



# ORACLE

Oracle Session Border Controller (SBC)  
and Enterprise Communication Broker  
(ECB) 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 and ECB integration with Cisco CUCM and Microsoft Teams Enterprise Model	24th April 2020
1.1	Adding Caveat Section for On HOLD issue.	24th April 2021
1.2	Minor Formatting Changes	12th November 2021
1.3	Removed reference to sip-all FQDN from the app note document	12th January 2022
1.4	Refreshed the app note with testing of Oracle SBC and ECB integration with Cisco CUCM and Microsoft Teams Enterprise Model (CUCM in 12.5 and Oracle SBC 9.0 version)	22 <sup>nd</sup> April 2022
1.5	Since sip-all FQDN is removed, add the following two sections:  Enable refer call xfer on realm  Added RespondOptionsManip	22 <sup>nd</sup> July 2022
1.6	Added DigiCert Global G2 Cert as root CA for Teams Changed certificate-record screenshots Added SIP Access control	5 <sup>th</sup> -Sep-2022

## Table of Contents

<b>1. INTENDED AUDIENCE</b> .....	<b>5</b>
<b>2. DOCUMENT OVERVIEW</b> .....	<b>5</b>
<b>3. INTRODUCTION</b> .....	<b>7</b>
3.1. AUDIENCE .....	7
3.2. REQUIREMENTS.....	7
3.3. ARCHITECTURE .....	8
<b>4. CONFIGURING THE CISCO CUCM</b> .....	<b>9</b>
4.1. CONFIGURING A NEW SIP TRUNK .....	9
4.2. CONFIGURE A NEW ROUTE PATTERN.....	11
4.3. END USER CONFIGURATION.....	12
4.4. ADDING SIP PHONE IN CUCM.....	14
4.5. ASSOCIATING END USER TO PHONE .....	16
<b>5. REQUIREMENTS TO CONFIGURE MICROSOFT TEAMS DIRECT ROUTING</b> .....	<b>17</b>
5.1. TENANT REQUIREMENTS .....	17
5.2. LICENSING REQUIREMENTS .....	17
5.3. DNS REQUIREMENTS .....	17
5.4. SBC DOMAIN NAMES .....	18
5.5. PUBLIC TRUSTED CERTIFICATE FOR THE SBC.....	19
<b>6. CONFIGURE TEAMS DIRECT ROUTING</b> .....	<b>20</b>
6.1. ESTABLISH A REMOTE POWERSHELL SESSION .....	20
6.2. PAIR THE SBC TO THE TENANT .....	21
6.3. ENABLE USERS FOR DIRECT ROUTING.....	23
6.4. ASSIGN A PHONE NUMBER TO THE USER.....	24
6.5. CONFIGURE VOICE ROUTING .....	24
<b>7. MICROSOFT TEAMS DIRECT ROUTING INTERFACE CHARACTERISTICS</b> .....	<b>26</b>
<b>8. NEW ECB CONFIGURATION</b> .....	<b>28</b>
8.1. ECB CLI INITIAL CONFIG.....	28
8.2 LOGGING INTO THE ECB .....	31
8.3. ADD NETWORK SETTINGS.....	32
8.4. CONFIGURE SIP INTERFACE .....	33
8.5. CONFIGURING THE AGENTS .....	34
8.6. CONFIGURING THE ROUTING.....	35
<b>9. CONFIGURING THE SBC</b> .....	<b>38</b>
9.1. VALIDATED ORACLE SBC VERSION.....	38
<b>10. NEW SBC CONFIGURATION</b> .....	<b>38</b>
10.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC.....	38
10.2. CONFIGURE SBC USING WEB GUI.....	42
10.3. CONFIGURE SYSTEM-CONFIG.....	44
10.4. CONFIGURE PHYSICAL INTERFACE VALUES .....	45
10.5. CONFIGURE NETWORK INTERFACE VALUES .....	46
10.6. ENABLE MEDIA MANAGER .....	49
10.7. CONFIGURE REALMS .....	50
10.8. ENABLE SIP-CONFIG .....	51

10.9. CONFIGURING A CERTIFICATE FOR SBC.....	52
10.10.TLS PROFILE.....	57
10.11. CONFIGURE SIP INTERFACES.....	58
10.12. CONFIGURE SESSION-AGENT .....	61
10.13. CONFIGURE SESSION-AGENT GROUP .....	64
10.14. CONFIGURE SIP-MANIPULATION .....	66
10.15. CONFIGURE LOCAL-POLICY .....	70
10.16. CONFIGURE MEDIA PROFILE AND CODEC POLICY.....	72
10.17. CONFIGURE ICE-PROFILE.....	75
10.18. CONFIGURE STEERING-POOL.....	77
10.19. CONFIGURE SDES PROFILE .....	78
10.20. CONFIGURE MEDIA SECURITY PROFILE.....	79
10.21. CONFIGURE RTCP POLICY AND RTCP MUX .....	80
<b>11. EXISTING SBC CONFIGURATION .....</b>	<b>82</b>
<b>12 SIP ACCESS CONTROLS .....</b>	<b>82</b>
<b>13. CAVEAT .....</b>	<b>84</b>
<b>APPENDIX A.....</b>	<b>87</b>

## 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) and Oracle Enterprise Communication Broker (ECB). 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 and Oracle ECB. The solution contained within this document has been tested using Oracle Communication **OS830m1p7** and **OS900p2** version and Oracle ECB version **PCZ310p4** and **PCZ330p4**. 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/Final\\_version\\_Media\\_bypass.pdf](https://www.oracle.com/webfolder/technetwork/acmepacket/Microsoft/Final_version_Media_bypass.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 and ECB 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 and ECB 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.

**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. 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.**

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>

## 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 and Oracle ECB. There will be steps that require navigating the CUCM 11.5 / CUCM 12.5 server configuration, Oracle SBC GUI interface, Oracle ECB 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.

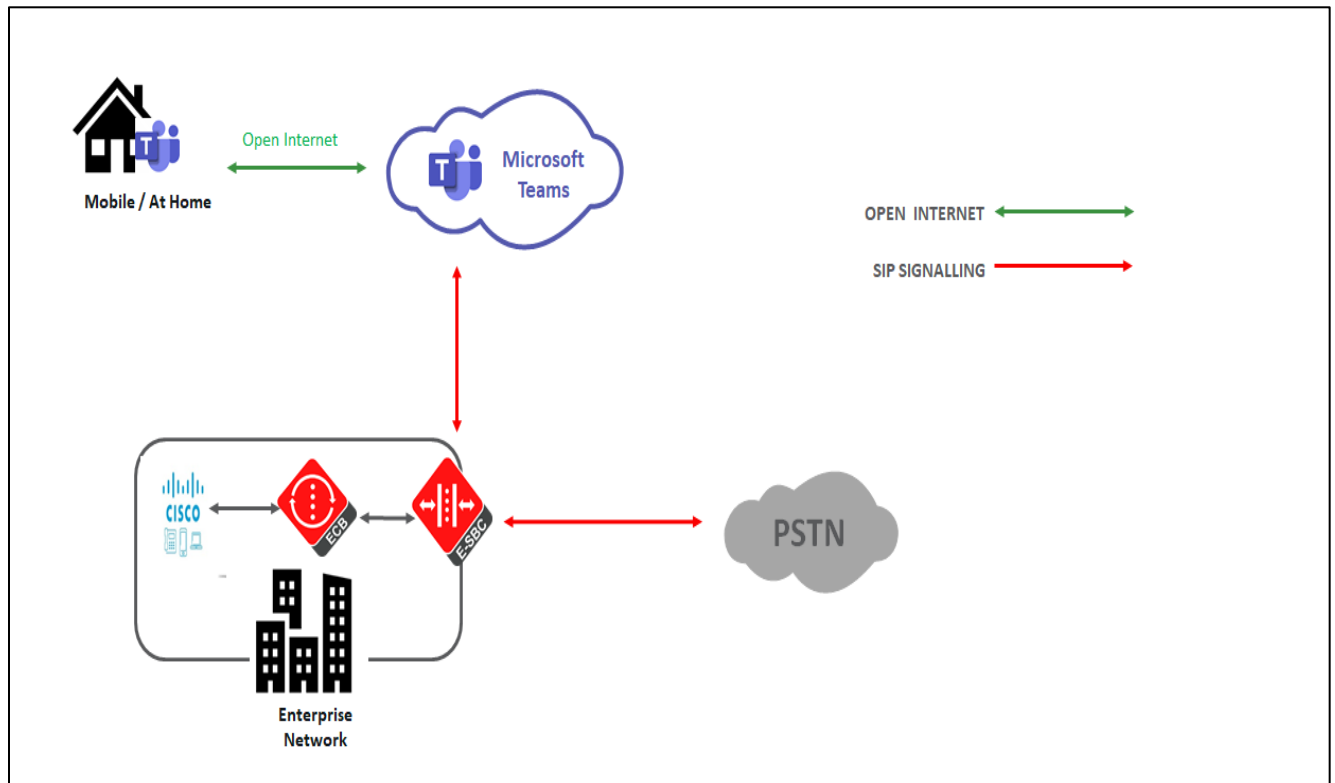
### 3.2. Requirements

- Fully functioning Cisco UCM 11.5 / CUCM 12.5
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.3.0 / 9.0.0 version
- Oracle Enterprise Communication Broker (hereafter Oracle ECB) running 3.1.0 / 3.3.0 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	ECB Version	Teams Client version
Revision 1	11.5	8.3.0	3.1.0	1.3.00.362 (64-bit) (Windows)
Revision 2	12.5	9.0.0	3.3.0	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 ECB
- Phase 4 – Configuring the Oracle SBC



## 4. Configuring the 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.

Please note that the pre-requisite for this config is that we have 10 digit DNs configured in the Cisco CUCM so that calls from CUCM is routed to Oracle ECB after the below configuration.

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

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

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

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

### 4.1. Configuring a new SIP Trunk

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



**Trunk Configuration**

Next

**Status**

Status: Ready

**Trunk Information**

Trunk Type*	SIP Trunk ▾
Device Protocol*	SIP ▾
Trunk Service Type*	None(Default) ▾

Next

\*- indicates required item.

**Status**

Status: Ready

**SIP Trunk Status**

**Service Status:** Full Service

**Duration:** Time In Full Service: 0 day 0 hour 1 minute

**Device Information**

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	<input type="text" value="CUCM-ECB"/>
Description	<input type="text"/>
Device Pool*	Default ▾
Common Device Configuration	< None > ▾
Call Classification*	Use System Default ▾
Media Resource Group List	< None > ▾
Location*	Hub_None ▾
AAR Group	< None > ▾

Please configure the IP of ECB sip interface as Destination Address here

SIP Information				
Destination				
<input type="checkbox"/>	Destination Address is an SRV			
	Destination Address	Destination Address IPv6	Destination Port	Status
1*	10.232.50.70		5060	up
MTP Preferred Originating Codec*	711ulaw			
BLF Presence Group*	Standard Presence group			
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile			
Rerouting Calling Search Space	< None >			
Out-Of-Dialog Refer Calling Search Space	< None >			
SUBSCRIBE Calling Search Space	< None >			
SIP Profile*	Standard Sip Profile - Options Enabled ISR <a href="#">View Details</a>			
DTMF Signaling Method*	No Preference			

## 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.

Route Pattern Configuration		Related
Save            Delete            Copy            Add New		
<b>Status</b>		
Status: Ready		
<b>Pattern Definition</b>		
Route Pattern*	1781443XXXX	
Route Partition	< None >	
Description	Route to ECB -SBC - Teams	
Numbering Plan	-- Not Selected --	
Route Filter	< None >	
MLPP Precedence*	Default	
<input type="checkbox"/> Apply Call Blocking Percentage		
Resource Priority Namespace Network Domain	< None >	
Route Class*	Default	
Gateway/Route List*	CUCM-ECB <a href="#">(Edit)</a>	
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern <input type="text" value="No Error"/>	

The route pattern that has been created is shown below:

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go  
admin | Search Documentation | About | Logout

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

**Find and List Route Patterns**

+ Add New Select All Clear All Delete Selected

Status  
12 records found

**Route Patterns (1 - 12 of 12)** Rows per Page 50

Find Route Patterns where Pattern begins with Find Clear Filter

Pattern	Description	Partition	Route Filter	Associated Device	Copy
1781443XXXX	Route to ECB -SBC - Teams			4600-SBC	
250[0-12]	toroutetoVM			CUC-VM-Trunk	
40XXXX	Route to SBC-Avaya-Endpoint			AvayaSip	
450[0-12]				CUC-VM-Trunk	
508255XXXX				4600-SBC	
6.184XXXXXXXXXXXX	NTT_anonymousprefix			NTT-Trunk	

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

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go  
admin | Search Documentation | About | Logout

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

**Find and List Trunks**

+ Add New Select All Clear All Delete Selected Reset Selected

SIP Trunk	Description	Partition	Route Filter	Associated Device	Service	Time In Full Service	Profile
CUC-VM-Trunk	forVM	Default	450[0-12]		No Service	Time not in Full Service: 4 days 5 hours 5 minutes	CUC-SIP trunk security profile
CUC-VM-Trunk	forVM	Default	250[0-12]		No Service	Time not in Full Service: 4 days 5 hours 5 minutes	CUC-SIP trunk security profile
CUCM-ECB		Default	1781443XXXX		Full Service	Time In Full Service: 0 day 0 hour 8 minutes	Non Secure SIP Trunk Profile
CUCM-ECB		Default	508255XXXX		Full Service	Time In Full Service: 0 day 0 hour 8 minutes	Non Secure SIP Trunk Profile
CUPS-SIP-Trunk		Default			No Service	Time not in Full Service: 4 days 5 hours 5 minutes	CUPS Trunk

### 4.3. End User Configuration

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

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

admin | Search Documentation | About

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

**End User Configuration** Related Links: [Back to Find List Users](#)

Save ~~X~~ Delete + Add New

**Status**

**i** Status: Ready

**User Information**

User Status: Enabled Local User

User ID\*: isrvolp1

Password: ..... [Edit Credential](#)

Confirm Password: .....

Self-Service User ID: 18507904044

PIN: ..... [Edit Credential](#)

Confirm PIN: .....

Last name\*: isrvolp1

Middle name: \_\_\_\_\_

First name: \_\_\_\_\_

Display name: \_\_\_\_\_

Title: \_\_\_\_\_

Directory URI: \_\_\_\_\_

Telephone Number: 18507904044

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go

admin | Search Documentation | About | Logout

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

**End User Configuration** Related Links: [Back to Find List Users](#) Go

Save ~~X~~ 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](#)

## 4.4. 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.

The screenshot displays the Cisco Unified CM Administration web interface for configuring a SIP phone. The page title is "Cisco Unified CM Administration" and the user is logged in as "admin". The navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The current page is "Phone Configuration" with a "Related Links" section containing "Back To Find/List".

At the top, there are action buttons: Save, Delete, Copy, Reset, Apply Config, and Add New. Below this is a "Status" section showing "Status: Ready".

The main configuration area is divided into three sections:

- Association:** Contains a table with two rows. Row 1: "Line [1] - 18507904044 (no partition)". Row 2: "Line [2] - Add a new DN". A "Modify Button Items" button is present above the table.
- Phone Type:** Shows "Product Type: Third-party SIP Device (Basic)" and "Device Protocol: SIP".
- Real-time Device Status:** Shows "Registration: Registered with Cisco Unified Communications Manager CUCM-Cisco.pe.oracle.com", "IPv4 Address: 10.232.50.2", "Active Load ID: None", and "Download Status: None".
- Device Information:** Shows "Device is Active" (checked), "Device is not trusted" (warning icon), "MAC Address\*: 00AABB11CCFF", "Description: ISRVolp1", "Device Pool\*: Default", "Common Device Configuration: < None >", and "Phone Button Template\*: Third-party SIP Device (Basic)".

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration  
admin | Search Documentation | About

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

**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 <a href="#">View Details</a>
Calling Search Space	< None >
AAR Calling Search Space	< None >
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Device Mobility Mode*	Default <a href="#">View Current Device Mobility Settings</a>
Owner	<input checked="" type="radio"/> User <input type="radio"/> 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

**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

## 4.5. 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.

The screenshot displays the 'End User Configuration' interface in Cisco Unified CM Administration. The page is divided into several sections:

- User Details:** Includes fields for Main ID, 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 a checked 'Home Cluster' checkbox, an unchecked 'Enable User for Unified CM IM and Presence' checkbox, and a 'UC Service Profile' dropdown set to 'Use System Default'.
- Device Information:** Features a 'Controlled Devices' dropdown menu with the value 'SEP00DC296352B' selected.
- Actions:** At the top left, there are buttons for 'Save', 'Delete', and 'Add New'. At the top right, there is a 'Related Links: Back to Find List Users' link with a 'Go' button.
- Device Association:** A 'Device Association' button is located at the bottom right, with a sub-label 'Line Appearance Association for Presence' below it.

