
Ribbon SBC Core 5K_7K_SWe R9.2 Interop with Google Voice SIP Link for Multitenancy : Interoperability Guide



Table of Contents

- Interoperable Vendors
- Copyright
- Document Overview
 - About Ribbon SBC Core
 - About Google Voice
 - Multitenancy
- Scope/Non-Goals
- Audience
- Prerequisites
- Product and Device Details
- Network Topology and E2E Flow Diagrams
 - Deployment Topology
 - Interoperability Test Lab Topology
 - Call Flow Diagram
- Document Workflow
- Installing Ribbon SBC Core
 - Ribbon SBC Standalone
 - Ribbon SBC High Availability
- Ribbon SBC Core Configuration
 - Global Configuration
 - Codec Entry
 - SBC Configuration for PSTN Side
 - Common Configuration for Carrier-1 and Carrier-2
 - Carrier-1 Configuration
 - Carrier-2 Configuration
 - SBC Configuration for Google Voice SIP Link Side
 - Common Configuration for Google Voice SIP Link Tenant-1 and Tenant-2
 - Tenant-1 Configuration
 - Tenant-2 Configuration
 - Call Routing
 - Routing Label
 - Route
 - Media Encryption
 - DTLS
 - SDES-SRTP
 - Ribbon SBC Core High Availability
 - HA Configuration
- 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 the Ribbon SBC Core (SBC 5K, 7K, SWe) when deployed with Google Voice SIP Link for Multi-tenant.

About Ribbon SBC Core

The SBC Core (SBC 5K, 7K, SWe) addresses the next-generation needs of SIP communications by delivering embedded media transcoding, robust security and advanced call routing in a high-performance, small form-factor device enabling service providers and enterprises to quickly and securely enhance their network by implementing services like SIP Trunking, secure Unified Communications and Voice over IP (VoIP).

The SBC Core provides a reliable, scalable platform for IP interconnect to deliver security, session control, bandwidth management, advanced media services and integrated billing/reporting tools in an SBC appliance. This versatile series of SBCs can be deployed as peering SBCs, access SBCs or enterprise SBCs (eSBCs). The SBC product family is tested for interoperability and performance against a variety of third-party products and call flow configurations in the customer networks.



Note

SBC 5x10, 5400, 7000 and SWe are represented as SBC Core in the subsequent sections.

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 U.S. 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.

Multitenancy

In a multitenancy environment, multiple customers share the same application, running on the same operating system, on the same hardware, with the same data-storage mechanism. The distinction between the customers is achieved during application design, thus customers do not share or see each other's data.

Scope/Non-Goals

This document provides configuration best practices for deploying Ribbon's SBC Core 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, and
- 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.

Prerequisites

The following aspects are required before proceeding with the interop:

- Ribbon SBC Core
- Ribbon SBC Core license
 - A valid license from Ribbon is required to enable functionality on Ribbon SBCs. Each SBC license provides a base set of capabilities to allow enabling and adding of additional features and capacity, as required.
- Public IP addresses
- TLS certificates for SBC Core
 - Please refer to [Managing 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	Appliance/ Application/ Tool	Software Version
Ribbon SBC	Ribbon SBC Core	9.2.0
Google Voice	Telephony Service	NA
Third-party Equipment	Cisco Unified Communications Manager	12.5.1.11900-146
	Poly VVX 411	5.9.3.2857
Administration and Debugging Tools	Wireshark	3.4.9

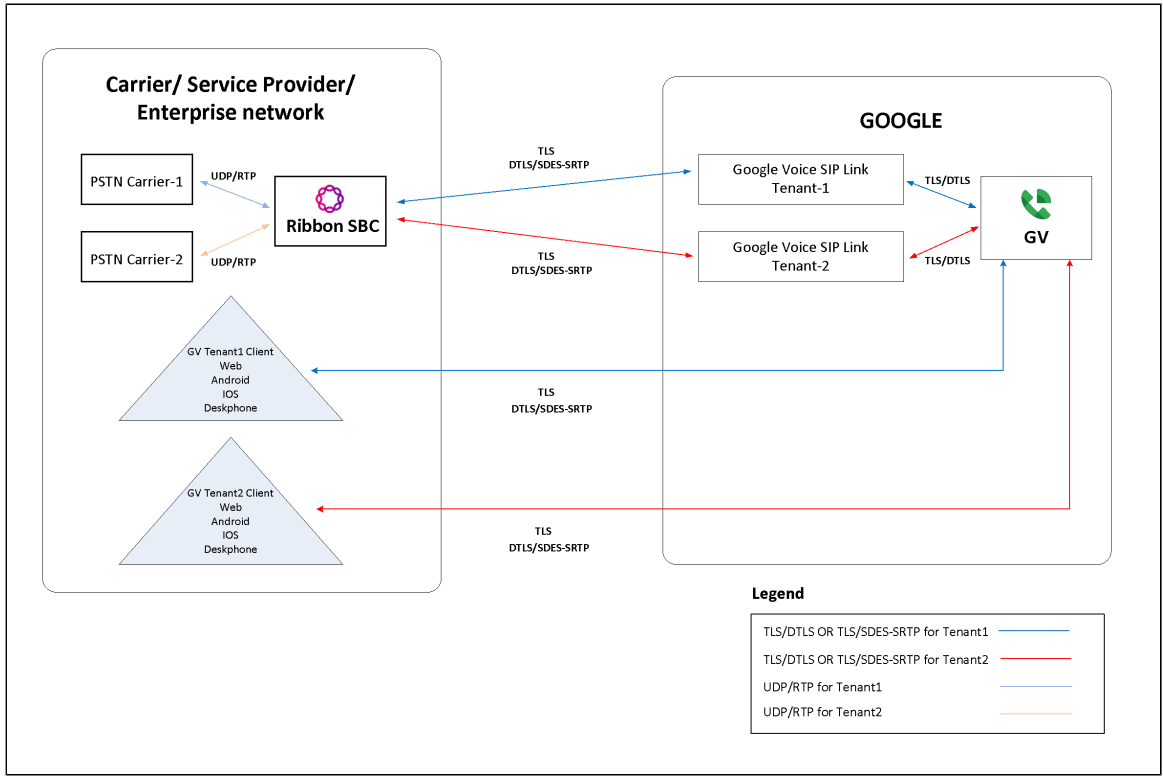


Note

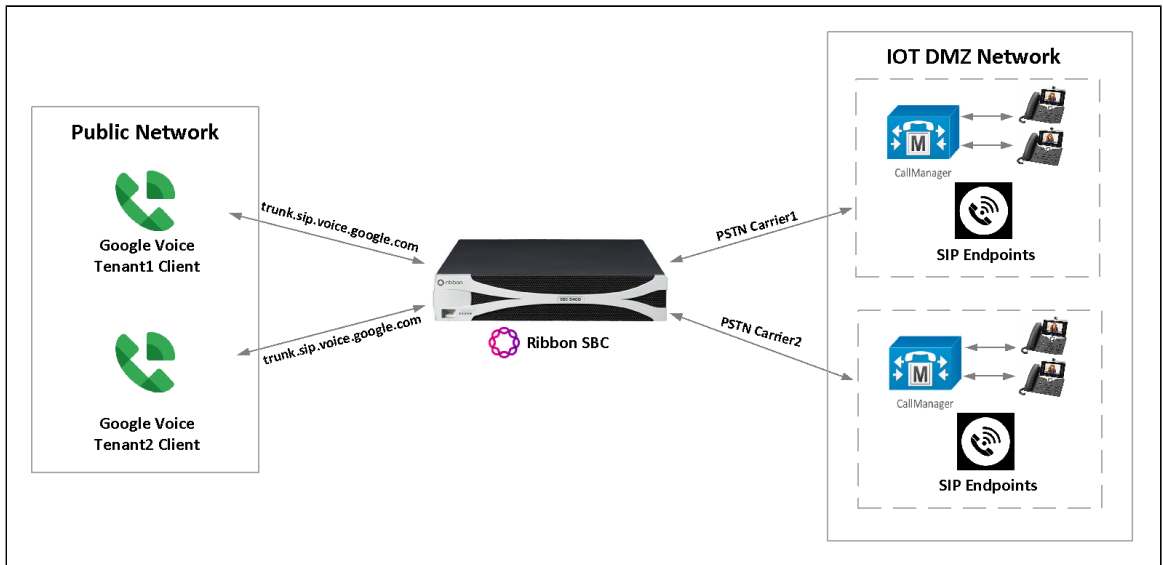
The Ribbon SBC Core portfolio includes SBC 5x10, SBC 5400, SBC 7000 (appliance based), and SBC SWe (virtualized platform). The software version is applicable to Ribbon SBC Core portfolio, and hence, this configuration guide is valid for all of these devices.

