Oracle SBC integration with Cisco CUCM and Microsoft Teams Enterprise Model

Technical Application Note

ORACLE
COMMUNICATIONS

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Revision History

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with Cisco CUCM and Microsoft Teams Enterprise Model	21st February 2020
1.1	Adding Caveat Section for On HOLD issue.	21st April 2021
1.2	Removed reference to sip-all FQDN from the app note document	12th January 2022
1.3	Refreshed the app note with testing of Teams with CUCM 12.5 and Oracle SBC 9.0 version	22nd April 2022
1.4	Since sip-all FQDN is removed, add the following two sections: Enable refer call xfer on realm Added RespondOptionsManip	22nd July 2022
1.5	Added DigiCert Global G2 Cert as root CA for Teams Changed certificate-record screenshots Added Access Control Lists	5th Sep 2022

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 Microsoft Teams Direct Routing Enterprise Model and Cisco CUCM.

2. Document Overview

This Oracle technical application note outlines the configuration needed to set up the interworking between on premises Cisco CUCM and Microsoft's Teams Enterprise Model(Cloud based) using Oracle SBC. The solution contained within this document has been tested using Oracle Communication SBC **OS 830m1p2** and **OS900p2** version. Our scope of this document is only limited to testing Teams Enterprise Model with Cisco CUCM.

Microsoft Teams Direct Routing lets you connect a supported, customer-provided Session Border Controller (SBC) to Microsoft Phone System. With Direct Routing, you can connect your SBC to almost any telephony trunk or interconnect with third-party Public Switched Telephone Network (PSTN) equipment. Direct Routing enables you to:

- Use virtually any PSTN trunk with Microsoft Phone System.
- Configure interoperability between customer-owned telephony equipment, such as a third-party private branch exchange (PBX), analog devices, and Microsoft Phone System.

Microsoft Teams works on two different methods which is given below:

1) **Media bypass**

Media bypass shortens the path of media traffic and reduces the number of hops in transit for better performance. With media bypass, media is kept between the Session Border Controller (SBC) and the client instead of sending it via the Microsoft Phone System. For more information on media bypass, please read the links given below.

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan-media-bypass

https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/SBC-MSFTTeams-MB.pdf

2) **Non-media bypass**

Without media bypass, when a client makes or receives a call, both signaling and media flow between the SBC, the Microsoft Phone System, and the Teams client. For more information on media bypass, please read the links given below.

https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/SBC-MSFTTeams-NONMB.pdf

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

It should be noted that while this application note focuses on the optimal configurations for the Oracle SBC in an enterprise Cisco CUCM 11.5 / CUCM 12.5 environment, the same SBC configuration model can also be used for other enterprise applications with a few tweaks to the configuration for required features. The Cisco Call Manager End User and Phone creation is not covered as part of this document

In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the Cisco CUCM Server associated parameters. Many SBC applications may have additional configuration requirements that are specific to individual customer requirements. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

For additional information on CUCM 11.5, please visit

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

For additional information on CUCM 12.5, please visit

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

Please note that the IP Addresses, FQDN and configuration names and details given in this document are used for reference purposes only. These same details cannot be used in customer configurations. End users of this document can use the configuration details according to their network requirements. There are some public facing IPs (externally routable IPs) that we use for our testing are masked in this document for security reasons.
The customers can configure any publicly routable IPs for these sections as per their network architecture needs.

3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Teams Direct Routing Enterprise Model with Cisco CUCM 11.5 / CUCM 12.5 version using Oracle Enterprise SBC. There will be steps that require navigating the CUCM 11.5 / CUCM 12.5 server configuration, Oracle SBC GUI interface, understanding the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

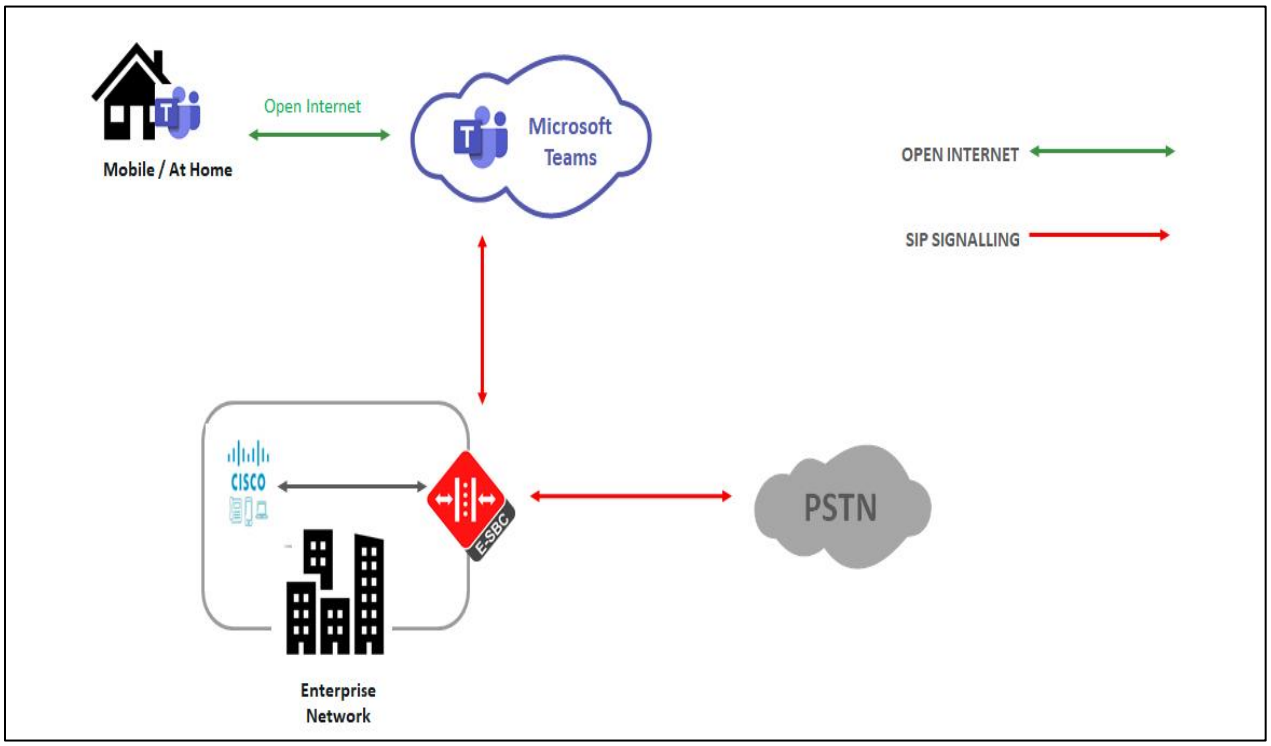
3.2. Requirements

- Fully functioning Cisco UCM 11.5 / CUCM 12.5 version.
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.3.0 / 9.0.0 version
- Teams Direct Routing Enterprise Model running Teams Client.

The below revision table explains the versions of the software used for each component:

Software Used	CUCM Version	SBC Version	Teams Client version
Revision 1	11.5	8.3.0	1.3.00.362 (64-bit) Windows OS
Revision 2	12.5	9.0.0	1.4.00.22472 (64-bit) Windows OS

3.3. Architecture

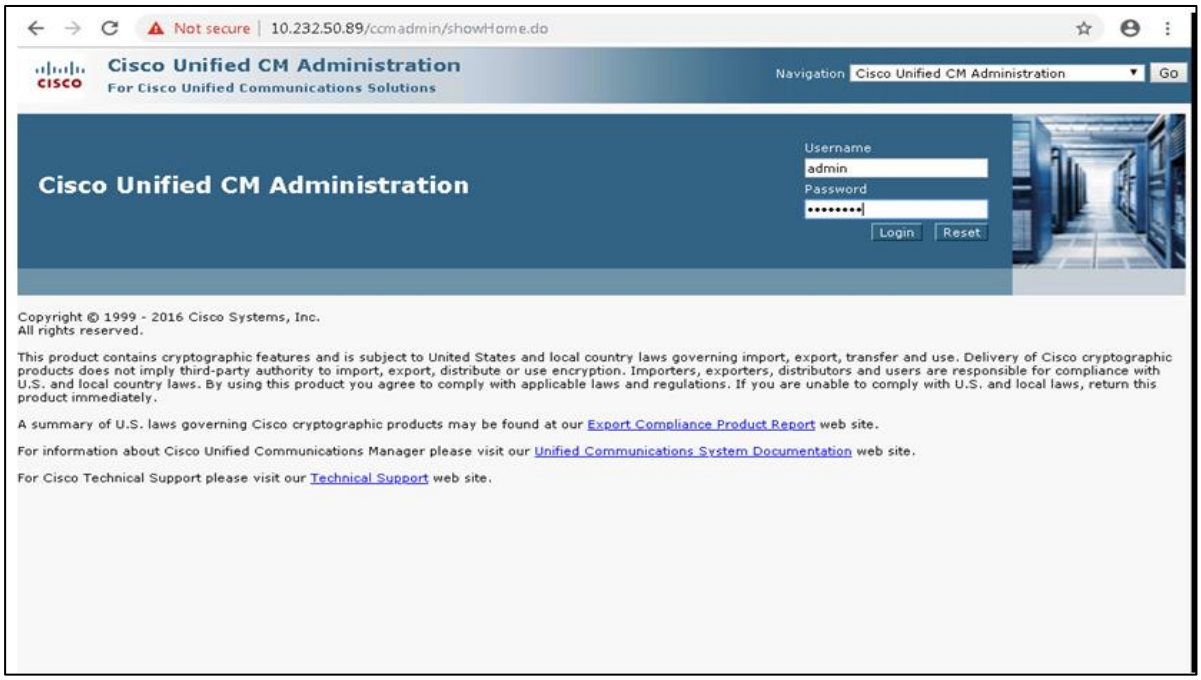


The configuration, validation and troubleshooting is the focus of this document and will be described in three phases:

- Phase 1 – Configuring the Cisco Unified Call Manager v11.5 / V 12.5 for Oracle SBC
- Phase 2 – Configuring the Teams Direct Routing Enterprise Model.
- Phase 3 – Configuring the Oracle SBC

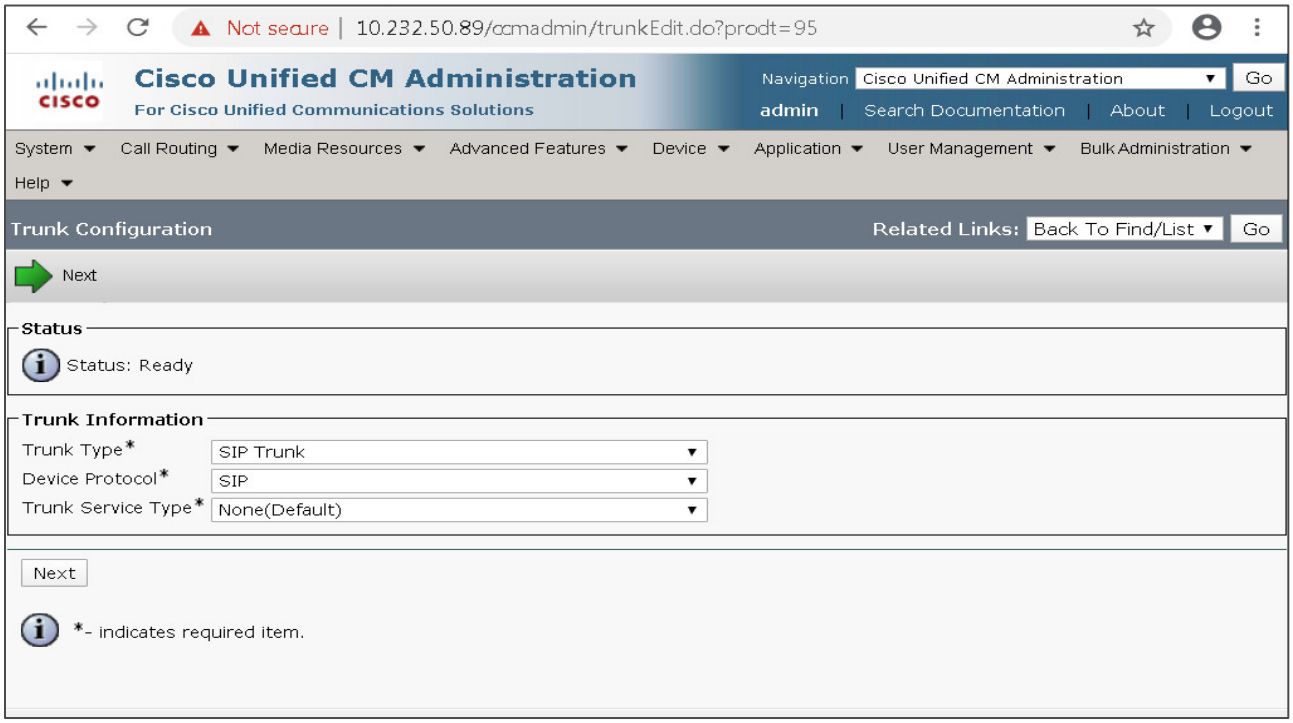
4. Configuring Cisco CUCM

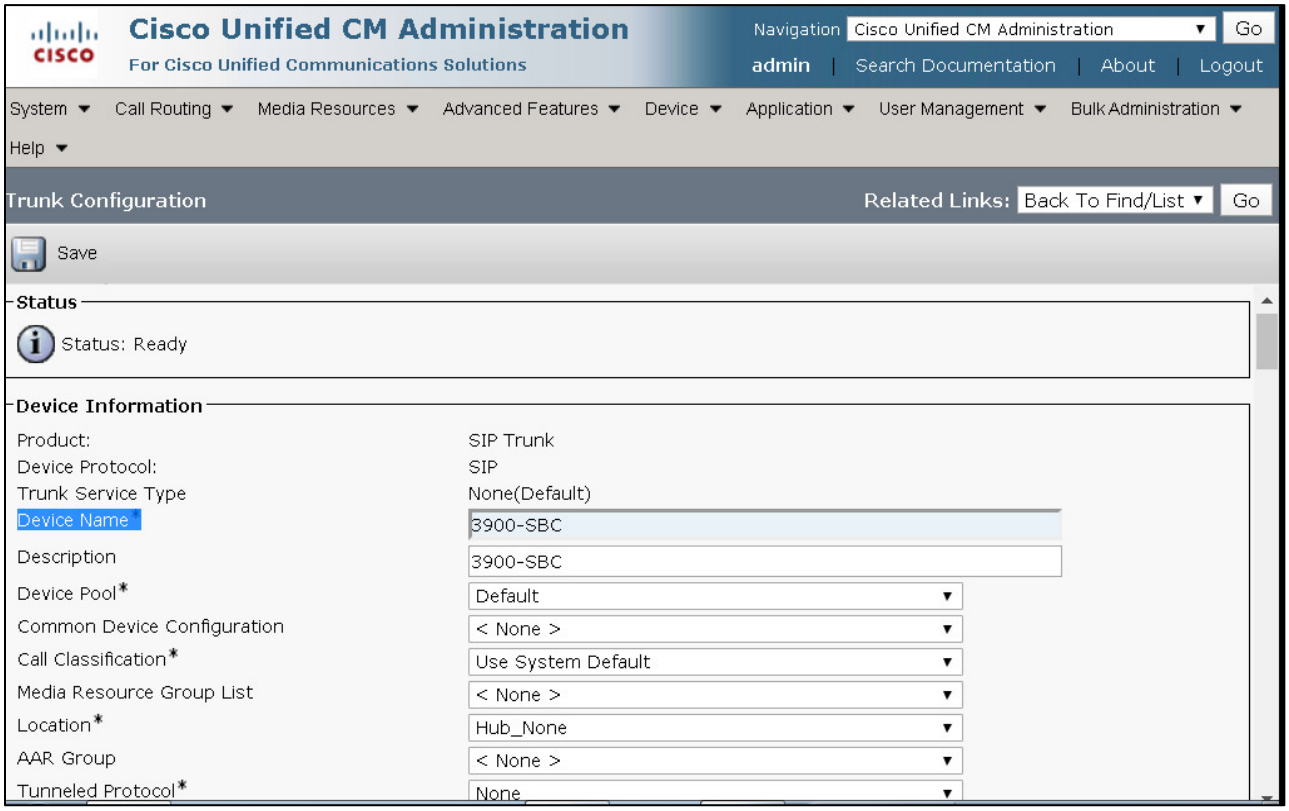
Please login to Cisco CUCM admin web GUI with proper login credentials (Username and password). After that, perform the steps below in the given order.

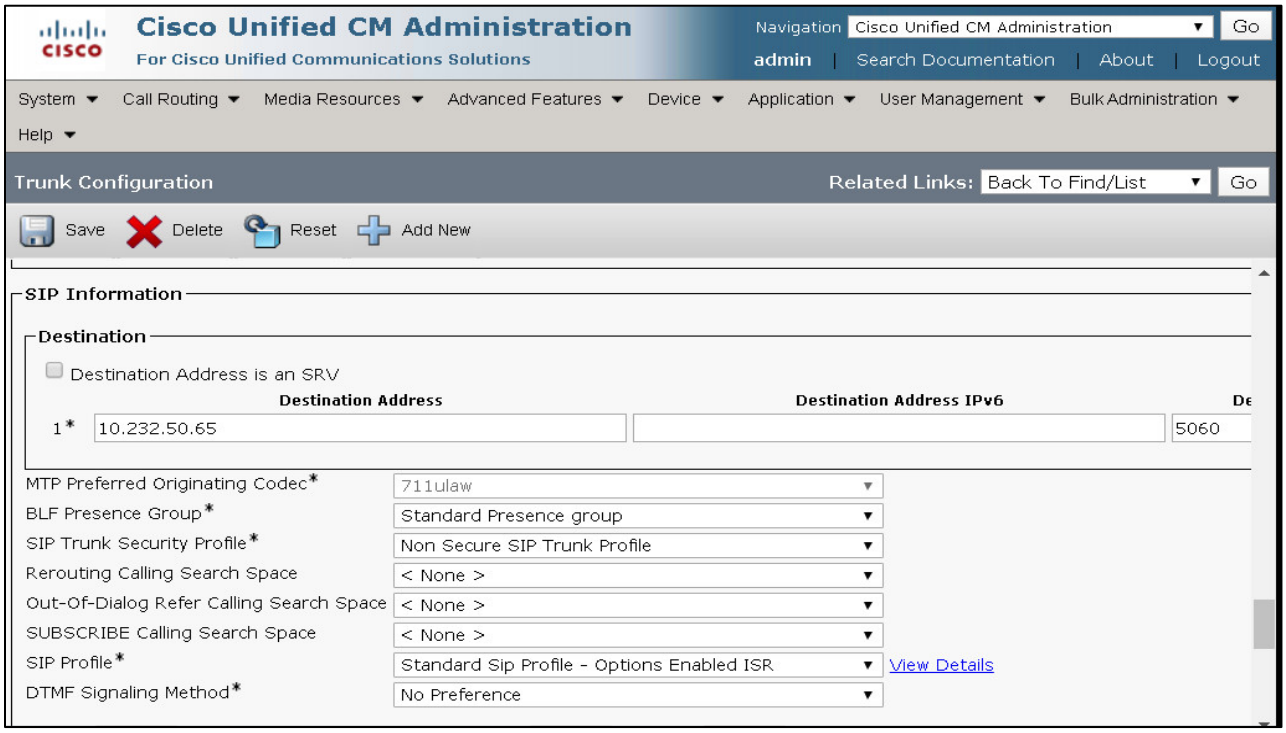


4.1. Configuring a new SIP Trunk

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


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

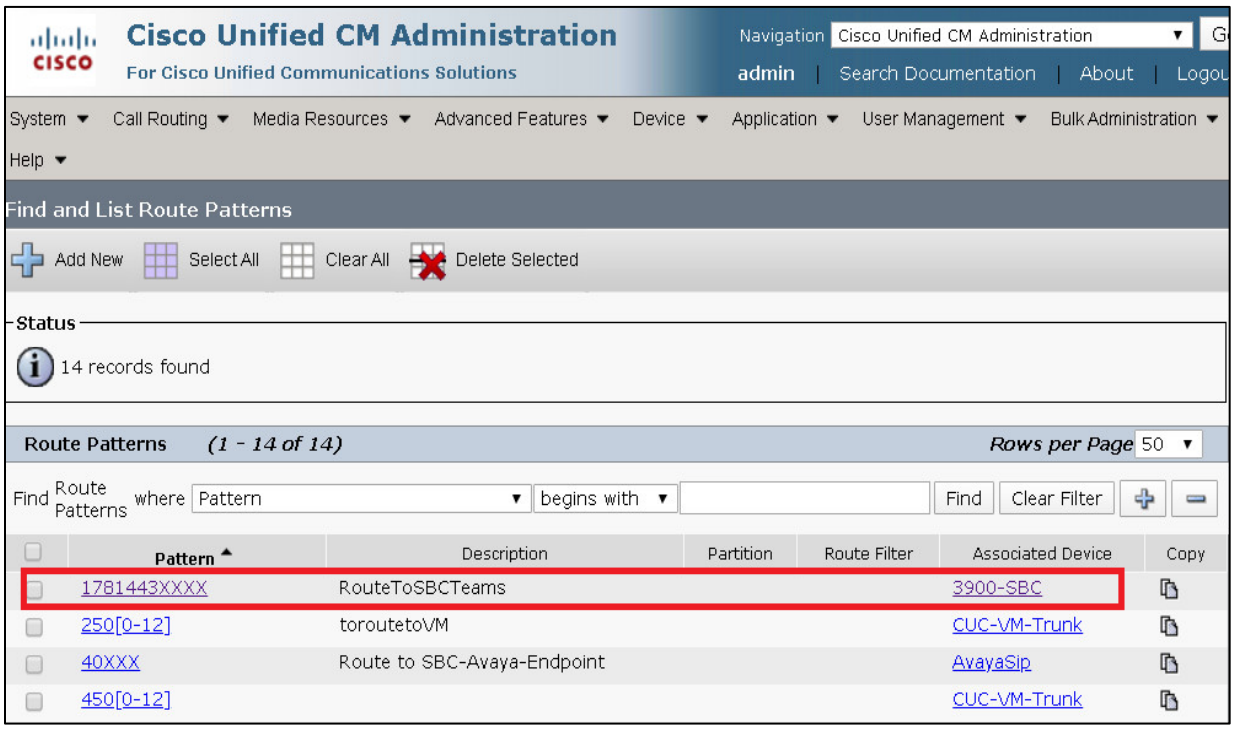

Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Trunk Configuration
Related Links: Back To Find/List Go
Save
Status
Status: Ready
Device Information
Product: SIP Trunk
Device Protocol: SIP
Trunk Service Type None(Default)
Device Name 3900-SBC
Description 3900-SBC
Device Pool* Default
Common Device Configuration < None >
Call Classification* Use System Default
Media Resource Group List < None >
Location* Hub_None
AAR Group < None >
Tunneled Protocol* None



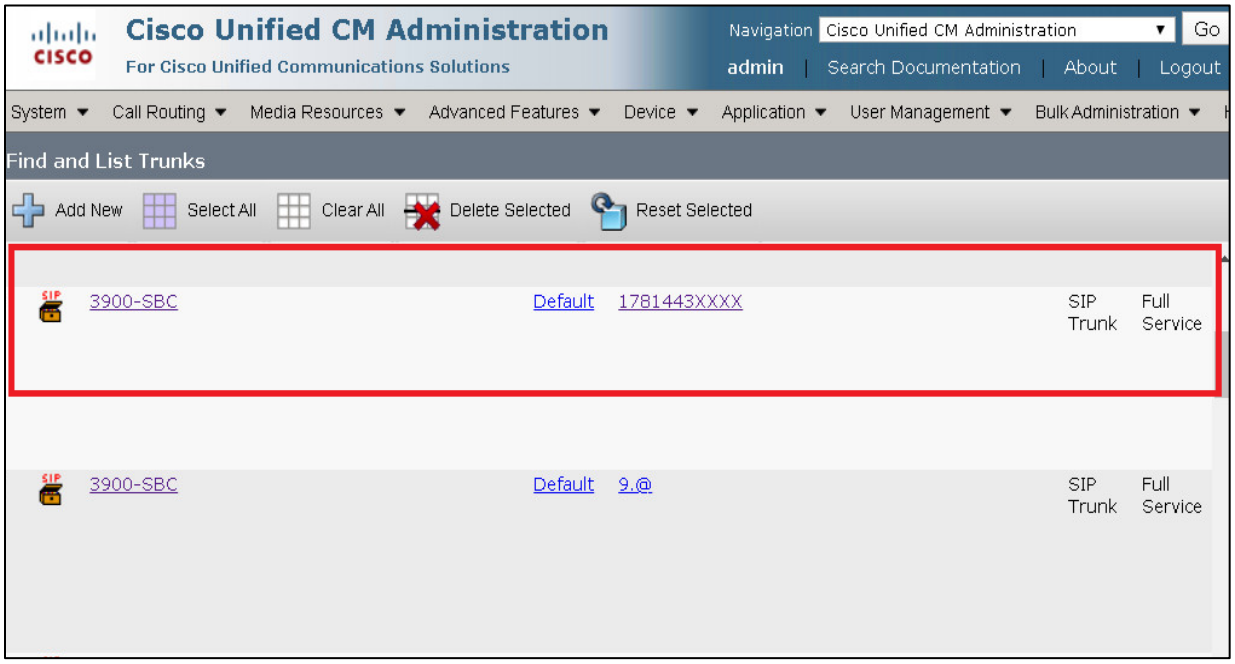
4.2. Configure a new Route Pattern

01) Go to Call Routing ------ Route/Hunt ------ Route Pattern and click Add New
02) Enter a Route Pattern according to the network requirements and calling plan.
03) From the Gateway/Route List drop-down list, select the created SIP Trunk device name.
04) Click Save.

The route pattern that has been created is shown below:

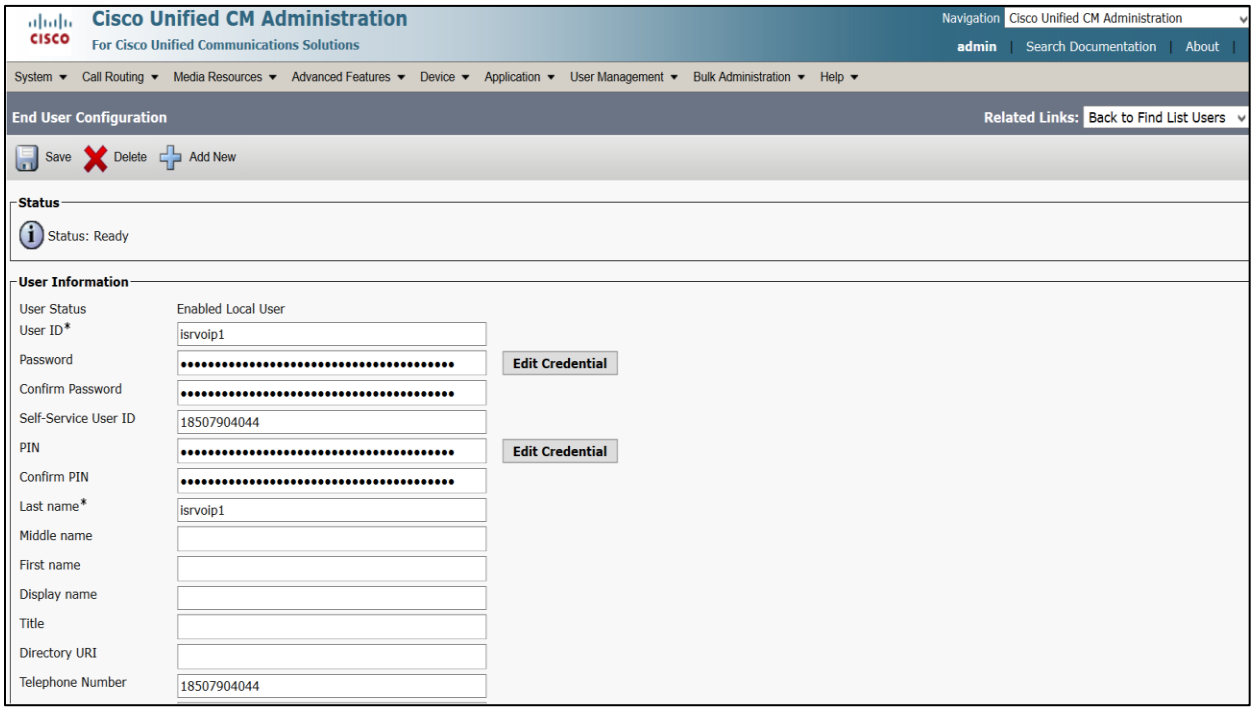


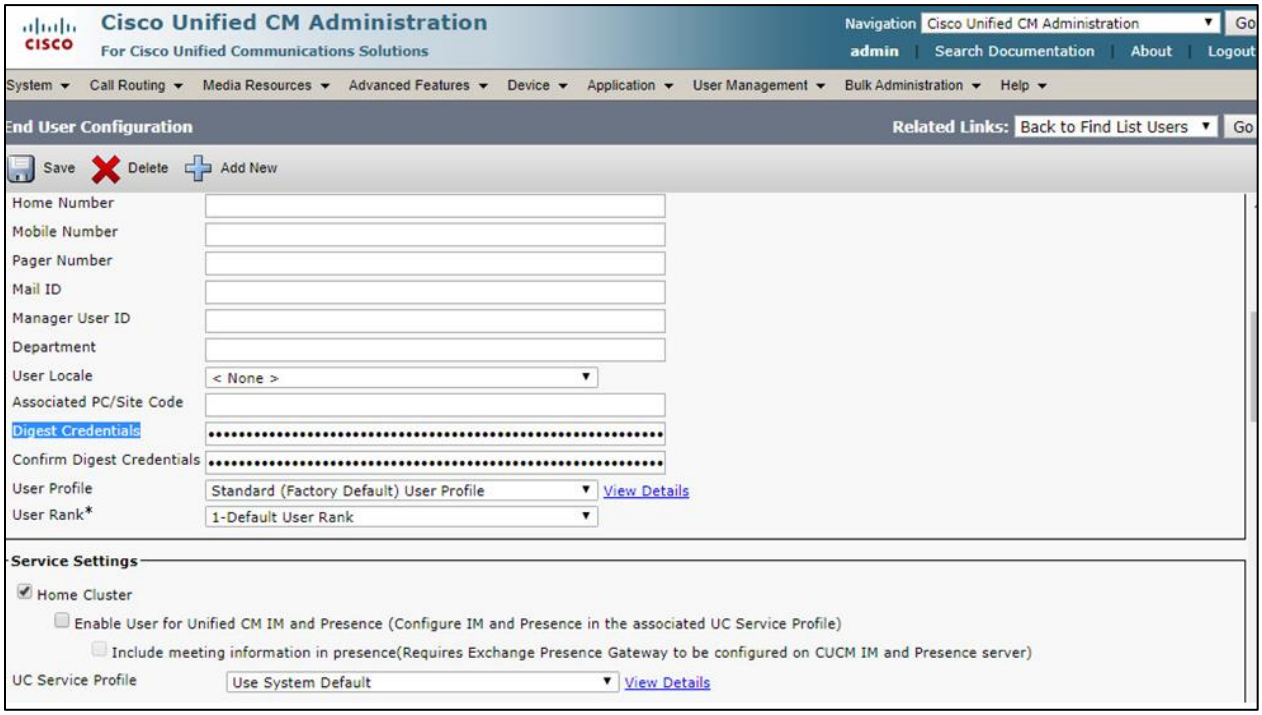
The created SIP trunk associated wuth the route pattern is shown below:



4.3. End User Configuration

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

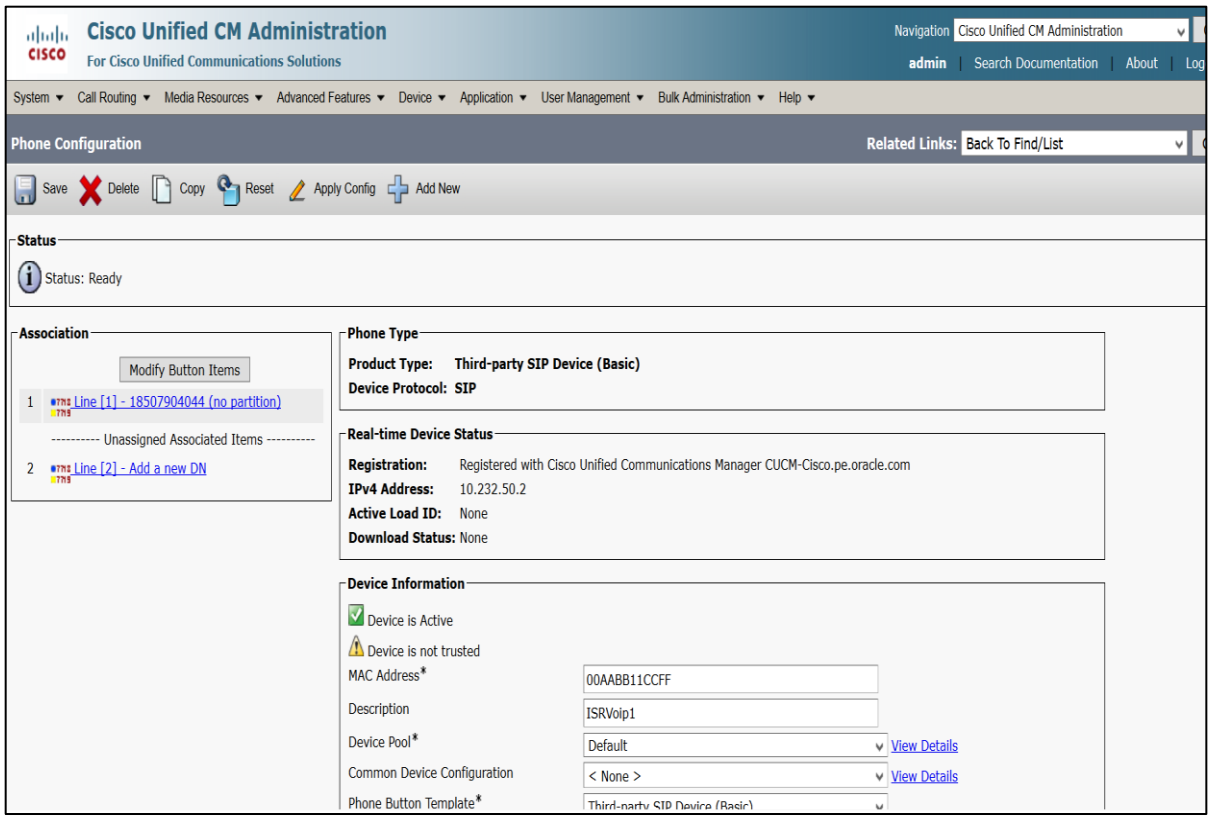


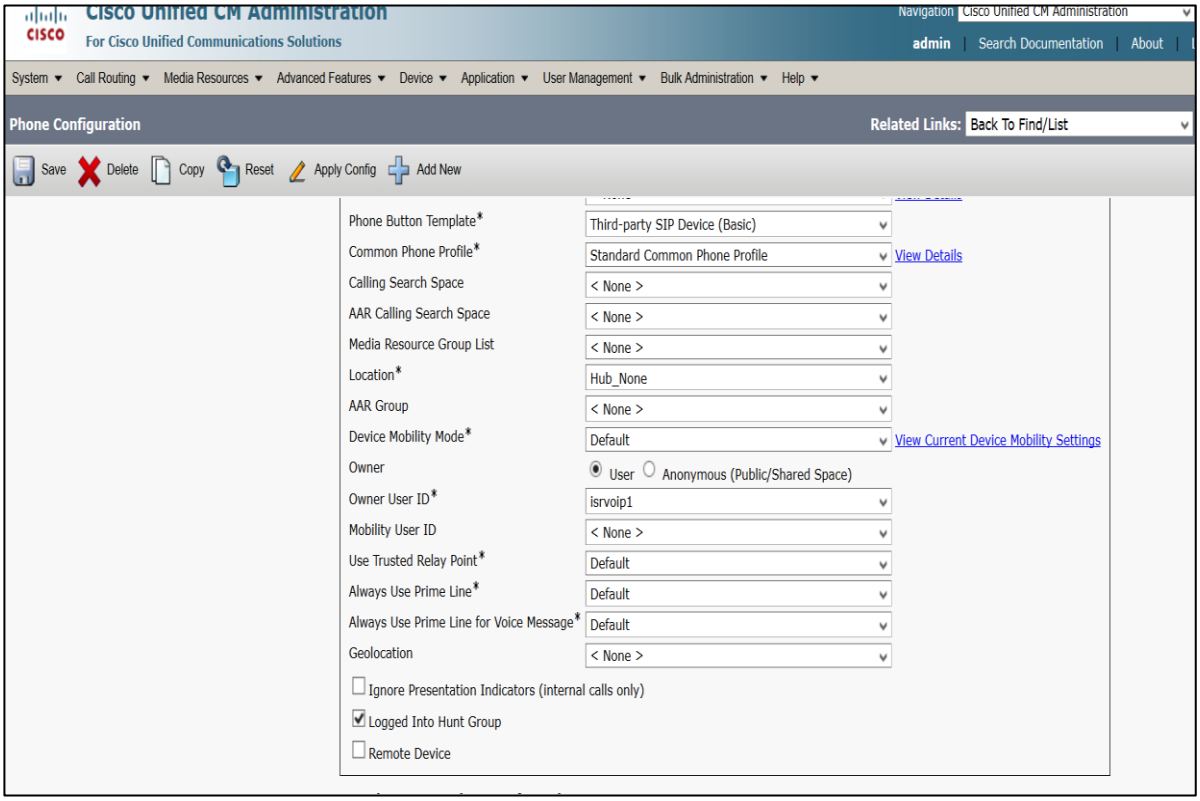


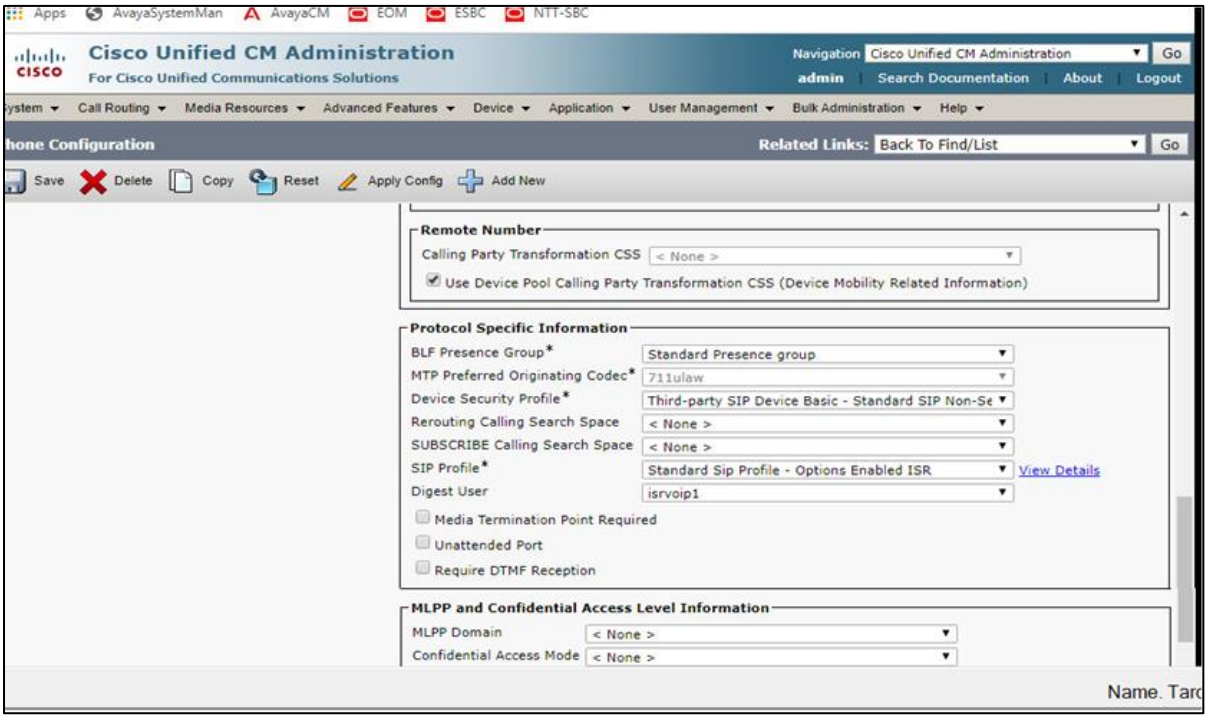
4.4. Adding SIP Phone in CUCM

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

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



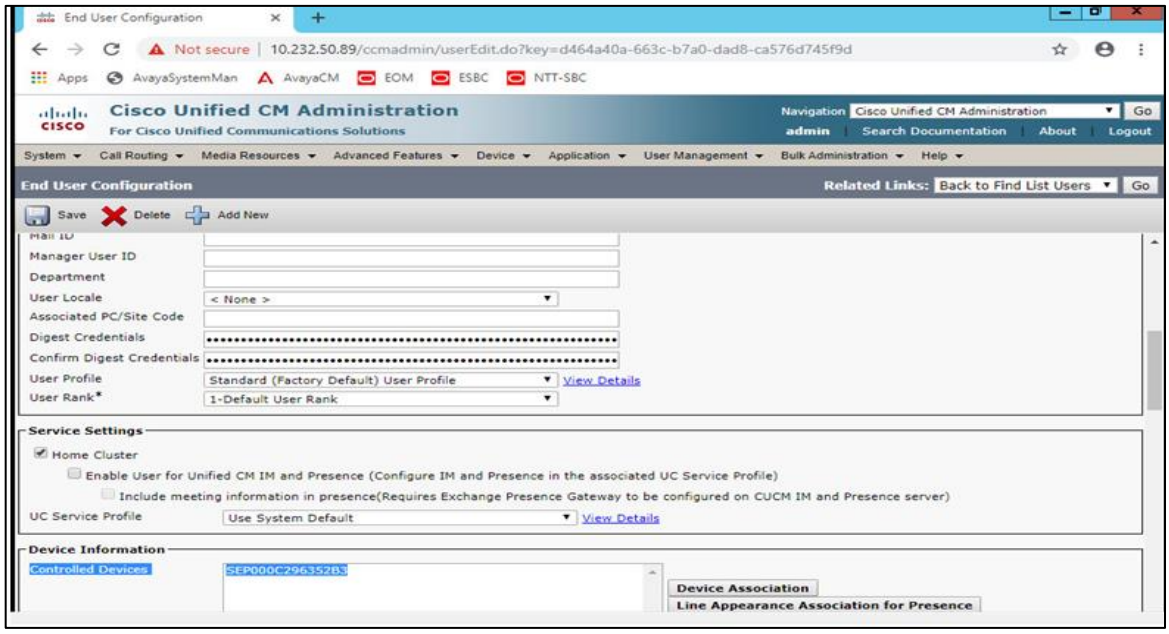

Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
admin | Search Documentation | About
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Phone Configuration
Related Links: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


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

4.5. Associating End User to Phone

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

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



With these steps, the CUCM configuration is complete.

5. Requirements to Configure Microsoft Teams Direct Routing

If you are planning to configure direct routing with Oracle SBC, you must ensure that the following prerequisites are completed before proceeding further

- Tenant requirements
- Licensing and other requirements
- SBC domain names
- Public trusted certificate for the SBC
- SIP Signaling: FQDNs

5.1. Tenant Requirements

Make sure that you have a custom domain on your O365 tenant. Here we have created an account soladmin@solutionslab.onmicrosoft.com.

Likewise create an account, which is not the default domain created for your tenant. For more information https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sbc-domain-names

5.2. Licensing Requirements

Make sure that the following license requirements are met by the Direct routing users.(ie the users must be assigned the following licenses in Office 365)

- Microsoft Phone System
- Microsoft Teams + Skype for Business Plan 2 if included in Licensing SKU

5.3. DNS Requirements

Create DNS records for domains in your network that resolve to your SBC.
Before you begin, make sure that you have the following per every SBC you want to pair:

- Public IP address
- FQDN name resolving to the Public IP address

5.4. SBC Domain Names

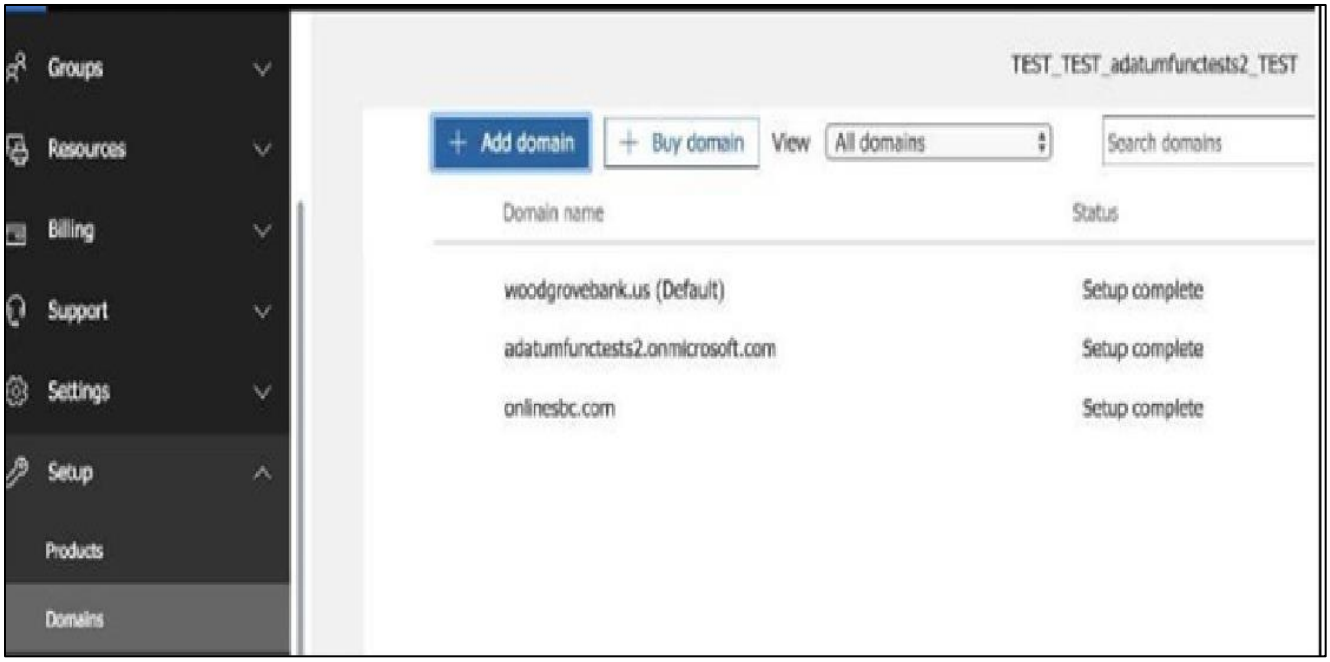
The SBC domain name must be from one of the names registered in “Domains” of the tenant.
You cannot use the *.onmicrosoft.com tenant for the domain name.

For example, on the picture below, the administrator registered the following DNS names for the tenant:

DNS Name	Can be used for SBC FQDN	Examples of FQDN names
woodgrovebank.us	Yes	Valid names: • sbc1.woodgrovebank.us; • ussbcs15.woodgrovebank.us • europe.woodgrovebank.us Non-Valid name: • sbc1.europe.woodgrovebank.us (requires registering domain name europe.atatum.biz in “Domains” first)
woodgrovebankus.onmicrosoft.com	No	Using *.onmicrosoft.com domains is not supported for SBC names

hybrdvoice.org	Yes	Valid names: • sbc1. hybridvoice.org • ussbcs15. hybridvoice.org • europe. hybridvoice.org Non-Valid name: • sbc1.europe.hybridvoice.org (requires registering domain name europe. hybridvoice.org in "Domains" first)

Please activate and register the domain of tenant.



In this document the following FQDN and IP is used as an example:

Public IP	FQDN Name
155.212.214.172	oracleesbc2.woodgrovebank.us

5.5. Public trusted certificate for the SBC

It is necessary to setup a public trusted certificate for direct routing. This certificate is used to establish TLS connection between Oracle SBC and MS Teams. The certificate needs to have the SBC FQDN in the subject, common name, or subject alternate name fields.

For root certificate authorities used to generate SBC certificate, refer Microsoft documentation.

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

6. Configure Teams Direct Routing

The SBC has to be paired with the direct routing interface for direct routing to work. To achieve this follow the below steps

6.1. Establish a remote PowerShell session

The first step is to download Microsoft PowerShell.
For more information and downloading the client, visit Microsoft's website

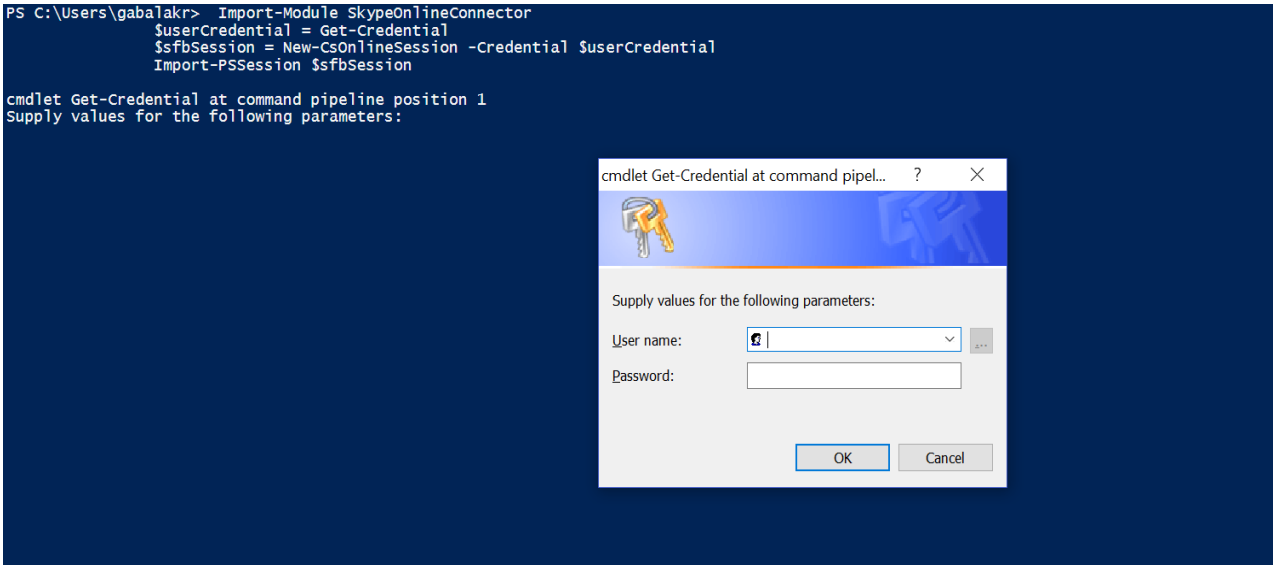
https://docs.microsoft.com/en-us/SkypeForBusiness/set-up-your-computer-for-windows-powershell/set-up-your-computer-for-windows-powershell.

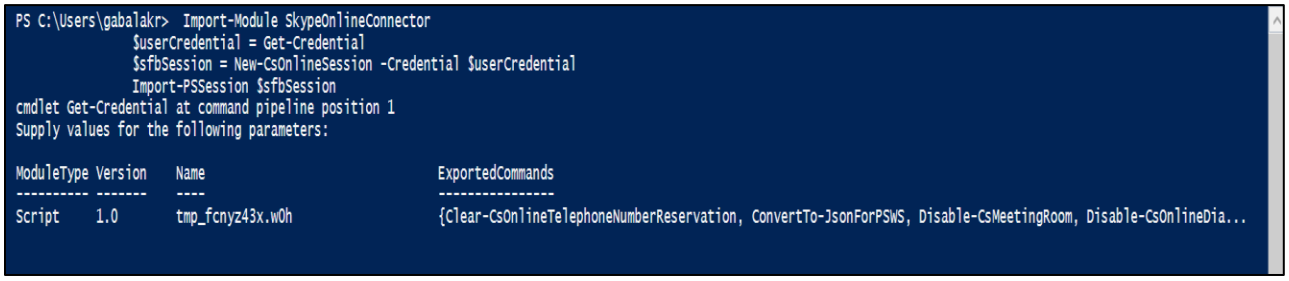
To establish a remote connection, follow the below steps
Open PowerShell and type in the below commands

- Import-Module SkypeOnlineConnector
- $userCredential = Get-Credential
- $sfbSession = New-CsOnlineSession -Credential $userCredential
- Import-PSSession $sfbSession

```
PS C:\Users\gabalakr> Import-Module SkypeOnlineConnector
                      $userCredential = Get-Credential
                      $sfbSession = New-CsOnlineSession -Credential $userCredential
                      Import-PSSession $sfbSession
```

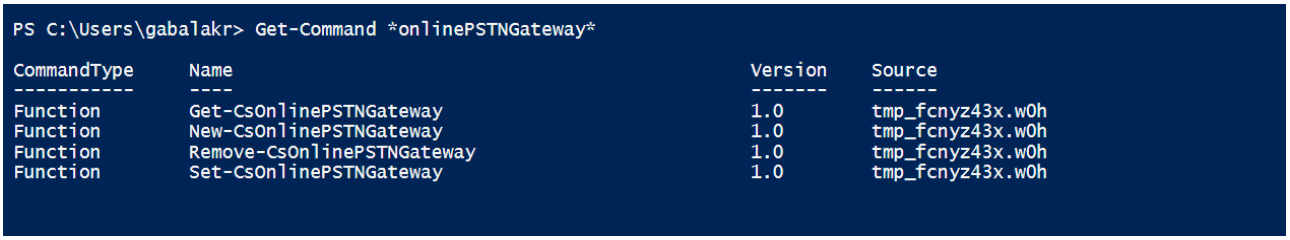
PowerShell prompts for a username and password. Enter the tenant username and password. Tenants are used in pairing the SBC with the direct routing interface.





Now the remote connection is established.
Check whether the remote connection is proper by using the below command
“Get-Command *onlinePSTNGateway*”

The command will return the four functions shown here that will let you manage the SBC.



6.2. Pair the SBC to the tenant

To pair SBC to the tenant, type the command as shown below. Here the FQDN used is oraclesbc.woodgrovebank.us

New-CsOnlinePSTNGateway -Fqdn <SBC FQDN> -SipSignallingPort <SBC SIP Port> -MaxConcurrentSessions <Max Concurrent Sessions the SBC can handle> -Enabled $true

For more information ,please visit the Microsoft documentation here:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure#connect-to-skype-for-business-online-by-using-powershell

```
PS C:\WINDOWS\system32> New-CsOnlinePSTNGateway -Fqdn oracleesbc2.woodgrovebank.us -SipSignallingPort 5061 -MaxConcurrentSessions 500 -MediaBypass $true
```

After pairing, we can check whether the SBC is present in the list of paired SBC's by typing in the command:

Get-CsOnlinePSTNGateway -Identity oracleesbc2.woodgrovebank.us

The details of the gateway are listed when the above command is entered.

Verify whether the enabled parameter is set to true.
The OPTIONS ping from the SBC is now responded with 200OK.
Once there are incoming options to the direct routing interface, it starts sending OPTIONS to the SBC.

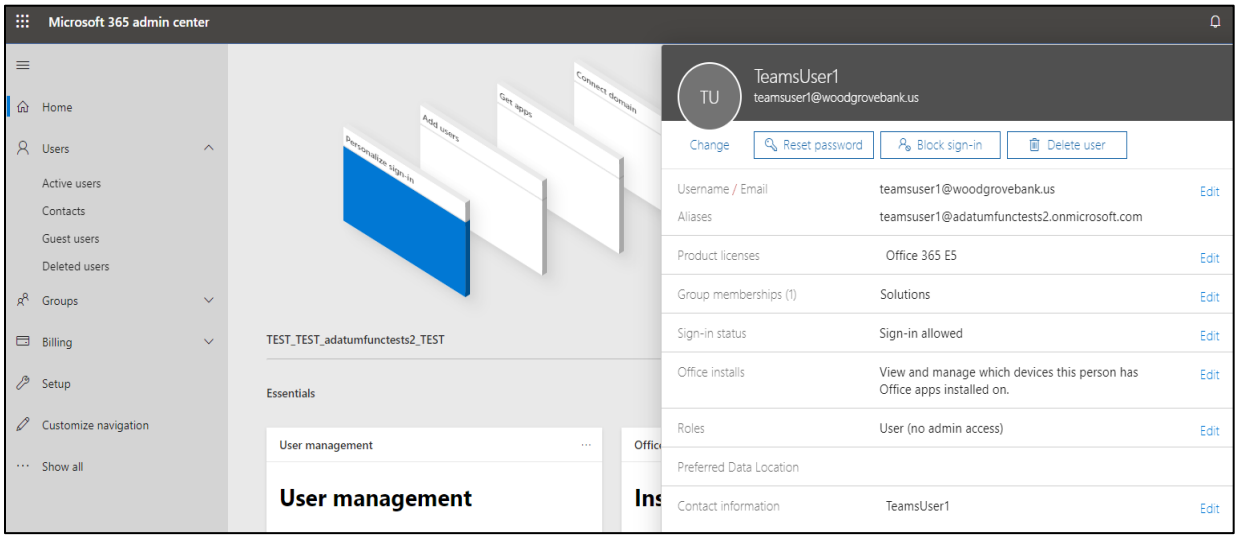
```
Identity                          : oracleesbc2.woodgrovebank.us
Fqdn                              : oracleesbc2.woodgrovebank.us
SipSignallingPort                 : 5061
FailoverTimeSeconds               : 10
ForwardCallHistory                : True
ForwardPai                        : True
SendSipOptions                    : True
MaxConcurrentSessions             :
Enabled                           : True
MediaBypass                       : True
GatewaySiteId                     :
GatewaySiteLbrEnabled             : False
FailoverResponseCodes             : 408,503,504
GenerateRingingWhileLocatingUser  : True
PidfLoSupported                   : False
MediaRelayRoutingLocationOverride :
ProxySbc                          :
BypassMode                        : None
```

6.3. Enable Users for Direct Routing.

To add users, create a user in Office 365 and assign a license. Here the following user is created: teamsuser1@woodgrovebank.us

Here the following license is added

- Office 365 Enterprise E5 (including SfB Plan2, Exchange Plan2, Teams, and Phone System)



Verify whether the user is homed in Skype for business Online by issuing the below command in PowerShell

“Get-CsOnlineUser -Identity "<User name>" | fl RegistrarPool”

Here the “infra.lync.com” verifies that the user is homed.

```
PS C:\WINDOWS\system32> Get-CsOnlineUser -Identity teamsuser1 | fl RegistrarPool

RegistrarPool : sippoolsn23a15.infra.lync.com
```

6.4. Assign a phone number to the User

After creating a user, a phone number and voice mail has to be assigned through Powershell. Enter the below command for assigning a phone number.

Set-CsUser -Identity "<User name>" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI tel:<E.164 phone number>

```
PS C:\WINDOWS\system32> set-CSuser -Identity teamsuser1 -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI tel:+17814437383
```

The phone number used has to be configured as a full E.164 phone number with country code.

6.5. Configure Voice Routing

Voice Routing is performed by the direct routing Interface based on the following elements

- Voice Routing Policy
- PSTN Usages
- Voice Routes
- Online PSTN Gateway

Here is an example to configure routes, PSTN usage, voice routing policy and assigning the policy to user.

1. Create the PSTN Usage "US and Canada".

```
PS C:\Users\gabalakr> Set-CsOnlinePstnUsage -Identity Global -Usage @{Add="US and Canada"}
```

2. Verify this by executing the command below

```
PS C:\Users\gabalakr> Get-CSOnlinePSTNUsage

Identity : Global
Usage    : {US and Canada}


PS C:\Users\gabalakr>
```

3. Configure voice route as shown below. Here all calls are routed to the same SBC.

   This is achieved by using -NumberPattern ".*"Set-CsOnlineVoiceRoute -id "Bedford 1"
   - NumberPattern ".*" -OnlinePstnGateway List oracleesbc2.woodgrovebank.us–Priority 1

```
PS C:\WINDOWS\system32> Set-CSOnlineVoiceRoute -id "Oracle_US" -NumberPattern ^(\+1[0-9]{10})$ -OnlinePstnGatewayList oracleesbc2.woodgrovebank.us -Priority 1
```

4. Verify the configuration by typing in the following command Get-CsOnlineVoiceRoute

```
Identity              : Oracle_US
Priority              : 3
Description           :
NumberPattern         : ^(\+1[0-9]{10})$
OnlinePstnUsages      : {Oracle_US}
OnlinePstnGatewayList : {sbc2.customers.telechat.o-test06161977.com, oracleesbc2.woodgrovebank.us}
Name                  : Oracle_US
```

5. Create a Voice Routing Policy "US Only" and add to the policy the PSTN Usage "US and Canada.".Use the following command

New-CsOnlineVoiceRoutingPolicy "US Only" -OnlinePstnUsages "US and Canada"

This can be verified through the following command.

```
PS C:\Users\gabalakr> Get-CsOnlineVoiceRoutingPolicy


Identity            : Global
OnlinePstnUsages    : {}
Description         :
RouteType           :

Identity            : Tag:US Only
OnlinePstnUsages    : {US and Canada}
Description         :
RouteType           : BYOT
```

6. Grant to user teamsuser1 a voice routing policy by using PowerShell

```
PS C:\WINDOWS\system32> Grant-CsOnlineVoiceRoutingPolicy -Identity "teamsuser1" -PolicyName "US Only"
```

7. Validate the same using the PowerShell command as shown below

```
PS C:\Users\gabalakr> Get-CsOnlineVoiceRoutingPolicy

Identity          : Global
OnlinePstnUsages  : {}
Description       :
RouteType         :

Identity          : Tag:US Only
OnlinePstnUsages  : {US and Canada}
Description       :
RouteType         : BYOT
```

7. Microsoft Teams Direct Routing Interface Characteristics

The Table below contains the technical characteristics of the Direct Routing Interface.

