Oracle Session Border Controller (SBC) integration with Five9 Cloud Contact Center

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.

Version History

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC and Five9 Cloud Contact Center Config	18 Nov 2021

Table of Contents

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 (E-SBC). It is assumed that the reader is familiar with basic operations of the Oracle Communications Enterprise Session Border Controller platform along with Five9 and how SIP Trunking is implemented.

2. Document Overview

This Oracle technical application note outlines the configuration needed to set up the interworking between Oracle SBC and Five9 Cloud Contact Center Platform. The solution contained within this document has been tested using Oracle Communication 840. Our scope of this document is only limited to testing Oracle SBC with Five9 Cloud Contact Center Platform.

It should be noted that this application note focuses on the optimal configurations for the Oracle SBC in a Five9 BYOC Calling Environment. Many SBC applications may have additional configuration requirements that are specific to individual customer requirements. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

Related Documentation can be found below:

2.1 Oracle SBC

- Oracle® Enterprise Session Border Controller ACLI Configuration Guide
- Oracle® Enterprise Session Border Controller Release Notes
- Oracle® Enterprise Session Border Controller Security Guide

2.2 Five9 BYOC

- Five9® Contact Center Resources
- Five9® Softphone-Software
- Five9® Cloud Contact Center
- Five9® Cloud PBX

Please note that the IP address, FQDN and config name and its details given in this document is used as reference purpose only. The same details cannot be used in customer config and the end users can use the configuration details according to their network requirements.

3. Introduction

3.1 Audience

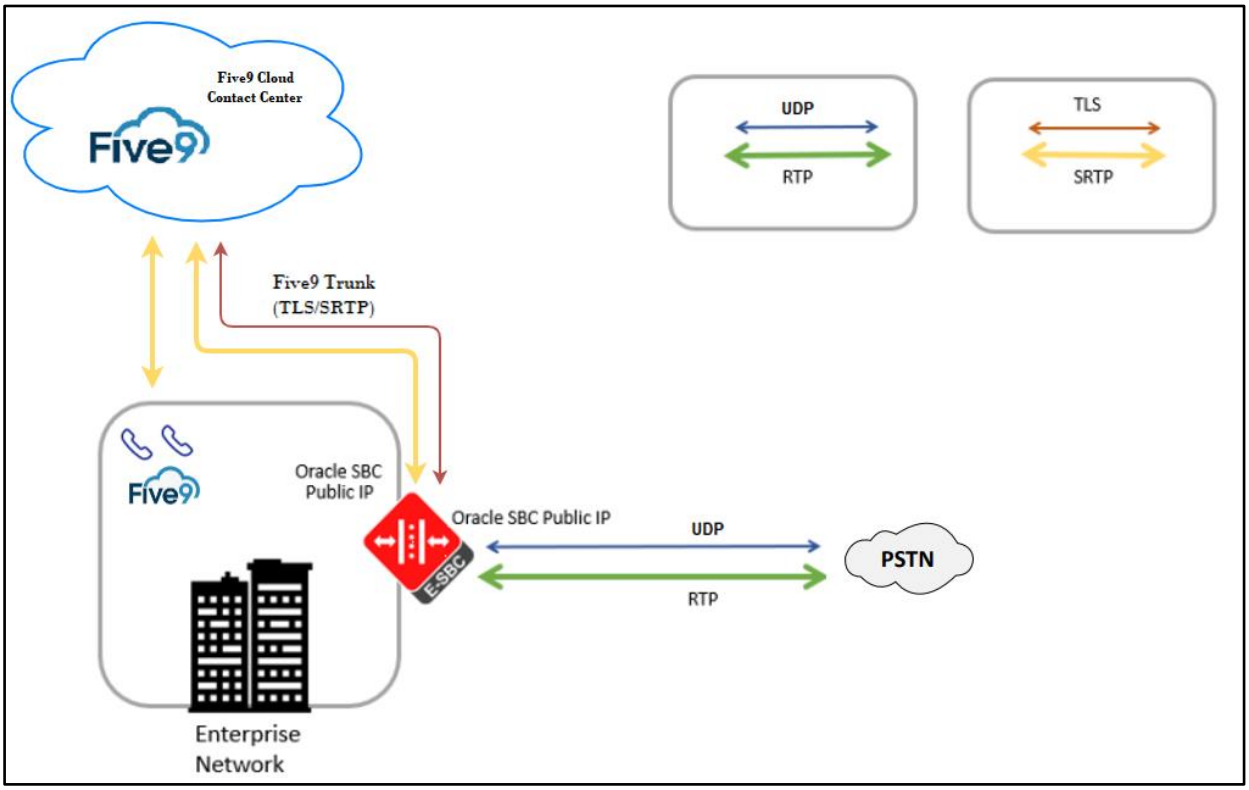
This is a technical document intended for telecommunications engineers with the purpose of configuring Five9 Cloud Contact Center Platform using Oracle Enterprise SBC. There will be steps that require navigating the Five9 Platform and Oracle SBC GUI interface. Having an understanding of the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

3.2 Requirements

- Five9 Cloud Contact Center Platform
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version

3.3 Architecture

This is a technical document intended for telecommunications engineers with the purpose of configuring Five9 Cloud Contact Center Platform using Oracle Enterprise SBC. There will be steps that require navigating the Five9 Platform and Oracle SBC GUI interface. Having an understanding of the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.



Above figure illustrates the connection between Five9, Oracle SBC and SIPTrunk. Both Five9 and SIPTrunk are connected to the Oracle SBC Public FQDN /IP. The connection between Five9 and Oracle SBC is TLS/SRTP and between SIPTrunk and Oracle SBC is UDP/RTP. Oracle SBC is used to steer the signaling, media to, and from the Five9 to SIPTrunk.

4. Configuring the Five9 Cloud Contact Center

Five9's "Bring your own carrier" (BYOC) enables users to dial out from a Five9-Cloud Contact Center to PSTN numbers such as landline phones, mobile phones and audio bridges, meaning that organizations no longer need a separate telephone in conference rooms. The customer selects and engages a telephony carrier and provides implementation details to their partner who then creates the necessary configuration. When a call is placed, the Five9 Service routes it out to the chosen carrier who then handles the call rest of the way.

Note: The document only includes the steps required to configure Oracle SBC. Additional configuration may apply which may not be covered in this document. Please work with your Five9 representative for the most optimal Five9 configuration as per your requirement.

5. Configuring the SBC

This chapter provides systematic guidance on how to configure Oracle SBC for interworking with Five9 Cloud Contact Center Platform and SIP Trunk.

5.1 Validated Oracle SBC version

All testing was completed using Oracle 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
- VME
- AP 3950 (Supported Software – 9.0)
- AP 4900 (Supported Software – 9.0)

6. New SBC configuration

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

6.1 Establishing a serial connection to the SBC

Note: The below method is applicable to the SBCs running on Hardware Platforms. For VME and Cloud SBCs the method of configuration will be different to as shown below. Follow the appropriate documentation or contact your Oracle representative for details about how to configure the VME and Cloud SBC platforms.

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

```
Starting tLemd...
Starting tServiceHealth...
Starting tCollect...
Starting tAtcpd...
Starting tAsctpd...
Starting tMbcd...
Starting tCommMonitord...
Starting tFped...
Starting tAlgd...
Starting tRadd...
Starting tEbmd...
Starting tSipd...
Starting tH323d...
Starting tbfdd...
Starting tIPTd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tTscfd...
Starting tFcgid...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Starting tIFMIBd...
Start platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...

Starting acliMgr...
password secure mode is enabled
Admin Security is disabled
Password:
```

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” for the Hardware and VME Platform.

Follow the appropriate documentation or contact your Oracle representative for details about how to configure the Cloud SBC platforms.

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

```
Password:
%
% Only alphabetic (upper or lower case), numeric and punctuation
% characters are allowed in the password.
% Password must be 8 - 64 characters,
% and have 3 of the 4 following character classes :
%      - lower case alpha
%      - upper case alpha
%      - numerals
%      - punctuation
%
Enter New Password:
Confirm New Password:

Password is acceptable.
```

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

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

```
OracleESBC#
OracleESBC# con t
OracleESBC(configure)# bootparam

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

Boot File               : /boot/nnSCZ840p8.bz
IP Address              : 10.138.194.139
VLAN                    : 0
Netmask                 : 255.255.255.192
Gateway                 : 10.138.194.129
IPv6 Address            :
IPv6 Gateway            :
Host IP                 :
FTP username            : vxftp
FTP password            : ********
Flags                   :
Target Name             : OracleESBC
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.



OracleESBC(configure)#
```

Note: There is no management IP configured by default.

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

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

```
OracleESBC# setup product

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

Last Modified 2021-11-16 16:15:17
----------------------------------------------------------------
 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.

Navigate to configure terminal->system->http-server-config.

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

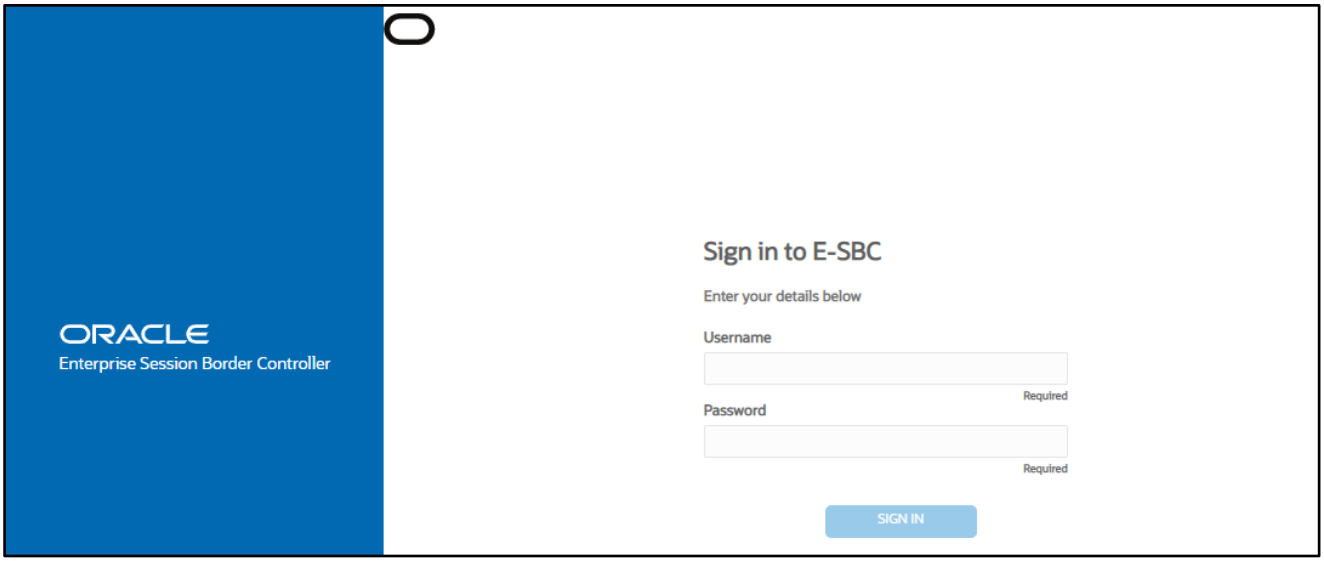
```
OracleESBC(http-server)# show
http-server
        name                                    webServerInstance
        state                                   enabled
        realm
        ip-address
        http-state                              enabled
        http-port                               80
        https-state                             disabled
        https-port                              443
        http-interface-list                     REST,GUI
        http-file-upload-size                   0
        tls-profile
        auth-profile
        last-modified-by                        admin@73.69.242.156
        last-modified-date                      2021-11-16 16:19:41

