Oracle ESBC – Zoom Client as Softphone with CUCM

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	Zoom App note with CUCM Integration	25th November 2019
2.0	Zoom App Note with some minor changes	22th July 2020

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 along with zoom client and Cisco CUCM.

2. Document Overview

This Oracle technical application note outlines the recommended configurations for the Zoom softphones registering to Cisco CUCM 11.5 version as SIP basic third party endpoints using Oracle enterprise session border controllers. Once zoom phones are registered to CUCM, certain basic and supplementary call features are tested with Zoom Phones. The solution contained within this document has been tested using Oracle's Acme Packet OS 830p7 version. Our scope of this document is only limited to zoom softphones and its features and the other features of Zoom is out of scope of this document.

Zoom softphone is cloud based application and we can register those softphones to the CUCM using Oracle SBC as a proxy server so that we can use Zoom softphone from anywhere. Zoom clients can register to CUCM in 2 ways as given below:

1) By entering the CUCM IP as Registrar Server IP
2) By entering the FQDN of the CUCM provided the DNS config is there for the CUCM.

It is recommended to use Zoom Desktop Client than Web client as some of the important features will be only available in zoom Desktop client. Hence this document covers configuration and provisioning of Zoom softphone with Zoom Desktop Client only. Oracle ESBC - Zoom Client as a Soft Phone with Cisco CUCM is explained in detail in the later sections.

The zoom client can also register (without using Oracle SBC) to CUCM by directly providing the CUCM IP as registrar server, provided both zoom client and CUCM are in the same network.
The intent of this document is to register Zoom Clients as Soft Phone with CUCM using Oracle SBC, the direct registration of Zoom client to CUCM is out of Scope of this document though it has been tested from our side.

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 CUCM 11.5 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 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.

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

For additional information on CUCM 11.5, please visit

https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-version-11-5/index.html

3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Zoom softphone with CUCM 11.5 version using Oracle Enterprise SBC. There will be steps that require navigating the CUCM 11.5 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.

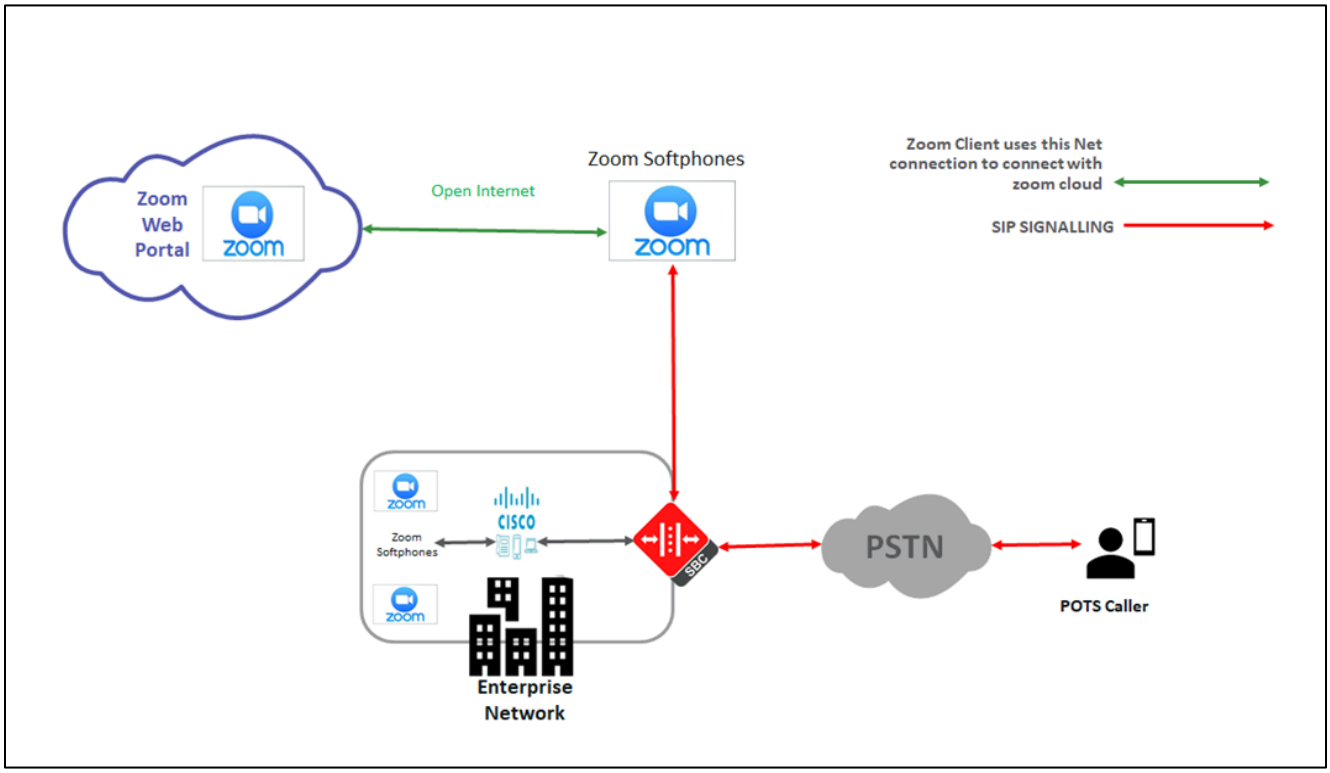
3.2. Requirements

- Fully functioning Cisco UCM 11.5
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.3.0 version
- Zoom Client configuration with softphone registered to Cisco CUCM using admin credentials

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

Software Used	CUCM Version	SBC Version	Zoom Client version
Revision 1	11.5	8.3.0	5.0.3

3.3. Architecture



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

- Phase 1 – Configuring the Cisco Unified Call Manager v11.5 for Zoom softphone
- Phase 2 – Configuring the Oracle SBC
- Phase 3 – Configuring the Zoom client softphones.

4. Configuring the Cisco CUCM 11.5 for Zoom Softphone

The enterprise should have a fully functioning CUCM v11.5 installed and deployed.

This section explains the Cisco CUCM config which is used for configuring the Zoom client softphone and CUCM registers those endpoints as 3rd party SIP basic endpoints. Though this topic is out of scope of Oracle SBC, this section has been added for the convenience of the users who will be using this app note.

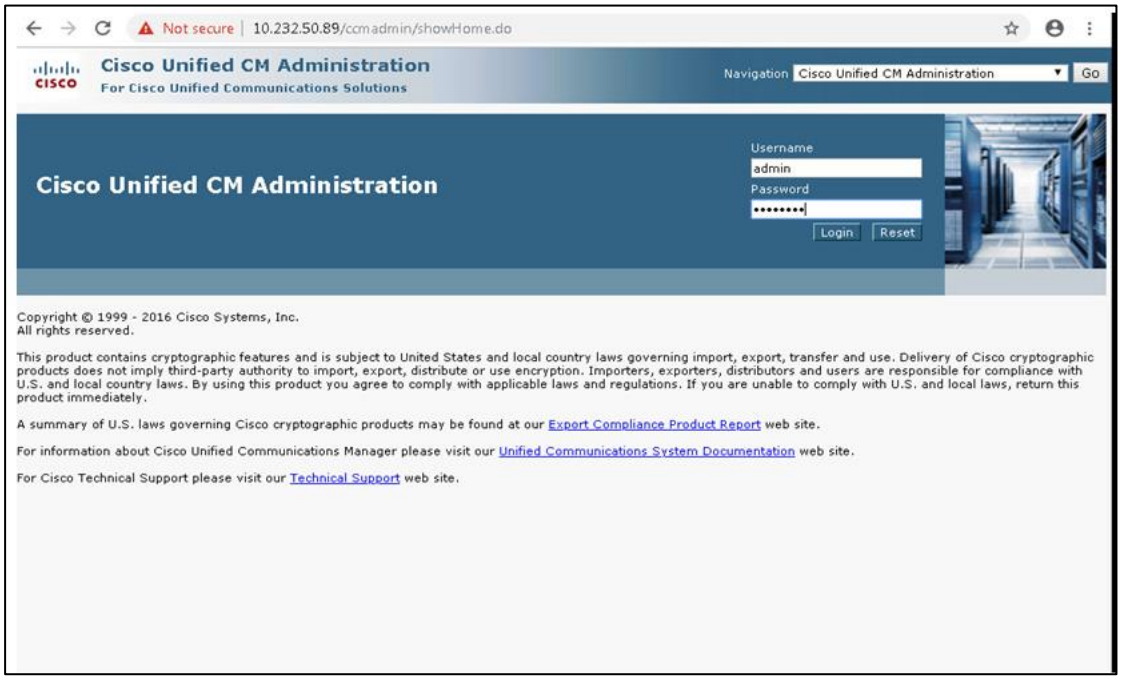
The same steps are given in zoom site and the link is given below for reference.

https://support.zoom.us/hc/en-us/articles/215537603-Zoom-Rooms-PBX-Support

Under this link, there is a pdf file which explains the Cisco CUCM integration with zoom.
The users can download the same and can follow the all the steps except the last step given there where it talks about configuration in zoom.

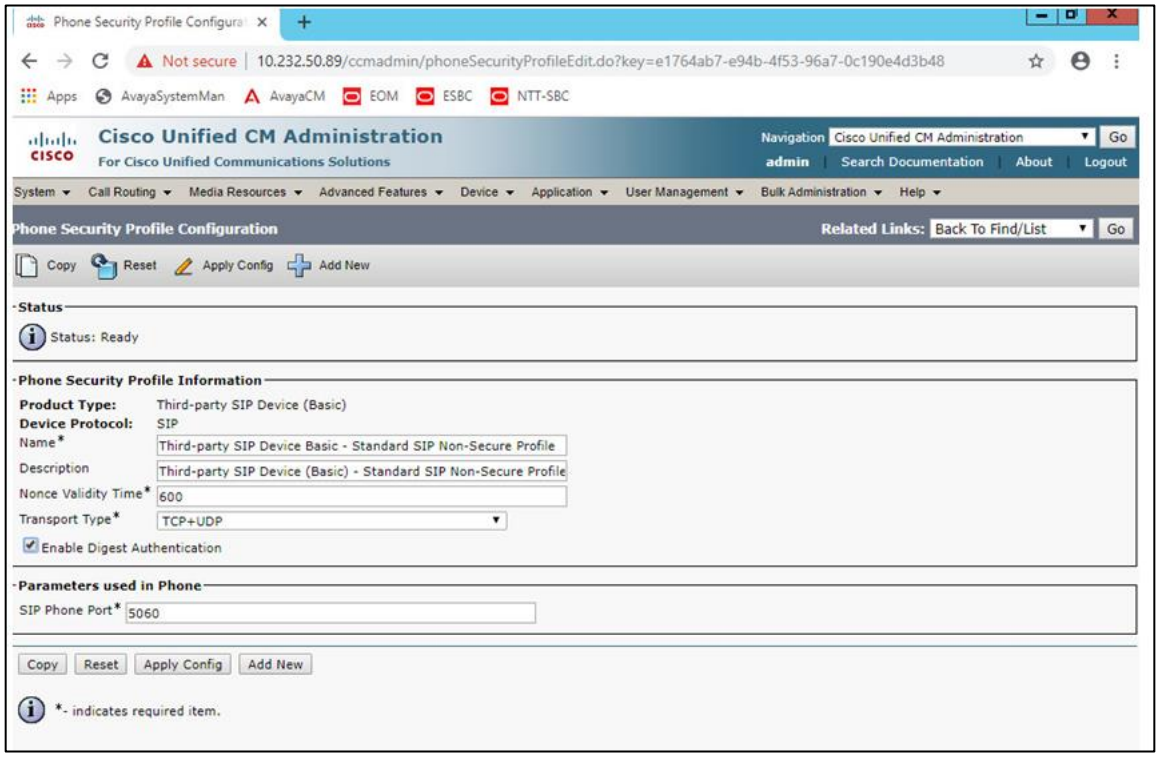
Else, they can use the below detailed steps to configure the same:

Please login to Cisco CUCM admin web GUI with proper login credentials and perform the steps below in the given order.



4.1. Configuring the Phone Security Profile for SIP Phone

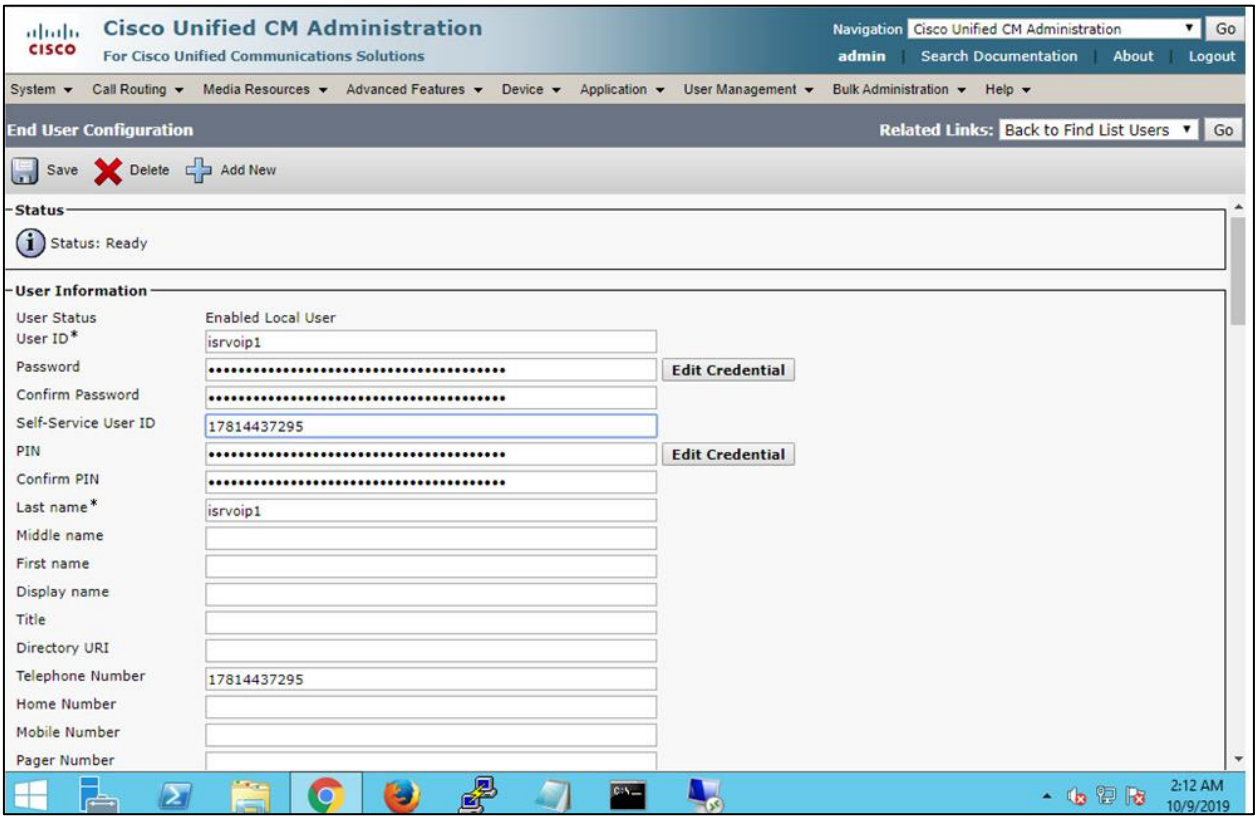
01) Go to System ----- Security Profile ----- Phone Security Profile
02) Simply hit Find and scroll down to the bottom of the list (you may need to click to a second page) and locate “Third-party SIP Device Basic – Standard SIP Non-Secure Profile” and click on it
03) Once you see its properties, simply hit COPY to create a new copy of it.
04) Give the new phone security profile a name; Example: “Third-party SIP Device Basic – Digest”
05) Check the checkbox next to Enable Digest Authentication and hit Save.

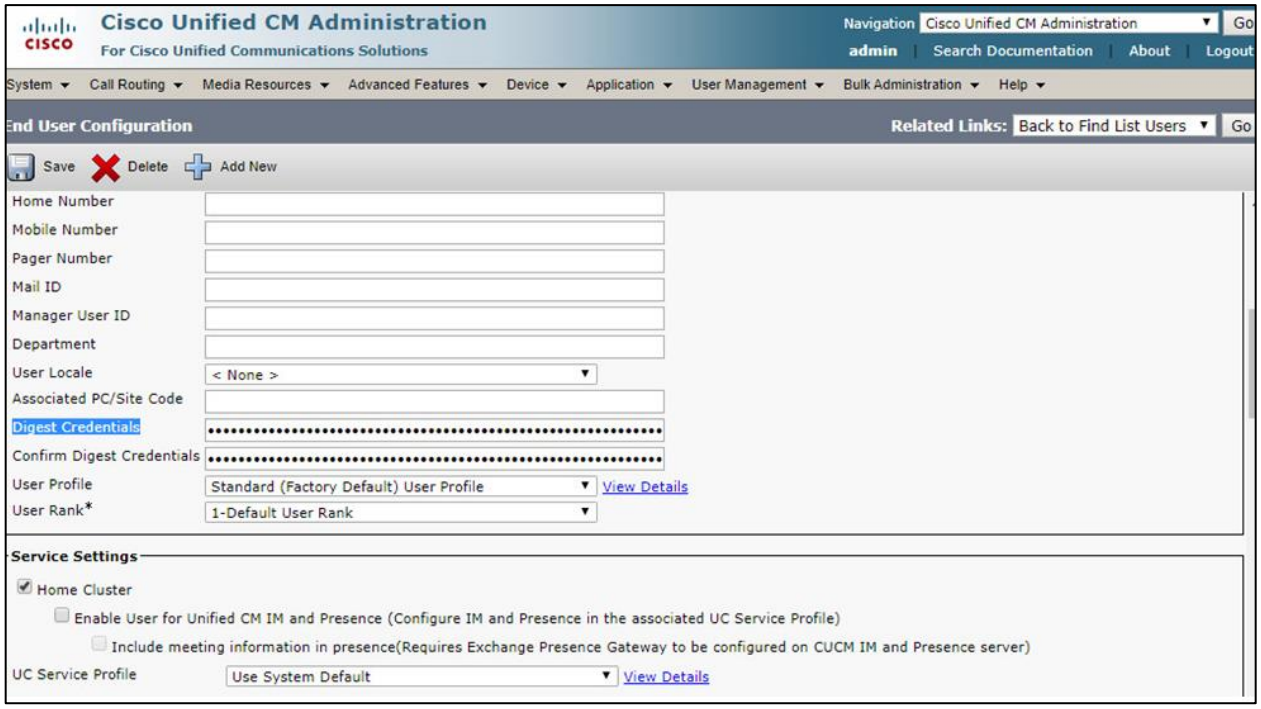


4.2. End User Configuration

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.
Digest Credentials field – this is the password that the SIP client will use to authenticate ***Update Note: If you are Active Directory Integrated, you still set the Digest Credentials in CUCM and use these credentials on the sip client***

04) Click Save (remember the User ID and Password and DN of the device)

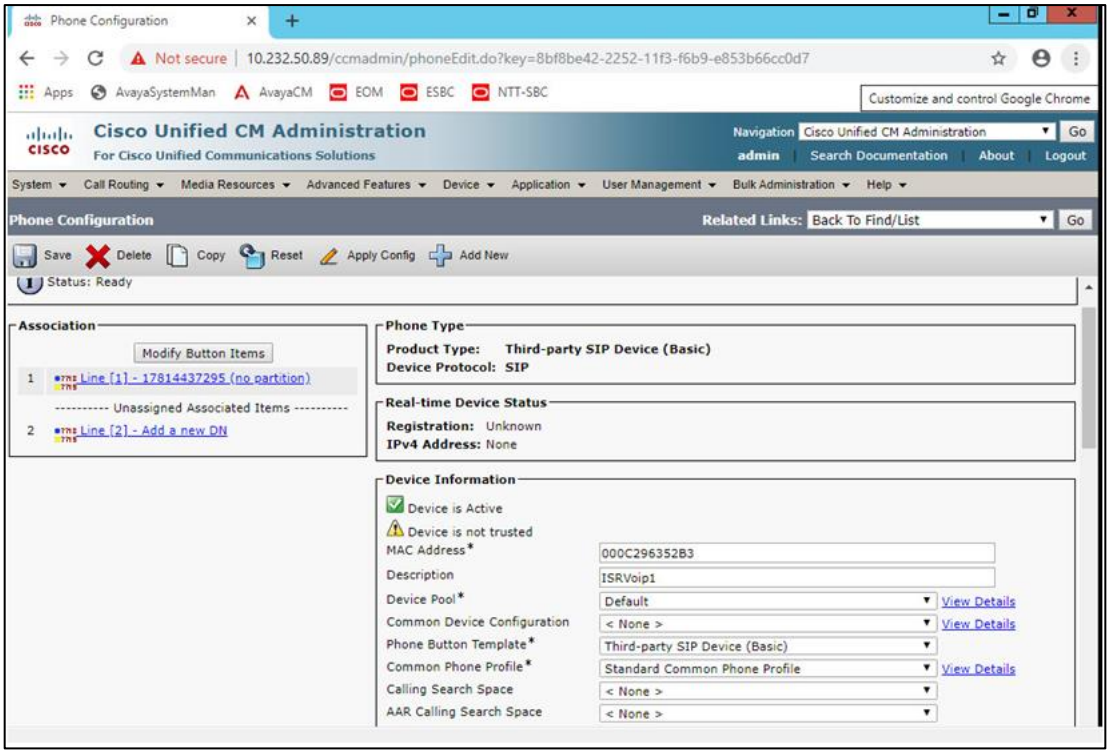


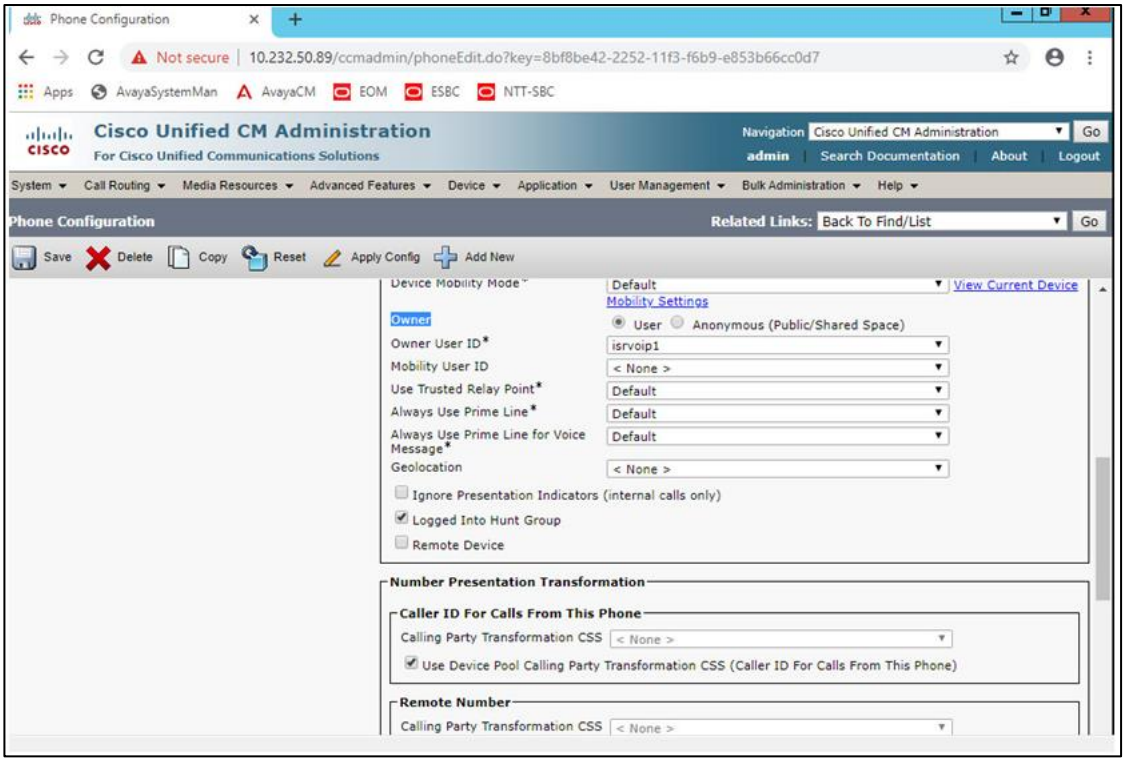

Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
End User Configuration
Related Links: Back to Find List Users Go
Save Delete Add New
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 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

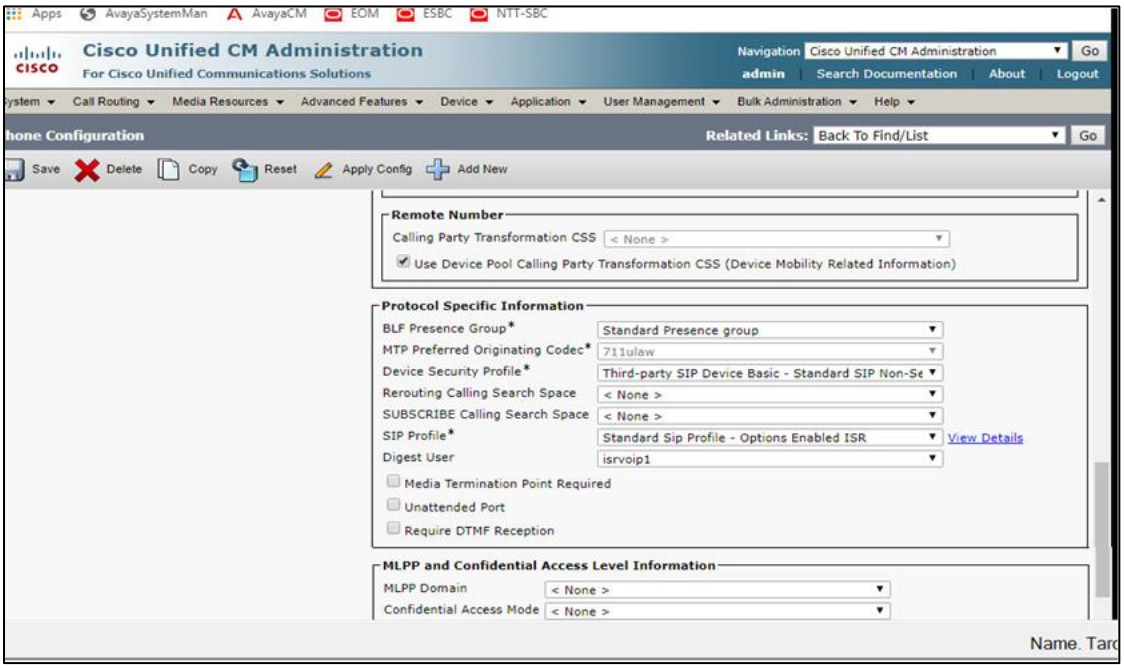
4.3. Adding SIP Phone in CUCM

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.



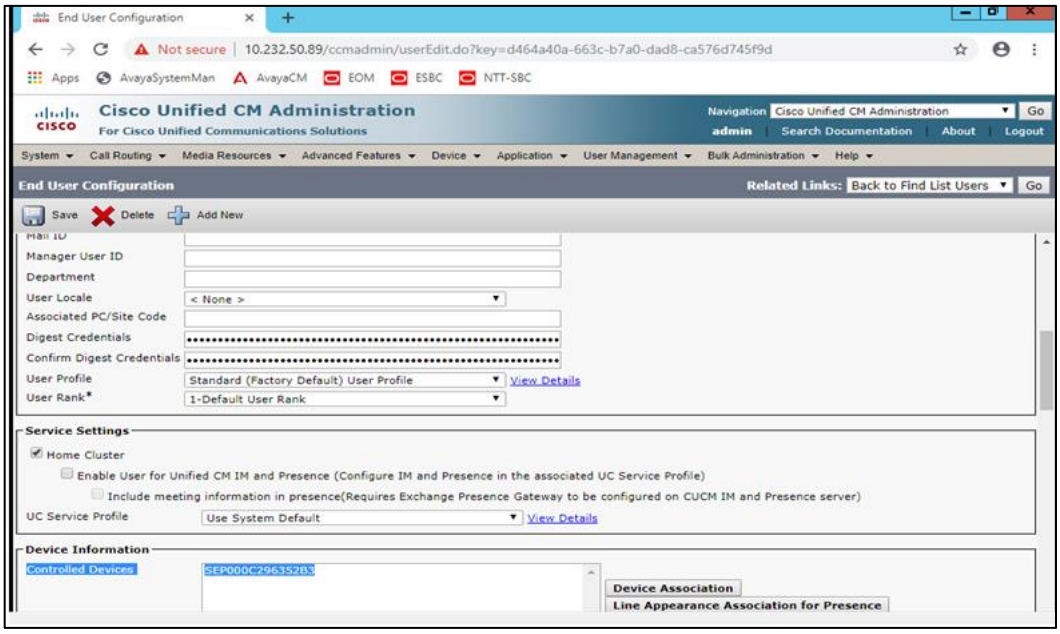

Phone Configuration
Not secure | 10.232.50.89/ccmadmin/phoneEdit.do?key=8bf8be42-2252-11f3-f6b9-e853b66cc0d7
Apps AvayaSystemMan AvayaCM EOM ESBC NTT-SBC
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Phone Configuration
Related Links: Back To Find/List Go
Save Delete Copy Reset Apply Config Add New
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
Number Presentation Transformation
Caller ID For Calls From This Phone
Calling Party Transformation CSS < None >
Use Device Pool Calling Party Transformation CSS (Caller ID For Calls From This Phone)
Remote Number
Calling Party Transformation CSS < None >


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
Phone 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 >

4.4. 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.



You have completed the steps to configure the SIP device in Cisco CUCM.

