Oracle SBC integration with Cisco CUCM and Generic Sip Trunk

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 CUCM and Generic SIP Trunk	10th May 2022

Table of Contents

1. INTENDED AUDIENCE 5

2. DOCUMENT OVERVIEW 5

2.1. CISCO CALL MANAGER (CISCO CUCM) 5

3. INTRODUCTION 6

3.1. AUDIENCE 6

3.2. REQUIREMENTS 6

3.3. ARCHITECTURE 7

4. CONFIGURING THE CISCO CALL MANAGER (CISCO CUCM) 8

4.1. CONFIGURING A NEW SIP TRUNK 8

4.2. CONFIGURE A NEW ROUTE PATTERN 10

4.3. END USER CONFIGURATION 12

4.4. ADDING SIP PHONE IN CUCM 13

4.5. ASSOCIATING END USER TO PHONE 15

5. CONFIGURING THE SBC 16

5.1. VALIDATED ORACLE SBC VERSION 16

6. NEW SBC CONFIGURATION 16

6.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC 16

6.2. CONFIGURE SBC USING WEB GUI 20

6.3. CONFIGURE SYSTEM-CONFIG 22

6.4. CONFIGURE PHYSICAL INTERFACE VALUES 23

6.5. CONFIGURE NETWORK INTERFACE VALUES 24

6.6. ENABLE MEDIA MANAGER 26

6.7. CONFIGURE REALMS 27

6.8. CONFIGURE SIP INTERFACES 29

6.9. CONFIGURE SESSION-AGENT 31

6.10. CONFIGURE LOCAL-POLICY 33

6.11. CONFIGURE STEERING-POOL 35

6.12. CONFIGURE PING RESPONSE 36

6.13. SBC CONFIG FOR CISCO OFFER LESS INVITE 37

6.14. CONFIGURE TRANSLATION RULES 39

6.15. CONFIGURE SESSION TRANSLATION RULES 40

7. SBC CONFIGURATION FOR CISCO REMOTE WORKER 42

7.1. CONFIGURE REALMS 42

7.2. ENABLE SIP-CONFIG 44

7.3. ENABLE MEDIA MANAGER 46

7.4. CONFIGURE SIP INTERFACES 47

7.5. CONFIGURE STEERING-POOL 49

7.6. CONFIGURE LOCAL POLICY (OPTIONAL) 50

8. NEW SBC CONFIG/DEPLOYMENT USING CONFIGURATION ASSISTANT 51

8.1. SECTION OVERVIEW AND REQUIREMENTS 51

8.2. INITIAL GUI ACCESS 51

8.3. CONFIGURATION ASSISTANT TEMPLATE NAVIGATION 54

8.3.1. PAGE 1-CISCO CALL MANAGER (CUCM) NETWORK 54

8.3.2. PAGE 2-OFFERLESS SDP INVITE 54

8.3.3. PAGE 3 - CISCO SIDE TRANSCODING 55

8.3.4. PAGE 4 - CISCO SIDE ADDITIONAL CONFIGURATION 56
8.3.5. PAGE 5 - GENERIC SIP TRUNK NETWORK 56
8.3.6. PAGE 6 – PSTN SESSION AGENT 57
8.3.7. PAGE 7 – PSTN SIDE TRANSCODING 57
8.3.8. PAGE 8 – PSTN SIDE ADDITIONAL CONFIGURATION 58
8.4. REVIEW 59
8.5. DOWNLOAD AND/OR APPLY 60
8.6. CONFIGURATION ASSISTANT ACCESS 61
9. EXISTING SBC CONFIGURATION 61
APPENDIX A 62

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 Call Manager (Cisco CUCM).

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Generic Sip Trunk with on premises Cisco CUCM. The solution contained within this document has been tested using Oracle Communication SBC with **OS900p2**

Please find the related documentation links below:

2.1. Cisco Call Manager (Cisco CUCM)

Cisco Unified Call Manager provides industry-leading reliability, security, scalability, efficiency, and enterprise call and session management and is the core call control application of the collaboration portfolio.

It should be noted that while this application note focuses on the optimal configurations for the Oracle SBC in an enterprise **Cisco CUCM 12.5** environment, the same SBC configuration model can also be used for other enterprise applications with a few tweaks to the configuration for required features.

In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the Cisco CUCM Server associated parameters. 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.

For additional information on **CUCM 12.5**, please visit

https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-version-12-5/index.html

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.
The customers can configure any publicly routable IPs for these sections as per their network architecture needs.

3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Cisco CUCM 12.5 version using Oracle Enterprise SBC. There will be steps that require navigating the CUCM 12.5 server configuration, Oracle SBC GUI interface, understanding 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.

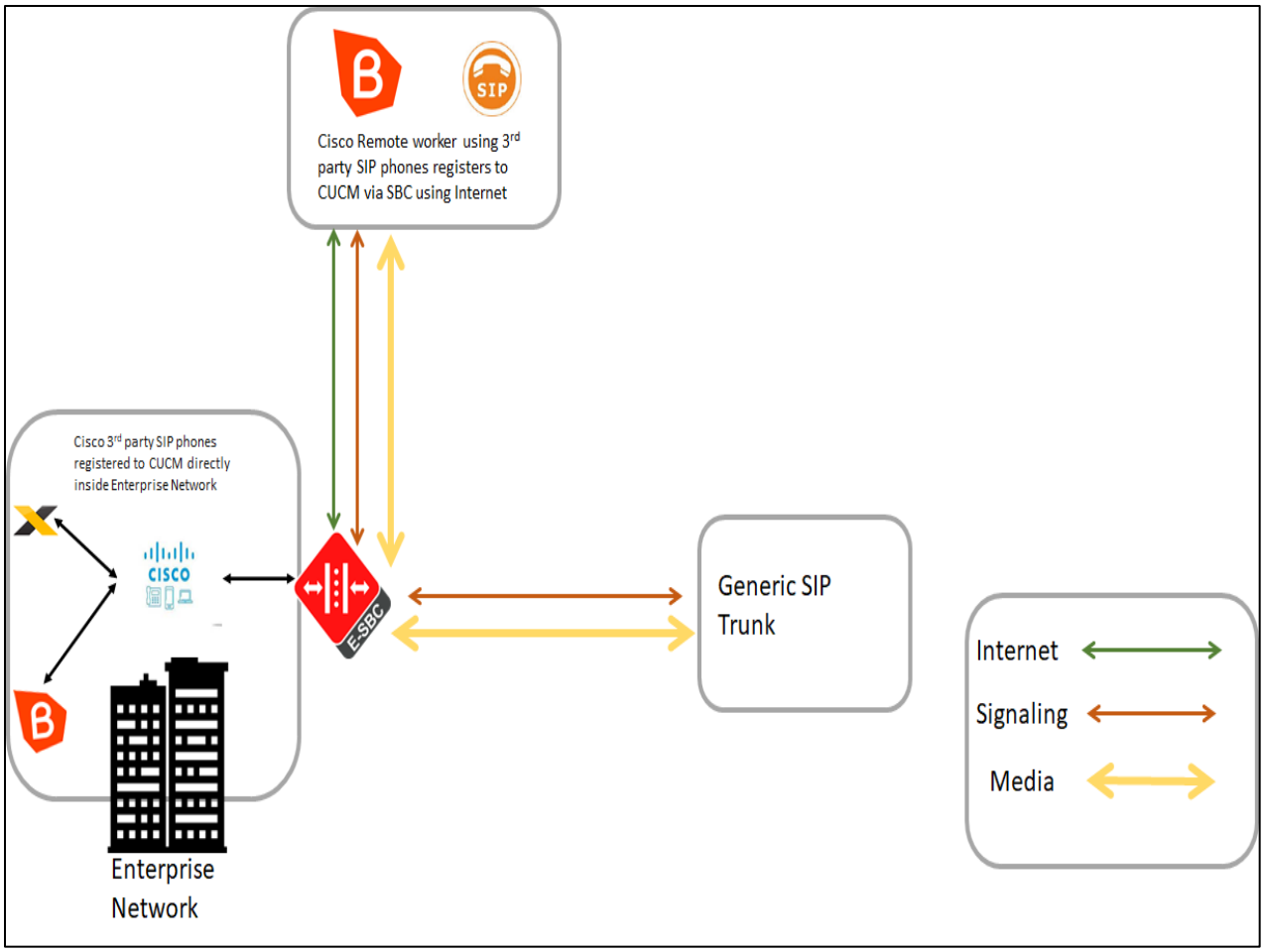
3.2. Requirements

- Fully functioning Cisco CUCM 12.5 version
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 9.0.0 version

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

Software Used	SBC Version	Cisco CUCM Version
Revision 1	9.0.0	12.5

3.3. Architecture

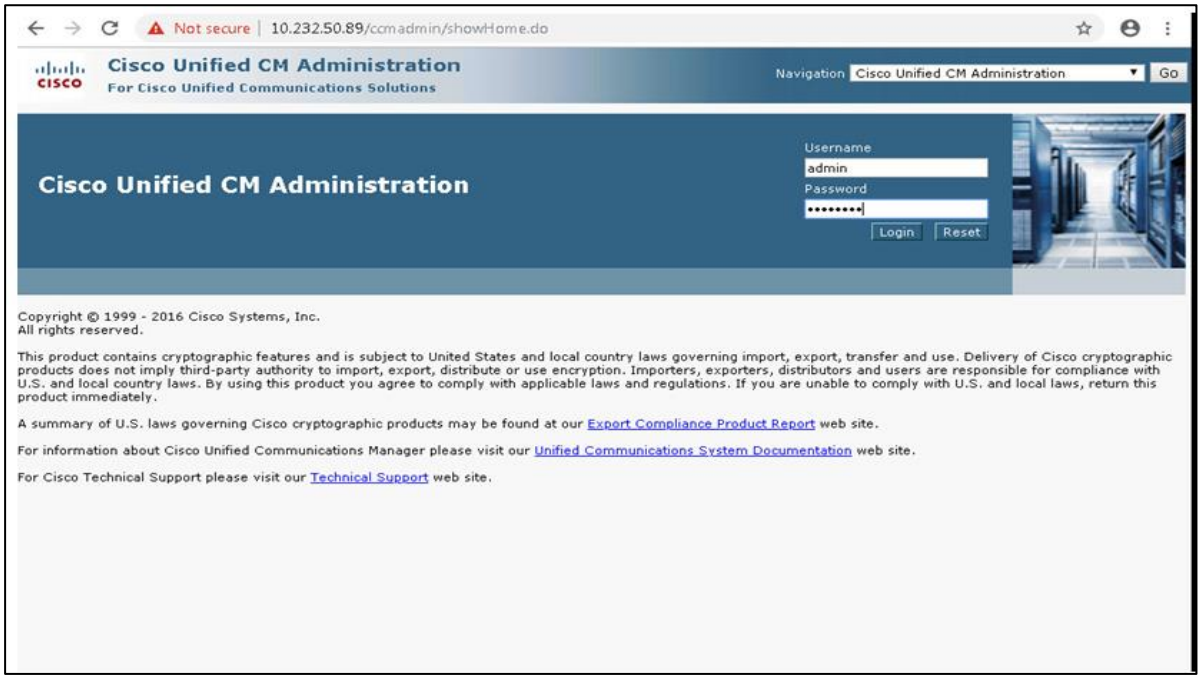


The configuration, validation and troubleshooting are the focuses of this document and will be described in two phases:

- Phase 1 – Configuring the Cisco Unified Call Manager v12.5 for Oracle SBC.
- Phase 2 – Configuring the Oracle SBC.

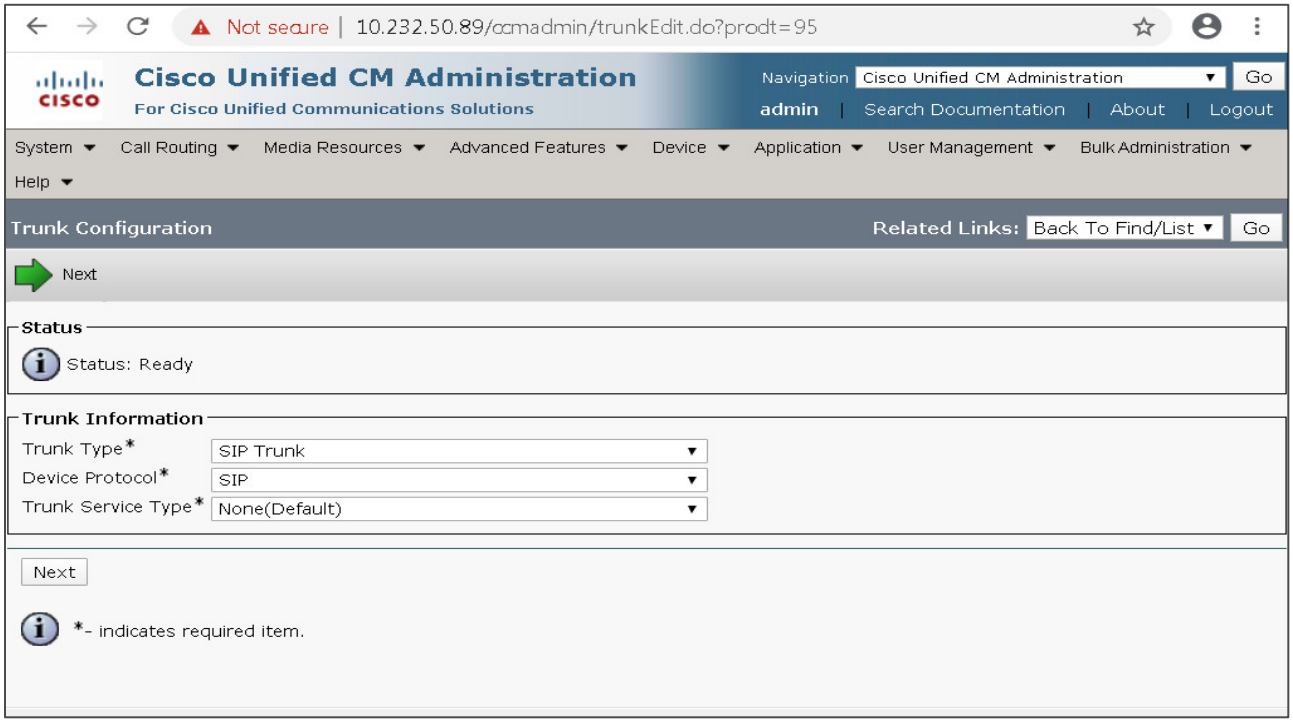
4. Configuring the Cisco Call Manager (Cisco CUCM)

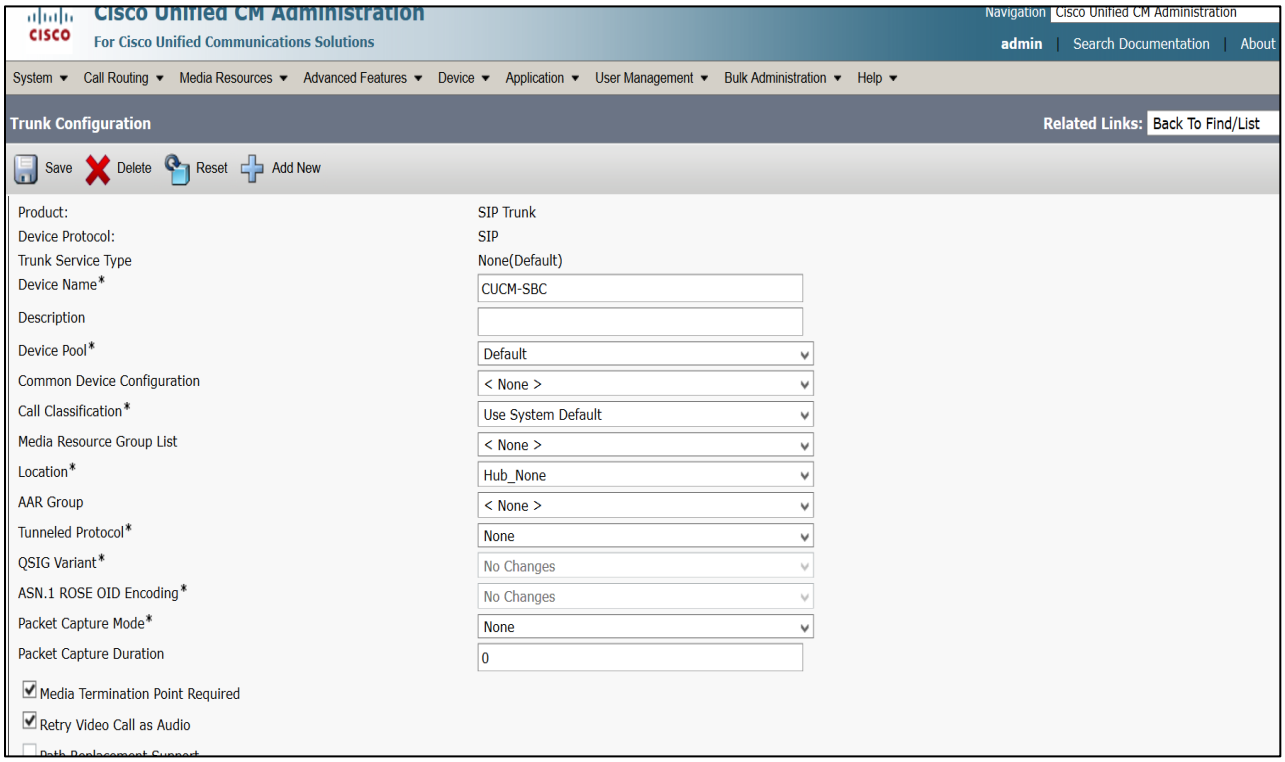
Please login to Cisco CUCM admin web GUI with proper login credentials (Username and password). After that, perform the steps below in the given order.

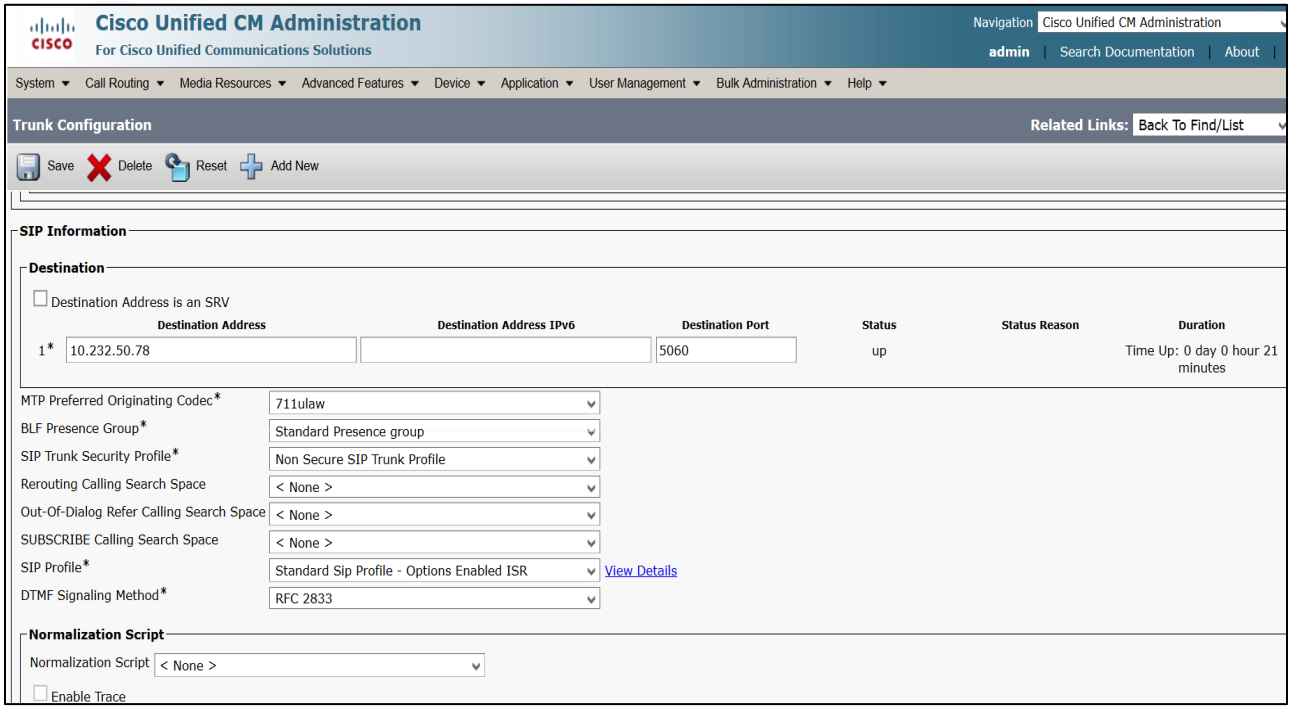


4.1. Configuring a new SIP Trunk

01) Go to Device ----- Trunk ----- Add New
02) Select Trunk Type – SIP Trunk and then Click Next
03) In the Device Name field, enter the SIP Trunk name and optionally provide a description.
04) In the Device Pool drop-down list, select a device pool id created already else select Default
05) Enter the Destination Address and Destination Port of the SBC under SIP Information.
06) Select appropriate SIP profile and SIP trunk security profile from the dropdown menu.
07) Click Save

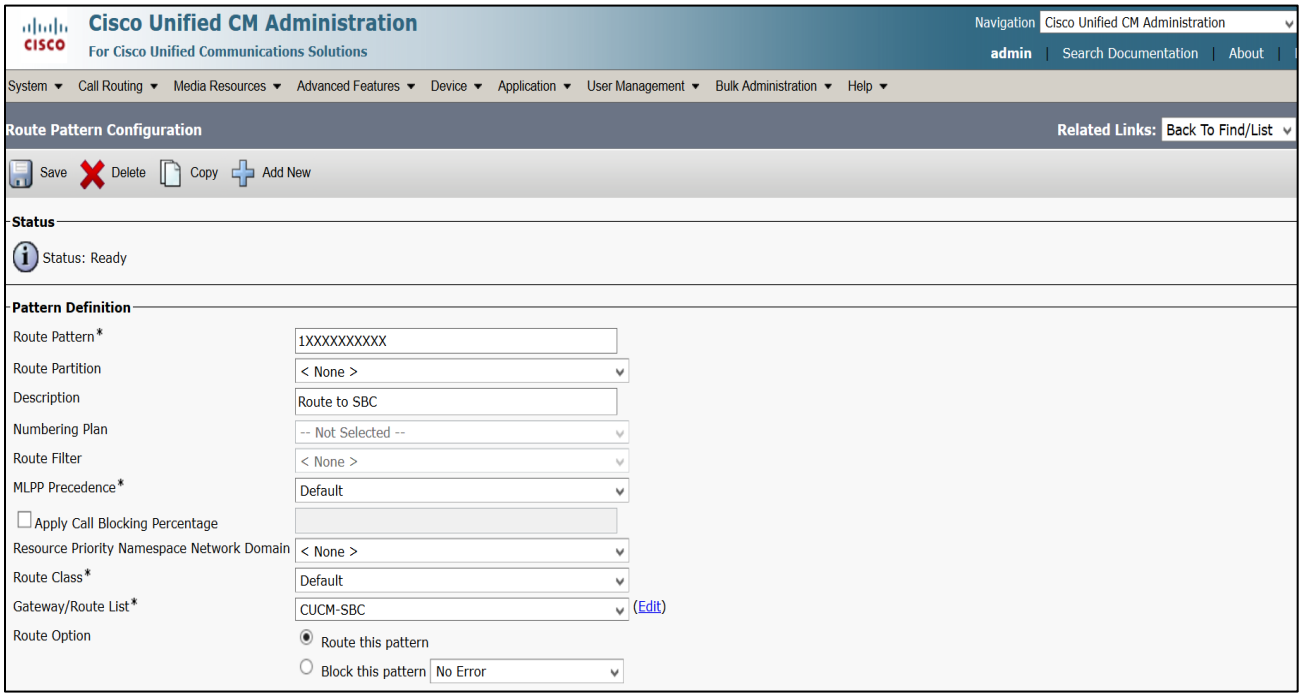

Not secure | 10.232.50.89/ccmadmin/trunkEdit.do?prodt=95
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Trunk Configuration
Related Links: Back To Find/List Go
Next
Status
Status: Ready
Trunk Information
Trunk Type* SIP Trunk
Device Protocol* SIP
Trunk Service Type* None(Default)
Next
*- indicates required item.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
admin | Search Documentation | About
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Trunk Configuration
Related Links: Back To Find/List
Save Delete Reset Add New
Product: SIP Trunk
Device Protocol: SIP
Trunk Service Type None(Default)
Device Name* CUCM-SBC
Description
Device Pool* Default
Common Device Configuration < None >
Call Classification* Use System Default
Media Resource Group List < None >
Location* Hub_None
AAR Group < None >
Tunneled Protocol* None
QSIG Variant* No Changes
ASN.1 ROSE OID Encoding* No Changes
Packet Capture Mode* None
Packet Capture Duration 0
Media Termination Point Required
Retry Video Call as Audio

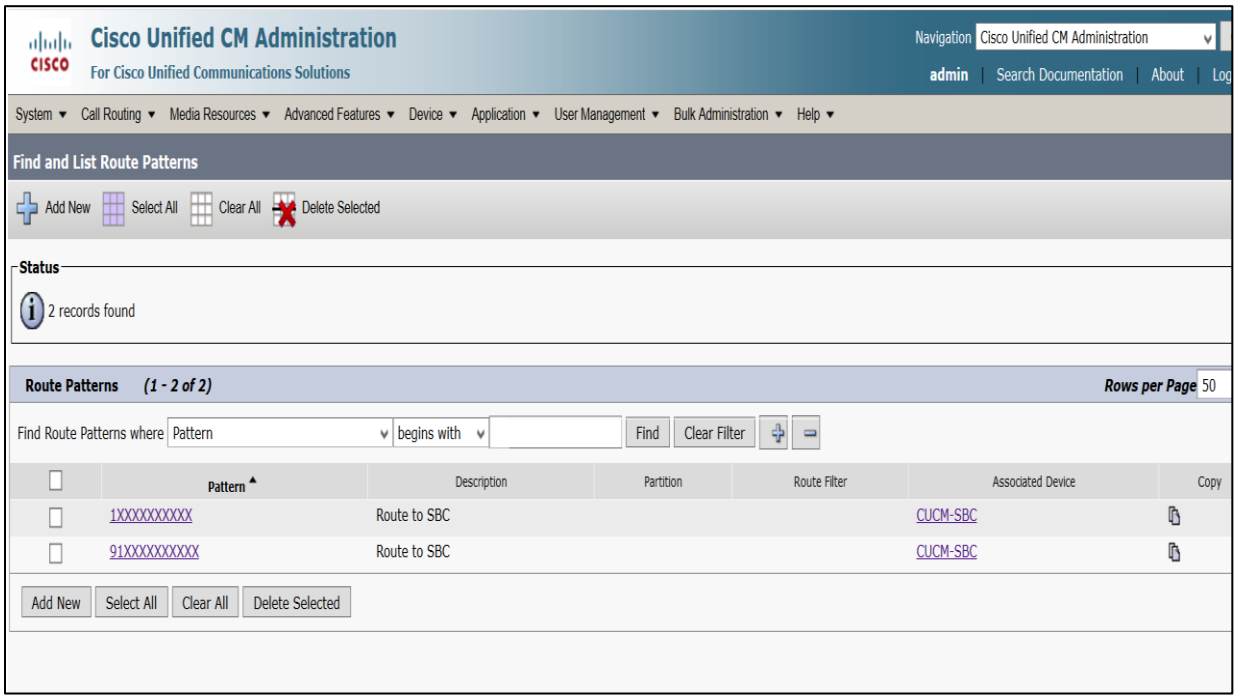


4.2. Configure a new Route Pattern

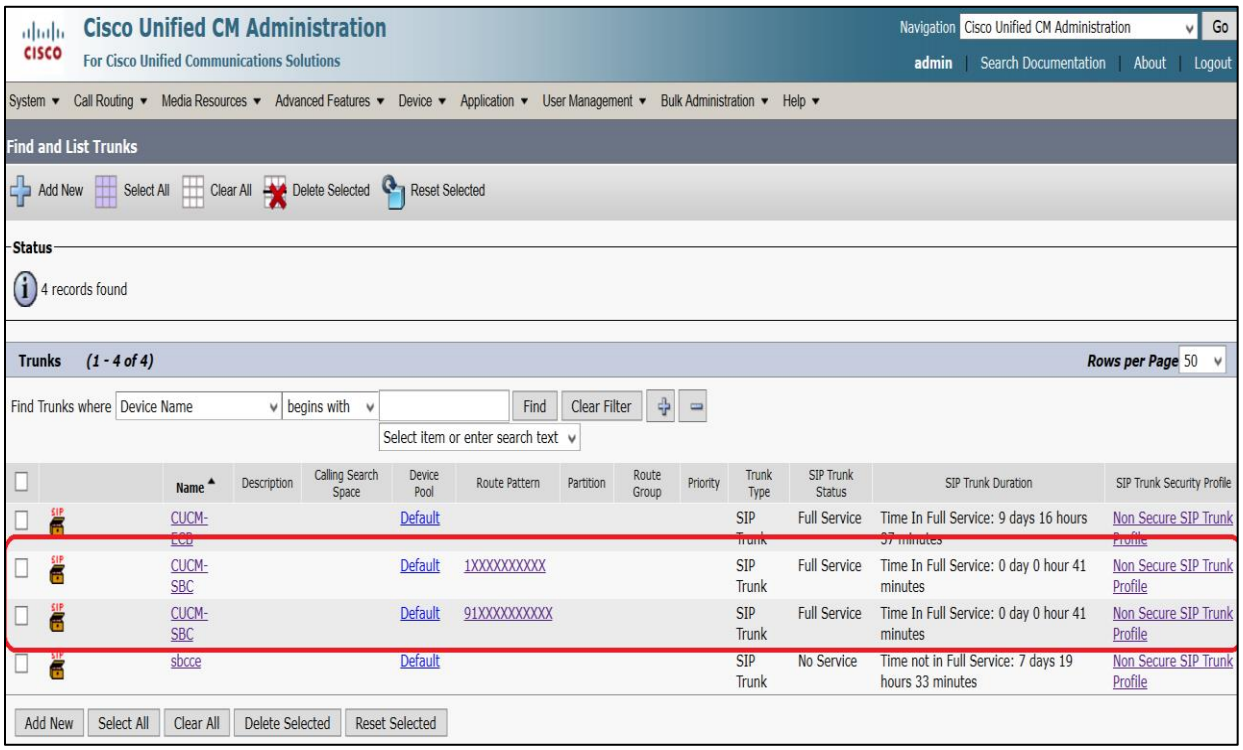
01) Go to Call Routing ------ Route/Hunt ------ Route Pattern and click Add New
02) Enter a Route Pattern according to the network requirements and calling plan.
03) From the Gateway/Route List drop-down list, select the created SIP Trunk device name.
04) Click Save. We can create other route patterns in the same way as shown below.



