



ORACLE

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

Table of Contents

1. INTENDED AUDIENCE	5
2. DOCUMENT OVERVIEW	5
3. INTRODUCTION	7
3.1. AUDIENCE.....	7
3.2. REQUIREMENTS.....	7
3.3. ARCHITECTURE	8
4. CONFIGURING THE CISCO CUCM 11.5 FOR ZOOM SOFTPHONE	9
4.1. CONFIGURING THE PHONE SECURITY PROFILE FOR SIP PHONE.....	10
4.2. END USER CONFIGURATION.....	11
4.3. ADDING SIP PHONE IN CUCM	13
4.4. ASSOCIATING END USER TO PHONE	15
5. NEW SBC CONFIGURATION	16
5.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC	16
5.2. CONFIGURE SBC USING WEB GUI	19
5.3. CONFIGURE SYSTEM-CONFIG.....	22
5.4. CONFIGURE PHYSICAL INTERFACE VALUES.....	23
5.5. CONFIGURE NETWORK INTERFACE VALUES.....	24
5.6. ENABLE MEDIA MANAGER	27
5.7. CONFIGURE REALMS.....	28
5.8. ENABLE SIP-CONFIG.....	29
5.9. CONFIGURE SIP INTERFACES.....	31
5.10. CONFIGURE SESSION-AGENT	32
5.11. CONFIGURE LOCAL-POLICY	34
5.12. CONFIGURE STEERING-POOL	36
5.13. CONFIGURE SIP PORT-MAPPING	37
6. CONFIGURE SBC FOR TLS/SRTP CALLS FROM ZOOM SOFTPHONE	39
6.1. CREATING SBC END ENTITY CERTIFICATE.....	39
6.2. GENERATE CERTIFICATE SIGNING REQUEST	40
6.3. IMPORT CERTIFICATES TO SBC.....	41
6.4. CREATING TLS PROFILE.....	42
6.5. CONFIGURE SDES PROFILE.....	43
6.6. CONFIGURE MEDIA SECURITY PROFILE	44
6.7. CONFIGURE REALMS.....	45
6.8. CONFIGURE SIP INTERFACES.....	47
6.9. CONFIGURE SESSION-AGENT	48
PLEASE CONFIGURE THE SESSION AGENT FOR CUCM SIDE AS BELOW	48
6.10. CONFIGURE LOCAL-POLICY	49
6.11. CONFIGURE STEERING-POOL	51
6.12. DELAYED OFFER TESTING FROM CISCO CUCM TO ZOOM CLIENT	52
7. EXISTING SBC CONFIGURATION.....	52
8. CONFIGURING THE ZOOM SOFTPHONE IN ADMIN PORTAL	53
8.1. DELETE THE USERS FROM “USERS AND ROOMS” UNDER “PHONE SYSTEM MANAGEMENT” OF ADMIN.....	56
8.2. CSV FILE CREATION FOR ZOOM SOFTPHONE IN ZOOM ADMIN PORTAL	57
8.3. CSV FILE UPLOAD AND REGISTRATION OF ZOOM SOFTPHONE IN ADMIN PORTAL.....	61



8.4. CALLING OPTIONS FROM THE ZOOM SOFTPHONE..... 63

APPENDIX A..... 64



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.

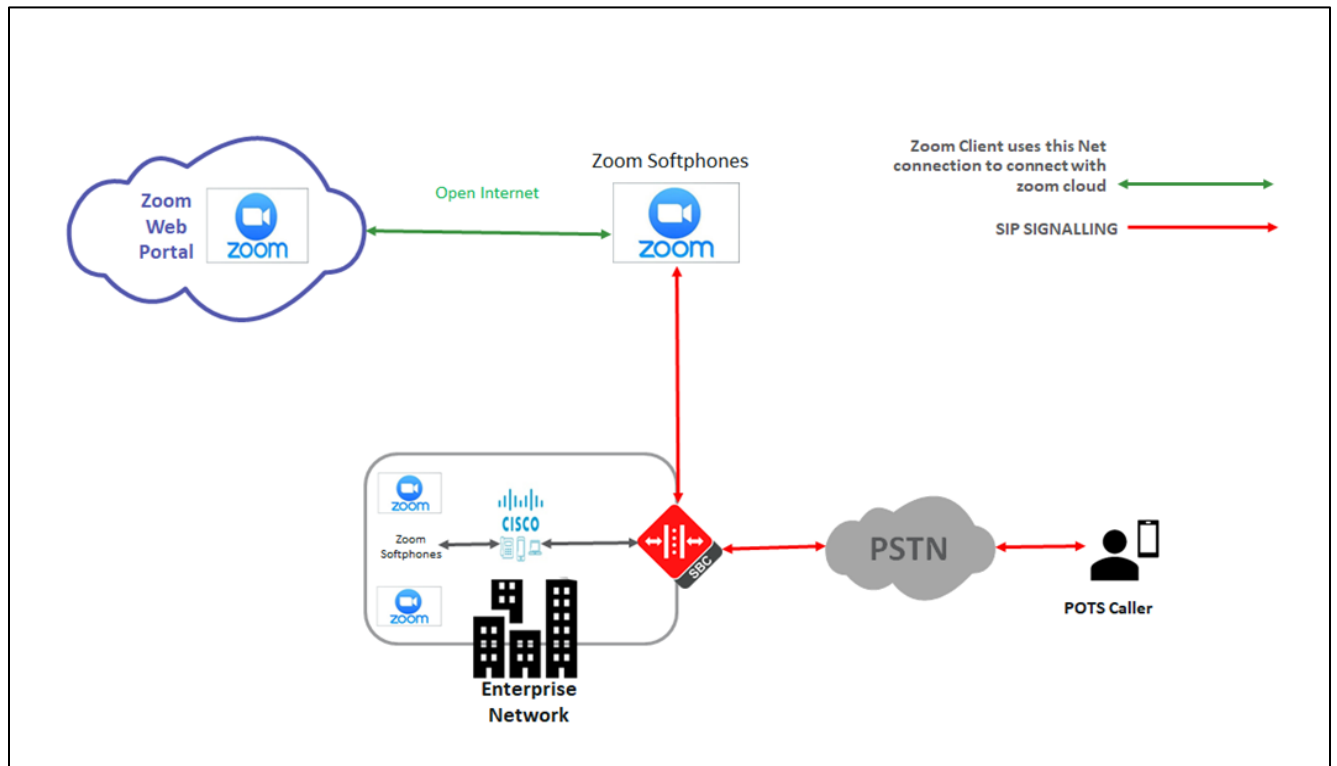
3.2. Requirements

- 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.

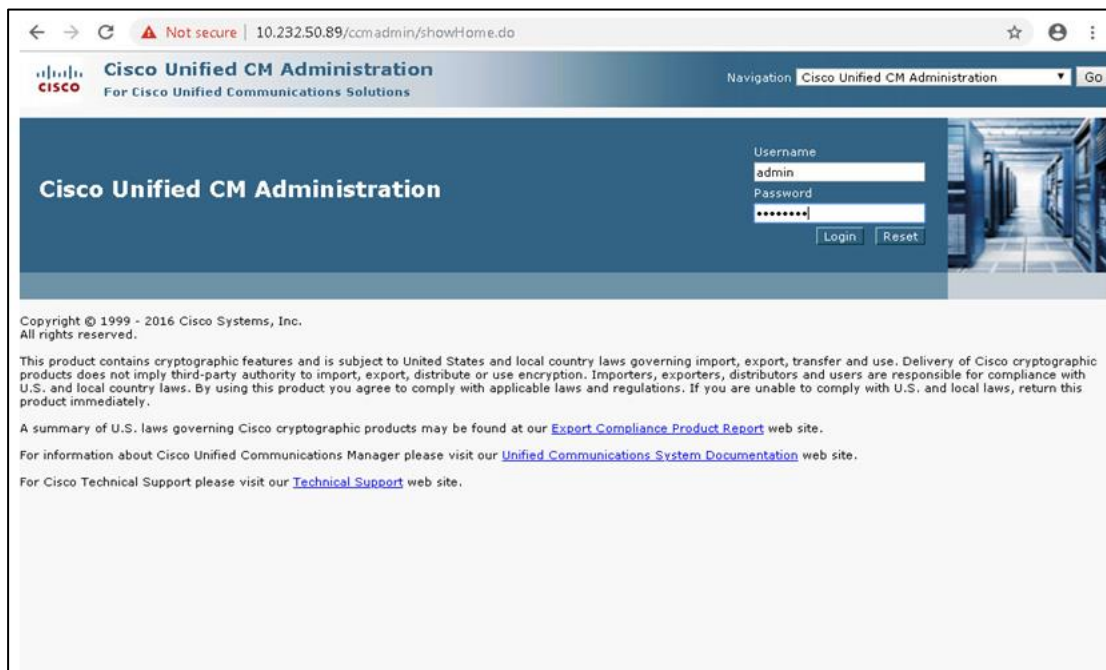
<https://support.zoom.us/hc/en-us/articles/215537603-Zoom-Rooms-PBX-Support>

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.



The screenshot shows the Cisco Unified CM Administration web interface. The browser address bar displays "10.232.50.89/ccnadmin/showHome.do". The page header includes the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions". A navigation menu shows "Cisco Unified CM Administration" selected. The main content area features a login form with fields for "Username" (containing "admin") and "Password" (masked with asterisks), and "Login" and "Reset" buttons. Below the login form, there is a copyright notice for 1999-2016 Cisco Systems, Inc., and several paragraphs of legal disclaimers regarding cryptographic features and compliance with U.S. and local laws.

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.

The screenshot shows the Cisco Unified CM Administration interface for configuring a Phone Security Profile. The browser address bar indicates the URL: 10.232.50.89/ccadmin/phoneSecurityProfileEdit.do?key=e1764ab7-e94b-4f53-96a7-0c190e4d3b48. The page title is "Phone Security Profile Configuration".

Status: Ready

Phone Security Profile Information:

- Product Type: Third-party SIP Device (Basic)
- Device Protocol: SIP
- Name*: Third-party SIP Device Basic - Standard SIP Non-Secure Profile
- Description: Third-party SIP Device (Basic) - Standard SIP Non-Secure Profile
- Nonce Validity Time*: 600
- Transport Type*: TCP+UDP
- Enable Digest Authentication

Parameters used in Phone:

- SIP Phone Port*: 5060

Buttons: Copy, Reset, Apply Config, Add New

*- indicates required item.

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)

The screenshot displays the Cisco Unified CM Administration interface for End User Configuration. The page title is "End User Configuration" and it includes a "Related Links" section with "Back to Find List Users" and "Go". The main content area is divided into sections: "Status" (Ready) and "User Information". The "User Information" section contains the following fields and values:

User Status	Enabled Local User
User ID*	isrvoip1
Password
Confirm Password
Self-Service User ID	17814437295
PIN
Confirm PIN
Last name*	isrvoip1
Middle name	
First name	
Display name	
Title	
Directory URI	
Telephone Number	17814437295
Home Number	
Mobile Number	
Pager Number	

The interface also shows a navigation menu at the top, a "Save" button, and a "Delete" button. The system tray at the bottom indicates the time is 2:12 AM on 10/9/2019.

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.

The screenshot displays the Cisco Unified CM Administration web interface for configuring a SIP device. The browser address bar shows the URL: 10.232.50.89/ccmadmin/phoneEdit.do?key=8bf8be42-2252-11f3-f6b9-e853b66cc0d7. The page title is "Cisco Unified CM Administration" and the user is logged in as "admin".

The main configuration area is titled "Phone Configuration" and includes a toolbar with the following actions: Save, Delete, Copy, Reset, Apply Config, and Add New. The status is "Ready".