Microsoft, in most cases, uses RFC standards as a guide during the development. However, Microsoft does not guarantee interoperability with SBCs even if they support all the parameters in table 1 due to specifics of implementation of the standards by SBC vendors. Microsoft has a partnership with some SBC vendors and guarantees their device's interoperability with the interface. All validated devices are listed on Microsoft's site. Microsoft only supports the validated devices to connect to Direct Routing Interface. Oracle is one of the vendors who have a partnership with Microsoft.

Ports and IP	SIP Interface FQDN Name	Refer to Microsoft documentation	
	IP Addresses range for SIP interfaces	Refer to Microsoft documentation	
	SIP Port	5061	
	IP Address range for Media	Refer to Microsoft documentation	
	Media port range on Media Processors	Refer to Microsoft documentation	
	Media Port range on the client	Refer to Microsoft documentation	

Transport and Security	SIP transport	TLS	
	Media Transport	SRTP	
	SRTP Crypto Suite	AES_CM_128_HMAC_SHA1_ 80, non-MKI	DTLS-SRTP is not supported
Codecs	Control protocol for media transport	SRTCP (SRTCP-Mux recommended)	Using RTCP mux helps reduce number of required ports
	Supported Certification Authorities	Refer to Microsoft documentation	
	Transport for Media Bypass	ICE-lite (RFC5245) – recommended, Client also has Transport Relays	
	Audio codecs	• G711 • G722 • Silk (Teams clients) • Opus (WebRTC clients) - Only if Media Bypass is used; • G729	
	Other codecs	• DTMF – Required • Events 0-16 • CN • Required narrowband and wideband • RED – Not required Silence Suppression – Not required	

8. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for interworking with Microsoft Teams Direct Routing Enterprise Model with CUCM.

8.1. Validated Oracle SBC version

Oracle conducted tests with Oracle SBC 8.3 / SBC 9.0 software – this software with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6350
- AP 6300
- AP 3950 (Starting from SBC 9.0 version)
- AP 4900 (Starting from SBC 9.0 version)
- VME

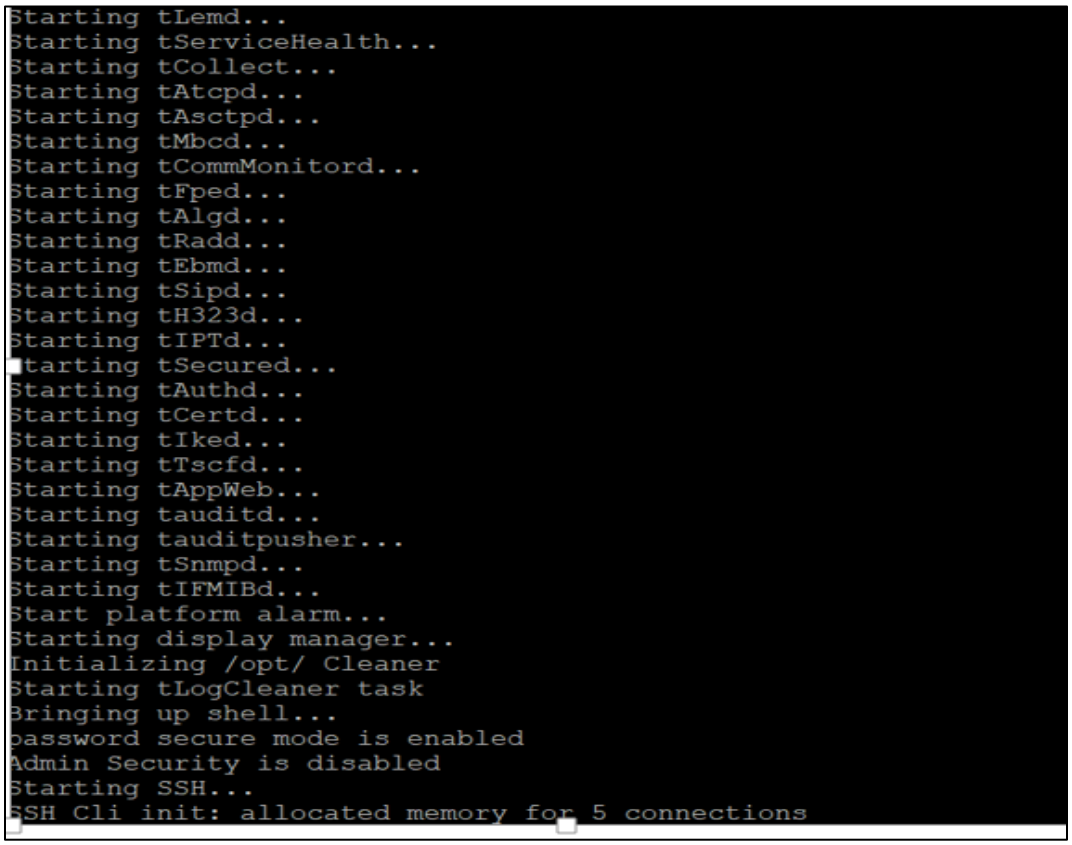
9. New SBC configuration

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

9.1. Establishing a serial connection to the SBC

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

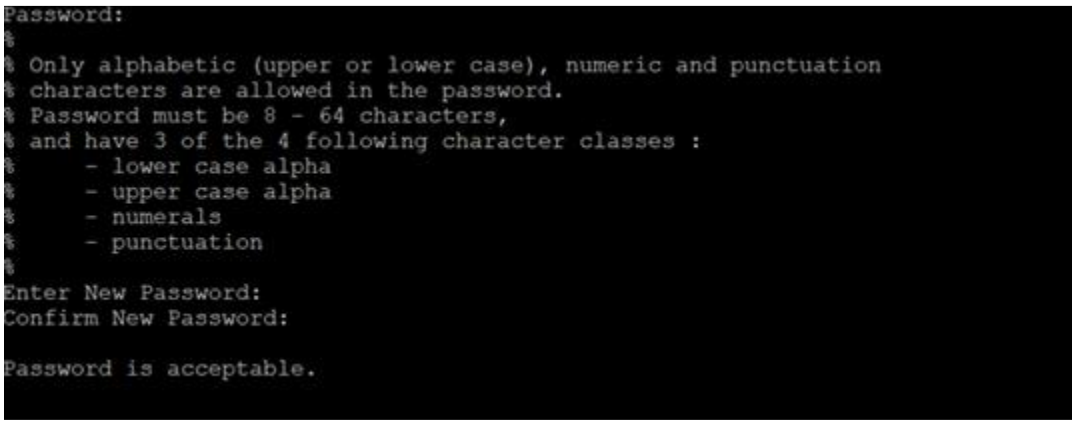
- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None



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

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

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



Now set the management IP of the SBC by setting the IP address in bootparam to access bootparam. Go to Configure terminal->bootparam.

Note: There is no management IP configured by default.

bootparam for 8.3.0 OS

```
NN3900-101# conf t
NN3900-101(configure)# bootparam

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

Boot File               : /boot/nnSCZ830m1p2.bz
IP Address              : 172.18.255.101
VLAN                    : 0
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             : NN3900-101
Console Device          : COM1
Console Baudrate        : 115200
Other                   :

NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.


        ERROR   : space in /boot      (Percent Free: 20)

NN3900-101(configure)#
```

bootparam for 9.0.0 OS

```
NN4600-139# conf t
NN4600-139(configure)# bootparam

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

Boot File               : /boot/nnSCZ900p2.bz
IP Address              : 10.138.194.139
VLAN                    : 0
Netmask                 : 255.255.255.192
Gateway                 : 10.138.194.129
IPv6 Address            :
IPv6 Gateway            :
Host IP                 :
FTP username            : vxftp
FTP password            : ********
Flags                   :
Target Name             : NN4600-139
Console Device          : COM1
Console Baudrate        : 115200
Other                   :

NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.


        ERROR   : space in /boot      (Percent Free: 5)

NN4600-139(configure)#
NN4600-139(configure)#
```

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

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

```
NN3900-101# setup product

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

Last Modified 2019-06-04 11:51:56
----------------------------------------------------------------
 1 : Product       : Enterprise Session Border Controller

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

Enable the features for the ESBC using the setup entitlements command as shown

Save the changes and reboot the SBC.

```
Entitlements for Enterprise Session Border Controller
Last Modified: Never
----------------------------------------------------------------
 1 : Session Capacity                       : 0
 2 :   Advanced                             :
 3 : Admin Security                         :
 4 : Data Integrity (FIPS 140-2)            :
 5 : Transcode Codec AMR Capacity           : 0
 6 : Transcode Codec AMRWB Capacity         : 0
 7 : Transcode Codec EVRC Capacity          : 0
 8 : Transcode Codec EVRCB Capacity         : 0
 9 : Transcode Codec EVS Capacity           : 0
 10: Transcode Codec OPUS Capacity          : 0
 11: Transcode Codec SILK Capacity          : 0

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

  Session Capacity (0-128000)               : 500

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 3

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

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

  Transcode Codec AMR Capacity (0-102375)   : 50

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

    Advanced (enabled/disabled)             : enabled

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

  Transcode Codec OPUS Capacity (0-102375)  : 50

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

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

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

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

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

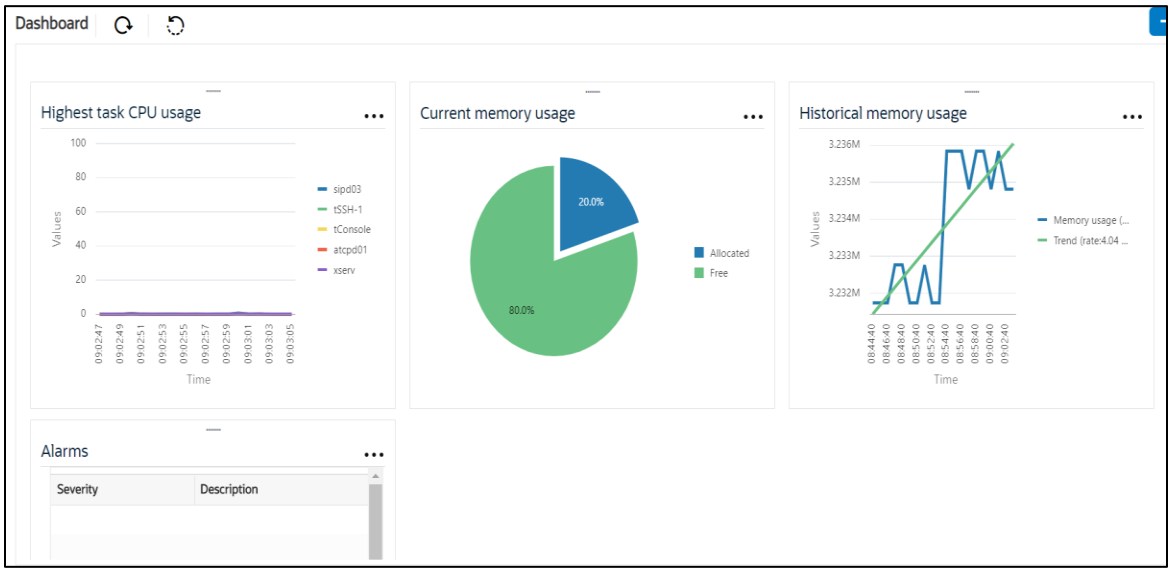
```
NN3900-101(web-server-config)# state enabled
NN3900-101(web-server-config)# done
web-server-config
        state                                   enabled
        inactivity-timeout                      5
        http-state                              enabled
        http-port                               80
        https-state                             disabled
        https-port                              443
        http-interface-list                     GUI
        tls-profile
        last-modified-by                        admin@172.18.0.130
        last-modified-date                      2020-02-20 02:46:51

**NN3900-101(web-server-config)# exit
**NN3900-101(system)# save
**NN3900-101(system)# exit
**NN3900-101(configure)# exit
**NN3900-101# save-config
checking configuration
-------------------------------------------------------------------------------
Results of config verification:
   4 configuration warnings
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'.
*NN3900-101# activate-config
Activate-Config received, processing.
waiting for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
```

9.2. Configure SBC using Web GUI

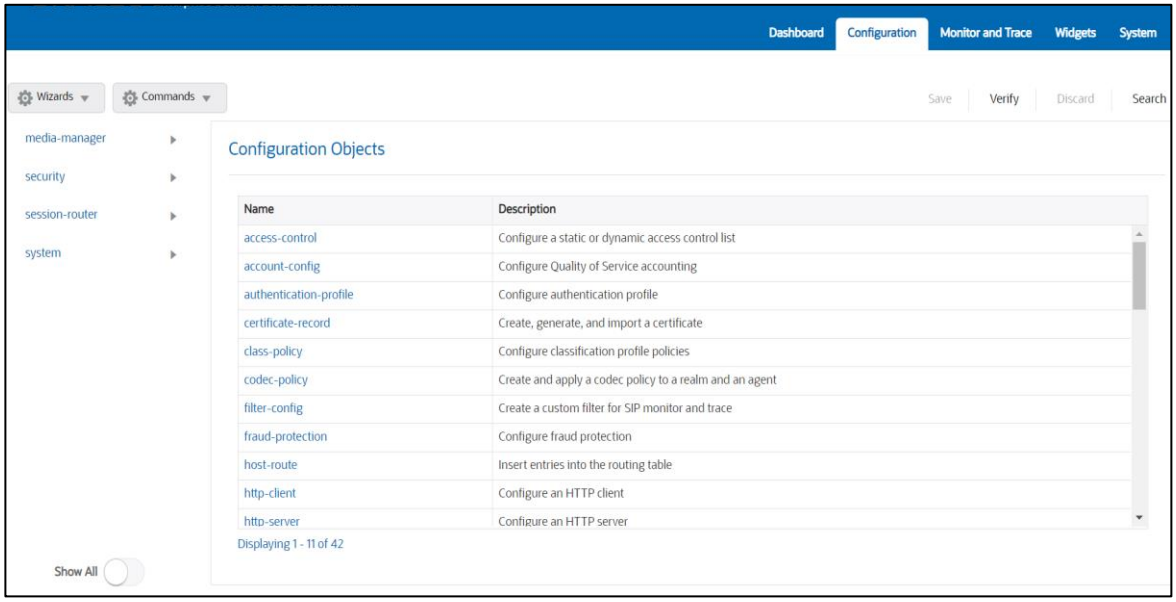
In this app note, we configure SBC using the WebGUI.

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 given below for more information.

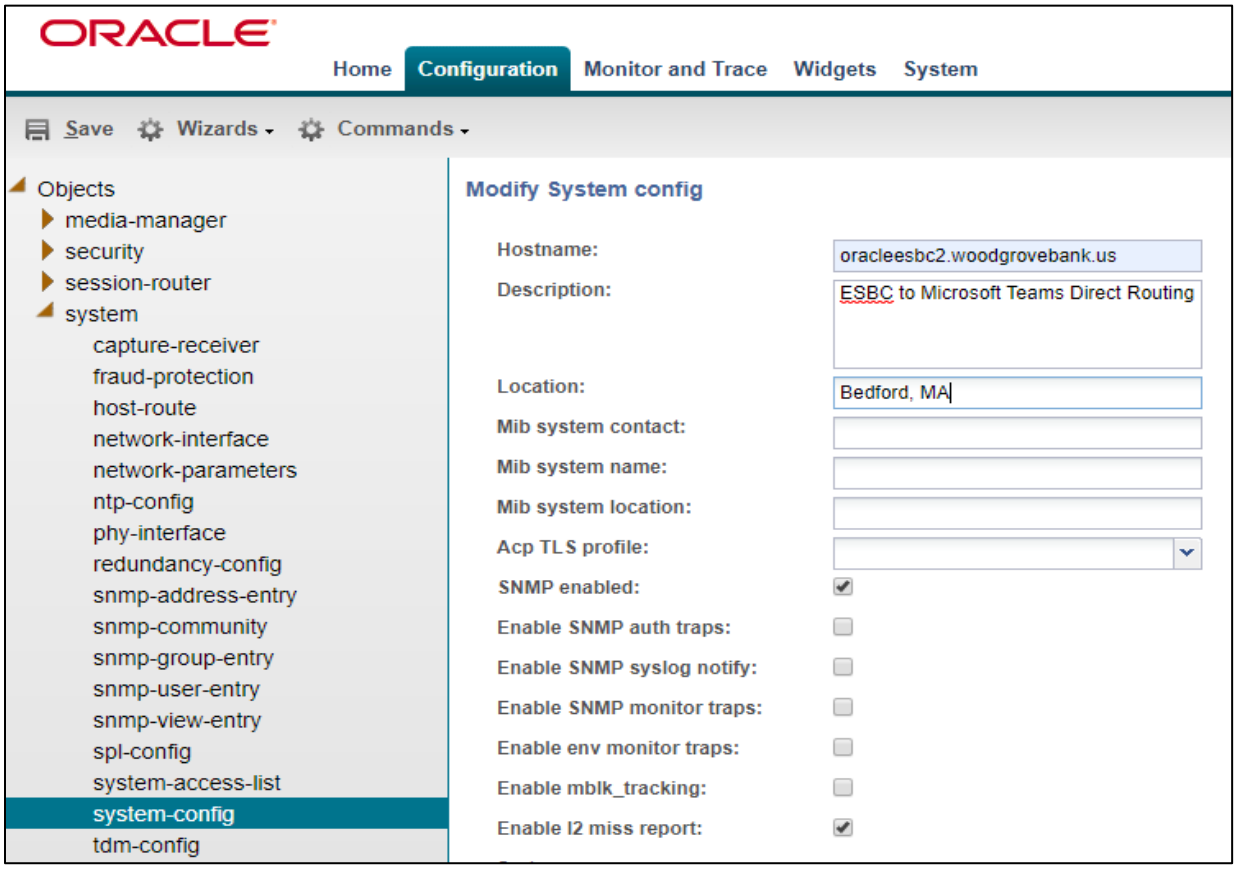
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.0.0/webgui/web-gui-guide.pdf

The expert mode is used for configuration.

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

9.3. 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/en/industries/communications/enterprise-session-border-controller/9.0.0/releasenotes/esbc-release-notes.pdf

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

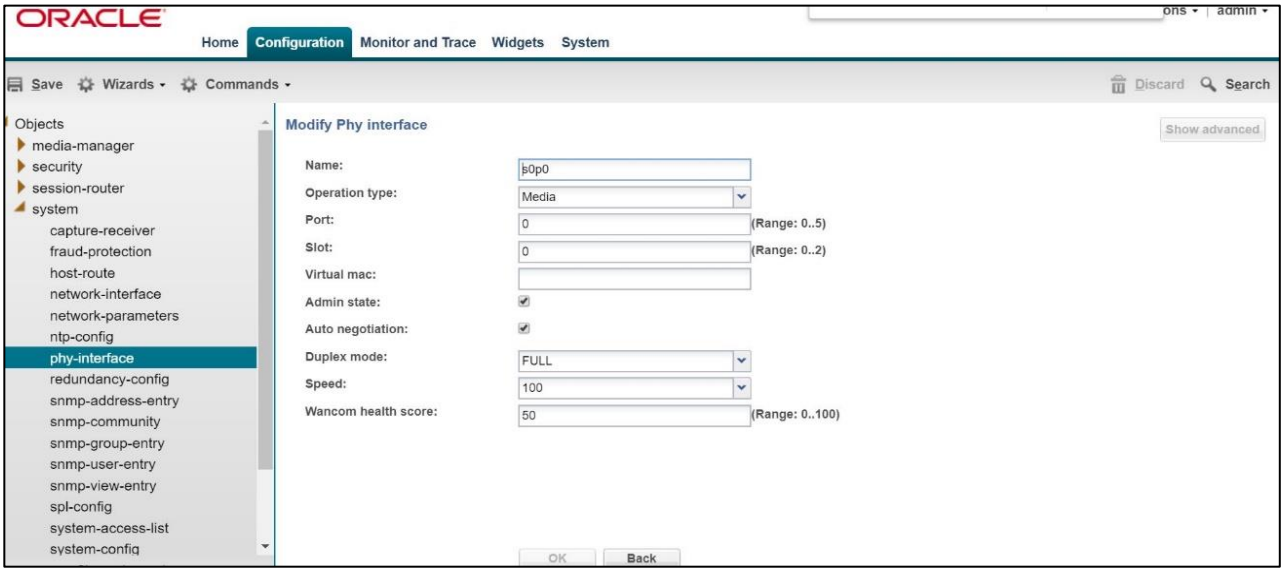
9.4. Configure Physical Interface values

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 (connection to the PSTN gateway) interface.
Teams is configured on the slot 0 port 1. Below is the screenshot for creating a phy-interface on s0p0

Create a similar interface for Teams as well from the Web GUI. The table below specifies the values for both teams and Trunk.

Parameter Name	Trunk(s0p0)	MSTeams(s0p1)
Slot	0	0
Port	0	1
Operation Mode	Media	Media

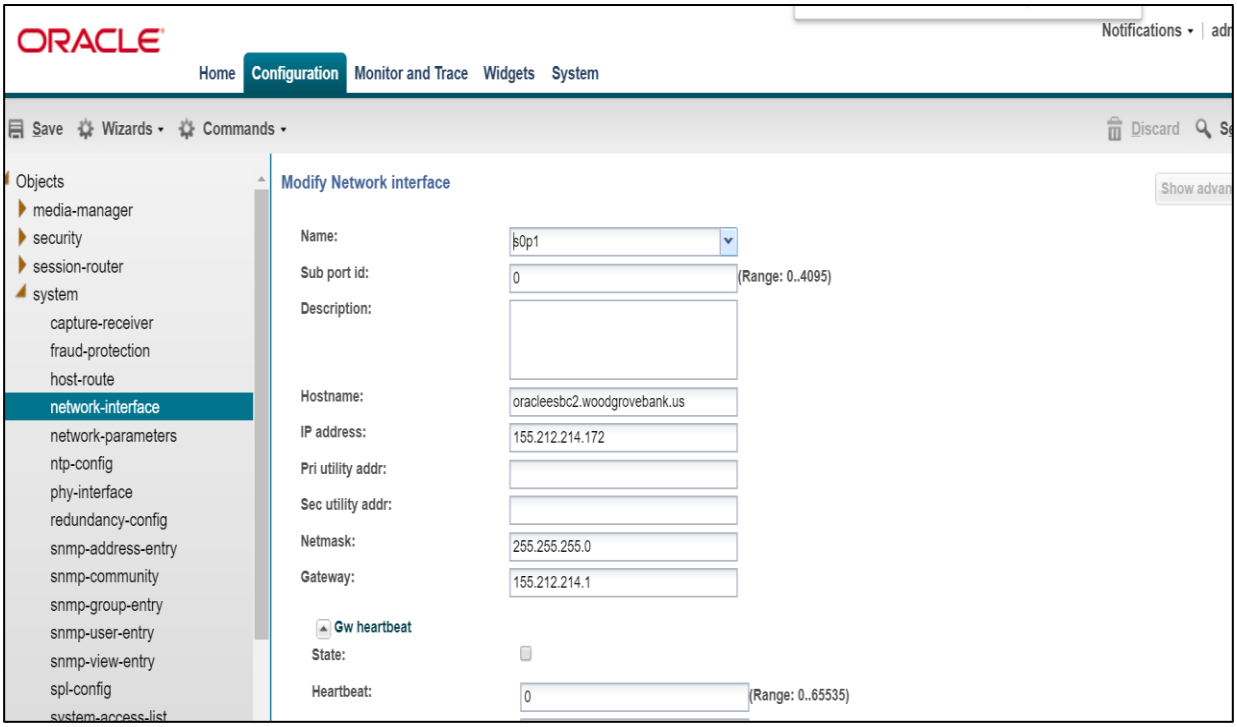


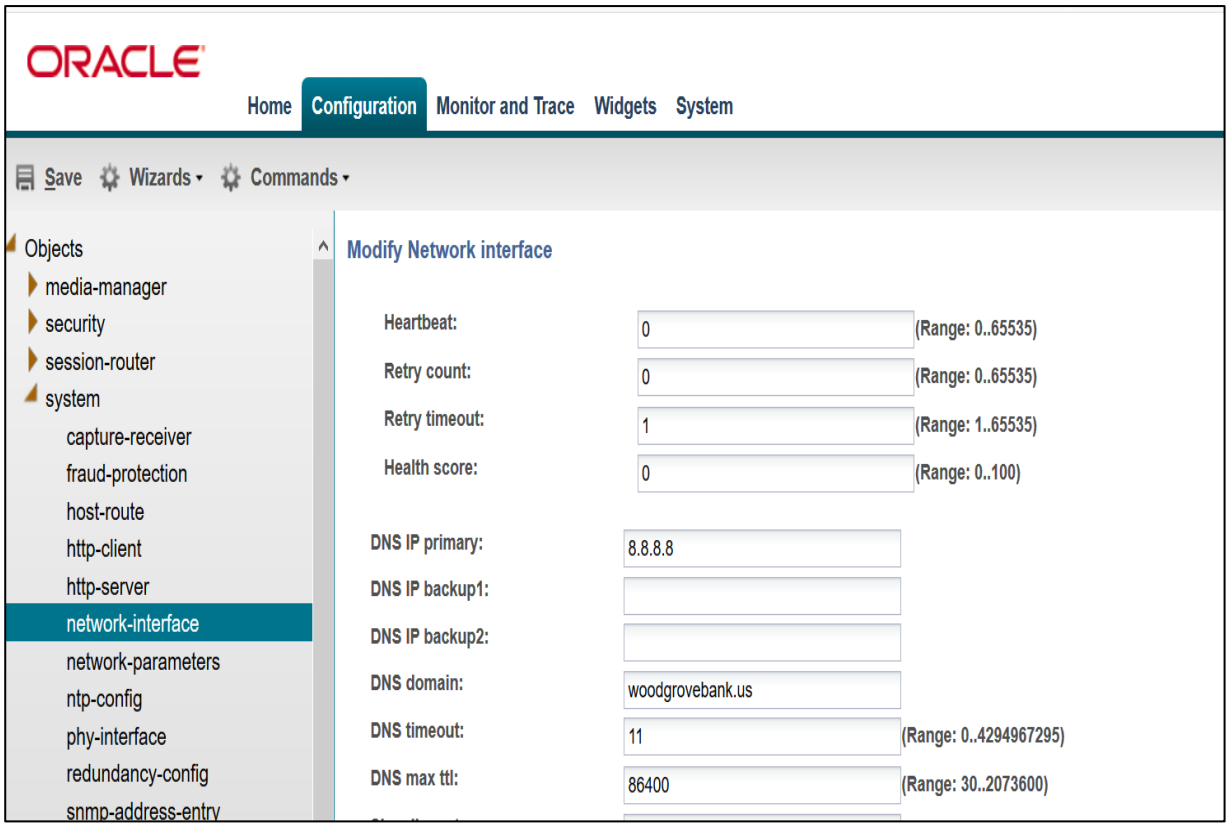
9.5. Configure Network Interface values

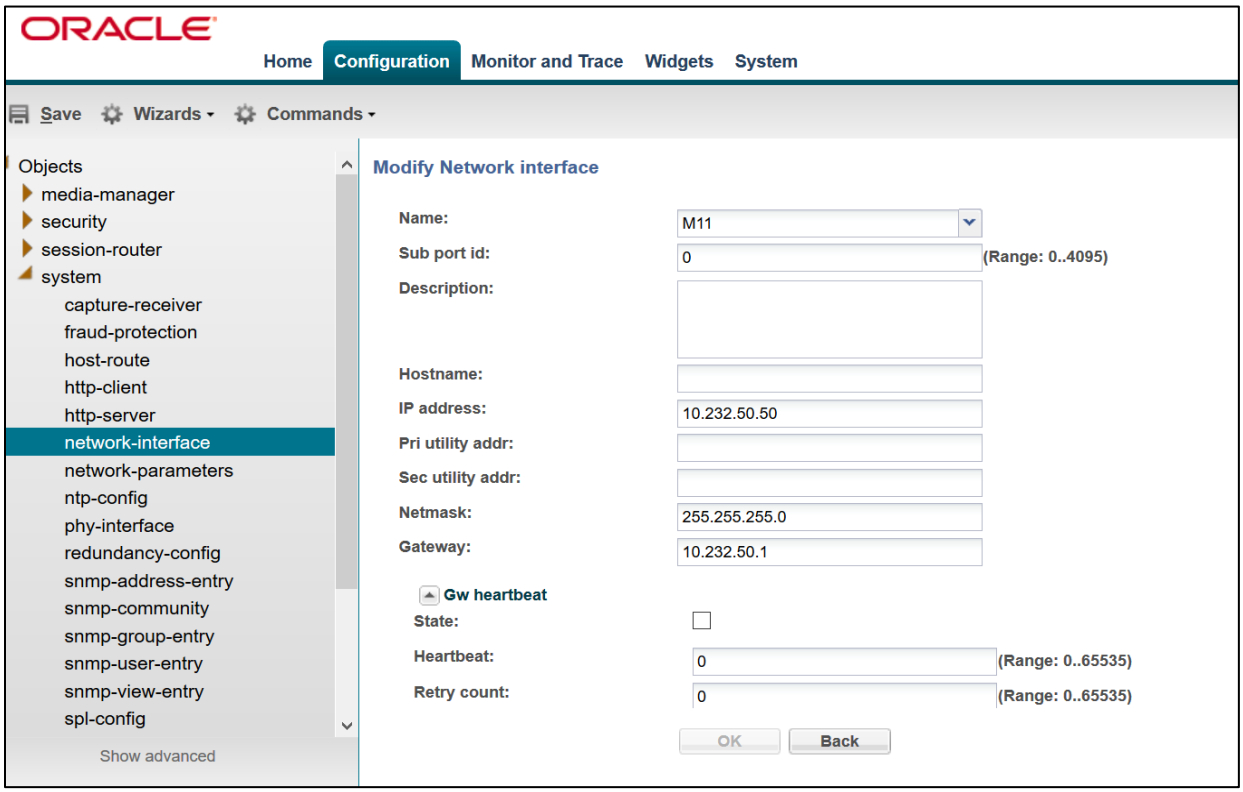
To configure network-interface, go to system->Network-Interface. Configure two interfaces, one for Teams side and one for CUCM side.

