



# ORACLE

## Oracle SBC integration with Avaya and Twilio Elastic Sip Trunking

Technical Application Note



## 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

<b>Version</b>	<b>Description of Changes</b>	<b>Date Revision Completed</b>
1.0	Oracle SBC integration with Avaya and Twilio Elastic SIP Trunking	07 <sup>th</sup> May 2021

## Table of Contents

<b>1. INTENDED AUDIENCE</b> .....	<b>4</b>
<b>2. DOCUMENT OVERVIEW</b> .....	<b>4</b>
2.1. TWILIO ELASTIC SIP TRUNKING .....	4
<b>3. INTRODUCTION</b> .....	<b>5</b>
3.1. AUDIENCE .....	5
3.2. REQUIREMENTS .....	5
3.3. ARCHITECTURE.....	6
<b>4. CONFIGURING THE AVAYA AURA SESSION MANAGER 8.1</b> .....	<b>7</b>
4.1. ADDING SIP DOMAIN .....	7
4.2. ADDING LOCATION.....	8
4.3. ADDING THE ORACLE SBC AS A SIP ENTITY AND CONFIGURING AN ENTITY LINK .....	8
4.4. ALLOWING UNSECURED PPM TRAFFIC (ONLY IF TLS IS NOT USED) AND PPM RATE LIMITING .....	11
4.5. ADDING ROUTING POLICIES .....	13
4.6. ADDING DIAL PATTERNS:.....	13
4.7. ADDING USERS TO AVAYA SESSION MANAGER. ....	15
4.8. ADDING THE ORACLE SBC AS A SIP ENTITY AND ENTITY LINK FOR REMOTE WORKER .....	18
4.9. ENABLING REMOTE OFFICE.....	19
<b>5. CONFIGURING THE SBC</b> .....	<b>21</b>
5.1. VALIDATED ORACLE SBC VERSION .....	21
<b>6. NEW SBC CONFIGURATION</b> .....	<b>21</b>
6.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC .....	21
6.2. CONFIGURE SBC USING WEB GUI .....	25
6.3. CONFIGURE SYSTEM-CONFIG.....	27
6.4. CONFIGURE PHYSICAL INTERFACE VALUES .....	28
6.5. CONFIGURE NETWORK INTERFACE VALUES .....	29
6.6. ENABLE MEDIA MANAGER.....	31
6.7. CONFIGURE REALMS .....	32
6.8. CONFIGURING A CERTIFICATE FOR SBC.....	34
6.9. TLS-PROFILE .....	37
6.10. CONFIGURE SIP INTERFACES .....	37
6.11. CONFIGURE SESSION-AGENT .....	39
6.12. CONFIGURE LOCAL-POLICY .....	40
6.13. CONFIGURE STEERING-POOL .....	42
6.14. CONFIGURE PING RESPONSE .....	43
6.15. CONFIGURE CODEC POLICY.....	45
6.16. CONFIGURE SDES PROFILE .....	46
6.17. CONFIGURE MEDIA SECURITY PROFILE .....	46
6.18. CONFIGURE TRANSLATION RULES .....	48
6.19. CONFIGURE SESSION TRANSLATION RULES.....	49
<b>7. SBC CONFIGURATION FOR AVAYA REMOTE WORKER</b> .....	<b>51</b>
7.1. CONFIGURE REALMS .....	51
7.2. ENABLE SIP-CONFIG.....	53
7.3. ENABLE MEDIA MANAGER.....	55
7.4. CONFIGURE SIP INTERFACES .....	56
7.5. CONFIGURE STEERING-POOL .....	58

7.6. CONFIGURE LOCAL-POLICY (OPTIONAL).....	59
<b>8. EXISTING SBC CONFIGURATION .....</b>	<b>60</b>
<b>9. TWILIO ELASTIC SIP TRUNKING CONFIGURATION .....</b>	<b>60</b>
9.1. CREATE AN IP-ACL RULE .....	61
9.2. CREATE A NEW TRUNK .....	62
9.3. ASSOCIATE PHONE NUMBERS ON YOUR TRUNK .....	65
<b>10. VERIFICATION OF SAMPLE CALL FLOWS.....</b>	<b>66</b>
<b>APPENDIX A.....</b>	<b>70</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). 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.

## 2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Twilio Elastic Sip Trunk with Avaya Session Manager. The solution contained within this document has been tested using Oracle Communication SBC with **OS840p4A**.

In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the Avaya Server and Twilio Elastic Sip Trunk related 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. Twilio Elastic SIP Trunking

[Twilio Elastic SIP Trunking](#) is a cloud-based solution that provides connectivity for IP-based communications infrastructure to connect to the PSTN for making and receiving telephone calls to the rest of the world via any broadband internet connection. Twilio's Elastic SIP Trunking service automatically scales, up or down, to meet your traffic needs with unlimited capacity. In just minutes you can deploy globally with Twilio's easy-to-use self-service tools without having to rely on slow providers.

Sign up for a [free Twilio trial](#) and learn more about [configuring your Twilio Elastic SIP Trunk](#).

**Please note that the IP Addresses, FQDN and configuration names and details given in this document are used for reference purposes only. These same details cannot be used in customer configurations. End users of this document can use the configuration details according to their network requirements.**

### 3. Introduction

#### 3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Avaya Session Manager using Oracle Enterprise SBC. There will be steps that require navigating the Avaya server configuration and Oracle SBC GUI interface. Understanding the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP, TLS/SRTP are also necessary to complete the configuration and for troubleshooting, if necessary.

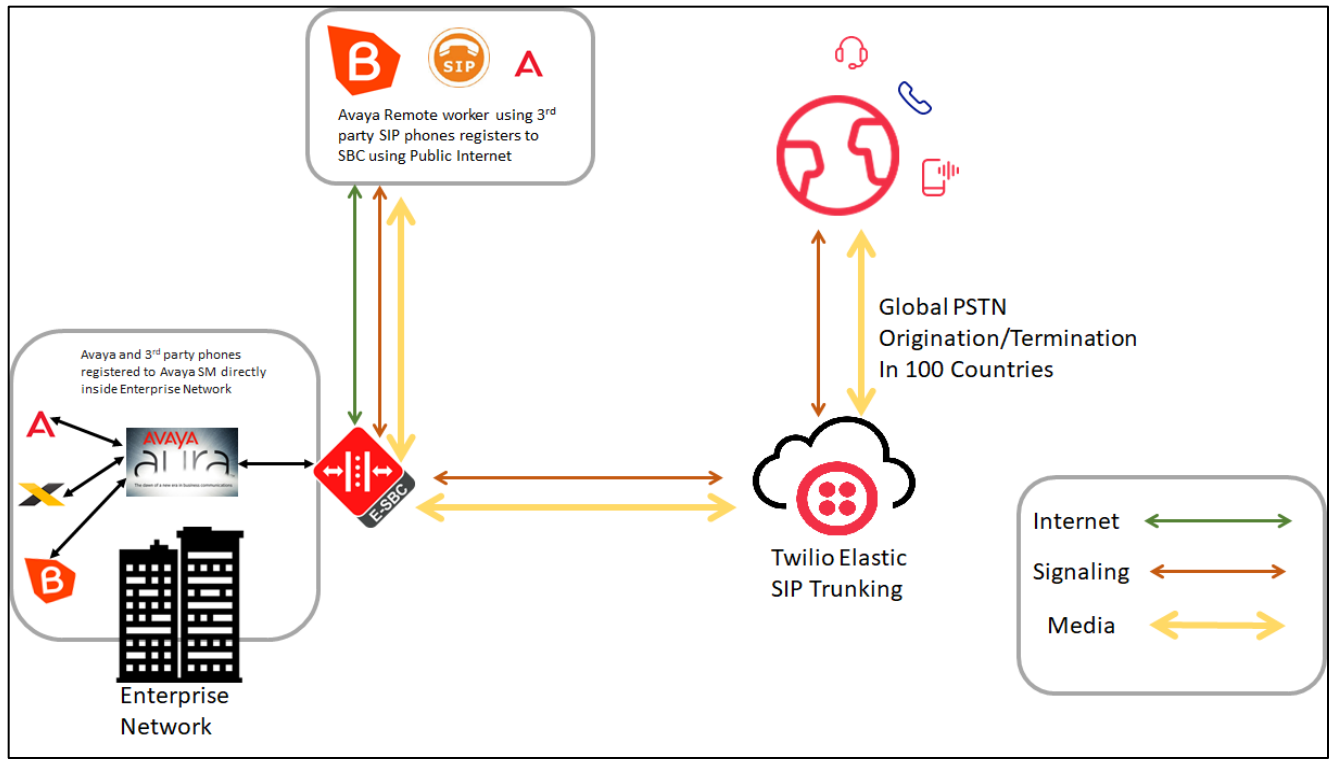
#### 3.2. Requirements

- Fully functioning Avaya Aura Session Manager 8.1 version
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version

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

Software Used	SBC Version	Avaya Aura Session Manager using Avaya Aura System Manager GUI
Revision 1	8.4.0	8.1

### 3.3. Architecture

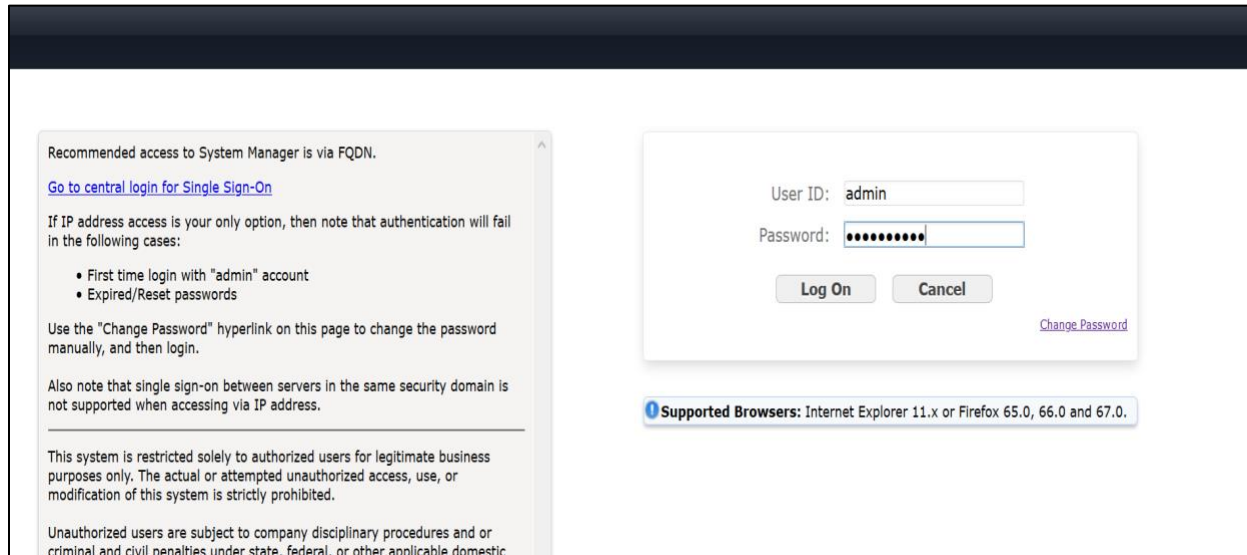


The configuration, validation and troubleshooting are the focuses of this document and will be described in three phases:

- Phase 1 – Configuring the Avaya Aura Session Manager
- Phase 2 – Configuring the Oracle SBC.
- Phase 3 – Configuring the Twilio Elastic SIP Trunk

## 4. Configuring the Avaya Aura Session Manager 8.1

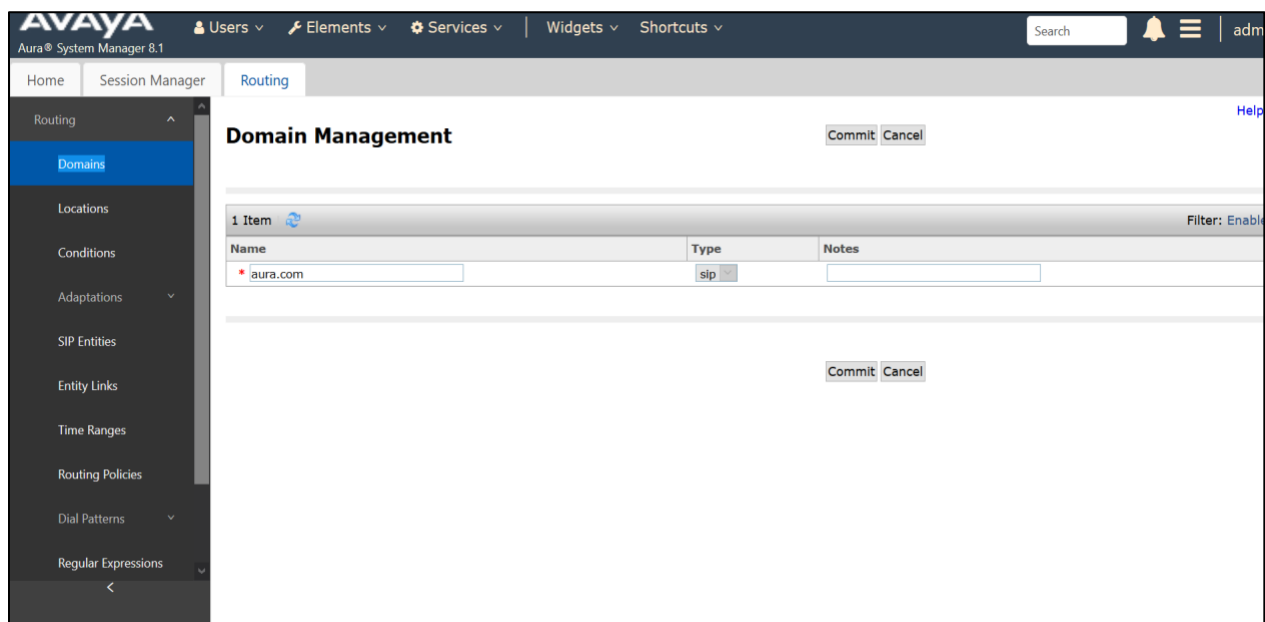
Please login to Avaya Aura System Manager Web GUI with proper login credentials (Username and password). After that, perform the steps below in the given order.



### 4.1. Adding SIP Domain

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

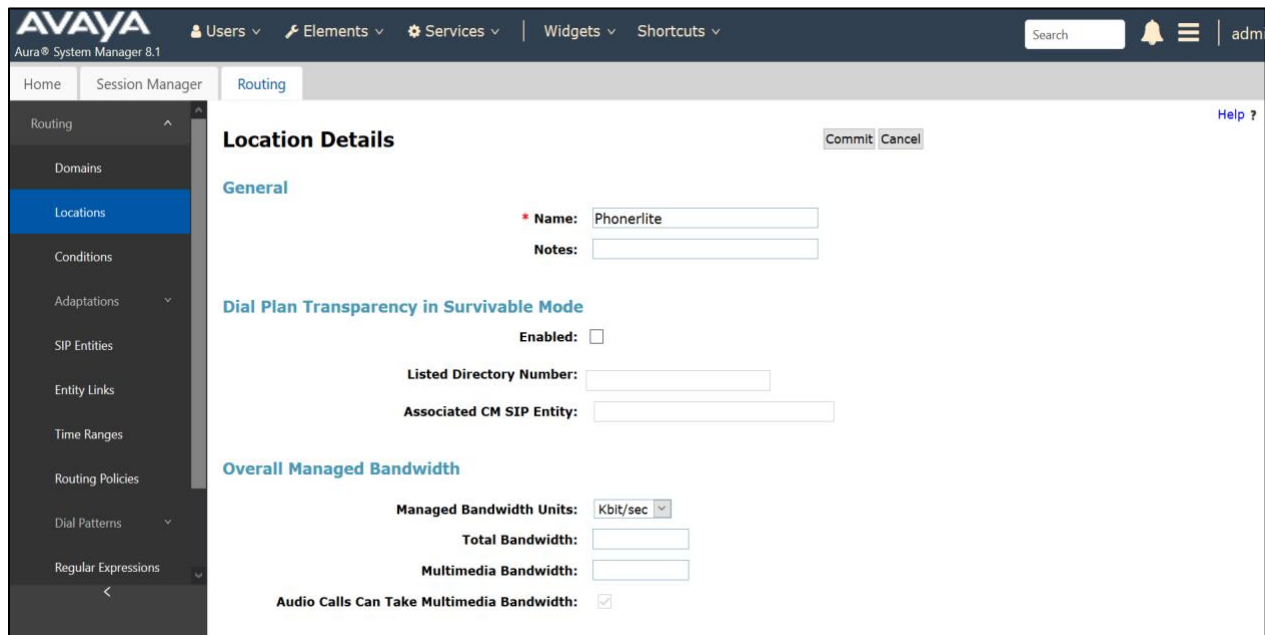
- Set domain name as aura.com (Example in this config)
- Set Type as SIP
- click "Commit" to save the configuration



## 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 displays 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:** The 'Name' field is set to 'Phonerlite'. The 'Notes' field is empty.
- Dial Plan Transparency in Survivable Mode:** The 'Enabled' checkbox is unchecked. The 'Listed Directory Number' and 'Associated CM SIP Entity' fields are empty.
- Overall Managed Bandwidth:** The 'Managed Bandwidth Units' dropdown is set to 'Kbit/sec'. The 'Total Bandwidth' and 'Multimedia Bandwidth' fields are empty. The 'Audio Calls Can Take Multimedia Bandwidth' checkbox is checked.

