

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



Table of Contents

1	Audience	3
1.1	Introduction	3
1.1.1	TekVizion Labs	3
2	SIP Trunking Network Components	4
3	Hardware Components	5
4	Software Requirements	5
5	Google CES Certified Oracle SBC Versions	5
6	Features	5
6.1	Caveats and Limitations	5
7	Configuration	5
7.1	Configuration Checklist	5
7.2	IP Address Worksheet	6
7.3	Google CES API Configuration	7
7.4	Oracle E-SBC Configuration	8
7.4.1	Media Manager	8
7.4.2	Physical Interface	10
7.4.3	Network Interface	11
7.4.4	SIP Config	15
7.4.5	System-Config	16
7.4.6	SIP Monitoring	20
7.4.7	HTTP Server	20
7.4.8	Codec Policy	21
7.4.9	Translation Rules	21
7.4.10	Session Translation	22
7.4.11	Realm Config	22
7.4.12	Steering Pool	27
7.4.13	SDES Profile	28
7.4.14	Media Sec Policy	29
7.4.15	TLS – Certificate Record	31
7.4.16	TLS – TLS Profile	33
7.4.17	Session Timer	34
7.4.18	SIP Interface	34
7.4.19	Session Agent	39

7.4.20	Local Policy	44
7.4.21	SIP Manipulation	46
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 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 Call Recording with Oracle Enterprise Session Border Controller (E-SBC) Acme Packet 4600 SCZ9.3.0 GA(Build46) configuration.

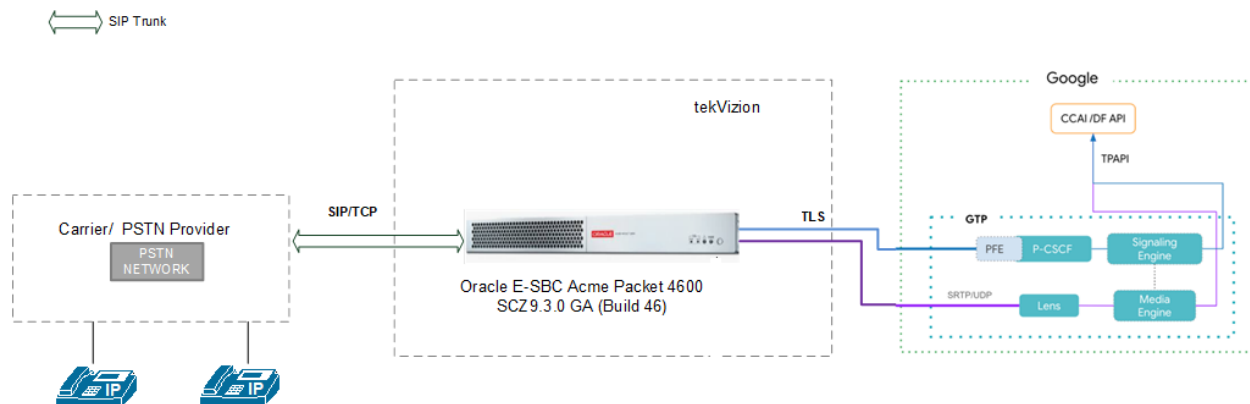


Figure 1: SIP Trunk Lab Reference Network.

The lab network consists of the following components.

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

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 SBC Versions

Table 1 – Google CES Certified Cisco UBE Version

Google CES Certified Cisco UBE Version	
Oracle SBC 4600	SC9.3.0 GA (Build46)

6 Features

6.1 Caveats and Limitations

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

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	
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 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

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)

Hint Rtcp ☐ enable

Algd Log Level NOTICE ▾

Mbcd Log Level NOTICE ▾

Options

Figure 2: Media Manager Configuration.

Configuration View Configuration

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 Signaling Bandwidth 10000000 (Range: 71000.10000000)

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 and PSTN Gateway as shown below.

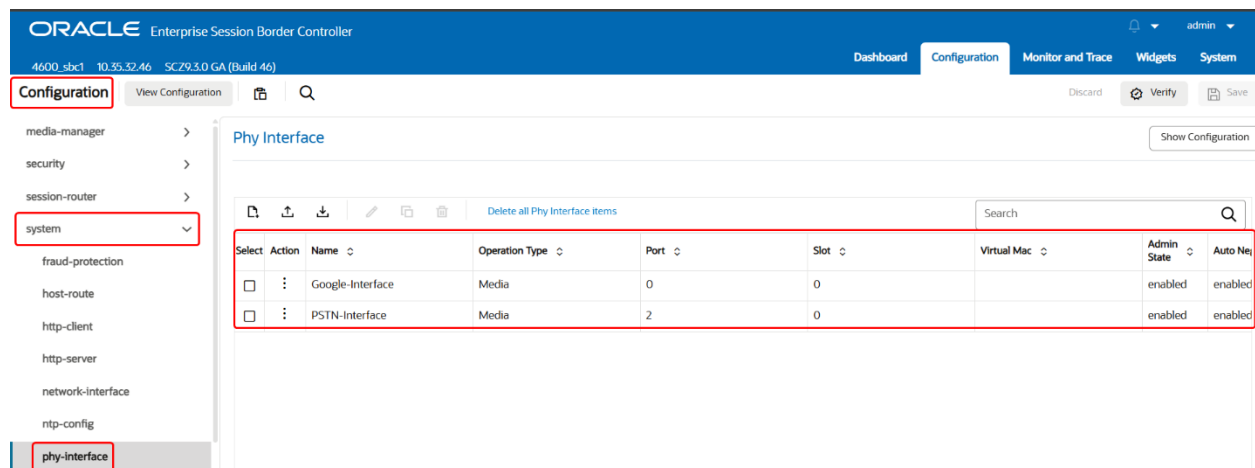


Figure 3: Physical Interfaces.