OracleESBC(http-server)#
```

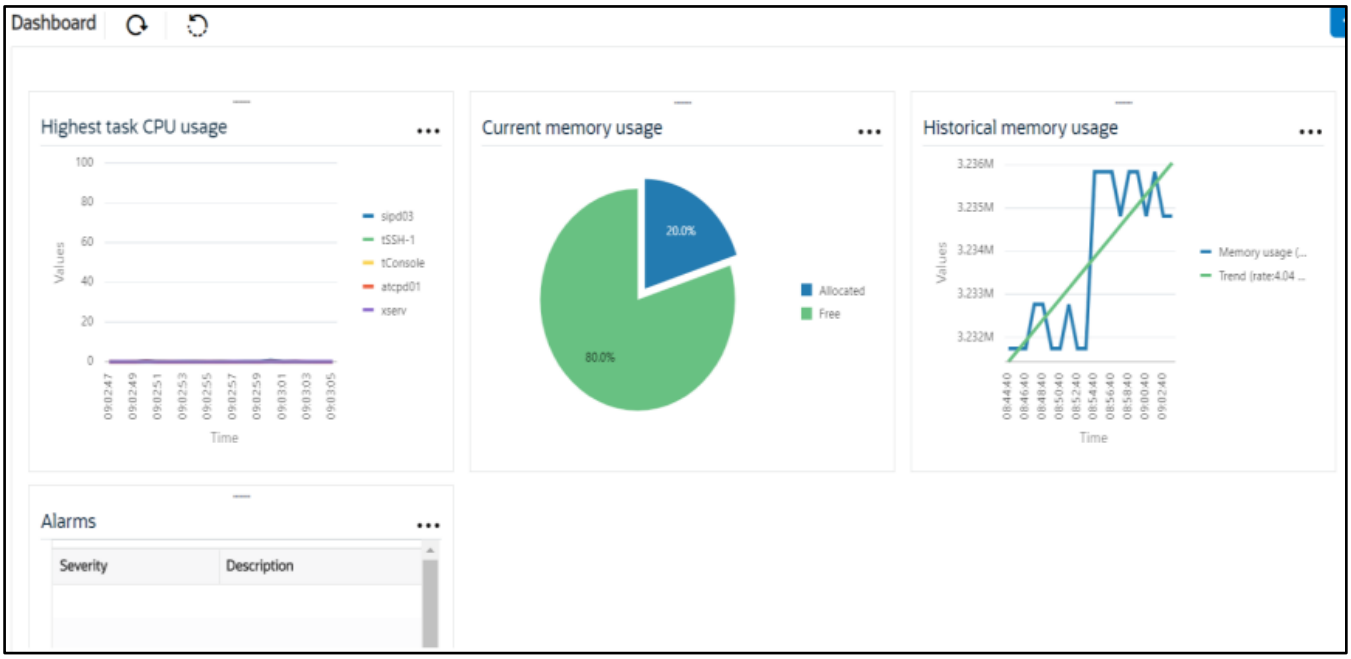
6.2 Configure SBC using Web GUI

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

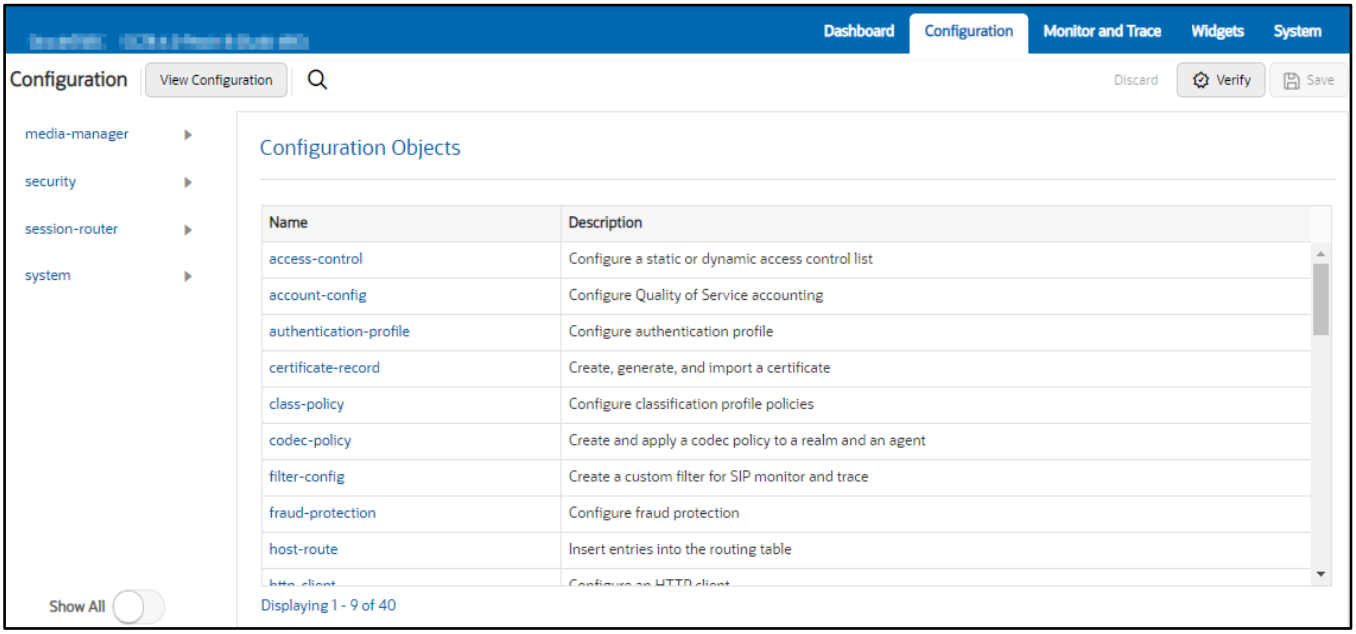
The Web GUI can be accessed through the URL http://<SBC_MGMT_IP>.



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



Navigate to Configuration as shown below, to configure the SBC.



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

https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.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.

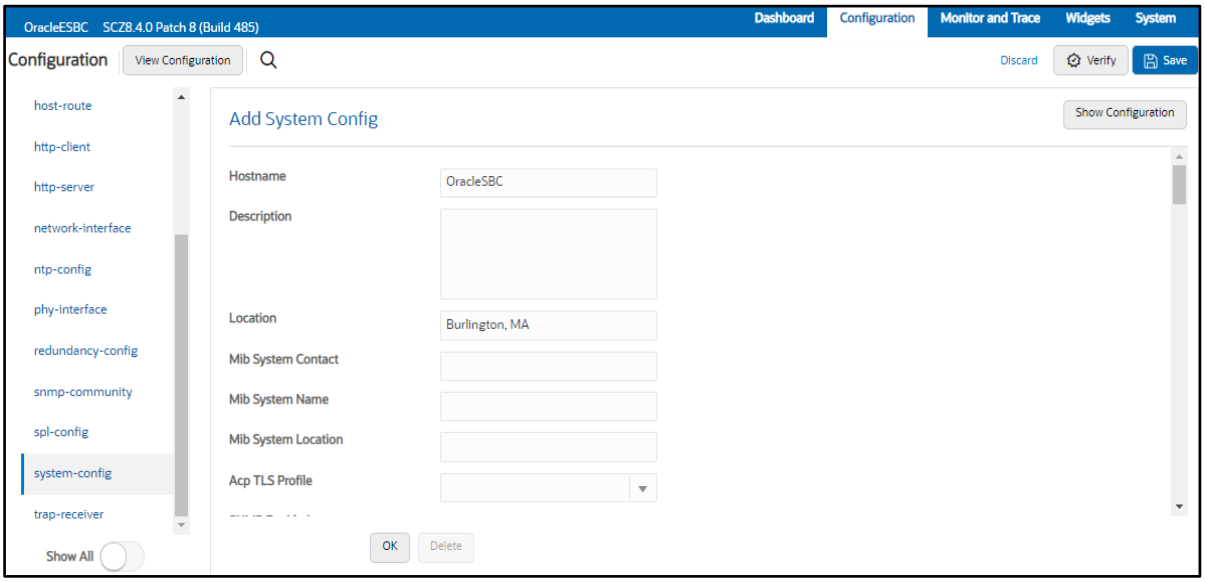
6.3 Configure system-config

To configure system level functionality for the OCSBC, you must first enable the system-config

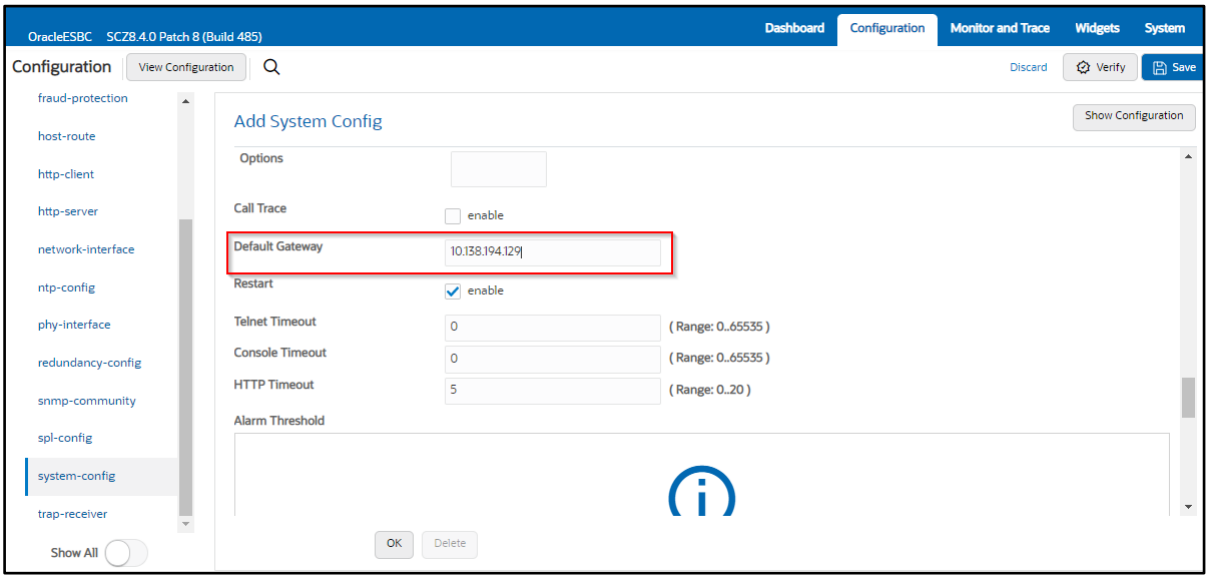
Navigate to system->system-config
ACLI Path: config t->system->system-config

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

- Hostname
- Description
- Location
- Default Gateway (recommended being the same as management interface gateway)



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



6.4 Configure Physical Interface values

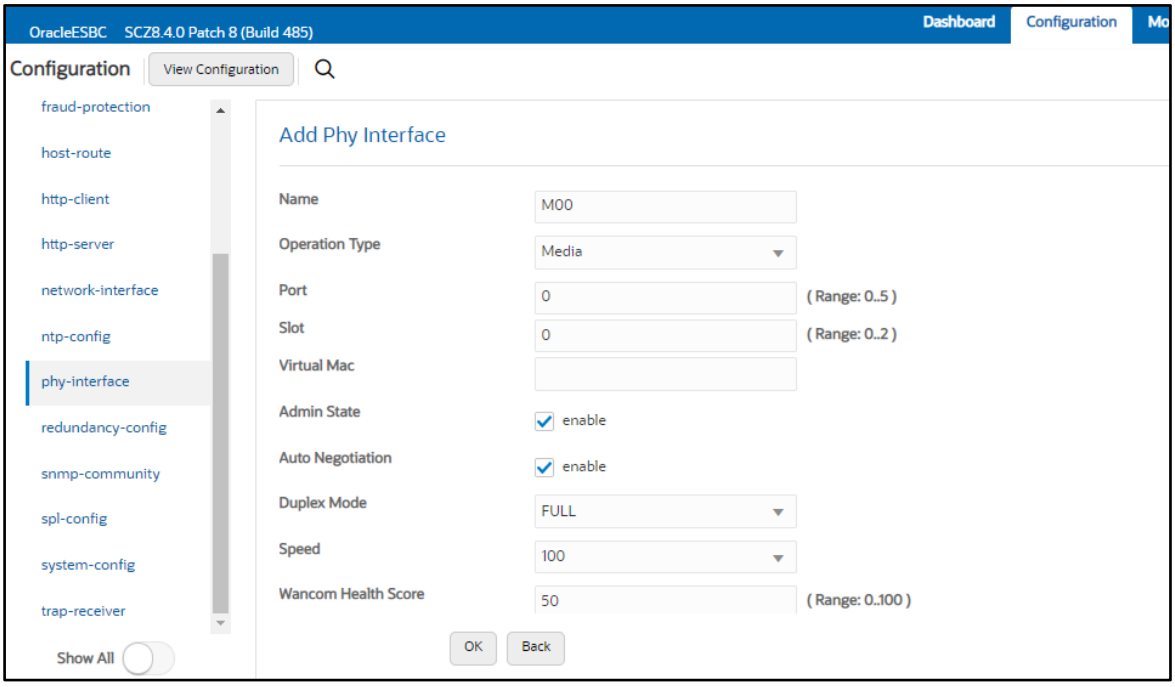
To configure physical Interface values, navigate to System->phy-interface.

ACLI Path: config t->system->phy-interface

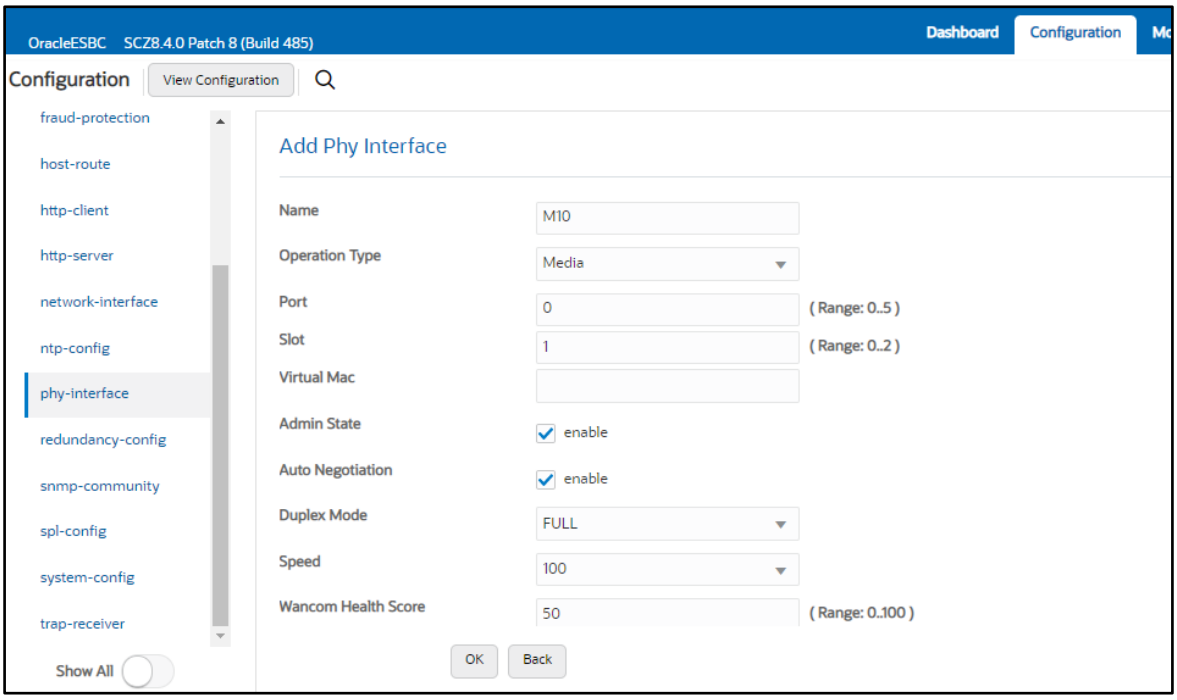
Please configure phy-interface M00 for Five9 side and M10 for SIPTrunk side.

Parameter Name	Five9 (M00)	SIPTrunk (M10)
Slot	0	1
Port	0	0
Operation Mode	Media	Media

Configure **M00** interface as per example shared below.



Configure **M10** interface as per example shared below.



6.5 Configure Network Interface values

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

ACLI Path: config t->system->network-interface

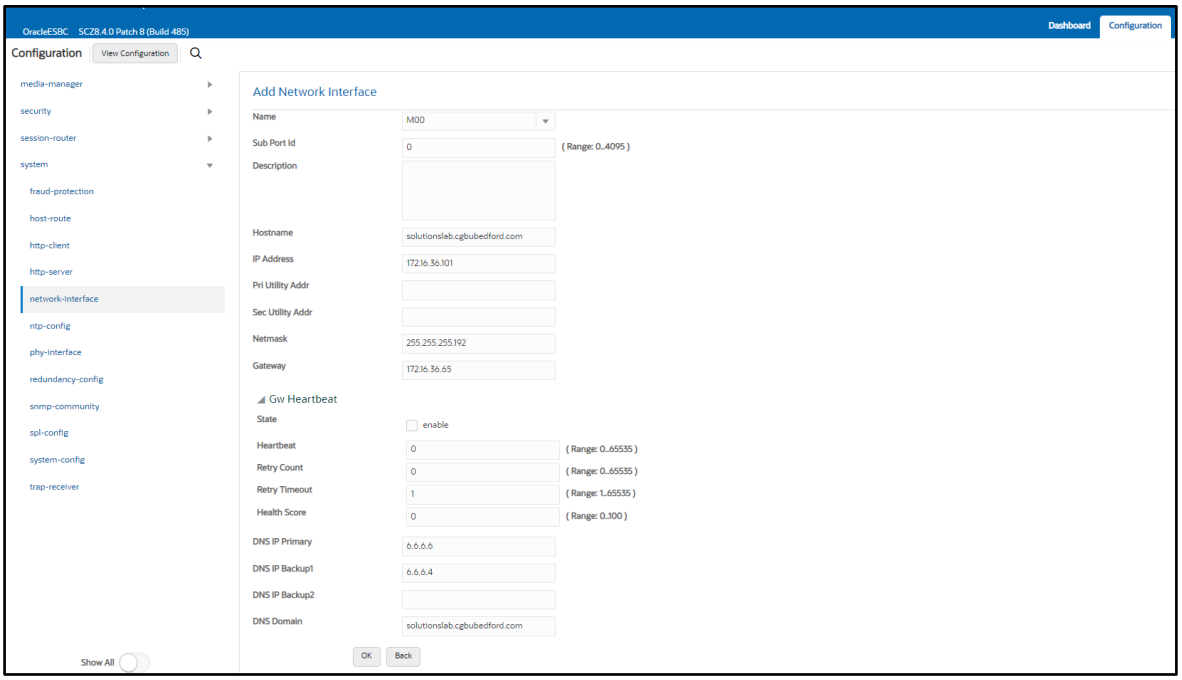
The table below lists the parameters, to be configured for both the interfaces.

