Latching	none 
Options	<input type="text"/>
SPL Options	<input type="text"/>
Delay Media Update	<input type="checkbox"/> enable
Refer Call Transfer	disabled 
Hold Refer Reinvite	<input type="checkbox"/> enable
Refer Notify Provisional	none 
Dyn Refer Term	<input type="checkbox"/> enable
Codec Policy	Google 
Codec ManIP In Realm	<input type="checkbox"/> enable
Codec ManIP In Network	<input checked="" type="checkbox"/> enable

Figure 14.3: Realm Config towards OnPrem PBX and PSTN Gateway Cont.

Configuration View Configuration  

media-manager 

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

Modify Realm Config



Session Recording Server	GoogleCCAI 
Session Recording Required	<input type="checkbox"/> 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)
TCP Initial Guard Timer	-1 (Range: -1.2147483647)
TCP Subsq Guard Timer	-1 (Range: -1.2147483647)

Figure 14.4: Realm Config towards OnPrem PBX and PSTN Gateway Cont.

7.4.13 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 OnPrem PBX and PSTN Gateway are shown below.

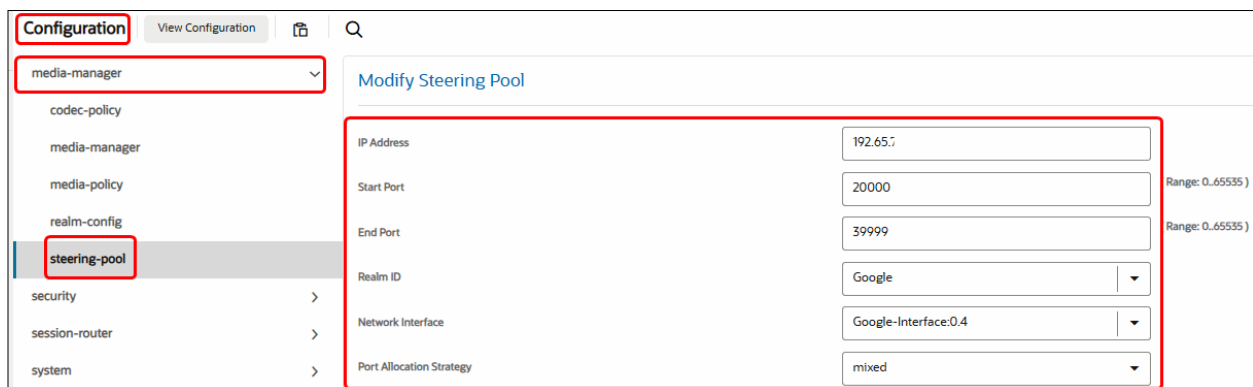


The screenshot shows the 'Steering Pool' configuration page. On the left, a sidebar menu has 'steering-pool' highlighted. The main area displays a table with the following data:

Select	Action	IP Address	Start Port	End Port	Realm ID	Network Interface	Port Allocation Strategy
<input type="checkbox"/>		10.80	50000	59999	PSTN	PSTN-Interface:0.4	mixed
<input type="checkbox"/>		192.65	20000	39999	Google	Google-Interface:0.4	mixed

Figure 15: Steering Pool.

- Steering Pool Configuration towards Google CES is shown below.

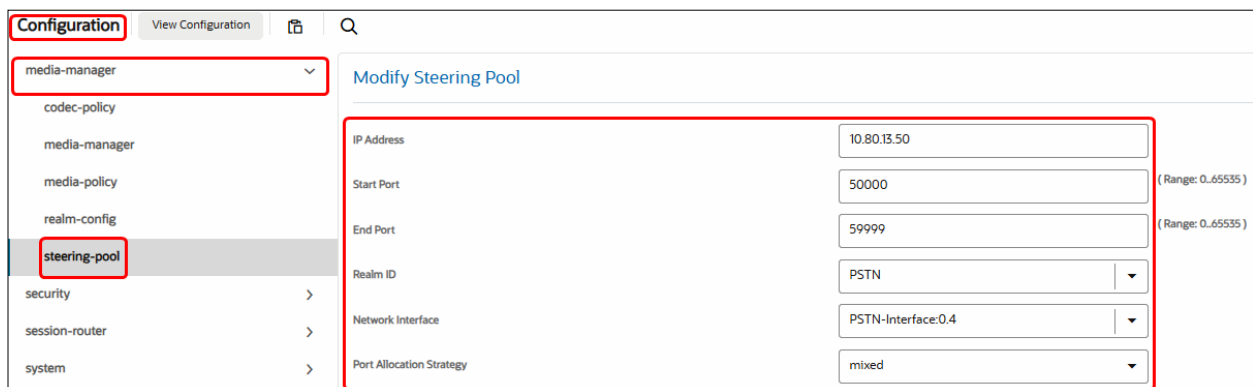


The screenshot shows the 'Modify Steering Pool' form. The sidebar menu has 'steering-pool' highlighted. The form fields are as follows:

IP Address	192.65.5	
Start Port	20000	(Range: 0.65535)
End Port	39999	(Range: 0.65535)
Realm ID	Google	
Network Interface	Google-Interface:0.4	
Port Allocation Strategy	mixed	

Figure 15.1: Steering Pool towards Google CES.

- Steering Pool Configuration towards Onprem PBX & PSTN is shown below



The screenshot shows the 'Modify Steering Pool' form. The sidebar menu has 'steering-pool' highlighted. The form fields are as follows:

IP Address	10.80.13.50	
Start Port	50000	(Range: 0.65535)
End Port	59999	(Range: 0.65535)
Realm ID	PSTN	
Network Interface	PSTN-Interface:0.4	
Port Allocation Strategy	mixed	

Figure 15.2: Steering Pool towards Google CES.

7.4.14 SDES Profile

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

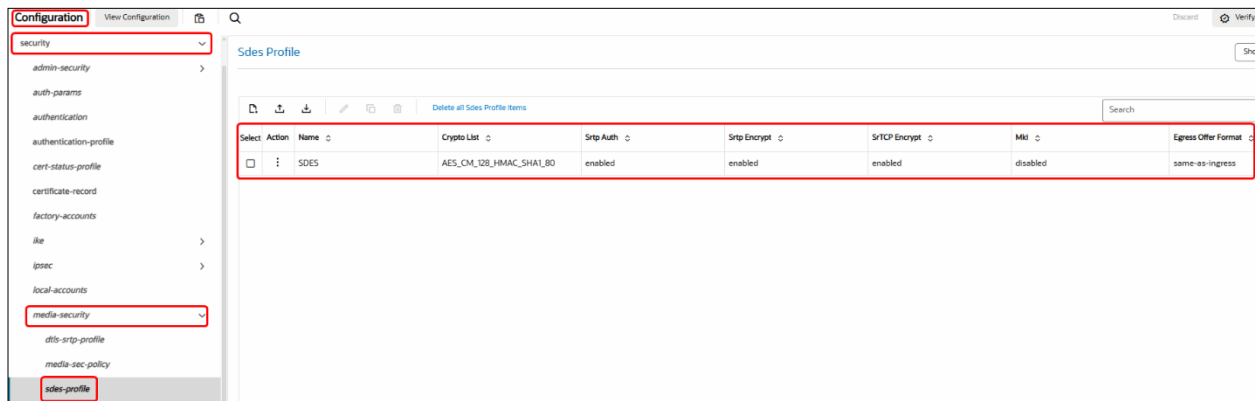


Figure 16: SDES Profile for TLS.

