Oracle SBC integration with RingCentral BYOC

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.

Revision History

Version	Description of Changes	Date Revision Completed
1.0	Initial Version	28th February 2025

1 Table of Contents

This Page is left intentionally blank

2 Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of the Oracle Enterprise Session Border Controller (SBC).
It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform along with RingCentral BYOC and CC Platforms.

3 Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork with RingCentral BYOC and RingCentral Cloud Connector (CC). The solution contained within this document has been tested using Oracle Communication SBC with software version **OS930 GA (SCZ9.3.0 Patch)**

Please note that we have covered the Oracle SBC integration with RingCentral BYOC in this application note document and for the RingCentral CC, the config remains the same for all except the Session Agent IP address or FQDN which changes for the CC platform. **For more assistance on this topic, please check with your RingCentral representative.**

Please note that the IP Addresses, FQDN and configuration names and details given in this document are used for reference purposes only. These same details cannot be used in customer configurations.
End users of this document can use the configuration details according to their network requirements.
The customers can configure any publicly routable IPs for these sections as per their network architecture needs.

4 About RingCentral BYOC

RingCentral offers a software as a service in which customers provide their own local telecommunication carrier services (“Bring Your Own Carrier” or “BYOC”). BYOC allows customers to receive the cloud PBX functionality of RingEX, by connecting their existing local voice carrier to the cloud PBX functionality, which includes videoconferencing, team messaging, and file sharing services. All calls to and from the Public Switched Telephone Network (“PSTN”) travel over the local voice carrier’s network via a gateway purchased and owned by the Customer (the “Gateway”).

RingCentral provides the BYOC solution only in connection with Services purchased in the Home Country. RingCentral makes available to Customer the use of RingCentral’s cloud PBX and related services so that Customer may deploy those services to support its End Users in the BYOC Locations. RingCentral has enabled such services at Customer’s direction, including call queues, call transfer, voicemail, extension-to-extension VoIP, and other related services. Customer acknowledges that RingCentral is not the provider of VoIP or voice services as part of the BYOC solution, and that. Customer, together with its local voice carrier, is the provider of any voice, VoIP, conferencing, or other related services to its users in BYOC Locations (“Local Telecommunications Service”).

For more information about the RingCentral BYOC, please refer to the below link:

https://www.ringcentral.com/solutions/BYOC.html

https://www.ringcentral.com/legal/BYOC-service-description.html

5 Introduction

5.1 Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring. RingCentral BYOC using Oracle Enterprise SBC. There will be steps that require navigating the Oracle SBC GUI interface, understanding the basic concepts of TCP/UDP, IP/Routing, DNS server, SIP/RTP and TLS/SRTP are also necessary to complete the configuration and for troubleshooting, if necessary.

5.2 Requirements

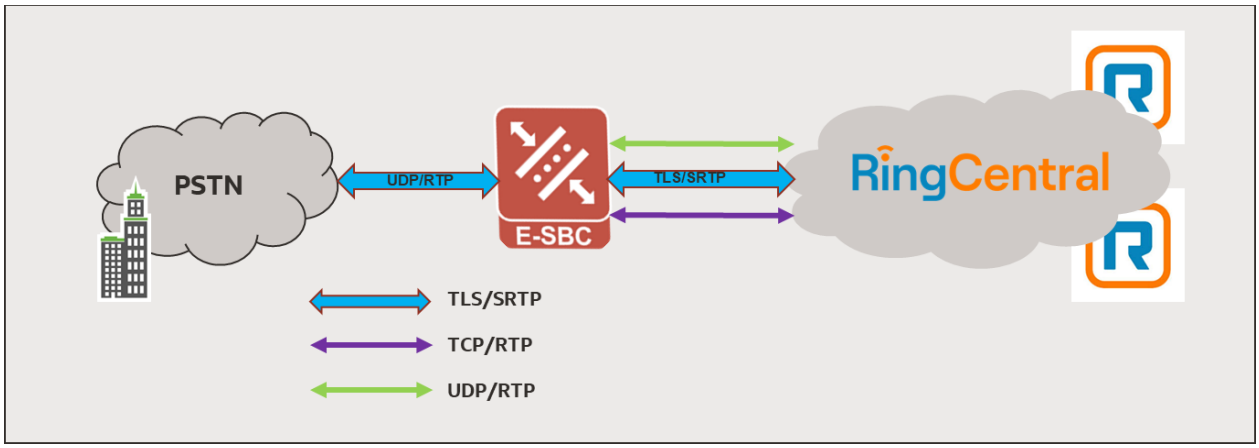
- Fully functioning RingCentral BYOC Environment.
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 9.3.0 version.

The below revision table explains the versions of the software used for each component:
This table is Revision 1 as of now:

Software Used	SBC Version
Revision 1	9.3.0

5.3 Architecture

The network configuration is illustrated below for RingCentral BYOC with Oracle Enterprise Session Border Controller and PSTN network



6 Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Configuring the RingCentral BYOC Environment. **In this SBC config, RingCentral BYOC side is secure (TLS/SRTP) and** PSTN side is unsecure (UDP or TCP/RTP).

6.1 Validated Oracle SBC Version

Oracle conducted tests with Oracle SBC 9.3 software – this software with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6300
- AP 6350
- AP 3950
- AP 4900
- VME

6.2 New SBC configuration

If the customer is looking to setup a new SBC from scratch, please follow the sections given below.

As there are many ways to install the SBC (purpose-built appliance, VM, and public cloud deployment), please follow the link given below for the type of install base used to deploy the Oracle SBC.

https://docs.oracle.com/en/industries/communications/session-border-controller/9.3.0/installation/index.html

Once the SBC is installed and logged in, please follow the steps given below.

6.2.1 Setup product

To configure product type, type in "*setup product*" in the terminal Setup.

```
NN4600-139# setup product

-------------------------------------------------------------
WARNING:
Alteration of product alone or in conjunction with entitlement
changes will not be complete until system reboot

Last Modified 2023-02-07 15:50:20
-------------------------------------------------------------
 1 : Product       : Enterprise Session Border Controller

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]:
```

6.2.2 Setup Entitlements

Enable features for the ESBC using the "*setup entitlements*" command as shown below.

```
Entitlements for Enterprise Session Border Controller
Last Modified: Never
------------------------------------------------------------
 1 : Session Capacity                       : 0
 2 :   Advanced                             :
 3 : Admin Security                         :
 4 : Data Integrity (FIPS 140-2)            :
 5 : Transcode Codec AMR Capacity           : 0
 6 : Transcode Codec AMRWB Capacity         : 0
 7 : Transcode Codec EVRC Capacity          : 0
 8 : Transcode Codec EVRCB Capacity         : 0
 9 : Transcode Codec EVS Capacity           : 0
 10: Transcode Codec OPUS Capacity          : 0
 11: Transcode Codec SILK Capacity          : 0

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Session Capacity (0-128000)               : 500

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 3

************************************************************
CAUTION: Enabling this feature activates enhanced security
functions. Once saved, security cannot be reverted without
resetting the system back to factory default state.
************************************************************
  Admin Security (enabled/disabled)         :

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 5

  Transcode Codec AMR Capacity (0-102375)   : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2

    Advanced (enabled/disabled)             : enabled

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10

  Transcode Codec OPUS Capacity (0-102375)  : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 11

  Transcode Codec SILK Capacity (0-102375)  : 50
```

Save changes and reboot the SBC.

The SBC comes up after reboot and is now ready for configuration.

6.2.3 Enable Management GUI

ALCI Path: config t→system→http-server

Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

```
http-server
        name                                    webServerInstance
        state                                   enabled
        realm
        ip-address
        http-state                              enabled
        http-port                               80
        HTTP-strict-transport-security-policy   disabled
        https-state                             disabled
        https-port                              443
        http-interface-list                     GUI
        http-file-upload-size                   0
        tls-profile
        auth-profile
        last-modified-by                        @
        last-modified-date                      2020-10-06 00:28:26
NN4600-139#
```

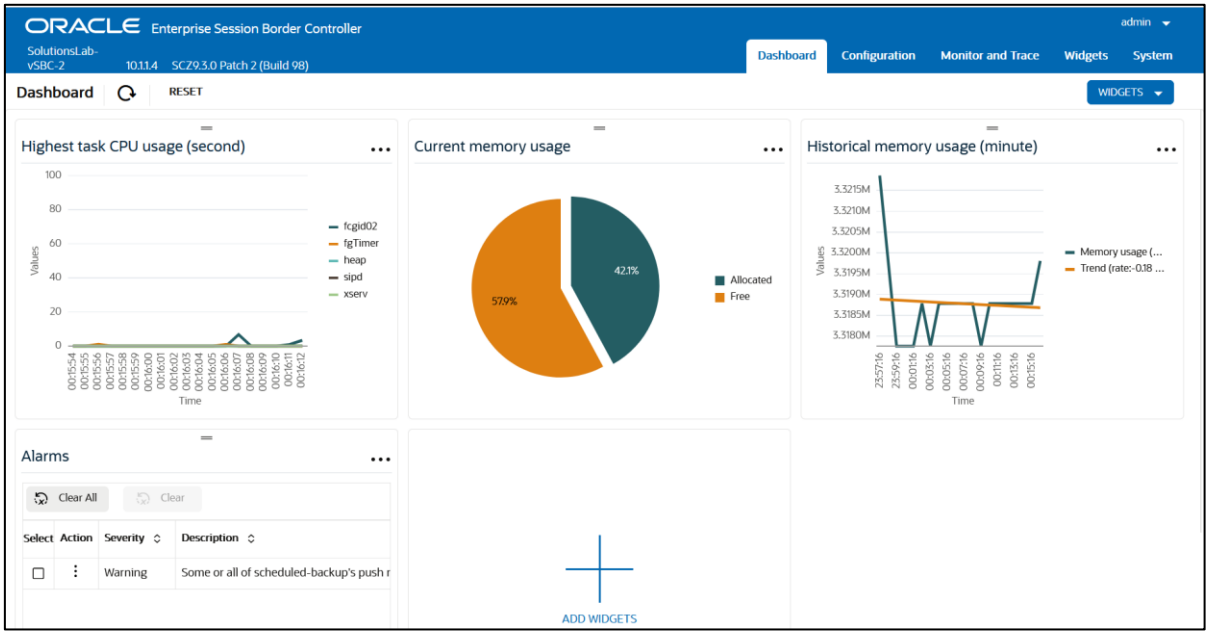
6.2.4 Configure SBC using Web GUI

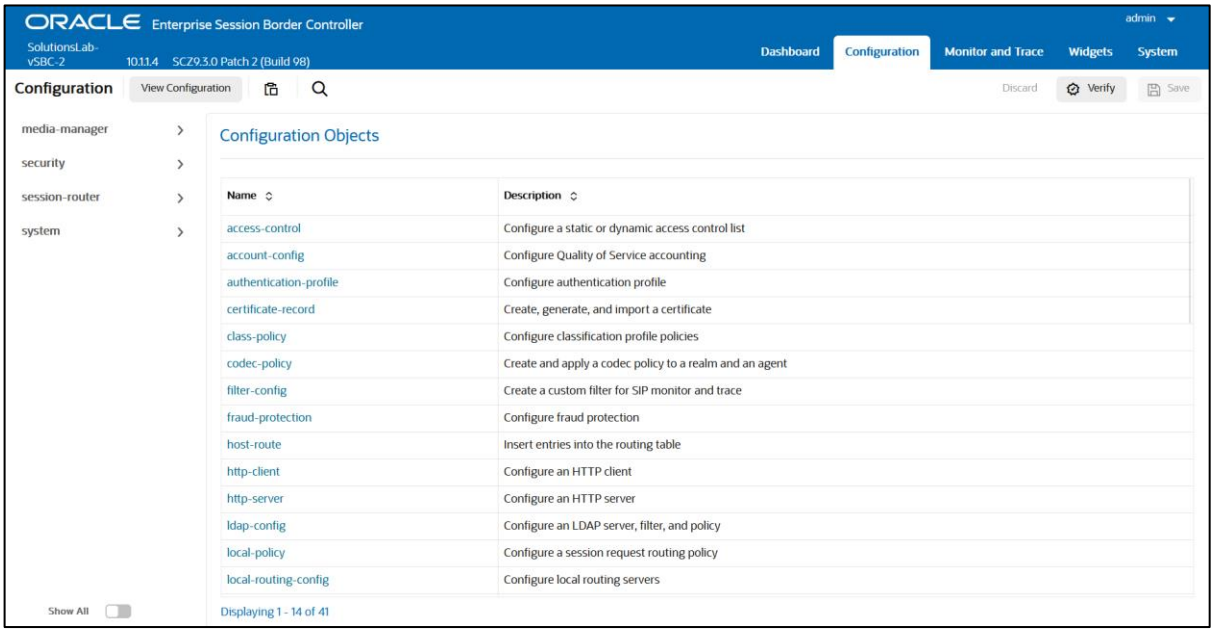
There are two methods for configuring the SBC, ACLI or GUI. For the purposes of this note, we'll be using the SBC GUI for all configuration examples. We will however provide the ACLI path to each element.

