
Ribbon SBC Edge 1K_2K_SWe Edge R9.0 Interop with Google Voice SIP Link : Interoperability Guide



Table of Contents

- [Interoperable Vendors](#)
- [Copyright](#)
- [Document Overview](#)
 - [About Ribbon SBC SWe Edge](#)
 - [About Google Voice](#)
- [Scope/Non-Goals](#)
- [Audience](#)
- [Pre-Requisites](#)
- [Product and Device Details](#)
- [Network Topology and E2E Flow Diagrams](#)
 - [Deployment Topology](#)
 - [Interoperability Test Lab Topology](#)
 - [Call Flow Diagram](#)
- [Document Workflow](#)
- [Installing Ribbon SBC SWe Edge](#)
- [Ribbon SBC SWe Edge Configuration](#)
 - [Accessing SBC SWe Edge](#)
 - [License and TLS Certificates](#)
 - [View License](#)
 - [SBC Certificate](#)
 - [Trusted CA Certificates](#)
 - [Networking Interfaces](#)
 - [Configure Static Routes](#)
 - [Global Configuration](#)
 - [Media Profiles](#)
 - [Transformation Table](#)
 - [SBC SWe Edge Configuration for PSTN side](#)
 - [Media List - PSTN](#)
 - [Message Manipulation - PSTN](#)
 - [SIP Profile - PSTN](#)
 - [SIP Server Table - PSTN](#)
 - [Call Routing Table - PSTN](#)
 - [SIP Signaling Group - PSTN](#)
 - [SBC SWe Edge Configuration for Google Voice SIP Link side](#)
 - [DNS](#)
 - [TLS Profile](#)
 - [SDES-SRTP Profile](#)
 - [Media List - GV](#)
 - [Message Manipulation - GV](#)
 - [SIP Profile - GV](#)
 - [SIP Server Table - GV](#)
 - [Call Routing Table - GV](#)
 - [SIP Signaling Group - GV](#)
 - [Call Routing Table Entry](#)
- [Google Voice Configuration](#)
- [Supplementary Services & Features Coverage](#)
- [Caveats](#)
- [Support](#)
- [References](#)
- [Conclusion](#)

Interoperable Vendors



Copyright

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved. The compilation (meaning the collection, arrangement and assembly) of all content on this site is protected by U.S. and international copyright laws and treaty provisions and may not be used, copied, reproduced, modified, published, uploaded, posted, transmitted or distributed in any way, without prior written consent of Ribbon Communications Inc.

The trademarks, logos, service marks, trade names, and trade dress ("look and feel") on this website, including without limitation the RIBBON and RIBBON logo marks, are protected by applicable US and foreign trademark rights and other proprietary rights and are the property of Ribbon Communications Operating Company, Inc. or its affiliates. Any third-party trademarks, logos, service marks, trade names and trade dress may be the property of their respective owners. Any uses of the trademarks, logos, service marks, trade names, and trade dress without the prior written consent of Ribbon Communications Operating Company, Inc., its affiliates, or the third parties that own the proprietary rights, are expressly prohibited.

Document Overview

This document outlines the configuration best practices for Ribbon SBC SWe Edge interworking with Google Voice SIP Link.

About Ribbon SBC SWe Edge

The Ribbon Session Border Controller Software Edition Lite (SBC SWe Edge) provides best-in-class communications security. The SBC SWe Edge dramatically simplifies the deployment of robust communications security services for SIP Trunking, Direct Routing, and Cloud UC services. SBC SWe Edge operates natively in the Azure and AWS Cloud as well as on virtual machine platforms including Microsoft Hyper-V, VMware and Linux KVM.

About Google Voice

Google Voice is a telephone service that provides a U.S. phone number to Google Account customers in the U.S. and Google Works customers in Canada, Denmark, France, the Netherlands, Portugal, Spain, Sweden, Switzerland and the United Kingdom. Calls are forwarded to the phone number that each user must configure in the account web portal. Users can answer and receive calls on any of the phones configured to ring in the web portal. While answering a call, the user can switch between the configured phones. Subscribers in the United States can make outgoing calls to domestic and international destinations. The service is configured and maintained by users in a web-based application, similar in style to Google's email service Gmail, or Android and iOS applications on smartphones or tablets.

Scope/Non-Goals

This document provides configuration best practices for deploying Ribbon's SBC SWe Edge for Google Voice SIP Link interop. Note that these are configuration best practices and each customer may have unique needs and networks. Ribbon recommends that customers work with network design and deployment engineers to establish the network design which best meets their requirements.

It is not the goal of this guide to provide detailed configurations that meet the requirements of every customer. Use this guide as a starting point, and build the SBC configurations in consultation with network design and deployment engineers.

Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring the Ribbon SBC.

To perform this interop, you need to

- use graphical user interface (GUI) or command line interface (CLI) of the Ribbon product.
- understand the basic concepts of TCP/UDP/TLS and IP/Routing.
- have SIP/RTP/SRTP to complete the configuration and for troubleshooting.

Note

This configuration guide is offered as a convenience to Ribbon customers. The specifications and information regarding the product in this guide are subject to change without notice. All statements, information, and recommendations in this guide are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided "AS IS". Users must take full responsibility for the application of the specifications and information in this guide.

Pre-Requisites

The following aspects are required before proceeding with the interop:

- Ribbon SBC SWe Edge
- Ribbon SBC SWe Edge license
 - This interop requires the acquisition and application of SIP sessions, as documented at [Working with Licenses](#)
- Public IP addresses
- TLS certificates for SBC SWe Edge
 - For more details, please visit [Working with Certificates](#)
- Google Workspace and Domain
 - Google Voice Premier license for the users
 - For more details, contact [Google support](#)

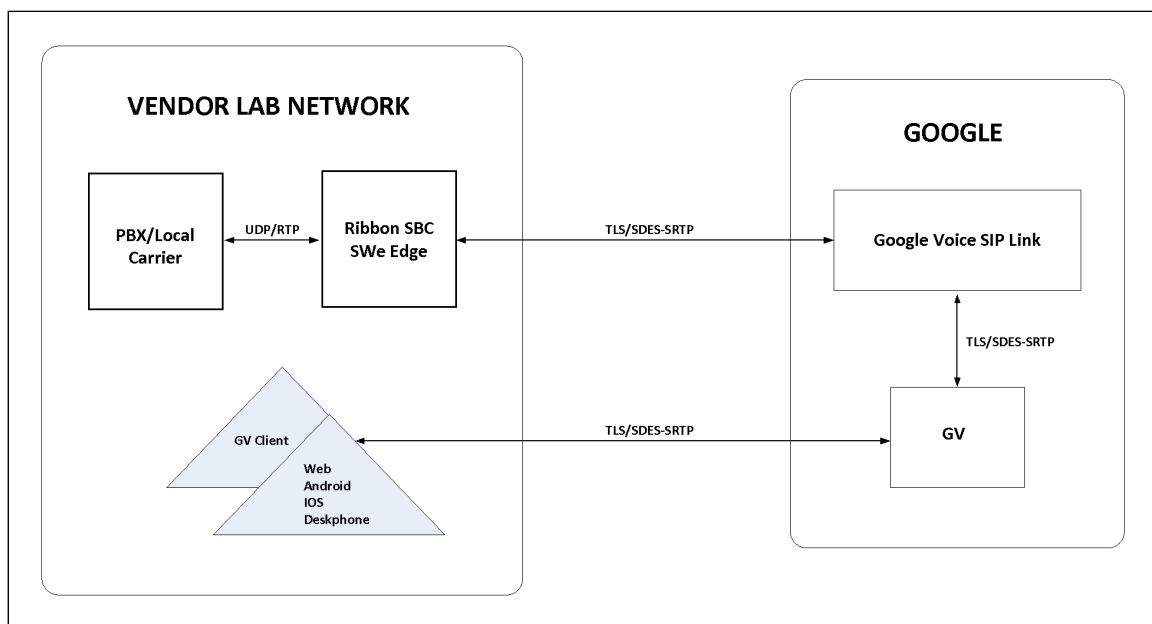
Product and Device Details

The configuration uses the following equipment and software:

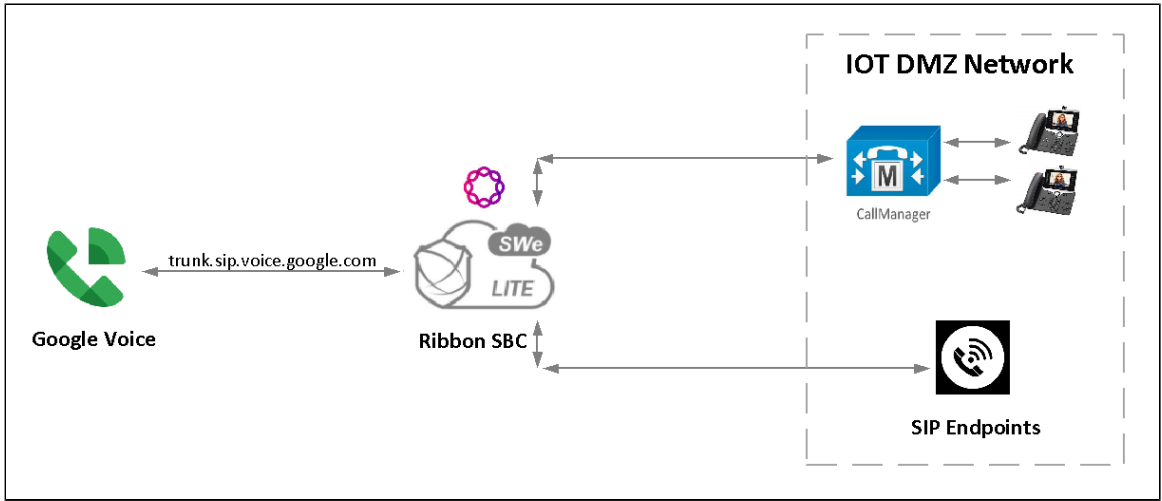
Product	Equipment/Service	Software Version
Ribbon SBC	Ribbon SBC SWe Edge	9.0.7
Google Voice SIP Link	Telephone Service	NA
Third-party Equipment	Cisco Unified Communications Manager	12.5.1.11900-146
Administration and Debugging Tools	Wireshark	3.4.9
	LX Tool	2.1.0.6

