Configuration Note

AudioCodes Professional Services – Interoperability Lab

Connecting Google Voice SIP Link with AudioCodes Mediant Gateway

audiocodes

Table of Contents

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: August-29-2022

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Document Name
Mediant 500 Gateway & E-SBC User's Manual
Mediant 800 Gateway & E-SBC User's Manual
Mediant 1000B Gateway & E-SBC User's Manual
SIP Message Manipulation Reference Guide
AudioCodes Configuration Notes

Document Revision Record

LTRT	Description
38145	Initial document release.
38146	Update Implementation Layout Figures; added section for SBC Session Refreshing Policy

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This Configuration Note describes how to add Session Border Controller functionality to the AudioCodes Mediant Gateways for interworking between PSTN (PBX or Switch) and the Google Voice SIP Link environment.

> This document assumes that the Customer has an already configured and up-and-running AudioCodes Mediant Gateway and now wishes to add SBC functionality for interconnecting with Google Voice SIP Link. As configuration settings of Gateway functionality may vary widely between customers, this document doesn't describe Gateway configuration. However, if you need assistance in your Gateway configuration and you have a valid support agreement with AudioCodes, please contact AudioCodes Professional Services (who will also do PoC testing, if required).

1.1 About the Google Voice SIP Link

Google Voice for Workspace today makes available to Premier customers the ability to connect any carrier of their choice to Google through a set of certified SBCs. Being able to connect other carriers to Google Voice allows customers to:

- Leverage existing investments in on-premises infrastructure.
- Maintain uninterrupted service with existing carriers.
- Accelerate adoption of Voice offering a unified experience for users while keeping in place past negotiated calling rates with their carrier.
- Reduce total cost of ownership.

1.2 About AudioCodes SBC Product Series

AudioCodes' family of SBC devices enables reliable connectivity and security between the Enterprise's and the service provider's VoIP networks.

The SBC provides perimeter defense as a way of protecting Enterprises from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP-PBX to any service provider; and Service Assurance for service quality and manageability.

Designed as a cost-effective appliance, the SBC is based on field-proven VoIP and network services with a native host processor, allowing the creation of purpose-built multiservice appliances, providing smooth connectivity to cloud services with integrated quality of service, SLA monitoring, security and manageability. The native implementation of SBC provides a host of additional capabilities that are not possible with standalone SBC appliances such as VoIP mediation, PSTN access survivability, and third-party value-added services applications. This enables Enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

AudioCodes SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware. The SBC can be offered as a Virtualized SBC, supporting the following platforms: Hyper-V, AWS, AZURE, AWP, KVM and VMWare.

2 Component Information

2.1 AudioCodes Mediant Gateway Version

Table 2-1: AudioCodes Mediant Gateway Version

SBC Vendor	AudioCodes
Models	■ Mediant 500 Gateway & E-SBC ■ Mediant 800B/C Gateway & E-SBC ■ Mediant 1000B Gateway & E-SBC
Certified Software Versions	■ 7.20A.258.628 or later ■ 7.40A.250.262 or later
Protocol	SIP/TLS (to the Google Voice SIP Link system)
Additional Notes	None

2.2 Google Voice SIP Link System Version

Table 2-2: Google Voice SIP Link System Version

Vendor	Google
Model	Google Voice
Software Version	
Protocol	SIP
Additional Notes	None

2.3 PSTN PBX Version

Table 2-3: PSTN PBX Version

Vendor/Service Provider	
SSW Model/Service	PBX
Software Version	
Protocol	
Additional Notes	None

