



# ORACLE

Oracle SBC and ECB integration with Avaya, Teams Direct  
Routing and Verizon Trunk

**Technical Application Note**

**ORACLE**  

---


**COMMUNICATIONS**

## Disclaimer

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

## Revision History

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with Avaya and Teams DR and Verizon Trunk	15 <sup>th</sup> February 2021
1.1	Oracle SBC integration with Avaya and Teams DR and Verizon Trunk – Added Screenshots for Sip-manipulation "RemoveAttribute" Header Rule and Element Rule	15 <sup>th</sup> September 2021
1.2	Minor Formatting changes	12 <sup>th</sup> November 2021
1.3	Removed reference to sip-all FQDN from the app note document	12 <sup>th</sup> January 2022
1.4	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



1.5	Added DigiCert Global G2 Cert as root CA Changed certificate-record screenshots	5 <sup>th</sup> Sep 2022
1.6	Added SIP success Controls	13 <sup>th</sup> Sep 2022

## Table of Contents

<b>1. INTENDED AUDIENCE</b> .....	<b>6</b>
<b>2. DOCUMENT OVERVIEW</b> .....	<b>6</b>
2.1. VERIZON BUSINESS .....	6
2.2. MICROSOFT TEAMS.....	6
<b>3. INTRODUCTION</b> .....	<b>7</b>
3.1. AUDIENCE .....	7
3.2. REQUIREMENTS.....	7
3.3. ARCHITECTURE .....	8
<b>4. CONFIGURING THE AVAYA AURA SESSION MANAGER 8.1</b> .....	<b>9</b>
4.1. ADDING SIP DOMAIN .....	9
4.2. ADDING LOCATION .....	10
4.3. ADDING THE ORACLE ECB AS A SIP ENTITY AND CONFIGURING AN ENTITY LINK.....	10
4.4. ALLOWING UNSECURED PPM TRAFFIC (ONLY IF TLS IS NOT USED) AND PPM RATE LIMITING .....	13
4.5. ADDING ROUTING POLICIES.....	15
4.6. ADDING DIAL PATTERNS:.....	15
4.7. ADDING USERS TO AVAYA SESSION MANAGER. ....	17
<b>5. CONFIGURE MICROSOFT TEAMS DIRECT ROUTING</b> .....	<b>20</b>
5.1. ACCESS TEAM ADMIN CENTER.....	20
5.2. CONFIGURE ONLINE PSTN GATEWAY.....	21
5.3. CONFIGURE ONLINE PSTN USAGE .....	21
5.4. CONFIGURE ONLINE VOICE ROUTES.....	22
5.5. CONFIGURE ONLINE VOICE ROUTING POLICY.....	23
5.6. ASSIGN VOICE ROUTING POLICY TO USERS .....	24
<b>6. NEW ECB CONFIGURATION</b> .....	<b>24</b>
6.1. ECB CLI INITIAL CONFIG.....	25
6.2. LOGGING INTO THE ECB .....	27
6.3. ADD NETWORK SETTINGS.....	28
6.4. CONFIGURE SIP INTERFACE .....	29
6.5. CONFIGURING THE AGENTS .....	29
6.6. CONFIGURING THE ROUTING.....	31
<b>7. CONFIGURING THE SBC</b> .....	<b>33</b>
7.1. VALIDATED ORACLE SBC VERSION.....	33
<b>8. NEW SBC CONFIGURATION</b> .....	<b>33</b>
8.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC.....	33
8.2. CONFIGURE SBC USING WEB GUI .....	37
8.3. CONFIGURE SYSTEM-CONFIG .....	39
8.4. CONFIGURE PHYSICAL INTERFACE VALUES .....	40
8.5. CONFIGURE NETWORK INTERFACE VALUES.....	41
8.6. ENABLE MEDIA MANAGER .....	43
8.7. CONFIGURE REALMS.....	44
8.8. ENABLE SIP-CONFIG.....	47
8.9. CONFIGURING A CERTIFICATE FOR SBC.....	48
8.10. TLS PROFILE.....	53
8.11. IKE/IPSEC CONFIG.....	54

8.12. CONFIGURE SIP INTERFACES .....	56
8.13. CONFIGURE SESSION-AGENT .....	58
8.14. CONFIGURE SESSION-AGENT GROUP .....	61
8.15. CONFIGURE LOCAL-POLICY .....	62
8.16. CONFIGURE STEERING-POOL.....	66
8.17. CONFIGURE SIP-MANIPULATION .....	67
8.18. CONFIGURE MEDIA PROFILE AND CODEC POLICY.....	79
8.19. CONFIGURE ICE PROFILE .....	80
8.20. CONFIGURE SDES PROFILE.....	81
8.21. CONFIGURE MEDIA SECURITY PROFILE.....	81
8.22. CONFIGURE RTCP POLICY AND RTCP MUX .....	82
8.23. QOS MARKING .....	83
8.24. CONFIGURE TRANSLATION RULES .....	83
8.25. CONFIGURE SESSION TRANSLATION RULES .....	84
<b>9.SIP ACCESS CONTROLS.....</b>	<b>87</b>
<b>10. VERIFICATION OF SAMPLE CALL FLOWS.....</b>	<b>89</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 Avaya Aura System Manager GUI and Avaya Aura Session Manager and Microsoft Teams Direct Routing Enterprise Model.

## 2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Verizon Business Sip Trunk with Avaya Session Manager and Microsoft Teams Direct Routing. The solution contained within this document has been tested using Oracle Communication SBC with OS 840p2 version and Oracle Communication ECB with OS 320p5. **Please note that all voice traffic from both Verizon and Teams is routed through the Avaya Aura platform, and there is no direct connection between Teams and Verizon.**

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

Please find the related documentation links below:

### 2.1. Verizon Business

<https://www.verizon.com/business/products/voice-collaboration/voip/ip-trunking/>

### 2.2. Microsoft Teams

<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure>

<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants#create-a-trunk-and-provision-users>

<https://www.oracle.com/a/otn/docs/vzbwithsbcsfteams-mb.pdf>

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

**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.**

### 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 Avaya Session Manager using Oracle Enterprise SBC and Oracle ECB. There will be steps that require navigating the Teams configuration, Avaya server configuration, Oracle SBC GUI interface and 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.

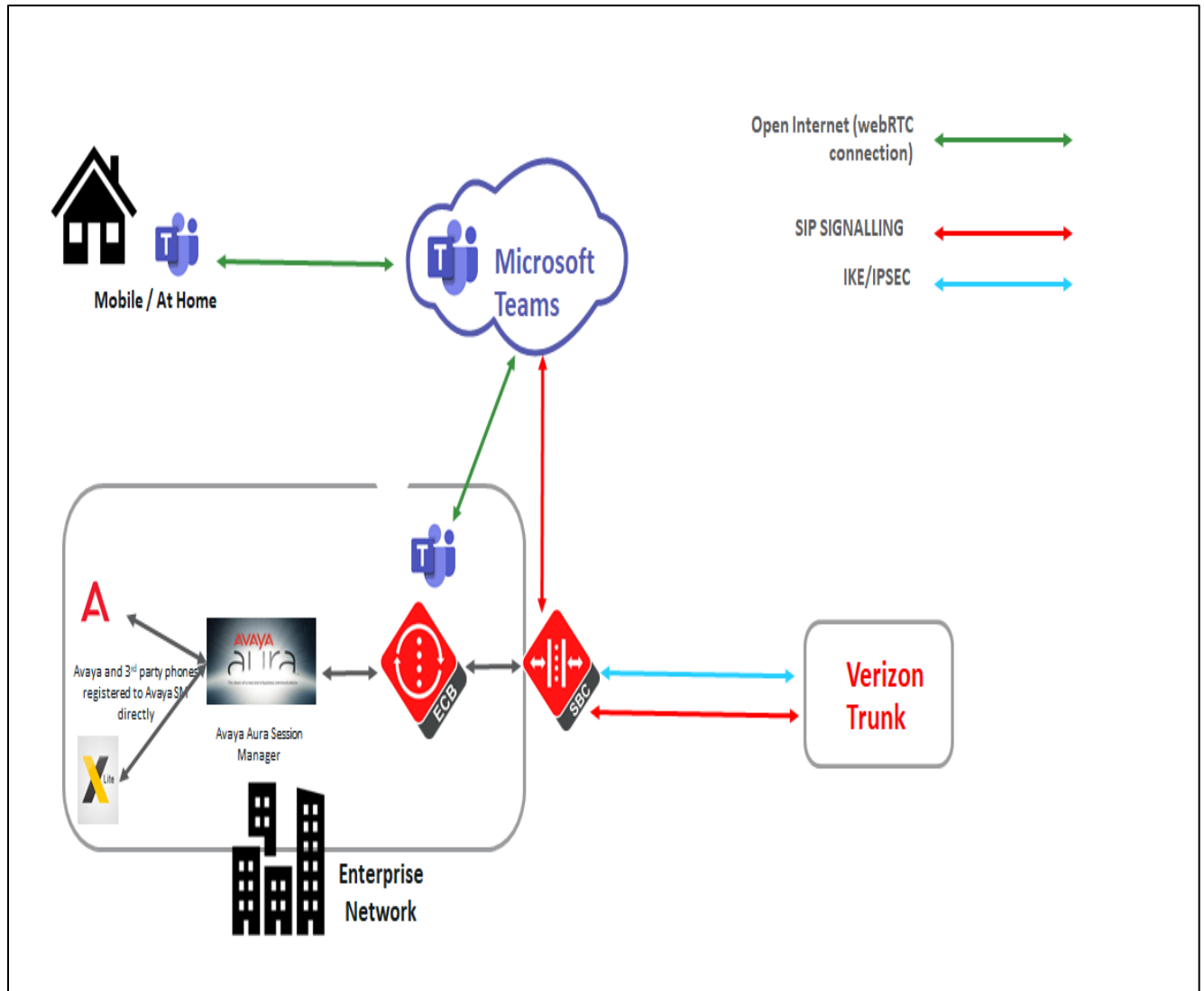
#### 3.2. Requirements

- Fully functioning Avaya Aura Session Manager 8.1 version.
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version
- Oracle Enterprise Communication Broker (hereafter Oracle ECB) running 3.2.0 version
- Teams Direct Routing Enterprise Model running Teams Client.

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

Software Used	Avaya Aura Session Manager using Avaya Aura System Manager GUI	SBC Version	ECB Version	Teams Client version
Revision 1	8.1	8.4.0	3.2.0	1.3.00.28779 (64-bit) (Windows) v.1416/1.0.0.2021010802 (Mobile)

### 3.3. Architecture



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

- Phase 1 – Configuring the Avaya Aura Session Manager.
- Phase 2 – Configuring the Teams Direct Routing Enterprise Model.
- Phase 3 – Configuring the Oracle ECB.
- Phase 4 – Configuring the Oracle SBC.



## 4. Configuring the Avaya Aura Session Manager 8.1

Please login to Avaya Aura System Manager web GUI with proper login credentials (Username and password). After that, perform the steps below in the given order.

Recommended access to System Manager is via FQDN.  
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic

User ID:

Password:

[Change Password](#)

**Supported Browsers:** Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

### 4.1. Adding SIP Domain

Click on Routing under the Elements section  
On the Routing tab, select Domains and Click New

- Set domain name as aura.com (Example in this config)
- Set Type as SIP
- click "Commit" to save the configuration

AVAYA Aura System Manager 8.1

Users Elements Services Widgets Shortcuts Search adm

Home Session Manager Routing

Routing Domains Locations Conditions Adaptations SIP Entities Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions

**Domain Management**

1 Item Filter: Enable

Name	Type	Notes
* aura.com	sip	

## 4.2. Adding Location

Click on Routing under the Elements section  
On the Routing tab, select Locations and Click New

- Set Name as Phonerlite
- Leave all other fields as default values and click “Commit” to save the configuration.

The screenshot shows the AVAYA Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The 'Routing' tab is active, and the 'Locations' menu item is selected in the left sidebar. The main content area is titled 'Location Details' and contains the following sections:

- General:** Name: Phonerlite, Notes: (empty field).
- Dial Plan Transparency in Survivable Mode:** Enabled: . Listed Directory Number: (empty field). Associated CM SIP Entity: (empty field).
- Overall Managed Bandwidth:** Managed Bandwidth Units: Kbit/sec. Total Bandwidth: (empty field). Multimedia Bandwidth: (empty field). Audio Calls Can Take Multimedia Bandwidth: .

Buttons for 'Commit' and 'Cancel' are visible at the top right of the configuration area.

## 4.3. Adding the Oracle ECB as a SIP Entity and Configuring an Entity Link

Click on Routing under the Elements section  
On the Routing tab, select SIP Entities from the menu on the left side of the screen.  
Click New to add the ECB as a SIP entity as shown below.

- Set Name: ECB-SM (example in this configuration)
- Set FQDN or IP Address: This is the “inside” IP address of Oracle ECB, 10.50.232.70 in this example.
- Set Type: Other
- Set Location: Select Phonerlite from drop down (example in this configuration)
- Set Time Zone: America/New\_York (example in this configuration)
- Under Entity Links, Click Add
- Set SIP Entity 1: Select acme-sm which was previously configured
- Set SIP Entity 2: leave the default value ECB-SM
- Set Protocol: UDP/TCP based on our testing
- Set Ports: Set both Ports to 5060 for testing
- Set Connection Policy: trusted

Leave all other fields as default values and click “Commit” to save the configuration.

**AVAYA** Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts | Search | admin

Home | Routing

### SIP Entity Details

Commit Cancel

**General**

\* Name: ECB-SM

\* FQDN or IP Address: 10.232.50.70

Type: Other

Notes:

Adaptation:

Location: Phonerlite

Time Zone: America/New\_York

\* SIP Timer B/F (in seconds): 4

Minimum TLS Version: Use Global Setting

Credential name:

Home | Routing

Routing

Domains

Locations

Conditions

Adaptations

**SIP Entities**

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Override Port & Transport with DNS SRV:

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* acme-sm_ECB-SM_5	acme-sm	TCP	* 5060	ECB-SM	* 5060	trusted
<input type="checkbox"/>	* acme-sm_ECB-SM_5	acme-sm	UDP	* 5060	ECB-SM	* 5060	trusted

Select : All, None

**SIP Responses to an OPTIONS Request**

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

Commit Cancel

Please configure Avaya Session Manager as another SIP entity in the same way as we added SBC:

- Set Name: acme-sm (example in this configuration)
- Set FQDN or IP Address: This is the SIP IP address of Avaya SM, 10.50.232.127 in this example.
- Set Type: Session Manager
- Leave all other fields as default values and click “Commit” to save the configuration.

**AVAYA** Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search | adm

Home User Management Routing

**SIP Entity Details** Commit Cancel

**General**

\* Name:

\* IP Address:

SIP FQDN:

Type:

Notes:

Location:

Outbound Proxy:

Time Zone:

Minimum TLS Version:

Credential name:

**Monitoring**

SIP Link Monitoring:

CRLF Keep Alive Monitoring:

**Entity Links**

#### 4.4. Allowing Unsecured PPM Traffic (only if TLS is not used) and PPM Rate Limiting

Navigate to: Elements->Session Manager->Global Settings

**Set Allow Unsecured PPM Traffic: checked.**

Note that this is only required if you're using HTTP for the PPM downloads.

If you're using HTTPS as shown in the E-SBC configuration, leave this unchecked.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The main content area is titled 'Global Settings' and contains various configuration options. The 'Allow Unsecured PPM Traffic' checkbox is checked, while 'Enable IPv6' is unchecked. Other settings include 'Failback Policy' (Auto), 'ELIN SIP Entity' (None), 'Minimum SIP Entity TLS Version' (1.2), and 'Minimum Endpoint TLS Version' (1.2). The 'Loop Detection Alarms Threshold (hours)' is set to 24. The 'Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location' checkbox is checked. The 'Enable Load Balancer' checkbox is unchecked.

Navigate to: Elements->Session Manager->Global Settings Session Manager Administration.

Select the proper Session Manager instance and click Edit

- Scroll down to PPM – Connection Settings
- Set Limited PPM Client Connection: unchecked
- Set PPM Packet Rate Limiting: unchecked
- Leave all other fields as default and Click Commit to save Session Manager Administration page.

AVAYA Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts | Search | adm

Home | Routing | Session Manager

Session Manager Administration

This page allows you to administer Session Manager instances and configure their global settings.

Session Manager Instances | Branch Session Manager Instances

Session Manager Instances

New | View | Edit | Delete

1 Item Filter: Enable

Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
acme-sm	Normal	4	0	4	

Select : None

AVAYA Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts | Search | adm

Home | Routing | Session Manager

Data File Format: Standard Flat File

Include User to User Calls

Include Incomplete Calls

**Personal Profile Manager (PPM) - Connection Settings**

Limited PPM Client Connection

\*Maximum Connection per PPM Client: 0

PPM Packet Rate Limiting

\*PPM Packet Rate Limiting Threshold: 200

**Event Server**

Clear Subscription on Notification Failure: No

**Syslog Servers**

Enable Syslog Server 1

Enable Syslog Server 2

\*Required

Commit Cancel

## 4.5. Adding Routing Policies

Navigate to: Routing tab, select Routing Policies and Click New

- Set Name: SMECBroute (example in this configuration)
- Set Retries : Default value is 0, can be used as same value
- Select SIP Entity as Destination: Select ECB-SM which was previously configured.
- Click Commit to save the configuration

**AVAYA** Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔔 admin

Home Routing

Routing Policy Details Commit Cancel

**General**

\* Name: SMECBroute

Disabled:

\* Retries: 0

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
ECB-SM	10.232.50.70	Other	

**Time of Day**

Add Remove View Gaps/Overlaps

## 4.6. Adding Dial Patterns:

Navigate to: Routing tab, select Dial Patterns, again Dial Patterns and Click New

- Set Pattern: 1xxxxxxxxx (example in this configuration)
- Set Min : 11 (example in this configuration)
- Set Max: 11 (example in this configuration)
- Select SIP Domain: aura.com which was previously configured.
- Click Commit to save the configuration.

AVAYA Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts | Search | adm

Home | Routing

### Dial Pattern Details

Commit Cancel

#### General

\* Pattern: 1xxxxxxxxx

\* Min: 11

\* Max: 11

Emergency Call:

SIP Domain: aura.com

Notes:

#### Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Phonerlite		SMECBroute	0	<input type="checkbox"/>	ECB-SM	

After configuring the dial patterns, Please add the dial patterns to the routing policies created above.

AVAYA Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts | Search | adm

Home | Session Manager | Routing

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

#### Dial Patterns

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	1xxxxxxxxx	11	11	<input type="checkbox"/>	aura.com	Phonerlite	

Select : All, None

#### Regular Expressions

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

Commit Cancel



## 4.7. Adding Users to Avaya Session Manager.

Navigate to: Users tab, select User Management, select Manage Users and Click New

Under **Identity Tab**, please enter the following

- Set Last Name: User1(example in this configuration)
- Set First Name: Avaya (example in this configuration)
- Set Login Name: 17813131034@aura.com (example in this configuration)

Under **Communication Profile** tab, click Communication Profile Password

- Set Comm-Profile Password: any password (Numbers or alphabets or alphanumeric)
- Re-enter Comm-Profile Password: Type the password again for confirmation.

Navigate to **Communication address tab**, click New

- Set Type: Avaya SIP
- Set Fully Qualified Address: Type the Directory number @domain.com  
17813131034@aura.com

Under **Profile tab**, enable **Session Manager Profile** and click it to open it.

- Set Primary Session Manager under SIP Registration: acme-sm (example in this configuration)
- Set Home Location Manager under Call Routing: Phonerlite (example in this configuration)
- Click Commit to save the configuration.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, a search bar, and user information (admin). The main navigation menu on the left shows 'User Management' with 'Manage Users' selected. The main content area is titled 'User Profile | Edit | 17813131034@aura.com' and features tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Identity' tab is active, showing the 'Basic Info' section. The 'User Provisioning Rule' is set to a dropdown menu. The 'Last Name' field contains 'User20', and the 'First Name' field contains 'Avaya'. The 'Login Name' field contains '17813131034@aura.com'. The 'Description' field contains 'Description Of User'. The 'Password' field is empty. The 'Last Name (Latin Translation)' field contains 'User20', and the 'First Name (Latin Translation)' field contains 'Avaya'. The 'Middle Name' field contains 'Middle Name Of User'. The 'Email Address' field contains 'Email Address Of User'. The 'User Type' dropdown menu is set to 'Basic'. Buttons for 'Commit & Continue', 'Commit', and 'Cancel' are visible at the top right of the form.

AVAYA Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts | Search | admin

Home | Routing | User Management

User Management

- Manage Users
- Public Contacts
- Shared Addresses
- System Presence ACLs
- Communication Profile ...

### User Profile | Edit | 17813131034@aura.com

Commit & Continue | Commit | Cancel

Identity | Communication Profile | Membership | Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

- Session Manager Profile
- CM Endpoint Profile

Comm-Profile Password

Comm-Profile Password : [masked]

Re-enter Comm-Profile Password : [masked] ✓

Generate Comm-Profile Password

Cancel | OK

AVAYA Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts | Search | admin

Home | Routing | User Management

User Management

- Manage Users
- Public Contacts
- Shared Addresses
- System Presence ACLs
- Communication Profile ...

### User Profile | Edit | 17813131034@aura.com

Commit & Continue | Commit | Cancel

Identity | Communication Profile | Membership | Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

- Session Manager Profile
- CM Endpoint Profile

Communication Address Add/Edit

\* Type : Avaya SIP

\*Fully Qualified Address : 17813131034 @ aura.com

Cancel | OK

**AVAYA** Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts

Search | adm

Home | Routing | **User Management**

User Management

**User Profile | Edit | 17813131034@aura.com**

Commit & Continue | Commit | Cancel

Identity | **Communication Profile** | Membership | Contacts

Communication Profile Password

PROFILE SET: Primary

Communication Address

PROFILES

Session Manager Profile

CM Endpoint Profile

**SIP Registration**

\* Primary Session Manager: acme-sm

Secondary Session Manager: Start typing...

Survivability Server: Start typing...

Max. Simultaneous Devices: 1

**AVAYA** Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts

Search | adm

Home | Session Manager | Routing | User Management | **User Management**

User Management

**Manage Users**

Public Contacts

Shared Addresses

System Presence ACLs

Communication Profile ...