Network Topology and E2E Flow Diagrams

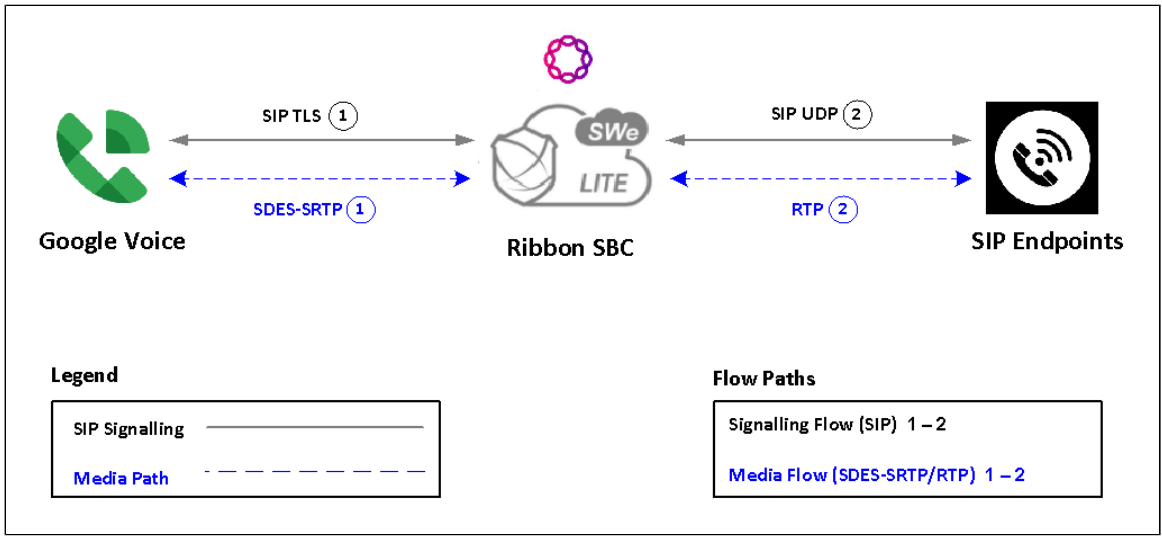
Deployment Topology



Interoperability Test Lab Topology

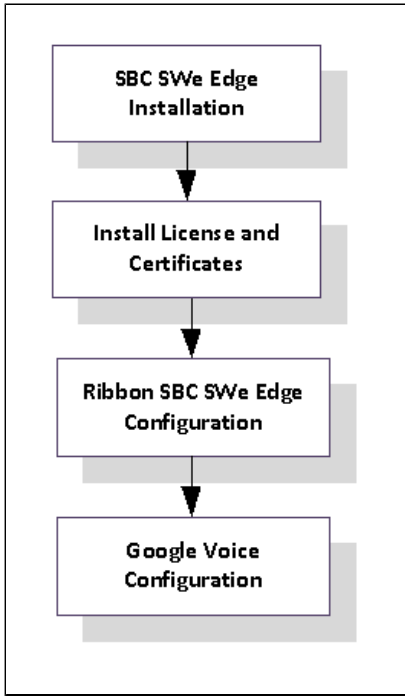


Call Flow Diagram



Document Workflow

The sections in this document follow the sequence below. The reader is advised to complete each section for successful configuration.



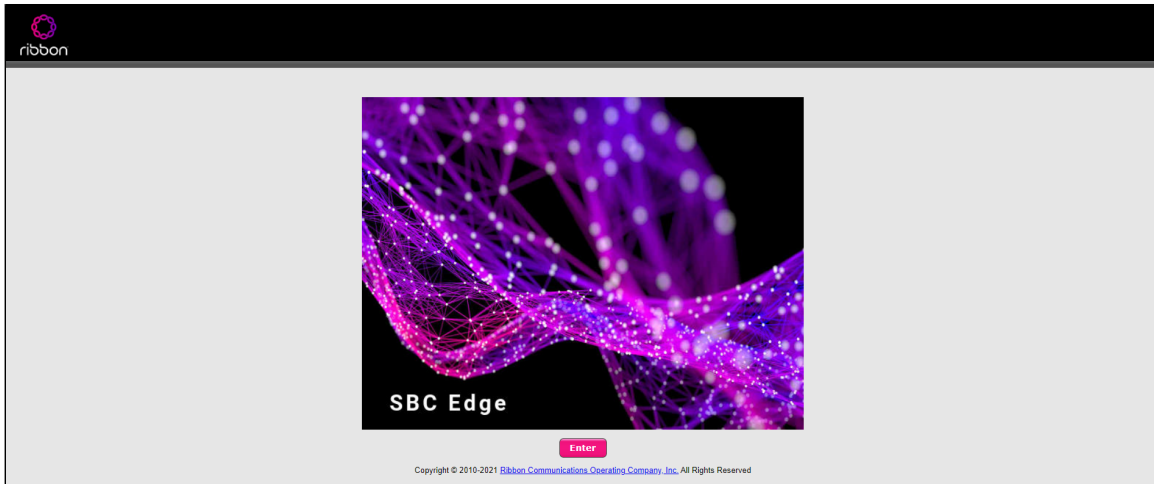
Installing Ribbon SBC SWe Edge

To deploy Ribbon SBC SWe Edge instance, refer to [Installing SBC SWe Edge](#).

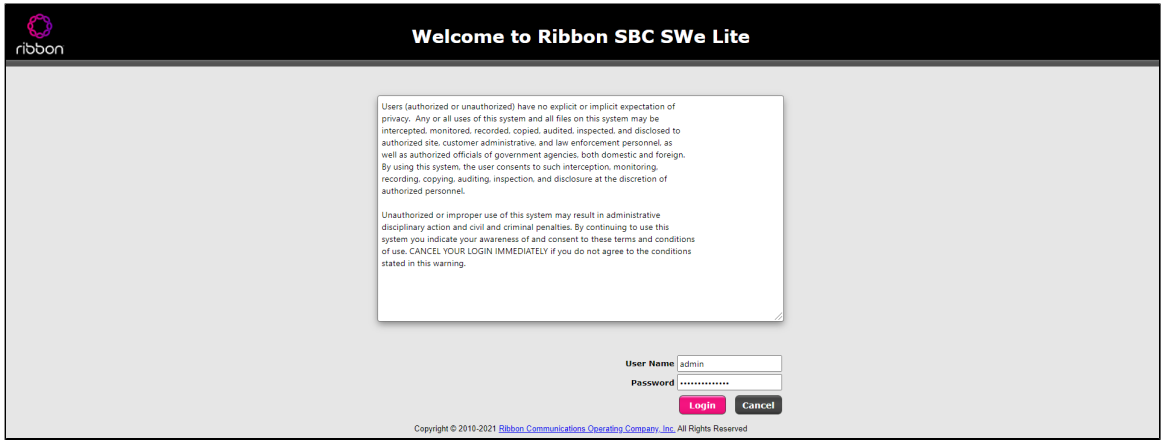
Ribbon SBC SWe Edge Configuration

Accessing SBC SWe Edge

Open any browser and enter the SBC SWe Edge IP address.



Click Enter and log in with a valid User ID and Password.

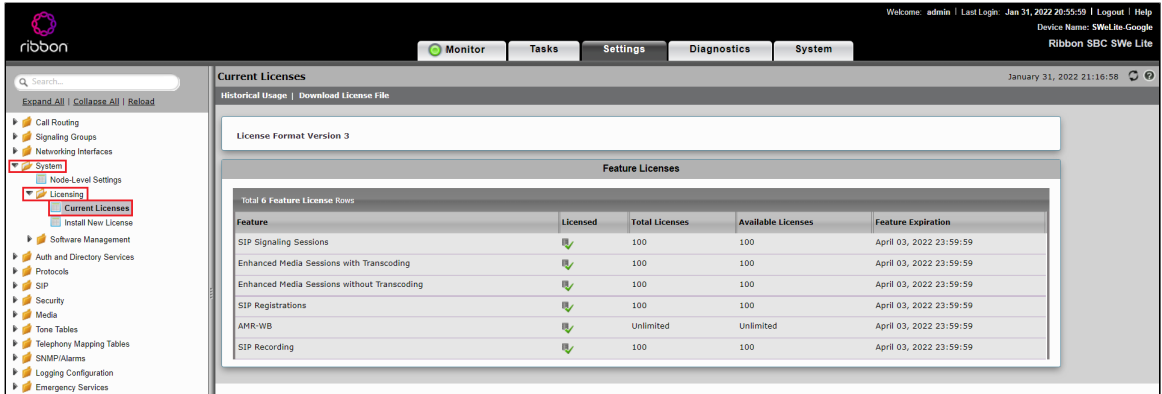


License and TLS Certificates

View License

This section describes how to view the status of each license along with a copy of the license keys installed on your SBC. The **Feature Licenses** panel enables you to verify whether a feature is licensed, along with the number of remaining licenses available for a given feature at run-time.

From the **Settings** tab, navigate to **System > Licensing > Current Licenses**.



For more details on Licenses, refer to [Working with Licenses](#).

SBC Certificate

From the **Settings** tab, navigate to **Security > SBC Certificates > Generate SBC Edge Certificates**.

1. Provide the Common Name of the SBC that includes Host and Domain.
2. Set the Key Length to 2048 bits.
3. Provide the location information.
4. Click OK.
5. The CSR will be generated and displayed in the result text box.

