Oracle SBC integration with Cisco Call Manager (CUCM) and Zoom Phone Premise Peering (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

Revision	**Description of Changes**	**Date Revision Completed**
1.0	Oracle SBC integration with Cisco CUCM and Zoom Phone Premise Peering (BYOC)	22nd May 2022
1.1	Updated the certificate related information for Zoom (using DigiCert G2 and G3 root certificate as their primary Root Certificate for TLS negotiation)	10th November 2023

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). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform, Cisco Call Manager (Cisco CUCM) along with Zoom Phone-Premise Peering - BYOC.

2. Document Overview

This Oracle technical application note outlines the configuration needed to set up the interworking between on premises Cisco CUCM using Oracle SBC and Zoom BYOC. The solution contained within this document has been tested using Oracle Communication SBC **900p3** version. Our scope of this document is testing the interoperability of Oracle SBC with CUCM and Zoom BYOC.

In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the Zoom BYOC and CUCM 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.

Please find the related documentation links below:

2.1**.** Zoom BYOC

https://Zoom.us/docs/doc/Zoom-Bring%20Your%20Own%20Carrier.pdf

https://Zoom.us/phonesystem

https://Zoom.us/Zoom-phone-features

2.2**.** 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 and Zoom BYOC. 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, TLS/SRTP are also necessary to complete the configuration and for troubleshooting, if necessary.

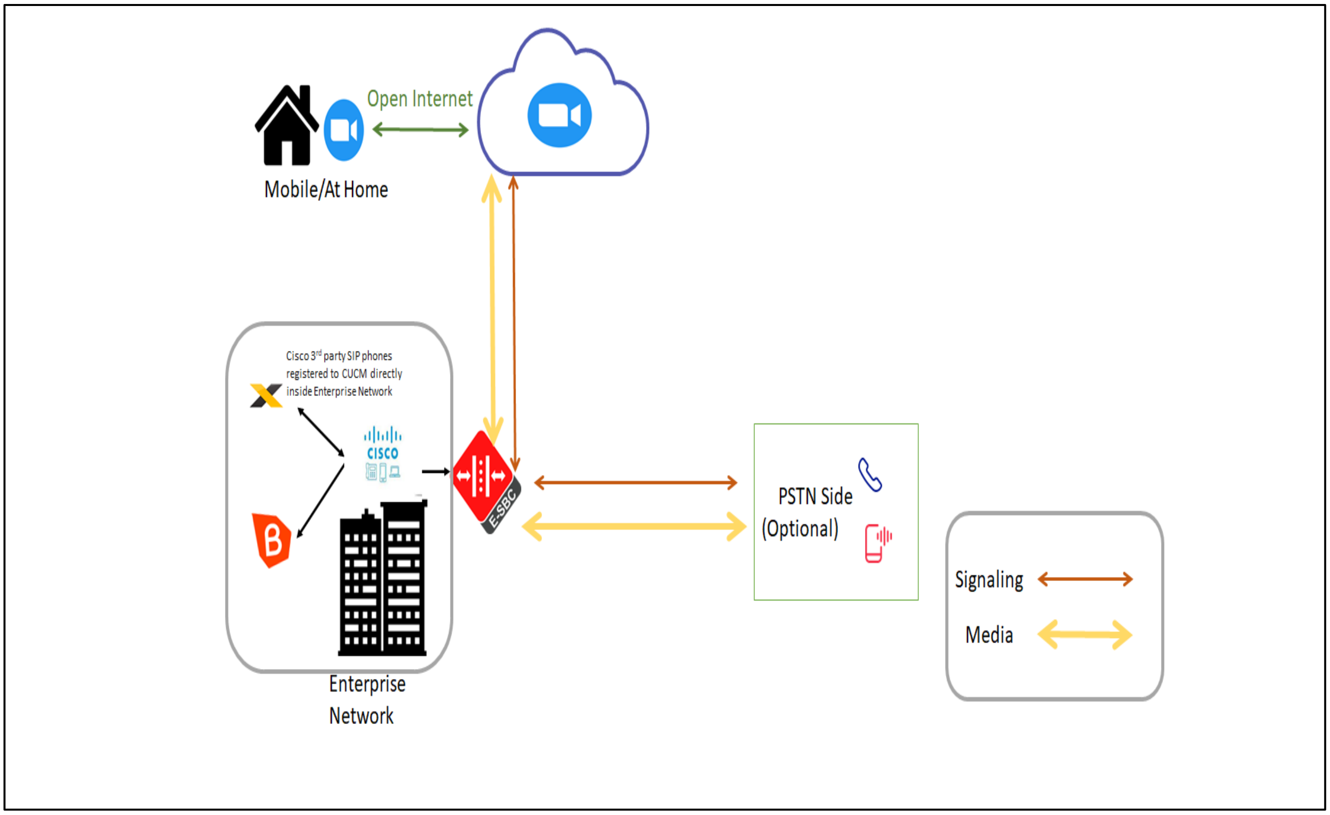
3.2. Requirements

- Fully functioning Cisco Call Manager (CUCM) 12.5 version.
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 9.0.0 version
- Zoom Phone subscription running Zoom Client.

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	Zoom Client version
Revision 1	9.0.0	12.5	Version: 5.10.6 (5263)

3.3. Architecture



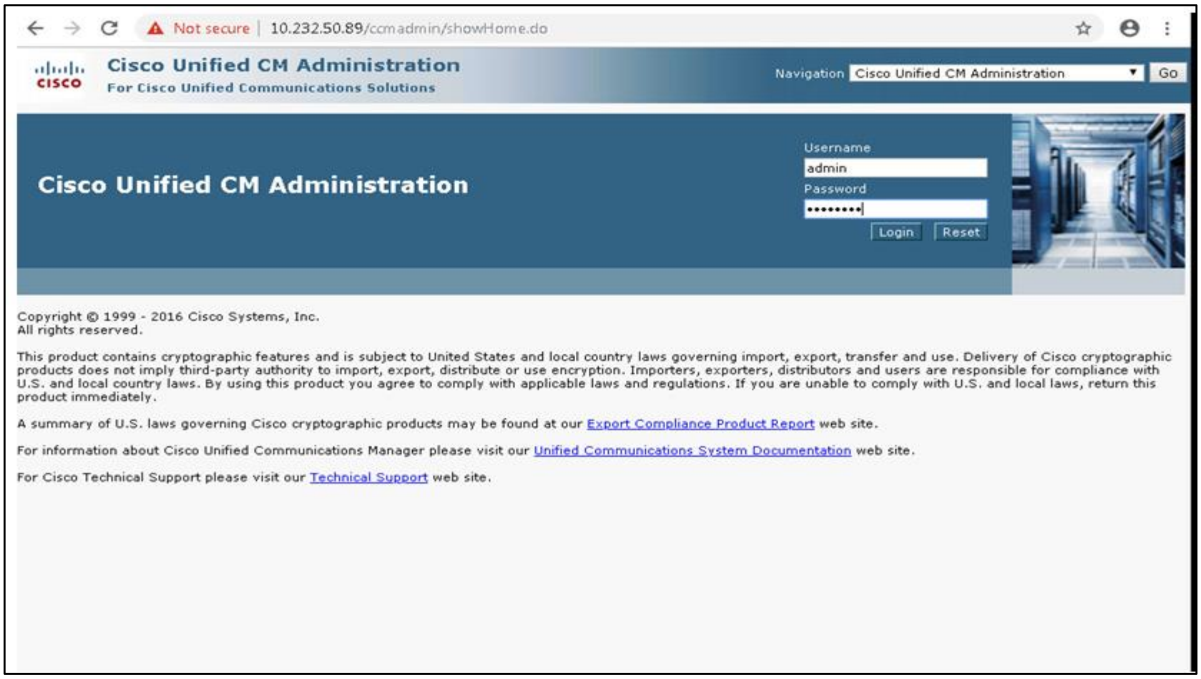
The PSTN part shown in the network architecture is not covered in this document (Out of scope for this document) and the end user can configure the PSTN part if they need it as per their requirements.

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

- Phase 1 – Configuring the Cisco Unified Call Manager v12.5 for Oracle SBC.
- Phase 2 – Configuring the Zoom BYOC.
- Phase 3 – 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.


Not secure
10.232.50.89/ccmadmin/showHome.do
cisco
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation
Cisco Unified CM Administration
Go
Cisco Unified CM Administration
Login
Reset

Username: admin

Password: ••••••••

Copyright © 1999 - 2016 Cisco Systems, Inc.
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

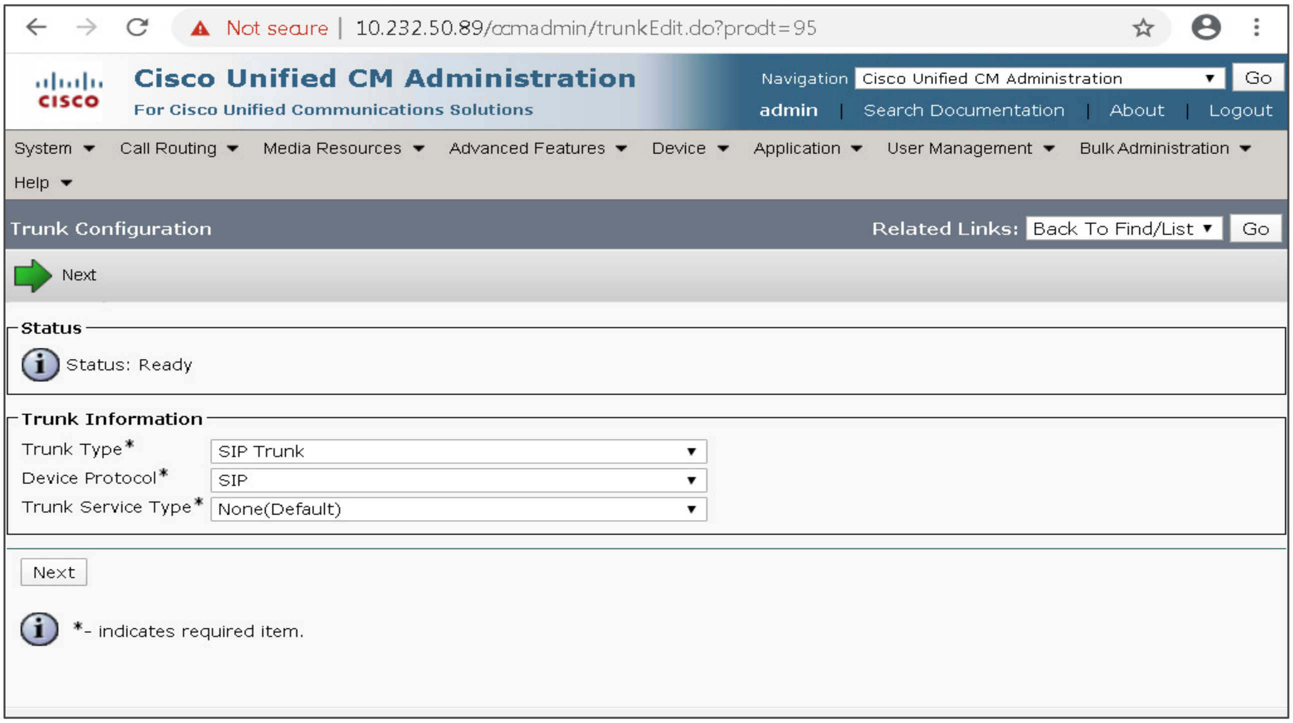
A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.

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
Related Links: Back To Find/List Go
Next

Trunk Configuration

Status

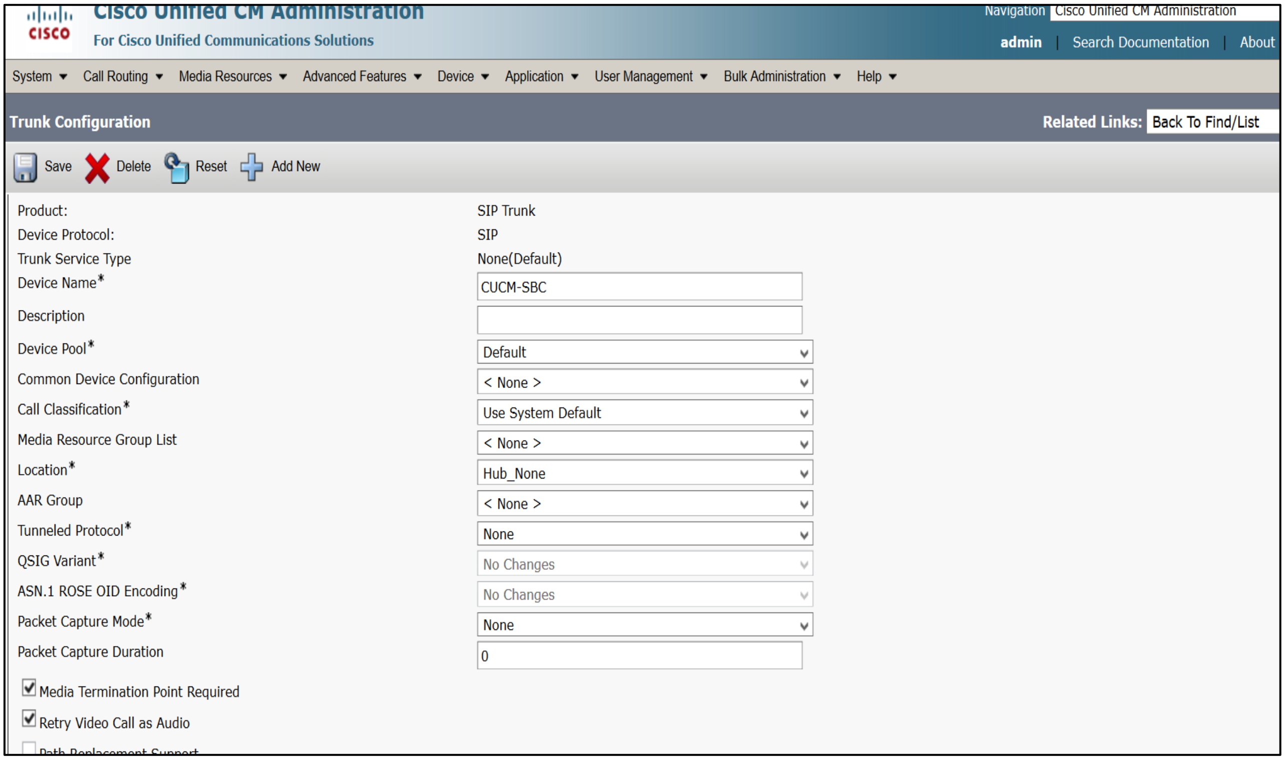
Status: Ready

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
Related Links: Back To Find/List
Save Delete Reset Add New

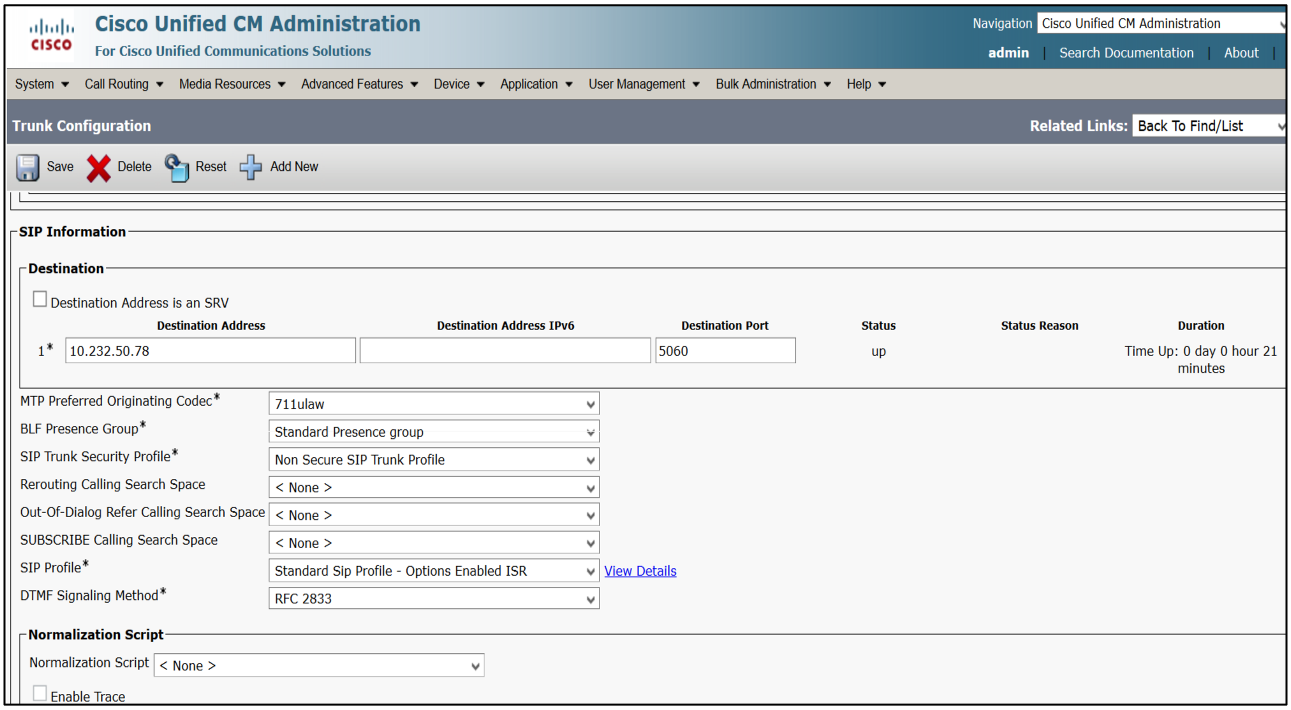
Trunk Configuration

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

□ Path Replacement Support


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
Related Links: Back To Find/List
Save Delete Reset Add New

Trunk Configuration

SIP Information

Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason	Duration
1*	10.232.50.78		5060	up		Time Up: 0 day 0 hour 21 minutes

MTP Preferred Originating Codec*	711ulaw
BLF Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard Sip Profile - Options Enabled ISR View Details
DTMF Signaling Method*	RFC 2833

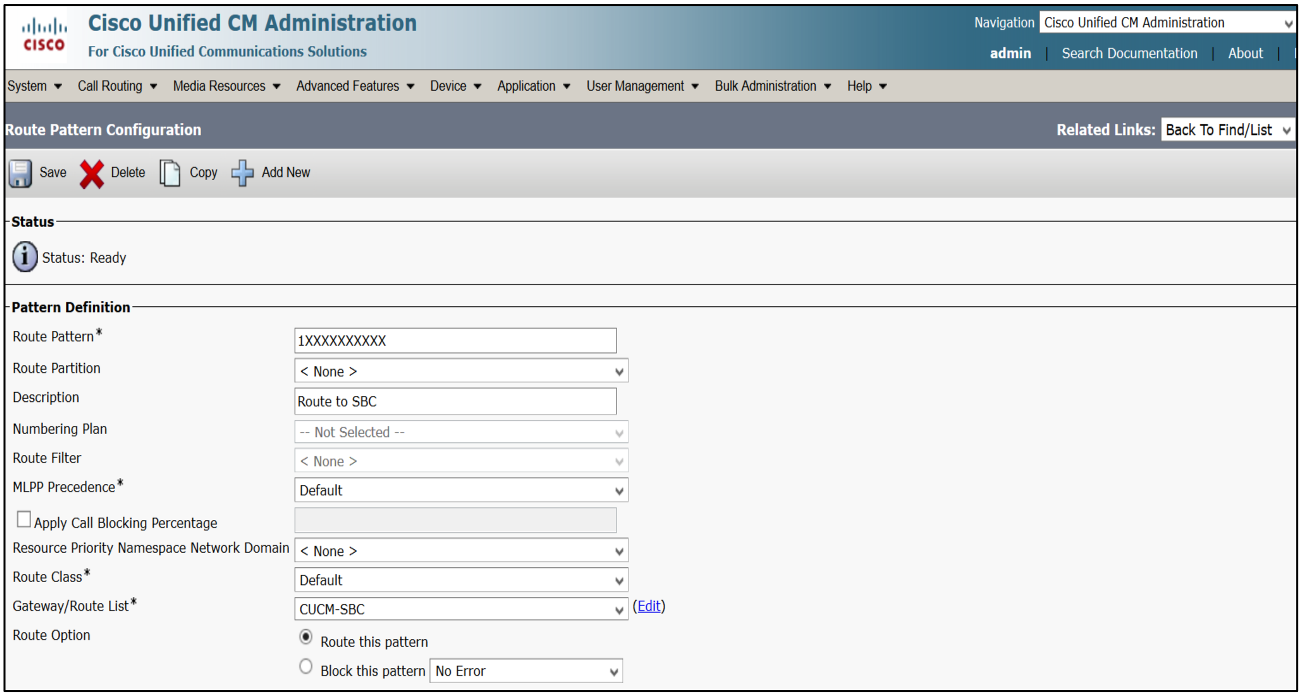
Normalization Script

Normalization Script < None >

□ Enable Trace

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.


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
Related Links: Back To Find/List
Save Delete Copy Add New

Route Pattern Configuration

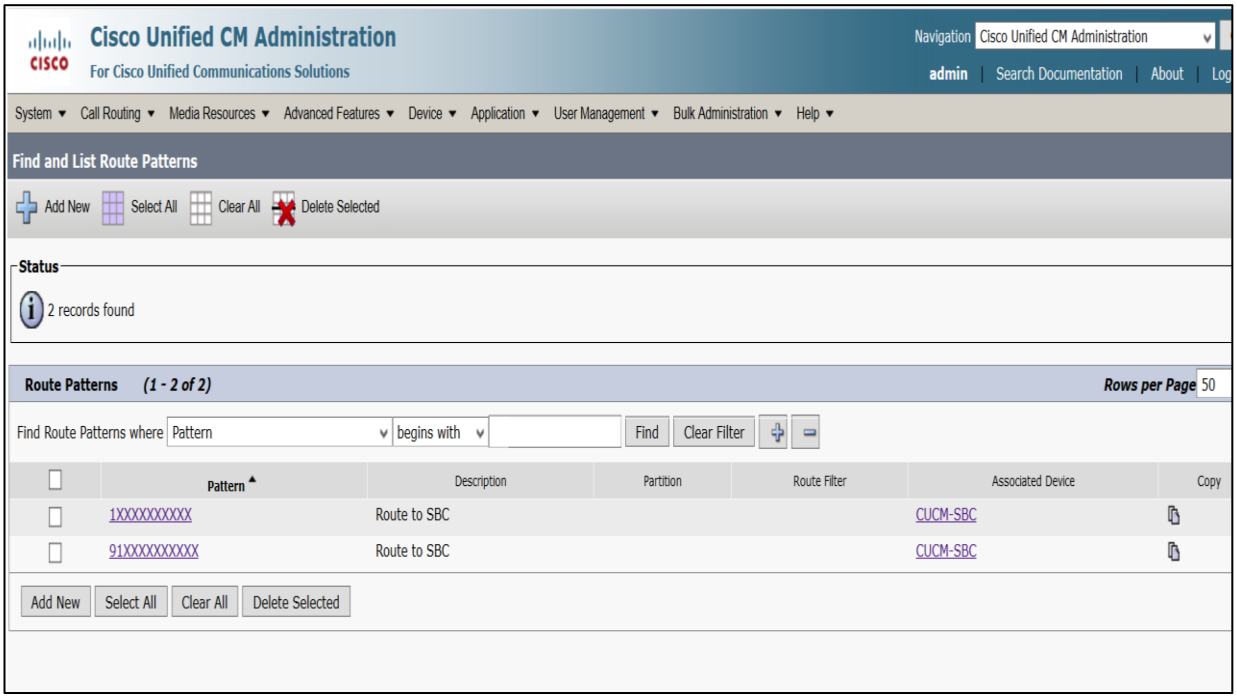
Status

Status: Ready

Pattern Definition

Route Pattern*	1XXXXXXXXXX
Route Partition	< None >
Description	Route to SBC
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
□ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	CUCM-SBC (Edit)
Route Option	● Route this pattern ○ Block this pattern No Error

The route patterns that has been created is shown below:



Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

admin | Search Documentation | About | Log
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Find and List Route Patterns

Add New
Select All
Clear All
Delete Selected

Status

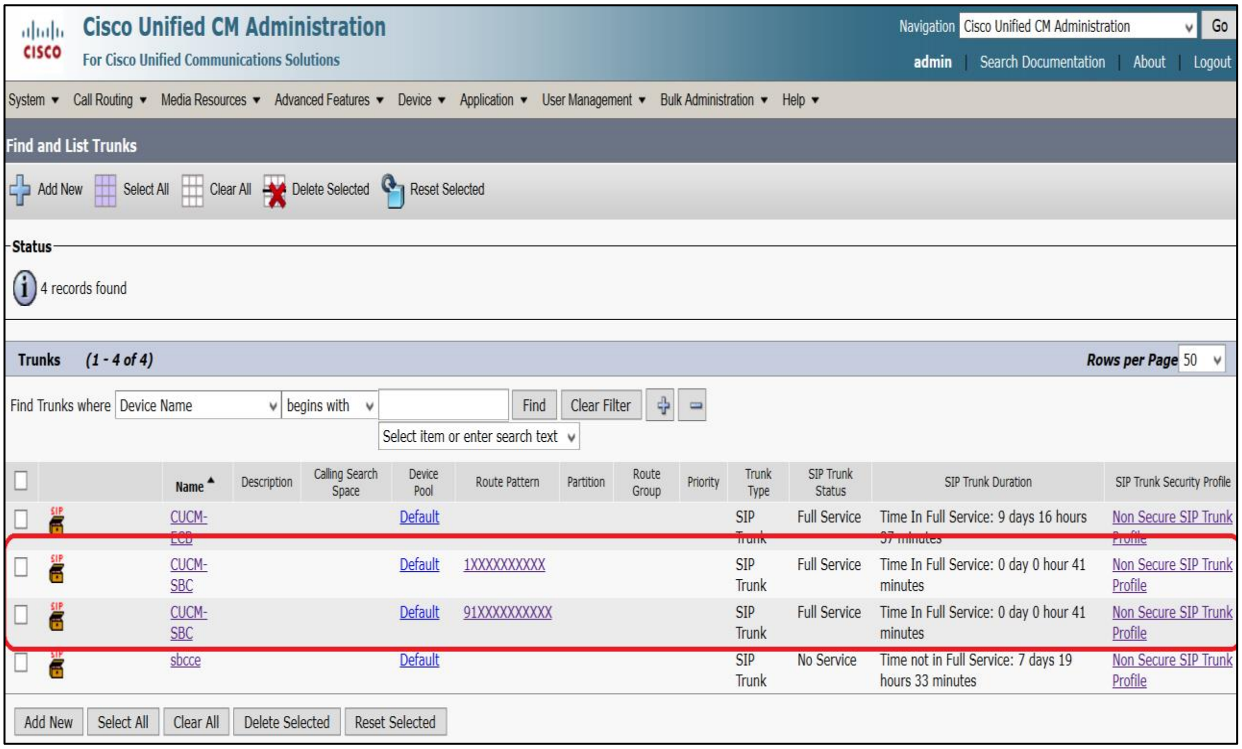
2 records found

Route Patterns (1 - 2 of 2) Rows per Page 50

Find Route Patterns where Pattern begins with

□	Pattern ▴	Description	Partition	Route Filter	Associated Device	Copy
□	1XXXXXXXXXX	Route to SBC			CUCM-SBC	
□	91XXXXXXXXXX	Route to SBC			CUCM-SBC	