Emergency Calling Origination Sequence: Select

Emergency Calling Termination Sequence: Select

**Call Routing Settings**

\* Home Location: Phonerlite

Conference Factory Set: Select

**Call History Settings**

Enable Centralized Call History?:

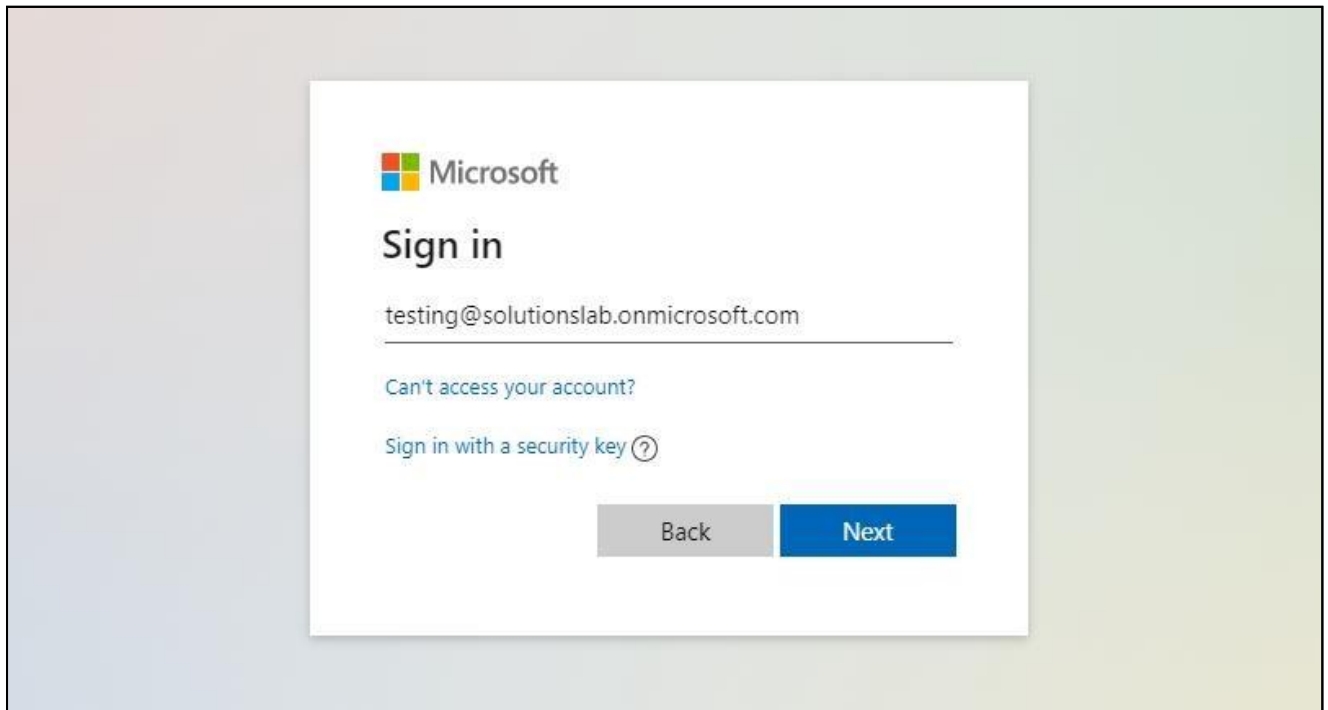
You can repeat the above steps to add more users to the Session Manager. With this, Avaya Session Manager Configuration is complete.

## 5. Configure Microsoft Teams Direct Routing

The steps outlined below is the minimum required configuration to pair your SBC with Microsoft Teams Direct Routing Interface. **This is to be used as an example only, and we highly recommend you work with your Microsoft Account representative to implement the correct configuration for your specific environment.**

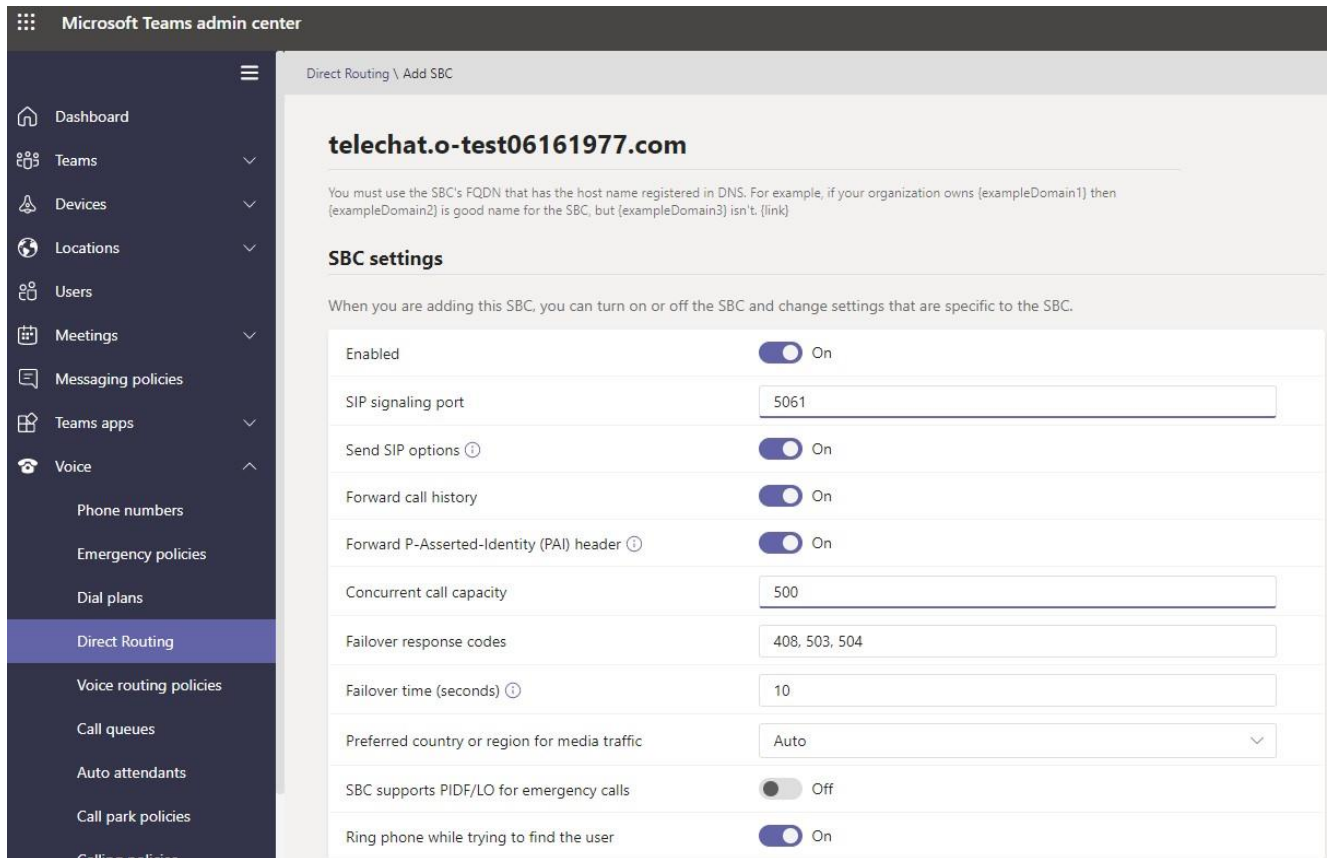
### 5.1. Access Team Admin center

The first step is to access the Teams Admin Center with administrator admin credentials:



## 5.2. Configure Online PSTN Gateway

Configuration Path: Voice/Direct Routing/SBC



The screenshot shows the Microsoft Teams admin center interface. The left sidebar is expanded to 'Voice' > 'Direct Routing'. The main content area is titled 'Direct Routing \ Add SBC' and shows configuration for 'telechat.o-test06161977.com'. A note states: 'You must use the SBC's FQDN that has the host name registered in DNS. For example, if your organization owns {exampleDomain1} then {exampleDomain2} is good name for the SBC, but {exampleDomain3} isn't. (link)'. Below this is the 'SBC settings' section with the following configuration:

Setting	Value
Enabled	On
SIP signaling port	5061
Send SIP options	On
Forward call history	On
Forward P-Asserted-Identity (PAI) header	On
Concurrent call capacity	500
Failover response codes	408, 503, 504
Failover time (seconds)	10
Preferred country or region for media traffic	Auto
SBC supports PIDF/LO for emergency calls	Off
Ring phone while trying to find the user	On

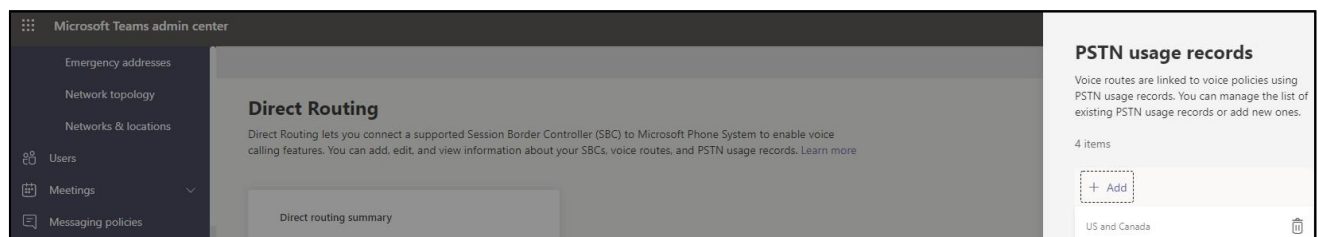
Click Save at the bottom of the page

Note: Some configuration fields are not available through the Microsoft Portal, and must be set via PowerShell. Please refer to [Microsoft Teams Documentation](#) for further details

## 5.3. Configure Online PSTN Usage

Configuration Path: Voice/Direct Routing/Manage PSTN usage Records (top right of screen)

Click Add, Type US and Canada, next, click Apply



The screenshot shows the Microsoft Teams admin center interface. The left sidebar is expanded to 'Voice' > 'Direct Routing'. The main content area is titled 'Direct Routing' and shows a 'Direct routing summary' section. On the right side, there is a 'PSTN usage records' section with the following text: 'Voice routes are linked to voice policies using PSTN usage records. You can manage the list of existing PSTN usage records or add new ones.' Below this text, it says '4 items' and shows a list with one item: 'US and Canada'. There is an '+ Add' button and a trash icon.

## 5.4. Configure Online Voice Routes

Configuration Path: Voice/Direct Routing/Voice Routes

The screenshot displays the Microsoft Teams admin center interface for configuring a voice route. The left-hand navigation pane is expanded to the 'Voice' section, with 'Direct Routing' selected. The main content area shows the configuration for the 'Oracle\_US' voice route. The 'Priority' is set to 1, and the 'Dialed number pattern' is set to `^\+1[0-9]{10}$`. Below this, the 'SBCs enrolled' section shows one SBC: 'sb2.customers.telechat.o-test06161977.com'. The 'PSTN usage records' section shows one record: 'US and Canada'.

Microsoft Teams admin center

Voice routes \ Oracle\_US

### Oracle\_US

Description

Priority: 1

Dialed number pattern: `^\+1[0-9]{10}$`

### SBCs enrolled

Select which SBC's you want calls to route to. All SBC's that you add will be tried in a random order.

Add/remove SBCs 1 item

✓	SBCs
	sb2.customers.telechat.o-test06161977.com

### PSTN usage records

The voice routing policy is linked to a voice route using the PSTN usage records below. You can add existing PSTN usage records, change the order in which the voice routing should be processed, and assign the policy to users.

Add/remove PSTN usage records ↑ Move up ↓ Move down 1 item

✓	PSTN usage record
	US and Canada

## 5.5. Configure Online Voice Routing Policy

Configuration Path: Voice/Voice Routing Policies

Microsoft Teams admin center

Voice routing policies \ US Only

### US Only

Add a friendly description so you know why it was created

#### PSTN usage records

PSTN usages are linked to both voice routing policies, which are assigned to users, and voice routes. PSTN usages are evaluated in the order they are listed until a match is found.

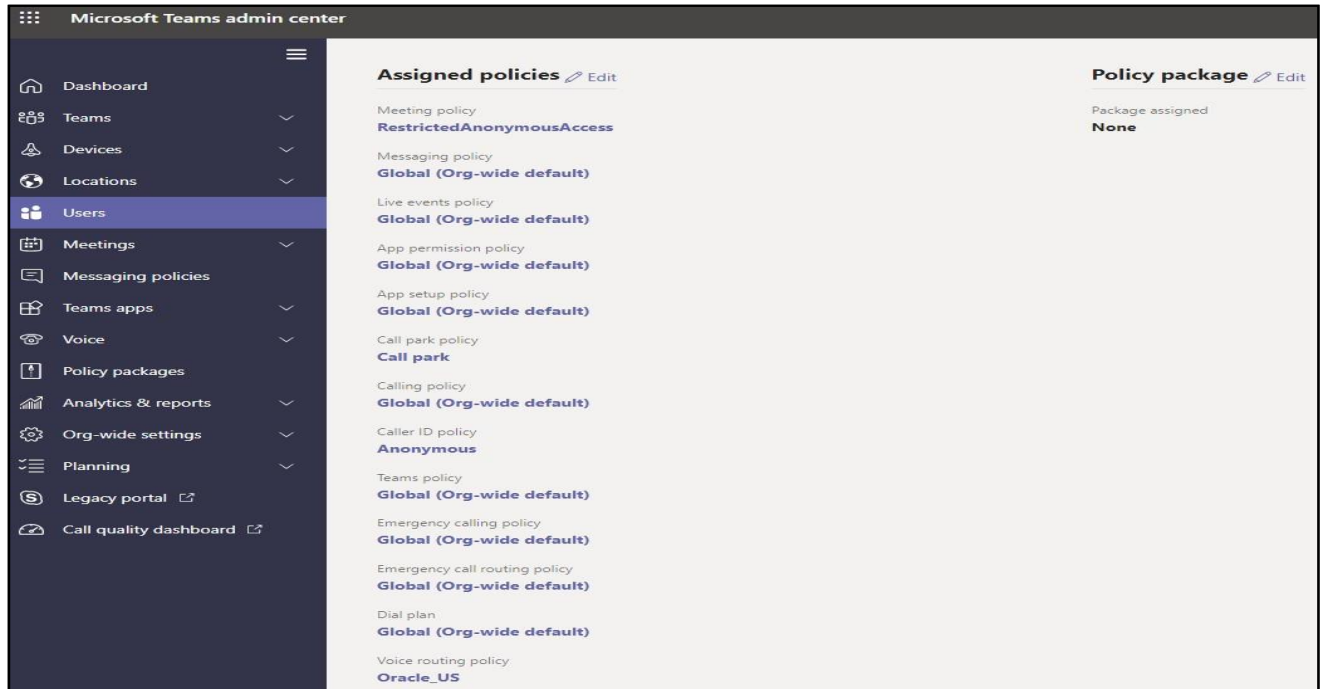
Add/remove PSTN usage records   ↑ Move up   ↓ Move down   1 item

✓	PSTN usage record
✓	US and Canada

## 5.6. Assign Voice Routing Policy to Users

Configuration Path: Users/Select the “User”/Policies

Next to Voice Routing Policy, Click Edit and Assign. In this example, we have selected Teamsuser1:



For More Information about configuring Microsoft Teams to Connect to your SBC, Setting up users, or configuration voice routing, please refer to the [Related Documentation](#) Section of this guide.

With this, Microsoft Teams Direct Routing config is complete.

## 6. 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.



## 6.1. 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.

```
login as: admin
admin@10.138.194.175's password:

LabECB# bootparam
% command not found
LabECB# conf t
LabECB (configure)# bootparam

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

Boot File      : /boot/nnPCZ320p5.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.

LabECB (configure)#
LabECB (configure)#
LabECB (configure)#
LabECB (configure)#
LabECB (configure)#
```

Setup product type to Enterprise Communication broker as shown below.

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

```
LabECB#
LabECB#
LabECB# 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]: 1
```

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

Save the changes and reboot the ECB.

```
LabECB#
LabECB# show entile
LabECB# show entil
LabECB# show entitlements
Provisioned Entitlements:
-----
Enterprise Communication Broker Base    : enabled
Session Capacity                        : 10000

Keyed (Licensed) Entitlements
-----
LabECB#
```

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.

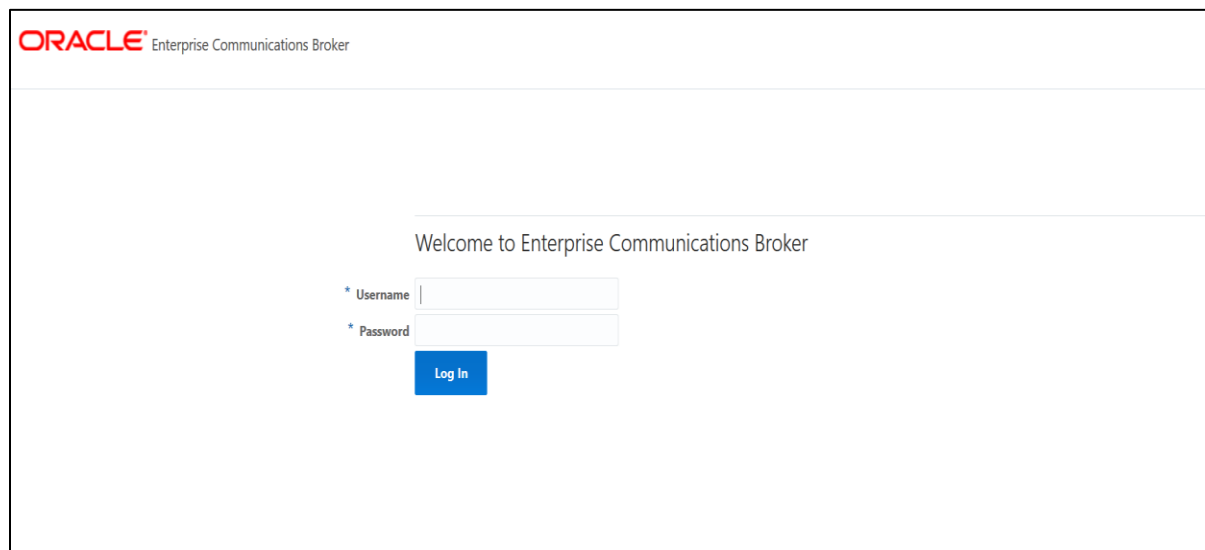
```
LabECB(web-server-config) #  
LabECB(web-server-config) # show  
web-server-config  
    state                enabled  
    inactivity-timeout   10  
    http-state           enabled  
    http-port            80  
    https-state          disabled  
    https-port           443  
    http-interface-list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

## 6.2 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.



ORACLE<sup>®</sup> Enterprise Communications Broker

Welcome to Enterprise Communications Broker

\* Username

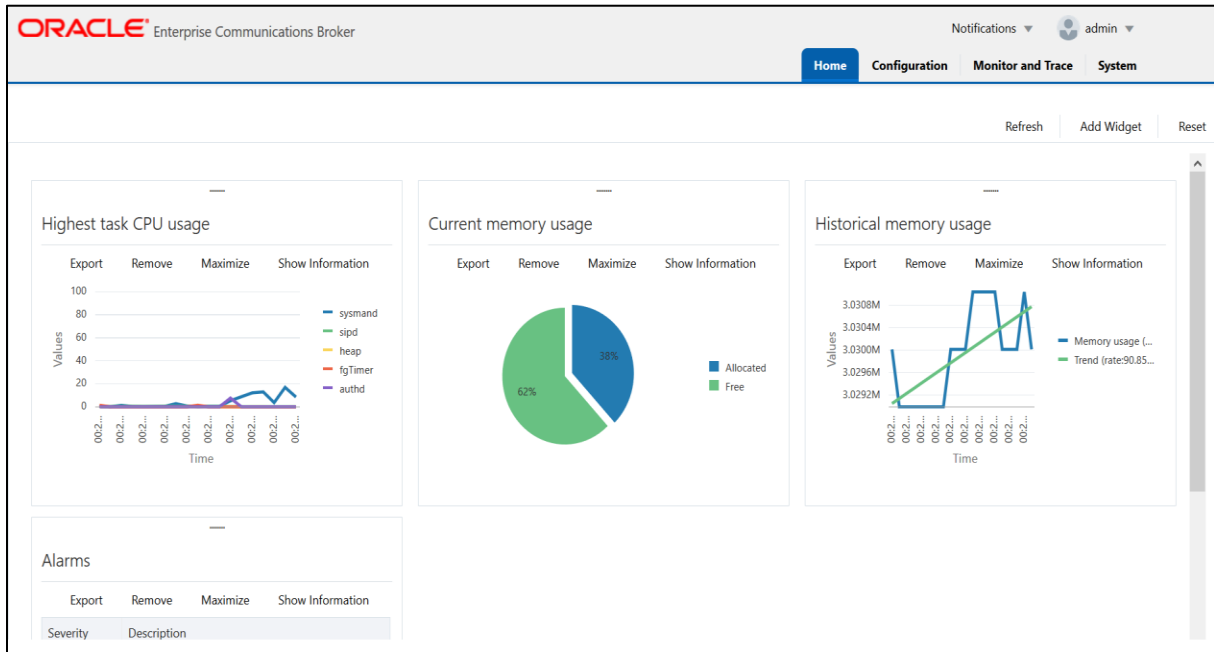
\* Password

Log In

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 four tabs across the top –Home, Configuration, Monitor and Trace, and System.



### 6.3. Add Network Settings

Click the Configuration button at the top to go to the Configuration tab.  
Go to System Administration ---- Network --- Network Settings and Click Add

The screenshot shows the 'Add Network Settings' configuration page in the Oracle Enterprise Communications Broker. The 'Configuration' tab is active, and the left sidebar shows 'Network Settings' selected under the 'Network' category.

The configuration form includes the following fields:

- Realm Identifier: ecb
- VLAN Id: 0
- Hostname: (empty)
- Network IP Address: 10.232.50.70
- Network IP Subnet Mask: 255.255.255.0
- Network IP Gateway Address: 10.232.50.1
- Preferred DNS Server IP Address: (empty)
- Alternate DNS Server IP Address: (empty)
- Alternate DNS Server IP Address: (empty)
- DNS Domain: (empty)
- Enable REFER Termination:  enable

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

## 6.4. Configure SIP Interface

Go to System Administration ---- SIP Interfaces --- Interfaces and Click Add

The screenshot shows the Oracle Enterprise Communications Broker interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', and 'System'. The left sidebar lists various configuration categories, with 'SIP Interface' and 'Interfaces' highlighted. The main content area is titled 'Modify SIP Interface' and contains the following fields:

- State:  enable
- Enable Early Media Inhibit:  enable
- Realm ID: ecb
- Description: ECB Interface

Below these fields is a table for 'SIP Port' configuration:

Address	Port	Transport Protocol	Allow Anonymous
10.232.50.70	5060	TCP	all
10.232.50.70	5060	UDP	all

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

## 6.5. Configuring the Agents

Click Configuration --- Service Provisioning ----- Agents --- Session Agents and Click Add.  
We will now add 10.232.50.65 as Agent to ECB (SBC SIP interface)

The screenshot shows the Oracle Enterprise Communications Broker interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', and 'System'. The left sidebar lists various configuration categories, with 'Service Provisioning' and 'Session Agent' highlighted. The main content area is titled 'Add Agents' and contains the following fields:

- Hostname: 10.232.50.65
- IP Address: 10.232.50.65
- Port: 5060
- State:  enable
- RURI With Hostname:  enable
- Transport Method: UDP+TCP
- TLS Profile: (empty)
- Realm ID: ecb
- Description: (empty)

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

ORACLE Enterprise Communications Broker

Notifications admin

Home Configuration Monitor and Trace System

Commands Save Verify Discard Sea

### Add Agents

Source Context

Egress URI Mode: no-conversion

Egress Number Translation Mode: E164-no-plus

Number Of Digits For N Digit Dialing: 4

Prepend Prefix On Egress

Outbound Translate From Number  enable

Stop Recurse

Constraints  enable

Max Sessions: 0

Max Inbound Sessions: 0

Max Outbound Sessions: 0

OK Back

Similarly, add another agent 10.232.50.127 (Avaya server) to the ECB.

ORACLE Enterprise Communications Broker

Notifications admin

Home Configuration Monitor and Trace System

Commands Save Verify Discard Sea

### Add Agents

Hostname: aura.com

IP Address: 10.232.50.127

Port: 5060

State:  enable

RURI With Hostname  enable

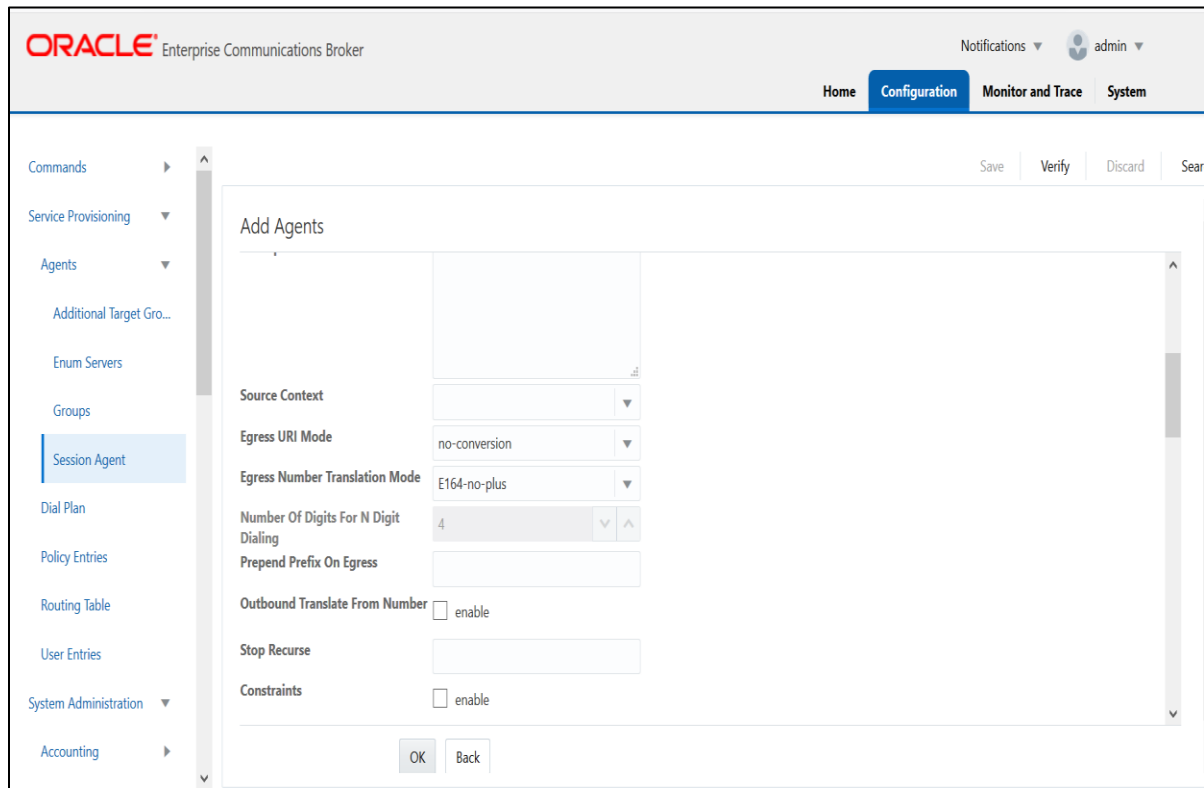
Transport Method: UDP+TCP

TLS Profile

Realm ID: ecb

Description

OK Back



## 6.6. 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.

Go to Configuration tab --- Service Provisioning and Click Routing table

Add a routing entry for the source agent Avaya server (10.232.50.127) with a route set to SBC IP (10.232.50.65) and click OK

The screenshot shows the Oracle Enterprise Communications Broker interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', and 'System'. The user is logged in as 'admin'. The left sidebar shows a tree view with 'Routing Table' selected under 'Policy Entries'. The main content area is titled 'Add Routing Table' and contains the following fields:

Source Agent	10.232.50.127
Calling Number	*
Dest Agent	*
Called Number	*
Route	10.232.50.65
Cost	0
Policy	
Description	
Tags	

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

When the ECB receives a call from 10.232.50.127, 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 Avaya server (10.232.50.127)

This screenshot shows the same 'Add Routing Table' configuration page, but with the source and destination agents swapped. The fields are:

Source Agent	10.232.50.65
Calling Number	*
Dest Agent	*
Called Number	*
Route	10.232.50.127
Cost	0
Policy	
Description	
Tags	

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

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





## 7. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Avaya Session Manager, Teams Direct Routing and Verizon Trunk. The SBC config here deals with Avaya end points registering directly to Avaya Session Manager.

**Note: The configuration of registering Avaya remote worker (Registering Avaya End points via Oracle SBC) is already explained in the app note link given below and it can be used as a reference to configure the same. Once the remote worker is registered to Avaya SM using Oracle SBC, we can use this document to make calls from Avaya User to Teams User/Verizon Trunk user and Vice versa.**

<https://www.oracle.com/a/otn/docs/avaya-remote-worker-with-tls.pdf>

### 7.1. Validated Oracle SBC version

Oracle conducted tests with Oracle SBC 8.4 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
- VME

## 8. New SBC configuration

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

### 8.1. Establishing a serial connection to the SBC

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

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

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

