Oracle SBC integration with Cisco Broadworks and Webex BYoPSTN

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	Oracle SBC integration with Cisco Broadworks and Webex BYoPSTN	27th October 2022
2.0	Added internal review comments	24 th November 2022

Table of Contents

1. INTENDED AUDIENCE 4

2. DOCUMENT OVERVIEW 4

2.1. WEBEX FOR CISCO BROADWORKS SERVICE PROVIDERS BYOPSTN 4

3. INTRODUCTION 5

3.1. AUDIENCE 5

3.2. REQUIREMENTS 5

3.3. ARCHITECTURE 6

4. CONFIGURING THE SBC 7

4.1. VALIDATED ORACLE SBC VERSION 7

5. NEW SBC CONFIGURATION 7

5.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC 7

5.2. CONFIGURE SBC USING WEB GUI 11

5.3. CONFIGURE SYSTEM-CONFIG 12

5.4. CONFIGURE PHYSICAL INTERFACE VALUES 13

5.5. CONFIGURE NETWORK INTERFACE VALUES 14

5.6. ENABLE MEDIA MANAGER 16

5.7. ENABLE SIP-CONFIG 17

5.8. CONFIGURE REALMS 18

5.9. CONFIGURING A CERTIFICATE FOR SBC 20

5.10. TLS-PROFILE 24

5.11. CONFIGURE SIP INTERFACES 25

5.12. CONFIGURE SESSION-AGENT 32

5.13. CONFIGURE LOCAL-POLICY 35

5.14. CONFIGURE STEERING-POOL 37

5.15. CONFIGURE SDES PROFILE 38

5.16. CONFIGURE MEDIA SECURITY PROFILE 39

6. EXISTING SBC CONFIGURATION 40

1. 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 Cisco Webex Meetings with 3rd Party Local Gateway.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between PSTN Trunk with Cisco Webex Meetings Solution. The solution contained within this document has been tested using Oracle Communication SBC with software version **OS840p12 (SCZ8.4.0 Patch 12)**

Please find the related documentation links below:

1. Webex for Cisco BroadWorks Solution Guide https://help.webex.com/en-us/article/n0h4eh4/Webex-for-Cisco-BroadWorks-Solution-Guide
2. Configure Webex Meetings in Cisco Webex Site Administration https://help.webex.com/en-us/article/6maub2/Configure-Webex-Meetings-in-Cisco-Webex-Site-Administration

2.1. Webex for Cisco BroadWorks Service Providers BYoPSTN

The BYoPSTN solution helps customers bring their own phone numbers while using Cisco Webex interconnected with Cisco Broadworks.

Configure the SBC FQDN on Webex Meetings
On the Webex Portal ,Go to Settings->BroadWorksCalling->Meeting Join Config.
Create a DNS SRV group with DNS SRV record as SBC FQDN.
For eg: **c**loudsbc.cgbusolutionslab.com

Configure test subscribers using the Subscriber API's that map phone number to meeting access codes.
A custom template that maps the Cisco Phone Number Group with the DNS SRV group.
A meeting UUID that is generated on Webex using a custom template on Webex Meetings .This UUID is configured on Cisco BroadWorks.
For more information refer here. https://help.webex.com/en-us/article/n0h4eh4/Webex-for-Cisco-BroadWorks-Solution-Guide

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. There are some public facing IPs (externally routable IPs) that we use for our testing are masked in this document for security reasons.

3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring BYoPSTN for Cisco BroadWorks Service providers 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.

3.2. Requirements

- Fully functioning Cisco Webex Control Hub (Provisioned Webex Control Hub with necessary Webex Meetings licenses/Subscription and also prepared Webex Meetings environment)

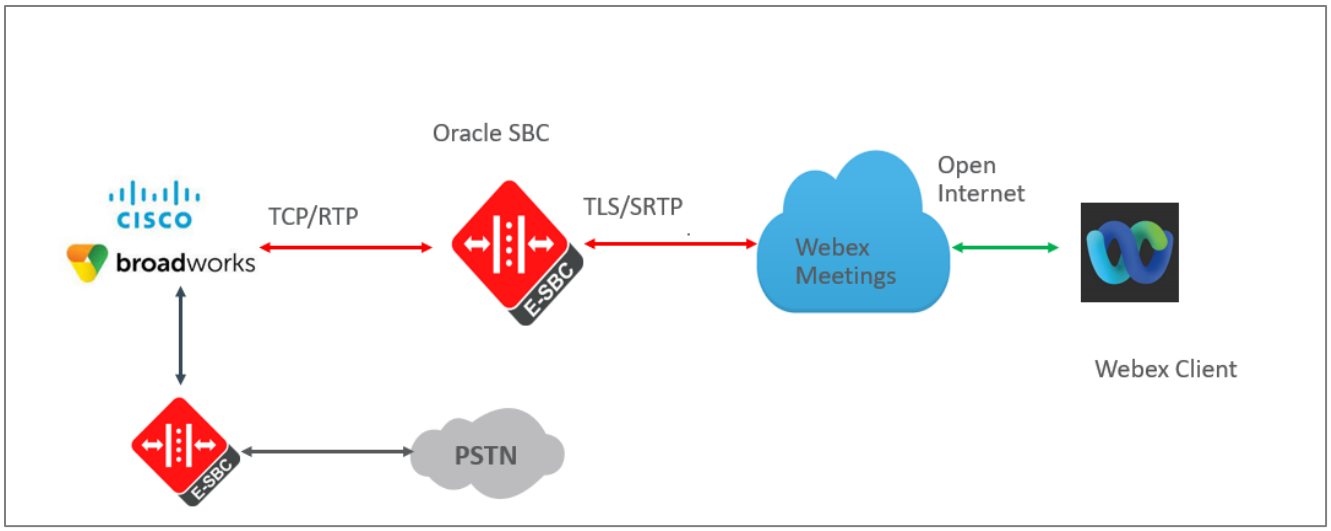
  http://cs.co/Webex-Calling-Environment

- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version
- Cisco BroadWorks version Rel23

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	8.4.0

3.3. Architecture



The configuration, validation and troubleshooting of this document will be configuring the Oracle SBC only. For configuring Cisco Webex for Broadworks and Cisco Webex Meetings please refer the documents listed here

4. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Cisco Webex Meetings and Cisco Broadworks. **In this SBC config, Cisco Webex Meeting (TLS/SRTP) and Cisco Broadworks (UDP or TCP/RTP).**

4.1. Validated Oracle SBC version

Oracle conducted tests with SBC 8.4 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 (Starting from SBC 9.0 version)
- AP 4900 (Starting from SBC 9.0 version)
- VME
- Oracle SBC on Public Cloud

5. New SBC configuration

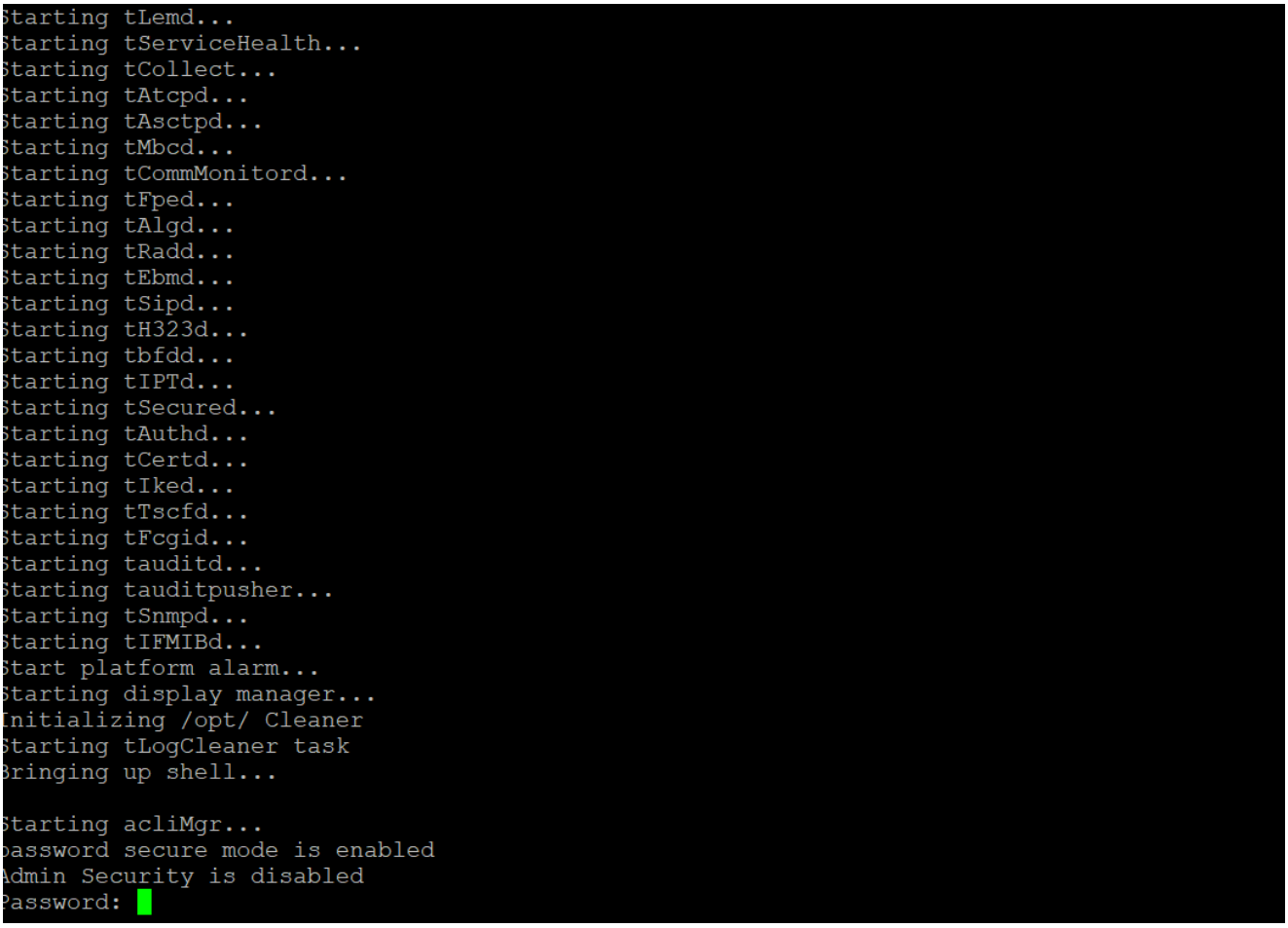
If the customer is looking to setup a new SBC from scratch, please follow the section below.

5.1. Establishing a serial connection to the SBC

Connect one end of a straight-through Ethernet cable to the front console port (which is active by default) on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB-9 adapter) to the DB-9 port on a workstation, running a terminal emulator application such as Putty. Start the terminal emulation application using the following settings:

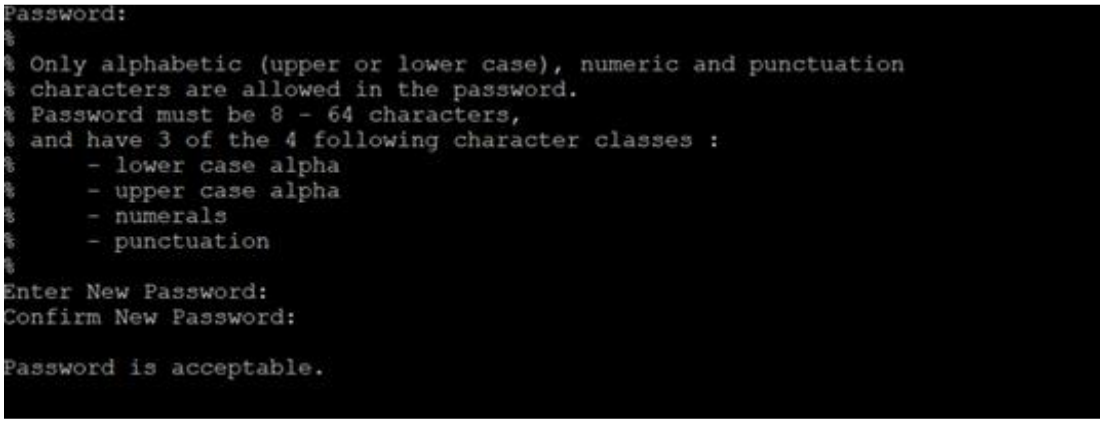
- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

Power on the SBC and confirm that you see the following output from the boot-up sequence



Enter the default password to log in to the SBC. Note that the default SBC password is “acme” and the default super user password is “packet”.

Both passwords have to be changed according to the rules shown below.



Now set the management IP of the SBC by setting the IP address in bootparam.

To access bootparam. Go to Configure terminal->bootparam.

```
SolutionsLab-vSBC-2(configure)# bootparam

'.' = clear field;  '-' = go to previous field;  q = quit

Boot File               : /boot/nnSCZ900p4.bz
IP Address              :
VLAN                    :
Netmask                 :
Gateway                 :
IPv6 Address            :
IPv6 Gateway            :
Host IP                 :
FTP username            : vxftp
FTP password            :
Flags                   : 0x00000040
Target Name             : SolutionsLab-vSBC-2
Console Device          : COM1
Console Baudrate        : 115200
Other                   :

NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.


        ERROR   : space in /boot      (Percent Free: 18)

SolutionsLab-vSBC-2(configure)#
SolutionsLab-vSBC-2(configure)#
```

Note: There is no management IP configured by default.

To configure product type, type in setup product in the terminal

Set product type to Enterprise Session Border Controller as shown below.

```
SolutionsLab-vSBC-2# setup product

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

Last Modified 2022-10-03 07:21:29
------------------------------------------------------------
 1 : Product       : Enterprise Session Border Controller

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

Enable the features for the ESBC using the setup entitlements command as shown

Save the changes and reboot the SBC.

```
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
```

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

Go to configure terminal->system->http-server-config. Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

```
SolutionsLab-vSBC-2(http-server)# show
http-server
       name                                  webserver
       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                   REST,GUI
       http-file-upload-size                 0
       tls-profile
       auth-profile
       last-modified-by                      webHTTP-admin@196.15.23.12:33336
       last-modified-date                    2022-07-07 17:34:44

