

Configuration Guide for Google
CES Agent Handoff Using
AudioCodes VE SBC
7.60A.100.022



Table of Contents

1	Audience	3
1.1	Introduction.....	3
1.1.1	TekVizionLabs	3
2	SIP Trunking Network Components	4
3	Hardware Components	5
4	Software Requirements	5
5	Certified AudioCodes VE SBC Version	5
6	Features	5
6.1	Caveats and Limitations.....	5
6.2	Failed Testcase.....	5
7	Configuration	6
7.1	Configuration Checklist.....	6
7.2	IP Address Worksheet.....	7
7.3	Google CES API Configuration.....	8
7.4	AudioCodes VE SBC Configuration.....	9
7.4.1	Network Interface IP	9
7.4.1.1	Configure LAN and WAN VLANs	9
7.4.1.2	Configure Network Interfaces	9
7.4.2	Configure TLS Context for Google CES	10
7.4.2.1	Create a TLS Context for Google CES 10	
7.4.2.2	Generate a CSR and Obtain the Certificate from a Supported CA	11
7.4.2.3	Upload the AudioCodes VE SBC Certificate	12
7.4.2.4	Upload Google Trusted Root Certificate	14
7.4.3	Configure Media Realms	14
7.4.4	Configure SIP Signaling Interfaces	15
7.4.5	Configure Proxy Sets and Proxy Address	17
7.4.6	Configure Coders	19
7.4.7	Configure IP Profiles	21
7.4.8	Configure IP Groups	25
7.4.9	Configure Media Security	28
7.4.10	Configure IP to IP Call Routing	28
7.4.11	Configure Message Manipulation Rules	29
8	SIP INVITE To GOOGLE CES	34
8.1	SIP INVITE for SIPREC call	34
8.2	SIP INVITE for GTP call	34
9	AudioCodes VE SBC Running configuration	35
10	Summary of Tests and Results	36

1 Audience

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

1.1 Introduction

This configuration guide describes configuration steps for **Google CES Agent Handoff** using **AudioCodes VE SBC 7.60A.100.022**.

1.1.1 TekVizionLabs

TekVizionLabs™ 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 Centre, is located in Plano, Texas.

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

2 SIP Trunking Network Components

The network for the SIP Trunk reference configuration is illustrated below and is representative of Google CES Agent Handoff with AudioCodes VE SBC 7.60A.100.022.

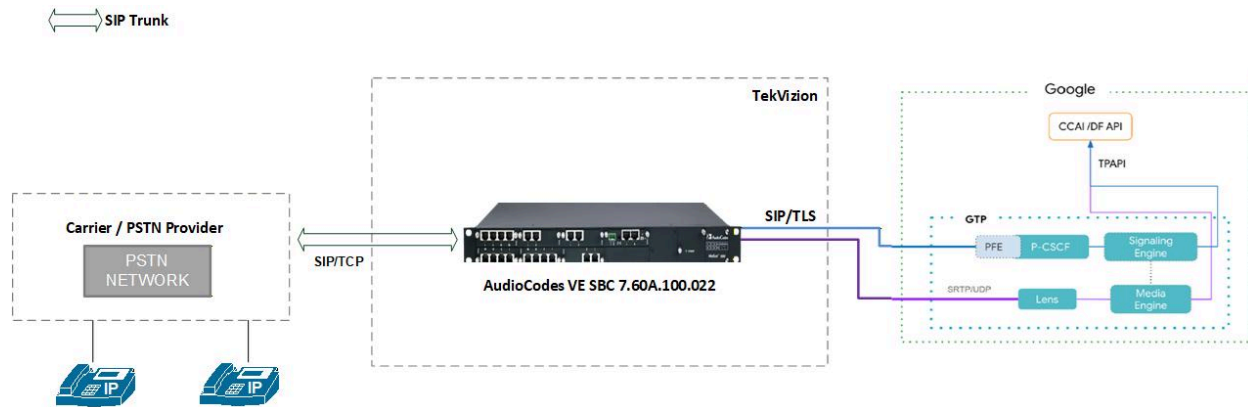


Figure 1: SIP Trunk Lab Reference Network

The lab network consists of the following components:

- Google CES cloud Environment
- AudioCodes VE SBC 7.60A.100.022
- PSTN Gateway

3 Hardware Components

- AudioCodes VE SBC running on ESXi host version 6.7.0

4 Software Requirements

- AudioCodes VE SBC version: 7.60A.100.022

5 Certified AudioCodes VE SBC Version

Table 1 – AudioCodes VE SBC Versions

Google CES - Verified version	
AudioCodes VE SBC	7.60A.100.022

6 Features

6.1 Caveats and Limitations

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

6.2 Failed Testcase

- None

7 Configuration

7.1 Configuration Checklist

Below are the steps that are required to configure AudioCodes VE SBC.

Table 2 – AudioCodes VE SBC Configuration Steps

Step	Description	Reference
Step 1	Network Interface IP	Section 7.4.1
Step 2	Configure TLS Context for Google CES	Section 7.4.2
Step 3	Configure Media Realms	Section 7.4.3
Step 4	Configure SIP Signaling Interfaces	Section 7.4.4
Step 5	Configure Proxy Sets and Proxy Address	Section 7.4.5
Step 6	Configure Coders	Section 7.4.6
Step 7	Configure IP Profiles	Section 7.4.7
Step 8	Configure IP Groups	Section 7.4.8
Step 9	Configure Media Security	Section 7.4.9
Step 10	Configure IP to IP Call Routing	Section 7.4.10
Step 11	Configure Message Manipulation Rules	Section 7.4.11

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
AudioCodes VE SBC	
LAN IP Address	10.80.X.X
WAN IP Address	192.65.X.X

7.3 Google CES API Configuration

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

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

7.4 AudioCodes VE SBC Configuration

The following is the configuration of AudioCodes VE SBC for Google CES Agent Handoff.

7.4.1 Network Interface IP

- Navigate to **SETUP** menu ☐ **IP NETWORK** tab ☐ **CORE ENTITIES** folder ☐ **IP Interfaces**.
- Configure IP Interfaces for PSTN Gateway and Google CES as shown below.

The screenshot shows the AudioCodes VE SBC configuration interface. The 'SETUP' menu is selected, and the 'IP NETWORK' tab is active. Under 'CORE ENTITIES', the 'IP Interfaces (2)' folder is selected. The table displays two IP interfaces:

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	PSTN	OAMP + Media + Cont	IPv4 Manual	10.80.11.48	24	10.80.11.1	10.85.0.12	0.0.0.0	vlan1
2	Google CCAI	Media + Control	IPv4 Manual	192.65	27	192.65	8.8.8.8	0.0.0.0	vlan2

Figure 2: IP Interfaces

7.4.1.1 Configure LAN and WAN VLANs

- Navigate to **SETUP** menu ☐ **IP NETWORK** tab ☐ **CORE ENTITIES** folder ☐ **Ethernet Devices**.
- Configure VLANs for LAN and WAN interfaces as shown below.

The screenshot shows the AudioCodes VE SBC configuration interface. The 'SETUP' menu is selected, and the 'IP NETWORK' tab is active. Under 'CORE ENTITIES', the 'Ethernet Devices (2)' folder is selected. The table displays two Ethernet devices:

INDEX	NAME	VLAN ID	UNDERLYING INTERFACE	TAGGING	MTU
0	LAN	1	GROUP_1	Untagged	1500
1	WAN	1	GROUP_2	Untagged	1500

Figure 3: VLAN Configuration

7.4.1.2 Configure Network Interfaces

- Navigate to **SETUP** menu ☐ **IP NETWORK** tab ☐ **CORE ENTITIES** folder ☐ **IP Interfaces**.
- Configure the IP Network interfaces for PSTN Gateway and Google CES as shown below.

The screenshot shows the AudioCodes VE SBC configuration interface. The 'SETUP' menu is selected, and the 'IP NETWORK' tab is active. Under 'CORE ENTITIES', the 'IP Interfaces (2)' folder is selected. The table displays two IP interfaces:

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	PSTN	OAMP + Media + Cont	IPv4 Manual	10.80.11.48	24	10.80.11.1	10.85.0.12	0.0.0.0	vlan1
2	Google CCAI	Media + Control	IPv4 Manual	192.65	27	192.65	8.8.8.8	0.0.0.0	vlan2

Figure 4: Network Interface Configuration

7.4.2 Configure TLS Context for Google CES

To establish a secure TLS connection between the AudioCodes VE SBC and Google CES, the TLS context must be configured accordingly.

7.4.2.1 Create a TLS Context for Google CES

- Navigate to **SETUP** menu ☐ **IP NETWORK** tab ☐ **SECURITY** folder ☐ **TLS Contexts**.
- Configure TLS context for Google CES as shown below.

The screenshot shows the AudioCodes Mediant VE SBC configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows 'CORE ENTITIES' with 'SECURITY' expanded to 'TLS Contexts (2)'. The main area displays a table of TLS Contexts:

INDEX	NAME	TLS VERSION	DTLS VERSION	CIPHER SERVER
0	Default	TLSv1.0 TLSv1.1 and TLSv1.2	DTLSv1.0 and DTLSv1.2	DEFAULT
1	Google CCAI	TLSv1.2	DTLSv1.0 and DTLSv1.2	DEFAULT

Figure 5: TLS Context for Google CES

The screenshot shows the detailed configuration for the 'Google CCAI' TLS Context. The 'GENERAL' tab is active, and the 'OCSP' tab is also visible. The configuration includes:

- Index: 1
- Name: Google CCAI
- TLS Version: TLSv1.2
- DTLS Version: DTLSv1.0 and DTLSv1.2
- Cipher Server: DEFAULT
- Cipher Client: DEFAULT
- Cipher Server TLS 1.3: TLS_AES_256_GCM_SHA384:TLS_CHACHA20_P
- Cipher Client TLS 1.3: TLS_AES_256_GCM_SHA384:TLS_CHACHA20_P
- Key Exchange Groups: X25519:P:256:P-384:X448
- Strict Certificate Extension Validation: Disable
- DH key Size: 2048
- TLS Renegotiation: Enable
- Use default CA Bundle: Disable

The 'OCSP' tab shows the following configuration:

- OCSP Server: Disable
- OCSP Interface: --
- Primary OCSP Server: 0.0.0.0
- Secondary OCSP Server: 0.0.0.0
- OCSP Port: 2560
- OCSP Default Response: Reject

Figure 6: TLS Context for Google CES (Cont.)

7.4.2.2 Generate a CSR and Obtain the Certificate from a Supported CA

- Navigate to **SETUP** menu ☐ **IP NETWORK** tab ☐ **SECURITY** folder ☐ **TLS Contexts**.
- In the TLS context page, select the **Google CES** TLS context index row and click on **Change Certificate** option.

The screenshot shows the Audiocodes management interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows 'CORE ENTITIES' with 'SECURITY' expanded, and 'TLS Contexts (2)' selected. The main content area displays a table of TLS contexts. The first context, indexed 1, is named 'Google' and has 'TLSv1.2 and TLSv1.3' as the TLS version. Below the table, the configuration for the selected context is shown, including 'GENERAL' and 'OCSP' settings. At the bottom of the configuration page, there are three links: 'Certificate Information >>', 'Change Certificate >>', and 'Trusted Root Certificates >>'. The 'Change Certificate >>' link is highlighted with a red box.

Figure 7: Change Certificate for CSR Generation

- Fill the required details in the Change Certificates link such as 'Common Name'(CN), Private Key Format, Private key size, and Click Generate Private Key.

The screenshot shows the Audiocodes management interface with the 'Change Certificates' form for the Google CES TLS context. The form is titled 'CERTIFICATE SIGNING REQUEST / GENERATE SELF-SIGNED CERTIFICATE REQUEST'. It contains several input fields for certificate details: 'Common Name [CN]' (filled with 'stc12.tekvizionlabs.com'), 'Organizational Unit [OU]', 'Company name [O]', 'Locality or city name [L]', 'State [ST]', 'Country code [C]', '1st Subject Alternative Name [SAN]', '2nd Subject Alternative Name [SAN]', '3rd Subject Alternative Name [SAN]', and '4th Subject Alternative Name [SAN]'. Below these fields, there is a section for 'GENERATE NEW PRIVATE KEY' with 'Private Key Format' set to 'RSA' and 'Private Key Size' set to '2048'. A red box highlights the 'Generate Private Key' button at the bottom of the form.