```
Starting tLemd...
Starting tServiceHealth...
Starting tCollect...
Starting tAtcpd...
Starting tAsctpd...
Starting tMbcd...
Starting tCommMonitord...
Starting tFped...
Starting tAlgd...
Starting tRadd...
Starting tEbmd...
Starting tSipd...
Starting tH323d...
Starting 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
```

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

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

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

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

```
NN4600-139 (configure) # bootparam

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

Boot File           : /boot/nnsCZ840p2.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         : NN4600-139
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: 25)

NN4600-139 (configure) #
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

```
NN4600-139#
NN4600-139# setup product

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

Last Modified 2020-04-30 22:38:15
-----

 1 : Product           : Enterprise Session Border Controller

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

Enable the features for the ESBC using the setup entitlements command as shown  
Save the changes and reboot the SBC.

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

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1
  Session Capacity (0-128000)           : 500

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 3
*****
CAUTION: Enabling this feature activates enhanced security
functions. Once saved, security cannot be reverted without
resetting the system back to factory default state.
*****
  Admin Security (enabled/disabled)      :

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 5
  Transcode Codec AMR Capacity (0-102375) : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2
  Advanced (enabled/disabled)           : enabled

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10
  Transcode Codec OPUS Capacity (0-102375) : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 11
  Transcode Codec SILK Capacity (0-102375) : 50
```

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

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

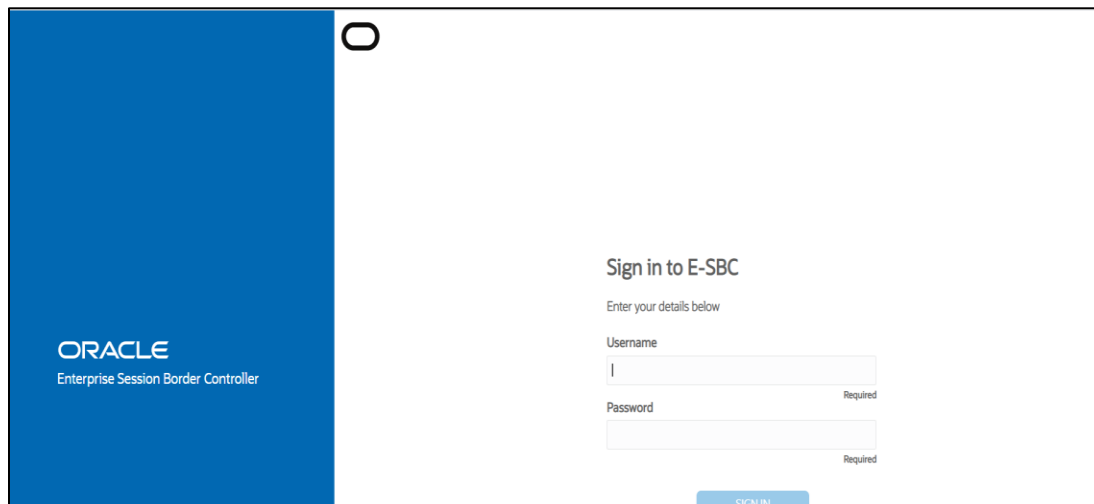
Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

```
NN4600-139(http-server)#
NN4600-139(http-server)# show
http-server
  name                webServerInstance
  state               enabled
  realm
  ip-address
  http-state          enabled
  http-port           80
  https-state         disabled
  https-port          443
  http-interface-list REST, GUI
  http-file-upload-size 0
  tls-profile
  auth-profile
  last-modified-by    @
  last-modified-date  2021-01-25 00:16:28
NN4600-139(http-server)# █
```

## 8.2. Configure SBC using Web GUI

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

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



ORACLE  
Enterprise Session Border Controller

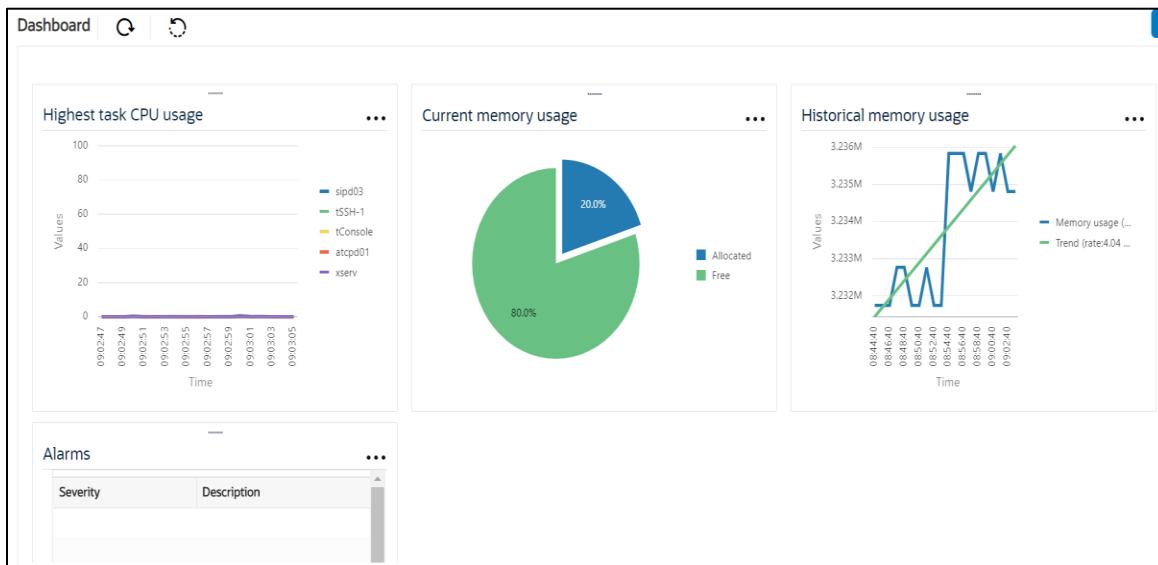
Sign in to E-SBC

Enter your details below

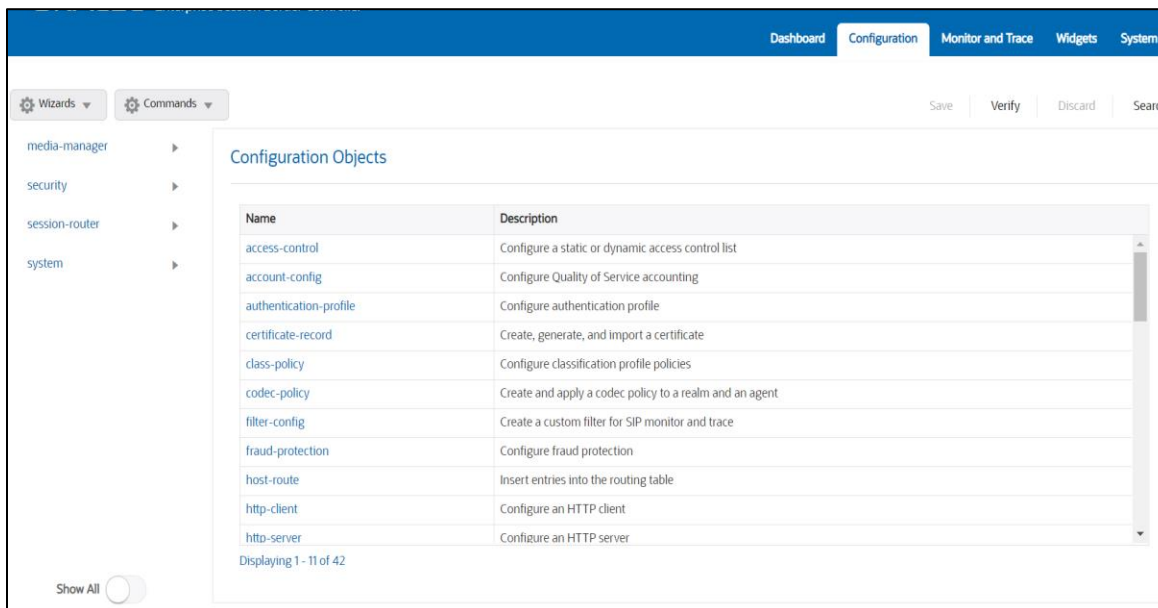
Username

Password  Required

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/8.4.0/webgui/esbc\\_scz840\\_webgui.pdf](https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf)

The expert mode is used for configuration.

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

### 8.3. Configure system-config

Go to system->system-config

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'system-config' option is selected in the left-hand menu. The main area displays the 'Modify System Config' form with the following fields:

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

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

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'system-config' option is selected in the left-hand menu. The main area displays the 'Modify System Config' form with the following fields:

Call Trace	<input type="checkbox"/> enable
Default Gateway	10.158.194.129
Restart	<input checked="" type="checkbox"/> enable
Telnet Timeout	0 ( Range: 0..65535 )
Console Timeout	0 ( Range: 0..65535 )
HTTP Timeout	5 ( Range: 0..20 )

The 'Default Gateway' field is highlighted with a red box. Buttons for 'Add', 'OK', and 'Delete' are visible at the bottom of the form.

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/8.4.0/releasenotes/esbc\\_scz840\\_releasenotes.pdf](https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/releasenotes/esbc_scz840_releasenotes.pdf)

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

## 8.4. 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 public interface. (For Teams and Verizon side)  
Avaya side is configured on the slot 0 port 1

Parameter Name	Public Interface(M00)	Avaya Side (M10)
Slot	0	0
Port	0	1
Operation Mode	Media	Media

Please configure M00 interface as below.

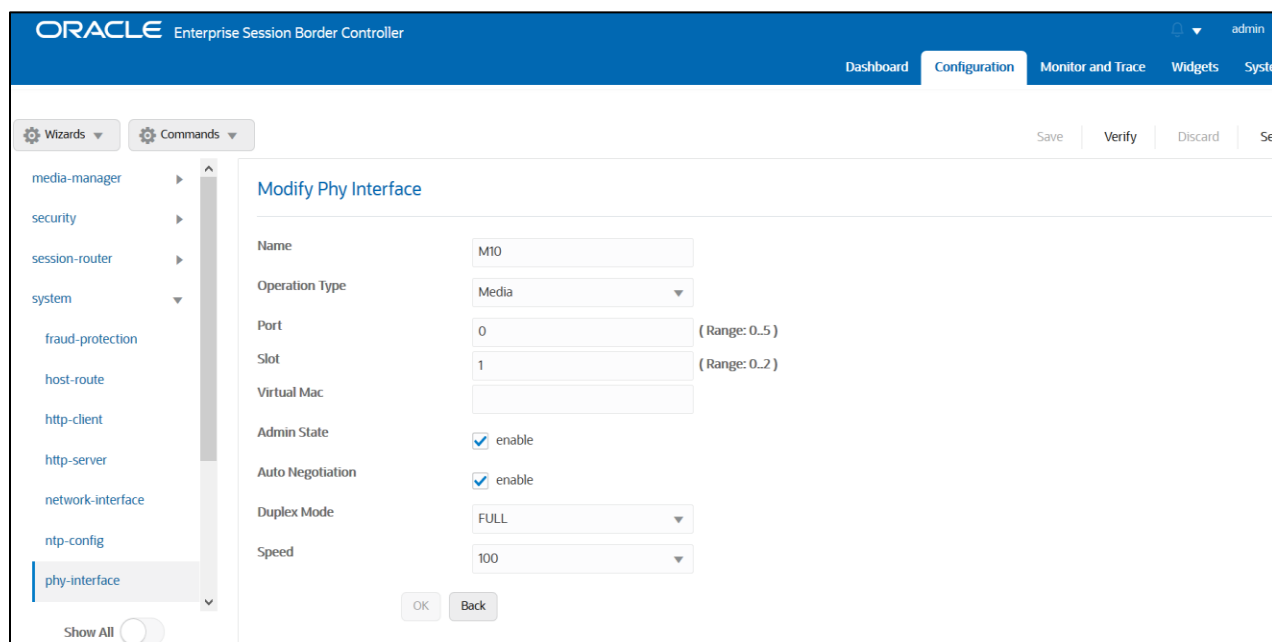
The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The main heading is "Modify Phy Interface". The form contains the following fields and values:

- Name: M00
- Operation Type: Media
- Port: 0 (Range: 0-5)
- Slot: 0 (Range: 0-2)
- Virtual Mac: (empty)
- Admin State:  enable
- Auto Negotiation:  enable
- Duplex Mode: FULL
- Speed: 100

At the bottom of the form are "OK" and "Back" buttons. The left sidebar shows a navigation menu with "phy-interface" selected. The top navigation bar includes "Dashboard", "Configuration", "Monitor and Trace", "Widgets", and "System".



Similarly, configure M10 interface as below.



### 8.5. Configure Network Interface values

To configure network-interface, go to system->Network-Interface. Configure two interfaces

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

Parameter Name	Public Interface (For Teams and Verizon)	Avaya Core side Network interface
Name	M00	M10
Host Name	customers.telechat.o-test06161977.com	
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

Please configure network interface M00 as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Network Interface". The left sidebar lists various configuration categories, with "network-interface" selected. The main form contains the following fields:

Name	M00
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	customers.telechat.o-test06161977.com
IP Address	
Pri Utility Addr	
Sec Utility Addr	

Buttons for "OK" and "Back" are visible at the bottom of the form.

Please configure network interface M10 as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Network Interface". The left sidebar lists various configuration categories, with "network-interface" selected. The main form contains the following fields:

Name	M10
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	
IP Address	10.252.50.65
Pri Utility Addr	
Sec Utility Addr	

Buttons for "OK" and "Back" are visible at the bottom of the form.

## 8.6. Enable media manager

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

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

The screenshot shows the 'Modify Media Manager' configuration page in the Oracle Enterprise Session Border Controller. The 'State' checkbox is checked and labeled 'enable'. Other configuration items include:

Parameter	Value	Range
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 )
Hint Rtcp	<input type="checkbox"/> enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	

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

The screenshot shows the 'Modify Media Manager' configuration page in the Oracle Enterprise Session Border Controller, specifically the 'Media Policing' section. The 'Media Policing' checkbox is checked and labeled 'enable'. Other configuration items include:

Parameter	Value	Range
Max Arp Rate	10	( Range: 0..100 )
Max Signaling Packets	0	( Range: 0..4294967295 )
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 )
AcI Monitor Window	30	( Range: 5..3600 )
Trap On Demote To Deny	<input type="checkbox"/> enable	

Red arrows point to the 'Max Untrusted Signaling' and 'Min Untrusted Signaling' fields, both of which are set to 1.

## 8.7. Configure Realms

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

Use the following table as a configuration example for the three realms used in this configuration:

Config Parameter	Teams Realm	Avaya Realm	Verizon Realm
Identifier	Teams	Avaya Realm	Verizon
Network Interface	M00	M10	M00
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Teams-FQDN	Telechat.o-test06161977.com		
Teams fqdn in uri	<input checked="" type="checkbox"/>		
Sdp inactive only	<input checked="" type="checkbox"/>		
Media Sec policy	sdespolicy	RTP	RTP
RTCP mux	<input checked="" type="checkbox"/>		
ice profile	ice		
Codec policy	addCN	OptimizeCodecs	OptimizeCodecs
RTCP policy	rtcpGen		
Access Control Trust Level	High	High	High
Pai-strip	Enabled	Enabled	
Media-policy			VerizonQOS
Refer Call Transfer	Enabled		

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Add Realm Config' form is displayed with the following fields and values:

- Identifier: Teams
- Description: (empty)
- Addr Prefix: 0.0.0.0
- Network Interfaces: M00:0.4
- Media Realm List: (empty)
- Mm In Realm:  enable

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

The screenshot shows the 'Modify Realm Config' interface in the Oracle Enterprise Session Border Controller. The left sidebar lists various configuration categories, with 'realm-config' selected. The main area contains several configuration fields:

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

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

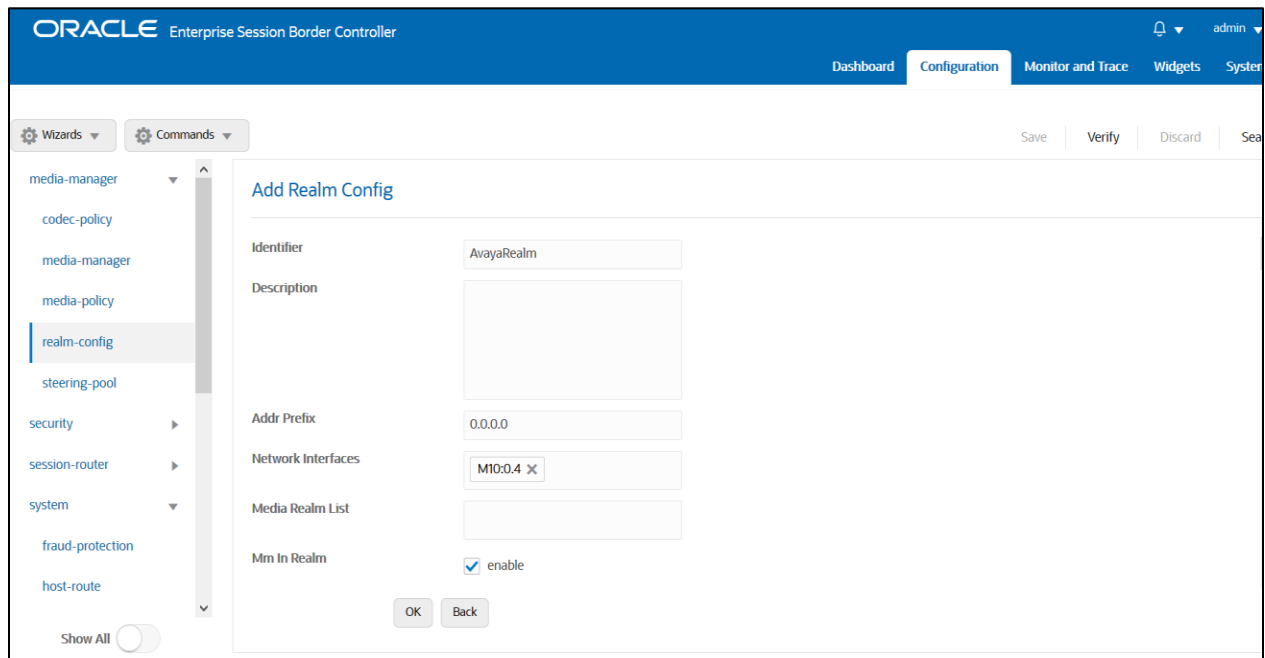
Similarly, Realm name is given as Verizon for Verizon Trunk Side.  
Please set the Access Control Trust Level as high for this realm

The screenshot shows the 'Add Realm Config' interface in the Oracle Enterprise Session Border Controller. The left sidebar lists various configuration categories, with 'realm-config' selected. The main area contains several configuration fields:

Field Name	Value
Identifier	Verizon
Description	
Addr Prefix	0.0.0.0
Network Interfaces	M00:0.4 X
Media Realm List	
Mm In Realm	<input checked="" type="checkbox"/> enable

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

Finally, Realm name is given as AvayaRealm for Avaya Side.  
Please set the Access Control Trust Level to high for this realm



The screenshot displays the Oracle Enterprise Session Border Controller (SBC) configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration' (selected), 'Monitor and Trace', 'Widgets', and 'System'. The user is logged in as 'admin'. The left sidebar shows a tree view of configuration categories: 'media-manager', 'codec-policy', 'media-manager', 'media-policy', 'realm-config' (selected), 'steering-pool', 'security', 'session-router', 'system', 'fraud-protection', and 'host-route'. The main content area is titled 'Add Realm Config' and contains the following fields:

- Identifier: AvayaRealm
- Description: (empty text area)
- Addr Prefix: 0.0.0.0
- Network Interfaces: M10:0.4
- Media Realm List: (empty text area)
- Mm In Realm:  enable

At the bottom of the form are 'OK' and 'Back' buttons. The top right of the form area has 'Save', 'Verify', 'Discard', and 'Sea' buttons.