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](mailto: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

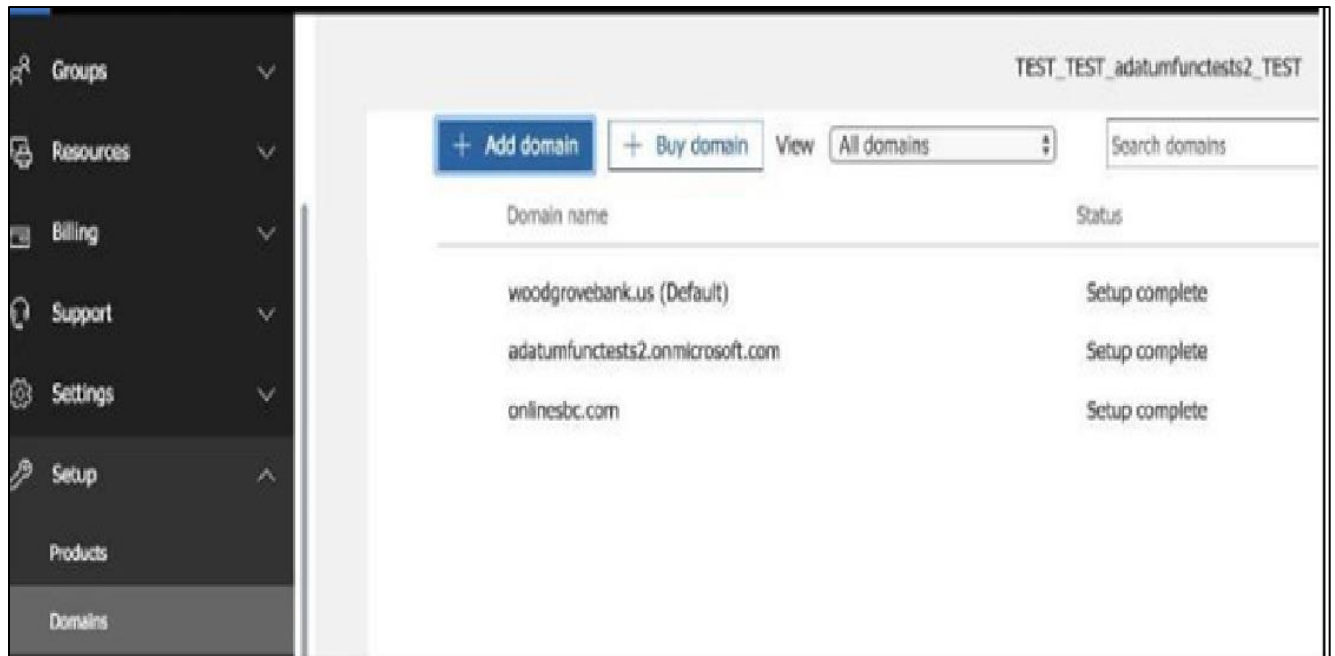
## 5.4. SBC Domain Names

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.

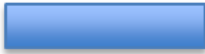
For example, on the picture below, the administrator registered the following DNS names for the tenant:

DNS Name	Can be used for SBC FQDN	Examples of FQDN names
woodgrovebank.us	Yes	Valid names: <ul style="list-style-type: none"> <li>• sbc1.woodgrovebank.us;</li> <li>• ussbcs15.woodgrovebank.us</li> <li>• europe.woodgrovebank.us</li> </ul> Non-Valid name: <ul style="list-style-type: none"> <li>• sbc1.europe.woodgrovebank.us (requires registering domain name europe.atatum.biz in “Domains” first)</li> </ul>
<a href="#">woodgrovebankus.onmicrosoft.com</a>	No	Using *.onmicrosoft.com domains is not supported for SBC names
<a href="#">hybrdvoice.org</a>	Yes	Valid names: <ul style="list-style-type: none"> <li>• <a href="#">sbc1.hybridvoice.org</a></li> <li>• <a href="#">ussbcs15.hybridvoice.org</a></li> <li>• <a href="#">europe.hybridvoice.org</a></li> </ul> Non-Valid name: <ul style="list-style-type: none"> <li>• <a href="#">sbc1.europe.hybridvoice.org</a> (requires registering domain name europe.<a href="#">hybridvoice.org</a> in “Domains” first)</li> </ul>

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
	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

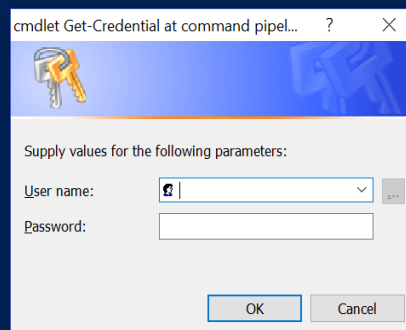
- Import-Module SkypeOnlineConnector
- \$userCredential = Get-Credential
- \$sfbSession = New-CsOnlineSession -Credential \$userCredential
- Import-PSSession \$sfbSession

```
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.

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

```
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
```



The screenshot shows a PowerShell console window with a dialog box titled "cmdlet Get-Credential at command pipel...". The dialog box has a blue header with a key icon and contains the text "Supply values for the following parameters:". Below this, there are two input fields: "User name:" with a dropdown menu and a small icon, and "Password:" with a text box. At the bottom of the dialog box are "OK" and "Cancel" buttons.

```
PS C:\Users\gabalakr> Import-Module SkypeOnlineConnector
    $userCredential = Get-Credential
    $sfbSession = New-CsOnlineSession -Credential $userCredential
    Import-PSSession $sfbSession
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:

ModuleType Version      Name                               ExportedCommands
-----
Script      1.0          tmp_fcnyz43x.w0h                 {Clear-CsOnlineTelephoneNumberReservation, ConvertTo-JsonForPSWS, Disable-CsMeetingRoom, Disable-CsOnlineDia...
```

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.

```
PS C:\Users\gabalakr> Get-Command *onlinePSTNGateway*

CommandType      Name                               Version      Source
-----
Function         Get-CsOnlinePSTNGateway          1.0          tmp_fcnyz43x.w0h
Function         New-CsOnlinePSTNGateway          1.0          tmp_fcnyz43x.w0h
Function         Remove-CsOnlinePSTNGateway       1.0          tmp_fcnyz43x.w0h
Function         Set-CsOnlinePSTNGateway          1.0          tmp_fcnyz43x.w0h
```

### 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 oraclesbc2.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.

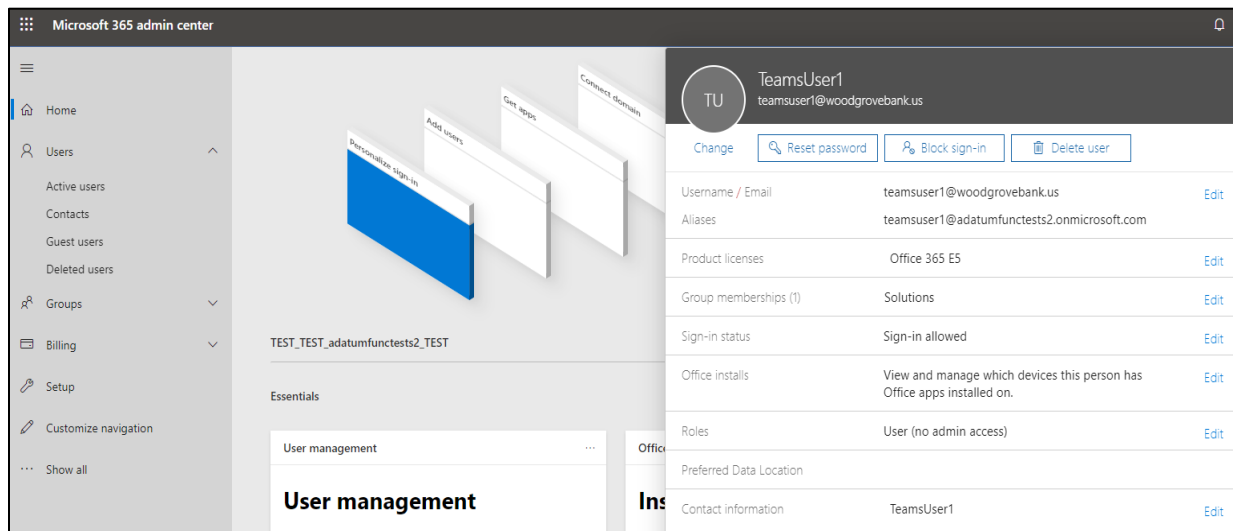
```
Identity           : oracleesbc2.woodgrovebank.us
Fqdn               : oracleesbc2.woodgrovebank.us
SipSignallingPort  : 5061
FailoverTimeSeconds : 10
ForwardCallHistory : True
ForwardPai        : True
SendSipOptions     : True
MaxConcurrentSessions :
Enabled           : True
MediaBypass       : 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](mailto: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 oraclelesbc2.woodgrovebank.us-Priority 1



```
PS C:\WINDOWS\system32> Set-CsOnlineVoiceRoute -id "Oracle_US" -NumberPattern ^(\+1[0-9]{10})$ -OnlinePstnGatewayList oraclesbc2.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, oraclesbc2.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	
Codecs	SRTP Crypto Suite	AES_CM_128_HMAC_SHA1_80, non-MKI	DTLS-SRTP is not supported
	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	<ul style="list-style-type: none"> <li>• G711</li> <li>• G722</li> <li>• Silk (Teams clients)</li> <li>• Opus (WebRTC clients) - Only if Media Bypass is used;</li> <li>• G729</li> </ul>	
	Other codecs	<ul style="list-style-type: none"> <li>• DTMF – Required</li> <li>• Events 0-16</li> <li>• CN</li> <li>• Required narrowband and wideband</li> <li>• RED – Not required</li> </ul> <p>Silence Suppression – Not required</p>	

## 8. New ECB Configuration

The Oracle ECB is available either as an appliance or as an application for operation on virtual machines. When running as an appliance, the Oracle ECB software is packaged with the Netra Server X3-2 and delivered to the end customers. When running as a virtual application, the Oracle ECB software can be deployed on any third-party COTS hardware that meets the specified guidelines.

Once the ECB is deployed (in the appliance mode or the application mode) and connected, you can power on the ECB. Software installation of the ECB is required upon first startup. Although the Oracle ECB is primarily configured through the GUI, you need to perform the software installation and certain steps via the CLI.

### 8.1. ECB CLI initial config

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

The default username for the User level is “user” and the default password is “acme”.

The default username for an Administrator level is “admin”, and the default 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 ECB 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 3.1.0 version

```
CUCM-ECB# conf t
CUCM-ECB(configure)# bootparam

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

Boot File      : /boot/nnPCZ310p4.bz
IP Address     : 10.138.194.175
VLAN           :
Netmask        : 255.255.255.192
Gateway        : 10.138.194.129
IPv6 Address   :
IPv6 Gateway   :
Host IP        :
FTP username   :
FTP password   :
Flags          :
Target Name    : CUCM-ECB
Console Device : VGA
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.
```

bootparam for 3.3.0 version

```
LabECB(configure)# bootparam

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

Boot File      : /boot/nnPCZ330p4.bz
IP Address     : 10.138.194.175
VLAN           :
Netmask        : 255.255.255.192
Gateway        : 10.138.194.129
IPv6 Address   :
IPv6 Gateway   :
Host IP        :
FTP username   :
FTP password   :
Flags          :
Target Name    : LabECB
Console Device : VGA
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.
```

Setup product type to Enterprise Communication broker as shown below.

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

```
CUCM-ECB# setup product

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

Last Modified 2017-02-03 09:44:20
-----
 1 : Product      : Enterprise Communication Broker

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

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

Save the changes and reboot the ECB.

```
CUCM-ECB# setup entitlements

-----
Entitlements for Enterprise Communication Broker
Last Modified: 2018-03-20 14:29:27
-----
 1 : Session Capacity      : 10000

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

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

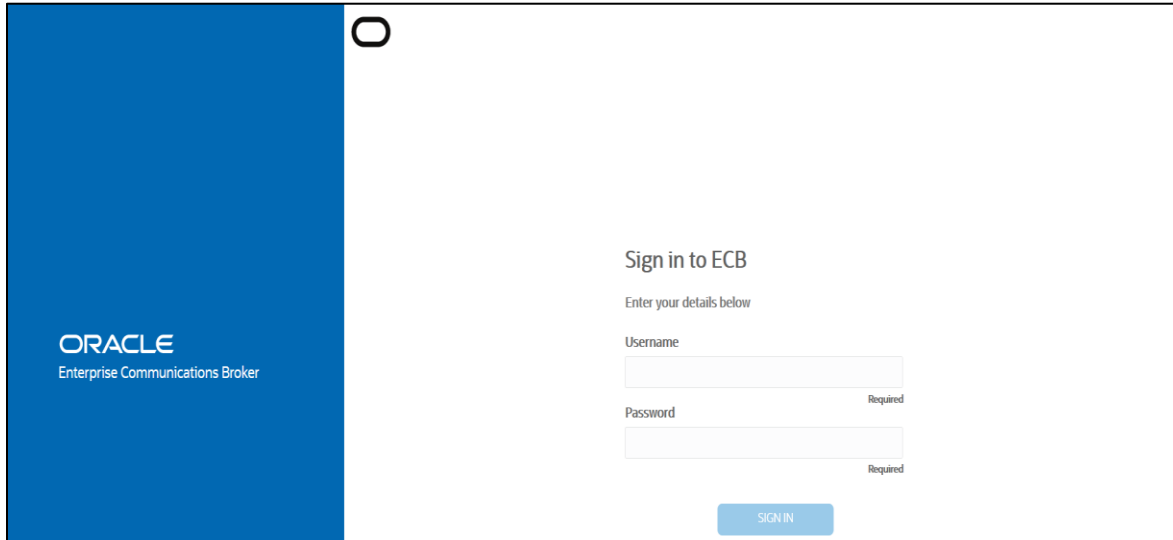
Enable the web-server-config to access the ECB using Web GUI. Save and activate the config.