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

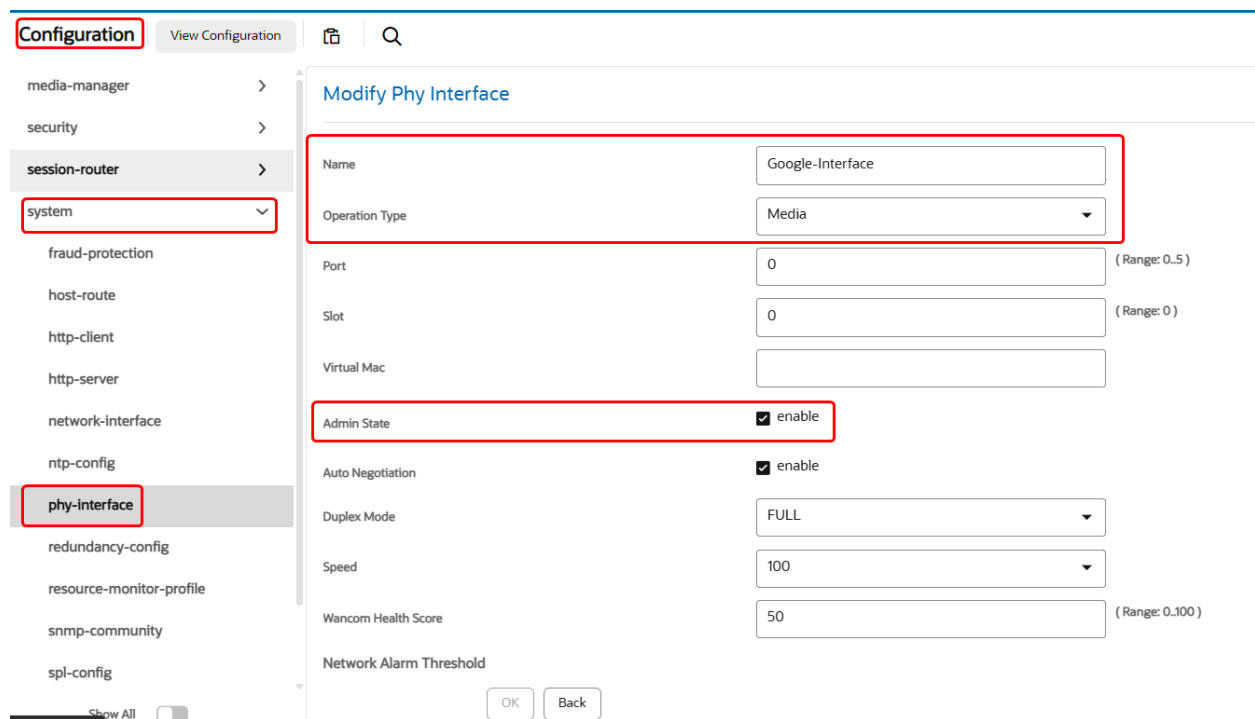


Figure 3.1: Physical Interface towards Google CES (Cont.)

- The interface designated towards PSTN Gateway are named as sOp2 (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

Wancom Health Score: 50 (Range: 0..100)

Network Alarm Threshold:

OK Back

Figure 3.2: 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

Configuration View Configuration

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

Network Interface

Delete all Network Interface items

Select	Action	Name	Sub Port Id	Description	Hostname	IP Address
☐	⋮	Google-Interface	0		sbc10.tekvizionlabs.com	192.65.
☐	⋮	PSTN-Interface	0			10.80.~ ~ ~

Figure 4: Network Interfaces.

- Configure Network interface towards Google CES 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
en-config

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 >
fraud-protection
host-route
http-client
http-server
network-interface
ntp-config
phy-interface
redundancy-config
resource-monitor-profile
snmp-community
en-config

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 tekvisionlabs.com

DNS Timeout 11 (Range: 1,999,999,999)

DNS Max Ttl 86400 (Range: 30,207,360)

Signalling 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 for 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: ▾

Pri Utility Addr

Sec Utility Addr

Netmask 255.255.255.0

Gateway 10.80

▼ 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 for 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)

Signalling Mtu

(Range: 0.576..4096)

HIP IP List

×

ICMP Address

×

Figure 4.5: Network Interface for PSTN Gateway (Cont.)

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 is titled 'Modify SIP Config'. The configuration is divided into two sections: 'State' and 'Options'. The 'State' section includes 'enable' (checked), 'Dialog Transparency' (checked), 'Home Realm ID' (Google), 'Egress Realm ID' (empty), 'Nat Mode' (None), 'Registrar Domain' (*), 'Registrar Host' (*), 'Registrar Port' (5060), 'Init Timer' (500), 'Max Timer' (4000), 'Trans Expire' (32), and 'Initial Inv Trans Expire' (0). The 'Options' section includes 'Invite Expire' (180), 'Session Max Life Limit' (0), 'Enforcement Profile' (empty), 'Emergency Dscp Profile' (empty), 'Red Max Trans' (10000), and 'Options' (max-udp-length=0 x).

Field	Value	Range
State	☒	
Dialog Transparency	☒	
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	
Enforcement Profile		
Emergency Dscp Profile		
Red Max Trans	10000	(Range: 0..50000)
Options	max-udp-length=0 x	

Figure 5: SIP-Config.

The screenshot shows the 'Configuration' menu on the left with 'session-router' expanded and 'sip-config' selected. The main area is titled 'Modify SIP Config'. The configuration is divided into two sections: 'SIP Message Len' and 'Options'. The 'SIP Message Len' section includes 'SIP Message Len' (65535). The 'Options' section includes 'Enum Sag Match' (enable), 'Extra Method Stats' (enable), 'Extra Enum Stats' (enable), 'Registration Cache Limit' (0), 'Register Use To For Lp' (enable), 'Refer Src Routing' (enable), 'Atcf Stn Sr' (empty), 'Atcf Pst Dn' (empty), 'Atcf Route To Scas' (enable), 'Eatf Stn Sr' (empty), 'Sag Lookup On Redirect' (enable), and 'Set Disconnect Time On Bye' (enable).