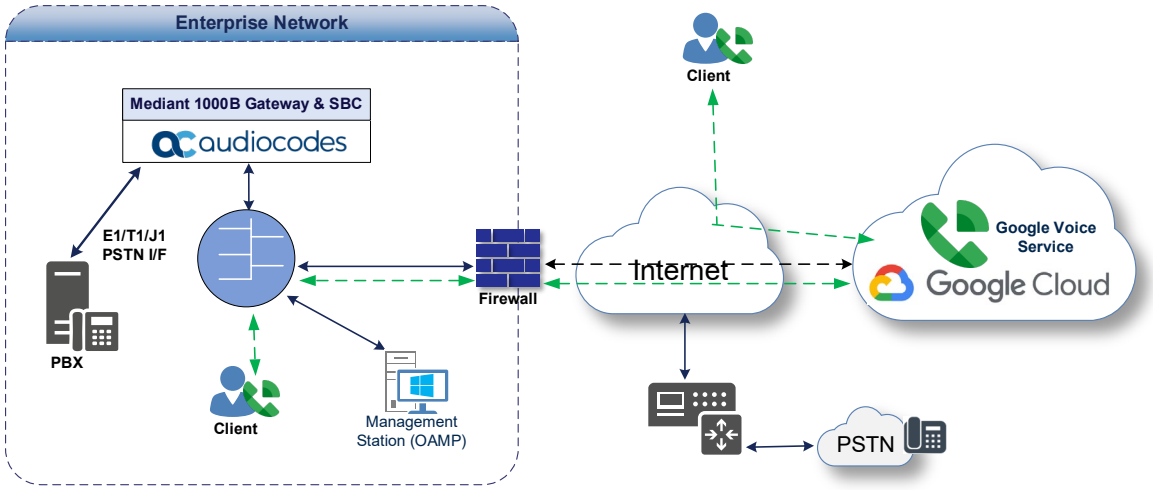
2.4 Interoperability Test Topology

The interoperability testing between the AudioCodes Mediant Gateway and PSTN PBX or Switch with the Google Voice SIP Link system, was done using the following topology setup:

- Enterprise deployed with the Administrator's management station, located on the LAN.
- Enterprise deployed with the Google Voice SIP Link system located on the WAN for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise PBX to the PSTN network, using the Google Voice SIP Link service or interconnect between PSTN Provider and Google Voice SIP Link.
- AudioCodes Mediant Gateway implemented to interconnect between the Enterprise PBX or PSTN Provider and the Google Voice SIP Link system.

The figures below illustrate possible topologies:

Figure 2-1: Layout with Mediant Gateway Implementation



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	■ Google Voice SIP Link system located on the WAN. ■ PSTN connection located in the enterprise branch.
Signaling Transcoding	■ Google Voice SIP Link system operates with SIP-over-TLS transport type. ■ PSTN connection can be done through E1 or T1 or J1 interface using different PSTN protocol types, like ISDN, R2MFC or CAS.
Codecs Transcoding	■ Google Voice SIP Link system supports OPUS, G.722, G.711U-law and G.711A-law coders. ■ Mediant 500 and Mediant 800B/C supports OPUS, G.722, G.711A-law, G.711U-law, and G.729 coders ■ Mediant 1000B supports G.711A-law, G.711U-law and G.729 coders.
Media Transcoding	■ Google Voice SIP Link system operates with SRTP media type, DTLS or SDES encryption methods. ■ Mediant 500 and Mediant 800B/C operates with SRTP media type with DTLS or SDES encryption methods. ■ Mediant 1000B operates with SRTP media type with SDES encryption only.

2.4.2 Known Limitations

Google Voice SIP Link system uses DTLS for securing media traffic. Mediant 1000B supports SDES encryption only. There were no other limitations observed in the interoperability tests performed for the AudioCodes Mediant Gateways interworking between the Google Voice SIP Link system and PSTN's PBX or Switch.

3 Configuring Google Voice SIP Link

For configuring your Google Voice SIP Link setup, go to *support.google.com/a?p=siplink*.

Before you begin configuration:

- Contact your local Google representative to enable Google Voice on your Corporate Google account.
- Make sure you have Google Workspace admin credentials.

4 Configuring SBC Application on Mediant Gateway

This section provides guidelines for configuring the SBC Application on the AudioCodes Mediant Gateway, used as a PSTN Gateway for supporting interworking with the Google Voice SIP Link system. To do this, SBC entities needed to be configured on the device. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 3.

This configuration is performed using the Mediant Gateway's embedded Web server (hereafter, referred to as *Web interface*).