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

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

Note: the configuration examples below were captured from a system running the latest GA software, 9.3.0





Refer to the SBC GUI User Guide for more information:

https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.3.0/webgui/web-gui-guide.pdf

Note: Expert Mode is used when adding or modifying the SBC configuration

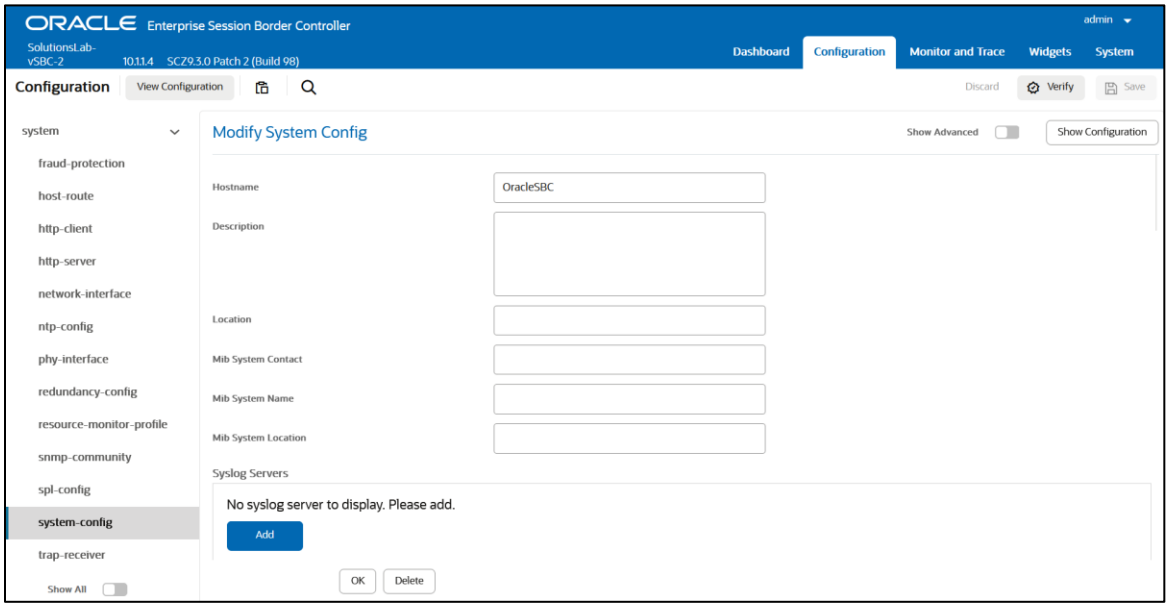
Tip: To make this configuration simpler, directly search the element to be configured from the Objects tab available.

6.3 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



If media transcoding is required in your environment and the SBC is deployed as VME SBC or in a public cloud, you'll need to enable transcoding cores under the system config element. Please see the document below for more information:

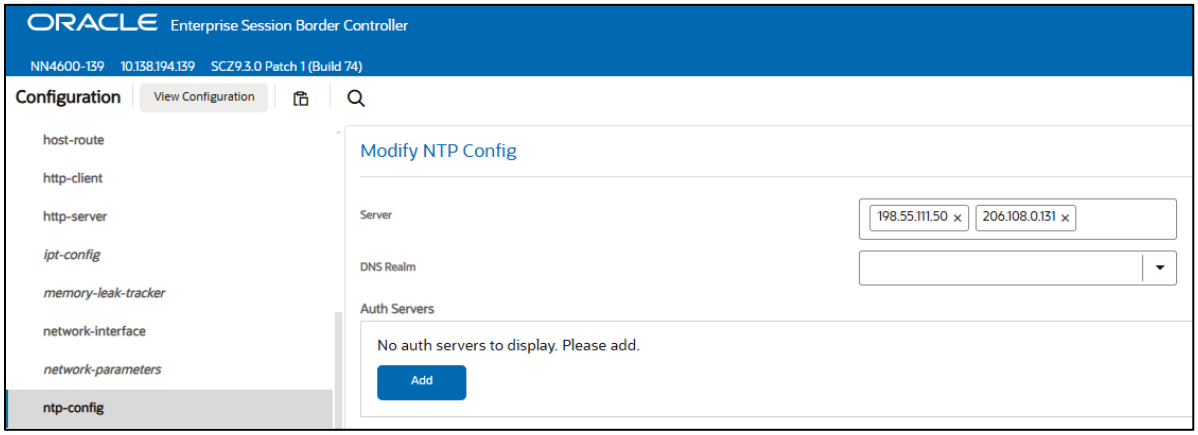
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.3.0/releasenotes/esbc-release-notes.pdf

6.3.1 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



- Select OK at the bottom

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

6.4 Networking 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 RingCentral BYOC, other to connect to PSTN Network.

Note: The slots and ports used in this example may be different from your network setup.

6.4.1 Physical Interfaces

GUI Path: system/phy-interface

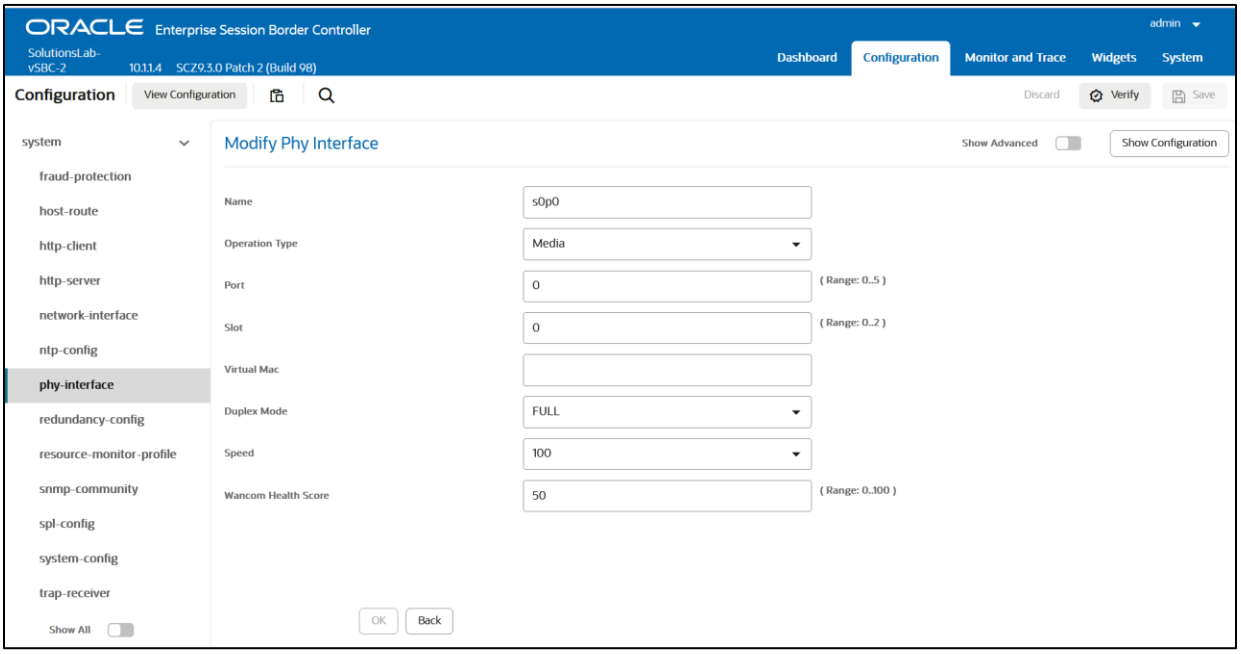
ACLI Path: config t→system→phy-interface

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

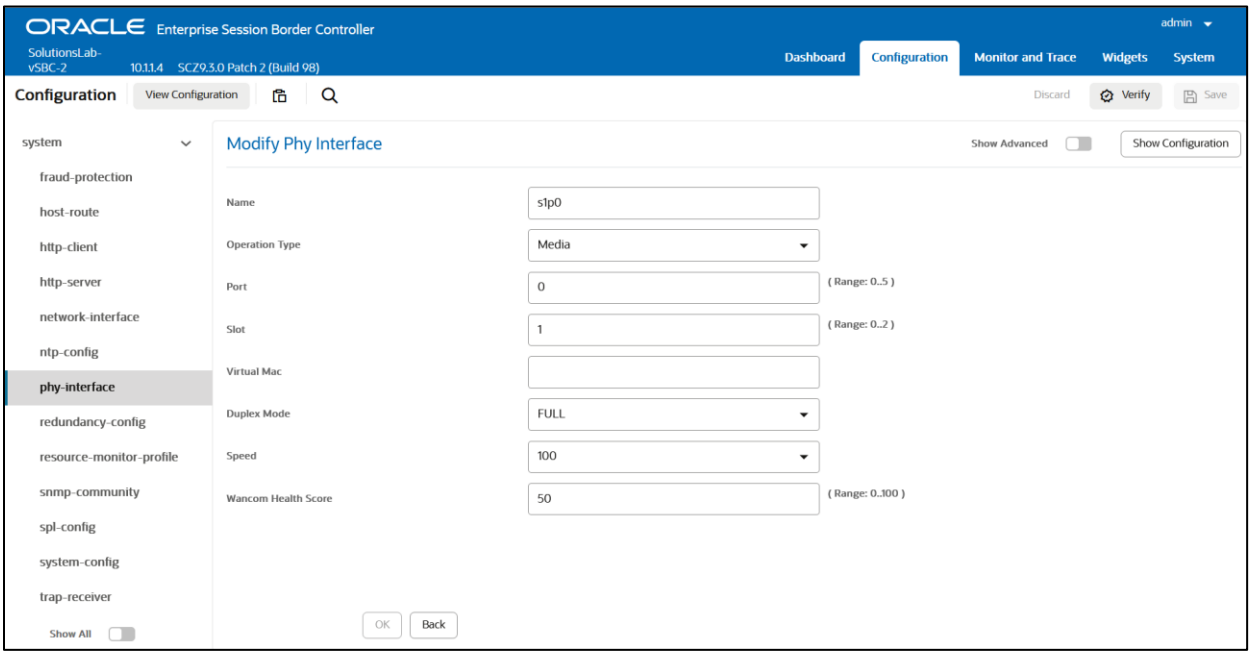
Parameter Name	PSTN side (s0p0)	RingCentral (s1p0)
Slot	0	1
Port	0	0
Operation Mode	Media	Media

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

Please configure s0p0 interface as below



Please configure s1p0 interface as below



6.4.2 Network Interfaces

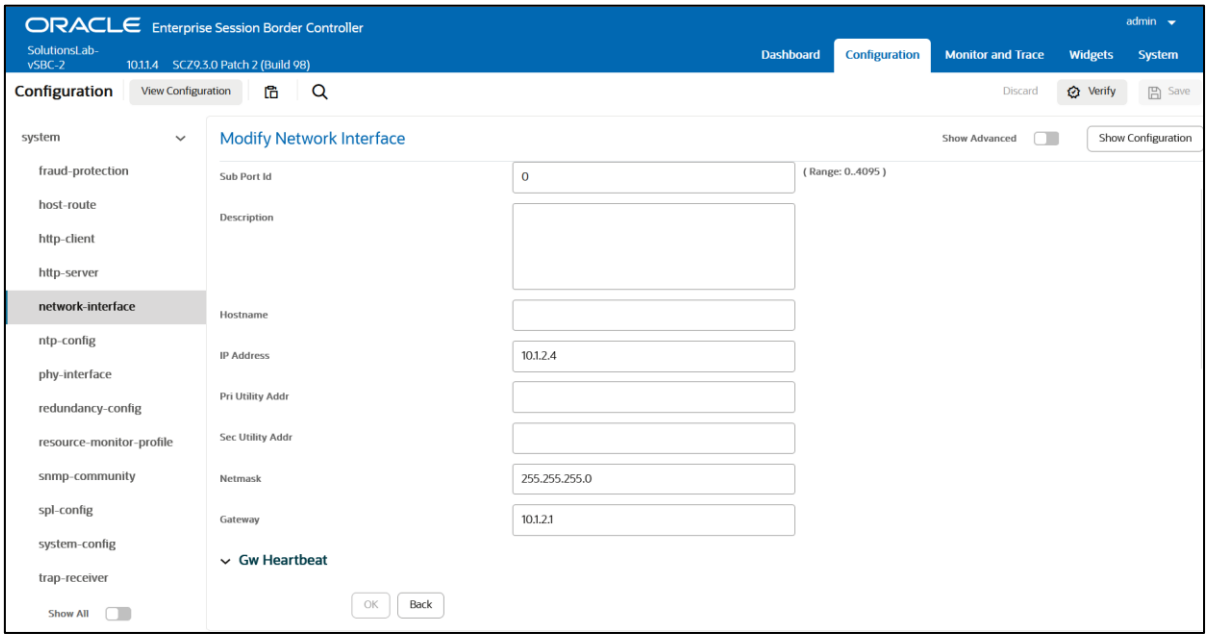
GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

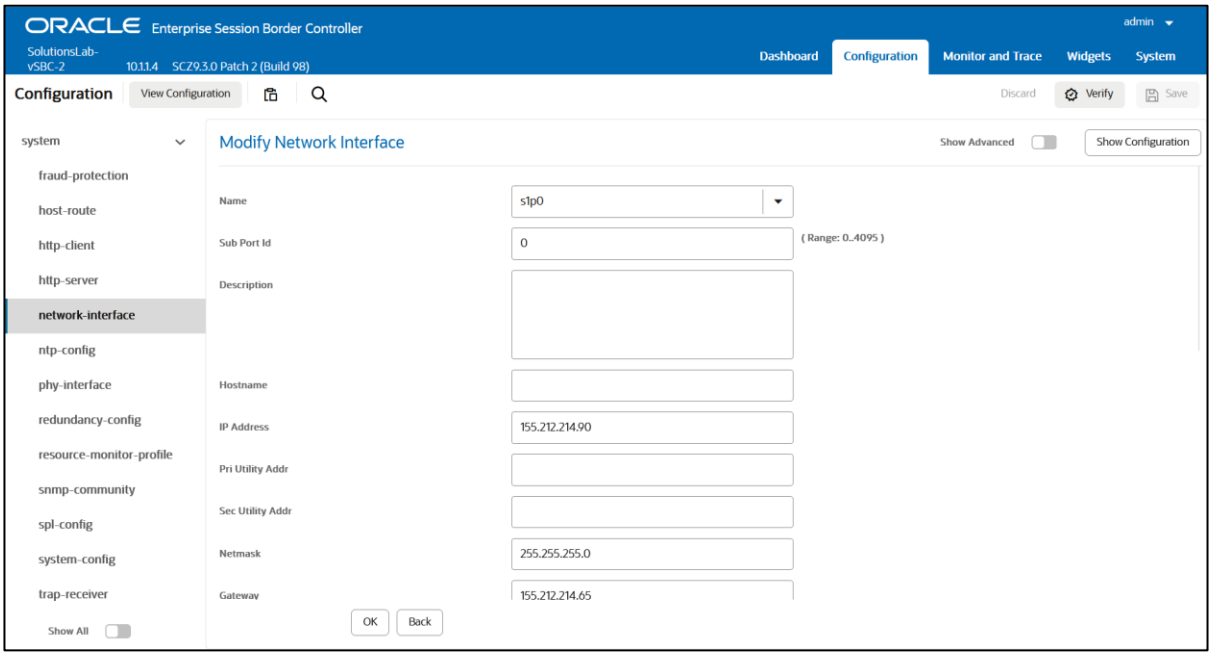
- Click Add, use the following table as a configuration example:

Config Parameter	PSTN	RingCentral
Name	s0p0	S1p0
IP Address	10.1.2.4	155.212.214.90
Netmask	255.255.255.0	255.255.255.0
Gateway	10.1.2.1	155.212.214.65

Please configure network interface s0p0 as below



Similarly, configure network interface s1p0 as below



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

Next, we'll configure the necessary elements to setup Media on the SBC.