The configuration is divided into several sections:

- Association:** Shows two lines associated with the device:
 - Line [1] - 17814437295 (no partition)
 - Line [2] - Add a new DN
- Phone Type:** Product Type: Third-party SIP Device (Basic); Device Protocol: SIP
- Real-time Device Status:** Registration: Unknown; IPv4 Address: None
- Device Information:**
 - Device is Active (checked)
 - Device is not trusted (warning icon)
 - MAC Address*: 000C296352B3
 - Description: ISRVoip1
 - Device Pool*: Default
 - Common Device Configuration: < None >
 - Phone Button Template*: Third-party SIP Device (Basic)
 - Common Phone Profile*: Standard Common Phone Profile
 - Calling Search Space: < None >
 - AAR Calling Search Space: < None >

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

Owner
 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

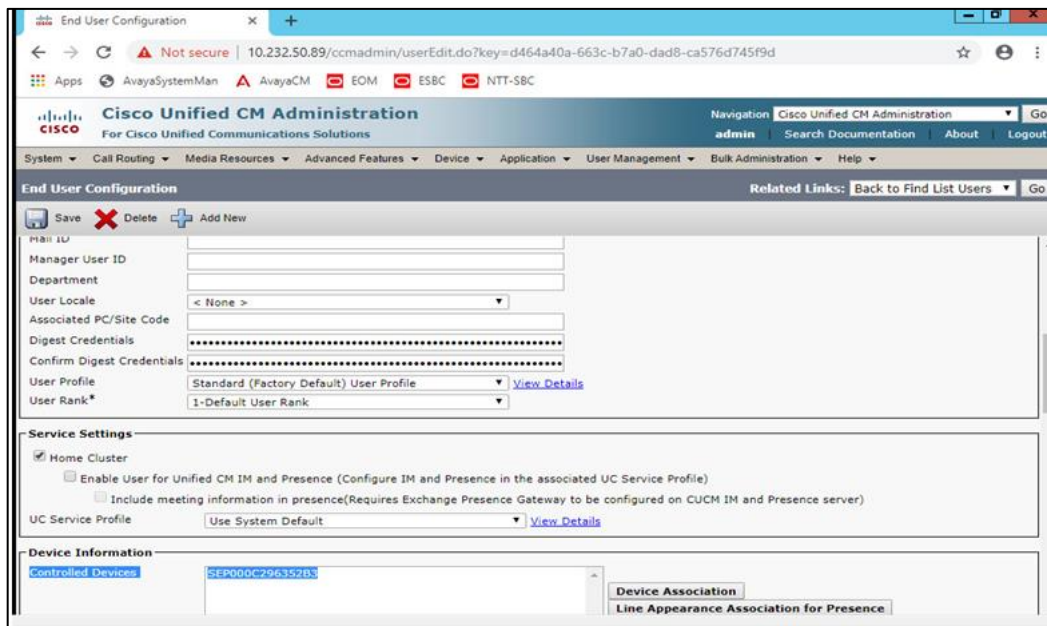
MLPP and Confidential Access Level Information

MLPP Domain: < None >
 Confidential Access Mode: < None >

Name: Tarc

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.



The screenshot displays the Cisco Unified CM Administration web interface for configuring an end user. The page is titled "End User Configuration" and includes the following sections:

- User Details:** Fields for First Name (FN), Manager User ID, Department, User Locale (set to "< None >"), Associated PC/Site Code, Digest Credentials, Confirm Digest Credentials, User Profile (Standard (Factory Default) User Profile), and User Rank* (1-Default User Rank).
- Service Settings:** Includes checkboxes for "Home Cluster", "Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)", and "Include meeting information in presence (Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)". The UC Service Profile is set to "Use System Default".
- Device Information:** A section titled "Controlled Devices" with a list containing the device ID "SEP000C796352B". A "Device Association" button is visible next to the device list.

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

```
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 tIPTd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tTscfd...
Starting tAppWeb...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Starting tIFMIBd...
Start platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...
password secure mode is enabled
Admin Security is disabled
Starting SSH...
SSH Cli init: allocated memory for 5 connections
```

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
1  Transcode Codec SILK Capacity (0-102375) : 50
2
3 Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
4 SAVE SUCCEEDED
5
6 PE-6300-1#
7 PE-6300-1#
8
9 PE-6300-1#
1 PE-6300-1# reboot
1

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.

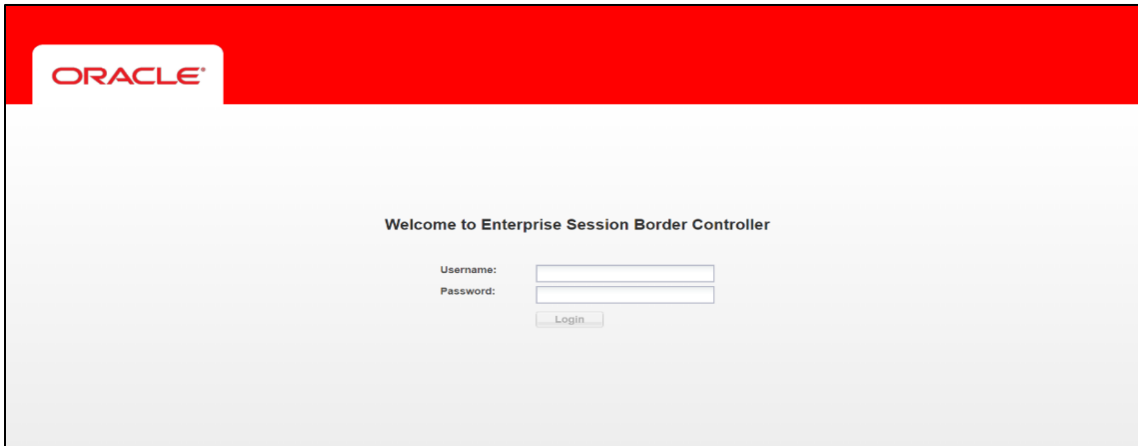
```
PE-6300-1(web-server-config)#
PE-6300-1(web-server-config)# state enabled
PE-6300-1(web-server-config)# done
web-server-config
state                               enabled
inactivity-timeout                  5
http-state                           enabled
http-port                            80
https-state                          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
```

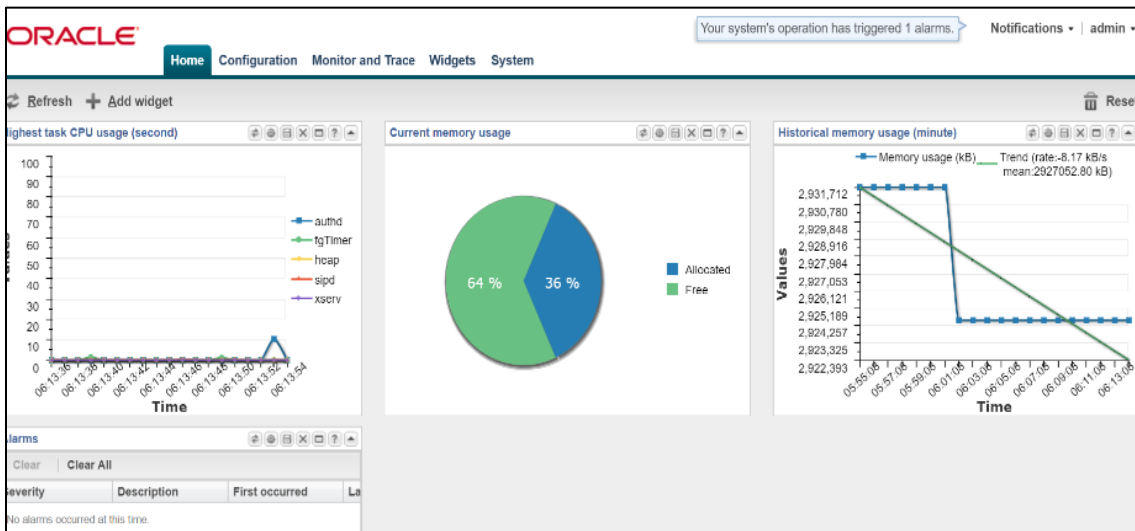
5.2. Configure SBC using Web GUI

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

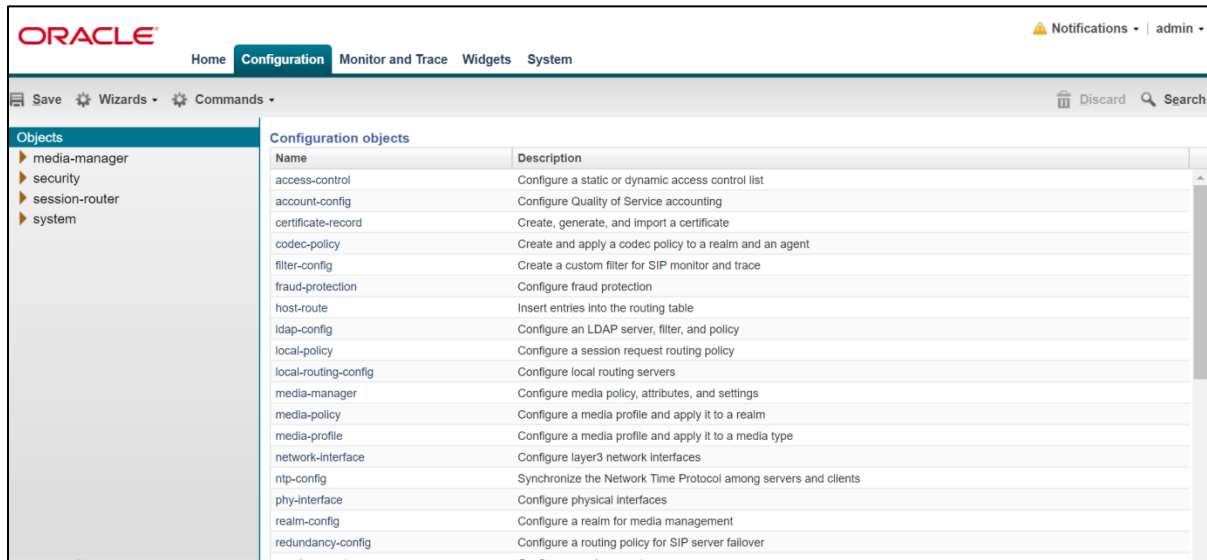
The Web GUI can be accessed through the url https://<SBC_MGMT_IP>.



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

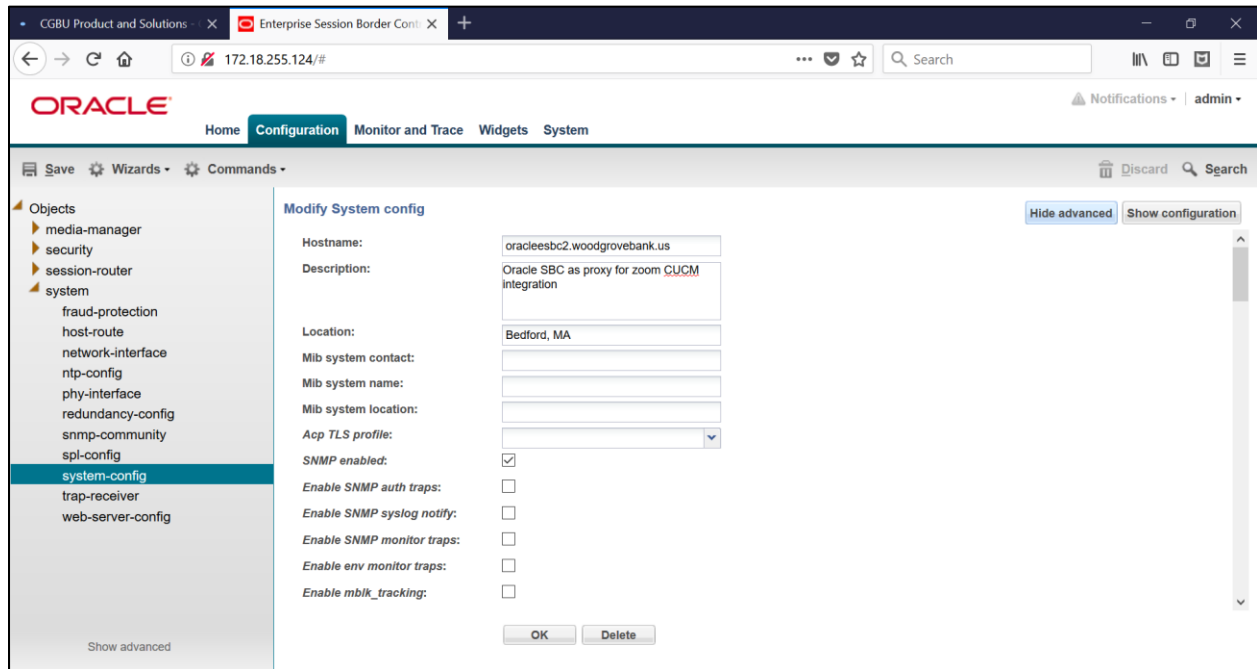
https://docs.oracle.com/cd/F13782_01/doc/esbc_scz830_webgui.pdf for more information

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

The screenshot shows the 'Modify Phy interface' configuration window in the Oracle Configuration Assistant. The interface includes a left-hand navigation pane with a tree view of system objects, where 'phy-interface' is selected. The main configuration area contains the following fields and values:

- Name:** s0p0
- Operation type:** Media
- Port:** 0 (Range: 0..5)
- Slot:** 0 (Range: 0..2)
- Virtual mac:** (empty field)
- Admin state:**
- Auto negotiation:**
- Duplex mode:** FULL
- Speed:** 100
- Wancom health score:** 50 (Range: 0..100)

Buttons for 'OK' and 'Back' are visible at the bottom of the dialog.