The route patterns that has been created is shown below:

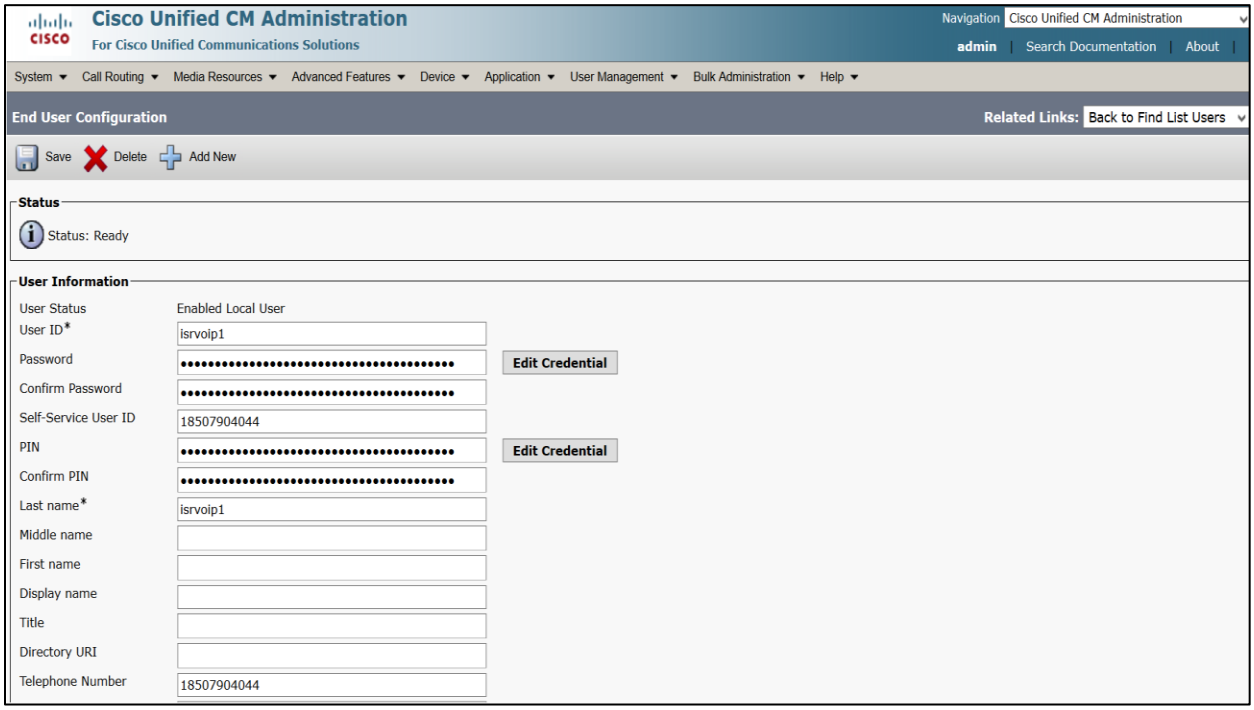


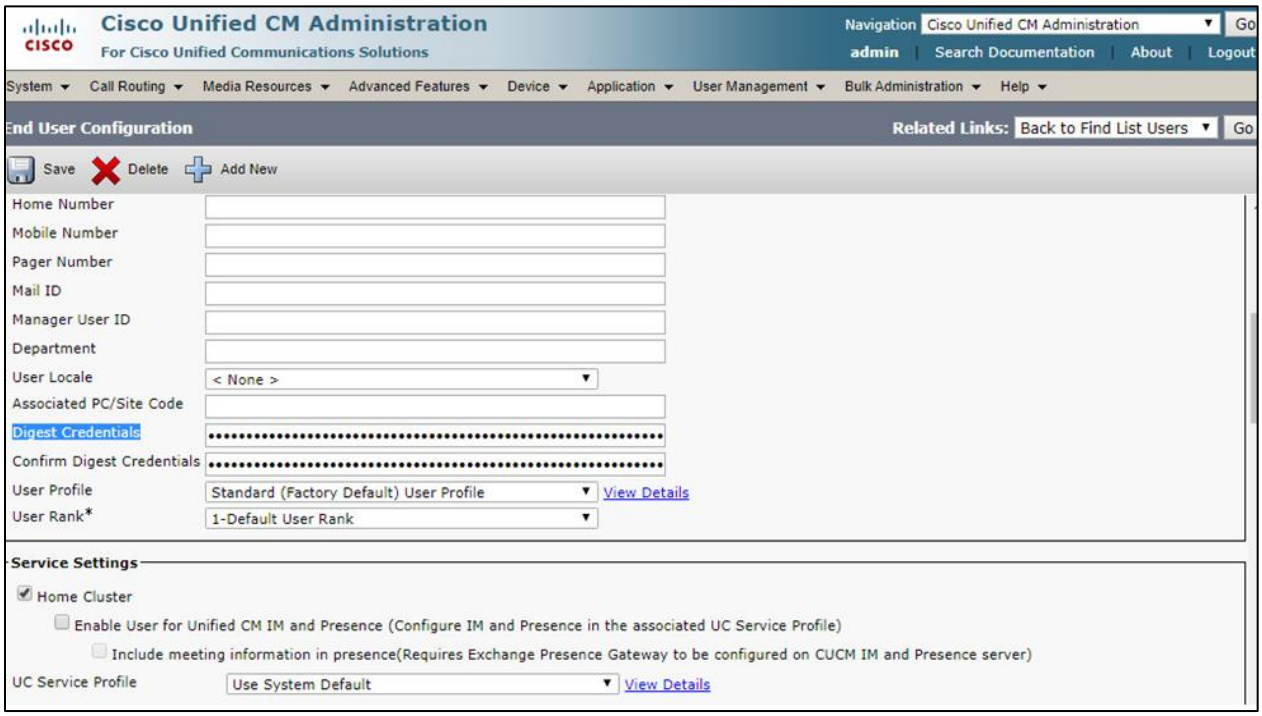
The created SIP trunk associated with the route pattern is shown below:



4.3. End User Configuration

01) Go to User Management ---- End User and click Add New
02) Enter in your User ID, password, pin, and Last Name
03) You must also enter in a password in the Digest Credentials and Confirm.
04) Click Save (remember the User ID and Password and DN of the device)

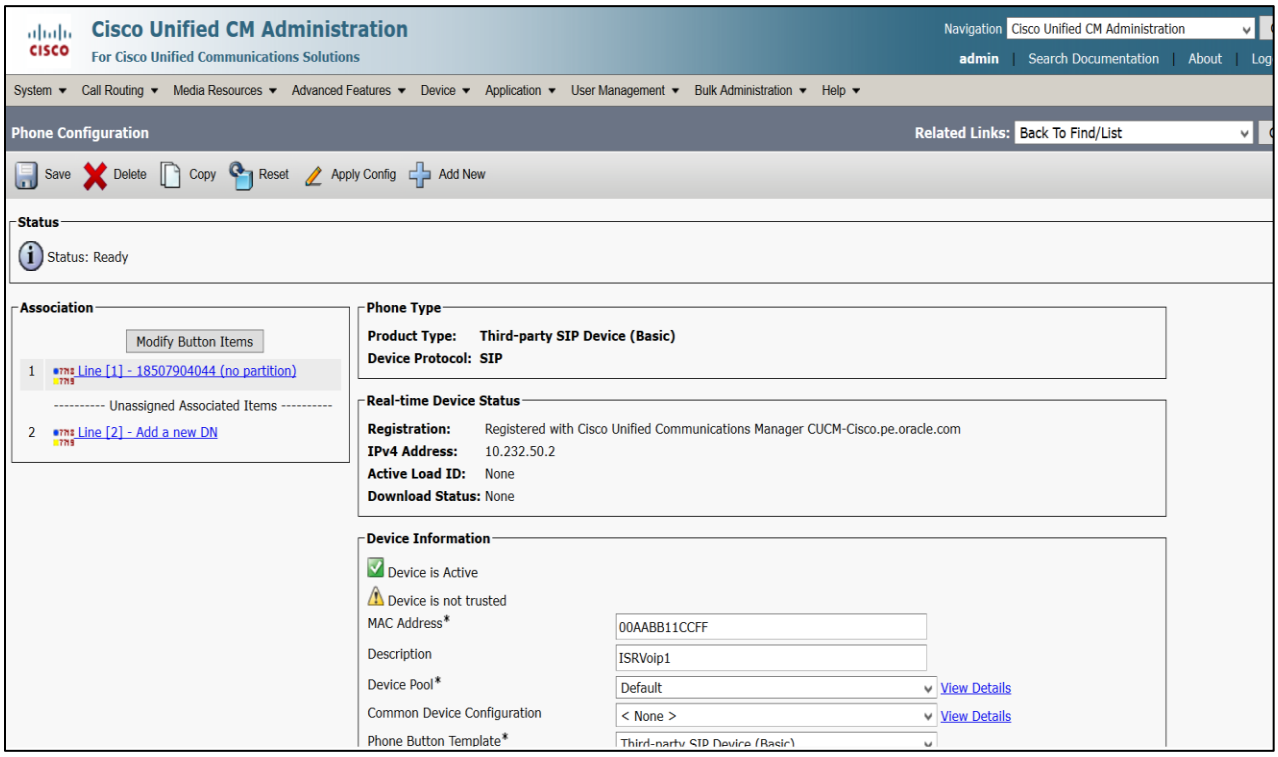


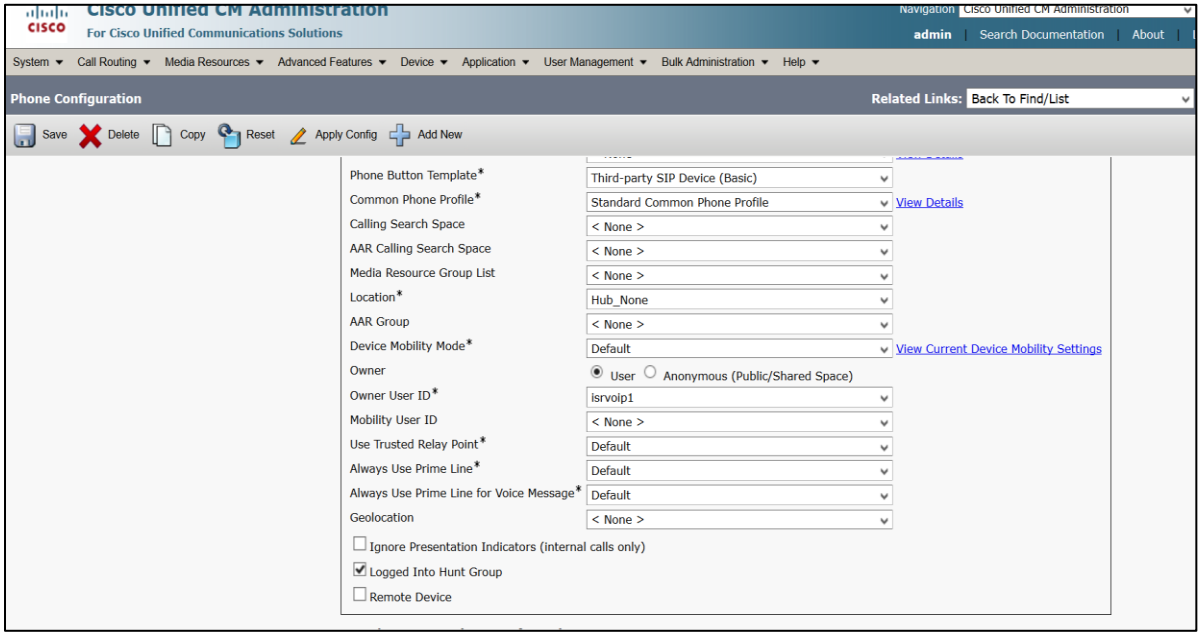


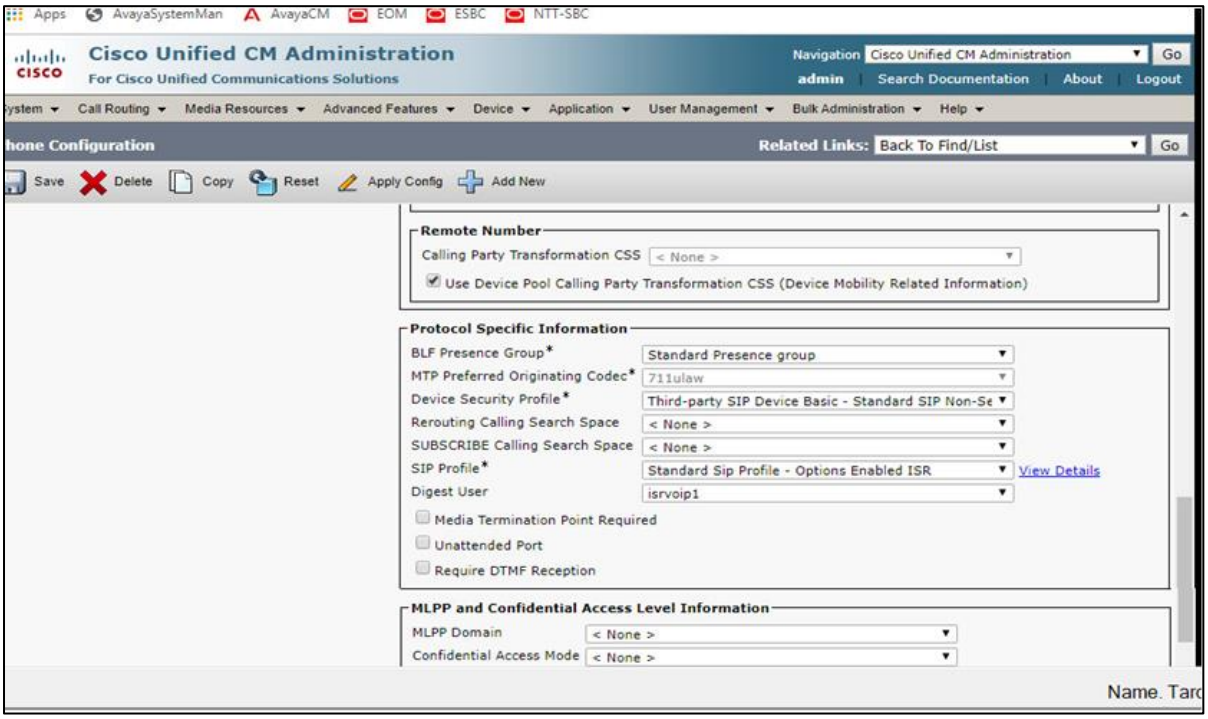
4.4. Adding SIP Phone in CUCM

01) Go to Device ---- Phone and click Add New
02) Select Third Party Sip Device (Basic) and click Next
03) Enter in a 12 digit MAC address (any dummy MAC address)
04) Enter the pertinent information for the SIP DEVICE settings – it should mostly be configured the same as a standard phone on your system except for the following settings
    a) in the owner user ID field select the user you created above
    b) in the Device Security Profile field select the security profile you created above
    c) in the Digest User field select the user you created above

05) Click Save.
06) Configure the line settings for the SIP device – the line settings should match the line settings of your standard user's Cisco IP phones
    There are no special attributes that we need to worry about on the line configuration.



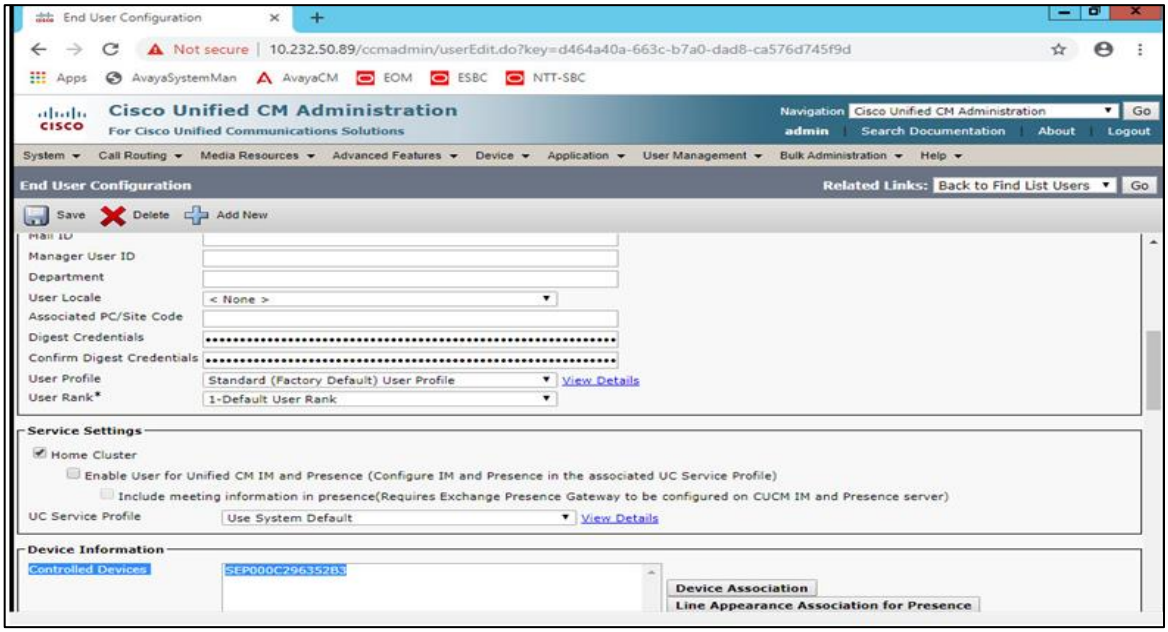

Cisco Unified CM Administration
For Cisco Unified Communications Solutions
admin | Search Documentation | About
System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help
Phone Configuration
Related Links: Back To Find/List
Save | Delete | Copy | Reset | Apply Config | Add New
Phone Button Template* Third-party SIP Device (Basic)
Common Phone Profile* Standard Common Phone Profile View Details
Calling Search Space < None >
AAR Calling Search Space < None >
Media Resource Group List < None >
Location* Hub_None
AAR Group < None >
Device Mobility Mode* Default View Current Device Mobility Settings
Owner User Anonymous (Public/Shared Space)
Owner User ID* isrvoip1
Mobility User ID < None >
Use Trusted Relay Point* Default
Always Use Prime Line* Default
Always Use Prime Line for Voice Message* Default
Geolocation < None >
Ignore Presentation Indicators (internal calls only)
Logged Into Hunt Group
Remote Device


Apps AvayaSystemMan AvayaCM EOM ESBC NTT-SBC
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help
hone Configuration
Related Links: Back To Find/List Go
Save | Delete | Copy | Reset | Apply Config | Add New
Remote Number
Calling Party Transformation CSS < None >
Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)
Protocol Specific Information
BLF Presence Group* Standard Presence group
MTP Preferred Originating Codec* 711ulaw
Device Security Profile* Third-party SIP Device Basic - Standard SIP Non-Se
Rerouting Calling Search Space < None >
SUBSCRIBE Calling Search Space < None >
SIP Profile* Standard Sip Profile - Options Enabled ISR View Details
Digest User isrvoip1
Media Termination Point Required
Unattended Port
Require DTMF Reception
MLPP and Confidential Access Level Information
MLPP Domain < None >
Confidential Access Mode < None >
Name. Tarc

4.5. Associating End User to Phone

01) Go to User Management ----- End Users and search for the sip user you created above, once you find it, click on it

02) Scroll down to Device Association and click on the Device Association button
03) Locate and select the sip device you created above
04) Check the checkbox next to this device and click Save Selected/Changes
05) Click Go next to the Back to User related link near the upper right-hand corner
06) Click Save one more time on the End User Configuration screen.



With these steps, the CUCM configuration is complete.

5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Cisco Call Manager (Cisco CUCM) and Generic SIP Trunk. If the Oracle SBC being deployed is new, with no existing configuration, the simplest way to configure it to interface with Cisco Call Manager (Cisco CUCM) is by utilizing the Configuration Assistant feature.

5.1. Validated Oracle SBC version

Oracle conducted tests with Oracle SBC 9.0 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

6. New SBC configuration

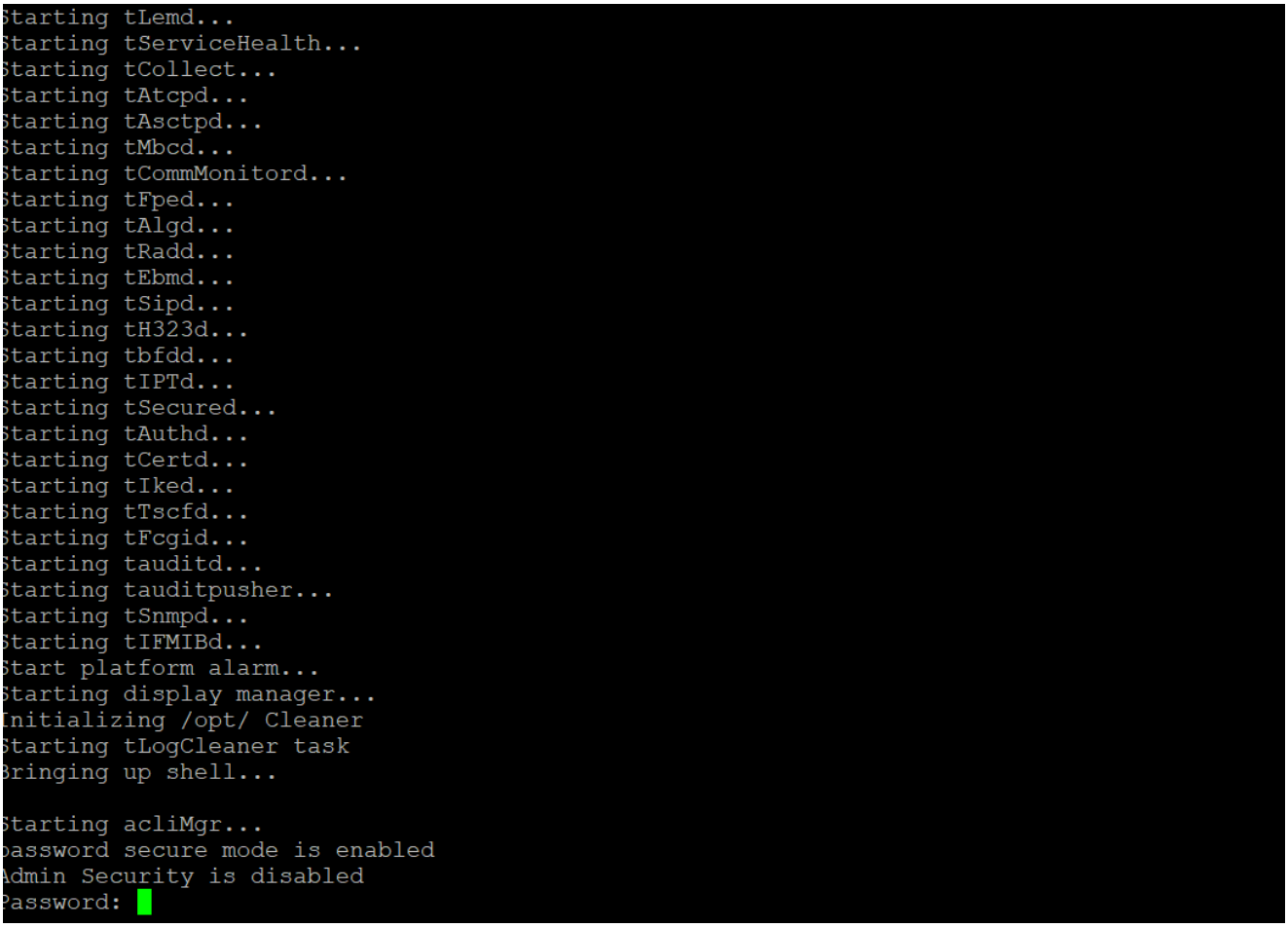
If the customer is looking to setup a new SBC from scratch, please follow the section below.

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. Start the terminal emulation application using the following settings:

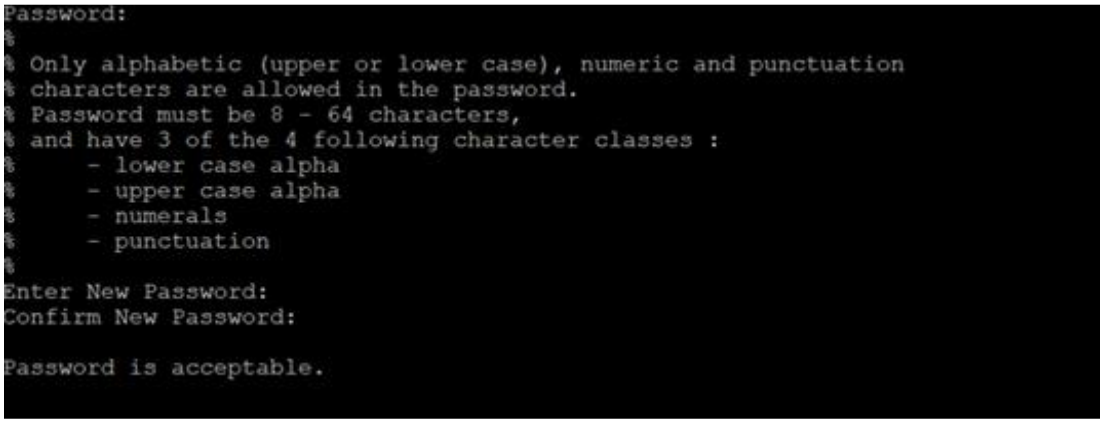
- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

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.

```
NN4600-139(configure)# bootparam

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

Boot File               : /boot/nnSCZ900p2.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             : NN4600-139
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: 30)

NN4600-139(configure)#
NN4600-139(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

```
NN3900-101# setup product

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

Last Modified 2020-07-21 04:51:24
------------------------------------------------------------
 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.

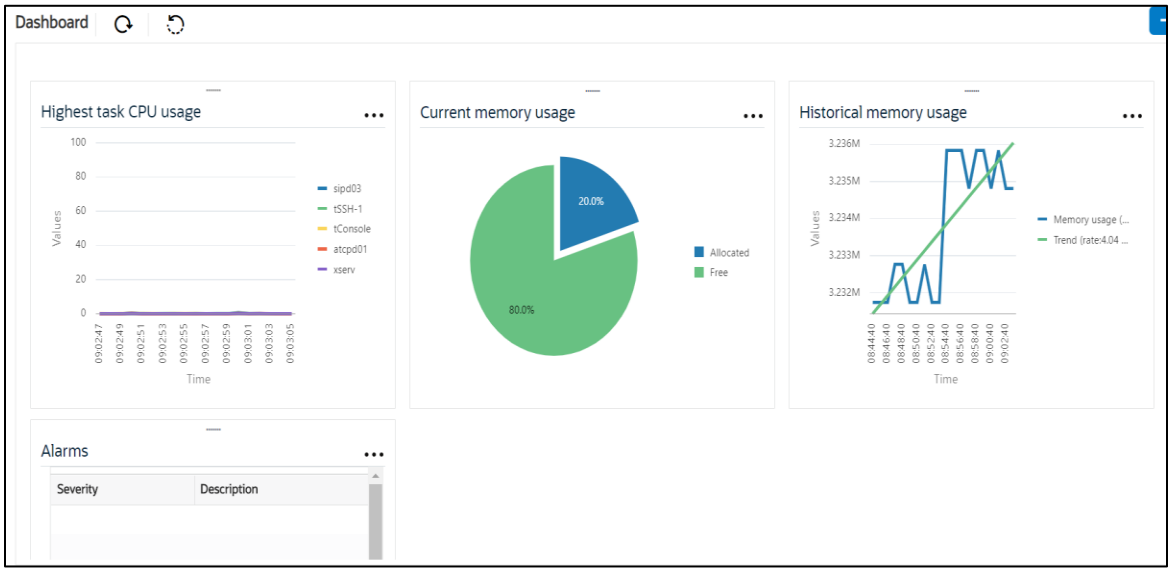
```
NN3900-101(http-server)# show
http-server
        name                                webServerInstance
        state                               enabled
        realm
        ip-address
        http-state                          enabled
        http-port                           80
        https-state                         disabled
        https-port                          443
        http-interface-list                 GUI
        http-file-upload-size               0
        tls-profile
        auth-profile
        last-modified-by                    @
        last-modified-date                  2020-10-06 00:28:26

NN3900-101(http-server)#
NN3900-101(http-server)#
```

6.2. Configure SBC using Web GUI

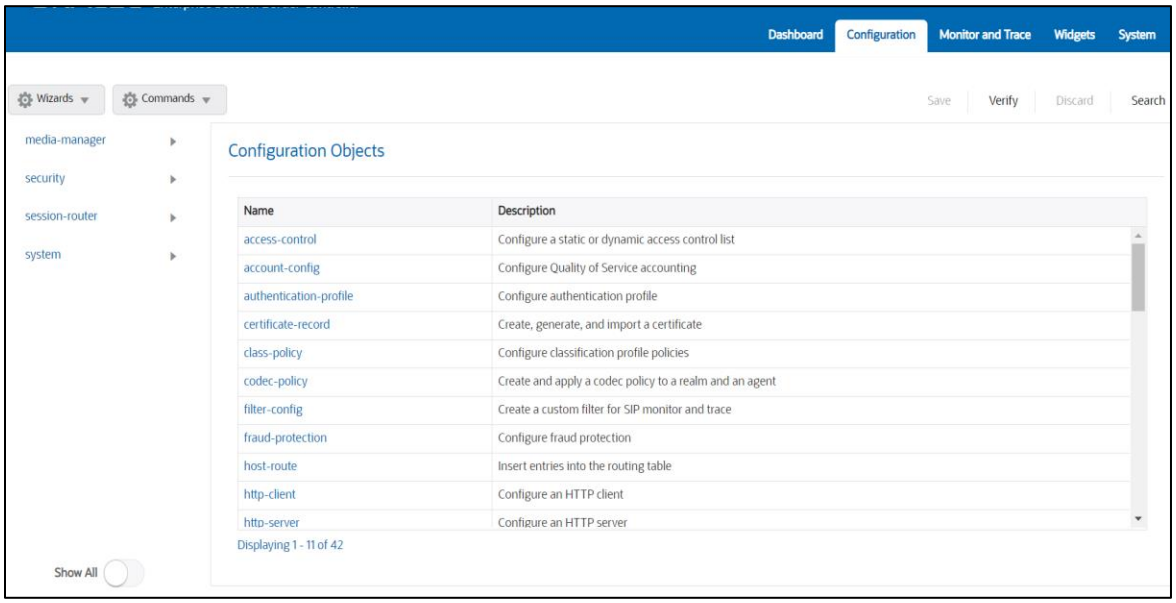
In this app note, we configure SBC using the WebGUI.

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

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



Go to Configuration as shown below, to configure the SBC



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

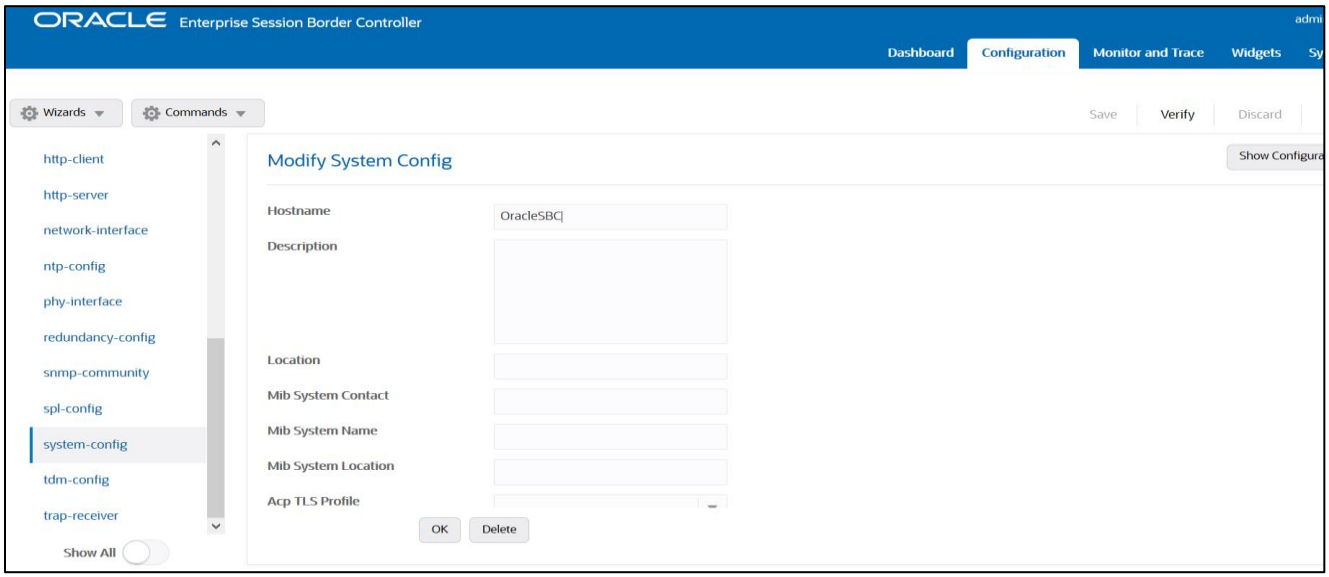
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.0.0/webgui/web-gui-guide.pdf

The expert mode is used for configuration.

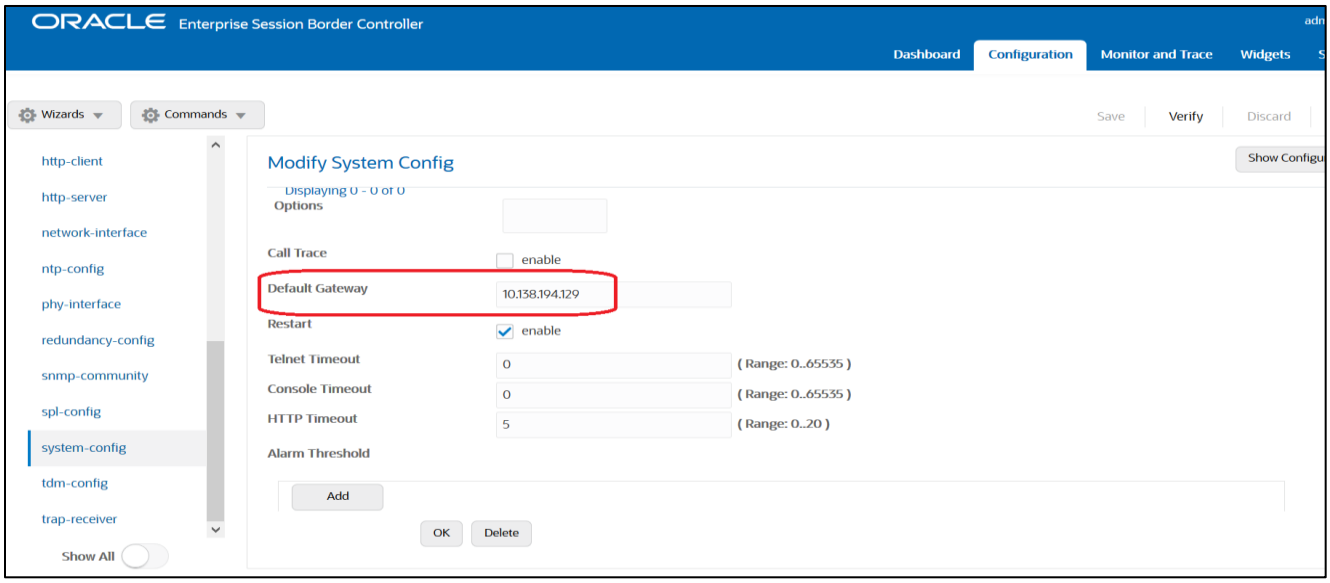
Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

6.3. Configure system-config

Go to system->system-config



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



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.