SolutionsLab-vSBC-2(http-server)#
SolutionsLab-vSBC-2(http-server)#
SolutionsLab-vSBC-2(http-server)#
```

5.2. Configure SBC using Web GUI

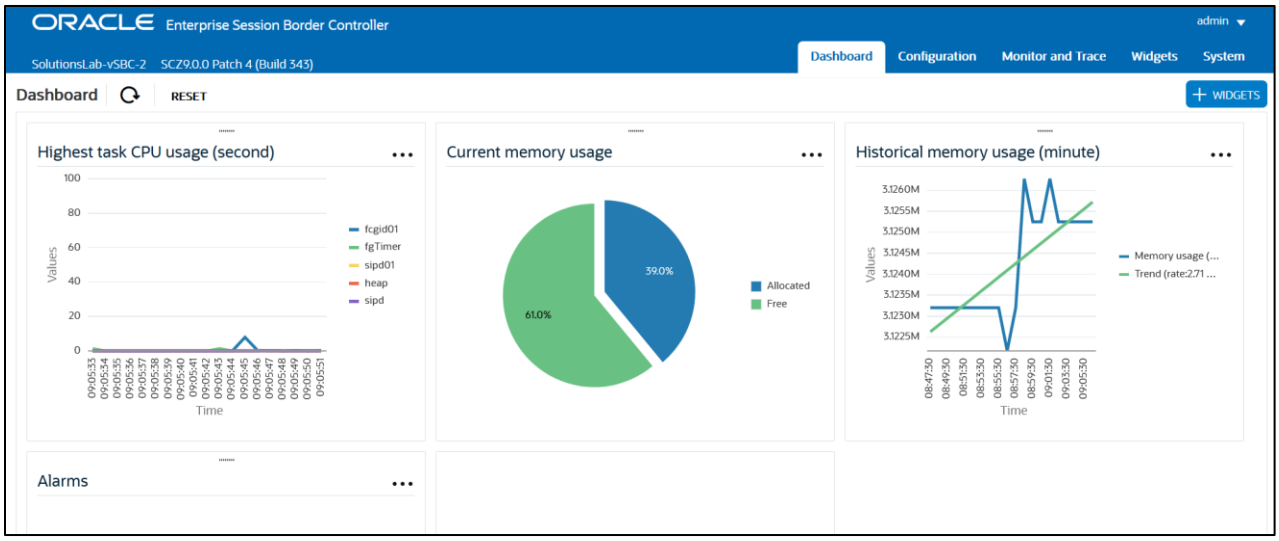
In this app note, we configure SBC using the WebGUI.

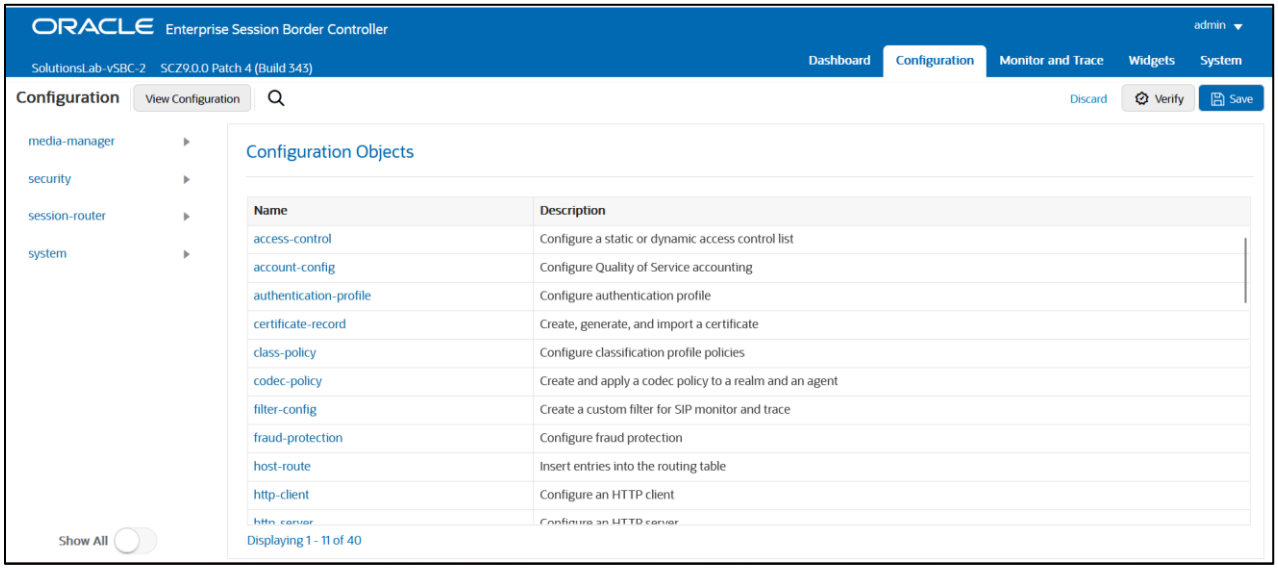
The Web GUI can be accessed through the url http://<SBC_MGMT_IP>.

The username and password is the same as that of CLI.

Go to Configuration as shown below, to configure the SBC

Note: The screenshots are taken from Release 9.0 of SBC .





Kindly refer to the GUI User Guide given below for more information.

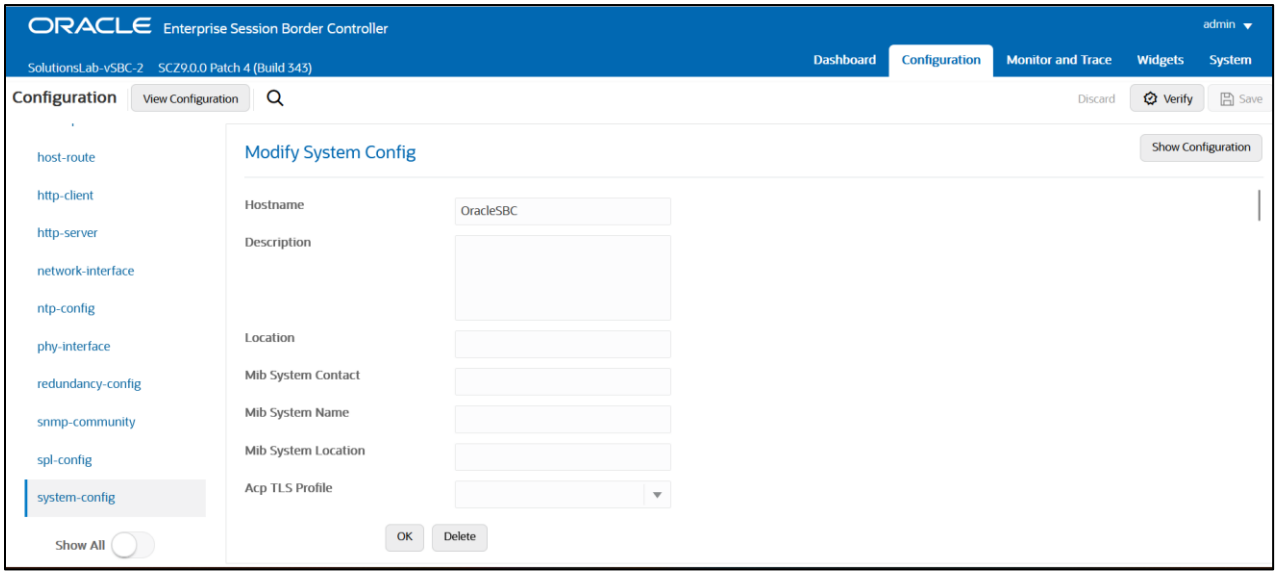
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.0.0/webgui/web-gui-guide.pdf

The expert mode is used for configuration.

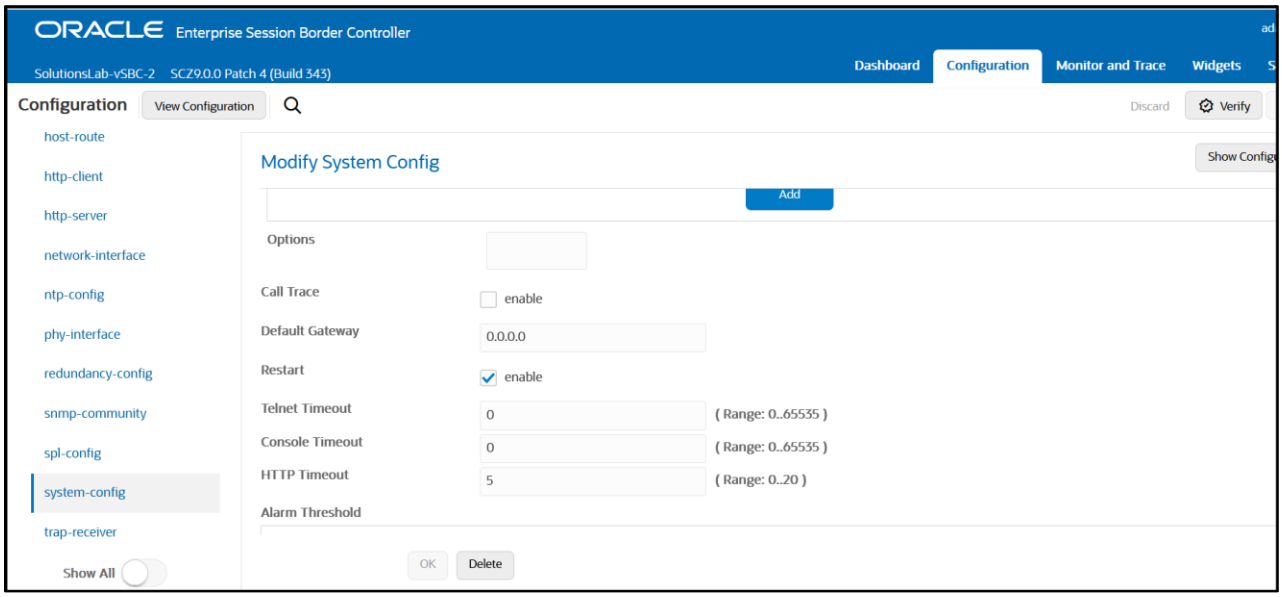
Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

5.3. Configure system-config

Go to system->system-config



Please enter the default gateway value in the system config page as below.



For VME, transcoding cores are required. Please refer the documentation here for more information

https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.0.0/releasenotes/esbc-release-notes.pdf

The above step is needed only if any transcoding is used in the configuration.
If there is no transcoding involved, then the above step is not needed.

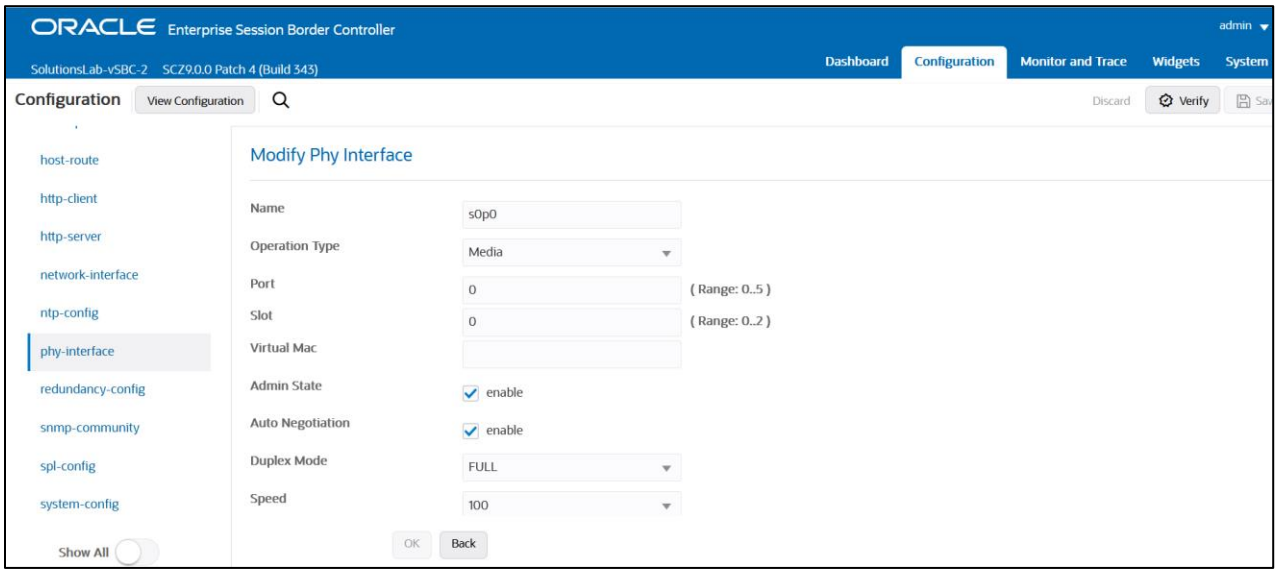
5.4. Configure Physical Interface values

To configure physical Interface values, go to System->phy-interface.

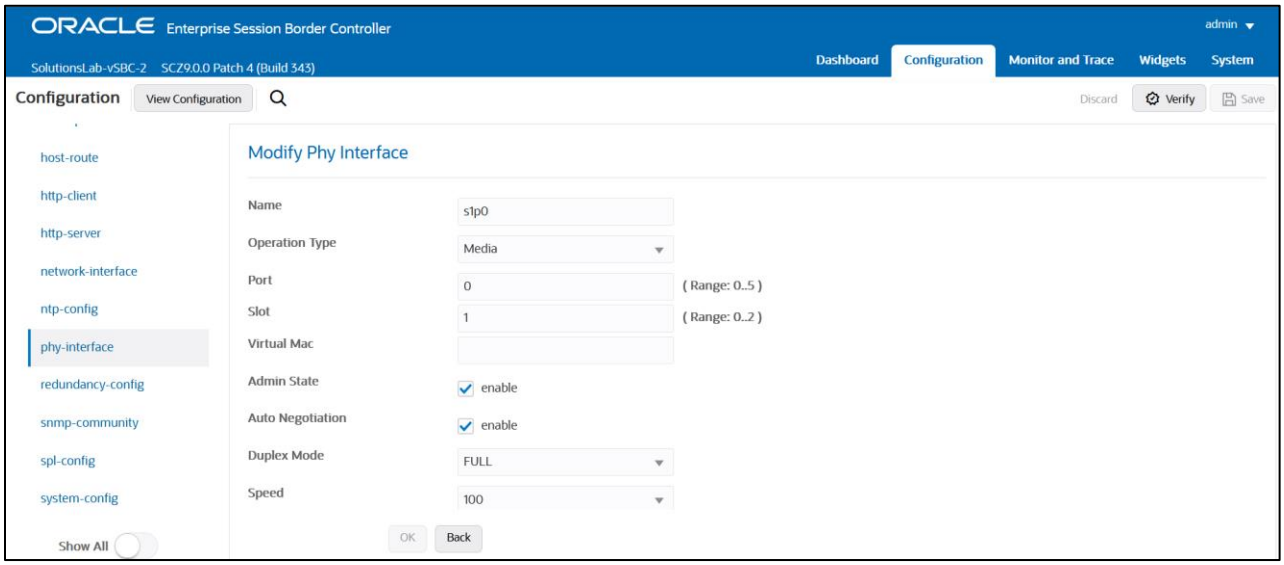
Please configure s0p0 for Cisco Broadworks and s1p0 for Cisco Webex Meetings .

Parameter Name	Cisco Broadworks (s0p0)	Cisco Webex Meetings (s1p0)
Slot	0	1
Port	0	0
Operation Mode	Media	Media

Please configure s0p0 interface as below.



Please configure s1p0 interface as below



5.5. Configure Network Interface values

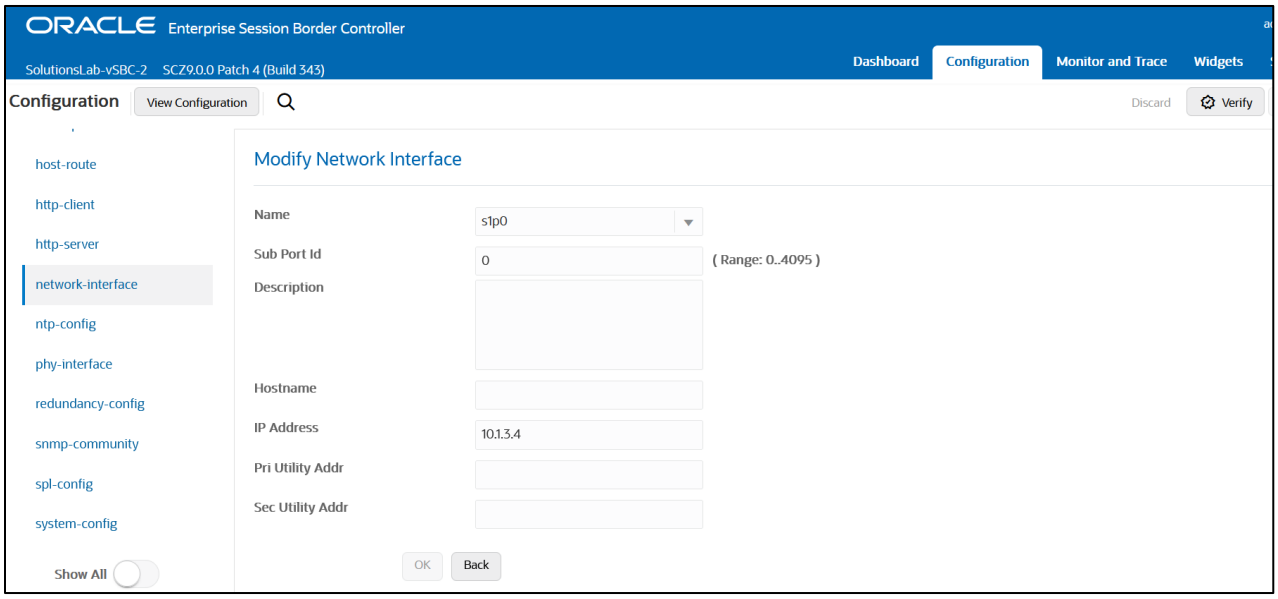
To configure network-interface, go to system->Network-Interface. Configure interface

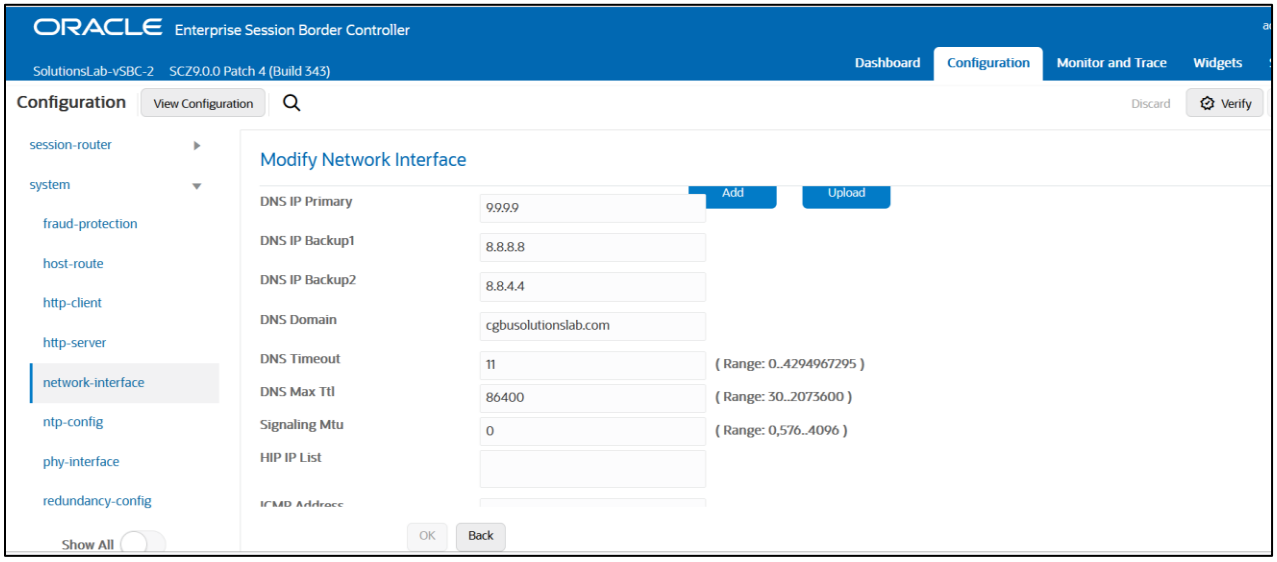
The table below lists the parameters, to be configured for both the interfaces.

Parameter Name	Cisco Broadworks Network Interface(s0p0)	Cisco Webex Meetings Network Interface(s1p0)
Name	s0p0	S1p0
Host Name		
IP Address	155.212.214.90	10.1.3.4
Net Mask	255.255.255.0	255.255.255.0
Gateway	155.212.214.65	10.1.3.1

Please configure network interface s0p0 as below

