Oracle SBC integration with Avaya Aura Session Manager for Avaya Workplace soft client in TLS/SRTP mode

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 Aura Session Manager for Avaya Workplace client in TLS/SRTP mode	20th December 2020
1.1	App Note updated with Minor changes (Caveat added)	30th March 2021
1.1	App Note updated with Minor formatting changes	12th November 2021

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 the configuration needed to set up the interworking between on premises Avaya Aura Session Manager using Oracle SBC. The solution contained within this document has been tested using Oracle Communication OS 840p3 version.

Our scope of this document is only limited to registering Avaya Workplace soft client for windows as remote worker (In Manual mode alone) to Avaya Session Manager using Oracle SBC and testing call features which are available using TLS/SRTP protocol. Testing Avaya Workspace soft client in automatic mode is out of scope of this document. The pre-requisite is also that the user should have downloaded the Avaya workspace client for windows 3.13 version (or above) from Avaya website and have installed that in the windows machine.

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

For more information about Avaya Workplace client configuration and other things, please refer to the below link:

https://downloads.avaya.com/css/P8/documents/101071816

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

3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Avaya Aura System Manager GUI and Avaya Aura Session manager server in 8.1 version using Oracle Enterprise SBC. There will be steps that require navigating to Oracle SBC GUI interface, understanding the basic concepts of TCP/UDP, IP/Routing, SIP/TLS/SRTP and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary. It is also understood that the end user has already configured Avaya Aura Session Manager Configuration before referring this document.

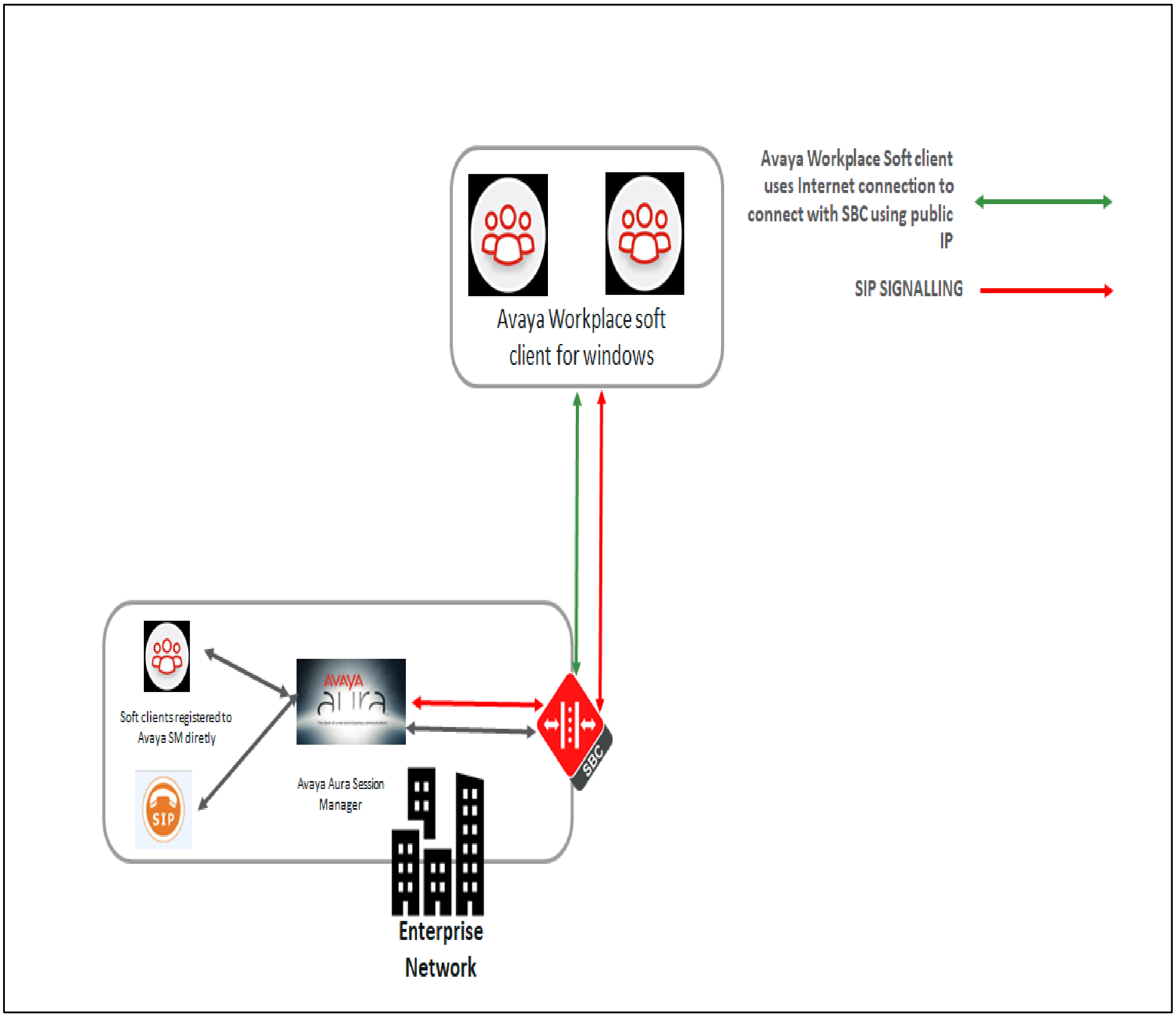
3.2. Requirements

- Avaya Workplace soft client for windows 3.13 version and above.
- Fully functioning Avaya Aura Session Manager 8.1 version.
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version

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

Software Used	Avaya Aura Session Manager using Avaya Aura System Manager GUI	SBC Version	Avaya Workplace soft client
Revision 1	8.1	8.4.0	3.13

3.3. Architecture

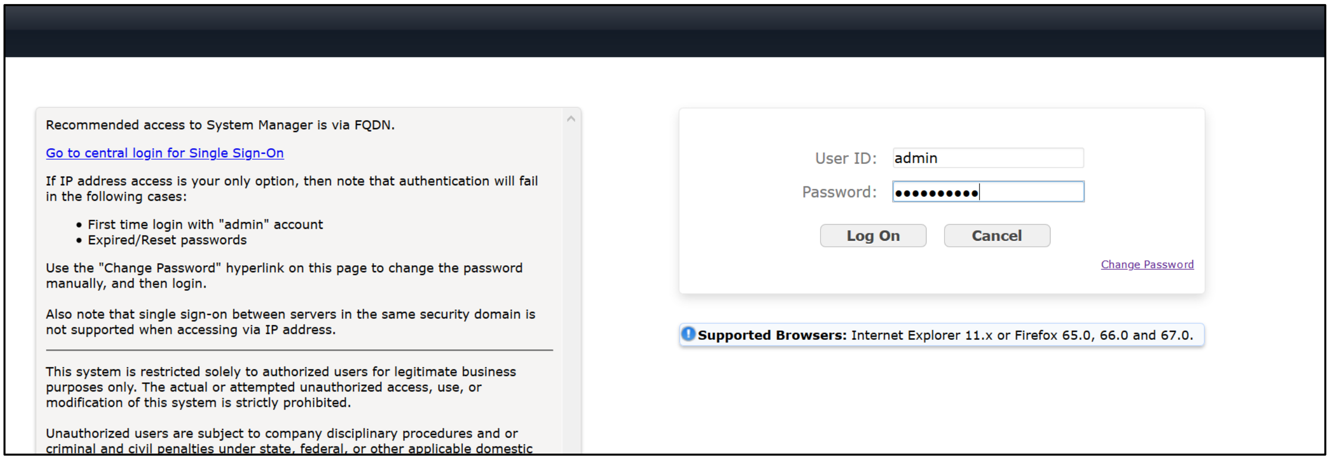

Avaya Workplace soft client for windows
Avaya Workplace Soft client uses Internet connection to connect with SBC using public IP
SIP SIGNALLING
Soft clients registered to Avaya SM diretly
SIP
AVAYA aura
Avaya Aura Session Manager
SBC
Enterprise Network

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

- Phase 1 – Configuring the Avaya Aura Session Manager for Oracle SBC
- Phase 2 – Configuring the Avaya Workplace soft client for windows 3.13 version
- Phase 3 – Configuring the Oracle SBC.

4. Configuring the Avaya Aura Session Manager 8.1

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



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

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

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

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

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

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

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

User ID: admin

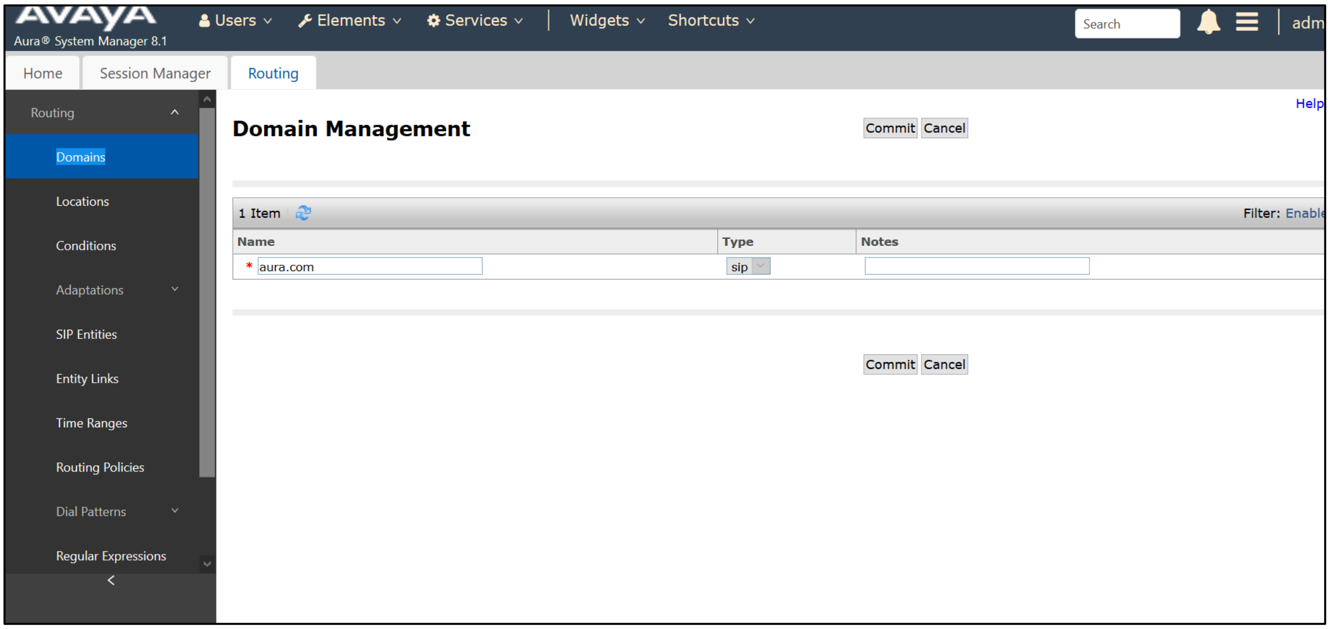
Password: ••••••••••

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

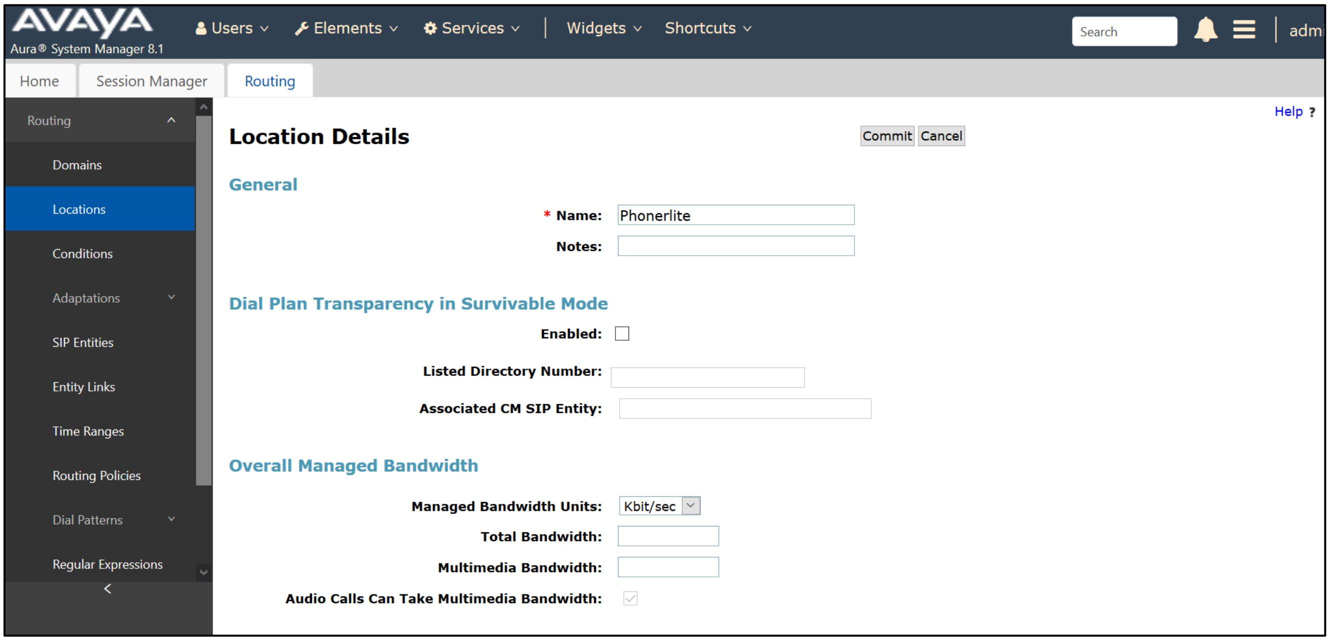
1 Item

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

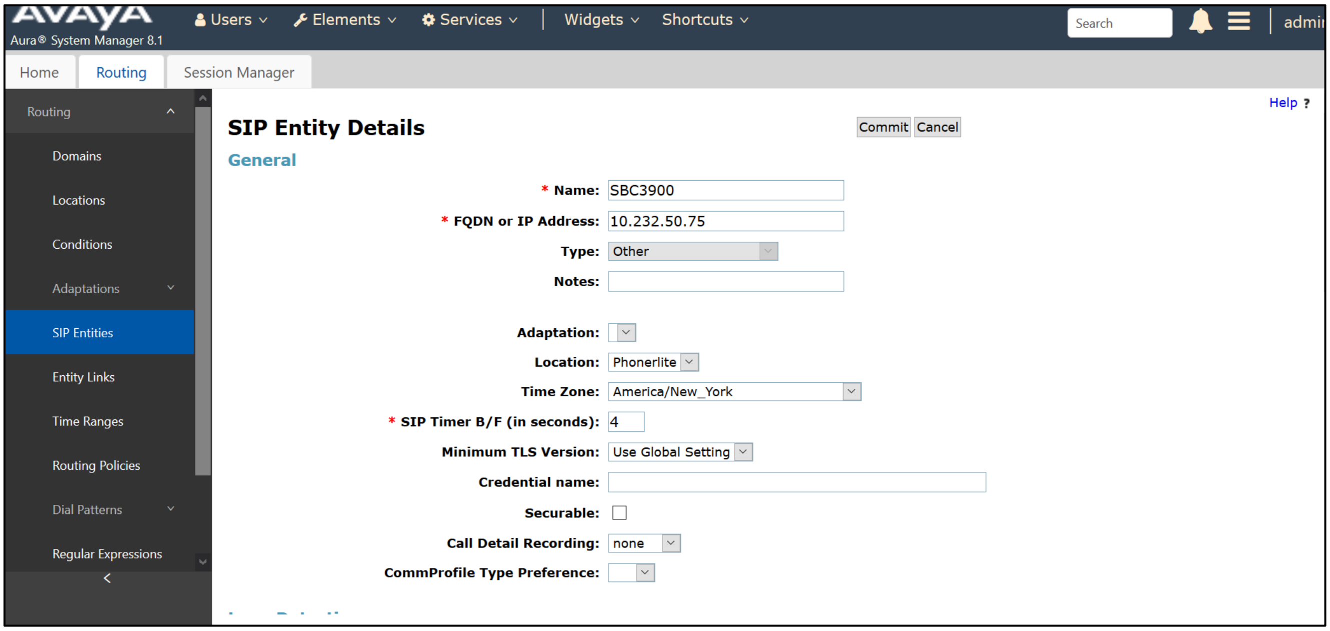
Managed Bandwidth Units: Kbit/sec
Total Bandwidth:
Multimedia Bandwidth:
Audio Calls Can Take Multimedia Bandwidth: ☑

4.3. Adding the 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: SBC3900 (example in this configuration)
- Set FQDN or IP Address: This is the “inside” IP address of Oracle E-SBC, 10.50.232.75 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 SBC3900
- Set Protocol: UDP/TCP/TLS based on our testing
- Set Ports: Set both Ports to 5060/5061 for testing
- Set Connection Policy: trusted

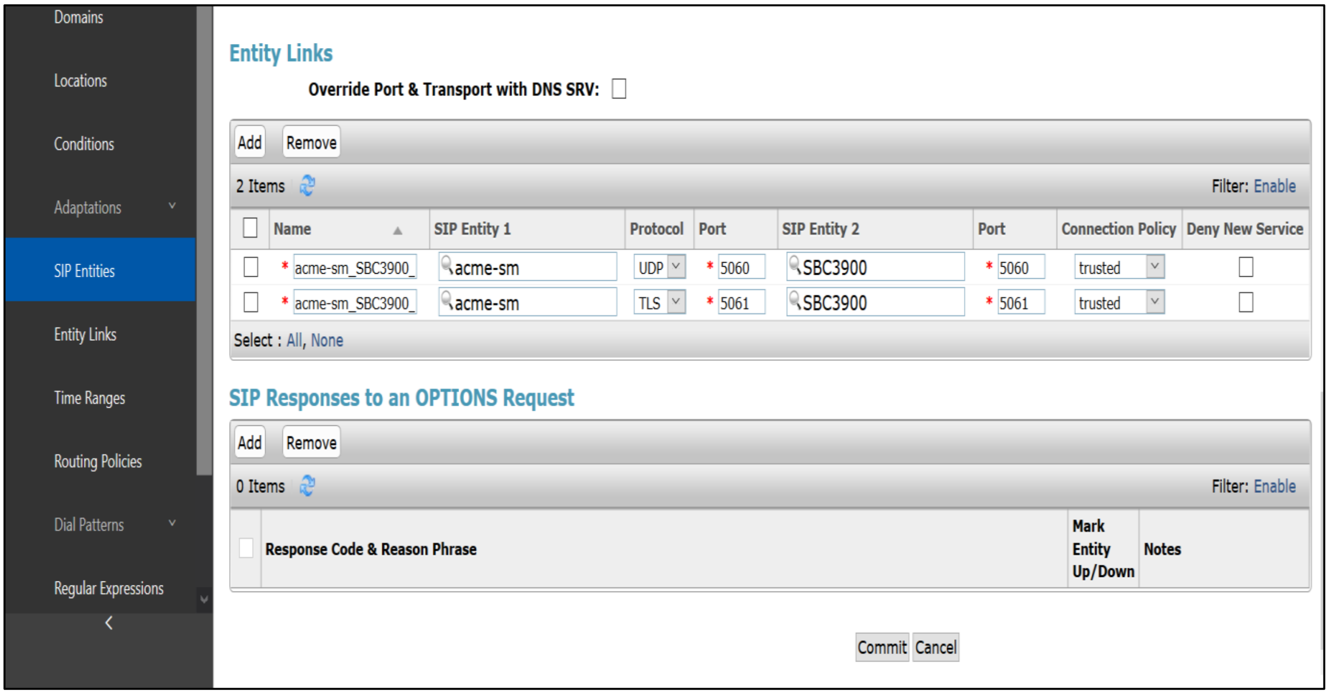
Leave all other fields as default values and click “Commit” to save the configuration.



SIP Entity Details

General

* Name:	SBC3900
* FQDN or IP Address:	10.232.50.75
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:	



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_SBC3900_	acme-sm	UDP	* 5060	SBC3900	* 5060	trusted	□
□	* acme-sm_SBC3900_	acme-sm	TLS	* 5061	SBC3900	* 5061	trusted	□

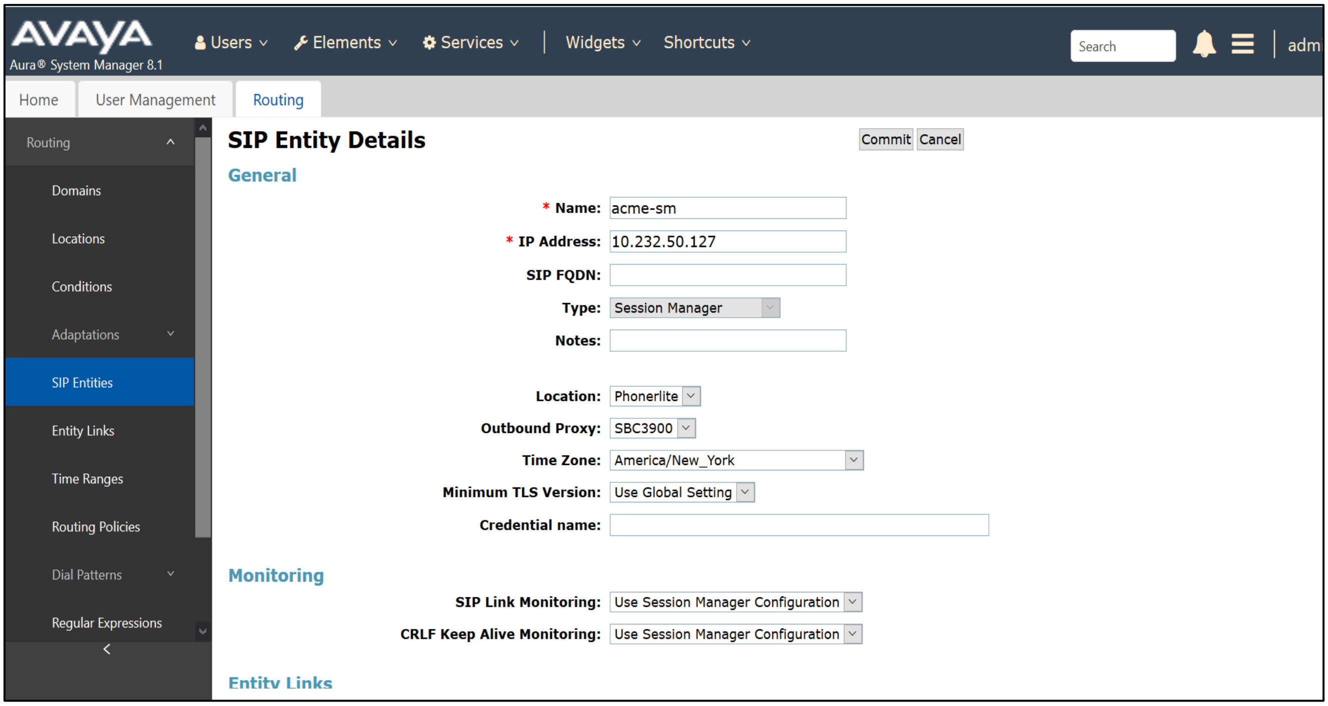
SIP Responses to an OPTIONS Request

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

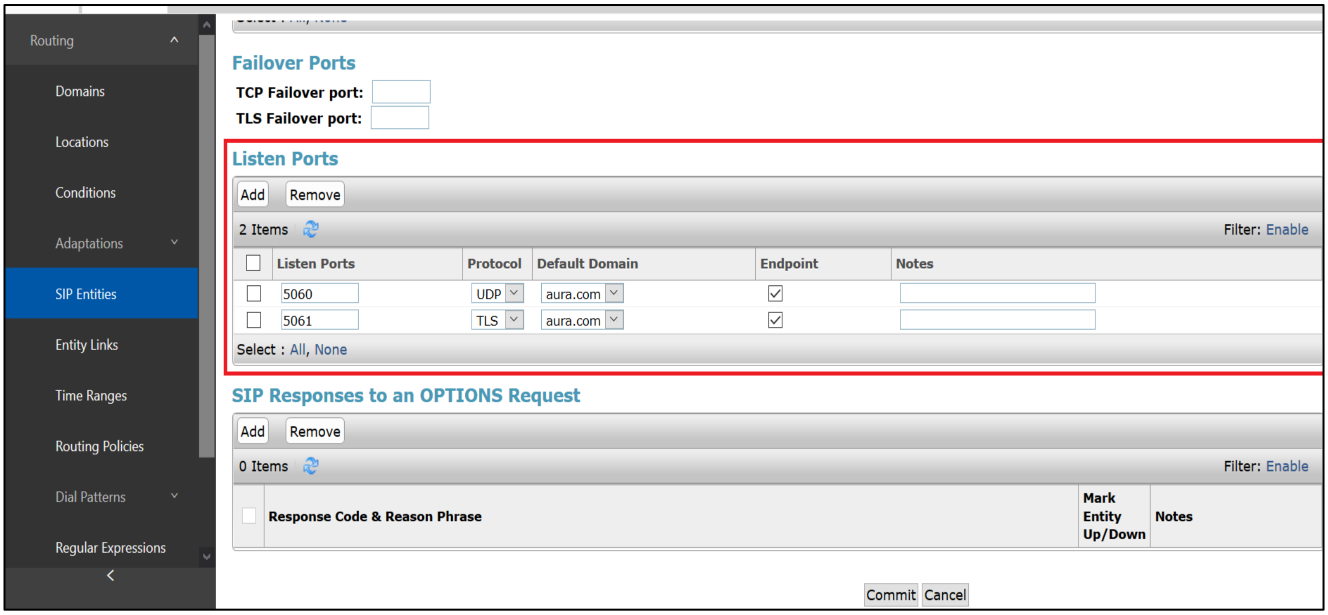
* Name:	acme-sm
* IP Address:	10.232.50.127
SIP FQDN:	
Type:	Session Manager
Notes:	
Location:	Phonerlite
Outbound Proxy:	SBC3900
Time Zone:	America/New_York
Minimum TLS Version:	Use Global Setting
Credential name:	

Monitoring

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

Entity Links

Please configure listen ports for the Avaya Session Manager as given below:



Failover Ports

TCP Failover port:

TLS Failover port:

Listen Ports

2 Items

□	Listen Ports	Protocol	Default Domain	Endpoint	Notes
□	5060	UDP	aura.com	☑	
□	5061	TLS	aura.com	☑	

Select : All, None

SIP Responses to an OPTIONS Request

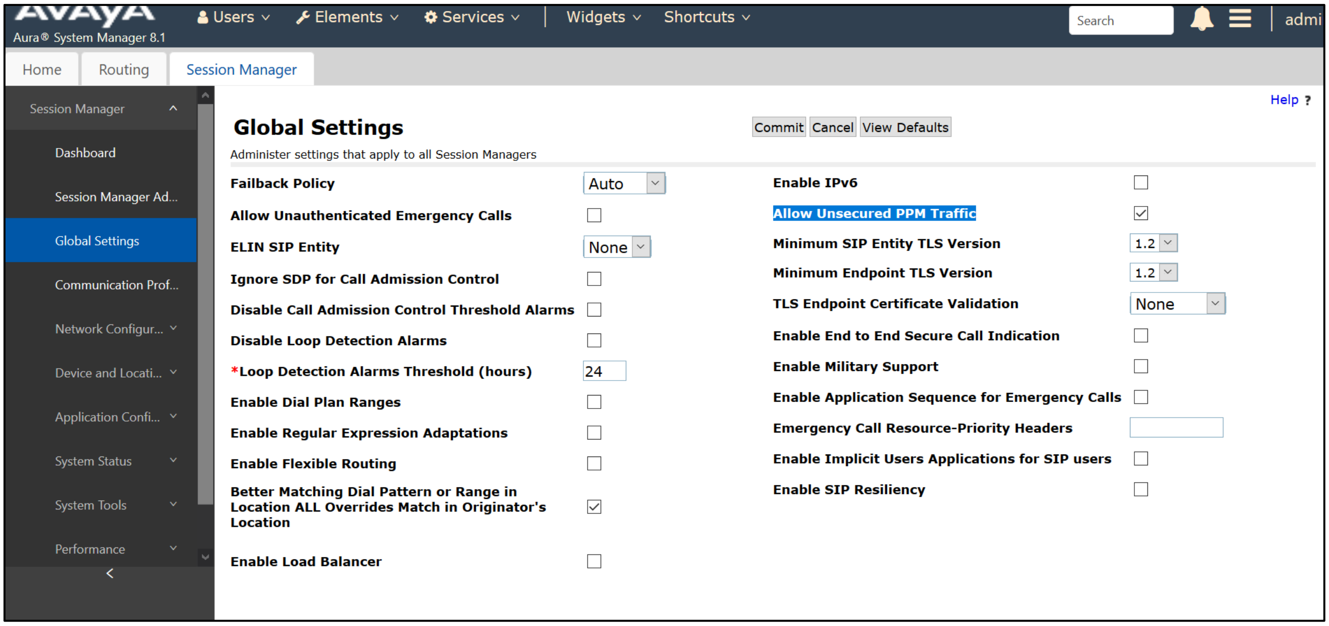
0 Items

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

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

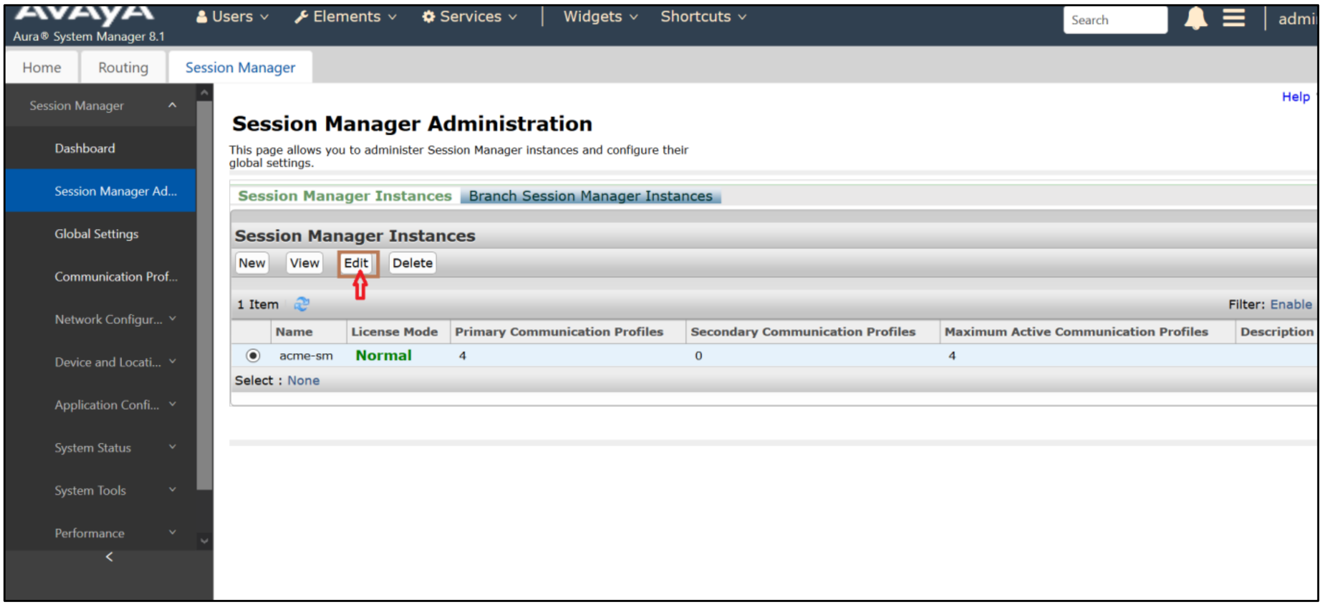
Administer settings that apply to all Session Managers

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

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 | Branch Session Manager Instances

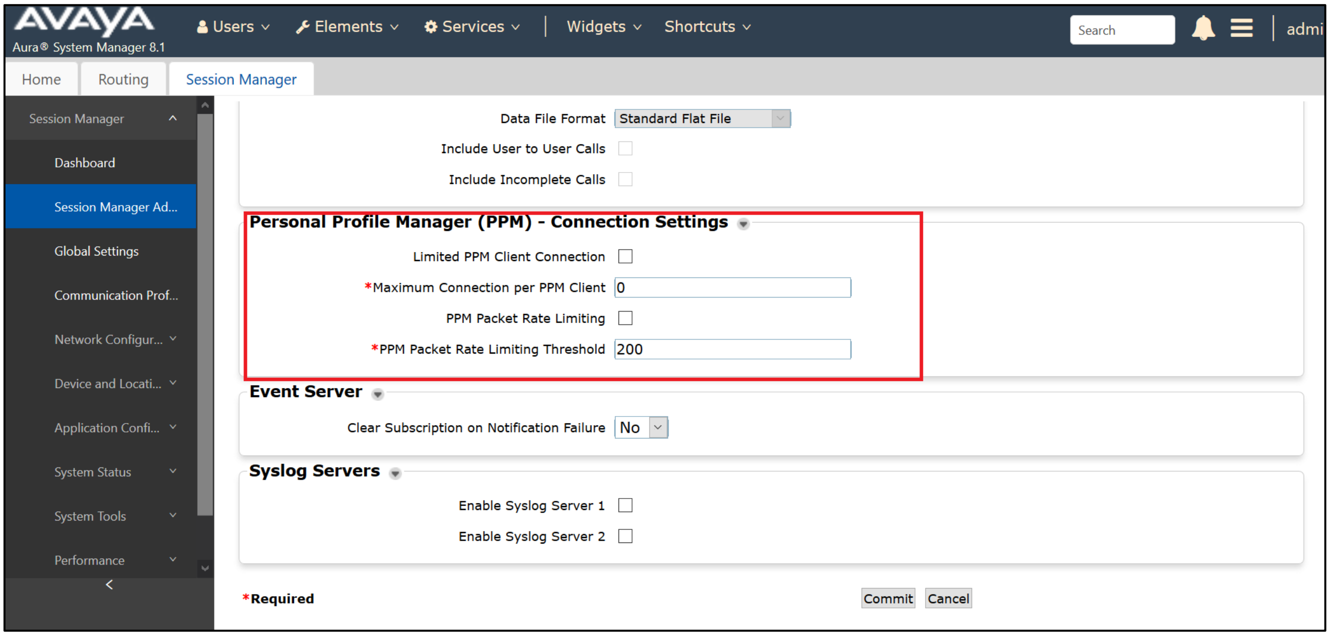
Session Manager Instances

New | View | Edit | Delete

1 Item — Filter: Enable

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

Select : None



Data File Format: Standard Flat File

Include User to User Calls □

Include Incomplete Calls □

Personal Profile Manager (PPM) - Connection Settings

Limited PPM Client Connection □

*Maximum Connection per PPM Client: 0

PPM Packet Rate Limiting □

*PPM Packet Rate Limiting Threshold: 200

Event Server

Clear Subscription on Notification Failure: No

Syslog Servers

Enable Syslog Server 1 □

Enable Syslog Server 2 □

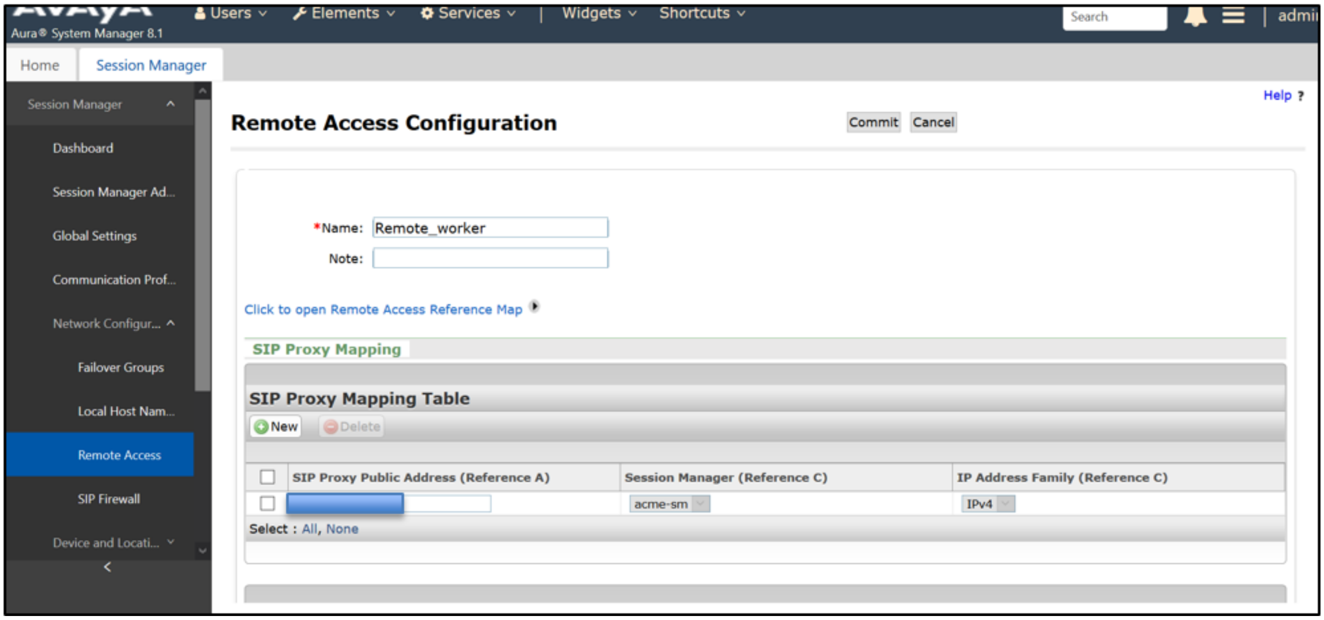
*Required

Commit | Cancel

4.5. 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, 10.232.50.75 is given in this example.
- Click Commit to save the configuration.



