

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



Table of Contents

1	Audience	4
1.1	Introduction	4
1.1.1	TekVizion Labs	4
2	SIP Trunking Network Components	4
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	11
7.4.3	Network Interface	12
7.4.4	SIP Config	15
7.4.5	System-Config	17
7.4.6	SIP Monitoring	19
7.4.7	HTTP Server	20
7.4.8	Codec Policy	20
7.4.9	Translation Rules	21
7.4.10	Session Translation	21
7.4.11	Session Recording Server	23
7.4.12	Realm Config	23
7.4.13	Steering Pool	32
7.4.14	SDES Profile	33
7.4.15	Media Sec Policy	34
7.4.16	TLS – Certificate Record	36

7.4.17	TLS – TLS Profile	40
7.4.18	Session Timer	40
7.4.19	SIP Interface	41
7.4.20	Session Agent	48
7.4.21	Local Policy	57
7.4.22	SIP Manipulation	59
8	SIP INVITE To GOOGLE CES	67
8.1	SIP INVITE for SIPREC call	67
8.2	SIP INVITE for GTP call	67
9	Oracle E-SBC Running configuration file	68
10	Summary of Tests and Results	69

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 (Build 46) configuration.

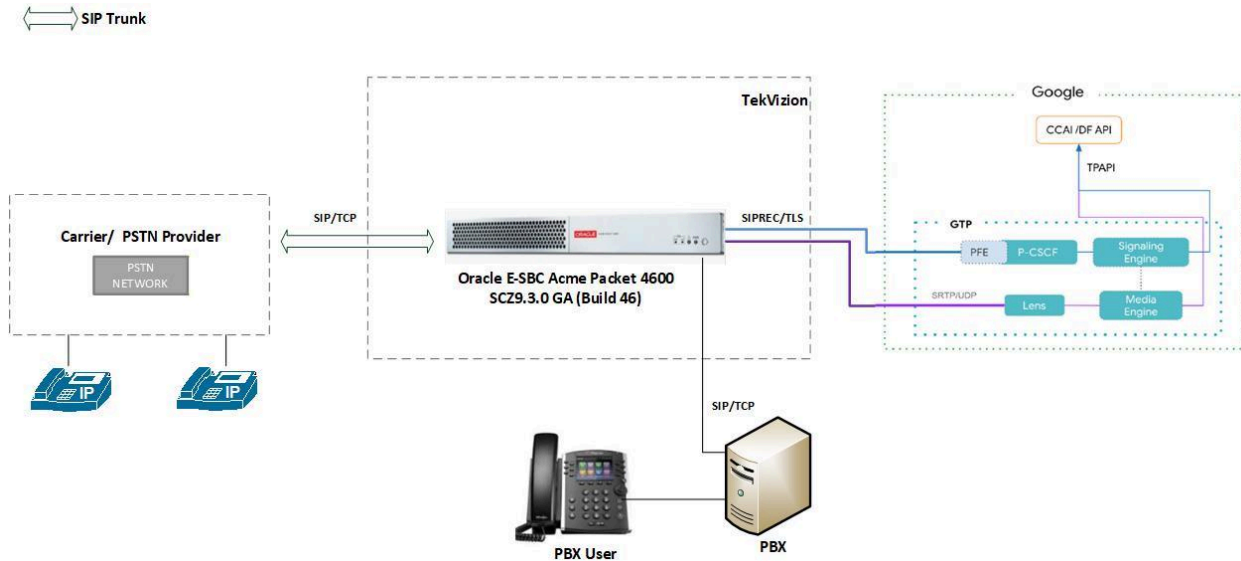


Figure 1: SIP Trunk Lab Reference Network

The lab network consists of the following components.

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

3 Hardware Components

- Oracle E-SBC Acme Packet 4600

4 Software Requirements

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

5 Google CES Certified Oracle E-SBC Versions

Table 1 – Google CES Certified Oracle E-SBC Version

Google CES Certified Oracle E-SBC Version	
Oracle E-SBC 4600	SCZ9.3.0 GA (Build46)
Oracle E-SBC 3900	SCZ9.3.0 GA (Build46)
Oracle E-SBC 3900	SCZ8.4.0 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 for troubleshooting Google CES API configuration for Call recording.

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

7.4 Oracle E-SBC Configuration

The following is the example configuration of Oracle E-SBC for Google CES Call Recording.

7.4.1 Media Manager

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

The screenshot shows the configuration page for the Media Manager. The 'Configuration' tab is selected, and the 'media-manager' configuration is chosen from the left-hand menu. The 'State' is set to 'enable'. The configuration parameters are as follows:

Parameter	Value	Range
Flow Time Limit	86400	(Range: 0.999999999)
Initial Guard Timer	300	(Range: 0.999999999)
Subsq Guard Timer	300	(Range: 0.999999999)
TCP Flow Time Limit	86400	(Range: 0.999999999)
TCP Initial Guard Timer	300	(Range: 0.999999999)
TCP Subsq Guard Timer	300	(Range: 0.999999999)
Hint Rtcp	<input type="checkbox"/> enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	
Options		
Red Max Trans	10000	(Range: 0.50000)
Red Sync Start Time	5000	(Range: 0.4294967295)
Red Sync Comp Time	1000	(Range: 0.4294967295)

Figure 2: Media Manager Configuration

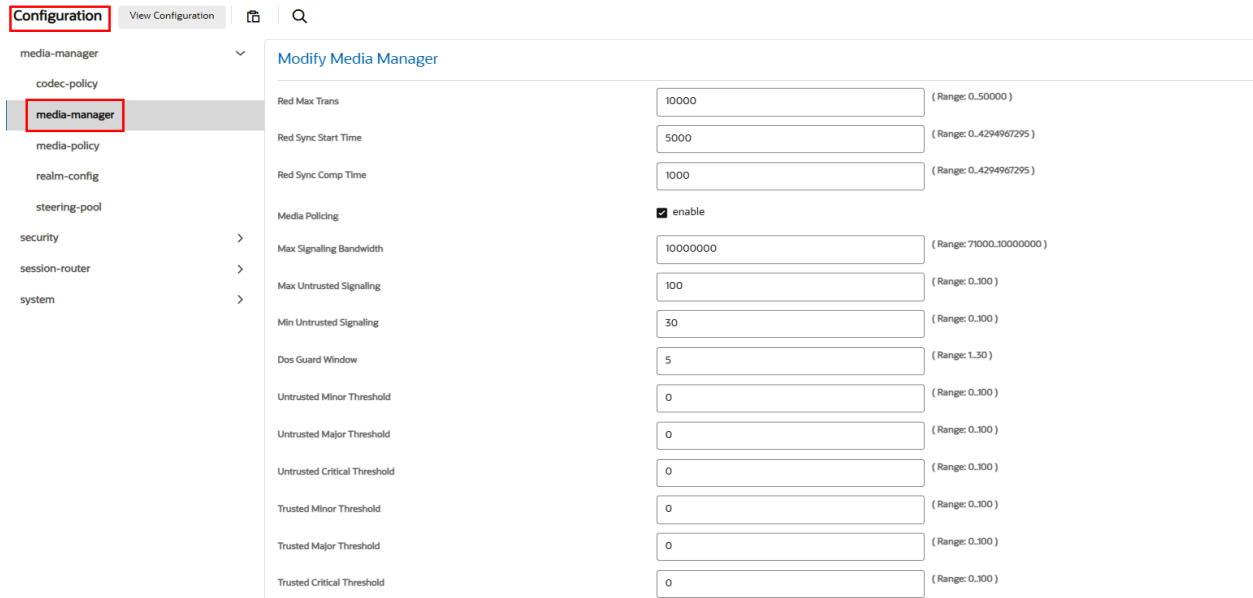


Figure 3: Media Manager Configuration (Cont.)

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.

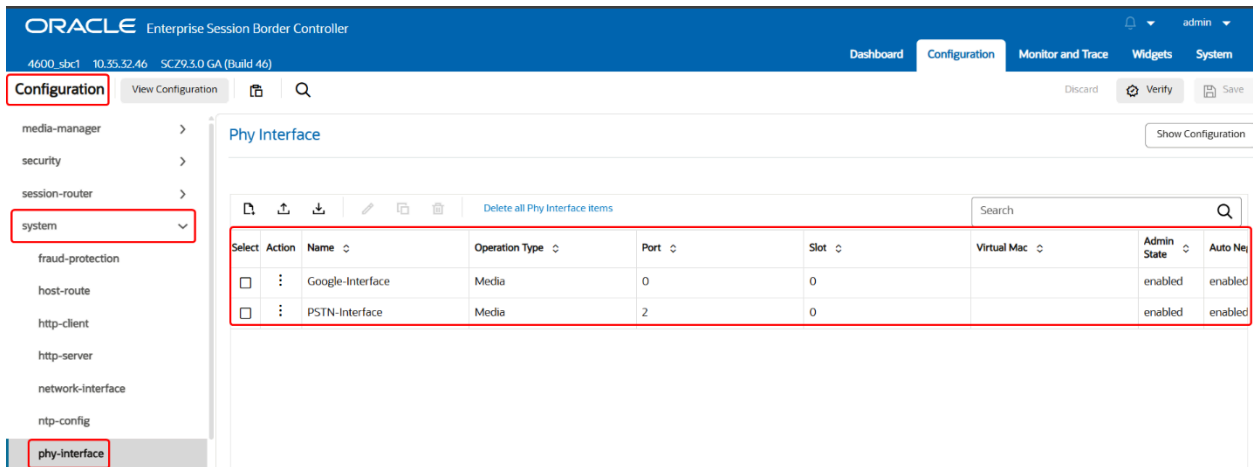


Figure 4: Physical Interfaces

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

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 Phy Interface

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

Network Alarm Threshold

No network alarm threshold to display. Please add or upload network alarm threshold.

[Add](#) [Upload](#)

Figure 5: Physical Interface towards Google CES

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

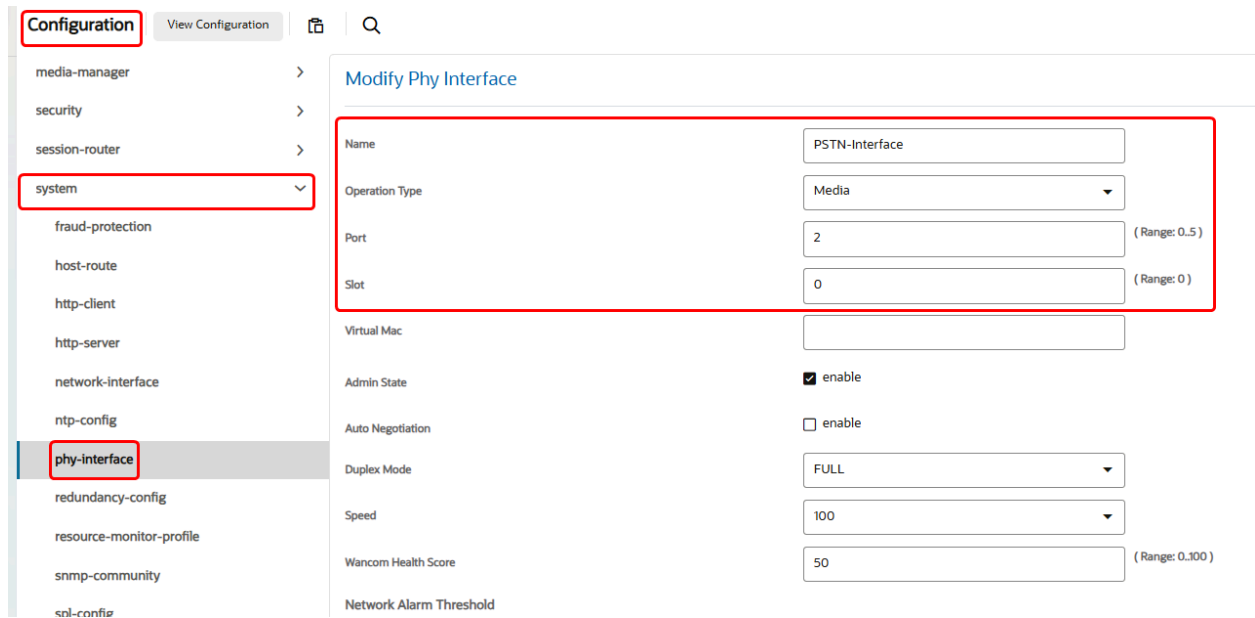


Figure 6: Physical Interface towards PSTN Gateway and OnPrem PBX

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.

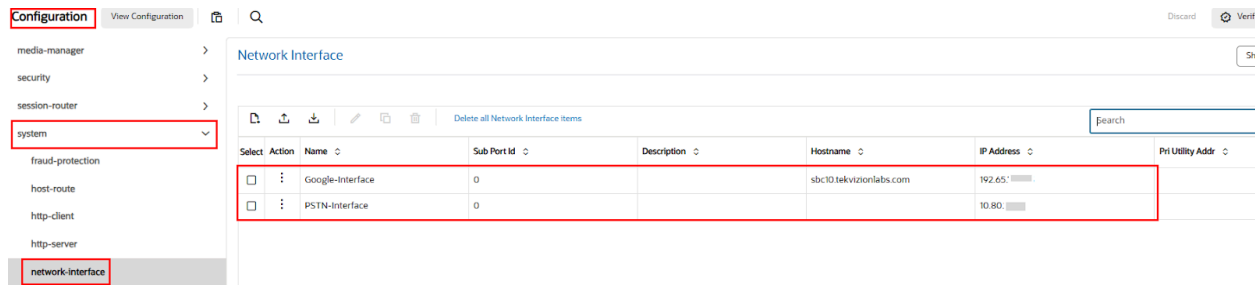


Figure 7: Network Interfaces

- Configure Network interface towards Google CES as shown below.

The screenshot shows the 'Modify Network Interface' configuration page. The left sidebar has 'network-interface' selected. The main form contains the following fields:

Name	Google-Interface
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	sbc10.tekvisionlabs.com
IP Address	192.65
Pri Utility Addr	
Sec Utility Addr	
Netmask	255.255.255.128
Gateway	192.65

Below the main form, there is a section for 'Gw Heartbeat' which is currently collapsed.

Figure 8: Network Interface towards Google CES

The screenshot shows the 'Gw Heartbeat' configuration page. The left sidebar has 'network-interface' selected. The main form contains the following fields:

State	<input checked="" type="checkbox"/> enable
Heartbeat	10 (Range: 0..65535)
Retry Count	3 (Range: 0..65535)
Retry Timeout	3 (Range: 1..65535)
Health Score	0 (Range: 0..100)

Below the main form, there is a section for 'Bfd Config' which is currently collapsed.

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

Configuration View Configuration

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

Modify Network Interface

DNS IP Primary	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 10: 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	10.80.13.50	
Pri Utility Addr		
Sec Utility Addr		
Netmask	255.255.255.0	
Gateway	10.80.13.1	
GW Heartbeat		
State	<input checked="" type="checkbox"/> enable	
Heartbeat	10	(Range: 0..65535)
Retry Count	3	(Range: 0..65535)
Retry Timeout	3	(Range: 1..65535)

Figure 11: Network Interface towards OnPrem PBX and PSTN Gateway

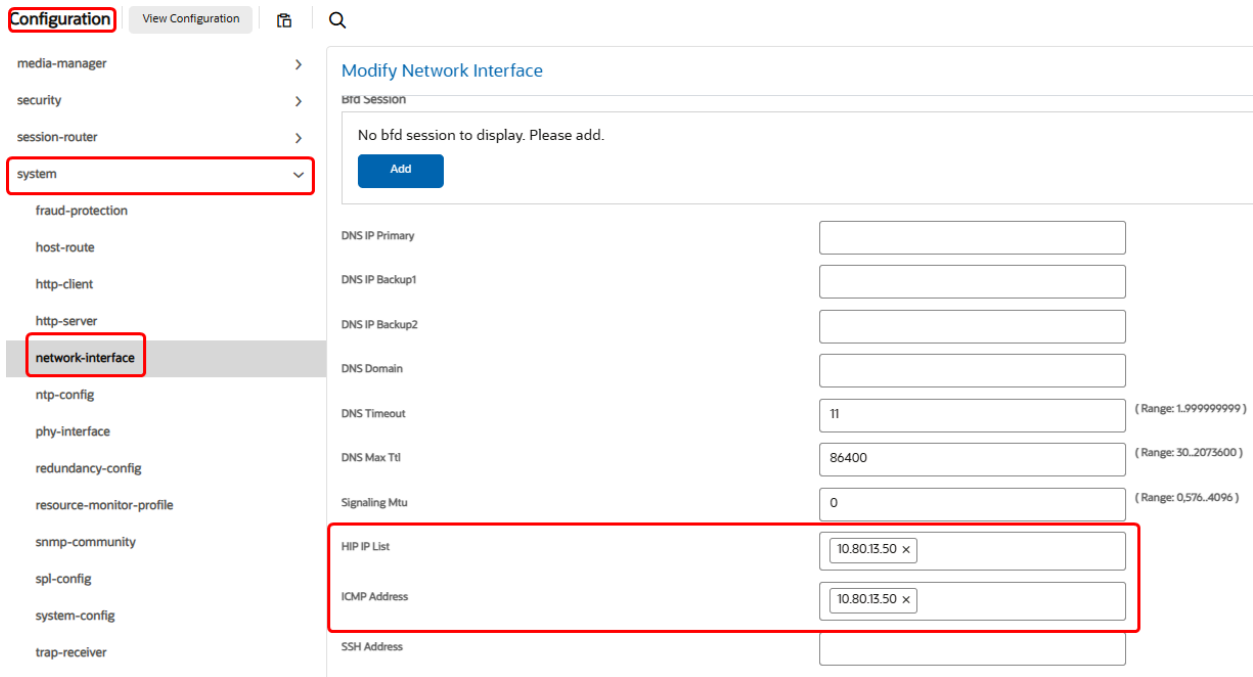


Figure 12: Network Interface towards OnPrem PBX and PSTN Gateway (Cont.)