Similarly, configure network interface s1p0 as below

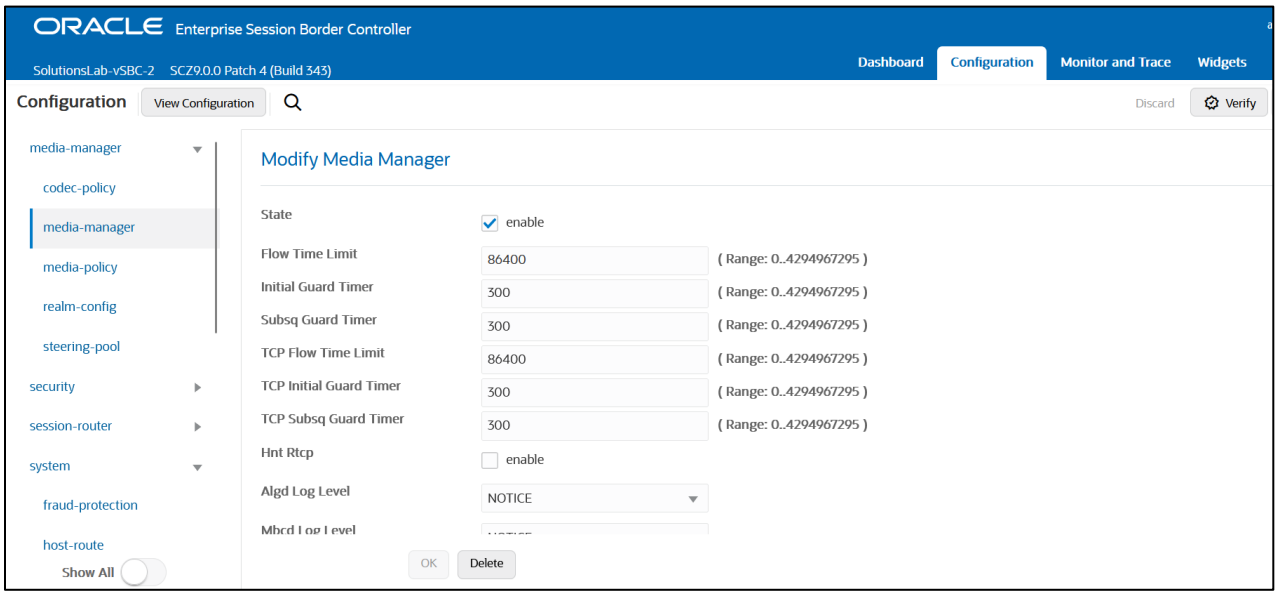


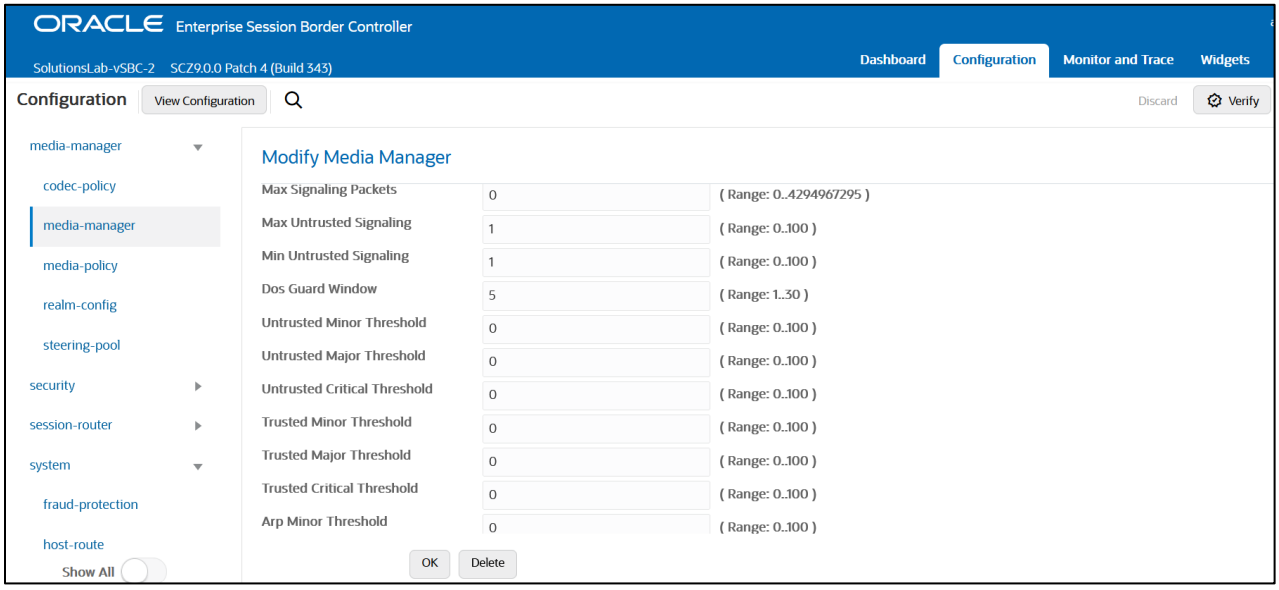


5.6. Enable media manager

Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

Go to Media-Manager->Media-Manager



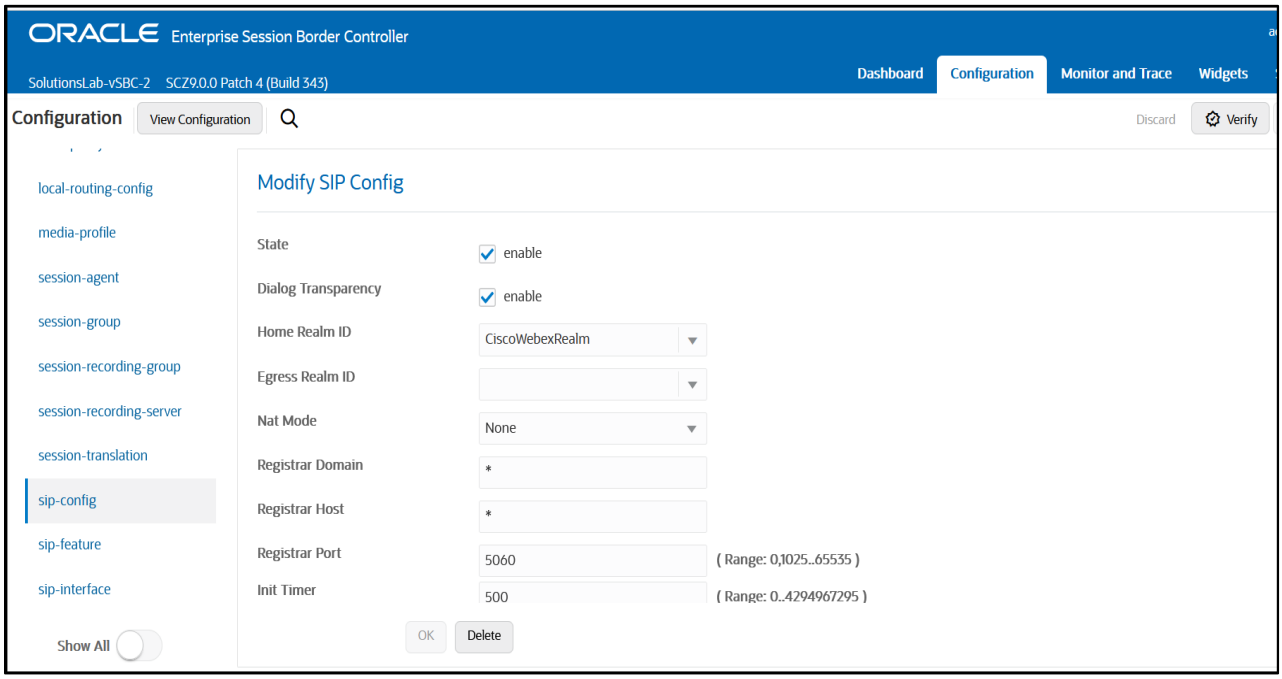


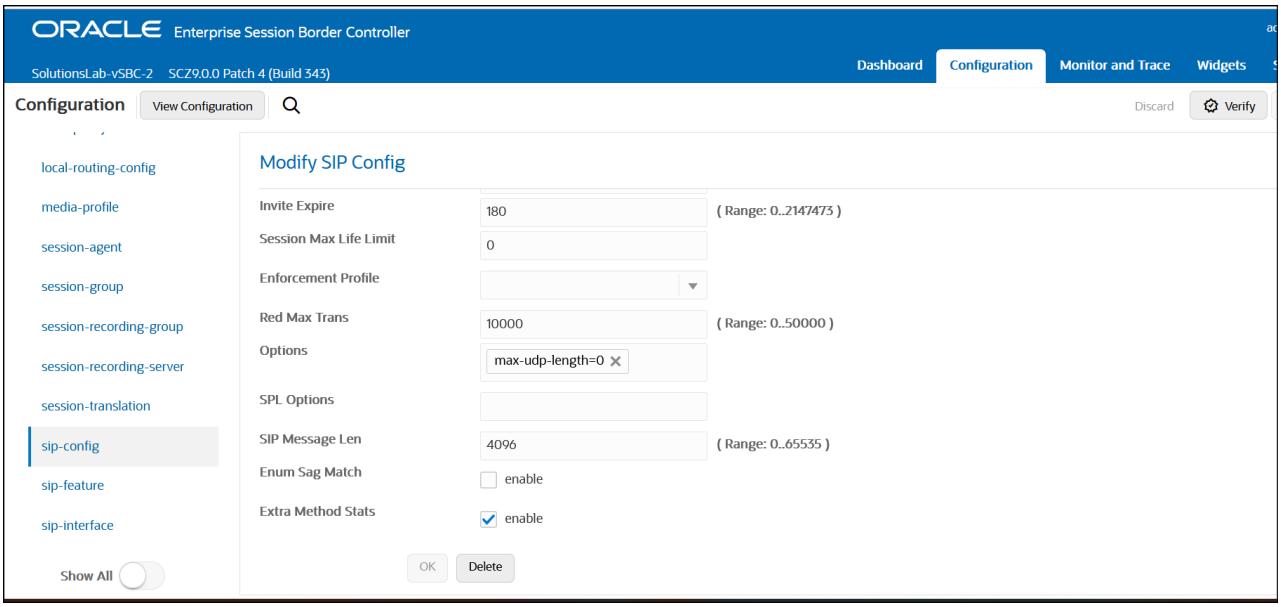
5.7. Enable sip-config

SIP config enables SIP handling in the SBC.
Make sure the home realm-id, registrar-domain and registrar-host are configured.

Also add the options to the sip-config as shown below.
To configure sip-config, Go to Session-Router->sip-config.

In options add max-udp-length =0.





5.8. Configure Realms

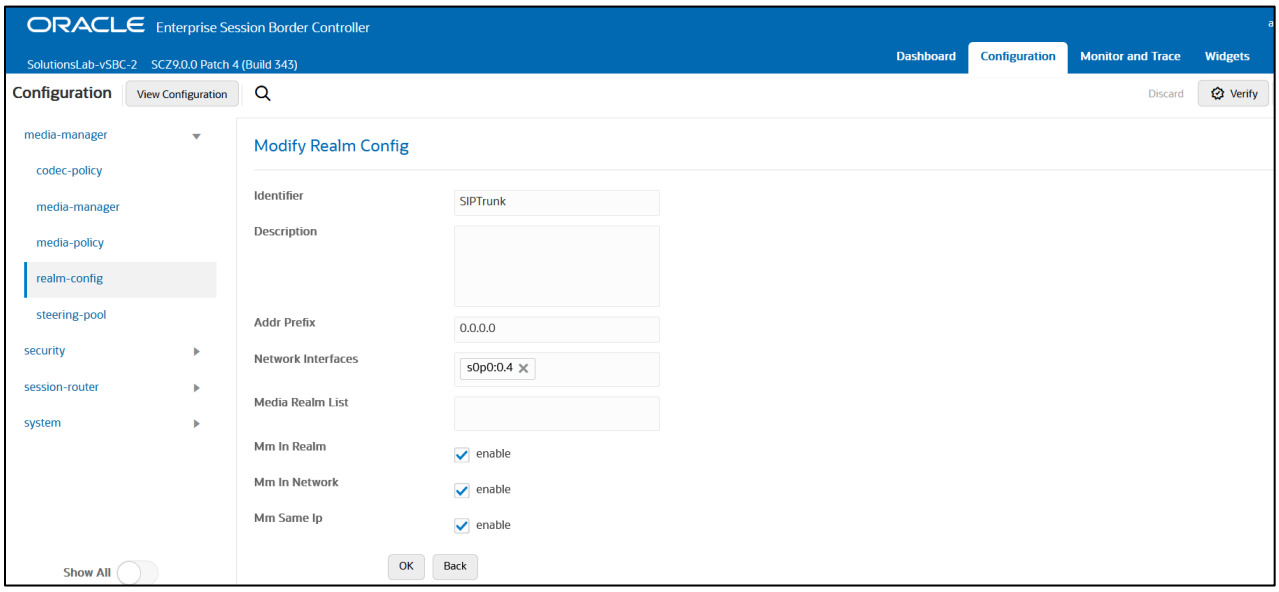
Navigate to realm-config under media-manager and configure a realm as shown below
The name of the Realm can be any relevant name according to the user convenience.

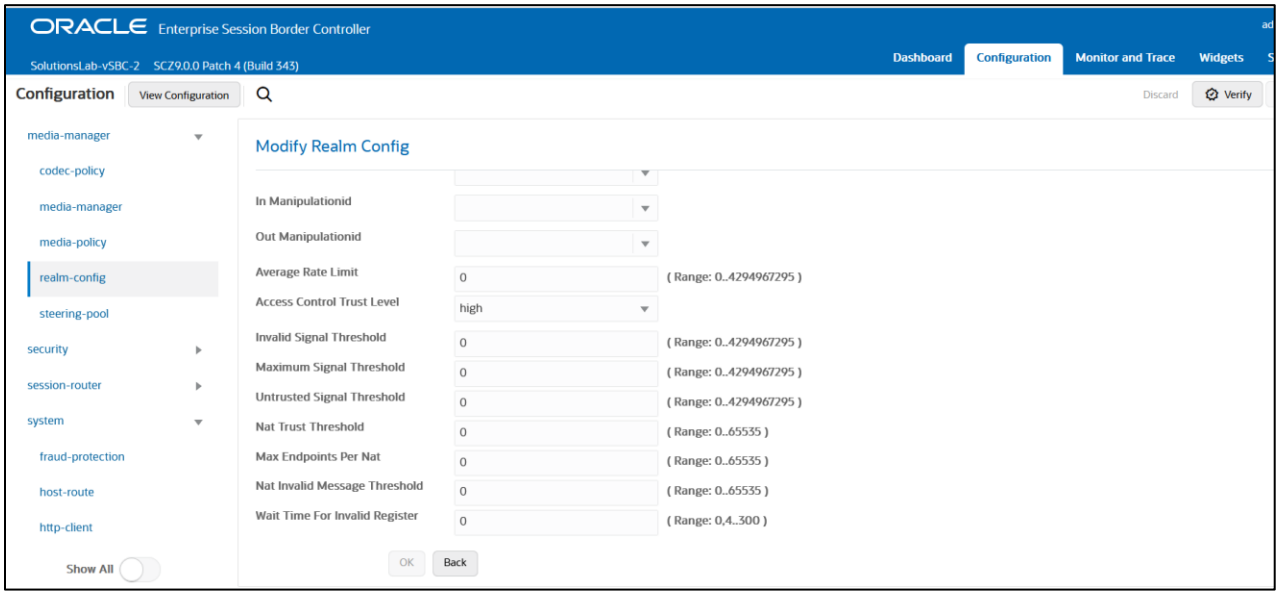
Use the following table as a configuration example for the two realms used in this configuration:

Config Parameter	Cisco Broadworks	Cisco Webex Meetings
Identifier	SIPTrunk	CiscoWebexRealm
Network Interface	S0p0	s1p0
Mm in realm	☑	☑
FQDN		
Media Sec policy	PSTNSide	CiscoWebexSecurity
Access Control Trust Level	High	High

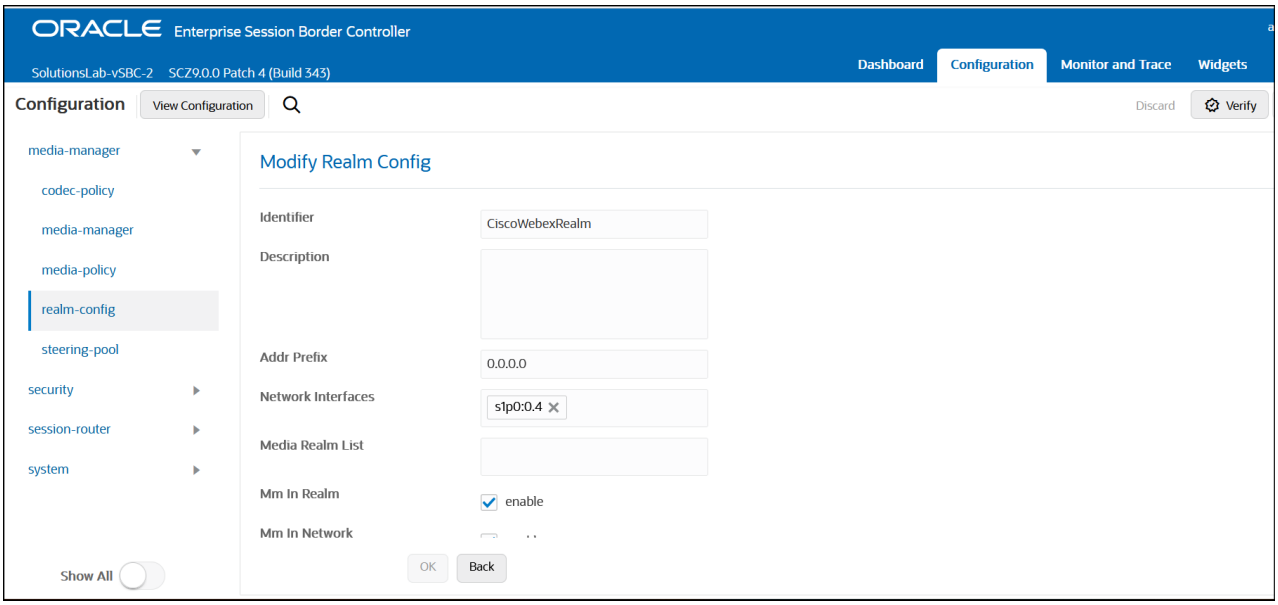
In the below case, Realm name is given as **SIPTrunk** for Cisco Broadworks

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





Similarly, Realm name is given as **CiscoWebexRealm** for Cisco Webex Meetings side.
Please set the Access Control Trust Level as high for this realm too.



For more information on Access Control Trust Level, please refer to SBC Security guide link given below:

https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/security/security-guide.pdf

5.9. Configuring a certificate for SBC

This section describes how to configure the SBC for TLS and SRTP communication for Cisco Webex Meetings. Cisco Webex Meetings side allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by the trusted Certificate Authorities like Go Daddy Root CA and also IdenTrust Root CA certificate as Cisco Webex has moved to a new Certificate Authority, IdenTrust Commercial Root CA from March 2021.

The links for Identrust certificate is given below:

https://help.Webex.com/en-us/article/WBX9000034330/New-Root-Certificate-Authority-for-Cisco-Webex-Services-from-March-2021