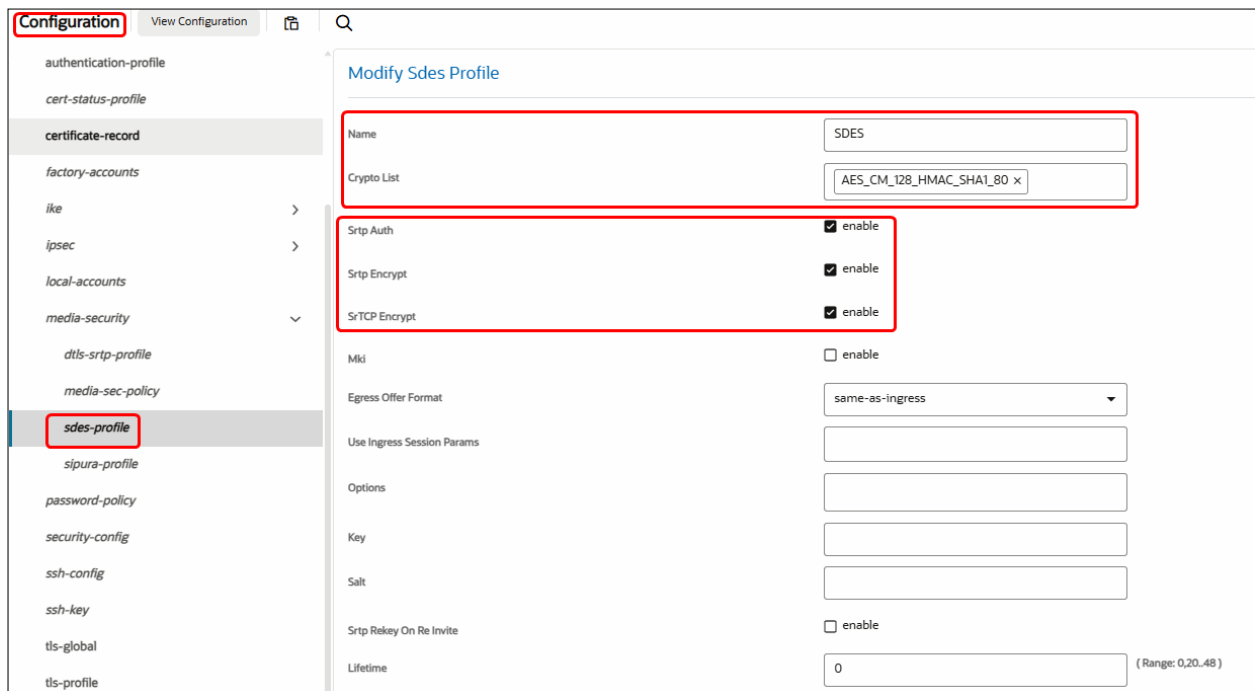


Figure 16.1: SDES Profile for TLS.