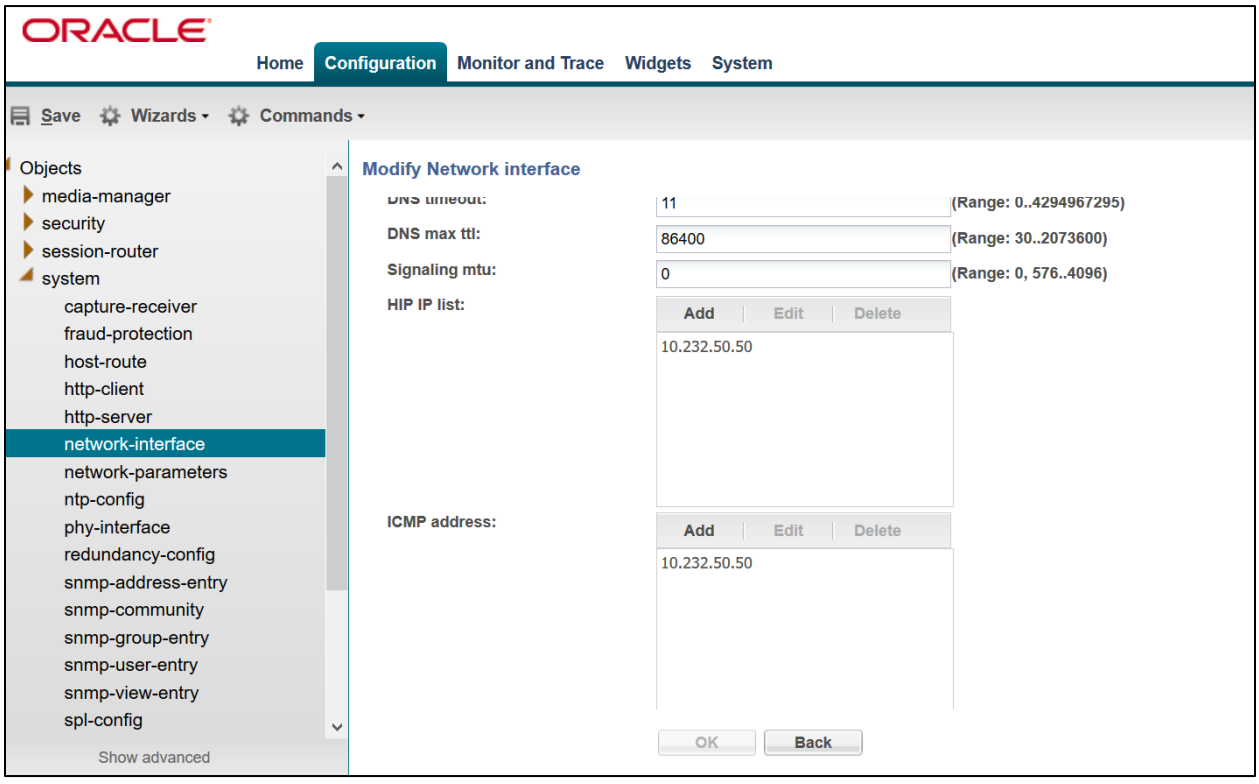
The table below lists the parameters, to be configured for both the interfaces.

Parameter Name	Teams side Network Interface	CUCM side Network interface
Name	s0p0	s1p1
Host Name	oracleesbc2.woodgrovebank.us	
IP address	155.212.214.172	10.232.50.50
Netmask	255.255.255.0	255.255.255.0
Gateway	155.212.214.1	10.232.50.1
DNS-IP Primary	8.8.8.8	
DNS-domain	Woodgrovebank.us	


ORACLE
Notifications
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Discard
Objects
media-manager
security
session-router
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
Modify Network interface
Name: s0p1
Sub port id: 0 (Range: 0..4095)
Description:
Hostname: oracleesbc2.woodgrovebank.us
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)


ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Objects
media-manager
security
session-router
system
capture-receiver
fraud-protection
host-route
http-client
http-server
network-interface
network-parameters
ntp-config
phy-interface
redundancy-config
snmp-address-entry
Modify Network interface
Heartbeat: 0 (Range: 0..65535)
Retry count: 0 (Range: 0..65535)
Retry timeout: 1 (Range: 1..65535)
Health score: 0 (Range: 0..100)
DNS IP primary: 8.8.8.8
DNS IP backup1:
DNS IP backup2:
DNS domain: woodgrovebank.us
DNS timeout: 11 (Range: 0..4294967295)
DNS max ttl: 86400 (Range: 30..2073600)


ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Objects
media-manager
security
session-router
system
capture-receiver
fraud-protection
host-route
http-client
http-server
network-interface
network-parameters
ntp-config
phy-interface
redundancy-config
snmp-address-entry
snmp-community
snmp-group-entry
snmp-user-entry
snmp-view-entry
spl-config
Show advanced
Modify Network interface
Name: M11
Sub port id: 0 (Range: 0..4095)
Description:
Hostname:
IP address: 10.232.50.50
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

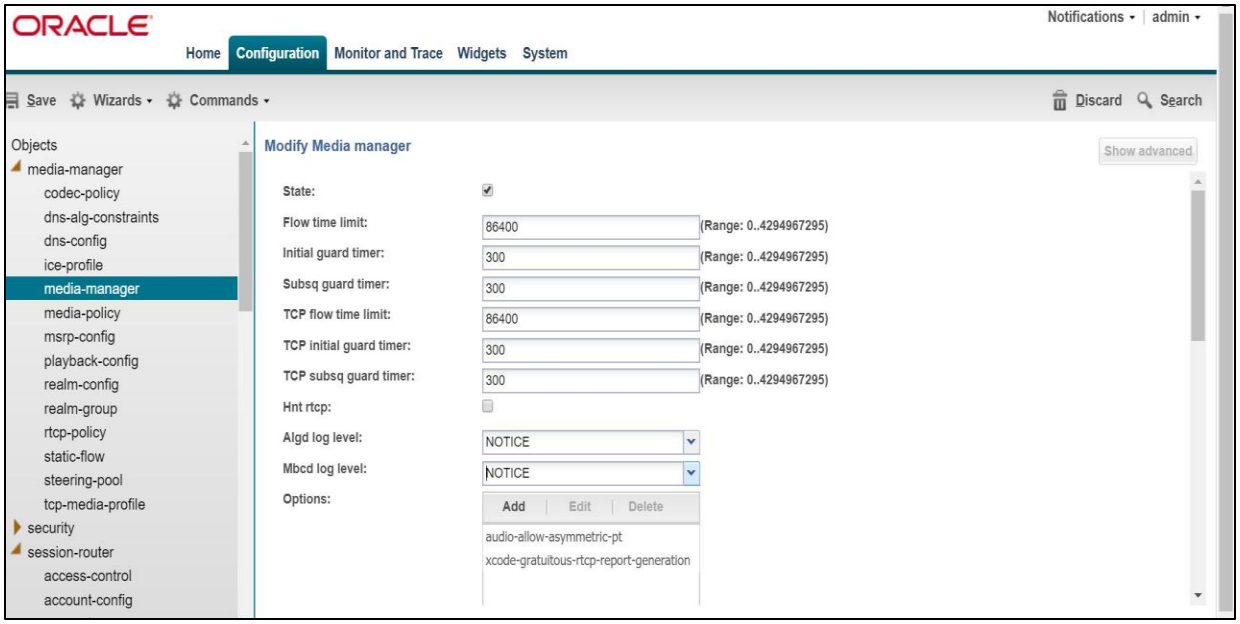

ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Objects
media-manager
security
session-router
system
capture-receiver
fraud-protection
host-route
http-client
http-server
network-interface
network-parameters
ntp-config
phy-interface
redundancy-config
snmp-address-entry
snmp-community
snmp-group-entry
snmp-user-entry
snmp-view-entry
spl-config
Show advanced
Modify Network interface
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
10.232.50.50
ICMP address:
Add
Edit
Delete
10.232.50.50
OK
Back

9.6. 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-gratuitous-rtcp-report-generation

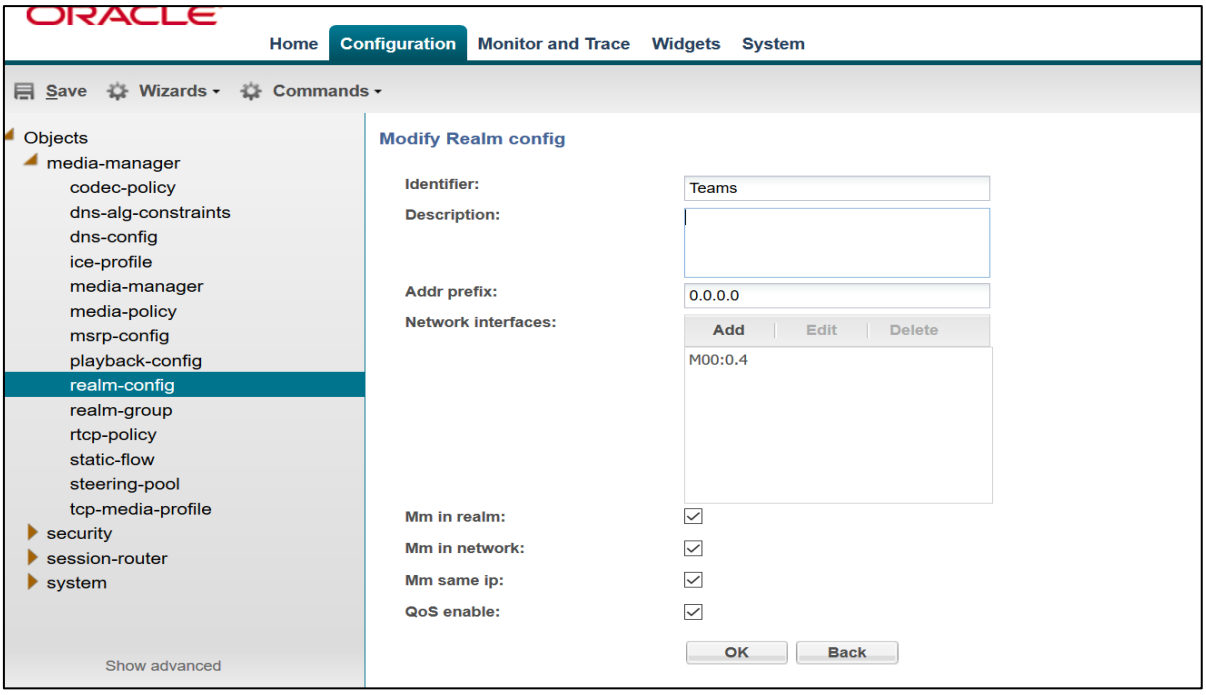
Go to Media-Manager->Media-Manager



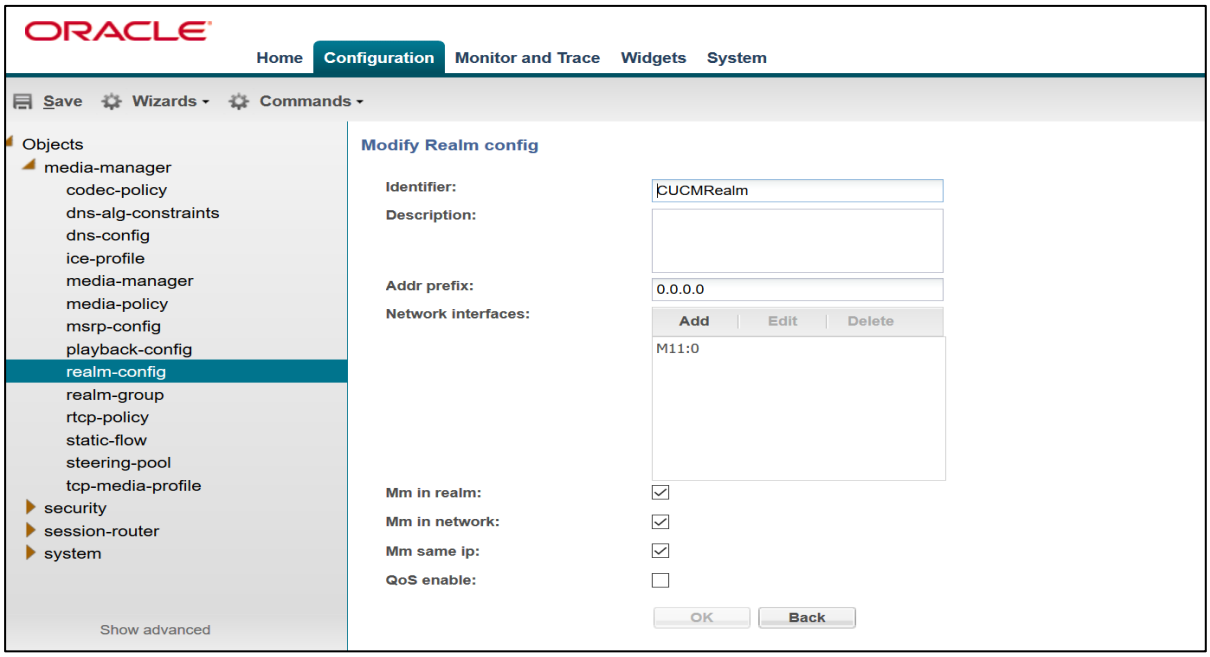
9.7. Configure Realms

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 Teams (SBC to Teams)
Please set “Refer Call Transfer” parameter to Enabled for Teams Realm



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



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

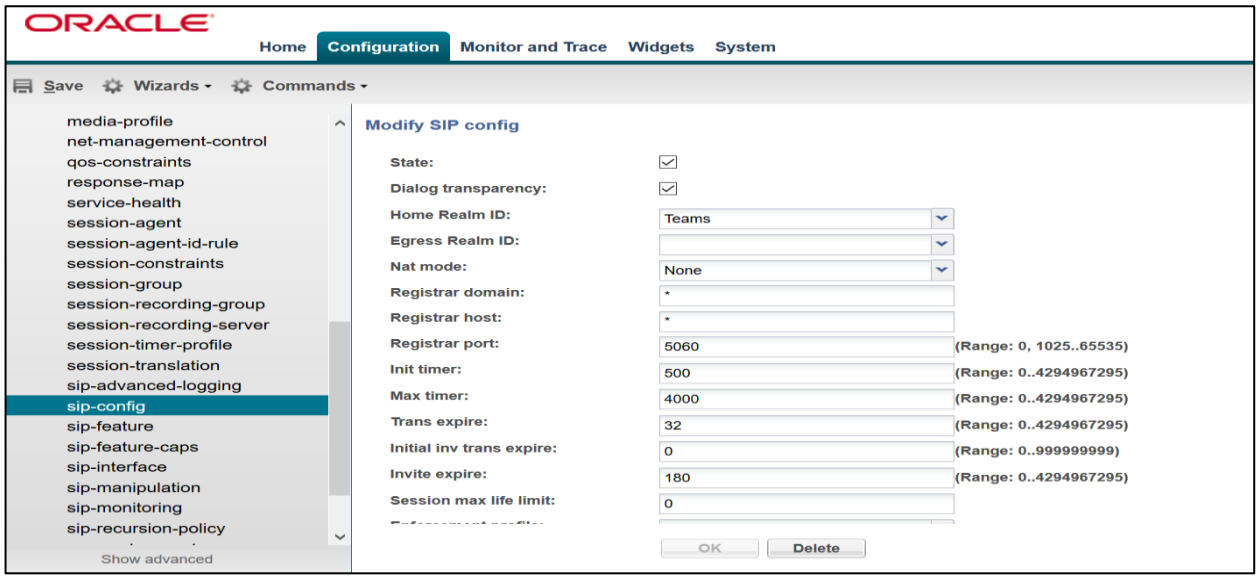
https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/security/security-guide.pdf

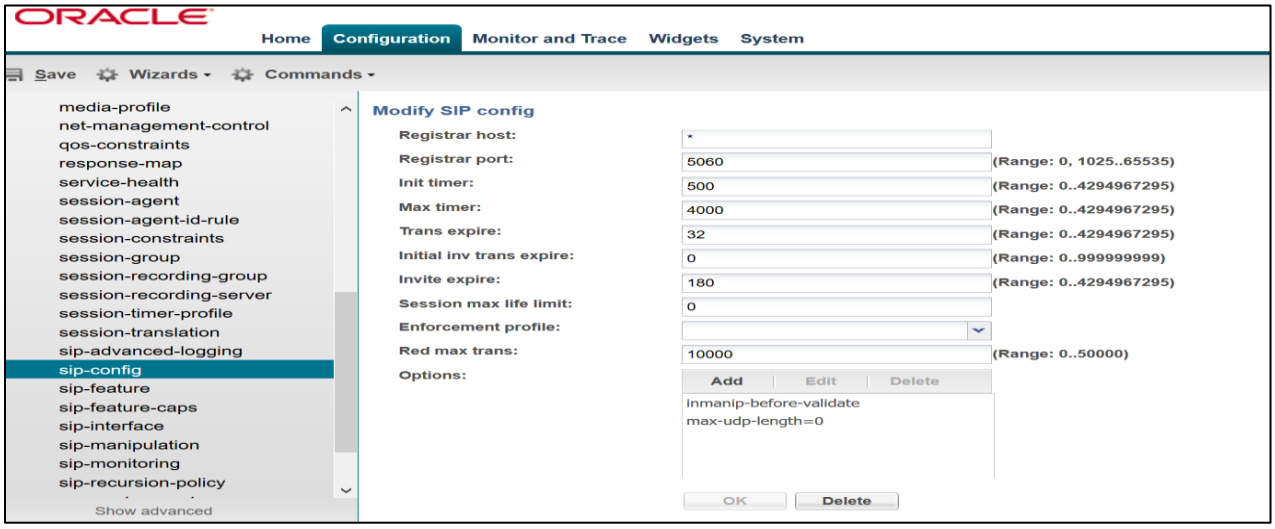
9.8. Enable sip-config

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





9.9. Configuring a certificate for SBC

Microsoft Teams Direct Routing Interface only allows TLS connections from SBCs for SIP traffic with a certificate signed by one of the trusted certification authorities.

For the purposes of this application note, we'll create these certificate records. They are as follows:

- SBC Certificate (end-entity certificate)
- GoDaddy Root Cert (Root CA used to sign the SBC's end entity certificate)
- BaltimoreRoot CA Cert (Microsoft Presents the SBC a certficate signed by this authority)
- DigiCert Global G2 Cert (Microsoft Presents the SBC a certficate signed by this authority)

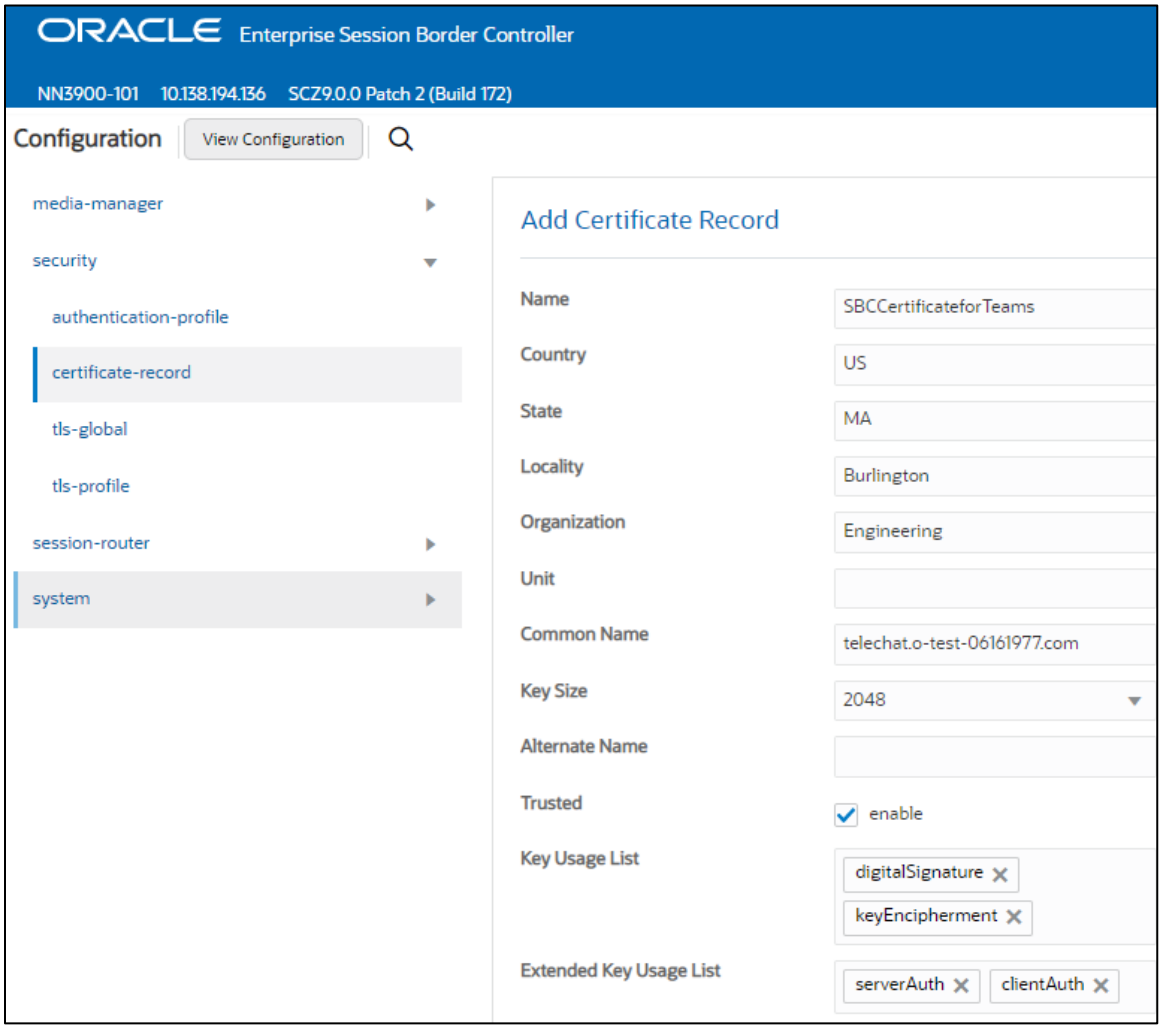
Note: The DigiCert RootCA is only part of this example, as that is the Authority we used to sign our SBC certificate. You would replace this with the root and/or intermediate certificates used to sign the CSR generated from your SBC.

SBC End Entity Certificate

The SBC's end entity certificate is the certificate the SBC presents to Microsoft to secure the connection. The only requirements when configuring this certificate is the common name must contain the SBC's FQDN. In this example our common name will be **telechat.o-test06161977.com.** You must also give it a name. All other fields are optional, and can remain at default values.

To Configure the certificate record:

Click Add, and use the following example to configure the SBC certificate



- Click OK at the bottom

Next, using this same procedure, configure certificate records for the Root CA certificates

Root CA and Intermediate Certificates

- **Go Daddy Root**

The following, GoDaddyRoot, is the root CA certificate used to sign the SBC's end entity certificate. As mentioned above, your root CA and/or intermediate certificate may differ. This is for example purposes only.

- **DigiCert Global Root G2**

The DNS name of the Microsoft Teams Direct Routing interface is sip.pstnhub.microsoft.com. Microsoft presents a certificate to the SBC which is signed by DigiCert Global Root G2.To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate. You can download this certificate here: DigiCert Global Root G2

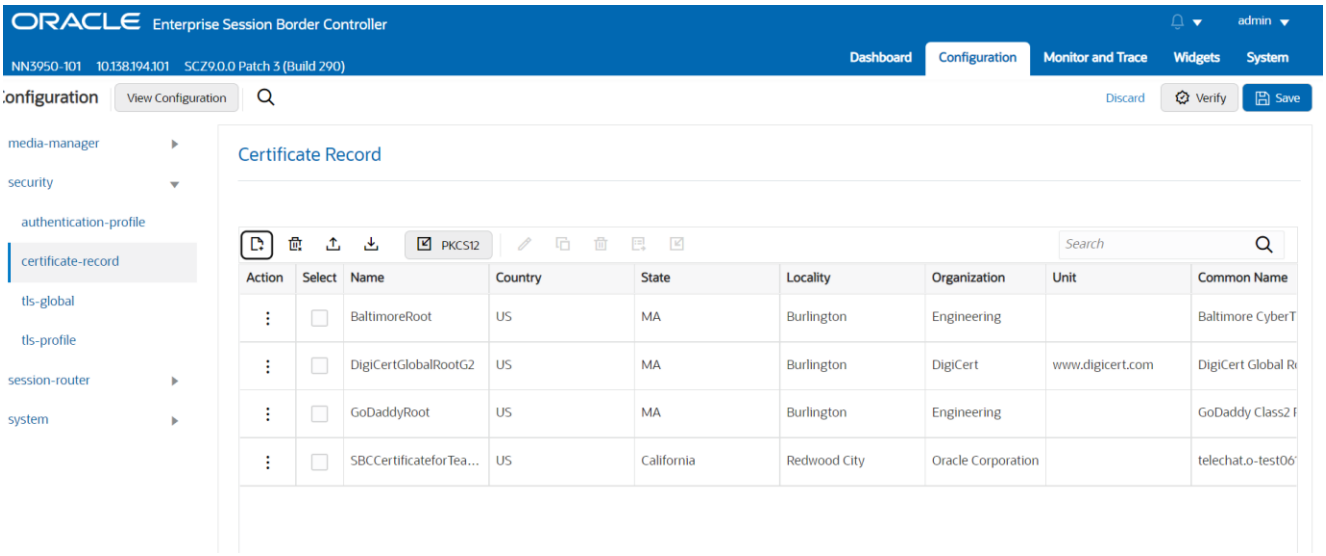
- **Baltimore Root**

The DNS name of the Microsoft Teams Direct Routing interface is sip.pstnhub.microsoft.com. Microsoft presents a certificate to the SBC which is signed by Baltimore Cyber Baltimore CyberTrust Root. To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate.

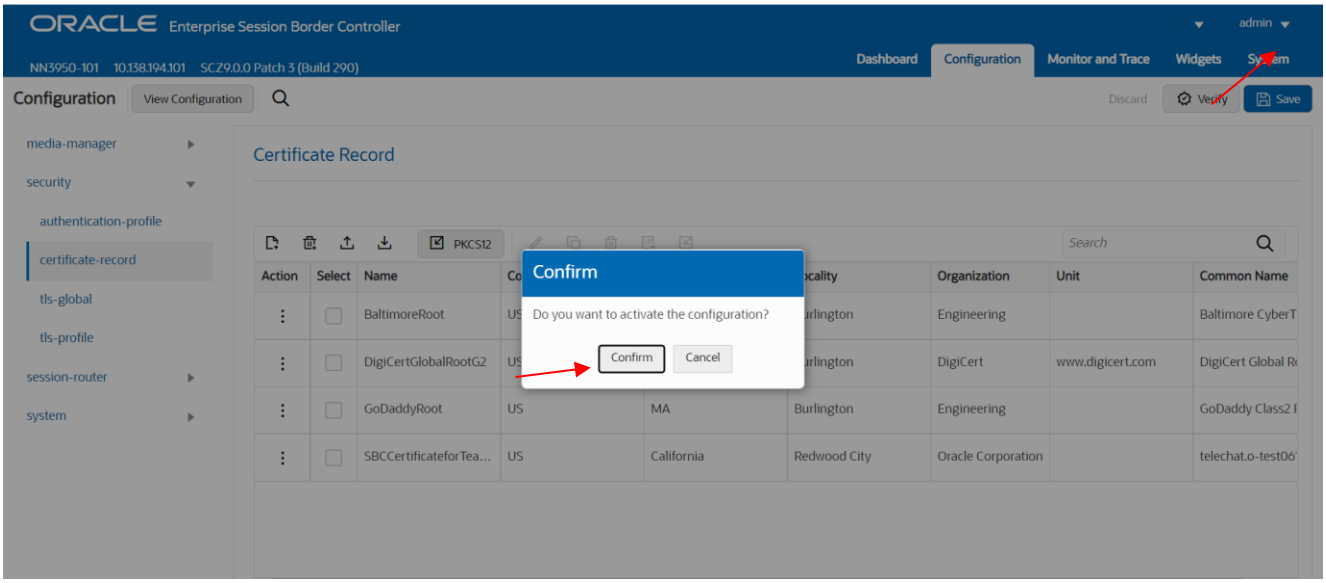
You can download this certificate here: https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt.pem

Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

Config Parameter	Baltimore Root	GoDaddy Root	DigiCert Global Root G2
Common Name	Baltimore CyberTrust Root	Go Daddy Class2 Root CA	DigiCert Global Root G2
Key Size	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256



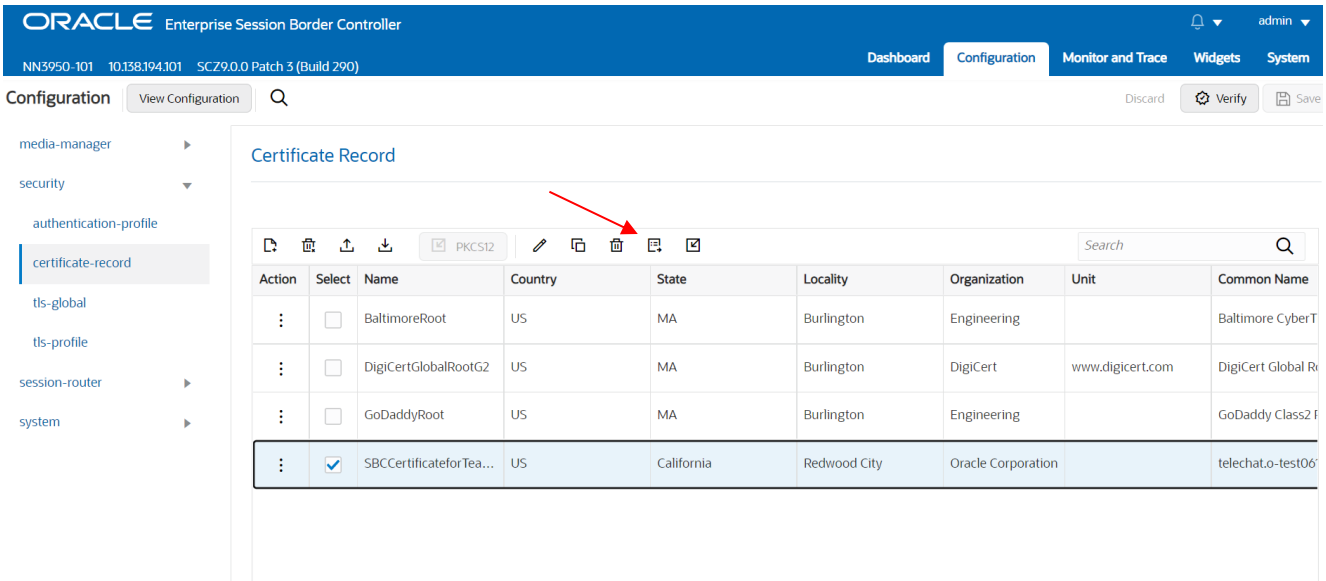
At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must **save and activate** the configuration of the SBC.



