# Oracle SBC integration with Cisco CUCM 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 Cisco CUCM and Twilio Elastic SIP Trunking | 21st 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 with CUCM 12.5 and Oracle SBC 9.0 version | 23rd March 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 Cisco Call Manager (Cisco CUCM).

## 2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Twilio Elastic Sip Trunk with on premises Cisco CUCM. The solution contained within this document has been tested using Oracle Communication SBC with **OS840p4A** and **OS900p3**

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.

### 2.2. Cisco Call Manager (Cisco CUCM)

Cisco Unified Call Manager provides industry-leading reliability, security, scalability, efficiency, and enterprise call and session management and is the core call control application of the collaboration portfolio.

It should be noted that while this application note focuses on the optimal configurations for the Oracle SBC in an enterprise Cisco CUCM 11.5 / CUCM 12.5 environment, the same SBC configuration model can also be used for other enterprise applications with a few tweaks to the configuration for required features.

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

For additional information on CUCM 11.5 and CUCM 12.5, please visit

https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-version-11-5/index.html

https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-version-12-5/index.html

**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 Cisco CUCM 11.5 / CUCM 12.5 version using Oracle Enterprise SBC. There will be steps that require navigating the CUCM 11.5 / CUCM 12.5 server configuration, Oracle SBC GUI interface, understanding the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

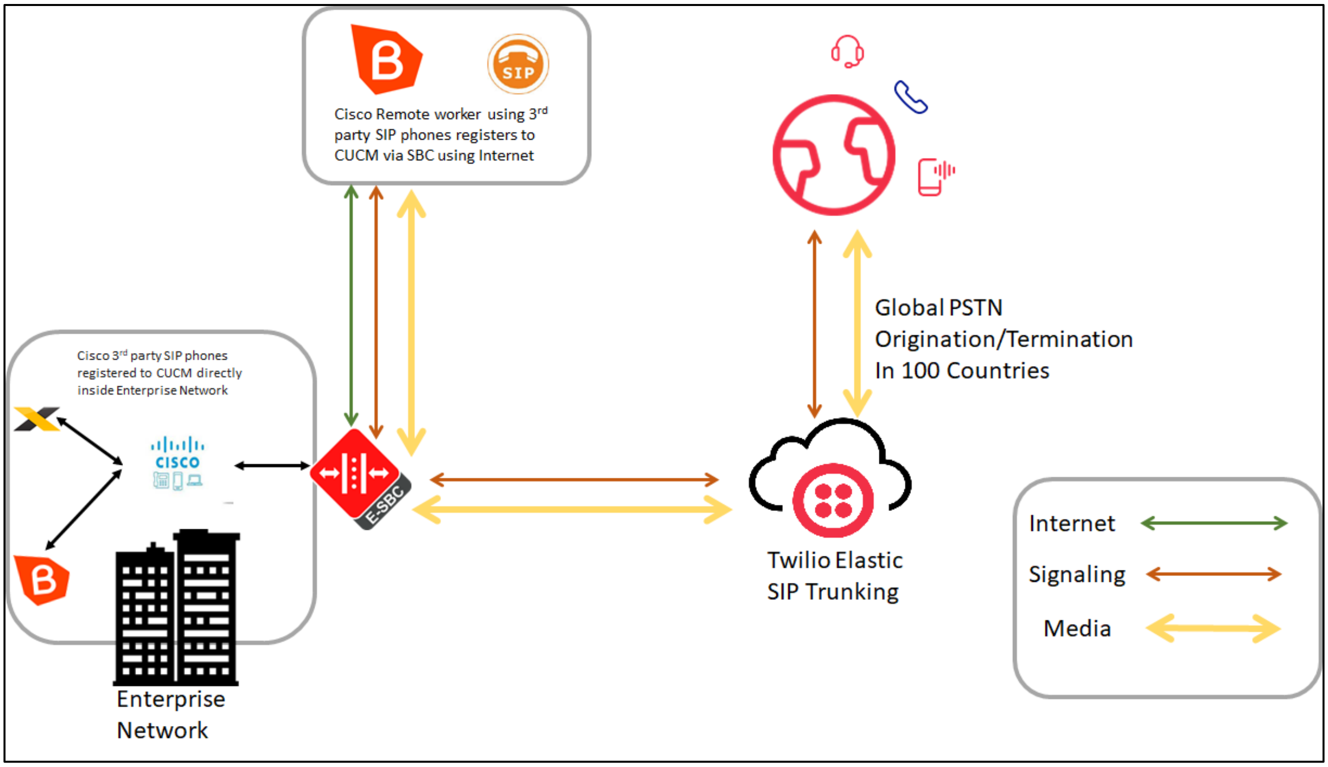
### 3.2. Requirements

- Fully functioning Cisco CUCM 11.5 / CUCM 12.5
- 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 | Cisco CUCM Version |
|---|---|---|
| Revision 1 | 8.4.0 | 11.5 |
| Revision 2 | 9.0.0 | 12.5 |

### 3.3. Architecture

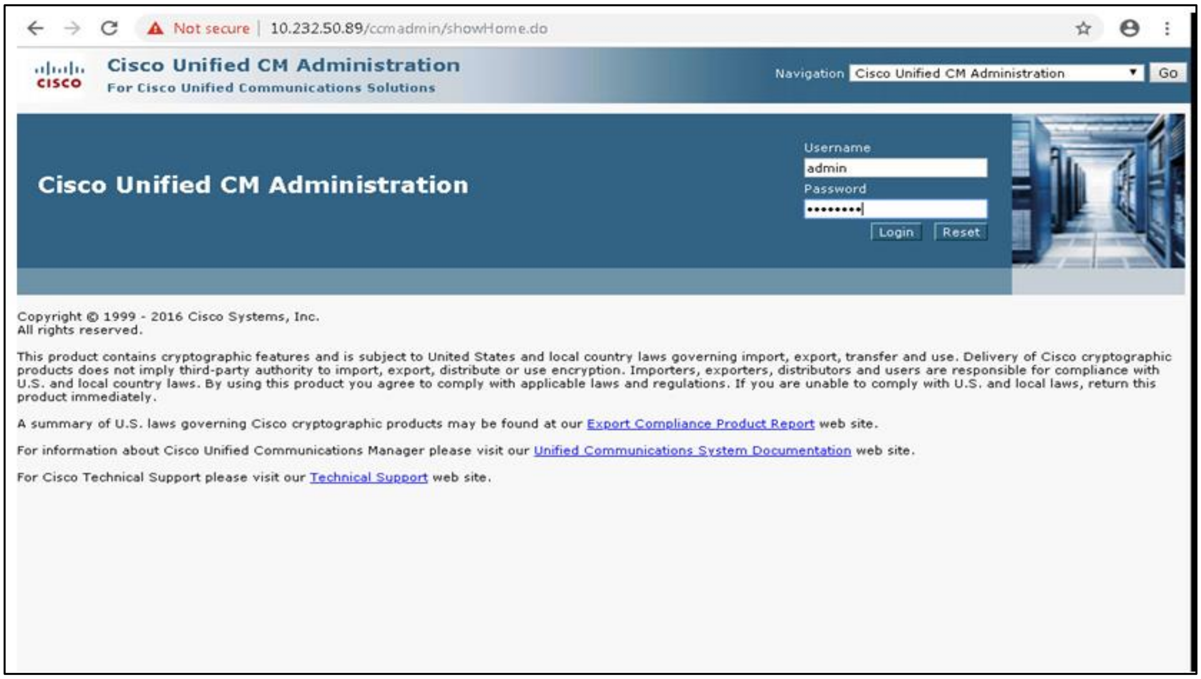

Cisco Remote worker using 3rd party SIP phones registers to CUCM via SBC using Internet
SIP
Cisco 3rd party SIP phones registered to CUCM directly inside Enterprise Network
cisco
E-SBC
Enterprise Network
Global PSTN Origination/Termination In 100 Countries
Twilio Elastic SIP Trunking
Internet
Signaling
Media

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

- Phase 1 – Configuring the Cisco Unified Call Manager v11.5 / V 12.5 for Oracle SBC.
- Phase 2 – Configuring the Oracle SBC.
- Phase 3 – Configuring the Twilio Elastic SIP Trunk

# 4. Configuring the Cisco Call Manager (Cisco CUCM)

Please login to Cisco CUCM admin web GUI with proper login credentials (Username and password). After that, perform the steps below in the given order.


Not secure | 10.232.50.89/ccmadmin/showHome.do
cisco
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
Go
Cisco Unified CM Administration
Login
Reset

Username admin

Password ••••••••

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

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

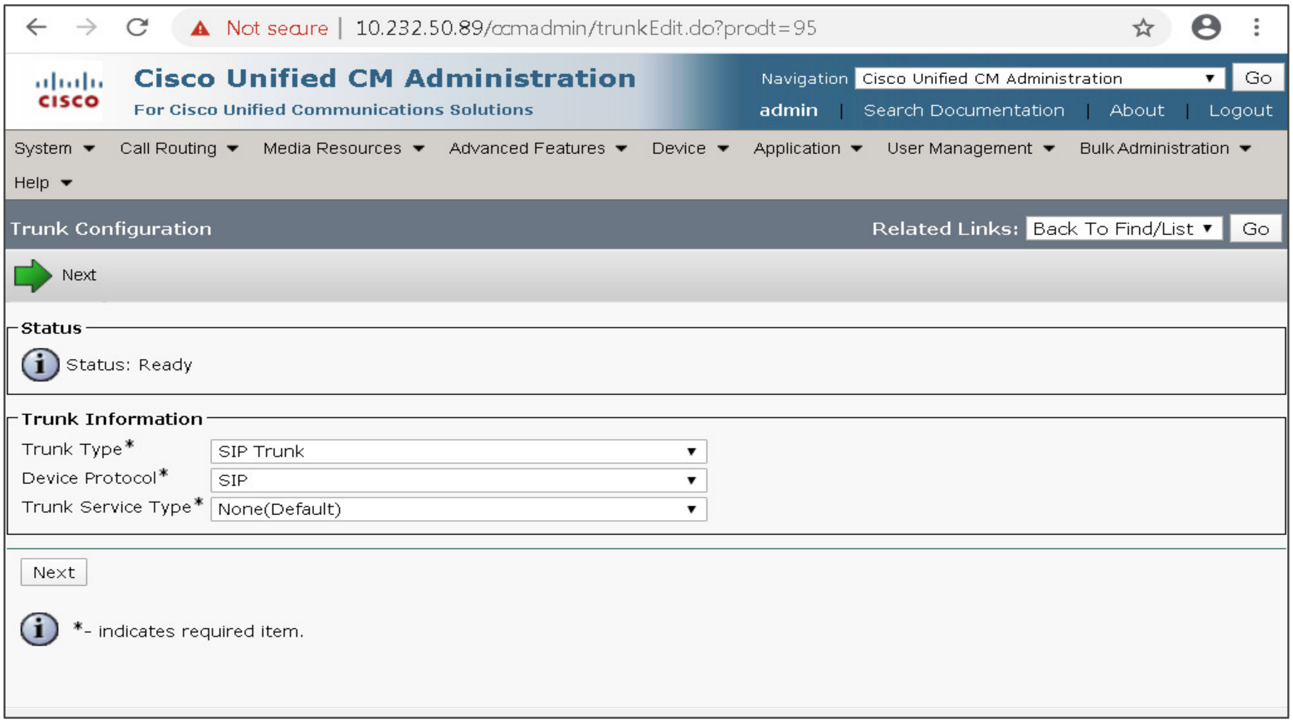
A summary of U.S. laws governing Cisco cryptographic products may be found at our Export Compliance Product Report web site.

For information about Cisco Unified Communications Manager please visit our Unified Communications System Documentation web site.

For Cisco Technical Support please visit our Technical Support web site.

## 4.1. Configuring a new SIP Trunk

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



Not secure | 10.232.50.89/ccmadmin/trunkEdit.do?prodt=95
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Related Links: Back To Find/List Go
Next

Trunk Configuration

Status

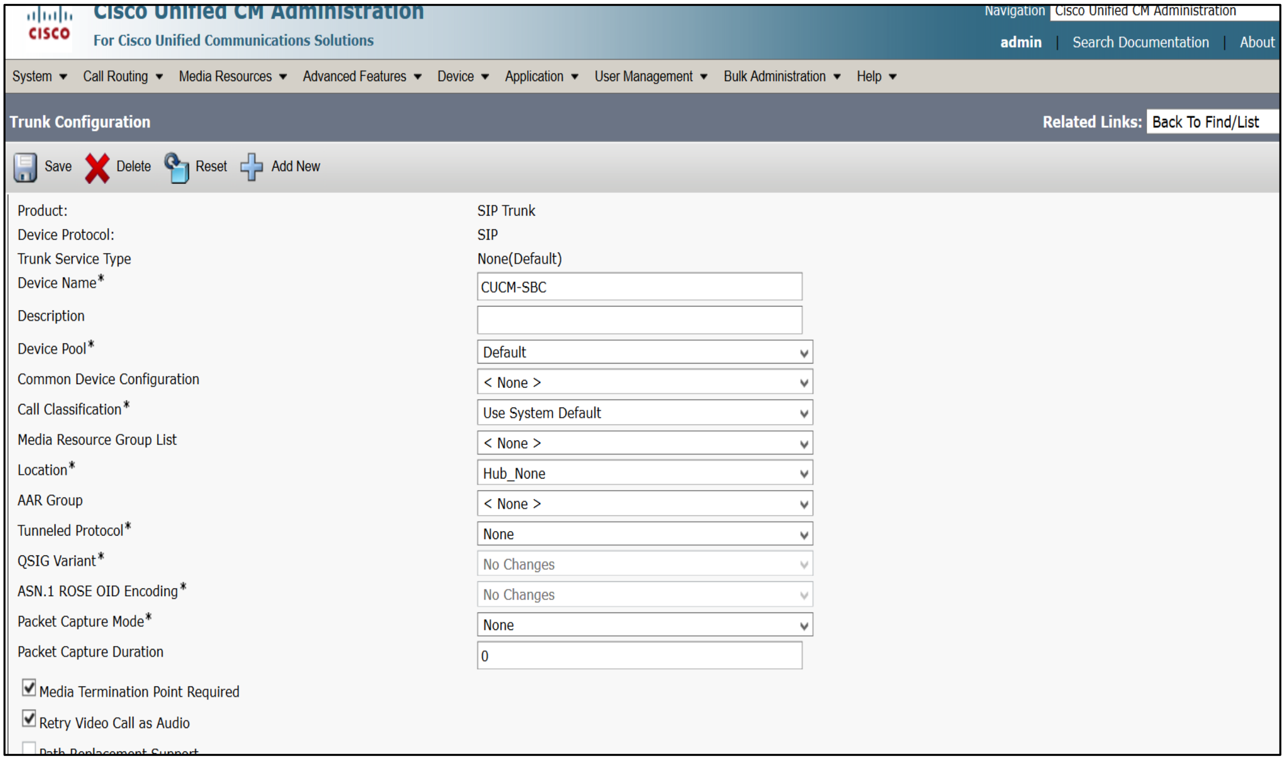
Status: Ready

Trunk Information

| | |
|---|---|
| Trunk Type* | SIP Trunk |
| Device Protocol* | SIP |
| Trunk Service Type* | None(Default) |

Next

*- indicates required item.



Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
admin | Search Documentation | About
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Related Links: Back To Find/List
Save Delete Reset Add New

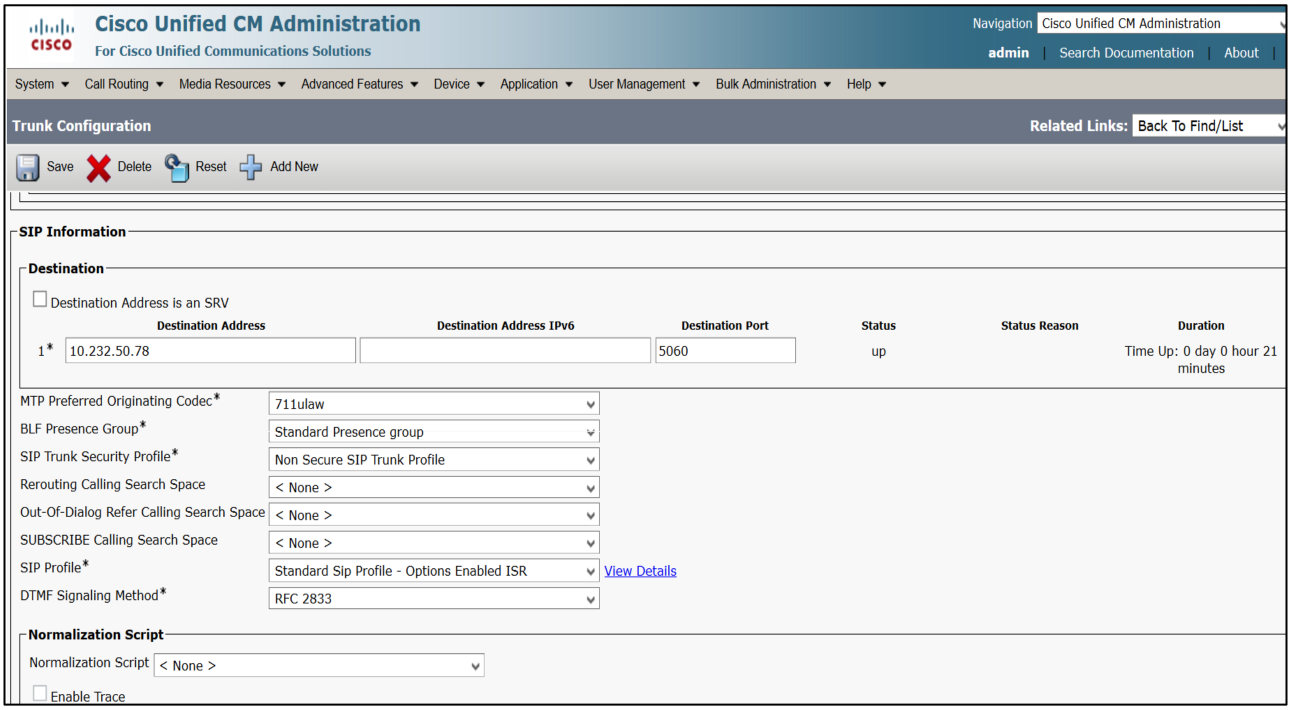
Trunk Configuration

| | |
|---|---|
| Product: | SIP Trunk |
| Device Protocol: | SIP |
| Trunk Service Type | None(Default) |
| Device Name* | CUCM-SBC |
| Description | |
| Device Pool* | Default |
| Common Device Configuration | < None > |
| Call Classification* | Use System Default |
| Media Resource Group List | < None > |
| Location* | Hub_None |
| AAR Group | < None > |
| Tunneled Protocol* | None |
| QSIG Variant* | No Changes |
| ASN.1 ROSE OID Encoding* | No Changes |
| Packet Capture Mode* | None |
| Packet Capture Duration | 0 |

☑ Media Termination Point Required

☑ Retry Video Call as Audio

□ Path Replacement Support


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
admin | Search Documentation | About |
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
Trunk Configuration
Related Links: Back To Find/List
Save Delete Reset Add New

**SIP Information**

**Destination**

□ Destination Address is an SRV

|  | Destination Address | Destination Address IPv6 | Destination Port | Status | Status Reason | Duration |
|---|---|---|---|---|---|---|
| 1* | 10.232.50.78 |  | 5060 | up |  | Time Up: 0 day 0 hour 21 minutes |

|  |  |
|---|---|
| MTP Preferred Originating Codec* | 711ulaw |
| BLF Presence Group* | Standard Presence group |
| SIP Trunk Security Profile* | Non Secure SIP Trunk Profile |
| Rerouting Calling Search Space | < None > |
| Out-Of-Dialog Refer Calling Search Space | < None > |
| SUBSCRIBE Calling Search Space | < None > |
| SIP Profile* | Standard Sip Profile - Options Enabled ISR View Details |
| DTMF Signaling Method* | RFC 2833 |

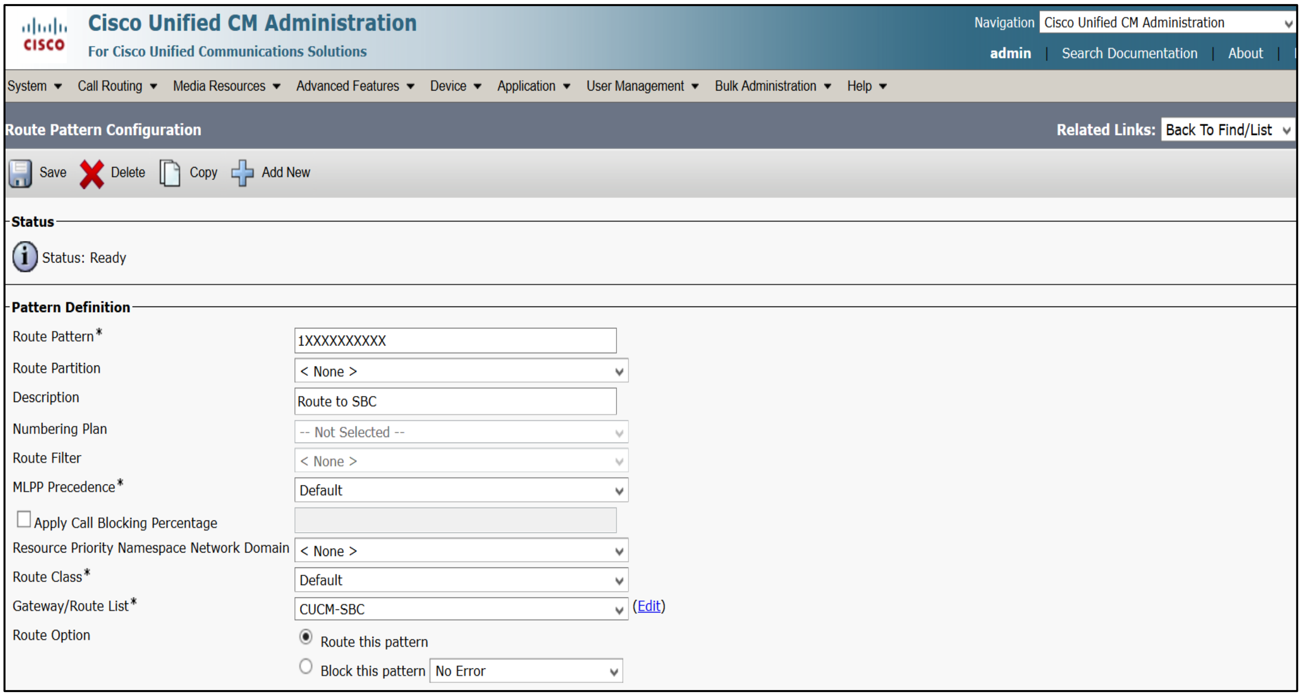
**Normalization Script**

Normalization Script < None >

□ Enable Trace

## 4.2. Configure a new Route Pattern

01) Go to Call Routing ------ Route/Hunt ------ Route Pattern and click Add New
02) Enter a Route Pattern according to the network requirements and calling plan.
03) From the Gateway/Route List drop-down list, select the created SIP Trunk device name.
04) Click Save. We can create other route patterns in the same way as shown below.


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
admin | Search Documentation | About |
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
Route Pattern Configuration
Related Links: Back To Find/List
Save Delete Copy Add New

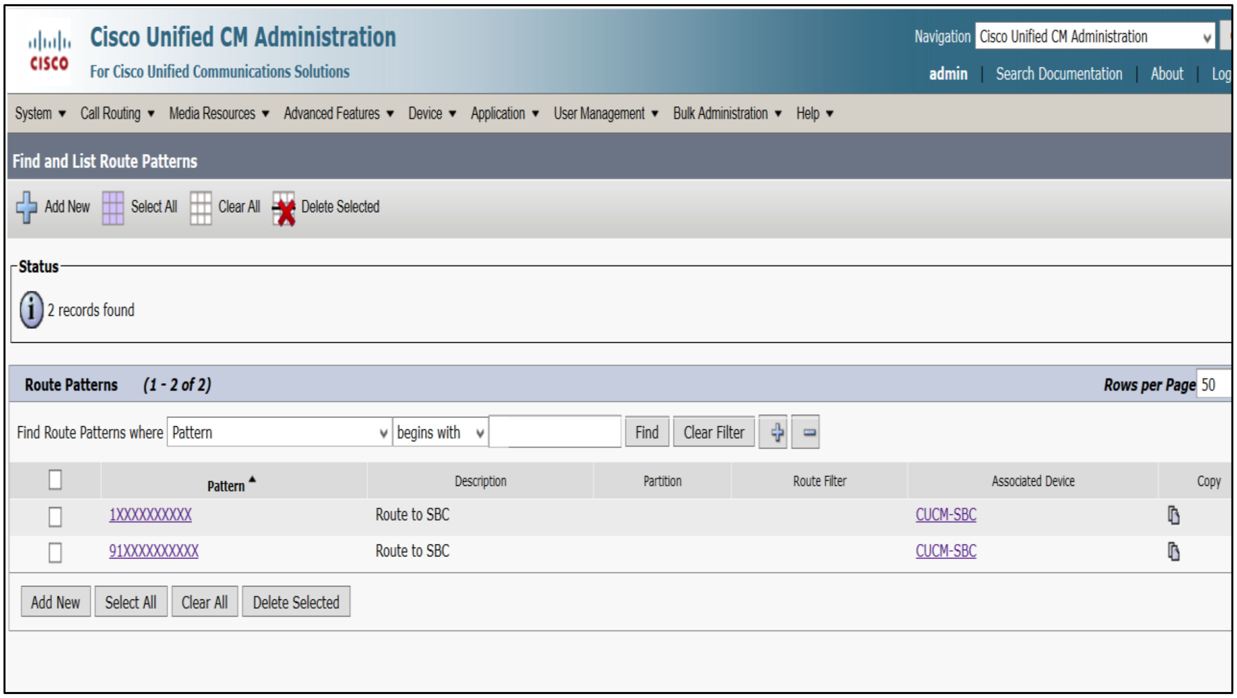
**Status**

Status: Ready

**Pattern Definition**

|  |  |
|---|---|
| Route Pattern* | 1XXXXXXXXXX |
| Route Partition | < None > |
| Description | Route to SBC |
| Numbering Plan | -- Not Selected -- |
| Route Filter | < None > |
| MLPP Precedence* | Default |
| □ Apply Call Blocking Percentage |  |
| Resource Priority Namespace Network Domain | < None > |
| Route Class* | Default |
| Gateway/Route List* | CUCM-SBC (Edit) |
| Route Option | ● Route this pattern<br>○ Block this pattern No Error |

The route patterns that has been created is shown below:


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
admin | Search Documentation | About | Log
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
Add New
Select All
Clear All
Delete Selected
Find
Clear Filter
Add New
Select All
Clear All
Delete Selected

Find and List Route Patterns

Status

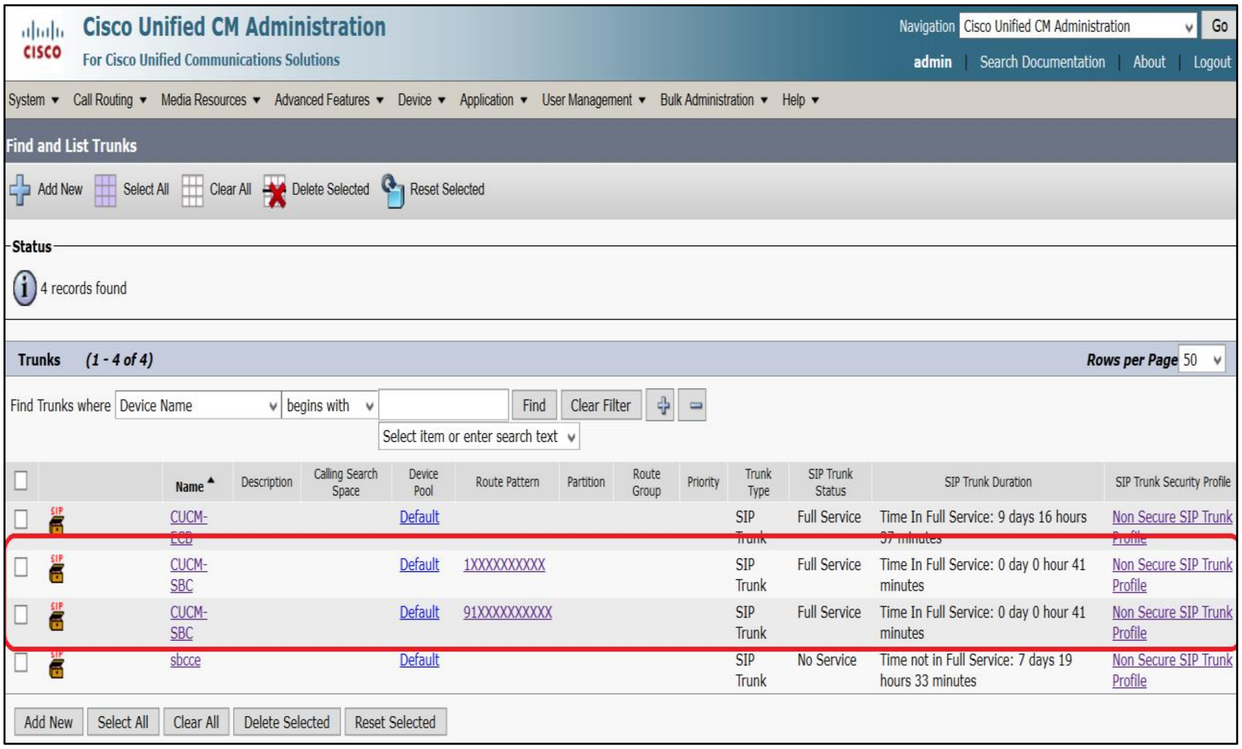
2 records found

Route Patterns (1 - 2 of 2) Rows per Page 50

Find Route Patterns where Pattern begins with

| □ | Pattern ▲ | Description | Partition | Route Filter | Associated Device | Copy |
|---|---|---|---|---|---|---|
| □ | 1XXXXXXXXXX | Route to SBC | | | CUCM-SBC | |
| □ | 91XXXXXXXXXX | Route to SBC | | | CUCM-SBC | |

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


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
Go
admin | Search Documentation | About | Logout
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
Add New
Select All
Clear All
Delete Selected
Reset Selected
Find
Clear Filter
Add New
Select All
Clear All
Delete Selected
Reset Selected

Find and List Trunks

Status

4 records found

Trunks (1 - 4 of 4) Rows per Page 50

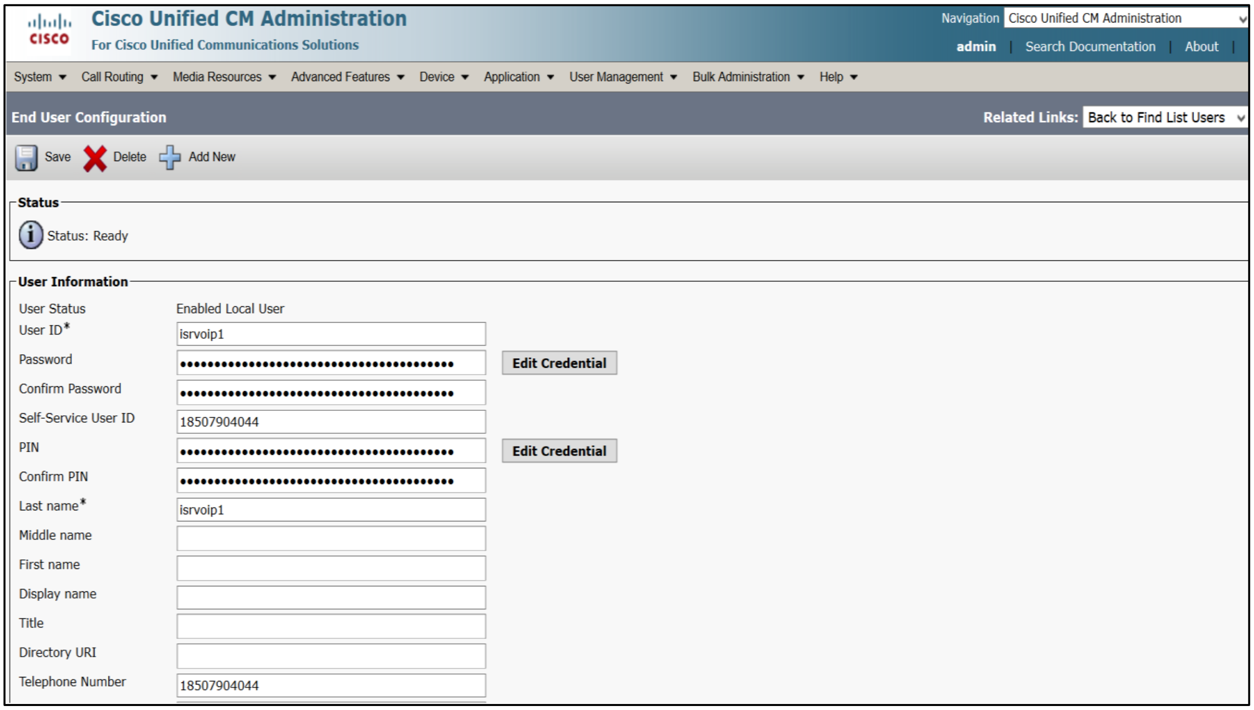
Find Trunks where Device Name begins with

Select item or enter search text

| □ | | Name ▲ | Description | Calling Search Space | Device Pool | Route Pattern | Partition | Route Group | Priority | Trunk Type | SIP Trunk Status | SIP Trunk Duration | SIP Trunk Security Profile |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | SIP | CUCM-ECB | | | Default | | | | | SIP Trunk | Full Service | Time In Full Service: 9 days 16 hours 37 minutes | Non Secure SIP Trunk Profile |
| □ | SIP | CUCM-SBC | | | Default | 1XXXXXXXXXX | | | | SIP Trunk | Full Service | Time In Full Service: 0 day 0 hour 41 minutes | Non Secure SIP Trunk Profile |
| □ | SIP | CUCM-SBC | | | Default | 91XXXXXXXXXX | | | | SIP Trunk | Full Service | Time In Full Service: 0 day 0 hour 41 minutes | Non Secure SIP Trunk Profile |
| □ | SIP | sbcce | | | Default | | | | | SIP Trunk | No Service | Time not in Full Service: 7 days 19 hours 33 minutes | Non Secure SIP Trunk Profile |

## 4.3. End User Configuration

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

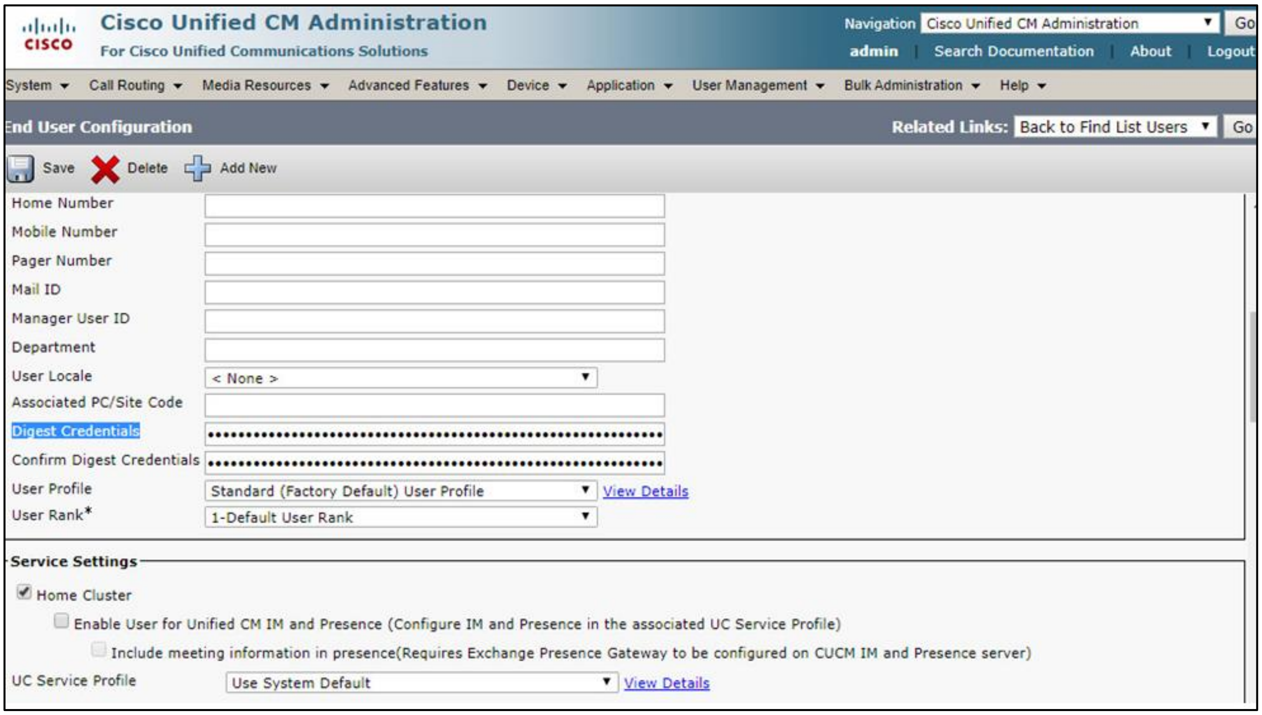

Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
admin | Search Documentation | About |
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
End User Configuration
Related Links: Back to Find List Users
Save Delete Add New
Edit Credential
Edit Credential

Status

Status: Ready

User Information

| | |
|---|---|
| User Status | Enabled Local User |
| User ID* | isrvoip1 |
| Password | •••••••••••••••••••••••••••••••••••••••• |
| Confirm Password | •••••••••••••••••••••••••••••••••••••••• |
| Self-Service User ID | 18507904044 |
| PIN | •••••••••••••••••••••••••••••••••••••••• |
| Confirm PIN | •••••••••••••••••••••••••••••••••••••••• |
| Last name* | isrvoip1 |
| Middle name | |
| First name | |
| Display name | |
| Title | |
| Directory URI | |
| Telephone Number | 18507904044 |


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾
End User Configuration
Related Links: Back to Find List Users Go
Save Delete Add New
View Details
View Details

| | |
|---|---|
| Home Number | |
| Mobile Number | |
| Pager Number | |
| Mail ID | |
| Manager User ID | |
| Department | |
| User Locale | < None > |
| Associated PC/Site Code | |
| Digest Credentials | •••••••••••••••••••••••••••••••••••••••••••••••••••••••••• |
| Confirm Digest Credentials | •••••••••••••••••••••••••••••••••••••••••••••••••••••••••• |
| User Profile | Standard (Factory Default) User Profile |
| User Rank* | 1-Default User Rank |

Service Settings

☑ Home Cluster

☐ Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)

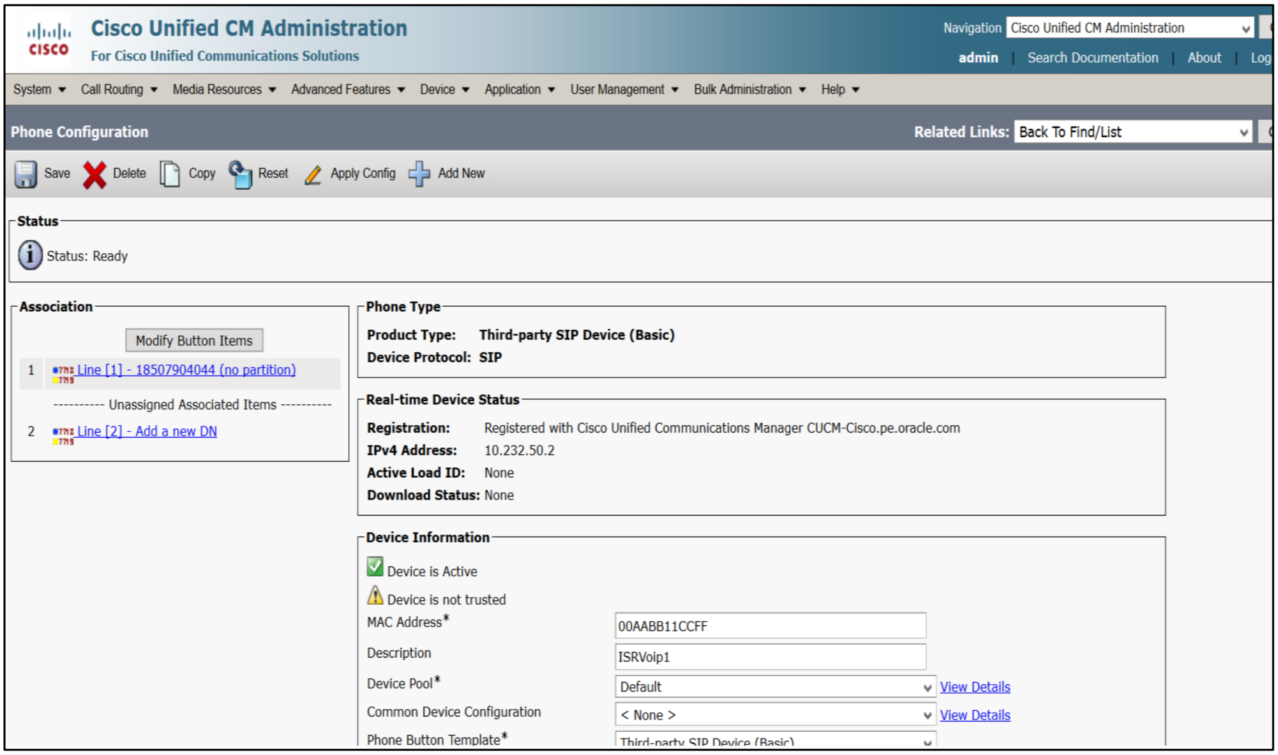
☐ Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)

UC Service Profile: Use System Default

## 4.4. Adding SIP Phone in CUCM

01) Go to Device ---- Phone and click Add New
02) Select Third Party Sip Device (Basic) and click Next
03) Enter in a 12 digit MAC address (any dummy MAC address)
04) Enter the pertinent information for the SIP DEVICE settings – it should mostly be configured the same as a standard phone on your system except for the following settings
    a) in the owner user ID field select the user you created above
    b) in the Device Security Profile field select the security profile you created above
    c) in the Digest User field select the user you created above

05) Click Save.
06) Configure the line settings for the SIP device – the line settings should match the line settings of your standard user's Cisco IP phones
    There are no special attributes that we need to worry about on the line configuration.



