Oracle Session Border Controller (SBC) integration with Pexip 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	Oracle SBC and Pexip Server BYOC Config	11-8-2021

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 (SBC) CB). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform along with Pexip BYOC.

2. Document Overview

This Oracle technical application note outlines the configuration needed to set up the interworking between Oracle SBC and Pexip BYOC PSTN Calling. The solution contained within this document has been tested using Oracle Communication 840p5A. Our scope of this document is only limited to testing Oracle SBC with Pexip BYOC PSTN Calling.

It should be noted that while this application note focuses on the optimal configurations for the Oracle SBC in a Pexip BYOC Calling Environment (Using Cisco DX70 and Polycom RealPresence Desktop Phone) 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.

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 Pexip BYOC PSTN Calling using Oracle Enterprise SBC.There will be steps that require navigating the Pexip Server 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.

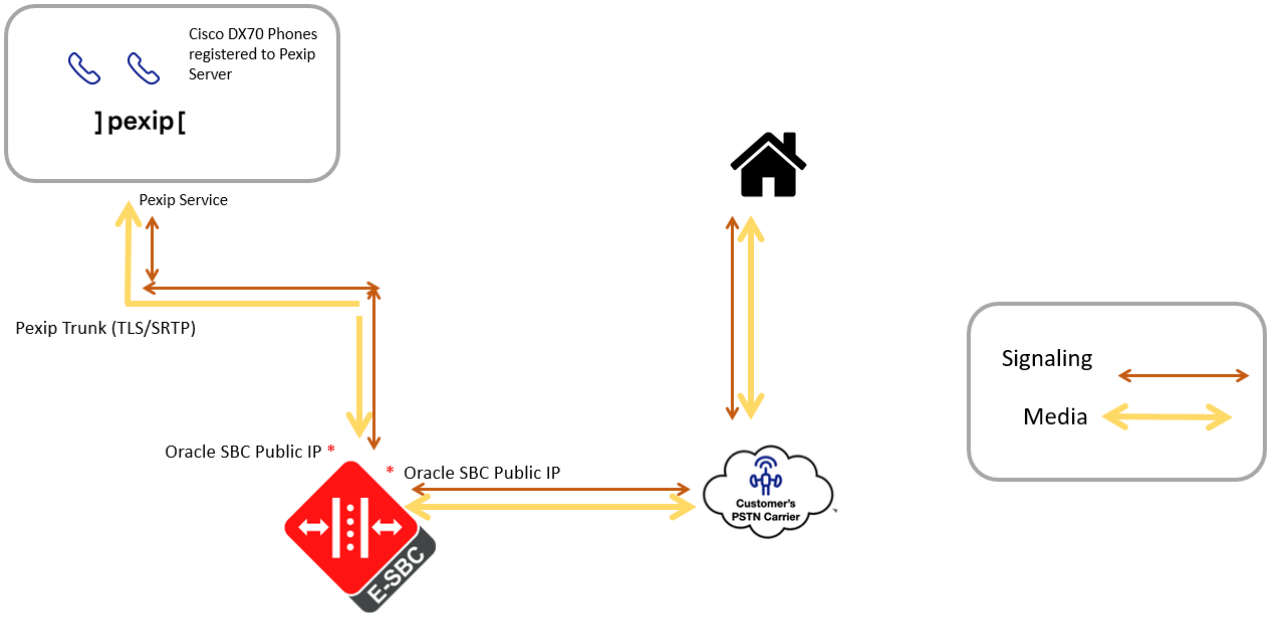
3.2. Requirements

- Pexip Service Platform
- Cisco DX70 and Polycom Phones connected to the Pexip Server
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 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	Pexip Version	SBC Version	Cisco DX70	Polycom Realpresence Desktop
Revision 1	Pexip service platform as at July 2021	8.4.0	ce 9.15.3.17 5cbbf23b617 2021-04-21	Polycom RealPresence Desktop v3.10.0.71107

3.3. Architecture



Note: Only dial out from the Pexip service is supported here.

The configuration, validation and troubleshooting is the focus of this document and will be described in two phases:

- Phase 1 – Configuring the Pexip Server for Oracle SBC
- Phase 2 – Configuring the Oracle SBC

4. Configuring the Pexip Server for Oracle SBC

Pexip's "Bring your own carrier" (BYOC) enables users to dial out from a Pexip-registered video endpoint 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 Pexip Service routes it out to the chosen carrier who then handles the call the rest of the way.
BYOC currently supports calling from video endpoints registered to the Pexip Service only (it does not currently support calling from Trusted devices or the Pexip apps.)

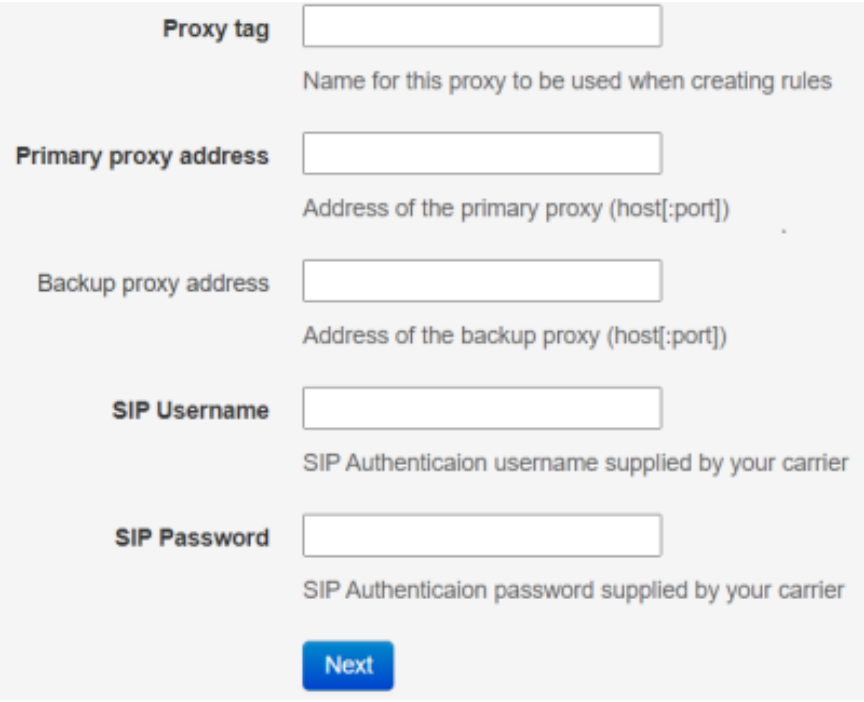
4.1.Steps to configure BYOC from Pexip Portal

Here are the steps required to configure BYOC in the Partner Portal.

Order a BYOC license. For help ordering licenses see Ordering a new license plan.
Complete BYOC configuration in the Partner Portal:
Configure a proxy for each carrier the customer wants to use.
Configure rules for different types of calls.

4.1.1. Configuring a proxy

To find the BYOC configuration screen, go to the company you want to configure and select the Interop tab.



First, you need to configure a separate proxy for each carrier to be used by the customer, they can have one or more carriers for BYOC. The proxy holds the information that the Pexip

Service needs to route the call to the SBC and authenticate with the carrier. The customer provides you with this information as they work with their chosen carrier directly.

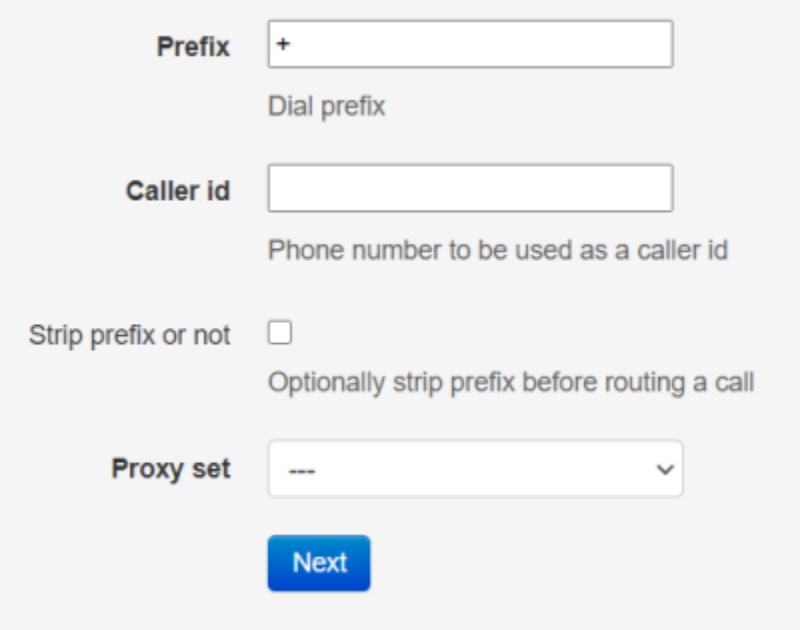
- Proxy tag is a name used to identify a carrier. When creating a rule, you select the proxy it belongs to.
- Primary and Backup proxy addresses are the carrier SIP addresses where Pexip sends the calls.
- SIP Username and Password: SIP authentication is optional, but strongly recommended.

4.2.Configuring a rule

Rules enable the Pexip Service to route calls to the correct SBC. Rules also determine the prefix that the end user enters on their video endpoint as the dial string.

The number of rules needed depends on how the customer and the SBC want to organize things. If the customer engages one SBC to deliver all the calls they want to make, then only one rule is needed, however, the customer could have more than one rule.

For example, a customer can have a rule for each destination country where calls are made to, or a rule per caller-id. Having one rule per country means they can set the prefix to the International Direct Dial and Country Code so that the end user doesn't have to enter those details in addition to the prefix when placing a call.



The Prefix is a customer-defined value that is entered by the end user as part of the dial string when they place a call from a video endpoint. It allows the Pexip Service to use the correct rule,

and hence the proxy, to route the call. Different carriers(through the SBC) have different requirements when it comes to the dial string they receive, so the carrier's requirements must be considered when deciding how to set the Prefix and Strip prefix or not fields.

- A prefix must be unique within a company. It can be between one and 15 characters long, and can contain alphanumeric and special characters, such as +.
- When Strip prefix or not is unchecked, the prefix value entered by the user becomes part of the dial string sent to the SBC.
- When Strip prefix or not is checked, the Pexip Service removes the prefix before sending the rest of the dial string .
- Caller id is sent to the SBC in the 'From' header field and is shown as the incoming caller id number on the receiving phone. In most cases, here you enter the phone number purchased from the carrier using E.164 format. If you're unsure, the carrier can confirm. Note that the same ID is used for all calls from all endpoints using the same rule.
- Proxy set is where you select the proxy/carrier to which this rule belongs.

Examples of different configurations and the resultant dial strings

Here are some examples showing different configurations of Prefix and Strip prefix or not, and consequently what the user must enter to place a call, and what the carrier receives. Note that all dial strings end with @example.com (where @example.com represents the fqdn configured on the SBC) to make a valid SIP address.

Prefix value	Strip prefix or not	Dial string entered by the user	Carrier receives
+44	No	+4412345678@example.com	+4412345678@example.com
+	No	+4412345678@example.com	+4412345678@example.com
*	Yes	*07911123456@example.com	07911123456@example.com

5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for interworking with Pexip BYOC Platform

5.1. Validated Oracle SBC version

Oracle conducted tests with 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 6350
- AP 6300
- VME

6. New SBC configuration

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

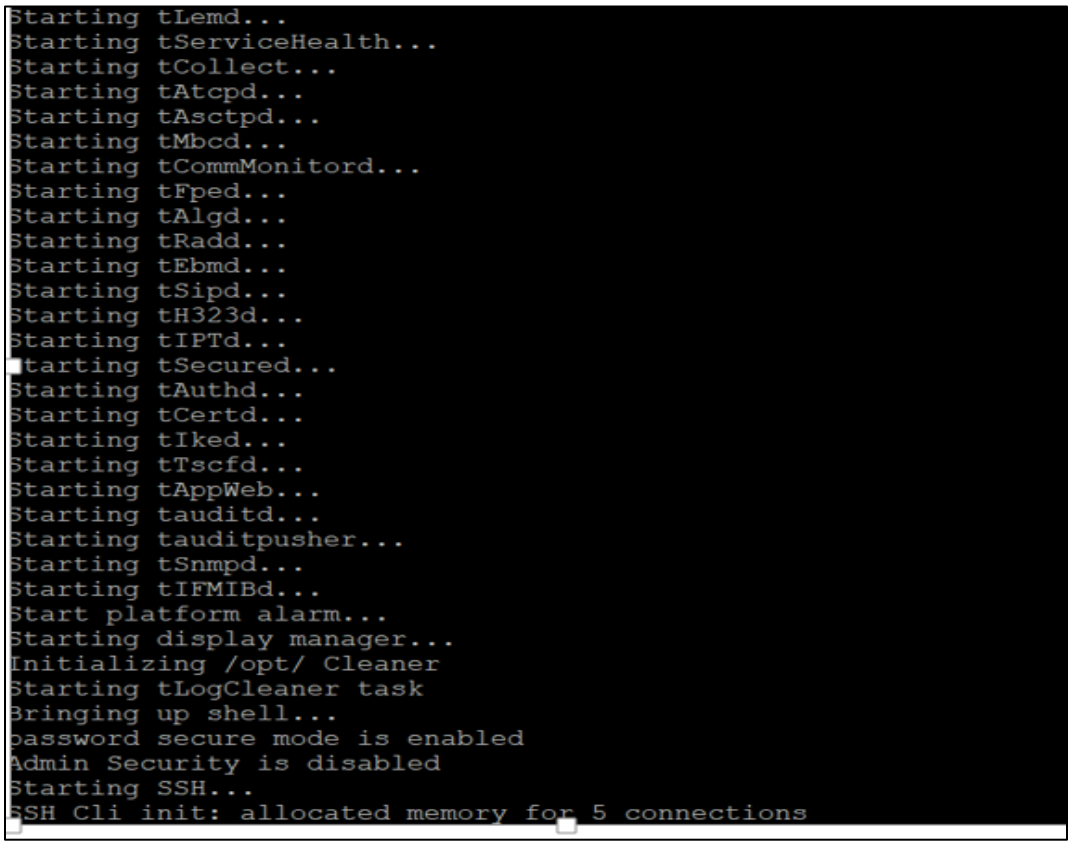
6.1.Establishing a serial connection to the SBC

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.

Note: This doesn't apply to VME and cloud deployments.

Start the terminal emulation application using the following settings:

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

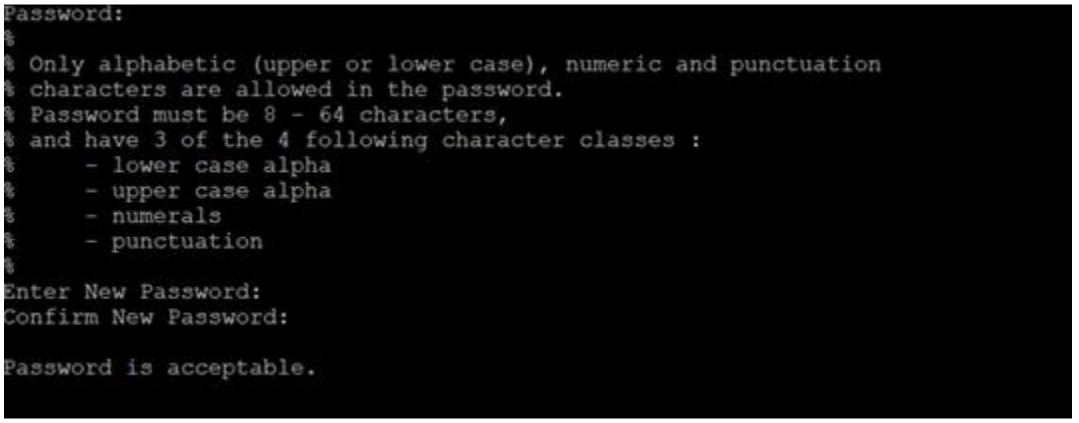


Power on the SBC and confirm that you see the following output from the boot-up sequence

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”.