- For implementing the Google Voice SIP Link system and PSTN SIP Trunk based on the configuration described in this section, the AudioCodes Mediant Gateway must be installed with a License Key that includes the following software features:
  - **Number of SBC sessions** [Based on requirements]
  - **IP Security**
  - **Coders** [Based on requirements]

  For more information about the License Key, contact your AudioCodes sales representative.
- The Gateway configuration (PSTN Interface) can vary from customer to customer. Therefore, in this document, we only provide the configuration changes that are necessary to add SBC functionality to the Gateway to work with the Google Voice SIP Link system.
- The scope of this document does **not** cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document, which can be found at AudioCodes website

4.1 Prerequisites

Before you begin configuration, make sure you have obtained the following for each Mediant Gateway you wish to pair with Google Voice SIP Link System:

- Public IP address
- Public certificate that is issued by one of the Google supported CAs

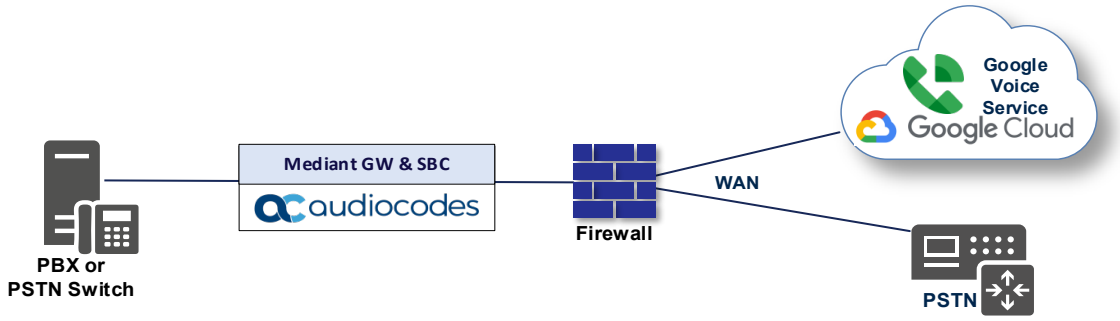
4.2 IP Network Interfaces

The Gateway configuration can vary from customer to customer, therefore in this document, we assume that there is no additional configuration of the IP network interfaces needed to add SBC functionality to the Gateway to work with the Google Voice SIP Link system.

This interoperability test topology employs the following deployment method:

- Mediant Gateway interfaces with the following IP entities:
  - Management Servers located on the LAN
  - Google Voice SIP Link system located on the WAN
- Mediant SBC application connects to the WAN through a DMZ network
- The type of physical connection depends on the method used to connect to the Enterprise's network. In the interoperability test topology, the Mediant Gateway and SBC connect to the DMZ using dedicated Ethernet port.

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.2.1 Network Interfaces

This section describes the example of the IP network interfaces, which can be already configured on the Mediant Gateway. If changes are need, proceed as follows.

To configure the IP network interfaces:

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Configure the IP interfaces as follows (your network parameters might be different):

Table 4-1: Configuration Example of the Network Interface Table

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	DNS	I/F Name	Ethernet Device
0	OAMP+ Media + Control	IPv4 Manual	10.15.77.77	16	10.15.0.1	10.15.27.1	LAN_IF	vlan 1
1	Media + Control (as this interface points to the internet, enabling OAMP is not recommended)	IPv4 Manual	195.189.192.156 (DMZ IP address of the Mediant)	25	195.189.192.129 (router's IP address)	According to your Internet provider's instructions	WAN_IF	vlan 2

4.2.2 Configure NAT Translation (Optional)

If the Mediant Gateway is in the corporate network with only LAN interface, then it probably implements private IP addresses. The NAT Translation table lets you configure network address translation (NAT) rules for translating source IP addresses into NAT IP addresses (*global* - *public*), used in front of the corporate firewall facing the Google Voice.

To configure the NAT translation rules:

1. Open the NAT Translation table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**).
2. Add a new NAT Translation rule by clicking **+New** at the top of the interface, and then configure the parameters using the table below as reference.