Remote Access Configuration

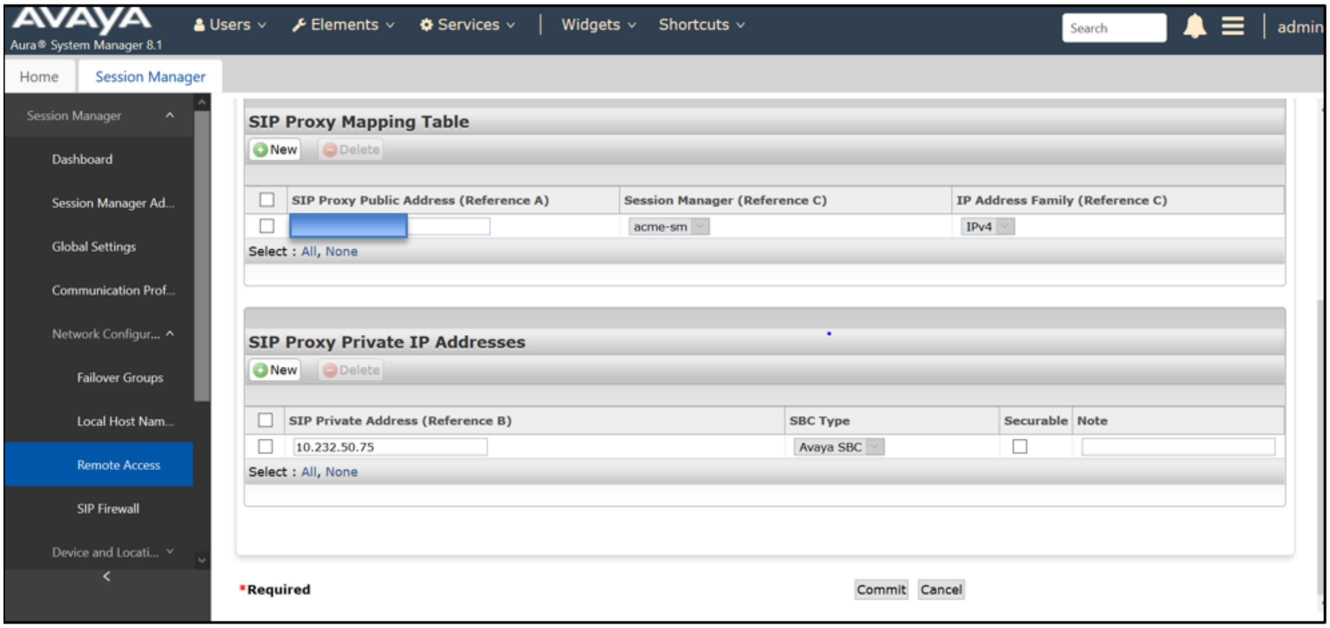
*Name: Remote_worker

Note:

SIP Proxy Mapping

SIP Proxy Mapping Table

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



SIP Proxy Mapping Table

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

SIP Proxy Private IP Addresses

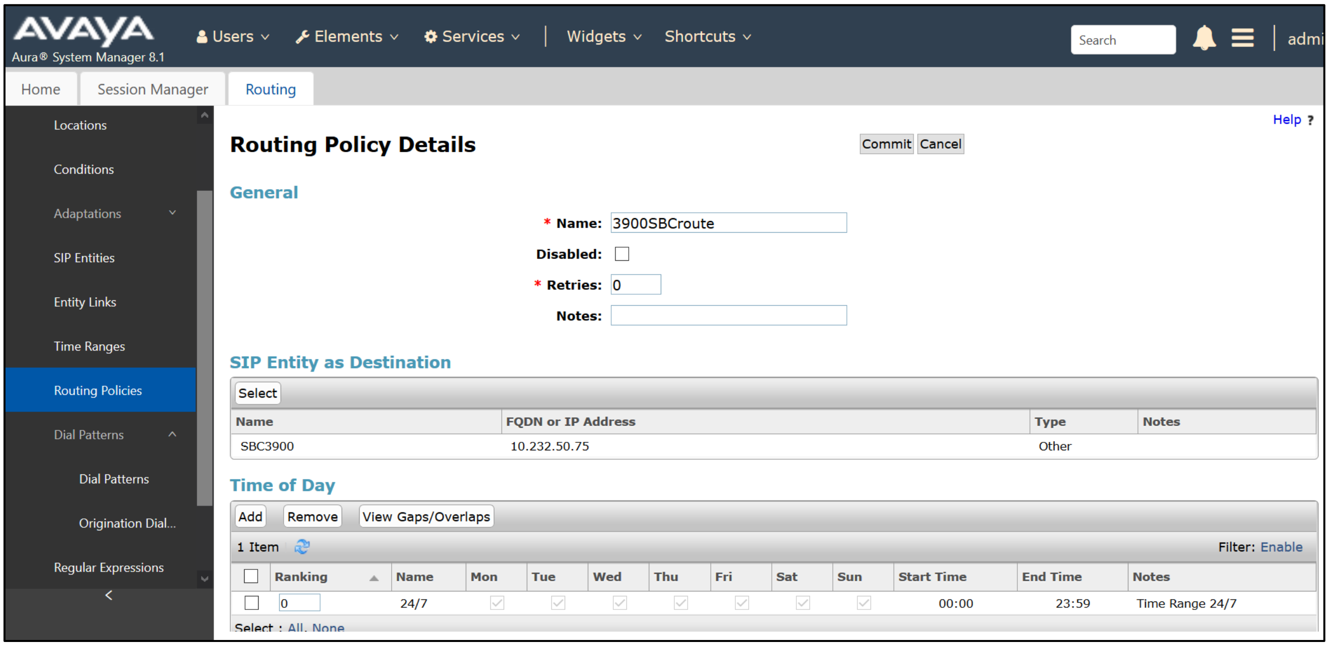
□	SIP Private Address (Reference B)	SBC Type	Securable	Note
□	10.232.50.75	Avaya SBC	□	

*Required

4.6. Adding Routing Policies

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

- Set Name: 3900SBCroute (example in this configuration)
- Set Retries : Default value is 0, can be used as same value
- Select SIP Entity as Destination: Select SBC3900 which was previously configured.
- Click Commit to save the configuration



Routing Policy Details

General

* Name:	3900SBCroute
Disabled:	□
* Retries:	0
Notes:	

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SBC3900	10.232.50.75	Other	

Time of Day

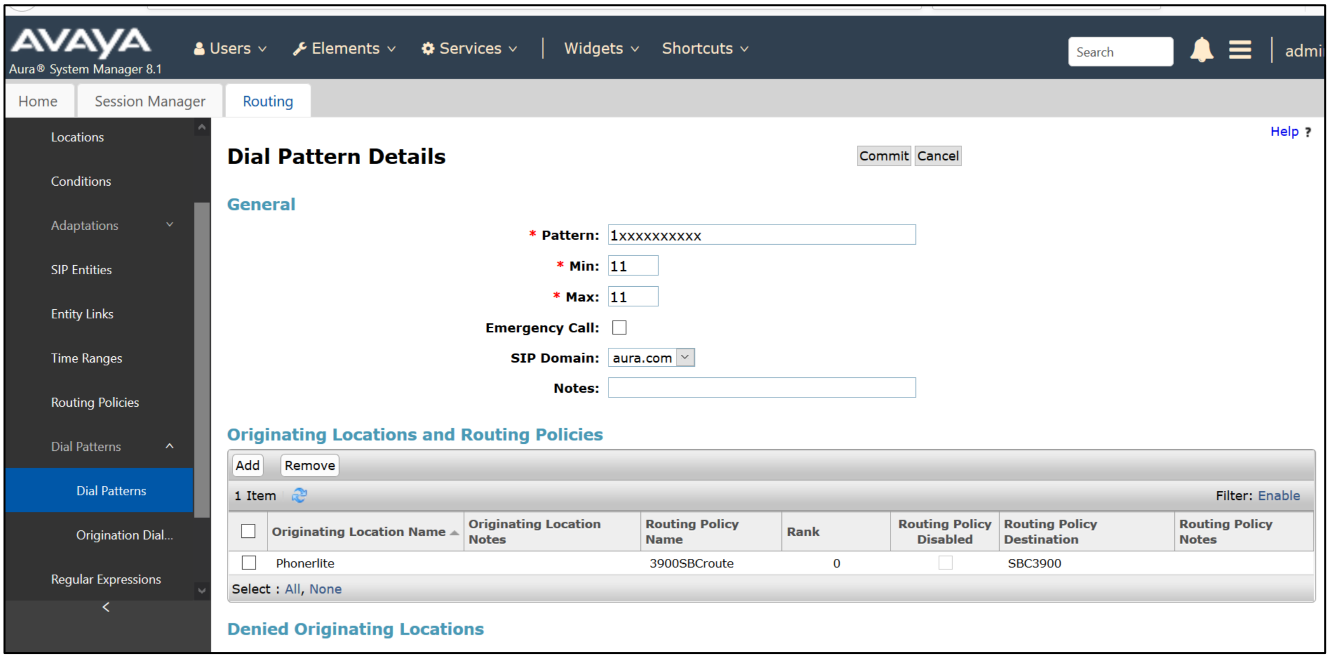
1 Item

□	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

4.7. 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.



Dial Pattern Details

General

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

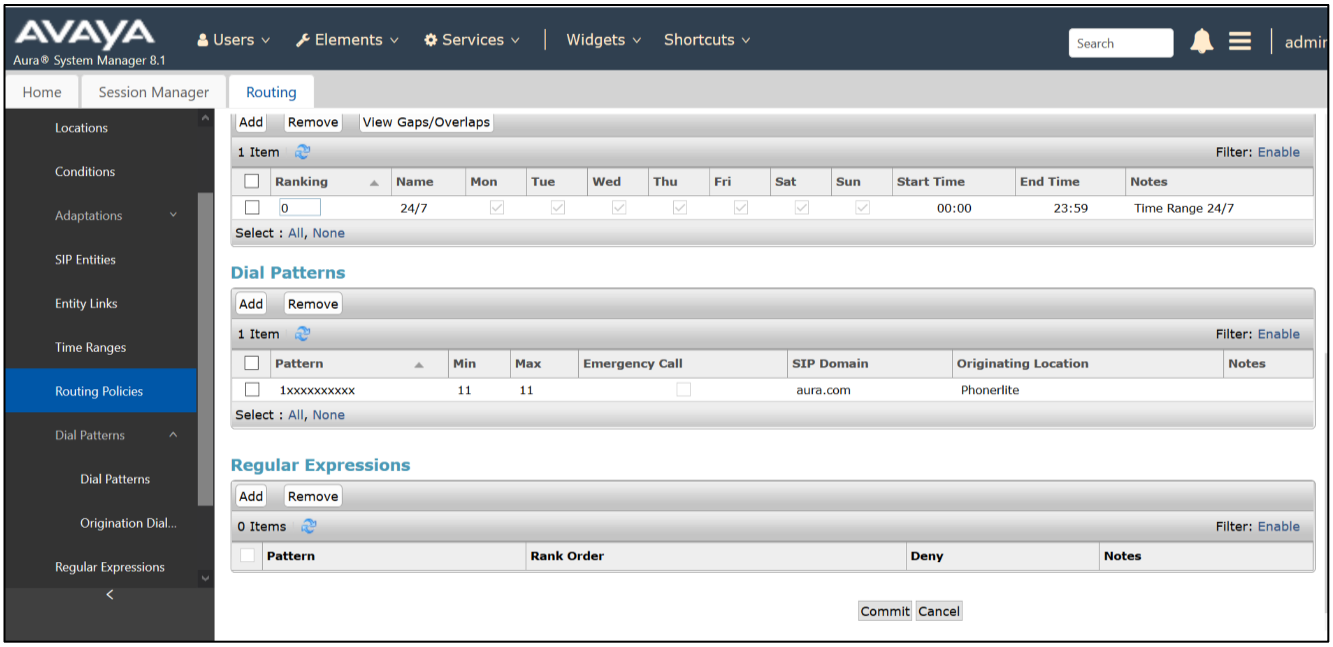
Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	Phonerlite		3900SBCroute	0	□	SBC3900	

Denied Originating Locations

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

1 Item

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

Regular Expressions

0 Items

□	Pattern	Rank Order	Deny	Notes

4.8. Adding Users to Avaya Session Manager.

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

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

- Set Last Name: User1(example in this configuration)
- Set First Name: Avaya (example in this configuration)
- Set Login Name: 17814437246@aura.com (example in this configuration)

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

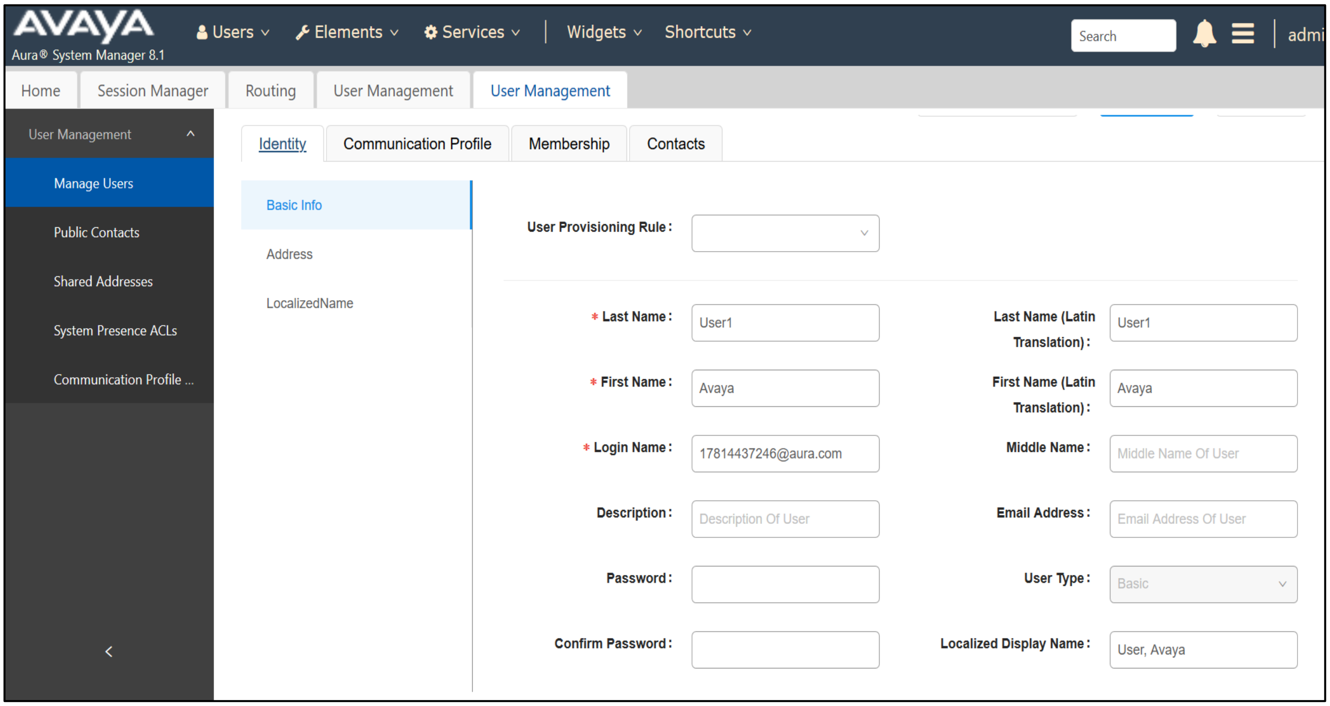
- Set Comm-Profile Password: any password (Numbers or alphabets or alphanumeric)
- Re-enter Comm-Profile Password: Type the password again for confirmation.

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

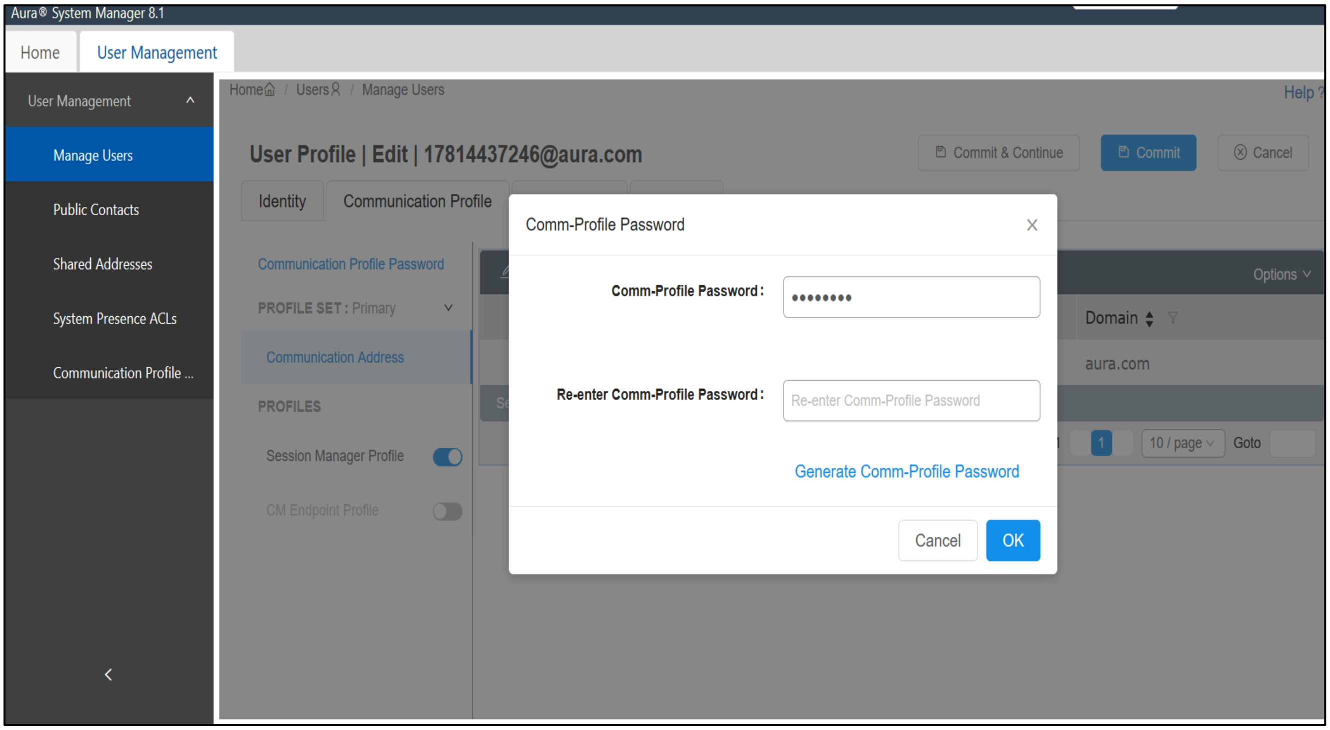
- Set Type: Avaya SIP
- Set Fully Qualified Address: Type the Directory number @domain.com
  17814437246@aura.com

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 Provisioning Rule :			
* Last Name :	User1	Last Name (Latin Translation) :	User1
* First Name :	Avaya	First Name (Latin Translation) :	Avaya
* Login Name :	17814437246@aura.com	Middle Name :	Middle Name Of User
Description :	Description Of User	Email Address :	Email Address Of User
Password :		User Type :	Basic
Confirm Password :		Localized Display Name :	User, Avaya

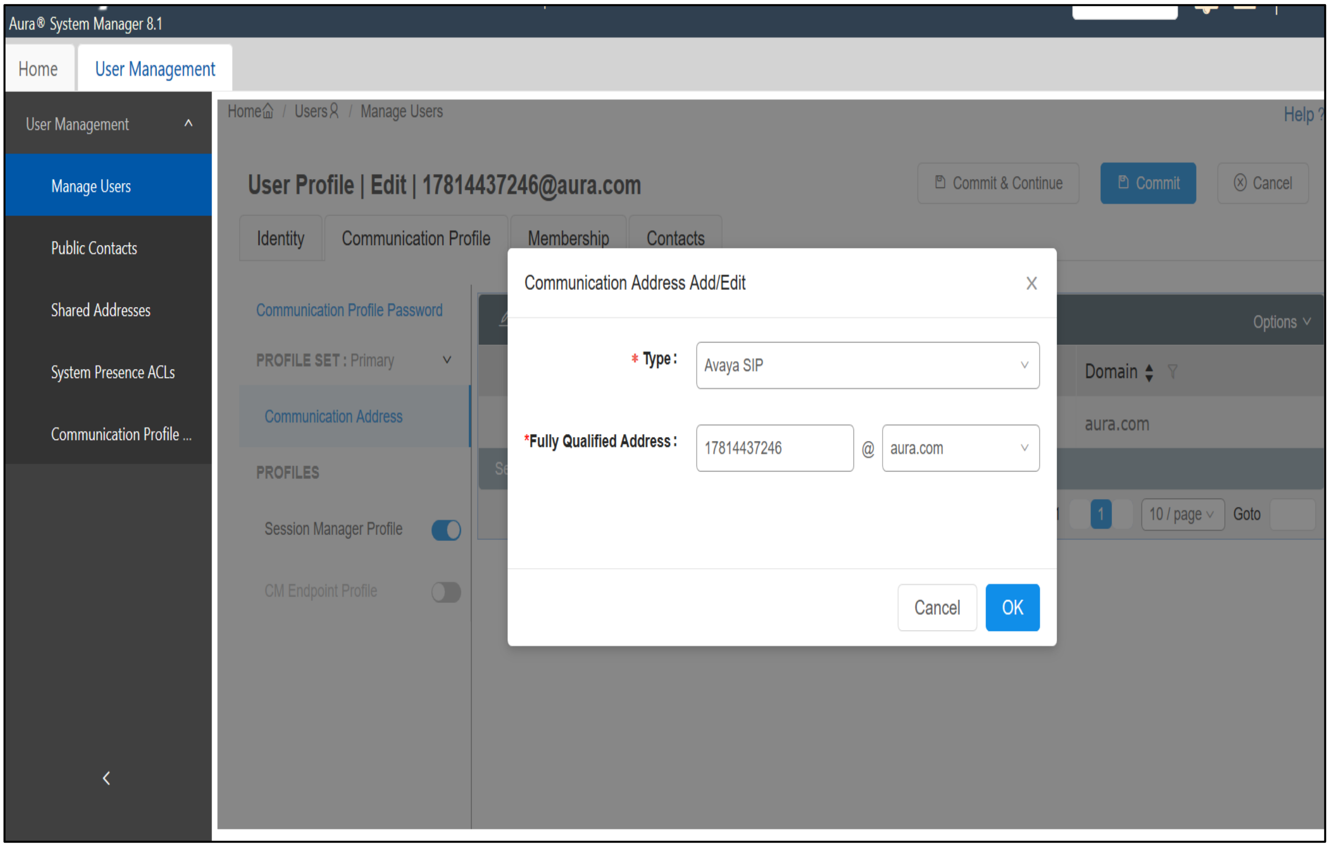


User Profile | Edit | 17814437246@aura.com

Comm-Profile Password

Comm-Profile Password : ••••••••

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

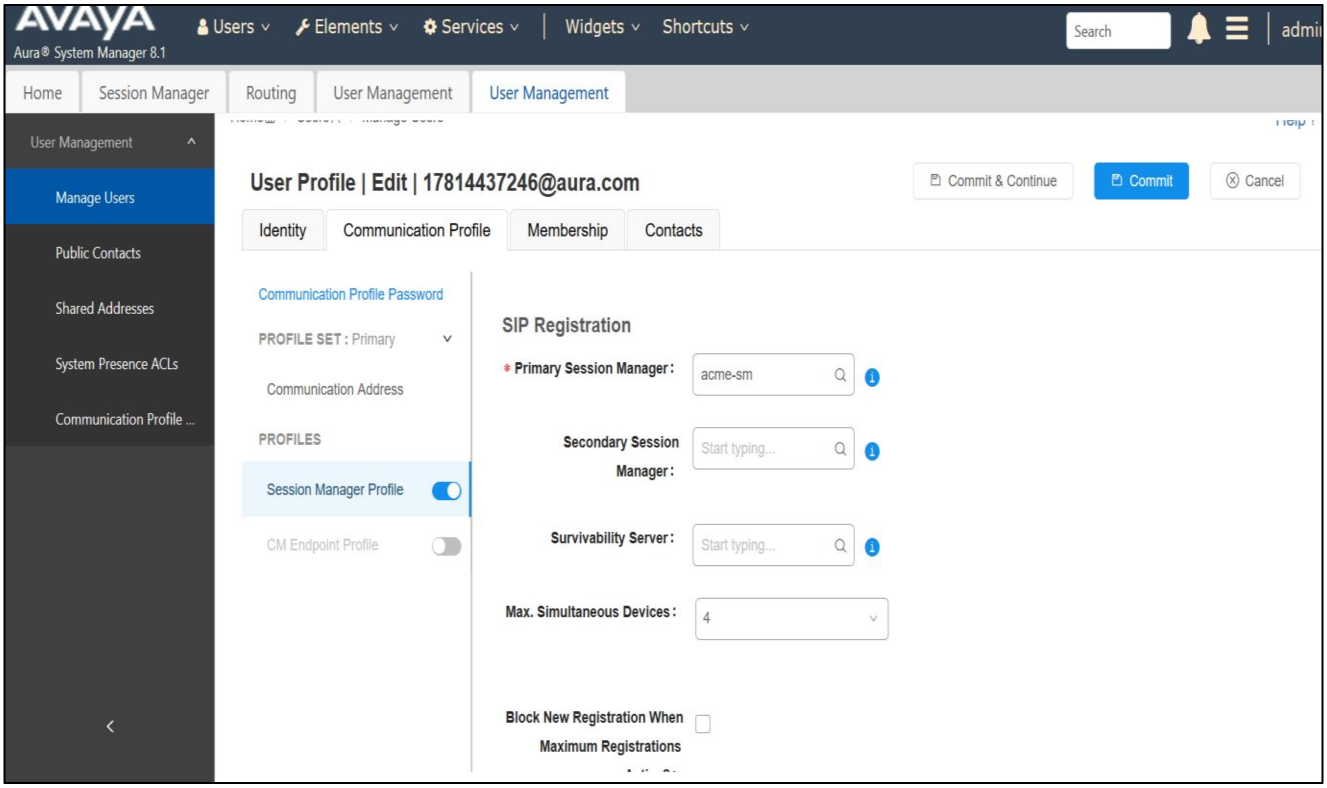


User Profile | Edit | 17814437246@aura.com

Communication Address Add/Edit

* Type : Avaya SIP

*Fully Qualified Address : 17814437246 @ aura.com



User Profile | Edit | 17814437246@aura.com

PROFILE SET : Primary

SIP Registration

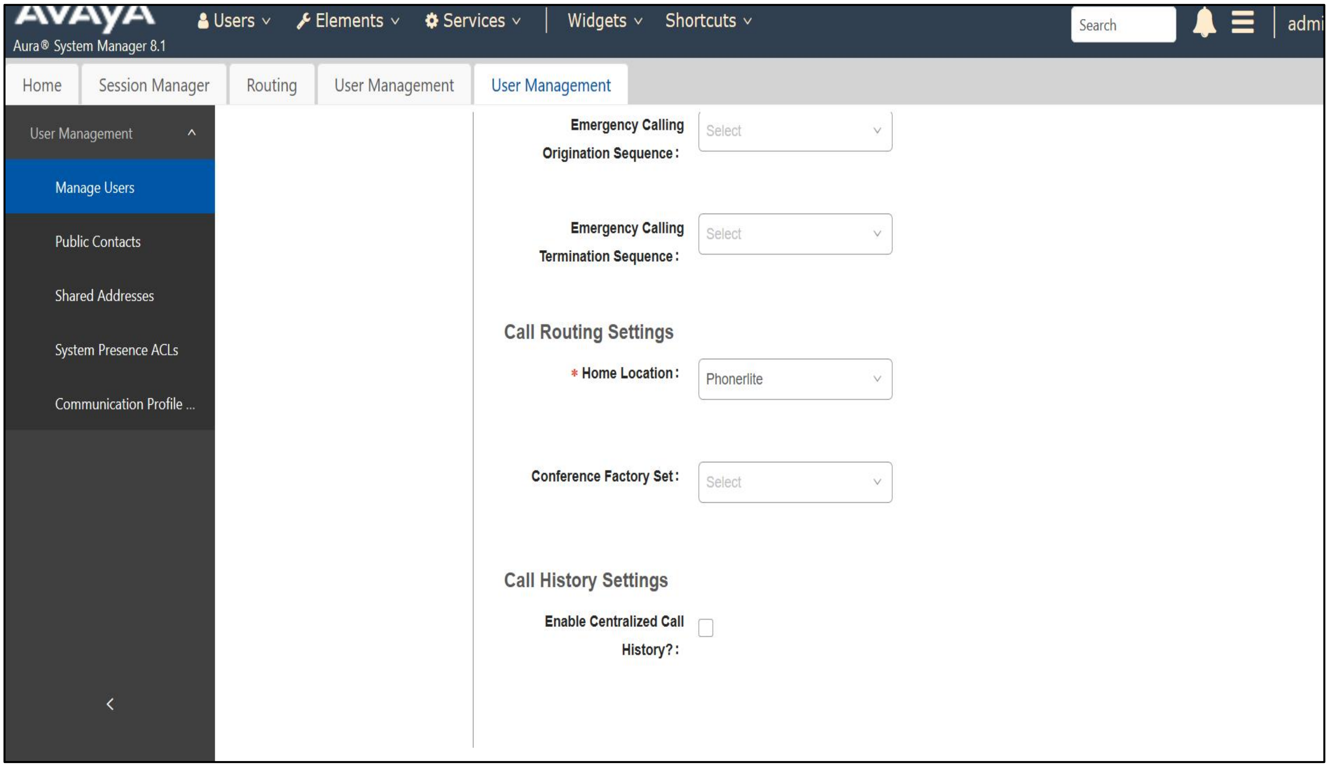
* Primary Session Manager : acme-sm

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.
With this, Avaya Session Manager Configuration is complete.

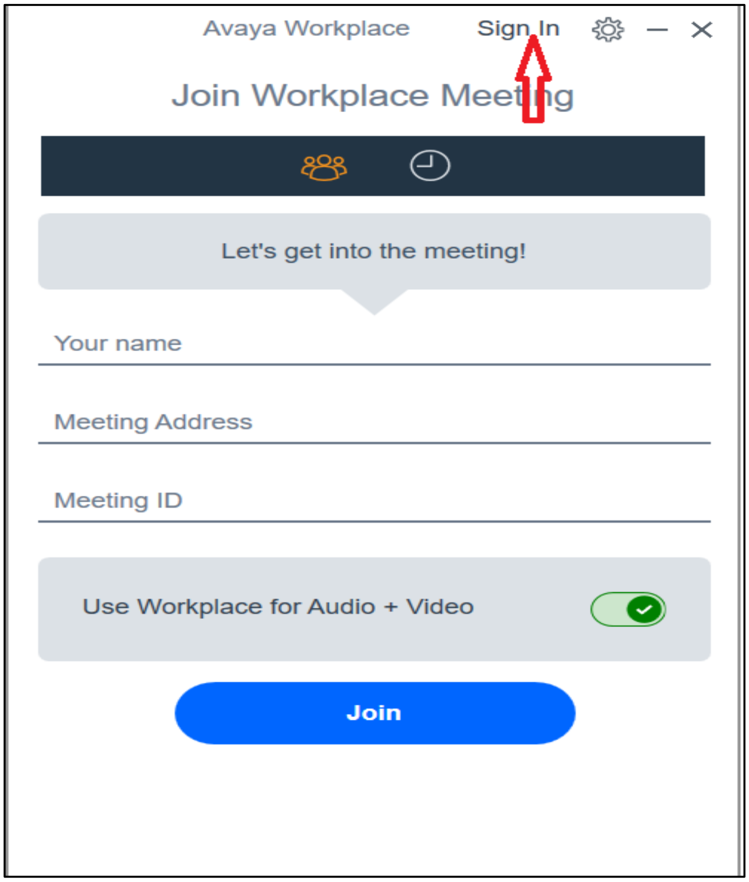
5. Configuring the Avaya Workplace soft client for Windows

This section provides step-by-step guidance on how to configure Avaya Workplace soft client to work with Oracle SBC. As we are configuring the client to work in Manual mode, we have to perform the following steps.

5.1. Turn ON the Manual mode

As a first step, please turn on the manual mode of the client by doing following steps.

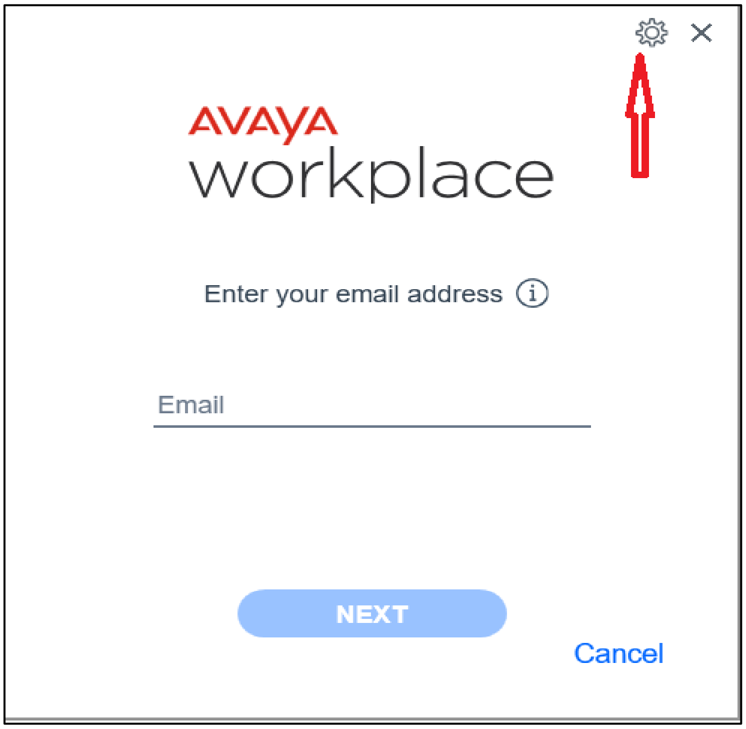
1) Please select the Sign in option when the client opens for the first time.
2) The client then gives the screen for automatic login and please select settings icon on top of the screen.
3) Select manually configure (Expert Mode) to enter the Manual mode option.



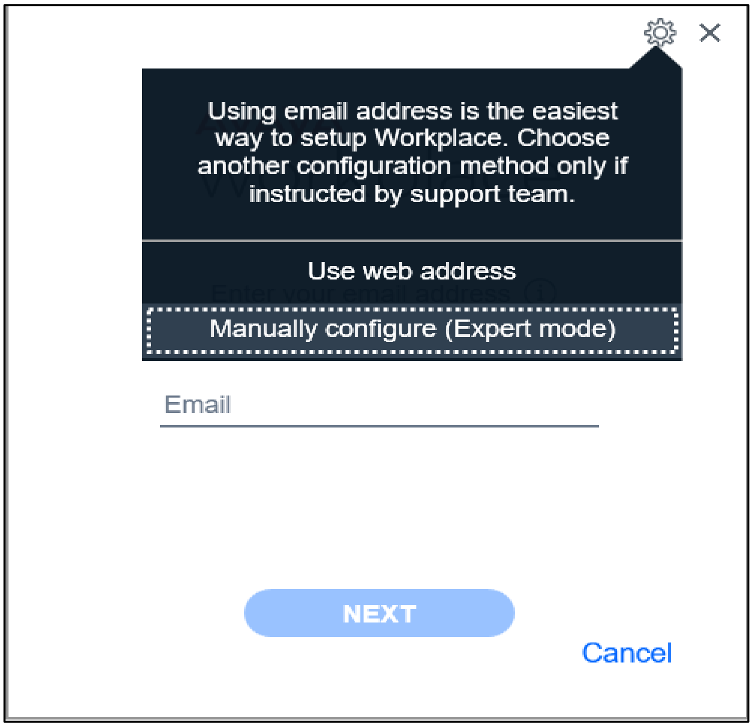
Avaya Workplace

Join Workplace Meeting

Let's get into the meeting!



Enter your email address ⓘ

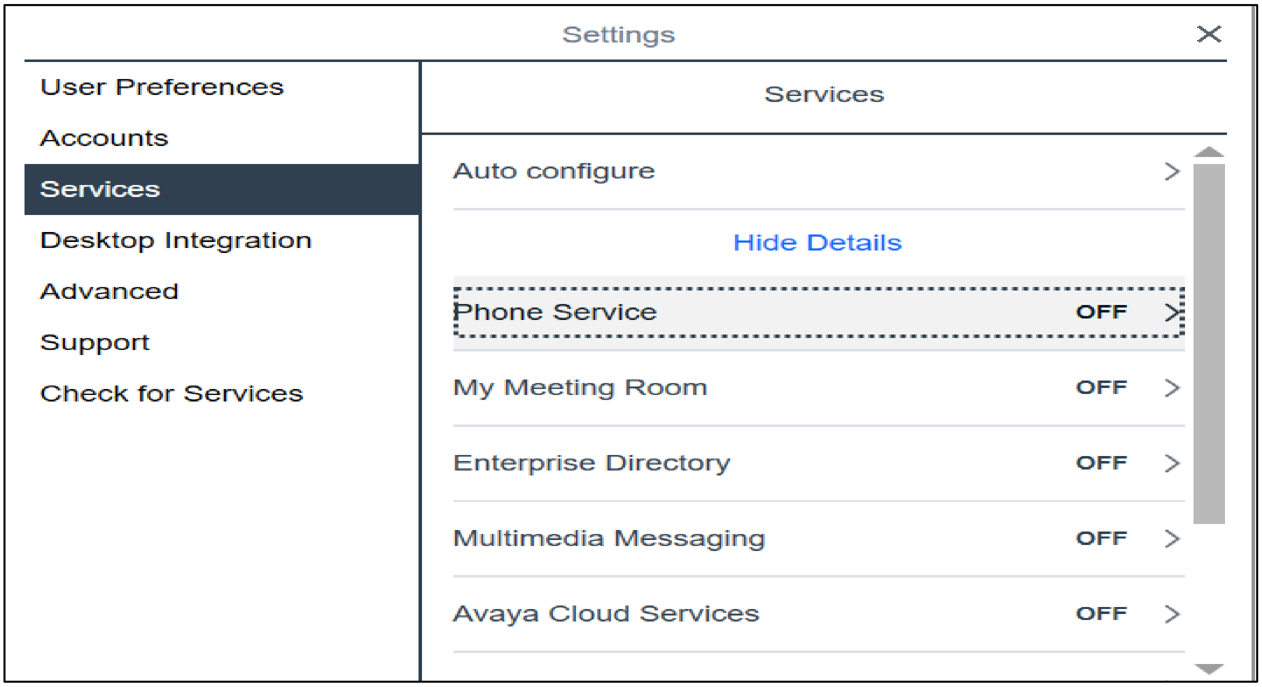


Using email address is the easiest way to setup Workplace. Choose another configuration method only if instructed by support team.

5.2. Configure Manual mode for the client

Once we select Manual Mode, the client opens the screen to enter the configuration.