Note: The password is different for cloud and VME deployments. Please check therequired documentation

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.

Note: There is no management IP configured by default.

```
NN4600-100# conf t
NN4600-100(configure)# bootparam

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

Boot File               : /boot/nnSCZ830m1p7.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            : vxftp
Flags                   :
Target Name             : NN4600-100
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.



NN4600-100(configure)#
NN4600-100(configure)#
NN4600-100(configure)#
```

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

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

```
NN4600-100# setup product

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

Last Modified 2019-06-28 14:05:33
------------------------------------------------------------
 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->web-server-config.

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

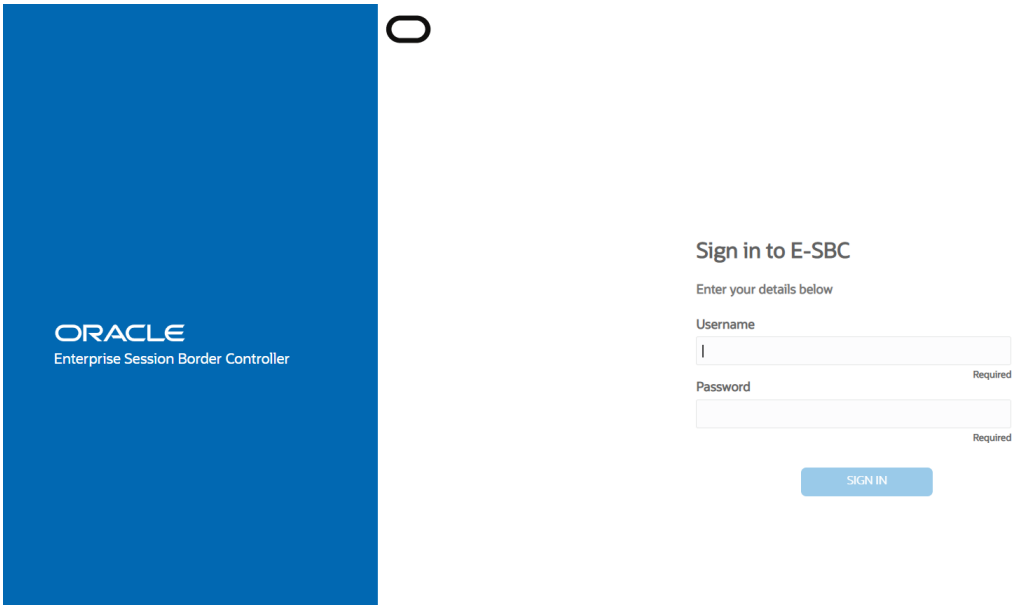
```
NN4600-100(web-server-config)# show
web-server-config
        state                                   enabled
        inactivity-timeout                      5
        http-state                              enabled
        http-port                               80
        https-state                             disabled
        https-port                              443
        http-interface-list                     REST,GUI
        tls-profile
        last-modified-by                        admin@console
        last-modified-date                      2020-04-03 00:21:22