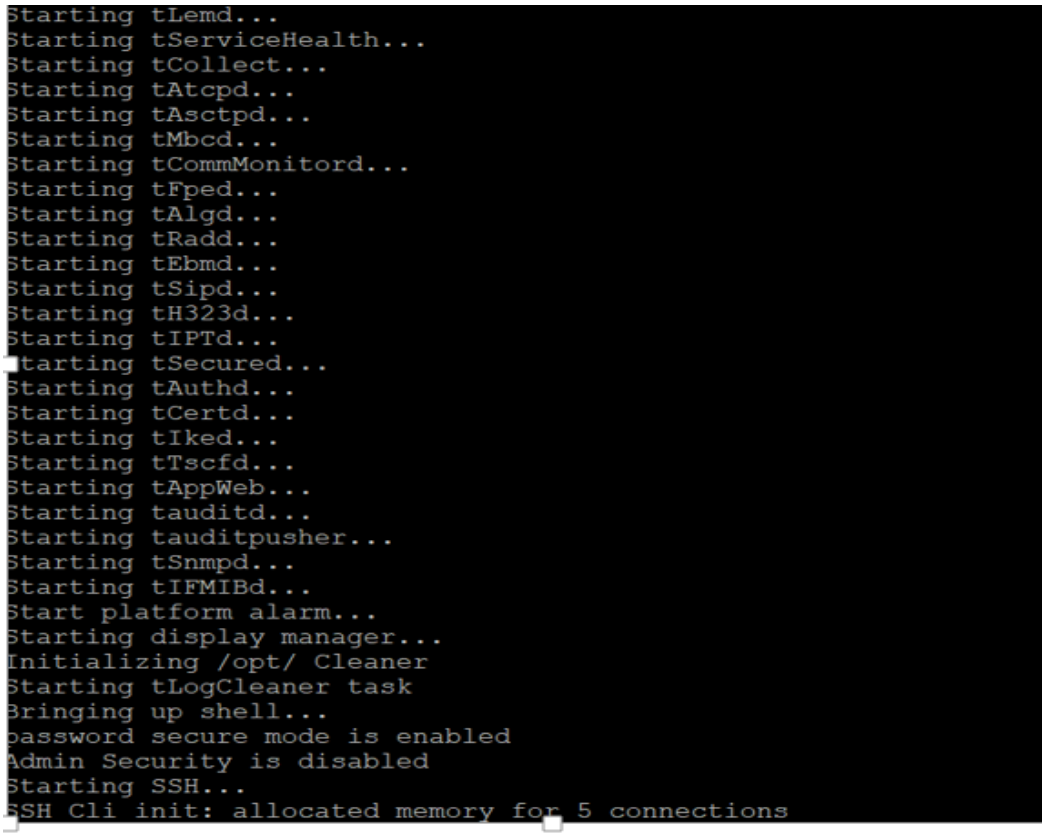
5. New SBC configuration

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

5.1. Establishing a serial connection to the SBC

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

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



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

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

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

```
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.

Note: There is no management IP configured by default.

```
PE-6300-1(configure)# bootparam

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

Boot File               : /boot/nnSCZ830p7.bz
IP Address              : 172.18.255.115
VLAN                    :
Netmask                 : 255.255.0.0
Gateway                 : 172.18.0.1
IPv6 Address            :
IPv6 Gateway            :
Host IP                 :
FTP username            : vxftp
FTP password            : vxftp
Flags                   :
Target Name             : PE-6300-1
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.

PE-6300-1(configure)#
```

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

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

```
PE-6300-1# setup product

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

Last Modified 2019-09-11 13:57:32
-----------------------------------------------------------------
 1 : Product        : Enterprise Session Border Controller
```

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
-----------------------------------------------------------------
  Transcode Codec SILK Capacity (0-102375)        : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
SAVE SUCCEEDED
PE-6300-1#
PE-6300-1#
PE-6300-1#
PE-6300-1# reboot

En-------------------------------------------------------------
  WARNING: you are about to reboot this ESBC!
  -------------------------------------------------------------
En

*************************************************************
CAUTION: Enabling this feature activates enhanced security
functions. Once saved, security cannot be reverted without
resetting the system back to factory default state.
*************************************************************
  Admin Security (enabled/disabled)             :

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 5

  Transcode Codec AMR Capacity (0-102375)       : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2

    Advanced (enabled/disabled)                 : enabled

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10

  Transcode Codec OPUS Capacity (0-102375)      : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 11

  Transcode Codec SILK Capacity (0-102375)      : 50
```

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

Go to configure terminal->system->web-server-config.

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

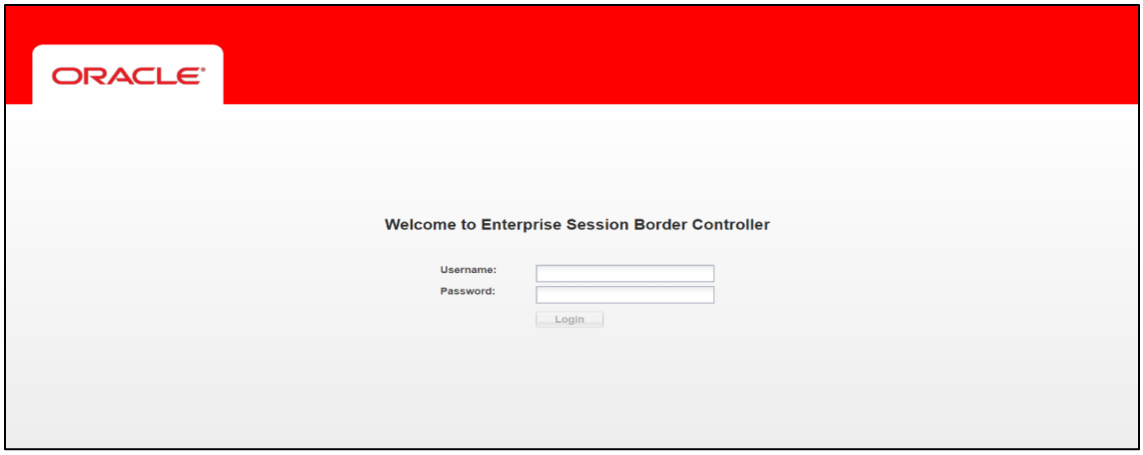
```
PE-6300-1(web-server-config)#
PE-6300-1(web-server-config)# state enabled
PE-6300-1(web-server-config)# done
web-server-config
        state                                   enabled
        inactivity-timeout                      5
        http-state                              enabled
        http-port                               80
        https-state                             disabled
        https-port                              443
        tls-profile
        last-modified-by                        admin@172.18.0.176
        last-modified-date                      2019-09-12 05:31:51

PE-6300-1(web-server-config)# exit
PE-6300-1(system)# exit
PE-6300-1(configure)# exit
PE-6300-1# save-config
checking configuration
-------------------------------------------------------------------------------
Results of config verification:
   1 configuration error
Run 'verify-config' for more details
-------------------------------------------------------------------------------
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
PE-6300-1# activate-config
Activate-Config received, processing.
waiting for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
```

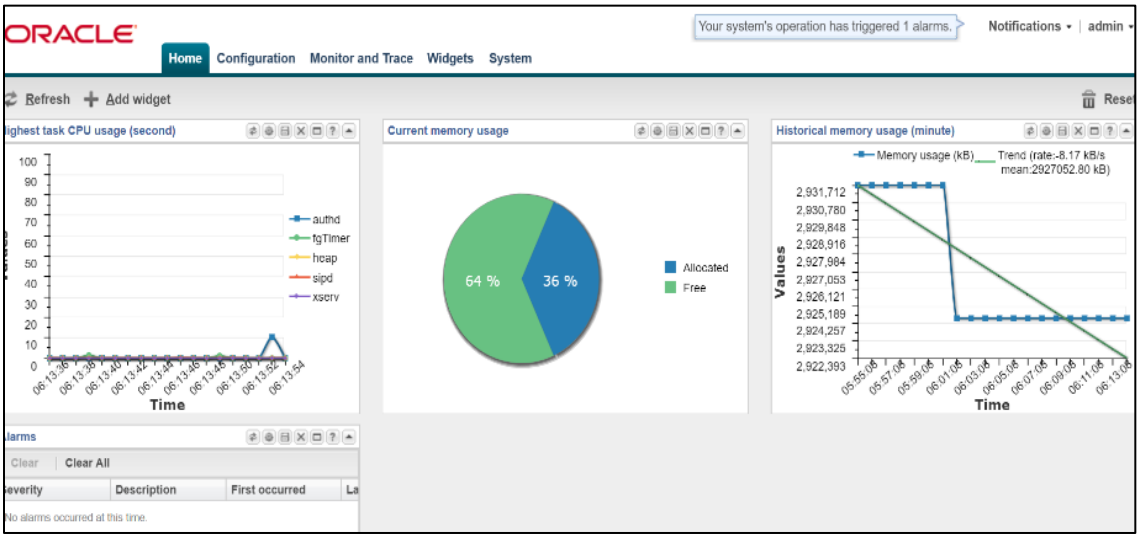
5.2. Configure SBC using Web GUI

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

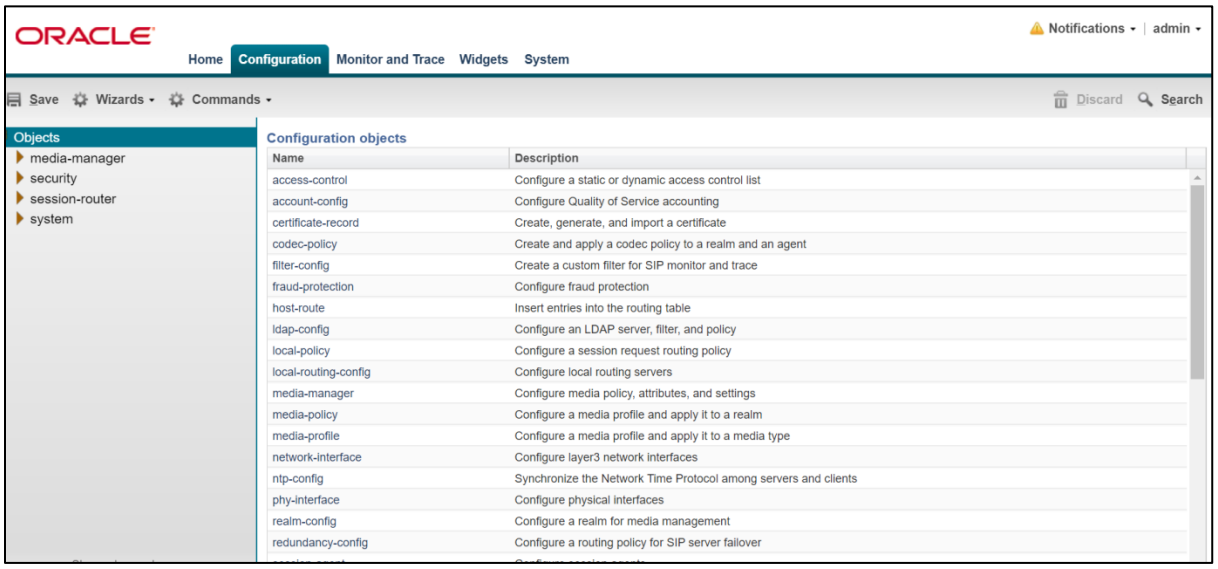
The Web GUI can be accessed through the url https://<SBC_MGMT_IP>.



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

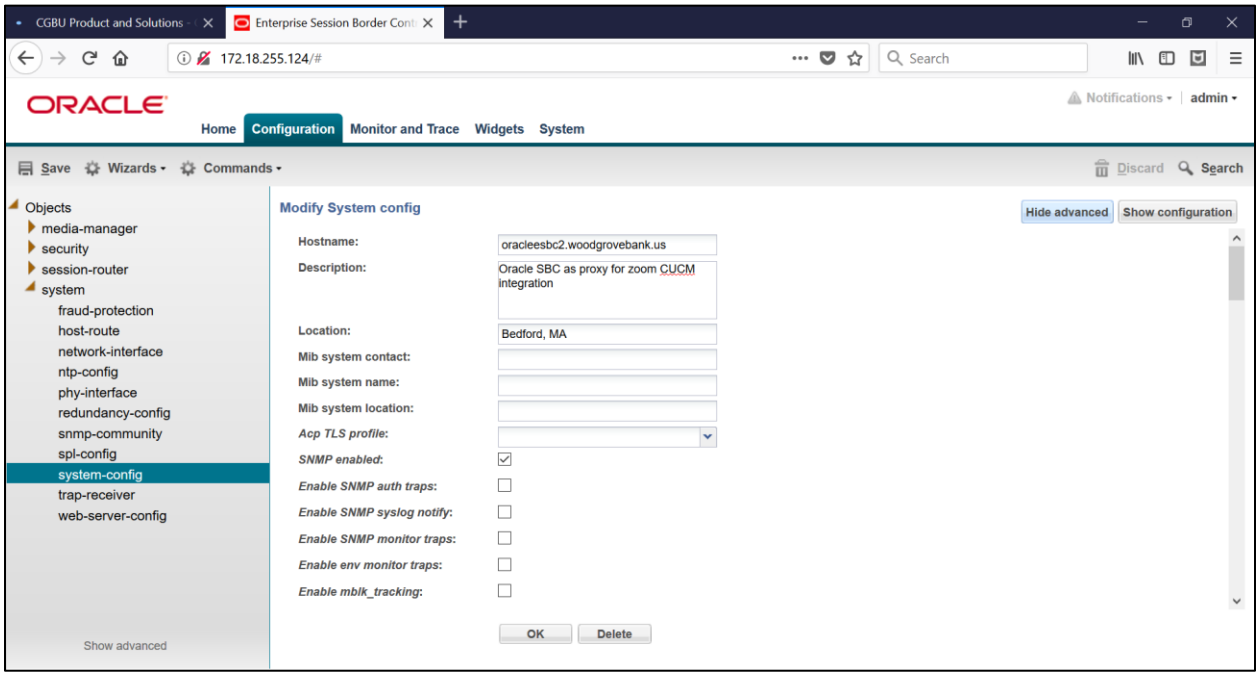
https://docs.oracle.com/cd/F13782_01/doc/esbc_scz830_webgui.pdf for more information

The expert mode is used for configuration.

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

5.3. Configure system-config

Go to system->system-config



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

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

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

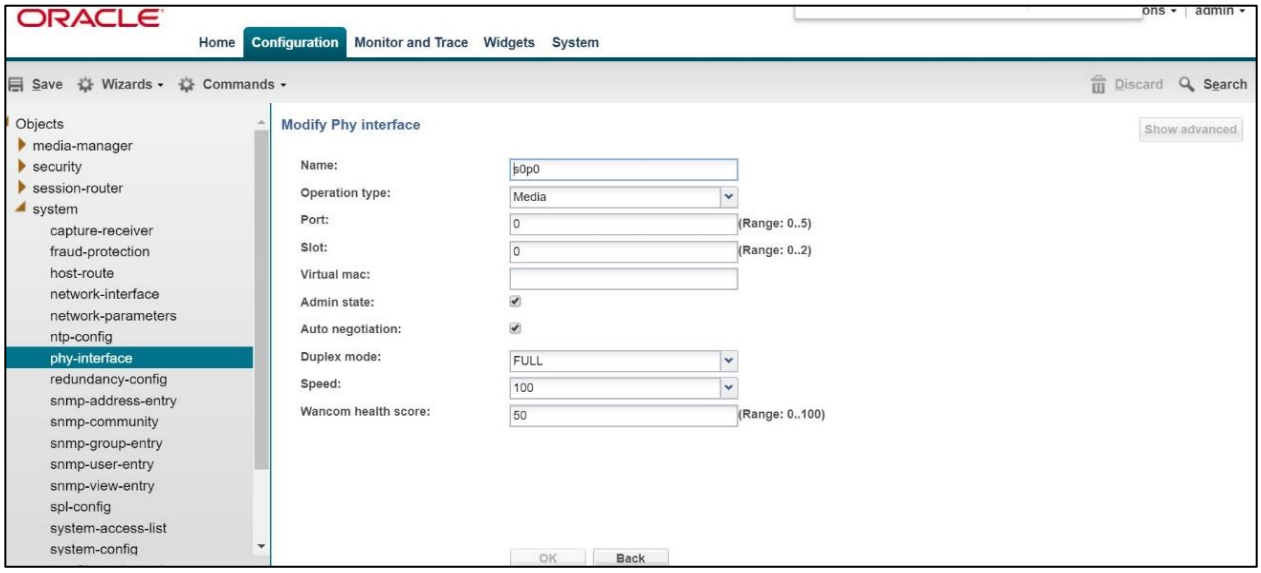
5.4. Configure Physical Interface values

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

You will first configure the slot 0, port 0 interface designated with the name s0p0. This will be the port plugged into your inside (Zoom softphone to SBC inside) interface.

CUCM is configured on the slot1port 1 interface designated with the name s1p1. Below is the screenshot for creating a phy-interface on s0p0

Parameter Name	To Zoom Side(s0p0)	To CUCM side(s1p1)
Slot	0	1
Port	0	1
Operation Mode	Media	Media

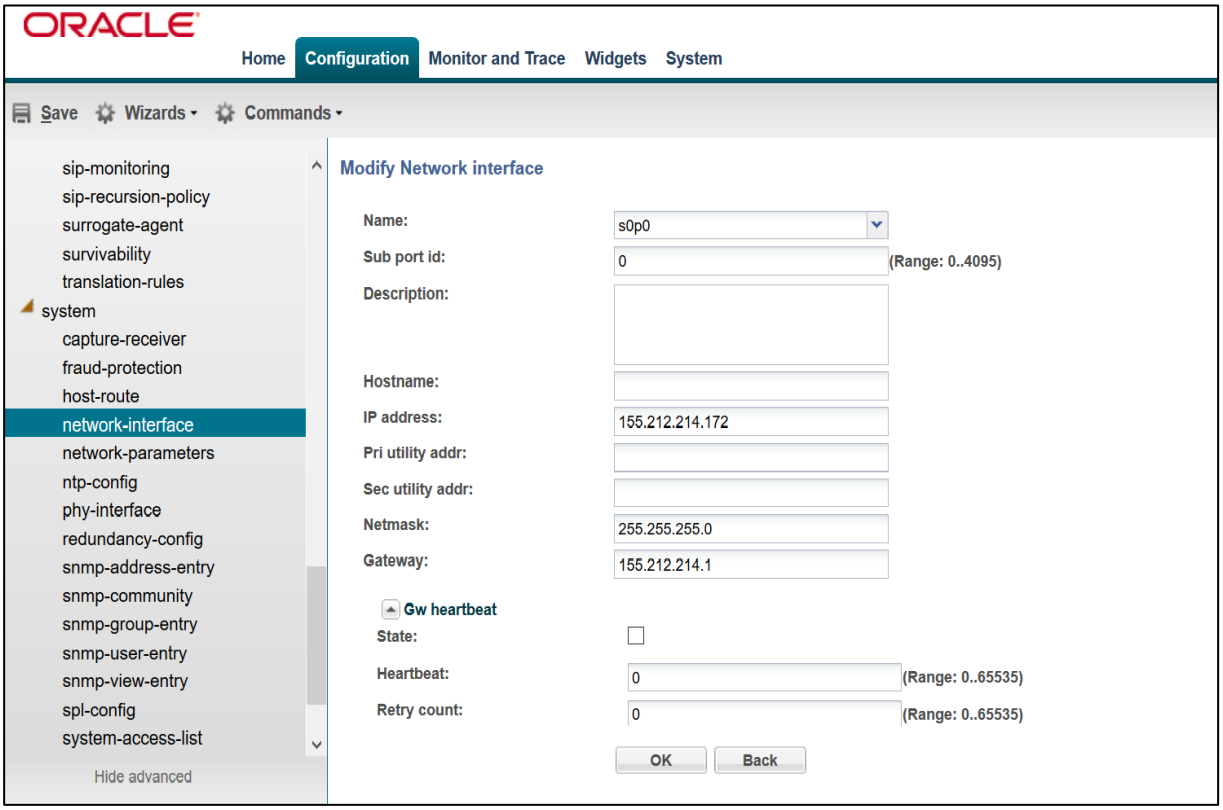


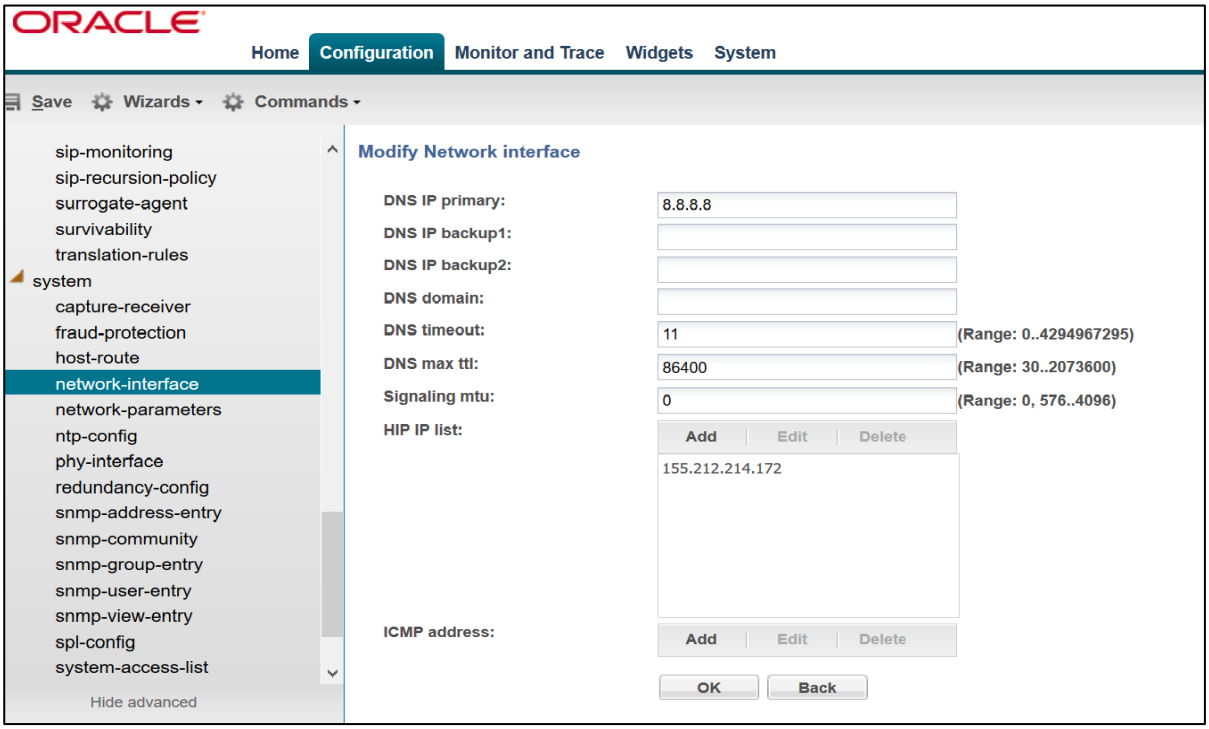
5.5. Configure Network Interface values

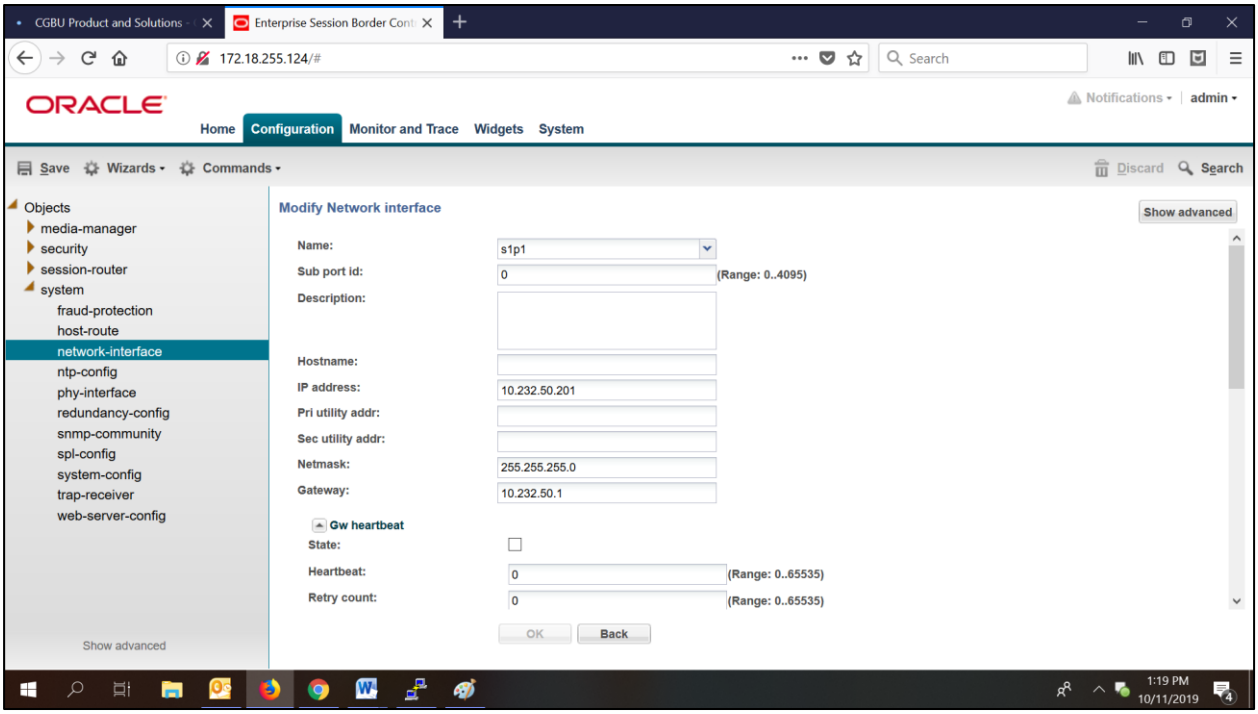
To configure network-interface, go to system->Network-Interface. Configure two interfaces, one for zoom side and one for CUCM side.

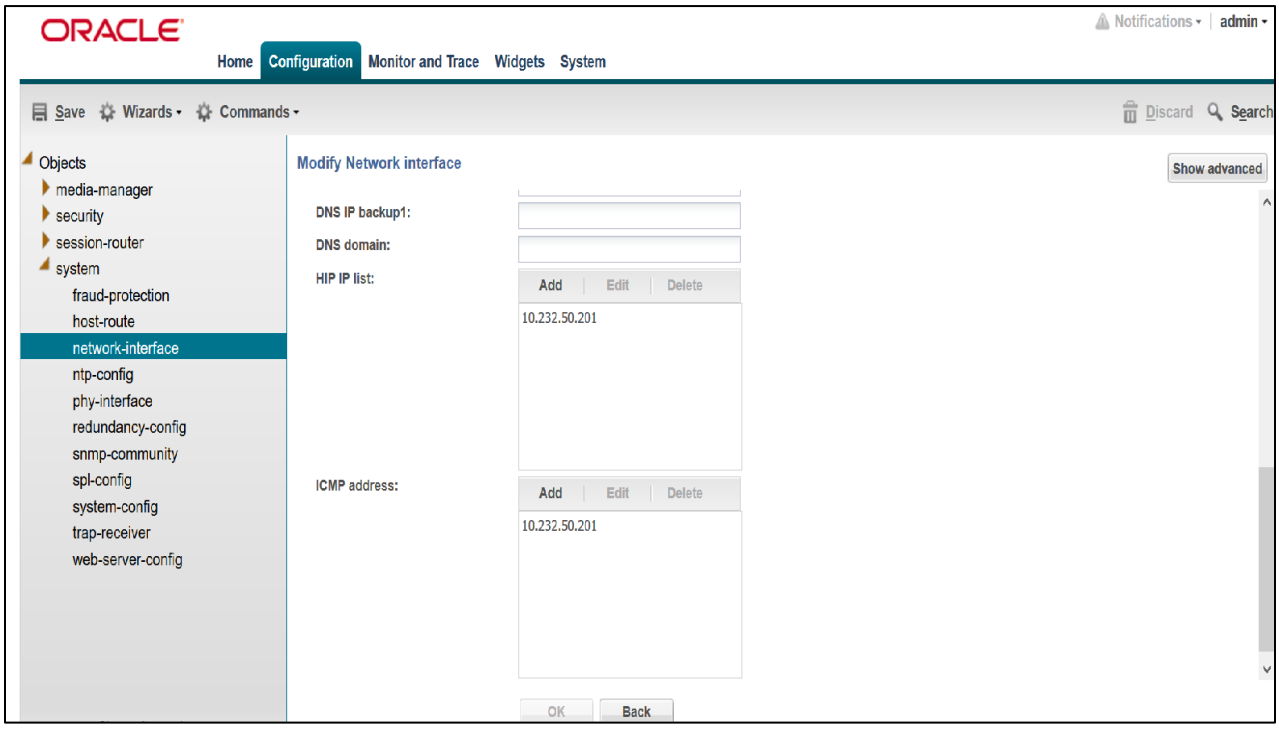
The table below lists the parameters, to be configured for both the interfaces.