Generate Certificate Signing Request

Subject Distinguished Name

Common Name * Hostname or FQDN

Subject Alternative Name DNS comma-separated FQDN list

Email Address

ISO Country Code

State/Province

Locality e.g.: City

Organization e.g.: Company

Organizational Unit e.g.: Department

Key Length

OK

After generating the CSR on Ribbon SBC, provide it to the Certificate Authority. CA would generally provide the following certificates:

- SBC Certificate
- CA's Root Certificate
- Intermediate Certificate

SBC Certificates Index

- Generate SBC Edge CSR
- SBC Primary Certificate
- SBC Supplementary Certificates
- Trusted CA Certificates

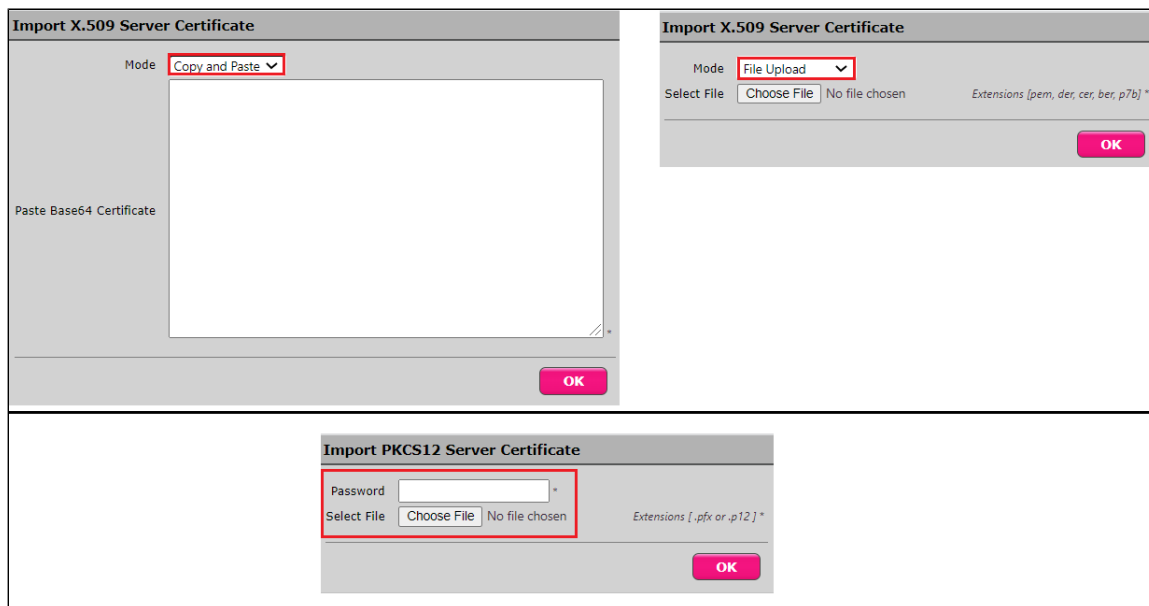
There are two ways to import SBC Primary Certificate as described below:

To import an X.509 signed certificate:

1. Select X.509 Signed Certificate from the Import menu at the top of the page.
2. Chose the import mode (Copy and Paste or File Upload) from the Mode pull-down menu.
3. If you chose File Upload, use the Browse button to find the file and click OK.
4. If you choose Copy and Paste, open the file in a text editor, paste the contents into the Paste Base64 Certificate text field and click OK.

To import a PKCS12 Certificate and Key:

1. Select PKCS12 Certificate and Key from the Import menu at the top of the page.
2. Enter the password used to export the certificate in the Password field.
3. Browse for the PKCS certificate and key file and click OK.



Trusted CA Certificates

A Trusted CA Certificate is a certificate issued by a Trusted Certificate Authority. Trusted CA Certificates are imported to the SBC SWe Edge to establish its authenticity on the network.

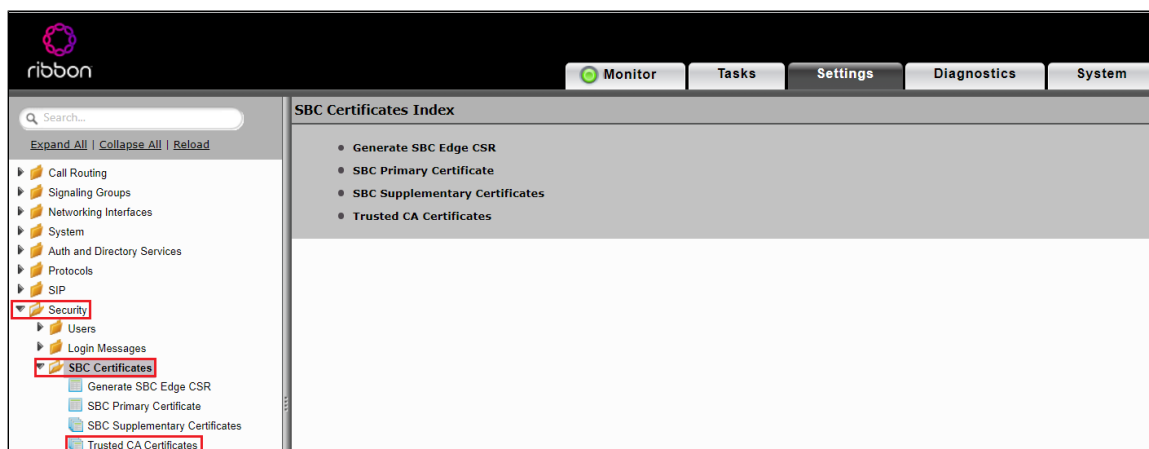
- For TLS to work, a Trusted CA (Certificate Authority) is required. For this interop, GoDaddy is used as Trusted CA.
- Add an entry in the Public DNS to resolve Ribbon SBC SWe Edge FQDN to Public IP Address.
- Ensure to have the following certificates as part of the root certificate trust:
 - GTS Root R1
 - GlobalSign Root CA (if required)




Note

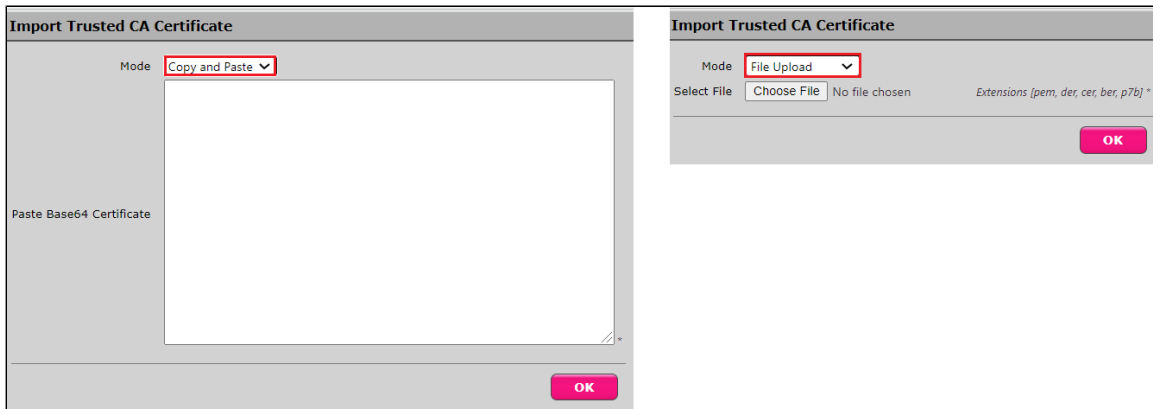
Refer to Google Voice SIP Link documentation for other compatible CAs.

From the **Settings** tab, navigate to **Security > SBC Certificates > Trusted CA Certificates**.



This section describes the process of importing Trusted Root CA Certificates using either the File Upload or Copy and Paste method.

1. To import a Trusted CA Certificate, click the Import Trusted CA Certificate () icon.
2. Select either Copy and Paste or File Upload from the Mode menu.
3. If you choose File Upload, use the Select File button to find the file.
4. Click OK.



Follow the steps above to import GTS Root R1 and GlobalSign Root CA certificates from Google Voice.



Note

When the **Verify Status** field in the Certificate panel indicates Expired or Expiring Soon, replace the Trusted CA Certificate. You must delete the old certificate before importing a new certificate successfully.



Warning

Most Certificate Vendors sign the SBC Edge certificate with an intermediate certificate authority. There is at least one, but there could be several intermediate CAs in the certificate chain. When importing the Trusted Root CA Certificates, import the root CA certificate and all Intermediate CA certificates. Failure to import all certificates in the chain causes the import of the SBC Edge certificate to fail. Please refer to [Unable To Get Local Issuer Certificate](#) for more information.

Networking Interfaces

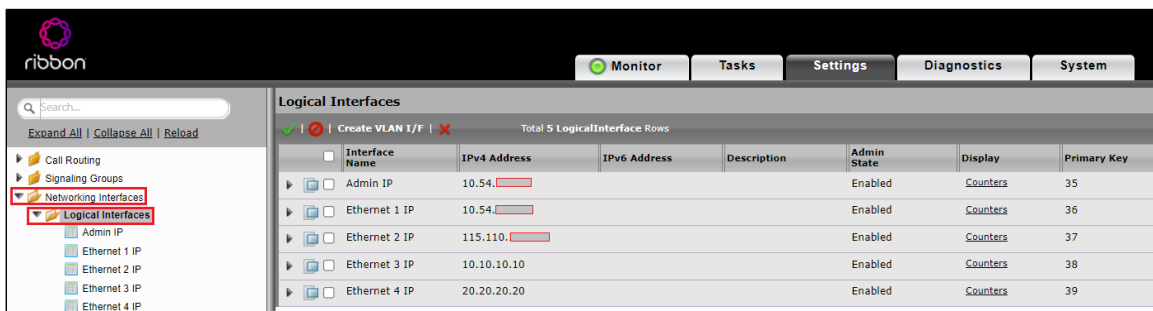
The SBC SWe Edge supports five system created logical interfaces known as Administrative IP, Ethernet 1 IP, Ethernet 2 IP, Ethernet 3 IP, and Ethernet 4 IP. In addition to the system created logical interfaces, the Ribbon SBC SWe Edge supports user created VLAN logical sub-interfaces.

Administrative IP, Ethernet 1 IP and Ethernet 2 IP are used for this interop.

From the **Settings** tab, navigate to **Networking Interfaces > Logical Interfaces**.

Administrative IP

The SBC SWe Edge system supports a logical interface called the Admin IP (Administrative IP, also known as the Management IP). A Static IP or DHCP is used for running Initial Setup of the SBC SWe Edge system.