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



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 ▾

Find and List Trunks

Add New
Select All
Clear All
Delete Selected
Reset Selected

Status

4 records found

Trunks (1 - 4 of 4) Rows per Page 50

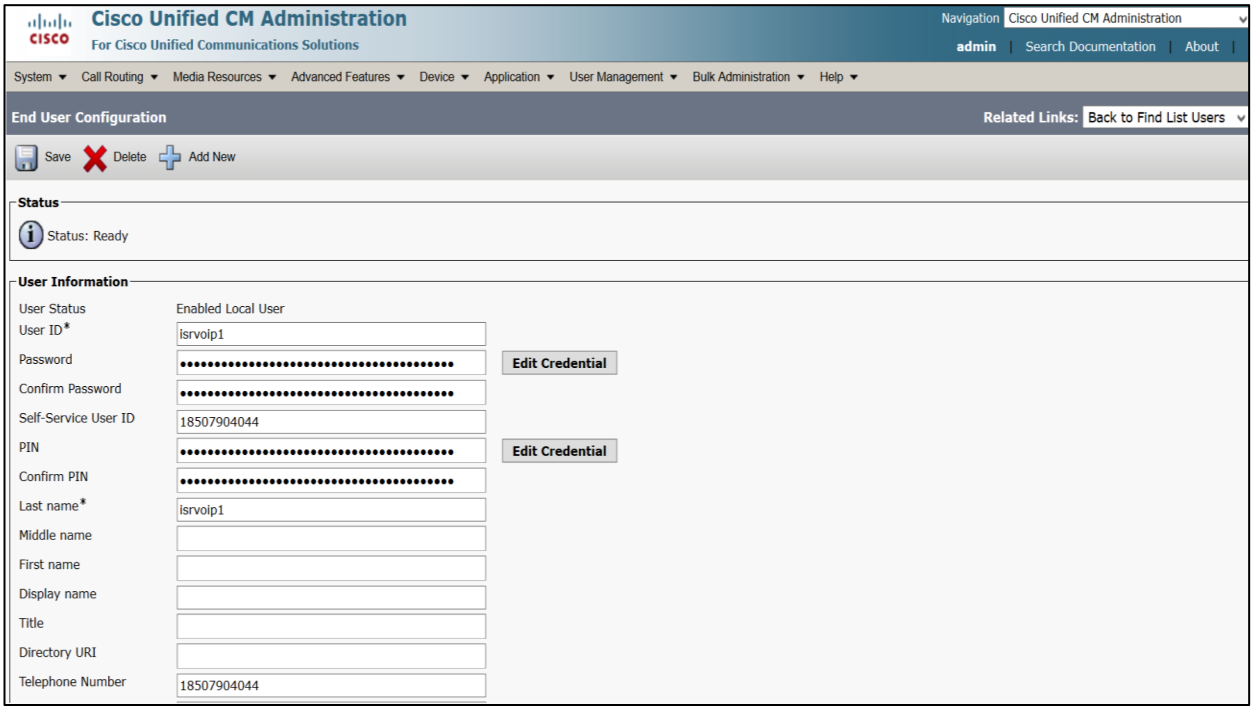
Find Trunks where Device Name begins with

Select item or enter search text

□		Name ▴	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration	SIP Trunk Security Profile
□	SIP	CUCM-ECB			Default					SIP Trunk	Full Service	Time In Full Service: 9 days 16 hours 37 minutes	Non Secure SIP Trunk Profile
□	SIP	CUCM-SBC			Default	1XXXXXXXXXX				SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 41 minutes	Non Secure SIP Trunk Profile
□	SIP	CUCM-SBC			Default	91XXXXXXXXXX				SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 41 minutes	Non Secure SIP Trunk Profile
□	SIP	sbcce			Default					SIP Trunk	No Service	Time not in Full Service: 7 days 19 hours 33 minutes	Non Secure SIP Trunk Profile

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)


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 ▾
Related Links: Back to Find List Users
Save Delete Add New
Edit Credential
Edit Credential

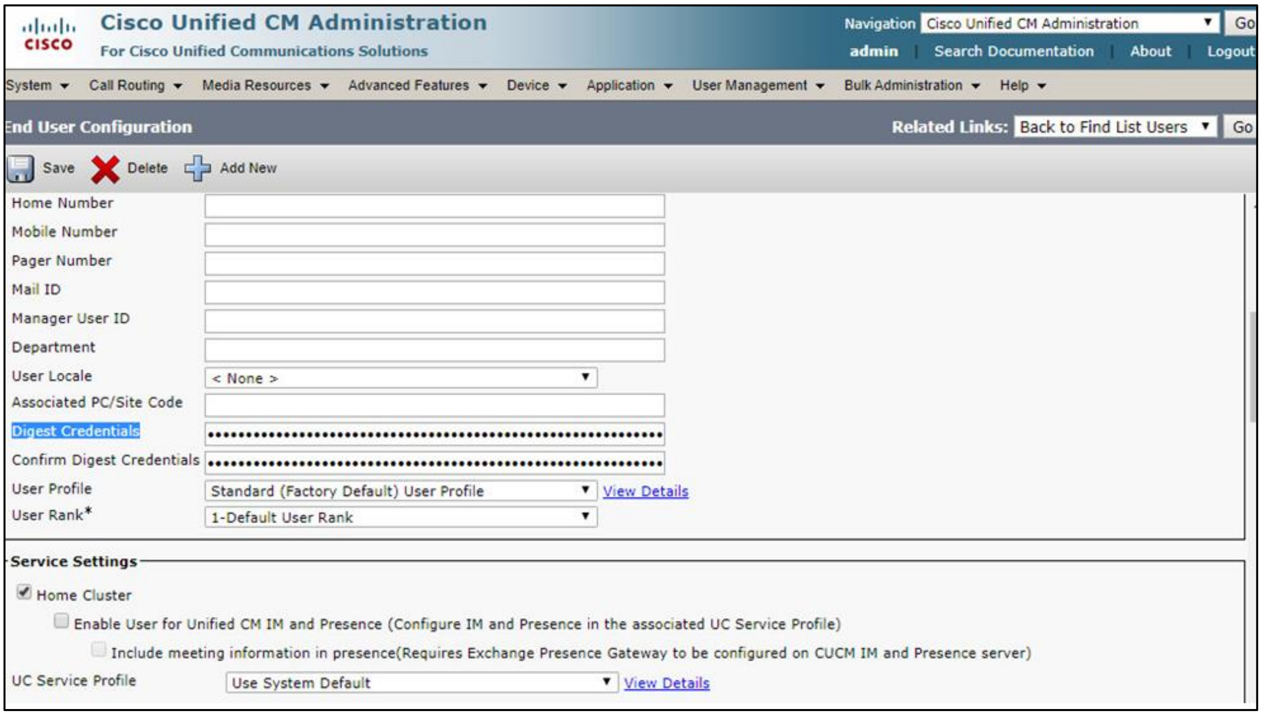
End User Configuration

Status

Status: Ready

User Information

User Status	Enabled Local User
User ID*	isrvoip1
Password	••
Confirm Password	••
Self-Service User ID	18507904044
PIN	••
Confirm PIN	••
Last name*	isrvoip1
Middle name	
First name	
Display name	
Title	
Directory URI	
Telephone Number	18507904044


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 ▾
Related Links: Back to Find List Users Go
Save Delete Add New
View Details
View Details

End User Configuration

Home Number	
Mobile Number	
Pager Number	
Mail ID	
Manager User ID	
Department	
User Locale	< None >
Associated PC/Site Code	
Digest Credentials	•••
Confirm Digest Credentials	•••
User Profile	Standard (Factory Default) User Profile
User Rank*	1-Default User Rank

Service Settings

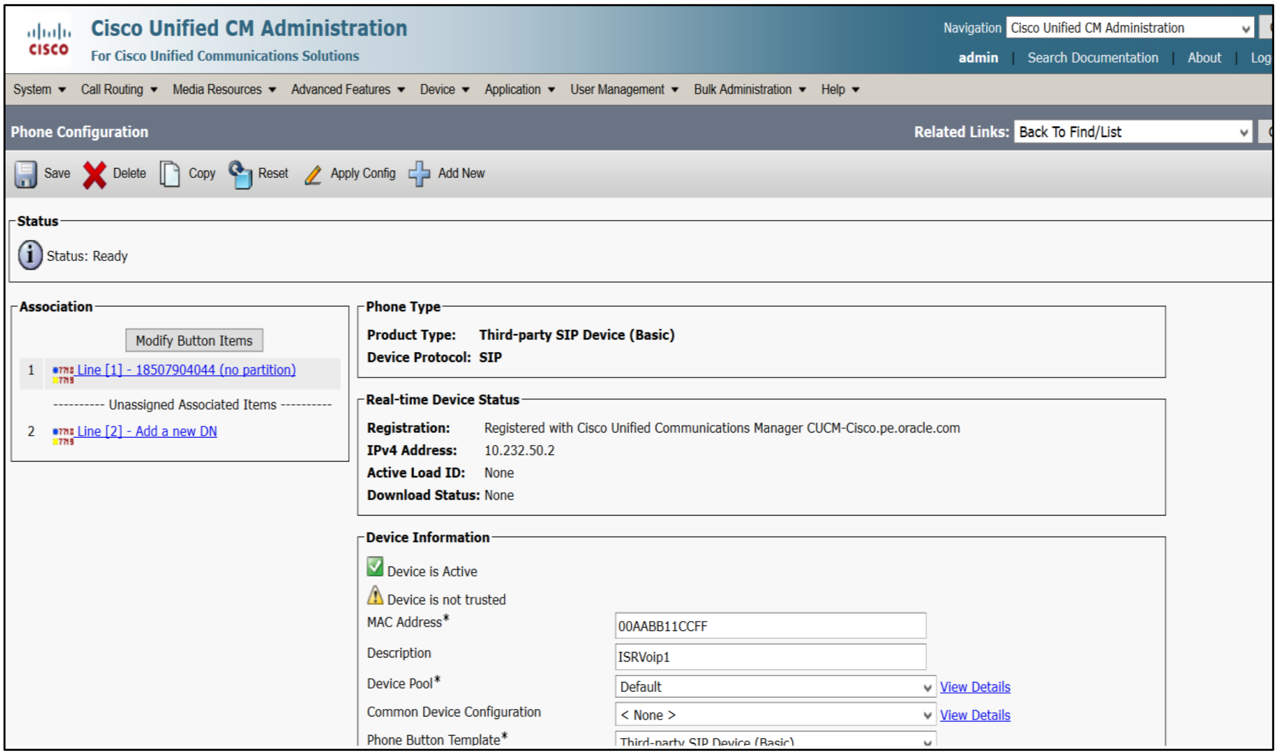
☑ Home Cluster
☐ Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)
☐ Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)

UC Service Profile: Use System Default

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
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
admin | Search Documentation | About | Log
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
Modify Button Items

Status

Status: Ready

Association

1 Line [1] - 18507904044 (no partition)

---------- Unassigned Associated Items ----------

2 Line [2] - Add a new DN

Phone Type

Product Type: Third-party SIP Device (Basic)
Device Protocol: SIP

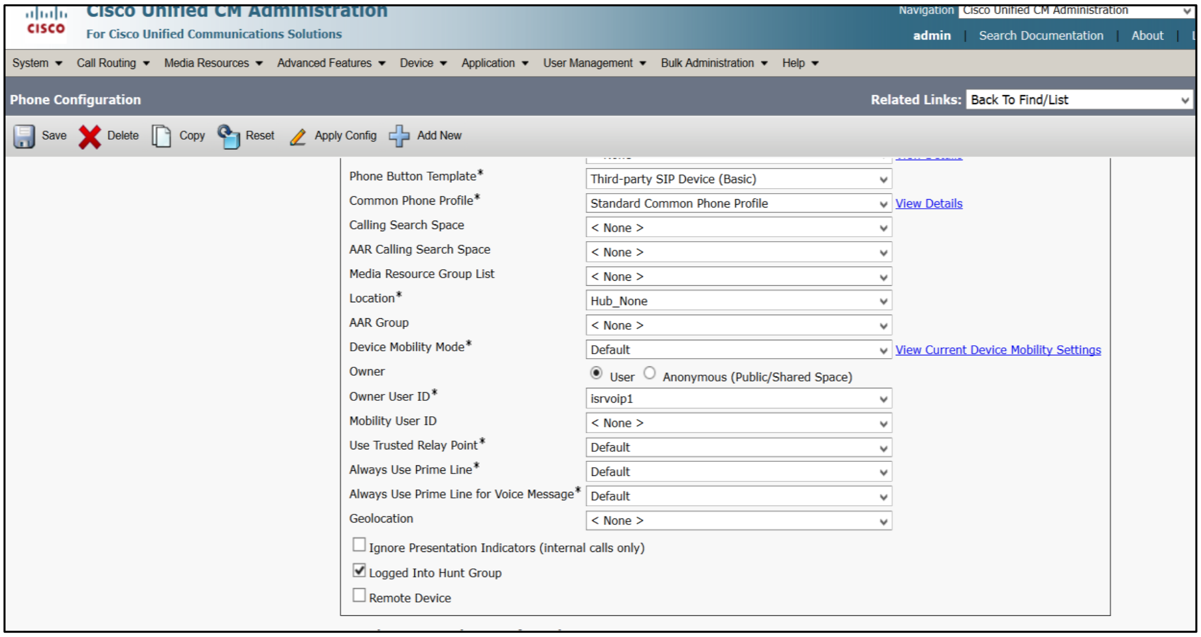
Real-time Device Status

Registration: Registered with Cisco Unified Communications Manager CUCM-Cisco.pe.oracle.com
IPv4 Address: 10.232.50.2
Active Load ID: None
Download Status: None

Device Information

☑ Device is Active
⚠ Device is not trusted

MAC Address*	00AABB11CCFF	
Description	ISRVoip1	
Device Pool*	Default	View Details
Common Device Configuration	< None >	View Details
Phone Button Template*	Third-party SIP Device (Basic)	


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
Save Delete Copy Reset Apply Config Add New

Phone Configuration

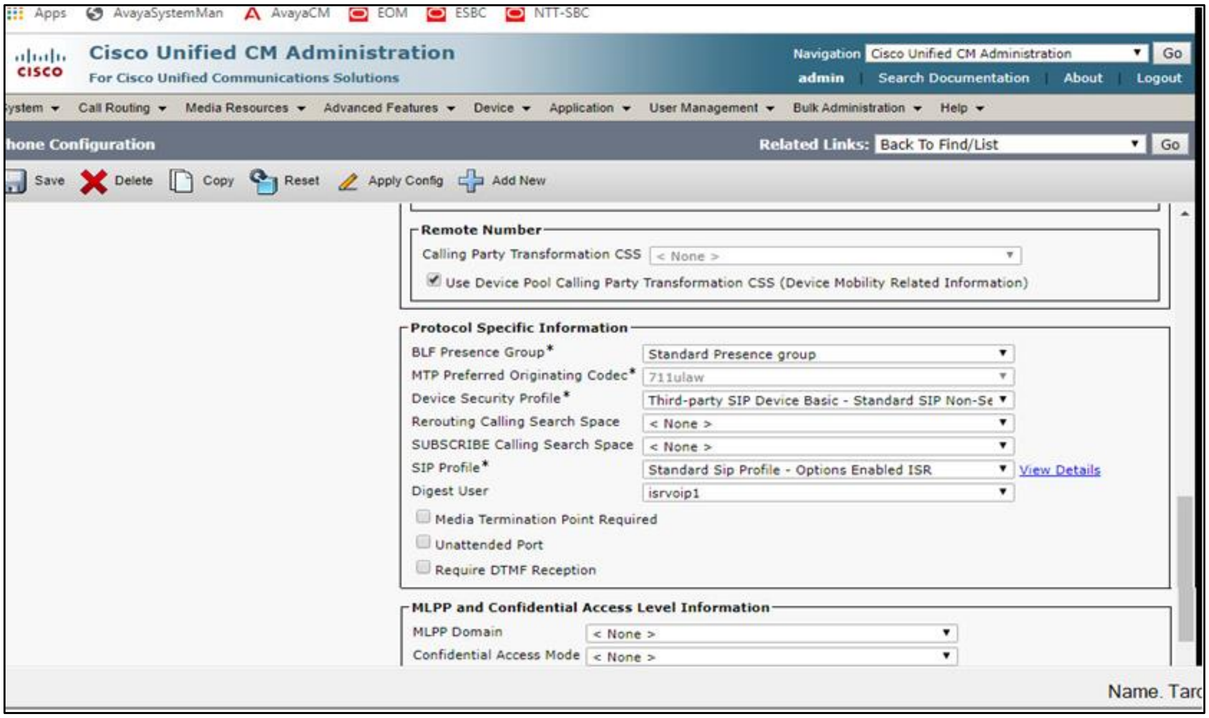
Related Links: Back To Find/List

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
ystem Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Save Delete Copy Reset Apply Config Add New
Name. Tarc

hone Configuration

Related Links: Back To Find/List Go

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

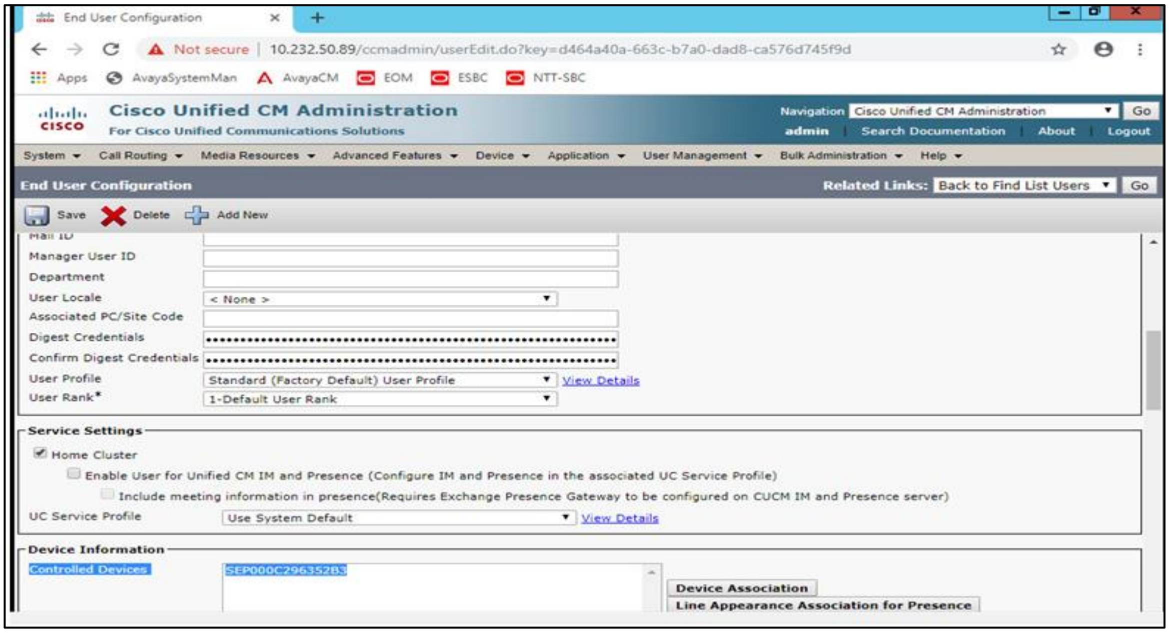
MLPP and Confidential Access Level Information

MLPP Domain	< None >
Confidential Access Mode	< None >

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.


End User Configuration
Not secure | 10.232.50.89/ccmadmin/userEdit.do?key=d464a40a-663c-b7a0-dad8-ca576d745f9d
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
End User Configuration
Related Links: Back to Find List Users Go
Save
Delete
Add New
Device Association
Line Appearance Association for Presence

Mail ID
Manager User ID
Department
User Locale < None >
Associated PC/Site Code
Digest Credentials ••
Confirm Digest Credentials ••
User Profile Standard (Factory Default) User Profile View Details
User Rank* 1-Default User Rank

Service Settings
☑ Home Cluster
☐ Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)
☐ Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)
UC Service Profile Use System Default View Details

Device Information
Controlled Devices SEP000C296352B3

With these steps, the CUCM configuration is complete.

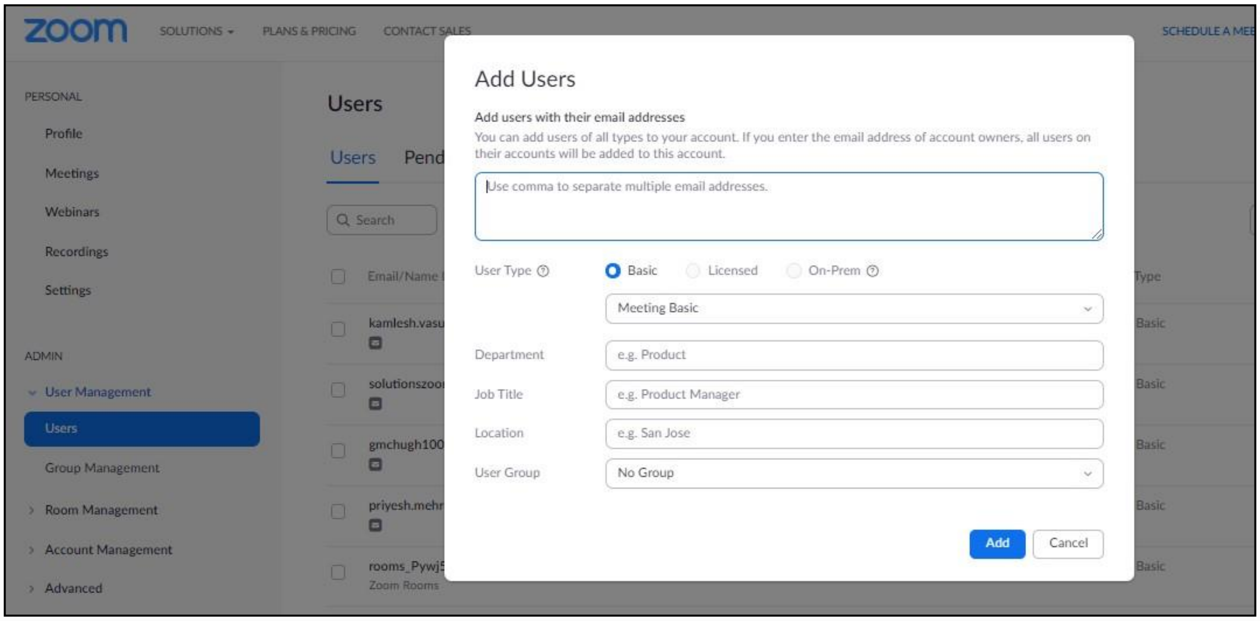
5. Zoom Phone configuration.

This Section describes the steps to configure BYOC Phone Numbers on the Zoom Admin Portal and assign the BYOC Number to a User. For detailed assistance with setting up and configuring your Zoom Phone System, please reach out to Zoom Sales: https://Zoom.us/contactsales

5.1. Create a Zoom User.

Navigate to **Admin>User Management > Users**.

Click Add to create new Zoom users. Provide the necessary details about the New User and Click on Add to Add the User.



Add Users

Add users with their email addresses

You can add users of all types to your account. If you enter the email address of account owners, all users on their accounts will be added to this account.

Use comma to separate multiple email addresses.

User Type: ● Basic ○ Licensed ○ On-Prem

Meeting Basic

Department: e.g. Product

Job Title: e.g. Product Manager

Location: e.g. San Jose

User Group: No Group

Once the New User is added it will start reflecting in **Admin >Users** Section on the Web portal

5.2. Add BYOC number

Navigate to **Phone Systems Management > Phone Numbers > BYOC**

Select **Add** to add external phone numbers provided by Twilio Trunk into the Zoom portal.