7.4.15 Media Sec Policy

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

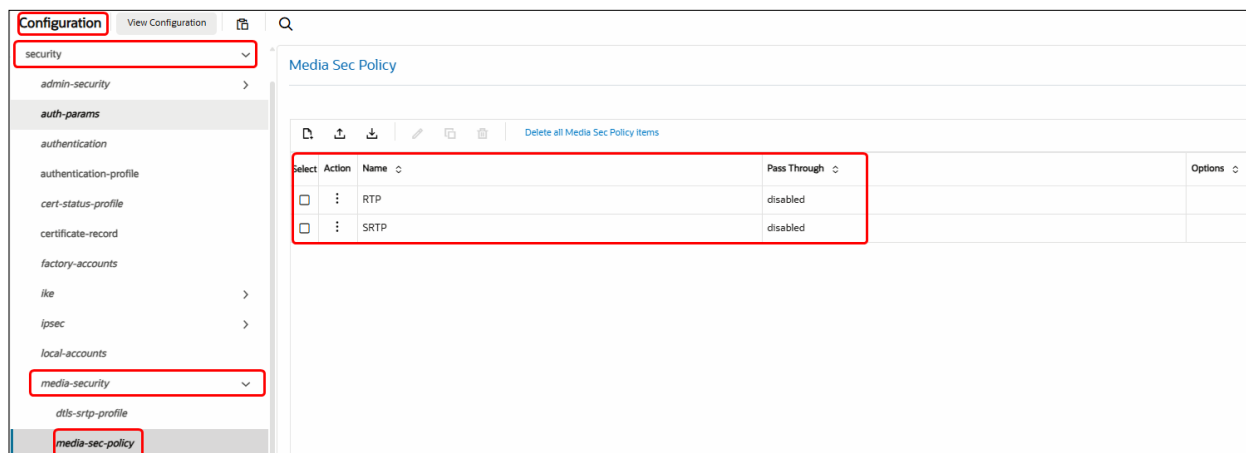


Figure 17: Media Security Policy

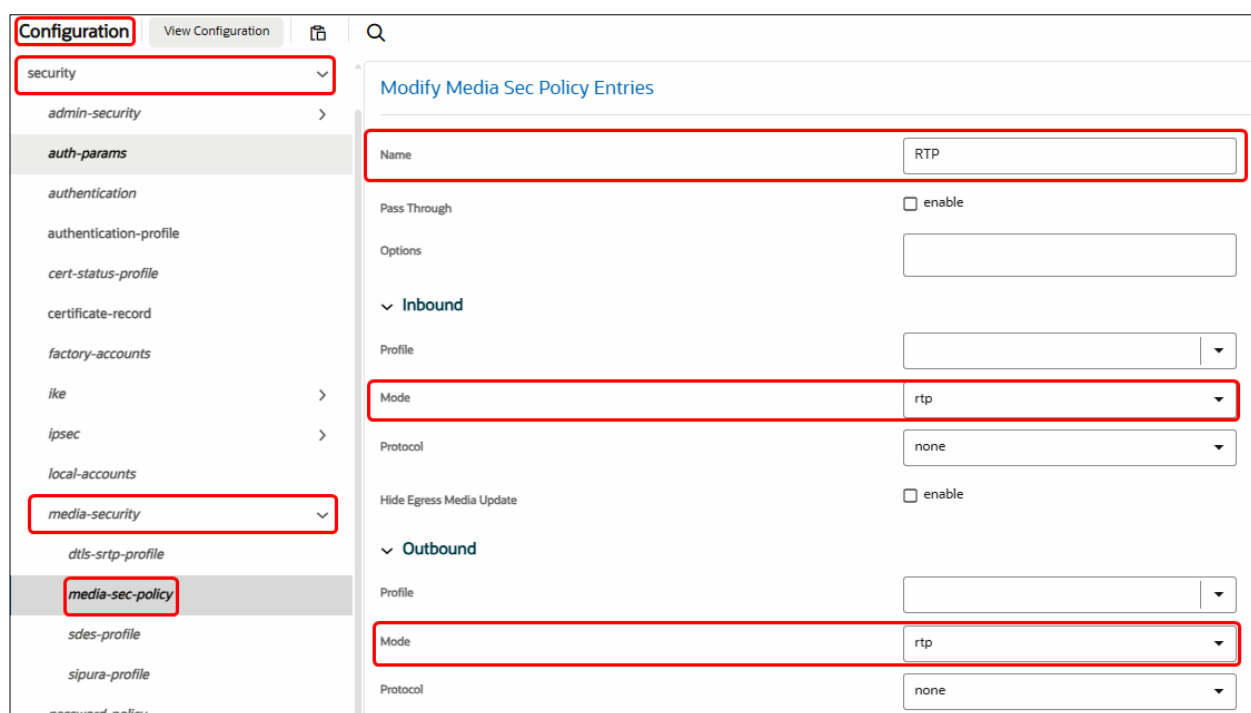


Figure 17.1: Media Security Policy for RTP.

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

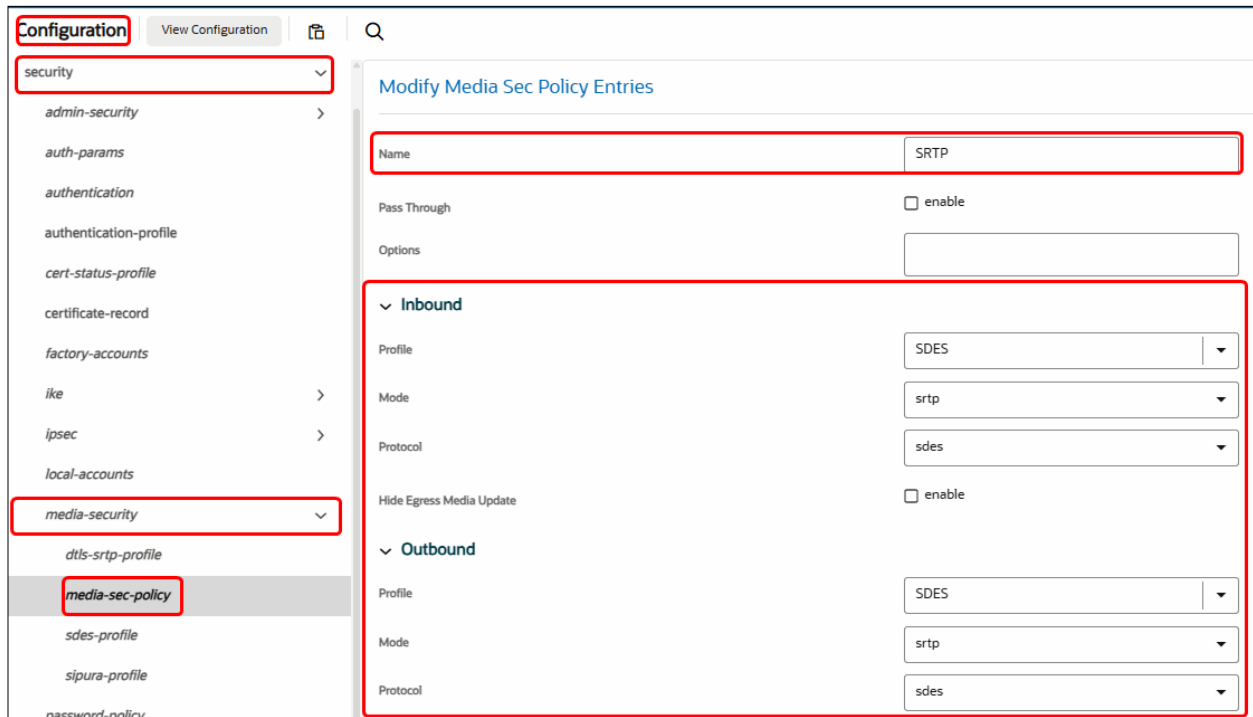


Figure 17.2: Media Security Policy for SRTP.

7.4.16 TLS – Certificate Record

- Certificate Record are configuration elements on Oracle SBC which captures information for a TLS certificate such as common-name, key-size etc.
- Navigate to **Configuration** → **security** → **certificate-record**.
- Create a certificate record for Oracle E-SBC as shown below.
 - Select the Certificate record and Click **Generate icon** to generate CSR.
 - Get the CSR signed and click **Import** to import the signed certificate.

Configuration View Configuration

media-manager >

security ▾

authentication-profile

certificate-record

tls-global

tls-profile

session-router >

system >

Modify Certificate Record

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

Digest Algor sha256

Ecdsa Key Size p256

Figure 18: Create Certificate Record for Oracle E-SBC

<input checked="" type="checkbox"/>	⋮	sbc10	US	Texas	Plano	tekvisionlabs	tekvision	sbc10.tekvisionlabs.com
<input type="checkbox"/>	✎	Edit	US	MA	Burlington	Engineering		
<input type="checkbox"/>	📄	Copy						
<input type="checkbox"/>	🗑️	Delete						
<input type="checkbox"/>	🔑	Generate						
<input type="checkbox"/>	📄	Import						

Figure 18.1: Import Certificate Record for Oracle E-SBC

- Download the Google certificate via link <https://pki.goog/roots.pem>
- Create a certificate record GTS Root R1 for Google CES.

The screenshot shows the 'Modify Certificate Record' configuration page. The left sidebar has a tree view with 'security' and 'certificate-record' highlighted. The main area contains the following fields:

Name	GTS_Root1
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	
Common Name	
Key Algor	rsa
Digest Algor	sha256
Ecdsa Key Size	p256
Cert Status Profile List	

Figure 18.2: Create Certificate Record for Google GTS Root R1 certificate

- Right click on the Certificate Record and Click Import. Import the root certificate stored in the local machine and click Import as shown below.

The screenshot shows the 'Import Certificate' dialog box. It contains the following fields:

Format	try-all
Import Method	File (selected)
Certificate File	upload button

Figure 18.3: Import Google GTS Root R1 certificate.

- Similarly create other certificate records for the 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 SBC to connect with Google CES.