https://help.Webex.com/en-us/article/WBX9000008850/What-Root-Certificate-Authorities-are-Supported-for-Calls-to-Cisco-Webex-Audio-and-Video-Platforms?

Though the links talks about Identrust certificates used by Cisco VCS and Expressway, we can still Download the Identrust root certificate and can upload it to the Oracle SBC with the steps given below.

The process includes the following steps:

1) Create a certificate-record – "Certificate-record" are configuration elements on Oracle SBC which captures 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.

- SBC – 1 certificate-record assigned to SBC
- Root – 1 certificate-record for root cert

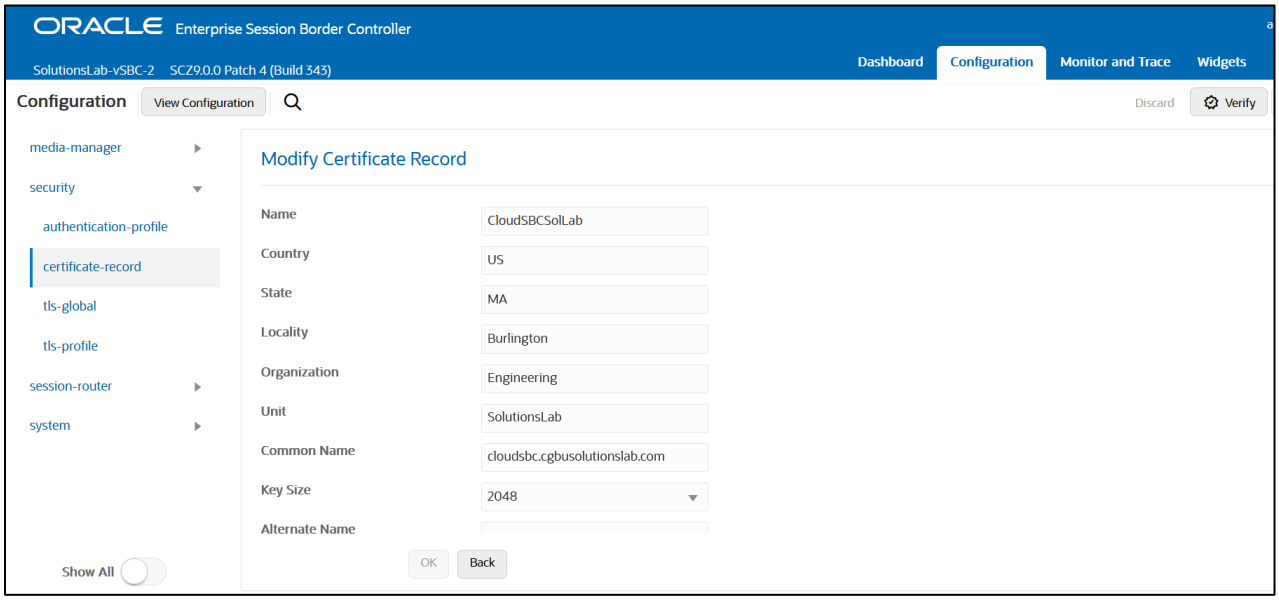
2) Deploy the SBC and Root certificates on the SBC

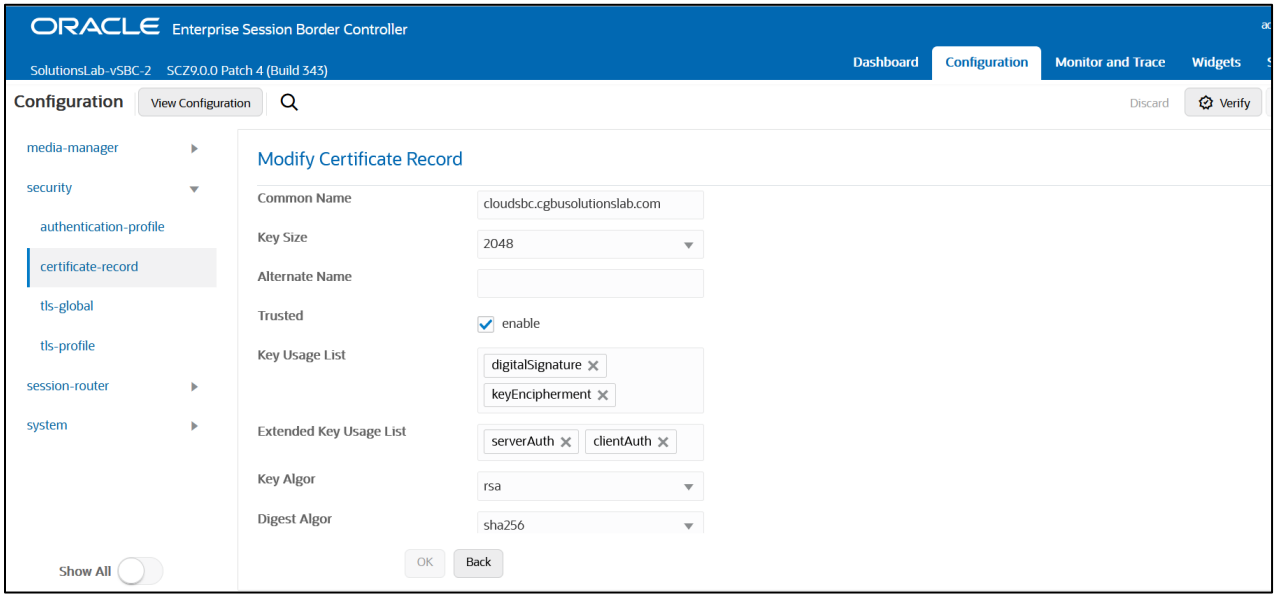
Step 1 – Creating the certificate record

Go to security->Certificate Record and configure the SBC entity certificate for SBC as shown below.

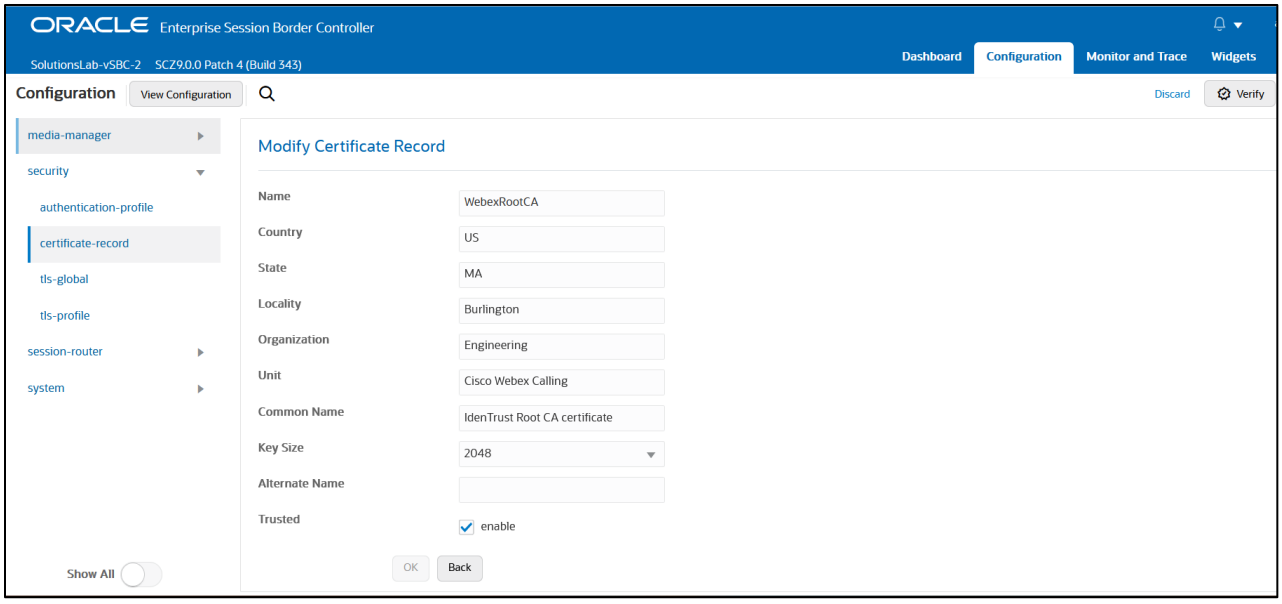
This value cloudsbc.cgbusolutionslab.com is configured as FQDN of SBC in the Cisco Webex Admin portal, and this will be used by Cisco Webex Meetings side to reach SBC when making calls.

Please note that the FQDN created on the Webex side must be the Common Name (CN) or Subject Alternative Name (SAN) of the certificate. As Cisco does an exact match and do not support wildcard certificates, each domain must be called out in CN or SAN of the certificate for validation.





Create a Certificate record for Identrust Root CA in SBC as below:



The table below specifies the parameters required for certificate configuration.
Modify the configuration according to the certificates in your environment.

Config Parameter	Go Daddy Root	IdenTrust Root
Common Name	Go Daddy class2 Root CA	IdenTrusrt Root CA
Key Size	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth
Key algor	rsa	rsa
Digest-algor	Sha256	Sha256

Step 2 – Generating a certificate signing request

(Only required for the SBC's end entity certificate, and not for root CA certs)

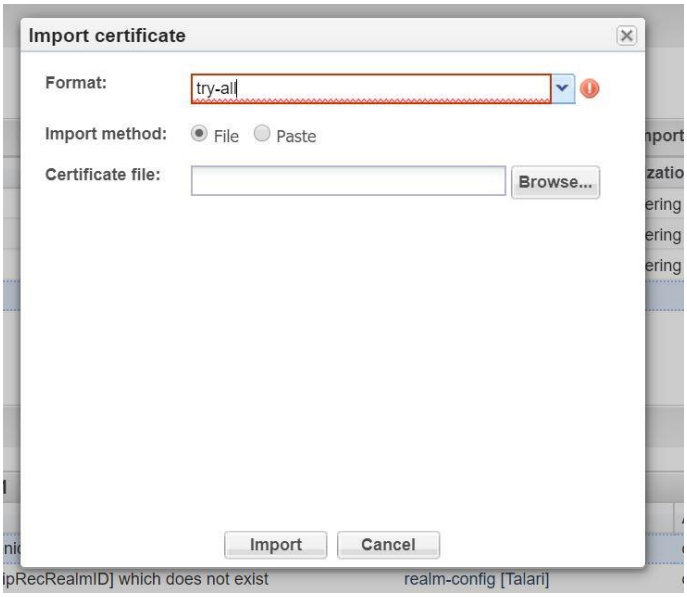
Please note – certificate signing request is only required to be executed for SBC Certificate – not for the root/intermediate certificates.

- Select the certificate and generate certificate on clicking the "Generate" command.
- Please copy/paste the text that gets printed on the screen as shown below and upload to your CA server for signature.