```
CUCM-ECB(web-server-config)#
CUCM-ECB(web-server-config)# show
web-server-config
state                enabled
inactivity-timeout   10
http-state           enabled
http-port            80
https-state          disabled
https-port          443
http-interface-list
tls-profile
last-modified-by     web@
last-modified-date   2020-03-20 06:26:42

CUCM-ECB(web-server-config)# █
```

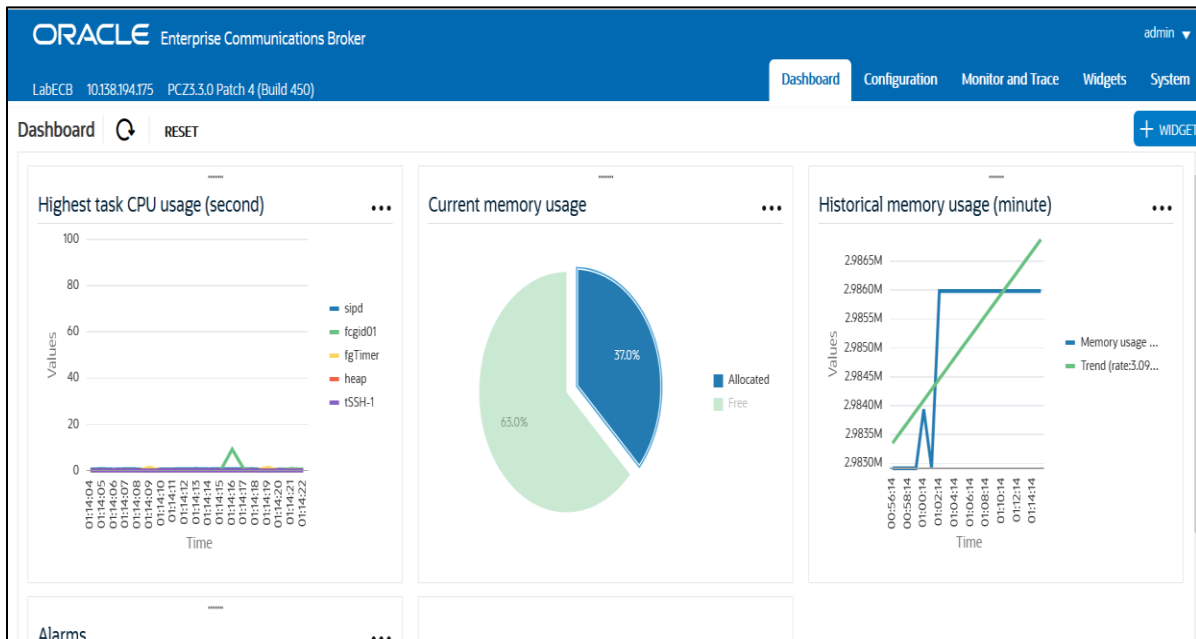
## 8.2 Logging into the ECB

You can now access the ECB through the Web GUI.  
Start an Internet browser and start the GUI using the URL: `http://server IP address/`.  
The login screen will appear.



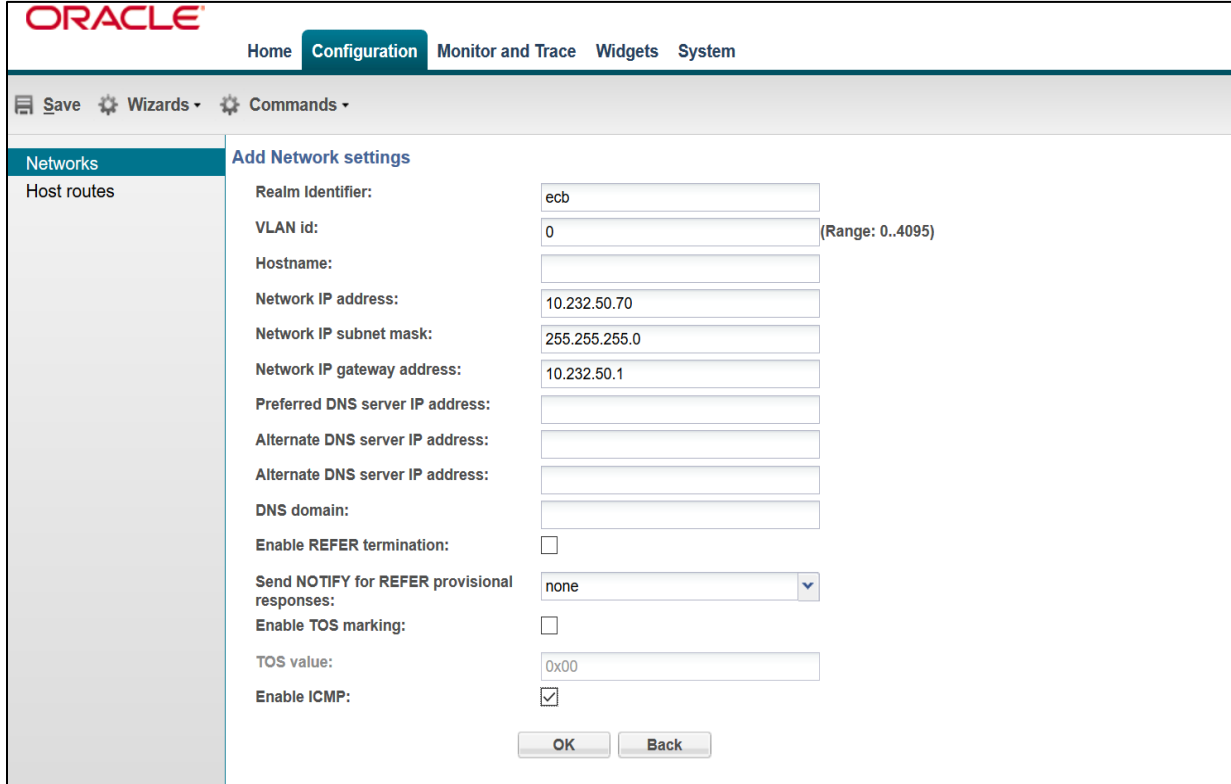
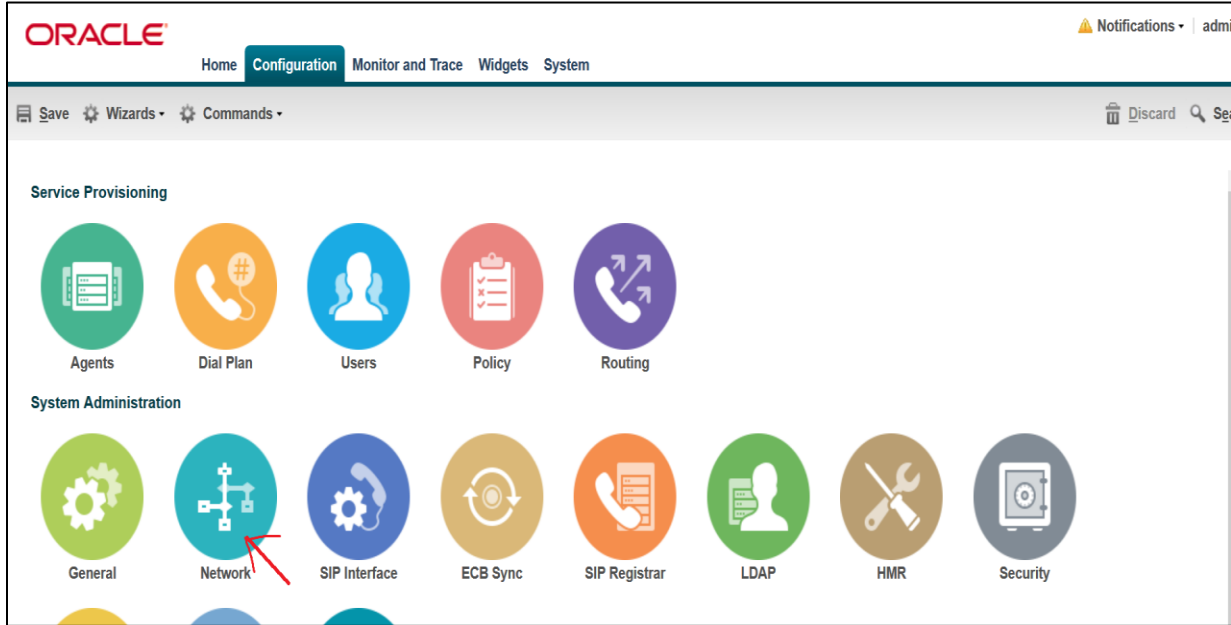
Enter the username and password and this is same as CLI username & password.  
After logging into the ECB, the Home screen will be displayed.

The Oracle ECB GUI has five tabs across the top –Home, Configuration, Monitor and Trace, Widgets and System.



### 8.3. Add Network Settings

Click the Configuration button at the top to go to the Configuration tab.  
Add network interface settings by clicking on the Network icon under System Administration

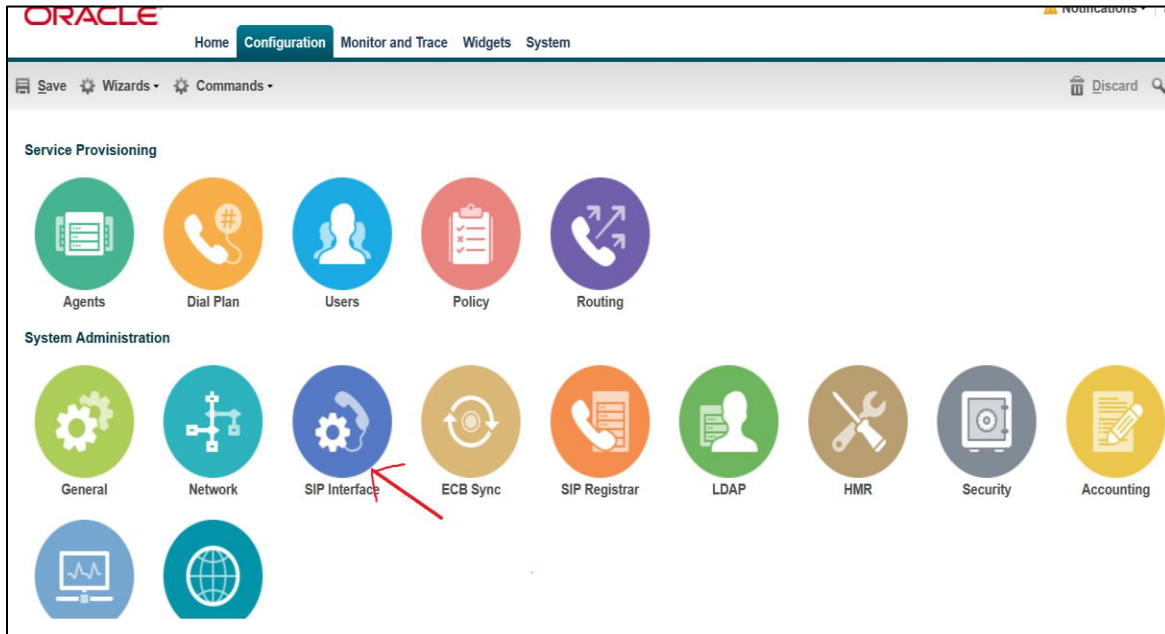




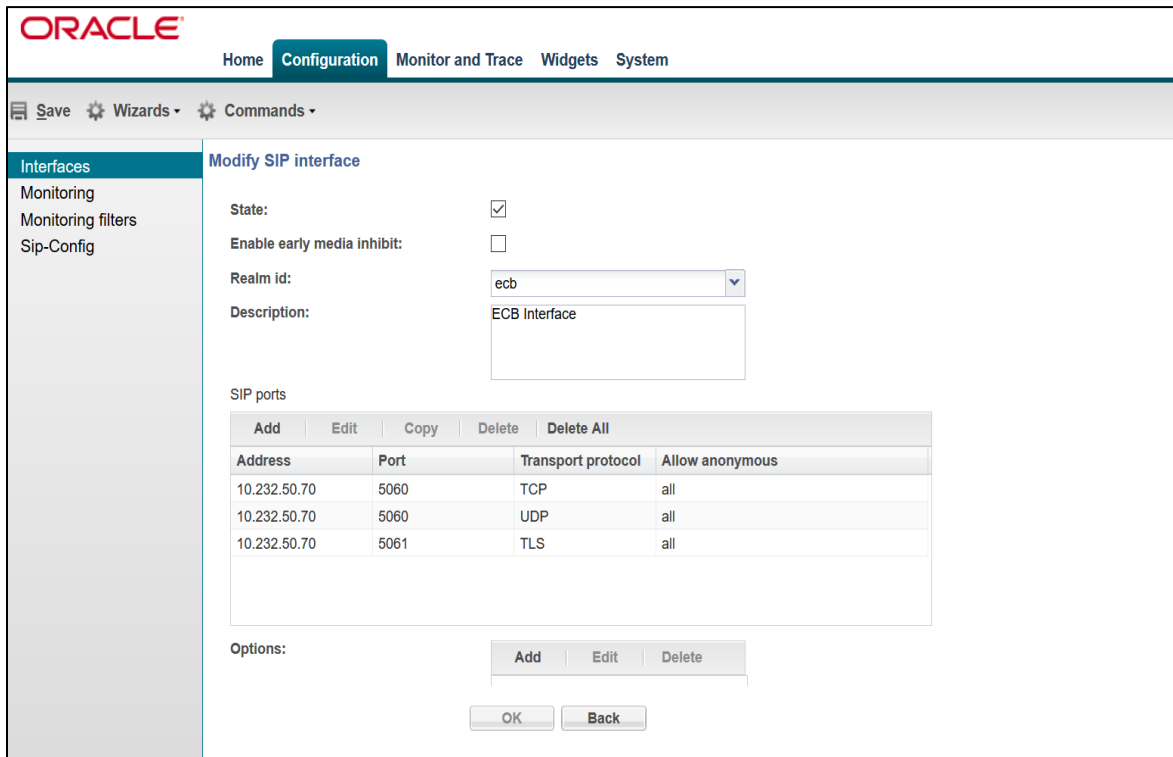
## 8.4. Configure SIP Interface

Click Configuration button to go to the Configuration tab.

Select the SIP Interface icon under System Administration to add the SIP interface of ECB.



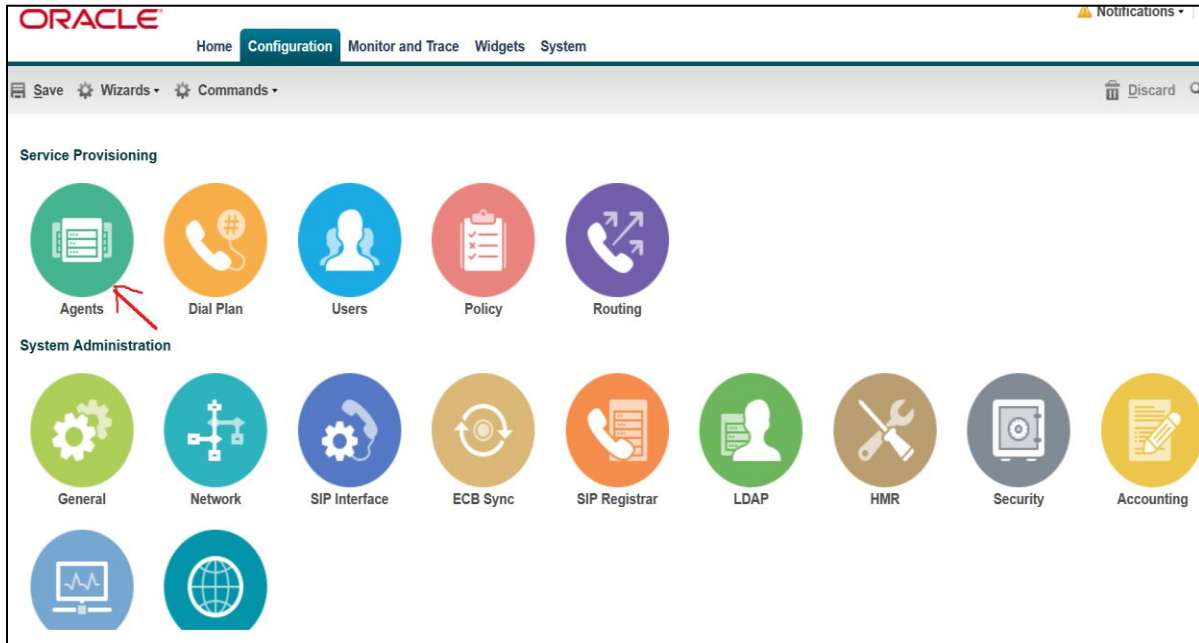
The following SIP interface is added with the sip-ports listed below



## 8.5. Configuring the Agents

Click Configuration --- Self Provisioning ----- Agents tab.

We will now add new Agents which are 10.232.50.89 (CUCM server) and 10.232.50.65 (SBC SIP interface)



The screenshot shows the 'Add Agents' form in the Oracle Self Provisioning Configuration interface. The top navigation bar and tabs are the same as in the previous screenshot. The left sidebar shows the 'Agent' menu with options for 'Enum server', 'Groups', and 'Additional Target Group'. The main content area is titled 'Add Agents' and contains the following fields:

Hostname:	<input type="text" value="10.232.50.89"/>
IP address:	<input type="text" value="10.232.50.89"/>
Port:	<input type="text" value="5060"/> (Range: 0, 1025..65535)
State:	<input checked="" type="checkbox"/>
RURI with Hostname:	<input type="checkbox"/>
Transport method:	<input type="text" value="UDP"/>
TLS profile:	<input type="text"/>
Realm id:	<input type="text" value="ecb"/>
Description:	<input type="text"/>
Source context:	<input type="text"/>
Egress URI mode:	<input type="text" value="no-conversion"/>
Egress number translation mode:	<input type="text" value="E164-no-plus"/>
Number of digits for n digit dialing:	<input type="text" value="4"/> (Range: 0..25)
Prepend prefix on egress:	<input type="text"/>

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

**ORACLE**

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands

**Agent** Add Agents

Enum server

Groups

Additional Target Group

Hostname: 10.232.50.65

IP address: 10.232.50.65

Port: 5060 (Range: 0, 1025..65535)

State:

RURI with Hostname:

Transport method: UDP

TLS profile:

Realm id: ecb

Description:

Source context:

Egress URI mode: no-conversion

Egress number translation mode: E164-no-plus

Number of digits for n digit dialing: 4 (Range: 0..25)

Prepend prefix on egress:

OK Back

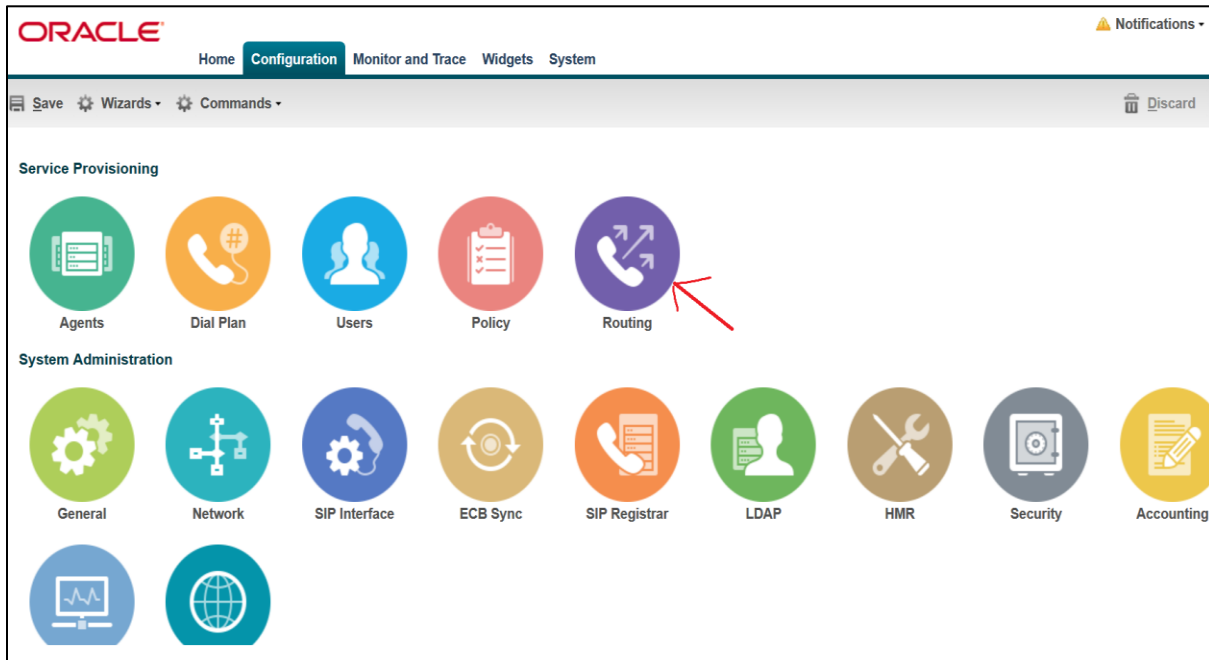
## 8.6. Configuring the Routing

The ECB performs its session routing via the route configuration. The route configuration establishes hop-by-hop paths to signaling endpoints.

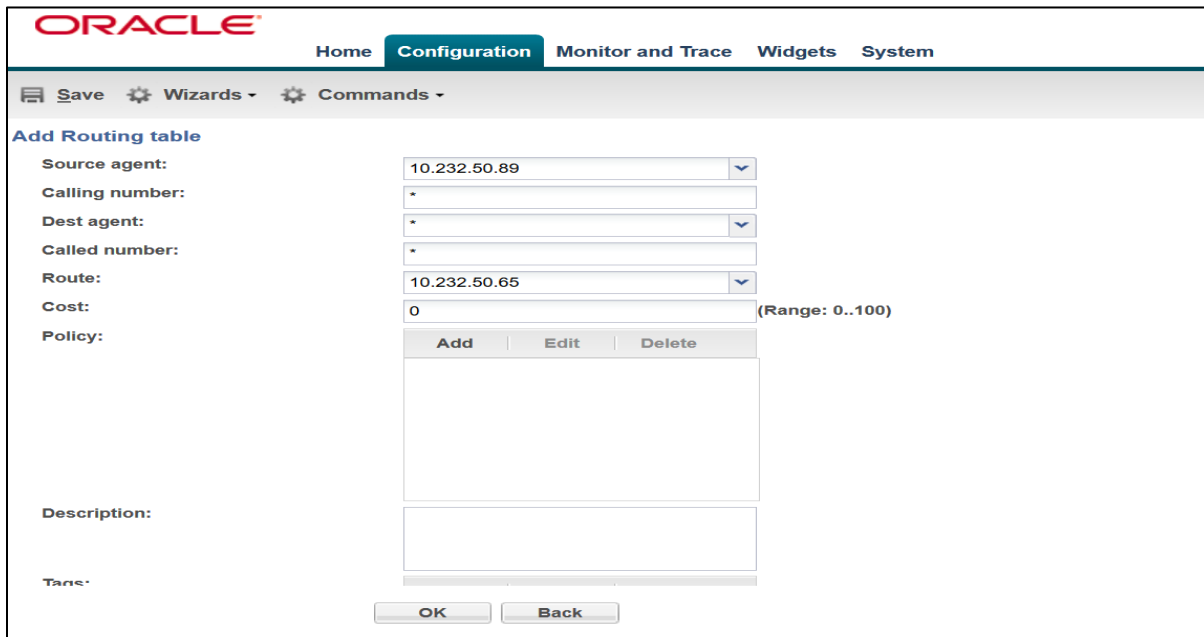
Oracle ECB routing configuration allows the user to specify a route's cost to specify route preference. Cost may or may not be based on monetary considerations. But the reach of an enterprise's network often does allow the user to configure routes that keep session traffic within the enterprise infrastructure rather than incurring cost associated with a service provider.

The Oracle ECB allows for a range of route preference criteria to differentiate between routing paths. Criteria include source routing based on the agent or calling number. Target-oriented criteria are also available, allowing the enterprise to designate preferred paths for specific called numbers.

Click on the Routing icon under Service Provisioning and Click Add to add a route.



Add a routing entry for the source agent CUCM server (10.232.50.89) with a route set to SBC IP (10.232.50.65) and click OK



When the ECB receives a call from 10.232.50.89, it looks up the user DB and finds that the agent 10.232.50.65 and routes the call to it.

Similarly, create a route from source agent 10.232.50.65 (SBC) to CUCM server (10.232.50.89)

The screenshot shows the Oracle Configuration interface. At the top, there is a navigation bar with the Oracle logo and tabs for Home, Configuration (selected), Monitor and Trace, Widgets, and System. Below the navigation bar, there are icons for Save, Wizards, and Commands. The main content area is titled "Add Routing table" and contains the following fields:

- Source agent: 10.232.50.65
- Calling number: \*
- Dest agent: \*
- Called number: \*
- Route: 10.232.50.89
- Cost: 0 (Range: 0..100)
- Policy: A table with columns Add, Edit, and Delete.
- Description: A text area.
- Tags: A text area.

At the bottom of the form, there are two buttons: OK and Back.

After making all the configurations in ECB, We will now save and activate our ECB configuration. The ECB configuration is now complete.

## 9. 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.

### 9.1. 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

## 10. New SBC configuration

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

### 10.1. 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.

### Bootparam for 8.3.0 version