Network Topology and E2E Flow Diagrams

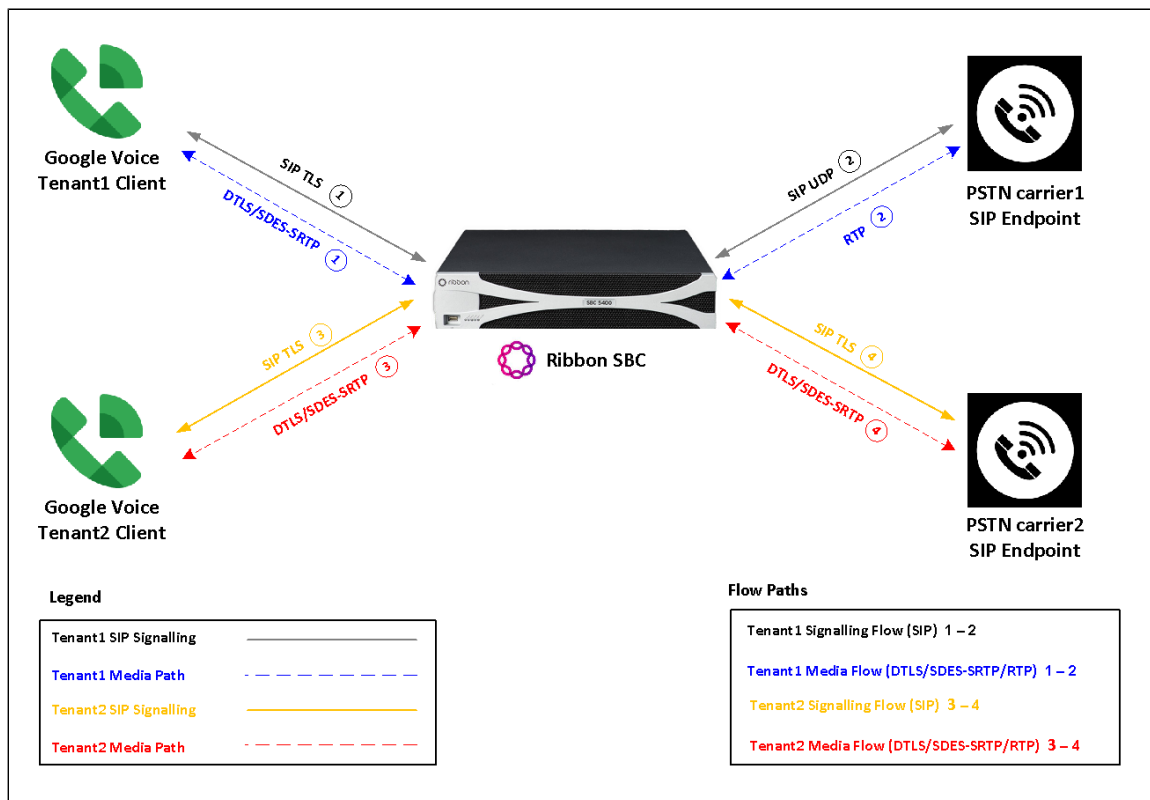
Deployment Topology



Interoperability Test Lab Topology

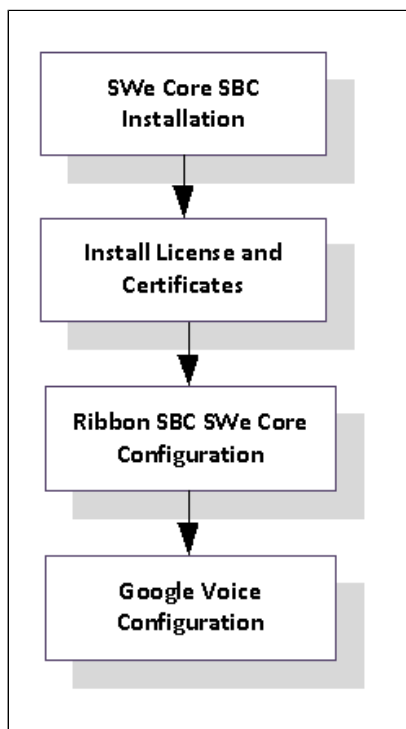


Call Flow Diagram



Document Workflow

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



Installing Ribbon SBC Core

Ribbon SBC Standalone

To deploy Ribbon SBC Core standalone instance, refer to [SBC Core 9.2.x Documentation](#).

Ribbon SBC High Availability

To deploy Ribbon SBC Core in HA mode on different platforms, refer to [SBC Core Software Installation and Upgrade Guide](#).



Info

During this interop, SBC Core HA was installed on VMware platform by following the procedure described in [Installing SBC Application in High Availability Mode](#).



Tip

- After successful installation, ensure the time on both Active and Standby SBCs is in sync.
- NTP Sync verification:
 - Run the command 'timedatectl' to check if NTP is synchronized.
 - File /etc/ntp.conf should contain the IP of the NTP server that you have configured during installation.

Ribbon SBC Core Configuration

Global Configuration

Codec Entry

Codecs define the audio encoding methods and their associated attributes. You can add custom codec entries which are then available to include when configuring codecs in a Packet Service Profile. When you add a codec entry, the parameters available change, depending on the base codec you select. You can also configure options for a selected Codec Entry that specify how to handle DTMF digits in the media stream.

```

set profiles media codecEntry G711-U codec g711
set profiles media codecEntry G711-U packetSize 20
set profiles media codecEntry G711-U fax failureHandling continue
set profiles media codecEntry G711-U fax toneTreatment faxRelayOrFallbackToG711
set profiles media codecEntry G711-U fax honorToneDetection disable
set profiles media codecEntry G711-U modem failureHandling continue
set profiles media codecEntry G711-U modem toneTreatment fallbackToG711
set profiles media codecEntry G711-U modem honorToneDetection disable
set profiles media codecEntry G711-U law ULaw
set profiles media codecEntry G711-U dtmf relay rfc2833
set profiles media codecEntry G711-U dtmf removeDigits enable
commit

set profiles media codecEntry G711-A codec g711
set profiles media codecEntry G711-A packetSize 20
set profiles media codecEntry G711-A fax failureHandling continue
set profiles media codecEntry G711-A fax toneTreatment faxRelayOrFallbackToG711
set profiles media codecEntry G711-A fax honorToneDetection disable
set profiles media codecEntry G711-A modem failureHandling continue
set profiles media codecEntry G711-A modem toneTreatment fallbackToG711
set profiles media codecEntry G711-A modem honorToneDetection disable
set profiles media codecEntry G711-A law ALaw
set profiles media codecEntry G711-A dtmf relay rfc2833
set profiles media codecEntry G711-A dtmf removeDigits enable
commit

set profiles media codecEntry OPUS codec opus
set profiles media codecEntry OPUS packetSize 20
set profiles media codecEntry OPUS preferredRtpPayloadType 111
set profiles media codecEntry OPUS fax failureHandling continue
set profiles media codecEntry OPUS fax toneTreatment none
set profiles media codecEntry OPUS modem failureHandling continue
set profiles media codecEntry OPUS modem toneTreatment none
set profiles media codecEntry OPUS dtmf relay rfc2833
set profiles media codecEntry OPUS dtmf removeDigits enable
set profiles media codecEntry OPUS maxAverageBitRate 20000
commit

set profiles media codecEntry G722 codec g722
set profiles media codecEntry G722 codingRate 64
set profiles media codecEntry G722 packetSize 20
set profiles media codecEntry G722 preferredRtpPayloadType 128
set profiles media codecEntry G722 fax failureHandling continue
set profiles media codecEntry G722 fax toneTreatment none
set profiles media codecEntry G722 modem failureHandling continue
set profiles media codecEntry G722 modem toneTreatment none
set profiles media codecEntry G722 dtmf relay rfc2833
set profiles media codecEntry G722 dtmf removeDigits enable
commit

```

SBC Configuration for PSTN Side

Common Configuration for Carrier-1 and Carrier-2

The configuration is to establish an end-to-end connectivity between PSTN carriers and Google Voice SIP Link. Here, Carrier-1 is connected to Tenant-1 and Carrier-2 to Tenant-2.