NN4600-100(web-server-config)#
```

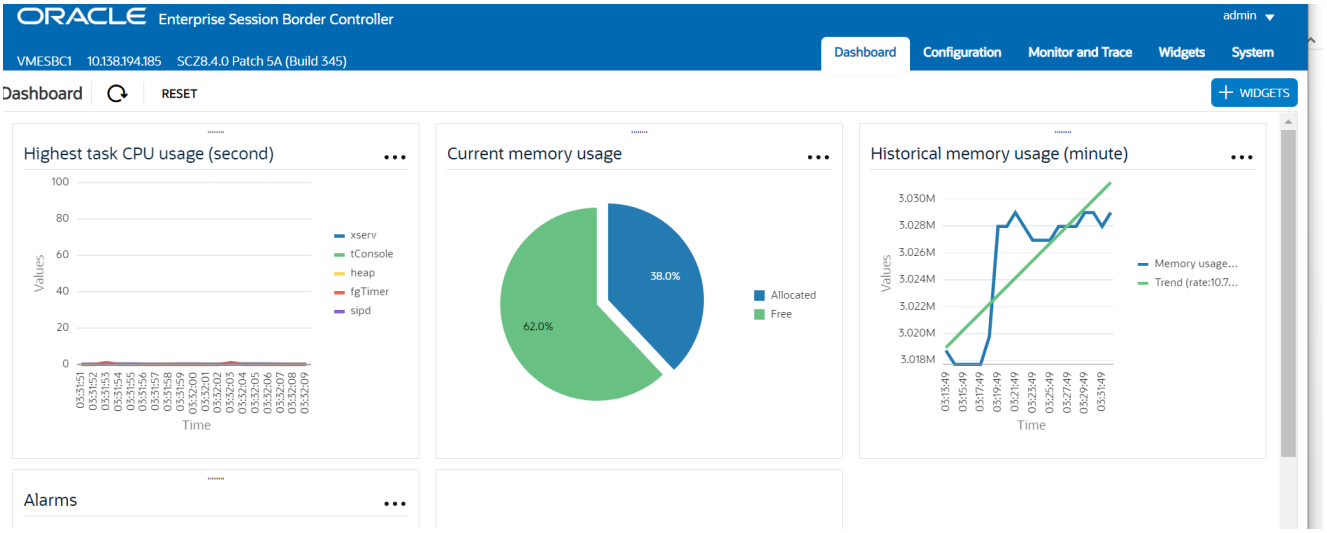
6.2.Configure SBC using Web GUI

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

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

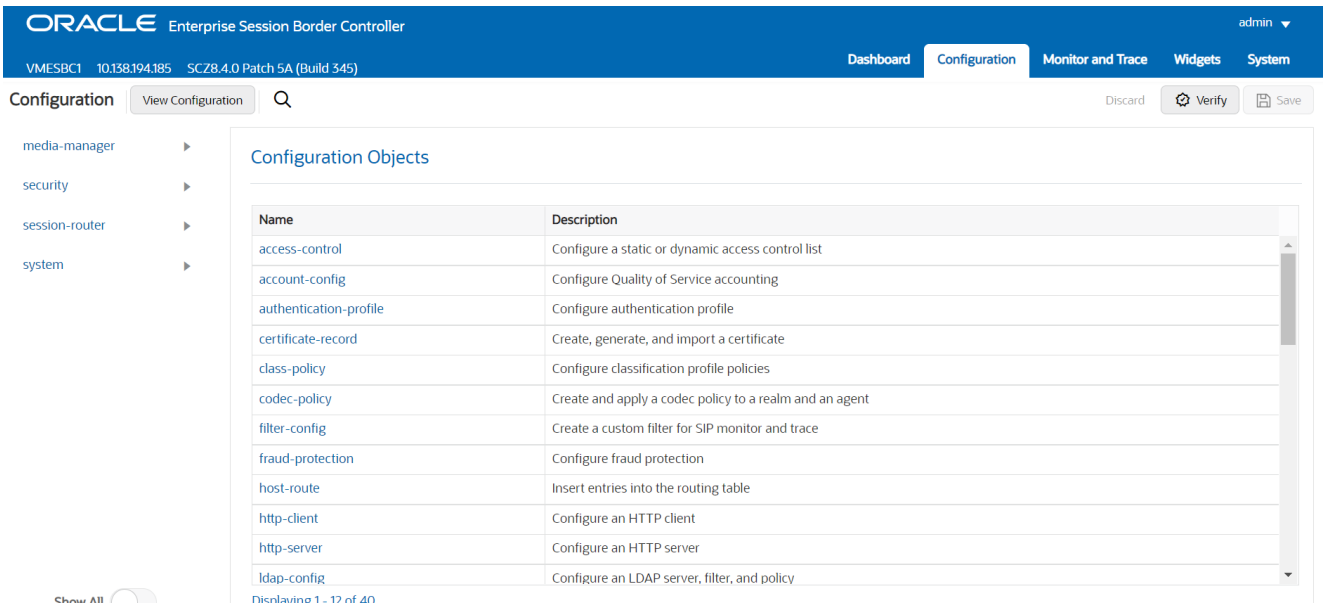


The username and password is the same as that of CLI.



Go to

Configuration as shown below, to configure the SBC



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

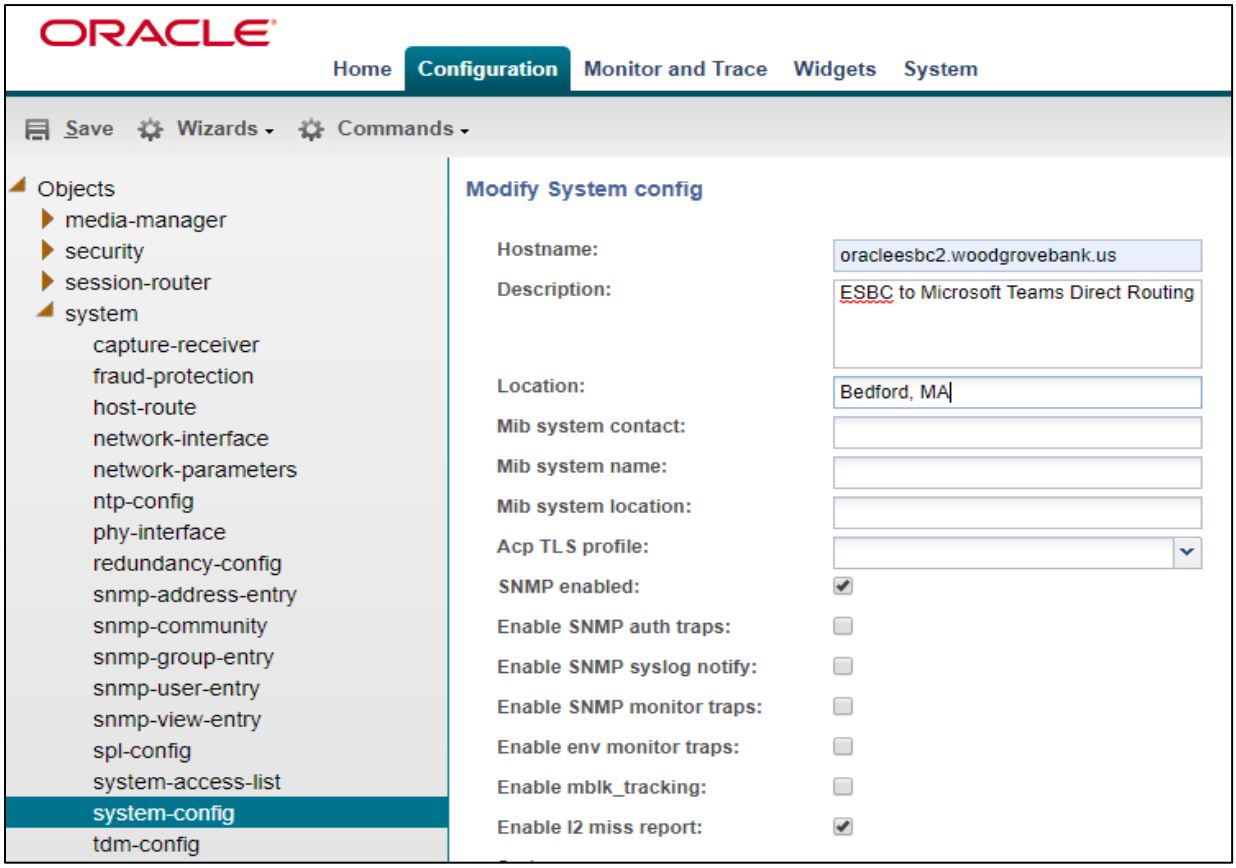
https://docs.oracle.com/cd/F13782_01/doc/esbc_scz830_webgui.pdf

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

Go to system->system-config



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

https://docs.oracle.com/cd/F13782_01/doc/esbc_scz830_releasenotes.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.

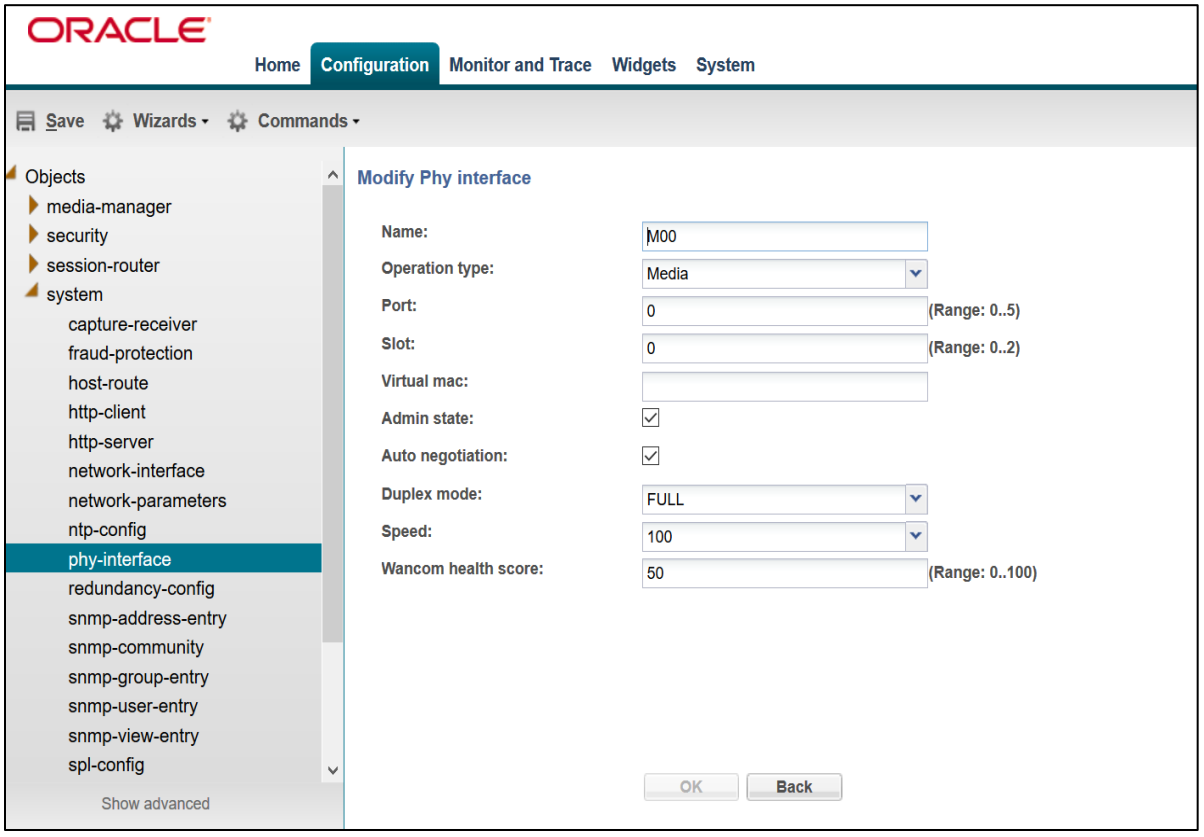
6.4.Configure Physical Interface values

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

You will first configure the slot 0, port 0 interface designated with the name M00.
This will be the port plugged into your (connection to the Pexip) interface.
SIPTRUNK side is configured on the slot 0 port 1.

Parameter Name	Pexip (M00)	SIPTRUNK (M01)
Slot	0	0
Port	0	1
Operation Mode	Media	Media

Below is the screenshot for creating a phy-interface on M00. Create a similar interface for Sip Trunk as well from the Web GUI. The table above specifies the values for both Pexip and SIPTRUNK.



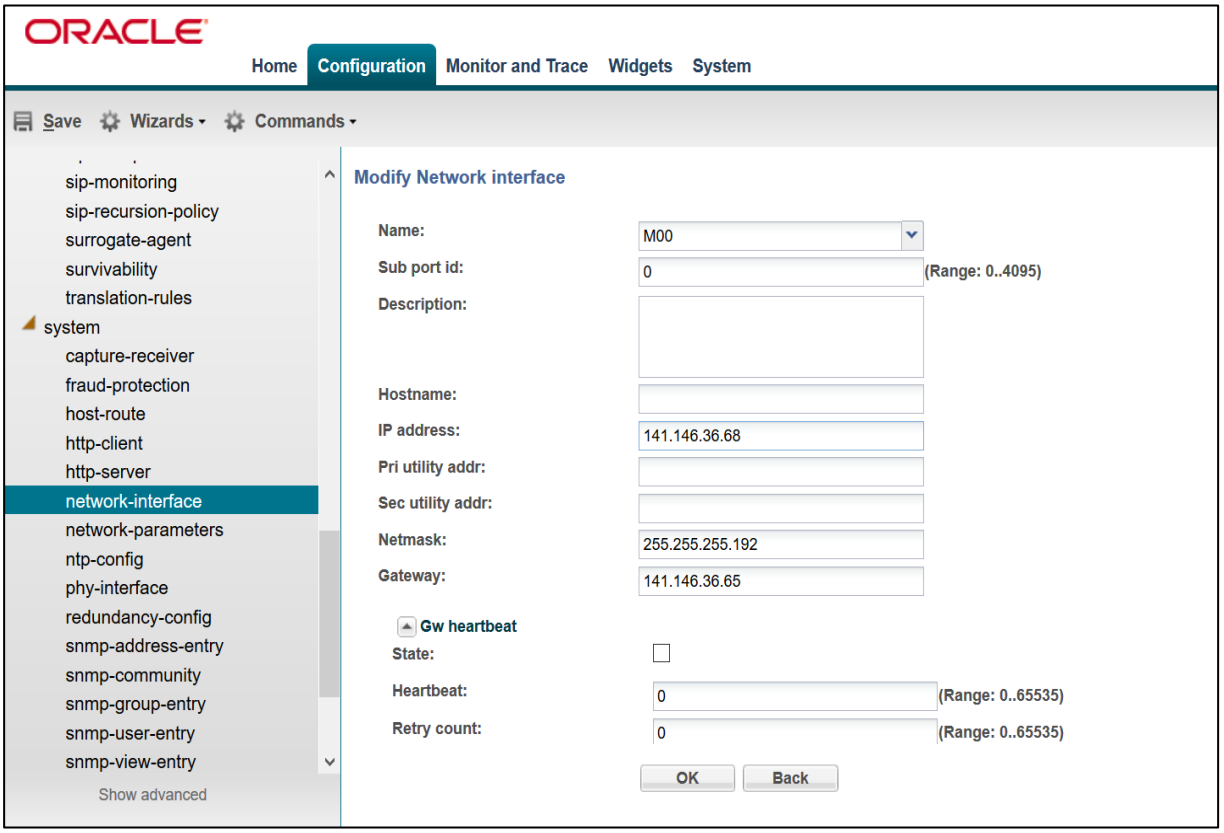
6.5. Configure Network Interface values

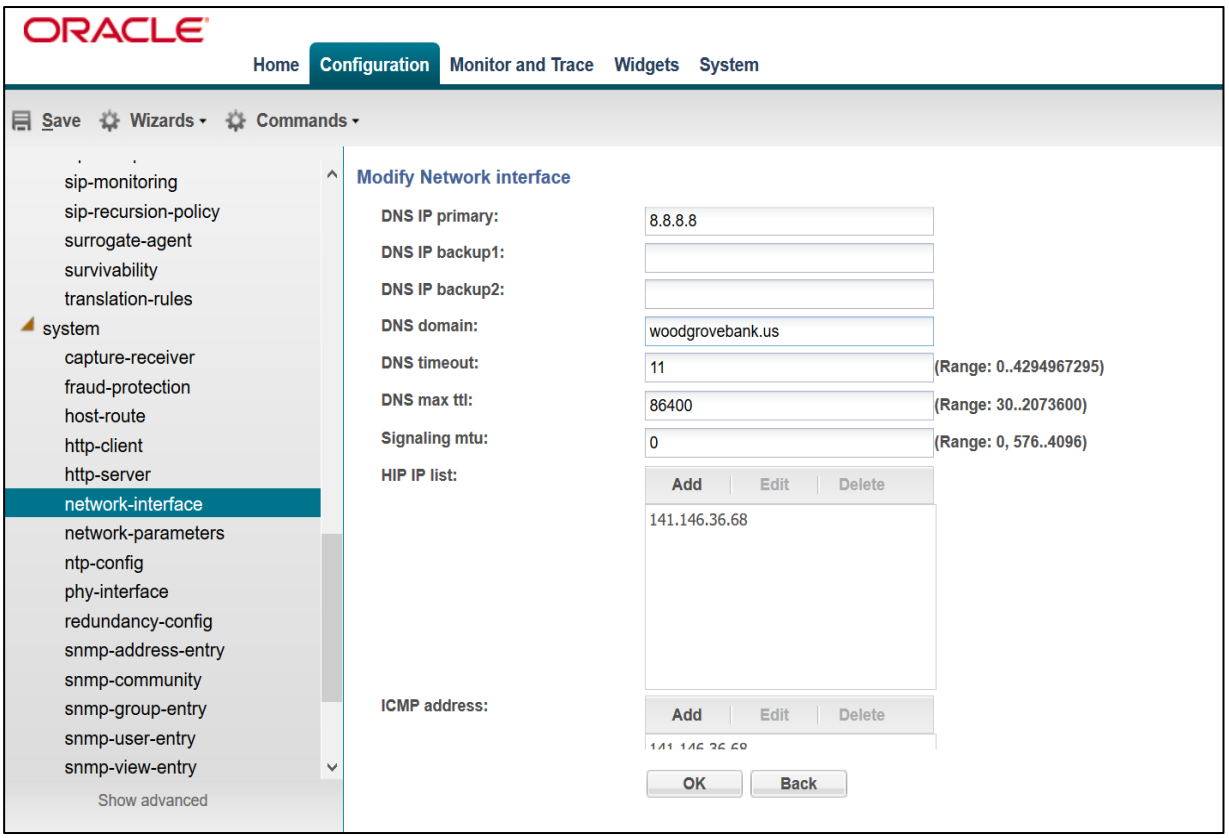
To configure network-interface, go to system->Network-Interface. Configure two interfaces,

- Pexip
- SipTrunk

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

Parameter Name	Pexip Network Interface	SipTrunk
Name	M00	M01
Host Name	oracleesbc2.woodgrovebank.us	
IP address	141.146.36.68	192.168.1.100
Netmask	255.255.255.192	255.255.255.0
Gateway	141.146.36.65	192.168.1.1
DNS-IP Primary	8.8.8.8	8.8.8.8
DNS-domain	woodgrovebank.us	


ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
sip-monitoring
sip-recursion-policy
surrogate-agent
survivability
translation-rules
system
capture-receiver
fraud-protection
host-route
http-client