Figure 8: CSR Generation for Google CES TLS Context

- Click on “Create CSR” to generate the CSR and get it signed by certificate authority.

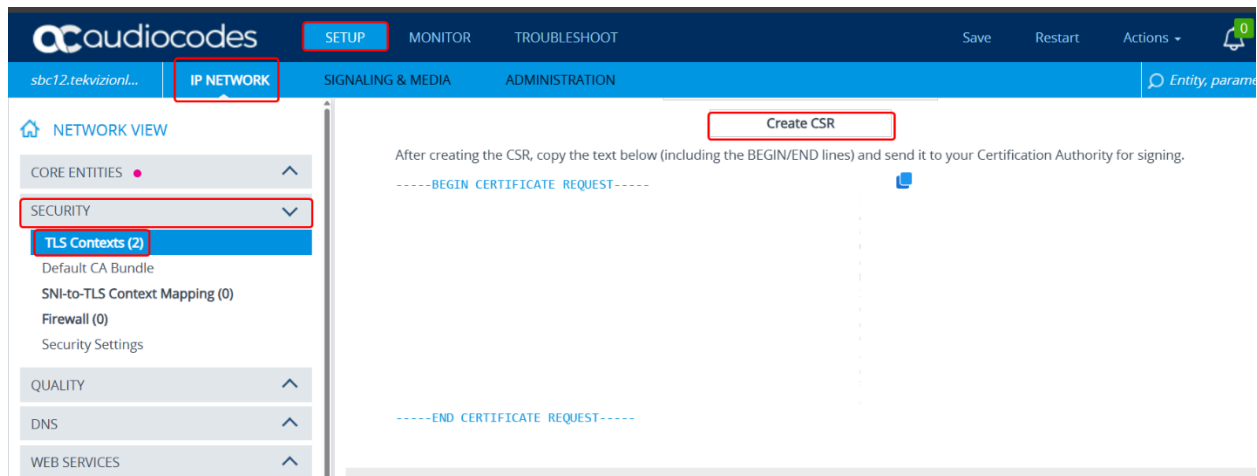


Figure 9: CSR Generation for Google CES TLS Context (Cont.)

7.4.2.3 Upload the AudioCodes VE SBC Certificate

- Navigate to **SETUP** menu ☐ **IP NETWORK** tab ☐ **SECURITY** folder ☐ **TLS Contexts**.
- In the TLS context page, select the Google CES TLS context index row and click on **Change Certificate** option.
- Scroll further down and opt for **Load Device Certificate File** to upload the AudioCodes VE SBC certificate to it.

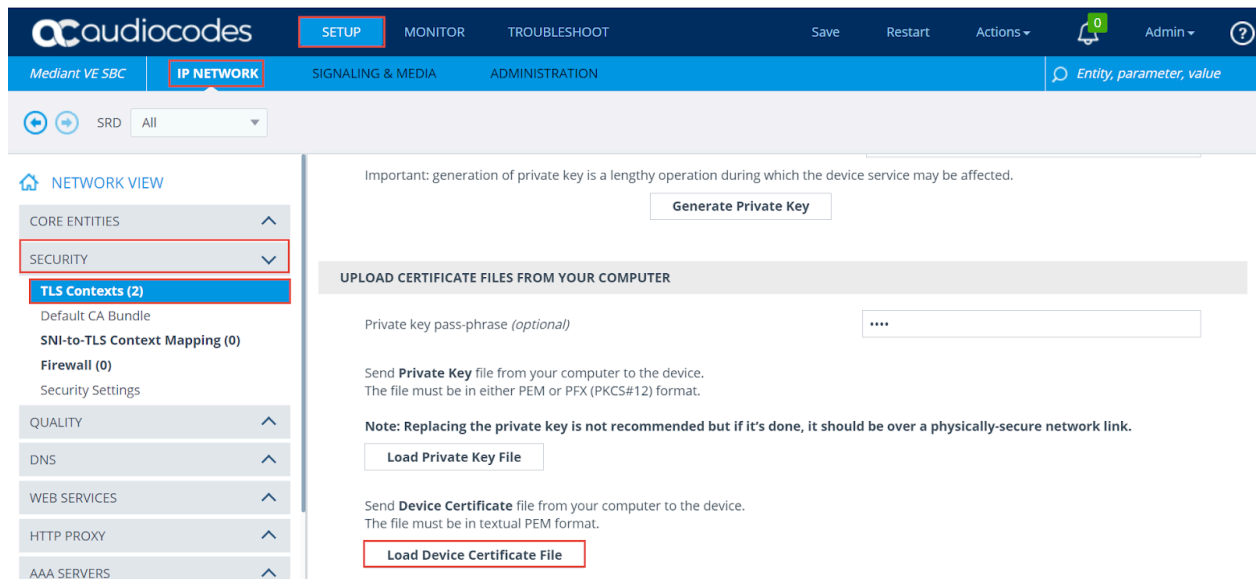


Figure 10: SBC Certificate Upload

Upload Intermediate Certificates:

- Navigate to **SETUP** menu ☐ **IP NETWORK** tab ☐ **SECURITY** folder ☐ **TLS Contexts**
- In the TLS context page, select the Google CES TLS context index row and click on **Trusted Root Certificates** option.

The screenshot shows the Audiocodes setup interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The left sidebar shows 'IP NETWORK' selected, with 'SECURITY' and 'TLS Contexts (2)' highlighted. The main content area displays the 'Trusted Root Certificates' page for a specific TLS context. It includes a 'GENERAL' section with fields like Name, TLS Version, and Cipher Server. An 'OCSP' section shows OSCP Server status and OSCP interface details. At the bottom, there are links for 'Certificate Information >>', 'Change Certificate >>', and 'Trusted Root Certificates >>'.

Figure 11: Trusted Root Certificates

- Within the Trusted Root Certificates page, click the Import button and import the Intermediate Certificates.

The screenshot shows the Audiocodes setup interface with the 'Trusted Root Certificates' page. The left sidebar shows 'SECURITY' and 'TLS Contexts (2)' highlighted. The main content area displays a table of trusted root certificates. The table has columns for INDEX, SUBJECT, ISSUER, and EXPIRES. Two certificates are listed: 'Go Daddy Root Certificate Autho' and 'Go Daddy Secure Certificate Aut'. The 'Import' button is highlighted in the top right corner.

INDEX	SUBJECT	ISSUER	EXPIRES
12	Go Daddy Root Certificate Autho	The Go Daddy Group, Inc.	Fri, 30 May 2031 01:30:00 GMT
13	Go Daddy Secure Certificate Aut	Go Daddy Root Certificate Autho	Sat, 03 May 2031 01:30:00 GMT

Figure 12: Import Trusted Root Certificates

7.4.2.4 Upload Google Trusted Root Certificate

- Download the Google Root Certificates from the following link <https://pki.goog/repository/> and select the label GTS Root R1 only.
- Navigate to **SETUP** menu ☐ **IP NETWORK** tab ☐ **SECURITY** folder ☐ **TLS Contexts**.
- In the TLS context page, select the Google CES TLS context index row and click on the **Trusted Root Certificates** option.
- Within the Trusted Root Certificates page, click the **Import** button and load Google Root Certificate as shown below.

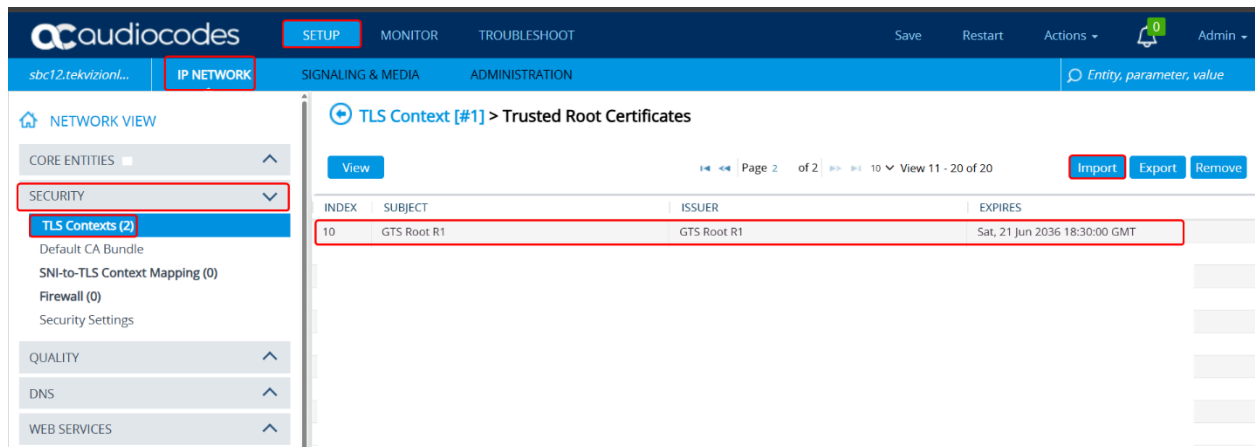


Figure : GTS Root R1 Certificate

7.4.3 Configure Media Realms

- Navigate to **SETUP** menu ☐ **SIGNALING & MEDIA** tab ☐ **CORE ENTITIES** folder ☐ **Media Realms**.
- Configure Media Realms for PSTN Gateway and Google CES as shown below.

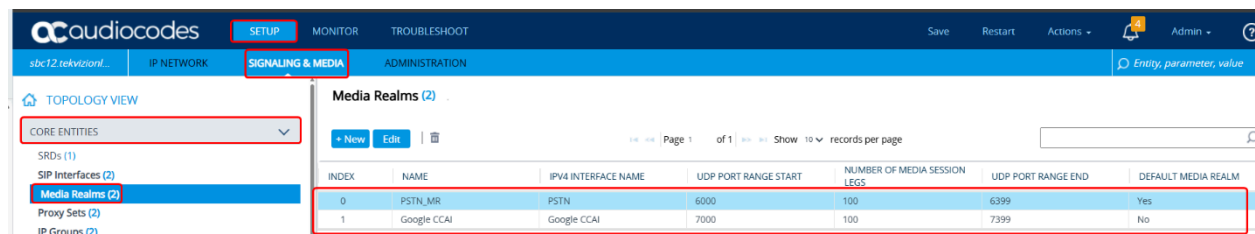
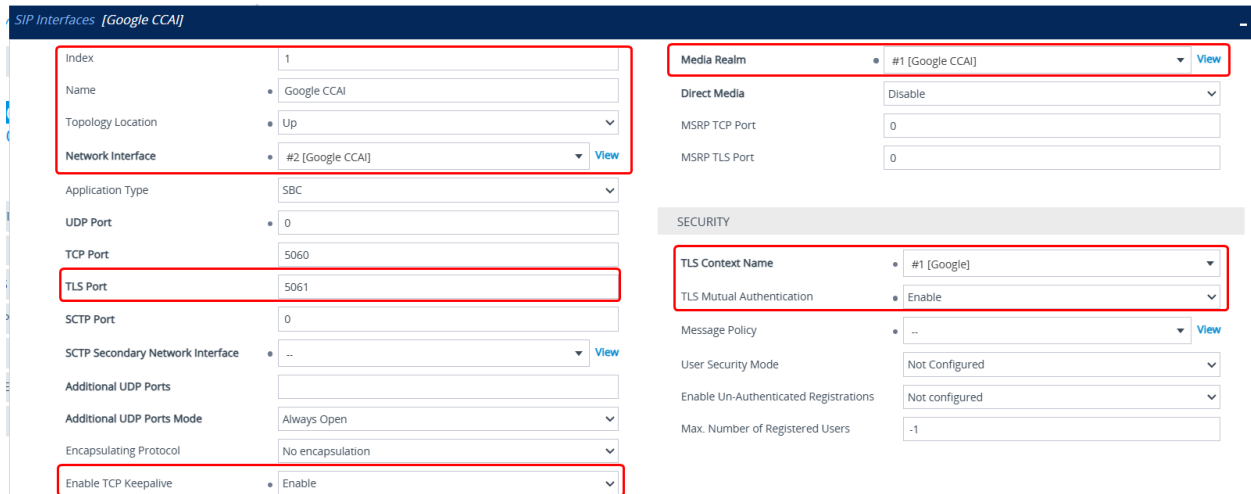


Figure : Configure Media Realms

7.4.4 Configure SIP Signaling Interfaces

- Navigate to **SETUP** menu ☐ **SIGNALING & MEDIA** tab ☐ **CORE ENTITIES** folder ☐ **SIP Interfaces.**
- Configure SIP Signaling Interfaces for PSTN Gateway and Google CES.