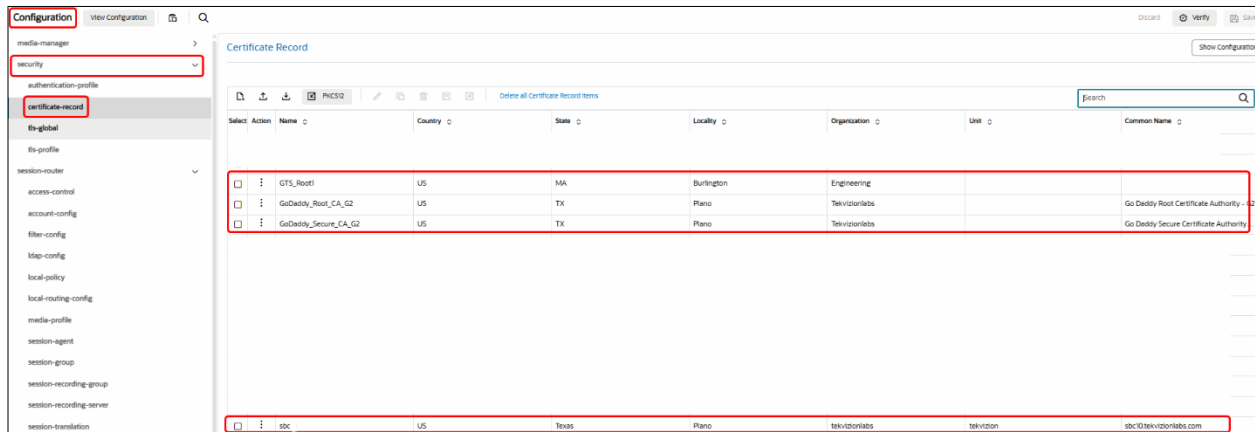


Figure 18.4: Certificate Records.

7.4.17 TLS – TLS Profile

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

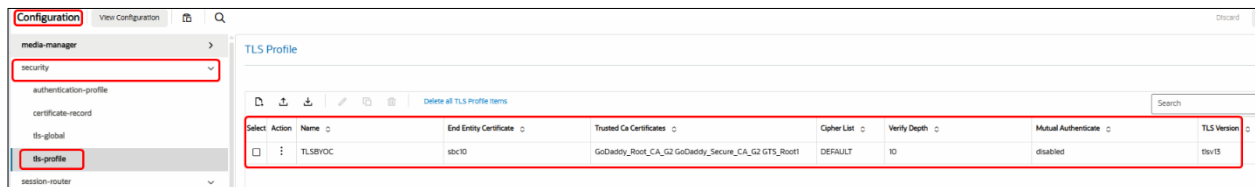


Figure 19: TLS Profile.

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

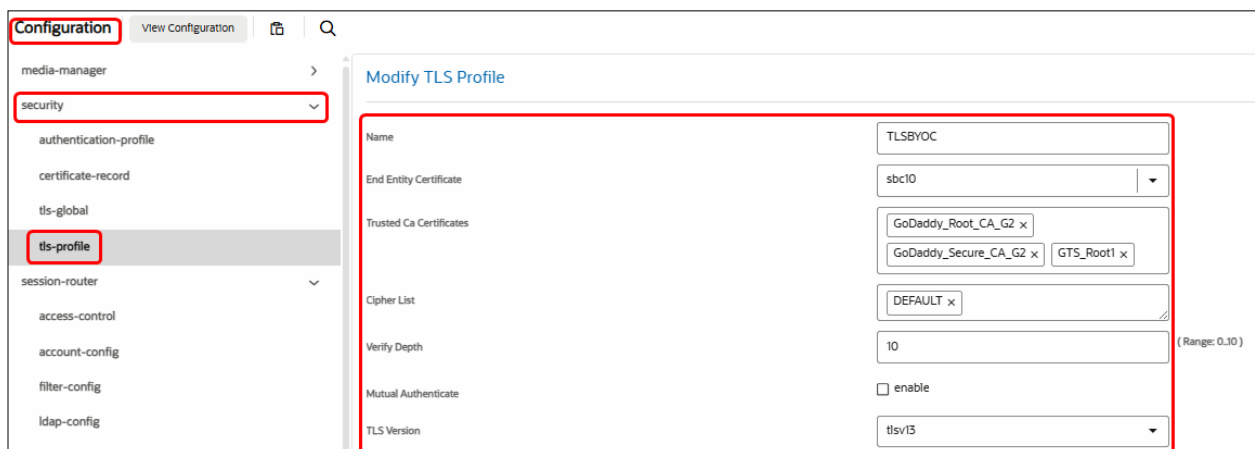


Figure 19.1: TLS Profile

7.4.18 Session Timer

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



Figure 20: Session Timer

7.4.19 SIP Interface

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

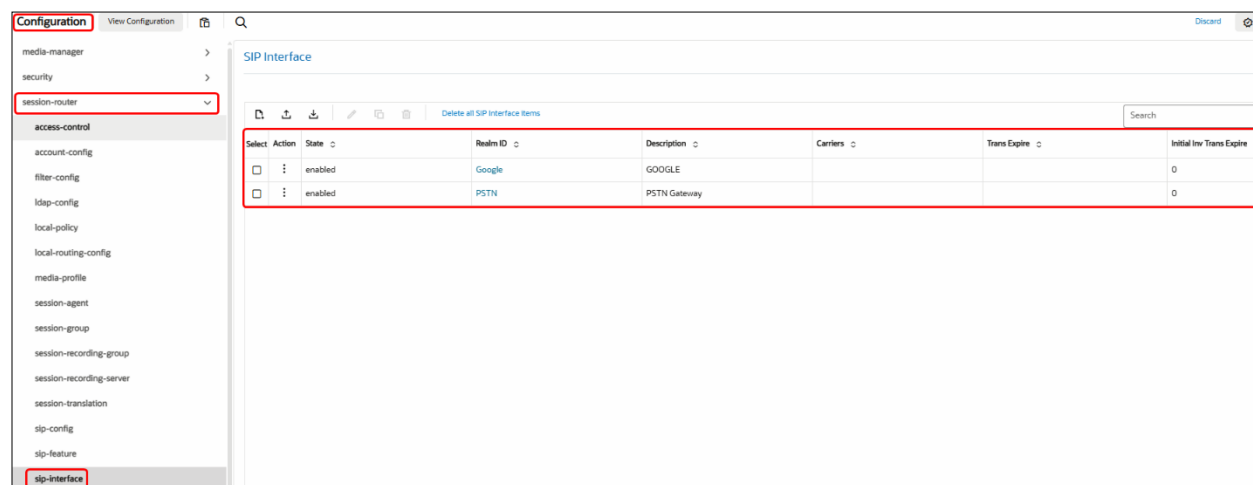


Figure 21: SIP Interface.

- Create SIP interface towards PSTN Gateway and OnPrem PBX by adding SIP Ports as shown below

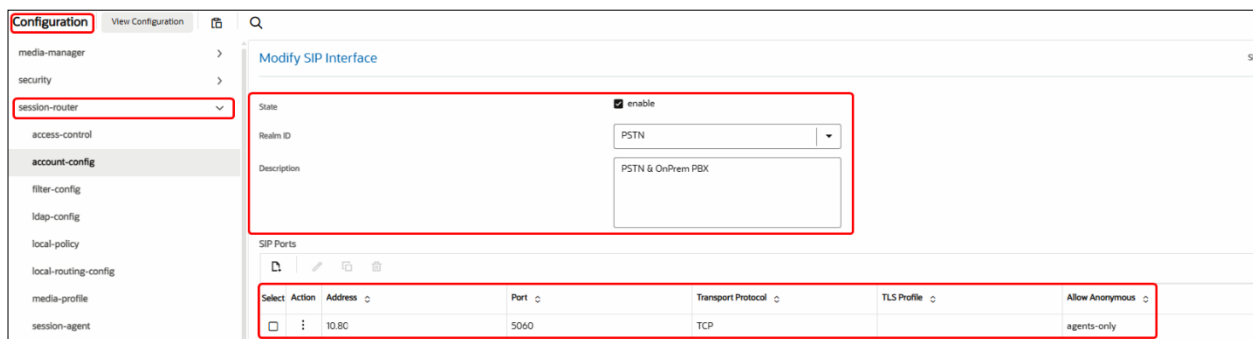


Figure 21.1: SIP Interface for PSTN & OnPrem PBX (Cont.)