http-server
network-interface
network-parameters
ntp-config
phy-interface
redundancy-config
snmp-address-entry
snmp-community
snmp-group-entry
snmp-user-entry
snmp-view-entry
Show advanced
Modify Network interface
Name: M00
Sub port id: 0 (Range: 0..4095)
Description:
Hostname:
IP address: 141.146.36.68
Pri utility addr:
Sec utility addr:
Netmask: 255.255.255.192
Gateway: 141.146.36.65
Gw heartbeat
State:
Heartbeat: 0 (Range: 0..65535)
Retry count: 0 (Range: 0..65535)
OK
Back


ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
sip-monitoring
sip-recursion-policy
surrogate-agent
survivability
translation-rules
system
capture-receiver
fraud-protection
host-route
http-client
http-server
network-interface
network-parameters
ntp-config
phy-interface
redundancy-config
snmp-address-entry
snmp-community
snmp-group-entry
snmp-user-entry
snmp-view-entry
Show advanced
Modify Network interface
DNS IP primary: 8.8.8.8
DNS IP backup1:
DNS IP backup2:
DNS domain: woodgrovebank.us
DNS timeout: 11 (Range: 0..4294967295)
DNS max ttl: 86400 (Range: 30..2073600)
Signaling mtu: 0 (Range: 0, 576..4096)
HIP IP list:
Add Edit Delete
141.146.36.68
ICMP address:
Add Edit Delete
OK
Back

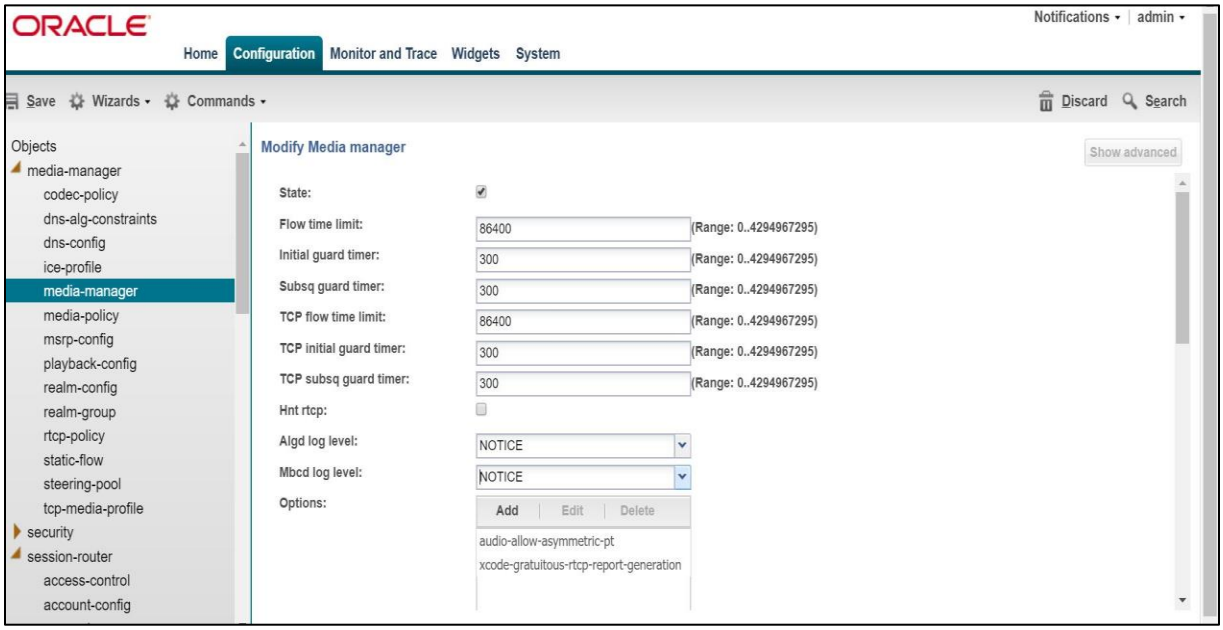
Similarly configure network interfaces for M01 (SipTrunk) as well

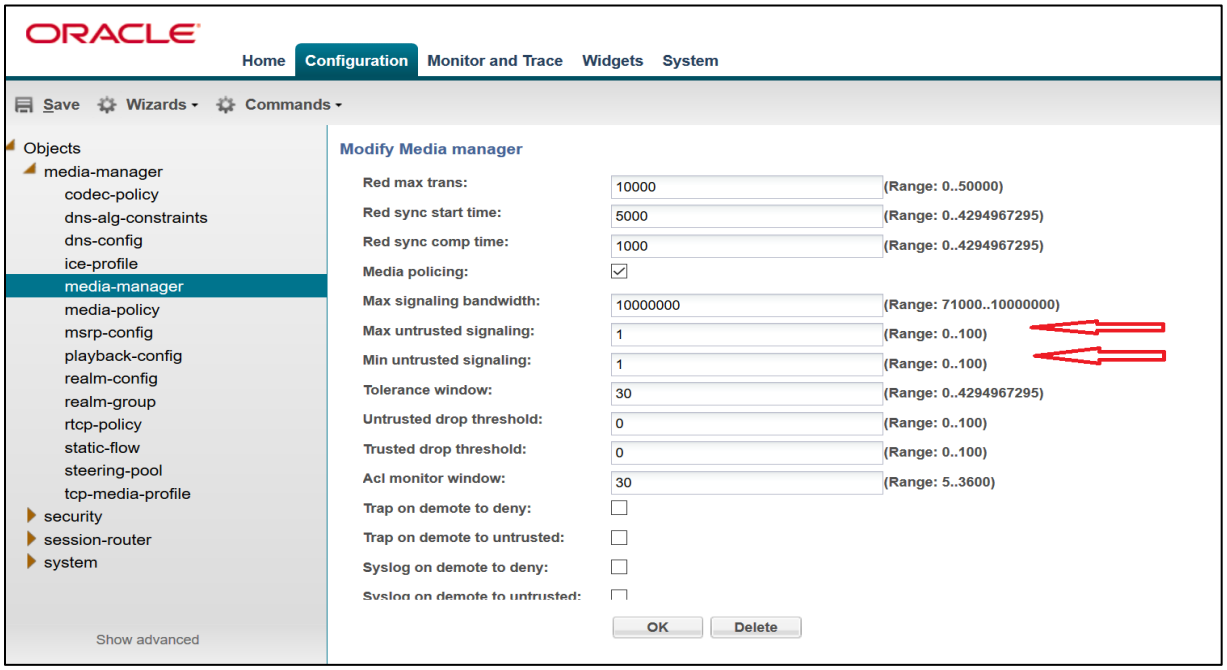
6.6.Enable media manager

Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager and configure the below option for generating rtcp reports. A reboot of SBC is needed after adding audio allow hidden option.

- audio-allow-asymmetric-pt
- xcode-gratuitous-rtcp-report-generation

In addition to the above config, please set the max and min untrusted signaling values to 1.
Go to Media-Manager->Media-Manager

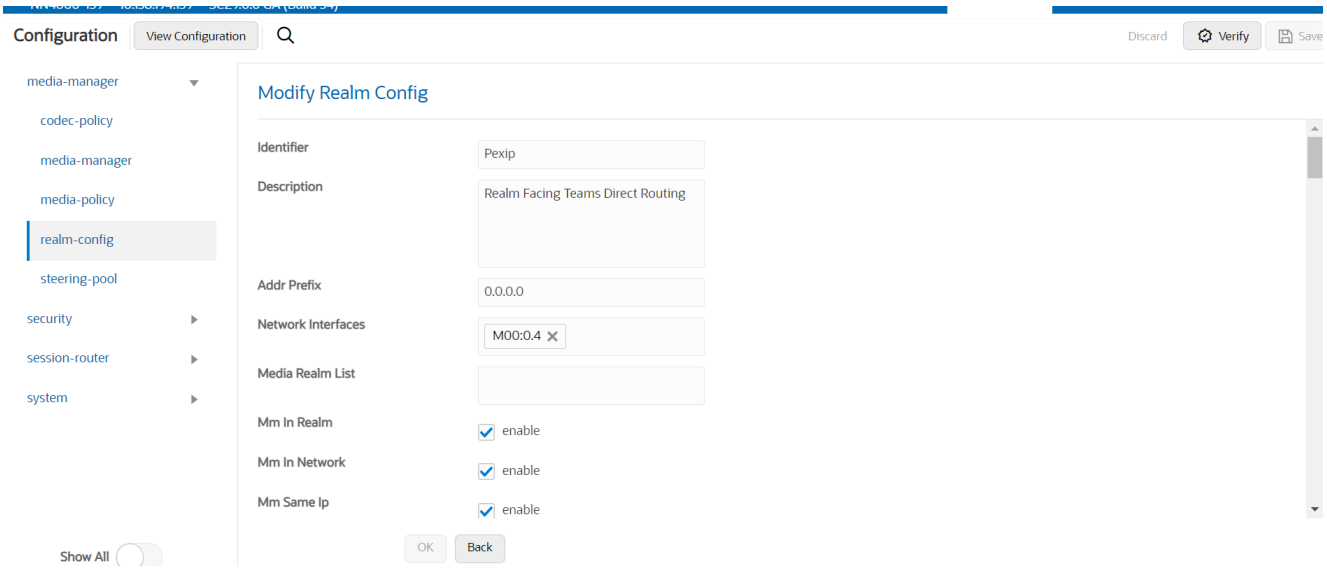




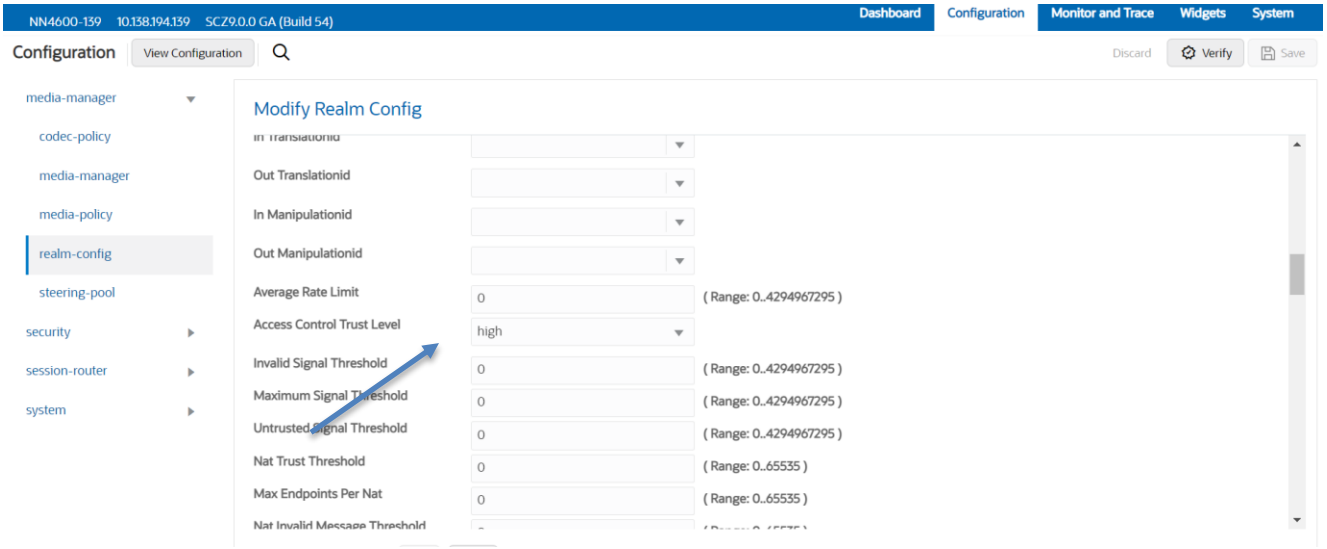
6.7.Configure Realms

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.

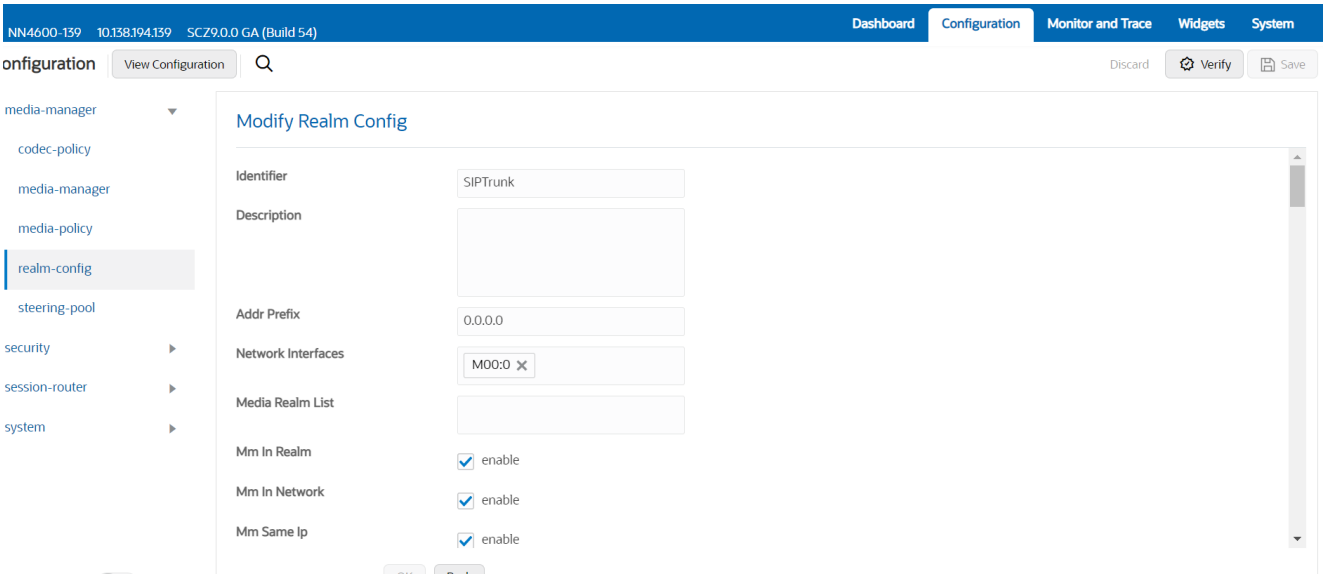
In the below case, Realm name is given as Pexip



Make sure the access control level is set as high.



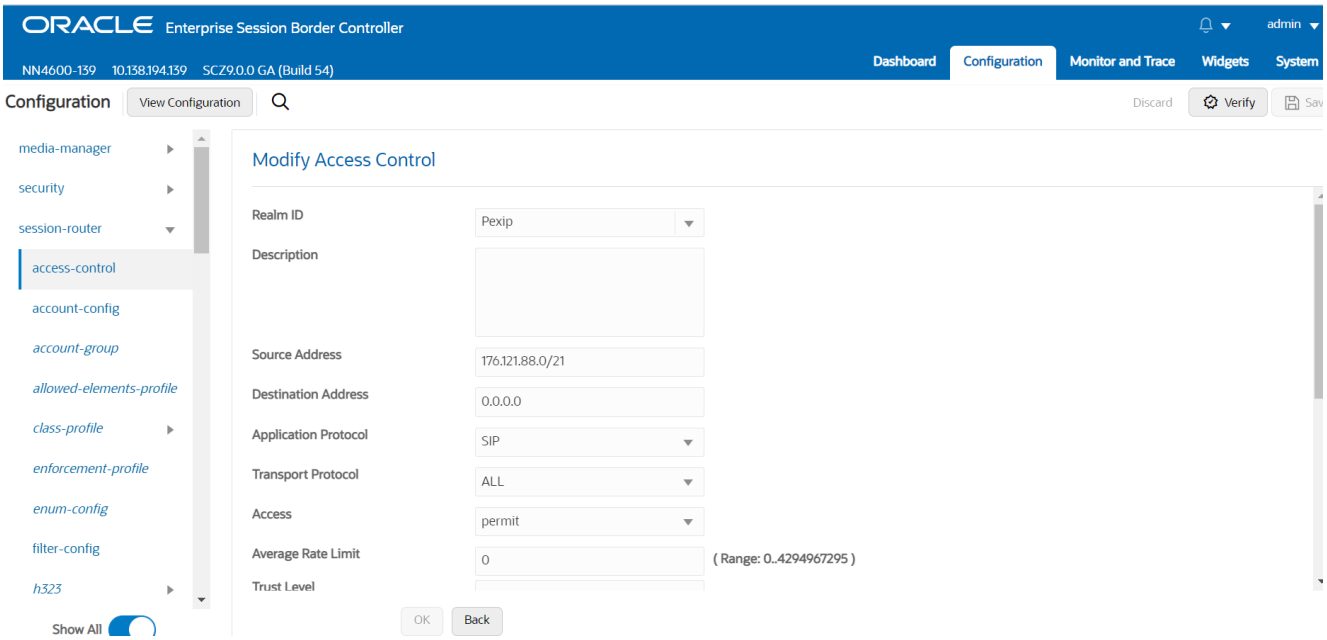
Similarly, Realm is named as SipTrunk for realm facing SipTrunk.



6.8.Access-control Lists