Parameter Name	Zoom side Network Interface	CUCM side Network interface
Name	s0p0	s1p1
Host Name		
IP address	155.212.214.172	10.232.50.201
Netmask	255.255.255.0	255.255.255.0
Gateway	155.212.214.1	10.232.50.1
DNS-IP Primary		
DNS-domain		


ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
sip-monitoring
sip-recursion-policy
surrogate-agent
survivability
translation-rules
system
capture-receiver
fraud-protection
host-route
network-interface
network-parameters
ntp-config
phy-interface
redundancy-config
snmp-address-entry
snmp-community
snmp-group-entry
snmp-user-entry
snmp-view-entry
spl-config
system-access-list
Hide advanced
Modify Network interface
Name:
s0p0
Sub port id:
0
(Range: 0..4095)
Description:
Hostname:
IP address:
155.212.214.172
Pri utility addr:
Sec utility addr:
Netmask:
255.255.255.0
Gateway:
155.212.214.1
Gw heartbeat
State:
Heartbeat:
0
(Range: 0..65535)
Retry count:
0
(Range: 0..65535)
OK
Back


ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
sip-monitoring
sip-recursion-policy
surrogate-agent
survivability
translation-rules
system
capture-receiver
fraud-protection
host-route
network-interface
network-parameters
ntp-config
phy-interface
redundancy-config
snmp-address-entry
snmp-community
snmp-group-entry
snmp-user-entry
snmp-view-entry
spl-config
system-access-list
Hide advanced
Modify Network interface
DNS IP primary:
8.8.8.8
DNS IP backup1:
DNS IP backup2:
DNS domain:
DNS timeout:
11
(Range: 0..4294967295)
DNS max ttl:
86400
(Range: 30..2073600)
Signaling mtu:
0
(Range: 0, 576..4096)
HIP IP list:
Add
Edit
Delete
155.212.214.172
ICMP address:
Add
Edit
Delete
OK
Back


CGBU Product and Solutions
Enterprise Session Border Cont
172.18.255.124/#
Search
ORACLE
Notifications
admin
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Discard
Search
Objects
media-manager
security
session-router
system
fraud-protection
host-route
network-interface
ntp-config
phy-interface
redundancy-config
snmp-community
spl-config
system-config
trap-receiver
web-server-config
Show advanced
Modify Network interface
Show advanced
Name:
s1p1
Sub port id:
0
(Range: 0..4095)
Description:
Hostname:
IP address:
10.232.50.201
Pri utility addr:
Sec utility addr:
Netmask:
255.255.255.0
Gateway:
10.232.50.1
Gw heartbeat
State:
Heartbeat:
0
(Range: 0..65535)
Retry count:
0
(Range: 0..65535)
OK
Back
1:19 PM
10/11/2019

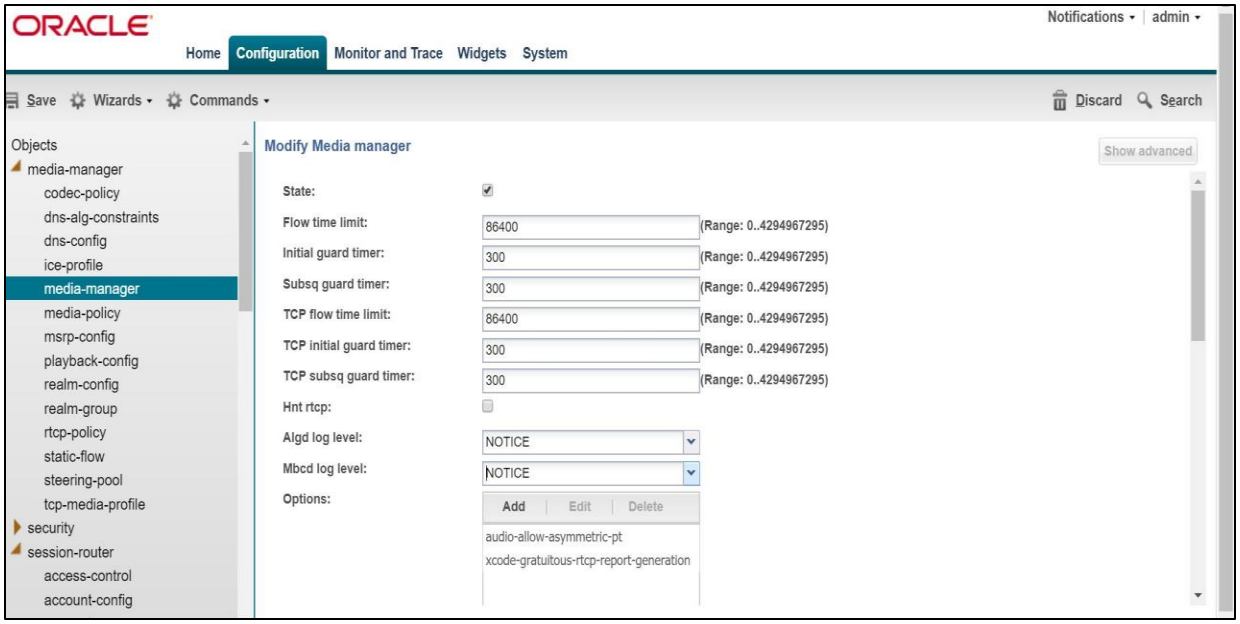

ORACLE
Notifications
admin
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Discard
Search
Objects
media-manager
security
session-router
system
fraud-protection
host-route
network-interface
ntp-config
phy-interface
redundancy-config
snmp-community
spl-config
system-config
trap-receiver
web-server-config
Modify Network interface
Show advanced
DNS IP backup1:
DNS domain:
HIP IP list:
Add
Edit
Delete
10.232.50.201
ICMP address:
Add
Edit
Delete
10.232.50.201
OK
Back

5.6. Enable media manager

Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager and configure the below option for generating rtcp reports.

audio-allow-assymetric-pt
xcode-gratutious-rtcp-report-generation

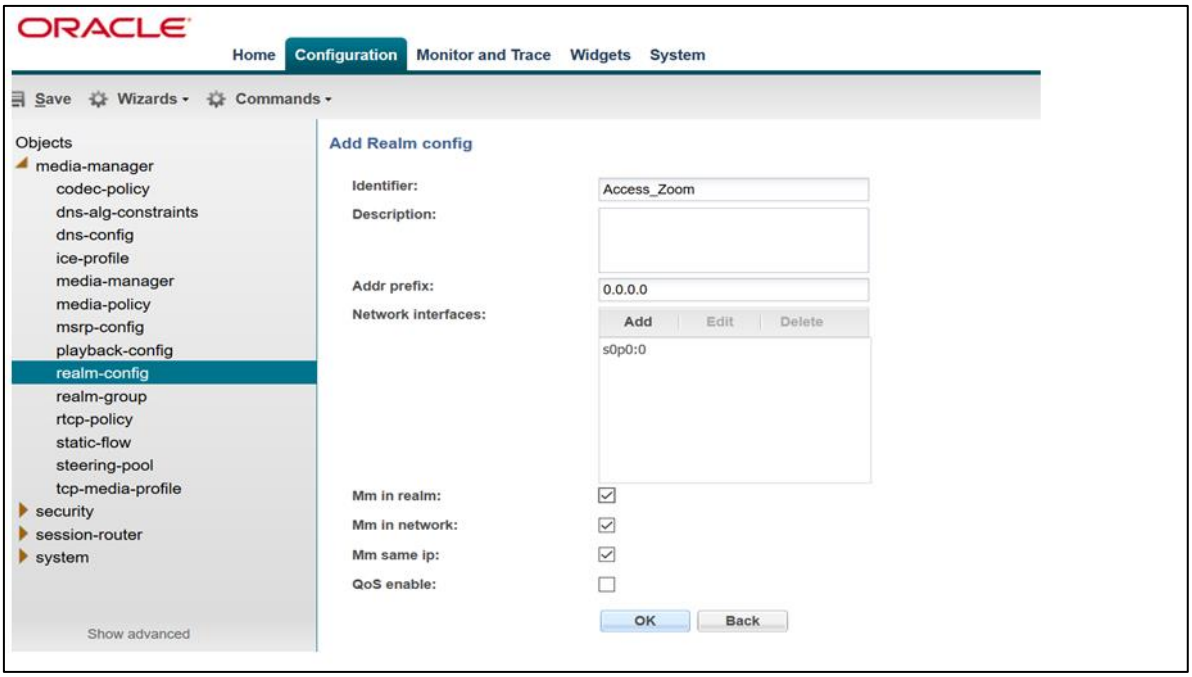
Go to Media-Manager->Media-Manager



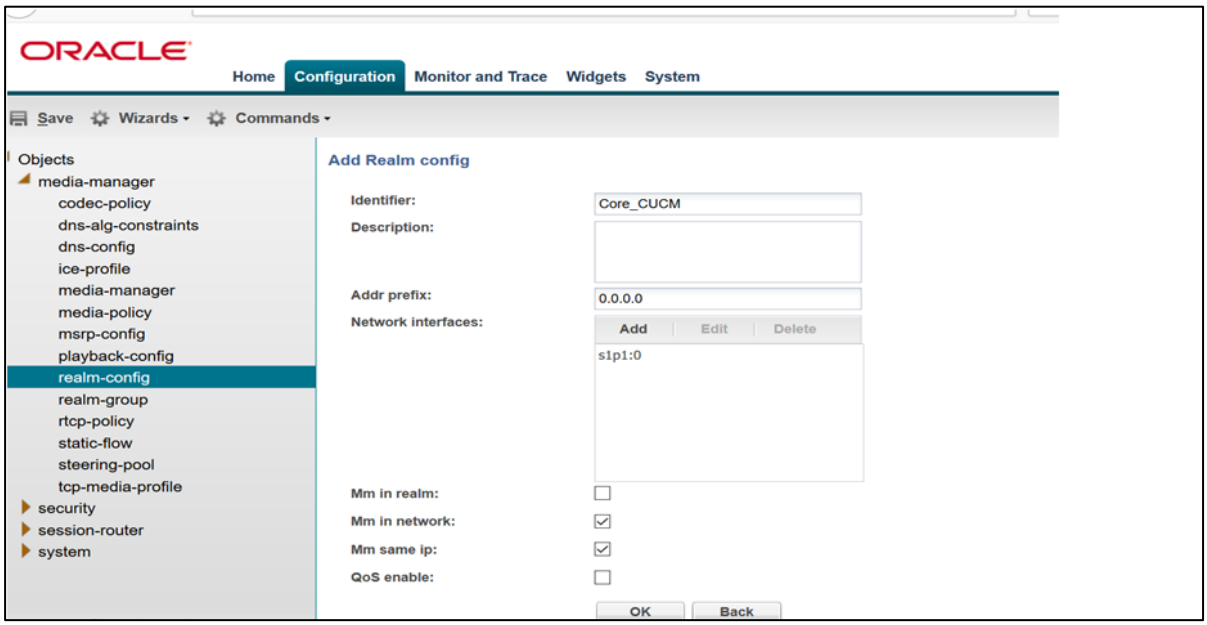
5.7. Configure Realms

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

In the below case, Realm name is given as Access_Zoom (Zoom to SBC)



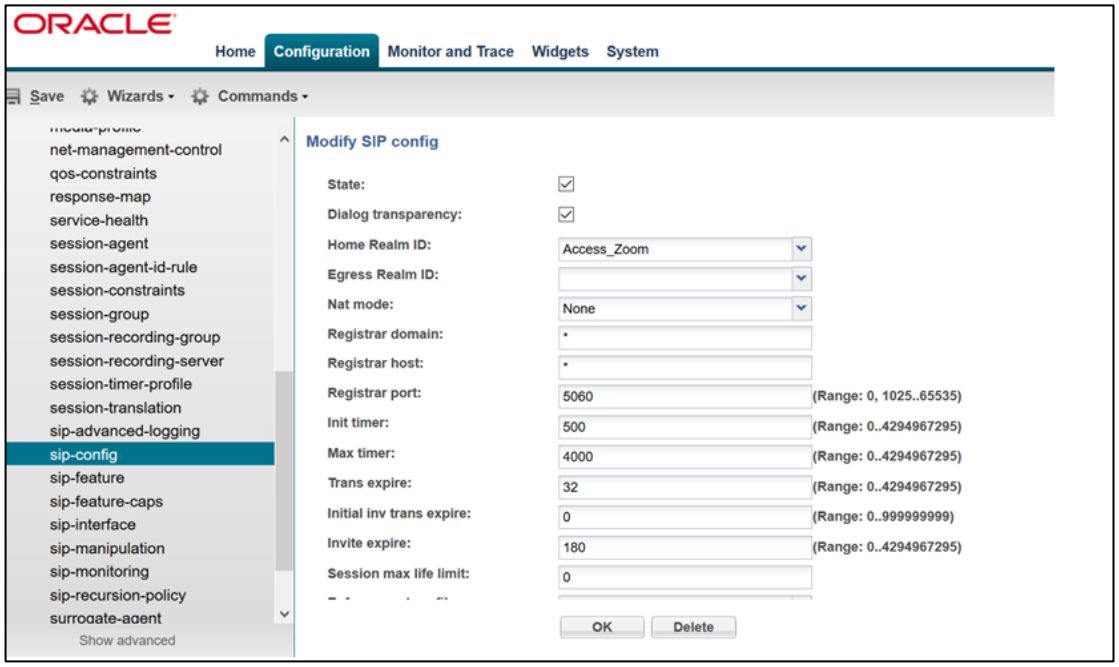
Similarly, Realm name is given as Core_CUCM (SBC to CUCM)

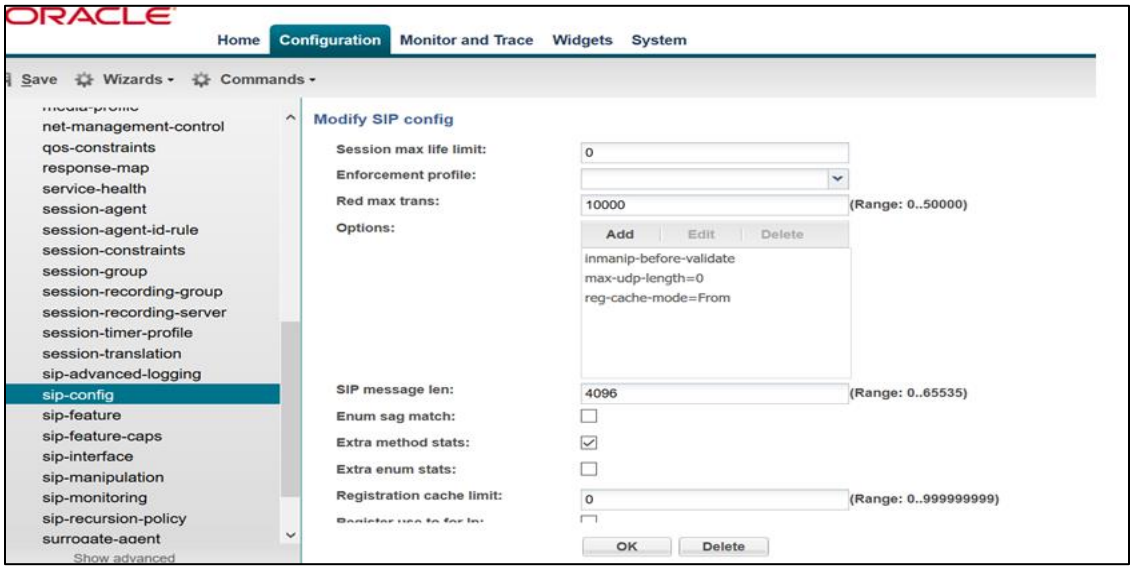


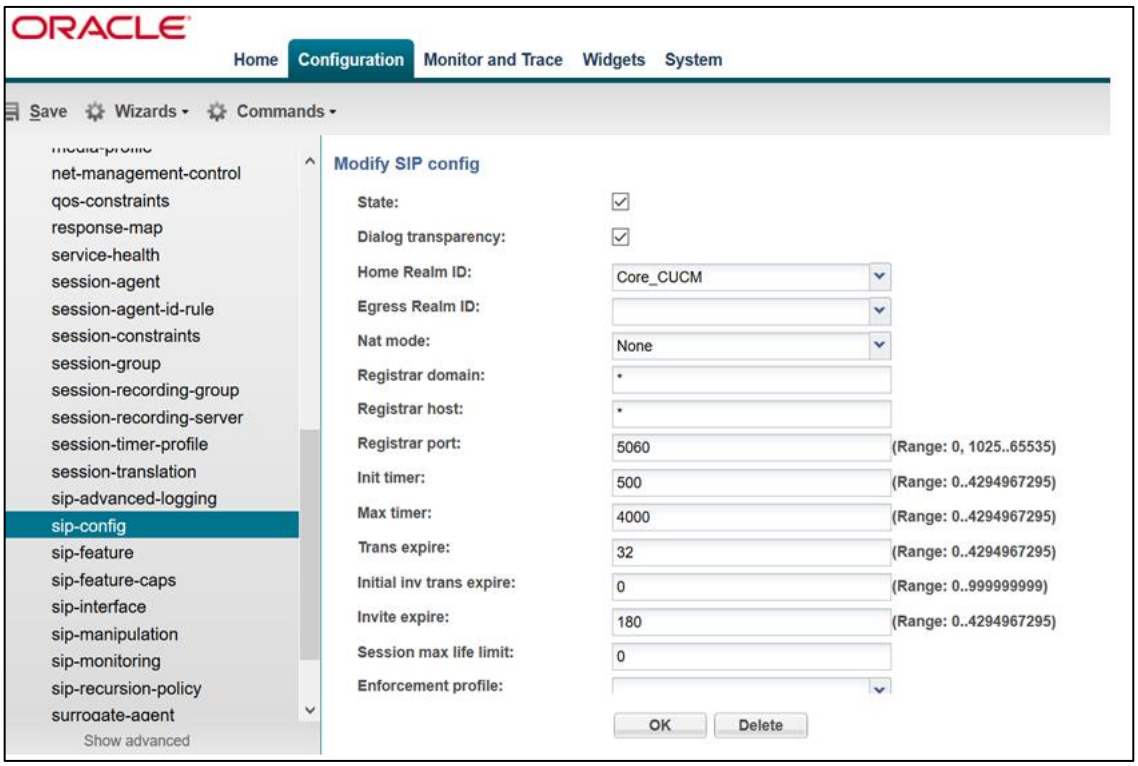
5.8. Enable sip-config

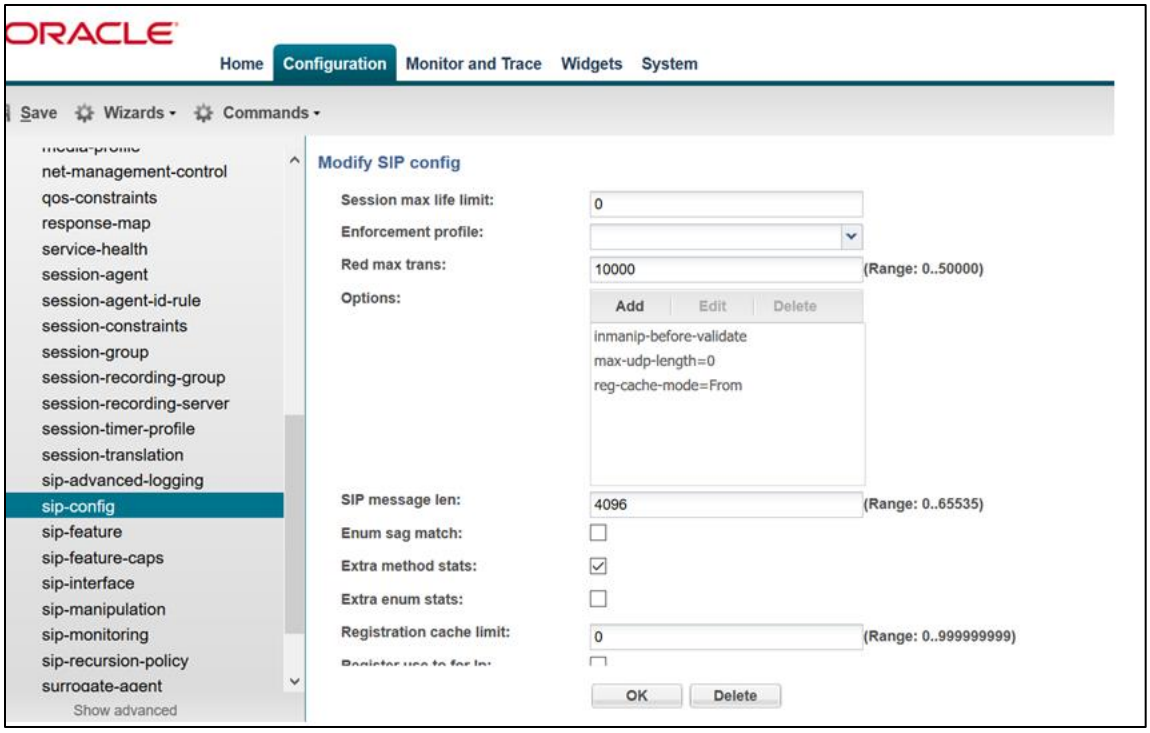
SIP config enables SIP handling in the SBC.
Make sure the home realm-id , registrar-domain and registrar-host are configured.
Also add the options to the sip-config as shown below.
To configure sip-config, Go to Session-Router->sip-config.

In options add max-udp-length =0.
inmanip-before-validate
reg-cache-mode=From (This parameter is needed to avoid issues with the cookie, if there is an issue with CUCM, not sending the cookie in Invites back to the SBC)





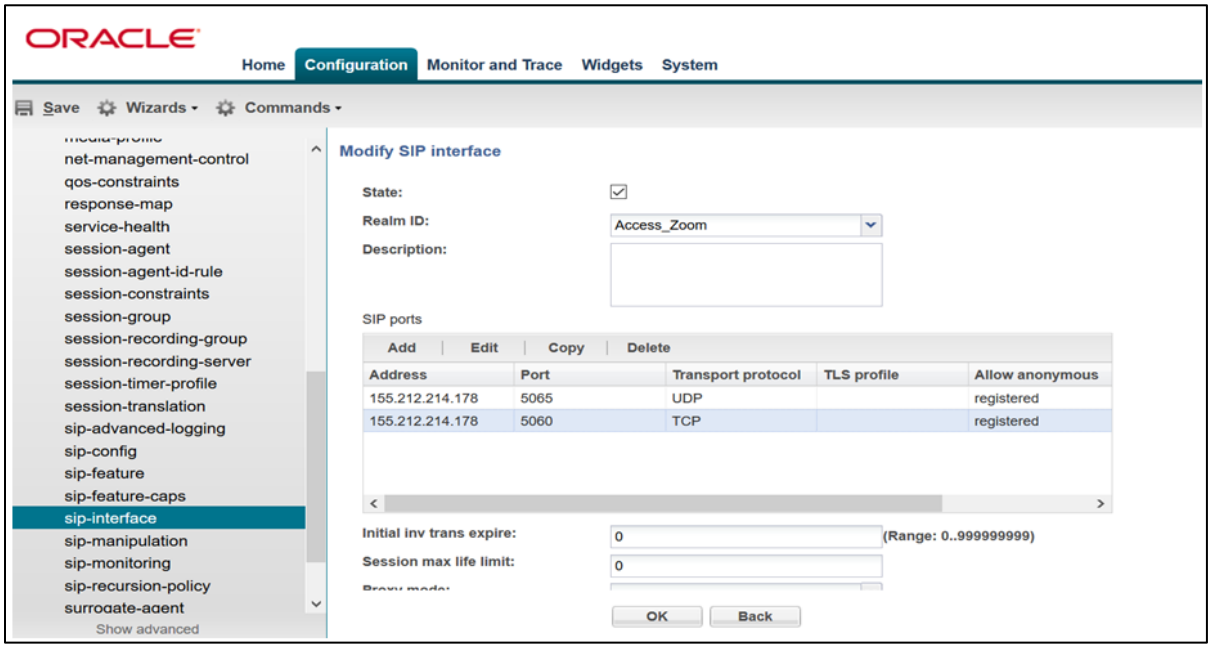

ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
net-management-control
qos-constraints
response-map
service-health
session-agent
session-agent-id-rule
session-constraints
session-group
session-recording-group
session-recording-server
session-timer-profile
session-translation
sip-advanced-logging
sip-config
sip-feature
sip-feature-caps
sip-interface
sip-manipulation
sip-monitoring
sip-recursion-policy
surrogate-agent
Show advanced
Modify SIP config
State:
Dialog transparency:
Home Realm ID:
Core_CUCM
Egress Realm ID:
Nat mode:
None
Registrar domain:
*
Registrar host:
*
Registrar port:
5060
(Range: 0, 1025..65535)
Init timer:
500
(Range: 0..4294967295)
Max timer:
4000
(Range: 0..4294967295)
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:
OK
Delete

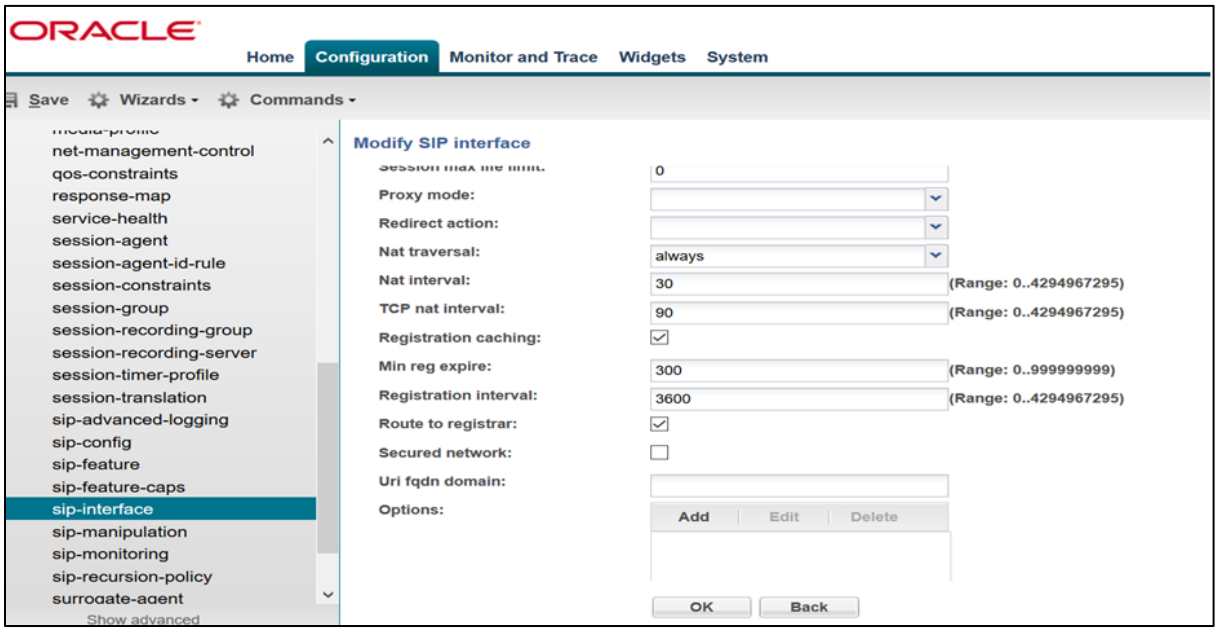

ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
net-management-control
qos-constraints
response-map
service-health
session-agent
session-agent-id-rule
session-constraints
session-group
session-recording-group
session-recording-server
session-timer-profile
session-translation
sip-advanced-logging
sip-config
sip-feature
sip-feature-caps
sip-interface
sip-manipulation
sip-monitoring
sip-recursion-policy
surrogate-agent
Show advanced
Modify SIP config
Session max life limit:
0
Enforcement profile:
Red max trans:
10000
(Range: 0..50000)
Options:
Add
Edit
Delete
inmanip-before-validate
max-udp-length=0
reg-cache-mode=From
SIP message len:
4096
(Range: 0..65535)
Enum sag match:
Extra method stats:
Extra enum stats:
Registration cache limit:
0
(Range: 0..999999999)
OK
Delete

5.9. Configure SIP Interfaces.

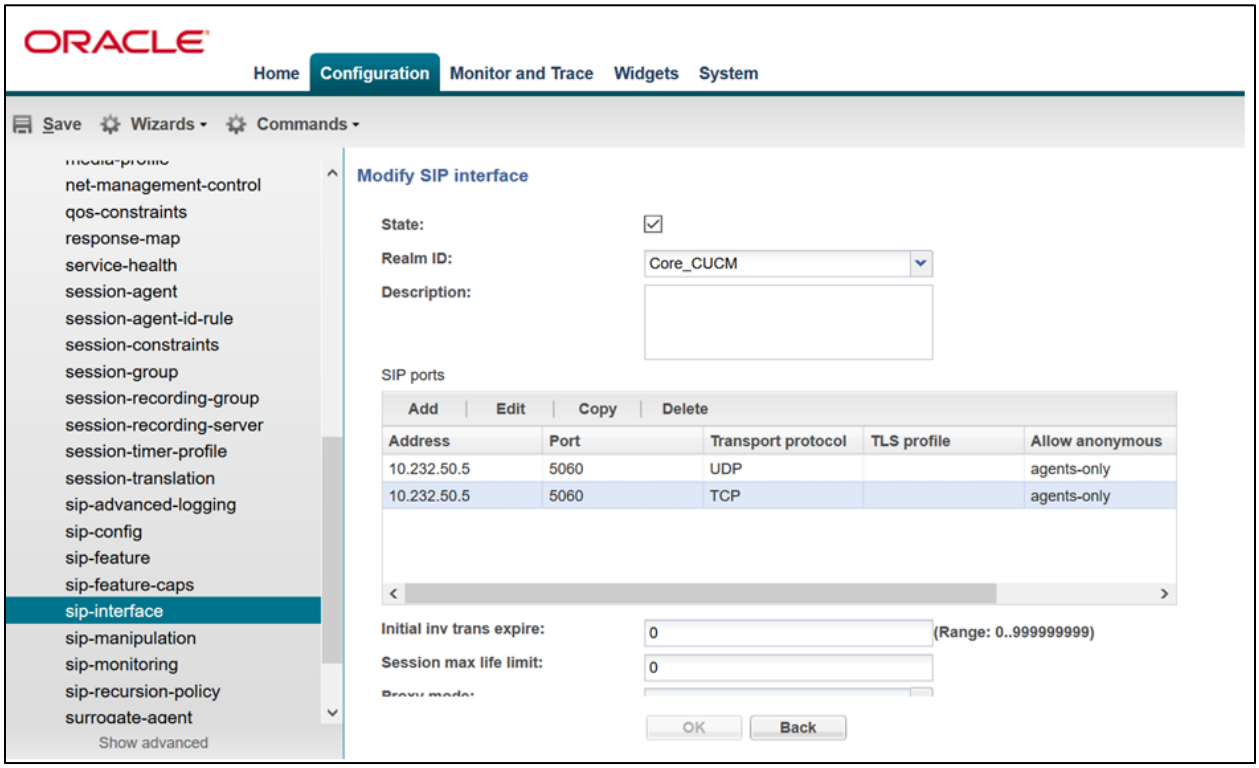
Navigate to sip-interface under session-router and configure the sip-interface as shown below

Configure the public facing IP under sip-port of sip-interface for Zoom Client.
Set allow-anonymous to registered to ensure that this sip-interface sends REGISTER from zoom phones to CUCM. Also, set the parameter “registration-caching” set to yes.