- Also, note that a save/activate is required

Step 3 – Deploy SBC & root certificates

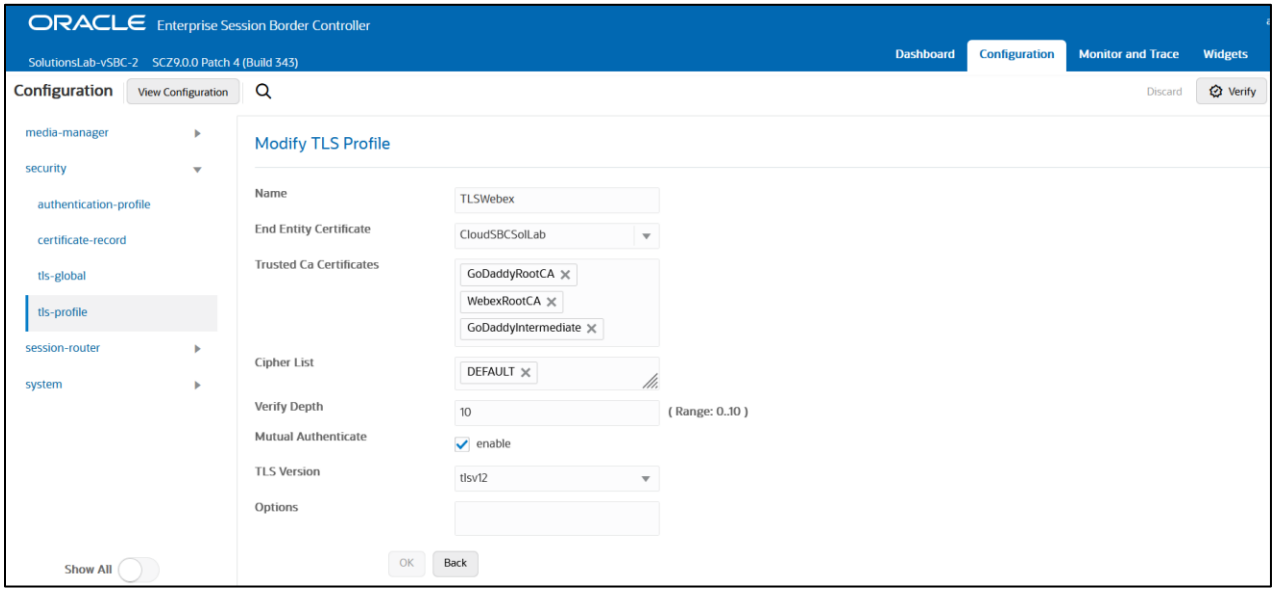
Once certificate signing request have been completed – import the signed certificate to the SBC.
Please note – all certificates including root and intermediate certificates are required to be imported to the SBC. Once done, issue save/activate from the WebGUI



Repeat these steps to import all the root and intermediate CA certificates into the SBC:
At this stage all the required certificates have been imported to the SBC for Cisco Webex Meetings.

5.10. TLS-Profile

A TLS profile configuration on the SBC allows for specific certificates to be assigned.
Go to security-> TLS-profile config element and configure the tls-profile as shown below
The below is the TLS profile configured for the Cisco Webex Meetings side:

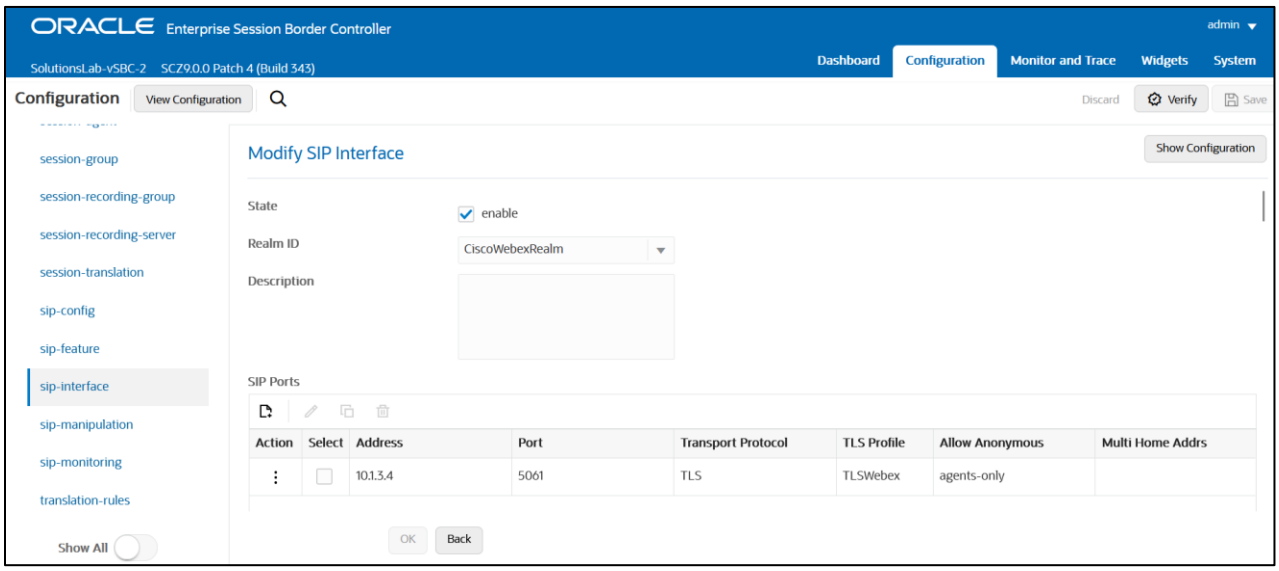


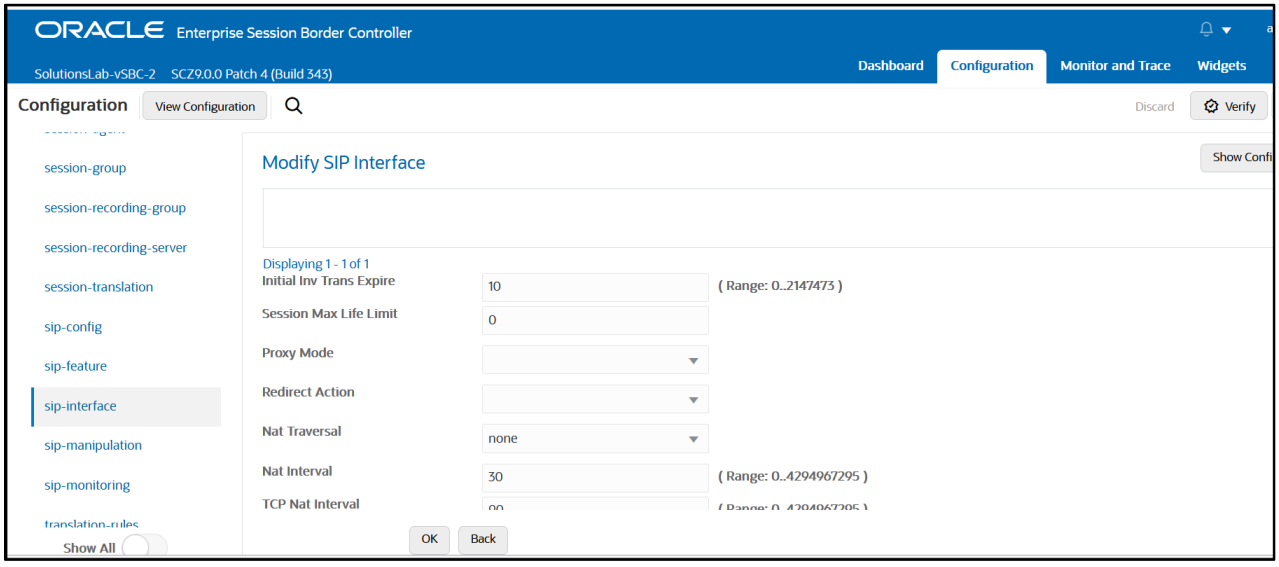
5.11. Configure SIP Interfaces

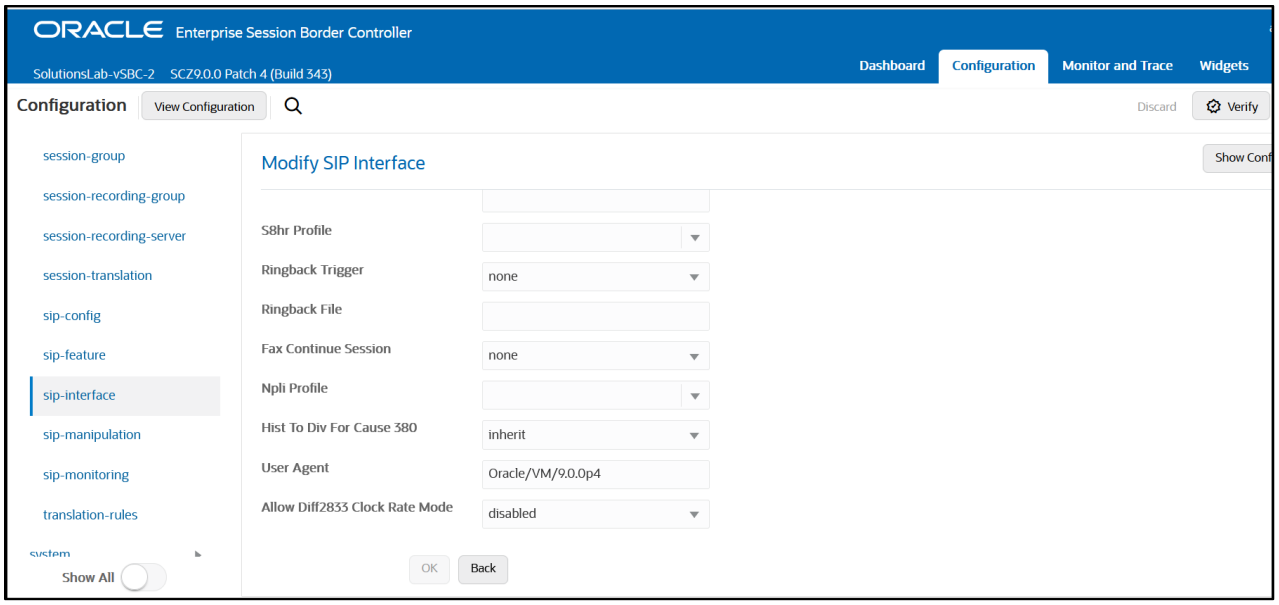
Navigate to sip-interface under session-router and configure the sip-interface as shown below. Please configure the below settings under the sip-interface.

Please Configure sip-interface for the Cisco Webex Meetings side as 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.



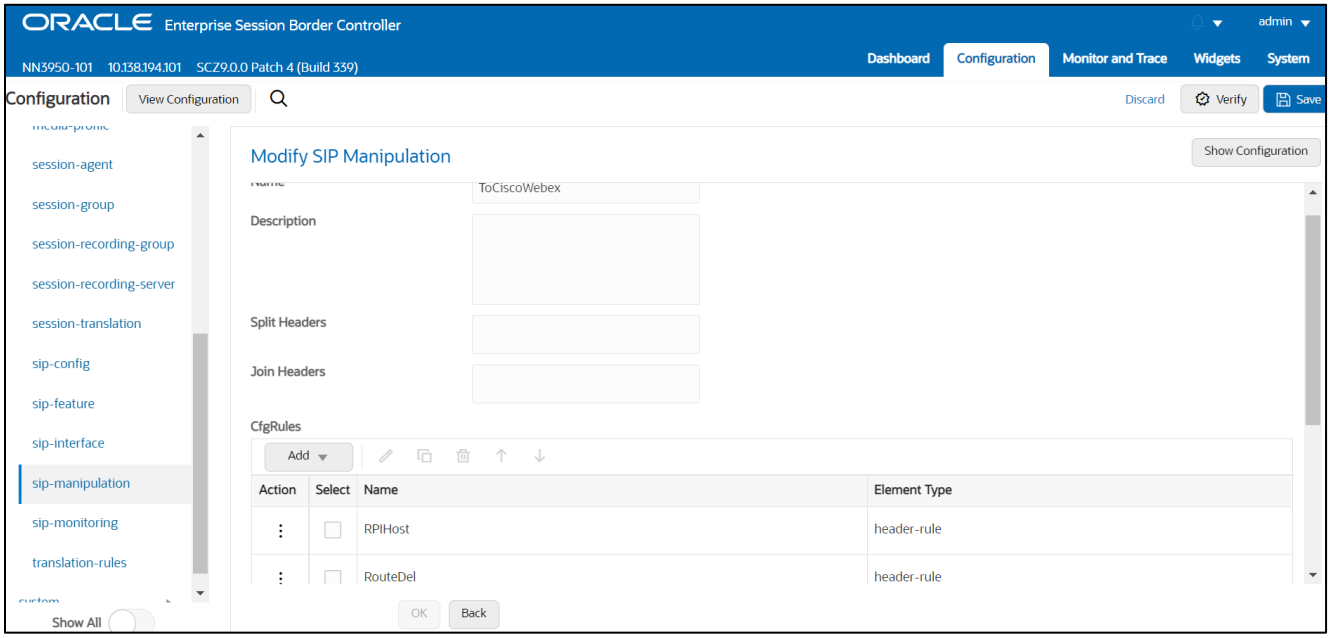


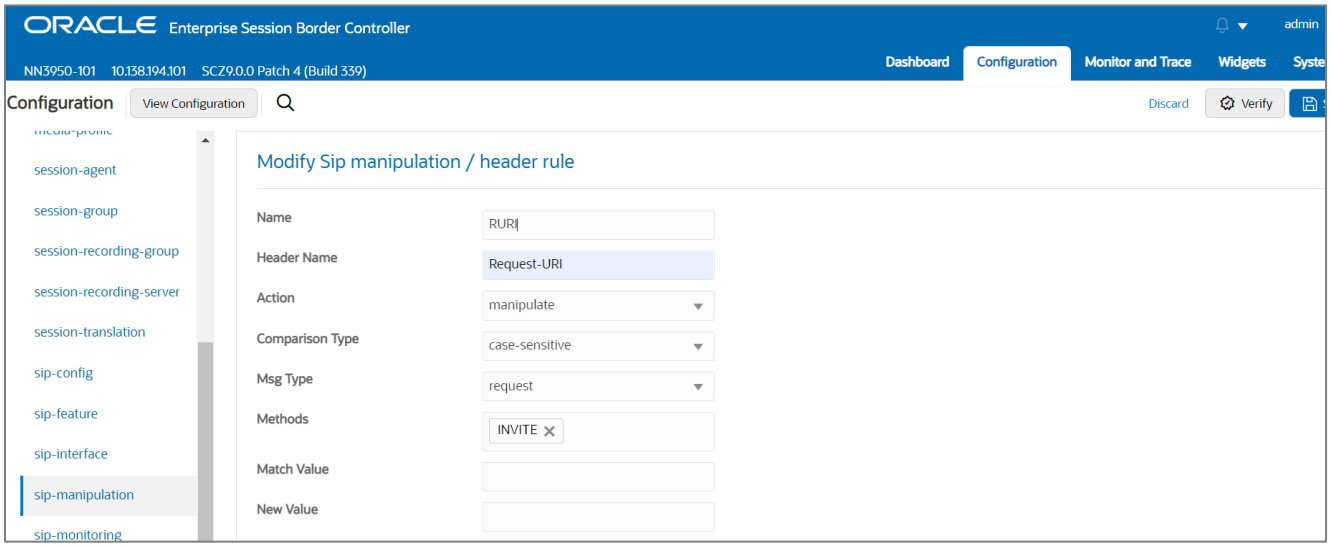


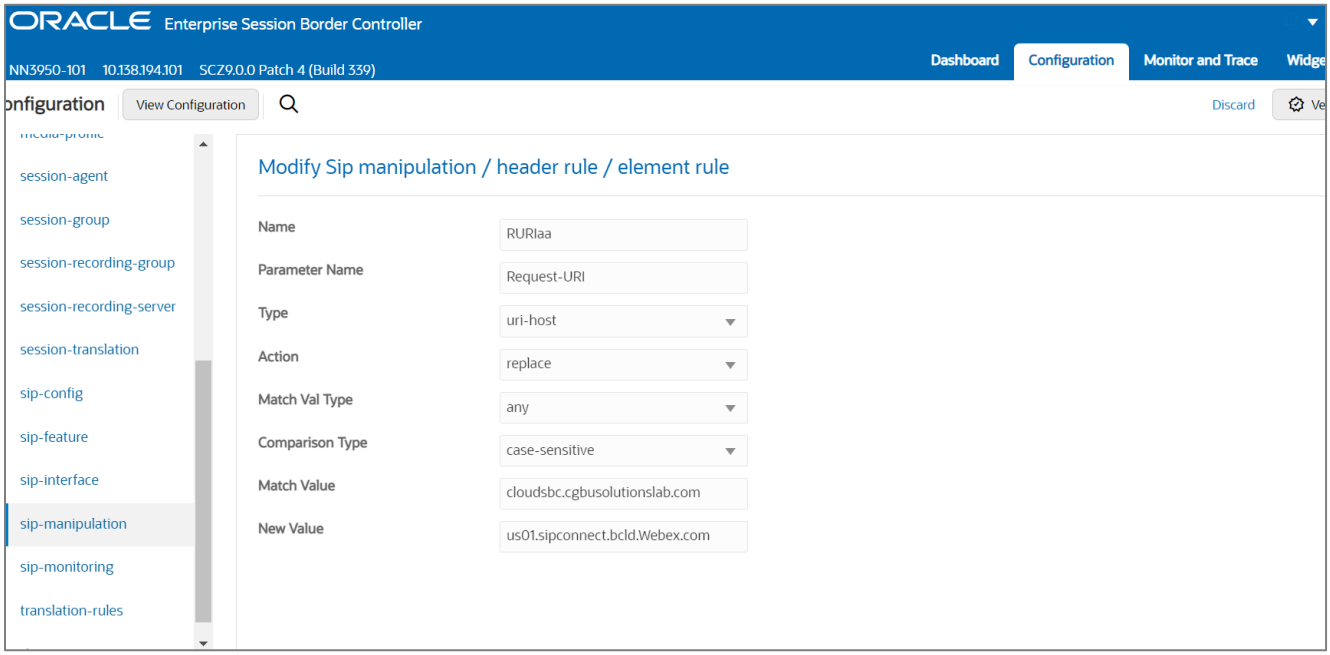
We have some mandatory sip-manipulations that needs to be used with the Oracle SBC so that call flow between Cisco Webex and PSTN will be successful. The User can add these sip manipulations to the SBC using either GUI or CLI mode and is free to decide the way they want to add the sip manipulations.
Please assign the below sip-manipulation as the out-manipulation ID in the Cisco Webex sip interface or Cisco Webex Session Agent as per customer need.
Please Configure sip-interface for the Cisco Webex Meetings as below

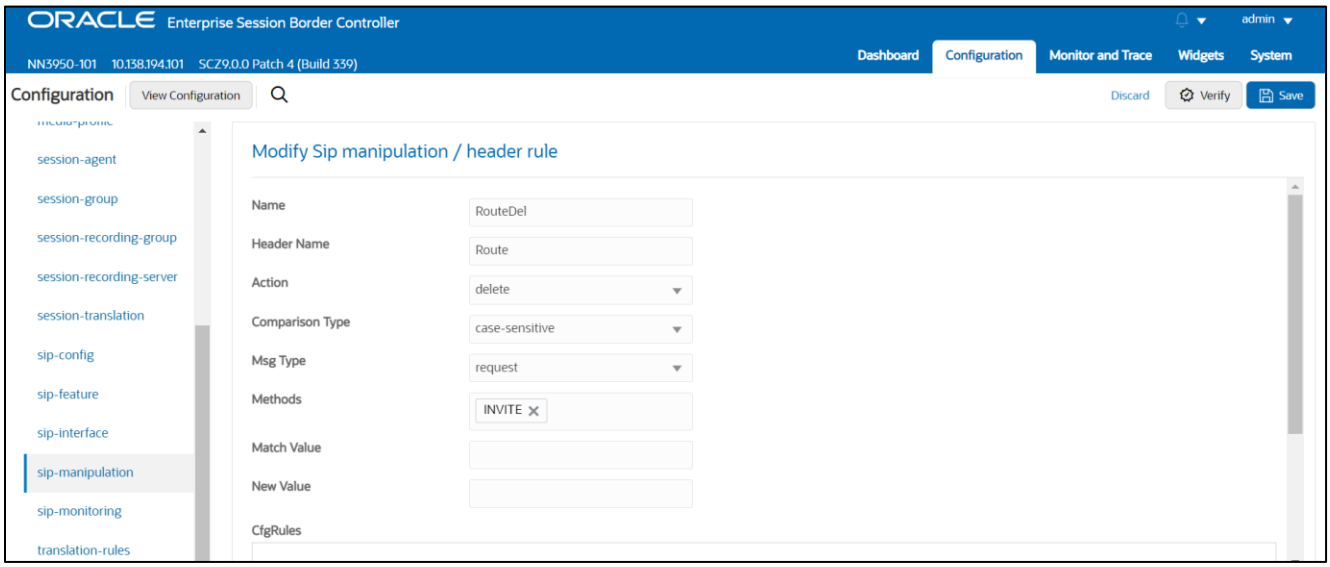
There are 2 sip manipulations to be configured

1. RPIHost : To change the SBC FQDN to Webex Meetings FQDN.
2. Route Del: To delete the Route header.


ORACLE Enterprise Session Border Controller
admin
NN3950-101 10.138.194.101 SCZ9.0.0 Patch 4 (Build 339)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
Save
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
translation-rules
Show All
Modify SIP Manipulation
Show Configuration