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. **This is not required for any of the Root CA or intermidiate certificates that have been created**.

On the certificate record page in the Oracle SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:



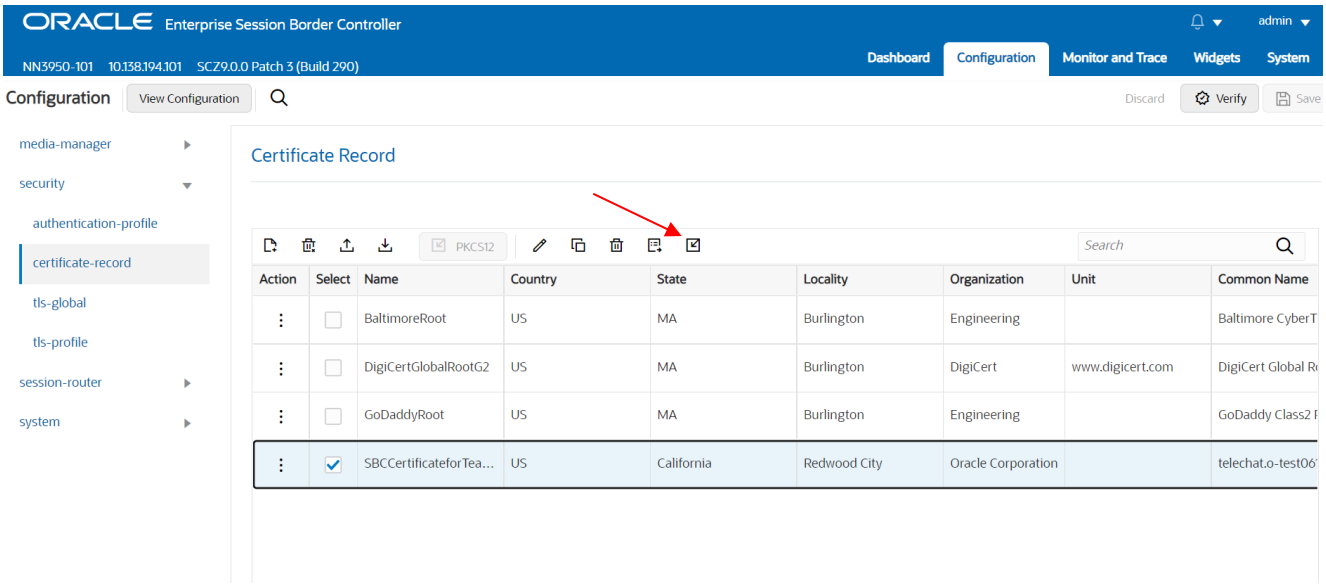
Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
Also note, at this point, **another save and activate is required** before you can import the certificates to each certificate record created above.

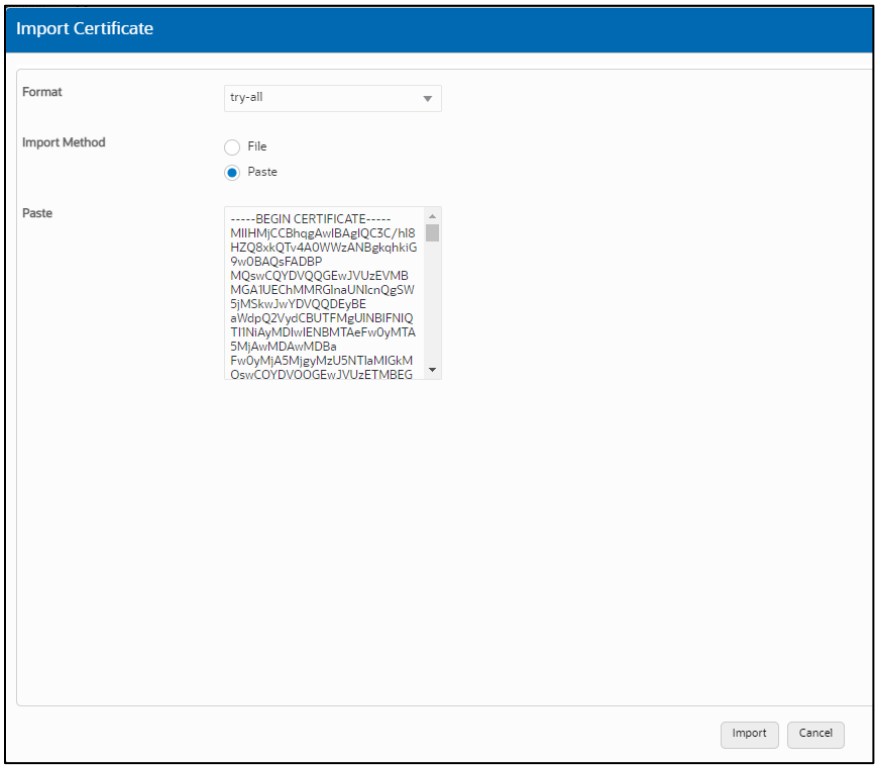
Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

Import Certificates to SBC

Once certificate signing request has been completed – import the signed certificate to the SBC.

Please note – all certificates including root and intermediate certificates are required to be imported to the SBC.
Once all certificates have been imported, issue a third **save/activate** from the WebGUI to complete the configuration of certificates on the Oracle SBC.





- Once pasted in the text box, select Import at the bottom, then **save and activate** your configuration.

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

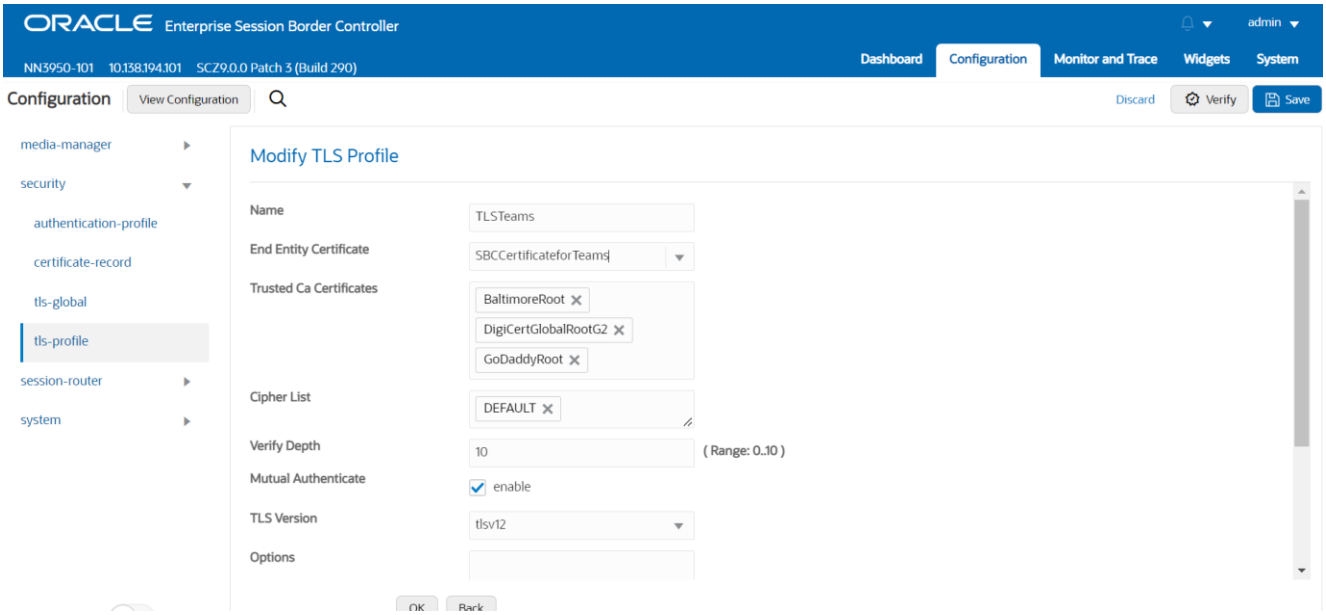
9.10.TLS Profile

TLS profile configuration on the SBC allows for specific certificates to be assigned.

GUI Path: security/tls-profile

ACLI Path: config t→security→tls-profile

- Click Add, use the example below to configure



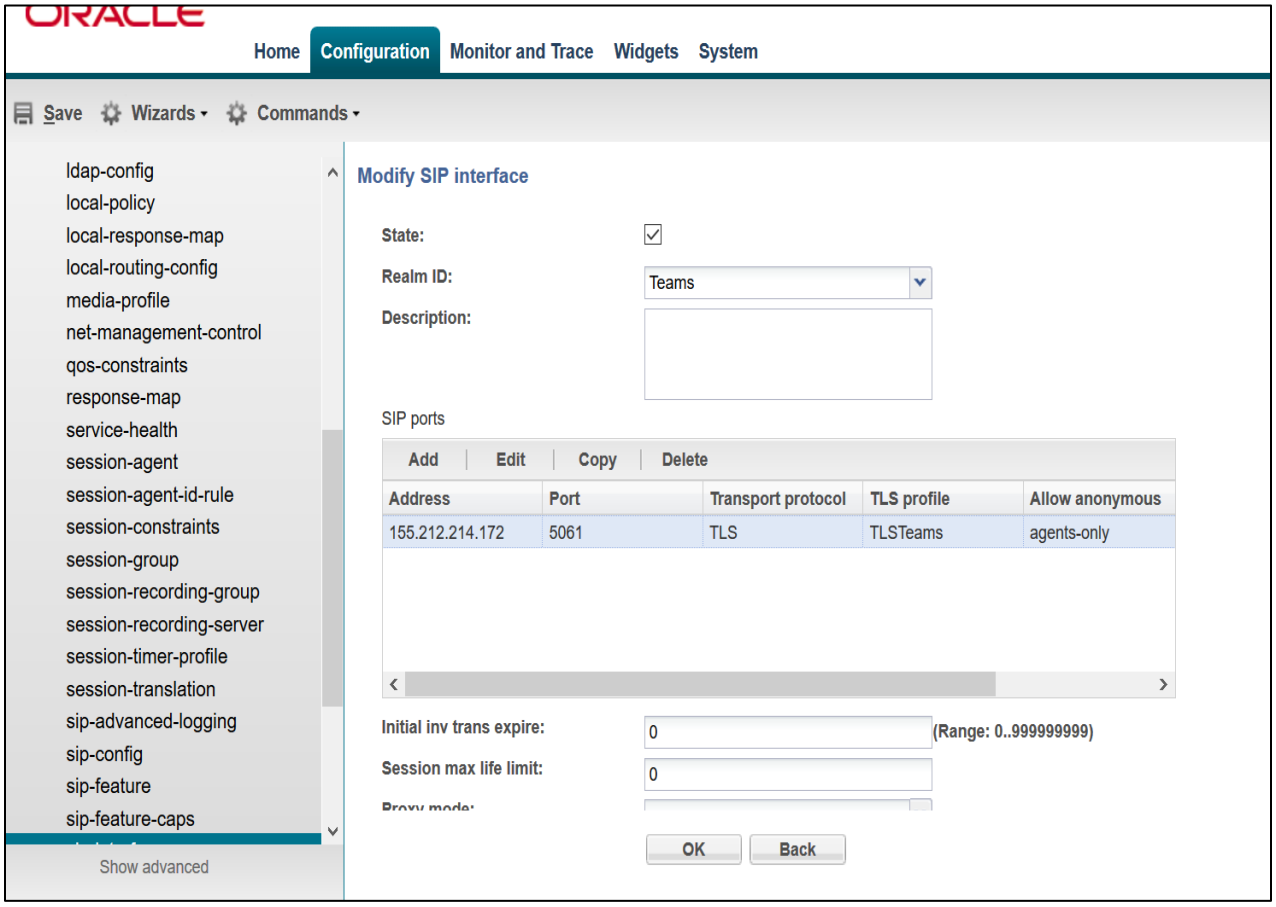
- Select OK at the bottom

9.11. Configure SIP Interfaces.

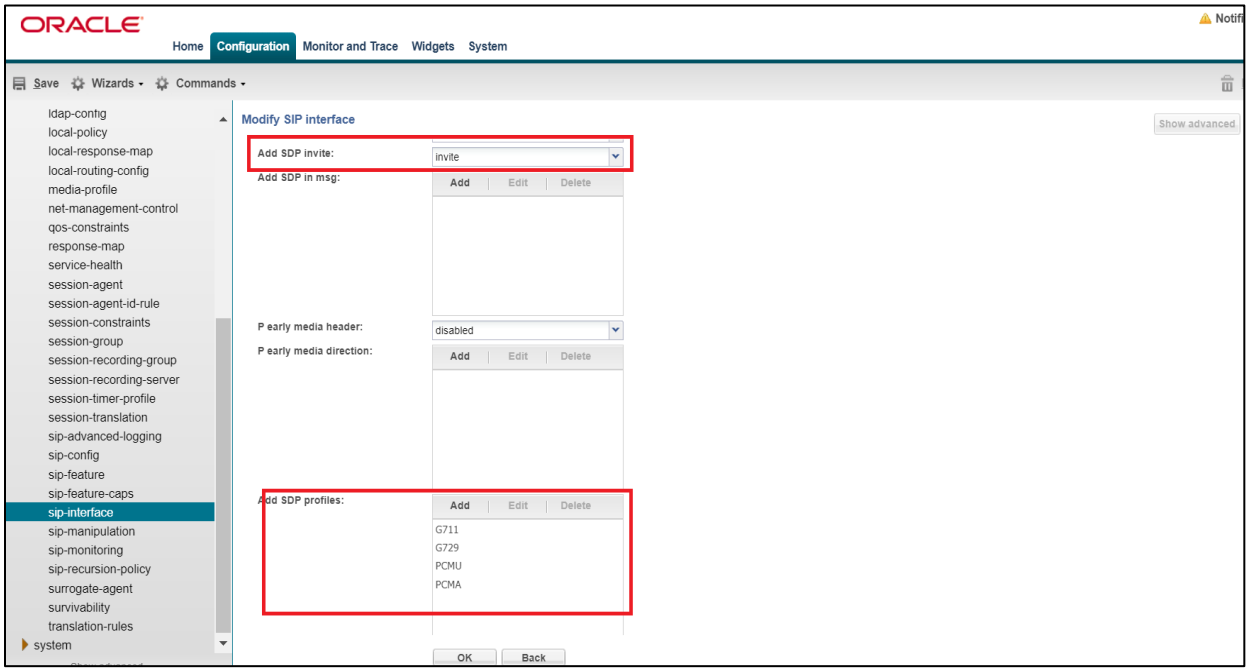
Navigate to sip-interface under session-router and configure the sip-interface as shown below
Please ensure that the IP address allocated to the SIP interface is the FQDN resolvable address.
i.e. if you issue command nslookup from another computer , “oracleesbc2.woodgrovebank.us” – it should resolve to 155.212.214.172. Note that the IP should be publicly routable IP address.

Note:

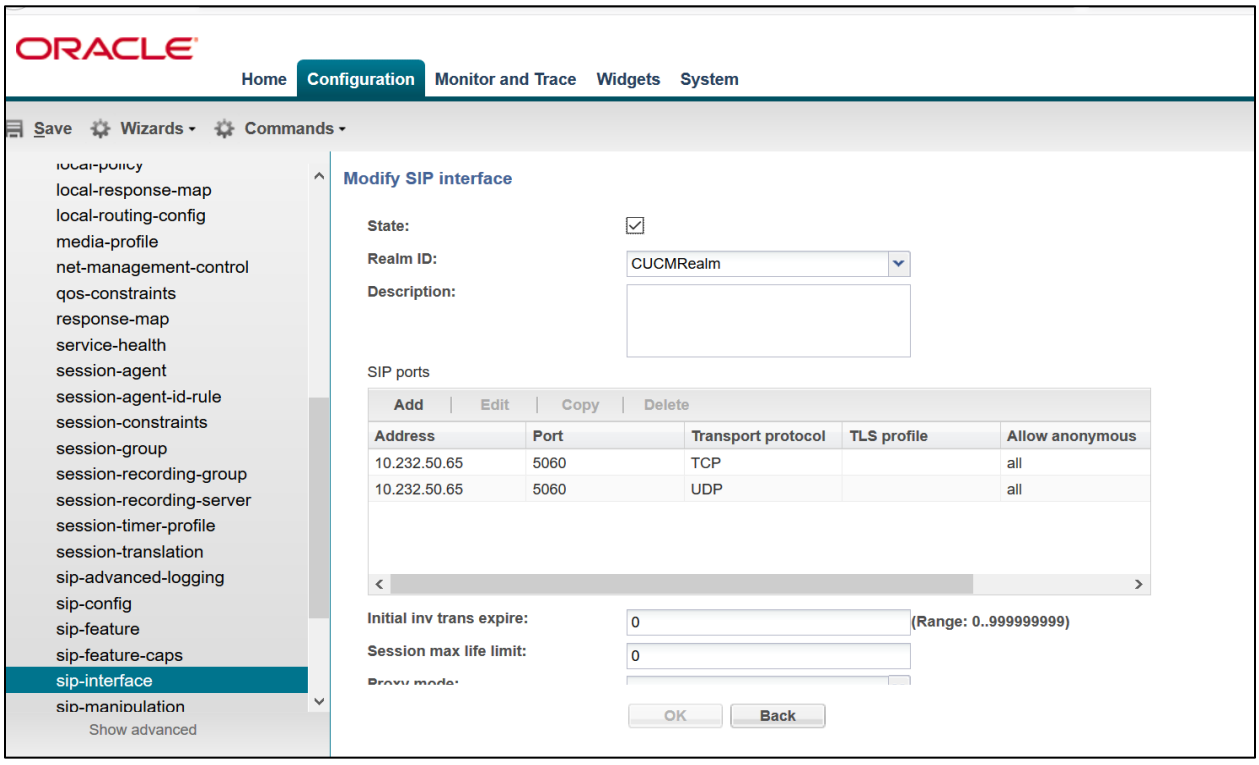
-Tls-profile needs to match the name of the tls-profile previously created
-Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from Teams server

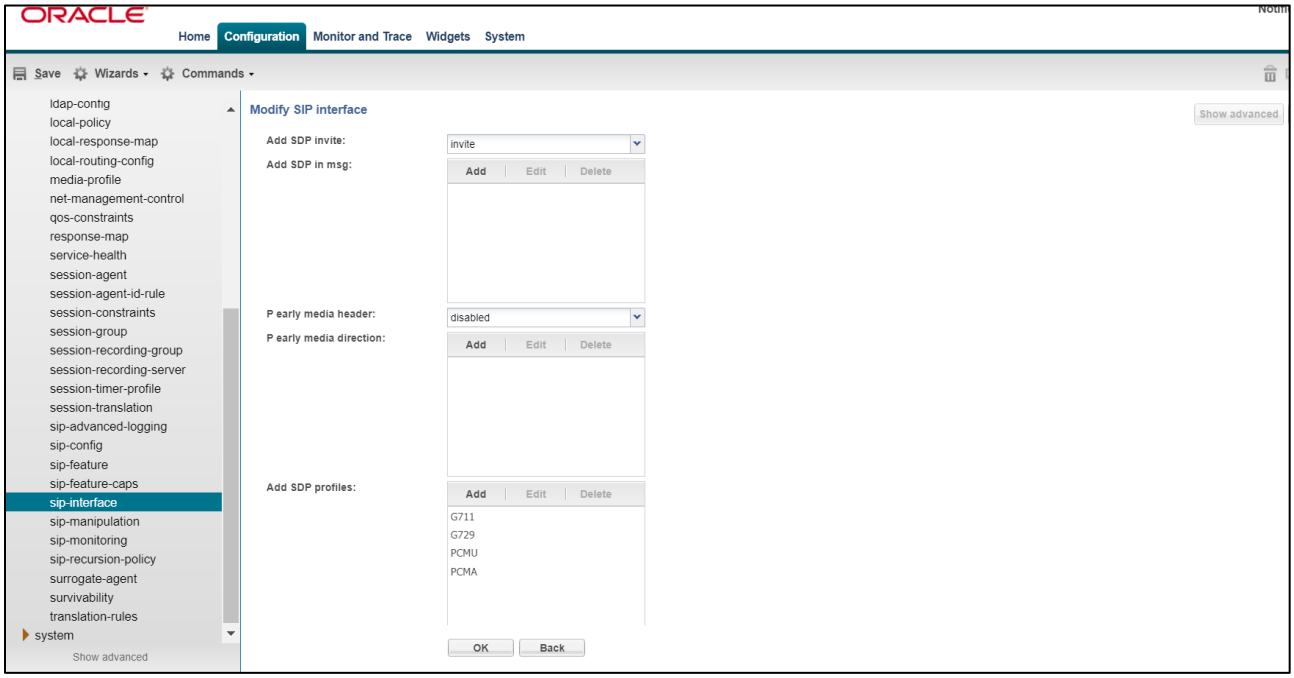


CUCM sends INVITE without SDP towards SBC. In order to send out INVITE with SDP towards trunk and vice versa, please enable the Add SDP Invite for INVITE only as highlighted for both interfaces.
When this option is enabled, codecs have to be configured under media profile.
The configured codecs should also be added here as shown below.



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





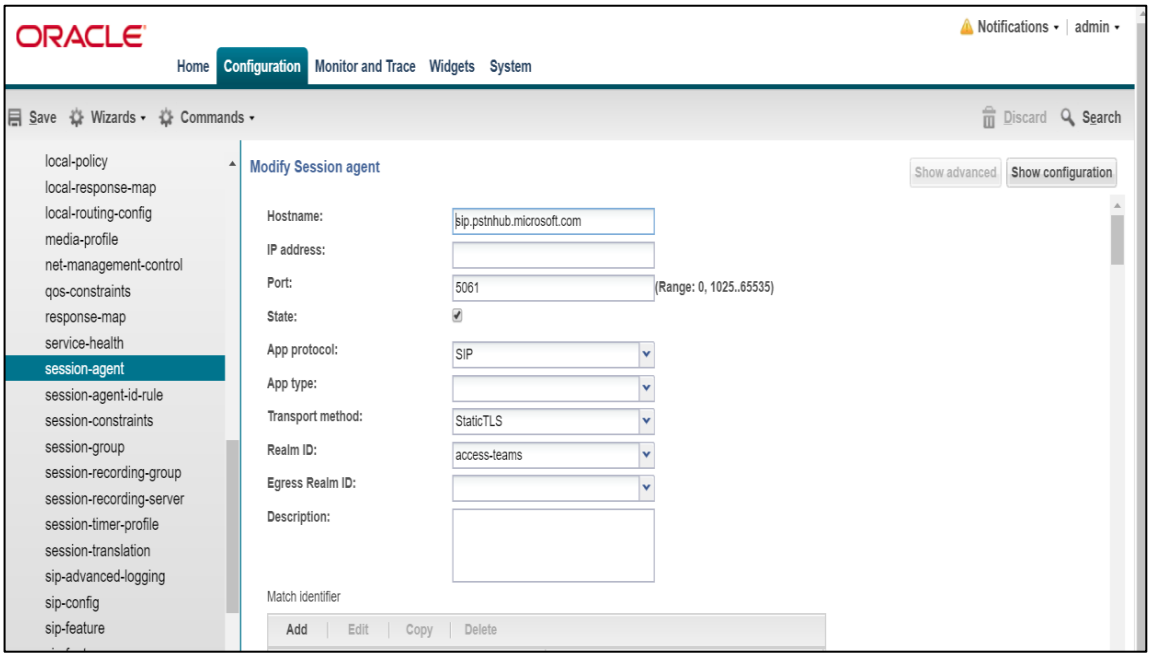
Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.
Now configure where the SBC sends the outbound traffic.

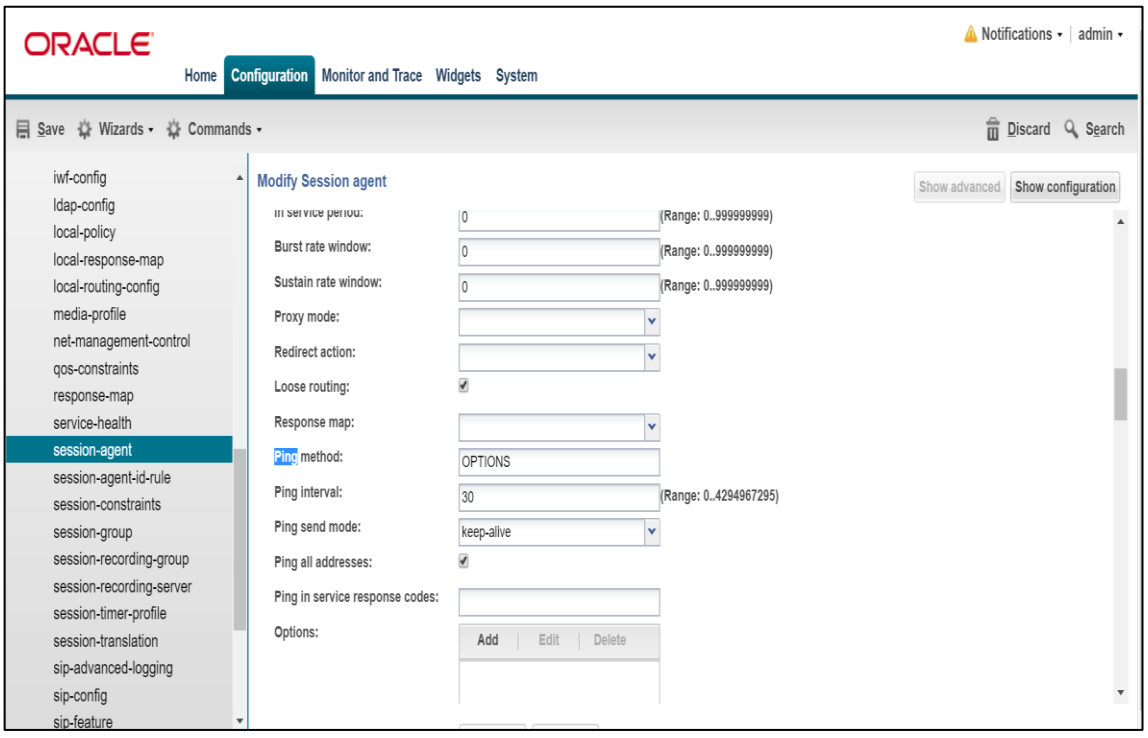
9.12. Configure session-agent

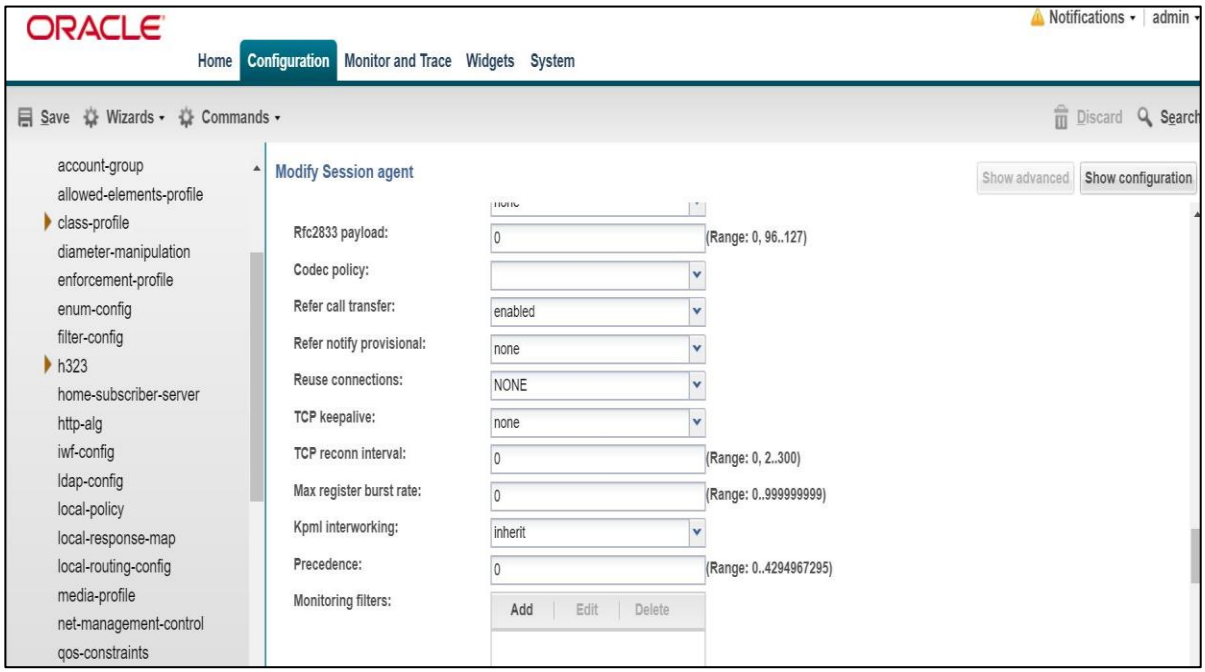
Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

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

- hostname to “sip.pstnhub.microsoft.com”
- port 5061
- realm-id – needs to match the realm created for teams
- transport set to “StaticTLS”
- refer-call-transfer set to enabled
- ping-method – send OPTIONS message to Microsoft to check health
- ping-interval to 30 secs
- Refer Call Transfer set to Enabled


ORACLE
Notifications
admin
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Discard
Search
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
session-recording-group
session-recording-server
session-timer-profile
session-translation
sip-advanced-logging
sip-config
sip-feature
Modify Session agent
Show advanced
Show configuration
Hostname:
sip.pstnhub.microsoft.com
IP address:
Port:
5061
(Range: 0, 1025..65535)
State:
App protocol:
SIP
App type:
Transport method:
StaticTLS
Realm ID:
access-teams
Egress Realm ID:
Description:
Match identifier
Add
Edit
Copy
Delete


ORACLE
Notifications
admin
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Discard
Search
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
session-recording-group
session-recording-server
session-timer-profile
session-translation
sip-advanced-logging
sip-config
sip-feature
Modify Session agent
Show advanced
Show configuration
(Range: 0..999999999)
Burst rate window:
0
(Range: 0..999999999)
Sustain rate window:
0
(Range: 0..999999999)
Proxy mode:
Redirect action:
Loose routing:
Response map:
Ping method:
OPTIONS
Ping interval:
30
(Range: 0..4294967295)
Ping send mode:
keep-alive
Ping all addresses:
Ping in service response codes:
Options:
Add
Edit
Delete