SIP Message Manipulation - PSTN

The SIP Adaptor Profile object is the main construct for SIP Message Manipulation (SMM) functionality. A SIP Adaptor Profile is associated with a SIP Trunk Group or Zone in order to act upon SIP messages passing into or out of that group. A SIP Trunk Group can have two SIP Adaptor Profiles, an input adaptor profile for manipulation of inbound messages, and an output adaptor profile for manipulation of outbound messages. Similarly, a Zone can have two SIP Adaptor Profiles.

SIP Message Manipulation (SMM) allows you to modify SIP messages as they are processed by the SBC Core in both inbound and outbound directions. Using SMM criteria and actions, you define SMM rules within a SIP adaptor profile, which the SBC applies to SIP messages in order to modify their headers and/or parameters. When a message comes into or out of the SBC and a SIP adaptor profile applies, the message is evaluated based on the set of criteria in the profile. If the message meets the criteria, it is modified according to actions defined in the profile.

Since a=inactive is not supported on Google Voice, the SMM PSTN_sendonly is used to modify the parameter to a=sendonly.

```

set profiles signaling sipAdaptorProfile PSTN_sendonly state enabled
set profiles signaling sipAdaptorProfile PSTN_sendonly advancedSMM disabled
set profiles signaling sipAdaptorProfile PSTN_sendonly profileType messageManipulation
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 applyMatchHeader one
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 criterion 1 type message
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 criterion 1 message
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 criterion 1 message methodTypes [ invite ]
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 criterion 2 type messageBody
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 criterion 2 messageBody
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 criterion 2 messageBody condition exist
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 action 1 type messageBody
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 action 1 operation regsub
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 action 1 from
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 action 1 from type value
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 action 1 from value a=sendonly
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 action 1 to
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 action 1 to type messageBody
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 action 1 to messageBodyValue all
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 action 1 regexp
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 action 1 regexp string a=inactive
set profiles signaling sipAdaptorProfile PSTN_sendonly rule 1 action 1 regexp matchInstance all
commit

```

IP Interface Group

An IP Interface Group is a named object containing one or more IP interfaces (IP addresses). The IP Interface Group is Address Context-specific (e.g. permanently bound to a particular Address Context), and is the primary tool to manage disjointed networks (separate networks that are not designed to communicate directly). An IP Interface Group is the local manifestation of a segregated network domain. The service section of an IP trunk group and a Signaling Port typically reference an IP Interface Group in order to restrict signaling and/or media activity to that IP Interface Group.

```

set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0 ceName GOOGLEVOICE
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0 portName pkt0
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0 ipAddress x.x.x.x
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0 prefix x
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0 mode inService state enabled
commit

```

IP Static Route

This object specifies the gateway to which you wish to direct traffic from your Packet, Management, or Link Interface. In effect, this object allows you to add, change, and delete gateways (next Hops) to these interfaces. Interface and static routes combine to form the IP routing table for your network.

An IP Static Route provides a route to each potential call destination IP address. The static route is used to add static IP routes for the IP interfaces. A static route indicates the next Hop gateway and IP interface to use for a particular peer network IP prefix.

```

set addressContext default staticRoute x.x.x.x x x.x.x.x LIF1 PKT0 preference 100
commit

```

Carrier-1 Configuration

Packet Service Profile

Each Packet Service Profile is configured for a pair of gateways, and includes entries for up to four audio/video encoding methods. The pair of gateways can be originating for destination gateways in the same gateway group, or can be originating for destination gateways in an inter-gateway group.


```

set profiles media packetServiceProfile PSTN_PSP codec codecEntry1 G711-U
set profiles media packetServiceProfile PSTN_PSP codec codecEntry2 G711-A
set profiles media packetServiceProfile PSTN_PSP codec codecEntry4 G722
set profiles media packetServiceProfile PSTN_PSP packetToPacketControl transcode conditional
set profiles media packetServiceProfile PSTN_PSP packetToPacketControl codecsAllowedForTranscoding thisLeg g711a,
g711u,g722
set profiles media packetServiceProfile PSTN_PSP packetToPacketControl codecsAllowedForTranscoding otherLeg g711a,
g711u,g722,opus
set profiles media packetServiceProfile PSTN_PSP preferredRtpPayloadTypeForDtmfRelay 127
commit

```

Zone

A zone is used to group a set of objects unique in a particular customer environment.

```

set addressContext default zone PSTN id 2
commit

```

SIP Signaling Port

A SIP Signaling Port is a logical address permanently bound to a specific zone, and is used to send and receive SIP call signaling packets. A SIP Signaling Port is capable of multiple transports such as UDP, TCP and TLS/TCP.

```

set addressContext default zone PSTN sipSigPort 2 ipInterfaceGroupName LIF1 ipAddressV4 x.x.x.x portNumber
<port_number> transportProtocolsAllowed sip-udp,sip-tcp
set addressContext default zone PSTN sipSigPort 2 mode inService state enabled
commit

```

Trunk Group

SIP Trunk Groups are used to apply a wide-ranging set of call management functions to a group of peer devices (endpoints) within the network. SIP Trunk Groups are created within a specific address context and zone.

All SBC signaling and routing (both Trunking and Access) are based upon Trunk Group configurations defined within zones. A zone can contain multiple Trunk Groups.

```

set addressContext default zone PSTN sipTrunkGroup PSTN_TG media mediaIpInterfaceGroupName LIF1
set addressContext default zone PSTN sipTrunkGroup PSTN_TG signaling timers sessionKeepalive 600
set addressContext default zone PSTN sipTrunkGroup PSTN_TG signaling timers sessionMinSE 90
set addressContext default zone PSTN sipTrunkGroup PSTN_TG ingressIpPrefix x.x.x.x x
set addressContext default zone PSTN sipTrunkGroup PSTN_TG policy media packetServiceProfile PSTN_PSP
set addressContext default zone PSTN sipTrunkGroup PSTN_TG signaling messageManipulation inputAdapterProfile
PSTN_sendonly
set addressContext default zone PSTN sipTrunkGroup PSTN_TG mode inService state enabled
commit

```

IP Peer

IP Peer is an entity of Session Border Controller, which is configured inside the Zone. It acts as a destination endpoint for the call to be routed. An IP Peer constitutes an IPv4/IPv6 address or a Fully Qualified Domain Name (FQDN) with a port number.

```

set addressContext default zone PSTN ipPeer PSTN_IPP ipAddress x.x.x.x ipPort <ip_peer_port>
commit

```

Carrier-2 Configuration

Packet Service Profile

```
set profiles media packetServiceProfile PSTN_Multitenant_PSP codec codecEntry1 G711-U
set profiles media packetServiceProfile PSTN_Multitenant_PSP codec codecEntry2 G711-A
set profiles media packetServiceProfile PSTN_Multitenant_PSP codec codecEntry4 G722
set profiles media packetServiceProfile PSTN_Multitenant_PSP packetToPacketControl transcode conditional
set profiles media packetServiceProfile PSTN_Multitenant_PSP packetToPacketControl codecsAllowedForTranscoding
thisLeg g711a,g711u,g722
set profiles media packetServiceProfile PSTN_Multitenant_PSP packetToPacketControl codecsAllowedForTranscoding
otherLeg g711a,g711u,g722,opus
set profiles media packetServiceProfile PSTN_Multitenant_PSP preferredRtpPayloadTypeForDtmfRelay 127
commit
```

Zone

```
set addressContext default zone PSTN_Multitenant id 4
commit
```

SIP Signaling Port

```
set addressContext default zone PSTN_Multitenant sipSigPort 4 ipInterfaceGroupName LIF1 ipAddressV4 x.x.x.x
portNumber <port_number> transportProtocolsAllowed sip-udp,sip-tcp
set addressContext default zone PSTN_Multitenant sipSigPort 4 mode inService state enabled
commit
```

Trunk Group

```
set addressContext default zone PSTN_Multitenant sipTrunkGroup PSTN_Multitenant_TG media mediaIpInterfaceGroupName
LIF1
set addressContext default zone PSTN_Multitenant sipTrunkGroup PSTN_Multitenant_TG signaling timers
sessionKeepalive 600
set addressContext default zone PSTN_Multitenant sipTrunkGroup PSTN_Multitenant_TG signaling timers sessionMinSE 90
set addressContext default zone PSTN_Multitenant sipTrunkGroup PSTN_Multitenant_TG ingressIpPrefix x.x.x.x x
set addressContext default zone PSTN_Multitenant sipTrunkGroup PSTN_Multitenant_TG policy media
packetServiceProfile PSTN_PSP
set addressContext default zone PSTN_Multitenant sipTrunkGroup PSTN_Multitenant_TG signaling messageManipulation
inputAdapterProfile PSTN_sendonly
set addressContext default zone PSTN_Multitenant sipTrunkGroup PSTN_Multitenant_TG mode inService state enabled
commit
```