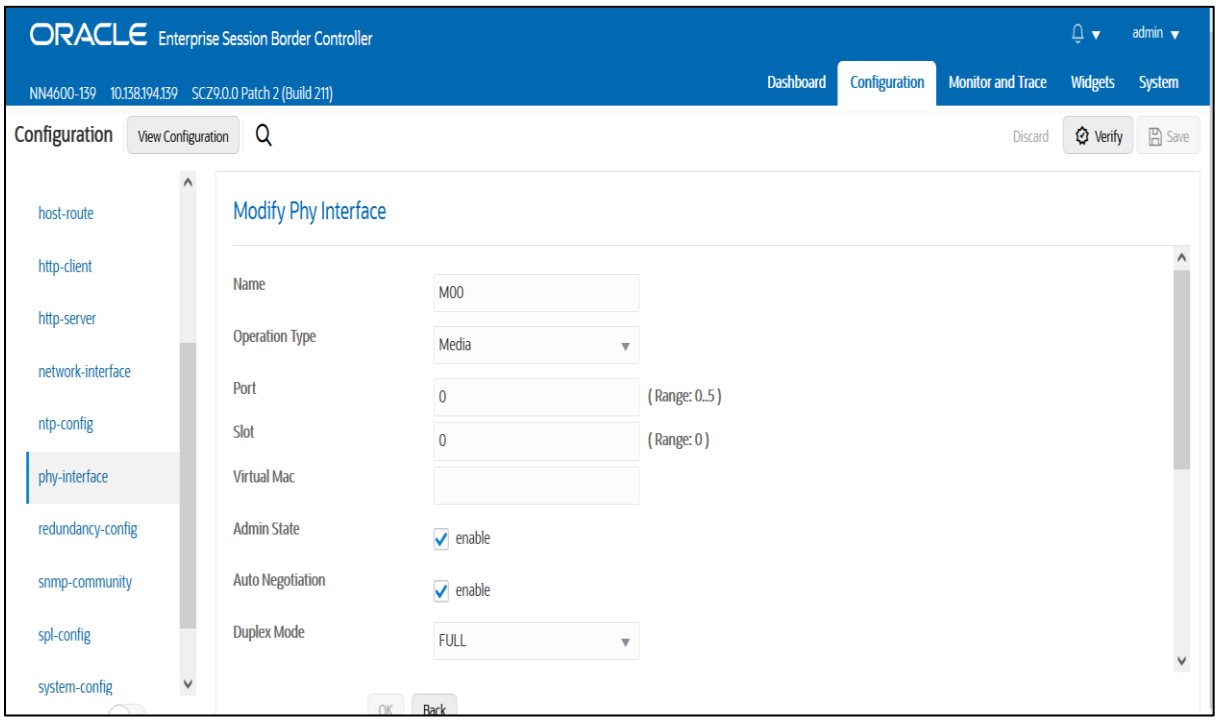
6.4. Configure Physical Interface values

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

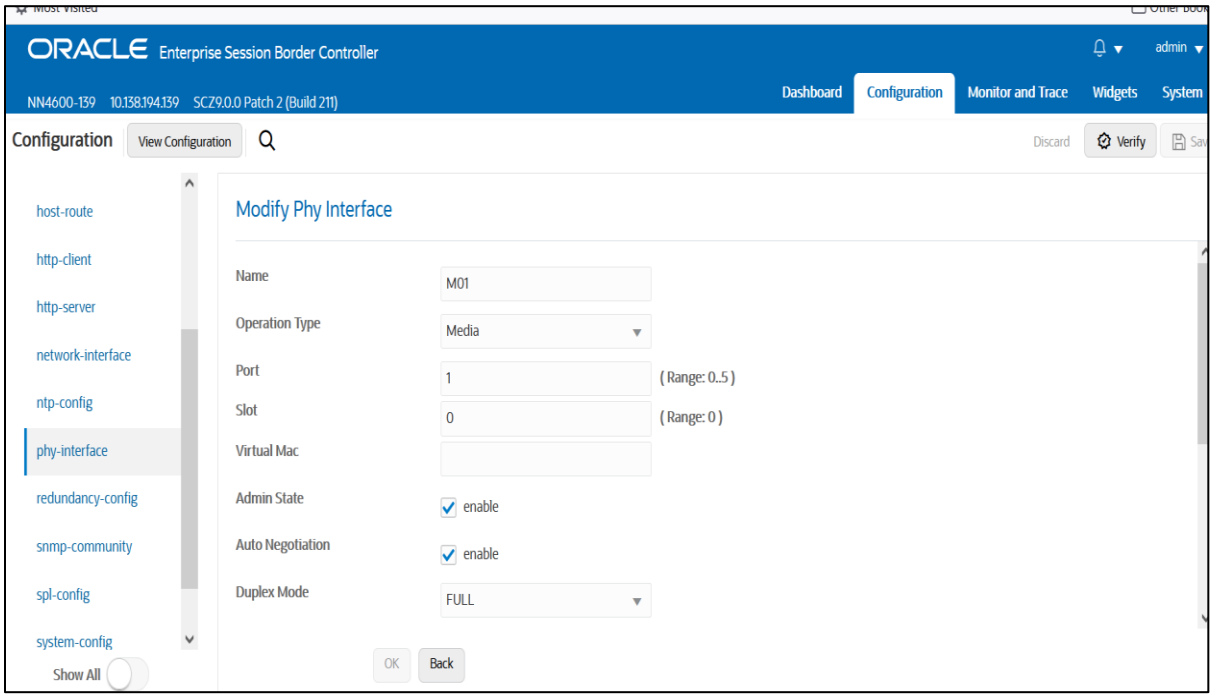
Please configure M10 for Generic Trunk side and M11 for Cisco side.

Parameter Name	Generic Sip Trunk side (M00)	Cisco side (M01)
Slot	0	1
Port	0	0
Operation Mode	Media	Media

Please configure M00 interface as below.



Please configure M01 interface as below



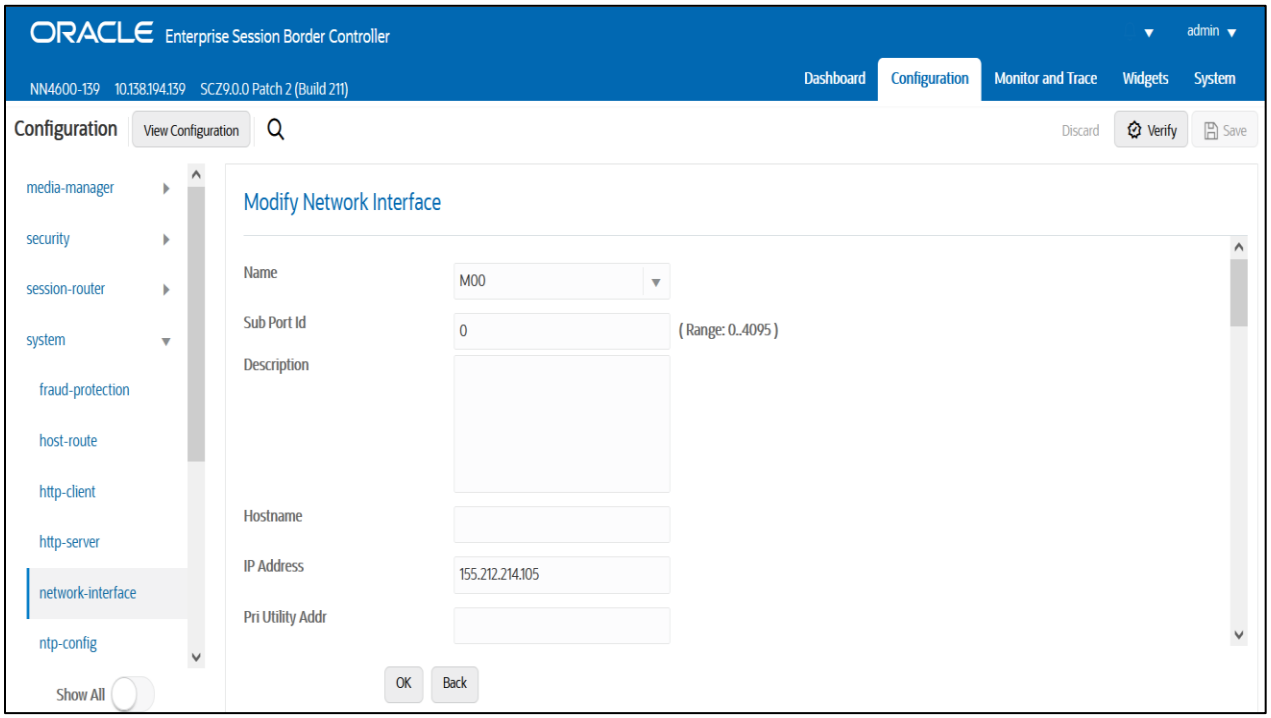
6.5. Configure Network Interface values

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

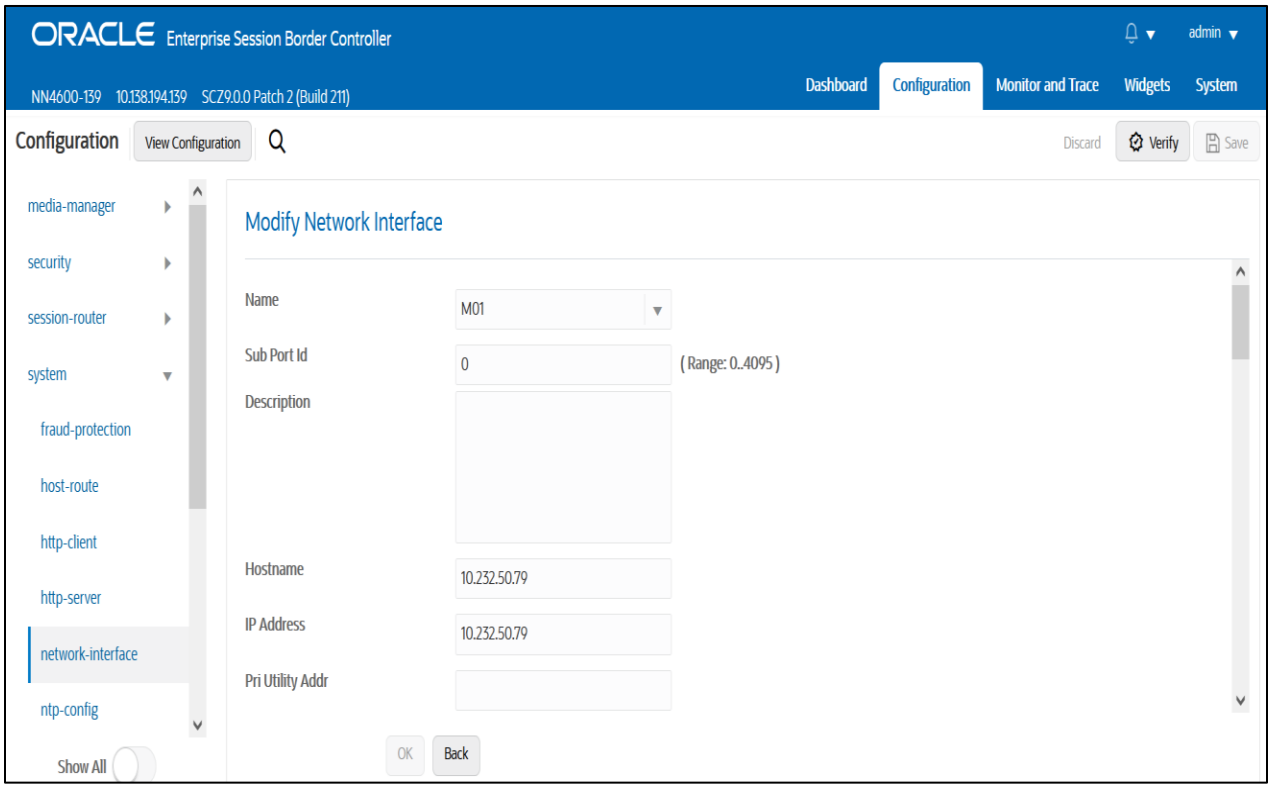
The table below lists the parameters, to be configured for both the interfaces.

Parameter Name	Generic Sip Trunk Side Network Interface(M00)	Cisco side Network Interface(M01)
Name	M00	M01
Host Name		
IP Address	155.212.214.105	10.232.50.79
Net Mask	255.255.255.0	255.255.255.0
Gateway	155.212.214.65	10.232.50.1

Please configure network interface M00 as below



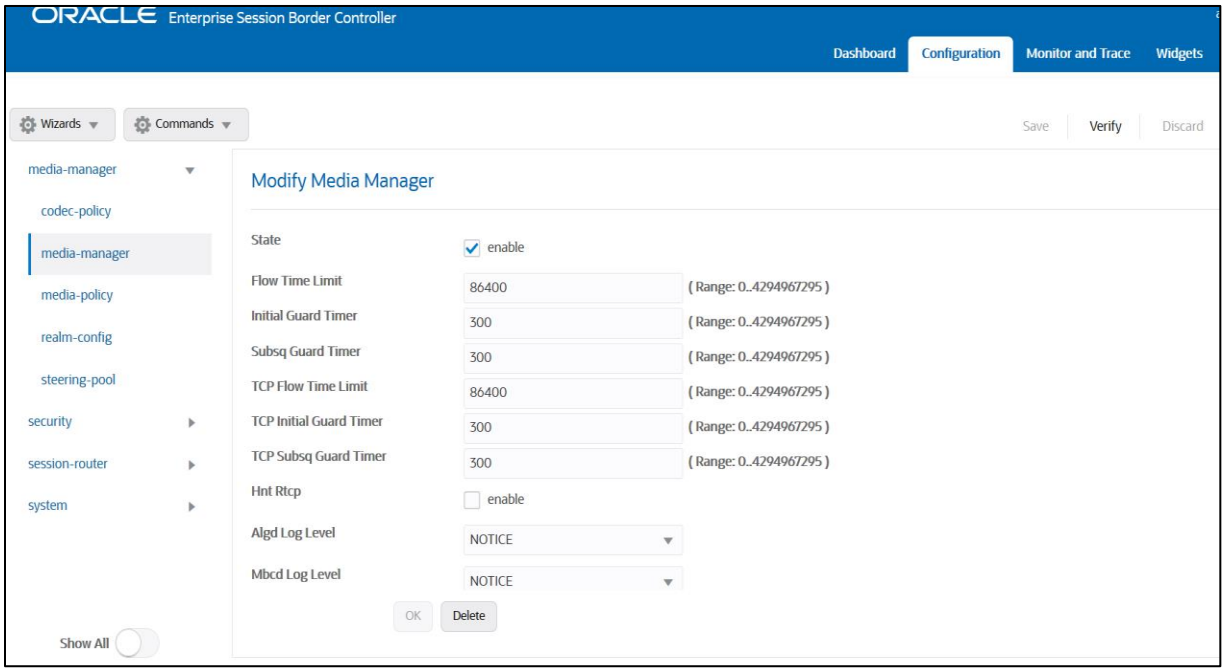
Similarly, configure network interface M01 as below

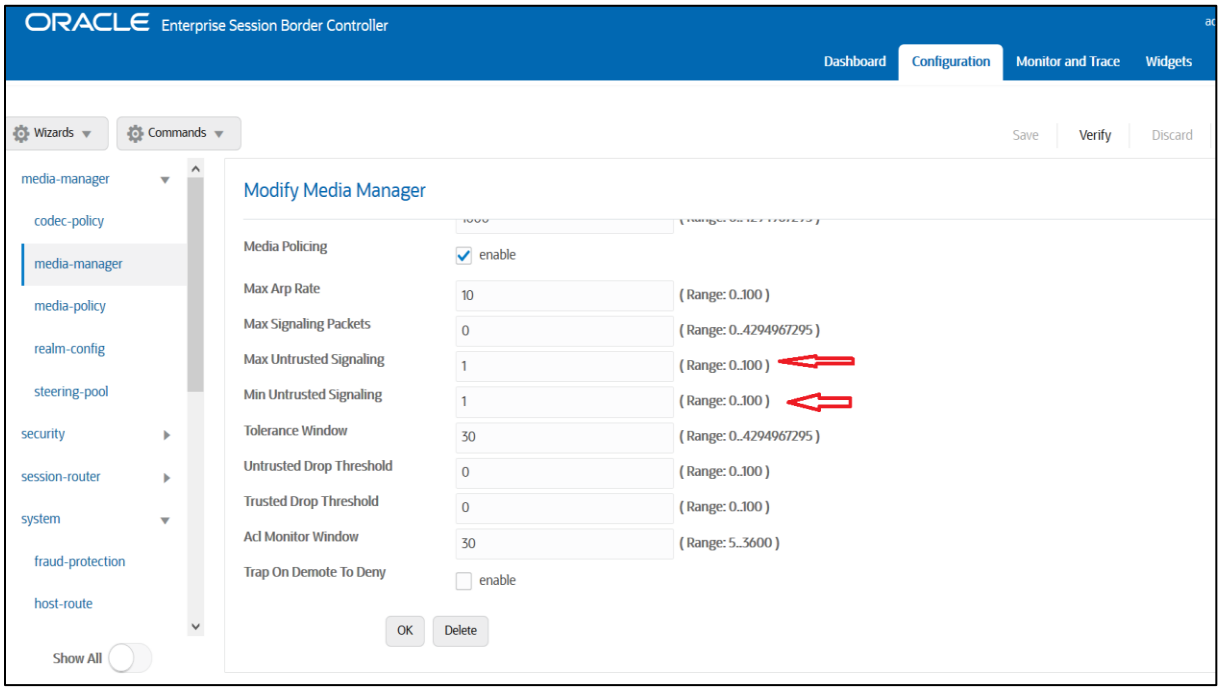


6.6. Enable media manager

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.
Go to Media-Manager->Media-Manager





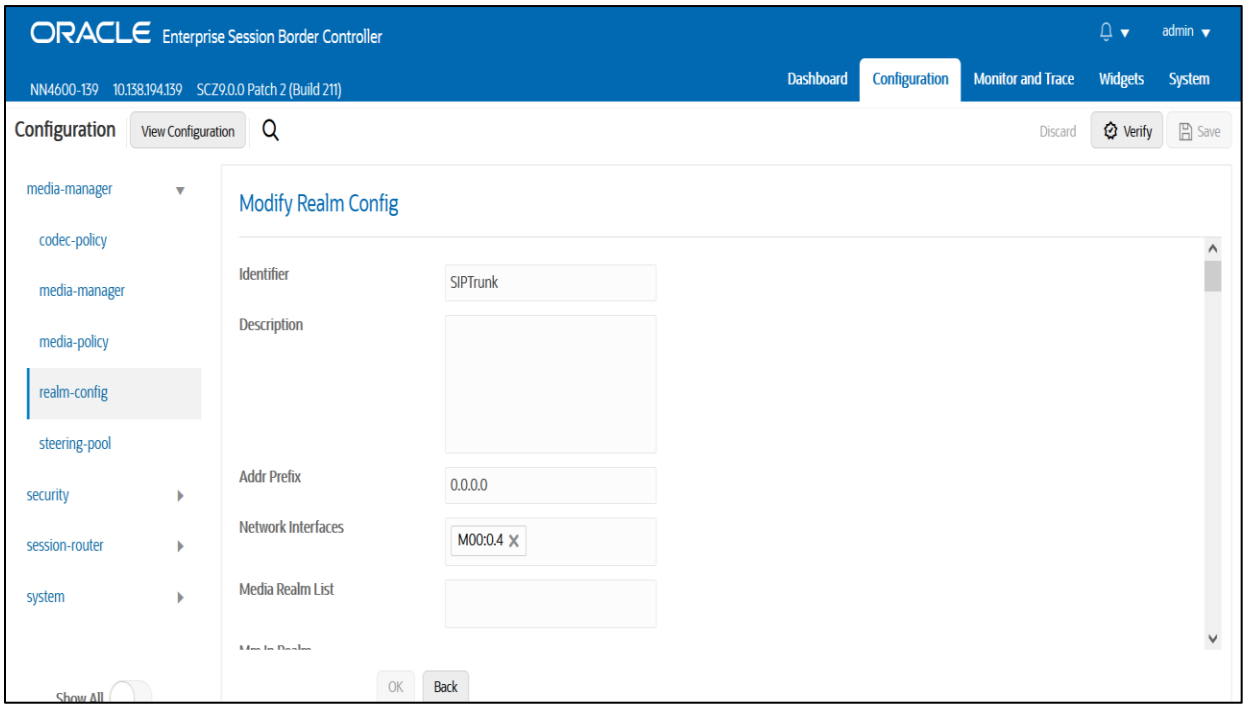
6.7. Configure Realms

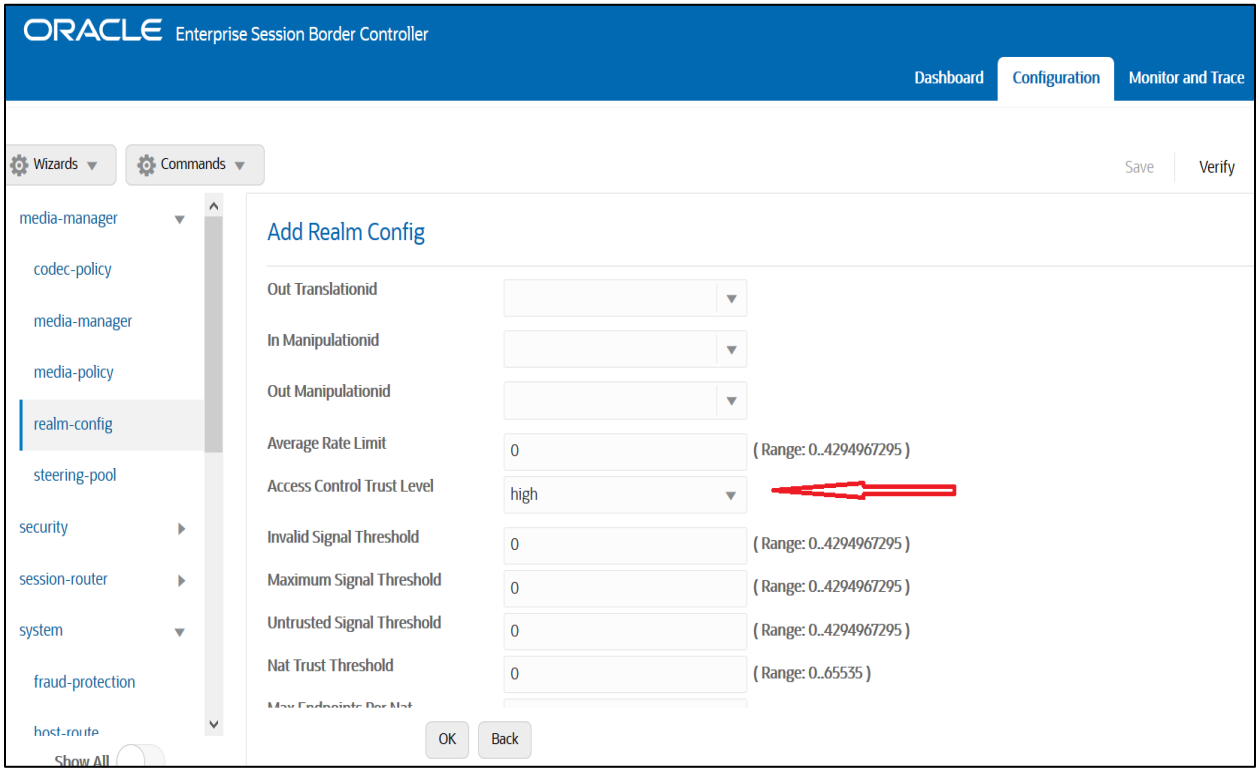
Navigate to realm-config under media-manager and configure a realm as shown below
The name of the Realm can be any relevant name according to the user convenience.

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

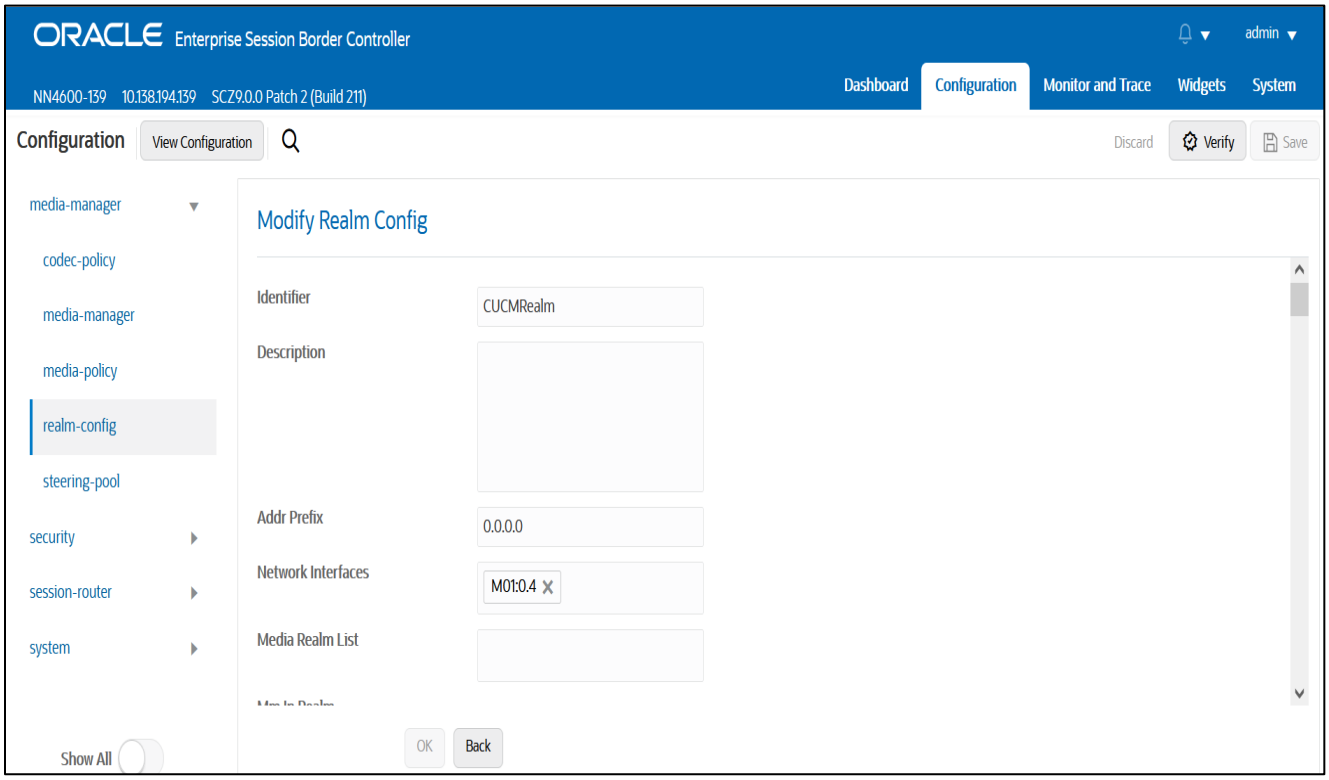
Config Parameter	Generic SIP Trunk	Cisco Side
Identifier	SIPTrunk	CUCMRealm
Network Interface	M00	M01
Mm in realm	☑	☑
FQDN		
Media Sec policy	RTP	RTP
Access Control Trust Level	High	High

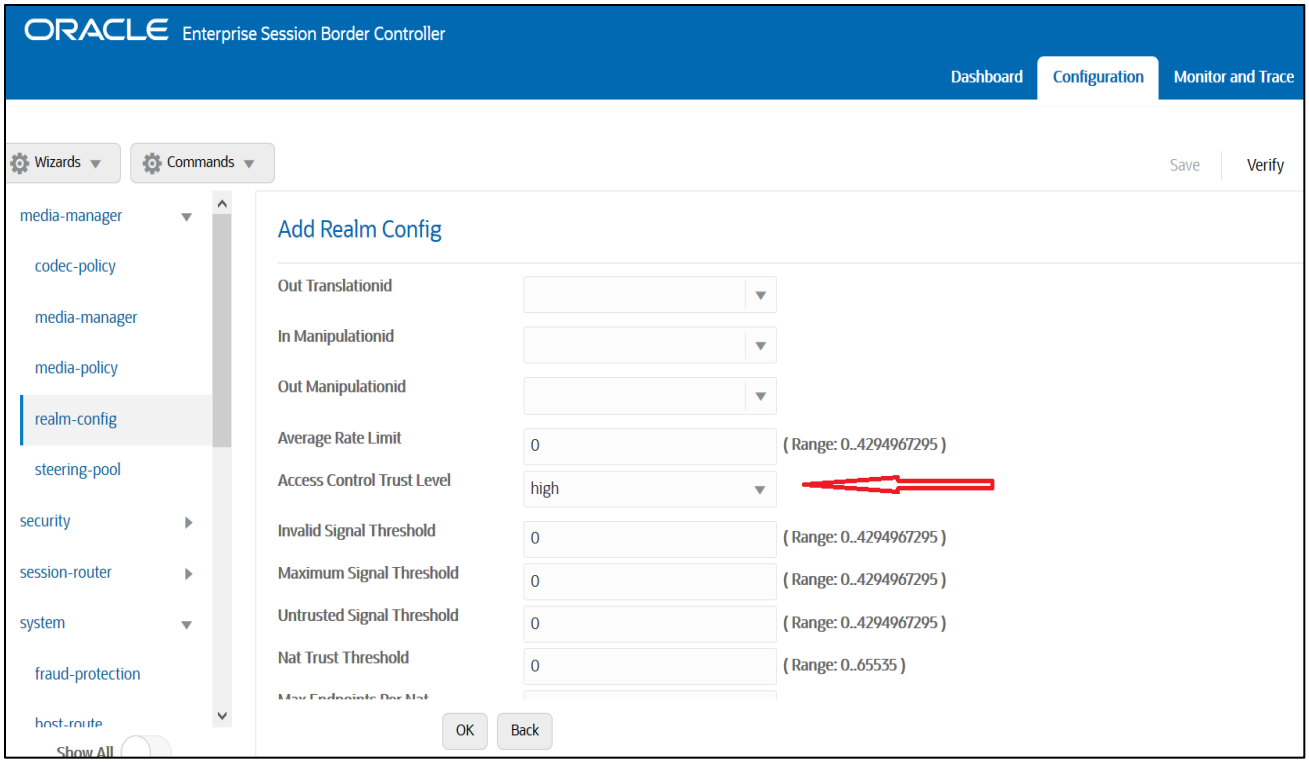
In the below case, Realm name is given as SIPTrunk for Generic SIP Trunk Side
Please set the Access Control Trust Level as high for this realm





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





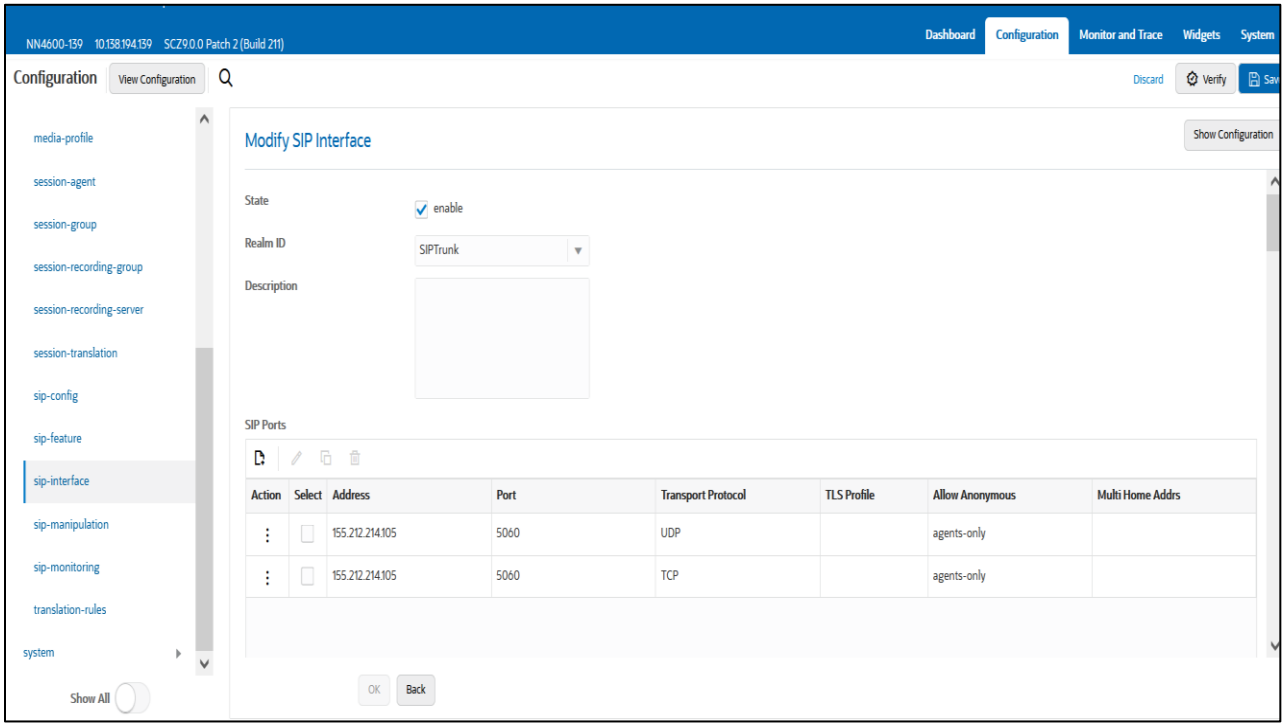
For more information on Access Control Trust Level, please refer to SBC Security guide link given below:

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

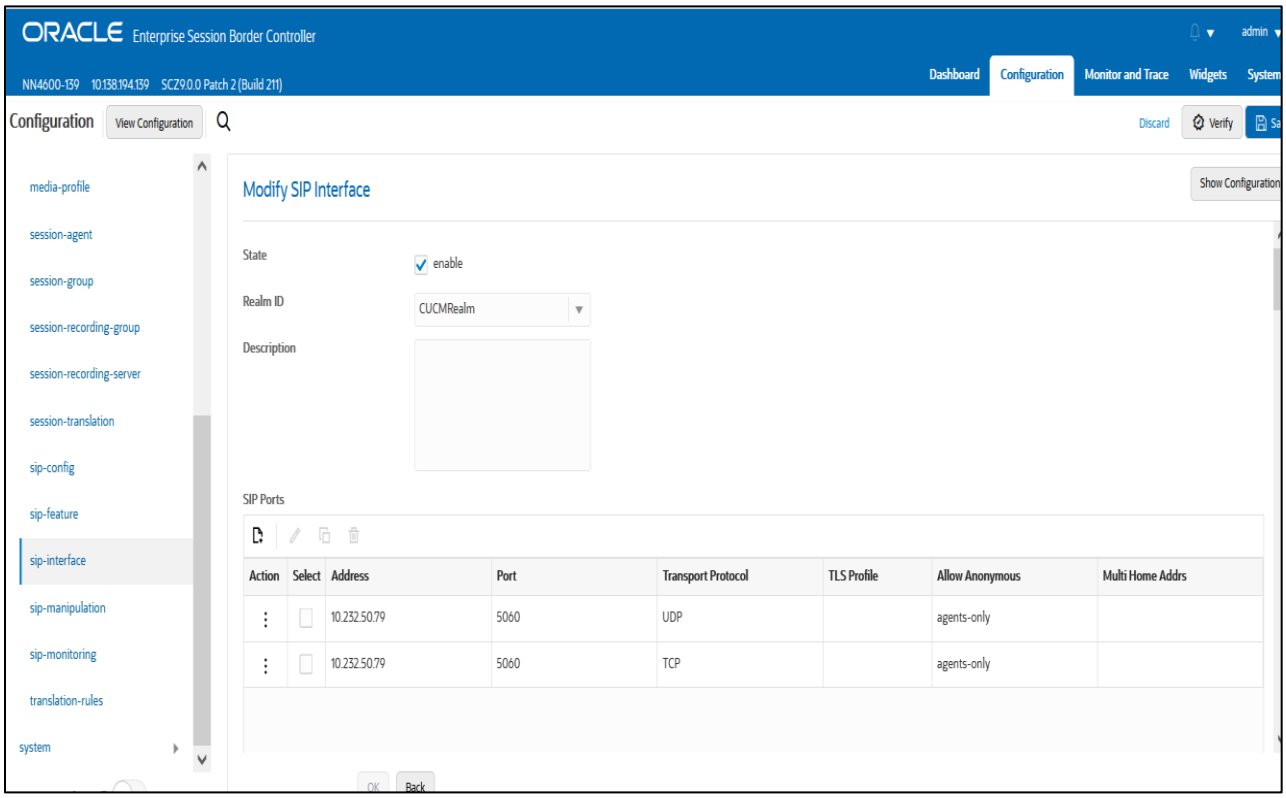
6.8. Configure SIP Interfaces

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 Generic SIP Trunk side as below.
Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from the particular Session agents added to the SBC.