Similarly, Configure Internal IP under sip-port of sip-interface for CUCM side.

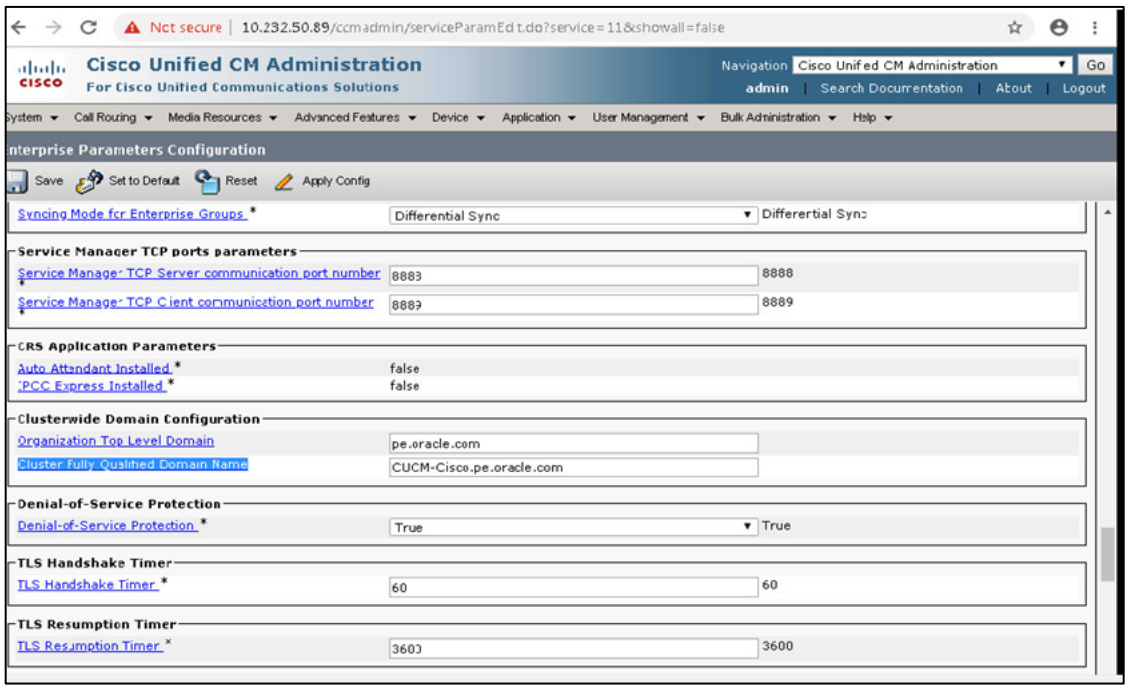


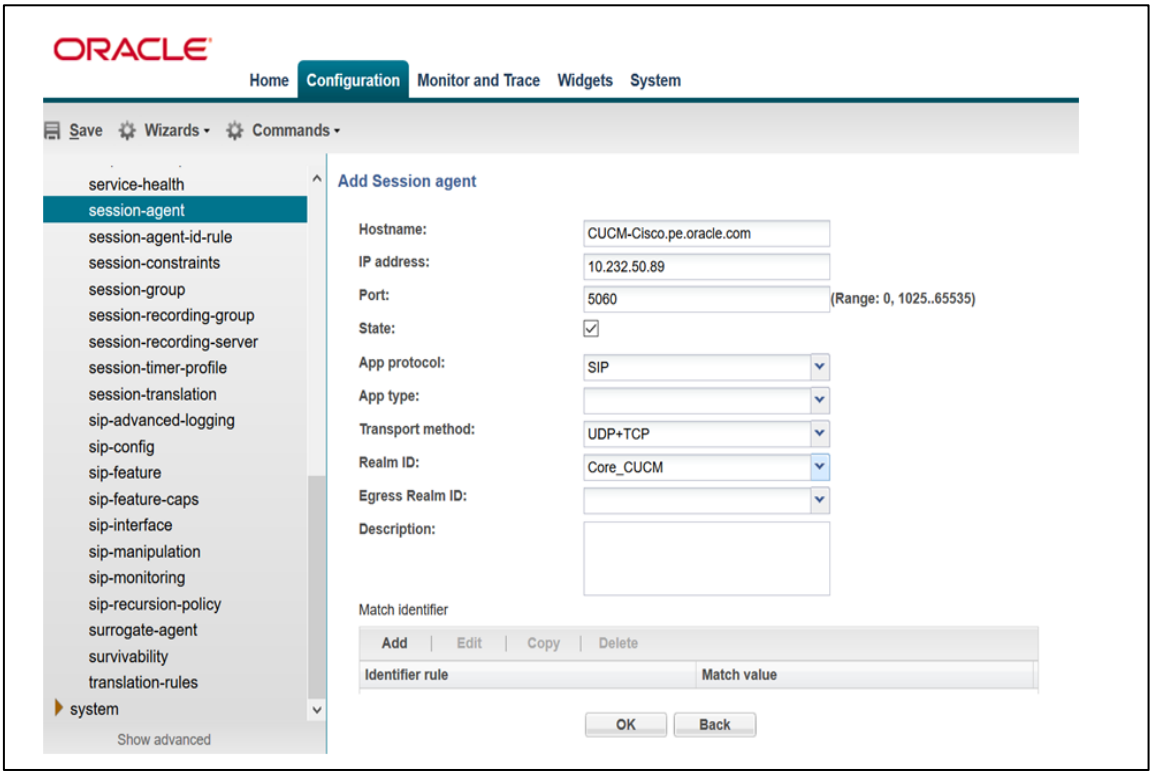
Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address. Now configure where the SBC sends the outbound traffic.

5.10. 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. Configure the Cisco CUCM session-agent to SBC with the following parameters, so that SBC can route the incoming traffic to the CUCM properly.

- hostname to FQDN of CUCM which is “CUCM-Cisco.pe.oracle.com” in this case. The same value is configured in Cisco CUCM under System → Enterprise Parameter → Cluster FQDN
- port 5060
- realm-id – needs to match the realm created for CUCM.
- transport set to “UDP+TCP”

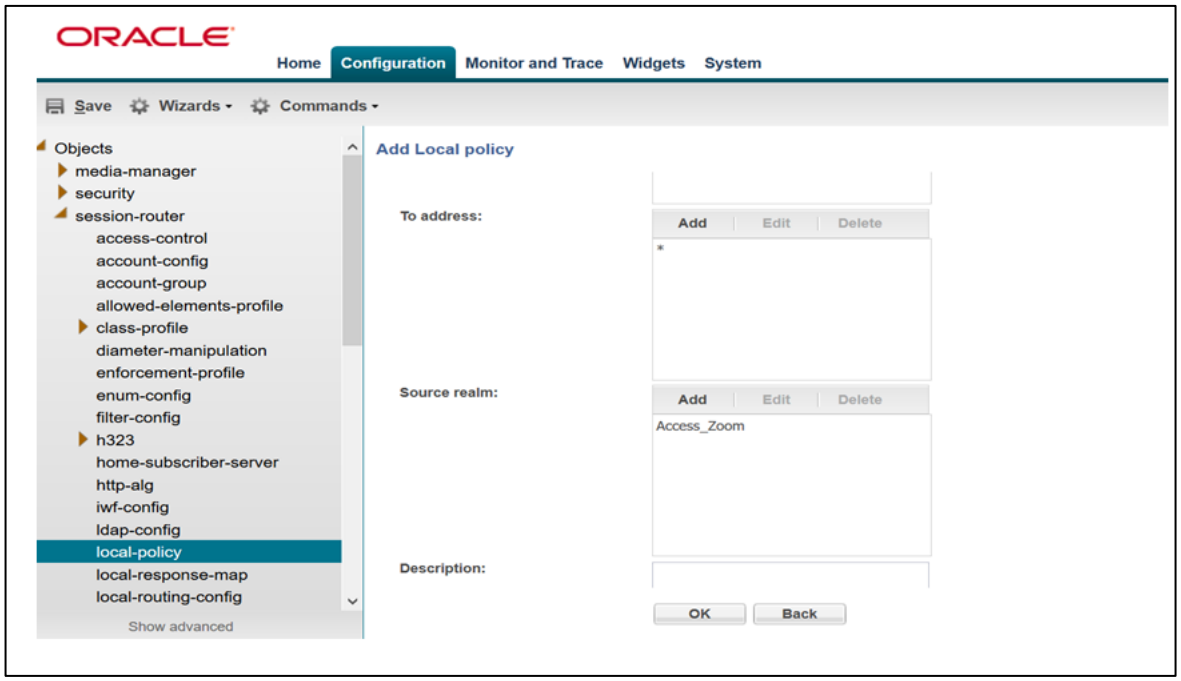

Not secure | 10.232.50.89/ccmadmin/serviceParamEdit.do?service=11&showall=false
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features 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 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

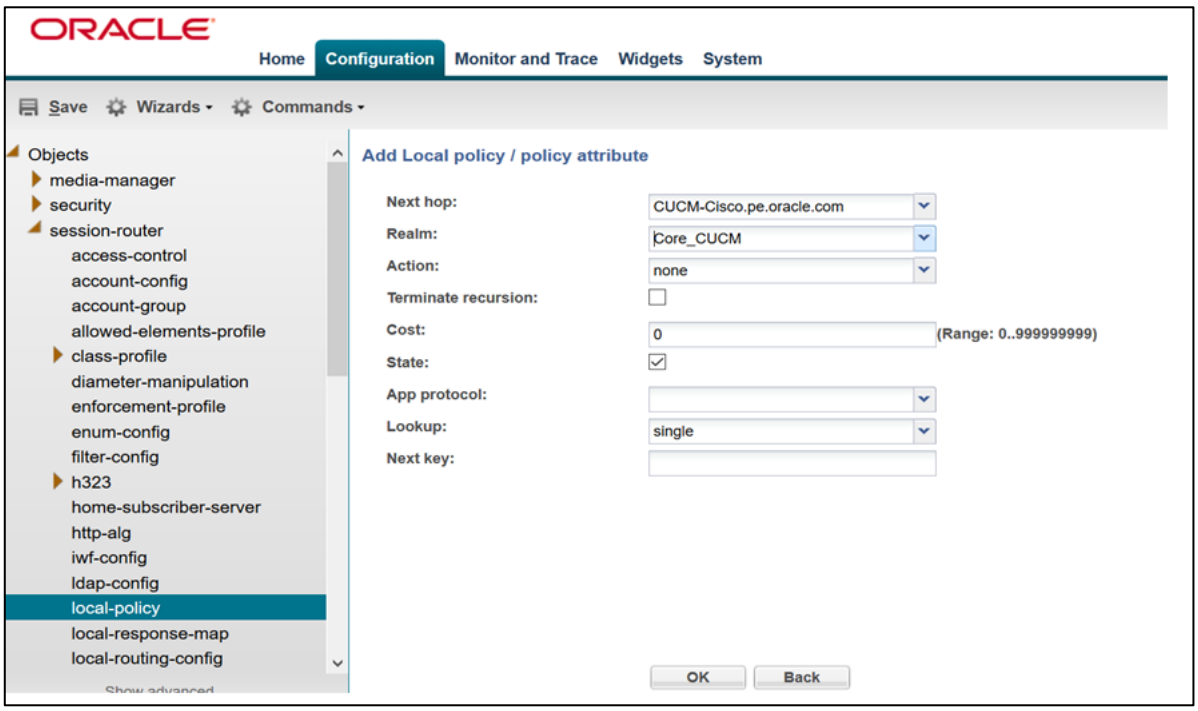

ORACLE
Home Configuration Monitor and Trace Widgets System
Save Wizards Commands
service-health
session-agent
session-agent-id-rule
session-constraints
session-group
session-recording-group
session-recording-server
session-timer-profile
session-translation
sip-advanced-logging
sip-config
sip-feature
sip-feature-caps
sip-interface
sip-manipulation
sip-monitoring
sip-recursion-policy
surrogate-agent
survivability
translation-rules
system
Show advanced
Add Session agent
Hostname: CUCM-Cisco.pe.oracle.com
IP address: 10.232.50.89
Port: 5060 (Range: 0, 1025..65535)
State:
App protocol: SIP
App type:
Transport method: UDP+TCP
Realm ID: Core_CUCM
Egress Realm ID:
Description:
Match identifier
Add Edit Copy Delete
Identifier rule Match value
OK Back

5.11. Configure local-policy

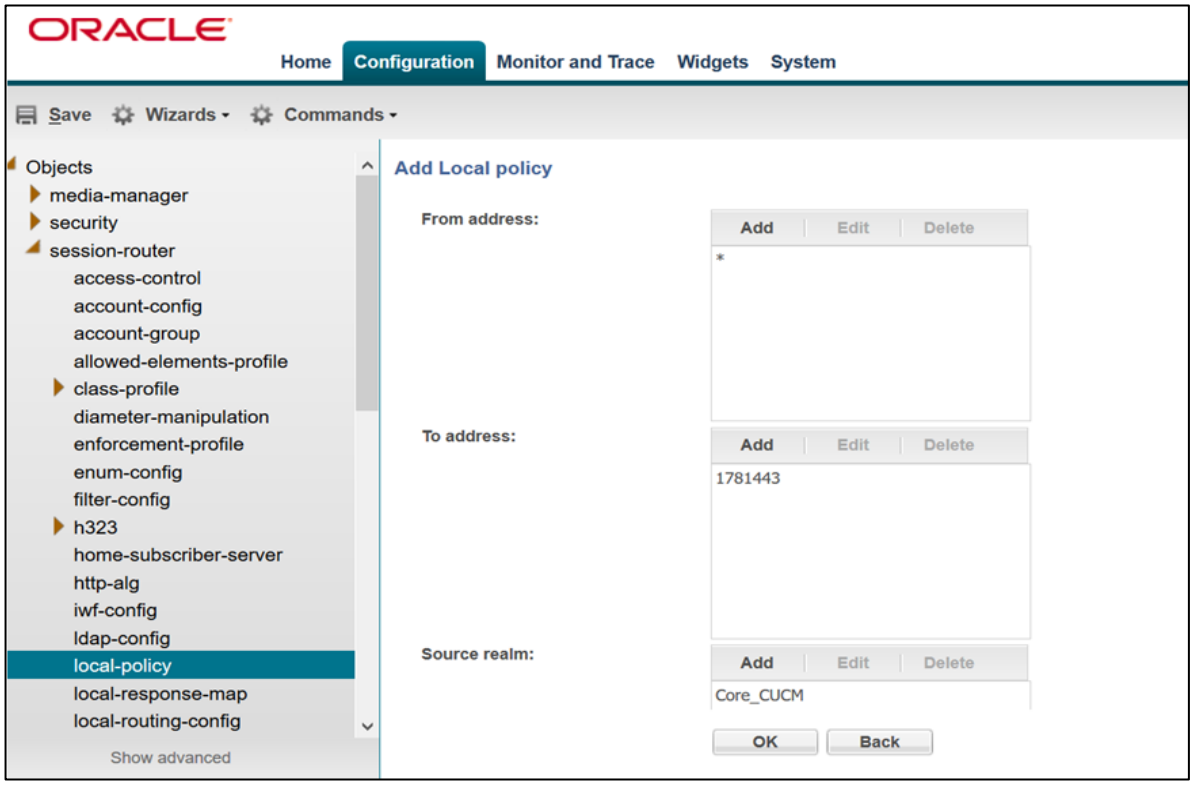
Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

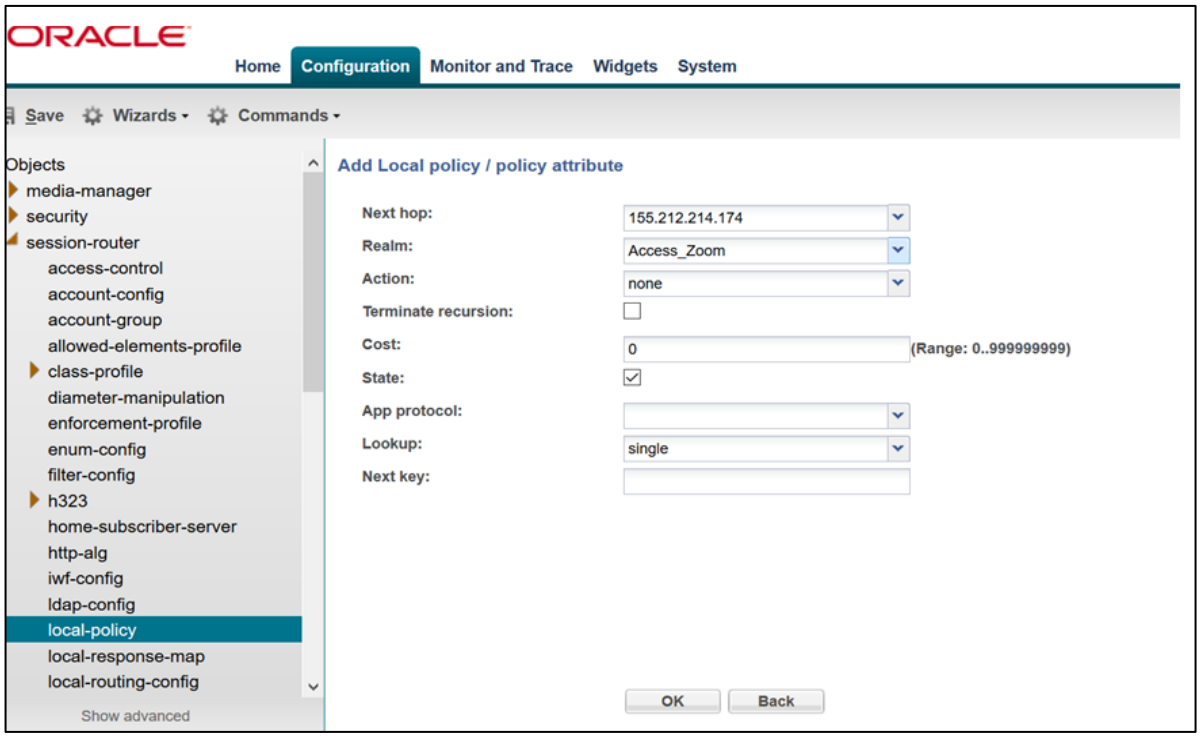
To make outgoing calls from Zoom phone, please configure the below local policy.





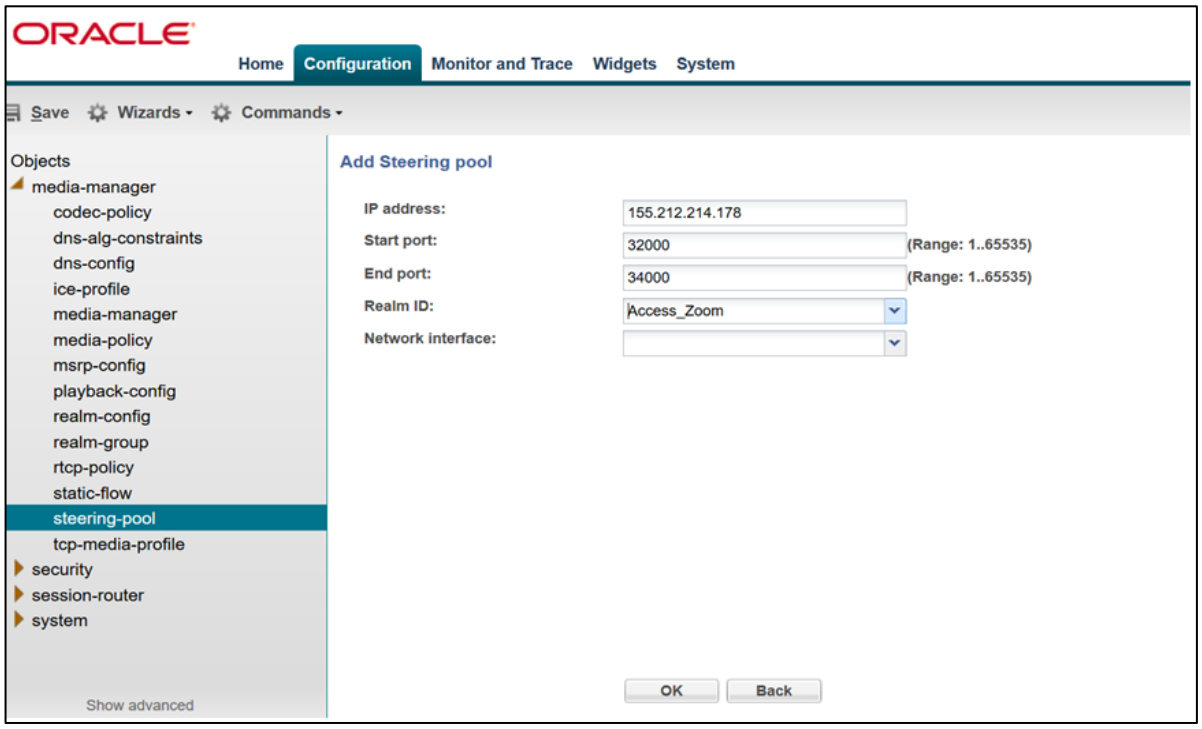
To make incoming calls to Zoom phone, please configure the below local policy.

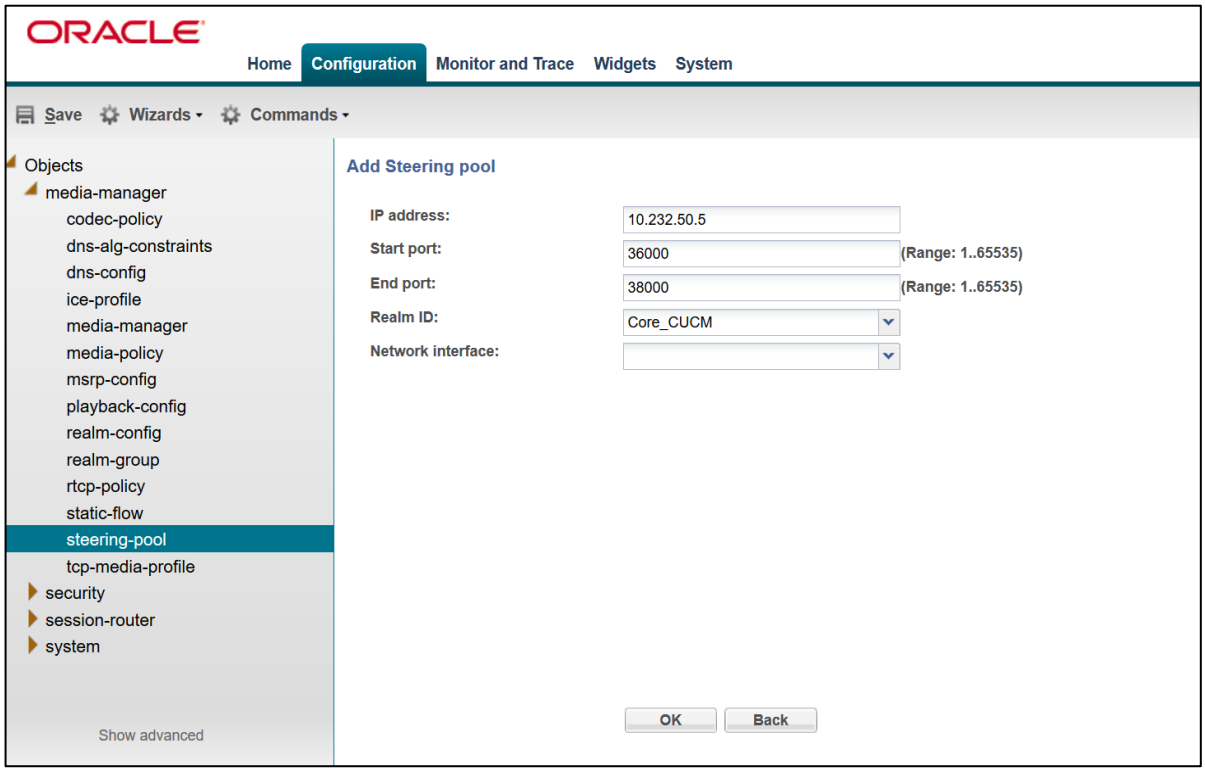




5.12. Configure steering-pool

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





5.13. Configure SIP Port-mapping

As the CUCM is not allowing registers from the same IP/Port combination, the zoom users may find difficulty in registering multiple End points in the CUCM as third party End points. This is the current limitation that is with CUCM now.

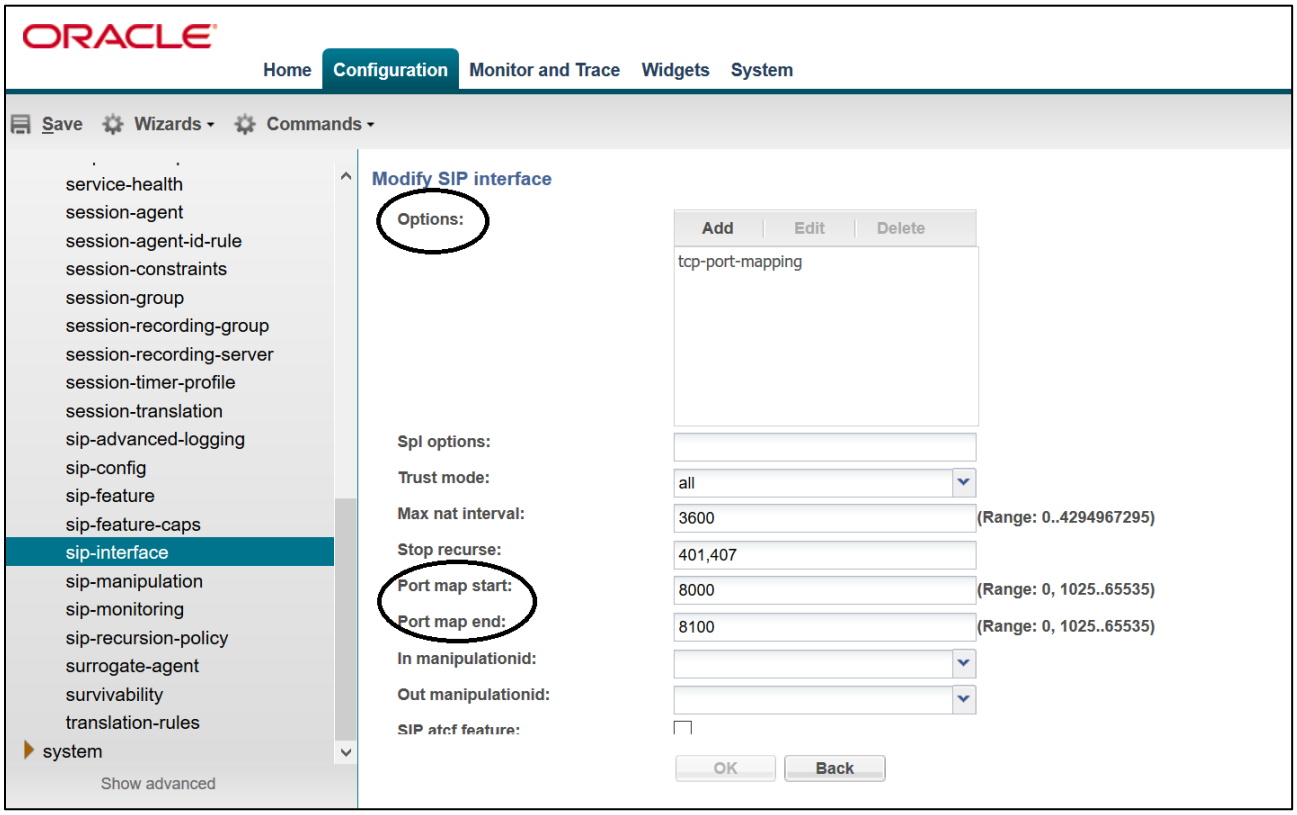
To overcome this issue/limitation, we can use SBC port mapping feature which changes the source port towards CUCM, thus changing the IP/Port combination received by CUCM, allowing multiple end points through the SBC.