IP Peer

```
set addressContext default zone PSTN_Multitenant ipPeer PSTN_Multitenant_IPP ipAddress x.x.x.x ipPort
<ip_peer_port>
commit
```

SBC Configuration for Google Voice SIP Link Side

Common Configuration for Google Voice SIP Link Tenant-1 and Tenant-2

Path Check Profile

The Path Check Profile specifies the conditions that constitute a connectivity failure, and in the event of such a failure, the conditions that constitute a connectivity recovery. This profile specifies the configuration for OPTIONS PING.

```
set profiles services pathCheckProfile GOOGLE protocol sipOptions
set profiles services pathCheckProfile GOOGLE sendInterval 30
set profiles services pathCheckProfile GOOGLE replyTimeoutCount 1
set profiles services pathCheckProfile GOOGLE recoveryCount 1
set profiles services pathCheckProfile GOOGLE transportPreference preference1 tls-tcp
set profiles services pathCheckProfile GOOGLE transportPreference preference2 tcp
commit
```

SIP Message Manipulation - OPTIONS

The SMM SIP_OPTIONS is used to modify the FQDN in request URI and To header of OPTIONS to Google specified FQDN, trunk.sip.voice.google.com.

```
set profiles signaling sipAdaptorProfile SIP_OPTIONS state enabled
set profiles signaling sipAdaptorProfile SIP_OPTIONS advancedSMM disabled
set profiles signaling sipAdaptorProfile SIP_OPTIONS profileType messageManipulation
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 applyMatchHeader one
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 criterion 1 type message
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 criterion 1 message methodTypes [ options ]
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 criterion 2 type header
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 criterion 2 header
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 criterion 2 header name request-line
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 criterion 2 header numberOfInstances number 1
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 criterion 2 header numberOfInstances qualifier equal
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 action 1 type token
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 action 1 operation regsub
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 action 1 from
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 action 1 from type value
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 action 1 from value trunk.sip.voice.google.com
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 action 1 to
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 action 1 to type token
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 action 1 to tokenValue urihostname
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 action 1 regexp
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 action 1 regexp string siplink.telephony.goog
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 1 action 1 regexp matchInstance one
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 applyMatchHeader one
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 criterion 1 type message
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 criterion 1 message
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 criterion 1 message methodTypes [ options ]
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 criterion 2 type header
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 criterion 2 header
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 criterion 2 header name To
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 criterion 2 header numberOfInstances number 1
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 criterion 2 header numberOfInstances qualifier equal
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 type header
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 operation regsub
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 headerInfo fieldValue
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 from
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 from type value
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 from value trunk.sip.voice.google.com
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 to
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 to type header
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 to value To
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 regexp
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 regexp string siplink.telephony.goog
set profiles signaling sipAdaptorProfile SIP_OPTIONS rule 2 action 1 regexp matchInstance one
commit
```

IP Interface Group

```
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1 ceName GOOGLEVOICE
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1 portName pkt1
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1 ipAddress x.x.x.x
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1 prefix x
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1 mode inService state enabled
commit
```

DNS Group

The Domain Name System (DNS) group object contains a list of DNS servers used to resolve SIP NAPTR, SRV, and A-record lookups. The DNS server group is contained in an Address Context and is referenced by Zones and SIP Trunk Groups in that Address Context.

```
set addressContext default dnsGroup DNS type ip
set addressContext default dnsGroup DNS interface LIF2
set addressContext default dnsGroup DNS server PRIMARY_DNS state enabled
set addressContext default dnsGroup DNS server PRIMARY_DNS ipAddress 8.8.8.8
set addressContext default dnsGroup DNS server PRIMARY_DNS priority 1
commit
```

IP Static Route

```
set addressContext default staticRoute x.x.x.x x x.x.x.x LIF2 PKT1 preference 100
commit
```

Tenant-1 Configuration

TLS Certificates

- For TLS to work, a Trusted Certificate Authority (CA) is required. For this interop, GoDaddy is used as a Trusted CA.
- Add an entry in the Public DNS to resolve Ribbon SBC Core FQDN to Public IP Address.
- In the trust store of the SBC, ensure you 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.

Create the certificate for Ribbon SBC with the CN containing SBC's FQDN for Tenant-1.

```
set system security pki certificate SBC_CERT_GV type local-internal
commit
```

Command to generate CSR on SBC

```
request system security pki certificate SBC_CERT_GV generateCSR csrSub /C=IN/ST=KA/L=Bangalore/O=Sonus
/CN=<common_name_for_tenant1> keySize keySize2K
```

After generating the CSR for tenant-1 on Ribbon SBC, provide it to the Certificate Authority. CA would generally provide the following certificates:

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

Upload the certificates to Ribbon SBC at /opt/sonus/external and convert them into SBC readable format using openssl

i.e. SBC certificate must be in .pem or .p12 format and root certificate in .cer or .der format

Converting .crt to .pem using openssl for SBC Certificate.

```
openssl x509 -in sbc_cert.crt -out sbc_cert.der -outform DER
openssl x509 -in sbc_cert.der -inform DER -out sbc_cert.pem -outform PEM
```

After generating sbc_cert.pem file, convert it to .p12 format using below command and provide the location of the certificate key

```
openssl pkcs12 -export -out sbc1_cert.p12 -in sbc_cert.pem -inkey /opt/sonus/company_san.key.temp
```

Converting .crt to .cer using openssl for CA's Root and Intermediate Certificates.

```
openssl x509 -in root_cert.crt -out root_cert.cer -outform DER
```

After converting all these certificates, upload them to Ribbon SBC at /opt/sonus/external location.

Add all the required certificates on SBC.

```

set system security pki certificate gtsrl state enabled
set system security pki certificate gtsrl fileName gtsrl.der
set system security pki certificate gtsrl type remote
set system security pki certificate GoDaddy state enabled
set system security pki certificate GoDaddy fileName gd_bundle.der
set system security pki certificate GoDaddy type remote
set system security pki certificate GlobalSign state enabled
set system security pki certificate GlobalSign fileName globalsign.der
set system security pki certificate GlobalSign type remote
set system security pki certificate SBC_CERT_GV state enabled
set system security pki certificate SBC_CERT_GV fileName b43ffd9ad0d7a03.pem
set system security pki certificate SBC_CERT_GV type local-internal
set system security pki certificate global_root state enabled
set system security pki certificate global_root fileName roots.der
set system security pki certificate global_root type remote
commit

```

TLS Profile

This object creates and configures a profile for implementing the Transport Layer Security (TLS) protocol to use with SIP over TLS. TLS is an IETF protocol for securing communications across an untrusted network. Normally, SIP packets travel in plain text over TCP or UDP connections. Secure SIP is a security measure that uses TLS, the successor to the Secure Sockets Layer (SSL) protocol.

To add a TLS protection-level policy, create a TLS PROFILE and configure each of the parameters. The TLS profile is specified on the SIP Signaling Port and controls behavior of all TLS connections established on that signaling port.

```

set profiles security tlsProfile TLS_PROF appAuthTimer 5
set profiles security tlsProfile TLS_PROF handshakeTimer 5
set profiles security tlsProfile TLS_PROF sessionResumpTimer 3600
set profiles security tlsProfile TLS_PROF cipherSuite1 rsa-with-aes-128-cbc-sha
set profiles security tlsProfile TLS_PROF cipherSuite2 tls_ecdhe_rsa_with_aes_128_gcm_sha256
set profiles security tlsProfile TLS_PROF cipherSuite3 tls_rsa_with_aes_256_gcm_sha384
set profiles security tlsProfile TLS_PROF allowedRoles clientandserver
set profiles security tlsProfile TLS_PROF authClient true
set profiles security tlsProfile TLS_PROF clientCertName SBC_CERT_GV
set profiles security tlsProfile TLS_PROF serverCertName SBC_CERT_GV
set profiles security tlsProfile TLS_PROF acceptableCertValidationErrors none
set profiles security tlsProfile TLS_PROF v1_0 enabled
set profiles security tlsProfile TLS_PROF v1_1 enabled
set profiles security tlsProfile TLS_PROF v1_2 enabled
set profiles security tlsProfile TLS_PROF suppressEmptyFragments disabled
set profiles security tlsProfile TLS_PROF peerNameVerify disabled
commit