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



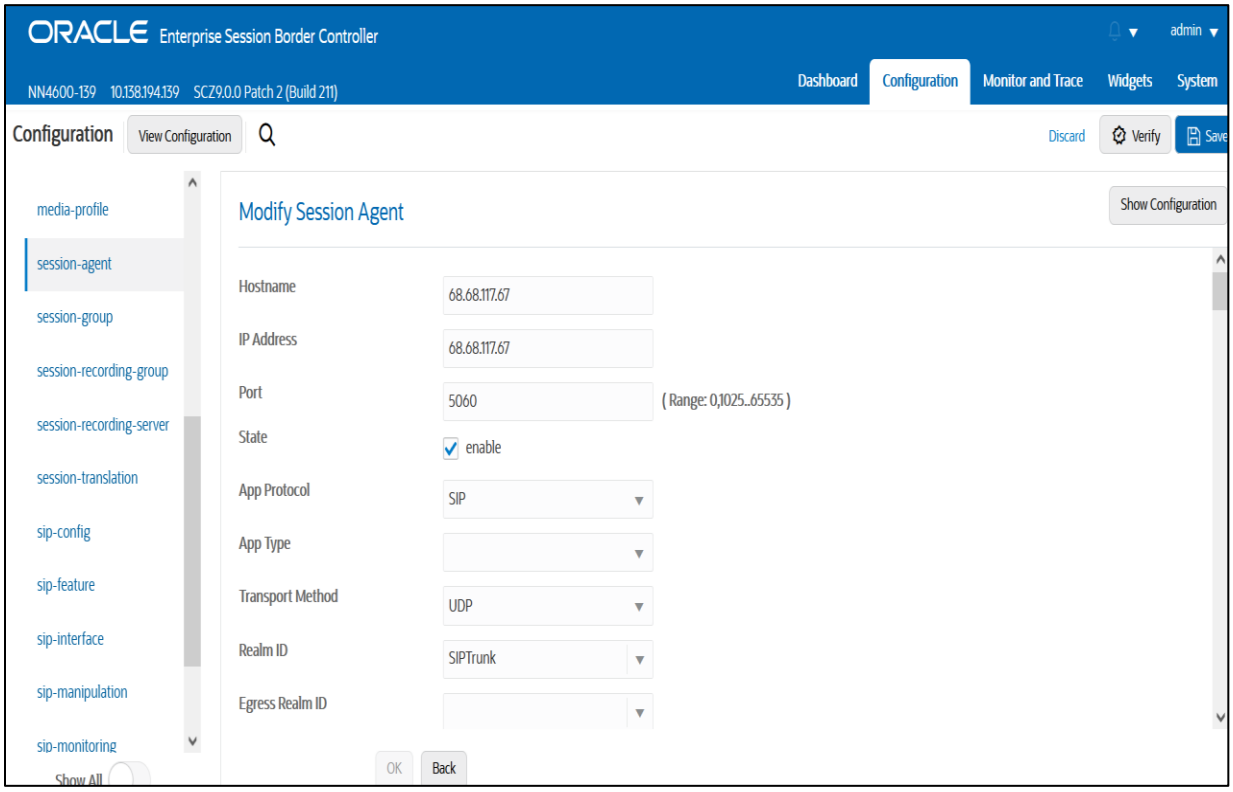
Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

6.9. 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.

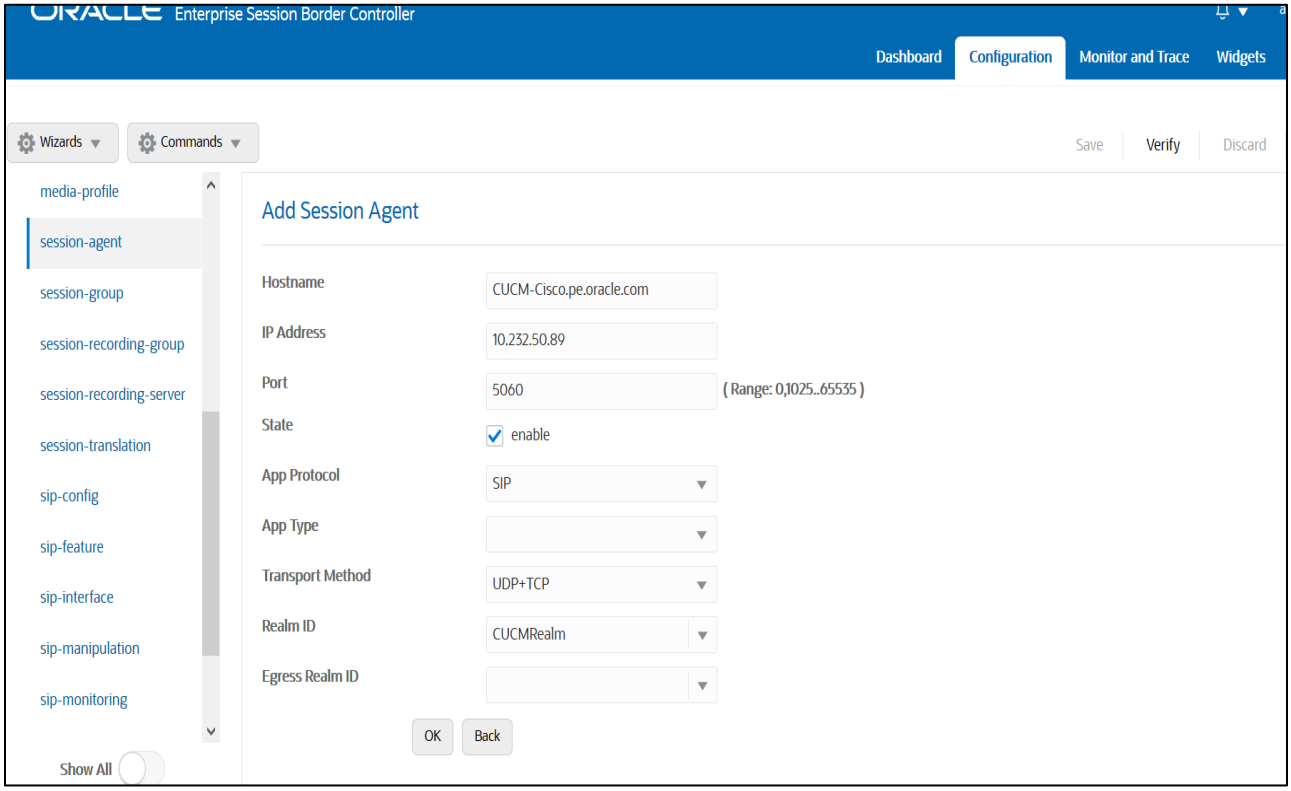
Go to session-router->Session-Agent and Configure the session-agents for the Generic SIP Trunk

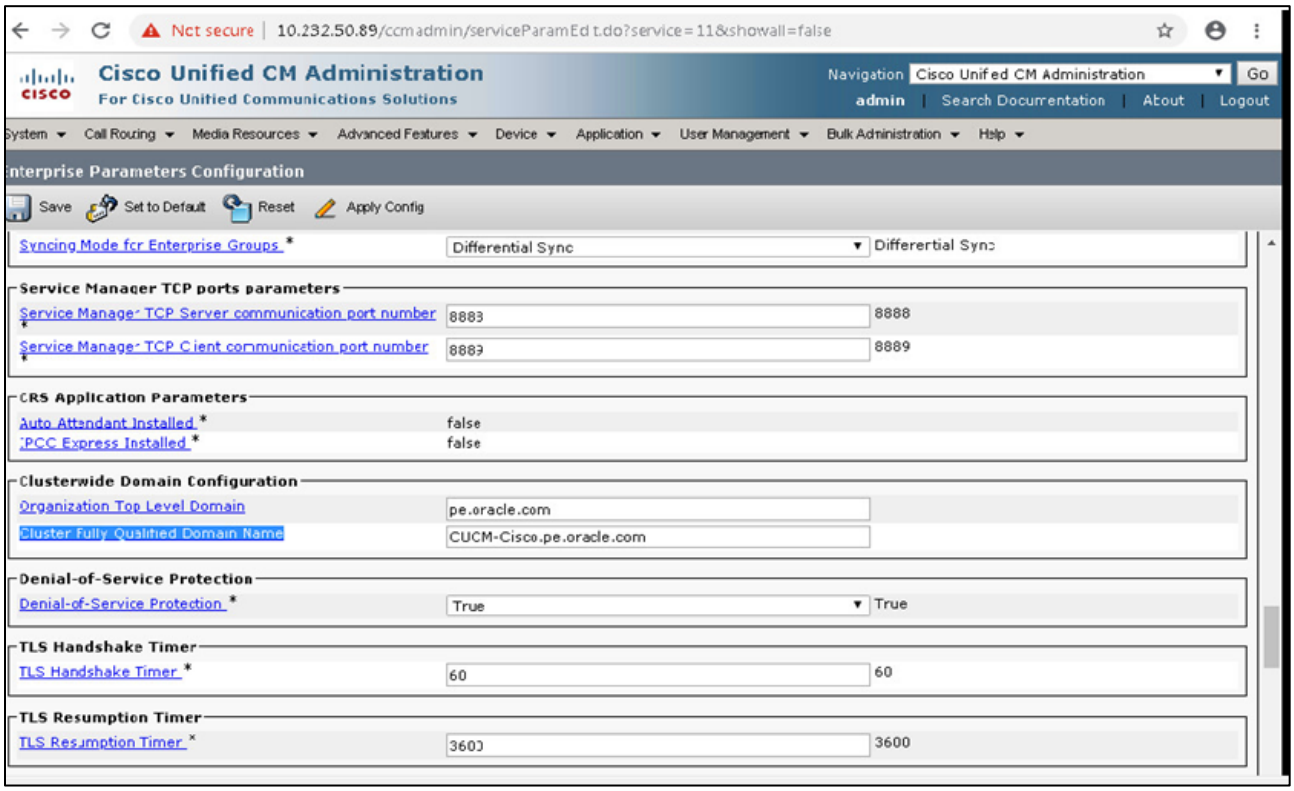
- Host name to “68.68.117.67”, port to 5060
- realm-id – needs to match the realm created for the Generic SIP Trunk



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

- Host name to FQDN of CUCM which is “CUCM-Cisco.pe.oracle.com” in our example. **We can also give Cisco CUCM IP address if there is no host name configured.**
- The same FQDN value should be configured in Cisco CUCM under System --- Enterprise Parameter ----Cluster FQDN.

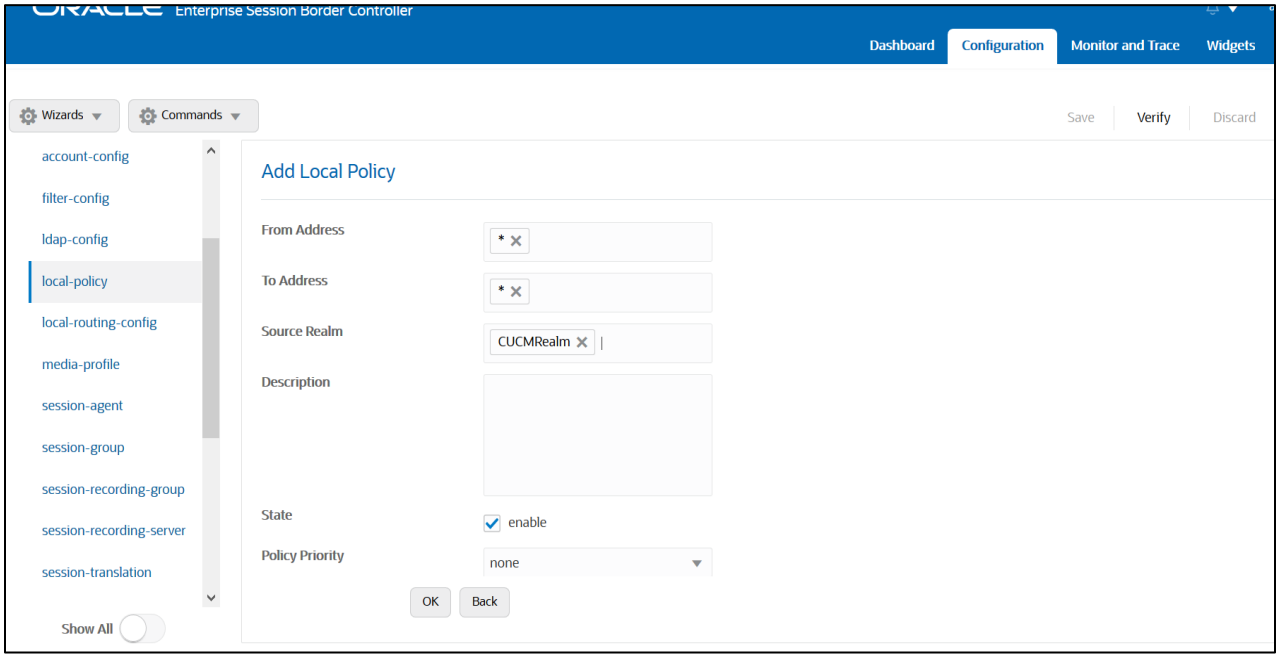

Enterprise Session Border Controller
Dashboard
Configuration
Monitor and Trace
Widgets
Wizards
Commands
Save
Verify
Discard
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
Show All
Add Session Agent
Hostname
CUCM-Cisco.pe.oracle.com
IP Address
10.232.50.89
Port
5060
(Range: 0,1025..65535)
State
enable
App Protocol
SIP
App Type
Transport Method
UDP+TCP
Realm ID
CUCMRealm
Egress Realm ID
OK
Back

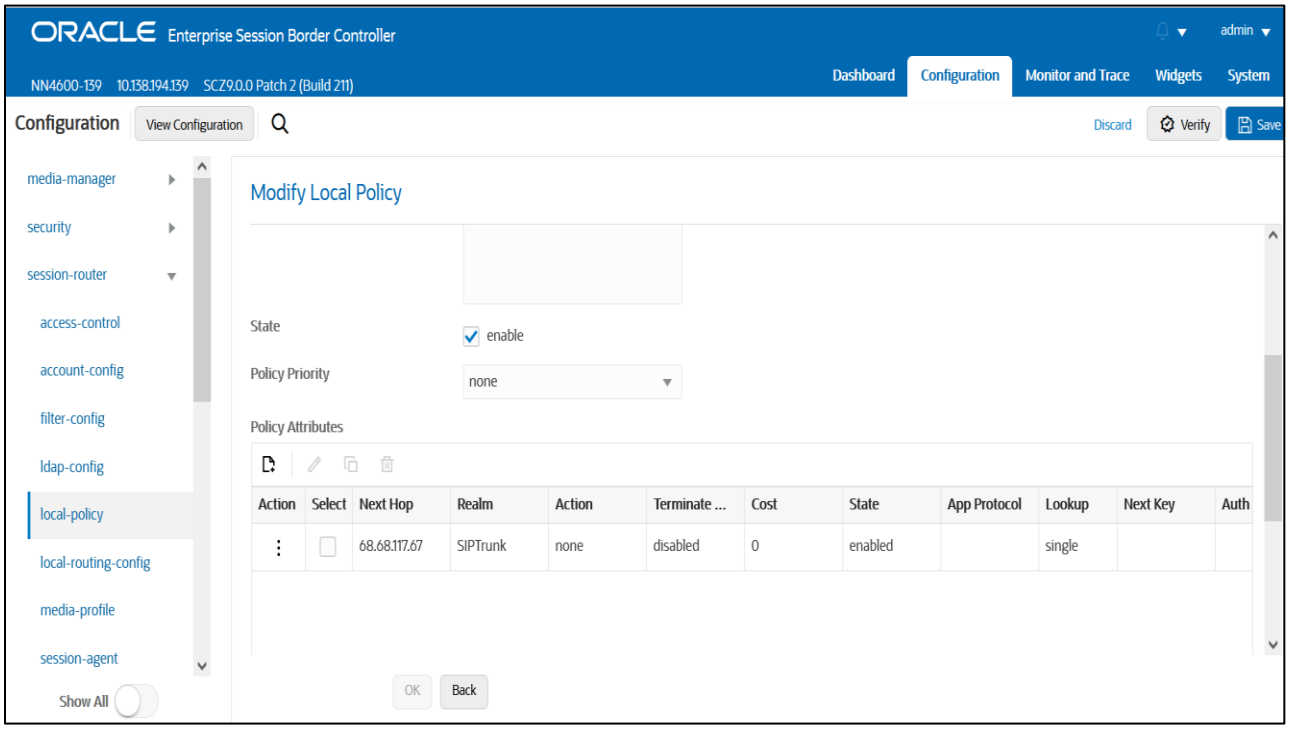

Not secure | 10.232.50.89/ccmadmin/serviceParamEdit.do?service=11&showall=false
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified CM Administration
Go
admin
Search Documentation
About
Logout
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help
Enterprise Parameters Configuration
Save
Set to Default
Reset
Apply Config
Syncing Mode for Enterprise Groups *
Differential Sync
Differential Sync
Service Manager TCP ports parameters
Service Manager TCP Server communication port number *
8883
8888
Service Manager TCP Client communication port number *
8889
8889
CRS Application Parameters
Auto Attendant Installed *
false
IPCC Express Installed *
false
Clusterwide Domain Configuration
Organization Top Level Domain
pe.oracle.com
Cluster Fully Qualified Domain Name
CUCM-Cisco.pe.oracle.com
Denial-of-Service Protection
Denial-of-Service Protection *
True
True
TLS Handshake Timer
TLS Handshake Timer *
60
60
TLS Resumption Timer
TLS Resumption Timer *
3600
3600

6.10. Configure local-policy

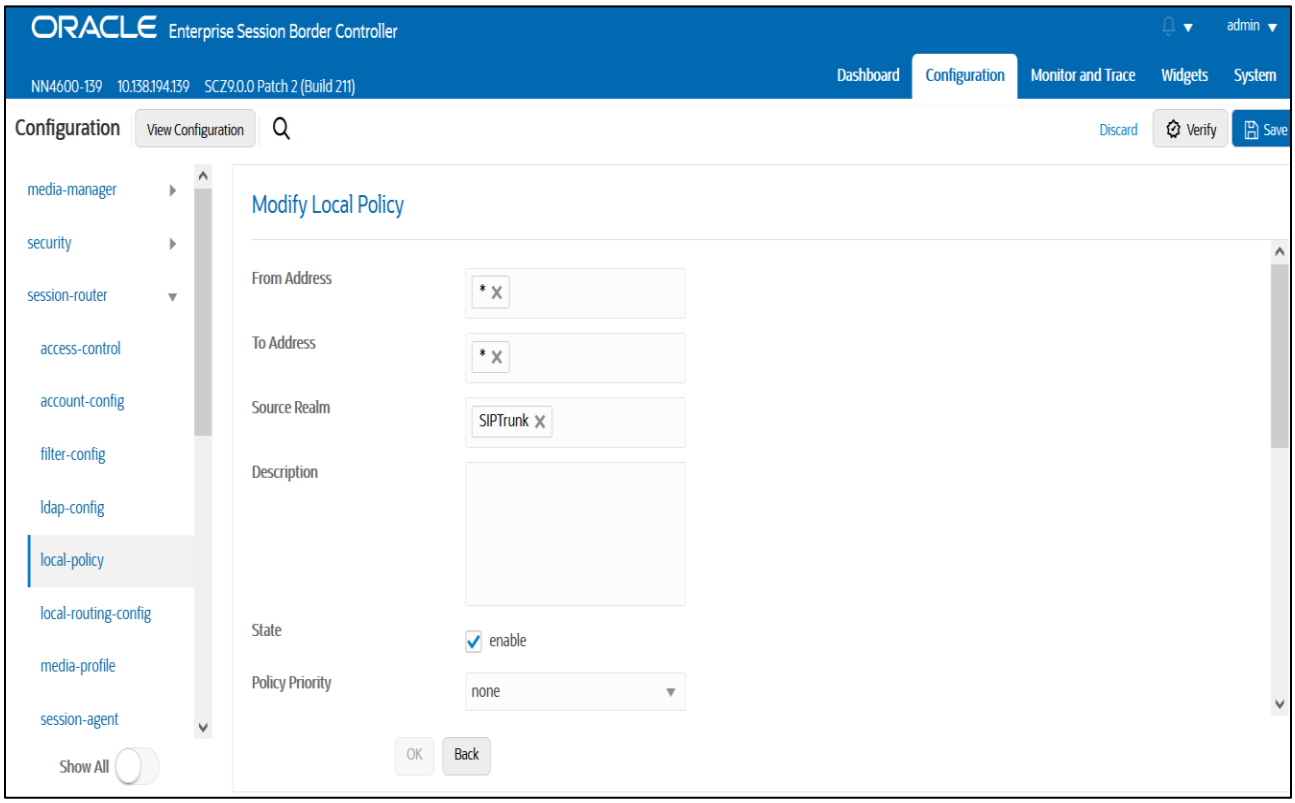
Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

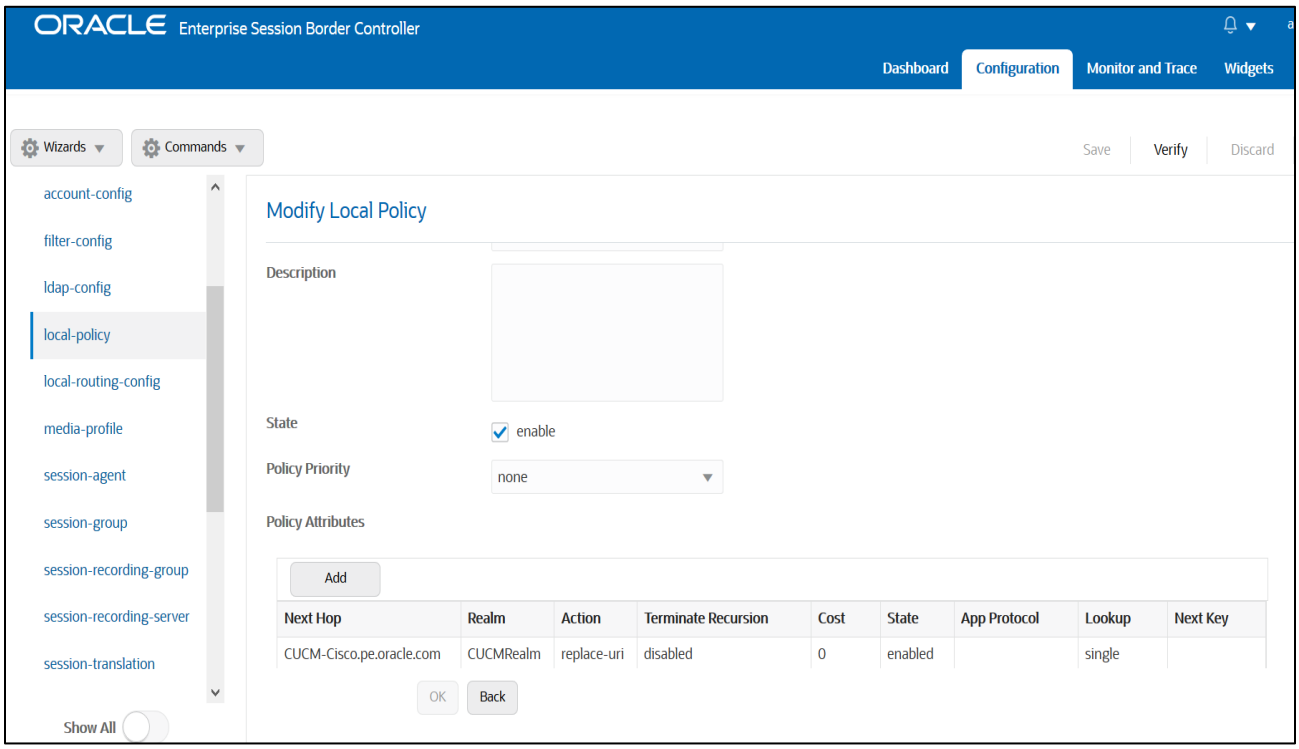
To route the calls from Cisco side to Generic SIP trunk side, Use the below local –policy





To route the calls from the Generic SIP Trunk side to Cisco side, Use the below local –policy

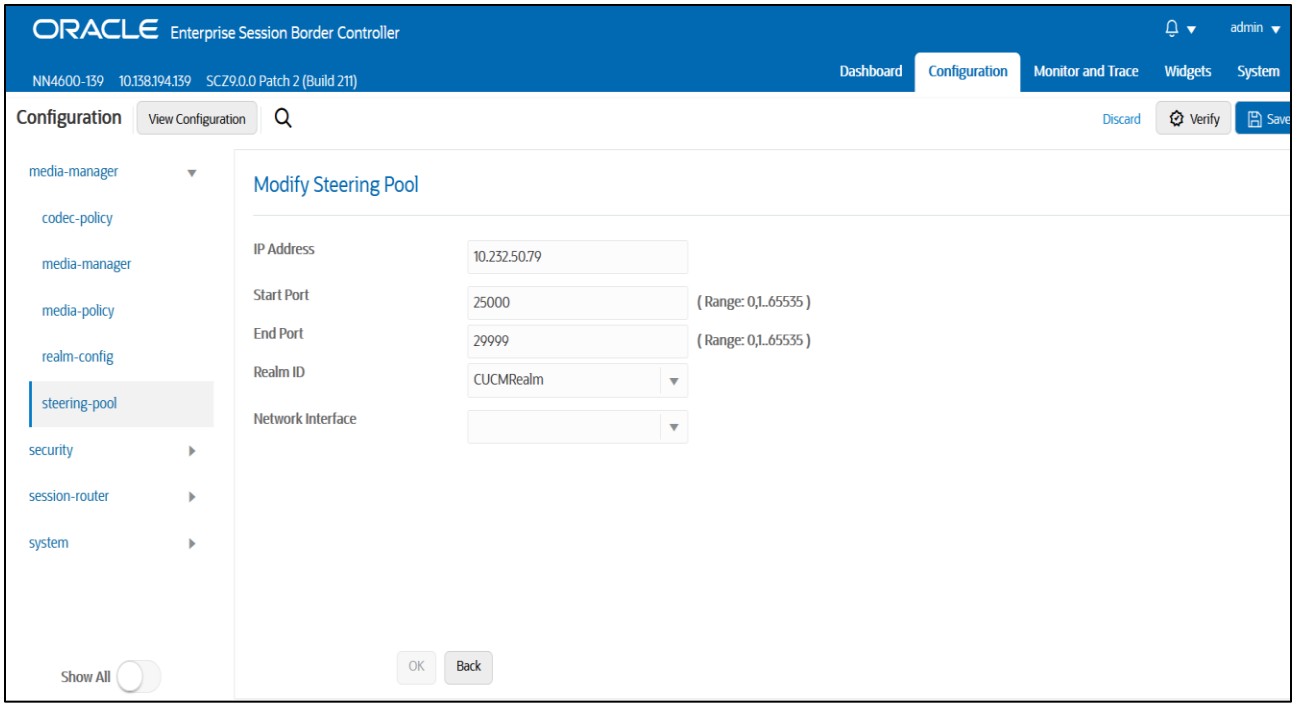




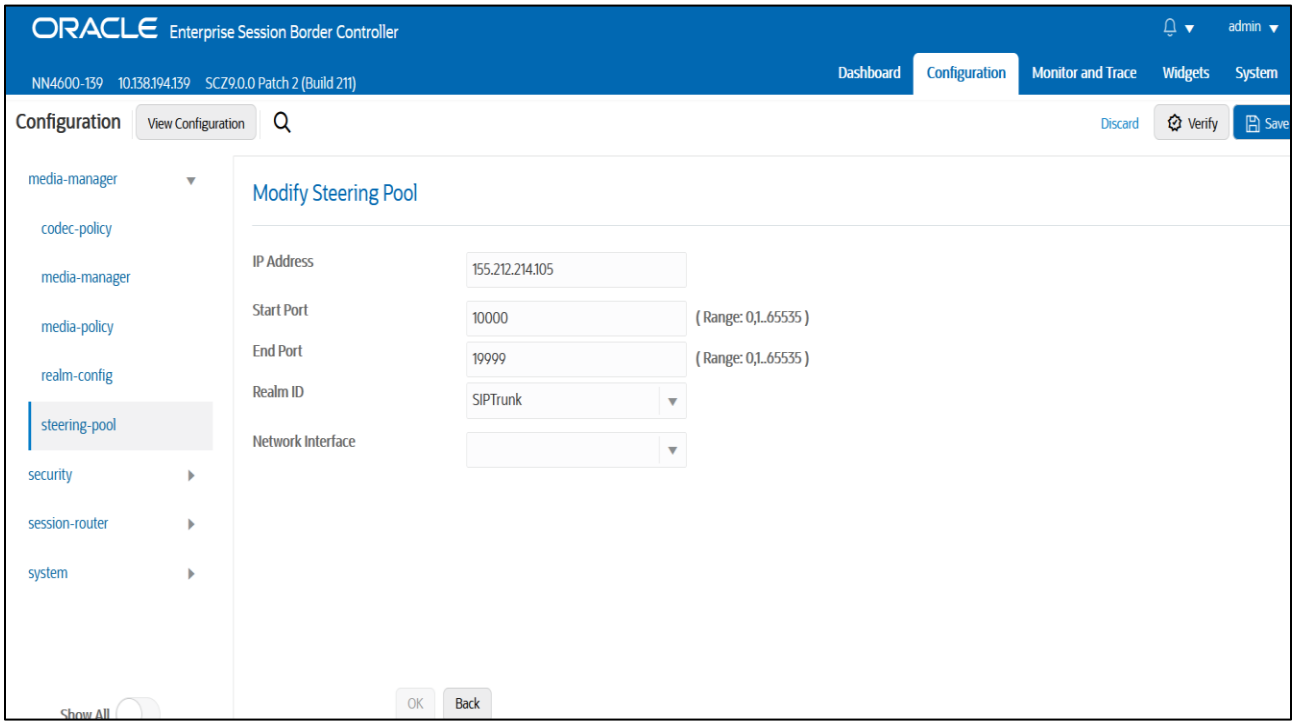
6.11. Configure steering-pool

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

Cisco side steering pool.



