Oracle SBC with Google Voice Sip Link

Technical Application Note

ORACLE
COMMUNICATIONS

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Contents

This Page is left Intentionally Blank

1 Revision History

Document Version	Description	Revision Date
1.0	• Initial Release	06/22/2022
1.1	• Added hardware and licensing requirements for TLS/SRTP	02/14/2023
1.2	• Added direct links for GTSR1 and GlobaSign Root CA	03/07/2023
1.3	• Retested the solution with SBC 9.2.0 (SCZ920) version	08/25/2023

2 Intended Audience

This document describes how to connect the Oracle SBC to Google Voice Sip Link. This paper is intended for IT or telephony professionals.

Note: To zoom in on screenshots of Web GUI configuration examples, press Ctrl and +.

3 Validated Oracle Software Versions

All testing was successfully conducted with the Oracle Communications SBC versions:

SCZ900, SCZ920

These software releases with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 3950 (Release SCZ9.x.x Only)
- AP 4600
- AP 4900 (Release SCZ9.x.x Only)
- AP 6350
- AP 6300
- VME
- Public Clouds (OCI, AWS, Azure)

Please visit https://support.google.com for further information

4 Related Documentation

4.1 Oracle SBC

- Oracle® Enterprise Session Border Controller Web GUI User Guide
- Oracle® Enterprise Session Border Controller ACLI Reference Guide
- Oracle® Enterprise Session Border Controller Release Notes

- Oracle® Enterprise Session Border Controller Configuration Guide
- Oracle® Enterprise Session Border Controller Security Guide

4.2 Google Voice Sip Link

- Google Voice SIP Link

5 About Google Voice SIP Link

With Google Voice SIP Link, you can connect your existing carrier to Google through a set of certified Session Border Controllers (SBC). This flexibility allows you to use your existing telecommunication infrastructure and maintain uninterrupted service with your current carrier.

5.1 Infrastructure Requirements

Session Border Controller (SBC)	**See Check Voice SIP Link Requirements for More Details**
SIP Trunks connected to the SBC	
Google Voice SIP Link	
Public IP address for the SBC	
Public trusted certificate for the SBC	
Firewall ports for SIP Link signaling	
Firewall IP addresses and ports for SIP Link media	
Media Transport Profile	
Firewall ports for client media	

5.2 SBC Domain Name

In this application note, we are using the following FQDN that is registered in our Google Admin account to pair the Oracle SBC to Google Voice SIP Link. Since our SBC is deployed behind NAT, we will only be displaying the private IP addresses configured on the SBC.

Public IP Address	FQDN Name
<Public IP of SBC or NAT>	solutionslab.cgbuburlington.com

6 Configuring Google Voice SIP Link

For detailed step-by-step guidance on setting up Google Voice SIP Link, go to:

support.google.com/a?p=siplink.

Before you begin configuring SIP Link you will need to do the following:

- Verify Google Voice has been enabled on your Corporate Google account.
- Make sure you log in using Google Workspace admin credentials.

For more information, please reach out to your local Google representative.

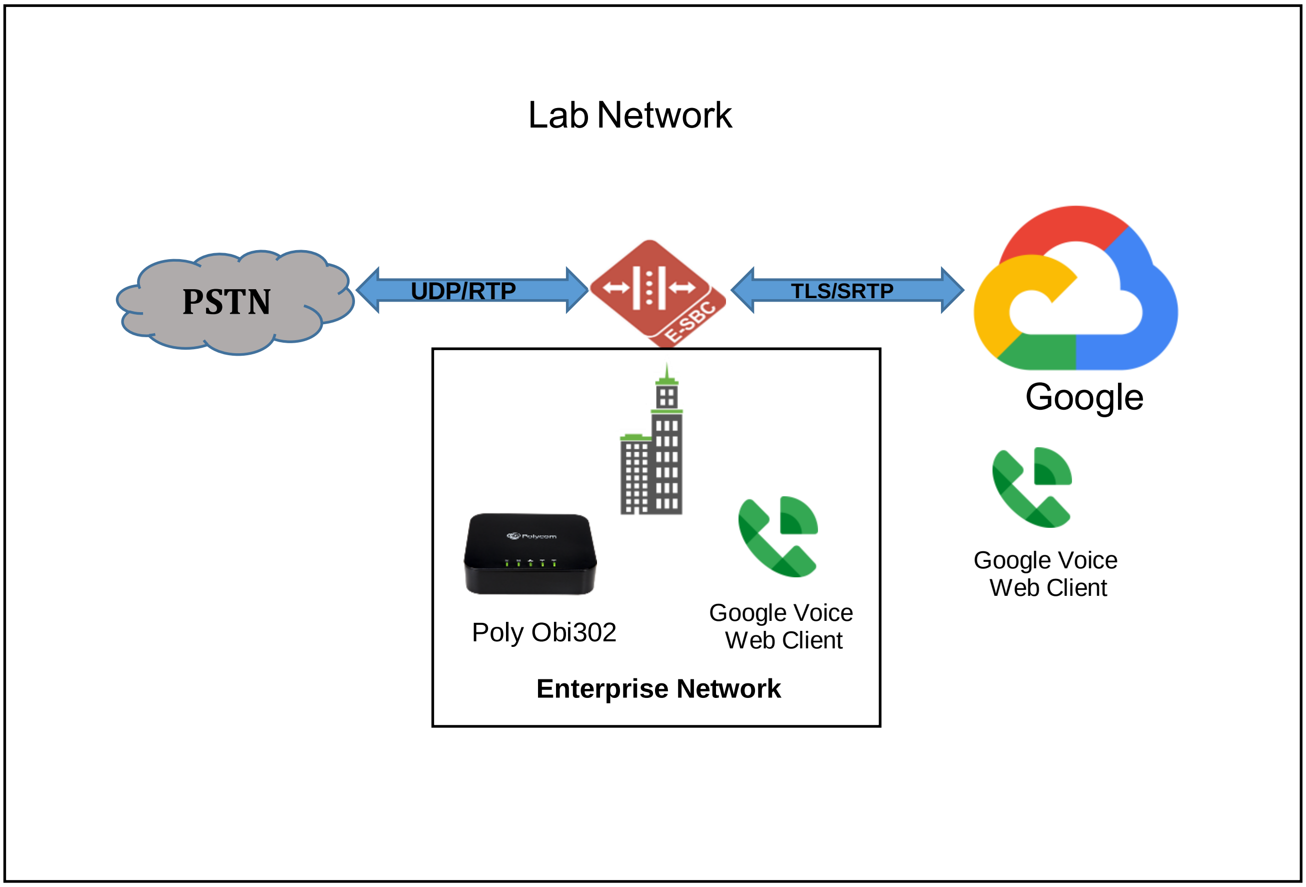
7 Oracle SBC Configuration

This chapter provides step-by-step guidance on how to configure Oracle SBC for interworking with Google Voice SIP Link.

Please follow the steps in this chapter to successfully configure the Oracle SBC.

There are multiple connections shown:

- Google SIP Link is on the WAN
- Service provider Sip trunk terminating on the SBC
- Google Voice Web Client both on prem and remote
- Poly OBI302 ATA on prem registering to Google Cloud



There are two methods for configuing the OCSBC, ACLI, or GUI.

For the purposes of this note, we'll be using the OCSBC GUI for all configuration examples. We will however provide the ACLI path to each element.

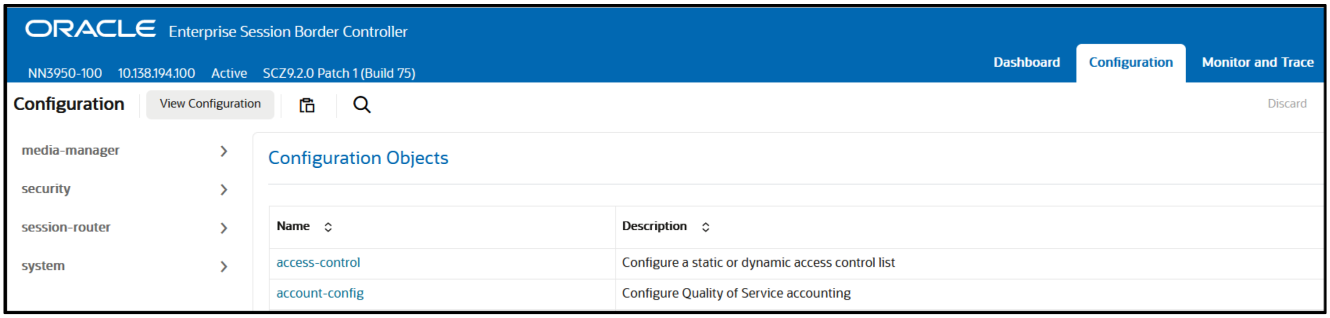
This guide assumes the OCSBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, http-server has been enabled for GUI access. If you require more information on how to install your SBC platform, please refer to the ACLI configuration guide.

To access the OCSBC GUI, enter the management IP address into a web brower.
When the login screen appears, enter the username and password to access the OCSBC.

Once you have access to the OCSBC GUI, at the top, click the Configuration Tab. This will bring up the OCSBC Configuration Objects List on the left hand side of the screen.

Any configuration parameter not specifically listed below can remain at the OCSBC default value and does not require a change for the connection to Google Voice SIP Link to function properly.

Note: the configuration examples below were captured from a system running the latest GA software, 9.2.0



Configuration Objects

Name	Description
access-control	Configure a static or dynamic access control list
account-config	Configure Quality of Service accounting

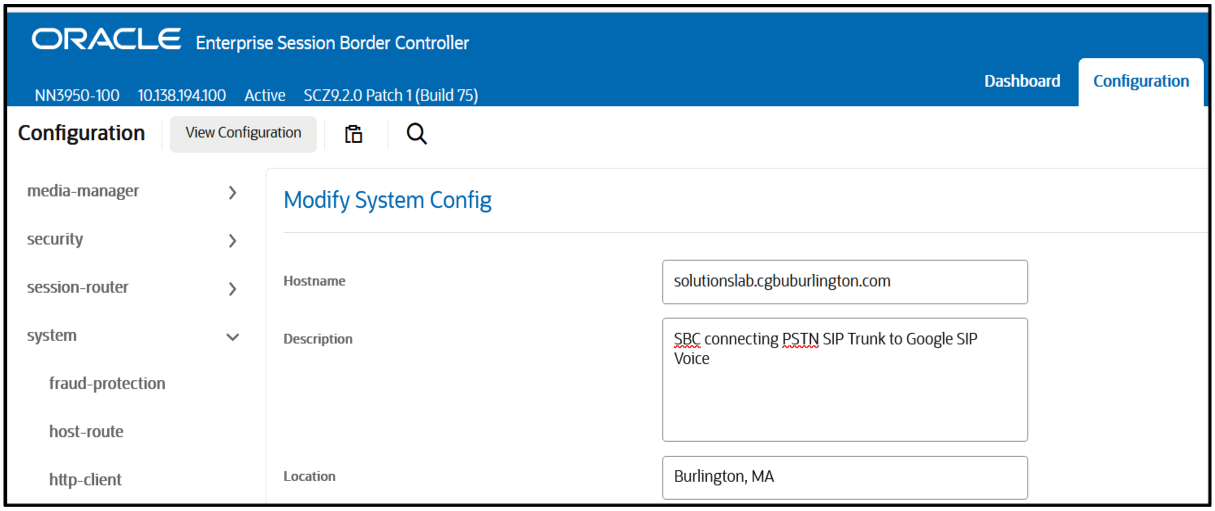
7.1 System-Config

To enable system level functionality for the OCSBC, you must first enable the system-config
.
GUI Path: system/system-config

ACLI Path: config t→system→system-config

Note: The following parameters are optional but recommended for system config

- Hostname
- Description
- Location
- Default Gateway (recommended to be the same as management interface gateway)
- Transcoding Core (This field is only required if you have deployed a VME SBC and plan to transcode media)



Modify System Config

Hostname: solutionslab.cgbuburlington.com

Description: SBC connecting PSTN SIP Trunk to Google SIP Voice

Location: Burlington, MA

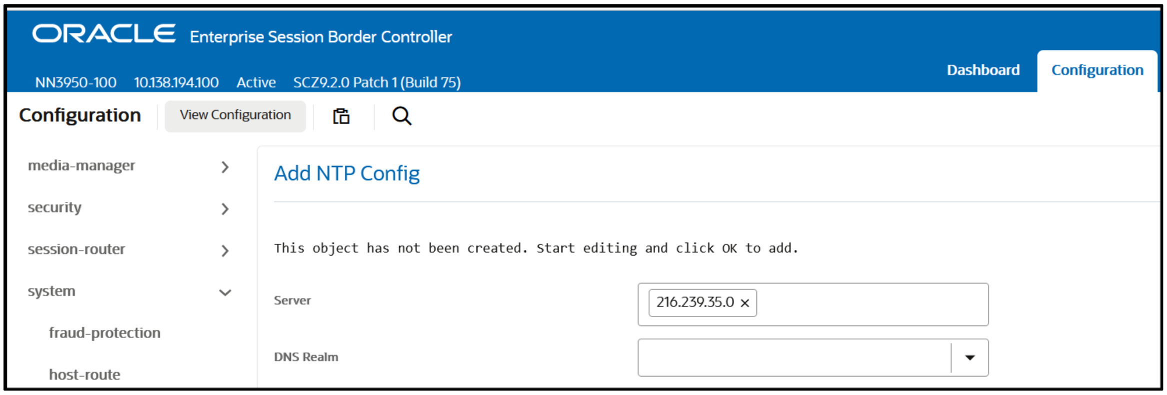
- Click OK at the bottom

7.1.1 NTP-Sync

You can use the following example to connect the Oracle SBC to any network time servers you have in your network. This is an optional configuration but recommended.

GUI Path: system/ntp-config

ACLI Path: config t→system→ntp-sync



Add NTP Config

This object has not been created. Start editing and click OK to add.

Server: 216.239.35.0 ×

DNS Realm:

- Select OK at the bottom

Now we'll move on configuring network connection on the SBC.

7.2 Network Configuration

To connect the SBC to network elements, we must configure both physical and network interfaces. For the purposes of this example, we will configure two physical interfaces, and two network interfaces. One to communicate with Google Voice SIP Link, the other to connect to PSTN Network. The slots and ports used in this example may be different from your network setup.