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

7.4.4 SIP Config

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

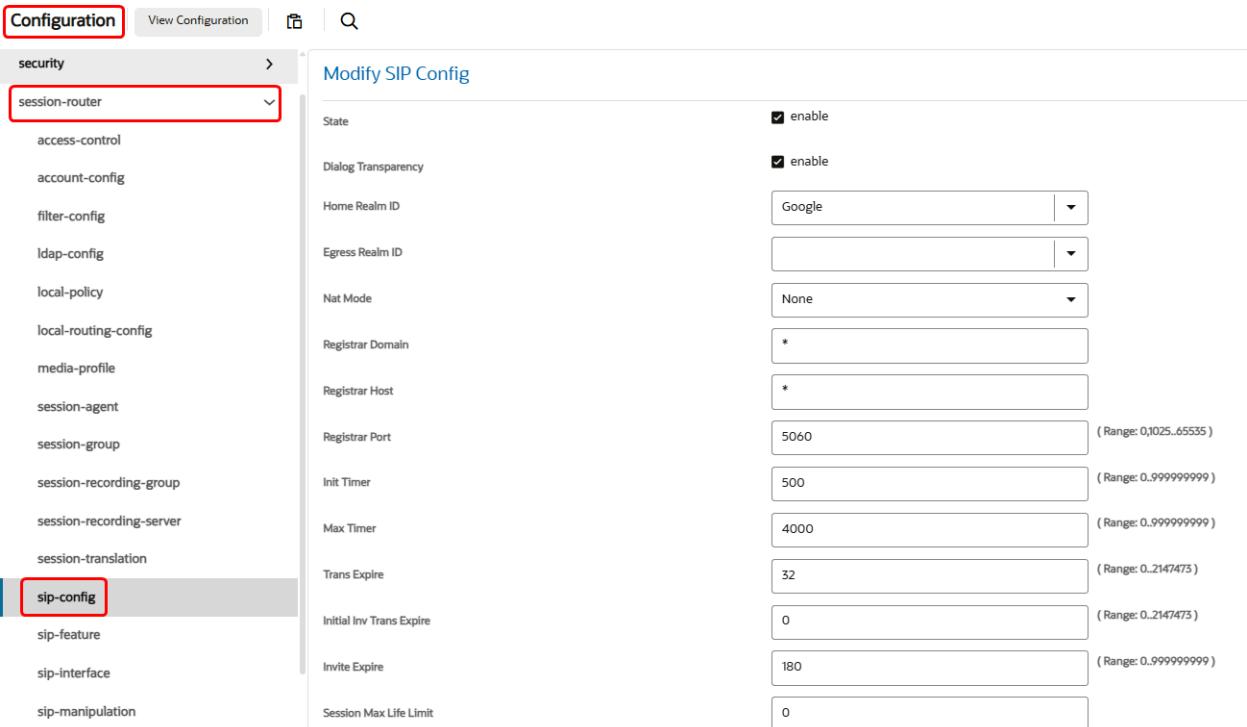


Figure 13: SIP-Config

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
- sip-interface
- sip-manipulation
- sip-monitoring
- translation-profile

Modify SIP Config

Emergency Dscp Profile	<input type="text"/>	
Red Max Trans	<input type="text" value="10000"/>	(Range: 0.50000)
Options	<input type="text" value="max-udp-length=0 x"/>	
SPL Options	<input type="text"/>	
SIP Message Len	<input type="text" value="65535"/>	(Range: 0.65535)
Enum Sag Match	<input type="checkbox"/>	enable
Extra Method Stats	<input checked="" type="checkbox"/>	enable
Extra Enum Stats	<input type="checkbox"/>	enable
Registration Cache Limit	<input type="text" value="0"/>	(Range: 0.999999999)
Register Use To For Lp	<input type="checkbox"/>	enable
Refer Src Routing	<input type="checkbox"/>	enable
Atcf Stn Sr	<input type="text"/>	
Atcf Psi Dn	<input type="text"/>	
Atcf Route To Sccas	<input type="checkbox"/>	enable
Eatf Stn Sr	<input type="text"/>	
Sag Lookup On Redirect	<input type="checkbox"/>	enable

Figure 14: SIP-Config (Cont.)

Configuration View Configuration

- media-manager >
- security >
- session-router
- access-control
- account-config
- filter-config
- ldap-config
- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config**
- sip-feature
- sip-interface

Modify SIP Config

Atcf Route To Sccas	<input type="checkbox"/>	enable
Eatf Stn Sr	<input type="text"/>	
Sag Lookup On Redirect	<input type="checkbox"/>	enable
Set Disconnect Time On Bye	<input type="checkbox"/>	enable
Refer Reinvite No Sdp	<input type="checkbox"/>	enable
Msrp Delayed Bye Timer	<input type="text" value="15"/>	(Range: 0.60)
Transcoding Realm	<input type="text"/>	
Transcoding Agents	<input type="text"/>	
Create Dynamic Sa	<input type="checkbox"/>	enable
Node Functionality	<input type="text" value="P-CSCF"/>	
Match SIP Instance	<input type="checkbox"/>	enable
Sa Routes Stats	<input type="checkbox"/>	enable
Sa Routes Traps	<input type="checkbox"/>	enable
Rx SIP Reason Mapping	<input type="checkbox"/>	enable

Figure 15: SIP-Config (Cont.)

Configuration View Configuration

- media-manager
- security
- session-router
- access-control
- account-config
- filter-config
- ldap-config
- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config
- sip-feature
- sip-interface

Modify SIP Config

Add Ue Location In Panel	inherit	
Hold Emergency Calls For Loc Info	0	(Range: 0..4294967295)
Retry After Upon Offline	0	(Range: 0..999999999)
Reg Reject Response Upon Offline	503	
Hold Invite Calls For Loc Info	0	(Range: 0..4294967295)
Cache Loc Info Expire	32	(Range: 0..4294967295)
Msg Hold For Loc Info	0	(Range: 0..30)
NpII Upon Register	inherit	
Start Hold Timer Event	AAR	
Hist To Div For Cause 380	inherit	
Anonymize History For Untrusted	<input type="checkbox"/> enable	
Asymm Preconditions Evs Swb Support	<input type="checkbox"/> enable	
Sms Report Timeout	32	(Range: 1..100000)
User Agent		

Figure 16: SIP-Config (Cont.)

Configuration View Configuration

- media-manager
- security
- session-router
- access-control
- account-config
- filter-config
- ldap-config
- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config
- sip-feature
- sip-interface
- sip-manipulation
- sip-monitoring

Modify SIP Config

Reg Reject Response Upon Offline	503	
Hold Invite Calls For Loc Info	0	(Range: 0..4294967295)
Cache Loc Info Expire	32	(Range: 0..4294967295)
Msg Hold For Loc Info	0	(Range: 0..30)
NpII Upon Register	inherit	
Start Hold Timer Event	AAR	
Hist To Div For Cause 380	inherit	
Anonymize History For Untrusted	<input type="checkbox"/> enable	
Asymm Preconditions Evs Swb Support	<input type="checkbox"/> enable	
Sms Report Timeout	32	(Range: 1..100000)
User Agent		
Precondition Enhancement	<input type="checkbox"/> enable	
Precondition Med Enhancement	<input type="checkbox"/> 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 17: 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

Figure 18: 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

Call Trace: enable

Default Gateway: 10.35.32.1

Restart: enable

Telnet Timeout: (Range: 0..65535)

Console Timeout: (Range: 0..65535)

HTTP Timeout: (Range: 0..20)

Reserved Nsep Session Capacity: (Range: 0..300)

Alarm Threshold
No alarm threshold to display. Please add.

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..3024)

Figure 19: System-Config (Cont.)

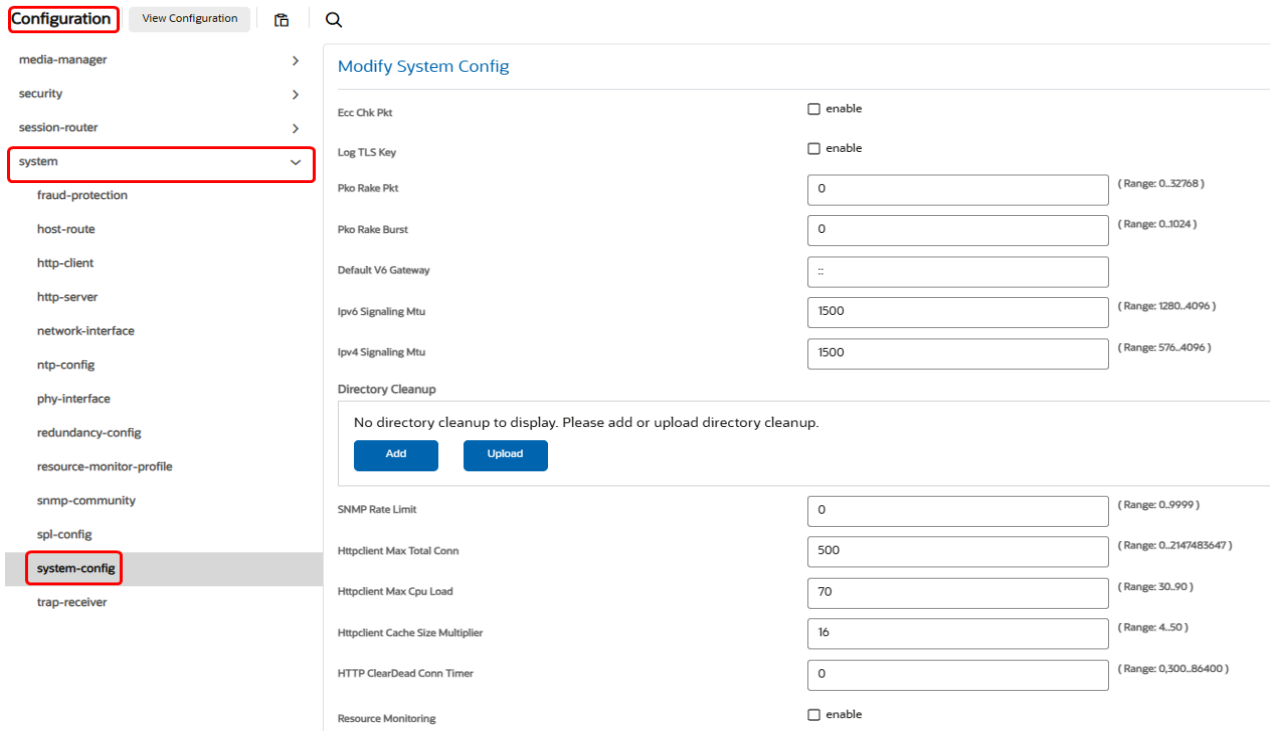


Figure 20: System-Config (Cont.)

7.4.6 SIP Monitoring

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

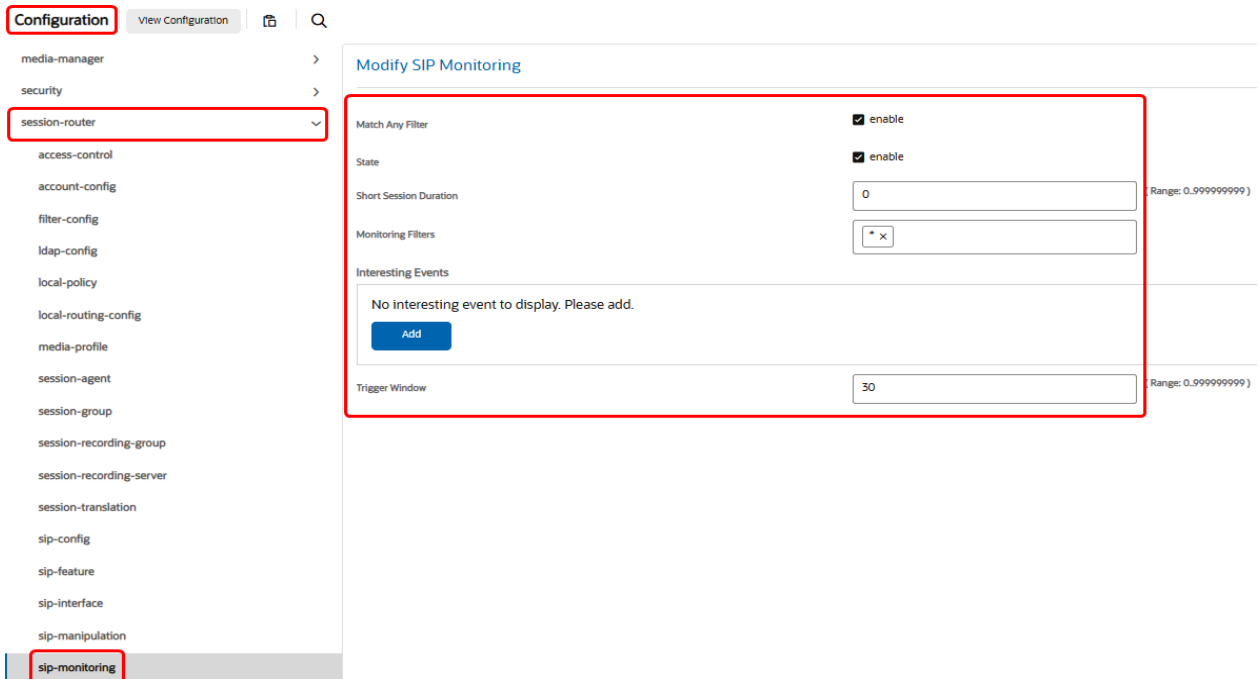


Figure 21: SIP Monitoring

7.4.7 HTTP Server

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

The screenshot shows the 'Modify HTTP Server' configuration page. The left sidebar is expanded to 'system' > 'http-server'. The main configuration area includes the following fields:

- Name: wancom0
- State: enable
- Realm: [dropdown]
- IP Address: [text]
- 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 22: HTTP Server

7.4.8 Codec Policy

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

The screenshot shows the 'Modify Codec Policy Entries' configuration page. The left sidebar is expanded to 'media-manager' > 'codec-policy'. The main configuration area includes the following fields:

- Name: Google
- Allow Codecs: telephone-event x, PCMU x, PCMA x
- Add Codecs On Egress: PCMU x, PCMA x
- Order Codecs: PCMU x, PCMA x, telephone-event x
- Packetization Time: 20
- Force Ptime: enable
- Secure Dtmf Cancellation: enable
- Dtmf In Audio: disabled
- Tone Detection: [text]
- Tone Detect Renegotiate Timer: 500 (Range: 50.32000)
- Reverse Fax Tone Detection Reinvite: enable
- Fax Single M Line: disabled
- Evrc Tty Baudot Transcode: enable

Figure 23: Codec Policy for Google CES

7.4.9 Translation Rules

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

The screenshot shows the 'Configuration' page with the 'translation-rules' menu item highlighted. The main content area displays a table of Translation Rules. The table has columns for Select, Action, Id, Description, Input Header Type, Input Header Value, Output Header Type, and Output Header Value. The rules are as follows:

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)(.*)\$	called-header	\$01+\$02
<input type="checkbox"/>	:	addplus1_calling-header	add	calling-header	^(0)(.*)\$	calling-header	\$01+\$02
<input type="checkbox"/>	:	addplus1_p-asserted-id-header	add	p-asserted-id-header	^(0)(.*)\$	p-asserted-id-header	\$01+\$02
<input type="checkbox"/>	:	addplus1_request-uri	add	request-uri	^(0)(.*)\$	request-uri	\$01+\$02
<input type="checkbox"/>	:	removeplus1_called-header	delete	called-header	^(.*)+!(.*)\$	called-header	\$1\$2
<input type="checkbox"/>	:	removeplus1_calling-header	delete	calling-header	^(.*)+!(.*)\$	calling-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 24: Translation Rule to add or remove E.164 format Google CES

7.4.10 Session Translation

- Navigate to **Configuration** > **session-router** > **session-translation**. The translation rules configured in [Section 7.4.9](#) is mapped to Google CES is shown below.

The screenshot shows the 'Configuration' page with the 'session-router' and 'session-translation' menu items highlighted. The main content area displays the 'Session Translation' configuration page. The table lists session translation rules as follows:

Select	Action	Id
<input type="checkbox"/>	:	addplus1
<input type="checkbox"/>	:	removeplus1

Figure 25: Session Translation 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 Session Translation

Id: addplus1

Session Trans Rule

Select	Action	Rule Id	Mandatory	State
<input type="checkbox"/>	:	addplus1_calling-header	disabled	enabled
<input type="checkbox"/>	:	addplus1_called-header	disabled	enabled
<input type="checkbox"/>	:	addplus1_request-uri	disabled	enabled
<input type="checkbox"/>	:	addplus1_p-asserted-id-header	disabled	enabled

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

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

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 Translation

Id: removeplus1

Session Trans Rule

Select	Action	Rule Id	Mandatory	State
<input type="checkbox"/>	:	removeplus1_calling-header	disabled	enabled
<input type="checkbox"/>	:	removeplus1_called-header	disabled	enabled
<input type="checkbox"/>	:	removeplus1_request-uri	disabled	enabled
<input type="checkbox"/>	:	removeplus1_p-asserted-id-header	disabled	enabled

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

7.4.11 Session Recording Server

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

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 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 28: Session Recording Server towards Google CES

7.4.12 Realm Config

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

Configuration View Configuration Discard Verify

media-manager >
codecs-policy
media-manager
media-policy
realm-config
steering-pool
security >

Realm Config

Delete all Realm Config Items

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

Figure 29: Realm Configuration

- Realm Config towards Google CES is shown below.

The screenshot shows the 'Modify Realm Config' page for the 'realm-config' profile. The left sidebar lists configuration categories, with 'realm-config' selected. The main area contains the following fields:

- Identifier:** Google
- Description:** (Empty text area)
- Addr Prefix:** 0.0.0.0
- Network Interfaces:** Google-Interface:0.4 x
- Media Realm List:** (Empty text area)
- 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:** (Dropdown menu)

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

The screenshot shows the 'Modify Realm Config' page for the 'realm-config' profile. The left sidebar lists configuration categories, with 'realm-config' selected. The main area contains the following fields:

- DNS Realm:** (Dropdown menu)
- Media Policy:** (Dropdown menu)
- Nsep Media Policy:** (Dropdown menu)
- Media Sec Policy:** SRTP
- RTCP Mux:** enable
- Ice Profile:** (Dropdown menu)
- Teams Fqdn:** (Text input)
- Teams Fqdn In Uri:** enable
- SDP Inactive Only:** enable
- DTLS Srtp Profile:** (Dropdown menu)
- Srtp Msm Passthrough:** enable
- Class Profile:** (Dropdown menu)

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

Configuration View Configuration

media-manager

codecc-policy

media-manager

media-policy

realm-config

steering-pool

security >

session-router >

system >

Modify Realm Config

In Session Translations

No in session translation list to display. Please add.