Using a list of IP addresses and subnets that are allowable as packet sources, you can configure what traffic the Oracle® Enterprise Session Border Controller accepts and what it denies. All IP packets arriving on the management interface are subject; if it does not match your configuration for system ACL, then the Oracle® Enterprise Session Border Controller drops it.

Configure the IP-addresses listed in the Pexip firewall listed here https://pexip.me/test/firewall Make sure the trust level is set to high here as well.



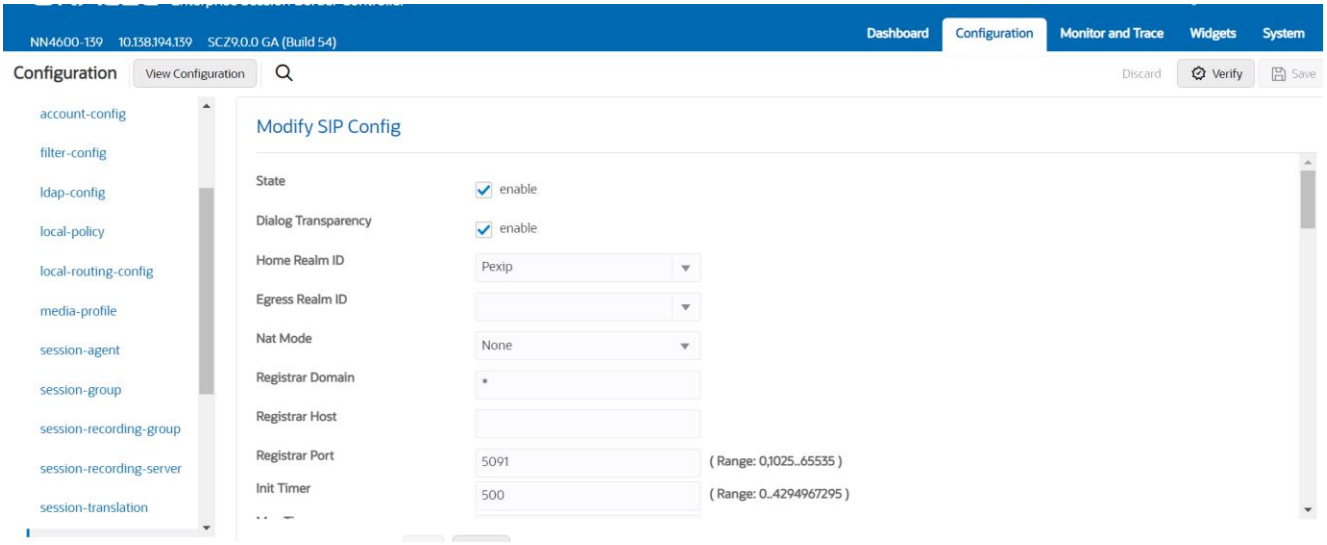
Since the access-control –level of realm is set to high,SBC allows only those entries present in this list.

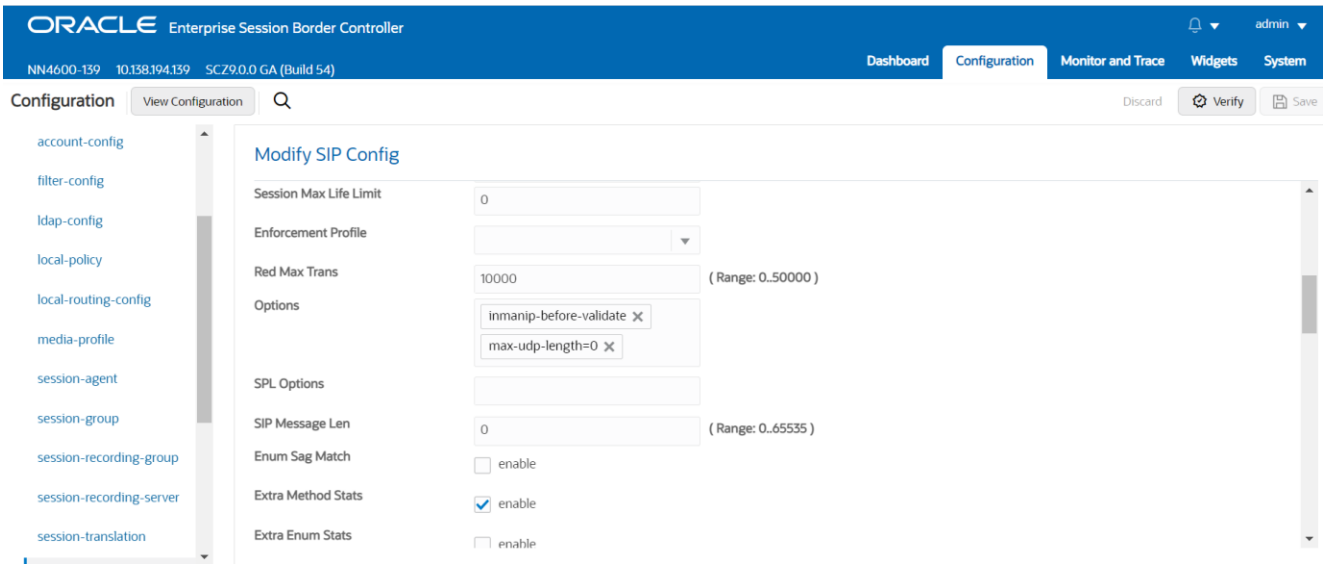
6.9.Enable sip-config

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





6.10. Configuring a certificate for SBC

Pexip allows both UDP and TLS connections for SIP signalling. However in this document, we are configuring the Oracle SBC server with TLS configuration.
The certificate used for this testing is signed by one of the trusted certification authorities.

The step below describes how to request a certificate for SBC External interface and configure it based on the example of DigiCert. 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.

The following certificate-records are required on the Oracle SBC in order for the SBC to connect with Pexip

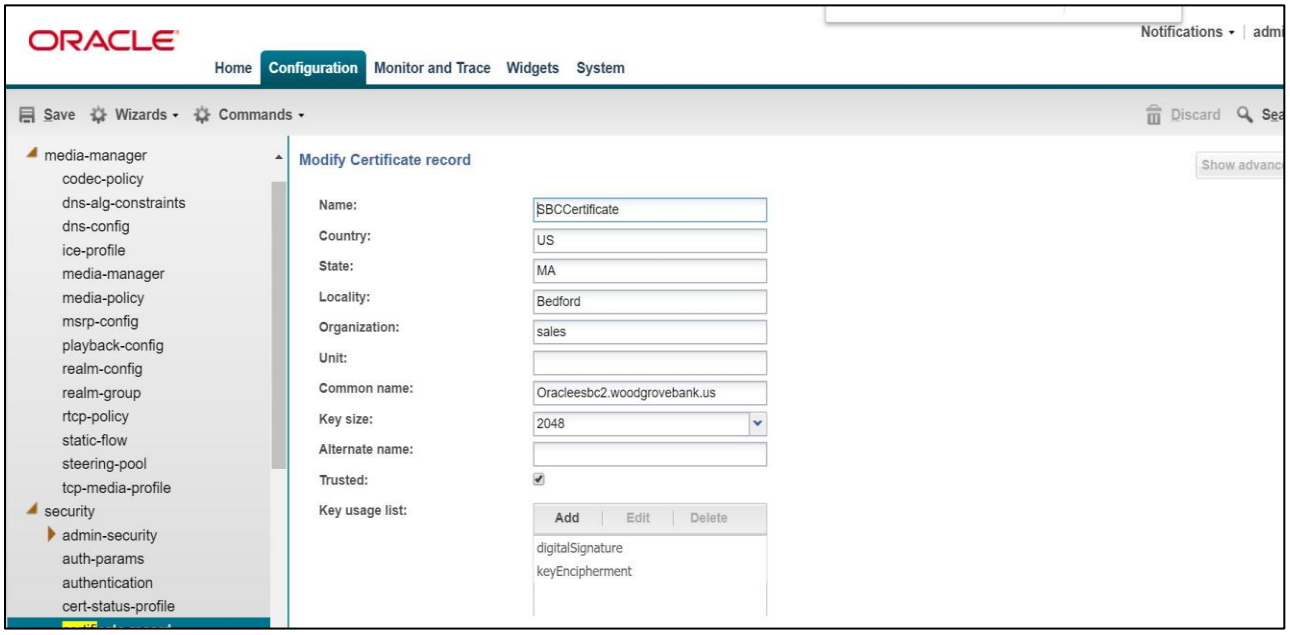
- SBC – 1 certificate-record assigned to SBC
- Root – 1 certificate-record for root cert
- Intermediate – 1 certificate-record for intermediate (this is optional – only required if your server certificate is signed by an intermediate)

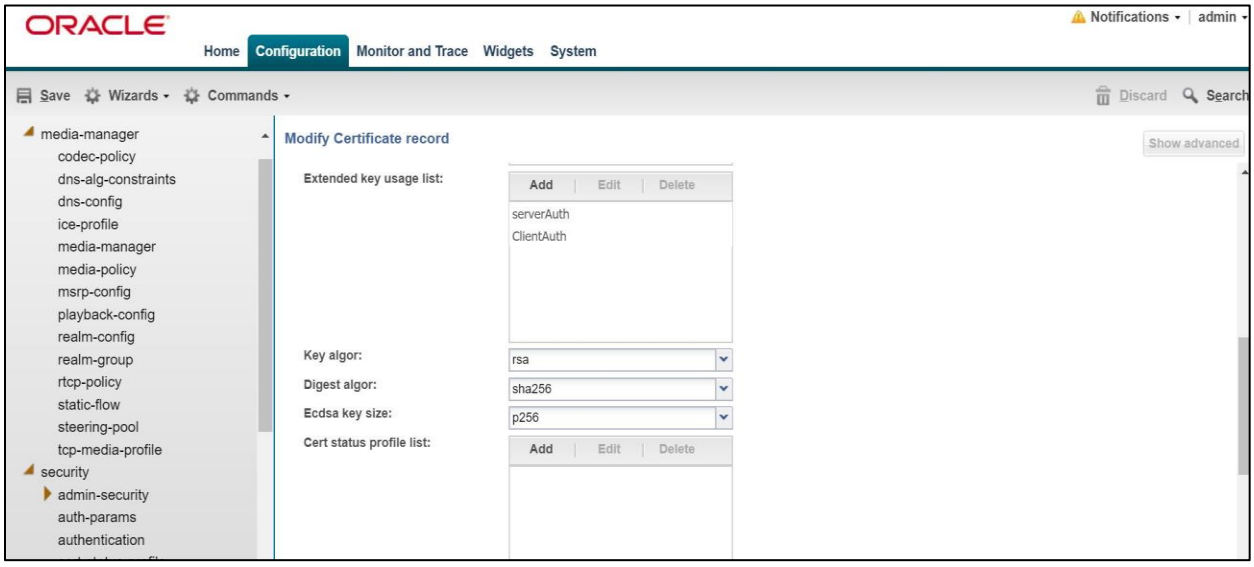
2) Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority

3) Deploy the SBC and Root/Intermediary certificates on the SBC

Step 1 – Creating the certificate record

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





Follow the same steps and create following intermediate and root certificates.
-BaltimoreRoot: This certificate is always required for MS Pexip.

See the link here, to get some additional information
https://baltimore-cybertrust-root.chain-demos.digicert.com/info/index.html

-DigiCertRoot