Google CES:



SIP Interfaces [Google CCAI]

Index	1
Name	Google CCAI
Topology Location	Up
Network Interface	#2 [Google CCAI]
Application Type	SBC
UDP Port	0
TCP Port	5060
TLS Port	5061
SCTP Port	0
SCTP Secondary Network Interface	--
Additional UDP Ports	
Additional UDP Ports Mode	Always Open
Encapsulating Protocol	No encapsulation
Enable TCP Keepalive	Enable

Media Realm: #1 [Google CCAI]

Direct Media: Disable

MSRP TCP Port: 0

MSRP TLS Port: 0

SECURITY

TLS Context Name: #1 [Google]

TLS Mutual Authentication: Enable

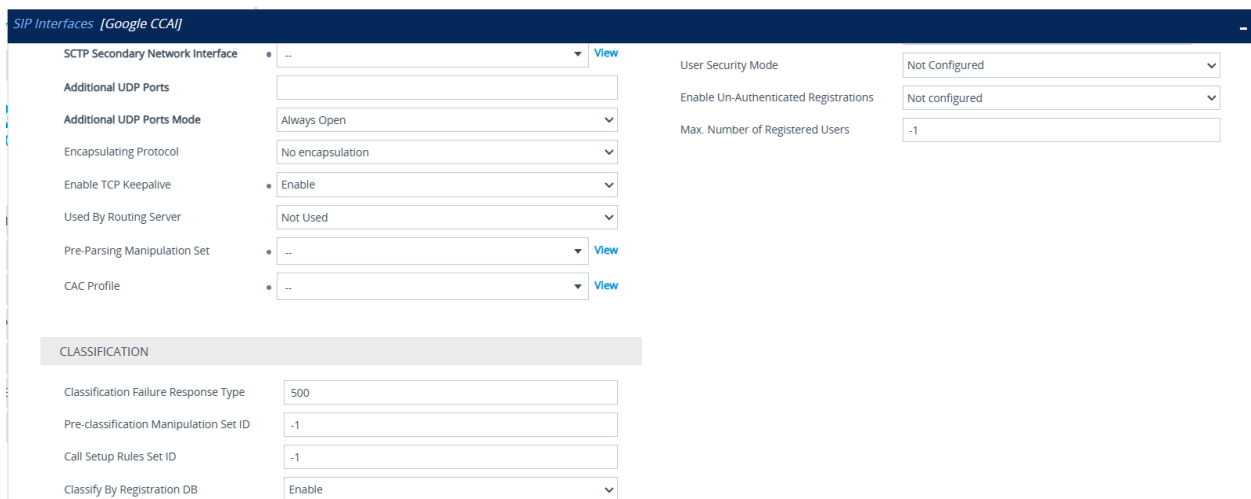
Message Policy: --

User Security Mode: Not Configured

Enable Un-Authenticated Registrations: Not configured

Max. Number of Registered Users: -1

Figure 15: SIP Signaling Interfaces for Google CES



SIP Interfaces [Google CCAI]

Sctp Secondary Network Interface: --

Additional UDP Ports: Always Open

Encapsulating Protocol: No encapsulation

Enable TCP Keepalive: Enable

Used By Routing Server: Not Used

Pre-Parsing Manipulation Set: --

CAC Profile: --

CLASSIFICATION

Classification Failure Response Type: 500

Pre-classification Manipulation Set ID: -1

Call Setup Rules Set ID: -1

Classify By Registration DB: Enable

User Security Mode: Not Configured

Enable Un-Authenticated Registrations: Not configured

Max. Number of Registered Users: -1

Figure 16: SIP Signaling Interfaces for Google CES (Cont.)

PSTN Gateway:

SIP Interfaces [PSTN]

GENERAL		MEDIA	
Index	2	Media Realm	#2 [PSTN_MR] View
Name	PSTN	Direct Media	Disable
Topology Location	Up	MSRP TCP Port	0
Network Interface	#1 [PSTN] View	MSRP TLS Port	0
Application Type	SBC		
UDP Port	5060		
TCP Port	5060		
TLS Port	0		
SCTP Port	0		
SCTP Secondary Network Interface	-- View		
Additional UDP Ports			
Additional UDP Ports Mode	Always Open		

SECURITY	
TLS Context Name	--
TLS Mutual Authentication	
Message Policy	-- View
User Security Mode	Not Configured
Enable Un-Authenticated Registrations	Not configured
Max. Number of Registered Users	-1

Figure 17: SIP Signaling Interfaces for PSTN Gateway

SIP Interfaces [PSTN]

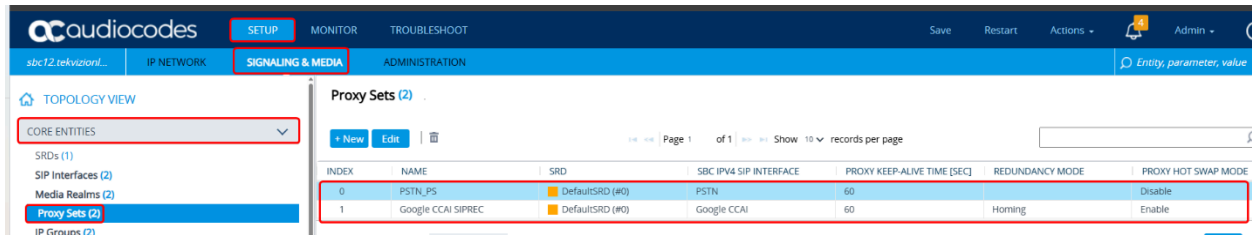
SCTP Secondary Network Interface	-- View	User Security Mode	Not Configured
Additional UDP Ports		Enable Un-Authenticated Registrations	Not configured
Additional UDP Ports Mode	Always Open	Max. Number of Registered Users	-1
Encapsulating Protocol	No encapsulation		
Enable TCP Keepalive	Disable		
Used By Routing Server	Not Used		
Pre-Parsing Manipulation Set	-- View		
CAC Profile	-- View		

CLASSIFICATION	
Classification Failure Response Type	500
Pre-classification Manipulation Set ID	-1
Call Setup Rules Set ID	-1
Classify By Registration DB	Enable

Figure 18: SIP Signaling Interfaces for PSTN Gateway (Cont.)

7.4.5 Configure Proxy Sets and Proxy Address

- Navigate to **SETUP** menu ☐ **SIGNALING & MEDIA** tab ☐ **CORE ENTITIES** folder ☐ **Proxy Sets**.
- Configure proxy sets for PSTN Gateway and Google CES as shown below.

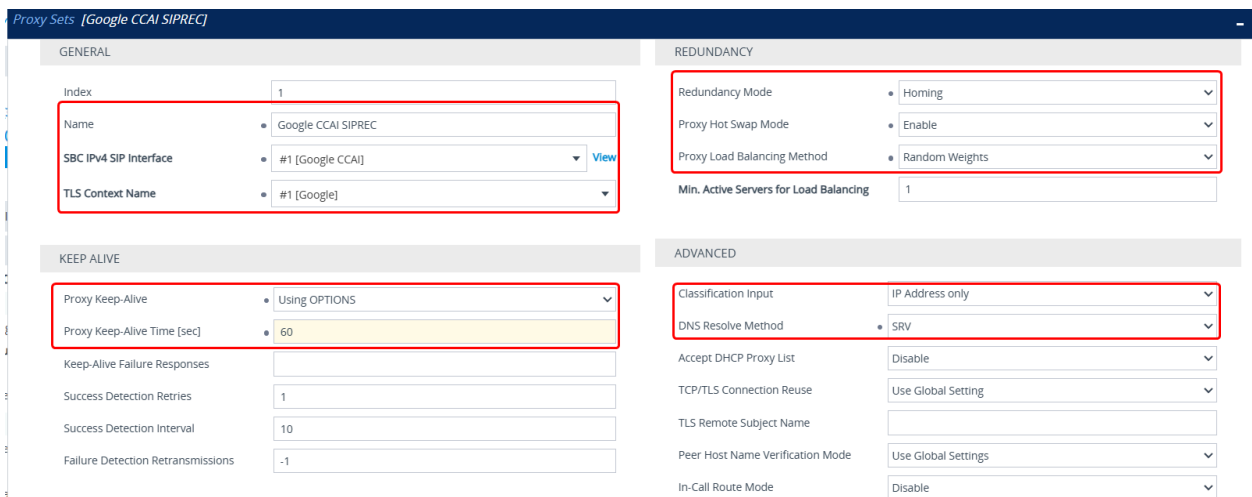


The screenshot shows the Audiocodes management console with the 'SIGNALING & MEDIA' tab selected. The 'Proxy Sets (2)' table is displayed, showing two entries:

INDEX	NAME	SRD	SBC IPv4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP MODE
0	PSTN_PS	DefaultSRD (#0)	PSTN	60		Disable
1	Google CCAI SIPREC	DefaultSRD (#0)	Google CCAI	60	Homing	Enable

Figure : Configurations of Proxy Sets

Google CES:

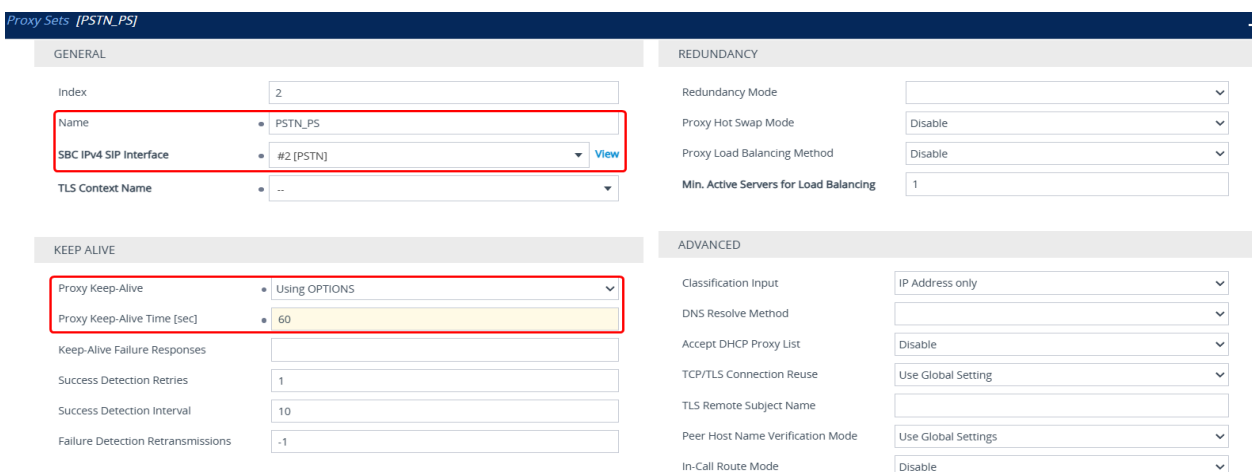


The screenshot shows the configuration page for the 'Google CCAI SIPREC' proxy set. The configuration is divided into several sections:

- GENERAL**: Index 1, Name 'Google CCAI SIPREC', SBC IPv4 SIP Interface '#1 [Google CCAI]', TLS Context Name '#1 [Google]'.
- REDUNDANCY**: Redundancy Mode 'Homing', Proxy Hot Swap Mode 'Enable', Proxy Load Balancing Method 'Random Weights', Min. Active Servers for Load Balancing '1'.
- KEEP ALIVE**: Proxy Keep-Alive 'Using OPTIONS', Proxy Keep-Alive Time [sec] '60'.
- ADVANCED**: Classification Input 'IP Address only', DNS Resolve Method 'SRV', Accept DHCP Proxy List 'Disable', TCP/TLS Connection Reuse 'Use Global Setting', TLS Remote Subject Name, Peer Host Name Verification Mode 'Use Global Settings', In-Call Route Mode 'Disable'.