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		

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

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 Control - 172.18.255.124/#

ORACLE 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

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 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

DNS IP backup1:

DNS domain:

HIP IP list:

Add Edit Delete

10.232.50.201

ICMP address:

Add Edit Delete

10.232.50.201

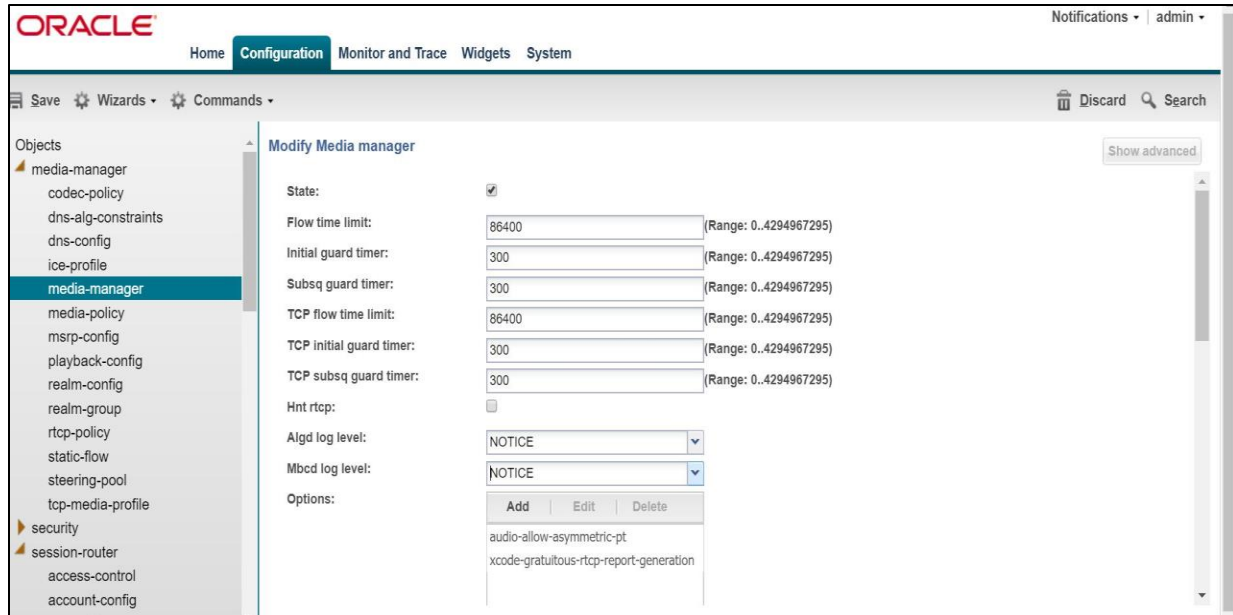
OK Back

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-assymmetric-pt
xcode-gratutious-rtcp-report-generation

Go to Media-Manager->Media-Manager



The screenshot displays the Oracle SBC configuration interface. The top navigation bar includes 'ORACLE', 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a tree view shows the 'media-manager' object selected. The main area is titled 'Modify Media manager' and contains the following settings:

- State:
- 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:
- AlgD log level: NOTICE
- Mbcd log level: NOTICE
- Options: Add | Edit | Delete

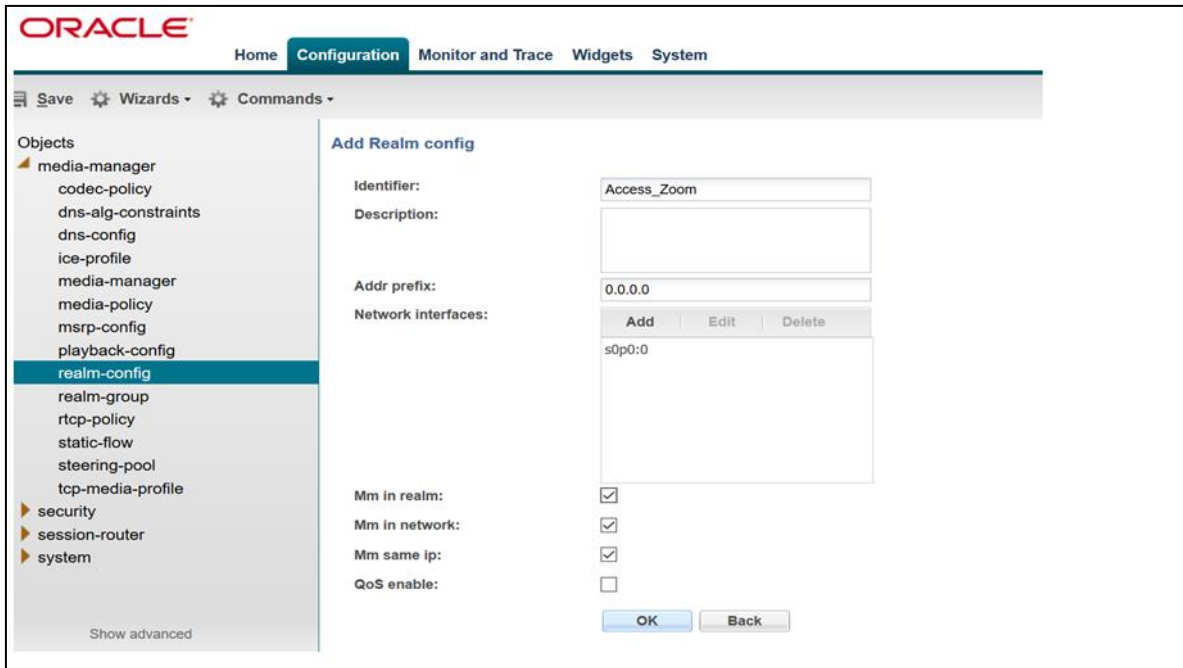
Under the 'Options' section, the following options are listed:

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

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)

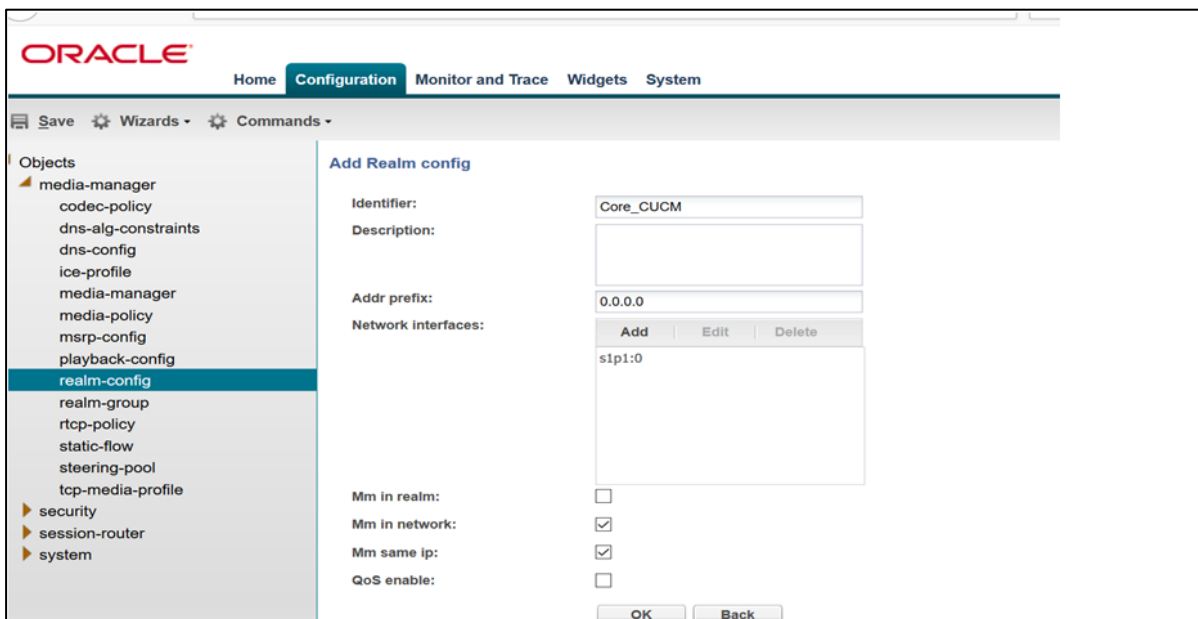


The screenshot shows the Oracle Configuration Manager interface. The 'Configuration' tab is active. In the left-hand 'Objects' tree, 'realm-config' is selected under the 'media-manager' folder. The main area displays the 'Add Realm config' dialog with the following fields and options:

- Identifier: Access_Zoom
- Description: (empty)
- Addr prefix: 0.0.0.0
- Network interfaces: s0p0:0 (with 'Add', 'Edit', and 'Delete' buttons)
- Mm in realm:
- Mm in network:
- Mm same ip:
- QoS enable:

Buttons for 'OK' and 'Back' are at the bottom.

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



The screenshot shows the Oracle Configuration Manager interface. The 'Configuration' tab is active. In the left-hand 'Objects' tree, 'realm-config' is selected under the 'media-manager' folder. The main area displays the 'Add Realm config' dialog with the following fields and options:

- Identifier: Core_CUCM
- Description: (empty)
- Addr prefix: 0.0.0.0
- Network interfaces: s1p1:0 (with 'Add', 'Edit', and 'Delete' buttons)
- Mm in realm:
- Mm in network:
- Mm same ip:
- QoS enable:

Buttons for 'OK' and 'Back' are at the bottom.

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)

The screenshot shows the Oracle Configuration interface for the 'Modify SIP config' page. The left sidebar contains a tree view of configuration categories, with 'sip-config' selected. The main area displays various configuration fields:

- State:
- Dialog transparency:
- Home Realm ID: Access_Zoom (dropdown)
- Egress Realm ID: (empty dropdown)
- Nat mode: None (dropdown)
- 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

Buttons for 'OK' and 'Delete' are visible at the bottom.

This screenshot shows the 'Options' section of the 'Modify SIP config' page. The 'Options' field is expanded to show a list of configuration options:

- Session max life limit: 0
- Enforcement profile: (empty dropdown)
- Red max trans: 10000 (Range: 0..50000)
- Options: A list containing:
 - 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)
- Registrar use for in:

Buttons for 'Add', 'Edit', and 'Delete' are visible above the options list. 'OK' and 'Delete' buttons are at the bottom.

ORACLE Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands

- media-profile
- 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

- media-profile
- 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)

Registrar use for in:

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.

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 interface

State:

Realm ID: Access_Zoom

Description:

SIP ports

Add	Edit	Copy	Delete	Address	Port	Transport protocol	TLS profile	Allow anonymous
				155.212.214.178	5065	UDP		registered
				155.212.214.178	5060	TCP		registered

Initial inv trans expire: 0 (Range: 0..99999999)

Session max life limit: 0

Proxy mode:

OK Back

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 interface

session max life limit: 0

Proxy mode: always

Redirect action: always

Nat traversal: always

Nat interval: 30 (Range: 0..4294967295)

TCP nat interval: 90 (Range: 0..4294967295)

Registration caching:

Min reg expire: 300 (Range: 0..99999999)

Registration interval: 3600 (Range: 0..4294967295)

Route to registrar:

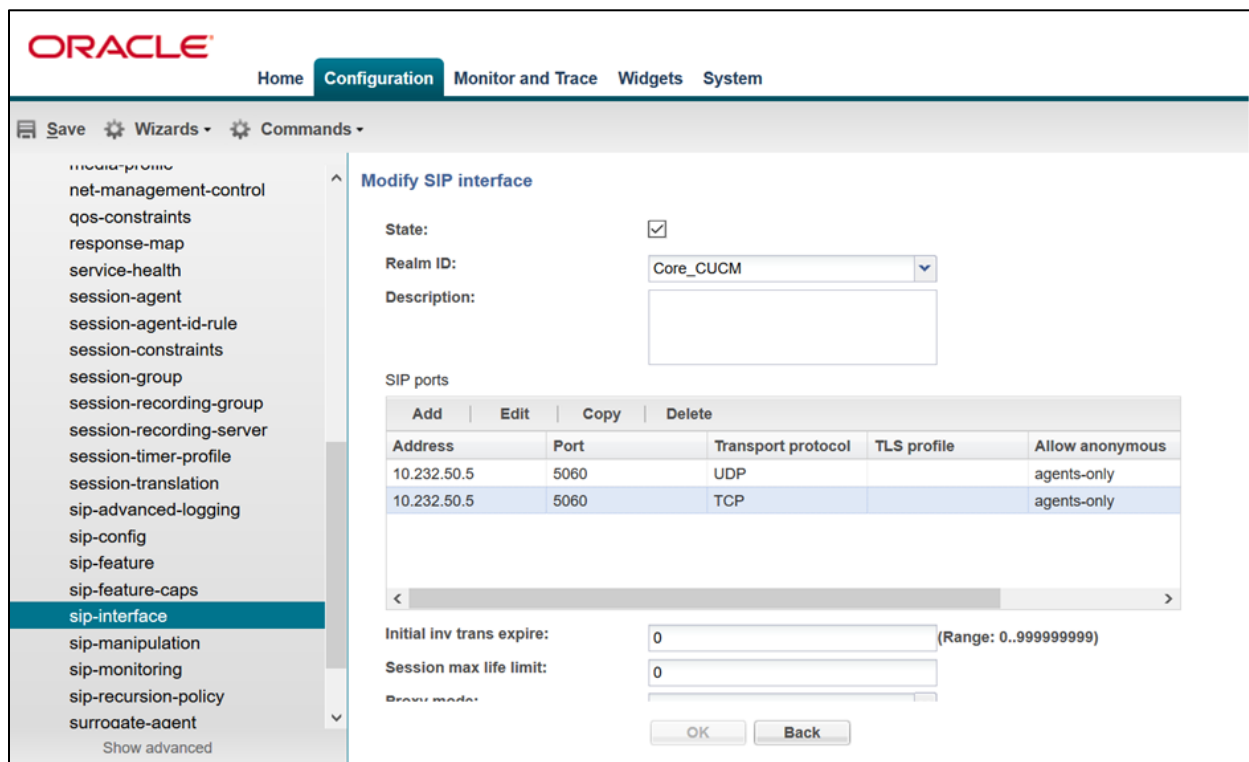
Secured network:

Uri fqdn domain:

Options: Add Edit Delete

OK Back

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”

← → ↻ 🔒 Nct secure | 10.232.50.89/ccmadmin/serviceParamEd.t.do?service=11&showall=false ☆ ⌵ ⋮

Cisco Unified CM Administration For Cisco Unified Communications Solutions Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

Enterprise Parameters Configuration

Save Set to Default Reset Apply Config

Syncing Mode for Enterprise Groups * Differential Sync Differential Sync

Service Manager TCP ports parameters

Service Manager TCP Server communication port number 8883 8888
Service Manager TCP Client communication port number 8882 8889

CRS Application Parameters

Auto Attendant Installed * false
PCC 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.