-DigiCertInter

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

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

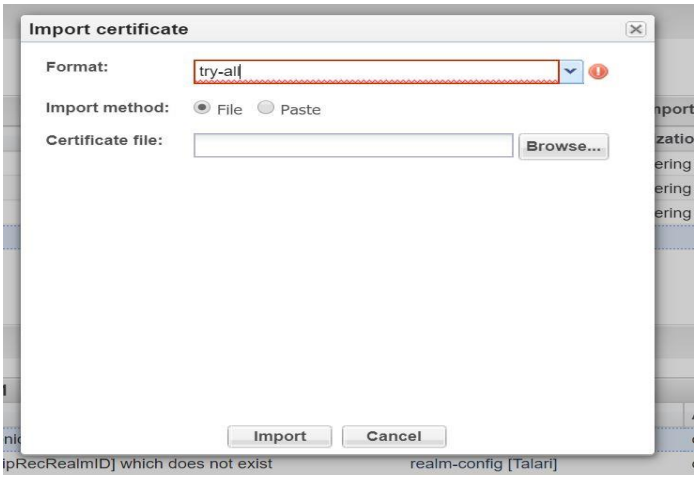
Please note – certificate signing request is only required to be executed for SBC Certificate – not for the root/intermediate certificates.

- 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/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:

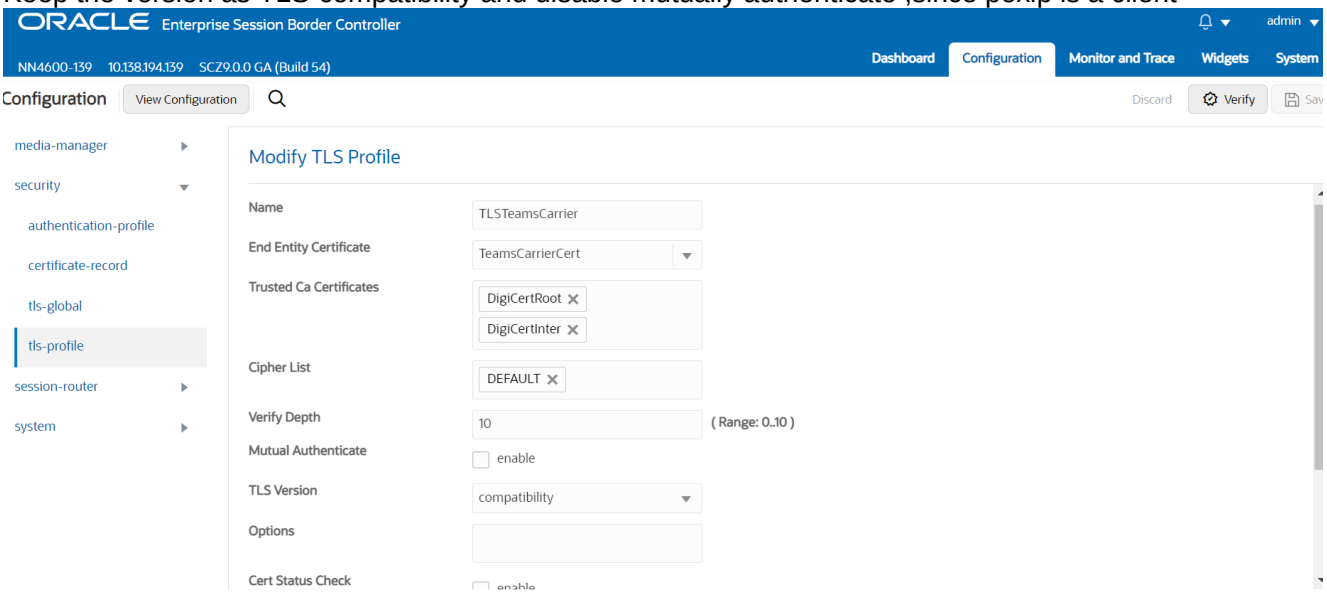
- BaltimoreRoot
- DigiCertInter
- DigiCertRoot.
-

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

6.11. 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

Keep the version as TLS-compatibility and disable mutually authenticate ,since pexip is a client



6.12. Configure SIP Interfaces.

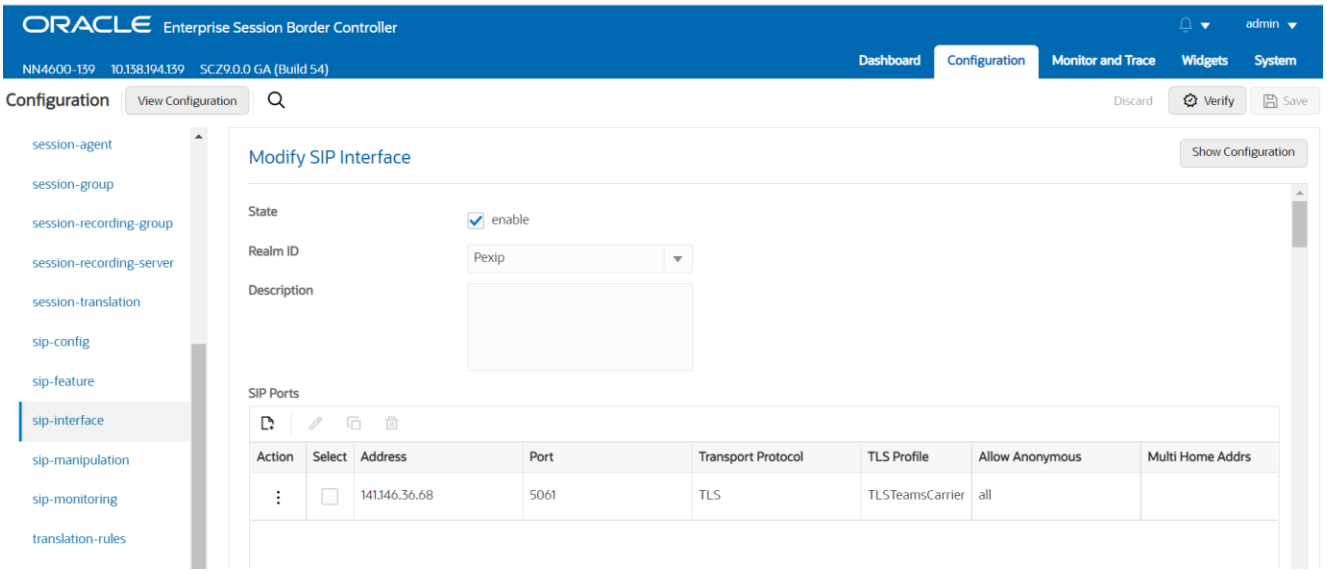
Navigate to sip-interface under session-router and configure the sip-interface as shown below
Pexip supports both UDP and TLS for SIP communication. The document describes TLS transport for SIP.

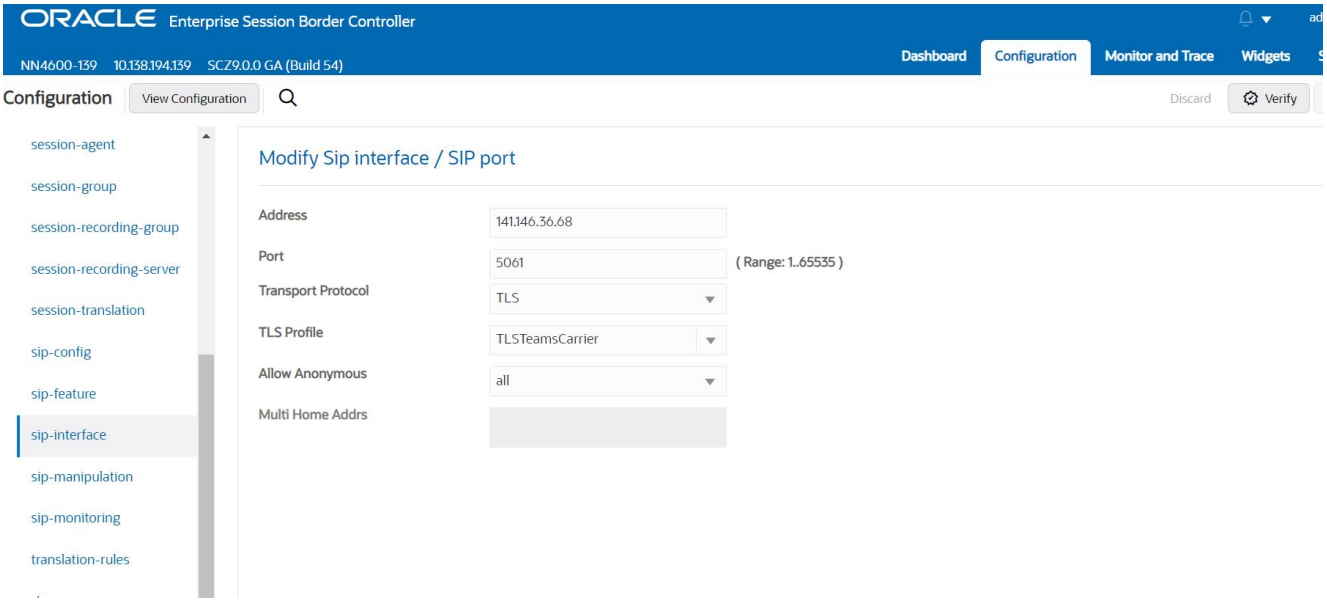
TLS Transport for SIP towards Pexip

Ensure that the IP address allocated to the SIP interface is the FQDN resolvable address.
I.e. if you issue command nslookup from another computer, “oracleesbc2.woodgrovebank.us” – it should resolve to 141.146.36.68. Note that the IP should be publicly routable IP address.

Note:

-Tls-profile needs to match the name of the tls-profile previously created
-Set allow-anonymous to all.

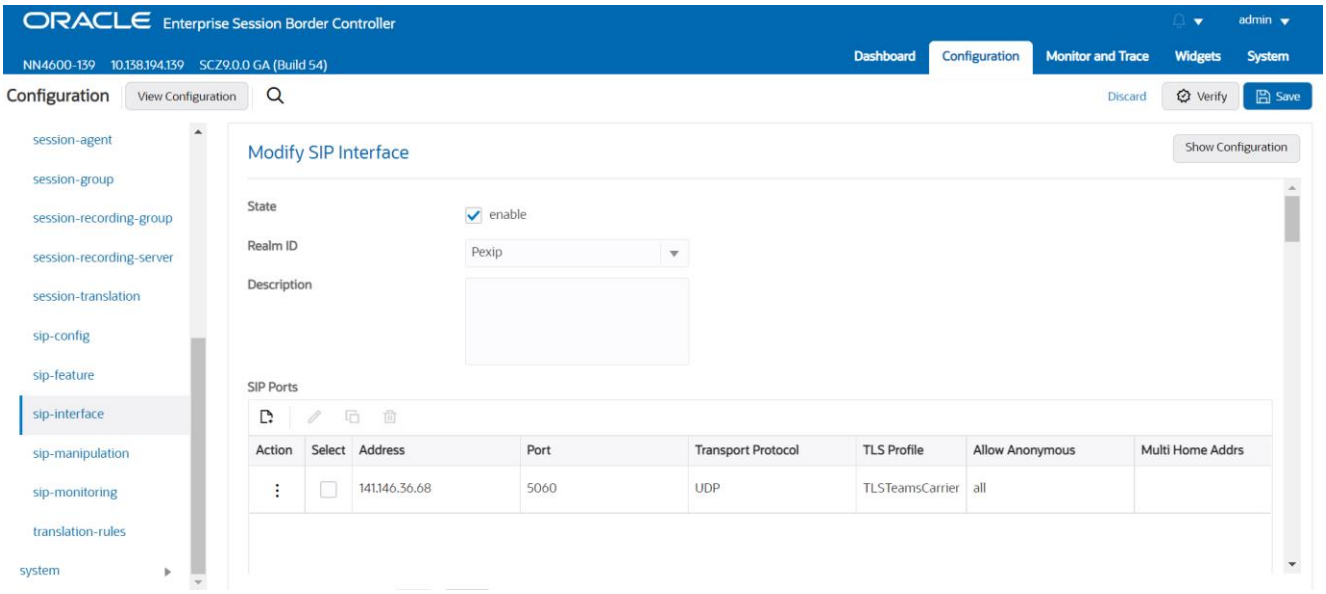




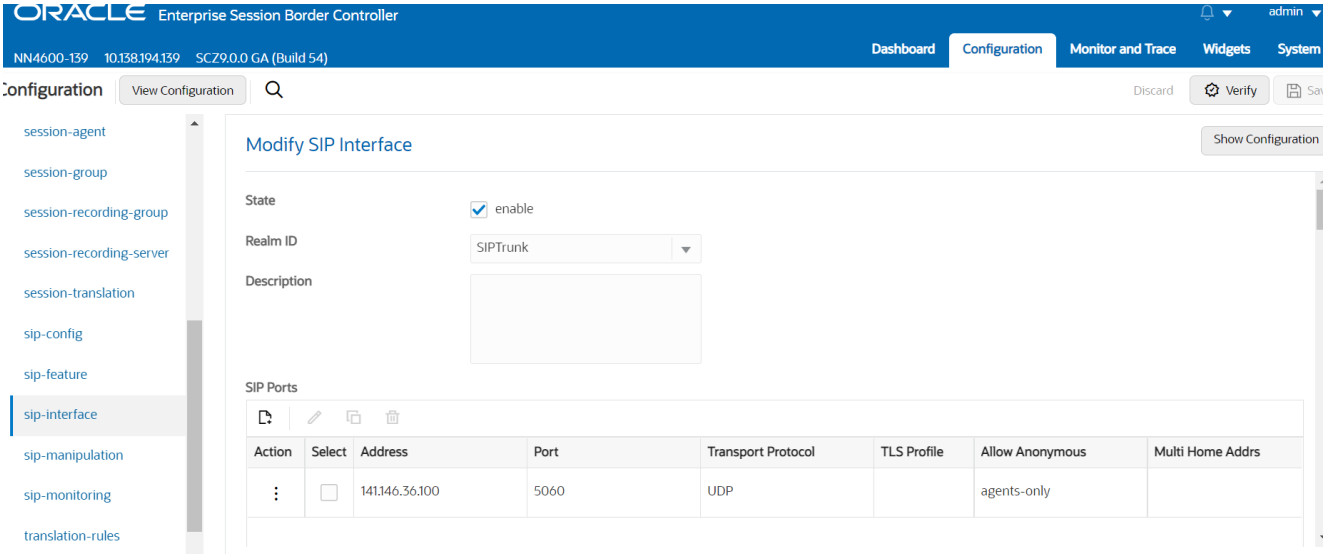
UDP Transport for SIP towards Pexip

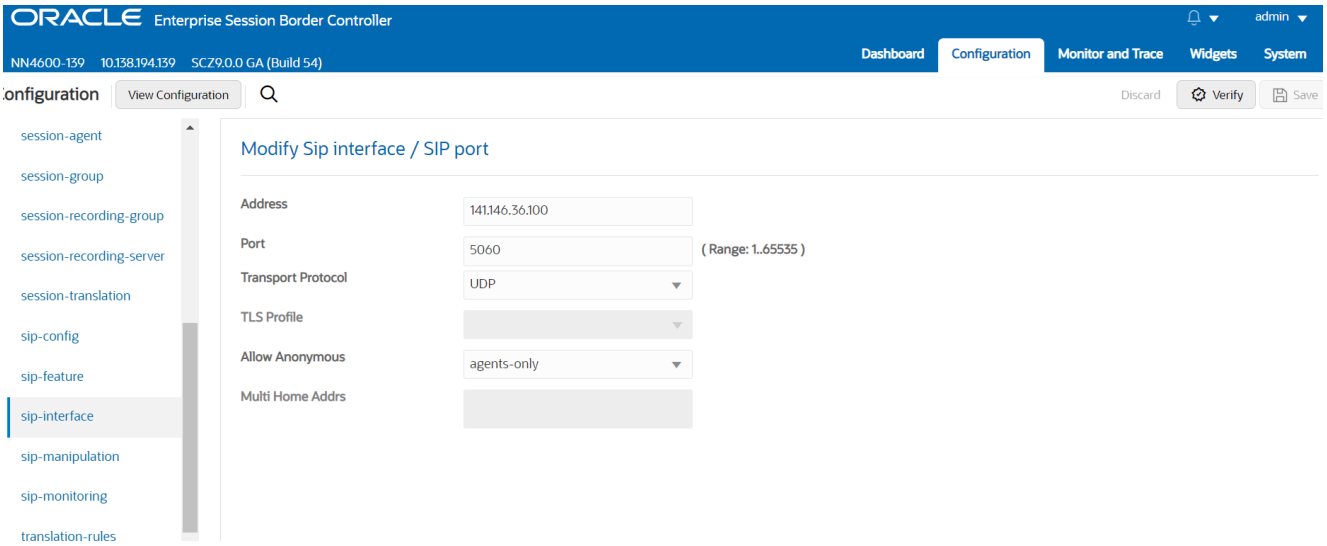
For UDP communication towards Pexip, configure the sip-interface as UDP with port as 5060 and allow-anonymous set as all.

Note: TLS Profile and certificates are not required for UDP mode.



Similarly, Configure Internal IP under sip-port of sip-interface for SIPTRUNK





Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.
Now configure where the SBC sends the outbound traffic.

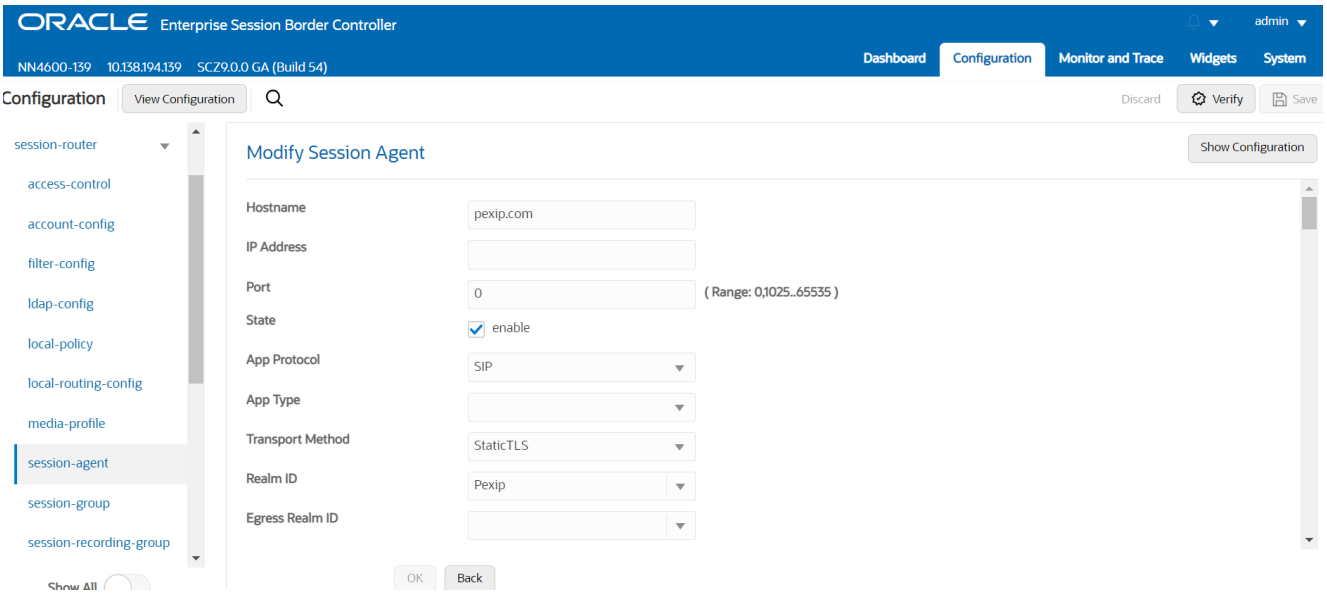
6.13. Configure session-agent

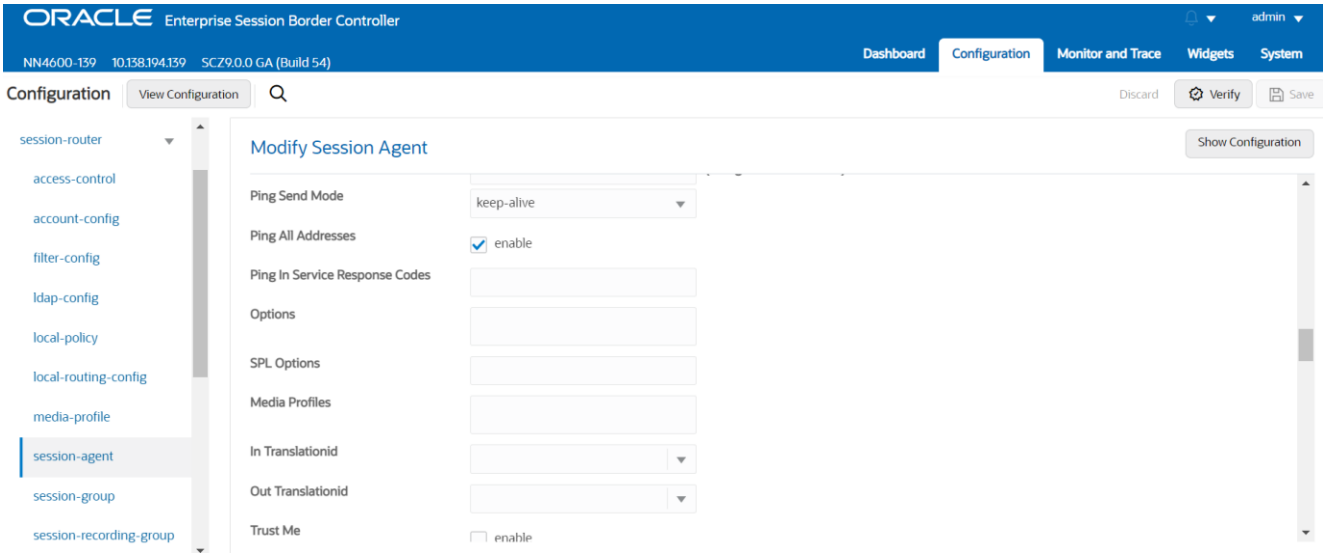
Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