Note: The provided network IP addresses are given for example purpose only.

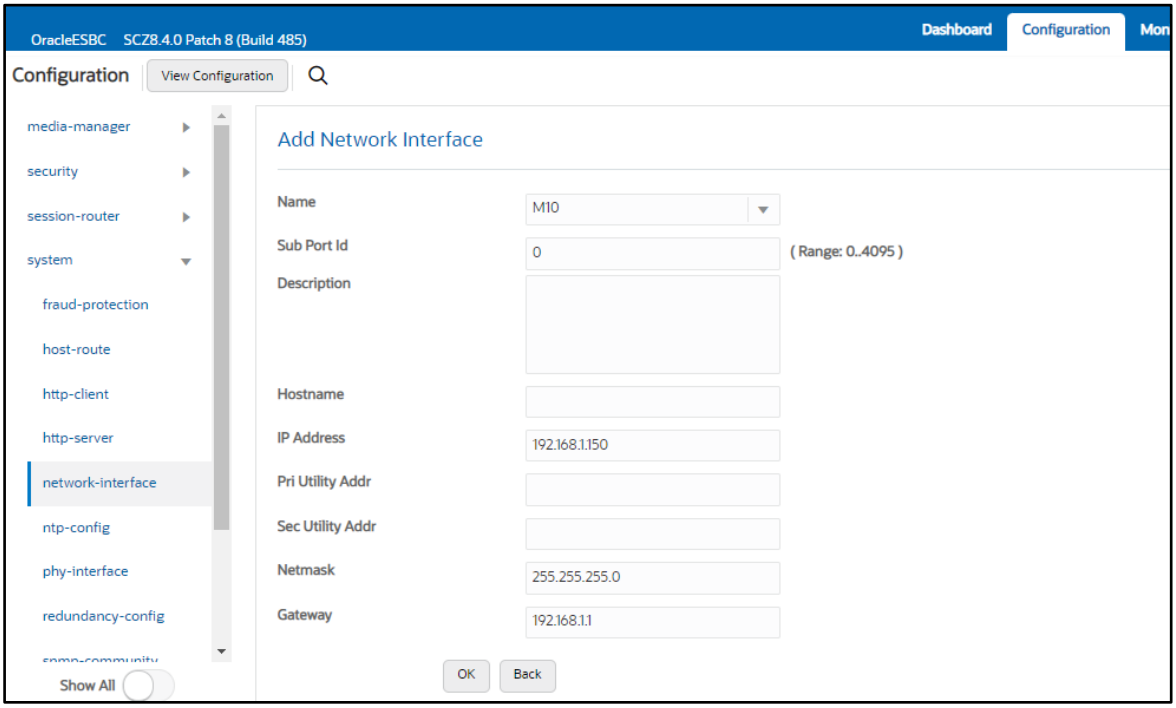
In this Setup, we are using Google Public DNS to resolve the DNS names to IP Addresses.

Parameter Name	Five9	SIPTrunk
Name	M00	M10
Host Name	solutionslab.cgbubedford.com	
IP address	172.16.36.101	192.168.1.150
Netmask	255.255.255.192	255.255.255.0
Gateway	172.16.36.65	192.168.1.1
dns-ip-primary	6.6.6.6	
dns-ip-backup1	6.6.6.4	
Dns-domain	solutionslab.cgbubedford.com	

Configure network interface **M00** as below.



Similarly, configure network interface **M10** as below.

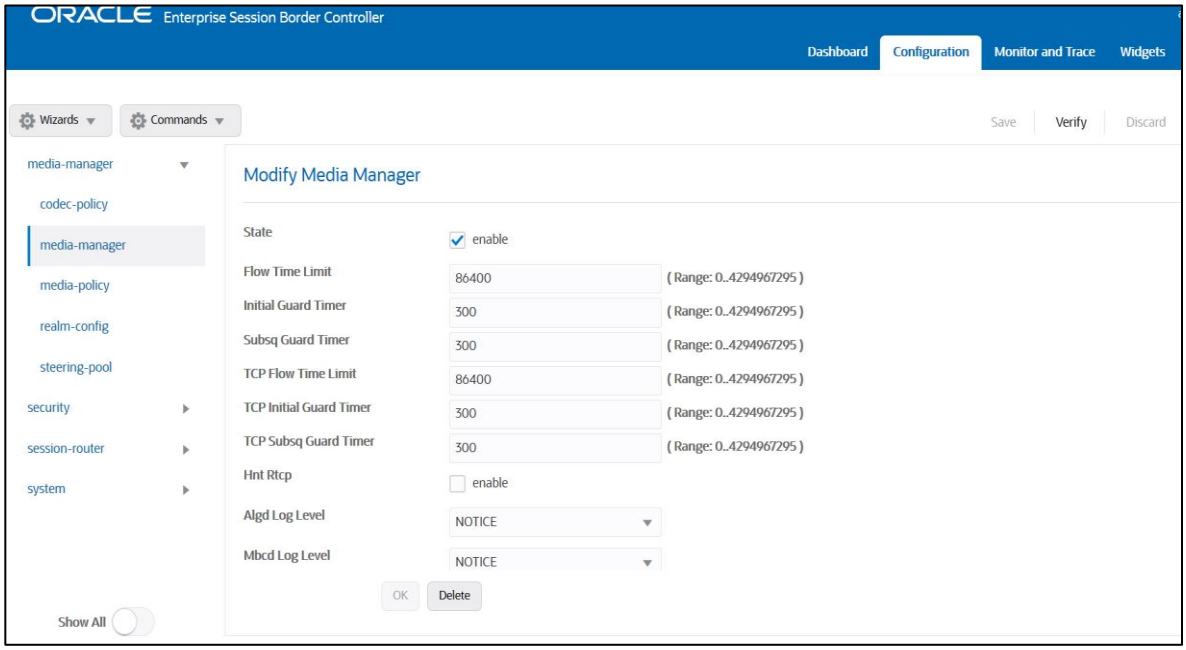


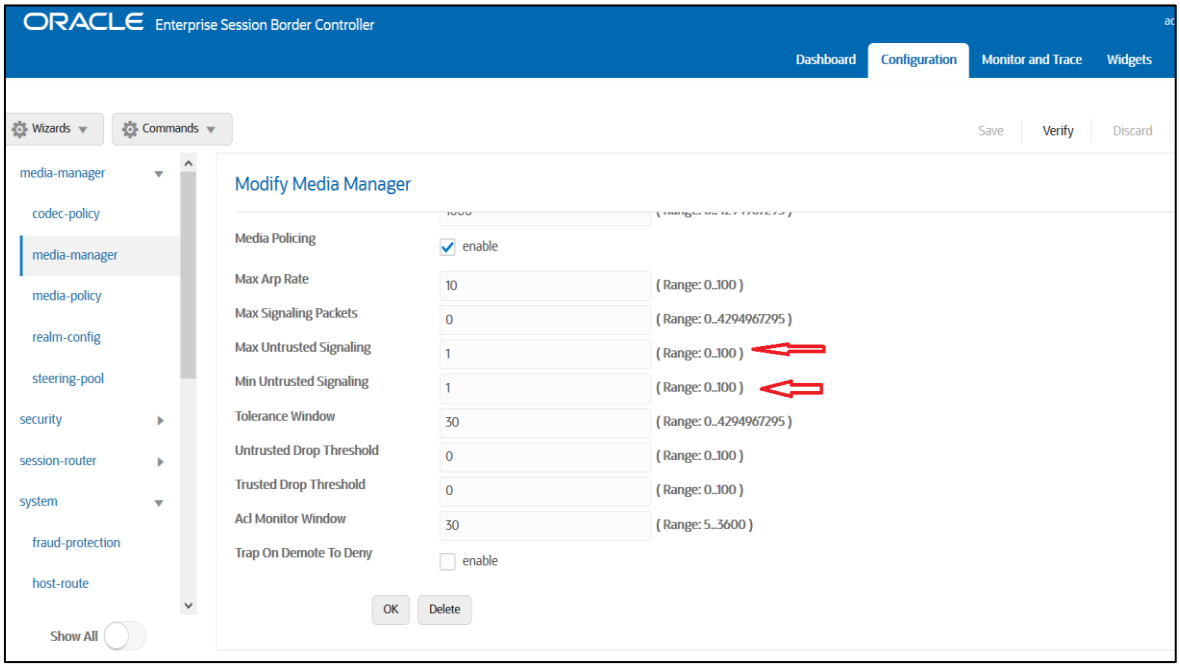
6.6 Enable media manager

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

In addition to the above config, please set the max and min untrusted signaling values to 1.

Navigate to Media->Manager->Media-Manager
ACLI Path: config t->media-manager->media-manager-config



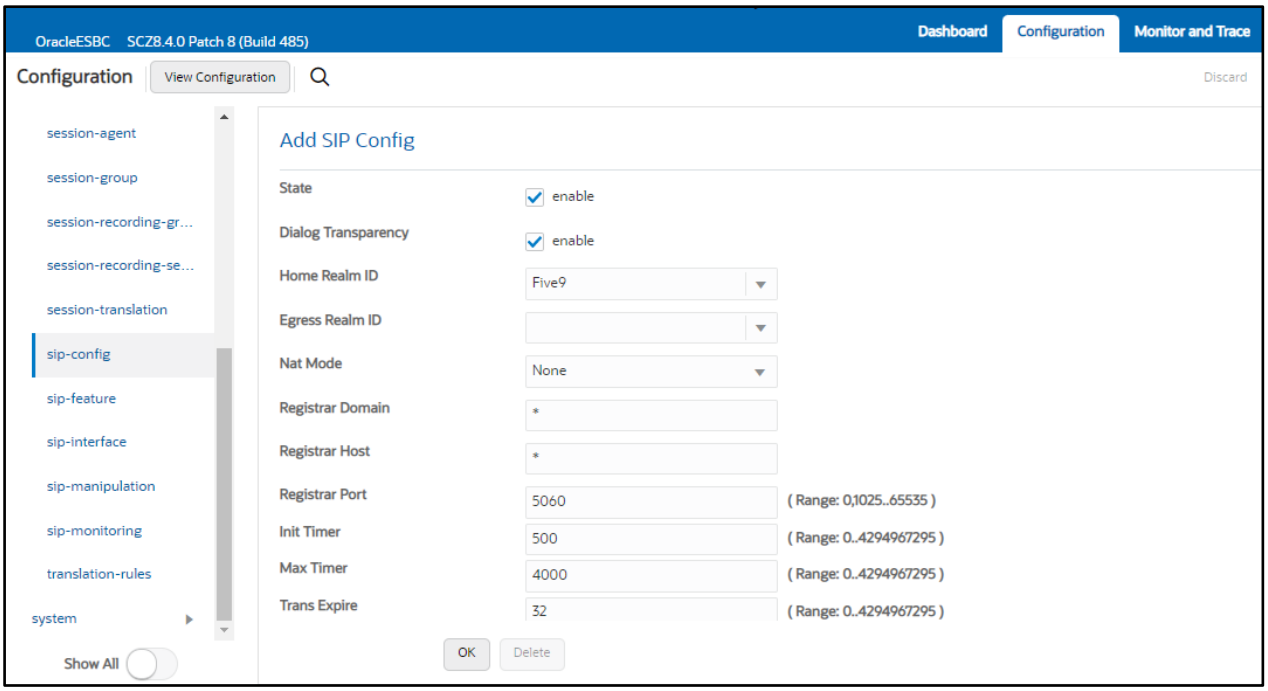


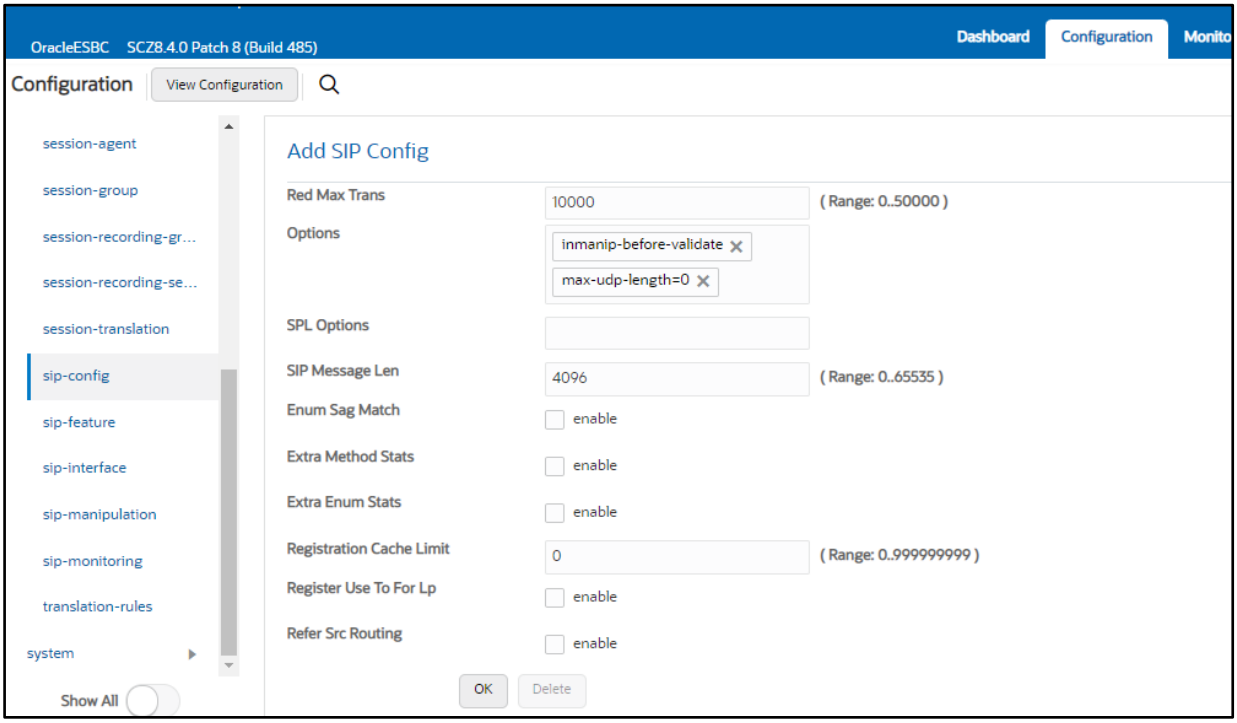
6.7 Enable sip-config

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 and in options, add the below

- inmanip-before-validate
- max-udp-length=0





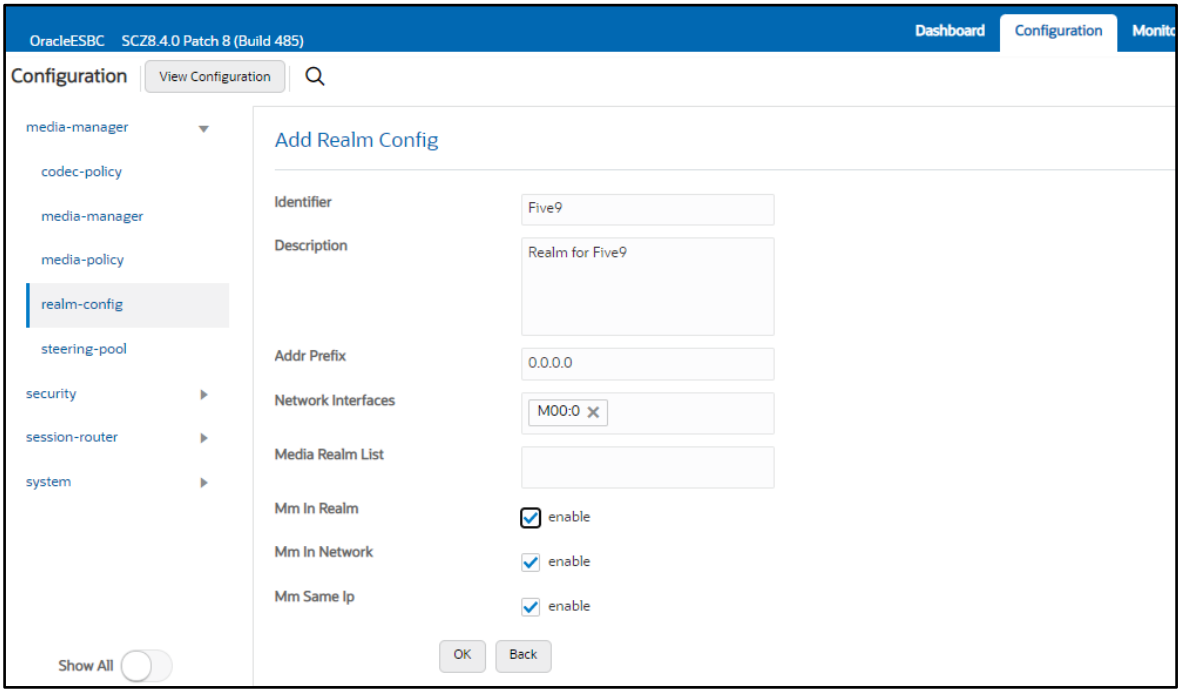
6.8 Configure Realms

Navigate to realm-config under media-manager and configure a realm as shown below.
ACLI Path: config t->media-manger->realm-config

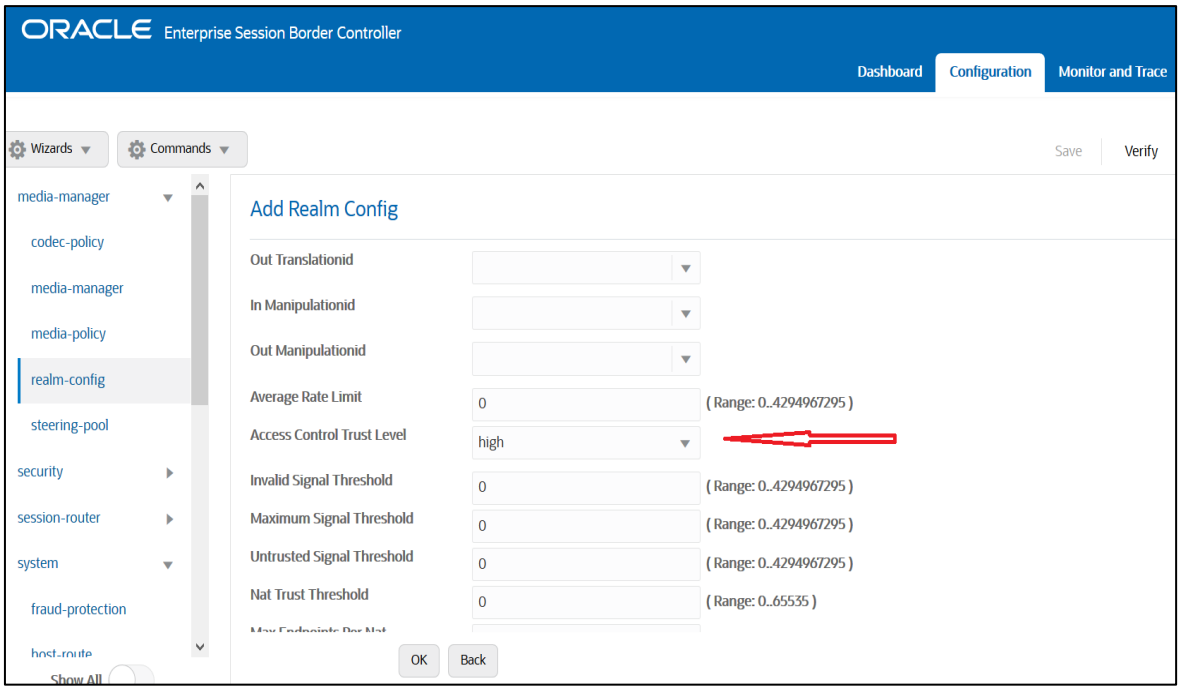
The name of the Realm can be any relevant name according to the user convenience. Use the following table as a configuration example for the two realms used in this configuration:

Config Parameter	Five9 Realm	SIPTrunk Realm
Identifier	Five9	SIPTrunk
Network Interface	M00	M10
Mm in realm	☑	☑
Access Control Trust Level	High	High
Media Sec policy	sdespolicy	RTP

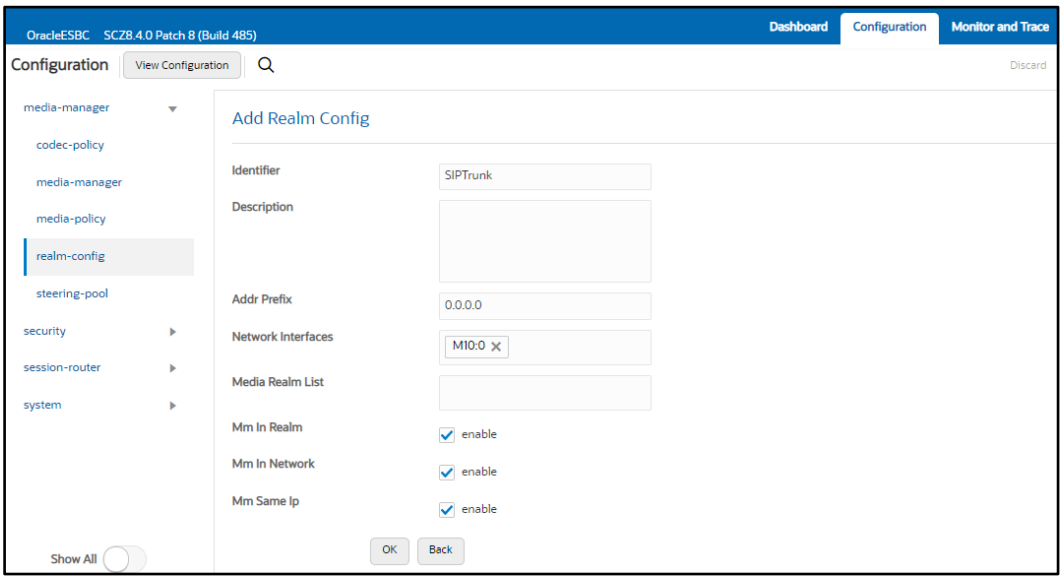
In the below case, Realm name is given as Five9 for Five9 Side. Please set the Access Control Trust Level as high for this realm.