7.2.1 Physical Interfaces

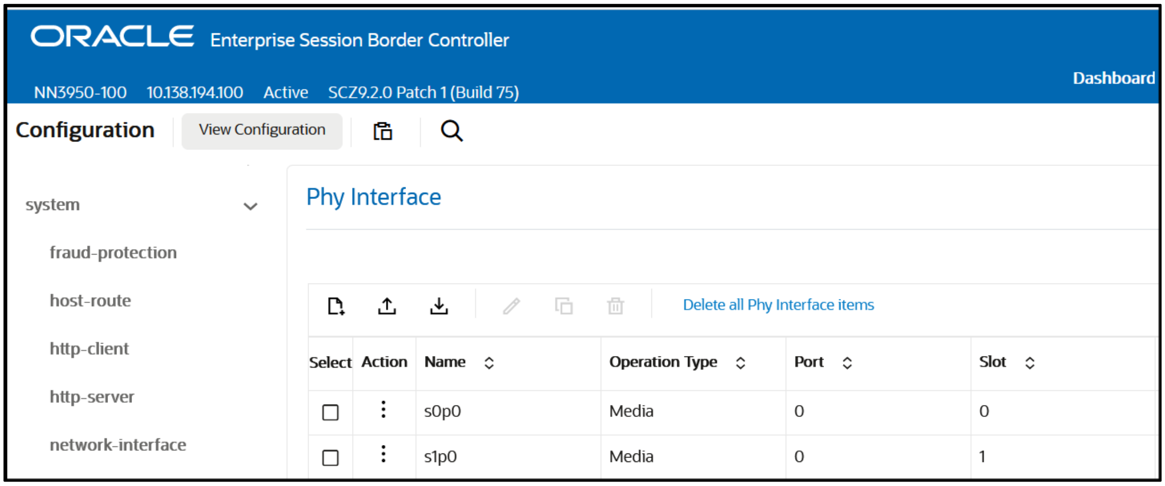
GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

- Click Add, use the following table as a configuration example:

Config Parameter	PSTN	Google
Name	s0p0	S1p0
Operation Type	Media	Media
Slot	0	1
Port	0	0

Note: Physical interface names, slot and port may vary depending on environment


ORACLE Enterprise Session Border Controller
NN3950-100 10.138.194.100 Active SCZ9.2.0 Patch 1 (Build 75)
Dashboard
Configuration
View Configuration
system
fraud-protection
host-route
http-client
http-server
network-interface
Phy Interface
Delete all Phy Interface items

Select	Action	Name	Operation Type	Port	Slot
□	⋮	s0p0	Media	0	0
□	⋮	s1p0	Media	0	1

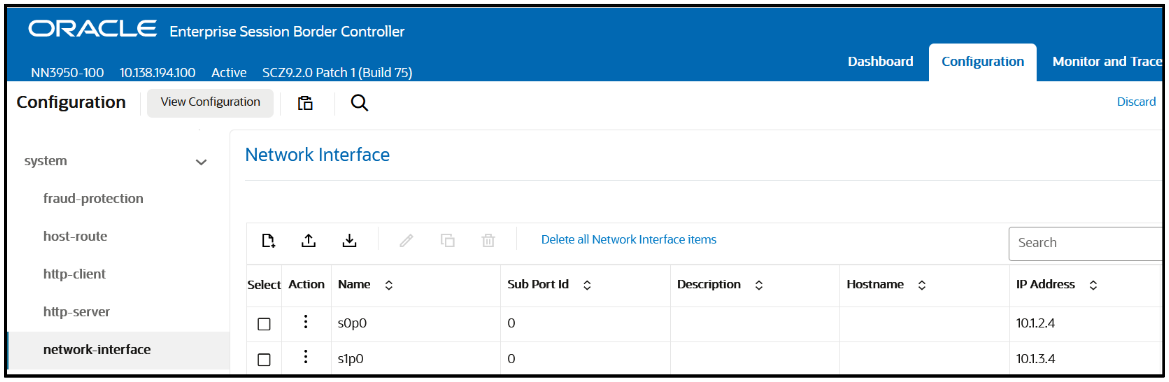
7.2.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

- Click Add, use the following table as a configuration example:

Configuration Parameter	GoogleVoice	PSTN
Name	s1p0	s0p0
IP Address	10.1.3.4	10.1.2.4
Netmask	255.255.255.0	255.255.255.0
Gateway	10.1.3.1	10.1.2.1
DNS Primary IP	8.8.8.8	
DNS Domain	Solutionslab.cgbuburlington.com	



Select	Action	Name	Sub Port Id	Description	Hostname	IP Address
□	⋮	s0p0	0			10.1.2.4
□	⋮	s1p0	0			10.1.3.4

- Click OK at the bottom of each after entering config information

Next, we’ll configure the necessary elements to secure signaling and media traffic between the Oracle SBC and Google Voice SIP Link.

7.3 Security Configuration

7.3.1 Hardware Requirements

The Acme Packet platforms and VNF all support SRTP.

SSM is required for TLS on Acme Packet 4600, 6100, 6300, and 6350. SSM is not required for TLS on Acme Packet 1100, 3900, 3950, 4900, and VME/VNF. TLS is used for encrypting signaling, and SRTP is used for encrypting media. In this case, then the SSM module is also required to run TLS.

```
# show security ssm
```

SSM (Security Service Module) v3 present.

7.3.2 Encryption for Virtual SBC

You must enable encryption for virtualized deployments with a license key. The following table lists which licenses are required for various encryption use cases.

Feature	License Key
IPSec Trunking	IPSEC
SRTP Sessions	SRTP
Transport Layer Security Sessions	TLS
MSRP	TLS

Note: The TLS license is only required for media and signaling. TLS for secure access, such as SSH, HTTPS, and SFTP is available without installing the TLS license key.

To enable the preceding features, you install a license key at the **system, license** configuration element. Request license keys at the License Codes website at

http:// www.oracle.com/us/support/licensecodes/acme-packet/index.html.

After you install the license keys, you must reboot the system to see them.

This section describes how to configure the SBC for both TLS and SRTP communication with Google Voice SIP Link.

Google Voice SIP Link only allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by a supported Certificate Authority (CA).

Voice SIP Link accepts TLS certificates from the following Certificate Authorities (CAs):

- DigiCert
- Entrust DataCard
- GlobalSign
- GoDaddy
- Sectigo

7.3.3 Certificate Records

"Certificate-records" are configuration elements on Oracle SBC which capture information for a TLS certificate such as common-name, key-size, key-usage etc.

This section walks you through how to configure certificate records, create a certificate signing request, and import the necessary certificates into the SBC's configuration.

GUI Path: security/certificate-record

ACLI Path: config t→security→certificate-record

For the purposes of this application note, we'll create three certificate records. They are as follows:

- SBC Certificate (end-entity certificate)
- DigiCert RootCA Cert (Root CA used to sign the SBC's end entity certificate)
- Google GTS Root R1 (GTSR1) (Google Presents the SBC a certficate signed by this authority)

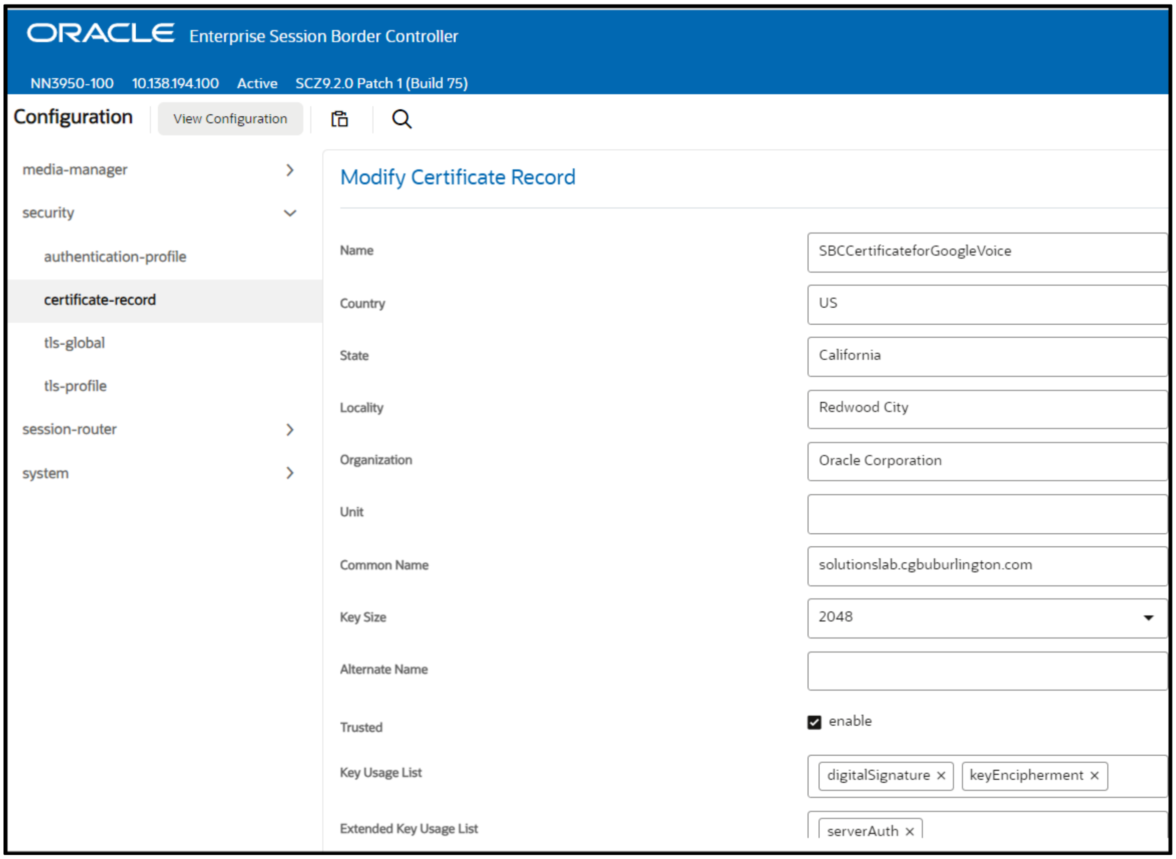
Note: The DigiCert RootCA is only part of this example, and is the Authority we used to sign our SBC certificate. You would replace this with the root and/or intermediate certificates used to sign the CSR generated from your SBC.

7.3.3.1 SBC End Entity Certificate

The SBC's end entity certificate is the certificate the SBC presents to Google to secure the connection. The only requirements when configuring this certificate is the common name must contain the SBC's FQDN. In this example our common name will be **solutionslab.cgbuburlington.com.** You must also give it a name. All other fields are optional, and can remain at default values.

To Configure the certificate record:

Click Add, and use the following example to configure the SBC certificate



Modify Certificate Record

Name	SBCCertificateforGoogleVoice
Country	US
State	California
Locality	Redwood City
Organization	Oracle Corporation
Unit	
Common Name	solutionslab.cgbuburlington.com
Key Size	2048
Alternate Name	
Trusted	☑ enable
Key Usage List	digitalSignature × keyEncipherment ×
Extended Key Usage List	serverAuth ×

- Click OK at the bottom

Next, using this same procedure, configure certificate records for the Root CA certificates

7.3.3.2 Root CA and Intermediate Certificates

7.3.3.2.1 DigiCert Root CA

The following, DigitCertRoot, is the root CA certificate used to sign the SBC's end entity certificate. As mentioned above, your root CA and/or intermediate certificate may differ. This is for example purposes only.

7.3.3.2.2 Google GTS Root 1 (GTSR1)

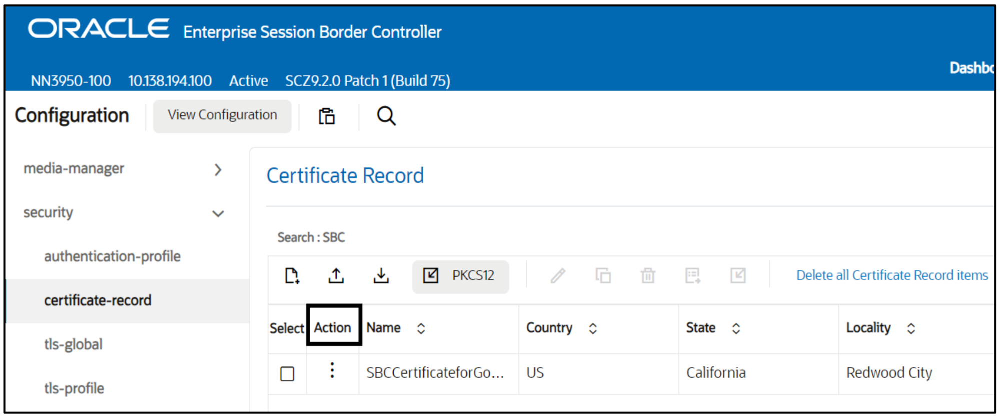
Google presents a certificate to the SBC which is signed by Google GTS Root 1. The TLS certificate and the trust chain from either of the public CAs must be added to the TLS profile of the SBC along with the Google Root certificate.