```

IP Signaling Profile

This object specifies parameters associated with H.323, SIP, SIP-I communication that are sent as part of the outgoing signaling message after standard protocol rules are applied.

```

set profiles signaling ipSignalingProfile GOOGLE_IPSP commonIpAttributes flags customizedSessionTimerBehavior
enable
set profiles signaling ipSignalingProfile GOOGLE_IPSP commonIpAttributes flags includeTransportTypeInContactHeader
enable
set profiles signaling ipSignalingProfile GOOGLE_IPSP commonIpAttributes flags sessionTimerRefreshUpdate enable
set profiles signaling ipSignalingProfile GOOGLE_IPSP commonIpAttributes transparencyFlags fromHeader disable
set profiles signaling ipSignalingProfile GOOGLE_IPSP commonIpAttributes transparencyFlags requestURI disable
set profiles signaling ipSignalingProfile GOOGLE_IPSP commonIpAttributes transparencyFlags toHeader disable
set profiles signaling ipSignalingProfile GOOGLE_IPSP egressIpAttributes numberGlobalizationProfile DEFAULT_IP
set profiles signaling ipSignalingProfile GOOGLE_IPSP egressIpAttributes privacy privacyInformation pAssertedId
set profiles signaling ipSignalingProfile GOOGLE_IPSP egressIpAttributes sipHeadersAndParameters
sessionExpiresRefresher notSend
set profiles signaling ipSignalingProfile GOOGLE_IPSP egressIpAttributes transport type1 tlsOverTcp
commit

```

Packet Service Profile

```

set profiles media packetServiceProfile GOOGLE_PSP rtcpOptions rtcp enable
set profiles media packetServiceProfile GOOGLE_PSP rtcpOptions rtcpMux enable
set profiles media packetServiceProfile GOOGLE_PSP codec codecEntry1 G711-U
set profiles media packetServiceProfile GOOGLE_PSP codec codecEntry2 G711-A
set profiles media packetServiceProfile GOOGLE_PSP codec codecEntry3 OPUS
set profiles media packetServiceProfile GOOGLE_PSP codec codecEntry4 G722
set profiles media packetServiceProfile GOOGLE_PSP packetToPacketControl transcode conditional
set profiles media packetServiceProfile GOOGLE_PSP packetToPacketControl codecsAllowedForTranscoding thisLeg g711a,
g711u,g722,opus
set profiles media packetServiceProfile GOOGLE_PSP packetToPacketControl codecsAllowedForTranscoding otherLeg
g711a,g711u,g722,opus
set profiles media packetServiceProfile GOOGLE_PSP preferredRtpPayloadTypeForDtmfRelay 127
set profiles media packetServiceProfile GOOGLE_PSP secureRtpRtcp cryptoSuiteProfile DEFAULT
set profiles media packetServiceProfile GOOGLE_PSP secureRtpRtcp flags allowFallback disable
set profiles media packetServiceProfile GOOGLE_PSP secureRtpRtcp flags enableSrtp disable
set profiles media packetServiceProfile GOOGLE_PSP secureRtpRtcp flags resetROConKeyChange disable
set profiles media packetServiceProfile GOOGLE_PSP secureRtpRtcp flags resetEncDecROConDecKeyChange disable
set profiles media packetServiceProfile GOOGLE_PSP secureRtpRtcp flags updateCryptoKeysOnModify disable
set profiles media packetServiceProfile GOOGLE_PSP secureRtpRtcp flags allowPassthru disable
set profiles media packetServiceProfile GOOGLE_PSP dtls dtlsCryptoSuiteProfile DEFAULT
set profiles media packetServiceProfile GOOGLE_PSP dtls dtlsFlags allowDtlsFallback disable
set profiles media packetServiceProfile GOOGLE_PSP dtls dtlsFlags enableDtlsSrtp enable
set profiles media packetServiceProfile GOOGLE_PSP dtls dtlsFlags dtlsSrtpRelay disable
set profiles media packetServiceProfile GOOGLE_PSP dtls dtlsFlags dtlsSctpRelay disable
commit

```

SIP Message Manipulation - Google

The SMM GOOGLE_ADP 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 for Tenant-1.
- To change the request URI of the 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.

```

set profiles signaling sipAdaptorProfile GOOGLE_ADP state enabled
set profiles signaling sipAdaptorProfile GOOGLE_ADP advancedSMM disabled
set profiles signaling sipAdaptorProfile GOOGLE_ADP profileType messageManipulation
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 applyMatchHeader one
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 criterion 1 type message
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 criterion 1 message
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 criterion 1 message messageTypes requestAll
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 action 1 type header
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 action 1 operation add
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 action 1 headerPosition last
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 action 1 from
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 action 1 from type header
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 action 1 from value <trunk_secret_key_for_tenant1>
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 action 1 to
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 action 1 to type header
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 1 action 1 to value X-Google-Pbx-Trunk-Secret-Key
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 applyMatchHeader one
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 criterion 1 type message
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 criterion 1 message
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 criterion 1 message methodTypes [ cancel invite ack ]
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 criterion 2 type header
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 criterion 2 header
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 criterion 2 header name request-line
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 criterion 2 header numberOfInstances number 1
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 criterion 2 header numberOfInstances qualifier equal
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 action 1 type token
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 action 1 operation regsub
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 action 1 from
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 action 1 from type value
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 action 1 from value trunk.sip.voice.google.com
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 action 1 to
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 action 1 to type token
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 action 1 to tokenValue urihostname

```

```

set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 action 1 regexp
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 action 1 regexp string "^(25[0-5]|(2[0-4]|1[0-9]|[1-9]
)[0-9])(\.(?!$)|$)){4}$"
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 2 action 1 regexp matchInstance one
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 applyMatchHeader one
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 criterion 1 type message
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 criterion 1 message
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 criterion 1 message methodTypes [ cancel invite ack ]
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 criterion 2 type header
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 criterion 2 header
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 criterion 2 header name To
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 criterion 2 header numberOfInstances number 1
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 criterion 2 header numberOfInstances qualifier equal
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 type header
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 operation regsub
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 headerInfo fieldValue
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 from
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 from type value
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 from value trunk.sip.voice.google.com
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 to
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 to type header
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 to value To
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 regexp
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 regexp string siplink.telephony.goog
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 3 action 1 regexp matchInstance one
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 applyMatchHeader one
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 criterion 1 type message
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 criterion 1 message
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 criterion 1 message methodTypes [ cancel invite ack ]
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 criterion 2 type header
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 criterion 2 header
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 criterion 2 header name request-line
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 criterion 2 header numberOfInstances number 1
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 criterion 2 header numberOfInstances qualifier equal
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 action 1 type token
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 action 1 operation regsub
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 action 1 from
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 action 1 from type value
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 action 1 from value trunk.sip.voice.google.com
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 action 1 to
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 action 1 to type token
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 action 1 to tokenValue urihostname
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 action 1 regexp
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 action 1 regexp string siplink.telephony.goog
set profiles signaling sipAdaptorProfile GOOGLE_ADP rule 4 action 1 regexp matchInstance one
commit

```

Zone

```

set addressContext default zone GOOGLE id 3
set addressContext default zone GOOGLE messageManipulation outputAdapterProfile SIP_OPTIONS
set addressContext default zone GOOGLE dnsGroup DNS
commit

```

SIP Signaling Port

```

set addressContext default zone GOOGLE sipSigPort 3 ipInterfaceGroupName LIF2 ipAddressV4 x.x.x.x portNumber
<tls_port1> transportProtocolsAllowed sip-tls-tcp
set addressContext default zone GOOGLE sipSigPort 3 tlsProfileName TLS_PROF
set addressContext default zone GOOGLE sipSigPort 3 tcpKeepaliveTime 100
set addressContext default zone GOOGLE sipSigPort 3 tcpKeepaliveInterval 60
set addressContext default zone GOOGLE sipSigPort 3 tcpKeepaliveProbes 2
set addressContext default zone GOOGLE sipSigPort 3 mode inService state enabled
commit

```

Trunk Group



Note

IngressIpPrefix must be entered with Google Voice SIP Link's Signaling IP address.

```
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG media mediaIpInterfaceGroupName LIF2
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG signaling timers sessionKeepalive 1800
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG signaling timers sessionMinSE 90
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG ingressIpPrefix x.x.x.x x
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG policy media packetServiceProfile GOOGLE_PSP
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG policy signaling ipSignalingProfile GOOGLE_IPSP
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG services natTraversal tcpKeepaliveTimer 240
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG signaling messageManipulation outputAdapterProfile
GOOGLE_ADP
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG mode inService state enabled
commit
```