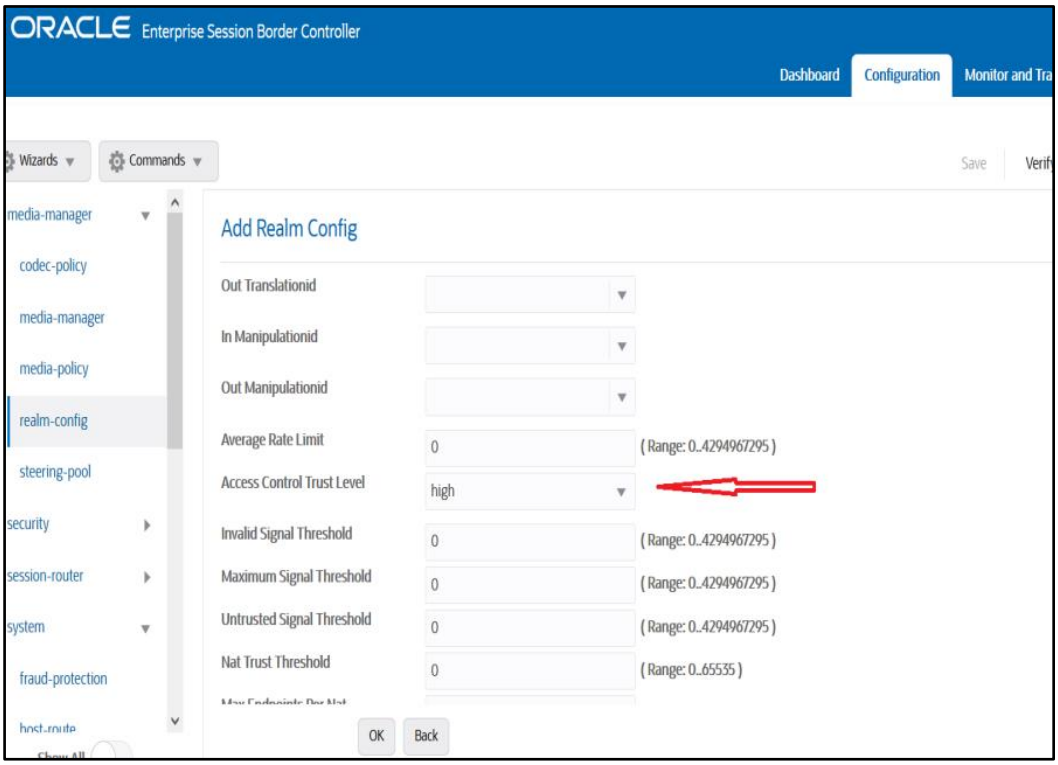

OracleESBC SCZ8.4.0 Patch 8 (Build 485)
Dashboard
Configuration
Configuration
View Configuration
media-manager
codec-policy
media-manager
media-policy
realm-config
steering-pool
security
session-router
system
Show All
Add Realm Config
Identifier
Five9
Description
Realm for Five9
Addr Prefix
0.0.0.0
Network Interfaces
M00:0
Media Realm List
Mm In Realm
enable
Mm In Network
enable
Mm Same Ip
enable
OK
Back


realm-config
steering-pool
security
session-router
system
Media Policy
Media Sec Policy
sdesPolicy
RTCP Mux
enable
Ice Profile
Teams Fqdn
Teams Fqdn In Uri
enable
SDP Inactive Only
enable


ORACLE Enterprise Session Border Controller
Dashboard
Configuration
Monitor and Trace
Wizards
Commands
Save
Verify
media-manager
codec-policy
media-manager
media-policy
realm-config
steering-pool
security
session-router
system
fraud-protection
Show All
Add Realm Config
Out Translationid
In Manipulationid
Out Manipulationid
Average Rate Limit
0
(Range: 0..4294967295)
Access Control Trust Level
high
Invalid Signal Threshold
0
(Range: 0..4294967295)
Maximum Signal Threshold
0
(Range: 0..4294967295)
Untrusted Signal Threshold
0
(Range: 0..4294967295)
Nat Trust Threshold
0
(Range: 0..65535)
OK
Back

Similarly, Realm name is given as SipTrunk for SIP Trunking side. Please set the Access Control Trust Level as high for this realm too.





We have set Access Control Trust Level on the Reams to High as we have static access-control configured and this is a peering environment.

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/8.4.0/security/sbc_scz840_security.pdf

6.9 Configuring a certificate for SBC

This section describes how to configure the SBC for both TLS and SRTP communication with **Five9**.

Five9 supports TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by one of the trusted Certificate Authorities.