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

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	<input checked="" type="checkbox"/> enable	
Min Reg Expire	300	(Range: 0.999999999)
Registration Interval	3600	(Range: 1.999999999)
Route To Registrar	<input checked="" type="checkbox"/> enable	
Secured Network	<input type="checkbox"/> enable	

Figure 21.2: SIP Interface for PSTN &OnPrem PBX (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 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	<input type="checkbox"/> 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	<input type="checkbox"/> enable	
Stop Recurse	401,407	
Port Map Start	0	(Range: 0,1025..65535)
Port Map End	0	(Range: 0,1025..65535)
In Manipulationid		
Out Manipulationid		

Figure 21.3: SIP Interface for PSTN &OnPrem PBX (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

slp-config

slp-feature

slp-interface

Modify SIP Interface

Rfc2833 Payload 101 (Rate)

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

Add SDP Profiles PCMU x PCMA x

Figure 21.4: SIP Interface for PSTN &OnPrem PBX (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

slp-config

slp-feature

slp-interface

Modify SIP Interface

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

Sm Icsi Match For Invite

Sm Icsi Match For Message

S8hr Profile

Ringback Trigger none

Figure 21.5: SIP Interface for PSTN &OnPrem PBX (Cont.)

- Create SIP interface towards Google CES by adding SIP Ports 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

Modify SIP Interface

State ☒ enable
Realm ID: Google
Description: GOOGLE

SIP Ports

Select	Action	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous
<input type="checkbox"/>	:	192.65	5061	TLS	TLSBYOC	agents-only

Figure 22: SIP Interface for 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
sip-config
sip-feature
sip-interface
sip-manipulation

Modify SIP Interface

Initial Inv Trans Expire: 0 (Range: 0..2147473)
Session Max Life Limit: 0
Proxy Mode:
Redirect Action:
Nat Traversal: always
Nat Interval: 3600 (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:
SPL Options:

Figure 22.1: 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

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: 0,1025..65535)

Port Map End

0

(Range: 0,1025..65535)

In Manipulationid

Out Manipulationid

Figure 22.2: 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

Modify SIP Interface

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

enabled

Add SDP Invite

both

Add SDP In Msg

P Early Media Header

disabled

P Early Media Direction

Add SDP Profiles

PCMU x

Figure 22.3: 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

Modify SIP Interface

Session Timer Profile: SessionTimer

Session Recording Server: [Text Field]

Session Recording Required: ☐ enable

Service Tag: [Text Field]

Reg Cache Route: ☐ enable

Diversion Info Mapping Mode: none

Atcf Icsi Match: [Text Field]

SIP Recursion Policy: [Text Field]

Asymmetric Preconditions: ☐ enable

Asymmetric Preconditions Mode: send-with-nodelay

Sm Icsi Match For Invite: [Text Field]

Sm Icsi Match For Message: [Text Field]

SBhr Profile: [Text Field]

Ringback Trigger: none

Figure 22.4: SIP Interface for Google CES (Cont.)

7.4.20 Session Agent

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

Delete all Session Agent items

Select	Action	Hostname	IP Address	Port	State	App Protocol	Realm ID	Description
<input type="checkbox"/>		10.64.1.72	10.64.1.72	5060	enabled	SIP	PSTN	
<input type="checkbox"/>		172.16.29.18	172.16.29.18	5060	enabled	SIP	PSTN	Free PBX 2
<input type="checkbox"/>		172.16.29.56	172.16.29.56	5060	enabled	SIP	PSTN	Free PBX 1
<input type="checkbox"/>		us.telephony.gong		5072	enabled	SIP	Google	

Figure 23: Session Agent.

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

Modify Session Agent

Hostname

IP Address

Port (Range: 0,1025..65535)

State ☒ enable

App Protocol



App Type

Transport Method

Realm ID

Egress Realm ID

Figure 23.1: 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

Modify Session Agent

Loose Routing ☒ enable

Response Map

Ping Method

Ping Interval

Ping Send Mode

Ping All Addresses ☐ enable

Ping In Service Response Codes

Load Balance DNS Query

Options

SPL Options

Media Profiles

Figure 23.2: Session Agent for Google CES (Cont.)

Configuration View Configuration  

media-manager >

security >

session-router >

access-control

account-config

filter-config

Modify Session Agent

Out Session Translations

Select	Action	Out Session Translation Id	State
<input type="checkbox"/>		addplus1	enabled

Figure 23.3: 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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

system >

Modify Session Agent

Ping Response ☒ enable

In Manipulationid

Out Manipulationid

Manipulation String

Manipulation Pattern

Trunk Group

Max Register Sustain Rate (Range: 0.999999999)

Invalidate Registrations ☐ enable

Rfc2833 Mode

Rfc2833 Payload (Range: 0.96.127)

Codec Policy

Emergency Dscp Profile

Refer Call Transfer

Refer Notify Provisional

Reuse Connections

TCP Keepalive

Figure 23.4: 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

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

system >

Modify Session Agent

TCP Reconn Interval (Range: 0.2.300)

Max Register Burst Rate (Range: 0.999999999)

Rate Constraints

No rate constraints to display. Please add.

[Add](#)

SIP Profile

SIP Isup Profile

Kpml Interworking

Kpml2833 lwf On Hairpin

Precedence (Range: 0.4294967295)

Monitoring Filters

Auth Attribute

No auth attributes to display. Please add.

[Add](#)

Session Recording Server

Session Recording Required ☐ enable

Figure 23.5: Session Agent for Google CES (Cont.)

- Configure the Session Agent for OnPrem PBX as shown below

Configuration View Configuration

session-router

session-agent

Modify Session Agent

Hostname: 172.16..

IP Address: 172.16..

Port: 5060 (Range: 0,1025..65535)

State: ☒ enable

App Protocol: SIP

App Type:

Transport Method: StaticTCP

Realm ID: PSTN

Egress Realm ID:

Description: Free PBX 1

Figure 24: Session Agent for OnPrem PBX

Configuration View Configuration

session-router

session-agent

Modify Session Agent

Loose Routing: ☒ enable

Response Map:

Ping Method: OPTIONS

Ping Interval: 60 (Range: 0.9999999999)

Ping Send Mode: keep-alive

Ping All Addresses: ☒ enable

Ping In Service Response Codes:

Load Balance DNS Query: hunt

Options:

SPL Options:

Media Profiles:

Figure 24.1: Session Agent for OnPrem PBX (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

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

Refer Notify Provisional none

Reuse Connections NONE

TCP Keepalive none

Figure 24.2: Session Agent for OnPrem PBX (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

Modify Session Agent

Kpml Interworking inherit

Kpml2833 Inv On Hairpin inherit

Precedence 0 (Range: 0..4294967295)

Monitoring Filters

Auth Attribute

No auth attributes to display. Please add.