Field	Value	Range
SIP Message Len	65535	(Range: 0..65535)
Enum Sag Match	☐	
Extra Method Stats	☐	
Extra Enum Stats	☐	
Registration Cache Limit	0	(Range: 0..999999999)
Register Use To For Lp	☐	
Refer Src Routing	☐	
Atcf Stn Sr		
Atcf Pst Dn		
Atcf Route To Scas	☐	
Eatf Stn Sr		
Sag Lookup On Redirect	☐	
Set Disconnect Time On Bye	☐	

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

sip-config

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 Pani

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

sip-config

sip-feature

sip-interface

sip-manipulation

sip-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)

Mag Hold For Loc Info

0

(Range: 0,30)

Npki 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 Sntp 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

No monitor collector to display. Please add.

Add

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.

Add

Upload

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.

The screenshot shows the 'Modify SIP Monitoring' configuration page. The left sidebar has a tree view with 'Configuration' selected, followed by 'session-router' and 'sip-monitoring'. The main panel has the title 'Modify SIP Monitoring' and the following settings:

- Match Any Filter: ☒ enable
- State: ☒ enable
- Short Session Duration: 0 (Range: 0.999999999)
- Monitoring Filters: + x
- Interesting Events: No interesting event to display. Please add. (Add button)
- Trigger Window: 30 (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 'Modify HTTP Server' configuration page. The left sidebar has a tree view with 'Configuration' selected, followed by 'system' and 'http-server'. The main panel has the title 'Modify HTTP Server' and the following settings:

- Name: wancom0
- State: ☒ enable
- Realm: (empty)
- IP Address: (empty)
- HTTP State: ☒ enable
- HTTP Port: 80 (Range: 1.65535)
- HTTP Strict Transport Security Policy: ☐ enable
- HTTPS State: ☐ enable
- HTTPS Port: 443 (Range: 1.65535)
- HTTP Interface List: REST x, GUI x

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 left sidebar containing a tree view. The 'media-manager' section is expanded, and 'codec-policy' is selected. The main content area is titled 'Modify Codec Policy Entries'. A red box highlights the configuration for 'Google'. The configuration includes:

- Name: Google
- Allow Codecs: PCMU x, PCMA x
- Add Codecs On Egress: PCMU x, PCMA x
- Order Codecs: PCMU x, PCMA x
- Packetization Time: 20
- Force Ptime: ☐ enable
- Secure Dtmf Cancellation: ☐ enable
- Dtmf In Audio: disabled
- Tone Detection:
- 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.

The screenshot shows the Configuration page with the left sidebar containing a tree view. The 'session-router' section is expanded, and 'translation-rules' is selected. The main content area is titled 'Translation Rules'. A table lists the translation rules, with two rules highlighted in red:

Select	Action	Id	Description	Input Header Type	Input Header Value	Output Header Type	Output Header Value
☐	add	adplus_called-header	add	called-header	*(0)\$.*\$	called-header	\$01+\$02
☐	add	adplus_request-uri	add	request-uri	*(0)\$.*\$	request-uri	\$01+\$02
☐	replace	mapping_name	replace	none	*(3500)\$.*\$	none	\$02\$425999\$02
☐	delete	removeplus_called-header	delete	called-header	*(*)\$.*\$	called-header	\$1\$2
☐	delete	removeplus_p-asserted-id-header	delete	p-asserted-id-header	*(*)\$.*\$	p-asserted-id-header	\$1\$2
☐	delete	removeplus_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.

The screenshot shows the management console interface. On the left, the 'Configuration' menu is expanded, and 'session-translation' is selected. The main panel displays the 'Session Translation' configuration page. A table lists the translation rules:

Select	Action	Id
☐	:	addplus1
☐	:	removeplus1

Figure 11: Session Translation towards Google CES.

7.4.11 Realm Config

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

The screenshot shows the management console interface. On the left, the 'Configuration' menu is expanded, and 'realm-config' is selected. The main panel displays the 'Realm Config' configuration page. A table lists the realm configurations:

Select	Action	Identifier	Description	Addr Prefix	Network Interfaces	Media Realm List	Min In Realm	Min In Network
☐	:	Google		0.0.0.0	Google-Interface:0.4		enabled	enabled
☐	:	PSTN		0.0.0.0	PSTN-Interface:0.4		enabled	enabled

Figure 12: Realm Config towards Google CES.

Configuration View Configuration  

media-manager 

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security >

session-router >

system >

Modify Realm Config

Identifier

Description

Addr Prefix

Network Interfaces

Media Realm List

Mm In Realm ☒ enable

Mm In Network ☒ enable

Mm Same Ip ☒ enable

QoS Enable ☒ enable

Max Bandwidth (Range: 0.999999999)

Max Priority Bandwidth (Range: 0.999999999)

Parent Realm

DNS Realm

Media Policy

Figure 13: Realm Config towards Google CES

Configuration View Configuration  

media-manager 

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security >

session-router >

system >

Modify Realm Config

Media Sec Policy

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 13.1: Realm Config towards Google CES (Cont.)

Configuration View Configuration  

media-manager 

codecs-policy

media-manager

media-policy

realm-config

steering-pool

Modify Realm Config

Out Session Translations

Select	Action	Out Session Translation Id	State
☐		addplus1	enabled

Figure 13.2: Realm Config towards Google CES (Cont.)

The screenshot shows the 'Modify Realm Config' page for the 'realm-config' entity. The left sidebar lists various configuration categories, with 'realm-config' selected. The main area displays a list of configuration parameters, each with a value field and a range indicator. The following table summarizes the visible configurations:

Parameter	Value	Range
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 13.3: Realm Config towards Google CES (Cont.)