Ethernet 1 IP

Ethernet 1 IP is assigned an IP address used for transporting all the VOIP media packets (for example, RTP, SRTP) and all protocol packets (for example, SIP, RTCP, TLS). DNS servers of the customer's network should map the SBC SWe Edge system hostname to this IP address. In the default software, **Ethernet 1 IP** is enabled and an IPv4 address is acquired via a connected DHCP server. This IP address is used for performing Initial Setup on the SBC SWe Edge.

Logical Interfaces

Interface Name	IPv4 Address	IPv6 Address	Description	Admin State	Display	Primary Key
Admin IP	10.54.1			Enabled	Counters	35
Ethernet 1 IP	10.54.1			Enabled	Counters	36

Identification/Status

Interface Name: Ethernet 1 IP
 I/F Index: 8
 Alias:
 Description:
 Admin State: Enabled

Networking

MAC Address:
 IP Addressing Mode: IPv4

IPv4 Information

IP Assign Method: Static
 Primary Address: 10.54.1
 Primary Netmask: 255.255.255.0
 Media Next Hop IP: 10.54.1

Ethernet 2 IP

After initial configuration, you may configure this logical interface using the Settings or Tasks tabs in the WebUI or you can use the IP address configured during Initial Setup.

Logical Interfaces

Interface Name	IPv4 Address	IPv6 Address	Description	Admin State	Display	Primary Key
Admin IP	10.54.1			Enabled	Counters	35
Ethernet 1 IP	10.54.1			Enabled	Counters	36
Ethernet 2 IP	115.110.1			Enabled	Counters	37

Identification/Status

Interface Name: Ethernet 2 IP
 I/F Index: 9
 Alias:
 Description:
 Admin State: Enabled

Networking

MAC Address:
 IP Addressing Mode: IPv4

IPv4 Information

IP Assign Method: Static
 Primary Address: 115.110.1
 Primary Netmask: 255.255.255.192
 Media Next Hop IP: 115.110.1

Configure Static Routes

Static routes are used to create communication to remote networks. In a production environment, static routes are mainly configured for routing from a specific network to another network that you can only access through one point or one interface (single path access or default route).

Derive the Private IP address and Gateway for each interface on AWS.

Destination IP

Specifies the destination IP address.

Mask

Specifies the network mask of the destination host or subnet. If the 'Destination IP Address' field and 'Mask' field are both 0.0.0.0, the static route is called the 'default static route'.

Gateway

Specifies the IP address of the next-hop router to use for this static route.

Metric

Specifies the cost of this route and therefore indirectly specifies the preference of the route. Lower values indicate more preferred routes. The typical value is 1 for most static routes, indicating that static routes are preferred to dynamic routes.

From the **Settings** tab, navigate to **Protocols > IP > Static Routes**. Click the **+** icon to add the entries.

The screenshot shows the 'Static IP Route Table' in the Ribbon SBC SWe Edge interface. The table has the following columns: Row ID, Destination IP, Mask, Gateway, Administrative Distance, and Primary Key. There are 5 rows of data.

Row ID	Destination IP	Mask	Gateway	Administrative Distance	Primary Key
1	172.16.0.0	255.255.255.0	10.54.0.0	1	1
2	74.125.0.0	255.255.255.0	115.110.0.0	1	2
3	216.239.0.0	255.255.255.255	115.110.0.0	1	3
4	8.8.8.8	255.255.255.255	115.110.0.0	1	4
5	10.70.0.0	255.255.0.0	10.54.0.0	1	5

Global Configuration

Media Profiles

Media Profiles allow you to specify the individual voice and fax compression codecs and their associated settings, for inclusion in a Media List. Different codecs provide varying levels of compression, allowing one to reduce bandwidth requirements at the expense of voice quality.

From the **Settings** tab, navigate to **Media > Media Profiles**. From the **Create Media Profile** drop-down, select **Voice Codec Profile**.

The screenshot shows the 'Media Profiles' configuration page in the Ribbon SBC SWe Edge interface. The 'Create Media Profile' dropdown menu is open, showing 'Voice Codec Profile' and 'Fax Codec Profile'. The table below shows two media profiles:

Create Media Profile	Description	Primary Key
Voice Codec Profile	Default G711A	1
Fax Codec Profile	Default G711u	2

The codecs G711A and G711U are configured on the SBC SWe Edge by default. Configure OPUS and G722 by following the steps provided below:



Note

OPUS is supported on the Ribbon SBC SWe Edge but not on the SBC 1K. During the 1K configuration, ignore the step below that describes the procedure to configure OPUS codec.

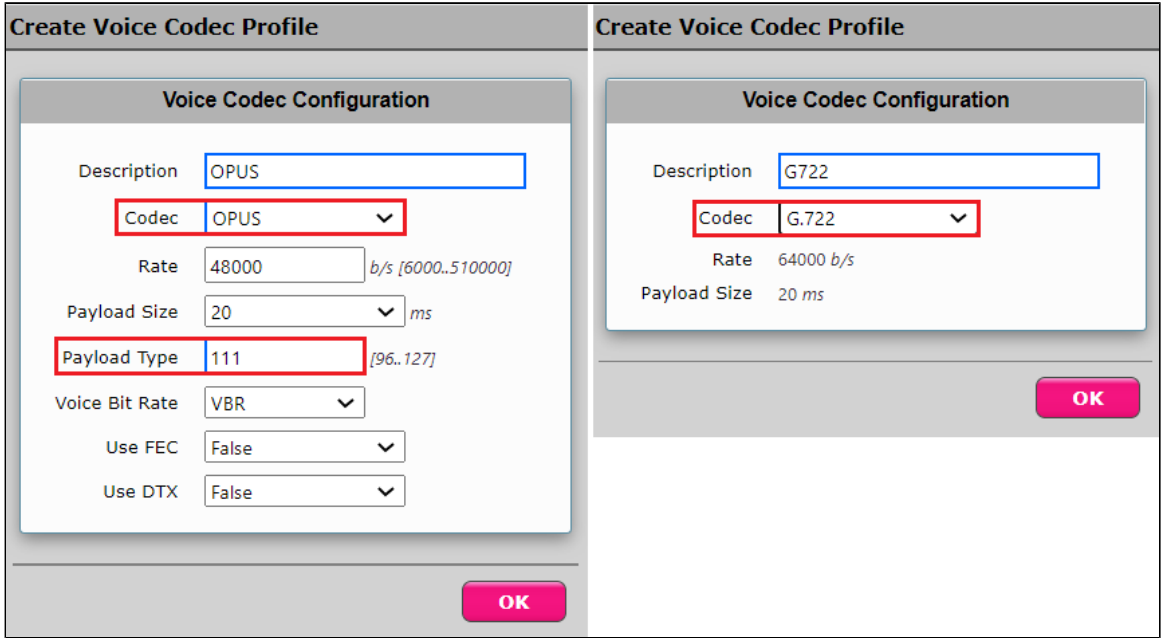
For OPUS:

1. Provide the profile's description.
2. Select OPUS from the Codec drop-down menu.
3. Configure 111 as the Payload Type.

4. Click OK.

For G722:

1. Provide the profile's description.
2. Select G.722 from the Codec drop-down menu.
3. Click OK.

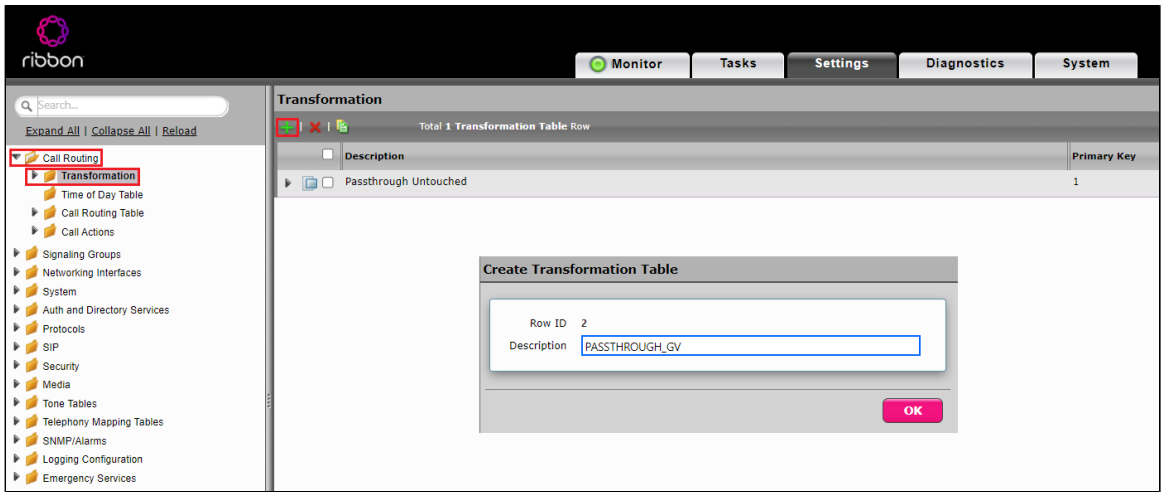


Transformation Table

Transformation Tables facilitate the conversion of names, numbers and other fields when routing a call. They can, for example, convert a public PSTN number into a private extension number, or into a SIP address (URI). Every entry in a Call Routing Table requires a Transformation Table. In addition, Transformation tables are configurable as a reusable pool that Action Sets can reference.

From the Settings tab, navigate to **Call Routing > Transformation**. Click the **+** icon to create a Transformation Table.