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

## 4.3. Adding the Oracle SBC 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 SBC as a SIP entity as shown below.

- Set Name: SBC4600Twilio (example in this configuration)
- Set FQDN or IP Address: This is the “inside” IP address of Oracle E-SBC, 10.232.50.78 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 we will add below after this config
- Set SIP Entity 2: leave the default value SBC4600Twilio
- Set Protocol: UDP/TCP/TLS based on our testing
- Set Ports: Set both Ports to 5060/5061 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

Home | Routing

### SIP Entity Details

Commit Cancel

#### General

\* Name: SBC4600Twilio

\* FQDN or IP Address: 10.232.50.78

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:

Securable:

Call Detail Recording: none

CommProfile Type Preference:

**AVAYA** Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts

Search

Home | Routing

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

#### Entity Links

Override Port & Transport with DNS SRV:

Add Remove

2 Items Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* acme-sm_SBC4600T	acme-sm	UDP	* 5060	SBC4600Twilio	* 5060	trusted	<input type="checkbox"/>
<input type="checkbox"/>	* acme-sm_SBC4600T	acme-sm	TLS	* 5061	SBC4600Twilio	* 5061	trusted	<input type="checkbox"/>

Select : All, None

#### SIP Responses to an OPTIONS Request

Add Remove

0 Items Filter: Enable

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

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.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, user information, and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a notification bell are also present. The main content area is titled "SIP Entity Details" and is divided into two sections: "General" and "Monitoring".

**General**

**Name:** acme-sm

**IP Address:** 10.232.50.127

**SIP FQDN:** [Empty field]

**Type:** Session Manager

**Notes:** [Empty field]

**Location:** Phonerlite

**Outbound Proxy:** [Empty field]

**Time Zone:** America/New\_York

**Minimum TLS Version:** Use Global Setting

**Credential name:** [Empty field]

**Monitoring**

**SIP Link Monitoring:** Use Session Manager Configuration

**CRLF Keep Alive Monitoring:** Use Session Manager Configuration

Buttons for "Commit" and "Cancel" are located at the top right of the configuration area.

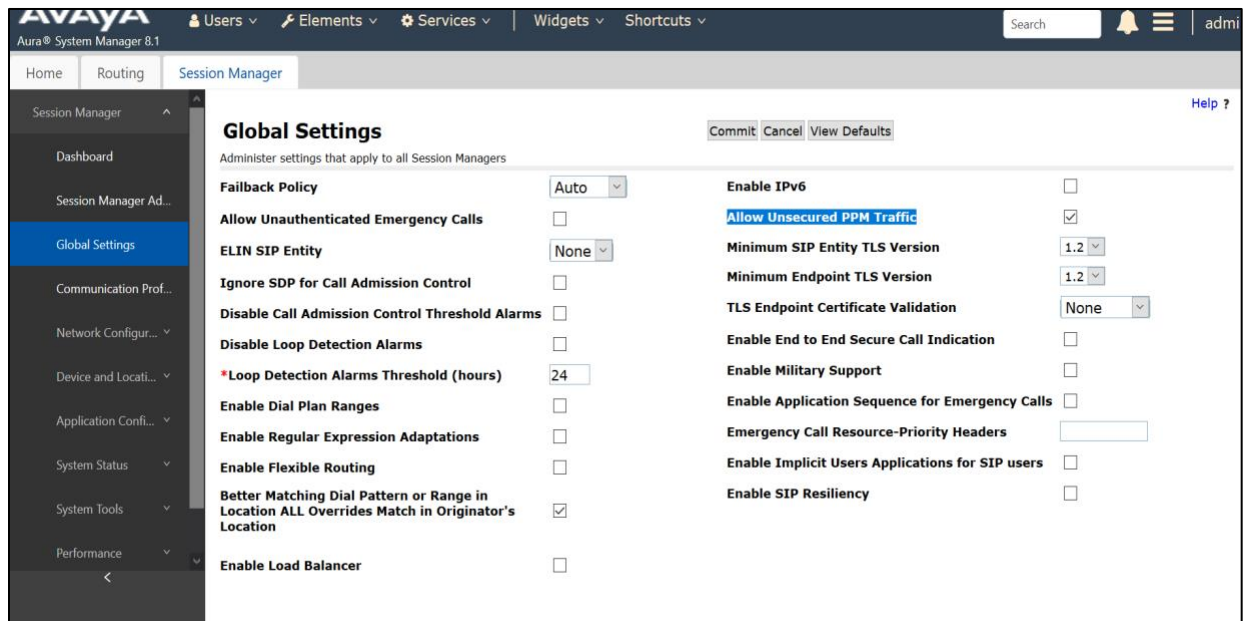
## 4.4. Allowing Unsecured PPM Traffic (only if TLS is not used) and PPM Rate Limiting

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.



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

Session Manager Administration

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: SMSBCroute (example in this configuration)
- Set Retries : Default value is 0, can be used as same value
- Select SIP Entity as Destination: Select SBC4600Twilio which was previously configured.
- Click Commit to save the configuration

The screenshot displays the Avaya Aura System Manager 8.1 interface for configuring a Routing Policy. The left sidebar shows the navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes the following sections:

- General:** Name: SMSBCroute, Disabled: , Retries: 0, Notes:
- SIP Entity as Destination:** A table with one entry: SBC4600Twilio, FQDN or IP Address: 10.232.50.78, Type: Other.
- Time of Day:** A table with one entry: Ranking: 0, Name: 24/7, Start Time: 00:00, End Time: 23:59, Notes: Time Range 24/7.

## 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.

The user can create other dial patterns as per their requirement using the config given above

AVAYA Aura® System Manager 8.1

Users Elements Services Widgets Shortcuts Search

Home Routing

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

### 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		SMSBCroute	0	<input type="checkbox"/>	SBC4600	

Select: All, None

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

Home Routing

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

Add Remove view Copy 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

2 Items 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	
<input type="checkbox"/>	91xxxxxxxxx	12	12	<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: User4(example in this configuration)
- Set First Name: Avaya (example in this configuration)
- Set Login Name: 18507904044@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  
18507904044@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 for editing a user profile. The breadcrumb trail is Home / Users / Manage Users. The user profile is for 18507904044@aura.com. The 'Identity' tab is active, showing the following fields:

- User Provisioning Rule: [Dropdown]
- Last Name: User4
- Last Name (Latin Translation): User4
- First Name: Avaya
- First Name (Latin Translation): Avaya
- Login Name: 18507904044@aura.com
- Middle Name: Middle Name Of User
- Description: Description Of User
- Email Address: Email Address Of User
- Password: [Field]
- User Type: Basic

The 'Communication Profile' tab is also visible, showing a 'User Provisioning Rule' dropdown. The 'Basic Info' section is expanded, showing 'Address' and 'LocalizedName' fields. The 'Manage Users' sidebar is visible on the left, and the 'Commit & Continue', 'Commit', and 'Cancel' buttons are at the top right.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, user profile (adm), and menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and notification bell are also present. The main navigation menu on the left is expanded to 'User Management', with 'Manage Users' selected. The main content area displays the 'User Profile | Edit | 18507904044@aura.com' page. The 'Communication Profile' tab is active, showing fields for 'Communication Profile Password', 'PROFILE SET: Primary', and 'Communication Address'. A modal dialog box titled 'Comm-Profile Password' is open in the foreground, containing two password input fields: 'Comm-Profile Password' and 'Re-enter Comm-Profile Password'. The second field has a green checkmark, indicating the passwords match. Below the fields is a 'Generate Comm-Profile Password' link and 'Cancel' and 'OK' buttons.

The screenshot shows the Avaya Aura System Manager 8.1 interface, similar to the first image. The main navigation menu is expanded to 'User Management', with 'Public Contacts' selected. The main content area displays the 'User Profile | Edit | 18507904044@aura.com' page. The 'Communication Profile' tab is active, and the 'Communication Address' sub-tab is selected. A modal dialog box titled 'Communication Address Add/Edit' is open in the foreground. It contains a dropdown menu for '\* Type:' with 'Avaya SIP' selected, and a field for '\* Fully Qualified Address:' with '18507904044' entered and '@ aura.com' selected from a dropdown. 'Cancel' and 'OK' buttons are at the bottom of the dialog.



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 'User Profile | Edit | 18507904044@aura.com'. The left sidebar shows 'User Management' with 'Manage Users' selected. The main panel has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing 'PROFILE SET: Primary' and 'Session Manager Profile' (checked). The 'SIP Registration' section includes:
 

- Primary Session Manager: acme-sm
- Secondary Session Manager: Start typing...
- Survivability Server: Start typing...
- Max. Simultaneous Devices: 4
- Block New Registration When Maximum Registrations:

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 'User Profile | Edit | 18507904044@aura.com'. The left sidebar shows 'User Management' with 'Manage Users' selected. The main panel has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing 'Emergency Calling' settings and 'Call Routing Settings'. The 'Call Routing Settings' section includes:
 

- Emergency Calling Origination Sequence: Select
- Emergency Calling Termination Sequence: Select
- 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.

Below are the configuration which are specific to Avaya Remote Worker configuration.

#### 4.8. Adding the Oracle SBC as a SIP Entity and Entity Link for Remote Worker

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 SBC as a SIP entity as shown below.

- Set Name: SBC4600 (example in this configuration)
- Set FQDN or IP Address: This is the “inside” IP address of Oracle E-SBC, 10.50.232.77 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 SBC4600
- Set Protocol: UDP/TCP/TLS based on our testing
- Set Ports: Set both Ports to 5060/5061 for testing
- Set Connection Policy: trusted

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 main content area is titled 'SIP Entity Details' and is currently on the 'General' tab. The configuration fields are as follows:

- Name: SBC4600
- FQDN or IP Address: 10.232.50.77
- Type: Other
- Notes: (empty)
- Adaptation: (empty)
- Location: Phonerlite
- Time Zone: America/New\_York
- SIP Timer B/F (in seconds): 4
- Minimum TLS Version: Use Global Setting
- Credential name: (empty)
- Securable:
- Call Detail Recording: none
- CommProfile Type Preference: (empty)

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

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top header includes the Avaya logo, user information (Users, Elements, Services, Widgets, Shortcuts), a search bar, and a user profile icon. The navigation menu on the left is expanded to show 'SIP Entities' and 'Entity Links'. The main content area displays the 'Entity Links' configuration page, which includes a 'Primary Session Manager Bandwidth Association' and a 'Backup Session Manager Bandwidth Association' dropdown menu. Below this is the 'Entity Links' section, which has an 'Override Port & Transport with DNS SRV' checkbox and a table with 2 items. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service. The two items are:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
* acme-sm_SBC4600	acme-sm	UDP	* 5060	SBC4600	* 5060	trusted	<input type="checkbox"/>
* acme-sm_SBC4600	acme-sm	TLS	* 5061	SBC4600	* 5061	trusted	<input type="checkbox"/>

Below the table is a 'SIP Responses to an OPTIONS Request' section, which has an 'Add' and 'Remove' button and a table with 0 items. The table has columns for Response Code & Reason Phrase, Mark Entity Up/Down, and Notes. At the bottom right of the page are 'Commit' and 'Cancel' buttons.

We can use the configured Avaya Session Manager as another SIP entity for remote worker too.

## 4.9. Enabling Remote Office

Navigate to: Elements->Session Manager->Network Configuration->Remote Access, Click New

- Set Name: Remote\_worker for this setup.
- Click New under SIP Proxy Mapping Table. Add the Oracle SBC outside interface IP address for SIP Proxy Public Address, 141.146.36.77 is given in this example.
- Click New under SIP Proxy Private IP Address. Add the Oracle SBC inside interface IP address for SIP Private Address, 10.232.50.77 is given in this example.
- Click Commit to save the configuration.

AVAYA Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts

Search | ad

Home | Routing | Session Manager

Session Manager

- Dashboard
- Session Manager Ad...
- Global Settings
- Communication Prof...
- Network Configur...
- Failover Groups
- Local Host Nam...
- Remote Access**
- SIP Firewall
- Device and Locati...

Remote Access Configuration

Commit Cancel

\*Name: Remote\_worker

Note:

[Click to open Remote Access Reference Map](#)

SIP Proxy Mapping

SIP Proxy Mapping Table

New Delete

<input type="checkbox"/>	SIP Proxy Public Address (Reference A)	Session Manager (Reference C)	IP Address Family (Reference C)
<input type="checkbox"/>	141.146.36.77	acme-sm	IPv4

Select : All, None

AVAYA Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts

Search | ad

Home | Routing | Session Manager

Session Manager

- Dashboard
- Session Manager Ad...
- Global Settings
- Communication Prof...
- Network Configur...
- Failover Groups
- Local Host Nam...
- Remote Access**
- SIP Firewall
- Device and Locati...

SIP Proxy Mapping Table

New Delete

<input type="checkbox"/>	SIP Proxy Public Address (Reference A)	Session Manager (Reference C)	IP Address Family (Reference C)
<input type="checkbox"/>	141.146.36.77	acme-sm	IPv4

Select : All, None

SIP Proxy Private IP Addresses

New Delete

<input type="checkbox"/>	SIP Private Address (Reference B)	SBC Type	Securable	Note
<input type="checkbox"/>	10.232.50.77	Avaya SBC	<input type="checkbox"/>	

Select : All, None

\*Required

Commit Cancel

With this, Avaya Session Manager Configuration is complete.

## 5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Avaya Session Manager and Twilio Elastic SIP Trunking. **In this SBC config, Twilio Elastic SIP trunk side is secure (TLS/SRTP) and Avaya Core Side is unsecure (UDP or TCP/RTP).**

### 5.1. 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 6300
- AP 6350
- VME

## 6. New SBC configuration

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

### 6.1. 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 tbfdd...
Starting tIPTd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tTscfd...
Starting tFcgid...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Starting tIFMIBd...
Start platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...

Starting acliMgr...
password secure mode is enabled
Admin Security is disabled
Password: █
```

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# conf t
NN4600-139(configure)# bootparam

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

Boot File           : /boot/nnSCZ840p3B.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: 40)

NN4600-139(configure)#
```

Note: There is no management IP configured by default.

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.

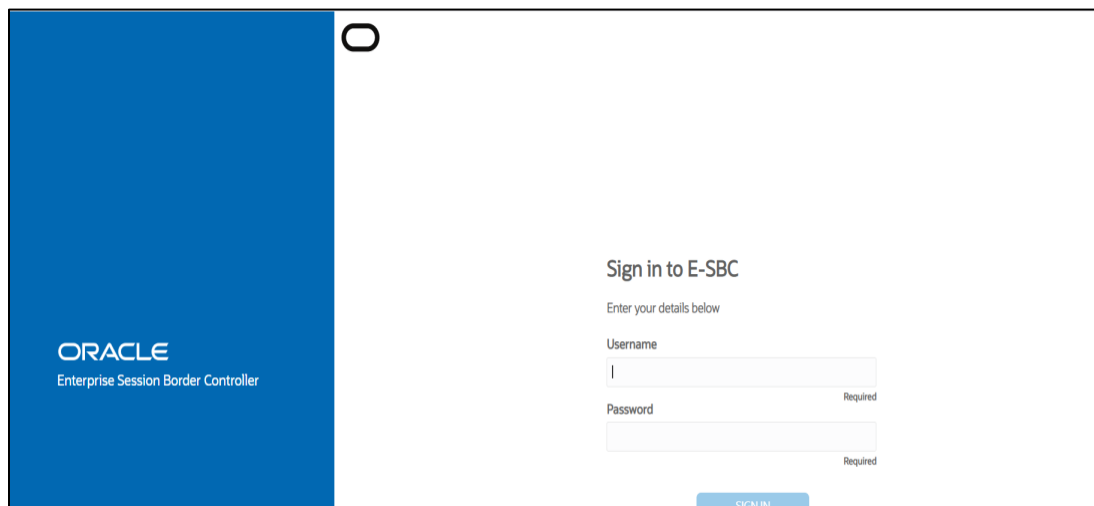
Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

```
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)# █
```

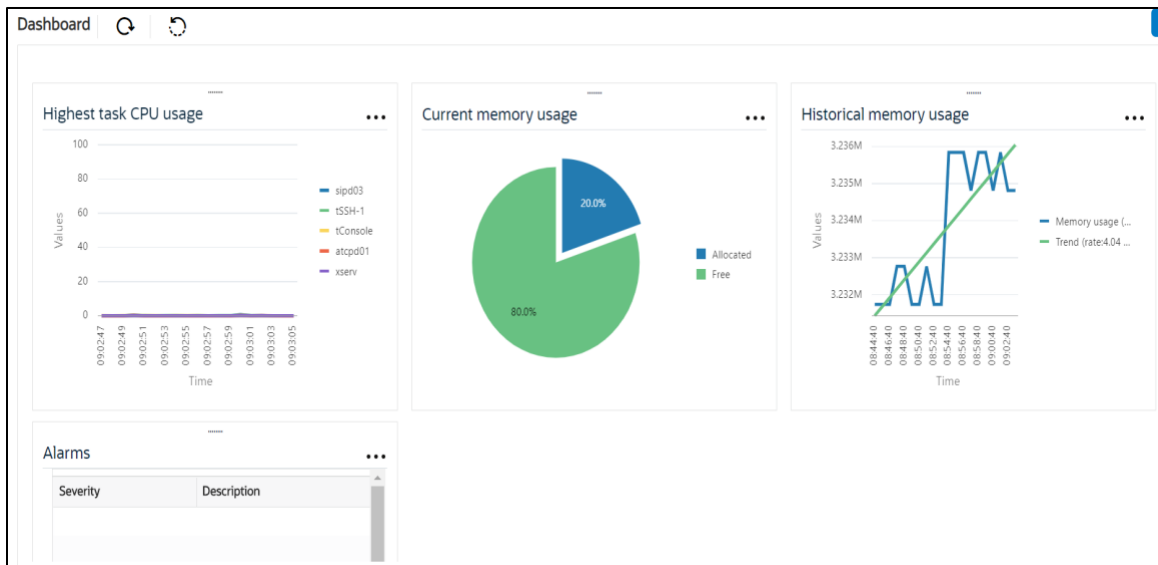
## 6.2. Configure SBC using Web GUI

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

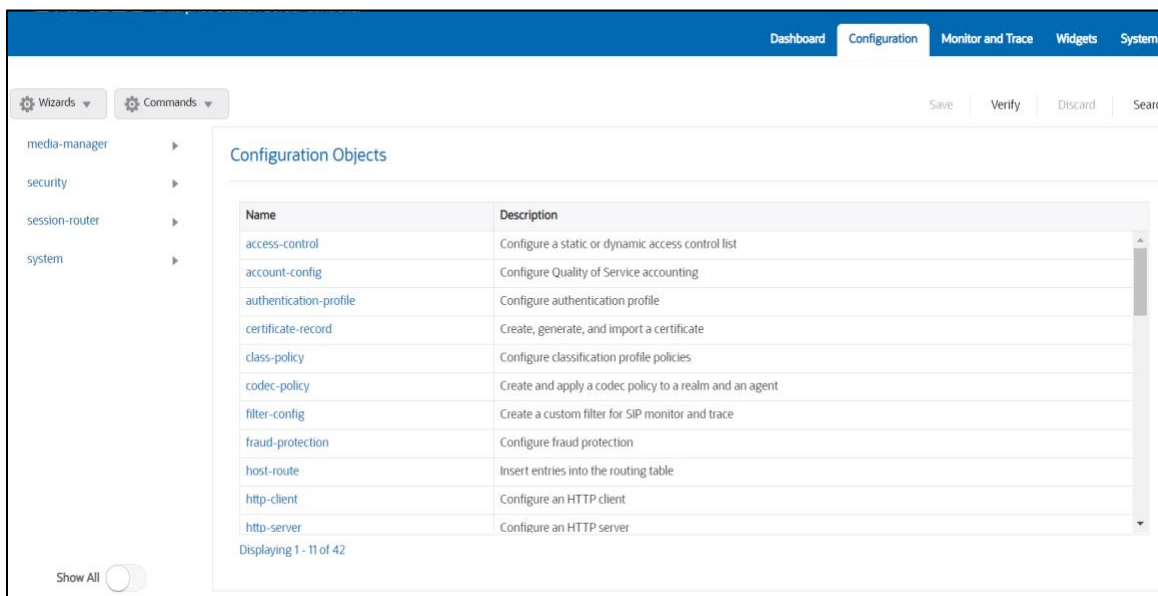
The Web GUI can be accessed through the url [http://<SBC\\_MGMT\\_IP>](http://<SBC_MGMT_IP>).