The screenshot shows the 'Modify Realm Config' page for the 'realm-config' entity. The left sidebar lists various configuration categories, with 'realm-config' selected. The main area displays a list of configuration parameters, each with a value field and a range indicator. The following table summarizes the visible configurations:

Parameter	Value	Range
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 13.4: 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

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 (Range: -1.2147483647)

Initial Guard Timer (Range: -1.2147483647)

Subsq Guard Timer (Range: -1.2147483647)

TCP Flow Time Limit (Range: -1.2147483647)

TCP Initial Guard Timer (Range: -1.2147483647)

TCP Subsq Guard Timer (Range: -1.2147483647)

SIP Isup Profile

QoS Constraint

Figure 13.5: Realm Config towards Google CES (Cont.)

- Realm Config for PSTN Gateway is shown below.

Configuration View Configuration

media-manager

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security >

session-router >

system >

Modify Realm Config

Identifier

Description

Addr Prefix

Network Interfaces

Media Realm List

Mm In Realm ☒ enable

Mm In Network ☒ enable

Mm Same Ip ☒ enable

QoS Enable ☒ enable

Max Bandwidth (Range: 0.999999999)

Max Priority Bandwidth (Range: 0.999999999)

Figure 14: Realm Config for PSTN Gateway.

Configuration

View Configuration

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Realm Config

Media Sec PolicyRTP

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

In Session Translations

No in session translation list to display. Please add.

Add

Out Session Translations

Select

Action

Out Session Translation Id

State

:

removeplus1

enabled

Figure 14.1: Realm Config for 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

In ManipulationId

Out ManipulationIdPSTNOUTBOUND

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 14.2: Realm Config towards for 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

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

Codec ManIP In Realm: ☐ enable

Codec ManIP In Network: ☒ enable

Figure 14.3: Realm Config towards for 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 for PSTN Gateway are shown below.

Configuration View Configuration

media-manager

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security

Steering Pool

Delete all Steering Pool Items

Select	Action	IP Address	Start Port	End Port	Realm ID	Network Interface	Port Allocation Strategy
☐		10.80	50000	59999	PSTN	PSTN-Interface.0.4	mixed
☐		192.65	20000	39999	Google	Google-Interface.0.4	mixed

Figure 15: Steering Pool.

- Steering Pool Configuration towards Google CES is shown below.

Configuration View Configuration

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

Modify Steering Pool

IP Address: 192.65.1

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 (Cont.)

- Steering Pool Configuration for 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 Steering Pool

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 (Cont.)

7.4.13 SDES Profile

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

Configuration View Configuration

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

Sdes Profile

Select	Action	Name	Crypto List	Srtp Auth	Srtp Encrypt	SrTCP Encrypt	Mki	Egress Offer Format
☐	:	SDES	AES_CM_128_HMAC_SHA1_80	enabled	enabled	enabled	disabled	same-as-ingress

Figure 16: SDES Profile for TLS.

Configuration View Configuration

security

admin-security

auth-params

authentication

authentication-profile

cert-status-profile

certificate-record

factory-accounts

ike

ipsec

local-accounts

media-security

media-sec-policy

sdes-profile

sipura-profile

password-policy

security-config

Modify Sdes Profile

Name: SDES

Crypto List: AES_CM_128_HMAC_SHA1_80 x

Srtp Auth: ☒ enable

Srtp Encrypt: ☒ enable

SrTCP Encrypt: ☒ enable

Mki: ☐ enable

Egress Offer Format: same-as-ingress

Use Ingress Session Params:

Options:

Key:

Salt:

Srtp Rekey On Re Invite: ☐ enable

Lifetime: 0 (Range: 0,20..48)

Figure 16.1: 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.

Configuration View Configuration

security

admin-security

auth-params

authentication

authentication-profile

cert-status-profile

certificate-record

factory-accounts

ike

ipsec

local-accounts

media-security

media-sec-policy

Media Sec Policy

select Action Name Pass Through Options

☐	:	RTP	disabled	
☐	:	SRTP	disabled	

Figure 17: Media Security Policy

Configuration View Configuration

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

password-policy

Modify Media Sec Policy Entries

Name: RTP

Pass Through: ☐ enable

Options:

Inbound

Profile:

Mode: rtp

Protocol: none

Hide Egress Media Update: ☐ enable

Outbound

Profile:

Mode: rtp

Protocol: none

Figure 17.1: Media Security Policy for RTP (Cont.)

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

Configuration View Configuration

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

password-policy

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 17.2: Media Security Policy for SRTP.

7.4.15 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

☒	☐	sbc10	US	Texas	Plano	tekvisionlabs	tekvision	sbc10.tekvisionlabs.com
☐	☐	Edit	US	MA	Burlington	Engineering		
☐	☐	Copy						
☐	☐	Delete						
☐	☐	Generate						
☐	☐	Import						

Figure 18.1: Import Certificate Record for Oracle E-SBC

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

The screenshot shows a configuration interface. On the left, a sidebar contains a tree view with the following items: media-manager, security (highlighted), authentication-profile, certificate-record (highlighted), tls-global, tls-profile, session-router, and system. The main area is titled 'Modify Certificate Record'. It contains a form with the following fields: Name (GTS_Root1), Country (US), State (MA), Locality (Burlington), Organization (Engineering), Unit (empty), Common Name (empty), Key Algor (rsa), Digest Algor (sha256), Ecdsa Key Size (p256), and Cert Status Profile List (empty).

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 a dialog box titled 'Import Certificate'. It has a blue header bar with a close button. The main area contains the following elements: a 'Format' dropdown menu set to 'try-all'; an 'Import Method' section with two radio buttons, 'File' (selected) and 'Paste'; and a 'Certificate File' section with an 'Upload' button and the text 'No file selected.'

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.