ToCiscoWebex
Description
Split Headers
Join Headers
CfgRules
Add
Action
Select
Name
Element Type
RPIHost
header-rule
RouteDel
header-rule
OK
Back

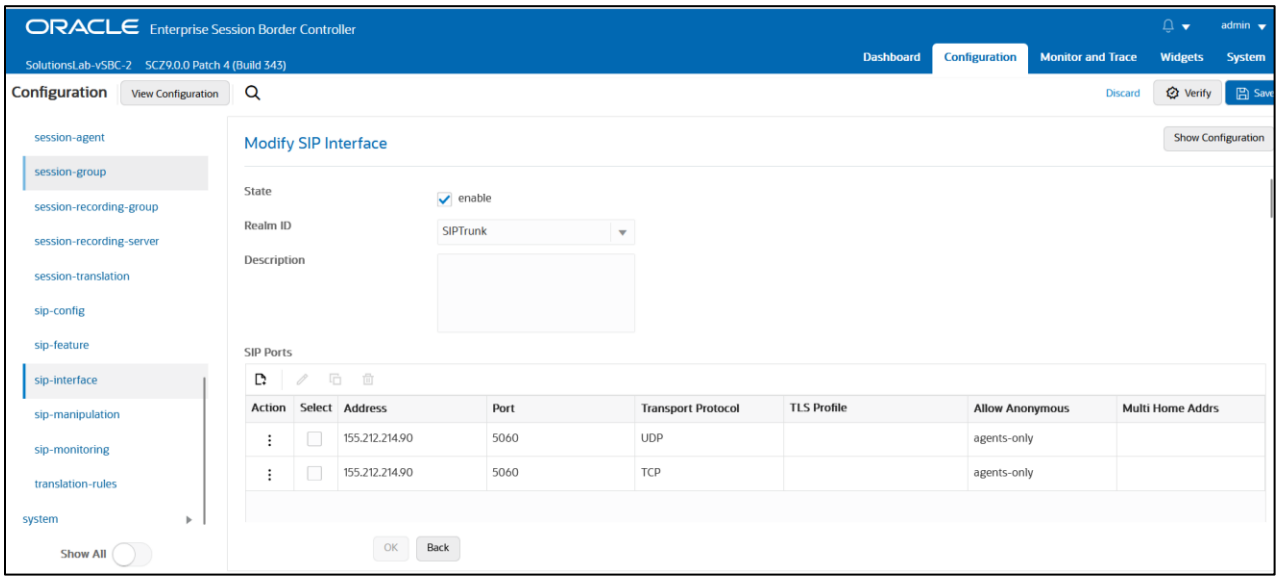

ORACLE Enterprise Session Border Controller
admin
NN3950-101 10.138.194.101 SCZ9.0.0 Patch 4 (Build 339)
Dashboard
Configuration
Monitor and Trace
Widgets
Configuration
View Configuration
Discard
Verify
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
Modify Sip manipulation / header rule
Name
RURI
Header Name
Request-URI
Action
manipulate
Comparison Type
case-sensitive
Msg Type
request
Methods
INVITE
Match Value
New Value


ORACLE Enterprise Session Border Controller
NN3950-101 10.138.194.101 SCZ9.0.0 Patch 4 (Build 339)
Dashboard
Configuration
Monitor and Trace
Widge
onfiguration
View Configuration
Discard
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
translation-rules
Modify Sip manipulation / header rule / element rule
Name
RURIaa
Parameter Name
Request-URI
Type
uri-host
Action
replace
Match Val Type
any
Comparison Type
case-sensitive
Match Value
cloudsbc.cgbusolutionslab.com
New Value
us01.sipconnect.bcld.Webex.com


ORACLE Enterprise Session Border Controller
admin
NN3950-101 10.138.194.101 SCZ9.0.0 Patch 4 (Build 339)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
Save
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
translation-rules
Modify Sip manipulation / header rule
Name
RouteDel
Header Name
Route
Action
delete
Comparison Type
case-sensitive
Msg Type
request
Methods
INVITE
Match Value
New Value
CfgRules

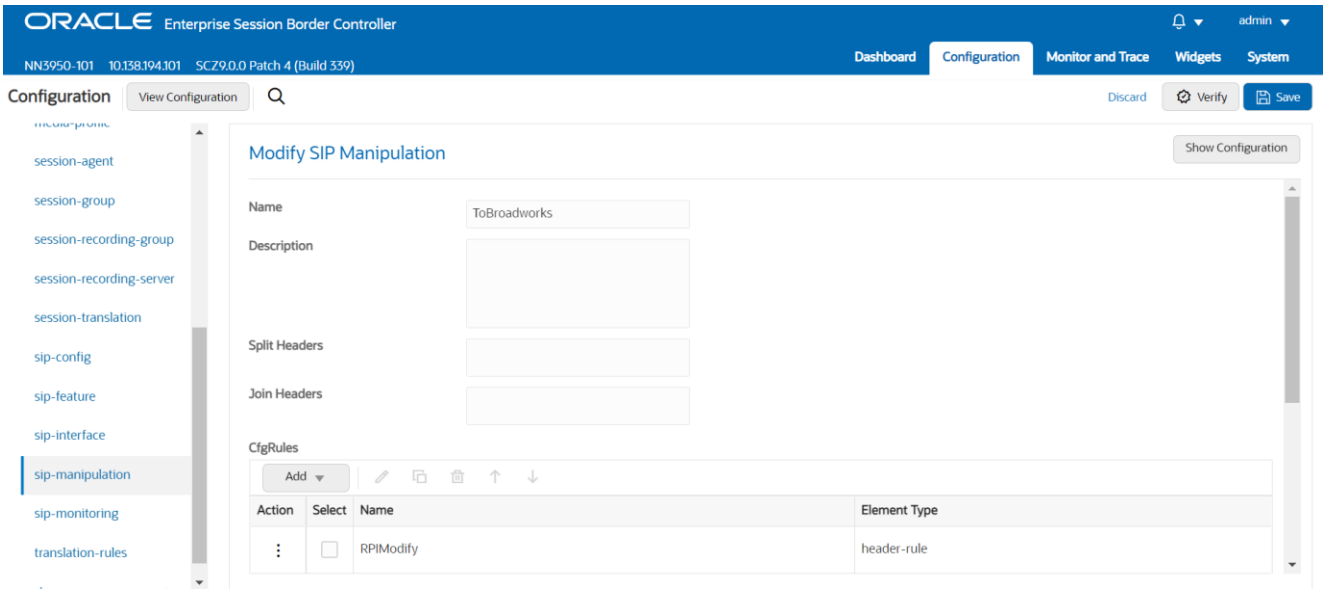
S

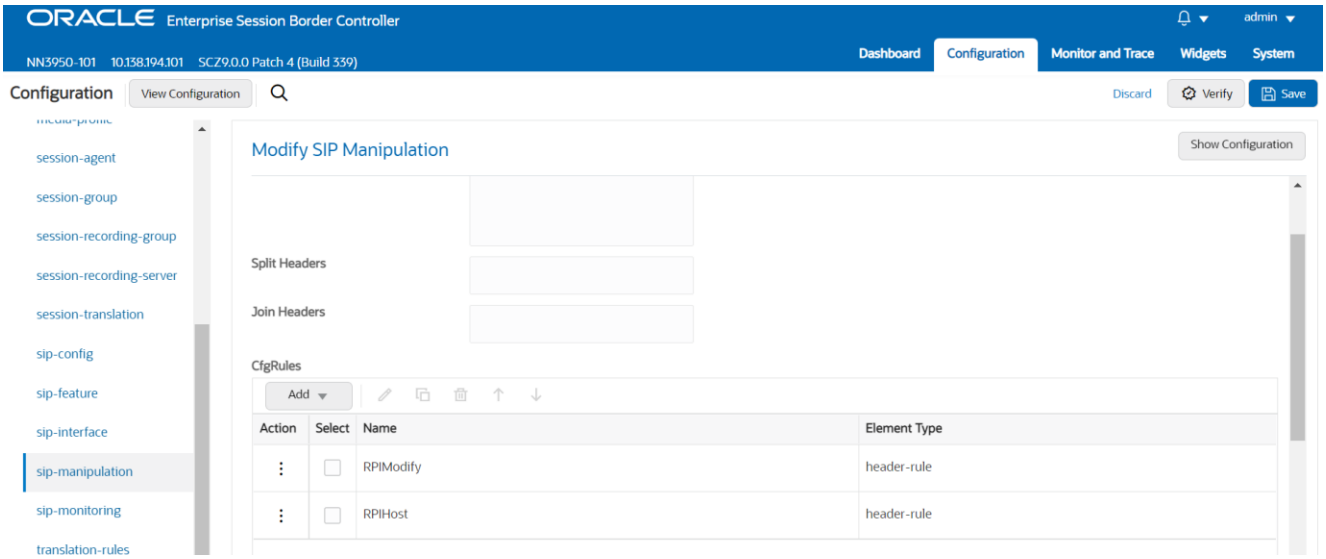
Similarly, Please Configure sip-interface for the Cisco Broadworks as below:

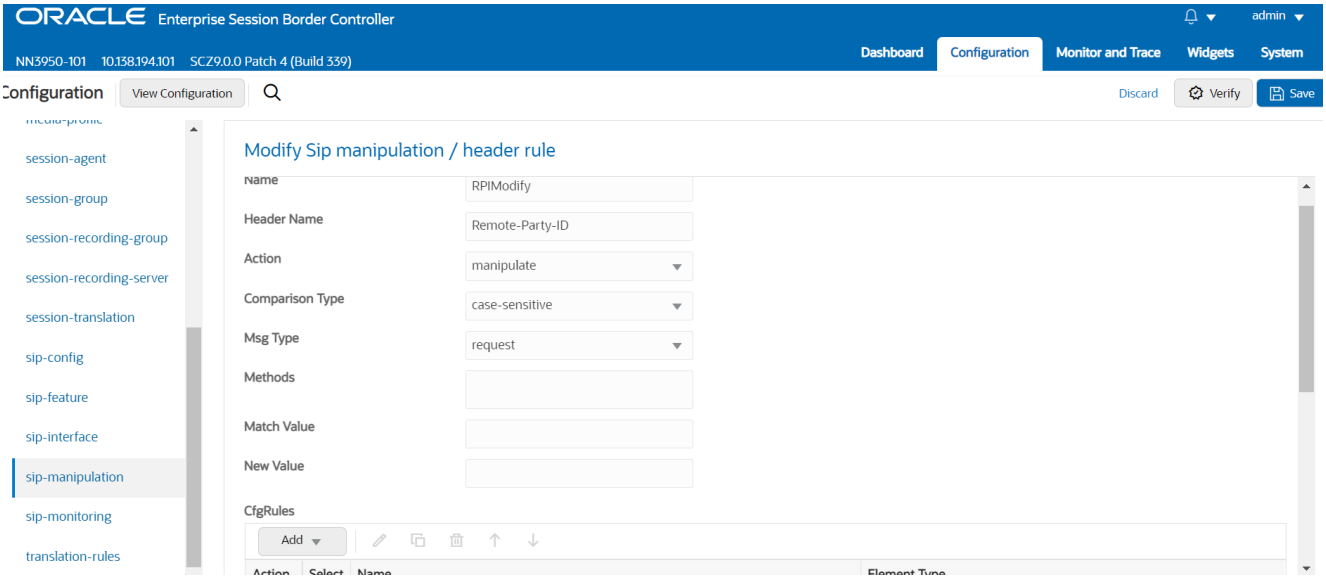


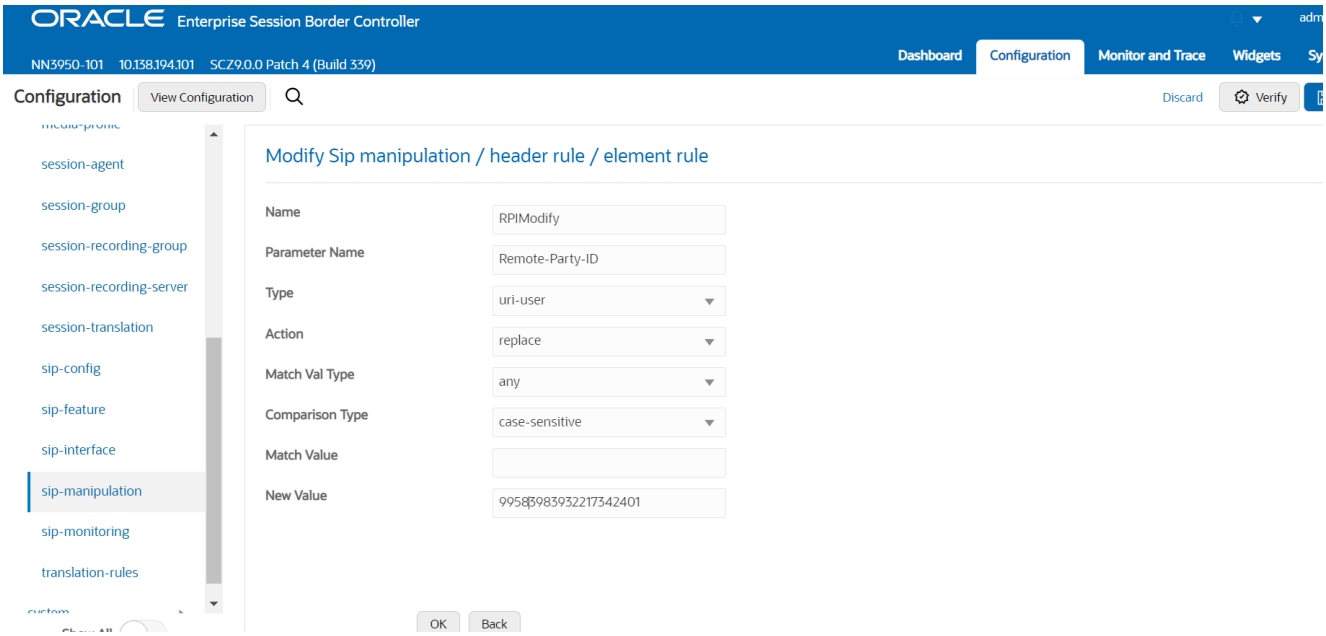
Please assign the below sip-manipulation as the out-manipulation ID in the PSTN sip interface. It consists of 2 sip-manipulations

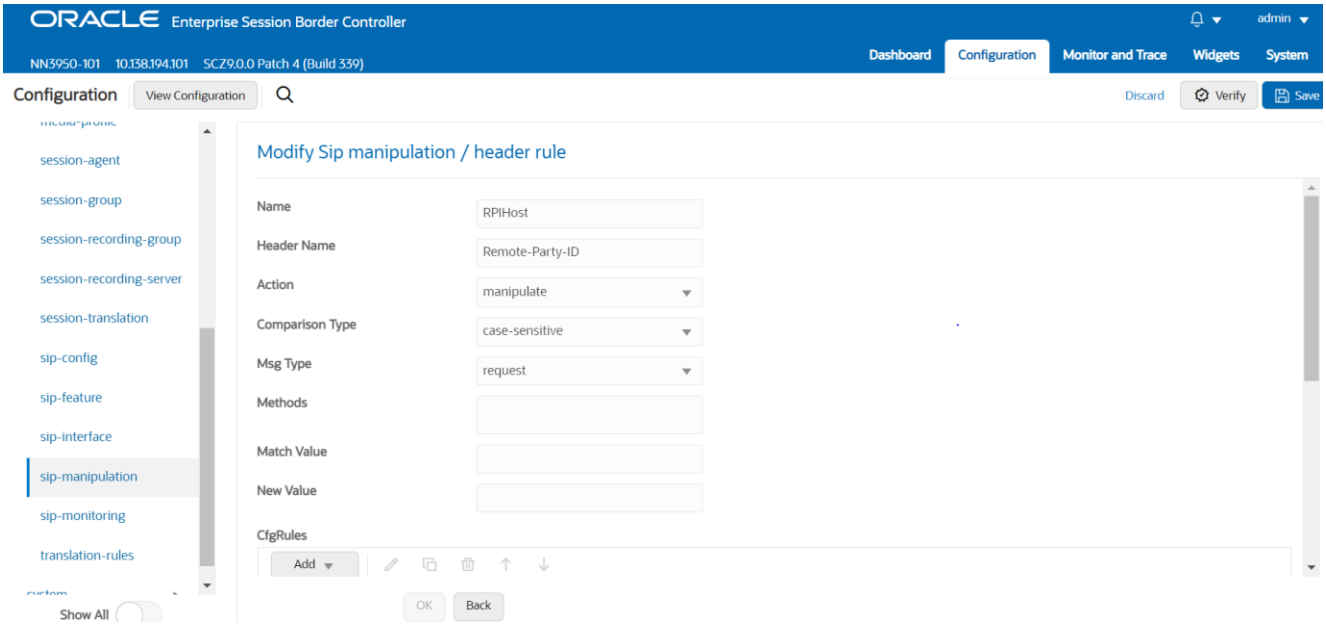
1. RPIModify: To replace the Remote-Party-ID user part to the Access code (for the meeting) that is generated as a apart of using Broadworks Subscriber API's on the Webex for a particular phone number and a SRV group.
2. RPIHost: To change the host part of uri from private fqdn to the Webex session-agent FQDN.

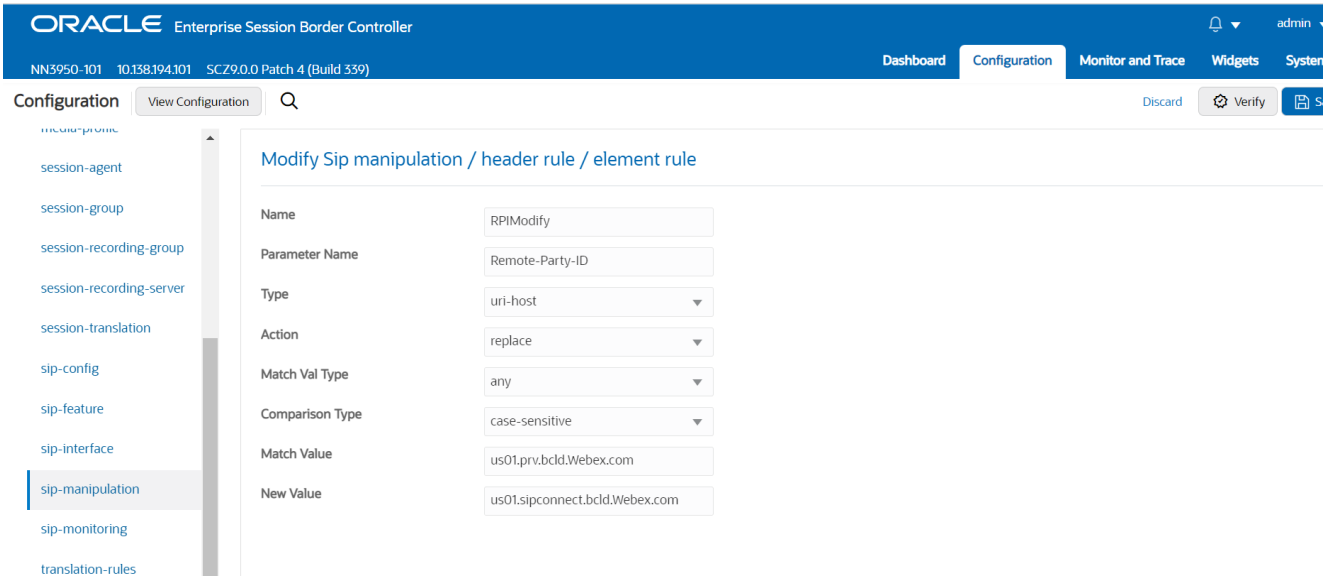



ORACLE Enterprise Session Border Controller
admin