Add

Out Session Translations

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

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

Configuration View Configuration

media-manager

codecc-policy

media-manager

media-policy

realm-config

steering-pool

security >

session-router >

system >

Modify Realm Config

In ManipulationId

Out ManipulationId GoogleManipulation

Average Rate Limit 0 (Range: 0..4294967295)

Access Control Trust Level high

Max Inbound Per Session Burst Rate 30 (Range: 1..999999999)

Burst Rate Window Per Session 1 (Range: 1..999999999)

Dos Action At Session none

Invalid Signal Threshold 0 (Range: 0..4294967295)

Maximum Signal Threshold 0 (Range: 0..4294967295)

Untrusted Signal Threshold 0 (Range: 0..4294967295)



Nat Trust Threshold 0 (Range: 0..65535)


Max Endpoints Per Nat 0 (Range: 0..65535)

Nat Invalid Message Threshold 0 (Range: 0..65535)

Wait Time For Invalid Register 0 (Range: 0..300)

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

Configuration View Configuration  

media-manager 

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

Modify Realm Config









Deny Period	<input type="text" value="30"/>	(Range: 0..4294967295)
Session Max Life Limit	<input type="text" value="0"/>	
Untrust Cac Failure Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Subscription Id Type	<input type="text" value="END_USER_NONE"/>	
Trunk Context	<input type="text"/>	
Early Media Allow	<input type="text"/>	
Enforcement Profile	<input type="text"/>	
Additional Prefixes	<input type="text"/>	
Restricted Latching	<input type="text" value="none"/>	
Options	<input type="text"/>	
SPL Options	<input type="text"/>	
Delay Media Update	<input type="checkbox"/> enable	
Refer Call Transfer	<input type="text" value="disabled"/>	
Hold Refer Rewrite	<input type="checkbox"/> enable	

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

Configuration View Configuration  

media-manager 

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

Modify Realm Config









Refer Notify Provisional	<input type="text" value="none"/>	
Dyn Refer Term	<input type="checkbox"/> enable	
Codec Policy	<input type="text" value="Google"/>	
Codec ManIP In Realm	<input type="checkbox"/> enable	
Codec ManIP In Network	<input checked="" type="checkbox"/> enable	
RTCP Policy	<input type="text"/>	
Constraint Name	<input type="text"/>	
Session Recording Server	<input type="text"/>	
Session Recording Required	<input type="checkbox"/> enable	
SIP Profile	<input type="text"/>	
Flow Time Limit	<input type="text" value="-1"/>	(Range: -1..2147483647)
Initial Guard Timer	<input type="text" value="-1"/>	(Range: -1..2147483647)
Subsq Guard Timer	<input type="text" value="-1"/>	(Range: -1..2147483647)
TCP Flow Time Limit	<input type="text" value="-1"/>	(Range: -1..2147483647)

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

Configuration View Configuration  



media-manager 


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

Modify Realm Config

TCP Initial Guard Timer	<input type="text" value="-1"/>	(Range: -1.2147483647)
TCP Subsq Guard Timer	<input type="text" value="-1"/>	(Range: -1.2147483647)
SIP Isup Profile	<input type="text"/>	
QoS Constraint	<input type="text"/>	
Hide Egress Media Update	<input type="checkbox"/> enable	
TCP Media Profile	<input type="text"/>	
Monitoring Filters	<input type="text"/>	
Node Functionality	<input type="text"/>	
Default Location String	<input type="text"/>	
Alt Family Realm	<input type="text"/>	
Pref Addr Type	<input type="text" value="none"/>	
Sm Icsi Match For Invite	<input type="text"/>	
Sm Icsi Match For Message	<input type="text"/>	

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

Configuration View Configuration  

media-manager 

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

Modify Realm Config

Ringback Trigger	<input type="text" value="none"/>	
Ringback File	<input type="text"/>	
Merge Early Dialogs	<input type="checkbox"/> enable	
User Site	<input type="text"/>	
Srvcc Trfo	<input type="text"/>	
Feature Trfo	<input type="text"/>	
Auth Attribute	<p>No auth attributes to display. Please add.</p> <p><input type="button" value="Add"/></p>	
Fqdn Hostname	<input type="text"/>	
Fqdn Hostname In Header	<input type="text"/>	
P Asserted Identity	<input type="text"/>	
P Asserted Identity For	<input type="text"/>	
Steering Pool Threshold	<input type="text" value="0"/>	(Range: 0.100)

Figure 37: 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

Srvc Trfo

Feature Trfo

Auth Attribute

No auth attributes to display. Please add.

Add

Fqdn Hostname

Fqdn Hostname In Header

P Asserted Identity

P Asserted Identity For

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

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

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

Suppress Hold Resume Reinvite enable

SNMP Sipmethod Stats enable

Figure 38: 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

DNS Realm

Media Policy

Nsep Media Policy

Media Sec Policy RTP

RTCP Mux enable

Ice Profile

Teams Fqdn

Teams Fqdn In Uri enable



SDP Inactive Only enable

DTLS Srtp Profile

Srtp Msm Passthrough enable

Class Profile

Figure 39: 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

Displaying 1 - 1 of 1

In Manipulationid	<input type="text"/>	
Out Manipulationid	<input type="text"/>	
Average Rate Limit	<input type="text" value="0"/>	(Range: 0..4294967295)
Access Control Trust Level	<input type="text" value="none"/>	
Max Inbound Per Session Burst Rate	<input type="text" value="30"/>	(Range: 1..999999999)
Burst Rate Window Per Session	<input type="text" value="1"/>	(Range: 1..999999999)
Dos Action At Session	<input type="text" value="none"/>	
Invalid Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Maximum Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Untrusted Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Nat Trust Threshold	<input type="text" value="0"/>	(Range: 0..65535)
Max Endpoints Per Nat	<input type="text" value="0"/>	(Range: 0..65535)
Nat Invalid Message Threshold	<input type="text" value="0"/>	(Range: 0..65535)
Wait Time For Invalid Register	<input type="text" value="0"/>	(Range: 0..4..300)

Figure 40: 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

Displaying 1 - 1 of 1

In Manipulationid	<input type="text"/>	
Out Manipulationid	<input type="text"/>	
Average Rate Limit	<input type="text" value="0"/>	(Range: 0..4294967295)
Access Control Trust Level	<input type="text" value="none"/>	
Max Inbound Per Session Burst Rate	<input type="text" value="30"/>	(Range: 1..999999999)
Burst Rate Window Per Session	<input type="text" value="1"/>	(Range: 1..999999999)
Dos Action At Session	<input type="text" value="none"/>	
Invalid Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Maximum Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Untrusted Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Nat Trust Threshold	<input type="text" value="0"/>	(Range: 0..65535)
Max Endpoints Per Nat	<input type="text" value="0"/>	(Range: 0..65535)
Nat Invalid Message Threshold	<input type="text" value="0"/>	(Range: 0..65535)
Wait Time For Invalid Register	<input type="text" value="0"/>	(Range: 0..4..300)

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

Configuration View Configuration  

media-manager 

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security >

session-router >

system >

Modify Realm Config









Refer Notify Provisional	none	
Dyn Refer Term	<input type="checkbox"/>	enable
Codec Policy	Google	
Codec ManIP In Realm	<input type="checkbox"/>	enable
Codec ManIP In Network	<input checked="" type="checkbox"/>	enable
RTCP Policy		
Constraint Name		
Session Recording Server	GoogleCCAI x	
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)

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

Configuration View Configuration  

media-manager 

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security >

session-router >

system >

Modify Realm Config










TCP Initial Guard Timer	-1	(Range: -1.2147483647)
TCP Subsq Guard Timer	-1	(Range: -1.2147483647)
SIP Isup Profile		
QoS Constraint		
Hide Egress Media Update	<input type="checkbox"/>	enable
TCP Media Profile		
Monitoring Filters		
Node Functionality		
Default Location String		
Alt Family Realm		
Pref Addr Type	none	
Sm Icsi Match For Invite		
Sm Icsi Match For Message		

Figure 43: 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

Ringback Trigger

Ringback File

Merge Early Dialogs enable

User Site

Srvcc Trfo

Feature Trfo

Auth Attribute

No auth attributes to display. Please add.

Fqdn Hostname



Fqdn Hostname In Header


P Asserted Identity

P Asserted Identity For

Steering Pool Threshold (Range: 0..100)

Figure 44: 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

Srvcc Trfo

Feature Trfo

Auth Attribute

No auth attributes to display. Please add.

Fqdn Hostname

Fqdn Hostname In Header

P Asserted Identity

P Asserted Identity For

Steering Pool Threshold (Range: 0..100)

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

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

Suppress Hold Resume Reinvite enable

SNMP Sipmethod Stats enable

Figure 45: 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.

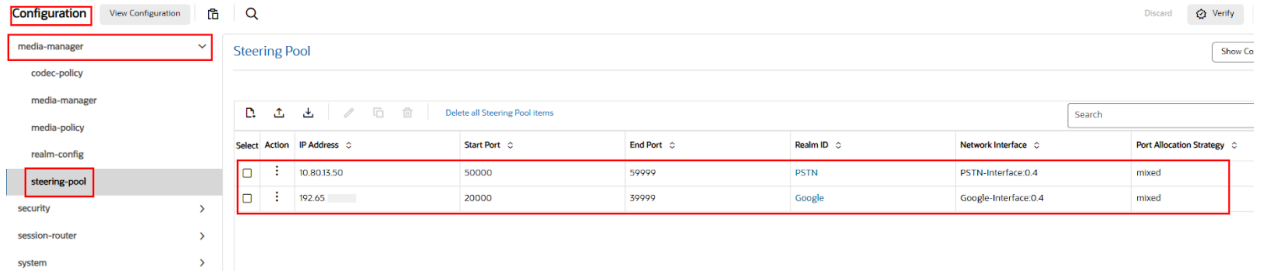


Figure 46: Steering Pool

- Steering Pool Configuration towards Google CES is shown below.

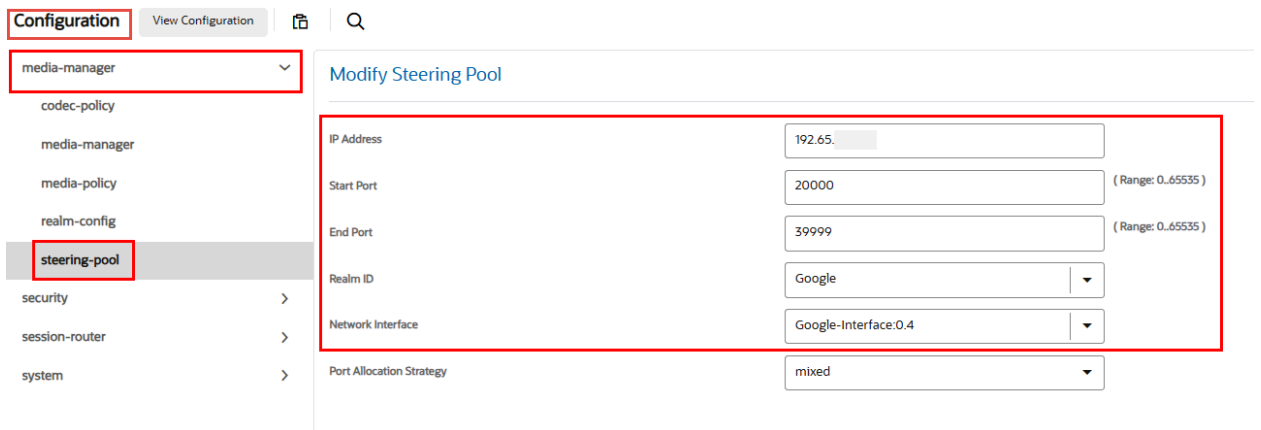


Figure 47: Steering Pool towards Google CES

- Steering Pool Configuration towards OnPrem PBX and PSTN Gateway is shown below.

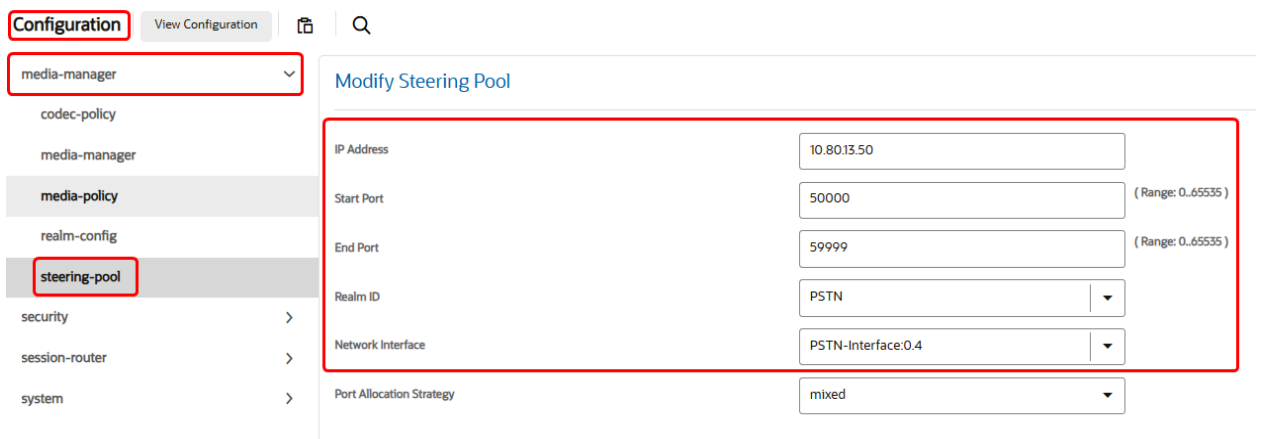


Figure 48: Steering Pool towards OnPrem PBX and PSTN

7.4.14 SDES Profile

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

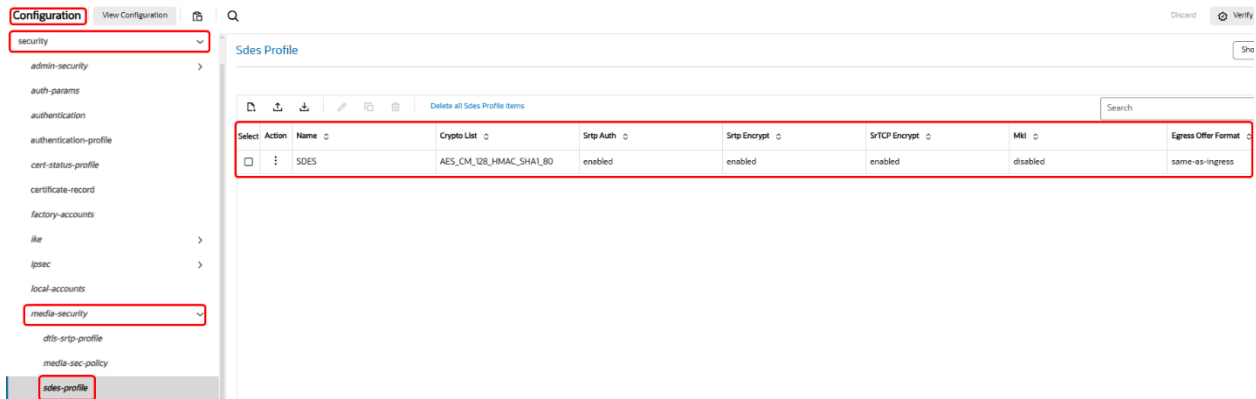


Figure 49: SDES Profile for TLS

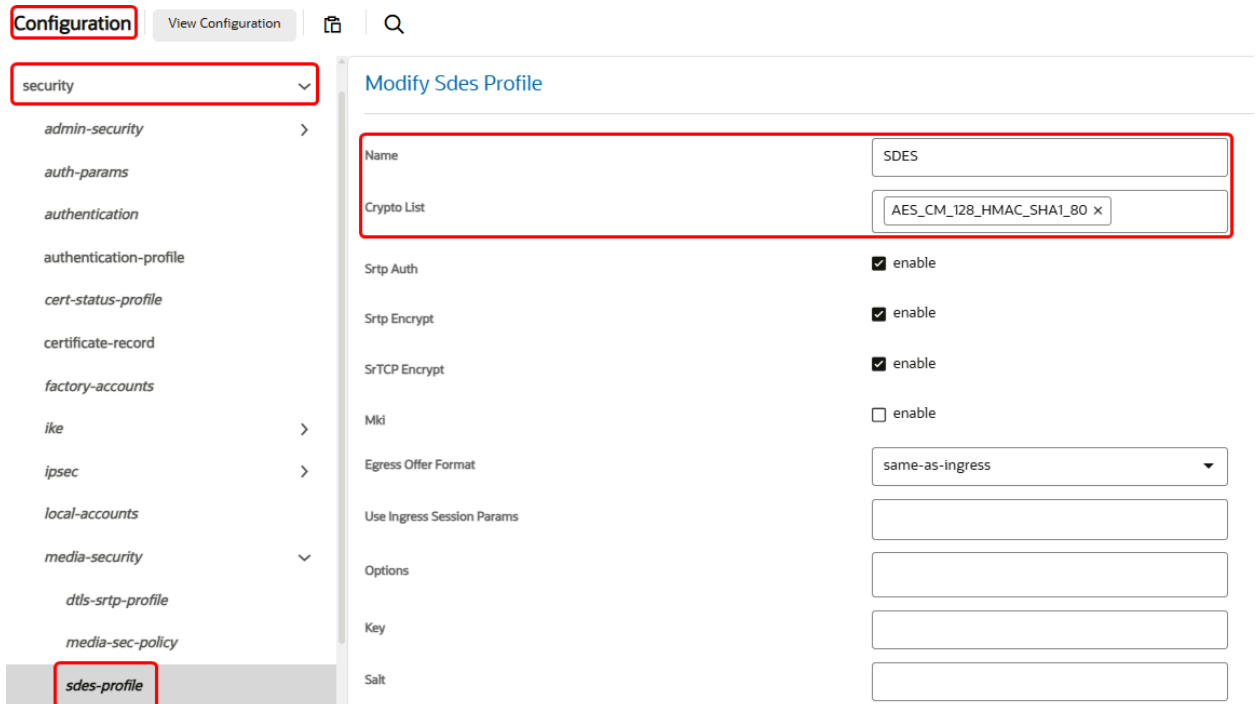


Figure 50: SDES Profile for TLS (Cont.)