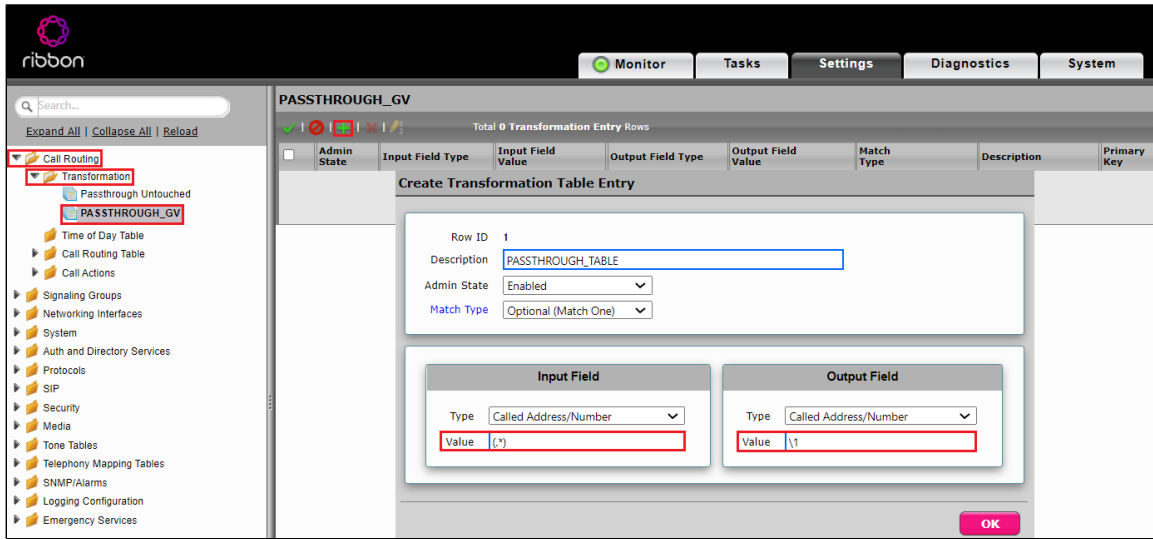
1. Provide a name for the Transformation Table in the Description field.
2. Click OK.



Transformation Table Entry

1. Click on the Transformation Table created in the previous step.

2. Click the **+** icon to create an entry.
3. Provide the values in Input and Output fields.
4. Click OK.



SBC SWe Edge Configuration for PSTN side

Media List - PSTN

From the Settings tab, navigate to **Media > Media List**. Click the **+** icon at the top of the Media List View page.

1. Provide a name for the profile.
2. Attach the Media Profiles by clicking Add/Edit.
3. Enable Dead Call Detection.
4. From the DTMF drop-down menu, select RFC2833.
5. Click OK.

Message Manipulation - PSTN

The Message Manipulation feature comprises two primary components that work in concert to modify SIP messages. Those components are Condition Rules and Rule Tables. SIP Message rules per table include all SIP rule types: Header, Request, Status and Raw.

The Message Manipulation PSTN_RULE is used for the following purposes:

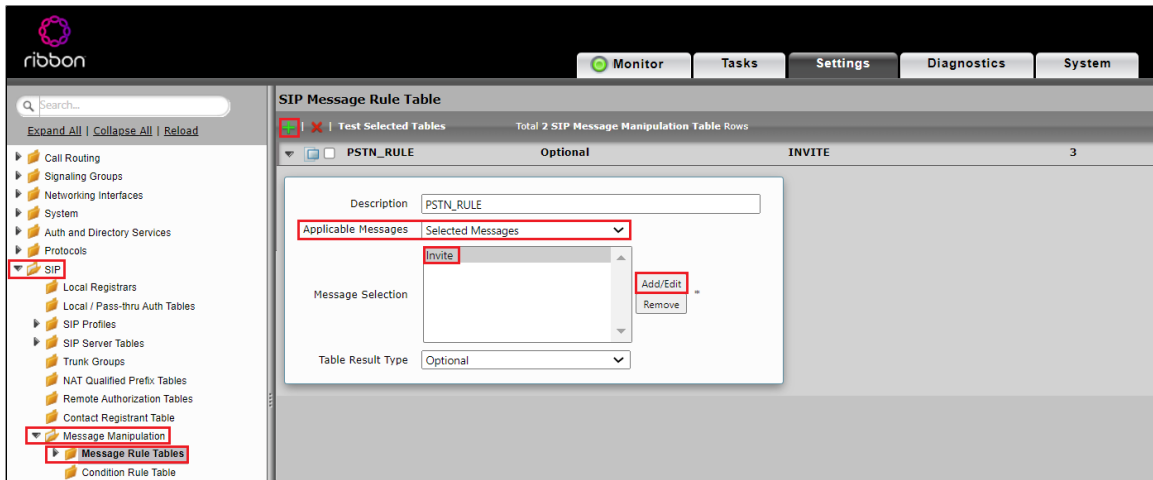
- To replace a=inactive with a=sendonly, as inactive is not supported on Google Voice
- To remove P-Preferred-Identity header to facilitate SWe Edge to send P-Asserted-Identity header to Google Voice instead of relaying P-Preferred-Identity received from PSTN

Message Rule Table

Message Rule can be added to: all messages, all requests, all responses or selected messages.

From the **Settings** tab, navigate to **SIP > Message Manipulation > Message Rule Table**. Click the **+** icon to create a Message Rule Table.

1. Provide a description for the Rule Table.
2. Apply Message Rule to the Selected messages and choose Invite from the Message Selection list.
3. Click OK.

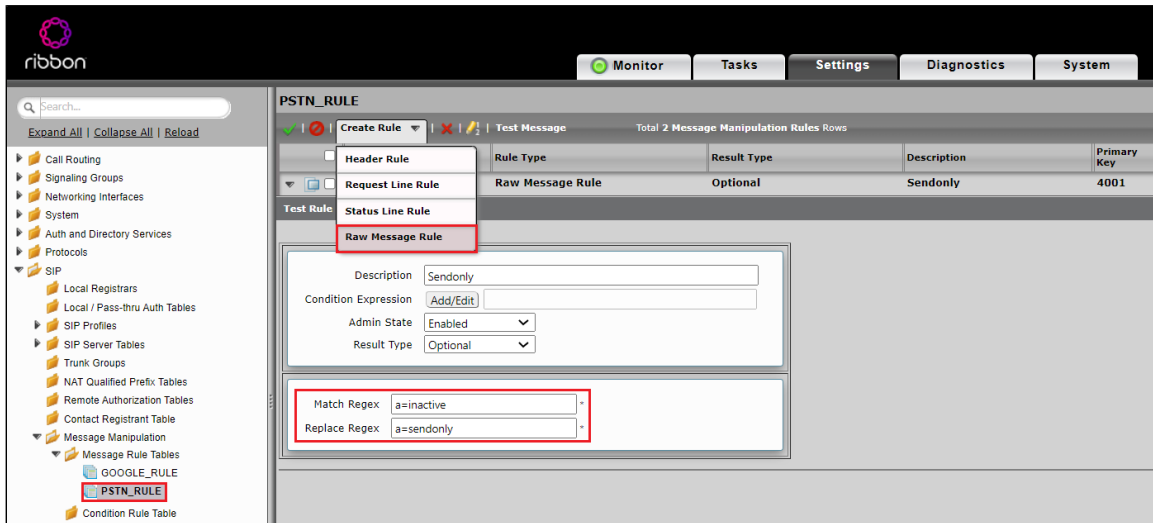


Message Rule Table Entry

Raw Message Rule:

Raw rules allow you to manipulate any string in the entire message: request, headers and payload. If the condition rule evaluates true, the MME will search the message for content matching the "Match Regex" and replace it with the content specified in the "Replace Regex".

1. Click on the Message Rule Table PSTN_RULE.
2. From the Create Rule drop-down menu, select Raw Message Rule.
3. Provide a name for the entry.
4. Replace a=inactive with a=sendonly using regex.



Header Rule:

1. Click on the Message Rule Table PSTN_RULE.
2. From the Create Rule drop-down menu, select Header Rule.
3. Provide a name for the entry.
4. Remove P-Preferred-Identity header using the Action "Remove".

The screenshot shows the Ribbon Communications Settings interface. The left navigation pane is expanded to 'SIP' > 'Message Manipulation' > 'PSTN_RULE'. The main area displays a table of Message Manipulation Rules:

Rule Type	Result Type	Description	Primary Key
Raw Message Rule	Optional	Sendonly	4001
Header Rule	Optional	REMOVE PPI	1

The 'Test Rule' dropdown is set to 'Raw Message Rule'. A configuration dialog is open for the 'Status Line Rule' (Header Rule), showing the following fields:

- Description: REMOVE PPI
- Condition Expression: Add/Edit
- Admin State: Enabled
- Result Type: Optional
- Header Action: Remove
- Header Name: P-Preferred-Identity
- Header Ordinal Number: 1st

SIP Profile - PSTN

SIP Profiles control how SBC Edge communicates with SIP devices. They control important characteristics such as Session Timers, SIP Header Customization, SIP Timers, MIME Payloads and Option Tags.

From the **Settings** tab, navigate to **SIP > SIP Profiles**. Click the **+** icon to create a new SIP Profile.

1. Provide a name for the profile in the Description field.
2. Enable Session Timer. This field specifies whether or not to use Session Timer to verify the SIP session. The remainder of the options in this panel are visible only after enabling Session Timer.
3. Set Minimum Acceptable Timer to 90 and Offered Session Timer to 1800.
4. In the Options Tags panel, set the Timer field to Required and the Update field to Supported.
5. Click OK.