Figure 20: Proxy Set Configuration of Google CES

PSTN Gateway:



The screenshot shows the configuration page for the 'PSTN_PS' proxy set. The configuration is divided into several sections:

- GENERAL**: Index 2, Name 'PSTN_PS', SBC IPv4 SIP Interface '#2 [PSTN]', TLS Context Name '--'.
- REDUNDANCY**: Redundancy Mode, Proxy Hot Swap Mode 'Disable', Proxy Load Balancing Method 'Disable', Min. Active Servers for Load Balancing '1'.
- KEEP ALIVE**: Proxy Keep-Alive 'Using OPTIONS', Proxy Keep-Alive Time [sec] '60'.
- ADVANCED**: Classification Input 'IP Address only', DNS Resolve Method, Accept DHCP Proxy List 'Disable', TCP/TLS Connection Reuse 'Use Global Setting', TLS Remote Subject Name, Peer Host Name Verification Mode 'Use Global Settings', In-Call Route Mode 'Disable'.

Figure 21: Proxy Set Configuration of PSTN Gateway

Proxy Address Configuration:

- Navigate into **SETUP** menu ☐ **SIGNALING & MEDIA** tab ☐ **CORE ENTITIES** folder ☐ **Proxy Sets**.
- Select the Google CES SIPREC Proxy Set and add the Proxy Address by clicking **Proxy Address items>>** and **+New**.

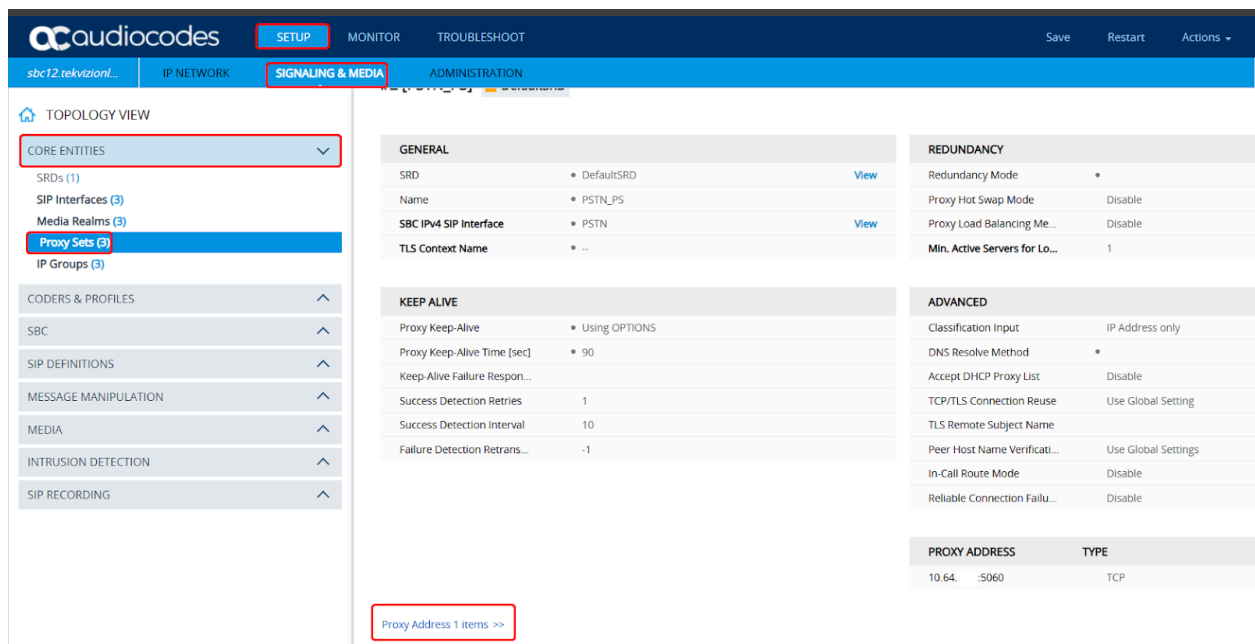


Figure 22: Proxy Address Configuration

- Enter the Google FQDN as proxy Address in the Google Proxy set and select transport type as TLS

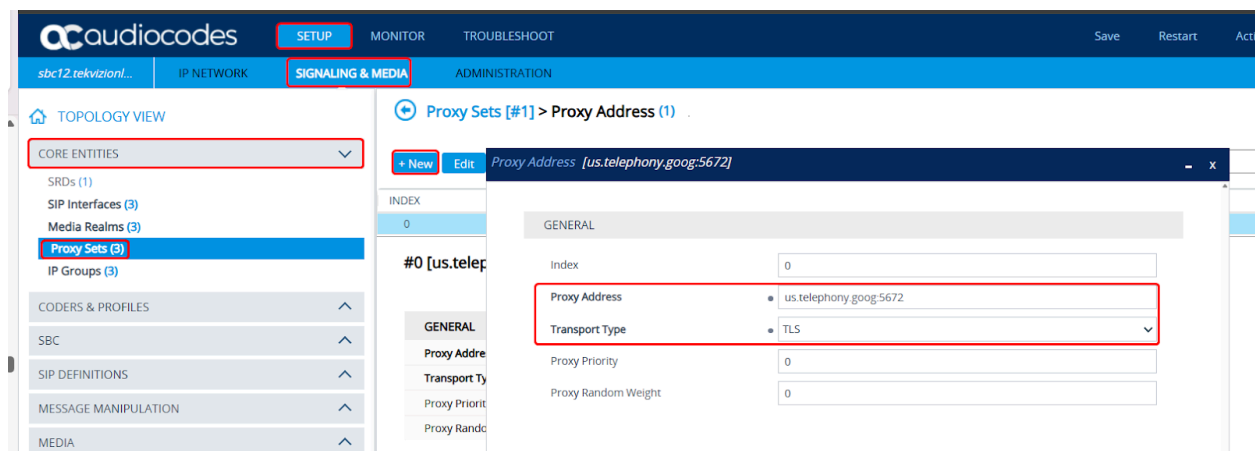


Figure 23: Proxy Address Configuration of Google CES

- Select the PSTN Proxy Set and add the Proxy Address by clicking **Proxy Address X items>>** and **+New**.
- Enter the PSTN gateway IP as Proxy Address in the PSTN proxy set and select transport as TCP.

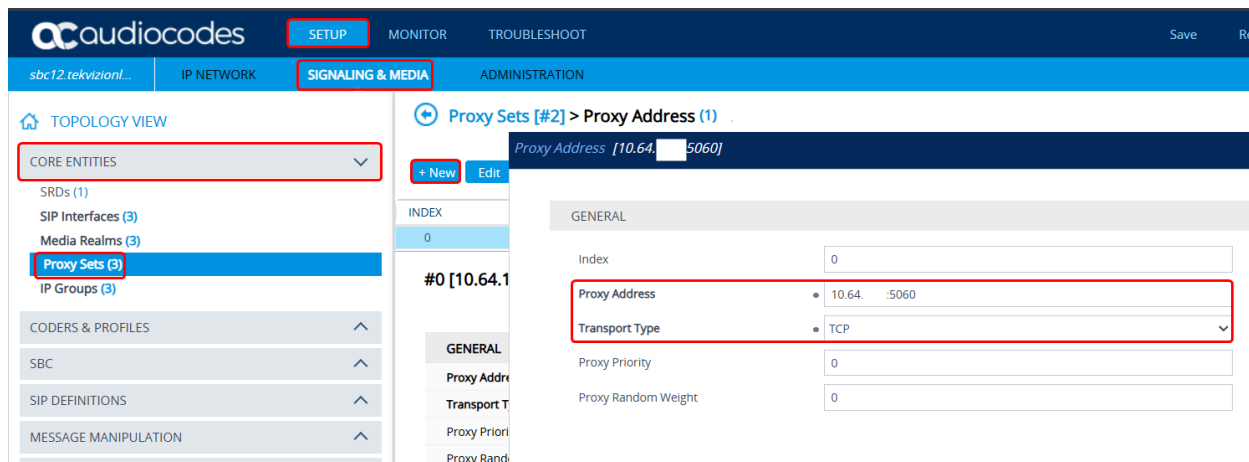


Figure 24: Proxy Address Configuration of PSTN Gateway

7.4.6 Configure Coders

- Navigate to **SETUP** menu ☐ **SIGNALING & MEDIA** tab ☐ **CODERS & PROFILES** folder ☐ **Coder Groups**.
- Configure the required Codecs as shown below.

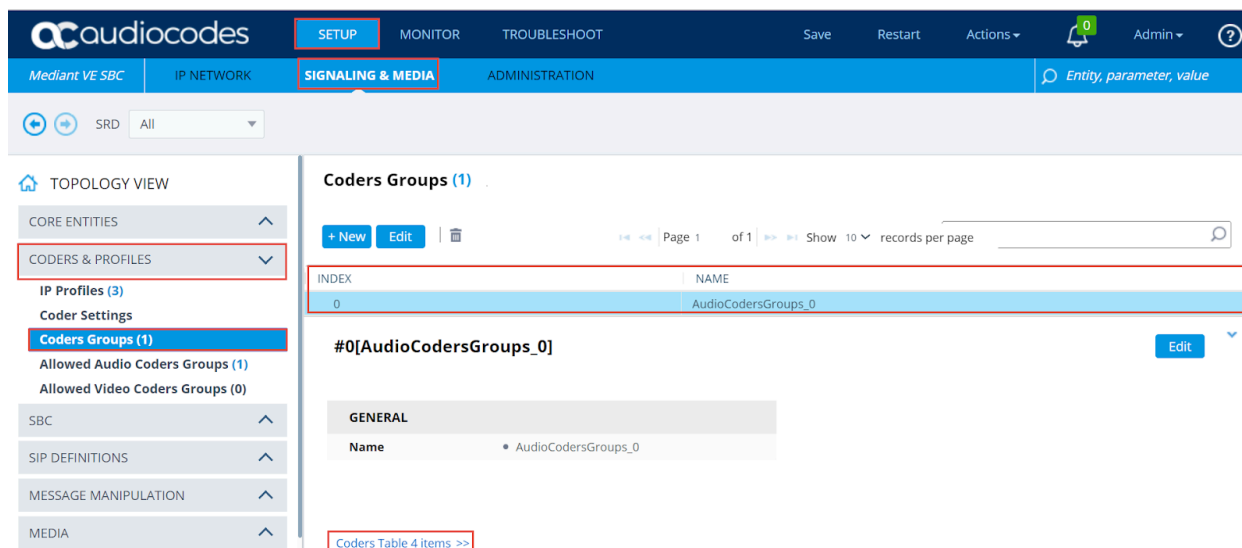


Figure 25: Coders Configurations

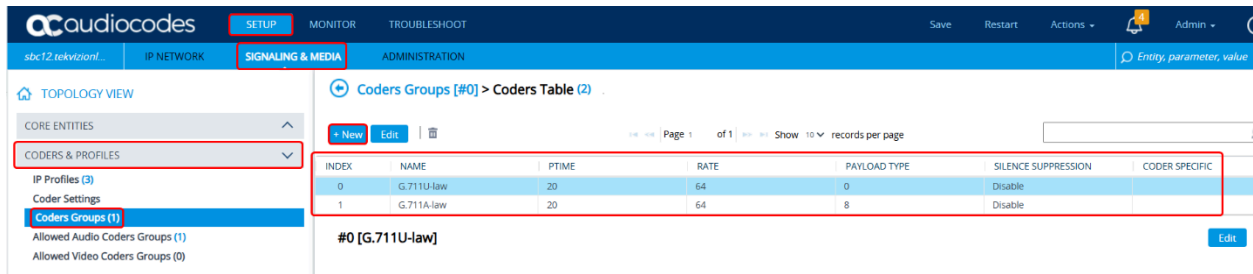


Figure 26: Coders Configurations (Cont.)