Phone Configuration

Status

Status: Ready

Association

1 Line [1] - 18507904044 (no partition)

---------- Unassigned Associated Items ----------

2 Line [2] - Add a new DN

Phone Type

**Product Type:** Third-party SIP Device (Basic)
**Device Protocol:** SIP

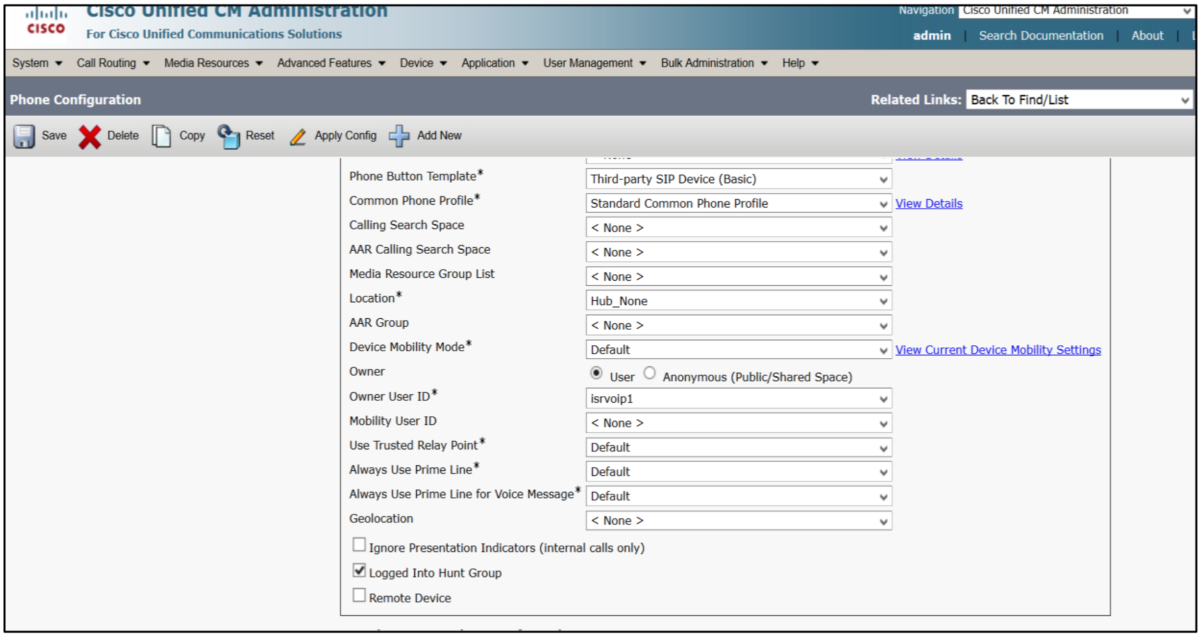
Real-time Device Status

**Registration:** Registered with Cisco Unified Communications Manager CUCM-Cisco.pe.oracle.com
**IPv4 Address:** 10.232.50.2
**Active Load ID:** None
**Download Status:** None

Device Information

☑ Device is Active
⚠ Device is not trusted

| | | |
|---|---|---|
| MAC Address* | 00AABB11CCFF | |
| Description | ISRVoip1 | |
| Device Pool* | Default | View Details |
| Common Device Configuration | < None > | View Details |
| Phone Button Template* | Third-party SIP Device (Basic) | |


Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration
admin | Search Documentation | About
System Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
Phone Configuration
Related Links: Back To Find/List
Save Delete Copy Reset Apply Config Add New

Phone Button Template* Third-party SIP Device (Basic)

Common Phone Profile* Standard Common Phone Profile View Details

Calling Search Space < None >

AAR Calling Search Space < None >

Media Resource Group List < None >

Location* Hub_None

AAR Group < None >

Device Mobility Mode* Default View Current Device Mobility Settings

Owner ● User ○ Anonymous (Public/Shared Space)

Owner User ID* isrvoip1

Mobility User ID < None >

Use Trusted Relay Point* Default

Always Use Prime Line* Default

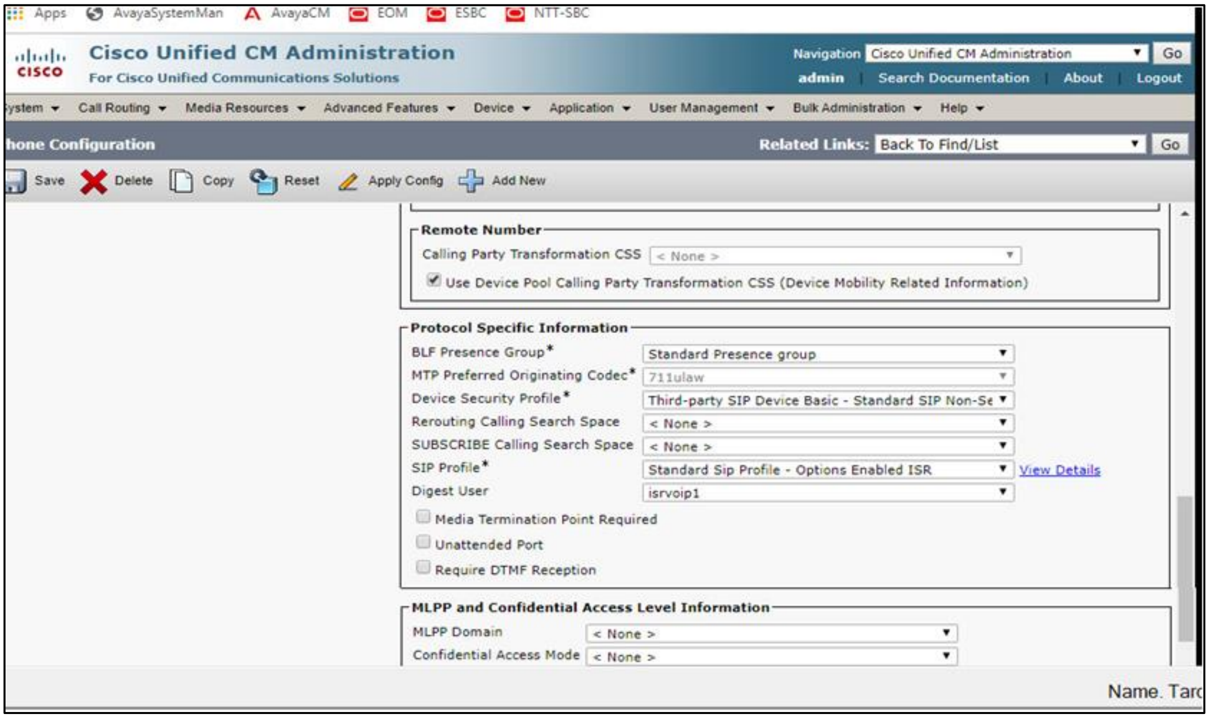
Always Use Prime Line for Voice Message* Default

Geolocation < None >

□ Ignore Presentation Indicators (internal calls only)

☑ Logged Into Hunt Group

□ Remote Device


Apps AvayaSystemMan AvayaCM EOM ESBC NTT-SBC
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified CM Administration Go
admin | Search Documentation | About | Logout
ystem Call Routing Media Resources Advanced Features Device Application User Management Bulk Administration Help
hone Configuration
Related Links: Back To Find/List Go
Save Delete Copy Reset Apply Config Add New

**Remote Number**

Calling Party Transformation CSS < None >

☑ Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)

**Protocol Specific Information**

BLF Presence Group* Standard Presence group

MTP Preferred Originating Codec* 711ulaw

Device Security Profile* Third-party SIP Device Basic - Standard SIP Non-Se

Rerouting Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard Sip Profile - Options Enabled ISR View Details

Digest User isrvoip1

□ Media Termination Point Required

□ Unattended Port

□ Require DTMF Reception

**MLPP and Confidential Access Level Information**

MLPP Domain < None >

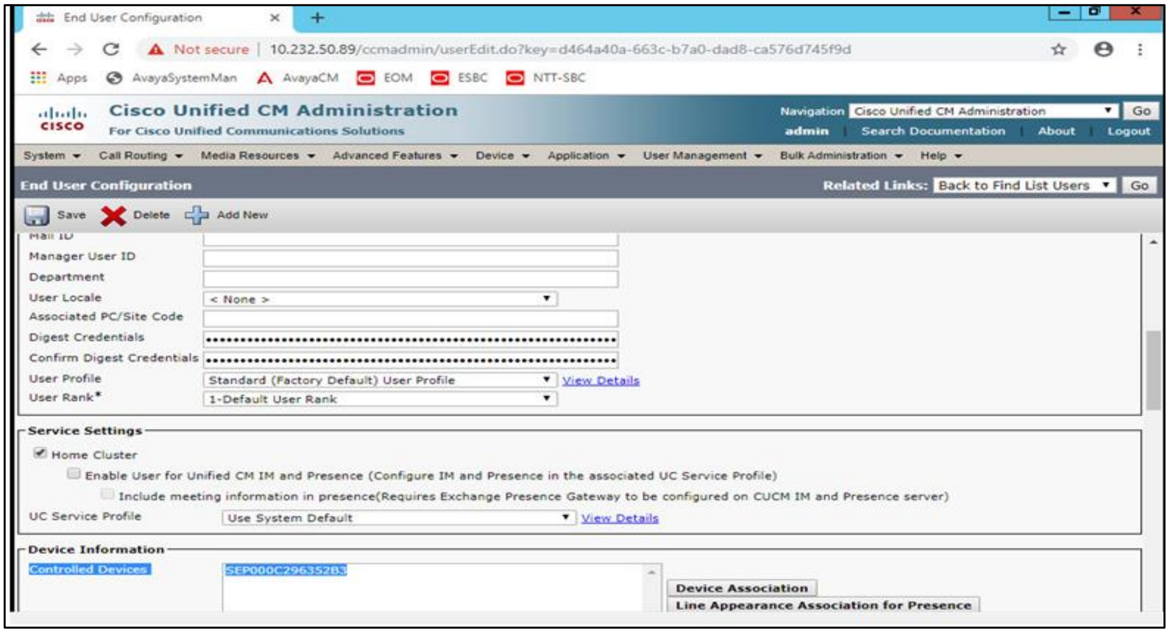
Confidential Access Mode < None >

Name. Tarc

### 4.5. Associating End User to Phone

01) Go to User Management ----- End Users and search for the sip user you created above, once you find it, click on it

02) Scroll down to Device Association and click on the Device Association button
03) Locate and select the sip device you created above
04) Check the checkbox next to this device and click Save Selected/Changes
05) Click Go next to the Back to User related link near the upper right-hand corner
06) Click Save one more time on the End User Configuration screen.



End User Configuration

Related Links: Back to Find List Users

Mail ID

Manager User ID

Department

User Locale: < None >

Associated PC/Site Code

Digest Credentials: ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••

Confirm Digest Credentials: ••••••••••••••••••••••••••••••••••••••••••••••••••••••••••••

User Profile: Standard (Factory Default) User Profile View Details

User Rank*: 1-Default User Rank

Service Settings

☑ Home Cluster

□ Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)

□ Include meeting information in presence(Requires Exchange Presence Gateway to be configured on CUCM IM and Presence server)

UC Service Profile: Use System Default View Details

Device Information

Controlled Devices: SEP000C296352B3

Device Association

Line Appearance Association for Presence

With these steps, the CUCM configuration is complete.

# 5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Cisco Call Manager (Cisco CUCM) and Twilio Elastic SIP Trunking. **In this SBC config, Twilio Elastic SIP trunk side is secure (TLS/SRTP) and Cisco 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 Cisco Call Manager (Cisco CUCM) 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

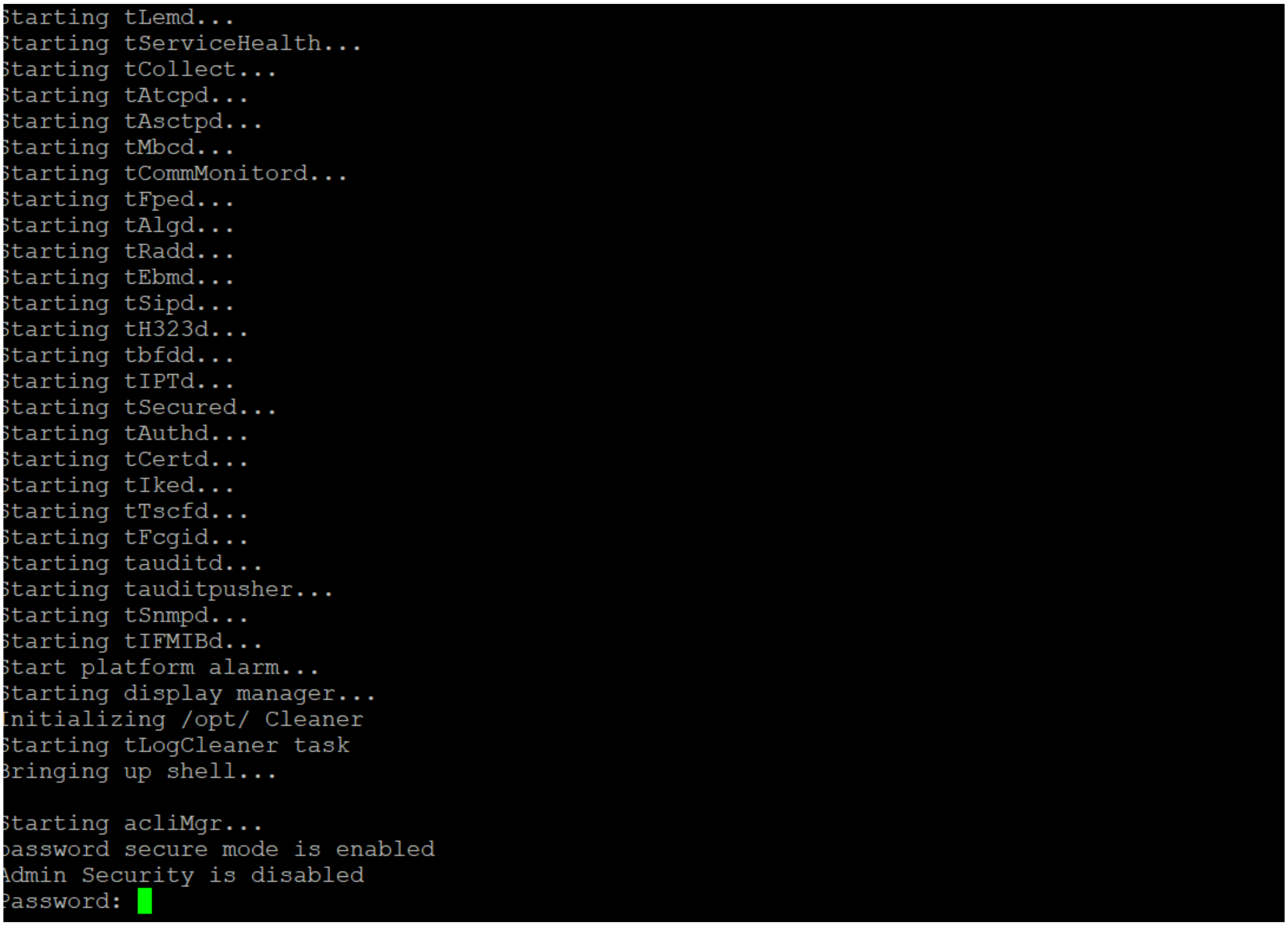
If the customer is looking to setup a new SBC from scratch, please follow the section below.

## 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

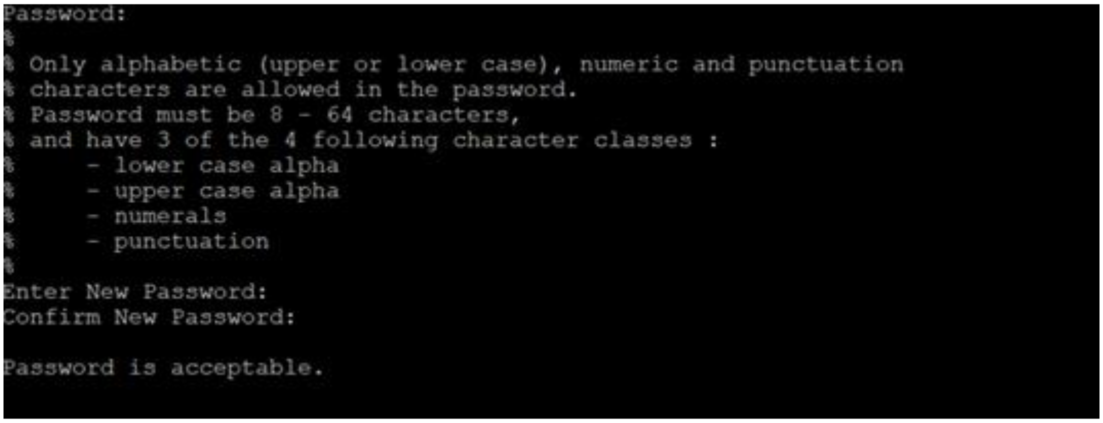
Power on the SBC and confirm that you see the following output from the boot-up sequence



```
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.

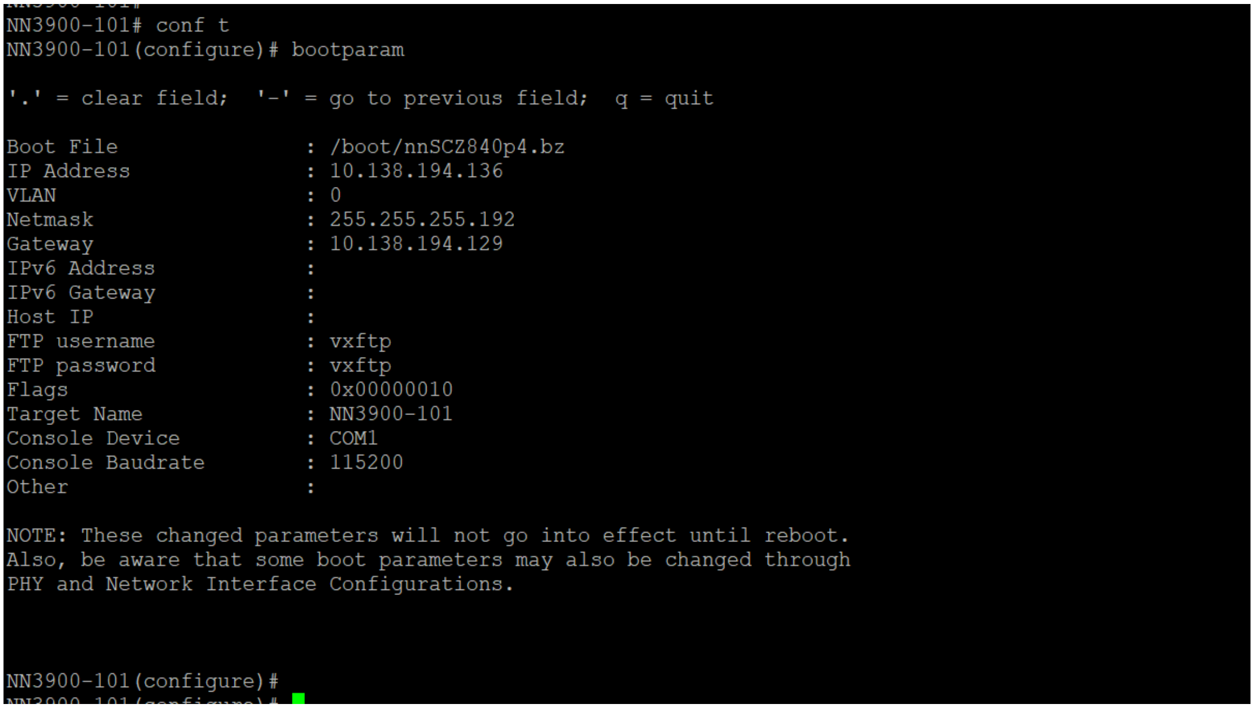


```
Password:
%
% Only alphabetic (upper or lower case), numeric and punctuation
% characters are allowed in the password.
% Password must be 8 - 64 characters,
% and have 3 of the 4 following character classes :
%      - lower case alpha
%      - upper case alpha
%      - numerals
%      - punctuation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

Password is acceptable.
```

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

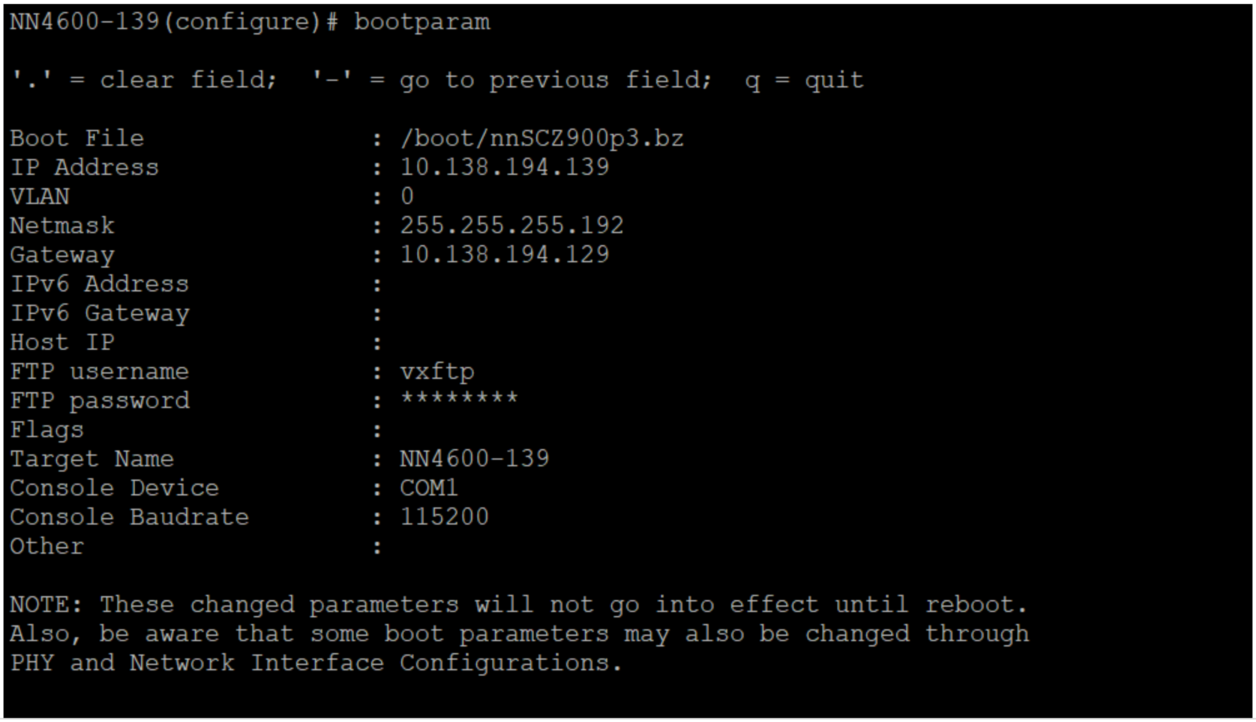
To access bootparam. Go to Configure terminal->bootparam.

bootparam for 8.4 OS



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

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

Boot File                : /boot/nnSCZ840p4.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)#
```

bootparam for 9.0 OS

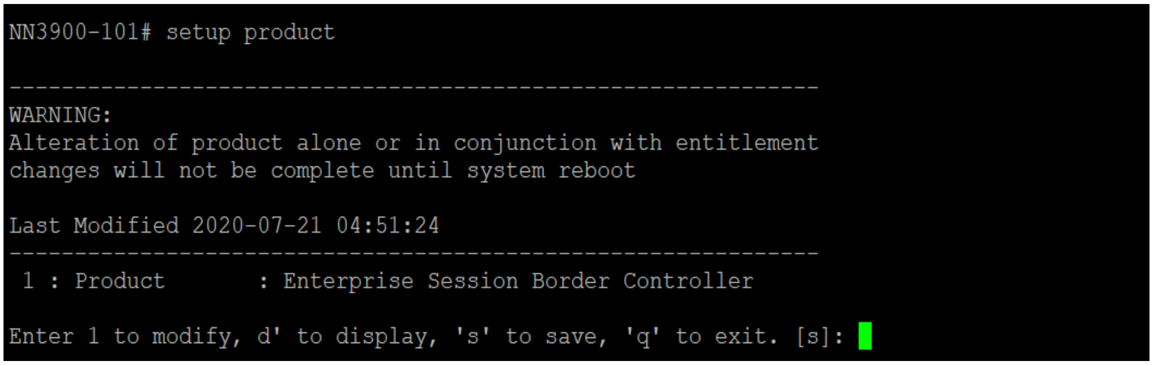


```
NN4600-139(configure)# bootparam

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

Boot File                : /boot/nnSCZ900p3.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.
```

Note: There is no management IP configured by default.

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

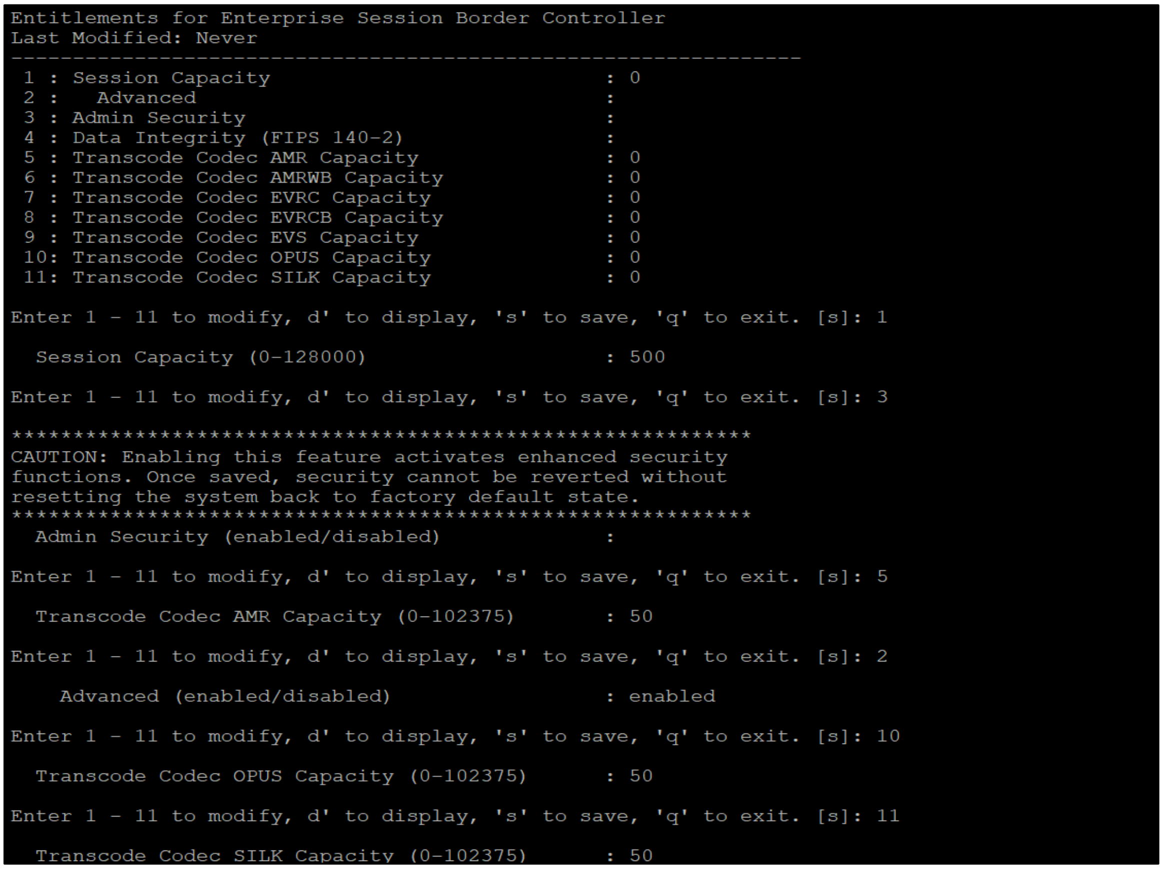
To configure product type, type in setup product in the terminal



```
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.

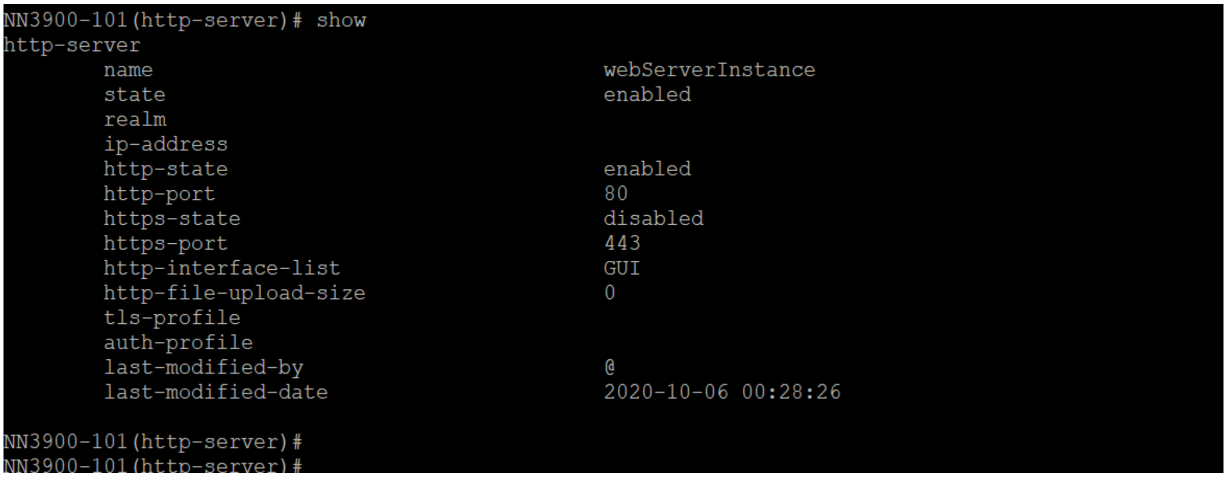


```
Entitlements for Enterprise Session Border Controller
Last Modified: Never
----------------------------------------------------------------
 1 : Session Capacity                              : 0
 2 :   Advanced                                    :
 3 : Admin Security                             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

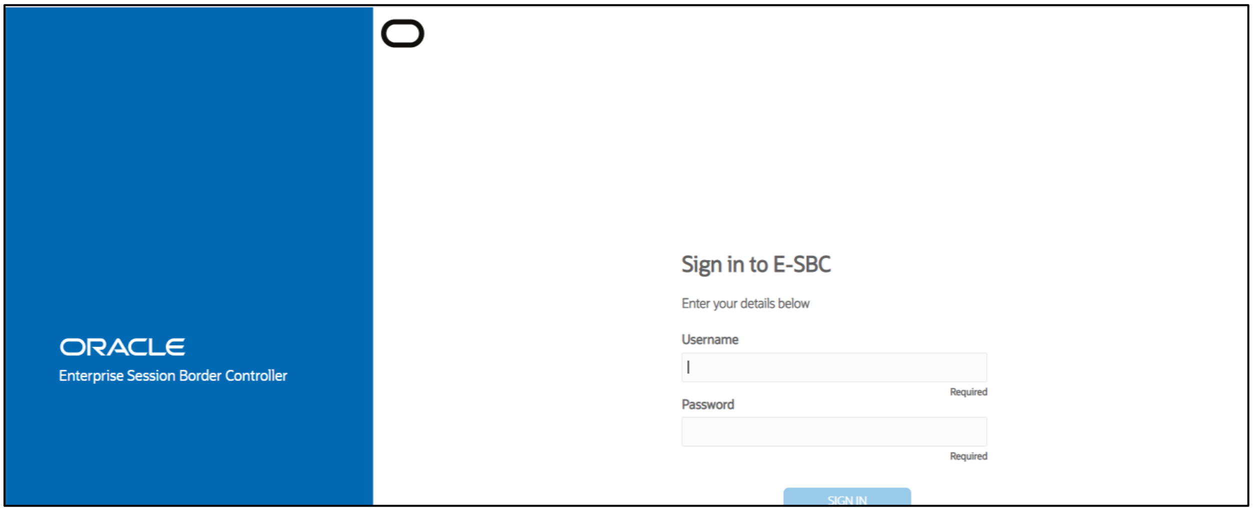


```
NN3900-101(http-server)# show
http-server
        name                                    webServerInstance
        state                                   enabled
        realm
        ip-address
        http-state                              enabled
        http-port                               80
        https-state                             disabled
        https-port                              443
        http-interface-list                     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)#
NN3900-101(http-server)#
```

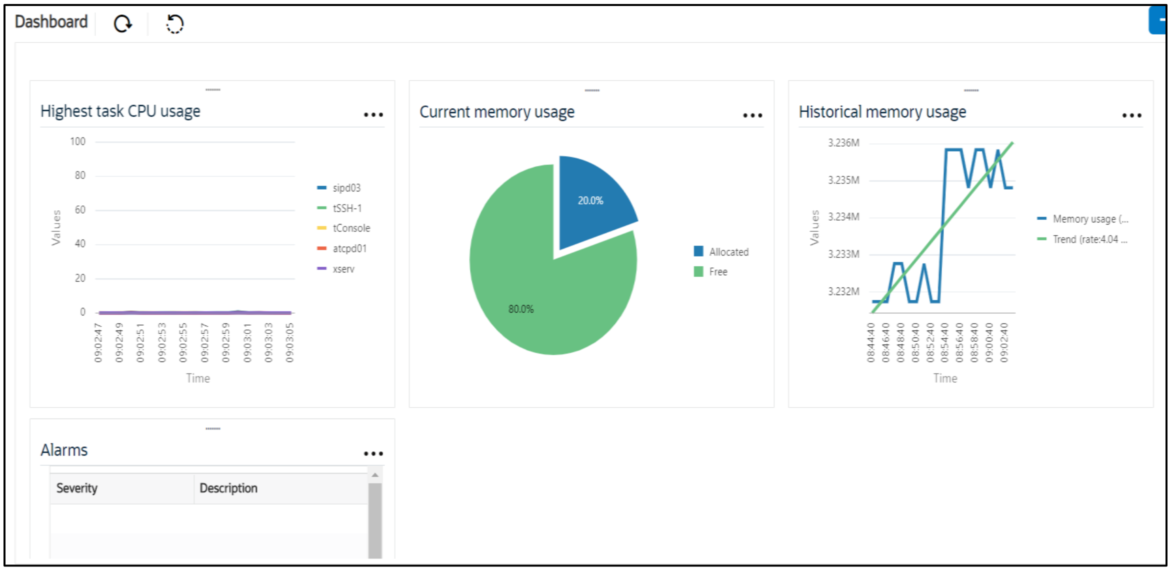
## 6.2. Configure SBC using Web GUI

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

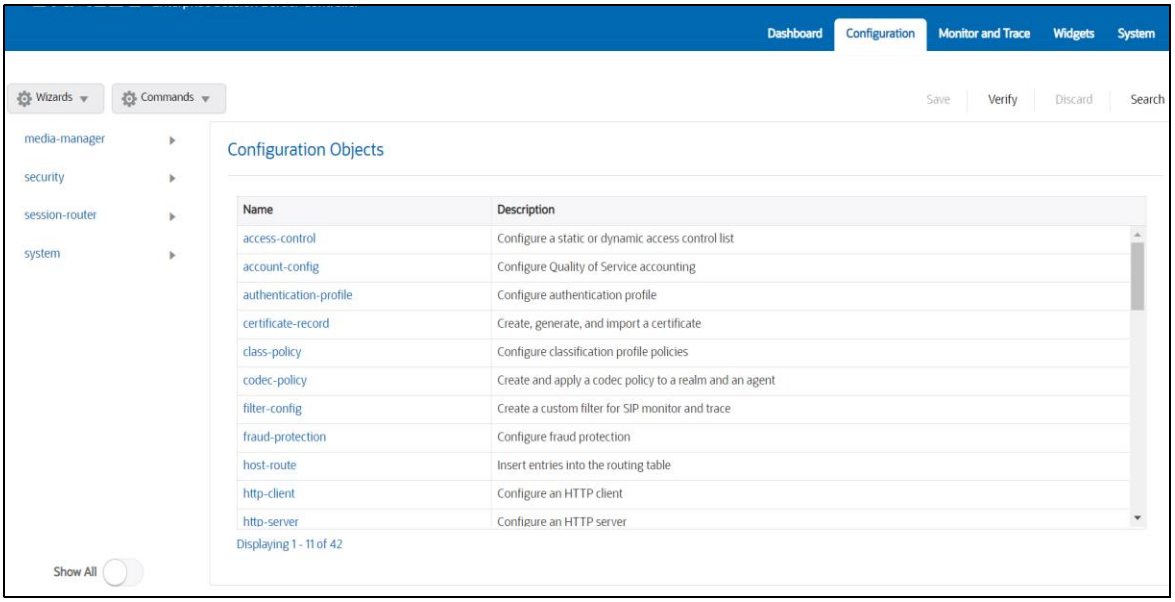
The Web GUI can be accessed through the url http://<SBC_MGMT_IP>.



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.