6.5 Security Configuration

This section describes how to configure the SBC for TLS and SRTP communication for RingCentral BYOC.

RingCentral allows TLS connections from SBCs for SIP traffic, and SRTP for media traffic along with other non-secure transport methods which are TLS-Unencrypted SRTP / TLS-RTP/ TCP-RTP. For the purposes of this application note, we'll focus only on TLS/SRTP.

6.5.1 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 two certificate records. The are as follows:

- SBC Certificate (end-entity certificate)
- GoDaddy Root Cert (Root CA used to sign the SBC's end entity certificate)

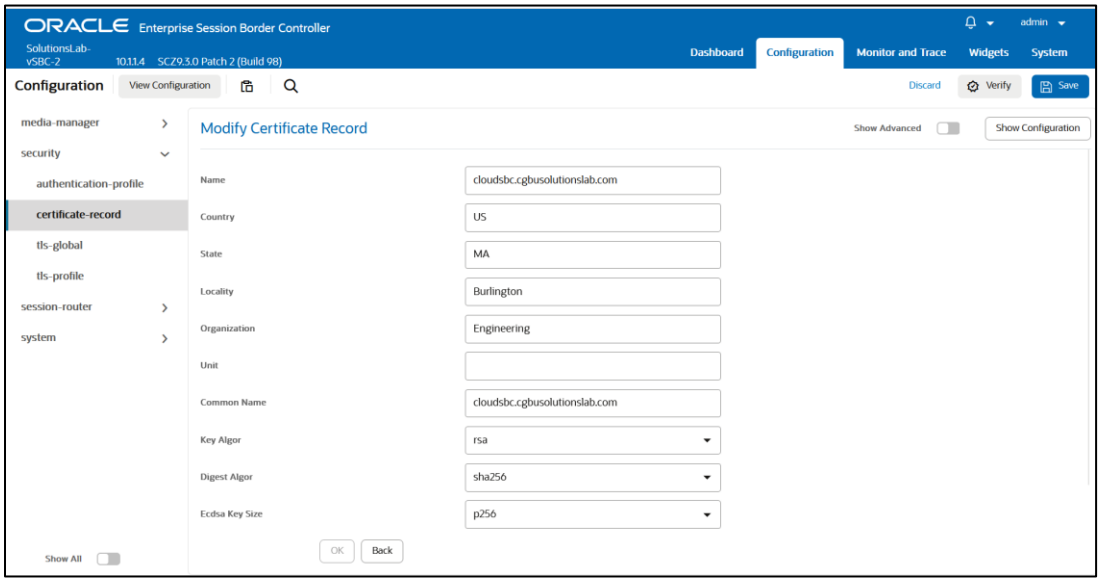
Note: Most deployments typically require additional root and intermediate certificates. However, in this instance, both Oracle and RingCentral use the same certificate authority, GoDaddy so these extra certificates are not needed.

6.5.1.1 SBC End Entity Certificate

The SBC's end entity certificate is the certificate the SBC presents to Ring Central to secure the connection. The only requirements when configuring this certificate is the common name must contain the SBC's FQDN and the extended key usage list must contain both serverAuth and clientAuth. In this example our common name will be cloudsbc.cgbusolutionslab.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



- Click OK at the bottom

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

6.5.1.2 Root CA Certificates

The following, GoDaddyRoot, is the root CA certificate used to sign both the SBC's end entity certificate as well as the certificate Ring Central presents to the SBC to secure the connection. As mentioned above, your root CA and/or intermediate certificate may differ. This is for example purposes only.

You can download the Ring Central Root CA certificate bundle here:

https://certs.godaddy.com/repository/gd_bundle-g2-g1.crt

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

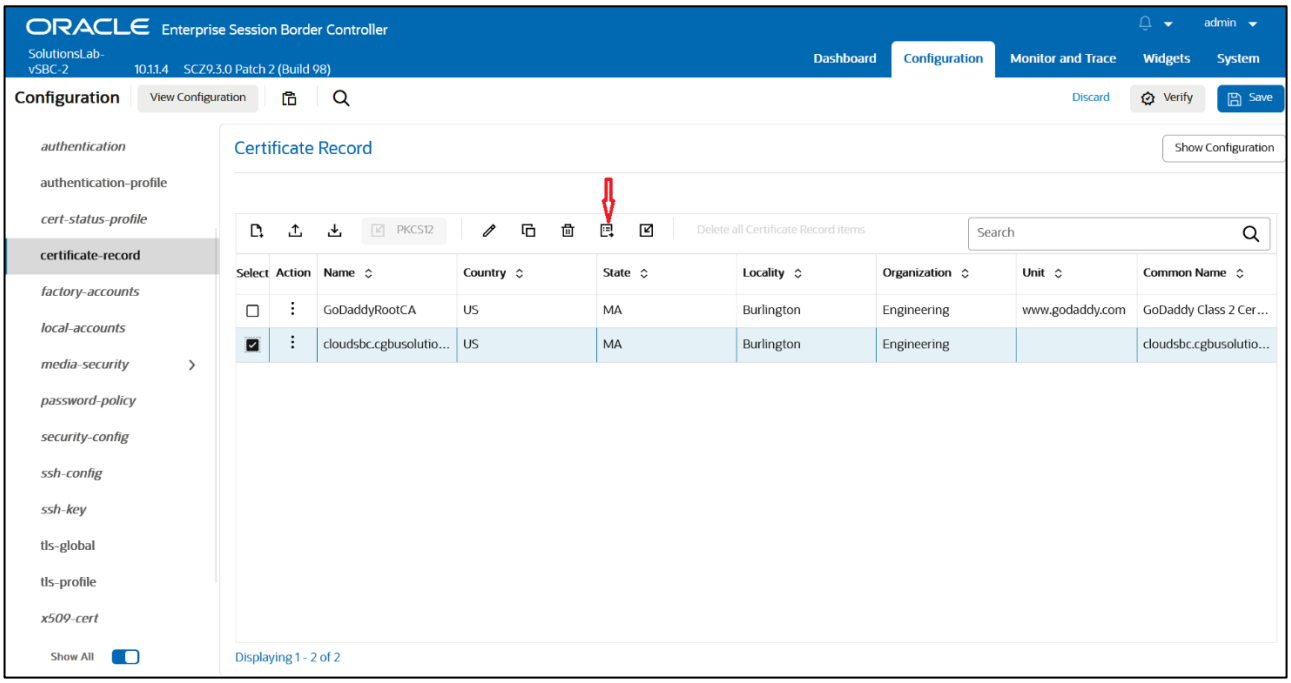
Config Parameter	GoDaddy Root CA
Common Name	GoDaddy Root CA
Key Size	2048
Key-Usage-List	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth clientAuth
Key algor	rsa
Digest-algor	Sha256

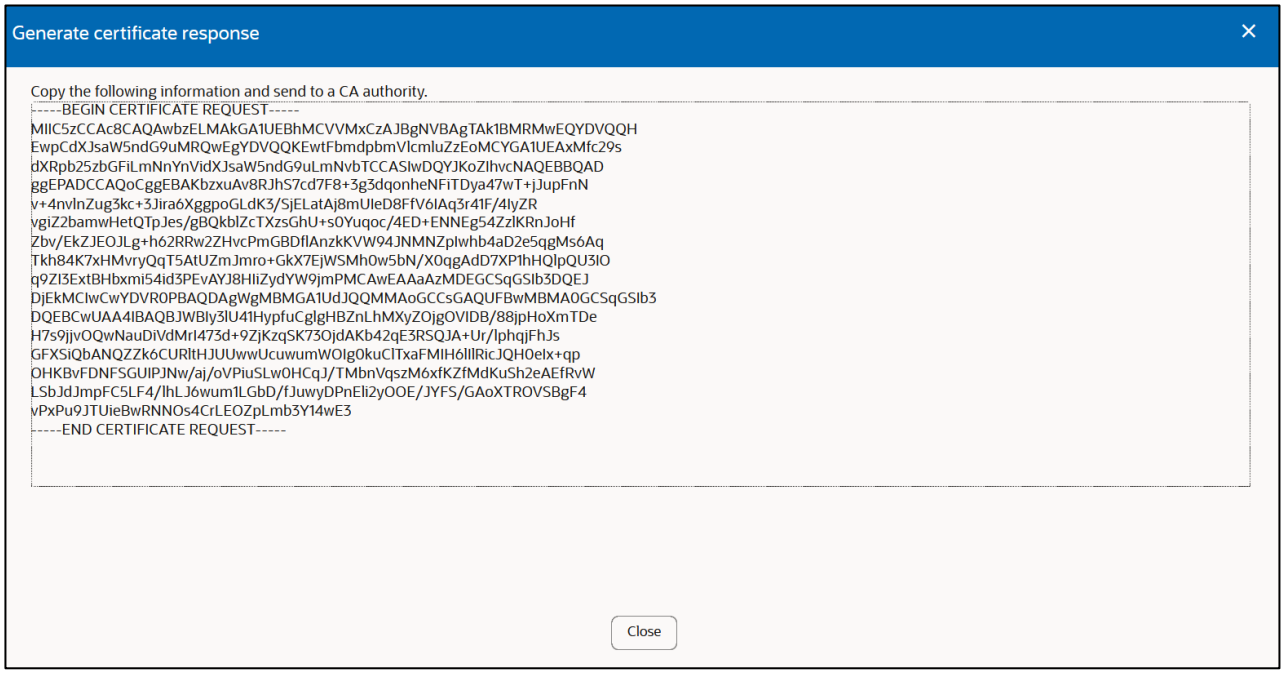
At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must save and activate the configuration of the SBC.

6.5.1.3 Generating a 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 intermediate 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:



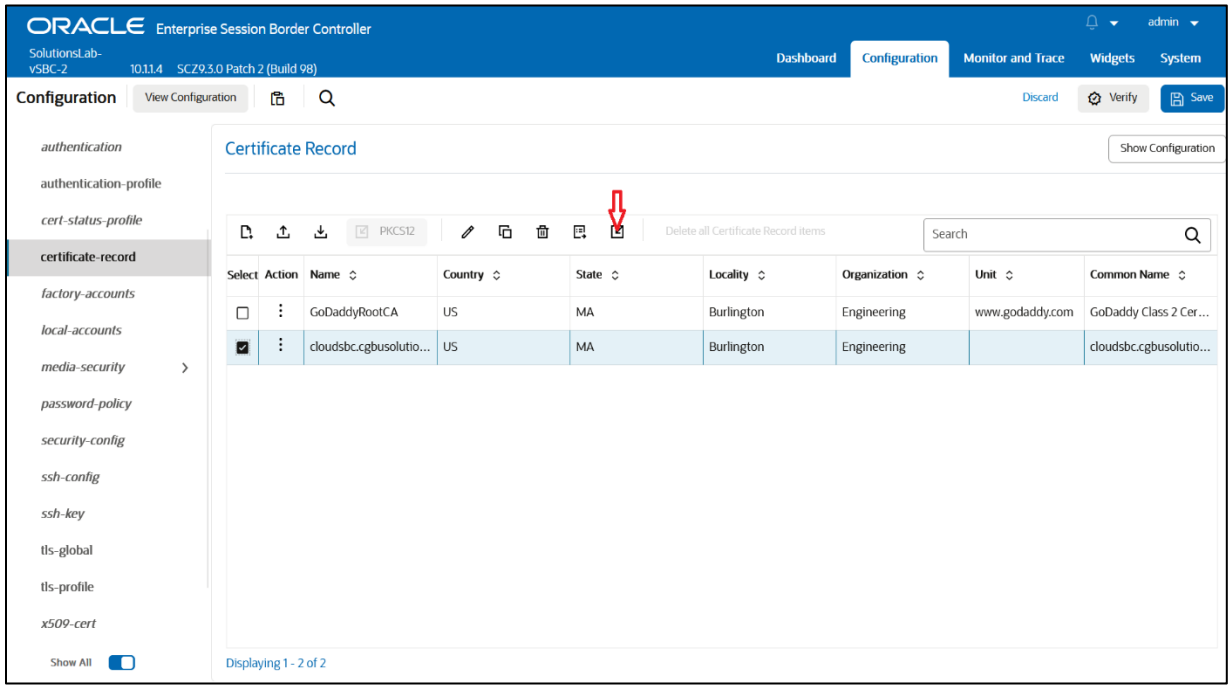


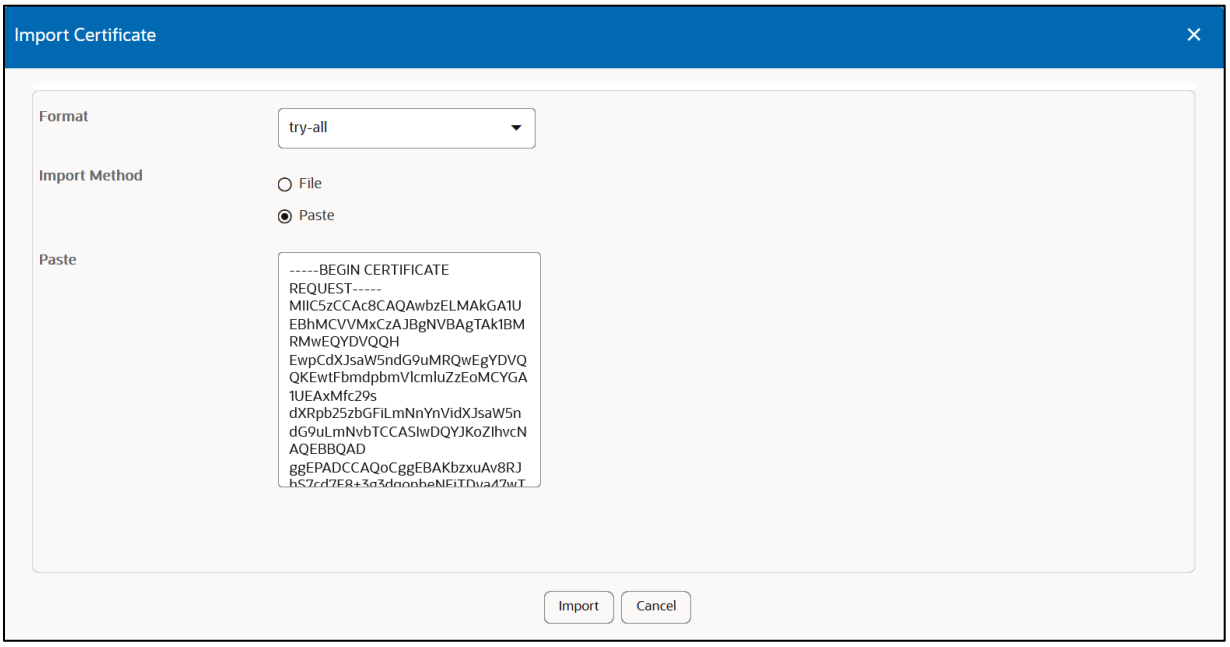
Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, another save and activate is required before you can import the certificates to each certificate record created above.

6.5.1.4 Import Certificates to SBC

Once certificate signing request have 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 done, issue save/activate from the WebGUI to complete the configuration of certificate records on the Oracle SBC.





Once pasted 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:

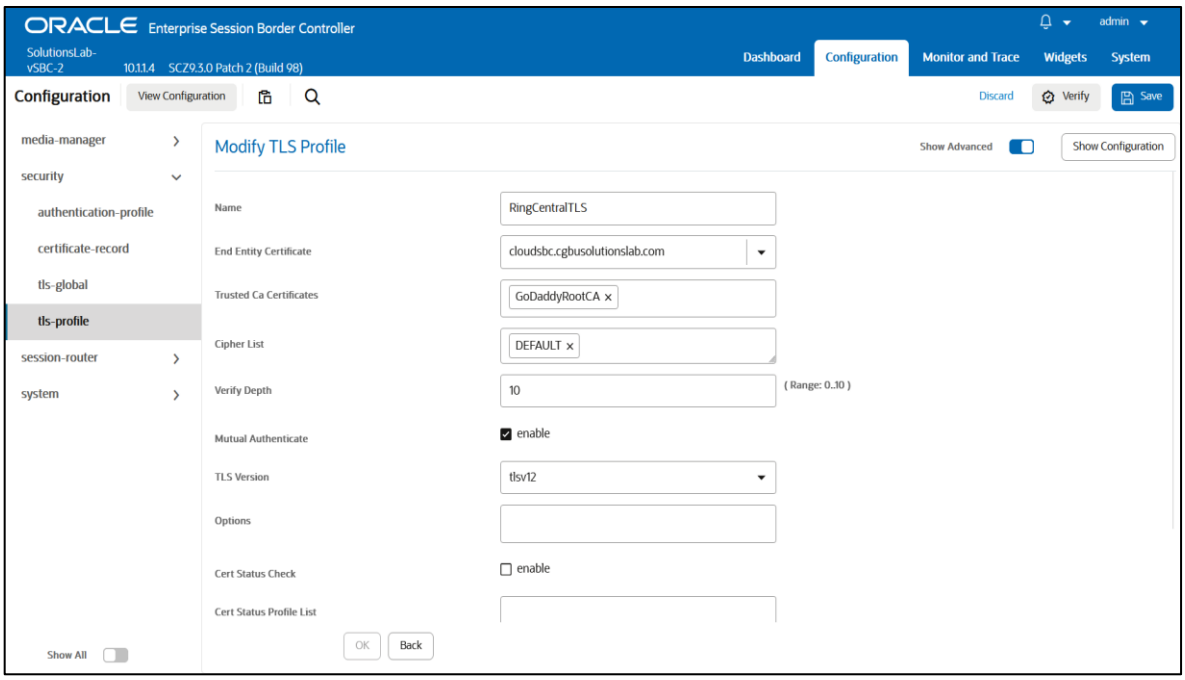
6.5.2 TLS-Profile

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:



- Select OK at the bottom

Next, we'll move to securing media between the SBC and Microsoft Teams.

6.5.3 Media Security

This section outlines how to configure support for media security between the OCSBC and Ring Central.

6.5.3.1 sdes-profile

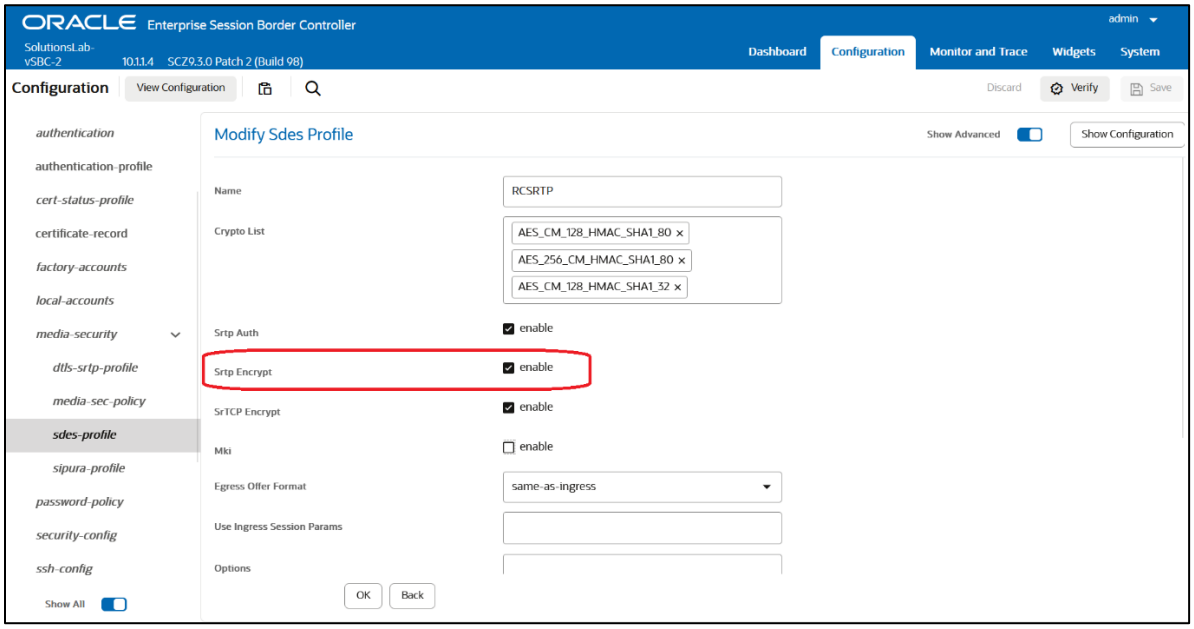
This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured.

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 →security→media-security→sdes-profile

Click Add, and use the example below to configure:



Also, please disable the “Srtp Encrypt” parameter shown above for the TLS/Unencrypted SRTP session.

- Select OK at the bottom

6.5.3.2 Media Security Policy

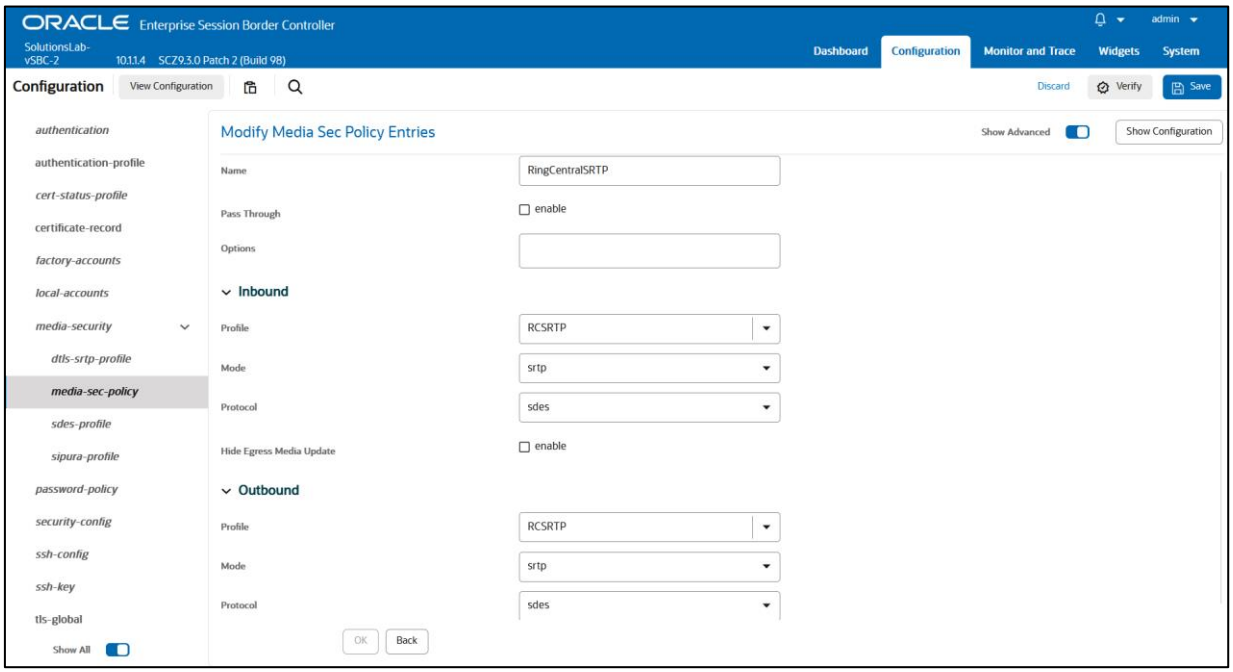
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any) and, if SRTP needs to be used, the sdes-profile that needs to be used.

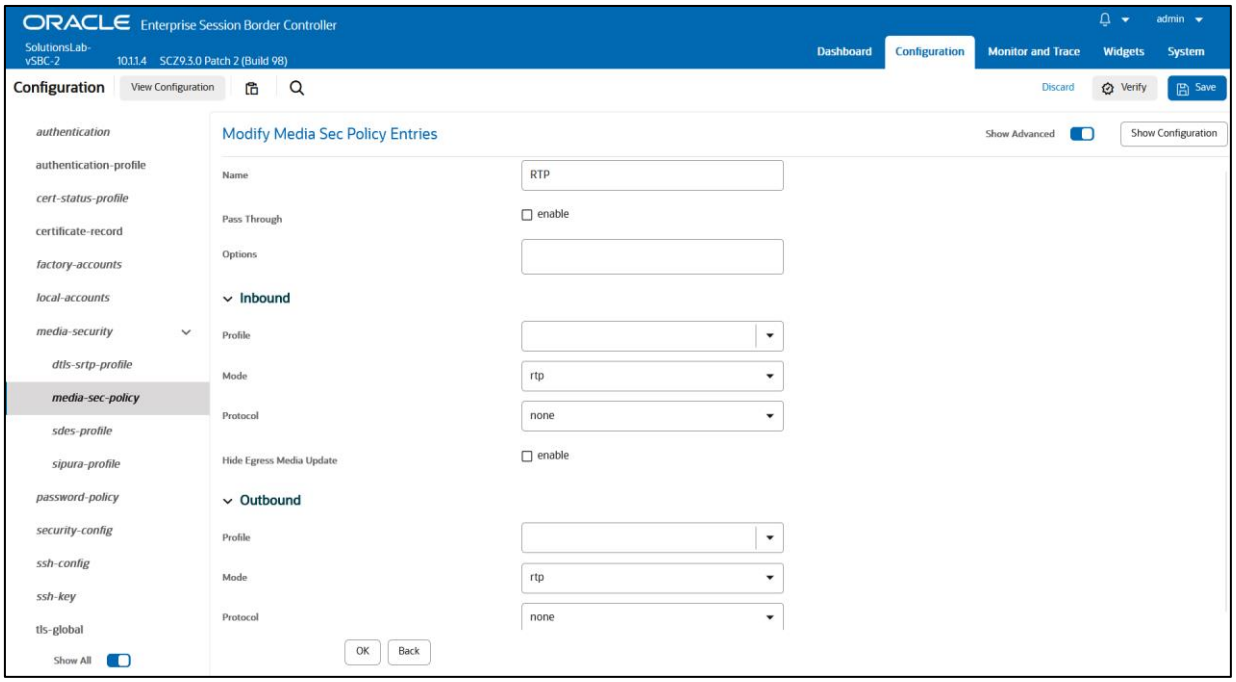
In this example, we are configuring two media security policies. One to secure and decrypt media toward Ring Central, the other for non-secure media facing PSTN.