Generic SIP trunk side steering pool.

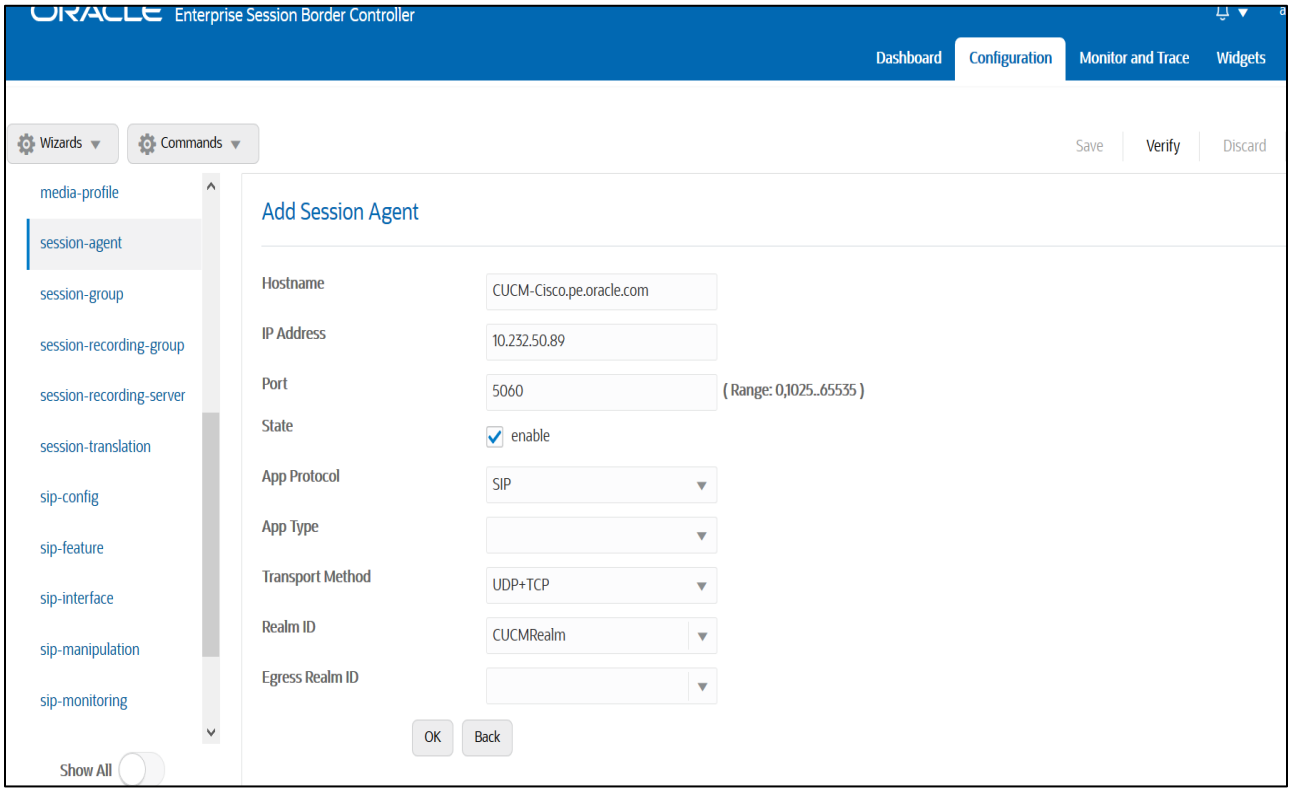


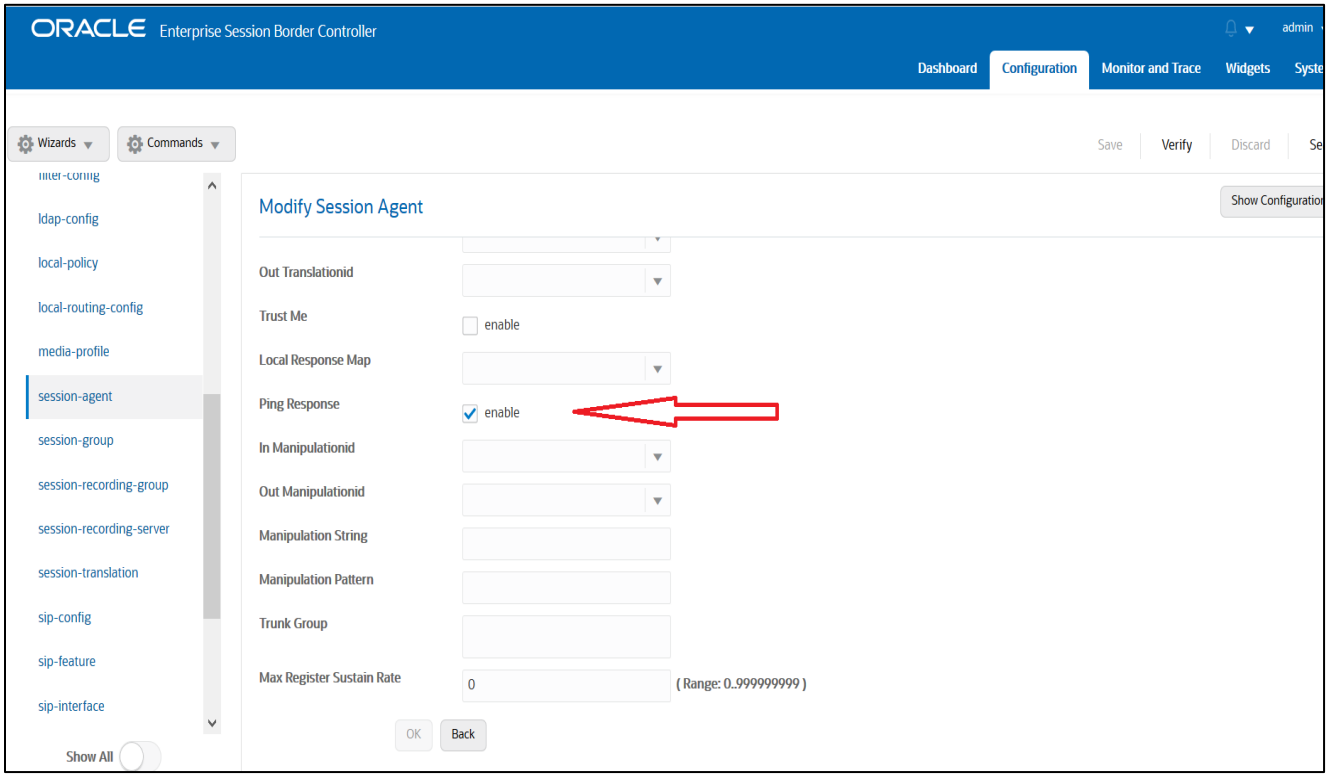
6.12. Configure Ping Response

To simplify the ORACLE SBC configuration, from GA Release SCZ830m1p7, there is a new parameter introduced under the **Session agent** configuration element. The parameter name is **Ping response**.

Ping Response:

When this parameter is enabled, the SBC responds with a 200 OK to all Sip Options Pings it receives from trusted agents. This takes the place of the current Sip Manipulation, RepondOptions.

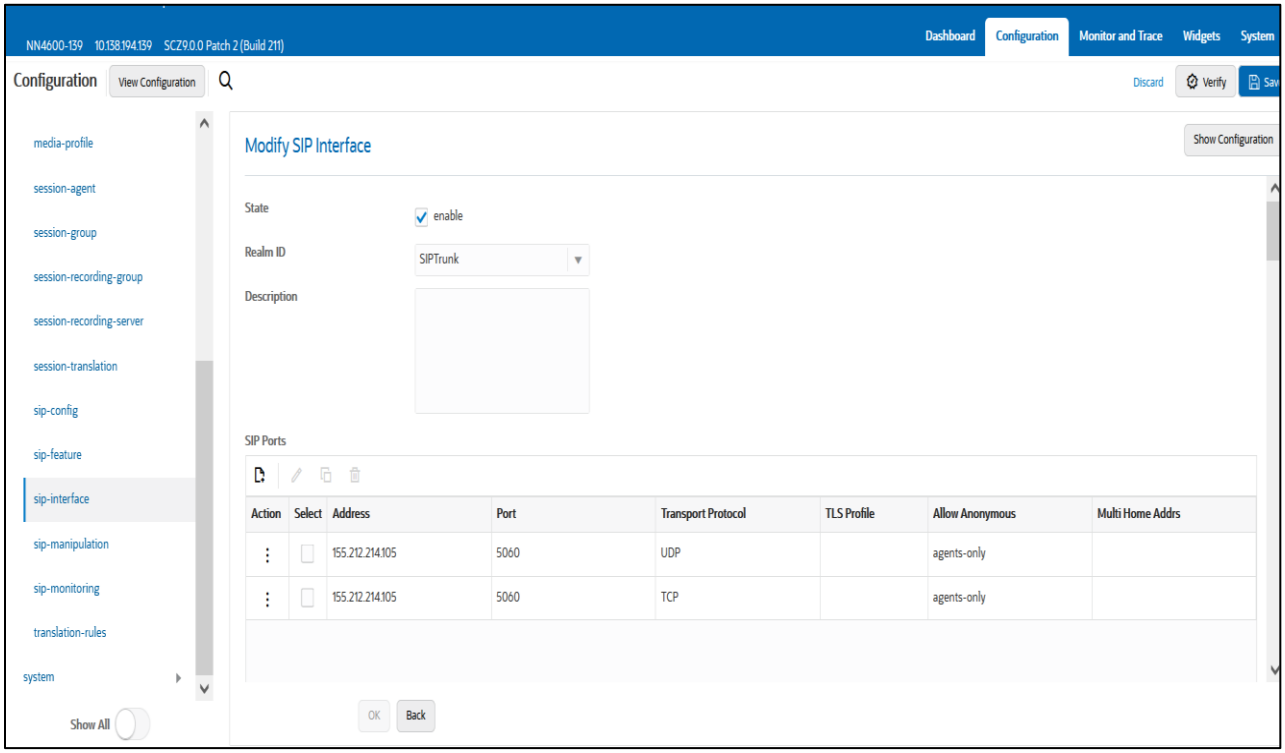


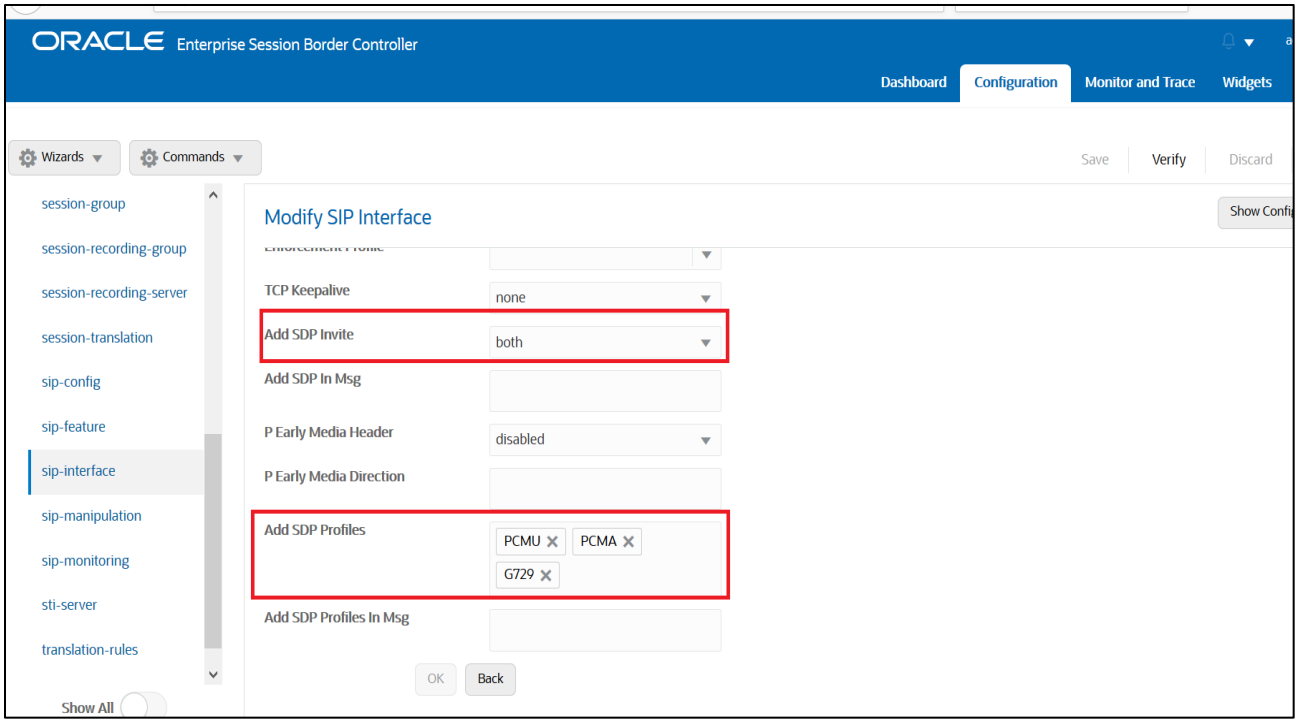


6.13. SBC config for Cisco Offer less INVITE

When CUCM sends INVITE without SDP towards SBC and in that case, SBC needs to send out INVITE with SDP towards Generic SIP trunk and vice versa. To do that, please set the parameter "**Add SDP Invite**" as both under sip interface (both SIP interfaces) as highlighted below. When this option is enabled, codecs have to be configured under the parameter "**Add SDP profiles**". The configured codecs is also shown below.

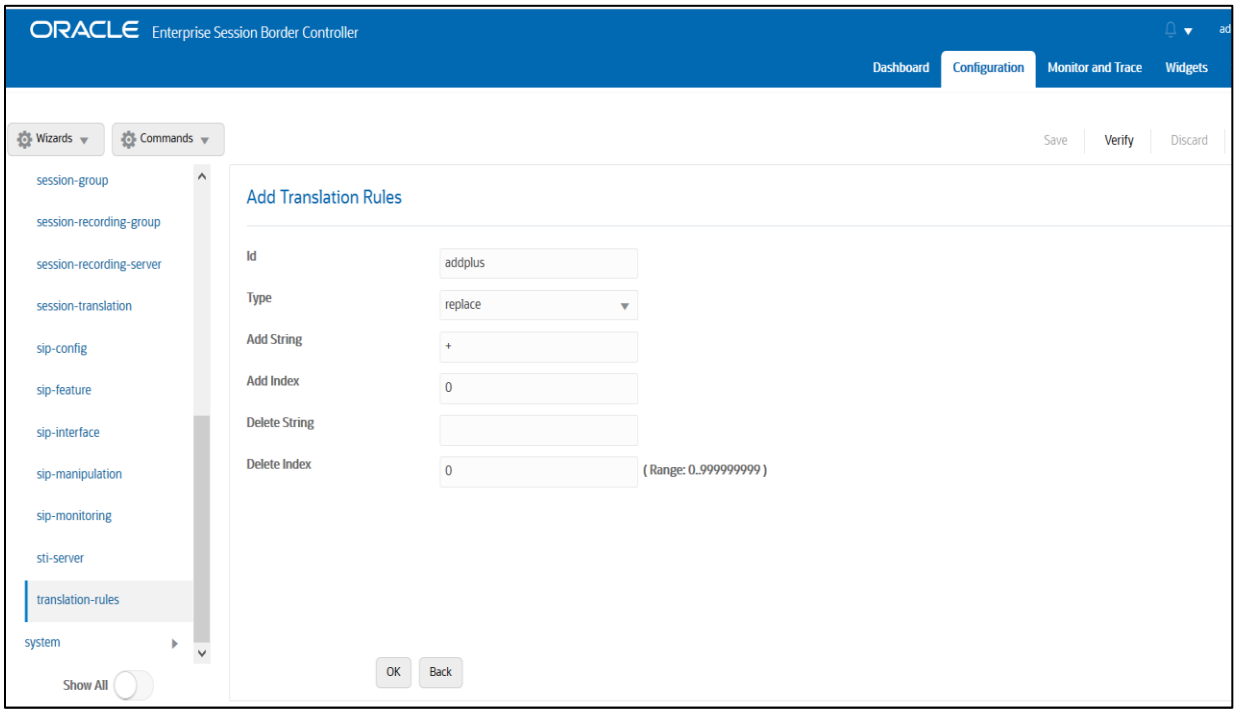
Note: this is an optional config – configure this only if CUCM sends offer less INVITE towards SBC.

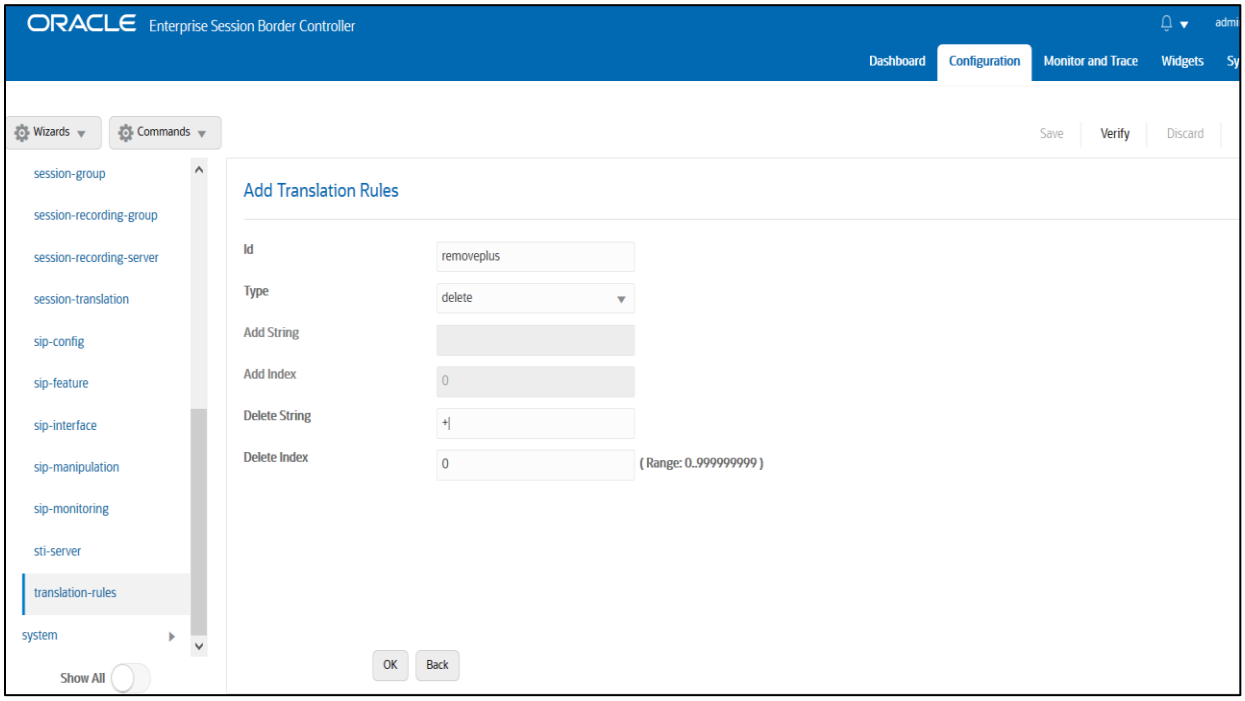

NN4600-139 10.138.194.139 SCZ9.0.0 Patch 2 (Build 211)
Dashboard
Configuration
Monitor and Trace
Widgets
System
Configuration
View Configuration
Discard
Verify
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
translation-rules
system
Show All
Modify SIP Interface
Show Configuration
State
enable
Realm ID
SIPTrunk
Description
SIP Ports
Action
Select
Address
Port
Transport Protocol
TLS Profile
Allow Anonymous
Multi Home Addrs
155.212.214.105
5060
UDP
agents-only
155.212.214.105
5060
TCP
agents-only
OK
Back


ORACLE Enterprise Session Border Controller
Dashboard
Configuration
Monitor and Trace
Widgets
Wizards
Commands
Save
Verify
Discard
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
sti-server
translation-rules
Show All
Modify SIP Interface
TCP Keepalive
none
Add SDP Invite
both
Add SDP In Msg
P Early Media Header
disabled
P Early Media Direction
Add SDP Profiles
PCMU
PCMA
G729
Add SDP Profiles In Msg
OK
Back

6.14. Configure Translation Rules

The translation rules sub-element is where the actual translation rules are created.
Go to Session router → translation-rules and create the below rule.

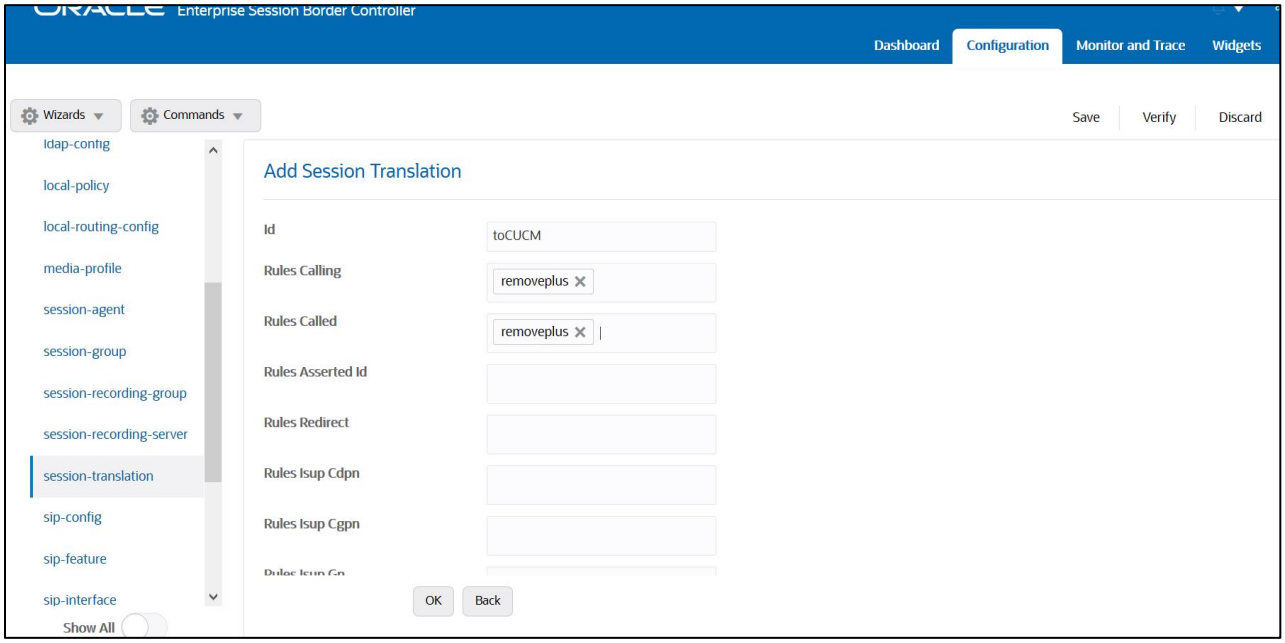




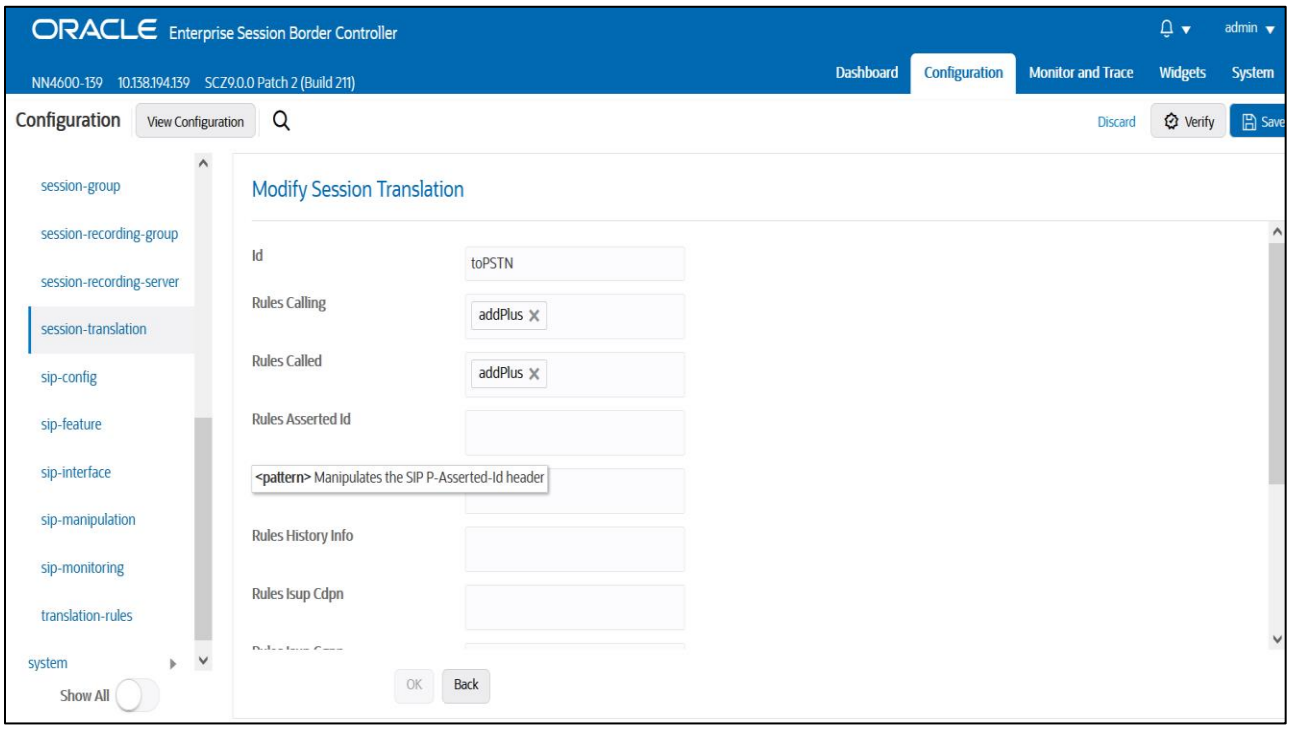
6.15. Configure Session Translation Rules

A session translation defines how translation rules are applied to calling and called numbers.
Go to Session Router → session-translation and configure the below translation rules.

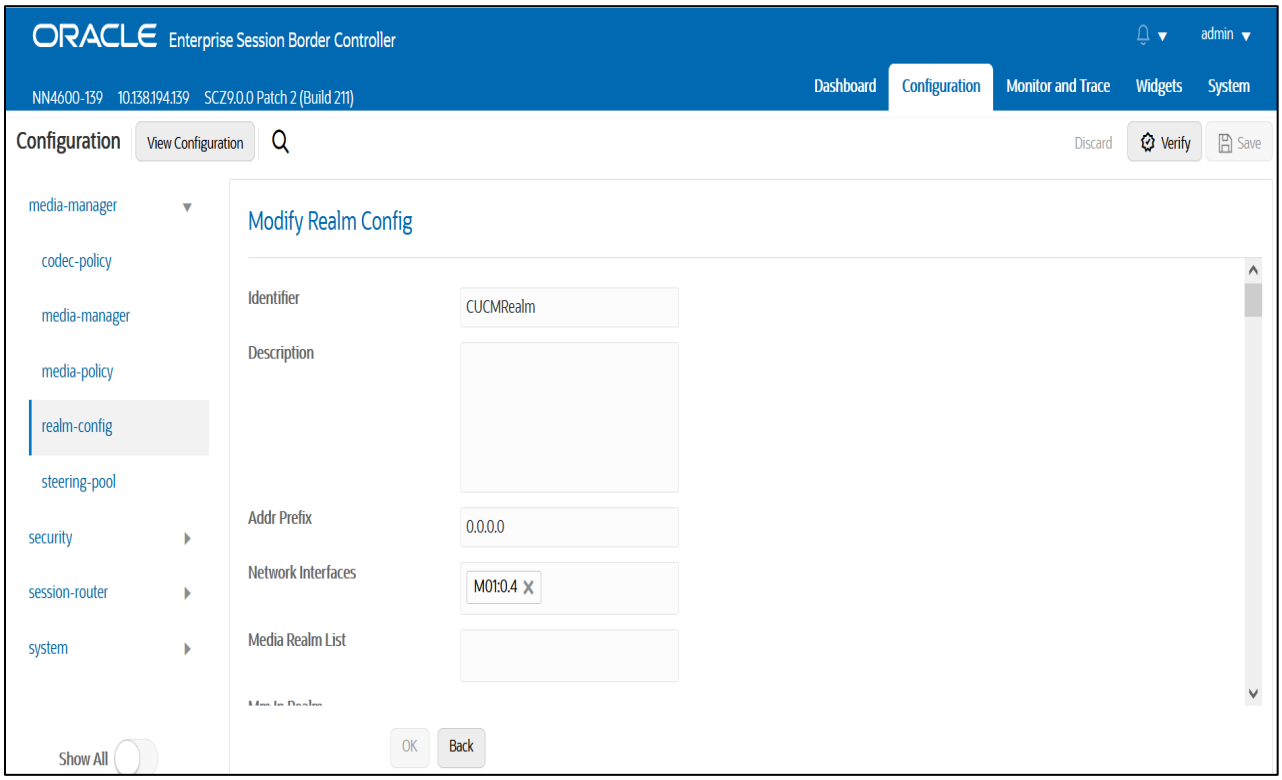
Add the below translation rule to Cisco side.

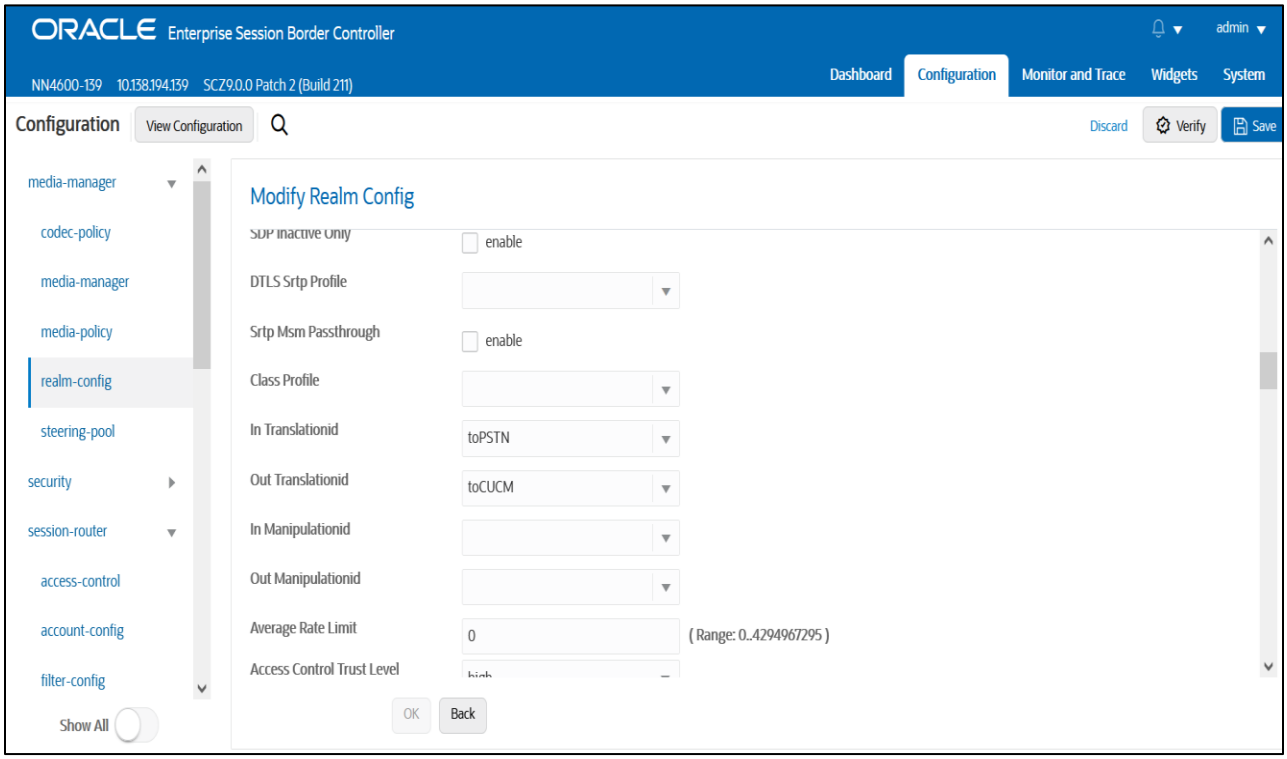


Add the below translation rule to SIP trunk side as PSTN expects call with + sign.