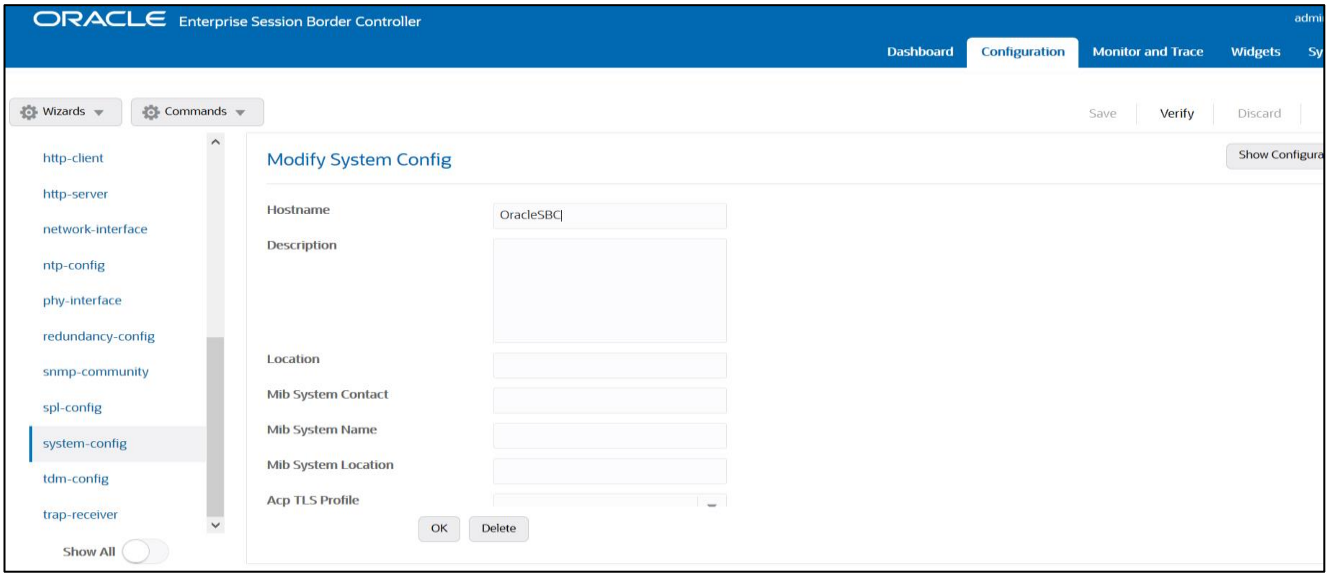
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.0.0/webgui/web-gui-guide.pdf

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

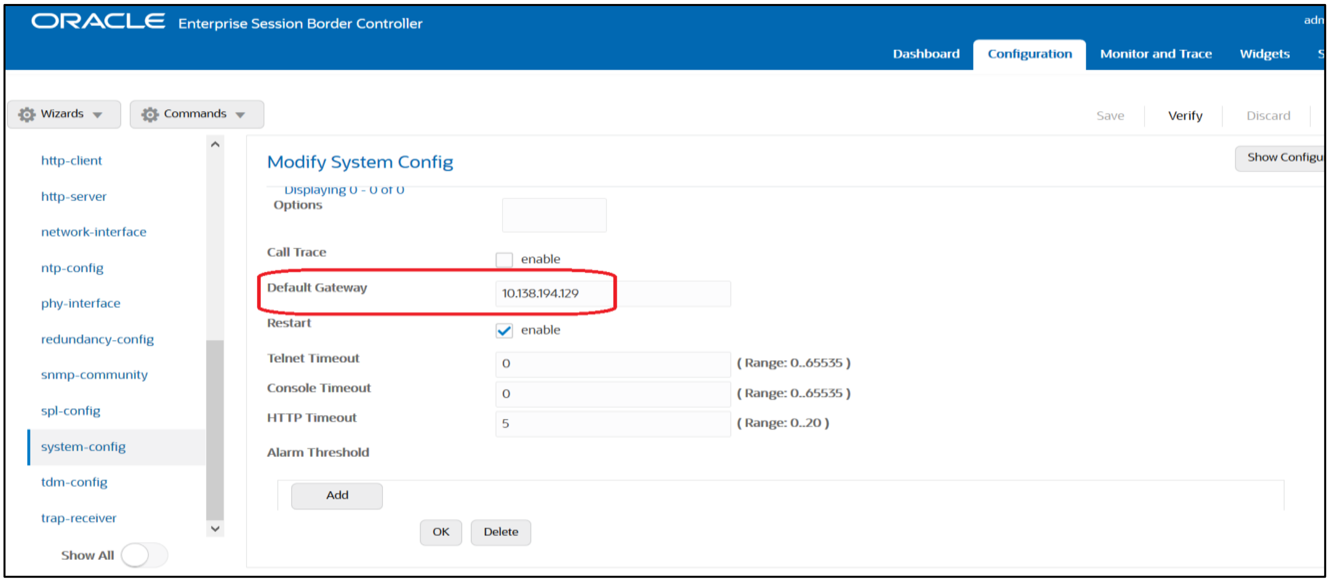
Mib System Contact

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.

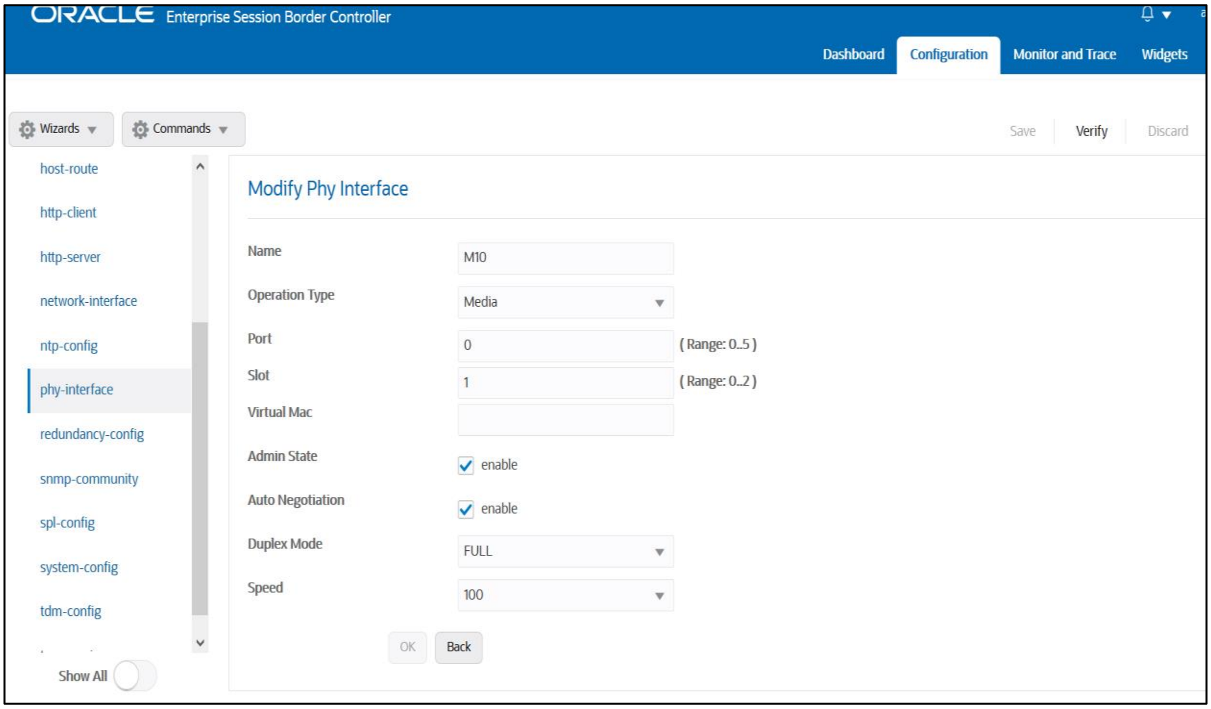
## 6.4. Configure Physical Interface values

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

Please configure M10 for Twilio side and M11 for Cisco side.

| Parameter Name | Twilio Elastic Sip Trunk side (M10) | Cisco side (M11) |
|---|---|---|
| Slot | 1 | 1 |
| Port | 0 | 1 |
| Operation Mode | Media | Media |

Please configure M10 interface as below.



Modify Phy Interface

Name: M10

Operation Type: Media

Port: 0 ( Range: 0..5 )

Slot: 1 ( Range: 0..2 )

Virtual Mac:

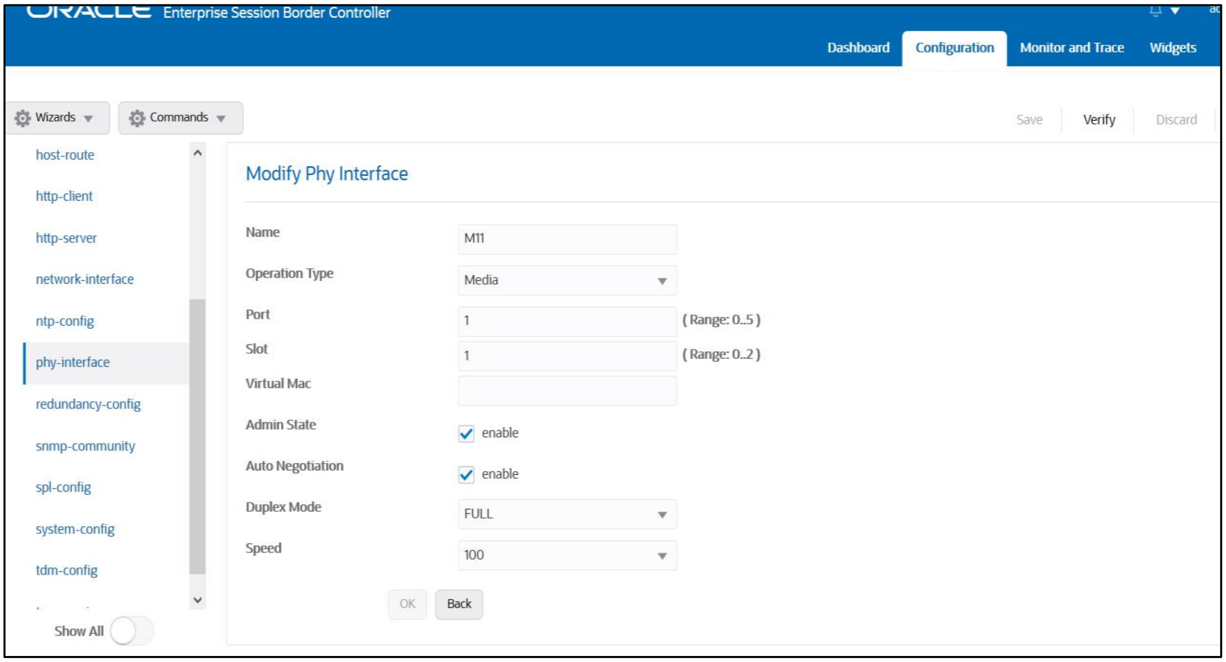
Admin State: ☑ enable

Auto Negotiation: ☑ enable

Duplex Mode: FULL

Speed: 100

Please configure M11 interface as below



Modify 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 |

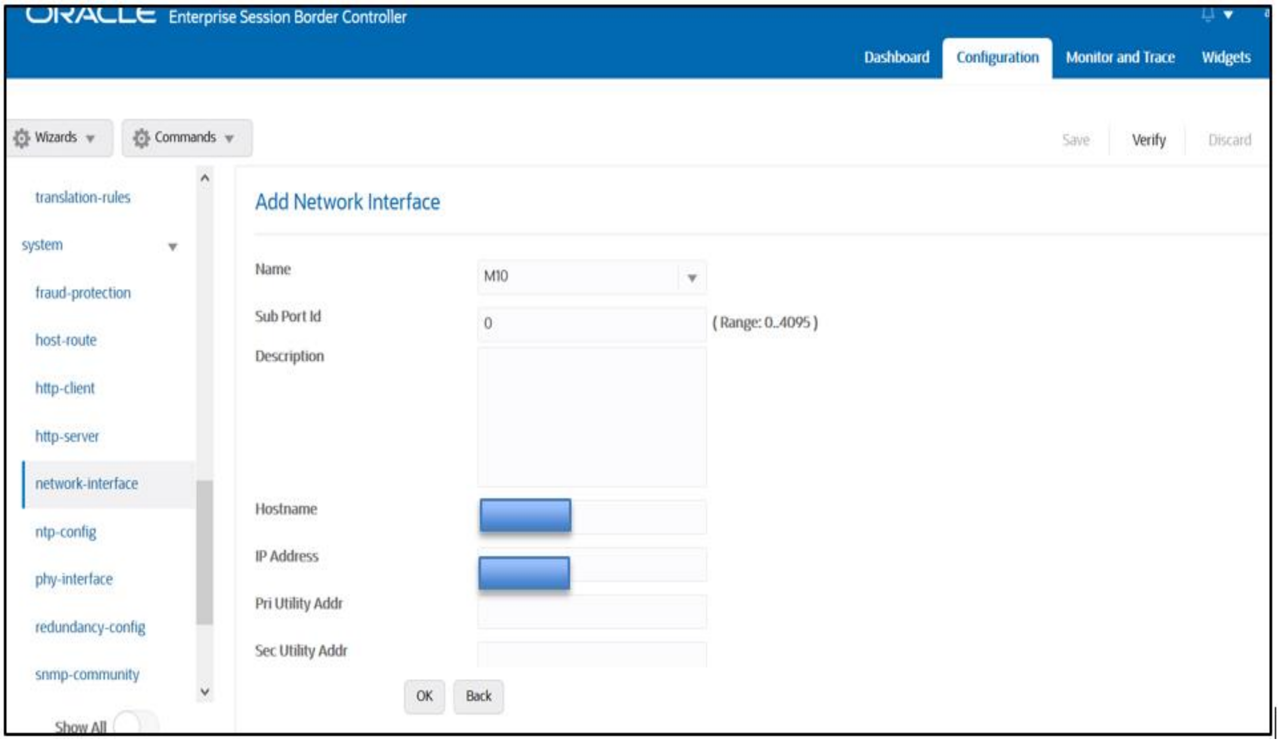
## 6.5. Configure Network Interface values

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 | Cisco side Network interface |
|---|---|---|
| Name | M10 | M11 |
| 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 M10 as below



Add Network Interface

Name: M10

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

Description:

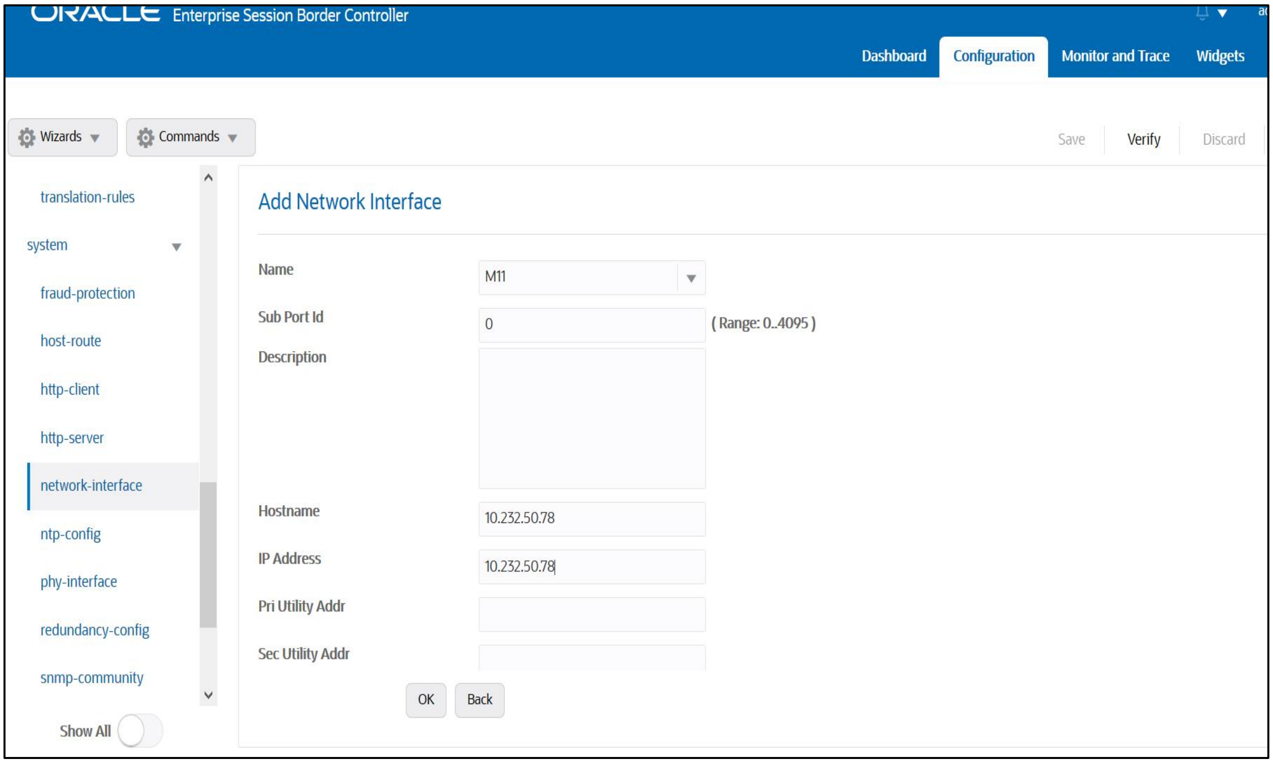
Hostname: [redacted]

IP Address: [redacted]

Pri Utility Addr:

Sec Utility Addr:

Similarly, configure network interface M11 as below



Add Network Interface

Name: M11

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

Description:

Hostname: 10.232.50.78

IP Address: 10.232.50.78

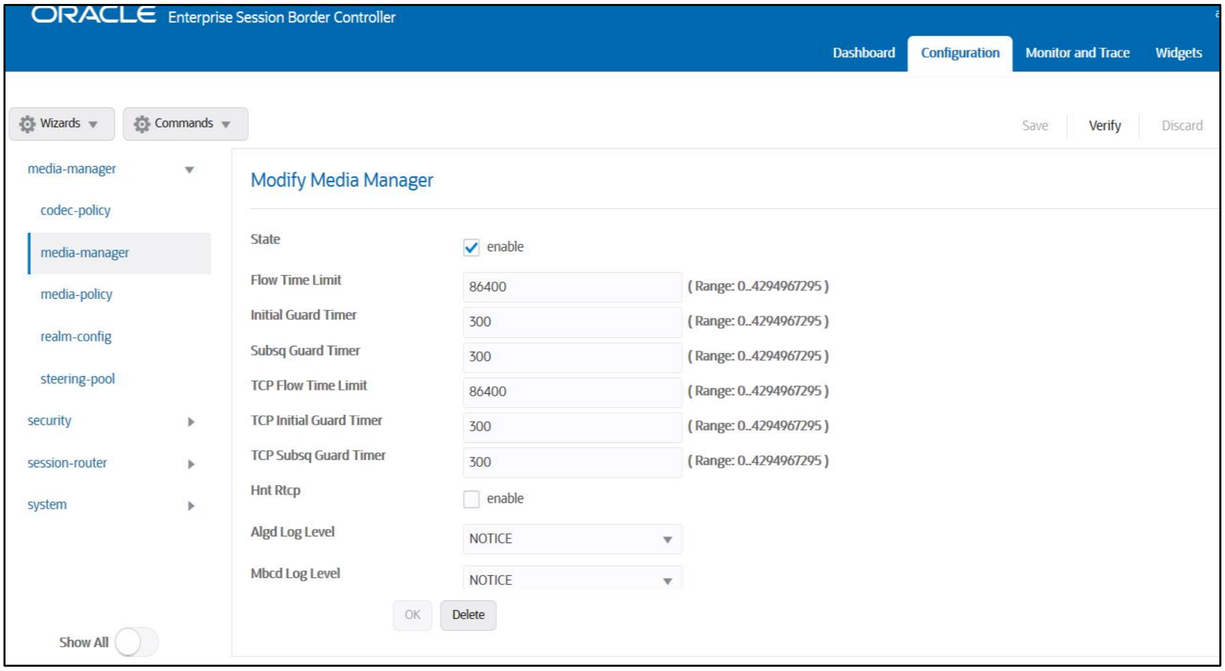
Pri Utility Addr:

Sec Utility Addr:

## 6.6. Enable media manager

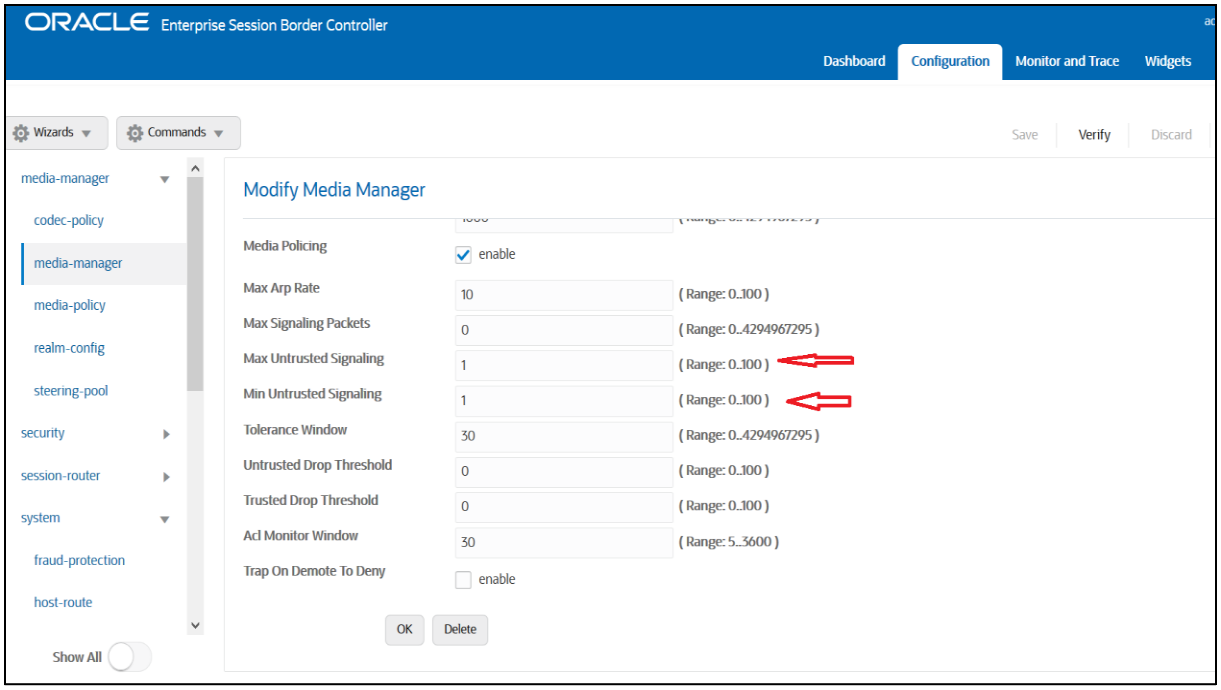
Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

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

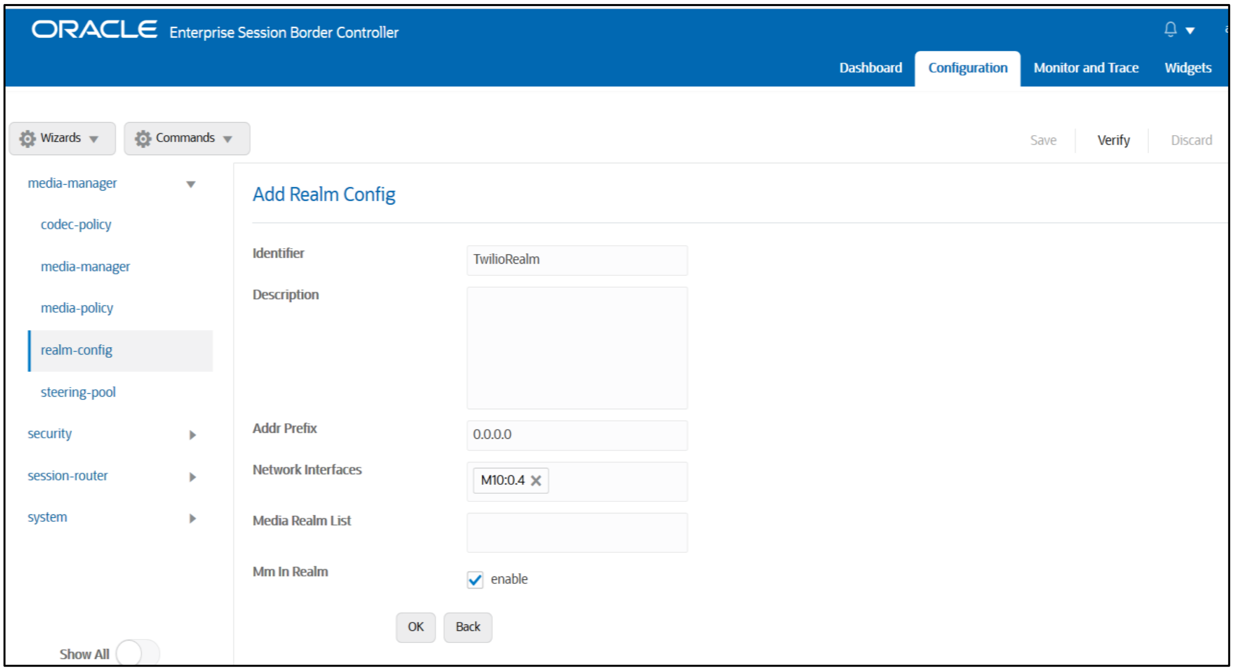
## 6.7. Configure Realms

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 | Cisco Side |
|---|---|---|
| Identifier | TwilioRealm | CUCMRealm |
| Network Interface | M10 | M11 |
| Mm in realm | ☑ | ☑ |
| FQDN | | |
| Media Sec policy | sdespolicy | RTP |
| Access Control Trust Level | High | High |

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

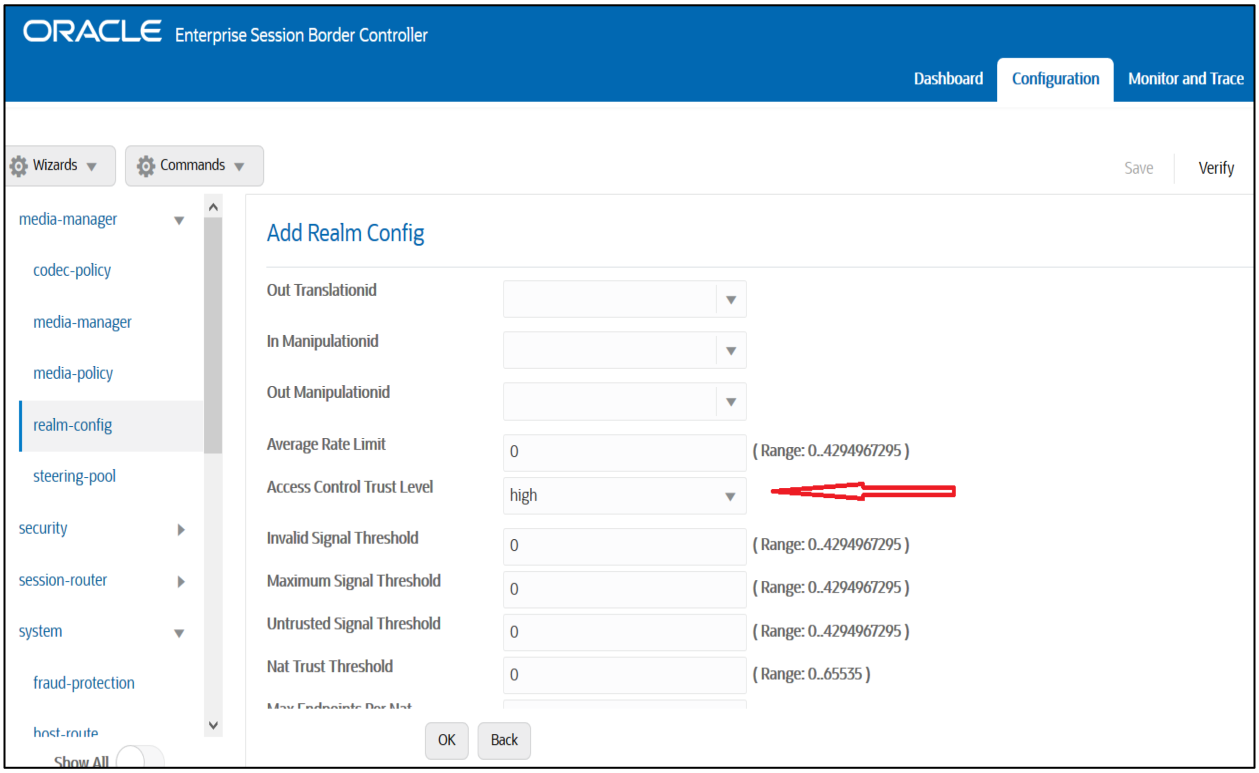
Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M10:0.4

Media Realm List:

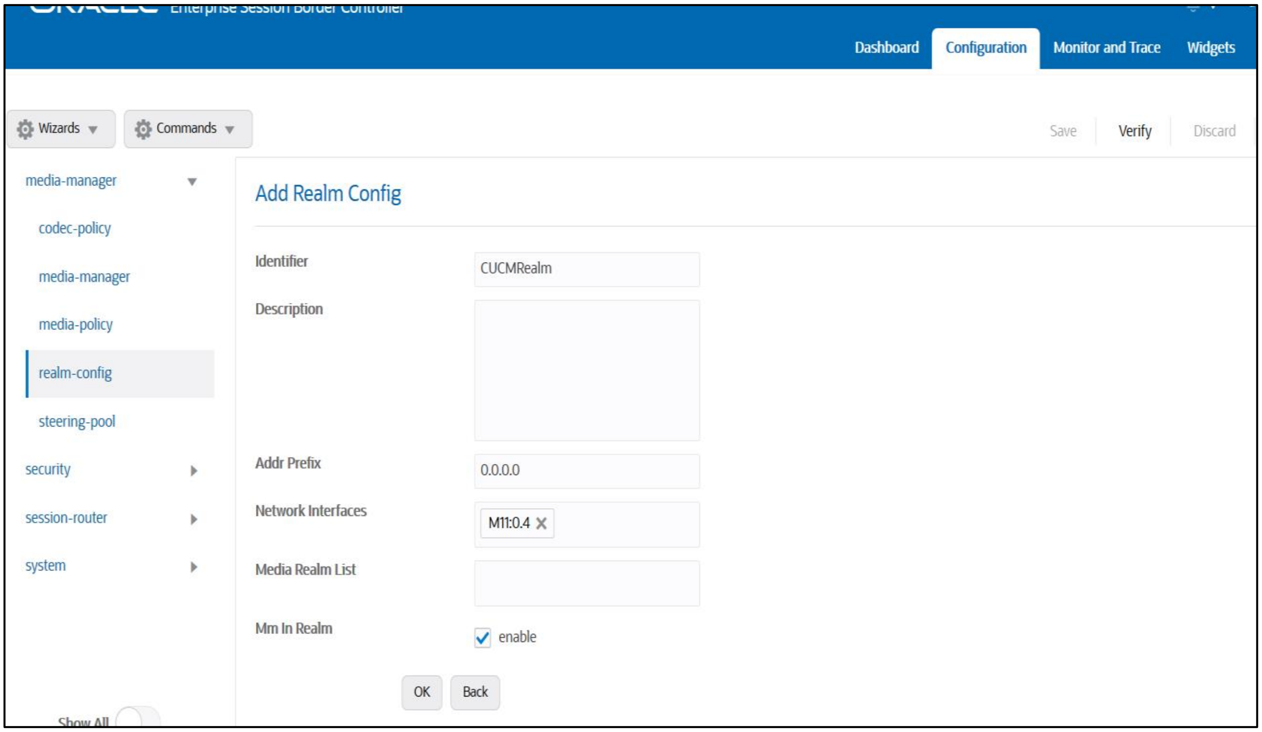
Mm In Realm: ☑ enable



Add Realm Config

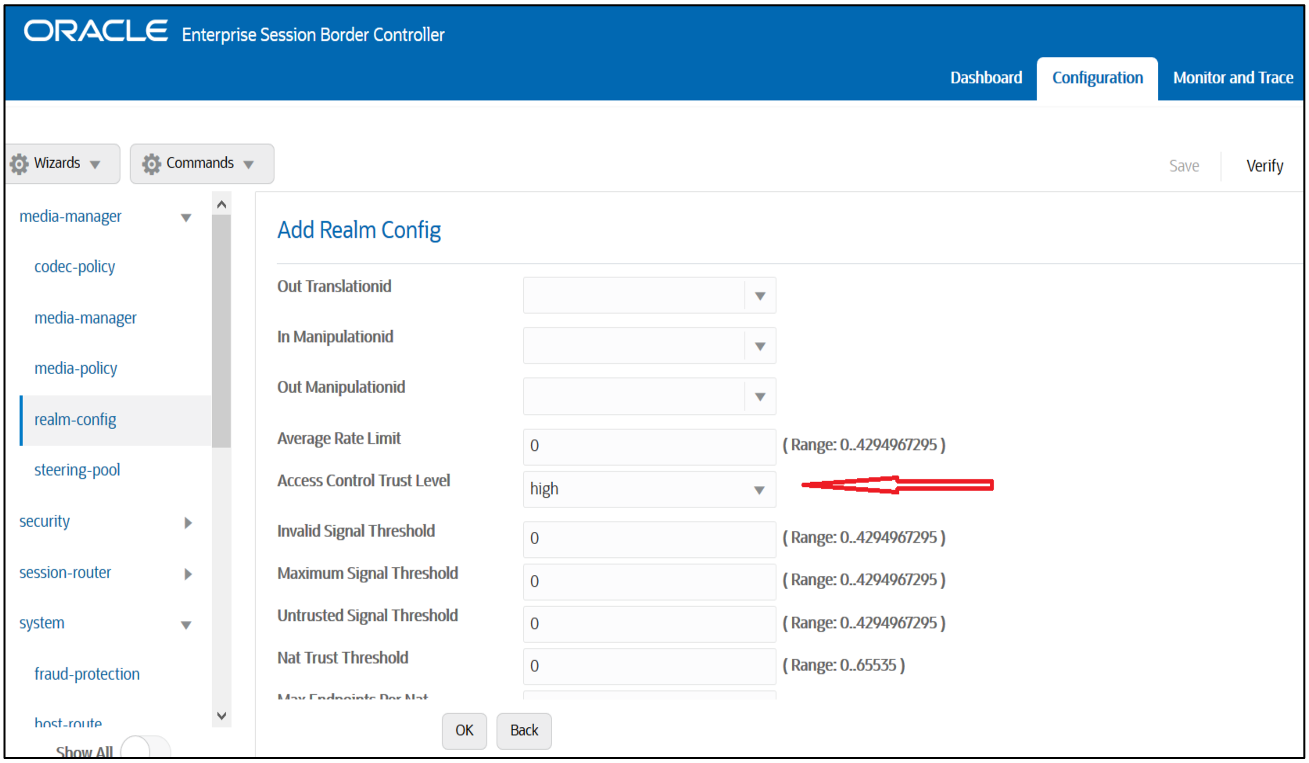
| | | |
|---|---|---|
| Out Translationid | | |
| In Manipulationid | | |
| Out Manipulationid | | |
| Average Rate Limit | 0 | ( Range: 0..4294967295 ) |
| Access Control Trust Level | high | |
| Invalid Signal Threshold | 0 | ( Range: 0..4294967295 ) |
| Maximum Signal Threshold | 0 | ( Range: 0..4294967295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

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



Add Realm Config

| | |
|---|---|
| Identifier | CUCMRealm |
| Description | |
| Addr Prefix | 0.0.0.0 |
| Network Interfaces | M11:0.4 ✕ |
| 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 | | |

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.

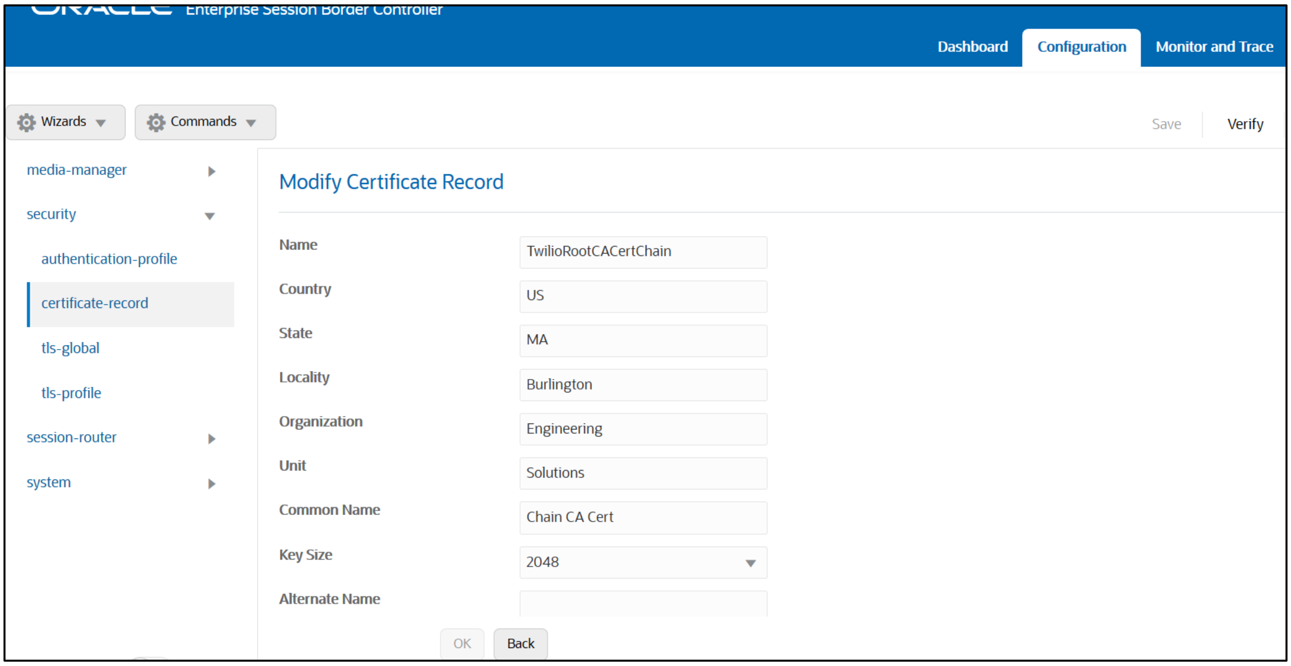
- SBC – 1 certificate-record assigned to SBC
- Root – 1 certificate-record for root cert

2) Deploy the SBC and Root certificates on the SBC

## Step 1 – Creating the certificate record

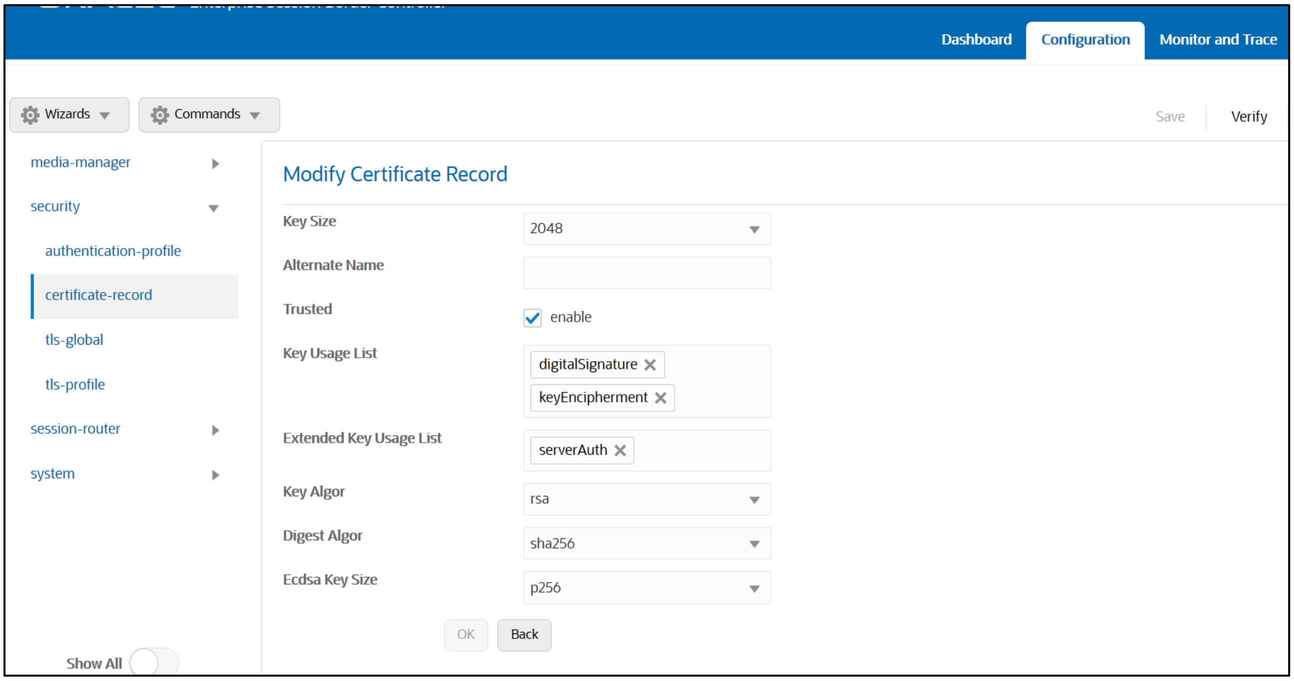
Twilio Elastic SIP Trunking uses certificates from a CA (Certificate Authority) for establishing the TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It is important that you add the following root certificate to establish TLS connection from the link given below:

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

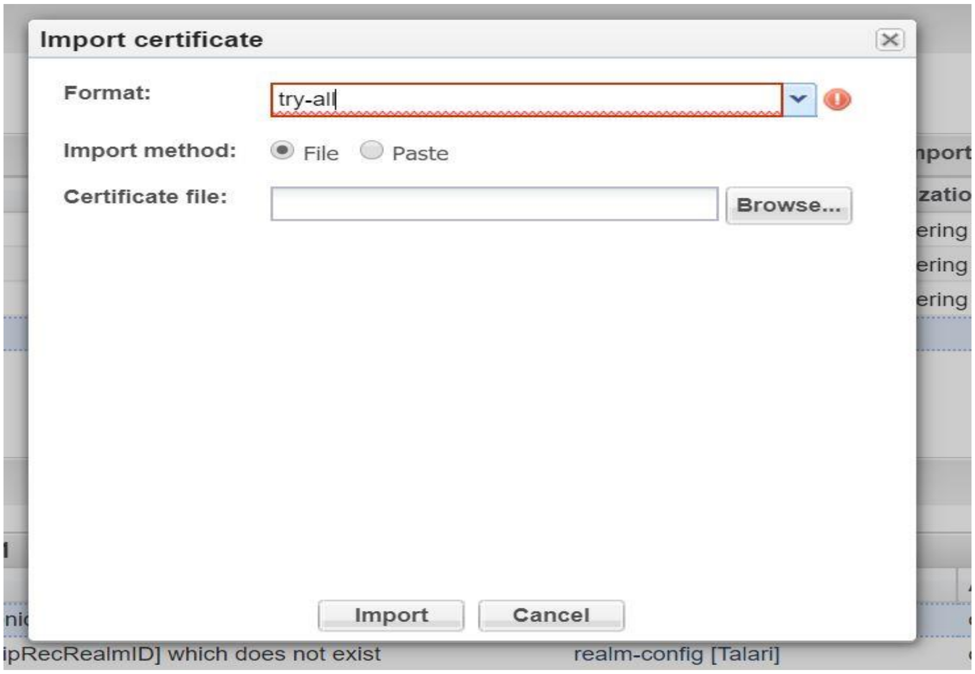
| | |
|---|---|
| Key Size | 2048 |
| Alternate Name | |
| Trusted | ☑ enable |
| Key Usage List | digitalSignature ✕<br>keyEncipherment ✕ |
| Extended Key Usage List | serverAuth ✕ |
| Key Algor | rsa |
| Digest Algor | sha256 |
| Ecdsa Key Size | p256 |