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:


ORACLE Enterprise Session Border Controller
admin
SolutionsLab-vSBC-2 10.1.1.4 SCZ9.3.0 Patch 2 (Build 98)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
Save
authentication
authentication-profile
cert-status-profile
certificate-record
factory-accounts
local-accounts
media-security
dtls-srtp-profile
media-sec-policy
sdes-profile
sipura-profile
password-policy
security-config
ssh-config
ssh-key
tls-global
Show All
Modify Media Sec Policy Entries
Show Advanced
Show Configuration
Name
RingCentralSRTP
Pass Through
enable
Options
Inbound
Profile
RCSRTP
Mode
srtp
Protocol
sdes
Hide Egress Media Update
enable
Outbound
Profile
RCSRTP
Mode
srtp
Protocol
sdes
OK
Back


ORACLE Enterprise Session Border Controller
admin
SolutionsLab-vSBC-2 10.1.1.4 SCZ9.3.0 Patch 2 (Build 98)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
Save
authentication
authentication-profile
cert-status-profile
certificate-record
factory-accounts
local-accounts
media-security
dtls-srtp-profile
media-sec-policy
sdes-profile
sipura-profile
password-policy
security-config
ssh-config
ssh-key
tls-global
Show All
Modify Media Sec Policy Entries
Show Advanced
Show Configuration
Name
RTP
Pass Through
enable
Options
Inbound
Profile
Mode
rtp
Protocol
none
Hide Egress Media Update
enable
Outbound
Profile
Mode
rtp
Protocol
none
OK
Back

6.6 Media Configuration

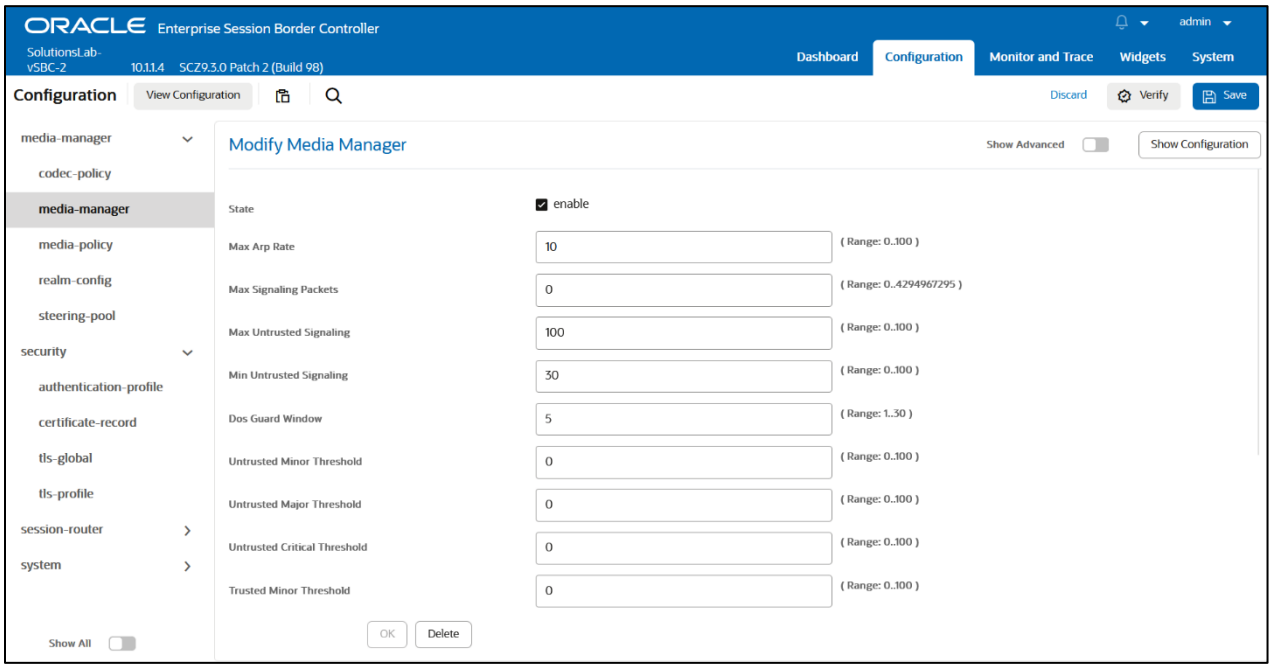
This section will guide you through the configuration of media manager, realms, and steering pools, all of which are required for the SBC to handle signaling and media flows through the SBC.

6.6.1 Media Manager

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

GUI Path: media-manager/media-manager

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



- Click OK at the bottom.

6.6.2 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

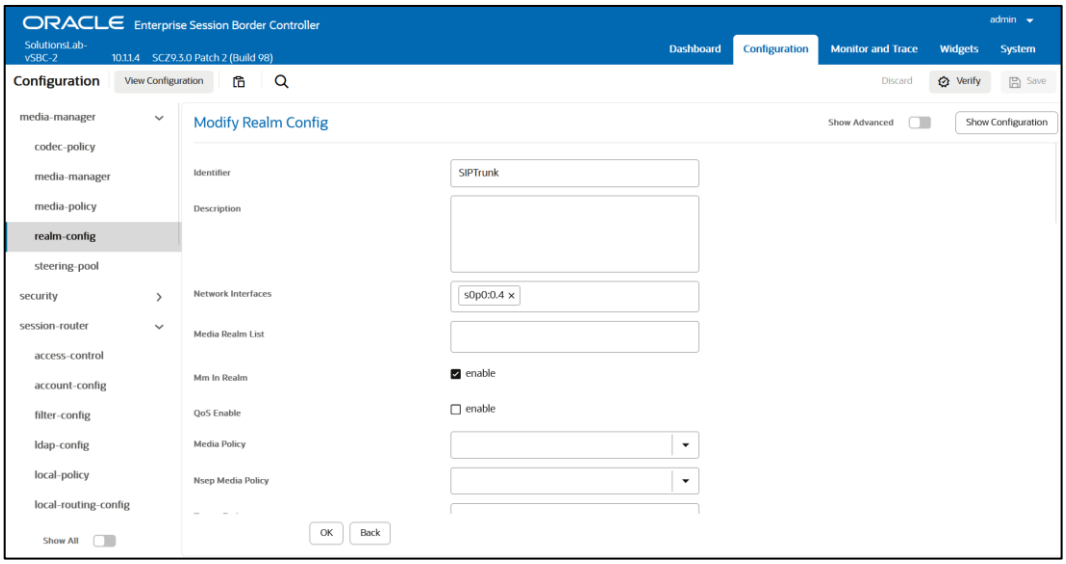
ACLI Path: config t→media-manger→realm-config

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	PSTN	RingCentral
Identifier	SIPTrunk	RingCentral
Network Interface	s0p0	S1p0
MM in Realm	☑	☑
Access Control trust level	High	High
Media Sec Policy		RingCentralSRTP

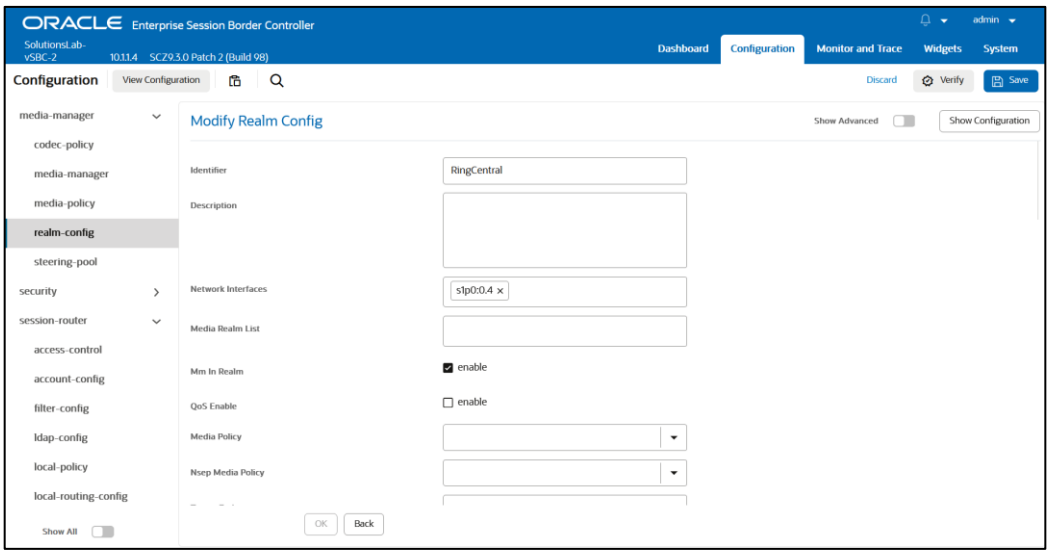
In the below case, Realm name is given as **SIPTrunk** for PSTN.

Please set the Access Control Trust Level as high for this realm



Similarly, Realm name is given as **RingCentral** for RingCentral BYOC.

Please set the Access Control Trust Level as high for this realm too.



- Select OK at the bottom of each.

6.6.3 Steering Pools

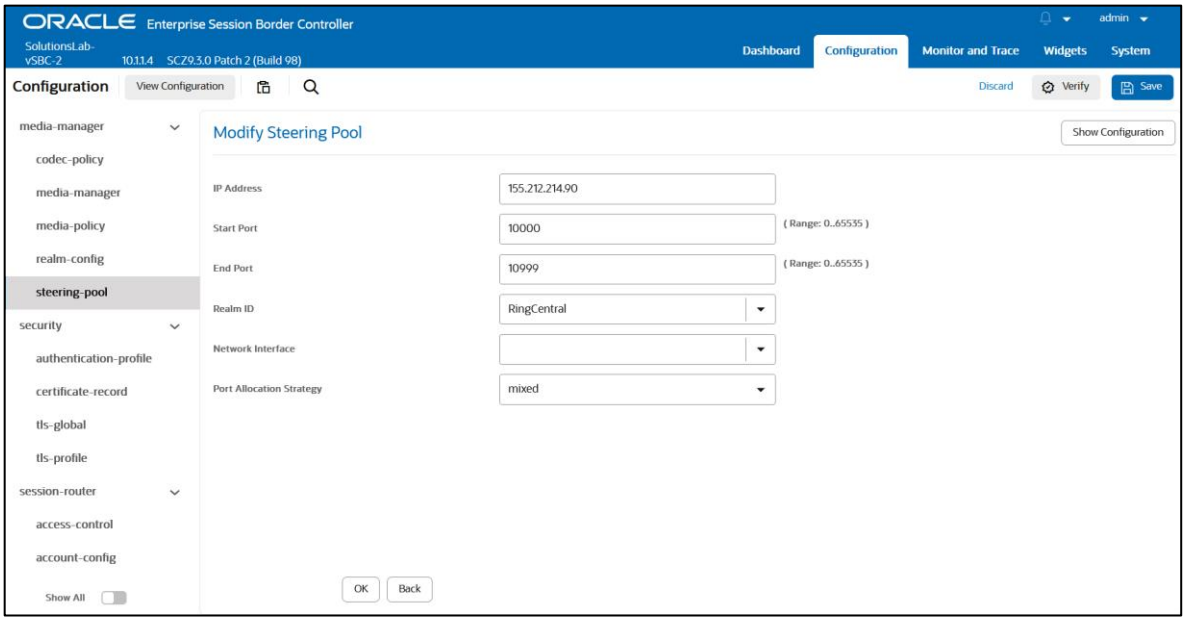
Steering pools define sets of ports that are used for steering media flows through the OCSBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

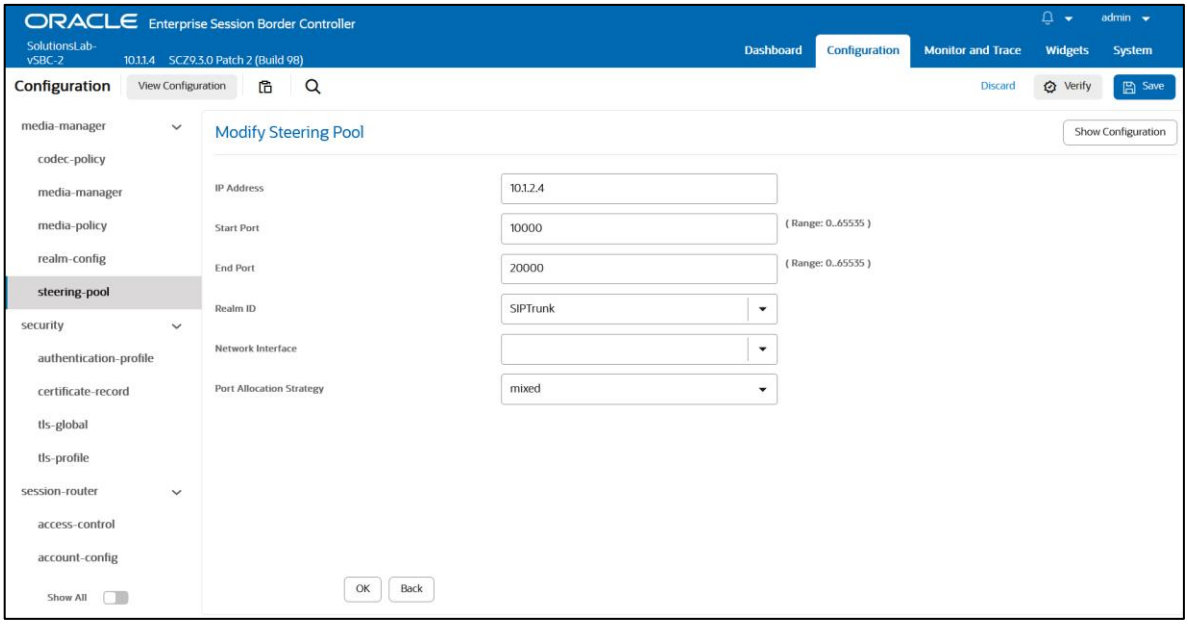
We configure one steering pool for PSTN. The other for Ring Central

GUI Path: media-manger/steering-pool

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

Click Add and use the below examples to configure.