7.4.15 Media Sec Policy

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

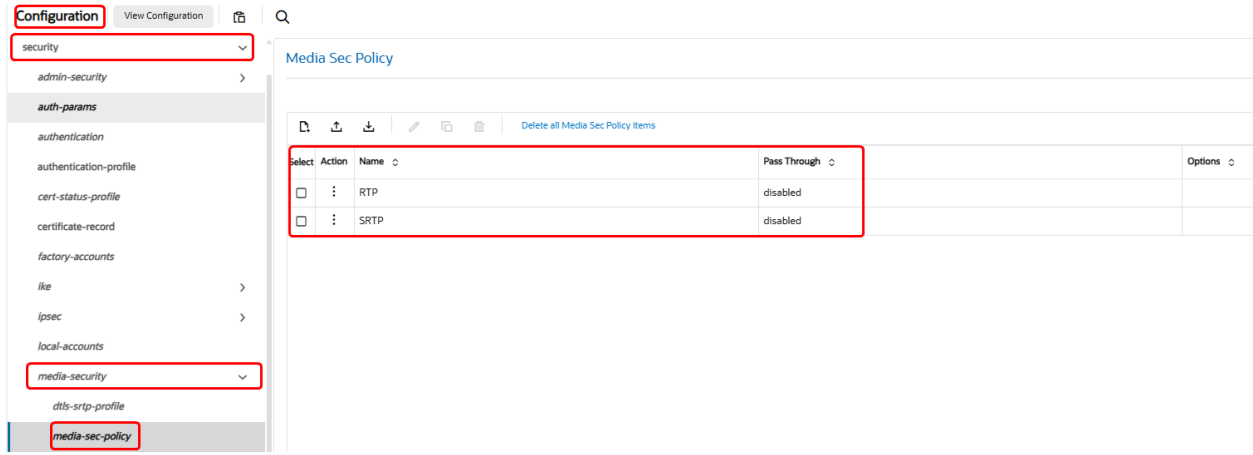


Figure 51: Media Security Policy

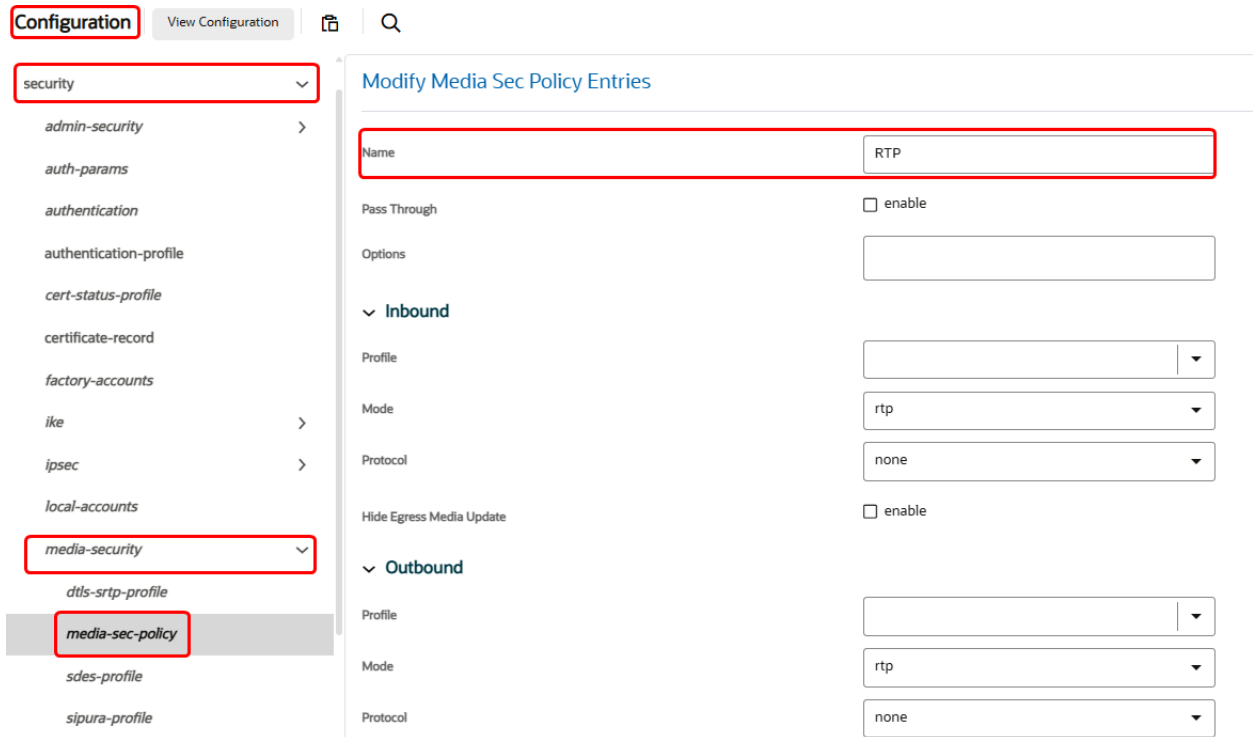


Figure 52: Media Security Policy for RTP

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

The screenshot shows a configuration page titled "Modify Media Sec Policy Entries". On the left is a navigation menu with "Configuration" at the top, followed by "security" (highlighted with a red box), "media-security" (highlighted with a red box), and "media-sec-policy" (highlighted with a red box). The main content area is divided into "Inbound" and "Outbound" sections. In the "Inbound" section, the "Name" field is set to "SRTP" (highlighted with a red box), "Pass Through" is unchecked, and "Options" is empty. Below this, the "Profile" is set to "SDES", "Mode" is "srtp", and "Protocol" is "sdes" (all three are highlighted with a red box). The "Outbound" section has the same settings: "Profile" is "SDES", "Mode" is "srtp", and "Protocol" is "sdes" (all three are highlighted with a red box). There are also checkboxes for "enable" under both "Pass Through" and "Hide Egress Media Update", which are currently unchecked.

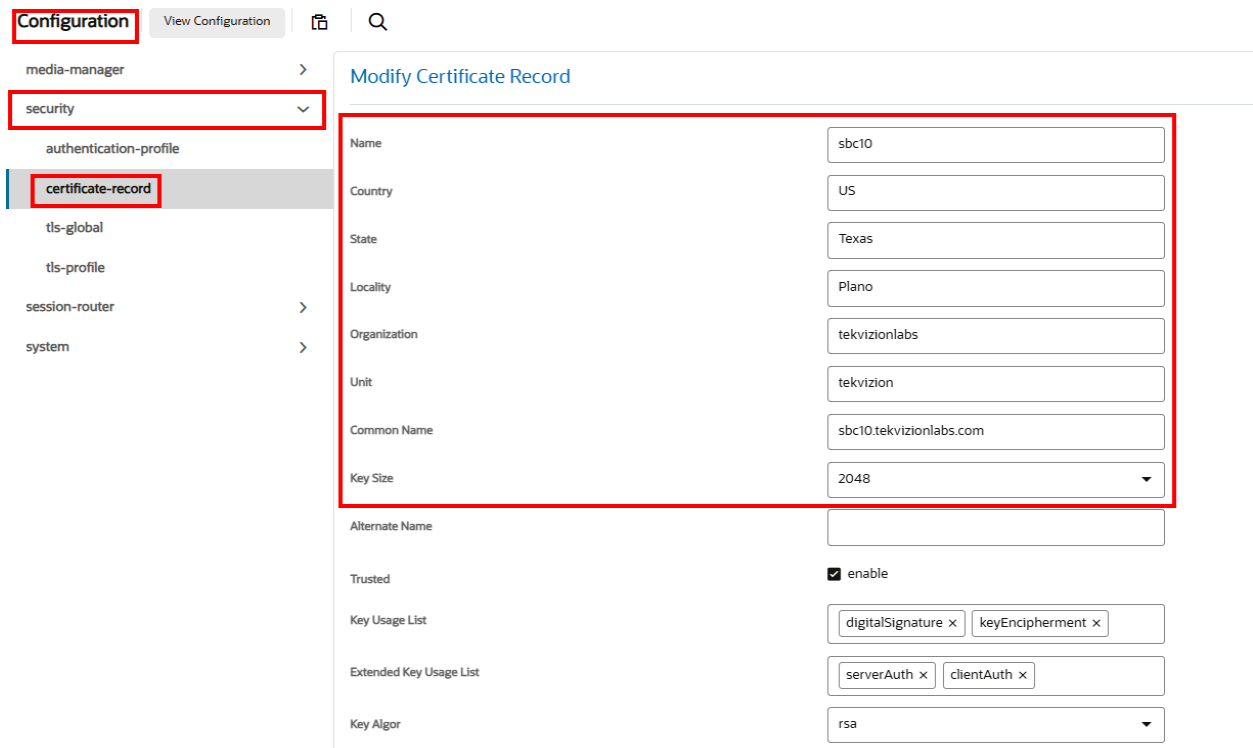
Figure 53: Media Security Policy for SRTP

7.4.16 TLS – Certificate Record

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

Certificate record for Oracle E-SBC:

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



The screenshot displays the Oracle E-SBC configuration interface. On the left, the 'Configuration' menu is expanded, showing a tree structure with 'security' > 'certificate-record' selected. The main area is titled 'Modify Certificate Record' and contains the following fields:

Name	sbci0
Country	US
State	Texas
Locality	Plano
Organization	tekvizionlabs
Unit	tekvizion
Common Name	sbci0.tekvizionlabs.com
Key Size	2048
Alternate Name	
Trusted	<input checked="" type="checkbox"/> enable
Key Usage List	digitalSignature x keyEncipherment x
Extended Key Usage List	serverAuth x clientAuth x
Key Algor	rsa

Figure 54: Create Certificate Record for Oracle E-SBC

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

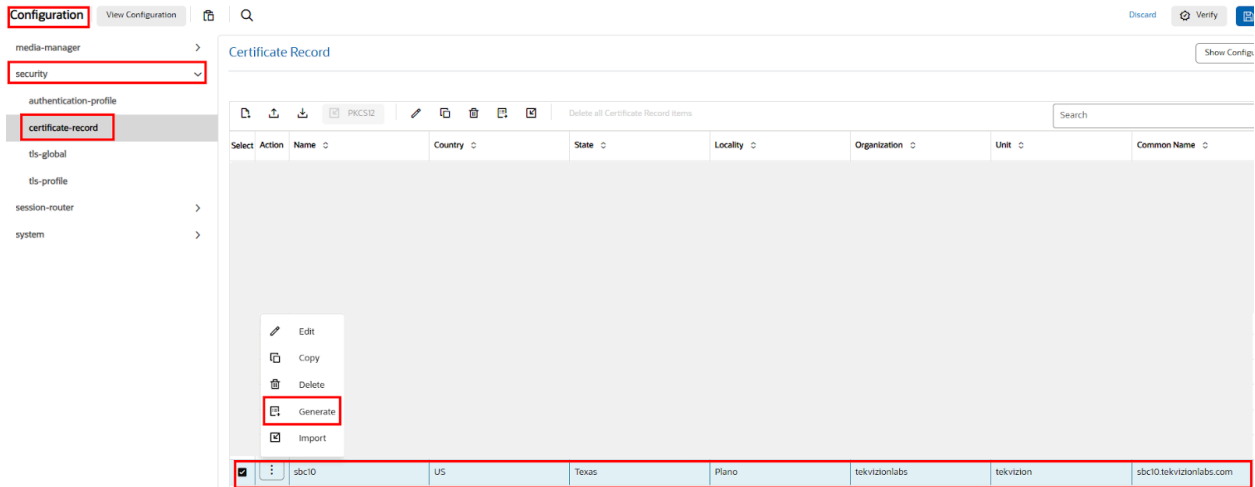


Figure 55: Generate Certificate Record for Oracle E-SBC

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

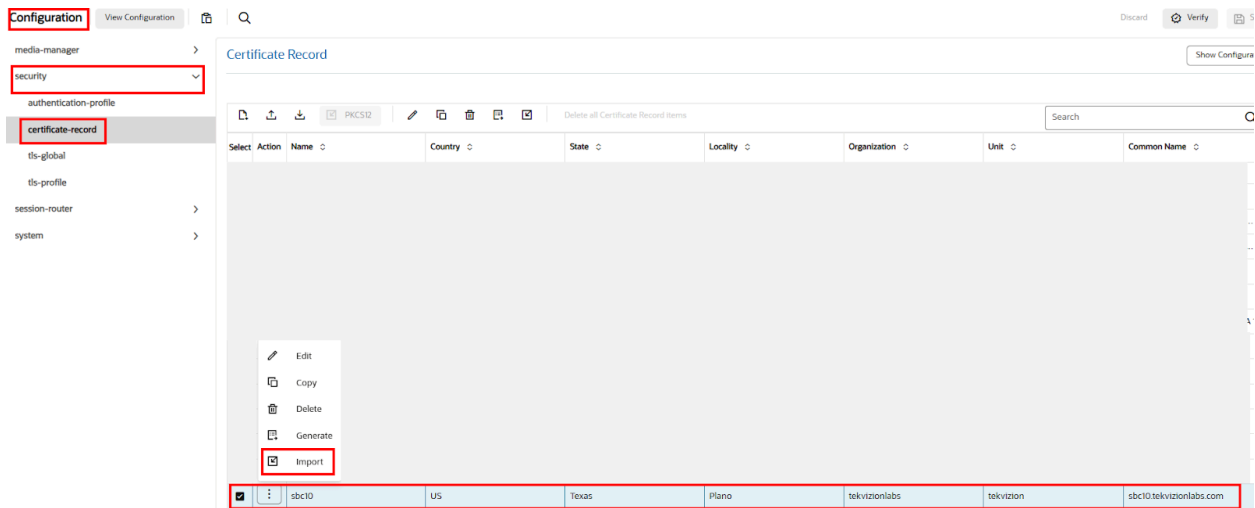


Figure 56: Import Certificate Record for Oracle E-SBC

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

Import Certificate

Format: try-all

Import Method: File, Paste

Certificate File: Upload 9c: 7.pem

Import Cancel

Figure 57: Import Certificate Record for Oracle E-SBC

Certificate record for Google Root CA:

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

Configuration View Configuration

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

Modify Certificate Record

Name: GTS_Root_R1
 Country: US
 State: MA
 Locality: Burlington
 Organization: Engineering

Unit:
 Common Name:
 Key Size: 2048
 Alternate Name:
 Trusted: enable
 Key Usage List: digitalSignature x keyEncipherment x
 Extended Key Usage List: serverAuth x
 Key Algor: rsa
 Digest Algor: sha256

Figure 58: Create Certificate Record for Google GTS Root R1 certificate

- Right click on the Certificate Record and Click Import.

Configuration View Configuration

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

Certificate Record

Discard Verify Save

Show Configuration

Select	Action	Name	Country	State	Locality	Organization	Unit	Common Name
<input checked="" type="checkbox"/>		GTS_Root	US	MA	Burlington	Engineering		
<input checked="" type="checkbox"/>		GTS_Root_R1	US	MA	Burlington	Engineering		
<input type="checkbox"/>	Edit	dotCAGOOOGLE	us	Texas	Plano	tekvizionlabs	tekvizion	
<input type="checkbox"/>	Copy	dot_CA_G2	US	TX	Plano	Tekvizionlabs		Go Daddy Root Certificate Author...
<input type="checkbox"/>	Delete	cure_CA_G2	US	TX	Plano	Tekvizionlabs		Go Daddy Secure Certificate Auth...
<input type="checkbox"/>	Generate	ICA	US	Texas	Plano	tekvizionLabs	tekvizion	
<input type="checkbox"/>	Import		US	MA	Burlington	Engineering		
<input type="checkbox"/>			US	TX	Plano	Tekvizionlabs		IdenTrust Commercial Root CA 1

Figure 59: Import Google GTS Root R1 certificate

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

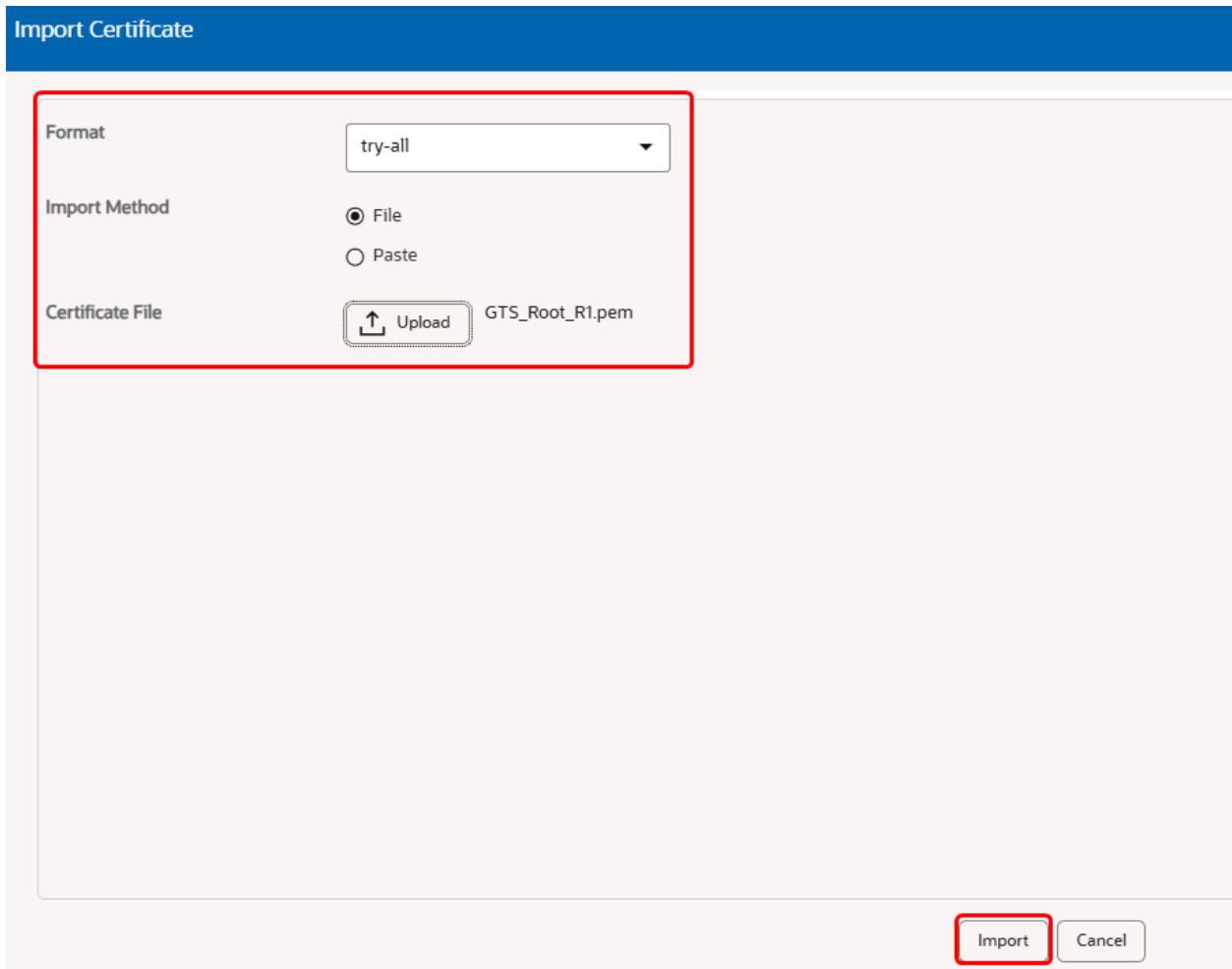


Figure 60: Import Google GTS Root R1 certificate (Cont.)