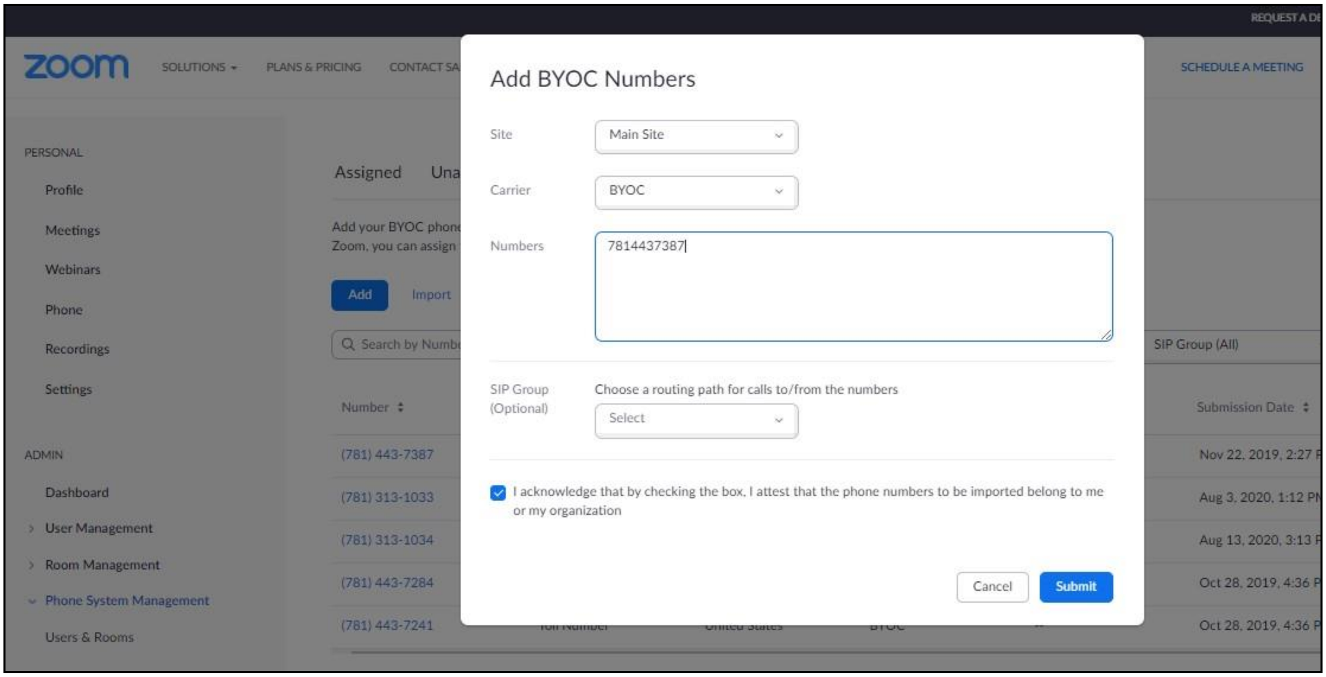
Site - Choose the relevant Site on which the Number needs to be added. For Example Main Site.

Carrier –Choose BYOC

Numbers- Put the BYOC DID Number provided by Twilio Trunk.

SIP Group – Optional Parameter (Can be Left Blank) Acknowledge that the Phone Number belongs to your organization.

Click **Submit**.



Add BYOC Numbers

Site: Main Site

Carrier: BYOC

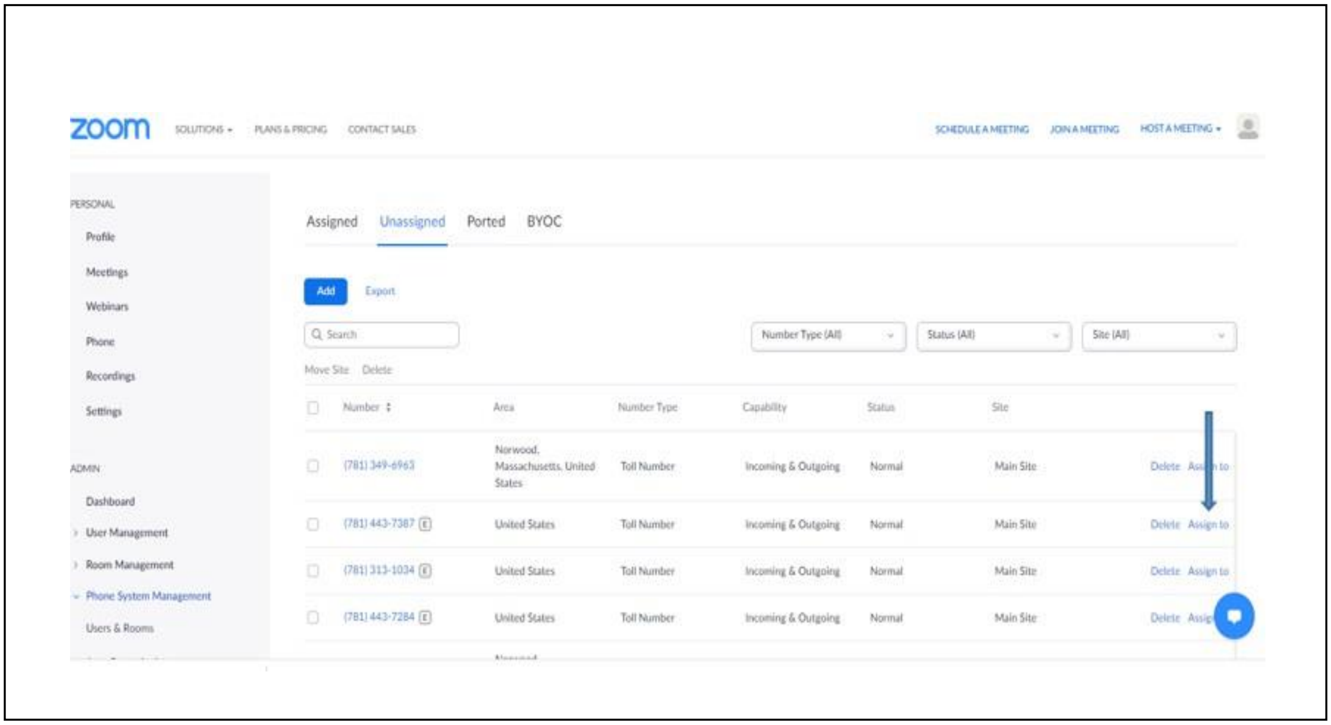
Numbers: 7814437387

SIP Group (Optional): Choose a routing path for calls to/from the numbers — Select

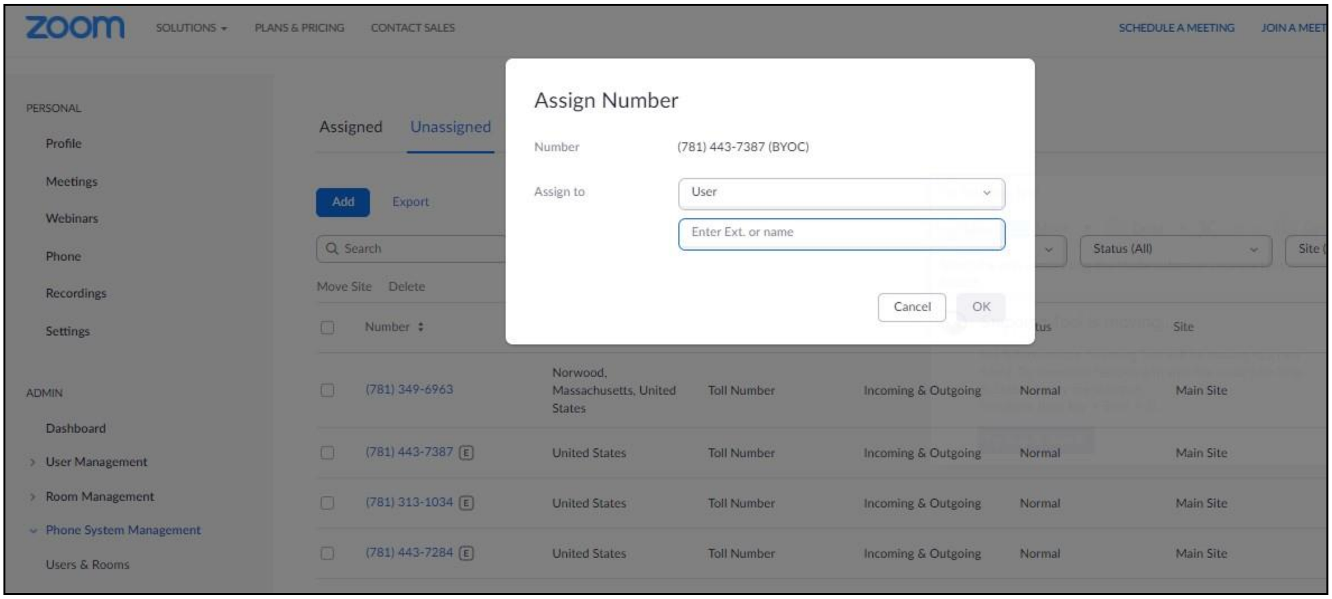
☑ I acknowledge that by checking the box, I attest that the phone numbers to be imported belong to me or my organization

5.3. Assign the BYOC number to a User

The BYOC Number will now be visible in the Unassigned Tab on the portal. Click on Assign to Tab to assign the Number to a User.



Number	Area	Number Type	Capability	Status	Site	
(781) 349-6963	Norwood, Massachusetts, United States	Toll Number	Incoming & Outgoing	Normal	Main Site	Delete Assign to
(781) 443-7387	United States	Toll Number	Incoming & Outgoing	Normal	Main Site	Delete Assign to
(781) 313-1034	United States	Toll Number	Incoming & Outgoing	Normal	Main Site	Delete Assign to
(781) 443-7284	United States	Toll Number	Incoming & Outgoing	Normal	Main Site	Delete Assig



Assign Number

Number (781) 443-7387 (BYOC)

Assign to User

Enter Ext. or name

Number					tus	Site
(781) 349-6963	Norwood, Massachusetts, United States	Toll Number	Incoming & Outgoing	Normal		Main Site
(781) 443-7387 E	United States	Toll Number	Incoming & Outgoing	Normal		Main Site
(781) 313-1034 E	United States	Toll Number	Incoming & Outgoing	Normal		Main Site
(781) 443-7284 E	United States	Toll Number	Incoming & Outgoing	Normal		Main Site

6. Infrastructure Requirements.

The table below shows the list of infrastructure prerequisites for deploying Zoom Premise Peering.

Session Border Controller (SBC)	**See Zoom Documentation for More Details**
SIP Trunks connected to the SBC	
Zoom Phone	
Public IP address for the SBC	
Public trusted certificate for the SBC	
Firewall ports for Zoom Voice signaling	
Firewall IP addresses and ports for Zoom Voice media	
Media Transport Profile	
Firewall ports for client media	

7. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Cisco Call Manager (Cisco CUCM) and Zoom BYOC.

7.1. 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

8. New SBC configuration

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

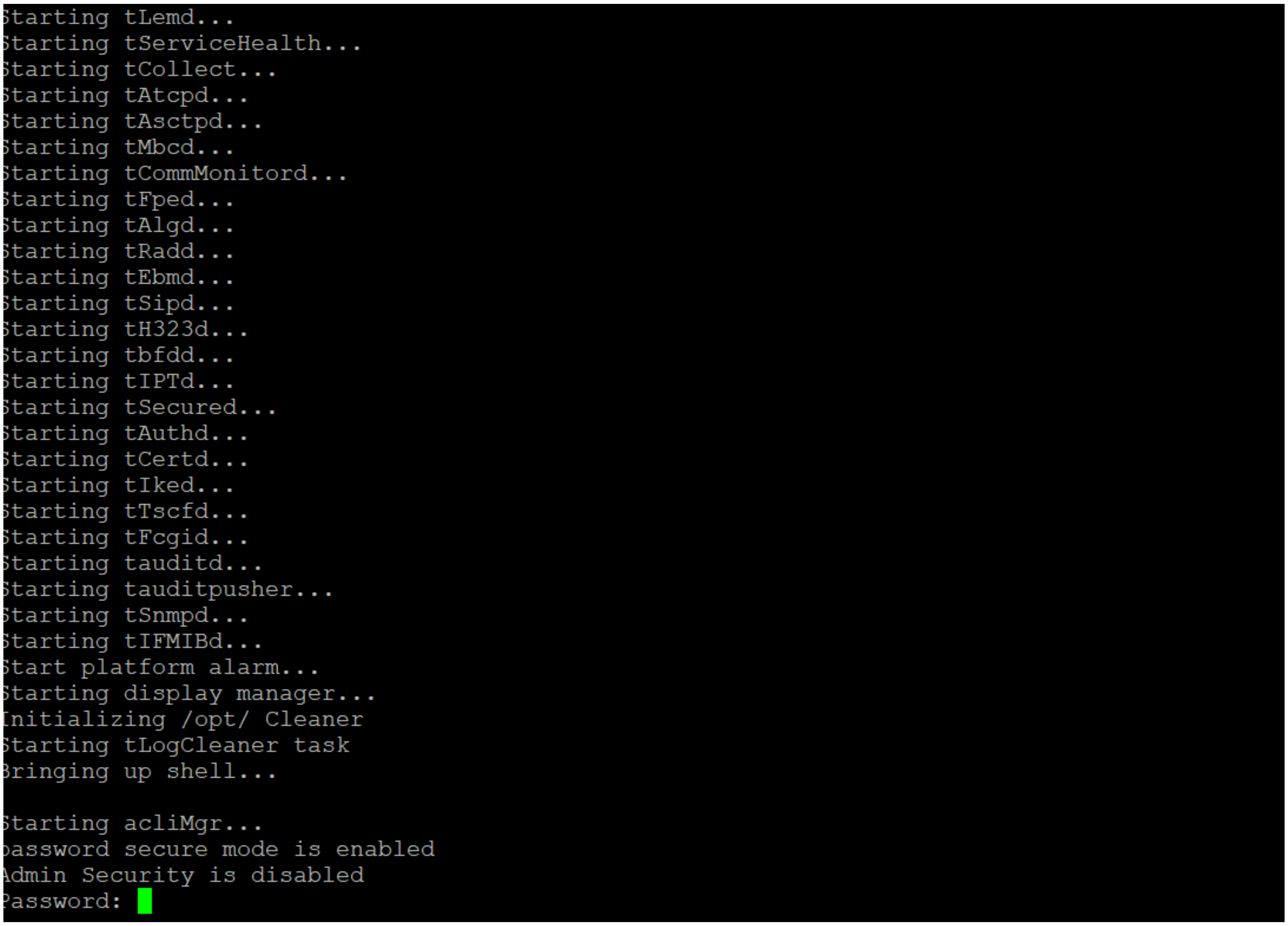
8.1. Establishing a serial connection to the SBC

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

Please note that the above console connection procedure does not apply to VME or cloud deployments of SBC and can be applied only to hardware platforms.

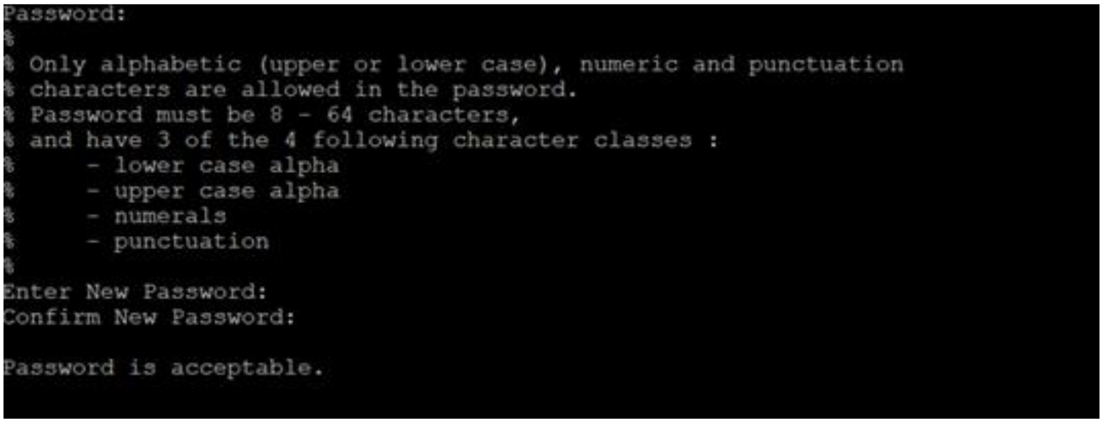
Power on the SBC and confirm that you see the following output from the boot-up sequence



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

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

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

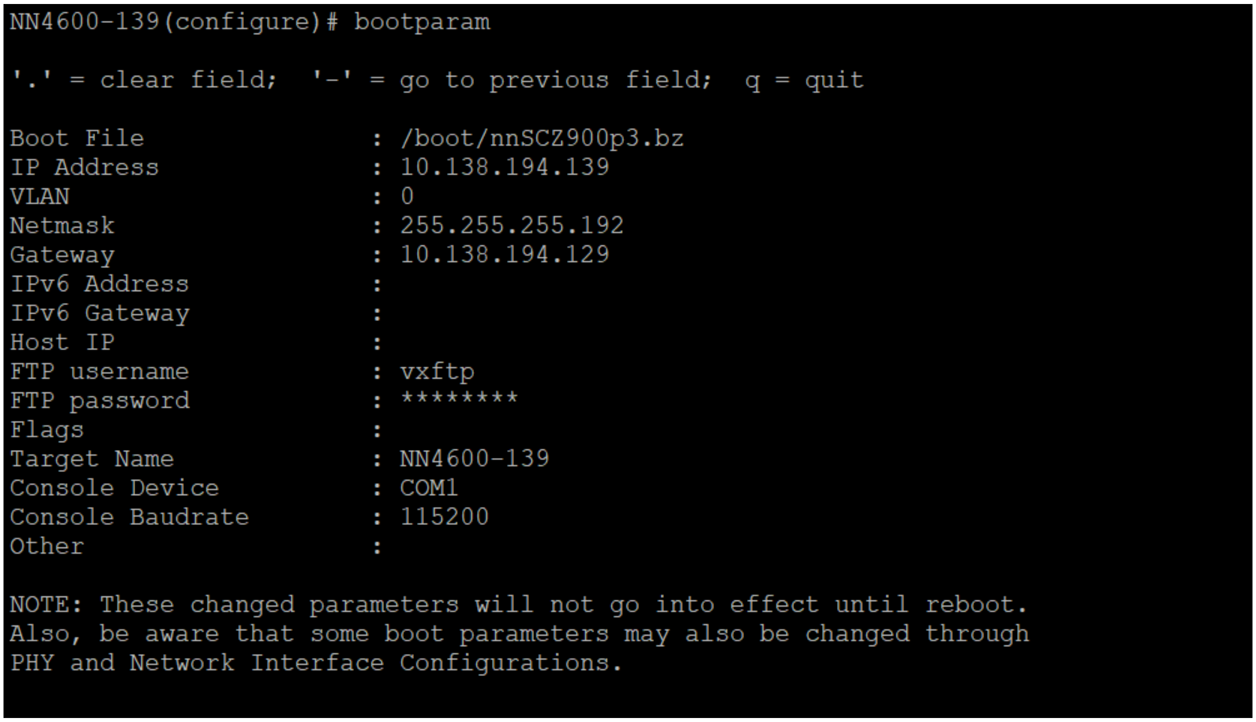
Both passwords have to be changed according to the rules shown below.



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

Password is acceptable.
```

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

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

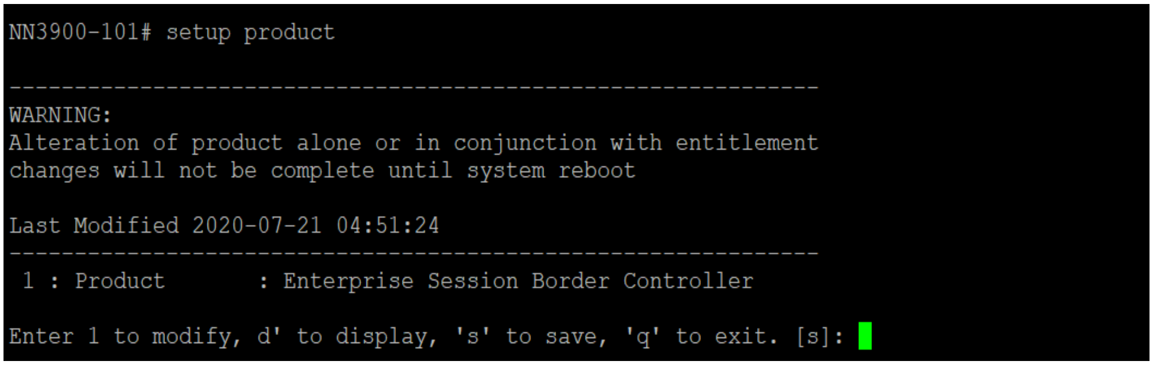


```
NN4600-139(configure)# bootparam

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

Boot File              : /boot/nnSCZ900p3.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.
```

Note: There is no management IP configured by default.

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

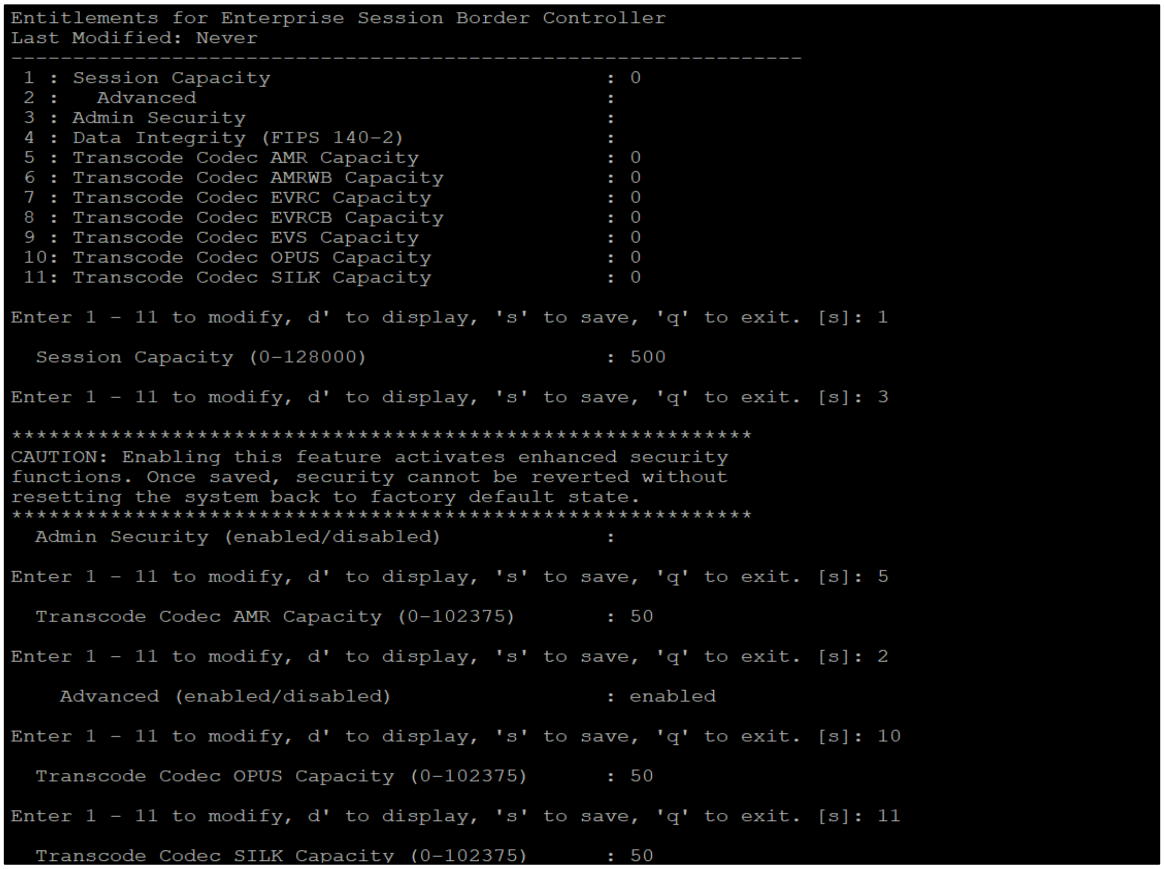
To configure product type, type in setup product in the terminal



```
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.