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

The process includes the following steps:

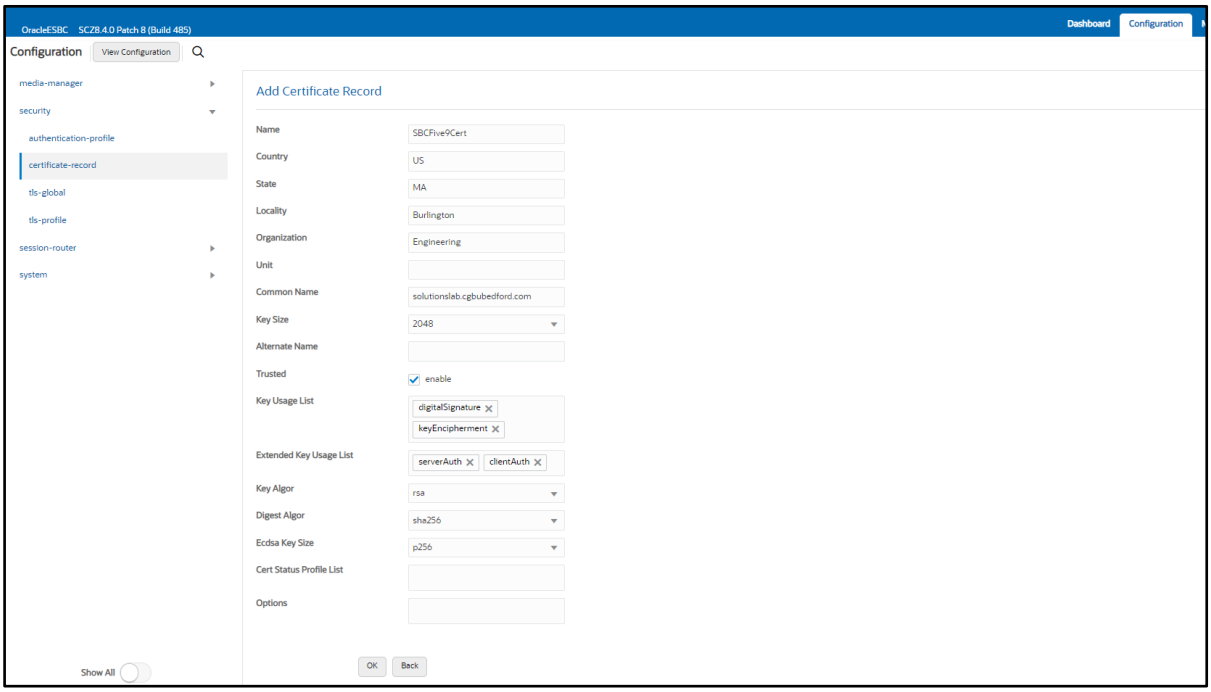
1) Create a certificate-record – "Certificate-record" are configuration elements on Oracle SBC that captures information for a TLS certificate – such as common-name, key-size, key-usage etc.

   - 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. We are creating this certificate for **Five9** Side. Five9 signs the BYOC Cloud endpoints with X.509 certificates issued by DigiCert, a public Certificate Authority.



Follow the same steps and create following intermediate and root certificates.
- DigiCert Root CA: This certificate is always required for Five9.
- DigiCert Intermidiate Cert (this is optional – only required if your server certificate is signed by an intermediate)

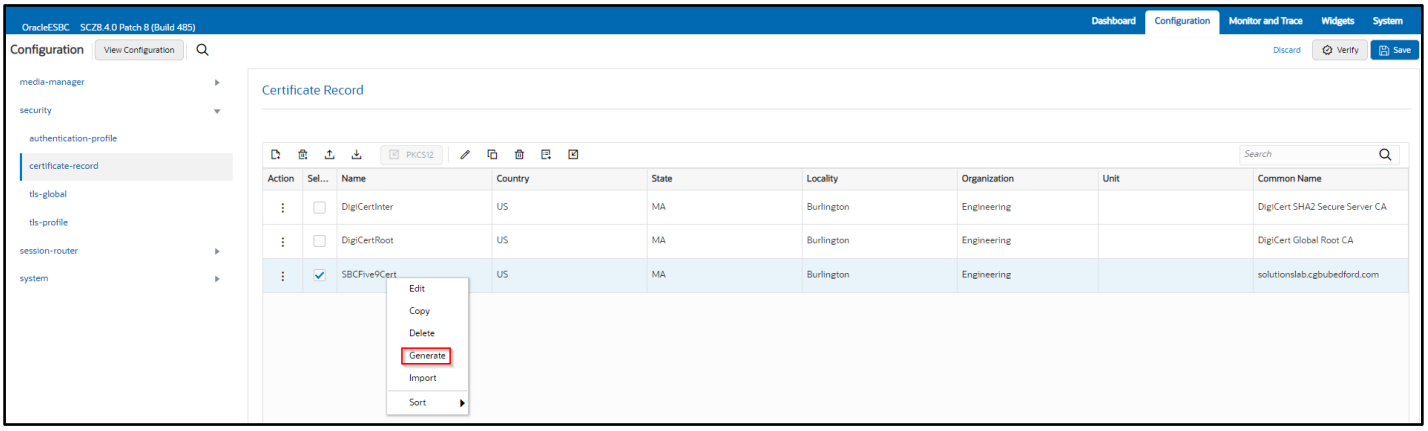
The table below specifies the parameters required for certificate configuration. Modify the configuration according to the certificates in your environment.

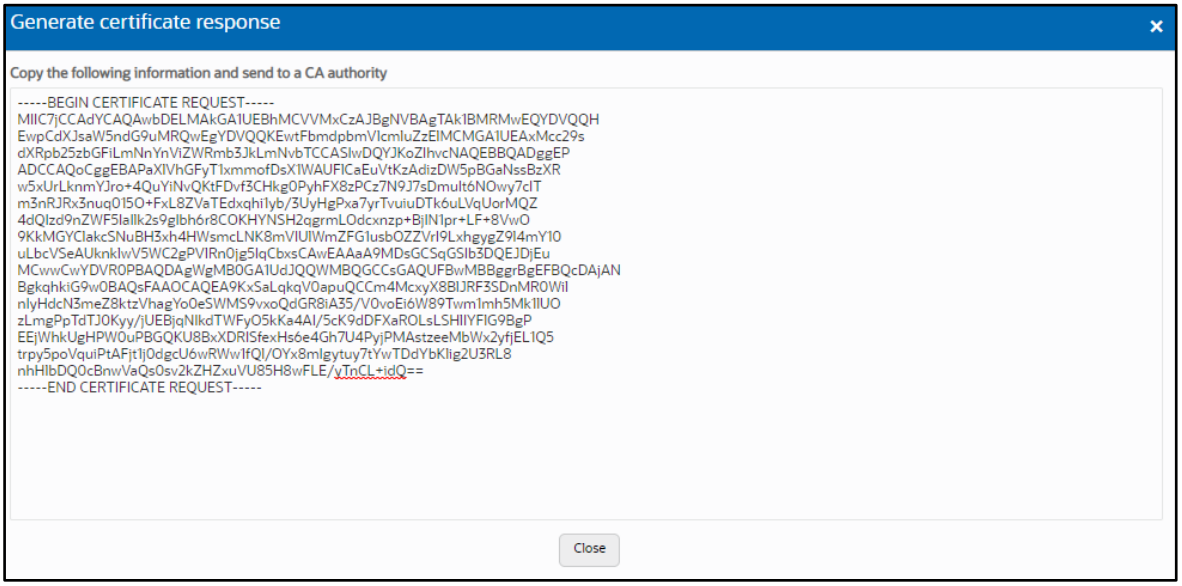
Parameter	DigicertInter	DigiCertRoot
Common-name	DigiCert SHA2 Secure Server CA	DigiCert Global Root CA
Key-size	2048	2048
Key-usage-list	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended-key-usage-list	serverAuth	serverAuth
key-algor	rsa	rsa
digest-algor	sha256	sha256

Step 2 – Generating a certificate signing request

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.
- The Step must be performed for SBCFive9Cert.
- Please copy/paste the text that is printed on the screen as shown below and upload to your CA server for signature.



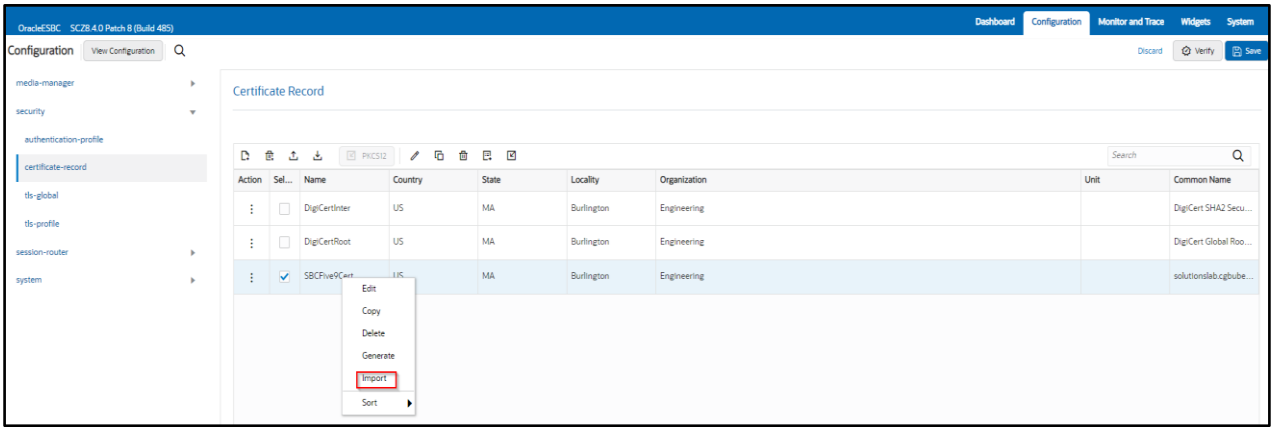


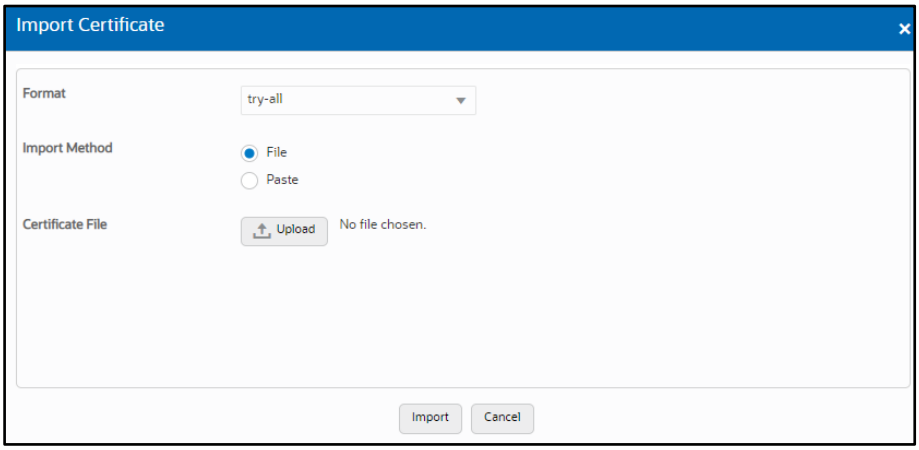
- Also note, at this point, **a save and activate is required** before you can import the certificates to each certificate record created above.