To Set a preferred coder for the Google CES:

- Navigate to the **SETUP** menu ☐ **SIGNALING & MEDIA** tab ☐ **CODERS & PROFILES** folder ☐ **Allowed Audio Coders Groups**.

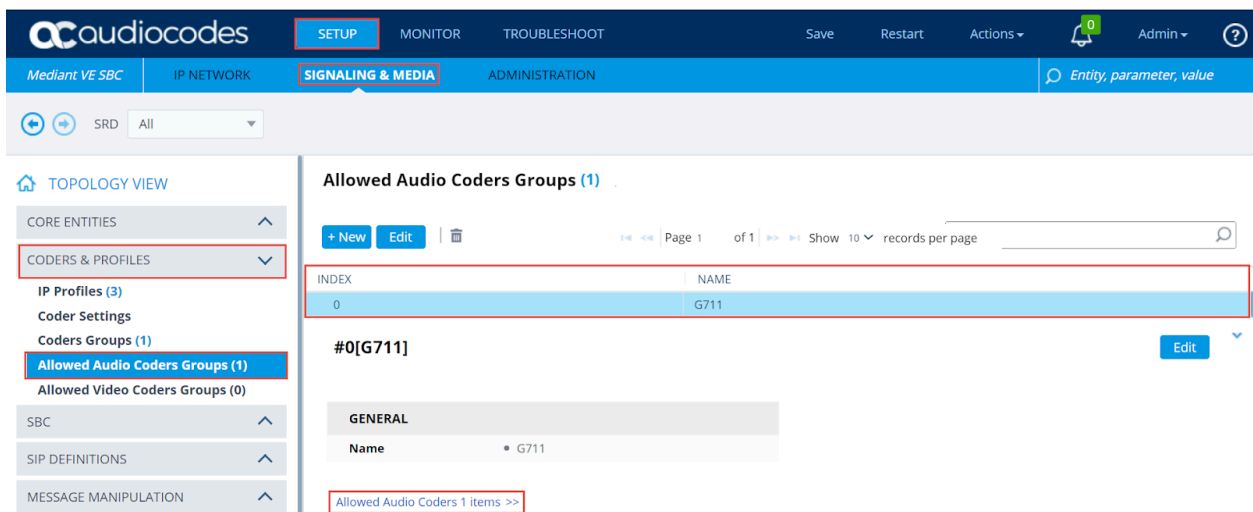


Figure 27: Coders Configurations (Cont.)

- Click **+New** and configure a new Allowed Audio Coders Group for Google CES with the preferred Codec list.
- Assign the configured Allowed Audio Coders Group to the respective Google CES IP Profile.

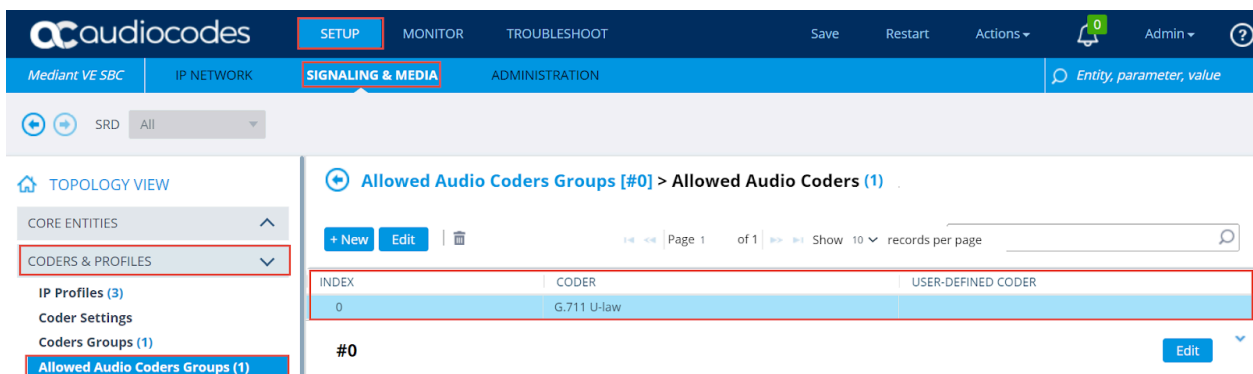


Figure : Coders Configurations (Cont.)

7.4.7 Configure IP Profiles

- Navigate to **SETUP** menu ☐ **SIGNALING & MEDIA** tab ☐ **CODERS & PROFILE** folder ☐ **IP Profiles**.
- IP Profile configuration for Google CES and PSTN Gateway are shown below.



Figure 29: IP Profile Configurations

PSTN Gateway IP:

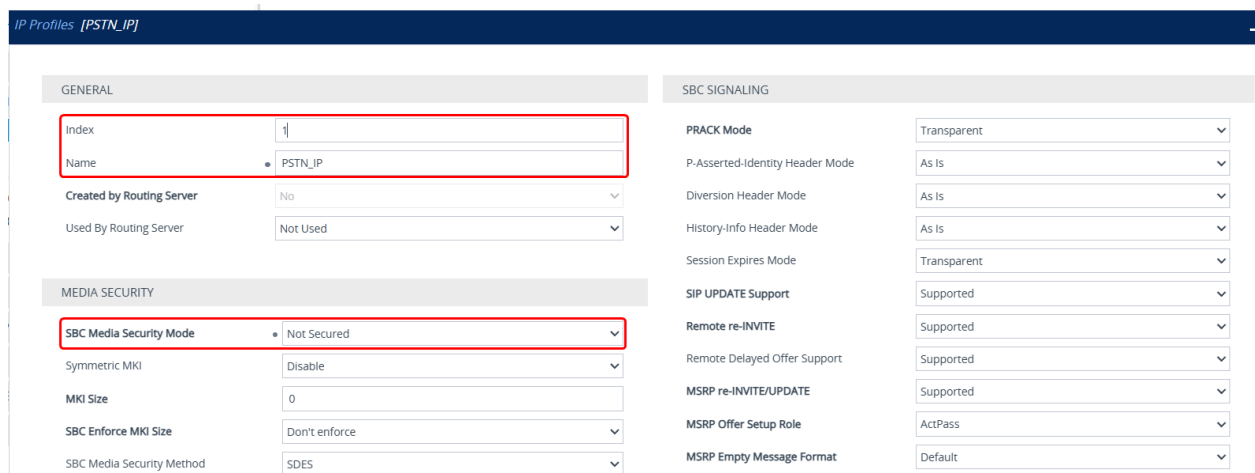


Figure 30: IP Profile Configurations of PSTN Gateway

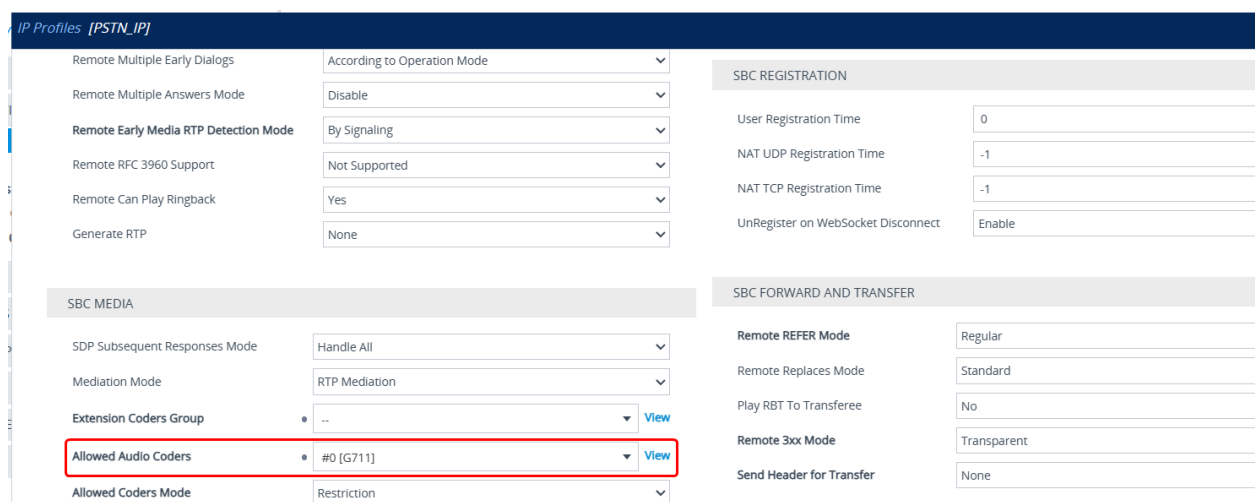


Figure 31: IP Profile Configurations of PSTN Gateway (Cont.)

IP Profiles [PSTN_IP]

Allowed Video Coders	• -- View	SBC HOLD	
Allowed Media Types		Remote Hold Format	Transparent
Direct Media Tag		Reliable Held Tone Source	Yes
RFC 2833 Mode	As Is	Play Held Tone	No
RFC 2833 DTMF Payload Type	0	SBC FAX	
Alternative DTMF Method	As Is	Fax Coders Group	• -- View
Send Multiple DTMF Methods	Disable	Fax Mode	As Is
Receive Multiple DTMF Methods	Disable	Fax Offer Mode	All coders
Adapt RFC2833 BW to Voice coder BW	Disabled	Fax Answer Mode	Single coder
SDP PTime Answer	Remote Answer	Remote Renegotiate on Fax Detection	Transparent
Preferred PTime	0	Fax Rerouting Mode	Disable
Use Silence Suppression	Transparent		
RTP Redundancy Mode	As Is		
RTCP Mode	Transparent		

Figure 32: IP Profile Configurations of PSTN Gateway (Cont.)

IP Profiles [PSTN_IP]

Jitter Compensation	Disable	MEDIA	
ICE Mode	Disable	Broken Connection Mode	Disconnect
SDP Handle RTCP	Don't Care	No RTP Mode	Disconnect
RTCP Mux	Not Supported	Media IP Version Preference	Only IPv4
RTCP Feedback	Feedback Off	RTP Redundancy Depth	Disable
Re-number MID	Disable	LOCAL TONES	
Voice Quality Enhancement	Disable	Local Ringback Tone Index	-1
Switch Coder Upon Voice Quality	Disable	Local Held Tone Index	-1
Max Opus Bandwidth	0		
Generate No-Op Packets	Disable		
Enhanced PLC	Disable		
SBC Multiple Coders	Not Supported		
SBC Allow Only Negotiated PT	Disable		
Add Media IP Change Header	Disable		

Figure 33: IP Profile Configurations of PSTN Gateway (Cont.)

IP Profiles [PSTN_IP]

SBC Precondition	Not Supported
BFCP IP from Audio Media	According to Global Parameter
Remove EXTMAP	Disable
QUALITY OF SERVICE	
RTP IP DiffServ	46
RTP Video DiffServ	-1
Signaling DiffServ	24
Data DiffServ	0
JITTER BUFFER	
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
Jitter Buffer Max Delay [msec]	300

Figure 34: IP Profile Configurations of PSTN Gateway (Cont.)

Google CES:

The screenshot displays the 'IP Profiles [Google CCAL_IP]' configuration page. It is divided into two main sections: 'GENERAL' and 'SBC SIGNALING'. In the 'GENERAL' section, the 'Index' is set to 2, the 'Name' is 'Google CCAL_IP', 'Created by Routing Server' is 'No', and 'Used By Routing Server' is 'Not Used'. In the 'SBC SIGNALING' section, 'PRACK Mode' is 'Transparent', 'P-Asserted-Identity Header Mode' is 'As Is', 'Diversion Header Mode' is 'As Is', 'History-Info Header Mode' is 'As Is', 'Session Expires Mode' is 'Supported', 'SIP UPDATE Support' is 'Supported', 'Remote re-INVITE' is 'Supported', and 'Remote Delayed Offer Support' is 'Supported'. The 'MEDIA SECURITY' section is partially visible at the bottom, showing 'SBC Media Security Mode' set to 'Secured'.