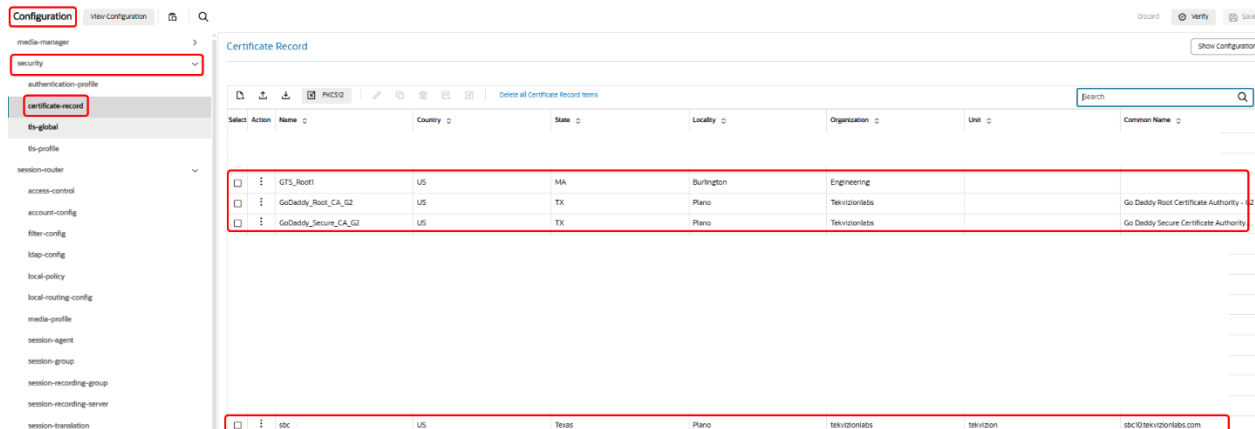


Figure 18.4: Certificate Records.

7.4.16 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.

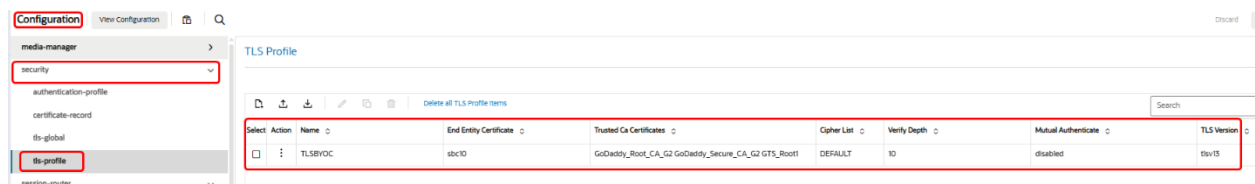


Figure 19: TLS Profile.

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

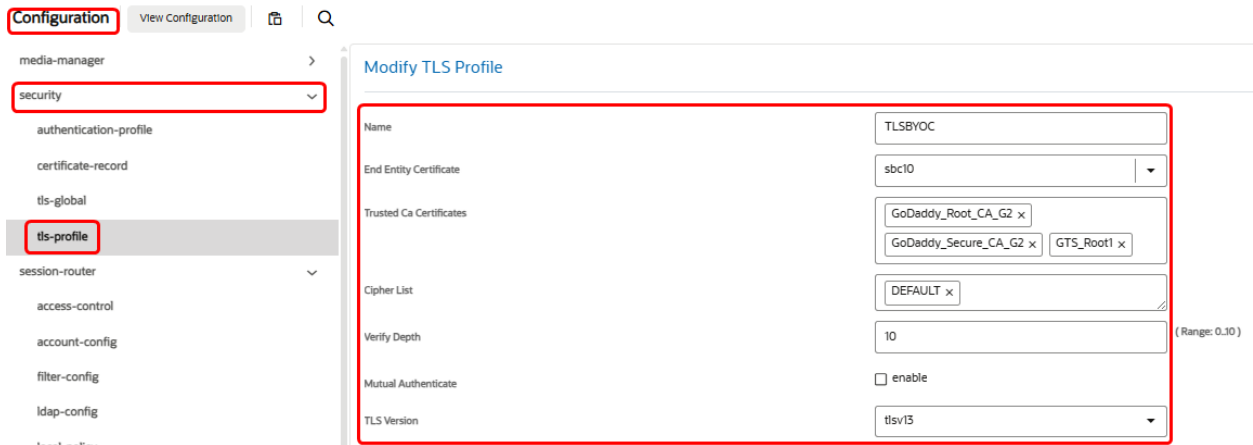


Figure 19.1: TLS Profile

7.4.17 Session Timer

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

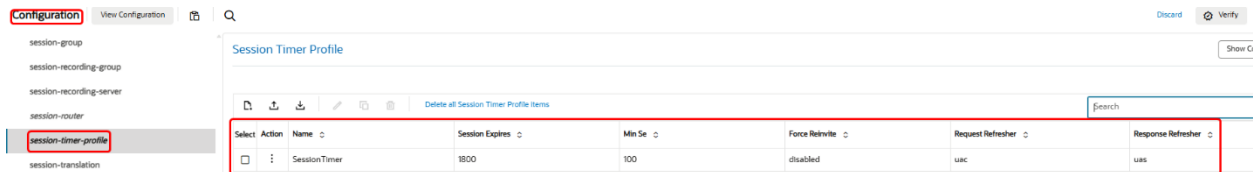


Figure 20: Session Timer.