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/8.4.0/security/sbc\\_scz840\\_security.pdf](https://docs.oracle.com/en/industries/communications/session-border-controller/8.4.0/security/sbc_scz840_security.pdf)

## 8.8. Enable sip-config

SIP config enables SIP handling in the SBC.

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

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

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

- add max-udp-length =0 & global-contact
- inmanip-before-validate & reg-cache-mode=from

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active. The left sidebar lists various configuration sections, with 'sip-config' selected. The main area is titled 'Modify SIP Config' and contains the following fields:

State	<input checked="" type="checkbox"/> enable
Dialog Transparency	<input checked="" type="checkbox"/> enable
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)

Buttons: OK, Delete

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active. The left sidebar lists various configuration sections, with 'sip-config' selected. The main area is titled 'Modify SIP Config' and contains the following fields:

Enforcement Profile	
Red Max Trans	10000 (Range: 0..50000)
Options	global-contact ✕ inmanip-before-validate ✕ max-udp-length=0 ✕ reg-cache-mode=from ✕
SPL Options	
SIP Message Len	4096 (Range: 0..65535)
Enum Sag Match	<input type="checkbox"/> enable
Extra Method Stats	<input checked="" type="checkbox"/> enable

Buttons: OK, Delete

## 8.9. Configuring a certificate for SBC

This section describes how to configure the SBC for both TLS and SRTP communication with Teams Direct Routing and IKE/IPSEC to connect to Verizon Business IP Trunk.

Microsoft Teams Direct Routing only allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by one of the trusted Certificate Authorities. A list of currently supported Certificate Authorities can be found at:

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

Similarly, Verizon Business requires a secure, IPSEC tunnel be established between the Oracle SBC and the VZB network. You must obtain the IPSEC Template from your Verizon Business account team before configuring IKE/IPSEC on the Oracle SBC.

For the purposes of this application note, we'll create three 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 content area is divided into a left sidebar and a right main panel. The sidebar, titled 'Configuration', contains a search bar and a list of configuration categories: 'media-manager', 'security', 'authentication-profile', 'certificate-record' (highlighted), 'tls-global', 'tls-profile', 'session-router', and 'system'. The main panel 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>

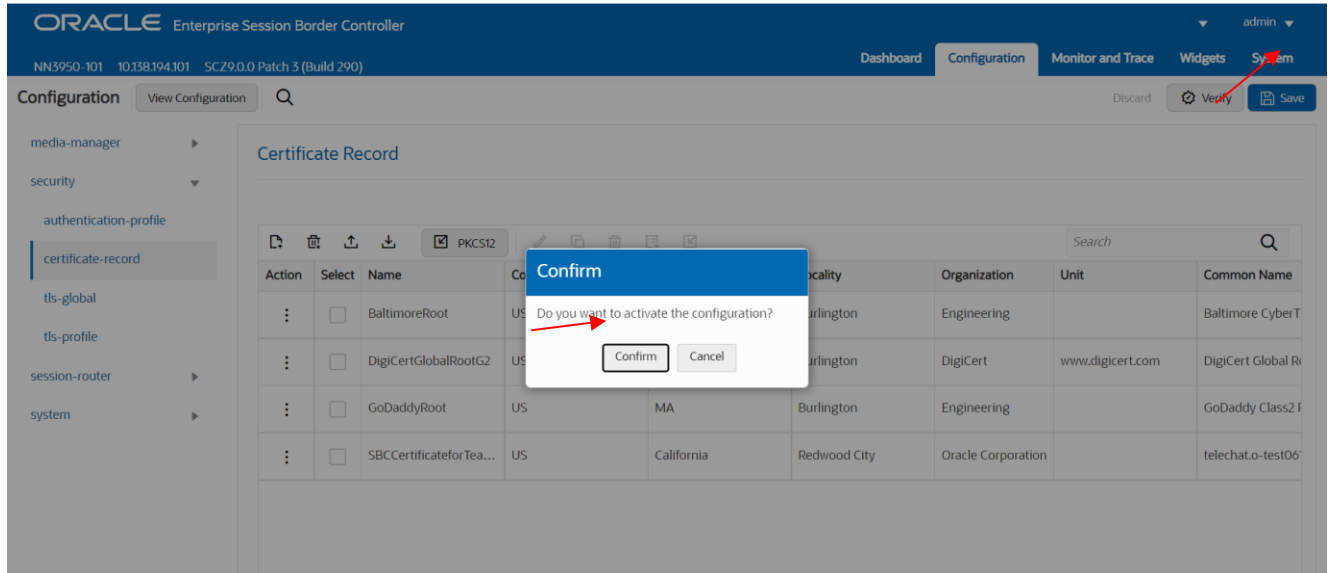
Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

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', version information (NN5950-101, 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 features a 'Certificate Record' table with columns: Action, Select, Name, Country, State, Locality, Organization, Unit, and Common Name. The table lists four certificates: 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 Ri
:	<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.



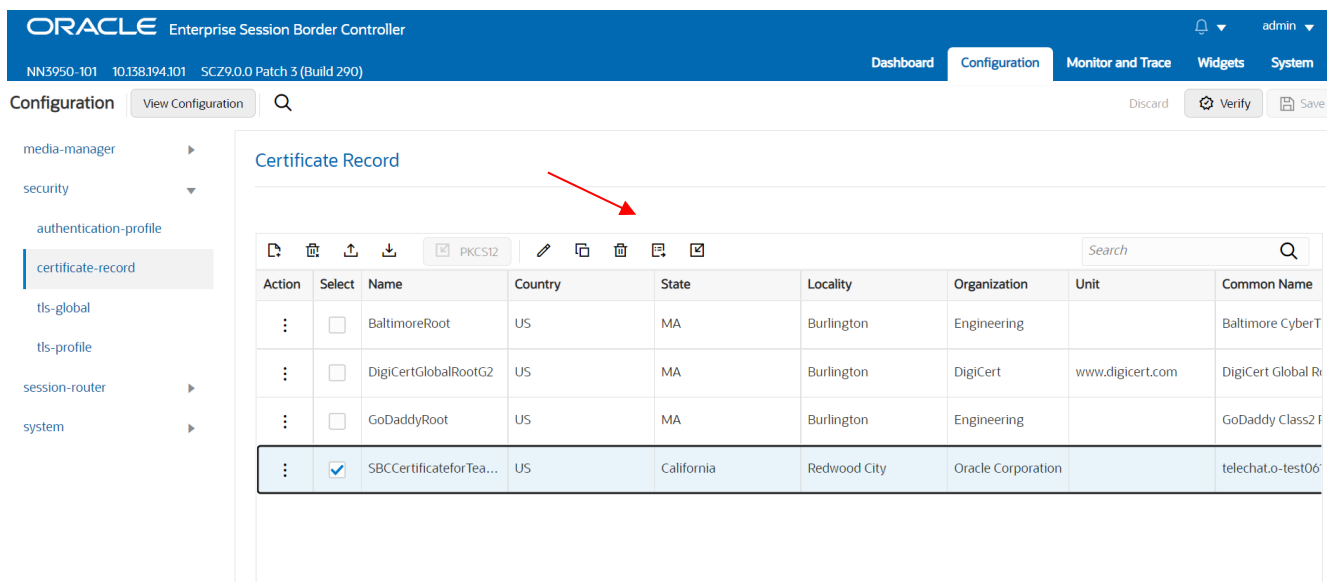
The screenshot shows the Oracle Enterprise Session Border Controller GUI. The 'Configuration' tab is active, and the 'Certificate Record' page is displayed. A table lists several certificates. A confirmation dialog box is overlaid on the table, asking 'Do you want to activate the configuration?' with 'Confirm' and 'Cancel' buttons. A red arrow points to the 'Confirm' button.

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'

### 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:



The screenshot shows the Oracle Enterprise Session Border Controller GUI. The 'Configuration' tab is active, and the 'Certificate Record' page is displayed. The 'SBCCertificateforTea...' certificate is selected, indicated by a checked checkbox and a red arrow pointing to the 'generate' tab at the top of 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'

## Generate certificate response

Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwbDELMakGATUEBhMCMVVMxGzAJBgNVBAgTAKIBMRMwEQYDVQQL
EwpCdXJsaW5ndG9uMRQwEgYDVQKKEwTfmdpbmVlcmluZzEIMCMGATUEAxMcdGVs
ZWN0eXQub3VlYXN0LTA2MTYxOTc3LmNvbTCCASlwdQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAK+uhx7951uhDgtQqWvo4EoZE68WDLIDYPPYcJWbvL5uWzk6y3Yh
s40ca4ZuZWmrLNLJLZfv9x9R5KzM4M8wqYiUvPOBC6oowuautu/swSKlReSpfDZh
NaAGUJrvAfVacyPz7KsyrJKgchzsOFNNJPDAAQsDQjuoFCDUbtOA1Z6xDFxpcDIF
nhq+dtB7gAtCdvWE/V6r4PAfJ1dj82YT4YBAWqwQJ2wGn+yc2FEPSmHIbWEiCvR
sMGfUeJcTM5i//AVcpF+jsJc8xswtE+Zr24kEiCrcrm0llgDHRvEgY1TuUteFoLy
d/60oaVPYHkKn250HQ2lwaMllkMxpBjlpUCAwEAAsA9MDsGCsGqGS1b3DQEJDEu
MCwwCwYDVROPAQDAgWgMB0GATUdJQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAN
BgkqhkiG9w0BAQsFAAOCAQEAnBLJuRPL82rkQDIB3I2JeOf3tacevMQeCIGcdFCf
uLcey+2XmtKF+HHPIECde+tLkXiJseVlnfBT2Ba4KymPwmTkQ5DfoLYQjWFOhEsm
LcuKMvjBYekJwebDk9CtDWwBZ9O1DzYbyuVNXPLbID5ludWbJBAYwd+9693VUVQb
/UR5rooNKwQIOFJMNmuPMW13v/p7kVsItk8aSwF6IHnx+k56MrR45YFqV//zCQTs
PeTYRyOVGYSQs0h5T5kcU0xjEXPI5K2gpdQz8YGbIAbKZXcpJn7zJEwgtodmRnhZ
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

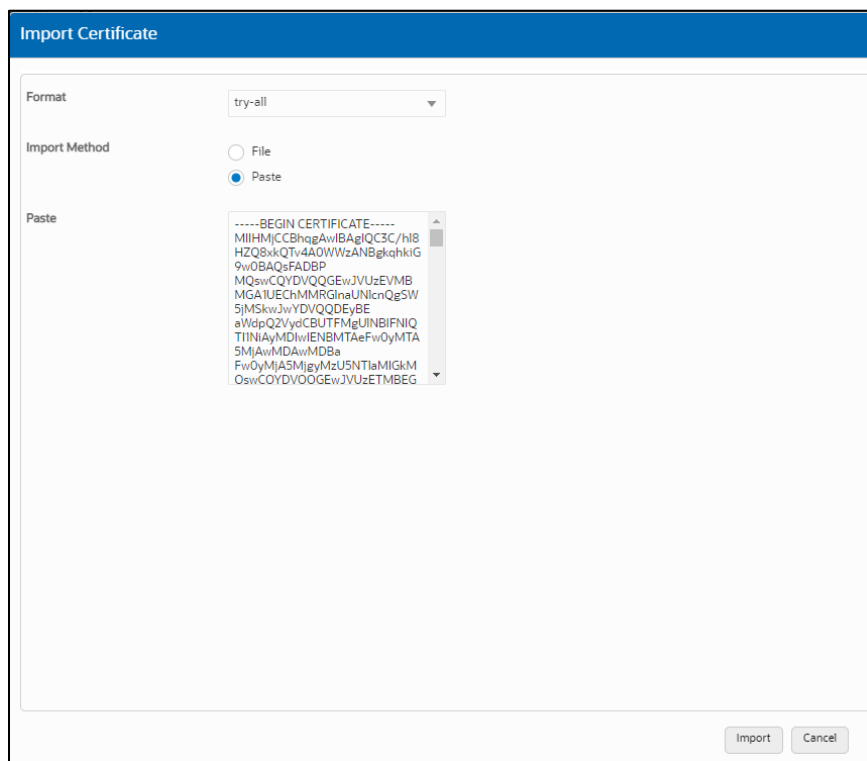
Once certificate signing request has been completed – import the signed certificate to the SBC.

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 the Oracle logo, the product name 'Enterprise Session Border Controller', and user information 'admin'. The main navigation menu has 'Configuration' selected. The left sidebar shows a tree view with 'certificate-record' selected. The main content area is titled 'Certificate Record' and contains a table with the following data:

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



- 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:

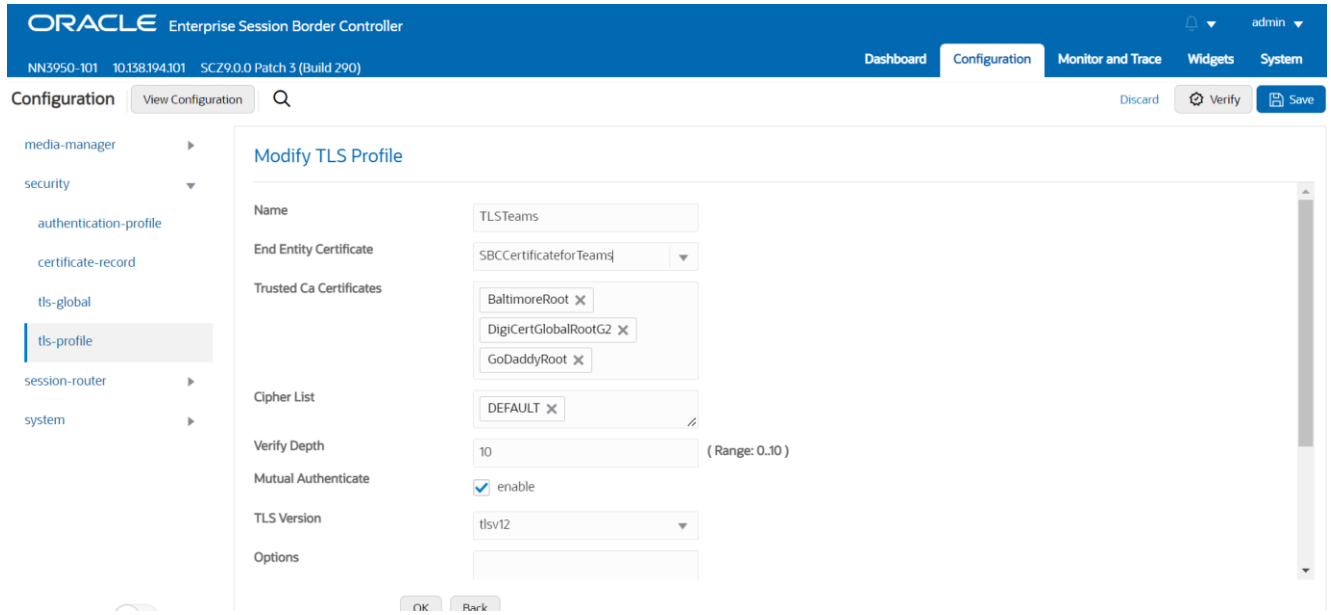
### 8.10.TLS Profile

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



- Select OK at the bottom

## 8.11. IKE/IPSEC Config

The configuration elements required for IKE are not available via the Oracle ESBC GUI, and must be configured from ACLI too.

**Note:** The examples provided will only display the parameters of each element that have been changed. All others can be left at default values unless required to be changed for your specific purpose.

### 8.11.1. IKE Config

ACLI Path: `config t → security → ike → ike-config`

Type Select, and use the below example to configure the global Ike configuration

ike-config

```

ike-version          1
log-level            NOTICE
phase1-dh-mode      dh-group2
phase2-exchangemode dh-group2
  
```

### 8.11.2. IKE Interface

ACLI Path: `config t → security → ike → ike-interface`

ike-interface

```

ike-version          1
address              155.212.214.101
realm-id             Verizon
ike-mode             initiator
shared-password      *****
  
```

sd-authentication-method shared-password

### 8.11.3. IKE Sainfo

ACLI Path: config t → security → ike → ike-sainfo

ike-sainfo

```
name VZ1
auth-algo md5
encryption-algo 3des
tunnel-local-addr 155.212.214.101
tunnel-remote-addr 152.188.29.84
```

ike-sainfo

```
name VZ2
auth-algo md5
encryption-algo 3des
tunnel-local-addr 155.212.214.101
tunnel-remote-addr 152.188.28.212
```

### 8.11.4. Security Policy

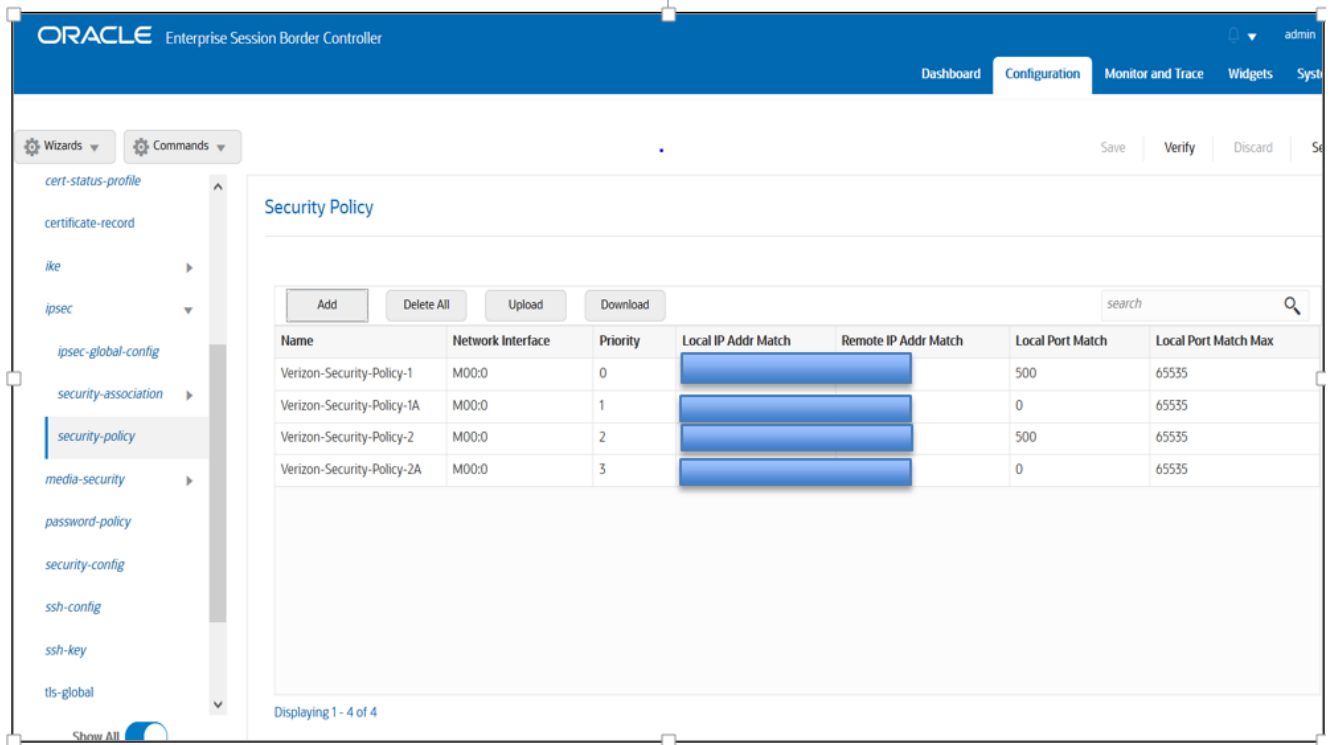
Security Policies are part of the IPSEC configuration on the SBC,

This is also available through the GUI. GUI Path: security/ipsec/security policy

ACLI Path: config t → security → ipsec → security-policy

Use the below table as an example to configure security policies on the SBC toward Verizon Business

Function	IPSEC	SIP	IPSEC	SIP
Name	Verizon-Security-Policy-1	Verizon-Security-Policy-1A	Verizon-Security-Policy-2	Verizon-Security-Policy-2A
Network-Interface	S1p0:0	S1p0:0	S1p0:0	S1p0:0
Priority	0	1	2	3
Local IP addr match	155.212.214.101	155.212.214.101	155.212.214.101	155.212.214.101
Remote ip addr match	<Vz-IPSEC-IP>	<VZ-SIP-IP>	<VZ-IPSEC-IP>	<VZ-Sip-IP>
Local port match	500	0	500	0
Remote port match	500	0	500	0
Local IP Mask	255.255.255.0	255.255.255.255	255.255.255.0	255.255.255.255
Remote IP mask	255.255.255.254	255.255.255.255	255.255.255.254	255.255.255.255
Ike-sainfo-name		VZ1		VZ2
Action	Allow	IPSEC	Allow	IPSEC
<b>Outbound-sa-fine-grained-mask</b>				
Local ip mask	255.255.255.255	255.255.255.0	255.255.255.255	255.255.255.0
Remote ip mask	255.255.255.255	255.255.255.254	255.255.255.255	255.255.255.224