GENERAL	
Index	2
Name	Google CCAL_IP
Created by Routing Server	No
Used By Routing Server	Not Used

SBC SIGNALING	
PRACK Mode	Transparent
P-Asserted-Identity Header Mode	As Is
Diversion Header Mode	As Is
History-Info Header Mode	As Is
Session Expires Mode	Supported
SIP UPDATE Support	Supported
Remote re-INVITE	Supported
Remote Delayed Offer Support	Supported

MEDIA SECURITY	
SBC Media Security Mode	Secured
Symmetric MKI	Disable

Figure 35: IP Profile configurations of Google CES

The screenshot continues the configuration page, showing 'SBC Remove' and 'SBC EARLY MEDIA' sections. In the 'SBC Remove' section, 'SBC Remove Crypto Lifetime in SDP' is 'Yes', 'SBC Remove Unknown Crypto' is 'No', 'Crypto Suites Group' is '#0 [WAN]' (with a 'View' link), and 'Encryption on RTCP Packets' is 'As Is'. In the 'SBC EARLY MEDIA' section, 'Remote Early Media' is 'Supported', 'Remote Multiple 18x' is 'Supported', 'Remote Early Media Response Type' is 'Transparent', and 'Remote Multiple Early Dialogs' is 'According to Operation Mode'. The 'SBC SIGNALING' section continues with 'Keep Incoming Routing Headers' as 'According to Operation Mode', 'Keep User-Agent Header' as 'According to Operation Mode', 'Use Initial Incoming INVITE for Re-INVITE' as 'Disable', 'Handle X-Detect' as 'No', 'ISUP Body Handling' as 'Transparent', 'ISUP Variant' as 'Itu92', 'Max Call Duration [min]' as '0', 'Broken Signaling Connection Mode' as 'Ignore', and 'Disconnect In-Dialog Subscribe Failure' as 'Enable'.

SBC Remove	
SBC Remove Crypto Lifetime in SDP	Yes
SBC Remove Unknown Crypto	No
Crypto Suites Group	#0 [WAN] View
Encryption on RTCP Packets	As Is

SBC EARLY MEDIA	
Remote Early Media	Supported
Remote Multiple 18x	Supported
Remote Early Media Response Type	Transparent
Remote Multiple Early Dialogs	According to Operation Mode

SBC SIGNALING (Continued)	
Keep Incoming Routing Headers	According to Operation Mode
Keep User-Agent Header	According to Operation Mode
Use Initial Incoming INVITE for Re-INVITE	Disable
Handle X-Detect	No
ISUP Body Handling	Transparent
ISUP Variant	Itu92
Max Call Duration [min]	0
Broken Signaling Connection Mode	Ignore
Disconnect In-Dialog Subscribe Failure	Enable

Figure 36: IP Profile Configurations of Google CES (Cont.)

The screenshot shows the bottom part of the configuration page, including 'SDP' and 'SBC HOLD' sections. In the 'SDP' section, 'SDP Subsequent Responses Mode' is 'Handle All', 'Mediation Mode' is 'RTP Mediation', 'Extension Coders Group' is '--' (with a 'View' link), 'Allowed Audio Coders' is '#0 [G711]' (with a 'View' link), 'Allowed Coders Mode' is 'Restriction', and 'Allowed Video Coders' is '--' (with a 'View' link). In the 'SBC HOLD' section, 'Remote REFER Mode' is 'Regular', 'Remote Replaces Mode' is 'Standard', 'Play RBT To Transferee' is 'No', 'Remote 3xx Mode' is 'Transparent', and 'Send Header for Transfer' is 'None'.

SDP	
SDP Subsequent Responses Mode	Handle All
Mediation Mode	RTP Mediation
Extension Coders Group	-- View
Allowed Audio Coders	#0 [G711] View
Allowed Coders Mode	Restriction
Allowed Video Coders	-- View

SBC HOLD	
Remote REFER Mode	Regular
Remote Replaces Mode	Standard
Play RBT To Transferee	No
Remote 3xx Mode	Transparent
Send Header for Transfer	None

Figure 37: IP Profile Configurations of Google CES (Cont.)

IP Profiles [Google CCAL_IP]

Allowed Video Coders	--	View
Allowed Media Types		
Direct Media Tag		
RFC 2833 Mode	As Is	
RFC 2833 DTMF Payload Type	0	
Alternative DTMF Method	As Is	
Send Multiple DTMF Methods	Disable	
Receive Multiple DTMF Methods	Disable	
Adapt RFC2833 BW to Voice coder BW	Disabled	
SDP Ptime Answer	Remote Answer	
Preferred PTime	0	
Use Silence Suppression	Transparent	
RTP Redundancy Mode	As Is	
RTCP Mode	Transparent	

SBC HOLD

Remote Hold Format	Transparent
Reliable Held Tone Source	Yes
Play Held Tone	No

SBC FAX

Fax Coders Group	--	View
Fax Mode	As Is	
Fax Offer Mode	All coders	
Fax Answer Mode	Single coder	
Remote Renegotiate on Fax Detection	Transparent	
Fax Rerouting Mode	Disable	

Figure 38: IP Profile Configurations of Google CES (Cont.)

IP Profiles [Google CCAL_IP]

Jitter Compensation	Disable
ICE Mode	Disable
SDP Handle RTCP	Don't Care
RTCP Mux	Not Supported
RTCP Feedback	Feedback Off
Re-number MID	Disable
Voice Quality Enhancement	Disable
Switch Coder Upon Voice Quality	Disable
Max Opus Bandwidth	0
Generate No-Op Packets	Disable
Enhanced PLC	Disable
SBC Multiple Coders	Not Supported
SBC Allow Only Negotiated PT	Disable
Add Media IP Change Header	Disable

MEDIA

Broken Connection Mode	Disconnect
No RTP Mode	Disconnect
Media IP Version Preference	Only IPv4
RTP Redundancy Depth	Disable

LOCAL TONES

Local Ringback Tone Index	-1
Local Held Tone Index	-1

Figure 39: IP Profile Configurations of Google CES (Cont.)

IP Profiles [Google CCAL_IP]

Remove CSRC	Disable
SBC Precondition	Not Supported
BFCP IP from Audio Media	According to Global Parameter
Remove EXTMAP	Disable

QUALITY OF SERVICE

RTP IP DiffServ	46
RTP Video DiffServ	-1
Signaling DiffServ	24
Data DiffServ	0

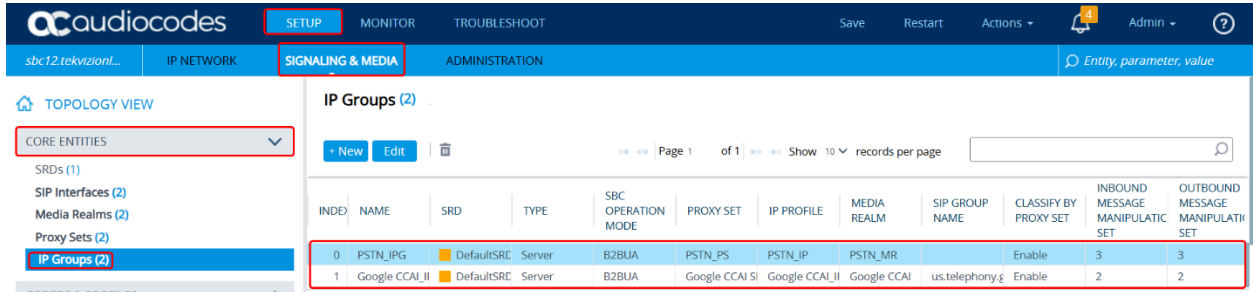
JITTER BUFFER

Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10

Figure 40: IP Profile Configurations of Google CES (Cont.)

7.4.8 Configure IP Groups

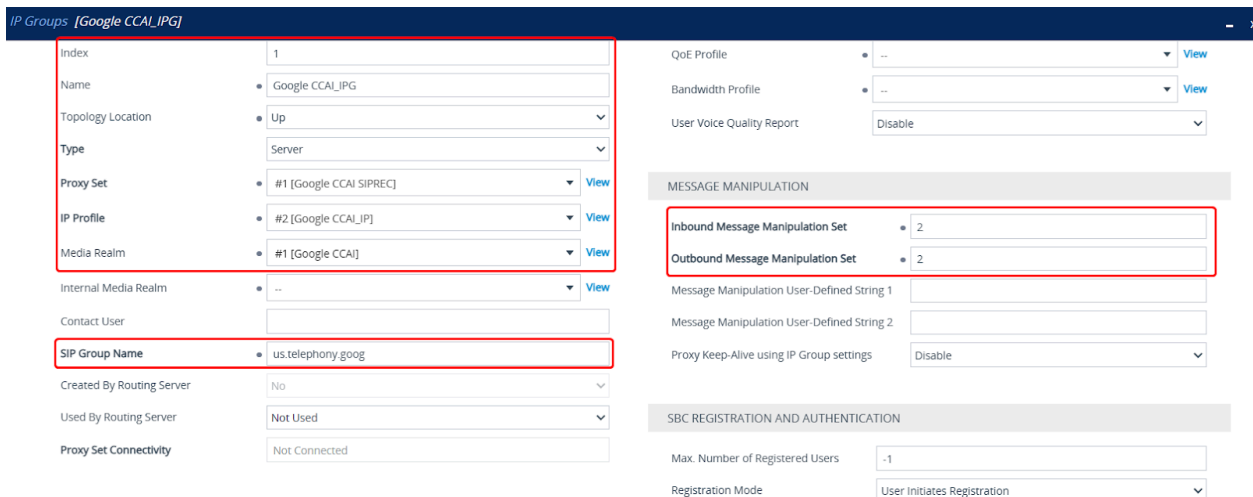
- Navigate to **SETUP** menu ☐ **SIGNALING & MEDIA** tab ☐ **CORE ENTITIES** folder ☐ **IP Groups**
- IP Groups Config towards Google CES and PSTN Gateway are shown below.



INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATION SET	OUTBOUND MESSAGE MANIPULATION SET
0	PSTN_IPG	DefaultSRD	Server	B2BUA	PSTN_PS	PSTN_IP	PSTN_MR		Enable	3	3
1	Google CCAI_IPG	DefaultSRD	Server	B2BUA	Google CCAI_S	Google CCAI_IP	Google CCAI	us.telephony.g	Enable	2	2

Figure 41: IP Group Configurations

- Select the respective Proxy Set, IP Profile, Media Realm and Media TLS Context for Google IP Group and enter Google FQDN as SIP Group Name.