```

NN4600-100# conf t
NN4600-100(configure)# bootparam

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

Boot File      : /boot/nnSCZ830mlp7.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   : vxftp
Flags          :
Target Name    : NN4600-100
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.

NN4600-100(configure)#
NN4600-100(configure)#
NN4600-100(configure)# █

```

### Bootparam for 9.0.0 version

```

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

```
NN4600-100# setup product
-----
WARNING:
Alteration of product alone or in conjunction with entitlement
changes will not be complete until system reboot

Last Modified 2019-06-28 14:05:33
-----
 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.

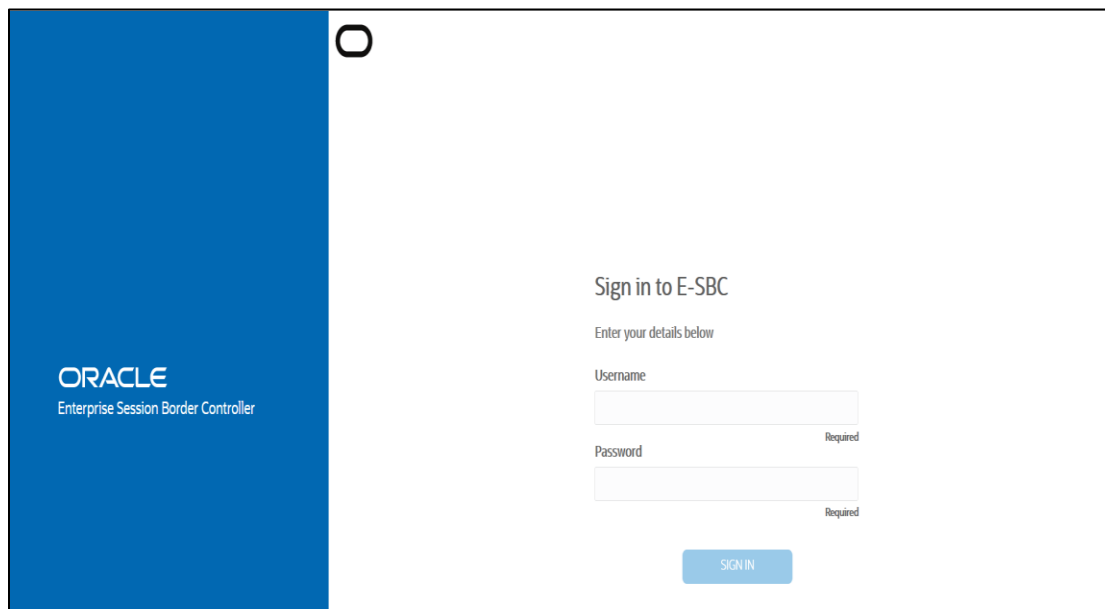
Enable the web-server-config to access the SBC using Web GUI. Save and activate the config.