Add

Session Recording Server

Session Recording Required ☐ enable

Hold Refer Reinstate ☐ enable

Send TCP Fin ☐ enable

SIP Recursion Policy

Sim Icsi Match For Invite

Sim Icsi Match For Message

Ringback Trigger none

Figure 24.3: Session Agent for OnPrem PBX (Cont.)

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

Configuration View Configuration

session-router

session-agent

Modify Session Agent

Hostname: 10.64.1.72

IP Address: 10.64.1.72

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

State: ☒ enable

App Protocol: SIP

App Type:

Transport Method: StaticTCP

Realm ID: PSTN

Egress Realm ID: PSTN

Figure 25: Session Agent for PSTN Gateway.

Configuration View Configuration

session-router

session-agent

Modify Session Agent

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

Options:

SPL Options:

Media Profiles:

Figure 25.1: Session Agent for PSTN Gateway (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 ManipulationId

Out ManipulationId

Manipulation String

Manipulation Pattern

Trunk Group

Max Register Sustain Rate

Invalidate Registrations

Rfc2833 Mode

Rfc2833 Payload

Codec Policy

Emergency Dscp Profile

Refer Call Transfer

Refer Notify Provisional

Reuse Connections

TCP Keepalive

0 (Range: 0.999999999)

☐ enable

transparent

0 (Range: 0.96.127)

Google

disabled

none

NONE

none

Figure 25.2: Session Agent 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

sip-manipulation

sip-monitoring

Modify Session Agent

Kpml Interworking

Kpml2833 lwf On Hairpin

Precedence

Monitoring Filters

Auth Attribute

Session Recording Server

Session Recording Required

Hold Refer Reinvite

Send TCP Fin

SIP Recursion Policy

Sm Icsi Match For Invite

Sm Icsi Match For Message

Ringback Trigger

0 (Range: 0.4294967295)

No auth attributes to display. Please add.

Add

☐ enable

☐ enable

☐ enable

none

Figure 25.3: Session Agent for PSTN Gateway (Cont.)

7.4.21 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.
- Navigate to **Configuration** → **session-router** → **local-policy**.
- Configure local policy for Google CES, OnPrem PBX and PSTN Gateway as shown below.

Select	Action	From Address	To Address	Source Realm	Description	Activate Time	Deactivate Time	State
<input type="checkbox"/>	:	*	214 *1214	PSTN	PBX user to PSTN			enabled
<input type="checkbox"/>	:	*	9728522625	PSTN	PBX2_2918			enabled
<input type="checkbox"/>	:	*	9728522631 9728522635	PSTN	PBX_29.56			enabled
<input type="checkbox"/>	:	*	9728522617 9728522648	PSTN	PSTN to CUCM PBX			enabled

Figure 26: Local Policy

- Below Local Policy is used to route calls from OnPrem PBX to PSTN Gateway.

Select	Action	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup
<input type="checkbox"/>	:	10.64.1.72	PSTN	none	disabled	0	enabled	SIP	single

Figure 26.1: Local Policy routing from PBX to PSTN

Next Hop	10.64.1.72
Realm	PSTN
Action	none
Terminate Recursion	<input type="checkbox"/> enable
Cost	0 (Range: 0.999999999)
State	<input checked="" type="checkbox"/> enable
App Protocol	SIP
Lookup	single
Next Key	
Auth User Lookup	

Figure 26.2: Local Policy routing Towards PSTN Gateway.

- Below Local Policy is used to route calls from PSTN Gateway to OnPrem PBX.

Select	Action	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup
<input type="checkbox"/>	:	172.16.	PSTN	none	disabled	0	enabled		single

Figure 26.3: Local Policy routing Towards PBX Gateway.

Next Hop: 172.16.

Realm: PSTN

Action: none

Terminate Recursion: ☐ enable

Cost: 0 (Range: 0.999999999)

State: ☒ enable

App Protocol:

Lookup: single

Next Key:

Auth User Lookup:

Figure 26.4: Local Policy routing Towards PBX Gateway.

7.4.22 SIP Manipulation

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

Action	Name	Element Type
⋮	changeRequiri	header-rule
⋮	changeFromIP	header-rule
⋮	changeToURlhost	header-rule
⋮	AddCallInfoHeader	header-rule
⋮	changelocalport	header-rule
⋮	deltransport	header-rule
⋮	delete_callinfo	header-rule

Figure 27: SIP Manipulation towards Google CES.

- Add a header-rule for Google CES

Action	Name	Element Type
⋮	changeRequiri	header-rule
⋮	changeFromIP	header-rule
⋮	changeToURlhost	header-rule
⋮	AddCallInfoHeader	header-rule
⋮	changelocalport	header-rule
⋮	deltransport	header-rule
⋮	delete_callinfo	header-rule

Figure 27.1: 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 **+1361880XXXX**.

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 27.2: SIP Manipulation towards Google CES- To change 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 27.3: SIP Manipulation towards Google CES – To change Request URI-host.

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

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 "+13618809831"

Figure 27.4: SIP Manipulation towards Google CES – Change Request URI-user.

- Below header rule is created to change FROM header IP address towards Google CES to IP address of Oracle SBC.

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 changeFromIP
Header Name FROM
Action manipulate
Comparison Type pattern-rule
Msg Type any
Methods INVITE x OPTIONS x
Match Value
New Value

CfgRules

Action	Name	Element Type
:	changeIP	element-rule
:	changetofo	element-rule

Figure 27.5: SIP Manipulation towards Google CES – Change FROM header.

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

Modify Sip manipulation / header rule / element rule

Name: changeIP

Parameter Name:

Type: uri-host ▾

Action: replace ▾

Match Val Type: any ▾

Comparison Type: pattern-rule ▾

Match Value:

New Value: \$LOCAL_IP

Figure 27.6: SIP Manipulation towards Google CES – Change FROM header uri-host.

- Match value : To:sips:"us.telephony.goog":5672;trasnafort=tls
- New Value : To:<sips:"+1361880XXXX@us.telephony.goog":5672;trasnafort=tls>

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

Modify Sip manipulation / header rule / element rule

Name: changetofof

Parameter Name:

Type: uri-user ▾

Action: replace ▾

Match Val Type: any ▾

Comparison Type: case-sensitive ▾

Match Value: To:<sips:"us.telephony.goog":5672;trasnafort=tls>

New Value: To:<sips:"+13618809831@us.telephony.goog":5672;t

Figure 27.7: SIP Manipulation towards Google CES – Change FROM header 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

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: 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
⋮	changeToURIhost	element-rule

Figure 27.8: SIP Manipulation towards Google CES – Change TO header.