NN3950-101 10.138.194.101 SCZ9.0.0 Patch 4 (Build 339)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
Save
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
translation-rules
Modify SIP Manipulation
Show Configuration
Split Headers
Join Headers
CfgRules
Add
Action
Select
Name
Element Type
RPIModify
header-rule
RPIHost
header-rule


ORACLE Enterprise Session Border Controller
admin
NN3950-101 10.138.194.101 SCZ9.0.0 Patch 4 (Build 339)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
Save
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
translation-rules
Modify Sip manipulation / header rule
Name
RPIModify
Header Name
Remote-Party-ID
Action
manipulate
Comparison Type
case-sensitive
Msg Type
request
Methods
Match Value
New Value
CfgRules
Add


ORACLE Enterprise Session Border Controller
NN3950-101 10.138.194.101 SCZ9.0.0 Patch 4 (Build 339)
Dashboard
Configuration
Monitor and Trace
Widgets
Configuration
View Configuration
Discard
Verify
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
translation-rules
Modify Sip manipulation / header rule / element rule
Name
RPIModify
Parameter Name
Remote-Party-ID
Type
uri-user
Action
replace
Match Val Type
any
Comparison Type
case-sensitive
Match Value
New Value
9958398393221734240 1
OK
Back


ORACLE Enterprise Session Border Controller
admin
NN3950-101 10.138.194.101 SCZ9.0.0 Patch 4 (Build 339)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
Save
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
translation-rules
Show All
Modify Sip manipulation / header rule
Name
RPIHost
Header Name
Remote-Party-ID
Action
manipulate
Comparison Type
case-sensitive
Msg Type
request
Methods
Match Value
New Value
CfgRules
Add
OK
Back



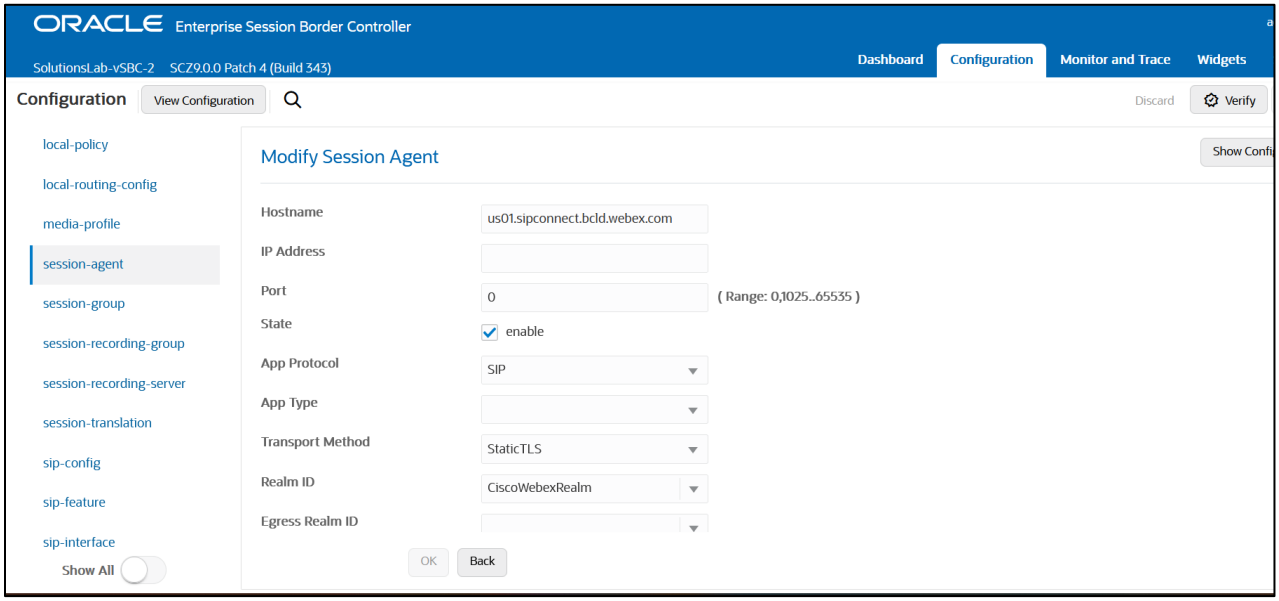
Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

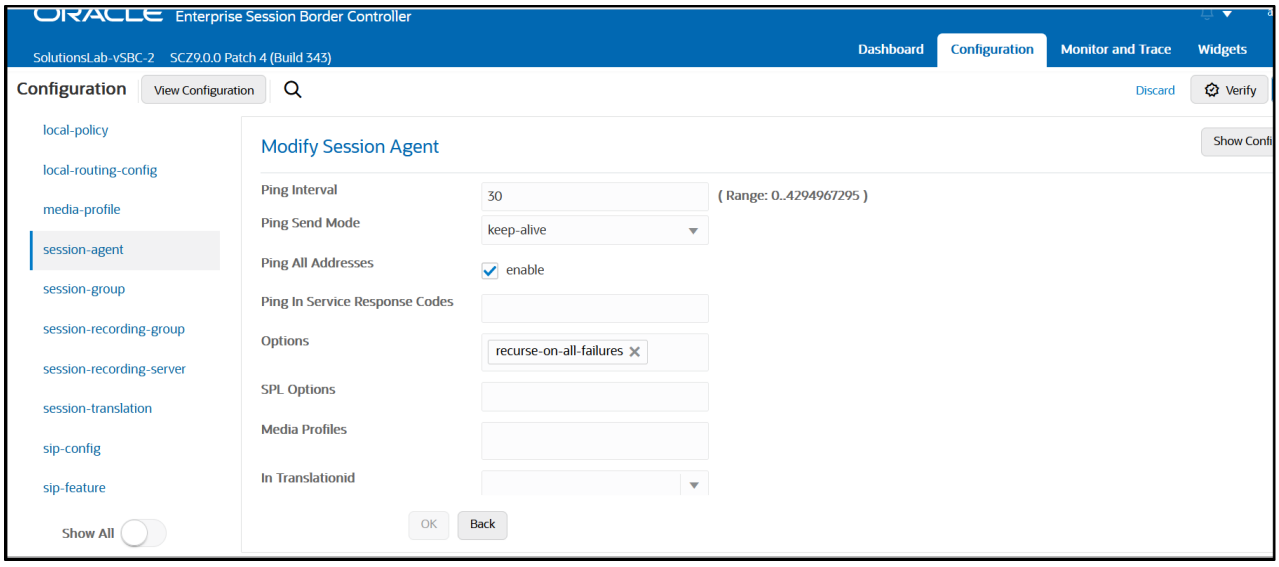
5.12. Configure session-agent

Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

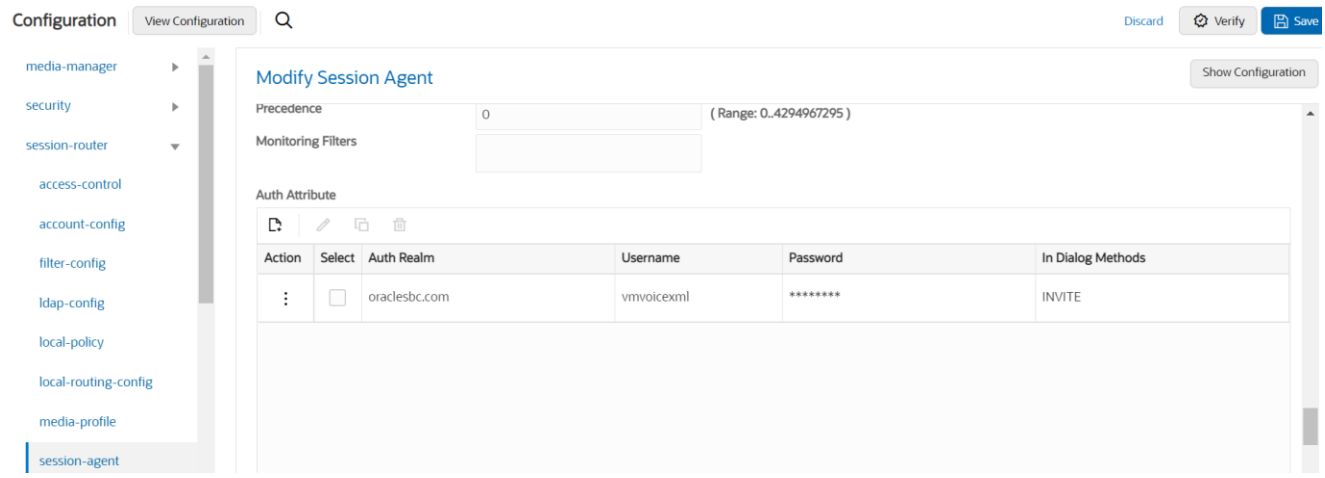
Go to session-router->Session-Agent and Configure the session-agents for the Cisco Webex Meetings

- Host name to "**us01.sipconnect.bcld.Webex.com**", which is SRV based SA.
- When Using SRV as session agent, please make **port as 0** so that SRV will work properly.
- realm-id – needs to match the realm created for the Cisco Webex Meetings .
- transport set to "staticTLS"
- Please enable the parameters **ping all addresses, ping-response**,