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



Go to Configuration as shown below, to configure the SBC



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

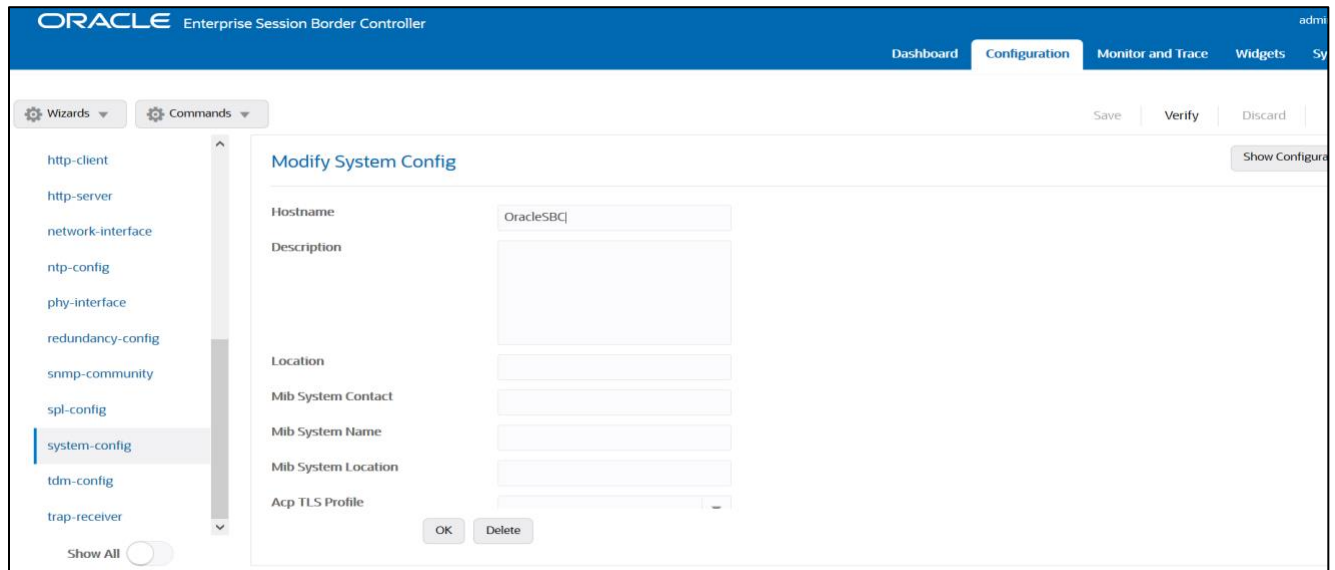
[https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc\\_scz840\\_webgui.pdf](https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf)

The expert mode is used for configuration.

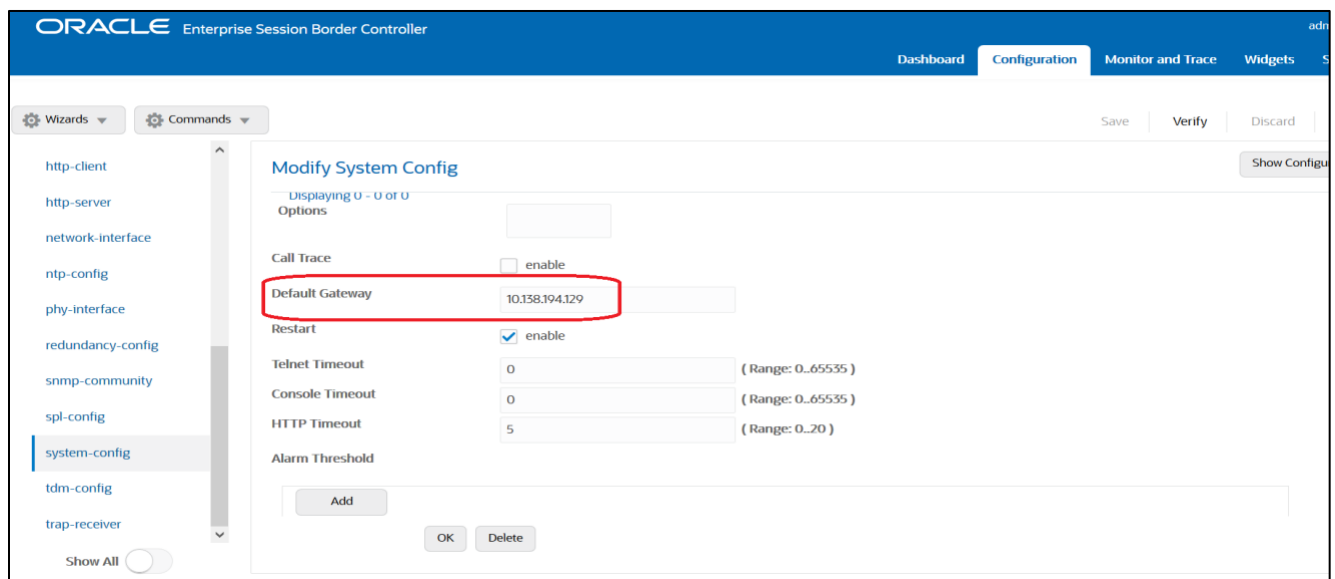
**Tip:** To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

### 6.3. Configure system-config

Go to system->system-config



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



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.

## 6.4. Configure Physical Interface values

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

Please configure M00 for Twilio side and M10 for Avaya side.

Parameter Name	Twilio Elastic Sip Trunk side (M00)	Avaya side (M10)
Slot	0	0
Port	0	1
Operation Mode	Media	Media

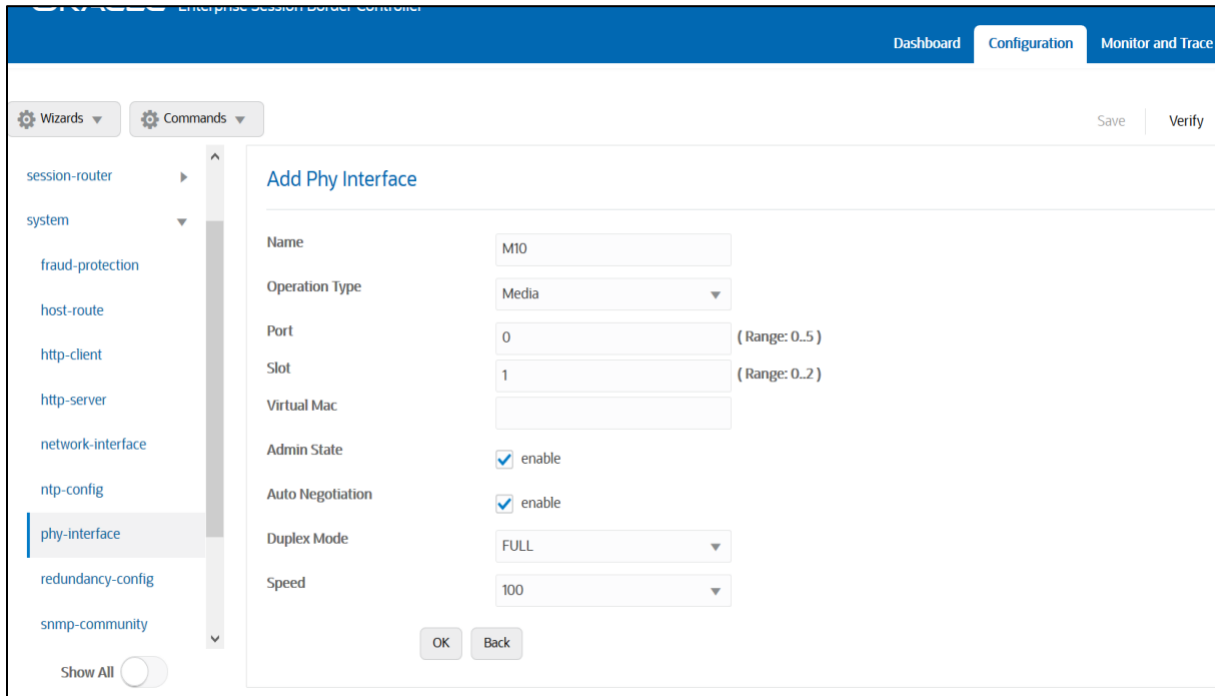
Please configure M00 interface as below.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration categories, with 'phy-interface' selected. The main content area is titled 'Add Phy Interface' and contains the following configuration fields:

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

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

Please configure M10 interface as below



## 6.5. Configure Network Interface values

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

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

Parameter Name	Twilio side Network interface	Avaya side Network interface
Name	M00	M10
Host Name		
IP address	141.146.36.102	10.232.50.78
Netmask	255.255.255.192	255.255.255.0
Gateway	141.146.36.65	10.232.50.1

Please configure network interface M00 as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar lists various configuration categories, with 'network-interface' selected. The main content area is titled 'Add Network Interface' and contains the following fields:

Name	M00
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	
IP Address	141.146.36.102
Pri Utility Addr	141.146.36.102
Sec Utility Addr	

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

Similarly, configure network interface M10 as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for network interface M10. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar lists various configuration categories, with 'network-interface' selected. The main content area is titled 'Add Network Interface' and contains the following fields:

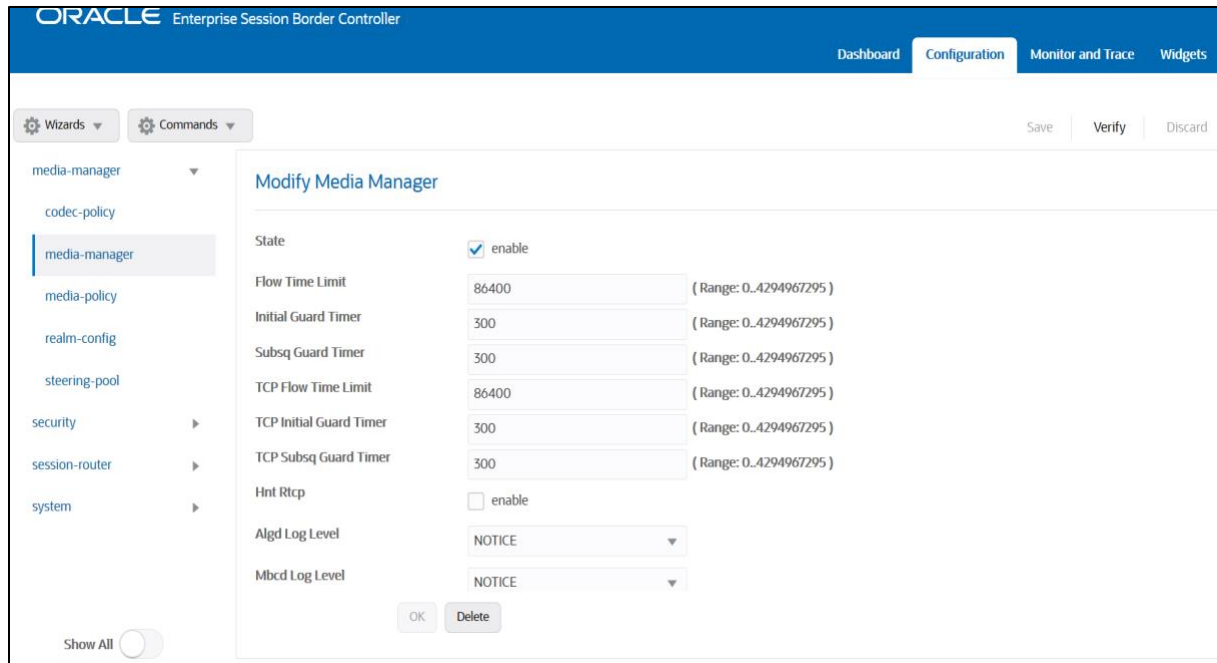
Name	M10
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	
IP Address	10.232.50.78
Pri Utility Addr	10.232.50.78
Sec Utility Addr	

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

## 6.6. Enable media manager

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

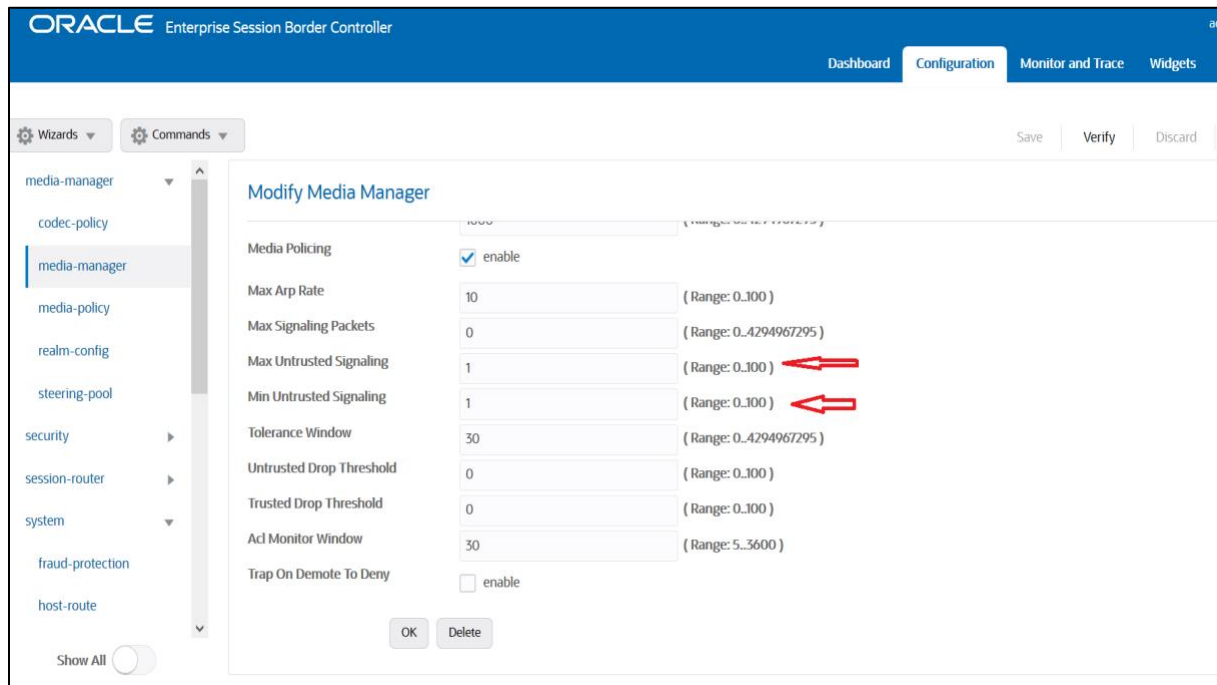
In addition to the above config, please set the max and min untrusted signaling values to 1. Go to Media-Manager->Media-Manager



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active, and the 'media-manager' configuration page is displayed. The 'State' is set to 'enable'. The following parameters are configured:

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 )
Hnt Rtcp	<input type="checkbox"/> enable	
Algld Log Level	NOTICE	
Mbcd Log Level	NOTICE	

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



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, specifically the 'Media Policing' section of the 'media-manager' configuration page. The 'Media Policing' is set to 'enable'. The following parameters are configured:

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 )
Acl 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 set to 1.

## 6.7. 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	Twilio Side	Avaya Side
Identifier	TwilioRealm	AvayaRealm
Network Interface	M00	M10
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FQDN		
Media Sec policy	sdespolicy	RTP
Access Control Trust Level	High	High
Codec-Policy	Twiliocodec	AvayaCodec

In the below case, Realm name is given as TwilioRealm for Twilio Elastic SIP Trunking Side  
Please set the Access Control Trust Level as high for this realm

The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration' (selected), 'Monitor and Trace', and 'Widgets'. Below the navigation bar, there are 'Wizards' and 'Commands' tabs, and 'Save', 'Verify', and 'Discard' buttons. The left sidebar shows a tree view with 'media-manager' expanded, and 'realm-config' selected. The main content area is titled 'Add Realm Config' and contains the following fields:

- Identifier: TwilioRealm
- Description: (empty text area)
- Addr Prefix: 0.0.0.0
- Network Interfaces: M00:0.4 X
- Media Realm List: (empty text area)
- Mm In Realm:  onshlo

At the bottom of the form are 'OK' and 'Back' buttons. A 'Show All' toggle is visible in the bottom left corner of the sidebar area.



ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace

Wizards Commands Save Verify

media-manager  
codec-policy  
media-manager  
media-policy  
realm-config  
steering-pool  
security  
session-router  
system  
fraud-protection  
host-route  
Show All

### Add Realm Config

Out Translationid	<input type="text"/>	
In Manipulationid	<input type="text"/>	
Out Manipulationid	<input type="text"/>	
Average Rate Limit	<input type="text" value="0"/>	( Range: 0..4294967295 )
Access Control Trust Level	<input type="text" value="high"/>	
Invalid Signal Threshold	<input type="text" value="0"/>	( Range: 0..4294967295 )
Maximum Signal Threshold	<input type="text" value="0"/>	( Range: 0..4294967295 )
Untrusted Signal Threshold	<input type="text" value="0"/>	( Range: 0..4294967295 )
Nat Trust Threshold	<input type="text" value="0"/>	( Range: 0..65535 )
Max Endpoints Per Host	<input type="text"/>	

OK Back

Similarly, Realm name is given as AvayaRealm for Avaya side.  
Please set the Access Control Trust Level as high for this realm too.

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  
Show All

### Add Realm Config

Identifier	<input type="text" value="AvayaRealm"/>
Description	<input type="text"/>
Addr Prefix	<input type="text" value="0.0.0.0"/>
Network Interfaces	<input type="text" value="M10:0.4"/>
Media Realm List	<input type="text"/>
Mm In Realm	<input checked="" type="checkbox"/> enable

OK Back

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)

## 6.8. Configuring a certificate for SBC

This section describes how to configure the SBC for TLS and SRTP communication for Twilio Elastic SIP Trunking.

Twilio Elastic SIP Trunking 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.

The process includes the following steps:

- 1) Create a certificate-record – “Certificate-record” are configuration elements on Oracle SBC which captures information for a TLS certificate – such as common-name, key-size, key-usage etc.
  - SBC – 1 certificate-record assigned to SBC
  - Root – 1 certificate-record for root cert
- 2) Deploy the SBC and Root certificates on the SBC

## Step 1 – Creating the certificate record

Twilio Elastic SIP Trunking uses certificates from a CA (Certificate Authority) for establishing the TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It is important that you add the following root certificate to establish TLS connection from the link given below:

<https://www.twilio.com/docs/sip-trunking#rootCA>

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar shows a tree view with 'security' expanded to 'certificate-record'. The main content area is titled 'Modify Certificate Record' and contains the following fields:

Name	TwilioRootCACertChain
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	Solutions
Common Name	Chain CA Cert
Key Size	2048
Alternate Name	

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

This screenshot shows the same 'Modify Certificate Record' configuration page, but with advanced settings visible. The 'Trusted' checkbox is checked, and the 'Key Usage List' and 'Extended Key Usage List' are populated with values.

Key Size	2048
Alternate Name	
Trusted	<input checked="" type="checkbox"/> enable
Key Usage List	digitalSignature X keyEncipherment X
Extended Key Usage List	serverAuth X
Key Algor	rsa
Digest Algor	sha256
Ecdsa Key Size	p256

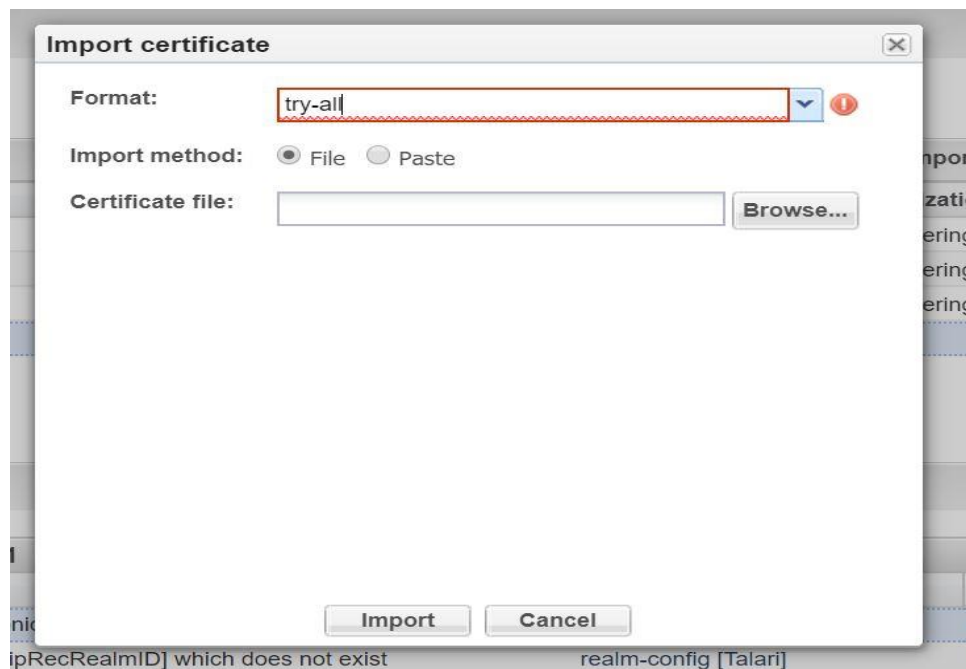
Buttons for 'OK' and 'Back' are located at the bottom of the form. A 'Show All' toggle is visible at the bottom left.

The table below specifies the parameters required for certificate configuration. Modify the configuration according to the certificates in your environment.

Config Parameter	DigiCert Root CA
Common Name	DigiCert Global Root CA
Key Size	2048
Key-Usage-List	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth
Key algor	rsa
Digest-algor	Sha256

## Step 2 – Deploy SBC & root certificates

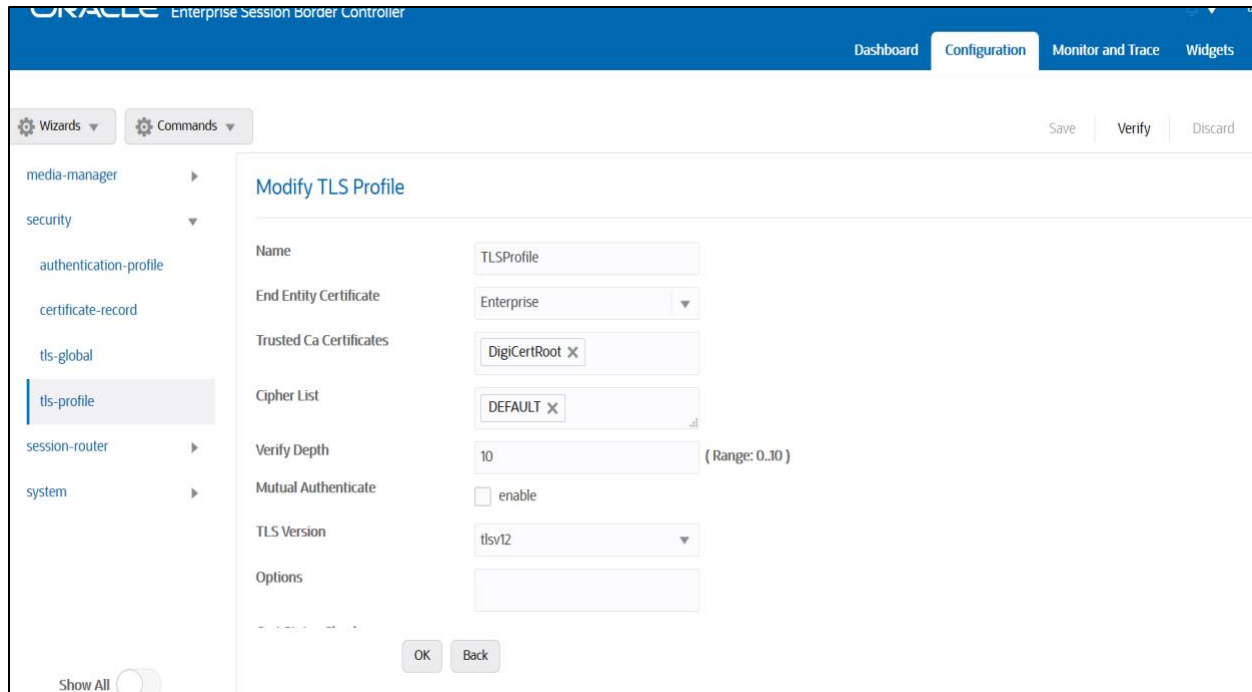
Once certificate record has been created – import the signed certificate to the SBC. Please note – all certificates including root certificates are required to be imported to the SBC. Once done, issue save/activate from the WebGUI



Repeat these steps to import all the root certificates into the SBC:  
**At this stage all the required certificates have been imported to the SBC for Twilio Elastic SIP Trunk.**

## 6.9. TLS-Profile

A TLS profile configuration on the SBC allows for specific certificates to be assigned. Go to security-> TLS-profile config element and configure the tls-profile as shown below. The below is the TLS profile configured for the Twilio Elastic SIP Trunk side:



The screenshot displays the Oracle Enterprise Session Border Controller (SBC) configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar shows a tree view with categories like 'media-manager', 'security', 'session-router', and 'system'. The 'security' category is expanded, and 'tls-profile' is selected. The main content area is titled 'Modify TLS Profile' and contains the following configuration fields:

Name	TLSPProfile
End Entity Certificate	Enterprise
Trusted Ca Certificates	DigiCertRoot X
Cipher List	DEFAULT X
Verify Depth	10 (Range: 0..10)
Mutual Authenticate	<input type="checkbox"/> enable
TLS Version	tlsv12
Options	

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

## 6.10. 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.

Please Configure sip-interface for the Twilio Elastic SIP Trunk side as below:

- 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.

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

- State:  enable
- Realm ID: TwilioRealm
- Description: (empty text area)

Below these fields is a table for 'SIP Ports' with an 'Add' button above it. The table has the following columns: Address, Port, Transport Protocol, TLS Profile, Allow Anonymous, and Multi Home Addr.

Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
141.146.36.102	5061	TLS	TLSProfile	agents-only	

At the bottom of the table are 'OK' and 'Back' buttons.

Similarly, Please Configure sip-interface for the Avaya side as below:

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

- State:  enable
- Realm ID: AvayaRealm
- Description: (empty text area)

Below these fields is a table for 'SIP Ports' with an 'Add' button above it. The table has the following columns: Address, Port, Transport Protocol, TLS Profile, Allow Anonymous, and Multi Home Addr.

Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
10.232.50.78	5060	UDP		agents-only	

At the bottom of the table are 'OK' and 'Back' buttons.

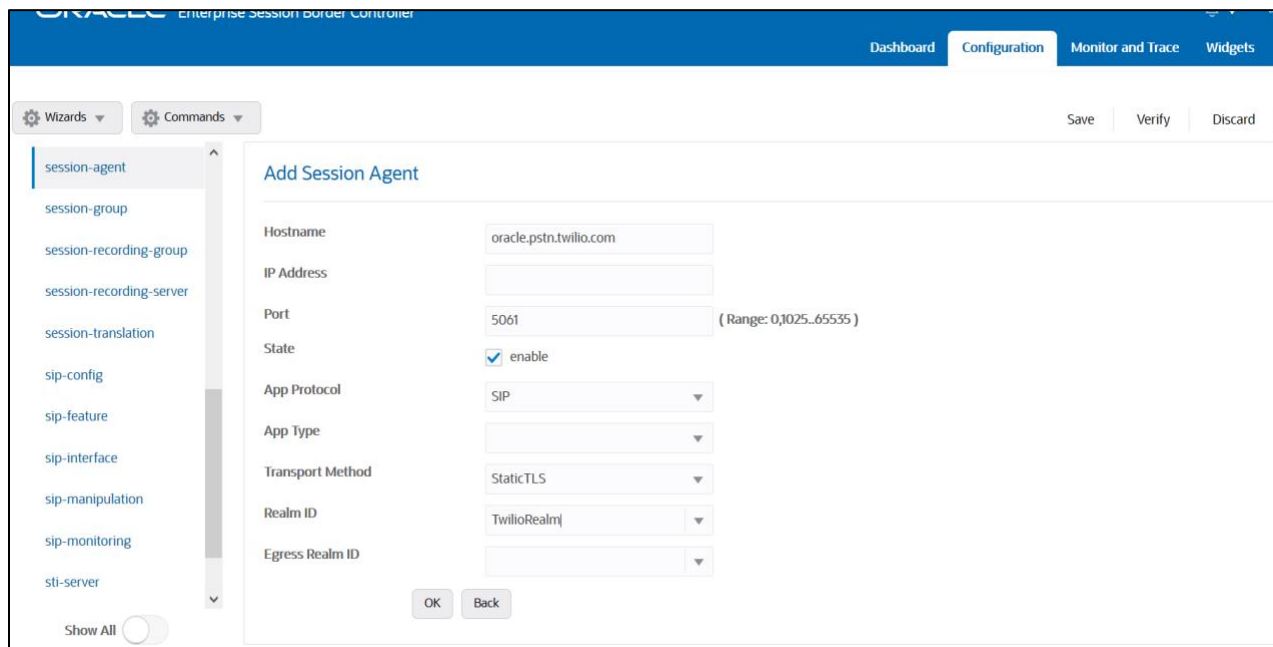
Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

## 6.11. 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.

Go to session-router->Session-Agent and Configure the session-agents for the Twilio Elastic SIP Trunk

- Host name to “oracle.pstn.twilio.com”, port to 5061
- realm-id – needs to match the realm created for the Twilio Elastic SIP Trunk
- transport set to “staticTLS”



The screenshot displays the Oracle Enterprise Session Border Controller (SBC) configuration interface. The main navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar shows a list of configuration categories, with 'session-agent' selected. The main content area is titled 'Add Session Agent' and contains the following fields:

- Hostname: oracle.pstn.twilio.com
- IP Address: (empty)
- Port: 5061 (Range: 0,1025..65535)
- State:  enable
- App Protocol: SIP
- App Type: (empty)
- Transport Method: StaticTLS
- Realm ID: TwilioRealm[
- Egress Realm ID: (empty)

Buttons for 'OK' and 'Back' are located at the bottom of the form. The top right of the configuration area has 'Save', 'Verify', and 'Discard' buttons.

**\*\*NOTE: Connection to Twilio Elastic SIP Trunking is available in multiple geographic edge locations. If you wish to manually connect to a specific geographic edge location that is closest to the location of your communications infrastructure, you may do so by pointing your communications infrastructure to any of the following localized Termination SIP URIs:**

- {example}.pstn.ashburn.twilio.com (North America Virginia)
- {example}.pstn.umatilla.twilio.com (North America Oregon)
- {example}.pstn.dublin.twilio.com (Europe Ireland)
- {example}.pstn.frankfurt.twilio.com (Europe Frankfurt)
- {example}.pstn.singapore.twilio.com (Asia Pacific Singapore)
- {example}.pstn.tokyo.twilio.com (Asia Pacific Tokyo)
- {example}.pstn.sao-paulo.twilio.com (South America São Paulo)
- {example}.pstn.sydney.twilio.com (Asia Pacific Sydney)

[Click here for more information on Twilio Elastic SIP Trunking IP Address](#)

Similarly, configure the session-agents for the Avaya Side as below:

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The main heading is "Add Session Agent". The left sidebar contains a list of configuration categories, with "session-agent" selected. The main content area contains the following fields:

Hostname	10.232.50.127
IP Address	10.232.50.127
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	

Buttons: OK, Back

## 6.12. Configure local-policy

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

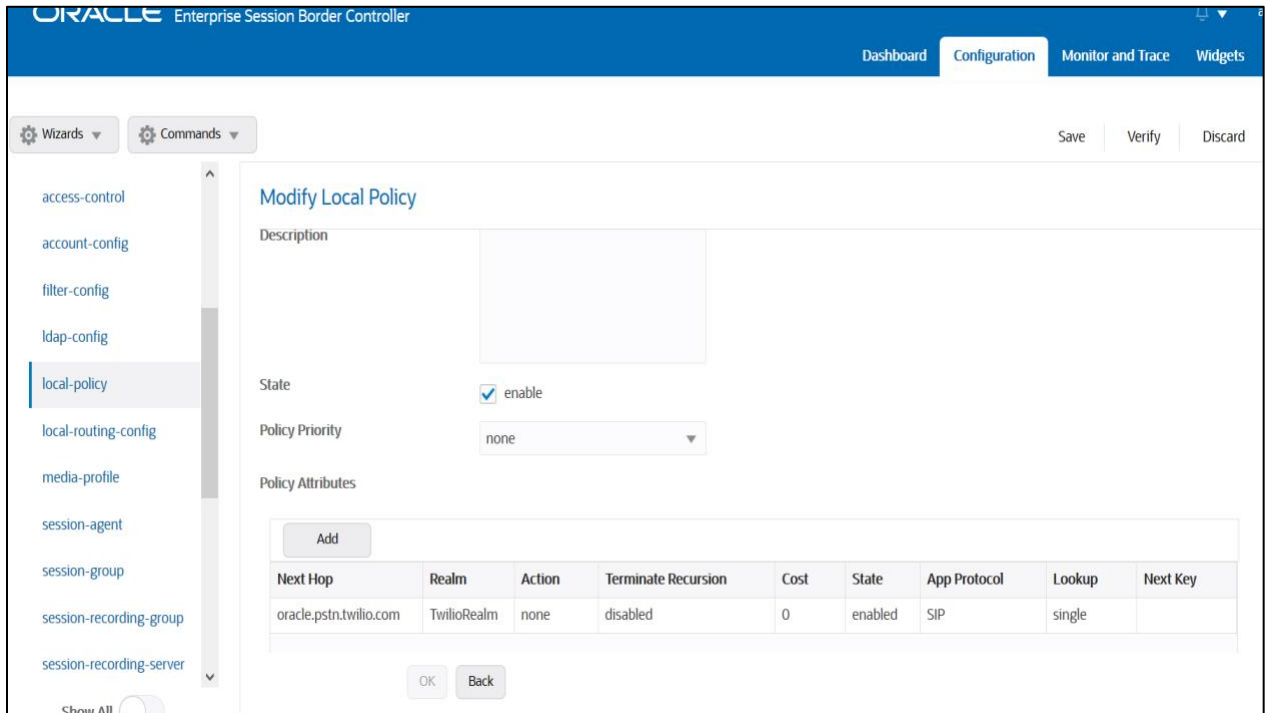
To route the calls from Avaya side to Twilio side, Use the below local –policy