IP Peer

```
set addressContext default zone GOOGLE ipPeer GOOGLE_IPP policy description ""
set addressContext default zone GOOGLE ipPeer GOOGLE_IPP policy sip fqdn siplink.telephony.goog
set addressContext default zone GOOGLE ipPeer GOOGLE_IPP policy sip fqdnPort 5671
set addressContext default zone GOOGLE ipPeer GOOGLE_IPP pathCheck profile GOOGLE
set addressContext default zone GOOGLE ipPeer GOOGLE_IPP pathCheck hostName siplink.telephony.goog
set addressContext default zone GOOGLE ipPeer GOOGLE_IPP pathCheck hostPort 5671
set addressContext default zone GOOGLE ipPeer GOOGLE_IPP pathCheck state enabled
set addressContext default zone GOOGLE ipPeer GOOGLE_IPP pathCheck statusUpdateSupport enabled
commit
```

Tenant-2 Configuration

TLS Certificates

Create the certificate for Ribbon SBC with the CN containing SBC's FQDN for Tenant-2.

```
set system security pki certificate SBC_CERT_GV_2 type local-internal
commit
```

Command to generate CSR on SBC

```
request system security pki certificate SBC_CERT_GV_2 generateCSR csrSub /C=IN/ST=KA/L=Bangalore/O=Sonus
/CN=<common_name_tenant2> keySize keySize2K
```

After generating the CSR for tenant-2 on Ribbon SBC, provide it to the Certificate Authority and get the required certificates.

After converting the certificates(SBC Certificate, Root Certificate and Intermediate Certificate) to suitable formats, upload them to Ribbon SBC at /opt/sonus/external location.

Add all the required certificates on SBC.

```
set system security pki certificate SBC_CERT_GV_2 state enabled
set system security pki certificate SBC_CERT_GV_2 fileName <sbccert_tenant_2.pem>
set system security pki certificate SBC_CERT_GV_2 type local-internal
commit
```

TLS Profile


```

set profiles security tlsProfile TLS_PROF_2 appAuthTimer 5
set profiles security tlsProfile TLS_PROF_2 handshakeTimer 5
set profiles security tlsProfile TLS_PROF_2 sessionResumpTimer 3600
set profiles security tlsProfile TLS_PROF_2 cipherSuite1 rsa-with-aes-128-cbc-sha
set profiles security tlsProfile TLS_PROF_2 cipherSuite2 tls_ecdhe_rsa_with_aes_128_gcm_sha256
set profiles security tlsProfile TLS_PROF_2 cipherSuite3 tls_rsa_with_aes_256_gcm_sha384
set profiles security tlsProfile TLS_PROF_2 allowedRoles clientandserver
set profiles security tlsProfile TLS_PROF_2 authClient true
set profiles security tlsProfile TLS_PROF_2 clientCertName SBC_CERT_GV_2
set profiles security tlsProfile TLS_PROF_2 serverCertName SBC_CERT_GV_2
set profiles security tlsProfile TLS_PROF_2 acceptableCertValidationErrors none
set profiles security tlsProfile TLS_PROF_2 v1_0 enabled
set profiles security tlsProfile TLS_PROF_2 v1_1 enabled
set profiles security tlsProfile TLS_PROF_2 v1_2 enabled
set profiles security tlsProfile TLS_PROF_2 suppressEmptyFragments disabled
set profiles security tlsProfile TLS_PROF_2 peerNameVerify disabled
commit

```

IP Signaling Profile

This object specifies parameters associated with H.323, SIP, SIP-I communication that are sent as part of the outgoing signaling message after standard protocol rules are applied.

```

set profiles signaling ipSignalingProfile GOOGLE_Multitenant_IPSP commonIpAttributes flags
customizedSessionTimerBehavior enable
set profiles signaling ipSignalingProfile GOOGLE_Multitenant_IPSP commonIpAttributes flags
includeTransportTypeInContactHeader enable
set profiles signaling ipSignalingProfile GOOGLE_Multitenant_IPSP commonIpAttributes flags
sessionTimerRefreshUpdate enable
set profiles signaling ipSignalingProfile GOOGLE_Multitenant_IPSP commonIpAttributes transparencyFlags fromHeader
disable
set profiles signaling ipSignalingProfile GOOGLE_Multitenant_IPSP commonIpAttributes transparencyFlags requestURI
disable
set profiles signaling ipSignalingProfile GOOGLE_Multitenant_IPSP commonIpAttributes transparencyFlags toHeader
disable
set profiles signaling ipSignalingProfile GOOGLE_Multitenant_IPSP egressIpAttributes numberGlobalizationProfile
DEFAULT_IP
set profiles signaling ipSignalingProfile GOOGLE_Multitenant_IPSP egressIpAttributes privacy privacyInformation
pAssertedId
set profiles signaling ipSignalingProfile GOOGLE_Multitenant_IPSP egressIpAttributes sipHeadersAndParameters
sessionExpiresRefresher notSend
set profiles signaling ipSignalingProfile GOOGLE_Multitenant_IPSP egressIpAttributes transport type1 tlsOverTcp
commit

```

Packet Service Profile

```

set profiles media packetServiceProfile GOOGLE_Multitenant_PSP rtcpOptions rtcp enable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP rtcpOptions rtcpMux enable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP codec codecEntry1 G711-U
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP codec codecEntry2 G711-A
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP codec codecEntry3 OPUS
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP codec codecEntry4 G722
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP packetToPacketControl transcode conditional
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP packetToPacketControl codecsAllowedForTranscoding
thisLeg g711a,g711u,g722,opus
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP packetToPacketControl codecsAllowedForTranscoding
otherLeg g711a,g711u,g722,opus
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP preferredRtpPayloadTypeForDtmfRelay 127
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP secureRtpRtcp cryptoSuiteProfile DEFAULT
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP secureRtpRtcp flags allowFallback disable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP secureRtpRtcp flags enableSrtp disable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP secureRtpRtcp flags resetROCOOnKeyChange disable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP secureRtpRtcp flags resetEncDecROCOOnDecKeyChange
disable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP secureRtpRtcp flags updateCryptoKeysOnModify disable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP secureRtpRtcp flags allowPassthru disable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP dtls dtlsCryptoSuiteProfile DEFAULT
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP dtls dtlsFlags allowDtlsFallback disable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP dtls dtlsFlags enableDtlsSrtp enable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP dtls dtlsFlags dtlsSrtpRelay disable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP dtls dtlsFlags dtlsSctpRelay disable
commit

```

SIP Message Manipulation - Google

The SMM GOOGLE_Multitenant_ADP 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 for Tenant-2.
- To change the request URI of the 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.

```

set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP state enabled
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP advancedSMM disabled
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP profileType messageManipulation
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 applyMatchHeader one
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 criterion 1 type message
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 criterion 1 message
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 criterion 1 message messageTypes requestAll
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 action 1 type header
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 action 1 operation add
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 action 1 headerPosition last
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 action 1 from
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 action 1 from type header
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 action 1 from value
<trunk_secret_key_for_tenant2>
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 action 1 to
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 action 1 to type header
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 1 action 1 to value X-Google-Pbx-Trunk-Secret-
Key
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 applyMatchHeader one
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 criterion 1 type message
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 criterion 1 message
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 criterion 1 message methodTypes [ cancel
invite ack ]
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 criterion 2 type header
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 criterion 2 header
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 criterion 2 header name request-line
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 criterion 2 header numberOfInstances number
1
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 criterion 2 header numberOfInstances
qualifier equal
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 action 1 type token
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 action 1 operation regsub