```
NN4600-100 (web-server-config)# show
web-server-config
state                enabled
inactivity-timeout   5
http-state           enabled
http-port            80
https-state          disabled
https-port           443
http-interface-list  REST,GUI
tls-profile
last-modified-by     admin@console
last-modified-date   2020-04-03 00:21:22
NN4600-100 (web-server-config)# █
```

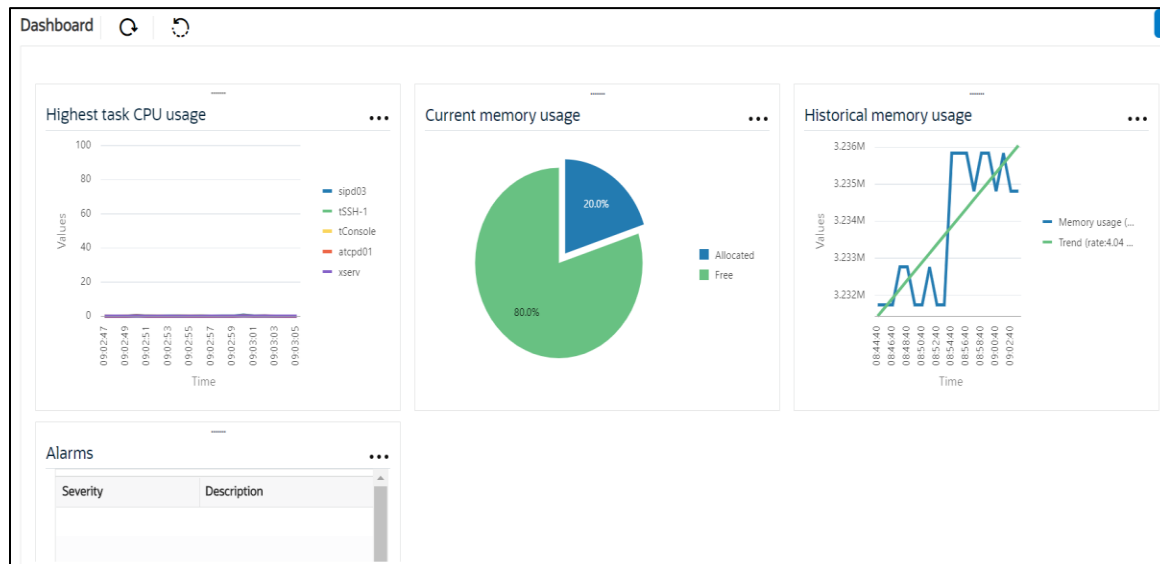
## 10.2. Configure SBC using Web GUI

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

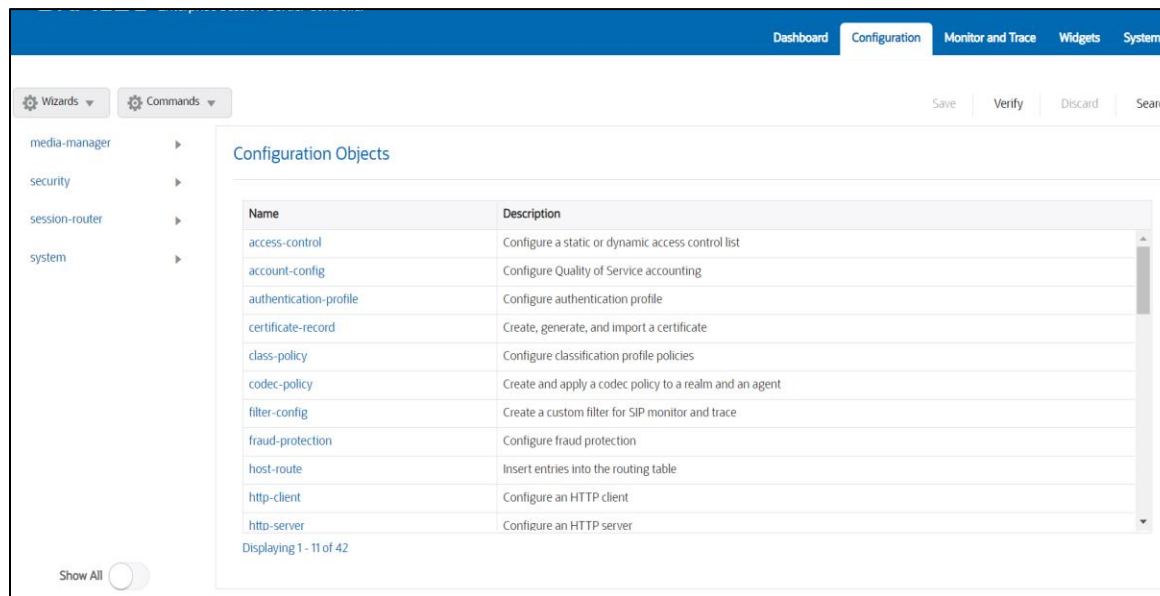
The Web GUI can be accessed through the url [http://<SBC\\_MGMT\\_IP>](http://<SBC_MGMT_IP>).



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



Go to Configuration as shown below, to configure the SBC



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

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

The expert mode is used for configuration.

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

### 10.3. Configure system-config

Go to system->system-config

The screenshot shows the Oracle Configuration Manager interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this is a toolbar with 'Save', 'Wizards', and 'Commands'. The left sidebar shows a tree view of objects, with 'system-config' selected. The main area is titled 'Modify System config' and contains the following fields and settings:

Hostname:	oracleesbc2.woodgrovebank.us
Description:	ESBC to Microsoft Teams Direct Routing
Location:	Bedford, MA
Mib system contact:	
Mib system name:	
Mib system location:	
Acp TLS profile:	
SNMP enabled:	<input checked="" type="checkbox"/>
Enable SNMP auth traps:	<input type="checkbox"/>
Enable SNMP syslog notify:	<input type="checkbox"/>
Enable SNMP monitor traps:	<input type="checkbox"/>
Enable env monitor traps:	<input type="checkbox"/>
Enable mblk_tracking:	<input type="checkbox"/>
Enable I2 miss report:	<input checked="" type="checkbox"/>

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.

## 10.4. 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 M00. This will be the port plugged into your (connection to the MS teams) interface. CUCM side is configured on the slot 0 port 1.

Parameter Name	MSTeams (M00)	CUCM (M10)
Slot	0	0
Port	0	1
Operation Mode	Media	Media

Below is the screenshot for creating a phy-interface on M00. Create a similar interface for Teams as well from the Web GUI. The table above specifies the values for both teams and CUCM.

The screenshot displays the Oracle Web GUI interface for configuring a physical interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below the navigation bar, there are icons for 'Save', 'Wizards', and 'Commands'. The left sidebar shows a tree view of objects, with 'phy-interface' selected under the 'system' category. The main content area is titled 'Modify Phy interface' and contains the following configuration fields:

- Name: M00
- 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)

At the bottom of the configuration area, there are 'OK' and 'Back' buttons.

## 10.5. 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	M00	M10
Host Name	<a href="http://oracleesbc2.woodgrovebank.us">oracleesbc2.woodgrovebank.us</a>	
IP address	<input type="text"/>	10.232.50.65
Netmask	255.255.255.192	255.255.255.0
Gateway	<input type="text"/>	10.232.50.1
DNS-IP Primary	8.8.8.8	
DNS-domain	woodgrovebank.us	

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

Save Wizards Commands

- 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

Show advanced

### Modify Network interface

Name: M00

Sub port id: 0 (Range: 0..4095)

Description:

Hostname:

IP address:

Pri utility addr:

Sec utility addr:

Netmask: 255.255.255.192

Gateway:

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

- 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

Show advanced

### Modify Network interface

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)

Signaling mtu: 0 (Range: 0, 576..4096)

HIP IP list:

Add Edit Delete

ICMP address:

Add Edit Delete

OK Back

Save Wizards Commands

- sip-monitoring
  - sip-recursion-policy
  - surrogate-agent
  - survivability
  - translation-rules
  - ▲ 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
- Show advanced

Modify Network interface

Name: M10

Sub port id: 0 (Range: 0..4095)

Description:

Hostname:

IP address: 10.232.50.65

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

Save Wizards Commands

- sip-monitoring
  - sip-recursion-policy
  - surrogate-agent
  - survivability
  - translation-rules
  - ▲ 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
- Show advanced

Modify Network interface

DNS IP primary:

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

10.232.50.65

ICMP address:

Add Edit Delete

10.232.50.65

OK Back



## 10.6. 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. A reboot of SBC is needed after adding audio allow hidden option.

- audio-allow-assymmetric-pt
- xcode-gratuitous-rtcp-report-generation

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

ORACLE Home Configuration Monitor and Trace Widgets System Notifications admin

Save Wizards Commands Discard Search

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
- access-control
- account-config

Modify Media manager

Show advanced

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

audio-allow-asymmetric-pt

xcode-gratuitous-rtcp-report-generation

ORACLE Home Configuration Monitor and Trace Widgets System Notifications admin

Save Wizards Commands Discard Search

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

Modify Media manager

Show advanced

Red max trans: 10000 (Range: 0..50000)

Red sync start time: 5000 (Range: 0..4294967295)

Red sync comp time: 1000 (Range: 0..4294967295)

Media policing:

Max signaling bandwidth: 10000000 (Range: 71000..10000000)

Max untrusted signaling: 1 (Range: 0..100)

Min untrusted signaling: 1 (Range: 0..100)

Tolerance window: 30 (Range: 0..4294967295)

Untrusted drop threshold: 0 (Range: 0..100)

Trusted drop threshold: 0 (Range: 0..100)

Acl monitor window: 30 (Range: 5..3600)

Trap on demote to deny:

Trap on demote to untrusted:

Syslog on demote to deny:

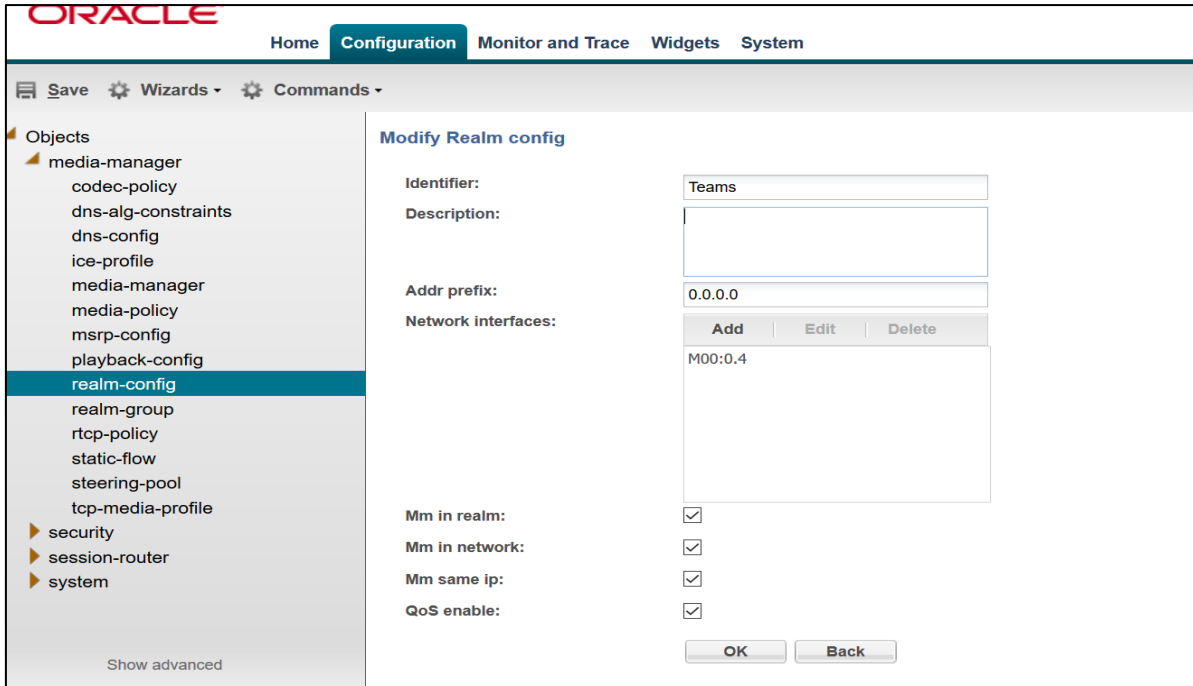
Svslog on demote to untrusted:

OK Delete

## 10.7. 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 (CUCM to Teams via ECB and SBC)  
Please set "Refer Call Transfer" parameter to Enabled for Teams Realm

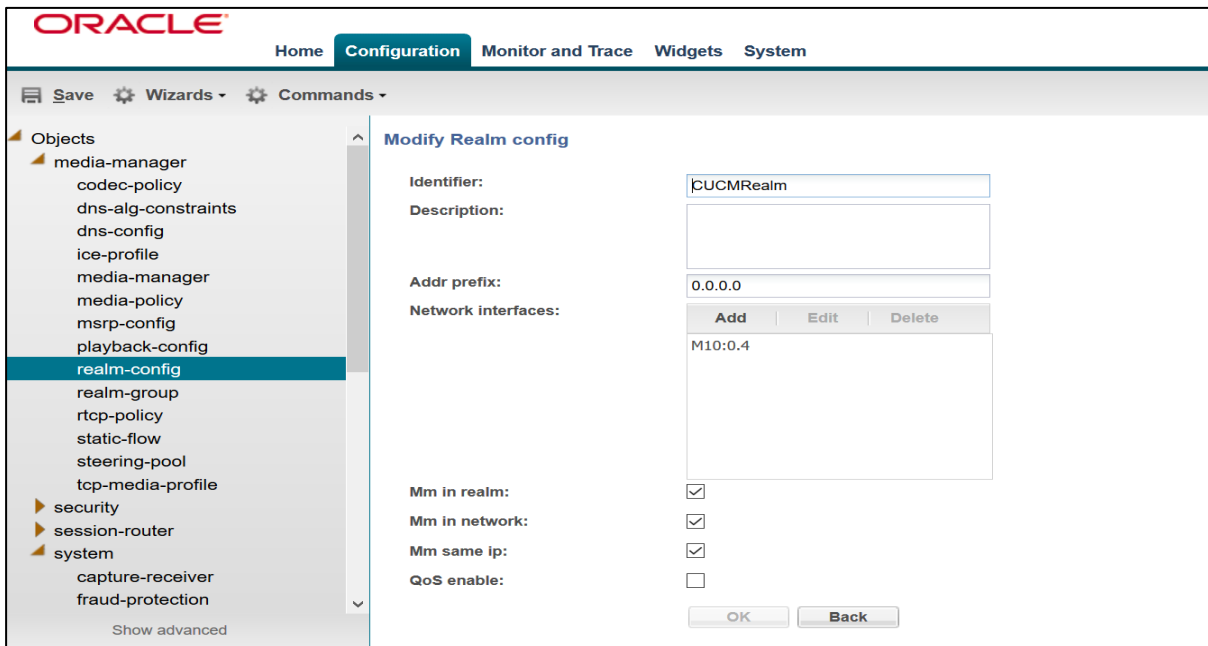


The screenshot shows the Oracle Configuration Manager interface. The 'Configuration' tab is active. In the left-hand 'Objects' tree, 'realm-config' is selected under 'media-manager'. The main area displays the 'Modify Realm config' dialog with the following fields and options:

- Identifier: Teams
- Description: (empty)
- Addr prefix: 0.0.0.0
- Network interfaces: A table with one entry: M00:0.4. Above the table are buttons for 'Add', 'Edit', and 'Delete'.
- Mm in realm:
- Mm in network:
- Mm same ip:
- QoS enable:

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

Similarly, Realm name is given as CUCMRealm (Teams to CUCM via SBC and ECB)



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

- Identifier: CUCMRealm
- Description: (empty)
- Addr prefix: 0.0.0.0
- Network interfaces: A table with one entry: M10:0.4. Above the table are buttons for 'Add', 'Edit', and 'Delete'.
- Mm in realm:
- Mm in network:
- Mm same ip:
- QoS enable:

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

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>

## 10.8. Enable sip-config

SIP config enables SIP handling in the SBC.

Make sure the home realm-id, registrar-domain and registrar-host are configured.

Also add the options to the sip-config as shown below.

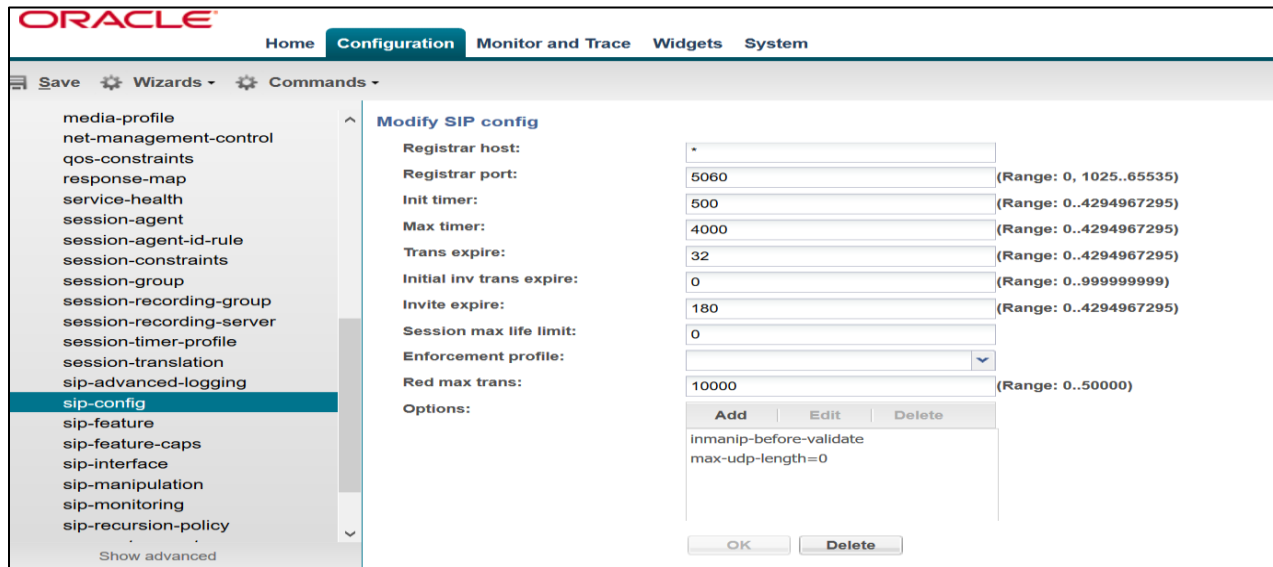
To configure sip-config, Go to Session-Router->sip-config and in options

- add max-udp-length =0.
- inmanip-before-validate

The screenshot displays the Oracle SBC Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this, there are tabs for 'Save', 'Wizards', and 'Commands'. A left-hand sidebar lists various configuration categories, with 'sip-config' highlighted. The main area is titled 'Modify SIP config' and contains the following fields:

State:	<input checked="" type="checkbox"/>
Dialog transparency:	<input checked="" type="checkbox"/>
Home Realm ID:	Teams
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

At the bottom of the form are 'OK' and 'Delete' buttons.



## 10.9. 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 certificate signed by this authority)
- DigiCert Global G2 Cert (Microsoft Presents the SBC a certificate 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

The screenshot shows the Oracle Enterprise Session Border Controller configuration page. The top navigation bar includes the Oracle logo and the text 'Enterprise Session Border Controller'. Below this, the system information 'NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)' is displayed. The main configuration area is titled 'Configuration' and includes a 'View Configuration' button and a search icon. A sidebar on the left lists various configuration categories: media-manager, security, authentication-profile, certificate-record (highlighted), tls-global, tls-profile, session-router, and system. The main content area is titled 'Add Certificate Record' and contains the following fields:

- Name: SBCCertificateforTeams
- Country: US
- State: MA
- Locality: Burlington
- Organization: Engineering
- Unit: (empty)
- Common Name: telechat.o-test-06161977.com
- Key Size: 2048
- Alternate Name: (empty)
- Trusted:  enable
- Key Usage List: digitalSignature, keyEncipherment
- Extended Key Usage List: serverAuth, clientAuth

- 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>

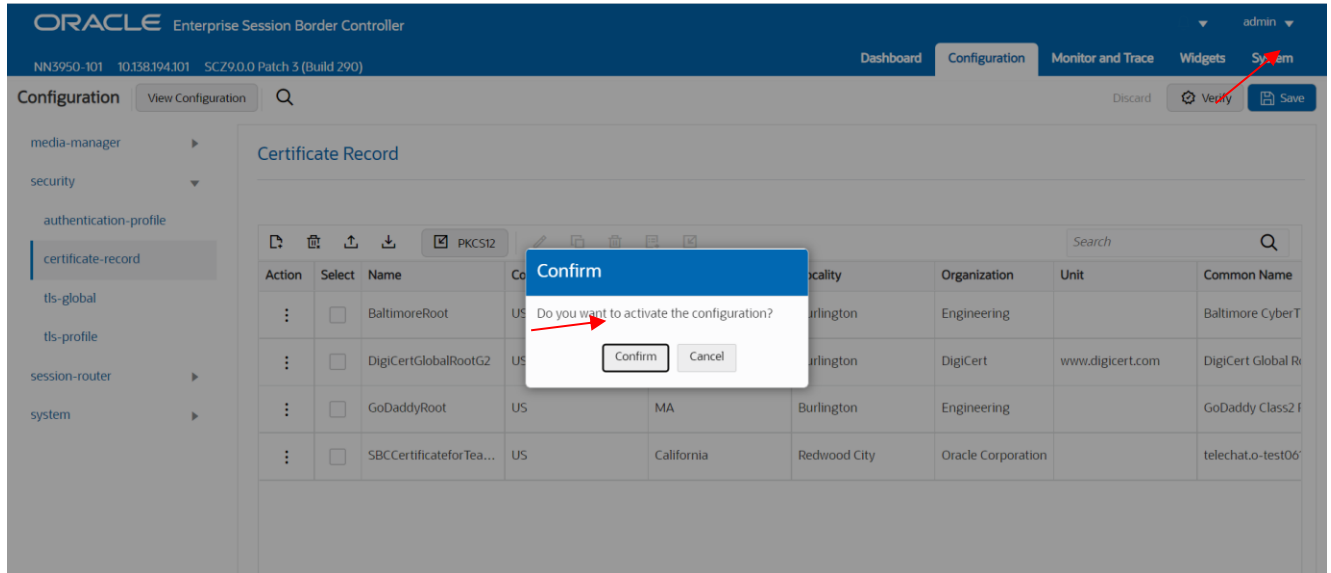
Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', user 'admin', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the 'Certificate Record' section is selected in the left sidebar. The main content area displays a table of certificate records with columns for Action, Select, Name, Country, State, Locality, Organization, Unit, and Common Name. The table contains four entries: BaltimoreRoot, DigiCertGlobalRootG2, GoDaddyRoot, and SBCCertificateforTea... (partially visible).

Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
:	<input type="checkbox"/>	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberT
:	<input type="checkbox"/>	DigiCertGlobalRootG2	US	MA	Burlington	DigiCert	www.digicert.com	DigiCert Global R
:	<input type="checkbox"/>	GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 F
:	<input type="checkbox"/>	SBCCertificateforTea...	US	California	Redwood City	Oracle Corporation		telechat.o-test06'

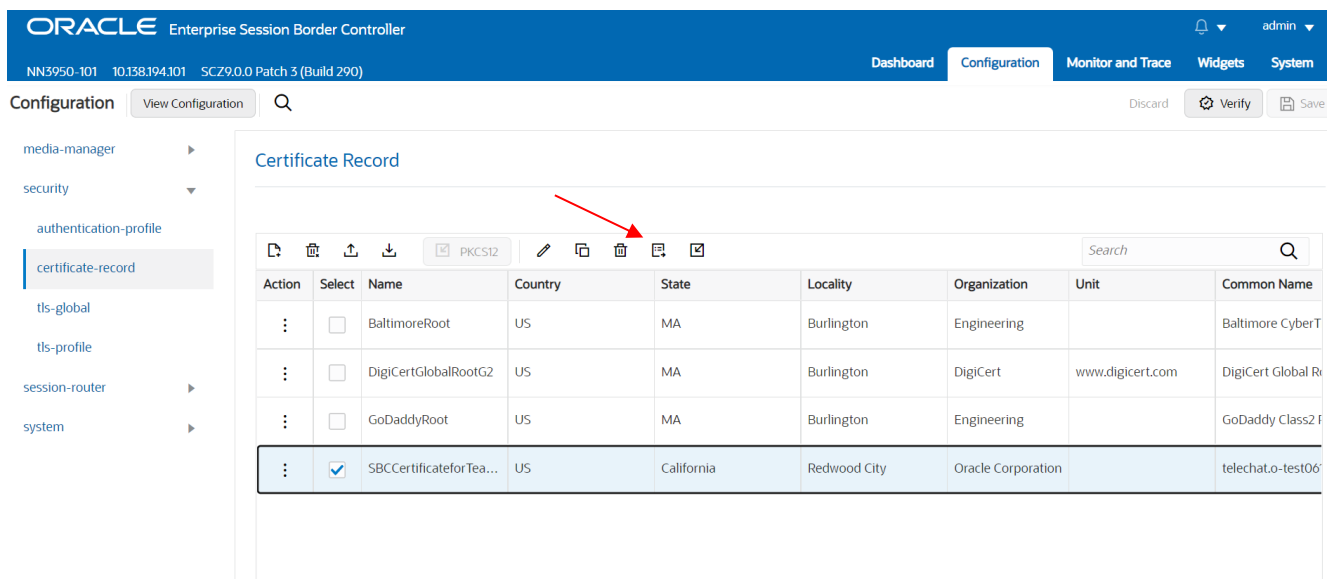
At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must **save and activate** the configuration of the SBC.



### 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 intermediate 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:



### Generate certificate response

Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwbDELMAkGA1UEBhMCVVMxZzA1BjBjNVBAgTAKIBMRMwEQYDVQQL
EwpCdXJsaW5ndG9uMRQwEgYDVQKEwTfmdpbmVlcmluZzEIMCMGAIUEAxMcdGVs
ZWNoYXQuYm9uZG9uMRQwEgYDVQKEwTfmdpbmVlcmluZzEIMCMGAIUEAxMcdGVs
ADCCAQoCggEBAK+uhx7951uhDgtQqWvo4EoZE68WDLIDYPPYcJWbvL5uWzk6y3Yh
s40ca4ZuZWmrLNJLJZFv9x9R5KzM4M8wqYiUvPOBC6oowuautu/swSKlReSpfDZh
NaAGUJrvAfVacyPz7KsyrJKgchzsOFNNJPDAAQsDQjuoFCDUbtOA1Z6xDFxpCdIF
nhq+dtB7gAtCdvWE/V6r4PAfJ1dj82YT4YBAWqwQJ2wGn+yc2FEPSmHlBWEiCvR
sMGfUeJcTM5i//AVcpF+jsJc8xswtE+Zr24kEiCrcrm0llgDHRvEgY1TuUteFoLy
d/60oaVPYHkKn250HQ2lwaMllkMxpBjlpUCAwEAAsA9MDsGCsGqGS1b3DQEJDIJEU
MCwwCwYDVROPAQDAgWgMB0GAlUdJQQWMBQGCsGAQUFBwMBBggrBgEFBQcDAjAN
BgkqhkiG9w0BAQsFAAOCAQEAnBLJuRPL82rkQDIB3I2JeOf3tacevMQeC1GcdFCf
uLcey+2XmtKF+HHPIECde+tLkXiJseVlnfBT2Ba4KymPwmTkQ5DfoLYQjWFOhEsm
LcuKMvjBYekJwebDk9CtDWwBZ9O1DzYbyuVNXPLbID5ludWbJBAYwd+9693VUVQb
/UR5rooNKwQIOFJMNmuPMW13v/p7kVsItk8aSwF6lHNx+k56MrR45YFqV//zCQTs
PeTYRyOVGYSQs0h5T5kcU0xjEXPI5K2gpdQz8YGblAbKZXcpJn7zJEwgtodmRnhZ
f7Gm45Jt45IA8QOpeq5H83ajFg0q8twMeVj9znA0ogle/g==
-----END CERTIFICATE REQUEST-----
```