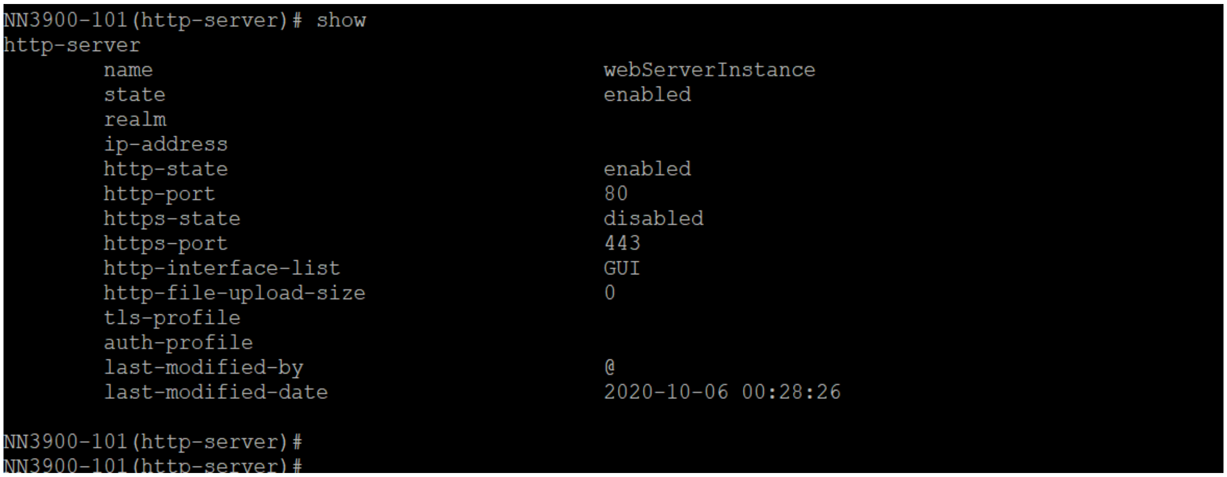


```
Entitlements for Enterprise Session Border Controller
Last Modified: Never
----------------------------------------------------------------
 1 : Session Capacity                              : 0
 2 :   Advanced                                    :
 3 : Admin Security                                :
 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.

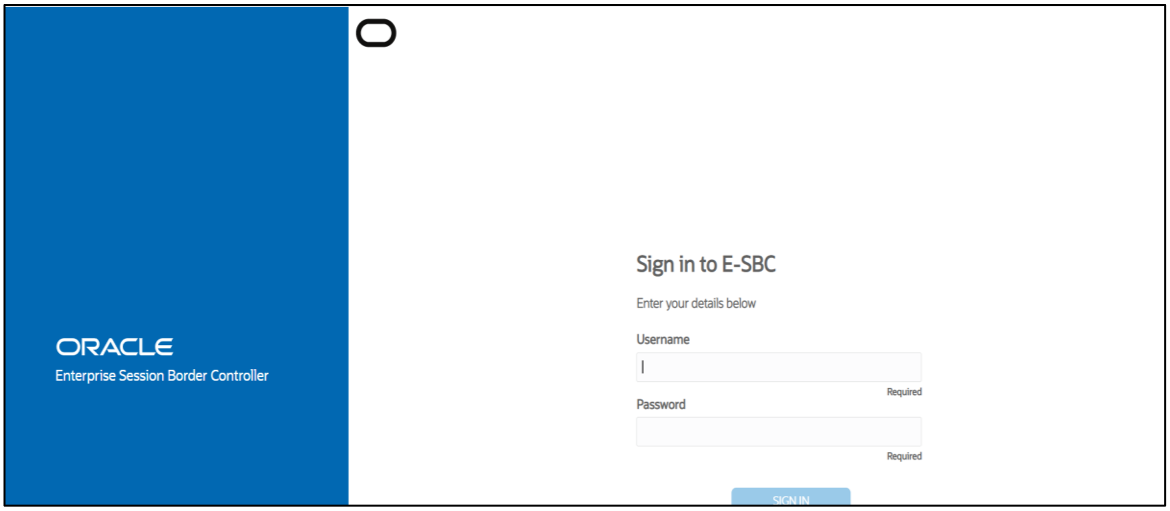