Please add the above session translation rules to Cisco realm as shown below





With this, SBC configuration is complete

7. SBC configuration for Cisco Remote Worker

This section of Cisco Remote Worker configuration is included for Cisco remote endpoints that register through the Oracle SBC to the Cisco Call Manager (Cisco CUCM). This would require additional configuration to be configured on the Oracle SBC along with the SIP trunking config as mentioned in the earlier description of the test bed. To complete the particular testing, we have configured Cisco endpoints which will register to Cisco CUCM through the SBC. SBC will handle the calls based on the registration information present in the cache. **Please note that Cisco Remote worker Access side is secured (TLS/SRTP) and Cisco Core side is unsecured (UDP or TCP/RTP)**

Note: Remote worker configuration through TLS for Jabber clients is not supported by CUCM.

In order to achieve the requirement, we have made below configuration on the Oracle SBC

Access and Core Realm for Cisco Remote worker
Steering Pool associated with the Realm for Cisco Remote worker
Sip-interface associated with the Realm for Cisco Remote worker
(Optional) A local policy to route the registration requests from this Realm to the SIP Server.

Note -The local-policy element is optional as we can enable the Route to registrar parameter on the sip-interface config to route the requests to the Registrar.
The registrar host and port are configured in the sip-config element on the SBC. The remote endpoint sends register requests from Cisco Access Realm onto the SBC and then SBC registers these endpoints onto the Cisco Core Realm maintaining the registration cache in its database to route inbound calls to these endpoints.

Below are the snippets from the Oracle SBC Web GUI for the Remote worker configuration.

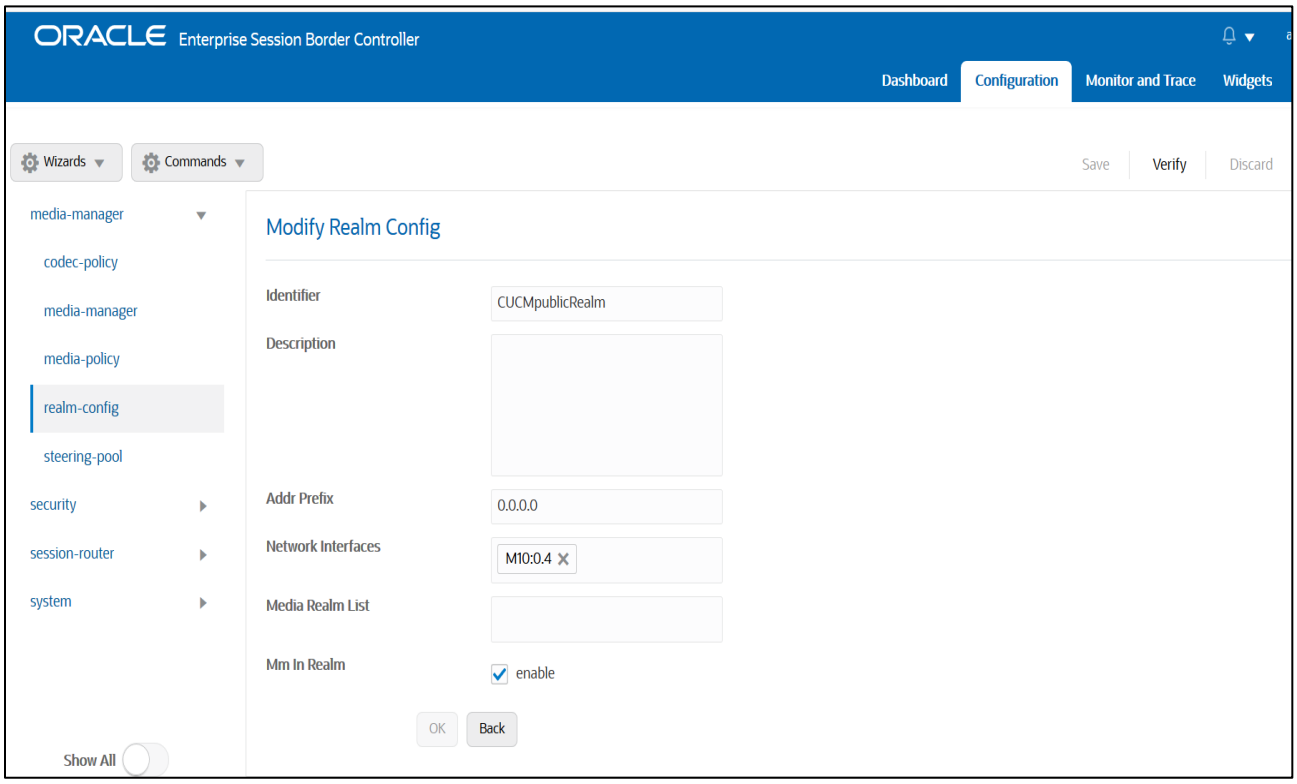
7.1. Configure Realms

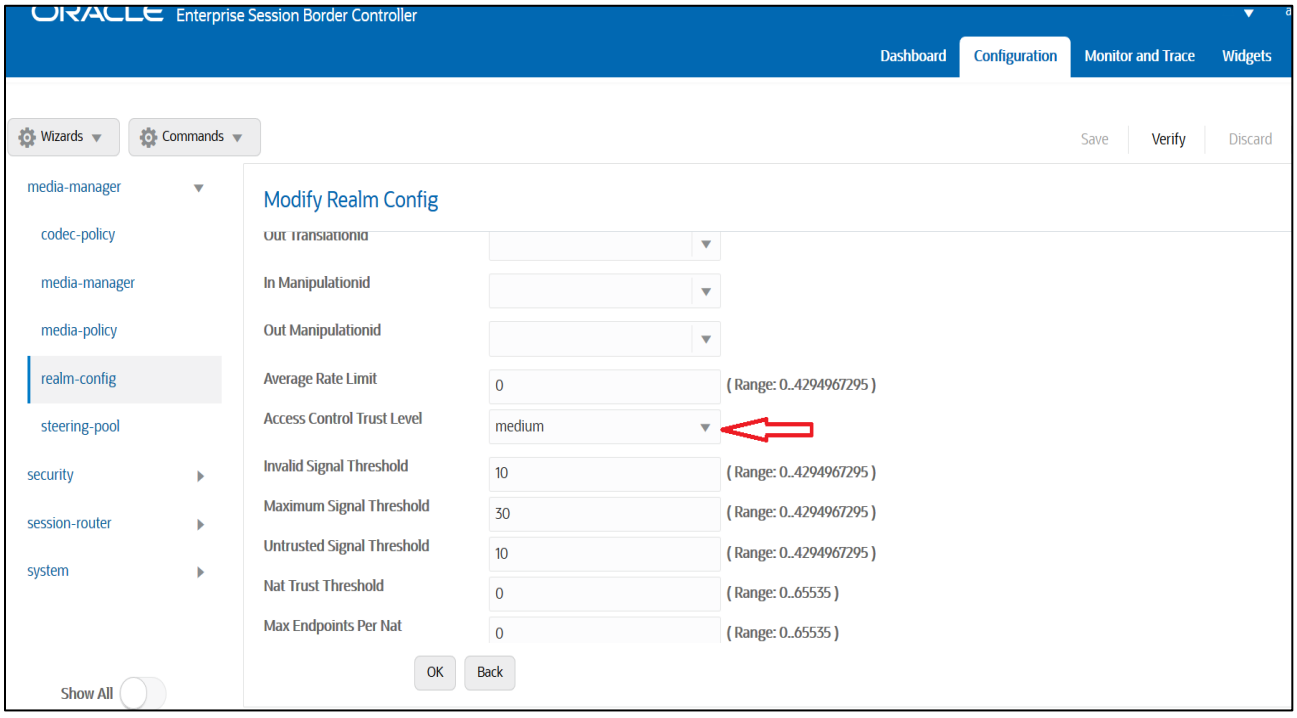
Navigate to realm-config under media-manager and configure a realm as shown below
The name of the Realm can be any relevant name according to the user convenience.

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

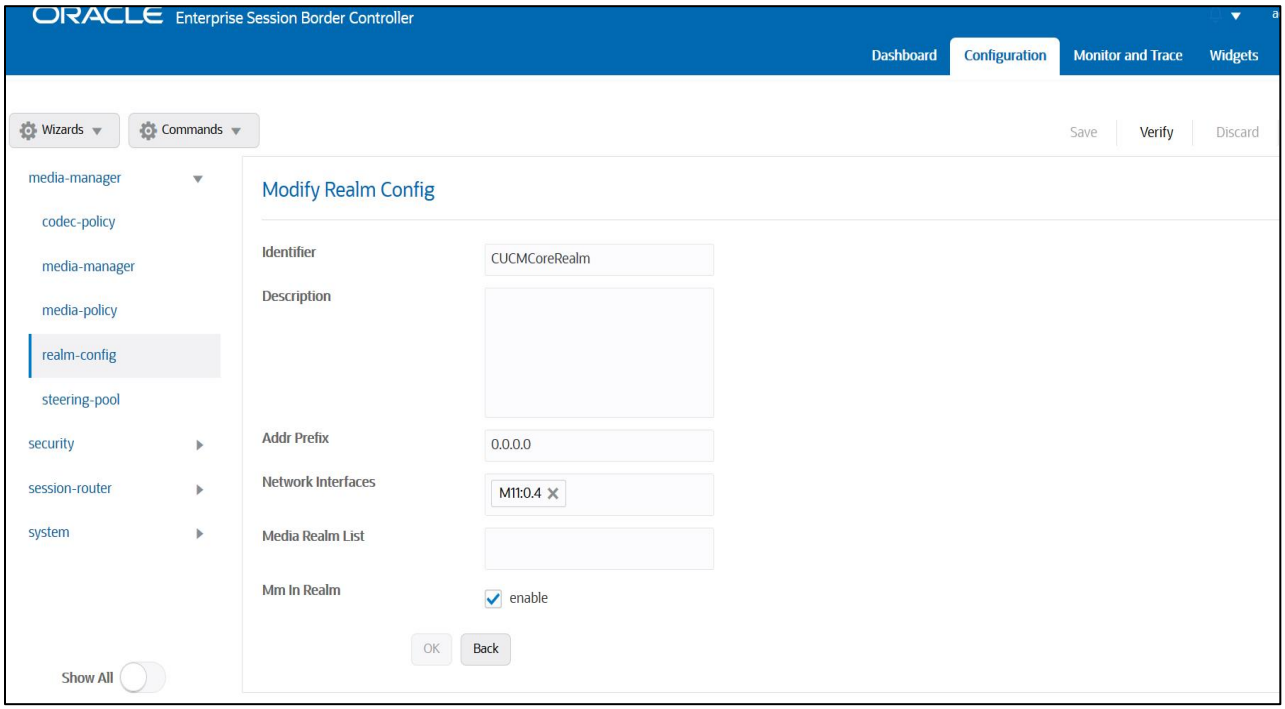
Config Parameter	Cisco Access Side	Cisco Core Side
Identifier	CUCMpublicRealm	CUCMCoreRealm
Network Interface	M10	M11
Mm in realm	☑	☑
FQDN		
Media Sec policy	sdespolicy	RTP
Access Control Trust Level	High	High

In the below example, Realm name is given as CUCMpublicRealm for Cisco Access Side.
Please set the Access Control Trust Level as medium for this realm





Similarly, Realm name is given as CUCMCoreRealm for Cisco Core side



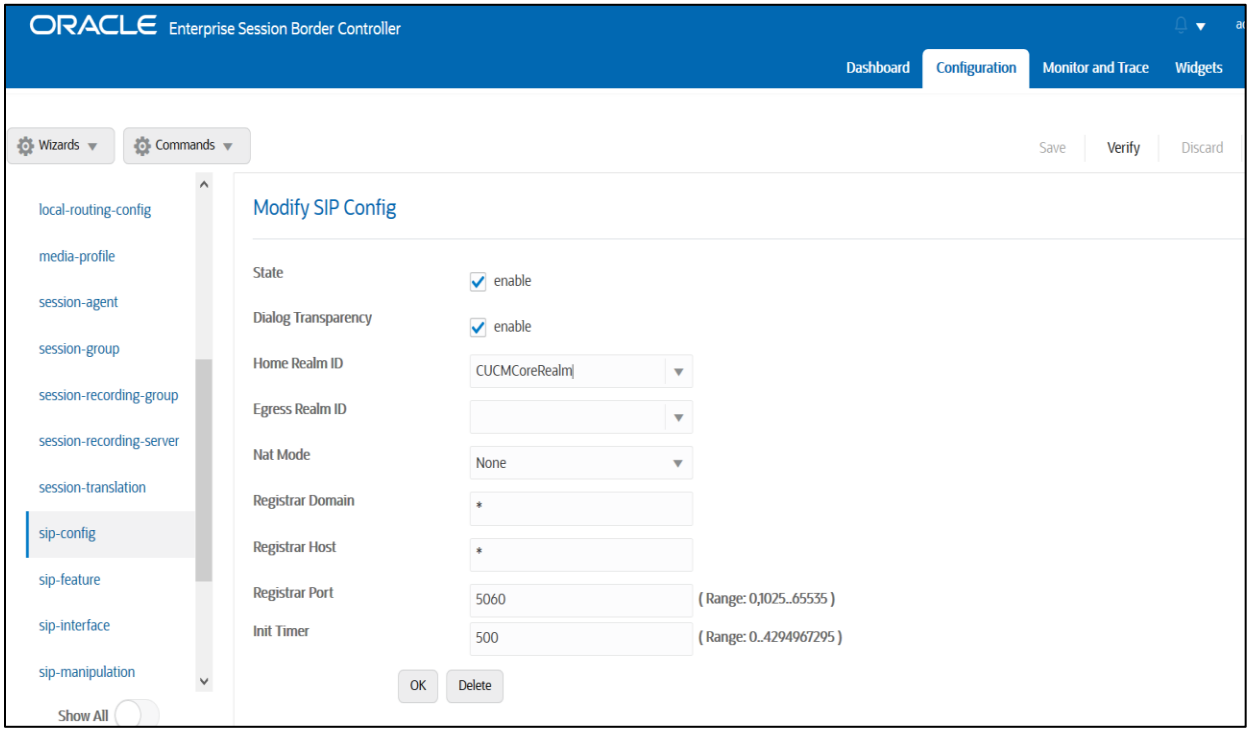
7.2. Enable sip-config

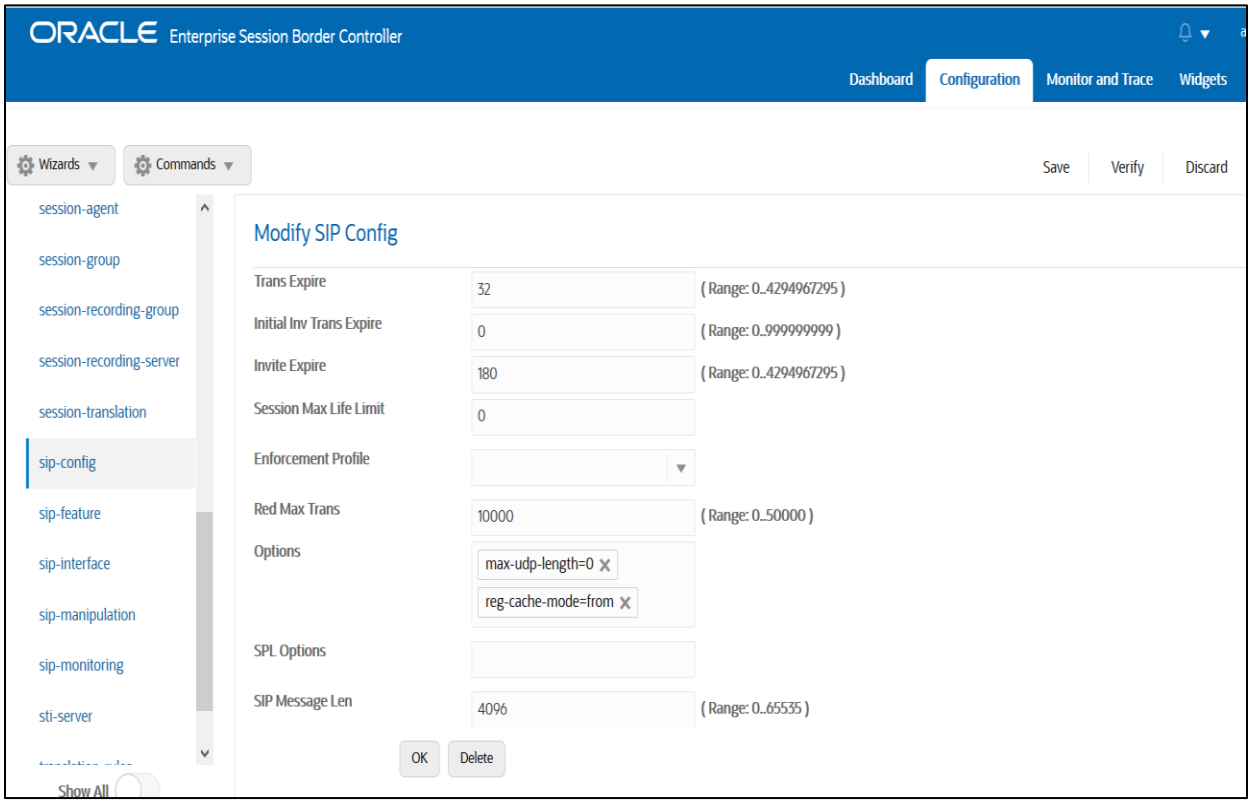
SIP config enables SIP handling in the SBC.
Make sure the home realm-id, registrar-domain and registrar-host are configured.
Also add the options to the sip-config as shown below.

To configure sip-config, Go to Session-Router->sip-config and in options, add the below

- add max-udp-length =0
- reg-cache-mode=from

  This option is used so that the userinfo from the From header is copied to the userinfo of the forwarded Contact header

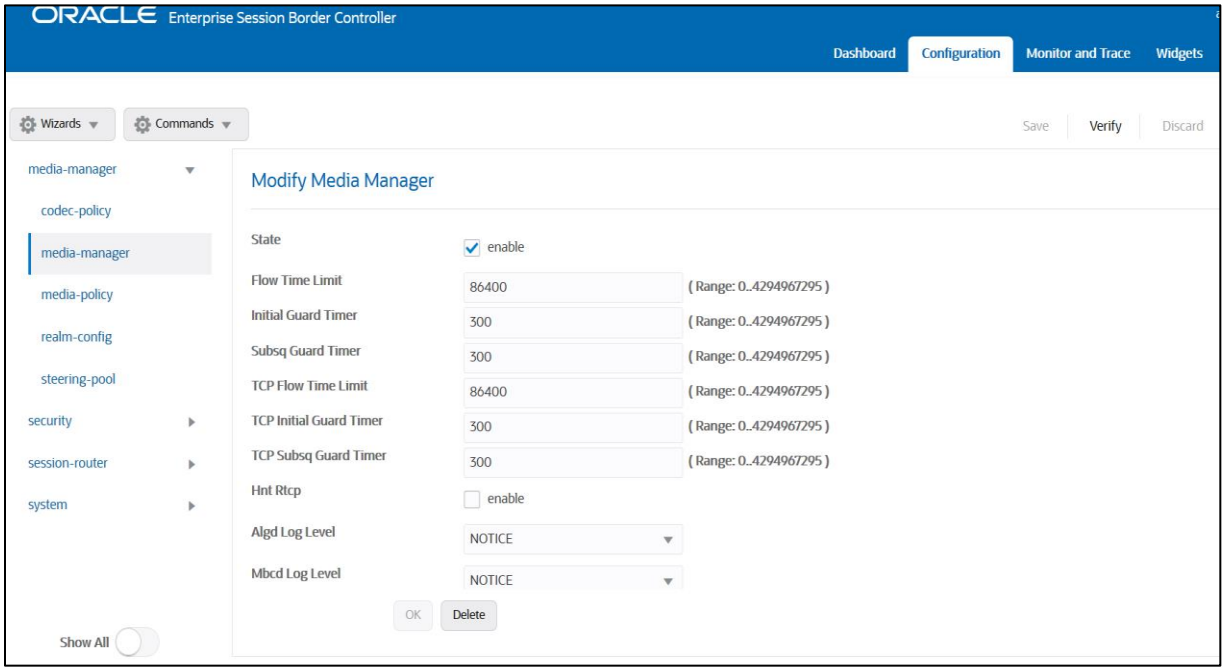

ORACLE Enterprise Session Border Controller
Dashboard
Configuration
Monitor and Trace
Widgets
Wizards
Commands
Save
Verify
Discard
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
Show All
Modify SIP Config
State
enable
Dialog Transparency
enable
Home Realm ID
CUCMCoreRealm
Egress Realm ID
Nat Mode
None
Registrar Domain
*
Registrar Host
*
Registrar Port
5060
(Range: 0,1025..65535)
Init Timer
500
(Range: 0..4294967295)
OK
Delete

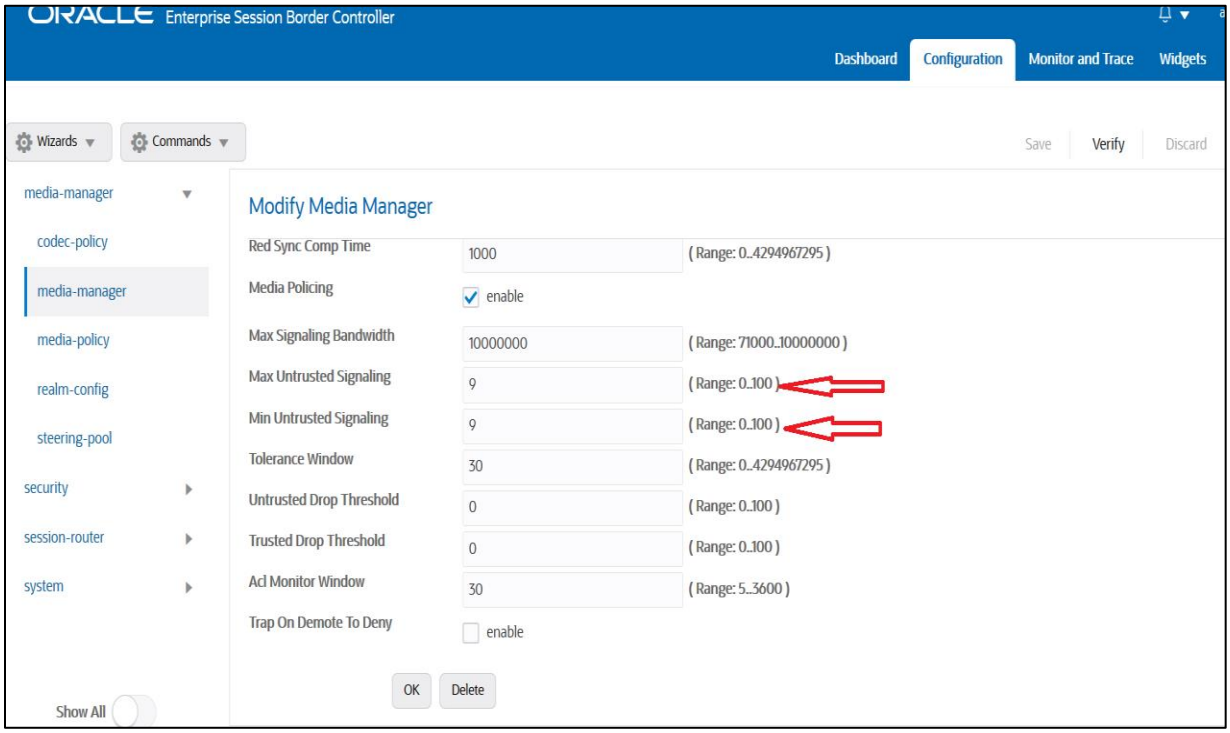

ORACLE Enterprise Session Border Controller
Dashboard
Configuration
Monitor and Trace
Widgets
Wizards
Commands
Save
Verify
Discard
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
sti-server
Show All
Modify SIP Config
Trans Expire
32
(Range: 0..4294967295)
Initial Inv Trans Expire
0
(Range: 0..999999999)
Invite Expire
180
(Range: 0..4294967295)
Session Max Life Limit
0
Enforcement Profile
Red Max Trans
10000
(Range: 0..50000)
Options
max-udp-length=0
reg-cache-mode=from
SPL Options
SIP Message Len
4096
(Range: 0..65535)
OK
Delete

7.3. 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 9 which takes care of Access Realm. Go to Media-Manager->Media-Manager



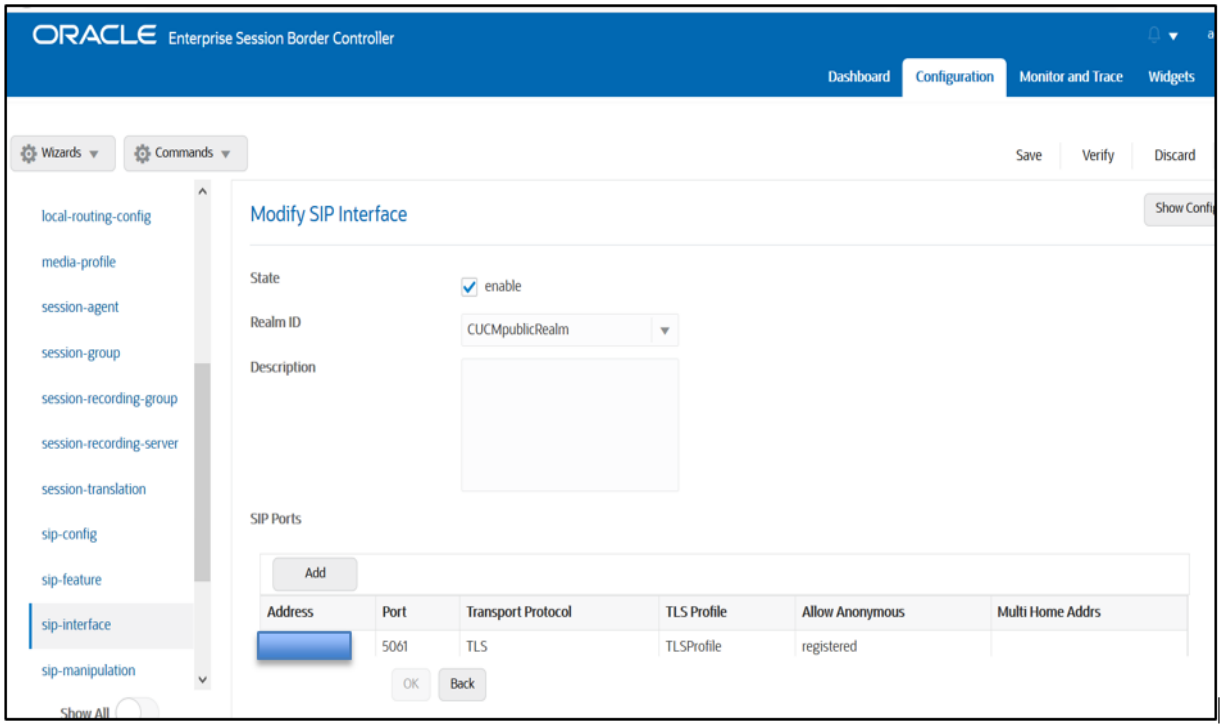


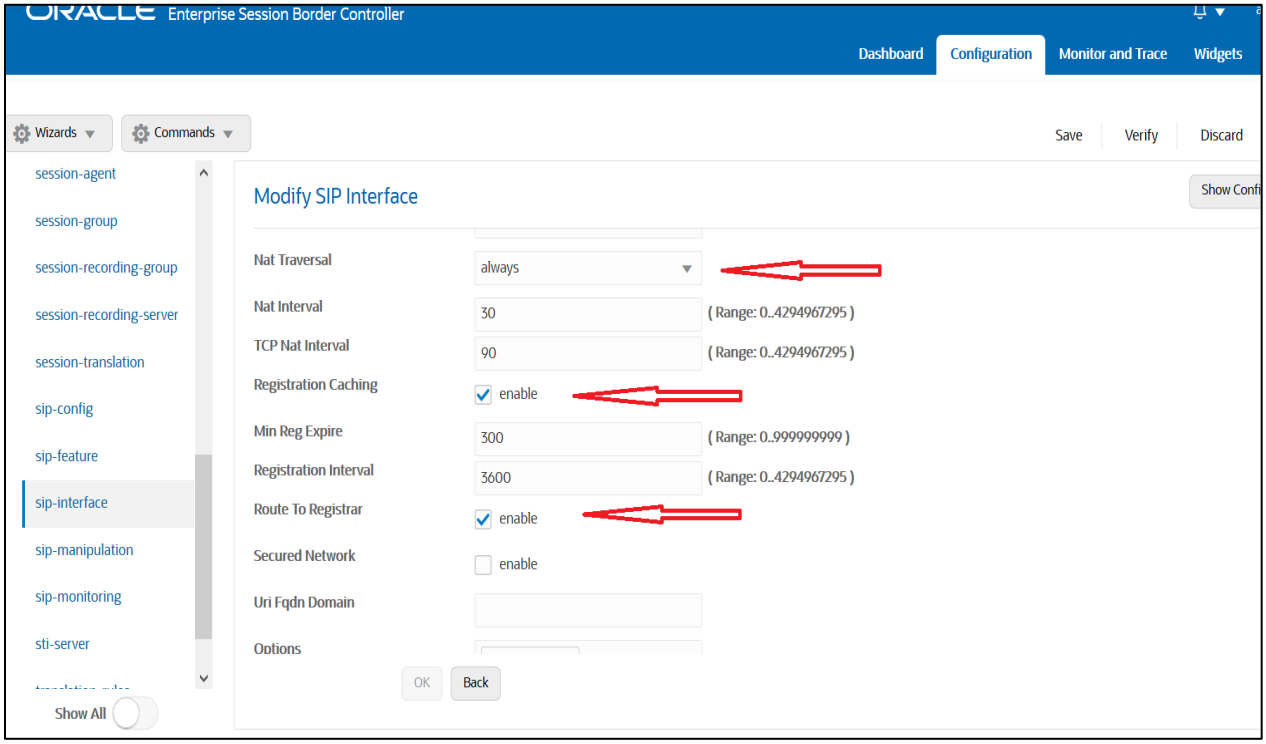
7.4. Configure SIP Interfaces

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

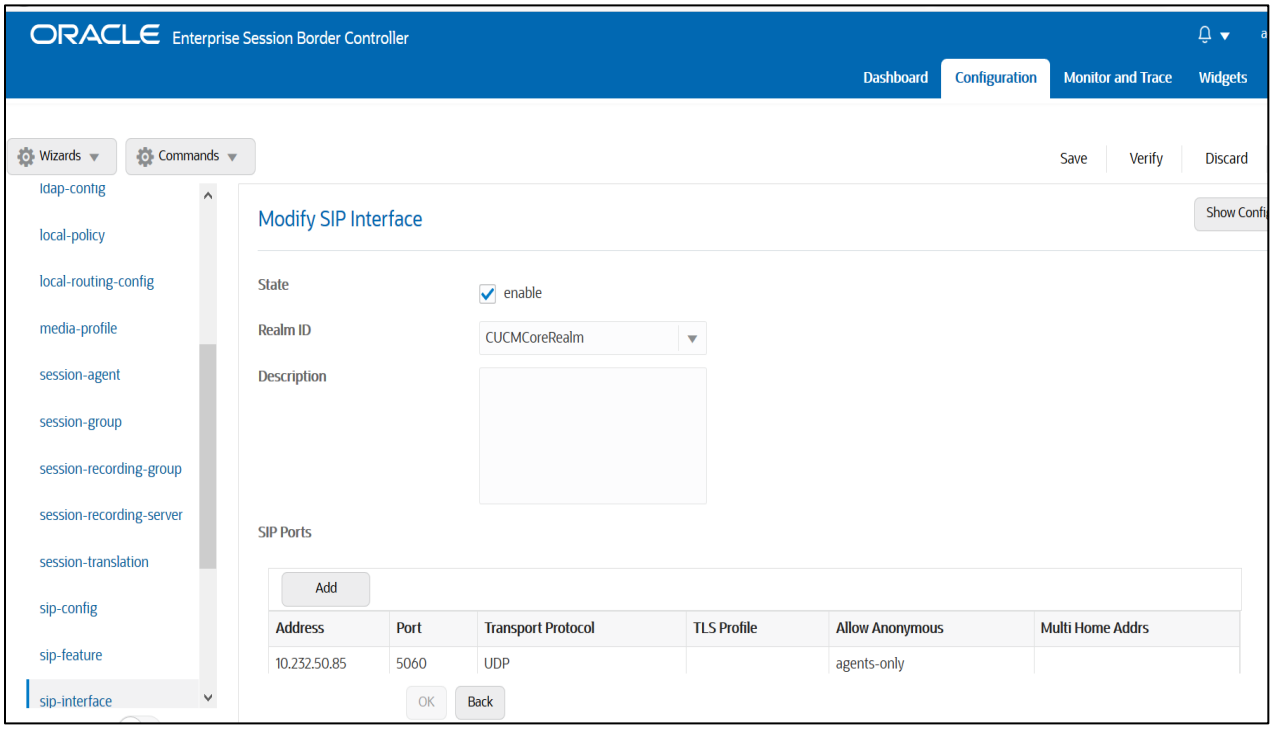
Please Configure sip-interface for the for Cisco Access side as below:

- Set allow-anonymous to Registered to ensure traffic to this sip-interface only comes from the registered user.
- Set NAT traversal to always for the remote workers to register.
- Enable Registration Caching and Route to Register





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

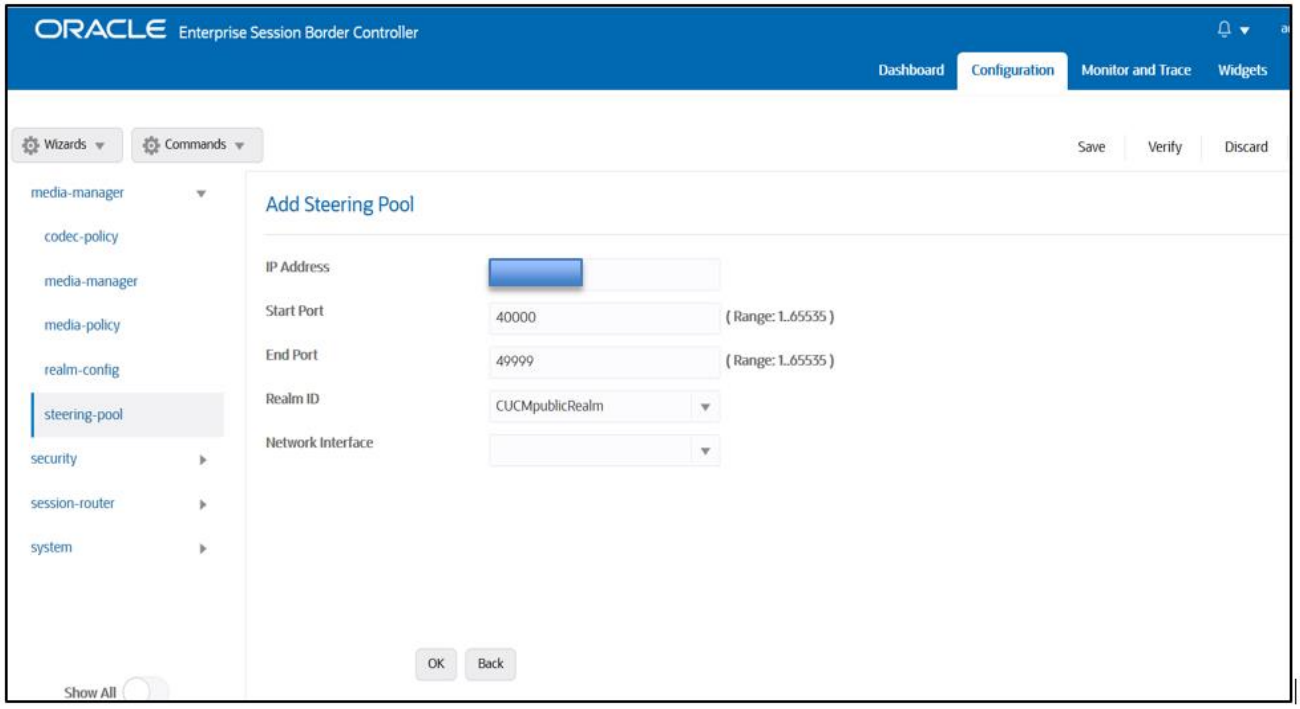


Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

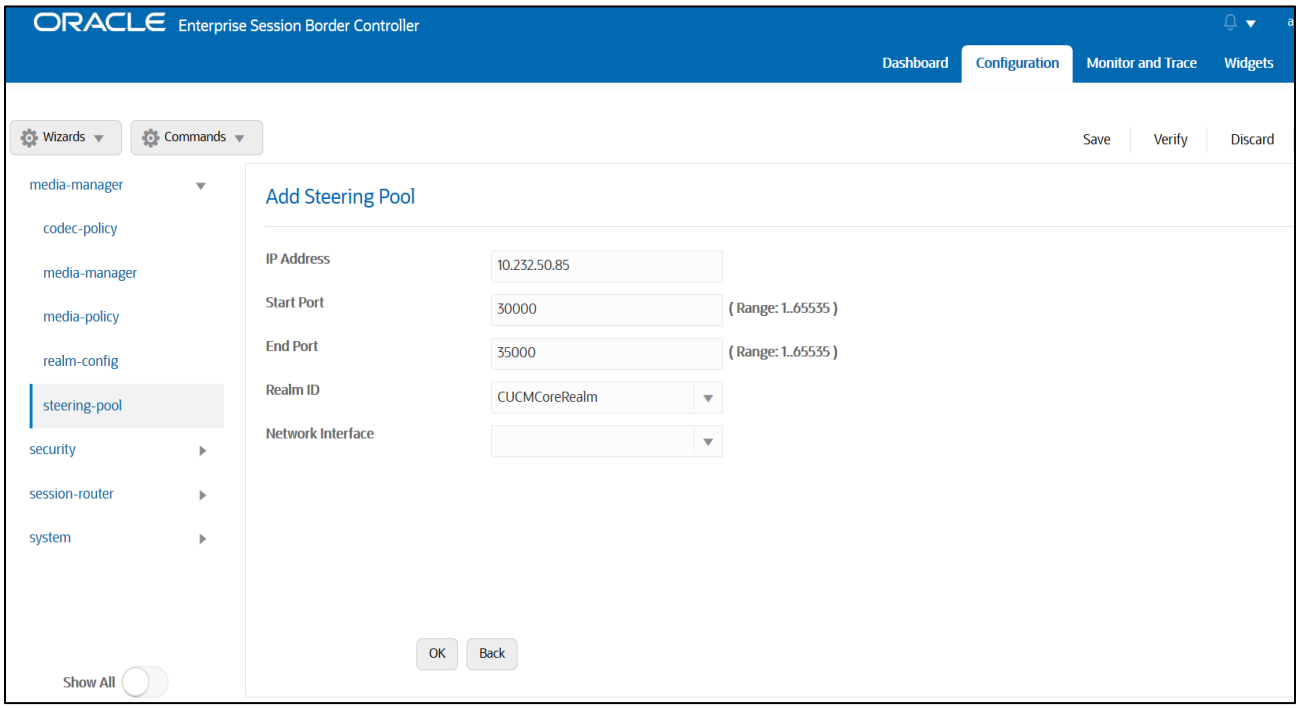
7.5. Configure steering-pool

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

Cisco Access side steering pool.



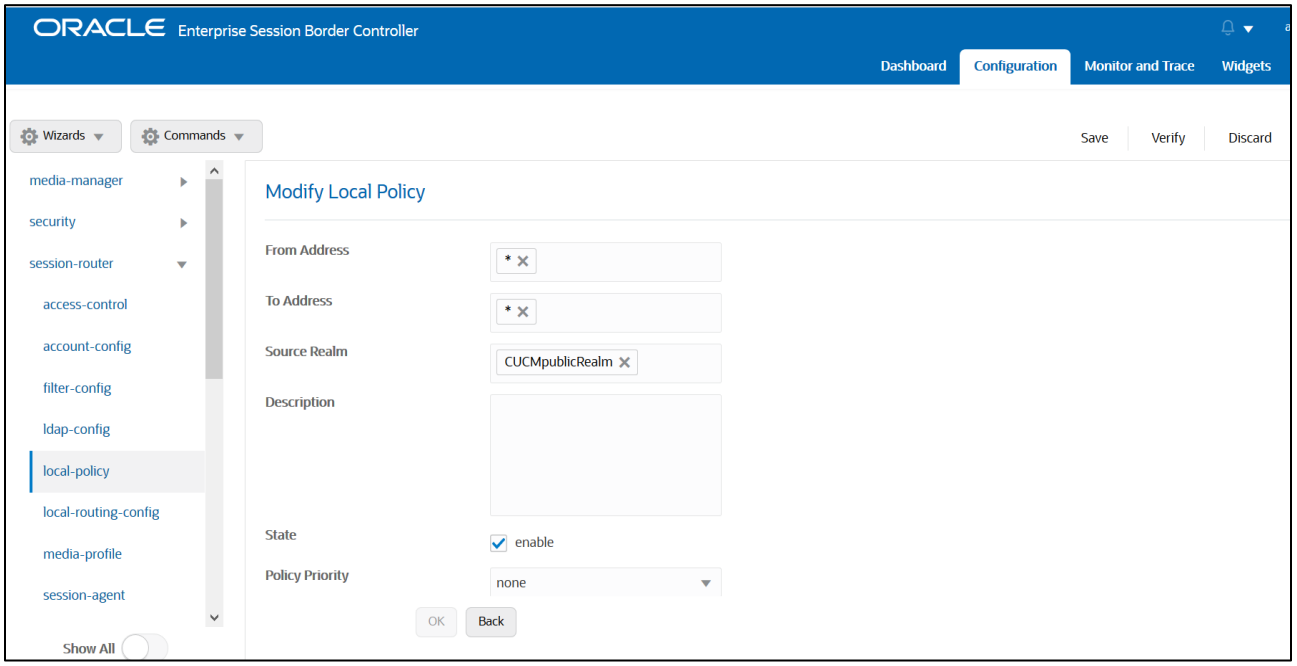
Cisco Core side steering pool.

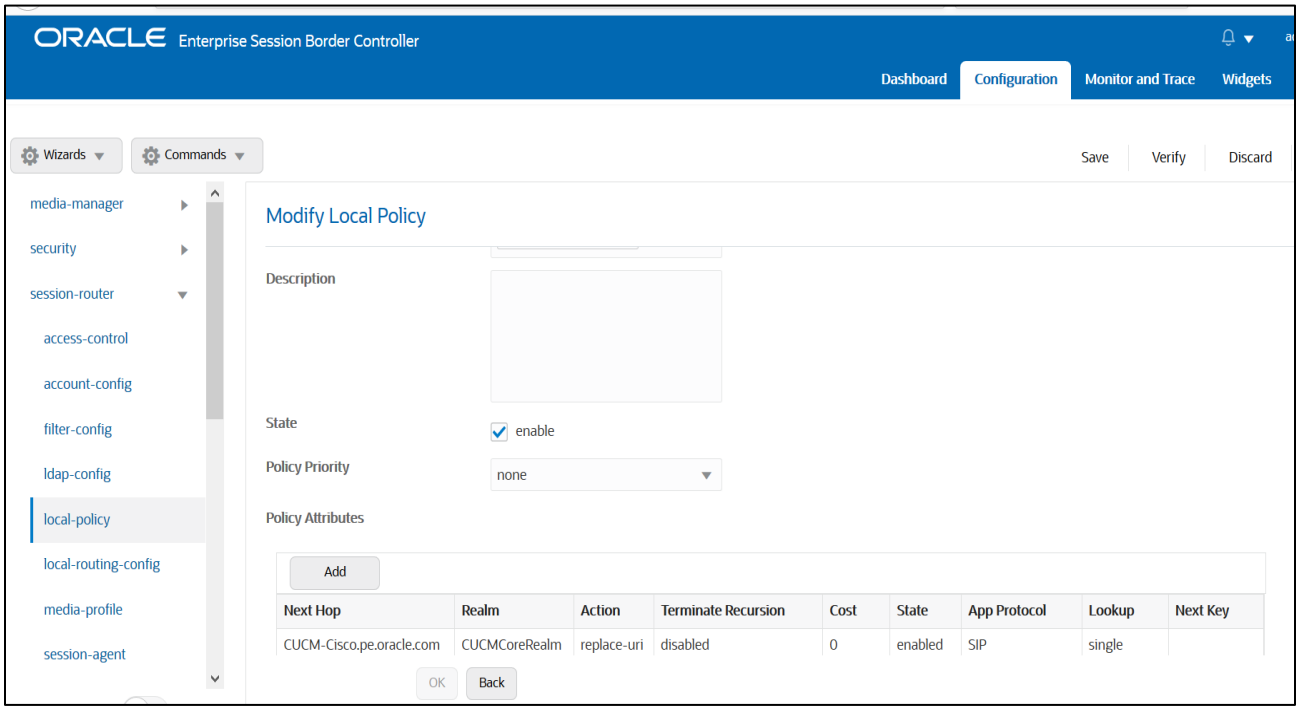


7.6. Configure local policy (Optional)

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 Access side to Cisco Core side and vice versa, Use the below local –policy





Cisco Offer less INVITE can happen in the Remote worker scenarios too.
In that case, please set the parameter "**Add SDP Invite**" as both and "**Add SDP profiles**" under Cisco Access side sip-interface. The configuration is similar to what we have done in Sec 6.13.

8. New SBC config/Deployment Using Configuration Assistant

When you first log on to the E-SBC, the system requires you to set the configuration parameters necessary for basic operation. To help you set the initial configuration with minimal effort, the E-SBC provides the Configuration Assistant. The Configuration Assistant, which you can run from the Web GUI or the Acme Command Line Interface (ACLI), asks you questions and uses your answers to set parameters for managing and securing call traffic. You can use the Configuration Assistant for the initial set up to make to the basic configuration. Please check "Configuration Assistant Operations" in the Web GUI User Guide and "Configuration Assistant Workflow and Checklist" in the ACLI Configuration Guide

Please note, applying a configuration to the SBC via the Configuration Assistant will overwrite any existing configuration currently applied to the SBC. **We highly recommend this only be used for initial setup of the SBC. This feature is not recommended to be used to make changes to existing configurations.**

8.1. Section Overview and Requirements

This section describes how to use our Configuration Assistant feature as a quick and simple way to configure the Oracle SBC for integration with Cisco Call Manager and Generic SIP Trunking. The pre-requisite is given below.

- SBC running release SCZ840p7 or later which will have this template package by default added to the SBC code.

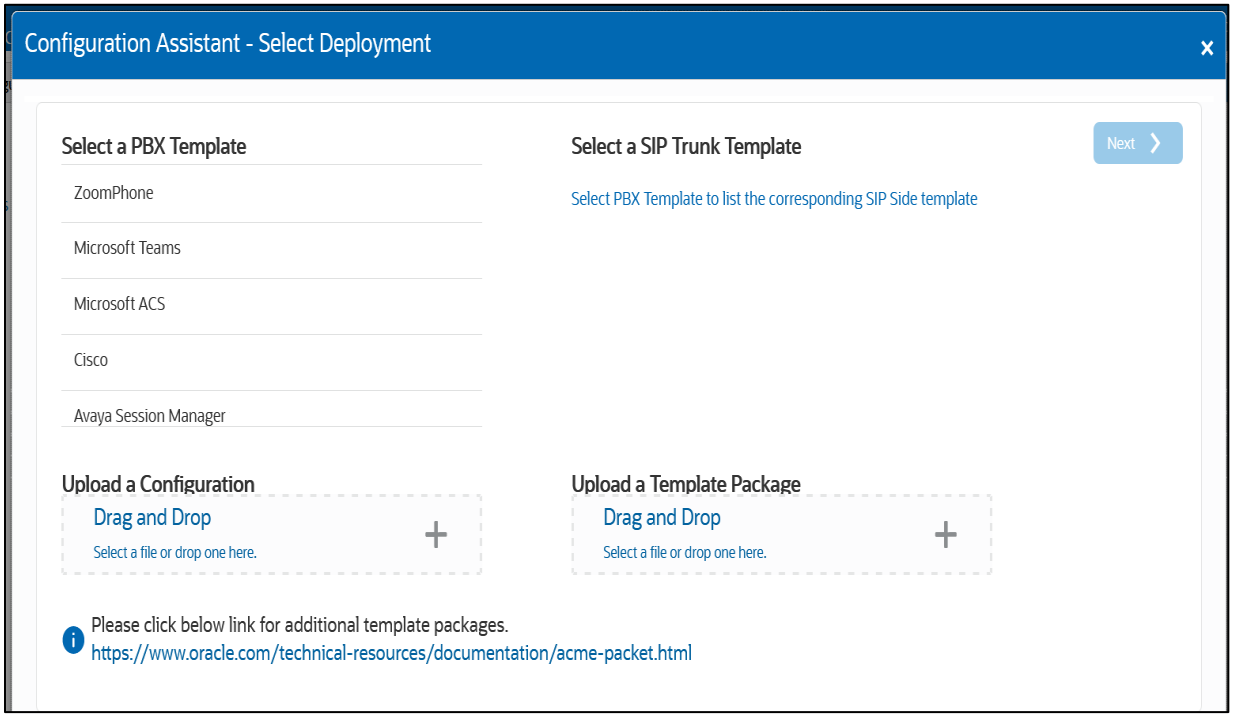
The following outline assumes you have established initial access to the SBC via console and completed the following steps:

- Configured boot parameters for management access
- Setup Product
- Set Entitlements
- Configured HTTP-Server to establish access to SBC GUI

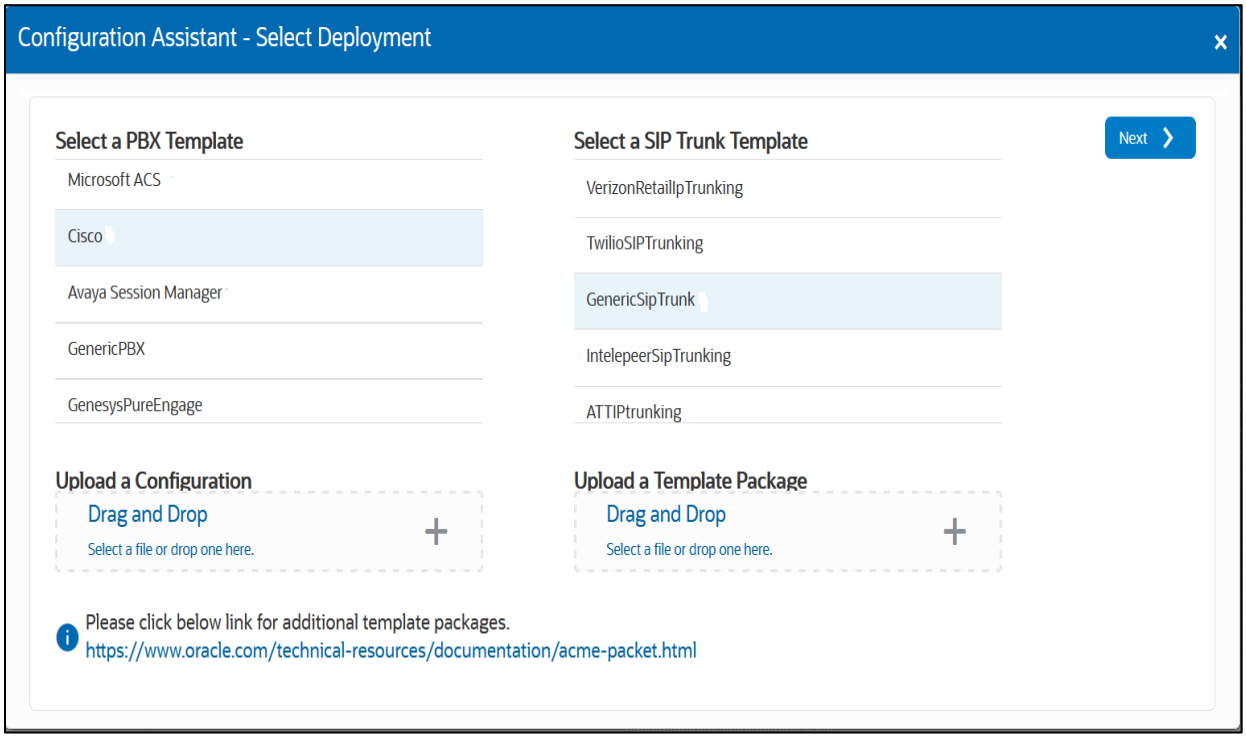
8.2. Initial GUI Access

The Oracle SBC WebGui can be accessed by entering the following in your web browser: http(s)://<SBC Management IP>.

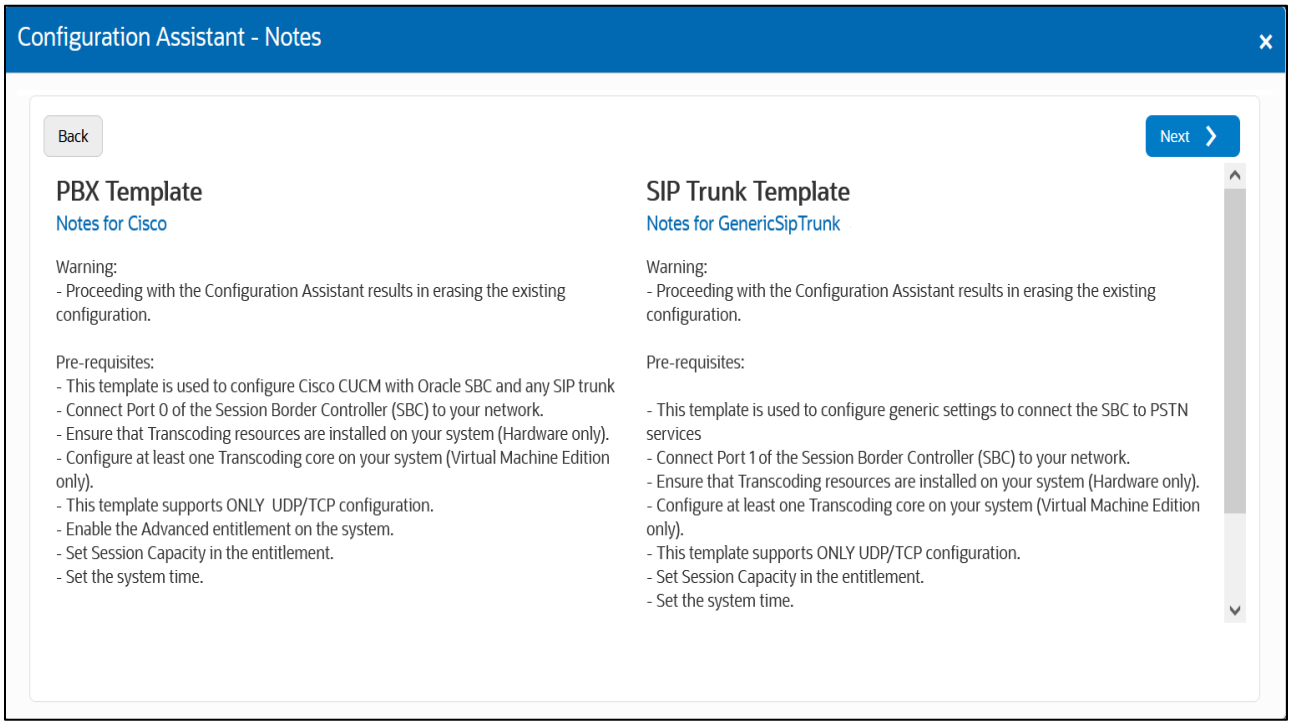
The username and password are the same as that of the CLI.
If there is no configuration on the SBC, the configuration assistant will show immediately upon login to the SBC GUI as shown below



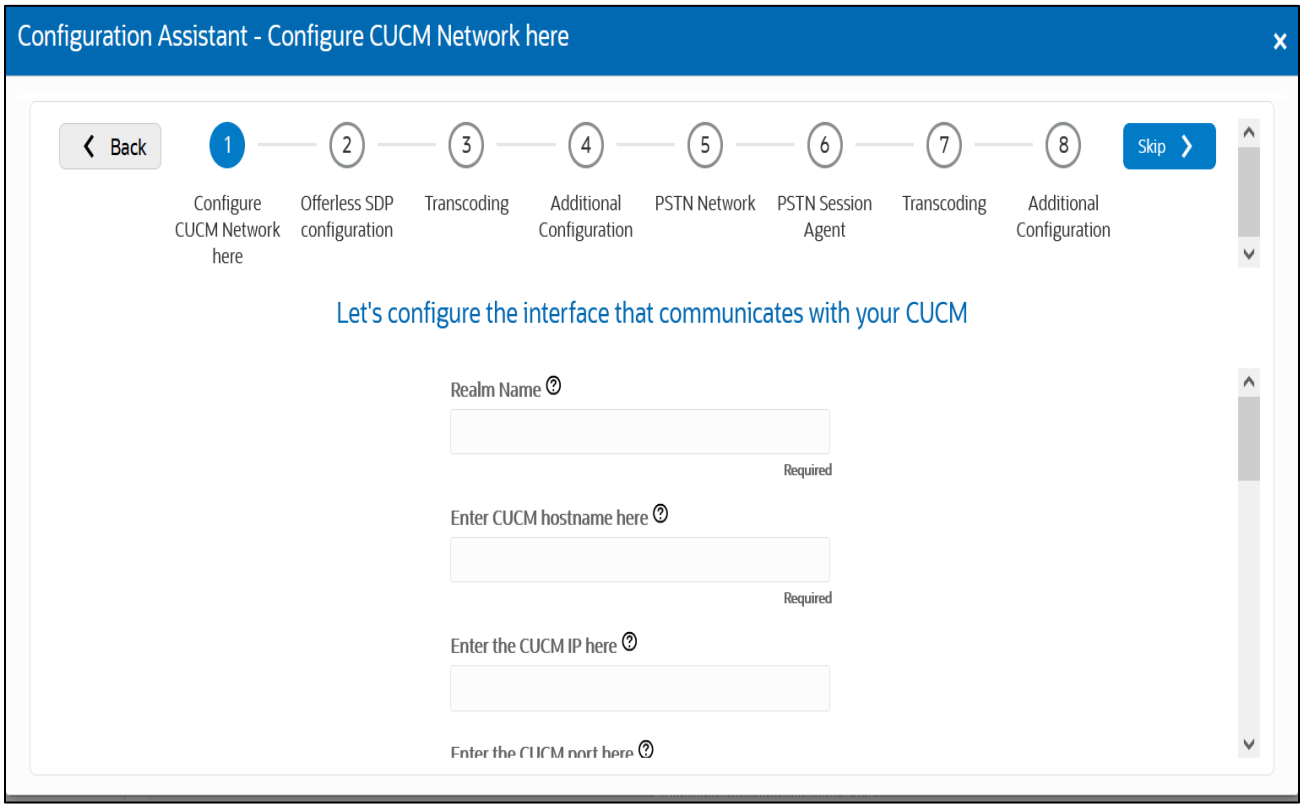
As we can see, there are some templates of PBX populated in the template and we can select the PBX template that we want to use with Generic SIP trunk and for this document, we have selected Cisco template and once we select that, it asks us to select the SIP trunk template. After we select Generic SIP trunk template, the Next option would be enabled.



Click *Next*: The following “Notes” will be displayed related to pre-requisite



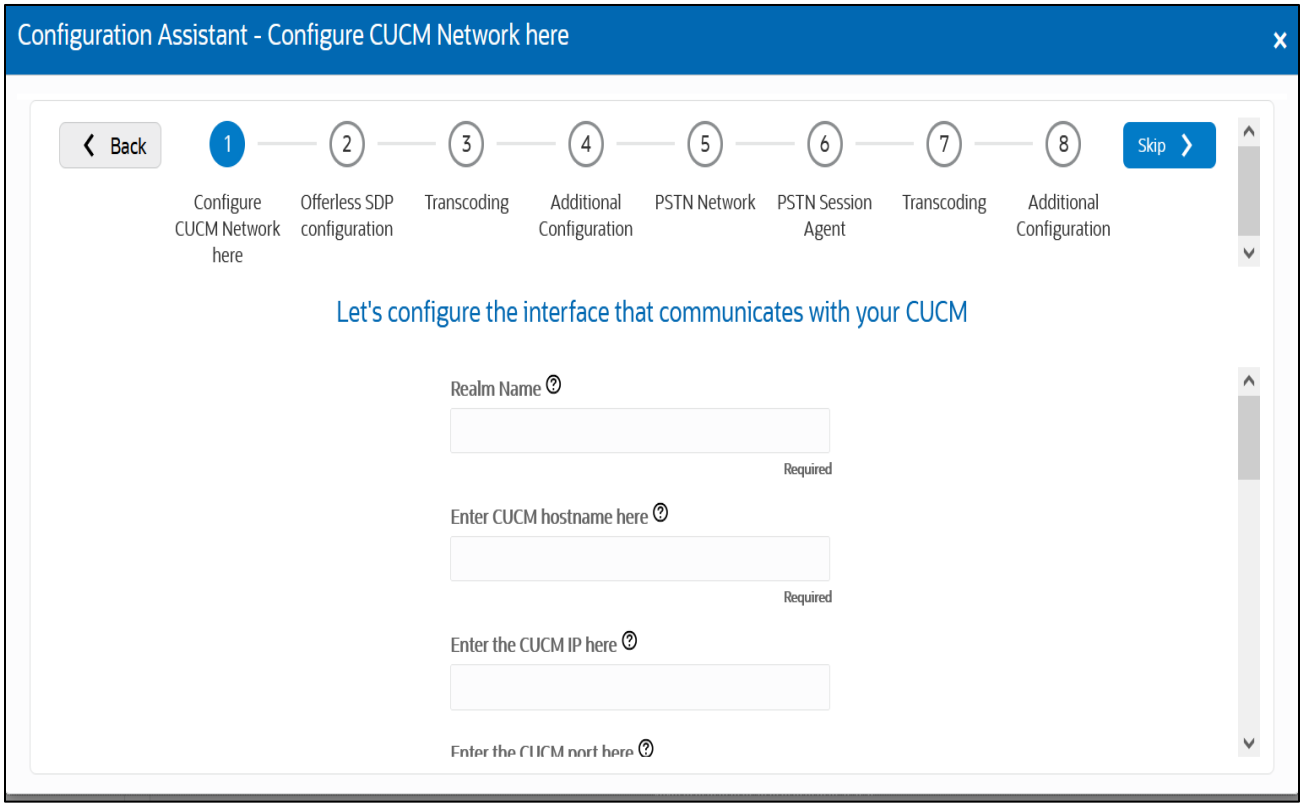
Click *Next* and we get the below screen where we need to enter the details for SBC configuration.



8.3. Configuration Assistant Template Navigation

8.3.1. Page 1-Cisco Call Manager (CUCM) Network

Page 1 of the template is where you will configure the network information to connect Cisco Call Manager. On this page, we will enter the CUCM hostname, IP and port which will be the next hop IP address/hostname for sip signaling to and from your CUCM

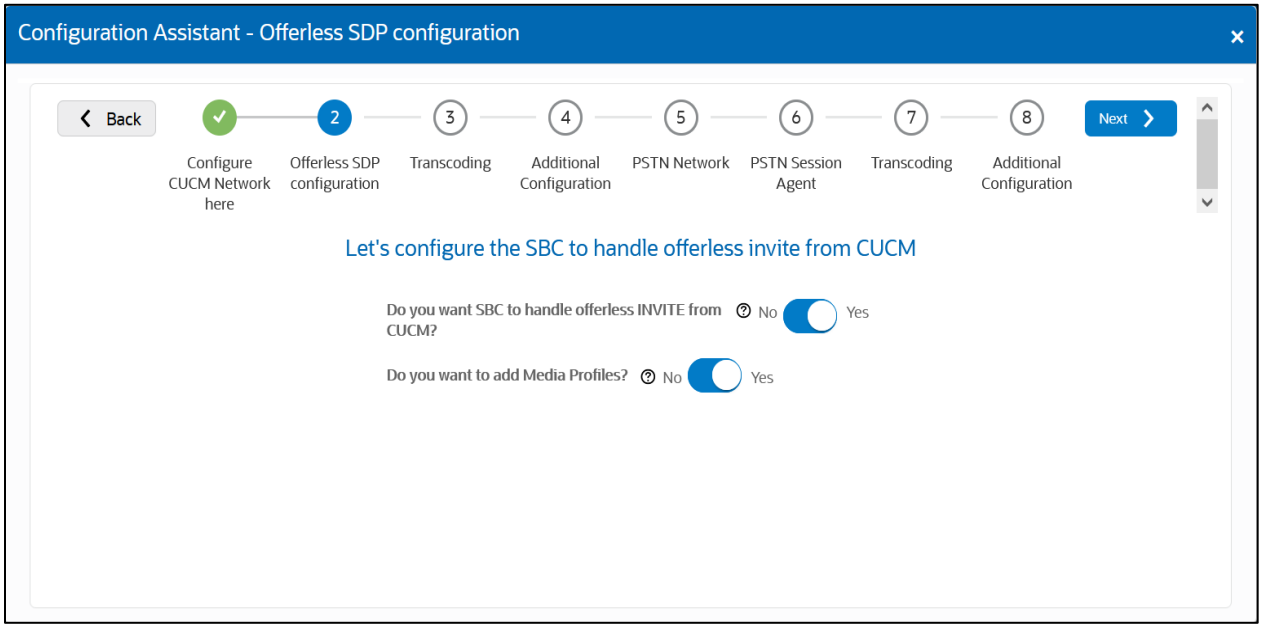


Next to each field is a help icon. If you hover over the icon, you will be provided with a description or definition of each filed. Also, pay close attention to which fields are listed as “required”.