To configure the port-mapping in SBC, please go to Session router --- SIP interface where you want this config and configure the below steps which is given as an example:

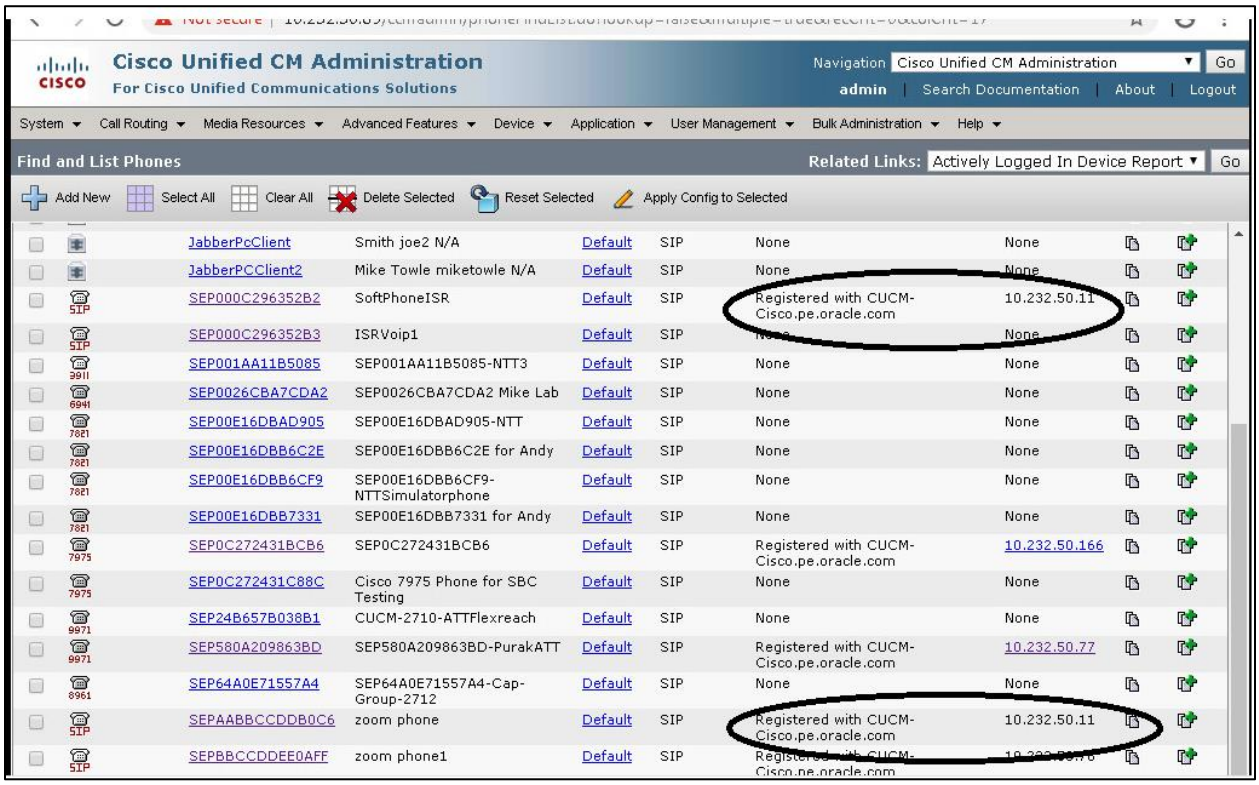
options --- tcp-port-mapping (This is only required if TCP or TLS is used between SBC and CUCM, and this is not needed for UDP connections)

and set the following port range:

port-map-start --- 8000
port-map-end --- 8100



After doing the above config along with all other required config, you can see that the CUCM now accepts register request from different end points which has the same IP.

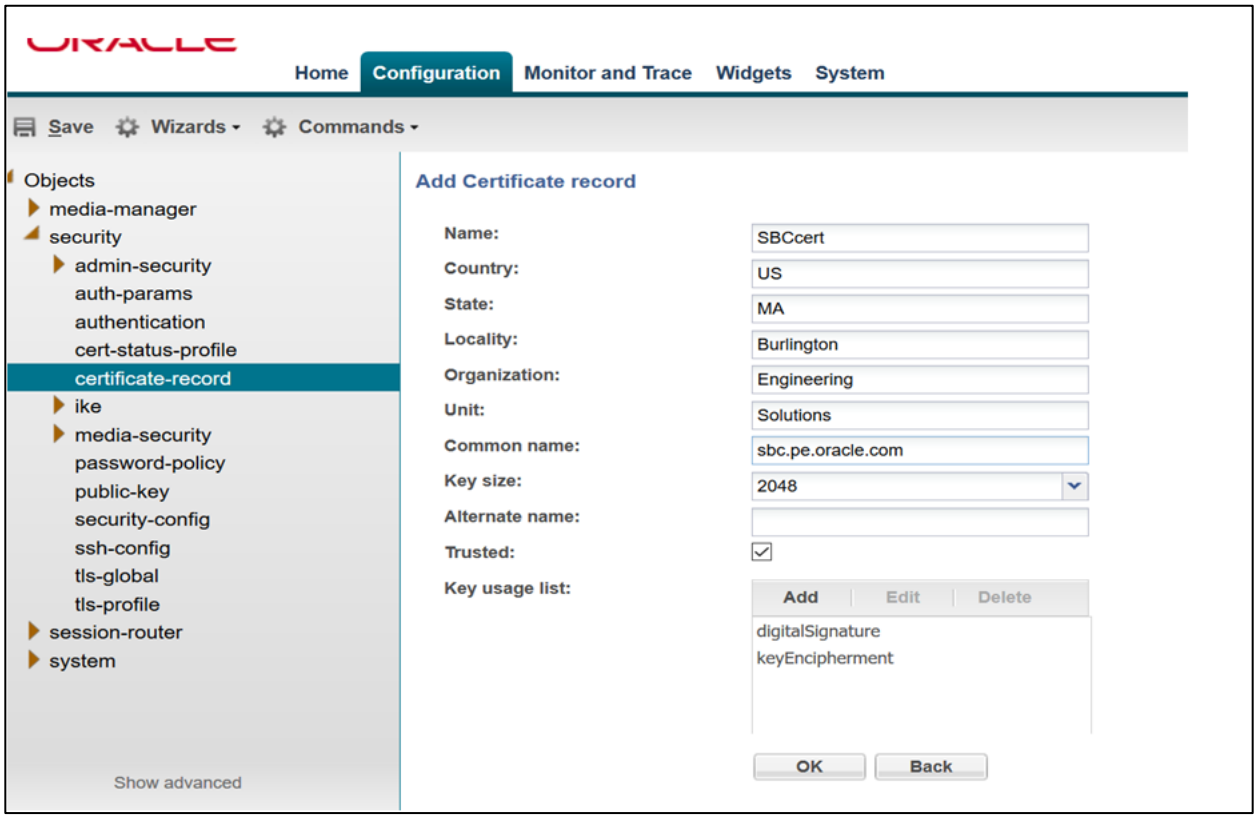


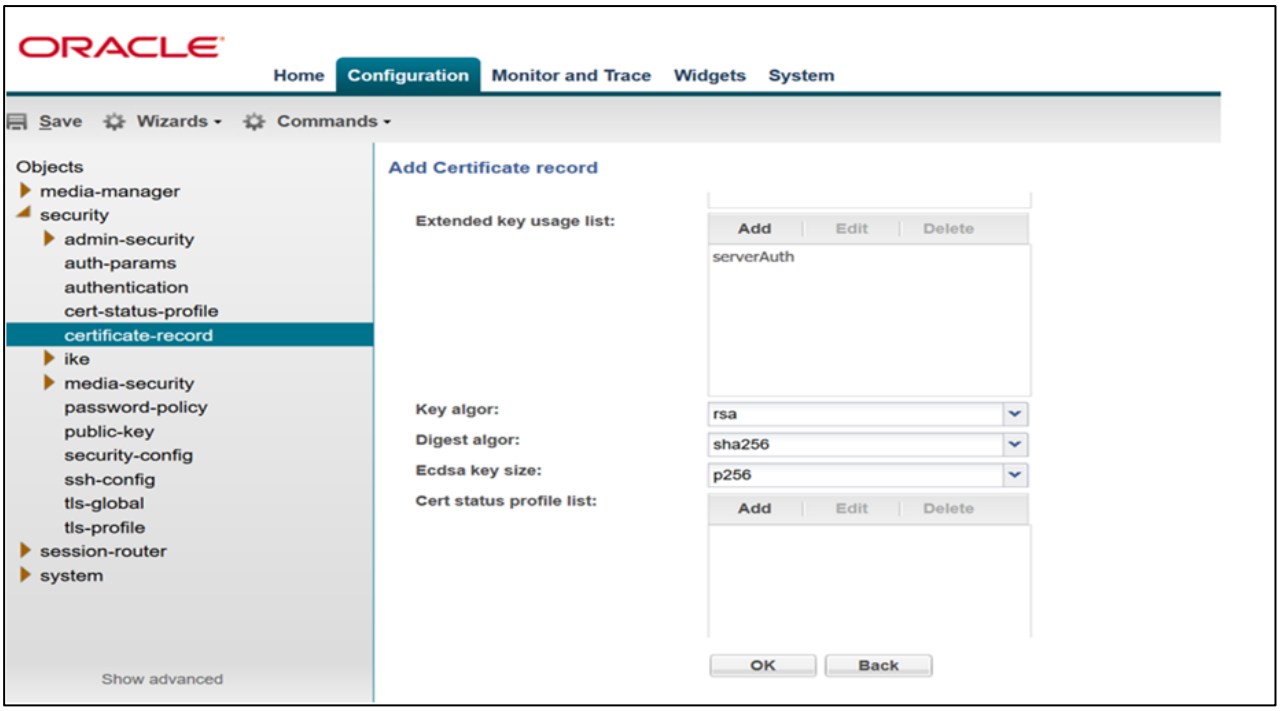
6. Configure SBC for TLS/SRTP Calls from Zoom Softphone

We have seen the SBC config in the previous sections where SBC receives the calls and registration from zoom client (Access realm) when transport protocol is either UDP or TCP. In case the SBC receives the packets from zoom client when the transport protocol is TLS, then the SBC configuration is different and the user has to do the below config in SBC to make the TLS/SRTP scenarios to be successful. Please note that this config is used for access realm (Zoom to SBC) and Core realm (SBC to CUCM) is still TCP/UDP.

6.1. Creating SBC End Entity Certificate

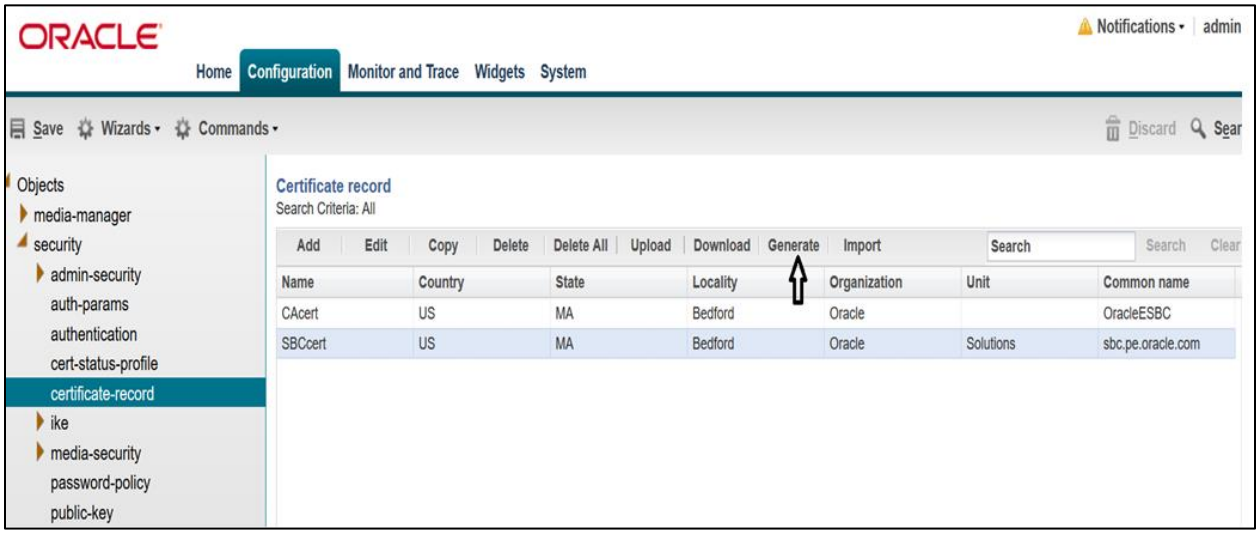
The first step is to create certificate record in the SBC and then adding it to TLS Profile for the zoom side. Please go to Configuration →Security → certificate record and create the SBC certificate:





6.2. Generate Certificate Signing Request

Now that the SBC's certificate has been configured, create a certificate signing request for the SBC's end entity only. On the certificate record page in the SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:

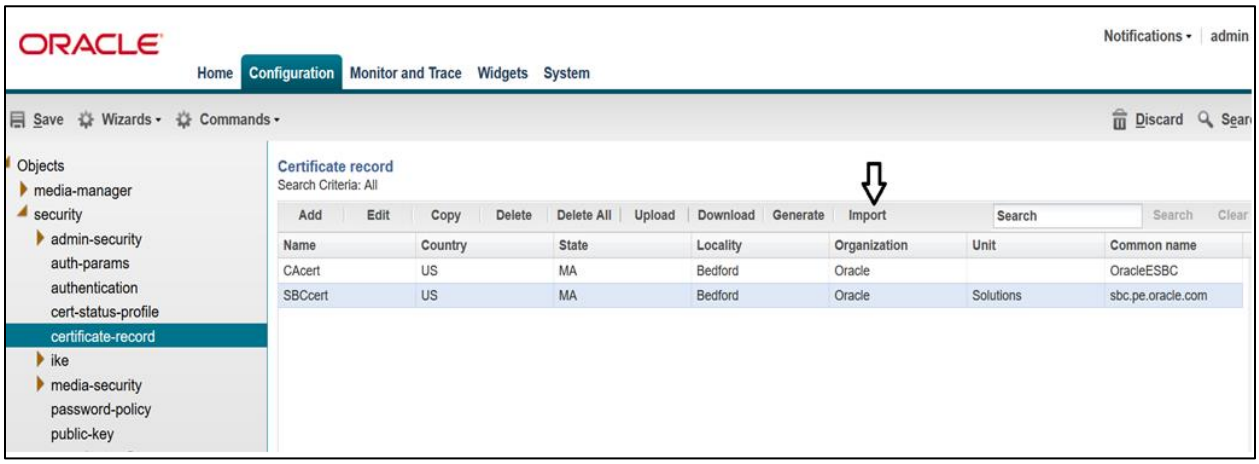


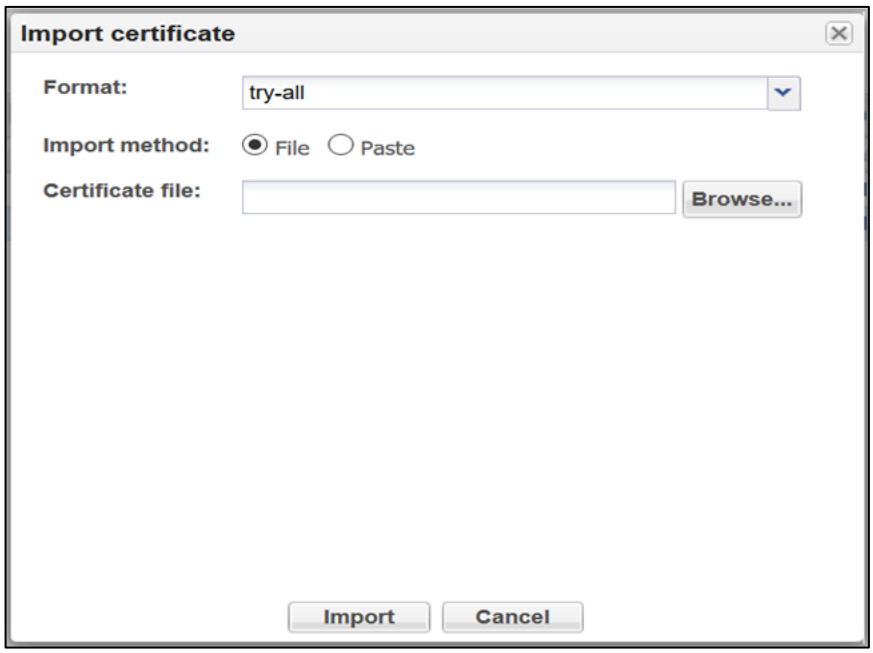
- Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.

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

6.3. Import Certificates to SBC

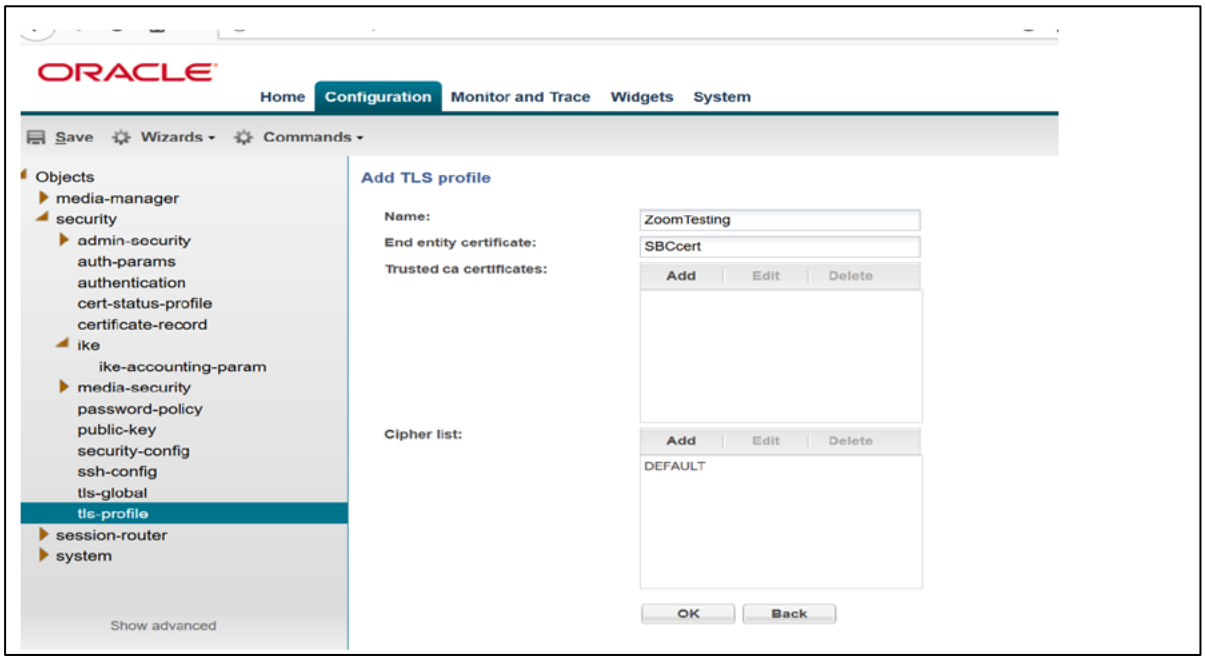
Once certificate signing request have been completed – import the signed certificate to the SBC. Once the certificate have been imported, please issue **save/activate** from the WebGUI





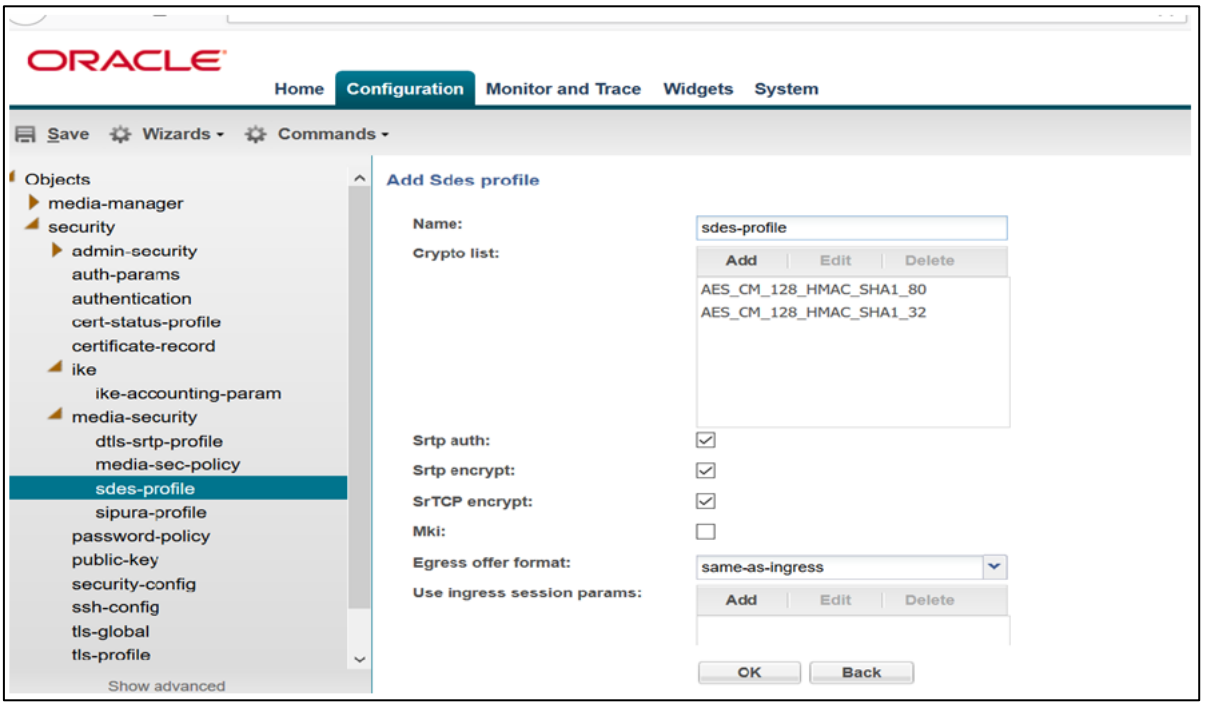
6.4. Creating TLS Profile

Please go to Configuration →Security → TLS profile and create the TLS profile as below:



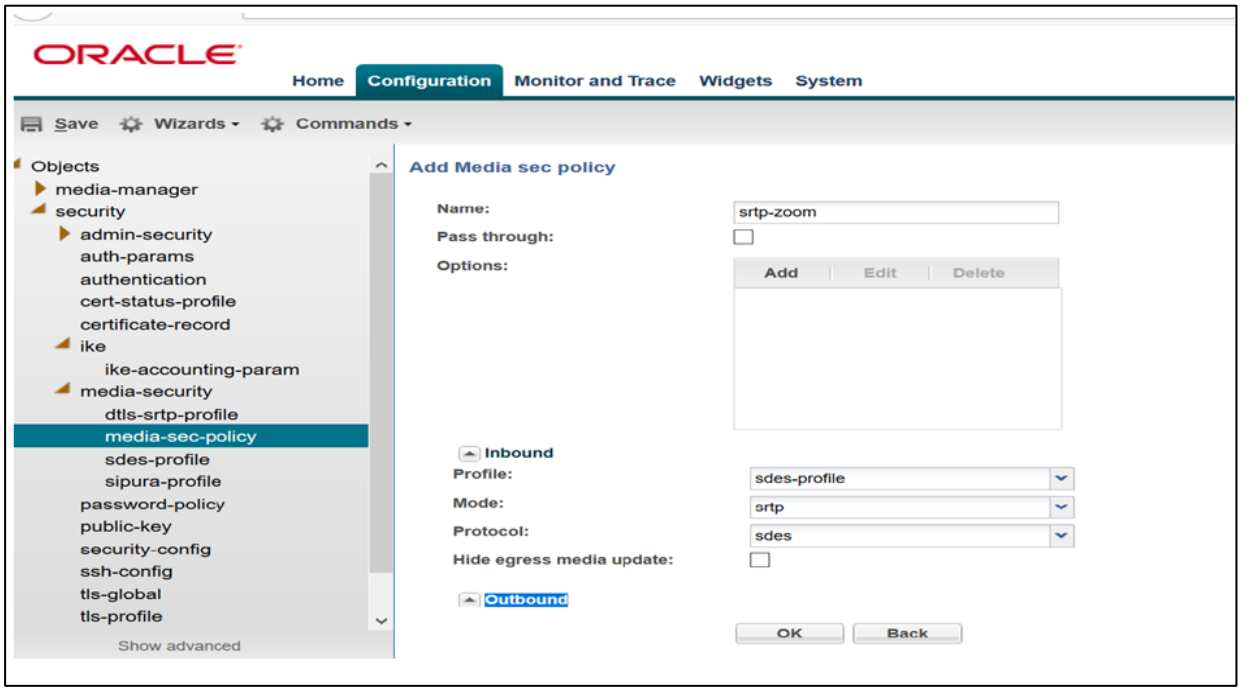
6.5. Configure sdes profile

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

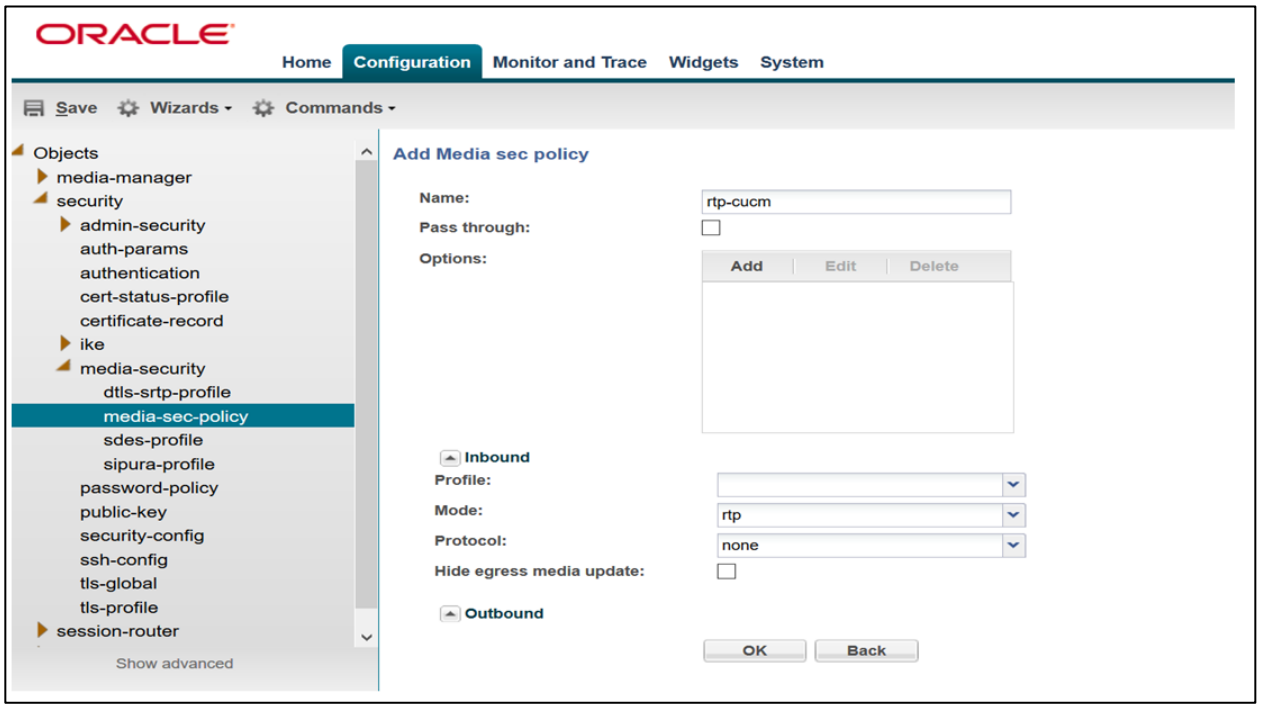


6.6. Configure Media Security Profile

Please go to →Security → Media Security →media Sec policy and create the policy as below:
Create Media Sec policy with name srtp-zoom for the access side which will have the sdes profile created above



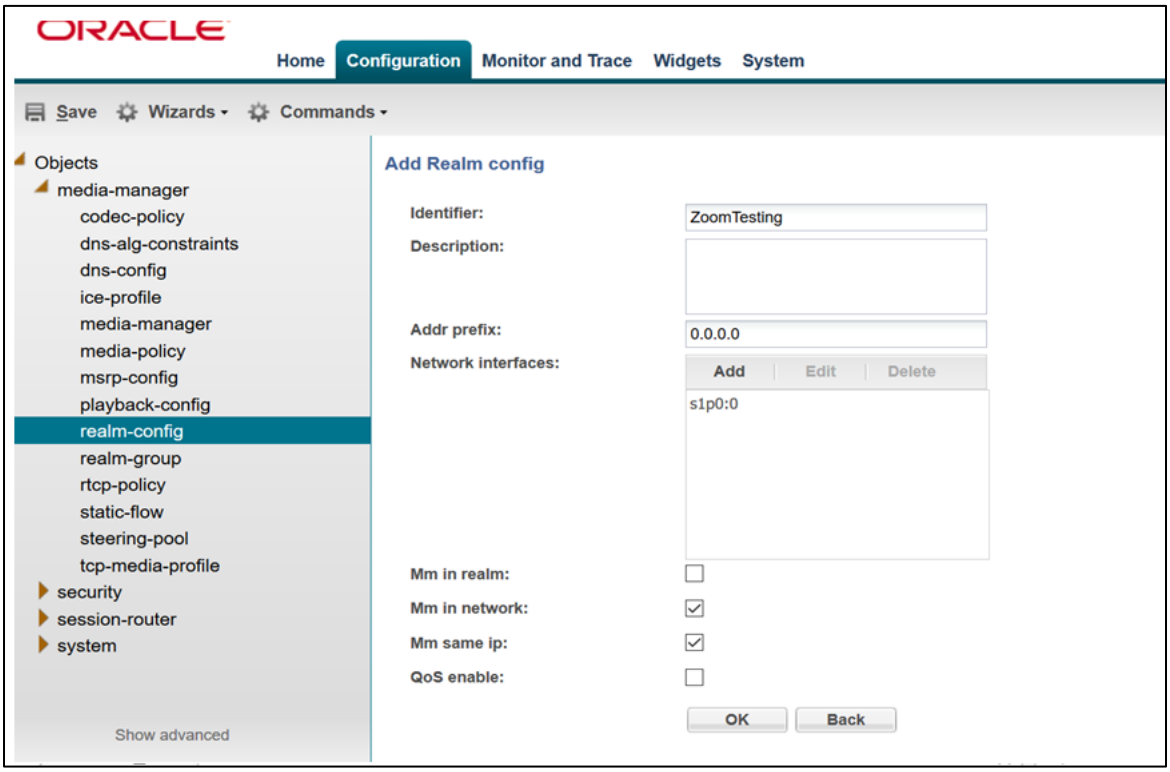
Similarly, Create Media Sec policy with name rtp-cucm to convert srtp to rtp for the core side which will use only TCP/UDP as transport protocol