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The main heading is "Modify Local Policy". The left sidebar contains a list of configuration categories, with "local-policy" selected. The main content area contains the following fields:

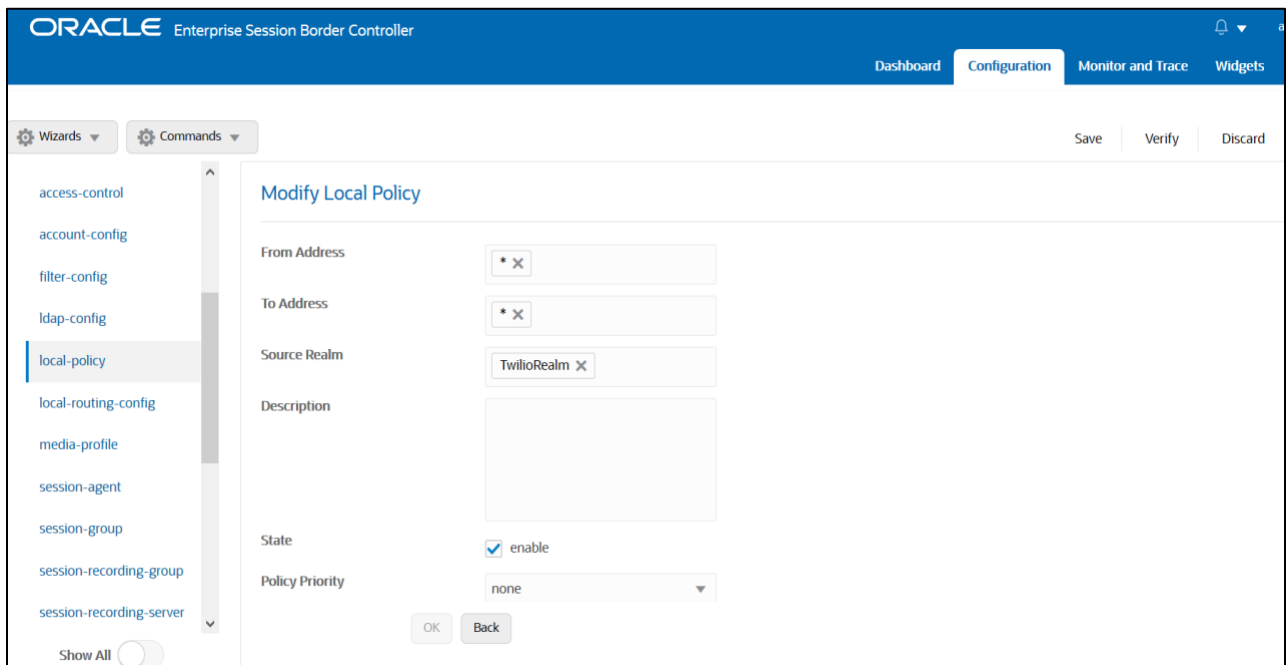
From Address	* X
To Address	* X
Source Realm	AvayaRealm X
Description	
State	<input checked="" type="checkbox"/> enable
Policy Priority	none

Buttons: OK, Back





To route the calls from the Twilio Elastic SIP Trunk side to Avaya side, Use the below local –policy



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar lists various configuration categories, with 'local-policy' selected. The main content area is titled 'Modify Local Policy' and contains the following fields:

- State:** A checkbox labeled 'enable' which is checked.
- Policy Priority:** A dropdown menu currently set to 'none'.
- Policy Attributes:** A table with columns: Next Hop, Realm, Action, Terminate Recursion, Cost, State, App Protocol, Lookup, and Next Key. One row is visible with the following values:
 

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

Buttons for 'Add', 'OK', and 'Back' are also present.

### 6.13. Configure steering-pool

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

Avaya side steering pool.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for adding a steering pool. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar lists various configuration categories, with 'steering-pool' selected. The main content area is titled 'Add Steering Pool' and contains the following fields:

- IP Address:** A text input field containing '10.232.50.78'.
- Start Port:** A text input field containing '25000' with a range indicator '( Range: 1.65535 )'.
- End Port:** A text input field containing '29999' with a range indicator '( Range: 1.65535 )'.
- Realm ID:** A dropdown menu currently set to 'AvayaRealm'.
- Network Interface:** A dropdown menu.

Buttons for 'OK' and 'Back' are also present.

Twilio side steering pool.

The screenshot displays the ORACLE Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar shows a tree view with 'steering-pool' selected. The main content area is titled 'Add Steering Pool' and contains the following fields:

IP Address	<input type="text" value="141.146.36.102"/>
Start Port	<input type="text" value="10000"/> ( Range: 1..65535 )
End Port	<input type="text" value="19999"/> ( Range: 1..65535 )
Realm ID	<input type="text" value="TwilioRealm"/>
Network Interface	<input type="text"/>

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

## 6.14. Configure Ping Response

To simplify the ORACLE SBC configuration, from GA Release SCZ830m1p7, there is a new parameter introduced under the **Session agent** configuration element. The parameter name is **Ping response**.

### **Ping Response:**

When this parameter is 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.

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

session-agent

### Modify Session Agent

Hostname: oracle.pstn.twilio.com

IP Address: [Empty]

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

State:  enable

App Protocol: SIP

App Type: [Empty]

Transport Method: StaticTLS

Realm ID: TwilioRealm

Foreign Realm ID: [Empty]

OK Back

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Wizards Commands Save Verify Discard Se

session-agent

### Modify Session Agent

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]

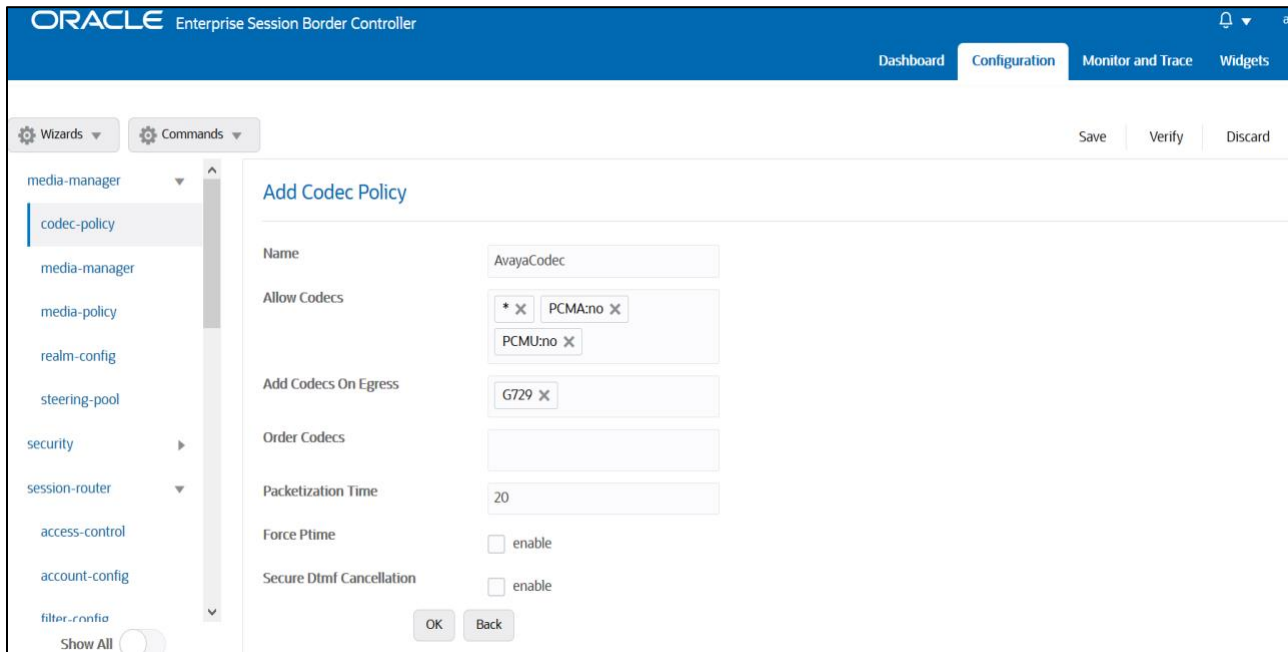
Max Register Sustain Rate: 0 (Range: 0.999999999)

OK Back

## 6.15. Configure 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. **Note: this is an optional config – configure codec policy only if deemed required.** Go to media manager ---- codec policy

Configure the below Codec policy for Avaya Side. **Assign this codec policy to the AvayaRealm.**

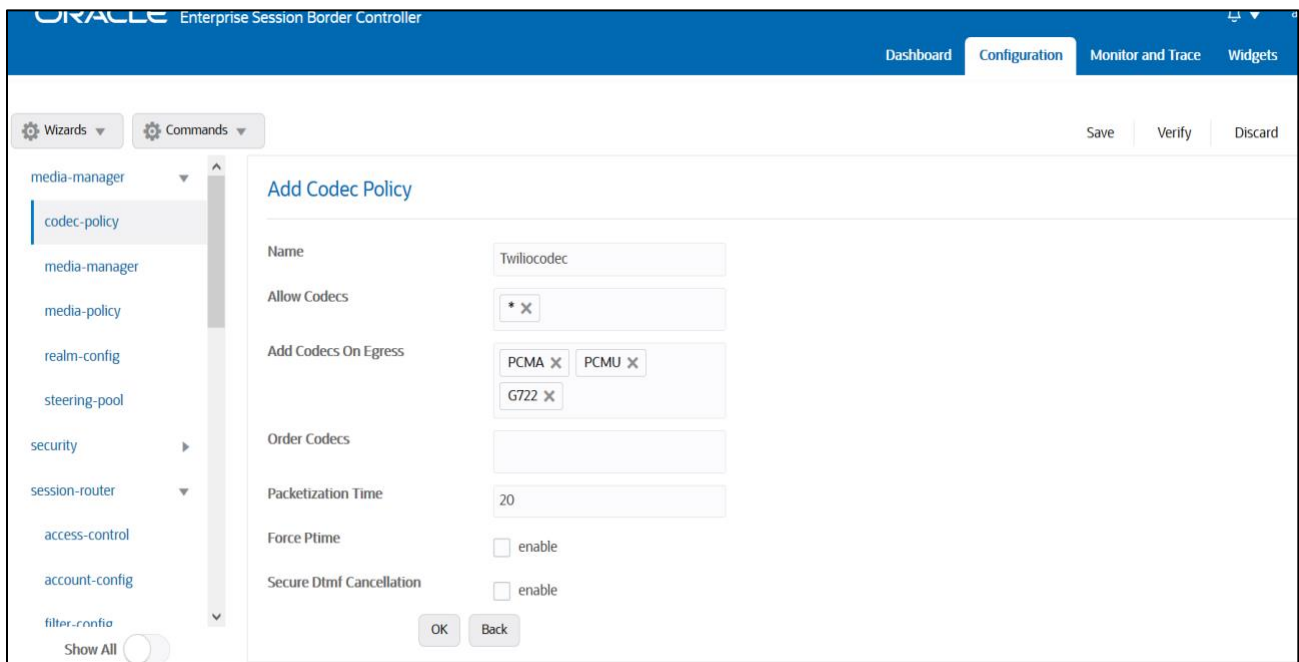


The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists navigation options under 'media-manager', with 'codec-policy' selected. The main area is titled 'Add Codec Policy' and contains the following fields:

- Name: AvayaCodec
- Allow Codecs: PCMA:no, PCMU:no
- Add Codecs On Egress: G729
- Order Codecs: (empty)
- Packetization Time: 20
- Force PTime:  enable
- Secure Dtmf Cancellation:  enable

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

Configure the below Codec policy for Twilio Side, **Assign this codec policy to the TwilioRealm.**



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists navigation options under 'media-manager', with 'codec-policy' selected. The main area is titled 'Add Codec Policy' and contains the following fields:

- Name: Twiliocodec
- Allow Codecs: \*
- Add Codecs On Egress: PCMA, PCMU, G722
- Order Codecs: (empty)
- Packetization Time: 20
- Force PTime:  enable
- Secure Dtmf Cancellation:  enable

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

## 6.16. 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 X, AES\_CM\_128\_HMAC\_SHA1\_32 X
- 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.

## 6.17. Configure Media Security Profile

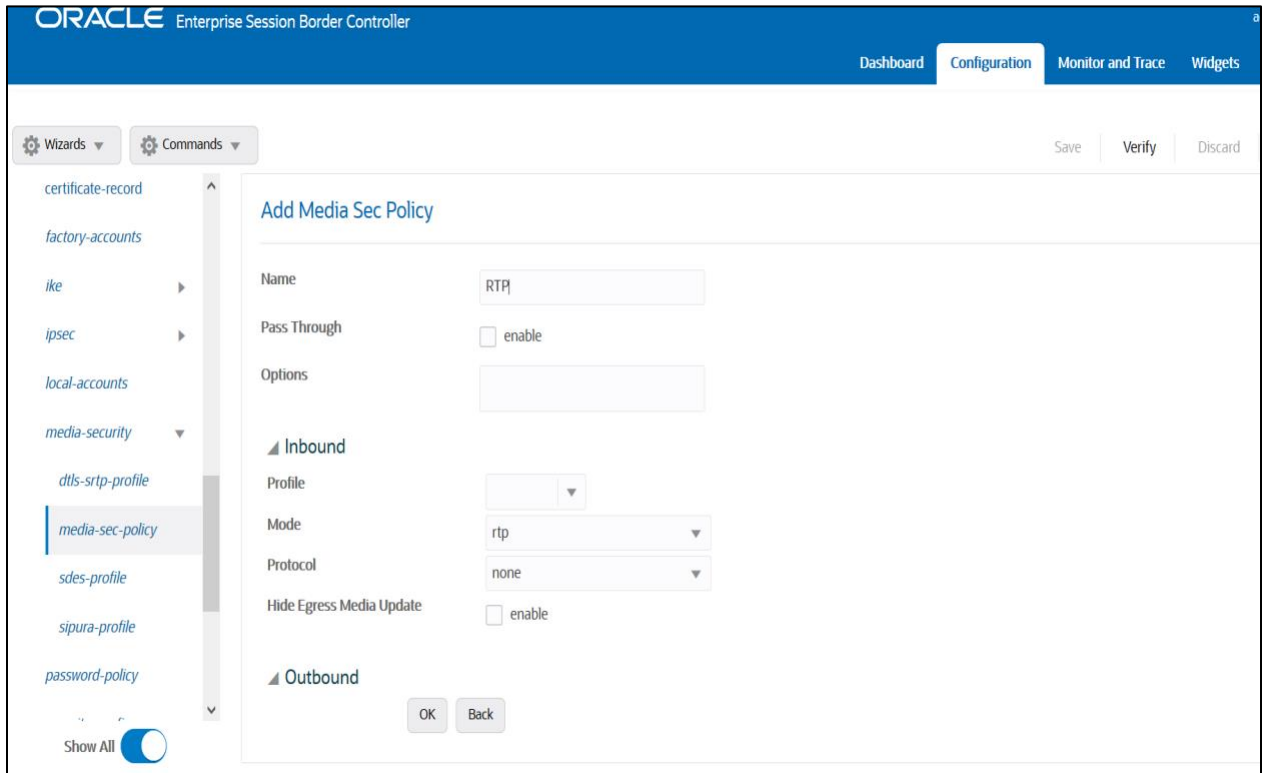
Please go to →Security → Media Security →media Sec policy and create the policy as below:  
Create Media Sec policy with name SDES which will have the sdes profile created above.  
**Assign this media policy to Twilio Realm as it use TLS/SRTP.**

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: (empty)

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 which will use only TCP/UDP as transport protocol. **Assign this media policy to the Avaya Realm.**



## 6.18. 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.

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

Id	addplus
Type	replace
Add String	+
Add Index	0
Delete String	
Delete Index	0 (Range: 0..999999999)

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

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

Id	removeplus
Type	delete
Add String	
Add Index	0
Delete String	+
Delete Index	0 (Range: 0..999999999)

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



## 6.19. 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 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 X
- Rules Called:** removeplus X
- Rules Asserted Id:** (empty)
- Rules Redirect:** (empty)
- Rules Isup Cdpn:** (empty)
- Rules Isup Cgpn:** (empty)
- Rules Isup Gn:** (empty)
- Rules Isup Rdn:** (empty)

Buttons for 'OK' and 'Back' are located at the bottom of the form. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The top right corner has 'Save', 'Verify', and 'Discard' buttons.

Add the below translation rule to Twilio 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:** toTwilio
- Rules Calling:** addPlus X
- Rules Called:** addPlus X
- Rules Asserted Id:** (empty)
- Rules Redirect:** (empty)
- Rules Isup Cdpn:** (empty)
- Rules Isup Cgpn:** (empty)

Buttons for 'OK' and 'Back' are located at the bottom of the form. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The top right corner has 'Save', 'Verify', and 'Discard' buttons.

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  
access-control  
account-config  
filter-config  
ldap-config  
local-policy

### Modify Realm Config

Identifier: AvayaRealm

Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M10:0.4

Media Realm List:

Mm In Realms:  enable

Mm In Network:  enable

Mm Same Ip:  enable

OK Back

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  
access-control  
account-config  
filter-config  
ldap-config  
local-policy

### Modify Realm Config

DTLS SrtP Profile:

SrtP Msm Passthrough:  enable

Class Profile:

In Translationid: toTwilio

Out Translationid: toAvaya

In Manipulationid:

Out Manipulationid:

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

Access Control Trust Level: none

Invalid Signal Threshold: 0 (Range: 0-4294967295)

Maximum Signal Threshold: 0 (Range: 0-4294967295)

OK Back

With this, SBC configuration is complete

## 7. SBC configuration for Avaya Remote Worker

This section of Avaya Remote Worker configuration is included for Avaya remote endpoints that register through the Oracle SBC to the Avaya Session Manager. This would require additional configuration to be configured on the Oracle SBC along with the SIP trunking config as mentioned in the earlier description of the test bed. To complete the particular testing we have configured Avaya endpoints which will register to Avaya Session Manager through the SBC. SBC will handle the calls based on the registration information present in the cache. **Please note that Avaya Remote worker Access side is secured (TLS/SRTP) and Avaya Core side is unsecured (UDP or TCP/RTP)**

In order to achieve the requirement we have made below configuration on the Oracle SBC

Access and Core Realm for Avaya Remote worker  
Steering Pool associated with the Realm for Avaya Remote worker  
Sip-interface associated with the Realm for Avaya Remote worker  
(Optional) A local-policy to route the registration requests from this Realm to the SIP Server.