SIP Profile Table

Total 3 SIP Profile Rows

Description	Primary Key
Default SIP Profile	1
GOOGLE_SIP_PROFILE	2
PSTN_SIP_PROFILE	3

Description: PSTN_SIP_PROFILE

Session Timer

Session Timer: Enable (dropdown)

Minimum Acceptable Timer: 90 (input) * secs [90..7200]

Offered Session Timer: 1800 (input) * secs [90..7200]

Terminate On Refresh Failure: False (dropdown)

MIME Payloads

ELIN Identifier: LOC (dropdown)

PIDF-LO Passthrough: Enable (dropdown)

Unknown Subtype Passthrough: Disable (dropdown)

Header Customization

FQDN in From Header: Disable (dropdown)

FQDN in Contact Header: Disable (dropdown)

Send Assert Header: Trusted Only (dropdown)

SBC Edge Diagnostics Header: Enable (dropdown)

Trusted Interface: Enable (dropdown)

UA Header: Ribbon SBC Edge (input)

Calling Info Source: RFC Standard (dropdown)

Diversion Header Selection: Last (dropdown)

Record Route Header: RFC 3261 Standard (dropdown)

Options Tags

100rel: Supported (dropdown)

Path: Not Present (dropdown)

Timer: Required (dropdown)

Update: Supported (dropdown)

Timers

Transport Timeout Timer: 5000 (input) ms [5000..32000]

Maximum Retransmissions: RFC Standard (dropdown)

Redundancy Retry Timer: 180000 (input) ms [5000..1800000]

RFC Timers

Timer T1: 500 (input) ms [100..10000]

Timer T2: 4000 (input) ms [1000..80000] (>= T1)

Timer T4: 5000 (input) ms [1000..100000]

Timer D: 32000 (input) ms [5000..640000]

Timer B: 32000 ms

Timer F: 32000 ms

Timer H: 32000 ms (64*TimerT1)

Timer J: 4000 (input) ms [4000..640000]

SDP Customization

Send Number of Audio Channels: False (dropdown)

Connection Info in Media Section: True (dropdown)

Origin Field Username: SBC (input) default: SBC

Session Name: VoipCall (input) default: VoipCall

Digit Transmission Preference: RFC 2833/Voice (dropdown)

SDP Handling Preference: Legacy Audio/Fax (dropdown)

SIP Server Table - PSTN

SIP Server Tables contain information about the SIP devices connected to the SBC Edge. The entries in the tables provide information about the IP Addresses, ports and protocols used to communicate with each server. The Table Entries also contain links to counters that are useful for troubleshooting. The SIP Server supports either an FQDN or IP Address (V4 or V6).

From the **Settings** tab, navigate to **SIP > SIP Server Tables**. Click the **+** icon to create a new SIP Server Table.

1. Provide a name for the SIP Server.
2. From the Type drop-down menu, choose SIP Server.
3. Click OK.

SIP Server Tables

Total 3 SIP Server Table Rows

Description	Primary Key
Default SIP Server	1
PSTN	2

Description: PSTN

Type: SIP Server (dropdown)

SIP Server Table Entry

1. Click on the SIP Server Table created in the previous step.
2. From the Create SIP Server drop-down menu, select IP/FQDN.
3. Provide IP Address and Port Number of the PSTN endpoint.
4. Enable OPTION pings by selecting SIP Options from the Monitor field.
5. Click OK.

The screenshot shows the 'Create SIP Server Entry' form with the following fields:

- Server Host:** Row ID: 1, Server Lookup: IP/FQDN, Priority: 1, Host FQDN/IP: 10.54, Port: 5060, Protocol: UDP.
- Transport:** Monitor: SIP Options, Keep Alive Frequency: 30, Recover Frequency: 5, Local Username: PSTN, Peer Username: PSTN.
- Remote Authorization and Contacts:** Remote Authorization Table: None, Contact Registrant Table: None, Session URI Validation: Liberal.

Call Routing Table - PSTN

Call Routing allows calls to be carried between Signaling Groups, thus allowing calls to be carried between ports and between protocols (like ISDN to SIP). Routes are defined by Call Routing Tables, which allow flexible configuration of how calls are to be carried and how they are translated. These tables are the central connection points of the system, linking [Transformation Tables](#), [Message Translations](#), [Cause Code Reroute Tables](#), [Media Lists](#) and the Signaling Groups.

From the **Settings** tab, navigate to **Call Routing > Call Routing Table**. Click the **+** icon to create a Call Routing Table.

1. Provide a name for the Routing Table.
2. Click OK.

The screenshot shows the 'Call Routing Tables' configuration interface. The table lists the following rows:

Description	Primary Key
Default Route Table	1
PSTN_TO_GV	2

The form below the table shows the 'Description' field set to 'PSTN_TO_GV'.

SIP Signaling Group - PSTN

Signaling groups allow telephony channels to be grouped together for the purposes of routing and shared configuration. They are the entity to which calls are routed, as well as the location from which [Call Routes](#) are selected. They are also the location from which [Tone Tables](#) and [Action Sets](#) are selected.

From the **Settings** tab, navigate to **Signaling Groups**. Click **Add SIP SG**.

1. Attach the Call Routing Table ([PSTN_TO_GV](#)).

2. Attach the SIP Profile ([PSTN_SIP_PROFILE](#)).
3. Attach the SIP Server Table ([PSTN](#)).
4. Attach the Media List ID ([PSTN](#)).
5. Associate the appropriate IP address in the "Signaling/Media Source IP" field.
 - a. This specifies the Logical IP address at which SIP messages are received.
 - b. This address is used as the source IP for all SIP messages leaving the SBC SWe Edge or SBC 1000/2000 through this Signaling Group
6. Configure Protocol and Listen Ports in the "Listen Ports" panel.
7. Create an entry in the Federated IP/FQDN panel.
 - a. Federated IP addresses and FQDNs specified in a SIP Signaling Group are whitelisted.
 - b. The Federated IP/FQDN feature acts as an access control by defining from which server a SIP Signaling Group will accept messages.
8. Enable Message Manipulation and attach the profile [PSTN_RULE](#) to Inbound Message Manipulation Table List.
 - a. This option allows the SBC to manipulate SIP messages using previously configured Message Tables.
9. Click OK.

The screenshot displays the 'Signaling Group Table' configuration for 'PSTN_SG'. The configuration is organized into several sections:

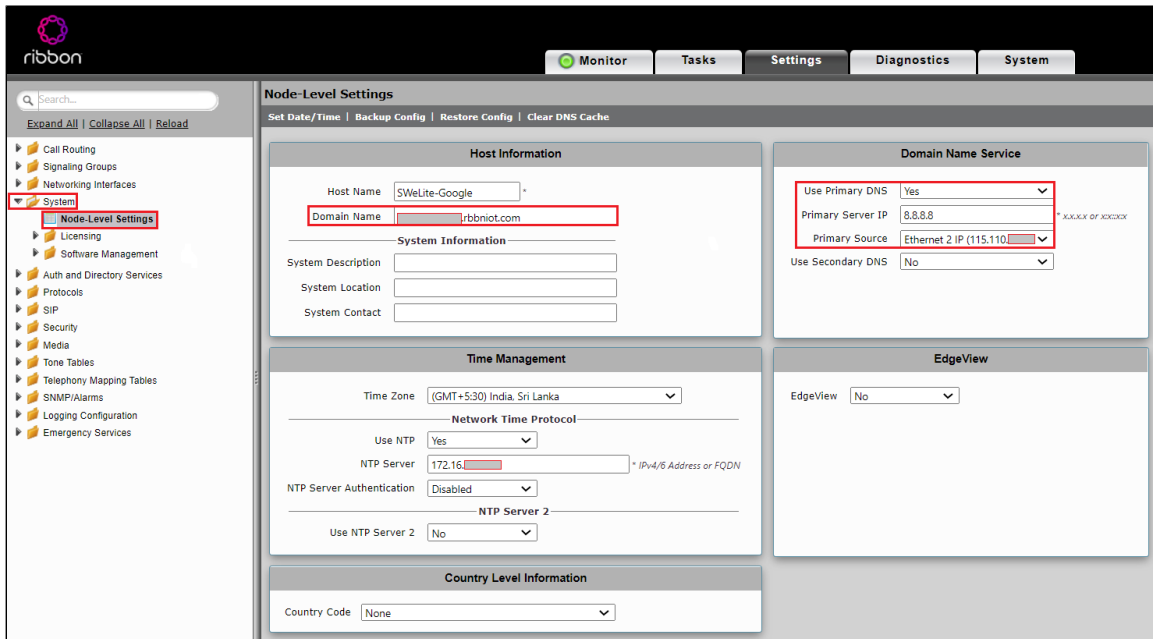
- SIP Channels and Routing:** Includes settings for Action Set Table (None), Call Routing Table (PSTN_TO_GV), No. of Channels (60), SIP Profile (PSTN_SIP_PROFILE), SIP Mode (Basic Call), Agent Type (Back-to-Back User Agent), SIP Server Table (PSTN), Load Balancing (Round Robin), Channel Hunting (Most Idle), Notify Lync CAC Profile (Disable), Challenge Request (Disable), Outbound Proxy IP/FQDN, Outbound Proxy Port (5060), Call Setup Response Timer (255), Call Proceeding Timer (180), Use Register as Keep Alive (Enable), and Forked Call Answered Too Soon (Disable).
- Media Information:** Includes Supported Audio Modes (DSP, Proxy, Direct, Proxy with Local SRTP), Supported Video/Application Modes (Proxy, Direct), Media List ID (PSTN), Proxy Local SRTP (None), Crypto Profile ID, Play Ringback (Auto on 180), Tone Table (Default Tone Table), Play Congestion Tone (Disable), Early 183 (Disable), Allow Refresh SDP (Enable), Music on Hold (Disabled), and RTCP Multiplexing (Disable).
- Mapping Tables:** Includes SIP To Q.850 Override Table (Default (RFC4497)), Q.850 To SIP Override Table (Default (RFC4497)), and Pass-thru Peer SIP Response Code (Enable).
- SIP IP Details:** Includes Teams Local Media Optimization (Disable), Signaling/Media Source IP (Ethernet 1 IP (10.54)), Signaling DSCP (40), NAT Traversal (ICE Support: Disabled, Static NAT - Outbound: Outbound NAT Traversal: None, Static NAT - Inbound: Detection: Disabled).
- Listen Ports:** Shows a single port configuration for 5060 UDP.
- Federated IP/FQDN:** Shows a single IP/FQDN configuration for 10.54 with Netmask/Prefix 255.255.255.255.
- Message Manipulation:** Includes Message Manipulation (Enabled), Inbound Message Manipulation (PSTN_RULE), and Outbound Message Manipulation.

SBC SWe Edge Configuration for Google Voice SIP Link side

DNS

From the **Settings** tab, navigate to **System > Node-Level Settings**.

1. From the Use Primary DNS drop-down menu, select Yes.
2. Provide the Primary DNS IP address.
3. Select the Ethernet facing Google Voice SIP Link from the Primary Source drop-down menu.
4. Click Apply.