7.4.18 SIP Interface

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

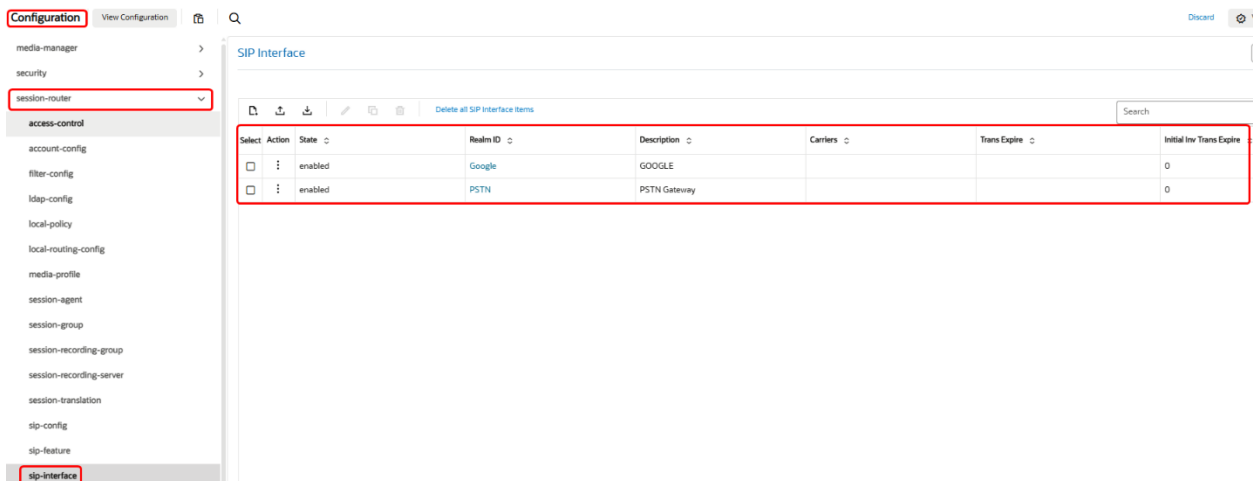


Figure 21: SIP Interface.

- Create SIP interface towards PSTN Gateway 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: PSTN

Description: PSTN & OnPrem PBX

SIP Ports

Select	Action	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous
☐		10.80	5060	TCP		agents-only

Figure 21.1: SIP Interface for PSTN

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: [dropdown]

Redirect Action: [dropdown]

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

Figure 21.2: SIP Interface for PSTN (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 21.3: SIP Interface for PSTN (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: 0.999999999)
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	

Add CND Profile in Mico

Figure 21.4: SIP Interface for PSTN (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

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 (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
☐		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 Payload101(Range: 96..127)

Rfc2833 Modetransparent

Response Map

Local Response Map

Sec Agree Feature☐ enable

Enforcement Profile

Emergency Dscp Profile

TCP Keepalivenabled

Add SDP Inviteboth

Add SDP In Msg

P Early Media Headerdisabled

P Early Media Direction

Add SDP ProfilesPCMU 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 ProfileSessionTimer

Session Recording Server

Session Recording Required☐ enable

Service Tag

Reg Cache Route☐ enable

Diversion Info Mapping Modenone

Atcf Icsi Match

SIP Recursion Policy

Asymmetric Preconditions☐ enable

Asymmetric Preconditions Modesend-with-nodelay

Sm Icsi Match For Invite

Sm Icsi Match For Message

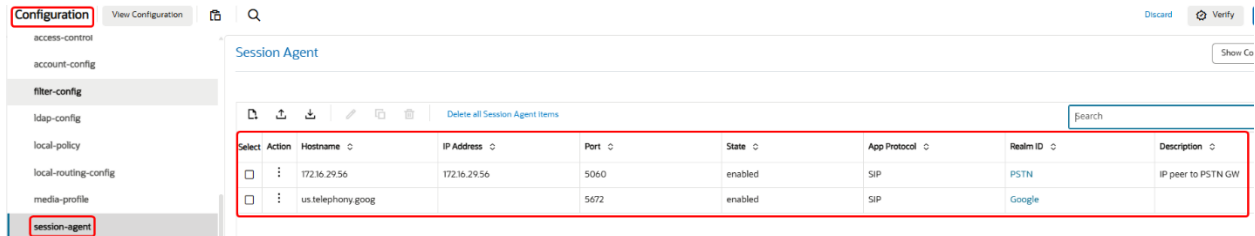
S8hr Profile

Ringback Triggernone

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

7.4.19 Session Agent

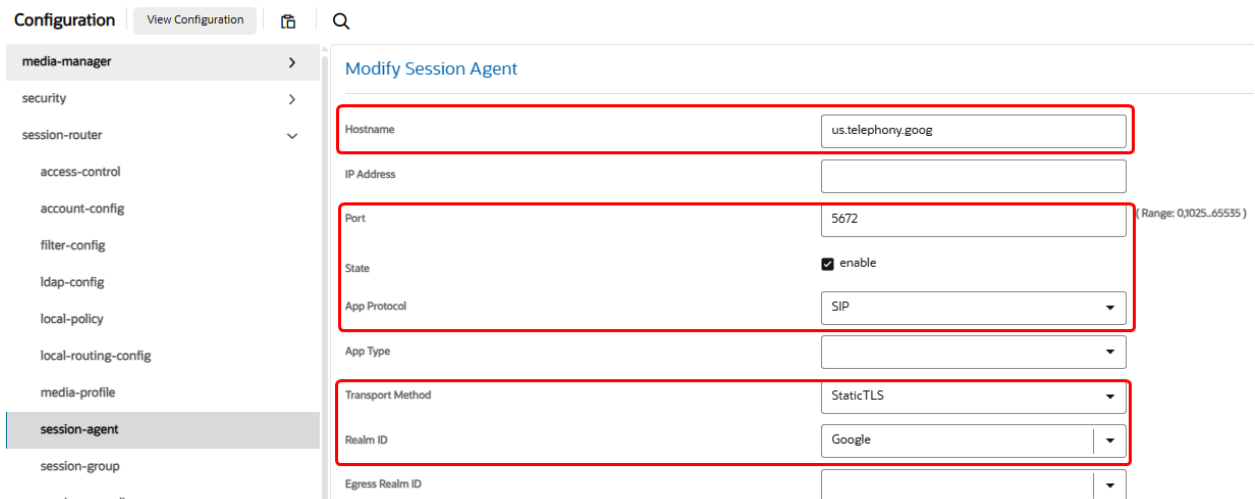
- Session-agents are config elements which are trusted agents which can send/receive traffic from the SBC with direct access to trusted data path.
- Navigate to **Configuration** ▢ **session-router** ▢ **session-agent**.
- Configure Session Agent for Google CES as shown below.