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 / element rule

Name: changeURIhost
Parameter Name:
Type: uri-host
Action: replace
Match Val Type: any
Comparison Type: pattern-rule
Match Value:
New Value: "us.telephony.goog"

Figure 27.9: SIP Manipulation towards Google CES – Change TO header uri-host.

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

Modify Sip manipulation / header rule / element rule

Name changeToURlhost

Parameter Name To

Type uri-user ▾

Action replace ▾

Match Val Type any ▾

Comparison Type case-sensitive ▾

Match Value

New Value "+13618809831"

Figure 27.10: SIP Manipulation towards Google CES – Change TO header uri-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 SBC for each call.
- New Value is set to "<[http://dialogflow.googleapis.com/v2beta1/projects/CES-389811/conversations/OR_+\\$CALL_ID.\\$0+](http://dialogflow.googleapis.com/v2beta1/projects/CES-389811/conversations/OR_+$CALL_ID.$0+)>;purpose=Goog-ContactCenter-Conversation"

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 AddCallInfoHeader

Header Name Call-info

Action add ▾

Comparison Type case-sensitive ▾

Msg Type any ▾

Methods INVITE x

Match Value

New Value "<http://dialogflow.googleapis.com/v2beta1/projec

CfgRules

No rules to display. Please add.

Add ▾

Figure 27.11: SIP Manipulation towards Google CES – Add Call-Info.

- Participation Label:**

- The transcript recording files stored in the Google CES bucket include two participant roles "HUMAN_AGENT" and "END_USER".
- To map the participant roles to the transcripts generated, Google uses the participant labels provided in the call-info header. Use the below rule only if Participant labels are required in your setup.
- Sample call-info header with participant roles:
 - Call-info: "<http://dialogflow.googleapis.com/v2beta1/projects/CES-389811/conversations/OR_\"+\$CALL_ID.\$0+\"?roles=HUMAN_AGENT,END_USER>;purpose=Goog-ContactCenter-Conversation"

The screenshot shows the 'Configuration' page with a sidebar on the left containing various configuration categories. The 'sip-manipulation' category is selected and highlighted. The main content area is titled 'Modify Sip manipulation / header rule'. It contains a form with the following fields:

- Name:** AddCallInfoHeader_Participation Label
- Header Name:** Call-info
- Action:** add
- Comparison Type:** case-sensitive
- Msg Type:** any
- Methods:** INVITE x
- Match Value:** (empty field)
- New Value:** "<http://dialogflow.googleapis.com/v2beta1/projeci

Below the form, there is a section labeled 'CfgRules' with the text 'No rules to display. Please add.' and an 'Add' button.

Figure 27.12: SIP Manipulation towards Google CES – Add Call-Info for Participation Label.

- Below header rule is created to delete the Google CES 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 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

Modify Sip manipulation / header rule

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.google)(.*)\$
New Value	\$1+\$3

Figure 27.13: 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

Add ▾

Action	Name	Element Type
⋮	chnagetransportnumber	element-rule

Figure 27.14: 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

Modify Sip manipulation / header rule / element rule

Name: chnagettransportnumber

Parameter Name:

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

Figure 27.15: SIP Manipulation towards Google CES – Change Request URI Port number.

- Below header rule is created to delete the transport parameter 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: deltransport
Header Name: Request-URI
Action: manipulate ▾
Comparison Type: case-sensitive ▾
Msg Type: any ▾
Methods: INVITE ×
Match Value:
New Value:

Cfgrules

Action	Name	Element Type
⋮	delparam	element-rule

Figure 27.16: SIP Manipulation towards Google CES – Delete Transport parameter.

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

delparam

Parameter Name

transport

Type

uri-param

Action

delete-element

Match Val Type

any

Comparison Type

case-sensitive

Match Value

New Value

Figure 27.17: SIP Manipulation towards Google CES Cont. – Delete Transport parameter.

8 SIP INVITE To Google CES

8.1 SIP INVITE for SIPREC call

```
INVITE sip:+13618809831@us.telephony.goog:5672 SIP/2.0
Via: SIP/2.0/TLS 192.65.79.223:5061;branch=z9hG4bKqtf9ng103ov0tbubt2n0
From: sip:acmeSrc@192.65.79.223;tag=fc4e824a0f617ddcbf1e98c90f7ead51
To: <sip:+13618809831@us.telephony.goog:5672;transport=tcp>
Call-ID: 44dd70a5480470e9f5932cb3f578484d020@us.telephony.goog
CSeq: 1080 INVITE
Contact: <sip:acmeSrc@192.65.79.223:5061;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-389811/conversations/
OR_44dd70a5480470e9f5932cb3f578484d020>;purpose=Goog-ContactCenter-Conversation

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

v=0
o=- 3562256 226213 IN IP4 192.65.79.223
s=-
c=IN IP4 192.65.79.223
t=0
m=audio 20910 RTP/SAVP 0 101
c=IN IP4 192.65.79.223
a=rtptime:0 PCMU/8000
a=rtptime: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:1ZbR91HLKuYJ8T4ejRWE1rWkdg42ket0XmrtM80k
m=audio 20914 RTP/SAVP 0 101
a=rtptime:0 PCMU/8000
a=rtptime: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:aUYfGWeUmqFDSeCQ655VEu4muW9bdcvCmuqpa1iD
```

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 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 28: SIPREC call