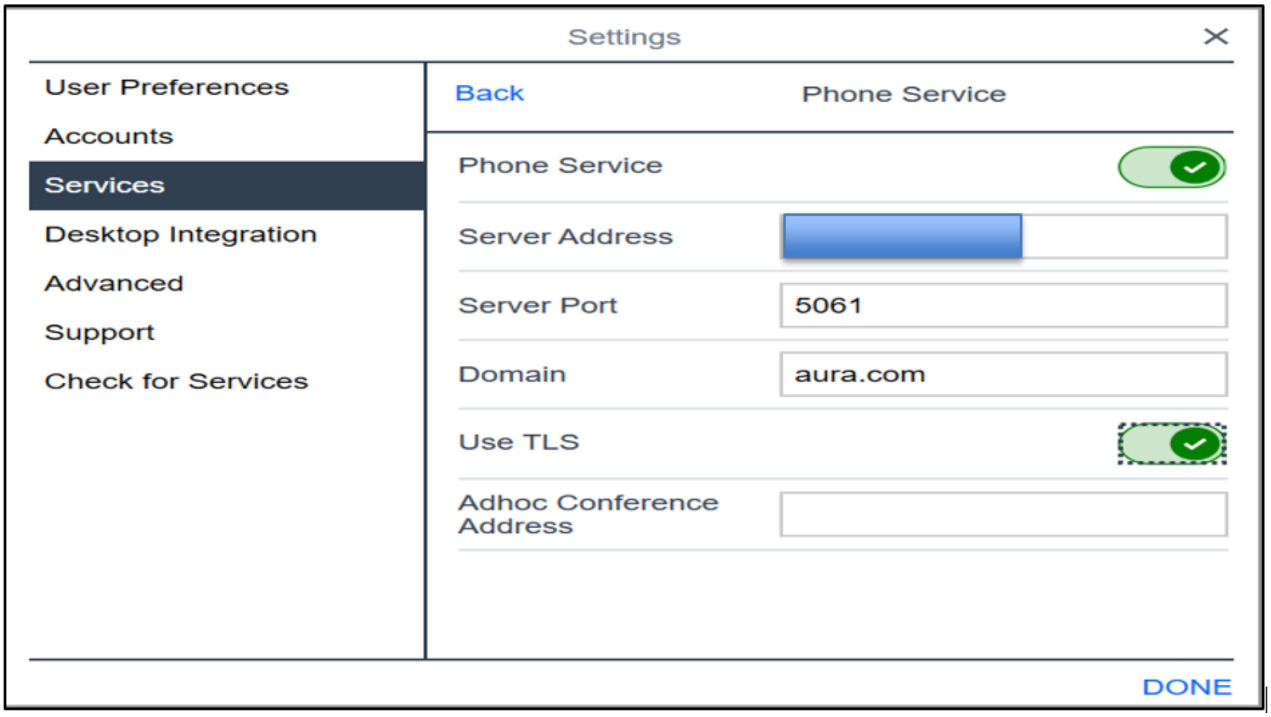
1) Please select Services ----- Phone services --- ON.
2) Please enter SBC public interface IP, Domain given in Avaya SM and the Server port and then enable TLS as transport protocol. Click Done to save the changes made.



Settings

Services

- Auto configure
- Hide Details
- Phone Service OFF
- My Meeting Room OFF
- Enterprise Directory OFF
- Multimedia Messaging OFF
- Avaya Cloud Services OFF



Settings

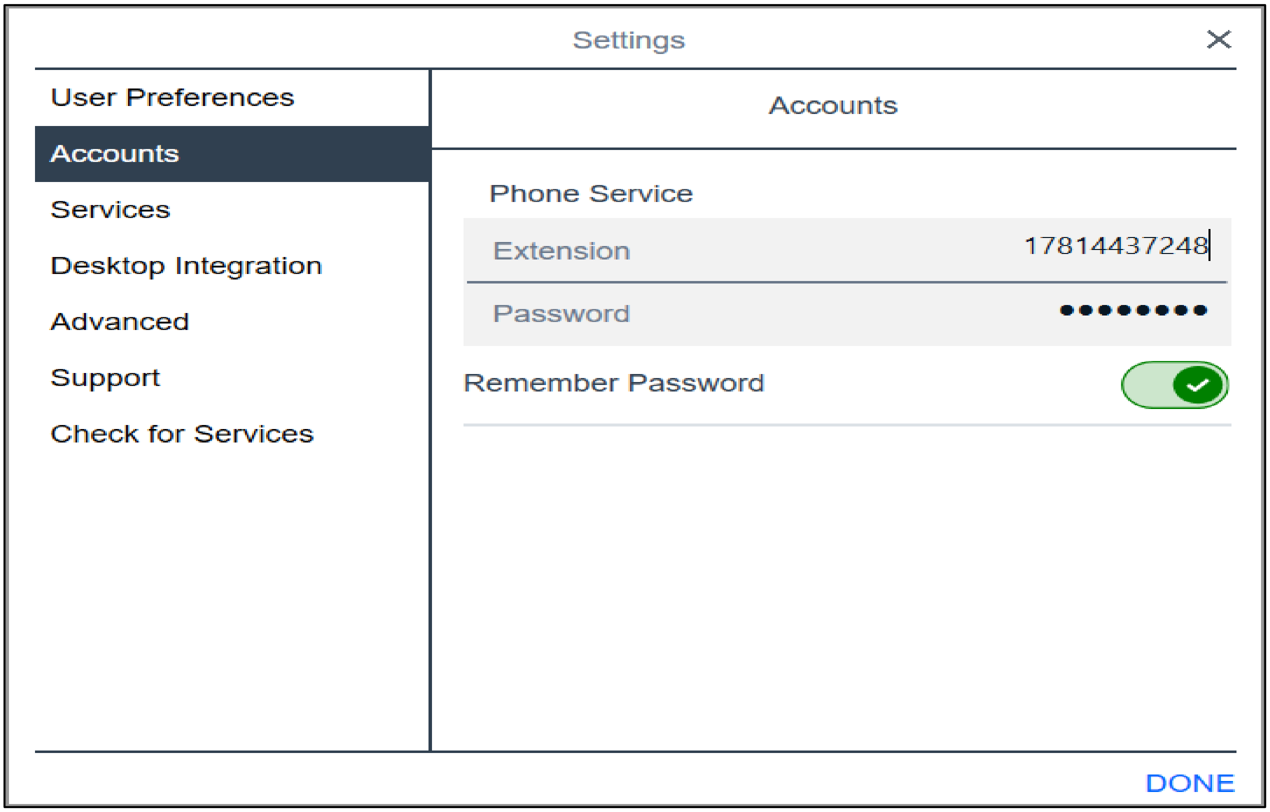
Phone Service

Phone Service	✓
Server Address	[redacted]
Server Port	5061
Domain	aura.com
Use TLS	✓
Adhoc Conference Address	

5.3. Configure the Directory Number for the Workspace client

Once we enable the phone services, please assign the directory number to the client (we can use one of the directory numbers that we created under users in Avaya Session Manager)

1) Please select Accounts ----- Extension --- Give the directory number created
2) Under Password ---- Enter the password for the directory number.
3) Enable Remember password if you want client to save the password
4) Click Done to save the changes.



Phone Service

Extension 17814437248

Password •••••••••

Remember Password ✓

With this, Avaya workplace client configuration is complete for the Manual Mode.

6. Configuring the SBC

This section provides step-by-step guidance on how to configure Oracle SBC for interworking with Avaya Session Manager for registering Avaya Workspace client and for making calls from Avaya Workspace client soft phones to other phones registered to the Avaya Session Manager 8.1

6.1. Validated Oracle SBC version

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

- AP 1100
- AP 3900
- AP 4600
- AP 6350
- AP 6300
- VME

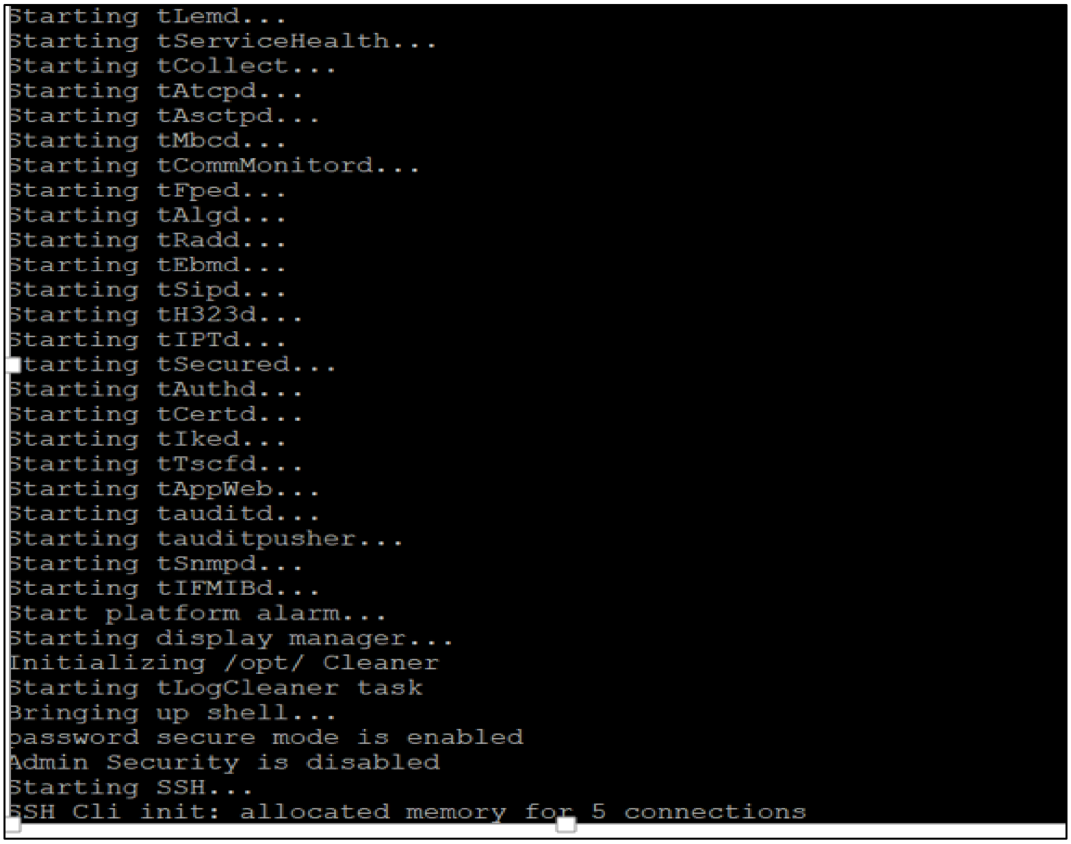
7. New SBC configuration

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

7.1. Establishing a serial connection to the SBC

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

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

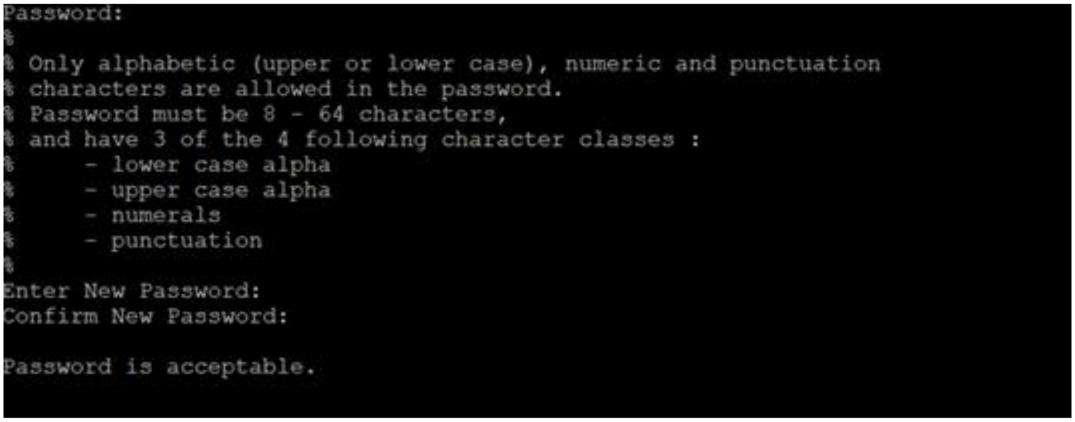


```
Starting tLemd...
Starting tServiceHealth...
Starting tCollect...
Starting tAtcpd...
Starting tAsctpd...
Starting tMbcd...
Starting tCommMonitord...
Starting tFped...
Starting tAlgd...
Starting tRadd...
Starting tEbmd...
Starting tSipd...
Starting tH323d...
Starting tIPTd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tTscfd...
Starting tAppWeb...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Starting tIFMIBd...
Start platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...
password secure mode is enabled
Admin Security is disabled
Starting SSH...
SSH Cli init: allocated memory for 5 connections
```

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

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

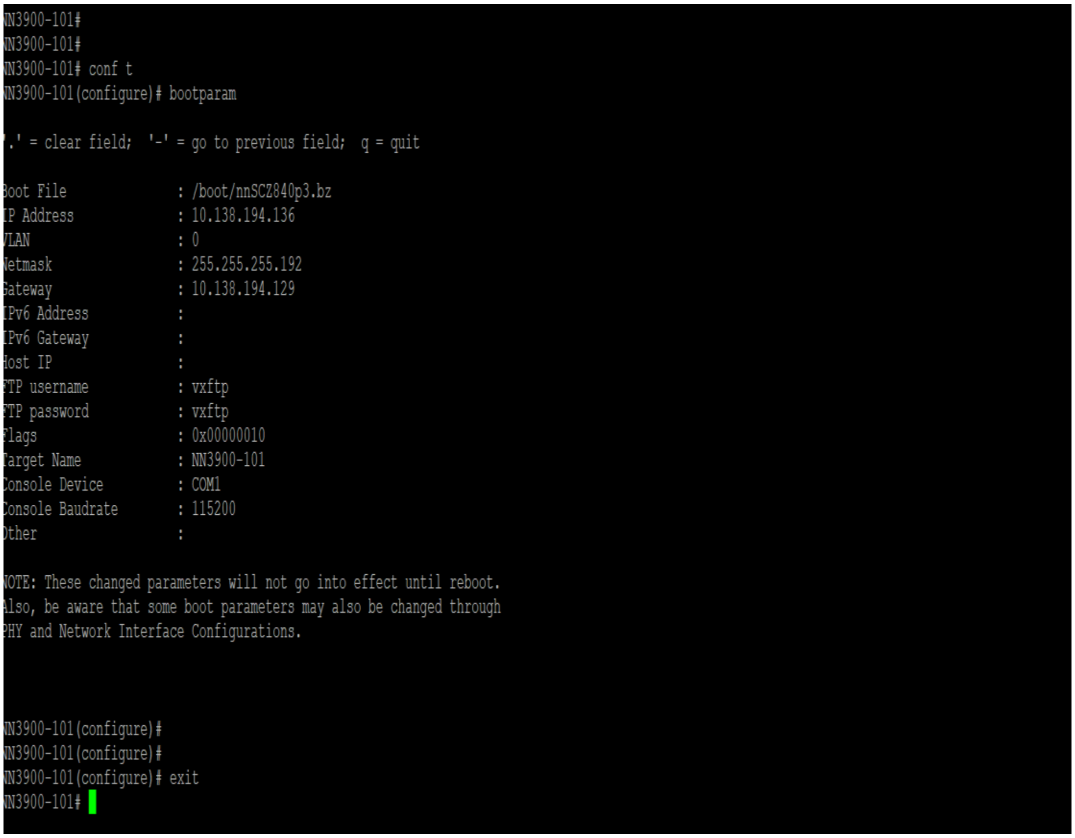
Both passwords have to be changed according to the rules shown below.



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

Password is acceptable.
```

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

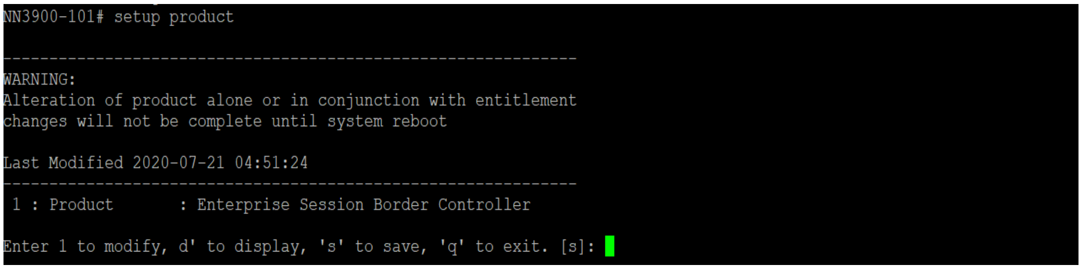
Note: There is no management IP configured by default.



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

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

Boot File              : /boot/nnSCZ840p3.bz
IP Address             : 10.138.194.136
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                  : 0x00000010
Target Name            : NN3900-101
Console Device         : COM1
Console Baudrate       : 115200
Other                  :

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



NN3900-101(configure)#
NN3900-101(configure)#
NN3900-101(configure)# exit
NN3900-101#
```

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

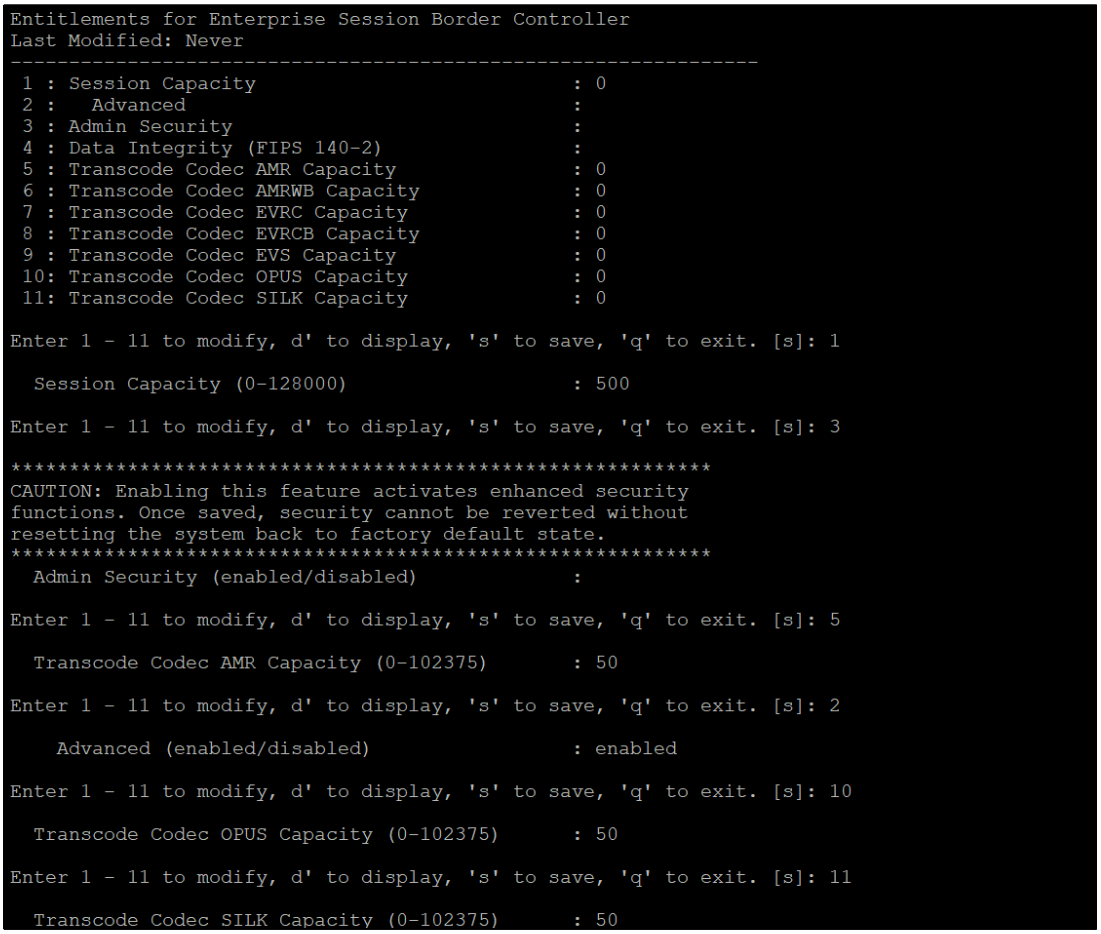
To configure product type, type in setup product in the terminal



```
NN3900-101# setup product

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

Last Modified 2020-07-21 04:51:24
--------------------------------------------------------------
 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.

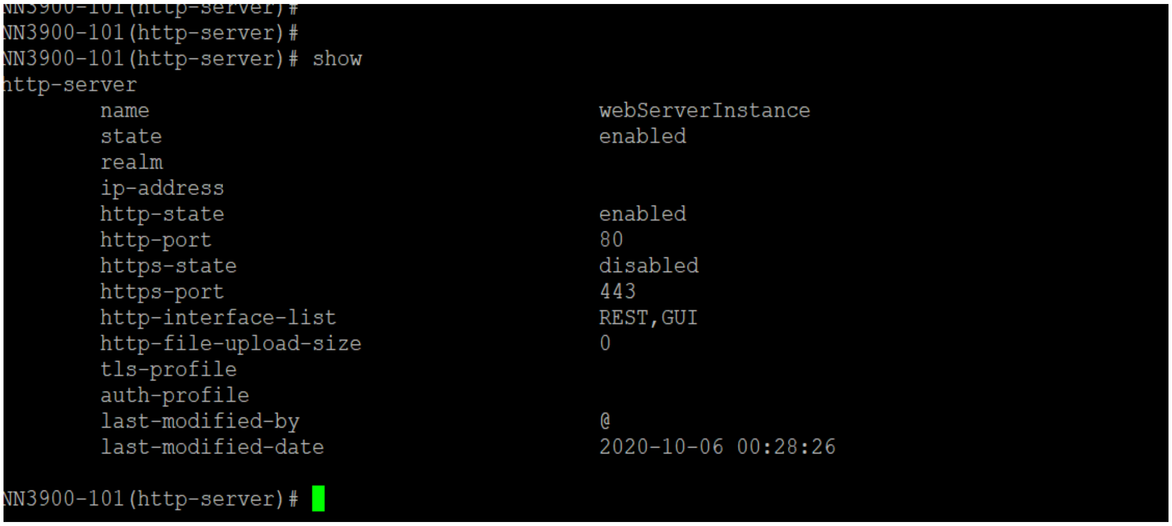


```
Entitlements for Enterprise Session Border Controller
Last Modified: Never
----------------------------------------------------------------
 1 : Session Capacity                             : 0
 2 :   Advanced                                   :
 3 : Admin Security                               :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

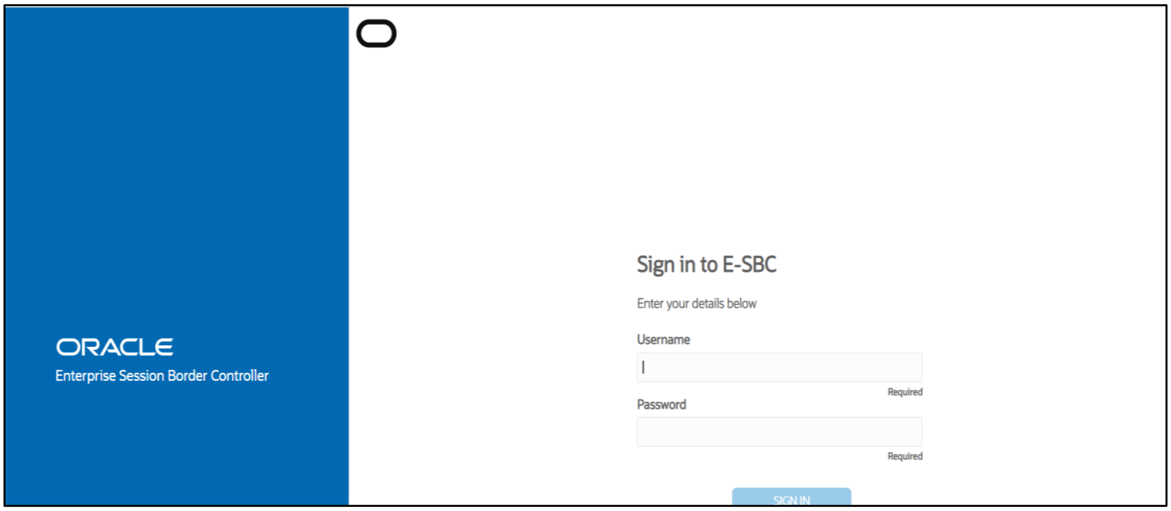


```
NN3900-101(http-server)#
NN3900-101(http-server)#
NN3900-101(http-server)# show
http-server
        name                                       webServerInstance
        state                                      enabled
        realm
        ip-address
        http-state                                 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                         2020-10-06 00:28:26

NN3900-101(http-server)#
```

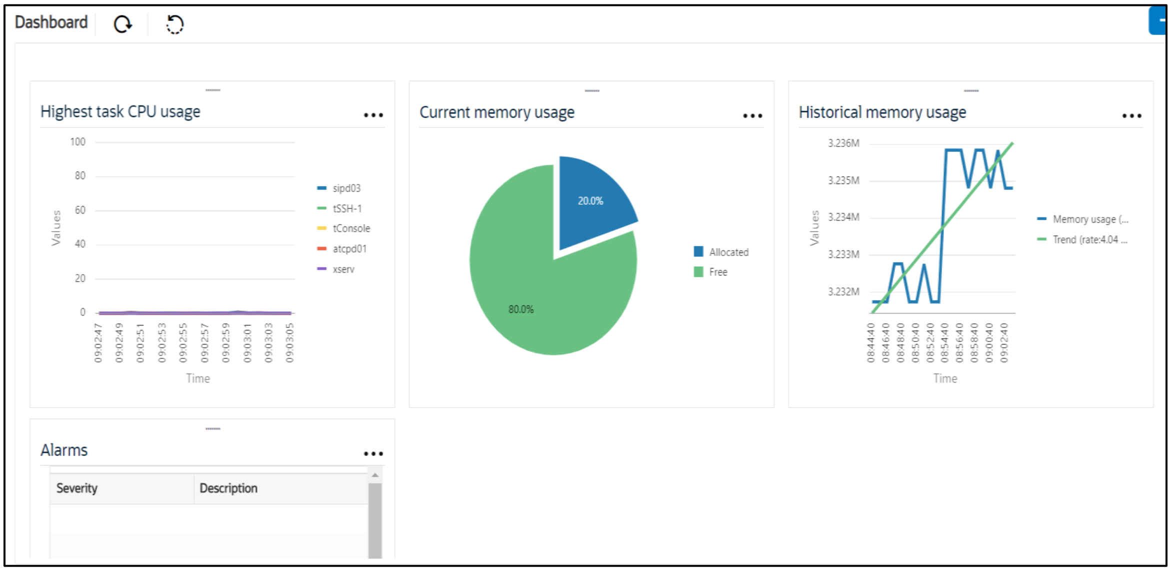
7.2. Configure SBC using Web GUI

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

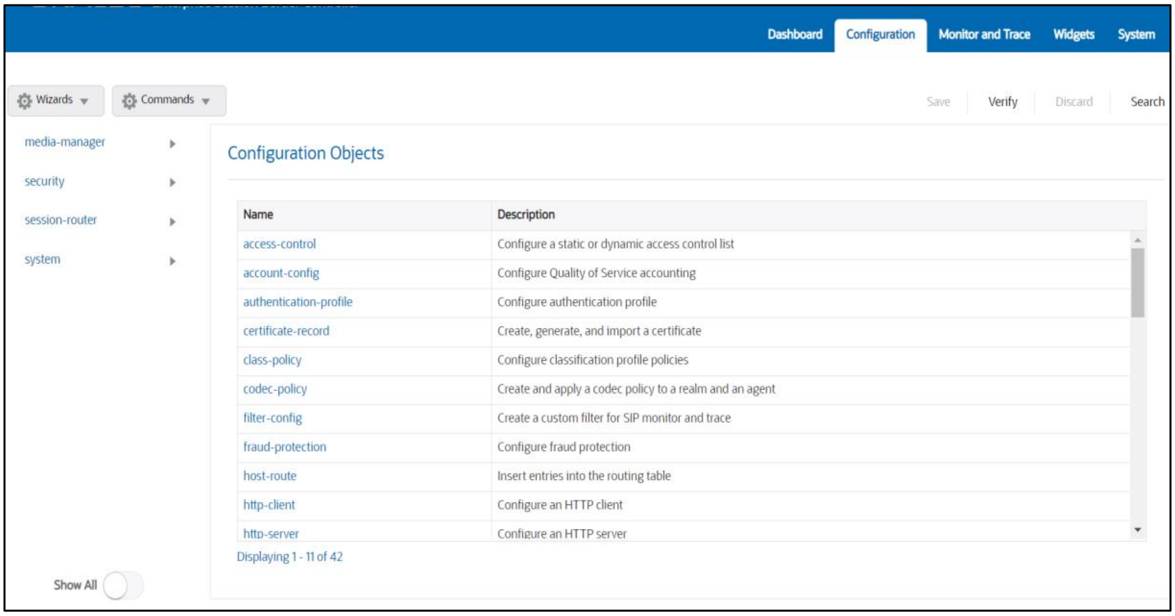
The Web GUI can be accessed through the url http://<SBC_MGMT_IP>.



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.

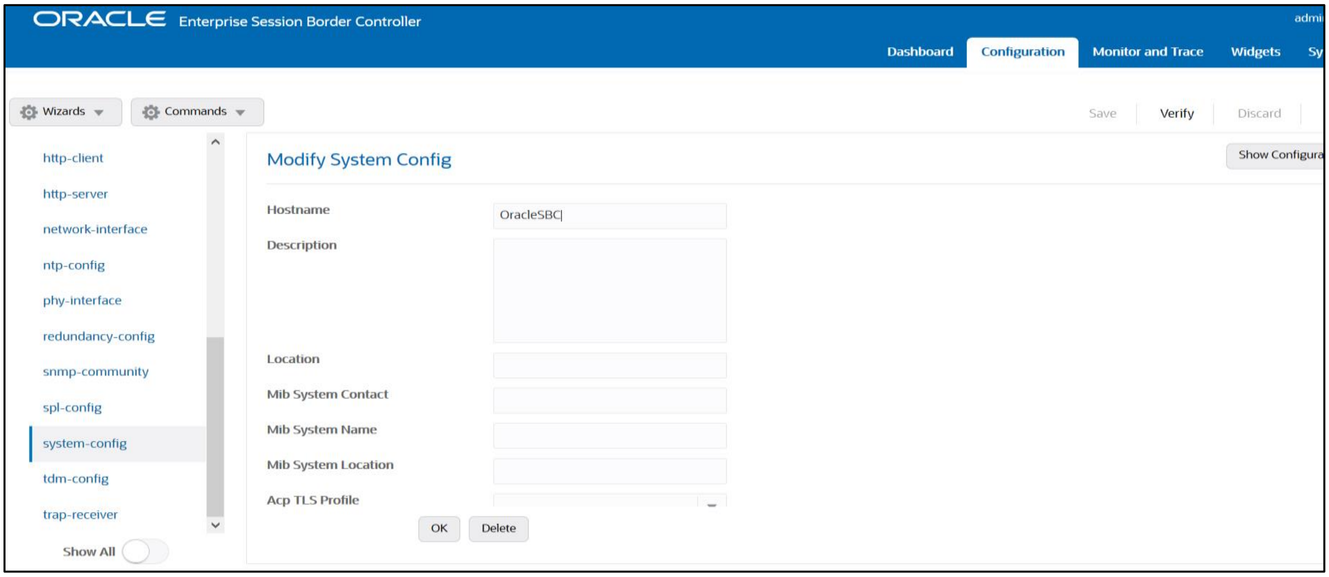
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf

The expert mode is used for configuration.

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

7.3. Configure system-config

Go to system->system-config



Modify System Config

Hostname: OracleSBC|

Description

Location

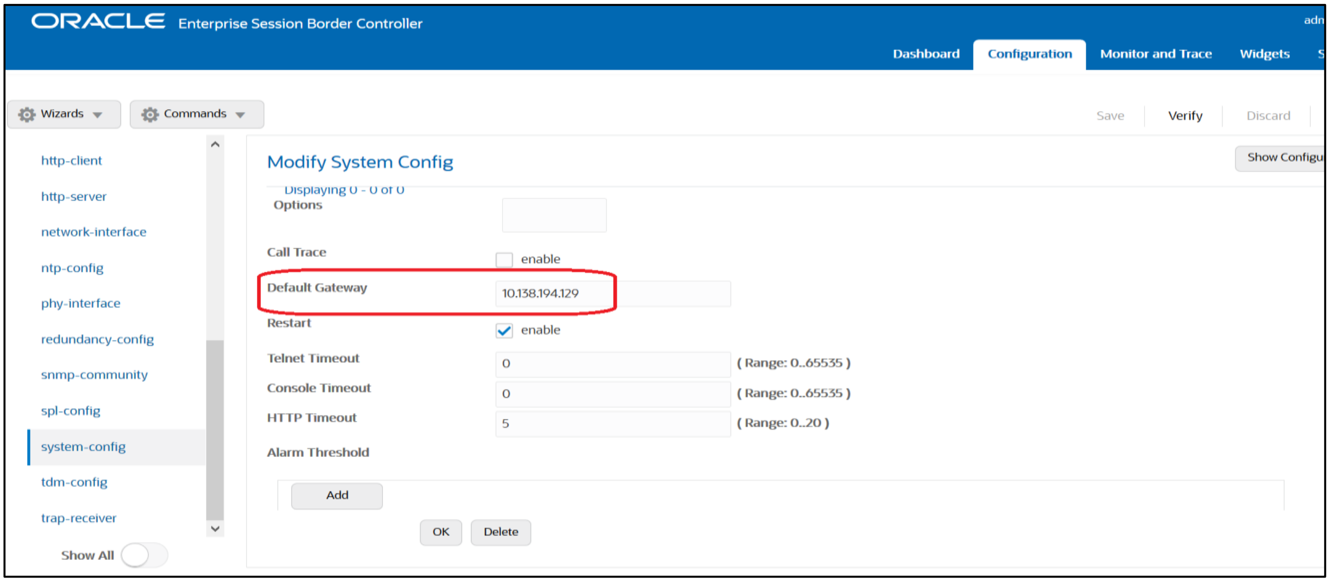
Mib System Contact

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/8.4.0/releasenotes/esbc_scz840_releasenotes.pdf

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

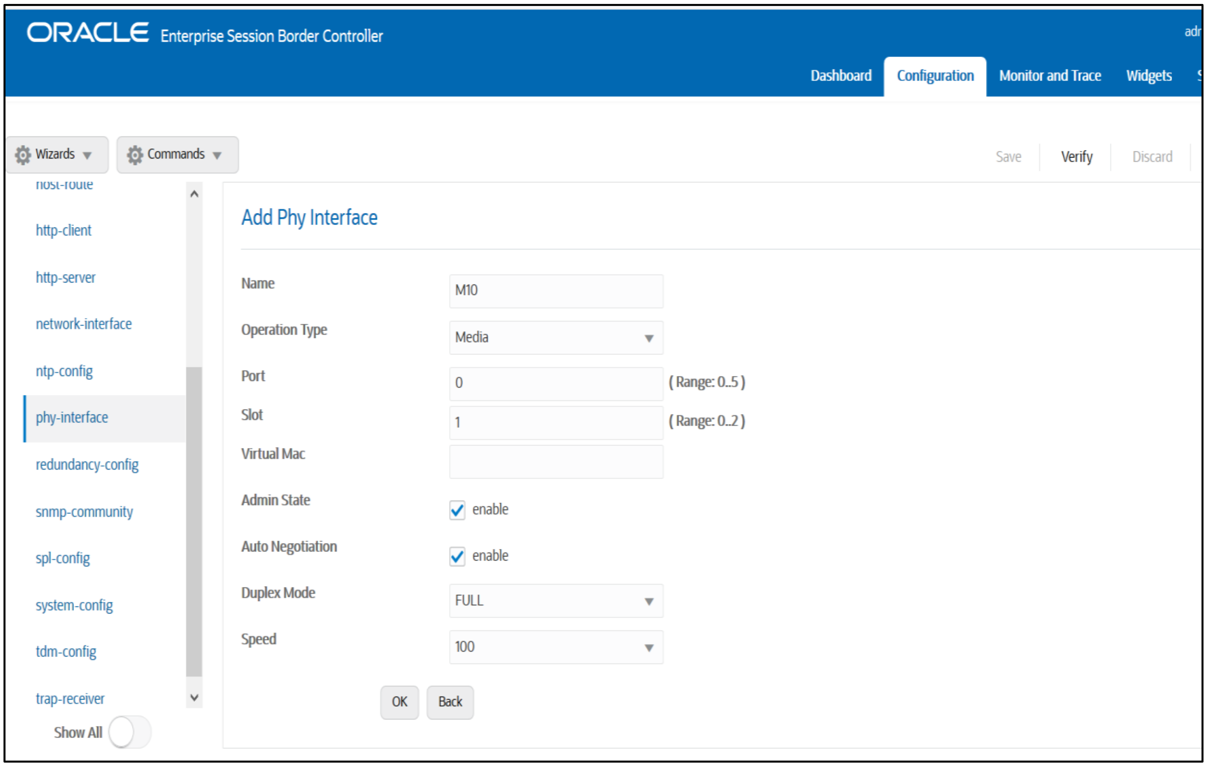
7.4. Configure Physical Interface values

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

You will first configure the slot 0, port 1 interface designated with the name M10.
This will be the port plugged into your (connection to the Avaya Workspace client) public interface.
Avaya Core side side is configured on the slot 1 port 1.