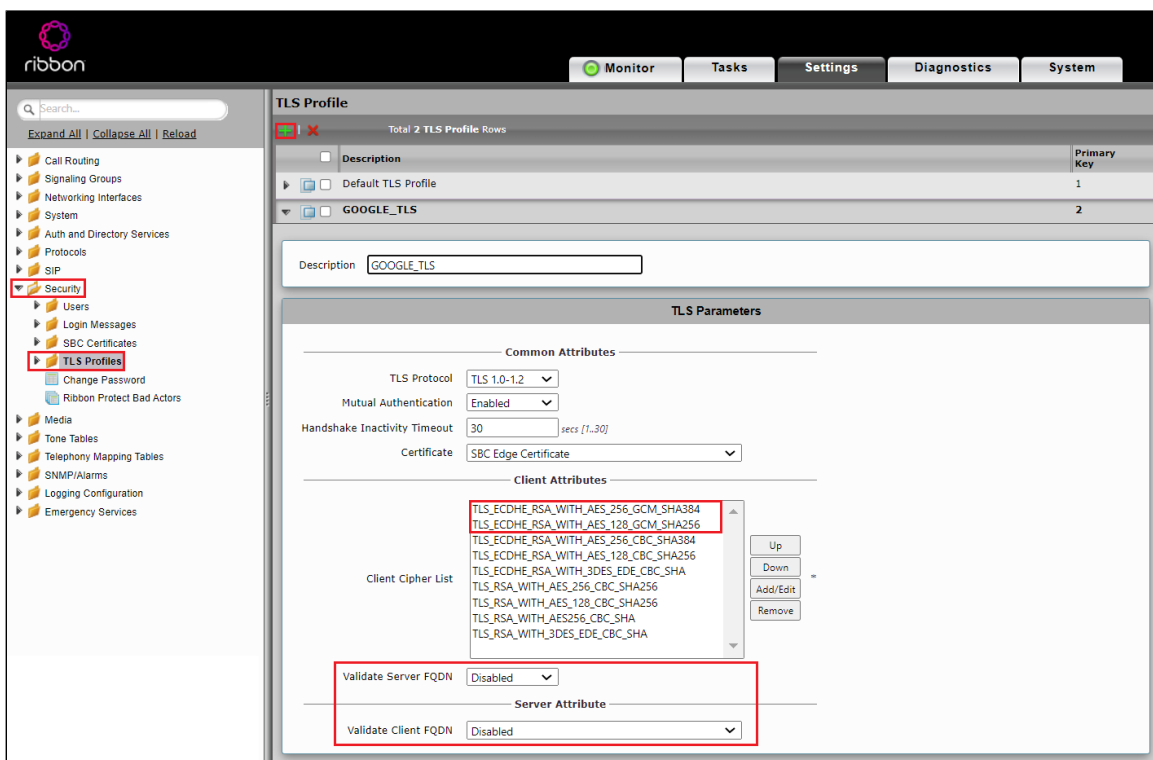


TLS Profile

TLS Profiles are used by SIP Signaling Groups when the TLS transport type is selected for incoming and outgoing SIP trunks (Listen Ports), and in SIP Server Tables when TLS is selected as the Server Host protocol.

From the **Settings** tab, navigate to **Security > TLS Profiles**. Click the **+** icon to create a new TLS profile.

1. From TLS Protocol drop-down menu, select TLS 1.0-1.2.
2. Add the cipher suites that are supported on Google Voice SIP Link (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256).
3. Disable the Validate Server and Client FQDN fields.
4. Click OK.

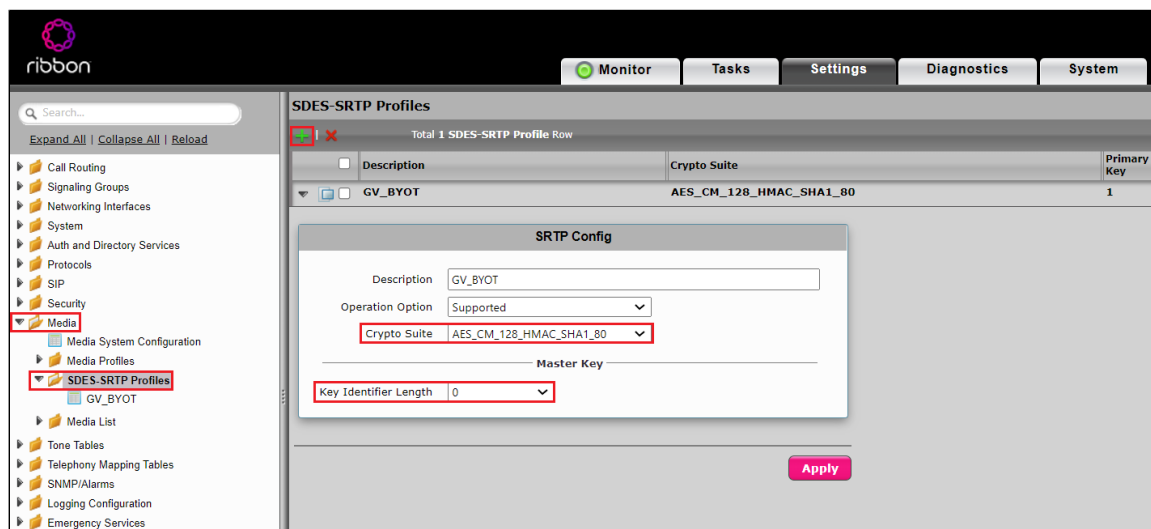


SDES-SRTP Profile

SDES-SRTP Profiles define a cryptographic context which is used in SRTP negotiation. SDES-SRTP Profiles are required for enabling media encryption and are applied to Media Lists.

From the **Settings** tab, navigate to **Media > SDES-SRTP Profiles**. Click the **+** icon to create a new SDES-SRTP profile.

1. Provide a name for the profile in the Description field.
2. Attach the Crypto suite "AES_CM_128_HMAC_SHA1_80", a crypto suite algorithm which uses the 128 bit AES-CM encryption key and a 80 bit HMAC_SHA1 message authentication tag length.
3. Set the Key Identifier Length to 0 to disable the MKI in SDP.
4. Click OK.



Note

Google Voice does not support MKI, hence the Key Identifier Length must be set to 0 on the Ribbon SBC SWe Edge.

Media List - GV

From the Settings tab, navigate to **Media > Media List**. Click the **+** icon at the top of the Media List View page

1. Provide a name for the profile.
2. Attach the Media Profiles by clicking Add/Edit.
3. Attach the SDES-SRTP profile ([GV_BYOT](#)).
4. Enable Dead Call Detection.
5. From the DTMF drop-down menu, select RFC2833.
6. Click OK.

Message Manipulation - GV

The Message Manipulation GOOGLE_RULE is used for the following purposes:

- To add the header “X-Google-Pbx-Trunk-Secret-Key” for Google Voice. The value of this header is generated when the SIP Trunk is created.
- To change the request URI of specific request messages to Google specified FQDN, trunk.sip.voice.google.com.
- To modify the FQDN in the To header to trunk.sip.voice.google.com.

Message Rule Table

From the **Settings** tab, navigate to **SIP > Message Manipulation > Message Rule Table**. Click the **+** icon to create a Message Rule Table.

1. Provide a description for the Rule Table.
2. Apply Message Rule to the selected messages and choose Invite, Cancel, Options and ACK from the Message Selection list.
3. Click OK.

Message Rule Table Entry

Header Rule:

1. Click on the Message Rule Table GOOGLE_RULE.
2. From the Create Rule drop-down menu, select **Header Rule**.
3. Provide a name for the entry.
4. Add the header "X-Google-Pbx-Trunk-Secret-Key".
5. To add the value, select **Add** from the Header Value drop-down menu and provide the literal value of the header.
6. Click **OK**.

The screenshot shows the Ribbon Communications web interface. On the left is a navigation tree with categories like Call Routing, Signaling Groups, and SIP. Under SIP, 'Message Manipulation' is expanded, and 'GOOGLE_RULE' is selected. The main area displays the configuration for 'GOOGLE_RULE' as a 'Header Rule'. A 'Create Rule' dropdown menu is open, showing 'Header Rule' selected. Below, the 'Header Action' is set to 'Add' and the 'Header Name' is 'X-Google-Pbx-Trunk-Secret-Key'. The 'Header Value' is set to 'Add' and the value is '43871d45-d275-4e90-b800-cd'. An 'Edit Message Field' dialog box is open, showing 'Type of Value' set to 'Literal' and 'Value' set to '43871d45-d275-4e90-b800-cd'. Buttons for 'OK' and 'Cancel' are visible at the bottom of the dialog.

Request Line Rule:

1. Click on the Message Rule Table GOOGLE_RULE.
2. From the Create Rule drop-down menu, select Request Line Rule.
3. Provide a name for the entry.
4. Replace the FQDN "siplink.telephony.goog" with "trunk.sip.voice.google.com" using regex.
5. Click OK.

The screenshot shows the Ribbon Communications interface. On the left is a navigation tree with categories like Call Routing, Signaling Groups, and SIP. The 'GOOGLE_RULE' is selected under Message Manipulation Tables. The main area displays a table of Message Manipulation Rules:

Rule Type	Result Type	Description	Primary Key
Header Rule	Optional	Google_header	1
Request Line Rule	Optional	Request_uri_FQDN	2001

The 'Request Line Rule' is selected, and the configuration fields are visible:

- Description: Request_uri_FQDN
- Condition Expression: Add/Edit
- Admin State: Enabled
- Result Type: Optional
- Request Line Value: Modify (dropdown), Add/Edit (button), Match: siplink.telephony.goog, Replace: trunk.sip.voice.google.com

The 'Edit Message Field' dialog is open, showing:

- Type of Value: Regex
- Match Regex: siplink.telephony.goog
- Replace Regex: trunk.sip.voice.google.com

Header Rule:

1. Click on the Message Rule Table GOOGLE_RULE.
2. From the Create Rule drop-down menu, select Header Rule.
3. Provide a name for the entry.
4. Select Header Action as Modify and choose To from the Header Name list.
5. Replace the FQDN "siplink.telephony.goog" with "trunk.sip.voice.google.com" using regex.
6. Click OK.