- Select OK at the bottom of each.

6.7 Sip Configuration

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

6.7.1 Sip-Config

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

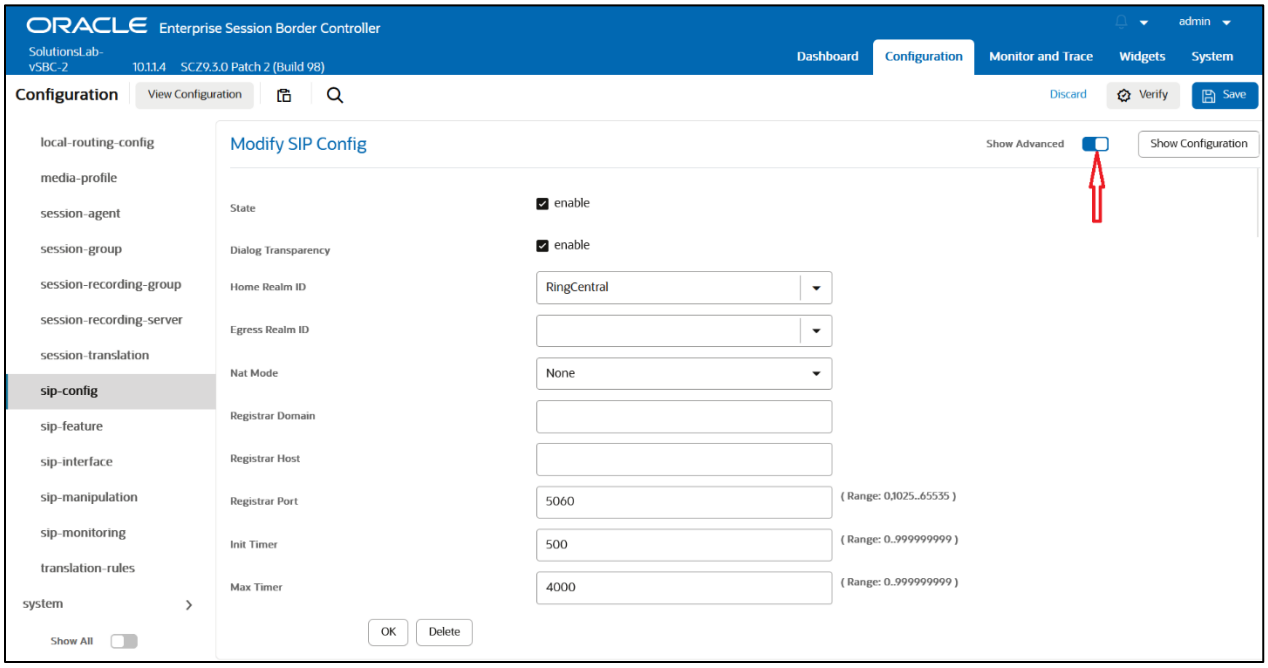
GUI Path: session-router/sip-config

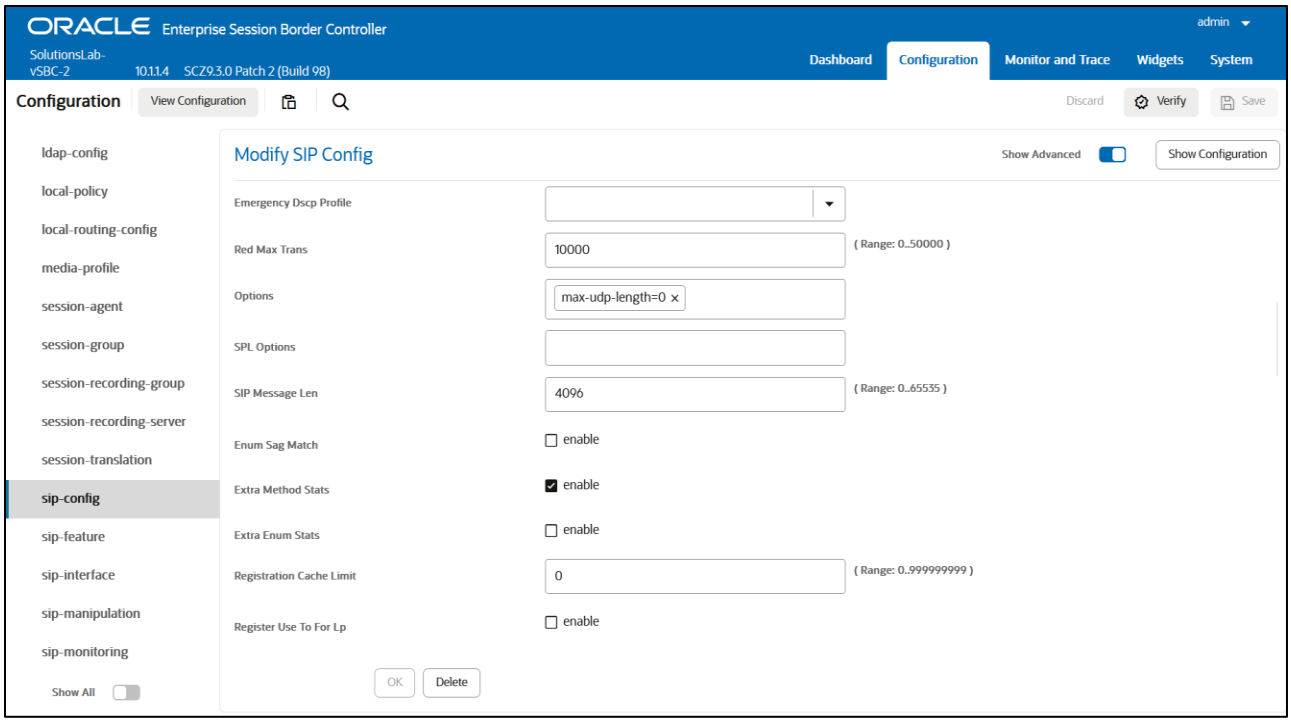
ACLI Path: config t→session-router→sip-config

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

- Set the home realm ID parameter to RingCentral 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).
- Enable sag-lookup-on-redirect if using a session agent group for your RingCentral platform.

Note: toggle show advanced to expose the "Option" parameter





- Select OK at the bottom.

6.7.2 Sip Interface

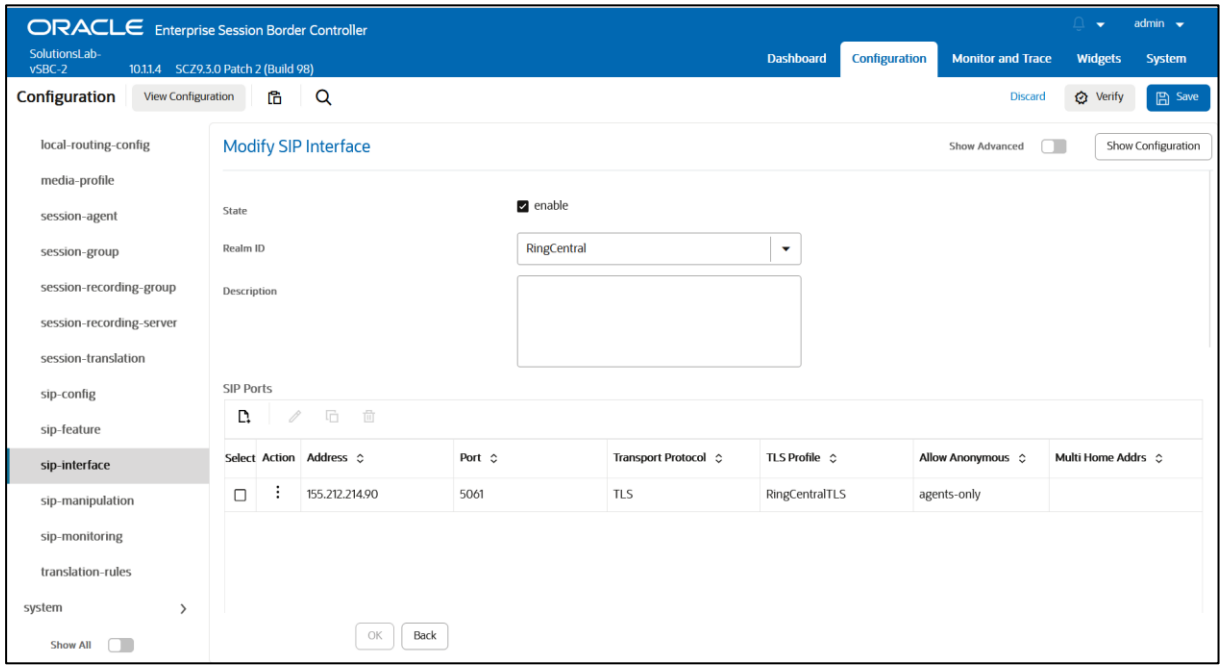
The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages.

GUI Path: session-router/sip-interface

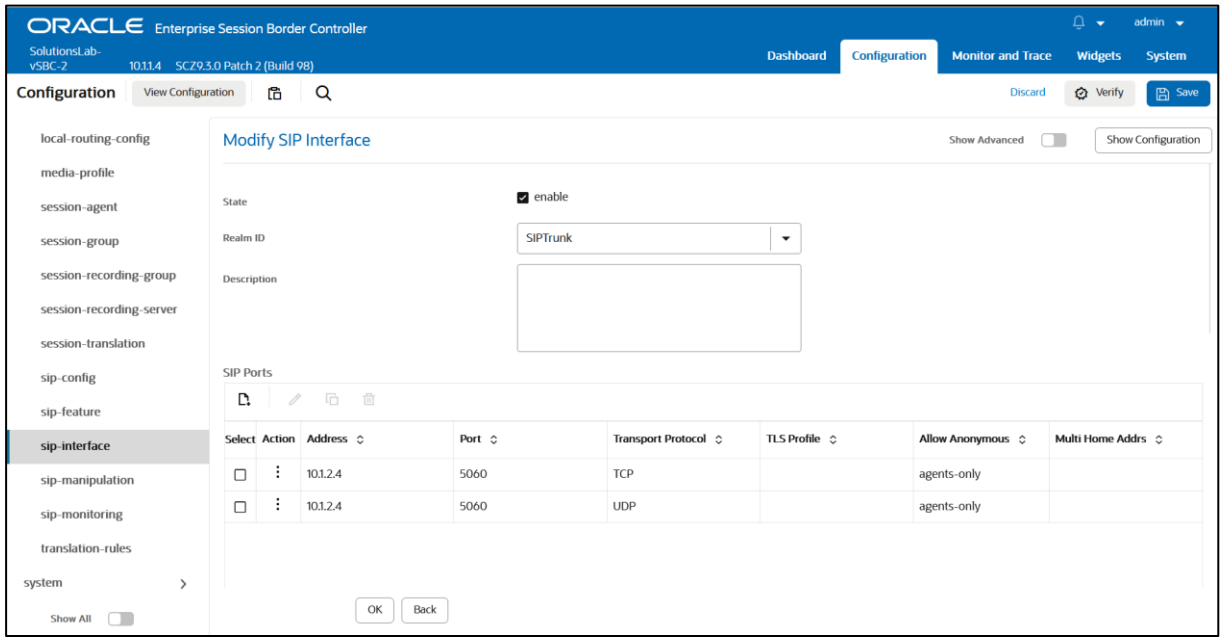
ACLI Path: config t→session-router→sip-interface

Please Configure sip-interface for the RingCentral BYOC as shown below:

- Tls-profile needs to match the name of the tls-profile previously created.
- Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from the particular Session agents added to the SBC.



Please Configure sip-interface for the PSTN as show below:



- Select OK at the bottom of each when applicable.

Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

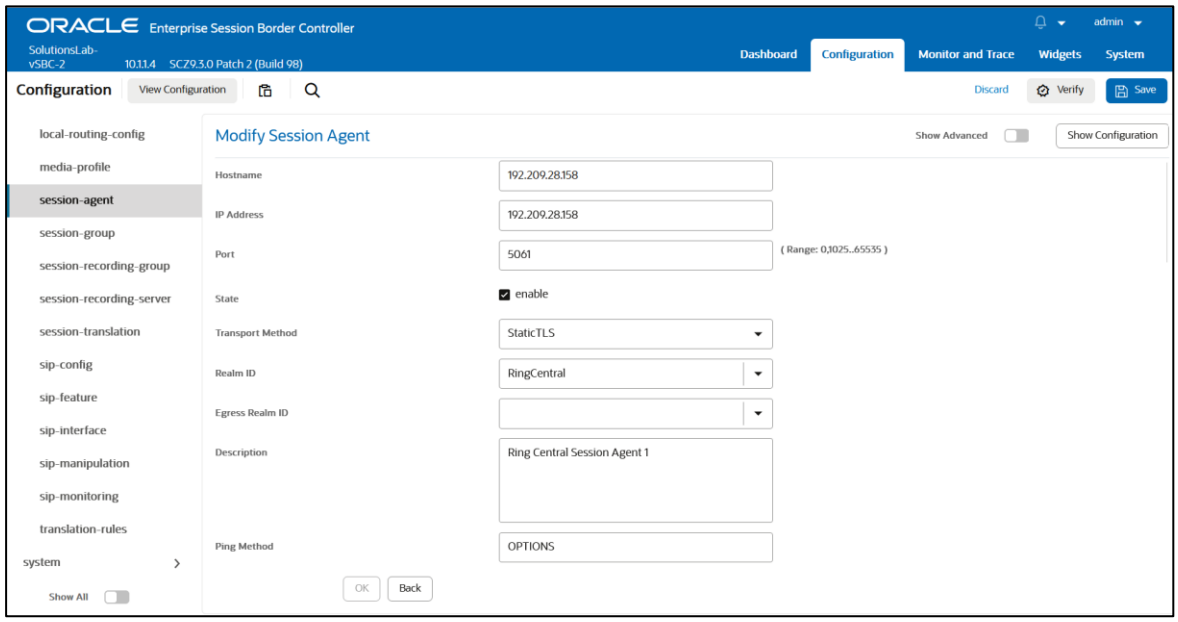
6.7.3 Session Agents

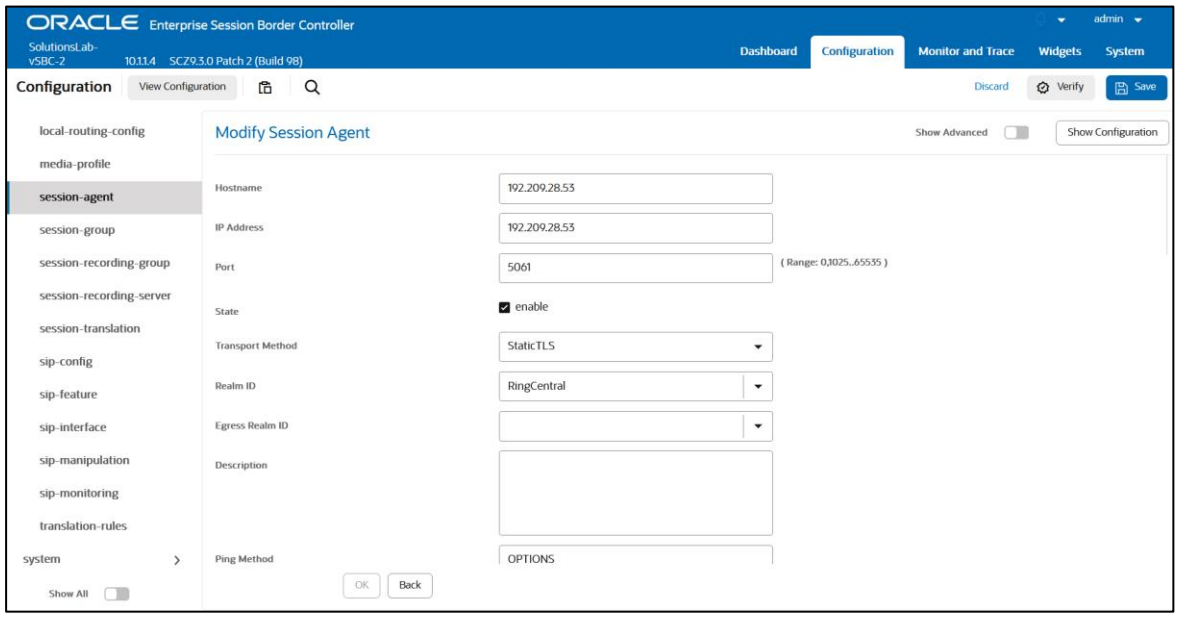
Session Agents are configuration elements which are trusted agents that can both send and receive traffic from the Oracle SBC with direct access to the trusted data path.

GUI Path: session-router/session-agent

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

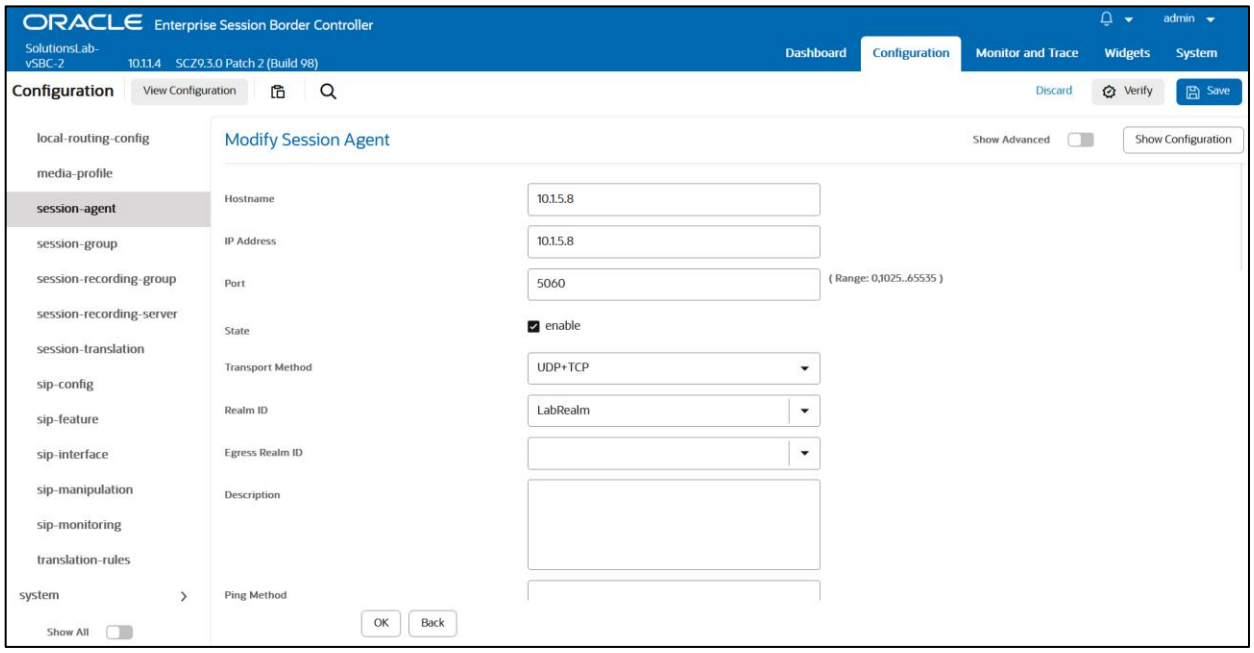
- transport set to “staticTLS”
- Please enable the parameter **ping-response**,
- Please set ping method to OPTIONS and ping-interval duration in secs





- Select OK at the bottom.

Similarly, configure the session-agents for the PSTN Side as below:

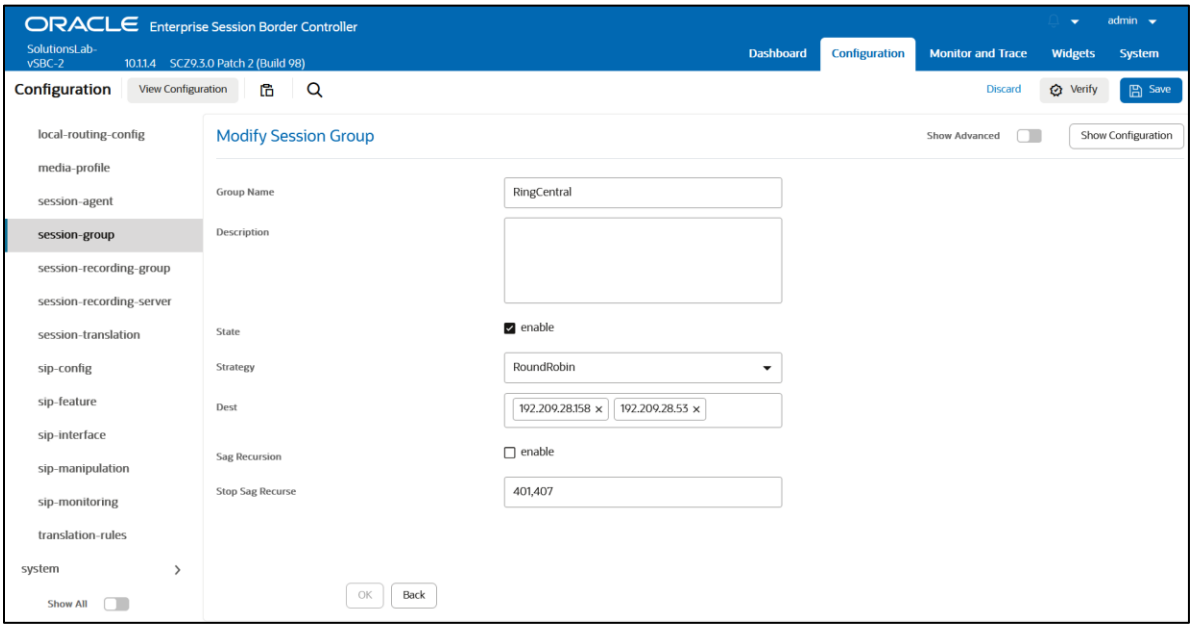


6.7.4 Session Group

A session agent group allows the SBC to create a load balancing model:

Session agents configured for the RingCentral in above section will be added to the group. The session agents listed under destination must be in this order, and the strategy to select the session agents can be selected by the End Users based on their needs and we have selected “RoundRobin” in this example.

Go to session-router-> session-group



6.8 Routing Configuration

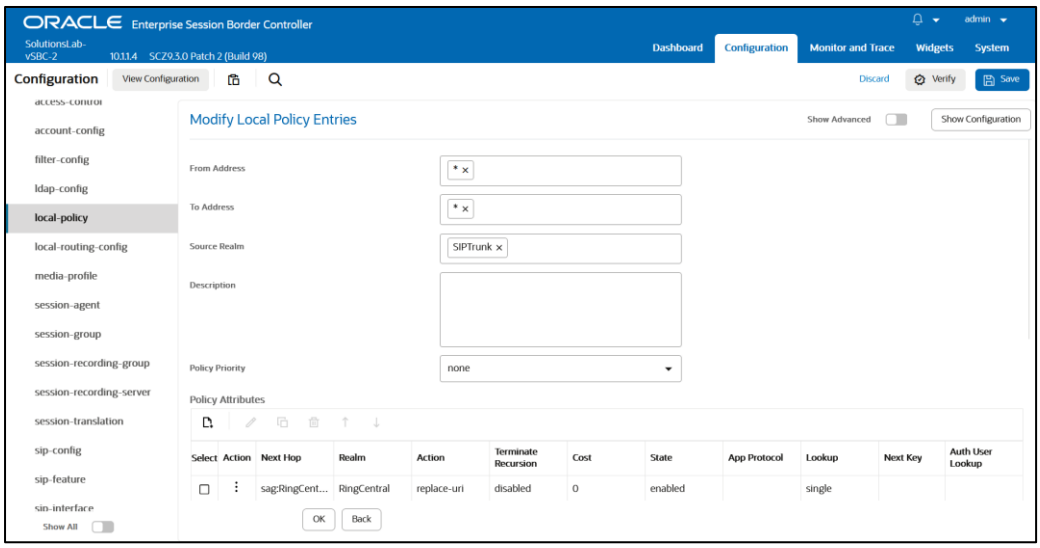
Now that most of the system, signaling, and media configuration is in place, we can configure the SBC to route calls from one end of the network to the other. The SBC has multiple routing features that can be utilized, but for the purposes of this example configuration, we'll configure local policies to route calls to and from PSTN and RingCentral BYOC.

6.8.1 Local Policy

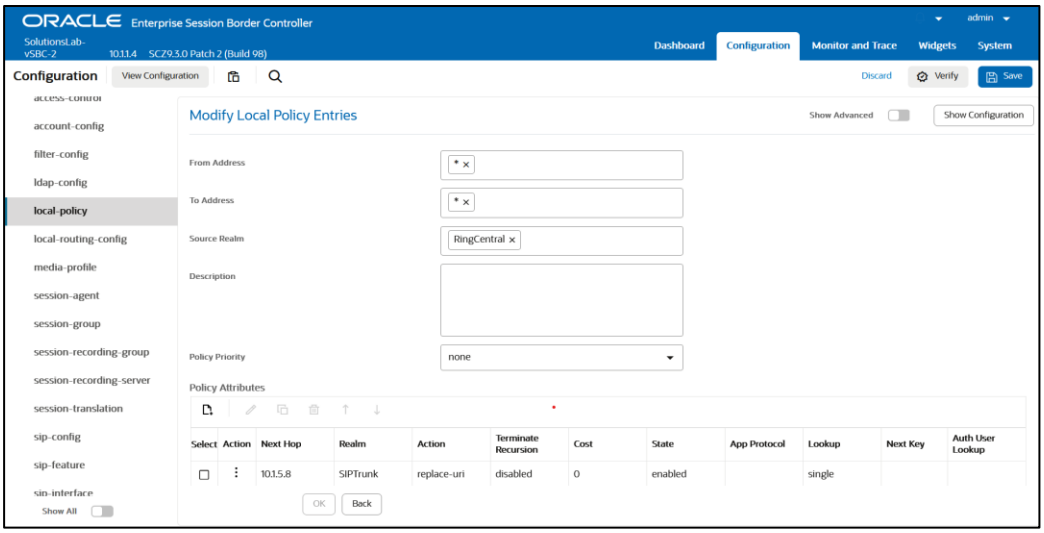
GUI Path: session-router/local-policy

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

To route the calls from PSTN side to RingCentral side, Use the below local policy.