You can download the GTSR1 trusted root certificate here: https://pki.goog/repo/certs/gtsr1.pem

You can access the GlobalSign trusted root certificate here: GlobalSignRootCA

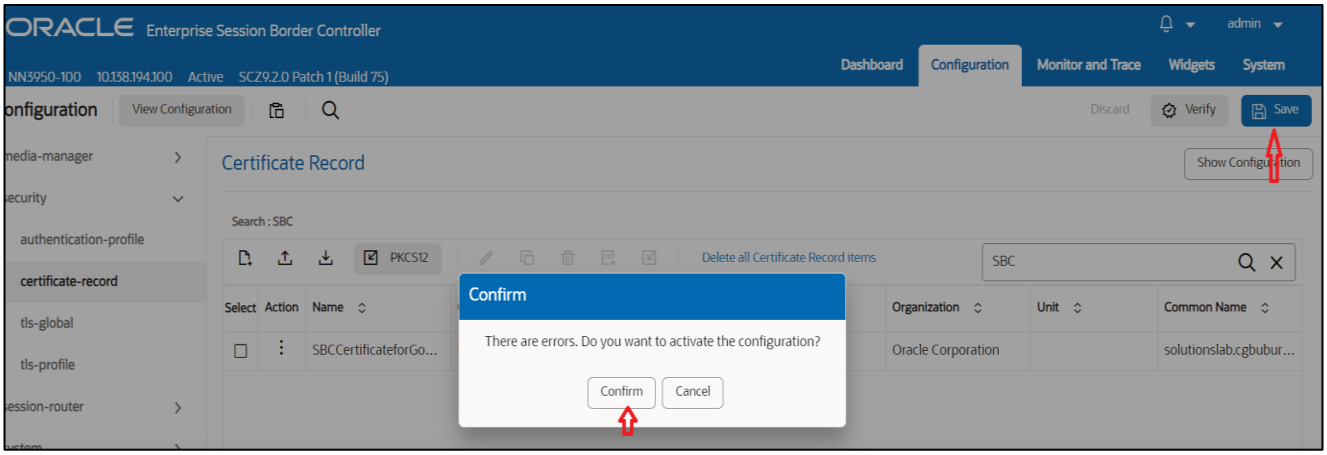
Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

Config Parameter	GTSR1	Global Sign Root CA	DigiCert Root CA
Common Name	GTS Root R1	GlobalSign Root	DigiCert Global Root CA
Key Size	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256



Select	Action	Name	Country	State	Locality
☐	⋮	SBCCertificateforGo...	US	California	Redwood City

At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must **save and activate** the configuration of the SBC.



Confirm

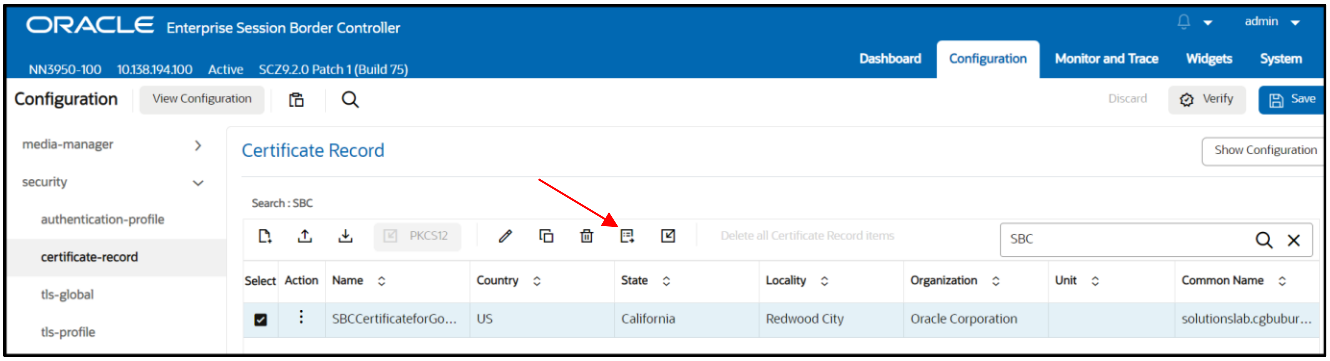
There are errors. Do you want to activate the configuration?

Select	Action	Name	Organization	Unit	Common Name
☐	⋮	SBCCertificateforGo...	Oracle Corporation		solutionslab.cgbubur...

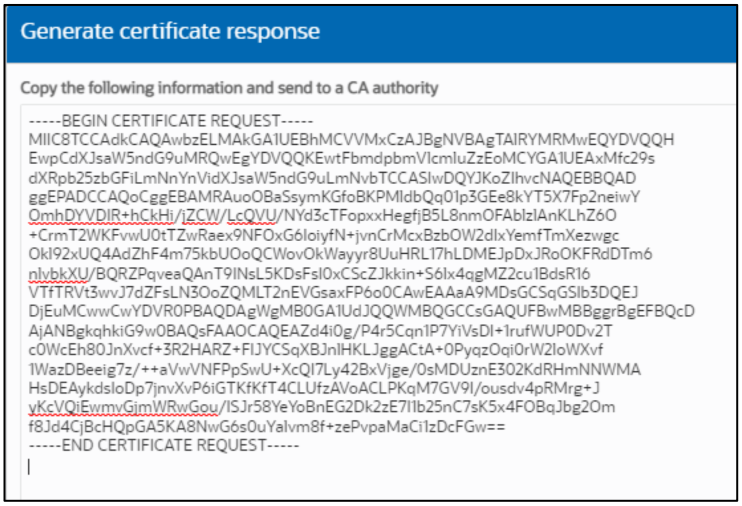
7.3.3.3 Generate Certificate Signing Request

Now that the SBC's certificate has been configured, create a certificate signing request for the SBC's end entity only. **This is not required for any of the Root CA or intermidiate certificates that have been created**.

On the certificate record page in the Oracle SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:



Select	Action	Name	Country	State	Locality	Organization	Unit	Common Name
☑	⋮	SBCCertificateforGo...	US	California	Redwood City	Oracle Corporation		solutionslab.cgbubur...


Generate certificate response

Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwbzELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAlRYMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEoMCYGA1UEAxMfc29s
dXRpb25zbGFiLmNnYnVidXJsaW5ndG9uLmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMRAuoOBaSsymKGfoBKPMIdbQq01p3GEe8kYT5X7Fp2neiwY
OmhDYVDIR+hCkHi/jZCW/LcQVU/NYd3cTFopxxHegfjB5L8nmOFAblzlAnKLhZ6O
+CrmT2WKFvwU0tTZwRaex9NFOxG6loiyfN+jvnCrMcxBzbOW2dlxYemfTmXezwgc
OkI92xUQ4AdZhF4m75kbUOoQCWovOkWayyr8UuHRL17hLDMEJpDxJRoOKFRdDTm6
nIvbkXU/BQRZPqveaQAnT9INsL5KDsFsI0xCScZJkkin+S6Ix4qgMZ2cu1BdsR16
VTfTRVt3wvJ7dZFsLN3OoZQMLT2nEVGsaxFP6o0CAwEAAaA9MDsGCSqGSIb3DQEJ
DjEuMCwwCwYDVR0PBAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcD
AjANBgkqhkiG9w0BAQsFAAOCAQEAZd4i0g/P4r5Cqn1P7YiVsDI+1rufWUP0Dv2T
c0WcEh80JnXvcf+3R2HARZ+FIJYCSqXBJnIHKLJggACtA+0PyqzOqi0rW2loWXvf
1WazDBeeig7z/++aVwVNFPpSwU+XcQI7Ly42BxVjge/0sMDUznE302KdRHmNNWMA
HsDEAykdsloDp7jnvXvP6iGTKfKfT4CLUfzAVoACLPKqM7GV9I/ousdv4pRMrg+J
yKcVQiEwmvGjmWRwGou/ISJr58YeYoBnEG2Dk2zE7I1b25nC7sK5x4FOBqJbg2Om
f8Jd4CjBcHQpGA5KA8NwG6s0uYaIvm8f+zePvpaMaCi1zDcFGw==
-----END CERTIFICATE REQUEST-----
```

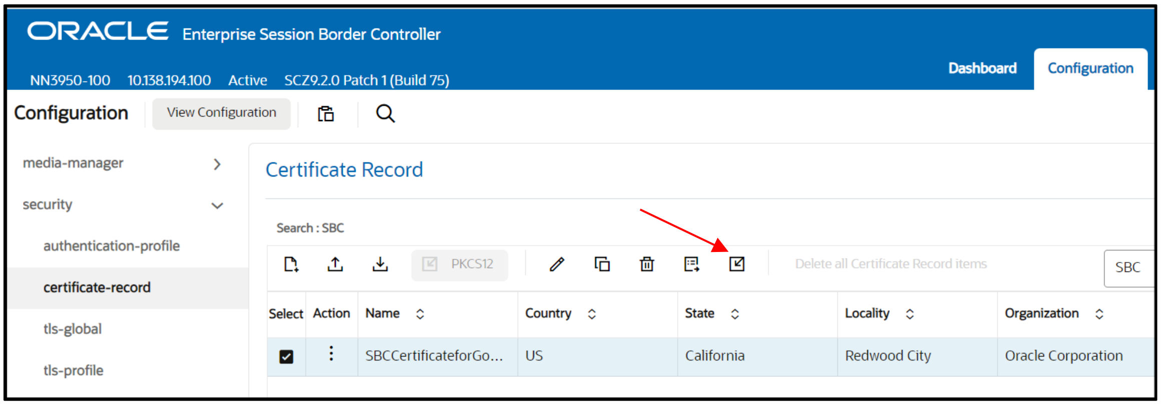
Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, at this point, **another save and activate is required** before you can import the certificates to each certificate record created above.

Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

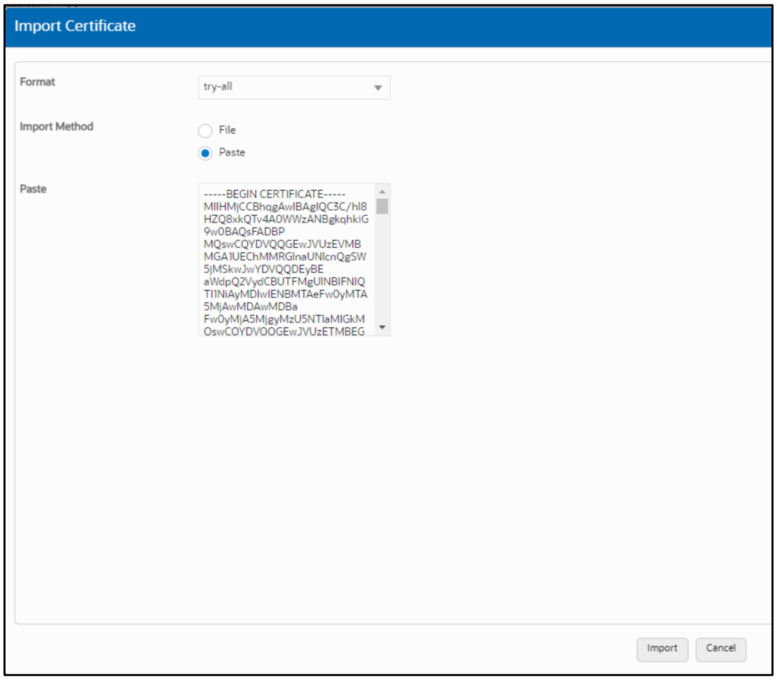
7.3.3.4 Import Certificates to SBC

Now that the certificate signing request has been completed – import the signed certificate to the SBC.

Please note – all certificates including root and intermediate certificates are required to be imported to the SBC. Once all certificates have been imported, issue a third **save/activate** from the WebGUI to complete the configuration of certificates on the Oracle SBC.



Select	Action	Name	Country	State	Locality	Organization
☑	⋮	SBCCertificateforGo...	US	California	Redwood City	Oracle Corporation



Format: try-all

Import Method: ○ File ● Paste

Paste:

```
-----BEGIN CERTIFICATE-----
MIIHMjCCBhqgAwIBAgIQC3C/hl8
HZQ8xkQTv4A0WWzANBgkqhkiG
9w0BAQsFADBP
MQswCQYDVQQGEwJVUzEVMB
MGA1UEChMMRGlnaUNlcnQgSW
5jMSkwJwYDVQQDEyBE
aWdpQ2VydCBUTFMgUlNBIFNIQ
TI1NiAyMDIwIENBMTAeFw0yMTA
5MjAwMDAwMDBa
Fw0yMjA5MjgyMzU5NTlaMIGkM
OswCOYDVOOGEwJVUzETMBEG
```

- After pasting in the text box, select Import at the bottom, then **save and activate** your configuration.

Repeat these steps to import all the root and intermediate CA certificates into the SBC:

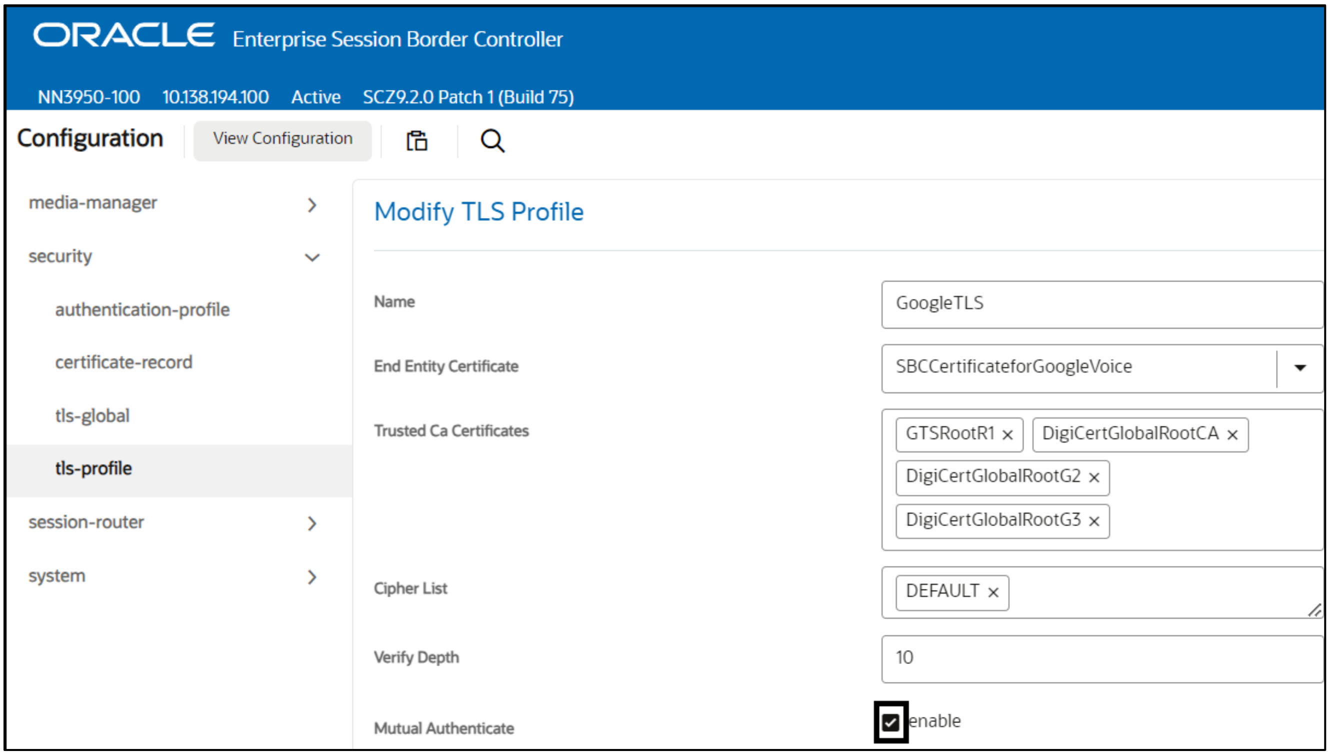
7.3.4 TLS Profile

TLS profile configuration on the SBC allows for specific certificates to be assigned.

GUI Path: security/tls-profile

ACLI Path: config t→security→tls-profile

- Click Add, use the example below to configure



Modify TLS Profile

Name: GoogleTLS

End Entity Certificate: SBCCertificateforGoogleVoice

Trusted Ca Certificates: GTSRootR1 × DigiCertGlobalRootCA × DigiCertGlobalRootG2 × DigiCertGlobalRootG3 ×

Cipher List: DEFAULT ×

Verify Depth: 10

Mutual Authenticate: ☑ enable

- Select OK at the bottom

Next, we'll move to securing media between the SBC and SIP Link.

7.3.5 Media Security

This section outlines how to configure support for media security between the OCSBC and Google Voice SIP Link.

7.3.5.1 SDES-Profile

This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured.

The Oracle SBC and Google Voice supports the following crypto's to secure media:

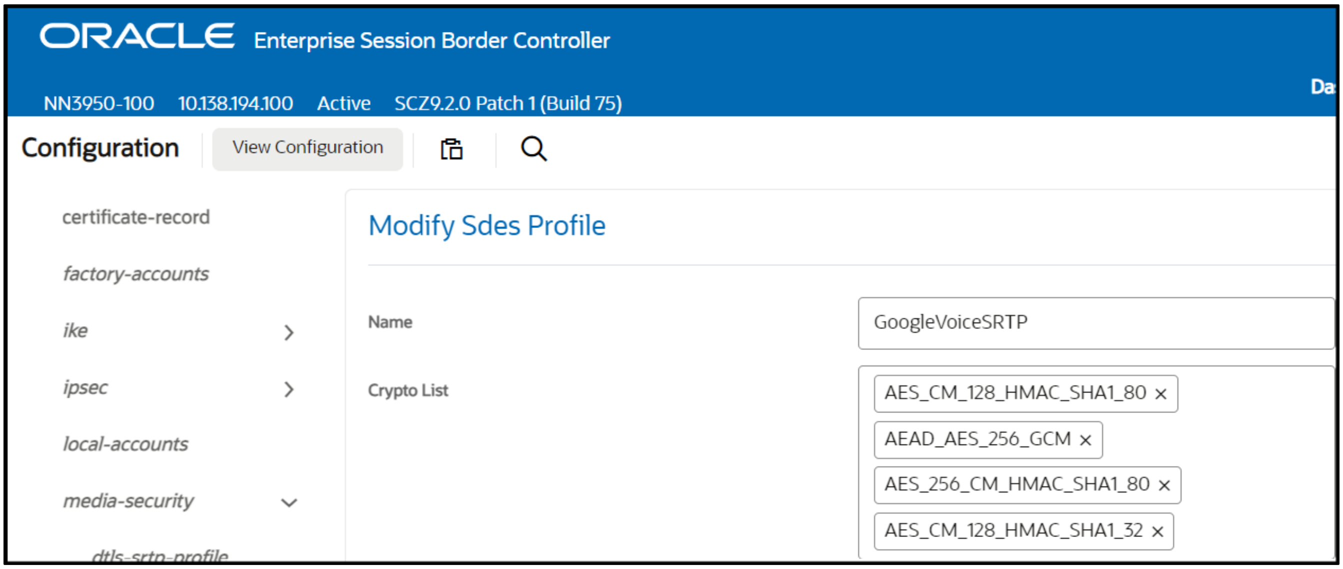
- AEAD_AES_256_GCM
- AES_256_CM_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

In the SBC's GUI, on the bottom left, you will need to enable the switch "Show All" to access the media security configuration elements.

GUI Path: security/media-security/sdes-profile

ACLI Path: config t→security→media-security→sdes-profile

- Click Add, and use the example below to configure



Modify Sdes Profile

Name: GoogleVoiceSRTP

Crypto List: AES_CM_128_HMAC_SHA1_80 ×, AEAD_AES_256_GCM ×, AES_256_CM_HMAC_SHA1_80 ×, AES_CM_128_HMAC_SHA1_32 ×

The screenshot above contains all supported crypto's for the Oracle SBC and Google Voice. This is only an example. It is not a requirement for all four to be added to the crypto list. You can choose all or any to best support your environment.

- Select OK at the bottom

7.3.5.2 Media Security Policy

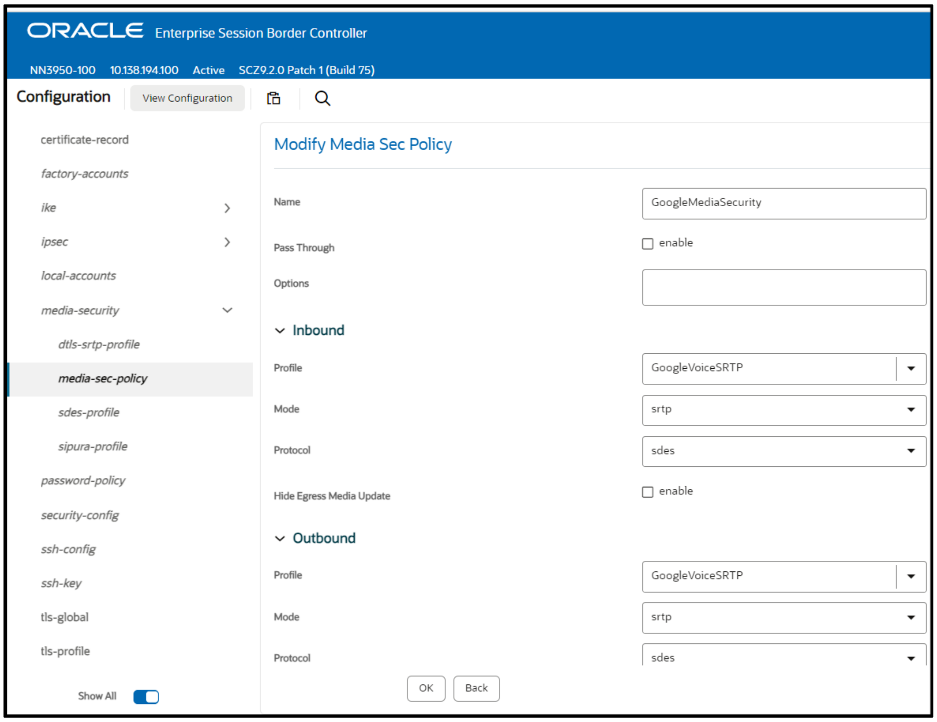
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any) and, if SRTP needs to be used, the sdes-profile that needs to be used

In this example, we are configuring two media security policies. One to secure and decrypt media toward Sip Link, the other for non-secure media facing PSTN.

GUI Path: security/media-security/media-sec-policy

ACLI Path: config t→security→media-security→media-sec-policy

- Click Add, use the examples below to configure



Modify Media Sec Policy

Name: GoogleMediaSecurity

Pass Through: □ enable

Options:

Inbound

Profile: GoogleVoiceSRTP

Mode: srtp

Protocol: sdes

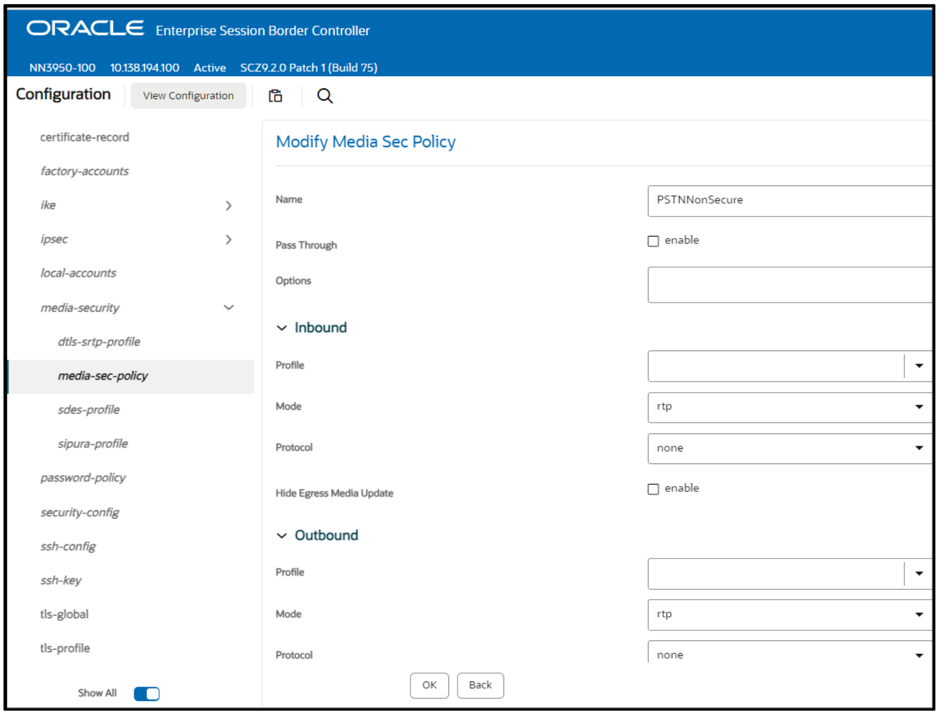
Hide Egress Media Update: □ enable

Outbound

Profile: GoogleVoiceSRTP

Mode: srtp

Protocol: sdes



Modify Media Sec Policy

Name: PSTNNonSecure

Pass Through: □ enable

Options:

Inbound

Profile:

Mode: rtp

Protocol: none

Hide Egress Media Update: □ enable

Outbound

Profile:

Mode: rtp

Protocol: none

- Select OK at the bottom of each when finished

This finishes the security configuration portion of the application note. We'll now move on to configuring media and transcoding.

7.4 Transcoding Configuration

Transcoding is the ability to convert between media streams that are based upon disparate codecs. The OCSBC supports IP-to-IP transcoding for SIP sessions and can connect two voice streams that use different coding algorithms with one another.

7.4.1 Codec Policies

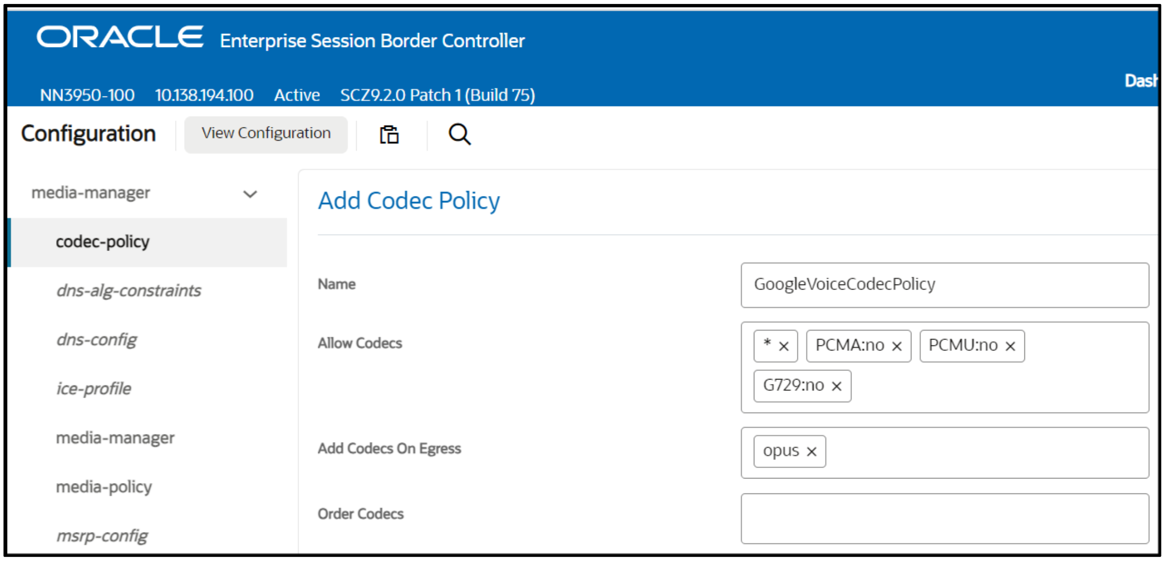
Codec policies are sets of rules that specify the manipulations to be performed on SDP offers allowing the Oracle SBC the ability to add, strip, and reorder codecs for SIP sessions.

While transcoding media codecs is optional, as Google supports both commonly used codecs PCMU and PCMA, it may be required in some environments if the supported codecs on each side differ. In the example below, we will configure codec policies to use the OPUS codec for Google Voice, and PCMU for PSTN.

GUI Path: media-manager/codec-policy

ACLI Path: config t→media-manager→codec-policy

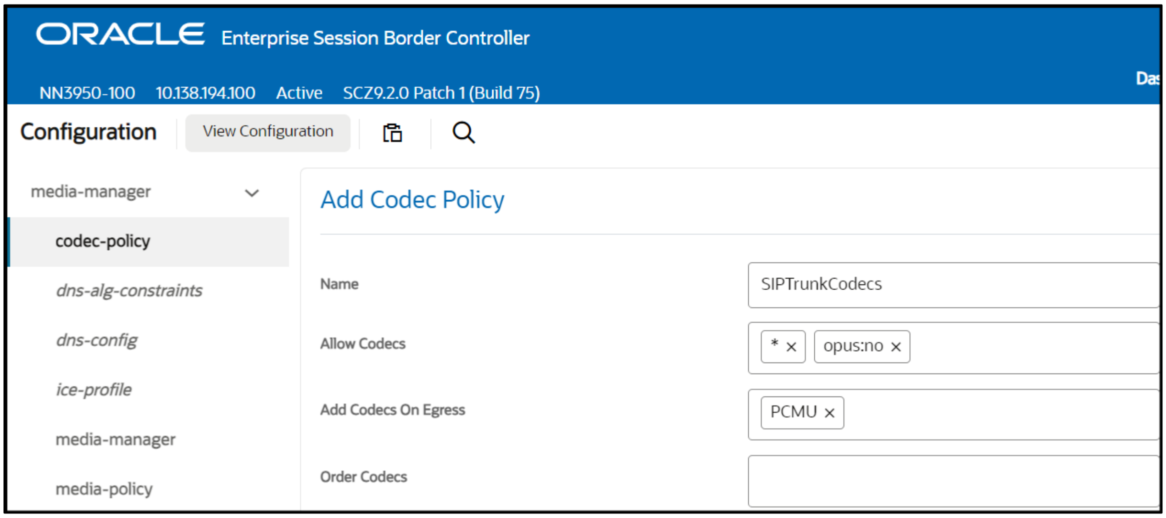
Here is an example config of a codec policy for the SBC to use the OPUS codec toward Google Voice SIP Link



Add Codec Policy

Name	GoogleVoiceCodecPolicy
Allow Codecs	* × PCMA:no × PCMU:no × G729:no ×
Add Codecs On Egress	opus ×
Order Codecs	

Since some SIP Trunks may have issues with the codecs being offered by Google Voice, you can create another codec policy to remove unwanted or unsupported codecs from the request/responses to your Sip Trunk provider.



Add Codec Policy

Name: SIPTrunkCodecs

Allow Codecs: * × opus:no ×

Add Codecs On Egress: PCMU ×

Order Codecs:

- Select OK at the bottom

This concludes the section of the application note on how to configure the Oracle SBC to trancode media. Next, we'll move on to the media configuration.

7.5 Media Configuration

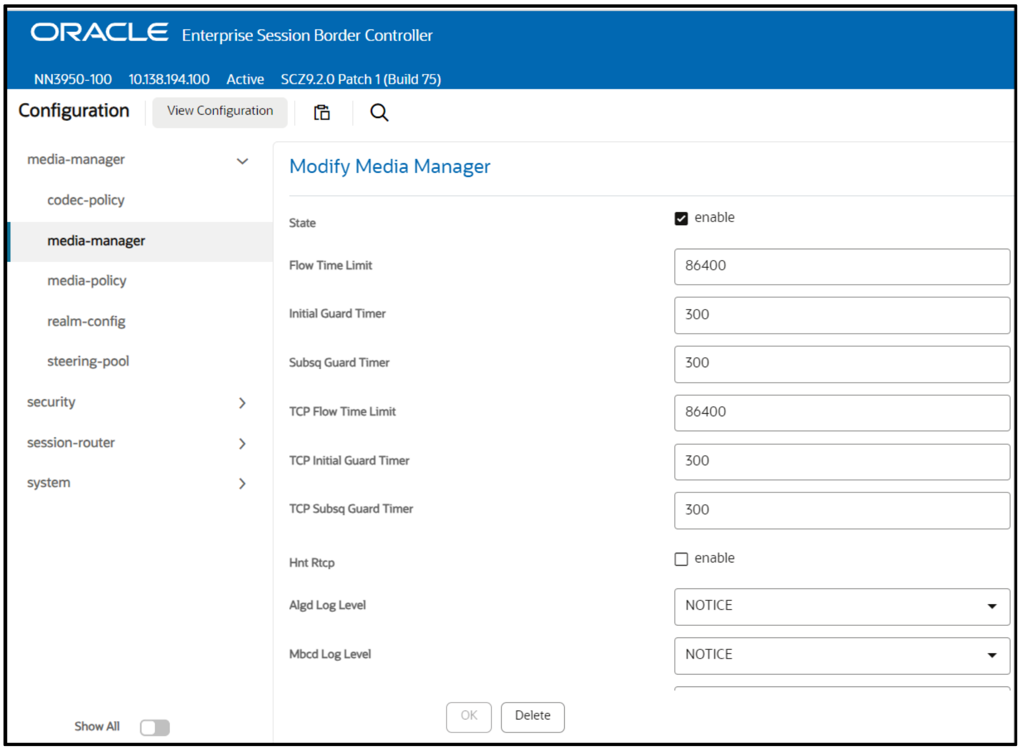
This section will guide you through the configuration of media manager, realms, and steering pools, all of which are required for the SBC to handle signaling and media flows toward Google and PSTN.