IP Groups: [Google CCAI_IPG]

Index: 1

Name: Google CCAI_IPG

Topology Location: Up

Type: Server

Proxy Set: #1 [Google CCAI SIPREC]

IP Profile: #2 [Google CCAI_IP]

Media Realm: #1 [Google CCAI]

SIP Group Name: us.telephony.goog

Internal Media Realm: --

Contact User:

Created By Routing Server: No

Used By Routing Server: Not Used

Proxy Set Connectivity: Not Connected

QoS Profile: --

Bandwidth Profile: --

User Voice Quality Report: Disable

MESSAGE MANIPULATION

Inbound Message Manipulation Set: 2

Outbound Message Manipulation Set: 2

Message Manipulation User-Defined String 1:

Message Manipulation User-Defined String 2:

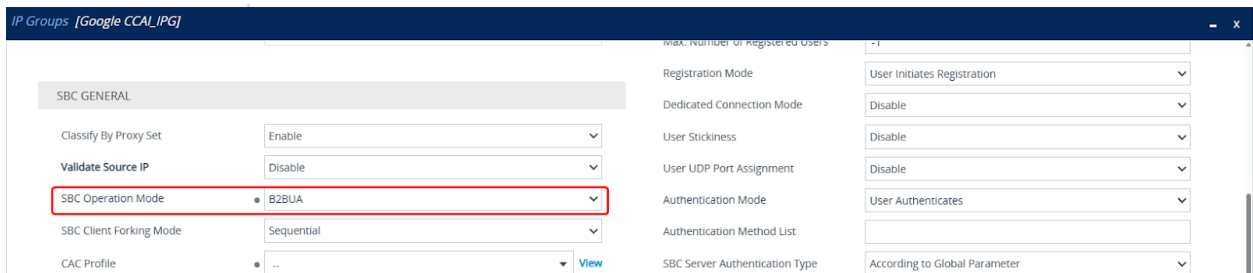
Proxy Keep-Alive using IP Group settings: Disable

SBC REGISTRATION AND AUTHENTICATION

Max. Number of Registered Users: -1

Registration Mode: User Initiates Registration

Figure 42: IP Group Configurations of Google CES



IP Groups: [Google CCAI_IPG]

SBC GENERAL

Classify By Proxy Set: Enable

Validate Source IP: Disable

SBC Operation Mode: B2BUA

SBC Client Forking Mode: Sequential

CAC Profile: --

Max. Number of Registered Users: -1

Registration Mode: User Initiates Registration

Dedicated Connection Mode: Disable

User Stickiness: Disable

User UDP Port Assignment: Disable

Authentication Mode: User Authenticates

Authentication Method List:

SBC Server Authentication Type: According to Global Parameter

Figure 43: IP Group Configurations of Google CES (Cont.)

IP Groups [Google CCAI_IPG]

SBC PSAP Mode	Disable
Route Using Request URI Port	Disable
Media TLS Context	#1 [Google]
Keep Original Call-ID	No
Dial Plan	-- View
Call Setup Rules Set ID	-1
Tags	
SBC Alternative Routing Reasons Set	-- View
Teams Local Media Optimization Handling	None
Teams Local Media Optimization Initial Behavior	DirectMedia
Teams Local Media Optimization Site	
Teams Direct Routing Mode	Disable
Metering Remote Type	Regular
Report Metering	Enable

Figure 44: IP Group Configurations of Google CES (Cont.)

- Select the respective Proxy Set, IP Profile and Media Realm for PSTN Gateway IP Group and enter the PSTN Gateway IP as SIP Group name.

IP Groups [PSTN_IPG]

SRD #0 [DefaultSRD]

GENERAL		QUALITY OF EXPERIENCE	
Index	0	QoE Profile	-- View
Name	PSTN_IPG	Bandwidth Profile	-- View
Topology Location	Up	User Voice Quality Report	Disable
Type	Server	MESSAGE MANIPULATION	
Proxy Set	#0 [PSTN_PS] View	Inbound Message Manipulation Set	3
IP Profile	#0 [PSTN_IP] View	Outbound Message Manipulation Set	3
Media Realm	#0 [PSTN_MR] View	Message Manipulation User-Defined String 1	
Internal Media Realm	-- View	Message Manipulation User-Defined String 2	
Contact User		Proxy Keep-Alive using IP Group settings	Disable
SIP Group Name			

Figure 45: IP Group Configurations of PSTN Gateway

IP Groups [PSTN_IPG]

SBC GENERAL		SBC ADVANCED	
Classify By Proxy Set	Enable	Dedicated Connection Mode	Disable
Validate Source IP	Disable	User Stickiness	Disable
SBC Operation Mode	B2BUA	User UDP Port Assignment	Disable
SBC Client Forking Mode	Sequential	Authentication Mode	User Authenticates
CAC Profile	-- View	Authentication Method List	
SIP Source Host Name		SBC Server Authentication Type	According to Global Parameter
ADVANCED		OAuth HTTP Service	-- View
Local Host Name		Username As Client	
UII Format	Disable	Password As Client	
Always Use Src Address	No	Username As Server	
		Password As Server	
		Teams Registration Mode	Disable

Figure 46: IP Group Configurations of PSTN Gateway (Cont.)

IP Groups [PSTN_IPG]

Avaya User SBC Address

190

SBC ADVANCED

Source URI Input

Destination URI Input

SIP Connect

No

SBC PSAP Mode

Disable

Route Using Request URI Port

Disable

Media TLS Context

#0 [default]

Keep Original Call-ID

No

Dial Plan

--

View

Call Setup Rules Set ID

-1

Tags

SBC Alternative Routing Reasons Set

--

View

GW GROUP STATUS

GW Group Registered IP Address

GW Group Registered Status

NA

Figure 47: IP Group Configurations of PSTN Gateway (Cont.)

IP Groups [PSTN_IPG]

SBC PSAP Mode

Disable

Route Using Request URI Port

Disable

Media TLS Context

#0 [default]

Keep Original Call-ID

No

Dial Plan

--

View

Call Setup Rules Set ID

-1

Tags

SBC Alternative Routing Reasons Set

--

View

Teams Local Media Optimization Handling

None

Teams Local Media Optimization Initial Behavior

DirectMedia

Teams Local Media Optimization Site

Teams Direct Routing Mode

Disable

Metering Remote Type

Regular

Report Metering

Enable

Figure 48: IP Group Configurations of PSTN Gateway (Cont.)

7.4.9 Configure Media Security

- Navigate to **SETUP** menu ☐ **SIGNALING & MEDIA** tab ☐ **MEDIA** folder ☐ **Media Security**.
- Enable Media Security as shown below.

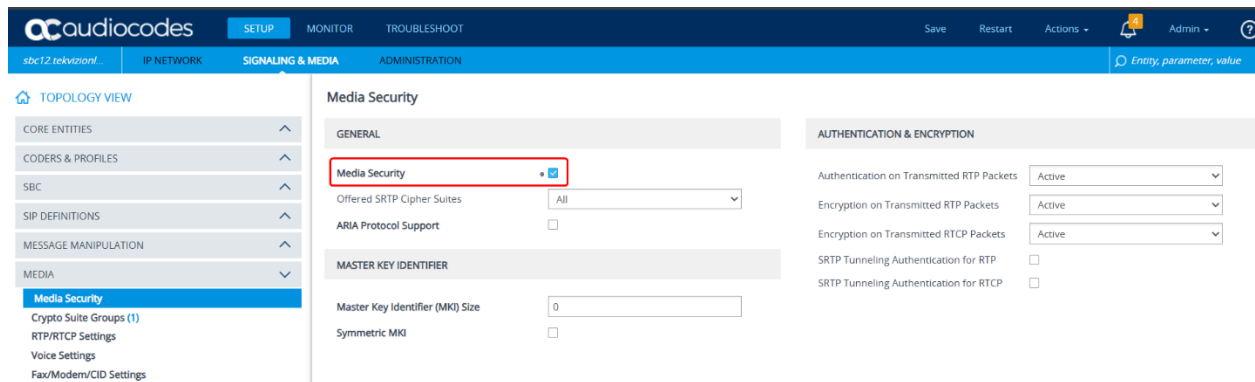


Figure 49: Media Security Configuration

7.4.10 Configure IP to IP Call Routing

- Navigate to **SETUP** menu ☐ **SIGNALING & MEDIA** tab ☐ **SBC** folder ☐ **Routing** ☐ **IP-to-IP Routing**
- Configure required routing rules as shown below.

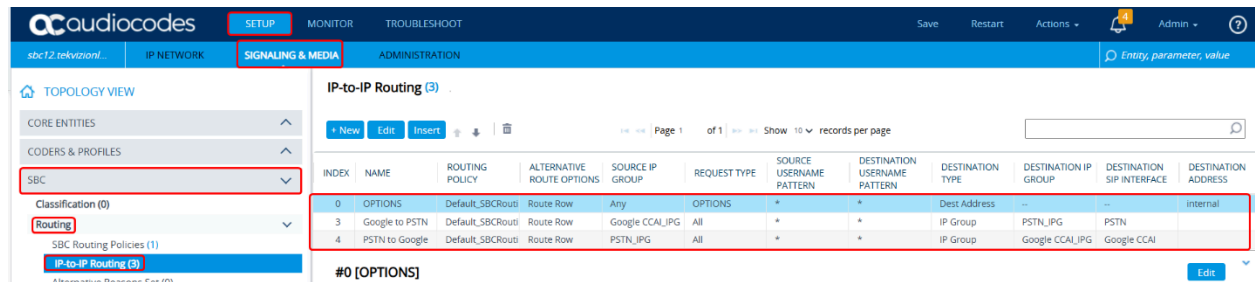


Figure 50: IP to IP Routing

7.4.11 Configure Message Manipulation Rules

- Navigate to **SETUP** menu ☐ **SIGNALING & MEDIA** tab ☐ **MESSAGE MANIPULATIONS** folder ☐ **Message Manipulations**
- Configure message manipulation towards Google CES as shown below.

The screenshot shows the Audiocodes SBC configuration interface. The left sidebar contains a tree view with categories like CORE ENTITIES, CODERS & PROFILES, SBC, SIP DEFINITIONS, MESSAGE MANIPULATION, and MEDIA. The 'MESSAGE MANIPULATION' category is expanded, showing 'Message Manipulations (11)'. The main area displays a table of message manipulations. The table has columns: INDEX, NAME, MANIPULATION SET ID, MESSAGE TYPE, CONDITION, ACTION SUBJECT, ACTION TYPE, ACTION VALUE, and ROW ROLE. The table contains 11 rows of configurations for various message types like 'call-info Google', 'removecallinfo', 'Request URI', 'from', 'PAI modify', 'Contact', 'To', 'To_Host', 'Request_URI_PSTN', 'To_PSTN', and 'User-to-User'.

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	call-info Google	2	Invite Request		Header:call-info	Add	<http://dialogflow.google	Use Current Condition
1	removecallinfo	2	Any Request	Header Call-Info regex (<	Header Call-Info	Modify	\$1+\$3	Use Current Condition
2	Request URI	2	Invite Request		Header Request-URI URL	Modify	*131494/	Use Current Condition
3	from	2	Invite Request		Header From-URL Host	Modify	*192.65.2	Use Current Condition
4	PAI modify	2	Invite Request		Header P-Asserted-Ident	Modify	*192.65	Use Current Condition
5	Contact	0	Invite Request		Header Contact-URL Host	Modify	*192.65	Use Current Condition
6	To	2	Invite Request		Header To-URL User	Modify	*131494/	Use Current Condition
7	To_Host	2	Invite Request		Header To-URL Host	Modify	*us.telephony.goog	Use Current Condition
8	Request_URI_PSTN	3	Any Request		Header Request-URI URL	Modify	*214242	Use Current Condition
9	To_PSTN	3	Any Request		Header To-URL User	Modify	*214242	Use Current Condition
10	User-to-User	0	Invite Request		Header User-to-User	Add	*66	Use Current Condition

Figure 51: Message Manipulation for Google CES

- 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 AudioCodes SBC for each call.
- New Value is set to `<http://dialogflow.googleapis.com/v2beta1/projects/ccai-3898XX/conversations/Sr_'+Header.Call-ID.ID+'>;purpose=Goog-ContactCenter-Conversation`.

The screenshot shows the Audiocodes SBC configuration interface for a specific message manipulation rule. The rule is named 'call-info Google' and is associated with Manipulation Set ID '2'. The rule is configured to add a 'Header:call-info' header to 'Invite Request' messages. The action value is set to a REST API endpoint for Google CES, including the conversation ID and purpose.

GENERAL	ACTION
Index: q Name: call-info Google Manipulation Set ID: 2 Row Role: Use Current Condition	Action Subject: Header:call-info Action Type: Add Action Value: <http://dialogflow.googleapis.com/v2beta1/projects/ccai-3898XX/conversations/Sr_'+Header.Call-ID.ID+'>;purpose=Goog-ContactCenter-Conversation
MATCH	
Message Type: Invite Request Condition:	

Figure 52: Message Manipulation: Call Info towards Google CES

- Below header rule is created to eliminate 192.65.X.X SBC WAN IP details from the call-Info header towards Google CES.