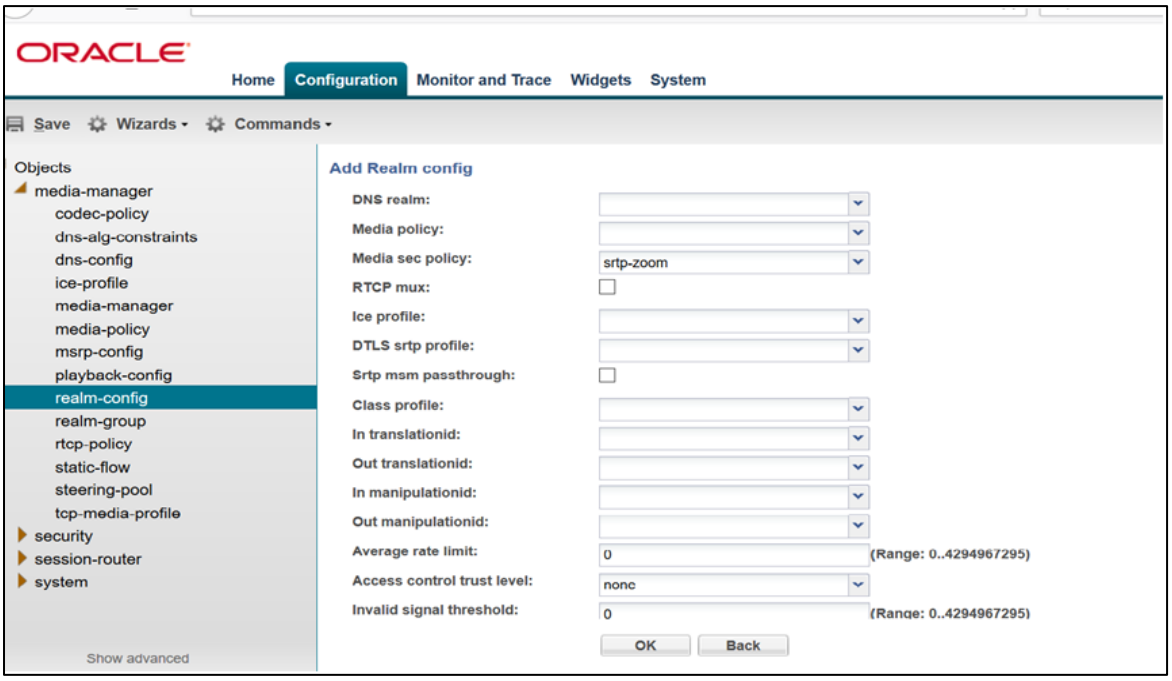


6.7. Configure Realms

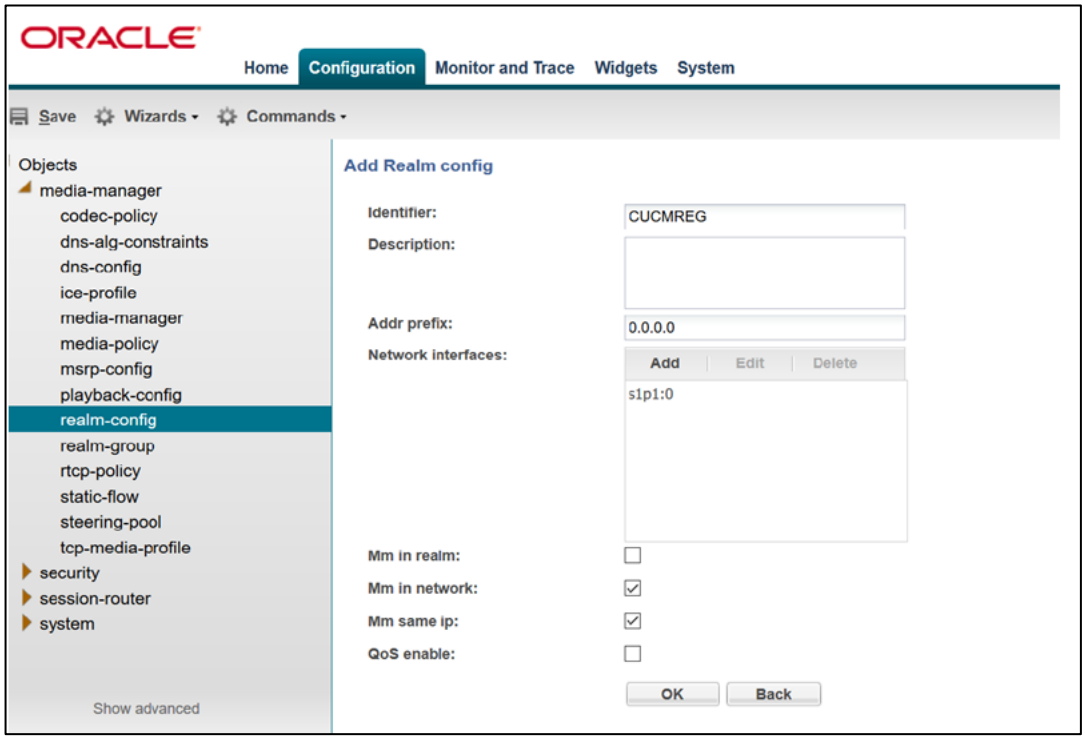
Navigate to realm-config under media-manager and configure a realm as shown below

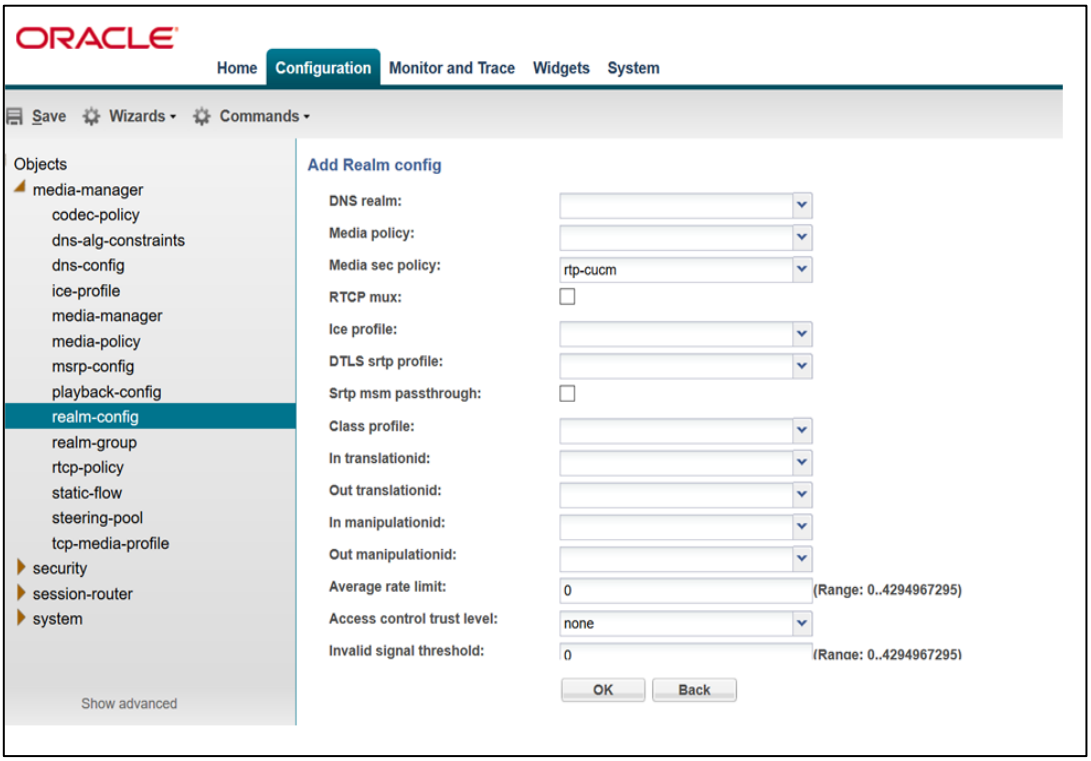
In the below case, Realm name is given as ZoomTesting for access side (Zoom Side)
Please note that corresponding Media Sec Policy is assigned to this Realm





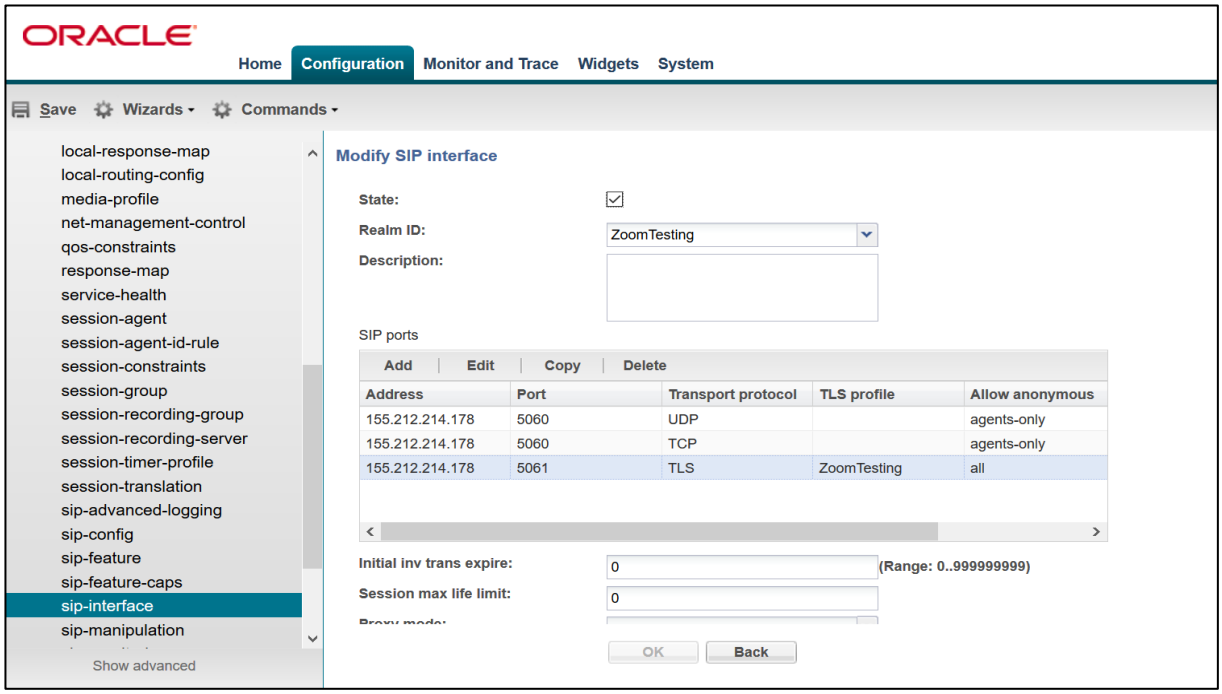
Similarly, configure the realm for the CUCM side as given below:
Please note that the corresponding Media Sec Policy is assigned to this Realm too



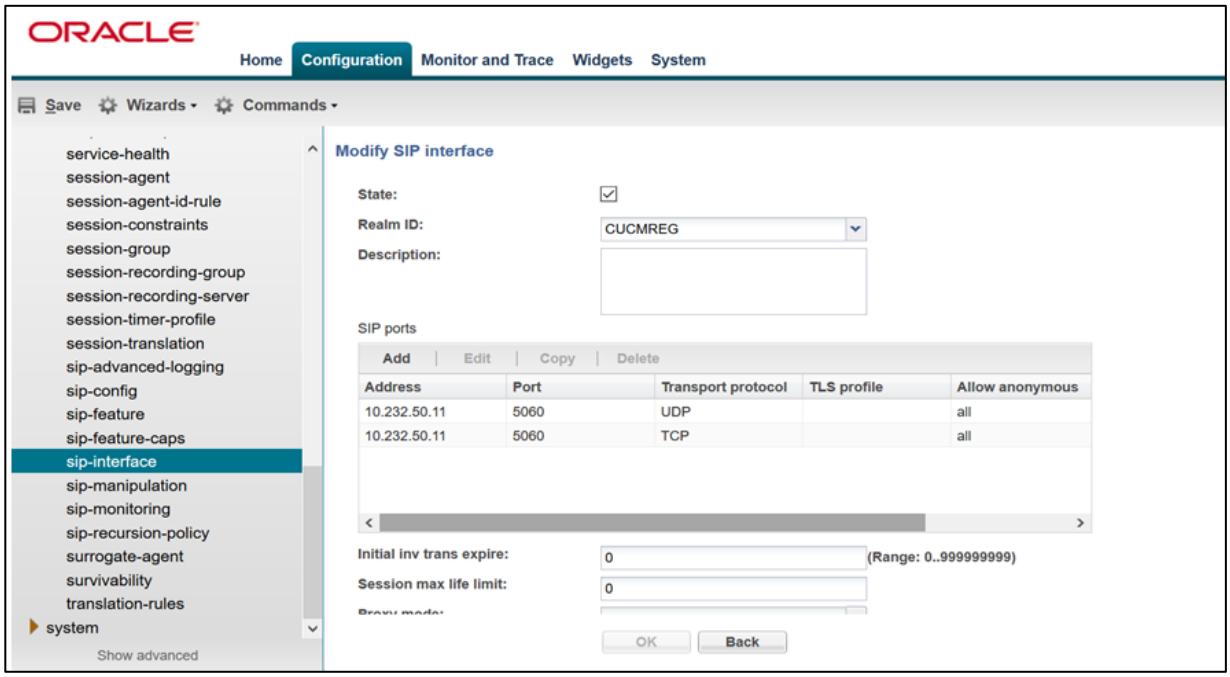


6.8. Configure SIP Interfaces.

Navigate to sip-interface under session-router and configure the sip-interface as shown below
Configure the interface IP under sip-port with TLS (5061) along with TCP/UDP for Zoom Client as below:



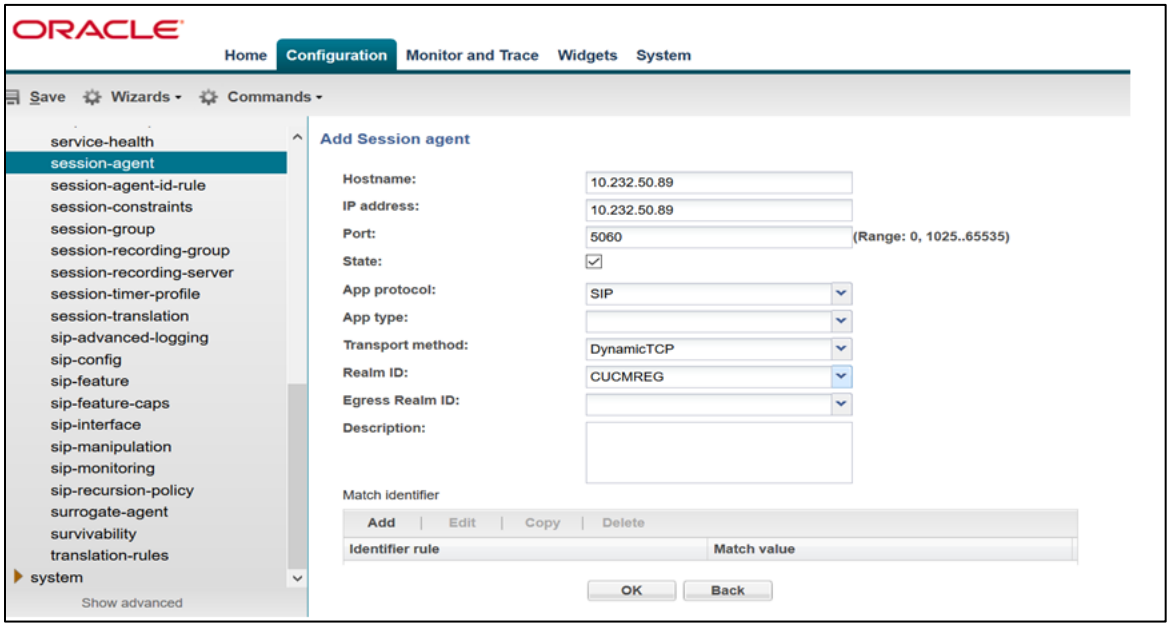
Similarly, create one more interface for CUCM side as below with only TCP/UDP.

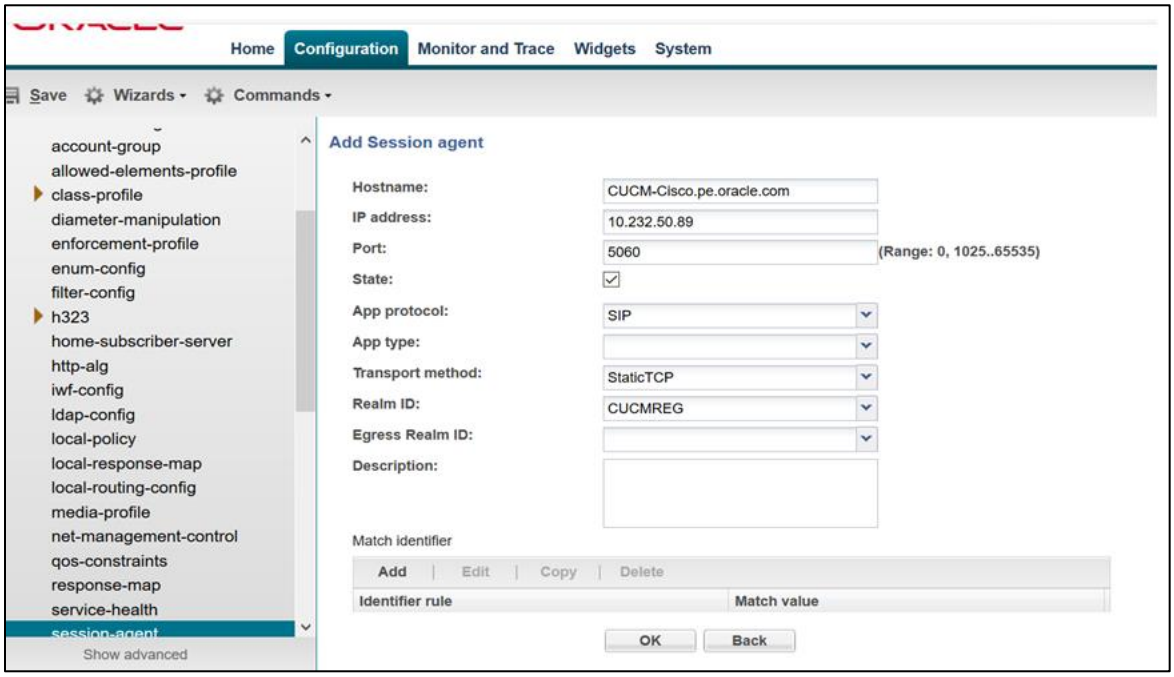


6.9. Configure session-agent

Please configure the Session Agent for CUCM side as below

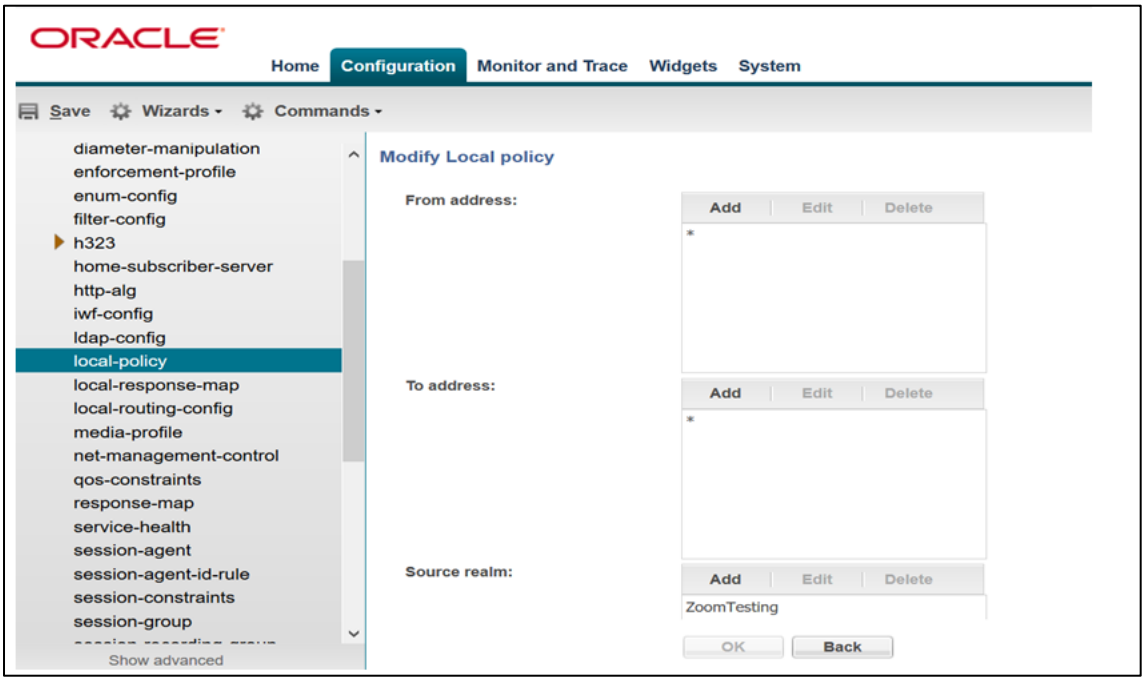
Please go to session-router and configure session-agent as shown

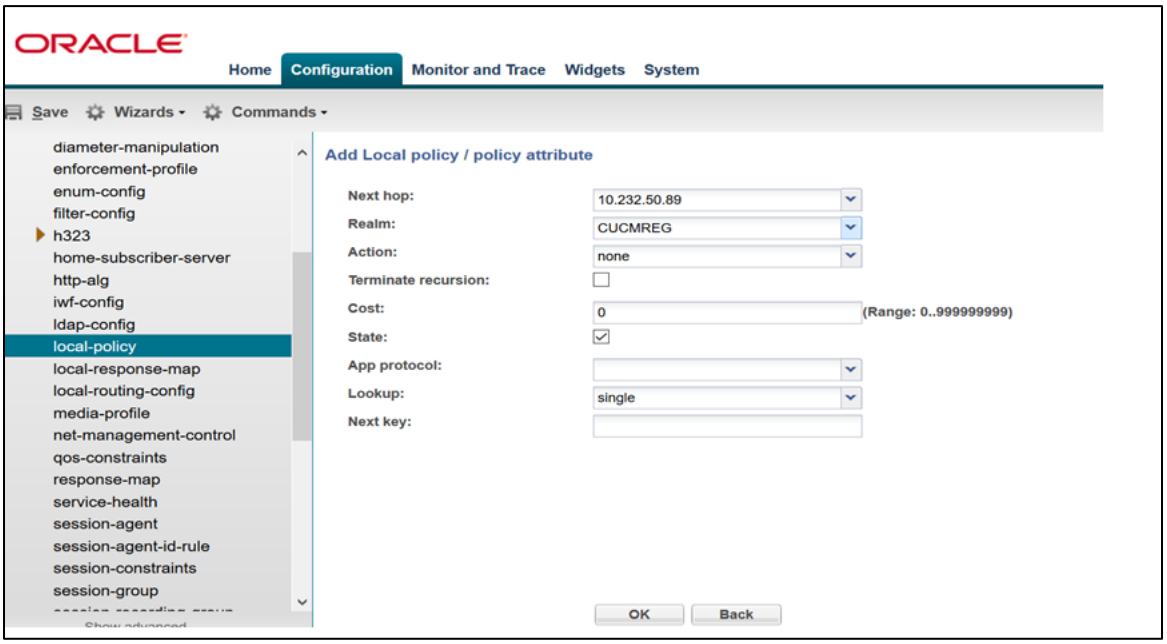


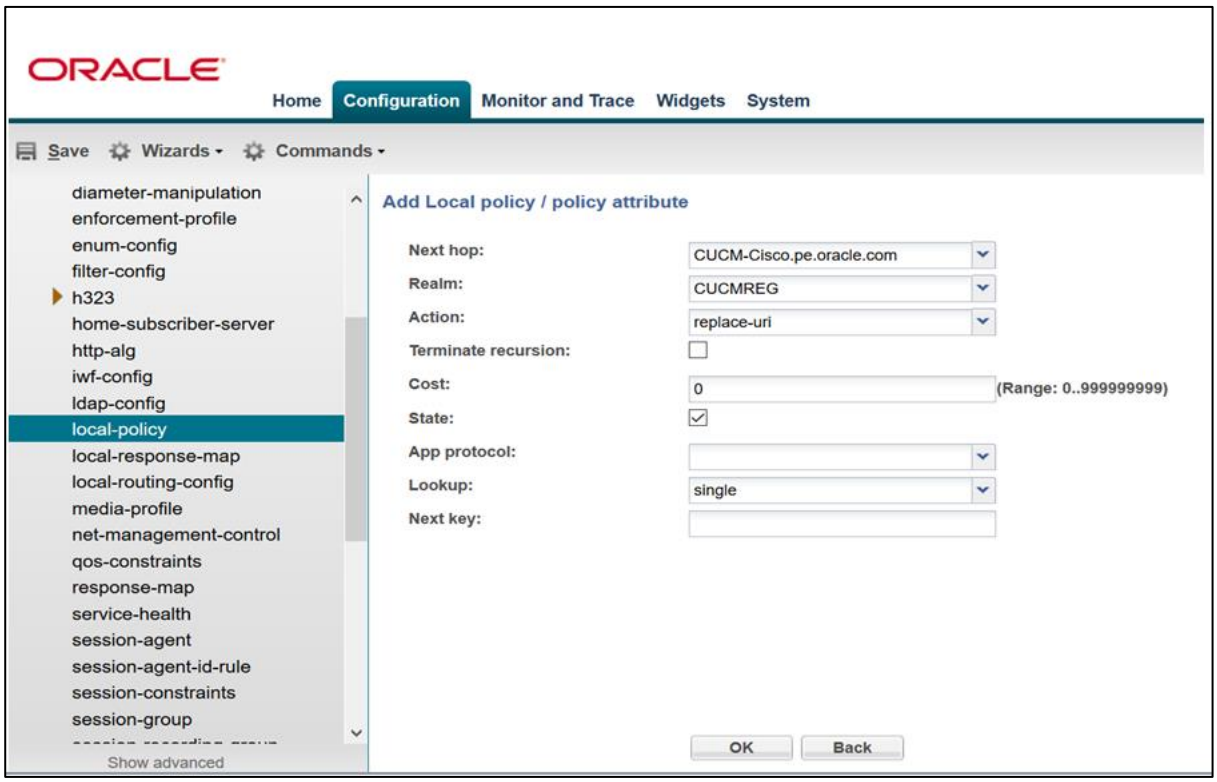


6.10. Configure local-policy

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 make calls from Zoom phone, please configure the below local policy.