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.

The screenshot shows the Oracle Enterprise Session Border Controller WebGUI interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'NN3950-101 10.138.194.101 SCZ9.0.0 Patch 3 (Build 290)', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the 'Certificate Record' page is displayed. The left sidebar shows a navigation tree with 'certificate-record' selected. The main content area shows a table of certificate records. A red arrow points to the 'Save' icon in the toolbar above the table.

Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
:	<input type="checkbox"/>	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberT
:	<input type="checkbox"/>	DigiCertGlobalRootG2	US	MA	Burlington	DigiCert	www.digicert.com	DigiCert Global R
:	<input type="checkbox"/>	GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 F
:	<input checked="" type="checkbox"/>	SBCCertificateforTea...	US	California	Redwood City	Oracle Corporation		telechat.o-test06



**Import Certificate**

Format: try-all

Import Method:  File  Paste

Paste:

```
-----BEGIN CERTIFICATE-----
MIIHMIJCChagAwIBAgIQC3C/hl8
HZQ8xkQTV4A0WwzANBgkqhkiG
9w0BAQsFAADBP
MQswCQYDVQQGEwJVUzEVMB
MGA1UEChMMRGlnaUNlcnQgSW
5jMSkwJwYDVQQDEyBE
aWdpQ2VyeiCBUTFMgUINBIFNIQ
TIIINAYMDIwEENBMTAeFw0yMTA
5MjAwMDAwMDBa
Fw0yMTA5MjgyMzU5NTIaMIGkM
OswCOYDVOOGEwJVUzETMBEG
-----
```

Import Cancel

- 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:

## 10.10.TLS Profile

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

GUI Path: security/tls-profile

ACL Path: config t→security→tls-profile

- Click Add, use the example below to configure

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes the Oracle logo, version information (NN3950-101, 10.138.194.101, SCZ9.0.0 Patch 3 (Build 290)), and menu items for Dashboard, Configuration, Monitor and Trace, Widgets, and System. The Configuration menu is active, and the 'Modify TLS Profile' dialog box is open. The dialog box contains the following fields:

- Name: TLSTeams
- End Entity Certificate: SBCCertificateforTeams
- Trusted Ca Certificates: BaltimoreRoot, DigiCertGlobalRootG2, GoDaddyRoot
- Cipher List: DEFAULT
- Verify Depth: 10 (Range: 0..10)
- Mutual Authenticate:  enable
- TLS Version: tlsv12
- Options: (empty)

At the bottom of the dialog box, there are 'OK' and 'Back' buttons.

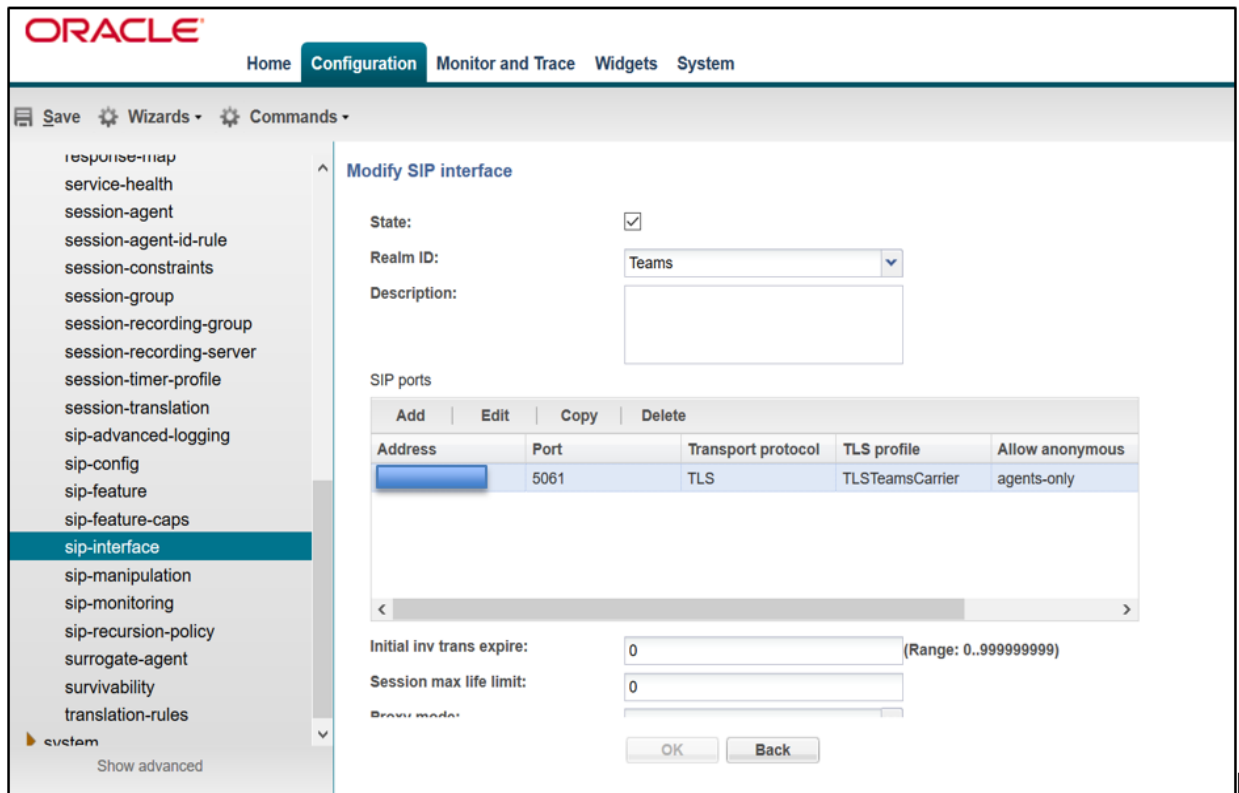
- Select OK at the bottom

## 10.11. Configure SIP Interfaces.

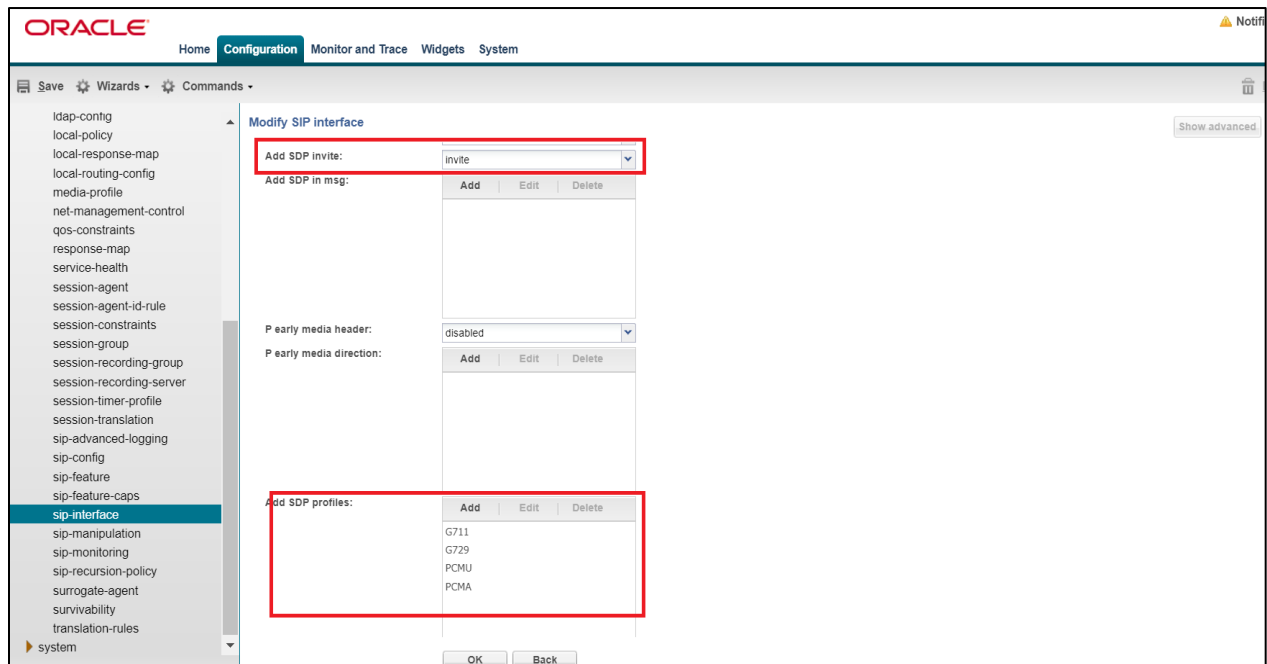
Navigate to sip-interface under session-router and configure the sip-interface as shown below. Please ensure that the IP address allocated to the SIP interface is the FQDN resolvable address. I.e. if you issue command nslookup from another computer, "oracleesbc2.woodgrovebank.us" – it should resolve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

ORACLE

Home Configuration Monitor and Trace Widgets System

Save Wizards Commands

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  
sip-feature-caps  
**sip-interface**  
sip-manipulation  
Show advanced

### Modify SIP interface

State:

Realm ID: CUCMRealm

Description:

SIP ports

Address	Port	Transport protocol	TLS profile	Allow anonymous
10.232.50.65	5060	TCP		all
10.232.50.65	5060	UDP		all

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

idap-confg  
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  
sip-feature-caps  
**sip-interface**  
sip-manipulation  
sip-monitoring  
sip-recursion-policy  
surrogate-agent  
survivability  
translation-rules  
system  
Show advanced

### Modify SIP interface

Add SDP invite: invite

Add SDP in msg:

P early media header: disabled

P early media direction:

Add SDP profiles:

Add	Edit	Delete
G711		
G729		
PCMU		
PCMA		

OK Back

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.

## 10.12. 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

The screenshot displays the Oracle SBC Configuration web interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a sidebar menu lists various configuration categories, with 'session-agent' highlighted. The main content area is titled 'Modify Session agent' and contains the following configuration fields:

- Hostname: sip.pstnhub.microsoft.com
- IP address: (empty)
- Port: 5061 (Range: 0, 1025..65535)
- State:
- App protocol: SIP
- App type: (empty)
- Transport method: StaticTLS
- Realm ID: access-teams
- Egress Realm ID: (empty)
- Description: (empty)

At the bottom of the configuration area, there is a 'Match identifier' section and a toolbar with 'Add', 'Edit', 'Copy', and 'Delete' buttons. On the right side of the configuration area, there are 'Show advanced' and 'Show configuration' buttons.

- 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

in service period:  (Range: 0..999999999)

Burst rate window:  (Range: 0..999999999)

Sustain rate window:  (Range: 0..999999999)

Proxy mode:

Redirect action:

Loose routing:

Response map:

Ping method:

Ping interval:  (Range: 0..4294967295)

Ping send mode:

Ping all addresses:

Ping in service response codes:

Options:

Add	Edit	Delete
-----	------	--------

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'ORACLE', 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The user is logged in as 'admin'. The left sidebar shows a tree view of configuration categories, with 'h323' selected. The main content area is titled 'Modify Session agent' and contains the following configuration items:

- Rfc2833 payload: 0 (Range: 0..127)
- Codec policy: [dropdown menu]
- Refer call transfer: enabled [dropdown menu]
- Refer notify provisional: none [dropdown menu]
- Reuse connections: NONE [dropdown menu]
- TCP keepalive: none [dropdown menu]
- TCP reconn interval: 0 (Range: 0..2..300)
- Max register burst rate: 0 (Range: 0..999999999)
- KpmI interworking: inherit [dropdown menu]
- Precedence: 0 (Range: 0..4294967295)
- Monitoring filters: [Add | Edit | Delete buttons]

Follow above steps to create 2 more sessions for:

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

Similarly, Configure the session-agent for CUCM which is Oracle ECB where SBC should route the calls. Go to session-router->Session-Agent.