Configure the session-agent for Pexip with the following parameters.
Go to session-router->Session-Agent.

- hostname to “pexip.com”
- port 0
- realm-id – needs to match the realm created for Pexip
- transport set to “StaticTLS”
- ping-all-addresses enabled

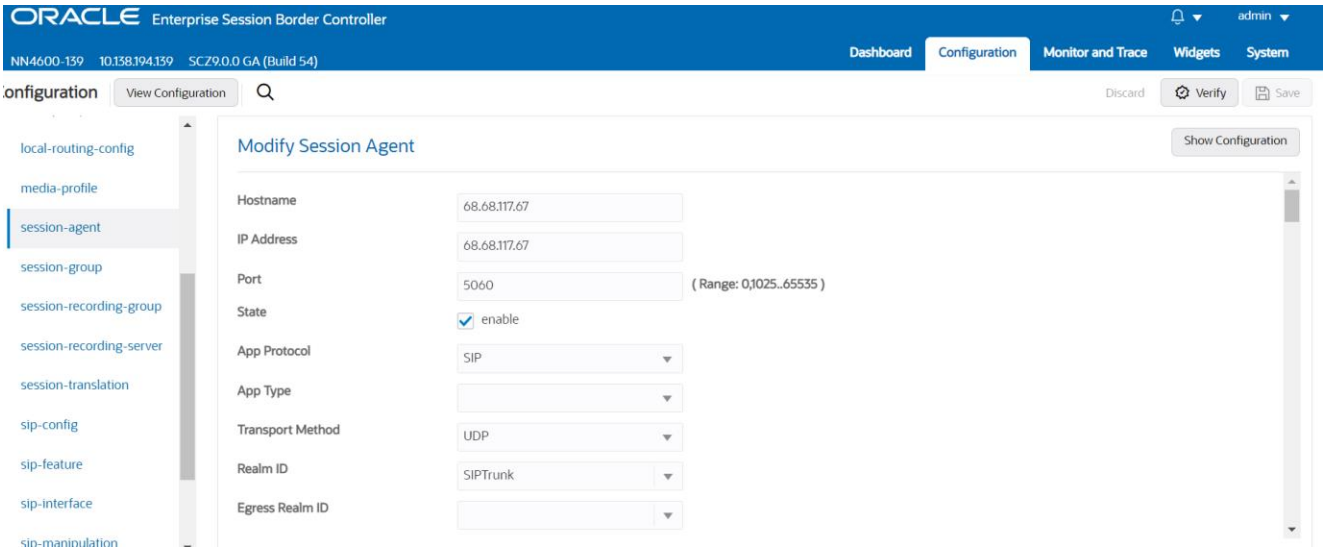
SBC will make a DNS query and resolve pexip.com since the port is set to zero and ping-all-addresses are enabled.





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

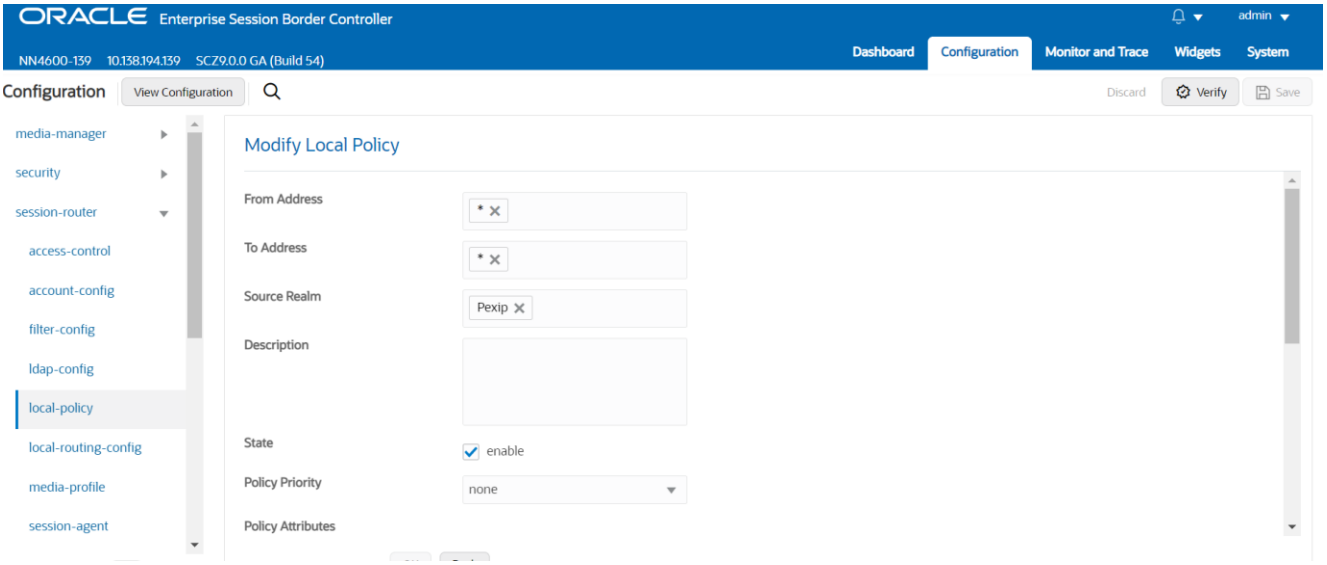
- Host name and IP address to ip-address of SIP Trunk.
- port 5060
- realm-id – needs to match the realm created for SIPTRUNK.
- transport set to “UDP”

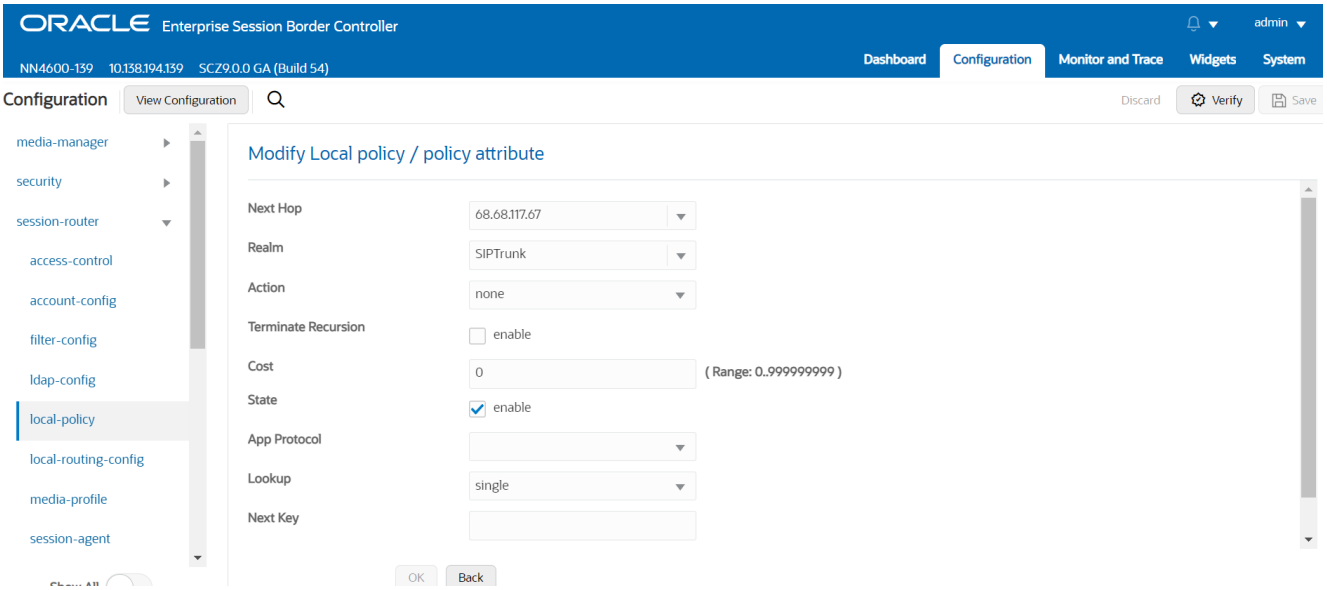


6.14. Configure local-policy

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.
Note: For Pexip environment, the requirement is to route calls only one way i.e. from Pexip to SIP Trunk, local policy is configured accordingly.

To make calls from Pexip to SIPTRUNK the following config is required:
The next hop should be the SIP trunk session-agent IP.





Note:If the customer requires call routing based on the caller-id,the Caller-ID given by Pexip for different dial plans can be configured in the From Address of the local policy,so that the other calls are rejected with a 480 No Routes Found.

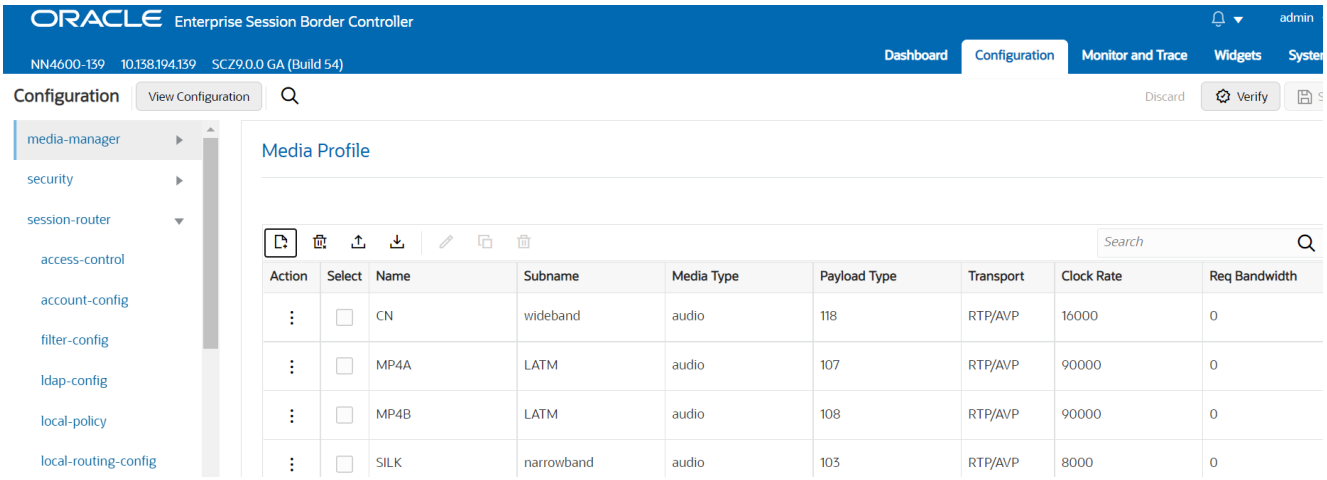
6.15. Configure Media Profile and Codec Policy

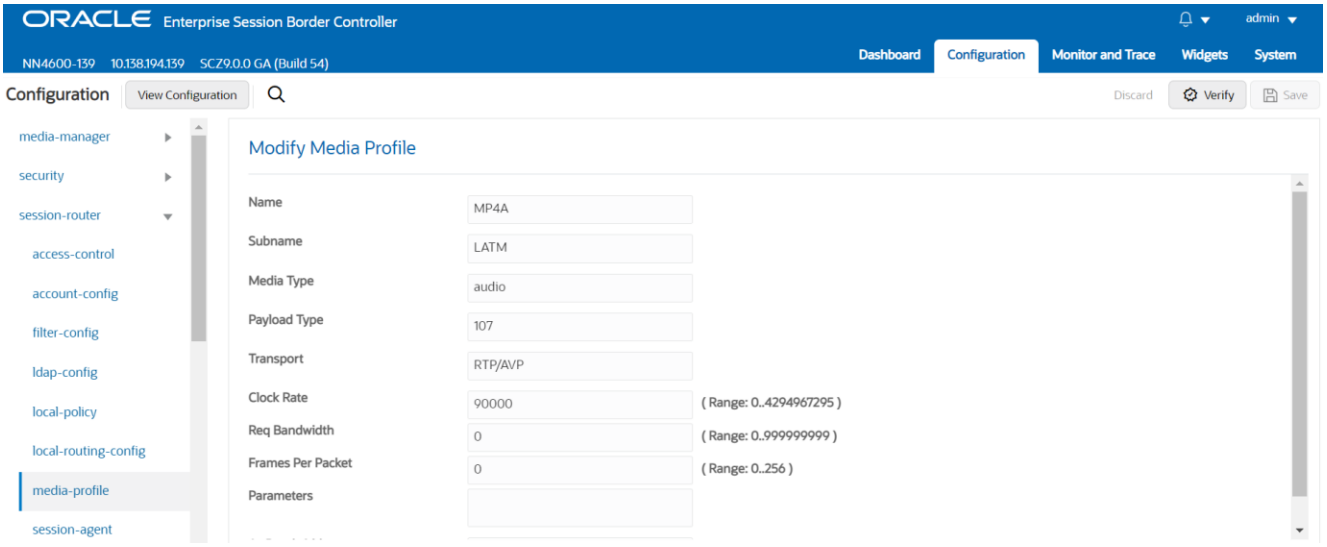
The Oracle Session Border Controller (SBC) uses codec policies to describe how to manipulate SDP messages as they cross the SBC. The SBC bases its decision to transcode a call on codec policy

configuration and the SDP. Each codec policy specifies a set of rules to be used for determining what codecs are retained, removed, and how they are ordered within SDP.

Note: this is an optional config – configure codec policy only if deemed required.
Some SIP Trunks do not support MP4A-LATM and MP4B-LATM codecs offered by the Cisco DX70 connected to Pexip.
On the SBC we configure media –profiles for them and remove the codecs towards SipTrunk with a NO.

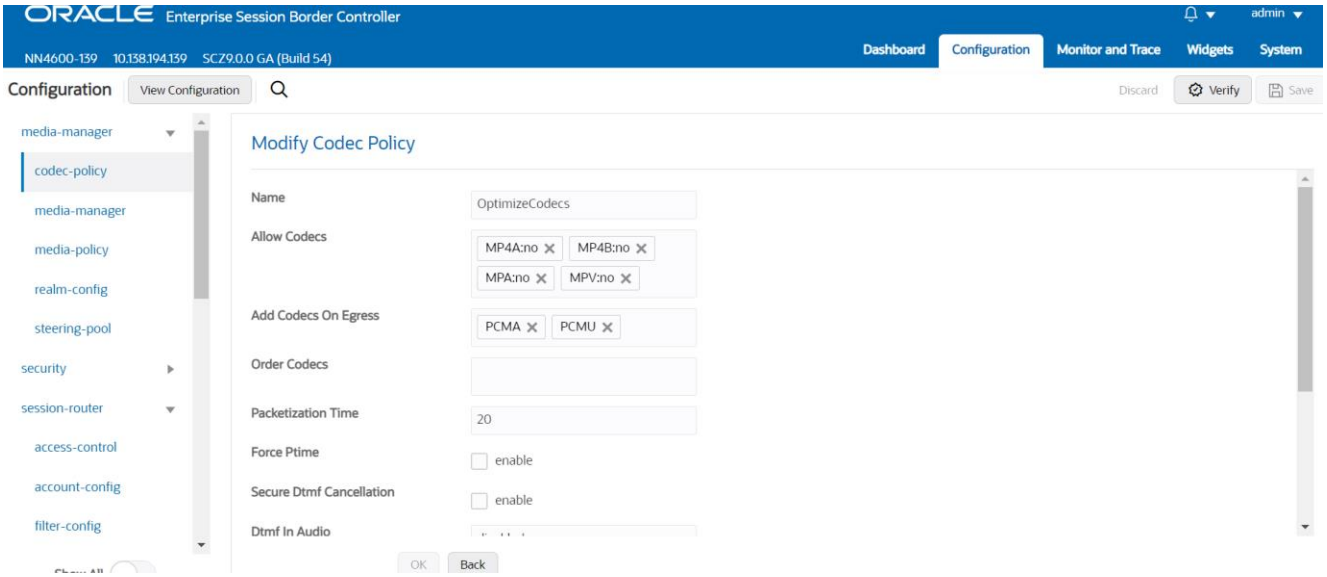
Go to Session-Router->Media Profile.Configure media profiles for MP4A-LATM and MP4B-LATM as shown