Note -The local-policy element is optional as we can enable the Route to registrar parameter on the sip-interface config to route the requests to the Registrar.

The registrar host and port is configured in the sip-config element on the SBC. The remote endpoint sends register requests from Avaya Access Realm onto the SBC and then SBC registers these endpoints onto the Avaya Core Realm maintaining the registration cache in its database to route inbound calls to these endpoint.

Below are the snippets from the Oracle SBC Web GUI for the Remote worker configuration.

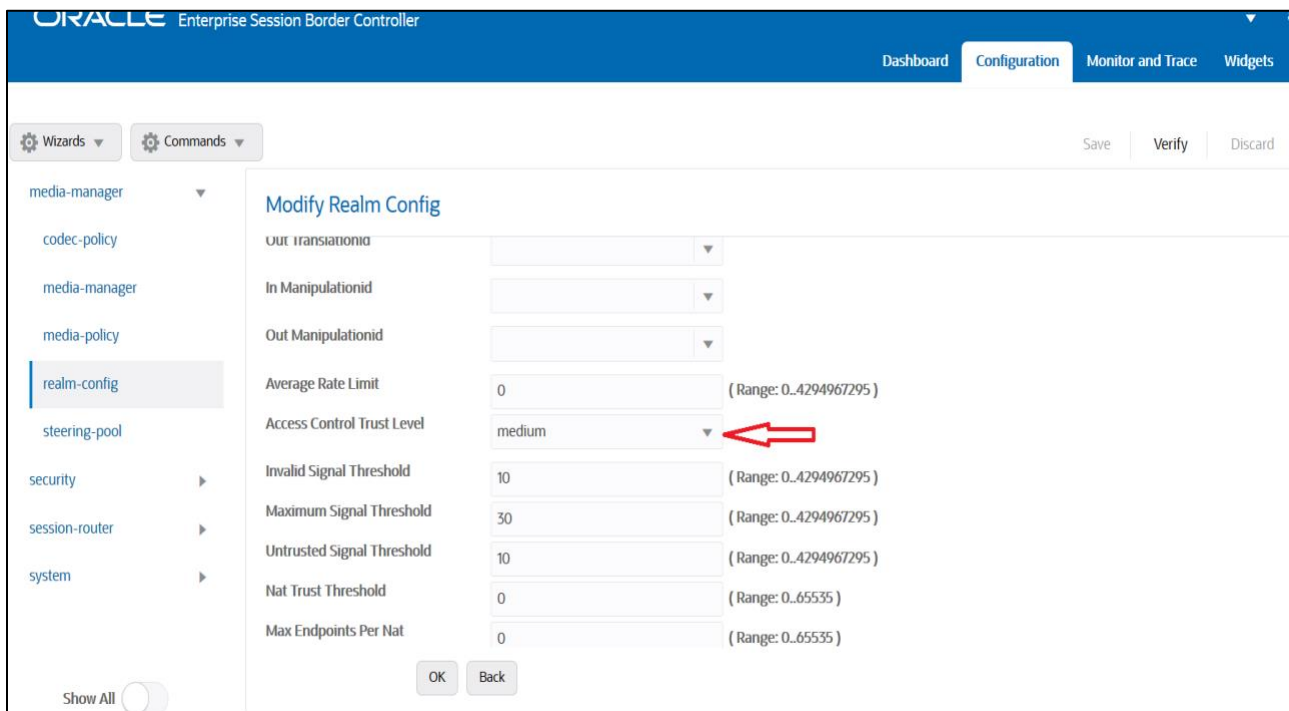
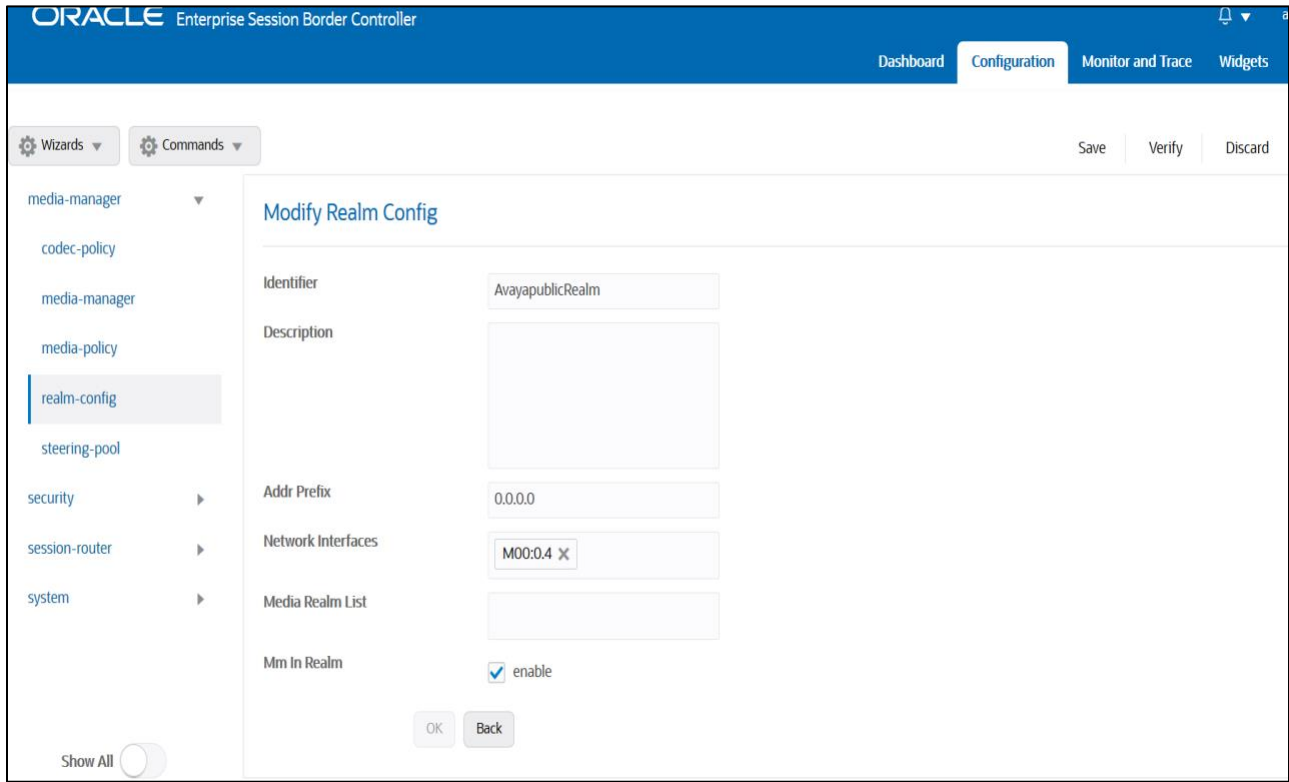
### 7.1. Configure Realms

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.

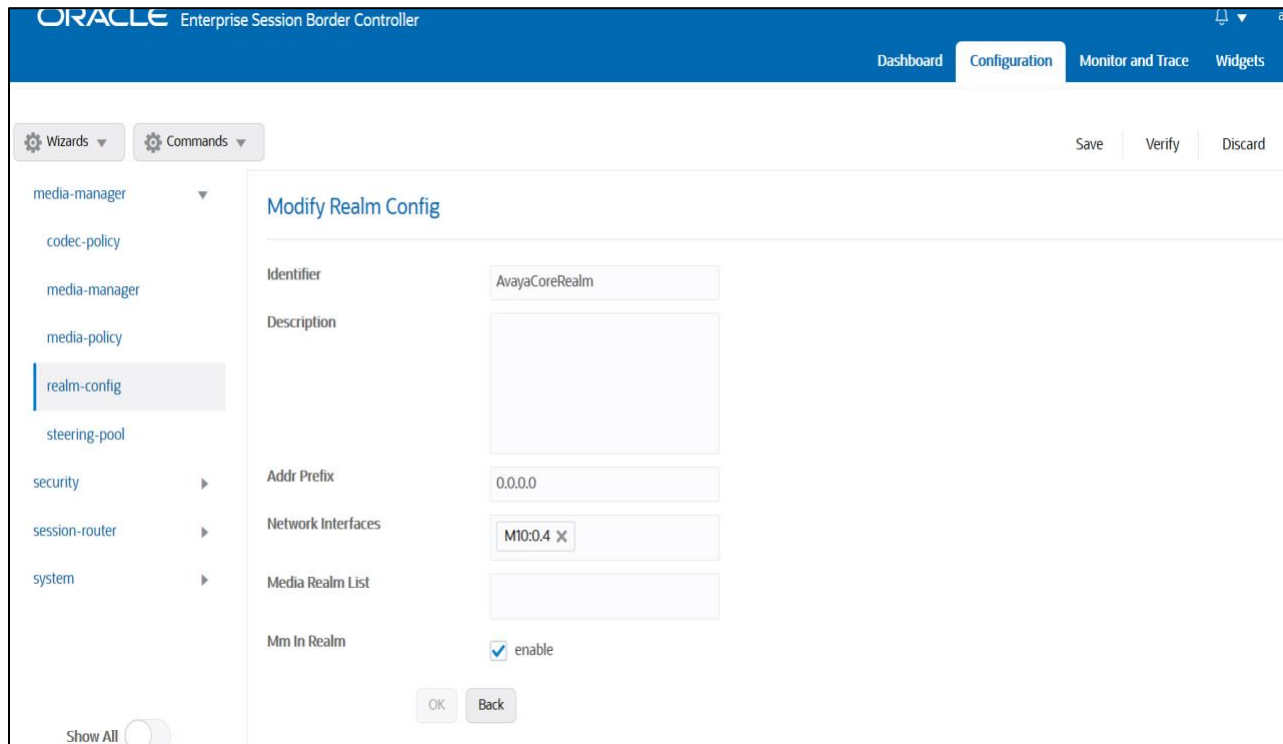
Use the following table as a configuration example for the three realms used in this configuration:

Config Parameter	AvayaAccess Side	Avaya Core Side
Identifier	AvayapublicRealm	AvayaCoreRealm
Network Interface	M00	M10
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FQDN		
Media Sec policy	sdespolicy	RTP
Access Control Trust Level	High	High
Codec-Policy	Twiliocodec	AvayaCodec

In the below example, Realm name is given as AvayapublicRealm for Avaya Access Side. Please set the Access Control Trust Level as medium for this realm



Similarly, Realm name is given as AvayaCoreRealm for Avaya Core side



## 7.2. 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
- reg-cach-mode=from

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

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

### Modify SIP Config

State	<input checked="" type="checkbox"/> enable
Dialog Transparency	<input checked="" type="checkbox"/> enable
Home Realm ID	AvayaCoreRealm
Egress Realm ID	
Nat Mode	None
Registrar Domain	*
Registrar Host	*
Registrar Port	5060 ( Range: 0,3025..65535 )
Init Timer	500 ( Range: 0..4294967295 )

OK Delete

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

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

### Modify SIP Config

Trans Expire	32 ( Range: 0..4294967295 )
Initial Inv Trans Expire	0 ( Range: 0..999999999 )
Invite Expire	180 ( Range: 0..4294967295 )
Session Max Life Limit	0
Enforcement Profile	
Red Max Trans	10000 ( Range: 0..50000 )
Options	max-udp-length=0 ✕ reg-cache-mode=from ✕
SPL Options	
SIP Message Len	4096 ( Range: 0..65535 )

OK Delete

### 7.3. 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 9. which takes care of Access Realm. 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 settings include Flow Time Limit (86400), Initial Guard Timer (300), Subsq Guard Timer (300), TCP Flow Time Limit (86400), TCP Initial Guard Timer (300), TCP Subsq Guard Timer (300), Hnt Rtcp (unchecked), Algd Log Level (NOTICE), and Mbcd Log Level (NOTICE). Range constraints are provided for several numeric fields.

Parameter	Value	Range
State	<input checked="" type="checkbox"/> enable	
Flow Time Limit	86400	( Range: 0..4294967295 )
Initial Guard Timer	300	( Range: 0..4294967295 )
Subsq Guard Timer	300	( Range: 0..4294967295 )
TCP Flow Time Limit	86400	( Range: 0..4294967295 )
TCP Initial Guard Timer	300	( Range: 0..4294967295 )
TCP Subsq Guard Timer	300	( Range: 0..4294967295 )
Hnt Rtcp	<input type="checkbox"/> enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	

The screenshot shows the 'Modify Media Manager' configuration page with additional signaling parameters. The 'Media Policing' checkbox is checked and labeled 'enable'. The 'Max Untrusted Signaling' and 'Min Untrusted Signaling' fields are both set to 9, with red arrows pointing to their respective range constraints (0..100). Other settings include Red Sync Comp Time (1000), Max Signaling Bandwidth (10000000), Tolerance Window (30), Untrusted Drop Threshold (0), Trusted Drop Threshold (0), Acl Monitor Window (30), and Trap On Demote To Deny (unchecked). Range constraints are provided for several numeric fields.

Parameter	Value	Range
Red Sync Comp Time	1000	( Range: 0..4294967295 )
Media Policing	<input checked="" type="checkbox"/> enable	
Max Signaling Bandwidth	10000000	( Range: 71000..100000000 )
Max Untrusted Signaling	9	( Range: 0..100 )
Min Untrusted Signaling	9	( Range: 0..100 )
Tolerance Window	30	( Range: 0..4294967295 )
Untrusted Drop Threshold	0	( Range: 0..100 )
Trusted Drop Threshold	0	( Range: 0..100 )
Acl Monitor Window	30	( Range: 5..3600 )
Trap On Demote To Deny	<input type="checkbox"/> enable	

## 7.4. 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.

Please Configure sip-interface for the for Avaya Access side as below:

- Tls-profile needs to match the name of the tls-profile created earlier.
- Set allow-anonymous to Registered to ensure traffic to this sip-interface only comes from the registered user.
- Set NAT traversal to always for the remote workers to register.
- Enable Registration Caching and Route to Register

The screenshot shows the Oracle Enterprise Session Border Controller configuration page for a SIP interface. The page title is "Modify SIP Interface". The interface includes a navigation menu on the left with options like "local-routing-config", "media-profile", "session-agent", "session-group", "session-recording-group", "session-recording-server", "session-translation", "sip-config", "sip-feature", "sip-interface" (selected), and "sip-manipulation". The main configuration area has the following fields:

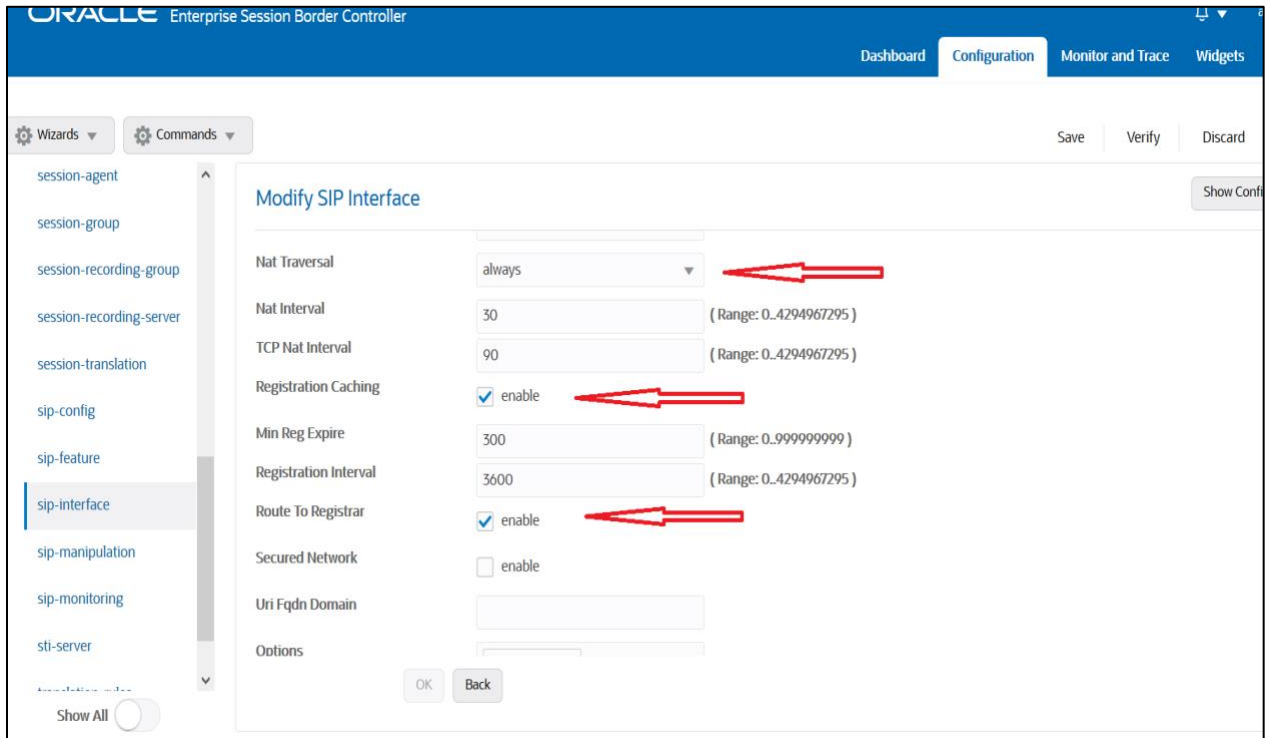
- State:  enable
- Realm ID: AvayapublicRealm
- Description: (empty text area)

Below these fields is a table for SIP Ports:

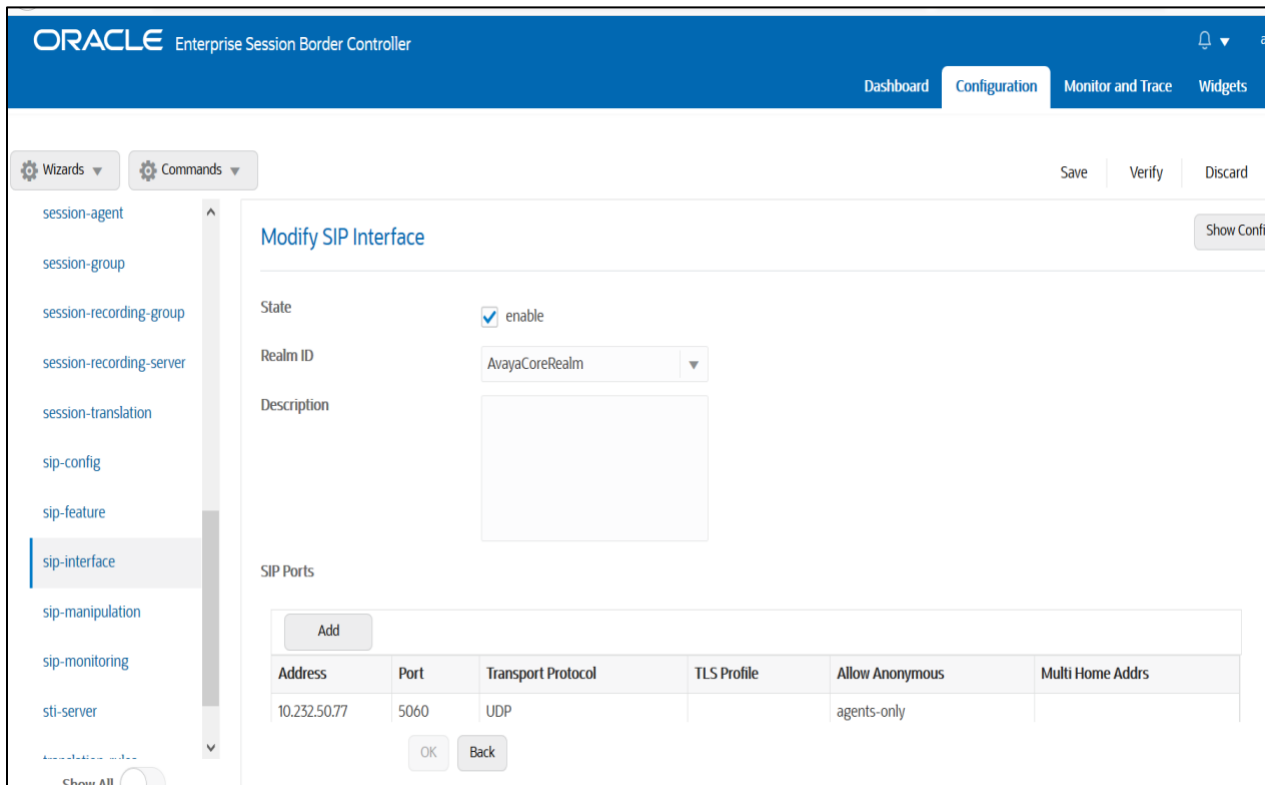
SIP Ports					
Add					
Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
141.146.36.77	5061	TLS	TLSProfile	registered	

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





Similarly, Please Configure sip-interface for the Avaya Core side as below:

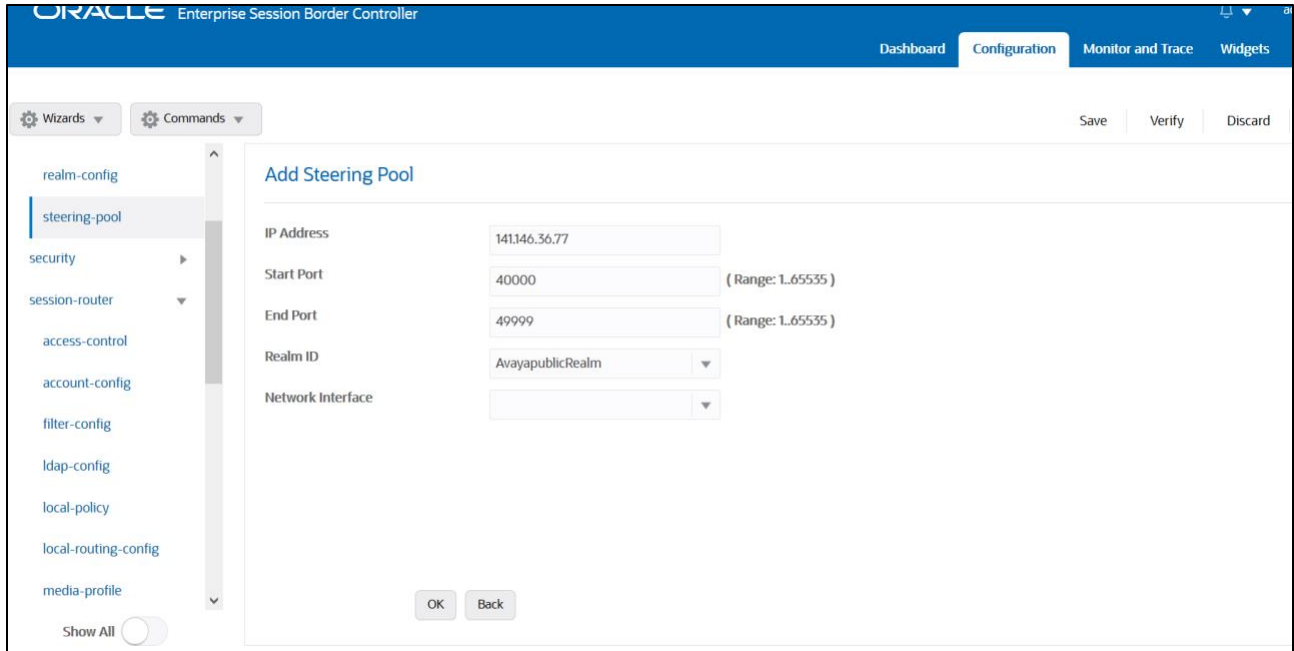


Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

## 7.5. Configure steering-pool

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

Avaya Access side steering pool.

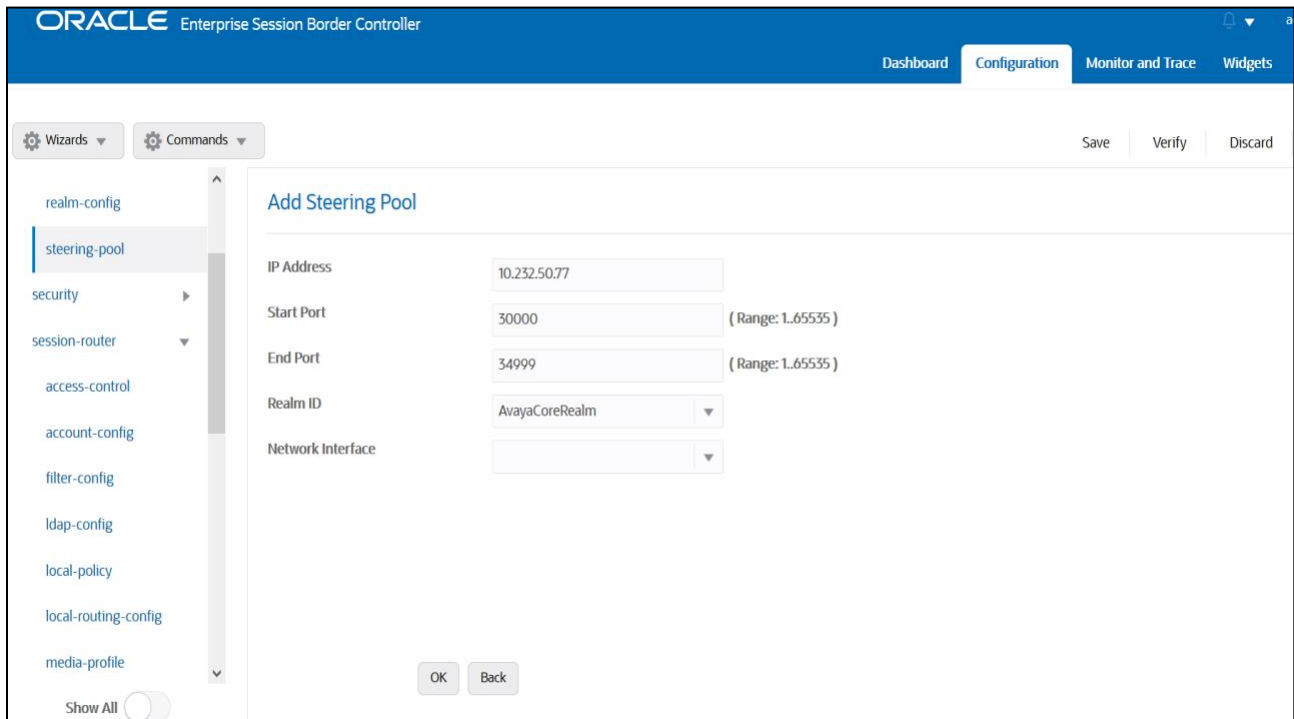


The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active. The left sidebar shows a tree view with 'steering-pool' selected. The main area is titled 'Add Steering Pool' and contains the following fields:

Field	Value	Notes
IP Address	141.146.36.77	
Start Port	40000	( Range: 1.65535 )
End Port	49999	( Range: 1.65535 )
Realm ID	AvayapublicRealm	Dropdown menu
Network Interface		Dropdown menu

Buttons: OK, Back, Save, Verify, Discard.

Avaya Core side steering pool.



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active. The left sidebar shows a tree view with 'steering-pool' selected. The main area is titled 'Add Steering Pool' and contains the following fields:

Field	Value	Notes
IP Address	10.232.50.77	
Start Port	30000	( Range: 1.65535 )
End Port	34999	( Range: 1.65535 )
Realm ID	AvayaCoreRealm	Dropdown menu
Network Interface		Dropdown menu

Buttons: OK, Back, Save, Verify, Discard.

## 7.6. Configure local-policy (Optional)

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

To route the calls from Avaya Access side to Avaya Core side and vice versa, Use the below local –policy

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'local-policy' option is selected in the left-hand navigation menu. The main configuration area is titled 'Modify Local Policy' and includes the following fields:

- From Address:** A text input field with a clear button (X).
- To Address:** A text input field with a clear button (X).
- Source Realm:** A dropdown menu with 'AvayapublicRealm' selected and a clear button (X).
- Description:** A large empty text area.
- State:** A checkbox labeled 'enable' which is checked.
- Policy Priority:** A dropdown menu with 'none' selected.

At the bottom of the configuration area are 'OK' and 'Back' buttons. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'.

This screenshot shows the same 'Modify Local Policy' configuration page, but with the 'Policy Attributes' section expanded. It features a table with the following data:

Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
10.232.50.127	AvayaCoreRealm	none	disabled	0	enabled	SIP	single	

The 'Policy Attributes' section also includes an 'Add' button above the table and 'OK' and 'Back' buttons at the bottom. The rest of the configuration fields (From Address, To Address, Source Realm, Description, State, Policy Priority) are visible but partially obscured or not the focus of this view.


## 8. Existing SBC configuration

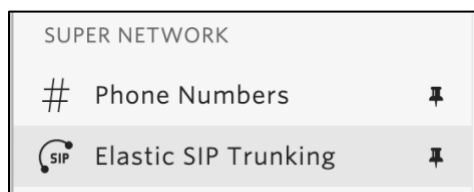
If the SBC being used is an existing SBC with functional configuration, following configuration elements are required:

- [New realm-config](#)
- [Configuring a certificate for SBC Interface](#)
- [TLS-Profile](#)
- [New sip-interface](#)
- [New session-agent](#)
- [New steering-pools](#)
- [New local-policy](#)
- [New Codec Policy](#)
- [SDES Profile](#)
- [Media-sec-Policy](#)
- [New Translation Rules](#)
- [Session Translation Rules](#)

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

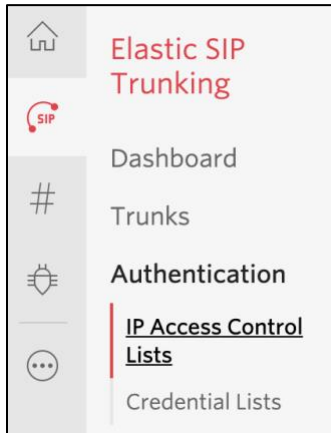
## 9. Twilio Elastic SIP Trunking Configuration

From your [Twilio Console](#), navigate to the [Elastic SIP Trunking](#) area (or click on the  icon on the left vertical navigation bar).

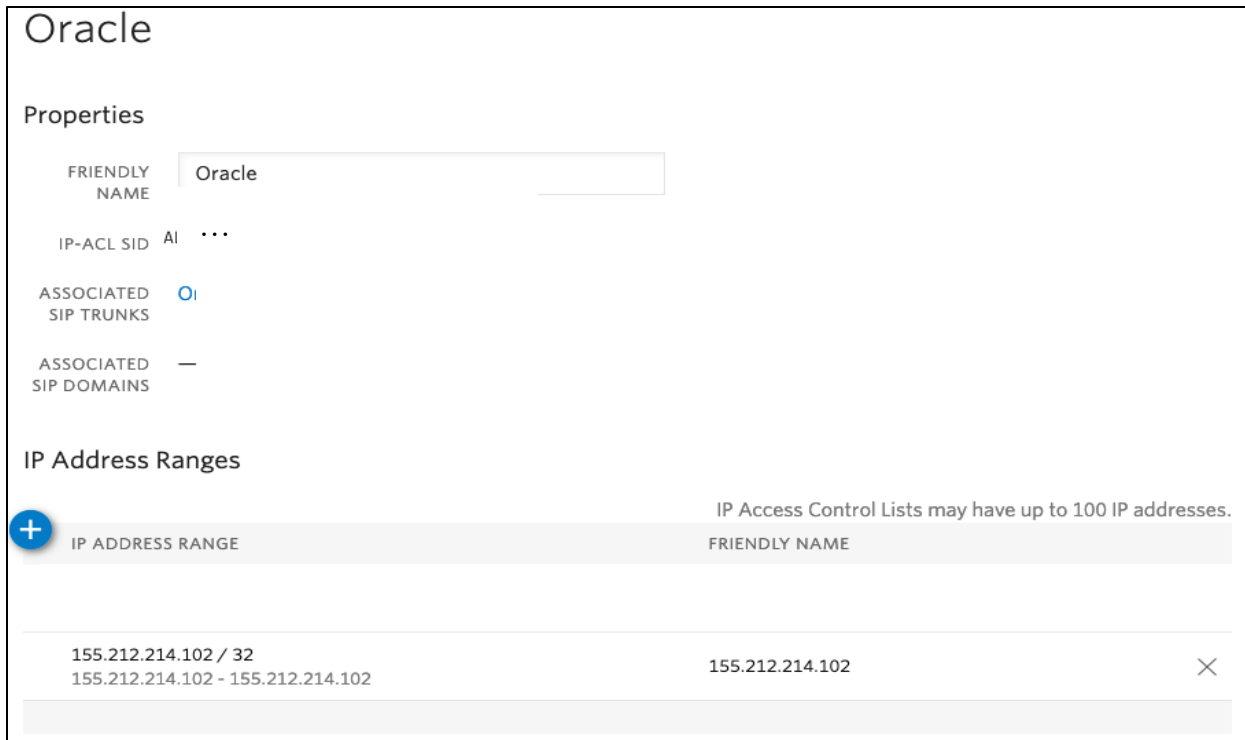


## 9.1. Create an IP-ACL rule

Click on [Authentication](#) in the left navigation, and then click on [IP Access Control Lists](#).



Create a new IP-ACL, for example call it "Oracle" and add your SBCs IP addresses.



## 9.2. Create a new Trunk

For each geographical region desired (e.g., North America, Europe), create a new Elastic SIP Trunk.

Now click on **Trunks** again on the left vertical navigation bar, and create a new Trunk.

Create A New SIP Trunk ✕

Name your new SIP Trunk, then configure it in the following steps.

FRIENDLY NAME

Under the **General Settings** you can enable different features as desired.

### Features

To learn more about SIP Trunking features, please [see our user documentation](#). 🔗

**Call Recording** ⓘ

**Enabled** Calls will be recorded.

**Call Recording**

**Recording Trim**

**Disabled** Silence will not be trimmed from recording

**Secure Trunking** ⓘ

**Enabled** TLS must be used to encrypt SIP messages on port 5061, and SRTP must be used to encrypt the media packets. Any non-encrypted calls will be rejected

**Call Transfer (SIP REFER)** ⓘ

**Enabled** Twilio will consume an incoming SIP REFER from your communications infrastructure and create an INVITE message to the address in the Refer-To header

**Enable PSTN Transfer** ⓘ  
Allow Call Transfers to the PSTN via your Trunk.

**Symmetric RTP** ⓘ

**Enabled** Twilio will detect where the remote RTP stream is coming from and start sending RTP to that destination instead of the one negotiated in the SDP

▶ **Additional Features**

In the **Termination** section, select a Termination SIP URI.

### Termination URI

Configure a SIP Domain Name to uniquely identify your Termination SIP URI for this Trunk. This URI will be used by your communications infrastructure to direct SIP traffic towards Twilio. Be sure to select a localized SIP URI to ensure your traffic takes the lowest latency path. If a localized version isn't selected, then your traffic will be sent to US1. [Learn more about Termination Settings](#) ↗

TERMINATION SIP URI

[Show Localized URIs](#)

Click on "Show localized URI's" and copy and paste this information as you will use this on your SBC to configure your Trunk.


NORTH AMERICA VIRGINIA	oracle.pstn.ashburn.twilio.com
NORTH AMERICA OREGON	oracle.pstn.umatilla.twilio.com
EUROPE DUBLIN	oracle.pstn.dublin.twilio.com
EUROPE FRANKFURT	oracle.pstn.frankfurt.twilio.com
SOUTH AMERICA SAO PAULO	oracle.pstn.sao-paulo.twilio.com
ASIA PACIFIC SINGAPORE	oracle.pstn.singapore.twilio.com
ASIA PACIFIC TOKYO	oracle.pstn.tokyo.twilio.com
ASIA PACIFIC SYDNEY	oracle.pstn.sydney.twilio.com


OR

Assign the IP ACL ("Oracle") that you created in the previous step.