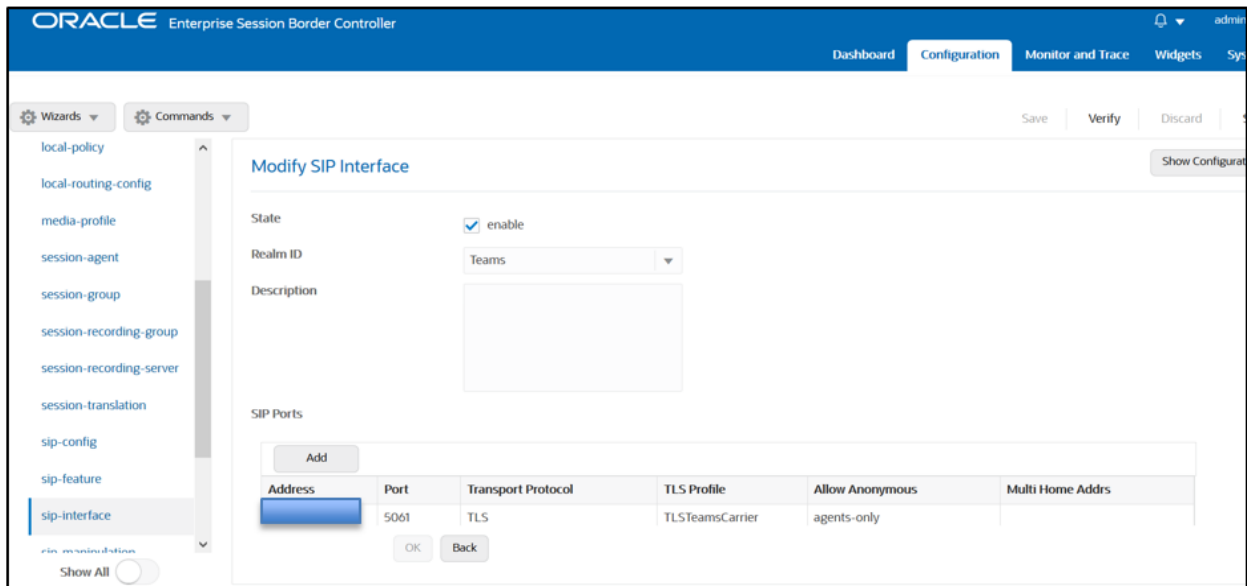
## 8.12. Configure SIP Interfaces

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

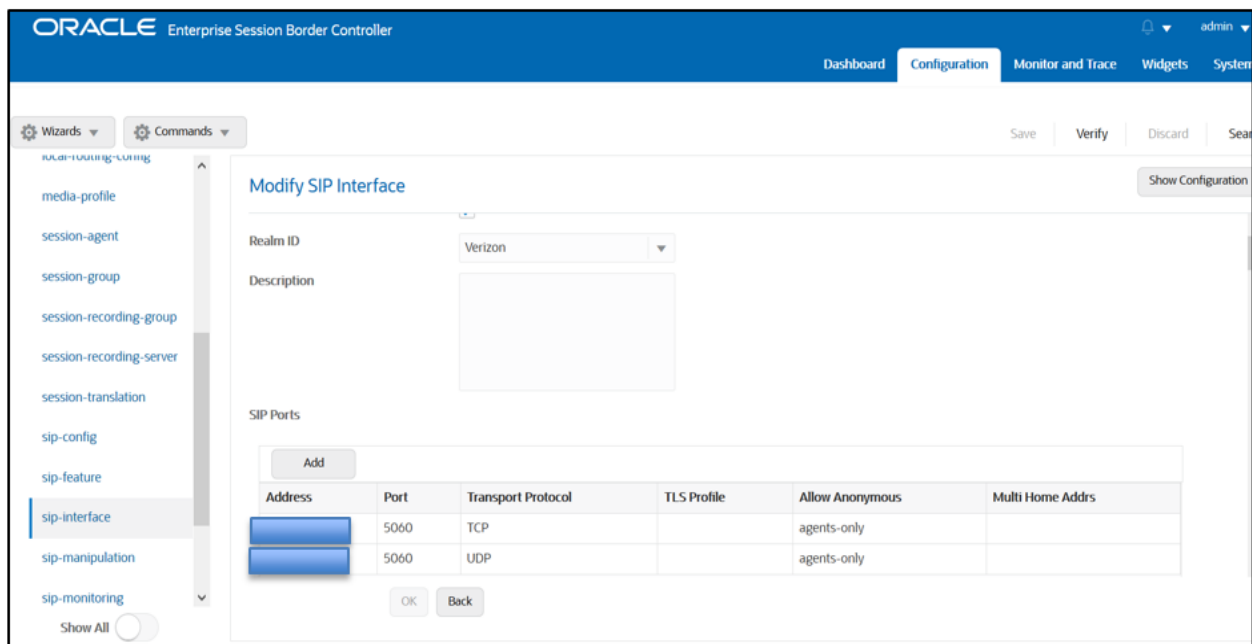
- Tls-profile needs to match the name of the tls-profile previously created
- Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from the particular Session agents added to the SBC. [Redacted]

Below is the sip-interface Configured for Teams side. [Redacted]

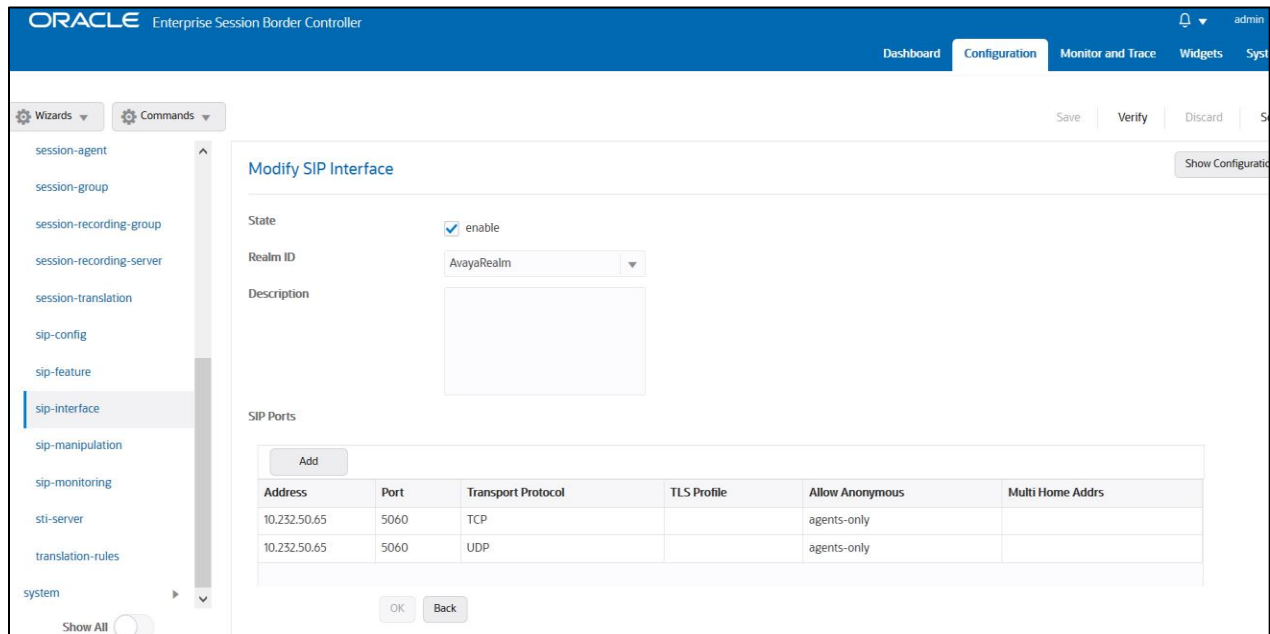




Similarly, Configure sip-interface for Verizon side as below:



Finally, configure sip-interface for Avaya side as below



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

### 8.13. Configure session-agent

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

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

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

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets Syst

Wizards Commands Save Verify Discard S

session-agent session-group session-recording-group session-recording-server session-translation sip-config sip-feature sip-interface sip-manipulation sip-monitoring sti-server translation-rules system

### Modify Session Agent

Show Configuration

Hostname: sip.pstnhub.microsoft.com

IP Address: [Empty]

Port: 5061 (Range: 0,1025..65535)

State:  enable

App Protocol: SIP

App Type: [Empty]

Transport Method: StaticTLS

Realm ID: Teams

Egress Realm ID: [Empty]

Description: [Empty]

OK Back

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets Syst

Wizards Commands Save Verify Discard S

session-agent session-group session-recording-group session-recording-server session-translation sip-config sip-feature sip-interface sip-manipulation sip-monitoring sti-server translation-rules system

### Modify Session Agent

Show Configuration

Proxy Mode: [Empty]

Redirect Action: [Empty]

Loose Routing:  enable

Response Map: [Empty]

Ping Method: OPTIONS

Ping Interval: 30 (Range: 0..4294967295)

Ping Send Mode: keep-alive

Ping All Addresses:  enable

Ping In Service Response Codes: [Empty]

Options: [Empty]

SPL Options: [Empty]

OK Back

Follow above steps to create 2 more sessions for:

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

Similarly, configure the session-agents for Verizon as below

- Host name to “sce10001.1259031211.globalipcom.com”and “ sce10002.1259031211.globalipcom.com”
- IP Address to 152.188.29.19 and 152.188.28.147
- port as 66292 and 5201
- realm-id – needs to match the realm created for Verizon
- transport set to “UDP+TCP

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Session Agent". The configuration fields are as follows:

Hostname	sce10001.1259031211.globalipcom.com
IP Address	152.188.29.19
Port	6292 (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
App Protocol	SIP
App Type	
Transport Method	UDP+TCP
Realm ID	Verizon
Egress Realm ID	
Description	

Buttons: OK, Back

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Session Agent". The configuration fields are as follows:

Hostname	sce10002.1259031211.globalipcom.com
IP Address	152.188.28.147
Port	5201 (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
App Protocol	SIP
App Type	
Transport Method	UDP+TCP
Realm ID	Verizon
Egress Realm ID	
Description	

Buttons: OK, Back

Finally, Configure the session-agent for Avaya Side 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 Avaya Side.
- transport set to “UDP+TCP”

The screenshot shows the Oracle Enterprise Session Border Controller (ESBC) configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The user is logged in as 'admin'. The left sidebar shows a tree view of configuration options, with 'session-agent' selected. The main area is titled 'Modify Session Agent' and contains the following configuration fields:

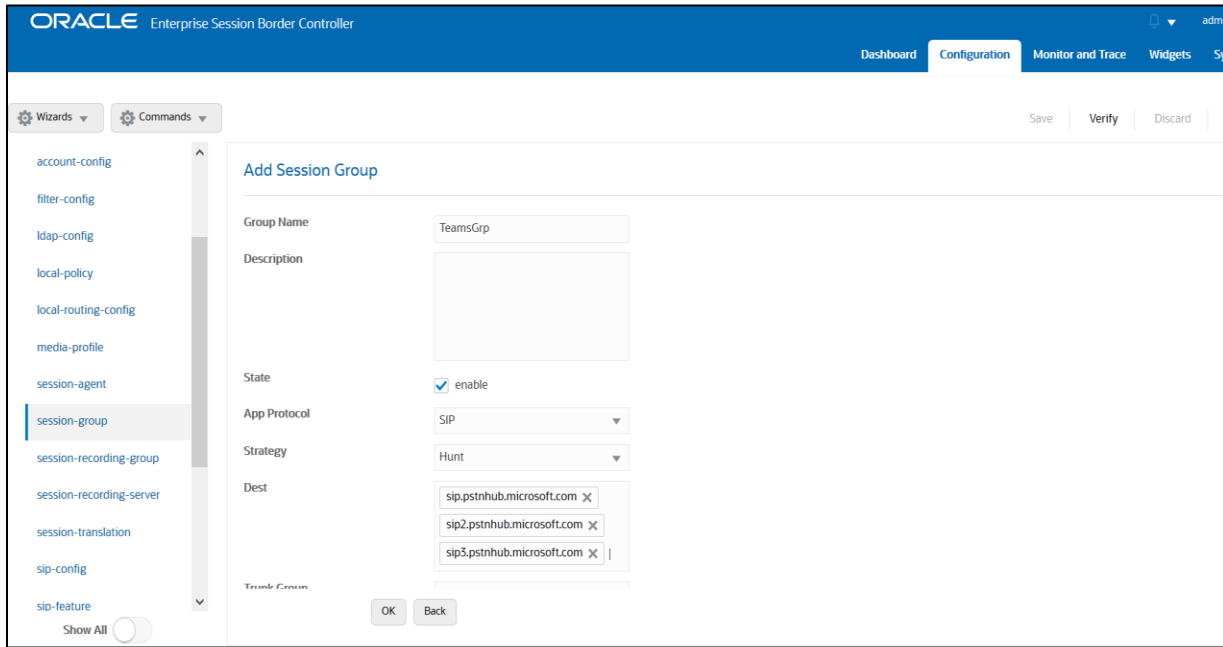
Hostname	10.232.50.70
IP Address	10.232.50.70
Port	5060 (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
App Protocol	SIP
App Type	
Transport Method	UDP+TCP
Realm ID	AvayaRealm
Egress Realm ID	
Description	

At the bottom of the form are 'OK' and 'Back' buttons. The top right of the form area has 'Save', 'Verify', and 'Discard' buttons, and a 'Show Configuration' button.

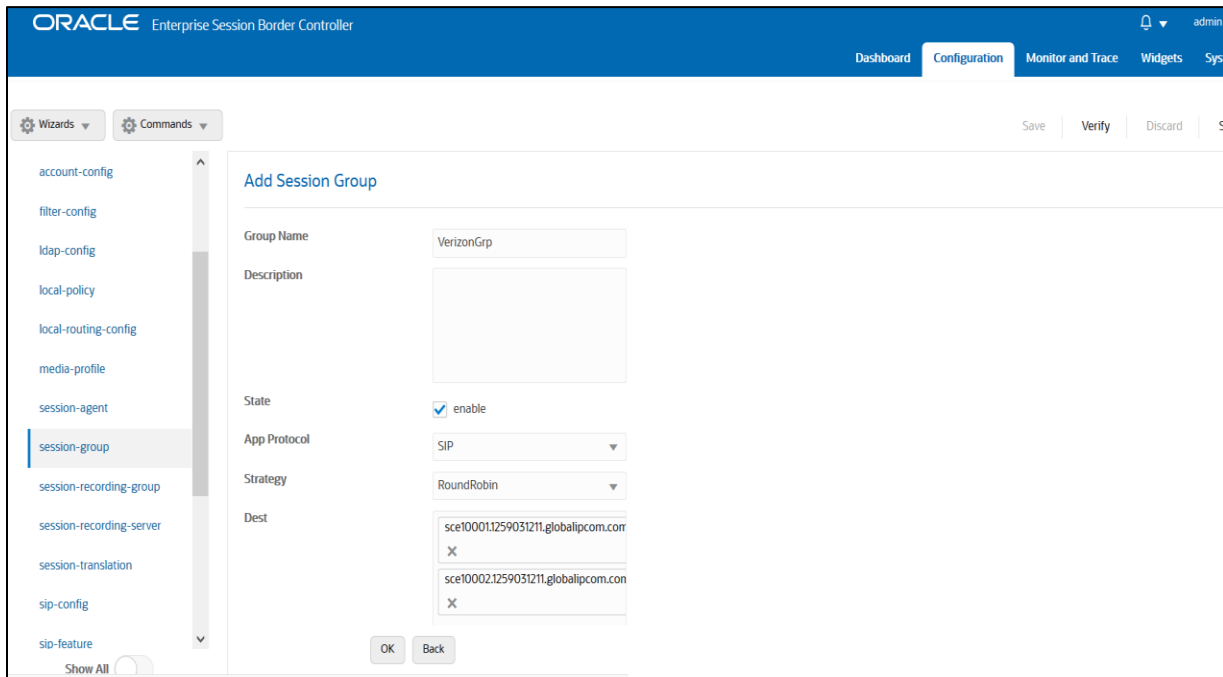
#### 8.14. Configure session-agent group

A session agent group allows the SBC to create a load balancing model. Go to Session-Router->Session-Group

Please configure the following group for Teams Session Agents



Please configure the following group for Verizon Session Agents

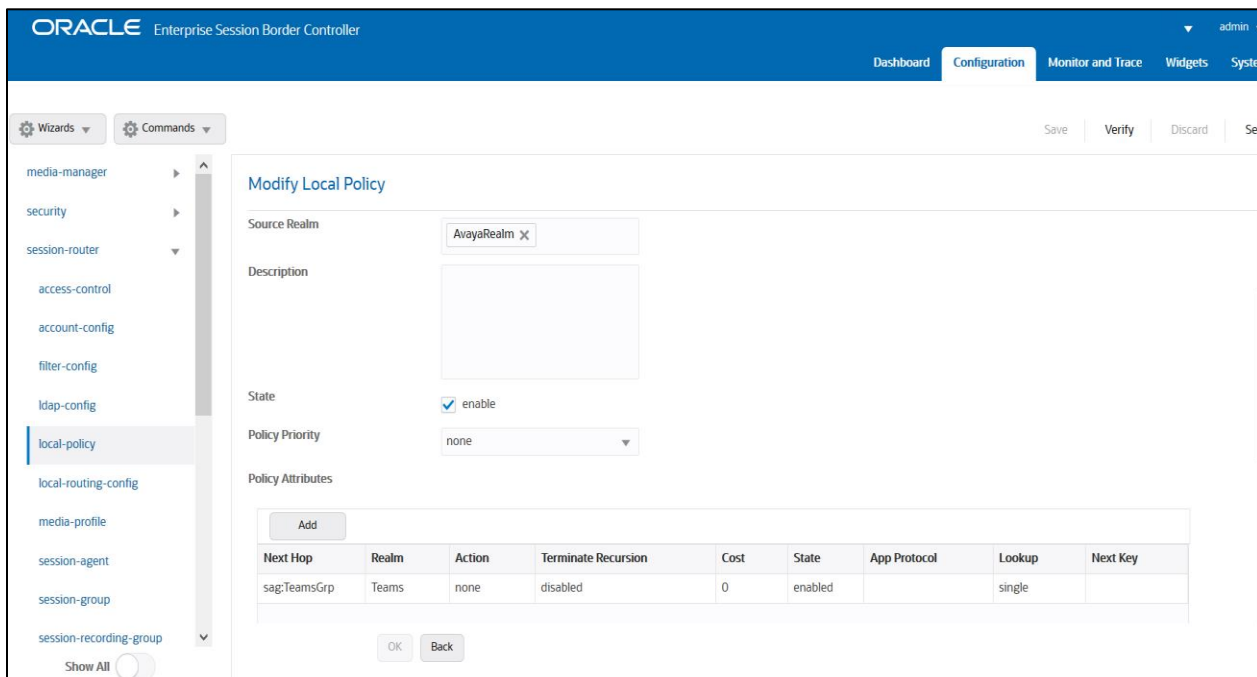
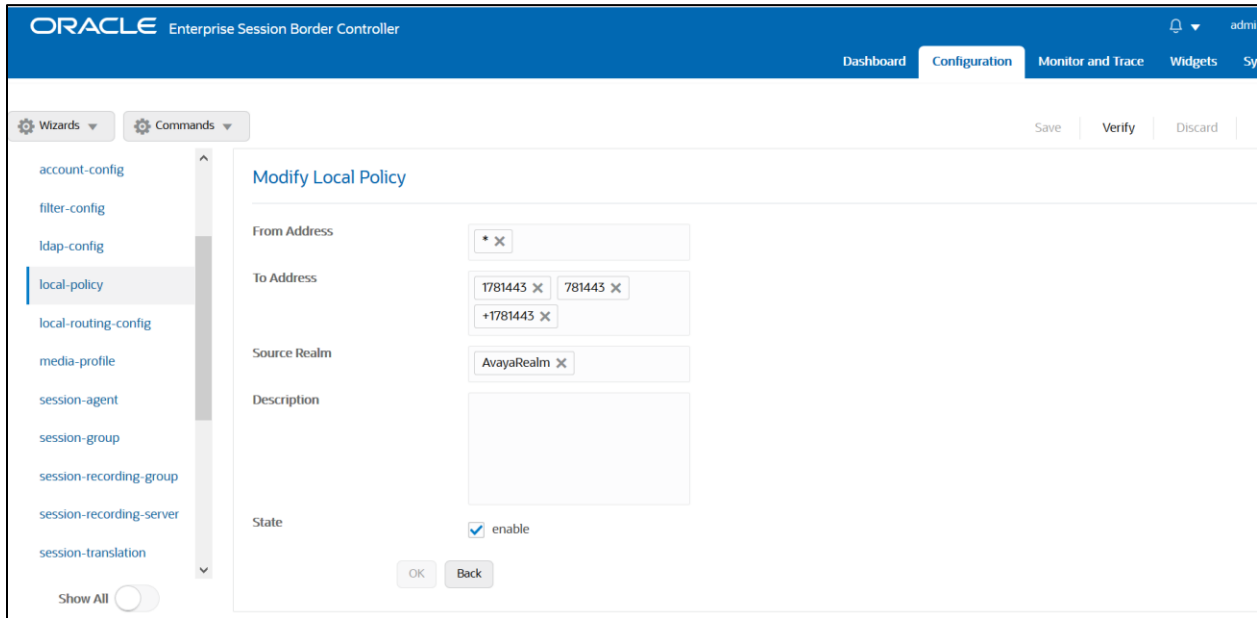


### 8.15. Configure local-policy

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.

We have the following three local policies to route the calls from Teams, Verizon and Avaya Realm respectively.

To route the calls from Avaya Realm to Teams, Use the below local –policy  
**This DID filter in TO address isolates the call to Teams instead of these calls going to Verizon.**



To route the calls from Avaya Realm to Verizon Trunk, Use the below local –policy

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Wizards Commands Save Verify Discard

media-manager security session-router access-control account-config filter-config ldap-config local-policy local-routing-config media-profile session-agent session-group session-recording-group Show All

### Modify Local Policy

From Address: \*

To Address: \*

Source Realm: AvayaRealm

Description:

State:  enable

Policy Priority: none

Policy Attributes:

OK Back

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Wizards Commands Save Verify Discard

media-manager security session-router access-control account-config filter-config ldap-config local-policy local-routing-config media-profile session-agent session-group session-recording-group Show All

### Modify Local Policy

State:  enable

Policy Priority: none

Policy Attributes:

Add

Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
sag:VerizonGrp	Verizon	replace-uri	disabled	0	enabled		single	

OK Back

To route the calls from either Teams or Verizon trunk to Avaya Realm, use the below local -policy  
**Please note that the next hop is ECB IP which is 10.232.50.70**



ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Wizards Commands Save Verify Discard See

media-manager security session-router access-control account-config filter-config ldap-config local-policy local-routing-config media-profile session-agent session-group session-recording-group Show All

### Modify Local Policy

From Address: \* X

To Address: \* X

Source Realm: Teams X Verizon X

Description:

State:  enable

Policy Priority: none

Policy Attributes:

OK Back

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets Sys

Wizards Commands Save Verify Discard

media-manager security session-router access-control account-config filter-config ldap-config local-policy local-routing-config media-profile session-agent session-group session-recording-group Show All

### Modify Local Policy

Source Realm: Teams X Verizon X

Description:

State:  enable

Policy Priority: none

Policy Attributes:

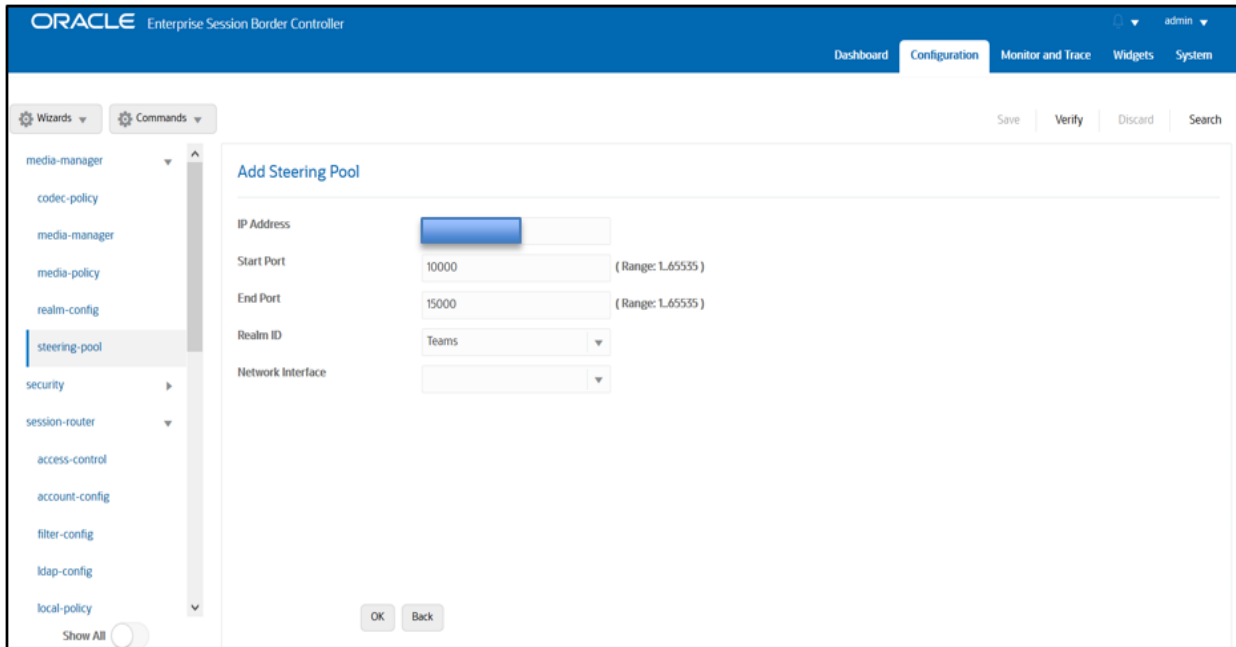
Add									
Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key	
10.232.50.70	AvayaRealm	none	disabled	0	enabled		single		