Step 3 – Deploy SBC & root/intermediate 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 the steps for the following certificates:

- DigiCertInter
- DigiCertRoot.

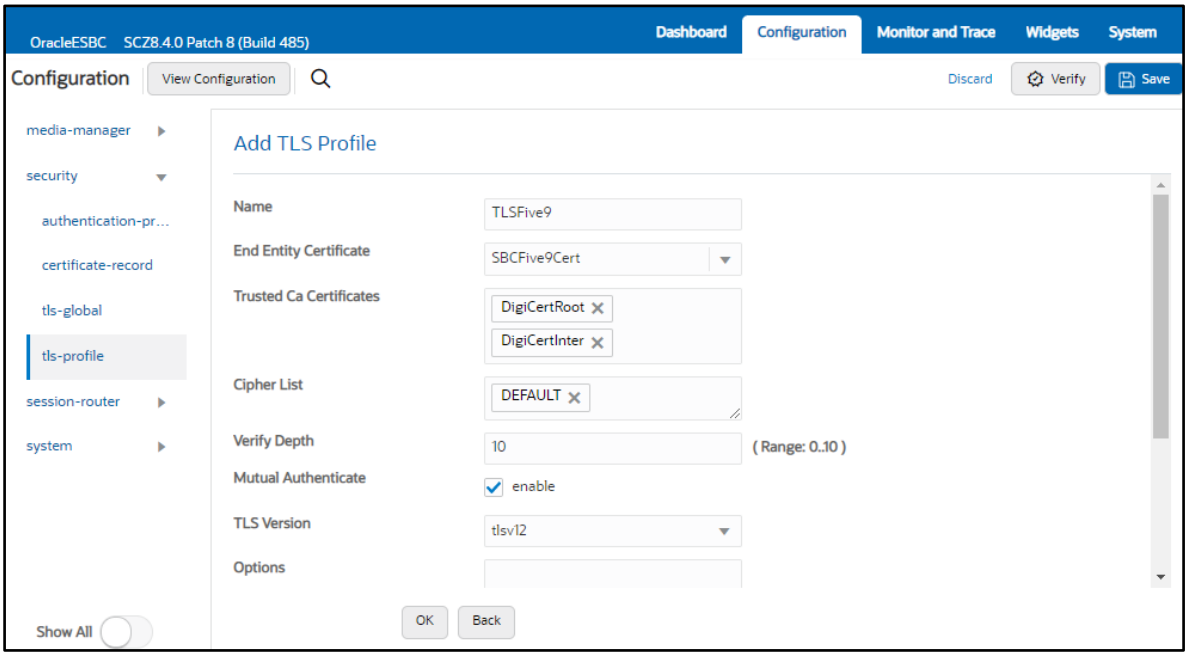
At this stage, all the required certificates have been imported to the SBC for Five9.

6.10 TLS-Profile

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

Go to security-> TLS-profile config element and configure the tls-profile as shown below.
ACLI Path: config t->security->tls-profile

The below is the TLS profile configured for Five9 side.



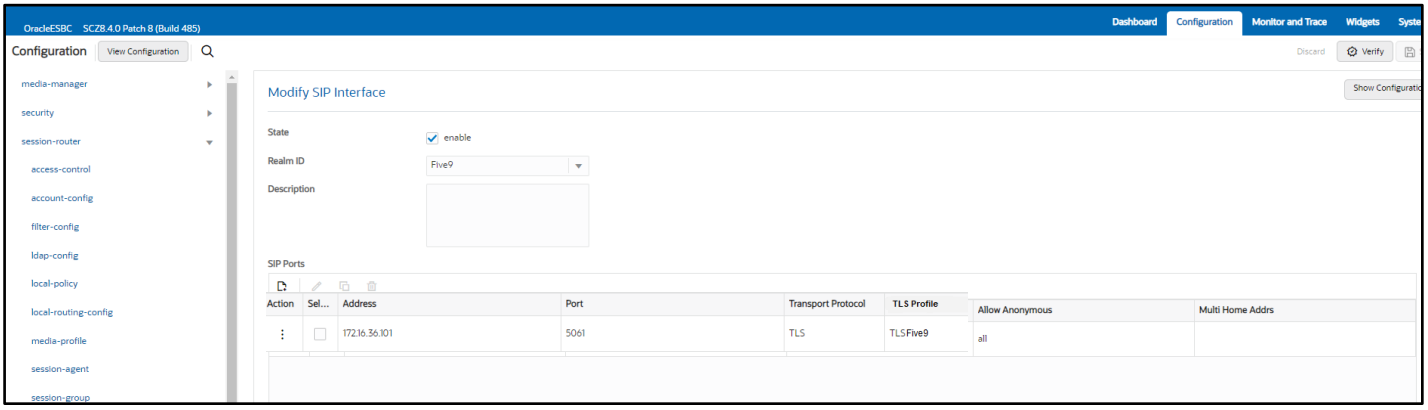
6.11 Configure SIP Interfaces

Navigate to sip-interface under session-router and configure the sip-interface as shown below.
ACLI Path: config t->session-router->sip-interface

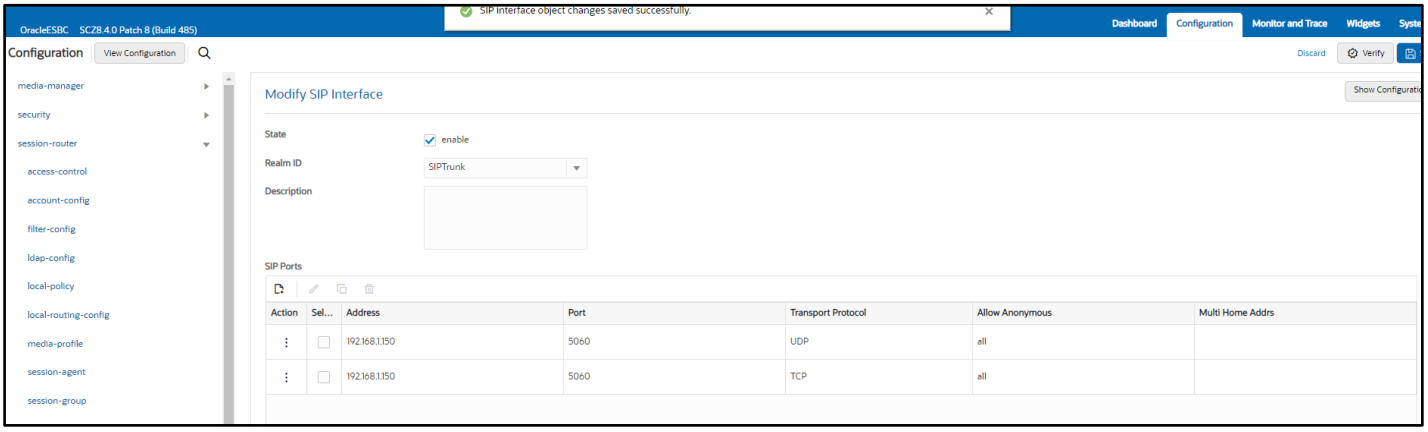
Please configure the below settings under the sip-interface.

- 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.

Below is the sip-interface Configured for Five9 side.



Similarly, Configure sip-interface for the SIPTrunk side as below:



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

6.12 Configure session-agent

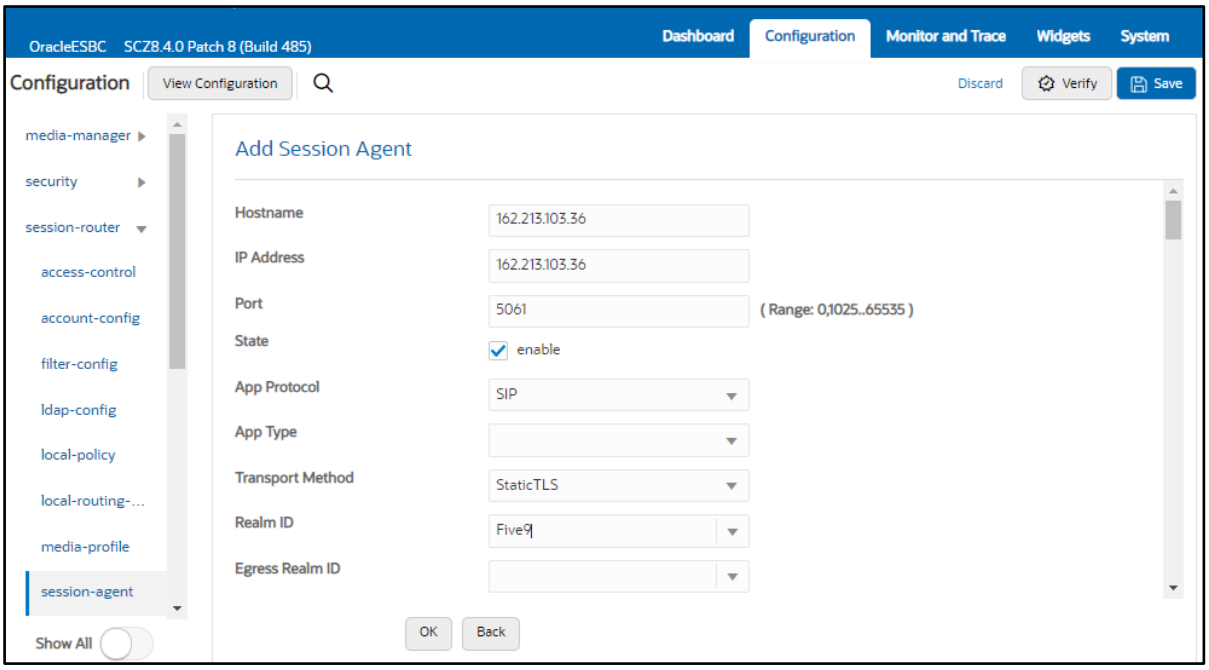
Session-agents are config elements, which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

Navigate to session-router->Session-Agent
ACLI Path: config t->session-router->session-agent

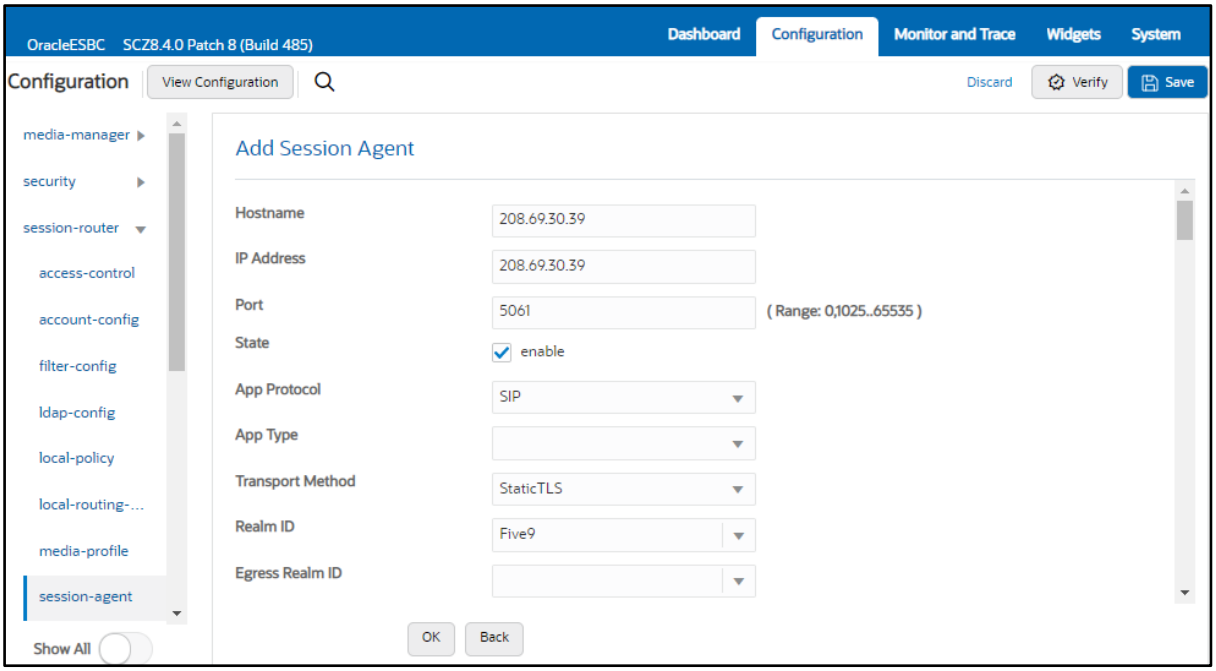
Configure two session-agents for Five9 with following parameters.

- hostname and IP address both same as “162.213.103.36 / 208.69.30.39”
- port to 5061
- realm-id – needs to match the realm created for Five9
- transport set to “staticTLS”
- ping-method – send OPTIONS message to Five9 to check health
- ping-interval to 30 sec

Five9 Session Agent 1

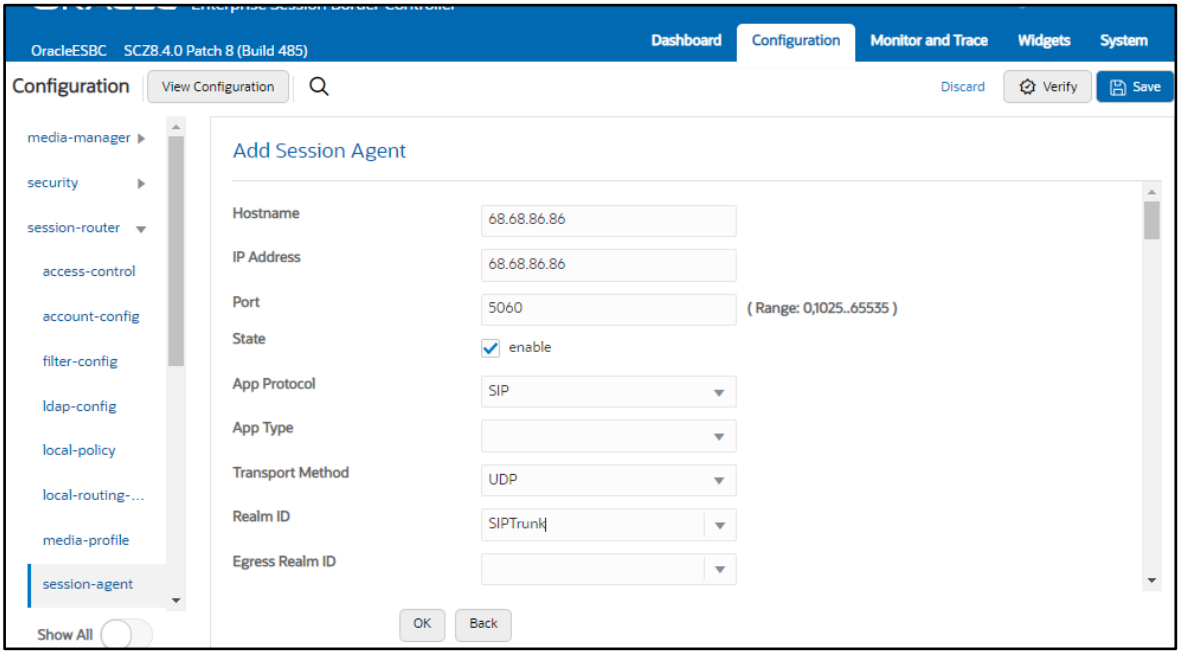


Five9 Session Agent 2



Similarly, Configure the session-agent for SIPTRUNK. Go to session-router->Session-Agent.