The screenshot shows the Ribbon Communications interface. On the left is a navigation tree with categories like Call Routing, Signaling Groups, and SIP. The 'GOOGLE_RULE' is selected under Message Manipulation Tables. The main area displays a table of Message Manipulation Rules:

Rule Type	Result Type	Description	Primary Key
Header Rule	Optional	Google_header	1
Request Line Rule	Optional	Request_uri_FQDN	2001
Header Rule	Optional	FQDN for To	2

The 'Header Rule' is selected, and the configuration fields are visible:

- Description: FQDN for To
- Condition Expression: Add/Edit
- Admin State: Enabled
- Result Type: Optional
- Header Action: Modify
- Header Name: To
- Header Value: Modify (dropdown), Add/Edit (button), Match: siplink.telephony.goog, Replace: trunk.sip.voice.google.com

The 'Edit Message Field' dialog is open, showing:

- Type of Value: Regex
- Match Regex: siplink.telephony.goog
- Replace Regex: trunk.sip.voice.google.com

SIP Profile - GV

From the **Settings** tab, navigate to **SIP > SIP Profiles**. Click the **+** icon to create a new SIP Profile.

1. Provide a name for the profile in the Description field.
2. Enable Session Timer.
3. Set the Minimum Acceptable Timer to 90 and the Offered Session Timer to 1800.
4. In the Options Tags panel, set the Timer field to Required and the Update field to Supported.
5. Click OK.

The screenshot shows the 'SIP Profile Table' with 3 rows. The selected profile is 'GOOGLE_SIP_PROFILE'. The configuration details are as follows:

Section	Field	Value	
Session Timer	Session Timer	Enable	
	Minimum Acceptable Timer	90 *secs [90..7200]	
	Offered Session Timer	1800 *secs [90..7200]	
	Terminate On Refresh Failure	False	
MIME Payloads	ELIN Identifier	LOC	
	PIDF-LO Passthrough	Enable	
	Unknown Subtype Passthrough	Disable	
Header Customization	FQDN in From Header	Disable	
	FQDN in Contact Header	Disable	
	Send Assert Header	Trusted Only	
	SBC Edge Diagnostics Header	Enable	
	Trusted Interface	Enable	
	UA Header	Ribbon SBC Edge	
	Calling Info Source	RFC Standard	
Options Tags	Timer	Required	
	Update	Supported	
Timers	Transport Timeout Timer	5000 ms [5000..32000]	
	Maximum Retransmissions	RFC Standard	
	Redundancy Retry Timer	180000 ms [5000..180000]	
RFC Timers	Timer T1	500 ms [100..10000]	
	Timer T2	4000 ms [1000..80000](>= T1)	
	Timer T4	5000 ms [1000..100000]	
	Timer D	32000 ms [5000..640000]	
	Timer B	32000 ms	
	Timer F	32000 ms	
	Timer H	32000 ms (64*TimerT1)	
	Timer J	4000 ms [4000..640000]	
	SDP Customization	Send Number of Audio Channels	False
		Connection Info in Media Section	True
Origin Field Username		SBC default: SBC	
Session Name		VoipCall default: VoipCall	
SDP Handling Preference		Legacy Audio/Fax	



Note

The session will always be refreshed by Ribbon SBC SWe Edge as per the Google Voice requirement.

SIP Server Table - GV

From the **Settings** tab, navigate to **SIP > SIP Server Tables**. Click the **+** icon to create a new SIP Server Table.

1. Provide a name for the SIP Server.
2. From the Type drop-down menu, choose SIP Server.
3. Click OK.

SIP Server Table Entry

1. Click on the SIP Server Table created in the previous step.
2. From the Create SIP Server drop-down menu, select IP/FQDN.
3. Provide the IP Address and the Port Number of the PSTN endpoint.
4. Enable OPTION pings by selecting SIP Options from the Monitor field.
5. Click OK.



Note

For production, the Google Voice (GV) hostname is siplink.telephony.goog.

Call Routing Table - GV

From the **Settings** tab, navigate to **Call Routing** > **Call Routing Table**. Click the **+** icon to create a Call Routing Table.

1. Provide a name for the Routing Table.
2. Click OK.

The screenshot shows the 'Call Routing Tables' configuration page in the Ribbon Communications interface. The left sidebar contains a navigation tree with 'Call Routing' expanded and 'Call Routing Table' selected. The main content area displays a table with 3 rows of Call Routing Table Rows. The table has columns for 'Description' and 'Primary Key'. The rows are: 'Default Route Table' (Primary Key 1), 'PSTN_TO_GV' (Primary Key 2), and 'GV_TO_PSTN' (Primary Key 3). Below the table, there is a search box with the text 'GV_TO_PSTN' entered.

SIP Signaling Group - GV

From the **Settings** tab, navigate to **Signaling Groups**. Click **Add SIP SG**.

1. Attach the Call Routing Table ([GV_TO_PSTN](#)).
2. Attach the SIP Profile ([GOOGLE_SIP_PROFILE](#)).
3. Attach the SIP Server Table ([GOOGLE](#)).
4. Attach the Media List ID ([GOOGLE](#)).
5. Select the SDES-SRTP Profile [GV_BYOT](#) in the Proxy Local SRTP Crypto Profile ID field.
6. Associate the appropriate IP address in the "Signaling/Media Source IP" field.
7. Configure the Protocol, TLS Listen Ports and TLS Profile ([GOOGLE_TLS](#)) in the "Listen Ports" panel.
8. Provide the Google Voice SIP Link's FQDN or IP address in the Federated IP/FQDN panel.
9. Enable Message Manipulation and attach the profile [GOOGLE_RULE](#) to the Outbound Message Manipulation Table List.
10. Click OK.



Note

Ignore step 5 if you are configuring SBC 1K.

Call Routing Table Entry

Call Routing entries must be created after creating SIP Signaling Groups as Destination SGs need to be attached to these entries.

PSTN to GV:

1. Click the **Create Routing Entry** (+) icon.
2. Attach the Transformation Table ([PASSTHROUGH_GV](#)).
3. Add the Destination Signaling Group which in this case is [GOOGLE_SG](#).

- In the Media panel, select DSP from the Audio Stream Mode and enable Media Transcoding.
- Click OK.

PSTN_TO_GV

Display Counters Total 1 Call Route Entry Row

Admin State	Priority	Transformation Table	Destination Type	First Signaling Group	Description	Fork Call	Primary Key
<input type="checkbox"/>	1	PASSTHROUGH_GV	Normal	(SIP) GOOGLE_SG	PSTN_TO_GV	No	1

Route Details

Description: PSTN_TO_GV

Admin State: Enabled

Route Priority: 1

Call Priority: Normal

Number/Name Transformation Table: PASSTHROUGH_GV

Time of Day Restriction: None

Destination Information

Destination Type: Normal

Message Translation Table: None

Cause Code Reroutes: None

Cancel Others upon Forwarding: Disabled

Fork Call: No

Destination Signaling Groups: (SIP) GOOGLE_SG

Enable Maximum Call Duration: Disabled

Media

Audio Stream Mode: DSP

Video/Application Stream Mode: Disabled

Media Transcoding: Enabled

Media List: Default Media List

Quality of Service

Quality Metrics Number of Calls: 10 [1..100]

Quality Metrics Time Before Retry: 10 [1-60] min.

Min. ASR Threshold: 0 % [0..100]

Enable Min MOS Threshold: Disabled

Enable Max. R/T Delay: Enabled

Max. R/T Delay: 65535 ms [1..65535]

Enable Max. Jitter: Enabled

Max. Jitter: 3000 ms [1..3000]

GV to PSTN :

- Click the **Create Routing Entry (+)** icon.
- Attach the Transformation Table (**PASSTHROUGH_GV**).
- Add the Destination Signaling Group **PSTN_SG**.
- In the Media panel, select DSP from the Audio Stream Mode and enable Media Transcoding.
- Click OK.

Google Voice Configuration

For configuration on Google Voice, visit support.google.com/a?p=siplink.

Supplementary Services & Features Coverage

The following checklist depicts the set of services/features covered through the configuration defined in this Interop Guide.

Sr. No.	Supplementary Services/ Features	Coverage
1	Auto Attendant	✓
2	DTMF - RFC2833	✓
3	Basic Call Setup & Termination	✓
4	Calls to/from GV Android Client, Web Client and Desk-phone (OBi based)	✓
5	Long Duration Calls	✓
6	Session Timers	✓
7	Voice Mail Deposit and Retrieval	✓
8	4xx/5xx Response Handling	✓

9	Ring Group	✓
10	Call Hold/Resume	✓
11	Call Transfer (Attended)	✓
12	Call Transfer (Blind/ Unattended)	✓
13	Call Forwarding Unconditional	✓
14	Call Forward No Answer	✓
15	Call Cancel/Reject	✓
16	Short Code Dialing	✗

Legend

Supported	✓
Not Supported	✗

Caveats

The following items should be noted in relation to this Interop - these are either limitations, untested elements, or useful information pertaining to the Interoperability.

- Short Code calls are not supported on Google Voice clients.
- When GV rejects or does not answer the call from PSTN, the call is expected to connect to GV Voice Mail after 30 seconds. However, the SWe Edge sends a CANCEL to GV to terminate the call before it connects.

These issues will be addressed by GV/Ribbon in their upcoming releases.

Support

For any support related queries about this guide, please contact your local Ribbon representative, or use the details below:

- Sales and Support: 1-833-742-2661
- Other Queries: 1-877-412-8867
- Website: <https://ribboncommunications.com/services/ribbon-support-portal>

References

For detailed information about Ribbon products & solutions, please visit:

<https://ribboncommunications.com/products>

Conclusion

This Interoperability Guide describes successful configuration for Google Voice SIP Link interop involving the Ribbon SBC SWe Edge.

All features and capabilities tested are detailed within this document - any limitations, notes, or observations are also recorded in order to provide the reader with an accurate understanding of what has been covered, and what has not.

Configuration guidance is provided to enable the reader to replicate the same base setup - there may be additional configuration changes required to suit the exact deployment environment.