The screenshot shows the Oracle Configuration Manager interface. The 'Configuration' tab is active. In the left-hand 'Objects' tree, 'session-router' is expanded, and 'local-policy' is selected. The main area displays the 'Add Local policy' dialog box. It contains three sections: 'To address:' with an empty list and 'Add', 'Edit', and 'Delete' buttons; 'Source realm:' with a list containing 'Access_Zoom' and 'Add', 'Edit', and 'Delete' buttons; and a 'Description:' text field. 'OK' and 'Back' buttons are at the bottom.

The screenshot shows the Oracle Configuration Manager interface. The 'Configuration' tab is active. In the left-hand 'Objects' tree, 'session-router' is expanded, and 'local-policy' is selected. The main area displays the 'Add Local policy / policy attribute' dialog box. It contains several fields: 'Next hop:' (CUCM-Cisco.pe.oracle.com), 'Realm:' (Core_CUCM), 'Action:' (none), 'Terminate recursion:' (checkbox), 'Cost:' (0, Range: 0..99999999), 'State:' (checked checkbox), 'App protocol:' (dropdown), 'Lookup:' (single), and 'Next key:' (text field). 'OK' and 'Back' buttons are at the bottom.

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

ORACLE

Home Configuration Monitor and Trace Widgets System

Save Wizards Commands

Objects

- media-manager
- security
- session-router
 - access-control
 - account-config
 - account-group
 - allowed-elements-profile
 - class-profile
 - 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

Show advanced

Add Local policy

From address: Add Edit Delete

To address: Add Edit Delete

Source realm: Add Edit Delete

OK Back

ORACLE

Home Configuration Monitor and Trace Widgets System

Save Wizards Commands

Objects

- media-manager
- security
- session-router
 - access-control
 - account-config
 - account-group
 - allowed-elements-profile
 - class-profile
 - 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

Show advanced

Add Local policy / policy attribute

Next hop: ▼

Realm: ▼

Action: ▼

Terminate recursion:

Cost: (Range: 0..999999999)

State:

App protocol: ▼

Lookup: ▼

Next key:

OK Back

5.12. Configure steering-pool

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

The screenshot shows the Oracle configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this is a toolbar with 'Save', 'Wizards', and 'Commands'. On the left, a tree view under 'Objects' lists various configuration items, with 'steering-pool' selected. The main area is titled 'Add Steering pool' and contains the following fields:

IP address:	<input type="text" value="155.212.214.178"/>
Start port:	<input type="text" value="32000"/> (Range: 1..65535)
End port:	<input type="text" value="34000"/> (Range: 1..65535)
Realm ID:	<input type="text" value="Access_Zoom"/>
Network interface:	<input type="text"/>

At the bottom of the form are 'OK' and 'Back' buttons. A 'Show advanced' link is located at the bottom left of the main area.

The screenshot shows the Oracle configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this is a toolbar with 'Save', 'Wizards', and 'Commands'. On the left, a tree view under 'Objects' lists various configuration items, with 'steering-pool' selected. The main area is titled 'Add Steering pool' and contains the following fields:

IP address:	<input type="text" value="10.232.50.5"/>
Start port:	<input type="text" value="36000"/> (Range: 1..65535)
End port:	<input type="text" value="38000"/> (Range: 1..65535)
Realm ID:	<input type="text" value="Core_CUCM"/>
Network interface:	<input type="text"/>

At the bottom of the form are 'OK' and 'Back' buttons. A 'Show advanced' link is located at the bottom left of the main area.

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

The screenshot shows the Oracle SBC configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this is a toolbar with 'Save', 'Wizards', and 'Commands'. A left sidebar lists various configuration categories, with 'sip-interface' selected and highlighted. The main content area is titled 'Modify SIP interface' and contains several configuration fields. The 'Options:' field is circled and contains 'tcp-port-mapping'. Below it are fields for 'Spl options:', 'Trust mode:' (set to 'all'), 'Max nat interval:' (set to 3600), 'Stop recurse:' (set to 401,407), 'Port map start:' (set to 8000), and 'Port map end:' (set to 8100). The 'Port map start' and 'Port map end' fields are also circled. There are also fields for 'In manipulationid:', 'Out manipulationid:', and 'SIP atcf feature:'. At the bottom right, there are 'OK' and 'Back' buttons.

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.

The screenshot shows the Cisco Unified CM Administration interface. The main content area is titled "Find and List Phones" and contains a table of phone records. The table has columns for phone name, description, status, protocol, device type, and IP address. Two rows are circled in black to highlight specific information.

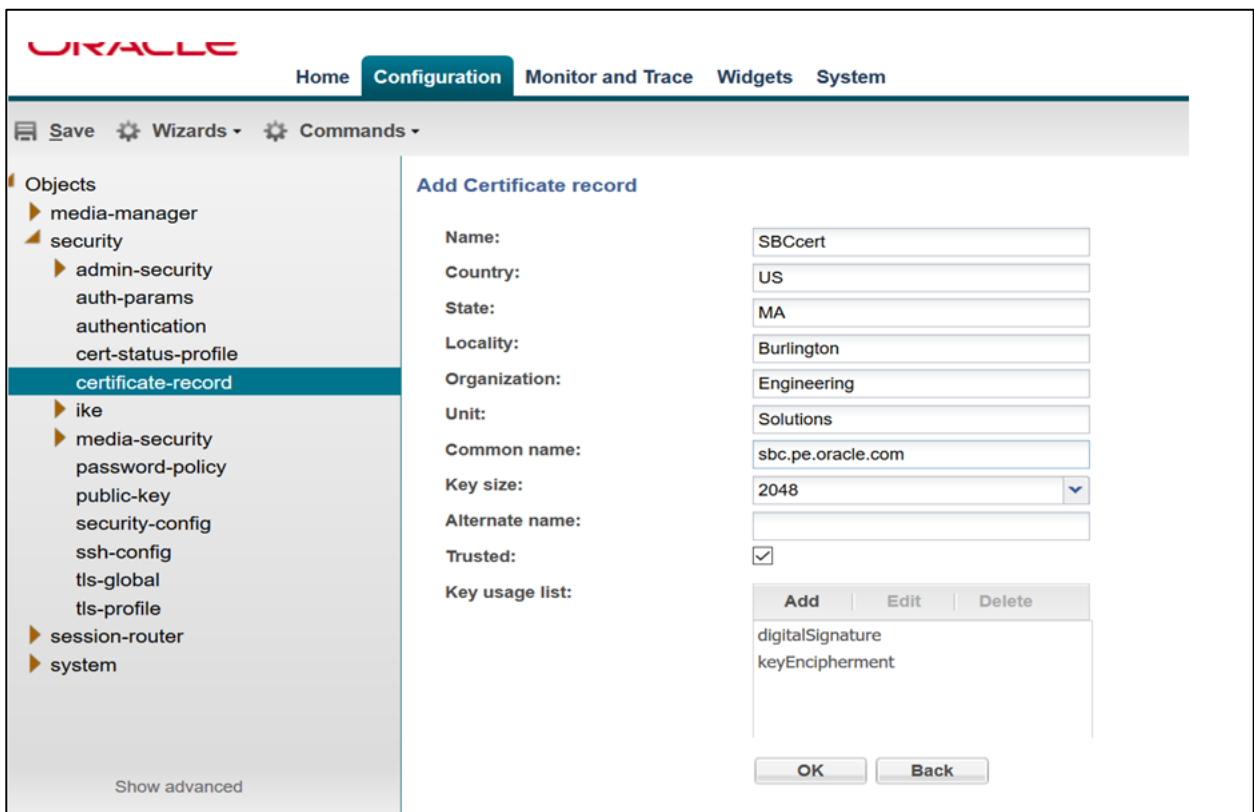
Phone Name	Description	Status	Protocol	Device Type	IP Address
JabberPcClient	Smith joe2 N/A	Default	SIP	None	None
JabberPcClient2	Mike Towle miketowle N/A	Default	SIP	None	None
SEP000C296352B2	SoftPhoneISR	Default	SIP	Registered with CUCM-Cisco.pe.oracle.com	10.232.50.11
SEP000C296352B3	ISRVoip1	Default	SIP	None	None
SEP001AA11B5085	SEP001AA11B5085-NTT3	Default	SIP	None	None
SEP0026CBA7CDA2	SEP0026CBA7CDA2 Mike Lab	Default	SIP	None	None
SEP00E16DBAD905	SEP00E16DBAD905-NTT	Default	SIP	None	None
SEP00E16DBB6C2E	SEP00E16DBB6C2E for Andy	Default	SIP	None	None
SEP00E16DBB6CF9	SEP00E16DBB6CF9-NTT Simulatorphone	Default	SIP	None	None
SEP00E16DBB7331	SEP00E16DBB7331 for Andy	Default	SIP	None	None
SEP0C272431BCB6	SEP0C272431BCB6	Default	SIP	Registered with CUCM-Cisco.pe.oracle.com	10.232.50.166
SEP0C272431C88C	Cisco 7975 Phone for SBC Testing	Default	SIP	None	None
SEP24B657B038B1	CUCM-2710-ATTFlexreach	Default	SIP	None	None
SEP580A209863BD	SEP580A209863BD-PurakATT	Default	SIP	Registered with CUCM-Cisco.pe.oracle.com	10.232.50.77
SEP64A0E71557A4	SEP64A0E71557A4-Cap-Group-2712	Default	SIP	None	None
SEPAABBCCDDB0C6	zoom phone	Default	SIP	Registered with CUCM-Cisco.pe.oracle.com	10.232.50.11
SEPBBCDDDEE0AFF	zoom phone1	Default	SIP	Registered with CUCM-Cisco.pe.oracle.com	10.232.50.11

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

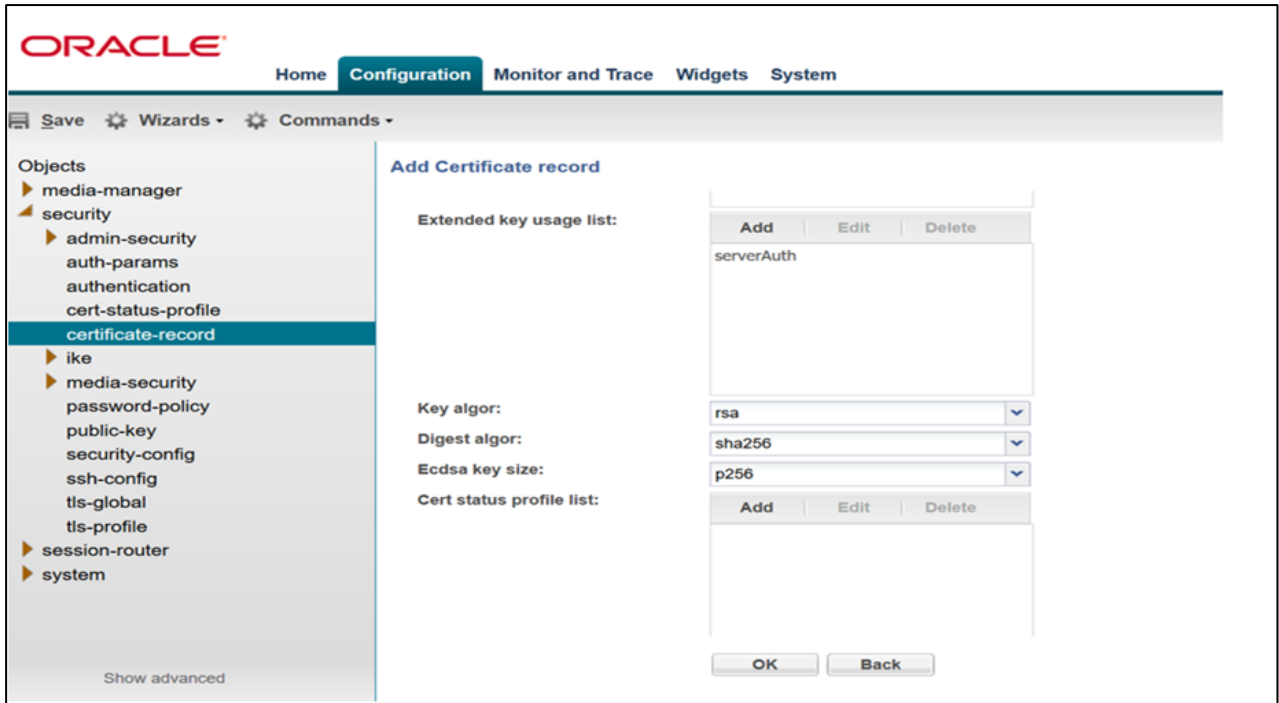
The first step is to create certificate record in the SBC and then adding it to TLS Profile for the zoom side. Please go to Configuration → Security → certificate record and create the SBC certificate:



The screenshot displays the Oracle SBC configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. Below the navigation bar, there are 'Save', 'Wizards', and 'Commands' options. The left sidebar shows a tree view of configuration objects, with 'certificate-record' selected under the 'security' folder. The main content area is titled 'Add Certificate record' and contains the following fields:

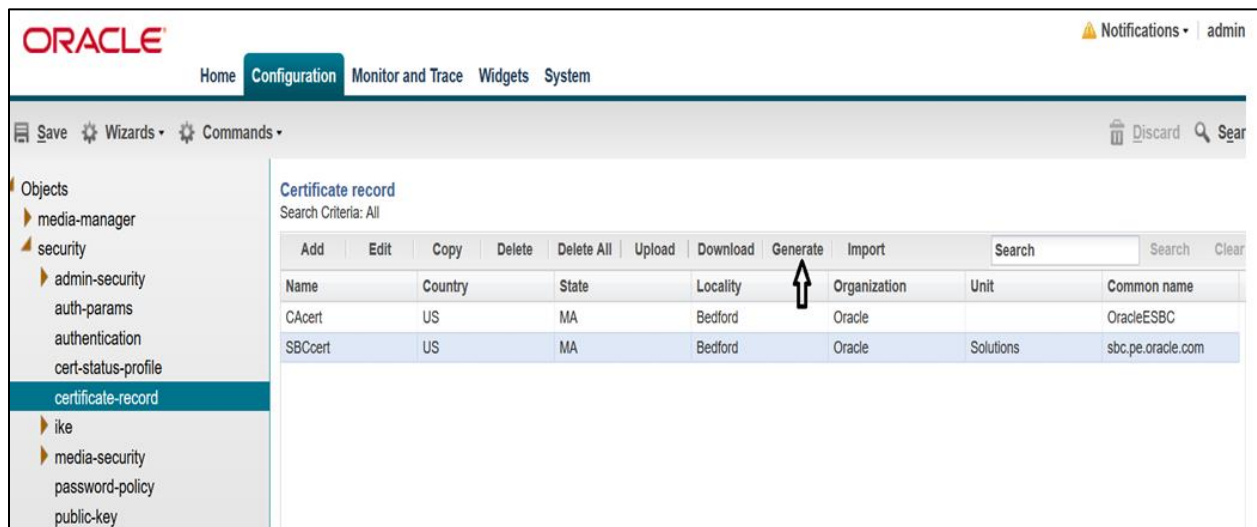
Name:	SBCcert									
Country:	US									
State:	MA									
Locality:	Burlington									
Organization:	Engineering									
Unit:	Solutions									
Common name:	sbccert.oracle.com									
Key size:	2048									
Alternate name:										
Trusted:	<input checked="" type="checkbox"/>									
Key usage list:	<table border="1"><tr><td>Add</td><td>Edit</td><td>Delete</td></tr><tr><td>digitalSignature</td><td></td><td></td></tr><tr><td>keyEncipherment</td><td></td><td></td></tr></table>	Add	Edit	Delete	digitalSignature			keyEncipherment		
Add	Edit	Delete								
digitalSignature										
keyEncipherment										

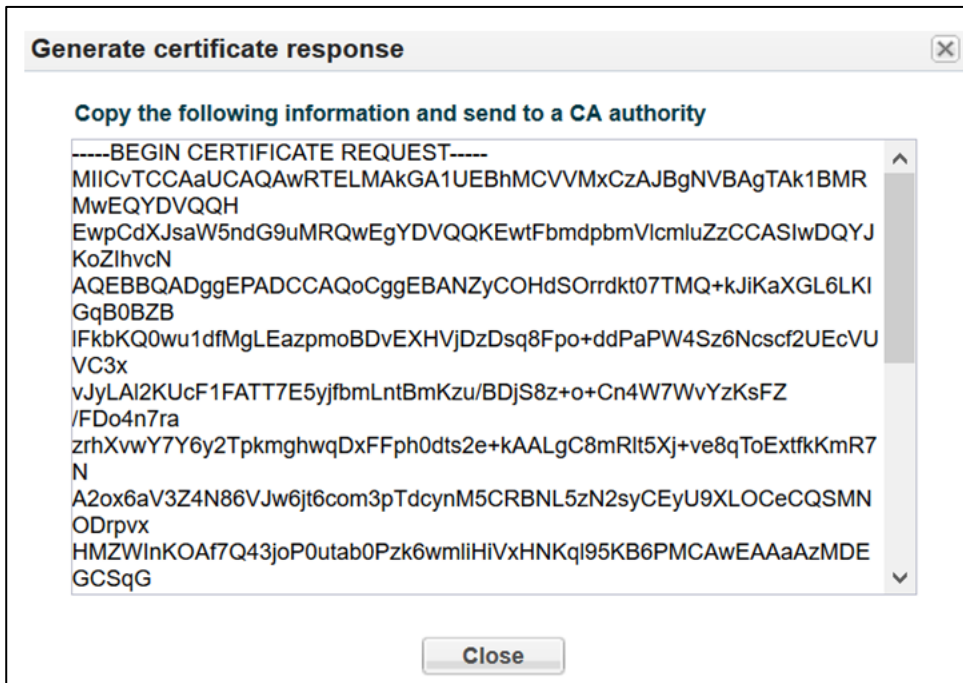
At the bottom of the form, there are 'OK' and 'Back' buttons. A 'Show advanced' link is located at the bottom left of the sidebar.



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:

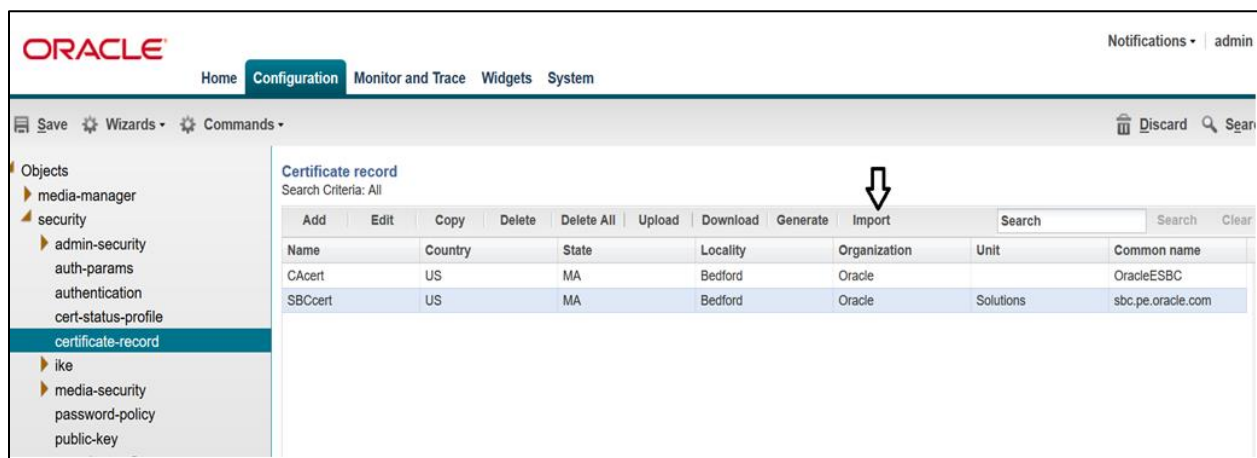


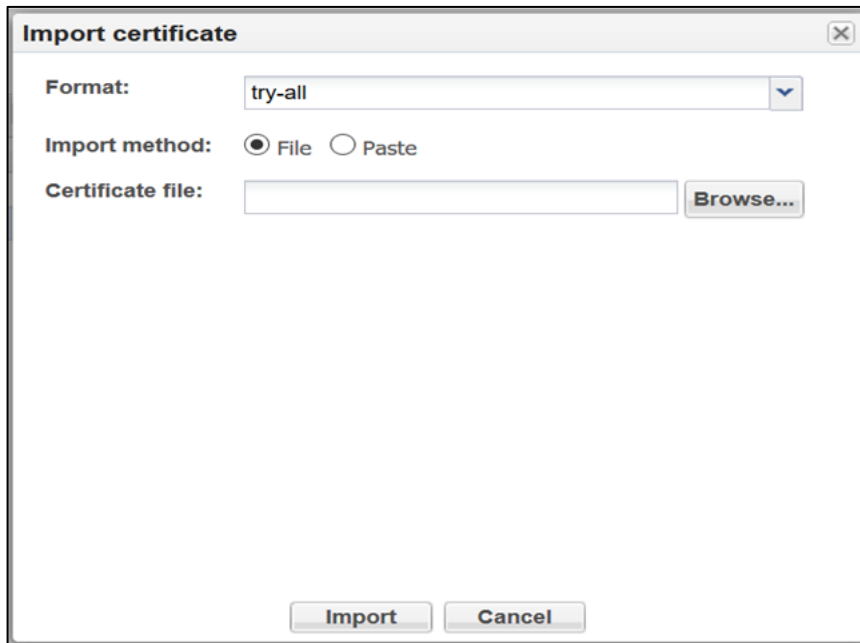


- Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, **a save and activate is required** before you can import the certificate record created above.

6.3. Import Certificates to SBC

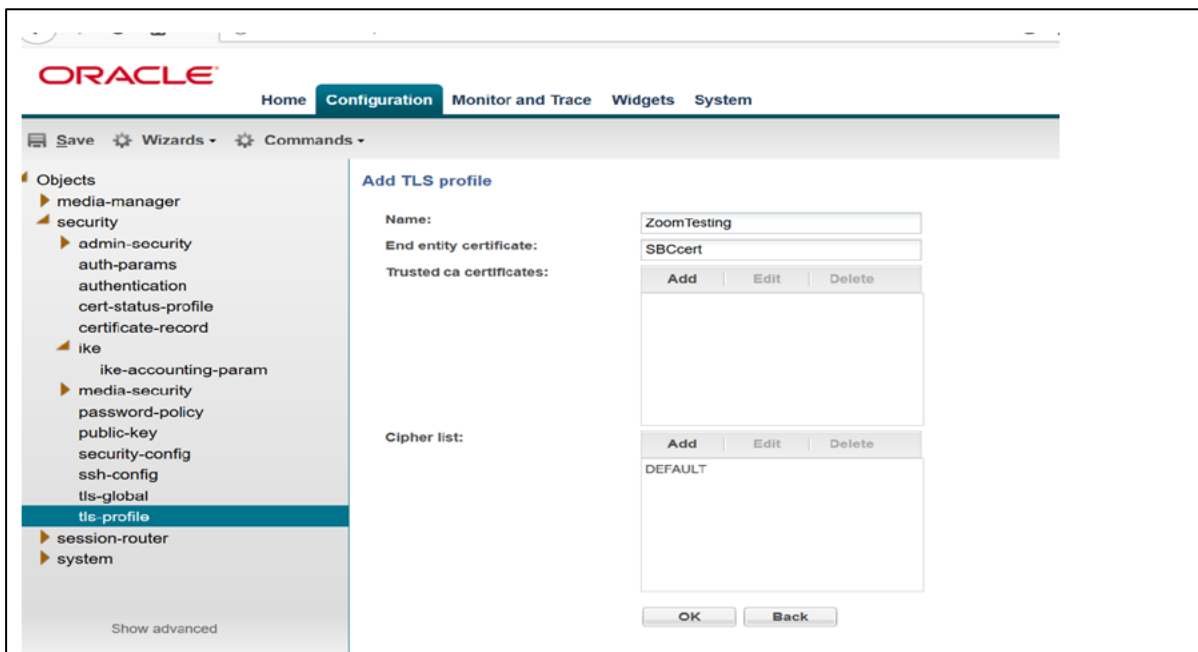
Once certificate signing request have been completed – import the signed certificate to the SBC. Once the certificate have been imported, please issue **save/activate** from the WebGUI





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.