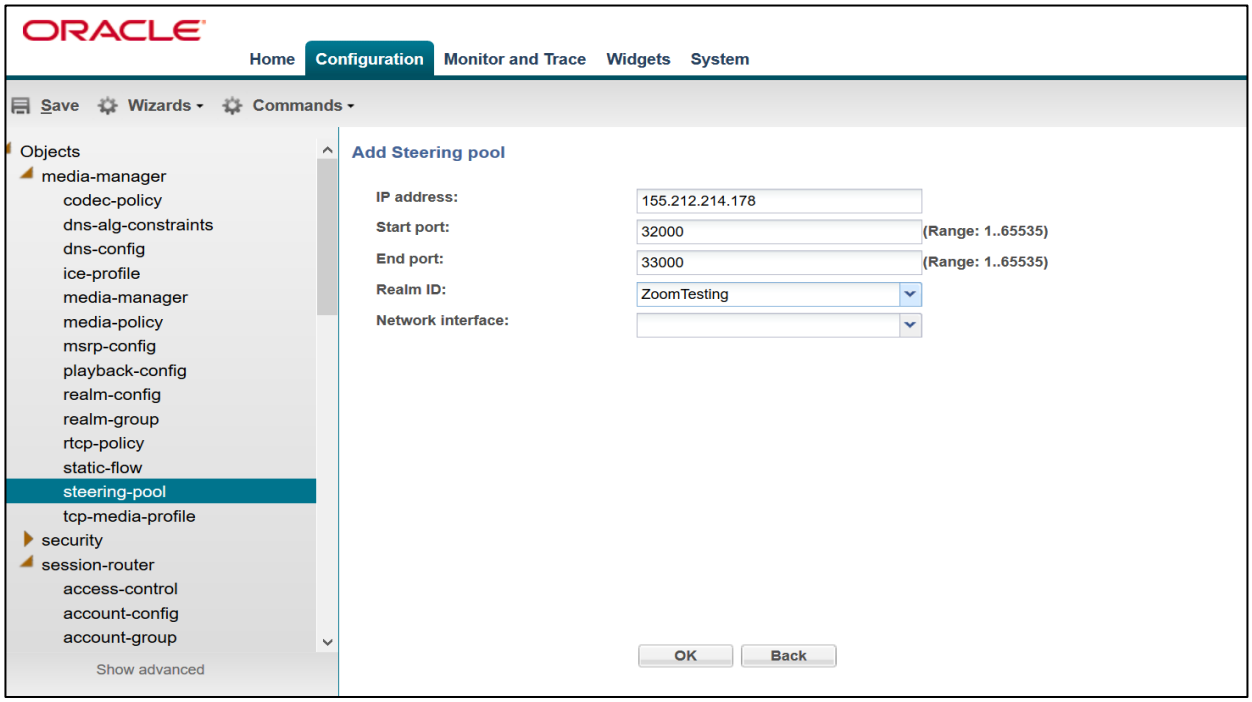


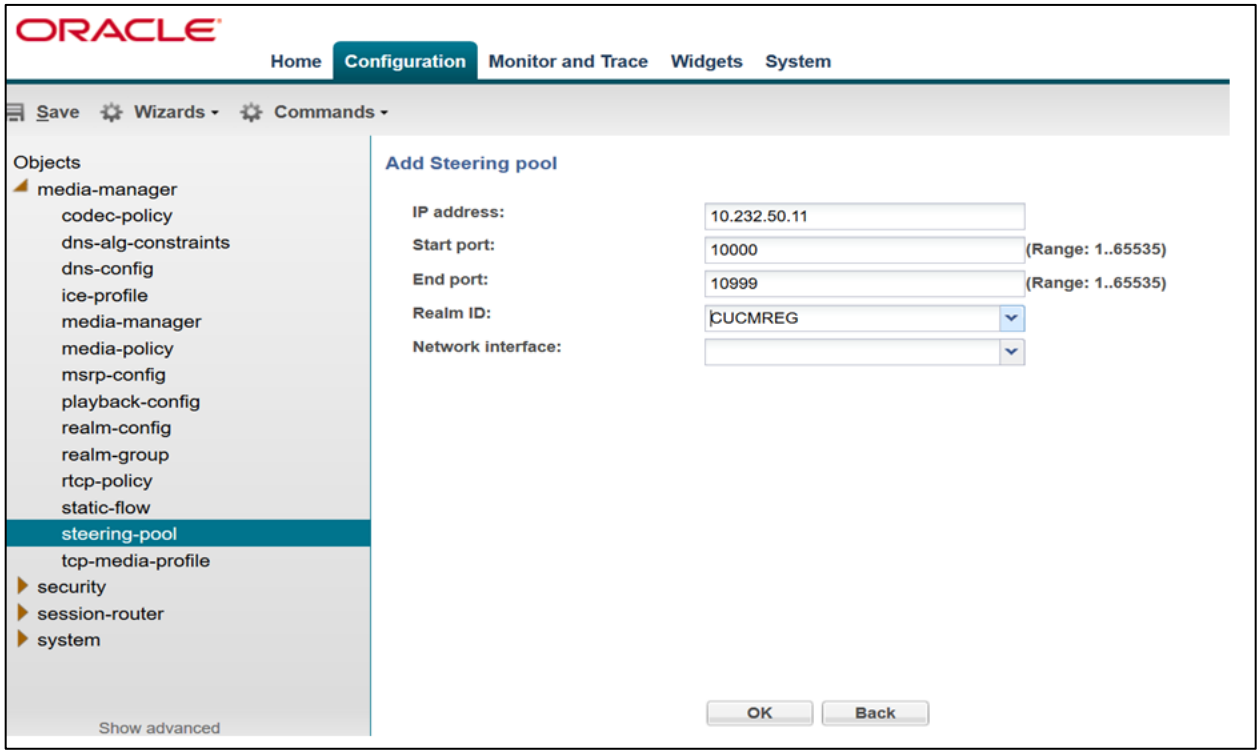



ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
diameter-manipulation
enforcement-profile
enum-config
filter-config
h323
home-subscriber-server
http-alg
iwf-config
ldap-config
local-policy
local-response-map
local-routing-config
media-profile
net-management-control
qos-constraints
response-map
service-health
session-agent
session-agent-id-rule
session-constraints
session-group
Show advanced
Add Local policy / policy attribute
Next hop:
CUCM-Cisco.pe.oracle.com
Realm:
CUCMREG
Action:
replace-uri
Terminate recursion:
Cost:
0
(Range: 0..999999999)
State:
App protocol:
Lookup:
single
Next key:
OK
Back

6.11. Configure steering-pool

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





6.12. Delayed Offer testing from Cisco CUCM to Zoom Client

In delayed offer testing from CUCM side, it is made sure that the CUCM does not include SDP in invites to the SBC on outbound calls to zoom endpoints registered through the SBC and SBC adds the SDP parameters to the outgoing invites to the Zoom client and then zoom client responds with its SDP on 200 OK and the call is established successfully after that. The testing is carried out in a manner that the CUCM to SBC leg is with TCP and SBC to zoom side is with TLS protocol.

Note: Using delayed offer/answer on CUCM with SBC and zoom, one need to configure add sdp invite, with media profiles in the corresponding sip interface of the SBC.

Note: As the Zoom client uses TCP and TLS messages and it uses TCP keep alive, this may trigger the invalid-signal-threshold timer which is related to DDOS settings and it will be the responsibility of the End User to take care of those settings and avoid the issue.

7. Existing SBC Configuration

If the SBC being used as Proxy for Zoom phone and CUCM integration is an existing SBC, then following configuration elements are required:

- New realm-config
- Enable sip-config
- New sip-interface
- New session-agent
- New Local-policy
- New steering-pools

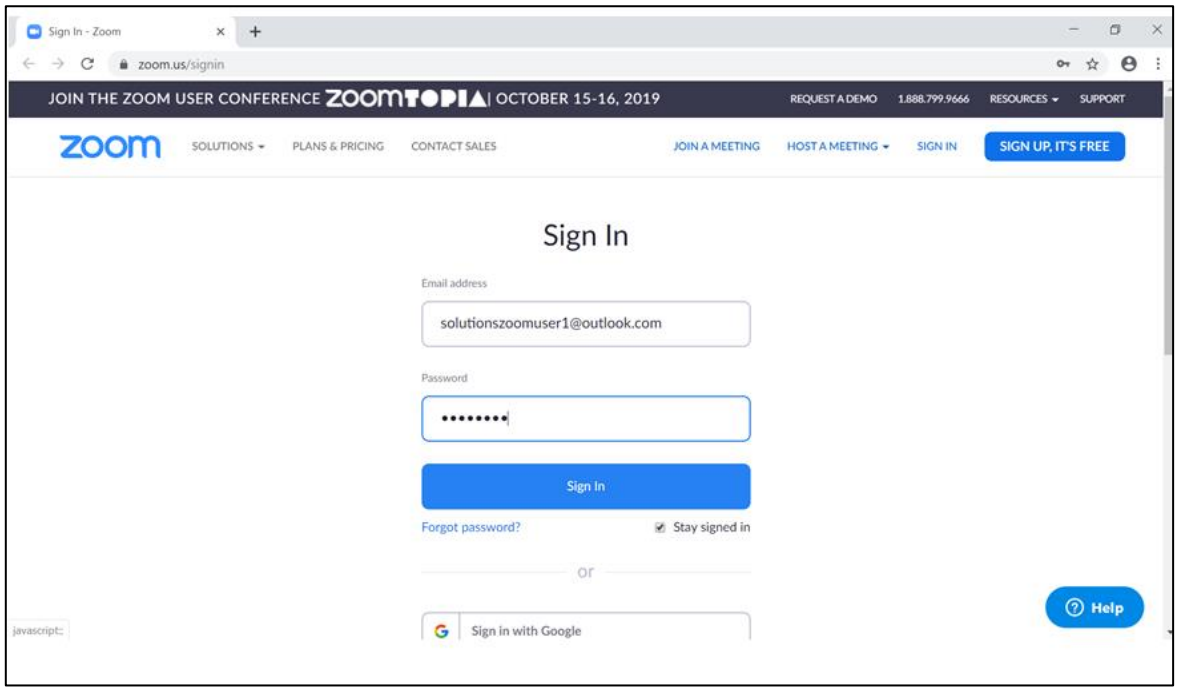
Please follow the steps mentioned in the above chapters, to configure these elements.

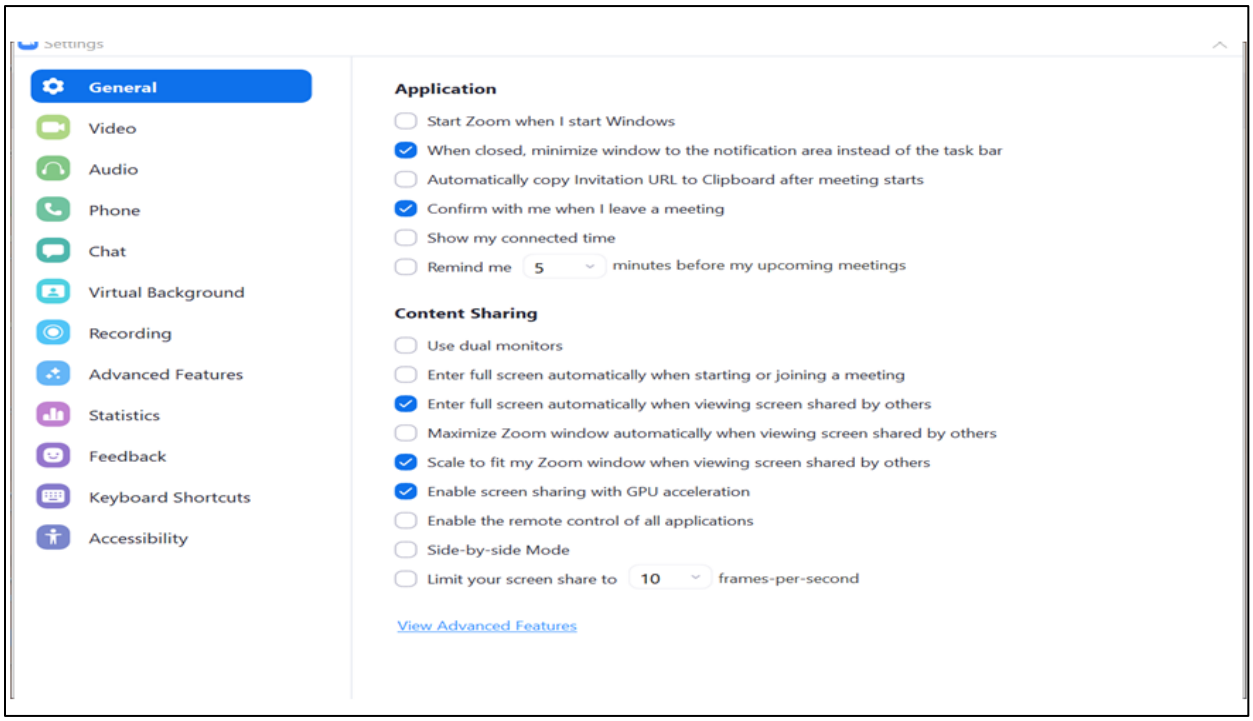
8. Configuring the Zoom softphone in Admin Portal

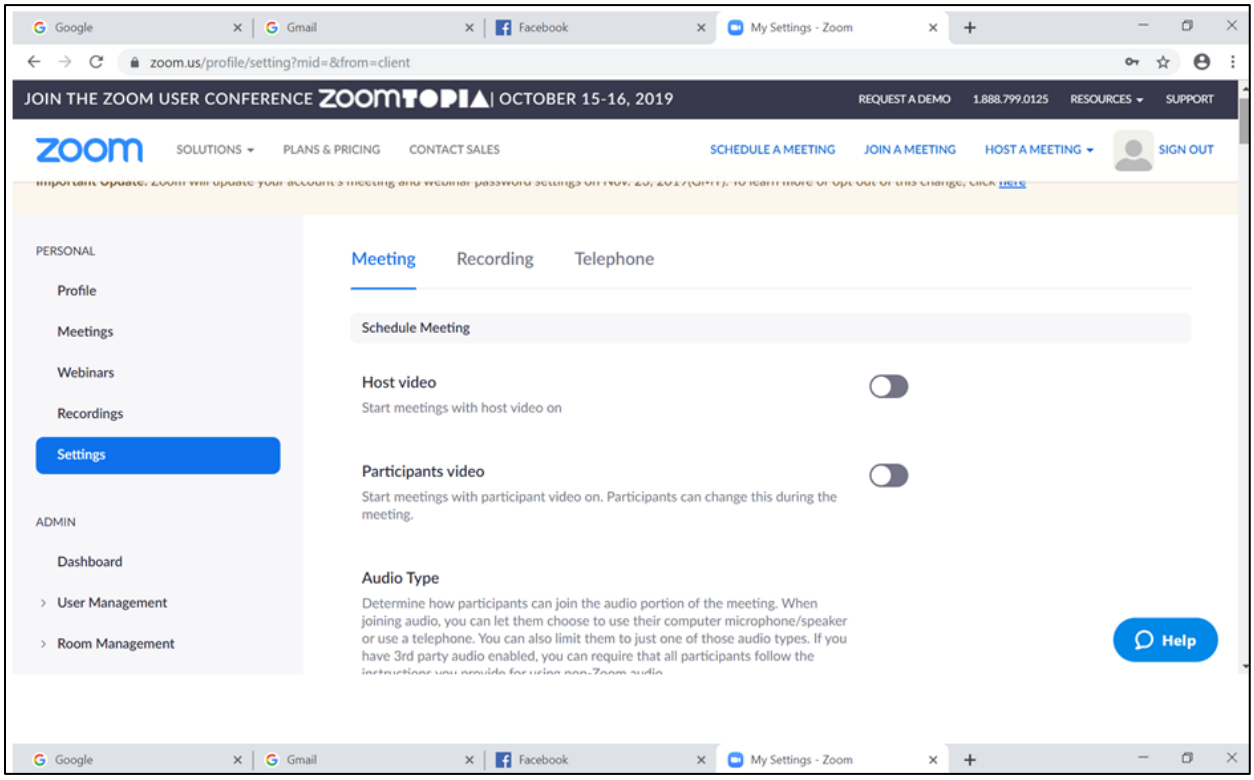
Once the CUCM and SBC configuration is done for the zoom softphones, we can now proceed to the zoom client side configuration. To proceed with zoom configuration, we need an admin account with a user created with credentials (Valid Email ID and Password) in zoom admin portal
It is assumed that whoever follows this document has the account with them and we can proceed with the steps below:

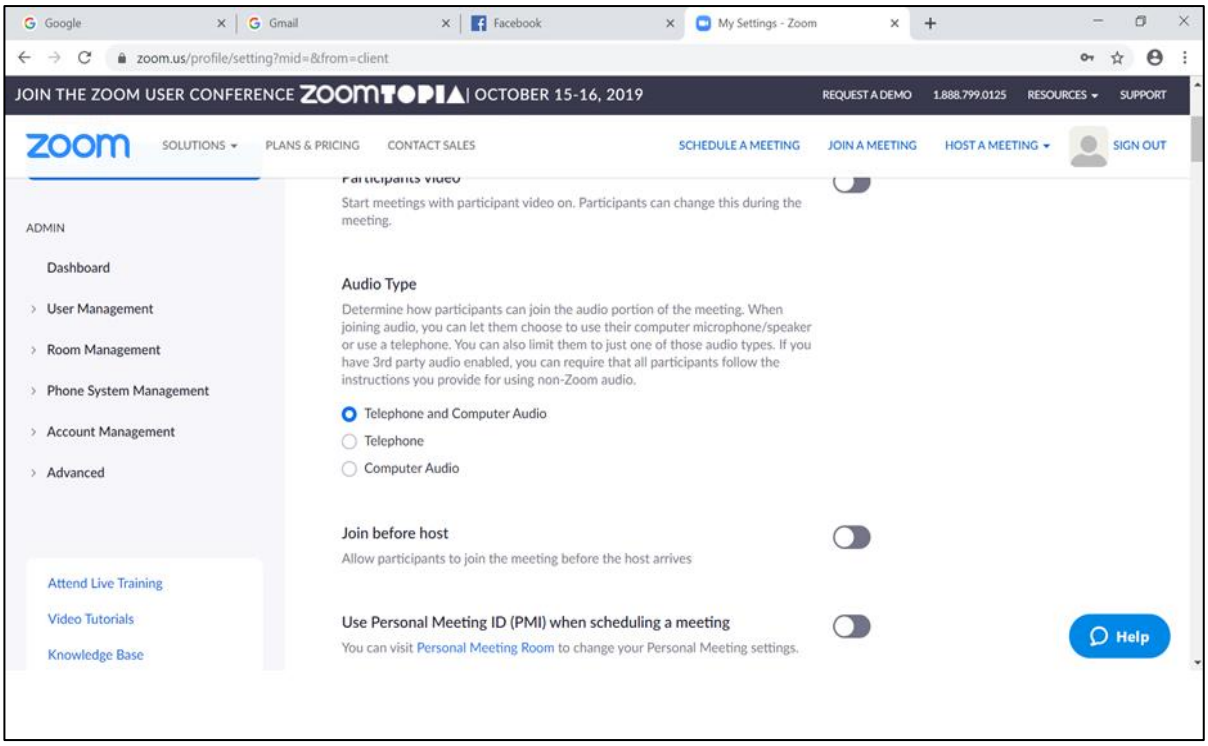
1) Please login to zoom admin portal in the local machine with admin credentials
2) After successful login, go to the user on the top right corner and click settings options.
3) After Settings options opens in a separate window, please click on the "View Advanced Features" option in the bottom of the window.
4) After that, new web page opens and asks for the credentials again and enter the credentials again.
5) This will open the advanced features of Zoom and the actual configuration for Zoom softphones are performed here under ADMIN option.

From now on, whenever the document refers to “Go to Advanced features" or “Admin” options, please note that the above steps have to be performed in Zoom admin portal to perform necessary configuration.




Settings
General
Video
Audio
Phone
Chat
Virtual Background
Recording
Advanced Features
Statistics
Feedback
Keyboard Shortcuts
Accessibility
Application
Start Zoom when I start Windows
When closed, minimize window to the notification area instead of the task bar
Automatically copy Invitation URL to Clipboard after meeting starts
Confirm with me when I leave a meeting
Show my connected time
Remind me 5 minutes before my upcoming meetings
Content Sharing
Use dual monitors
Enter full screen automatically when starting or joining a meeting
Enter full screen automatically when viewing screen shared by others
Maximize Zoom window automatically when viewing screen shared by others
Scale to fit my Zoom window when viewing screen shared by others
Enable screen sharing with GPU acceleration
Enable the remote control of all applications
Side-by-side Mode
Limit your screen share to 10 frames-per-second
View Advanced Features

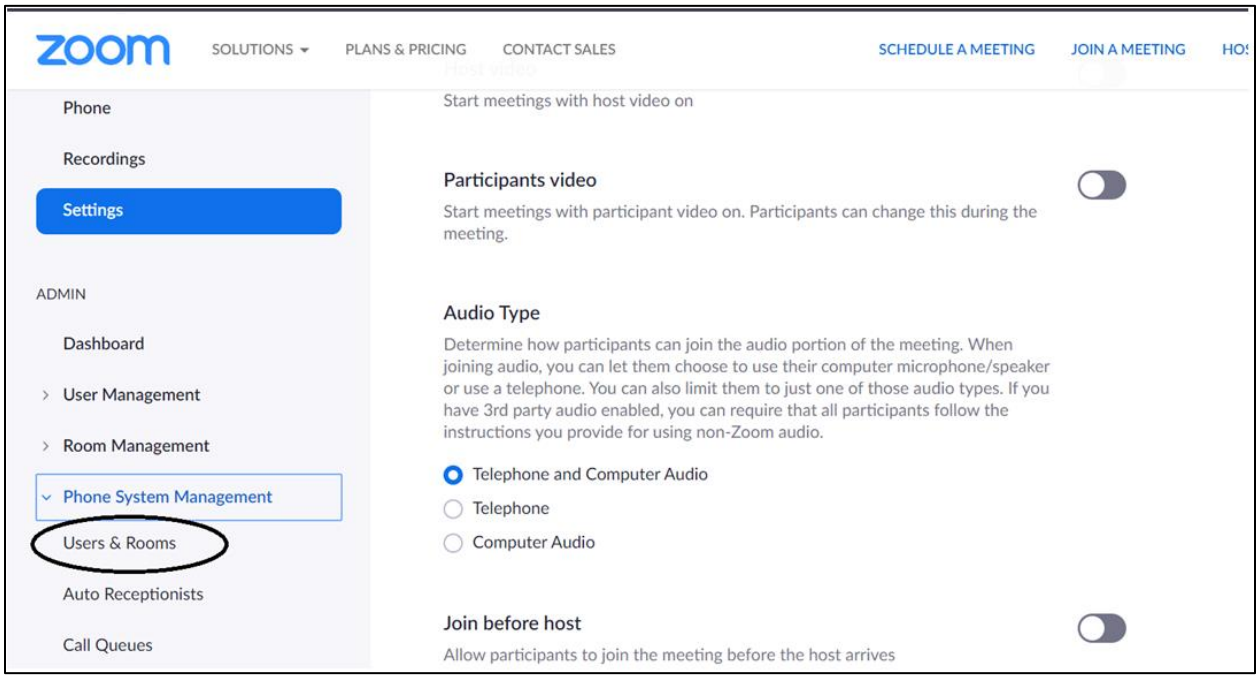

Google
Gmail
Facebook
My Settings - Zoom
zoom.us/profile/setting?mid=&from=client
JOIN THE ZOOM USER CONFERENCE ZOOMTOPIA | OCTOBER 15-16, 2019
REQUEST A DEMO
1.888.799.0125
RESOURCES
SUPPORT
zoom
SOLUTIONS
PLANS & PRICING
CONTACT SALES
SCHEDULE A MEETING
JOIN A MEETING
HOST A MEETING
SIGN OUT
PERSONAL
Profile
Meetings
Webinars
Recordings
Settings
ADMIN
Dashboard
User Management
Room Management
Meeting
Recording
Telephone
Schedule Meeting
Host video
Start meetings with host video on
Participants video
Start meetings with participant video on. Participants can change this during the meeting.
Audio Type
Determine how participants can join the audio portion of the meeting. When joining audio, you can let them choose to use their computer microphone/speaker or use a telephone. You can also limit them to just one of those audio types. If you have 3rd party audio enabled, you can require that all participants follow the
Help


Google
Gmail
Facebook
My Settings - Zoom
zoom.us/profile/setting?mid=&from=client
JOIN THE ZOOM USER CONFERENCE ZOOMTOPIA | OCTOBER 15-16, 2019
REQUEST A DEMO
1.888.799.0125
RESOURCES
SUPPORT
zoom
SOLUTIONS
PLANS & PRICING
CONTACT SALES
SCHEDULE A MEETING
JOIN A MEETING
HOST A MEETING
SIGN OUT
ADMIN
Dashboard
User Management
Room Management
Phone System Management
Account Management
Advanced
Attend Live Training
Video Tutorials
Knowledge Base
Start meetings with participant video on. Participants can change this during the meeting.
Audio Type
Determine how participants can join the audio portion of the meeting. When joining audio, you can let them choose to use their computer microphone/speaker or use a telephone. You can also limit them to just one of those audio types. If you have 3rd party audio enabled, you can require that all participants follow the instructions you provide for using non-Zoom audio.
Telephone and Computer Audio
Telephone
Computer Audio
Join before host
Allow participants to join the meeting before the host arrives
Use Personal Meeting ID (PMI) when scheduling a meeting
You can visit Personal Meeting Room to change your Personal Meeting settings.
Help

8.1. Delete the Users from “Users and Rooms” under “Phone System Management” of Admin.

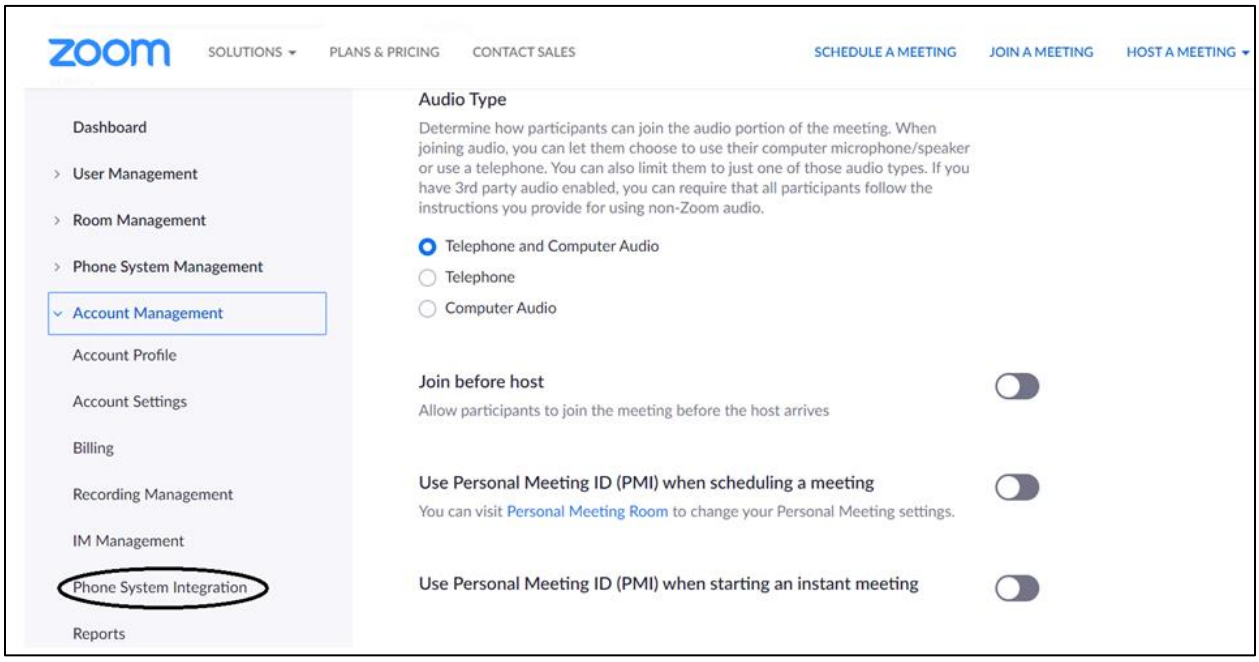
Please navigate to the above page and check whether a user is already present with the same user name that is used to login to zoom client.
If it is already there, please delete that user from Admin portal as zoom softphone will not register with CUCM as it will try to assign a DN for this user and register internally.

In our testing, we have used a user called solutionszoomuser1@outlook.com and this user should not be listed under “**Users and Rooms**” page.

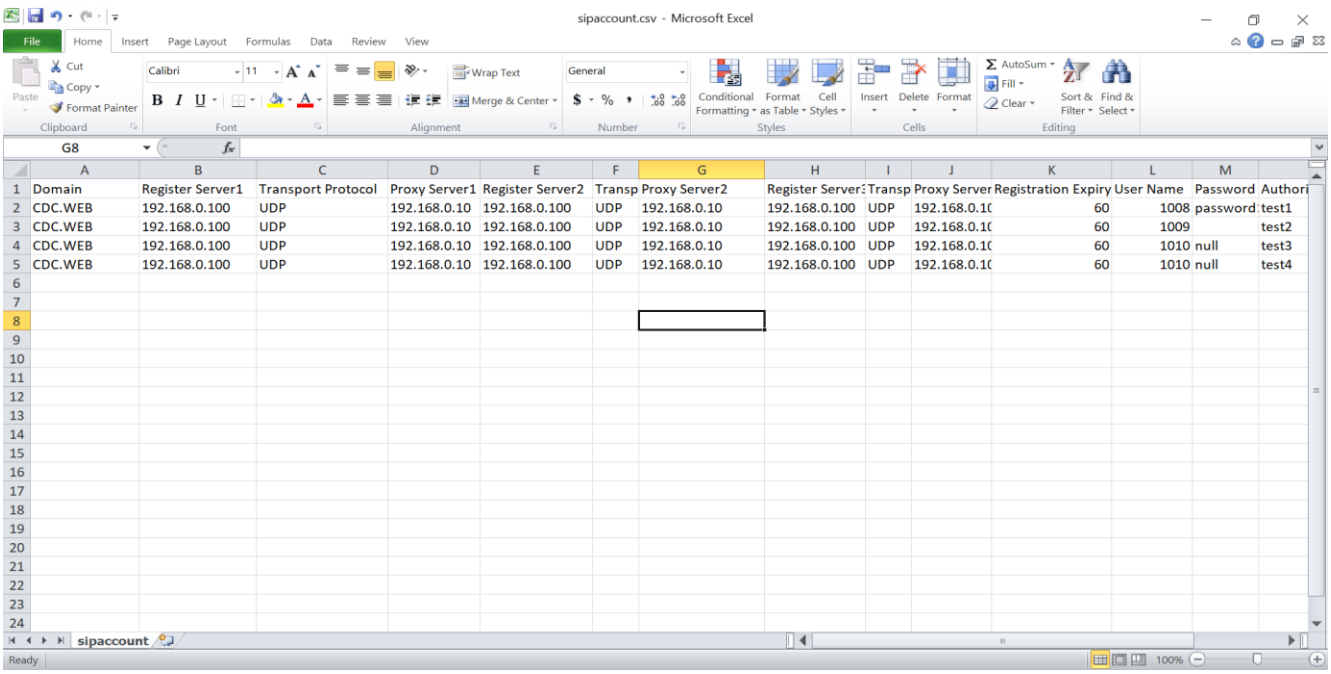


8.2. Csv File Creation for Zoom softphone in Zoom Admin portal

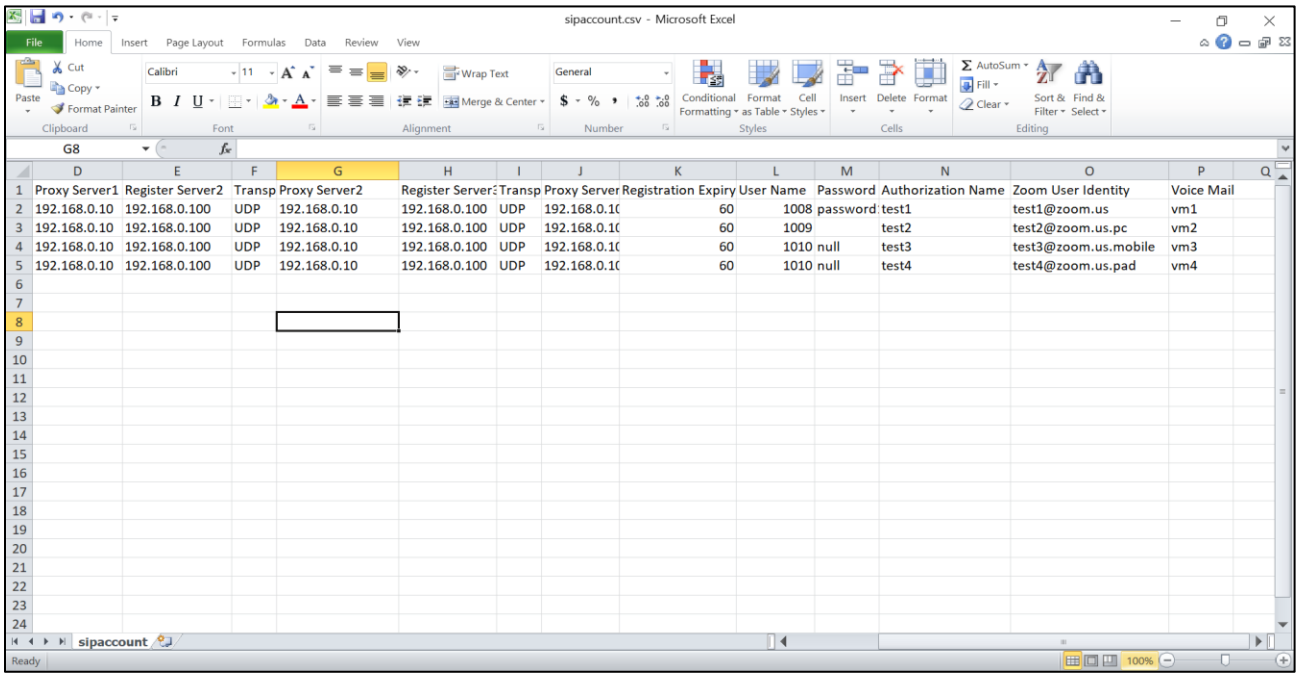
We primarily use one particular config in advanced features which is "**Phone system integration**" under "**Account Management**" of Admin. Please navigate to this page and there is an option to download a sample .csv file which we need to downloaded and used for Zoom softphones.