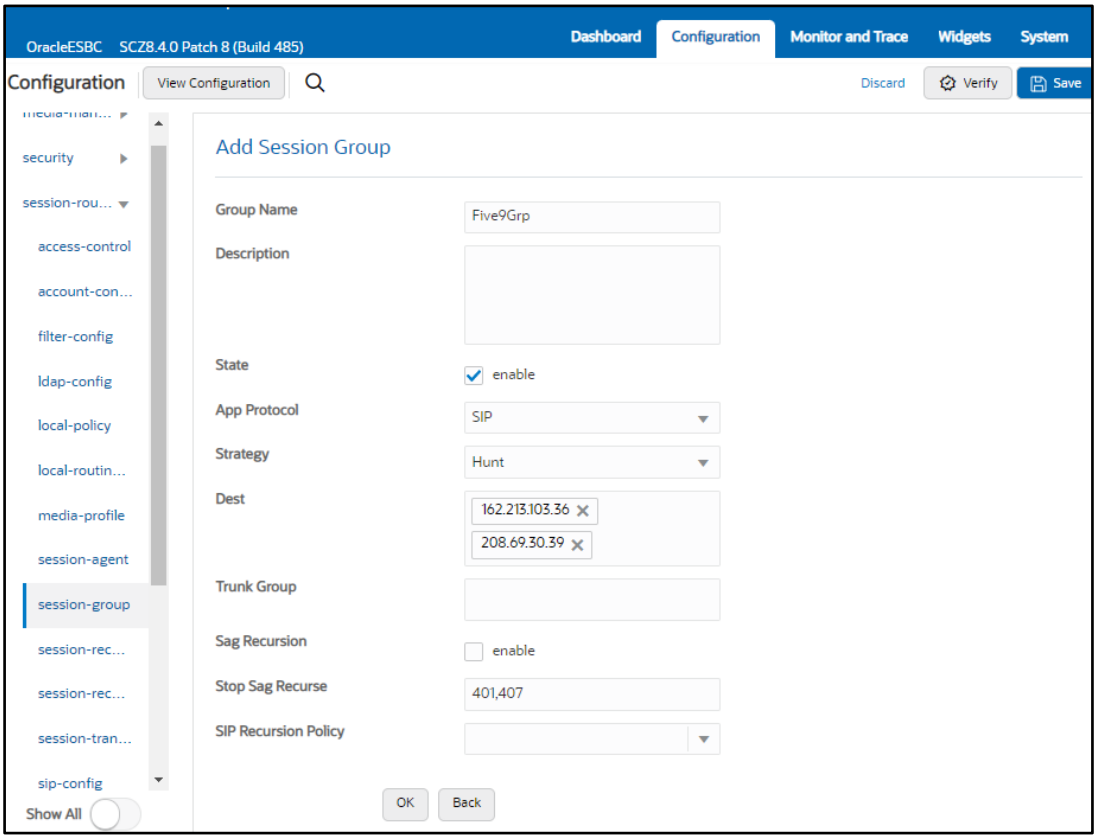
- Host name and IP address of SIP Trunk.
- port 5060
- realm-id – needs to match the realm created for SIPTRUNK.
- transport set to “UDP”



6.13 Configure session-agent group

A session agent group allows the SBC to create a load-balancing model.
Navigate to Session-Router->Session-Group.
ACLI Path: config t->session-router->session-group

Please configure the following group for Five9 Session Agents.

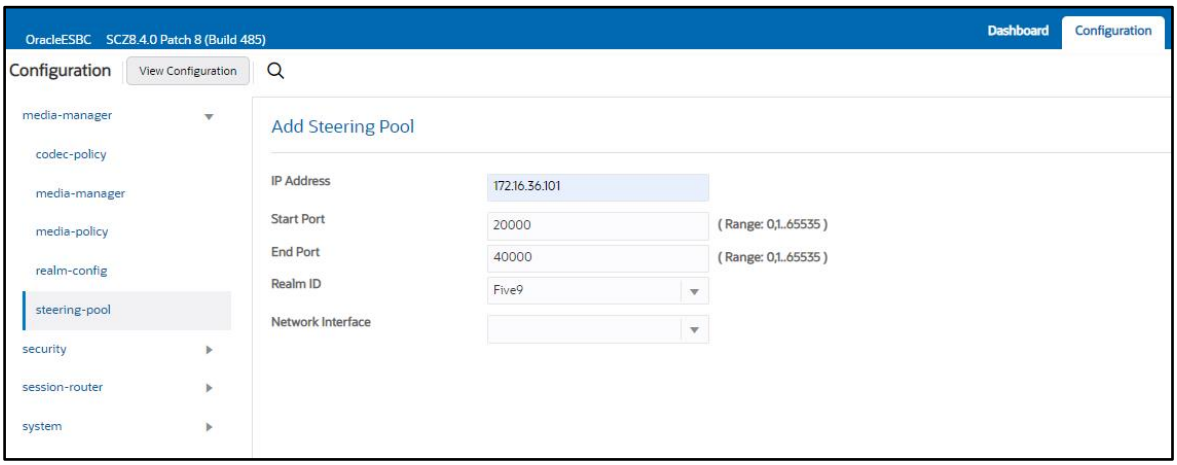


6.14 Configure steering-pool

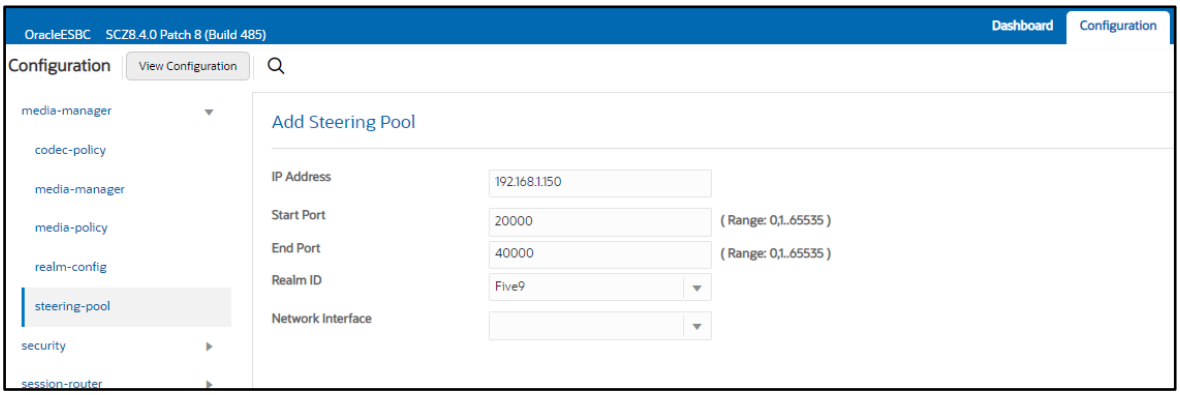
Steering-pool config allows configuration to assign IP address(s), ports & a realm. They define sets of ports that are used for steering media flows through the OCSBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

Navigate to GUI Path: media-manger->steering-pool
ACLI Path: config t->media-manger->steering-pool

Five9 side Steering pool.



SIPTrunk side Steering pool.

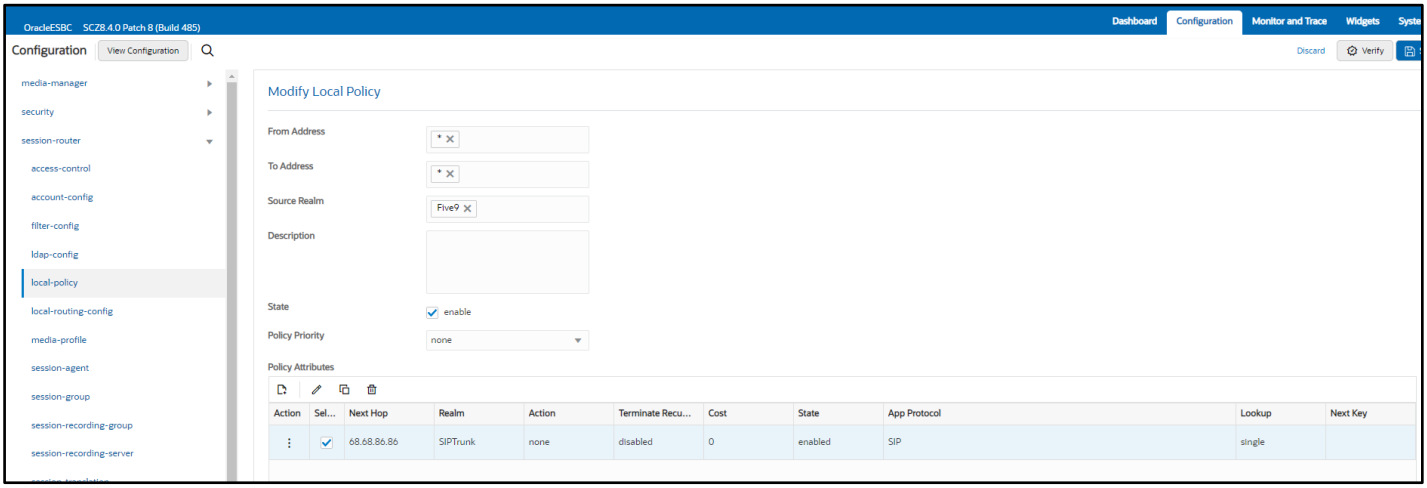


6.15 Configure local-policy

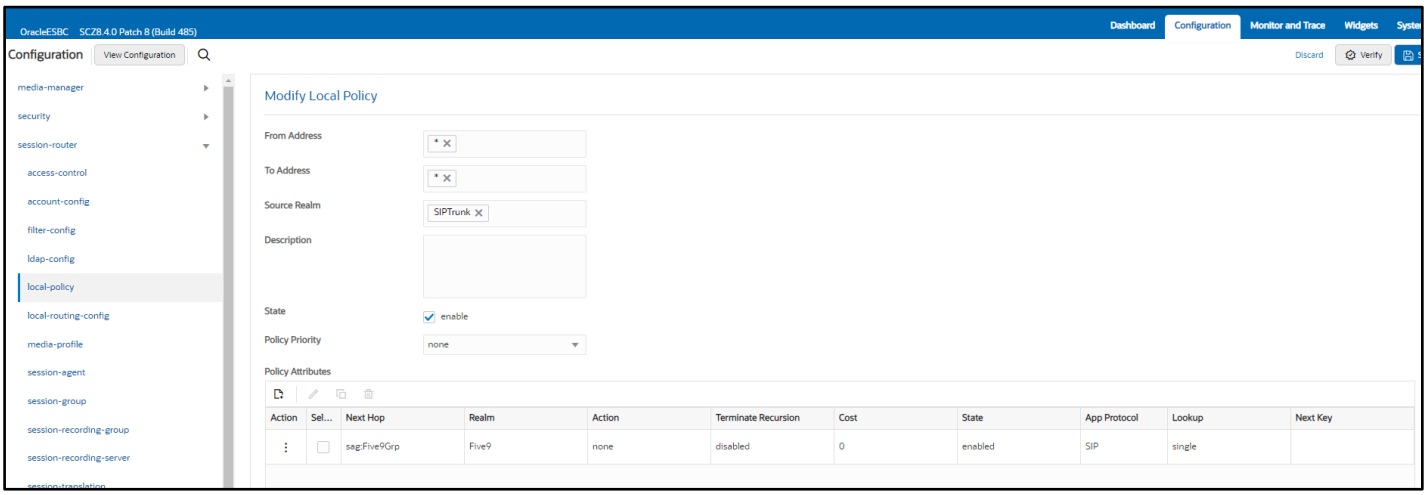
Local policy config allows the SBC to route calls from one end of the network to the other based on routing criteria.

To configure local-policy, Navigate to Session-Router->local-policy
ACLI Path: config t->session-router->local-policy

To route the calls from Five9 side to SIPTrunk side, Use the below local–policy.



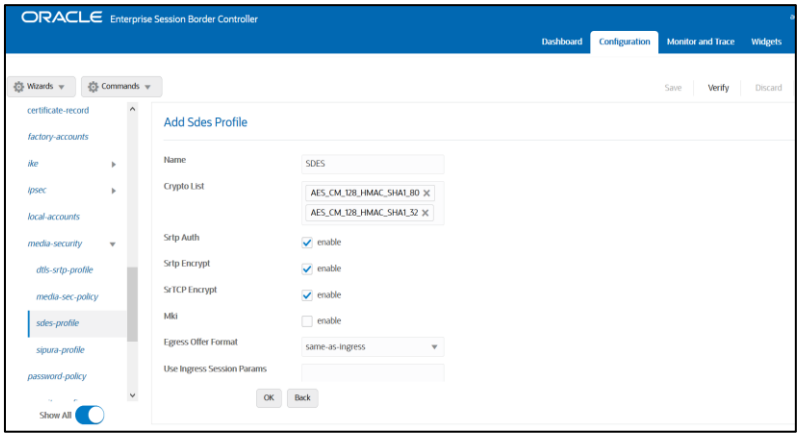
To route the calls from the SIPTrunk side to Five9 side, Use the below local–policy.



6.16 Configure 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.

Navigate to config t ->Security -> Media Security ->sdes profile and create the policy as below.
ACLI Path: config t->security->media-security->sdes-profile



6.17 Configure Media Security Profile

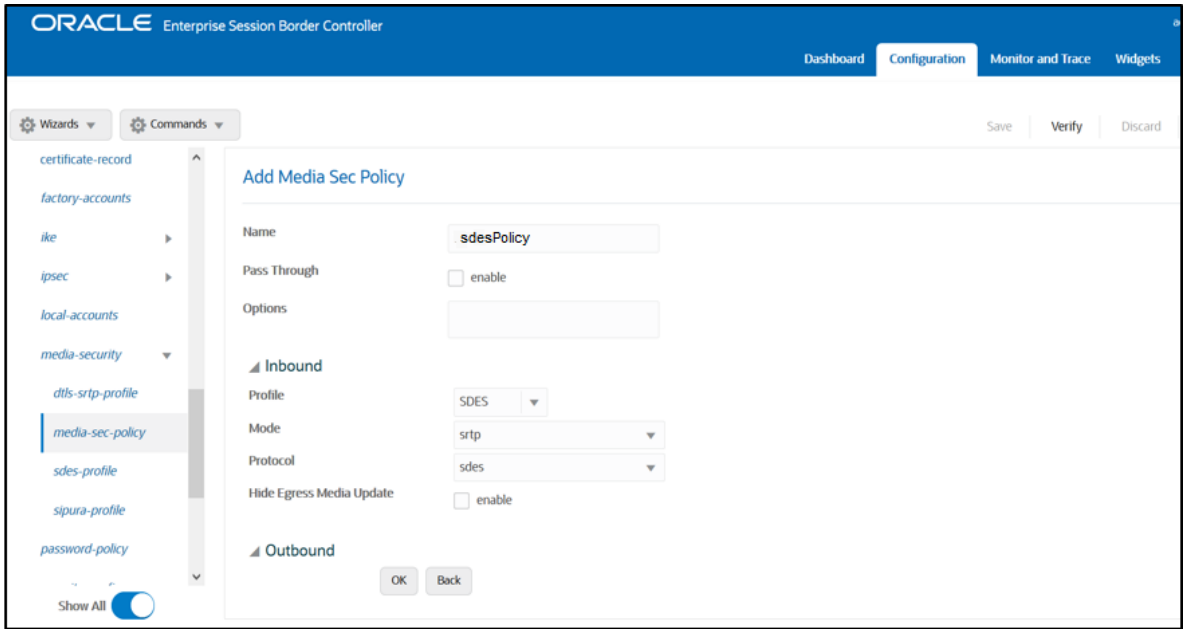
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them).