OK Back

## 8.16. Configure steering-pool

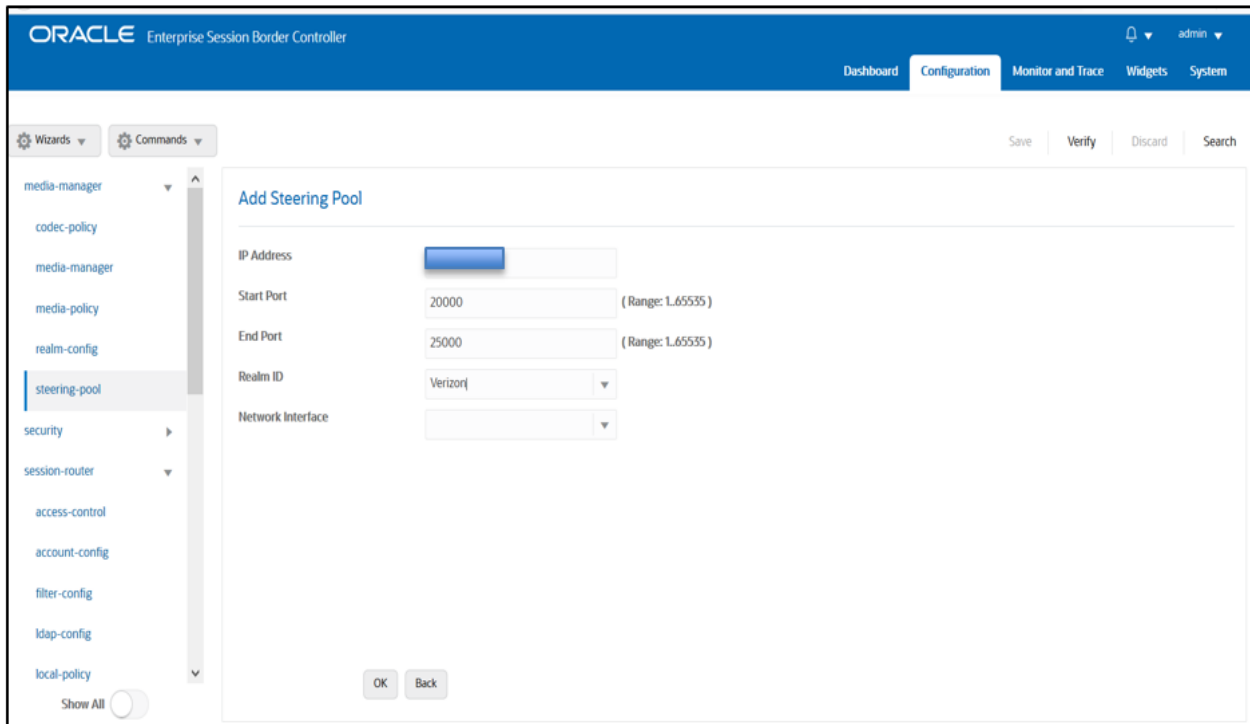
Steering-pool config allows configuration to assign IP address(es), ports & a realm.

Teams side steering pool.



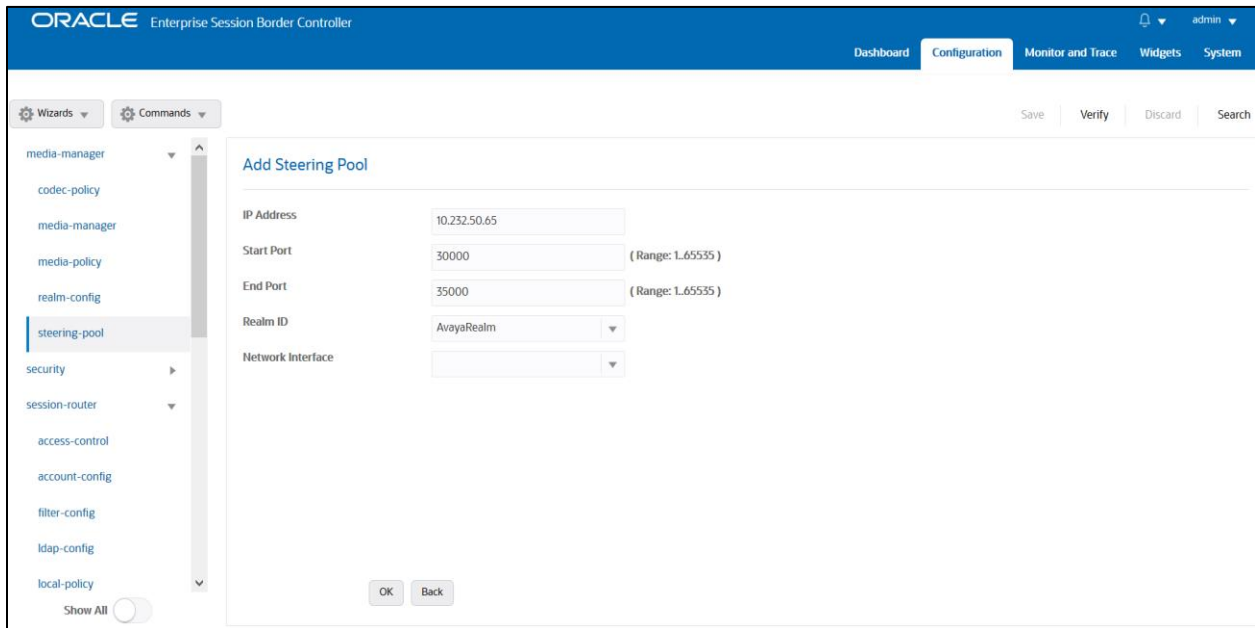
The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Add Steering Pool". The left sidebar contains a tree view with categories like "media-manager", "security", and "session-router". The "steering-pool" option is selected. The main form fields are: IP Address (empty), Start Port (10000, Range: 1.65535), End Port (15000, Range: 1.65535), Realm ID (Teams), and Network Interface (empty). Buttons for "Save", "Verify", "Discard", "Search", "OK", and "Back" are visible.

Verizon side steering pool.



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Add Steering Pool". The left sidebar contains a tree view with categories like "media-manager", "security", and "session-router". The "steering-pool" option is selected. The main form fields are: IP Address (empty), Start Port (20000, Range: 1.65535), End Port (25000, Range: 1.65535), Realm ID (Verizon), and Network Interface (empty). Buttons for "Save", "Verify", "Discard", "Search", "OK", and "Back" are visible.

Avaya side steering pool.



## 8.17. Configure sip-manipulation

To simplify the ORACLE SBC sip manipulation, from 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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Modify Realm Config' page is active, showing the following fields:

- Identifier: Teams
- Description: Realm Facing Teams Direct Routing
- Addr Prefix: 0.0.0.0
- Network Interfaces: M00:0.4
- Media Realm List: (empty)
- Mm In Realm:  enable
- Mm In Network:  enable
- Mm Same Ip:  enable

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

This screenshot shows the 'Modify Realm Config' page with additional configuration options. Two red arrows point to the 'Teams Fqdn In Uri' and 'SDP Inactive Only' fields, both of which are checked and set to 'enable'.

- Media Policy: (empty dropdown)
- Media Sec Policy: sdesPolicy
- RTCP Mux:  enable
- Ice Profile: ice
- Teams Fqdn: customers.telechat.o-test06161977.cor
- Teams Fqdn In Uri:  enable
- SDP Inactive Only:  enable
- DTLS SrtP Profile: (empty dropdown)
- SrtP Msm Passthrough:  enable
- Class Profile: (empty dropdown)
- In Translationid: (empty dropdown)

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

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 Enterprise Session Border Controller configuration interface. The 'session-agent' configuration element is selected in the left-hand menu. The main configuration 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:  enable
- App Protocol: SIP
- App Type: (empty)
- Transport Method: StaticTLS
- Realm ID: Teams
- Egress Realm ID: (empty)
- Description: (empty)

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

This screenshot shows the same 'Modify Session Agent' configuration page, but with the 'Ping Response' field highlighted by a red arrow. The configuration fields are:

- Out Translationid: (empty)
- Trust Me:  enable
- Local Response Map: (empty)
- Ping Response:  enable
- In Manipulationid: (empty)
- Out Manipulationid: (empty)
- Manipulation String: (empty)
- Manipulation Pattern: (empty)
- Trunk Group: (empty)
- Max Register Sustain Rate: 0 (Range: 0..999999999)

The 'OK' and 'Back' buttons are also present at the bottom.

Similarly, create one more sip-manipulation remove attribute to remove certain parameters from Requests going towards Avaya realm. Please check the sip-manipulation created as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active. The left sidebar shows the 'sip-manipulation' menu item selected. The main area is titled 'Modify SIP Manipulation' and contains the following fields:

- Name:** RemoveAttribute
- Description:** (Empty text area)
- Split Headers:** (Empty text input)
- Join Headers:** (Empty text input)
- CfgRules:** A table with one entry:
 

Name	Element Type
RemoveXAttribute	mime-sdp-rule

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active. The left sidebar shows the 'sip-manipulation' menu item selected. The main area is titled 'Modify SIP Manipulation' and shows a list of rules under the 'CfgRules' section:

- Split Headers:** (Empty text input)
- Join Headers:** (Empty text input)
- CfgRules:** A table with 6 entries:
 

Name	Element Type
RemoveXAttribute	mime-sdp-rule
AcmeNATFrom	header-rule
AcmeNatTo	header-rule
RemovePrivacy	header-rule
DeletePAI	header-rule
DeletePAIO	header-rule

Buttons for 'OK' and 'Back' are visible at the bottom. A pagination indicator shows 'Displaying 1 - 6 of 6'.

Now, we can see each rule of the sip-manipulation in detail as given below.  
 We will start with RemoveXAttribute mime-SDP-rule

The screenshot shows the configuration page for a SIP manipulation rule. The left sidebar lists various configuration categories, with 'sip-manipulation' selected. The main area is titled 'Modify Sip manipulation / mime SDP rule'. The configuration fields are as follows:

- Name: RemoveXAttribute
- Msg Type: request
- Methods: Invite
- Action: manipulate
- Comparison Type: case-sensitive
- Match Value: (empty)
- New Value: (empty)

Below the fields is a table for 'CfgRules' with one entry:

Action	Select	Name	Element Type
:	<input type="checkbox"/>	RemoveX	sdp-media-rule

The screenshot shows the configuration page for an SDP media rule. The left sidebar is the same as the previous screenshot. The main area is titled 'Modify Sip manipulation / mime SDP rule / SDP media rule'. The configuration fields are as follows:

- Name: RemoveX
- Media Type: audio
- Action: manipulate
- Comparison Type: case-sensitive
- Match Value: (empty)
- New Value: (empty)

Below the fields is a table for 'CfgRules' with one entry:

Action	Select	Name	Element Type
:	<input type="checkbox"/>	RemoveA	sdp-line-rule

Configuration View Configuration Q Discard Verify

local-policy  
local-routing-config  
media-profile  
session-agent  
session-group  
session-recording-group  
session-recording-server  
session-translation  
sip-config  
sip-feature  
sip-interface  
sip-manipulation  
sip-monitoring

Show All

Modify Sip manipulation / mime SDP rule / SDP media rule / SDP line rule

Name: RemoveA  
Type: a  
Action: delete  
Comparison Type: pattern-rule  
Match Value: x-candidate-info  
New Value:

OK Back

We will now check the next AcmeNATFrom header rule.

Configuration View Configuration Q Discard Verify

local-policy  
local-routing-config  
media-profile  
session-agent  
session-group  
session-recording-group  
session-recording-server  
session-translation  
sip-config  
sip-feature  
sip-interface  
sip-manipulation  
sip-monitoring  
translation-rules  
system

Show All

Modify Sip manipulation / header rule

Name: AcmeNATFrom  
Header Name: From  
Action: manipulate  
Comparison Type: case-sensitive  
Msg Type: request  
Methods: Invite X  
Match Value:  
New Value:

CfgRules

Add

Action	Select	Name	Element Type
:	<input type="checkbox"/>	FromHost	element-rule
:	<input type="checkbox"/>	FromPort	element-rule

OK Back



Configuration View Configuration Q Discard Verify

- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config
- sip-feature
- sip-interface
- sip-manipulation**
- sip-monitoring
- translation-rules
- system

Show All

### Modify Sip manipulation / header rule / element rule

Name:

Parameter Name:

Type:

Action:

Match Val Type:

Comparison Type:

Match Value:

New Value:

Configuration View Configuration Q Discard Verify

- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config
- sip-feature
- sip-interface
- sip-manipulation**
- sip-monitoring
- translation-rules
- system

Show All

### Modify Sip manipulation / header rule / element rule

Name:

Parameter Name:

Type:

Action:

Match Val Type:

Comparison Type:

Match Value:

New Value:

We will now check the next AcmeNatTo header rule.

The screenshot shows a configuration page titled "Modify Sip manipulation / header rule". The left sidebar lists various configuration categories, with "sip-manipulation" selected. The main area contains the following fields:

- Name: AcmeNatTo
- Header Name: To
- Action: manipulate
- Comparison Type: case-sensitive
- Msg Type: request
- Methods: Invite X
- Match Value: (empty)
- New Value: (empty)

Below these fields is a "CIGRules" section with a table:

Action	Select	Name	Element Type
:	<input type="checkbox"/>	ToHost	element-rule
:	<input type="checkbox"/>	ToPort	element-rule

At the bottom of the page are "OK" and "Back" buttons.

The screenshot shows a configuration page titled "Modify Sip manipulation / header rule / element rule". The left sidebar is the same as in the previous screenshot, with "sip-manipulation" selected. The main area contains the following fields:

- Name: ToHost
- Parameter Name: (empty)
- Type: uri-host
- Action: replace
- Match Val Type: any
- Comparison Type: case-sensitive
- Match Value: (empty)
- New Value: \$REMOTE\_IP

At the bottom of the page are "OK" and "Back" buttons.

Configuration View Configuration Q Discard Verify

local-policy  
local-routing-config  
media-profile  
session-agent  
session-group  
session-recording-group  
session-recording-server  
session-translation  
sip-config  
sip-feature  
sip-interface  
sip-manipulation  
sip-monitoring  
translation-rules  
system

Show All

### Modify Sip manipulation / header rule / element rule

Name: ToPort

Parameter Name:

Type: uri-port

Action: replace

Match Val Type: any

Comparison Type: case-sensitive

Match Value:

New Value: \$REMOTE\_PORT

We will check the RemovePrivacy header rule.

Configuration View Configuration Q Discard Verify

local-policy  
local-routing-config  
media-profile  
session-agent  
session-group  
session-recording-group  
session-recording-server  
session-translation  
sip-config  
sip-feature  
sip-interface

Show All

### Modify Sip manipulation / header rule

Name: RemovePrivacy

Header Name: Privacy

Action: delete

Comparison Type: case-sensitive

Msg Type: request

Methods: Invite X

Match Value:

New Value:

CfgRules

We will check the DeletePAI header rule as below.

The screenshot shows a configuration page titled "Modify Sip manipulation / header rule". On the left is a navigation menu with categories like "local-policy", "local-routing-config", "media-profile", "session-agent", "session-group", "session-recording-group", "session-recording-server", "session-translation", "sip-config", "sip-feature", and "sip-interface". A "Show All" toggle is at the bottom of the menu. The main area contains the following fields:

Name	DeletePAI
Header Name	P-Asserted-Identity[1]
Action	delete
Comparison Type	case-sensitive
Msg Type	request
Methods	INVITE X
Match Value	
New Value	
CfgRules	

At the bottom of the main area are "OK" and "Back" buttons. The top right of the page has "Discard" and "Verify" buttons.

We will check the DeletePAI0 header rule as below.

The screenshot shows a configuration page titled "Modify Sip manipulation / header rule". On the left is a navigation menu with categories like "local-policy", "local-routing-config", "media-profile", "session-agent", "session-group", "session-recording-group", "session-recording-server", "session-translation", "sip-config", "sip-feature", and "sip-interface". A "Show All" toggle is at the bottom of the menu. The main area contains the following fields:

Name	DeletePAI0
Header Name	P-Asserted-Identity[0]
Action	delete
Comparison Type	case-sensitive
Msg Type	request
Methods	INVITE X
Match Value	
New Value	
CfgRules	

At the bottom of the main area are "OK" and "Back" buttons. The top right of the page has "Discard" and "Verify" buttons.

Please assign this sip-manipulation to the Avaya Realm sip-interface as shown below:

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Wizards Commands Save Verify Discard

local-policy local-routing-config media-profile session-agent session-group session-recording-group session-recording-server session-translation sip-config sip-feature sip-interface sip-manipulation sip-monitoring Show All

### Modify SIP Interface

Show Configuration

State  enable

Realm ID AvayaRealm

Description

SIP Ports

Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
10.232.50.65	5060	TCP		agents-only	
10.232.50.65	5060	UDP		agents-only	

OK Back

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Wizards Commands Save Verify Discard

local-policy local-routing-config media-profile session-agent session-group session-recording-group session-recording-server session-translation sip-config sip-feature sip-interface sip-manipulation sip-monitoring Show All

### Modify SIP Interface

Show Configuration

Trust Mode all

Max Nat Interval 3600 (Range: 0..4294967295)

Stop Recurse 401,407

Port Map Start 0 (Range: 0,1025..65535)

Port Map End 0 (Range: 0,1025..65535)

In Manipulationid

Out Manipulationid RemoveAttribute

SIP Atcf Feature  enable

Rfc2833 Payload 101 (Range: 96..127)

Rfc2833 Mode transparent

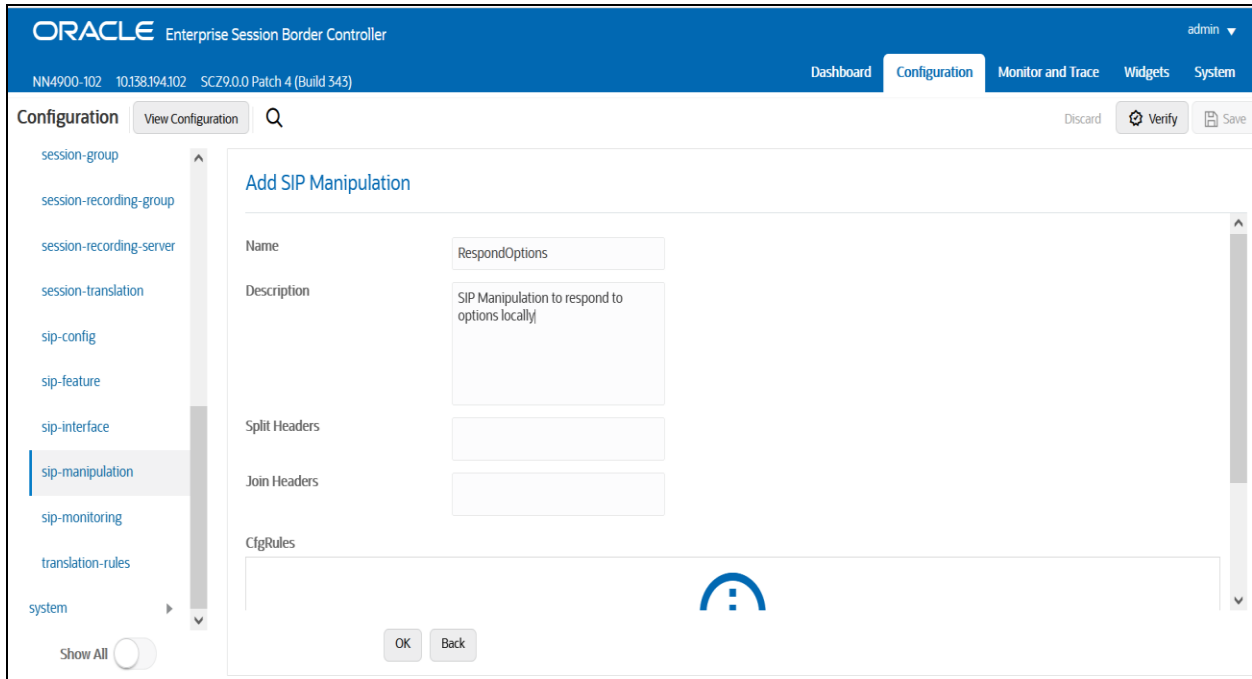
Response Map

OK Back

## 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:

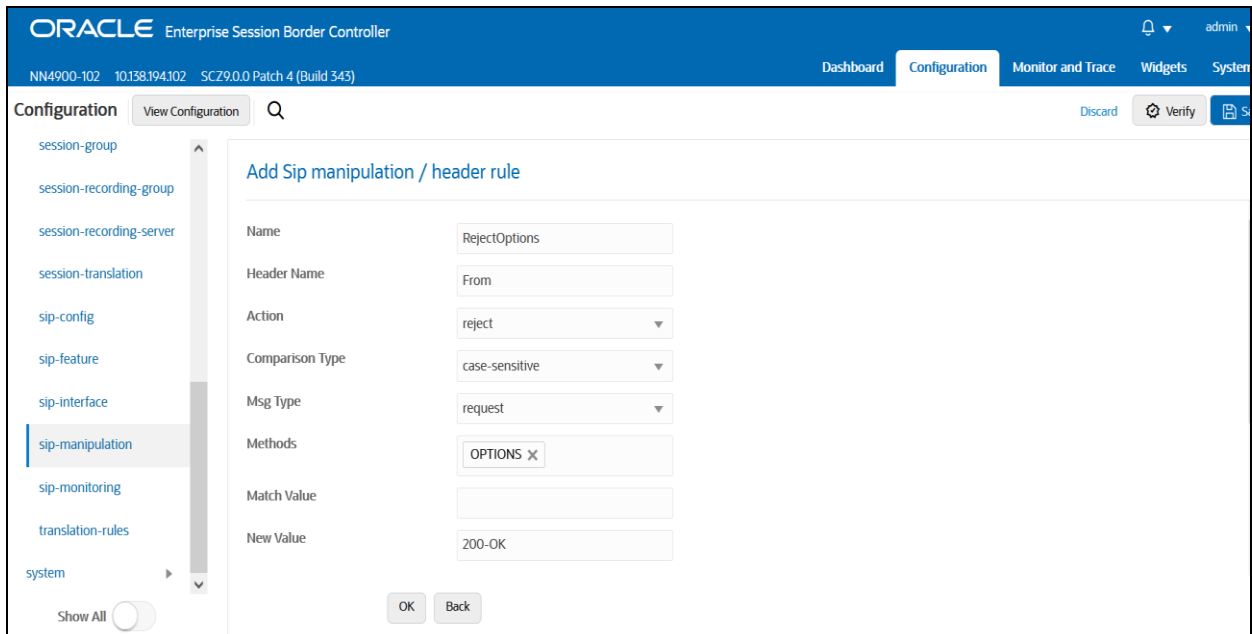


The screenshot shows the Oracle Enterprise Session Border Controller GUI. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a sidebar lists various configuration categories, with 'sip-manipulation' selected. The main 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 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. With this sip-manipulation is complete.