```
NN3900-101(http-server)# show
http-server
        name                                    webServerInstance
        state                                   enabled
        realm
        ip-address
        http-state                              enabled
        http-port                               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)#
```

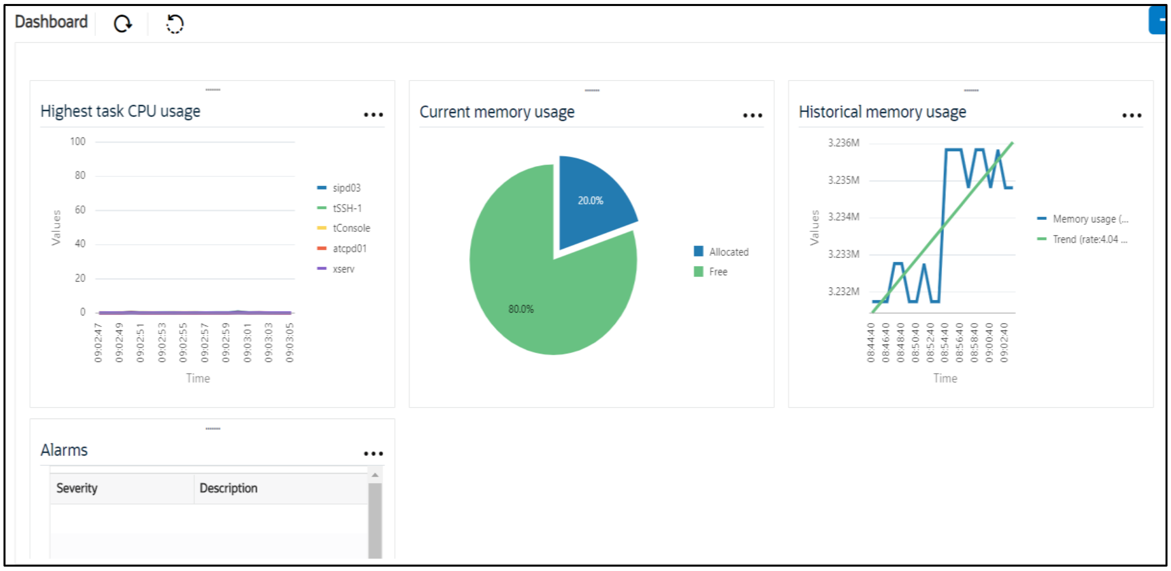
8.2. Configure SBC using Web GUI

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

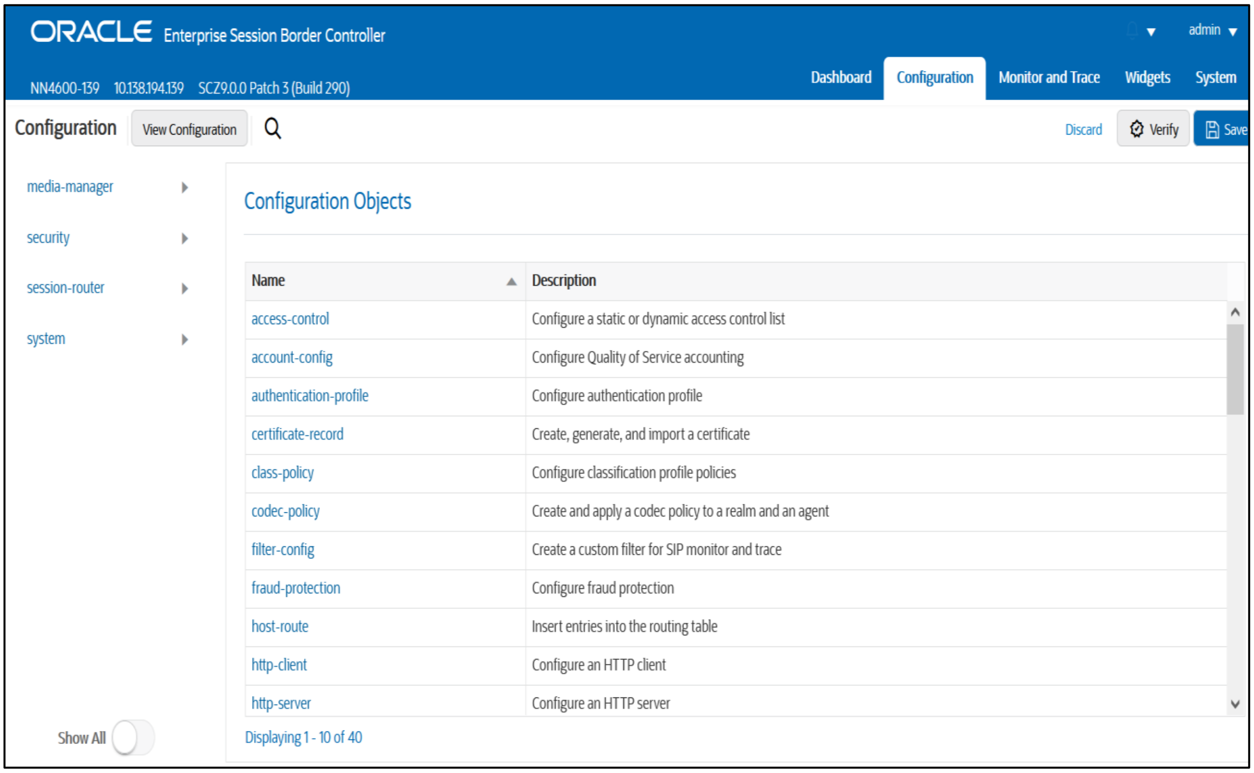
The Web GUI can be accessed through the url http://<SBC_MGMT_IP>.



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



Go to Configuration as shown below, to configure the SBC



Name	Description
access-control	Configure a static or dynamic access control list
account-config	Configure Quality of Service accounting
authentication-profile	Configure authentication profile
certificate-record	Create, generate, and import a certificate
class-policy	Configure classification profile policies
codec-policy	Create and apply a codec policy to a realm and an agent
filter-config	Create a custom filter for SIP monitor and trace
fraud-protection	Configure fraud protection
host-route	Insert entries into the routing table
http-client	Configure an HTTP client
http-server	Configure an HTTP server

Displaying 1 - 10 of 40

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

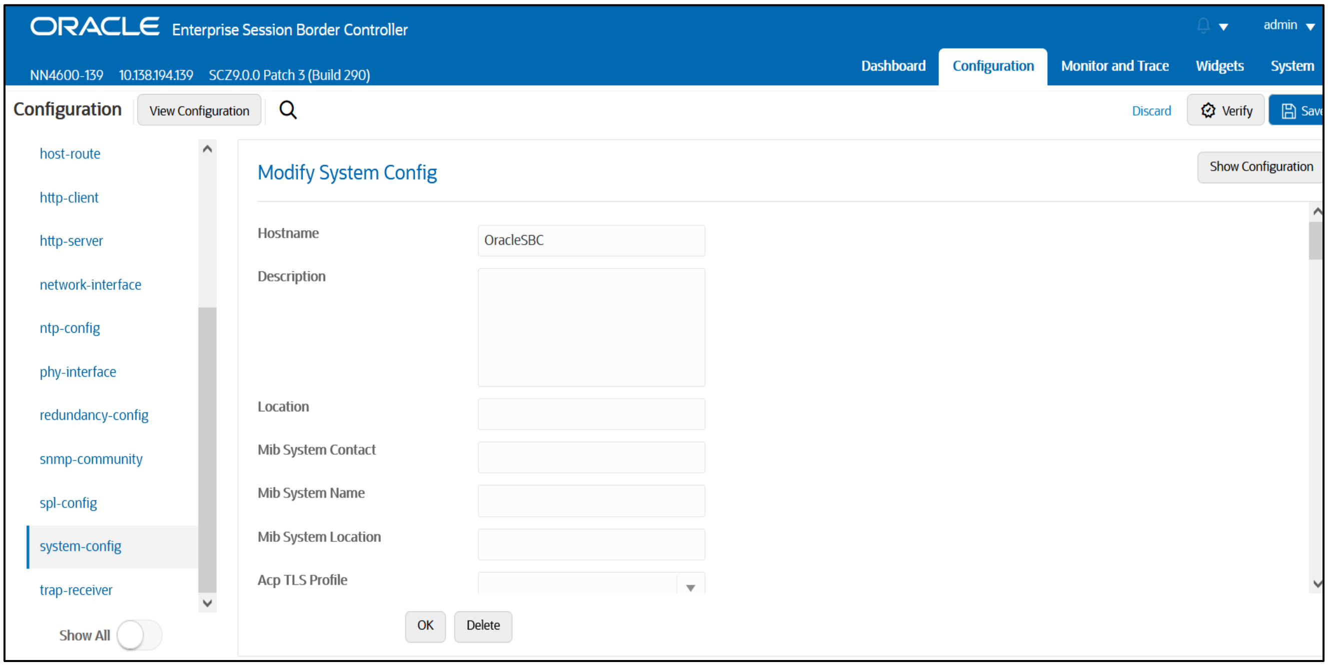
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.0.0/webgui/web-gui-guide.pdf

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.

8.3. Configure system-config

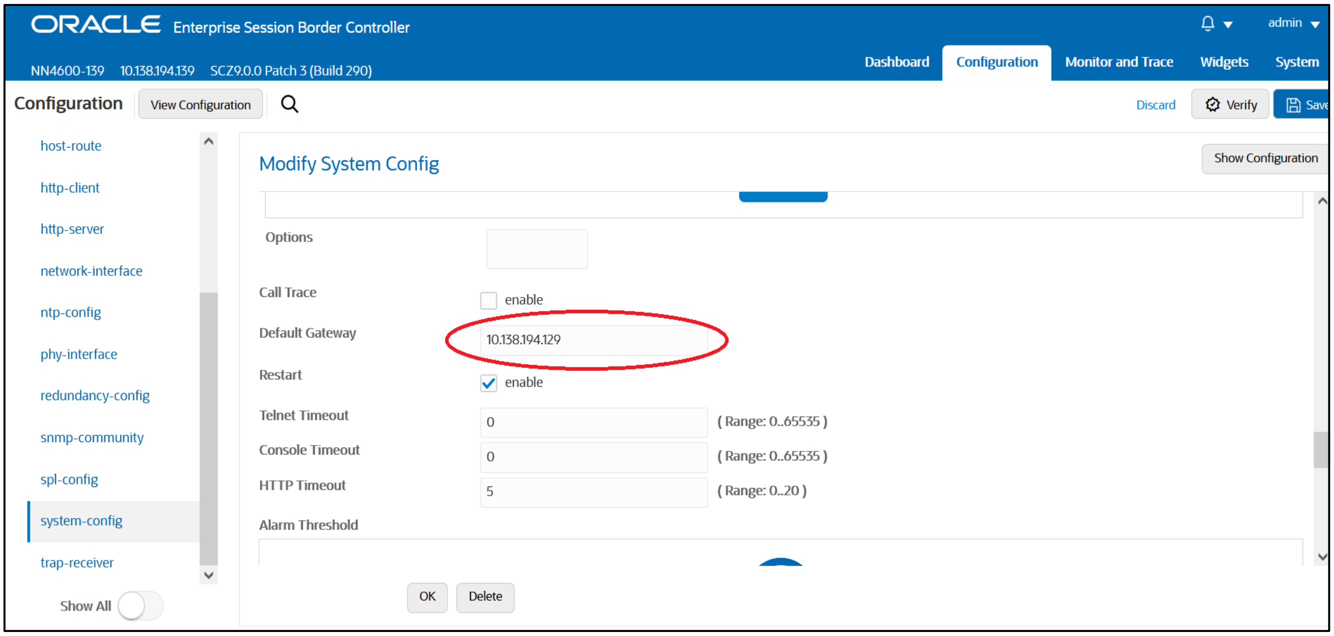
Go to system->system-config



Modify System Config

Hostname	OracleSBC
Description	
Location	
Mib System Contact	
Mib System Name	
Mib System Location	
Acp TLS Profile	

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



Modify System Config

Options		
Call Trace	□ enable	
Default Gateway	10.138.194.129	
Restart	☑ enable	
Telnet Timeout	0	(Range: 0..65535)
Console Timeout	0	(Range: 0..65535)
HTTP Timeout	5	(Range: 0..20)
Alarm Threshold		

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.

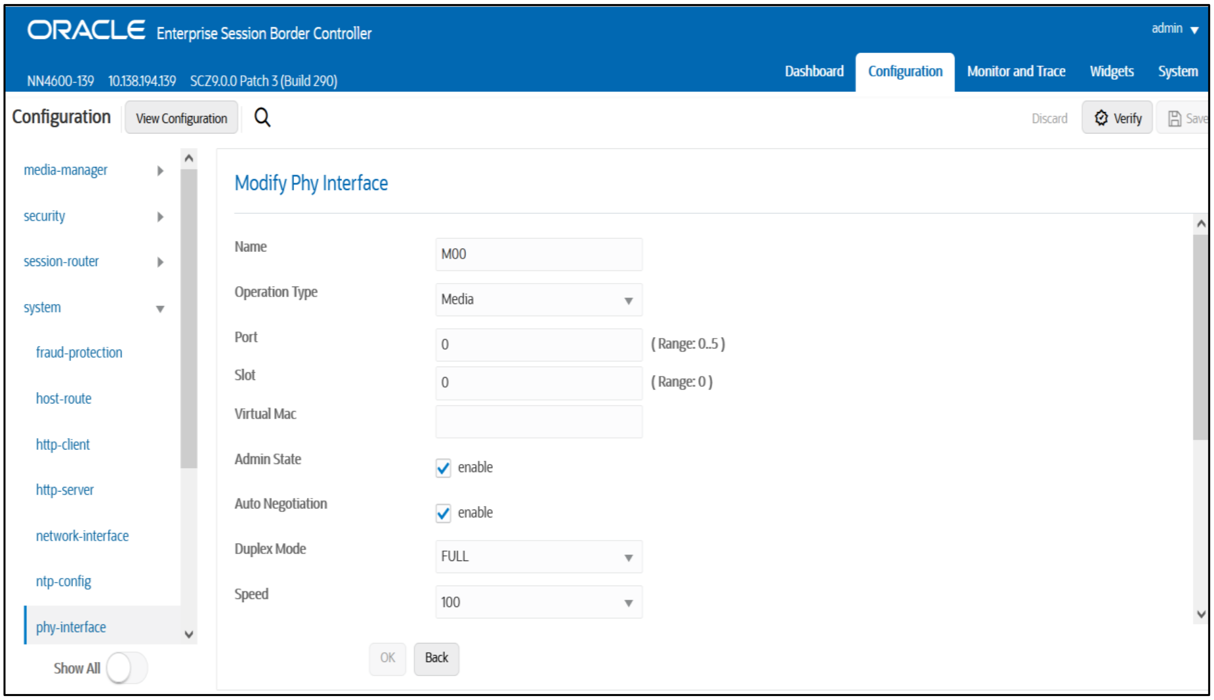
8.4. Configure Physical Interface values

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

Please configure M00 for Zoom side and M01 for Cisco side.

Parameter Name	Zoom BYOC (M00)	Cisco side (M01)
Slot	0	1
Port	0	0
Operation Mode	Media	Media

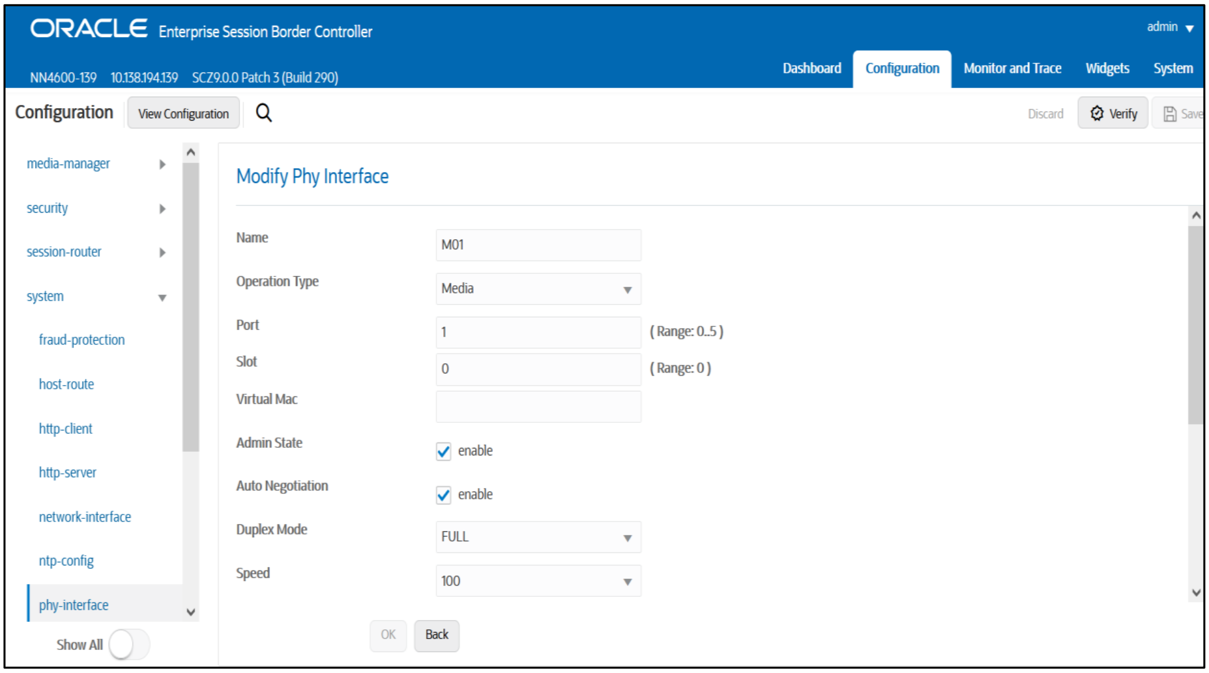
Please configure M00 interface as below.



Modify Phy Interface

Name	M00
Operation Type	Media
Port	0 (Range: 0..5)
Slot	0 (Range: 0)
Virtual Mac	
Admin State	☑ enable
Auto Negotiation	☑ enable
Duplex Mode	FULL
Speed	100

Please configure M01 interface as below



Modify Phy Interface

Name: M01

Operation Type: Media

Port: 1 (Range: 0..5)

Slot: 0 (Range: 0)

Virtual Mac:

Admin State: ☑ enable

Auto Negotiation: ☑ enable

Duplex Mode: FULL

Speed: 100

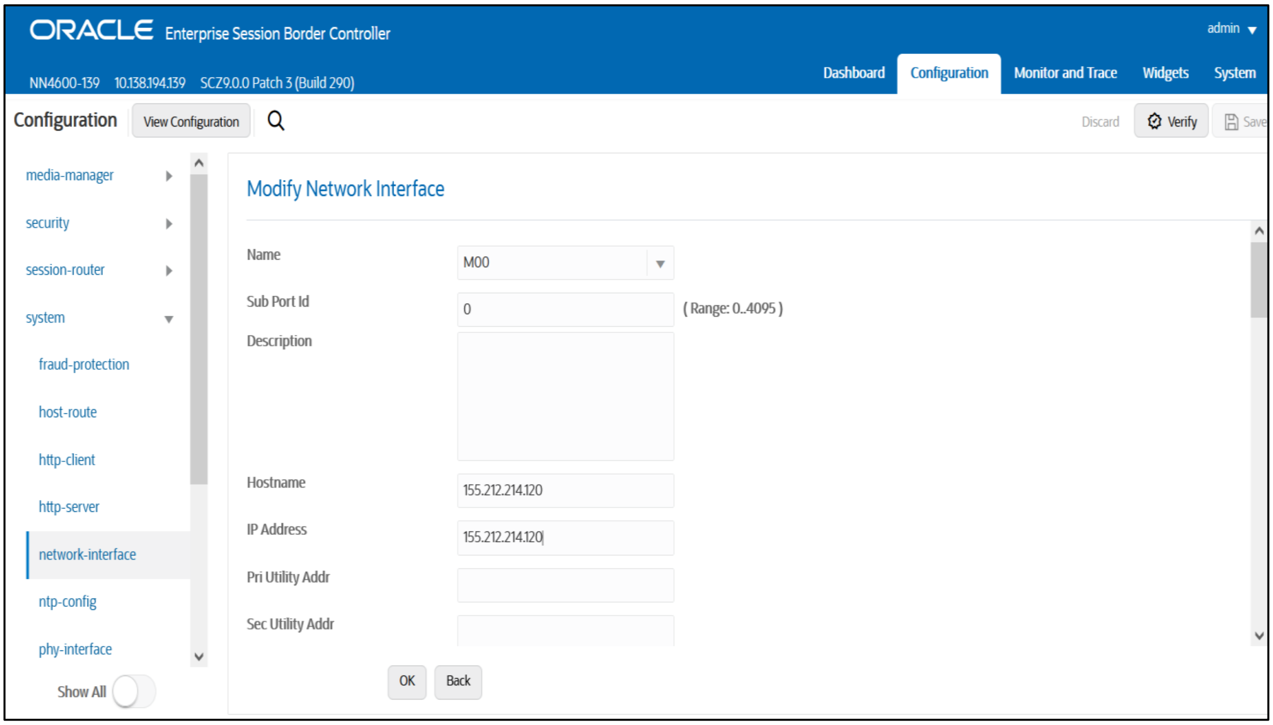
8.5. Configure Network Interface values

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	Zoom BYOC Network Interface(M00)	Cisco side Network Interface(M01)
Name	M00	M01
Host Name		
IP Address	155.212.214.120	10.232.50.79
Net Mask	255.255.255.0	255.255.255.0
Gateway	155.212.214.65	10.232.50.1

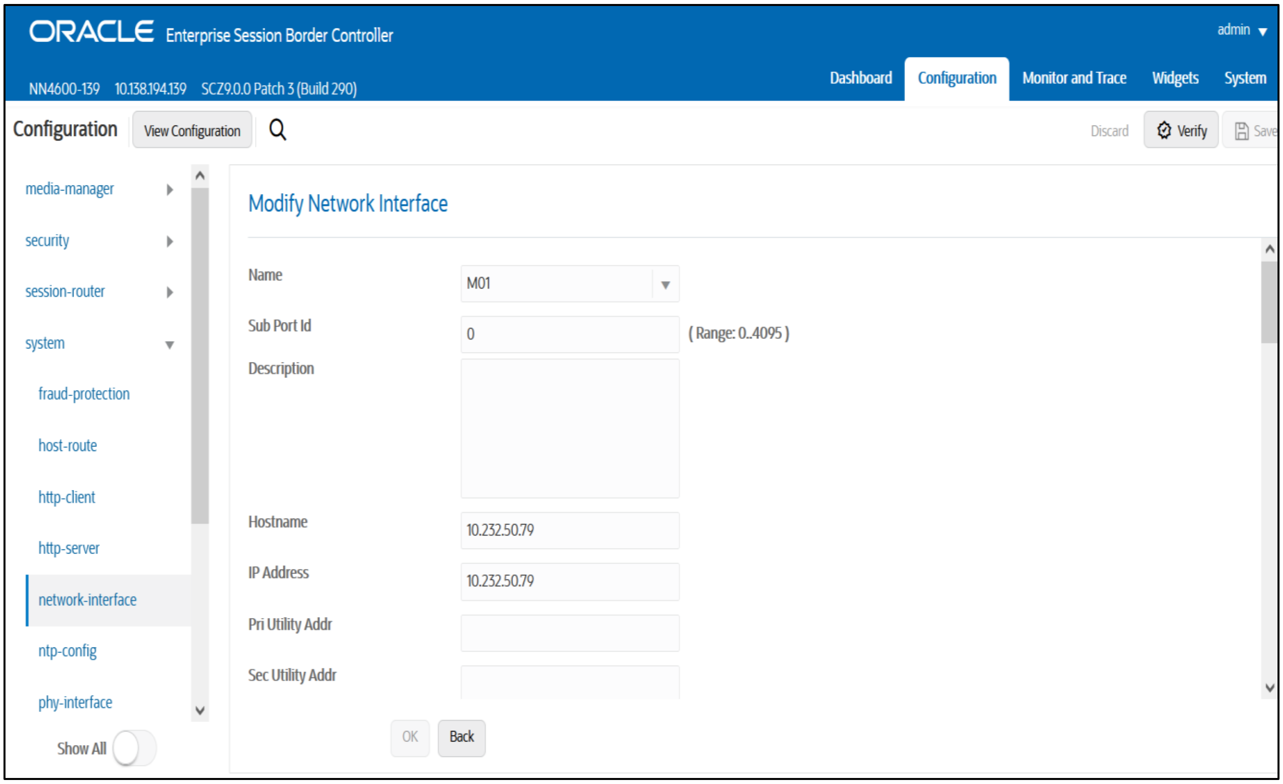
Please configure network interface M00 as below



Modify Network Interface

Name	M00
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	155.212.214.120
IP Address	155.212.214.120
Pri Utility Addr	
Sec Utility Addr	

Similarly, configure network interface M01 as below



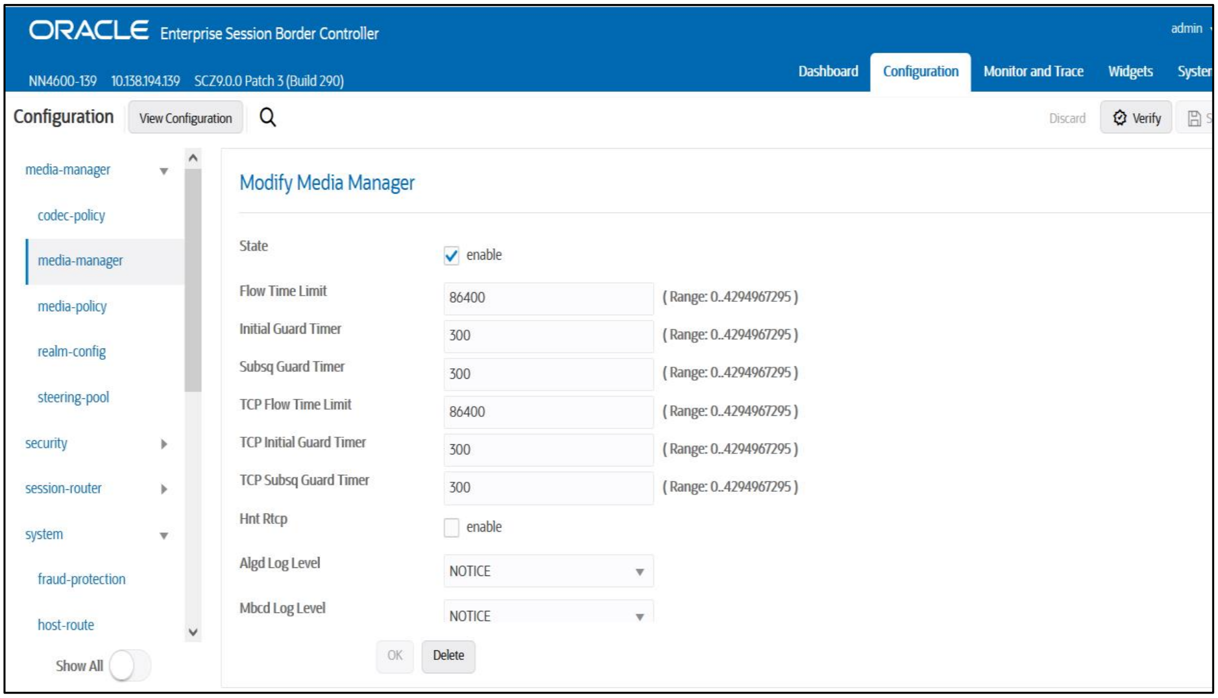
Modify Network Interface

Name	M01
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	10.232.50.79
IP Address	10.232.50.79
Pri Utility Addr	
Sec Utility Addr	

8.6. Enable media manager

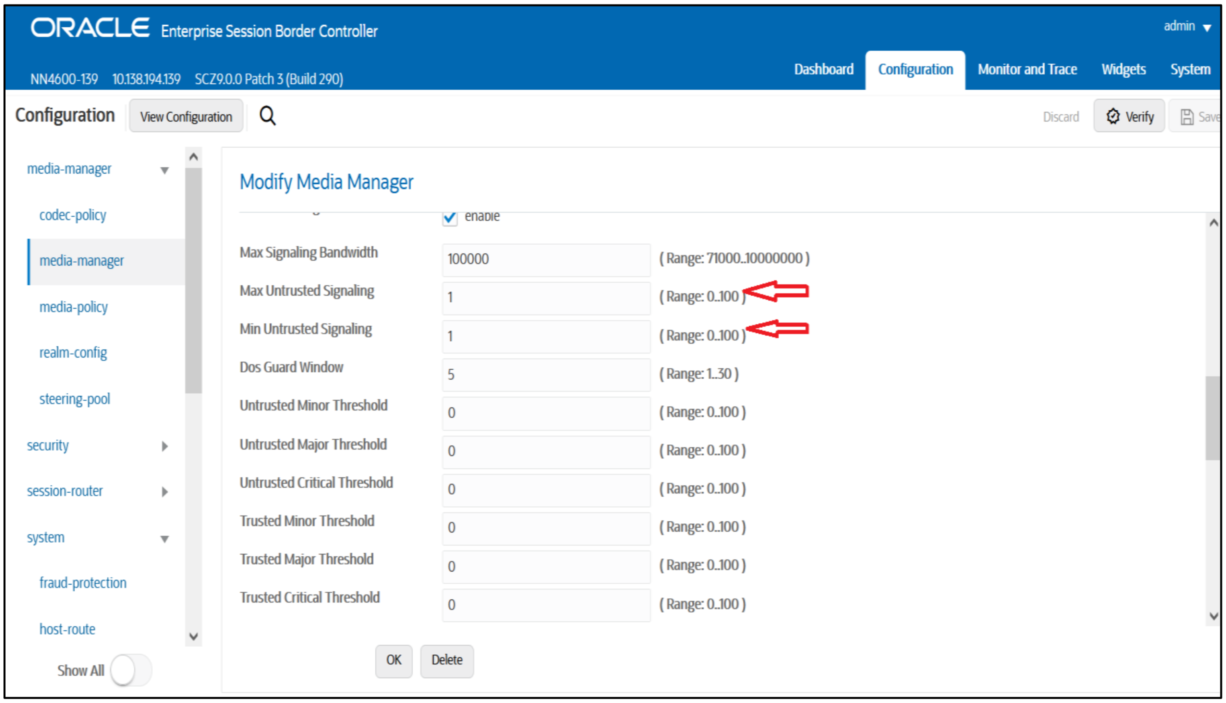
Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

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



Modify Media Manager

State	☑ enable	
Flow Time Limit	86400	(Range: 0..4294967295)
Initial Guard Timer	300	(Range: 0..4294967295)
Subsq Guard Timer	300	(Range: 0..4294967295)
TCP Flow Time Limit	86400	(Range: 0..4294967295)
TCP Initial Guard Timer	300	(Range: 0..4294967295)
TCP Subsq Guard Timer	300	(Range: 0..4294967295)
Hnt Rtcp	□ enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	



Modify Media Manager

	☑ enable	
Max Signaling Bandwidth	100000	(Range: 71000..10000000)
Max Untrusted Signaling	1	(Range: 0..100)
Min Untrusted Signaling	1	(Range: 0..100)
Dos Guard Window	5	(Range: 1..30)
Untrusted Minor Threshold	0	(Range: 0..100)
Untrusted Major Threshold	0	(Range: 0..100)
Untrusted Critical Threshold	0	(Range: 0..100)
Trusted Minor Threshold	0	(Range: 0..100)
Trusted Major Threshold	0	(Range: 0..100)
Trusted Critical Threshold	0	(Range: 0..100)

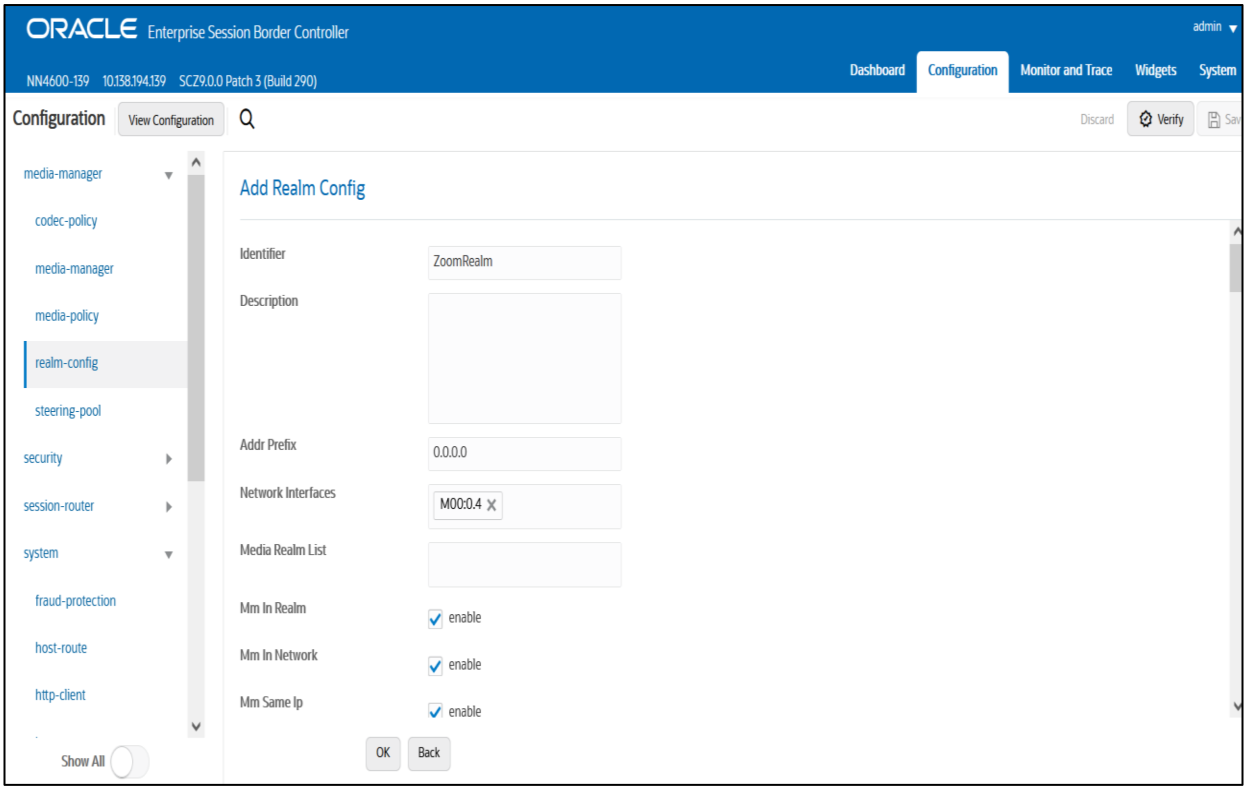
8.7. Configure Realms

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	Zoom Side	**Cisco Side**
Identifier	ZoomRealm	CUCMRealm
Network Interface	M00	M01
Mm in realm	☑	☑
FQDN		
Media Sec policy	sdespolicy	RTP
Access Control Trust Level	High	High

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



Add Realm Config

Identifier: ZoomRealm

Description:

Addr Prefix: 0.0.0.0

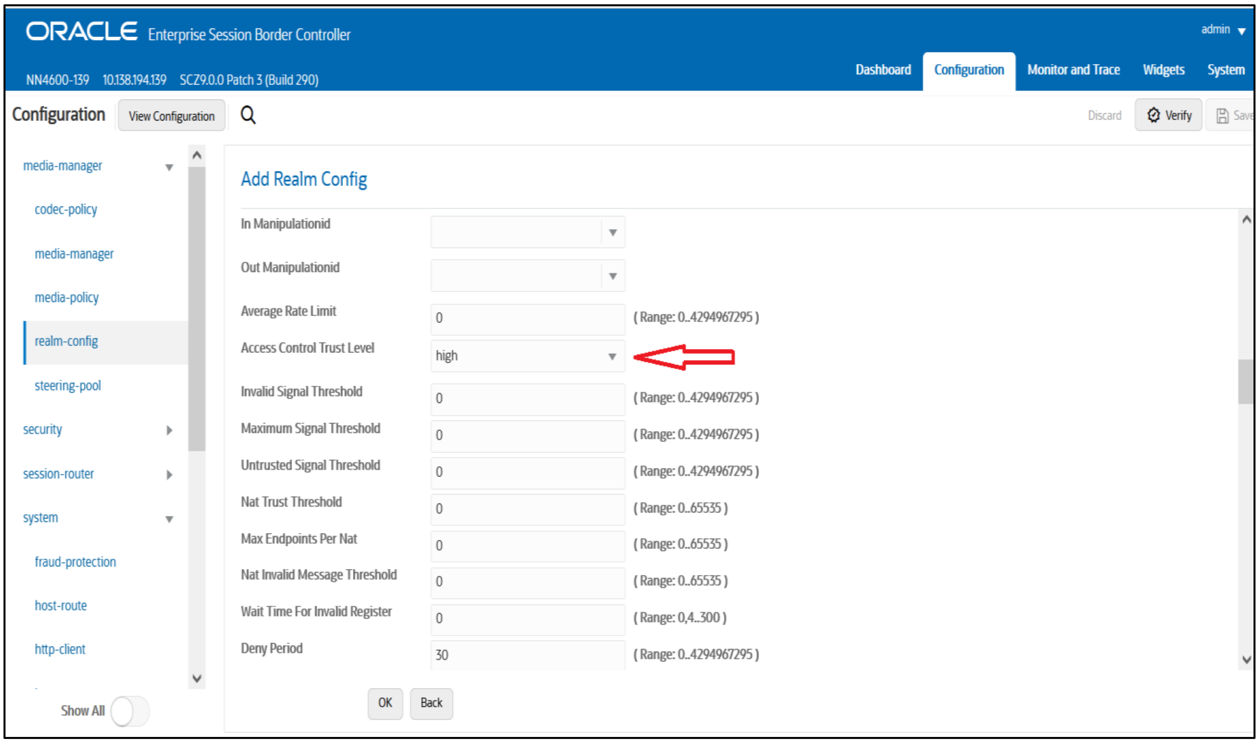
Network Interfaces: M00:0.4

Media Realm List:

Mm In Realm: ☑ enable

Mm In Network: ☑ enable

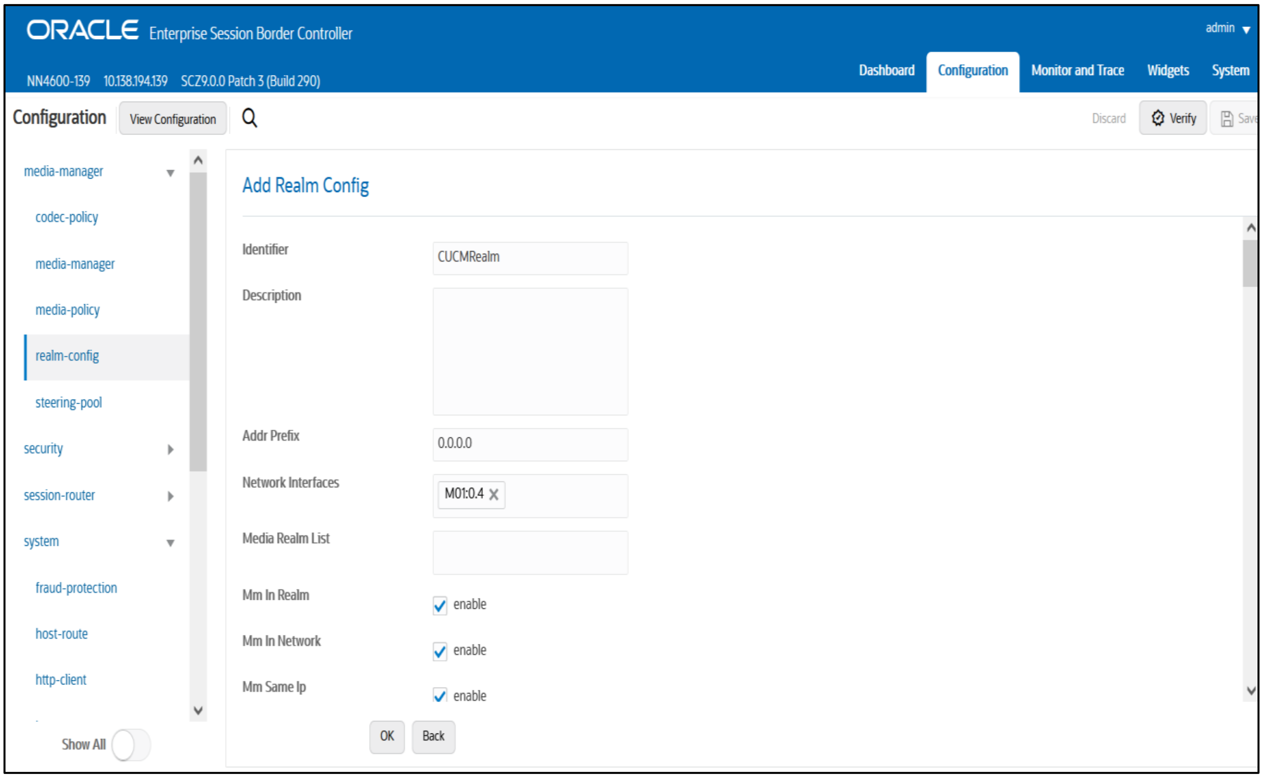
Mm Same Ip: ☑ enable



Add Realm Config

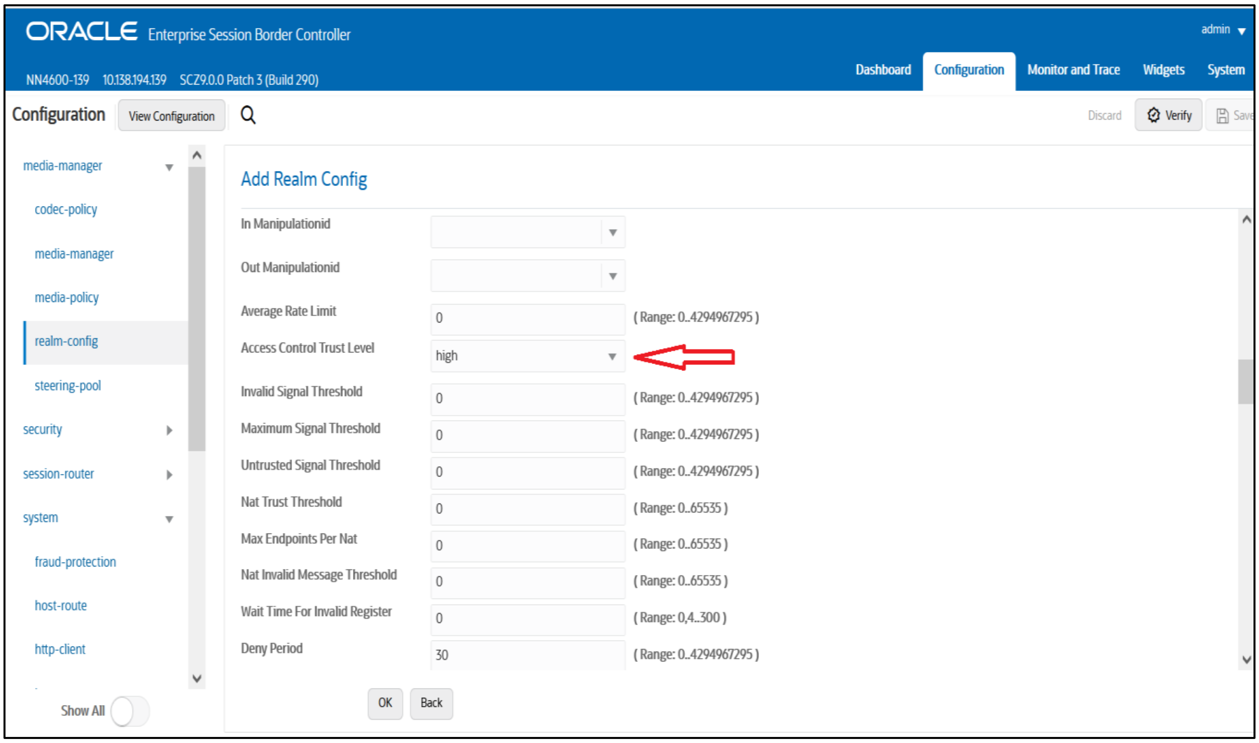
In Manipulationid		
Out Manipulationid		
Average Rate Limit	0	(Range: 0..4294967295)
Access Control Trust Level	high	
Invalid Signal Threshold	0	(Range: 0..4294967295)
Maximum Signal Threshold	0	(Range: 0..4294967295)
Untrusted Signal Threshold	0	(Range: 0..4294967295)
Nat Trust Threshold	0	(Range: 0..65535)
Max Endpoints Per Nat	0	(Range: 0..65535)
Nat Invalid Message Threshold	0	(Range: 0..65535)
Wait Time For Invalid Register	0	(Range: 0,4..300)
Deny Period	30	(Range: 0..4294967295)

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



Add Realm Config

Identifier	CUCMRealm
Description	
Addr Prefix	0.0.0.0
Network Interfaces	M01:0.4
Media Realm List	
Mm In Realm	☑ enable
Mm In Network	☑ enable
Mm Same Ip	☑ enable



Add Realm Config

In Manipulationid		
Out Manipulationid		
Average Rate Limit	0	(Range: 0..4294967295)
Access Control Trust Level	high	
Invalid Signal Threshold	0	(Range: 0..4294967295)
Maximum Signal Threshold	0	(Range: 0..4294967295)
Untrusted Signal Threshold	0	(Range: 0..4294967295)
Nat Trust Threshold	0	(Range: 0..65535)
Max Endpoints Per Nat	0	(Range: 0..65535)
Nat Invalid Message Threshold	0	(Range: 0..65535)
Wait Time For Invalid Register	0	(Range: 0,4..300)
Deny Period	30	(Range: 0..4294967295)

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

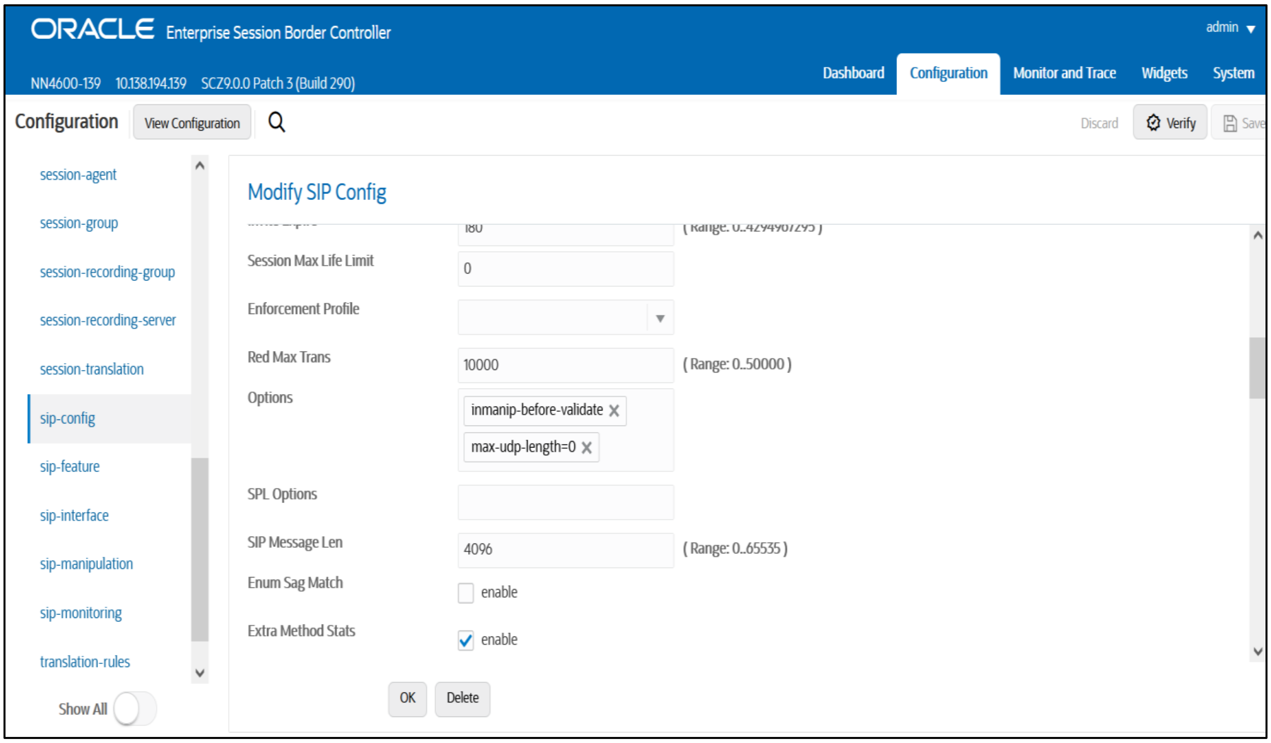
8.8. Enable sip-config

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
- inmanip-before-validate

For more info, please refer to SBC security guide given in the above section.



Modify SIP Config

	180	(Range: 0..4294967295)
Session Max Life Limit	0	
Enforcement Profile		
Red Max Trans	10000	(Range: 0..50000)
Options	inmanip-before-validate max-udp-length=0	
SPL Options		
SIP Message Len	4096	(Range: 0..65535)
Enum Sag Match	☐ enable	
Extra Method Stats	☑ enable	

8.9. Configuring a certificate for SBC

This section describes how to configure the SBC for both TLS and SRTP communication with Zoom

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

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.

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

2) Deploy the SBC and Root certificates on the SBC

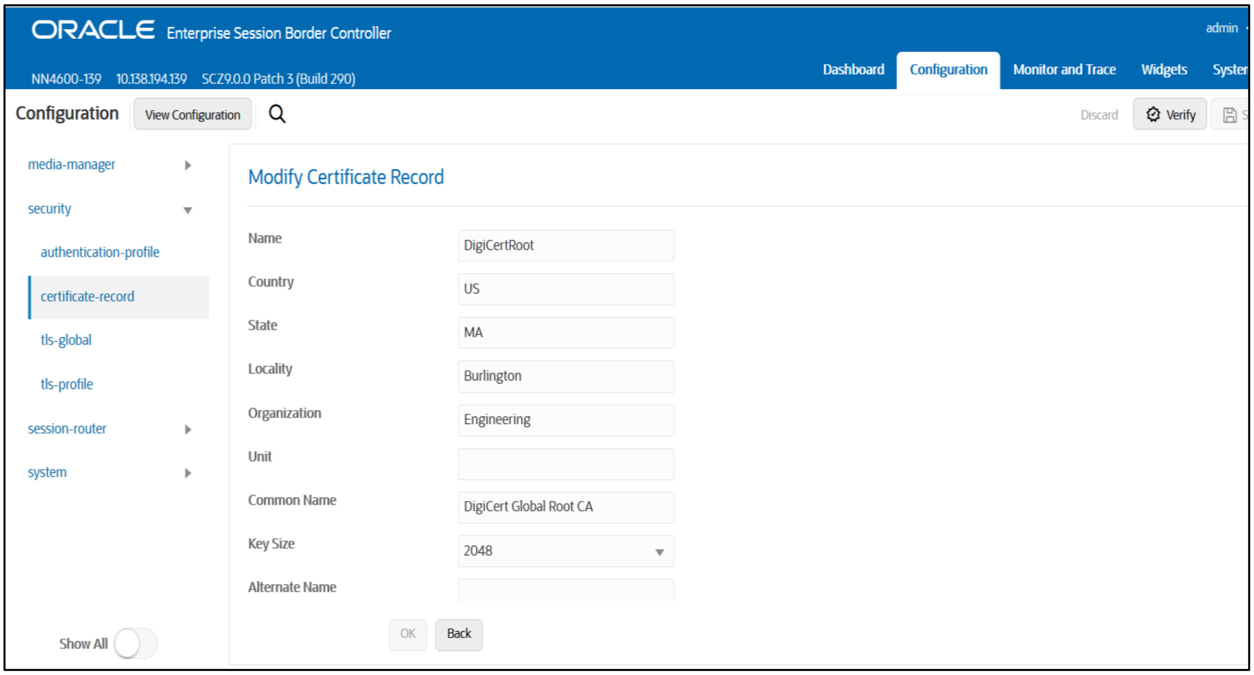
The following, DigitCert GlobalRootCA and DigiCert SHA2 Secure Server CA are the root and intermediate CA certificates used to sign the SBC's end entity certificate.

To trust Zoom certificates, your SBC must have below DigiCert Global Root CA, DigiCert Global Root G2 and DigiCert Global Root G3 installed.

Note : Since both Oracle SBC and Zoom use DigiCert Global Root CA only one certificate record should be created for the DigiCert Global Root CA certificate.

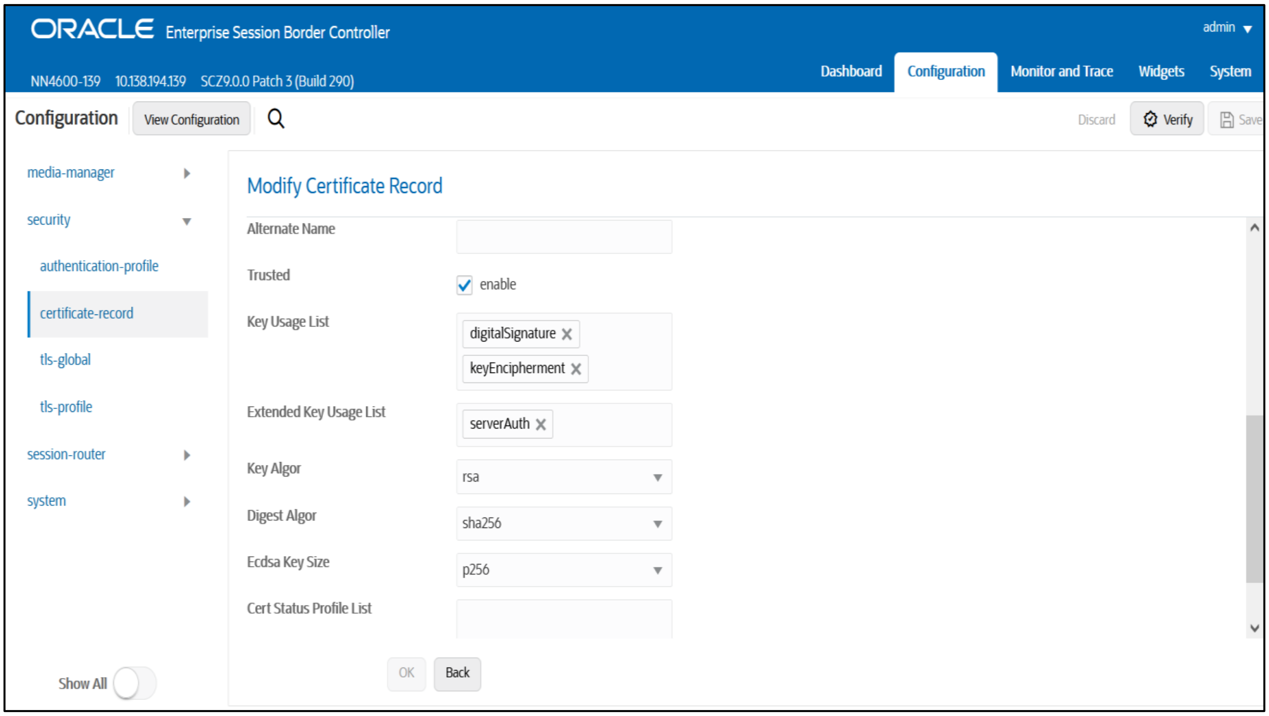
Step 1 – Creating the certificate record

Go to security->Certificate Record and configure the SBC entity certificate for SBC as shown below. **We are creating this certificate for Zoom Side.** The certificate can be from any root CA which is supported by Zoom.



Modify Certificate Record

Name: DigiCertRoot
Country: US
State: MA
Locality: Burlington
Organization: Engineering
Unit:
Common Name: DigiCert Global Root CA
Key Size: 2048
Alternate Name:



Modify Certificate Record

Alternate Name:
Trusted: ☑ enable
Key Usage List: digitalSignature, keyEncipherment
Extended Key Usage List: serverAuth
Key Algor: rsa
Digest Algor: sha256
Ecdsa Key Size: p256
Cert Status Profile List:

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

Config Parameter	Digicert Intermediate	DigiCert Root CA	DigiCertRootG2	DigiCertRootG3
Common Name	DigiCert SHA2 Secure Server CA	DigiCert Global Root CA	DigiCert Global RootG2	DigiCert Global RootG3
Key Size	2048	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignaturekey Encipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage list	serverAuth	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256	Sha256

Below is the list of Zoom approved CA Vendors. Oracle SBC Certificate can be signed by any of these Certificate Authorities.

Certificate Issuer Organization	Common Name or Certificate Name
Buypass AS-983163327	Buypass Class 2 Root CA
Buypass AS-983163327	Buypass Class 3 Root CA
Baltimore	Baltimore CyberTrust Root
Cybertrust, Inc	Cybertrust Global Root
DigiCert Inc	DigiCert Assured ID Root CA
DigiCert Inc	DigiCert Assured ID Root G2
DigiCert Inc	DigiCert Assured ID Root G3
DigiCert Inc	DigiCert Global Root CA
DigiCert Inc	DigiCert Global Root G2
DigiCert Inc	DigiCert Global Root G3
DigiCert Inc	DigiCert High Assurance EV Root CA
DigiCert Inc	DigiCert Trusted Root G4

GeoTrust Inc.	GeoTrust Global CA
GeoTrust Inc.	GeoTrust Primary Certification Authority
GeoTrust Inc.	GeoTrust Primary Certification Authority - G2
GeoTrust Inc.	GeoTrust Primary Certification Authority - G3
GeoTrust Inc.	GeoTrust Universal CA
GeoTrust Inc.	GeoTrust Universal CA 2
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G6
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G6
Thawte, Inc.	Thawte Primary Root CA
Thawte, Inc.	Thawte Primary Root CA - G2
Thawte, Inc.	Thawte Primary Root CA - G3
VeriSign, Inc.	VeriSign Class 1 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 2 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G4
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign, Inc.	VeriSign Universal Root Certification Authority
AffirmTrust	AffirmTrust Commercial
AffirmTrust	AffirmTrust Networking
AffirmTrust	AffirmTrust Premium
AffirmTrust	AffirmTrust Premium ECC
Entrust, Inc.	Entrust Root Certification Authority
Entrust, Inc.	Entrust Root Certification Authority - EC1
Entrust, Inc.	Entrust Root Certification Authority - G2
Entrust, Inc.	Entrust Root Certification Authority - G4
Entrust.net	Entrust.net Certification Authority (2048)
GlobalSign	GlobalSign

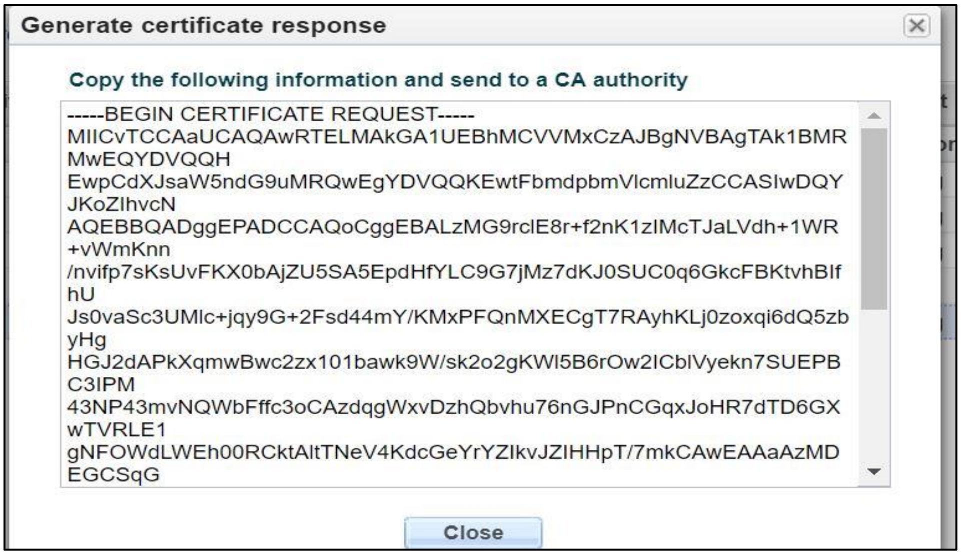
GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign nv-sa	GlobalSign Root CA
The GoDaddy Group, Inc.	Go Daddy Class 2 CA
GoDaddy.com, Inc.	Go Daddy Root Certificate Authority - G2
Starfield Technologies, Inc.	Starfield Class 2 CA
Starfield Technologies, Inc.	Starfield Root Certificate Authority - G2
QuoVadis Limited	QuoVadis Root CA 1 G3
QuoVadis Limited	QuoVadis Root CA 2
QuoVadis Limited	QuoVadis Root CA 2 G3
QuoVadis Limited	QuoVadis Root CA 3
QuoVadis Limited	QuoVadis Root CA 3 G3
QuoVadis Limited	QuoVadis Root Certification Authority
Comodo CA Limited	AAA Certificate Services
AddTrust AB	AddTrust Class 1 CA Root
AddTrust AB	AddTrust External CA Root
COMODO CA Limited	COMODO Certification Authority
COMODO CA Limited	COMODO ECC Certification Authority
COMODO CA Limited	COMODO RSA Certification Authority
The USERTRUST Network	USERTrust ECC Certification Authority
The USERTRUST Network	USERTrust RSA Certification Authority
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 2
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 3

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.



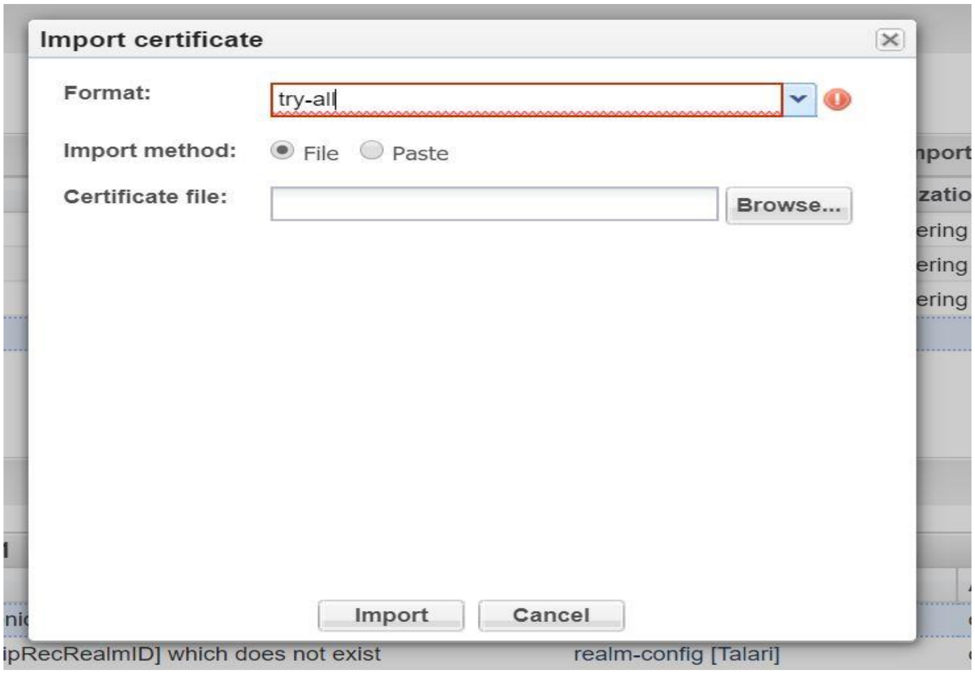
Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvTCCAaUCAQAwRTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMR
MwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzCCASIwDQY
JKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALzMG9rclE8r+f2nK1zIMcTJaLVdh+1WR
+vWmKnn
/nvifp7sKsUvFKX0bAjZU5SA5EpdHfYLC9G7jMz7dKJ0SUC0q6GkcFBKtvhBIf
hU
Js0vaSc3UMlc+jqy9G+2Fsd44mY/KMxPFQnMXECgT7RAyhKLj0zoxqi6dQ5zb
yHg
HGJ2dAPkXqmwBwc2zx101bawk9W/sk2o2gKWI5B6rOw2ICblVyekn7SUEPB
C3IPM
43NP43mvNQWbFffc3oCAzdqgWxvDzhQbvhu76nGJPnCGqxJoHR7dTD6GX
wTVRLE1
gNFOWdLWEh00RCktAltTNeV4KdcGeYrYZIkvJZIHHpT/7mkCAwEAAaAzMD
EGCSqG
```