8.2 SIP INVITE for GTP call

```
INVITE sip:+13149445469@us.telephony.goog:5672 SIP/2.0
Via: SIP/2.0/TLS 192.65.79.223:5061;branch=z9hG4bK1b6trn0000e10aih
From: <sip:+19728522631@192.65.79.223>;tag=d6de37c9-7561-4937-a8b9-0ca72644801a
To: <sip:+13149445469@us.telephony.goog>
Contact: <sip:9728522631@192.65.79.223:5061;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-389811/conversations/
/OR_02e58ba8-b22e-41a5-aa3d-d3e88a671c0c>;purpose=Goog-ContactCenter-Conversation

v=0
o=- 1738828058 1738828058 IN IP4 192.65.79.223
s=Asterisk
c=IN IP4 192.65.79.223
t=0
m=audio 21204 RTP/SAVP 0 8 101 107
a=rtptime:0 PCMU/8000
a=rtptime:8 PCMA/8000
a=rtptime:101 telephone-event/8000
a=fmtp:101 0-16
a=rtptime:107 opus/48000/2
a=fmtp:107 useinbandfec=1
a=ptime:20
a=sendrecv
a=ptime:20
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 call

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 29: GTP call

9 Oracle E-SBC Running configuration

Attached is the Oracle E-SBC running configuration.



Google_SIPREC_TLS_New1_2025_11_18_15_13_30.gz

10Summary of Tests and Results

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
SBC Configuration Verification					
1	SBC Configuration Verification	TLS connection setup. SBC initiates TLS connection with CES	Successful 4way handshake with Google CES. Validate the right certificates are being negotiated. SBC should be loaded with GTSR1 cert for Google. SBC should also send the certificate chain when sending its cert.	PASSED	TLS handshake is verified
2	SBC Configuration Verification	TCP Keep Alive. SBC will perform monitoring checks by attempting TCP Keep Alive to ensure Network Connectivity	Successful 3way handshake and thereafter termination	PASSED	
3	SBC Configuration Verification	TCP link is persistent. Establish calls, send multiple calls that should all use the same TCP transport connection	Persistent TCP connection, we should establish a single connection and multiplex all calls over that connection.	PASSED	
4	SBC Configuration Verification	Session Timer support. SBC should be initiator for the Session Refresh timer using Update or Re-Invite	every 900 secs the SBC should refresh the SIP session.	PASSED	Re-INVITE is sent for Session refresh
5	SBC Configuration Verification	SIP Header Manipulation (call-info header)	Validate if the Google requested header manipulation is present in the SIP INVITE. Ensure every SDP media has a label.	PASSED	

6	SBC Configuration Verification	*SBCs may need further Header manipulations based on SIP stack constraints. Verify required manipulation are added in SBC to support Google CES Example: FROM, TO header manipulations HOST part change in headers etc.,	All signaling in e.164 format	PASSED	
7	SBC Configuration Verification	SDES for SRTP. Configure the SDES parameters for crypto negotiation for the BYOT trunk	Validate the crypto is successfully negotiated and media is encrypted. All SBCs should support SDES for media encryption.	PASSED	
8	SBC Configuration Verification	DTLS for Media Encryption. Configure the DTLS parameters for crypto negotiation for the BYOT trunk, certificate for DTLS must be self-signed by the SBC.	Validate the crypto is successfully negotiated and media is encrypted. DTLS is not supported by Oracle and can be skipped.	NOT SUPPORTED	
Inbound					
9	Inbound	SIP OPTIONS. SBC send SIP options every 60 seconds	Verify SBC sends SIP OPTIONS every 60 seconds and responds with 200 OK	PASSED	
10	Inbound	Inbound call: Calling Party disconnects the call. Inbound siprec call, ensure recordings are present, disconnect call from calling party and confirm proper disconnect	Verify Call is established with audio and transcripts from both participants Verify call is disconnected properly	PASSED	

11	Inbound	Inbound call: Called Party disconnects the call. Inbound siprec call, ensure recording are present, disconnect call from called party and confirm proper disconnect	Verify Call is established with audio and transcripts from both participants Verify call is disconnected properly	PASSED	
12	Inbound	Long duration call- Outbound Call- 1 hour max. Long duration siprec call	Ensure siprec calls stay up for an hour, confirm transcripts are present for entire duration	PASSED	
13	Inbound	Long duration hold and resume (wait until session audit\session refresh occurs from DUT). Long duration siprec call, have the call placed on hold by agent, have call resume. Have customer place on hold then have call resume.	Call is connected, we have two active streams, confirm once a stream goes on hold, we receive corresponding signaling events, and that we no longer record transcripts for the participant on hold.	PASSED	
14	Inbound	Handling Error codes 603 decline. User A Calls PSTN A PSTN A rejects the incoming call	Verify SBC handles Call rejected properly	PASSED	
15	Inbound	Inbound call hold	Validate if media is	PASSED	Call recording

		scenarios. Call starts out inactive for both participants; session moves to active	present when expected, confirm signaling events modify sdp properly, once call is move to active validate media and transcripts		is deactivated using API command. Audio during the inactive state is not recorded.
--	--	--	---	--	--

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
16	Inbound	Inbound call hold scenarios. call starts out as active for both participants, session move to inactive, and transitions back to active	Validate if media is present when expected, confirm signaling events modify sdp properly, once call is moved to active validate media and transcripts	PASSED	Recording was not present after deactivating conversation and recording resumed after activating conversation via API
17	Inbound	Update. Validate that update sent prior to call establishment do not contain SDP	Validate that update prior to call establishment do not contain SDP as expected	PASSED	REINVITE message is sent from SBC every 900 seconds without SDP
18	Inbound	Update. Validate that updates post call establishment contain SDP to modify session	If SBC uses update to modify sessions, ensure SDP is included	NOT APPLICABLE	REINVITE message is sent from SBC every 900 seconds without SDP
19	Inbound	re-invites. Ensure re-invites that modify session include SDP	Ensure re-invites that modify session include SDP	PASSED	REINVITE is sent to Google CES as part of session refresh, hold scenarios
20	Inbound	Codec negotiation. Ensure that g711 u-law is preferred codec	Ensure we can prioritize g711 as preferred codec, note where SBC configures preferred codec	PASSED	
21	Inbound	3 way conference. Determine	Determine requirements,	PASSED	

		requirements, record all leg.	record all legs		
22	Inbound	CES cloud project setup. Establish CES cloud project, provision the project with a GTP phone number for access (Create conversations/participants on the fly through SIP headers)	Verify project is setup, functional test to confirm you can connect to the GTP access phone number	PASSED	
23	Inbound	CES cloud project setup. Establish CES cloud project, provision the project with a GTP phone number for access (Pre-creation of conversations/participants)	Verify project is setup, functional test to confirm you can connect to the GTP access phone number	NOT APPLICABLE	This test case is not applicable for call recording
24	Inbound	Consultative transfer. Consultative transfer from 1. PSTN > User1 > User2 2. PSTN > User1 > PSTN user2		PASSED	
25	Inbound	Blind transfer. Blind transfer from 1. PSTN > User1 > User2 2. PSTN > User1 > PSTN user2		PASSED	
26	Use documentation to build trunk using self service model			PASSED	
27	Inbound call	Call starts out	Inbound call hold	PASSED	

	hold scenarios using A-law as codec	inactive for both participants; session moves to active	scenarios using A-law as codec		
28	Inbound call: Called Party disconnects the call. using a a-law codec	Inbound siprec call, ensure recording are present , disconnect call from called party and confirm proper disconnect	Inbound call: Called Party disconnects the call. using a a-law codec	PASSED	
29	Long duration call- Outbound Call- 1 hour max using a-law codec	Long duration siprec call	Long duration call- Outbound Call- 1 hour max using a-law codec	PASSED	REINVITE messages are sent from SBC to Google CES every 15min (900 seconds)
30	Inbound call: Configure trunk in non-default region,	Confirm call is processed within the region for signaling and media that corresponds to the region trunk was provisioned in	"Verify Call is established with audio and transcripts from both participants	PASSED	Testing conducted in US region
31	Participant Labels test	Configure call info header to specify roles, ensure the media streams align	"Frist media stream HUMAN_AGENT role and	PASSED	When the roles are set to "HUMAN_AGENT" and "END_USER," Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/CES-389811/conversations/OR_0e39f42930cb0a5b0aba6241e11d8346?roles=HUMAN_AGENT, END_USER

					>;purpose=Goog-ContactCenter-Conversation the transcript shows the first media stream with the participation role as "HUMAN AGENT," followed by "END USER." It showed 5/10 attempts. The call-id in the call-info header is sent with hyphen sign
32	DTLS test			Not Supported	
33	Conference TEST	Conference call between PSTN and PBX users	Validate both-way audio	PASSED	Both-way audio for all users was present.
34	Validate Call recording			PASSED	