```

```

set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 action 1 from
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 action 1 from type value
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 action 1 from value trunk.sip.voice.google.
com
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 action 1 to
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 action 1 to type token
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 action 1 to tokenValue urihostname
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 action 1 regexp
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 action 1 regexp string "^((25[0-5]|(2[0-4]|1
[0-9]|[1-9]))[0-9])(\.(?!$)|$)){4}$"
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 2 action 1 regexp matchInstance one
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 applyMatchHeader one
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 criterion 1 type message
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 criterion 1 message
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 criterion 1 message methodTypes [ cancel
invite ack ]
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 criterion 2 type header
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 criterion 2 header
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 criterion 2 header name To
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 criterion 2 header numberOfInstances number
1
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 criterion 2 header numberOfInstances
qualifier equal
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 type header
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 operation regsub
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 headerInfo fieldValue
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 from
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 from type value
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 from value trunk.sip.voice.google.
com
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 to
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 to type header
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 to value To
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 regexp
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 regexp string siplink.telephony.
goog
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 3 action 1 regexp matchInstance one
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 applyMatchHeader one
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 criterion 1 type message
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 criterion 1 message
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 criterion 1 message messageTypes request
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 criterion 1 message methodTypes [ cancel
invite ack ]
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 criterion 2 type header
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 criterion 2 header
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 criterion 2 header name request-line
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 criterion 2 header numberOfInstances number
1
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 criterion 2 header numberOfInstances
qualifier equal
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 action 1 type token
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 action 1 operation regsub
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 action 1 from
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 action 1 from type value
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 action 1 from value trunk.sip.voice.google.
com
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 action 1 to
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 action 1 to type token
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 action 1 to tokenValue urihostname
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 action 1 regexp
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 action 1 regexp string siplink.telephony.
goog
set profiles signaling sipAdaptorProfile GOOGLE_Multitenant_ADP rule 4 action 1 regexp matchInstance one
commit

```

Zone

```
set addressContext default zone GOOGLE_Multitenant id 5
set addressContext default zone GOOGLE_Multitenant messageManipulation outputAdapterProfile SIP_OPTIONS
set addressContext default zone GOOGLE_Multitenant dnsGroup DNS
commit
```

SIP Signaling Port

```
set addressContext default zone GOOGLE_Multitenant sipSigPort 5 ipInterfaceGroupName LIF2 ipAddressV4 x.x.x.x
portNumber <tls_port2> transportProtocolsAllowed sip-tls-tcp
set addressContext default zone GOOGLE_Multitenant sipSigPort 5 tlsProfileName TLS_PROF_2
set addressContext default zone GOOGLE_Multitenant sipSigPort 5 tcpKeepaliveTime 100
set addressContext default zone GOOGLE_Multitenant sipSigPort 5 tcpKeepaliveInterval 60
set addressContext default zone GOOGLE_Multitenant sipSigPort 5 tcpKeepaliveProbes 2
set addressContext default zone GOOGLE_Multitenant sipSigPort 5 mode inService state enabled
commit
```

Trunk Group

```
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG media
mediaIpInterfaceGroupName LIF2
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG signaling timers
sessionKeepalive 1800
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG signaling timers
sessionMinSE 90
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG ingressIpPrefix x.x.x.x x
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG policy media
packetServiceProfile GOOGLE_Multitenant_PSP
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG policy signaling
ipSignalingProfile GOOGLE_Multitenant_IPSP
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG services natTraversal
tcpKeepaliveTimer 240
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG signaling
messageManipulation outputAdapterProfile GOOGLE_Multitenant_ADP
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG mode inService state enabled
commit
```

IP Peer

```
set addressContext default zone GOOGLE_Multitenant ipPeer GOOGLE_Multitenant_IPP policy description ""
set addressContext default zone GOOGLE_Multitenant ipPeer GOOGLE_Multitenant_IPP policy sip fqdn siplink.telephony.
goog
set addressContext default zone GOOGLE_Multitenant ipPeer GOOGLE_Multitenant_IPP policy sip fqdnPort 5671
set addressContext default zone GOOGLE_Multitenant ipPeer GOOGLE_Multitenant_IPP pathCheck profile GOOGLE
set addressContext default zone GOOGLE_Multitenant ipPeer GOOGLE_Multitenant_IPP pathCheck hostName siplink.
telephony.goog
set addressContext default zone GOOGLE_Multitenant ipPeer GOOGLE_Multitenant_IPP pathCheck hostPort 5671
set addressContext default zone GOOGLE_Multitenant ipPeer GOOGLE_Multitenant_IPP pathCheck state enabled
set addressContext default zone GOOGLE_Multitenant ipPeer GOOGLE_Multitenant_IPP pathCheck statusUpdateSupport
enabled
commit
```



Note

- For production, the Google Voice (GV) hostname is siplink.telephony.goog.
- GV listens on port 5672. Port 5671 is configured on Ribbon SBC Core as it adds 1 to the existing port for TLS.

Call Routing

Routing management allows you to manage all the configurations associated with routing calls based on the carriers' business requirements.

Routing Label

Routing label is associated with a route. Each route includes a gateway/trunk group pair. Routing labels provide the link between an entry in the Standard Route table and the set of routes associated with that Standard Route table entry.

```
set global callRouting routingLabel GOOGLE_RL routingLabelRoute 1 trunkGroup GOOGLE_TG ipPeer GOOGLE_IPP inService
inService
set global callRouting routingLabel PSTN_RL routingLabelRoute 1 trunkGroup PSTN_TG ipPeer PSTN_IPP inService
inService
set global callRouting routingLabel GOOGLE_Multitenant_RL routingLabelRoute 1 trunkGroup GOOGLE_Multitenant_TG
ipPeer GOOGLE_Multitenant_IPP inService inService
set global callRouting routingLabel PSTN_Multitenant_RL routingLabelRoute 1 trunkGroup PSTN_Multitenant_TG ipPeer
PSTN_Multitenant_IPP inService inService
commit
```

Route

Routing allows you send calls to the correct destination. You can use routing options based on your requirements. Configure the standard and specific routes (with usernames) to ensure that no matter how the called party is addressed (a number or username), the SBC routes the message to the Core. Create Route entries for standard Trunk Group routing with Matching Criteria and a Routing Label destination.

```
set global callRouting route trunkGroup GOOGLE_TG GOOGLEVOICE standard Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel PSTN_RL
set global callRouting route trunkGroup GOOGLE_TG GOOGLEVOICE username Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel PSTN_RL
set global callRouting route trunkGroup PSTN_TG GOOGLEVOICE standard Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel GOOGLE_RL
set global callRouting route trunkGroup PSTN_TG GOOGLEVOICE username Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel GOOGLE_RL
set global callRouting route trunkGroup GOOGLE_Multitenant_TG GOOGLEVOICE standard Sonus_NULL 1 all all ALL none
Sonus_NULL routingLabel PSTN_Multitenant_RL
set global callRouting route trunkGroup GOOGLE_Multitenant_TG GOOGLEVOICE username Sonus_NULL 1 all all ALL none
Sonus_NULL routingLabel PSTN_Multitenant_RL
set global callRouting route trunkGroup PSTN_Multitenant_TG GOOGLEVOICE standard Sonus_NULL 1 all all ALL none
Sonus_NULL routingLabel GOOGLE_Multitenant_RL
set global callRouting route trunkGroup PSTN_Multitenant_TG GOOGLEVOICE username Sonus_NULL 1 all all ALL none
Sonus_NULL routingLabel GOOGLE_Multitenant_RL
commit
```

Media Encryption

Customers can choose to encrypt the media using either DTLS or SDES-SRTP based on the requirement.



Warning

Configuring both DTLS and SDES-SRTP will result in call failure. Hence, customers are advised to use only one method of Media encryption.

DTLS

The Datagram Transport Layer Security (DTLS) protocol provides authentication, data integrity, and confidentiality for communications between two applications over an Unreliable Datagram Protocol (UDP). The Secure Real-time Transport Protocol (SRTP) provides encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications. DTLS-SRTP is an extension to the DTLS protocol, where DTLS acts as the key management protocol. DTLS protocol is also extended to negotiate the SRTP crypto suites and parameters for use with those keys.

WebRTC is a signaling protocol defined for real-time communication between Web browsers. WebRTC has assigned DTLS-SRTP protocol for the media exchange between the browsers. The SBC includes the following DTLS functionality:

- Real-time communication between the web browsers by using DTLS-SRTP while interworking with SIP networks.
- DTLS on the media path for key management for the SRTP-based media.
- The self-signed certificates to secure and authenticate DTLS associations. DTLS connections are secured by the two browsers sharing self-signed certificates as part of the media connection during a DTLS handshake between the browsers. The certificates are authenticated by checking a fingerprint, which is passed in the signaling path as part of the Session Description Protocol (SDP).

The SBC includes DTLS crypto suites that define a set of ciphers (algorithms used for encrypting data) which allow the selection of an appropriate level of security. When a TLS connection is established, the client and server exchange information about which cipher suites they have in common.