- Also, note that a save/activate is required

Step 3 – Deploy SBC & root certificates

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



Import certificate

Format: try-all

Import method: ● File ○ Paste

Certificate file:

Repeat these steps to import all the root and intermediate CA certificates into the SBC:

- DigiCertIntermediate
- DigiCertGlobalRootCA
- DigiCertGlobalRootG2
- DigiCertGlobalRootG3

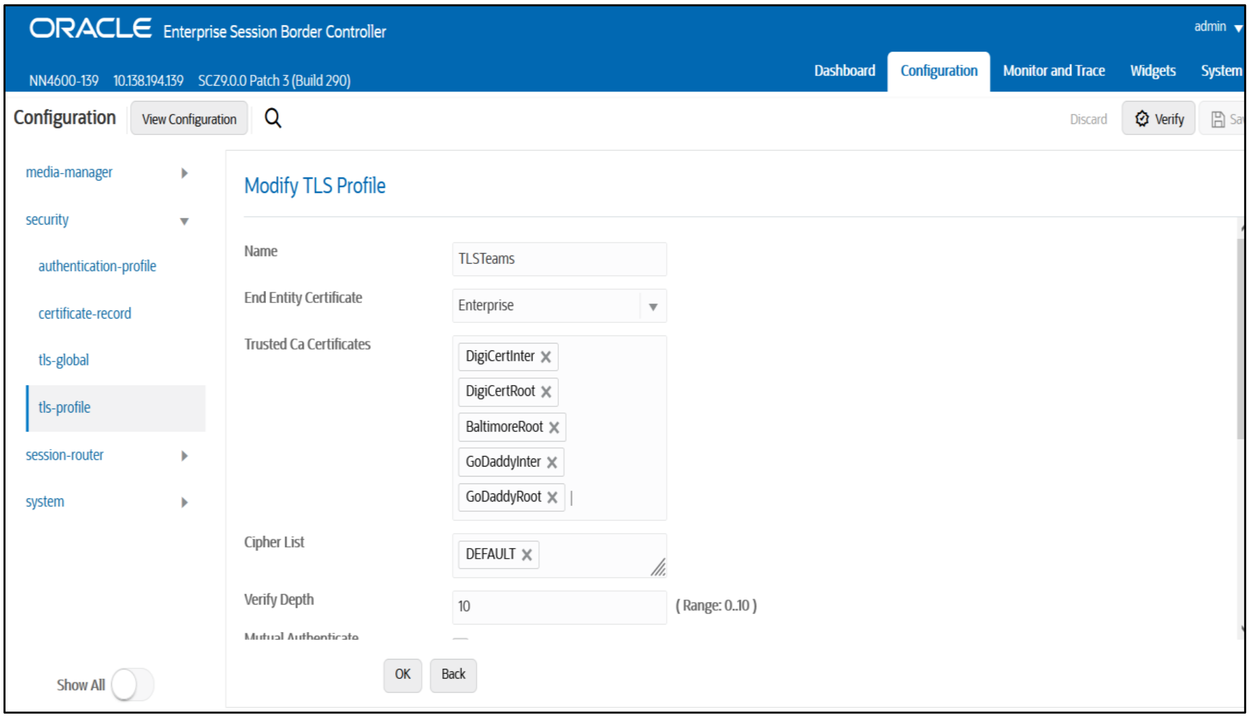
At this stage all the required certificates have been imported to the SBC for Zoom.

8.10. TLS-Profile

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

Zoom supports the following signaling ciphers that need to be added to the TLS profile:

- TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA-384
- RSA-WITH-AES-256-CBC-SHA-256



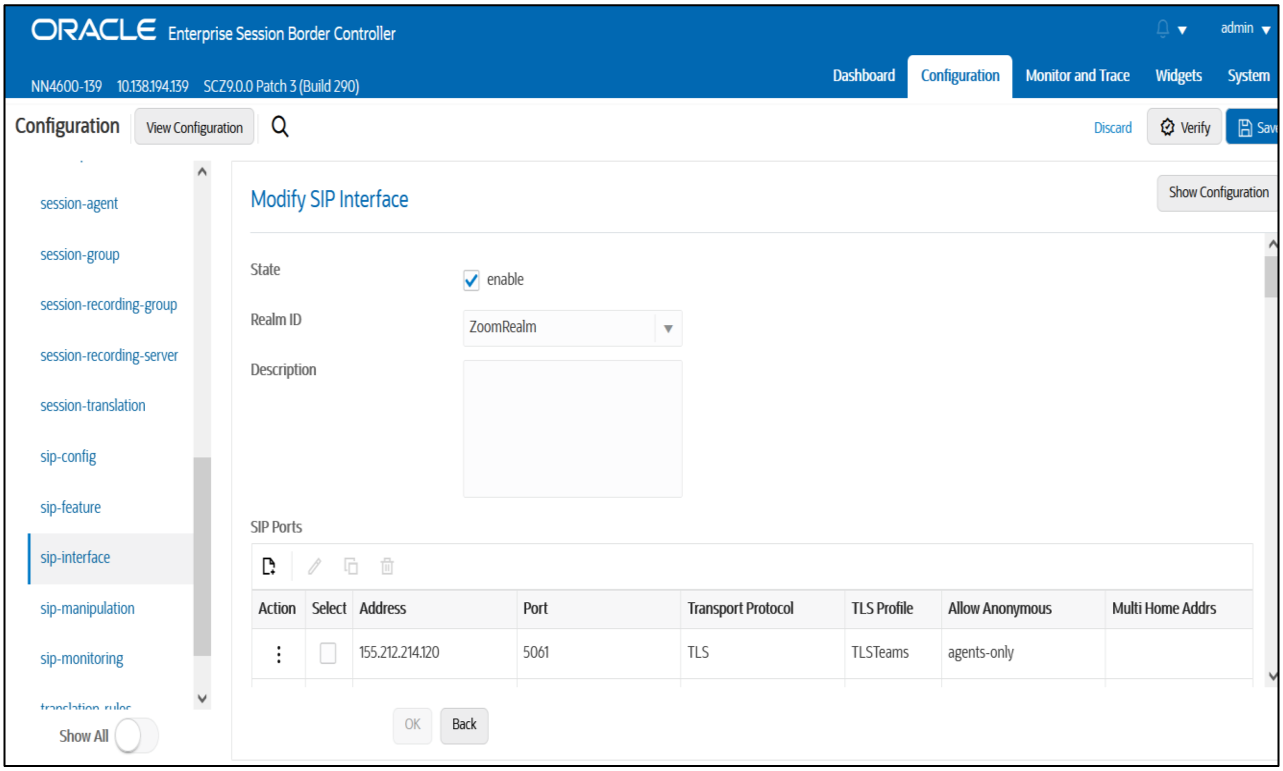
Modify TLS Profile

Name	TLSTeams
End Entity Certificate	Enterprise
Trusted Ca Certificates	DigiCertInter DigiCertRoot BaltimoreRoot GoDaddyInter GoDaddyRoot
Cipher List	DEFAULT
Verify Depth	10 (Range: 0..10)
Mutual Authenticate	

8.11. Configure SIP Interfaces

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

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



Modify SIP Interface

State ☑ enable

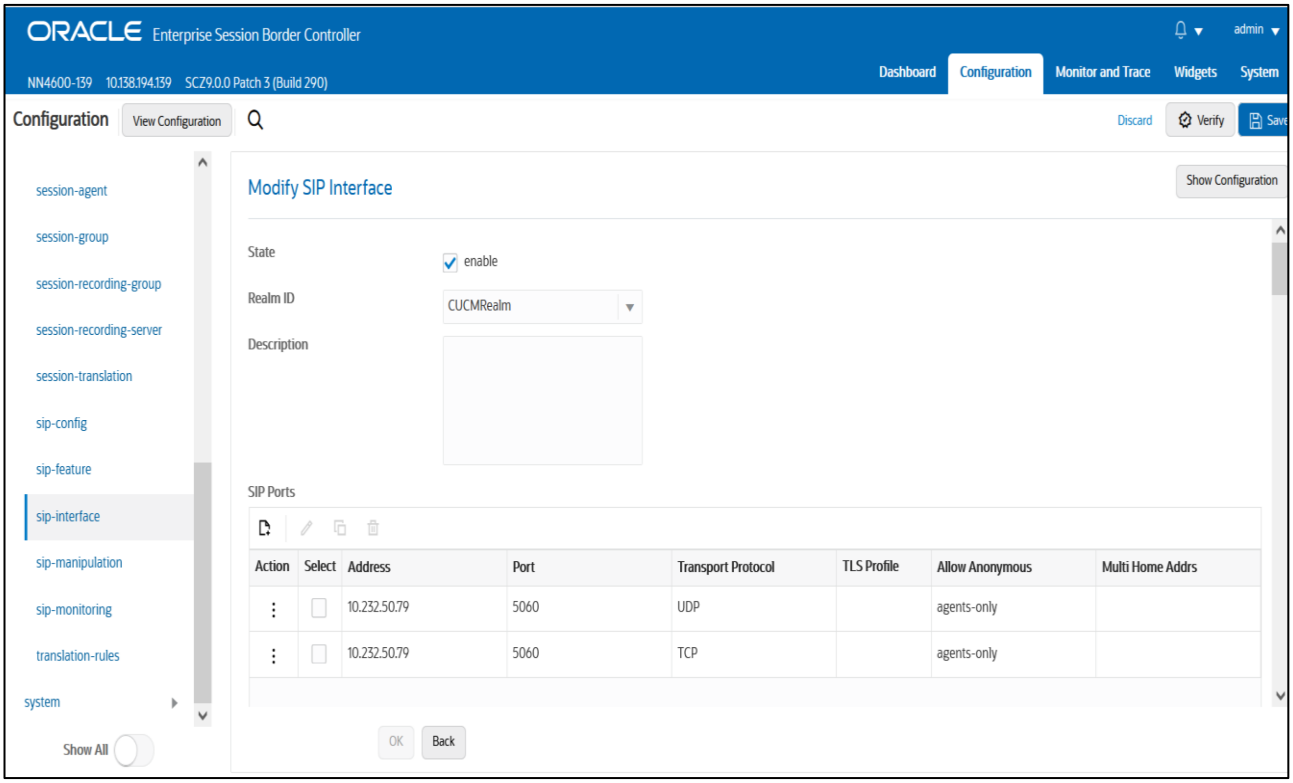
Realm ID ZoomRealm

Description

SIP Ports

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
⋮	□	155.212.214.120	5061	TLS	TLSTeams	agents-only	

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



Modify SIP Interface

State ☑ enable

Realm ID CUCMRealm

Description

SIP Ports

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
⋮	□	10.232.50.79	5060	UDP		agents-only	
⋮	□	10.232.50.79	5060	TCP		agents-only	

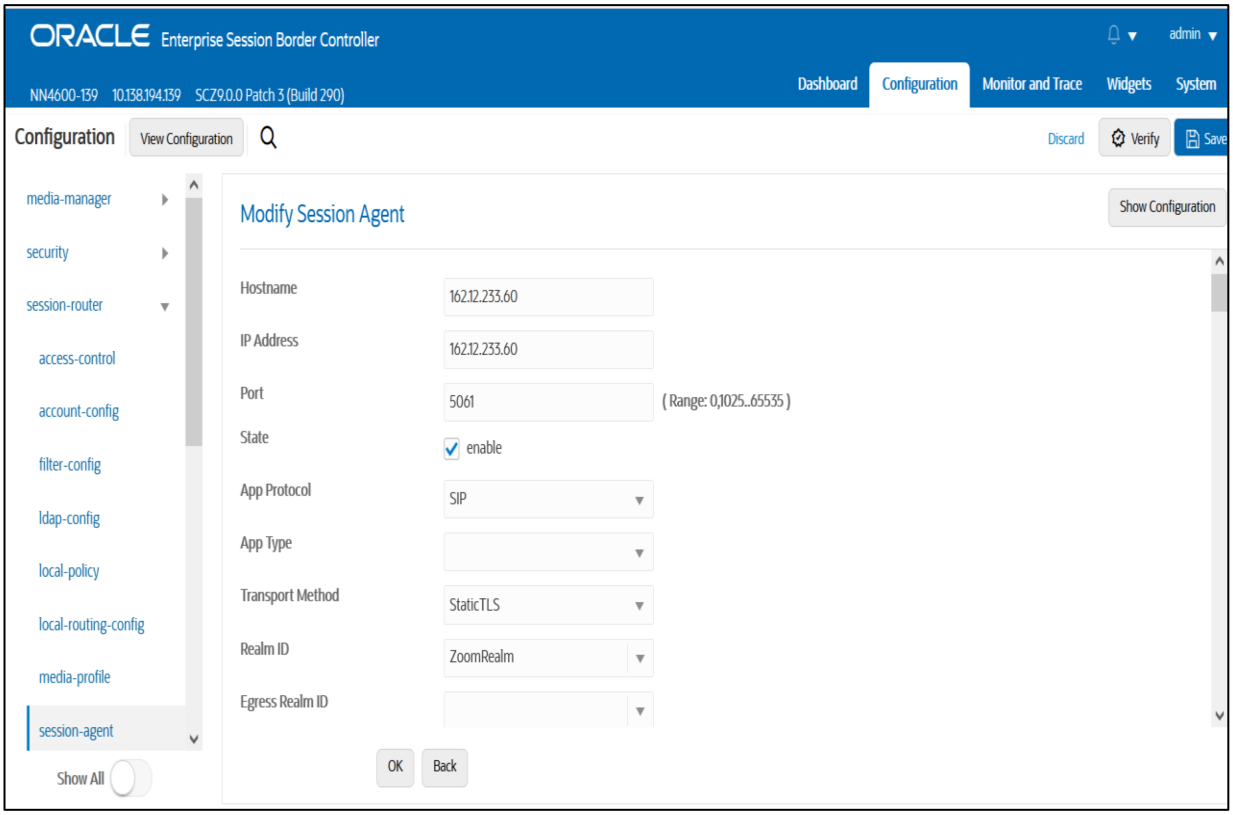
Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

8.12. Configure session-agent

Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. 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 Zoom with the following parameters.
Go to session-router->Session-Agent.