Once the .csv file is downloaded, the sample file looks like the below:
This sample file needs to edited according to the configuration of the particular user



	A	B	C	D	E	F	G	H	I	J	K	L	M	
1	Domain	Register Server1	Transport Protocol	Proxy Server1	Register Server2	Transp	Proxy Server2	Register Server2	Transp	Proxy Server	Registration Expiry	User Name	Password	Authori
2	CDC.WEB	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.1(	60	1008	password	test1
3	CDC.WEB	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.1(	60	1009		test2
4	CDC.WEB	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.1(	60	1010	null	test3
5	CDC.WEB	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.1(	60	1010	null	test4



Proxy Server1	Register Server2	Transp	Proxy Server2	Register Server3	Transp	Proxy Server	Registration Expiry	User Name	Password	Authorization Name	Zoom User Identity	Voice Mail
192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.1(	60	1008	password	test1	test1@zoom.us	vm1
192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.1(	60	1009		test2	test2@zoom.us.pc	vm2
192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.1(	60	1010	null	test3	test3@zoom.us.mobile	vm3
192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.1(	60	1010	null	test4	test4@zoom.us.pad	vm4

The .csv file has many entries which is given below:

- **Domain** (optional field) - Can be used to give the domain of the registrar server which is the CUCM server in our testing.
- **Registrar server IP** 1, 2 and 3 (The Registrar server 2 and 3 are used if there are multiple Registrar servers used), - Ideally CUCM server IP in our testing. We can give multiple CUCM IPs as server1, server 2 and server3 if multiple CUCM are in the network.
- **Transport Protocol** (can be UDP, TCP and AUTO)
- **Proxy server** 1, 2 and 3 (Used in case if more than one proxy servers are used) – Need to give the public IP address of the Oracle SBC's SIP Interface that is facing the Zoom side.
- **Registration expiry** which is by default set as 60 minutes,
- **User name** – Directory number created in End User section of CUCM.
- **Authorization Name** – User ID created in the End user section of CUCM
- **Password** – Password of the User ID created.
- **Zoom User Identity** – Zoom Admin User login ID and

- **Voicemail** – Voicemail number, if any

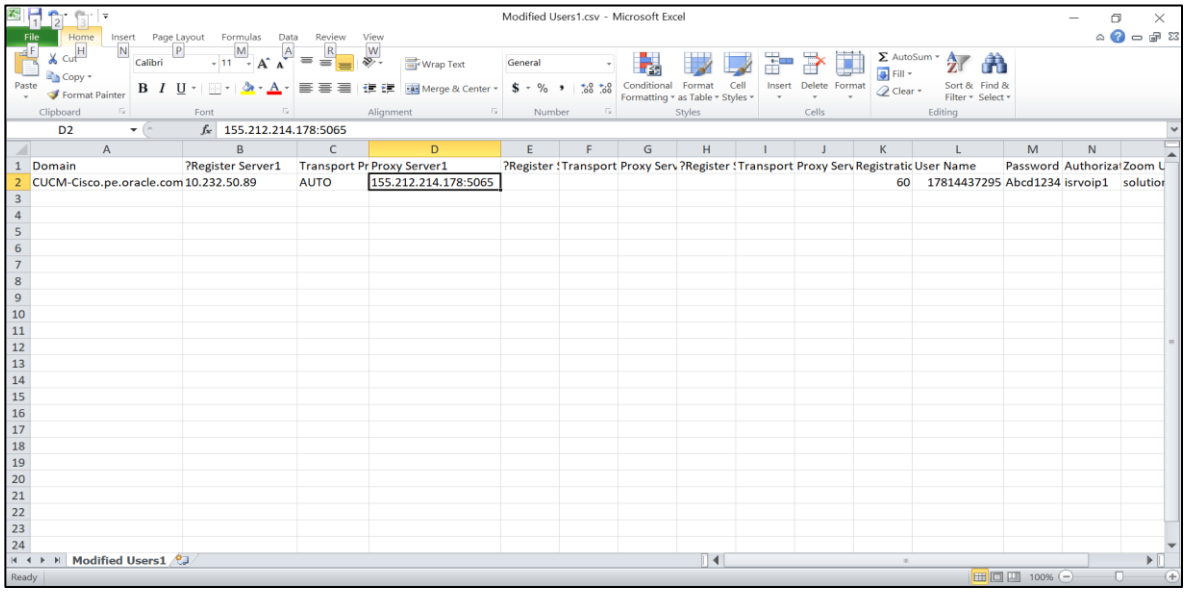
- We need to fill the details in .csv file with values that we have created already in CUCM and upload the file to zoom admin portal using "Import CSV file" option.

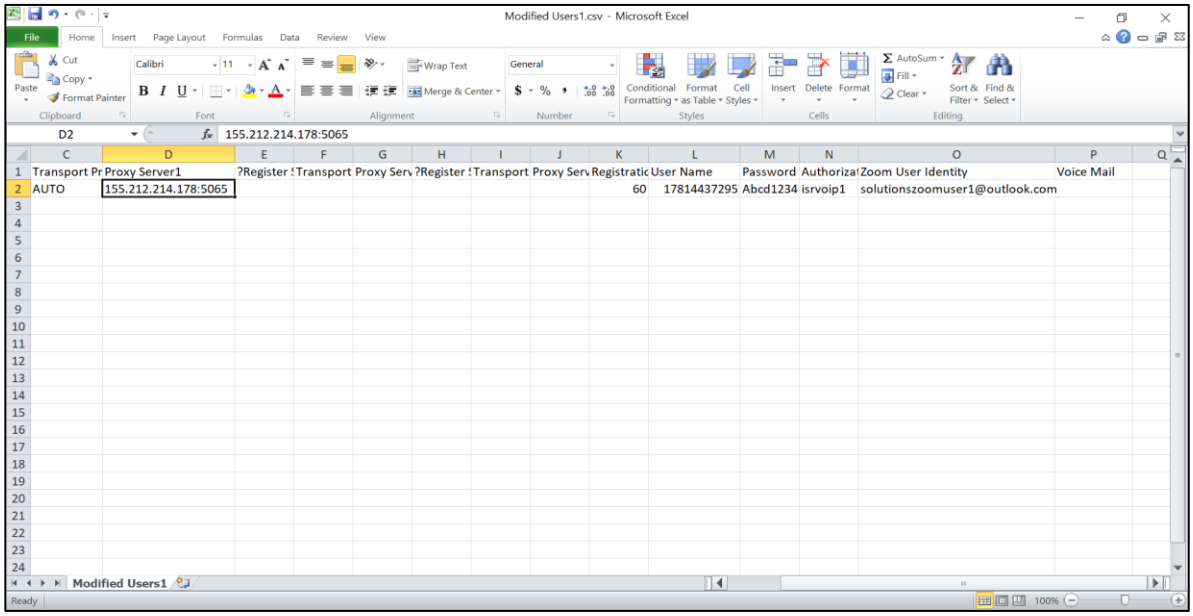
- We also use this .csv file template to do different types of zoom client registrations in CUCM (Giving CUCM IP as registrar IP and giving CUCM FQDN as registrar IP).

- When Transport protocol is set to AUTO in .csv file, the protocol can also be TLS along with TCP/UDP. When Zoom Client sends register with TLS as protocol to Oracle SBC, SBC gets it properly and sends it to CUCM with TCP protocol and zoom client is successfully registered with Cisco CUCM after that and calls also works fine.

- This scenario is tested with TLS only on access side (Zoom Client to SBC) and core side (SBC to CUCM) still works with TCP/UDP protocol.

The modified .csv file uploaded to zoom client is given below for reference:
The below .csv file indicates the registrar server details as CUCM IP address along with other details.

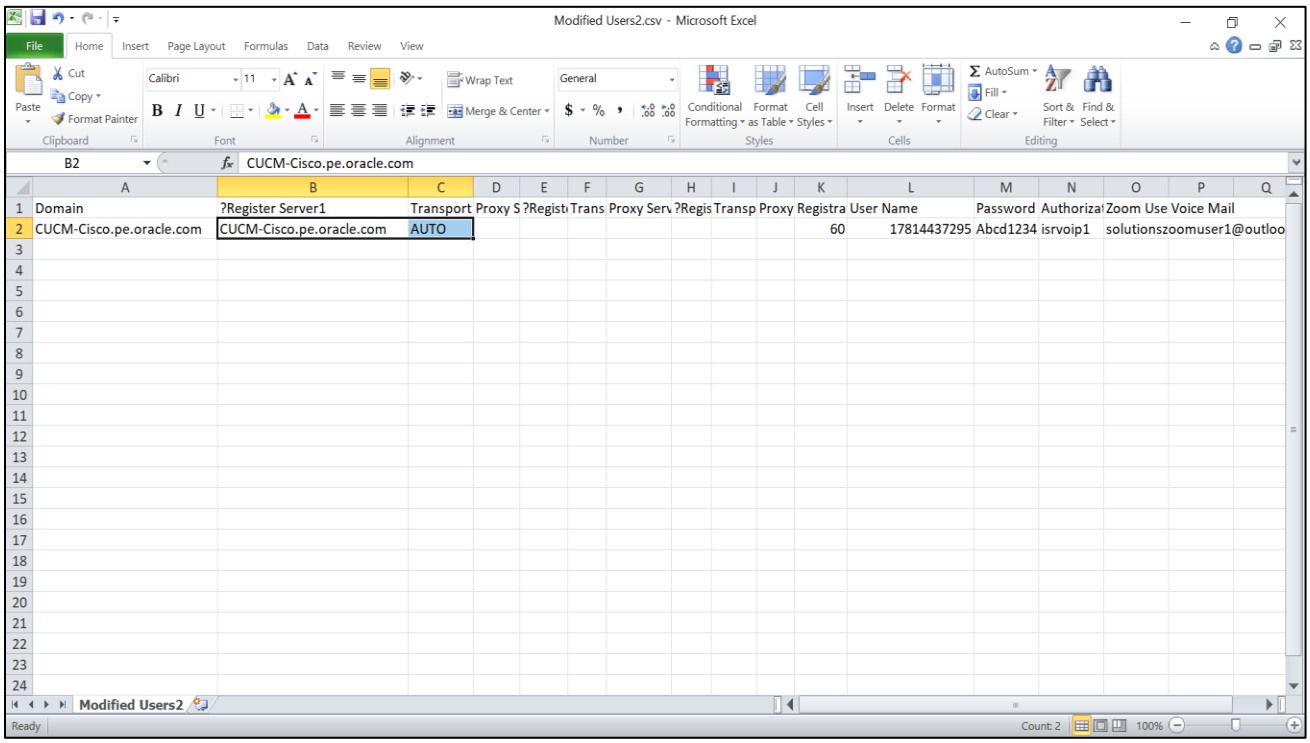




Transport Pr	Proxy Server1	?Register !	Transport	Proxy Serv	?Register !	Transport	Proxy Serv	Registratic	User Name	Password	Authoriza	Zoom User Identity	Voice Mail
AUTO	155.212.214.178:5065							60	17814437295	Abcd1234	isrvoip1	solutionszoomuser1@outlook.com	

If the customer environment has an DNS configured and if it is able to resolve the FQDN of the registrar server which is Cisco CUCM in our case, then we can specify the FDQN in the registrar server entry instead of giving IP address of the registrar server and zoom client will be able to register successfully to the CUCM. The DNS config part is anyways out of scope of this document.

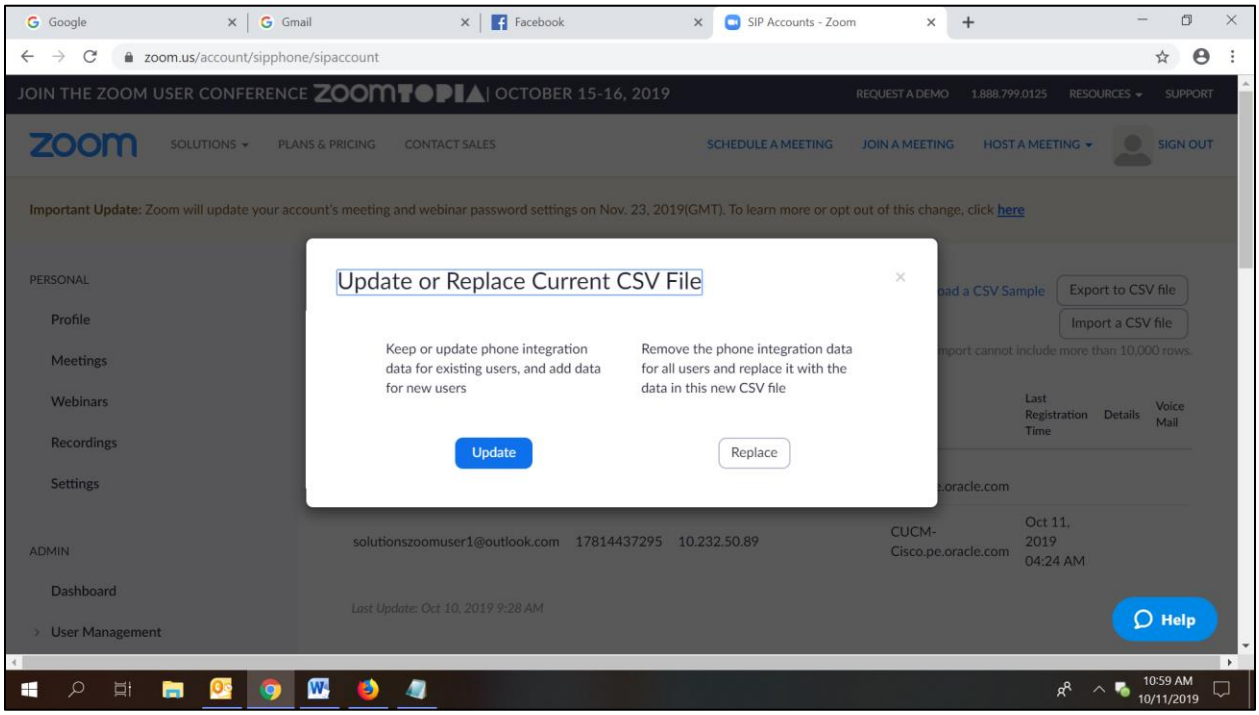
The below .csv file indicates the registrar server details as CUCM FQDN along with other details:

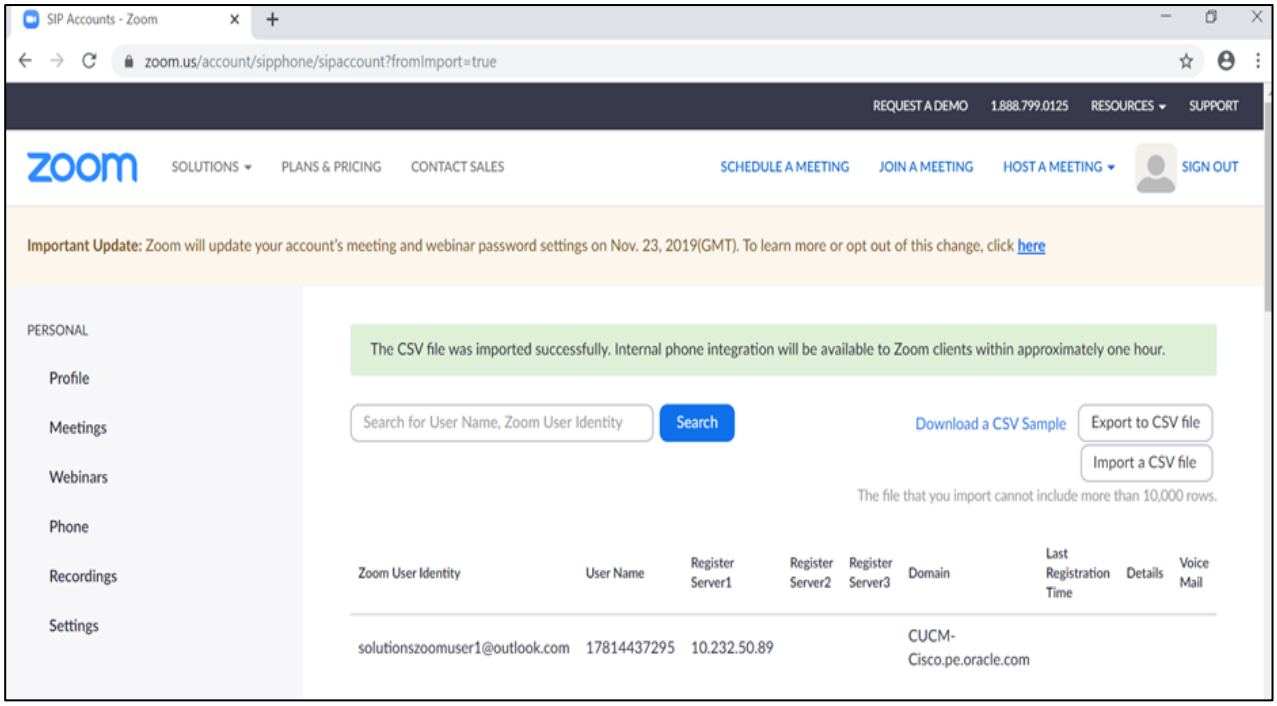


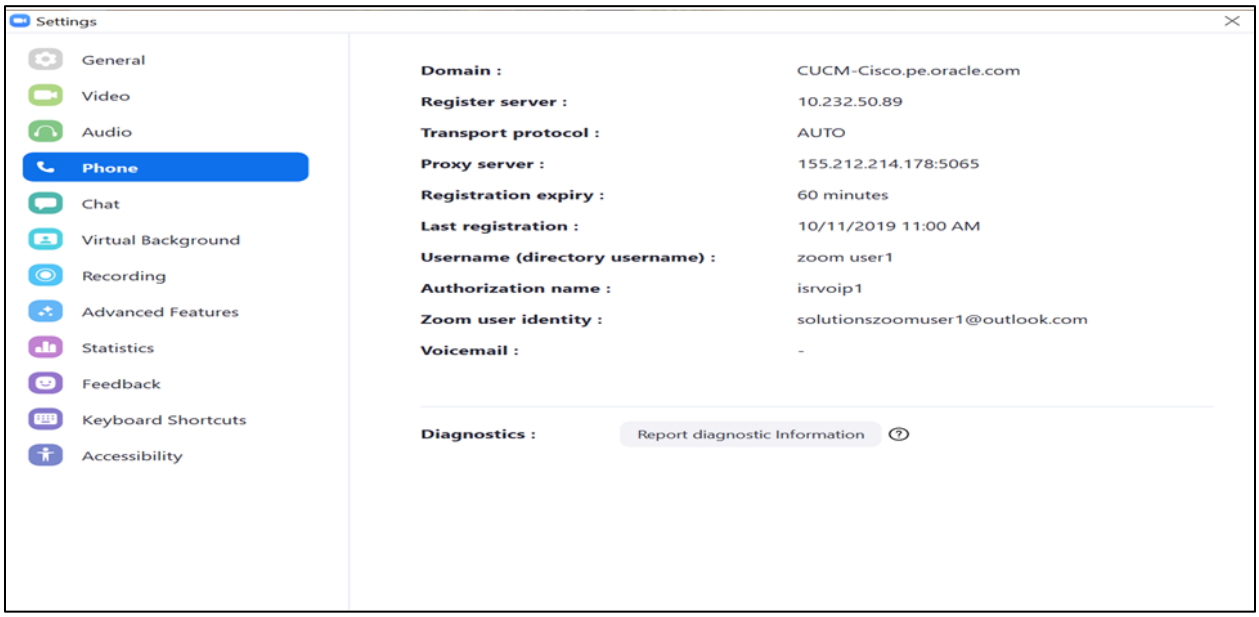
Domain	?Register Server1	Transport	Proxy S	?Regist	Trans	Proxy Serv	?Regis	Transp	Proxy	Registra	User Name	Password	Authoriza	Zoom Use	Voice Mail
CUCM-Cisco.pe.oracle.com	CUCM-Cisco.pe.oracle.com	AUTO								60	17814437295	Abcd1234	isrvoip1	solutionszoomuser1@outloo	

8.3. Csv File Upload and Registration of Zoom softphone in Admin Portal

After uploading the .csv file to the zoom Admin portal, a successful message from the portal will be displayed for the file upload and the zoom phone should be registered successfully with CUCM after this step.



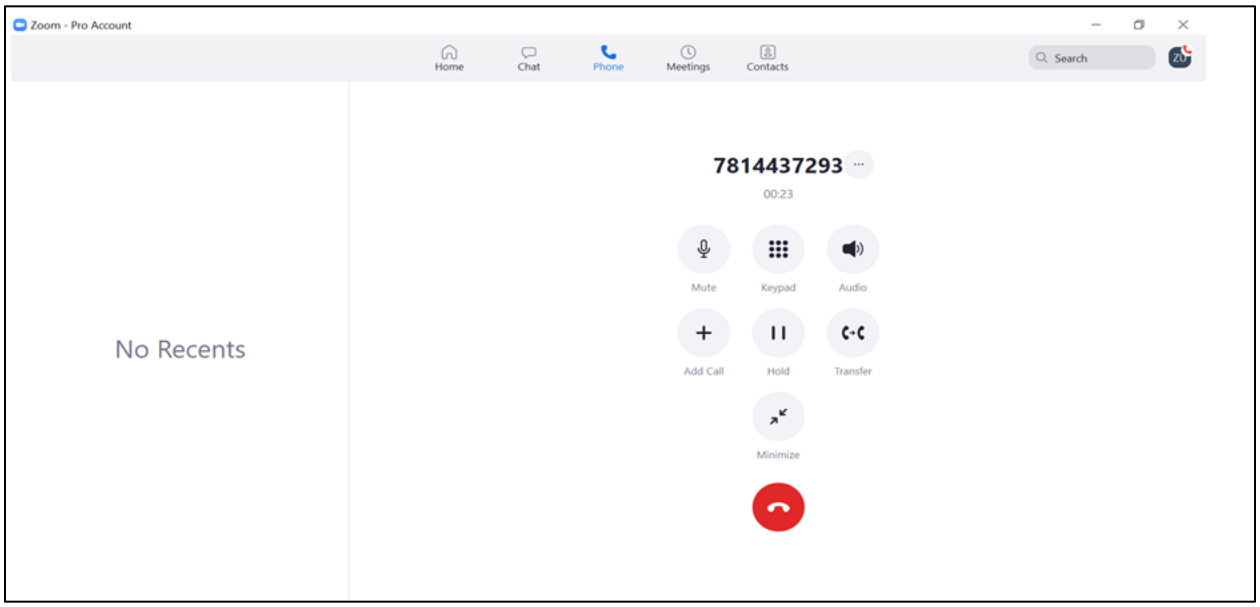


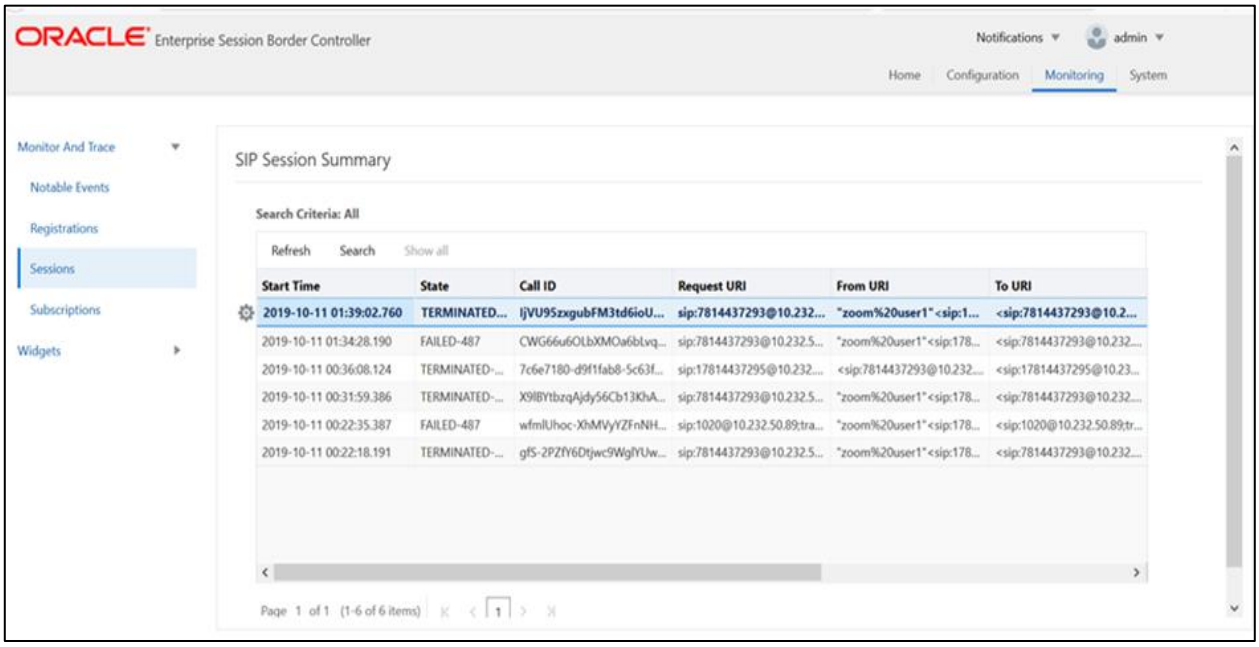

Settings
General
Video
Audio
Phone
Chat
Virtual Background
Recording
Advanced Features
Statistics
Feedback
Keyboard Shortcuts
Accessibility
Domain :
CUCM-Cisco.pe.oracle.com
Register server :
10.232.50.89
Transport protocol :
AUTO
Proxy server :
155.212.214.178:5065
Registration expiry :
60 minutes
Last registration :
10/11/2019 11:00 AM
Username (directory username) :
zoom user1
Authorization name :
isrvoip1
Zoom user identity :
solutionszoomuser1@outlook.com
Voicemail :
-
Diagnostics :
Report diagnostic Information

8.4. Calling Options from the Zoom Softphone

The zoom softphone option will also be available now and calls should be working from now on. We can check the call details from SBC GUI under Monitor and trace option.

With Zoom phone and CUCM integration, the basic calls and supplementary call features like Call Hold, Call Transfer (Consultative and Blind Transfer) and Call conference scenarios are tested and confirmed that those call flows are working fine. The executed test cases are given in the tabular format under Appendix A Section.





Appendix A

Following are the test cases that are executed as part of Zoom Client as Softphone with CUCM.

Serial Number	Test Cases Executed	Result
1	Inbound Calls to Zoom client from 3rd party Phones via CUCM	Pass
2	Outbound Calls from Zoom client from 3rd party Phones via CUCM	Pass
3	Call Hold by remote party during 2 way audio call (Incoming call to Zoom)	Pass
4	Call Hold by Zoom phone during 2 way audio call (Incoming call to Zoom)	Pass
5	Call Hold by remote party during 2 way audio call (Outgoing call from Zoom)	Pass
6	Call Hold by Zoom phone during 2 way audio call (Outgoing call from Zoom)	Pass
7	Consultative Call Transfer from Zoom phone during incoming call to Zoom from 3rd party Phones	Pass
8	Consultative Call Transfer from Zoom phone during outgoing call from Zoom from 3rd party Phones	Pass
9	Blind Call Transfer during incoming call to Zoom from 3rd party Phones	Pass
10	Blind Call Transfer during outgoing call from Zoom from 3rd party Phones	Pass
11	Conference Call Scenario with Zoom phone included	Pass
12	Do Not Disturb on Zoom Phones	Pass
13	Long Duration Call (20 Minute Phone Call)	Pass
14	DTMF (Verify RFC 2833 Packets are being sent through)	Pass
15	Direct Outward Dialing Through CUCM	Pass
16	Call Waiting	Pass
17	Transcoded call through SBC	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

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/Oracle/

twitter.com/Oracle

oracle.com

Integrated Cloud Applications & Platform Services