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<br>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



Format: try-all

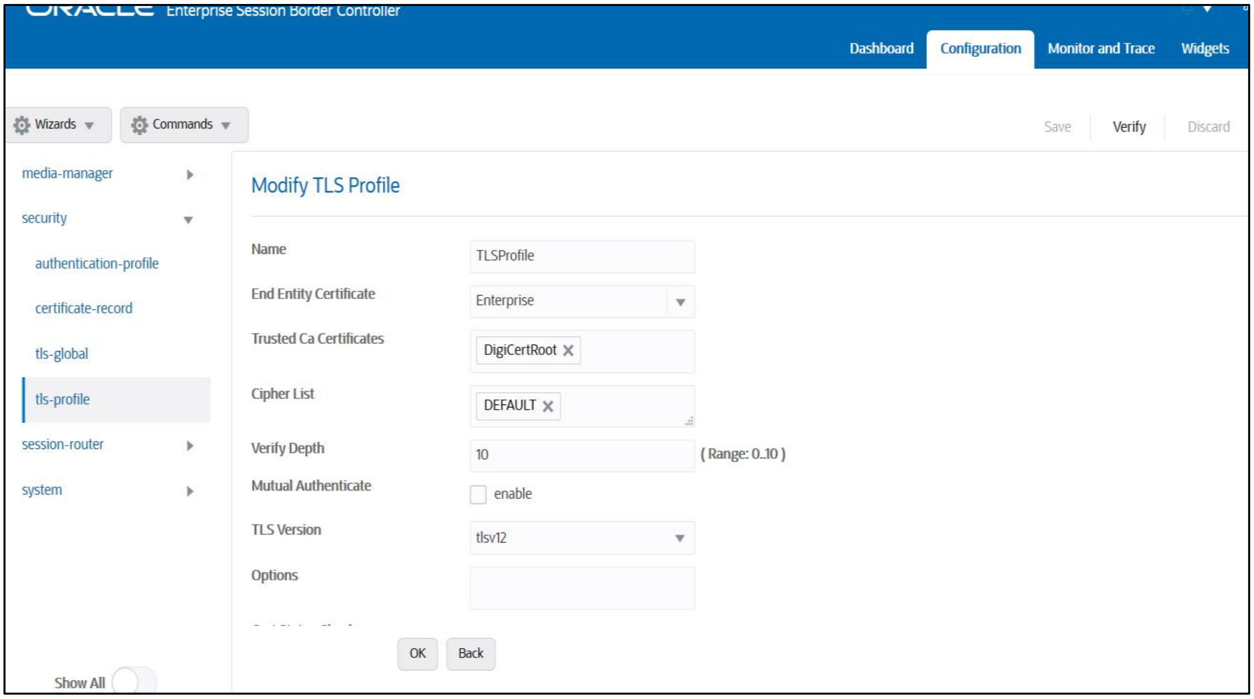
Import method: ● File ○ Paste

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

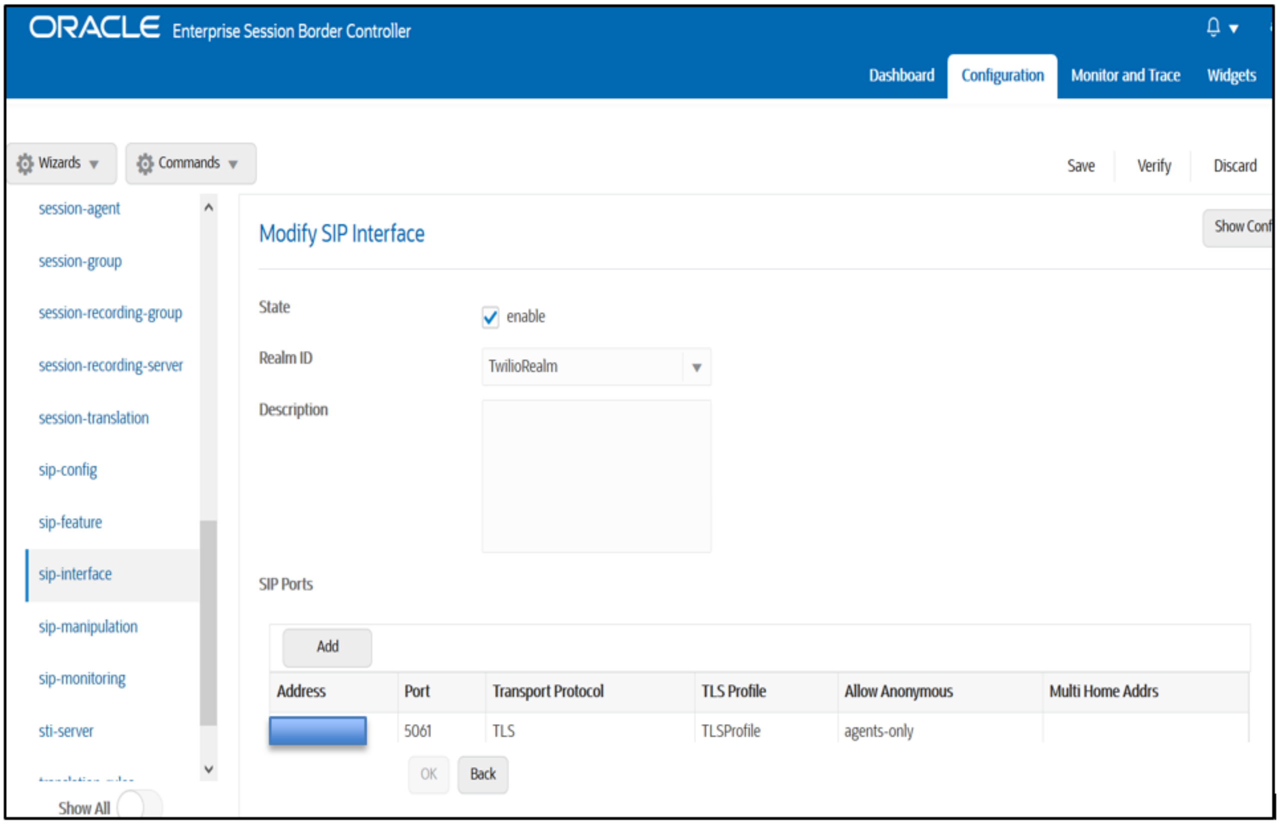
Name: TLSProfile
End Entity Certificate: Enterprise
Trusted Ca Certificates: DigiCertRoot
Cipher List: DEFAULT
Verify Depth: 10 ( Range: 0..10 )
Mutual Authenticate: □ enable
TLS Version: tlsv12
Options:

## 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

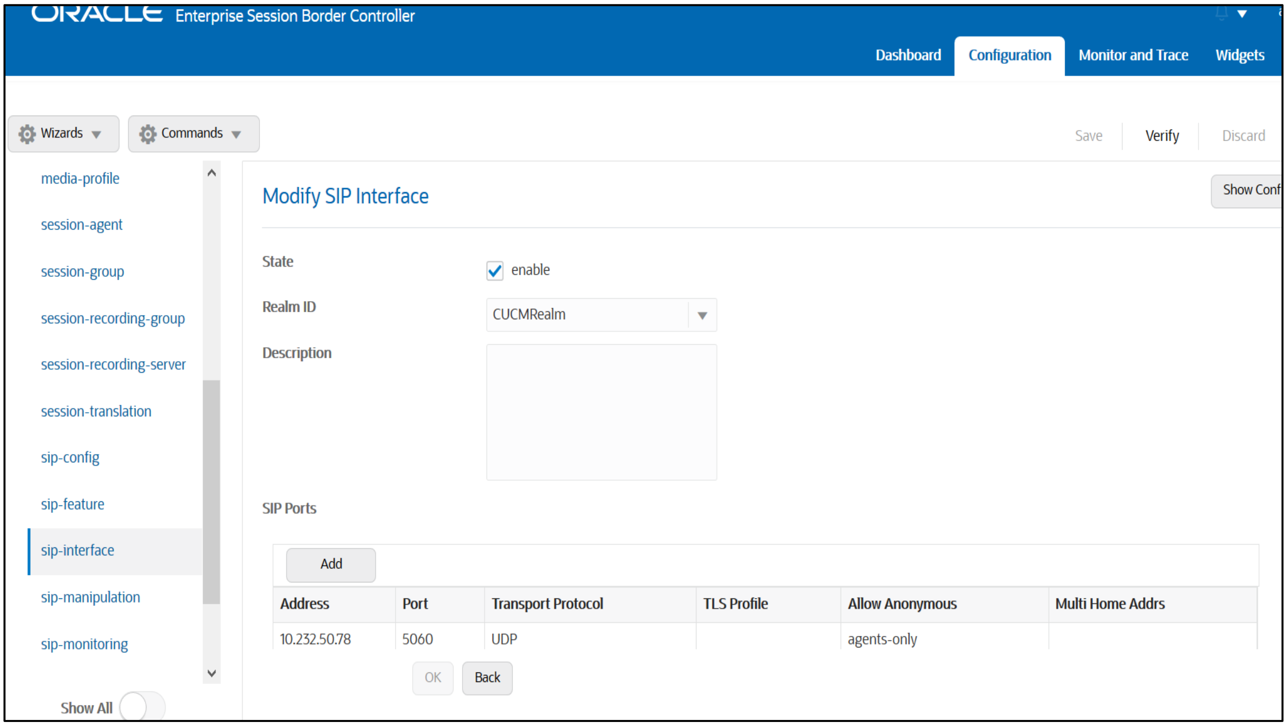
Realm ID TwilioRealm

Description

SIP Ports

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

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



Modify SIP Interface

State ☑ enable

Realm ID CUCMRealm

Description

SIP Ports

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

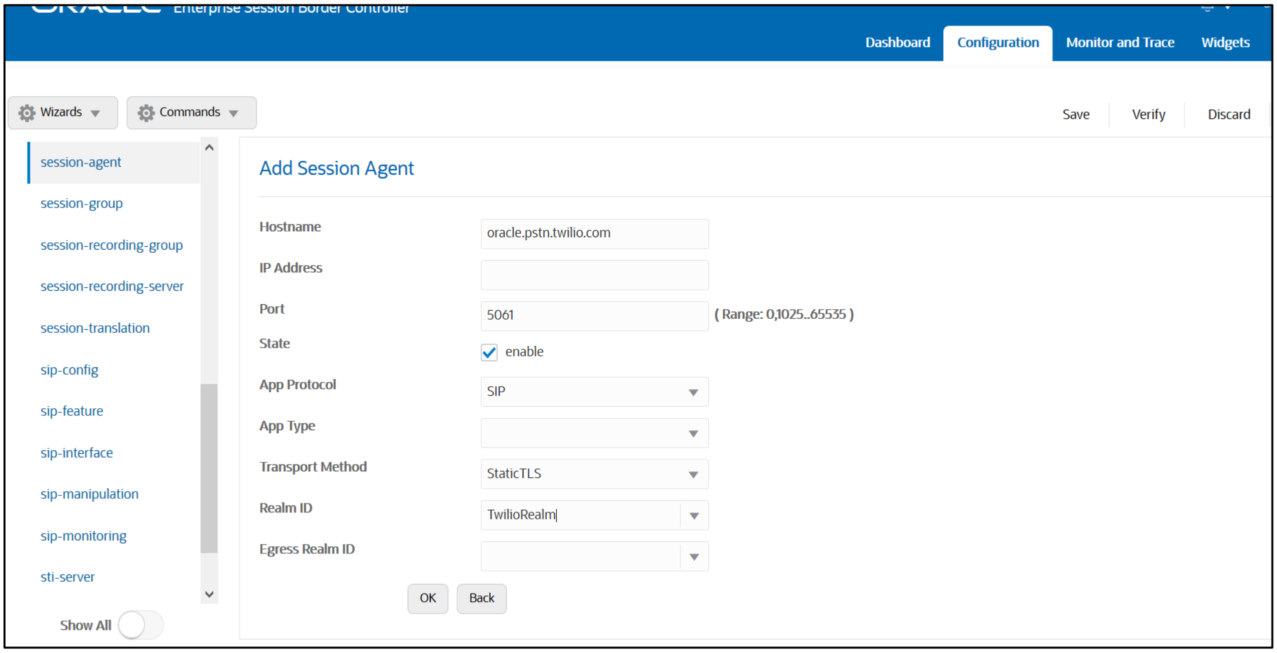
Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

## 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 | |

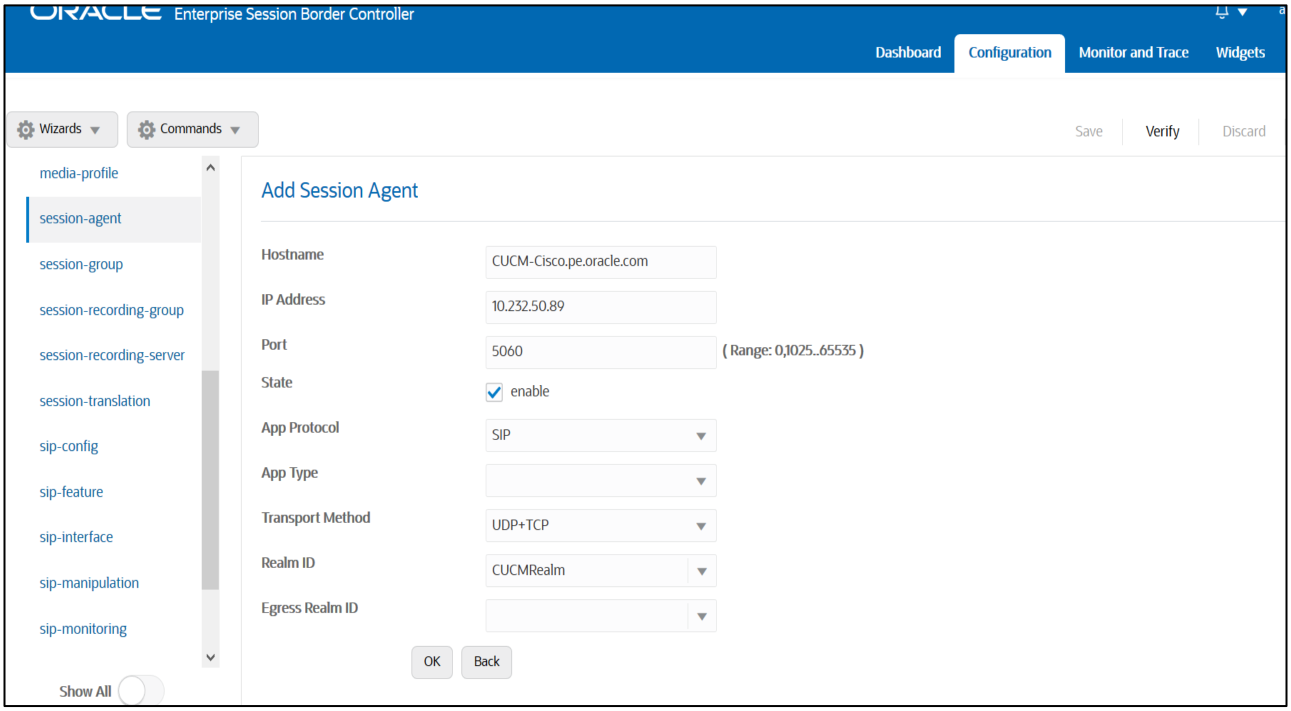
**NOTE: Connection to Twilio Elastic SIP Trunking is available in multiple geographic edge locations. If you wish to manually connect to a specific geographic edge location that is closest to the location of your communications infrastructure, you may do so by pointing your communications infrastructure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

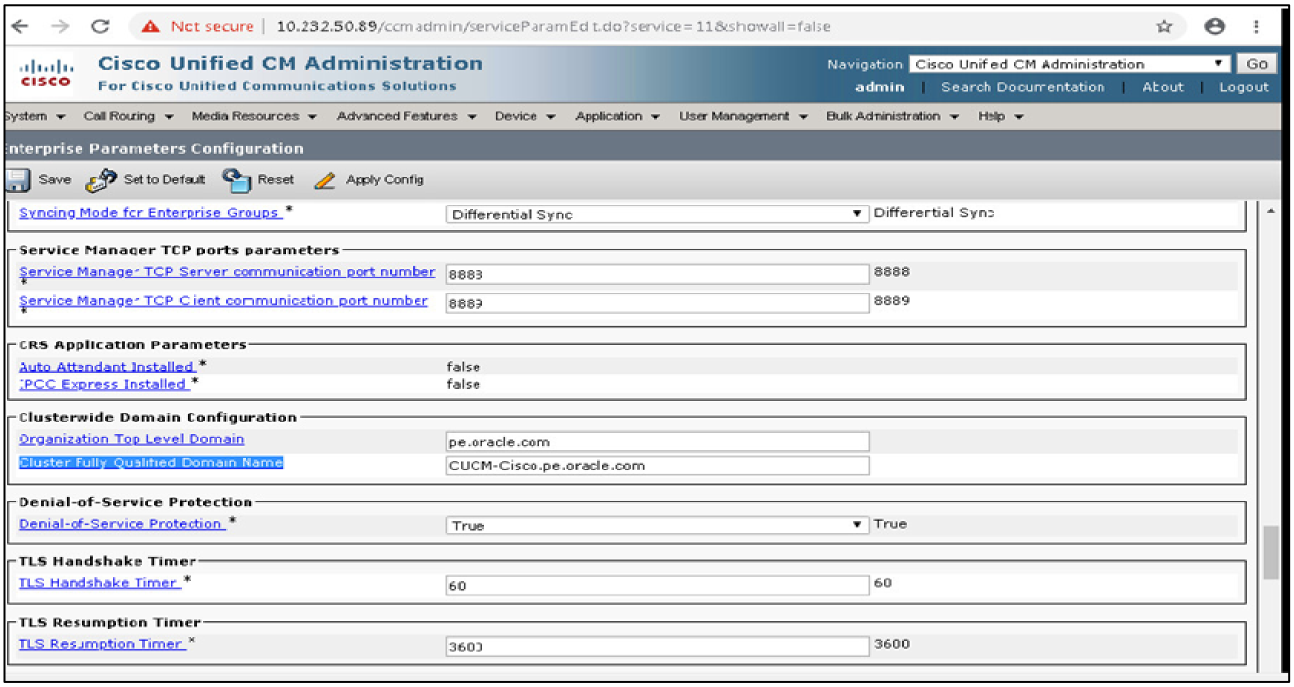
Similarly, configure the session-agents for the Cisco Side as below:

- Host name to FQDN of CUCM which is “CUCM-Cisco.pe.oracle.com” in our example. **We can also give Cisco CUCM IP address if there is no host name configured.**
- The same FQDN value should be configured in Cisco CUCM under System ---Enterprise Parameter ----Cluster FQDN.



Add Session Agent

| | |
|---|---|
| Hostname | CUCM-Cisco.pe.oracle.com |
| IP Address | 10.232.50.89 |
| Port | 5060 ( Range: 0,1025..65535 ) |
| State | ☑ enable |
| App Protocol | SIP |
| App Type | |
| Transport Method | UDP+TCP |
| Realm ID | CUCMRealm |
| Egress Realm ID | |


Nct secure | 10.232.50.89/ccmadmin/serviceParamEdt.do?service=11&showall=false
Cisco Unified CM Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unifed CM Administration Go
admin | Search Documentation | About | Logout
System
Call Routing
Media Resources
Advanced Features
Device
Application
User Management
Bulk Administration
Help
Save
Set to Default
Reset
Apply Config

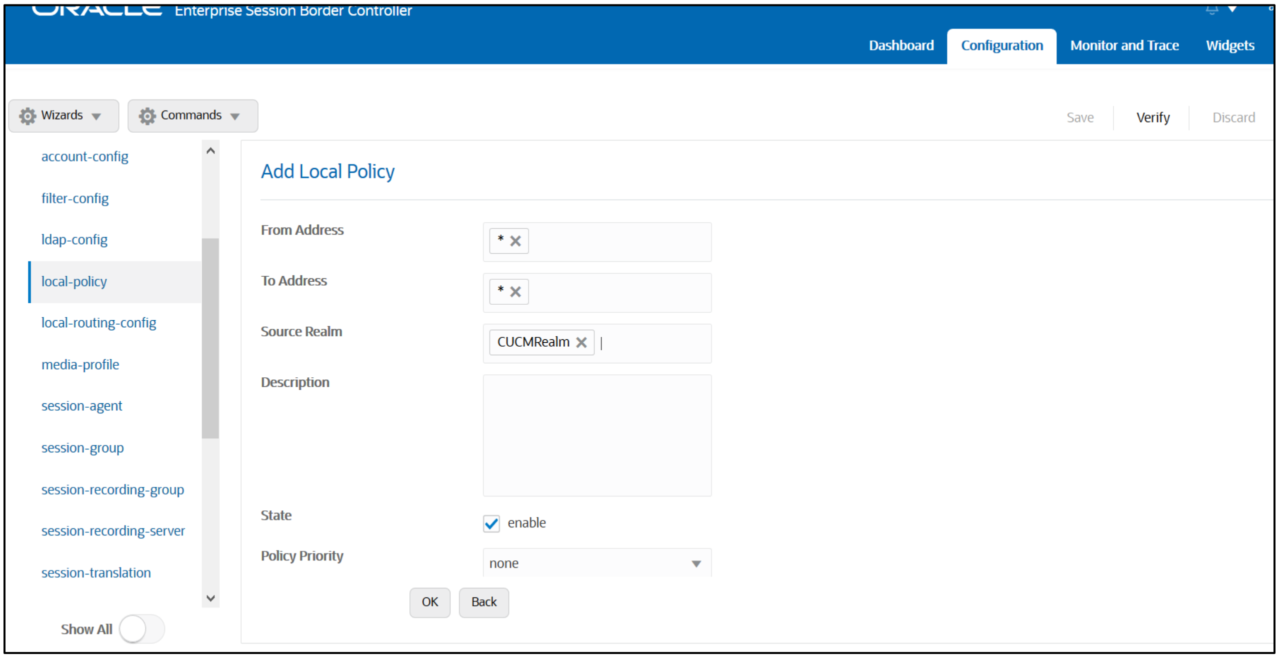
Enterprise Parameters Configuration

| | | |
|---|---|---|
| Syncing Mode for Enterprise Groups * | Differential Sync | Differential Sync |
| **Service Manager TCP ports parameters** | | |
| Service Manager TCP Server communication port number * | 8883 | 8888 |
| Service Manager TCP Client communication port number * | 8889 | 8889 |
| **CRS Application Parameters** | | |
| Auto Attendant Installed * | false | |
| IPCC Express Installed * | false | |
| **Clusterwide Domain Configuration** | | |
| Organization Top Level Domain | pe.oracle.com | |
| Cluster Fully Qualified Domain Name | CUCM-Cisco.pe.oracle.com | |
| **Denial-of-Service Protection** | | |
| Denial-of-Service Protection * | True | True |
| **TLS Handshake Timer** | | |
| TLS Handshake Timer * | 60 | 60 |
| **TLS Resumption Timer** | | |
| TLS Resumption Timer * | 3600 | 3600 |

## 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 Cisco side to Twilio side, Use the below local –policy



Add Local Policy

From Address: *

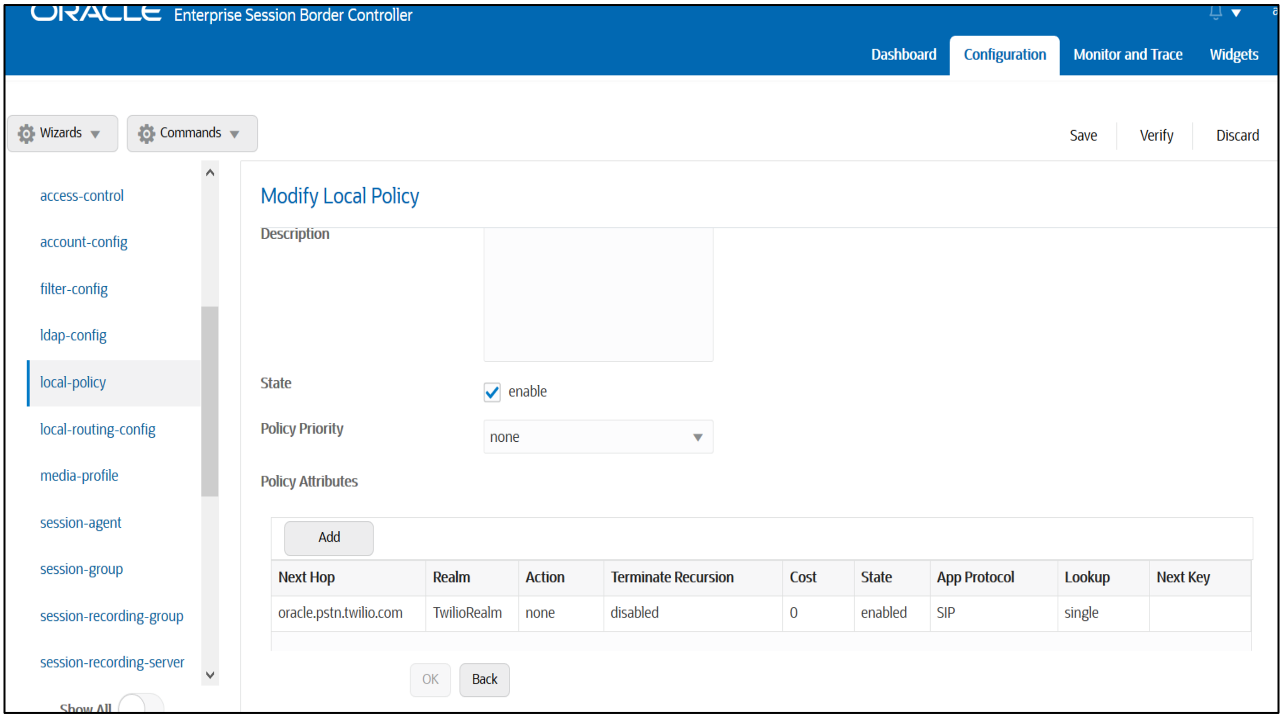
To Address: *

Source Realm: CUCMRealm

Description:

State: ☑ enable

Policy Priority: none



Modify Local Policy

Description:

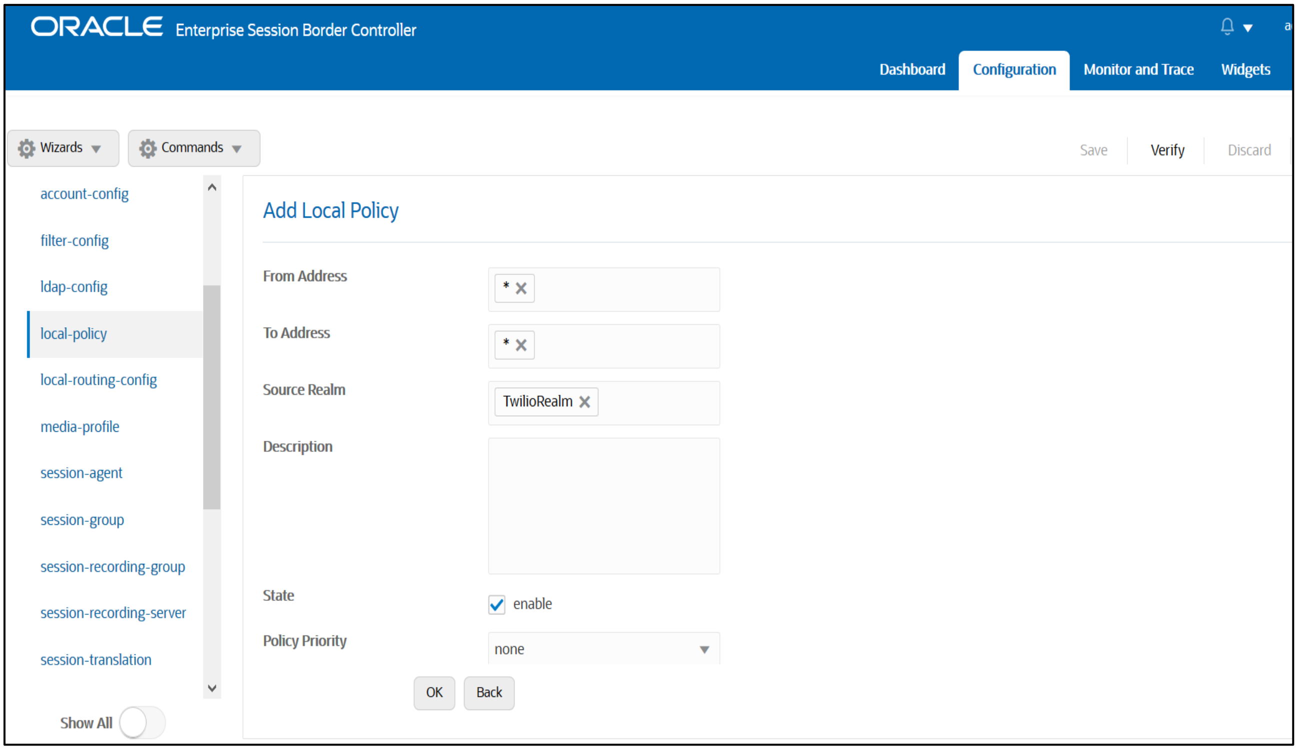
State: ☑ enable

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 Cisco side, Use the below local –policy



Add Local Policy

From Address: *

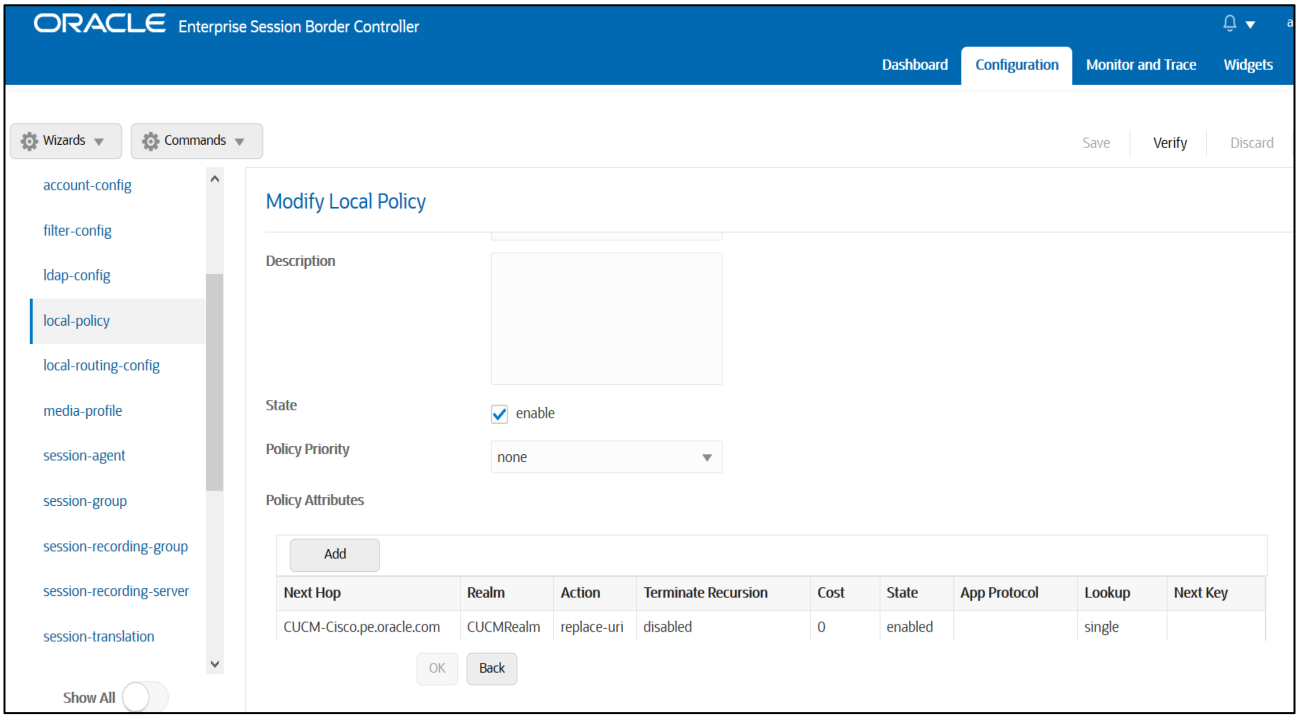
To Address: *

Source Realm: TwilioRealm

Description:

State: ☑ enable

Policy Priority: none



Modify Local Policy

Description:

State: ☑ enable

Policy Priority: none

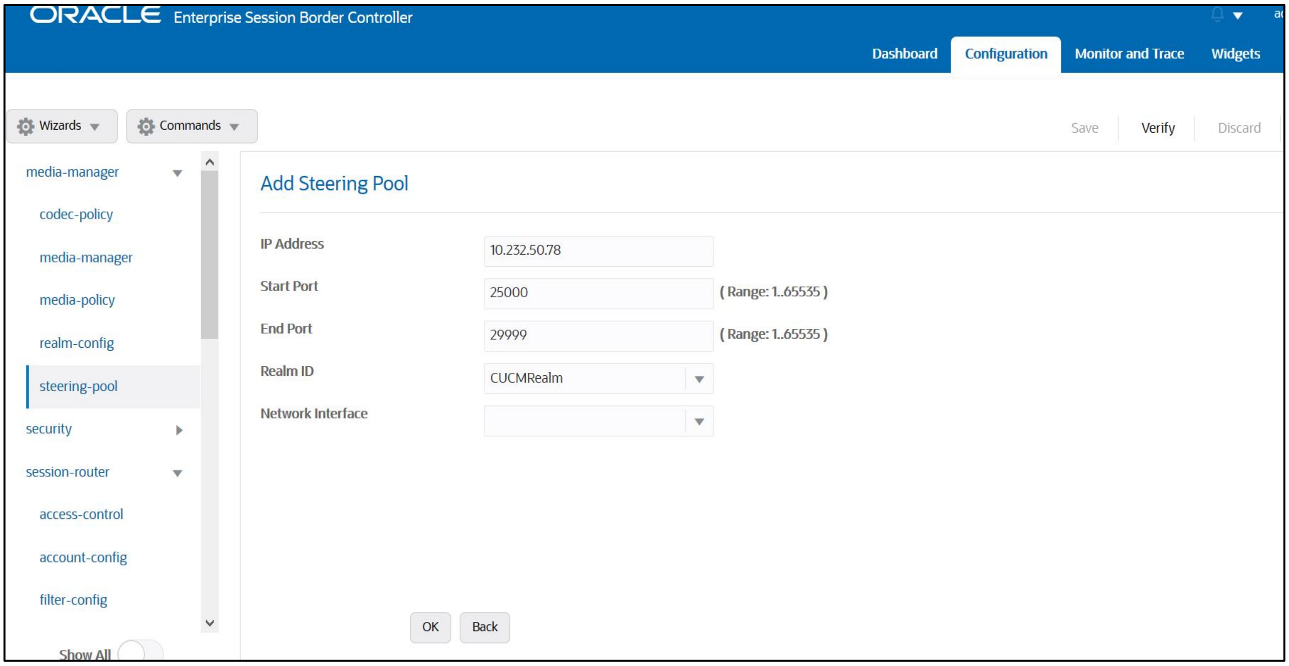
Policy Attributes

| Next Hop | Realm | Action | Terminate Recursion | Cost | State | App Protocol | Lookup | Next Key |
|---|---|---|---|---|---|---|---|---|
| CUCM-Cisco.pe.oracle.com | CUCMRealm | replace-uri | disabled | 0 | enabled | | single | |

## 6.13. Configure steering-pool

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

Cisco side steering pool.