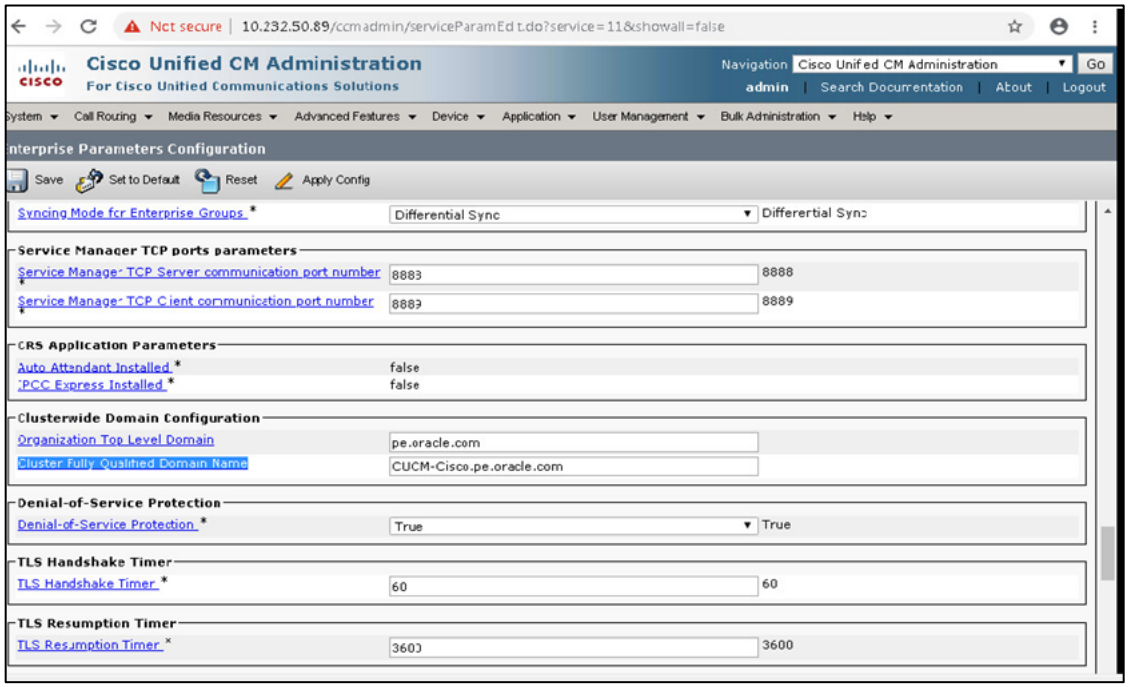


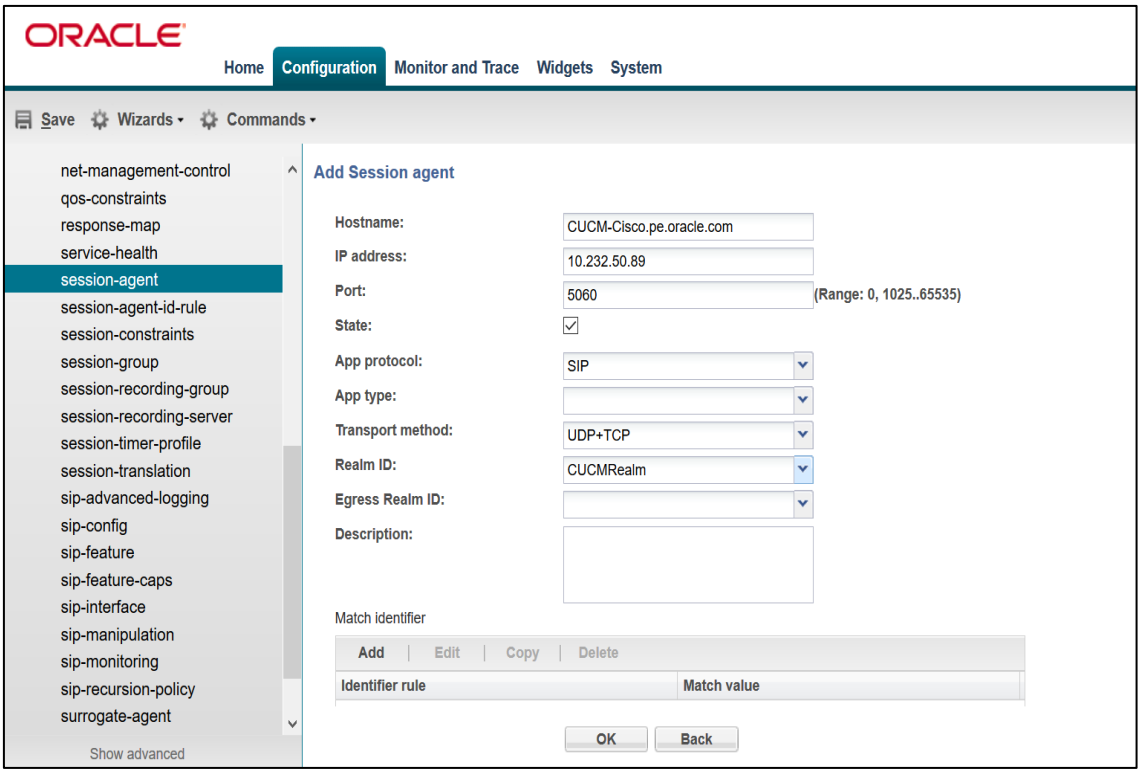
Follow above steps to create 2 more sessions for:

- sip2.pstnhub.microsoft.com
- sip3.pstnhub.microsoft.com

Similarly, Configure the session-agent for CUCM side with the following parameters.
Go to session-router->Session-Agent.

- Host name 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”

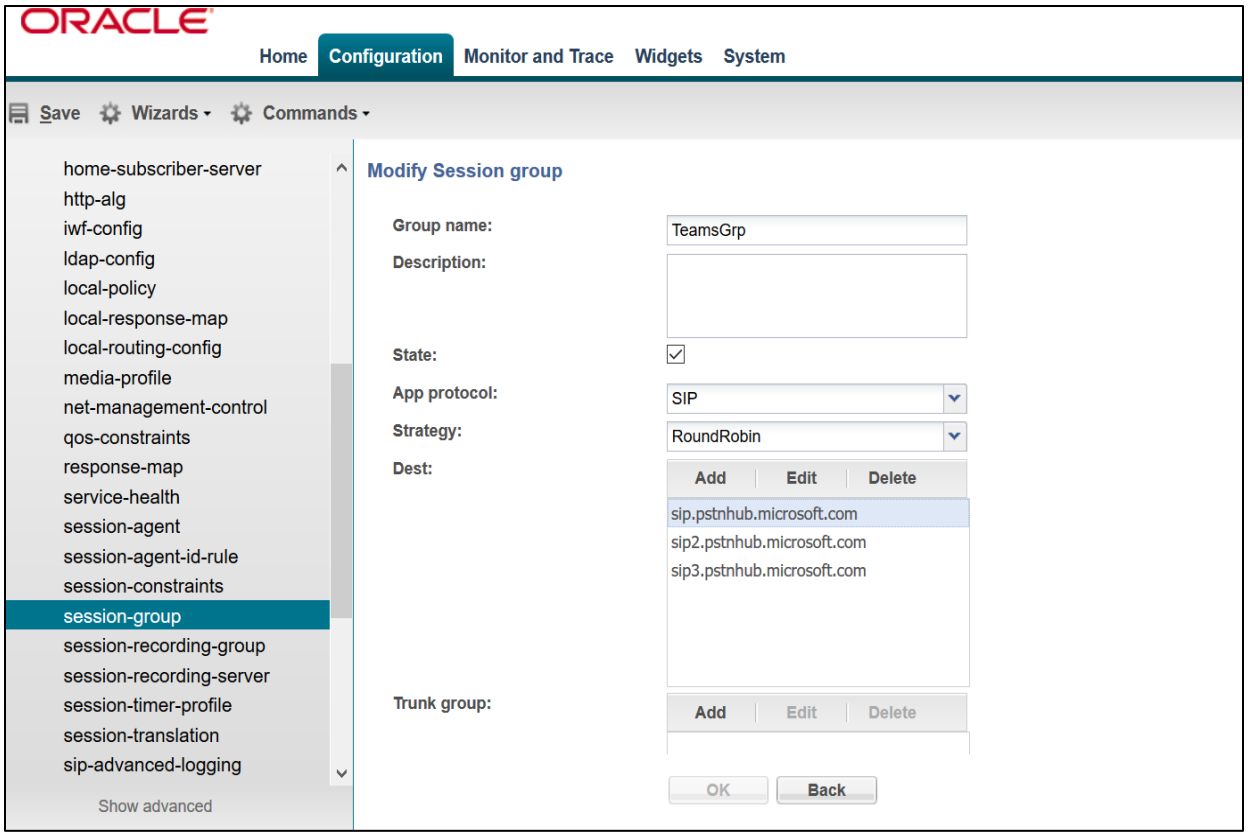

Not secure | 10.232.50.89/ccmadmin/serviceParamEdit.do?service=11&showall=false
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features 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 * 8883 8888
Service Manager TCP Client communication port number * 8883 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

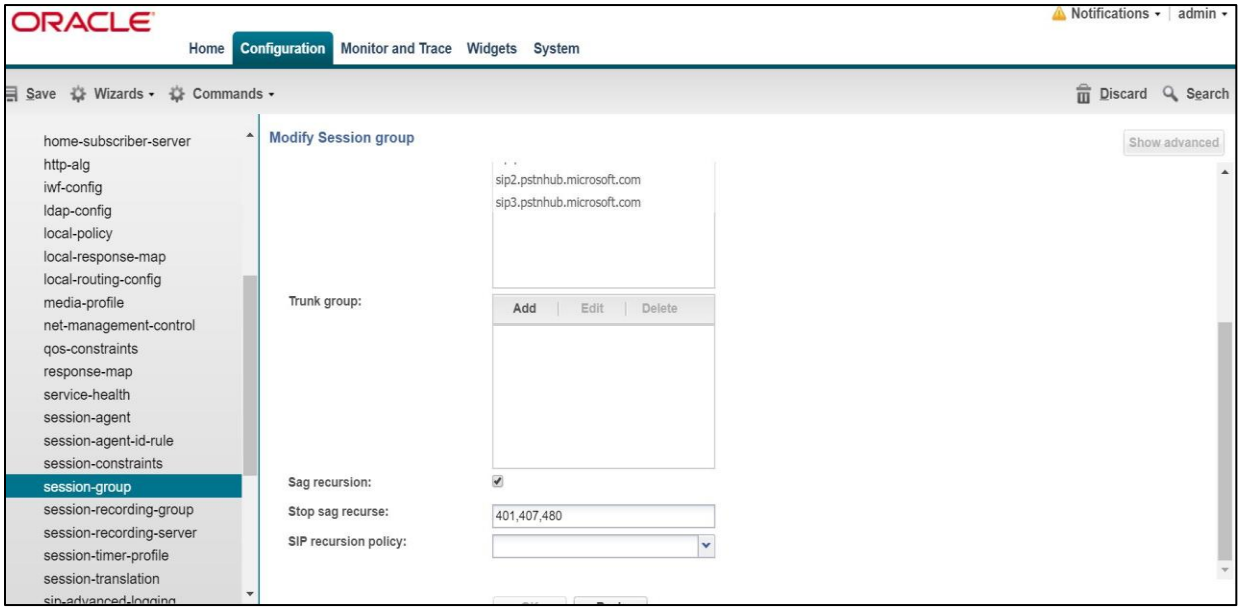

ORACLE
Home Configuration Monitor and Trace Widgets System
Save Wizards Commands
net-management-control
qos-constraints
response-map
service-health
session-agent
session-agent-id-rule
session-constraints
session-group
session-recording-group
session-recording-server
session-timer-profile
session-translation
sip-advanced-logging
sip-config
sip-feature
sip-feature-caps
sip-interface
sip-manipulation
sip-monitoring
sip-recursion-policy
surrogate-agent
Show advanced
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: CUCMRealm
Egress Realm ID:
Description:
Match identifier
Add Edit Copy Delete
Identifier rule Match value
OK Back

9.13. Configure session-agent group

A session agent group allows the SBC to create a load balancing model.

Go to Session-Router->Session-Group.

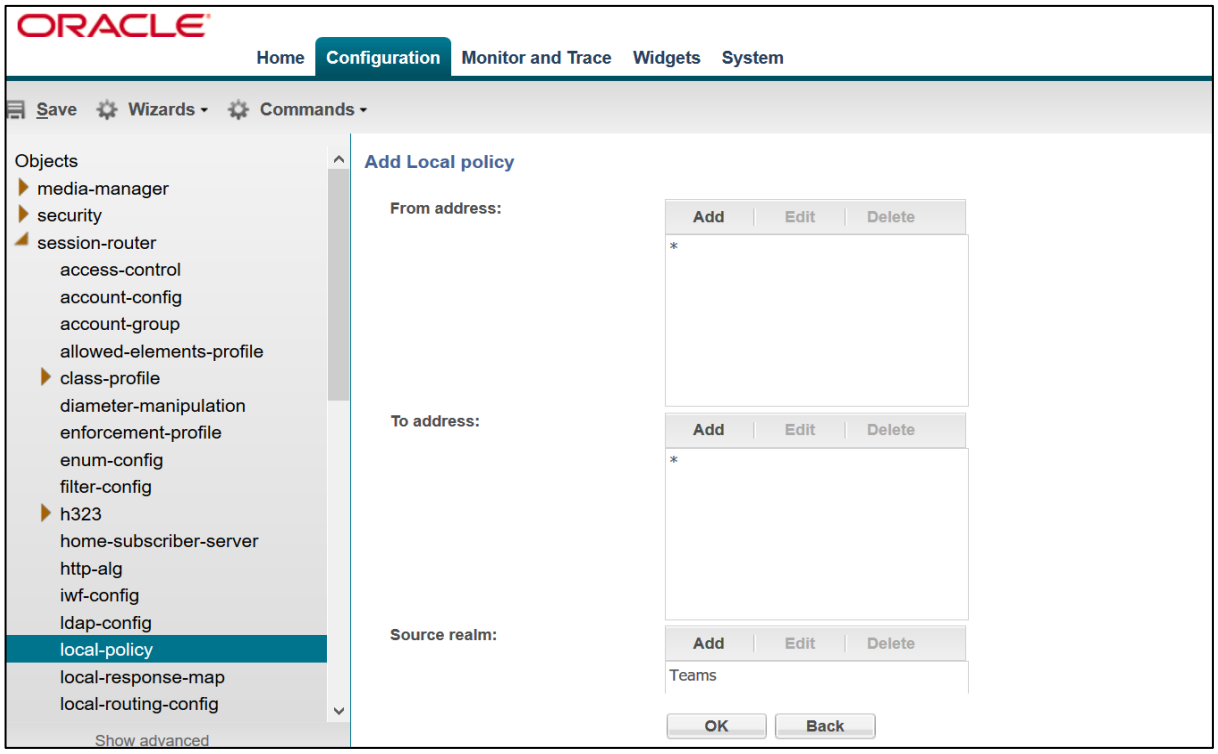


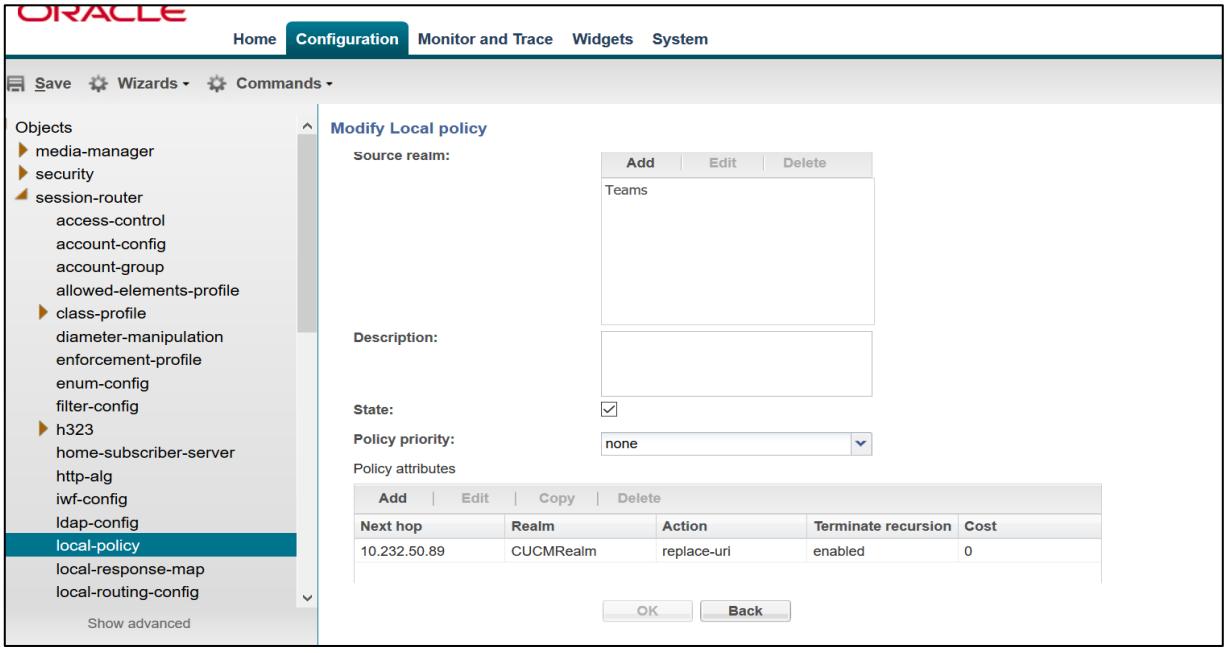


9.14. Configure local-policy

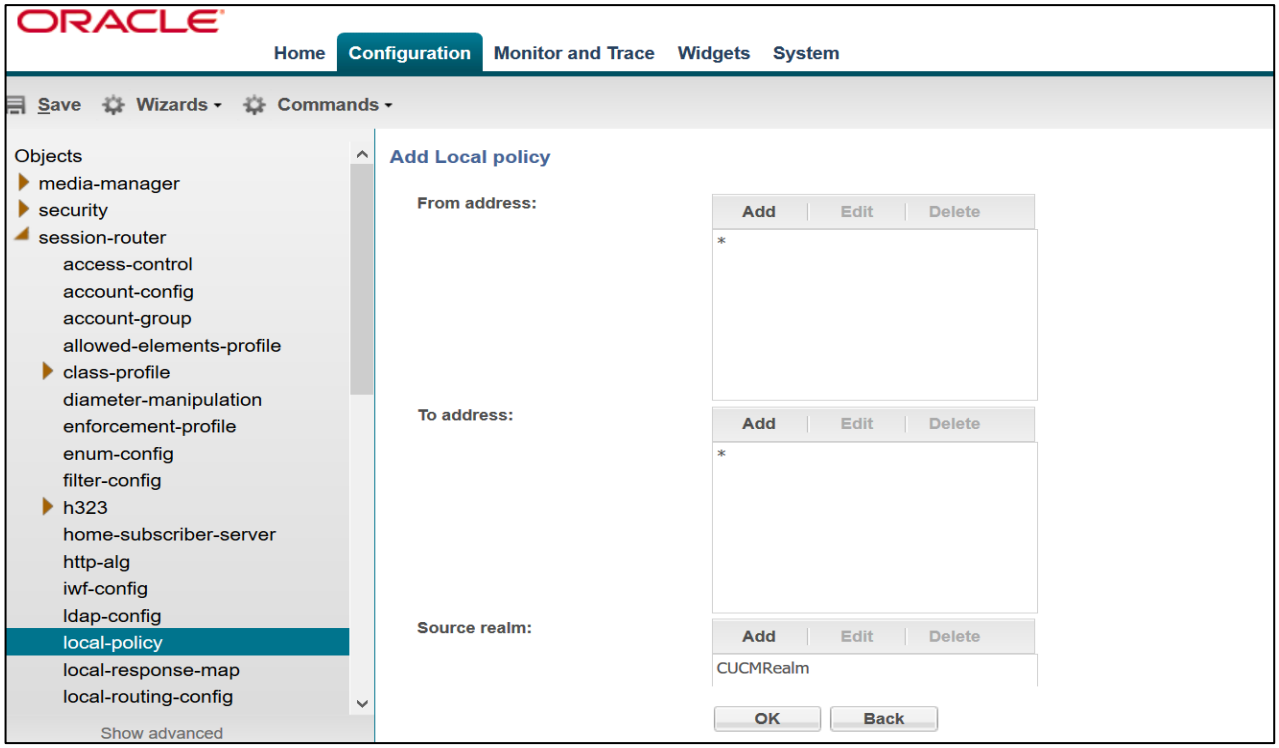
Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

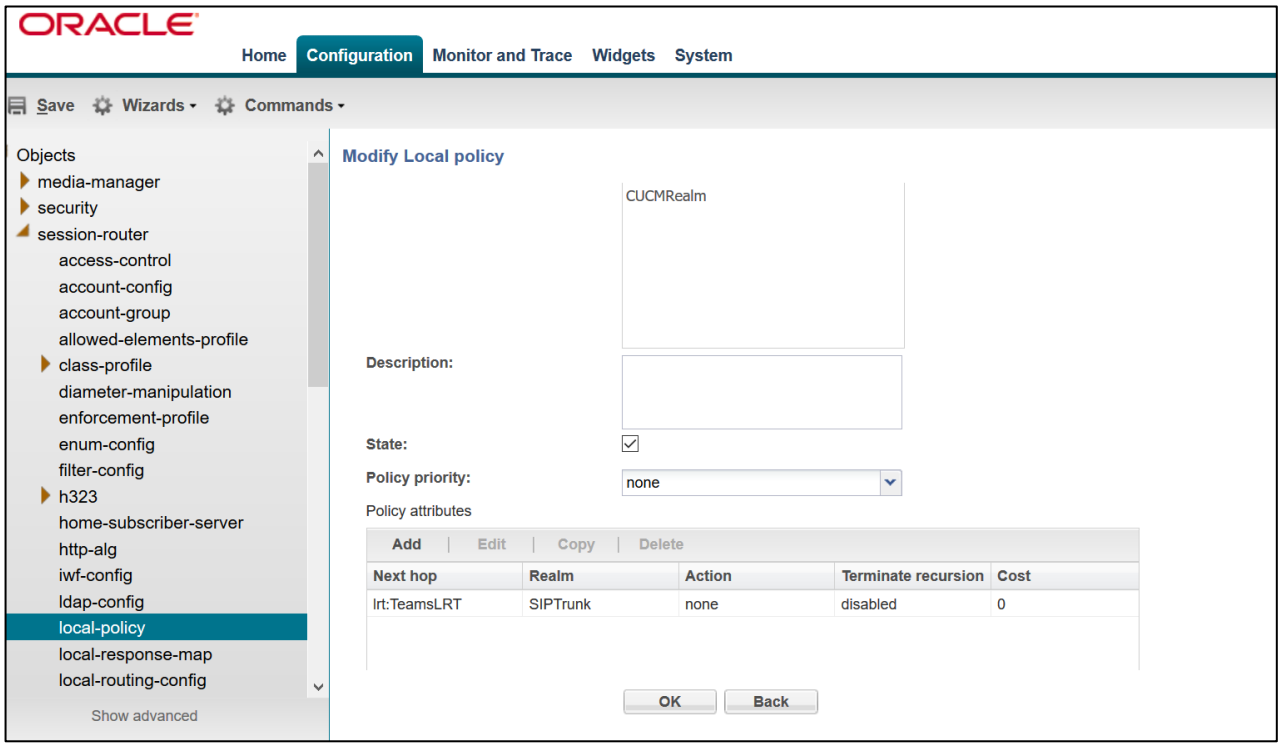
To make calls from Teams to CUCM, the following config is required:





To make calls from CUCM to Teams, please configure the below local policy.



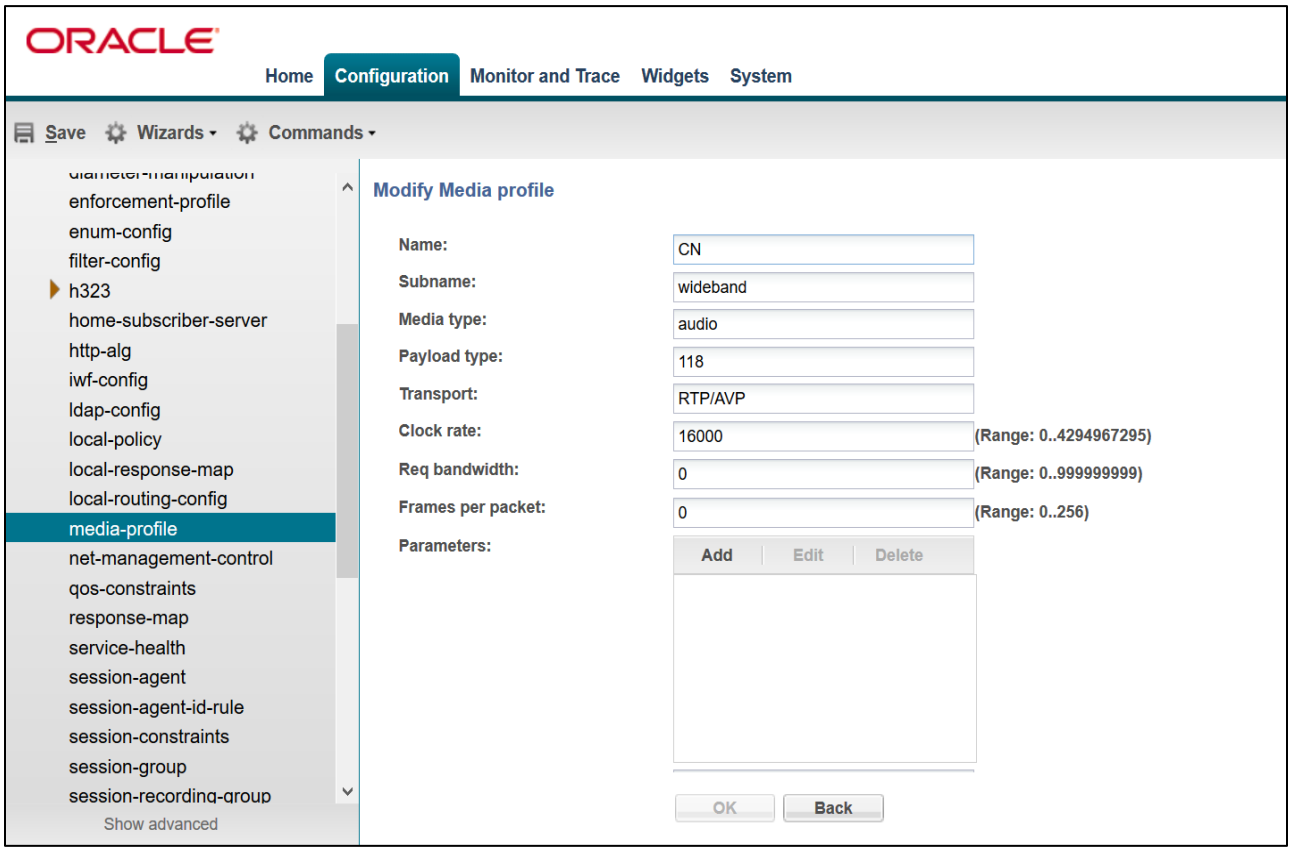


9.15. Configure Media Profile and Codec Policy

The Oracle Session Border Controller (SBC) uses codec policies to describe how to manipulate SDP messages as they cross the SBC. The SBC bases its decision to transcode a call on codec policy configuration and the SDP. Each codec policy specifies a set of rules to be used for determining what codecs are retained, removed, and how they are ordered within SDP.

Note: this is an optional config – configure codec policy only if deemed required

SILK & CN offered by Microsoft teams are using a payload type which is different than usual.
Configure the media-profile as shown below,
Go to Session-Router->Media-profile

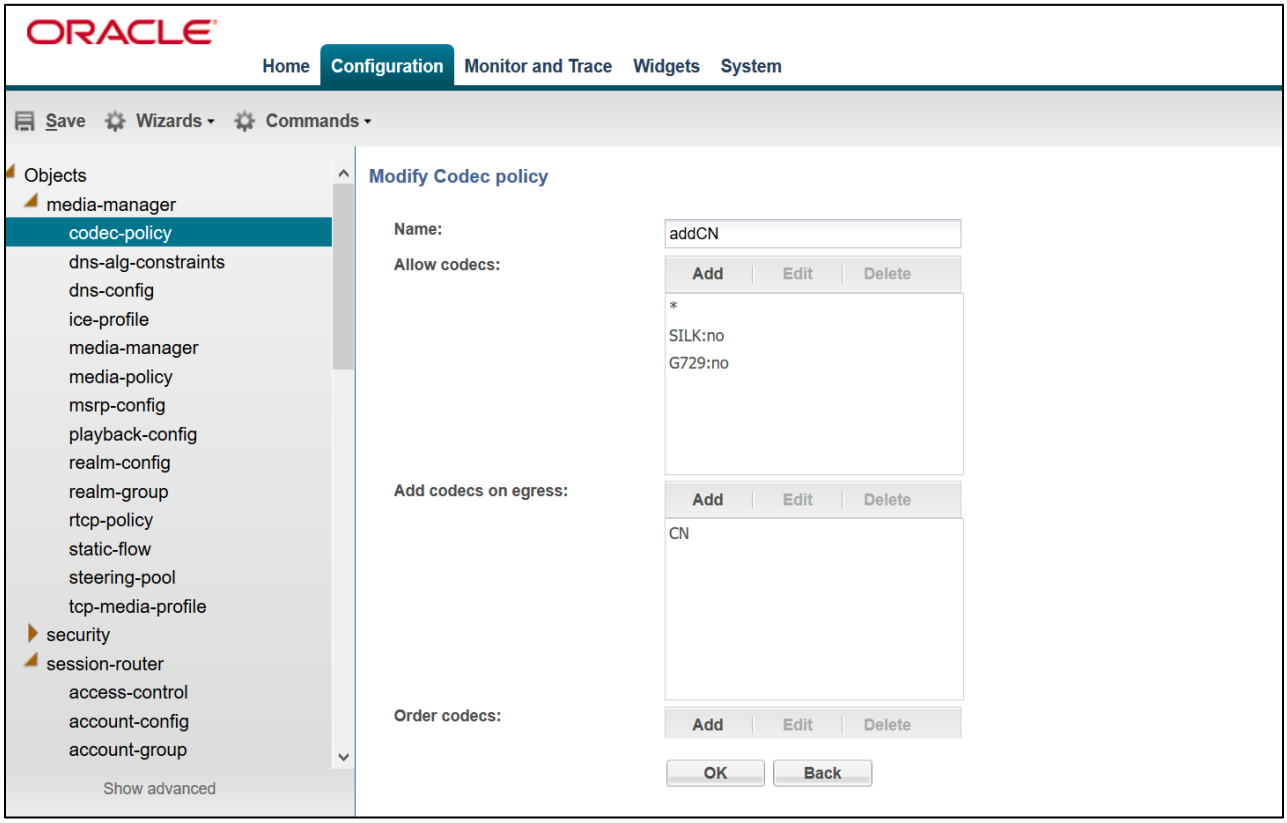


Configure media profiles similarly, for silk codec also as given below.