In this example, we are configuring two media security policies. One to secure and decrypt media toward Five9, the other for non-secure media facing SIPTrunk.

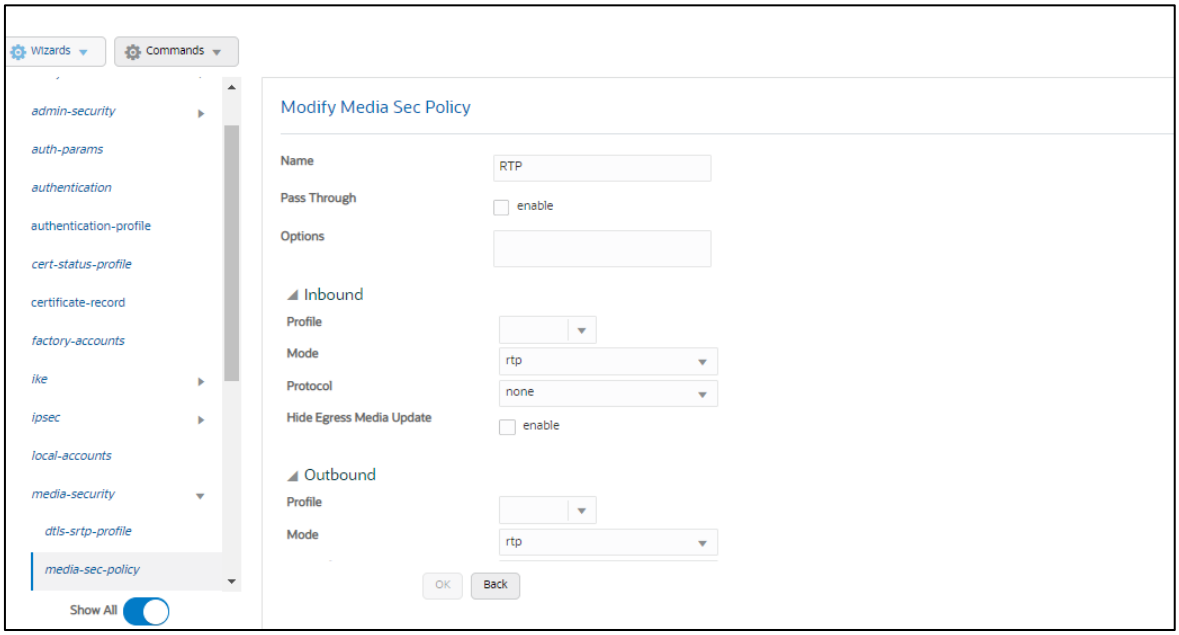
Navigate to config t->Security -> Media Security ->media Sec policy and create the policy as below:
ACLI Path: config t->security->media-security->media-sec-policy

Create Media Sec policy with name sdesPolicy, which will have the sdes profile, created above.

Assign this media policy to Five9 Realm.



Similarly, Create Media Sec policy with name RTP to convert srtp to rtp for the SIPTRUNK (if the call is encrypted from Five9) which will use only TCP/UDP as transport protocol. Assign this media policy to the SIPTrunk Realm.

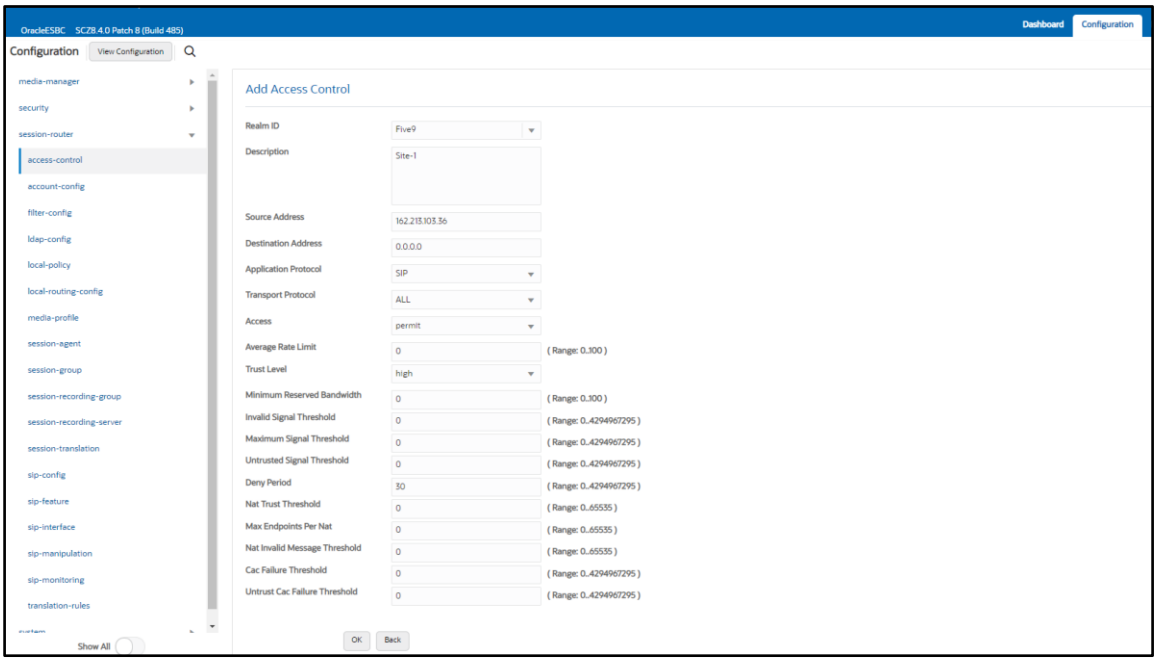


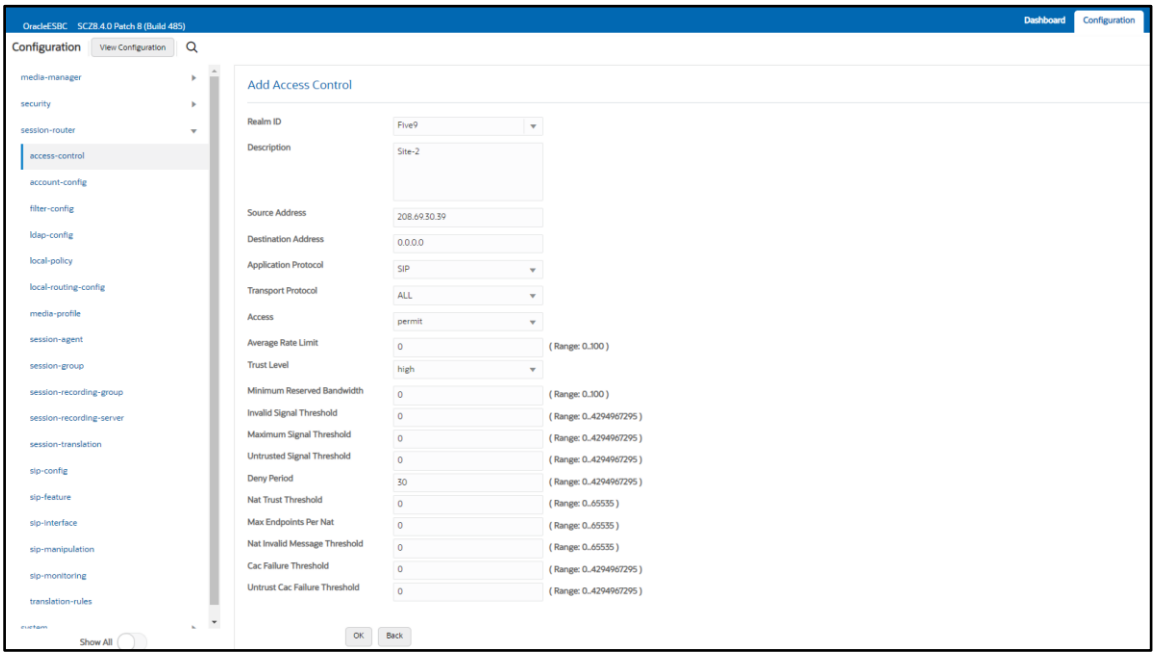
6.18 Access Control

To enhance the security of your Oracle Session Border Controller, we recommend configuration access controls to limit traffic to only trusted IP addresses on all public facing interfaces

GUI Path: session-router/access-control

Please use the example below to configure access controls in your environment for both Five9 IP's, as well as SIP Trunk IP's (if applicable).





Notice the trust level on this ACL is set to high. When the trust level on an ACL is set to the same value of as the access control trust level of its associated realm, this creates an implicit deny, so only traffic from IP addresses configured as ACL's with the same trust level will be allowed to send traffic to the SBC. For more information about trust level on ACL's and Realms, please see the SBC Security Guide, Page 3-10

7. 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 session-group
- New steering-pools
- New local-policy
- SDES Profile
- Media-Sec-Policy
- Access Control

Please follow the steps mentioned in the above chapters to configure these elements.

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services