Add Steering Pool

IP Address: 10.232.50.78

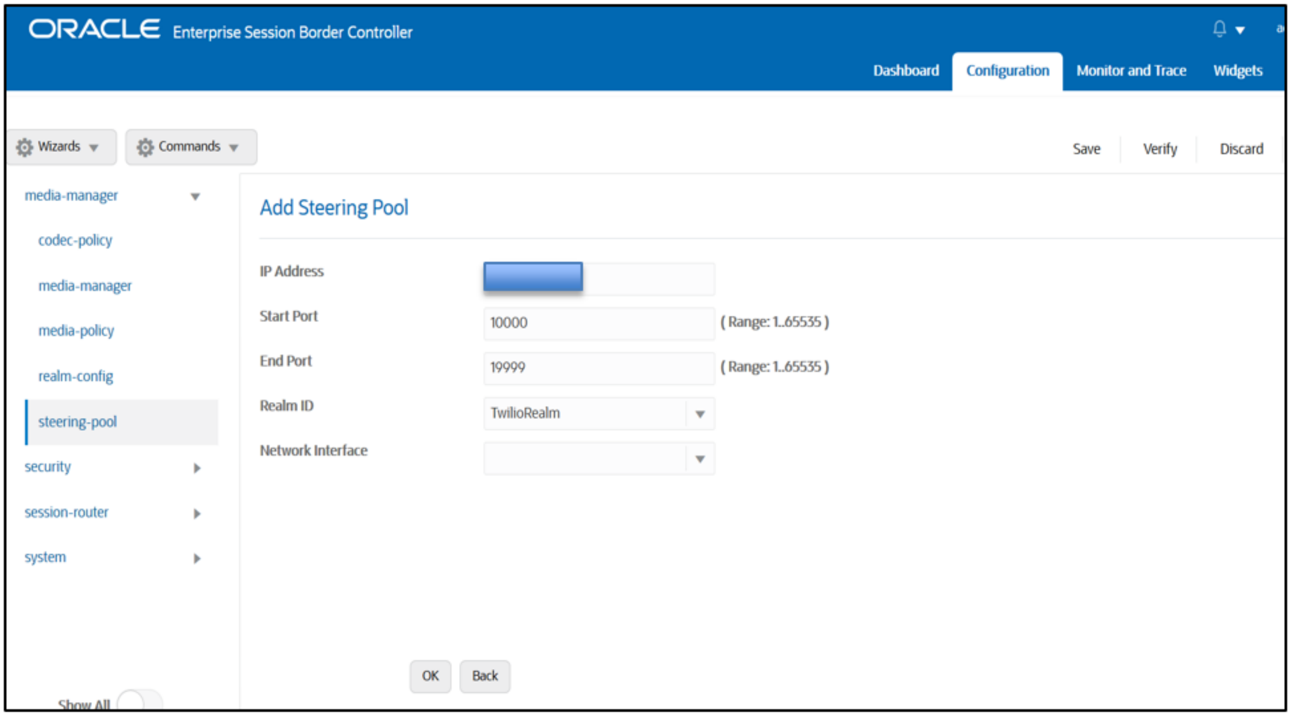
Start Port: 25000 ( Range: 1..65535 )

End Port: 29999 ( Range: 1..65535 )

Realm ID: CUCMRealm

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

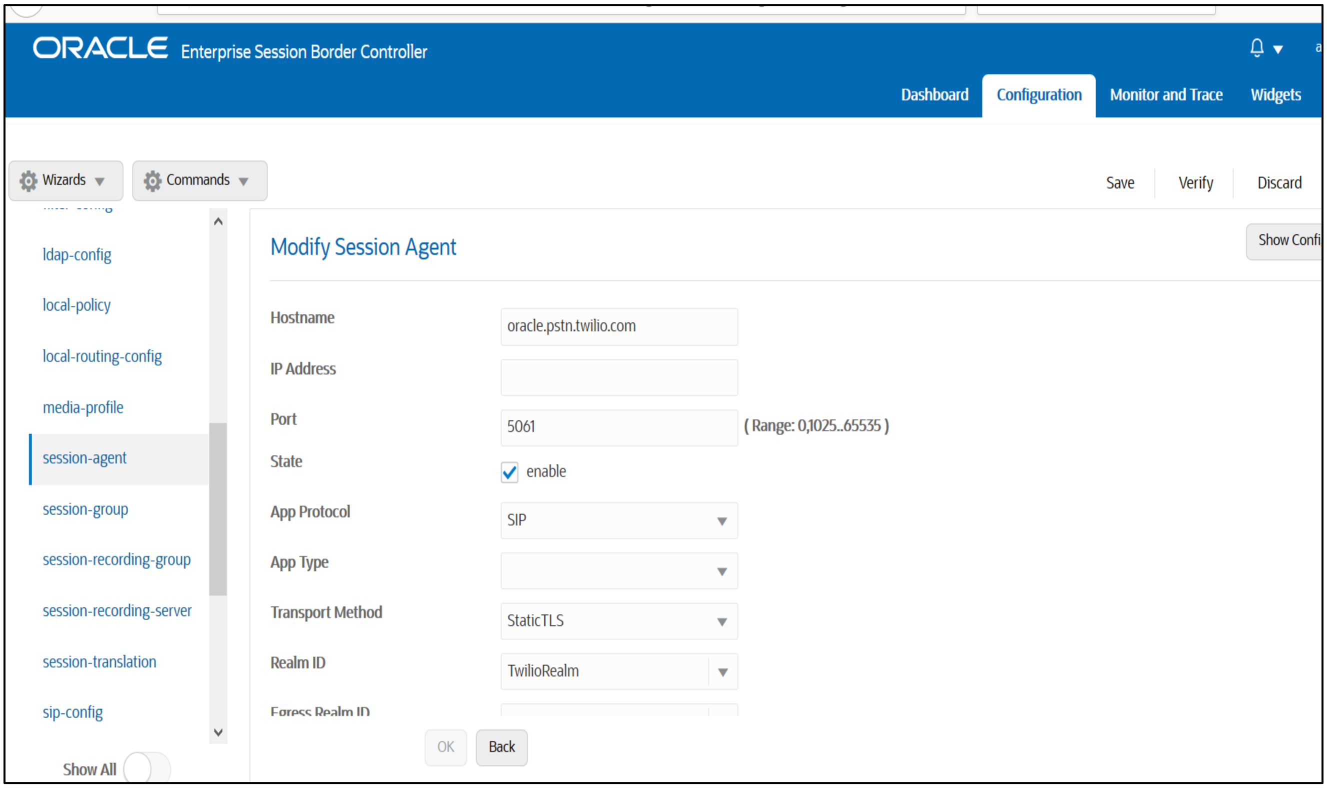
Network Interface:

## 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**.

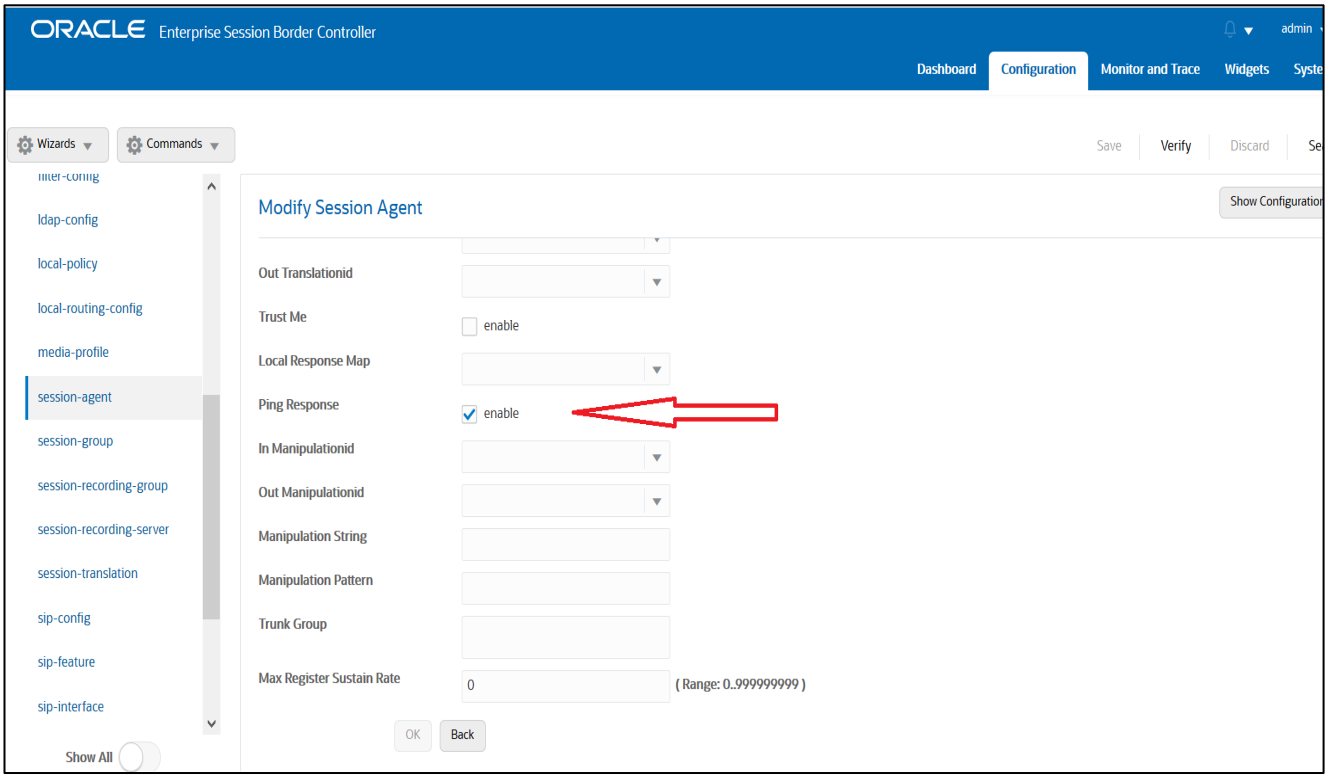
### Ping Response:

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

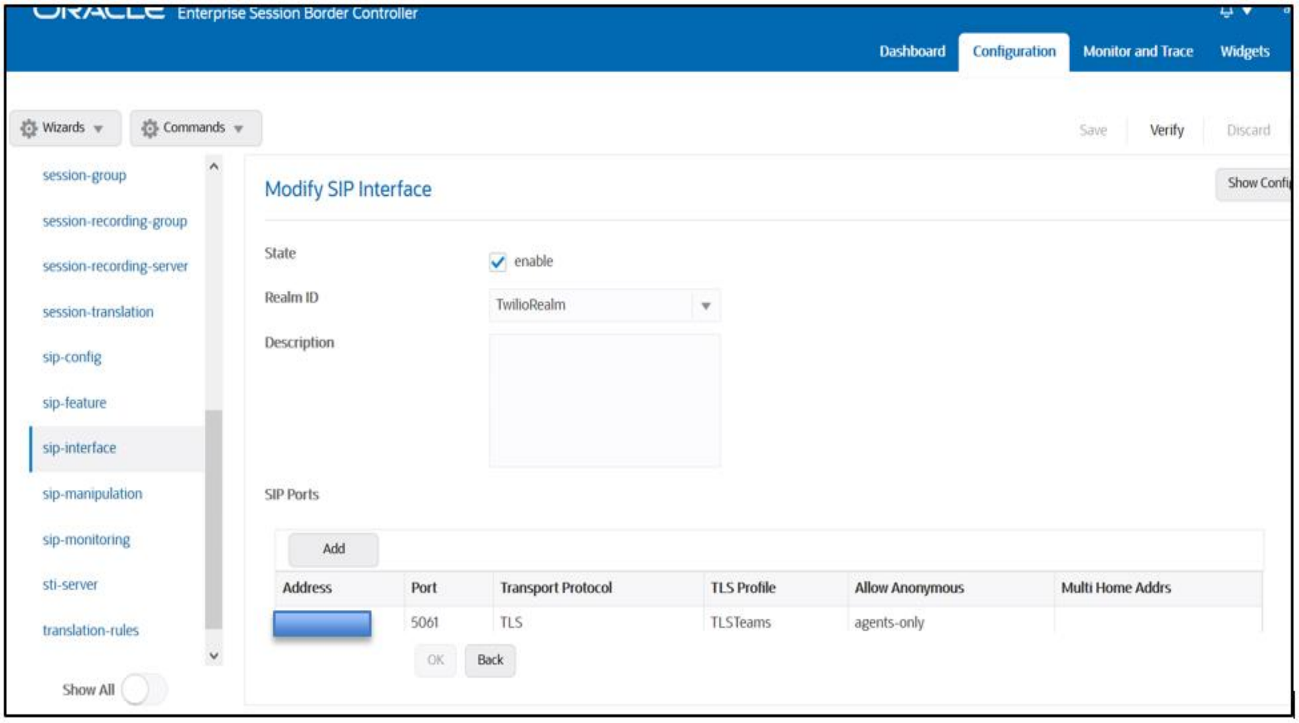
Trunk Group

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

## 6.15. SBC config for Cisco Offer less INVITE

When CUCM sends INVITE without SDP towards SBC and in that case, SBC needs to send out INVITE with SDP towards Twilio Elastic SIP trunk and vice versa. To do that, please set the parameter "**Add SDP Invite**" as both under Twilio sip interface as highlighted below. When this option is enabled, codecs have to be configured under the parameter "**Add SDP profiles**”. The configured codecs is also shown below.

**Note: this is an optional config – configure this only if CUCM sends offer less INVITE towards SBC.**



Modify SIP Interface

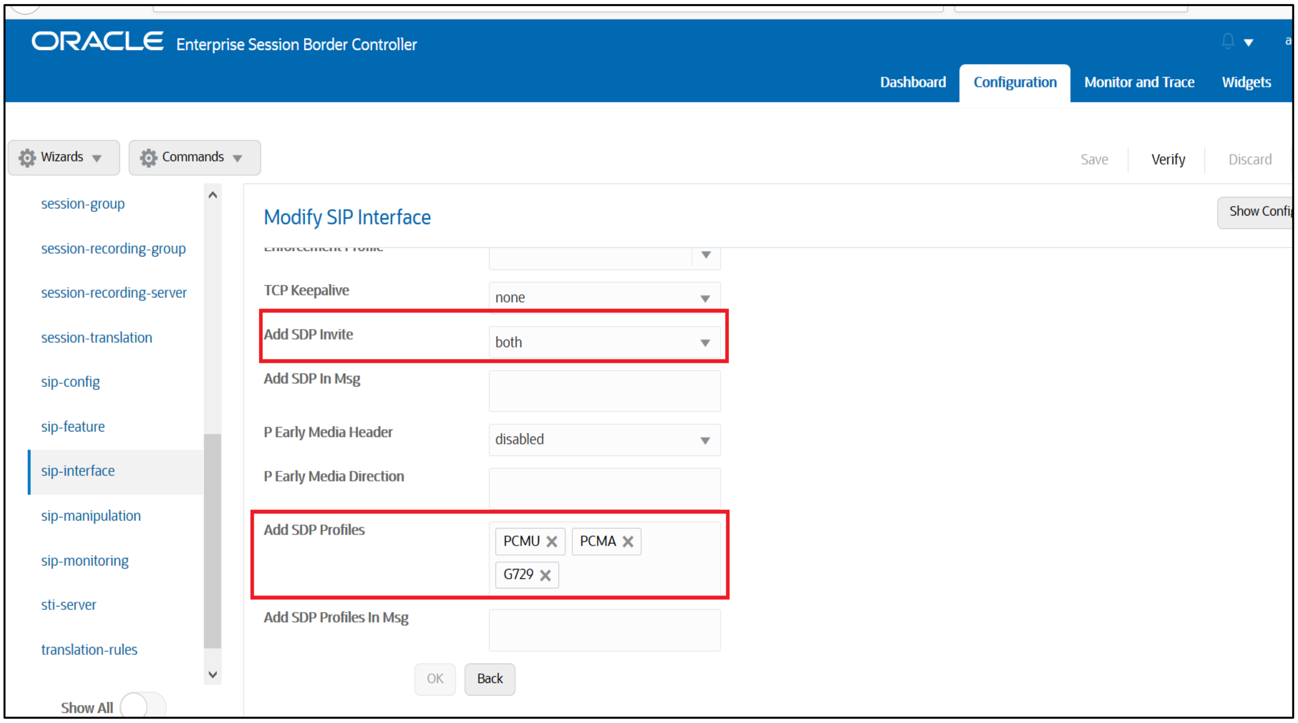
State ☑ enable

Realm ID TwilioRealm

Description

SIP Ports

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

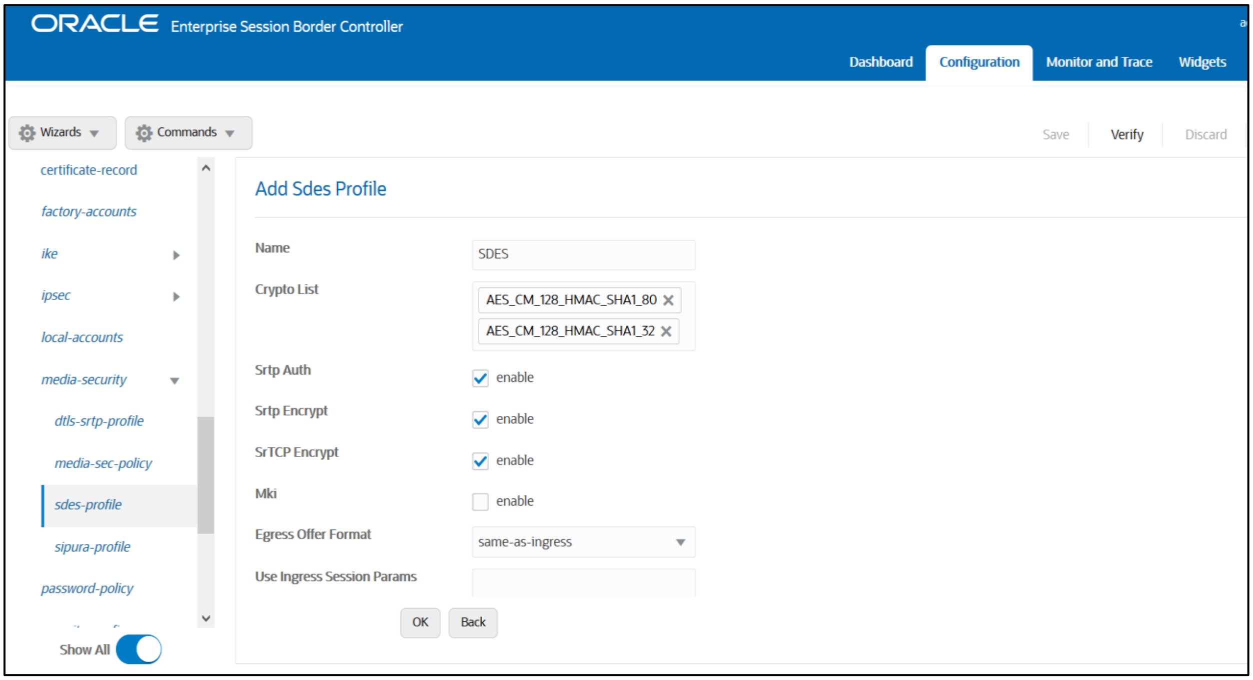


Modify SIP Interface

| | |
|---|---|
| Enforcement Profile | |
| TCP Keepalive | none |
| Add SDP Invite | both |
| Add SDP In Msg | |
| P Early Media Header | disabled |
| P Early Media Direction | |
| Add SDP Profiles | PCMU ✕ PCMA ✕ G729 ✕ |
| Add SDP Profiles In Msg | |

## 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

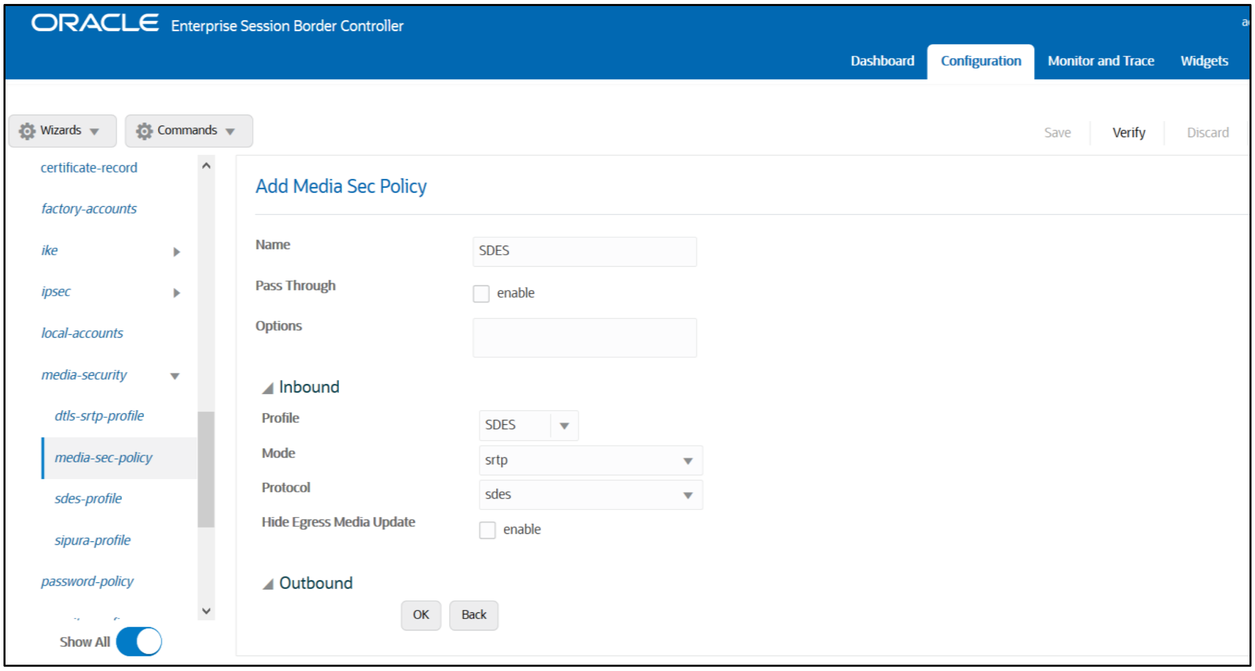
Mki: □ enable

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

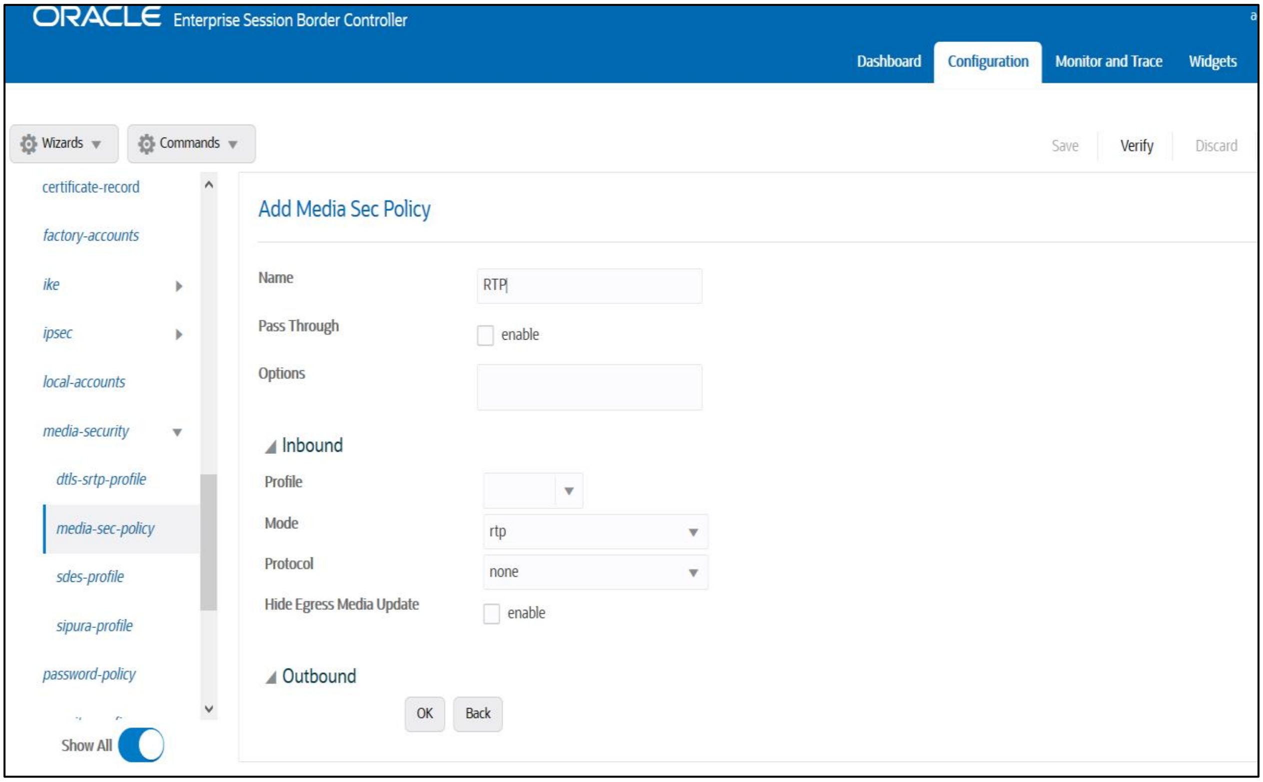
Mode: srtp

Protocol: sdes

Hide Egress Media Update: □ enable

Outbound

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



Add Media Sec Policy

Name: RTP

Pass Through: □ enable

Options:

Inbound

Profile:

Mode: rtp

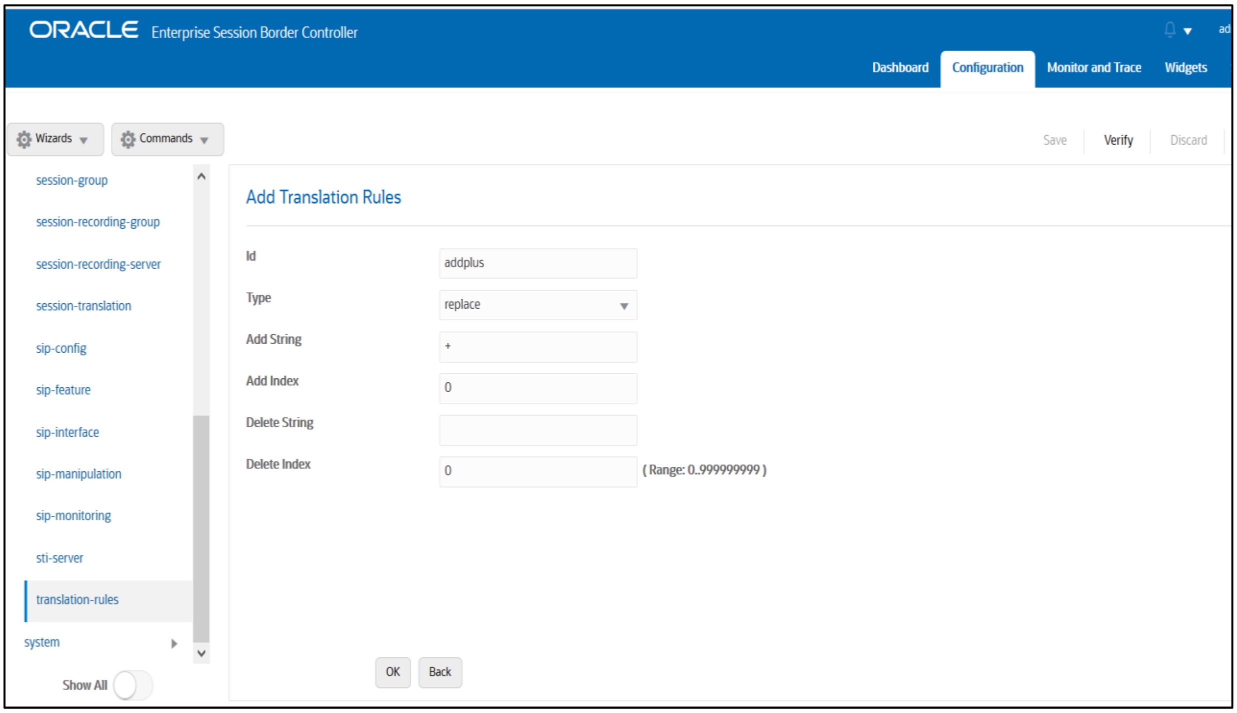
Protocol: none

Hide Egress Media Update: □ enable

Outbound

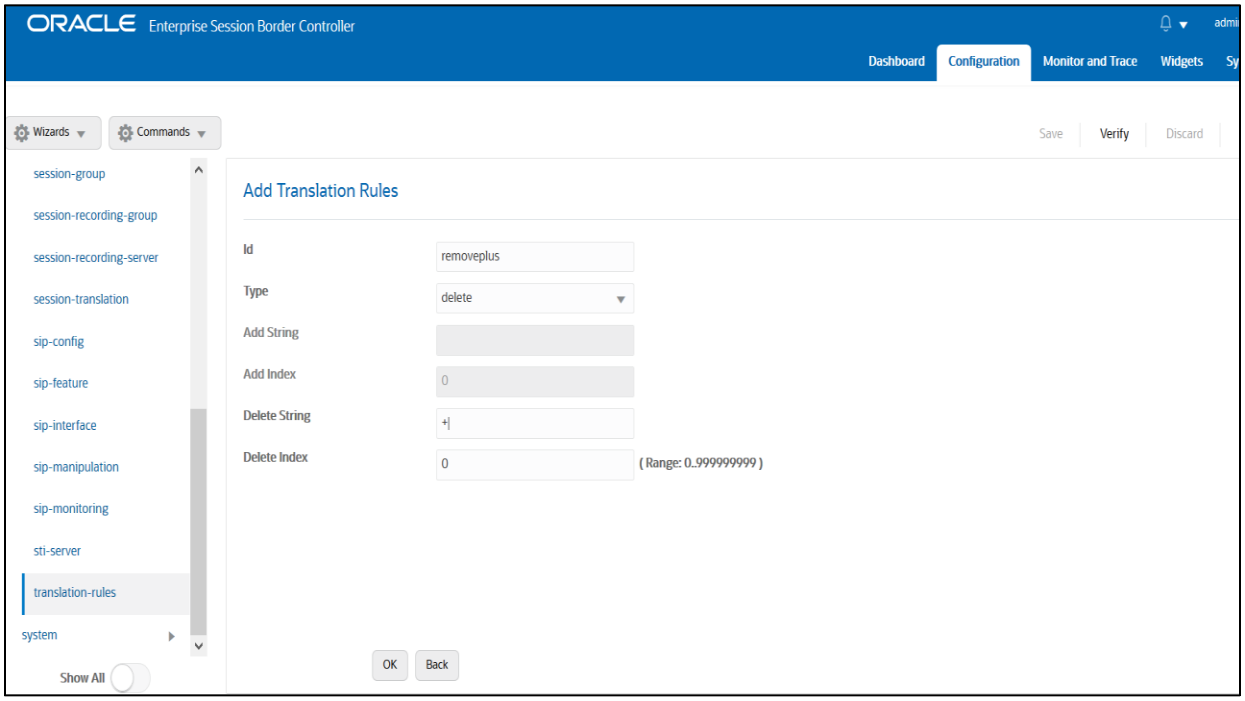
## 6.18. Configure Translation Rules

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 ) |



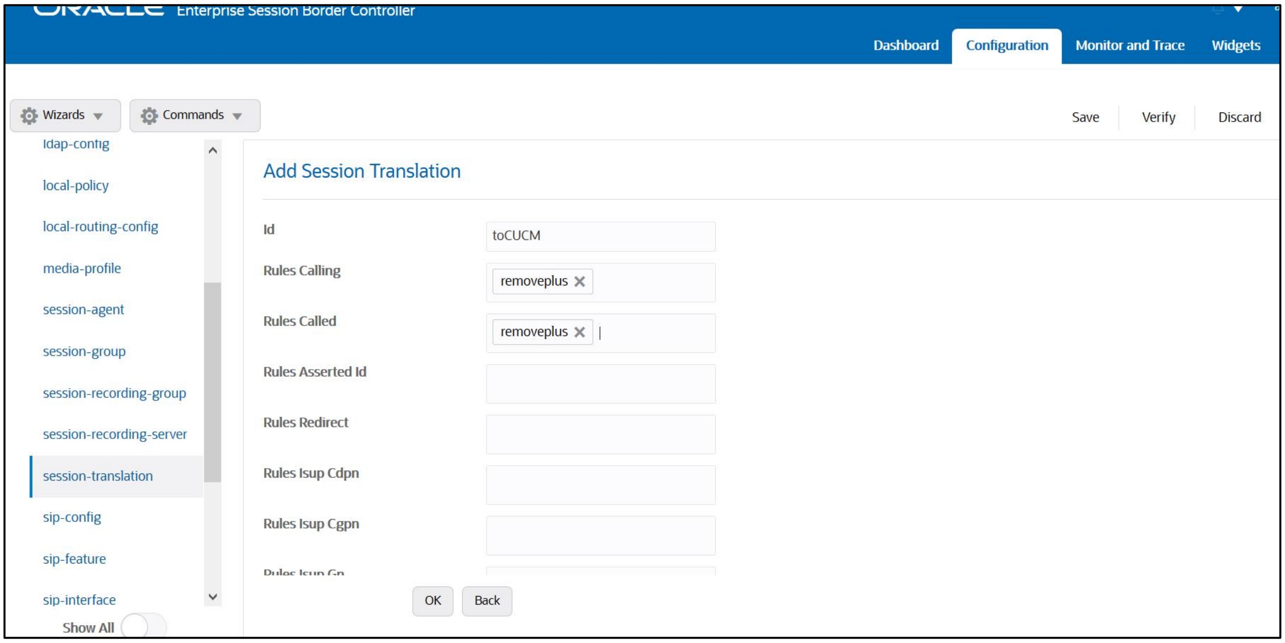
Add Translation Rules

| | |
|---|---|
| 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 Cisco side.



Add Session Translation

Id: toCUCM

Rules Calling: removeplus

Rules Called: removeplus

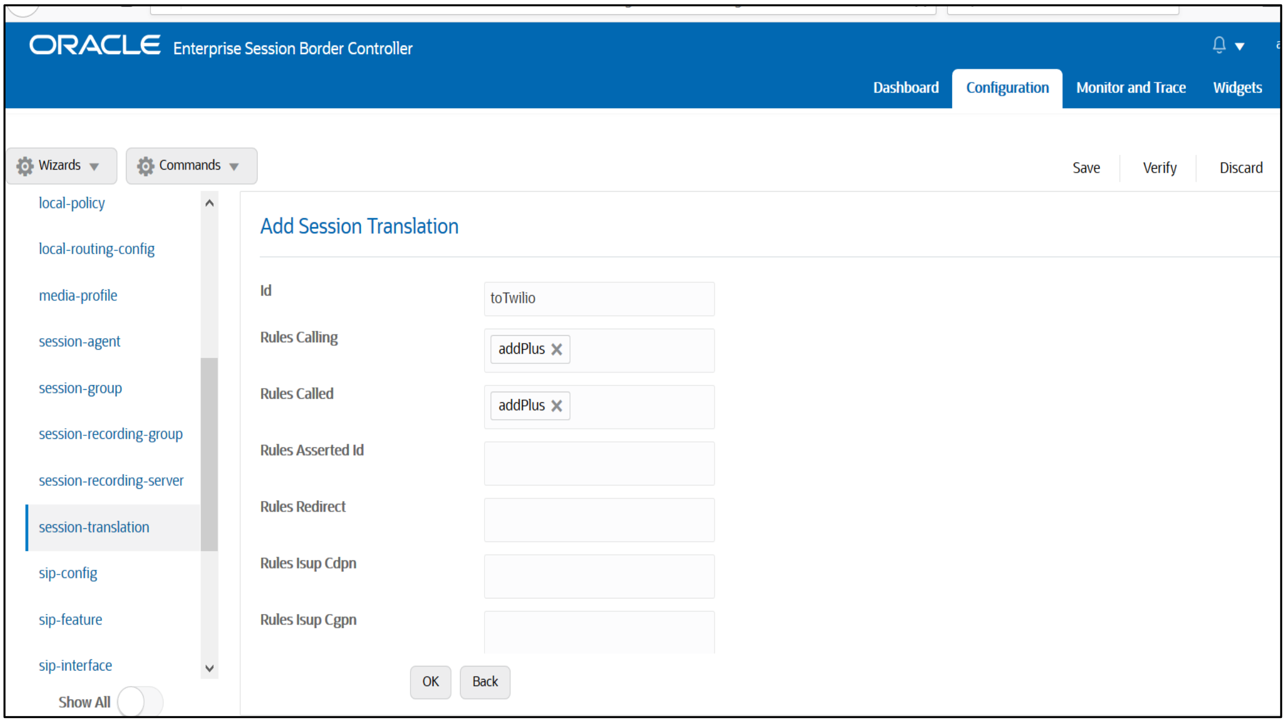
Rules Asserted Id

Rules Redirect

Rules Isup Cdpn

Rules Isup Cgpn

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

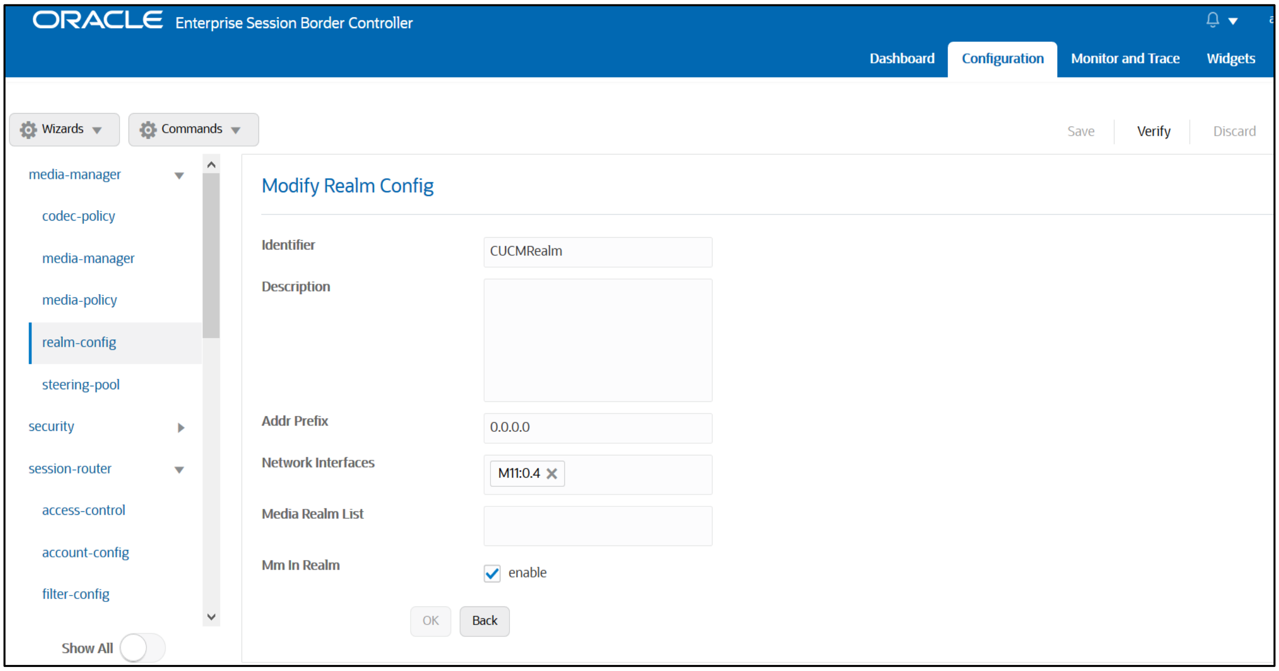
Rules Asserted Id

Rules Redirect

Rules Isup Cdpn

Rules Isup Cgpn

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



Modify Realm Config

Identifier: CUCMRealm

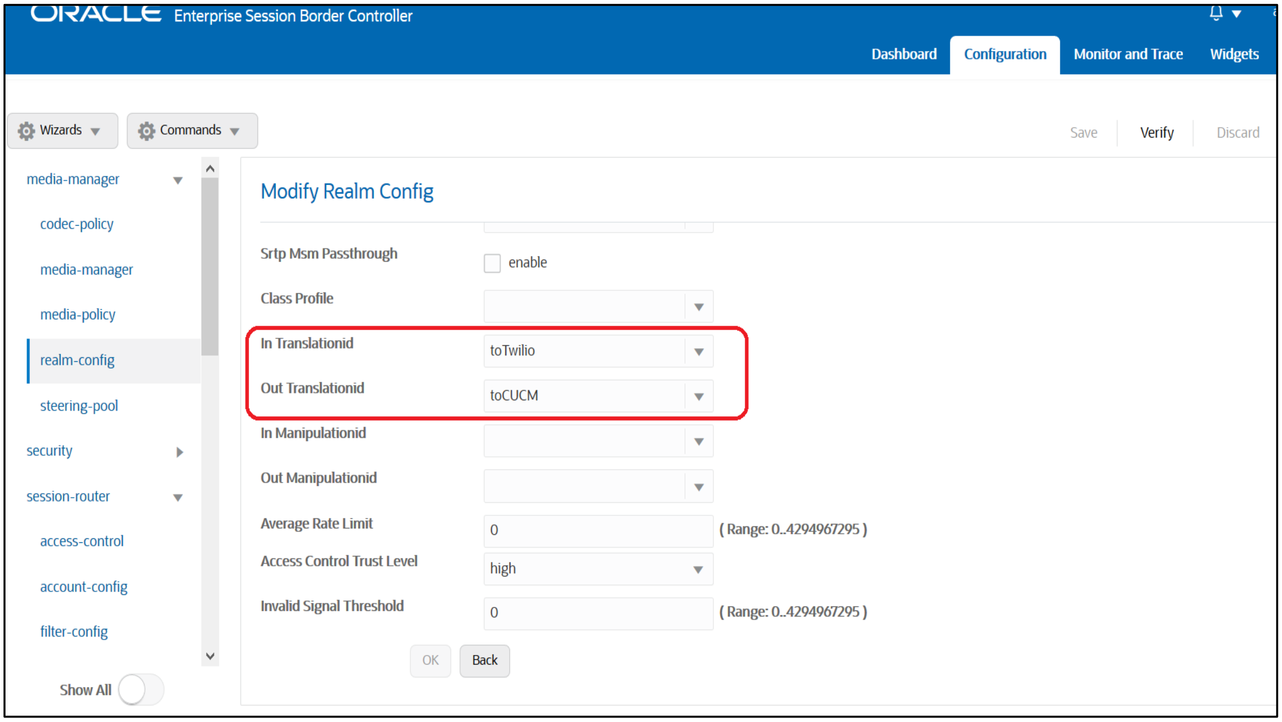
Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M11:0.4 ✕

Media Realm List:

Mm In Realm: ☑ enable



Modify Realm Config

Srtp Msm Passthrough: □ enable

Class Profile:

In Translationid: toTwilio

Out Translationid: toCUCM

In Manipulationid:

Out Manipulationid:

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

Access Control Trust Level: high

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

With this, SBC configuration is complete

# 7. SBC configuration for Cisco Remote Worker

This section of Cisco Remote Worker configuration is included for Cisco remote endpoints that register through the Oracle SBC to the Cisco Call Manager (Cisco CUCM). 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 Cisco endpoints which will register to Cisco CUCM through the SBC. SBC will handle the calls based on the registration information present in the cache. **Please note that Cisco Remote worker Access side is secured (TLS/SRTP) and Cisco 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 Cisco Remote worker
Steering Pool associated with the Realm for Cisco Remote worker
Sip-interface associated with the Realm for Cisco 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 Cisco Access Realm onto the SBC and then SBC registers these endpoints onto the Cisco 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.