Table 4-2: NAT Translation Rule

Index	Source Interface	Source Start Port	Source End Port	Target IP Address	Target Start Port	Target End Port
0	LAN_IF (arbitrary descriptive name)	1	65535	<Public IP Address>	1	65535

3. Click **Apply**.

4.3 Configure TLS Context for Google Voice

This section describes how to configure the SBC for using a TLS connection with the Google Voice SIP Link System. This configuration is essential for a secure SIP TLS connection and for secure SDES media transport.

For more certificate structure options, refer to Google Voice SIP Link System documentation.

4.3.1 Configure the NTP Server Address

This section describes how to configure the NTP server's IP address. It is recommended to implement an NTP server (local NTP server or another global NTP server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties. It is important, that the NTP Server is located on the OAMP IP Interface (LAN_IF in our case) or will be accessible through it.

To configure the NTP server address:

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).
2. In the 'Primary NTP Server Address' field, enter the IP address of the first NTP server (e.g., time.google.com).
3. In the 'Secondary NTP Server Address' field, enter the IP address of the second NTP server (e.g., time2.google.com).
4. Click Apply.

4.3.2 Create a TLS Context for Google Voice SIP Link System

This section describes how to request a certificate for the Mediant SBC WAN interface and configure it. The certificate is used by the Mediant SBC to authenticate the connection with the Google Voice SIP Link System.

The procedure involves the following main steps:

- Create a TLS Context for Google Voice SIP Link System
- Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority
- Deploy the SBC and Root / Intermediate certificates on the SBC

To create a TLS Context for Google Voice SIP LINK System:

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Create a new TLS Context by clicking **+New**, and then configure the parameters using the table below as reference.

Table 4-3: New TLS Context

Index	Name	TLS Version
1	Google (arbitrary descriptive name)	TLSv1.2
All other parameters can be left unchanged with their default values.		

3. Click **Apply**; you should see the new TLS Context and option to manage the certificates at the bottom of 'TLS Context' table.

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

This section describes how to generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority.

To generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority:

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the Google TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Under the **Certificate Signing Request** group, do the following:
    a. In the 'Common Name [CN]' field, enter the SBC FQDN name (for example, **sbc.audiocodes.com**).
    b. In the '1st Subject Alternative Name [SAN]' field, change the type to 'DNS' and enter the SBC FQDN name (based on example above, **sbc.audiocodes.com**).
    c. Change the 'Private Key Size' based on the requirements of your Certification Authority. Many CAs do not support private key of size 1024.
    d. To change the key size on TLS Context, go to: **Generate New Private Key and Self-Signed Certificate**, change the 'Private Key Size' and then click **Generate Private-Key**. To use 2048 as a Private Key Size value, you can click **Generate Private-Key** without changing the default key size value.
    e. Fill in the rest of the request fields according to your security provider's instructions.
    f. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:
4. Copy the CSR from the line "**----BEGIN CERTIFICATE**" to "**END CERTIFICATE REQUEST----**" to a text file (such as Notepad), and then save it to a folder on your computer with an identifiable file name, for example, *certreq.txt*.
5. Send *certreq.txt* file to the Certified Authority Administrator for signing.

4.3.4 Deploy the SBC and Root / Intermediate Certificates on the SBC

After obtaining the SBC signed and Trusted Root/Intermediate Certificate from the CA, install the following:

- SBC certificate.
- Root / Intermediate certificates.

To install the SBC certificate:

1. In the SBC's Web interface, return to the TLS Contexts page and do the following:
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
   b. Scroll down to the Upload certificates files from your computer group, click the **Choose File** button corresponding to the 'Send Device Certificate...' field, navigate to the certificate file obtained from the CA, and then click **Load File** to upload the certificate to the SBC.
2. Validate that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page:
3. In the SBC's Web interface, return to the TLS Contexts page, select the required TLS Context index row, and then click the **Certificate Information** link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name.
4. In the SBC's Web interface, return to the TLS Contexts page.
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the Trusted Root **Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
   b. Click the **Import** button, and then select all Root/Intermediate Certificates obtained from your Certification Authority to load.
5. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

> The above method creates a signed certificate for an explicit device, on which a Certificate Sign Request was generated (and signed with private key).

4.3.5 Deploy Google Trusted Root Certificate

> Loading Google Trusted Root Certificates to AudioCodes' SBC is mandatory for implementing an MTLS connection with the Google Voice network.