8.3.2. Page 2-Offerless SDP Invite

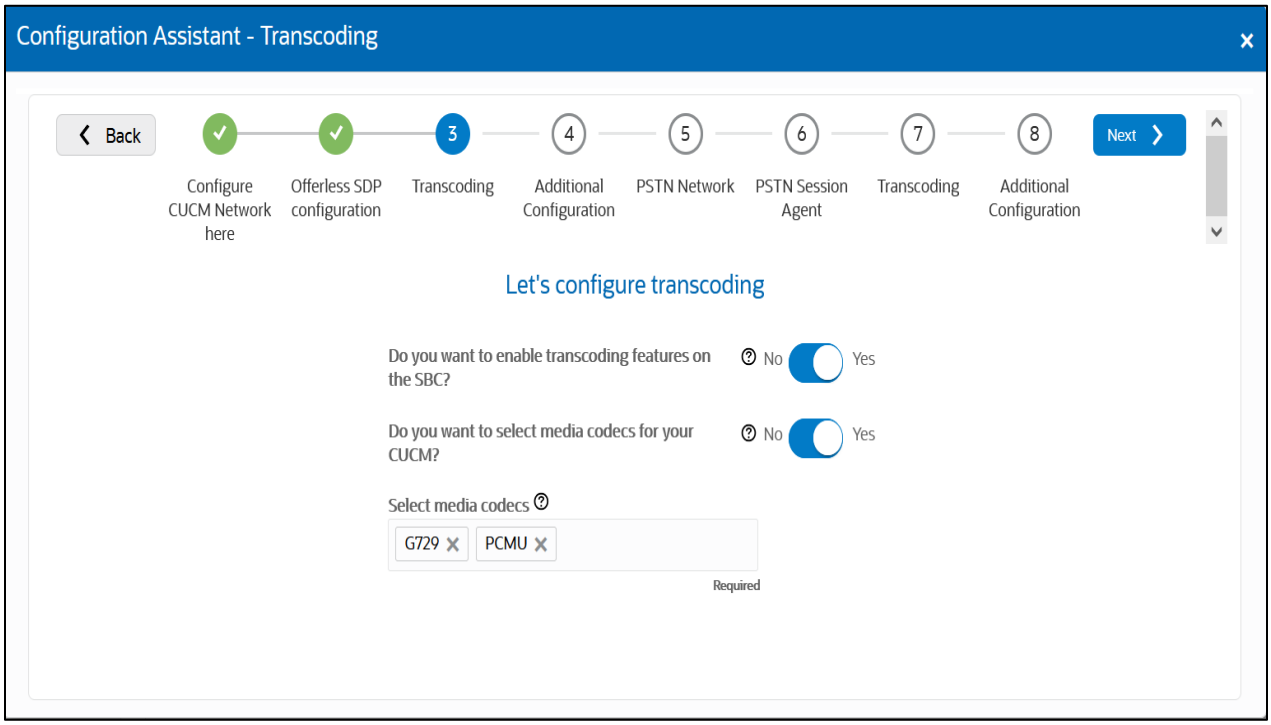
Page 2 of the template is where you will configure the information related to Cisco’s offer less SDP Invite configuration. You can enable or disable the configuration through the Yes/No Radio Button.

Note Click on the ? icon to know more about the configuration parameters and their usage.



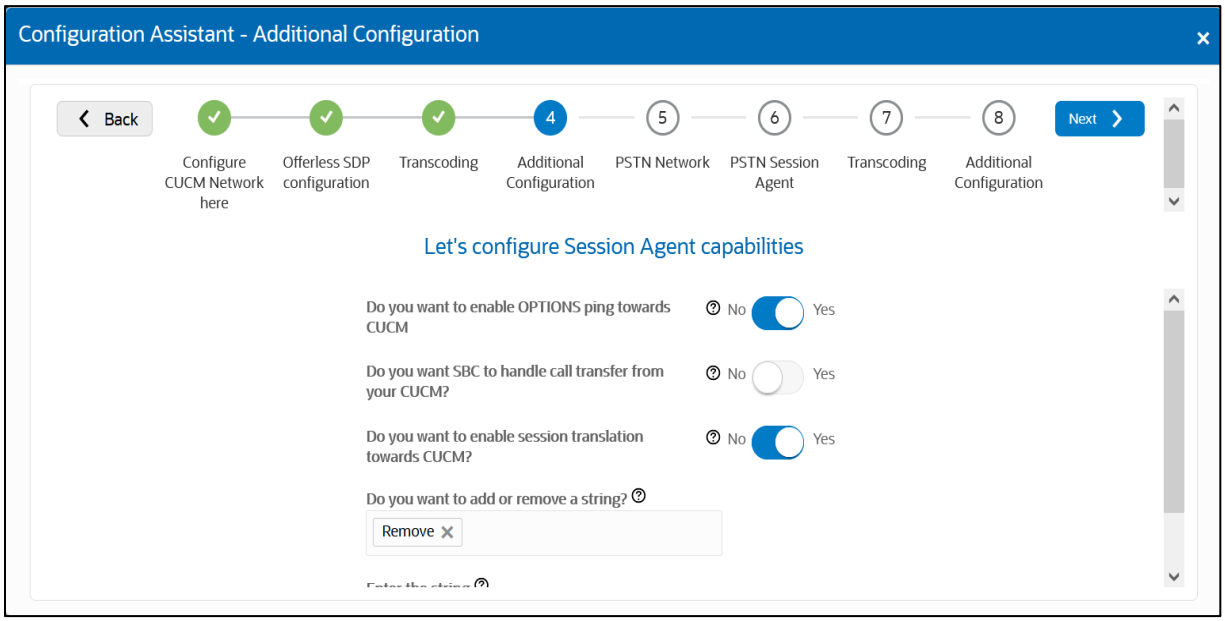
8.3.3. Page 3 - Cisco side Transcoding

Page 3 is where you will be able to configure transcoding between the SBC and Cisco Call Manager. Once transcoding features is set to “yes”, you will then have an option to select additional media codecs you want included in offers/answers towards Cisco Call Manger. If you select yes to either question regarding media codecs, you will be presented with a required drop down. You can select as many codecs from the list presented.



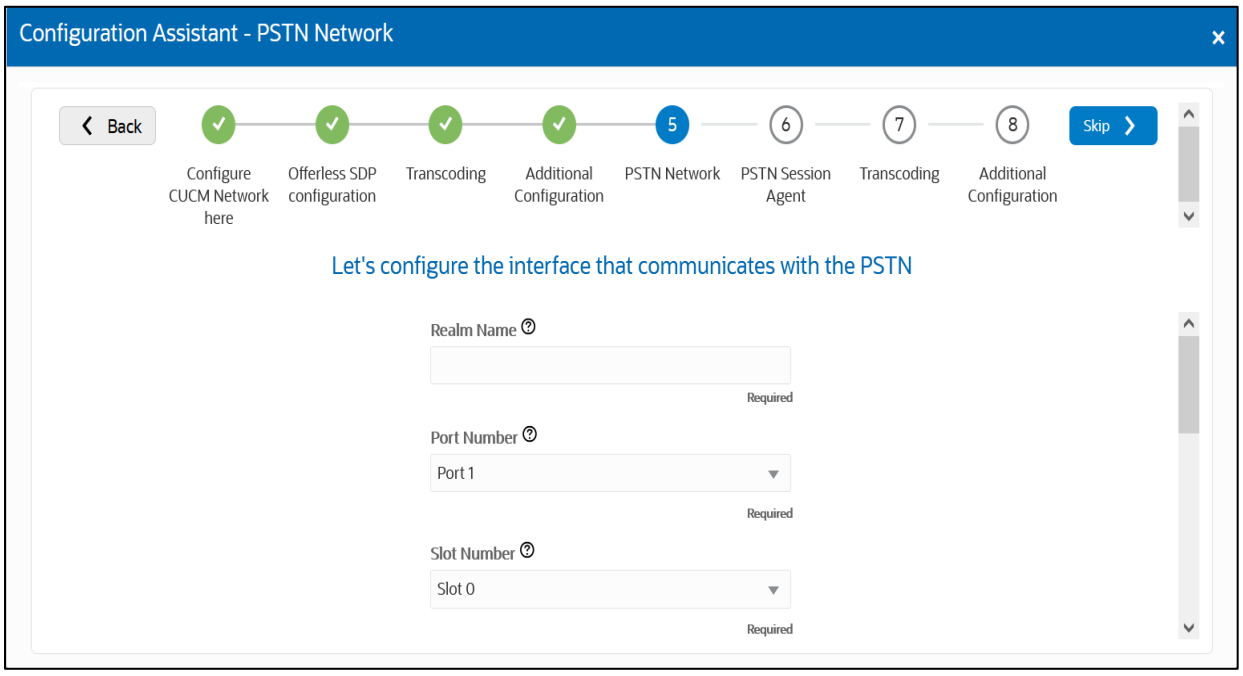
8.3.4. Page 4 - Cisco side Additional Configuration

Page 4 is where you will be able to configure Session Agent Capabilities towards CUCM side. This includes enabling OPTIONS, enabling session translation etc towards CUCM side as shown below. . You can enable or disable the configuration through the Yes/No Radio Button



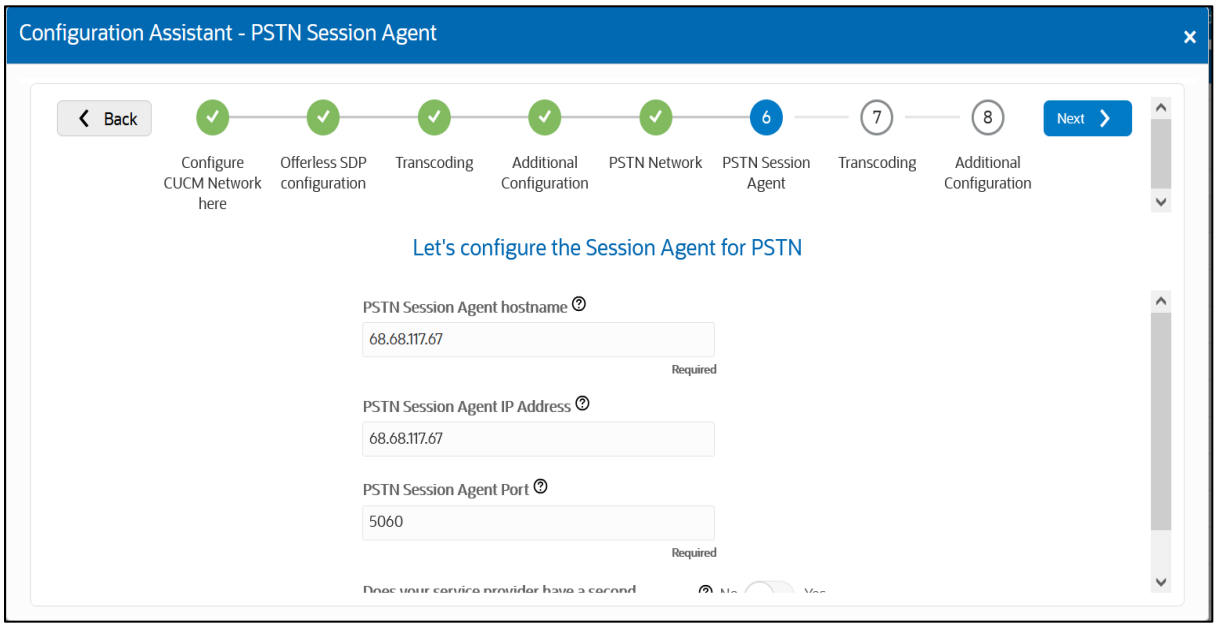
8.3.5. Page 5 - Generic SIP Trunk Network

Page 5 of the template is where you will configure the network information to connect to Generic SIP trunk Network (PSTN side). Please fill the required fields and Press Next.



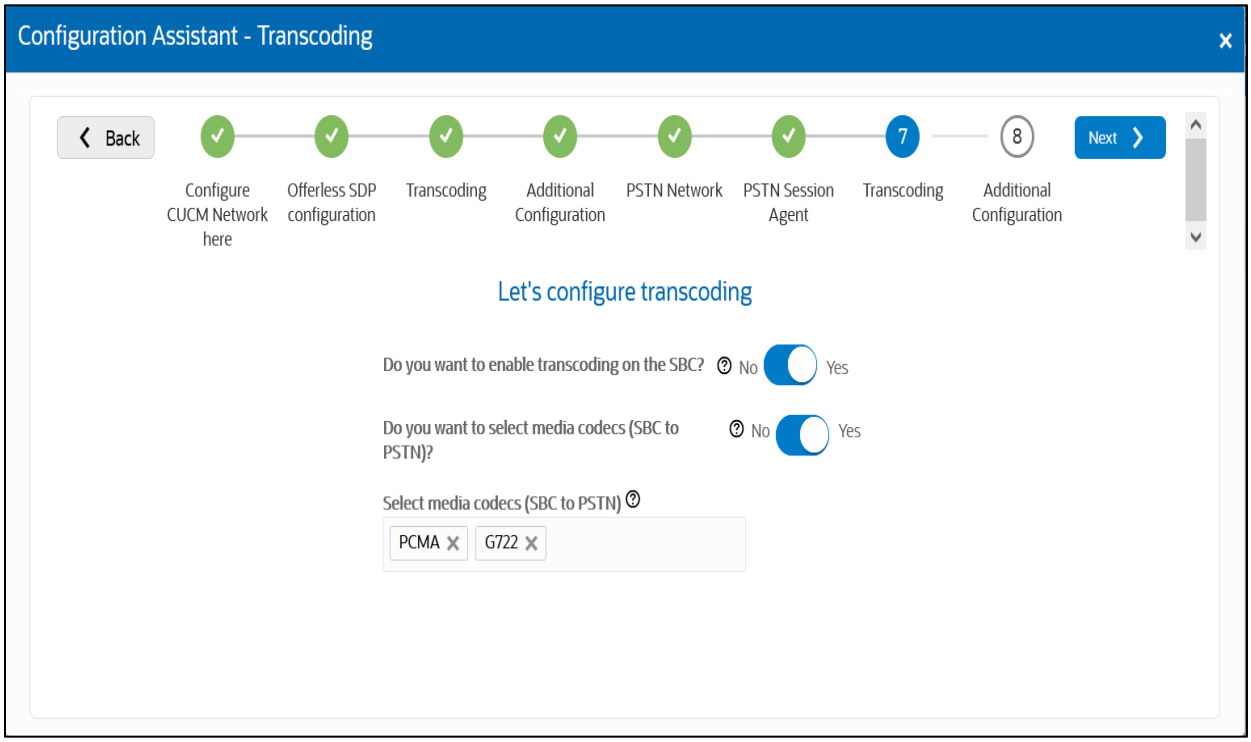
8.3.6. Page 6 – PSTN Session Agent

Page 6 of the template is where you will configure the PSTN Session Agent details where you will enter the next hop IP address and port for sip signaling to and from your Generic SIP trunk. Please fill the required fields and click Next.



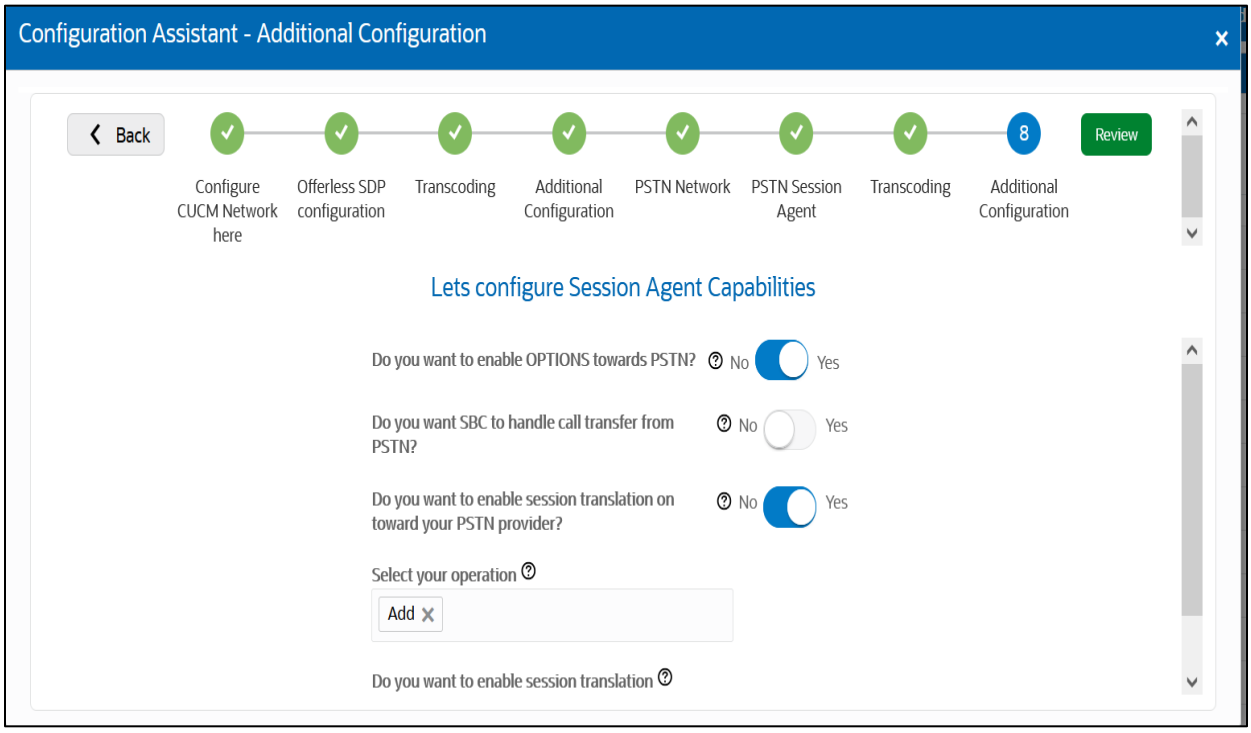
8.3.7. Page 7 – PSTN side Transcoding

Page 7 is where you will be able to configure transcoding between the SBC and Generic SIP Trunk. Once transcoding features is set to “yes”, you will then have an option to select additional media codecs you want included in offers/answers towars PSTN side. If you select yes to either question regarding media codecs, you will be presented with a required drop down. You can select as many codecs from the list presented.



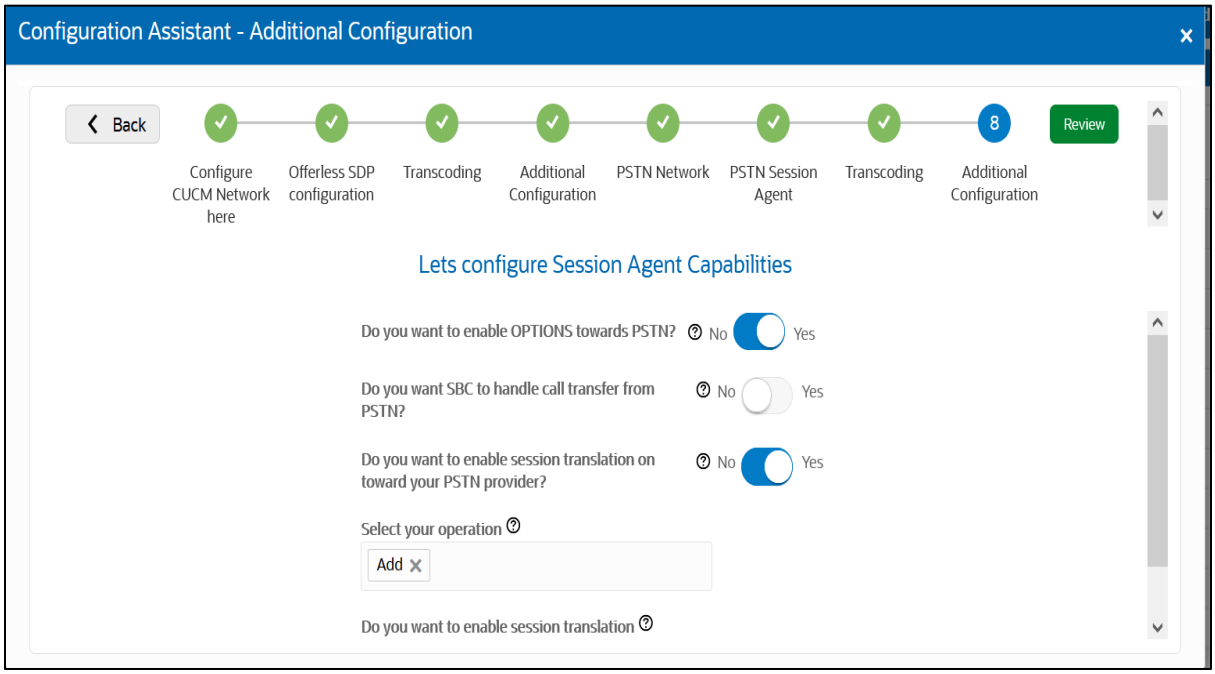
8.3.8. Page 8 – PSTN side Additional Configuration

Page 8 is where you will be able to configure Session Agent Capabilities towards PSTN side. This includes enabling OPTIONS, enabling session translation etc towards PSTN side as shown below. You can enable or disable the configuration through the Yes/No Radio Button

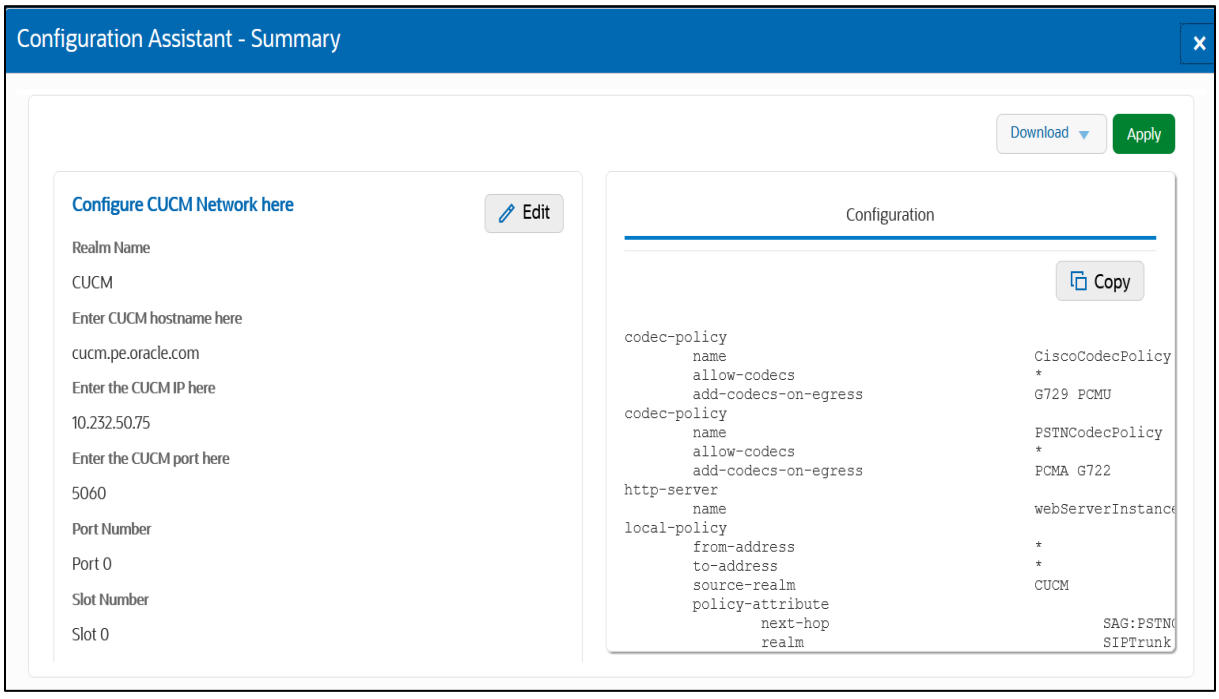


8.4. Review

At the end of the template, you will notice in the top right, a "*Review*" tab. If all 8 pages presented across the top are showing green, indicting there are no errors with the information entered, click on the "Review" tab.



The screen looks like below after clicking the Review Tab.

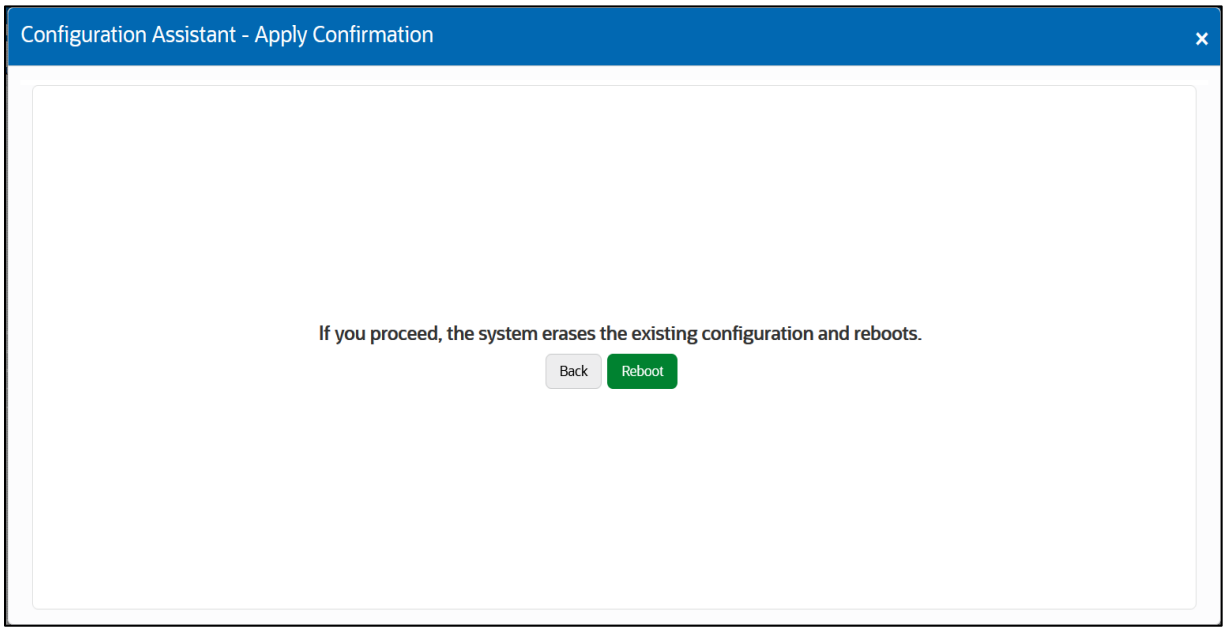


On the left side of the review contains the entries for each page. Each page has an "*Edit*" tab that can be used to make changes to the information entered on that specific page without having to go through the entire template again.

On the right side of the review page, under the "*Configuration*" tab is the ACLI output from the SBC. This is the complete configuration of the SBC based on the information entered throughout the template.

8.5. Download and/or Apply

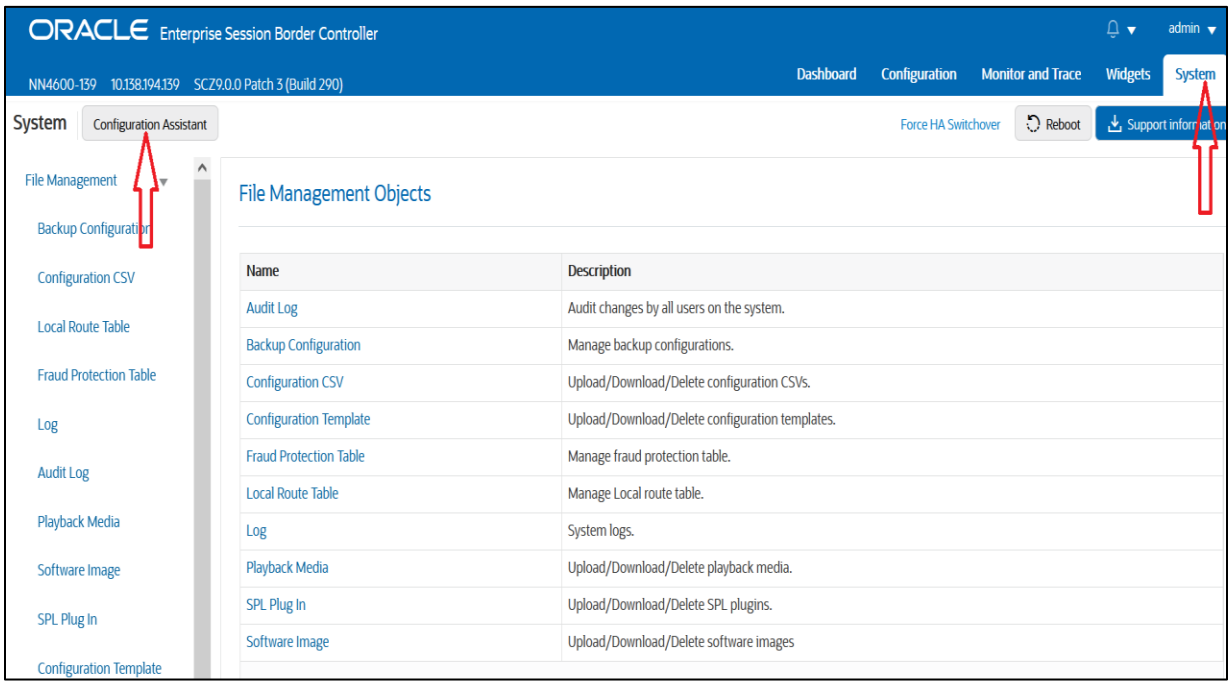
Now that the entries provided throughout the template have been reviewed, the template provides you with the ability to "Download" the config by clicking the "*Download*" tab on the top right. Next, click the "*Apply*" button on the top right, and you will see the following pop-up box appear.



Now you can click "*Reboot*" to confirm you want to apply the configuration to the SBC. The SBC will reboot. When it comes back up, the SBC will have a basic configuration in place for Cisco Call Manager with Generic SIP trunking.

8.6. Configuration Assistant Access

Upon initial login, if the Configuration Assistant Template does not immediately appear on the screen, you can access by clicking on the "*SYSTEM*" tab, top right of your screen. After that, click on the "*Configuration Assistant*" tab, top left. This allows end users to access the Configuration Assistance at any time through the SBC GUI.



9. Existing SBC configuration

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

- New realm-config
- New sip-interface
- New session-agent
- New steering-pools
- New local-policy
- New Translation Rules
- Session Translation Rules

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

Appendix A

Following are the test cases that are executed between Cisco User with the Generic SIP Trunk (PSTN user). **Please note that Cisco User here refers both Cisco User inside Enterprise network as well as Cisco Remote worker.**

Serial Number	Test Cases Executed	Result
1	Cisco user disconnects an inbound connected call	Pass
2	Cisco user disconnects an outbound connected call	Pass
3	Generic SIP Trunk user disconnects an inbound connected call	Pass
4	Generic SIP Trunk User disconnects an outbound connected call	Pass
5	Cisco user places inbound call from Generic SIP Trunk user on hold and then resumes	Pass
6	Cisco user makes outbound call to Generic SIP Trunk user and put that call on hold and then resumes	Pass
7	Generic SIP Trunk user places inbound call from Cisco user on hold and then resumes	Pass
8	Generic SIP Trunk user makes outbound call to Cisco user and put that call on hold and then resumes	Pass
9	Cisco user places inbound call from Generic SIP Trunk user on hold for over 15/30 minutes and then resumes	Pass
10	Cisco user makes outbound call to Generic SIP Trunk user and places the call on hold for over 15/30 minutes and then resumes	Pass
11	Inbound Generic SIP Trunk call to Cisco blind transferred to second Cisco/ PSTN User	Pass
12	Outbound Generic SIP Trunk call from Cisco user blind transferred to second Cisco/ PSTN User	Pass
13	Inbound Generic SIP Trunk Call to Cisco consultatively transferred to Cisco/ PSTN User	Pass
14	Outbound Generic SIP Trunk call from Cisco user consultatively transferred to Cisco/ PSTN User	Pass
15	Cisco user makes outbound call to Generic SIP Trunk user and makes a conference call by adding another Cisco/ PSTN user.	Pass
16	Generic SIP Trunk user makes outbound call to Cisco user and Cisco user makes a conference call by adding another Cisco/ PSTN user.	Pass

17	Cisco user mutes inbound call from Generic SIP Trunk user and then unmutes	Pass
18	Cisco user mutes outbound call made to Generic SIP Trunk user and then unmutes	Pass
19	Generic SIP Trunk user mutes inbound call from Cisco user and then unmutes	Pass
20	Generic SIP Trunk user mutes outbound call made to Cisco user and then unmutes	Pass
21	Generic SIP Trunk User disconnects outbound call to Cisco user before it is answered	Pass
22	Cisco user disconnects outbound call to Generic SIP Trunk user before it is answered	Pass

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

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615