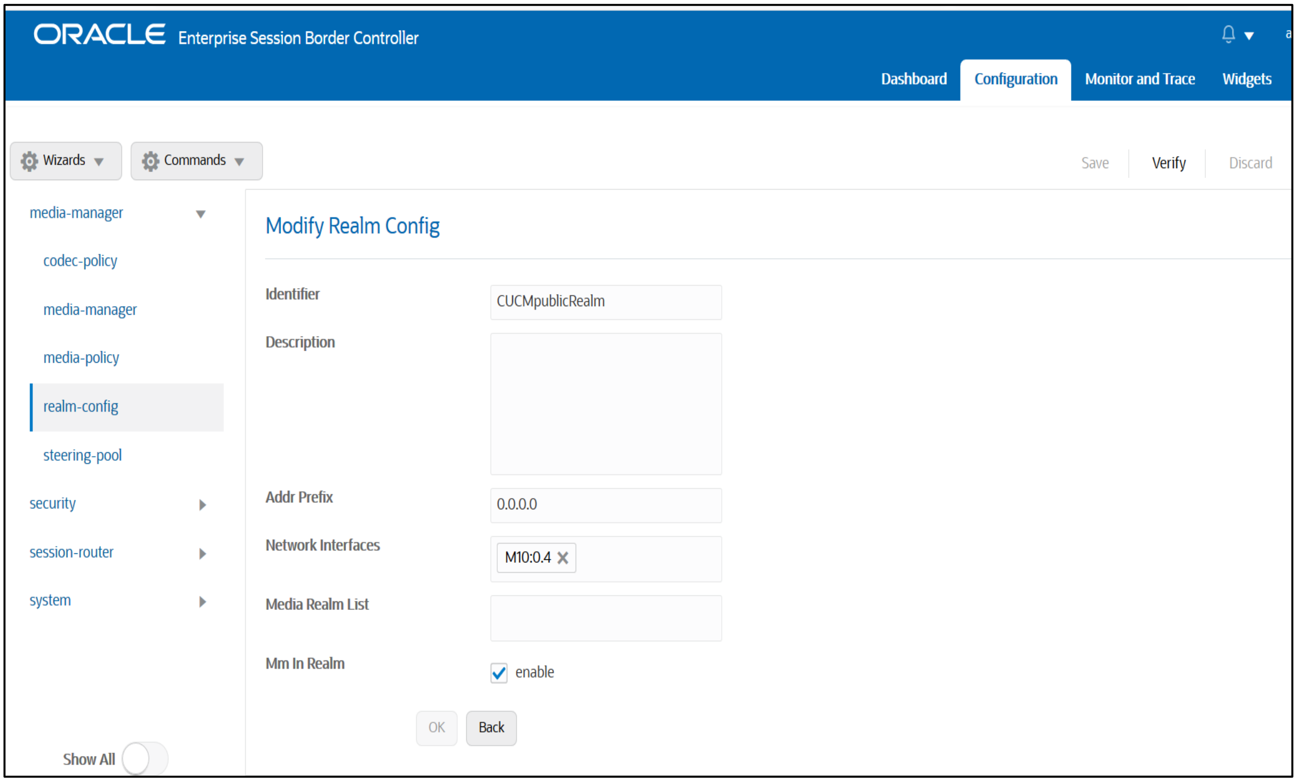
## 7.1. Configure Realms

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 | Cisco Access Side | Cisco Core Side |
|---|---|---|
| Identifier | CUCMpublicRealm | CUCMCoreRealm |
| Network Interface | M10 | M11 |
| Mm in realm | ☑ | ☑ |
| FQDN | | |
| Media Sec policy | sdespolicy | RTP |
| Access Control Trust Level | High | High |

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



Modify Realm Config

Identifier: CUCMpublicRealm

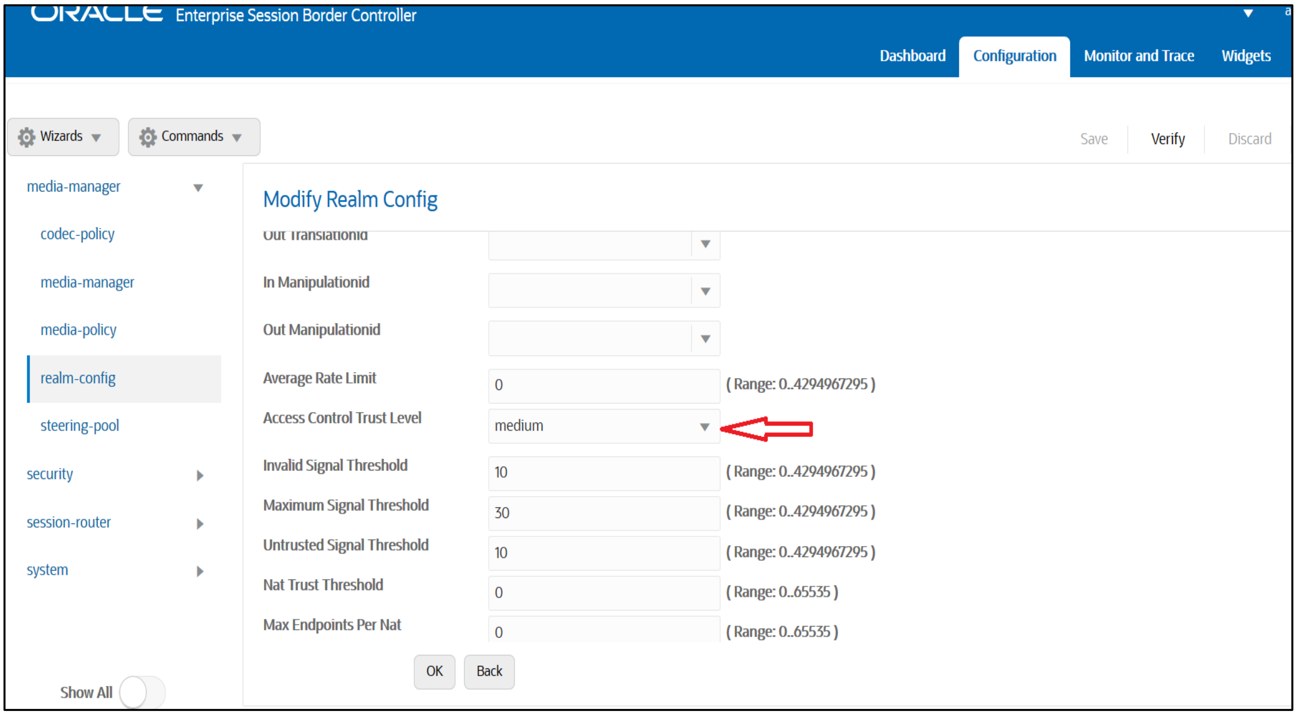
Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M10:0.4

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 )

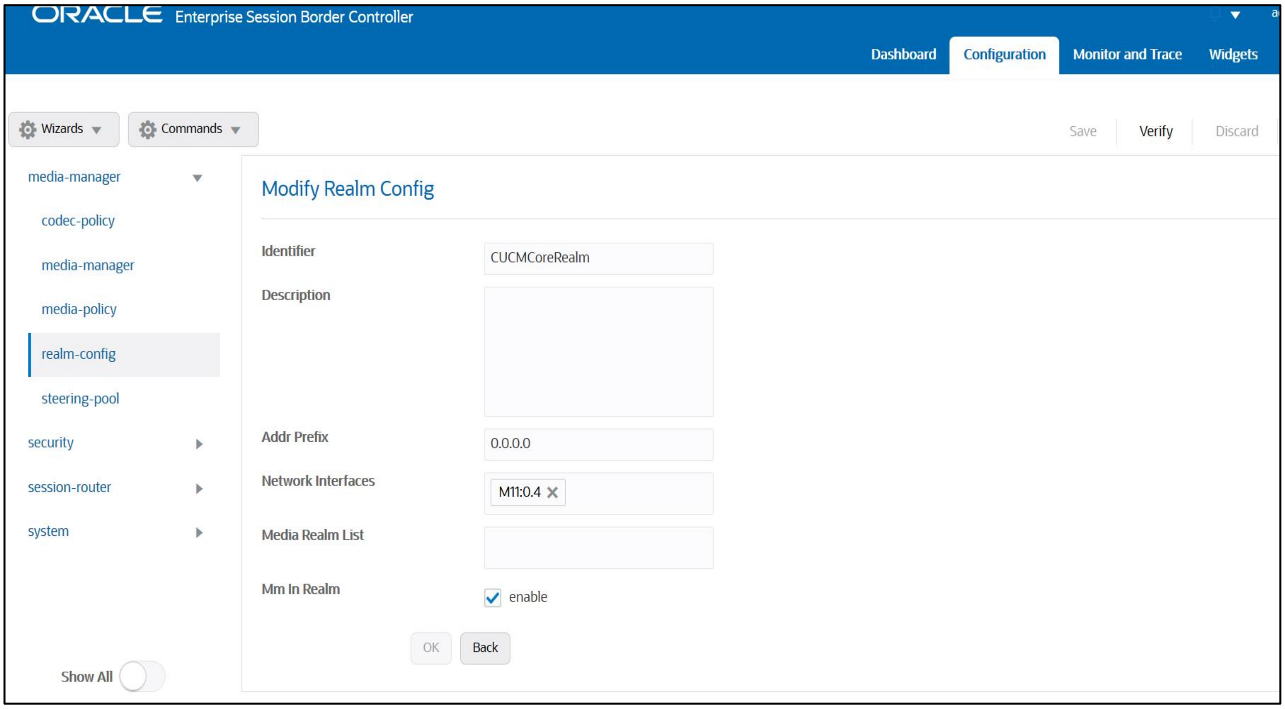
Maximum Signal Threshold: 30 ( Range: 0..4294967295 )

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 CUCMCoreRealm for Cisco Core side



Modify Realm Config

Identifier: CUCMCoreRealm

Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M11:0.4

Media Realm List:

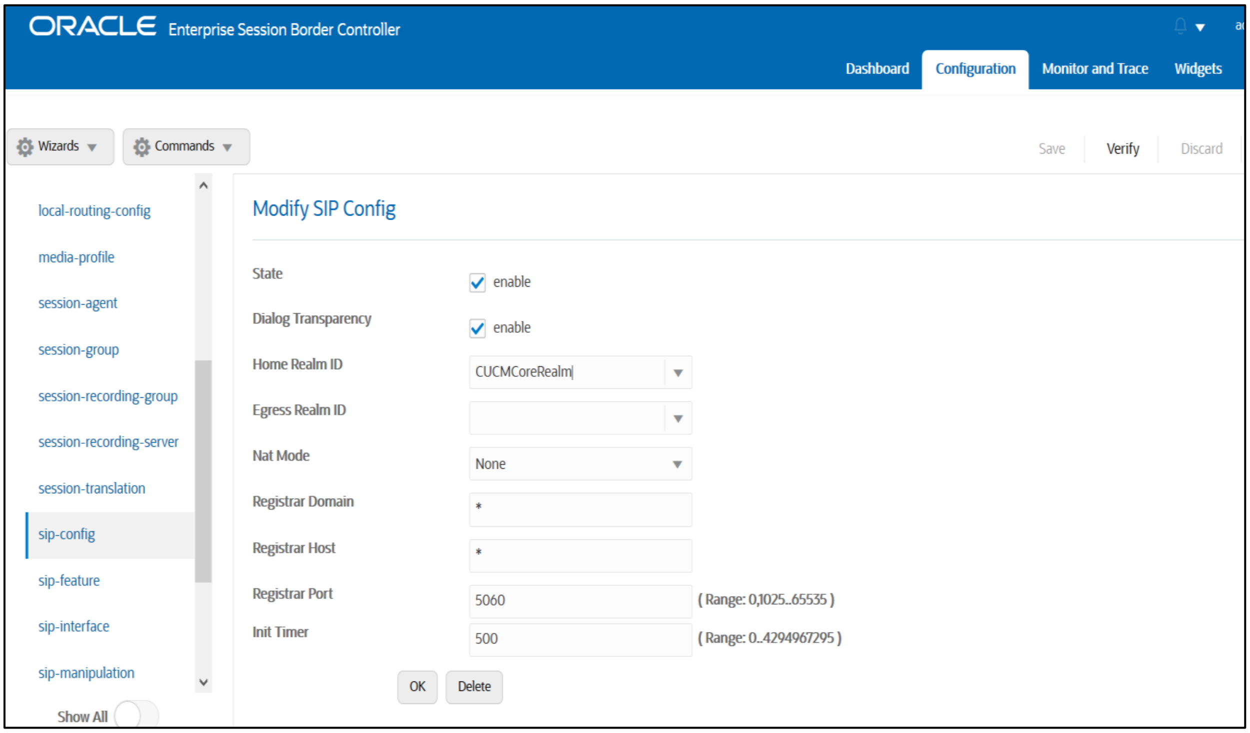
Mm In Realm: ☑ enable

## 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.

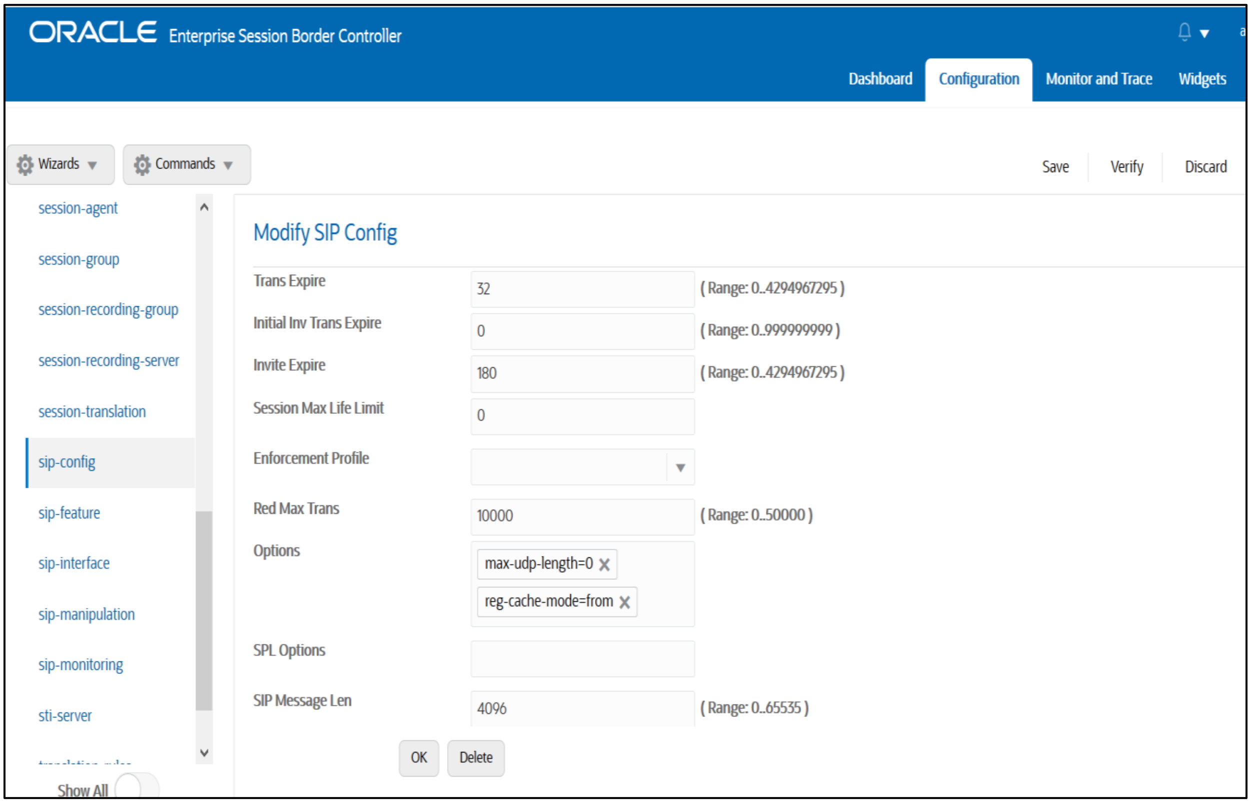
To configure sip-config, Go to Session-Router->sip-config and in options, add the below

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



Modify SIP Config

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



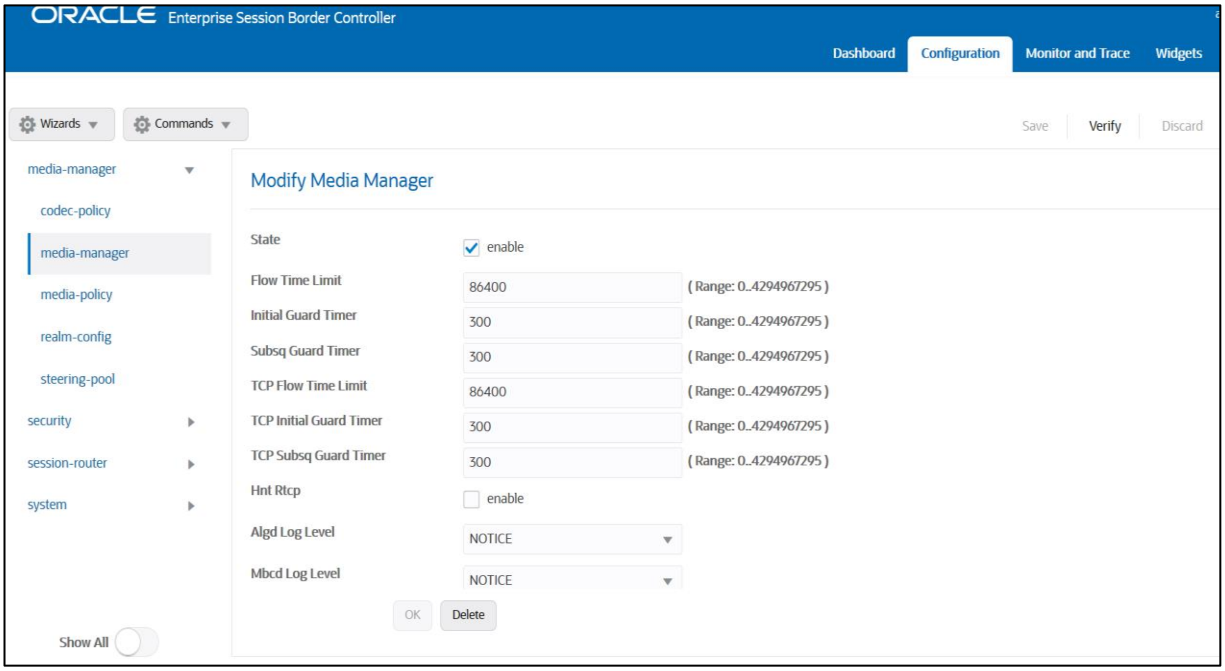
Modify SIP Config

| | |
|---|---|
| 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<br>reg-cache-mode=from |
| SPL Options | |
| SIP Message Len | 4096 ( Range: 0..65535 ) |

### 7.3. Enable media manager

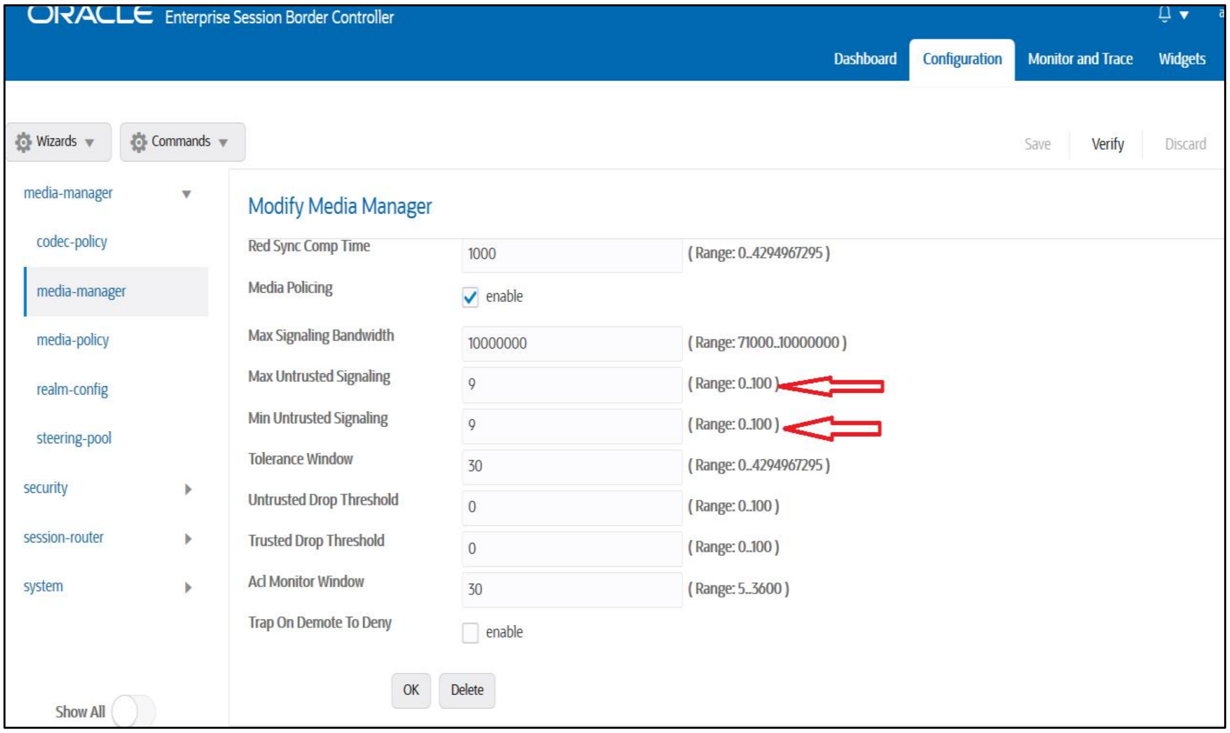
Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

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

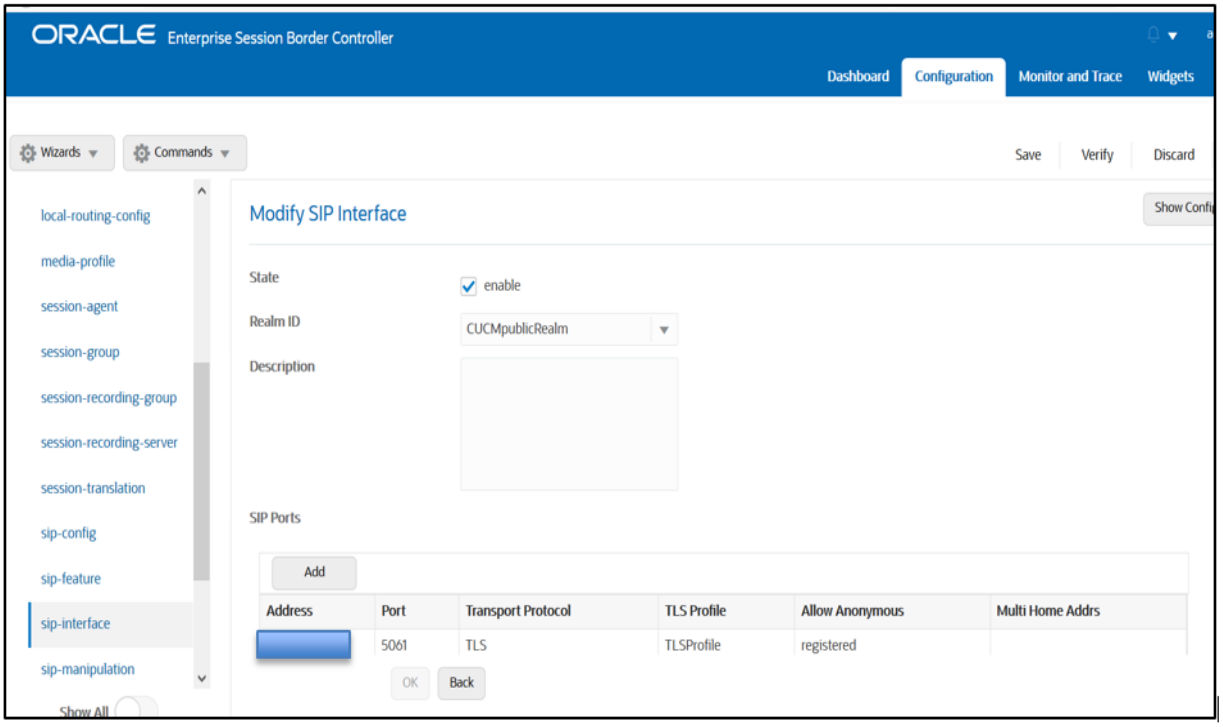
Red Sync Comp Time 1000 ( Range: 0..4294967295 )
Media Policing ☑ enable
Max Signaling Bandwidth 10000000 ( Range: 71000..10000000 )
Max Untrusted Signaling 9 ( Range: 0..100 )
Min Untrusted Signaling 9 ( Range: 0..100 )
Tolerance Window 30 ( Range: 0..4294967295 )
Untrusted Drop Threshold 0 ( Range: 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 Cisco 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

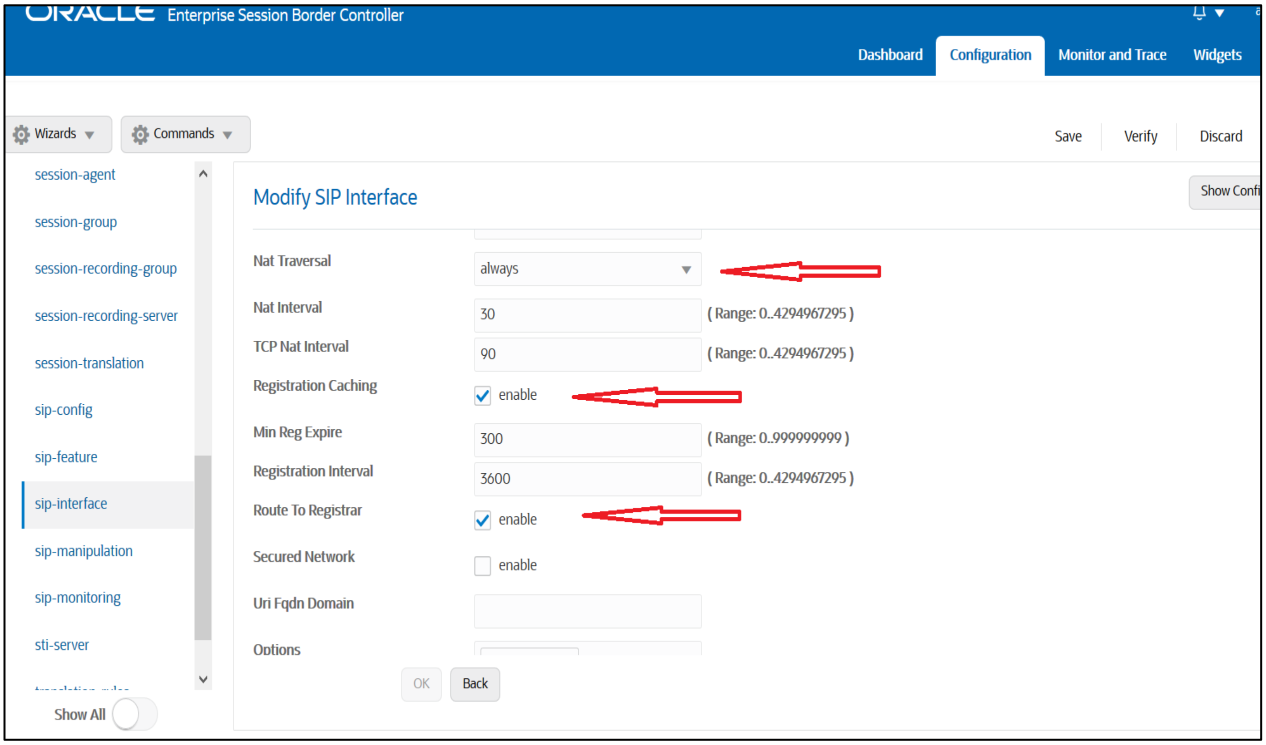
State ☑ enable

Realm ID CUCMpublicRealm

Description

SIP Ports

| Address | Port | Transport Protocol | TLS Profile | Allow Anonymous | Multi Home Addrs |
|---|---|---|---|---|---|
|  | 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 )

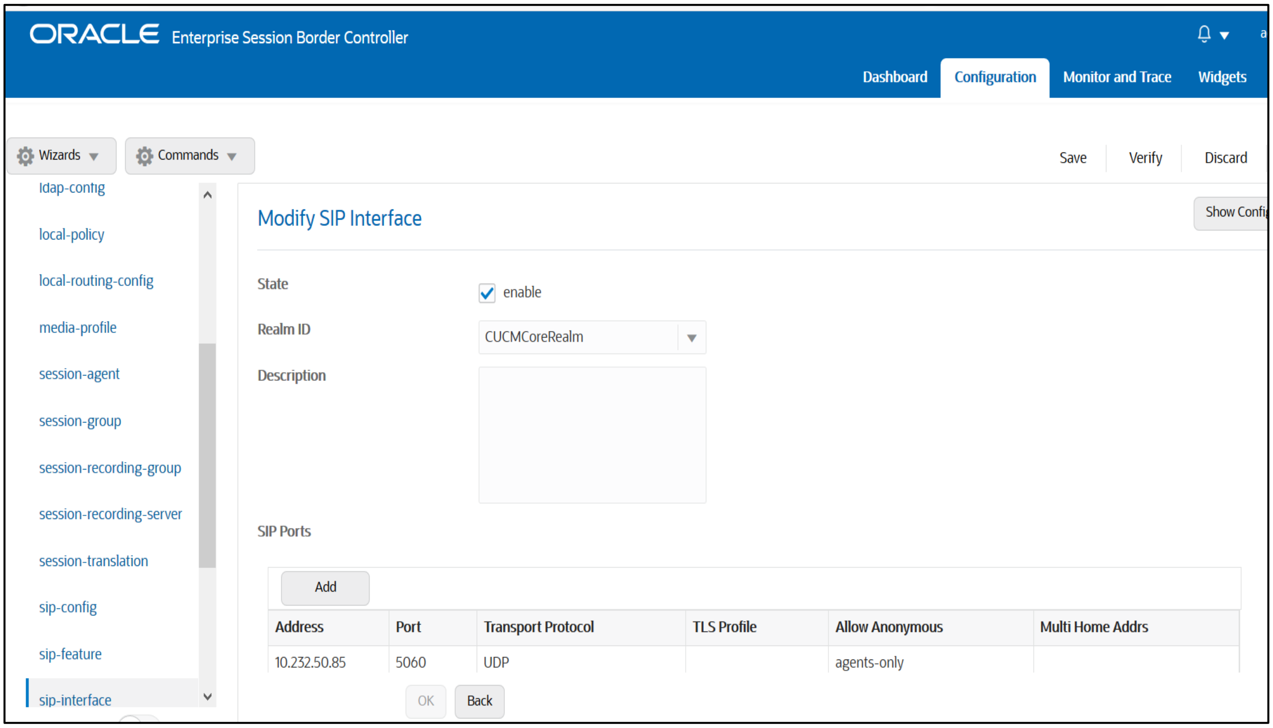
Route To Registrar: ☑ enable

Secured Network: □ enable

Uri Fqdn Domain:

Options:

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



Modify SIP Interface

State: ☑ enable

Realm ID: CUCMCoreRealm

Description:

SIP Ports

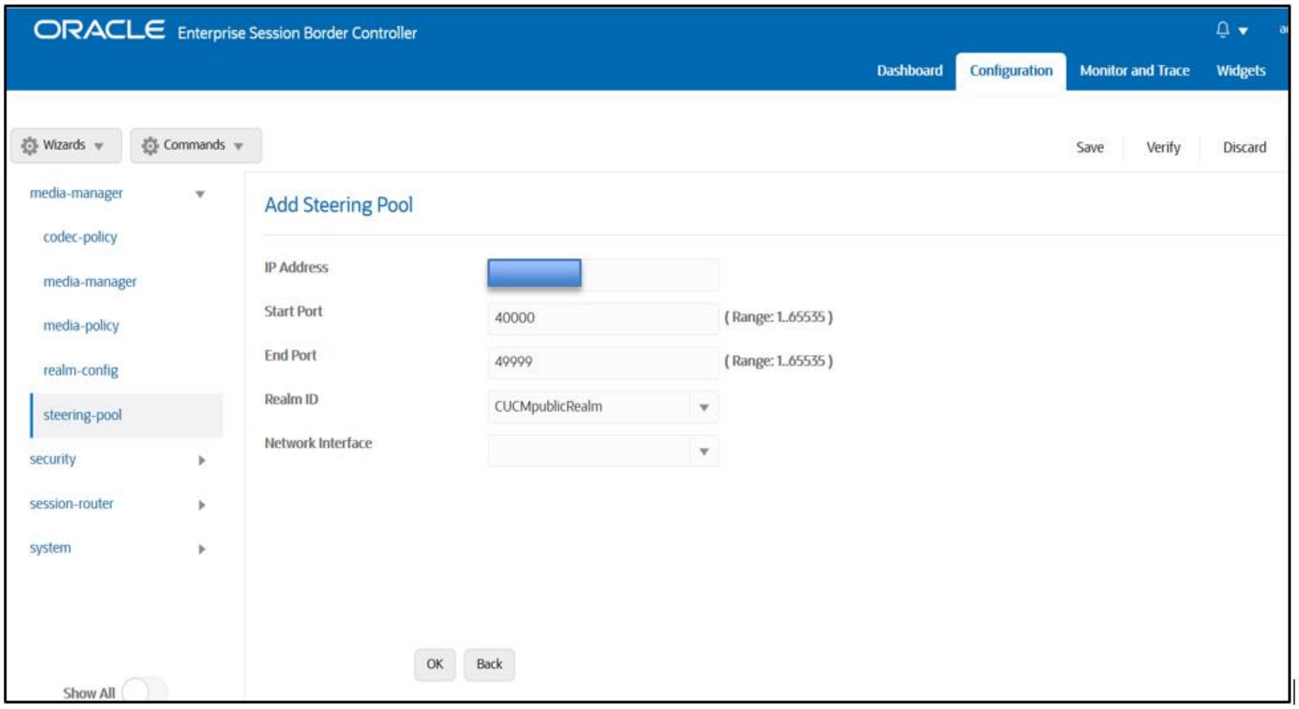
| Address | Port | Transport Protocol | TLS Profile | Allow Anonymous | Multi Home Addrs |
|---|---|---|---|---|---|
| 10.232.50.85 | 5060 | UDP |  | agents-only |  |

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.

Cisco Access side steering pool.



Add Steering Pool

IP Address [redacted]

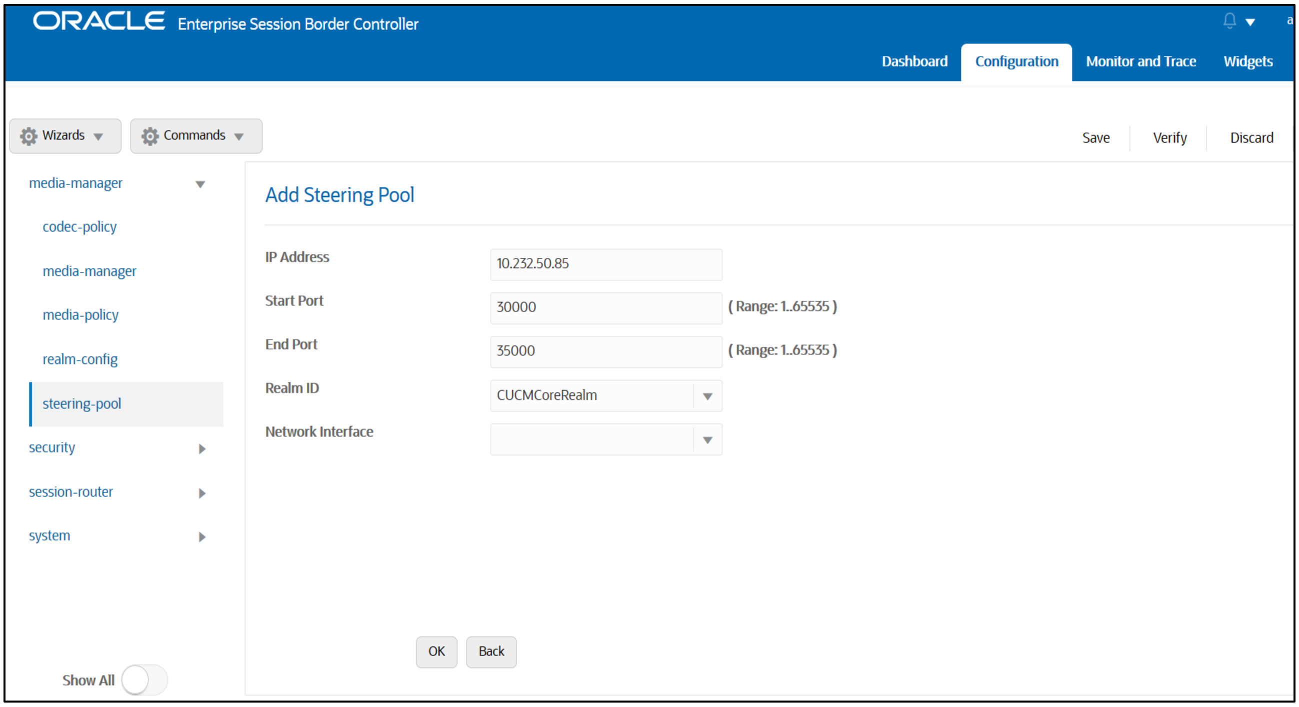
Start Port 40000 ( Range: 1..65535 )

End Port 49999 ( Range: 1..65535 )

Realm ID CUCMpublicRealm

Network Interface

Cisco Core side steering pool.



Add Steering Pool

IP Address 10.232.50.85

Start Port 30000 ( Range: 1..65535 )

End Port 35000 ( Range: 1..65535 )

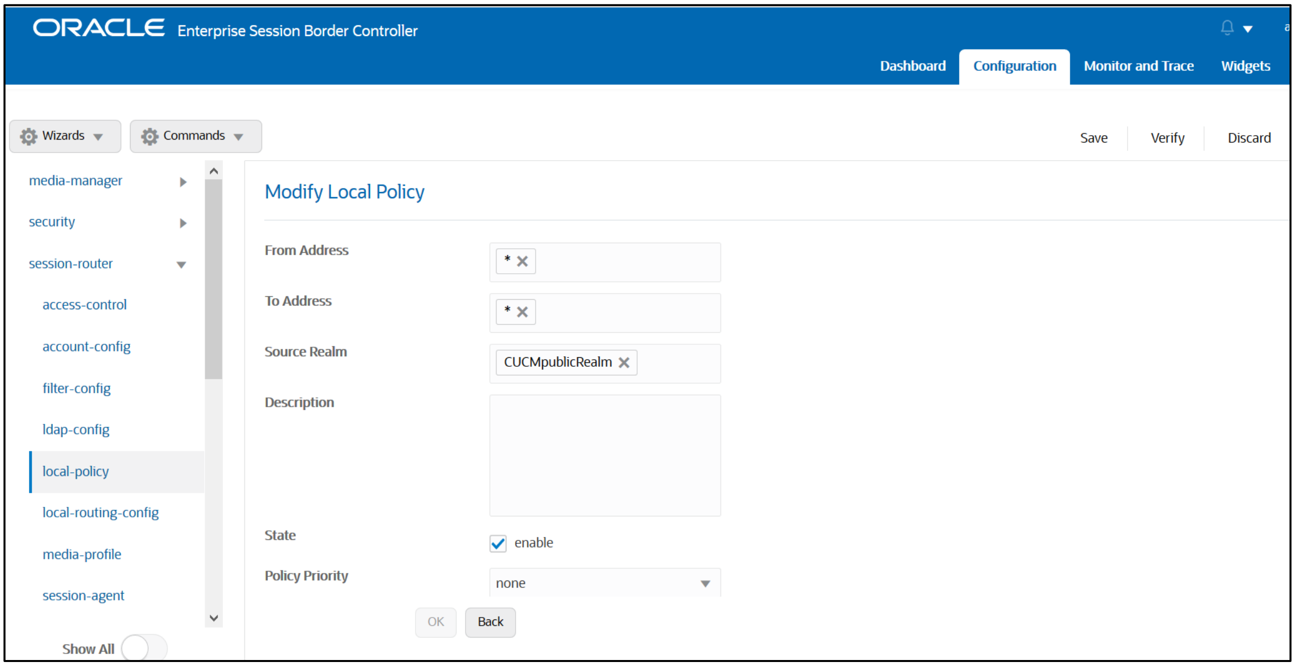
Realm ID CUCMCoreRealm

Network Interface

## 7.6. Configure local-policy (Optional)

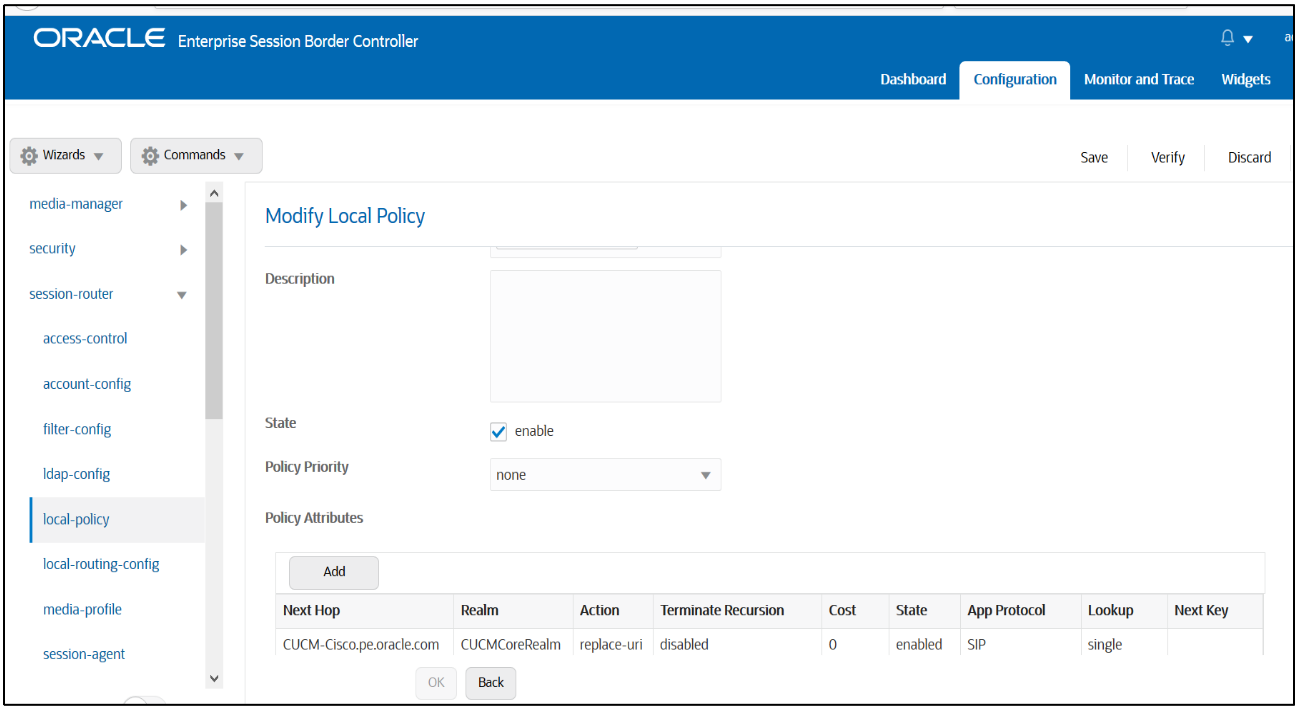
Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

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



Modify Local Policy

| | |
|---|---|
| From Address | * |
| To Address | * |
| Source Realm | CUCMpublicRealm |
| 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 |
|---|---|---|---|---|---|---|---|---|
| CUCM-Cisco.pe.oracle.com | CUCMCoreRealm | replace-uri | disabled | 0 | enabled | SIP | single | |

Cisco Offer less INVITE can happen in the Remote worker scenarios too.
In that case, please set the parameter "**Add SDP Invite**" as both and "**Add SDP profiles**" under Cisco Access side sip-interface. The configuration is similar to what we have done in Sec 6.15.