- Host name and IP address to 10.232.50.70 which is the ECB IP.
- port 5060
- realm-id – needs to match the realm created for CUCM.
- transport set to “UDP+TCP

The screenshot shows the Oracle Configuration Assistant 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 icons for 'Save', 'Wizards', and 'Commands'. The left sidebar contains a tree view of configuration categories, with 'session-agent' selected. The main content area is titled 'Modify Session agent' and contains the following fields:

- Hostname: 10.232.50.70
- IP address: 10.232.50.70
- Port: 5060 (Range: 0, 1025..65535)
- State:
- App protocol: SIP
- App type: [Empty]
- Transport method: UDP+TCP
- Realm ID: CUCMRealm
- Egress Realm ID: [Empty]
- Description: [Empty text area]

Below the fields is a 'Match identifier' section with a table:

Identifier rule	Match value

Buttons for 'Add', 'Edit', 'Copy', and 'Delete' are located above the table. At the bottom of the page are 'OK' and 'Back' buttons.

### 10.13. Configure session-agent group

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

Go to Session-Router->Session-Group.



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

Save Wizards Commands

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**  
session-recording-group  
session-recording-server  
session-timer-profile  
session-translation  
sip-advanced-logging

Show advanced

### Modify Session group

Group name: TeamsGrp

Description:

State:

App protocol: SIP

Strategy: RoundRobin

Dest:

Add	Edit	Delete
sip.pstnhub.microsoft.com		
sip2.pstnhub.microsoft.com		
sip3.pstnhub.microsoft.com		

Trunk group:

Add	Edit	Delete
-----	------	--------

OK Back

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

Save Wizards Commands Discard Search

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**  
session-recording-group  
session-recording-server  
session-timer-profile  
session-translation  
sip-advanced-logging

Show advanced

### Modify Session group

Trunk group:

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

Add Edit Delete

Sag recursion:

Stop sag recurse: 401,407,480

SIP recursion policy:

## 10.14. 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:

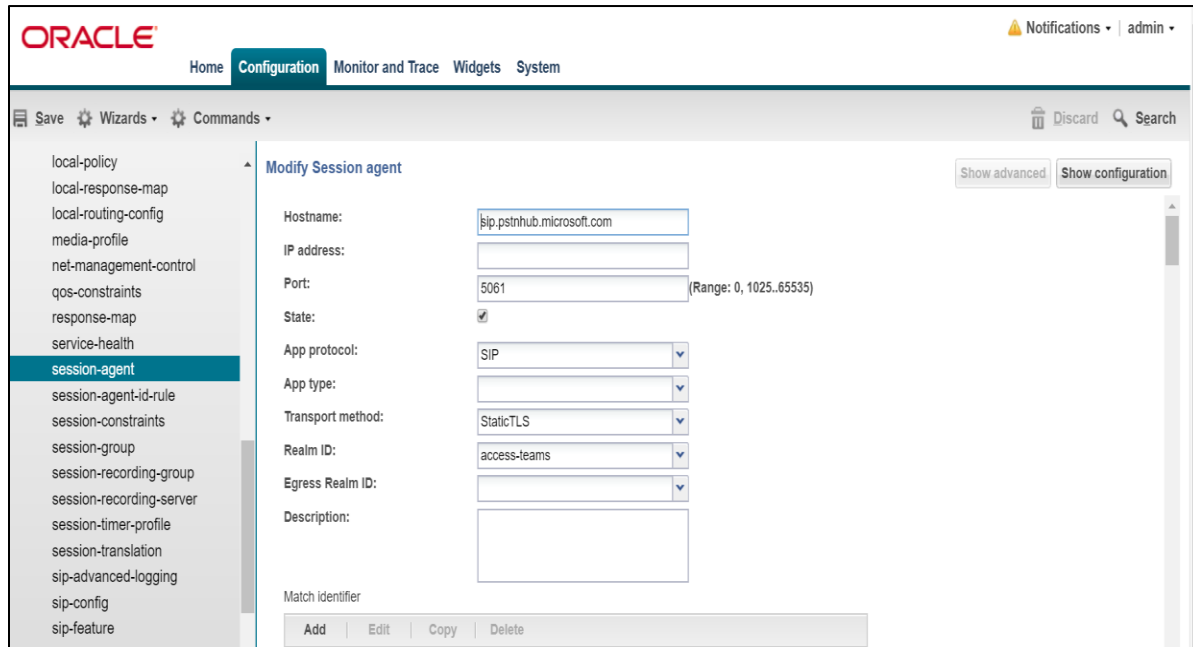
Out manipulationid:

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:

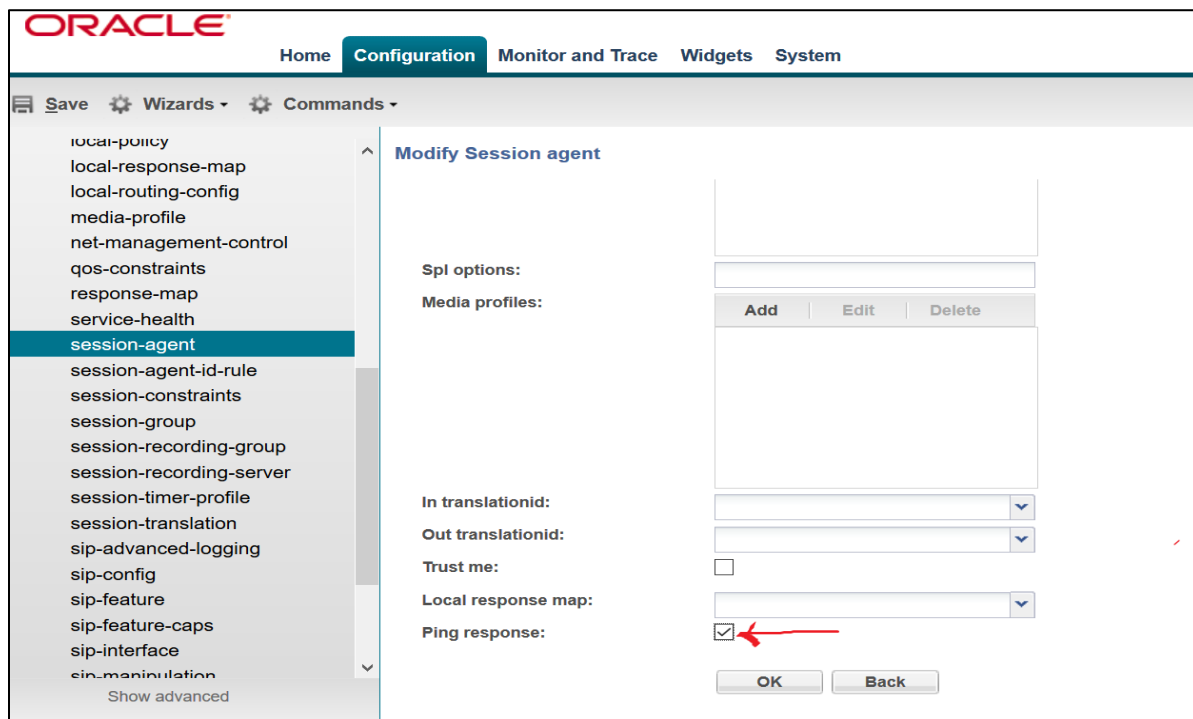
When enabled, the SBC responds with a 200 OK to all Sip Options Pings it receives from trusted agents. This takes the place of the current Sip Manipulation, RepondOptions.



The screenshot shows the Oracle SBC configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration categories, with 'session-agent' selected. The main content area is titled 'Modify Session agent' and contains the following fields:

- Hostname: sip.pstnhub.microsoft.com
- IP address: (empty)
- Port: 5061 (Range: 0, 1025..65535)
- State:
- App protocol: SIP
- App type: (empty)
- Transport method: Static-TLS
- Realm ID: access-teams
- Egress Realm ID: (empty)
- Description: (empty)

At the bottom, there is a 'Match Identifier' section with 'Add', 'Edit', 'Copy', and 'Delete' buttons.



The screenshot shows the Oracle SBC configuration interface, specifically the 'Modify Session agent' form. The left sidebar lists various configuration categories, with 'session-agent' selected. The main content area is titled 'Modify Session agent' and contains the following fields:

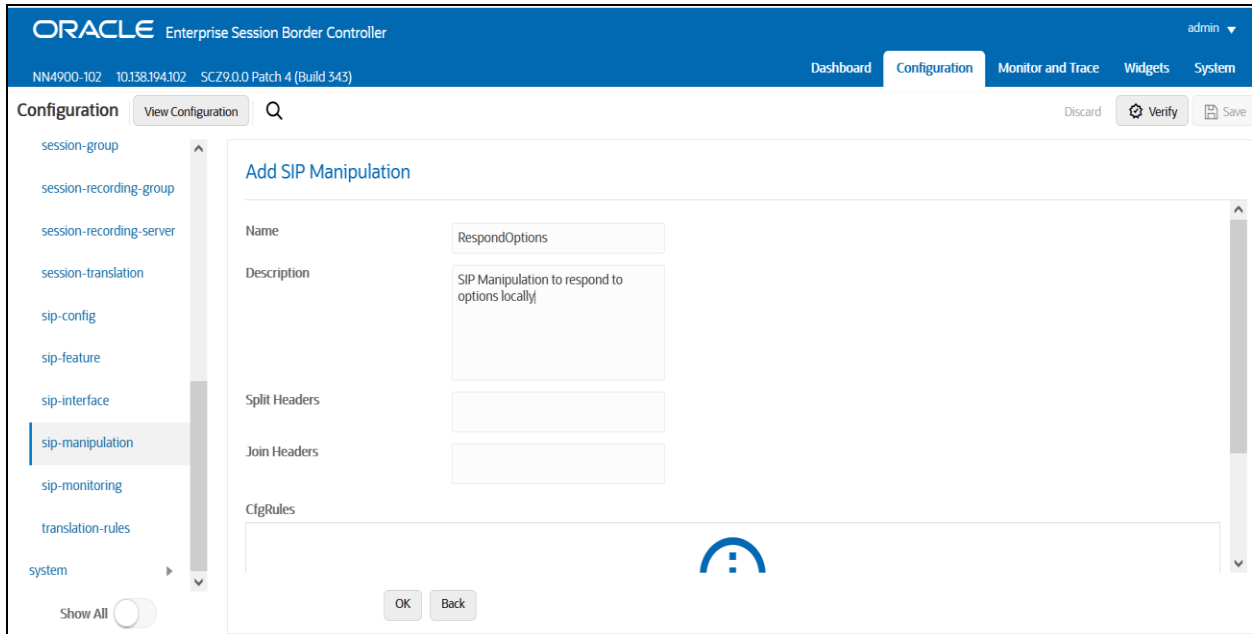
- Spl options: (empty)
- Media profiles: (empty)
- In translationid: (empty)
- Out translationid: (empty)
- Trust me:
- Local response map: (empty)
- Ping response:  (indicated by a red arrow)

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

## 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:

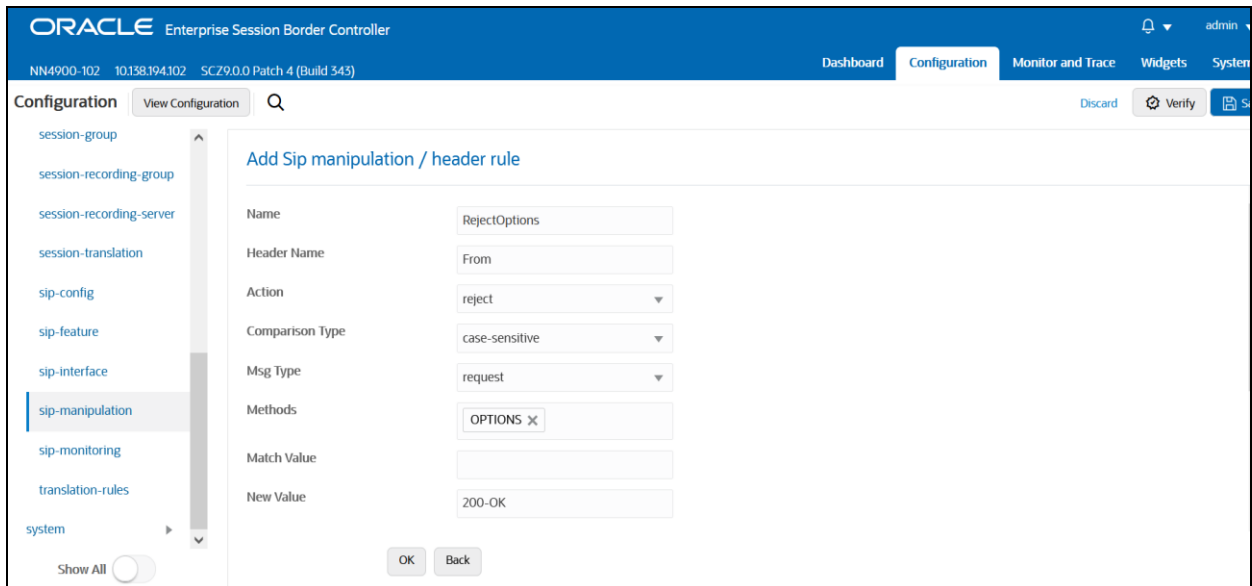


The screenshot shows the Oracle Enterprise Session Border Controller GUI. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a sidebar lists various configuration categories, with 'sip-manipulation' selected. The main content area is titled 'Add SIP Manipulation' and contains the following fields:

- Name: RespondOptions
- Description: SIP Manipulation to respond to options locally
- Split Headers: (empty)
- Join Headers: (empty)
- CfgRules: (empty)

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

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



The screenshot shows the Oracle Enterprise Session Border Controller GUI. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a sidebar lists various configuration categories, with 'sip-manipulation' selected. The main content area is titled 'Add Sip manipulation / header rule' and contains the following fields:

- Name: RejectOptions
- Header Name: From
- Action: reject
- Comparison Type: case-sensitive
- Msg Type: request
- Methods: OPTIONS
- Match Value: (empty)
- New Value: 200-OK

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

Click OK at the bottom when finished.

## 10.15. 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 via ECB, the following config is required:  
The next hop here should be the ECB IP which is 10.232.50.70

The screenshot shows the Oracle Session Manager configuration interface. The 'Configuration' tab is active. The left sidebar shows a tree view of objects, with 'local-policy' selected under 'session-router'. The main area displays the 'Add Local policy' form. The form has three sections: 'From address:', 'To address:', and 'Source realm:'. Each section has an 'Add', 'Edit', and 'Delete' button above a text input field. The 'From address' and 'To address' fields contain an asterisk (\*). The 'Source realm' field contains 'Teams'. At the bottom of the form are 'OK' and 'Back' buttons.

The screenshot shows the Oracle Session Manager configuration interface. The 'Configuration' tab is active. The left sidebar shows a tree view of objects, with 'local-policy' selected under 'session-router'. The main area displays the 'Modify Local policy' form. The form has several fields: 'Source realm:' with a dropdown menu showing 'Teams'; 'Description:' with a text input field; 'State:' with a checked checkbox; 'Policy priority:' with a dropdown menu showing 'none'; and 'Policy attributes' with a table. The table has columns for 'Next hop', 'Realm', 'Action', 'Terminate recursion', and 'Cost'. Below the table are 'OK' and 'Back' buttons.

Next hop	Realm	Action	Terminate recursion	Cost
10.232.50.70	CUCMRealm	replace-uri	enabled	0

To make calls from CUCM to Teams, 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

### Modify Local policy

Description:

State:

Policy priority:

Policy attributes

Next hop	Realm	Action	Terminate recursion	Cost
Irt:TeamsLRT	SIPTrunk	none	disabled	0

OK Back

## 10.16. 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

The screenshot displays the Oracle SBC Configuration web 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 icons for 'Save', 'Wizards', and 'Commands'. A left-hand sidebar lists various configuration categories, with 'media-profile' selected and highlighted in blue. The main content area is titled 'Modify Media profile' and contains the following fields:

- Name: CN
- Subname: wideband
- Media type: audio
- Payload type: 118
- Transport: RTP/AVP
- Clock rate: 16000 (Range: 0..4294967295)
- Req bandwidth: 0 (Range: 0..999999999)
- Frames per packet: 0 (Range: 0..256)
- Parameters: A table with 'Add', 'Edit', and 'Delete' buttons.