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

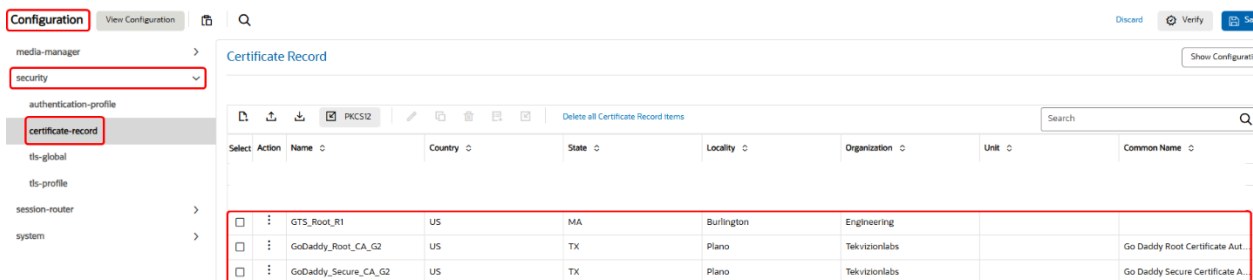


Figure 61: Certificate Records

7.4.17 TLS – TLS Profile

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

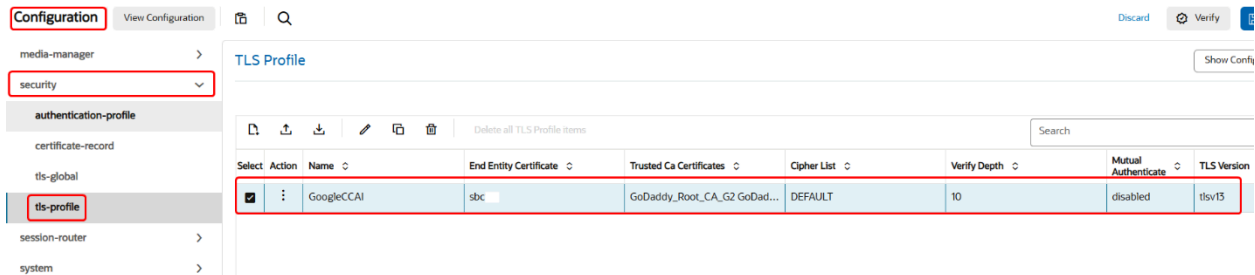


Figure 62: TLS Profile for Google CES

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

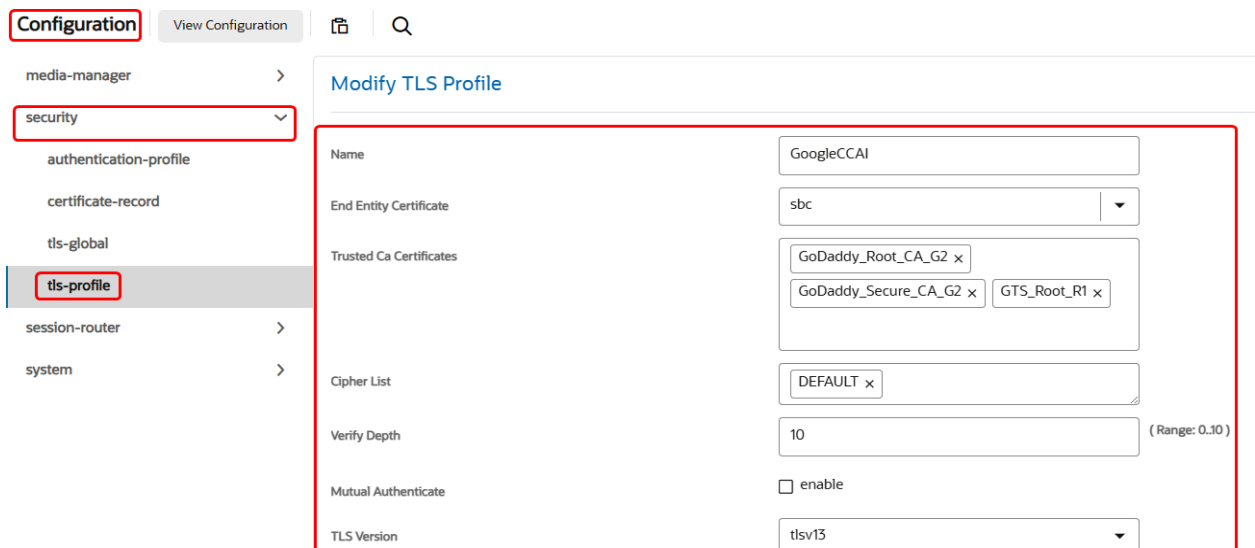


Figure 63: TLS Profile for Google CES (Cont.)

7.4.18 Session Timer

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

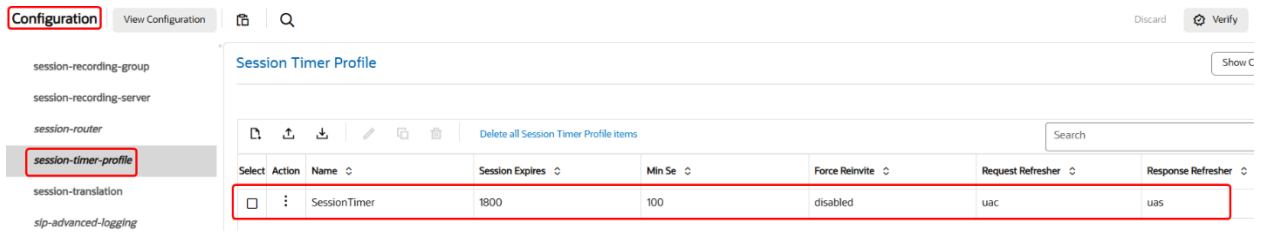


Figure 64: Session Timer

7.4.19 SIP Interface

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

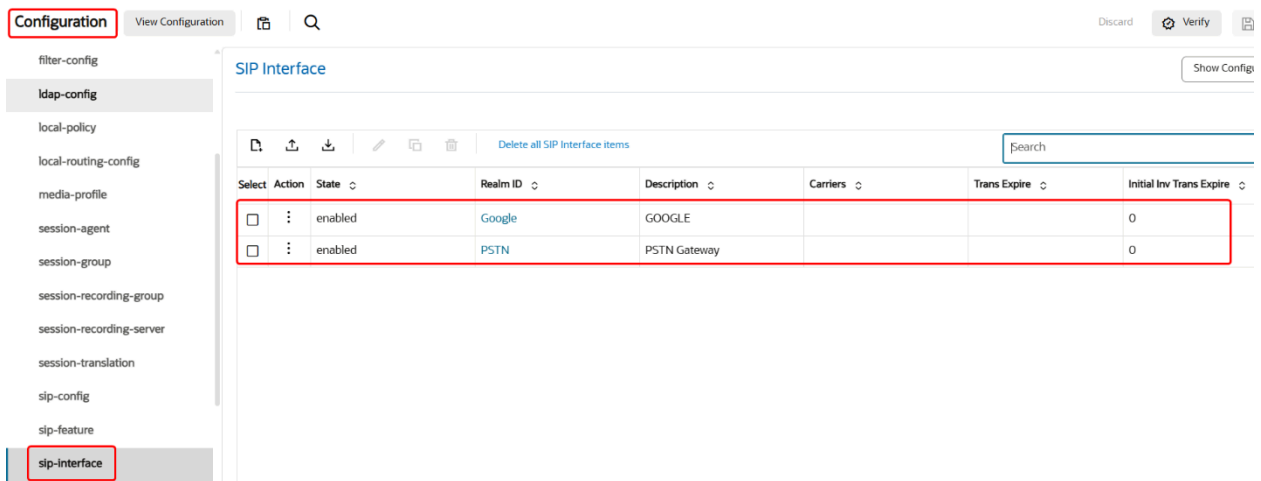


Figure 65: SIP Interface

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

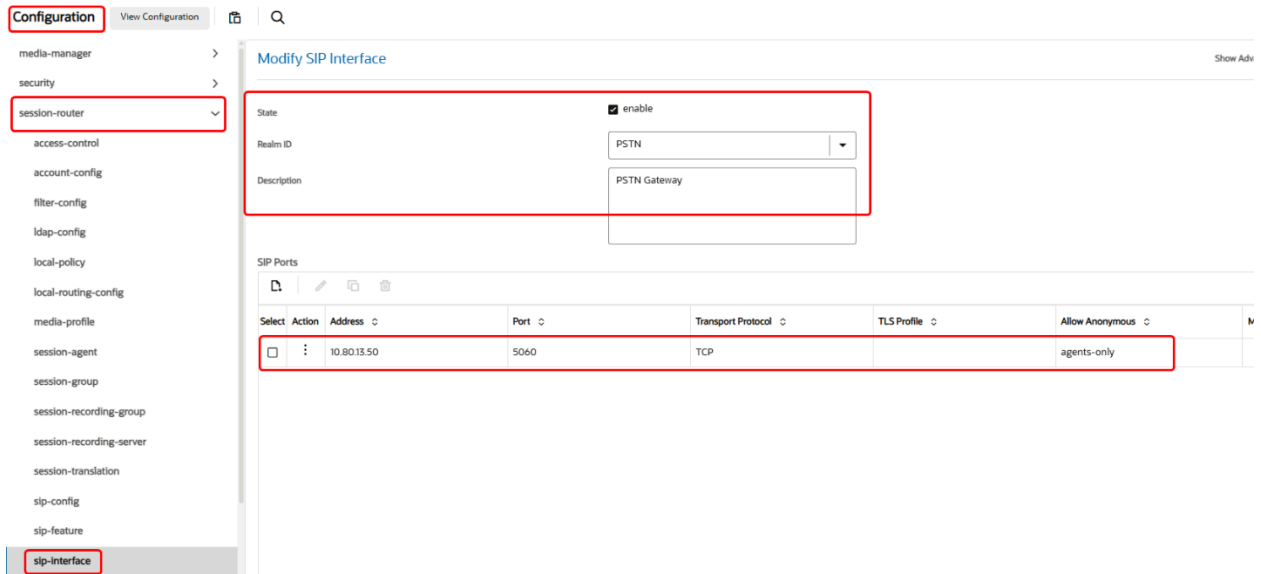


Figure 66: SIP Interface for PSTN Gateway and OnPrem PBX

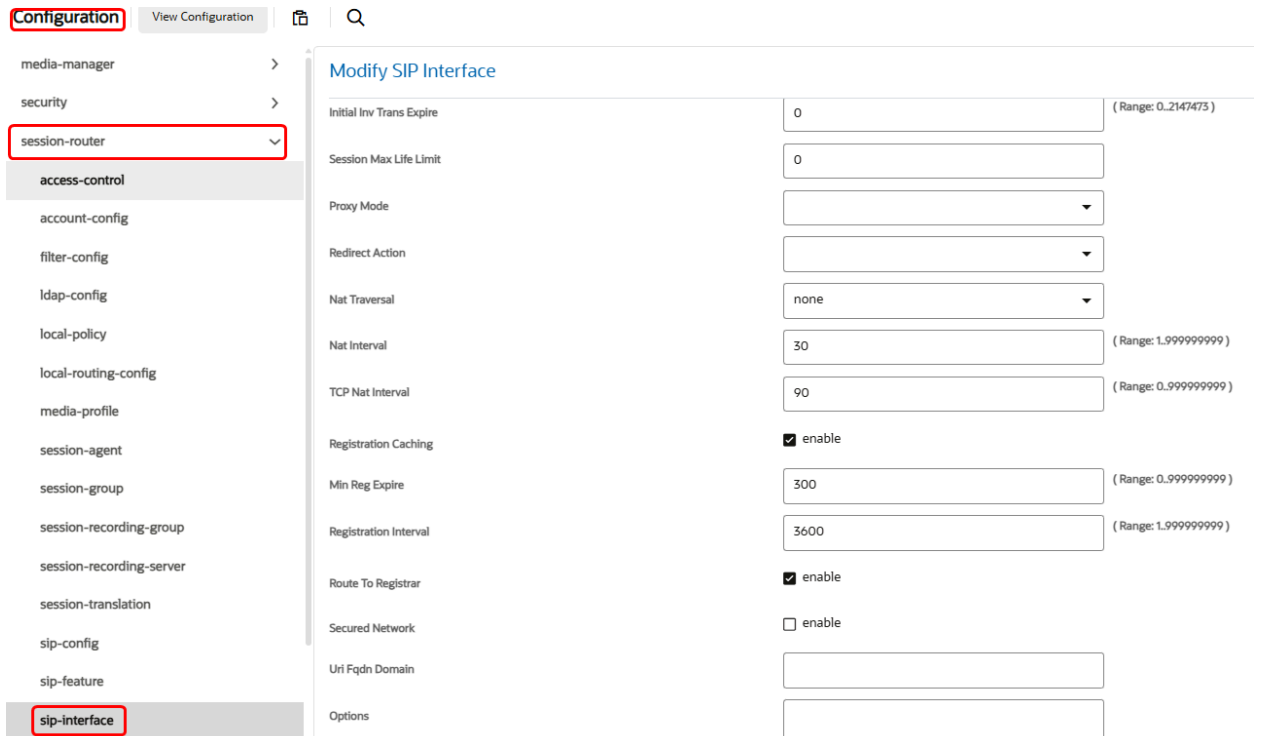




Figure 67: SIP Interface for PSTN Gateway and OnPrem PBX (Cont.)



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-interface**
- sip-manipulation
- sip-monitoring
- translation-rules
- system

Modify SIP Interface

SPL Options	<input type="text"/>	
Trust Mode	<input type="text" value="all"/>	
Max Nat Interval	<input type="text" value="3600"/>	(Range: 0..999999999)
Nat Int Increment	<input type="text" value="10"/>	(Range: 0..999999999)
Nat Test Increment	<input type="text" value="30"/>	(Range: 0..999999999)
SIP Dynamic Hnt	<input type="checkbox"/> enable	
TCP Max Nat Interval	<input type="text" value="3600"/>	(Range: 0..999999999)
TCP Nat Int Increment	<input type="text" value="10"/>	(Range: 0..999999999)
TCP Nat Test Increment	<input type="text" value="30"/>	(Range: 0..999999999)
TCP SIP Dynamic Hnt	<input type="checkbox"/> enable	
Stop Recurse	<input type="text" value="401,407"/>	
Port Map Start	<input type="text" value="0"/>	(Range: 0,1025..65535)
Port Map End	<input type="text" value="0"/>	(Range: 0,1025..65535)
In Manipulationid	<input type="text"/>	

Figure 68: SIP Interface for PSTN Gateway and OnPrem PBX (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-interface**
- sip-manipulation
- sip-monitoring
- translation-rules
- system

Modify SIP Interface

Out Manipulationid	<input type="text"/>	
SIP Atcf Feature	<input type="checkbox"/> enable	
Rfc2833 Payload	<input type="text" value="101"/>	(Range: 96..327)
Rfc2833 Mode	<input type="text" value="transparent"/>	
Response Map	<input type="text"/>	
Local Response Map	<input type="text"/>	
Sec Agree Feature	<input type="checkbox"/> enable	
Enforcement Profile	<input type="text"/>	
Emergency Dscp Profile	<input type="text"/>	
TCP Keepalive	<input type="text" value="none"/>	
Add SDP Invite	<input type="text" value="both"/>	
Add SDP In Msg	<input type="text"/>	
P Early Media Header	<input type="text" value="disabled"/>	
P Early Media Direction	<input type="text"/>	

Figure 69: SIP Interface for PSTN Gateway and OnPrem PBX (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-interface**
- sip-manipulation
- sip-monitoring
- translation-rules

Modify SIP Interface

Add SDP Profiles	<input type="text"/>
Add SDP Profiles In Msg	<input type="text"/>
SIP Profile	<input type="text" value=""/>
SIP Isup Profile	<input type="text" value=""/>
TCP Conn Dereg	<input type="text" value="0"/> (Range: 0..999999999)
Kpml Interworking	<input type="checkbox"/> enable
Kpml2833 Iwf On Hairpin	<input type="checkbox"/> enable
Msrp Delay Egress Bye	<input type="checkbox"/> enable
Send 380 Response	<input type="text"/>
Pscf Restoration	<input type="text"/>
Session Timer Profile	<input type="text" value=""/>
Session Recording Server	<input type="text"/>
Session Recording Required	<input type="checkbox"/> enable

Figure 70: SIP Interface for PSTN Gateway and OnPrem PBX (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-interface**
- sip-manipulation
- sip-monitoring
- translation-rules
- system

Modify SIP Interface

Session Recording Required	<input type="checkbox"/> enable
Service Tag	<input type="text"/>
Reg Cache Route	<input type="checkbox"/> enable
Diversion Info Mapping Mode	<input type="text" value="none"/>
Atcf Icsi Match	<input type="text"/>
SIP Recursion Policy	<input type="text" value=""/>
Asymmetric Preconditions	<input type="checkbox"/> enable
Asymmetric Preconditions Mode	<input type="text" value="send-with-nodelay"/>
Sm Icsi Match For Invite	<input type="text"/>
Sm Icsi Match For Message	<input type="text"/>
S8hr Profile	<input type="text" value=""/>
Ringback Trigger	<input type="text" value="none"/>
Ringback File	<input type="text"/>
Fax Continue Session	<input type="text" value="none"/>