Download the certificate from *support.google.com/a?p=siplink* and follow the steps above to import the Google root certificate (GTSR1) to the Trusted Root storage.

4.4 Configure Media Realms

Media Realms allow the dividing of the UDP port ranges for use on different interfaces. Since default Media Realms configuration was used in this interoperability test topology, no additional configuration is needed. Just check that the Media Realm is configured as the default and assigned to the WAN IP interface (as in our example).

To confirm configuration of the Media Realm:

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Check that the default (Index 0) Media Realm is configured as follows:

Table 4-4: Configuration Example of Media Realm in Media Realm Table

Index	Name	IPv4 Interface Name	Port Range Start	Number of Media Session Legs	Default Media Realm
0	DefaultRealm	WAN_IF	6000	100 (media sessions assigned with port range)	Yes
All other parameters can be left unchanged at their default values.					

4.5 Configure SIP Signaling Interfaces

This section describes how to configure SIP Signaling Interfaces. A SIP Interface defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface (configured in the Interface Table above) and a Media Realm.

Since the default (Index 0) SIP Interface is already configured with Gateway Type, you need to add an additional SIP Interface for SBC application.

To configure SIP Interfaces:

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Configure SIP Interfaces. The table below is an example of the configuration. You can change some parameters according to your requirements.

Table 4-5: Configuration Example of SIP Interfaces in SIP Interface Table

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Enable TCP Keepalive	Classification Failure Response Type	TLS Context Name	TLS Mutual Authentication
0	SI-GW (arbitrary name)	WAN_IF	GW	5070	0	0	-	500 (default)	-	-
1	SI-SBC (arbitrary name)	WAN_IF	SBC	5060	0	5061[1]	Enable	0[2]	Google	Enable
All other parameters can be left unchanged at their default values.										

[1] Port 5061 is mentioned as an example when any TLS port can be used.
[2] Recommended to prevent DoS attacks.

4.6 Configure Proxy Sets and Proxy Address

This section describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

For the interoperability test topology, two Proxy Sets need to be configured for the following IP entities:

- Move the default Proxy Set (Index 0) to the SBC SIP Interface
- Google Voice SIP Link system
- Gateway Application

The Proxy Sets are later applied to the VoIP network by assigning them to IP Groups.

To configure Proxy Sets:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Configure Proxy Sets as shown in the table below:

Table 4-6: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Redundancy Mode	Proxy Hot Swap	Proxy Load Balancing Method
0	ProxySet_0	SI-SBC	-	Leave default	-	Leave default	Leave default
1	PS-Google (arbitrary name)	SI-SBC	Google[3]	Using Options	Homing	Enable	Round Robin
2	PS-Gateway (arbitrary name)	SI-SBC	default	Using Options	-	Leave default	Leave default

[3] Configured in Section 4.3.2.

4.6.1 Configure a Proxy Address

This section describes how to configure a Proxy Address.

To configure a Proxy Address for Google Voice:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) click the Proxy Set **PS-Google**, and then click the Proxy Address link located below the table; the Proxy Address table opens.
2. Click **+New** and configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-7: Configuration Proxy Address for Google Voice SIP Link System

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	siplink.telephony.goog:5672	TLS	0	0

3. Click **Apply**.

To configure a Proxy Address for Gateway Application:

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**) and then click the Proxy Set **PS-Gateway**, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
2. Click **+New** and configure the address of the Proxy Set according to the parameters described in the table below:

Table 4-8: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	195.189.192.156:5070 (IP and port of the Gateway SIP Interface[4])	UDP	0	0

3. Click **Apply**.

[4] Configured in Section 4.5

4.7 Configure Coders

This section describes how to configure coders (termed *Coder Group*). The Google Voice SIP Link system supports OPUS and G.722 coders. While the Mediant Gateway may support other dedicated coders, you need to configure the Coder Group with the supported coders for the Google Voice SIP Link system.

> The Coder Group ID for this entity will be assigned to its corresponding IP Profile in the next step.