Message Manipulations [removecallinfo]

GENERAL		ACTION	
Index	1	Action Subject	Header.Call-Info
Name	removecallinfo	Action Type	Modify
Manipulation Set ID	2	Action Value	\$1+\$3
Row Role	Use Current Condition		

MATCH	
Message Type	Any.Request
Condition	Header.Call-Info regex (<http://.*)(@192.65.X.*\$)

Figure 53: Message Manipulation: Call Info Modification towards Google CES

- Below header rule is created to change Request URI towards Google CES as '+1349XXXXXX'

Message Manipulations [Request URI]

GENERAL		ACTION	
Index	2	Action Subject	Header.Request-URI.URL.User
Name	Request URI	Action Type	Modify
Manipulation Set ID	2	Action Value	'+13149.'
Row Role	Use Current Condition		

MATCH	
Message Type	Invite.Request
Condition	

- Below header rule is created to change from header host part towards Google CES as '192.65.X.X'

Message Manipulations [from]

GENERAL		ACTION	
Index	3	Action Subject	Header.From.URL.Host
Name	from	Action Type	Modify
Manipulation Set ID	2	Action Value	'192.65.'
Row Role	Use Current Condition		

MATCH	
Message Type	Invite.Request
Condition	

Figure 54: Message Manipulation: From Header host Part Modification towards Google CES

- Below header rule is created to change P-Asserted Identity host part towards Google CES as '192.65.X.X'

Message Manipulations: [PAI modify]

GENERAL	ACTION
Index 4 Name PAI modify Manipulation Set ID 2 Row Role Use Current Condition	Action Subject Header:P-Asserted-Identity URL:Host Action Type Modify Action Value '192.65.X.X'

MATCH

Message Type Invite.Request	Condition
---	--

Figure 55: Message Manipulation: PAI Host Part Modification towards Google CES

- Below header rule is created to change To User part towards Google CES as '+1349XXXXXX'

Message Manipulations: [To]

GENERAL	ACTION
Index 6 Name To Manipulation Set ID 2 Row Role Use Current Condition	Action Subject Header.To:URL:User Action Type Modify Action Value '+1349XXXXXX'

MATCH

Message Type Invite.Request	Condition
---	--

Figure 56: Message Manipulation: To User Part Modification towards Google CES

- Below header rule is created to change To host part towards Google CES as 'us.telephony.goog'

Message Manipulations: [To_Host]

GENERAL	ACTION
Index 7 Name To_Host Manipulation Set ID 2 Row Role Use Current Condition	Action Subject Header.To:URL:Host Action Type Modify Action Value 'us.telephony.goog'

MATCH

Message Type Invite.Request	Condition
---	--

Figure 57: Message Manipulation: To Host Part Modification towards Google CES

Manipulation towards Google CES via UUI header:

- This SIP manipulation to insert a Hexa encoded value as a User-to-User header during Google CES Agent-Handoff.

The **URL** :
http://dialogflow.googleapis.com/v2beta1/projects/ccai-3898XX/conversations/SR_QAZ
Hexa Encoded : 6XXXXXXXXXXXXXXXXXXXXXXXXXXXXX5A

Message Manipulations [User-to-User]

GENERAL	ACTION
Index 10 Name User-to-User Manipulation Set ID 0 Row Role Use Current Condition	Action Subject Header:User-To-User Editor Action Type Add Action Value 60 61 5F51415AA;encoding=hex;purpose=Goog.Session.Param Editor

MATCH
Message Type Invite:Request Editor Condition Editor

Figure 58: Message Manipulation: User-to-User header addition towards Google CES

Manipulation for Inbound messages from Google CES

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

Request URI header:

Message Manipulations [Request_URI_PSTN]

GENERAL		ACTION	
Index	8	Action Subject	Header:Request-URI.URL.User Editor
Name	Request_URI_PSTN	Action Type	Modify
Manipulation Set ID	3	Action Value	'214242' Editor
Row Role	Use Current Condition		

MATCH	
Message Type	Any.Request Editor
Condition	Editor

Figure 59: Message Manipulation: Request URI header towards PSTN

To Header:

Message Manipulations [To_PSTN]

GENERAL		ACTION	
Index	9	Action Subject	Header:To.URL.User Editor
Name	To_PSTN	Action Type	Modify
Manipulation Set ID	3	Action Value	'214242' Editor
Row Role	Use Current Condition		

MATCH	
Message Type	Any.Request Editor
Condition	Editor

Figure 60: Message Manipulation: To header towards PSTN

8 SIP INVITE To GOOGLE CES

8.1 SIP INVITE for SIPREC call

```
INVITE sip:+13614000000@us.telephony.goog;user=phone SIP/2.0
Via: SIP/2.0/TLS 192.65.100.222:5061;alias;branch=z9hG4bKac1515878973
Max-Forwards: 70
From: <sip:Audiocodes@192.65.100.222>;user=phone;tag=1c1451797144
To: <sip:Audiocodes@us.telephony.goog;user=phone>
Call-ID: 14526490261920251384@192.65.100.222
CSeq: 1 INVITE
Contact: <sip:192.65.100.222:5061;transport=tls>;src
Supported: timer,replaces,resource-priority,sdp-anat
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO
Require: siprec
Session-Expires: 1800;refresher=uas
Min-SE: 90
User-Agent: Mediant VE SBC/v.7.60A.100.022
Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/ccai-3898XX/conversations/Sr_14584>;purpose=Goog-ContactCenter-Conversation
Content-Type: multipart/mixed;boundary=boundary_aclc32
Content-Length: 2798
--boundary_aclc32
Content-Type: application/sdp
v=0
o=AudiocodesGW 1438053757 169388785 IN IP4 192.65.100.222
s=SBC-Call
c=IN IP4 192.65.100.222
t=0 0
m=audio 7064 RTP/SAVP 0 101
a=ptime:20
a=sendonly
a=label:1
a=fmtp:101 0-15,16
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:hH6VwqXGmE4z2J8Nnp6IXQeXrfah4JxiX4ogHir0
a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline:rtQOZfvjF5y/Ajk0b0DySxQmA/Sh+6GTjko78ik
a=crypto:3 AES_256_CM_HMAC_SHA1_80 inline:WpppEpYoE4mUe7JfXKdDCzcpUMP1fGsXfyeZErq1q82u61/qRD+cdQ612fCwg==
a=crypto:4 AES_256_CM_HMAC_SHA1_32 inline:1iIjZjIMiUkl1RE00FqYHkGoHuc6THFMk+w9tifiXu+ZwPcx6RDUsQNMd87G0w==
m=audio 7068 RTP/SAVP 0 101
c=IN IP4 192.65.100.222
a=ptime:20
a=sendonly
a=label:2
a=fmtp:101 0-15,16
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:7k4TFERSclDu+C6C9TdXTCHzN+0fyWuEqW+hcGoi
a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline:3Qq96EGBNFmJiwxj6wXXX1fLfhUV9Yt0aSgUGz+D
a=crypto:3 AES_256_CM_HMAC_SHA1_80 inline:QbNdrW3B+ELV54j6+vwfijFfwOW7WC/kLkKjo7wdfetie2m/njVVDk5tjRA==
a=crypto:4 AES_256_CM_HMAC_SHA1_32 inline:0/kJ2CCn2hm6jWR6Db6HJQpkk3L0FV8SEieqO3RsitgeappqrnFimeZ/C1XzfA==
```

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/Sr_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 single media lines with `a=sendonly`, for SIP GTP there will be a multiple 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 61: SIPREC Call

8.2 SIP INVITE for GTP call

```
INVITE sip:+13149000000@us.telephony.goog SIP/2.0
Via: SIP/2.0/TLS 192.65.100.222:5061;alias;branch=z9hG4bKac210501
Max-Forwards: 69
From: "Pradeep Gopal" <sip:214550000@192.65.100.222>;tag=1c1363300463
To: <sip:+13149000000@us.telephony.goog>
Call-ID: 1851113439268202513032@192.65.100.222
CSeq: 1 INVITE
Contact: <sip:214550000@192.65.100.222:5061;transport=tls>
Supported: 100rel,timer,replaces,resource-priority,sdp-anat
Allow: INVITE,OPTIONS,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,INFO
Expires: 180
Session-Expires: 1800;refresher=uas
Min-SE: 1800
User-Agent: Mediant VE SBC/v.7.60A.100.022
P-Asserted-Identity: "Pradeep Gopal" <sip:214550000@192.65.100.222>
Call-Info: <http://dialogflow.googleapis.com/v2beta1/projects/ccai-3898XX/conversations/Sr_1851113439268202513032>;purpose=Goog-ContactCenter-Conversation
Date: Tue, 26 Aug 2025 13:00:55 GMT
Allow-Events: telephone-event
Content-Type: application/sdp
Content-Length: 633
Cisco-Guid: 2295206282-2175996100-2295210062-2295217322
Timestamp: 1756213255
v=0
o=CiscoSystemsSIP-GW-UserAgent 658476784 1219741378 IN IP4 192.65.100.222
s=SIP Call
c=IN IP4 192.65.100.222
t=0 0
m=audio 7192 RTP/SAVP 0 101
a=ptime:20
a=fmtp:101 0-16
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:gV51G4J4rFnAKwmtb6U9Hd9OyEsbBVwNrIkQgBVQ
a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline:3HvTldAZ/quJlW23Wchl14yLx+7777iVXym2tXurW
a=crypto:3 AES_256_CM_HMAC_SHA1_80 inline:7Jj1VVOjE00Io9gR2ztFnaLGISugSqFlafy6751dZYMyq+LGRB5BSyH0d8djw==
a=crypto:4 AES_256_CM_HMAC_SHA1_32 inline:UvPiO2AA0v13J3RyUyBEU8mx5/Hrojmrgrs/T/hIEA0hJ3KvfvS1cFJ3aZkRQBYA==
```

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/Sr_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 single media lines with `a=sendonly`, for SIP GTP there will be a multiple 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 62:GTP Call

9 AudioCodes VE SBC Running configuration

Attached is the AudioCodes VE SBC Running configuration.



AudioCodes -
Running config.ini

10 Summary of Tests and Results

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
35	UUI header test	Use the UUI header as opposed to call-info header to send conversation id	Call should process as normal, and recording under conversation ID derived from UUI header as opposed to call-info	PASSED	Calls get successfully connected to Live agent when using UUI header instead of call-info header.
36	Keep_conversation_running=TRUE test	ConversationProfile needs to have SipConfig set with keepConversationRunning = TRUE. Send first call with a Call-Info header and have a call for 2 turns. End the call. Send second call with the SAME Call-Info header as above and have a call for 3 turns. End the call.	Two calls having the same call-info has both conversation details.	PASSED	Both call transcripts are present for the same conversation session id.
37	Live Agent Transfer	Call goes to virtual agent, initial live agent handoff and verify outgoing SIP INVITE, call connection and disconnection		PASSED	Call gets connected successfully to BOT and INVITE sent successfully to connect with Agent.
38	Live Agent Transfer	Call goes to virtual agent, initial live agent handoff and verify outgoing SIP INVITE, call connection and disconnection. Make calls to +13149XXXXXX, "speak		PASSED	Call was connected successfully with live agent and when performing conversation "Speak to an agent", a new INVITE was sent

ID	Title	Description	Expected Results	Status (Passed or Failed etc)	Observations
		to an agent", +1-972-852-XXXX should then ring and get connected as the agent			from Google to transfer to an agent and call gets connected successfully with both-way audio.
39	UUI headers	Call goes to virtual agent, say "end the call", validate that the SIP BYE has a UUI header Make calls to +13149XXXXXX, "end the call", check SIP BYE and ensure there is one or more (identify if there are 3 or 1) UUI headers with purpose Goog-Session-Param		PASSED	Calls get connected successfully to live agents and when performing conversation "End the call", the call gets disconnected normally with 3 UUI header.
4 0	SIP REFER	Call goes to virtual agent, say "send a sip refer", validate that a SIP REFER is received to 972-852-XXXX. Make calls to +1314XXXXXX "send a sip refer", SIP REFER should be received with refer to set to 972-852-XXXX		PASSED	REFER request & transfer is successful.