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

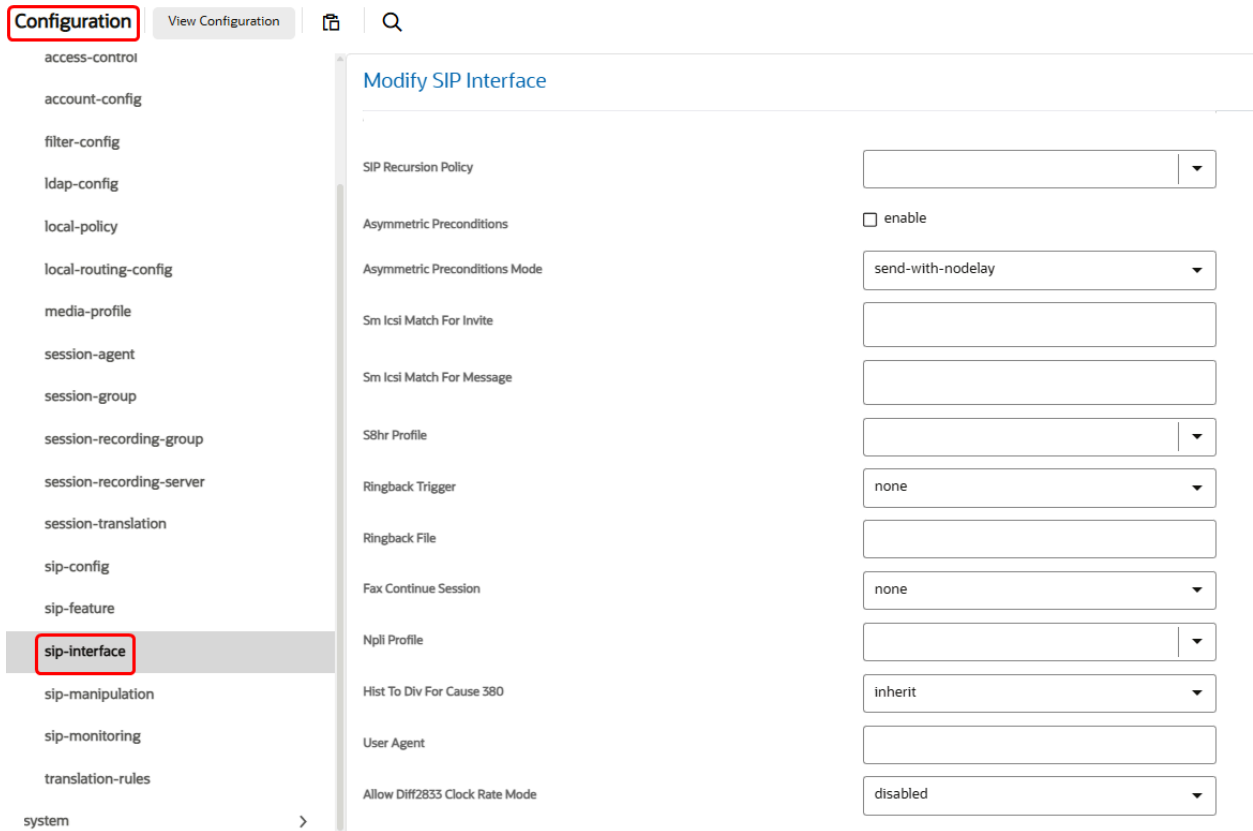


Figure 72: SIP Interface for PSTN Gateway and OnPrem PBX (Cont.)

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

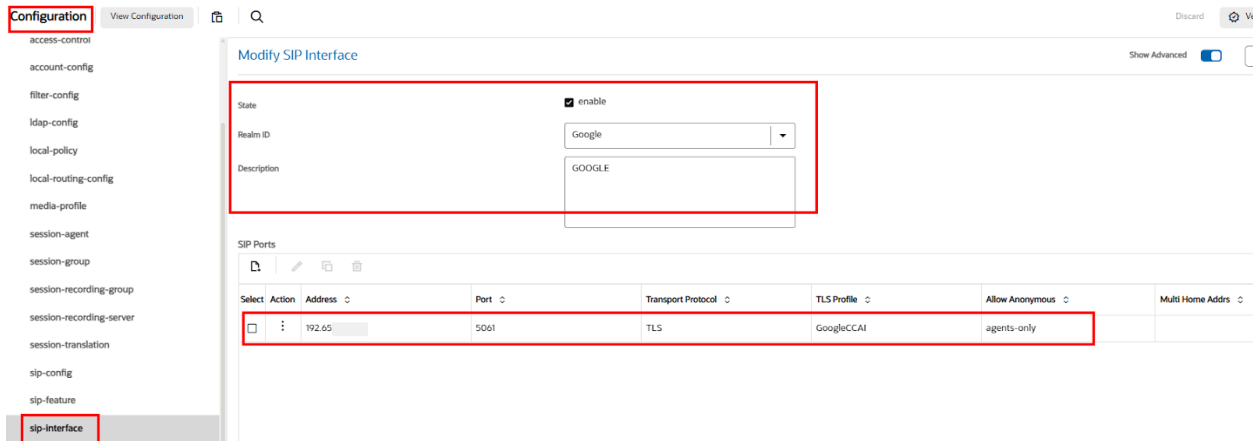




Figure 73: SIP Interface for Google CES



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**

Modify SIP Interface

Initial Inv Trans Expire	<input type="text" value="0"/>	(Range: 0..2147473)
Session Max Life Limit	<input type="text" value="0"/>	
Proxy Mode	<input type="text"/>	
Redirect Action	<input type="text"/>	
Nat Traversal	<input type="text" value="none"/>	
Nat Interval	<input type="text" value="30"/>	(Range: 1..999999999)
TCP Nat Interval	<input type="text" value="90"/>	(Range: 0..999999999)
Registration Caching	<input checked="" type="checkbox"/> enable	
Min Reg Expire	<input type="text" value="300"/>	(Range: 0..999999999)
Registration Interval	<input type="text" value="3600"/>	(Range: 1..999999999)
Route To Registrar	<input checked="" type="checkbox"/> enable	
Secured Network	<input type="checkbox"/> enable	
Uri Fqdn Domain	<input type="text"/>	
Options	<input type="text"/>	

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

Configuration View Configuration  

- media-manager** >
- security >
- session-router ▾
- access-control
- account-config
- filter-config
- ldap-config
- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config
- sip-feature
- sip-interface**
- sip-manipulation
- sip-monitoring
- translation-rules

Modify SIP Interface

Trust Mode	<input type="text" value="all"/>	
Max Nat Interval	<input type="text" value="3600"/>	(Range: 0..999999999)
Nat Int Increment	<input type="text" value="10"/>	(Range: 0..999999999)
Nat Test Increment	<input type="text" value="30"/>	(Range: 0..999999999)
SIP Dynamic Hnt	<input type="checkbox"/> enable	
TCP Max Nat Interval	<input type="text" value="3600"/>	(Range: 0..999999999)
TCP Nat Int Increment	<input type="text" value="10"/>	(Range: 0..999999999)
TCP Nat Test Increment	<input type="text" value="30"/>	(Range: 0..999999999)
TCP SIP Dynamic Hnt	<input type="checkbox"/> enable	
Stop Recurse	<input type="text" value="401,407"/>	
Port Map Start	<input type="text" value="0"/>	(Range: 0,1025..65535)
Port Map End	<input type="text" value="0"/>	(Range: 0,1025..65535)
In Manipulationid	<input type="text"/>	
Out Manipulationid	<input type="text"/>	
SIP Atcf Feature	<input type="checkbox"/> enable	
Rfc2833 Payload	<input type="text" value="101"/>	(Range: 96..127)

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

Configuration View Configuration

- access-control
- account-config
- filter-config
- ldap-config
- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config
- sip-feature
- sip-interface**
- sip-manipulation
- sip-monitoring
- translation-rules

Modify SIP Interface

Rfc2833 Mode	transparent
Response Map	
Local Response Map	
Sec Agree Feature	<input type="checkbox"/> enable
Enforcement Profile	
Emergency Dscp Profile	
TCP Keepalive	enabled
Add SDP Invite	disabled
Add SDP In Msg	
P Early Media Header	disabled
P Early Media Direction	
Add SDP Profiles	
Add SDP Profiles In Msg	

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

Configuration View Configuration

- media-manager >
- security >
- session-router** ▾
- access-control
- account-config
- filter-config
- ldap-config
- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config
- sip-feature
- sip-interface**
- sip-manipulation
- sip-monitoring
- translation-rules

Modify SIP Interface

TCP Conn Dereg (Range: 0.999999999)

KpmI Interworking enable

KpmI2833 Iwf On Hairpin enable

Msrp Delay Egress Bye enable

Send 380 Response

Pcscf Restoration

Session Timer Profile ▾

Session Recording Server

Session Recording Required enable

Service Tag

Reg Cache Route enable

Diversion Info Mapping Mode ▾

Atcf Icsi Match

SIP Recursion Policy ▾

Asymmetric Preconditions enable

Asymmetric Preconditions Mode ▾

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

Configuration View Configuration

- media-manager >
- security >
- session-router** ▾
- access-control
- account-config
- filter-config
- ldap-config
- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config
- sip-feature
- sip-interface**
- sip-manipulation
- sip-monitoring
- translation-rules

Modify SIP Interface

Reg Cache Route enable

Diversion Info Mapping Mode ▾

Atcf Icsi Match

SIP Recursion Policy ▾

Asymmetric Preconditions enable

Asymmetric Preconditions Mode ▾

Sm Icsi Match For Invite

Sm Icsi Match For Message

SBhr Profile ▾

Ringback Trigger ▾

Ringback File

Fax Continue Session ▾

Npli Profile ▾

Hist To Div For Cause 380 ▾

User Agent

Allow Diff2833 Clock Rate Mode ▾

Figure 78: 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 Oracle E-SBC with direct access to trusted data path.
- Navigate to **Configuration** > **session-router** > **session-agent**.
- Configure Session Agent for PSTN Gateway, OnPrem PBX and Google CES.

Configure the Session Agent for Google CES as shown below.

Select	Action	Hostname	IP Address	Port	State	App Protocol	Realm ID	Description
<input type="checkbox"/>	⋮	10.64.	10.64	5060	enabled	SIP	PSTN	
<input type="checkbox"/>	⋮	172.16.	172.16.	5060	enabled	SIP	PSTN	Free PBX 1
<input type="checkbox"/>	⋮	us.telephony.goog		5672	enabled	SIP	Google	

Figure 79: Session Agent

Modify Session Agent

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]

Description: [Empty]

Figure 80: Session Agent for Google CES

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

Associated Agents

Constraints enable

Max Sessions (Range: 0.999999999)

Max Inbound Sessions (Range: 0.999999999)

Max Outbound Sessions (Range: 0.999999999)

Max Burst Rate (Range: 0.999999999)

Max Inbound Burst Rate (Range: 0.999999999)

Max Outbound Burst Rate (Range: 0.999999999)

Max Sustain Rate (Range: 0.999999999)

Max Inbound Sustain Rate (Range: 0.999999999)

Max Outbound Sustain Rate (Range: 0.999999999)

Min Asr (Range: 0.100)

Cac Trap Threshold (Range: 0.99)

Session Max Life Limit

Time To Resume (Range: 0.999999999)

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

Configuration View Configuration 🔍

security >

session-router ▾

access-control

account-config

filter-config

ldap-config

local-policy

local-routing-config

media-profile

session-agent

session-group

session-recording-group

session-recording-server

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

system >

Modify Session Agent

In Service Period (Range: 0.999999999)

Burst Rate Window (Range: 0.999999999)

Sustain Rate Window (Range: 0.999999999)

Max Inbound Per Session Burst Rate (Range: 1.999999999)

Burst Rate Window Per Session (Range: 1.999999999)

Dos Action At Session

Proxy Mode

Redirect Action

Loose Routing enable

Response Map

Ping Method

Ping Interval (Range: 0.999999999)

Ping Send Mode

Ping All Addresses enable

Ping In Service Response Codes

Load Balance DNS Query

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

Configuration View Configuration

- security
 - session-router
 - access-control
 - account-config
 - filter-config
 - ldap-config
 - local-policy
 - local-routing-config
 - media-profile
 - session-agent
 - session-group
 - session-recording-group
 - session-recording-server

Modify Session Agent

Options:

SPL Options:

Media Profiles:

In Session Translations

No in session translation list to display. Please add.

Out Session Translations

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

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

Configuration View Configuration

- media-manager
- security
- session-router
 - access-control
 - account-config
 - filter-config
 - ldap-config
 - local-policy
 - local-routing-config
 - media-profile
 - session-agent
 - session-group
 - session-recording-group
 - session-recording-server
 - session-translation
 - sip-config
 - sip-feature
 - sip-interface
 - sip-manipulation
 - sip-monitoring
 - translation-rules

Modify Session Agent

Trust Me: enable

Stop Recurse:

Local Response Map:

Ping Response: enable

In Manipulationid:

Out Manipulationid:

Manipulation String:

Manipulation Pattern:

Trunk Group:

Max Register Sustain Rate: (Range: 0.0000000000)

Invalidate Registrations: enable

Rfc2833 Mode:



Rfc2833 Payload: (Range: 0.06.127)

Codec Policy:

Emergency Dscp Profile:

Refer Call Transfer:

Figure 84: 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

Modify Session Agent



Refer Notify Provisional	<input type="text" value="none"/>	
Reuse Connections	<input type="text" value="NONE"/>	
TCP Keepalive	<input type="text" value="enabled"/>	
TCP Reconn Interval	<input type="text" value="60"/>	(Range: 0,2..300)
Max Register Burst Rate	<input type="text" value="0"/>	(Range: 0..999999999)

Rate Constraints

No rate constraints to display. Please add.

SIP Profile	<input type="text"/>	▾
SIP Isup Profile	<input type="text"/>	▾
Kpml Interworking	<input type="text" value="inherit"/>	▾
Kpml2853 Iwf On Hairpin	<input type="text" value="inherit"/>	▾
Precedence	<input type="text" value="0"/>	(Range: 0..4294967295)
Monitoring Filters	<input type="text"/>	

Figure 85: 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

Auth Attribute

No auth attributes to display. Please add.

Session Recording Server	<input type="text"/>
Session Recording Required	<input type="checkbox"/> enable
Hold Refer Reinvite	<input type="checkbox"/> enable
Send TCP Fin	<input type="checkbox"/> enable
SIP Recursion Policy	<input type="text"/>
Sm Icsi Match For Invite	<input type="text"/>
Sm Icsi Match For Message	<input type="text"/>
Ringback Trigger	<input type="text" value="none"/>
Ringback File	<input type="text"/>
Fax Servers	<input type="text"/>
Trigger Oos Alarm	<input type="checkbox"/> enable
Static TCP Source Port	<input type="text" value="0"/> (Range: 0,1025..65535)

Figure 86: Session Agent for Google CES (Cont.)

- Configure the Session Agent for OnPrem PBX as shown below.

Configuration View Configuration

session-agent

Modify Session Agent

Hostname: 172.16. (Range: 0,1025..65535)

IP Address: 172.16.

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

State: enable

App Protocol: SIP

App Type: (empty)

Transport Method: StaticTCP

Realm ID: PSTN

Egress Realm ID: (empty)

Description: Free PBX 1

Figure 87: Session Agent for OnPrem PBX

Configuration View Configuration

session-agent

Modify Session Agent

Associated Agents: (empty)

Constraints: enable

Max Sessions: 0 (Range: 0..999999999)

Max Inbound Sessions: 0 (Range: 0..999999999)

Max Outbound Sessions: 0 (Range: 0..999999999)

Max Burst Rate: 0 (Range: 0..999999999)

Max Inbound Burst Rate: 0 (Range: 0..999999999)

Max Outbound Burst Rate: 0 (Range: 0..999999999)

Max Sustain Rate: 0 (Range: 0..999999999)

Max Inbound Sustain Rate: 0 (Range: 0..999999999)

Max Outbound Sustain Rate: 0 (Range: 0..999999999)

Min Asr: 0 (Range: 0..100)

Cac Trap Threshold: 0 (Range: 0..99)

Session Max Life Limit: 0

Time To Resume: 0 (Range: 0..999999999)

Figure 88: Session Agent for 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
 - sip-manipulation
 - sip-monitoring
 - translation-rules

Modify Session Agent

Trust Me enable

Stop Recurse

Local Response Map

Ping Response enable

In Manipulationid

Out Manipulationid

Manipulation String

Manipulation Pattern

Trunk Group

Max Register Sustain Rate (Range: 0.999999999)

Invalidate Registrations enable

Rfc2833 Mode

Rfc2833 Payload (Range: 0,96.127)

Codec Policy

Emergency Dscp Profile

Refer Call Transfer

Figure 89: 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

Modify Session Agent

Reuse Connections

TCP Keepalive

TCP Reconn Interval (Range: 0.2-300)

Max Register Burst Rate (Range: 0.999999999)

Rate Constraints

No rate constraints to display. Please add.

SIP Profile

SIP Isup Profile

Kpml Interworking



Kpml2833 Iwf On Hairpin

Precedence (Range: 0.4294967295)

Monitoring Filters

Auth Attribute

Figure 90: 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

Auth Attribute

No auth attributes to display. Please add.

Session Recording Server	<input type="text"/>
Session Recording Required	<input type="checkbox"/> enable
Hold Refer Reinvite	<input type="checkbox"/> enable
Send TCP Fin	<input type="checkbox"/> enable
SIP Recursion Policy	<input type="text" value=""/> ▾
Sm Icsi Match For Invite	<input type="text"/>
Sm Icsi Match For Message	<input type="text"/>
Ringback Trigger	none ▾
Ringback File	<input type="text"/>
Fax Servers	<input type="text"/>
Trigger Oos Alarm	<input type="checkbox"/> enable
Static TCP Source Port	<input type="text" value="0"/> (Range: 0,1025..65535)

Figure 91: Session Agent for OnPrem PBX (Cont.)