### Authentication [View all Authentication lists](#)

The following IP ACLs and Credential Lists will be used to authenticate the INVITE for termination calls inbound to Twilio.

IP ACCESS CONTROL LISTS  × ▾ 

CREDENTIAL LISTS  ▾ 

In the **Origination** section, we'll need to add Origination URI's to route traffic towards your Oracle SBC. The recommended practice is to configure a redundant mesh per geographic region (in this context a region is one of North America, Europe, etc.). In this case, we configure two Origination URIs, each egressing from a different Twilio Edge.

Click on 'Add New Origination URI', we'll depict the configuration for North America:

### Add Origination URL

ORIGINATION SIP URI

PRIORITY   
Priority ranks the importance of the URI. Values range from 0 to 65535, where the lowest number represents the highest importance.

WEIGHT   
Weight is used to determine the share of load when more than one URI has the same priority. Its values range from 1 to 65535. The higher the value, the more load a URI is given.

ENABLED

Continue to add the other Origination URIs, so you have the following configuration:

#### Origination URIs

Configure the IP address (or FQDN) of the network element entry point into your communications infrastructure (e.g. IP-PBX, SBC).

Show more about provisioning for high service availability

ORIGINATION URI	PRIORITY	WEIGHT	ENABLED	
sip:155.212.214.102;edge=ashburn	10	10	✓	×
sip:155.212.214.103;edge=umatilla	20	10	✓	×

In this example, Origination traffic is first routed via Twilio's Ashburn edge, if that fails then we'll route from Twilio's Umatilla edge.



### 9.3. Associate Phone Numbers on your Trunk

In the **Numbers** section of your Trunk, add the Phone Numbers that you want to associate with each Trunk. Remember to associate the Numbers from a given country in the right Trunk. For example, associate US & Canada Numbers with the North American Trunk and European Numbers with the European Trunk etc.

## Numbers [View my Addresses](#)

**Emergency Calling Update:** Each number must be associated with an emergency address with matching ISO Country. Please select numbers to enable from one country at a time.

+

Number

Filter

Choose Action ▼

NUMBER	FRIENDLY NAME	COUNTRY	EMERGENCY CALLING STATUS	EMERGENCY ADDRESS	<input type="checkbox"/>
+18 07904044	(850) 790-4044	US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	<input type="checkbox"/>
+16 092203033	(689) 220-3033	US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	<input type="checkbox"/>
+17 071 05055	(749) 210-5055	US	Disabled		<input type="checkbox"/>

## 10. Verification of Sample Call flows

Once the configuration is complete, we can try making sample calls and can check the signaling path between Twilio Elastic Sip Trunk (PSTN Users) and Avaya Users

1. Make Call from Avaya user to the Twilio Elastic Sip Trunk and check the call flow.  
The calls flow from 10.232.50.78 (Avaya SIP Interface) to 141.146.36.102 (Twilio Elastic SIP Trunking Interface) and to Twilio Session Agent and the call reaches the PSTN user after that.

Session List: 8066255B-IDA7-EB11-942F-1A3881DA89A7@10.232.50.2

**[+] Session Summary**

Time	10.232.50.127	10.232.50.78	141.146.36.102	54.172.60.0
2021-04-29 01:54:34.946		→ INVITE (324)		
2021-04-29 01:54:34.947	←	Status:100 (324)		
2021-04-29 01:54:34.960			→ MEDIA FLOW ADD, ID=16777217, DIRECTION=CALLING	
2021-04-29 01:54:34.960			→ MEDIA FLOW ADD, ID=16777218, DIRECTION=CALLED	
2021-04-29 01:54:34.964			→ EGRESS ROUTE, TYPE=, NEXT HOP=sip:+917338391101@aura.com	
2021-04-29 01:54:34.964				→ INVITE (324)
2021-04-29 01:54:35.061				← Status:100 (324)
2021-04-29 01:54:36.202				← Status:183 (324)
2021-04-29 01:54:36.219				→ MEDIA FLOW MODIFY, ID=16777218, DIRECTION=CALLED
2021-04-29 01:54:36.220				→ MEDIA FLOW MODIFY, ID=16777217, DIRECTION=CALLING
2021-04-29 01:54:36.225	←	Status:183 (324)		
2021-04-29 01:54:45.685				← Status:200 (324)
2021-04-29 01:54:45.695	←	Status:200 (324)		
2021-04-29 01:54:45.711	→	ACK (324)		
2021-04-29 01:54:45.714				→ ACK (324)

Buttons: Refresh, Export diagram, Export session details

Session List: 8066255B-IDA7-EB11-942F-1A3881DA89A7@10.232.50.2

2021-04-29 01:54:34.964				→ INVITE (324)
2021-04-29 01:54:35.061				← Status:100 (324)
2021-04-29 01:54:36.202				← Status:183 (324)
2021-04-29 01:54:36.219				→ MEDIA FLOW MODIFY, ID=16777218, DIRECTION=CALLED
2021-04-29 01:54:36.220				→ MEDIA FLOW MODIFY, ID=16777217, DIRECTION=CALLING
2021-04-29 01:54:36.225	←	Status:183 (324)		
2021-04-29 01:54:45.685				← Status:200 (324)
2021-04-29 01:54:45.695	←	Status:200 (324)		
2021-04-29 01:54:45.711	→	ACK (324)		
2021-04-29 01:54:45.714				→ ACK (324)
2021-04-29 01:55:01.410				← BYE (1)
2021-04-29 01:55:01.413	→	Status:200 (1)		
2021-04-29 01:55:01.433				→ Status:200 (1)
2021-04-29 01:55:01.437				→ MEDIA FLOW DELETE, ID=16777217, DIRECTION=CALLING
2021-04-29 01:55:01.438				→ MEDIA FLOW DELETE, ID=16777218, DIRECTION=CALLED

**Details for INVITE (324)**

Buttons: Refresh, Export diagram, Export session details

- When we register Avaya Remote Worker, we can see the registration happening through Oracle SBC to Avaya Session Manager as given below.

Oracle Enterprise Session Border Controller - Monitor and Trace

Registration List: 020055abfec34ebc8072ea7389c42df6

[+] Session Summary			
122.166.131.210	141.146.36.77	10.232.50.77	10.232.50.127
2021-04-29 02:00:48.342	→ REGISTER (34168) →		
2021-04-29 02:00:48.345	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:10.232.50.127:5060		
2021-04-29 02:00:48.345			→ REGISTER (34168) →
2021-04-29 02:00:48.352			← Status:401 (34168) ←
2021-04-29 02:00:48.354	← Status:401 (34168) ←		
2021-04-29 02:00:48.695	→ REGISTER (34169) →		
2021-04-29 02:00:48.698	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:10.232.50.127:5060		
2021-04-29 02:00:48.698			→ REGISTER (34169) →
2021-04-29 02:00:48.708			← Status:200 (34169) ←
2021-04-29 02:00:48.710	← Status:200 (34169) ←		

SIP Message Details

Buttons: Refresh, Export diagram, Export session details

- Make Call from Avaya Remote user to the Twilio Elastic Sip Trunk user and check the call flow. Now, there will be 2 call legs (hair pinned call) as the call reaches Avaya Session Manager first and then reaches Twilio trunk user after that as given below.

Oracle Enterprise Session Border Controller - Monitor and Trace

Session List: a6418588e4074f01885c03591974b88f

[+] Session Summary			
122.166.131.210	141.146.36.77	10.232.50.77	10.232.50.127
2021-04-29 02:02:27.290	→ INVITE (30056) →		
2021-04-29 02:02:27.290	← Status:100 (30056) ←		
2021-04-29 02:02:27.305	MEDIA FLOW ADD, ID=33554433, DIRECTION=CALLING		
2021-04-29 02:02:27.306	MEDIA FLOW ADD, ID=33554434, DIRECTION=CALLED		
2021-04-29 02:02:27.312	EGRESS ROUTE, TYPE=, NEXT HOP=< sip:919535410905@aura.com;transport=tl>		
2021-04-29 02:02:27.312			→ INVITE (30056) →
2021-04-29 02:02:27.319			← Status:100 (30056) ←
2021-04-29 02:02:27.323			← Status:407 (30056) ←
2021-04-29 02:02:27.324			→ ACK (30056) →
2021-04-29 02:02:27.328	← Status:407 (30056) ←		
2021-04-29 02:02:28.000	→ ACK (30056) →		
2021-04-29 02:02:28.048	→ INVITE (30057) →		
2021-04-29 02:02:28.049	← Status:100 (30057) ←		
2021-04-29 02:02:28.064	EGRESS ROUTE, TYPE=, NEXT HOP=< sip:919535410905@aura.com;transport=tl>		
2021-04-29 02:02:28.064			→ INVITE (30057) →

Buttons: Refresh, Export diagram, Export session details

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Sessions Registrations Subscriptions Notable Events

Session List a6418588e4074f01885c03591974b88f x

[+] Session Summary			
10.232.50.127	10.232.50.78	141.146.36.102	54.172.60.0
2021-04-29 02:02:28.083	→ INVITE (30057)	→	
2021-04-29 02:02:28.084	← Status:100 (30057)	←	
2021-04-29 02:02:28.099	MEDIA FLOW ADD, ID=50331649, DIRECTION=CALLING		
2021-04-29 02:02:28.100	MEDIA FLOW HAIRPIN		
2021-04-29 02:02:28.100	MEDIA FLOW ADD, ID=50331650, DIRECTION=CALLED		
2021-04-29 02:02:28.103	EGRESS ROUTE, TYPE=, NEXT HOP=<sip:+919535410905@aura.com;transport=tl>		
2021-04-29 02:02:28.103		→ INVITE (30057)	→
2021-04-29 02:02:28.198		← Status:100 (30057)	←
2021-04-29 02:02:29.065		← Status:183 (30057)	←
2021-04-29 02:02:29.086	MEDIA FLOW MODIFY, ID=50331650, DIRECTION=CALLED		
2021-04-29 02:02:29.087	MEDIA FLOW MODIFY, ID=50331649, DIRECTION=CALLING		
2021-04-29 02:02:29.092	← Status:183 (30057)	←	
2021-04-29 02:02:40.318			← Status:200 (30057)
2021-04-29 02:02:40.330	← Status:200 (30057)	←	
2021-04-29 02:02:40.709	→ ACK (30057)	→	

Refresh Export diagram Export session details

- Make Call from the Twilio Elastic Sip Trunk to Avaya User and check the call flow. The calls flow from 141.146.36.102 (Twilio Elastic SIP Trunking Interface) to 10.232.50.78 (Avaya SIP Interface) and the call reaches the Avaya user after that.

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Sessions Registrations Subscriptions Notable Events

Session List 49451ffc697c96a9253e97df44043fe9@0.0.0.0 x

[+] Session Summary			
54.172.60.2	141.146.36.102	10.232.50.78	10.232.50.127
2021-04-29 02:25:43.377	→ INVITE (541073)	→	
2021-04-29 02:25:43.378	← Status:100 (541073)	←	
2021-04-29 02:25:43.391	MEDIA FLOW ADD, ID=50331649, DIRECTION=CALLING		
2021-04-29 02:25:43.392	MEDIA FLOW ADD, ID=50331650, DIRECTION=CALLED		
2021-04-29 02:25:43.394	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:+17692105055@10.232.50.127:5060		
2021-04-29 02:25:43.394		→ INVITE (541073)	→
2021-04-29 02:25:43.401		← Status:100 (541073)	←
2021-04-29 02:25:43.462		← Status:180 (541073)	←
2021-04-29 02:25:43.467	← Status:180 (541073)	←	
2021-04-29 02:26:02.699		← Status:200 (541073)	←
2021-04-29 02:26:02.718	MEDIA FLOW MODIFY, ID=50331650, DIRECTION=CALLED		
2021-04-29 02:26:02.719	MEDIA FLOW MODIFY, ID=50331649, DIRECTION=CALLING		
2021-04-29 02:26:02.723	← Status:200 (541073)	←	
2021-04-29 02:26:02.827	→ ACK (541073)	→	
2021-04-29 02:26:02.830			→ ACK (541073)

Refresh Export diagram Export session details

- Make Call from Twilio Elastic Sip Trunk user to Avaya Remote user and check the call flow. Now, there will be 2 call legs (hair pinned call) as the call reaches Avaya Session Manager first and then reaches Avaya Remote user after that as given below.

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Sessions

Registrations

Subscriptions

Notable Events

Session List [4f529a309690e421dad38e84446572a4@0.0.0.0](#)

[*] Session Summary			
54.172.60.1	141.146.36.102	10.232.50.78	10.232.50.127
2021-04-29 02:14:06.881	→ INVITE (105203)	→	
2021-04-29 02:14:06.882	← Status:100 (105203)	←	
2021-04-29 02:14:06.898	MEDIA FLOW ADD, ID=16777217, DIRECTION=CALLING		
2021-04-29 02:14:06.898	MEDIA FLOW ADD, ID=16777218, DIRECTION=CALLED		
2021-04-29 02:14:06.900	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:+18507904044@10.232.50.127:5060		
2021-04-29 02:14:06.900		→ INVITE (105203)	→
2021-04-29 02:14:06.908		← Status:100 (105203)	←
2021-04-29 02:14:06.936	MEDIA FLOW HAIRPIN		
2021-04-29 02:14:07.687		← Status:180 (105203)	←
2021-04-29 02:14:07.692	← Status:180 (105203)	←	
2021-04-29 02:14:12.049		← Status:200 (105203)	←
2021-04-29 02:14:12.068	MEDIA FLOW MODIFY, ID=16777218, DIRECTION=CALLED		
2021-04-29 02:14:12.068	MEDIA FLOW MODIFY, ID=16777217, DIRECTION=CALLING		
2021-04-29 02:14:12.073	← Status:200 (105203)	←	
2021-04-29 02:14:12.177	→ ACK (105203)	→	

Refresh Export diagram Export session details

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Sessions

Registrations

Subscriptions

Notable Events

Session List [4f529a309690e421dad38e84446572a4@0.0.0.0](#)

[*] Session Summary			
10.232.50.127	10.232.50.77	141.146.36.77	122.166.131.210
2021-04-29 02:14:06.919	→ INVITE (105203)	→	
2021-04-29 02:14:06.920	← Status:100 (105203)	←	
2021-04-29 02:14:06.934	MEDIA FLOW ADD, ID=33554433, DIRECTION=CALLING		
2021-04-29 02:14:06.935	MEDIA FLOW HAIRPIN		
2021-04-29 02:14:06.936	MEDIA FLOW ADD, ID=33554434, DIRECTION=CALLED		
2021-04-29 02:14:06.939	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:18507904044@122.166.131.210:50095;transport=TLS;ob;acme_nat=18507904044+122.166.131.210@192.168.1.6:50095>		
2021-04-29 02:14:06.939		→ INVITE (105203)	→
2021-04-29 02:14:06.939		← Status:100 (105203)	←

Refresh Export diagram Export session details

## Appendix A

Following are the test cases that are executed between Avaya User with the Twilio Elastic SIP Trunk (PSTN user). **Please note that Avaya User here refers both Avaya User inside Enterprise network as well as Avaya Remote worker.**

Serial Number	Test Cases Executed	Result
1	Avaya user disconnects an inbound connected call	Pass
2	Avaya user disconnects an outbound connected call	Pass
3	Twilio Elastic SIP Trunk user disconnects an inbound connected call	Pass
4	Twilio Elastic SIP Trunk User disconnects an outbound connected call	Pass
5	Avaya user places inbound call from Twilio Elastic SIP Trunk user on hold and then resumes	Pass
6	Avaya user makes outbound call to Twilio Elastic SIP Trunk user and put that call on hold and then resumes	Pass
7	Twilio Elastic SIP Trunk user places inbound call from Avaya user on hold and then resumes	Pass
8	Twilio Elastic SIP Trunk user makes outbound call to Avaya user and put that call on hold and then resumes	Pass
9	Avaya user places inbound call from Twilio Elastic SIP Trunk user on hold for over 15/30 minutes and then resumes	Pass
10	Avaya user makes outbound call to Twilio Elastic SIP Trunk user and places the call on hold for over 15/30 minutes and then resumes	Pass
11	Inbound Twilio Elastic SIP Trunk call to Avaya blind transferred to second Avaya/ PSTN User	Pass
12	Outbound Twilio Elastic SIP Trunk call from Avaya user blind transferred to second Avaya/ PSTN User	Pass
13	Inbound Twilio Elastic SIP Trunk Call to Avaya consultatively transferred to Avaya/ PSTN User	Pass
14	Outbound Twilio Elastic SIP Trunk call from Avaya user consultatively transferred to Avaya/ PSTN User	Pass
15	Avaya user makes outbound call to Twilio Elastic SIP Trunk user and makes a conference call by adding another Avaya/ PSTN user.	Pass

16	Twilio Elastic SIP Trunk user makes outbound call to Avaya user and Avaya user makes a conference call by adding another Avaya/ PSTN user.	Pass
17	Avaya user mutes inbound call from Twilio Elastic SIP Trunk user and then unmutes	Pass
18	Avaya user mutes outbound call made to Twilio Elastic SIP Trunk user and then unmutes	Pass
19	Twilio Elastic SIP Trunk user mutes inbound call from Avaya user and then unmutes	Pass
20	Twilio Elastic SIP Trunk user mutes outbound call made to Avaya user and then unmutes	Pass
21	Twilio Elastic SIP Trunk User disconnects outbound call to Avaya user before it is answered	Pass
22	Avaya user disconnects outbound call to Twilio Elastic SIP Trunk user before it is answered	Pass

**ORACLE**

CONNECT WITH US

 [blogs.oracle.com/oracle](https://blogs.oracle.com/oracle)

 [facebook.com/Oracle/](https://facebook.com/Oracle/)

 [twitter.com/Oracle](https://twitter.com/Oracle)

 [oracle.com](https://oracle.com)

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

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

### Integrated Cloud Applications & Platform Services

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

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

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