The screenshot shows the 'Session Agent' configuration page. On the left is a navigation menu with 'session-agent' highlighted. The main area displays a table of session agents. A red box highlights the table content.

Select	Action	Hostname	IP Address	Port	State	App Protocol	Realm ID	Description
☐		172.16.29.56	172.16.29.56	5060	enabled	SIP	PSTN	IP peer to PSTN GW
☐		us.telephony.goog		5672	enabled	SIP	Google	

Figure 23: Session Agent



The screenshot shows the 'Modify Session Agent' form. The left navigation menu has 'session-agent' highlighted. The form fields are as follows:

- Hostname: us.telephony.goog
- IP Address: (empty)
- Port: 5672 (Range: 0;1025..65535)
- State: ☒ enable
- App Protocol: SIP
- App Type: (empty)
- Transport Method: StaticTLS
- Realm ID: Google
- Egress Realm ID: (empty)

Figure 23.1: Session Agent 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

Modify Session Agent

Loose Routing ☒ enable

Response Map

Ping Method OPTIONS

Ping Interval 60

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 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
☐	⋮	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

Kpm1 Interworking

Kpm12833 lwf On Halrpin

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 PSTN as shown below

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

slip-config

slip-features

Modify Session Agent

Hostname: 172.16.1

IP Address: 172.16.1

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 PSTN

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

slip-config

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 24.1: Session Agent for PSTN (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

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..327)

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 PSTN (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

Kpml Interworking

inherit

Kpml2833 Iwf 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 Reinvite

enable

Send TCP Fin

enable

SIP Recursion Policy

Sm Icsi Match For Invite

Sm Icsi Match For Message

Ringback Trigger

none

Figure 24.3: Session Agent for PSTN (Cont.)

7.4.20 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 and PSTN Gateway as shown below.

Select	Action	From Address	To Address	Source Realm	Description	Activate Time	Deactivate Time	State
☐	:	*	*	Google	PBX user to PSTN			enabled
☐	:	*	97259	Google	PSTN_to_Google			disabled
☐	:	*	9728522626	Google	PSTN_to_Webex			enabled
☐	:	*	*	PSTN	GOOGLE TO PSTN			enabled

Figure 25: Local Policy

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

From Address: * x

To Address: 9728522626 x

Source Realm: Google x

Description: PSTN_to_Google

Policy Priority: none

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

Figure 25.1: Local Policy routing from PSTN to Google

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

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 25.2: Local Policy routing Towards PSTN Gateway (Cont.)

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

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

Modify Local Policy Entries

From Address

* x

To Address

* x

Source Realm

Google x

Description

Google to PSTN

Policy Priority

none

Policy Attributes

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

Figure 25.3: Local Policy routing Towards 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

Modify Local policy / policy attribute

Next Hop: 172.16.29.56

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 25.4: Local Policy routing Towards PSTN Gateway (Cont.)

7.4.21 SIP Manipulation

- Navigate to **Configuration** > **session-router** > **sip-manipulation**.
- Configure SIP manipulation towards 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-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation

Modify SIP Manipulation

Name: GoogleManipulation

Description: Manipulation on google side

Split Headers:

Join Headers:

CfgRules

Action	Name	Element Type
:	changeRequiri	header-rule
:	changeFromIP	header-rule
:	changeToURIhost	header-rule
:	AddCallInfoHeader	header-rule
:	changelocalport	header-rule
:	deltransport	header-rule
:	delete_callinfo	header-rule

Figure 26: SIP Manipulation towards Google CES.

- Add a header-rule 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 Manipulation

Name: GoogleManipulation
Description: Manipulation on google side
Split Headers:
Join Headers:

CfgRules

Add

Action	Name	Element Type
header-rule		header-rule
mime-rule		header-rule
mime-isup-rule		header-rule
mime-sdp-rule		header-rule
:	changelocalport	header-rule
:	deltransport	header-rule
:	delete_callinfo	header-rule

Figure 26.1: SIP Manipulation towards Google CES (Cont.)

- 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

Add

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

Figure 26.2: 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-translation

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

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	AddURI
Parameter Name	Request-URI
Type	uri-user ▾
Action	replace ▾
Match Val Type	any ▾
Comparison Type	pattern-rule ▾
Match Value	
New Value	"+13149445469"

Figure 26.4: 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

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-rule

Modify Sip manipulation / header rule

Name: changeFromIP

Header Name: FROM

Action: manipulate

Comparison Type: pattern-rule

Msg Type: request

Methods: INVITE x

Match Value:

New Value:

CfgRules

Action	Name	Element Type
⋮	changeIP	element-rule
⋮	changetofo	element-rule
⋮	changefromuser	element-rule

Figure 26.5: 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 26.6: SIP Manipulation towards Google CES – Change FROM header uri-host.

- Match value : To:sips:"us.telephony.goog":5672;trasnairport=tls
- New Value : To:<sips:"+ 1314944XXXX@us.telephony.goog":5672;trasnairport=tls>

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

Modify Sip manipulation / header rule / element rule

Name	changetofofor
Parameter Name	
Type	uri-user
Action	replace
Match Val Type	any
Comparison Type	case-sensitive
Match Value	
New Value	

Figure 26.7: SIP Manipulation towards Google CES – Change FROM header uri-user.

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	changefromuser
Parameter Name	From
Type	uri-user
Action	add
Match Val Type	any
Comparison Type	pattern-rule
Match Value	
New Value	"*19728522631"

Figure 26.8: 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: changeToURlhost
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
⋮	changeURlhost	element-rule
⋮	changeToURlhost	element-rule

Figure 26.9: 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: changeURlhost
Parameter Name:
Type: uri-host
Action: replace
Match Val Type: any
Comparison Type: pattern-rule
Match Value:
New Value: "us.telephony.goog"

Figure 26.10: SIP Manipulation towards Google CES – Change TO header uri-host.