- Configure the Session agent for PSTN Gateway 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

sip-config

sip-feature

Modify Session Agent

Hostname: 10.64

IP Address: 10.64

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

State: enable

App Protocol: SIP

App Type: []

Transport Method: StaticTCP

Realm ID: PSTN

Egress Realm ID: PSTN

Description: []

Figure 92: Session Agent for PSTN Gateway

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

Associated Agents: []

Constraints: enable

Max Sessions: 0 (Range: 0..999999999)

Max Inbound Sessions: 0 (Range: 0..999999999)

Max Outbound Sessions: 0 (Range: 0..999999999)

Max Burst Rate: 0 (Range: 0..999999999)

Max Inbound Burst Rate: 0 (Range: 0..999999999)

Max Outbound Burst Rate: 0 (Range: 0..999999999)

Max Sustain Rate: 0 (Range: 0..999999999)

Max Inbound Sustain Rate: 0 (Range: 0..999999999)

Max Outbound Sustain Rate: 0 (Range: 0..999999999)

Min Asr: 0 (Range: 0..100)

Cac Trap Threshold: 0 (Range: 0..99)

Session Max Life Limit: 0

Time To Resume: 0 (Range: 0..999999999)

Figure 93: Session Agent for PSTN Gateway (Cont.)

Configuration View Configuration

- media-manager >
- security >
- session-router >
 - access-control
 - account-config
 - filter-config
 - ldap-config
 - local-policy
 - local-routing-config
 - media-profile
 - session-agent**
 - session-group
 - session-recording-group
 - session-recording-server
 - session-translation
 - sip-config
 - sip-feature
 - sip-interface
 - sip-manipulation
 - sip-monitoring
 - translation-rules

Modify Session Agent

Trust Me	<input type="checkbox"/> enable
Stop Recurse	<input type="text"/>
Local Response Map	<input type="text"/>
Ping Response	<input checked="" type="checkbox"/> enable
In Manipulationid	<input type="text"/>
Out Manipulationid	<input type="text"/>
Manipulation String	<input type="text"/>
Manipulation Pattern	<input type="text"/>
Trunk Group	<input type="text"/>
Max Register Sustain Rate	<input type="text" value="0"/> (Range: 0.999999999)
Invalidate Registrations	<input type="checkbox"/> enable
Rfc2833 Mode	<input type="text" value="none"/>
Rfc2833 Payload	<input type="text" value="0"/> (Range: 0,96.127)
Codec Policy	<input type="text"/>
Emergency Dscp Profile	<input type="text"/>
Refer Call Transfer	<input type="text" value="disabled"/>

Figure 94: Session Agent for PSTN Gateway (Cont.)

Configuration View Configuration

- security >
- session-router** >
 - access-control
 - account-config
 - filter-config
 - ldap-config
 - local-policy
 - local-routing-config
 - media-profile
 - session-agent**
 - session-group
 - session-recording-group
 - session-recording-server
 - session-translation
 - sip-config
 - sip-feature
 - sip-interface
 - sip-manipulation

Modify Session Agent

Reuse Connections	<input type="text" value="NONE"/>
TCP Keepalive	<input type="text" value="disabled"/>
TCP Reconn Interval	<input type="text" value="0"/> (Range: 0.2-300)
Max Register Burst Rate	<input type="text" value="0"/> (Range: 0.999999999)
Rate Constraints	
No rate constraints to display. Please add.	
<input type="button" value="Add"/>	
SIP Profile	<input type="text"/>
SIP Isup Profile	<input type="text"/>
Kpml Interworking	<input type="text" value="inherit"/>
Kpml2833 Iwf On Hairpin	<input type="text" value="inherit"/>
Precedence	<input type="text" value="0"/> (Range: 0.4294967295)
Monitoring Filters	<input type="text"/>
Auth Attribute	<input type="text"/>

Figure 95: Session Agent for PSTN Gateway (Cont.)

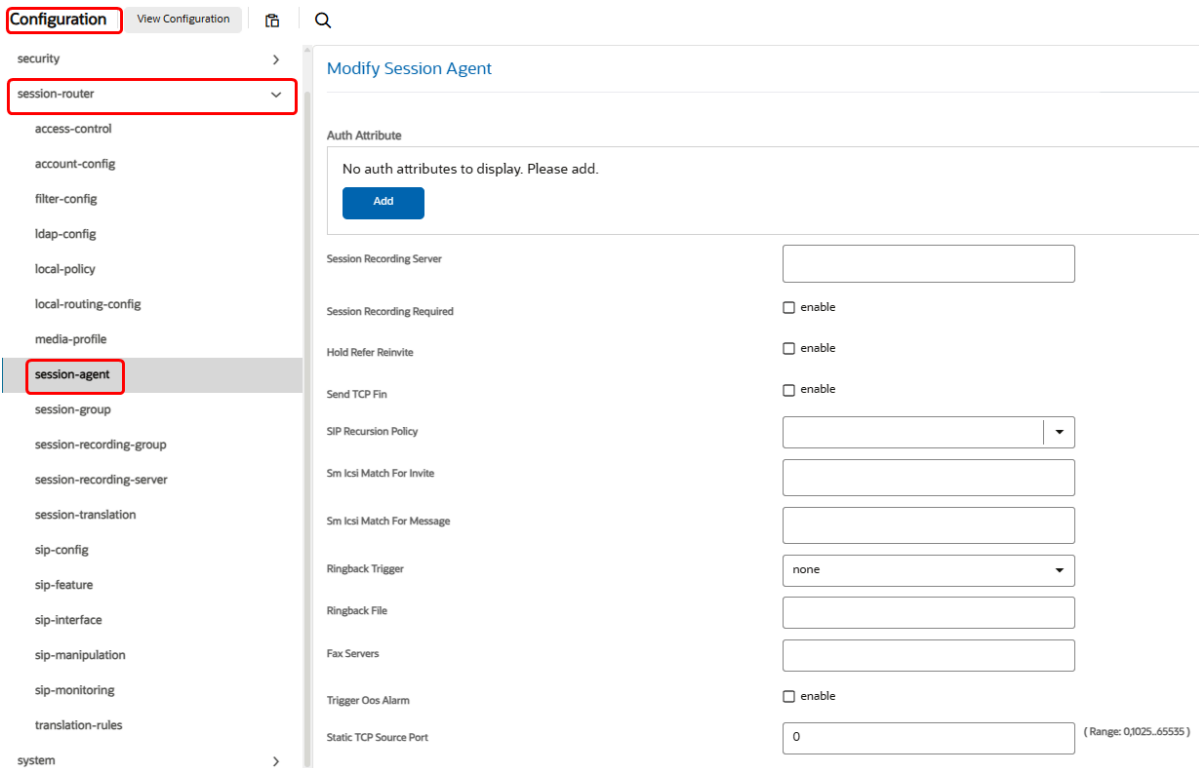


Figure 96: Session Agent for PSTN Gateway (Cont.)

7.4.21 Local Policy

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

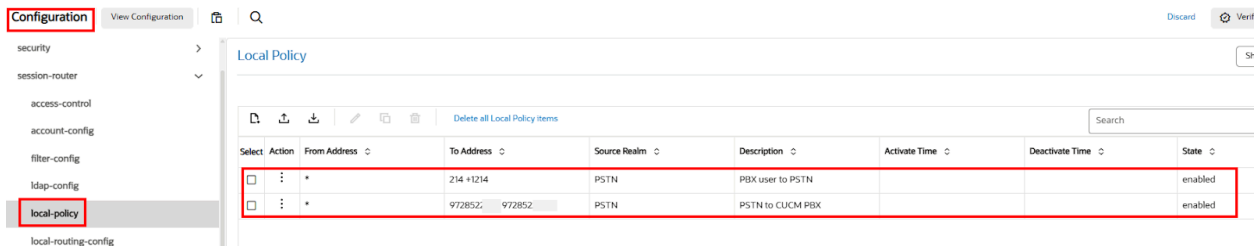


Figure 97: Local Policy

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

Configuration View Configuration

session-router

local-policy

Modify Local Policy Entries

From Address: * x

To Address: 214 x +1214 x

Source Realm: PSTN x

Description: PBX user to PSTN

State: enable

Parallel Forking: enable

Policy Priority: none

Select	Action	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
<input type="checkbox"/>	:	10.64	PSTN	none	disabled	0	enabled	SIP	single	

Figure 98: Local Policy routing from OnPrem PBX to PSTN Gateway

Configuration View Configuration

session-router

local-policy

Modify Local policy / policy attribute

Next Hop: 10.64

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 99: Local Policy routing attributes towards PSTN Gateway

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

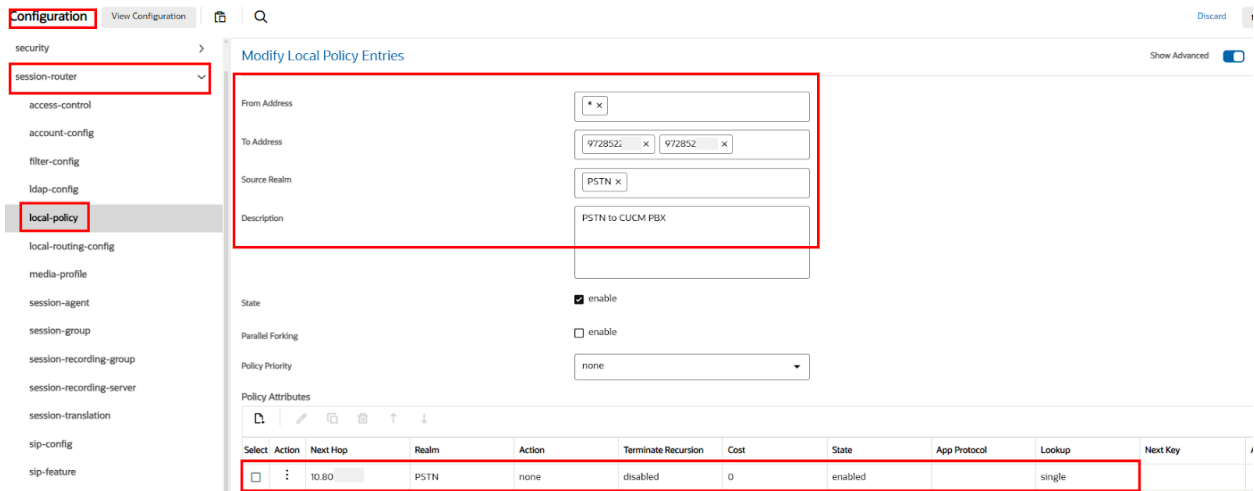


Figure 100: Local Policy routing Towards OnPrem PBX from PSTN Gateway

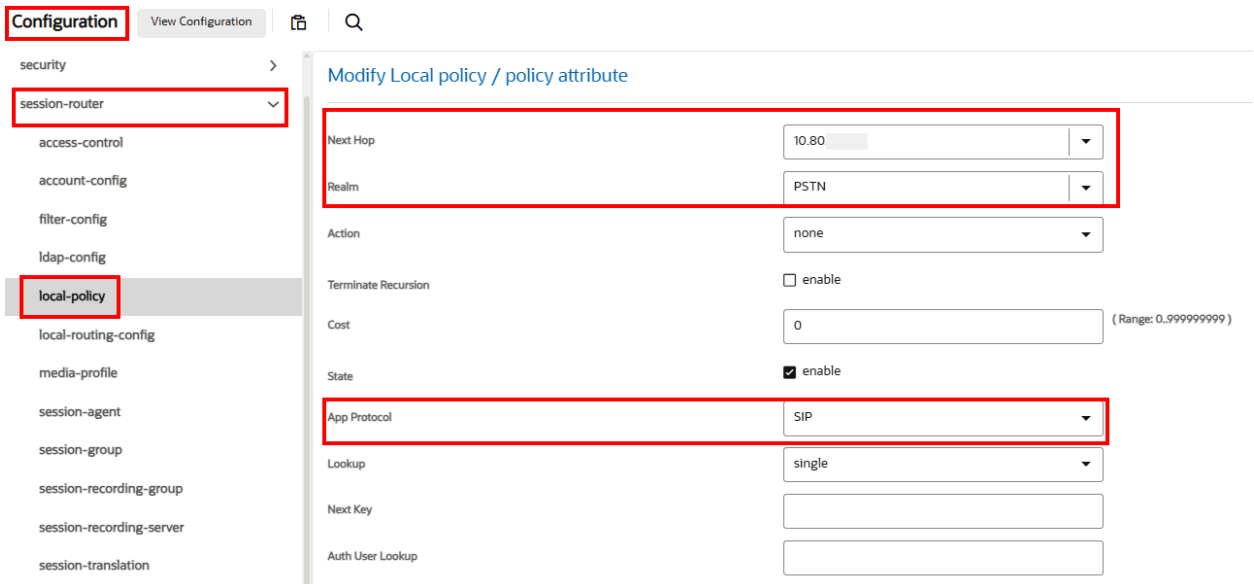


Figure 101: Local Policy routing attributes towards OnPrem PBX

7.4.22 SIP Manipulation

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

The screenshot shows the configuration page for SIP Manipulation. The left sidebar has 'Configuration' selected, and 'sip-manipulation' is highlighted in the tree. The main area is titled 'Modify SIP Manipulation'. The 'Name' field is 'GoogleManipulation' and the 'Description' is 'Manipulation on google side'. Below these are fields for 'Split Headers' and 'Join Headers'. The 'CfgRules' section contains a table of rules:

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

Figure 102: SIP Manipulation towards Google CES

- Add a header-rule for Google CES.

The screenshot shows the configuration page for SIP Manipulation with 'session-router' selected in the sidebar. The 'CfgRules' table is expanded, and the 'Add' button is highlighted. A dropdown menu is open, showing 'header-rule' as the selected option. The table below shows the updated list of rules:

Action	Name	Element Type
:	uri	header-rule
:	mime-rule	header-rule
:	mime-lsup-rule	header-rule
:	Rihost	header-rule
:	iHeader	header-rule
:	changelocalport	header-rule
:	deltransport	header-rule
:	delete_callinfo	header-rule

Figure 103: Header rule addition for SIP Manipulation towards Google CES

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

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

Figure 104: SIP Manipulation towards Google CES Request URI

Configuration View Configuration

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

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 105: SIP Manipulation towards Google CES change Request URI-host

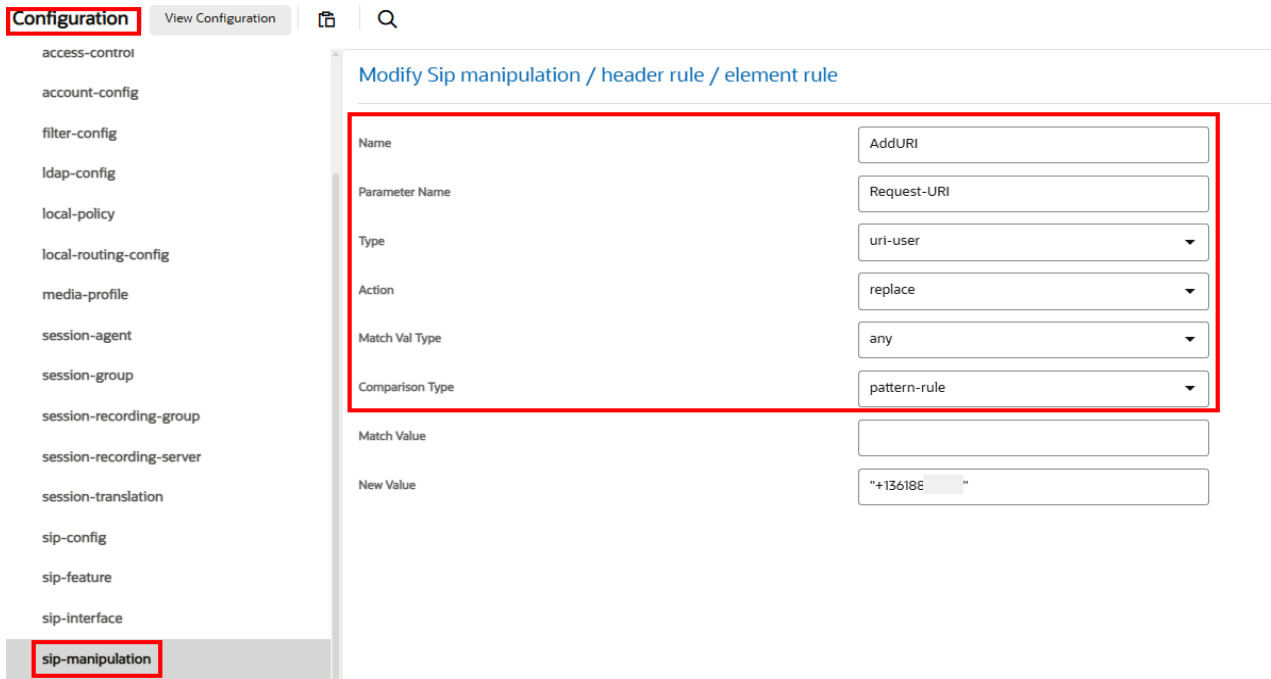


Figure 106: SIP Manipulation towards Google CES change Request URI-user

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

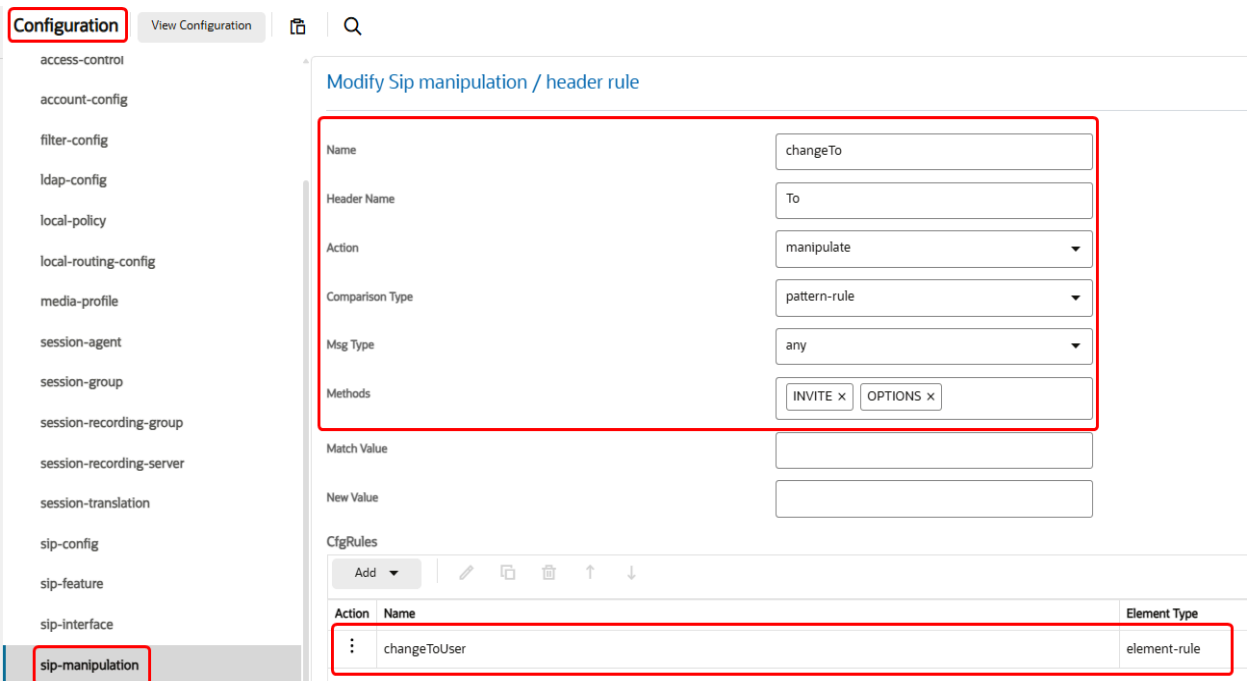




Figure 107: SIP Manipulation towards Google CES TO header

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	changeToUser
Parameter Name	To
Type	uri-user
Action	replace
Match Val Type	any
Comparison Type	case-sensitive
Match Value	
New Value	" +136188 "

Figure 108: SIP Manipulation towards Google CES – Change TO header user

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

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	<input type="text" value="AddCallInfoHeader"/>
Header Name	<input type="text" value="Call-info"/>
Action	<input type="text" value="add"/>
Comparison Type	<input type="text" value="case-sensitive"/>
Msg Type	<input type="text" value="any"/>
Methods	<input type="text" value="INVITE"/>
Match Value	<input type="text"/>
New Value	<input type="text" value="*http://dialogflow.googleapis.com/v2beta1/projec"/>

CfgRules

No rules to display. Please add.