- Please enable hidden option **load-balance-dns-query** and **recurse-on-all-failures and set out-service-response-codes parameter to 408,503**
- Please set ping method to OPTIONS and ping-interval duration in secs.



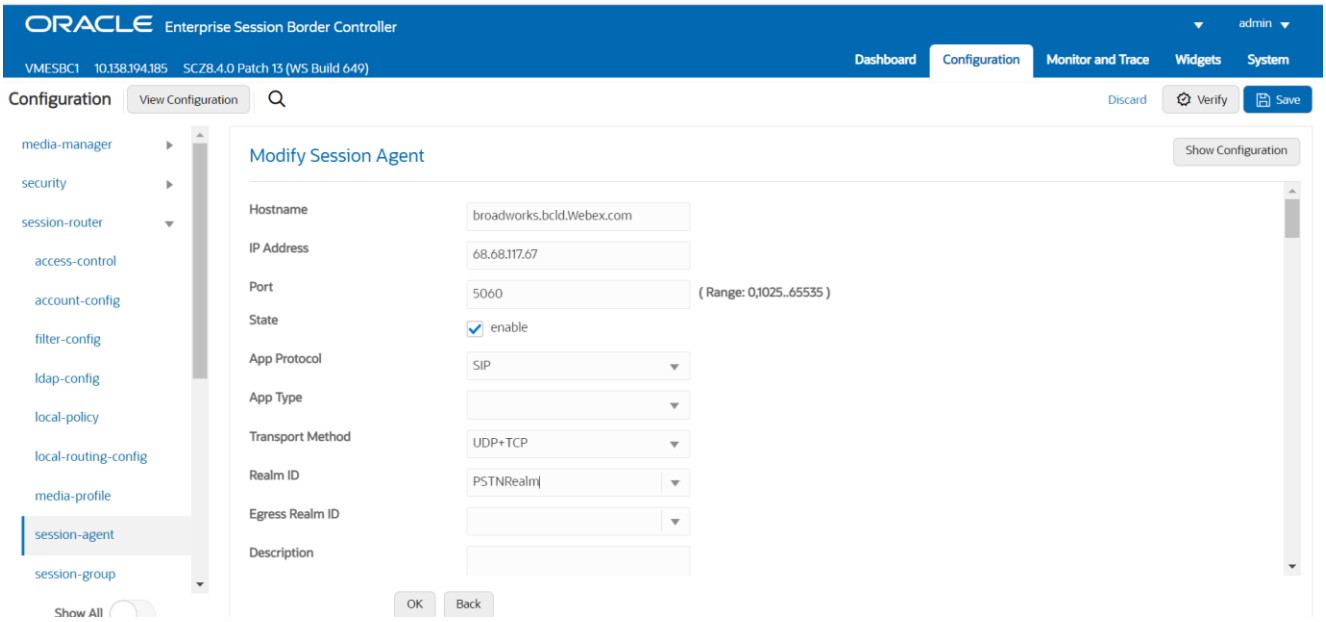


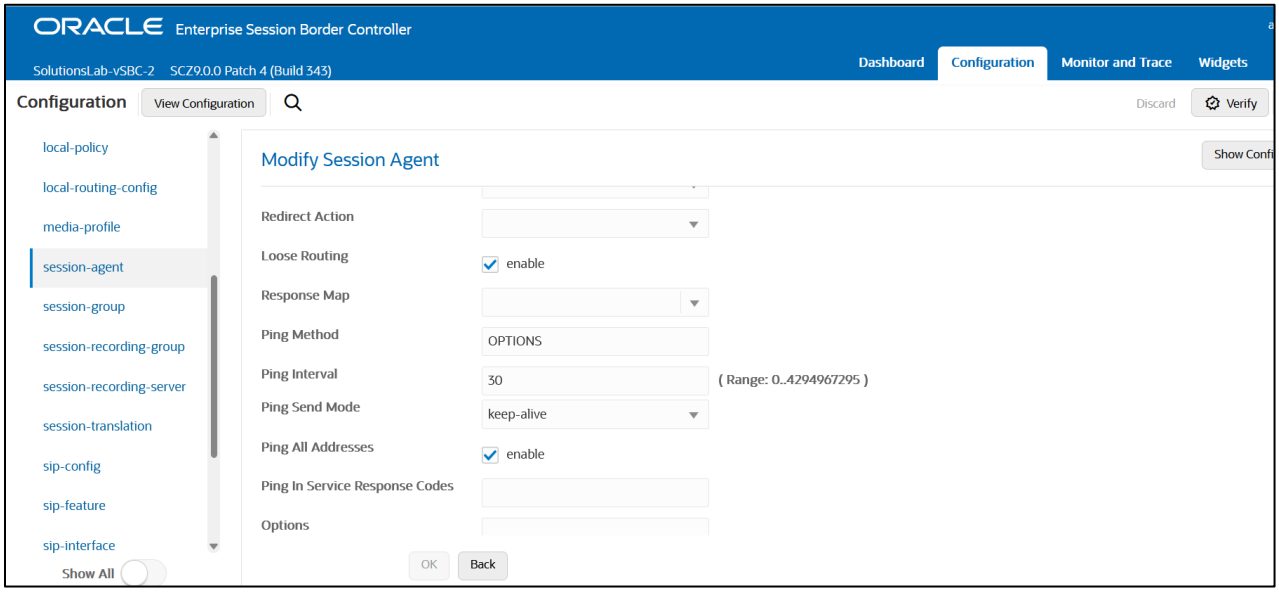
Add the auth-attributes (username and password)as configured on Cisco Broadworks Authentication config.This config is only on the Webex Meetings session-agent.



Similarly, configure the session-agents for the Cisco Broadworks as below:

Configure the hostname as the FQDN and IP Address as IP of Cisco Broadworks as shown below. Protocol should be UDP+TCP.

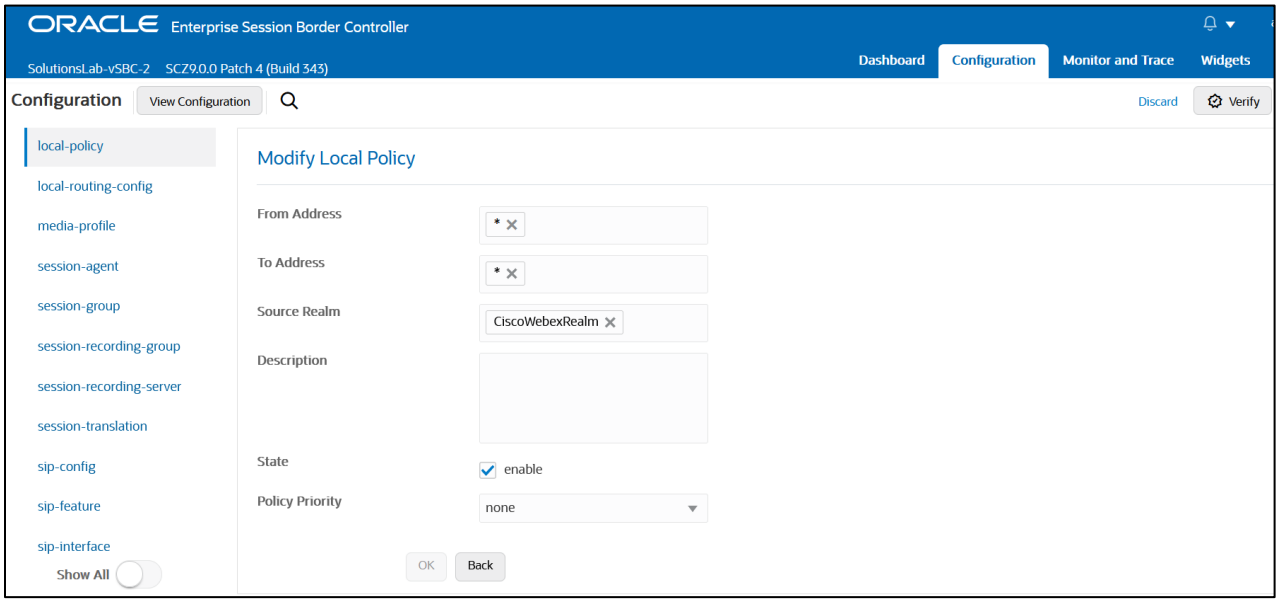


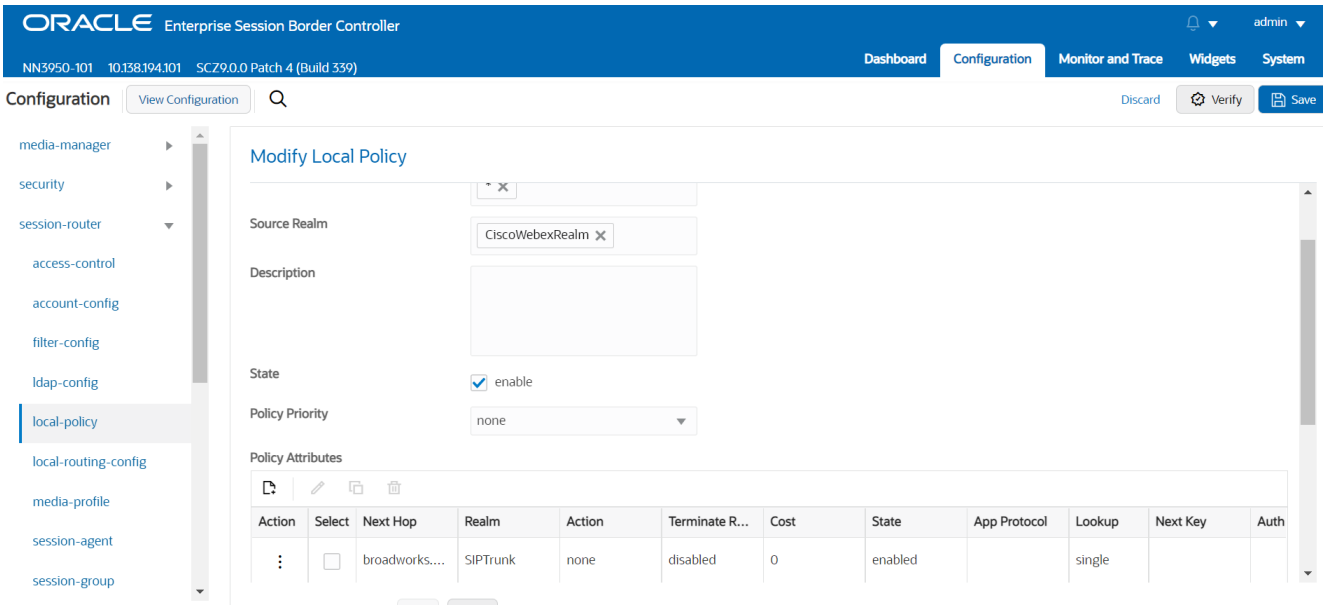


5.13. Configure local-policy

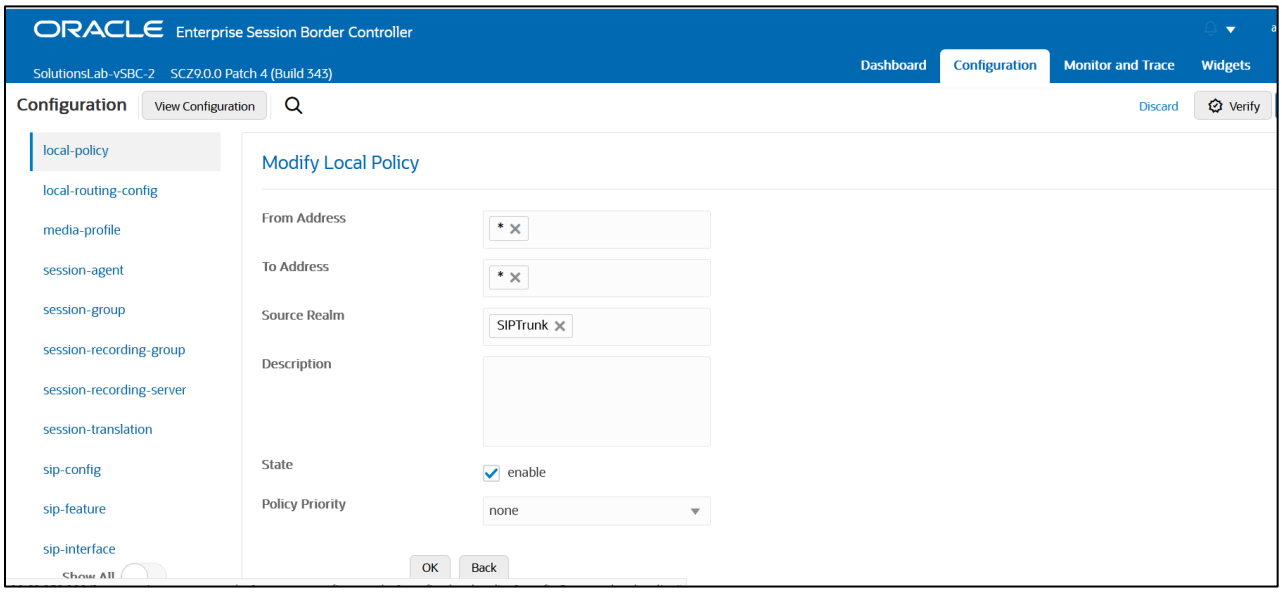
Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

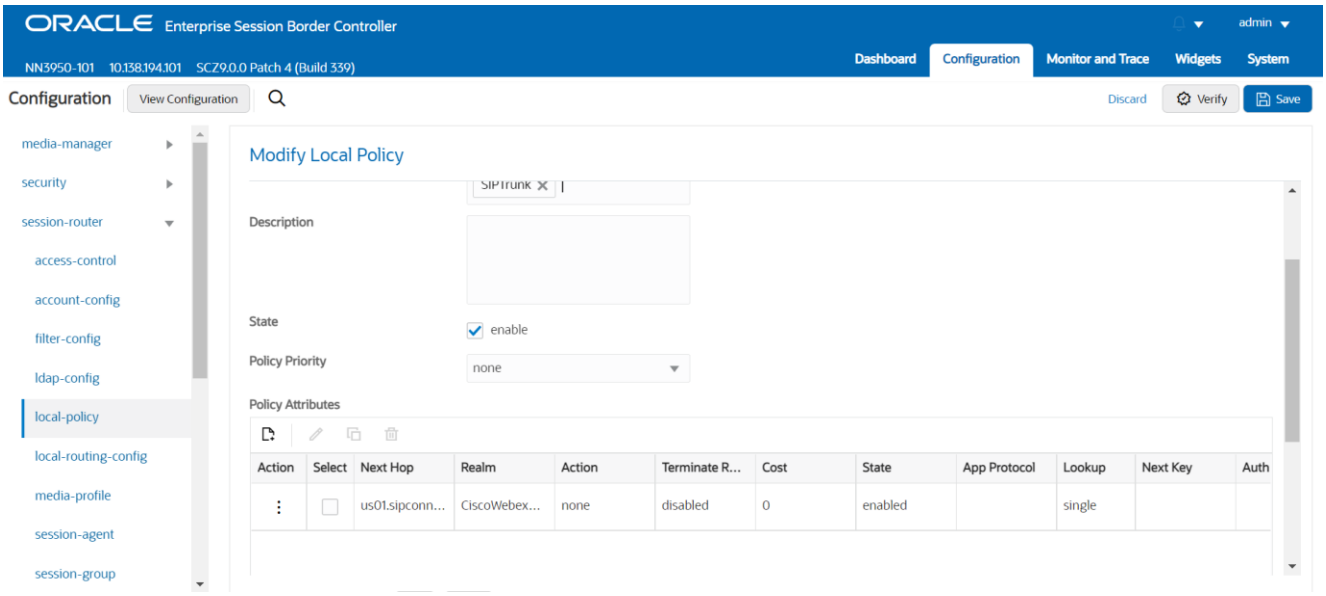
To route the calls from Cisco Webex Meetings to Cisco Broadworks, Use the below local –policy





To route the calls from the Cisco Broadworks to Cisco Webex Meetings , Use the below local–policy

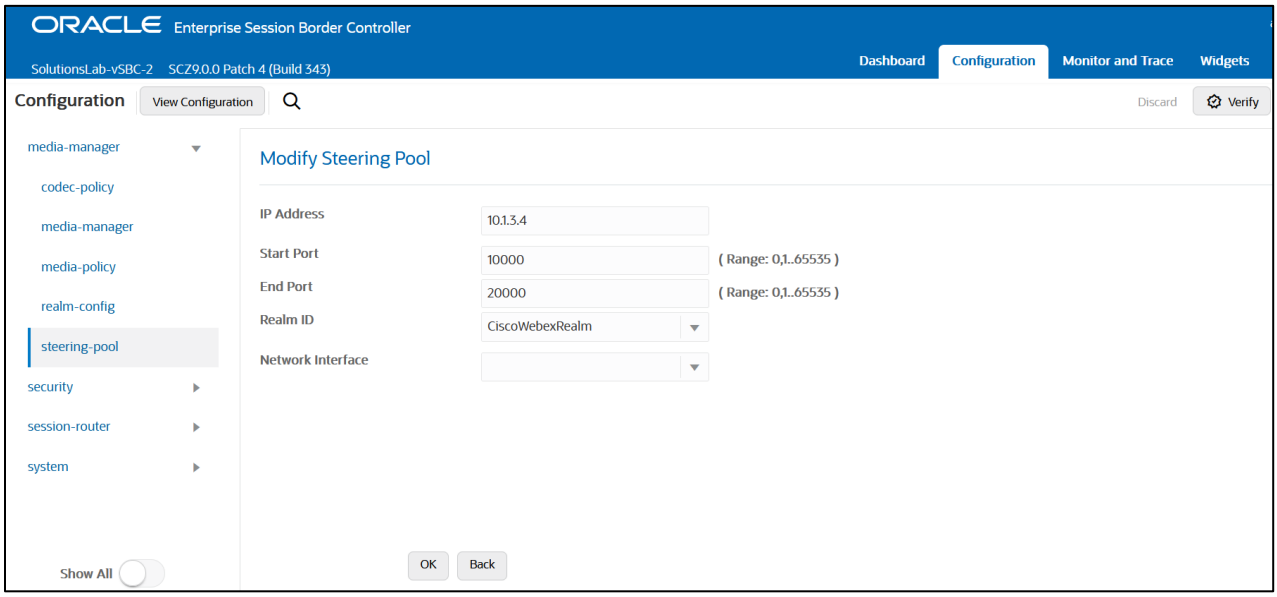




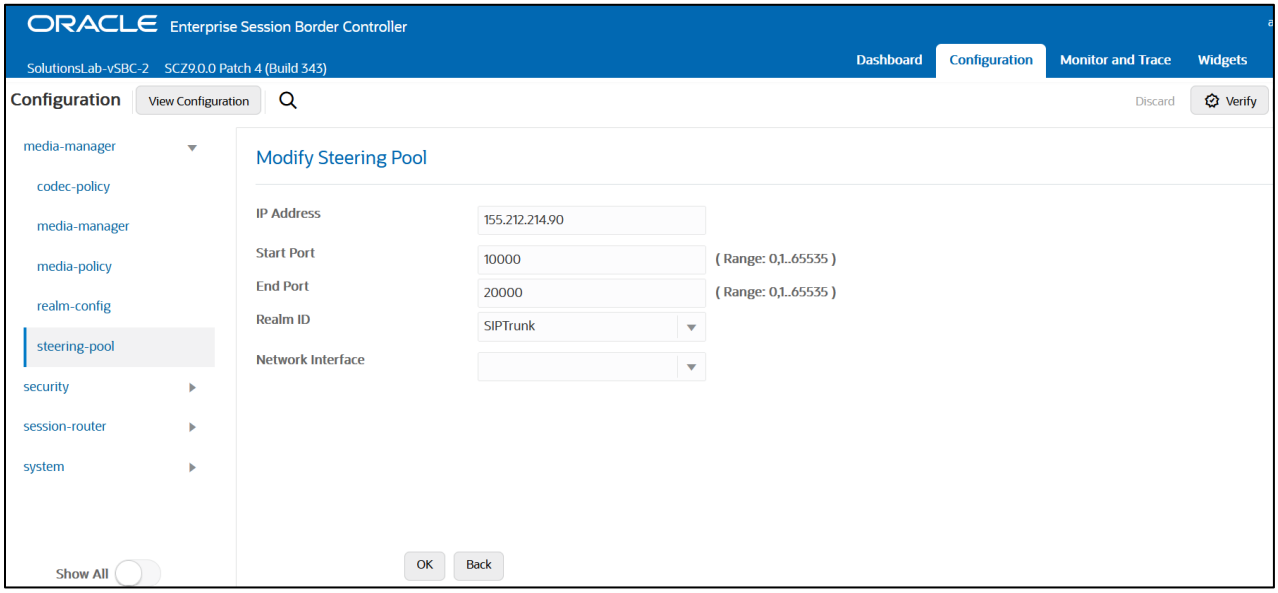
5.14. Configure steering-pool

Steering-pool config allows configuration to assign IP address(es), ports & a realm.

Cisco Webex Meetings steering pool.

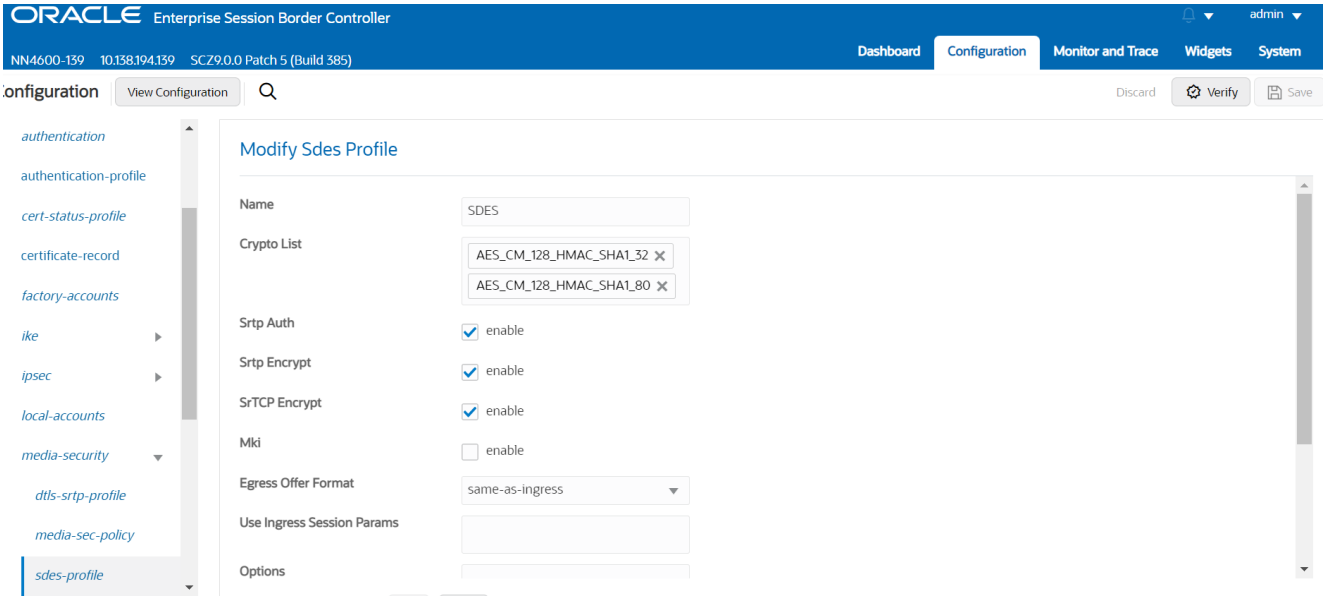


Cisco Broadworks steering pool.



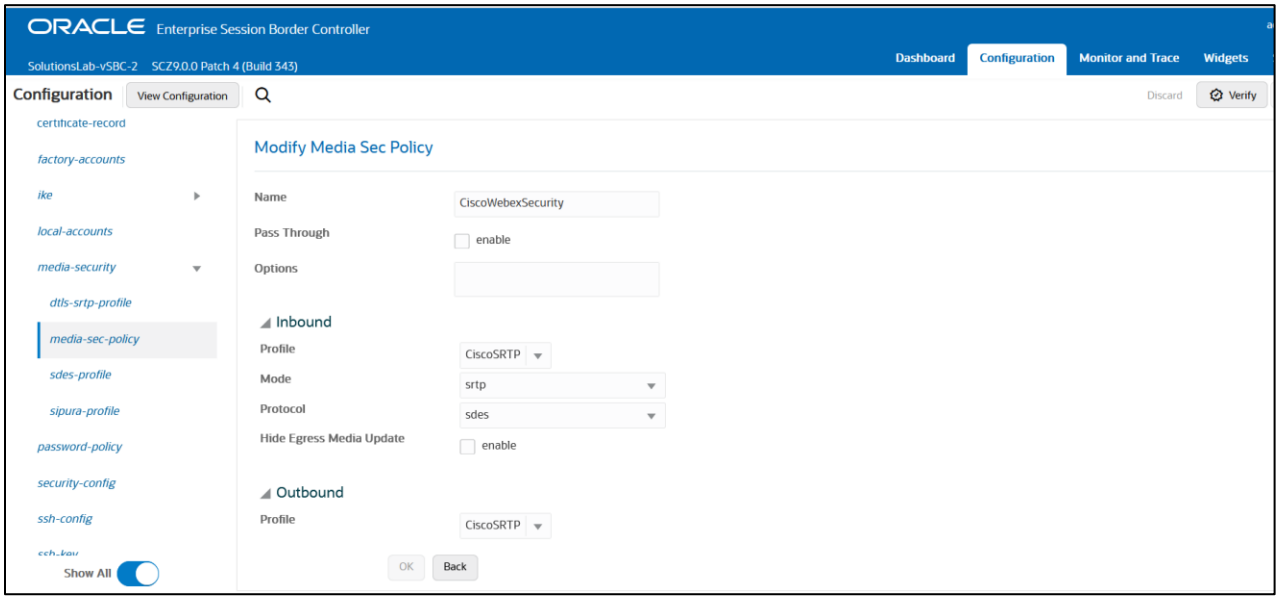
5.15. Configure sdes profile

Please go to →Security → Media Security →sdes profile and create the policy as below.

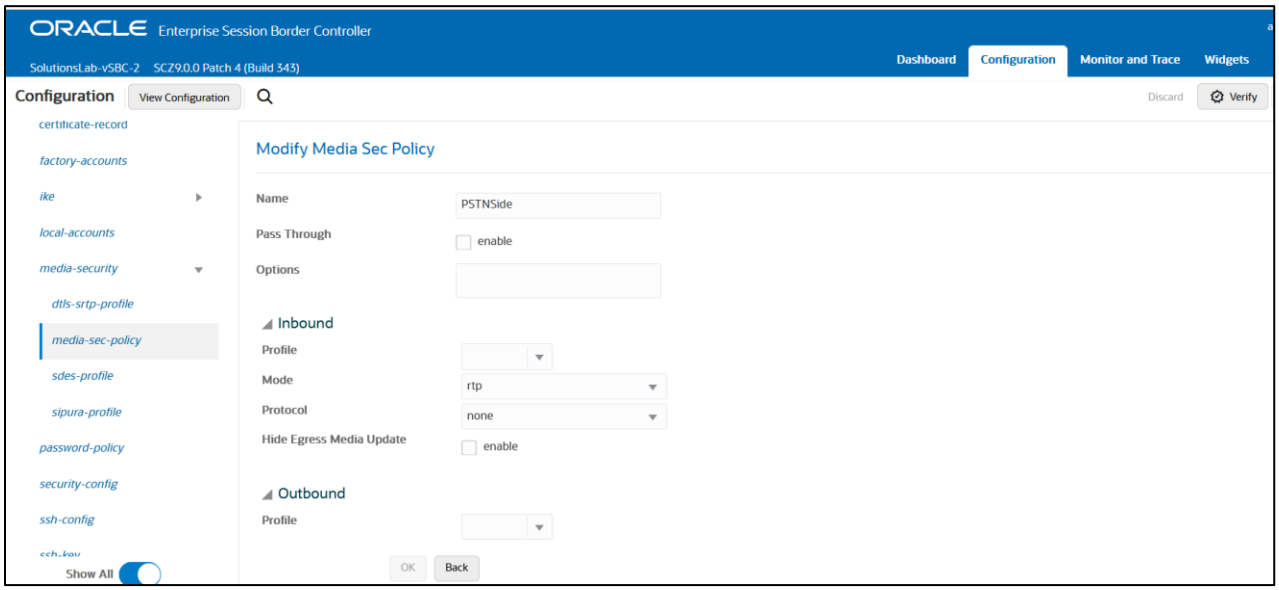


5.16. Configure Media Security Profile

Please go to →Security → Media Security →media Sec policy and create the policy as below:
Create Media Sec policy with name CiscoWebexSecurity which will have the sdes profile created above.
Assign this media policy to the Cisco Webex Realm



Similarly, Create Media Sec policy with name PSTNSide to convert srtp to rtp for the Cisco Broadworks which
will use only TCP/UDP as transport protocol. **Assign this media policy to the PSTN Realm.**



6. Existing SBC configuration

If the SBC being used is an existing SBC with functional configuration, following configuration elements are required:

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

ORACLE

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