- hostname and IP address as “162.12.233.60”
- port 5061
- realm-id – needs to match the realm created for Zoom
- transport set to “StaticTLS”
- ping-method –OPTIONS message
- ping-interval to 30 secs

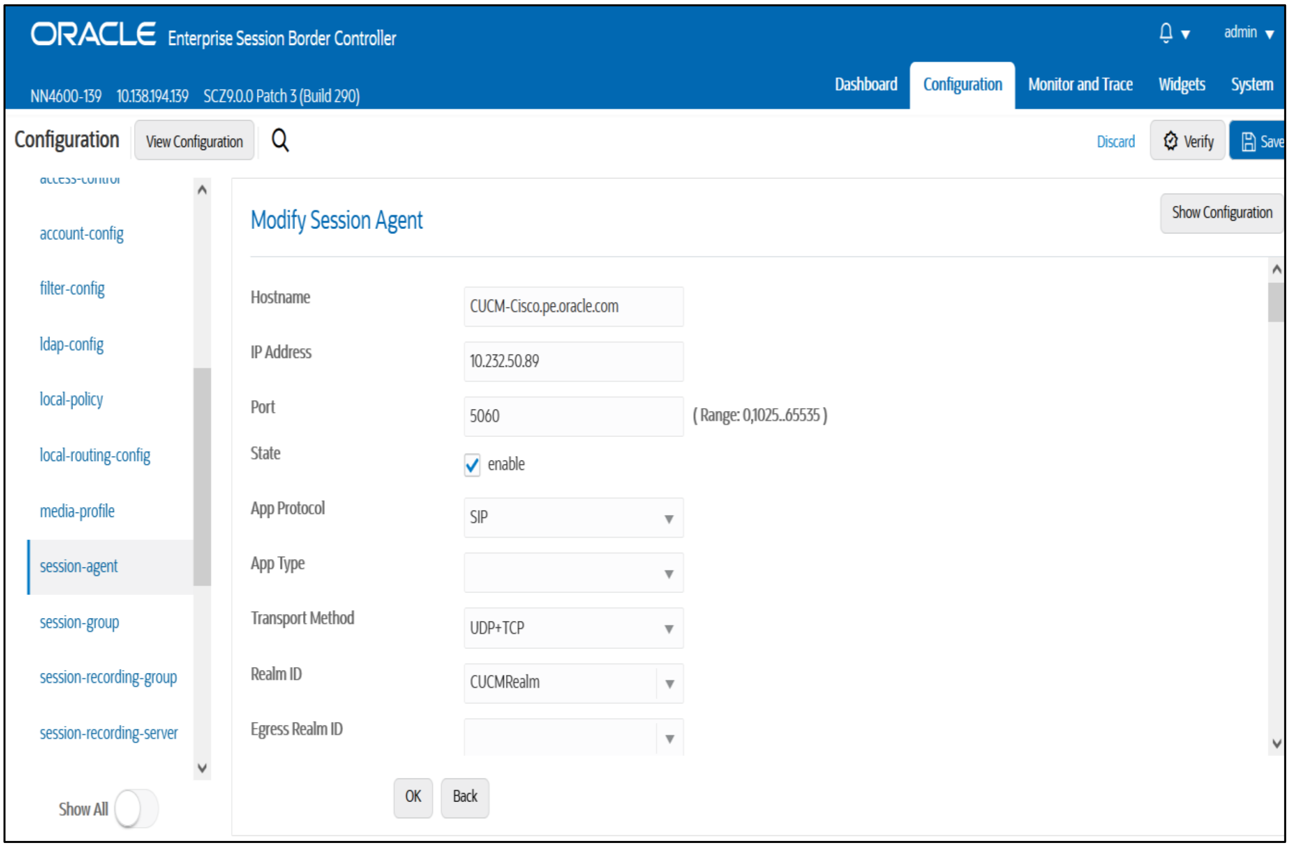


Modify Session Agent

Hostname: 162.12.233.60
IP Address: 162.12.233.60
Port: 5061 (Range: 0,1025..65535)
State: ☑ enable
App Protocol: SIP
App Type:
Transport Method: StaticTLS
Realm ID: ZoomRealm
Egress Realm ID:

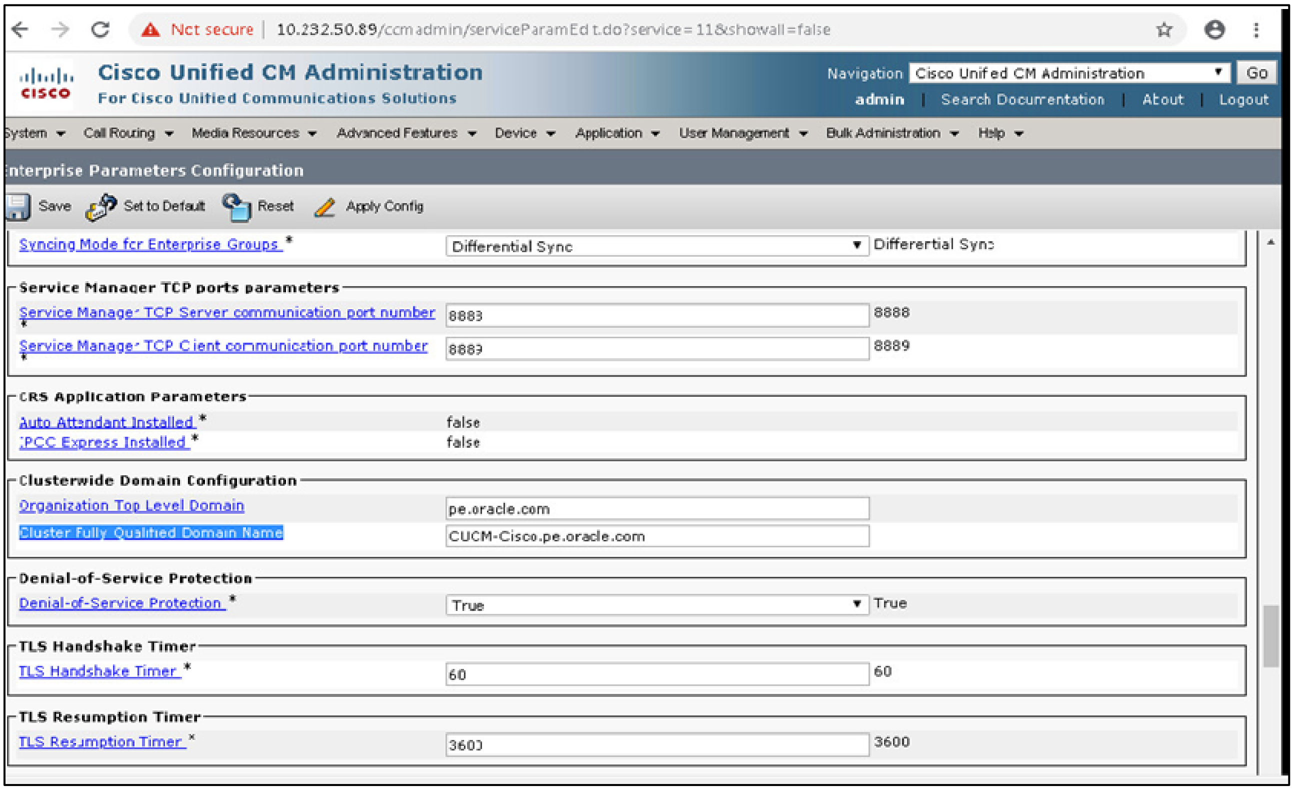
Similarly, configure the session-agents for the Cisco Side as below:

- 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.



Modify 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	



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
Save
Set to Default
Reset
Apply Config

Enterprise Parameters Configuration

Syncing Mode for Enterprise Groups *	Differential Sync	Differential Sync

Service Manager TCP ports parameters

Service Manager TCP Server communication port number *	8888	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

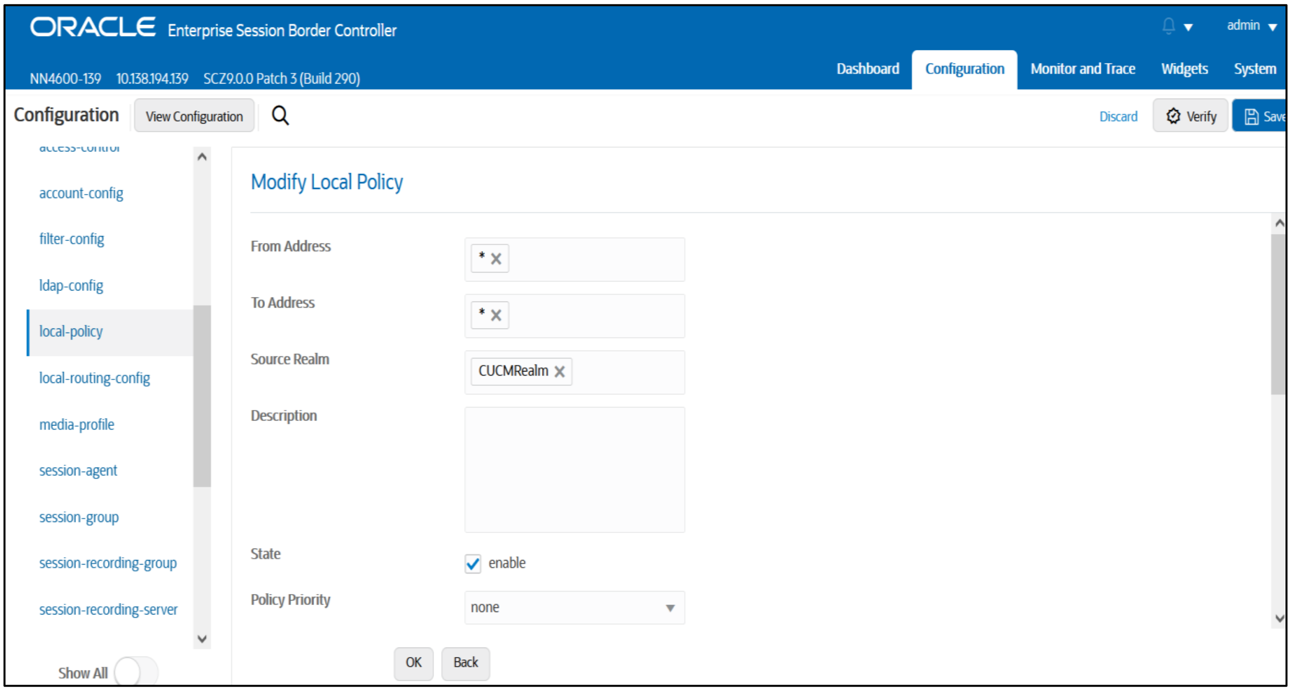
TLS Resumption Timer

TLS Resumption Timer *	3600	3600

8.13. Configure local-policy

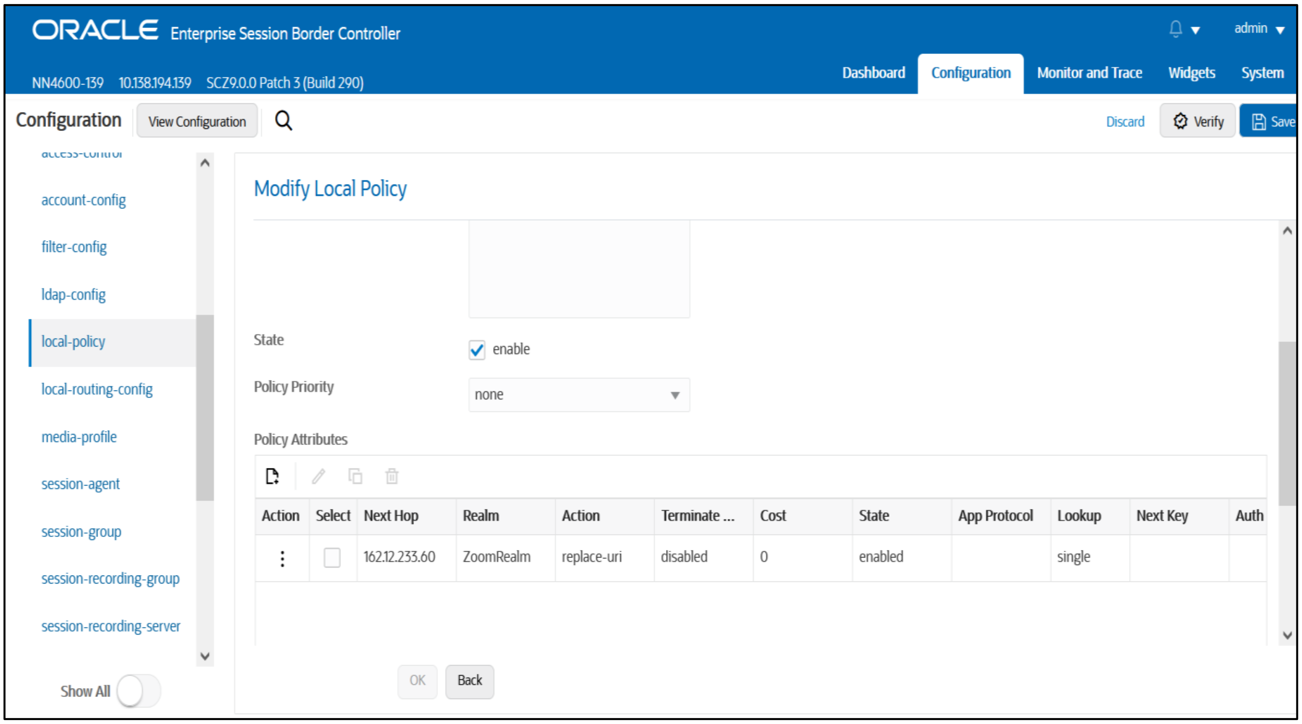
Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

To route the calls from Cisco side to Zoom side, Use the below local –policy



Modify Local Policy

From Address	*
To Address	*
Source Realm	CUCMRealm
Description	
State	☑ enable
Policy Priority	none



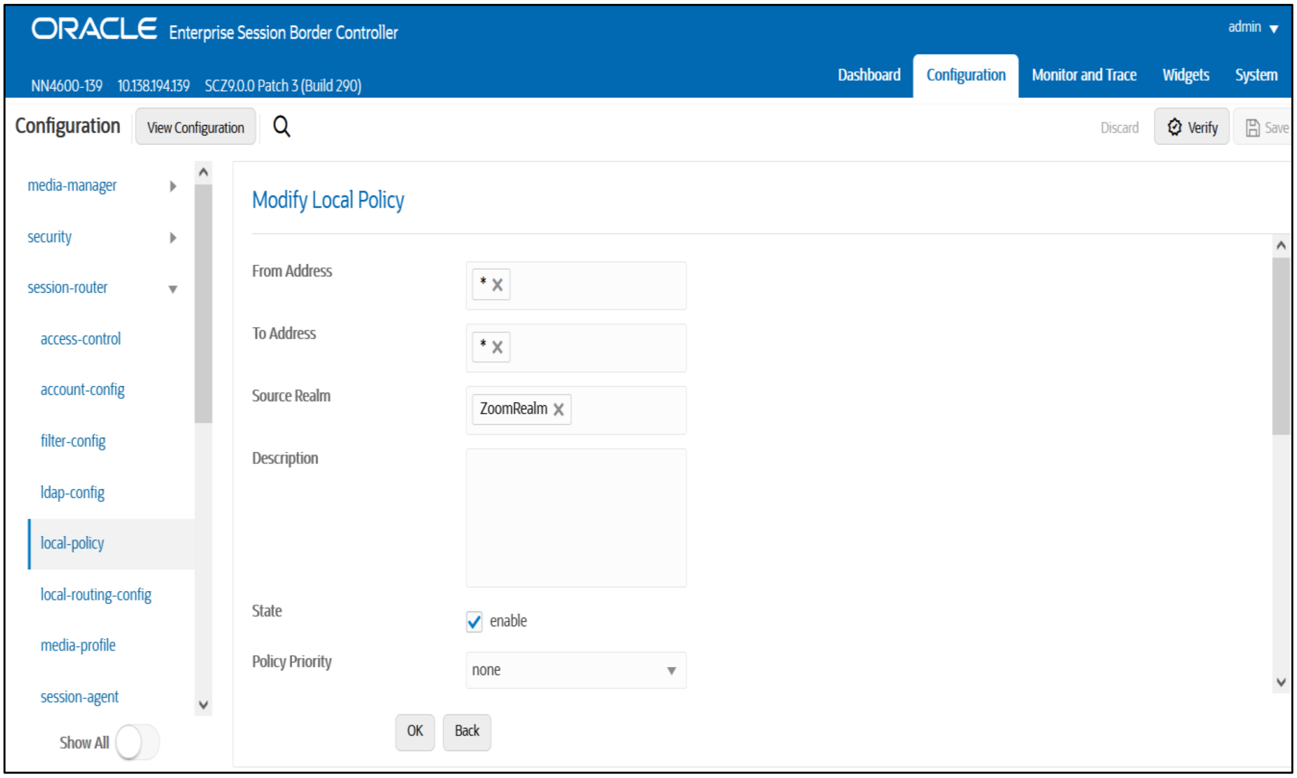
Modify Local Policy

State	☑ enable
Policy Priority	none

Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate ...	Cost	State	App Protocol	Lookup	Next Key	Auth
⋮	□	162.12.233.60	ZoomRealm	replace-uri	disabled	0	enabled		single		

To route the calls from the Zoom side to Cisco side, Use the below local –policy



Modify Local Policy

From Address: *

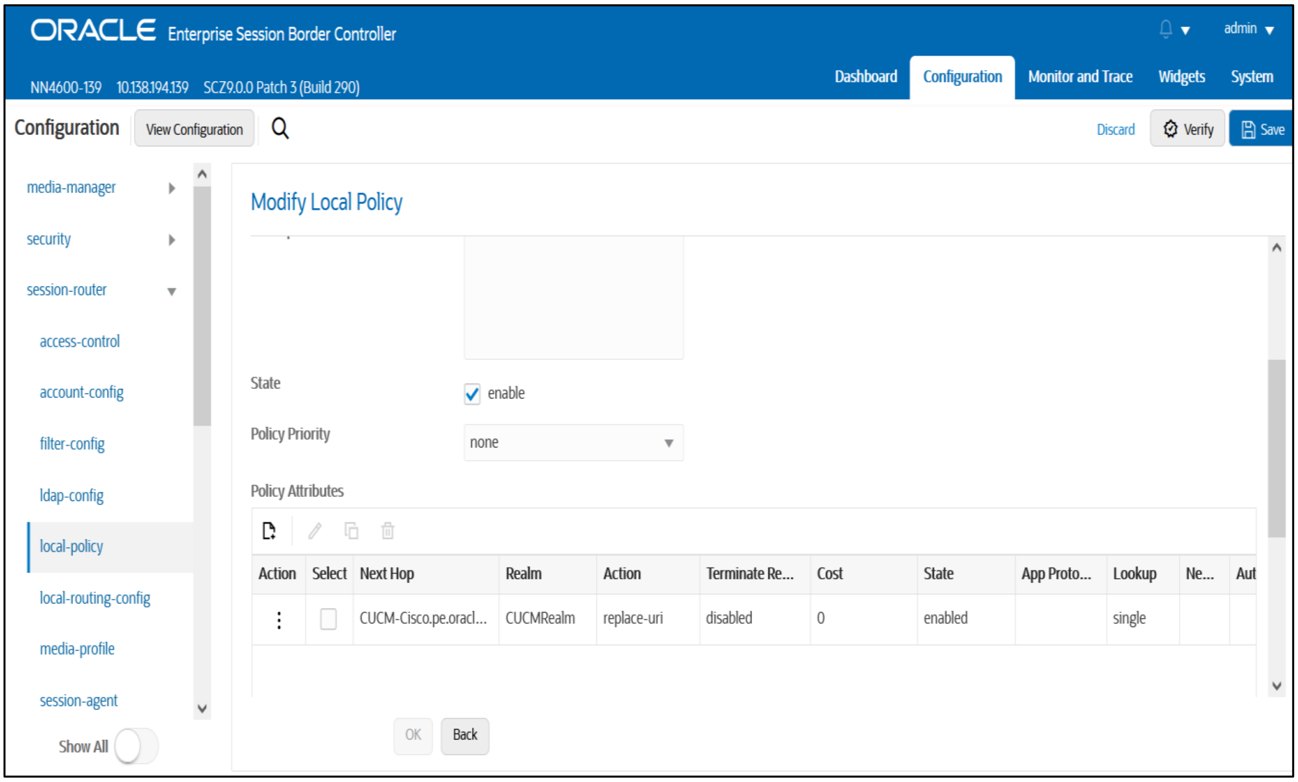
To Address: *

Source Realm: ZoomRealm

Description:

State: ☑ enable

Policy Priority: none



Modify Local Policy

State: ☑ enable

Policy Priority: none

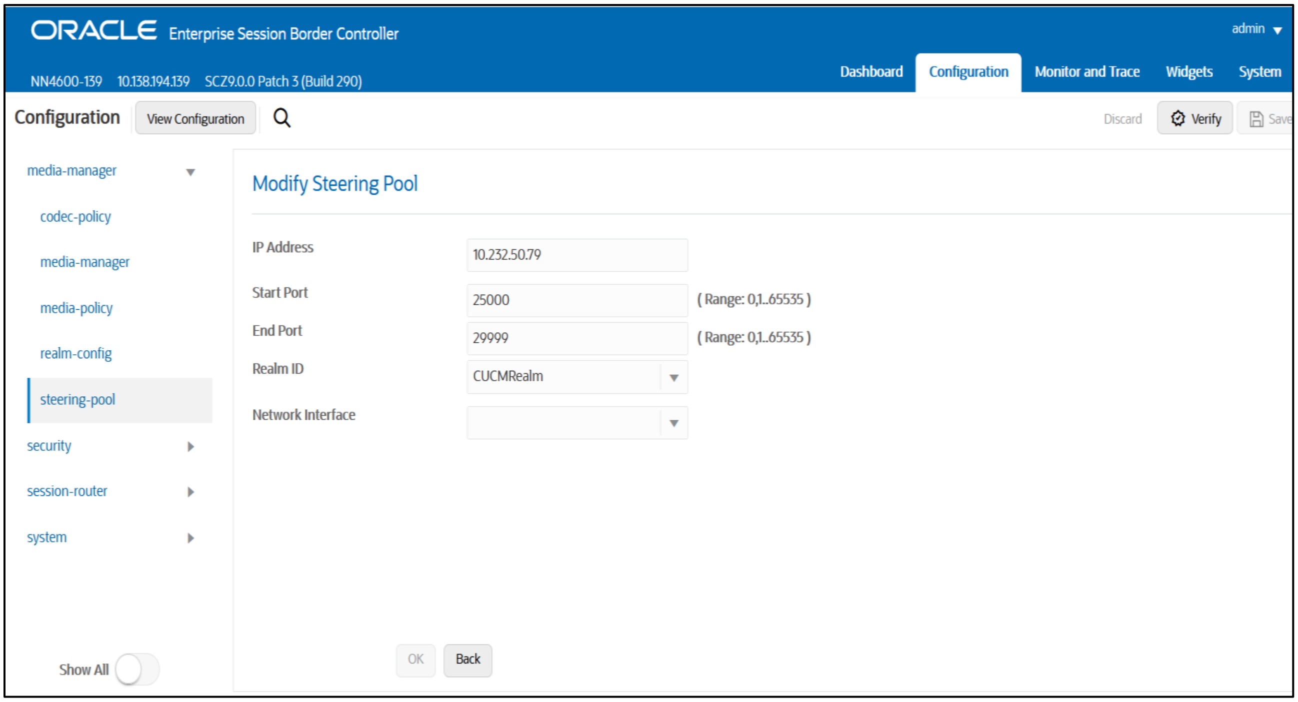
Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Re...	Cost	State	App Proto...	Lookup	Ne...	Aut
⋮	□	CUCM-Cisco.pe.oracl...	CUCMRealm	replace-uri	disabled	0	enabled		single		

8.14. Configure steering-pool

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

Cisco side steering pool.