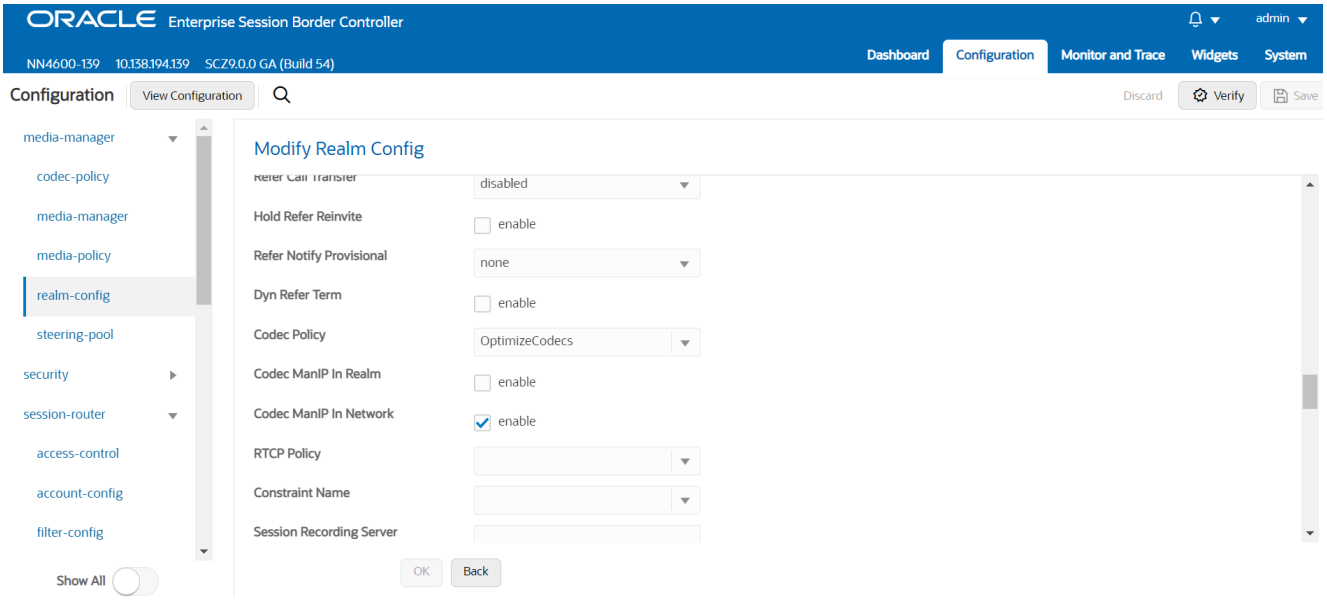


Parameters	MP4A	MP4B
Subname	LATM	LATM
Payload-Type	107	108
Clock-rate	90000	90000

After creating media profile, create codec-policy, which denies these codecs towards the SIP Trunk.
Go to media manager ---- codec policy.

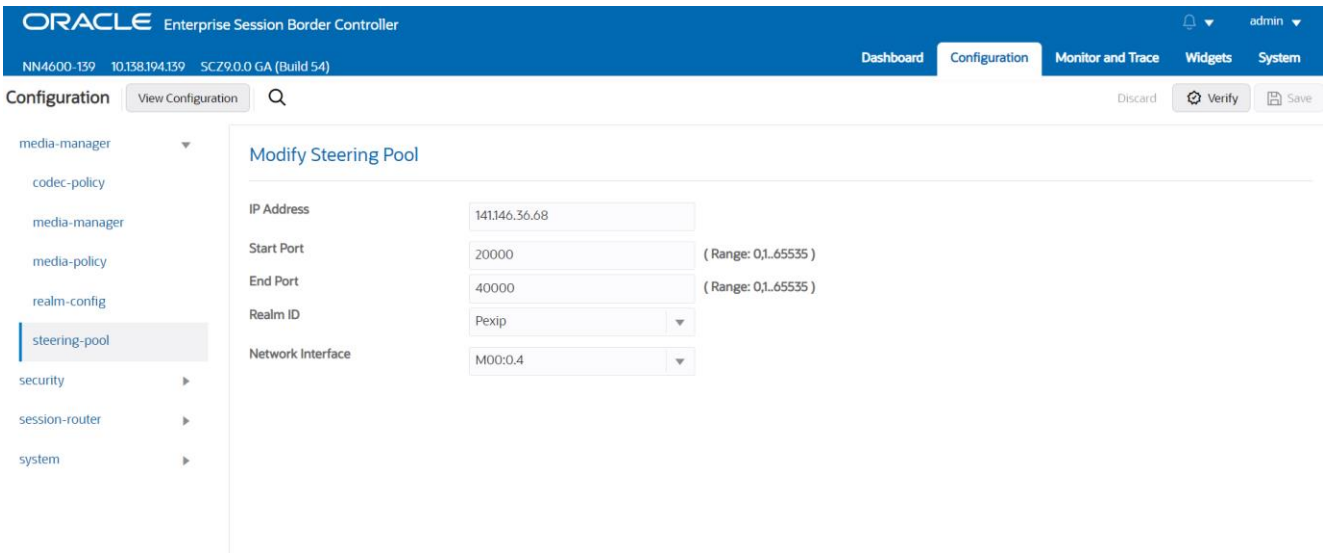


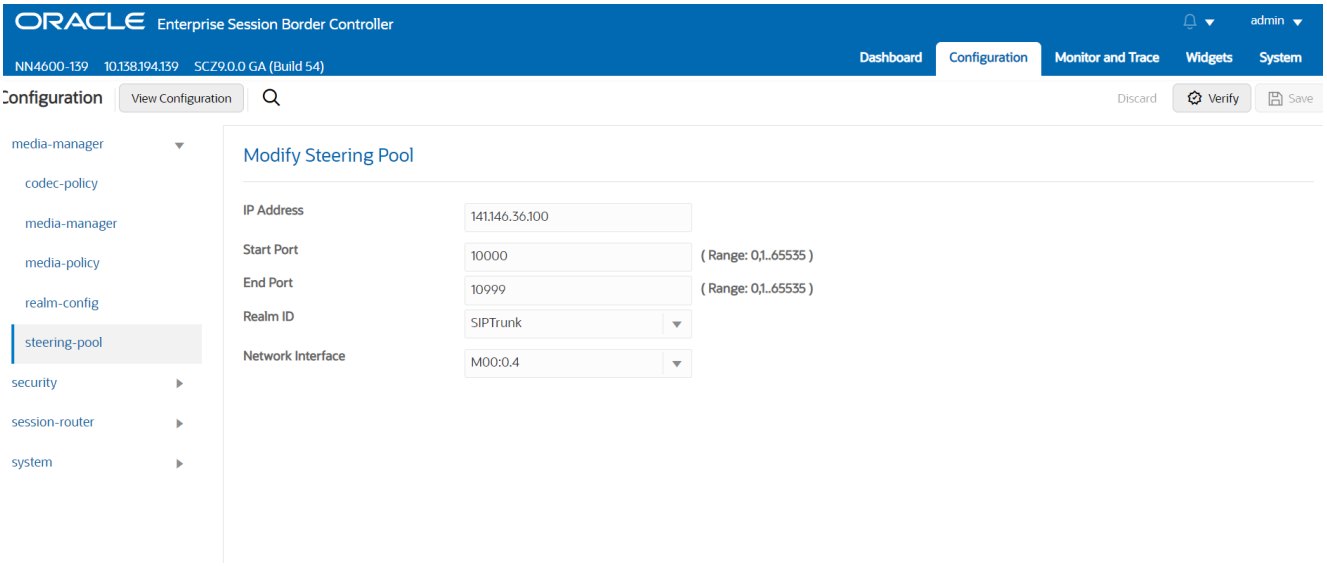
Go to media manager ---- realm config and assign the codec policy to the SIP Trunk realm



6.16. Configure steering-pool

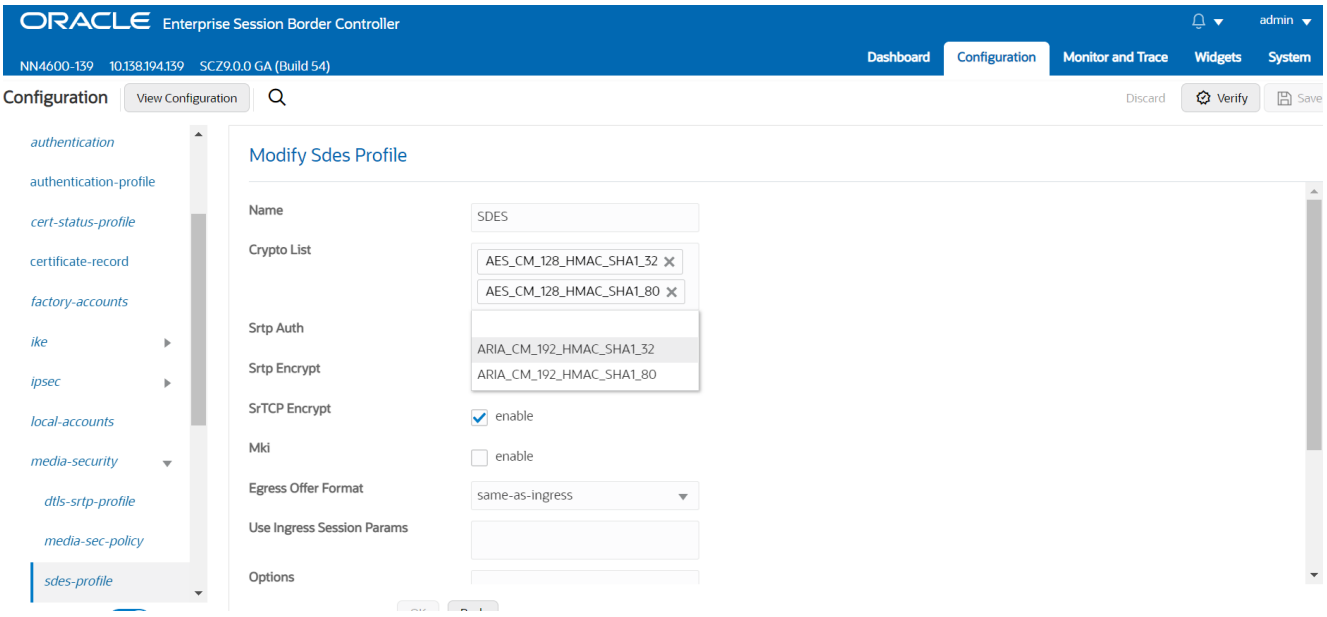
Steering-pool config allows configuration to assign port range for media handling on the SBC.





6.17. Configure sdes profile

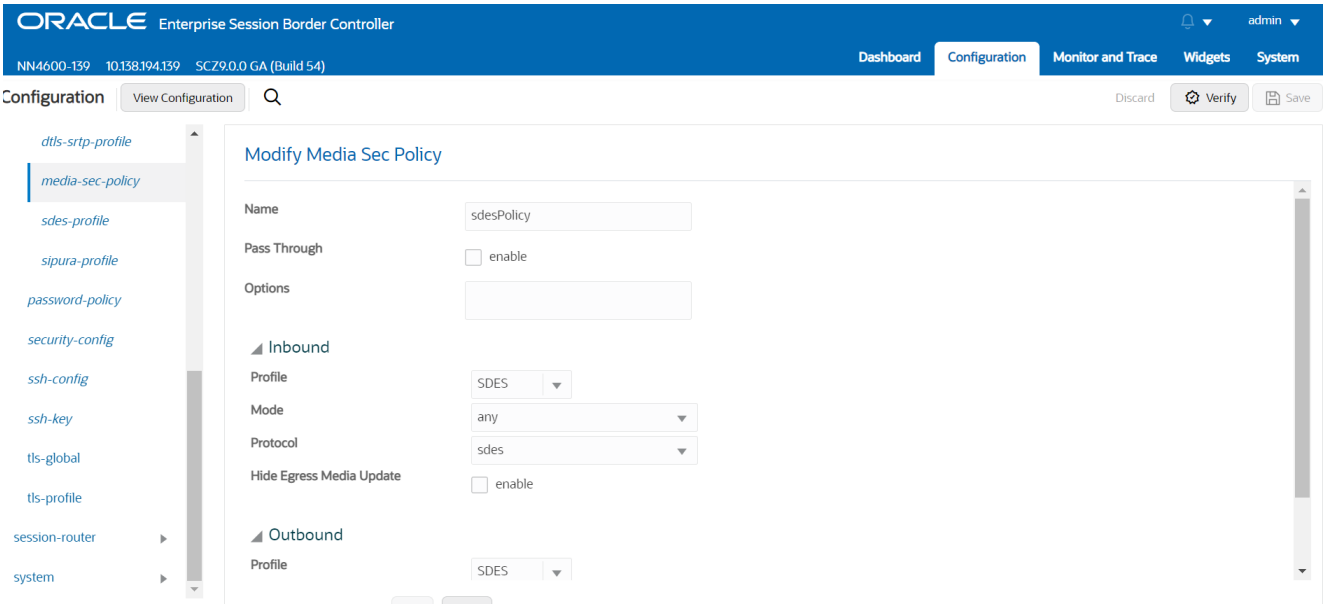
Pexip supports both RTP and SRTP for Media.For SRTP mod ciphers have to be configured on the SBC. Please go to →Security → Media Security →sdes profile and create the policy as below.
For testing purposes we have configured two ciphers .



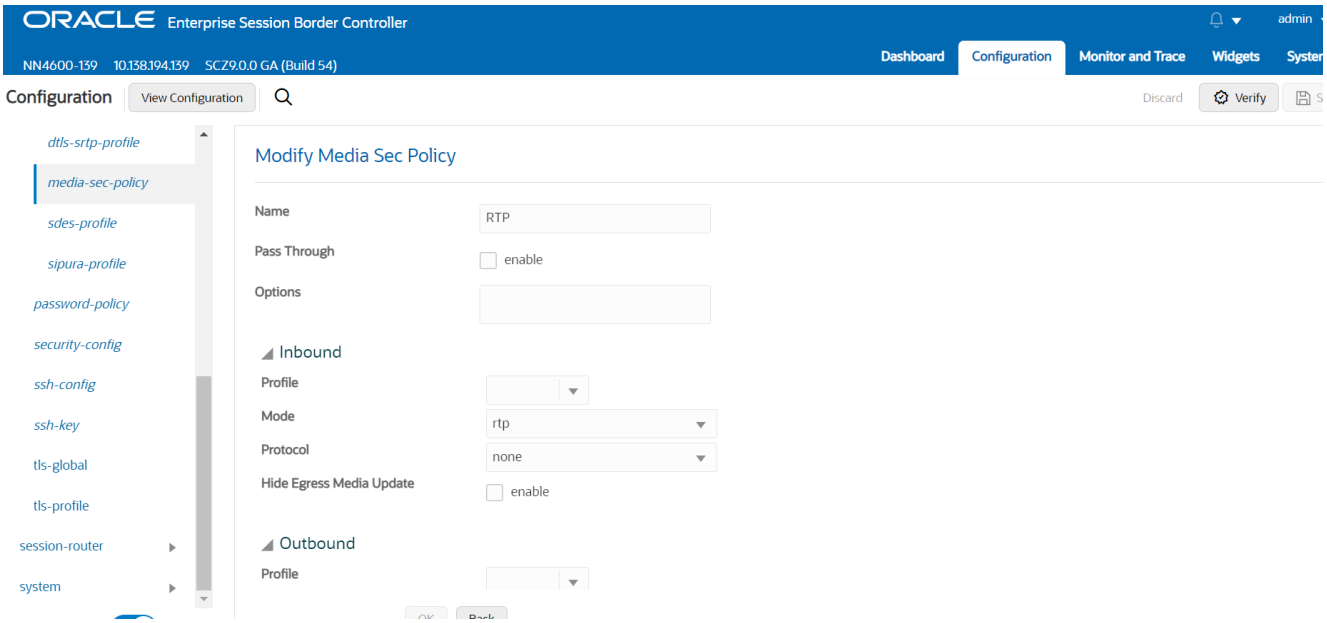
6.18. Configure Media Security Profile

Please go to →Security → Media Security →media Sec policy and create the policy as below:
Create Media Sec policy with name SDES for the Pexip side which will have the sdes profile created above.
Note: Since calls from Pexip can be encrypted as well as unencrypted set the mode to any in the media-sec-policy.

Assign this media policy to the Pexip Realm.



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



7. Existing SBC configuration

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

- New realm-config
- Configuring a certificate for SBC Interface
- TLS-Profile
- Enable DNS
- New sip-interface
- New session-agent
- New-Session-Agent-Group
- Sip Manipulation
- New steering-pools
- New Local-policy
- Media-profile
- Codec-policy
- SDES Profile
- Media-sec-Policy
-

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

8. Caveat

Currently the testing involves making calls one-way from Pexip server to the SIP Trunk.Also calls only from the Cisco DX70 and Polycom registered on the Pexip server are tested.

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/Oracle/

twitter.com/Oracle

oracle.com

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services