## 8.18. 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 shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active, and the 'media-profile' option is selected in the left-hand navigation menu. The main area displays the 'Modify Media Profile' form with the following fields and values:

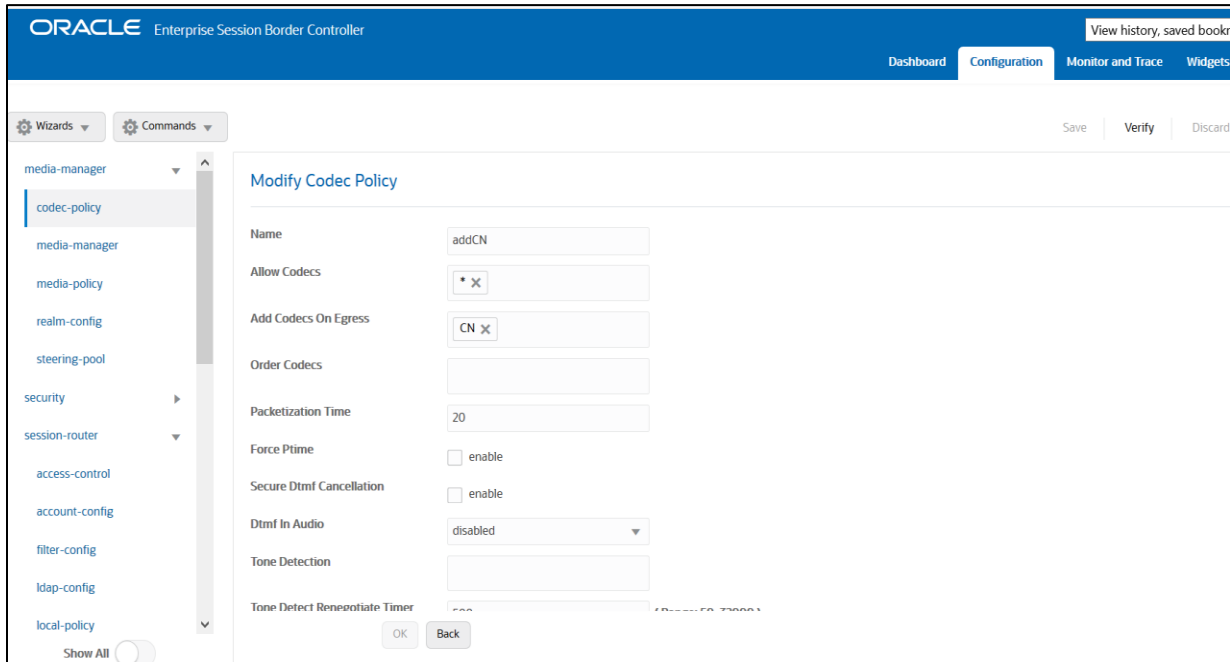
- Name: CN
- Subname: wideband
- Media Type: audio
- Payload Type: 118
- Transport: RTP/AVP
- Clock Rate: 16000 (Range: 0..4294967295)
- Req Bandwidth: 0 (Range: 0..999999999)
- Frames Per Packet: 0 (Range: 0..256)
- Parameters: (empty field)
- As Bandwidth: 0 (Range: 0..4294967295)

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

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. Go to media manager ---- codec policy

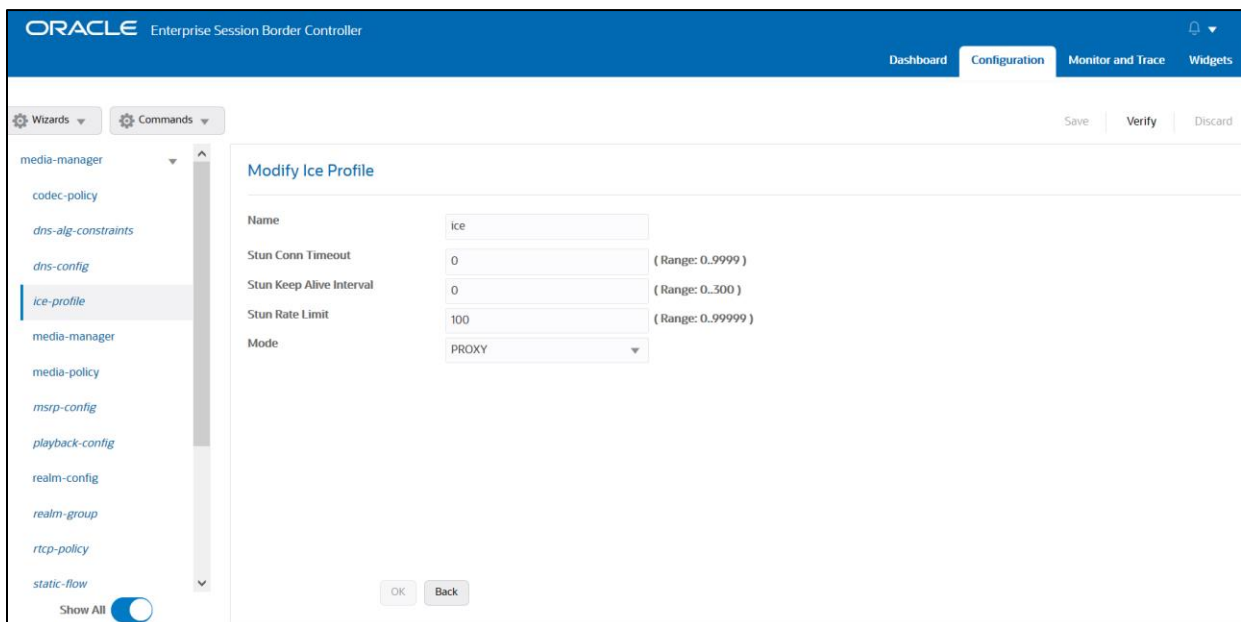


Apply this codec policy on the Teams realm

### 8.19. 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. **Note: This config is required only for Media bypass model and its not needed for Non media bypass model.**





## 8.20. Configure sdes profile

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'media-security' expanded and 'sdes-profile' selected. The main content area is titled 'Add Sdes Profile' and contains the following fields:

- Name: SDES
- Crypto List: AES\_CM\_128\_HMAC\_SHA1\_80, AES\_CM\_128\_HMAC\_SHA1\_32
- Srtp Auth:  enable
- Srtp Encrypt:  enable
- SrTCP Encrypt:  enable
- Mki:  enable
- Egress Offer Format: same-as-ingress
- Use Ingress Session Params: (empty)

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

## 8.21. Configure Media Security Profile

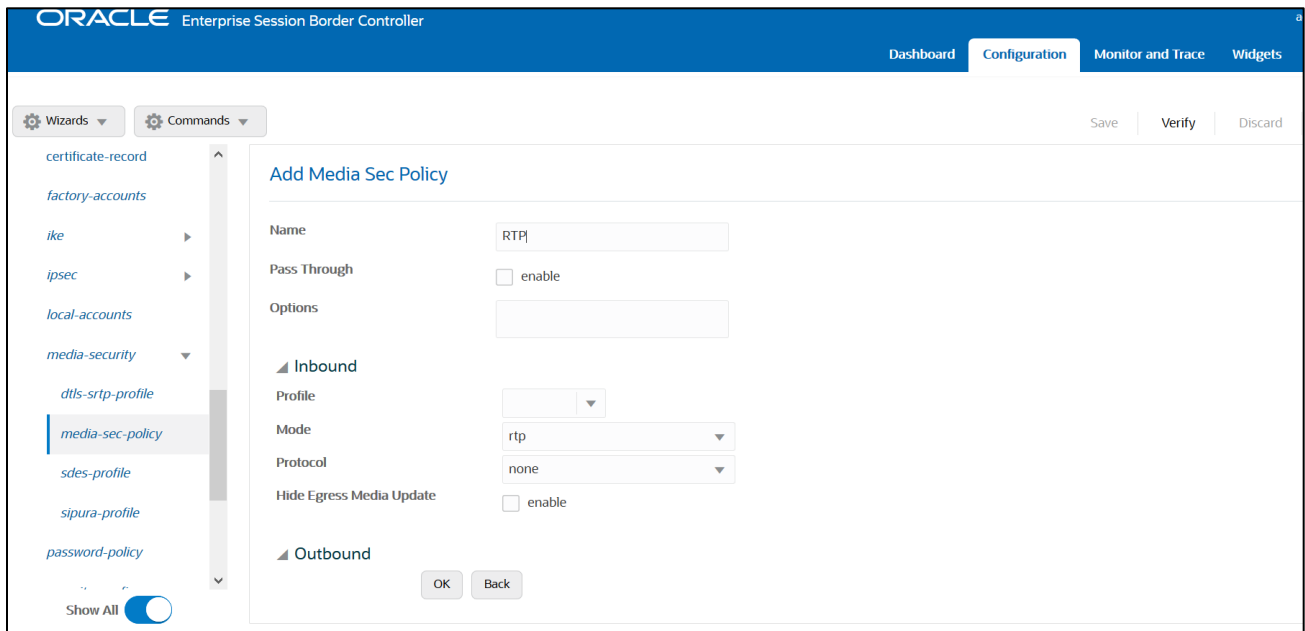
Please go to →Security → Media Security →media Sec policy and create the policy as below:  
Create Media Sec policy with name SDES for the Teams Public Side which will have the sdes profile created above. Assign this media policy to the Teams Realm.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'media-security' expanded and 'media-sec-policy' selected. The main content area is titled 'Add Media Sec Policy' and contains the following fields:

- Name: SDES
- Pass Through:  enable
- Options: (empty)
- Inbound**
  - Profile: SDES
  - Mode: srtp
  - Protocol: sdes
  - Hide Egress Media Update:  enable
- Outbound**

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

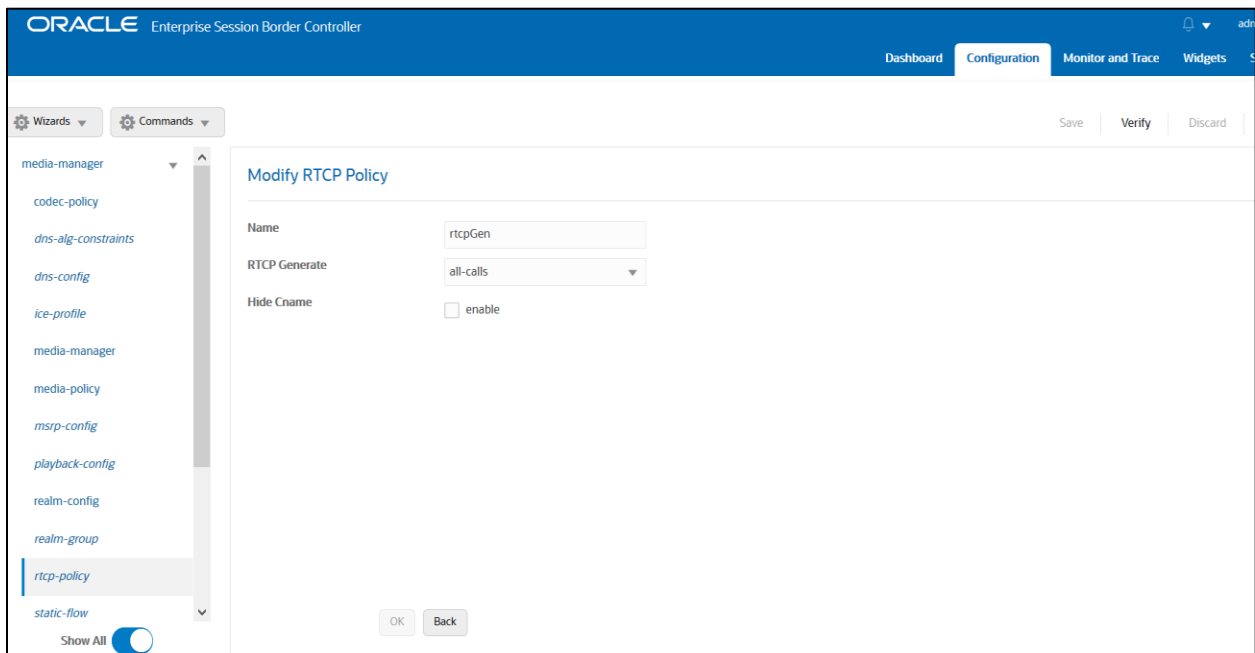
Similarly, Create Media Sec policy with name RTP to convert srtp to rtp for the Avaya side and Verizon side which will use only TCP/UDP as transport protocol. Assign this media policy to the Verizon Realm and Avaya Realm.



## 8.22. Configure RTCP Policy and RTCP Mux

The RTCP policy needs to be configured in order to generate RTCP reports towards Teams

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



Apply this RTCP policy on the Teams realm. Enable rtcp-mux also in the realm.

## 8.23. QoS Marking

QoS marking allows you to apply a set of TOS/DiffServ mechanisms that enable you to provide better service for selected networks. Add this policy to Verizon Realm media policy.

Go to media manager/media policy

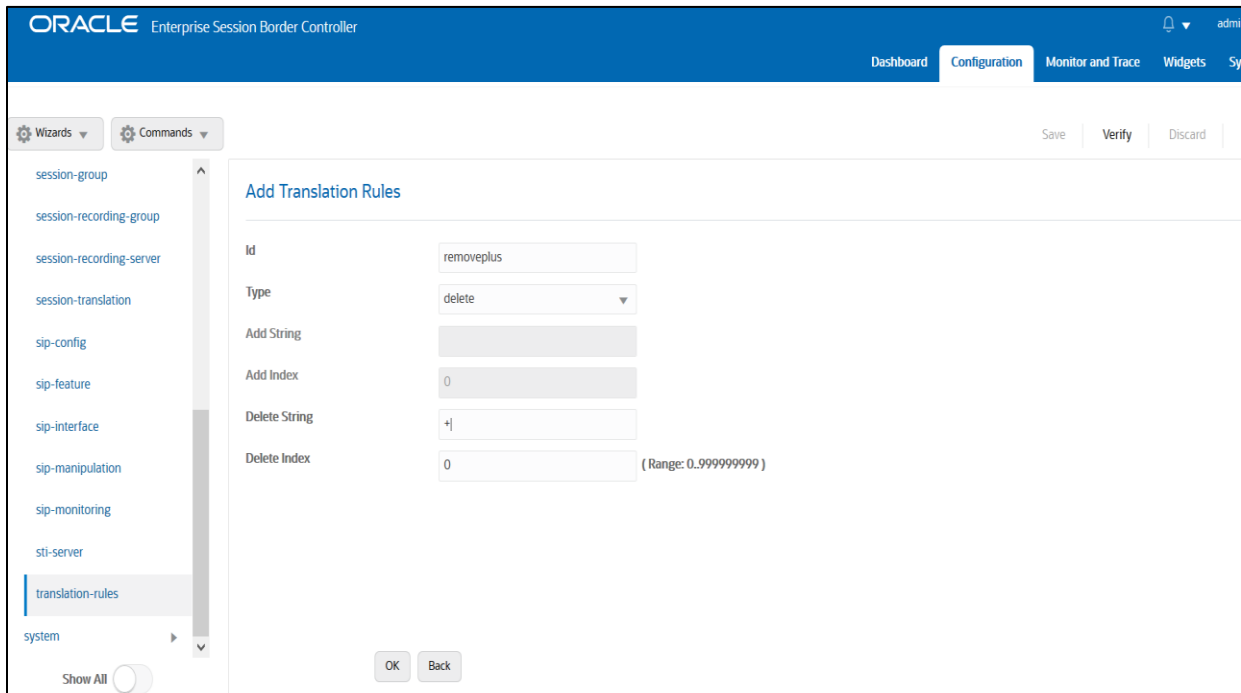
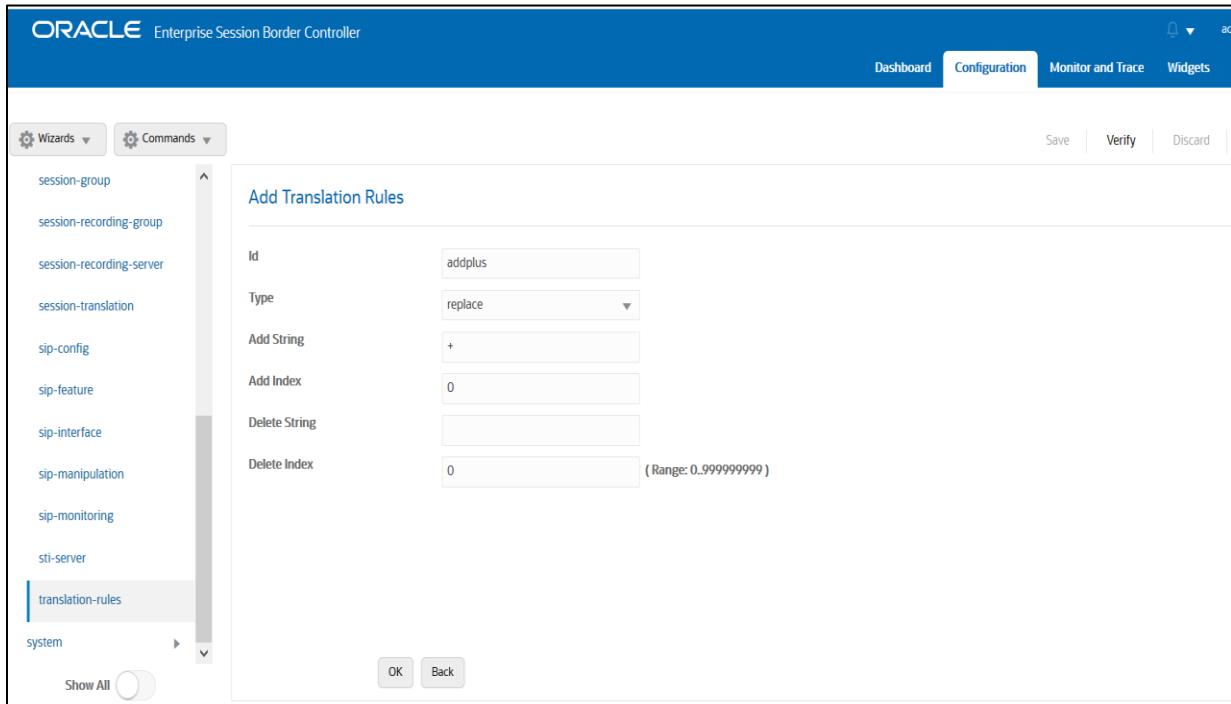
The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The main title is 'Modify Media Policy'. The 'Name' field is set to 'VerizonQOS'. Under 'Tos Settings', there is an 'Add' button and a table with the following data:

Media Type	Media Sub Type	Tos Value	Media Attributes
audio		0xb8	
message	sip	0xb8	

At the bottom of the table, there are 'OK' and 'Back' buttons. The left sidebar shows a navigation menu with 'media-policy' selected. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'.

## 8.24. Configure Translation Rules

The translation rules sub-element is where the actual translation rules are created. Go to Session router → translation-rules and create the below rule.



## 8.25. Configure Session Translation Rules

A session translation defines how translation rules are applied to calling and called numbers. Go to Session Router → session-translation and configure the below translation rules.

Add the below translation rule to Avaya realm side as Avaya rejects call with + sign

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'session-translation' selected. The main area is titled 'Add Session Translation' and contains the following fields:

Id	toAvaya
Rules Calling	removeplus ✕
Rules Called	removeplus ✕
Rules Asserted Id	
Rules Redirect	
Rules Isup Cdpn	
Rules Isup Cgpn	
Rules Isup Gn	
Rules Isup Rdn	

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

Add the below translation rule to Verizon realm side as PSTN expects call with + sign.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'session-translation' selected. The main area is titled 'Add Session Translation' and contains the following fields:

Id	toPSTN
Rules Calling	addPlus ✕
Rules Called	addPlus ✕
Rules Asserted Id	
Rules Redirect	
Rules Isup Cdpn	
Rules Isup Cgpn	
Rules Isup Gn	
Rules Isup Rdn	

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

Please add the above session translation rules to Avaya realm as shown below

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

media-manager  
codec-policy  
media-manager  
media-policy  
realm-config  
steering-pool  
security  
session-router  
system

### Modify Realm Config

Identifier: AvayaRealm

Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M10:0

Media Realm List:

Mm In Realm:  enable

Mm In Network:  enable

Mm Same Ip:  enable

OK Back

Show All

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

media-manager  
codec-policy  
media-manager  
media-policy  
realm-config  
steering-pool  
security  
session-router  
system

### Modify Realm Config

Teams Fqdn In Uri:  enable

SDP Inactive Only:  enable

DTLS Srtp Profile:

Srtp Msm Passthrough:  enable

Class Profile:

In Translationid: toPSTN

Out Translationid: toAvaya

In Manipulationid:

Out Manipulationid:

Average Rate Limit: 0 (Range: 0..4294967295)

Access Control Trust Level: high

OK Back

Show All

With this, SBC configuration is complete



## 9.SIP Access Controls

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

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

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

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

1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high
2. Set the access control trust level on public facing [realms](#) to HIGH

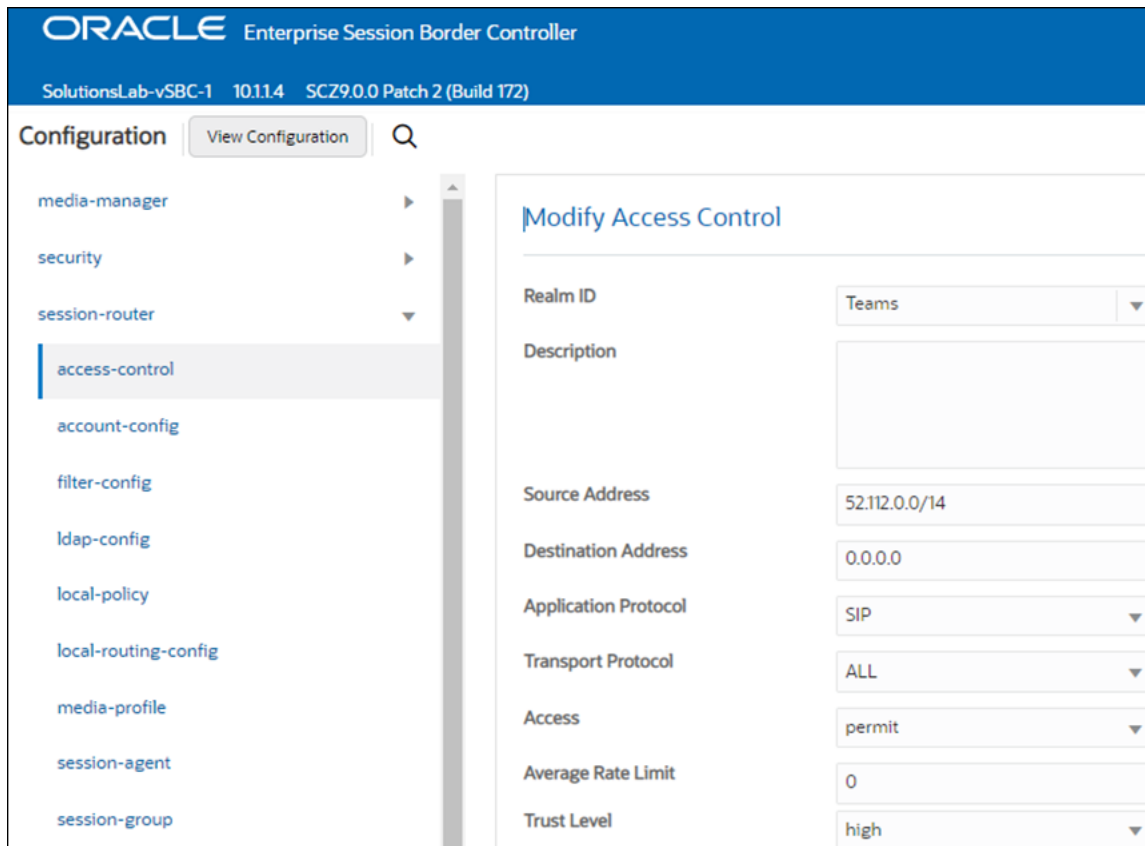
Microsoft Teams has two subnets, 52.112.0.0/14 and 52.120.0.0/14 that must be allowed to send traffic to the SBC. Both must be configured as an access control on the Oracle SBC and associated with the realm facing Teams.