DTLS Profile

This object specifies the parameters associated with DTLS Flags. These are supporting parameters for DTLS objects.

```
set profiles security dtlsProfile byotDTLS handshakeTimer 5
set profiles security dtlsProfile byotDTLS sessionResumpTimer 300
set profiles security dtlsProfile byotDTLS cipherSuite1 rsa-with-aes-128-cbc-sha
set profiles security dtlsProfile byotDTLS cipherSuite2 nosuite
set profiles security dtlsProfile byotDTLS cipherSuite3 nosuite
set profiles security dtlsProfile byotDTLS dtlsRole client
set profiles security dtlsProfile byotDTLS hashType sha256
set profiles security dtlsProfile byotDTLS CertName defaultDtlsSBCCert
set profiles security dtlsProfile byotDTLS cookieExchange enabled
set profiles security dtlsProfile byotDTLS v1_0 enabled
set profiles security dtlsProfile byotDTLS v1_1 enabled
set profiles security dtlsProfile byotDTLS v1_2 enabled
commit
```

DTLS Configuration for Tenant-1

Packet Service Profile

Disable SRTP.

```
set profiles media packetServiceProfile GOOGLE_PSP secureRtpRtcp flags enableSrtp disable
commit
```

Enable the flag for DTLS.

```
set profiles media packetServiceProfile GOOGLE_PSP dtls dtlsCryptoSuiteProfile DEFAULT
set profiles media packetServiceProfile GOOGLE_PSP dtls dtlsFlags allowDtlsFallback disable
set profiles media packetServiceProfile GOOGLE_PSP dtls dtlsFlags enableDtlsSrtp enable
set profiles media packetServiceProfile GOOGLE_PSP dtls dtlsFlags dtlsSrtpRelay disable
set profiles media packetServiceProfile GOOGLE_PSP dtls dtlsFlags dtlsSctpRelay disable
commit
```

Trunk Group

Associate the DTLS profile to the Trunk Group.

```
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG state disabled
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG media dtlsProfileName byotDTLS
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG state enabled
commit
```

DTLS configuration for Tenant-2

Packet Service Profile

Disable SRTP.

```
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP secureRtpRtcp flags enableSrtp disable
commit
```

Enable the flag for DTLS.

```
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP dtls dtlsCryptoSuiteProfile DEFAULT
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP dtls dtlsFlags allowDtlsFallback disable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP dtls dtlsFlags enableDtlsSrtp enable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP dtls dtlsFlags dtlsSrtpRelay disable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP dtls dtlsFlags dtlsSctpRelay disable
commit
```

Trunk Group

Associate the DTLS profile to the Trunk Group.

```
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG state disabled
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG media dtlsProfileName
byotDTLS
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG state enabled
commit
```

SDES-SRTP

SRTP is an IETF cryptographic protocol that provides secure communications over untrusted networks as described in RFC 3711. SRTP provides confidentiality, message authentication and replay protection to Internet media traffic such as audio and video. The SBC Core supports Secure RTP and its associated secure real-time transport control protocol (Secure RTCP) for IPv4/IPv6 addressing for both audio and video streams.

SDES-SRTP Configuration for Tenant-1

Trunk Group

Remove the DTLS profile from the Trunk Group.

```
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG state disabled
delete addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG media dtlsProfileName byotDTLS
set addressContext default zone GOOGLE sipTrunkGroup GOOGLE_TG state enabled
commit
```

Packet Service Profile

Enable SRTP.

```
set profiles media packetServiceProfile GOOGLE_PSP dtls dtlsFlags enableDtlsSrtp disable
set profiles media packetServiceProfile GOOGLE_PSP secureRtpRtcp flags enableSrtp enable
commit
```

SDES-SRTP Configuration for Tenant-2

Trunk Group

Remove the DTLS profile from the Trunk Group.

```
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG state disabled
delete addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG media dtlsProfileName
byotDTLS
set addressContext default zone GOOGLE_Multitenant sipTrunkGroup GOOGLE_Multitenant_TG state enabled
commit
```

Packet Service Profile

Enable SRTP.

```
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP dtls dtlsFlags enableDtlsSrtp disable
set profiles media packetServiceProfile GOOGLE_Multitenant_PSP secureRtpRtcp flags enableSrtp enable
commit
```

Ribbon SBC Core High Availability



Info

During this interop, SBC SWe was configured in HA mode with the configuration below for High Availability.

In an HA configuration, the two SBC VMs are connected to each other using the HA ports on the respective VMs. The HA logical ports must be in the same network and routable using the switch and they must be connected to a switch. Failure of the connection is via link detection and also TIPC keep-alives.

HA Configuration

Link Detection Group:

The Link Detection Group allows you to group interfaces and associated Link Monitors together and track link verification failures within the group. A Link Detection Group (LDG) is configured with a unique name and a failover threshold. The LDG tracks the number of link verification failures that have occurred among the Link Monitors configured.

Create Link Detection Groups for both pkt0 and pkt1 interfaces.

```
set addressContext default linkDetectionGroup PKT0_ACT_LDG ceName GOOGLEACTIVE
set addressContext default linkDetectionGroup PKT0_ACT_LDG type ip
set addressContext default linkDetectionGroup PKT0_ACT_LDG threshold 1
set addressContext default linkDetectionGroup PKT0_ACT_LDG state enabled
set addressContext default linkDetectionGroup PKT0_ACT_LDG linkMonitor PKT0_ACT_LM interfaceGroup LIF1
set addressContext default linkDetectionGroup PKT0_ACT_LDG linkMonitor PKT0_ACT_LM interface PKT0
set addressContext default linkDetectionGroup PKT0_ACT_LDG linkMonitor PKT0_ACT_LM destination
<pkt0_default_gateway>
set addressContext default linkDetectionGroup PKT0_ACT_LDG linkMonitor PKT0_ACT_LM state enabled
set addressContext default linkDetectionGroup PKT0_STB_LDG ceName GOOGLESTANDBY
set addressContext default linkDetectionGroup PKT0_STB_LDG type ip
set addressContext default linkDetectionGroup PKT0_STB_LDG threshold 1
set addressContext default linkDetectionGroup PKT0_STB_LDG state enabled
set addressContext default linkDetectionGroup PKT0_STB_LDG linkMonitor PKT0_STB_LM interfaceGroup LIF1
set addressContext default linkDetectionGroup PKT0_STB_LDG linkMonitor PKT0_STB_LM interface PKT0
set addressContext default linkDetectionGroup PKT0_STB_LDG linkMonitor PKT0_STB_LM destination
<pkt0_default_gateway>
set addressContext default linkDetectionGroup PKT0_STB_LDG linkMonitor PKT0_STB_LM state enabled
set addressContext default linkDetectionGroup PKT1_ACT_LDG ceName GOOGLEACTIVE
set addressContext default linkDetectionGroup PKT1_ACT_LDG type ip
set addressContext default linkDetectionGroup PKT1_ACT_LDG threshold 1
set addressContext default linkDetectionGroup PKT1_ACT_LDG state enabled
set addressContext default linkDetectionGroup PKT1_ACT_LDG linkMonitor PKT1_ACT_LM interfaceGroup LIF2
set addressContext default linkDetectionGroup PKT1_ACT_LDG linkMonitor PKT1_ACT_LM interface PKT1
set addressContext default linkDetectionGroup PKT1_ACT_LDG linkMonitor PKT1_ACT_LM destination
<pkt1_default_gateway>
set addressContext default linkDetectionGroup PKT1_ACT_LDG linkMonitor PKT1_ACT_LM state enabled
set addressContext default linkDetectionGroup PKT1_STB_LDG ceName GOOGLESTANDBY
set addressContext default linkDetectionGroup PKT1_STB_LDG type ip
set addressContext default linkDetectionGroup PKT1_STB_LDG threshold 1
set addressContext default linkDetectionGroup PKT1_STB_LDG state enabled
set addressContext default linkDetectionGroup PKT1_STB_LDG linkMonitor PKT1_STB_LM interfaceGroup LIF2
set addressContext default linkDetectionGroup PKT1_STB_LDG linkMonitor PKT1_STB_LM interface PKT1
set addressContext default linkDetectionGroup PKT1_STB_LDG linkMonitor PKT1_STB_LM destination
<pkt1_default_gateway>
set addressContext default linkDetectionGroup PKT1_STB_LDG linkMonitor PKT1_STB_LM state enabled
commit
```

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	Basic Call Setup & Termination	✓
2	Call Transfer (Attended/ Consultative/ Warm)	✓
3	Call Transfer (Unattended/ Blind/ Cold)	✓

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.

- Attended call transfer is not supported on Google Voice Web and Android clients.

This issue will be addressed by GV 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 Ribbon SBC Core interop involving Google Voice SIP Link for Multitenancy.

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.

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved.