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

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with Avaya and Twilio Elastic SIP Trunking	07th May 2021
1.1	Added new section for SBC config/Deployment Using Configuration Assistant	14th December 2021
1.2	Refreshed the app note with testing of Twilio Trunk and Avaya with Oracle SBC 9.0 version	08th April 2022

Table of Contents

1. Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of the Oracle Enterprise Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform along with 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** and **OS900p2**

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. There are some public facing IPs (externally routable IPs) that we use for our testing are masked in this document for security reasons.
The customers can configure any publicly routable IPs for these sections as per their network architecture needs.

3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring 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.

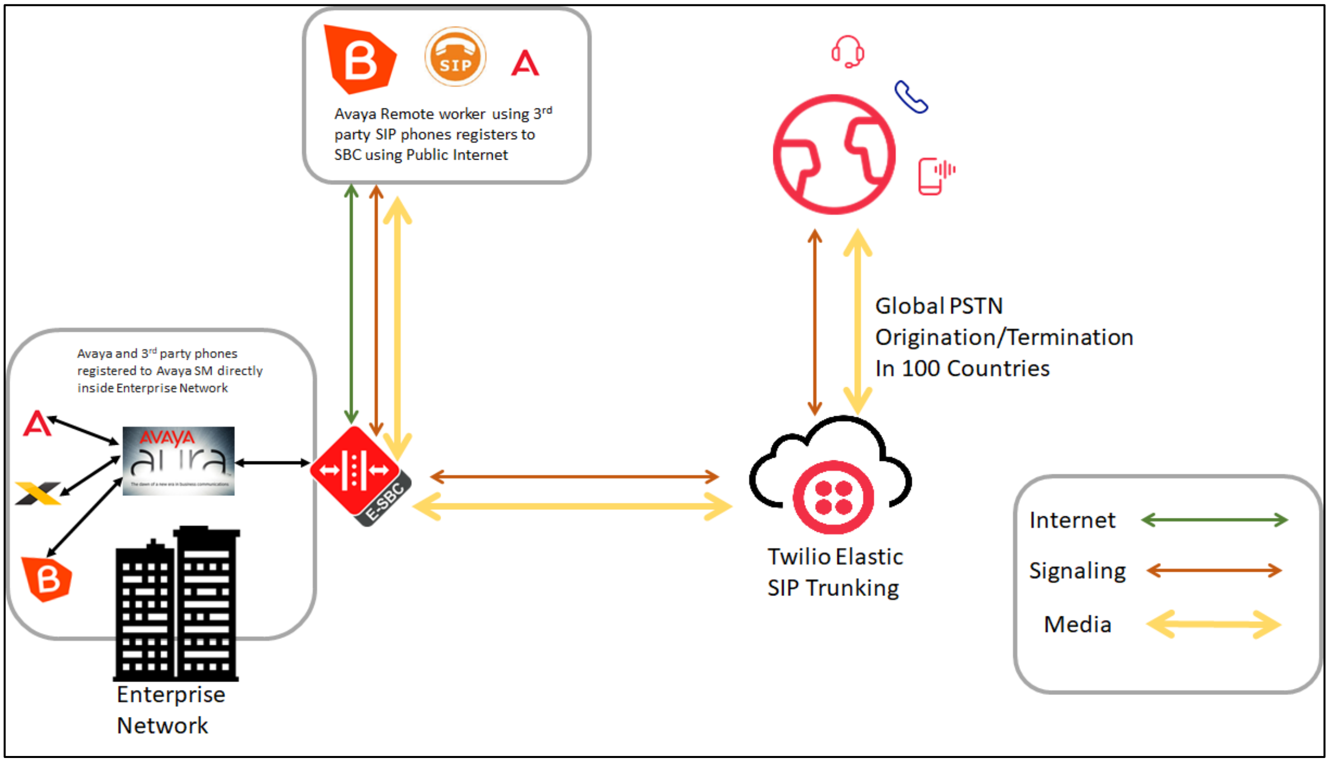
3.2. Requirements

- Fully functioning Avaya Aura Session Manager 8.1 version
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 / 9.0.0 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
Revision 2	9.0.0	8.1

3.3. Architecture

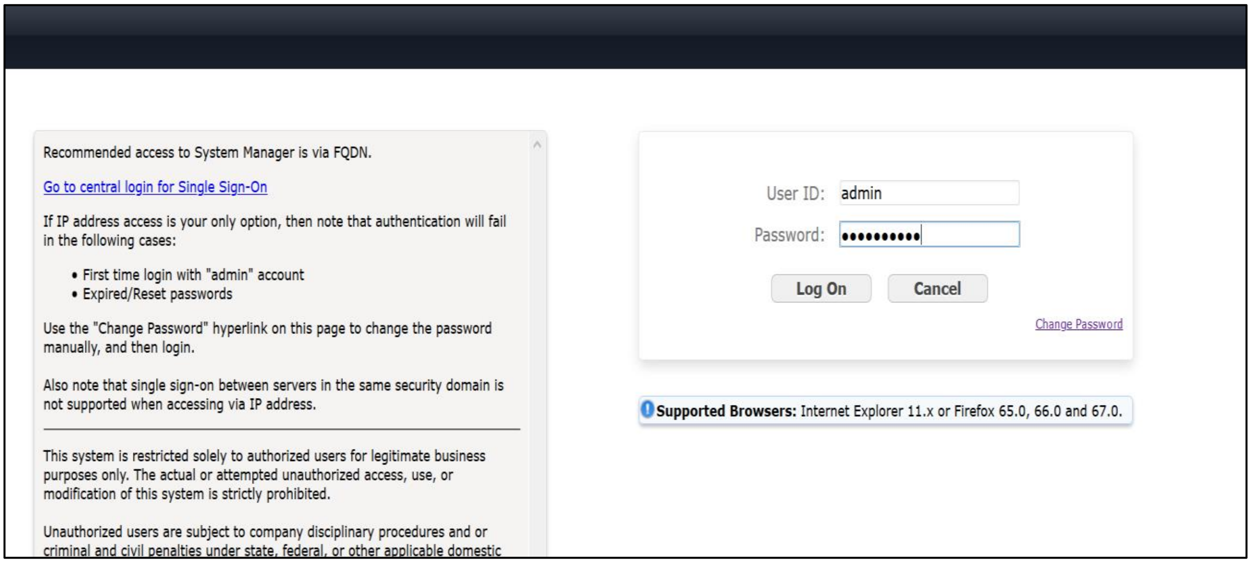

Avaya Remote worker using 3rd party SIP phones registers to SBC using Public Internet
SIP
Avaya and 3rd party phones registered to Avaya SM directly inside Enterprise Network
AVAYA aura
E-SBC
Enterprise Network
Global PSTN Origination/Termination In 100 Countries
Twilio Elastic SIP Trunking
Internet
Signaling
Media

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.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

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

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

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

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

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

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

User ID: admin

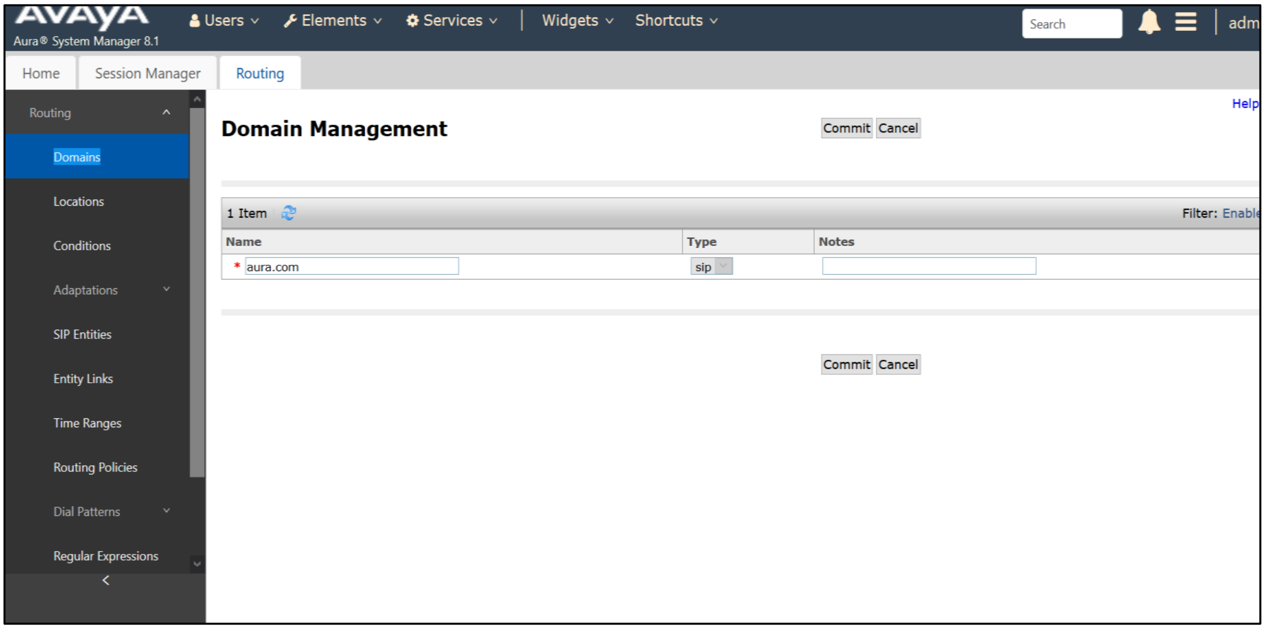
Password: ••••••••••

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

4.1. Adding SIP Domain

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

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



Domain Management

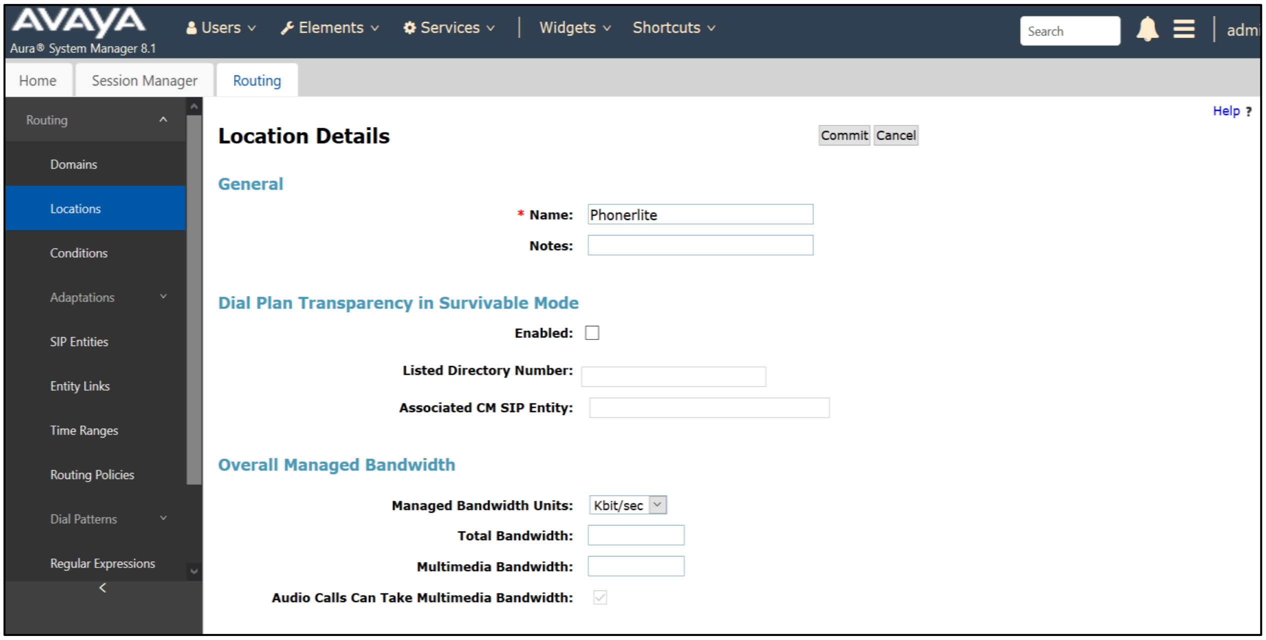
1 Item

Name	Type	Notes
* aura.com	sip	

4.2. Adding Location

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

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



Location Details

General

* Name:	Phonerlite
Notes:	

Dial Plan Transparency in Survivable Mode

Enabled:	☐
Listed Directory Number:	
Associated CM SIP Entity:	

Overall Managed Bandwidth

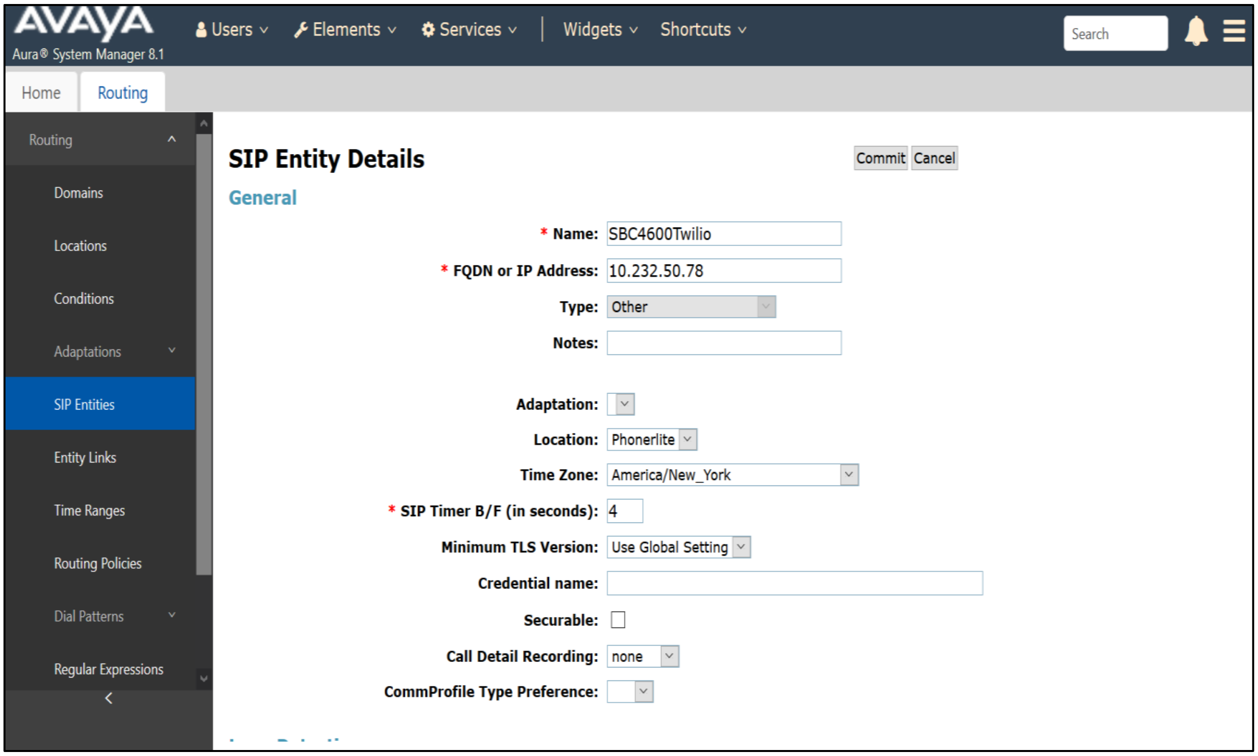
Managed Bandwidth Units:	Kbit/sec
Total Bandwidth:	
Multimedia Bandwidth:	
Audio Calls Can Take Multimedia Bandwidth:	☑

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

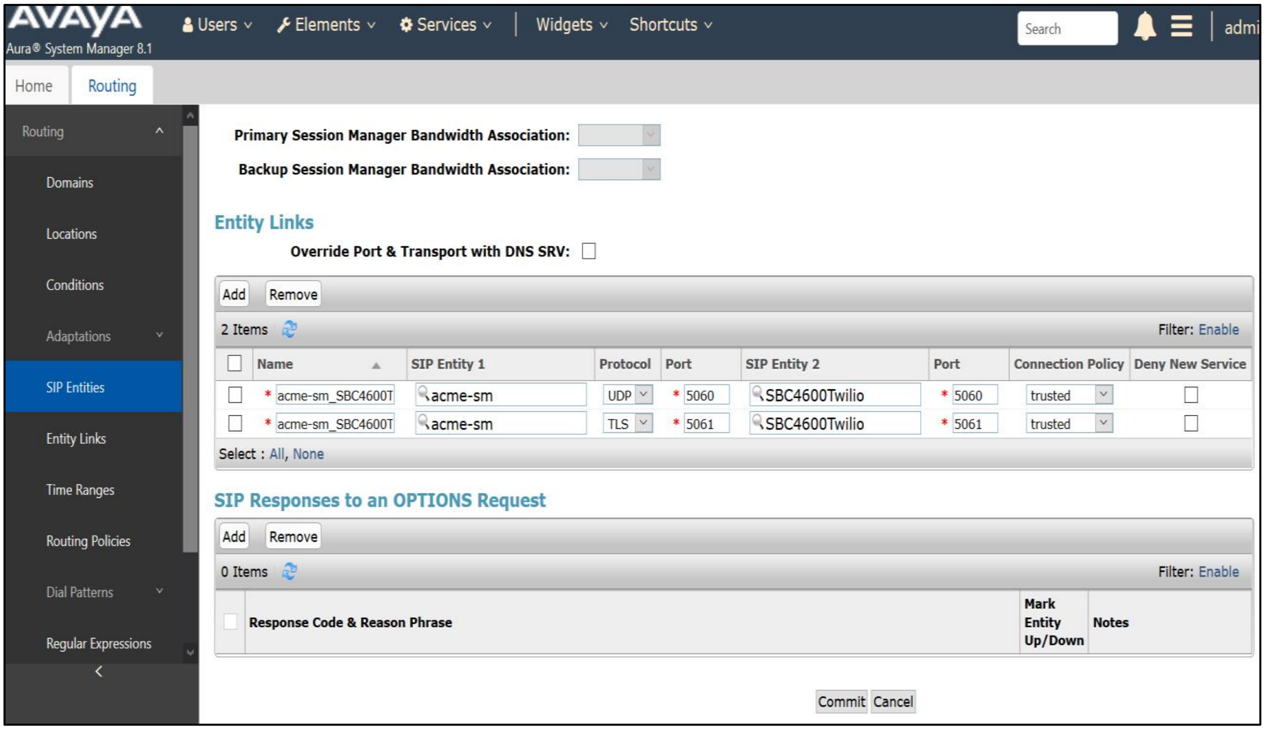
Leave all other fields as default values and click “Commit” to save the configuration.



SIP Entity Details

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:	



Primary Session Manager Bandwidth Association:	
Backup Session Manager Bandwidth Association:	

Entity Links

Override Port & Transport with DNS SRV: □

2 Items

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* acme-sm_SBC4600T	acme-sm	UDP	* 5060	SBC4600Twilio	* 5060	trusted	□
□	* acme-sm_SBC4600T	acme-sm	TLS	* 5061	SBC4600Twilio	* 5061	trusted	□

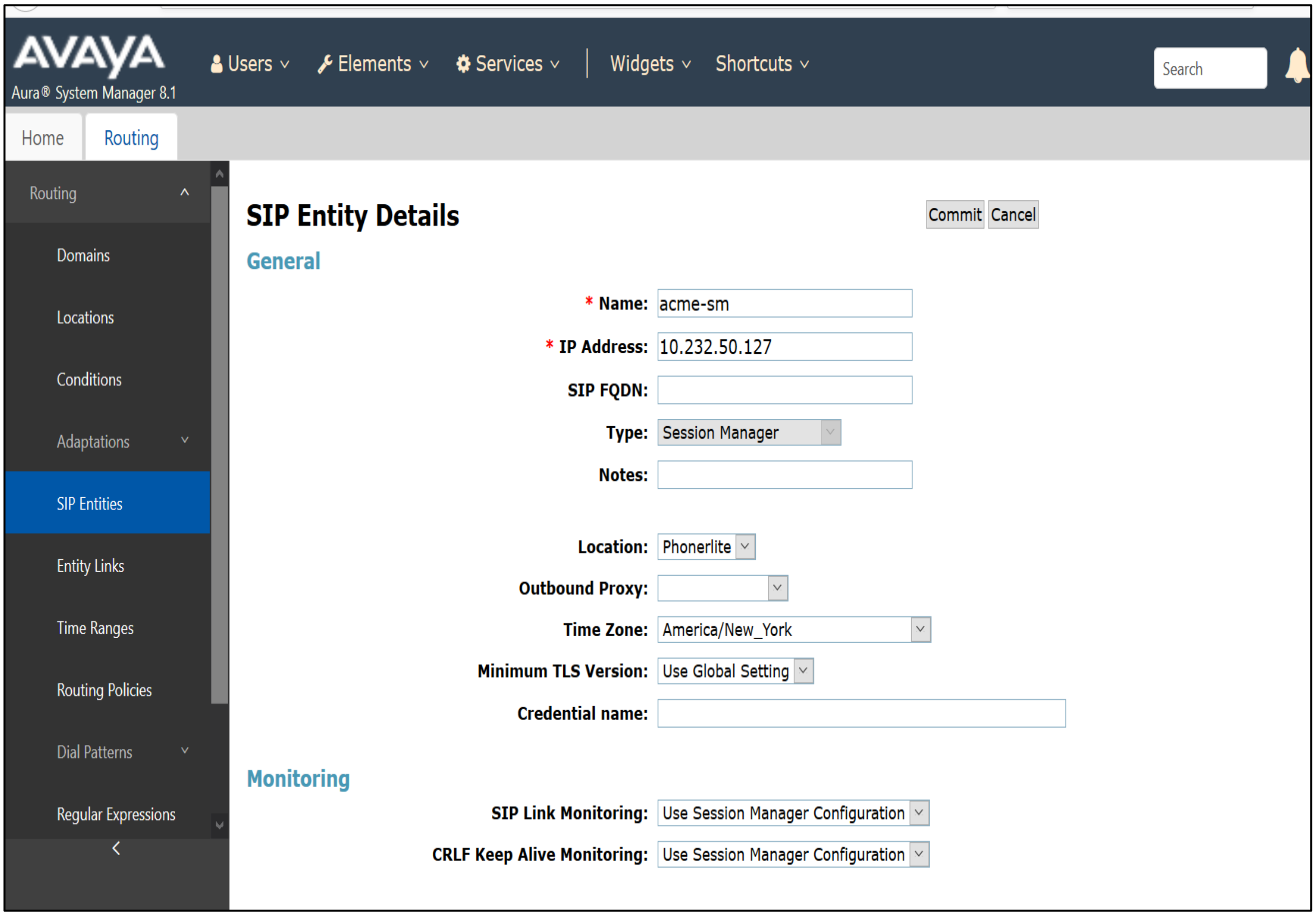
SIP Responses to an OPTIONS Request

0 Items

□	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

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.



SIP Entity Details

General

* Name:	acme-sm
* IP Address:	10.232.50.127
SIP FQDN:	
Type:	Session Manager
Notes:	
Location:	Phonerlite
Outbound Proxy:	
Time Zone:	America/New_York
Minimum TLS Version:	Use Global Setting
Credential name:	

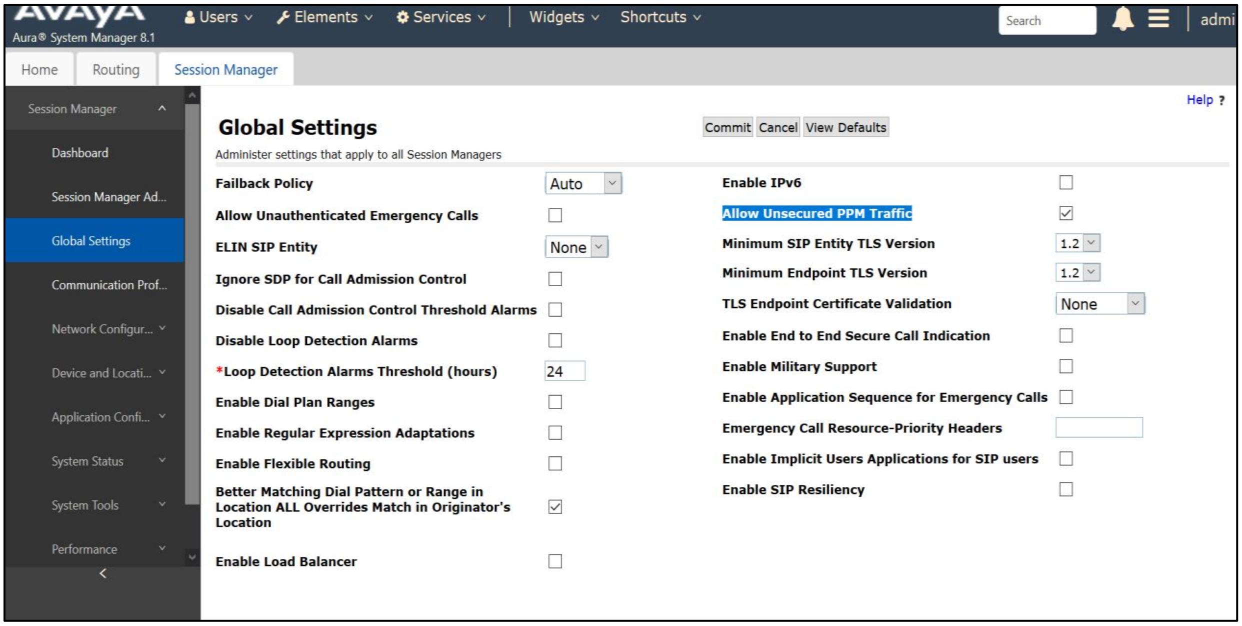
Monitoring

SIP Link Monitoring:	Use Session Manager Configuration
CRLF Keep Alive Monitoring:	Use Session Manager Configuration

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.



Global Settings

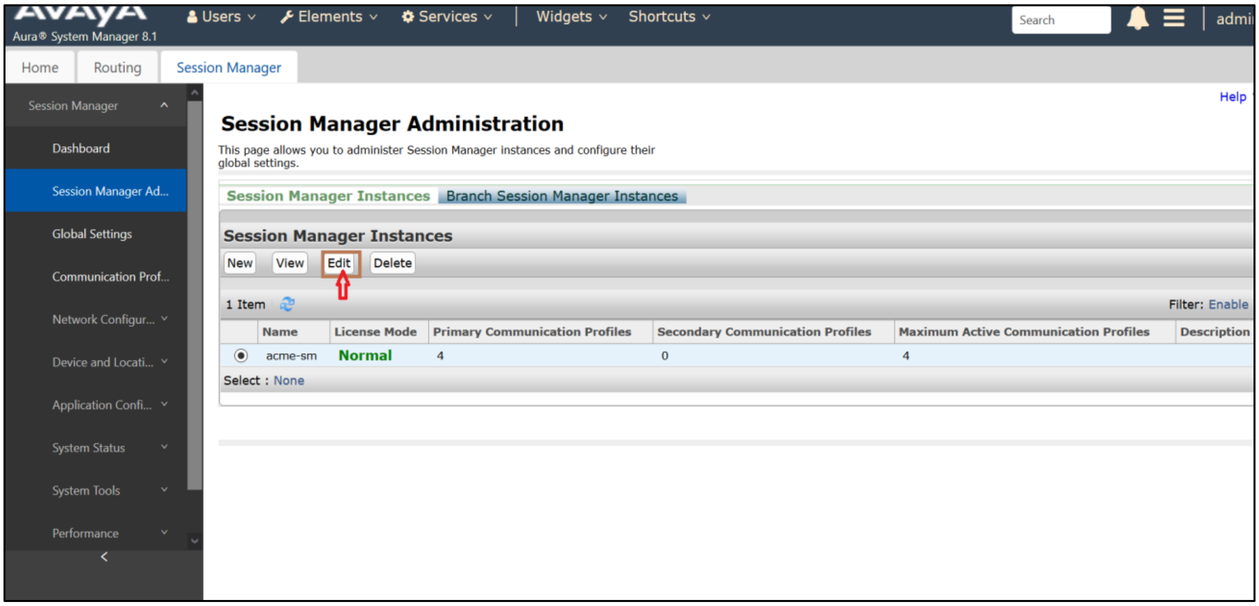
Administer settings that apply to all Session Managers

Failback Policy	Auto
Allow Unauthenticated Emergency Calls	☐
ELIN SIP Entity	None
Ignore SDP for Call Admission Control	☐
Disable Call Admission Control Threshold Alarms	☐
Disable Loop Detection Alarms	☐
*Loop Detection Alarms Threshold (hours)	24
Enable Dial Plan Ranges	☐
Enable Regular Expression Adaptations	☐
Enable Flexible Routing	☐
Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location	☑
Enable Load Balancer	☐
Enable IPv6	☐
Allow Unsecured PPM Traffic	☑
Minimum SIP Entity TLS Version	1.2
Minimum Endpoint TLS Version	1.2
TLS Endpoint Certificate Validation	None
Enable End to End Secure Call Indication	☐
Enable Military Support	☐
Enable Application Sequence for Emergency Calls	☐
Emergency Call Resource-Priority Headers	
Enable Implicit Users Applications for SIP users	☐
Enable SIP Resiliency	☐

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.

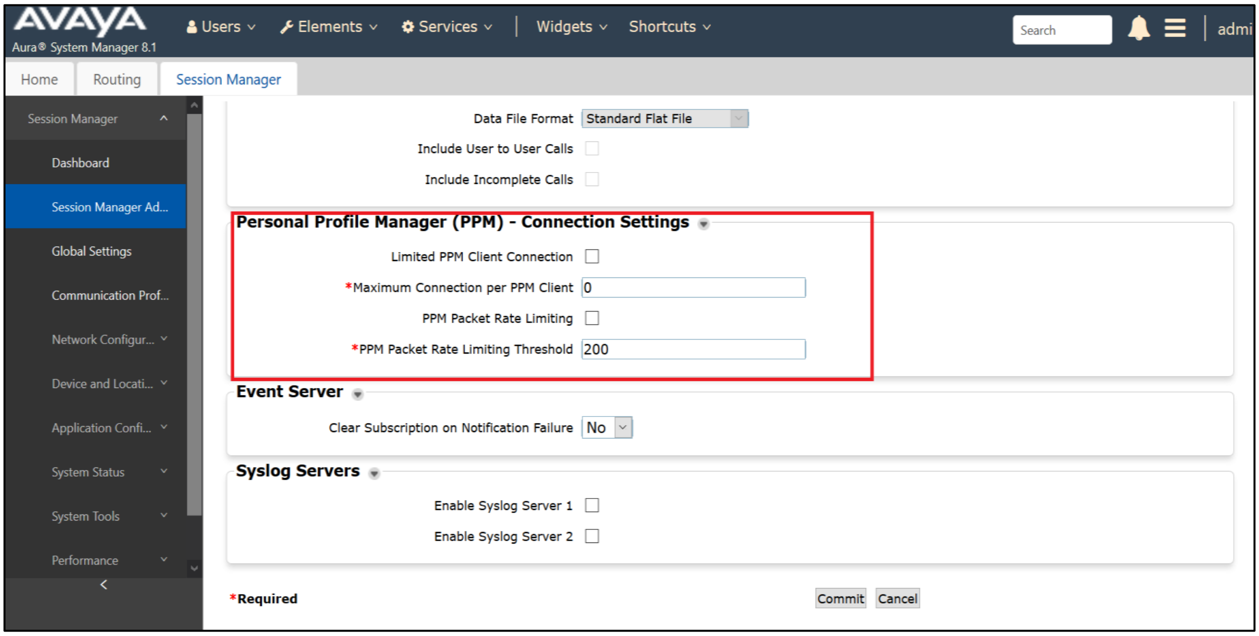


Session Manager Administration

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

Session Manager Instances

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



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 □

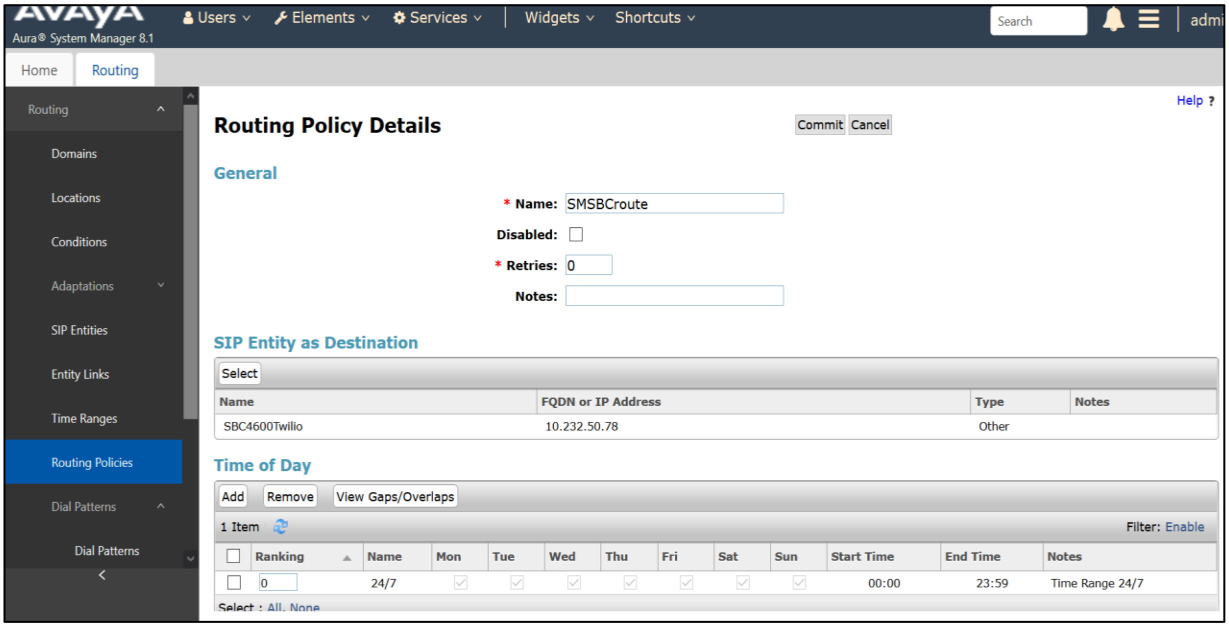
Enable Syslog Server 2 □

*Required

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



Routing Policy Details

General

* Name: SMSBCroute

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SBC4600Twilio	10.232.50.78	Other	

Time of Day

1 Item

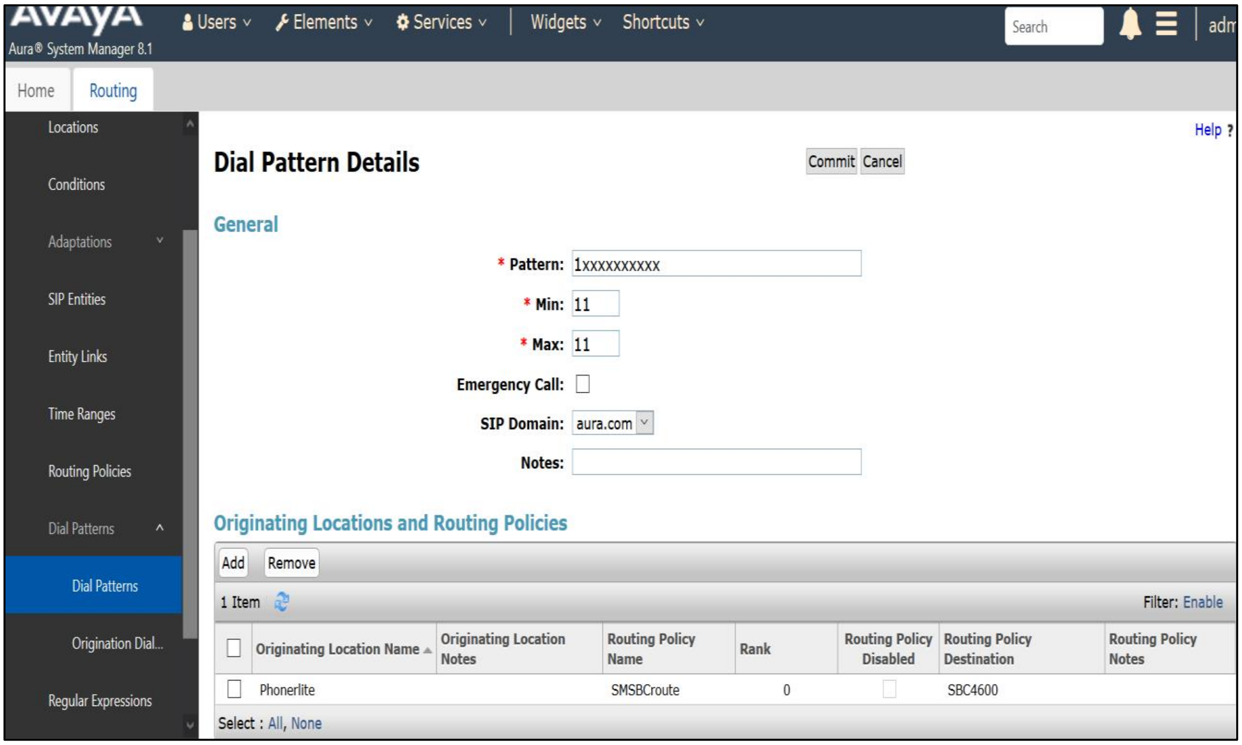
□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

4.6. Adding Dial Patterns:

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

- Set Pattern: 1xxxxxxxxxx (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



Dial Pattern Details

General

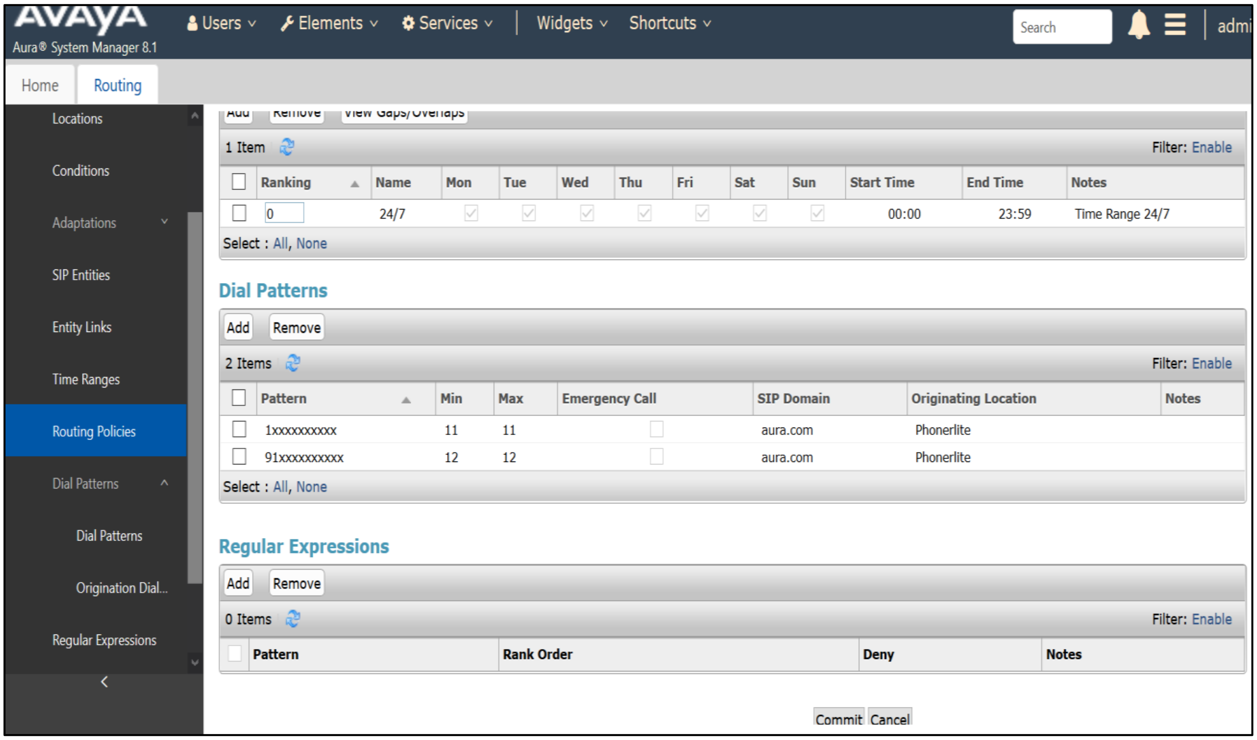
* Pattern:	1xxxxxxxxxx
* Min:	11
* Max:	11
Emergency Call:	□
SIP Domain:	aura.com
Notes:	

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Phonerlite		SMSBCroute	0	□	SBC4600	

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



1 Item

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Dial Patterns

2 Items

□	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
□	1xxxxxxxxxx	11	11	□	aura.com	Phonerlite	
□	91xxxxxxxxxx	12	12	□	aura.com	Phonerlite	

Regular Expressions

0 Items

□	Pattern	Rank Order	Deny	Notes

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

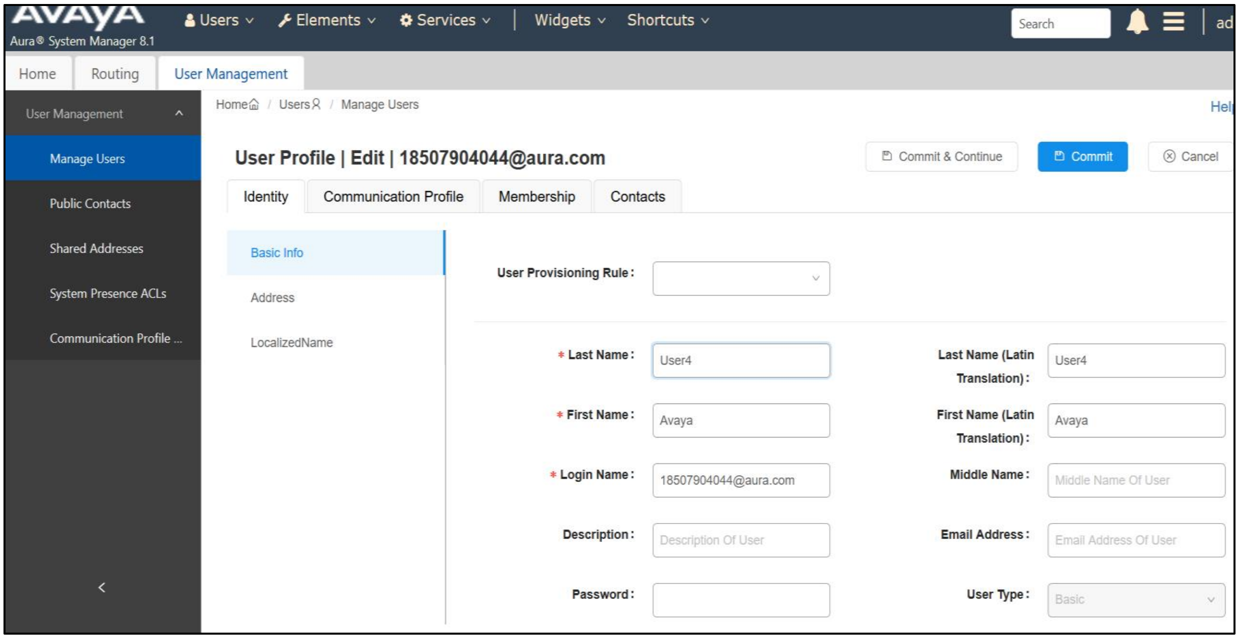
- Set Comm-Profile Password: any password (Numbers or alphabets or alphanumeric)
- Re-enter Comm-Profile Password: Type the password again for confirmation.

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

- Set Type: Avaya SIP
- Set Fully Qualified Address: Type the Directory number @domain.com
  18507904044@aura.com

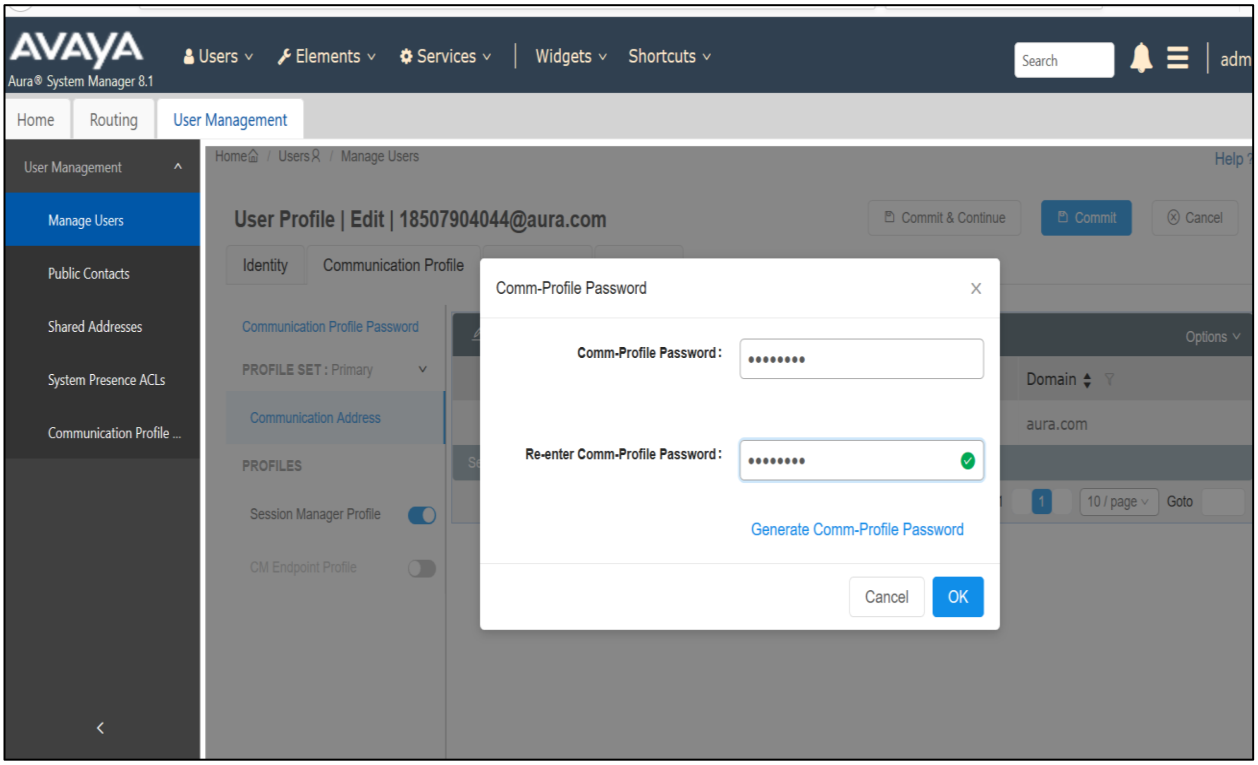
Under **Profile tab,** enable **Session Manager Profile** and click it to open it.

- 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.



User Profile | Edit | 18507904044@aura.com

User Provisioning Rule :			
* 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 :		User Type :	Basic



User Profile | Edit | 18507904044@aura.com

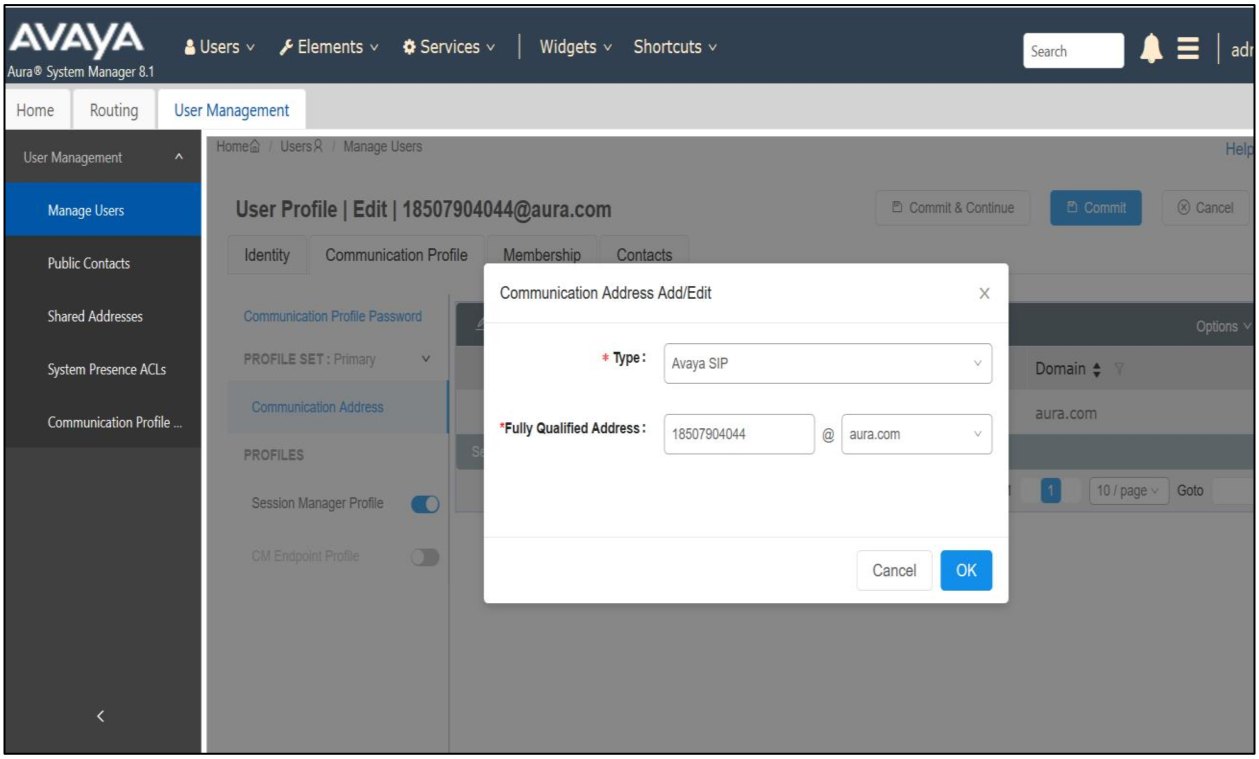
Comm-Profile Password

Comm-Profile Password : ••••••••

Re-enter Comm-Profile Password : ••••••••

Generate Comm-Profile Password

Cancel OK



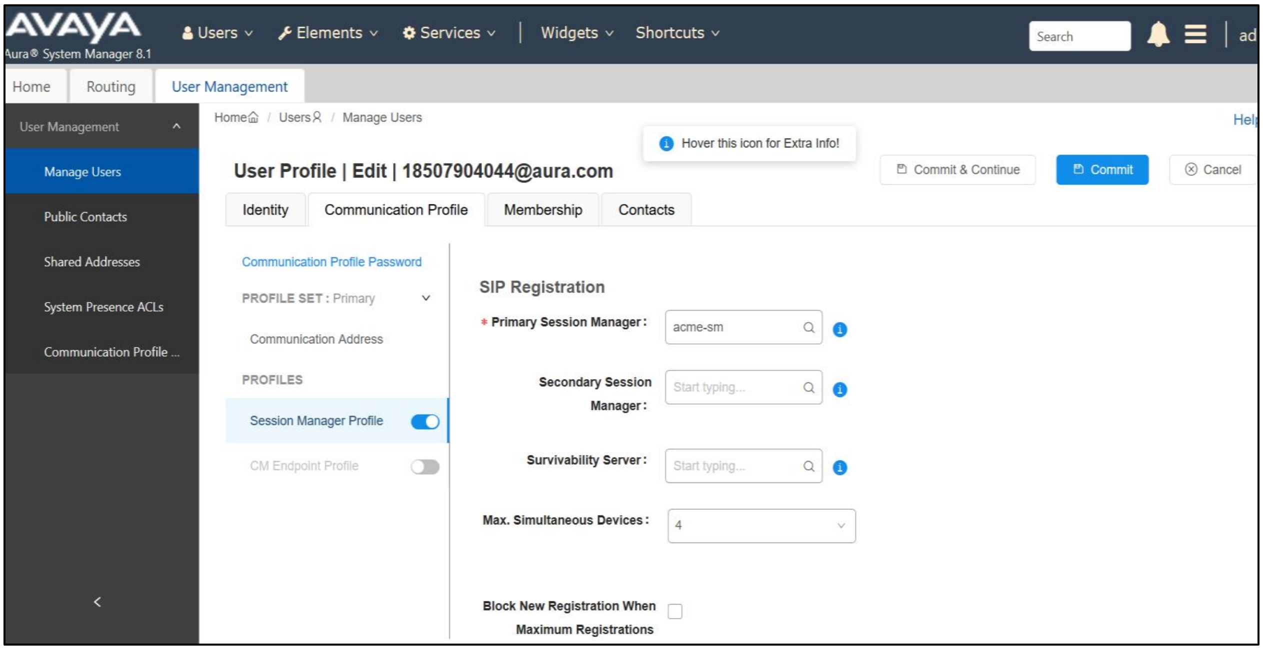
User Profile | Edit | 18507904044@aura.com

Communication Address Add/Edit

* Type : Avaya SIP

*Fully Qualified Address : 18507904044 @ aura.com

Cancel OK



User Profile | Edit | 18507904044@aura.com

SIP Registration

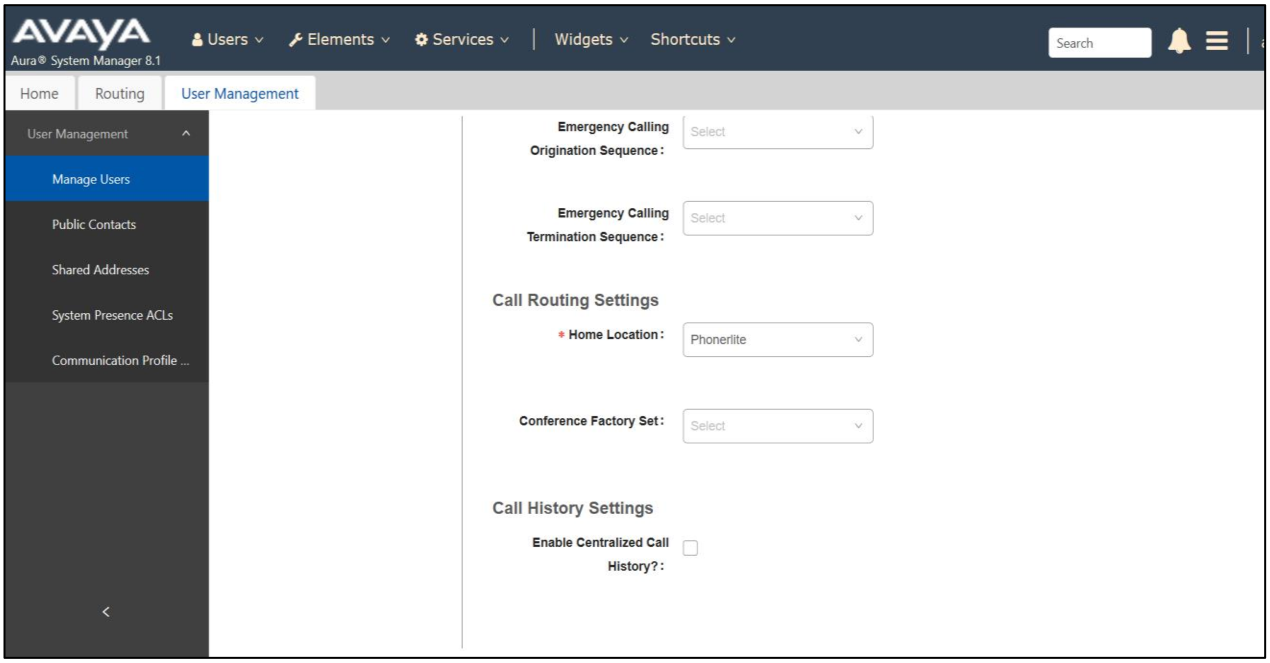
* Primary Session Manager : acme-sm

Secondary Session Manager : Start typing...

Survivability Server : Start typing...

Max. Simultaneous Devices : 4

Block New Registration When Maximum Registrations □



Emergency Calling Origination Sequence : Select

Emergency Calling Termination Sequence : Select

Call Routing Settings

* Home Location : Phonerlite

Conference Factory Set : Select

Call History Settings

Enable Centralized Call History? : □

You can repeat the above steps to add more users to the Session Manager.

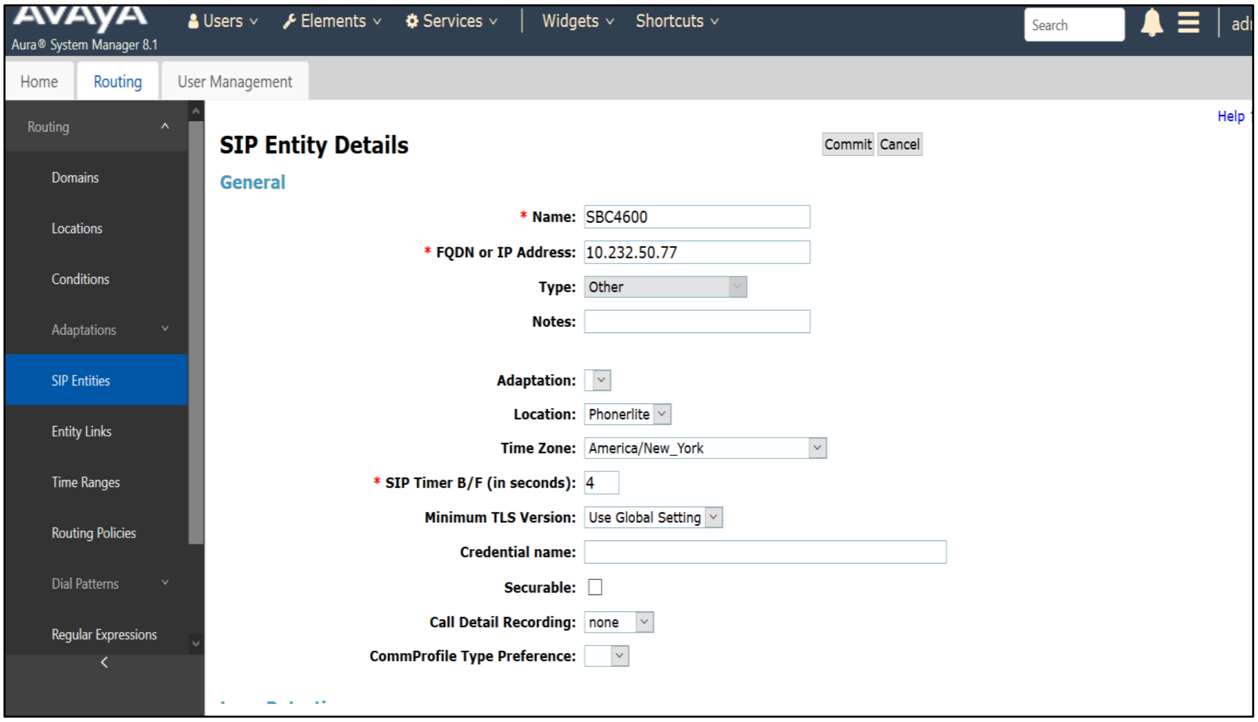
Below are the configuration which are specific to Avaya Remote Worker configuration.

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

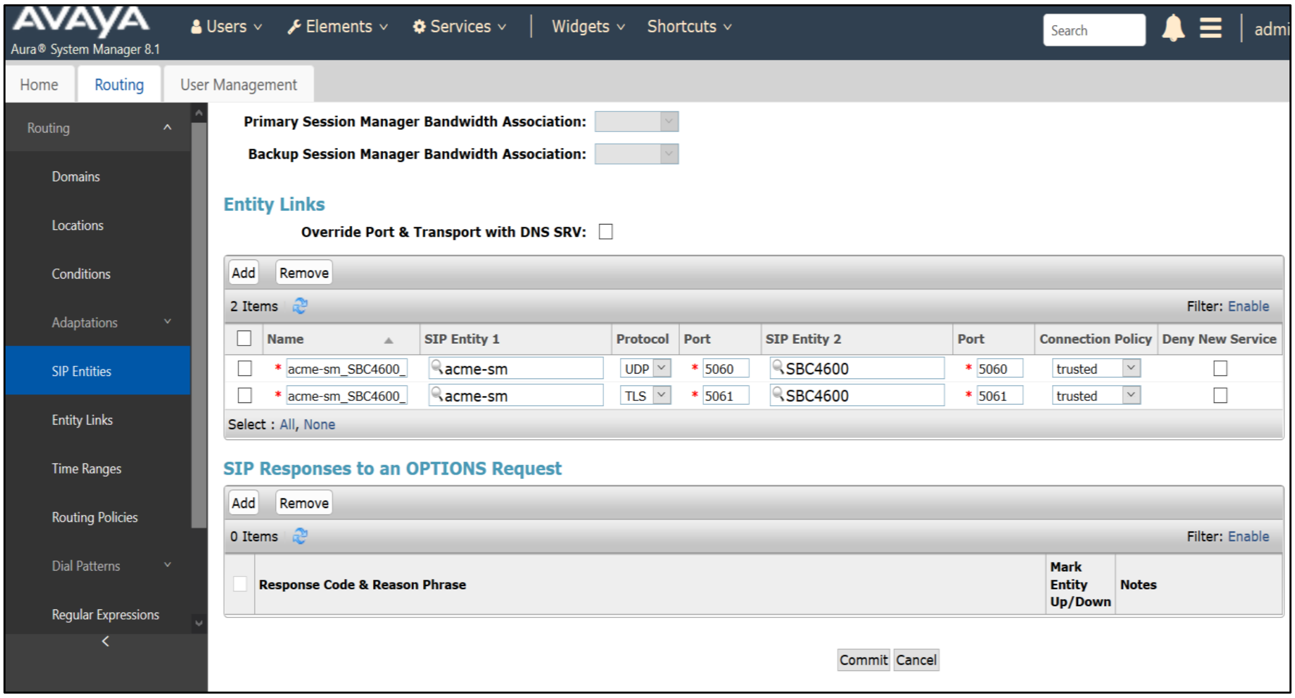
Leave all other fields as default values and click “Commit” to save the configuration.



SIP Entity Details

General

* Name:	SBC4600
* FQDN or IP Address:	10.232.50.77
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:	



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
□	* acme-sm_SBC4600_	acme-sm	UDP	* 5060	SBC4600	* 5060	trusted	□
□	* acme-sm_SBC4600_	acme-sm	TLS	* 5061	SBC4600	* 5061	trusted	□

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items Filter: Enable

□	Response Code & Reason Phrase	Mark Entity Up/Down	Notes

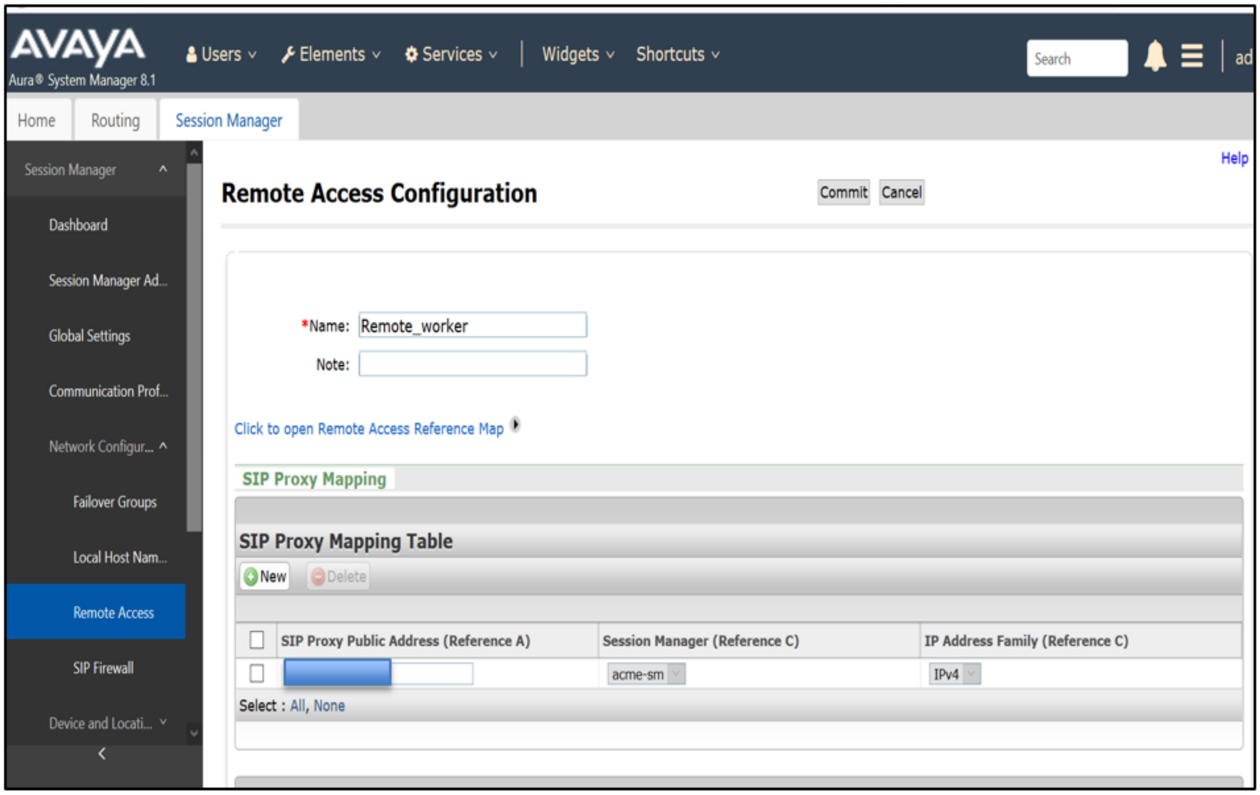
Commit Cancel

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.
- Click New under SIP Proxy Private IP Address. Add the Oracle SBC inside interface IP address for SIP Private Address.
- Click Commit to save the configuration.



Remote Access Configuration

*Name: Remote_worker

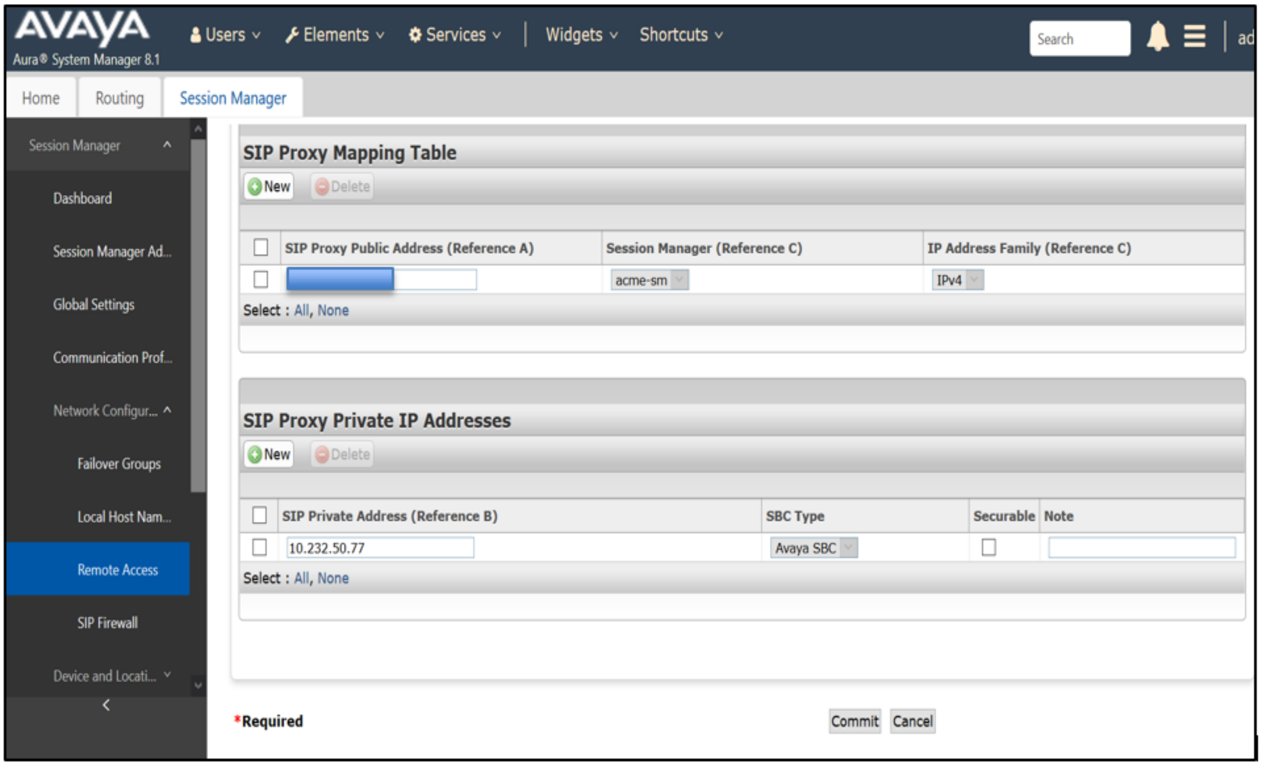
Note:

SIP Proxy Mapping

SIP Proxy Mapping Table

□	SIP Proxy Public Address (Reference A)	Session Manager (Reference C)	IP Address Family (Reference C)
□	[redacted]	acme-sm	IPv4

Select : All, None



SIP Proxy Mapping Table

□	SIP Proxy Public Address (Reference A)	Session Manager (Reference C)	IP Address Family (Reference C)
□	[redacted]	acme-sm	IPv4

Select : All, None

SIP Proxy Private IP Addresses

□	SIP Private Address (Reference B)	SBC Type	Securable	Note
□	10.232.50.77	Avaya SBC	□	

Select : All, None

*Required

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).** If the Oracle SBC being deployed is new, with no existing configuration, the simplest way to configure it to interface with Avaya Session Manager is by utilizing the Configuration Assistant feature.

5.1. Validated Oracle SBC version

Oracle conducted tests with Oracle SBC 8.4 / SBC 9.0 software – this software with the configuration listed below can run on any of the following products:

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

6. New SBC configuration

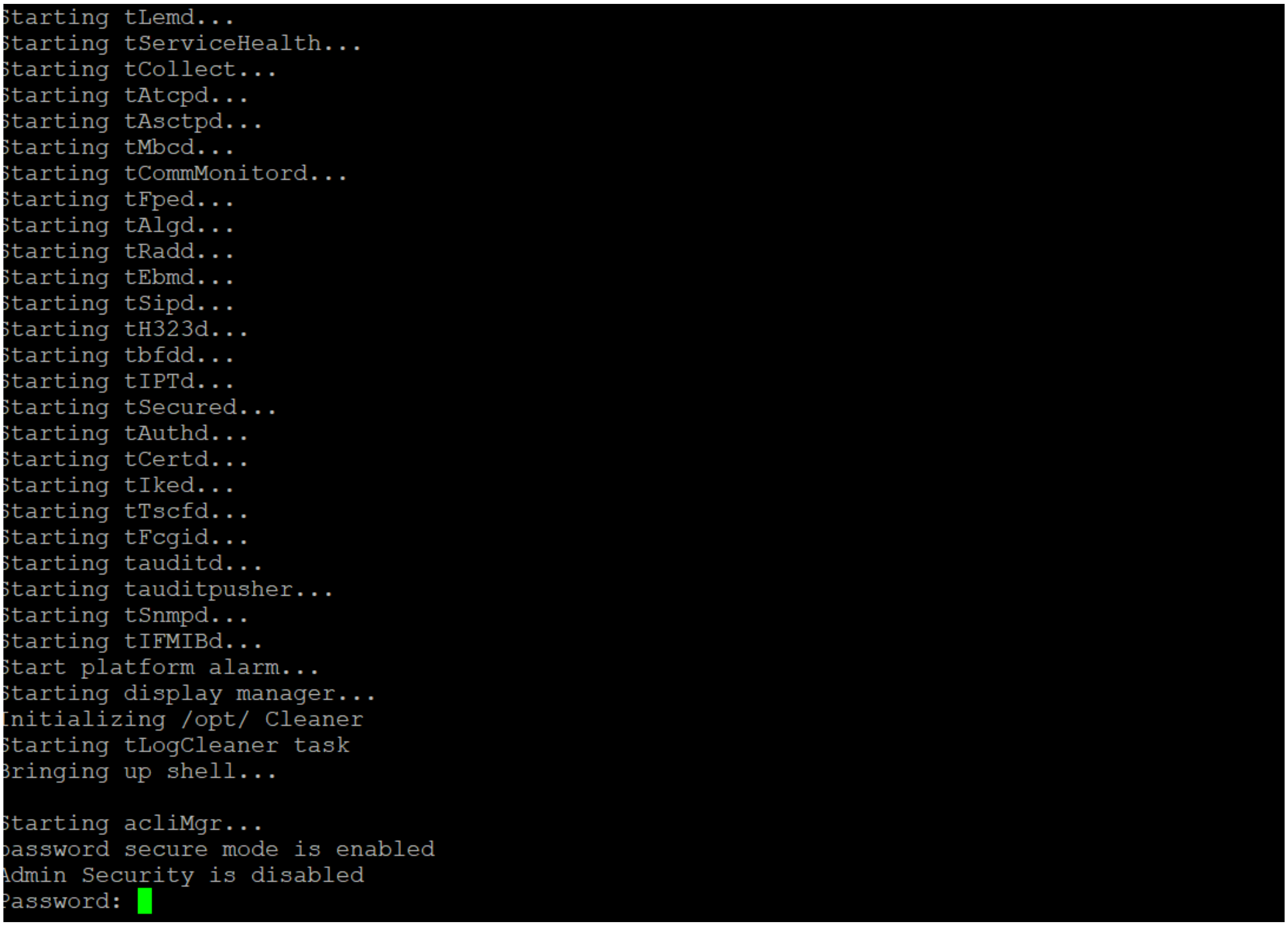
If the customer is looking to setup a new SBC from scratch, please follow the section below.

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

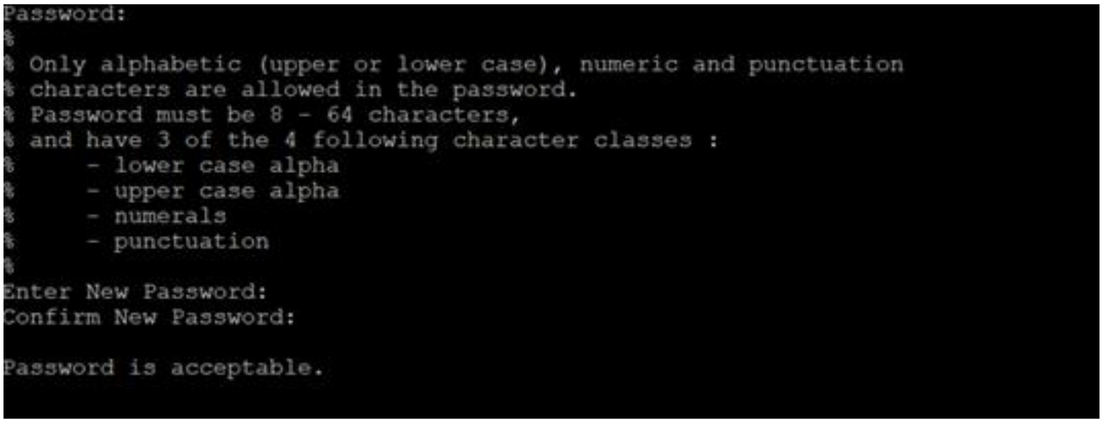
Power on the SBC and confirm that you see the following output from the boot-up sequence



```
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”.

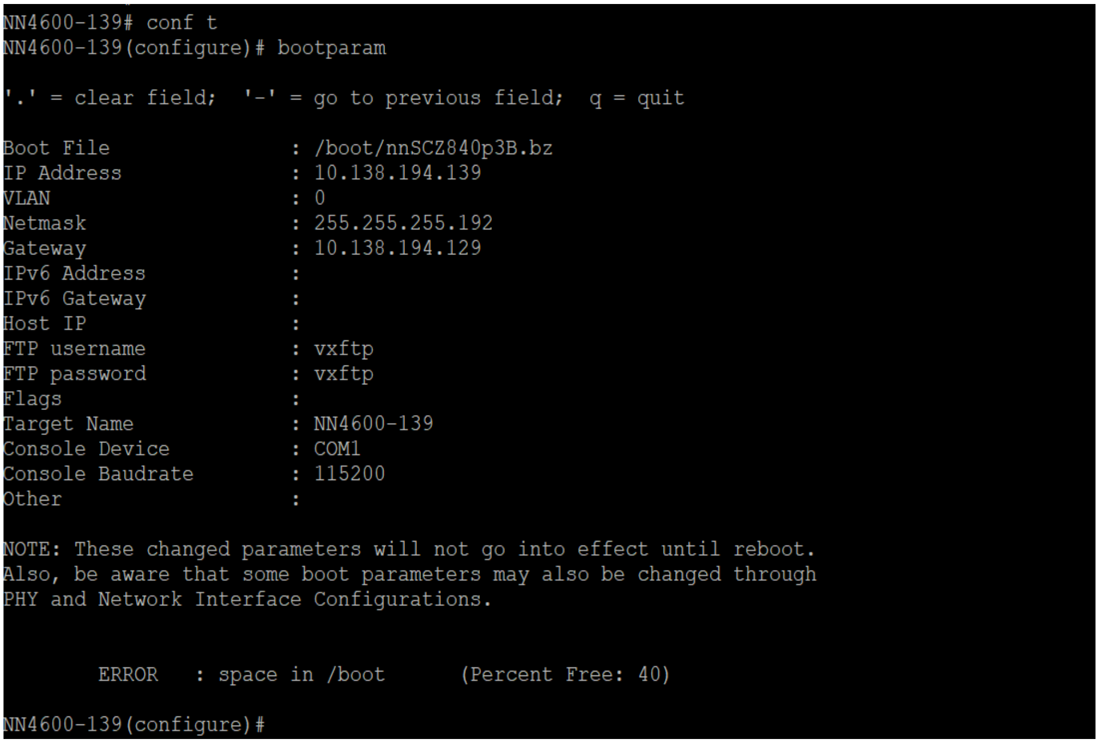
Both passwords have to be changed according to the rules shown below.



```
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.
```

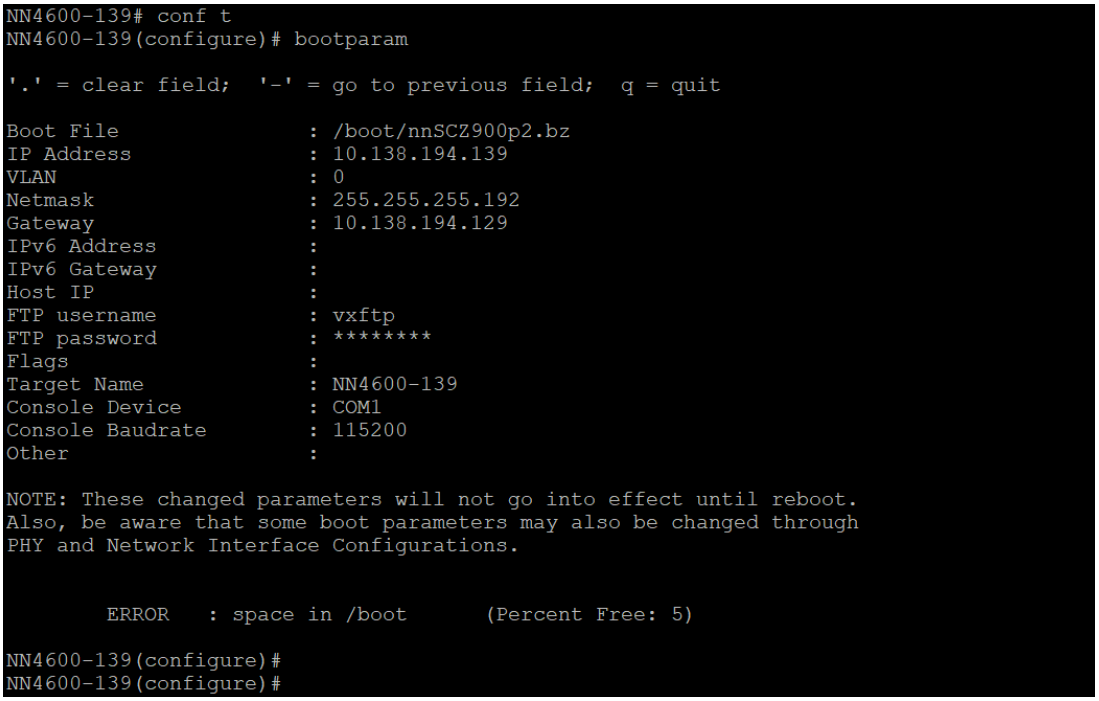
Now set the management IP of the SBC by setting the IP address in bootparam.

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)#
```

SBC 9.0 bootparam screen

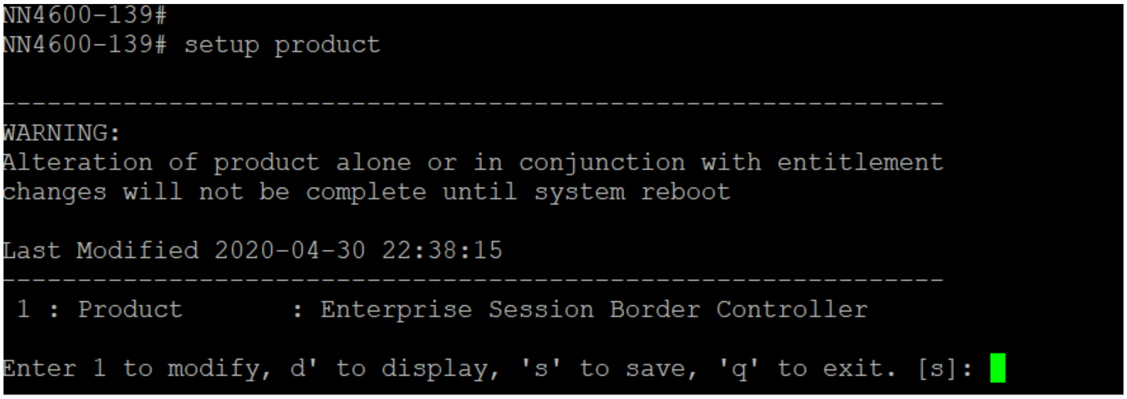


```
NN4600-139# conf t
NN4600-139(configure)# bootparam

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

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

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


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

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

Note: There is no management IP configured by default.

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

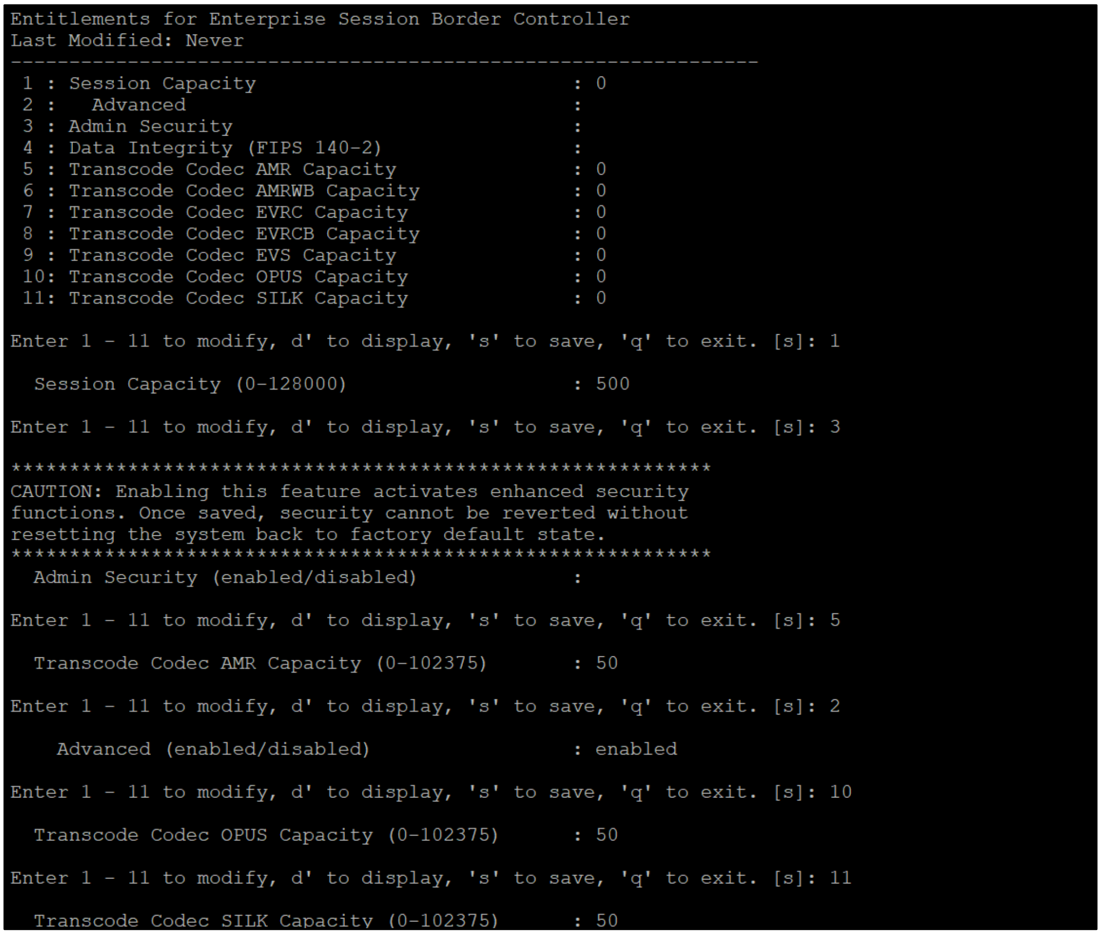
To configure product type, type in setup product in the terminal



```
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.

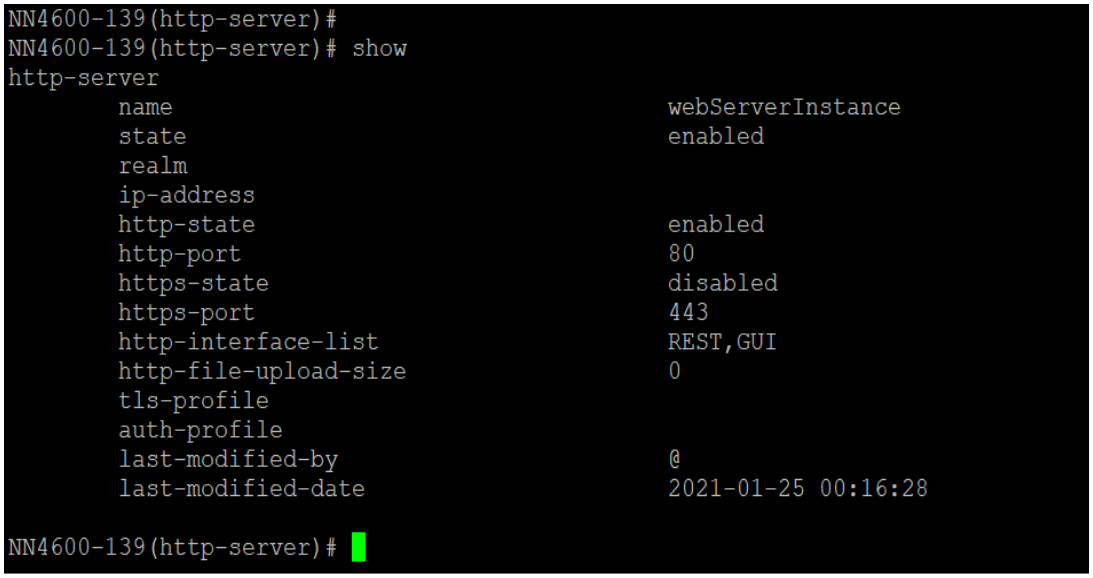


```
Entitlements for Enterprise Session Border Controller
Last Modified: Never
----------------------------------------------------------------
 1 : Session Capacity                           : 0
 2 :   Advanced                                 :
 3 : Admin Security                             :
 4 : 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.

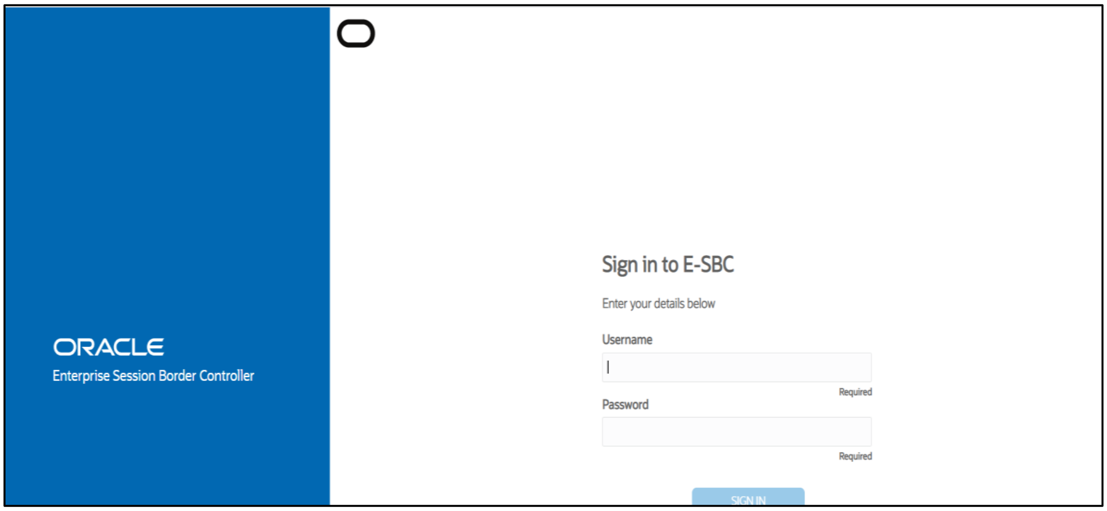


```
NN4600-139(http-server)#
NN4600-139(http-server)# show
http-server
        name                                    webServerInstance
        state                                   enabled
        realm
        ip-address
        http-state                              enabled
        http-port                               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)#
```

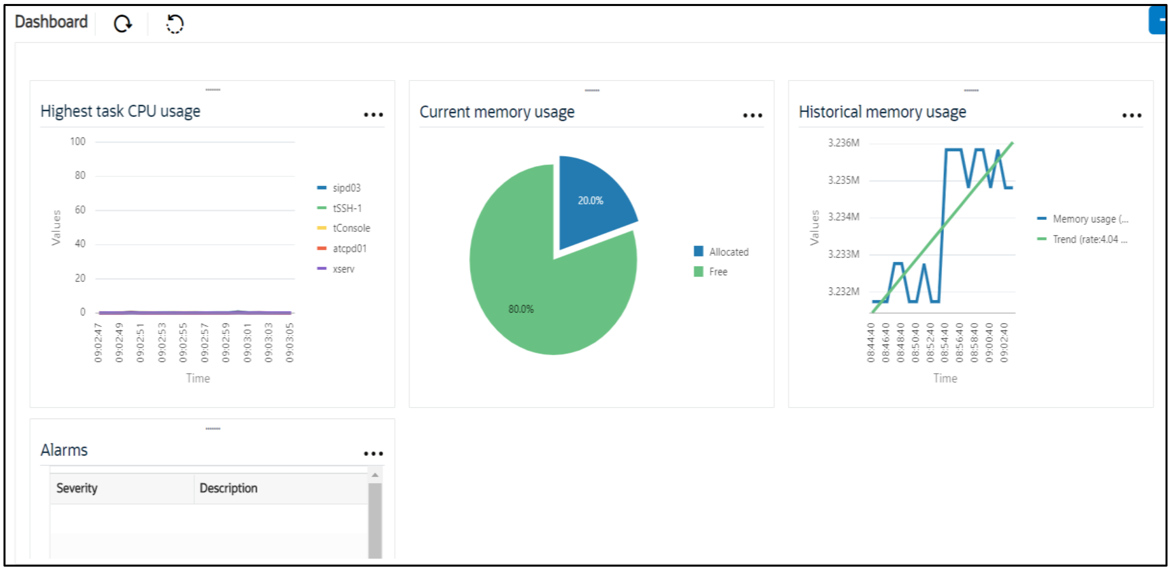
6.2. Configure SBC using Web GUI

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

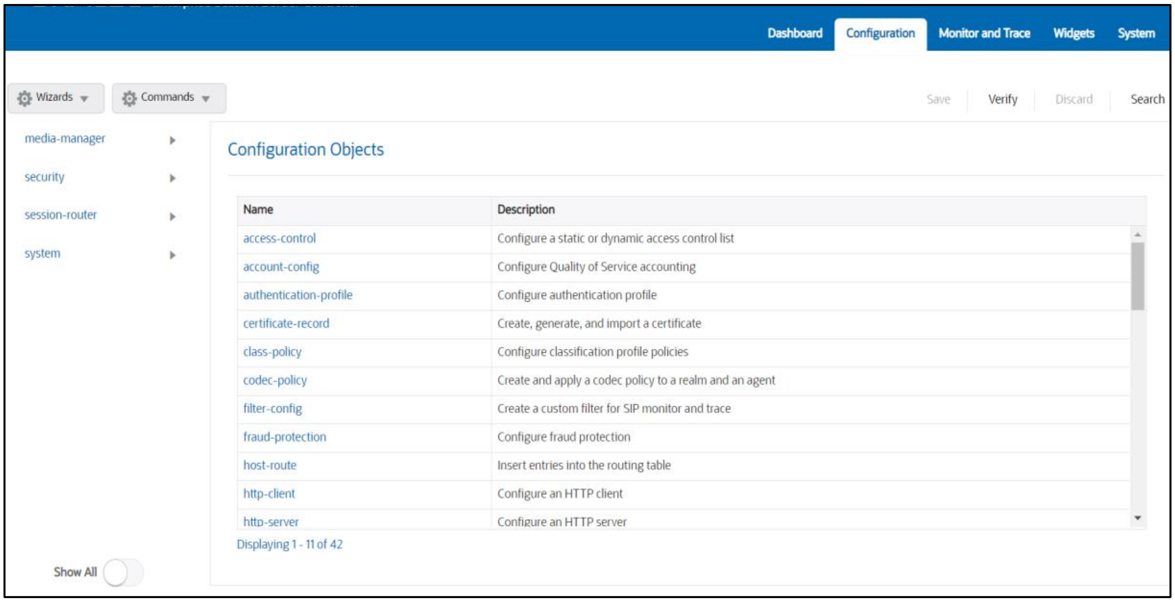
The Web GUI can be accessed through the url http://<SBC_MGMT_IP>.



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



Go to Configuration as shown below, to configure the SBC



Configuration Objects

Name	Description
access-control	Configure a static or dynamic access control list
account-config	Configure Quality of Service accounting
authentication-profile	Configure authentication profile
certificate-record	Create, generate, and import a certificate
class-policy	Configure classification profile policies
codec-policy	Create and apply a codec policy to a realm and an agent
filter-config	Create a custom filter for SIP monitor and trace
fraud-protection	Configure fraud protection
host-route	Insert entries into the routing table
http-client	Configure an HTTP client
http-server	Configure an HTTP server

Displaying 1 - 11 of 42

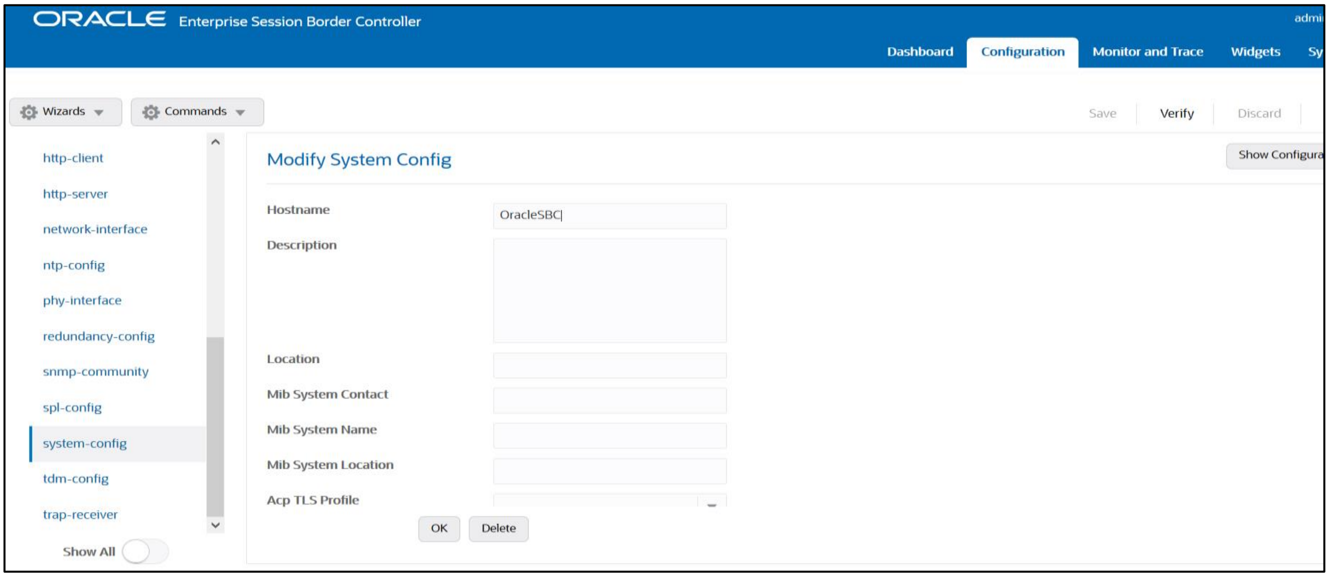
Kindly refer to the GUI User Guide given below for more information.

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

The expert mode is used for configuration.
Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

6.3. Configure system-config

Go to system->system-config



Modify System Config

Hostname: OracleSBC|

Description

Location

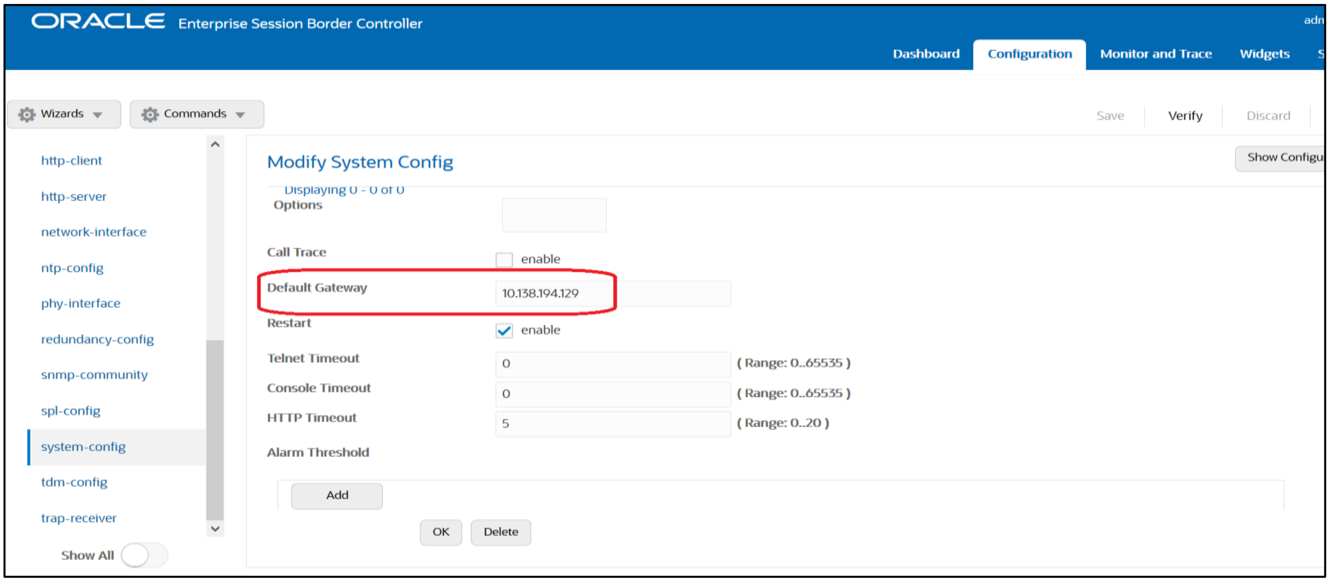
Mib System Contact

Mib System Name

Mib System Location

Acp TLS Profile

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



Modify System Config

Displaying 0 - 0 of 0

Options

Call Trace: □ enable

Default Gateway: 10.138.194.129

Restart: ☑ enable

Telnet Timeout: 0 (Range: 0..65535)

Console Timeout: 0 (Range: 0..65535)

HTTP Timeout: 5 (Range: 0..20)

Alarm Threshold

For VME, transcoding cores are required. Please refer the documentation here for more information

https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.0.0/releasenotes/esbc-release-notes.pdf

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

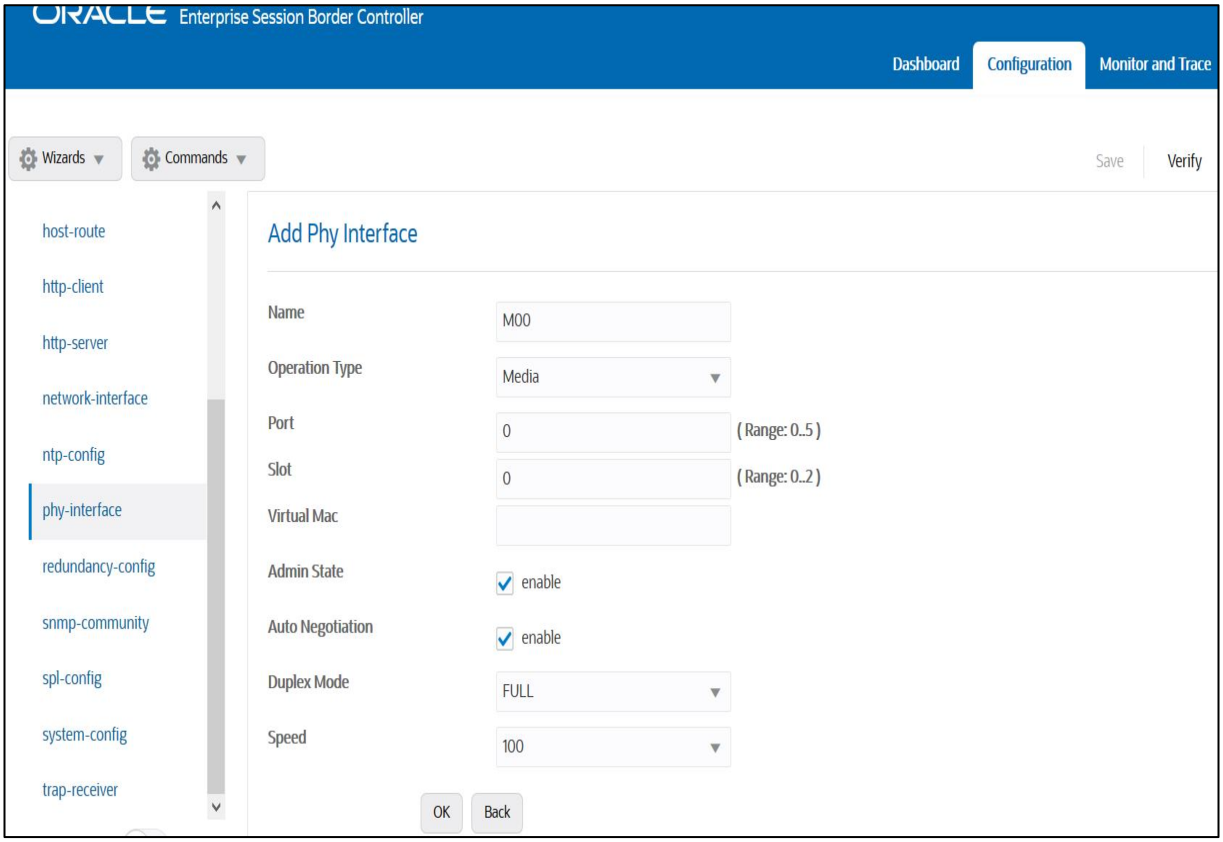
6.4. Configure Physical Interface values

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

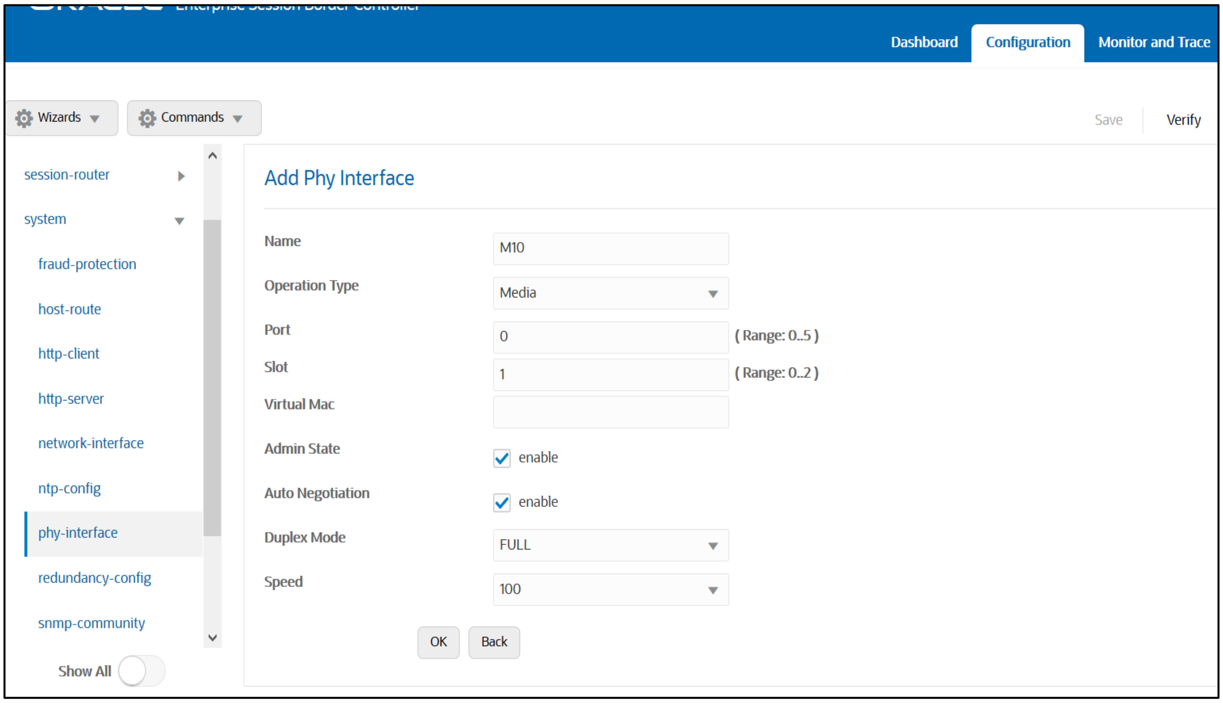
Please configure M00 interface as below.



Add Phy Interface

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

Please configure M10 interface as below



Add Phy Interface

Name	M10
Operation Type	Media
Port	0 (Range: 0..5)
Slot	1 (Range: 0..2)
Virtual Mac	
Admin State	☑ enable
Auto Negotiation	☑ enable
Duplex Mode	FULL
Speed	100

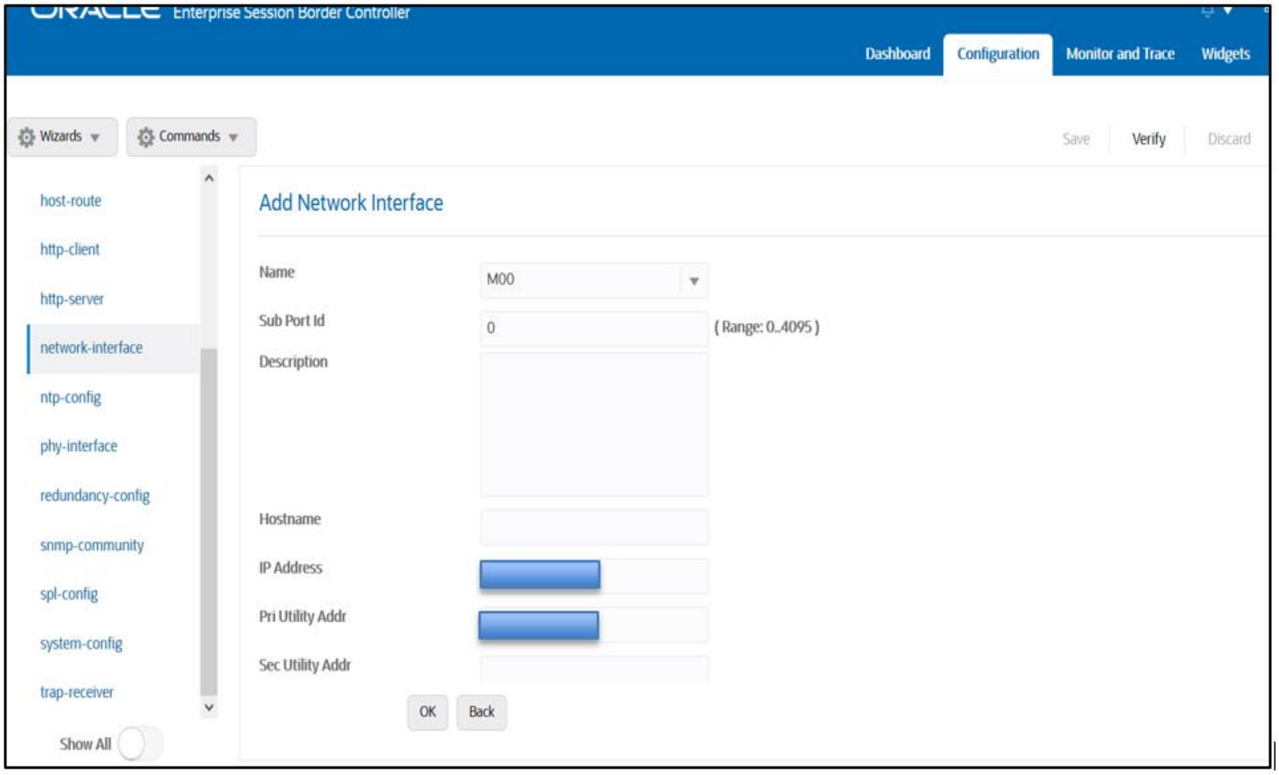
6.5. Configure Network Interface values

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	[redacted]	10.232.50.78
Netmask	255.255.255.192	255.255.255.0
Gateway	[redacted]	10.232.50.1

Please configure network interface M00 as below



Add Network Interface

Name: M00

Sub Port Id: 0 (Range: 0..4095)

Description:

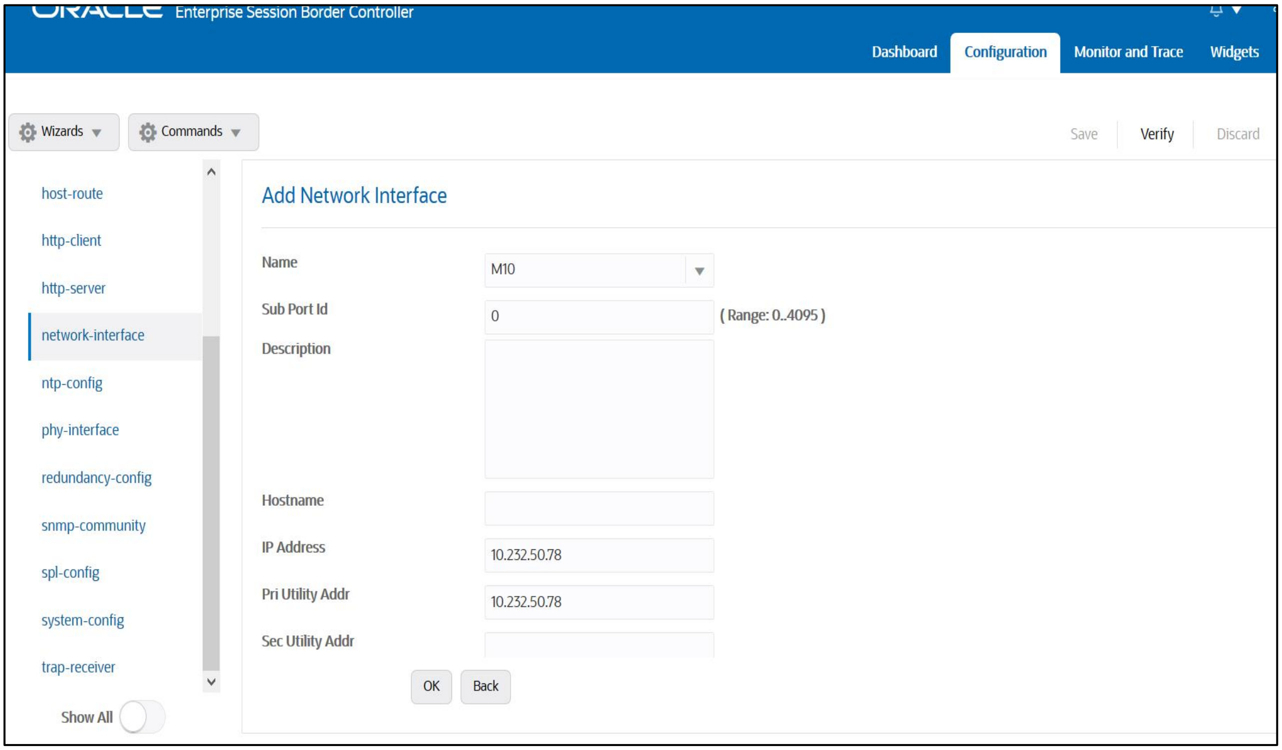
Hostname:

IP Address: [redacted]

Pri Utility Addr: [redacted]

Sec Utility Addr:

Similarly, configure network interface M10 as below



Add Network Interface

Name: M10

Sub Port Id: 0 (Range: 0..4095)

Description:

Hostname:

IP Address: 10.232.50.78

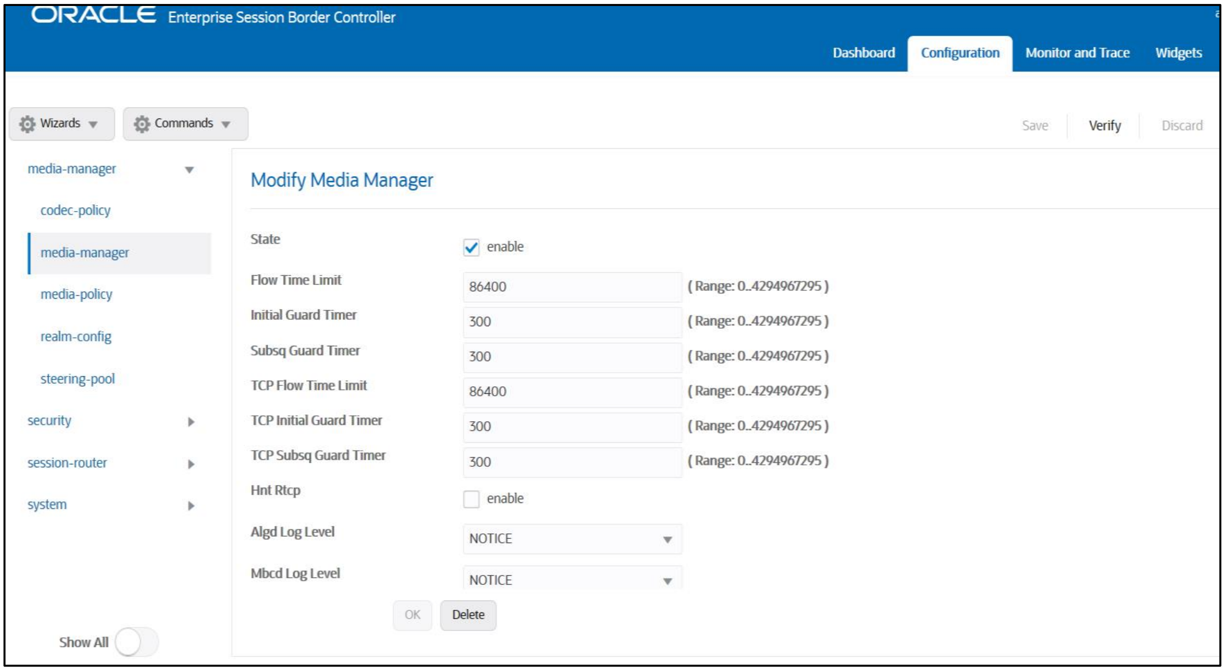
Pri Utility Addr: 10.232.50.78

Sec Utility Addr:

6.6. Enable media manager

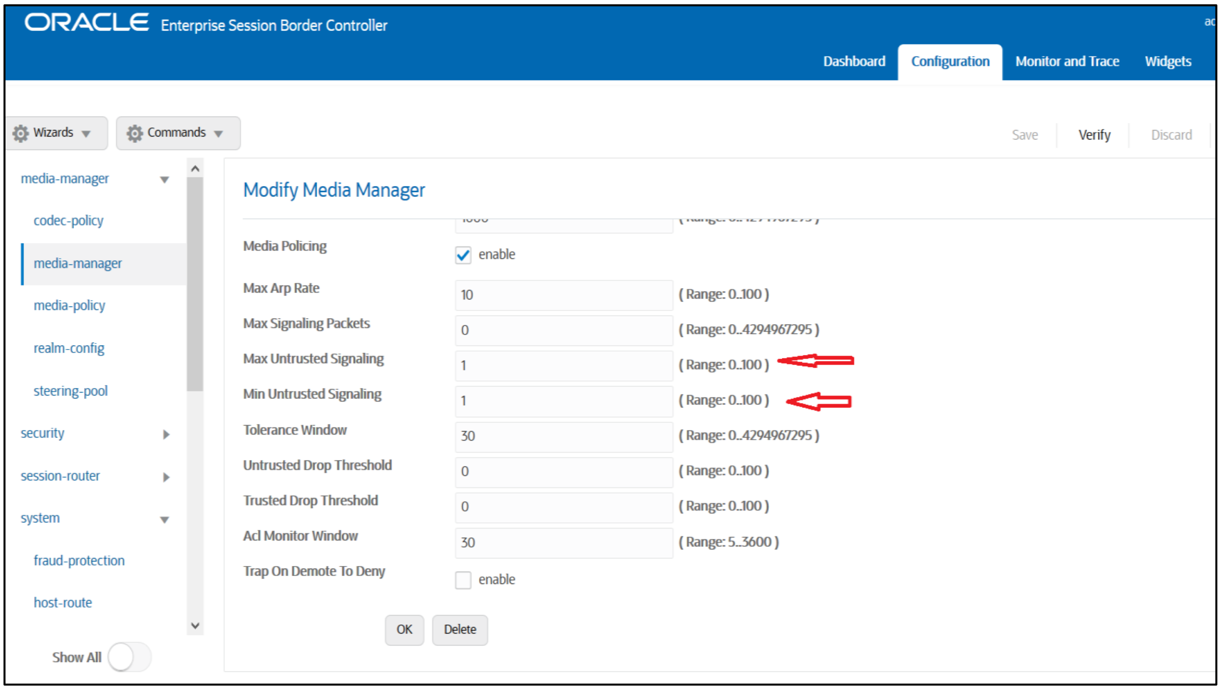
Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

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



Modify Media Manager

State	☑ 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	□ enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	



Modify Media Manager

Media Policing	☑ enable	
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	□ enable	

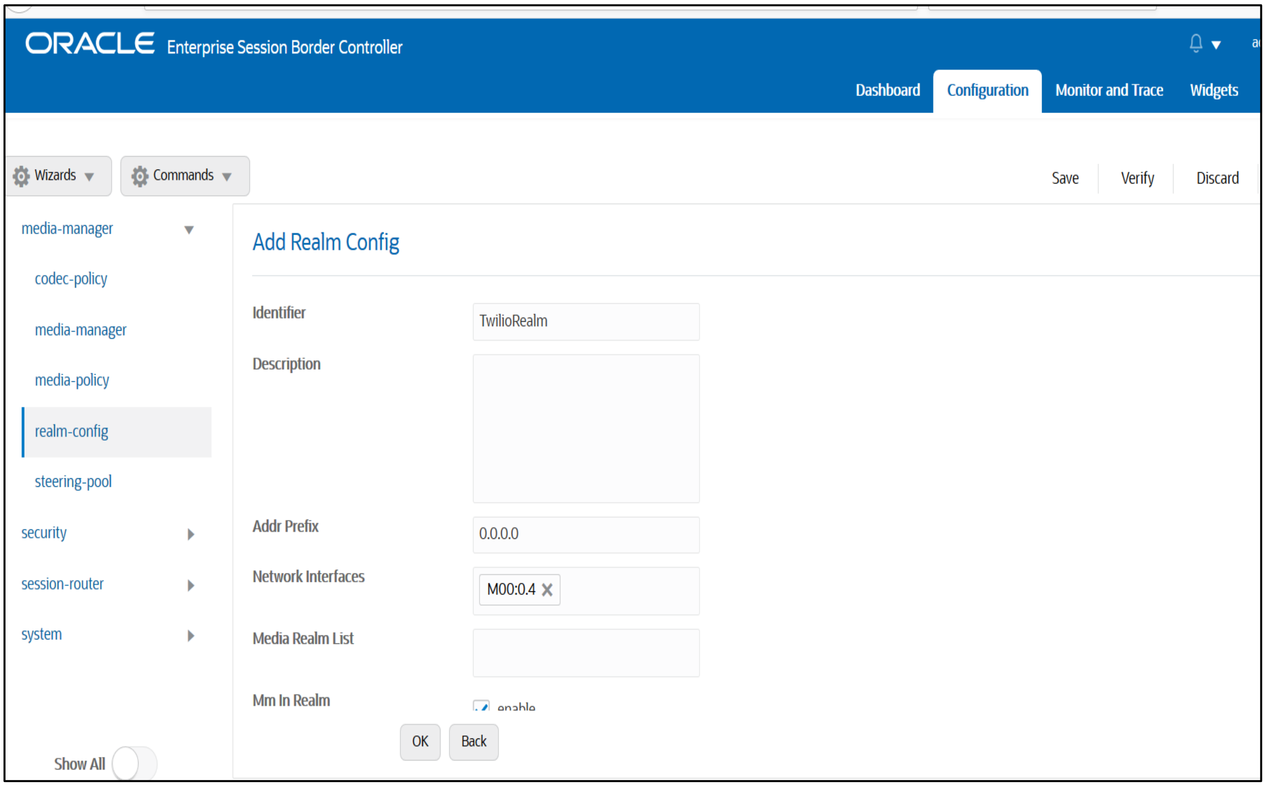
6.7. Configure Realms

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 two realms used in this configuration:

Config Parameter	Twilio Side	Avaya Side
Identifier	TwilioRealm	AvayaRealm
Network Interface	M00	M10
Mm in realm	☑	☑
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



Add Realm Config

Identifier: TwilioRealm

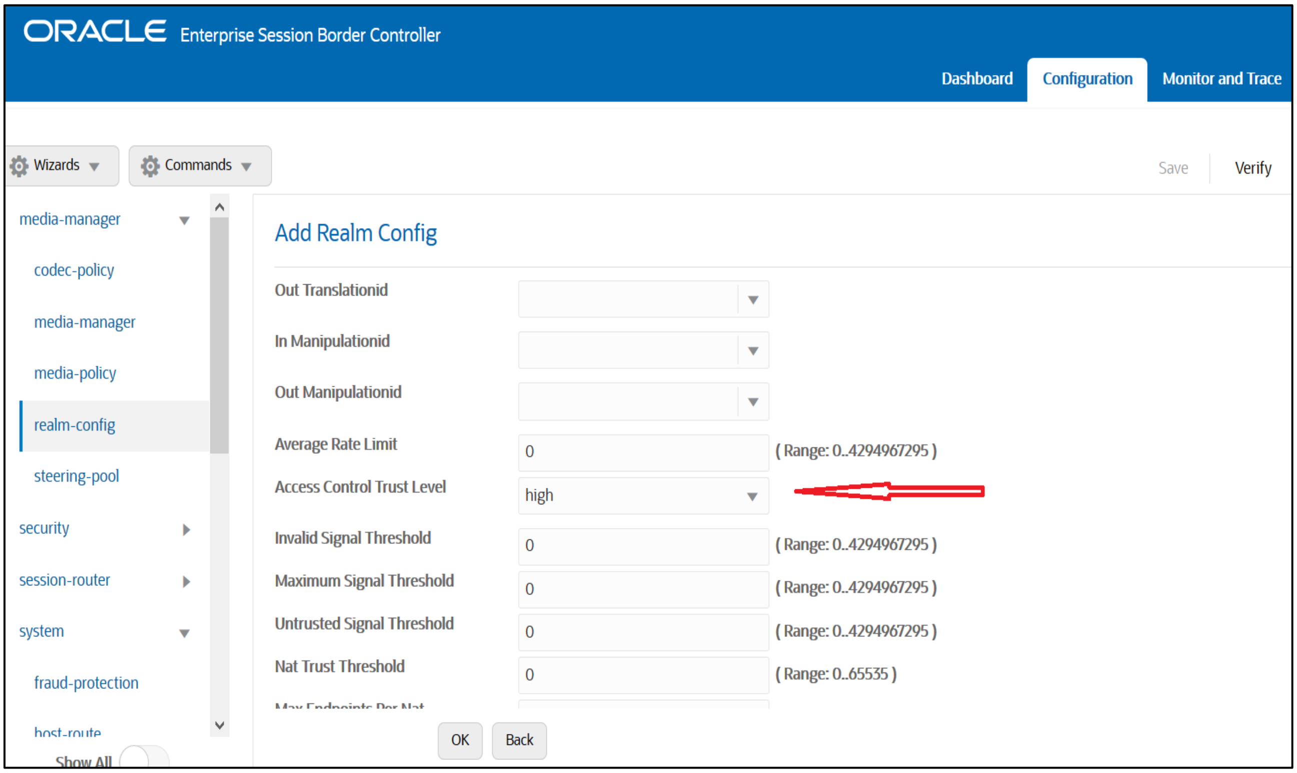
Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M00:0.4 ✕

Media Realm List:

Mm In Realm: ☑ enable



Add Realm Config

Out Translationid

In Manipulationid

Out Manipulationid

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

Access Control Trust Level: high

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

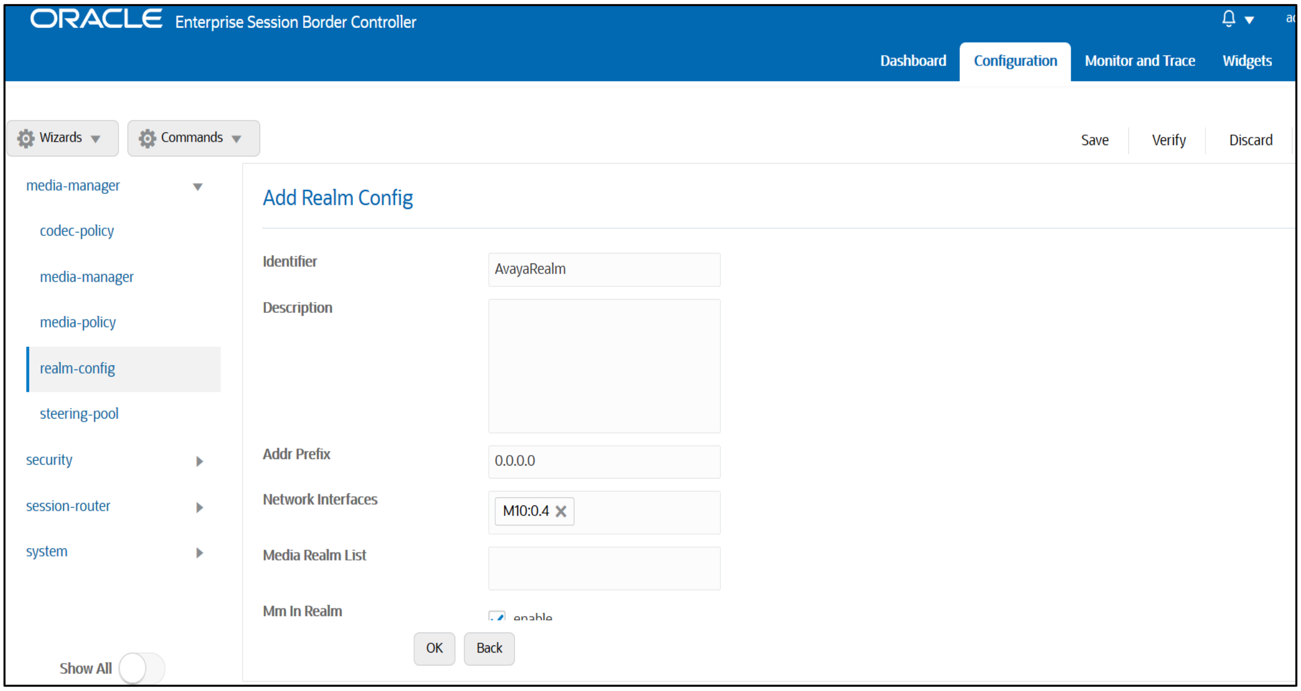
Maximum Signal Threshold: 0 (Range: 0..4294967295)

Untrusted Signal Threshold: 0 (Range: 0..4294967295)

Nat Trust Threshold: 0 (Range: 0..65535)

Max Endpoints Per Nat

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



Add Realm Config

Identifier: AvayaRealm

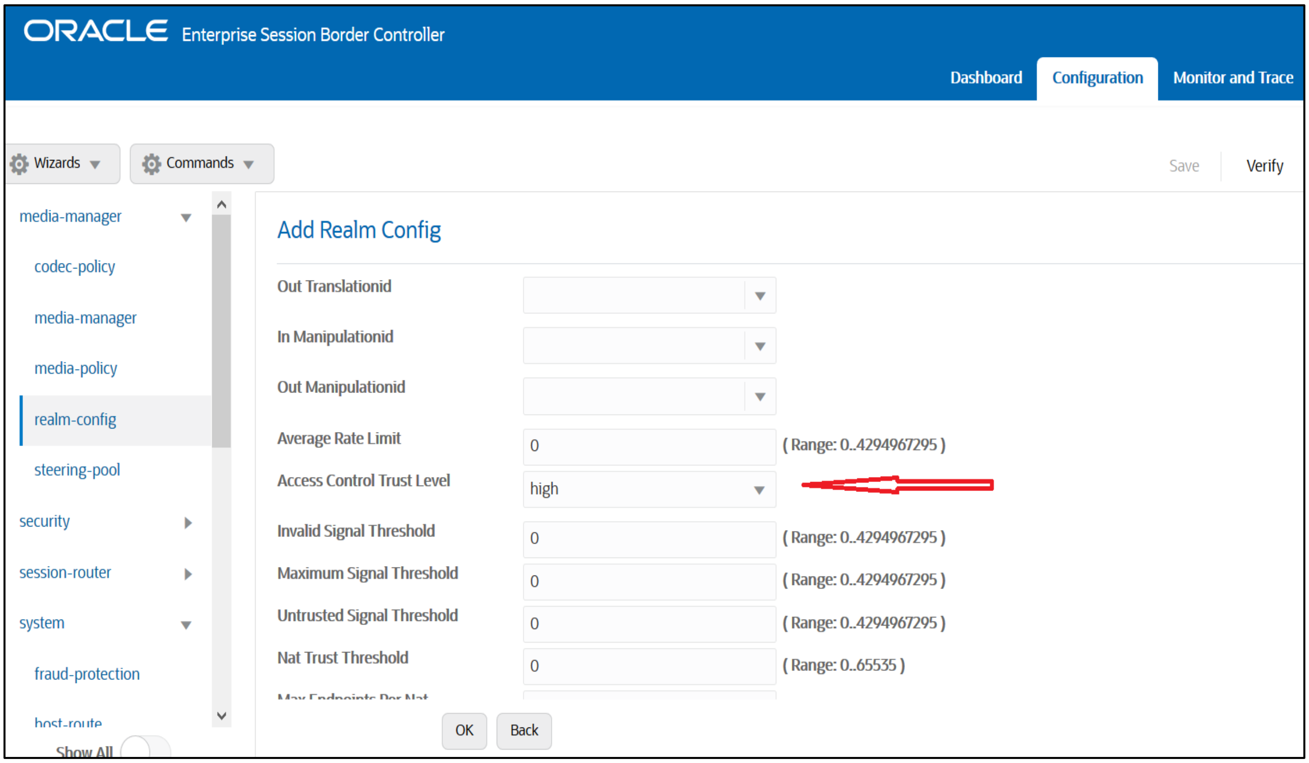
Description

Addr Prefix: 0.0.0.0

Network Interfaces: M10:0.4 ✕

Media Realm List

Mm In Realm: ☑ enable



Add Realm Config

Out Translationid		
In Manipulationid		
Out Manipulationid		
Average Rate Limit	0	(Range: 0..4294967295)
Access Control Trust Level	high	
Invalid Signal Threshold	0	(Range: 0..4294967295)
Maximum Signal Threshold	0	(Range: 0..4294967295)
Untrusted Signal Threshold	0	(Range: 0..4294967295)
Nat Trust Threshold	0	(Range: 0..65535)

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

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

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.

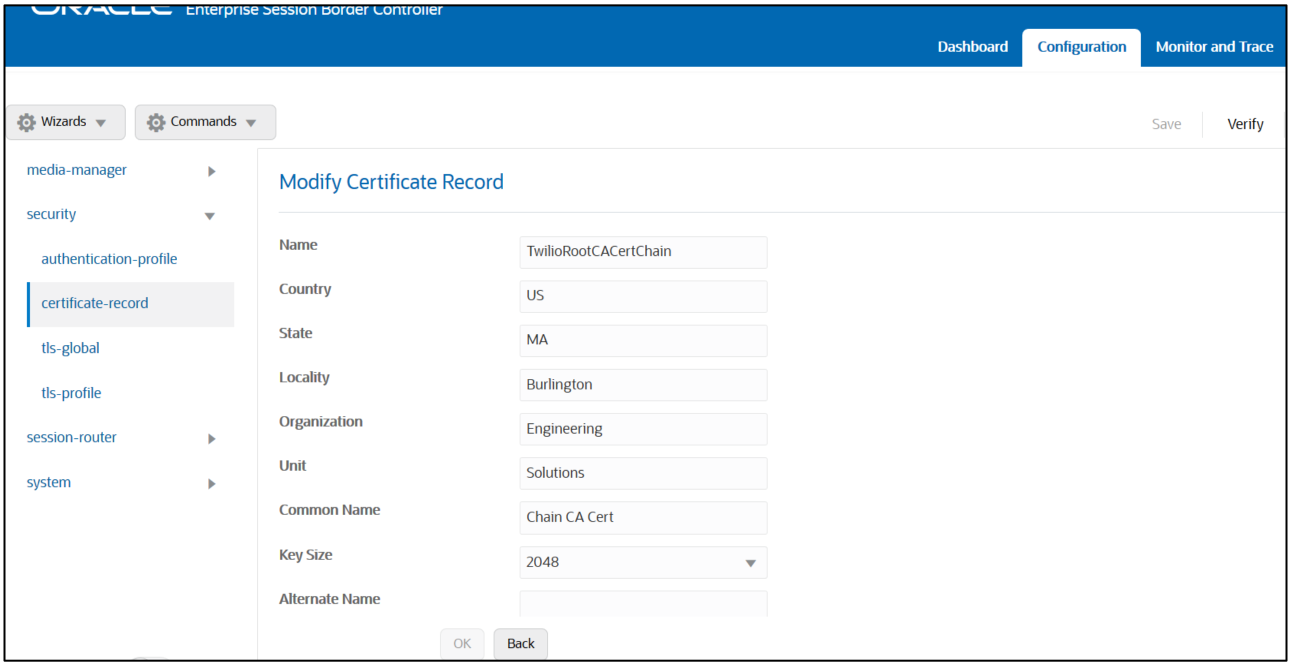
- SBC – 1 certificate-record assigned to SBC
- Root – 1 certificate-record for root cert

2) Deploy the SBC and Root certificates on the SBC

Step 1 – Creating the certificate record

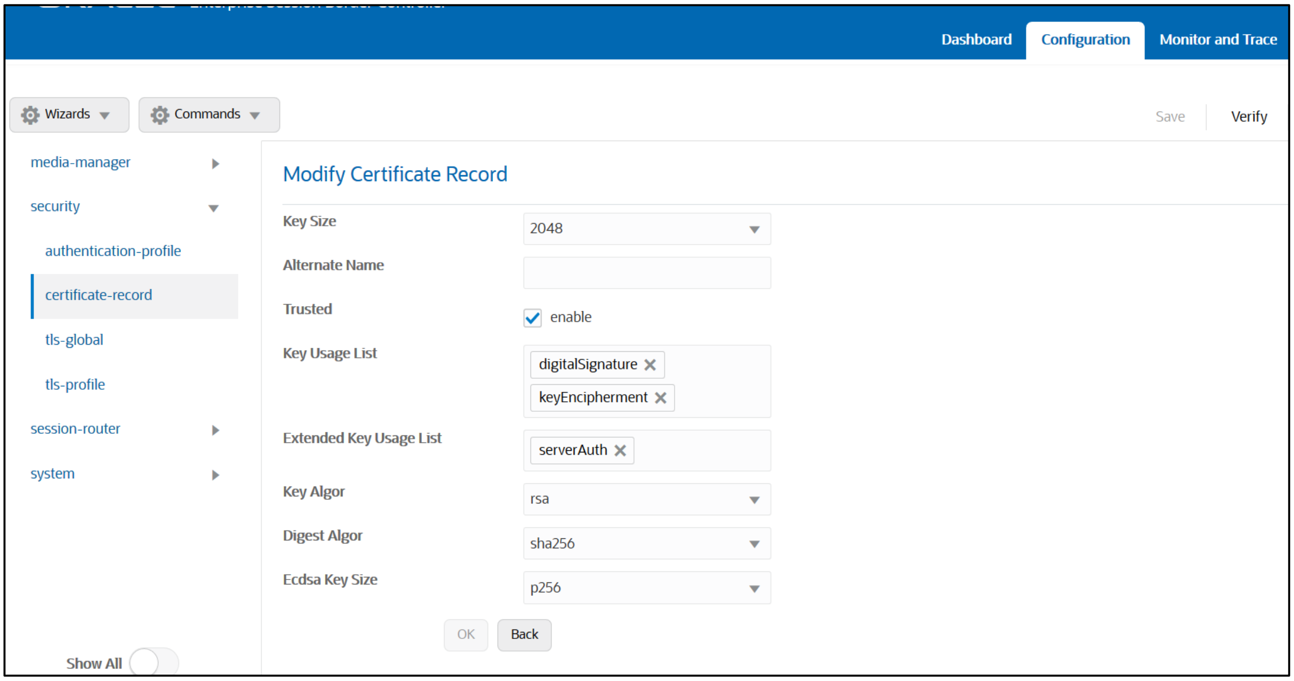
Twilio Elastic SIP Trunking uses certificates from a CA (Certificate Authority) for establishing the TLS connections from SBC’s for SIP traffic, and SRTP for media traffic. It is important that you add the following root certificate to establish TLS connection from the link given below:

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



Modify Certificate Record

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



Modify Certificate Record

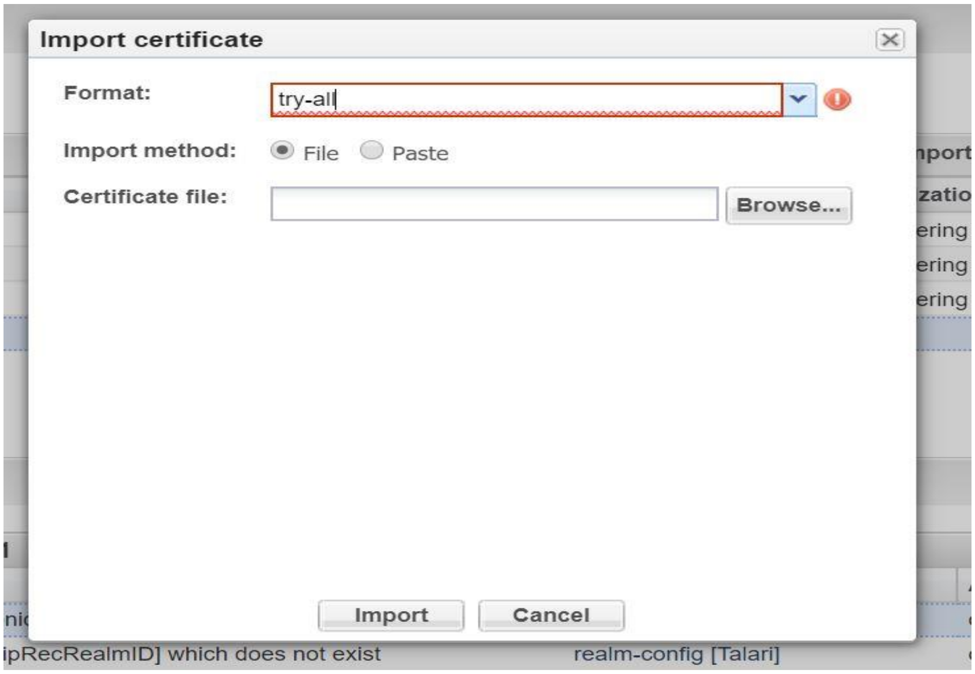
Key Size	2048
Alternate Name	
Trusted	☑ enable
Key Usage List	digitalSignature ✕ keyEncipherment ✕
Extended Key Usage List	serverAuth ✕
Key Algor	rsa
Digest Algor	sha256
Ecdsa Key Size	p256

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



Import certificate

Format: try-all

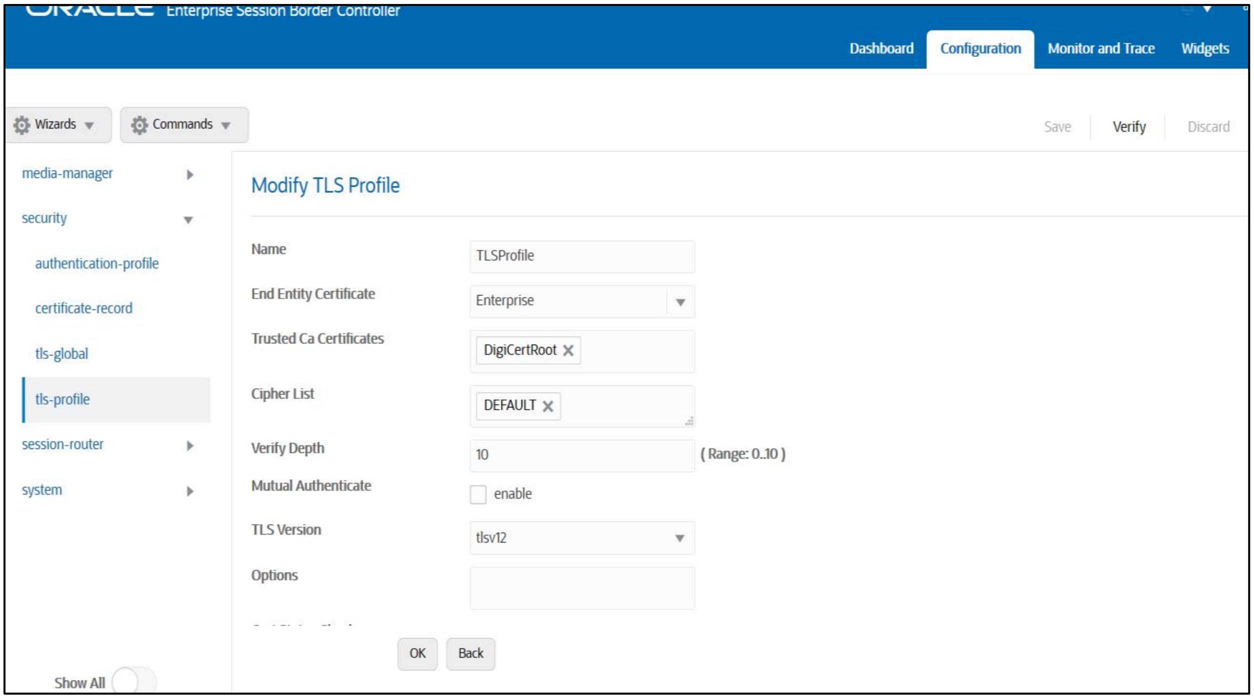
Import method: ● File ○ Paste

Certificate file:

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:



Modify TLS Profile

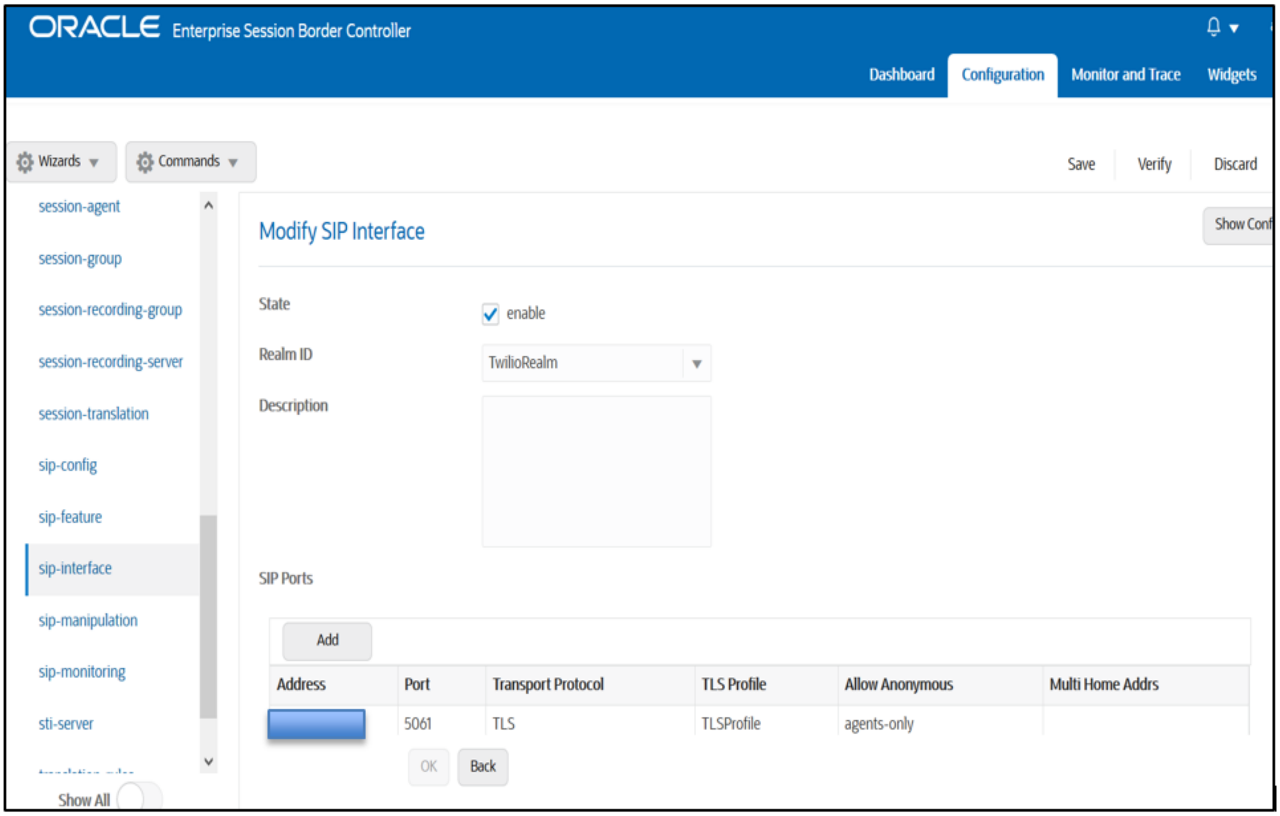
Name	TLSProfile
End Entity Certificate	Enterprise
Trusted Ca Certificates	DigiCertRoot
Cipher List	DEFAULT
Verify Depth	10 (Range: 0..10)
Mutual Authenticate	□ enable
TLS Version	tlsv12
Options	

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.



Modify SIP Interface

State ☑ enable

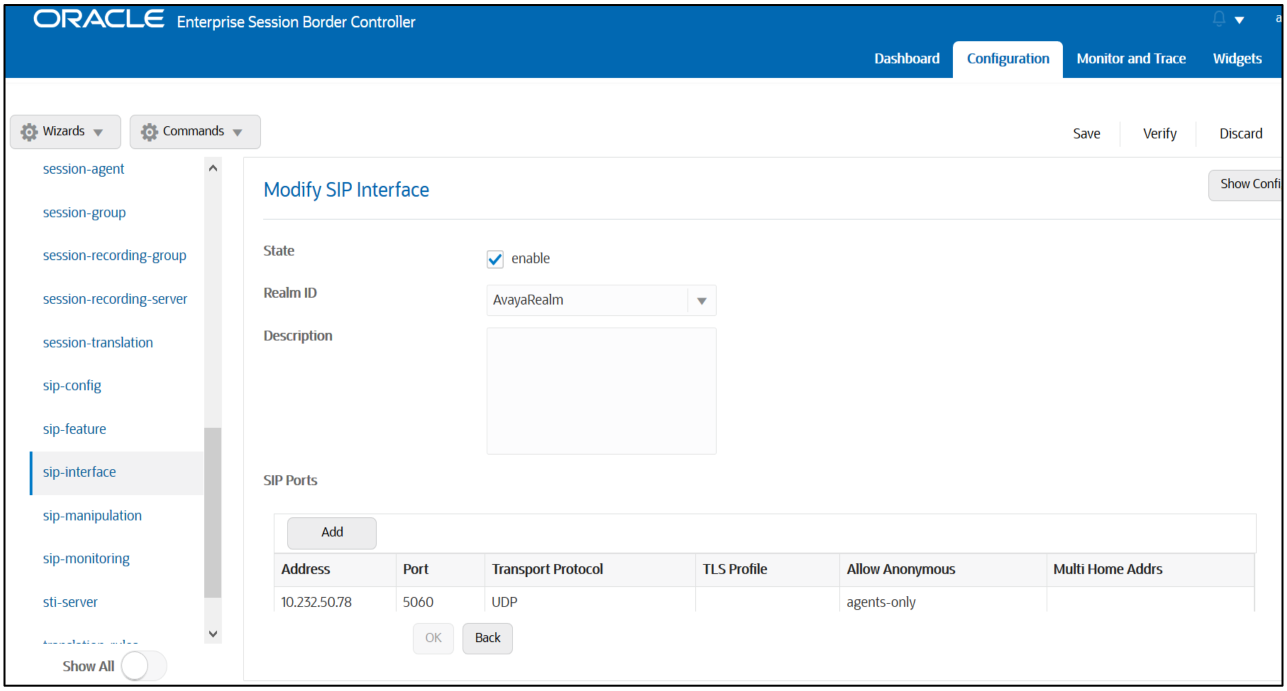
Realm ID TwilioRealm

Description

SIP Ports

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

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



Modify SIP Interface

State ☑ enable

Realm ID AvayaRealm

Description

SIP Ports

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

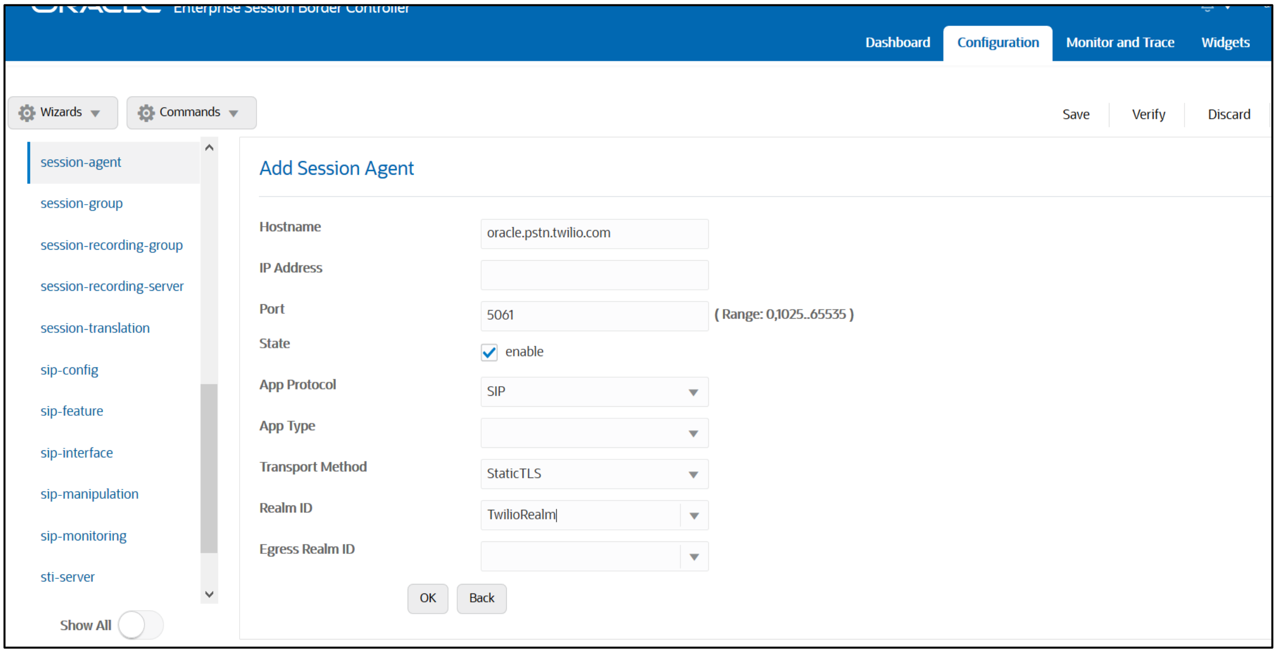
Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

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”



Add Session Agent

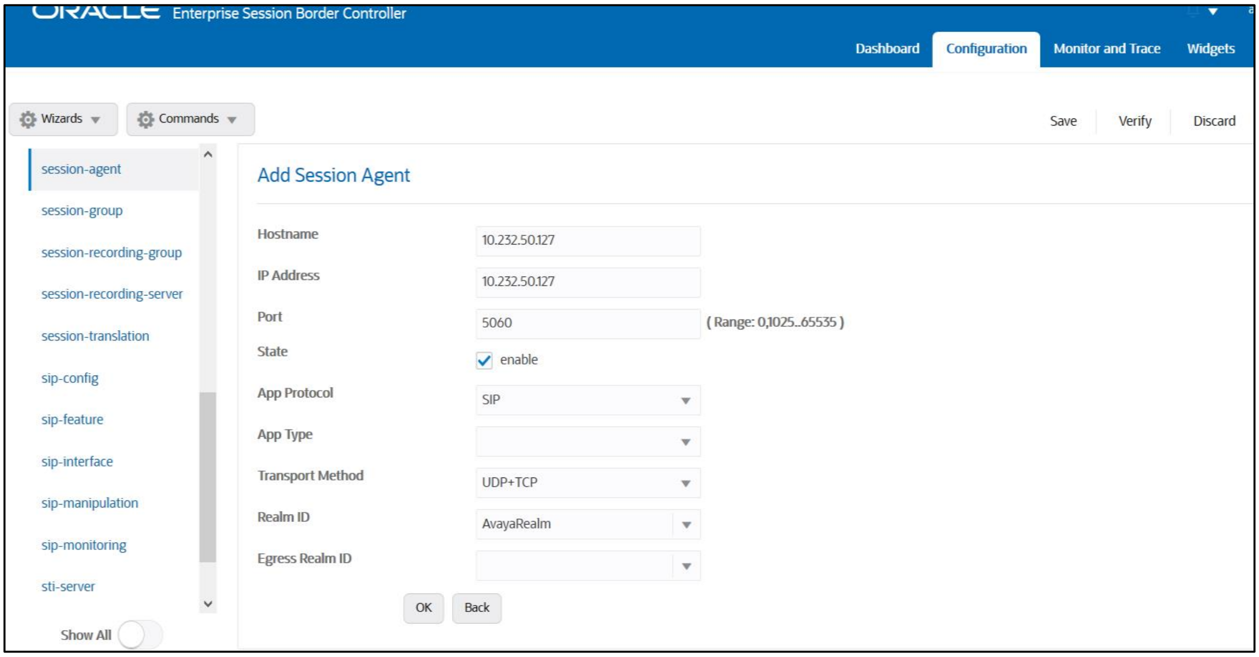
Hostname: oracle.pstn.twilio.com
IP Address:
Port: 5061 (Range: 0,1025..65535)
State: ☑ enable
App Protocol: SIP
App Type:
Transport Method: StaticTLS
Realm ID: TwilioRealm
Egress Realm ID:

****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:



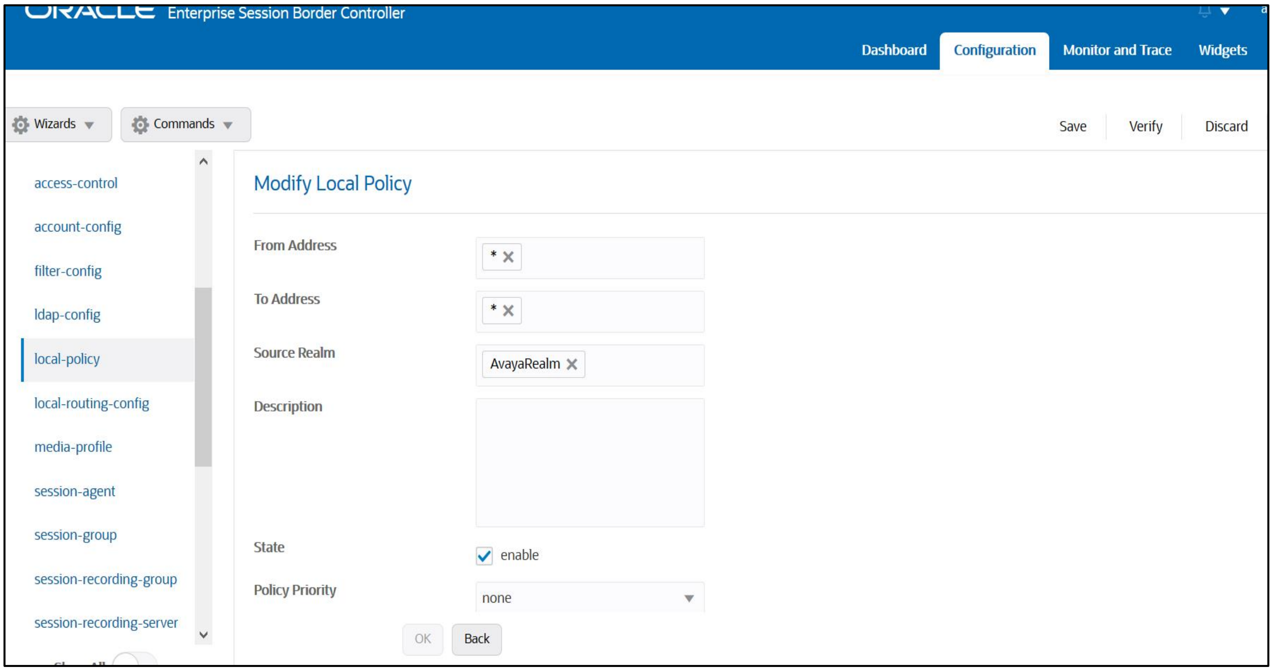
Add Session Agent

Hostname	10.232.50.127
IP Address	10.232.50.127
Port	5060 (Range: 0,1025..65535)
State	☑ enable
App Protocol	SIP
App Type	
Transport Method	UDP+TCP
Realm ID	AvayaRealm
Egress Realm ID	

6.12. Configure local-policy

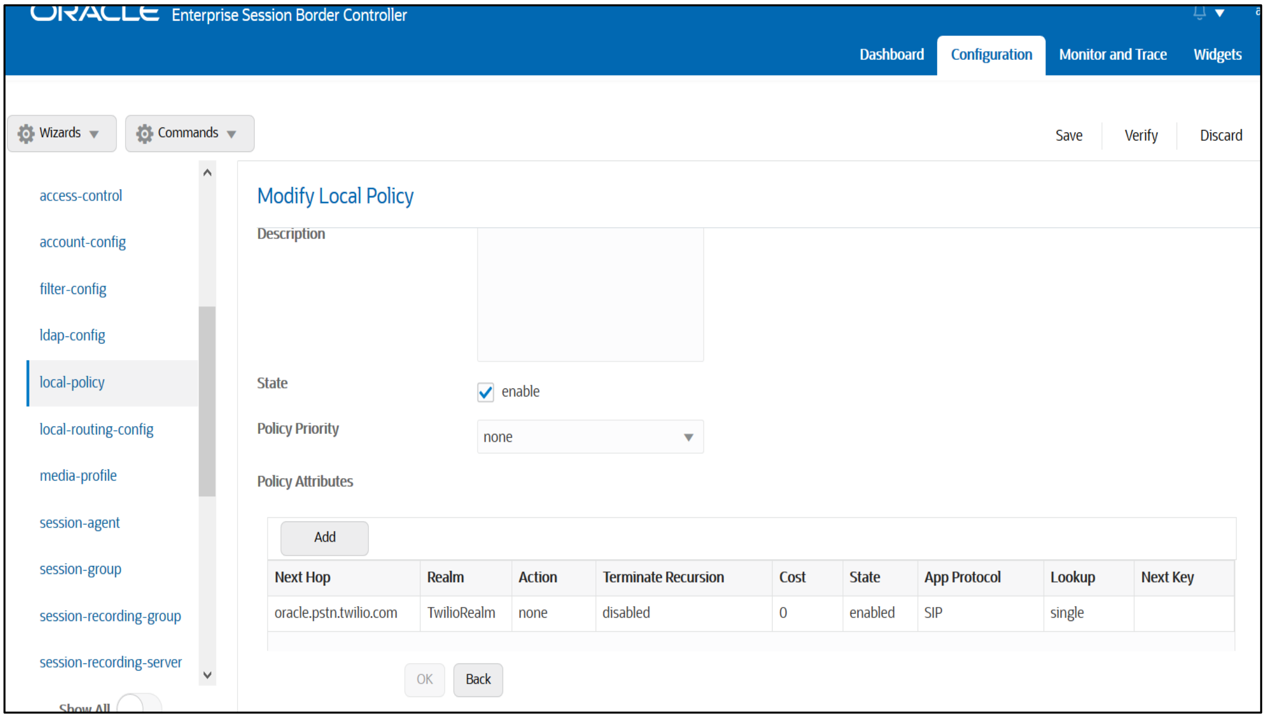
Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

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



Modify Local Policy

From Address	*
To Address	*
Source Realm	AvayaRealm
Description	
State	☑ enable
Policy Priority	none



Modify Local Policy

Description

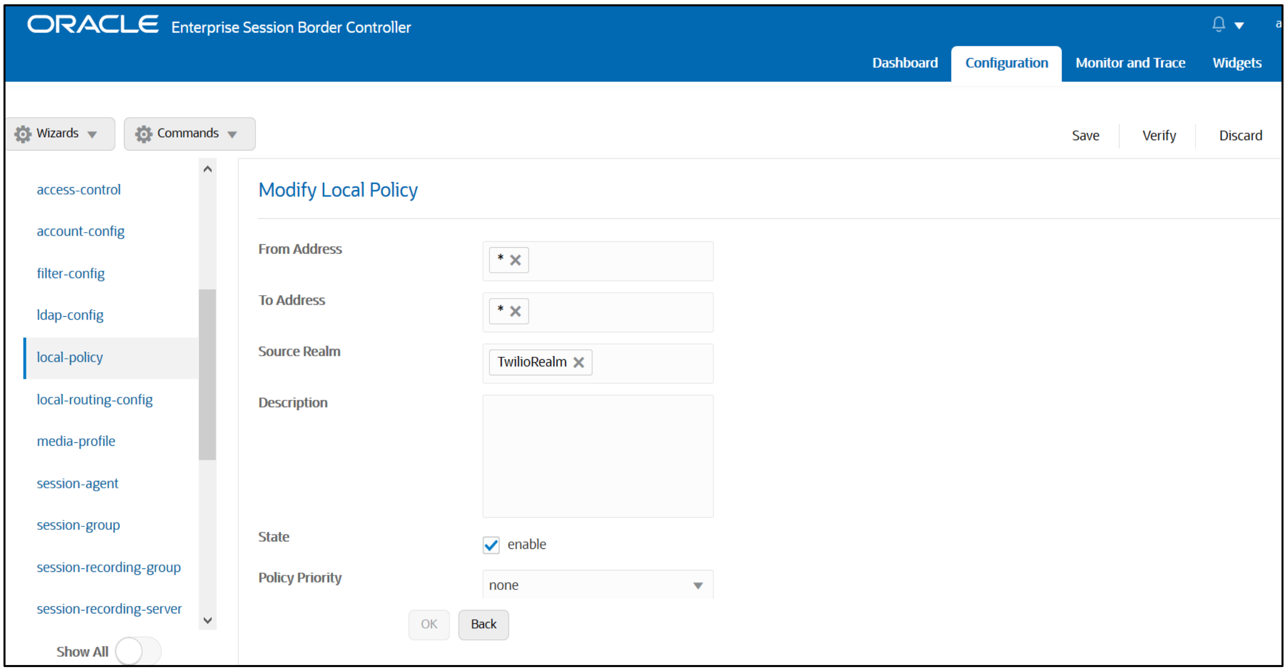
State ☑ enable

Policy Priority: none

Policy Attributes

Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
oracle.pstn.twilio.com	TwilioRealm	none	disabled	0	enabled	SIP	single	

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



Modify Local Policy

From Address: *

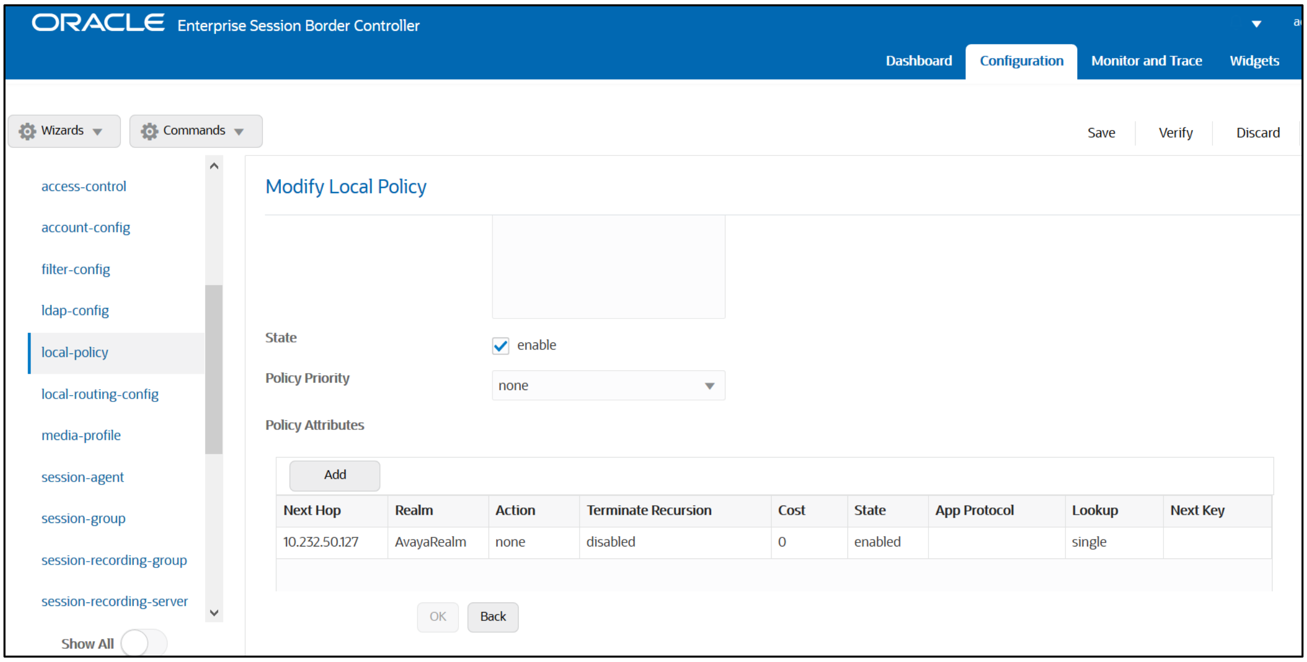
To Address: *

Source Realm: TwilioRealm

Description

State ☑ enable

Policy Priority: none



Modify Local Policy

State ☑ enable

Policy Priority: none

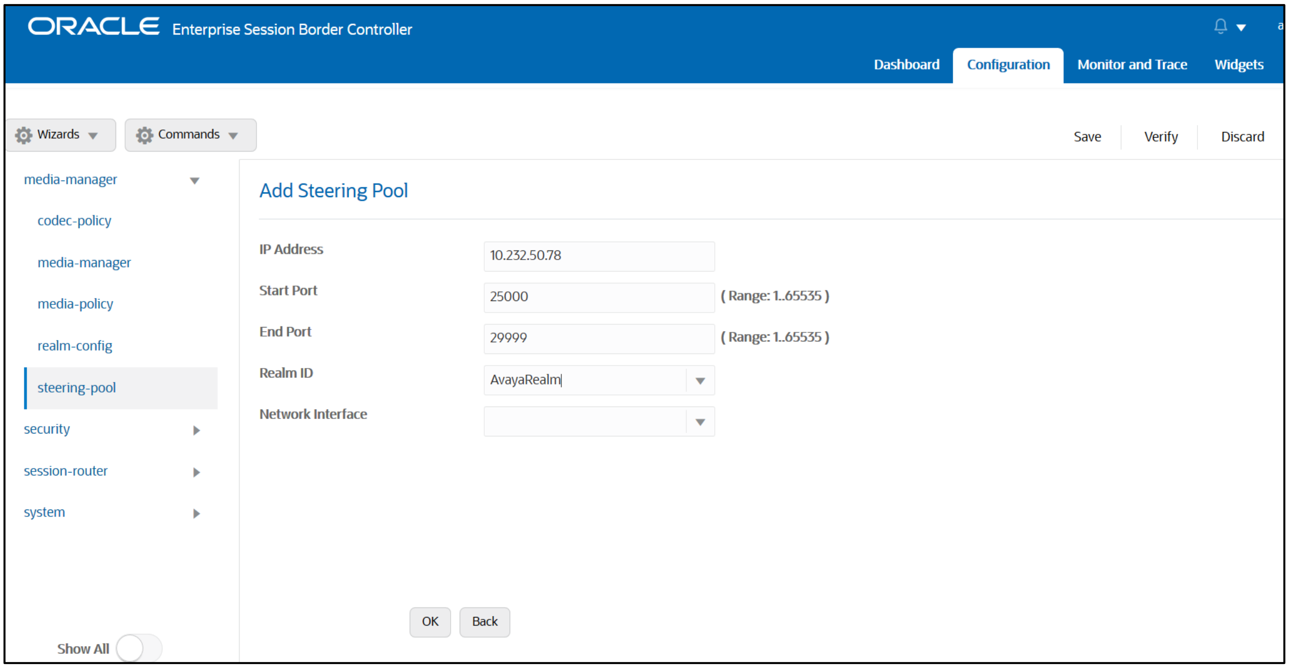
Policy Attributes

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

6.13. Configure steering-pool

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

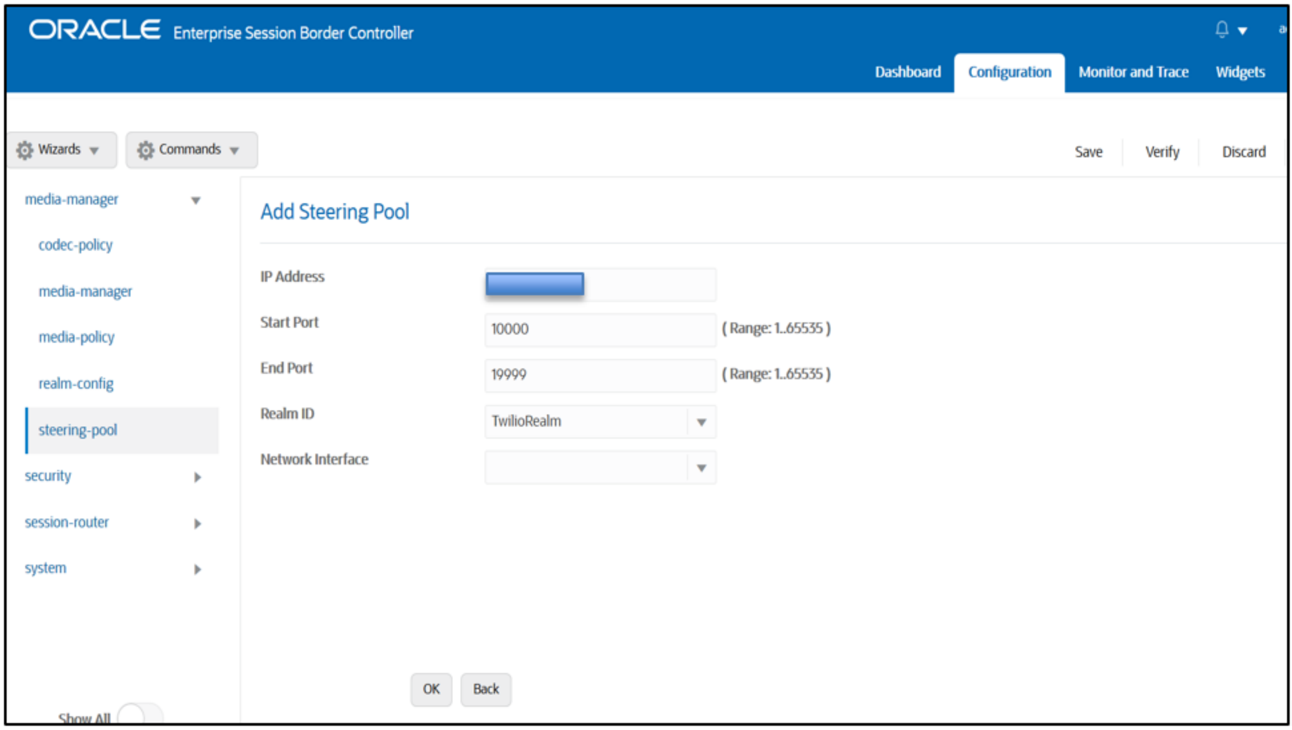
Avaya side steering pool.



Add Steering Pool

IP Address	10.232.50.78
Start Port	25000 (Range: 1..65535)
End Port	29999 (Range: 1..65535)
Realm ID	AvayaRealm
Network Interface	

Twilio side steering pool.



Add Steering Pool

IP Address [redacted]

Start Port 10000 (Range: 1..65535)

End Port 19999 (Range: 1..65535)

Realm ID TwilioRealm

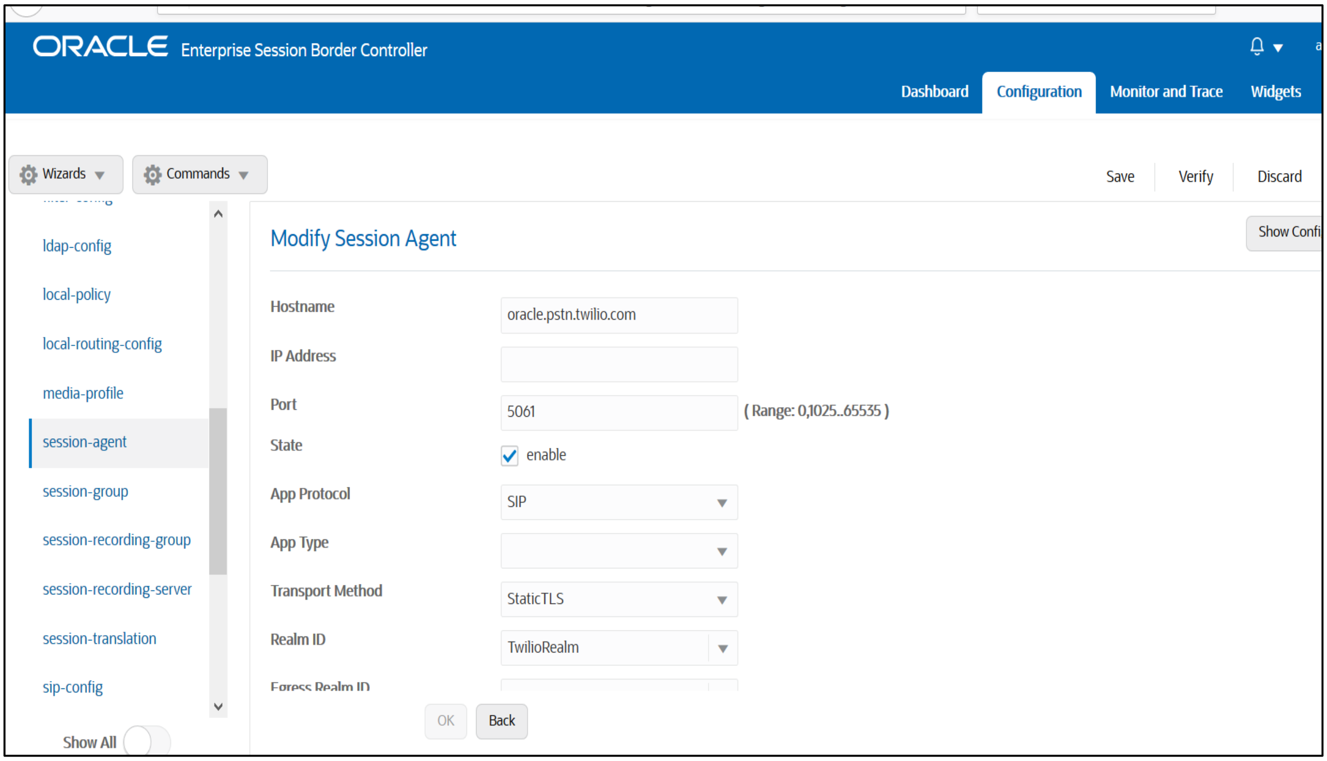
Network Interface

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.



Modify Session Agent

Hostname: oracle.pstn.twilio.com

IP Address:

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

State: ☑ enable

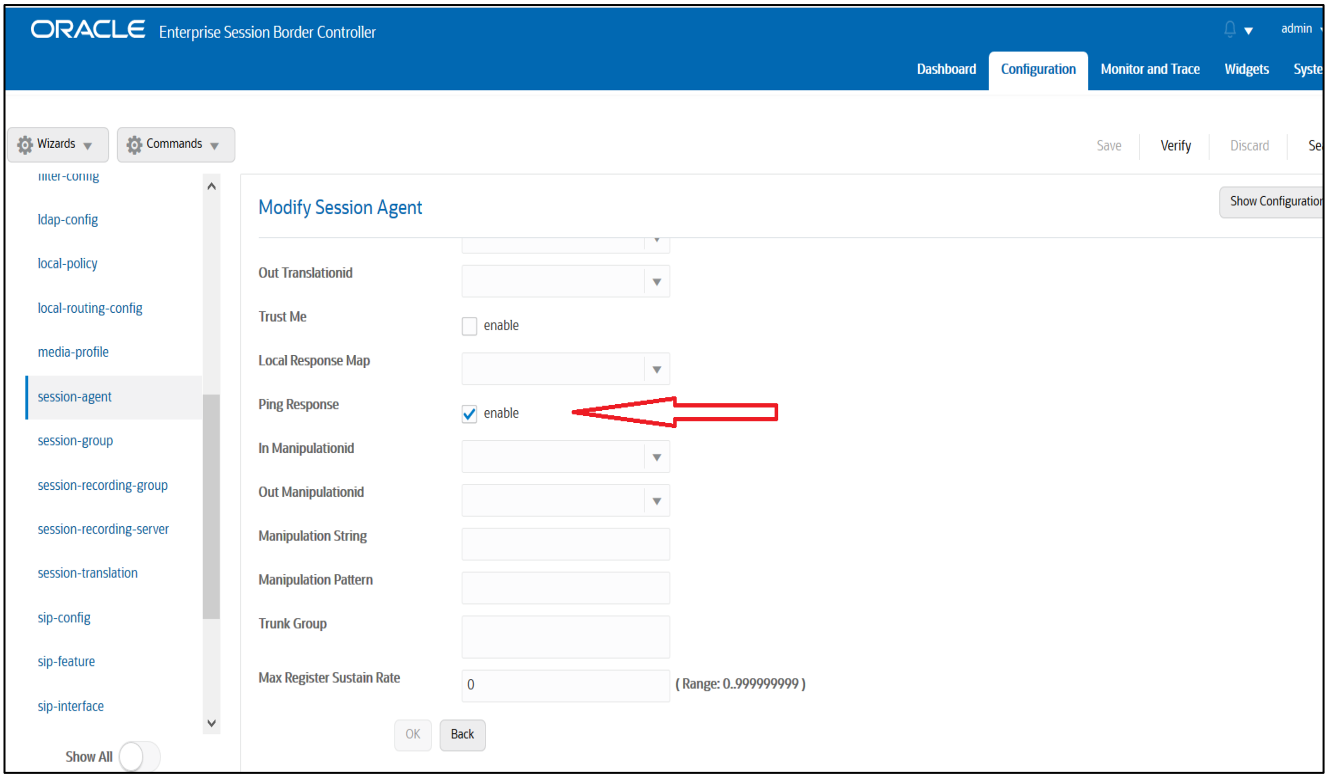
App Protocol: SIP

App Type:

Transport Method: StaticTLS

Realm ID: TwilioRealm

Egress Realm ID



Modify Session Agent

Out Translationid:

Trust Me: □ enable

Local Response Map:

Ping Response: ☑ enable

In Manipulationid:

Out Manipulationid:

Manipulation String:

Manipulation Pattern:

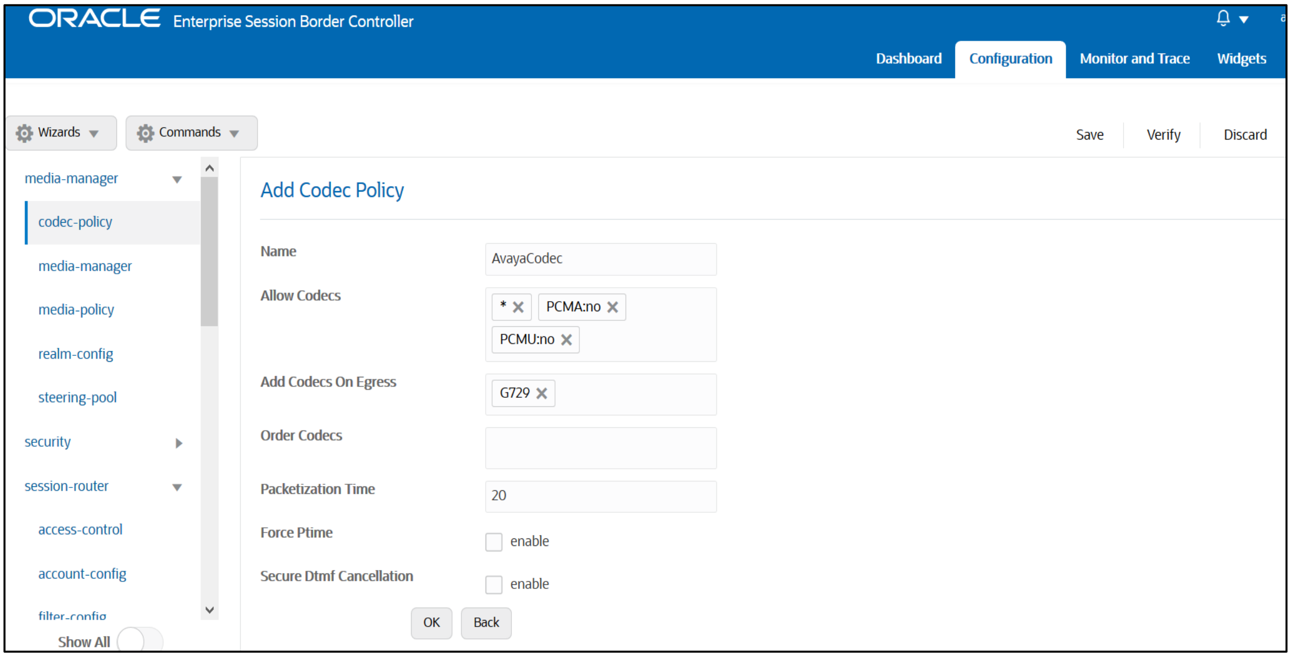
Trunk Group:

Max Register Sustain Rate: 0 (Range: 0..999999999)

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

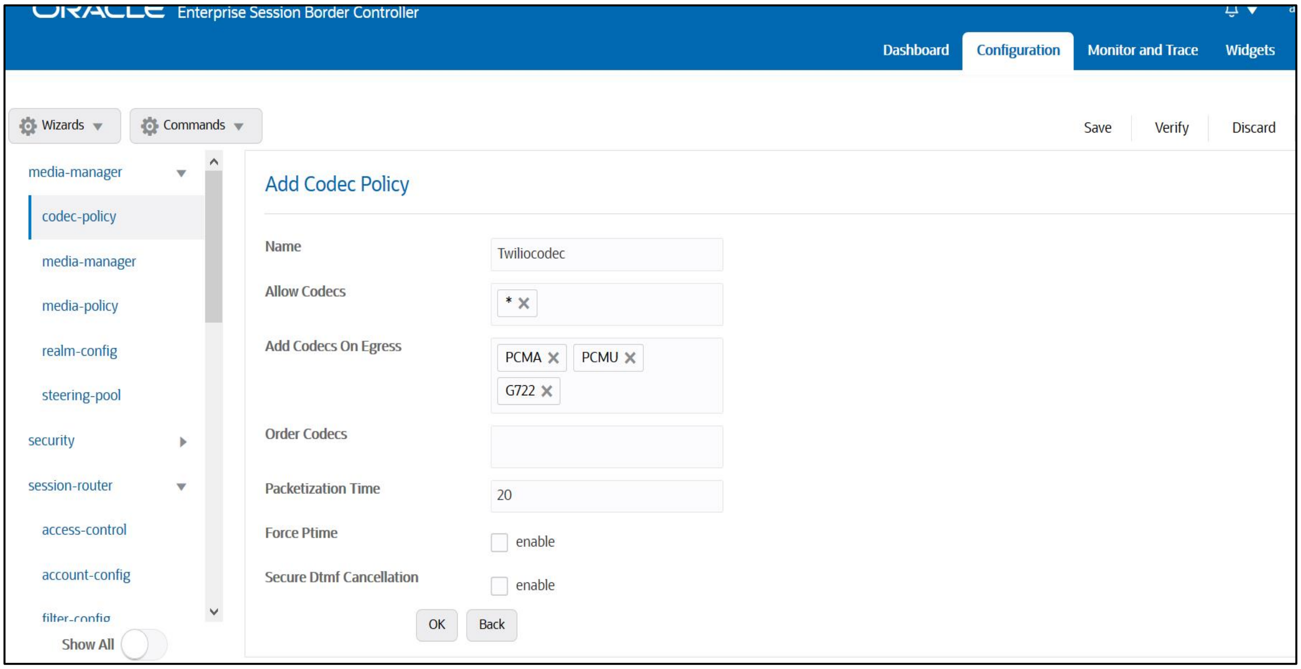
Configure the below Codec policy for Avaya Side. **Assign this codec policy to the AvayaRealm.**



Add Codec Policy

Name	AvayaCodec
Allow Codecs	* PCMA:no PCMU:no
Add Codecs On Egress	G729
Order Codecs	
Packetization Time	20
Force Ptime	□ enable
Secure Dtmf Cancellation	□ enable

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

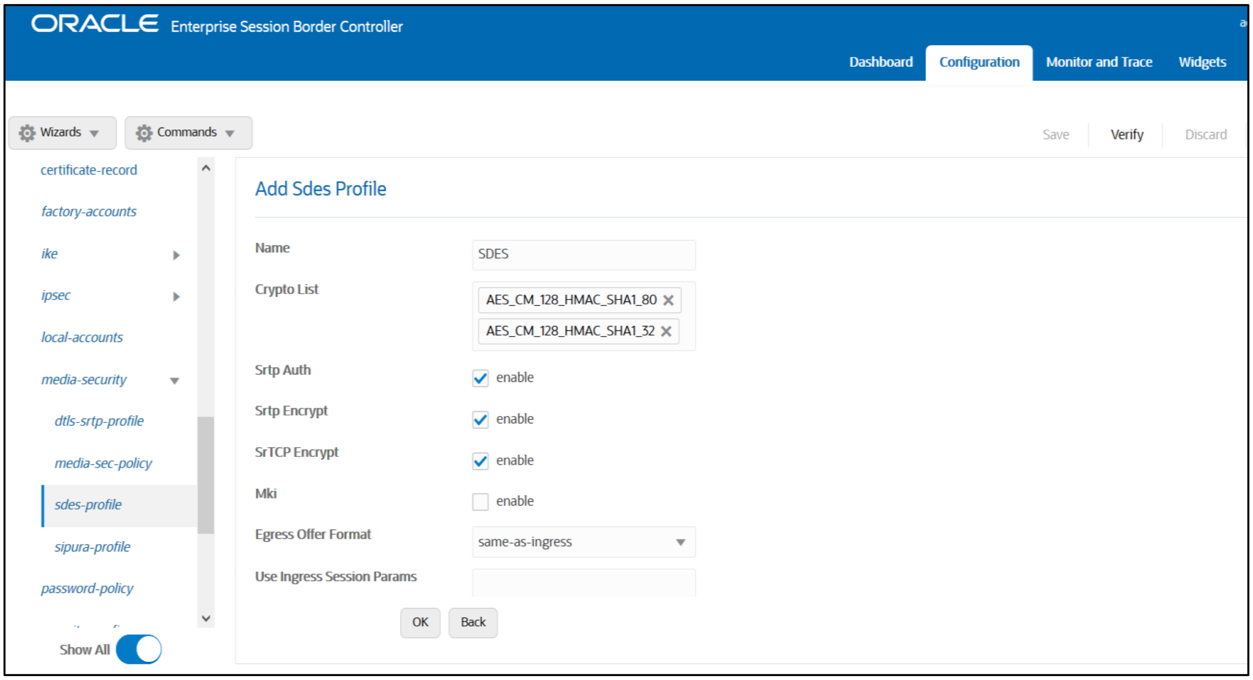


Add Codec Policy

Name	Twiliocodec
Allow Codecs	*
Add Codecs On Egress	PCMA PCMU G722
Order Codecs	
Packetization Time	20
Force Ptime	□ enable
Secure Dtmf Cancellation	□ enable

6.16. Configure sdes profile

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

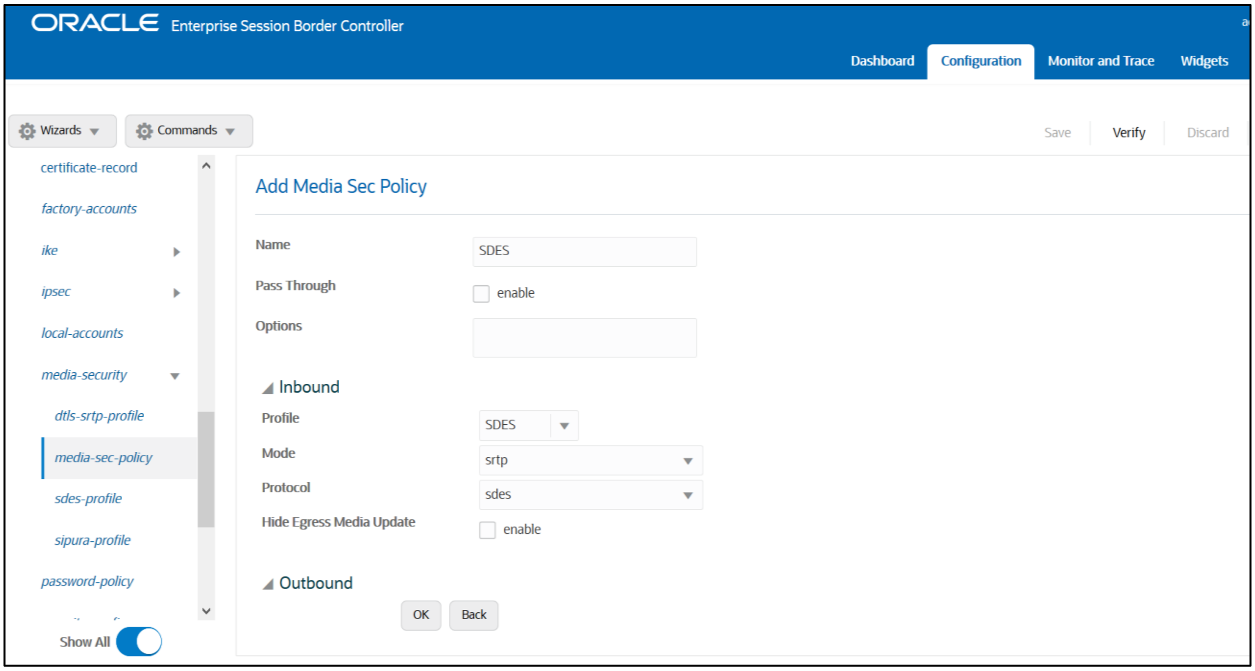


Add Sdes Profile

Name	SDES
Crypto List	AES_CM_128_HMAC_SHA1_80 ✕ AES_CM_128_HMAC_SHA1_32 ✕
Srtp Auth	☑ enable
Srtp Encrypt	☑ enable
SrTCP Encrypt	☑ enable
Mki	□ enable
Egress Offer Format	same-as-ingress
Use Ingress Session Params	

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.



Add Media Sec Policy

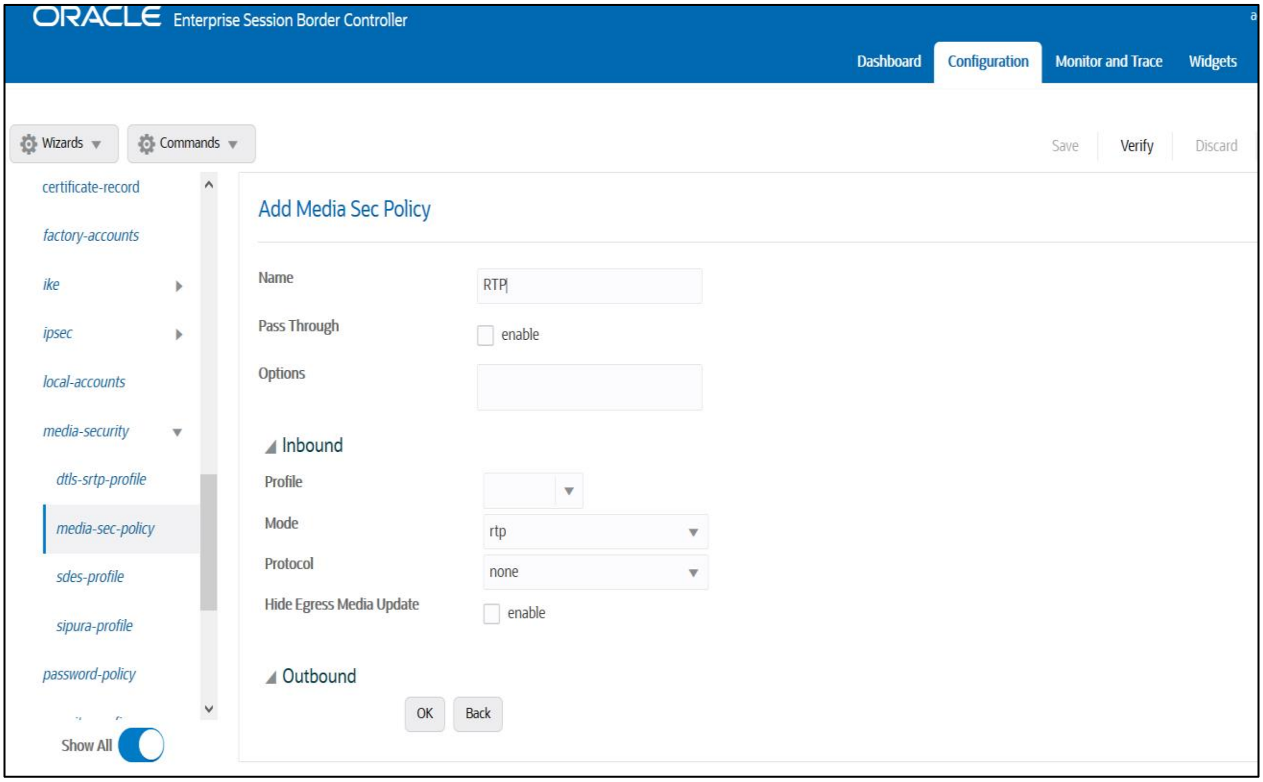
Name	SDES
Pass Through	□ enable
Options	

◢ Inbound

Profile	SDES
Mode	srtp
Protocol	sdes
Hide Egress Media Update	□ enable

◢ Outbound

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.**



Add Media Sec Policy

Name: RTP

Pass Through: □ enable

Options:

Inbound

Profile:

Mode: rtp

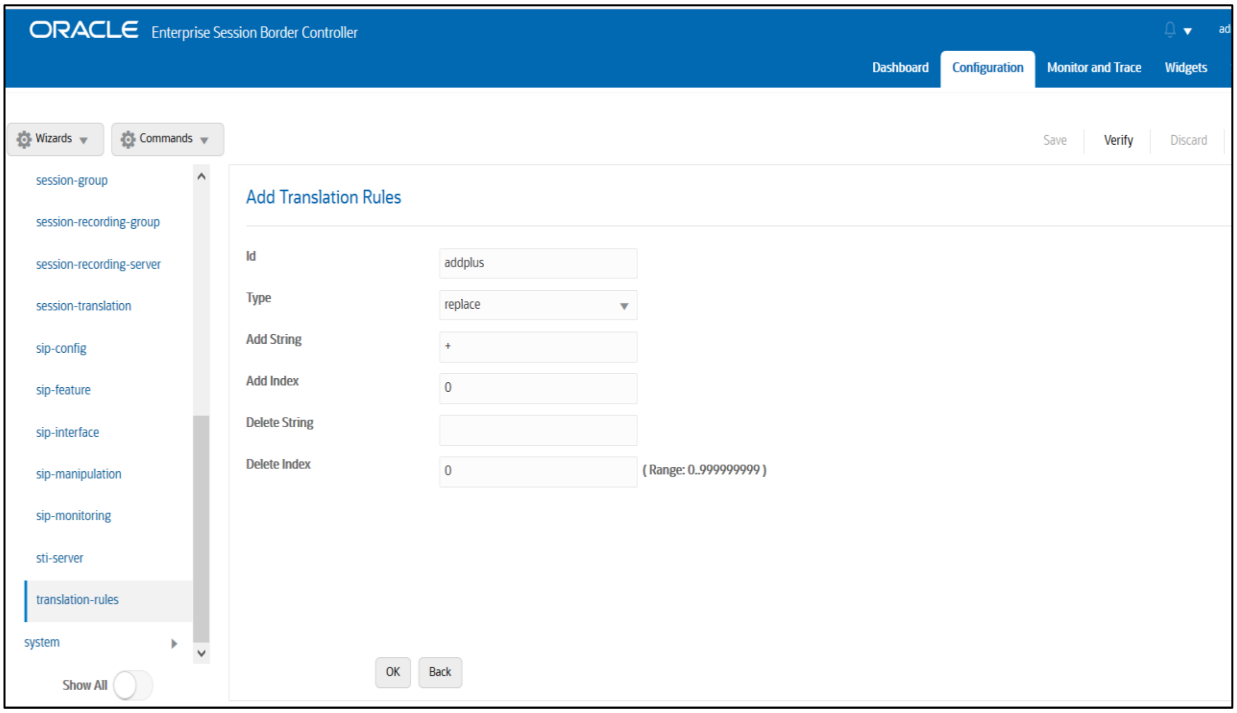
Protocol: none

Hide Egress Media Update: □ enable

Outbound

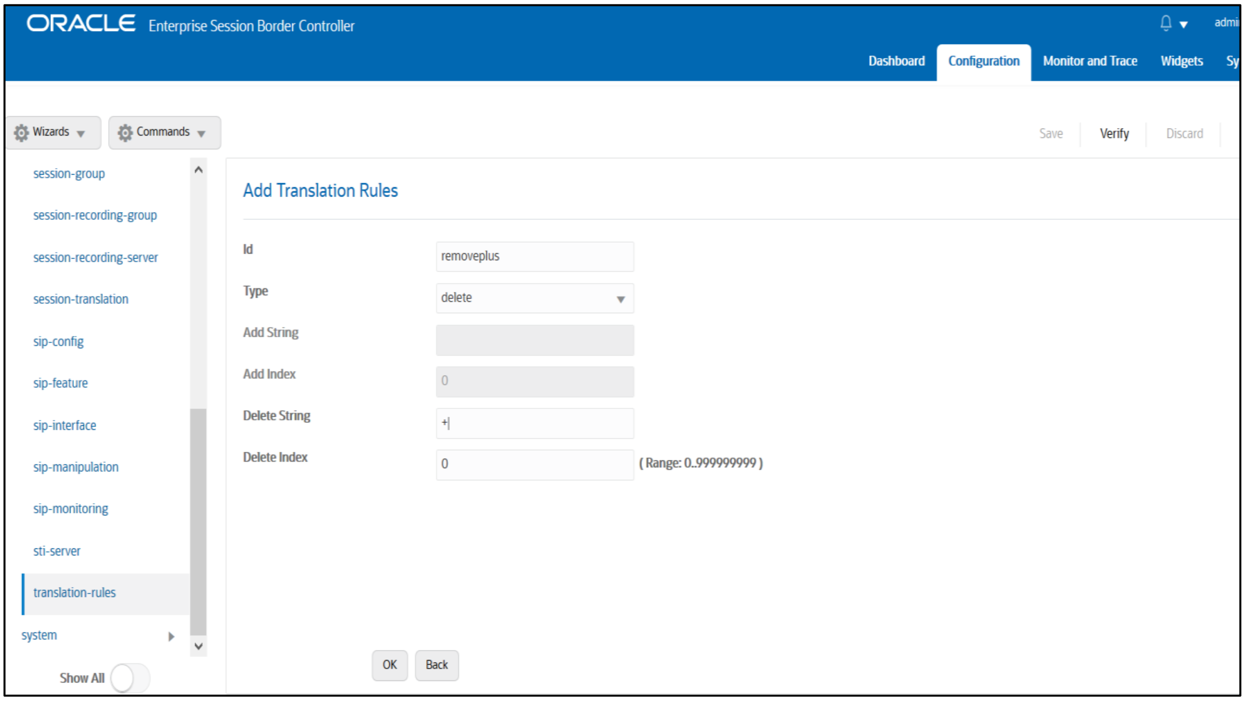
6.18. Configure Translation Rules

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



Add Translation Rules

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



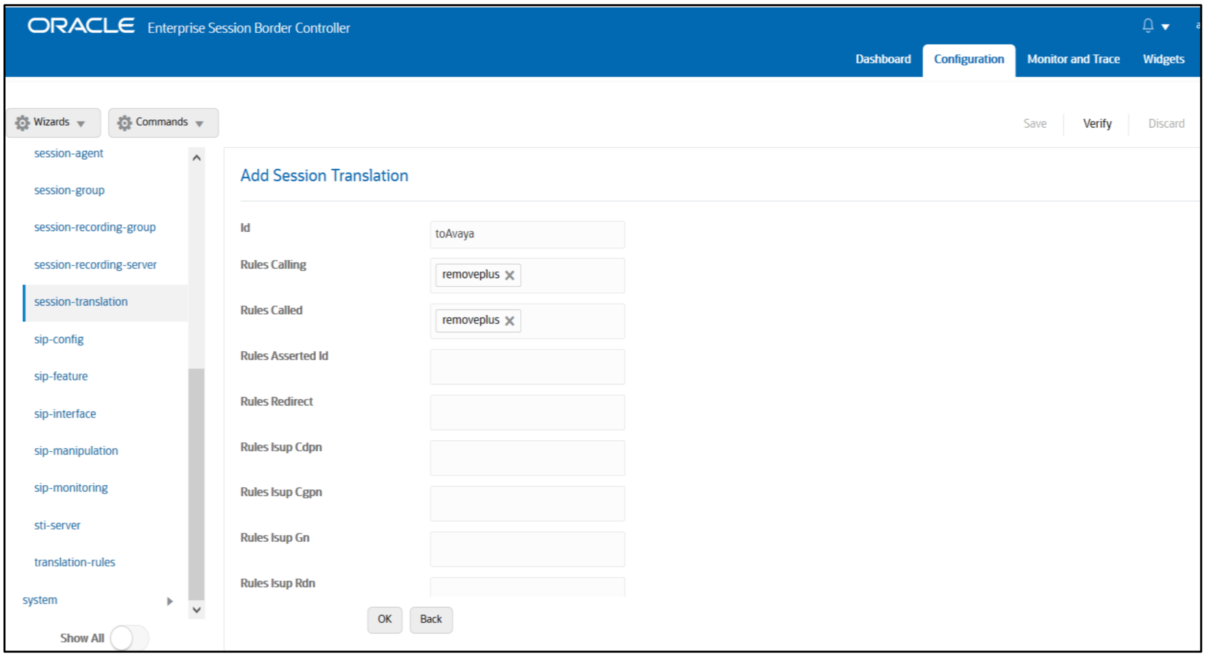
Add Translation Rules

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

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



Add Session Translation

Id: toAvaya

Rules Calling: removeplus

Rules Called: removeplus

Rules Asserted Id:

Rules Redirect:

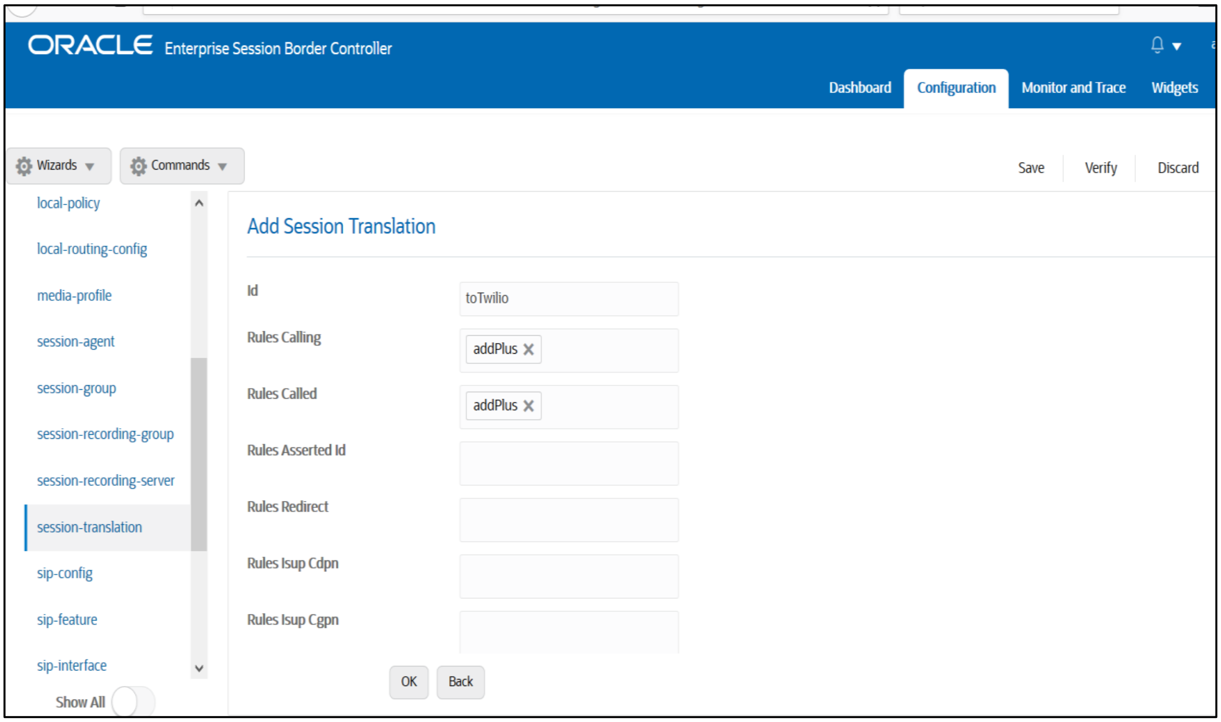
Rules Isup Cdpn:

Rules Isup Cgpn:

Rules Isup Gn:

Rules Isup Rdn:

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



Add Session Translation

Id: toTwilio

Rules Calling: addPlus

Rules Called: addPlus

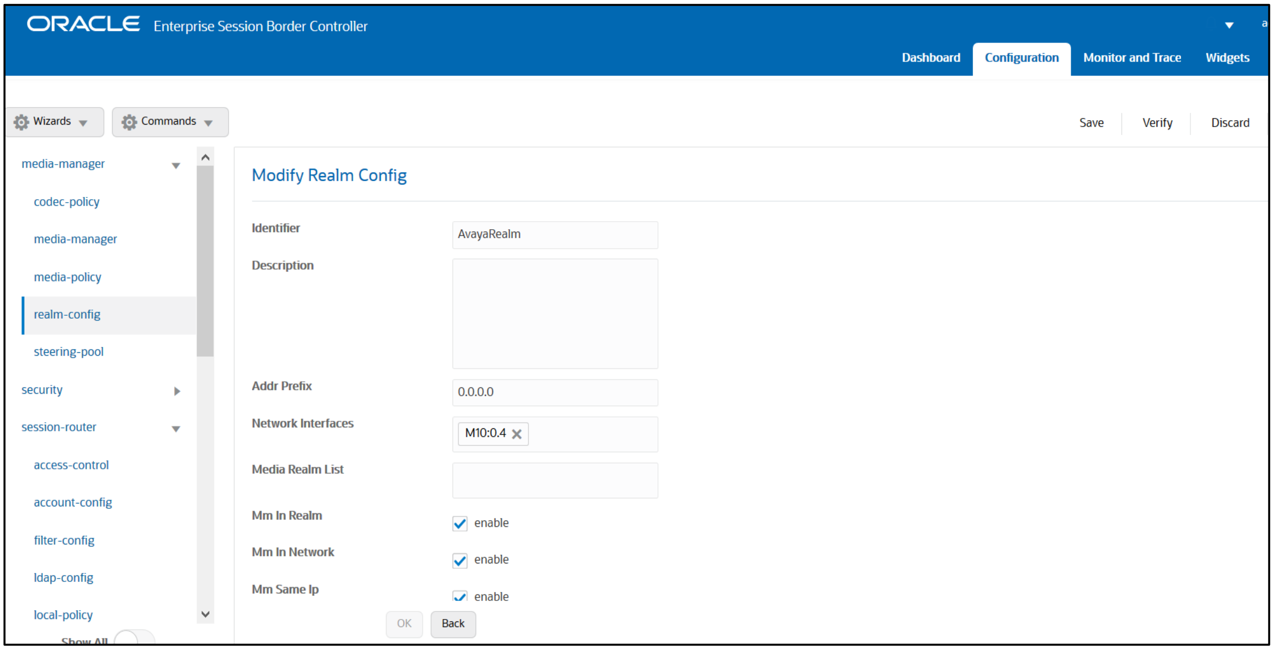
Rules Asserted Id:

Rules Redirect:

Rules Isup Cdpn:

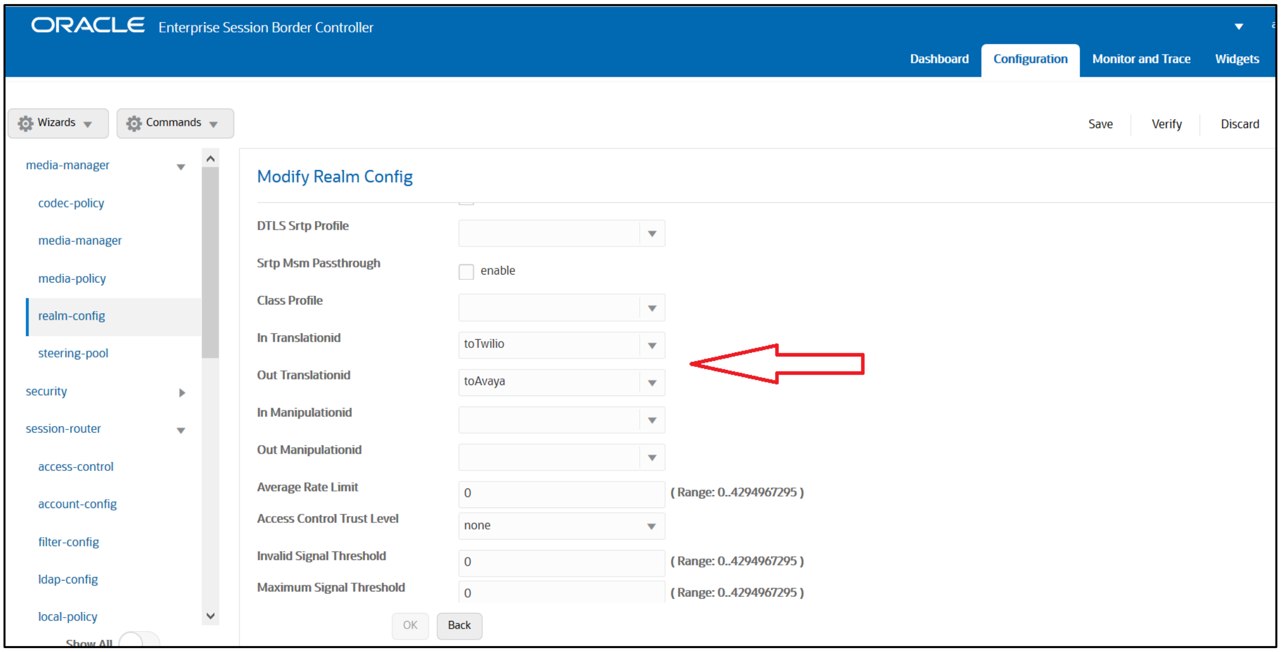
Rules Isup Cgpn:

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



Modify Realm Config

Identifier	AvayaRealm
Description	
Addr Prefix	0.0.0.0
Network Interfaces	M10:0.4
Media Realm List	
Mm In Realm	☑ enable
Mm In Network	☑ enable
Mm Same Ip	☑ enable



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)

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.

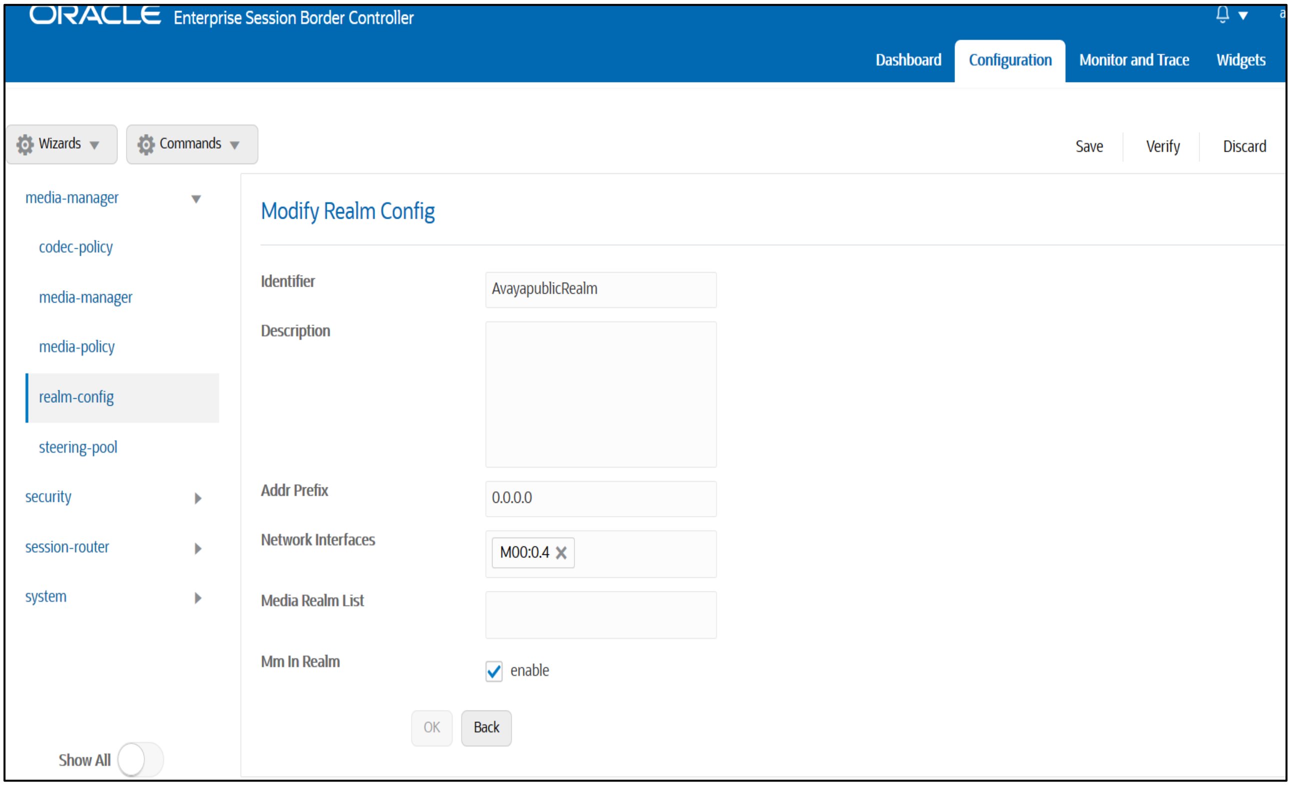
7.1. Configure Realms

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 two realms used in this configuration:

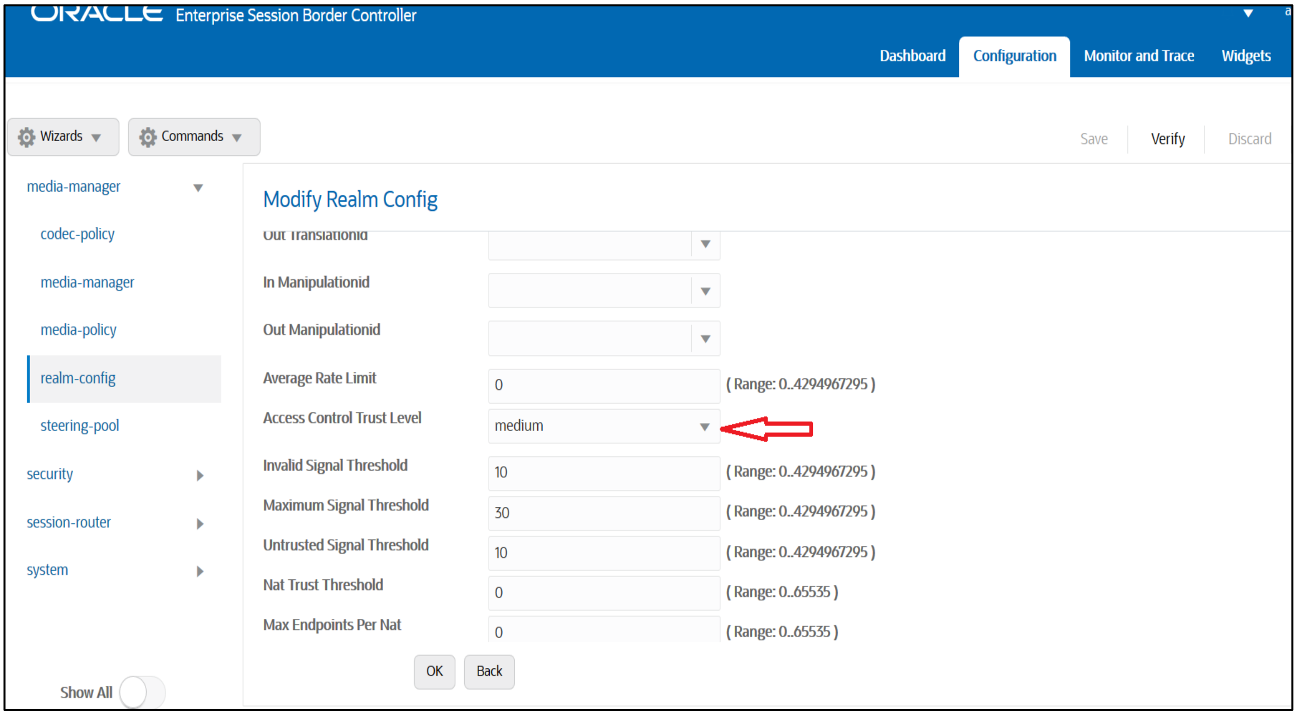
Config Parameter	AvayaAccess Side	Avaya Core Side
Identifier	AvayapublicRealm	AvayaCoreRealm
Network Interface	M00	M10
Mm in realm	☑	☑
FQDN		
Media Sec policy	sdespolicy	RTP
Access Control Trust Level	High	High
Codec-Policy	Twiliocodec	AvayaCodec

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



Modify Realm Config

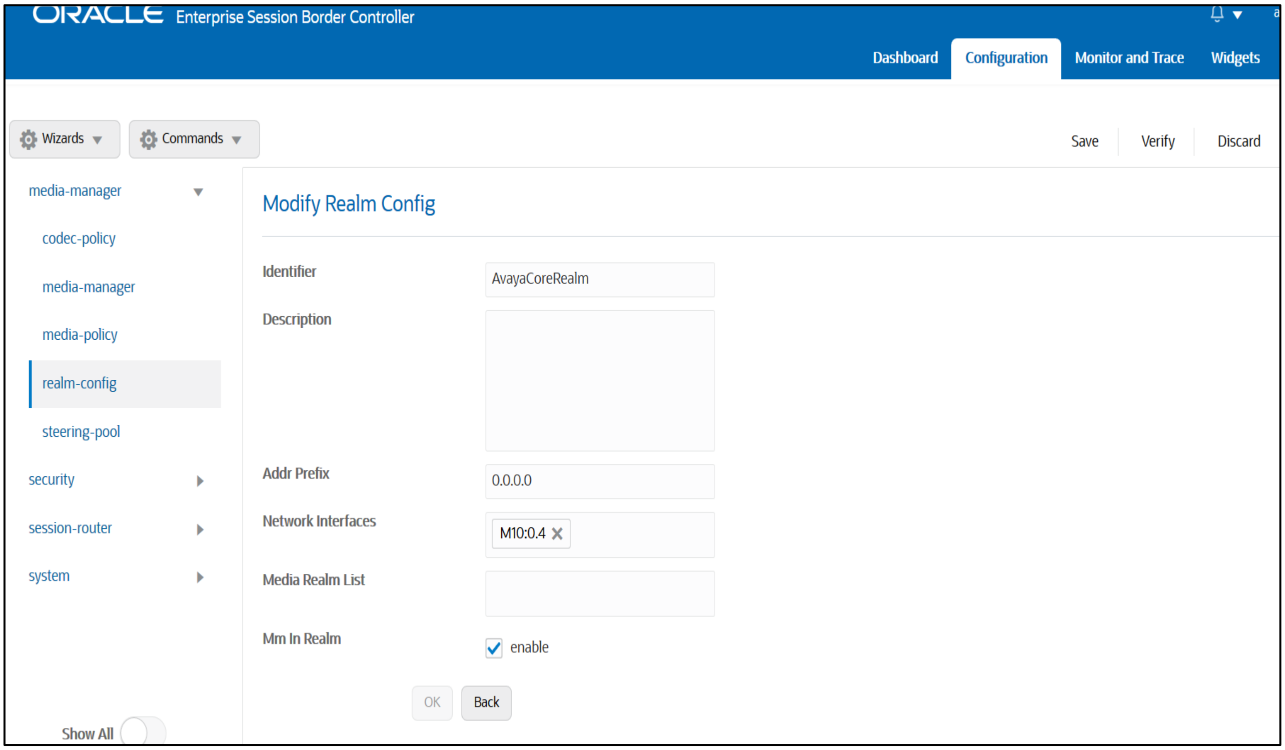
Identifier	AvayapublicRealm
Description	
Addr Prefix	0.0.0.0
Network Interfaces	M00:0.4 ✕
Media Realm List	
Mm In Realm	☑ enable



Modify Realm Config

Out Translationid		
In Manipulationid		
Out Manipulationid		
Average Rate Limit	0	(Range: 0..4294967295)
Access Control Trust Level	medium	
Invalid Signal Threshold	10	(Range: 0..4294967295)
Maximum Signal Threshold	30	(Range: 0..4294967295)
Untrusted Signal Threshold	10	(Range: 0..4294967295)
Nat Trust Threshold	0	(Range: 0..65535)
Max Endpoints Per Nat	0	(Range: 0..65535)

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



Modify Realm Config

Identifier: AvayaCoreRealm

Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M10:0.4

Media Realm List:

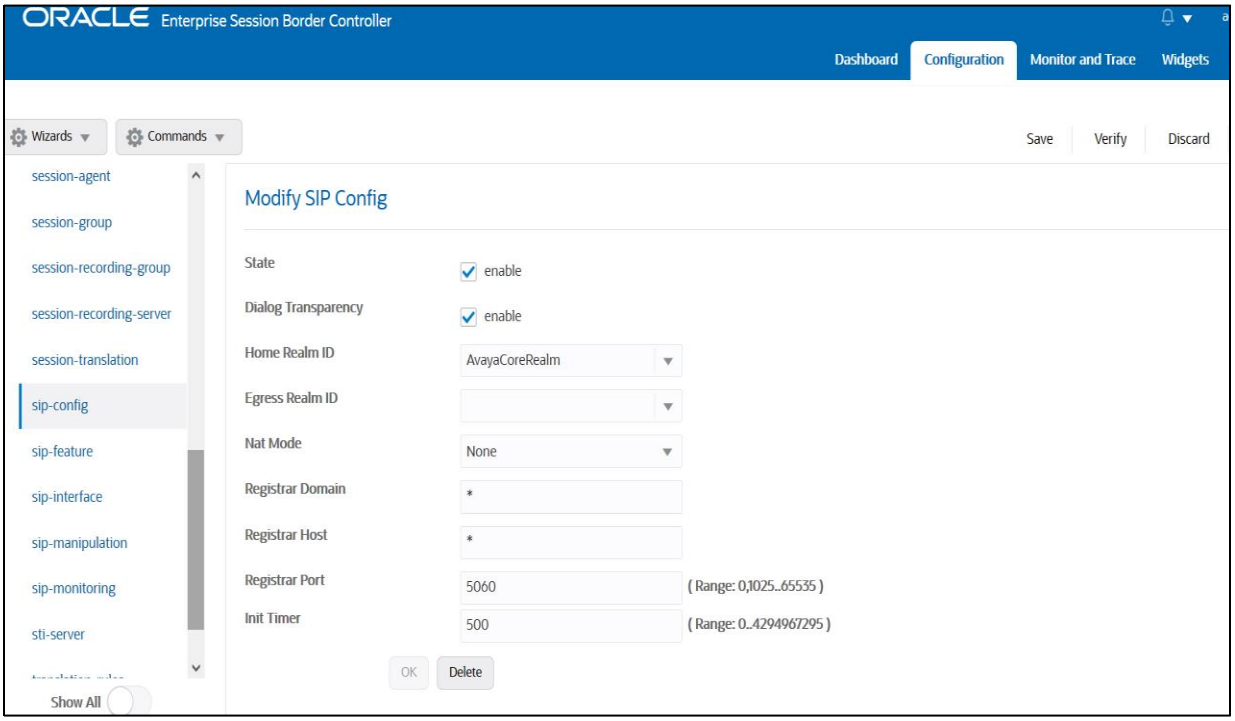
Mm In Realm: ☑ enable

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.

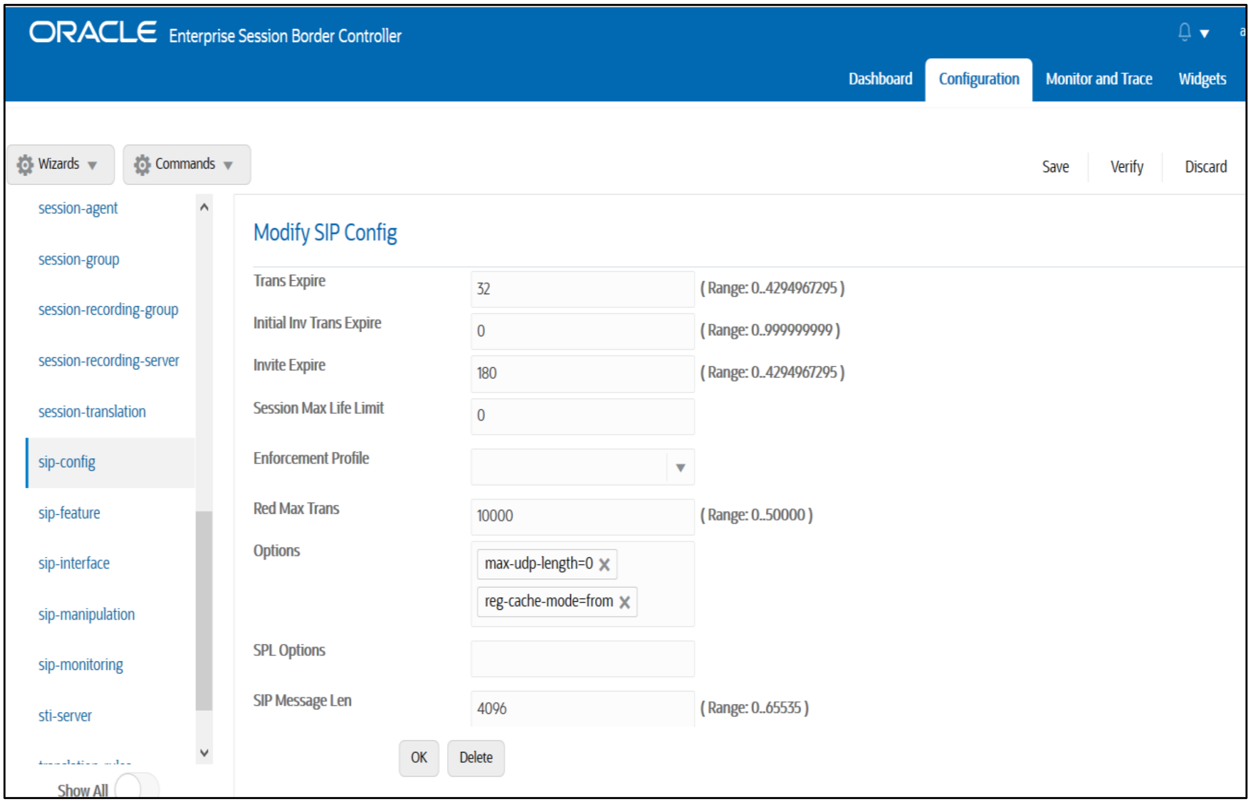
To configure sip-config, Go to Session-Router->sip-config and in options, add the below

- add max-udp-length =0
- reg-cach-mode=from



Modify SIP Config

State	☑ enable
Dialog Transparency	☑ enable
Home Realm ID	AvayaCoreRealm
Egress Realm ID	
Nat Mode	None
Registrar Domain	*
Registrar Host	*
Registrar Port	5060 (Range: 0,1025..65535)
Init Timer	500 (Range: 0..4294967295)



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)

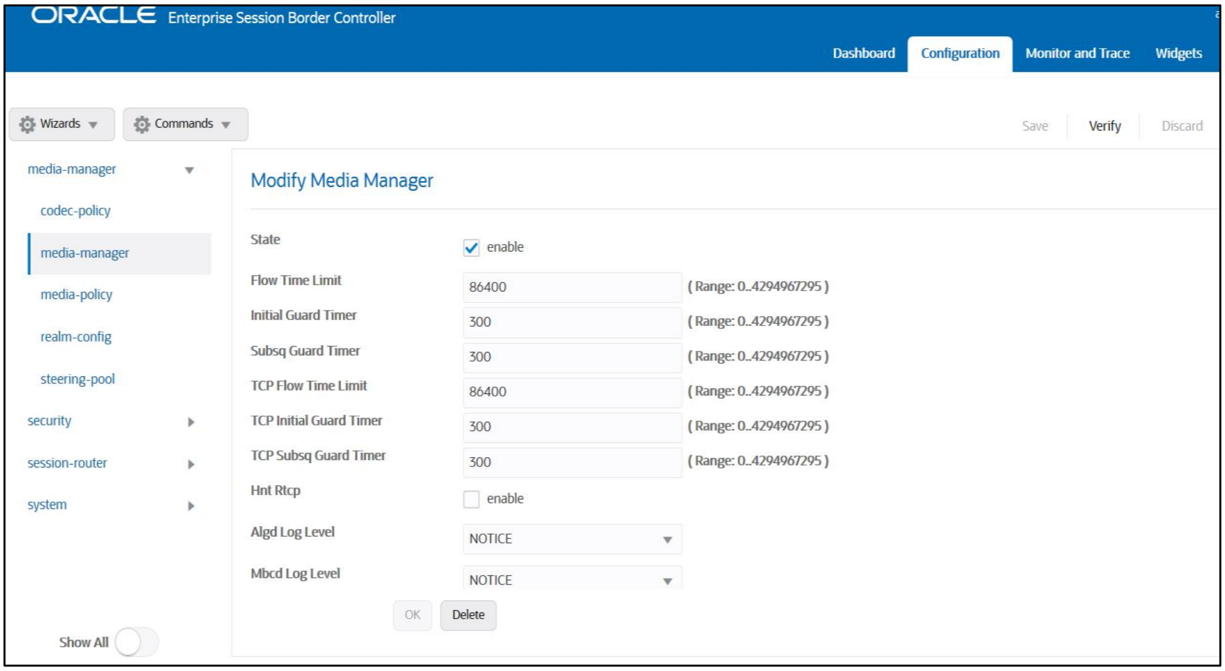
Options	max-udp-length=0 ✕
	reg-cache-mode=from ✕

SPL Options	
SIP Message Len	4096 (Range: 0..65535)

7.3. Enable media manager

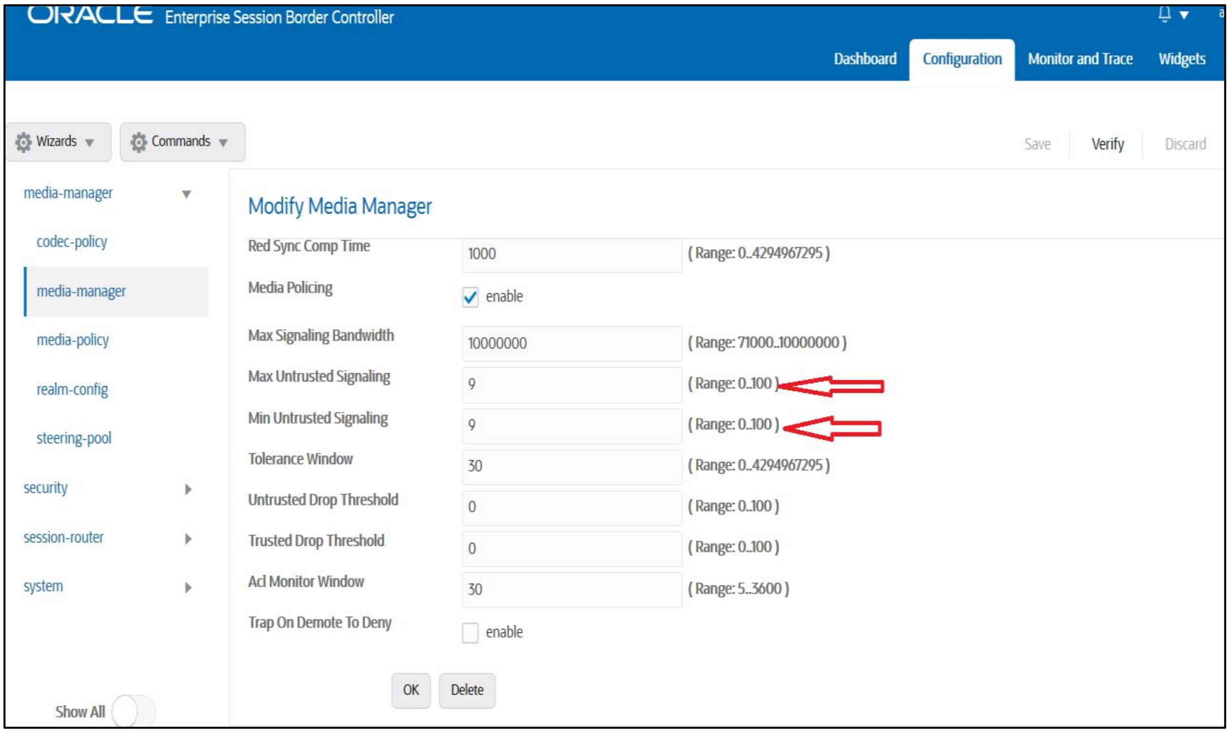
Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

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



Modify Media Manager

State	☑ 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	□ enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	



Modify Media Manager

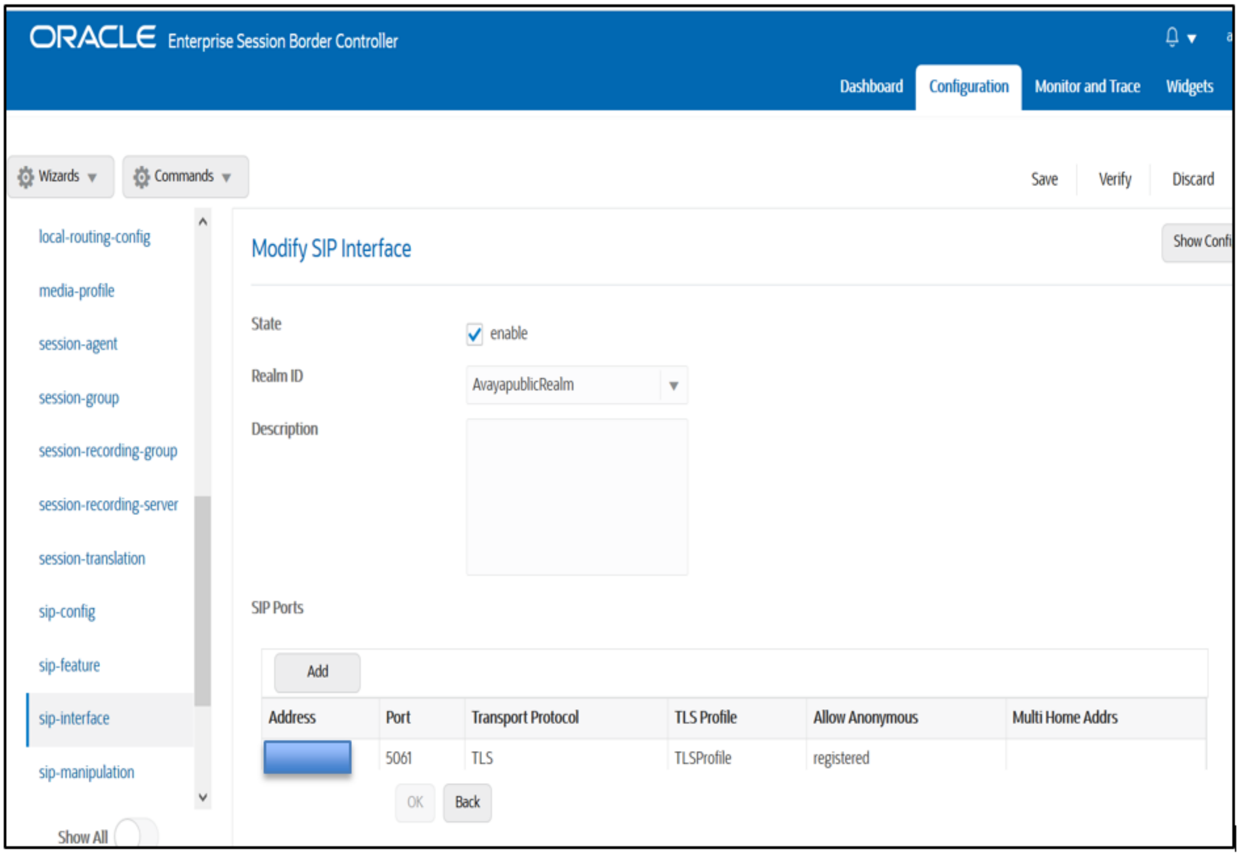
Red Sync Comp Time	1000	(Range: 0..4294967295)
Media Policing	☑ enable	
Max Signaling Bandwidth	10000000	(Range: 71000..10000000)
Max Untrusted Signaling	9	(Range: 0..100)
Min Untrusted Signaling	9	(Range: 0..100)
Tolerance Window	30	(Range: 0..4294967295)
Untrusted Drop Threshold	0	(Range: 0..100)
Trusted Drop Threshold	0	(Range: 0..100)
Acl Monitor Window	30	(Range: 5..3600)
Trap On Demote To Deny	□ 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



Modify SIP Interface

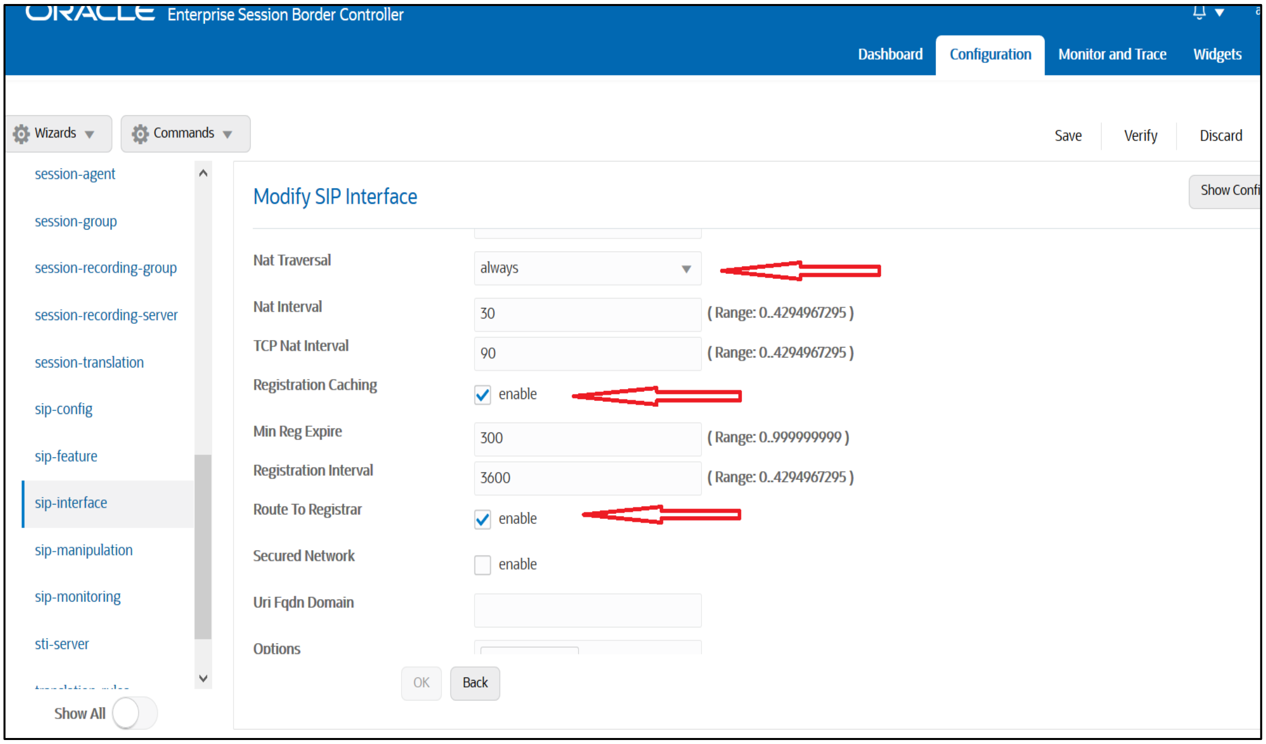
State ☑ enable

Realm ID AvayapublicRealm

Description

SIP Ports

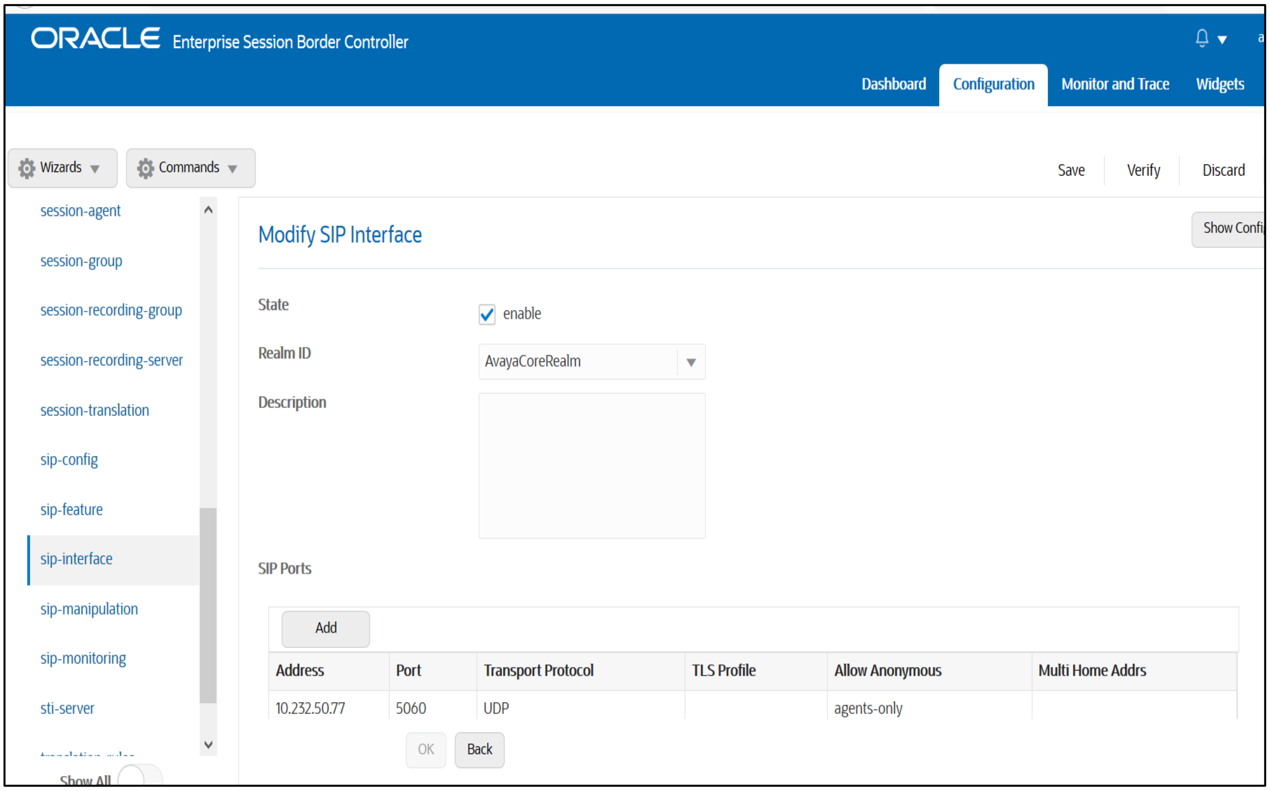
Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
[redacted]	5061	TLS	TLSProfile	registered	



Modify SIP Interface

Nat Traversal	always	
Nat Interval	30	(Range: 0..4294967295)
TCP Nat Interval	90	(Range: 0..4294967295)
Registration Caching	☑ enable	
Min Reg Expire	300	(Range: 0..999999999)
Registration Interval	3600	(Range: 0..4294967295)
Route To Registrar	☑ enable	
Secured Network	□ enable	
Uri Fqdn Domain		
Options		

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



Modify SIP Interface

State	☑ enable
Realm ID	AvayaCoreRealm
Description	

SIP Ports

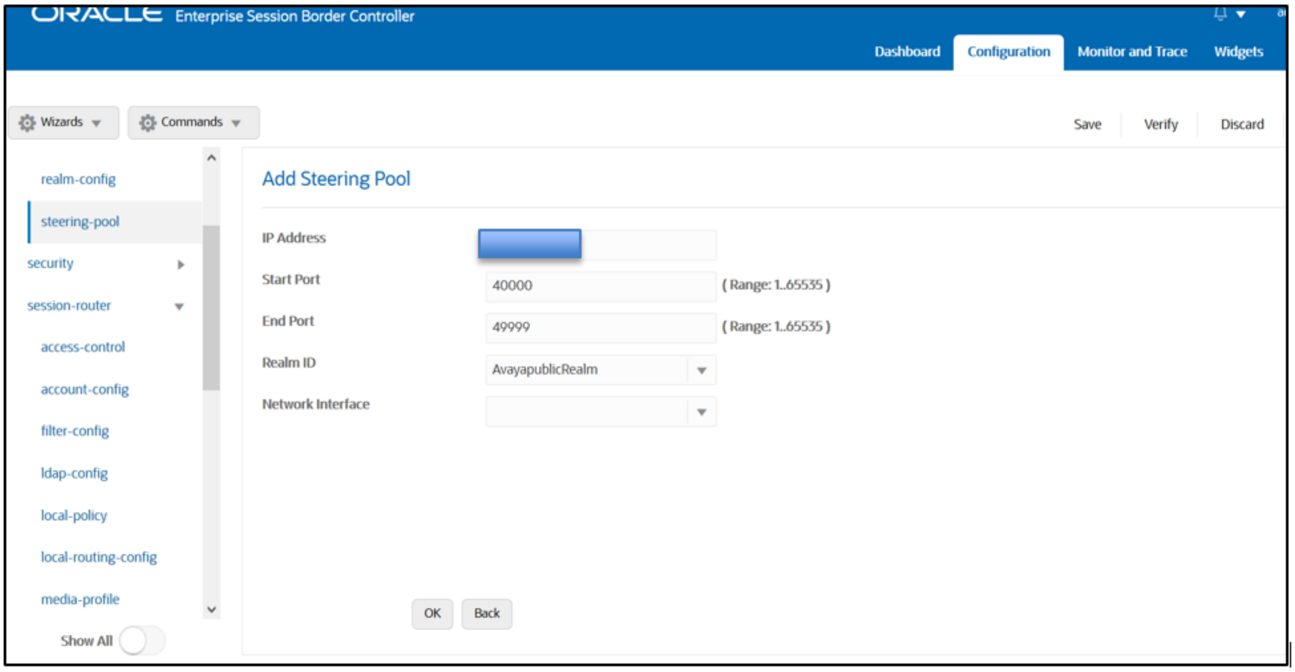
Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
10.232.50.77	5060	UDP		agents-only	

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.



Add Steering Pool

IP Address [redacted]

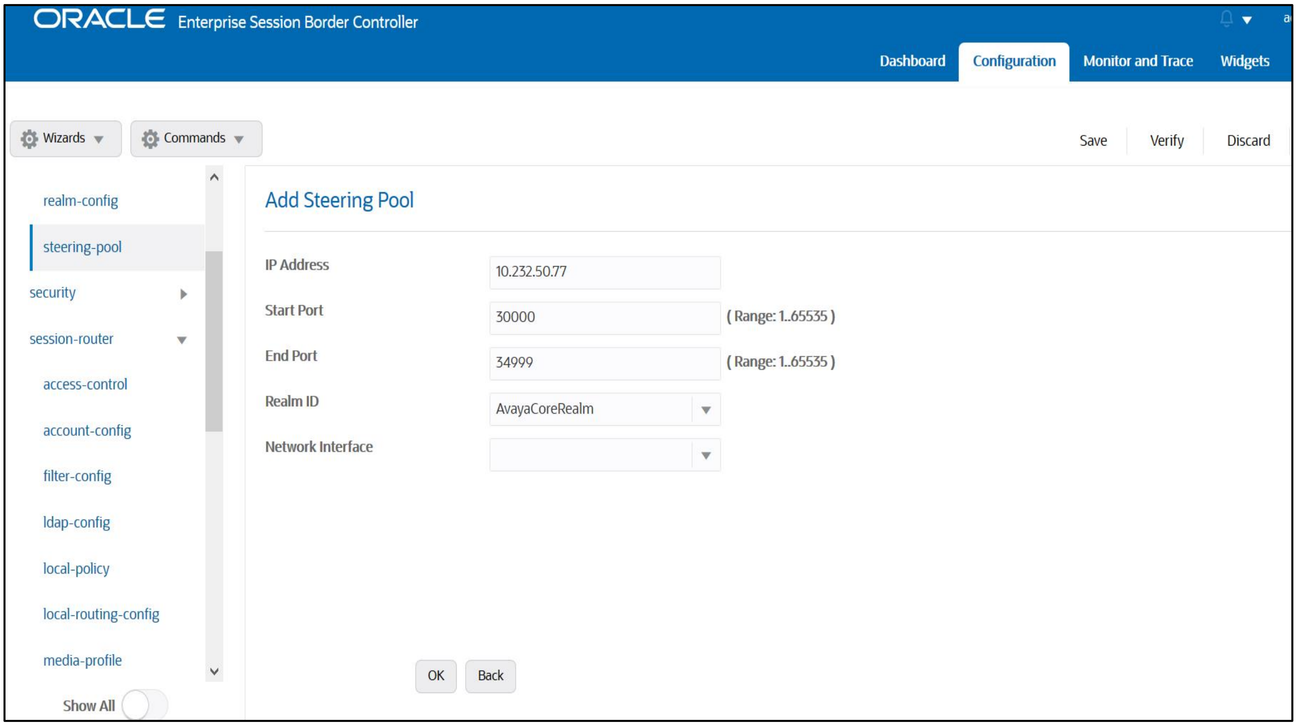
Start Port 40000 (Range: 1..65535)

End Port 49999 (Range: 1..65535)

Realm ID AvayapublicRealm

Network Interface

Avaya Core side steering pool.



Add Steering Pool

IP Address 10.232.50.77

Start Port 30000 (Range: 1..65535)

End Port 34999 (Range: 1..65535)

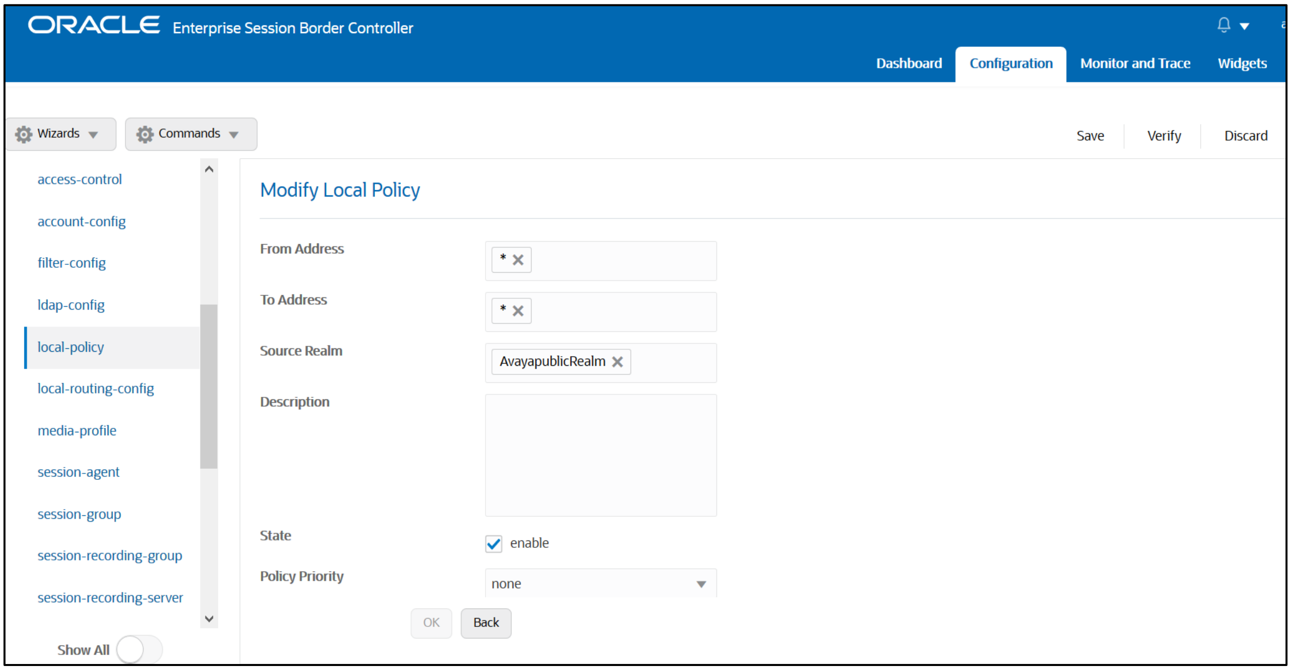
Realm ID AvayaCoreRealm

Network Interface

7.6. Configure local-policy (Optional)

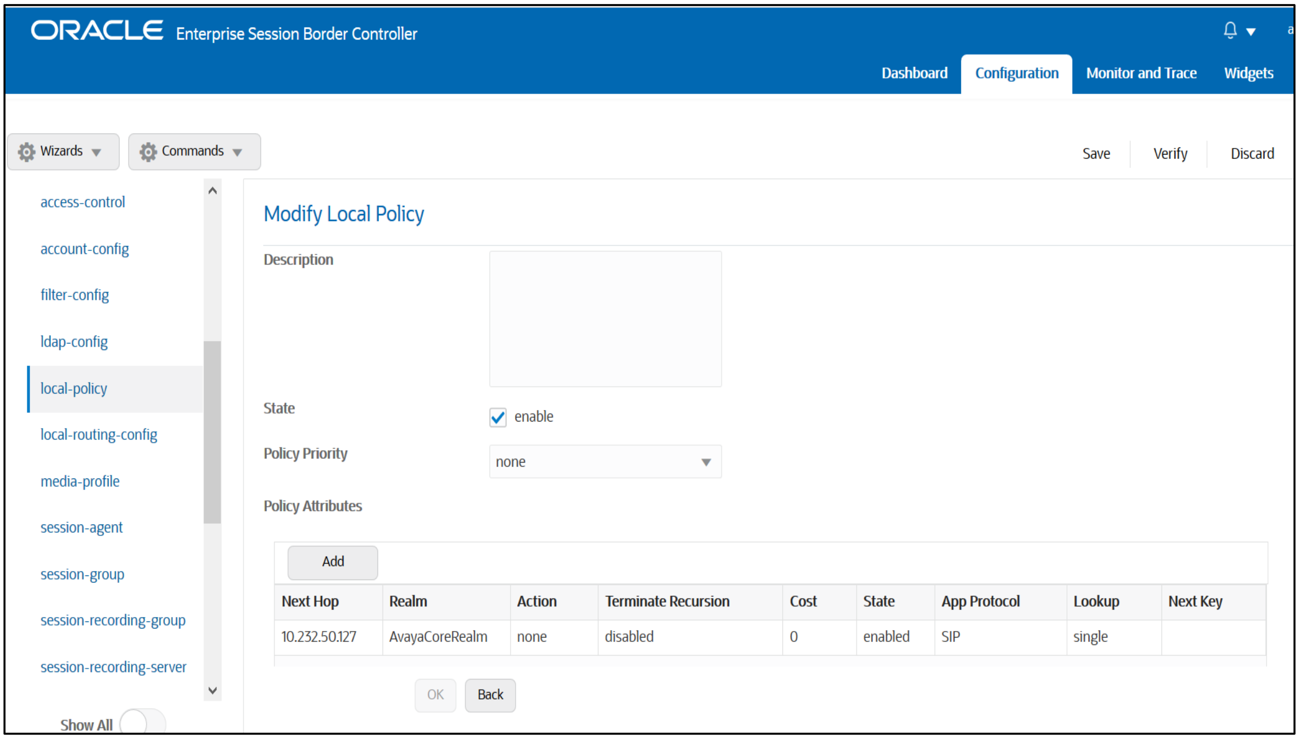
Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

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



Modify Local Policy

From Address	*
To Address	*
Source Realm	AvayapublicRealm
Description	
State	☑ enable
Policy Priority	none



Modify Local Policy

Description	
State	☑ enable
Policy Priority	none

Policy Attributes

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

8. New SBC config/Deployment Using Configuration Assistant

When you first log on to the E-SBC, the system requires you to set the configuration parameters necessary for basic operation. To help you set the initial configuration with minimal effort, the E-SBC provides the Configuration Assistant. The Configuration Assistant, which you can run from the Web GUI or the Acme Command Line Interface (ACLI), asks you questions and uses your answers to set parameters for managing and securing call traffic. You can use the Configuration Assistant for the initial set up to make to the basic configuration. Please check "Configuration Assistant Operations" in the Web GUI User Guide and "Configuration Assistant Workflow and Checklist" in the ACLI Configuration Guide

Please note, applying a configuration to the SBC via the Configuration Assistant will overwrite any existing configuration currently applied to the SBC. **We highly recommend this only be used for initial setup of the SBC. This feature is not recommended to be used to make changes to existing configurations.**

8.1. Section Overview and Requirements

This section describes how to use our Configuration Assistant feature as a quick and simple way to configure the Oracle SBC for integration with Avaya Session Manager and Twilio Elastic SIP Trunking. The pre-requisite are given below.

- SBC running release SCZ840p7 or later which will have this template package by default added to the SBC code.
- TLS certificate for the SBC preferably in PKCS format, or CSR is generated by the SBC. For Twilio side, list of supported CA's can be found here

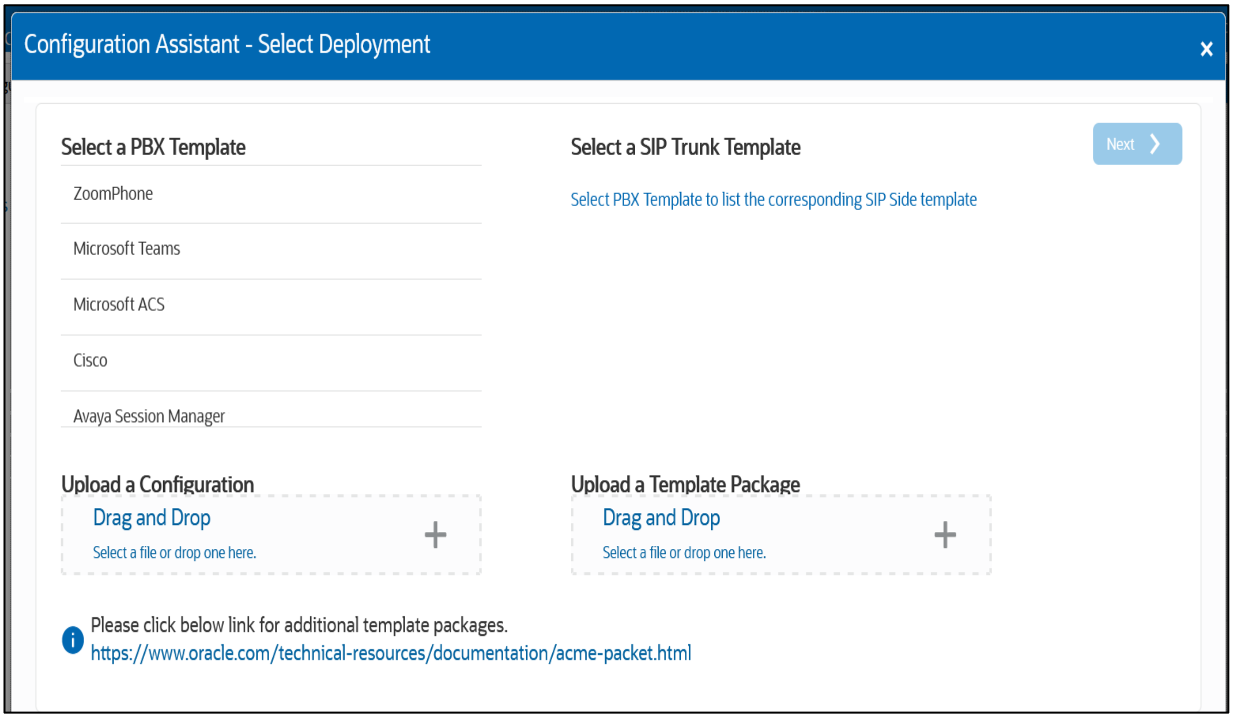
The following outline assumes you have established initial access to the SBC via console and completed the following steps:

- Configured boot parameters for management access
- Setup Product
- Set Entitlements
- Configured HTTP-Server to establish access to SBC GUI

8.2. Initial GUI Access

The Oracle SBC WebGui can be accessed by entering the following in your web browser: http(s)://<SBC Management IP>.

The username and password are the same as that of the CLI.
If there is no configuration on the SBC, the configuration assistant will show immediately upon login to the SBC GUI as shown below



Configuration Assistant - Select Deployment

Select a PBX Template

- ZoomPhone
- Microsoft Teams
- Microsoft ACS
- Cisco
- Avaya Session Manager

Select a SIP Trunk Template

Select PBX Template to list the corresponding SIP Side template

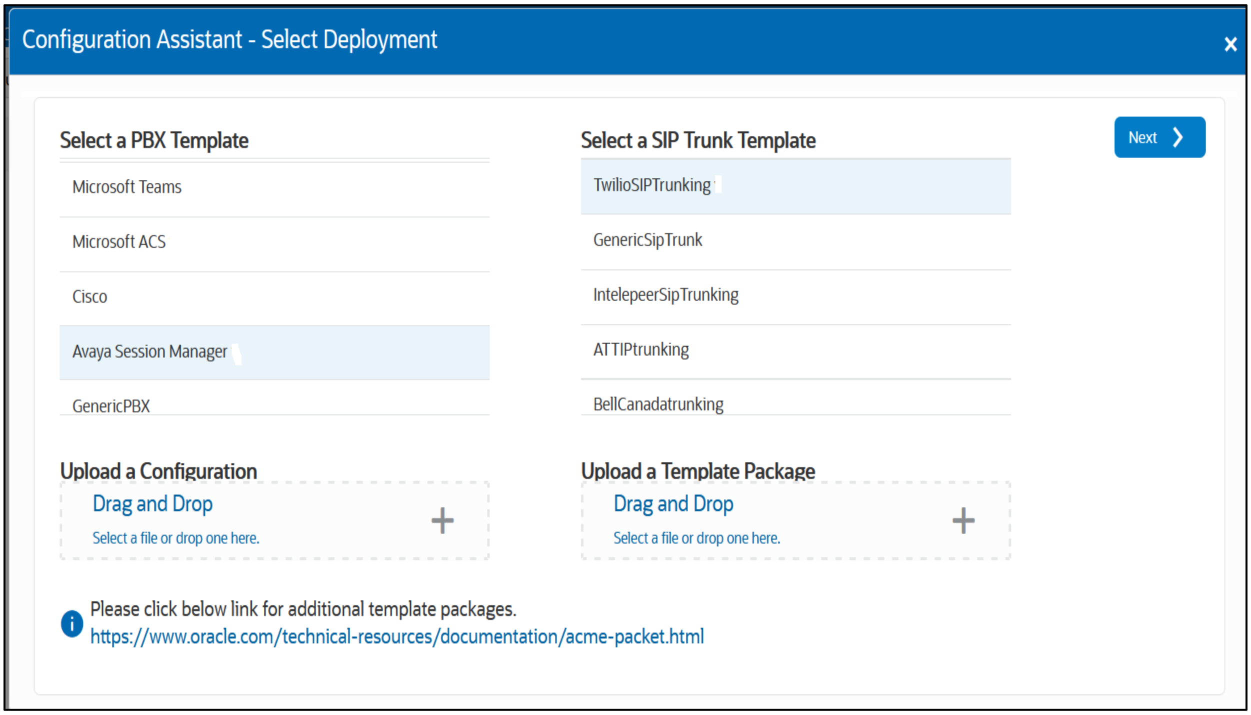
Upload a Configuration

Upload a Template Package

Please click below link for additional template packages.
https://www.oracle.com/technical-resources/documentation/acme-packet.html

×
Next
Drag and Drop
Select a file or drop one here.
Drag and Drop
Select a file or drop one here.

As we can see, there are some templates of PBX populated in the template and we can select the PBX template that we want to use with our Twilio trunk and for this document, we have selected Avaya Session Manager template and once we select that, it asks us to select the SIP trunk template. After we select Twilio trunk template, the Next option would be enabled.



Configuration Assistant - Select Deployment

Select a PBX Template

- Microsoft Teams
- Microsoft ACS
- Cisco
- Avaya Session Manager
- GenericPBX

Select a SIP Trunk Template

- TwilioSIPTrunking
- GenericSipTrunk
- IntelepeerSipTrunking
- ATTIPtrunking
- BellCanadatrunking

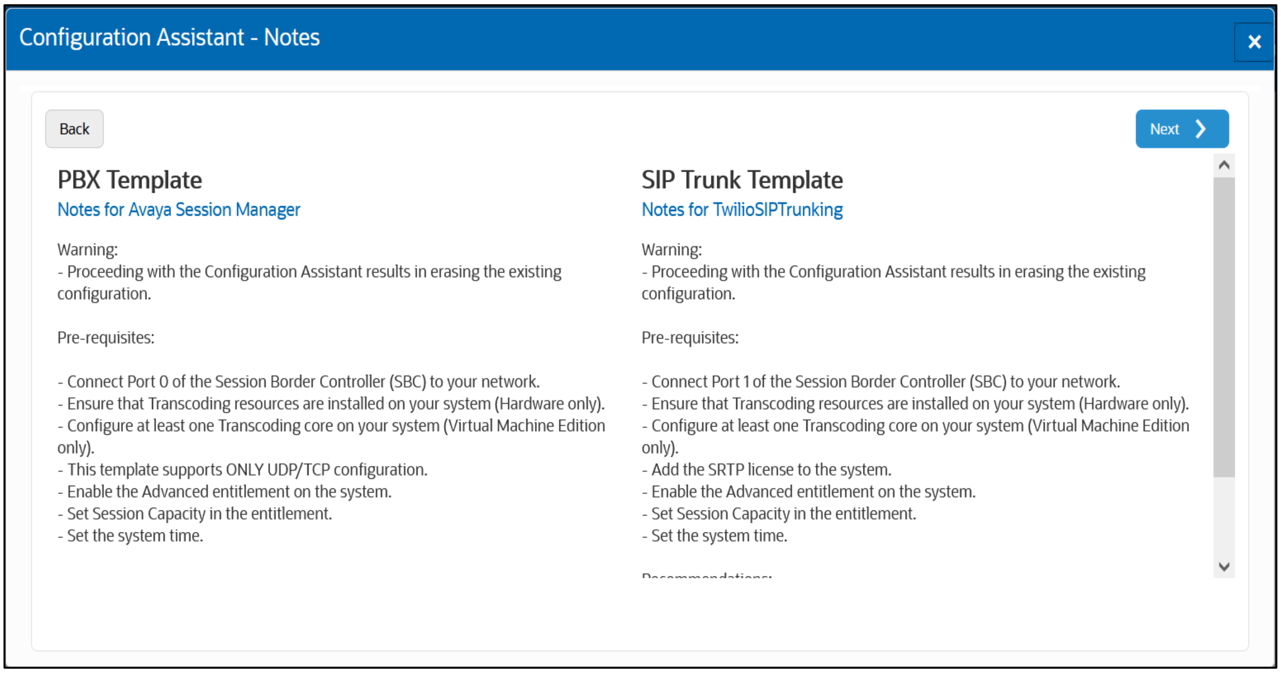
Upload a Configuration

Upload a Template Package

Please click below link for additional template packages.
https://www.oracle.com/technical-resources/documentation/acme-packet.html

×
Next
Drag and Drop
Select a file or drop one here.
Drag and Drop
Select a file or drop one here.

Click *Next*: The following “Notes” will be displayed related to pre-requisite



Configuration Assistant - Notes

PBX Template

Notes for Avaya Session Manager

Warning:
- Proceeding with the Configuration Assistant results in erasing the existing configuration.

Pre-requisites:

- Connect Port 0 of the Session Border Controller (SBC) to your network.
- Ensure that Transcoding resources are installed on your system (Hardware only).
- Configure at least one Transcoding core on your system (Virtual Machine Edition only).
- This template supports ONLY UDP/TCP configuration.
- Enable the Advanced entitlement on the system.
- Set Session Capacity in the entitlement.
- Set the system time.

SIP Trunk Template

Notes for TwilioSIPTrunking

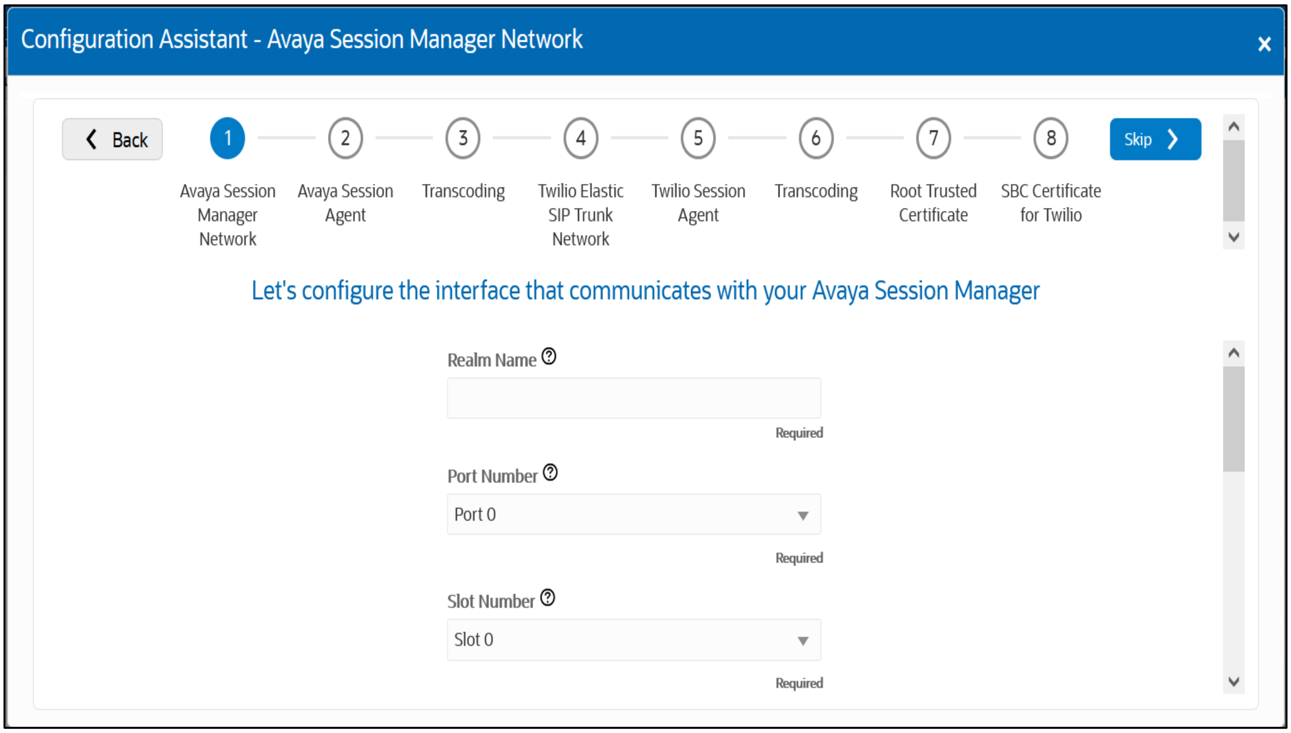
Warning:
- Proceeding with the Configuration Assistant results in erasing the existing configuration.

Pre-requisites:

- Connect Port 1 of the Session Border Controller (SBC) to your network.
- Ensure that Transcoding resources are installed on your system (Hardware only).
- Configure at least one Transcoding core on your system (Virtual Machine Edition only).
- Add the SRTP license to the system.
- Enable the Advanced entitlement on the system.
- Set Session Capacity in the entitlement.
- Set the system time.

Recommendations:

Click *Next* and we get the below screen where we need to enter the details for SBC configuration.



Configuration Assistant - Avaya Session Manager Network

×
Back
1 Avaya Session Manager Network
2 Avaya Session Agent
3 Transcoding
4 Twilio Elastic SIP Trunk Network
5 Twilio Session Agent
6 Transcoding
7 Root Trusted Certificate
8 SBC Certificate for Twilio
Skip

Let's configure the interface that communicates with your Avaya Session Manager

Realm Name

Required

Port Number: Port 0

Required

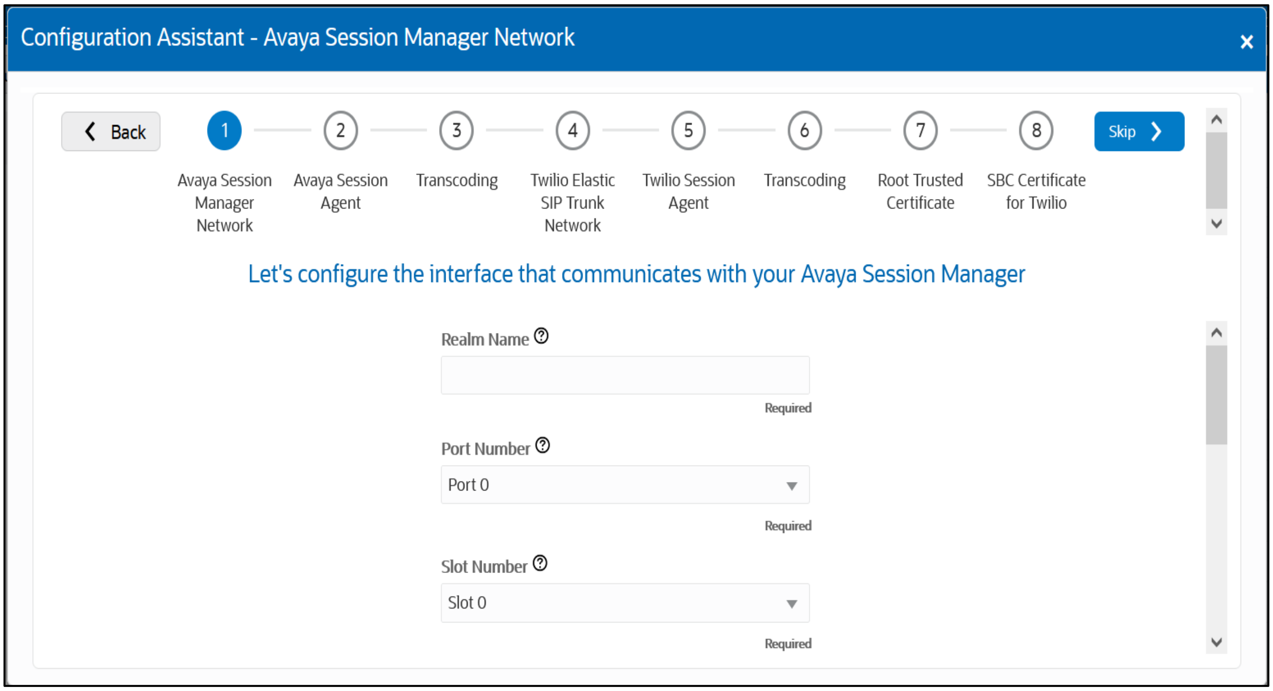
Slot Number: Slot 0

Required

8.3. Configuration Assistant Template Navigation

8.3.1. Page 1-Avaya Session manager Network

Page 1 of the template is where you will configure the network information to connect Avaya Session Manager.



Configuration Assistant - Avaya Session Manager Network

×
Back
1 Avaya Session Manager Network
2 Avaya Session Agent
3 Transcoding
4 Twilio Elastic SIP Trunk Network
5 Twilio Session Agent
6 Transcoding
7 Root Trusted Certificate
8 SBC Certificate for Twilio
Skip

Let's configure the interface that communicates with your Avaya Session Manager

Realm Name ⓘ

Required

Port Number ⓘ

Port 0

Required

Slot Number ⓘ

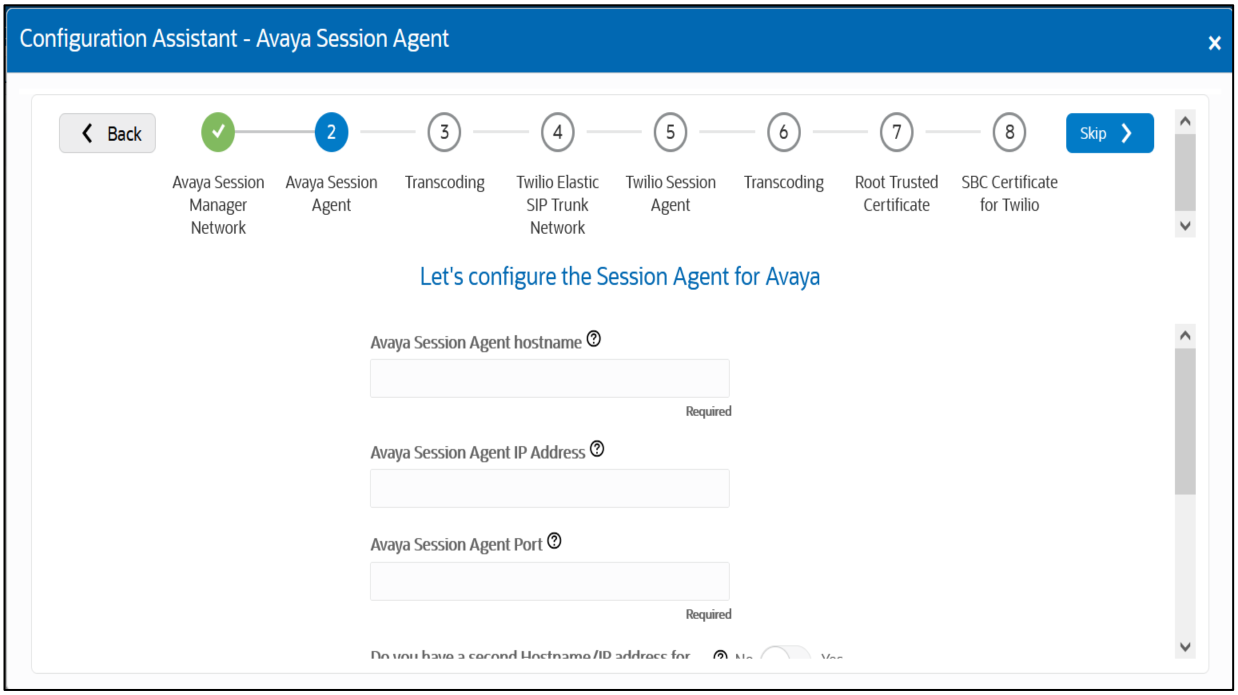
Slot 0

Required

Next to each field is a help icon. If you hover over the icon, you will be provided with a description or definition of each filed. Also, pay close attention to which fields are listed as “required”.

8.3.2. Page 2-Avaya Session agent

Page 2 of the template is where you will configure the Avaya Session Agent details where you will enter the next hop IP address and port for sip signaling to and from your Avaya Session Agent. Please fill the required fields and click Next.



Configuration Assistant - Avaya Session Agent

×
Back
✓ Avaya Session Manager Network
2 Avaya Session Agent
3 Transcoding
4 Twilio Elastic SIP Trunk Network
5 Twilio Session Agent
6 Transcoding
7 Root Trusted Certificate
8 SBC Certificate for Twilio
Skip

Let's configure the Session Agent for Avaya

Avaya Session Agent hostname

Required

Avaya Session Agent IP Address

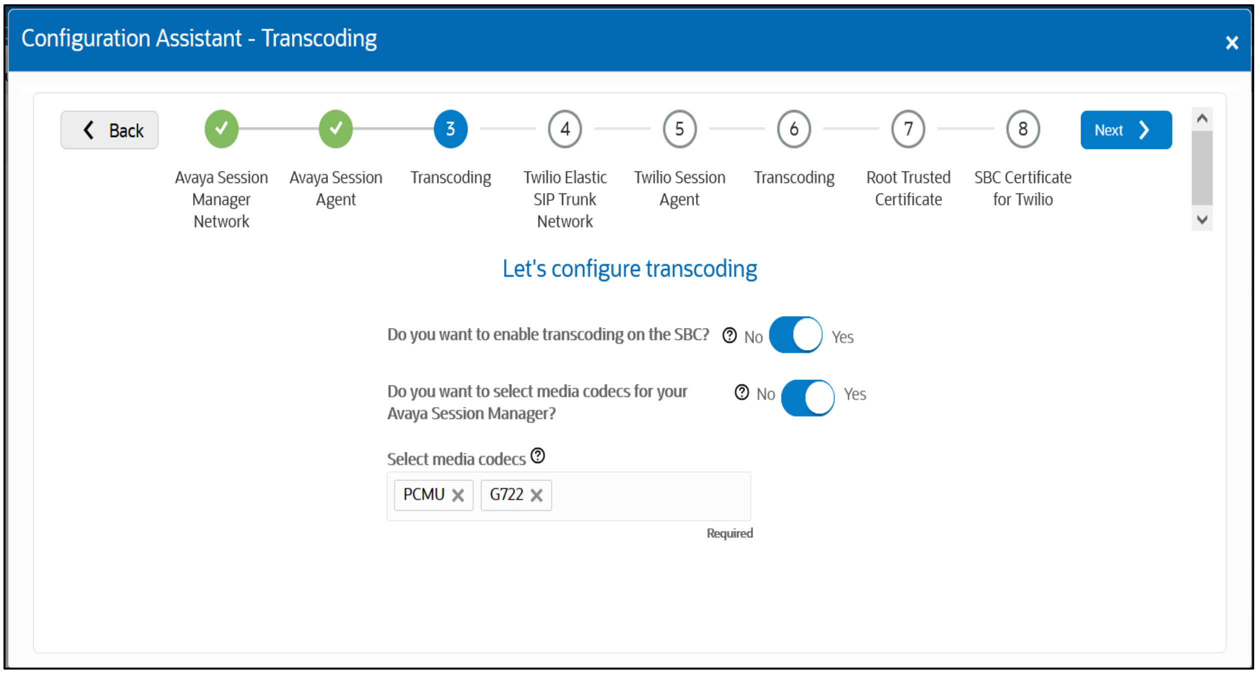
Avaya Session Agent Port

Required

Do you have a second Hostname/IP address for ... No Yes

8.3.3. Page 3 - Avaya side Transcoding

Page 3 is where you will be able to configure transcoding between the SBC and Avaya Session Manager. Once transcoding features is set to “yes”, you will then have an option to select additional media codecs you want included in offers/answers towards Avaya Session Manager. If you select yes to either question regarding media codecs, you will be presented with a required drop down. You can select as many codecs from the list presented.



Configuration Assistant - Transcoding

×
Back
✓ Avaya Session Manager Network
✓ Avaya Session Agent
3 Transcoding
4 Twilio Elastic SIP Trunk Network
5 Twilio Session Agent
6 Transcoding
7 Root Trusted Certificate
8 SBC Certificate for Twilio
Next

Let's configure transcoding

Do you want to enable transcoding on the SBC? No [✓ Yes]

Do you want to select media codecs for your Avaya Session Manager? No [✓ Yes]

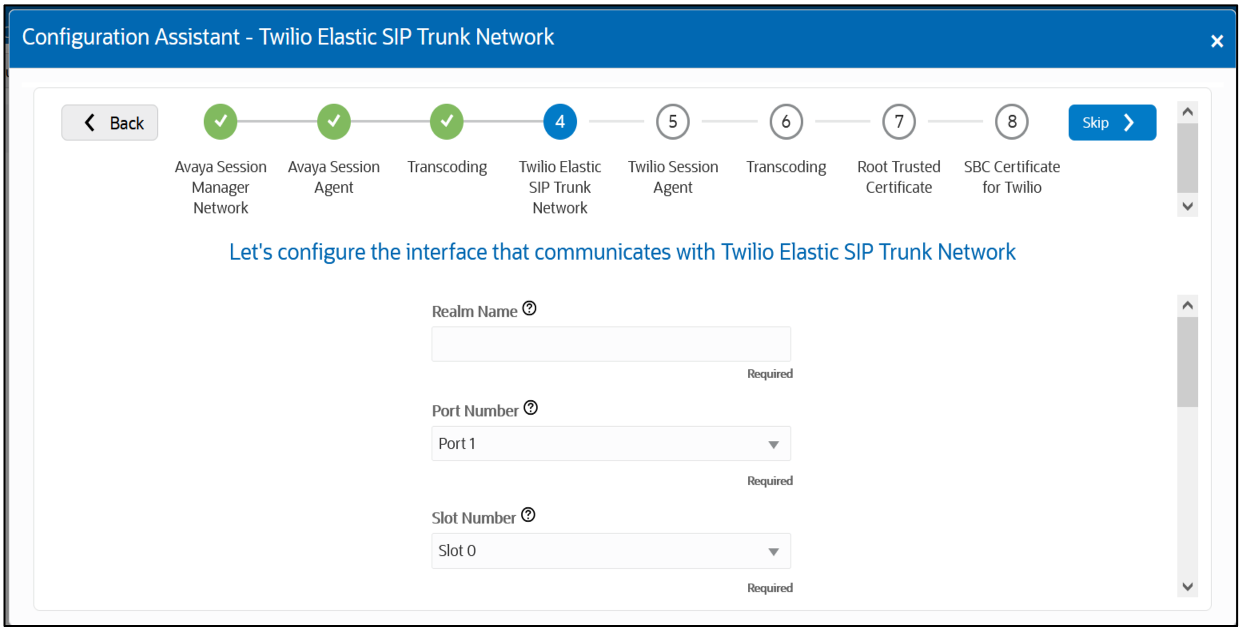
Select media codecs

PCMU ✕ G722 ✕

Required

8.3.4. Page 4 - Twilio Elastic SIP Trunk Network

Page 4 of the template is where you will configure the network information to connect to Twilio Elastic SIP trunk Network. Please fill the required fields and Press Next.



Configuration Assistant - Twilio Elastic SIP Trunk Network

×
Back
✓ Avaya Session Manager Network
✓ Avaya Session Agent
✓ Transcoding
4 Twilio Elastic SIP Trunk Network
5 Twilio Session Agent
6 Transcoding
7 Root Trusted Certificate
8 SBC Certificate for Twilio
Skip

Let's configure the interface that communicates with Twilio Elastic SIP Trunk Network

Realm Name ⓘ

Required

Port Number ⓘ

Port 1

Required

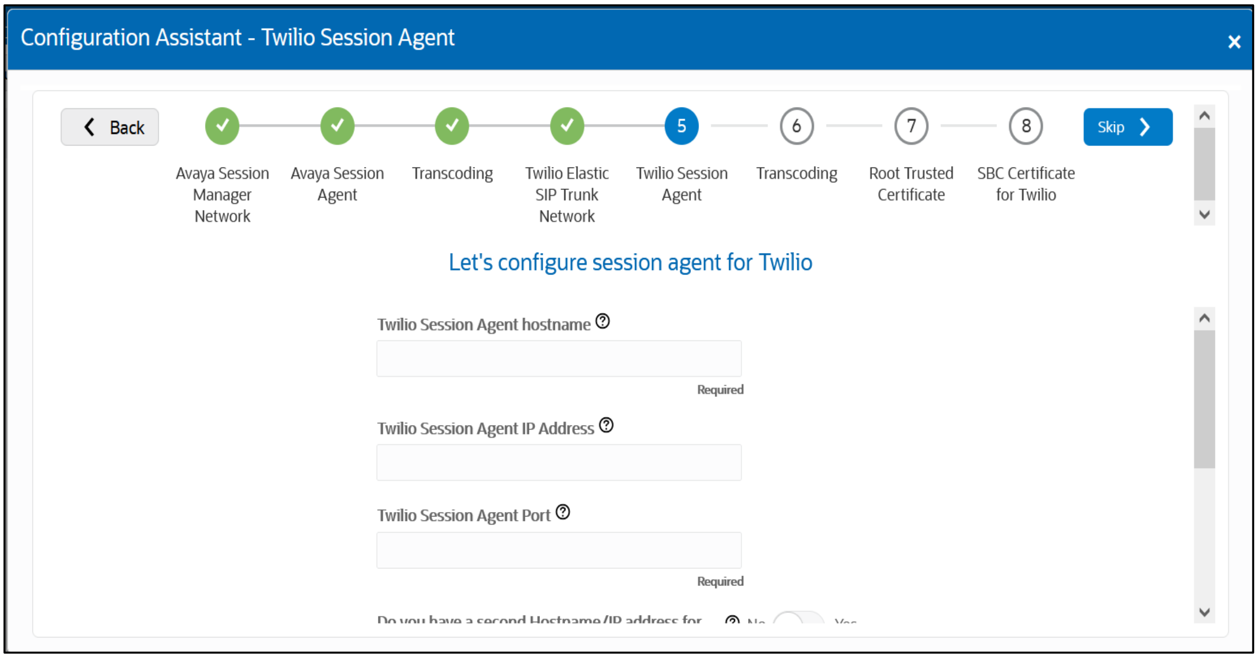
Slot Number ⓘ

Slot 0

Required

8.3.5. Page 5 - Twilio Session Agent

Page 5 of the template is where you will configure the Twilio Session Agent details where you will enter the next hop IP address and port for sip signaling to and from your Twilio Elastic SIP trunk. Please fill the required fields and click Next.



Configuration Assistant - Twilio Session Agent

×
Back
✓ Avaya Session Manager Network
✓ Avaya Session Agent
✓ Transcoding
✓ Twilio Elastic SIP Trunk Network
5 Twilio Session Agent
6 Transcoding
7 Root Trusted Certificate
8 SBC Certificate for Twilio
Skip

Let's configure session agent for Twilio

Twilio Session Agent hostname ⓘ

Required

Twilio Session Agent IP Address ⓘ

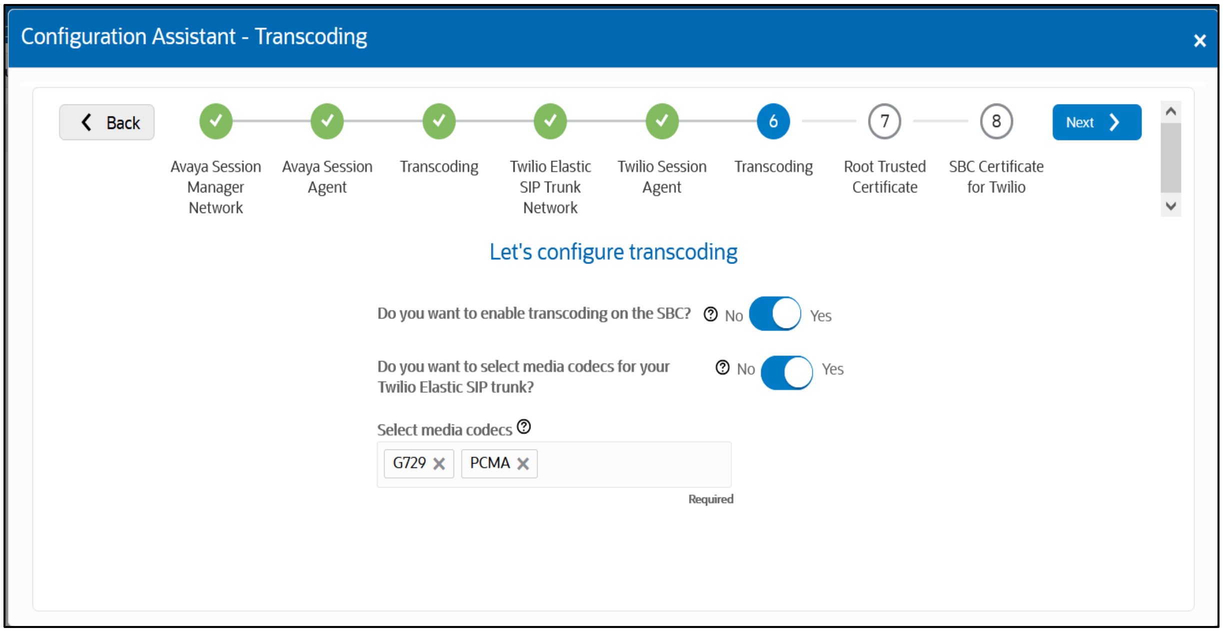
Twilio Session Agent Port ⓘ

Required

Do you have a second Hostname/IP address for ⓘ No Yes

8.3.6. Page 6 - Twilio side Transcoding

Page 6 is where you will be able to configure transcoding between the SBC and Twilio Trunk. Once transcoding features is set to “yes”, you will then have an option to select additional media codecs you want included in offers/answers toward Twilio trunk. If you select yes to either question regarding media codecs, you will be presented with a required drop down. You can select as many codecs from the list presented.



Configuration Assistant - Transcoding

Let's configure transcoding

Do you want to enable transcoding on the SBC? No [✓ Yes]

Do you want to select media codecs for your Twilio Elastic SIP trunk? No [✓ Yes]

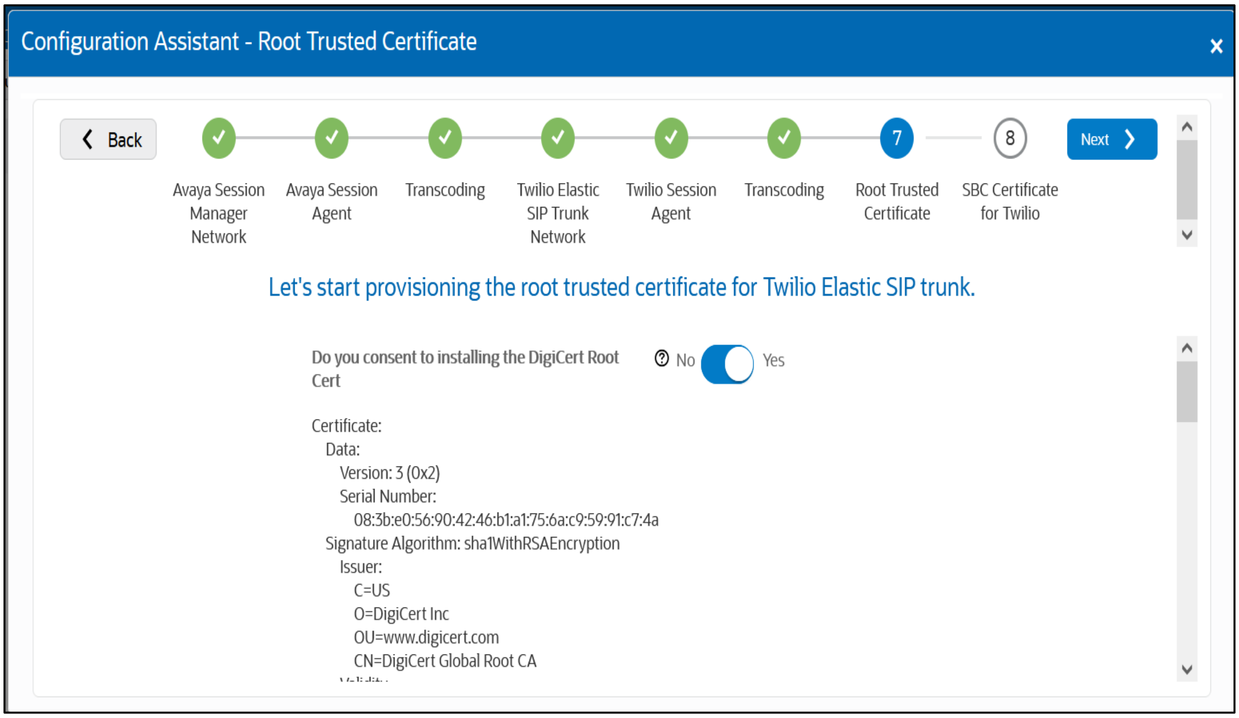
Select media codecs

G729 × PCMA ×

Required

8.3.7. Page 7 - Import Digi Cert Root CA Certificate for Twilio Side

Page 7 of this template is where the SBC will import the DigiCert Root CA certificate, which Twilio uses to sign the certs it presents to the SBC during the TLS handshake. Importing the DigiCert Root CA certs is enabled by default.


Configuration Assistant - Root Trusted Certificate
×
Back
Avaya Session Manager Network
Avaya Session Agent
Transcoding
Twilio Elastic SIP Trunk Network
Twilio Session Agent
Transcoding
7
Root Trusted Certificate
8
SBC Certificate for Twilio
Next

Let's start provisioning the root trusted certificate for Twilio Elastic SIP trunk.

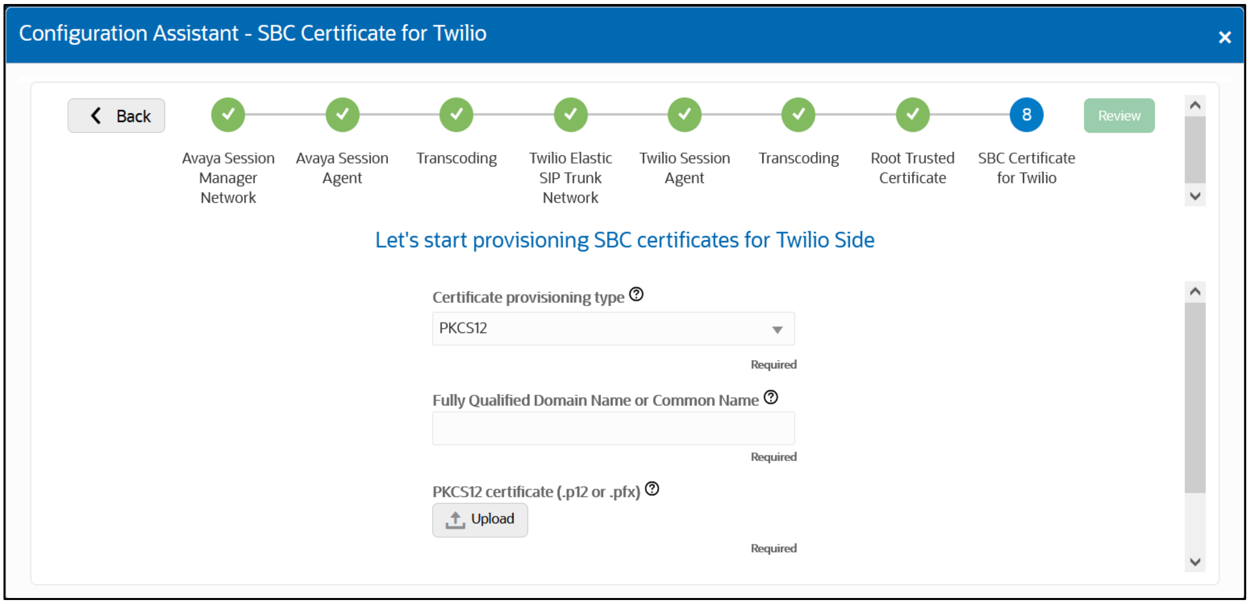
Do you consent to installing the DigiCert Root Cert ⓘ No ● Yes

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      08:3b:e0:56:90:42:46:b1:a1:75:6a:c9:59:91:c7:4a
  Signature Algorithm: sha1WithRSAEncryption
    Issuer:
      C=US
      O=DigiCert Inc
      OU=www.digicert.com
      CN=DigiCert Global Root CA
```

8.3.8. Page 8 - SBC Certificates for Twilio side

PKCS12 Import

By default, the SBC is set to import a certificate in PKCS 12 format. This is the simplest and recommended way to add a certificate to the Oracle SBC. Using this method, you will add the SBC's hostname under "FQDN or Common Name" field, upload a certificate from a supported CA, and enter the certificates password.


Configuration Assistant - SBC Certificate for Twilio
×
Back
Avaya Session Manager Network
Avaya Session Agent
Transcoding
Twilio Elastic SIP Trunk Network
Twilio Session Agent
Transcoding
Root Trusted Certificate
8
SBC Certificate for Twilio
Review

Let's start provisioning SBC certificates for Twilio Side

Certificate provisioning type ⓘ
PKCS12
Required

Fully Qualified Domain Name or Common Name ⓘ

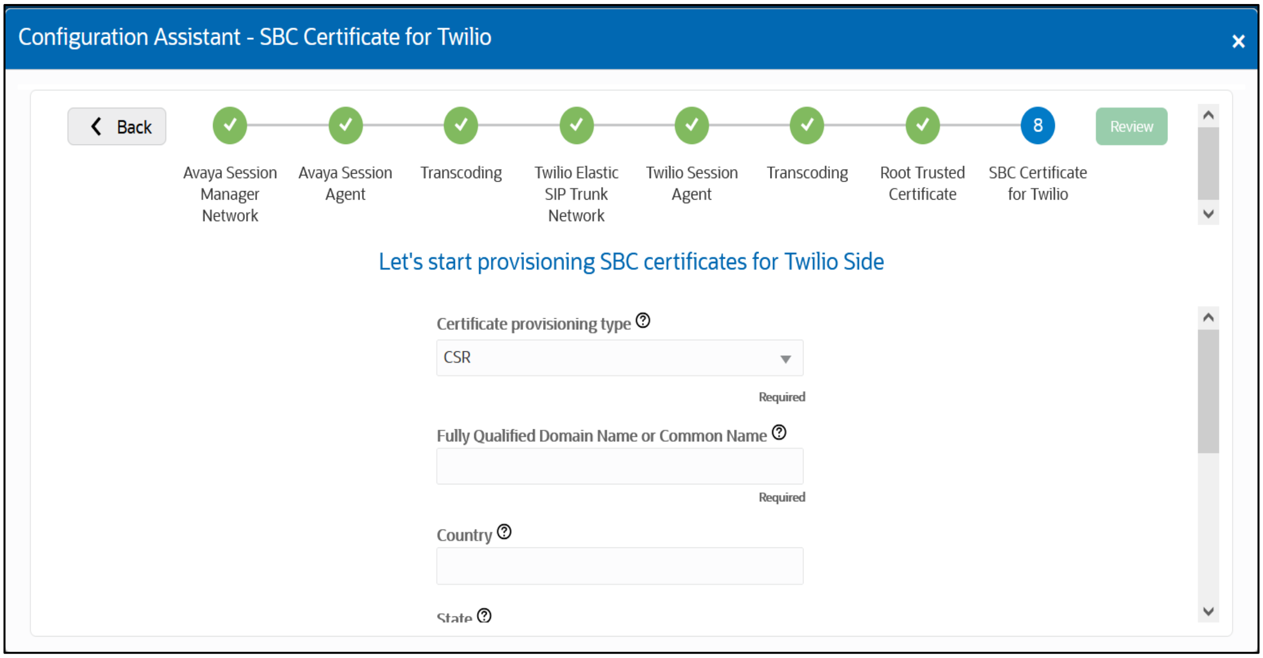
Required

PKCS12 certificate (.p12 or .pfx) ⓘ
Upload
Required

Certificate Signing Request (CSR)

The alternative to importing a PKCS12 certificate to the SBC is to configure a certificate and generate a certificate signing request that you will have signed by a supported CA

Same as PKCS12, you will enter the SBC's hostname under "FQDN or Common Name" and "Country" field (required) and answer the remaining question presented on this page (optional).



Configuration Assistant - SBC Certificate for Twilio

Let's start provisioning SBC certificates for Twilio Side

Certificate provisioning type ⓘ

CSR ▾

Required

Fully Qualified Domain Name or Common Name ⓘ

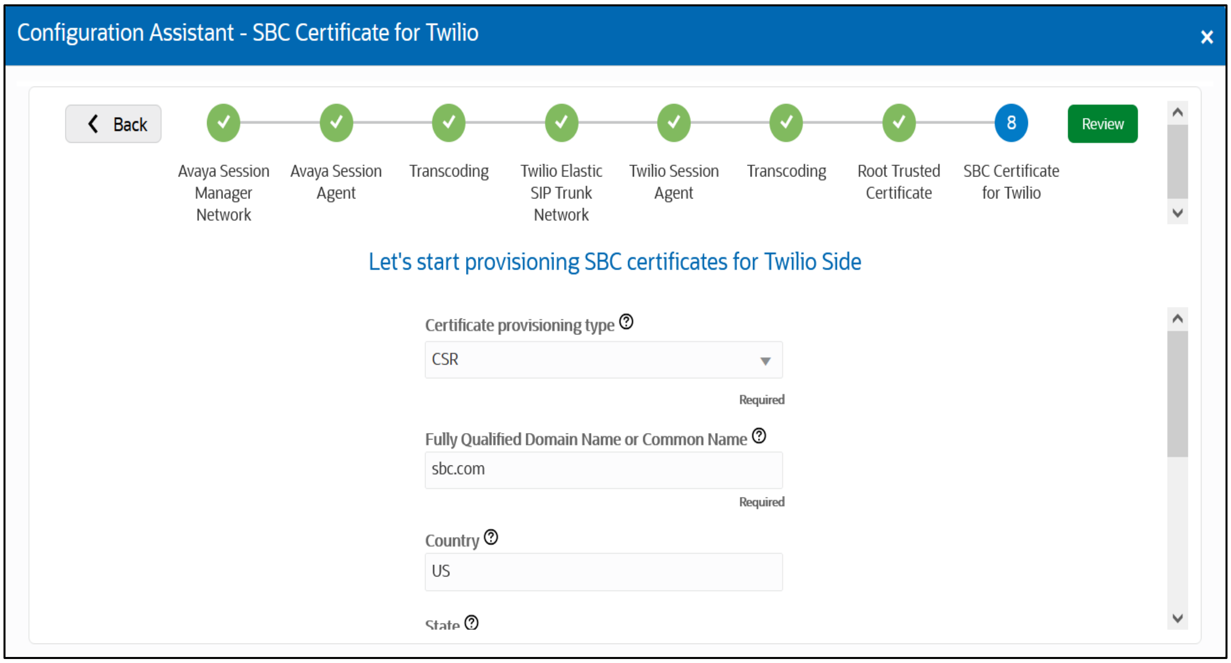
Required

Country ⓘ

State ⓘ

8.4. Review

At the end of the template, you will notice in the top right, a "*Review*" tab. If all 8 pages presented across the top are showing green, indicting there are no errors with the information entered, click on the "Review" tab.


Configuration Assistant - SBC Certificate for Twilio
×
Back
✓
Avaya Session Manager Network
✓
Avaya Session Agent
✓
Transcoding
✓
Twilio Elastic SIP Trunk Network
✓
Twilio Session Agent
✓
Transcoding
✓
Root Trusted Certificate
8
SBC Certificate for Twilio
Review

Let's start provisioning SBC certificates for Twilio Side

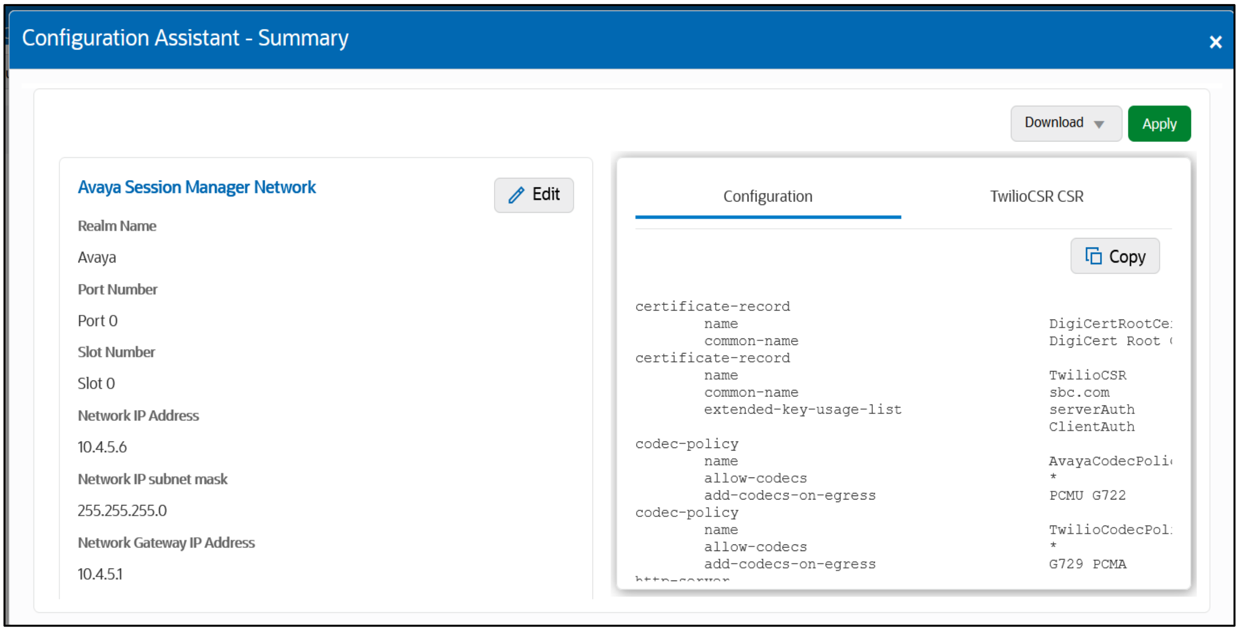
Certificate provisioning type: CSR (Required)

Fully Qualified Domain Name or Common Name: sbc.com (Required)

Country: US

State

The screen looks like below after clicking the Review Tab.



Avaya Session Manager Network

Realm Name: Avaya

Port Number: Port 0

Slot Number: Slot 0

Network IP Address: 10.4.5.6

Network IP subnet mask: 255.255.255.0

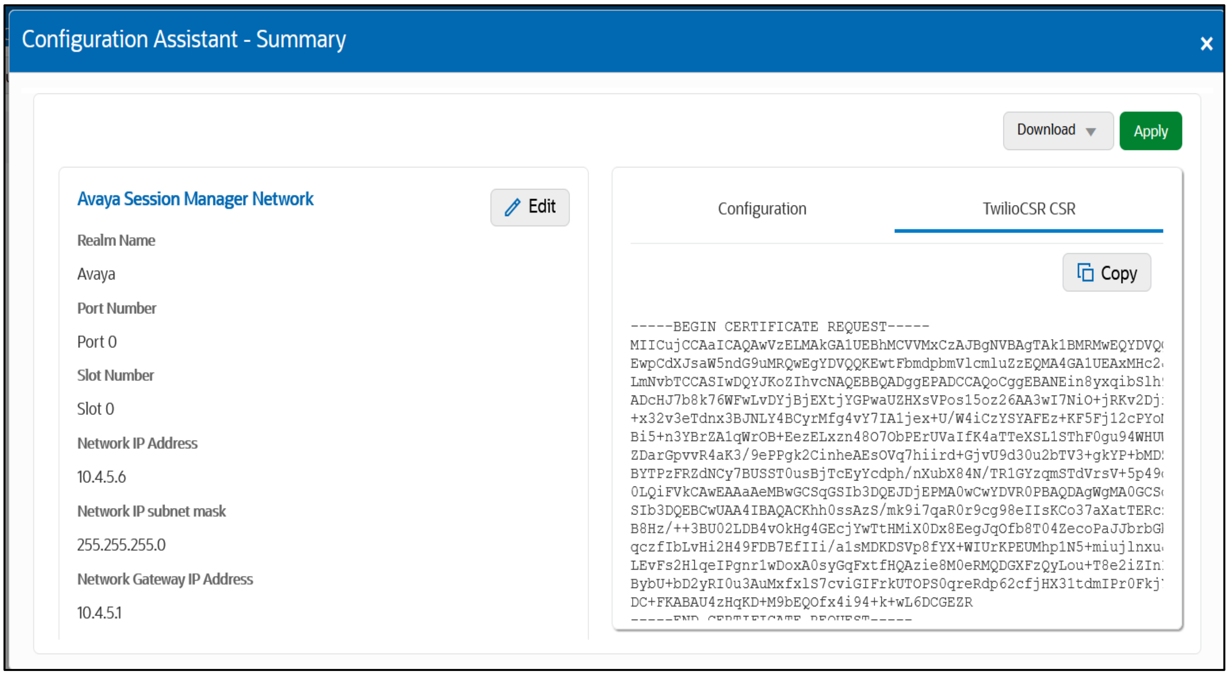
Network Gateway IP Address: 10.4.5.1

```
certificate-record
        name                                        DigiCertRootCe
        common-name                                 DigiCert Root (
certificate-record
        name                                        TwilioCSR
        common-name                                 sbc.com
        extended-key-usage-list                     serverAuth
                                                    ClientAuth
codec-policy
        name                                        AvayaCodecPoli
        allow-codecs                                *
        add-codecs-on-egress                        PCMU G722
codec-policy
        name                                        TwilioCodecPol
        allow-codecs                                *
        add-codecs-on-egress                        G729 PCMA
http-server
```

On the left side of the review contains the entries for each page. Each page has an “*Edit*” tab that can be used to make changes to the information entered on that specific page without having to go through the entire template again.

On the right side of the review page, under the “*Configuration*” tab is the ACLI output from the SBC. This is the complete configuration of the SBC based on the information entered throughout the template. Also on the right side of the review page you may see another tab, “*TwilioCSR CSR*”.

On Page 8 of the template, if you chose CSR from the drop down menu instead of PKCS, the SBC configures a certificate record and generates a certificate signing request for you as shown below.



Configuration Assistant - Summary

Avaya Session Manager Network

Realm Name
Avaya
Port Number
Port 0
Slot Number
Slot 0
Network IP Address
10.4.5.6
Network IP subnet mask
255.255.255.0
Network Gateway IP Address
10.4.5.1

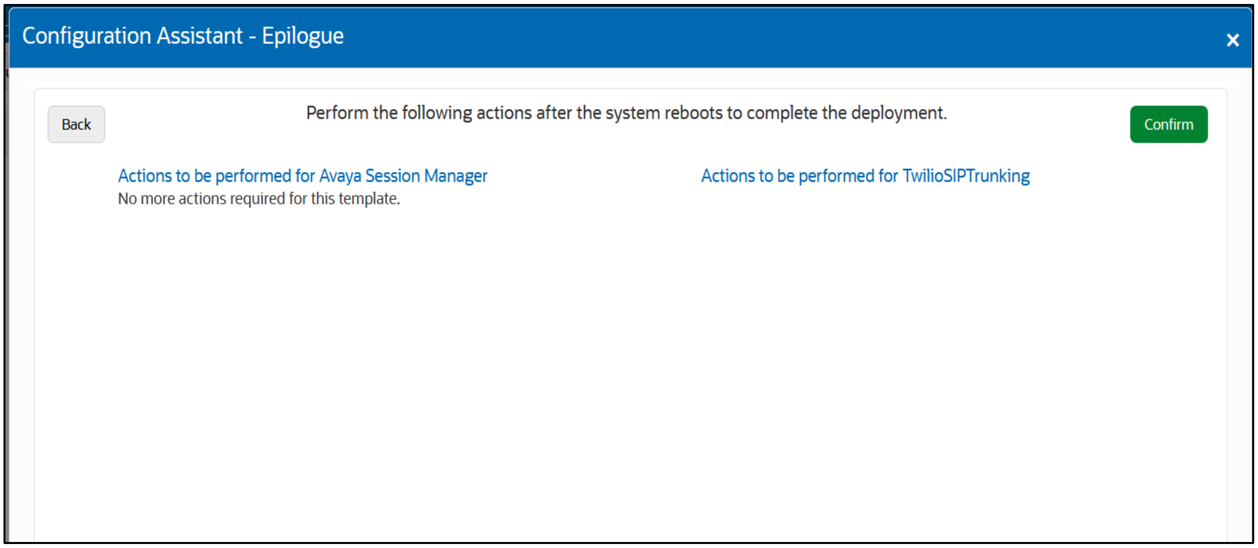
```
-----BEGIN CERTIFICATE REQUEST-----
MIICujCCAaICAQAwVzELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQ
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEQMA4GA1UEAxMHc2
LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANEin8yxqibSlh
ADcHJ7b8k76WFwLvDYjBjEXtjYGPwaUZHXsVPos15oz26AA3wI7NiO+jRKv2Dj
+x32v3eTdnx3BJNLY4BCyrMfg4vY7IA1jex+U/W4iCzYSYAFEz+KF5Fj12cPYo
Bi5+n3YBrZA1qWrOB+EezELxzn48O7ObPErUVaIfK4aTTeXSL1SThF0gu94WHU
ZDarGpvvR4aK3/9ePPgk2CinheAEsOVq7hiird+GjvU9d30u2bTV3+gkYP+bMD
BYTPzFRZdNCy7BUSST0usBjTcEyYcdph/nXubX84N/TR1GYzqmSTdVrsV+5p49
0LQiFVkCAwEAAaAeMBwGCSqGSIb3DQEJDjEPMA0wCwYDVR0PBAQDAgWgMA0GCS
SIb3DQEBCwUAA4IBAQACKhh0ssAzS/mk9i7qaR0r9cg98eIIsKCo37aXatTERc
B8Hz/++3BU02LDB4vOkHg4GEcjYwTtHMiX0Dx8EegJqOfb8T04ZecoPaJJbrbG
qczfIbLvHi2H49FDB7EfIIi/a1sMDKDSVp8fYX+WIUrKPEUMhp1N5+miujlnxu
LEvFs2HlqeIPgnr1wDoxA0syGqFxtfHQAzie8M0eRMQDGXFzQyLou+T8e2iZIn
BybU+bD2yRI0u3AuMxfxlS7cviGIFrkUTOPS0qreRdp62cfjHX31tdmIPr0Fkj
DC+FKABAU4zHqKD+M9bEQOfx4i94+k+wL6DCGEZR
-----END CERTIFICATE REQUEST-----
```

Click the copy button under the CSR, and paste the output into a text file. Next, provide the txt file to your CA for signature. Once the certificate is signed by a Twilio supported CA, you will need to import that certificate into the SBC manually, either via ACLI or through the GUI.

Note: if you chose to import a certificate in PKCS12 format on page 8, the CSR tab will not be present under review.

8.5. Download and/or Apply

Now that the entries provided throughout the template have been reviewed, and the CSR has been copied into a text file (optional), the template provides you with the ability to "Download" the config by clicking the "*Download*" tab on the top right. Next, click the "*Apply*" button on the top right, and you will see the following pop up box appear.



Configuration Assistant - Epilogue

Perform the following actions after the system reboots to complete the deployment.

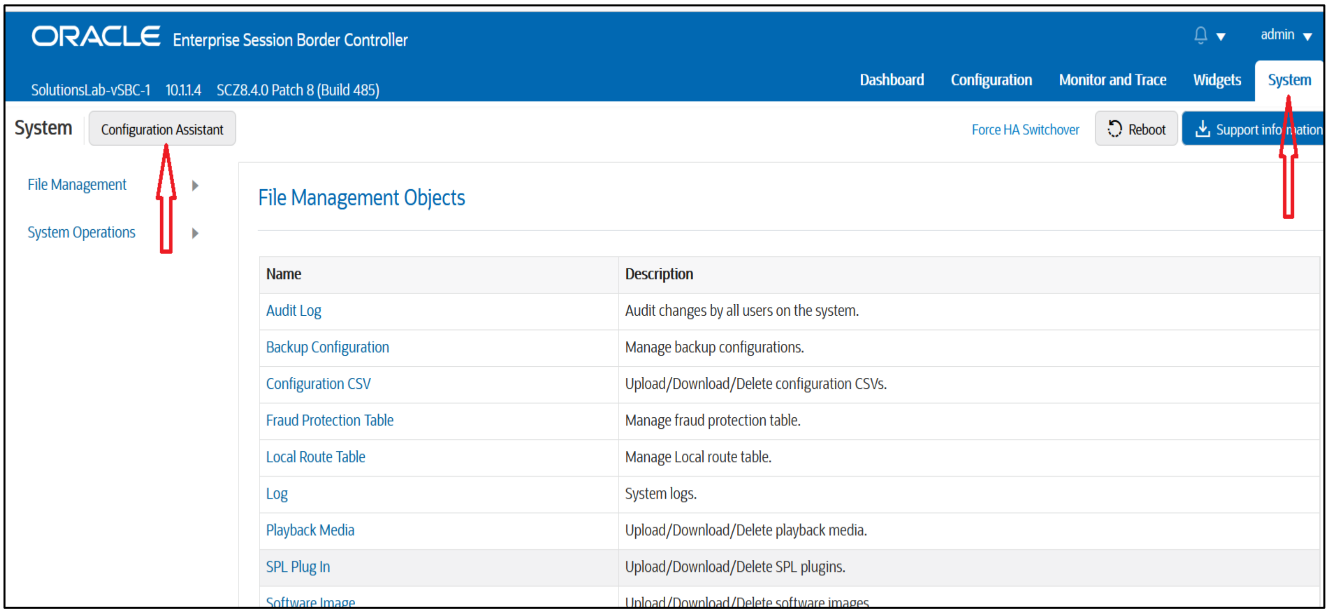
Actions to be performed for Avaya Session Manager
No more actions required for this template.

Actions to be performed for TwilioSIPTrunking

Now you can click "*Confirm*" to confirm you want to apply the configuration to the SBC. The SBC will reboot. When it comes back up, the SBC will have a basic configuration in place for Avaya Session Manager with Twilio SIP trunking.