7.5.1 Media Manager

To configure media functionality on the SBC, you must first enabled the global media manager

GUI Path: media-manager/media-manager

ACLI Path: config t→media-manager→media-manager-config



Modify Media Manager

State ☑ enable

Flow Time Limit 86400

Initial Guard Timer 300

Subsq Guard Timer 300

TCP Flow Time Limit 86400

TCP Initial Guard Timer 300

TCP Subsq Guard Timer 300

Hnt Rtcp □ enable

Algd Log Level NOTICE

Mbcd Log Level NOTICE

- Click OK at the bottom

7.5.2 Realm Config

Realms are a logical distinction representing routes (or groups of routes) reachable by the Oracle® Session Border Controller and what kinds of resources and special functions apply to those routes. Realms are used as a basis for determining ingress and egress associations to network interfaces.

.
GUI Path; media-manger/realm-config

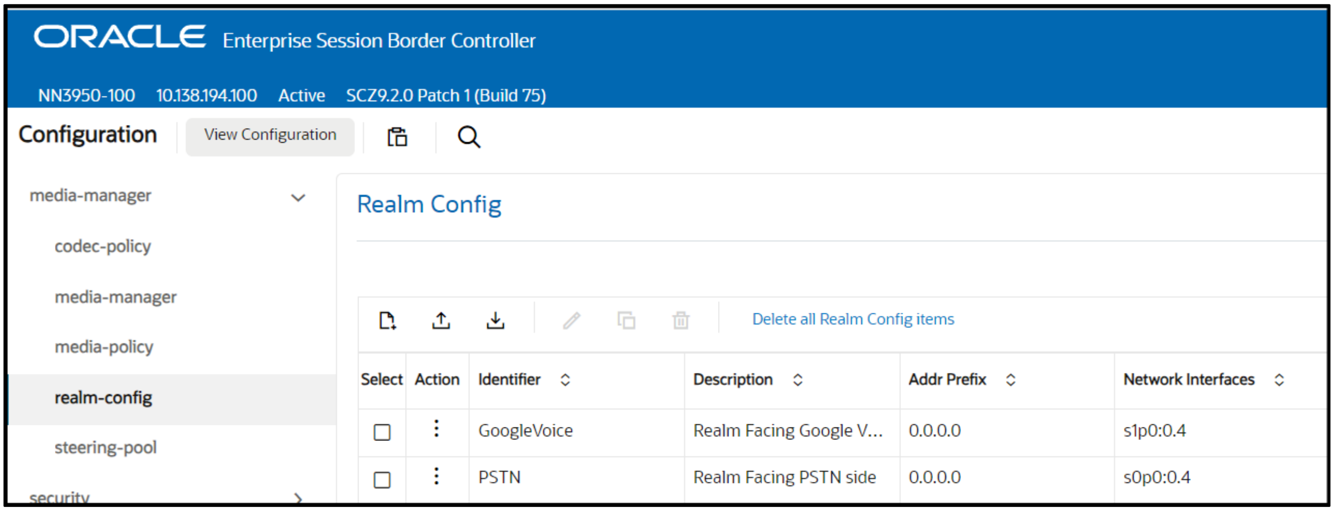
ACLI Path: config t→media-manger→realm-config

- Click Add and use the following table as a configuration example for the realms. The following parameters are all required unless mentioned as optional below.

Config Parameter	GoogleVoice Realm	PSTN Realm
Identifier	GoogleVoice	PSTN
Network Interface	S1p0:0	S0p0:0
Mm in realm	☑	☑
Media Sec policy	GoogleMediaSecurity	PSTNNonSecure
Teams-FQDN	solutionslab.cgbuburlington.com	
Teams-fqdn-in-uri	☑	
Codec policy	GoogleVoiceCodecPolicy	SipTrunkCodecs
Access-control-trust-level	HIGH	HIGH

Also notice the realm configuration is where we assign some of the elements configured earlier in this document. IE…

- Network Interface
- Media Security Policy
- Codec Policy (optional on the PSTN Realm)


ORACLE Enterprise Session Border Controller
NN3950-100 10.138.194.100 Active SCZ9.2.0 Patch 1 (Build 75)
Configuration
View Configuration
media-manager
codec-policy
media-manager
media-policy
realm-config
steering-pool
security
Realm Config
Delete all Realm Config items

Select	Action	Identifier	Description	Addr Prefix	Network Interfaces
□	⋮	GoogleVoice	Realm Facing Google V…	0.0.0.0	s1p0:0.4
□	⋮	PSTN	Realm Facing PSTN side	0.0.0.0	s0p0:0.4

- Select OK at the bottom of each

7.5.3 Steering Pools

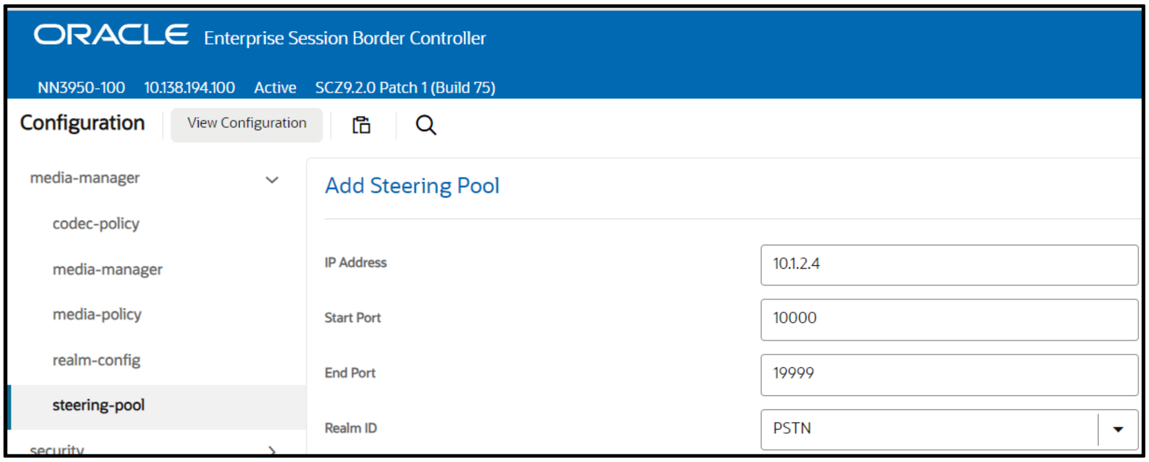
Steering pools define sets of ports that are used for steering media flows through the OCSBC.
These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We configure one steering pool for PSTN. The other facing Google Voice SIP Link.

GUI Path: media-manger/steering-pool

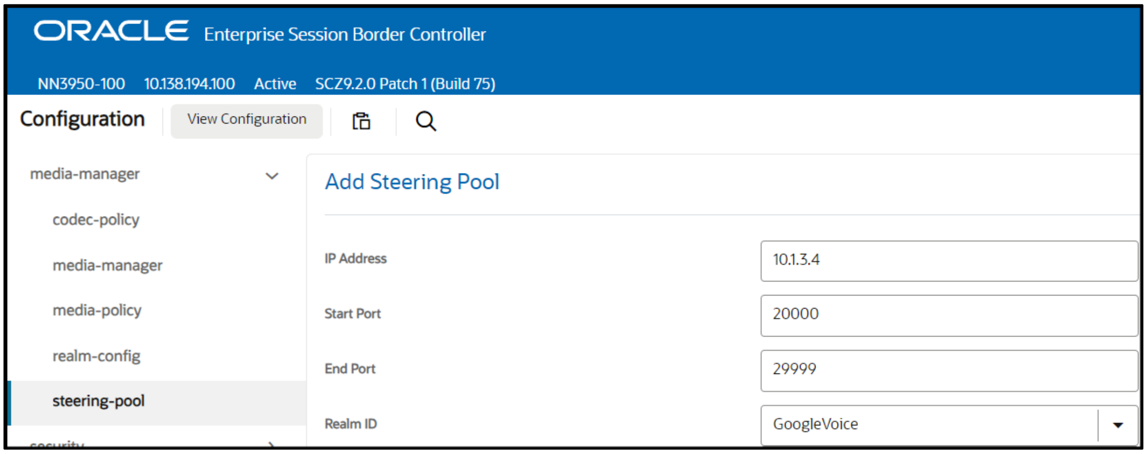
ACLI Path: config t→media-manger→steering-pool

- Click Add, and use the below examples to configure



Add Steering Pool

IP Address	10.1.2.4
Start Port	10000
End Port	19999
Realm ID	PSTN



Add Steering Pool

IP Address	10.1.3.4
Start Port	20000
End Port	29999
Realm ID	GoogleVoice

- Select OK at the bottom

We will now work through configuring what is needed for the SBC to handle SIP signaling.

7.6 Sip Configuration

This section outlines the configuration parameters required for processing, modifying, and securing sip signaling traffic.

7.6.1 Sip-Config

To enable sip related objects on the Oracle SBC, you must first configure the global Sip Config element:

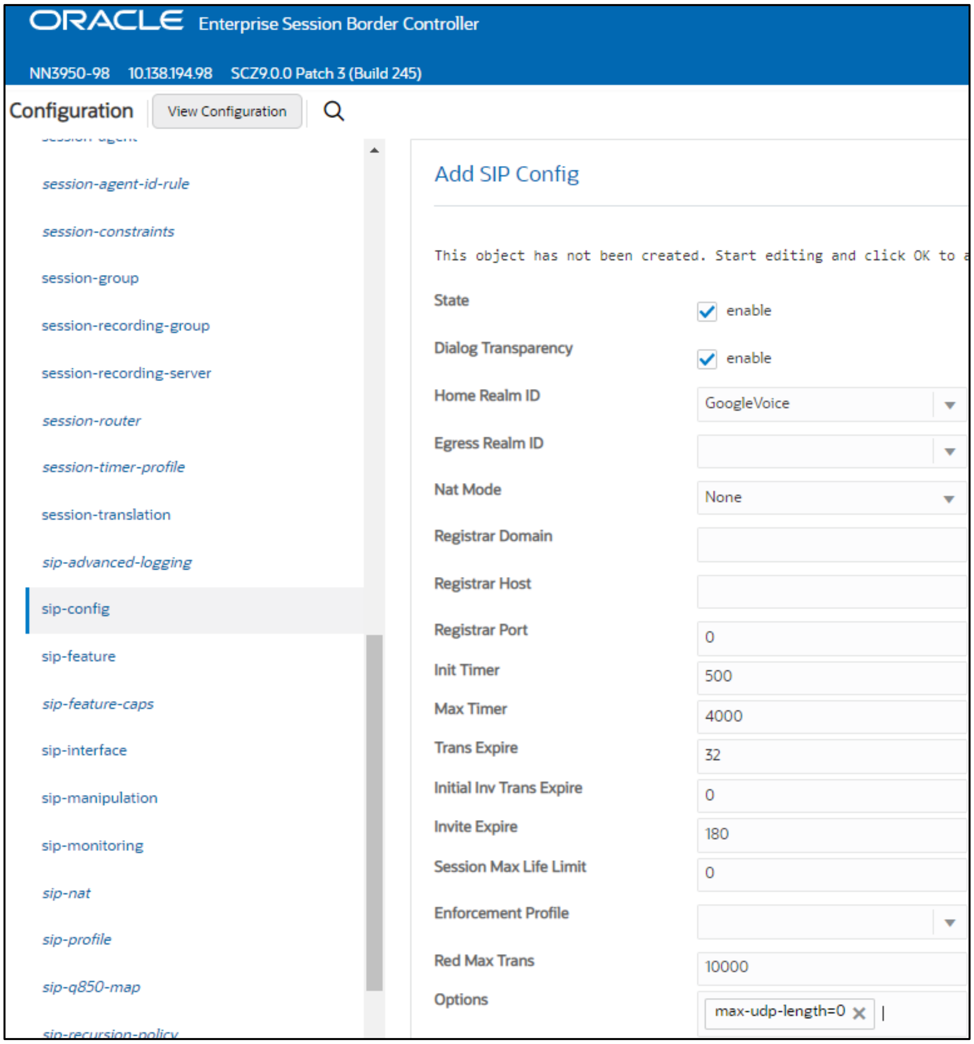
GUI Path: session-router/sip-config

ACLI Path: config t→session-router→sip-config

There are only two recommended changes/additions to the global Sip Config.

- Set the home realm ID parameter to GoogleVoice Realm,
  and add the following hidden option:

- Max-udp-length=0: Setting this option to zero (0) forces sipd to send fragmented UDP packets. Using this option, you override the default value of the maximum UDP datagram size (1500 bytes; sipd requires the use of SIP/TCP at 1300 bytes).



Add SIP Config

This object has not been created. Start editing and click OK to a

State	☑ enable
Dialog Transparency	☑ enable
Home Realm ID	GoogleVoice
Egress Realm ID	
Nat Mode	None
Registrar Domain	
Registrar Host	
Registrar Port	0
Init Timer	500
Max Timer	4000
Trans Expire	32
Initial Inv Trans Expire	0
Invite Expire	180
Session Max Life Limit	0
Enforcement Profile	
Red Max Trans	10000
Options	max-udp-length=0

- Select OK at the bottom

7.6.2 Sip Manipulation

Variances among SIP networks, like incompatible vendor deployments or disparate SIP services, can degrade SIP services or disrupt SIP operations. To resolve these variances, Oracle deploys Header Manipulation Rules (HMR), giving network administrators the ability to control SIP traffic by manipulating SIP messages

We utilize this feature to present calls to Google Voice SIP Link from the SBC. The SBC would require alterations to the SIP signaling it natively created. The following are manipulations required on the SBC for to present signaling to SIP Link.

This sip manipulation changes the following for both Sip Invites and SIP Options.

- the host and port of the Request URI and TO header to the value specified by Google
- Adds a new SIP header that contains the secret key obtained when creating a SIP trunk in the Google Voice admin portal

GUI Path: session router/sip manipulation

ACLI Path: config t→session-router→sip-manipulation

The sip manipulation below is easily added to the Oracle SBC configuration via the GUI,
but for ease of viewing, we have provided the output from ACLI.