# 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 Cisco Call 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

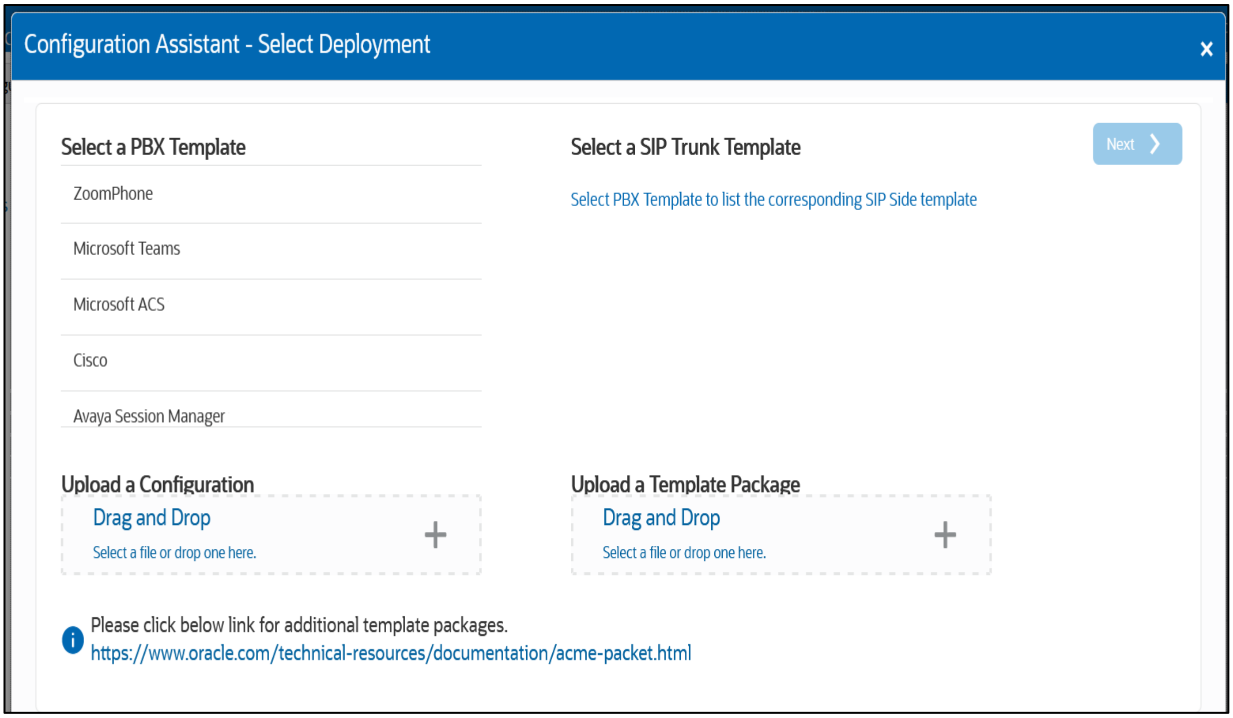
The following outline assumes you have established initial access to the SBC via console and completed the following steps:

- 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

Next ❯

Select PBX Template to list the corresponding SIP Side template

Upload a Configuration

Drag and Drop

Select a file or drop one here. +

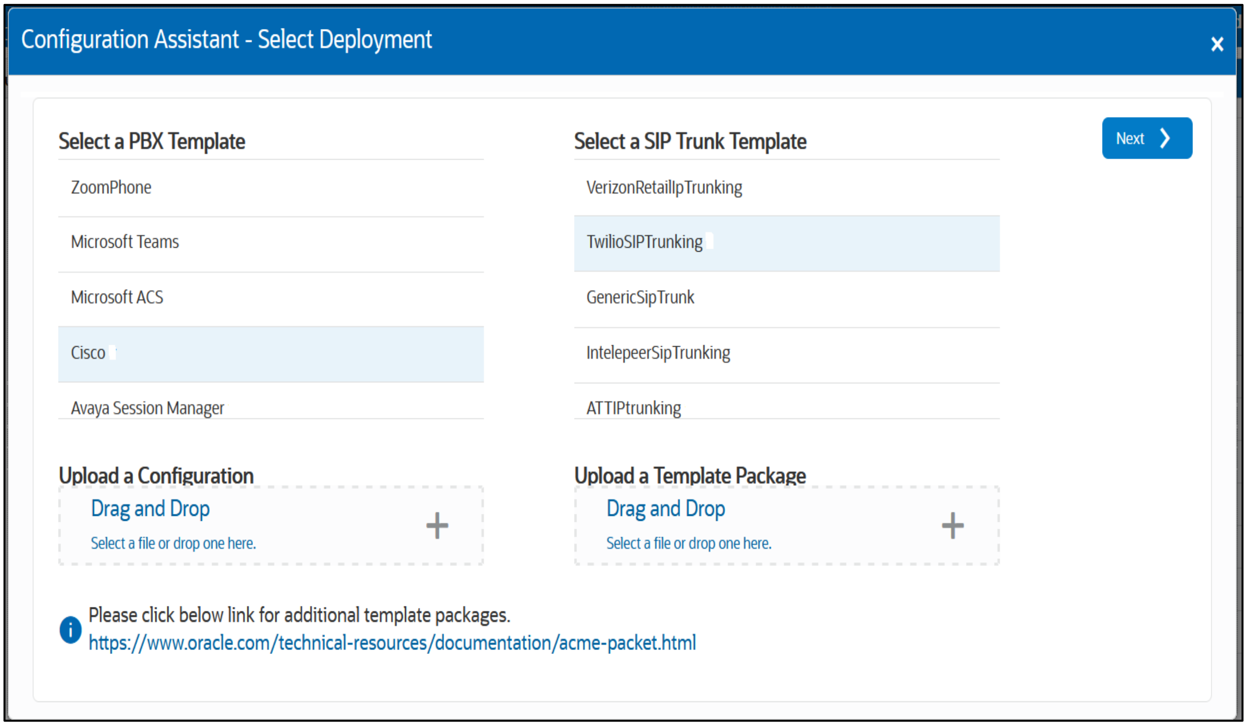
Upload a Template Package

Drag and Drop

Select a file or drop one here. +

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

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 Cisco 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

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

Select a SIP Trunk Template

Next ❯

- VerizonRetailIpTrunking
- TwilioSIPTrunking
- GenericSipTrunk
- IntelepeerSipTrunking
- ATTIPtrunking

Upload a Configuration

Drag and Drop

Select a file or drop one here. +

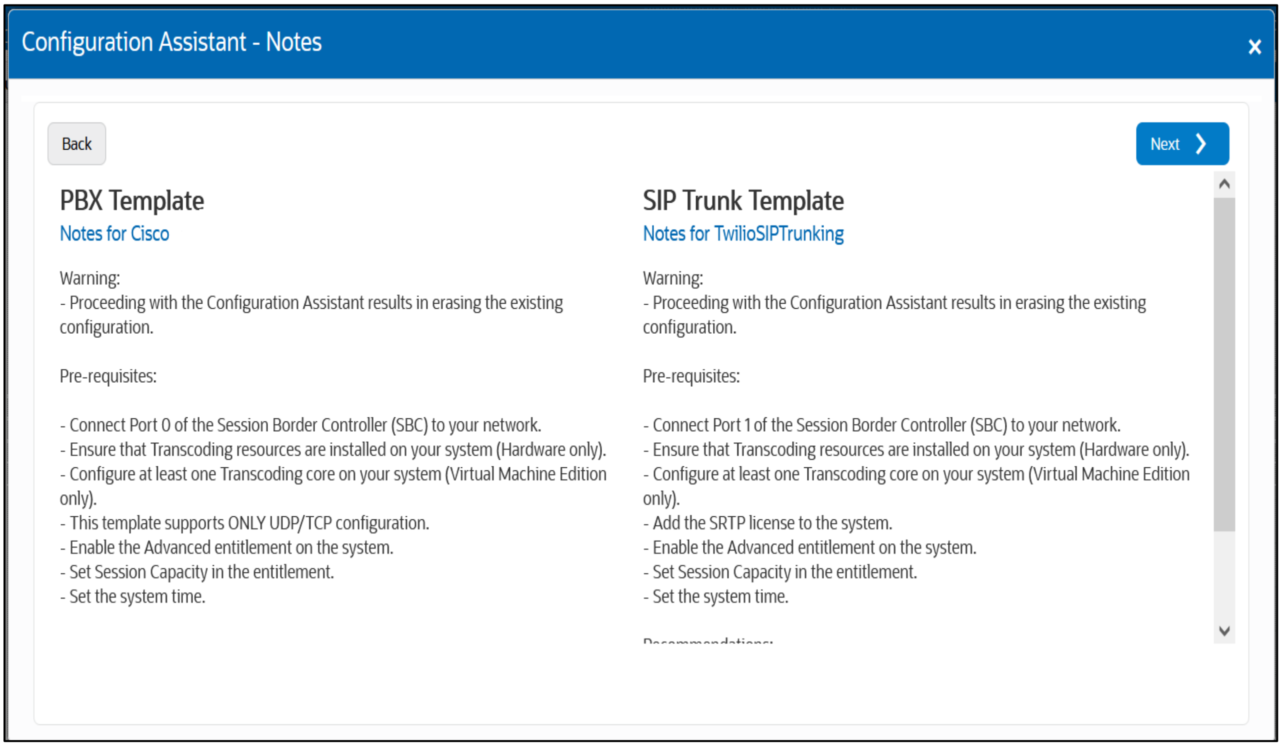
Upload a Template Package

Drag and Drop

Select a file or drop one here. +

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

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



PBX Template

Notes for Cisco

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

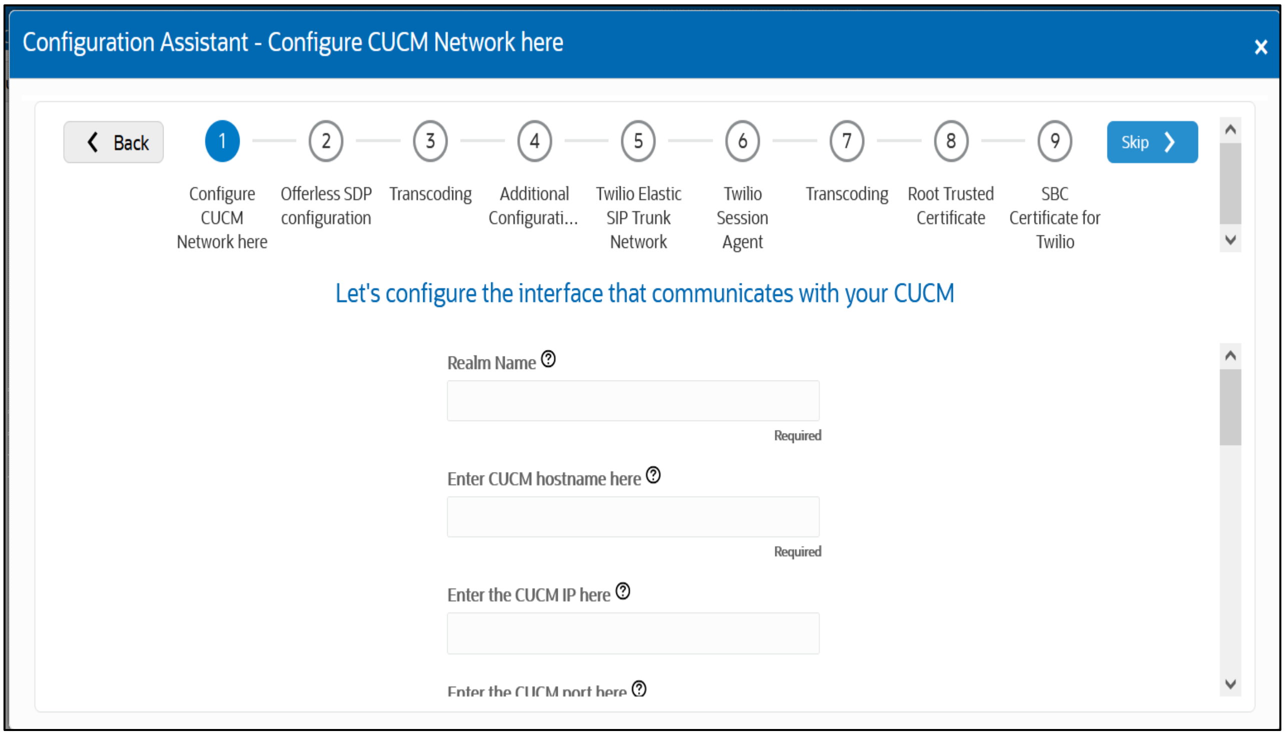
Warning:
- Proceeding with the Configuration Assistant results in erasing the existing configuration.

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 - Configure CUCM Network here
×
❮ Back
1 Configure CUCM Network here
2 Offerless SDP configuration
3 Transcoding
4 Additional Configurati...
5 Twilio Elastic SIP Trunk Network
6 Twilio Session Agent
7 Transcoding
8 Root Trusted Certificate
9 SBC Certificate for Twilio
Skip ❯

Let's configure the interface that communicates with your CUCM

Realm Name ⓘ

Required

Enter CUCM hostname here ⓘ

Required

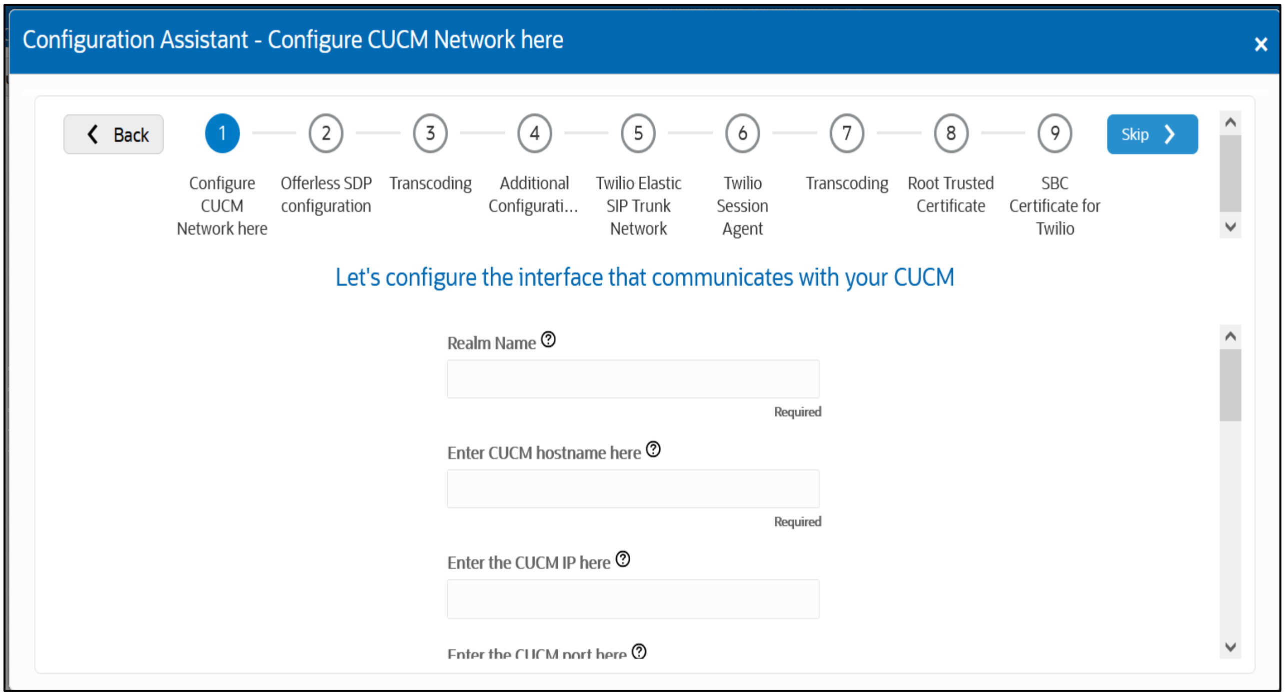
Enter the CUCM IP here ⓘ

Enter the CUCM port here ⓘ

## 8.3. Configuration Assistant Template Navigation

### 8.3.1. Page 1-Cisco Call Manager (CUCM) Network

Page 1 of the template is where you will configure the network information to connect Cisco Call Manager. On this page, we will enter the CUCM hostname, IP and port which will be the next hop IP address/hostname for sip signaling to and from your CUCM



Configuration Assistant - Configure CUCM Network here

×
Back
1 Configure CUCM Network here
2 Offerless SDP configuration
3 Transcoding
4 Additional Configurati...
5 Twilio Elastic SIP Trunk Network
6 Twilio Session Agent
7 Transcoding
8 Root Trusted Certificate
9 SBC Certificate for Twilio
Skip

Let's configure the interface that communicates with your CUCM

Realm Name ⓘ

Required

Enter CUCM hostname here ⓘ

Required

Enter the CUCM IP here ⓘ

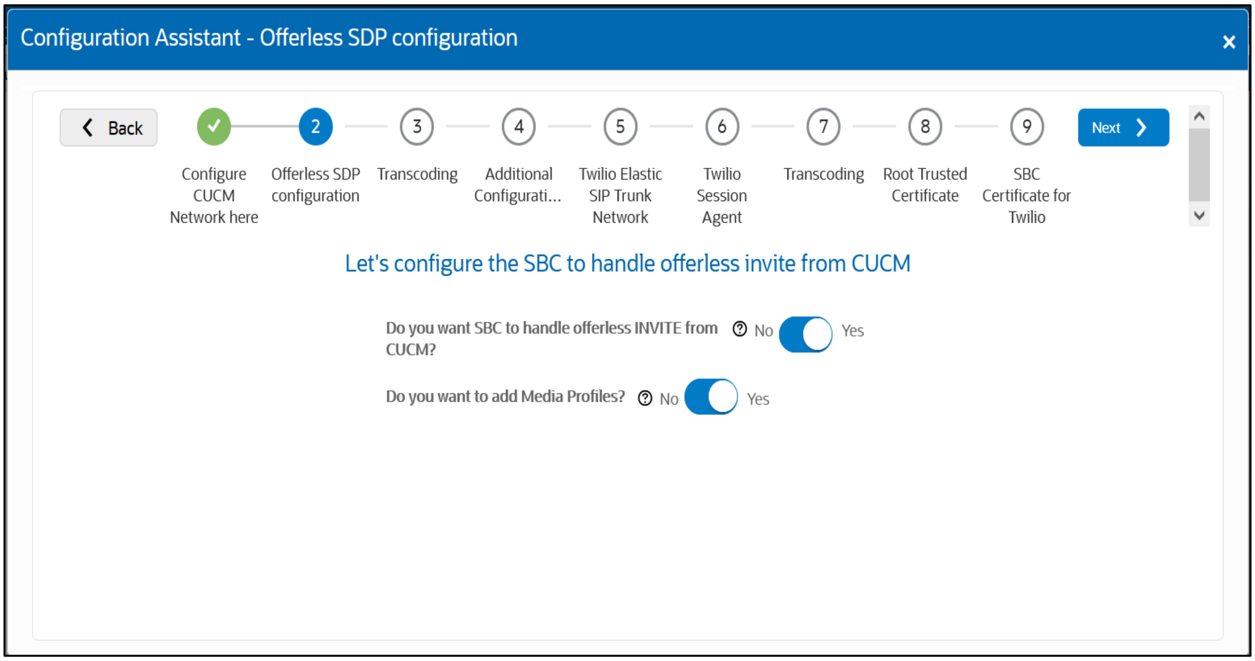
Enter the CUCM port here ⓘ

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-Offerless SDP Invite

Page 2 of the template is where you will configure the information related to Cisco’s offer less SDP Invite configuration. You can enable or disable the configuration through the Yes/No Radio Button.

Note Click on the ? icon to know more about the configuration parameters and their usage.


Configuration Assistant - Offerless SDP configuration
×
Back
Configure CUCM Network here
2
Offerless SDP configuration
3
Transcoding
4
Additional Configurati...
5
Twilio Elastic SIP Trunk Network
6
Twilio Session Agent
7
Transcoding
8
Root Trusted Certificate
9
SBC Certificate for Twilio
Next

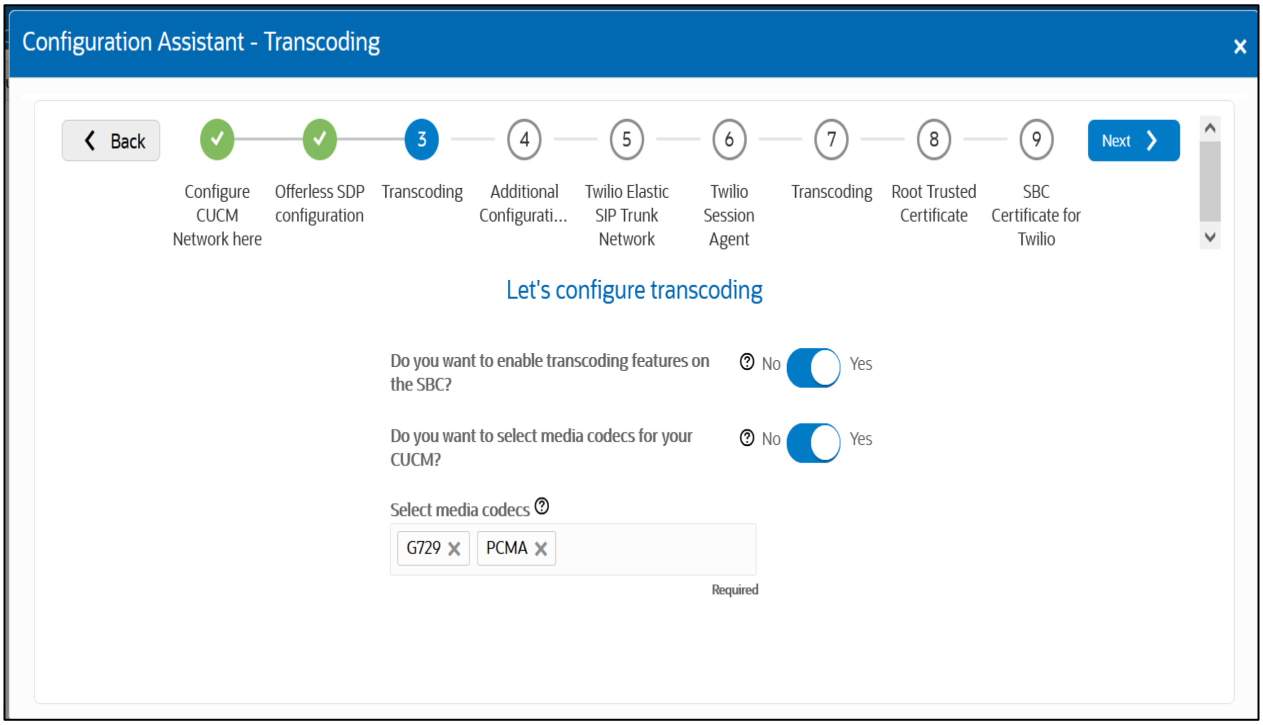
Let's configure the SBC to handle offerless invite from CUCM

Do you want SBC to handle offerless INVITE from CUCM? No ● Yes

Do you want to add Media Profiles? No ● Yes

### 8.3.3. Page 3 - Cisco side Transcoding

Page 3 is where you will be able to configure transcoding between the SBC and Cisco Call 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 Cisco Call Manger. 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
Configure CUCM Network here
Offerless SDP configuration
3
Transcoding
4
Additional Configurati...
5
Twilio Elastic SIP Trunk Network
6
Twilio Session Agent
7
Transcoding
8
Root Trusted Certificate
9
SBC Certificate for Twilio
Next

Let's configure transcoding

Do you want to enable transcoding features on the SBC? No ● Yes

Do you want to select media codecs for your CUCM? No ● Yes

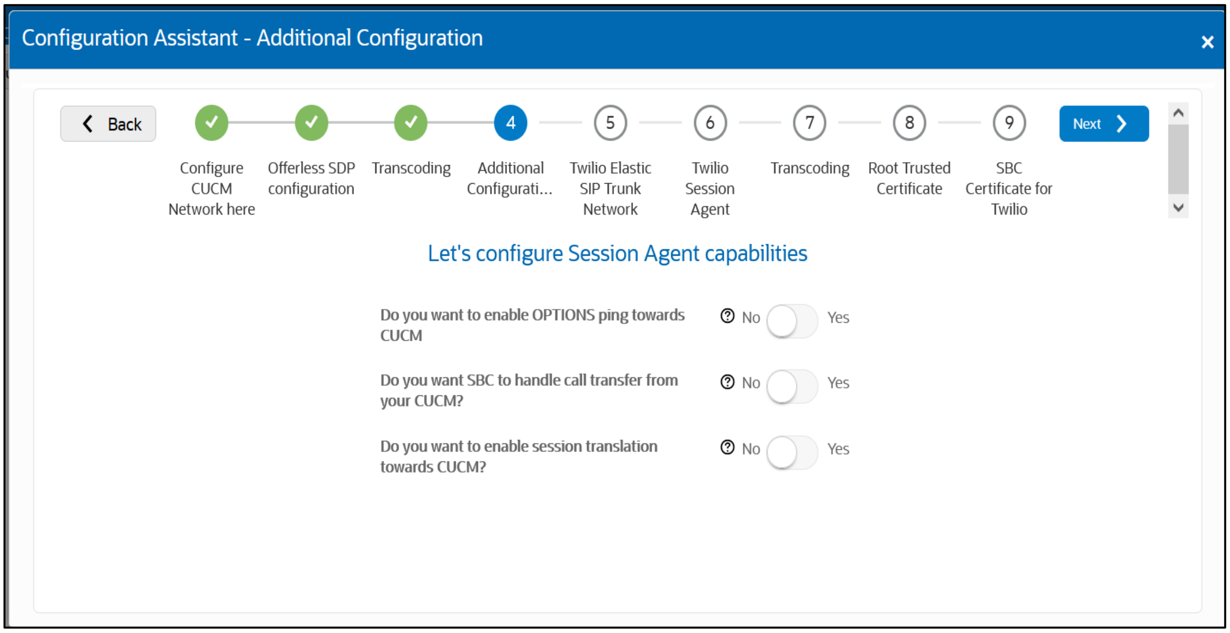
Select media codecs

G729 ✕ PCMA ✕

Required

### 8.3.4. Page 4 - Cisco side Additional Configuration

Page 4 is where you will be able to configure Session Agent Capabilities towards CUCM side. This includes enabling OPTIONS, enabling session translation etc towards CUCM side as shown below. . You can enable or disable the configuration through the Yes/No Radio Button


×
Back
Configure CUCM Network here
Offerless SDP configuration
Transcoding
Additional Configurati...
Twilio Elastic SIP Trunk Network
Twilio Session Agent
Transcoding
Root Trusted Certificate
SBC Certificate for Twilio
Next

Configuration Assistant - Additional Configuration

Let's configure Session Agent capabilities

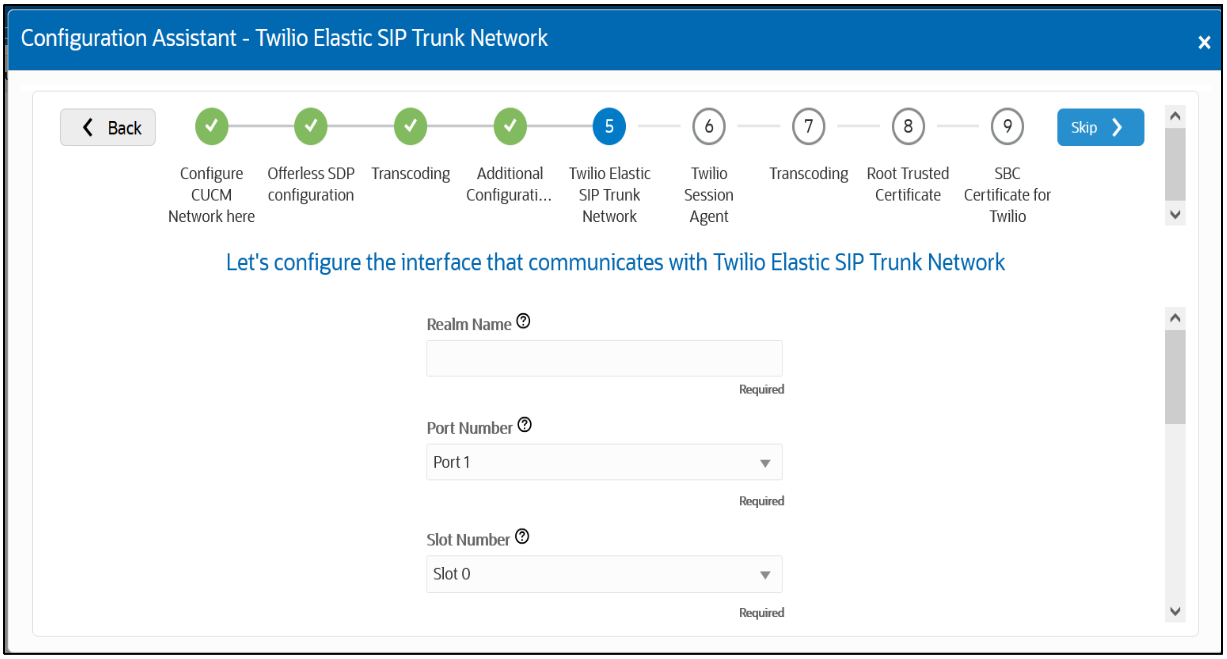
Do you want to enable OPTIONS ping towards CUCM — No ○ Yes

Do you want SBC to handle call transfer from your CUCM? — No ○ Yes

Do you want to enable session translation towards CUCM? — No ○ Yes

### 8.3.5. Page 5 - Twilio Elastic SIP Trunk Network

Page 5 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.


×
Back
Configure CUCM Network here
Offerless SDP configuration
Transcoding
Additional Configurati...
Twilio Elastic SIP Trunk Network
Twilio Session Agent
Transcoding
Root Trusted Certificate
SBC Certificate for Twilio
Skip

Configuration Assistant - Twilio Elastic SIP Trunk Network

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

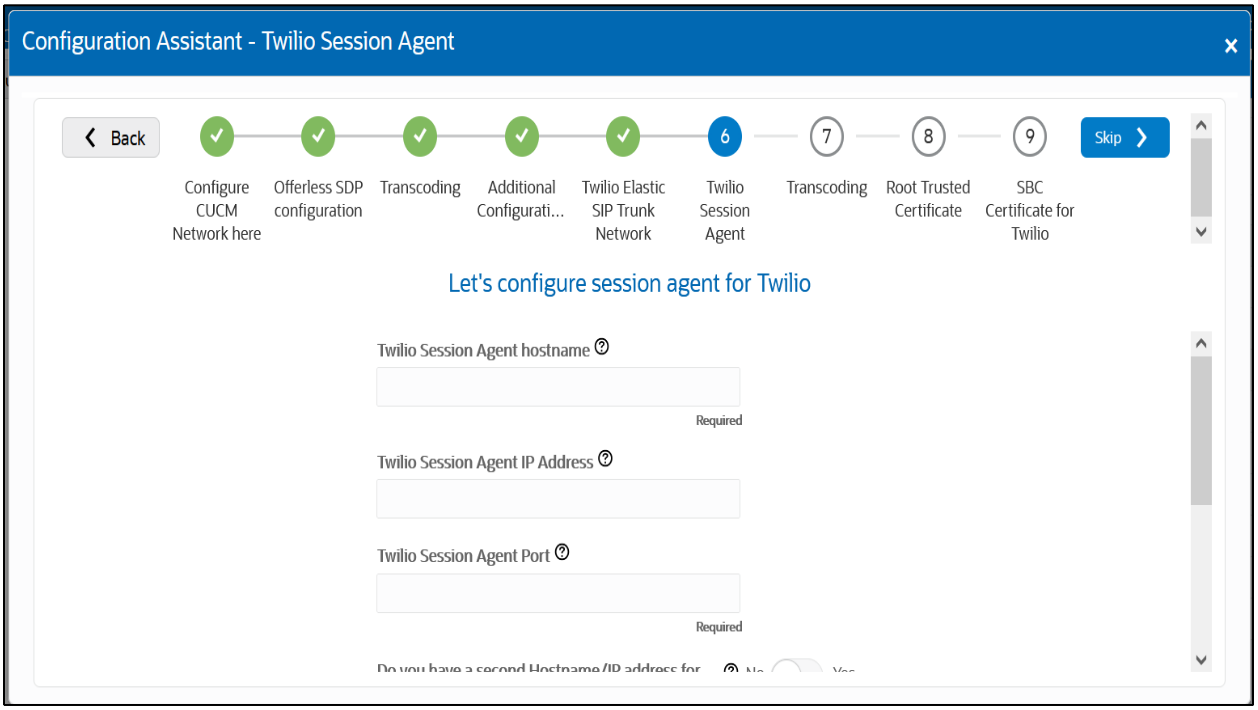
Realm Name: (empty) — Required

Port Number: Port 1 — Required

Slot Number: Slot 0 — Required

#### 8.3.6. Page 6 - Twilio Session Agent

Page 6 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
Configure CUCM Network here
Offerless SDP configuration
Transcoding
Additional Configurati...
Twilio Elastic SIP Trunk Network
6
Twilio Session Agent
7
Transcoding
8
Root Trusted Certificate
9
SBC Certificate for Twilio
Skip

Let's configure session agent for Twilio

Twilio Session Agent hostname
Required

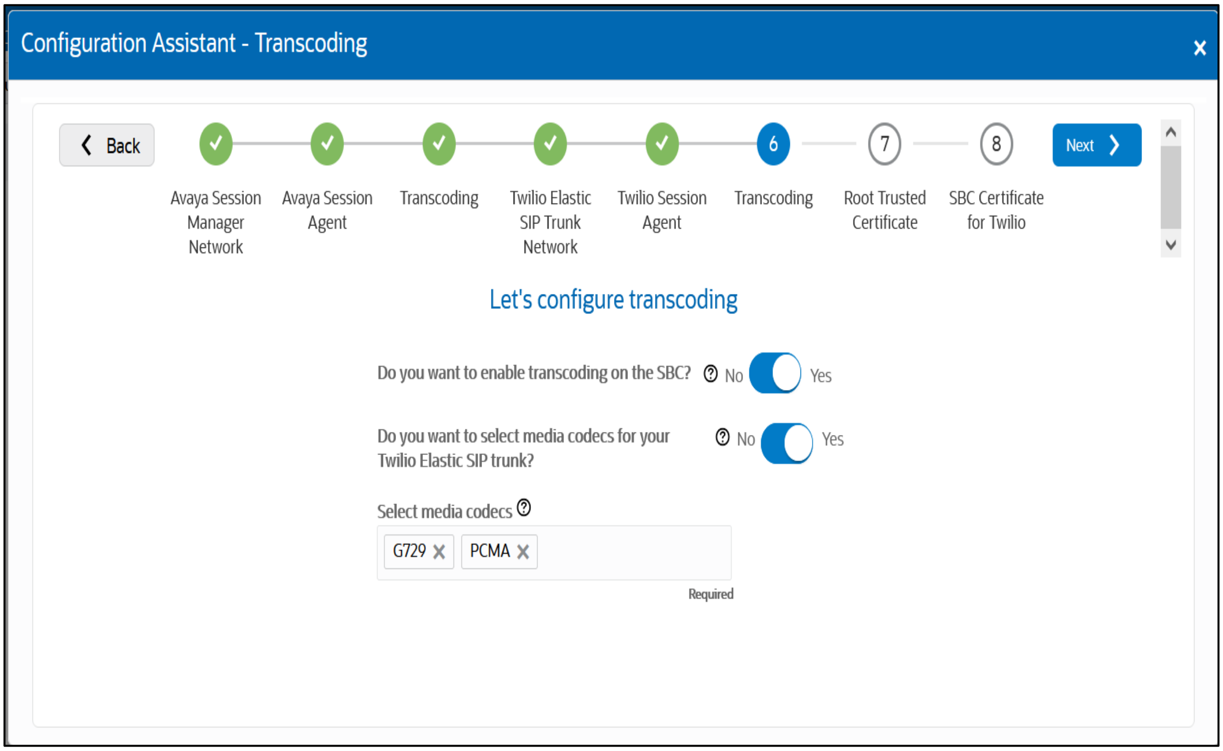
Twilio Session Agent IP Address

Twilio Session Agent Port
Required

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

#### 8.3.7. Page 7 - Twilio side Transcoding

Page 7 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]

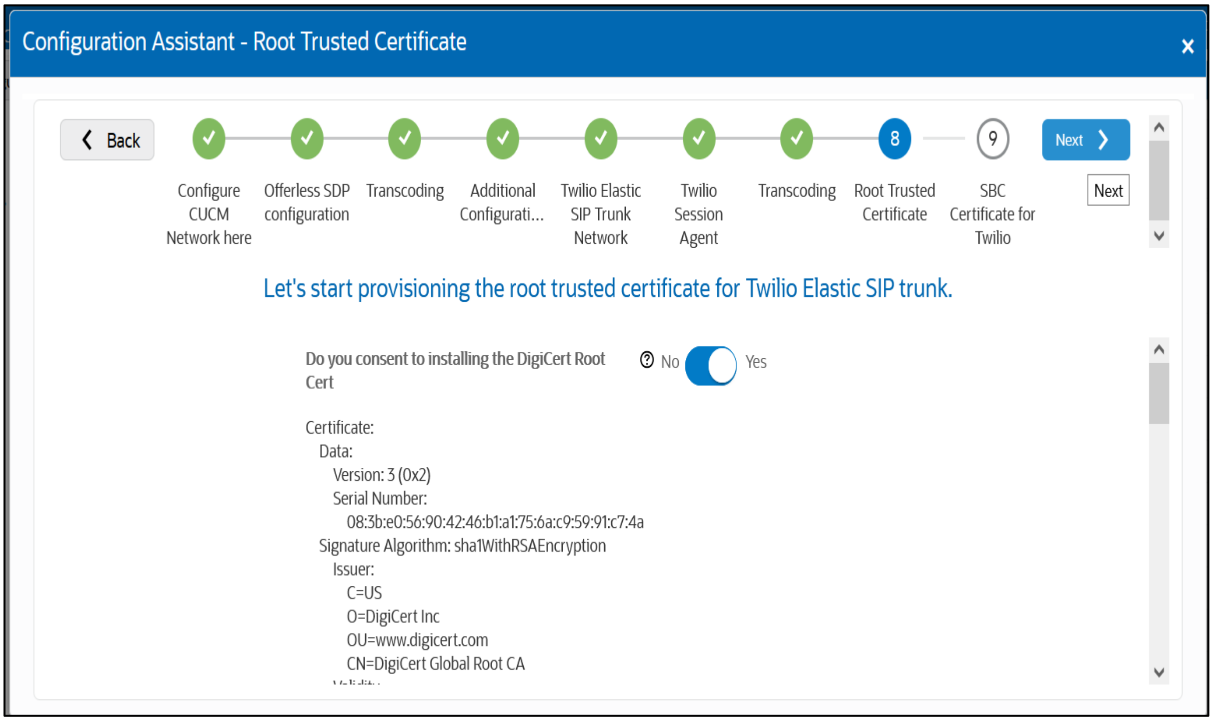
Do you want to select media codecs for your Twilio Elastic SIP trunk? No [✓ Yes]