8.6. Configuration Assistant Access

Upon initial login, if the Configuration Assistant Template does not immediately appear on the screen, you can access by clicking on the "*SYSTEM*" tab, top right of your screen. After that, click on the "*Configuration Assistant*" tab, top left. This allows end users to access the Configuration Assistance at any time through the SBC GUI.



File Management Objects

Name	Description
Audit Log	Audit changes by all users on the system.
Backup Configuration	Manage backup configurations.
Configuration CSV	Upload/Download/Delete configuration CSVs.
Fraud Protection Table	Manage fraud protection table.
Local Route Table	Manage Local route table.
Log	System logs.
Playback Media	Upload/Download/Delete playback media.
SPL Plug In	Upload/Download/Delete SPL plugins.
Software Image	Upload/Download/Delete software images.

9. Existing SBC configuration

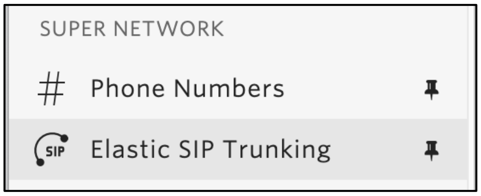
If the SBC being used is an existing SBC with functional configuration, following configuration elements are required:

- 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.

10. Twilio Elastic SIP Trunking Configuration

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



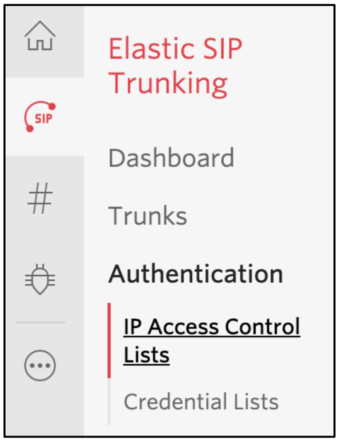
SUPER NETWORK

Phone Numbers

SIP Elastic SIP Trunking

10.1. Create an IP-ACL rule

Click on Authentication in the left navigation, and then click on IP Access Control Lists.



Elastic SIP Trunking

Dashboard

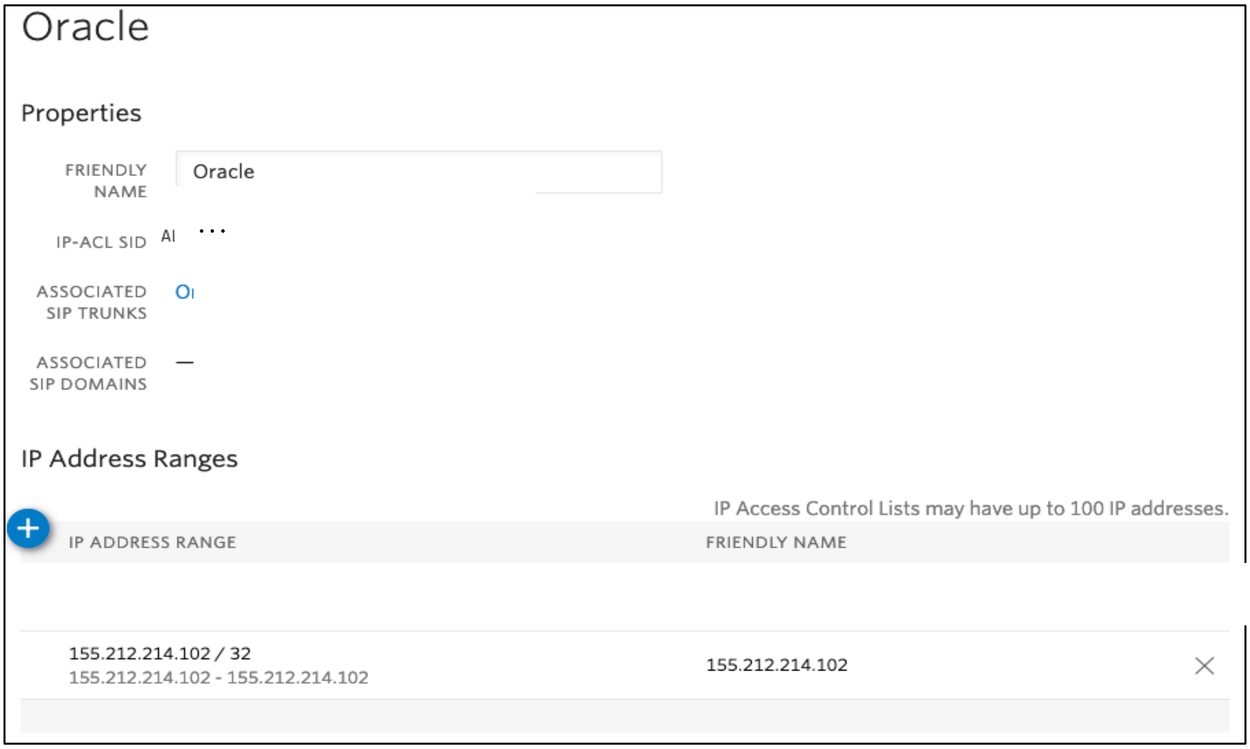
Trunks

Authentication

IP Access Control Lists

Credential Lists

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



Oracle

Properties

FRIENDLY NAME: Oracle

IP-ACL SID: Al ...

ASSOCIATED SIP TRUNKS: O

ASSOCIATED SIP DOMAINS: —

IP Address Ranges

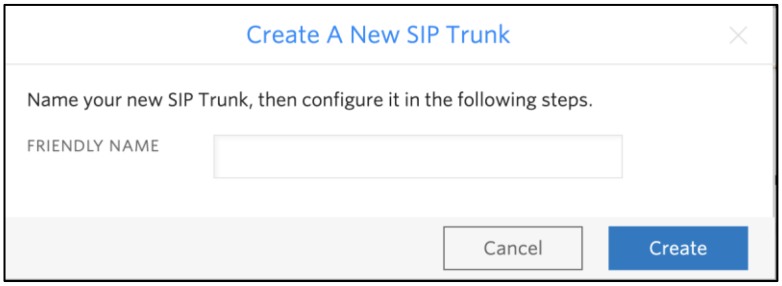
IP Access Control Lists may have up to 100 IP addresses.

IP ADDRESS RANGE	FRIENDLY NAME
155.212.214.102 / 32 155.212.214.102 - 155.212.214.102	155.212.214.102

10.2. 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.

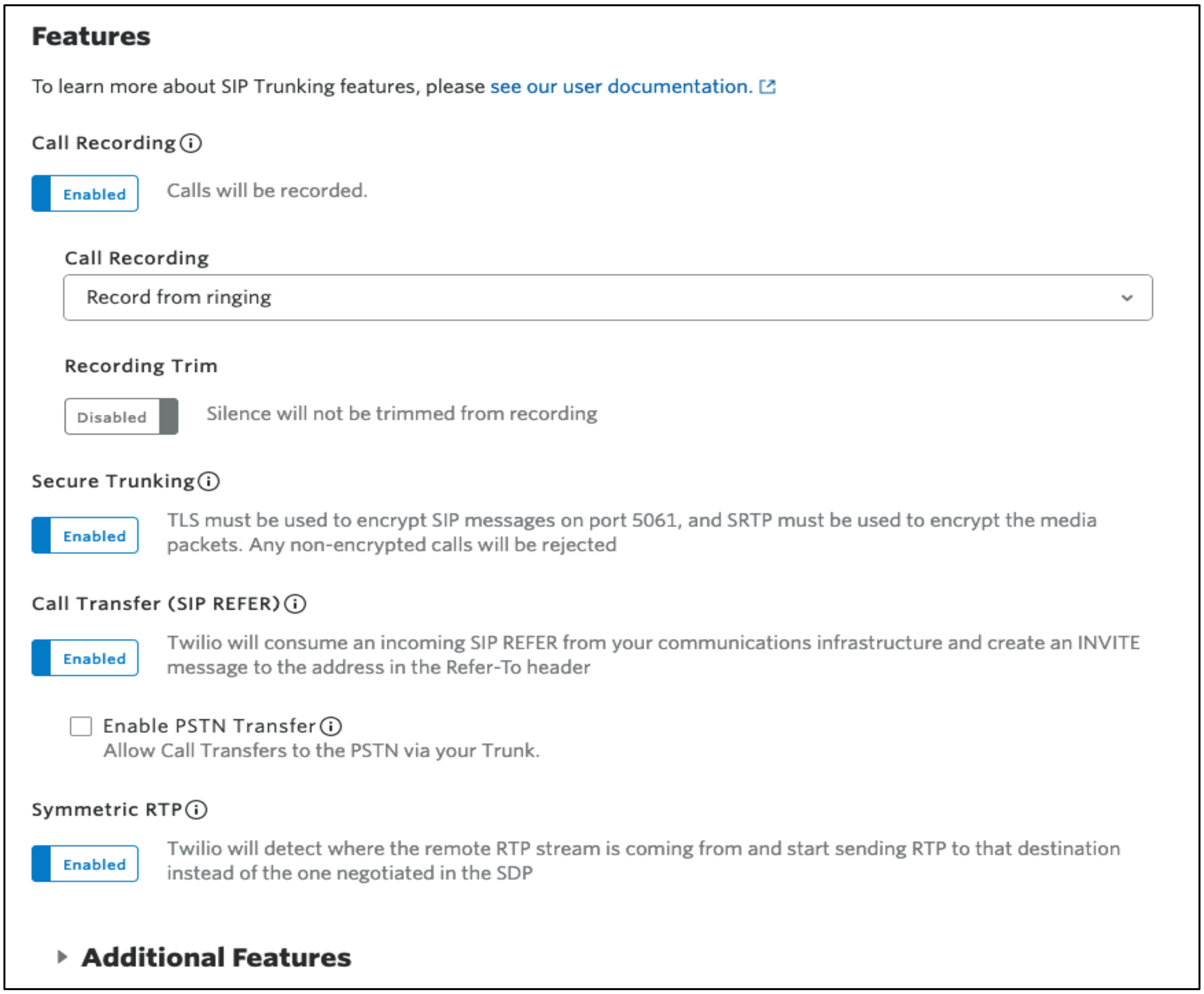


Create A New SIP Trunk

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: Record from ringing

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

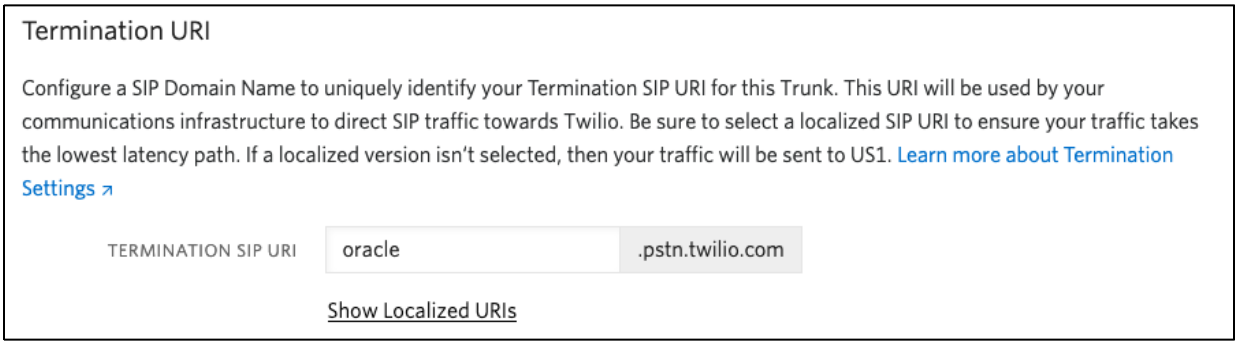
□ Enable PSTN Transfer ⓘ
Allow Call Transfers to the PSTN via your Trunk.

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.



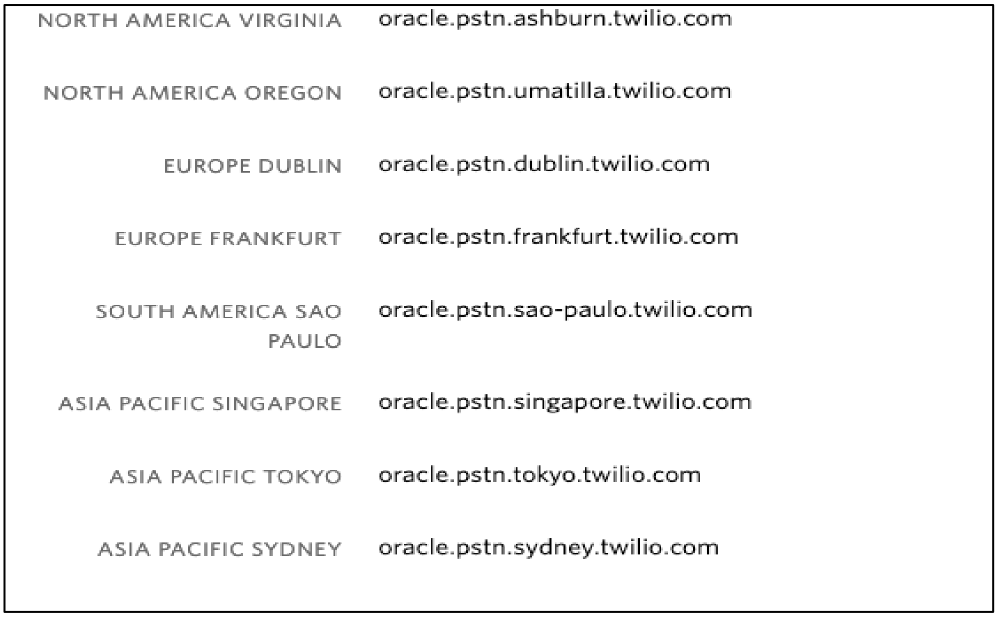
Termination URI

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: oracle .pstn.twilio.com

Show Localized URIs

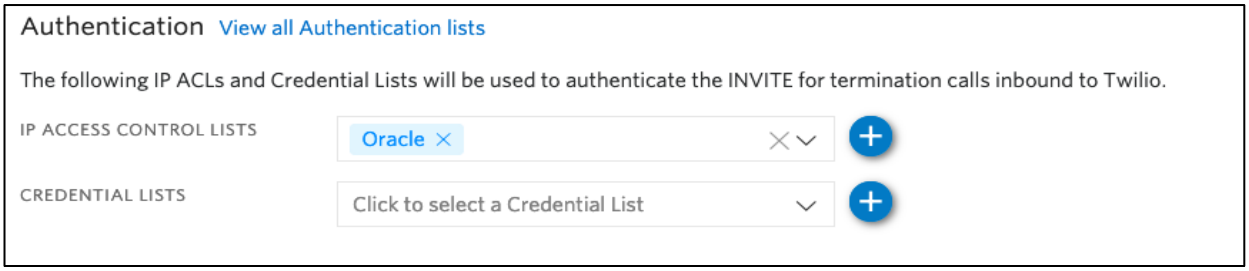
Click on "Show localized URI's" and copy and paste this information as you will use this on your SBC to configure your Trunk.



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

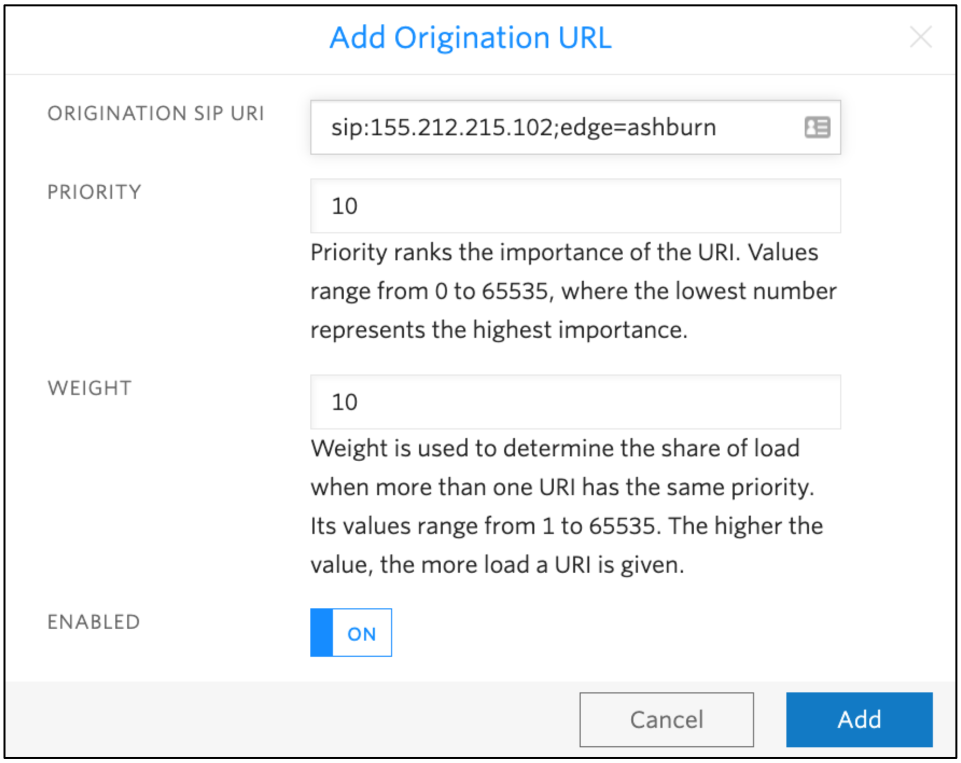
The following IP ACLs and Credential Lists will be used to authenticate the INVITE for termination calls inbound to Twilio.

IP ACCESS CONTROL LISTS: Oracle ×

CREDENTIAL LISTS: Click to select a Credential List

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: sip:155.212.215.102;edge=ashburn

PRIORITY: 10

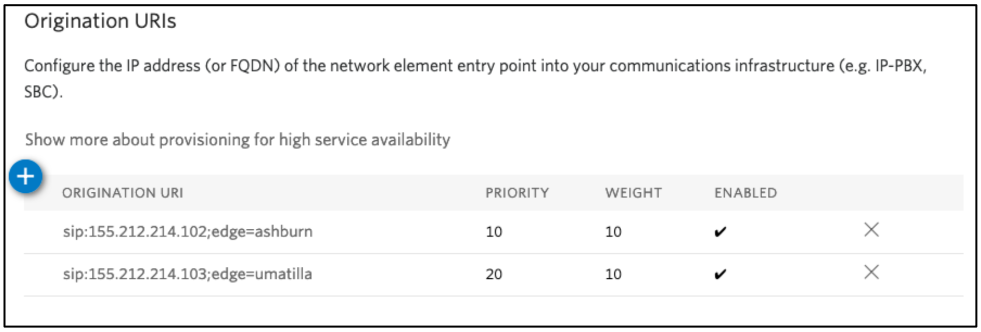
Priority ranks the importance of the URI. Values range from 0 to 65535, where the lowest number represents the highest importance.

WEIGHT: 10

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: ON

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).

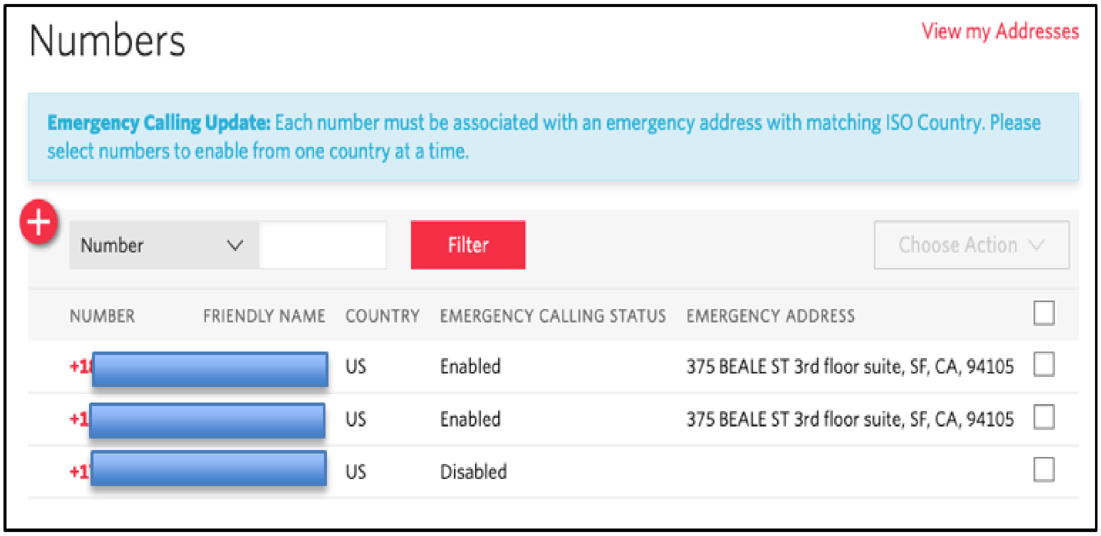
Show more about provisioning for high service availability

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.

10.3. 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

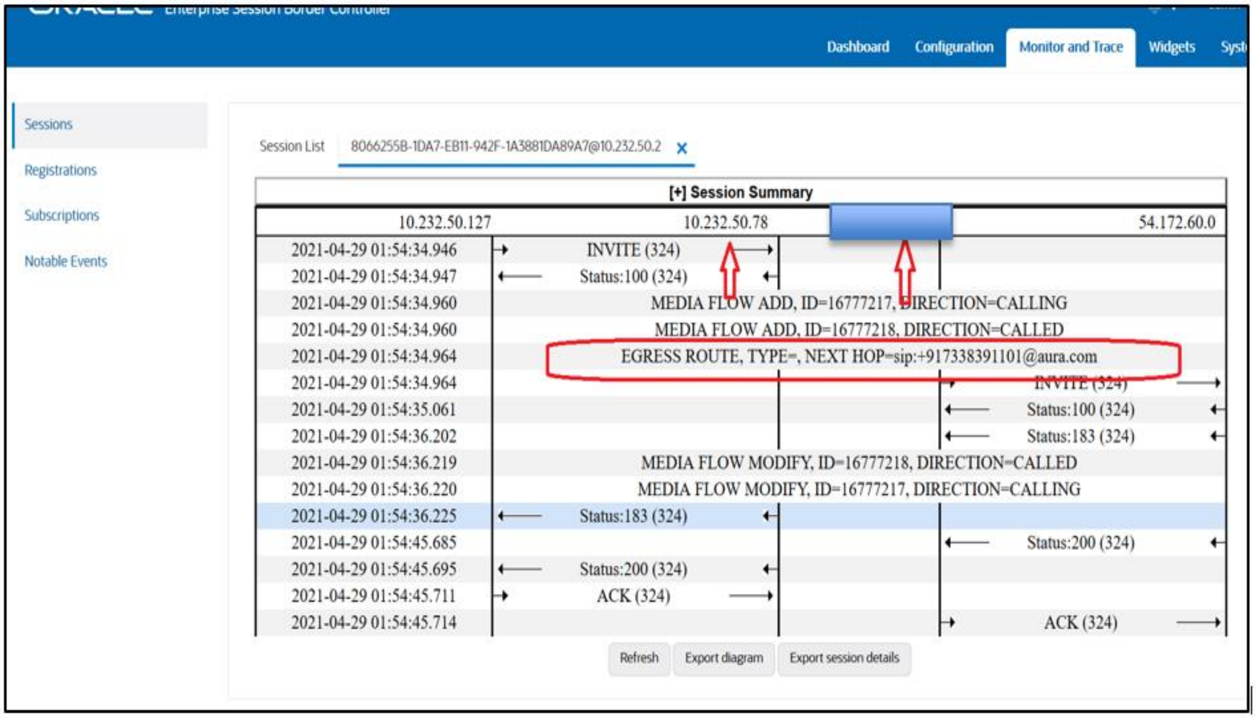
Emergency Calling Update: Each number must be associated with an emergency address with matching ISO Country. Please select numbers to enable from one country at a time.

NUMBER	FRIENDLY NAME	COUNTRY	EMERGENCY CALLING STATUS	EMERGENCY ADDRESS	□
+1[redacted]		US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	□
+1[redacted]		US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	□
+1[redacted]		US	Disabled		□

11. 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

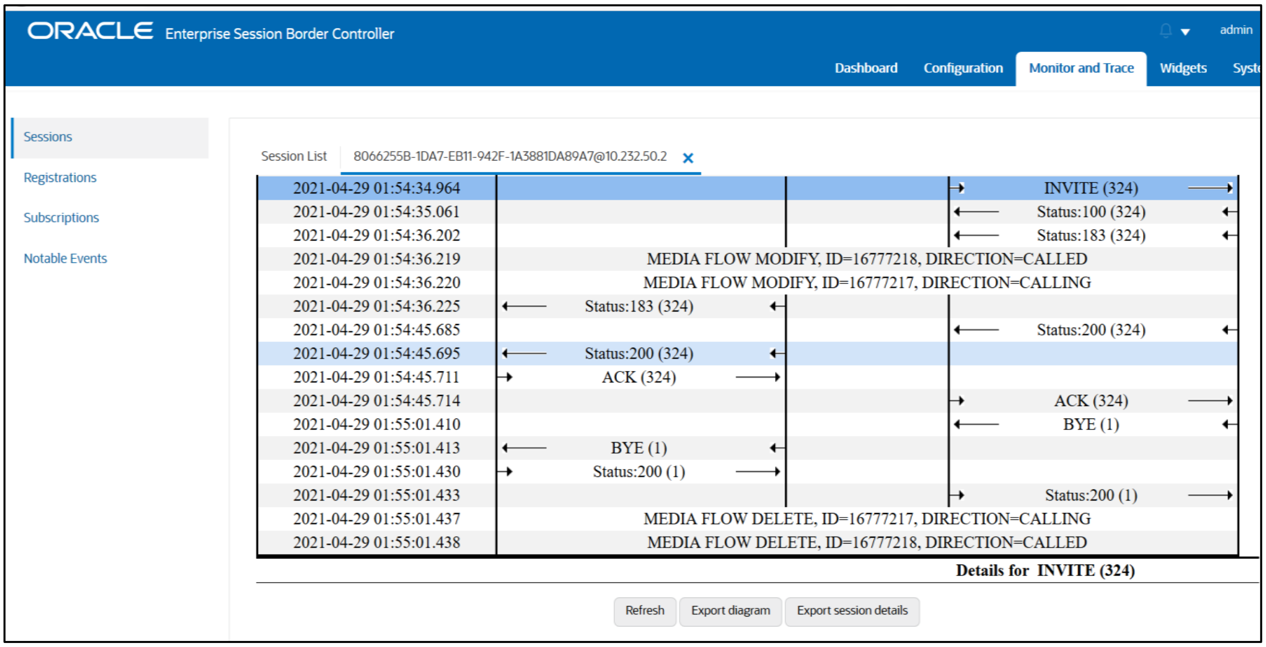
1. Make Call from Avaya user to the Twilio Elastic Sip Trunk and check the call flow. The calls flow from Avaya SIP Interface to Twilio Elastic SIP Trunking Interface and to Twilio Session Agent and the call reaches the PSTN user after that.



Session List 8066255B-1DA7-EB11-942F-1A3881DA89A7@10.232.50.2 ×

[+] Session Summary

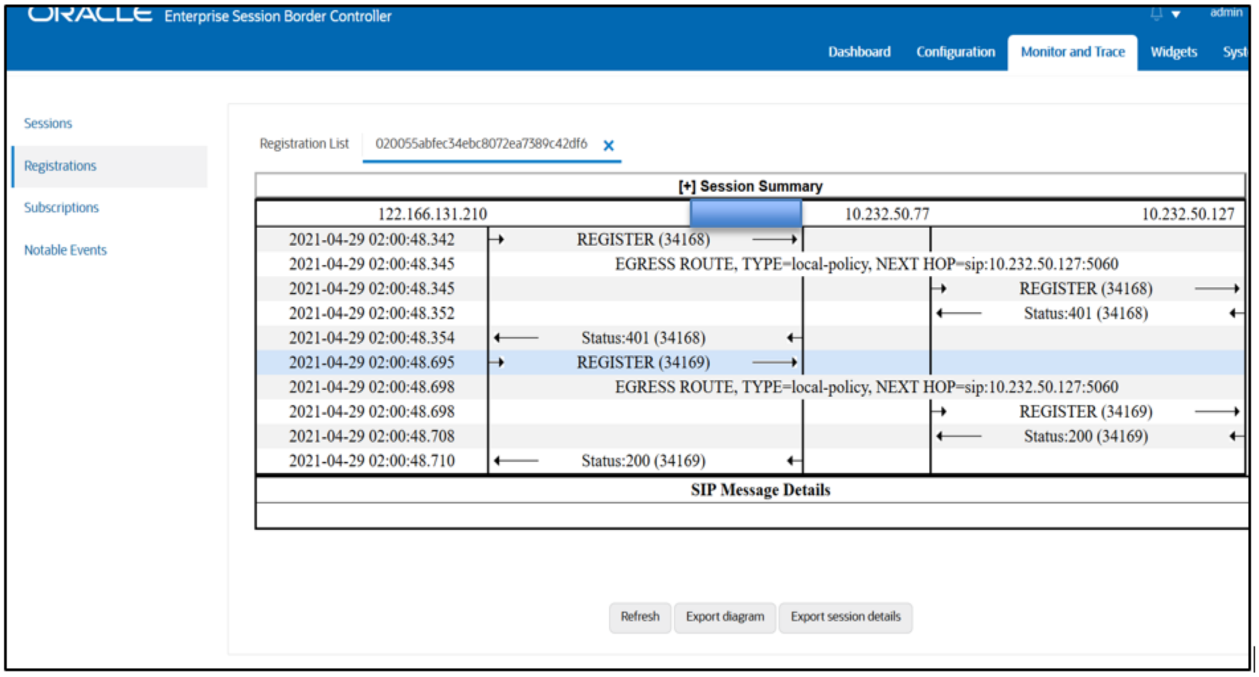
```
                         10.232.50.127              10.232.50.78      [redacted]                       54.172.60.0
2021-04-29 01:54:34.946  →      INVITE (324)       →
2021-04-29 01:54:34.947  ←      Status:100 (324)   ←
2021-04-29 01:54:34.960         MEDIA FLOW ADD, ID=16777217, DIRECTION=CALLING
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)          →
```



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	← BYE (1)	
2021-04-29 01:55:01.430	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)

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

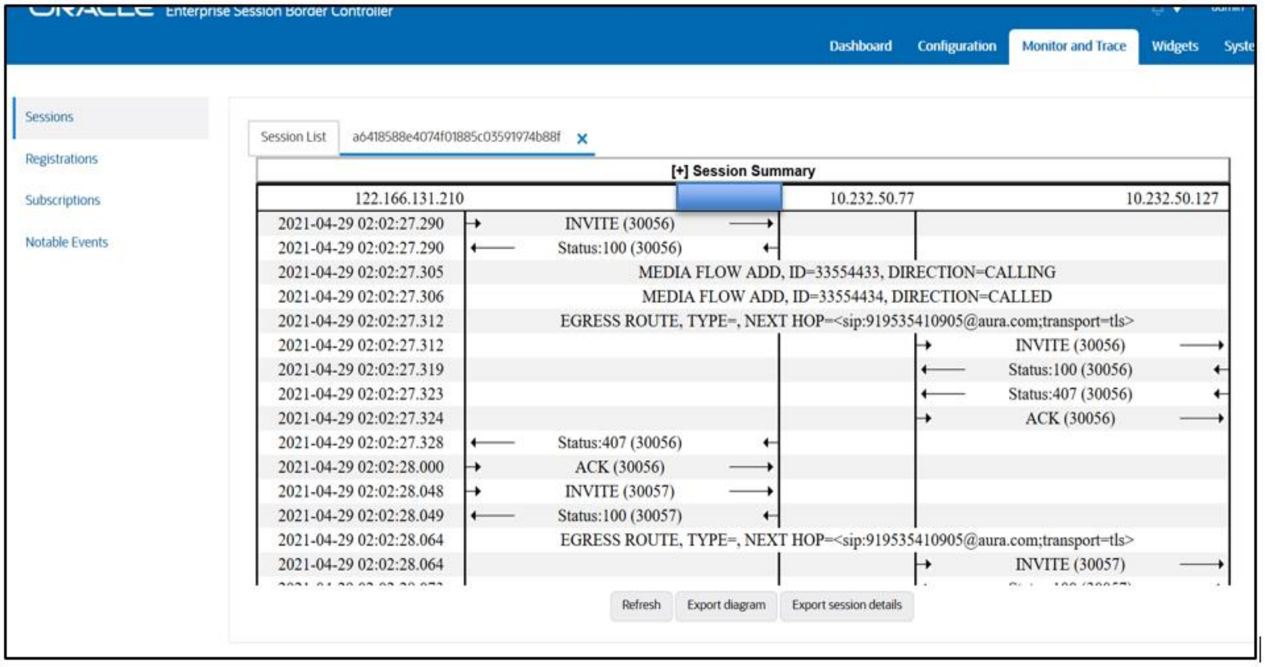


[+] Session Summary

	122.166.131.210	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)		

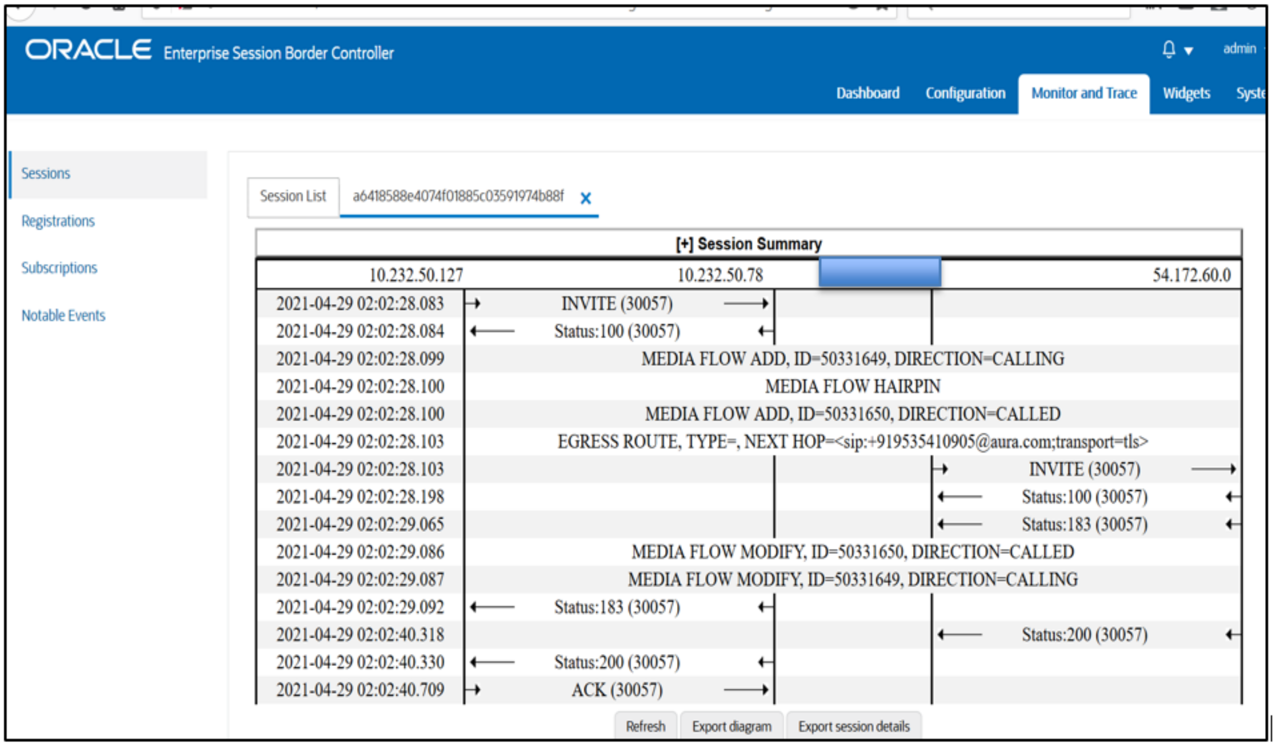
SIP Message Details

3. 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.



[+] Session Summary

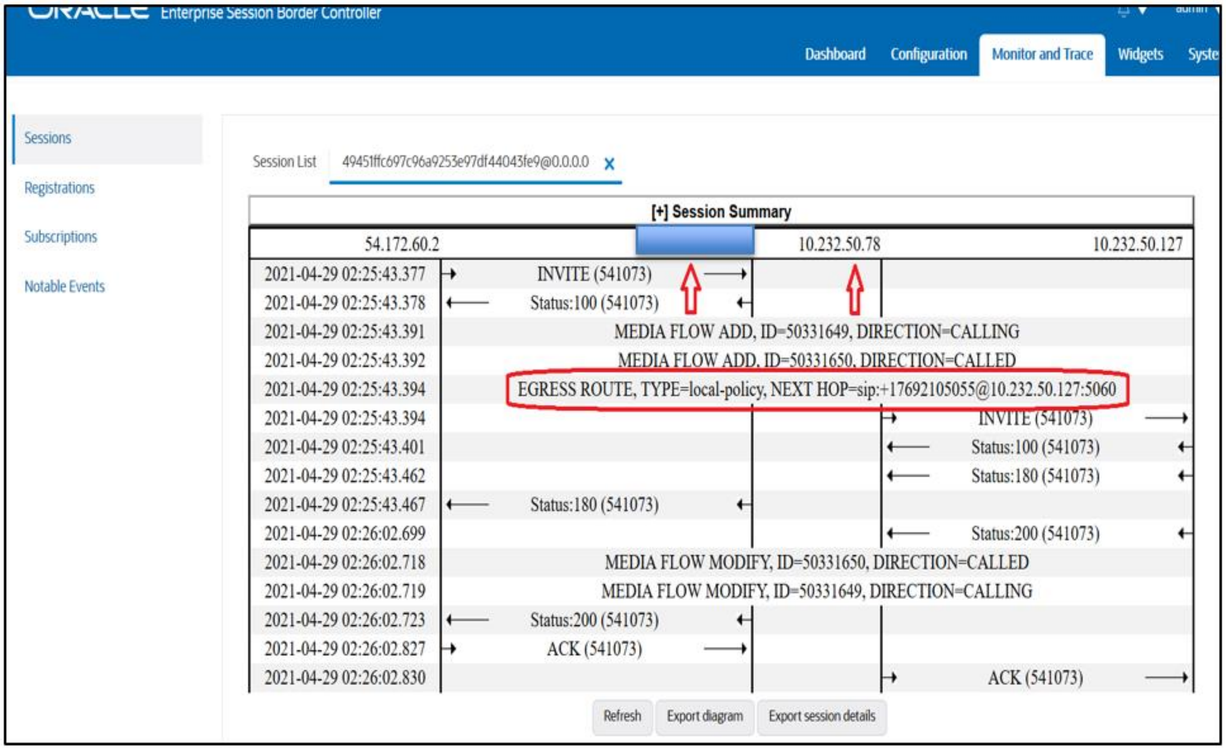
```
                          122.166.131.210                         10.232.50.77                10.232.50.127
2021-04-29 02:02:27.290   →   INVITE (30056)   →
2021-04-29 02:02:27.290   ←   Status:100 (30056)   ←
2021-04-29 02:02:27.305   MEDIA FLOW ADD, ID=33554433, DIRECTION=CALLING
2021-04-29 02:02:27.306   MEDIA FLOW ADD, ID=33554434, DIRECTION=CALLED
2021-04-29 02:02:27.312   EGRESS ROUTE, TYPE=, NEXT HOP=<sip:919535410905@aura.com;transport=tls>
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=tls>
2021-04-29 02:02:28.064                                   →   INVITE (30057)   →
```



[+] Session Summary

```
                          10.232.50.127            10.232.50.78                               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=tls>
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)   →
```

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

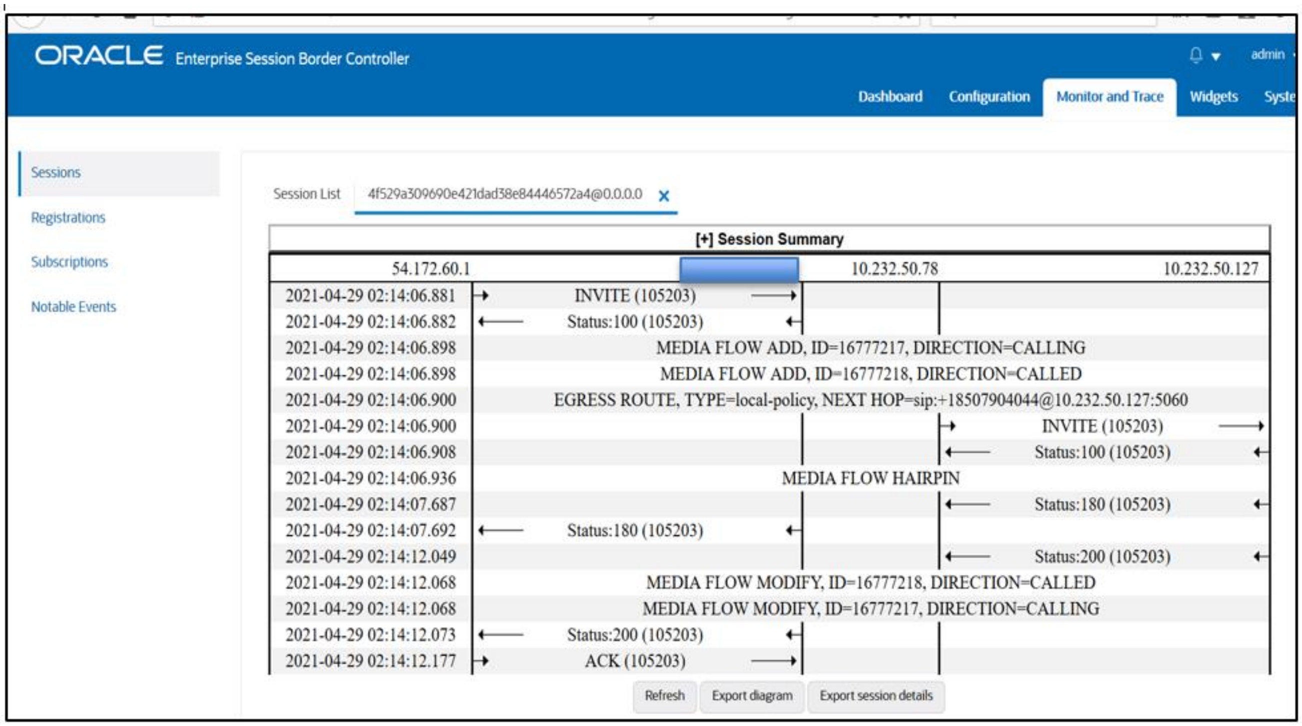


4945ffc697c96a9253e97df44043fe9@0.0.0.0

[+] Session Summary

```
                          54.172.60.2                     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)         →
```

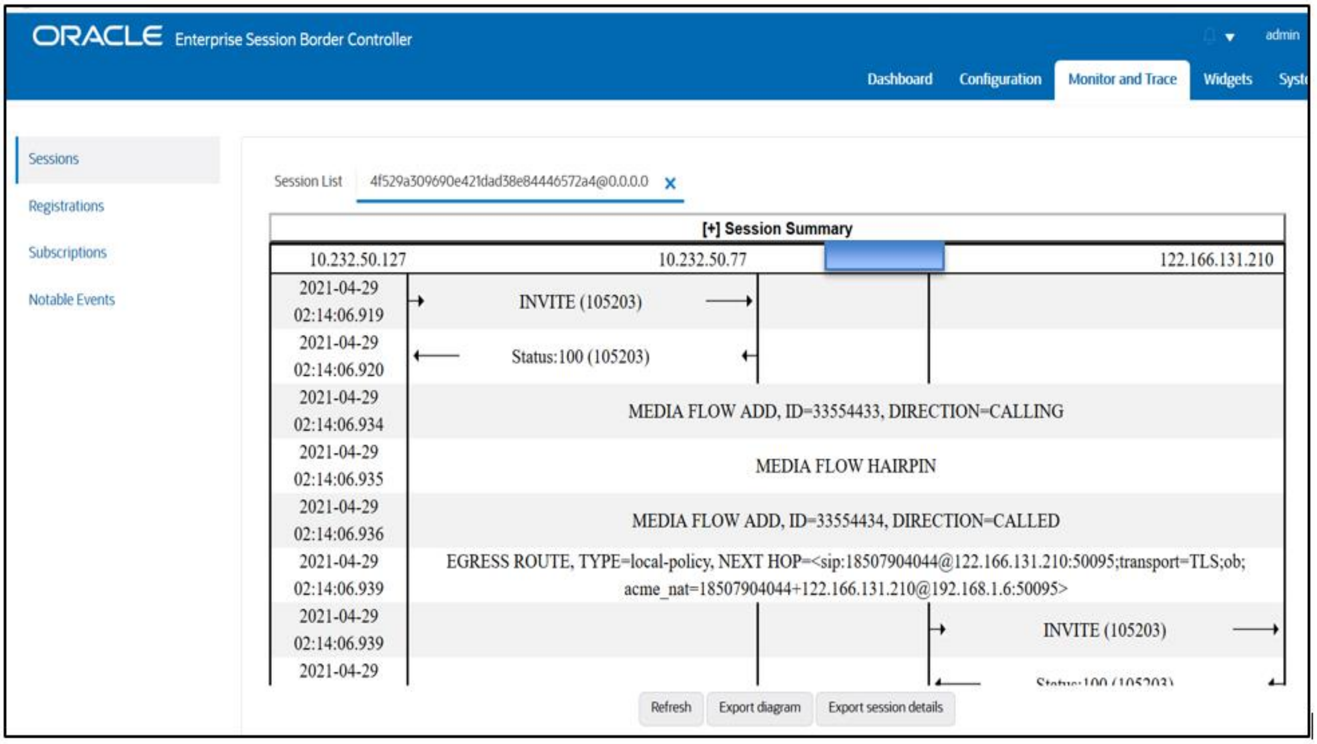
5. Make Call from Twilio Elastic Sip Trunk user to Avaya Remote user and check the call flow. Now, there will be 2 call legs (hair pinned call) as the call reaches Avaya Session Manager first and then reaches Avaya Remote user after that as given below



Session List 4f529a309690e421dad38e84446572a4@0.0.0.0

[+] Session Summary

	54.172.60.1	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) →		



Session List 4f529a309690e421dad38e84446572a4@0.0.0.0

[+] Session Summary

	10.232.50.127	10.232.50.77	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			← Status:100 (105203)

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

facebook.com/Oracle/

twitter.com/Oracle

oracle.com

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services