```
sip-manipulation
        name                                GoogleOutManip
        description
        split-headers
        join-headers
        header-rule
                name                                RequRIHost
                header-name                              Request-URI
                action                            manipulate
                comparison-type                          case-sensitive
                msg-type                             request
                methods                              INVITE,OPTIONS
                match-value
                new-value
                element-rule
                        name                                RequRIHost
                        parameter-name
                        type                              uri-host
                        action                            replace
                        match-val-type                          any
                        comparison-type                           case-sensitive
                        match-value
                        new-value                             "trunk.sip.voice.google.com"
                element-rule
                        name                                RequRIPort
                        parameter-name
                        type                              uri-port
                        action                            replace
                        match-val-type                          any
                        comparison-type                           case-sensitive
                        match-value
                        new-value                             $REMOTE_PORT
        header-rule
                name                                GoogleXHeader
                header-name                              X-Google-Pbx-Trunk-Secret-Key
                action                            add
                comparison-type                          case-sensitive
                msg-type                             request
                methods                              Invite,OPTIONS
                match-value
                new-value                             "a7e[redacted]c0ce"
```

```
header-rule
            name                               ToHost
            header-name                           TO
            action                            manipulate
            comparison-type                         case-sensitive
            msg-type                            request
            methods                             Invite,Options
            match-value
            new-value
            element-rule
                  name                                tohost
                  parameter-name
                  type                              uri-host
                  action                             replace
                  match-val-type                          any
                  comparison-type                           case-sensitive
                  match-value
                  new-value                             "trunk.sip.voice.google.com"
            element-rule
                  name                                toport
                  parameter-name
                  type                              uri-port
                  action                             replace
                  match-val-type                          any
                  comparison-type                           case-sensitive
                  match-value
                  new-value                             $REMOTE_PORT
```

7.6.3 Session Timer Profile

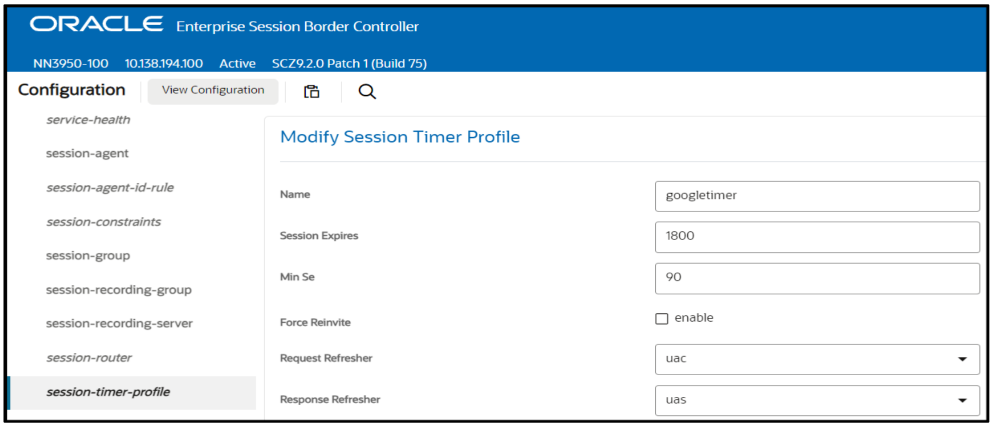
The use of session timers is a requirement when integrating the Oracle SBC with Google Voice Sip Link. Google requires the SBC to be the refresher on calls to and from SIP Link and only UPDATE messages are supported. The below session-timer-config satisfies these requirements.

GUI Path: session-router/session-timer-profile

ACLI Path: config t→session-router→session-timer-profile

Note: to see the session-timer-profile in SBC GUI, you must toggle Show All at the bottom

Click add, and use the example below to configure a session timer profile:



Modify Session Timer Profile

Name	googletimer
Session Expires	1800
Min Se	90
Force Reinvite	□ enable
Request Refresher	uac
Response Refresher	uas

- Select OK at the bottom

7.6.4 Sip Interface

The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages

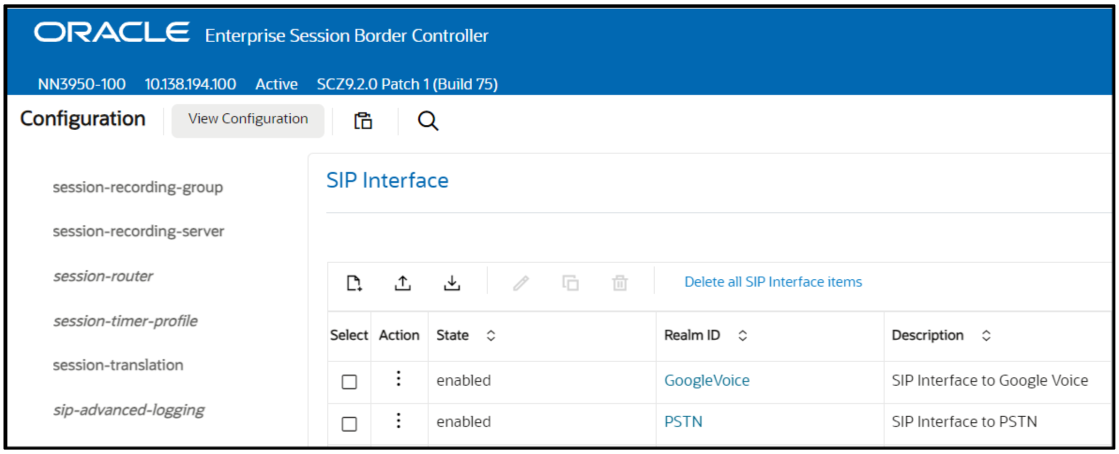
Configure two sip interfaces, one associated with PSTN Realm, and the other for Google Voice SIP Link.

GUI Path: session-router/sip-interface

ACLI Path: config t→session-router→sip-interface

Click Add, and use the table below as an example to configure:

Config Parameter	**PSTN**	**GoogleVoice**
Realm ID	PSTN	GoogleVoice
OutmanipulationID		GoogleOutManip
Session-timer-profile		googletimer
Sip Port Config Parmeter	**PSTN**	**GoogleVoice**
Address	10.1.2.4	10.1.3.4
Port	5060	5061
Transport protocol	UDP	TLS
TLS profile		GoogleVoiceTLSProfile
Allow anonymous	agents-only	agents-only


ORACLE Enterprise Session Border Controller

NN3950-100 10.138.194.100 Active SCZ9.2.0 Patch 1 (Build 75)

Configuration | View Configuration

session-recording-group
session-recording-server
session-router
session-timer-profile
session-translation
sip-advanced-logging

SIP Interface

Delete all SIP Interface items

Select	Action	State	Realm ID	Description
☐	⋮	enabled	GoogleVoice	SIP Interface to Google Voice
☐	⋮	enabled	PSTN	SIP Interface to PSTN

Notice this is where we assign the TLS profile configured under the Security section of this guide, and the sip manipulation used to authenticate the call through GoogleVoice, and the session timer profile.

- Select OK at the bottom of each when applicable

7.6.5 Session Agents

Session Agents are configuration elements which are trusted agents that can both send and receive traffic from the Oracle SBC with direct access to the trusted data path.

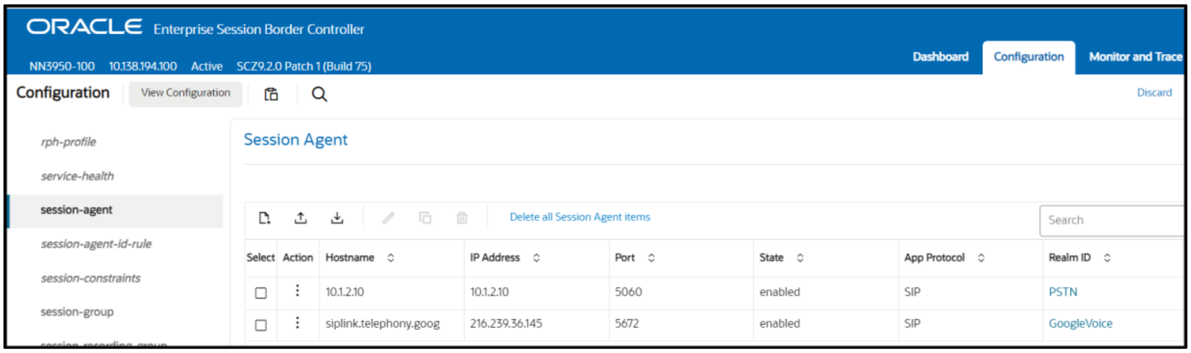
GUI Path: session-router/session-agent

ACLI Path: config t→session-router→session-agent

For this example, we'll configure one session agent for Google Voice SIP Link, and another for PSTN.

- Click Add, and use the table below to configure:

Config parameter	Google Voice SIP Link	PSTN
Hostname	siplink.telephony.goog	10.1.2.10
Ip-address		10.1.2.10
Port	5672	5060
Transport method	StaticTLS	UDP
Realm ID	GoogleVoice	SIPTrunk
Ping Method	OPTIONS	OPTIONS
Ping Interval	30	30
Ping Response	☑	☑



Select	Action	Hostname	IP Address	Port	State	App Protocol	Realm ID
□	⋮	10.1.2.10	10.1.2.10	5060	enabled	SIP	PSTN
□	⋮	siplink.telephony.goog	216.239.36.145	5672	enabled	SIP	GoogleVoice

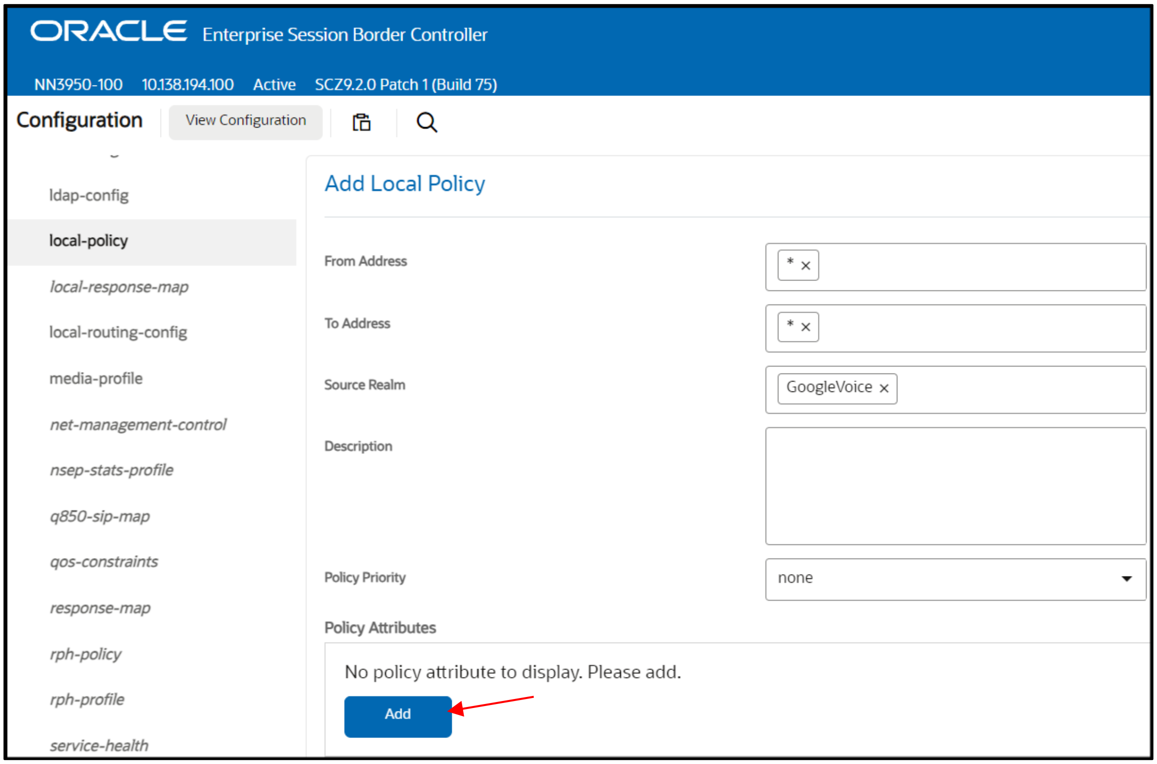
- Select OK at the bottom

7.7 Routing Configuration

Now that a majority of the signaling, security and media configuration is in place, we can configure the SBC to route calls from one end of the network to the other. The SBC has multiple routing features that can be utilized, but for the purposes of this example configuration, we'll configure local policies to route calls from Google Voice SIP Link to our Sip trunk, and vice versa…

GUI Path: session-router/local-policy

ACLI Path: config t→session-router→local-policy



From Address: * ×

To Address: * ×

Source Realm: GoogleVoice ×

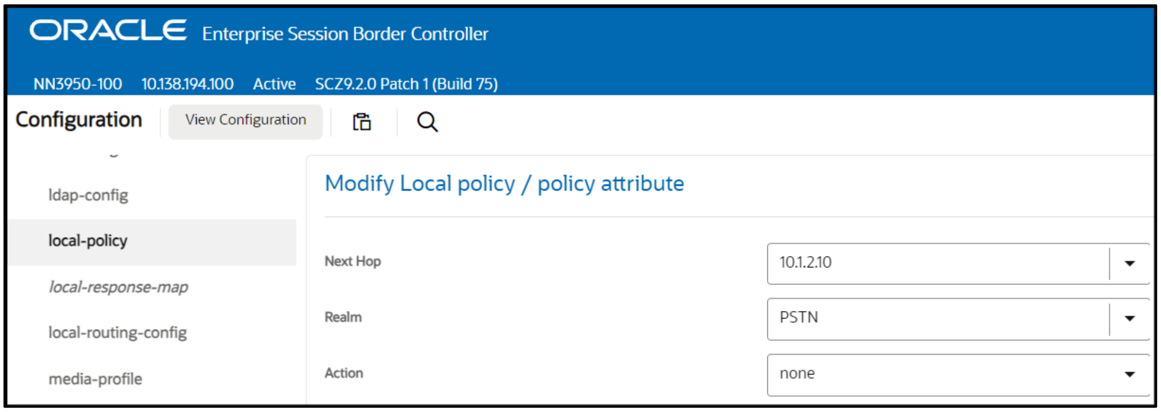
Description:

Policy Priority: none

Policy Attributes

No policy attribute to display. Please add.

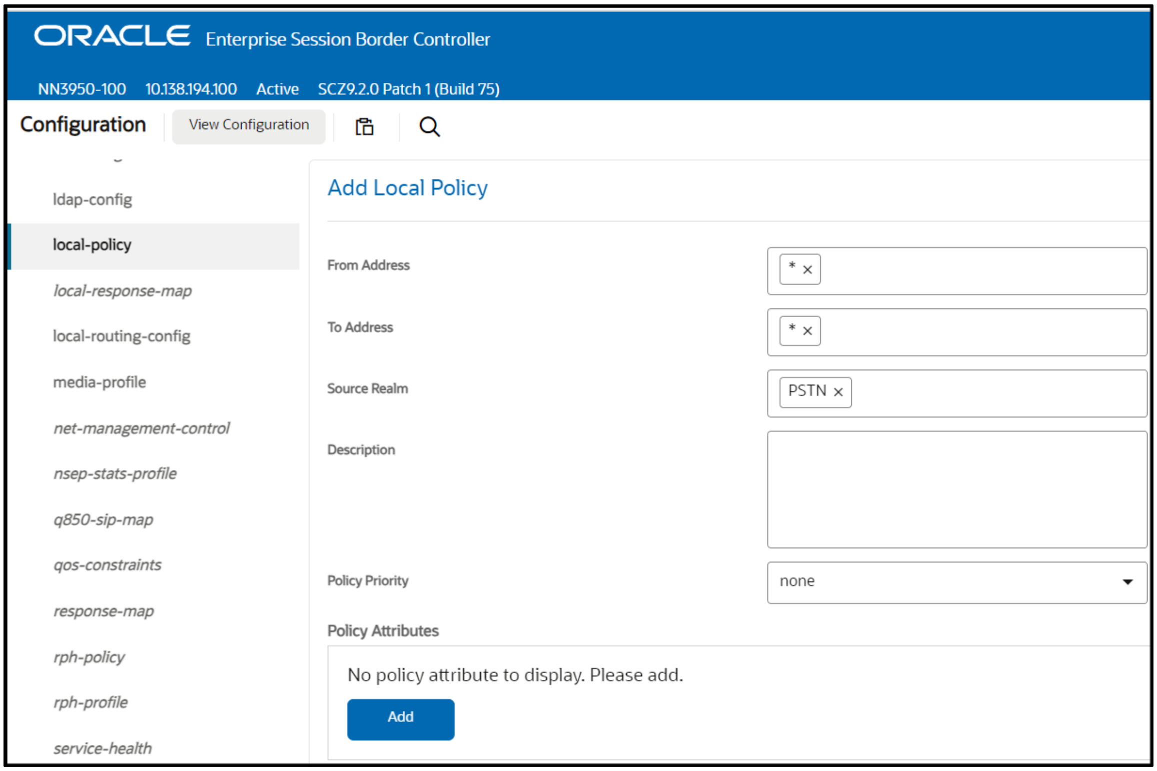
After entering values for to and from address and source realm, click Add under policy attribute to configure the next hop destination.



Modify Local policy / policy attribute

Next Hop	10.1.2.10
Realm	PSTN
Action	none

Next, we'll setup routing from our SIP Trunk to SIP Link:



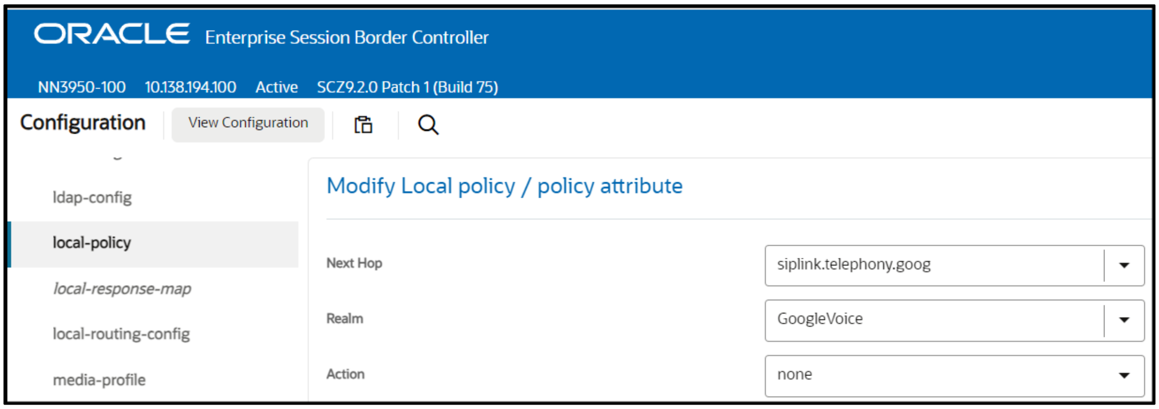
Add Local Policy

From Address	* ×
To Address	* ×
Source Realm	PSTN ×
Description	
Policy Priority	none

Policy Attributes

No policy attribute to display. Please add.

Add



Modify Local policy / policy attribute

Next Hop	siplink.telephony.goog
Realm	GoogleVoice
Action	none

- Select OK when applicable on each screen

This concludes the configuration portion of this application note. We'll now move on to verifying the connection between the Oracle SBC and Google Voice SIP Link.

8 Verify Connectivity

8.1 Oracle SBC Options Pings

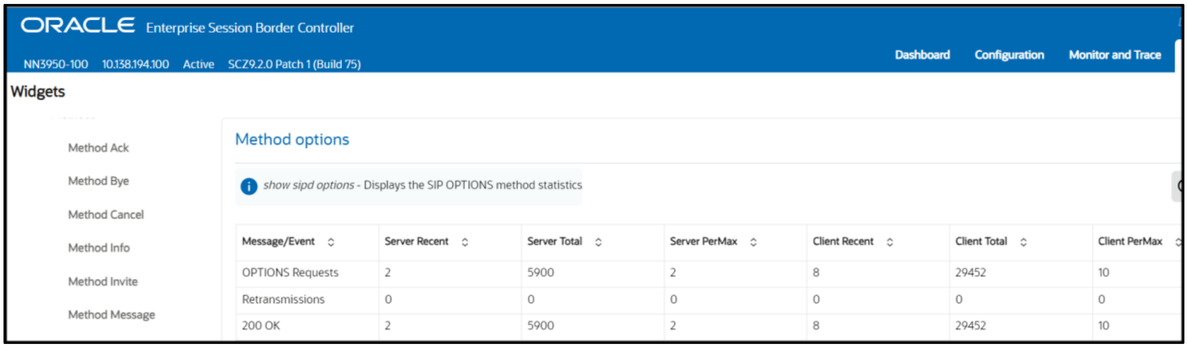
After you've paired the OCSBC with SIPLink, validate that the SBC can successfully exchange SIP Options with Google Voice SipLink.

While in the Oracle SBC GUI, Utilize the "Widgets" to check for OPTIONS to and from the SBC.

- At the top, click "Wigits"

This brings up the Wigits menu on the left hand side of the screen

GUI Path: Signaling/SIP/Method Options



Method options

show sipd options - Displays the SIP OPTIONS method statistics

Message/Event	Server Recent	Server Total	Server PerMax	Client Recent	Client Total	Client PerMax
OPTIONS Requests	2	5900	2	8	29452	10
Retransmissions	0	0	0	0	0	0
200 OK	2	5900	2	8	29452	10

- Looking at both the **Server Recent** and **Client Recent**, verify the counters are showing OPTIONS Requests and 200OK responses.

9 Syntax Requirements for SIP Invite and SIP Options:

Google Voice Sip Link has requirements for the syntax of SIP messages.
This section covers high-level requirements to SIP syntax of Invite and Options messages. The information can be used as a first step during troubleshooting when calls don't go through. From our experience most of the issues are related to the wrong syntax of SIP messages.

9.1 Terminology

- Recommended – not required, but to simplify the troubleshooting, it is recommended to configure as in examples as follow
- Must – strict requirement, the system does not work without the configuration of these parameters

9.2 Requirements for Invite Messages

Picture 1 Example of INVITE and 200 OK