Figure 109: SIP Manipulation towards Google CES – Add Call-Info

SIP Manipulation 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 the setup.
- Sample call-info header with participant roles:
- Call-info: "<http://dialogflow.googleapis.com/v2beta1/projects/ccai-389XX/conversations/O R_ "+\$CALL_ID.\$0+"?roles=HUMAN_AGENT,END_USER>;purpose=Goog-ContactCenter-Co nversation"

The screenshot shows a configuration page for SIP manipulation. The left sidebar lists various configuration categories, with 'sip-manipulation' selected. The main area is titled 'Modify Sip manipulation / header rule'. A form is used to define a rule:

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

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

Figure 110: 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 E-SBC during the creation of Conversation ID (this rule is applied only when Conversation on the Fly is set to True in Google CES).

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 ×
Match Value	^(<http://.*)(@us.telephony.google)(.*)\$
New Value	\$1+\$3

Figure 111: 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.

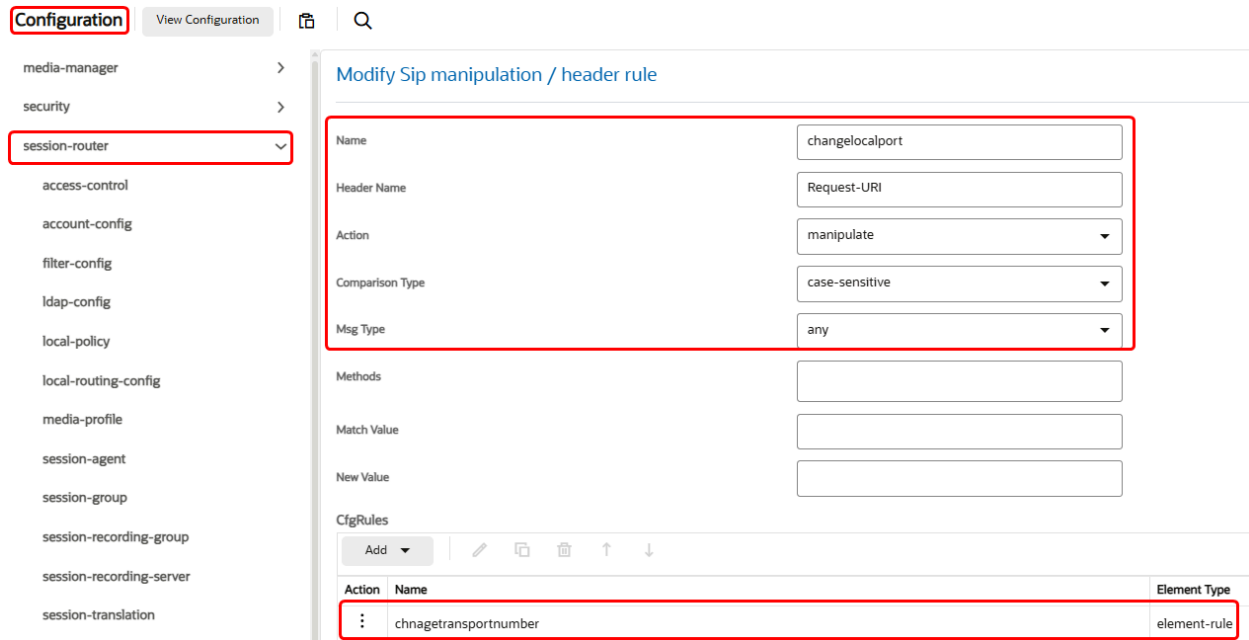


Figure 112: SIP Manipulation towards Google CES – Change Request URI Port number

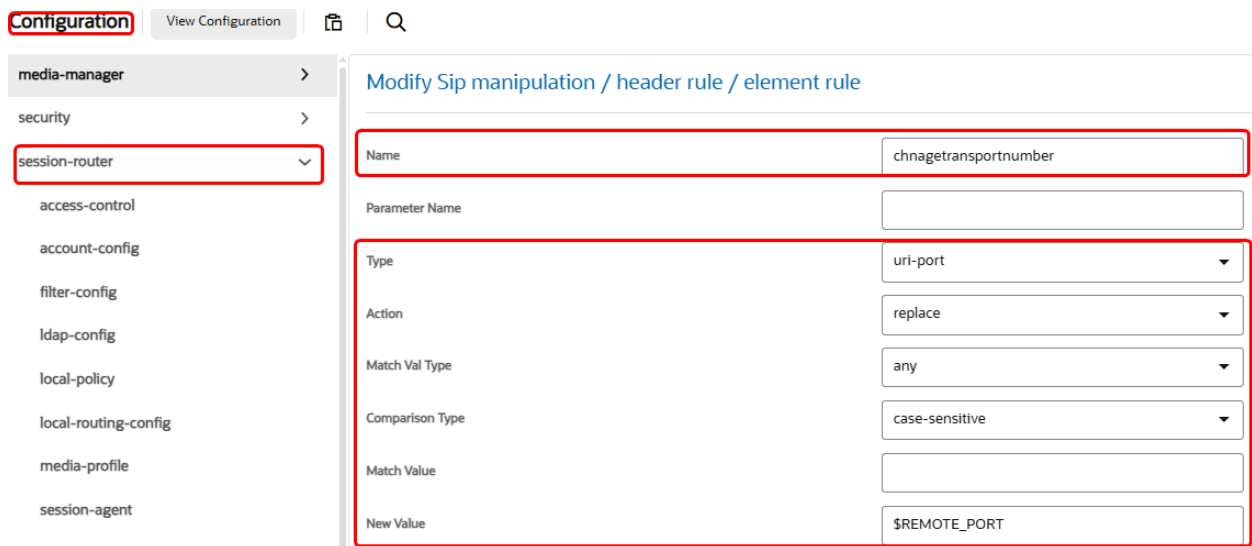


Figure 113: SIP Manipulation towards Google CES – Change Request URI Port number (Cont.)

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

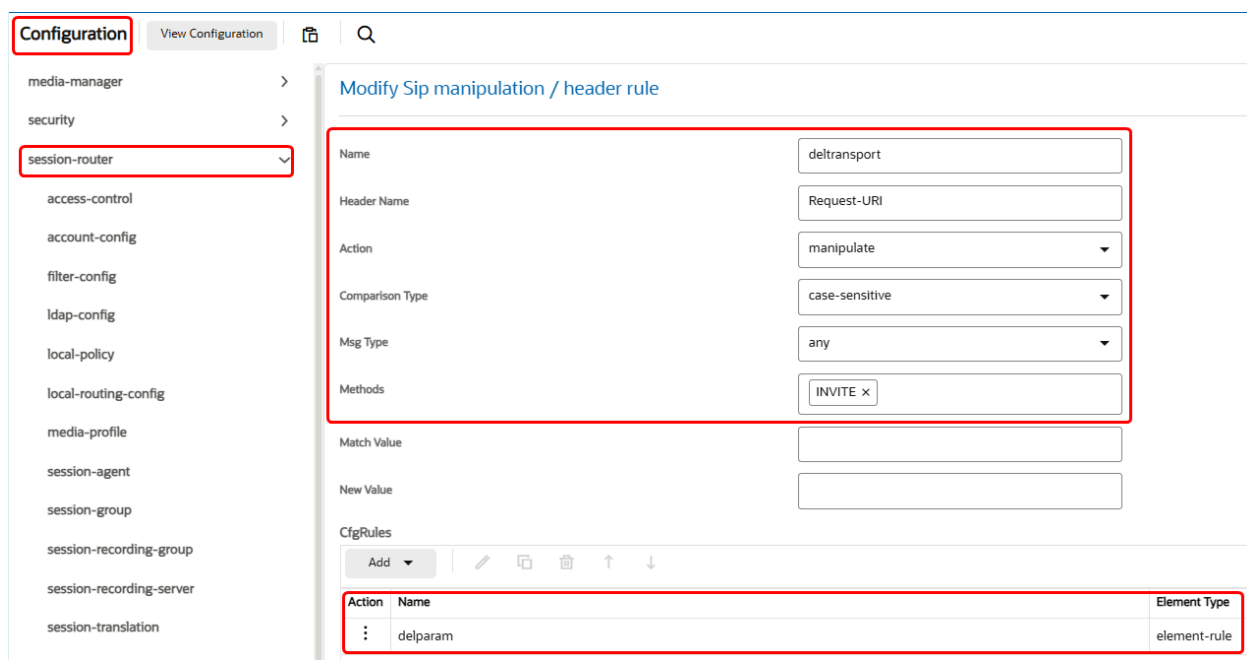


Figure 114: SIP Manipulation towards Google CES – Delete Transport parameter

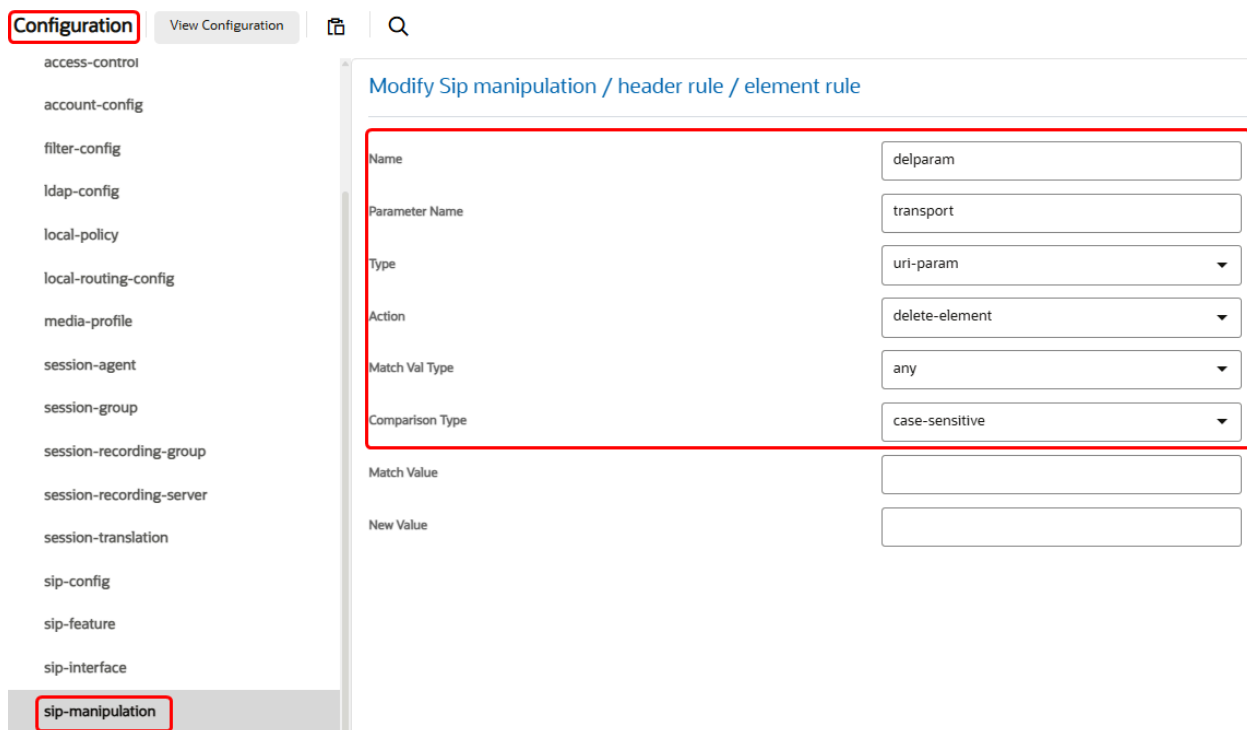


Figure 115: SIP Manipulation towards Google CES – Delete Transport parameter (Cont.)

8 SIP INVITE To GOOGLE CES

8.1 SIP INVITE for SIPREC call

```
INVITE sip:+13618.....@us.telephony.goog:5672 SIP/2.0
Via: SIP/2.0/TLS 192.65.....:5061;branch=29hg4BkqfF9nq103ov0tbubt2n0
From: sip:acmeSrc@192.65.....;tag=f04e824a0f617ddcbf1e98e90f7ead51
To: <sip:+13618.....@us.telephony.goog:5672>;transport=tcp>
Call-ID: 44dd70a5480470e9f5932cb3f578484d020@us.telephony.goog
CSeq: 1080 INVITE
Contact: <sip:acmeSrc@192.65.....:5061>;transport=tcp;+sip.src
Max-Forwards: 70
Require: siprec
Content-Type: multipart/mixed; boundary=unique-boundary-1
Content-Length: 2237
MIME-Version: 1.0
Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/ccai-38.../conversations/
OR_44d...:purpose=Goog-ContactCenter-Conversation
--unique-boundary-1
Content-Type: application/sdp

v=0
o=- 3562256 226213 IN IP4 192.65.....
s=-
c=IN IP4 192.65.....
t=0 0
m=audio 20910 RTP/SAVP 0 101
c=IN IP4 192.65.....
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=label:234881075
a=sendonly
a=crypto:1 AES_CM 128_HMAC_SHA1_80 inline:1ZbR91HLKuYJ8T4ejRWE1rWkdq4Zket0XmrtM8Jk
m=audio 20914 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=maxptime:150
a=label:234881076
a=sendonly
a=crypto:1 AES_CM 128_HMAC_SHA1_80 inline:aUYfgWeUmqFDSeCq65SVEu4muW9bdvNCmuqpaLiD
```

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

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

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

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

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

It must be a supported crypto suite by Google.

Figure 116: SIPREC Call

8.2 SIP INVITE for GTP call

```
INVITE sip:+13149.....@us.telephony.goog:5672 SIP/2.0
Via: SIP/2.0/TLS 192.65.....:5061;branch=29hg4BkqfF9nq103ov0tbubt2n0
From: <sip:+19728522631@192.65.....>;tag=d6de37c9-7561-4937-a8b9-0ca72644801a
To: <sip:+13149.....@us.telephony.goog>
Contact: <sip:9728522631@192.65.....: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, noferesub, histinfo
Session-Expires: 1800; refresher=uac
Min-SE: 90
Max-Forwards: 69
User-Agent: FPFX-16.0.40.13(20.4.0)
Content-Type: application/sdp
Content-Length: 405
Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/ccai-389.../conversations/
OR_02e...:purpose=Goog-ContactCenter-Conversation
--unique-boundary-1
Content-Type: application/sdp

v=0
o=- 1738828058 1738828058 IN IP4 192.65.....
s=Asterisk
c=IN IP4 192.65.....
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:ydaFiGf4WVGacrEmG0HNx9d1V8cWoG0fdwG0x0P5
```

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

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

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

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 117: GTP Call

9 Oracle E-SBC Running configuration file

Attached is the Oracle E-SBC running configuration file.



Google_SIPREC_Running Config

10 Summary of Tests and Results

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
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

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
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 APPLICABLE	

Inbound

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
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	

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
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 scenarios. Call starts out inactive for both participants; session moves to active	Validate if media is present when expected, confirm signaling events modify sdp properly, once call is move to active validate media and transcripts	PASSED	Call recording 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	Update is not sent, rather re-INVITE 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	re-INVITE 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	re-INVITE is sent to Google CES as part of session refresh, hold scenarios

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
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 requirements, record all leg.	Determine requirements , record all legs	PASSED	
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	

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
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 hold scenarios using A-law as codec	Call starts out inactive for both participants; session moves to active	Inbound call hold scenarios using A-law as codec	PASSED	
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	re-INVITE 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

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
31	Participant Labels test	Configure call info header to specify roles, ensure the media streams align	"Frist media stream HUMAN_AGENT role and	PASSED	<p>When the roles are set to "HUMAN AGENT" and "END USER," Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/cai-3898XX/conversations/OR_XX X?roles=HUMAN_AGENT,END_USER>;purpose=Google-ContactCenter-Conversation the transcript shows the first media stream with the participation role as "HUMAN AGENT," followed by "END USER."</p> <p>The transcript indicates that HUMAN AGENT was listed first, followed by the END USER, in 5 out of 10 attempts.</p>
32	DTLS test			NOT APPLICABLE	
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	