Parameter Name	Avaya Workspace client side (M10)	Avaya Core Side (M11)
Slot	0	1
Port	1	1
Operation Mode	Media	Media

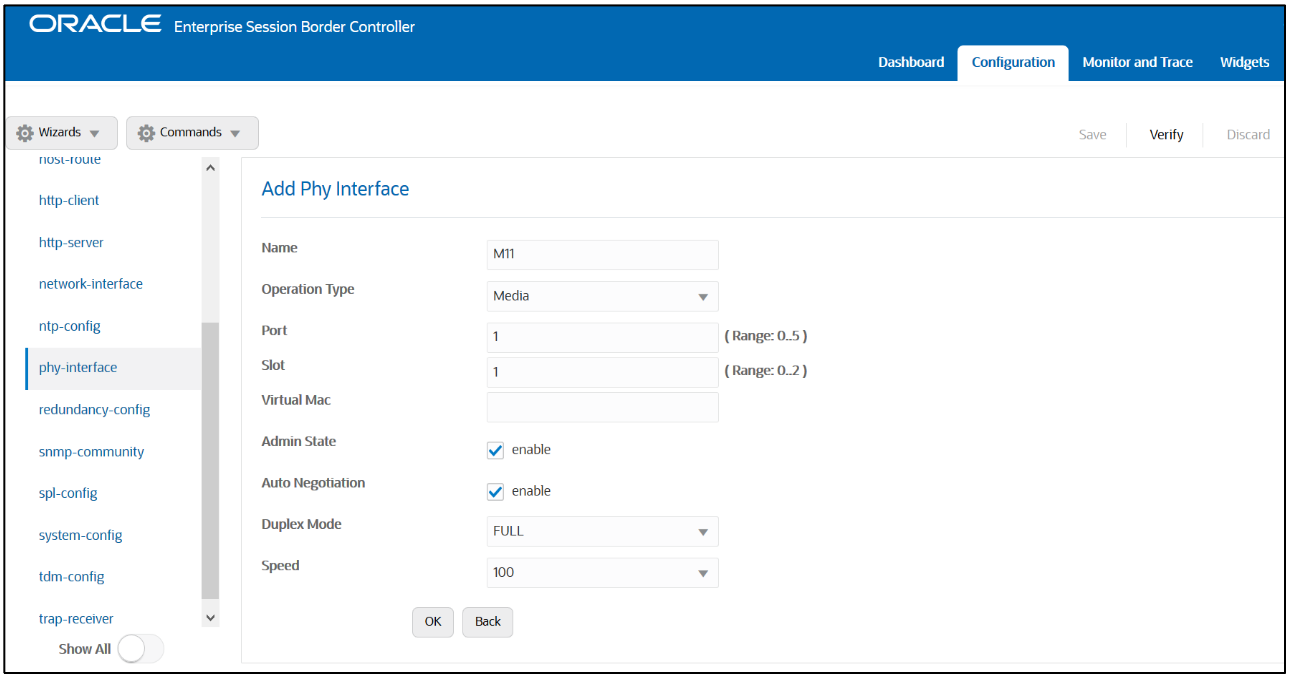
Please configure M10 interface as below.



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

Similarly, configure M11 interface as below.



Add Phy Interface

Name	M11
Operation Type	Media
Port	1 (Range: 0..5)
Slot	1 (Range: 0..2)
Virtual Mac	
Admin State	☑ enable
Auto Negotiation	☑ enable
Duplex Mode	FULL
Speed	100

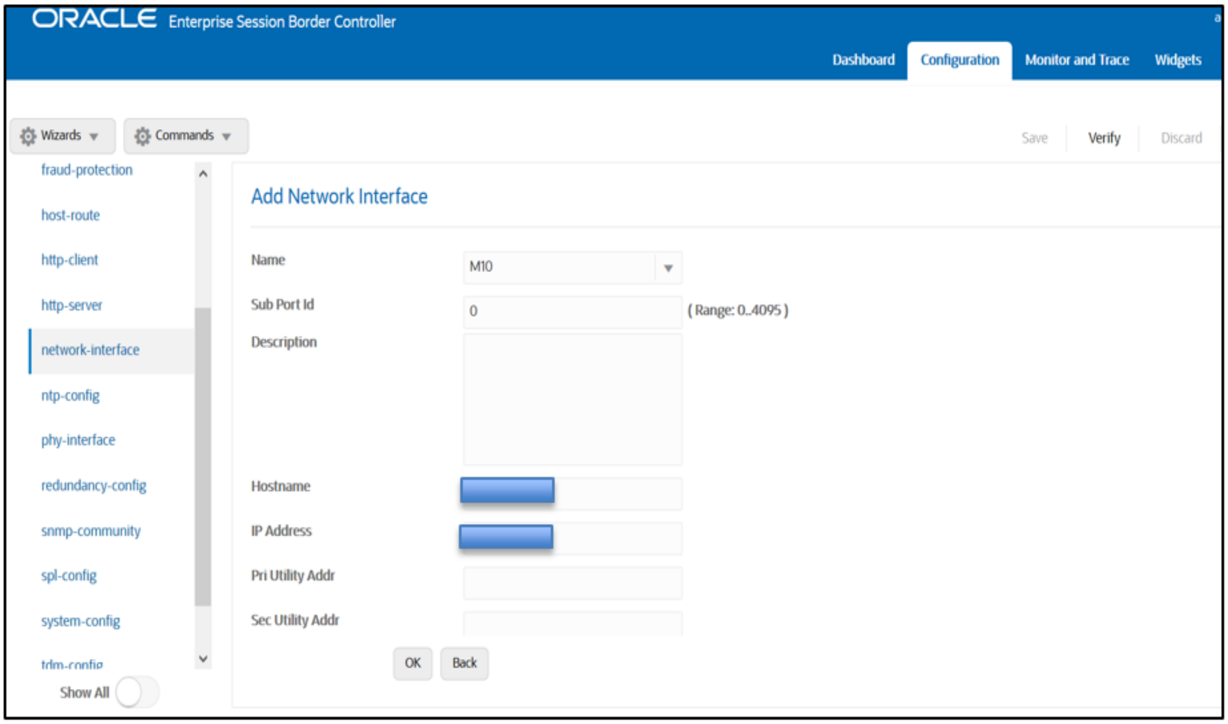
7.5. Configure Network Interface values

To configure network-interface, go to system->Network-Interface. Configure two interfaces, one for Avaya Workspace client side and one for Avaya Core side.

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

Parameter Name	Avaya Workspace client side Network Interface (Avaya Public Interface)	Avaya Core side Network interface (Avaya Core Interface)
Name	M10	M11
Host Name		
IP address	[redacted]	10.232.50.75
Netmask	255.255.255.192	255.255.255.0
Gateway	[redacted]	10.232.50.1

Please configure network interface M10 as below



Add Network Interface

Name: M10

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

Description:

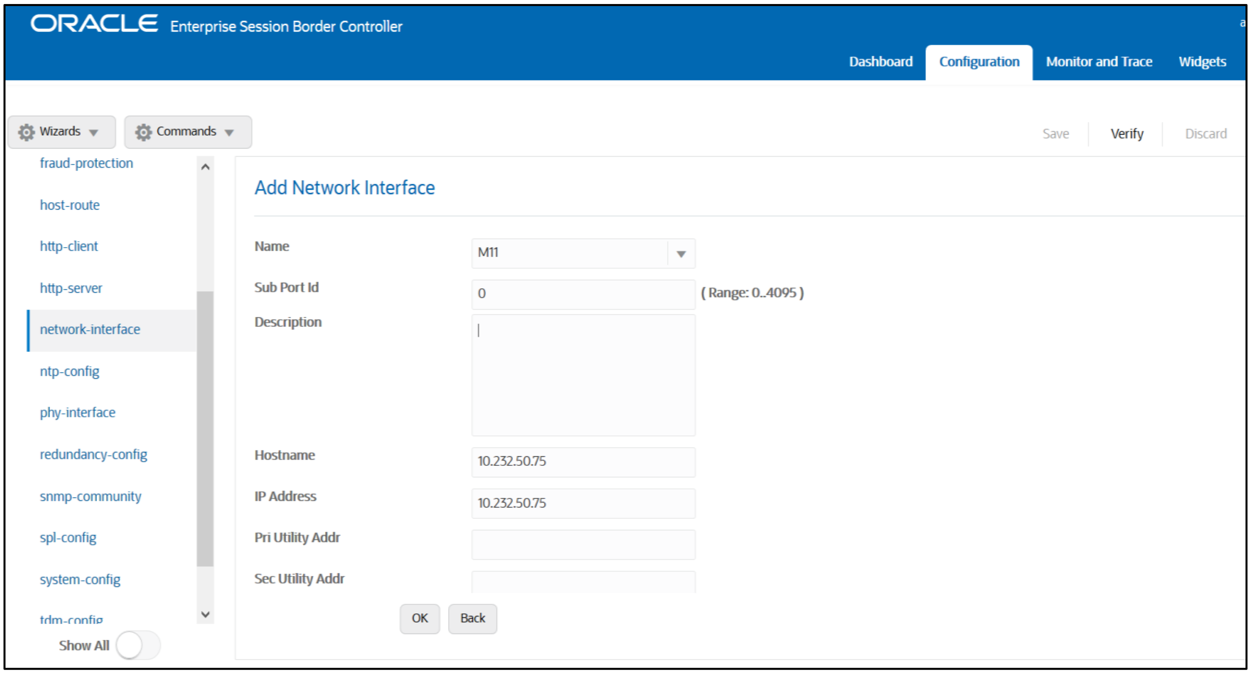
Hostname: [redacted]

IP Address: [redacted]

Pri Utility Addr:

Sec Utility Addr:

Please configure network interface M11as below



Add Network Interface

Name: M11

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

Description:

Hostname: 10.232.50.75

IP Address: 10.232.50.75

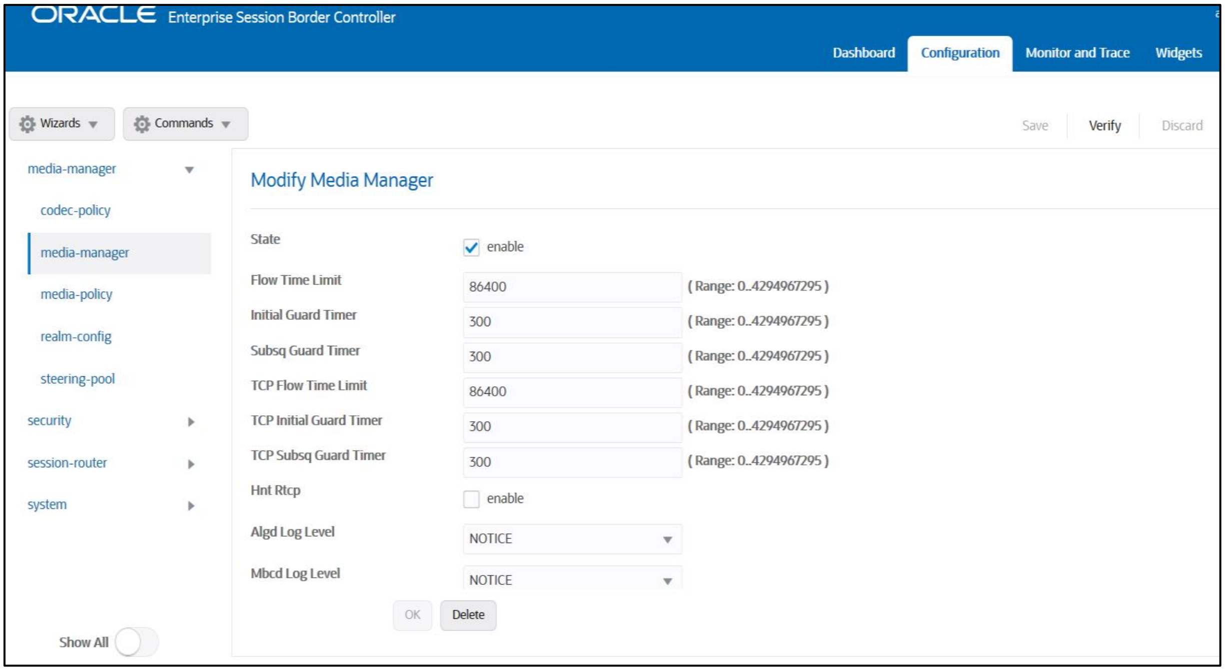
Pri Utility Addr:

Sec Utility Addr:

7.6. Enable media manager

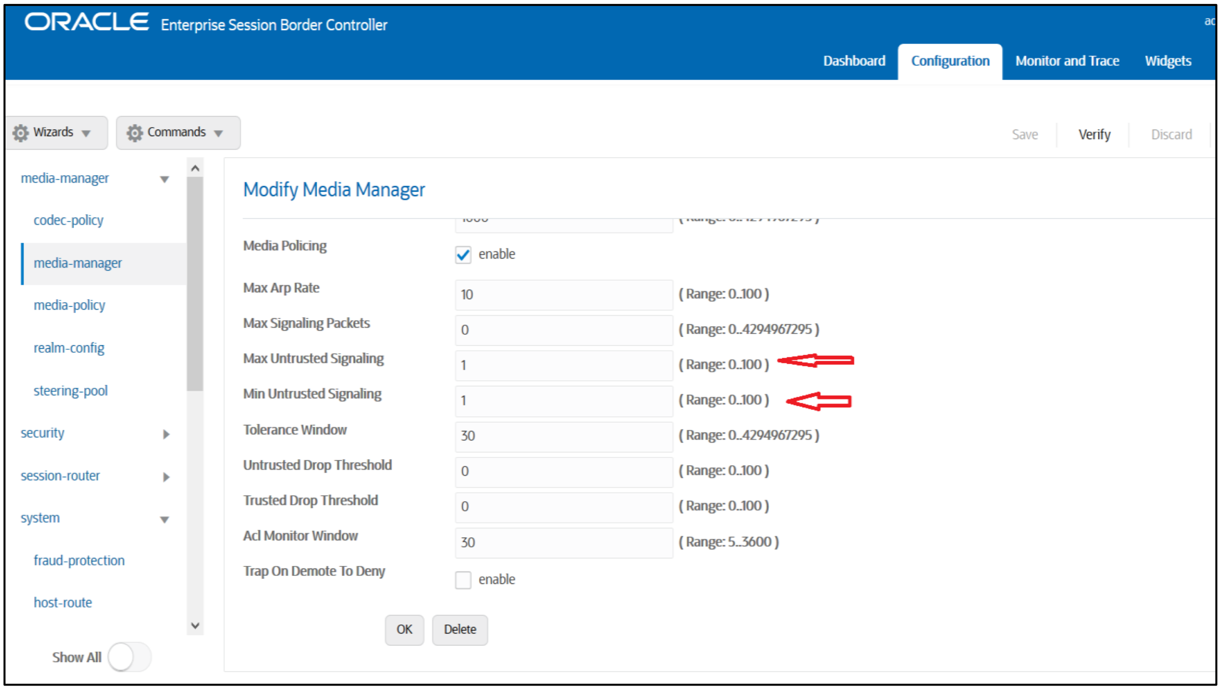
Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

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



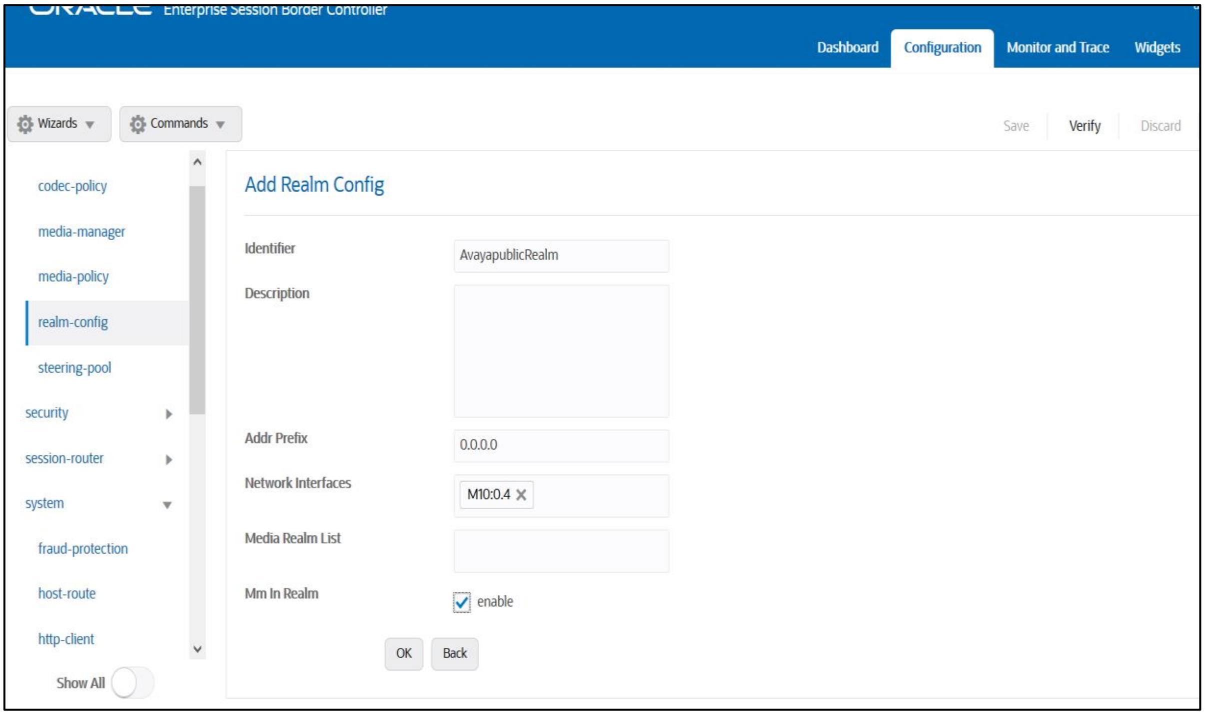
Modify Media Manager

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

7.7. Configure Realms

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

In the below case, Realm name is given as AvayapublicRealm (Avaya Workplace client to SBC side).
Please set the Access Control Trust Level to medium for this realm



Add Realm Config

Identifier: AvayapublicRealm

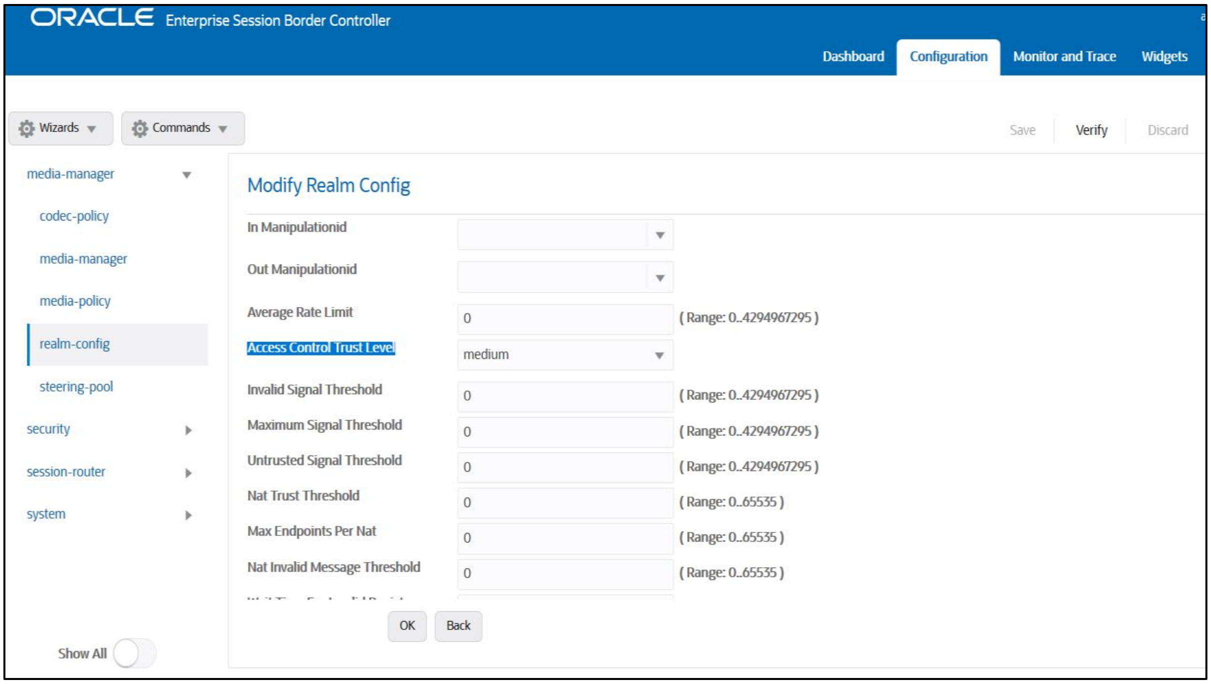
Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M10:0.4 ×

Media Realm List:

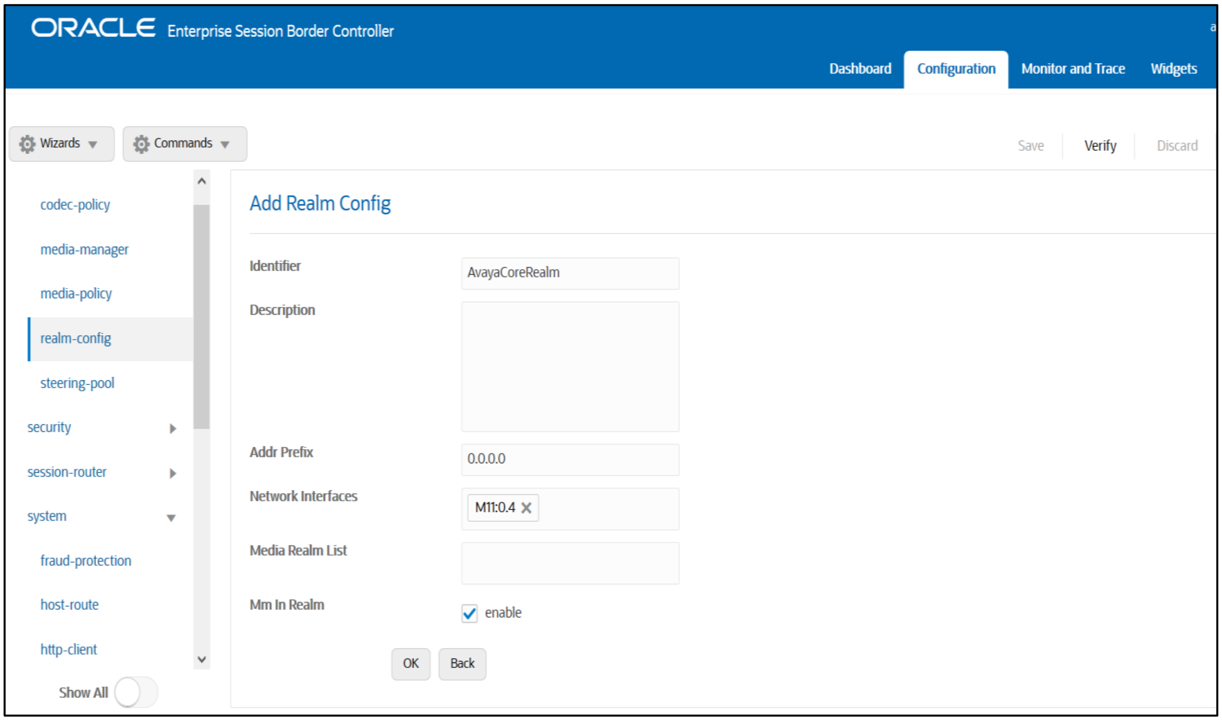
Mm In Realm: ☑ enable



Modify Realm Config

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

Similarly, Realm name is given as AvayaCoreRealm (SBC to Avaya Session Manager)
Please set the Access Control Trust Level to high for this realm



Add Realm Config

Identifier: AvayaCoreRealm

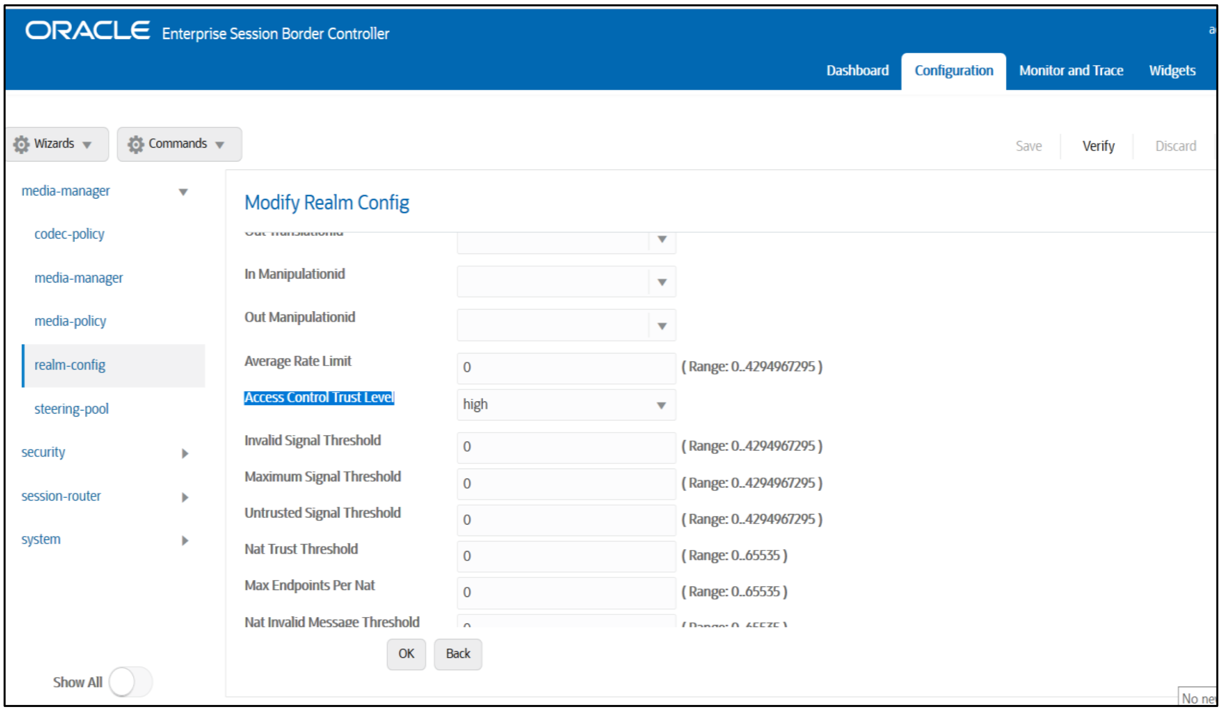
Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M11:0.4 ✕

Media Realm List:

Mm In Realm: ☑ enable



Modify Realm Config

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: 0 (Range: 0..65535)

Nat Invalid Message Threshold

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

https://docs.oracle.com/en/industries/communications/session-border-controller/8.4.0/security/sbc_scz840_security.pdf

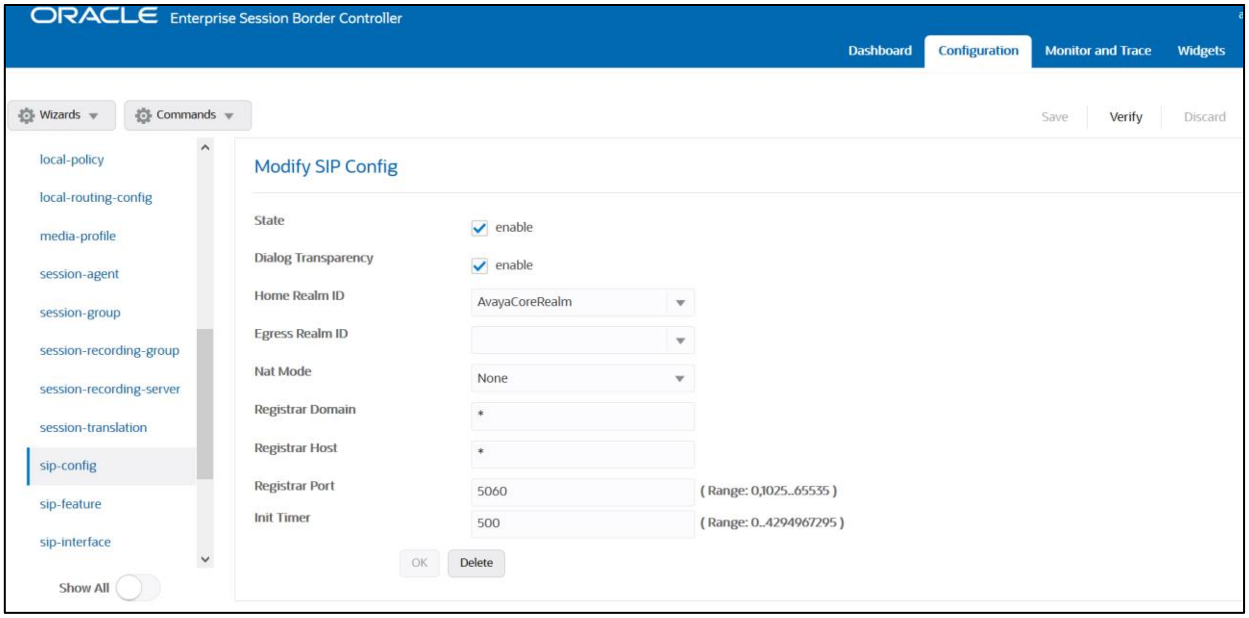
7.8. Enable sip-config

SIP config enables SIP handling in the SBC.
Make sure the home realm-id, registrar-domain and registrar-host are configured.

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

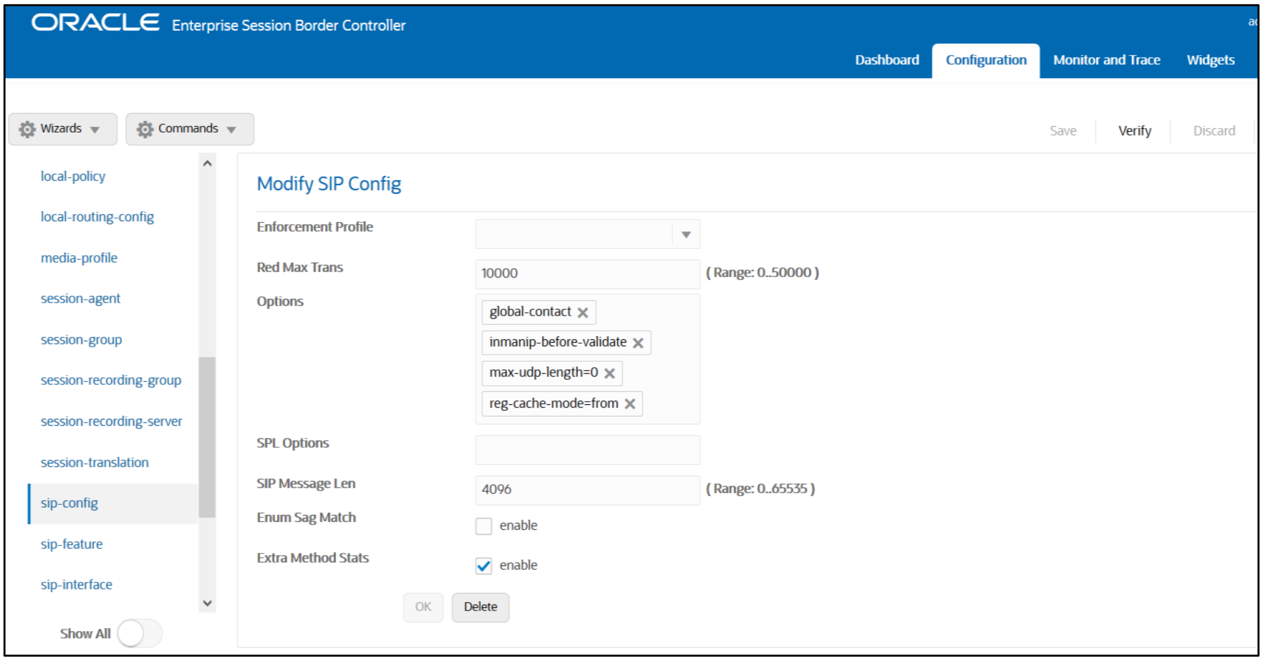
- add max-udp-length =0 & global-contact
- inmanip-before-validate & reg-cache-mode=from

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



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

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

7.9. Configuring a certificate for SBC

As we need to test Avaya Workspace client configuration with TLS connections (Avaya Workspace client to SBC side which is access side), we need to have certificates for the same.

The step below describes how to request a certificate for SBC External interface and configure it based on the example of DigiCert. The process includes the following steps:

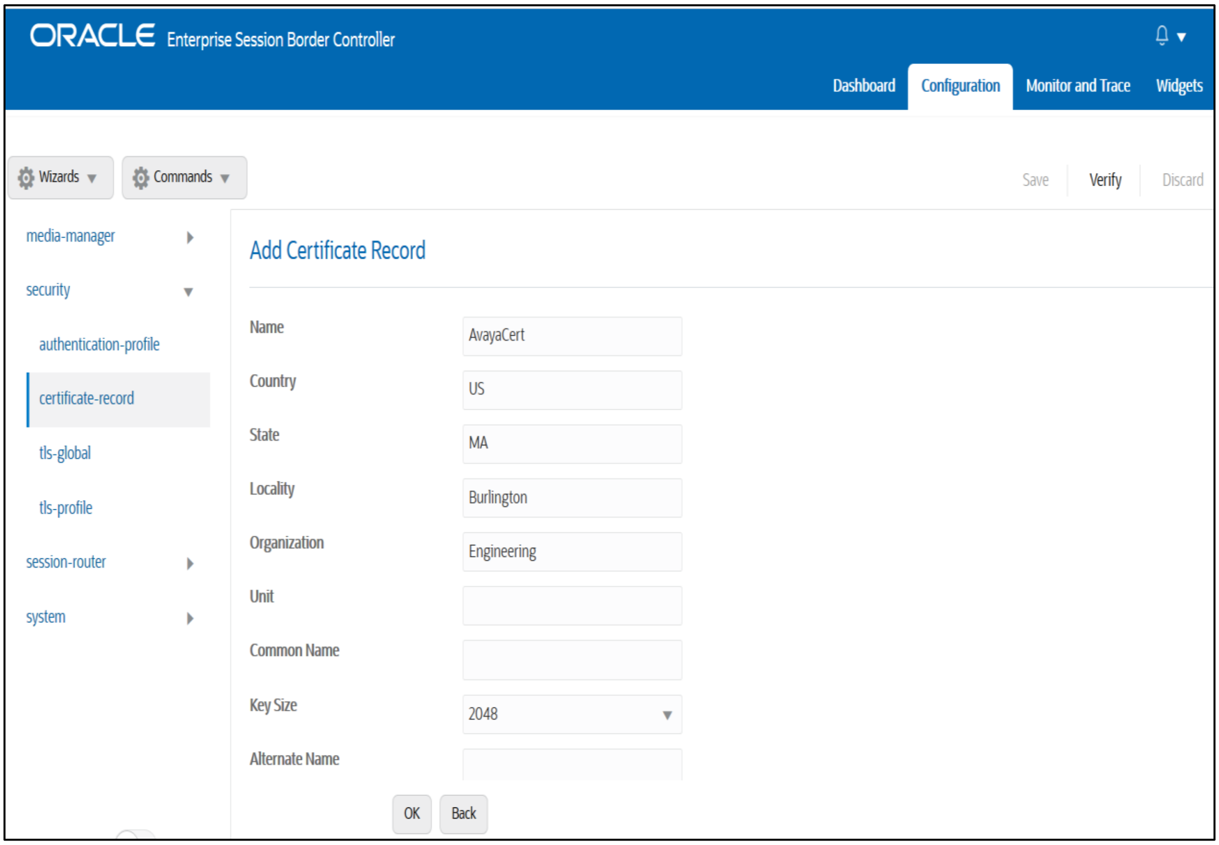
1) Create a certificate-record – “Certificate-record” are configuration elements on Oracle SBC which captures information for a TLS certificate – such as common-name, key-size, key-usage etc.

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

2) Deploy the SBC and Root certificates on the SBC

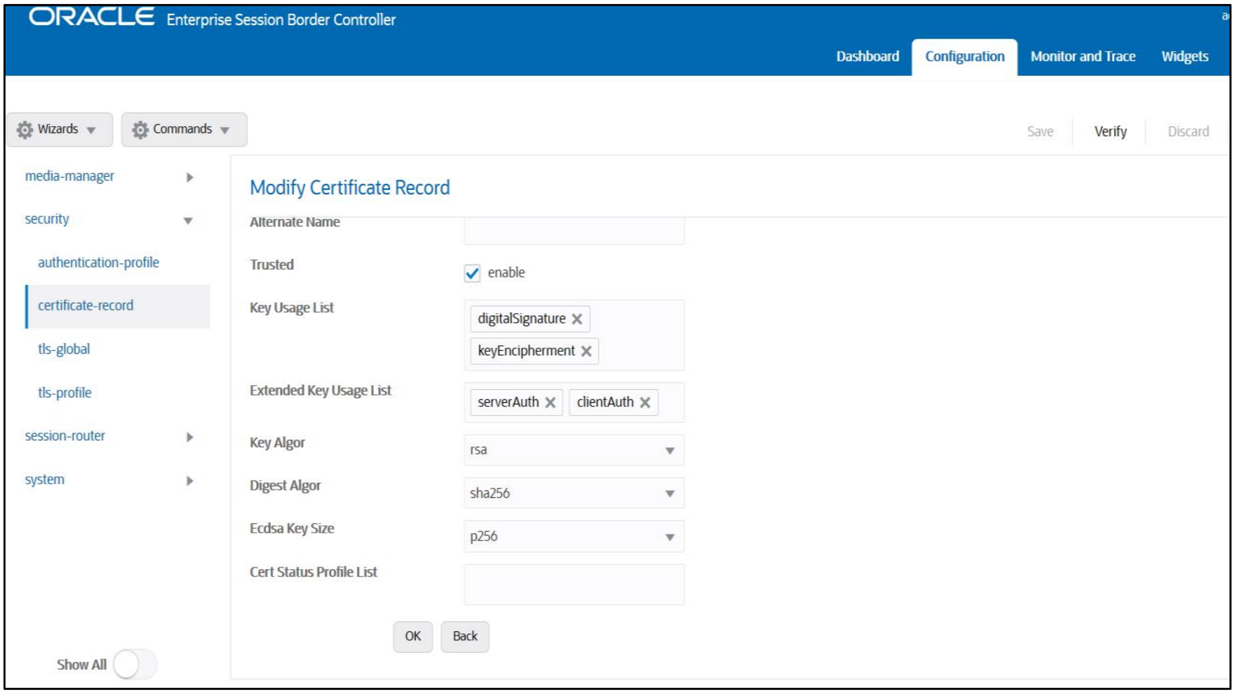
Step 1 – Creating the certificate record

Go to security->Certificate Record and configure the SBC entity certificate for SBC as shown below.



Add Certificate Record

Name	AvayaCert
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	
Common Name	
Key Size	2048
Alternate Name	



Modify Certificate Record

Alternate Name

Trusted ☑ enable

Key Usage List: digitalSignature ✕ keyEncipherment ✕

Extended Key Usage List: serverAuth ✕ clientAuth ✕

Key Algor: rsa

Digest Algor: sha256

Ecdsa Key Size: p256

Cert Status Profile List

Repeat the above steps again to create DigiCert root certificate.
We need to import this root certificate to Windows machine where the Avaya Workplace client is installed. Once this certificate is imported, the soft client will work in TLS mode.

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

Parameter	DigiCertRoot
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

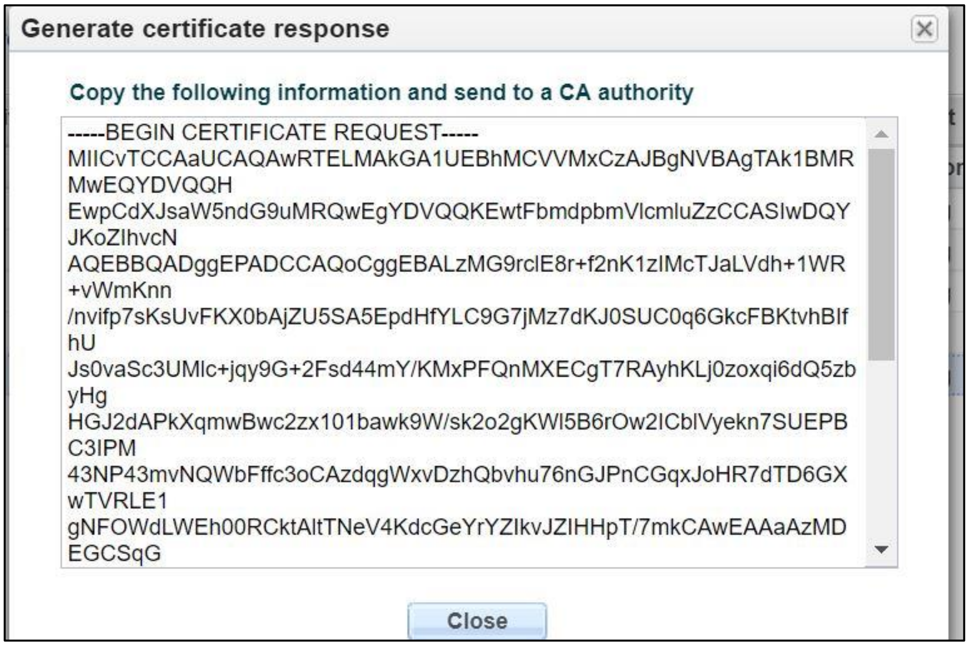
Step 2 – Generating a certificate signing request

(Only required for the SBC’s end entity certificate, and not for root CA certs)

Please note – certificate signing request is only required to be executed for SBC Certificate – not for the root/intermediate certificates.

- Select the certificate and generate certificate on clicking the “Generate” command.

- Please copy/paste the text that gets printed on the screen as shown below and upload to your CA server for signature.



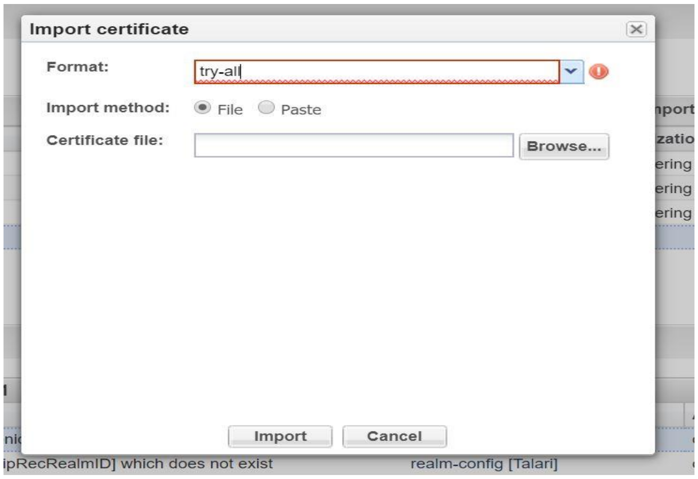
Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvTCCAaUCAQAwRTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMR
MwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzCCASIwDQY
JKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALzMG9rclE8r+f2nK1zIMcTJaLVdh+1WR
+vWmKnn
/nvifp7sKsUvFKX0bAjZU5SA5EpdHfYLC9G7jMz7dKJ0SUC0q6GkcFBKtvhBIf
hU
Js0vaSc3UMIc+jqy9G+2Fsd44mY/KMxPFQnMXECgT7RAyhKLj0zoxqi6dQ5zb
yHg
HGJ2dAPkXqmwBwc2zx101bawk9W/sk2o2gKWI5B6rOw2ICblVyekn7SUEPB
C3IPM
43NP43mvNQWbFffc3oCAzdqgWxvDzhQbvhu76nGJPnCGqxJoHR7dTD6GX
wTVRLE1
gNFOWdLWEh00RCktAltTNeV4KdcGeYrYZIkvJZIHHpT/7mkCAwEAAaAzMD
EGCSqG
```

- Also, note that a save/activate is required

Step 3 – Deploy SBC & root certificates

Once certificate signing request have been completed – import the signed certificate to the SBC. Please note – all certificates including root and intermediate certificates are required to be imported to the SBC. Once done, issue save/activate from the WebGUI



Import certificate

Format: try-all

Import method: ● File ○ Paste

Certificate file:

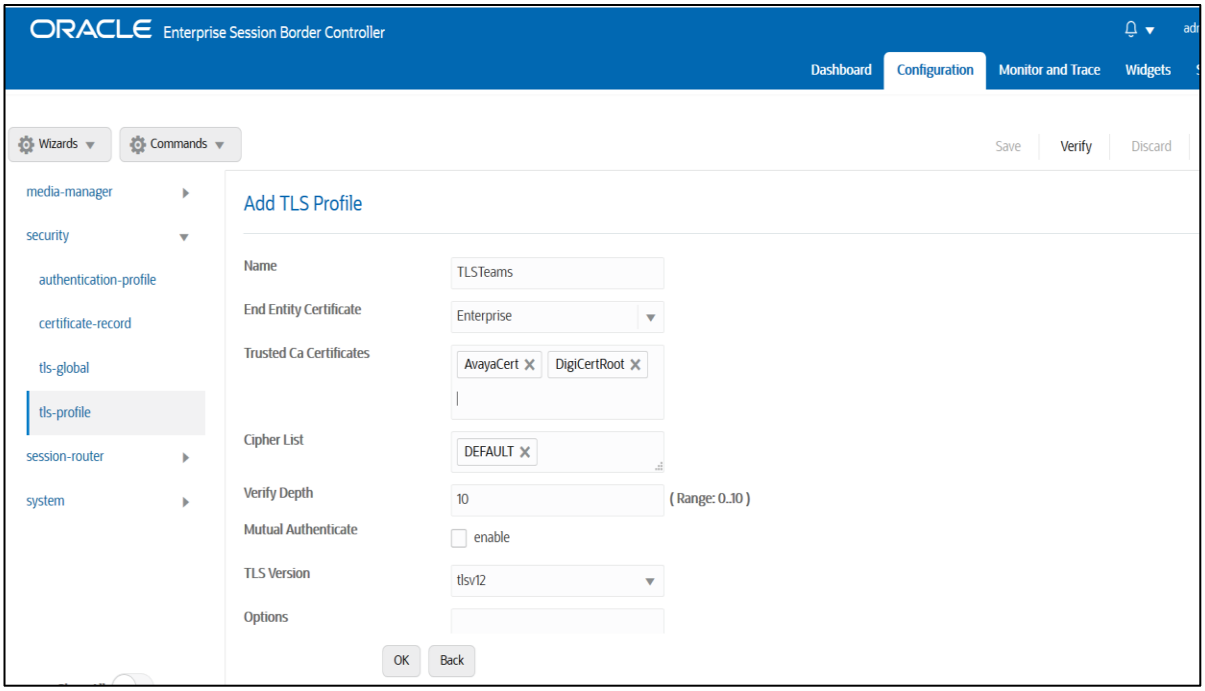
Repeat the steps for the following certificates:

- DigiCertRoot.

At this stage all the required certificates have been imported to the SBC.

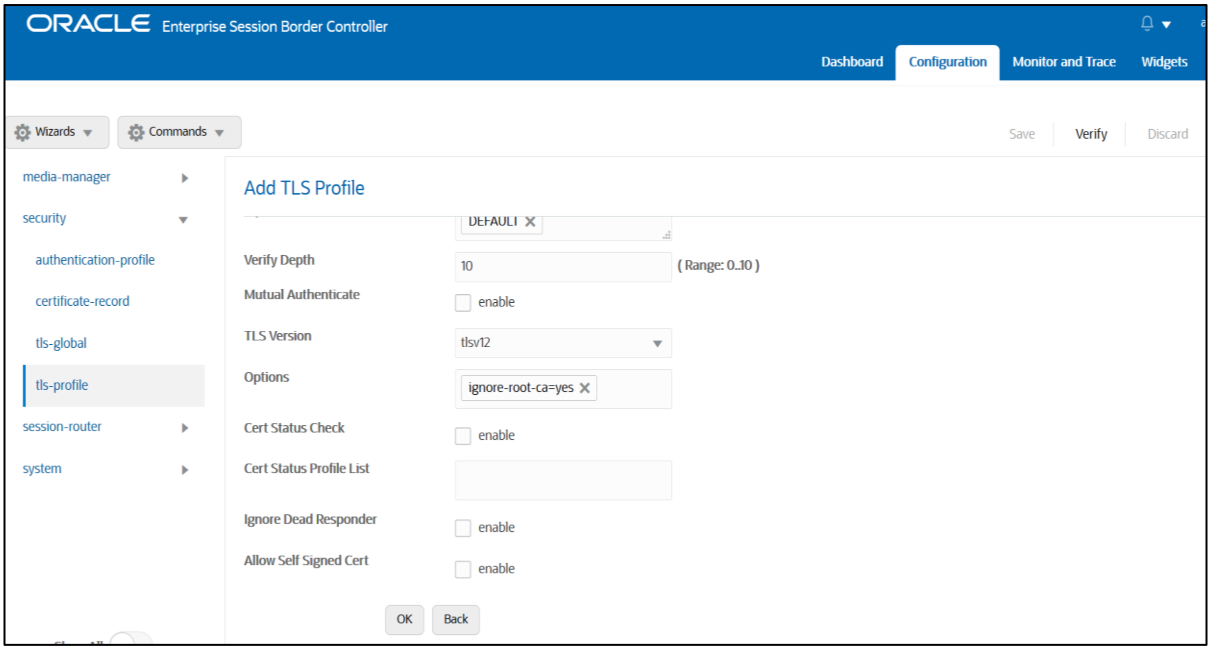
7.10. TLS-Profile

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
Please disable mutual authenticate option and also add options “ignore-root-ca=yes”



Add TLS Profile

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



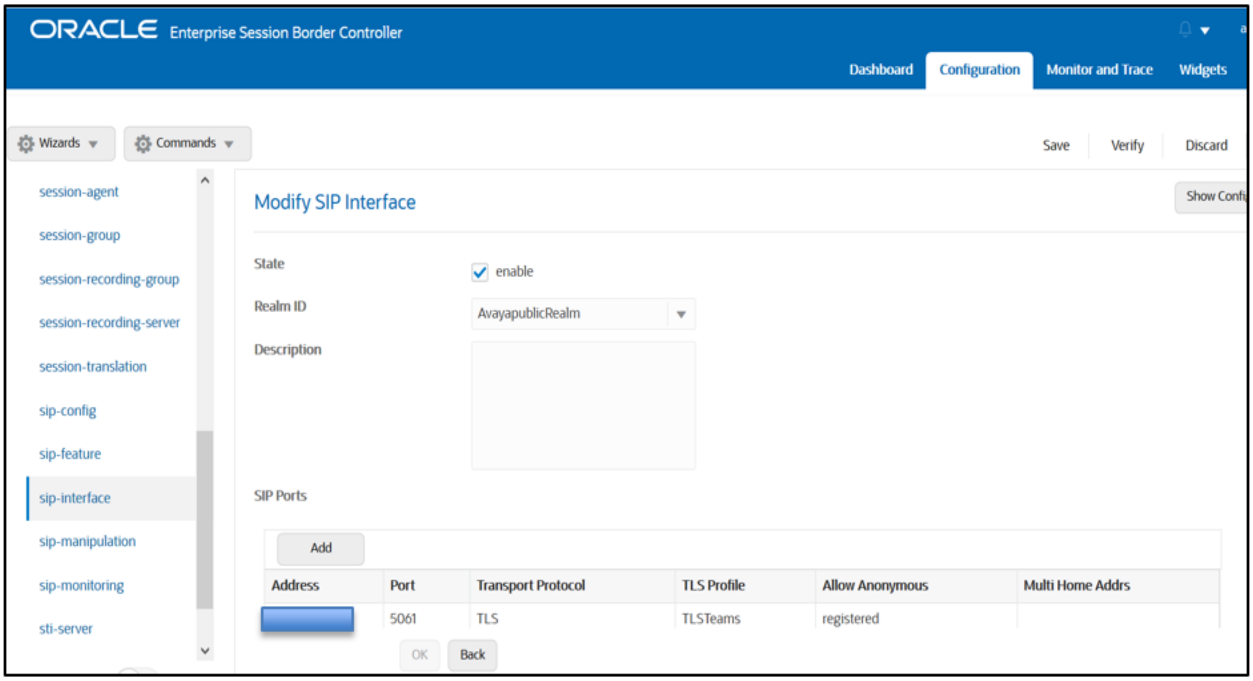
Add TLS Profile

	DEFAULT ✕
Verify Depth	10 (Range: 0..10)
Mutual Authenticate	□ enable
TLS Version	tlsv12
Options	ignore-root-ca=yes ✕
Cert Status Check	□ enable
Cert Status Profile List	
Ignore Dead Responder	□ enable
Allow Self Signed Cert	□ enable

7.11. 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 which is configured for Avaya Workspace client.

- Tls-profile needs to match the name of the tls-profile previously created
- Set allow-anonymous to registered to ensure traffic to this sip-interface only comes from Workplace client which is registered to Avaya Session Manager via SBC.
- Set NAT traversal to always for the Avaya Workspace client to register.



Modify SIP Interface

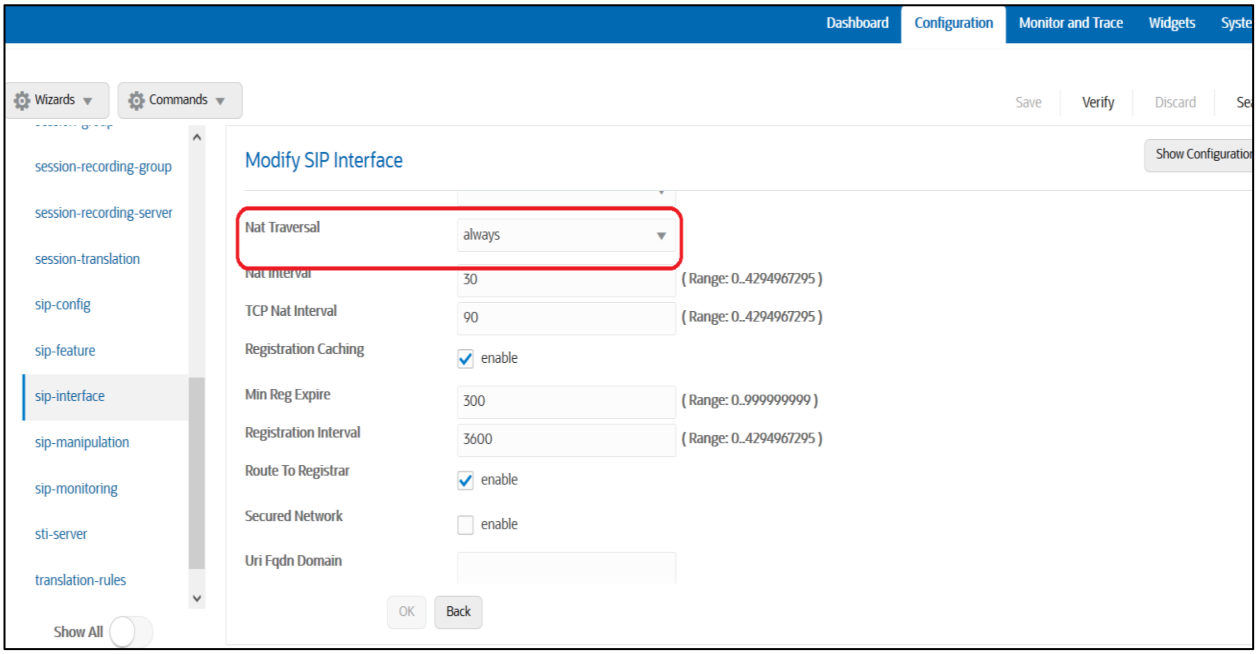
State ☑ enable

Realm ID AvayapublicRealm

Description

SIP Ports

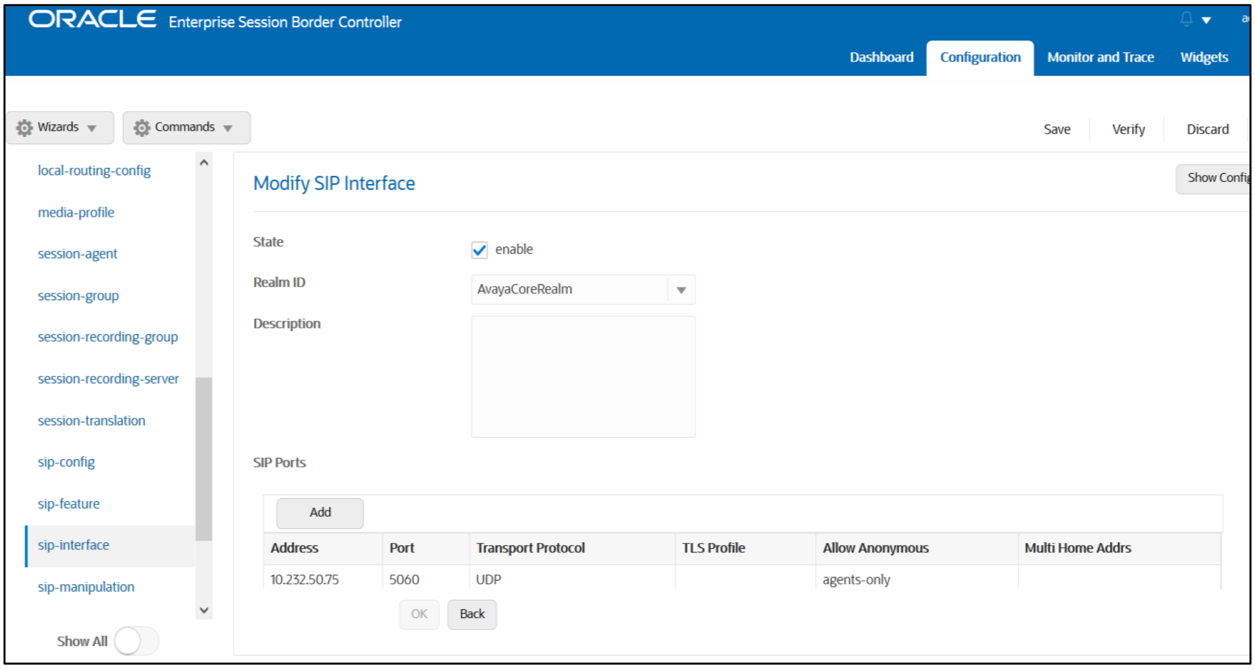
Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
	5061	TLS	TLSTeams	registered	



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		

Similarly, Configure Internal IP under sip-port of sip-interface for Avaya Session Manager side. (Avaya Core Side). Set allow-anonymous to agents-only.



Modify SIP Interface

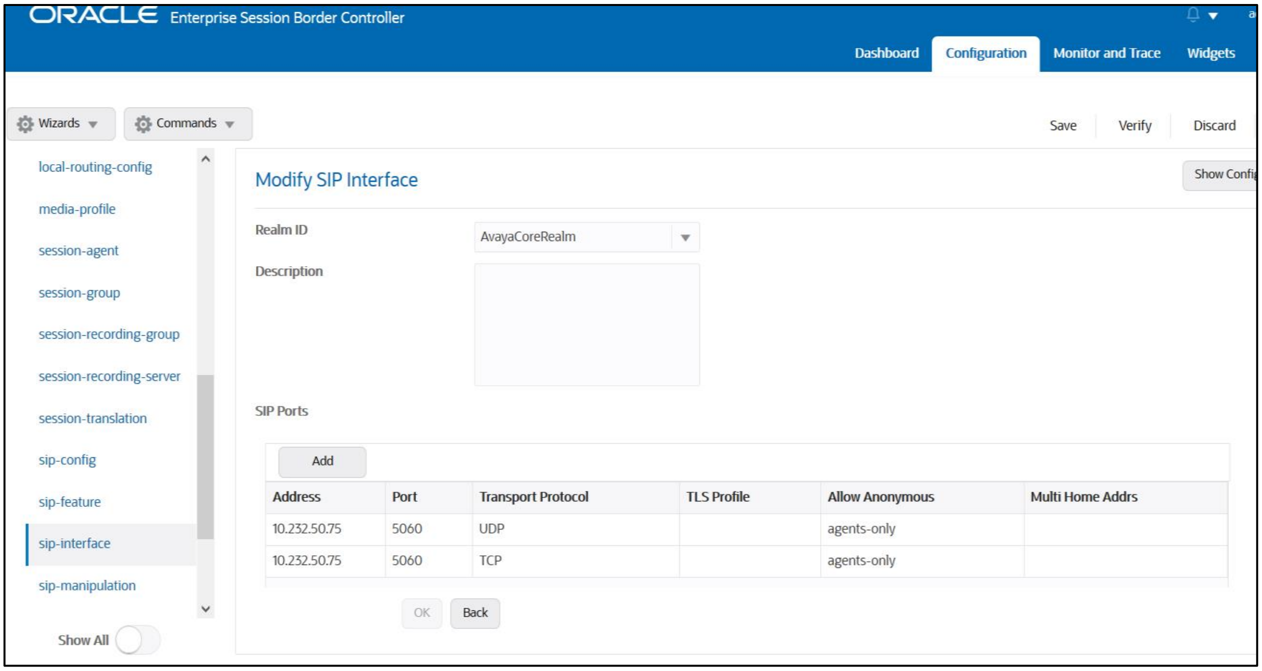
State ☑ enable

Realm ID AvayaCoreRealm

Description

SIP Ports

Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
10.232.50.75	5060	UDP		agents-only	



Modify SIP Interface

Realm ID AvayaCoreRealm

Description

SIP Ports

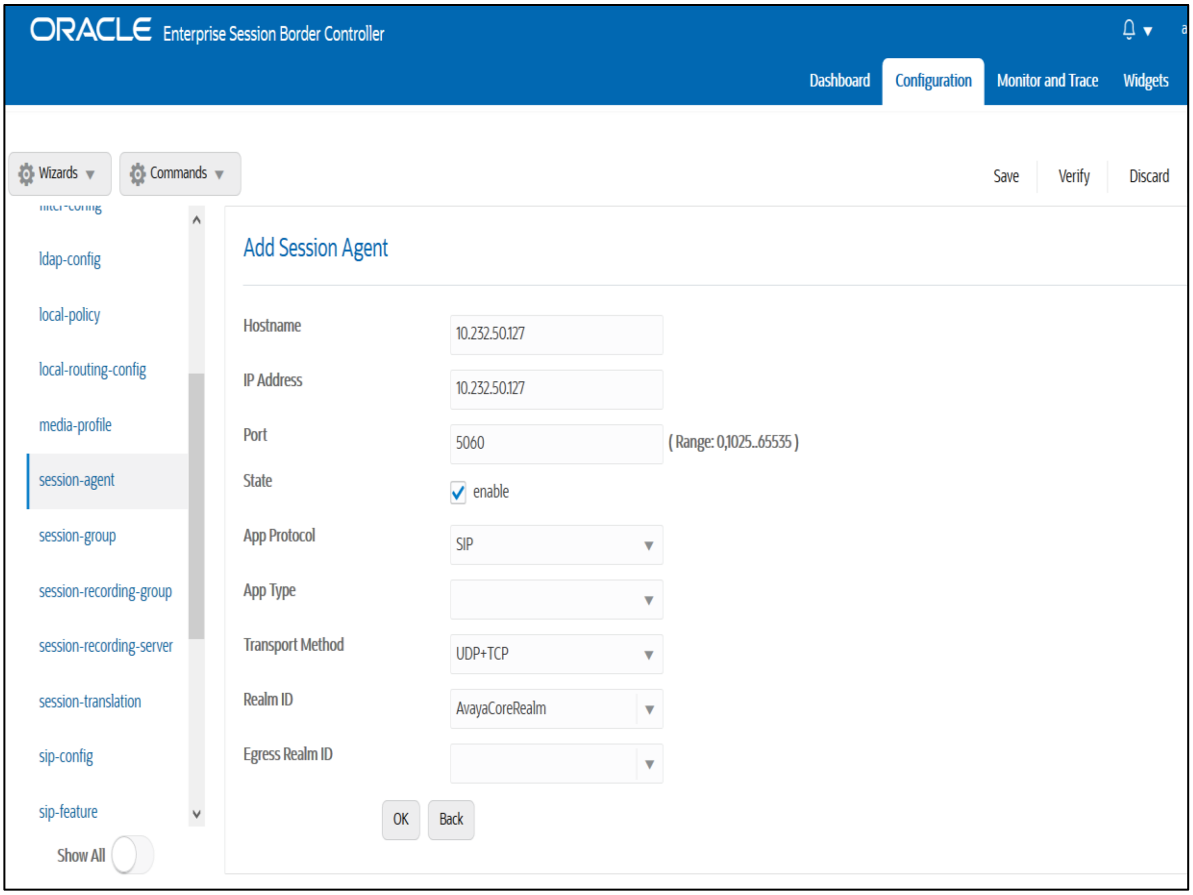
Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
10.232.50.75	5060	UDP		agents-only	
10.232.50.75	5060	TCP		agents-only	

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

7.12. Configure session-agent

Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data.
Configure the session-agent for Avaya Session Manager where SBC should route the calls.
Go to session-router->Session-Agent.

- Host name and IP address to 10.232.50.127 which is the Avaya SM IP.
- Port set to 5060
- Realm ID – Needs to match the realm created for Avaya SM.
  Transport set to “UDP+TCP



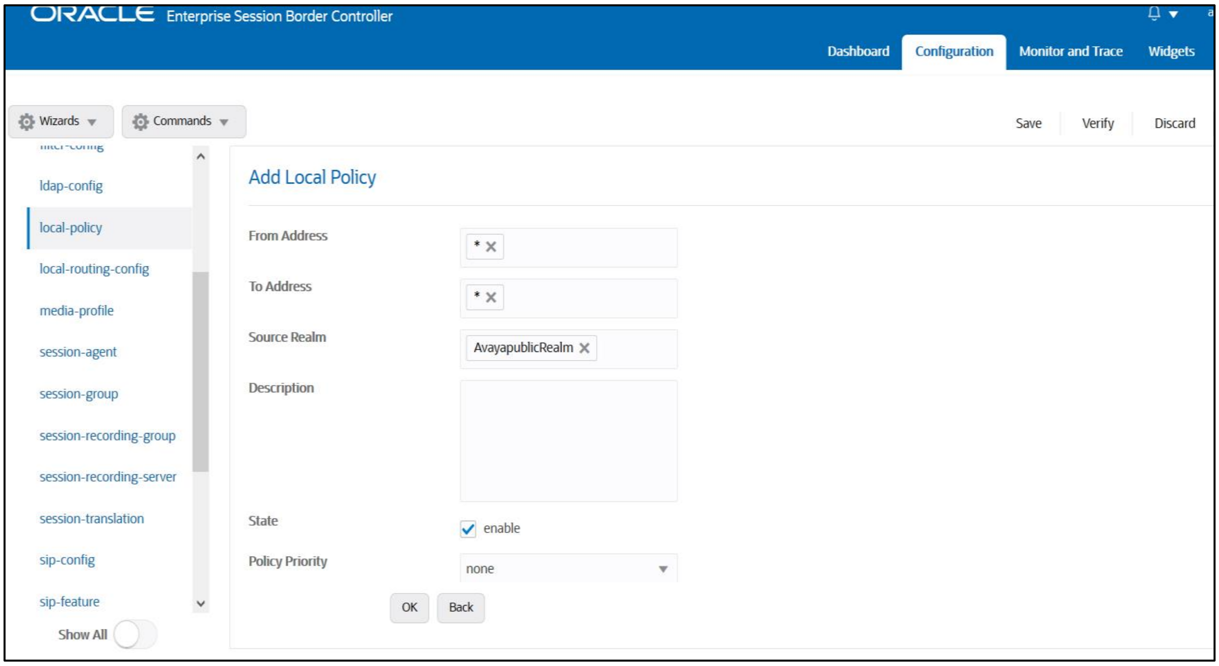
Add Session Agent

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	AvayaCoreRealm
Egress Realm ID	

7.13. 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 register and make calls from Avaya Workspace client to Other Phones via sbc,
The next hop here should be the Avaya SM IP which is 10.232.50.127



Add Local Policy

From Address: * ×

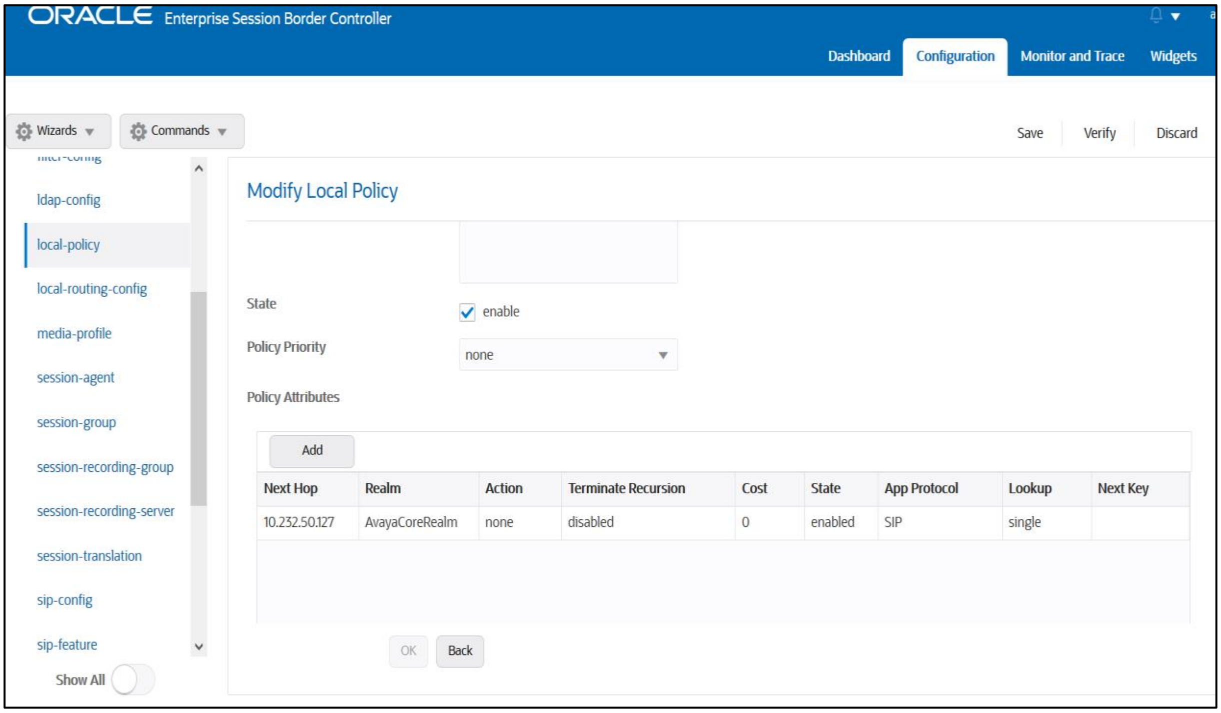
To Address: * ×

Source Realm: AvayapublicRealm ×

Description:

State: ☑ enable

Policy Priority: none



Modify Local Policy

State: ☑ enable

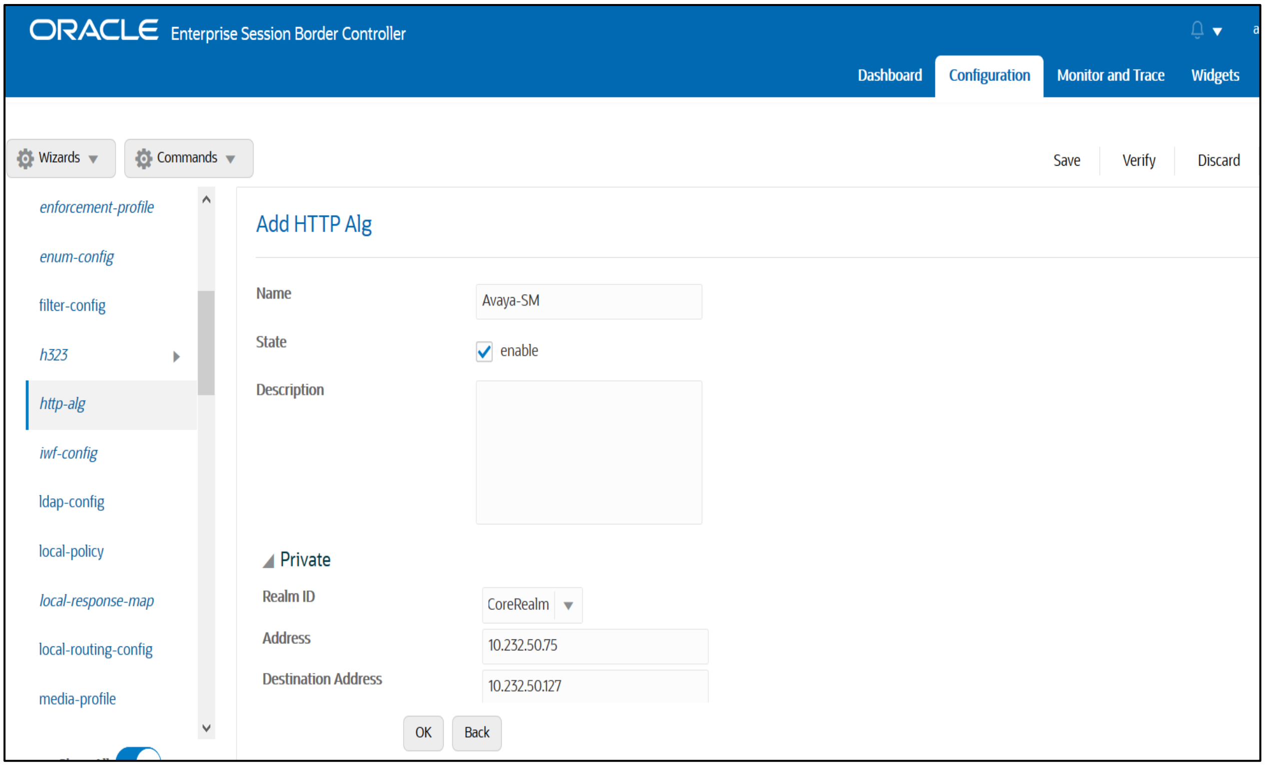
Policy Priority: none

Policy Attributes

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

7.14. Configure http-alg

The http-alg config is done for PPM support from SBC to Avaya SM.
Navigate to http-alg under session-router and configure that as shown below



Add HTTP Alg

Name: Avaya-SM

State: ☑ enable

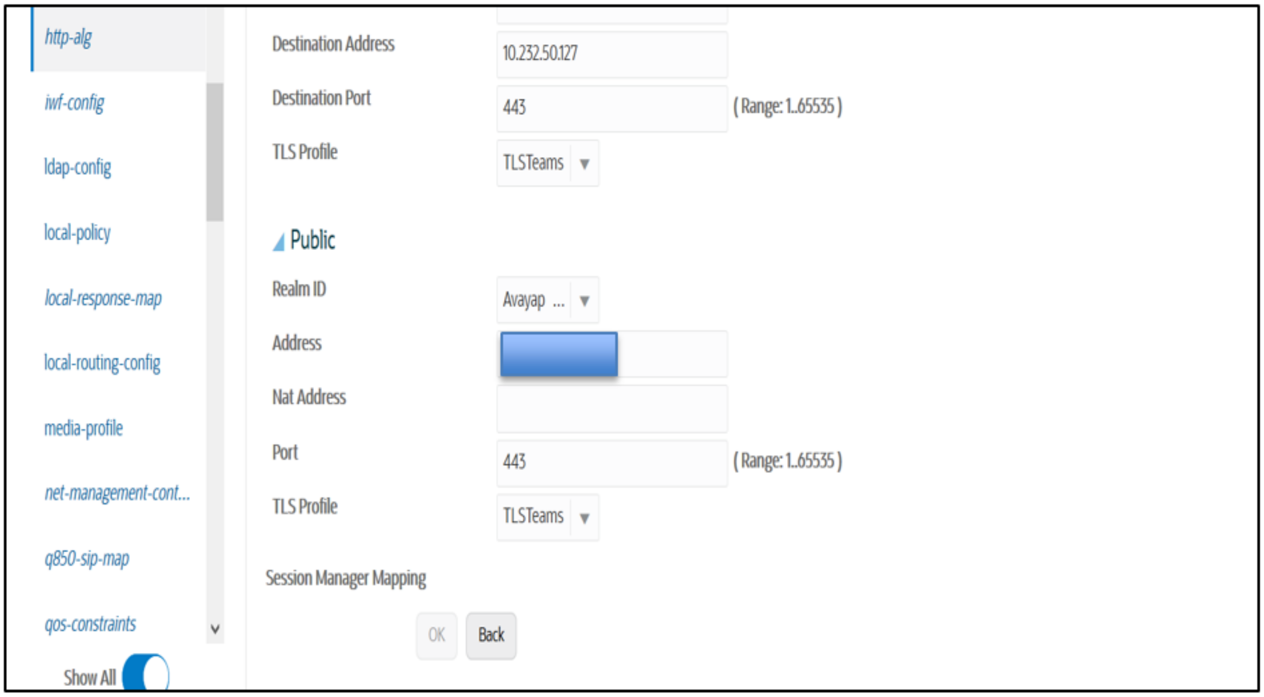
Description:

Private

Realm ID: CoreRealm

Address: 10.232.50.75

Destination Address: 10.232.50.127



Destination Address: 10.232.50.127

Destination Port: 443 (Range: 1..65535)

TLS Profile: TLSTeams

Public

Realm ID: Avayap ...

Address: [redacted]

Nat Address:

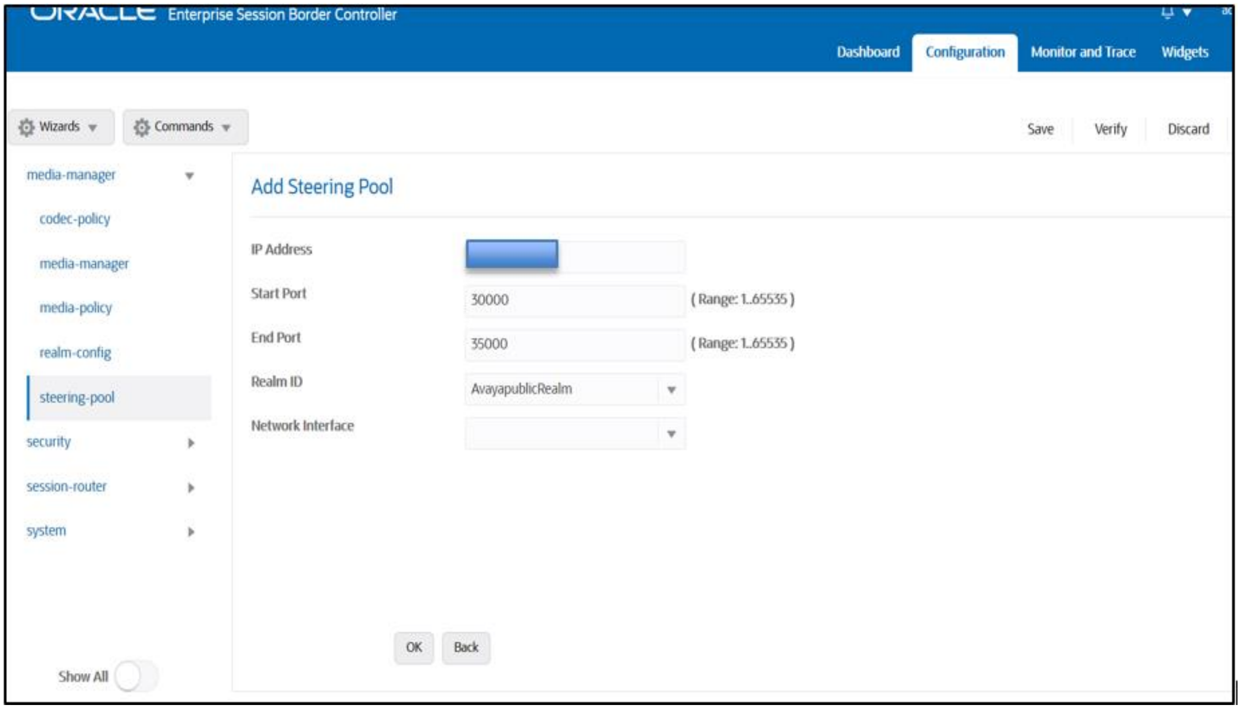
Port: 443 (Range: 1..65535)

TLS Profile: TLSTeams

Session Manager Mapping

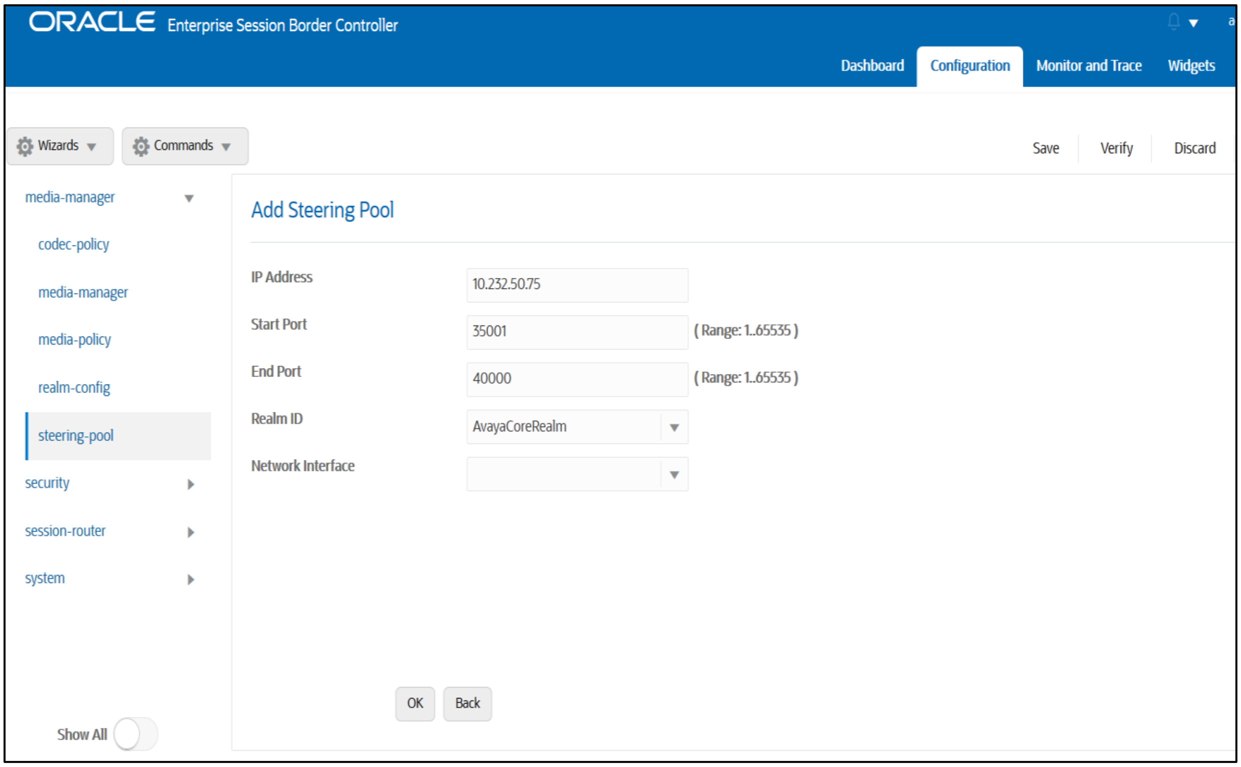
7.15. Configure steering-pool

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



Add Steering Pool

IP Address		
Start Port	30000	(Range: 1..65535)
End Port	35000	(Range: 1..65535)
Realm ID	AvayapublicRealm	
Network Interface		

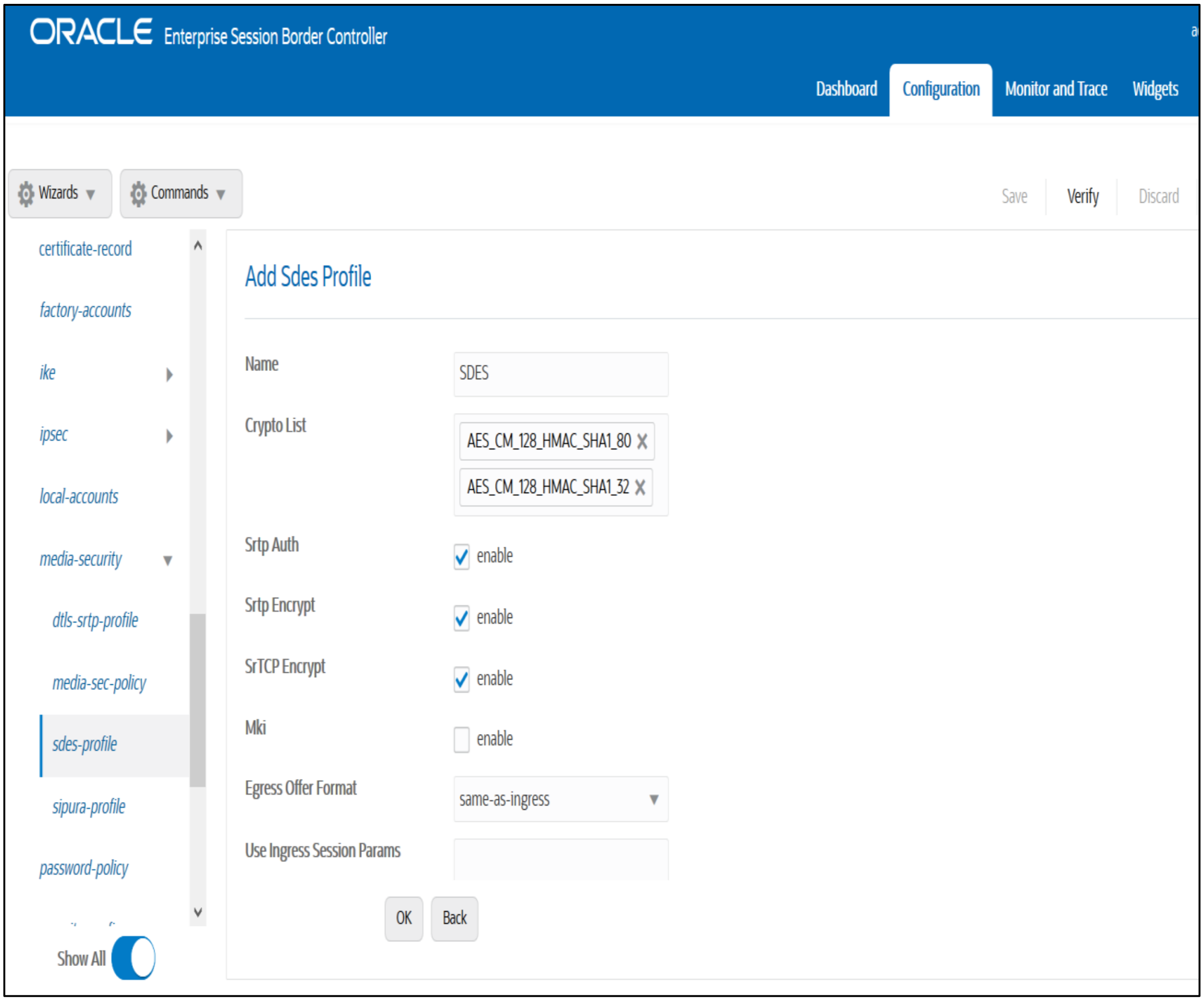


Add Steering Pool

IP Address	10.232.50.75	
Start Port	35001	(Range: 1..65535)
End Port	40000	(Range: 1..65535)
Realm ID	AvayaCoreRealm	
Network Interface		

7.16. Configure sdes profile

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



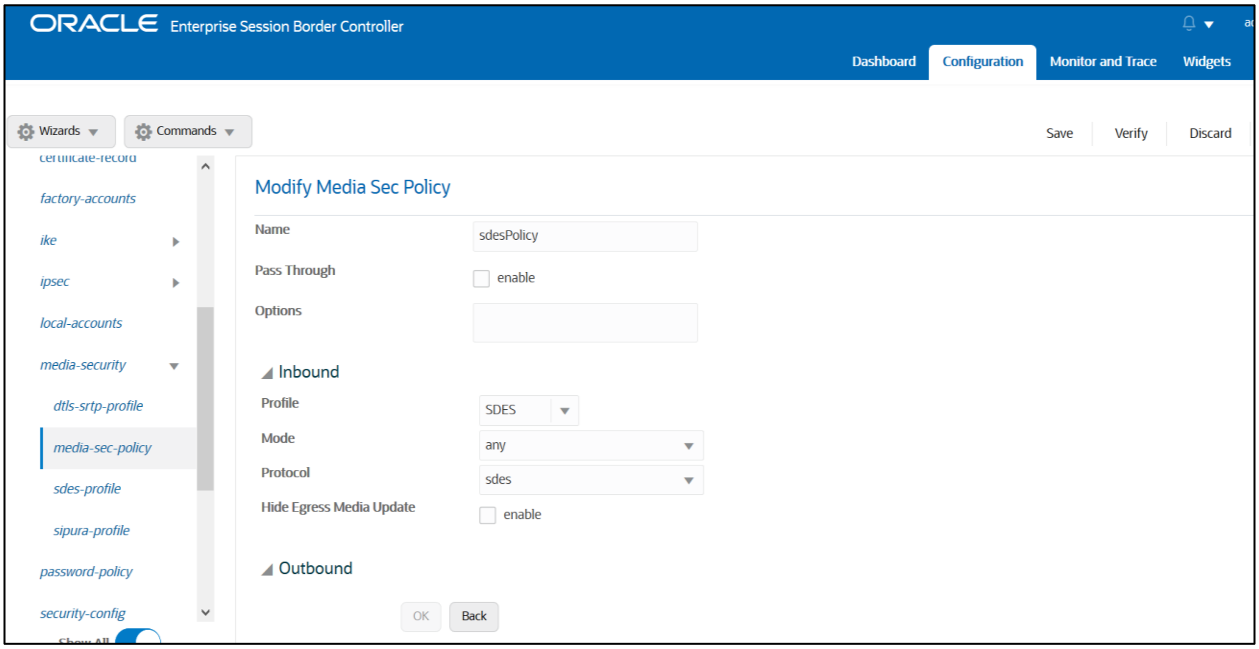
Add Sdes Profile

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	

7.17. 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 for the Avaya Public Side which will have the sdes profile created above.

Please set Mode to “any” for Inbound Media sec policy and Avaya Workplace client works in SRTP mode both ways after making this change and Assign this media policy to the AvayapublicRealm.



Modify Media Sec Policy

Name sdesPolicy

Pass Through □ enable

Options

Inbound

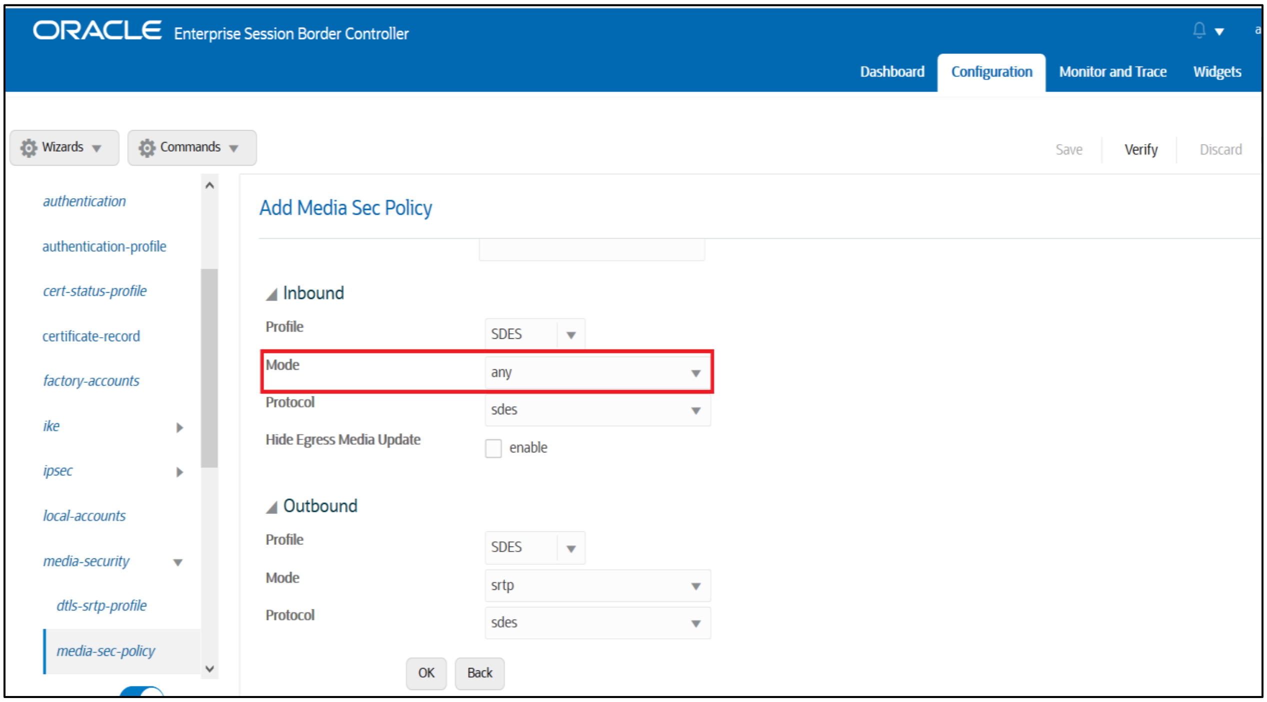
Profile SDES

Mode any

Protocol sdes

Hide Egress Media Update □ enable

Outbound



Add Media Sec Policy

Inbound

Profile SDES

Mode any

Protocol sdes

Hide Egress Media Update □ enable

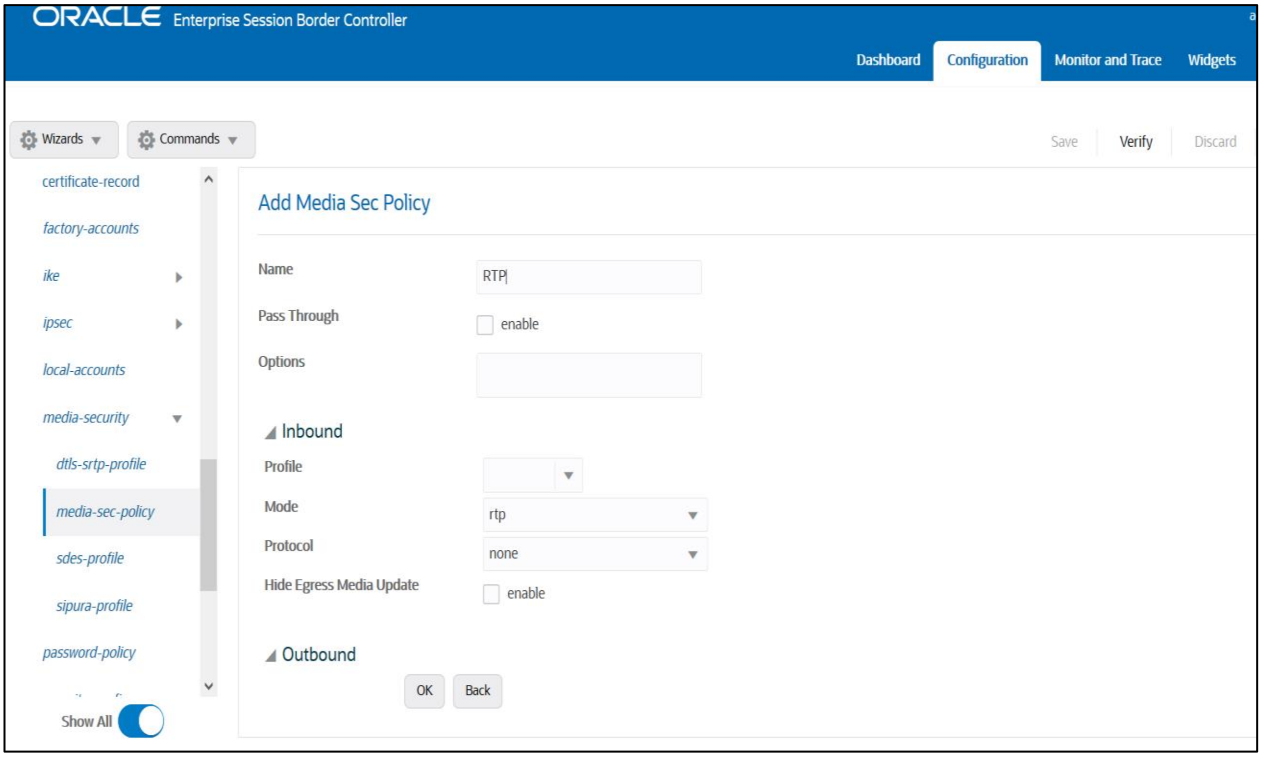
Outbound

Profile SDES

Mode srtp

Protocol sdes

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



Add Media Sec Policy

Name: RTP

Pass Through: □ enable

Options:

Inbound

Profile:

Mode: rtp

Protocol: none

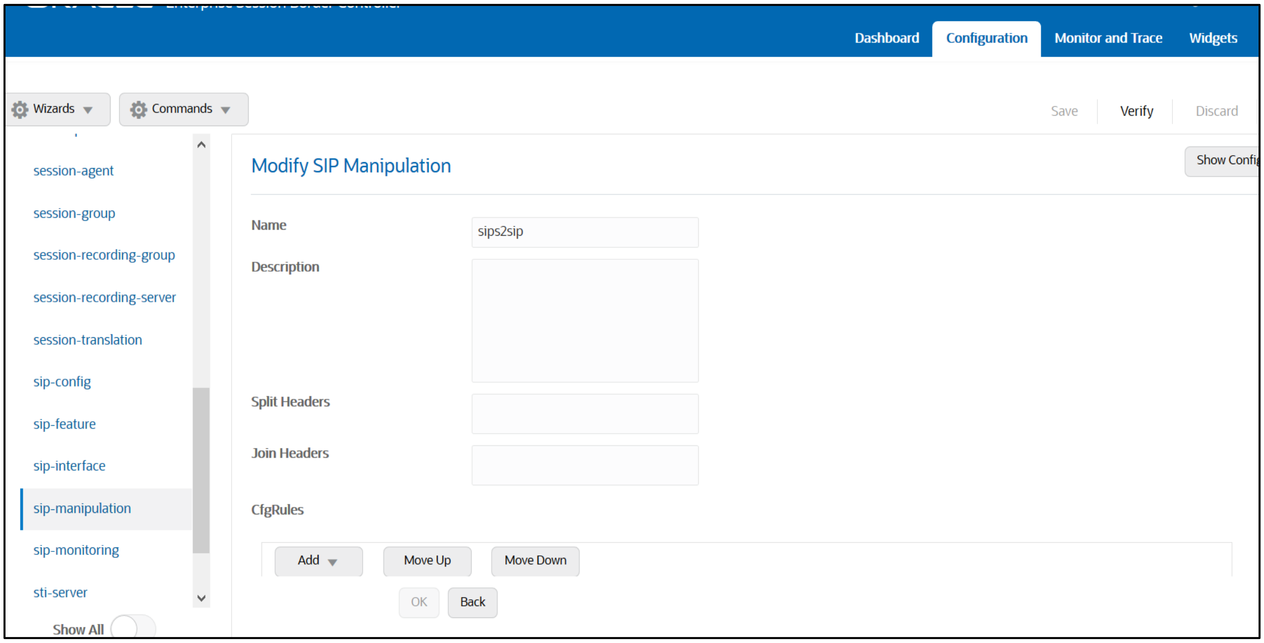
Hide Egress Media Update: □ enable

Outbound

7.18. Configure Header Manipulation Rules (HMR)

As Avaya workspace client sends the requests in sips format, we need to add HMR in SBC to convert the incoming sips mode from access side to normal sip mode and send it to the core side. To achieve the same, we use the sip- manipulations as below as we need to convert URI, to, from, Contact Headers and mime rule to change rfc5939_to_rfc3711 from the incoming requests. The following sip-manipulation called **sips2sip** is configured with header rules and element rules for this purpose.

To configure sip-manipulations, go to session-router->sip-manipulation



Modify SIP Manipulation

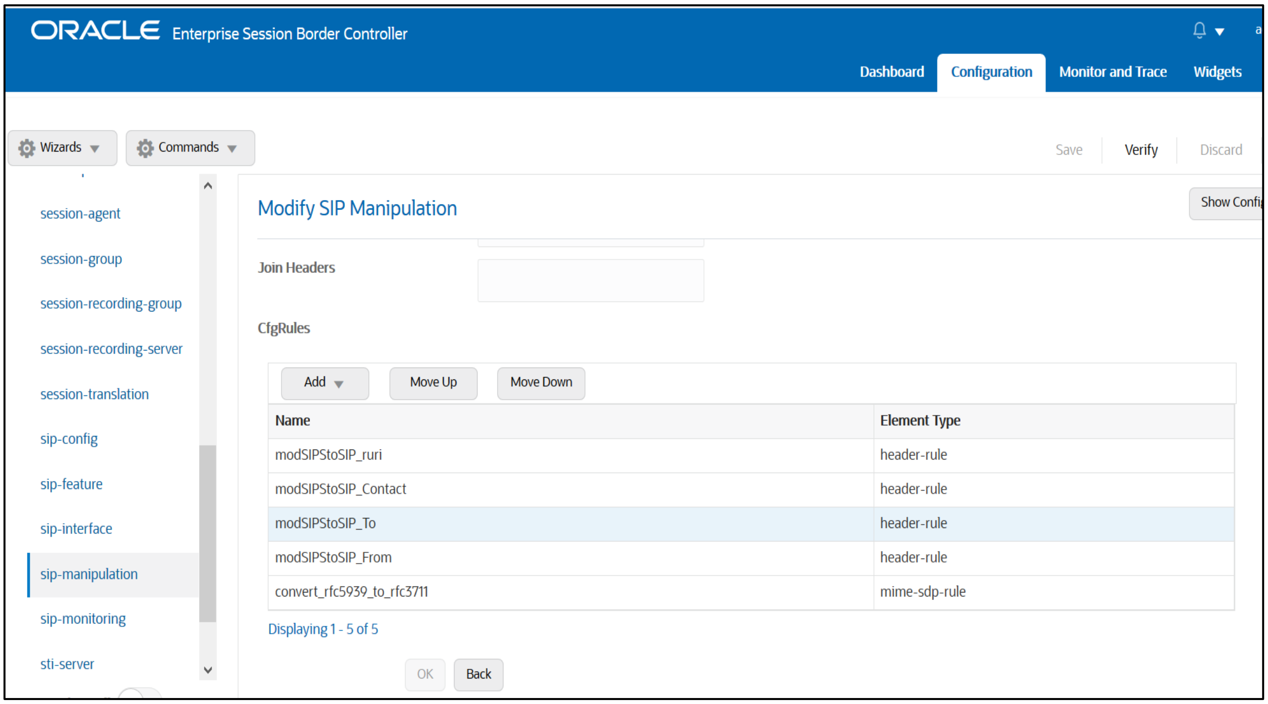
Name: sips2sip

Description

Split Headers

Join Headers

CfgRules



Modify SIP Manipulation

Join Headers

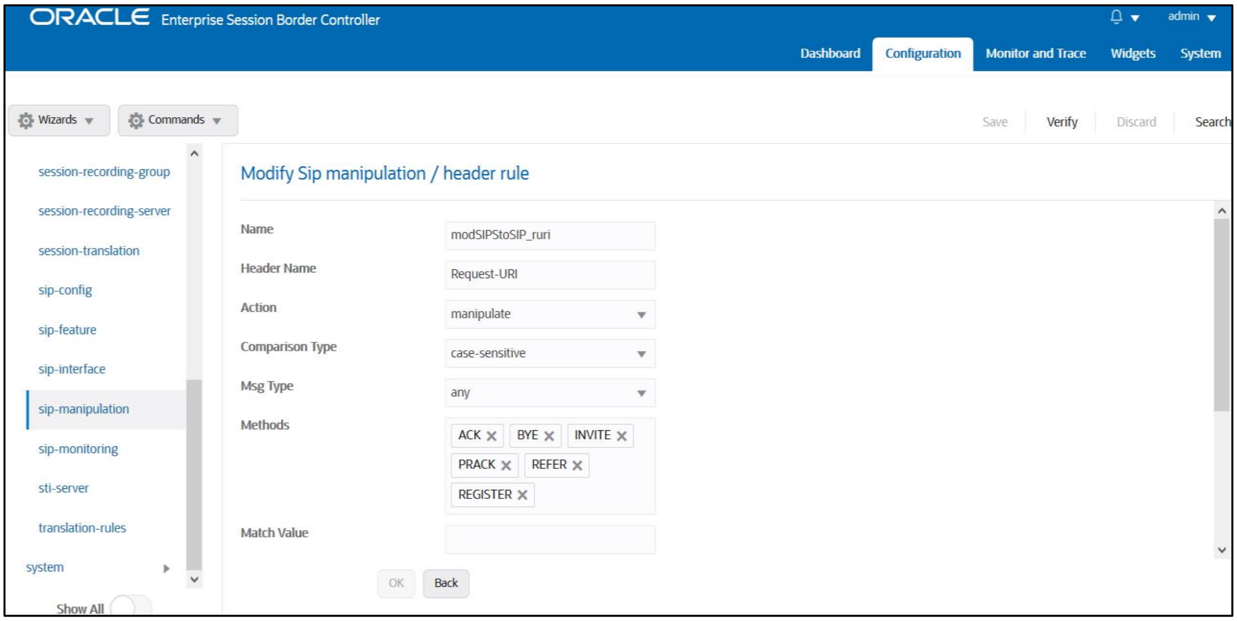
CfgRules

Name	Element Type
modSIPStoSIP_ruri	header-rule
modSIPStoSIP_Contact	header-rule
modSIPStoSIP_To	header-rule
modSIPStoSIP_From	header-rule
convert_rfc5939_to_rfc3711	mime-sdp-rule

Displaying 1 - 5 of 5

Each Header rule and its element-rule config are given below:

Header Rule and Element Rule of Request URI header.



Modify Sip manipulation / header rule

Name: modSIPStoSIP_ruri

Header Name: Request-URI

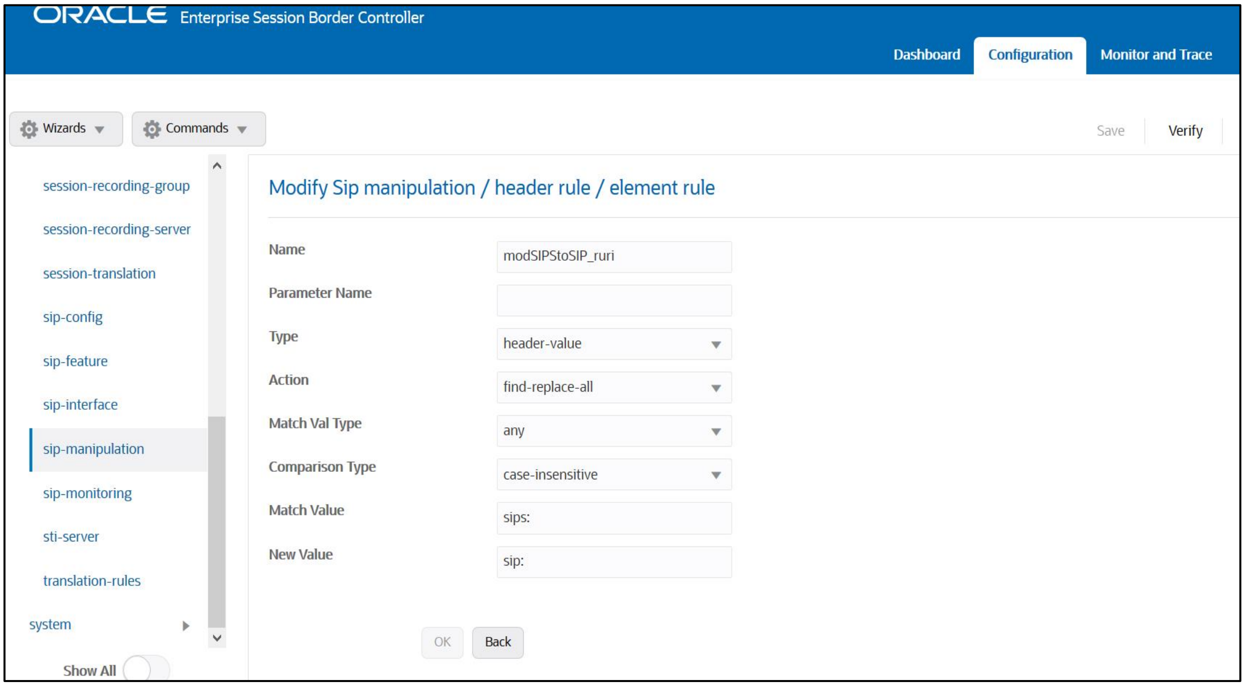
Action: manipulate

Comparison Type: case-sensitive

Msg Type: any

Methods: ACK, BYE, INVITE, PRACK, REFER, REGISTER

Match Value:



Modify Sip manipulation / header rule / element rule

Name: modSIPStoSIP_ruri

Parameter Name:

Type: header-value

Action: find-replace-all

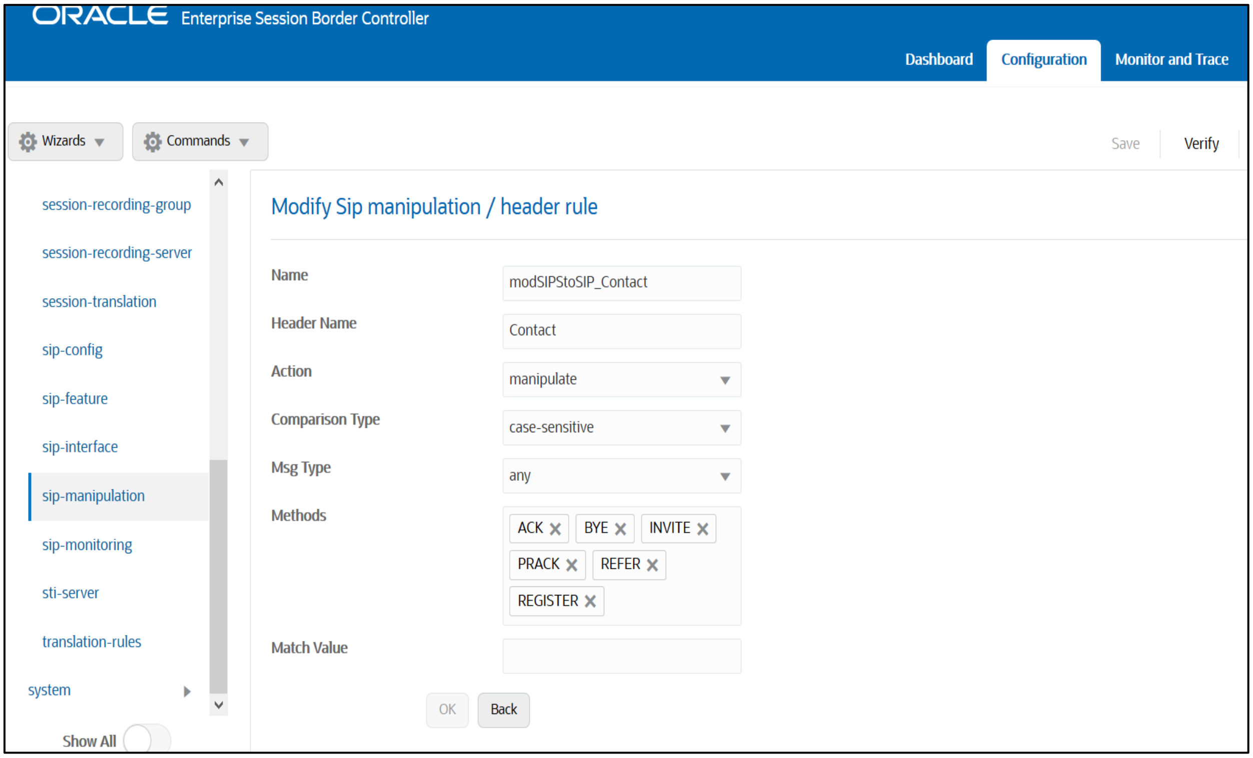
Match Val Type: any

Comparison Type: case-insensitive

Match Value: sips:

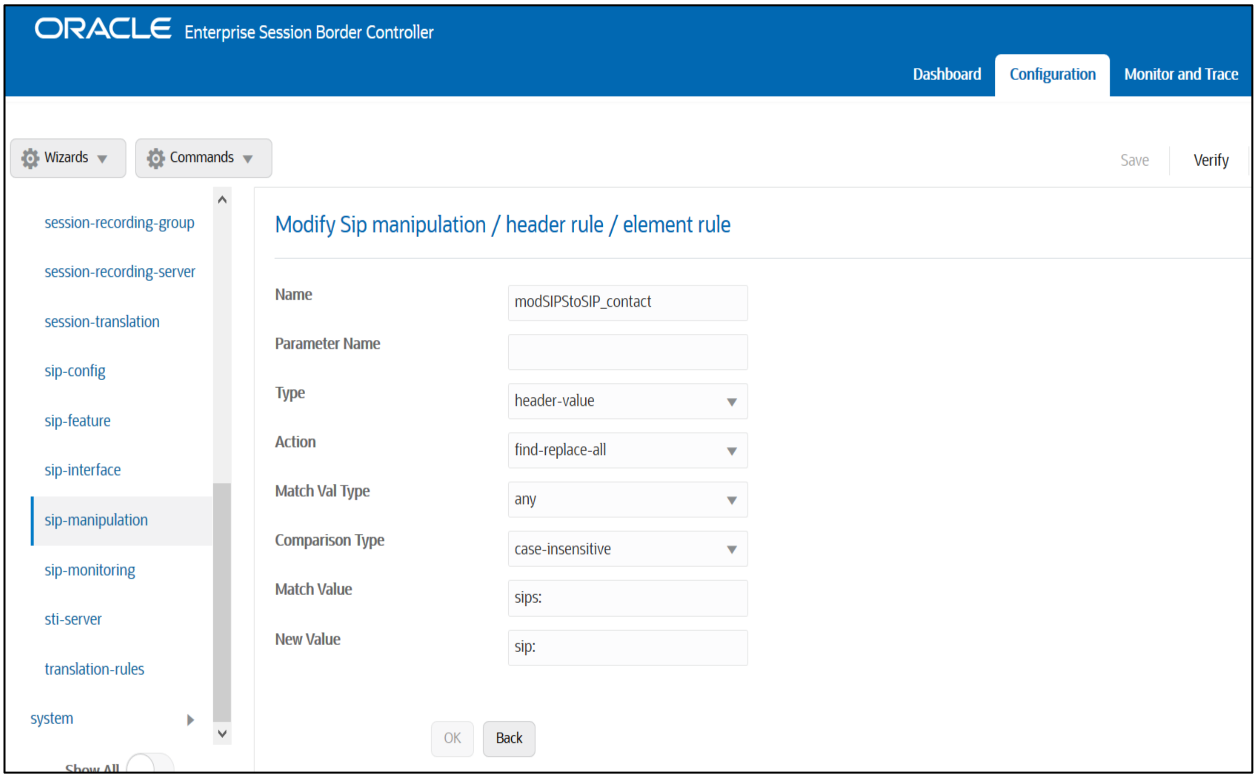
New Value: sip:

Header Rule and Element Rule of Contact header.



Modify Sip manipulation / header rule

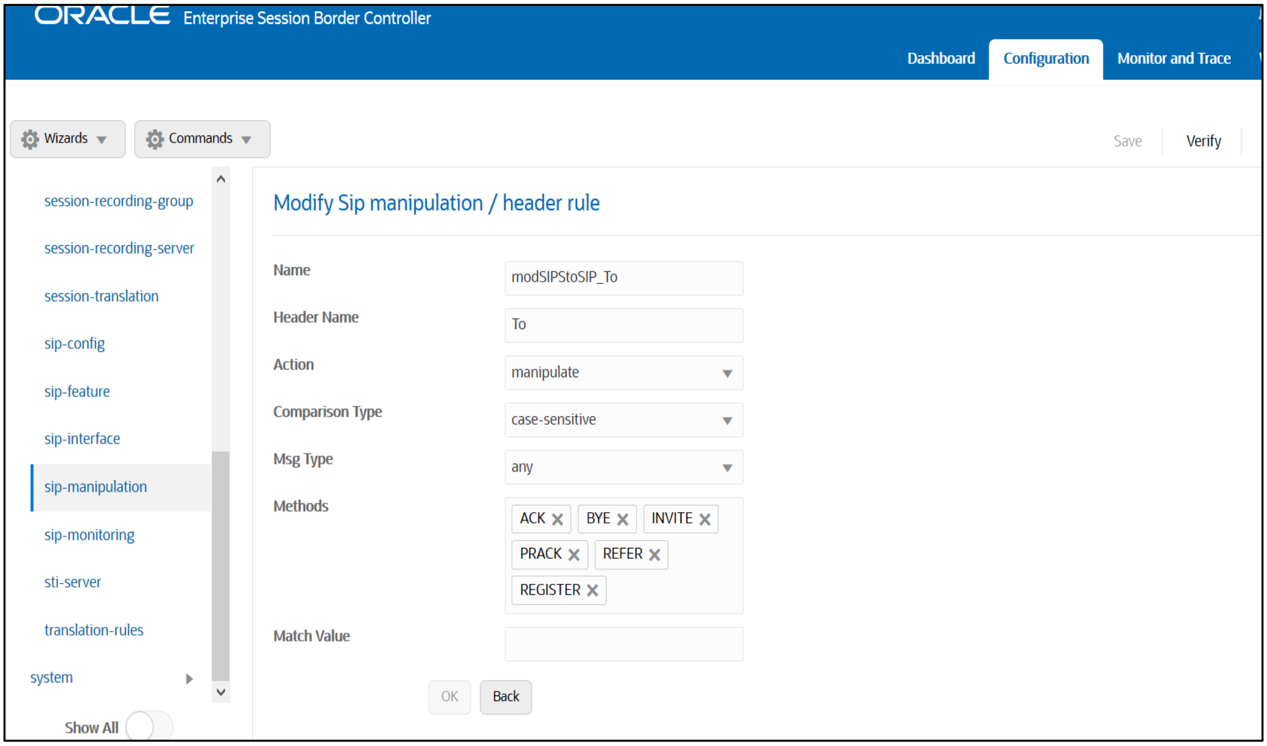
Name	modSIPStoSIP_Contact
Header Name	Contact
Action	manipulate
Comparison Type	case-sensitive
Msg Type	any
Methods	ACK, BYE, INVITE, PRACK, REFER, REGISTER
Match Value	



Modify Sip manipulation / header rule / element rule

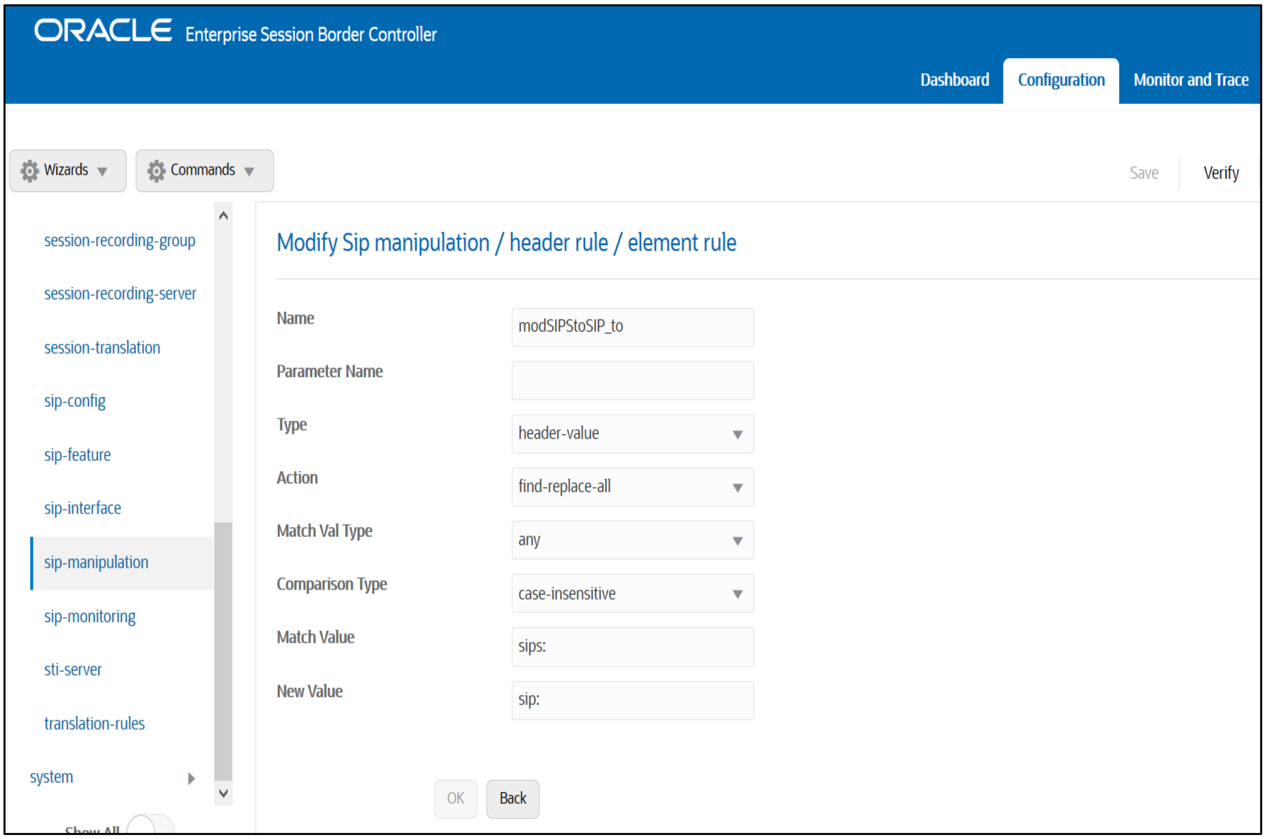
Name	modSIPStoSIP_contact
Parameter Name	
Type	header-value
Action	find-replace-all
Match Val Type	any
Comparison Type	case-insensitive
Match Value	sips:
New Value	sip:

Header Rule and Element Rule of To header.



Modify Sip manipulation / header rule

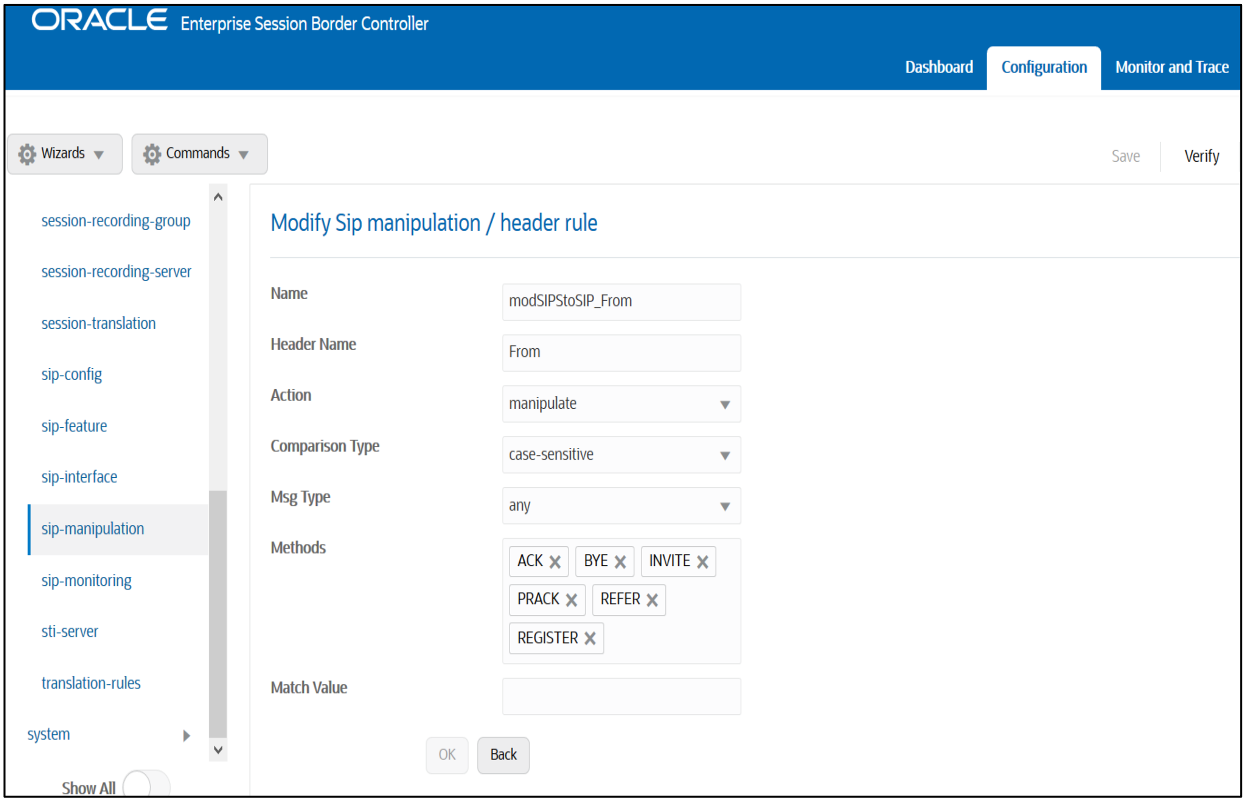
Name	modSIPStoSIP_To
Header Name	To
Action	manipulate
Comparison Type	case-sensitive
Msg Type	any
Methods	ACK ✕ BYE ✕ INVITE ✕ PRACK ✕ REFER ✕ REGISTER ✕
Match Value	



Modify Sip manipulation / header rule / element rule

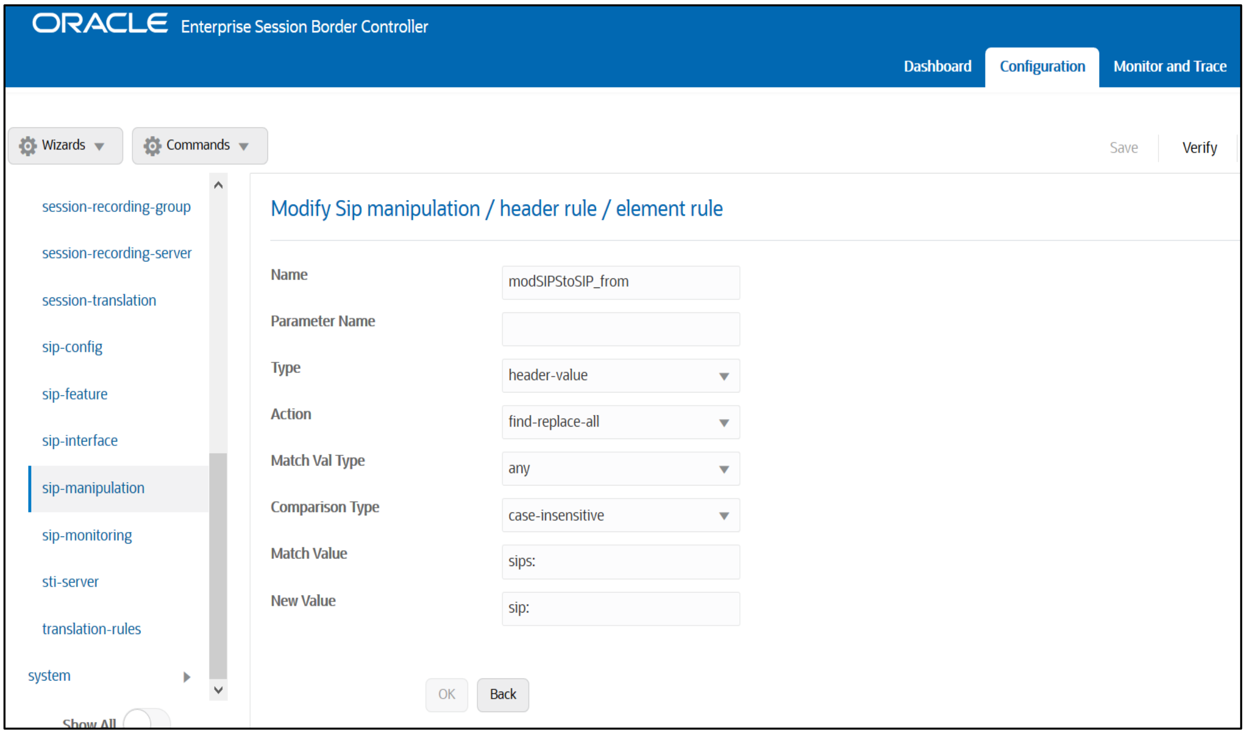
Name	modSIPStoSIP_to
Parameter Name	
Type	header-value
Action	find-replace-all
Match Val Type	any
Comparison Type	case-insensitive
Match Value	sips:
New Value	sip:

Header Rule and Element Rule of From header.



Modify Sip manipulation / header rule

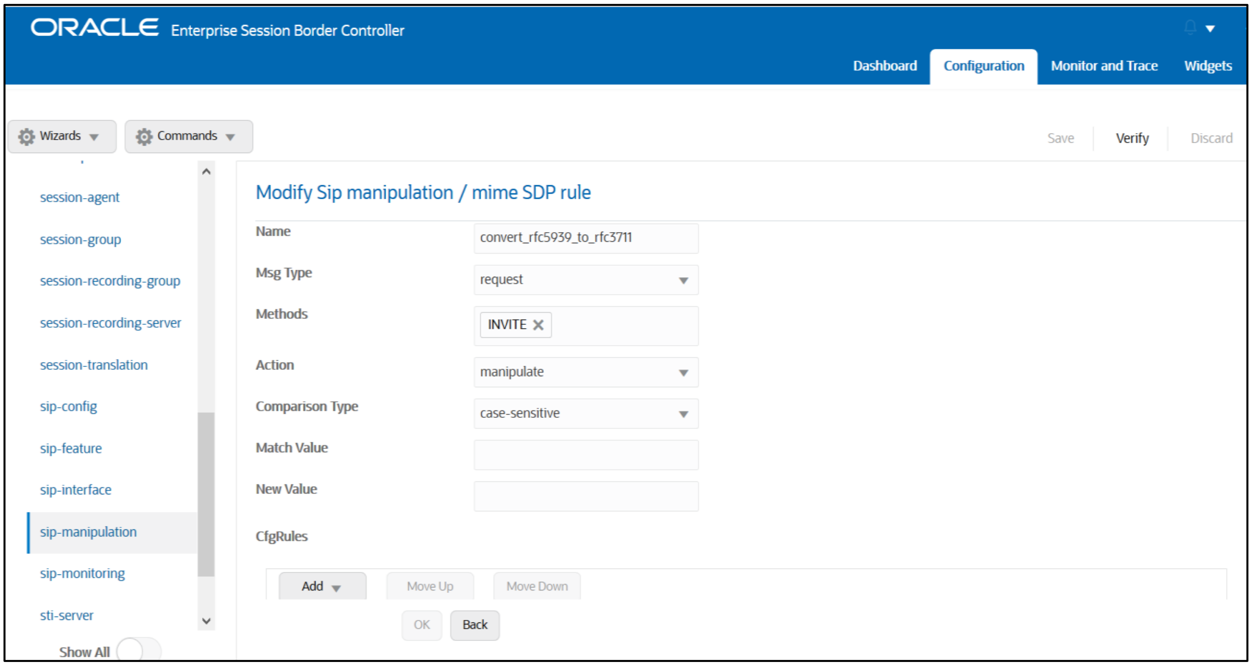
Name	modSIPStoSIP_From
Header Name	From
Action	manipulate
Comparison Type	case-sensitive
Msg Type	any
Methods	ACK ✕ BYE ✕ INVITE ✕ PRACK ✕ REFER ✕ REGISTER ✕
Match Value	



Modify Sip manipulation / header rule / element rule

Name	modSIPStoSIP_from
Parameter Name	
Type	header-value
Action	find-replace-all
Match Val Type	any
Comparison Type	case-insensitive
Match Value	sips:
New Value	sip:

Header Rule and Element Rule of mime-sdp-rule



Modify Sip manipulation / mime SDP rule

Name: convert_rfc5939_to_rfc3711

Msg Type: request

Methods: INVITE

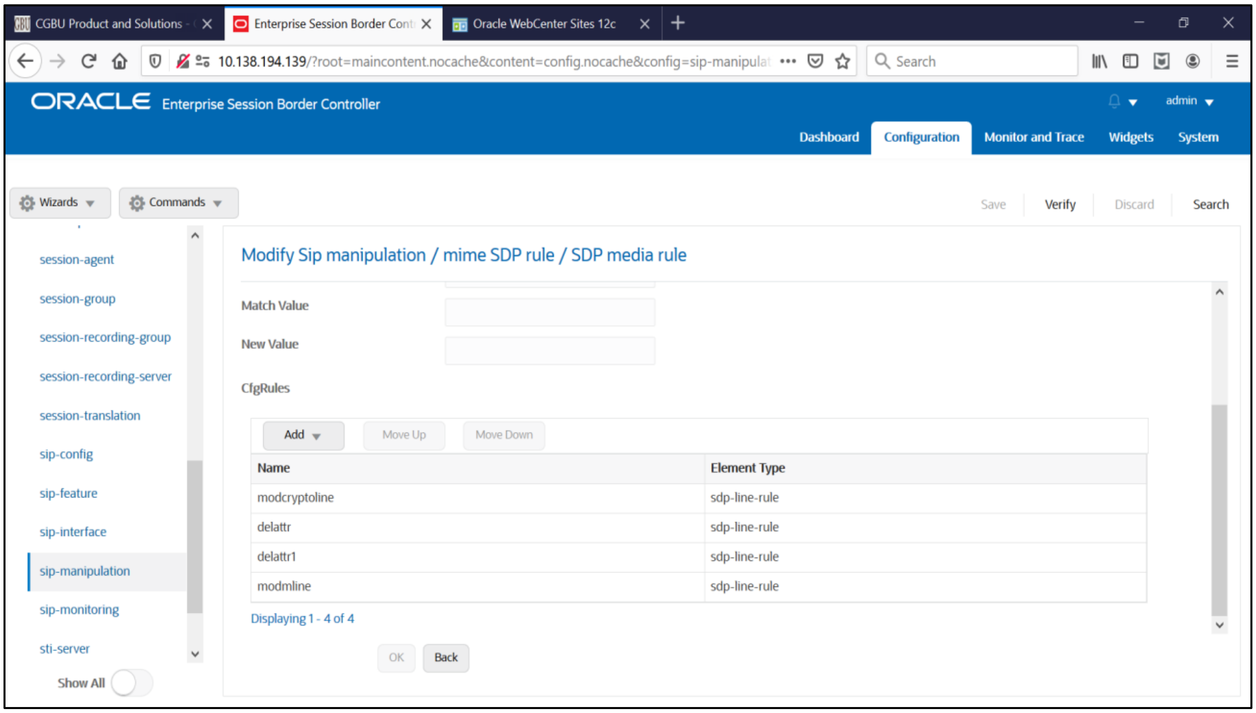
Action: manipulate

Comparison Type: case-sensitive

Match Value:

New Value:

CfgRules



Modify Sip manipulation / mime SDP rule / SDP media rule

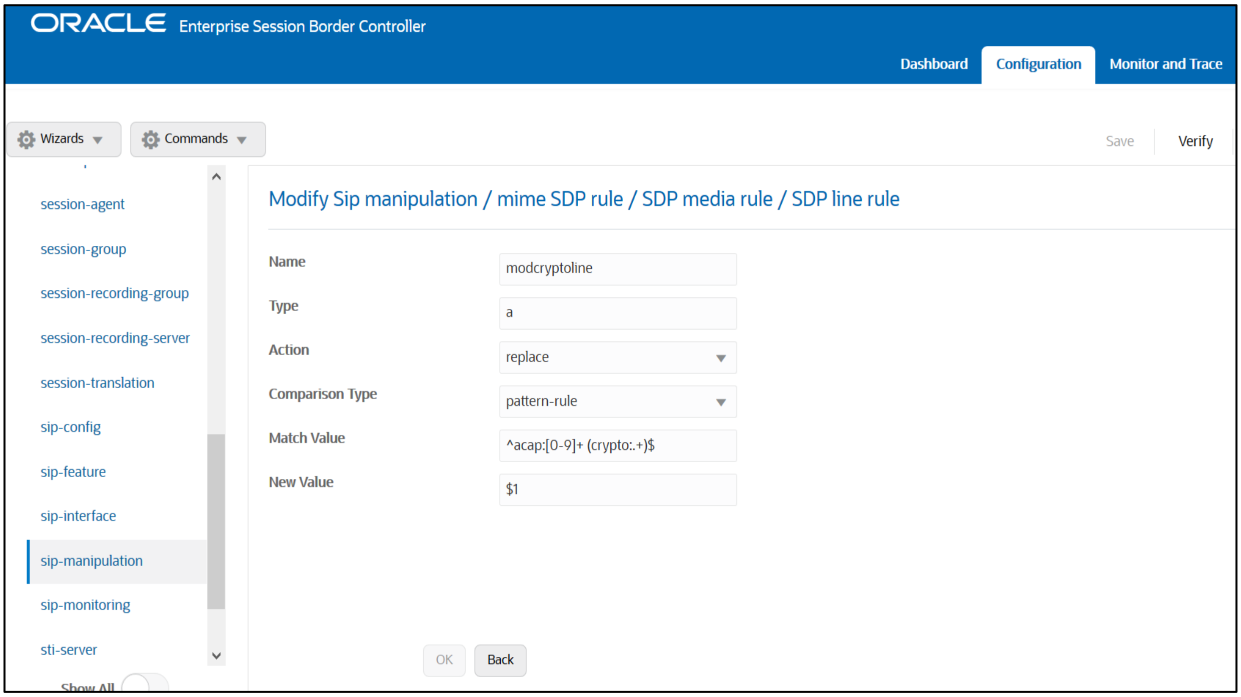
Match Value:

New Value:

CfgRules

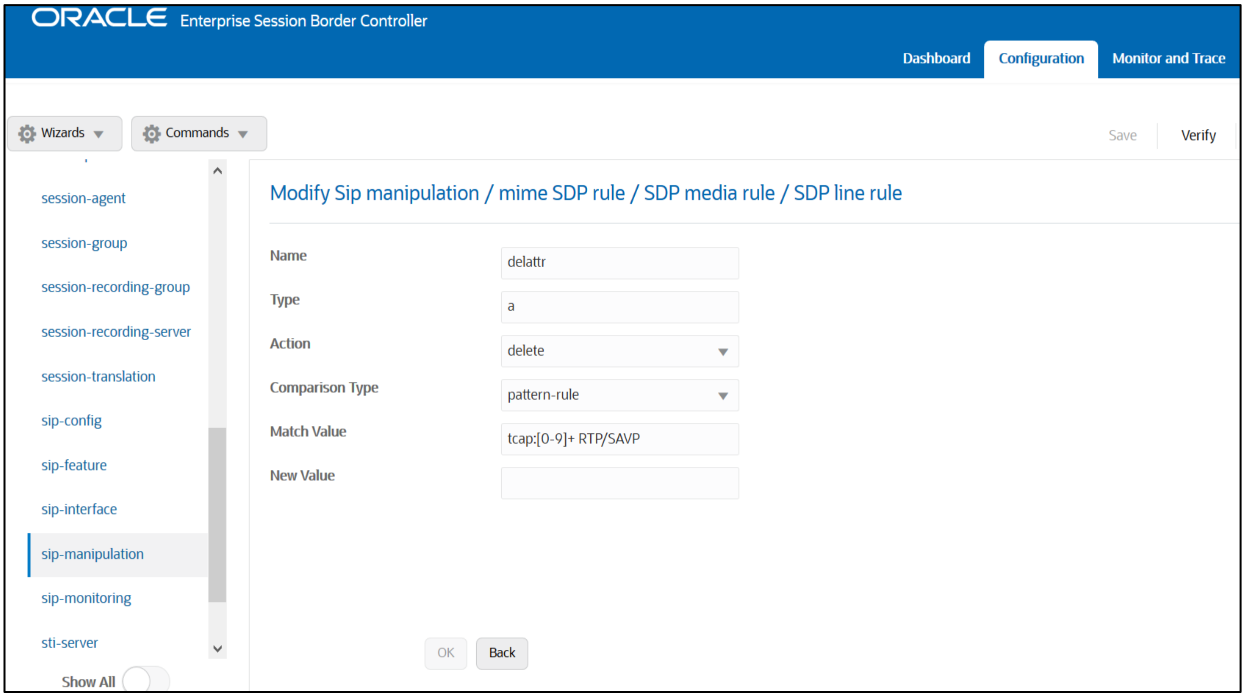
Name	Element Type
modcryptoline	sdp-line-rule
delattr	sdp-line-rule
delattr1	sdp-line-rule
modmline	sdp-line-rule

Displaying 1 - 4 of 4



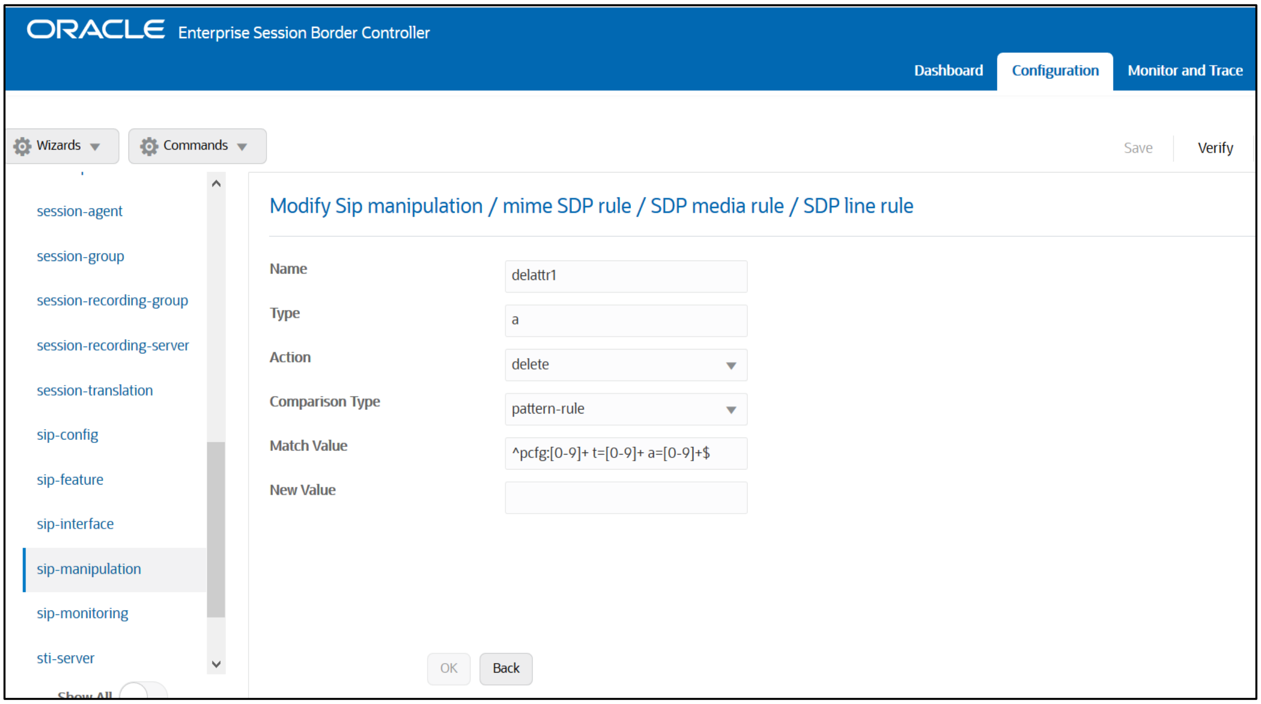
Modify Sip manipulation / mime SDP rule / SDP media rule / SDP line rule

Name	modcryptoline
Type	a
Action	replace
Comparison Type	pattern-rule
Match Value	^acap:[0-9]+ (crypto:.+)$
New Value	$1



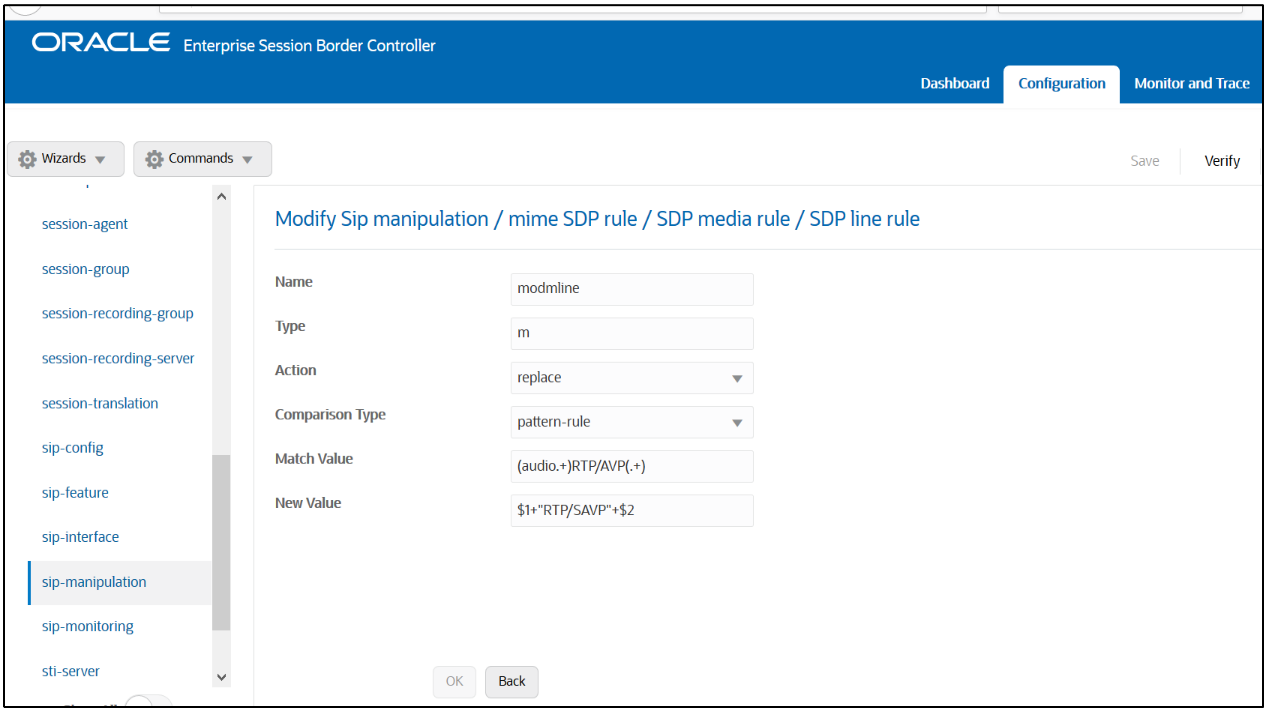
Modify Sip manipulation / mime SDP rule / SDP media rule / SDP line rule

Name	delattr
Type	a
Action	delete
Comparison Type	pattern-rule
Match Value	tcap:[0-9]+ RTP/SAVP
New Value	



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

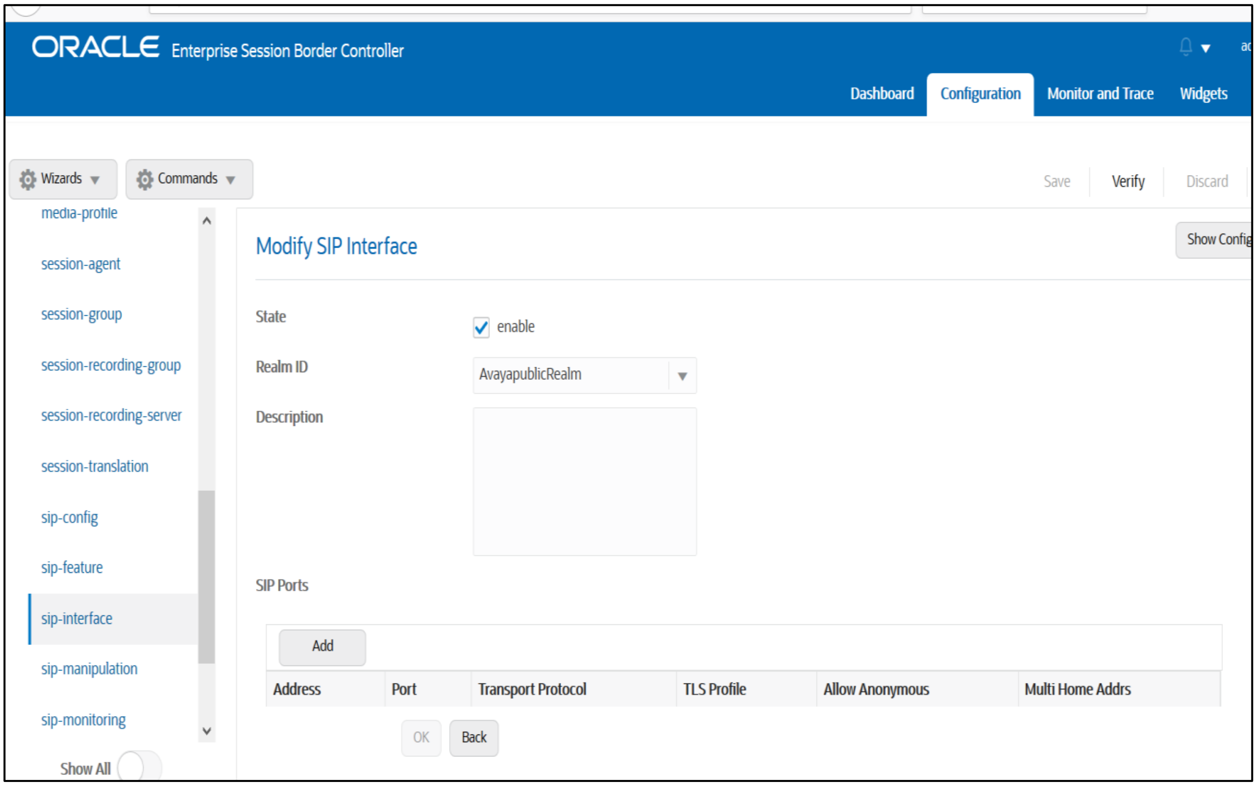
Name	delattr1
Type	a
Action	delete
Comparison Type	pattern-rule
Match Value	^pcfg:[0-9]+ t=[0-9]+ a=[0-9]+$
New Value	



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

Name	modmline
Type	m
Action	replace
Comparison Type	pattern-rule
Match Value	(audio.+)RTP/AVP(.+)
New Value	$1+"RTP/SAVP"+$2

Assign this sip manipulation sips2sip as InManipulationID to the access side SIP Interface.

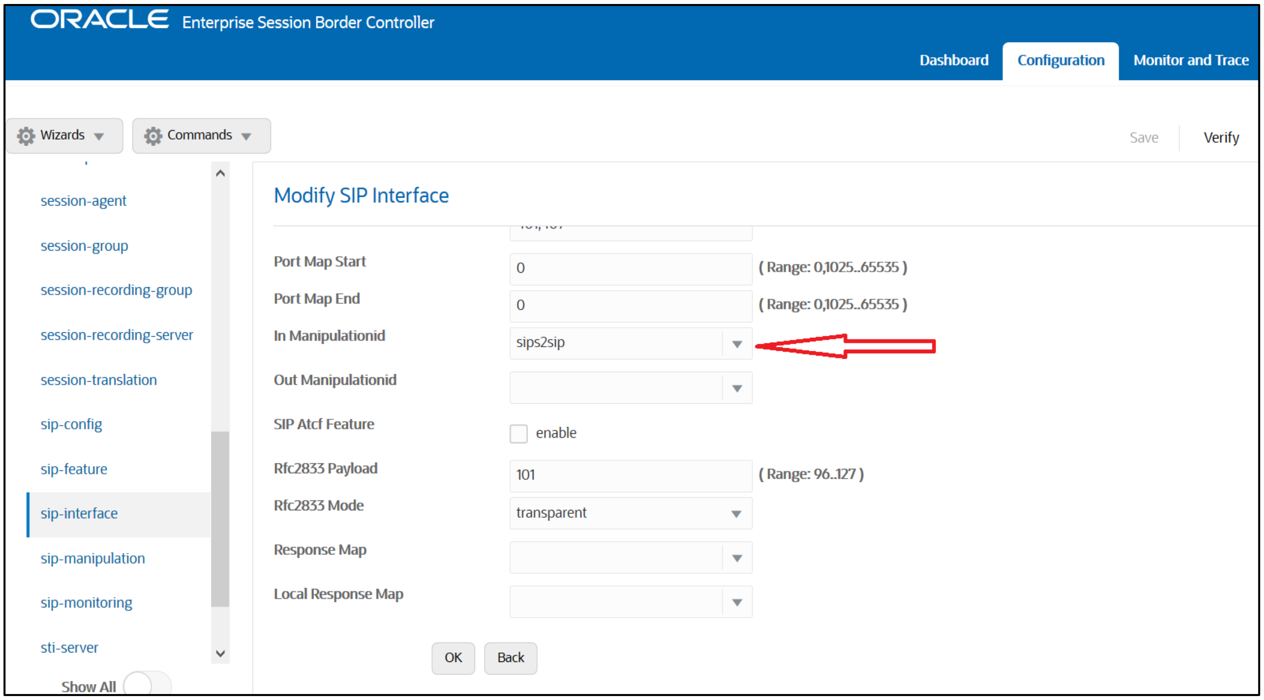


Modify SIP Interface

State	☑ enable
Realm ID	AvayapublicRealm
Description	

SIP Ports

Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs



Modify SIP Interface

Port Map Start	0	(Range: 0,1025..65535)
Port Map End	0	(Range: 0,1025..65535)
In Manipulationid	sips2sip	
Out Manipulationid		
SIP Atcf Feature	□ enable	
Rfc2833 Payload	101	(Range: 96..127)
Rfc2833 Mode	transparent	
Response Map		
Local Response Map		

With this, the SBC configuration is complete.

8. Existing SBC configuration

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

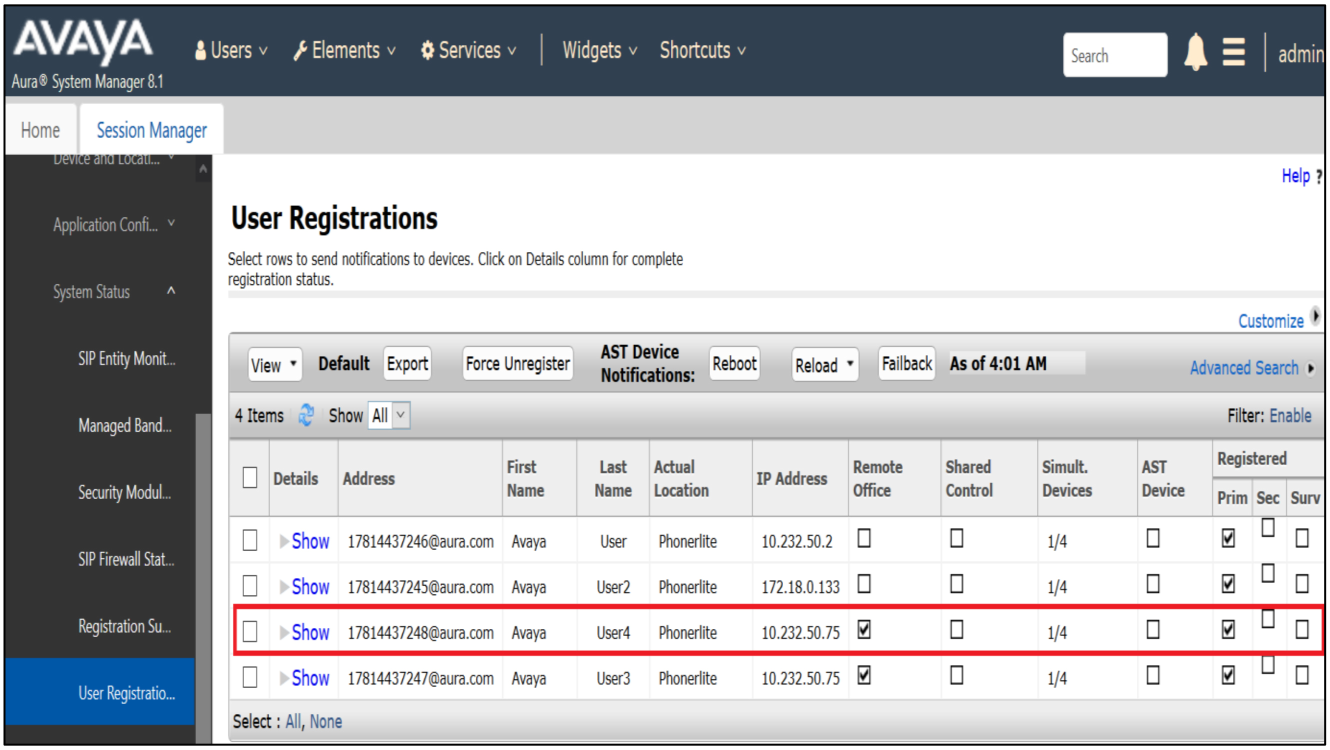
- New realm-config
- Configuring a certificate for SBC Interface
- TLS-Profile
- New sip-interface
- New session-agent
- HTTP-ALG
- New local-policy
- New steering-pools
- SDES Profile
- Media-sec-Policy
- SIP-Manipulations

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

9. Registration and Verification of Avaya Workspace Client for Windows Configuration

Once the SBC and Avaya Session Manager configuration is complete, we can try registering the Avaya Workplace client (17814437248 as DN) along with other remote phones and local phones and can verify whether they are successfully registered to the Avaya Session Manager.

Please Navigate to: Elements->Session Manager->System Status-> User registration.
Verify whether the users are registered successfully to the Session Manager.



User Registrations

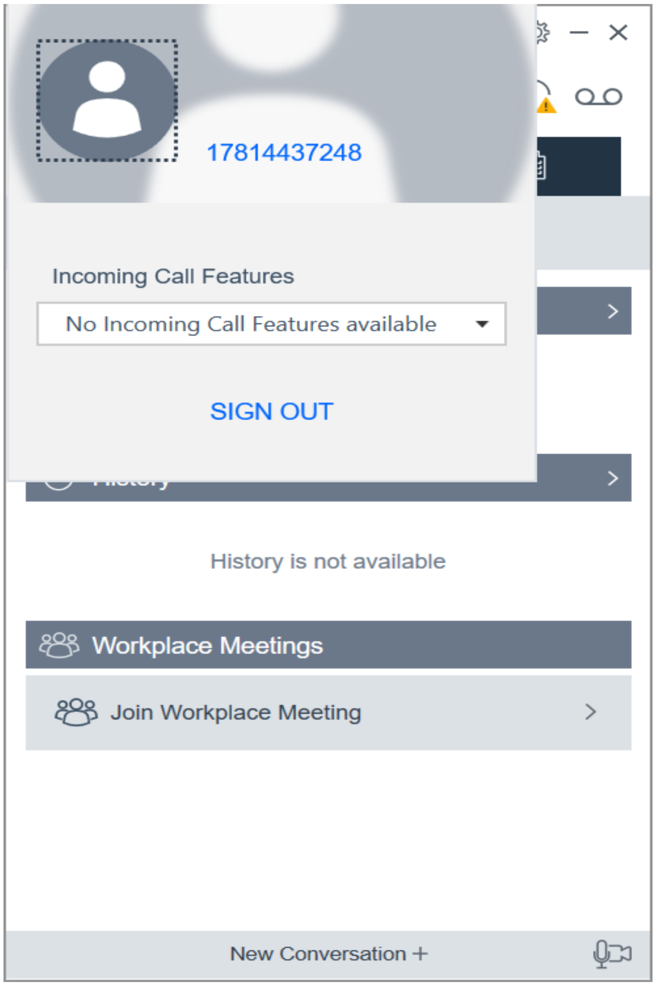
Select rows to send notifications to devices. Click on Details column for complete registration status.

□	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
											Prim	Sec	Surv
□	▸Show	17814437246@aura.com	Avaya	User	Phonerlite	10.232.50.2	□	□	1/4	□	☑	□	□
□	▸Show	17814437245@aura.com	Avaya	User2	Phonerlite	172.18.0.133	□	□	1/4	□	☑	□	□
□	▸Show	17814437248@aura.com	Avaya	User4	Phonerlite	10.232.50.75	☑	□	1/4	□	☑	□	□
□	▸Show	17814437247@aura.com	Avaya	User3	Phonerlite	10.232.50.75	☑	□	1/4	□	☑	□	□

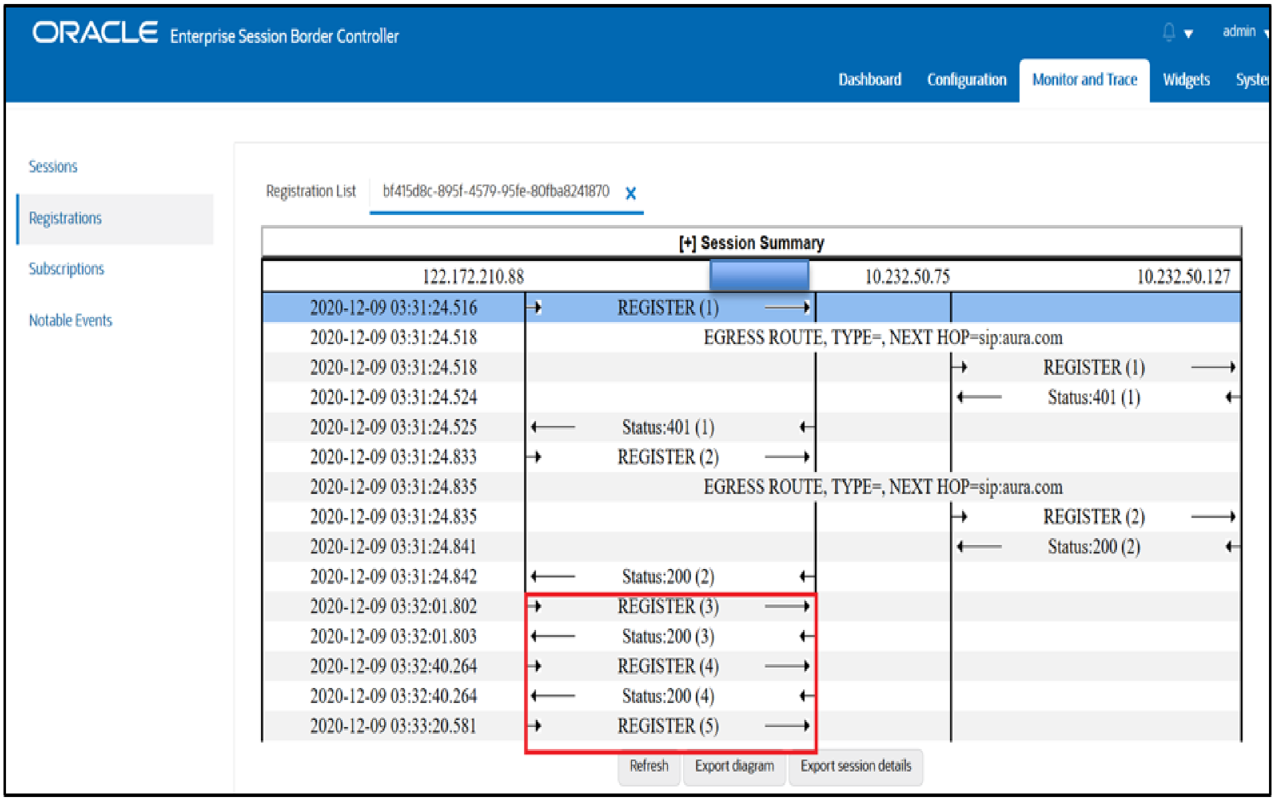
Select : All, None

As we can see, there are couple of DNs registered as Remote office phones which has the IP address of SBC inside IP (10.232.50.75) out of which Avaya Workplace client is one phone and these phones are registered via Oracle SBC to Avaya Session Manager. There are also two phones registered to Avaya Session Manager directly

As we are specifically testing Avaya Workplace soft client in this document, we can confirm that client is successfully registered to Avaya SM through Oracle SBC as shown below.

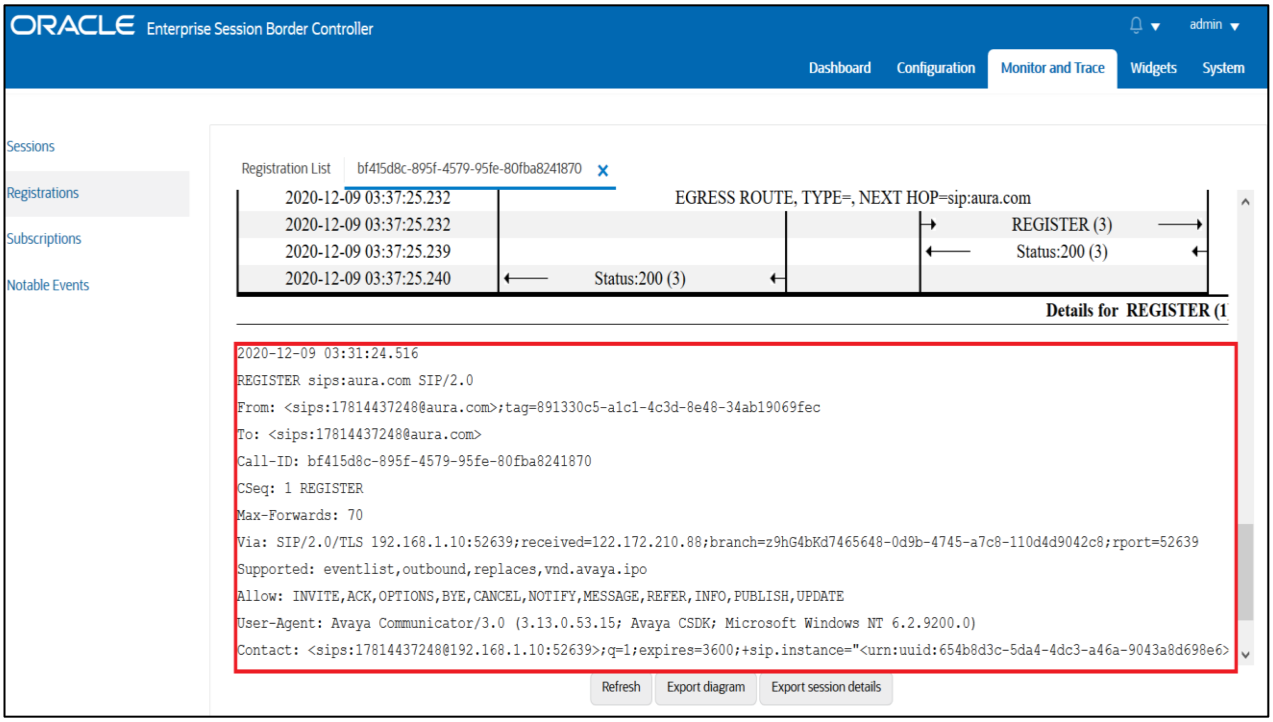


We can also see the registration flow below. We can see that REGISTER is successful and also SBC caches registration info. After that, register is directly answered by SBC instead of routing to Avaya SM till next expires time.



[+] Session Summary

	122.172.210.88	10.232.50.75	10.232.50.127
2020-12-09 03:31:24.516	→ REGISTER (1) →		
2020-12-09 03:31:24.518	EGRESS ROUTE, TYPE=, NEXT HOP=sip:aura.com		
2020-12-09 03:31:24.518		→ REGISTER (1) →	
2020-12-09 03:31:24.524		← Status:401 (1) ←	
2020-12-09 03:31:24.525	← Status:401 (1) ←		
2020-12-09 03:31:24.833	→ REGISTER (2) →		
2020-12-09 03:31:24.835	EGRESS ROUTE, TYPE=, NEXT HOP=sip:aura.com		
2020-12-09 03:31:24.835		→ REGISTER (2) →	
2020-12-09 03:31:24.841		← Status:200 (2) ←	
2020-12-09 03:31:24.842	← Status:200 (2) ←		
2020-12-09 03:32:01.802	→ REGISTER (3) →		
2020-12-09 03:32:01.803	← Status:200 (3) ←		
2020-12-09 03:32:40.264	→ REGISTER (4) →		
2020-12-09 03:32:40.264	← Status:200 (4) ←		
2020-12-09 03:33:20.581	→ REGISTER (5) →		

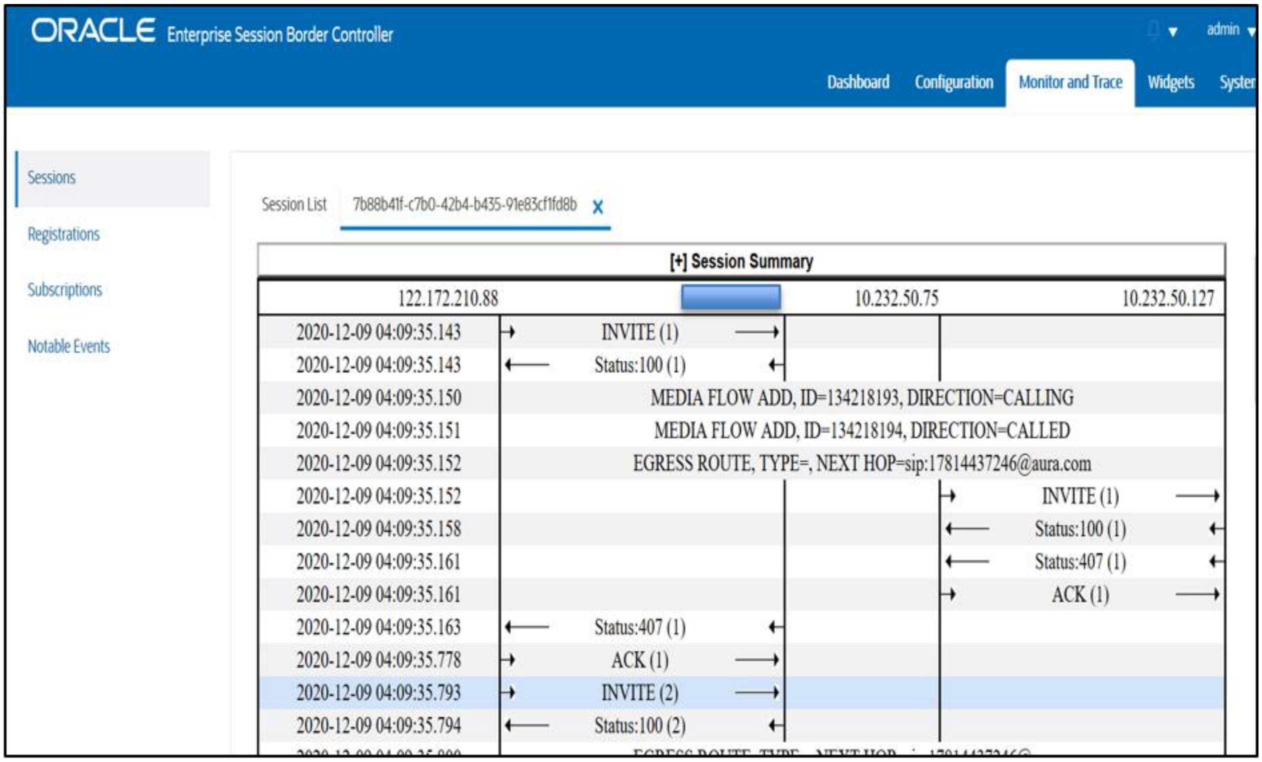


2020-12-09 03:37:25.232	EGRESS ROUTE, TYPE=, NEXT HOP=sip:aura.com		
2020-12-09 03:37:25.232		→ REGISTER (3) →	
2020-12-09 03:37:25.239		← Status:200 (3) ←	
2020-12-09 03:37:25.240	← Status:200 (3) ←		

Details for REGISTER (1

```
2020-12-09 03:31:24.516
REGISTER sips:aura.com SIP/2.0
From: <sips:17814437248@aura.com>;tag=891330c5-a1c1-4c3d-8e48-34ab19069fec
To: <sips:17814437248@aura.com>
Call-ID: bf415d8c-895f-4579-95fe-80fba8241870
CSeq: 1 REGISTER
Max-Forwards: 70
Via: SIP/2.0/TLS 192.168.1.10:52639;received=122.172.210.88;branch=z9hG4bKd7465648-0d9b-4745-a7c8-110d4d9042c8;rport=52639
Supported: eventlist,outbound,replaces,vnd.avaya.ipo
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
User-Agent: Avaya Communicator/3.0 (3.13.0.53.15; Avaya CSDK; Microsoft Windows NT 6.2.9200.0)
Contact: <sips:17814437248@192.168.1.10:52639>;q=1;expires=3600;+sip.instance="<urn:uuid:654b8d3c-5da4-4dc3-a46a-9043a8d698e6>
```

We can also make calls from Avaya Communicator Workplace soft client and we can verify the signaling path. The above call is made from access side to core side.



7b88b41f-c7b0-42b4-b435-91e83cf1fd8b

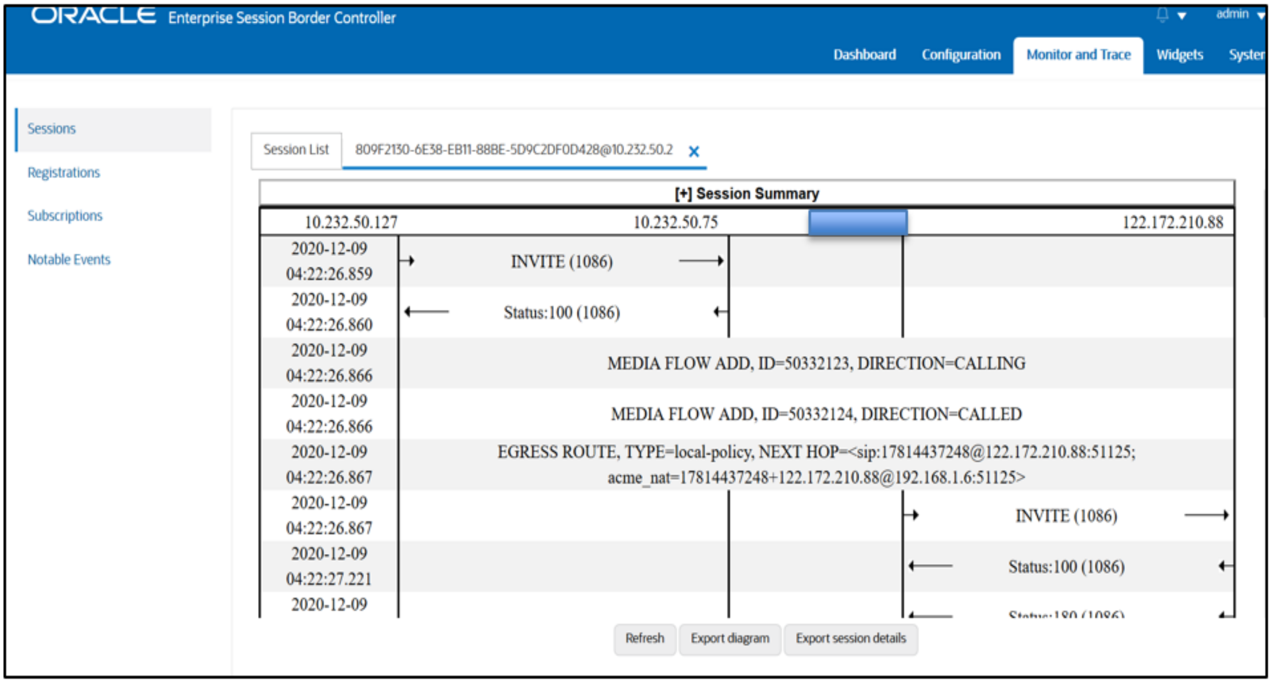
[+] Session Summary

122.172.210.88 | 10.232.50.75 | 10.232.50.127

2020-12-09 04:09:35.143 → INVITE (1) →
2020-12-09 04:09:35.143 ← Status:100 (1) ←
2020-12-09 04:09:35.150 MEDIA FLOW ADD, ID=134218193, DIRECTION=CALLING
2020-12-09 04:09:35.151 MEDIA FLOW ADD, ID=134218194, DIRECTION=CALLED
2020-12-09 04:09:35.152 EGRESS ROUTE, TYPE=, NEXT HOP=sip:17814437246@aura.com
2020-12-09 04:09:35.152 → INVITE (1) →
2020-12-09 04:09:35.158 ← Status:100 (1) ←
2020-12-09 04:09:35.161 ← Status:407 (1) ←
2020-12-09 04:09:35.161 → ACK (1) →
2020-12-09 04:09:35.163 ← Status:407 (1) ←
2020-12-09 04:09:35.778 → ACK (1) →
2020-12-09 04:09:35.793 → INVITE (2) →
2020-12-09 04:09:35.794 ← Status:100 (2) ←

Here the INVITE from access side comes with TLS protocol and from SBC it is changed to TCP/UDP

Similarly, we can also make calls from core side to access side and check the SIP path.
Here the call is converted to TLS after reaching SBC.



809F2130-6E38-EB11-88BE-5D9C2DF0D428@10.232.50.2

[+] Session Summary

10.232.50.127 | 10.232.50.75 | 122.172.210.88

2020-12-09 04:22:26.859 → INVITE (1086) →
2020-12-09 04:22:26.860 ← Status:100 (1086) ←
2020-12-09 04:22:26.866 MEDIA FLOW ADD, ID=50332123, DIRECTION=CALLING
2020-12-09 04:22:26.866 MEDIA FLOW ADD, ID=50332124, DIRECTION=CALLED
2020-12-09 04:22:26.867 EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:17814437248@122.172.210.88:51125;
acme_nat=17814437248+122.172.210.88@192.168.1.6:51125>
2020-12-09 04:22:26.867 → INVITE (1086) →
2020-12-09 04:22:27.221 ← Status:100 (1086) ←
2020-12-09 ← Status:180 (1086) ←

Appendix A

Following are the test cases that are executed as part of Avaya workspace client config and Avaya Session Manager with Oracle SBC in between. We get limited call options in manual mode and the Test cases that has been executed are listed below.

Note: Please note that the workspace client side is configured to work in TLS/SRTP mode (Avaya Workspace client to SBC) and Core side is configured to work in TCP/UDP mode (SBC to Avaya Session Manager). Call Merge or Conference option is not working in Avaya Workplace client and we cannot check this issue with Avaya as our SBC is not tested/certified by Avaya as supported SBC as of today.

Serial Number	Test Cases Executed	Result
1	Register Avaya Workspace client to Avaya Session manager via Oracle SBC	Pass
2	Outbound Call from Avaya Workspace client to other users, calling party hangs up after call	Pass
3	Outbound Call from Avaya Workspace client to other users, called party hangs up after call	Pass
4	Inbound Call to Avaya Workspace client from other user, calling party hangs up	Pass
5	Inbound Call to Avaya Workspace client from other user, called party hangs up	Pass
6	Outbound call from Avaya Workspace client and client CANCEL the call before call is established	Pass
7	Outbound Call from Avaya Workspace client to other user, answers the call, caller puts call on hold, then retrieves the call to ensure speech path is returned	Pass
8	Inbound call to Avaya Workspace client, answers the call, caller puts call on hold, then retrieve the call to ensure speech path is returned	Pass
9	Outbound Call from Avaya Workspace client phone to other device; Keep the call active for more than 30 minutes	Pass
10	Inbound Call to Avaya Workspace client and keep the call active for more than 30 minutes	Pass
11	Avaya Workspace client makes outbound call User A, User A attends the call and then Avaya Workspace client transfers the call to User B	Pass
12	User A calls inbound call to Avaya Workspace client and Avaya Workspace client attends the call and transfers to User B	Pass

10. Caveat

10.1. SRTP Call flow scenarios.

In some cases if we set **Mode to “any” for Inbound Media sec policy** as described in Section 7.17, the SRTP is not flowing towards the other side. To solve this issue, Use the given HMR **chg3711to5939** as **OutManipulationid** to the access side SIP Interface and then set the **Mode to “SRTP” for Inbound Media sec policy**. After making this change, the call works with TLS/SRTP both ways. The end user can add this HMR from the SBC GUI or through CLI according to their convenience. We have also provided the other HMR **sips2sip** config below for reference.

The configuration elements mentioned in this section maybe necessary to support SRTP exchanges between the client and the Oracle SBC (OCSBC). A protocol mismatch between the client and the OCSBC can result in unintelligible audio being experienced by both calling and called parties.

Calls from Client - SDP offers from the client may use RFC5939 to signal support for SRTP. One of the roles of HMR "**sips2sip**" (in this section) is to convert these SDP offers to RFC 3711 (i.e. a SRTP format currently supported by the OCSBC). HMR "**chg3711to5939**" presents SDP answers (from the OCSBC) as per RFC5939 to the client.

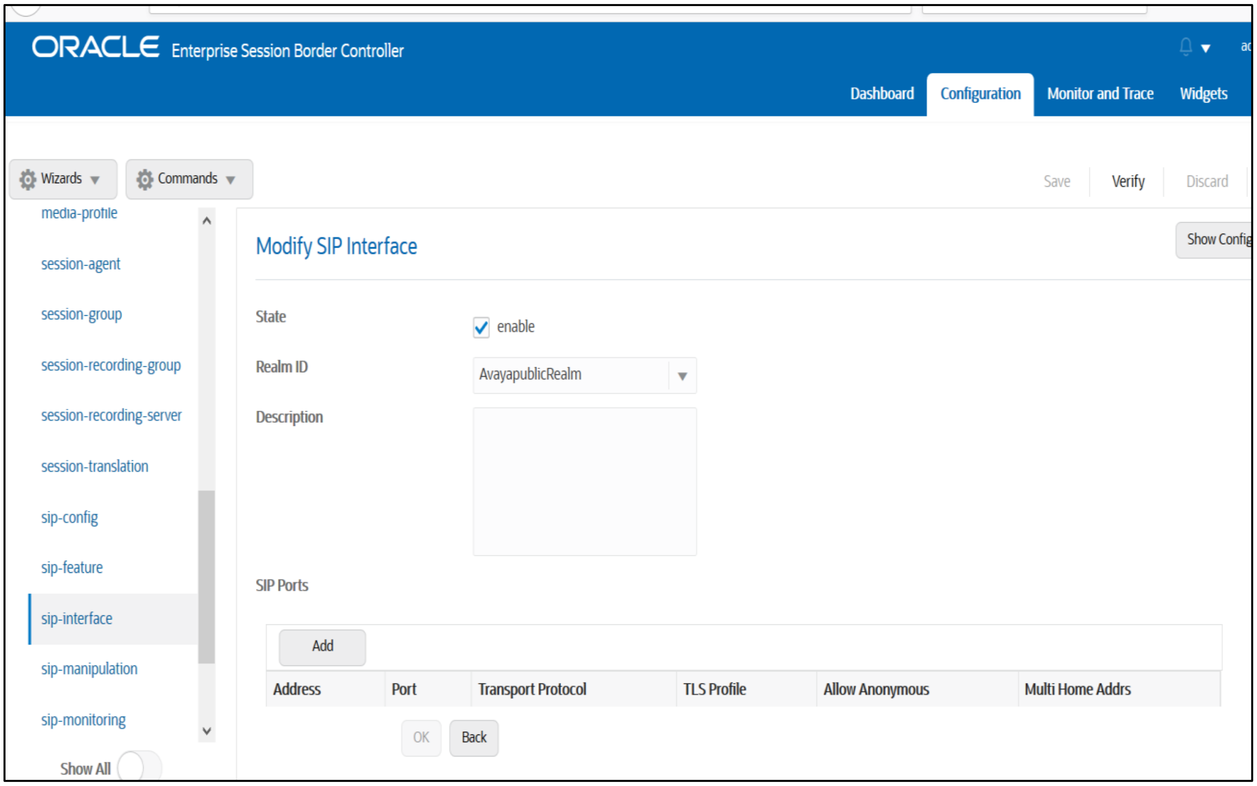
Calls to Client - SDP offers from the OCSBC are sent as RFC3711 to the client.
The client responds using RFC3711.