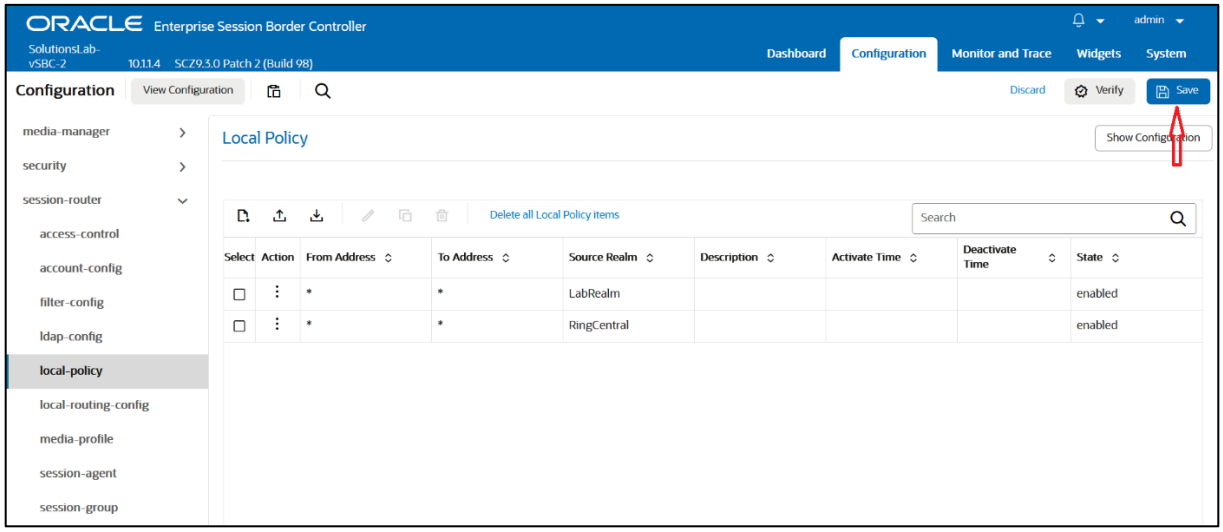


To route the calls from RingCentral side to PSTN side, Use the below local policy.

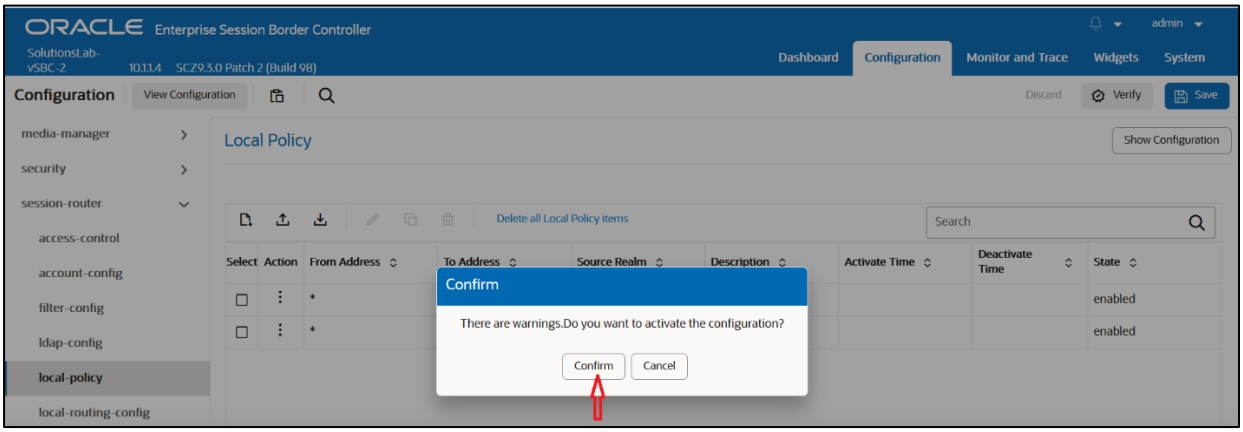


6.9 Save and Activate

6.9.1 Save Config



6.9.2 Activate Config



This concludes the minimum required configuration to successfully integrate RingCentral BYOC with your Oracle Session Border Controller.

7 Existing SBC configuration

If your environment has an Oracle SBC deployed with a fully functional configuration, the following configuration elements are required to integrate RingCentral BY into your existing config.

- Configuring a certificate for SBC Interface
- TLS-Profile
- SDES Profile
- Media-sec-Policy
- New realm-config
- New steering-pools
- New sip-interface
- New session-agent
- Session Group
- New local-policy

7 Appendix A

7.1 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 Ring Central SIP interface.

HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4

HeaderNatPublicSipIfIp is the public interface IP.
HeaderNatPrivateSipIfIp is the private IP.

To configure header NAT SPL from ACLI

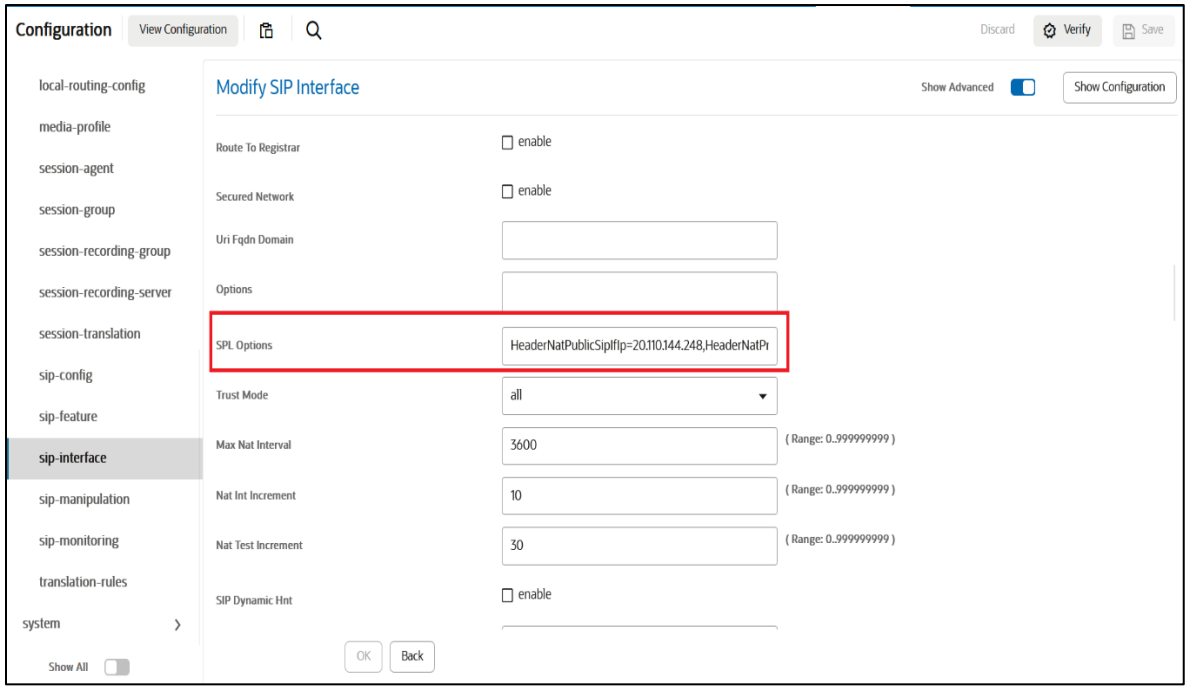
GUI Path: session-router/sip-interface

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

Choose the sip interface on which the header NAT SPL needs to be applied under spl-options.
Add the entry as per example shared below.

spl-options

HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4



- Perform a **save and activate** configuration for changes to take effect.

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

8 Appendix B

8.1 ACLI Running Config

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.

```
SolutionsLab-vSBC-2# show running-config short
access-control
        realm-id                        SIPTrunk
        source-address                      10.1.5.8
        application-protocol                SIP
        trust-level                     high
access-control
        realm-id                        RingCentral
        source-address                      192.209.0.0/16
        application-protocol                SIP
        trust-level                     high
certificate-record
        name                            GoDaddyRootCA
        unit                           www.godaddy.com
        common-name                         GoDaddy Class 2 Certification Authority Root Certificate
certificate-record
        name                            cloudsbc.cgbusolutionslab.com
        common-name                         cloudsbc.cgbusolutionslab.com
http-server
        name                            webserver
local-policy
        from-address                      *
        to-address                       *
        source-realm                      RingCentral
        policy-attribute
                next-hop                        10.1.5.8
                realm                          SIPTrunk
                action                         replace-uri
local-policy
        from-address                      *
        to-address                       *
        source-realm                      SIPTrunk
        policy-attribute
                next-hop                        sag:RingCentral
                realm                          RingCentral
                action                         replace-uri
```

```
media-manager
media-sec-policy
      name                        PSTNSide
media-sec-policy
      name                        RingCentralSRTP
      inbound
            profile                   RCSRTP
            mode                      srtp
            protocol                  sdes
      outbound
            profile                   RCSRTP
            mode                      srtp
            protocol                  sdes
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                   155.212.214.90
      netmask                      255.255.255.0
      gateway                      155.212.214.65
      dns-ip-primary                 9.9.9.9
      dns-ip-backup1                  8.8.8.8
      dns-ip-backup2                  8.8.4.4
      dns-domain                     cgbusolutionslab.com
phy-interface
      name                        s0p0
      operation-type                 Media
phy-interface
      name                        s1p0
      operation-type                 Media
      slot                      1
sdes-profile
      name                        RCSRTP
      crypto-list               AES_CM_128_HMAC_SHA1_80
                                AES_256_CM_HMAC_SHA1_80
                                AES_CM_128_HMAC_SHA1_32
      srtp-rekey-on-re-invite         enabled
```

```
realm-config
        identifier                      RingCentral
        network-interfaces                s1p0:0.4
        mm-in-realm                     enabled
        access-control-trust-level        high
        trunk-context                   cloudsbc.cgbusolutionslab.com
        rtcp-policy                     RingCentralRTCP
realm-config
        identifier                      SIPTrunk
        network-interfaces                s0p0:0.4
        mm-in-realm                     enabled
        access-control-trust-level        high
session-agent
        hostname                        10.1.5.8
        ip-address                      10.1.5.8
        transport-method                  UDP+TCP
        realm-id                        SIPTrunk
        ping-interval                   30
        ping-response                     enabled
        reuse-connections                 TCP
session-agent
        hostname                        192.209.28.158
        ip-address                      192.209.28.158
        port                            5061
        transport-method                StaticTLS
        realm-id                        RingCentral
        ping-method                     OPTIONS
        ping-interval                   30
        ping-response                     enabled
session-agent
        hostname                        192.209.28.53
        ip-address                      192.209.28.53
        port                            5061
        transport-method                StaticTLS
        realm-id                        RingCentral
        ping-method                     OPTIONS
        ping-interval                   30
        ping-response                     enabled
```

```
session-group
      group-name                    RingCentral
      strategy                      RoundRobin
      dest                          192.209.28.158
                                    192.209.28.53
sip-config
      home-realm-id                 RingCentral
      registrar-port                5060
      options                       max-udp-length=0
      extra-method-stats            enabled
sip-interface
      realm-id                      RingCentral
      sip-port
            address                 155.212.214.90
            port                    5061
            transport-protocol      TLS
            tls-profile             RingCentralTLS
            allow-anonymous         agents-only
      secured-network               enabled
sip-interface
      realm-id                      SIPTrunk
      sip-port
            address                 10.1.2.4
            transport-protocol      TCP
            allow-anonymous         agents-only
      sip-port
            address                 10.1.2.4
            allow-anonymous         agents-only
      secured-network               enabled
      spl-options
HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4
sip-monitoring
      match-any-filter              enabled
      monitoring-filters            *
steering-pool
      ip-address                    10.1.2.4
      start-port                    10000
      end-port                      20000
      realm-id                      SIPTrunk
steering-pool
      ip-address                    155.212.214.90
      start-port                    10000
      end-port                      10999
      realm-id                      RingCentral
```

9 Appendix C

9.1 Test Case Execution status

Sl No	Test Case	Description	Status
1	Incoming from GW	GW dials DL number, both participants hangup in turn	Pass
2	Outgoing to GW	DL dials a GW, both participants hangup in turn	Pass
3	Hold/Resume by DL	DL puts GW on hold and resumes	Pass
4	Hold/Resume by GW	GW puts DL on hold and resumes	Pass
5	Anonymous call to GW	DL dials GW anonymously (the From is anonymous, the PAI contains a number, the Privacy header is "id")	Pass
6	Anonymous call from GW	GW dials DL anonymously	Pass
7	Long duration call	The participants keep the call for at least 30 minutes	Pass
8	G.711 fax to GW	DL sends G.711 encoded fax to GW	Pass
9	G.711 fax from GW	GW sends G.711 encoded fax to DL	Pass
10	T.38 fax to GW	DL sends T.38 fax to GW	Pass
11	T.38 fax from GW	GW sends T.38 fax to DL	Pass

Oracle Corporation, World Headquarters

2300 Oracle Way
Austin, TX 78741, USA

Worldwide Inquiries

Phone: +1.650.506.7000 or
Phone: +1.800.392.2999

ORACLE

CONNECT WITH US

blogs.oracle.com

facebook.com/oracle

twitter.com/oracle

oracle.com/

Integrated Cloud Applications & Platform Services