```
INVITE sip:+17814437243@trunk.sip.voice.google.com:5672;user=phone;transport=tls SIP/2.0
Via: SIP/2.0/TLS 141.146.36.70:5061;branch=z9hG4bKnkabte0040j1680u6ut0.1
Max-Forwards: 22
From: <sip:+19783559868@solutionslab.cgbuburlington.com:5060;user=phone>;tag=11c1edca0a020200
To: <sip:+17814437243@trunk.sip.voice.google.com:5672;user=phone>
Call-ID: 1-11c1edca0a020200.6ff26788@68.68.117.67
CSeq: 2 INVITE
Contact: <sip:+19783559868@solutionslab.cgbuburlington.com:5061;user=phone;transport=tls>
Allow: ACK, BYE, CANCEL, INVITE, OPTIONS, PRACK, REFER
User-Agent: T7100/3.0
Supported: 100rel,timer
Content-Type: application/sdp
Content-Length: 293
Session-Expires: 1800; refresher=uac
Min-SE: 90
X-MS-SBC: Oracle/AP3950/9.0.0p3
X-Google-Pbx-Trunk-Secret-Key: a7e[redacted]c0ce
```

9.2.1 Contact Header-Invite

- Must have the Google Voice Sip Link FQDN in RURI and TO Host
- Must contain the X-Google-Pbx-Trunk-Secret-Key header obtained when creating a SIP trunk in the Google Voice admin
- Must contain the SBC's FQDN in Contact host

9.3 Requirements for OPTIONS Messages

Example of OPTIONS message