The screenshot displays the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this, there are tabs for 'Save', 'Wizards', and 'Commands'. The left sidebar shows a tree view of objects, with 'media-security' expanded to show 'sdes-profile' selected. The main area is titled 'Add Sdes profile' and contains the following configuration fields:

- Name:** sdes-profile
- Crypto list:** A list containing 'AES_CM_128_HMAC_SHA1_80' and 'AES_CM_128_HMAC_SHA1_32'. Above the list are 'Add', 'Edit', and 'Delete' buttons.
- Srtp auth:**
- Srtp encrypt:**
- SrTCP encrypt:**
- Mki:**
- Egress offer format:** same-as-ingress (dropdown menu)
- Use ingress session params:** A list containing 'Add', 'Edit', and 'Delete' buttons.

At the bottom of the configuration area, there are 'OK' and 'Back' buttons. A 'Show advanced' link is located at the bottom left of the sidebar.

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

The screenshot shows the Oracle Configuration Assistant interface. The 'Configuration' tab is active. The left-hand 'Objects' tree is expanded to 'media-security' > 'media-sec-policy'. The main area displays the 'Add Media sec policy' dialog with the following fields:

- Name: srtp-zoom
- Pass through:
- Options: (Empty list with Add, Edit, Delete buttons)
- Inbound Profile: sdes-profile
- Mode: srtp
- Protocol: sdes
- Hide egress media update:

Buttons for 'OK' and 'Back' are visible at the bottom right.

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

The screenshot shows the Oracle Configuration Assistant interface. The 'Configuration' tab is active. The left-hand 'Objects' tree is expanded to 'media-security' > 'media-sec-policy'. The main area displays the 'Add Media sec policy' dialog with the following fields:

- Name: rtp-cucm
- Pass through:
- Options: (Empty list with Add, Edit, Delete buttons)
- Inbound Profile: (Empty dropdown)
- Mode: rtp
- Protocol: none
- Hide egress media update:

Buttons for 'OK' and 'Back' are visible at the bottom right.

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

The screenshot shows the Oracle configuration interface for 'Add Realm config'. The left sidebar lists various configuration objects, with 'realm-config' selected. The main panel contains the following fields:

- Identifier: ZoomTesting
- Description: (empty)
- Addr prefix: 0.0.0.0
- Network interfaces: A list containing 'sip0:0' with 'Add', 'Edit', and 'Delete' buttons.
- Mm in realm:
- Mm in network:
- Mm same ip:
- QoS enable:

Buttons for 'OK' and 'Back' are located at the bottom right.

The screenshot shows the Oracle configuration interface for 'Add Realm config' with advanced options visible. The left sidebar is the same as in the previous screenshot. The main panel contains the following fields:

- DNS realm: (dropdown)
- Media policy: (dropdown)
- Media sec policy: srtp-zoom (dropdown)
- RTCP mux:
- Ice profile: (dropdown)
- DTLS srtp profile: (dropdown)
- Srtp msm passthrough:
- Class profile: (dropdown)
- In translationid: (dropdown)
- Out translationid: (dropdown)
- In manipulationid: (dropdown)
- Out manipulationid: (dropdown)
- Average rate limit: 0 (Range: 0..4294967295)
- Access control trust level: none (dropdown)
- Invalid signal threshold: 0 (Range: 0..4294967295)

Buttons for 'OK' and 'Back' are located at the bottom right.

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

The screenshot shows the Oracle configuration interface for adding a realm. The left sidebar lists various objects, with 'realm-config' selected. The main area is titled 'Add Realm config' and contains the following fields:

- Identifier: CUCMREG
- Description: (empty text box)
- Addr prefix: 0.0.0.0
- Network interfaces: A list containing 'slp1:0' with 'Add', 'Edit', and 'Delete' buttons above it.
- Mm in realm:
- Mm in network:
- Mm same ip:
- QoS enable:

At the bottom right, there are 'OK' and 'Back' buttons.

This screenshot shows the advanced configuration options for the realm. The left sidebar remains the same. The main area is titled 'Add Realm config' and contains the following fields:

- DNS realm: (dropdown menu)
- Media policy: (dropdown menu)
- Media sec policy: rtp-cucm (dropdown menu)
- RTCP mux:
- Ice profile: (dropdown menu)
- DTLS srtp profile: (dropdown menu)
- Srtp msm passthrough:
- Class profile: (dropdown menu)
- In translationid: (dropdown menu)
- Out translationid: (dropdown menu)
- In manipulationid: (dropdown menu)
- Out manipulationid: (dropdown menu)
- Average rate limit: 0 (Range: 0..4294967295)
- Access control trust level: none (dropdown menu)
- Invalid signal threshold: 0 (Range: 0..4294967295)

At the bottom right, there are 'OK' and 'Back' buttons.

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:

ORACLE
Home Configuration Monitor and Trace Widgets System

Save Wizards Commands

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
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

Show advanced

Modify SIP interface

State:

Realm ID: ZoomTesting

Description:

SIP ports

Add Edit Copy Delete					
Address	Port	Transport protocol	TLS profile	Allow anonymous	
155.212.214.178	5060	UDP		agents-only	
155.212.214.178	5060	TCP		agents-only	
155.212.214.178	5061	TLS	ZoomTesting	all	

Initial inv trans expire: 0 (Range: 0..999999999)

Session max life limit: 0

Proxy mode:

OK Back

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

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

Modify SIP interface

State:

Realm ID: CUCMREG

Description:

SIP ports

Add Edit Copy Delete					
Address	Port	Transport protocol	TLS profile	Allow anonymous	
10.232.50.11	5060	UDP		all	
10.232.50.11	5060	TCP		all	

Initial inv trans expire: 0 (Range: 0..999999999)

Session max life limit: 0

Proxy mode:

OK Back

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

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: 10.232.50.89
IP address: 10.232.50.89
Port: 5060 (Range: 0, 1025..65535)
State:
App protocol: SIP
App type:
Transport method: DynamicTCP
Realm ID: CUCMREG
Egress Realm ID:
Description:

Match Identifier

Add Edit Copy Delete

Identifier rule	Match value
-----------------	-------------

OK Back

ORACLE
Home Configuration Monitor and Trace Widgets System

Save Wizards Commands

account-group
allowed-elements-profile
class-profile
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

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: StaticTCP
Realm ID: CUCMREG
Egress Realm ID:
Description:

Match Identifier

Add Edit Copy Delete

Identifier rule	Match value
-----------------	-------------

OK Back

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

Modify Local policy

From address: Add Edit Delete

To address: Add Edit Delete

Source realm: Add Edit Delete
ZoomTesting

OK Back

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: 10.232.50.89

Realm: CUCMREG

Action: none

Terminate recursion:

Cost: 0 (Range: 0..999999999)

State:

App protocol:

Lookup: single

Next key:

OK Back

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:	<input type="text" value="CUCM-Cisco.pe.oracle.com"/>
Realm:	<input type="text" value="CUCMREG"/>
Action:	<input type="text" value="replace-uri"/>
Terminate recursion:	<input type="checkbox"/>
Cost:	<input type="text" value="0"/> (Range: 0..999999999)
State:	<input checked="" type="checkbox"/>
App protocol:	<input type="text"/>
Lookup:	<input type="text" value="single"/>
Next key:	<input type="text"/>

OK Back

6.11. Configure steering-pool

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

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below the navigation bar, there are tabs for 'Save', 'Wizards', and 'Commands'. On the left, a tree view under 'Objects' lists various configuration items, with 'steering-pool' selected. The main area is titled 'Add Steering pool' and contains the following fields:

IP address:	<input type="text" value="155.212.214.178"/>
Start port:	<input type="text" value="32000"/> (Range: 1..65535)
End port:	<input type="text" value="33000"/> (Range: 1..65535)
Realm ID:	<input type="text" value="ZoomTesting"/>
Network interface:	<input type="text"/>

At the bottom right, there are 'OK' and 'Back' buttons.

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below the navigation bar, there are tabs for 'Save', 'Wizards', and 'Commands'. On the left, a tree view under 'Objects' lists various configuration items, with 'steering-pool' selected. The main area is titled 'Add Steering pool' and contains the following fields:

IP address:	<input type="text" value="10.232.50.11"/>
Start port:	<input type="text" value="10000"/> (Range: 1..65535)
End port:	<input type="text" value="10999"/> (Range: 1..65535)
Realm ID:	<input type="text" value="CUCMREG"/>
Network interface:	<input type="text"/>

At the bottom right, there are 'OK' and 'Back' buttons.

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.

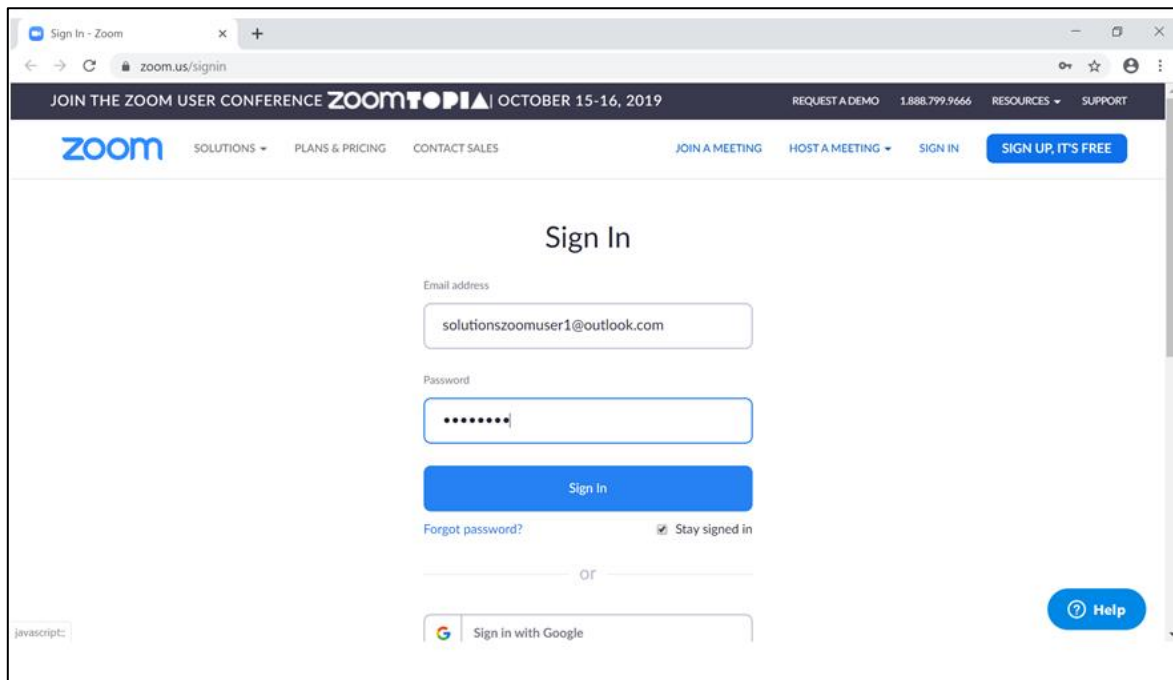
8. Configuring the Zoom softphone in Admin Portal

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.