At the bottom of the form are 'OK' and 'Back' buttons. The sidebar also includes a 'Show advanced' link at the bottom.



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.

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this is a toolbar with 'Save', 'Wizards', and 'Commands'. The left sidebar shows a tree view of objects, with 'media-manager' expanded and 'codec-policy' selected. The main area is titled 'Modify Codec policy' and contains the following configuration fields:

- Name:** addCN
- Allow codecs:** A list containing '\*' and 'SILK:no'. Below the list are 'Add', 'Edit', and 'Delete' buttons.
- Add codecs on egress:** A list containing 'CN'. Below the list are 'Add', 'Edit', and 'Delete' buttons.
- Order codecs:** A section with 'Add', 'Edit', and 'Delete' buttons.

At the bottom of the main area are 'OK' and 'Back' buttons. The bottom left of the sidebar has a 'Show advanced' link.

Go to media manager ---- realm config and assign the codec policy to the Teams 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 are 'Save', 'Wizards', and 'Commands' options. The left sidebar shows a tree view of objects, with 'realm-config' selected under the 'media-manager' category. The main area is titled 'Modify Realm config' and contains the following fields:

- Identifier: Teams
- Description: (empty text box)
- Addr prefix: 0.0.0.0
- Network interfaces: A table with columns 'Add', 'Edit', and 'Delete'. It contains one entry: M00:0.4.
- Mm in realm:
- Mm in network:
- Mm same ip:
- QoS enable:

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

This screenshot shows the same 'Modify Realm config' page but with advanced options expanded. The left sidebar now shows 'realm-group' selected under the 'realm-config' category. The main area includes the following additional fields:

- Restricted latching: none (dropdown menu)
- Options: (empty text box)
- Spl options: (empty text box)
- Delay media update:
- Refer call transfer: disabled (dropdown menu)
- Hold refer reinvoke:
- Refer notify provisional: none (dropdown menu)
- Dyn refer term:
- Codec policy: addCN (dropdown menu)
- Codec manIP in realm:
- Codec manIP in network:
- RTCP policy: rtcpGen (dropdown menu)

'OK' and 'Back' buttons are at the bottom right. The 'Show advanced' link is at the bottom left of the sidebar.

## 10.17. Configure ice-profile

SBC supports ICE-Lite. This configuration is only required to support Teams media-bypass. Configure the following ice profile and apply it on the realm towards Teams. Go to media-manager->ice-profile

The screenshot shows the Oracle SBC Configuration interface. The 'Configuration' tab is active. The left sidebar shows a tree view of objects, with 'ice-profile' selected under 'media-manager'. The main area is titled 'Add Ice profile' and contains the following configuration fields:

Name:	ice	
Stun conn timeout:	0	(Range: 0..9999)
Stun keep alive interval:	0	(Range: 0..300)
Stun rate limit:	100	(Range: 0..99999)

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

The screenshot shows the Oracle SBC Configuration interface. The 'Configuration' tab is active. The left sidebar shows a tree view of objects, with 'realm-config' selected under 'media-manager'. The main area is titled 'Modify Realm config' and contains the following configuration fields:

Max bandwidth:	0	(Range: 0..999999999)
Max priority bandwidth:	0	(Range: 0..999999999)
Parent realm:		
DNS realm:		
Media policy:		
Media sec policy:	sdesPolicy	
RTCP mux:	<input checked="" type="checkbox"/>	
Ice profile:	ice	←
Teams fqdn in uri:	<input type="checkbox"/>	
SDP inactive only:	<input type="checkbox"/>	
DTLS srtp profile:		
Srtp msm passthrough:	<input type="checkbox"/>	
Class profile:		
In translationid:		
Out translationid:		

Buttons for 'OK' and 'Back' are located at the bottom right of the configuration area. A red arrow points to the 'ice profile' dropdown menu.

In addition to applying the ice-profile on the Teams realm, we need to enable nat-traversal on the sip-interface for this realm

The screenshot shows the Oracle Configuration Assistant interface. At the top, the Oracle logo is on the left, and navigation tabs for 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System' are on the right. Below the navigation is a toolbar with 'Save', 'Wizards', and 'Commands' options. A left-hand sidebar lists various configuration categories, with 'sip-interface' highlighted in blue. The main area is titled 'Modify SIP interface' and contains several configuration fields:

- Initial inv trans expire: 0 (Range: 0..999999999)
- Session max life limit: 0
- Proxy mode: [dropdown]
- Redirect action: [dropdown]
- Nat traversal: always (indicated by a red arrow)
- Nat interval: 30 (Range: 0..4294967295)
- TCP nat interval: 90 (Range: 0..4294967295)
- Registration caching: [checkbox]
- Min reg expire: 300 (Range: 0..999999999)
- Registration interval: 3600 (Range: 0..4294967295)
- Route to registrar: [checkbox]
- Secured network: [checkbox]
- Uri fqdn domain: [text field]
- Options: [Add | Edit | Delete buttons]

At the bottom of the configuration area are 'OK' and 'Back' buttons.

## 10.18. 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 this is a toolbar with 'Save', 'Wizards', and 'Commands'. A left-hand 'Objects' tree lists various configuration categories, with 'steering-pool' selected. The main area is titled 'Add Steering pool' and contains the following fields:

- IP address:
- Start port:  (Range: 1..65535)
- End port:  (Range: 1..65535)
- Realm ID:
- Network interface:

At the bottom right of the dialog are 'OK' and 'Back' buttons. A 'Show advanced' link is located at the bottom left of the objects list.

This screenshot shows the same 'Add Steering pool' dialog, but with the following values entered:

- IP address:
- Start port:  (Range: 1..65535)
- End port:  (Range: 1..65535)
- Realm ID:
- Network interface:

The 'OK' and 'Back' buttons are visible at the bottom right, and the 'Show advanced' link is at the bottom left of the objects list.

## 10.19. 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.

The screenshot shows the Oracle Configuration Assistant 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. On the left, a tree view shows the 'Objects' hierarchy: 'media-manager', 'security', 'admin-security', 'auth-params', 'authentication', 'authentication-profile', 'cert-status-profile', 'certificate-record', 'ike', 'ipsec', 'media-security', 'dtls-srtp-profile', 'media-sec-policy', 'sdes-profile' (highlighted), 'sipura-profile', 'password-policy', 'public-key', 'security-config', 'ssh-config', and 'tls-global'. The main area is titled 'Add Sdes profile' and contains the following configuration fields:

- Name:** SDES
- Crypto list:** A list containing 'AES\_CM\_128\_HMAC\_SHA1\_80' with 'Add', 'Edit', and 'Delete' buttons above it.
- Srtp auth:**
- Srtp encrypt:**
- SrTCP encrypt:**
- Mki:**
- Egress offer format:** same-as-ingress (dropdown menu)
- Use ingress session params:** A list with 'Add', 'Edit', and 'Delete' buttons above it.

At the bottom of the configuration area are 'OK' and 'Back' buttons.

## 10.20. 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.

The screenshot shows the Oracle Configuration interface. The left sidebar contains a tree view of objects, with 'media-sec-policy' selected. The main area is titled 'Add Media sec policy' and contains the following fields:

- Name: SDES
- Pass through:
- Options: A table with columns 'Add', 'Edit', and 'Delete'.
- Inbound section:
  - Profile: SDES
  - Mode: srtp
  - Protocol: sdes
  - Hide egress media update:
- Outbound section: (empty)

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

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

The screenshot shows the Oracle Configuration interface. The left sidebar contains a tree view of objects, with 'media-sec-policy' selected. The main area is titled 'Modify Media sec policy' and contains the following fields:

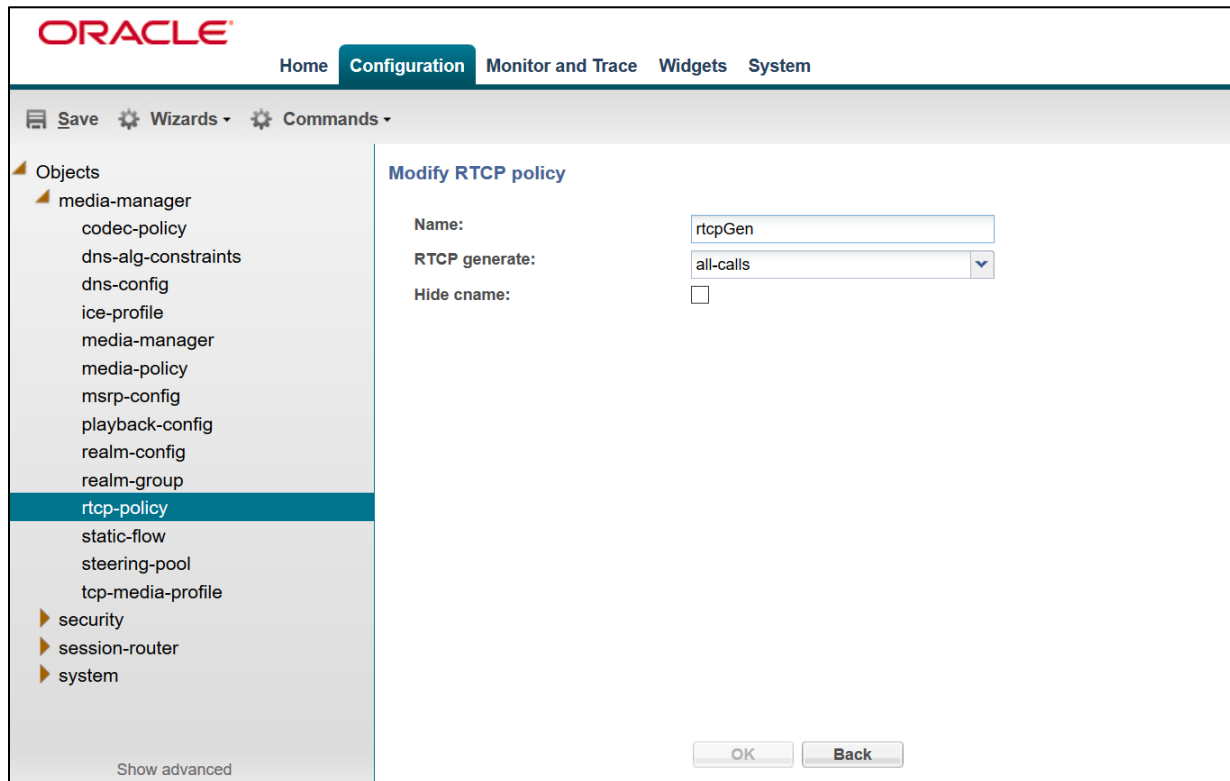
- Name: RTP
- Pass through:
- Options: A table with columns 'Add', 'Edit', and 'Delete'.
- Inbound section:
  - Profile: (empty)
  - Mode: rtp
  - Protocol: none
  - Hide egress media update:
- Outbound section: (empty)

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

## 10.21. 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.



The screenshot shows the Oracle Configuration interface. At the top, there is a navigation bar with the Oracle logo and tabs for Home, Configuration, Monitor and Trace, Widgets, and System. Below the navigation bar, there is a toolbar with icons for Save, Wizards, and Commands. On the left side, there is a tree view of objects under 'media-manager', with 'rtcp-policy' selected. The main content area is titled 'Modify RTCP policy' and contains the following fields:

- Name: rtcpGen
- RTCP generate: all-calls
- Hide cname:

At the bottom right of the form, there are 'OK' and 'Back' buttons. At the bottom left, there is a 'Show advanced' link.



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

**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

**Modify Realm config**

RTCP policy: rtcpGen

Constraint name: Teams911Restraint

Session recording server:

Session recording required:

Flow time limit: -1 (Range: -1..2147483647)

Initial guard timer: -1 (Range: -1..2147483647)

Subsq guard timer: -1 (Range: -1..2147483647)

TCP flow time limit: -1 (Range: -1..2147483647)

TCP initial guard timer: -1 (Range: -1..2147483647)

TCP subsq guard timer: -1 (Range: -1..2147483647)

QoS constraint:

TCP media profile:

Monitoring filters:

Add Edit Delete

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
  - admin-security
    - audit-logging
  - auth-params
  - authentication

**Modify Realm config**

Parent realm:

DNS realm:

Media policy:

Media sec policy:

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

Show advanced

## 11. 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](#)
- [Sip Manipulation](#)
- [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.

## 12 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

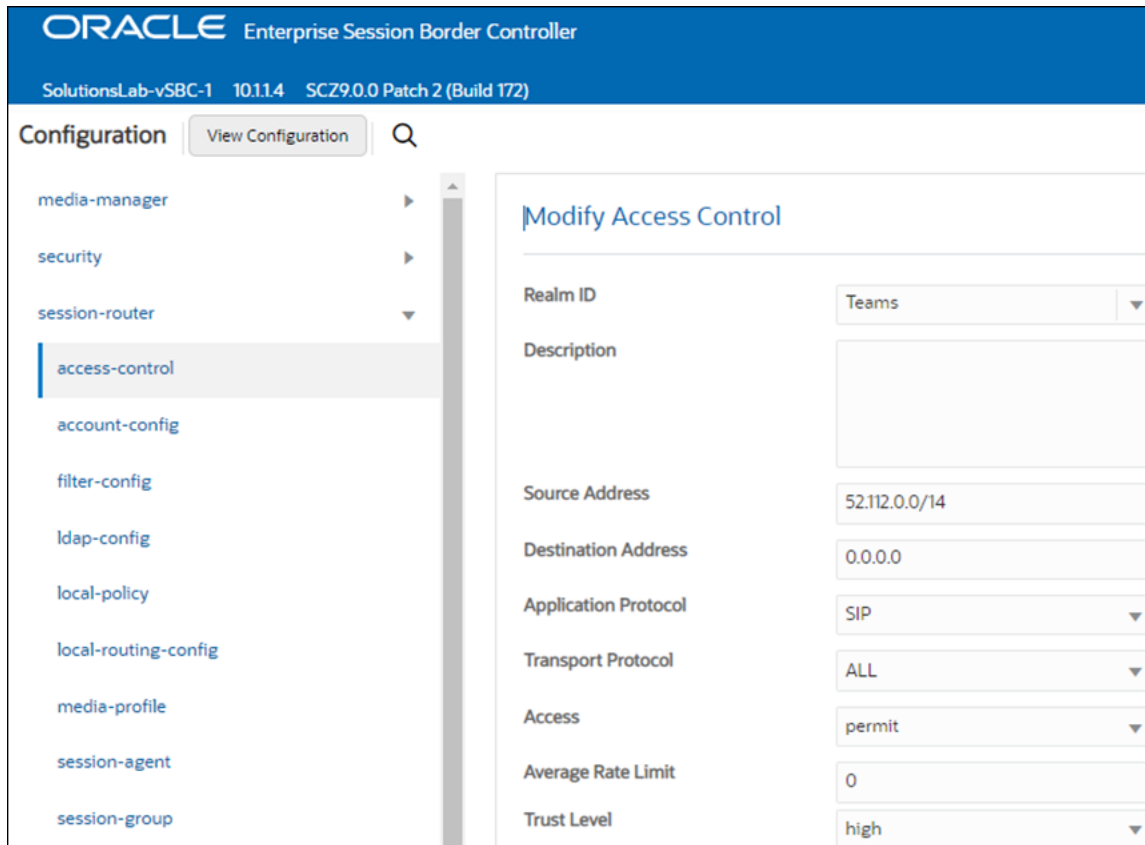
Microsoft Teams has two subnets, 52.112.0.0/14 and 52.120.0.0/14 that must be allowed to send traffic to the SBC. Both must be configured as an access control on the Oracle SBC and associated with the realm facing Teams.

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

ACL Path: config t session-router access-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.

## 13. Caveat

In some environments, the methods in which Cisco CUCM uses to place a call on hold is not supported 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
mime-sdp-rule
  name          FixSDP
  msg-type      ModifySDP
  methods       request
               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          DeleteInactive
  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**

CONNECT WITH US

-  [blogs.oracle.com/oracle](https://blogs.oracle.com/oracle)
-  [facebook.com/Oracle/](https://facebook.com/Oracle/)
-  [twitter.com/Oracle](https://twitter.com/Oracle)
-  [oracle.com](https://oracle.com)

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

**Worldwide Inquiries**  
 Phone: +1.650.506.7000  
 Fax: +1.650.506.7200

**Integrated Cloud Applications & Platform Services**

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

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

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