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

changeToURihost

Parameter Name

To

Type

uri-user

Action

replace

Match Val Type

any

Comparison Type

case-sensitive

Match Value

New Value

"+13149445469"

Figure 26.11: 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 26.12: SIP Manipulation towards Google CES – Add Call-Info.

- 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.goog)(.*)\$
New Value	\$1+\$3

Figure 26.13: 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

Action	Name	Element Type
⋮	chnagetransportnumber	element-rule

Figure 26.14: 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
session-group
session-recording-group
session-recording-server
session-translation

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 26.15: 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 x

Match Value:
New Value:

CfgRules

Action	Name	Element Type
delparam		element-rule

Figure 26.16: 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 26.17: SIP Manipulation towards Google CES Cont. – Delete Transport parameter.

Manipulation for Inbound messages from Google CES

- A call from Google (or another provider) is sent toward PSTN Gateway, both the Request-URI, To and REFER-To headers are rewritten so that Agent sees the request as being directly addressed to it.

The screenshot shows a web-based configuration interface. On the left is a sidebar menu with various configuration categories. The 'session-router' category is expanded, and 'sip-manipulation' is selected. The main area is titled 'Modify SIP Manipulation'. It contains several input fields: 'Name' (PSTNOUTBOUND), 'Description' (PSTNOUTBOUND), 'Split Headers', and 'Join Headers'. Below these is a 'CfgRules' section with a table of rules. The table has three columns: 'Action', 'Name', and 'Element Type'. Three rules are listed: 'changereqURI', 'changeTo', and 'ReferTo', all of which are 'header-rule' type.

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

Figure 27: SIP Manipulation towards PSTN Gateway

- Create a Request URI 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: changereqURI

Header Name: Request-URI

Action: manipulate ▾

Comparison Type: pattern-rule ▾

Msg Type: any ▾

Methods: INVITE × REFER ×

Match Value:

New Value:

CfgRules

Add ▾     

Action	Name	Element Type
⋮	Changerequiuser	element-rule

Figure 27.1: SIP Manipulation towards PSTN Gateway – 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

session-recording-group

session-recording-server

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

Modify Sip manipulation / header rule / element rule

Name: Changerequiuser

Parameter Name: Request-URI

Type: uri-user ▾

Action: replace ▾

Match Val Type: any ▾

Comparison Type: pattern-rule ▾

Match Value:

New Value: "9728522625"

Figure 27.2: SIP Manipulation towards PSTN Gateway – Request URI (Cont.)

- Create 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

Header Name

Action

Comparison Type

Msg Type

Methods

Match Value

New Value

CfgRules

Add ▾     

Action	Name	Element Type
⋮	changetouser	element-rule

Figure 27.3: SIP Manipulation towards PSTN Gateway – 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	changetouser
Parameter Name	changetouser
Type	uri-user
Action	replace
Match Val Type	any
Comparison Type	pattern-rule
Match Value	
New Value	"9728522625"

Figure 27.4: SIP Manipulation towards PSTN Gateway – To Header (Cont.)

- Create a REFER-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	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

Figure 27.5: SIP Manipulation towards PSTN Gateway – Refer-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

changereferertouser

Parameter Name

changereferertouser

Type

uri-user ▾

Action

replace ▾

Match Val Type

any ▾

Comparison Type

pattern-rule ▾

Match Value

New Value

"9728522625"

Figure 27.6: SIP Manipulation towards PSTN Gateway – Refer-To Header (Cont.)

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/CES-389811/conversations/OR_QAZ

Hexa Encoded :

687474703A2F2F6469616C6F67666C6F772E676F676C65617069732E636F6D2F763262657461312F70726F6A656374732F636361692D3338393831312F636F6E766572736174696F6E732F4F525F51415A

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	AddUIIheader
Header Name	User-to-User
Action	add
Comparison Type	case-sensitive
Msg Type	any
Methods	INVITE x
Match Value	
New Value	"687474703A2F2F6469616C6F67666C6F772E676F676C65617069732E636F6D2F763262657461312F70726F6A656374732F636361692D3338393831312F636F6E766572736174696F6E732F4F525F51415A"

CfgRules

No rules to display. Please add.

Add

Figure 28: SIP Manipulation towards Google CES – UII Header

1 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=z9hG4bKqtf9nq103ov0tbubt2n0
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 0
m=audio 20910 RTP/SAVP 0 101
c=IN IP4 192.65.79.223
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=label:234881075
a=sendrecv
a=crypto:1 AES_CM 128_HMAC_SHA1_80 inline:1ZbR91HLKuYJ8T4ejRWE1rWkdq42ket0XmrtM8Jk
a=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:aUYfqWeUmQFDSecQ65SVe4muW9bdvNCmuqpaId

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 29: 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: FFBX-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 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=maxptime:20
a=sendrecv
a=ptime:20
a=crypto:1 AES_CM 128_HMAC_SHA1_80 inline:ydaFiGf4WVGacrEmG0HNx9d1V8cW0G0fdwG0x0PS

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 30: GTP call

2 Oracle E-SBC Running configuration

Attached is the Oracle E-SBC running configuration.



Google_Agent_All_2025_11_13_14_47_32.gz

3 Summary of Tests and Results

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
35	UI header test	Use the UI header as opposed to call-info header to send conversation id	Call should process as normal, and recording under conversation ID derived from UI header as opposed to call-info	PASSED	Calls gets successfully connected to Live agent when using UI 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		PASSED	Call was connected successfully with live agent and when performing conversation "Speak to an agent", a new

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
		+13149445469, "speak to an agent", +1-972-852-2626 should then ring and get connected as the agent			INVITE was sent from Google to transfer to an agent and call gets connected successfully with both-way audio.
39	UUI headers	Call goes to virtual agent, say "end the call", validate that the SIP BYE has a UUI header Make calls to +13149445469, "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 972-852-2626. Make calls to +13149445469, "send a sip refer", SIP REFER should be received with refer to set to 972-852-2626		PASSED	REFER request & transfer is successful.