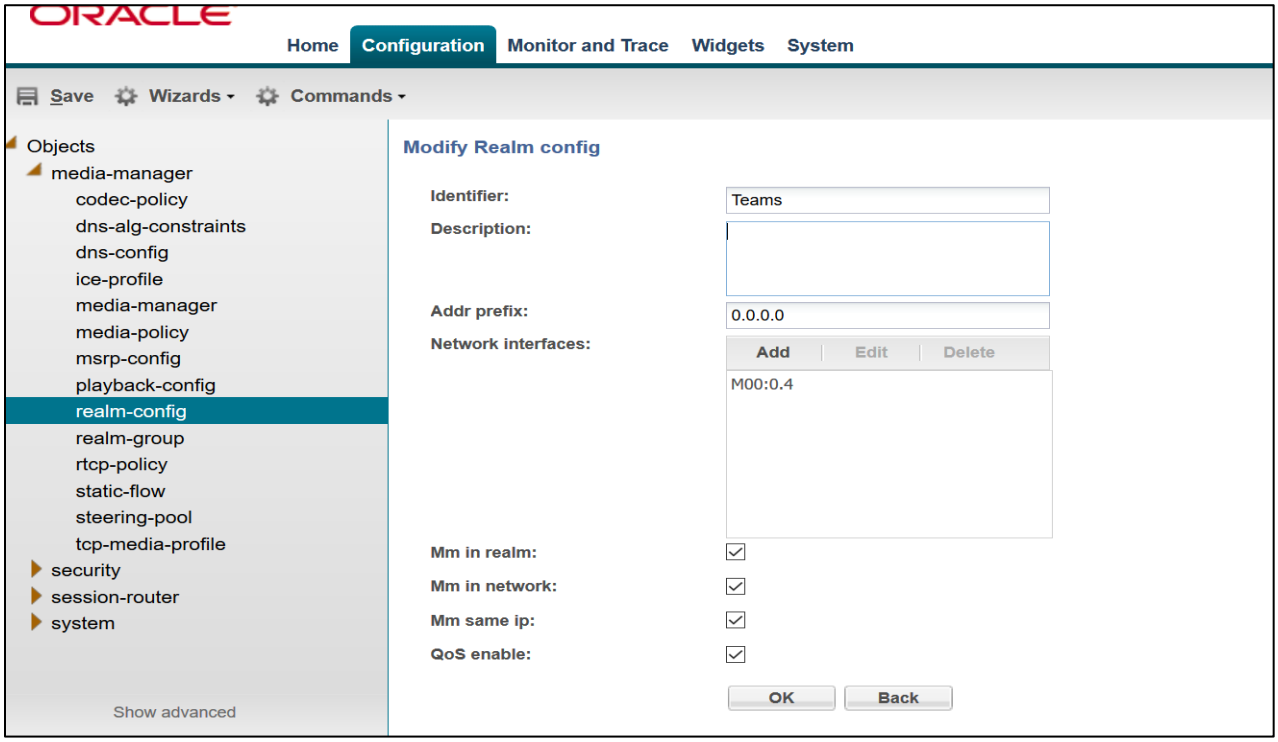
Parameters	SILK-1	SILK-2
Subname	narrowband	wideband
Payload-Type	103	104
Clock-rate	8000	16000

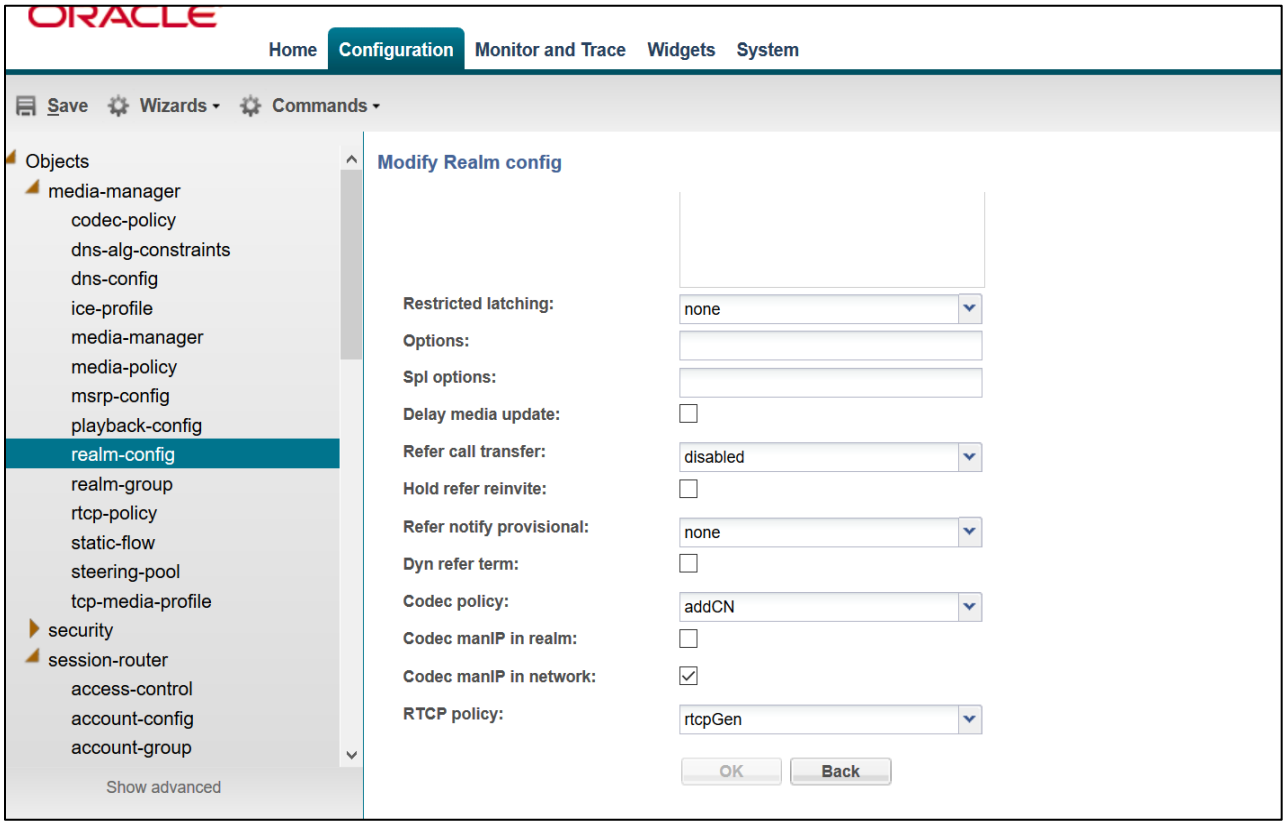
After creating media profile, create codec-policy, addCN, to add comfort noise towards Teams and apply it on the realm for Teams

Go to media manager ---- codec policy.



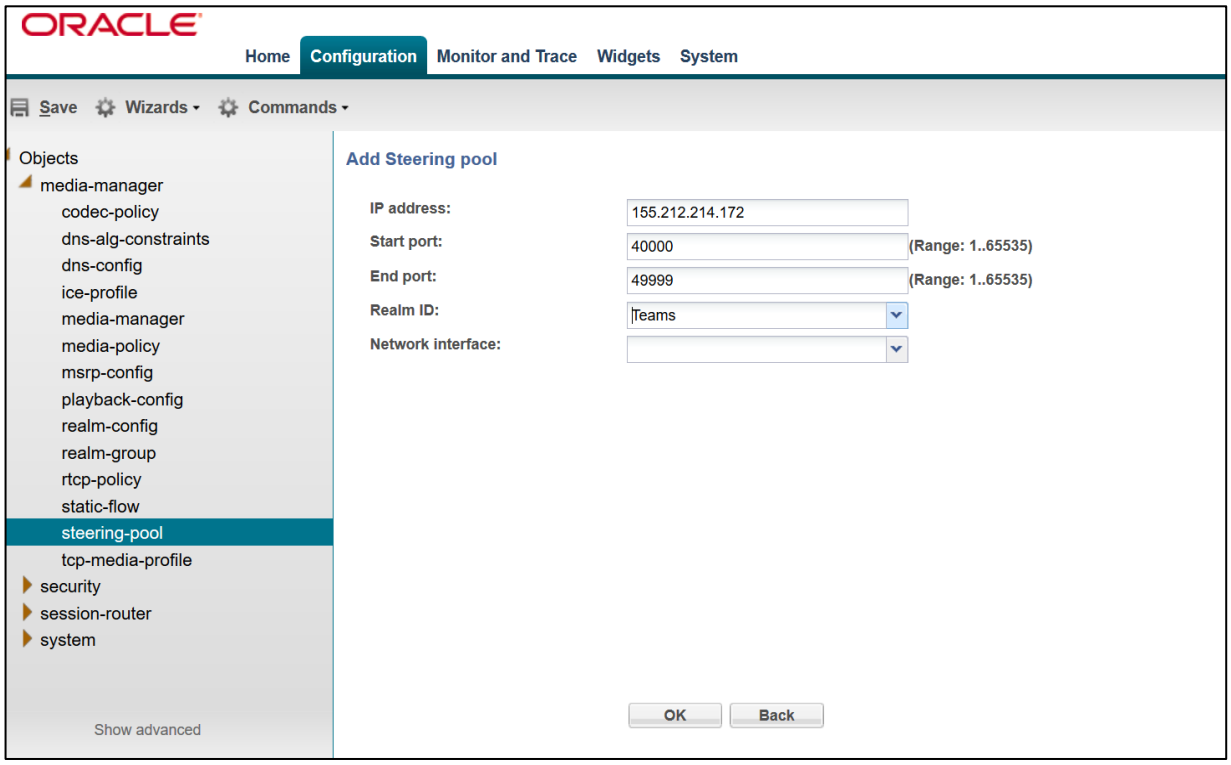
Go to media manager ---- realm config and assign the codec policy to the Teams realm

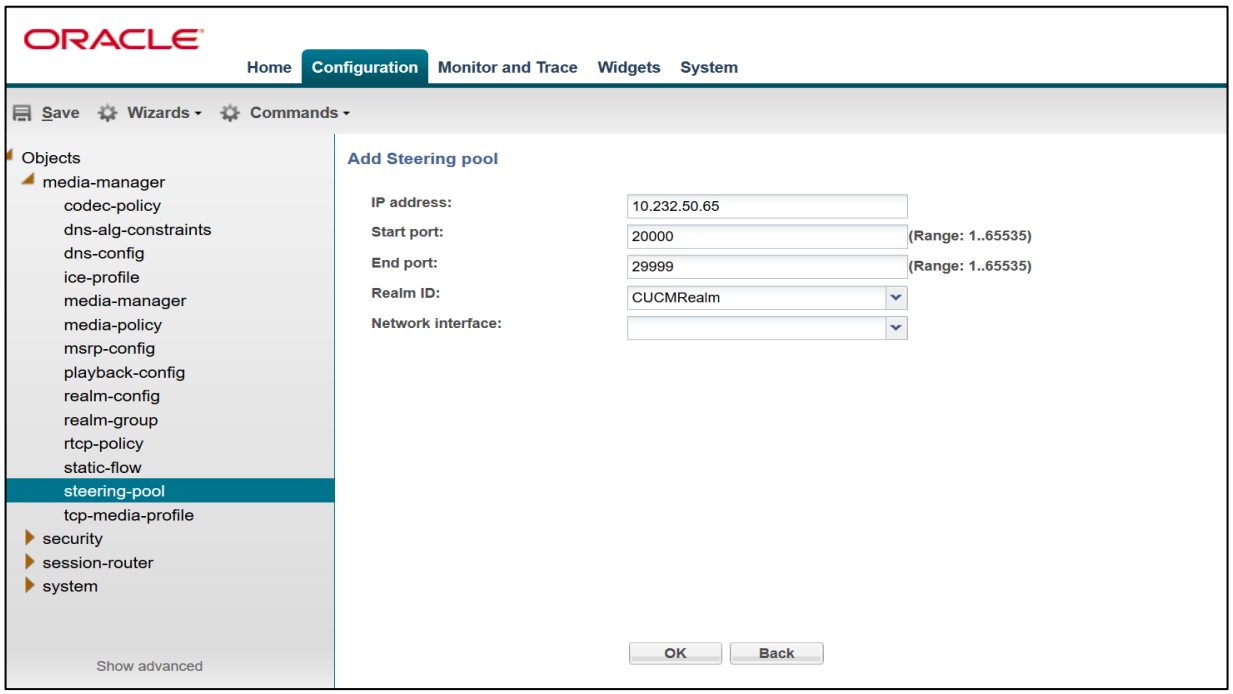




9.16. Configure steering-pool

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

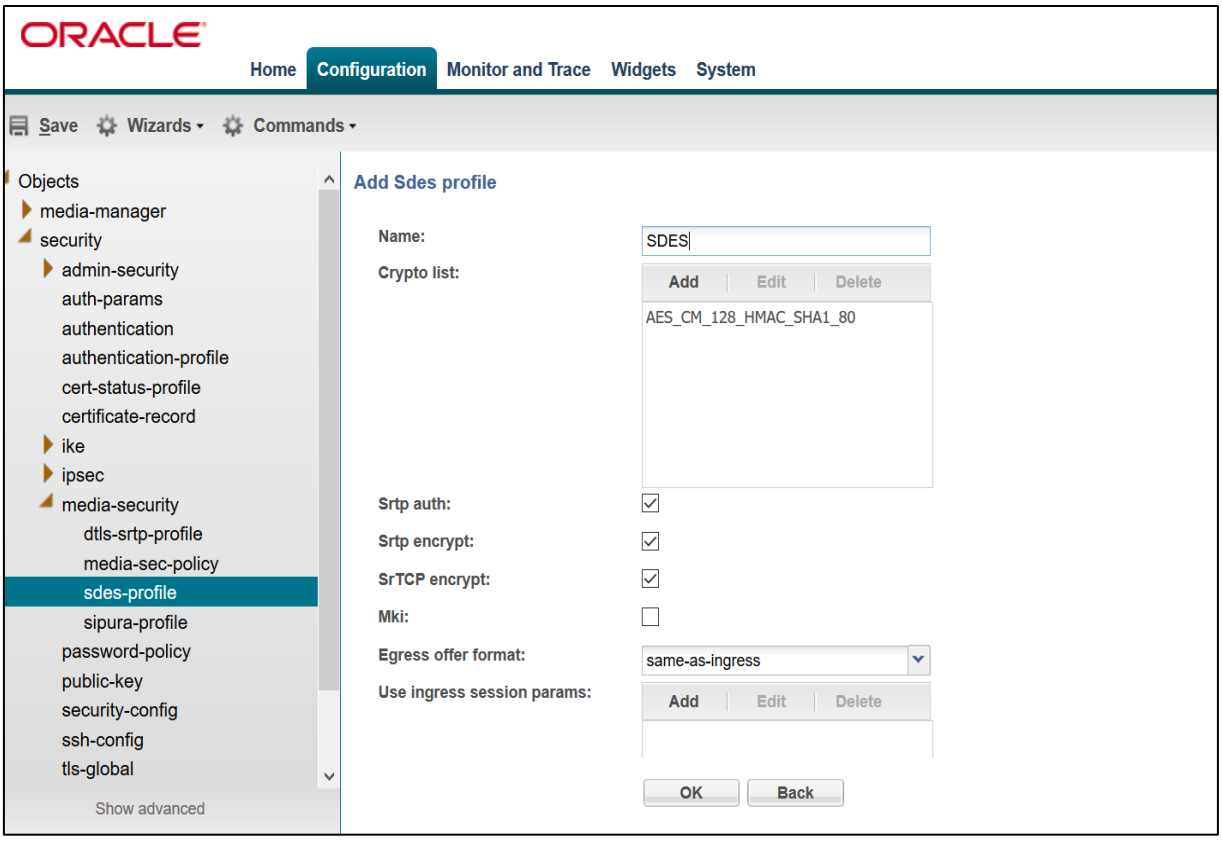




9.17. Configure sdes profile

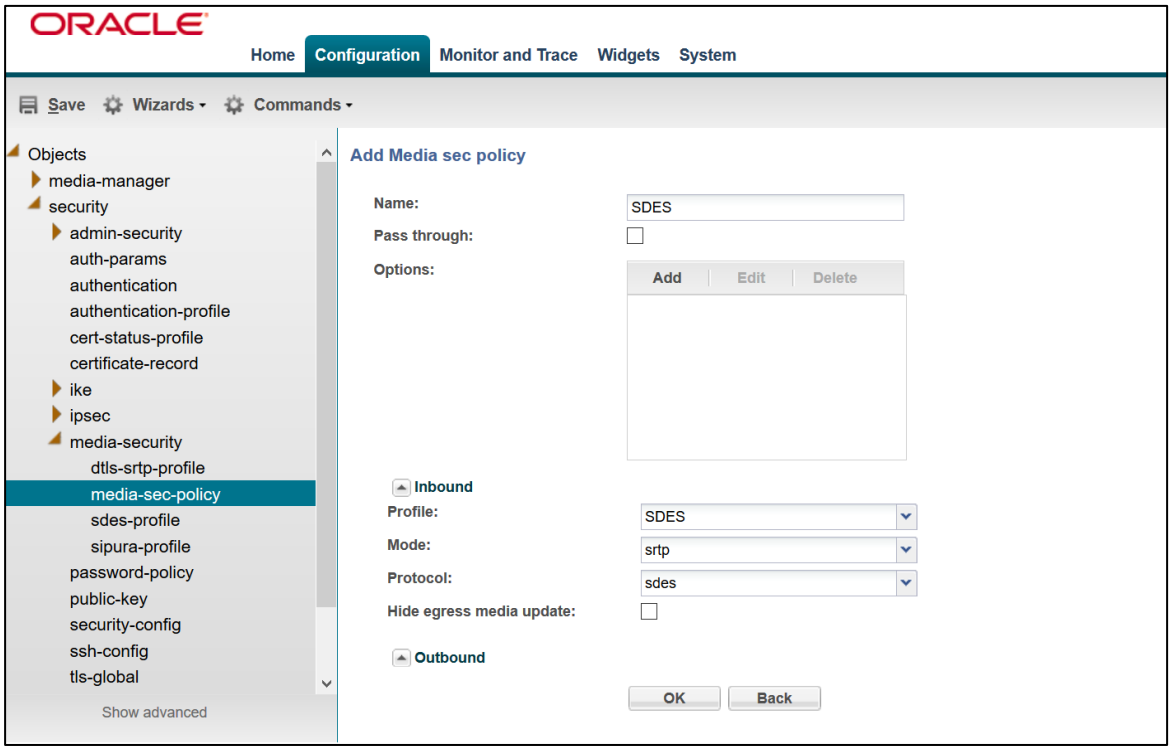
Please go to →Security → Media Security →sdes profile and create the policy as below.

Microsoft only supports AES_CM_128_HMAC_SHA1_80 encryption.

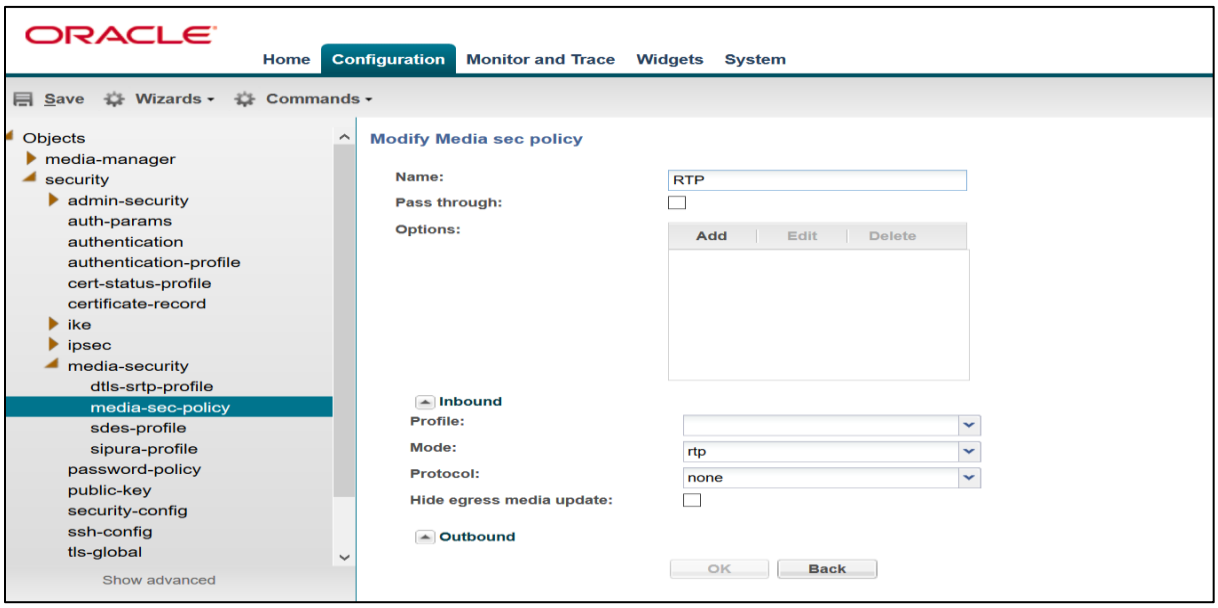


9.18. Configure Media Security Profile

Please go to →Security → Media Security →media Sec policy and create the policy as below:
Create Media Sec policy with name SDES for the Teams side which will have the sdes profile created above. Assign this media policy to the Teams Realm.



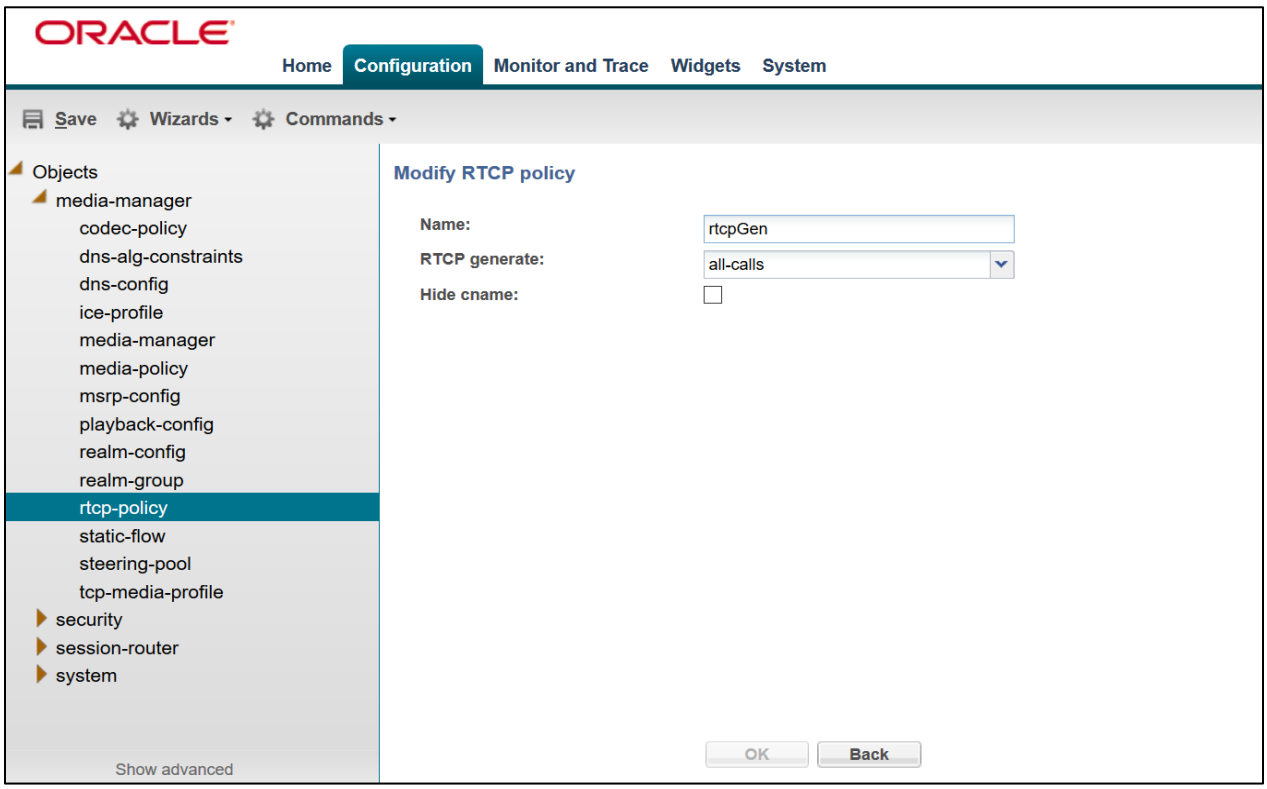
Similarly, Create Media Sec policy with name RTP to convert srtp to rtp for the CUCM side which will use only TCP/UDP as transport protocol. Assign this media policy to the CUCMRealm



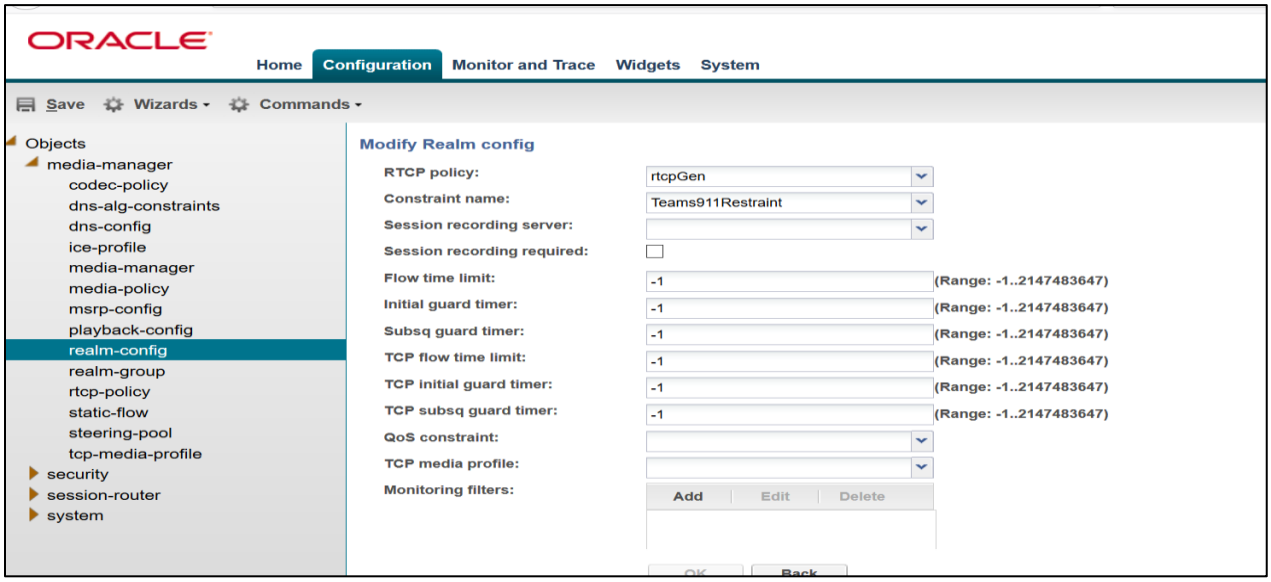
9.19. Configure RTCP Policy and RTCP Mux

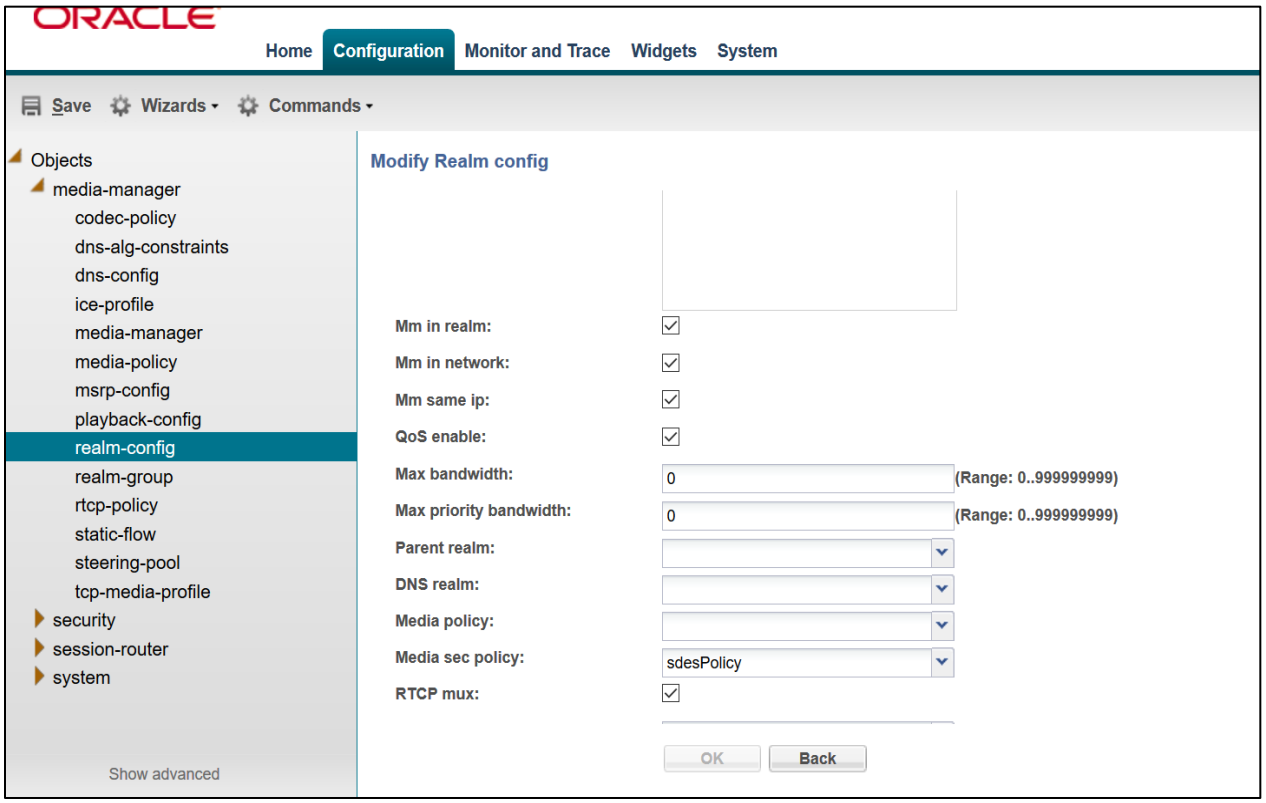
The RTCP policy needs to be configured in order to generate RTCP reports towards Teams. It is then applied on the Teams realm.