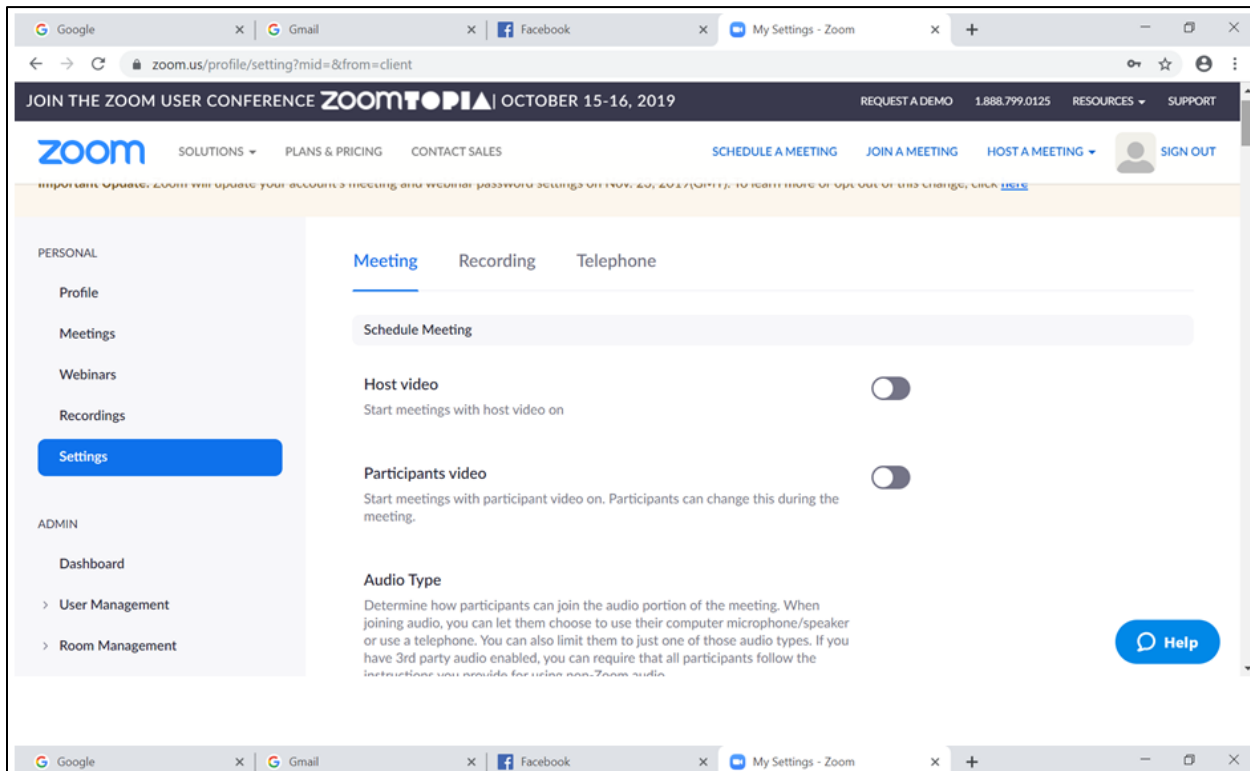
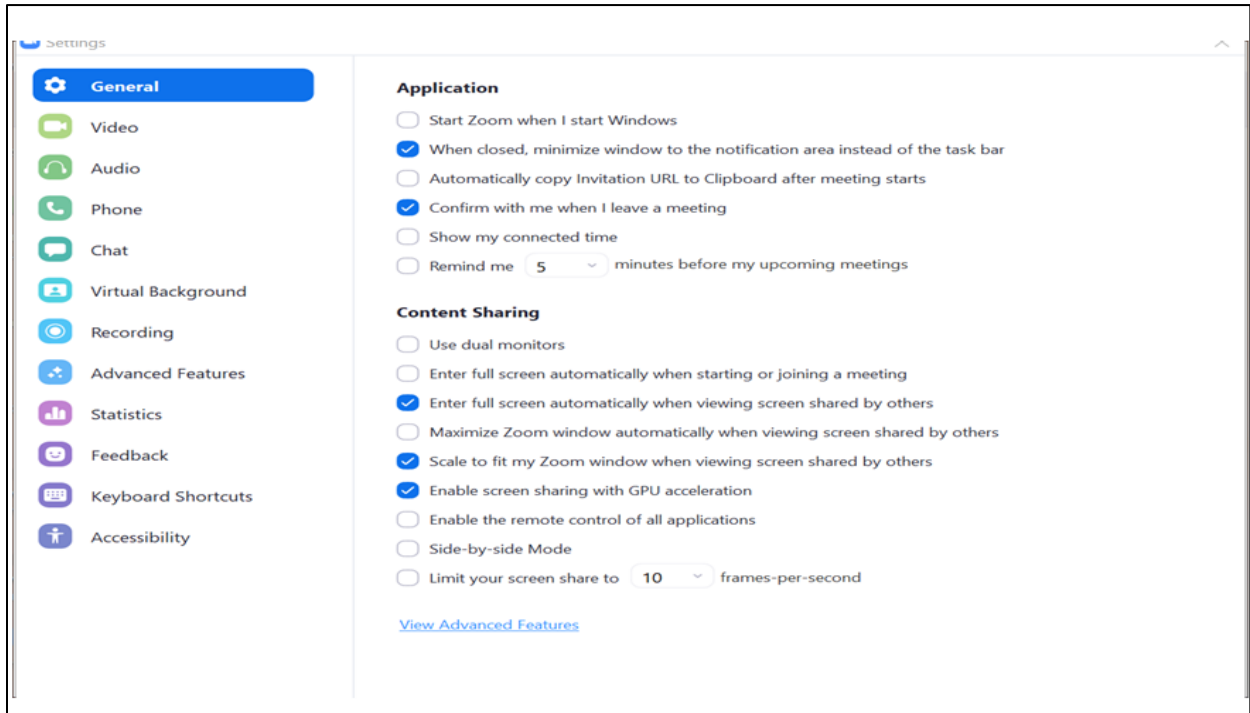
From now on, whenever the document refers to "Go to Advanced features" or "Admin" options, please note that the above steps have to be performed in Zoom admin portal to perform necessary configuration.



The screenshot shows the Zoom Sign In page in a web browser. The browser address bar displays "zoom.us/signin". The page header includes the Zoom logo and navigation links: SOLUTIONS, PLANS & PRICING, CONTACT SALES, JOIN A MEETING, HOST A MEETING, SIGN IN, and a blue button labeled "SIGN UP, IT'S FREE". The main content area is titled "Sign In" and contains the following elements:

- An "Email address" field with the text "solutionszoomuser1@outlook.com".
- A "Password" field with masked characters "*****".
- A blue "Sign in" button.
- Links for "Forgot password?" and a checked "Stay signed in" checkbox.
- An "or" separator.
- A "Sign in with Google" button.
- A blue "Help" button in the bottom right corner.

At the bottom left of the page, there is a small "javascript:" error message.



The screenshot shows a web browser window with the Zoom user settings page. The browser's address bar shows the URL `zoom.us/profile/setting?mid=&from=client`. The page header includes the Zoom logo, navigation links for SOLUTIONS, PLANS & PRICING, CONTACT SALES, SCHEDULE A MEETING, JOIN A MEETING, HOST A MEETING, and SIGN OUT. A dark banner at the top of the page promotes the 'JOIN THE ZOOM USER CONFERENCE ZOOMTOPIA | OCTOBER 15-16, 2019' with links for REQUEST A DEMO, 1.888.799.0125, RESOURCES, and SUPPORT.

The main content area is titled 'Participants Video' and contains the following settings:

- Participants Video:** A toggle switch is currently turned off. The text below reads: 'Start meetings with participant video on. Participants can change this during the meeting.'
- Audio Type:** A section with the heading 'Audio Type' and a descriptive paragraph: '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.' Below this are three radio button options: 'Telephone and Computer Audio' (which is selected), 'Telephone', and 'Computer Audio'.
- Join before host:** A toggle switch is currently turned off. The text below reads: 'Allow participants to join the meeting before the host arrives'.
- Use Personal Meeting ID (PMI) when scheduling a meeting:** A toggle switch is currently turned off. The text below reads: 'You can visit [Personal Meeting Room](#) to change your Personal Meeting settings.'

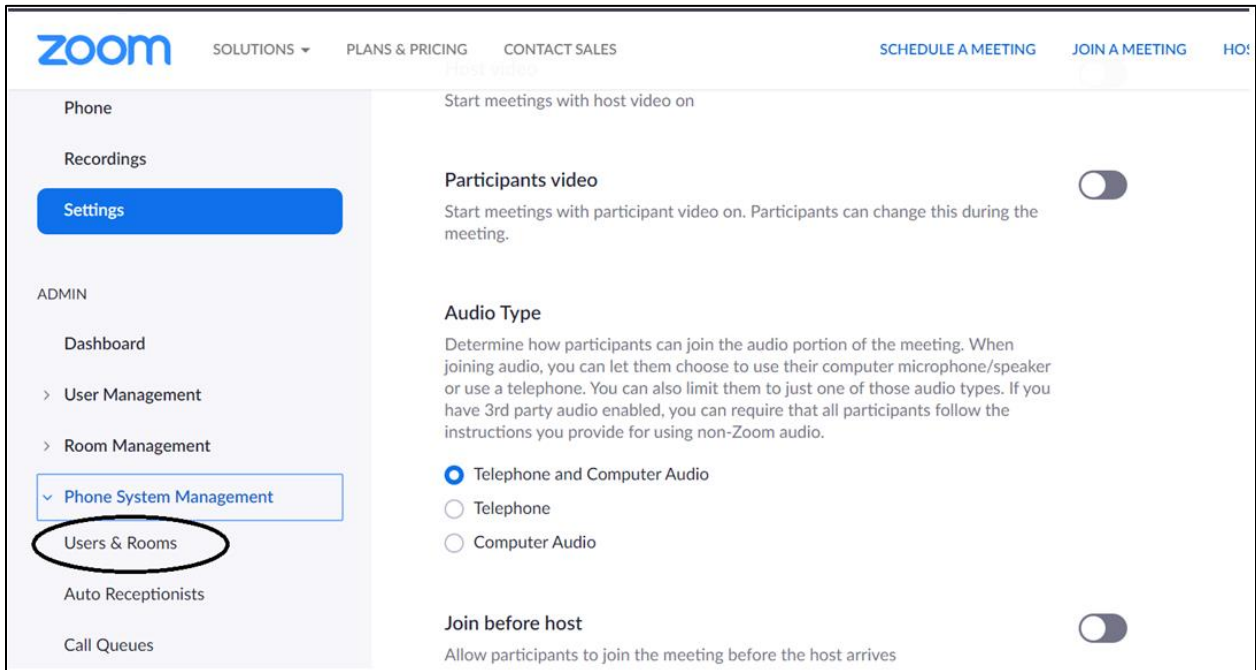
On the left side, there is an 'ADMIN' sidebar menu with the following items: Dashboard, User Management, Room Management, Phone System Management, Account Management, and Advanced. Below the sidebar are links for 'Attend Live Training', 'Video Tutorials', and 'Knowledge Base'. A blue 'Help' button is located in the bottom right corner of the settings area.

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.

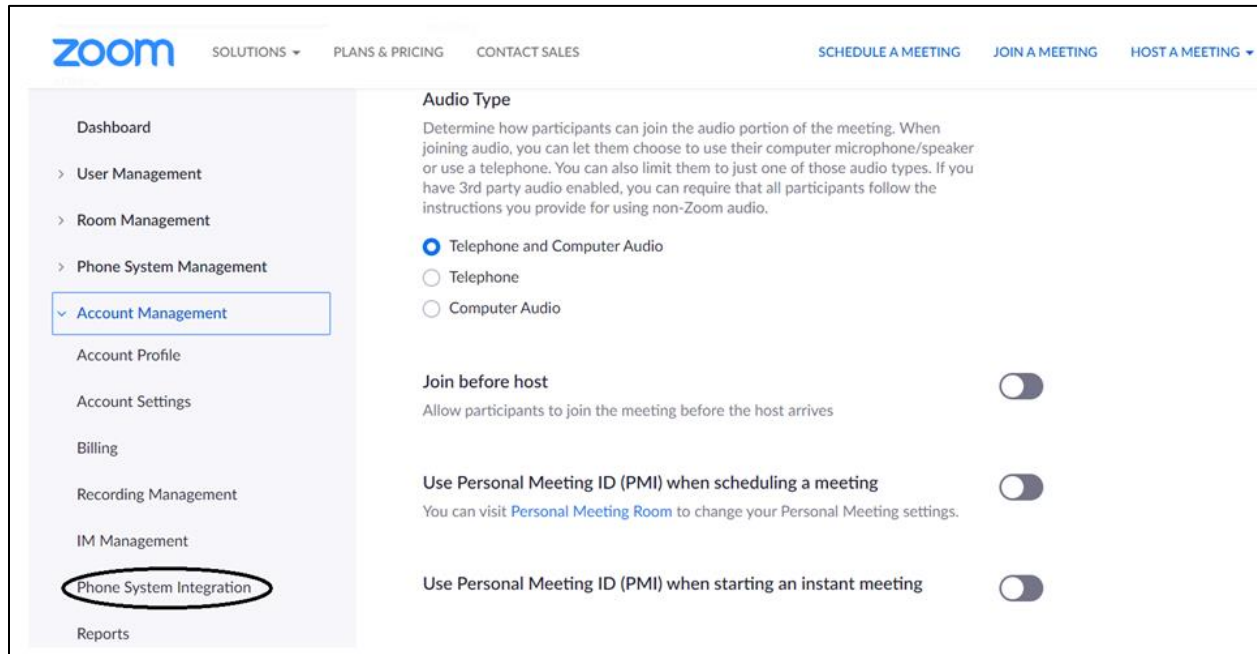


The screenshot shows the Zoom Admin Portal interface. The left sidebar contains the following navigation items: Phone, Recordings, Settings (highlighted in blue), ADMIN, Dashboard, > User Management, > Room Management, > Phone System Management (expanded), Users & Rooms (circled in black), Auto Receptionists, and Call Queues. The main content area is titled "Phone System Management" and includes the following settings:

- Start meetings with host video on** (toggle)
- Participants video** (toggle, currently off). Description: Start meetings with participant video on. Participants can change this during the meeting.
- Audio Type** (radio buttons):
 - Telephone and Computer Audio
 - Telephone
 - Computer AudioDescription: 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.
- Join before host** (toggle, currently off). Description: Allow participants to join the meeting before the host arrives.

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 download and used for Zoom softphones.