Modify Steering Pool

IP Address: 10.232.50.79

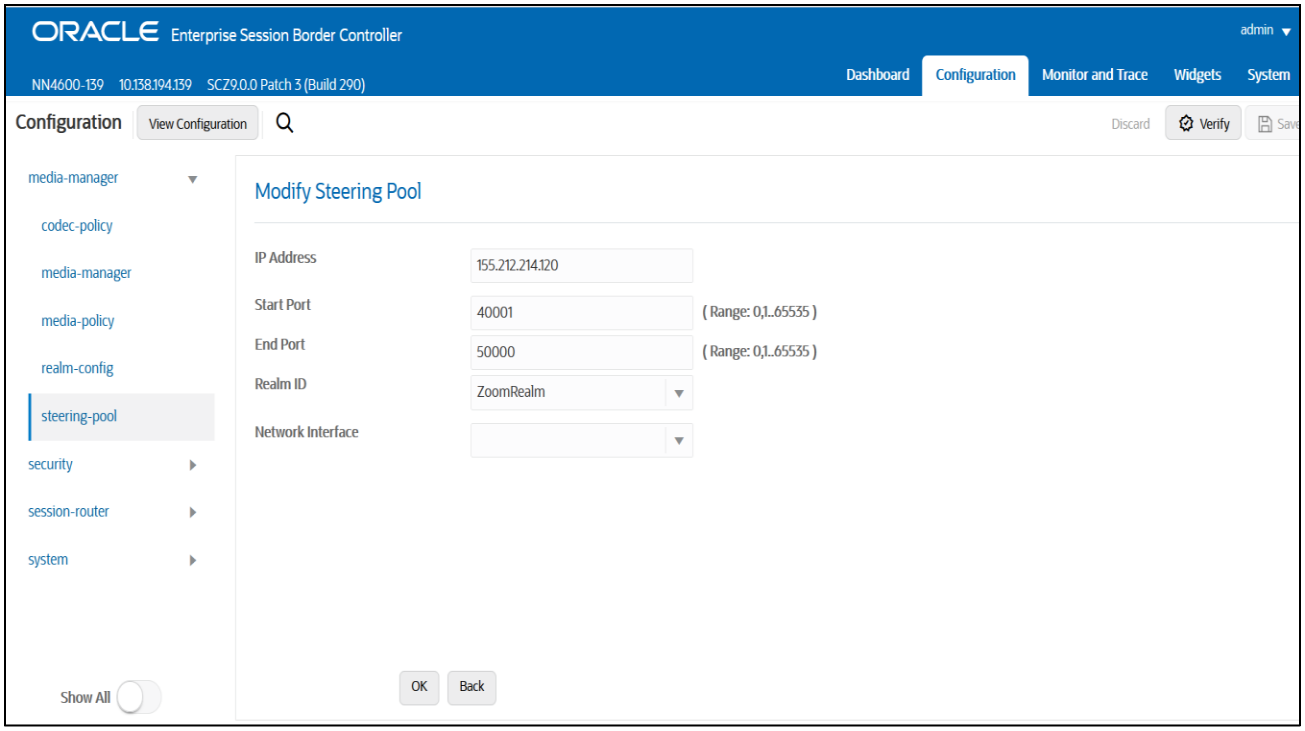
Start Port: 25000 (Range: 0,1..65535)

End Port: 29999 (Range: 0,1..65535)

Realm ID: CUCMRealm

Network Interface:

Zoom side steering pool.



Modify Steering Pool

IP Address: 155.212.214.120

Start Port: 40001 (Range: 0,1..65535)

End Port: 50000 (Range: 0,1..65535)

Realm ID: ZoomRealm

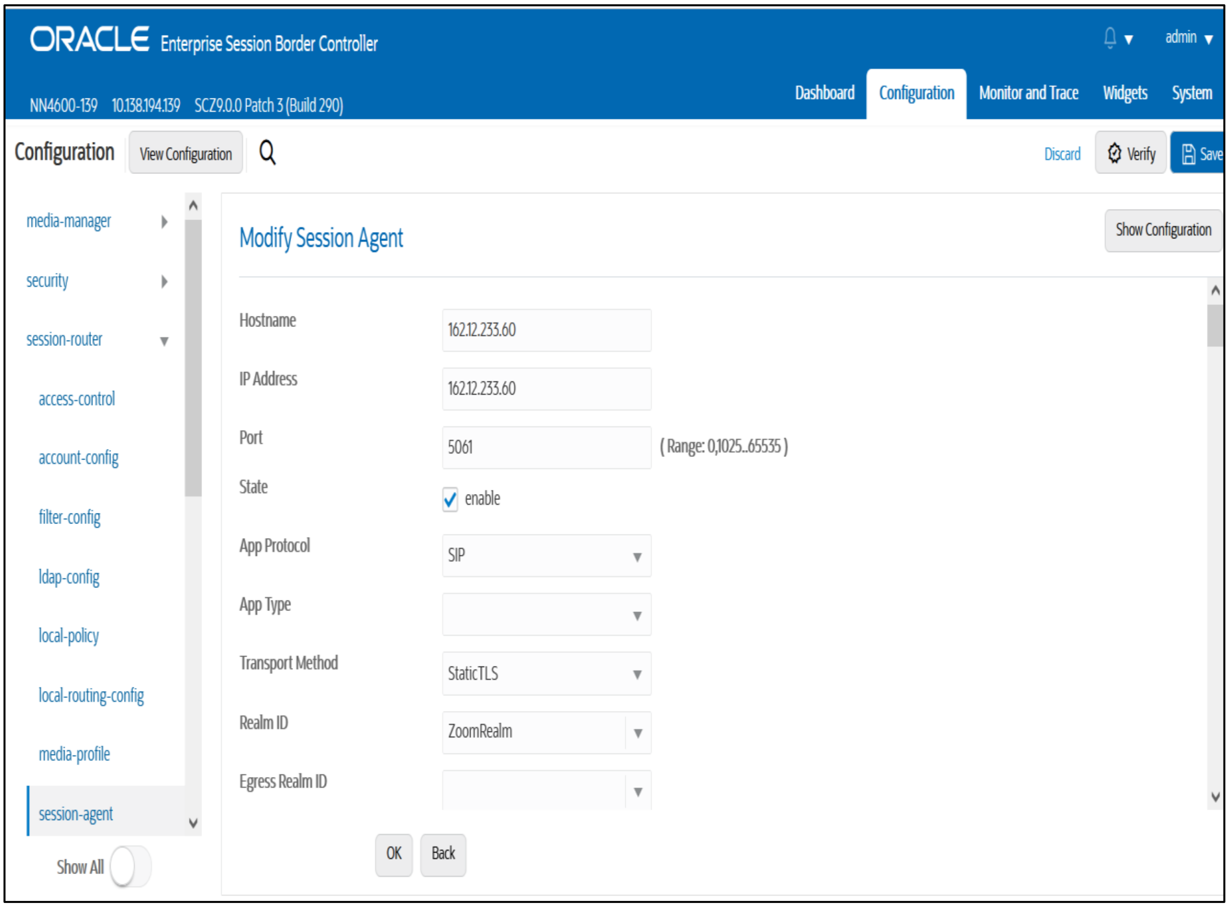
Network Interface:

8.15. 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**.

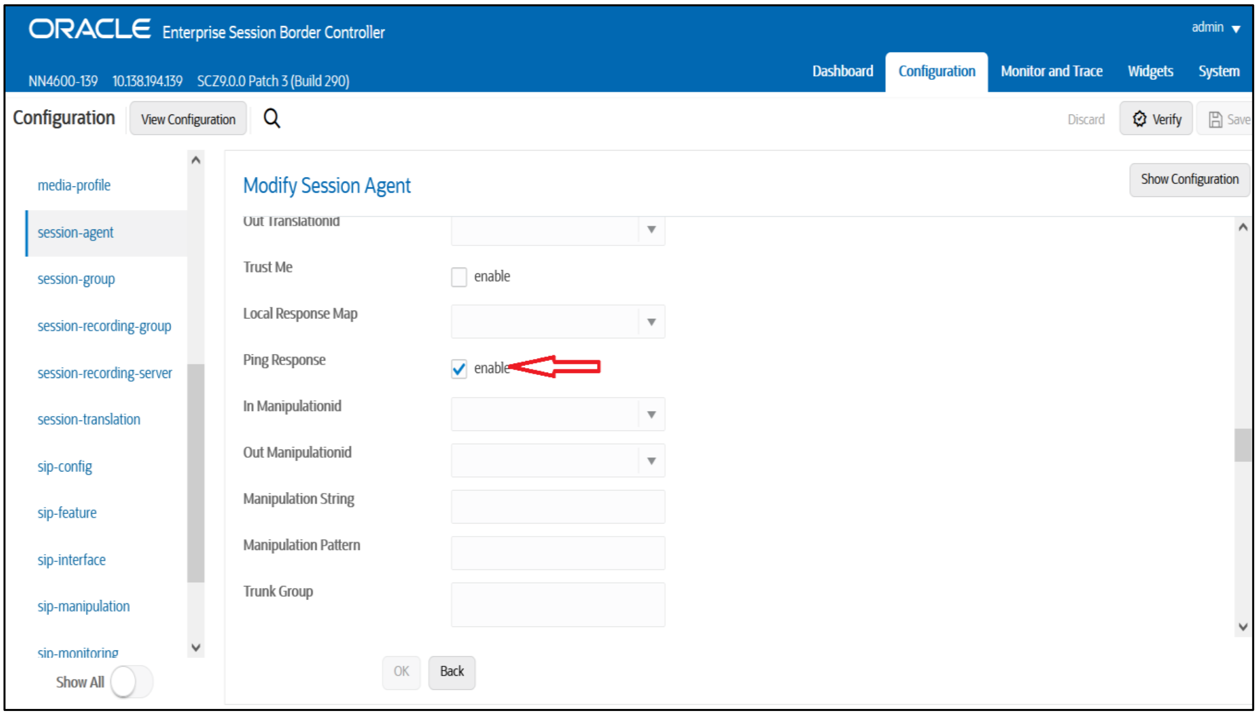
Ping Response:

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.



Modify Session Agent

Hostname	162.12.233.60
IP Address	162.12.233.60
Port	5061 (Range: 0,1025..65535)
State	☑ enable
App Protocol	SIP
App Type	
Transport Method	StaticTLS
Realm ID	ZoomRealm
Egress Realm ID	



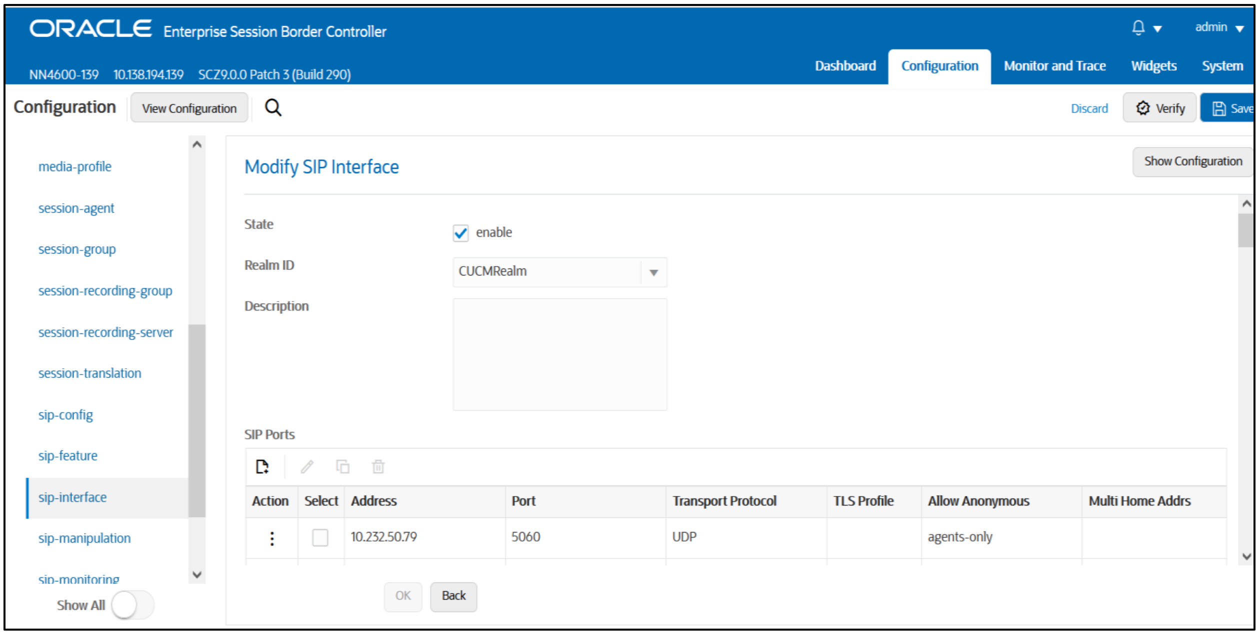
Modify Session Agent

Out Translationid	
Trust Me	☐ enable
Local Response Map	
Ping Response	☑ enable
In Manipulationid	
Out Manipulationid	
Manipulation String	
Manipulation Pattern	
Trunk Group	

8.16. 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 Zoom and vice versa. To do that, please set the parameter "**Add SDP Invite**" as both under Zoom sip interface 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.

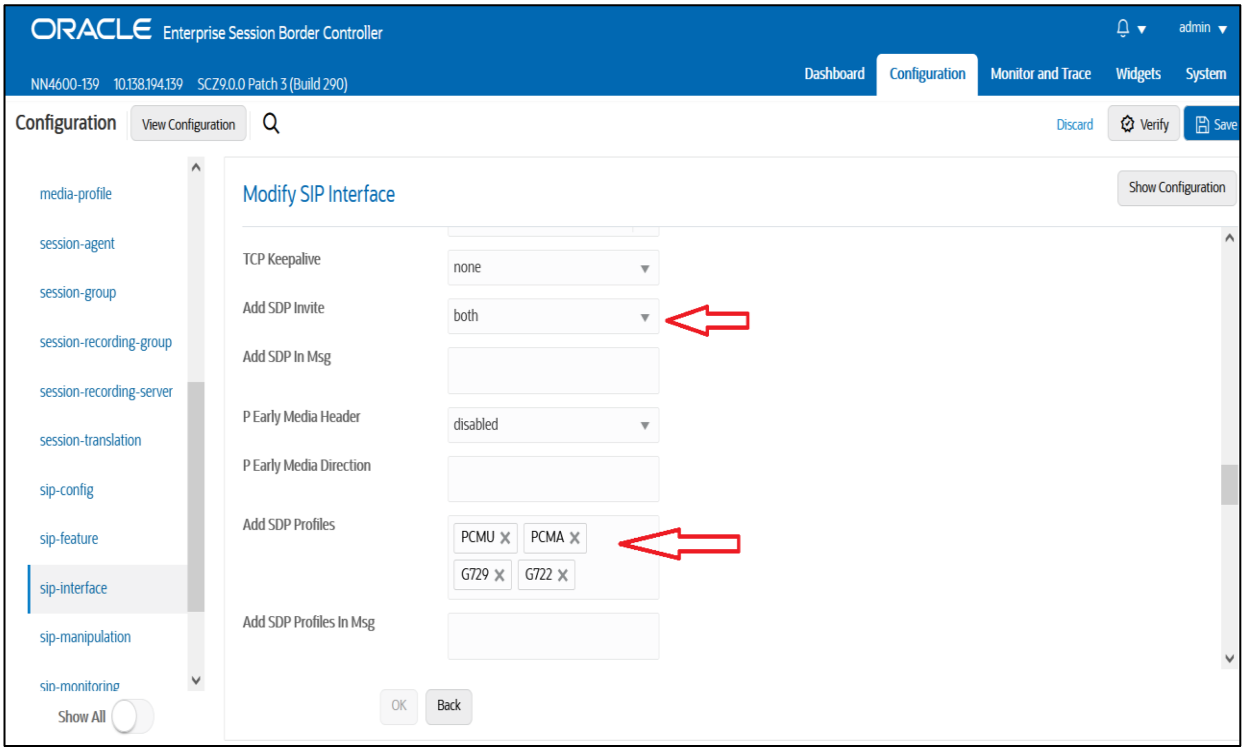


Modify SIP Interface

State	☑ enable
Realm ID	CUCMRealm
Description	

SIP Ports

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
⋮	☐	10.232.50.79	5060	UDP		agents-only	

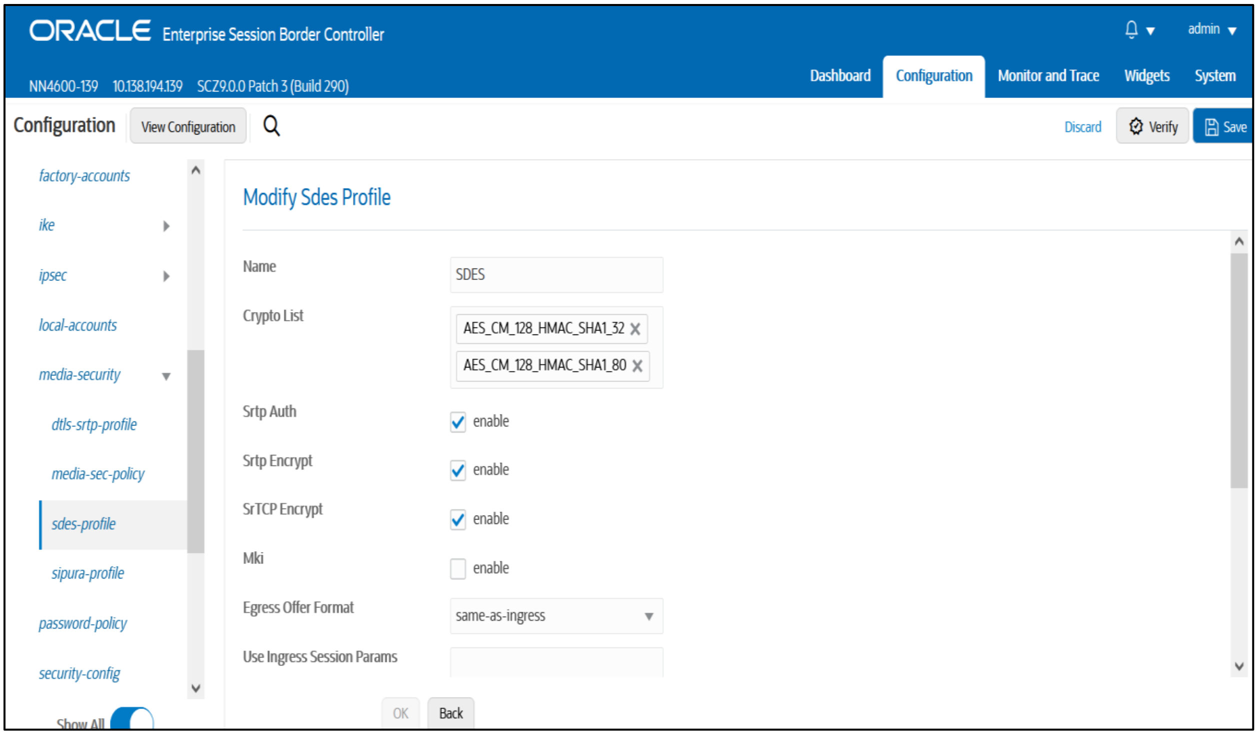


Modify SIP Interface

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, G722
Add SDP Profiles In Msg	

8.17. Configure sdes profile

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

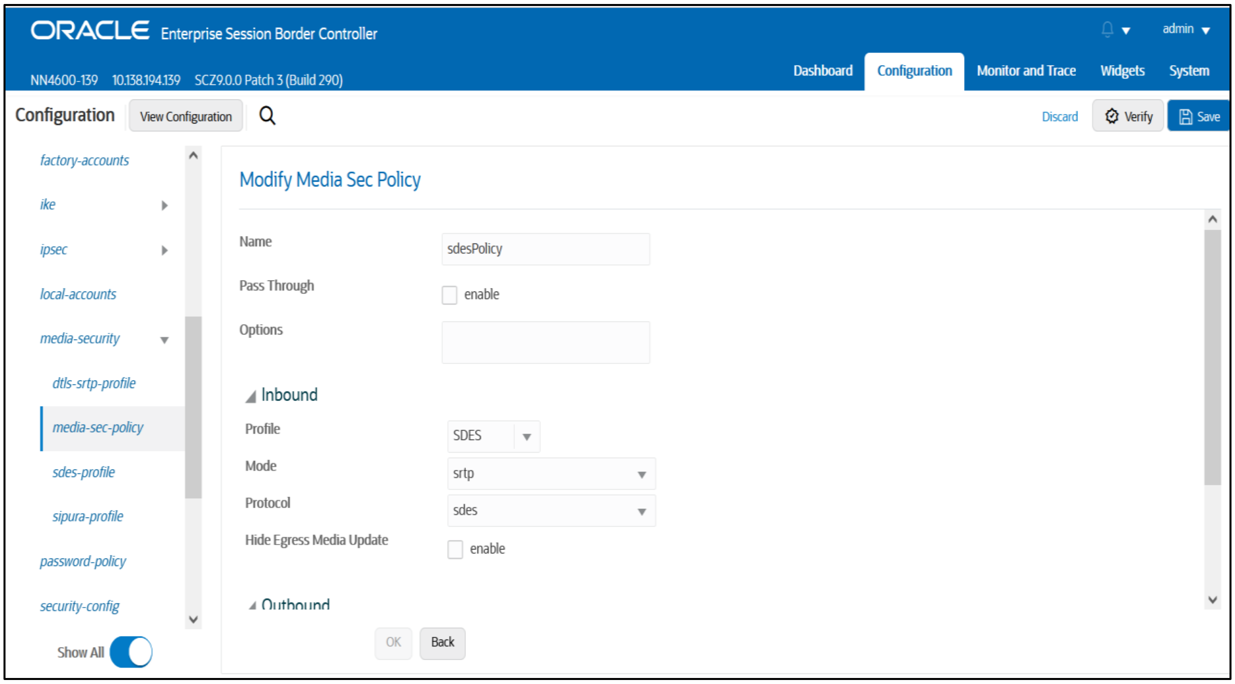


Modify Sdes Profile

Name	SDES
Crypto List	AES_CM_128_HMAC_SHA1_32 AES_CM_128_HMAC_SHA1_80
Srtp Auth	☑ enable
Srtp Encrypt	☑ enable
SrTCP Encrypt	☑ enable
Mki	□ enable
Egress Offer Format	same-as-ingress
Use Ingress Session Params	

8.18. 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 which will have the sdes profile created above.
Assign this media policy to Zoom side as it uses TLS/SRTP.

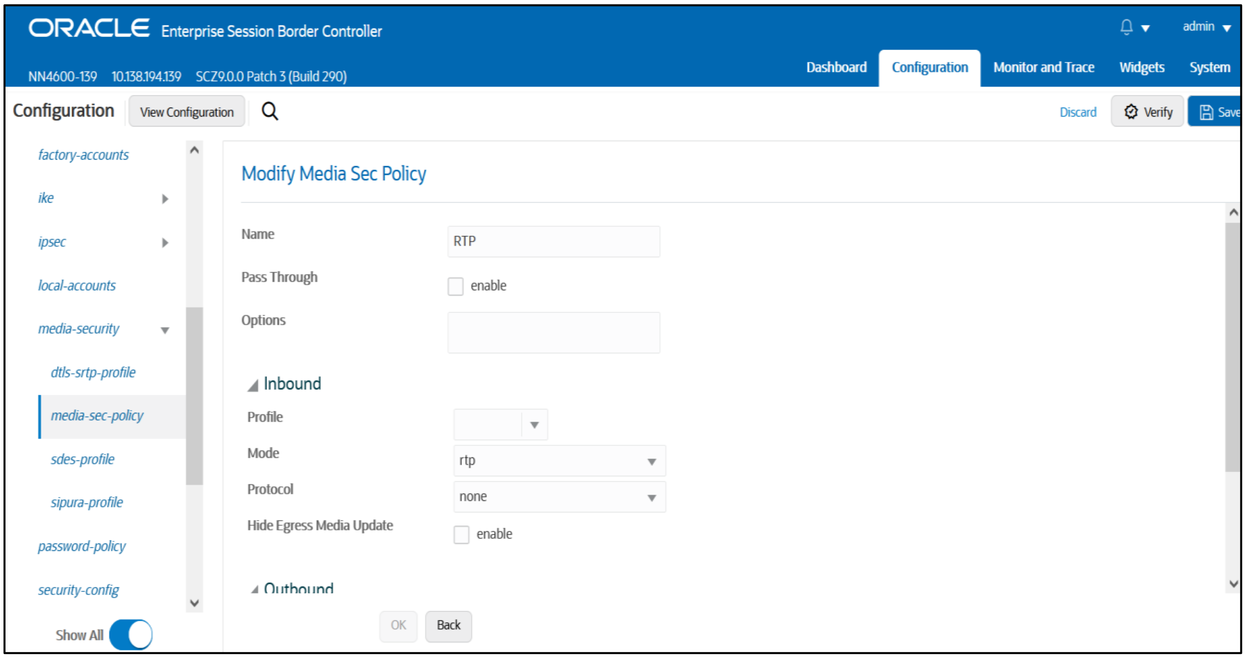


Modify Media Sec Policy

Name: sdesPolicy
Pass Through: □ enable
Options:

Inbound
Profile: SDES
Mode: srtp
Protocol: sdes
Hide Egress Media Update: □ enable

Similarly, Create Media Sec policy with name RTP to convert srtp to rtp for the CUCM side.
Assign this media policy to the CUCM side as this will use only TCP/UDP



Modify Media Sec Policy

Name: RTP
Pass Through: □ enable
Options:

Inbound
Profile:
Mode: rtp
Protocol: none
Hide Egress Media Update: □ enable

With this, SBC configuration is complete

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 SBC Certificate
- New TLS Profile
- New sip-interface
- New session-agent
- New steering-pools
- New local-policy
- New Media Security Profile

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 Zoom (ZOOM 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	Zoom user disconnects an inbound connected call	Pass
4	Zoom User disconnects an outbound connected call	Pass
5	Cisco user places inbound call from Zoom user on hold and then resumes	Pass
6	Cisco user makes outbound call to Zoom user and put that call on hold and then resumes	Pass
7	Zoom user places inbound call from Cisco user on hold and then resumes	Pass
8	Zoom user makes outbound call to Cisco user and put that call on hold and then resumes	Pass
9	Cisco user places inbound call from Zoom user on hold for over 15/30 minutes and then resumes	Pass
10	Cisco user makes outbound call to Zoom user and places the call on hold for over 15/30 minutes and then resumes	Pass
11	Inbound Zoom call to Cisco blind transferred to second Cisco/ Zoom User	Pass
12	Outbound Zoom call from Cisco user blind transferred to second Cisco/ Zoom User	Pass
13	Inbound Zoom Call to Cisco consultatively transferred to Cisco/ Zoom User	Pass
14	Outbound Zoom call from Cisco user consultatively transferred to Cisco/ Zoom User	Pass
15	Cisco user makes outbound call to Zoom user and makes a conference call by adding another Cisco/ Zoom user.	Pass
16	Zoom user makes outbound call to Cisco user and Cisco user makes a conference call by adding another Cisco/ Zoom user.	Pass

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

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services