```
OPTIONS sip:trunk.sip.voice.google.com:5672;transport=tls SIP/2.0
Via: SIP/2.0/TLS 141.146.36.70:5061;branch=z9hG4bKvikjce10boa65ukfe2b0
Call-ID: 3caeb5f07a4adbc1f4b1a0033059bd860000g20100@141.146.36.70
To: sip:ping@ trunk.sip.voice.google.com:5672
From: <sip:ping@solutionslab.cgbuburlington.com>;tag=a9f585c41fce93dd711ac9a06b97f8480000g20
Max-Forwards: 70
CSeq: 5 OPTIONS
Contact: <sip:ping@solutionslab.cgbuburlington.com:5061;transport=tls>
Expires: 30
Route: <sip:216.239.36.157:5672;lr>
X-MS-SBC: Oracle/AP3950/9.0.0p3
Content-Length: 0
X-Google-Pbx-Trunk-Secret-Key: a7e[redacted]c0ce
```

9.3.1 Contact Header-OPTIONS:

- When sending OPTIONS to Sip Link, “Contact” header should have SBC FQDN in URI
- OPTIONS must contain the X-Google-Pbx-Trunk-Secret-Key header obtained when creating a SIP trunk in the Google Voice admin portal

10 Appendix A

10.1 Oracle SBC TDM with Sip Link

Oracle® designed the Time Division Multiplexing (TDM) functionality for companies planning to migrate from TDM to SIP trunks by using a hybrid TDM-SIP infrastructure, rather than adopting VoIP-SIP as their sole means of voice communications. The TDM interface on the Oracle® Enterprise Session Border Controller (E-SBC) provides switchover for egress audio calls, when the primary SIP trunk becomes unavailable. You can use TDM with legacy PBXs and other TDM devices.

- Only the Acme Packet 1100, Acme Packet 3900 and Acme Packet 3950 platforms support TDM, which requires the optional TDM card.
- TDM supports bidirectional calls as well as unidirectional calls.
- TDM operations require you to configure TDM Config and TDM Profile, as well as local policies for inbound and outbound traffic.
- The software upgrade procedure supports the TDM configuration.
- Options for the Acme Packet 1100, Acme Packet 3900 and Acme Packet 3950 platforms include CallingLine Identification Presentation (CLIP) and Connected-Line Identification Presentation (COLP).
- Options for the Acme Packet 1100 platform include the four-port Primary Rate Interface (PRI), the Euro ISDN Basic Rate Interface (BRI), and the Foreign Exchange Office-Foreign Exchange Subscriber (FXO-FXS) card.

10.1.1 Interface Requirements

- PRI—Digium1TE133F single-port or Digium 1TE435BF four-port card.
- BRI—Digium 1B433LF four-port card
- FXS—Digium 1A8B04F eight-port card, green module (ports 1-4)
- FXO—Diguim 1A8B04F eight-port card, red module (ports 5-8)

For further information on the setup and configuration of TDM on the Oracle SBC, please refer to the TDM Configuration Guide

11 Appendix B

11.1 Oracle SBC deployed behind NAT

The Support for SBC Behind NAT SPL plug-in changes information in SIP messages to hide the end point located inside the private network.

The specific information that the Support for SBC Behind NAT SPL plug-in changes depends on the direction of the call, for example, from the NAT device to the SBC or from the SBC to the NAT device.

Configure the Support for SBC Behind NAT SPL plug-in for each SIP interface that is connected to a NAT device. One public-private address pair is required for each SIP interface that uses the SPL plug-in, as follows.

- The private IP address must be the same IP as configured on both the SIP Interface and Steering Pool
- The public IP address must be the public IP address of the NAT device

Here is an example configuration with SBC Behind NAT SPL config.

The SPL is applied to the Google side SIP interface.

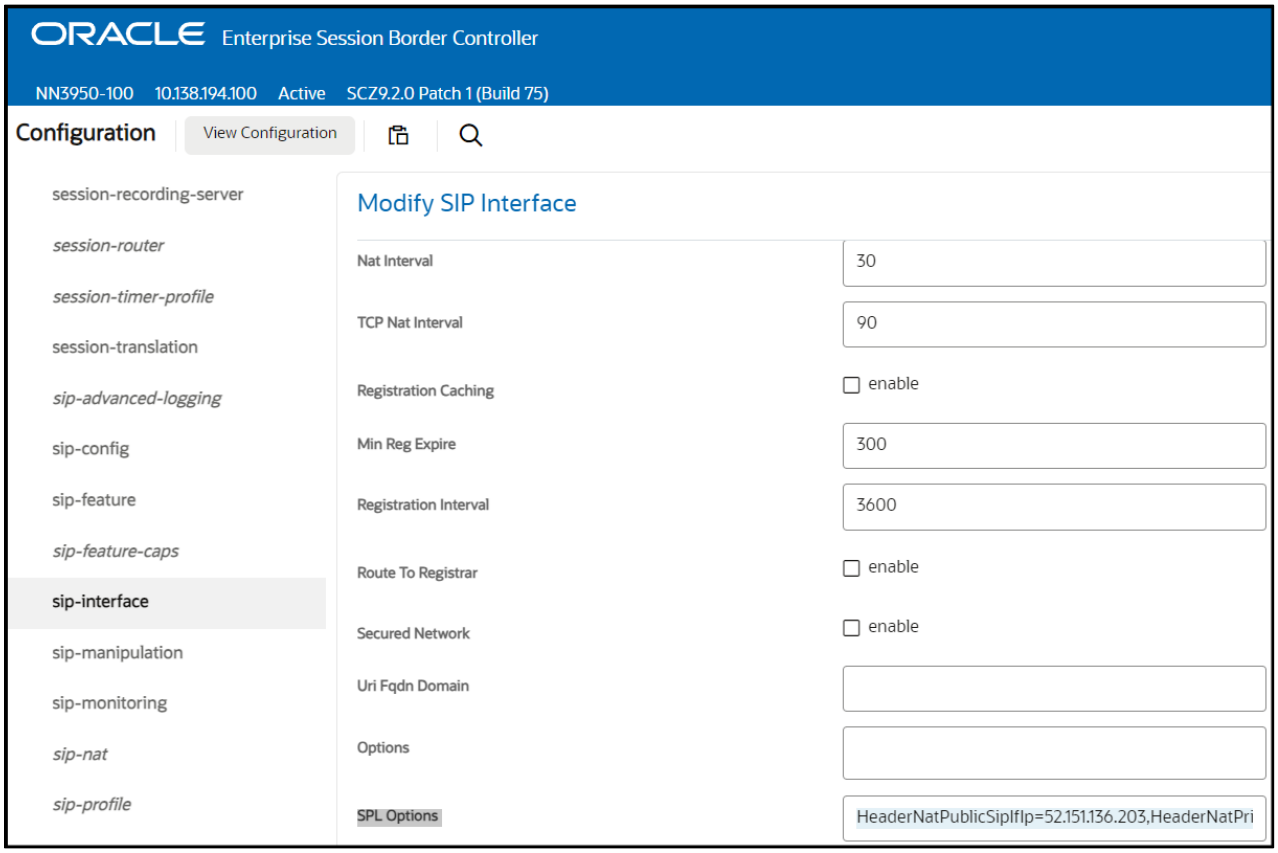
GUI Path: session-router/sip-interface

ACLI Path: config t→session-router→sip-interface

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.1.3.4

HeaderNatPublicSipIfIp is the public interface ip

HeaderNatPrivateSipIfIp is the private ip.



Modify SIP Interface

Nat Interval	30
TCP Nat Interval	90
Registration Caching	□ enable
Min Reg Expire	300
Registration Interval	3600
Route To Registrar	□ enable
Secured Network	□ enable
Uri Fqdn Domain	
Options	
SPL Options	HeaderNatPublicSipIfIp=52.151.136.203,HeaderNatPri

You will need to apply these options to every sip interface on the SBC that is connected through a NAT.

12 ACLI Running Configuration

Below is a complete output of the running configuration used to create this application note. This output includes all the configuration elements used in our examples, including some of the optional configuration features outlined throughout this document. Be aware that not all parameters may be applicable to every Oracle SBC setup, so please take this into consideration if planning to copy and paste this output into your SBC.

```
certificate-record
        name                           DigiCertRoot
        common-name                            DigiCert Global Root CA
certificate-record
        name                           DigiCertTLSRSA
        organization                     DigiCert Inc
        unit                          www.digicert.com
        common-name                            DigiCert TLS RSA SHA256 2020 CA1
certificate-record
        name                           GTSRootR1
        state                                      CA
        organization                     Google Trust Services LLC
        common-name                            GTS Root R1
certificate-record
        name                           GlobalSignRoot
        state                                      CA
        organization                     GlobalSign
        common-name                            GlobalSign Root
certificate-record
        name                           SBCCertificateforGoogleVoice
        state                                      TX
        locality                                   Austin
        common-name                            solutionslab.cgbuburlington.com
        extended-key-usage-list                  serverAuth
                                                 clientAuth
codec-policy
        name                           GoogleVoiceCodecPolicy
        allow-codecs                       * PCMU:NO
        add-codecs-on-egress                     PCMA
        order-codecs                       PCMA *
codec-policy
        name                           SipTrunkCodecs
        allow-codecs                       * PCMA:NO
        add-codecs-on-egress                     PCMU
        order-codecs                       OPUS PCMU *
filter-config
        name                           all
        user                          *
http-server
        name                           webServerInstance
        http-interface-list              GUI
ice-profile
        name                           ice
local-policy
        from-address                       *
        to-address                       *
        source-realm                       GoogleVoice
```

```
        policy-attribute
                next-hop                              10.1.2.10
                realm                               SIPTrunk
                action                              replace-uri
local-policy
        from-address                              *
        to-address                              *
        source-realm                              SIPTrunk
        policy-attribute
                next-hop                              siplink.telephony.goog
                realm                               GoogleVoice
media-manager
media-sec-policy
        name                              GoogleMediaSecurity
        inbound
                profile                             SDES
                mode                                 srtp
                protocol                             sdes
        outbound
                profile                             SDES
                mode                                 srtp
                protocol                             sdes
media-sec-policy
        name                               PSTNNonSecure
network-interface
        name                              s0p0
        ip-address                          10.1.2.4
        netmask                             255.255.255.0
        gateway                             10.1.2.1

network-interface
        name                              s1p0
        ip-address                          10.1.3.4
        netmask                             255.255.255.0
        gateway                             10.1.3.4
        dns-ip-primary                        8.8.8.8
        dns-ip-backup1                         8.8.4.4
        dns-domain                            solutionslab.cgbuburlington.com
phy-interface
        name                              s0p0
        operation-type                        Media
phy-interface
        name                              s1p0
        operation-type                        Media
        port                                  0
        slot                                  1
realm-config
        identifier                        GoogleVoice
        network-interfaces                       s1p0:0.4
        mm-in-realm                           enabled
        media-sec-policy                        GoogleMediaSecurity
        teams-fqdn                           solutionslab.cgbuburlington.com
        teams-fqdn-in-uri                      enabled
        access-control-trust-level               high
        codec-policy                         GoogleVoiceCodecPolicy
```

```
realm-config
        identifier                          SIPTrunk
        network-interfaces                      s0p0:0.4
        mm-in-realm                           enabled
        media-sec-policy                        PSTNNonSecure
        access-control-trust-level               high
        codec-policy                           SipTrunkCodecs
sdes-profile
        name                                GoogleVoiceSRTP
session-agent
        hostname                              10.1.2.10
        ip-address                           10.1.2.10
        realm-id                            SIPTrunk
        ping-interval                        30
        ping-response                          enabled
session-agent
        hostname                              siplink.telephony.goog
        port                                       5672
        transport-method                         StaticTLS
        realm-id                            GoogleVoice
        ping-method                             OPTIONS
        ping-interval                        30
        ping-send-mode                            keepalive
        ping-response                          enabled
session-timer-profile
        name                                googletimer
sip-config
        home-realm-id                            GoogleVoice
        registrar-domain                         *
        registrar-host                        *
        registrar-port                       5060
        options                             inmanip-before-validate
                                        max-udp-length=0
        allow-pani-for-trusted-only              disabled
        add-ue-location-in-pani                 disabled
        npli-upon-register                     disabled
sip-interface
        realm-id                            GoogleVoice
        sip-port
                address                             10.1.3.4
                port                             5061
                transport-protocol                      TLS
                tls-profile                        GoogleVoiceTLSProfile
                allow-anonymous                         agents-only
        out-manipulationid                      GoogleOutManip
        session-timer-profile                   googletimer
sip-interface
        realm-id                            SIPTrunk
        sip-port
                address                             10.1.2.4
                allow-anonymous                         agents-only
sip-manipulation
        name                                GoogleOutManip
        header-rule
                name                                ReqURIHost
                header-name                              Request-URI
```

```
            action                          manipulate
            msg-type                          request
            methods                           INVITE,OPTIONS
            element-rule
                  name                              ReqURIHost
                  type                            uri-host
                  action                          replace
                  new-value                          "trunk.sip.voice.google.com"
            element-rule
                  name                              ReqURIPort
                  type                            uri-port
                  action                          replace
                  new-value                          $REMOTE_PORT
      header-rule
            name                             GoogleXHeader
            header-name                          X-Google-Pbx-Trunk-Secret-Key
            action                          add
            msg-type                          request
            methods                           Invite,OPTIONS
            new-value                          "a7e[redacted]c0ce"
      header-rule
            name                             ToHost
            header-name                          TO
            action                          manipulate
            msg-type                          request
            methods                           Invite,Options
            element-rule
                  name                              tohost
                  type                            uri-host
                  action                          replace
                  new-value                          "trunk.sip.voice.google.com"
            element-rule
                  name                              toport
                  type                            uri-port
                  action                          replace
                  new-value                          $REMOTE_PORT
steering-pool
      ip-address                         10.1.3.4
      start-port                       20000
      end-port                          20999
      realm-id                          GoogleVoice
steering-pool
      ip-address                         10.1.2.4
      start-port                       10000
      end-port                          10999
      realm-id                          SIPTrunk
system-config
tls-profile
      name                              GoogleVoiceTLSProfile
      end-entity-certificate                SBCCertificateforGoogleVoice
      trusted-ca-certificates                GTSRootR1
                                           GlobalSignRoot
      mutual-authenticate                    enabled
```

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/Oracle/
- twitter.com/Oracle
- oracle.com

Integrated Cloud Applications & Platform Services