To configure coders:

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).
2. From the 'Coder Group Name' dropdown, select **0:AudioCodersGroups_0** and add the required codecs as follows:

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711 U-law	20	64	0	Disabled
G.711 A-law	20	64	8	Disabled

3. Click **Apply** and confirm the configuration change in the prompt that pops up.

4.8 Configure IP Profiles

This section describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

To configure IP Profile for the Google Voice SIP Link system:

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **+New** and add the IP Profile for Google Voice SIP Link System interface. Configure the parameters using the table below as reference.

Table 4-9: Configuration Example: Google Voice IP Profile

Parameter	Value
General	
Index	**0**
Name	**Google** (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
Symmetric MKI	**Enable** (relevant only with SDES method, for DTLS don't configure)
SBC Enforce MKI Size	**Enforce** (relevant only with SDES method, for DTLS don't configure)
SBC Media Security Method	Use **SDES** (the default value) for this parameter, as the Mediant 1000B does not support DTLS. For Mediant 500/800, **DTLS** can be configured. Note: Google does not support the **BOTH** value for this parameter.
Reset SRTP Upon Re-key	**Enable**
Generate SRTP Keys Mode	**Always**
SBC Remove Crypto Lifetime in SDP	**Yes**
SBC Media	
Extension Coders Group	**AudioCodersGroups_0**
SDP Handle SRTP	**Add**
RTCP Mux	**Supported**
SBC Signaling	
P-Asserted-Identity Header Mode	**Add**
Session Expires Mode	**Supported**
Remote re-INVITE	**Not Supported**
All other parameters can be left unchanged with their default values.	

3. Click **Apply**.

To configure an IP Profile for the Gateway Application:

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **+New** add the IP Profile for the Gateway Application. Configure the parameters using the table below as reference.

Table 4-10: Configuration Example: Gateway Application IP Profile

Parameter	Value
General	
Index	**1**
Name	**GW**
Media Security	
SBC Media Security Mode	**Not Secured**
All other parameters can be left unchanged with their default values.	

3. Click **Apply**.

4.9 Configure IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In this interoperability test topology, IP Groups must be configured for the following IP entities:

- Google Voice SIP Link system
- Gateway Application

To configure IP Groups:

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Configure an IP Group for the Google Voice SIP Link system:

Parameter	Value
Index	**1**
Name	**IPG-Google** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**PS-Google**
IP Profile	**Google**
SIP Group Name	**trunk.sip.voice.google.com** (according to Google requirement)
SIP Source Host Name	**trunk.sip.voice.google.com** (according to Google requirement)
Proxy Keep-Alive using IP Group settings	**Enable**
All other parameters can be left unchanged with their default values.	

3. Configure an IP Group for the Gateway Application:

Parameter	Value
Index	**2**
Name	**IPG-Gateway** (arbitrary descriptive name)
Type	**Server**
Proxy Set	**PS-Gateway**
IP Profile	**GW**
All other parameters can be left unchanged with their default values.	

4.10 Configure SRTP

This section describes how to configure media security. The Google Voice SIP Link System Interface uses SRTP only, so you need to configure the SBC to operate in the same manner. By default, SRTP is disabled.

To configure media security:

1. Open the Media Security page (**Setup menu > Signaling & Media tab > Media folder > Media Security**).
2. From the '**Media Security**' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.

4.11 Configure IP-to-IP Call Routing Rules

This section describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between Google Voice SIP Link system and PSTN SIP Trunk:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity
- Calls from Google Voice SIP Link system to the PSTN Interface
- Calls from PSTN Interface to the Google Voice SIP Link system

To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure routing rules as shown in the table below:

Table 4-11: Configuration IP-to-IP Routing Rules

Index	Name	Source IP Group	Request Type	Dest Type	Dest IP Group	Internal Action
0	Terminate OPTIONS	Any	OPTIONS	Internal		Reply(Response='200')
1	Google to PSTN (arbitrary name)	IPG-Google		IP Group	IPG-Gateway	
2	PSTN to Google (arbitrary name)	IPG-Gateway		IP Group	IPG-Google	

The routing configuration may change according to your specific deployment topology.

4.12 Configure Number Manipulation Rules

This section describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.9 on page 17) to denote the source and destination of the call.

Adapt the manipulation table according to your environment dial plan.

For example, for this interoperability test topology, a manipulation is configured to add the "+" (plus sign) to the destination and source numbers (if it does not exists) for calls from the PSTN Gateway IP Group to the Google Voice SIP Link system IP Group, for any destination username pattern.

To configure a number manipulation rule:

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).

2. Configure the rules according to your setup.

The table below is an example of configured IP-to-IP outbound manipulation rules for calls between the Google Voice SIP Link system IP Group and PSTN SIP Trunk IP Group:

Rule Index	Description
0	Calls from any IP Group to Google IP Group with any destination number between 1 to 9, add "+" to the prefix of the destination number.
1	Calls from any IP Group to Google IP Group with a source number between 1 to 9, add "+" to the prefix of the source number.

4.13 Configure Message Manipulation Rules

This section describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity).

Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

To configure SIP message manipulation rule for Google Voice SIP Link:

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 1) for Google Voice IP Group. This rule applies to messages sent to the Google Voice IP Group. This rule adds specific SIP Header (X-Google-Pbx-Trunk-Secret-Key), required by Google. This key will be returned to the customer from Google once the SIP Trunk is created on Google Voice admin console.

Parameter	Value
Index	**0**
Name	**Add X-Google Header** (arbitrary name)
Manipulation Set ID	**1**
Message Type	**Invite**
Action Subject	**Header.X-Google-Pbx-Trunk-Secret-Key**
Action Type	**Add**
Action Value	**'xxxxxxxxxx'** (Google Secret Key)

3. Configure another manipulation rule (Manipulation Set 1) for the Google Voice IP Group. This rule applies to messages sent to the Google Voice IP Group. This rule replaces the host part of the SIP To header with the 'trunk.sip.voice.google.com' value as required by Google.

Parameter	Value
Index	**1**
Name	**Change To Header** (arbitrary name)
Manipulation Set ID	**1**
Message Type	**Invite**
Action Subject	**Header.To.URL.Host**
Action Type	**Modify**
Action Value	**'trunk.sip.voice.google.com'**

4. Configure another manipulation rule (Manipulation Set 1) for the Google Voice IP Group. This rule applies to messages sent to the Google Voice IP Group. This rule replaces the user part of the SIP Contact header with the value from the SIP From header as required by Google.

Parameter	Value
Index	**2**
Name	**User part of Contact** (arbitrary name)
Manipulation Set ID	**1**
Message Type	**Invite**
Action Subject	**Header.Contact.URL.User**
Action Type	**Modify**
Action Value	**Header.From.URL.User**

5. Assign Manipulation Set ID 1 to the Google Voice IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the Google Voice IP Group, and then click **Edit**.
   c. Set the 'Outbound Message Manipulation Set' field to **1**.
   d. Click **Apply**.

4.14 Configure Firewall Settings (Optional)

As an additional security measure, there is an option to configure traffic filtering rules (access list) for incoming traffic on AudioCodes SBC. For each packet received on the configured network interface, the SBC searches the table from top to bottom until the first matching rule is found. The matched rule can permit (allow) or deny (block) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted. Please note that the firewall is stateless. The blocking rules will apply to all incoming packets, including UDP or TCP responses.

To configure a firewall rule:

1. Open the Firewall table (**Setup** menu > **IP Network** tab > **Security** folder> **Firewall**).
2. Configure the following Access list rules for WAN IP Interface, based on the list of Google Voice SIP Link System Servers:

Table 4-12: Firewall Table Rules

Index	Source IP	Subnet Prefix	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
0	<Public DNS Server IP> (e.g., 8.8.8.8)	32	0	65535	Any	Enable	WAN_IF	Allow
1	216.236.36.145	32	0	65535	TCP	Enable	WAN_IF	Allow
2	<SIP Trunk>	32	0	65535	UDP	Enable	WAN_IF	Allow
49	0.0.0.0	0	0	65535	Any	Enable	WAN_IF	Block

Be aware, that if in your configuration, connectivity to other entities is performed through the same IP Interface as Google Voice (WAN_IF in our example), you must add rules to allow traffic from these entities. See an example in row 2.