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

GUI Path: session-router/access-control

ACLI Path: config 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.

## 10. Existing SBC configuration

If the SBC being used is an existing SBC with functional configuration, following configuration elements are required:

- [New realm-config](#)
- [Configuring a certificate for SBC Interface](#)
- [TLS-Profile](#)
- [IKE/IPSEC Config](#)
- [New sip-interface](#)
- [New session-agent](#)
- [New session-agent group](#)
- [New steering-pools](#)
- [New local-policy](#)
- [New sip-manipulation](#)
- [New media-profile and codec-policy](#)
- [ICE profile](#)
- [SDES Profile](#)
- [Media-sec-Policy](#)
- [RTCP Policy and RTP Mux](#)
- [QOS Marking](#)



- [New Translation Rules](#)
- [New Session Translation Rules](#)

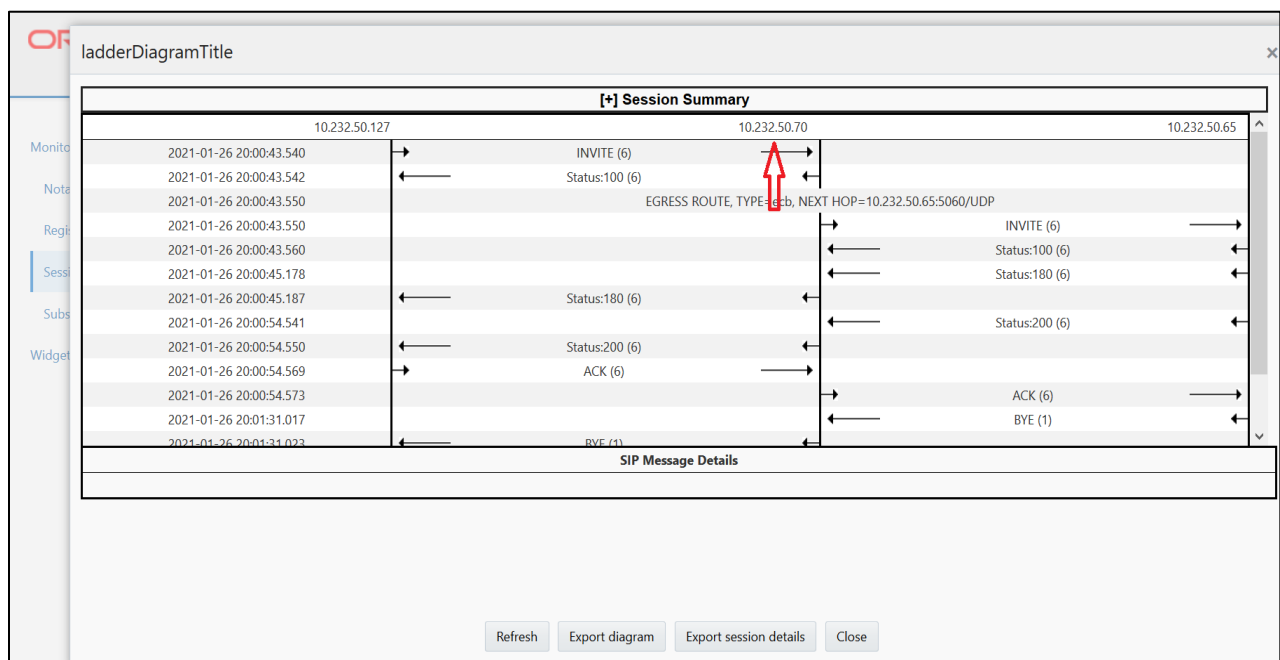
Please follow the steps mentioned in the above chapters to configure these elements.

## 10. Verification of Sample Call flows

Once the configuration is complete, we can try making sample calls and can check the signaling path and the call trace details as below:

1. Make Call from Avaya User to Teams user and check the call flow.

The Call from Avaya Session manager reaches ECB IP and then routed to SBC and to Teams.



ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Sessions

Registrations

Subscriptions

Notable Events

Session List 00B0E040-C45E-EB11-93D1-C33A12C2F333@10.232.50.2

[+] Session Summary

10.232.50.70	10.232.50.65	52.114.148.0
2021-01-26 23:14:34.307	→ INVITE (6)	→
2021-01-26 23:14:34.307	← Status:100 (6)	←
2021-01-26 23:14:34.309	MEDIA FLOW ADD, ID=16777217, DIRECTION=CALLING	
2021-01-26 23:14:34.309	MEDIA FLOW ADD, ID=16777218, DIRECTION=CALLED	
2021-01-26 23:14:34.310	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:+17814437247@sip.pstnhub.microsoft.com:5061;transport=tls>	
2021-01-26 23:14:34.310		→ INVITE (6)
2021-01-26 23:14:34.429		← Status:100 (6)
2021-01-26 23:14:35.921		← Status:180 (6)
2021-01-26 23:14:35.921	← Status:180 (6)	←
2021-01-26 23:14:45.279		← Status:200 (6)
2021-01-26 23:14:45.282	MEDIA FLOW MODIFY, ID=16777218, DIRECTION=CALLED	
2021-01-26 23:14:45.282	MEDIA FLOW MODIFY, ID=16777217, DIRECTION=CALLING	
2021-01-26 23:14:45.282	← Status:200 (6)	←
2021-01-26 23:14:45.329	→ ACK (6)	→
2021-01-26 23:14:45.407		→ ACK (6)
2021-01-26 23:15:21.763		← BYE (1)
2021-01-26 23:15:21.763	← BYE (1)	←

Refresh Export diagram Export session details

2. Make Call from Teams user to Avaya User and check the call flow.  
The Call from Teams reaches SBC and then to ECB and then routed to Avaya User as below.

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Sessions

Registrations

Subscriptions

Notable Events

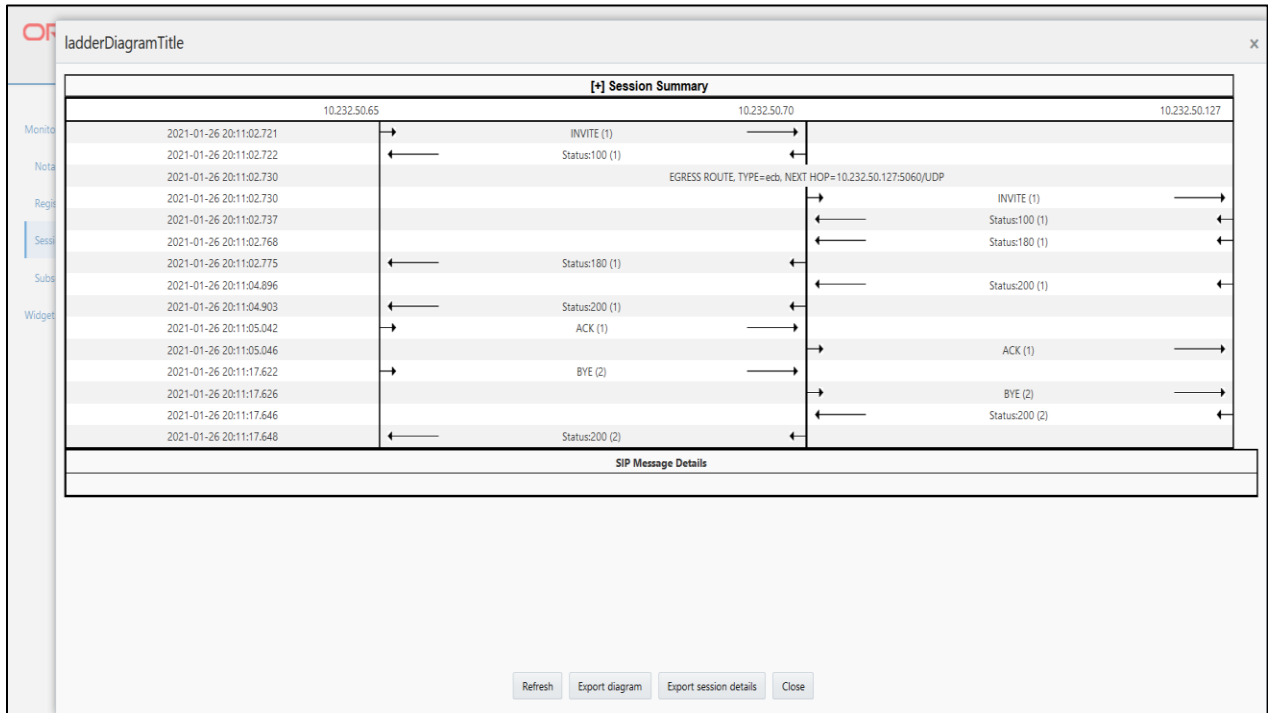
Session List 224051f1b9f55c91ca4ea3c99a8ce

[+] Session Summary

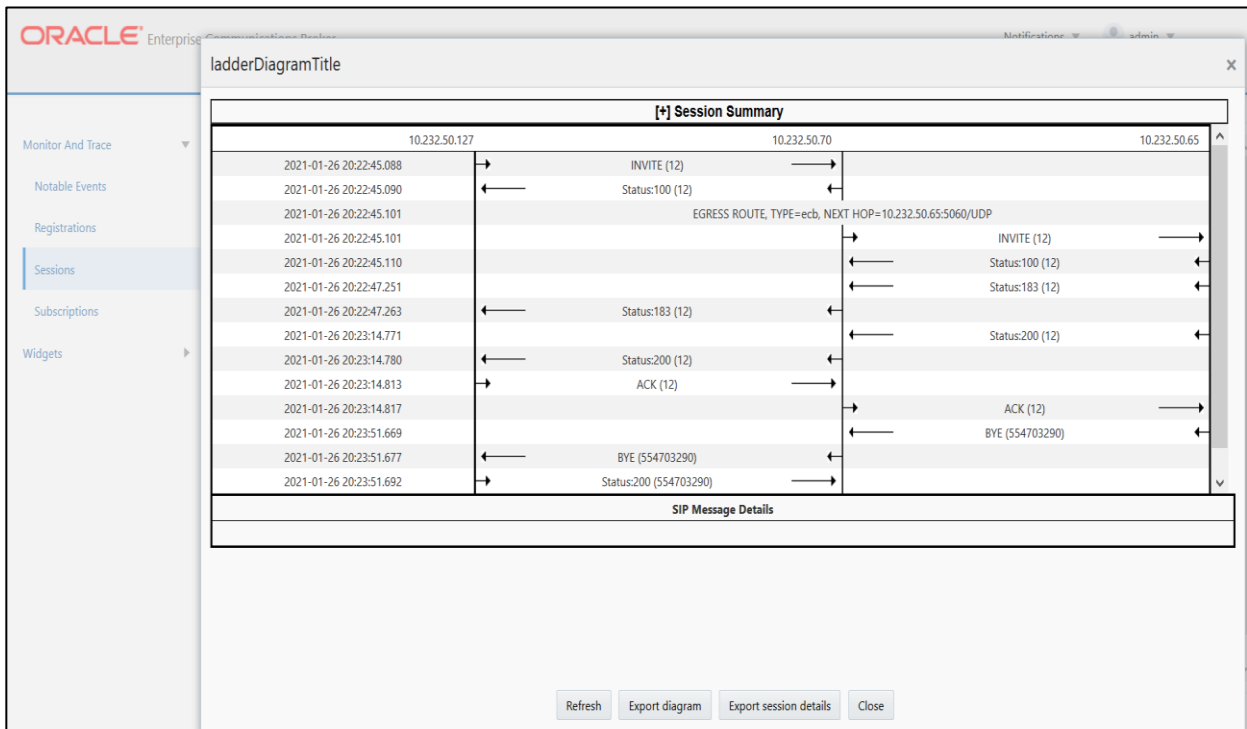
52.114.148.0	10.232.50.65	10.232.50.70
2021-01-26 23:24:53.526	→ INVITE (1)	→
2021-01-26 23:24:53.526	← Status:100 (1)	←
2021-01-26 23:24:53.529	MEDIA FLOW ADD, ID=33554433, DIRECTION=CALLING	
2021-01-26 23:24:53.529	MEDIA FLOW ADD, ID=33554434, DIRECTION=CALLED	
2021-01-26 23:24:53.529	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:+17813131034@10.232.50.70:5060;user=phone>	
2021-01-26 23:24:53.529		→ INVITE (1)
2021-01-26 23:24:53.539		← Status:100 (1)
2021-01-26 23:24:53.594		← Status:180 (1)
2021-01-26 23:24:53.594	← Status:180 (1)	←
2021-01-26 23:24:55.724		← Status:200 (1)
2021-01-26 23:24:55.726	MEDIA FLOW MODIFY, ID=33554434, DIRECTION=CALLED	
2021-01-26 23:24:55.726	MEDIA FLOW MODIFY, ID=33554433, DIRECTION=CALLING	
2021-01-26 23:24:55.726	← Status:200 (1)	←
2021-01-26 23:24:55.852	→ ACK (1)	→
2021-01-26 23:24:55.852		→ ACK (1)
2021-01-26 23:25:08.433	→ BYE (2)	→
2021-01-26 23:25:08.433		→ BYE (2)
2021-01-26 23:25:08.433	ID=33554434, DIRECTION=CALLED	
2021-01-26 23:25:08.469		← Status:200 (2)
2021-01-26 23:25:08.469	← Status:200 (2)	←
2021-01-26 23:25:08.469	MEDIA FLOW DELETE, ID=33554433, DIRECTION=CALLING	
2021-01-26 23:25:08.469	MEDIA FLOW DELETE, ID=33554434, DIRECTION=CALLED	

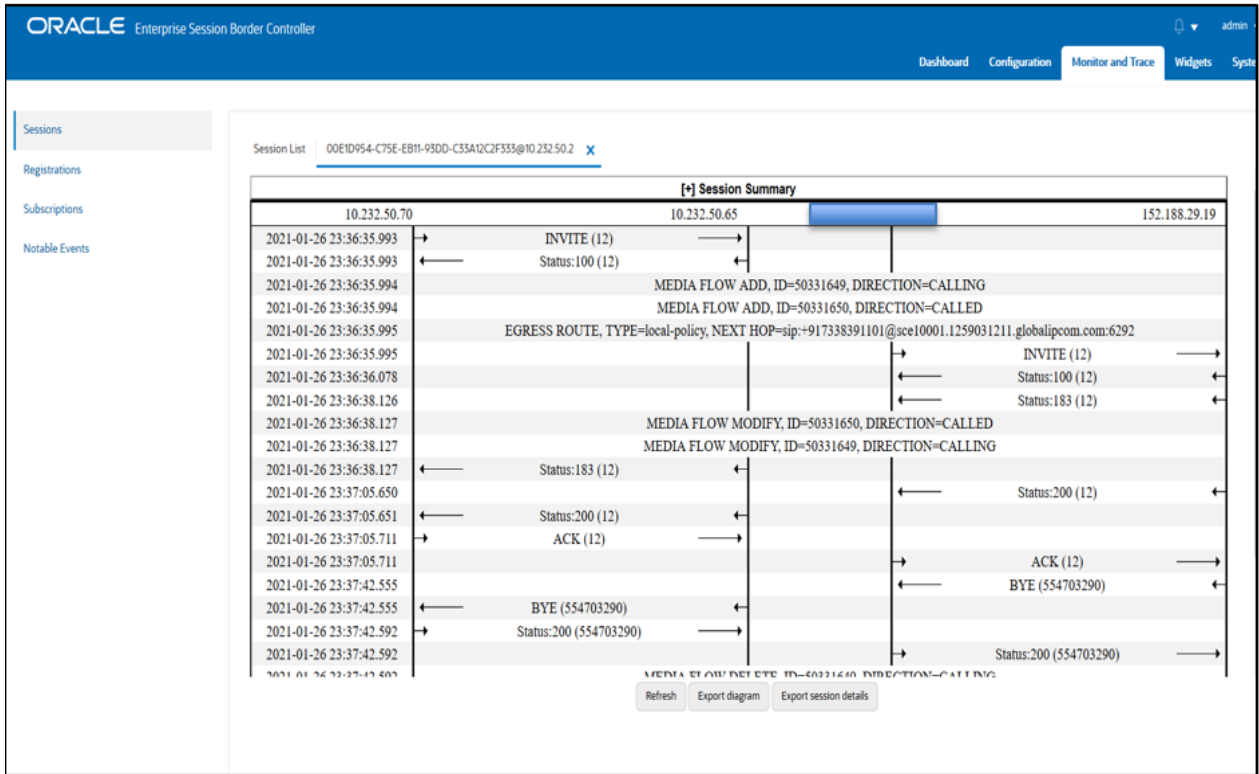
SIP Message Details

Refresh Export diagram Export session details

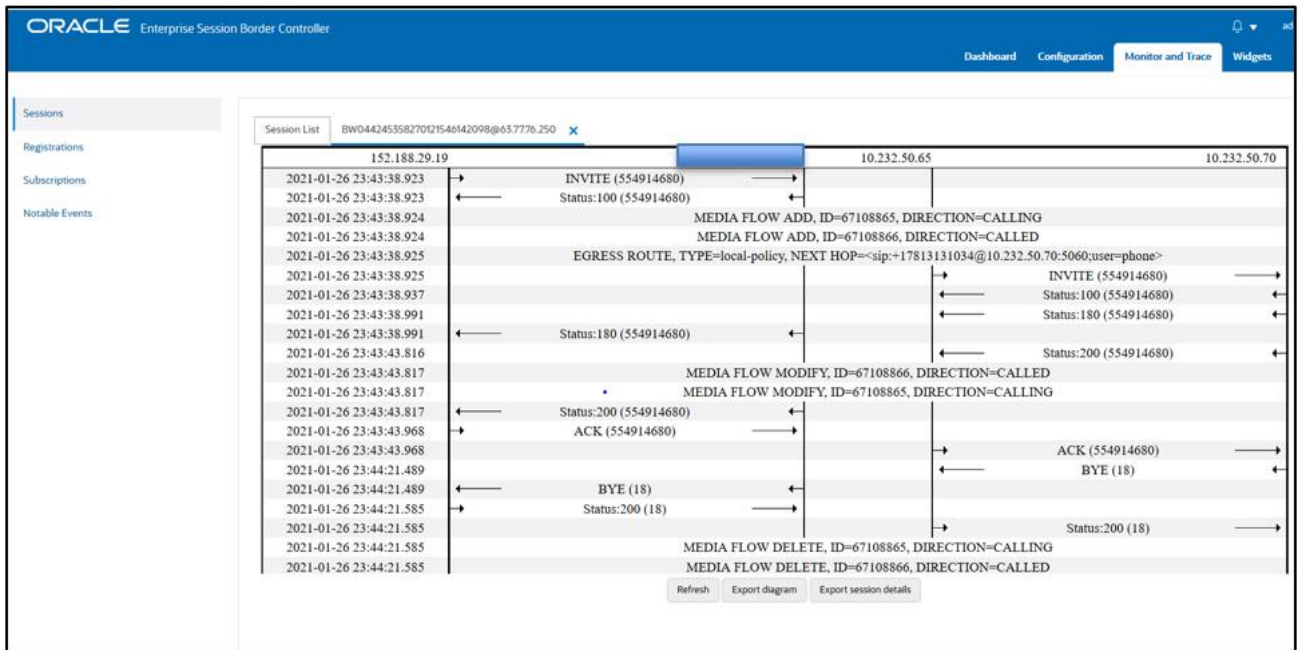


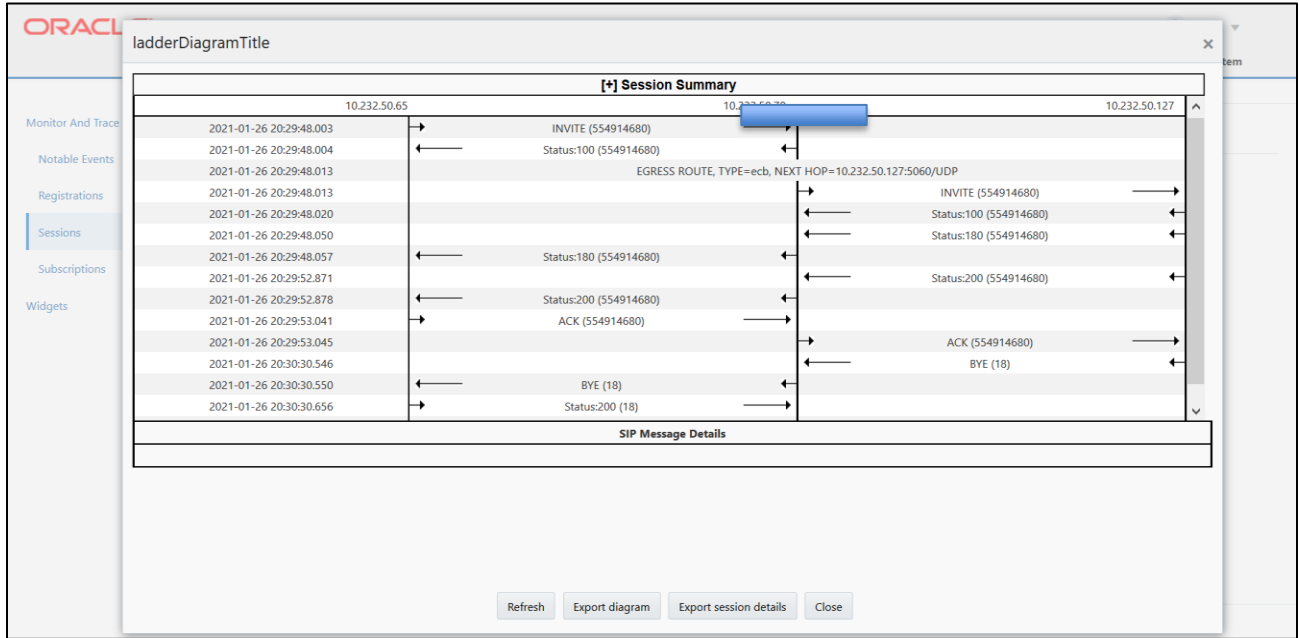
3. Make Call from Avaya User to Verizon Trunk user and check the call flow. The Call from Avaya Session manager reaches ECB IP and then routed to SBC and to Verizon trunk user.






4. Make Call from Verizon Trunk user to Avaya User and check the call flow. The Call from Verizon Trunk reaches SBC and then to ECB and then routed to Avaya User as below





**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 Worldwide Inquiries**

500 Oracle Parkway Phone: +1.650.506.7000  
 Redwood Shores, CA 94065, USA 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