```
sip-manipulation
    name                      chg3711to5939
    mime-sdp-rule
            name                       modsdp
            msg-type                    reply
            methods                     INVITE
            action                    manipulate
            comparison-type               case-sensitive
            match-value
            new-value
            sdp-media-rule
                name                       modmline
                media-type                  audio
                action                    manipulate
                comparison-type               case-sensitive
                match-value
                new-value
                sdp-line-rule
                    name                       getacapvalue
                    type                      a
                    action                    store
                    comparison-type               pattern-rule
                    match-value                 ^crypto:([0-9]+)\s[\w\s\:\/]+
                    new-value
                sdp-line-rule
                    name                       addcfg
                    type                       a
                    action                    add
                    comparison-type          boolean
                    match-value              $modsdp.$modmline.$getacapvalue
```

```
                        new-value              acfg:+$modsdp.$modmline.$getacapvalue.$1
                                               +" t=1 a="+$modsdp.$modmline.$getacapvalue.$1

sip-manipulation
        name                        sips2sip
        description
        split-headers
        join-headers
        header-rule
                name                        modSIPStoSIP_ruri
                header-name                 Request-URI
                action                      manipulate
                comparison-type                 case-sensitive
                msg-type                      any
                methods                       ACK,BYE,INVITE,PRACK,REFER,REGISTER
                match-value
                new-value
                element-rule
                        name                        modSIPStoSIP_ruri
                        parameter-name
                        type                      header-value
                        action                    find-replace-all
                        match-val-type                  any
                        comparison-type                   case-insensitive
                        match-value                    sips:
                        new-value                     sip:
        header-rule
                name                        modSIPStoSIP_Contact
                header-name                      Contact
                action                      manipulate
                comparison-type                 case-sensitive
                msg-type                      any
                methods                       ACK,BYE,INVITE,PRACK,REFER,REGISTER
                match-value
                new-value
                element-rule
                        name                        modSIPStoSIP_contact
                        parameter-name
                        type                      header-value
                        action                    find-replace-all
                        match-val-type                  any
                        comparison-type                   case-insensitive
                        match-value                    sips:
                        new-value                     sip:
        header-rule
                name                        modSIPStoSIP_To
                header-name                      To
                action                      manipulate
                comparison-type                 case-sensitive
                msg-type                      any
                methods                       ACK,BYE,INVITE,PRACK,REFER,REGISTER
                match-value
                new-value
```

```
    element-rule
          name                          modSIPStoSIP_to
          parameter-name
          type                         header-value
          action                        find-replace-all
          match-val-type                   any
          comparison-type                   case-insensitive
          match-value                     sips:
          new-value                       sip:
header-rule
     name                          modSIPStoSIP_From
     header-name                      From
     action                       manipulate
     comparison-type                   case-sensitive
     msg-type                       any
     methods                        ACK,BYE,INVITE,PRACK,REFER,REGISTER
     match-value
     new-value
     element-rule
          name                          modSIPStoSIP_from
          parameter-name
          type                         header-value
          action                        find-replace-all
          match-val-type                   any
          comparison-type                   case-insensitive
          match-value                     sips:
          new-value                       sip:
mime-sdp-rule
     name                          convert_rfc5939_to_rfc3711
     msg-type                       request
     methods                        INVITE
     action                       manipulate
     comparison-type                   case-sensitive
     match-value
     new-value
     sdp-media-rule
          name                          modmline
          media-type                      audio
          action                        manipulate
          comparison-type                   case-sensitive
          match-value
          new-value
          sdp-line-rule
              name                          modcryptoline
              type                         a
              action                        replace
              comparison-type                   pattern-rule
              match-value                     ^acap:[0-9]+ (crypto:.+)$
              new-value                      $1
          sdp-line-rule
              name                          delattr
              type                         a
          action                    delete
          comparison-type                   pattern-rule
          match-value                    tcap:[0-9]+ RTP/SAVP
          new-value

sdp-line-rule
          name                       delattr1
          type                     a
          action                    delete
          comparison-type                   pattern-rule
          match-value                    ^pcfg:[0-9]+ t=[0-9]+ a=[0-9]+$
          new-value
  sdp-line-rule
          name                       modmline
          type                     m
          action                    replace
          comparison-type                   pattern-rule
          match-value                    (audio.+)RTP/AVP(.+)
          new-value                   $1+"RTP/SAVP"+$2
```

The screenshot of the particular config is given below for reference.



Modify SIP Interface

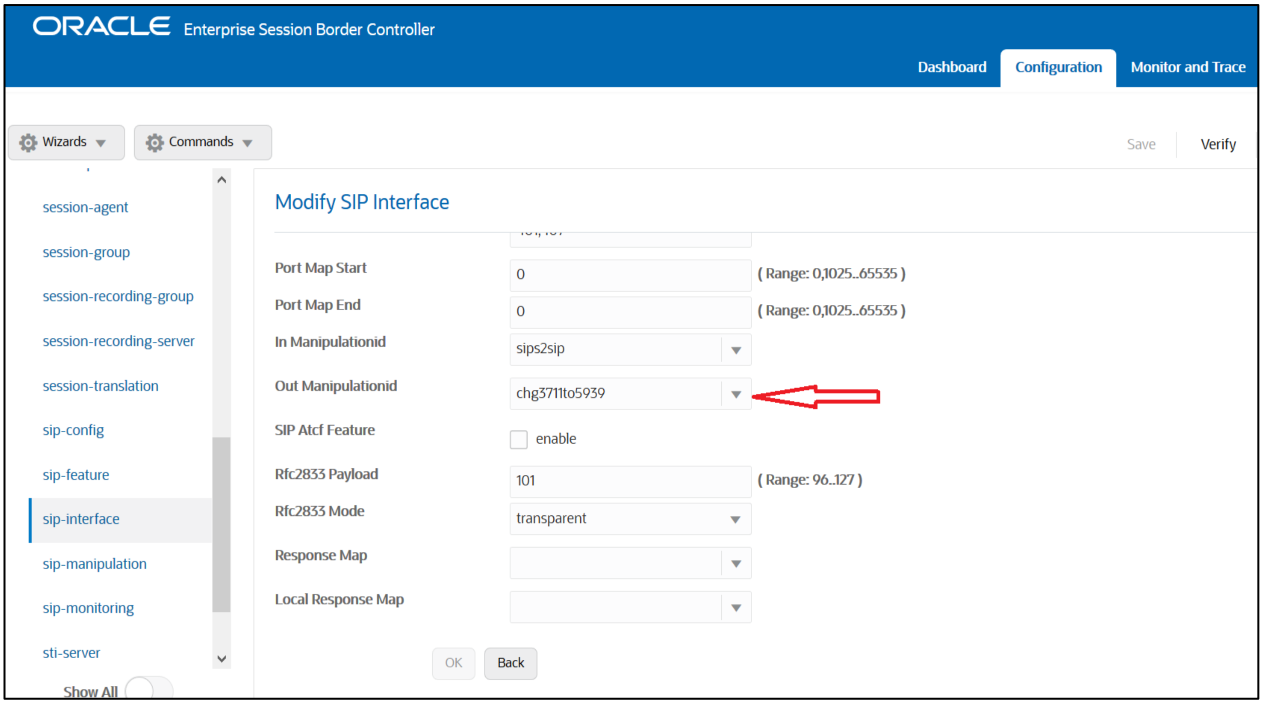
State ☑ enable

Realm ID AvayapublicRealm

Description

SIP Ports

Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs



Modify SIP Interface

Port Map Start	0	(Range: 0,1025..65535)
Port Map End	0	(Range: 0,1025..65535)
In Manipulationid	sips2sip	
Out Manipulationid	chg3711to5939	
SIP Atcf Feature	□ enable	
Rfc2833 Payload	101	(Range: 96..127)
Rfc2833 Mode	transparent	
Response Map		
Local Response Map		

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/Oracle/
- twitter.com/Oracle
- oracle.com

Integrated Cloud Applications & Platform Services