4.15 Configure SBC Session Refreshing Policy

This section describes how to configure the 'SBC Session Refreshing Policy' parameter. In some cases, Google does not perform a refresh of Session Timer even when it confirms that it will be refresher. To resolve this issue, the SBC is configured as Session Expire refresher.

To configure SBC Session Refreshing Policy:

1. Open the Admin page: Append the case-sensitive suffix 'AdminPage' to the device's IP address in your Web browser's URL field (e.g., http://10.15.77.77/AdminPage).
2. In the left pane of the page that opens, click ***ini Parameters***.
3. Enter these values in the 'Parameter Name' and 'Enter Value' fields:

Parameter	Value
SBCSESSIONREFRESHINGPOLICY	**1** (enables SBC as refresher of Session Timer)

4. Click the **Apply New Value** button for each field.

According to Google requirements, refreshment interval should be 15 minutes.

To configure SBC Session Refresh Timer:

1. Open the SIP Definitions General Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **SIP Definitions General Settings**).
2. In the 'Session-Expires [sec]' field, enter **900** (SBC session refresh timer in seconds).
3. Click **Apply**.

4.16 Adopt Gateway Configuration

This section describes changes required in the Gateway Application configuration in order adopt it work with SBC application.

4.16.1 Configure Gateway Tel-to-IP Routing Rule

This section describes how to configure the Gateway Tel-to-IP routing rule for routing calls from PSTN to Google Voice through the SBC application. We assume that Gateway is already configured with Trunk Group (e.g., Index 1).

To configure Tel-to-IP routing rules:

1. Open the Tel-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Routing** > **Tel -> IP Routing**).
2. Click on existing routing rule and configure it as shown in the table below.
3. Click **Apply**.

Table 13: Gateway Tel-to-IP Routing Rule

Name	Source Trunk Group ID	Destination IP Address	Destination Port	Transport Type
PSTN to Google Voice (arbitrary name)	1	195.189.192.156	5060	UDP
		(IP and port of the SBC SIP Interface[5])		
All other parameters can be left unchanged with their default values.				

4.16.2 Configure Gateway IP-to-Tel Routing Rule

This section describes how to configure Gateway IP-to-Tel routing rule for routing calls from Google Voice to PSTN through SBC application. We assume that Gateway already configured with Trunk Group (e.g., Index 1).

To configure Tel-to-IP routing rules:

1. Open the IP-to-Tel Routing table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Routing** > **IP -> Tel Routing**).
2. Click on existing routing rule and configure it as shown in the table below.
3. Click **Apply**.

Table 14: Gateway IP-to-Tel Routing Rule

Name	Source SIP Interface	Destination Type	Trunk Group ID	IP Profile
PSTN to Google Voice (arbitrary name)	Any	Trunk Group	1	GW[6]
All other parameters can be left unchanged with their default values.				

[5] Configured in Section 4.5
[6] Configured in Section 4.8

4.16.3 Configuring Gateway Source/Destination Number Manipulation Rules

The number manipulation tables let you configure rules for manipulating source and destination telephone numbers for IP-to-Tel and Tel-to-IP calls. This section describes how to configure Gateway rules for manipulating with the source and destination number in the IP-to-Tel calls from Google Voice to PSTN because most PSTN PBXs didn't support full E.164 format (with '+' sign).

To configure a number manipulation rules:

1. Open the required Phone Number Manipulation table (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Manipulation** > **Dest Number IP->Tel** or **Source Number IP->Tel**).
2. Click **New** and configure a number manipulation rule according to the parameters described in the tables below.
3. Click **Apply**.

Table 15: Gateway Destination Phone Number Manipulation for IP-to-Tel Calls

Name	Destination Phone Pattern	Stripped Digits From Left
Strip + (arbitrary name)	+	1
All other parameters can be left unchanged with their default values.		

Table 16: Gateway Source Phone Number Manipulation for IP-to-Tel Calls

Name	Source Phone Pattern	Stripped Digits From Left
Strip + (arbitrary name)	+	1
All other parameters can be left unchanged with their default values.		

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com

Document #: LTRT-38146