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

The screenshot shows a Microsoft Excel spreadsheet titled 'sipaccount.csv'. The spreadsheet contains a table with the following data:

1	Domain	Register Server1	Transport Protocol	Proxy Server1	Register Server2	Transp	Proxy Server2	Register Server2:Transp	Proxy Server1	Registration Expiry	User Name	Password	Author	
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	192.168.0.10	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	192.168.0.10	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	192.168.0.10	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	192.168.0.10	60	1010	null	test4

	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Proxy Server1	Register Server2	Transp	Proxy Server2	Register Server: Transp	Proxy Server	Registration Expiry	User Name	Password	Authorization Name	Zoom User Identity	Voice Mail	
2	192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.10	60	1008	password	test1	test1@zoom.us	vm1
3	192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.10	60	1009	test2	test2@zoom.us.pc	vm2	
4	192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.10	60	1010	null	test3	test3@zoom.us.mobile	vm3
5	192.168.0.10	192.168.0.100	UDP	192.168.0.10	192.168.0.100	UDP	192.168.0.10	60	1010	null	test4	test4@zoom.us.pad	vm4
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
24													

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.**

1	Domain	?Register Server1	Transport Pr	Proxy Server1	?Register !	Transport Proxy Serv	?Register !	Transport Proxy Serv	Registratic	User Name	Password	Authorizal	Zoom T
2	CUCM-Cisco.pe.oracle.com	10.232.50.89	AUTO	155.212.214.178:5065						60	17814437295	Abcd1234	isrvoip1 solution
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
24													

	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Transport Pr	Proxy Server1	?Register	:Transport	Proxy Serv	?Register	:Transport	Proxy Serv	Registratic	User Name	Password	Authorizal	Zoom User	Voice Mail
2	AUTO	155.212.214.178:5065							60	17814437295	Abcd1234	isrvoip1	solutionszoomuser1@outlook.com	

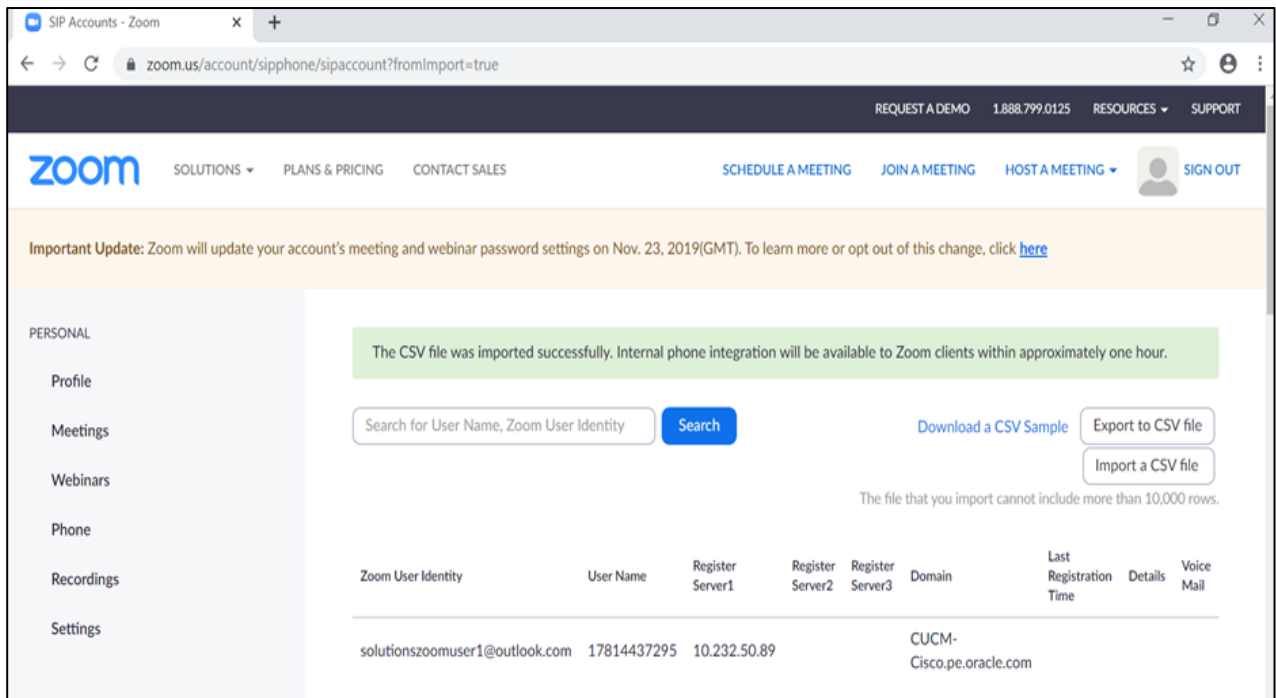
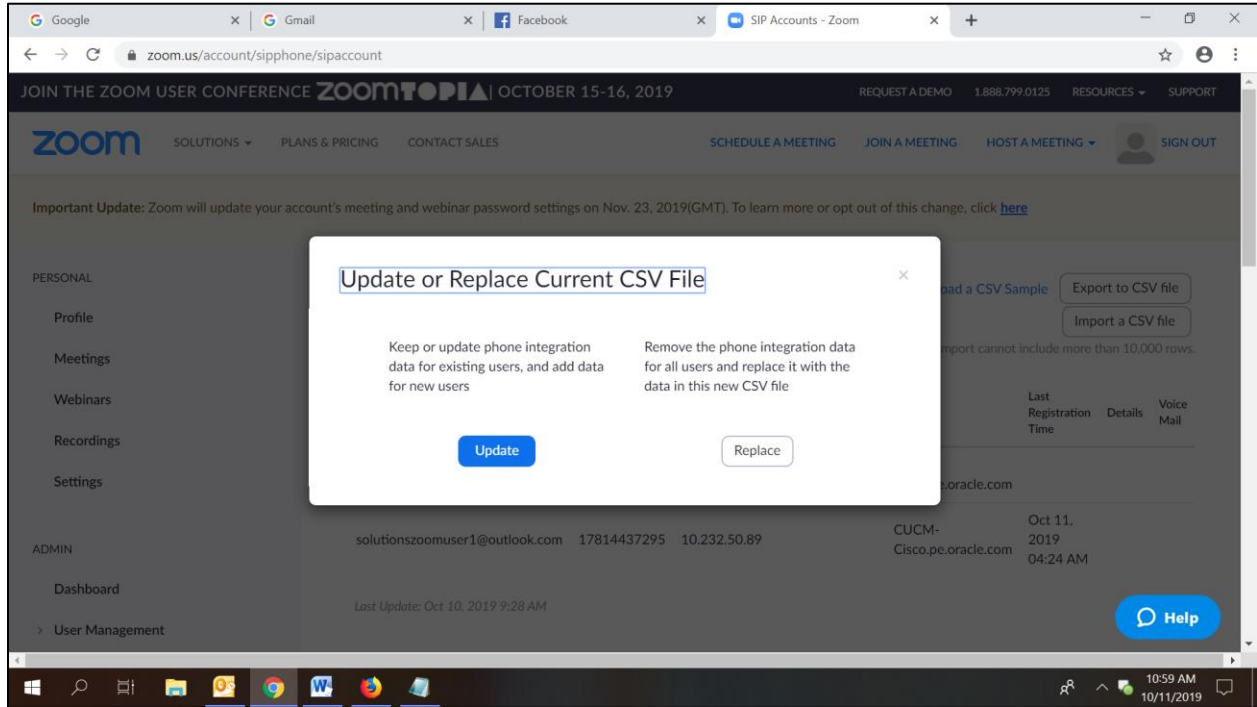
If the customer environment has a DNS configured and if it is able to resolve the FQDN of the registrar server which is Cisco CUCM in our case, then we can specify the FQDN in the registrar server entry instead of giving IP address of the registrar server and zoom client will be able to register successfully 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:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Domain	?Register Server1	Transport Proxy S	?Regist	Trans	Proxy Serv	?Regis	Transp	Proxy Registra	User Name	Password	Authorizal	Zoom Use	Voice Mail		
2	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.



The screenshot shows the Zoom Phone Settings window. The left sidebar contains a list of settings categories: General, Video, Audio, Phone (highlighted), Chat, Virtual Background, Recording, Advanced Features, Statistics, Feedback, Keyboard Shortcuts, and Accessibility. The main content area displays the following configuration details:

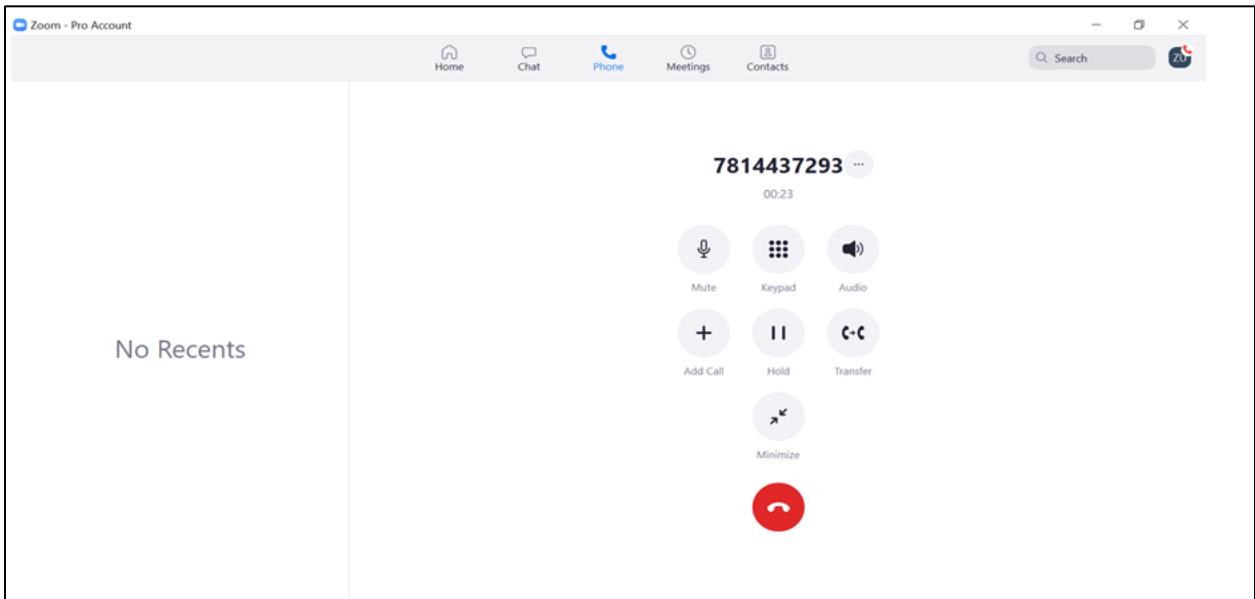
Domain :	CUCM-Cisco.pe.oracle.com
Register server :	10.232.50.89
Transport protocol :	AUTO
Proxy server :	155.212.214.178:5065
Registration expiry :	60 minutes
Last registration :	10/11/2019 11:00 AM
Username (directory username) :	zoom user1
Authorization name :	isrvoip1
Zoom user identity :	solutionszoomuser1@outlook.com
Voicemail :	-

At the bottom, there is a **Diagnostics :** section with a button labeled "Report diagnostic Information" and a help icon.

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.



ORACLE Enterprise Session Border Controller

Notifications admin

Home Configuration Monitoring System

Monitor And Trace

- Notable Events
- Registrations
- Sessions
- Subscriptions
- Widgets

SIP Session Summary

Search Criteria: All

Start Time	State	Call ID	Request URI	From URI	To URI
2019-10-11 01:39:02.760	TERMINATED...	ljVU95zxbubFM3td6ioU...	sip:7814437293@10.232...	"zoom%20user1" <sip:178...	<sip:7814437293@10.232...
2019-10-11 01:34:28.190	FAILED-487	CWG66u6OLbXMOa6blvq...	sip:7814437293@10.232.5...	"zoom%20user1" <sip:178...	<sip:7814437293@10.232...
2019-10-11 00:36:08.124	TERMINATED...	7c6e7180-d9f1fab8-5c63f...	sip:17814437295@10.232...	<sip:7814437293@10.232...	<sip:17814437295@10.23...
2019-10-11 00:31:59.386	TERMINATED...	X9lBYtbzqAjdy56Cb13KhA...	sip:7814437293@10.232.5...	"zoom%20user1" <sip:178...	<sip:7814437293@10.232...
2019-10-11 00:22:35.387	FAILED-487	wfmlUhoc-XhMVyYZFnNH...	sip:1020@10.232.50.89;tra...	"zoom%20user1" <sip:178...	<sip:1020@10.232.50.89;tr...
2019-10-11 00:22:18.191	TERMINATED...	gFS-2PZfy6Djtjwe9WgYUw...	sip:7814437293@10.232.5...	"zoom%20user1" <sip:178...	<sip:7814437293@10.232...

Page 1 of 1 (1-6 of 6 items)

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

CONNECT WITH US

 blogs.oracle.com/oracle

 facebook.com/Oracle/

 twitter.com/Oracle

 oracle.com

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2019, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

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