Go to Media-manager->rtcp-policy to configure rtcp-policy.



Please add the above policy to Ream Teams and also enable support for RTCP-Mux in the realm.





9.20. Configure sip-manipulation

To simplify the ORACLE SBC sip manipulation, the latest GA Release, SCZ830m1p7 contains three additional SBC configuration parameters which are not found in prior releases.

The purpose of these three parameters is to replace the majority of the sip manipulation rules required to be configured in the ORACLE SBC in order to properly interface with Microsoft Teams Direct Routing.

The first two parameters are found under the **realm-config**, and would be enabled in realms facing Microsoft Teams.

They are **Teams FQDN in URI** and **SDP inactive only**.
The detailed description is given below for each config parameter.

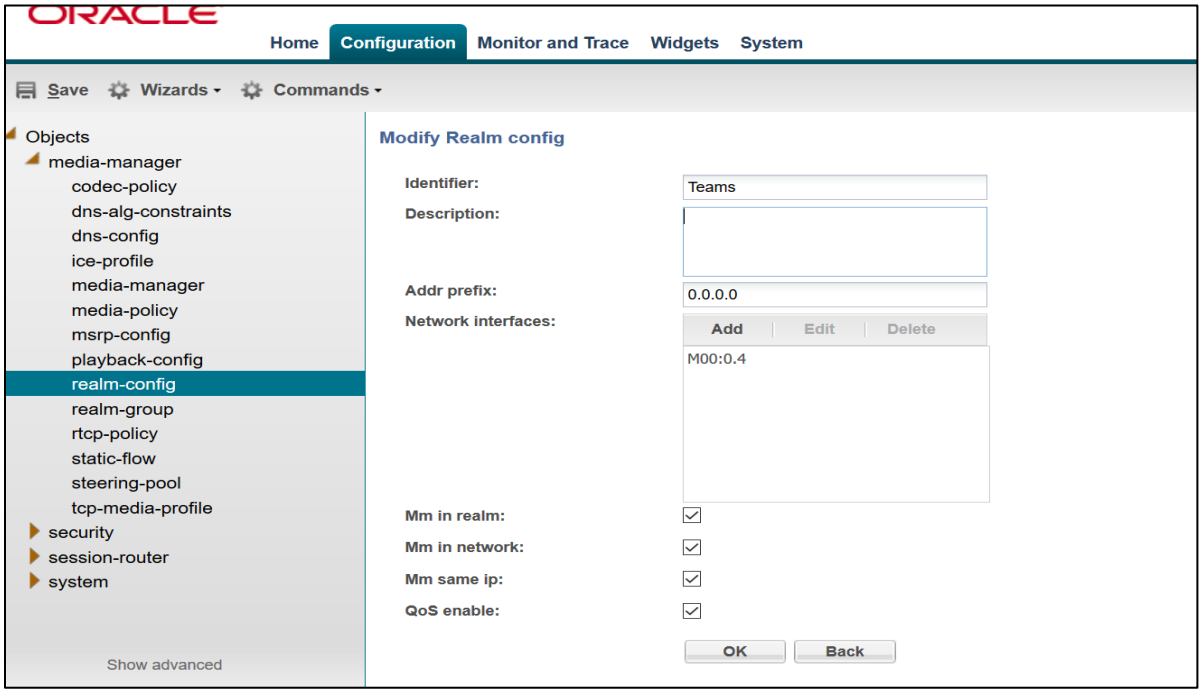
Teams FQDN in URI:

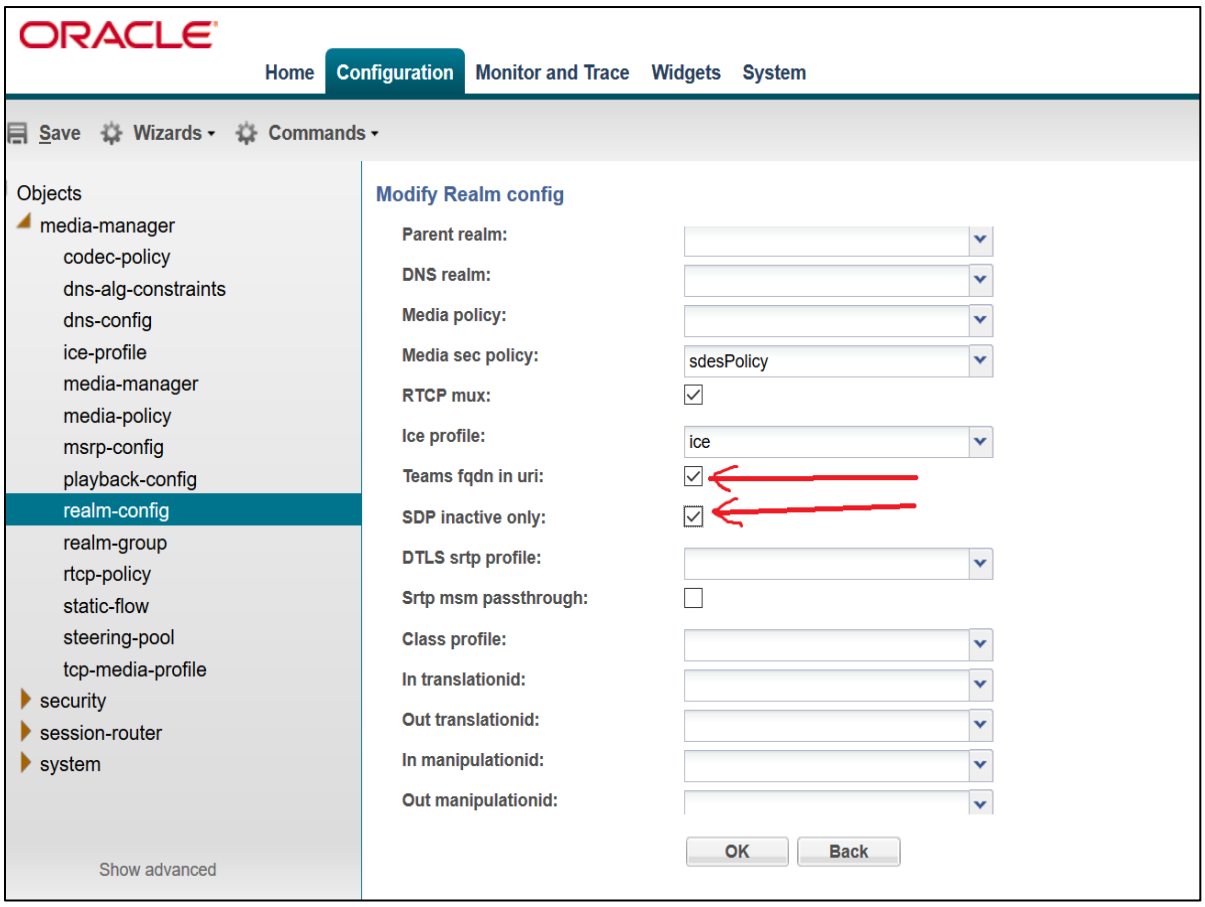
When enabled, this parameter takes the FQDN configured under hostname of the network interface, and inserts that into the Contact and FROM headers of Invites generated by the SBC towards Teams. This also adds a new "X-MS-SBC" Header to both Invite and OPTIONS Requests, which takes the place of the User-Agent header currently being added via Sip Manipulation. Lastly, SBC will add a Contact Header to outgoing SIP Options Pings, also containing the FQDN of the SBC listed under the hostname field of the network interface, and with the Contact Header added to OPTION Requests generated by the SBC, Record Route is no longer required.

SDP inactive only:

When enabled on Teams facing realm(s), this will modify the following SDP attributes in both requests and responses to and from Microsoft Teams

Message Type	Match Value	New Value
request	inactive	sendonly
reply	inactive	recvonly
request	sendonly	inactive
reply	recvonly	inactive

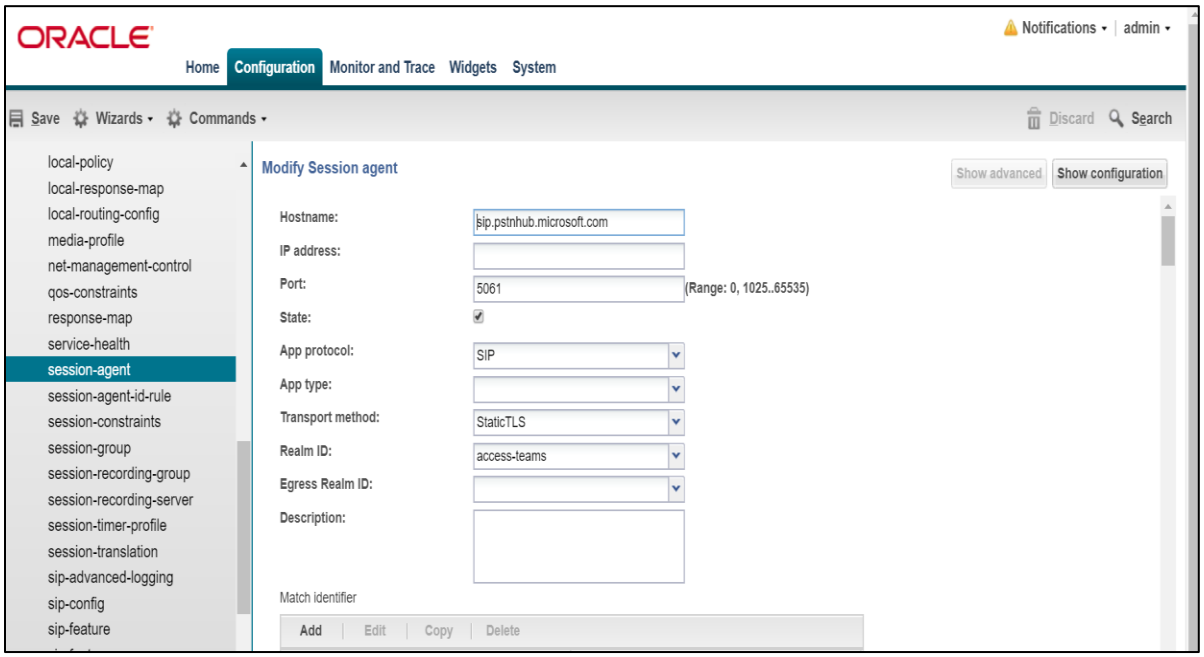

ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Objects
media-manager
codec-policy
dns-alg-constraints
dns-config
ice-profile
media-manager
media-policy
msrp-config
playback-config
realm-config
realm-group
rtcp-policy
static-flow
steering-pool
tcp-media-profile
security
session-router
system
Show advanced
Modify Realm config
Identifier:
Teams
Description:
Addr prefix:
0.0.0.0
Network interfaces:
Add
Edit
Delete
M00:0.4
Mm in realm:
Mm in network:
Mm same ip:
QoS enable:
OK
Back

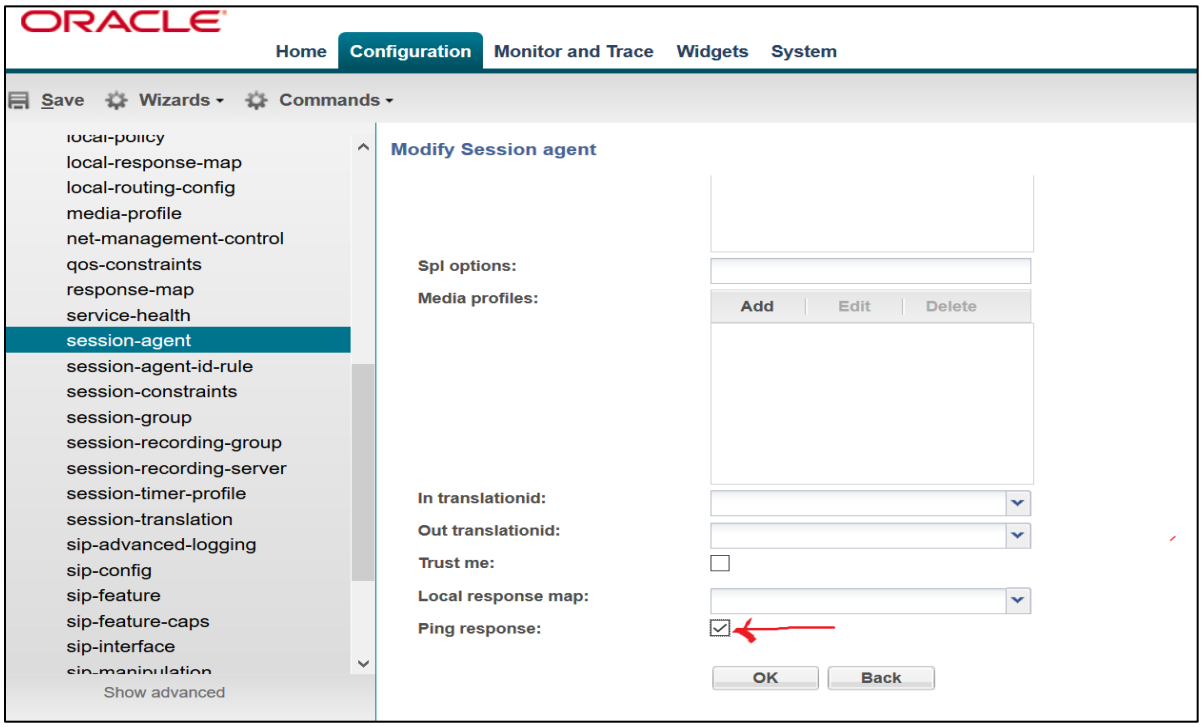

ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
Objects
media-manager
codec-policy
dns-alg-constraints
dns-config
ice-profile
media-manager
media-policy
msrp-config
playback-config
realm-config
realm-group
rtcp-policy
static-flow
steering-pool
tcp-media-profile
security
session-router
system
Show advanced
Modify Realm config
Parent realm:
DNS realm:
Media policy:
Media sec policy:
sdesPolicy
RTCP mux:
Ice profile:
ice
Teams fqdn in uri:
SDP inactive only:
DTLS srtp profile:
Srtp msm passthrough:
Class profile:
In translationid:
Out translationid:
In manipulationid:
Out manipulationid:
OK
Back

The third parameter is found under the **Session agent** configuration element and will be enabled on all three session agents configured for Microsoft Teams. The parameter name is **Ping response**.

Ping Response:

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

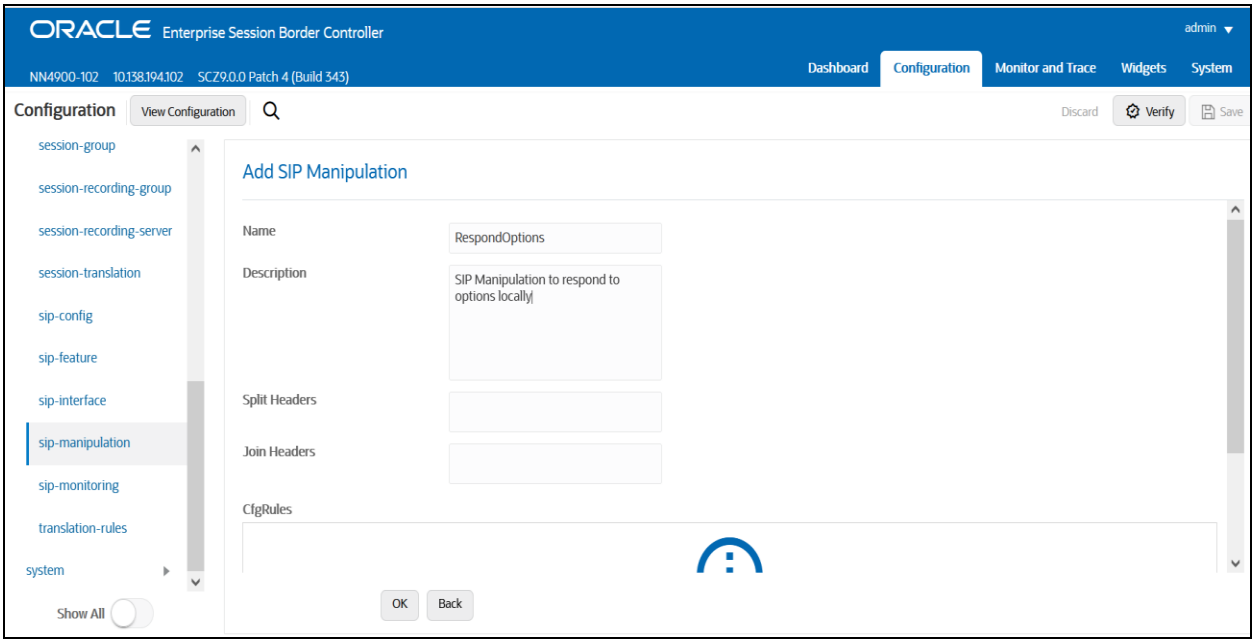




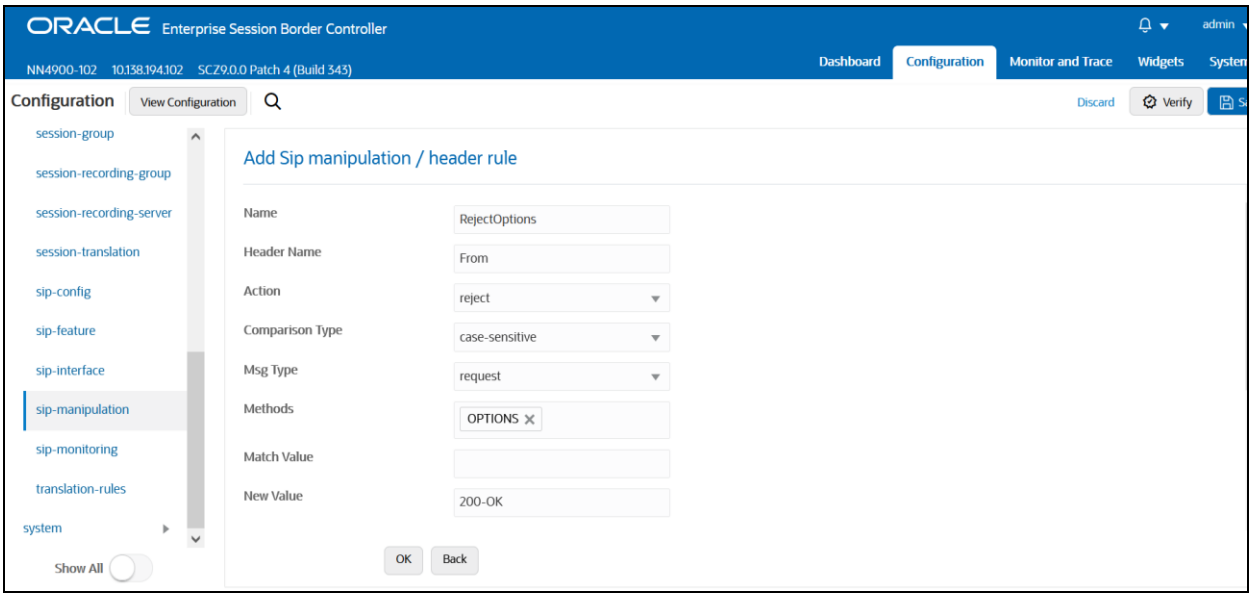
Respond to Options:

To ensure the SBC generates a 200OK response to SIP Options messages received from Teams, we'll configure the following sip-manipulation rule

Go to GUI Path: session router/sip manipulation and add the following:



Next, under CfgRules, select "header rule" in the "Add" drop down menu:



Click OK at the bottom when finished.

10. Existing SBC configuration

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

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

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

11. SIP Access Controls

The Oracle Session Border Controller (SBC) family of products are designed to increase security when deploying Voice over IP (VoIP) or Unified Communications (UC) solutions. Properly configured, Oracle's SBC family helps protect IT assets, safeguard confidential information, and mitigate risks—all while ensuring the high service levels which users expect from the corporate phone system and the public telephone network.

Please note, DDOS values are specific to platform and environment. For more detailed information please refer to the Oracle Communications SBC Security Guide.

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

However. While some values are environment specific, there are some basic security parameters that can be implemented on the SBC that will help secure your setup.

1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high

2. Set the access control trust level on public facing realms to HIGH

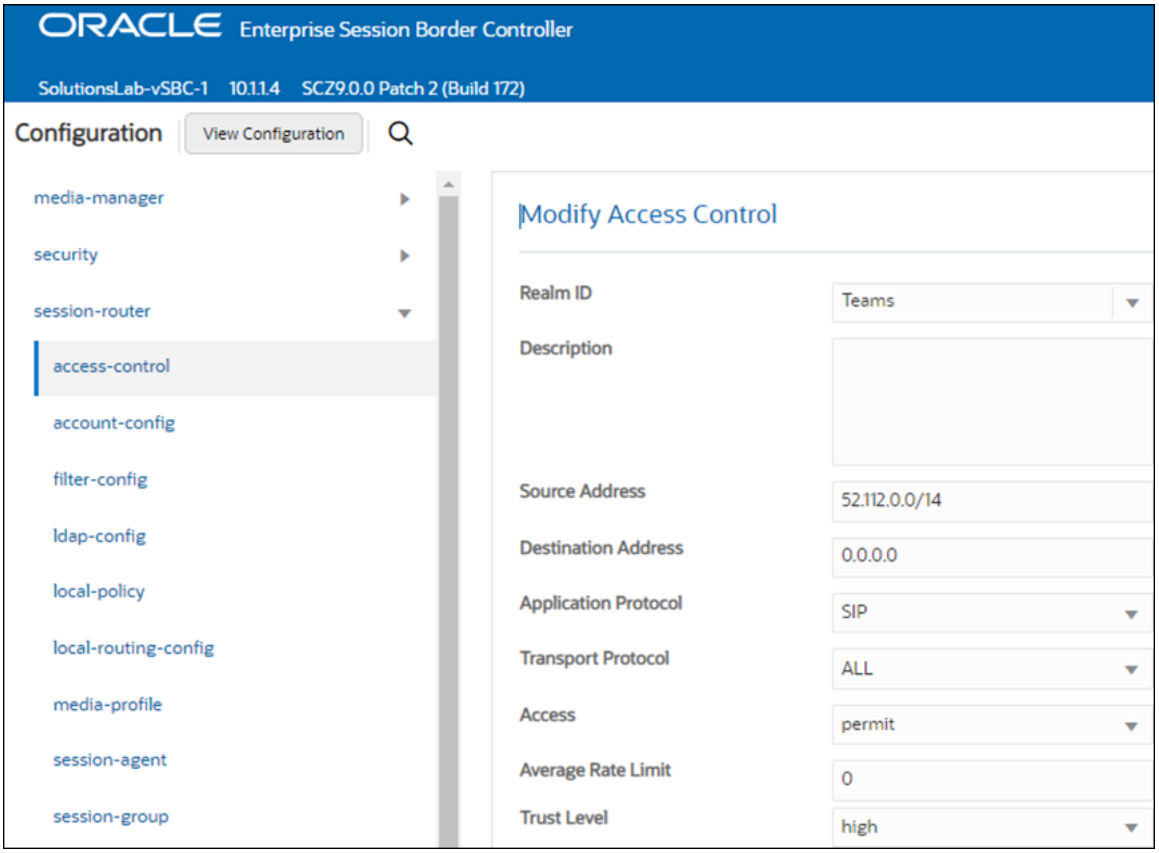
Microsoft Teams has two subnets, 52.112.0.0/14 and 52.120.0.0/14 that must be allowed to send traffic to the SBC. Both must be configured as an access control on the Oracle SBC and associated with the realm facing Teams.

Use this example to create ACL's for all MSFT Teams subnets. This example can be followed for any of the public facing interfaces, ie…SipTrunk, etc…

GUI Path: session-router/access-control

ACLI Path: config tàsession-routeràaccess-control

Use this example to create ACL's for both MSFT Teams subnets, 52.112.0.0/14 and 52.120.0.0/14.



- Select OK at the bottom

This concludes the required configuration of the SBC to properly interface with Microsoft Teams Phone System Direct Routing.

12 Caveat

In some environments, the methods in which Cisco CUCM uses to place a call on hold is not support by Microsoft Teams. In order to interwork between these two platforms, the Oracle SBC uses a series of sip manipulations given below as well as the **add-sdp-invite feature (Under SIP Interface where we can select re-invite as an option)** in order to avoid any disruptions to these call flows.

When CUCM places a user on hold, it uses RFC 2543, which is not supported by Microsoft Teams, so we create a sip manipulation to add the SBC's IP to the C line of SDP. Also, when retrieving the call from hold, Cisco sends an offer less invite. When this happens, MSFT returns a 200 OK to that invite, with a=inactive. In order to avoid this, we use the add sdp feature on the SBC set to re-invite. Unfortunately, when this happens, the SBC will take the last SDP it forwarded to Teams, which also contains a=inactive which needs to be removed. So we are not removing this attribute from all Invites towards Teams, we create Sip manipulation to identify re-invites without sdp, and then match on that identifier to strip a=inactive from the SDP, the SBC is adding with add-sdp-invite. This allows CUCM users to place calls on hold, and retrieve with no issues.

You can add these Sip manipulation to the SBC using either GUI or CLI mode and user is free to decide the way they want to add the sip manipulation.

1) Please add the below sip-manipulation as In-Manipulation on the Cisco Side to check for SDP, if no SDP, add Dummy Header.....

```
sip-manipulation
        name                            addNewHeaderNoSDP
        description
        split-headers
        join-headers
        header-rule
                name                    checkContentType
                header-name             Content-Type
                action                  store
                comparison-type         pattern-rule
                msg-type                request
                methods                 INVITE
                match-value             application/sdp
                new-value
        header-rule
                name                    addInfoHeader
                header-name             Info
                action                  add
                comparison-type         boolean
                msg-type                request
                methods                 INVITE
                match-value             !($checkContentType)
                new-value               "Cisco-INVITE-No-SDP"
```

2) Please add the below sip-manipulation as Out-Manipulation on the Teams side to change C line from all zero's to IP address, and then check for Dummy Header. If dummy header exists, delete inactive attribute. If it doesn't exist, inactive attribute remains.

```
sip-manipulation
    name                        FixSDP
    mime-sdp-rule
        name                    ModifySDP
        msg-type                request
        methods                 ACK,INVITE
        action                  manipulate
        sdp-session-rule
            name                ChangeCLine
            action              manipulate
            sdp-line-rule
                name            ChangeCLine
                type            c
                action          find-replace-all
                match-value     0.0.0.0
                new-value       <Public IP>

    header-rule
        name                    storeInfo
        header-name             Info
        action                  store
        comparison-type         case-sensitive
        msg-type                request
        methods                 INVITE
        match-value
        new-value
    mime-sdp-rule
        name                    removeInactive
        msg-type                request
        methods                 INVITE
        action                  manipulate
        comparison-type         boolean
        match-value             $storeInfo
        new-value
        sdp-media-rule
            name                DeleteAInactive
            media-type          audio
            action              manipulate
            comparison-type     boolean
            match-value         $storeInfo
            new-value
            sdp-line-rule
                name            DeleteInactive
                type            a
                action          delete
                comparison-type pattern-rule
                match-value     inactive
```

3) Finally, add the below sip manipulation as Out-Manipulation on the Cisco Side to match on inactive attribute in SDP of 200OK response. If a match is found, change the C line from IP address back to all zero's.

```
sip-manipulation
        name                            ChangIPSDPtoZero
        header-rule
                name                            FindInActiveAttribute
                header-name                     Content-Type
                action                          store
                msg-type                        reply
                methods                         INVITE
                element-rule
                        name                            IfFoundInActive
                        parameter-name                  application/sdp
                        type                            mime
                        action                          store
                        comparison-type                 pattern-rule
                        match-value                     a=inactive
        mime-sdp-rule
                name                            ChangeIP
                msg-type                        reply
                methods                         Invite
                action                          manipulate
                comparison-type                 boolean
                match-value                     $FindInActiveAttribute.$IfFoundInActive
                sdp-session-rule
                        name                            ChangeClineIP
                        action                          manipulate
                        sdp-line-rule
                                name                            IpChange
                                type                            c
                                action                          replace
                                new-value                       IN+" "+IP4+" "+0.0.0.0
```

Appendix A

Following are the test cases that are executed as part of Teams Direct Routing Enterprise Model with CUCM.

Serial Number	Test Cases Executed	Result
1	Device supports ptime of 20 ms for an inbound call to CUCM user	Pass
2	Device sends its own FQDN in the contact header	Pass
3	Device(CUCM Endpoint) accepts call from Teams user where the user's calling line identity is set to anonymous	Pass
4	Teams user places inbound call from CUCM on hold and then resumes	Pass
5	Teams user places outbound call to CUCM on hold and then resumes	Pass
6	Teams user places outbound call to CUCM on hold for over 15 minutes and then resumes	Pass
7	Inbound CUCM Call to Teams blind transferred to second Teams User	Pass
8	Outbound CUCM call from Teams user blind transferred to second Teams User	Pass
9	Inbound CUCM Call to Teams consultatively transferred to Teams User	Pass
10	Outbound CUCM call from Teams user consultatively transferred to Teams User	Pass
11	CUCM user calls Teams user that simultaneously rings second TEAMS/CUCM user and second user answers	Pass
12	CUCM user calls Teams user that is forwarded to second CUCM/TEAMS user	Pass
13	CUCM User calls Teams user when only SILK Codec is enabled on the Device trunk towards Teams but not on the Device trunk towards customer’s SIP trunk	Pass
14	Teams user calls CUCM user when only SILK Codec is enabled on the Device trunk towards Teams but not on the Device trunk towards customer’s SIP trunk	Pass
15	Teams user calls an IVR number and navigates through the IVR menu after call connection	Pass

16	Teams user calls into an external conference bridge and pastes a string of conference ID into Teams which is recognized by Device and IVR	Pass
17	Device sends comfort noise packets to Direct Routing interface when CUCM user mutes an outbound call	Pass
18	Device sends comfort noise packets to Direct Routing interface when CUCM user mutes an inbound call	Pass
19	Teams user mutes inbound call from CUCM and then unmutes	Pass
20	Device must provide SRTCP for a transcoded inbound call when service provider or gateway does not send SRTCP	Pass
21	Device must provide SRTCP for a transcoded outbound call when service provider or gateway does not send SRTCP	Pass
22	Device must provide SRTCP for an inbound call that doesn't involve transcoding when service provider or gateway does not send SRTCP	Pass
23	Device must provide SRTCP for an outbound call that doesn't involve transcoding when service provider or gateway does not send SRTCP	Pass
24	Device must indicate support for SRTCP multiplexing by including the a=rtcp-mux attribute in the offer	Pass
25	Device must respond with a=rtcp-mux attribute in the SDP response if the offer contains the same attribute	Pass

ORACLE

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