Select media codecs: G729 ✕ PCMA ✕

Required

### 8.3.8. Page 8 - Import Digi Cert Root CA Certificate for Twilio Side

Page 8 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
Configure CUCM Network here
Offerless SDP configuration
Transcoding
Additional Configurati...
Twilio Elastic SIP Trunk Network
Twilio Session Agent
Transcoding
8
Root Trusted Certificate
9
SBC Certificate for Twilio
Next
Next

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

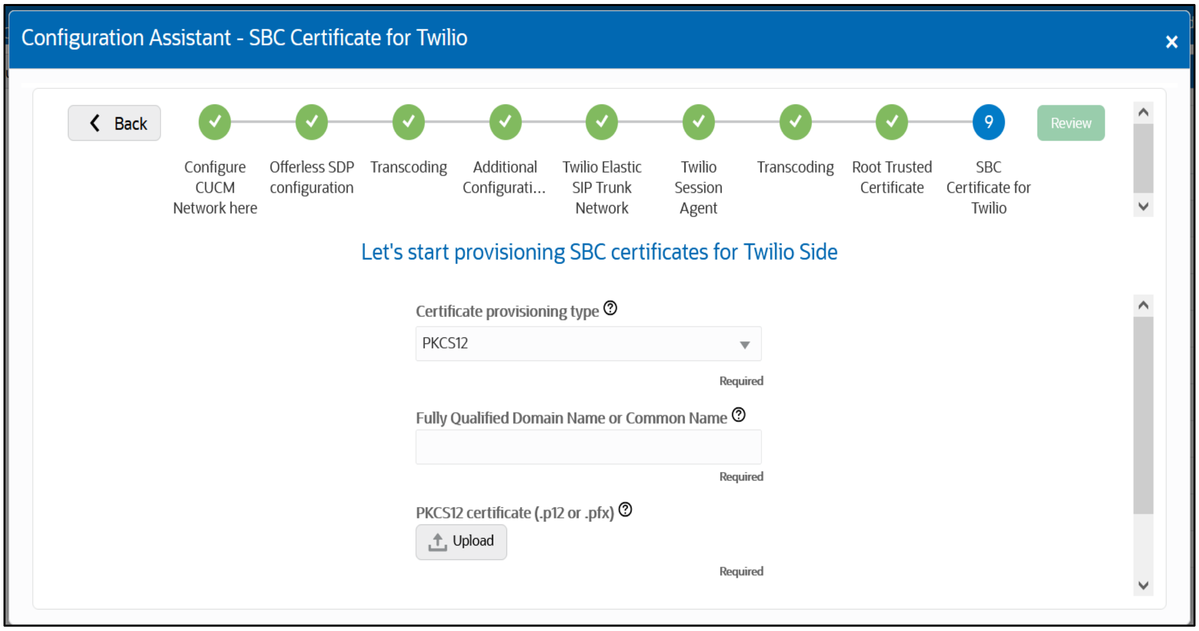
Do you consent to installing the DigiCert Root Cert No [✓ Yes]

```
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
```

### 8.3.9. Page 9 - 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
Configure CUCM Network here
Offerless SDP configuration
Transcoding
Additional Configurati...
Twilio Elastic SIP Trunk Network
Twilio Session Agent
Transcoding
Root Trusted Certificate
9
SBC Certificate for Twilio
Review

Let's start provisioning SBC certificates for Twilio Side

Certificate provisioning type: PKCS12 (Required)

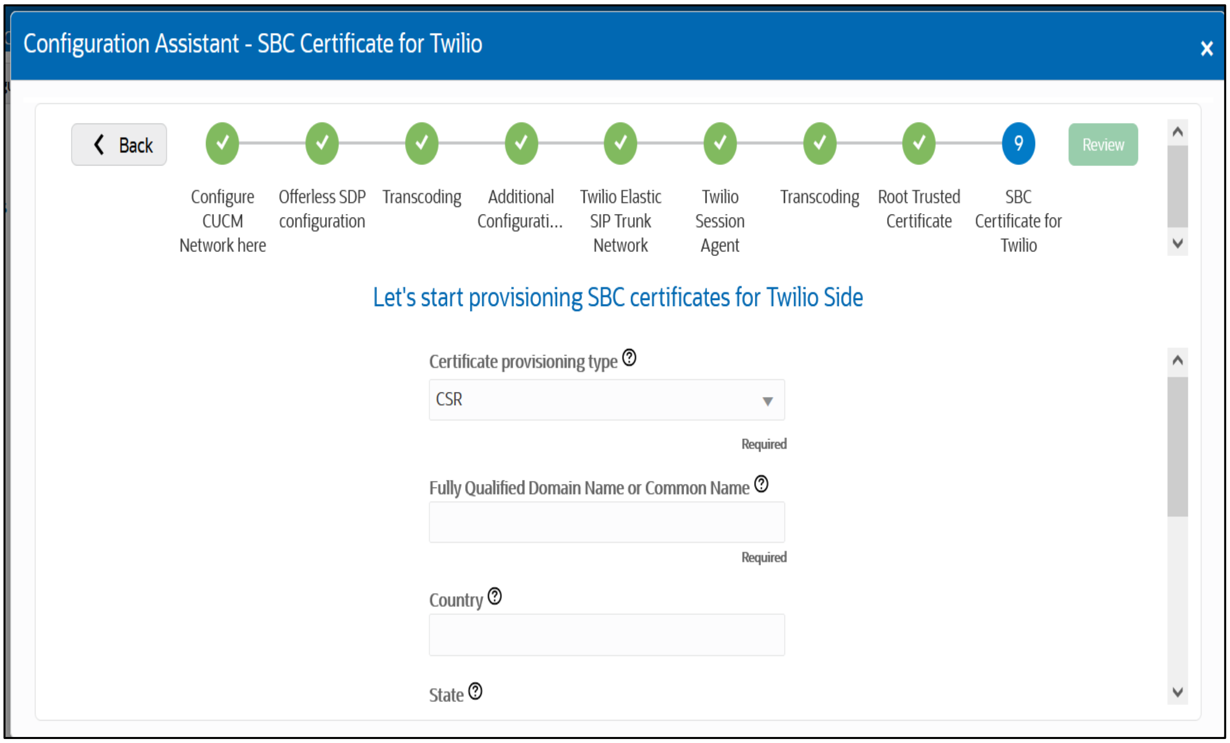
Fully Qualified Domain Name or Common Name (Required)

PKCS12 certificate (.p12 or .pfx) (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)

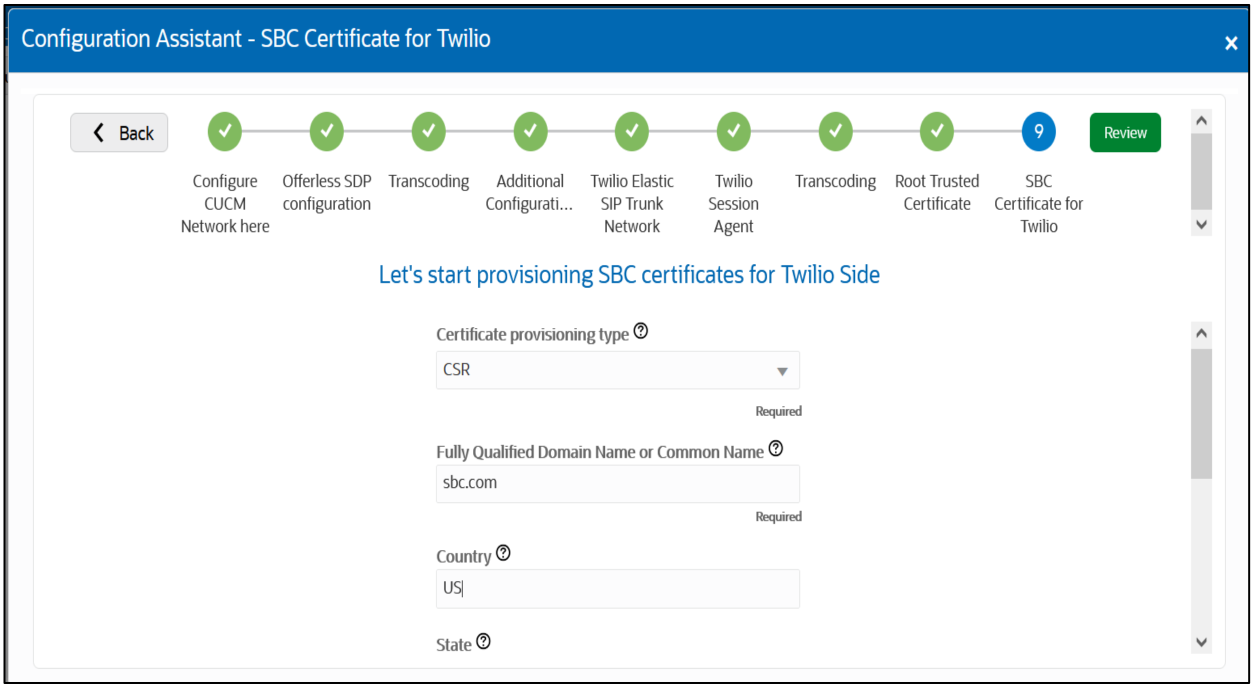
Country:

State

×
Back
Configure CUCM Network here
Offerless SDP configuration
Transcoding
Additional Configurati...
Twilio Elastic SIP Trunk Network
Twilio Session Agent
Transcoding
Root Trusted Certificate
9
SBC Certificate for Twilio
Review

## 8.4. Review

At the end of the template, you will notice in the top right, a "*Review*" tab.  If all 9 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

Let's start provisioning SBC certificates for Twilio Side

Certificate provisioning type: CSR (Required)

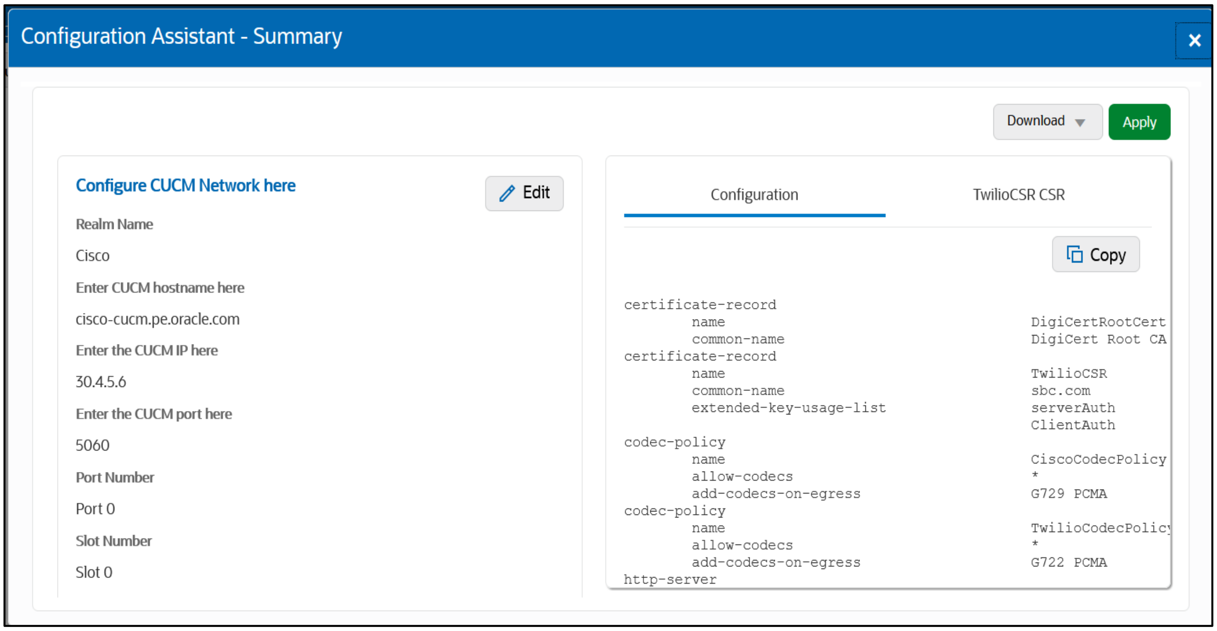
Fully Qualified Domain Name or Common Name: sbc.com (Required)

Country: US

State

×
Back
Configure CUCM Network here
Offerless SDP configuration
Transcoding
Additional Configurati...
Twilio Elastic SIP Trunk Network
Twilio Session Agent
Transcoding
Root Trusted Certificate
9
SBC Certificate for Twilio
Review

The screen looks like below after clicking the Review Tab.



Configure CUCM Network here

Realm Name

Cisco

Enter CUCM hostname here

cisco-cucm.pe.oracle.com

Enter the CUCM IP here

30.4.5.6

Enter the CUCM port here

5060

Port Number

Port 0

Slot Number

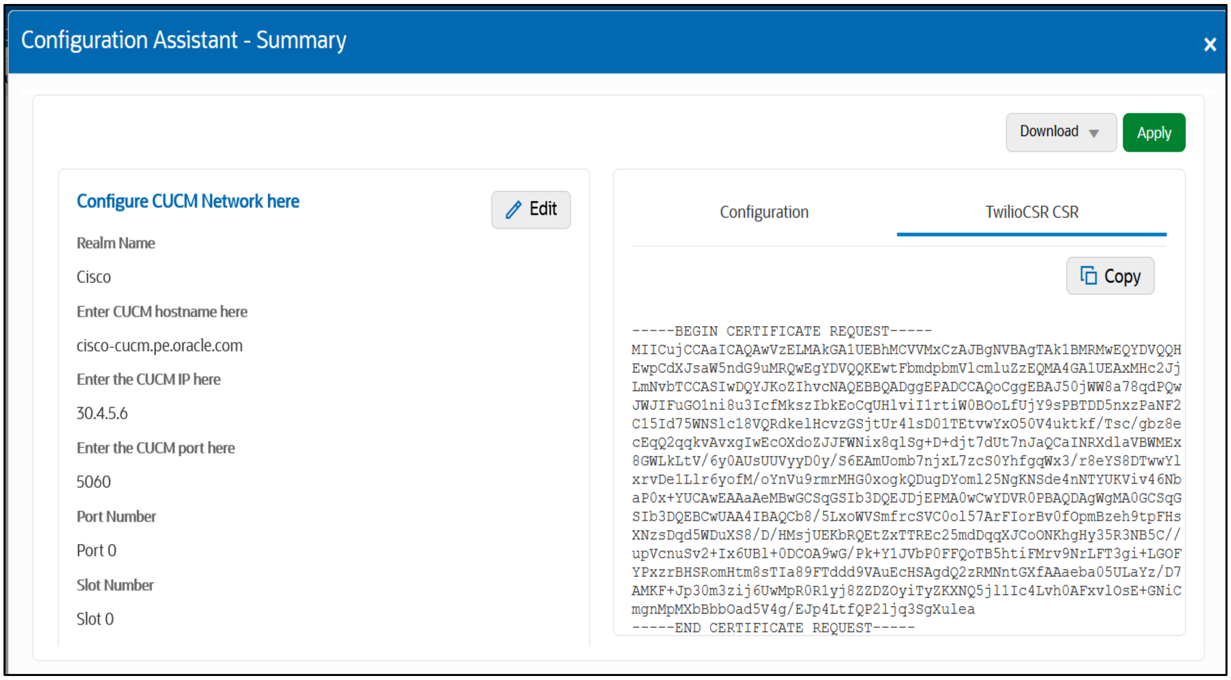
Slot 0

```
certificate-record
        name                                                DigiCertRootCert
        common-name                                         DigiCert Root CA
certificate-record
        name                                                TwilioCSR
        common-name                                         sbc.com
        extended-key-usage-list                             serverAuth
                                                            ClientAuth
codec-policy
        name                                                CiscoCodecPolicy
        allow-codecs                                        *
        add-codecs-on-egress                                G729 PCMA
codec-policy
        name                                                TwilioCodecPolicy
        allow-codecs                                        *
        add-codecs-on-egress                                G722 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 9 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.



Configure CUCM Network here

Realm Name

Cisco

Enter CUCM hostname here

cisco-cucm.pe.oracle.com

Enter the CUCM IP here

30.4.5.6

Enter the CUCM port here

5060

Port Number

Port 0

Slot Number

Slot 0

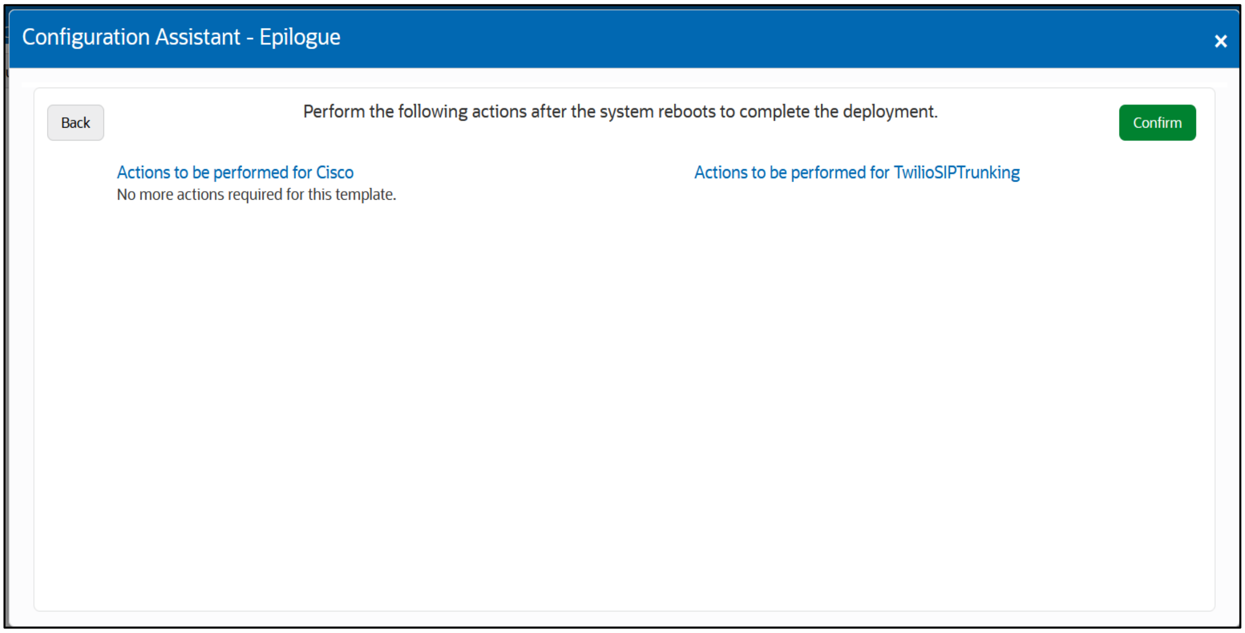
```
-----BEGIN CERTIFICATE REQUEST-----
MIICujCCAaICAQAwVzELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEQMA4GA1UEAxMHc2Jj
LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ50jWW8a78qdPQw
JWJIFuGO1ni8u3IcfMkszIbkEoCqUHlviI1rtiW0BOoLfUjY9sPBTDD5nxzPaNF2
C15Id75WNSlc18VQRdkelHcvzGSjtUr4lsD01TEtvwYxO50V4uktkf/Tsc/gbz8e
cEqQ2qqkvAvxgIwEcOXdoZJJFWNix8qlSg+D+djt7dUt7nJaQCaINRXdlaVBWMEx
8GWLkLtV/6y0AUsUUVyyD0y/S6EAmUomb7njxL7zcS0YhfgqWx3/r8eYS8DTwwYl
xrvDe1Llr6yofM/oYnVu9rmrMHG0xogkQDugDYoml25NgKNSde4nNTYUKViv46Nb
aP0x+YUCAwEAAaAeMBwGCSqGSIb3DQEJDjEPMA0wCwYDVR0PBAQDAgWgMA0GCSqG
SIb3DQEBCwUAA4IBAQCb8/5LxoWVSmfrcSVC0ol57ArFIorBv0fOpmBzeh9tpFHs
XNzsDqd5WDuXS8/D/HMsjUEKbRQEtZxTTREc25mdDqqXJCoONKhgHy35R3NB5C//
upVcnuSv2+Ix6UBl+0DCOA9wG/Pk+Y1JVbP0FFQoTB5htiFMrv9NrLFT3gi+LGOF
YPxzrBHSRomHtm8sTIa89FTddd9VAuEcHSAgdQ2zRMNntGXfAAaeba05ULaYz/D7
AMKF+Jp30m3zij6UwMpR0R1yj8ZZDZOyiTyZKXNQ5jl1Ic4Lvh0AFxvlOsE+GNiC
mgnMpMXbBbbOad5V4g/EJp4LtfQP2ljq3SgXulea
-----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 9, 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 Cisco

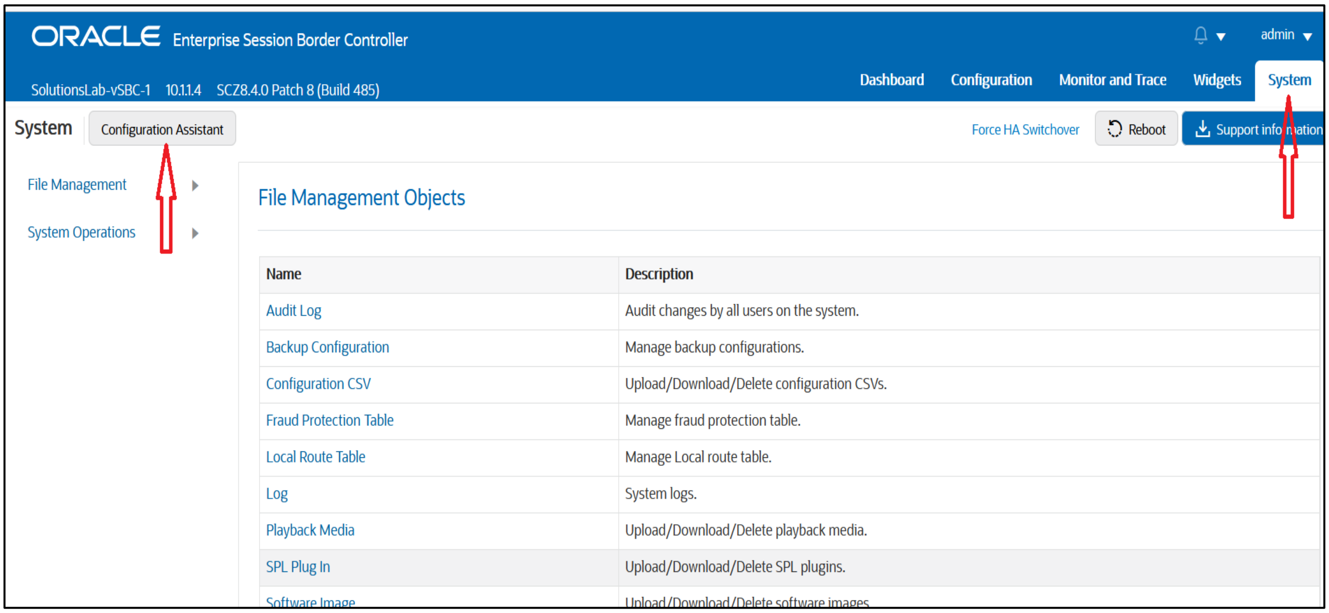
No more actions required for this template.

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 Cisco Call 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

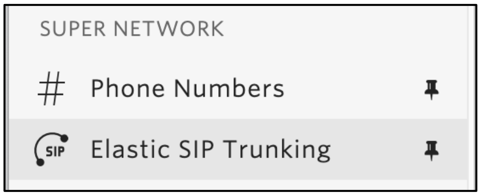
If the SBC being used is an existing SBC with functional configuration, following configuration elements are required:

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

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

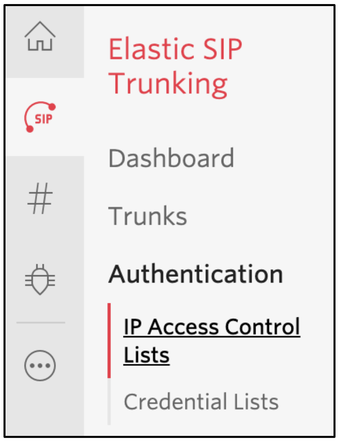
# 10. Twilio Elastic SIP Trunking Configuration

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

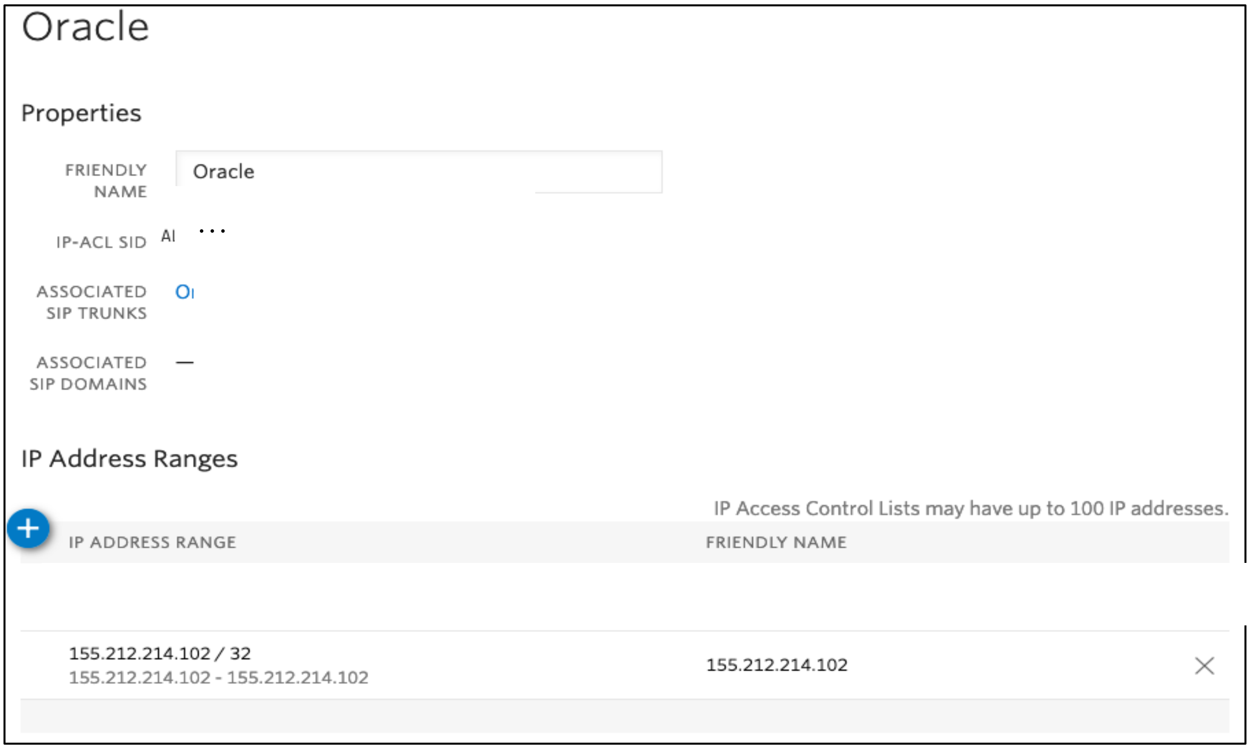


## 10.1. Create an IP-ACL rule

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



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



Oracle

Properties

FRIENDLY NAME: Oracle

IP-ACL SID: AI ...

ASSOCIATED SIP TRUNKS: Oı

ASSOCIATED SIP DOMAINS: —

IP Address Ranges

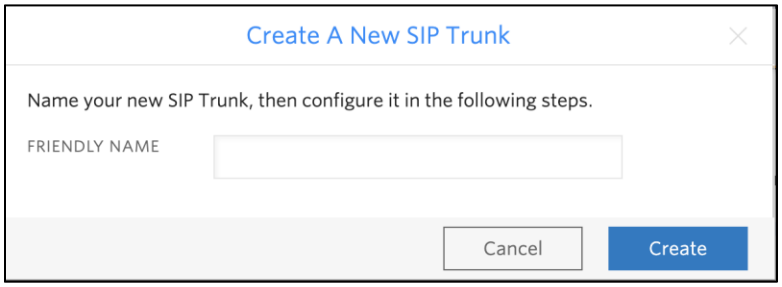
IP Access Control Lists may have up to 100 IP addresses.

| IP ADDRESS RANGE | FRIENDLY NAME |
|---|---|
| 155.212.214.102 / 32<br>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.

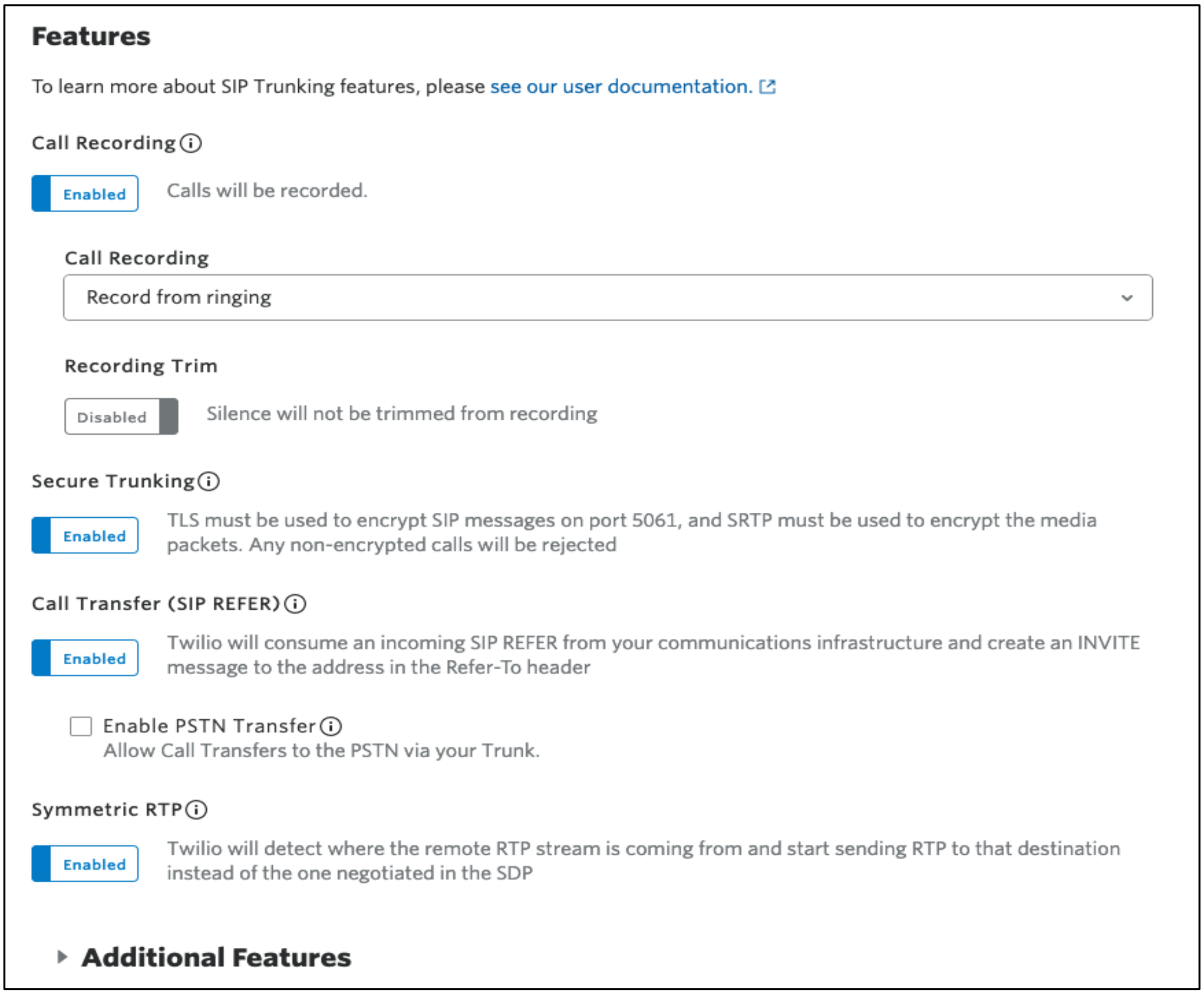


Create A New SIP Trunk

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 ⓘ

Calls will be recorded.

Call Recording

Record from ringing

Recording Trim

Silence will not be trimmed from recording

Secure Trunking ⓘ

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) ⓘ

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

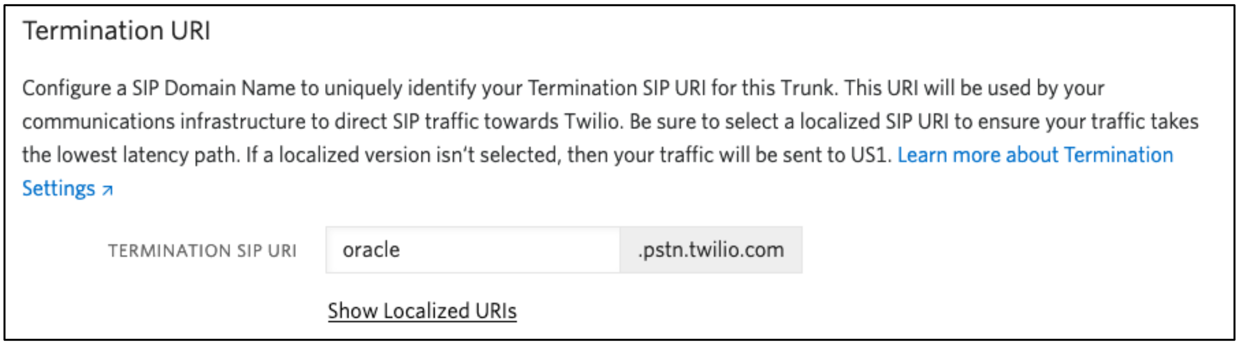
□ Enable PSTN Transfer ⓘ
Allow Call Transfers to the PSTN via your Trunk.

Symmetric RTP ⓘ

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.

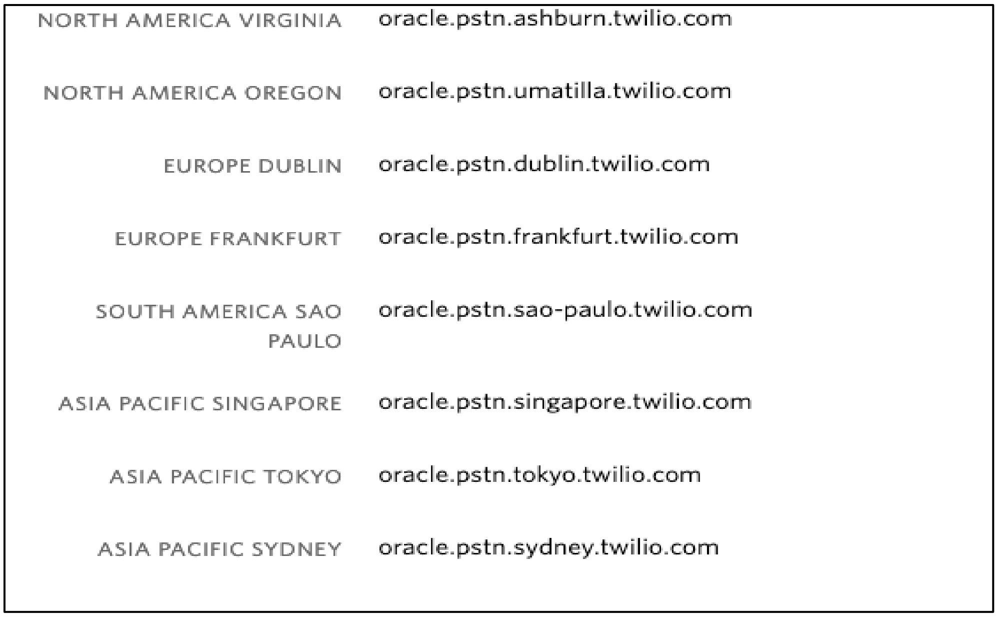


Termination URI

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

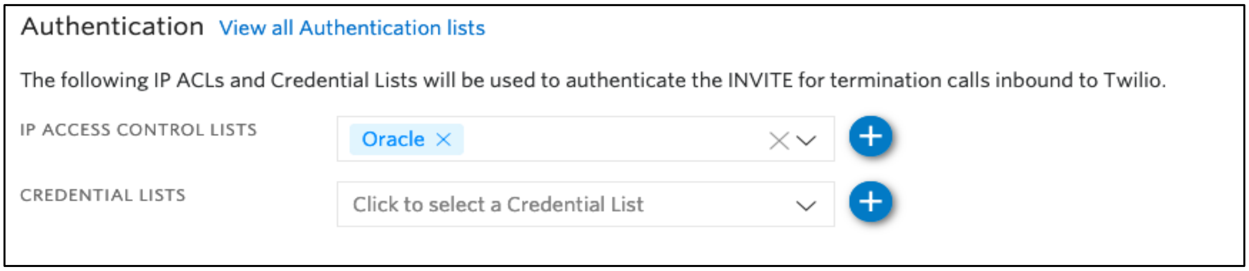
Click on "Show localized URI's" and copy and paste this information as you will use this on your SBC to configure your Trunk.



| | |
|---|---|
| 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

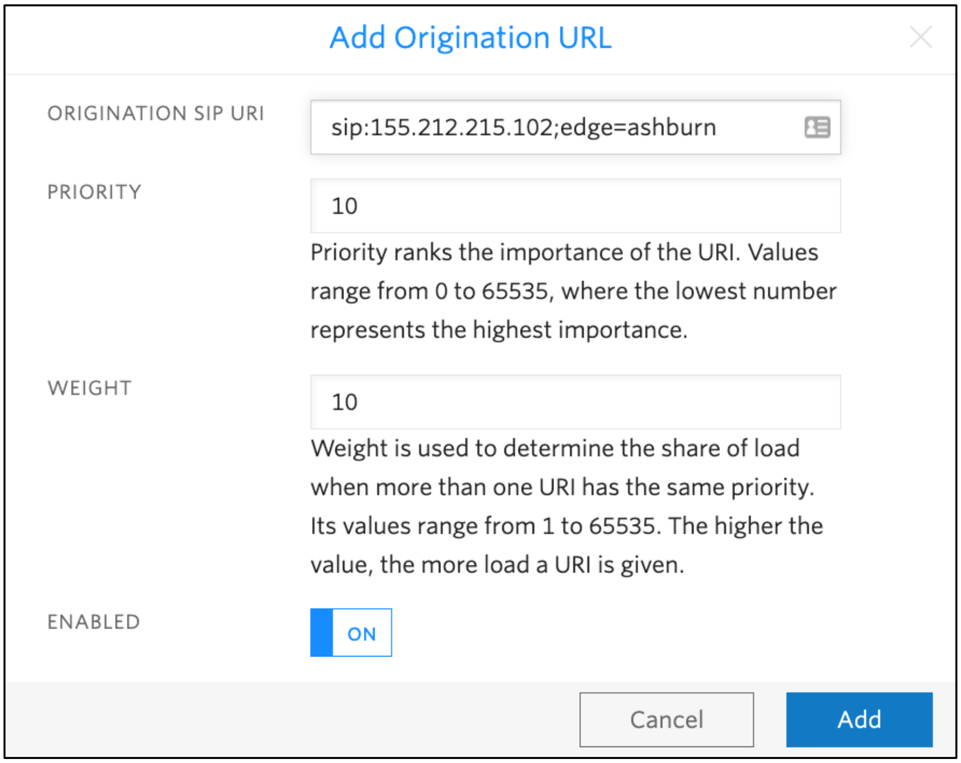
The following IP ACLs and Credential Lists will be used to authenticate the INVITE for termination calls inbound to Twilio.

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

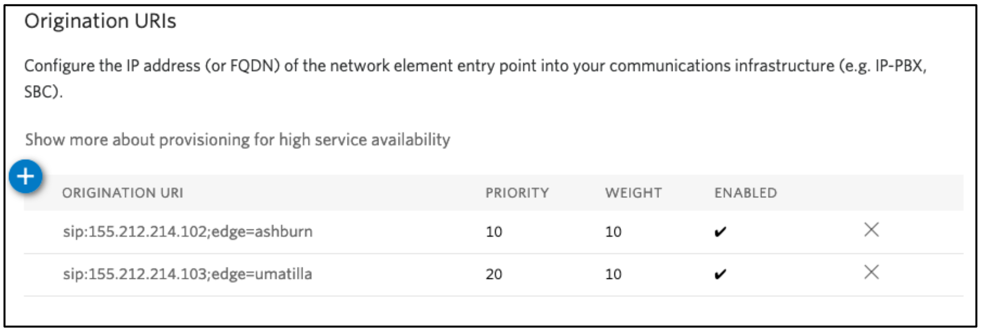
Priority ranks the importance of the URI. Values range from 0 to 65535, where the lowest number represents the highest importance.

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).

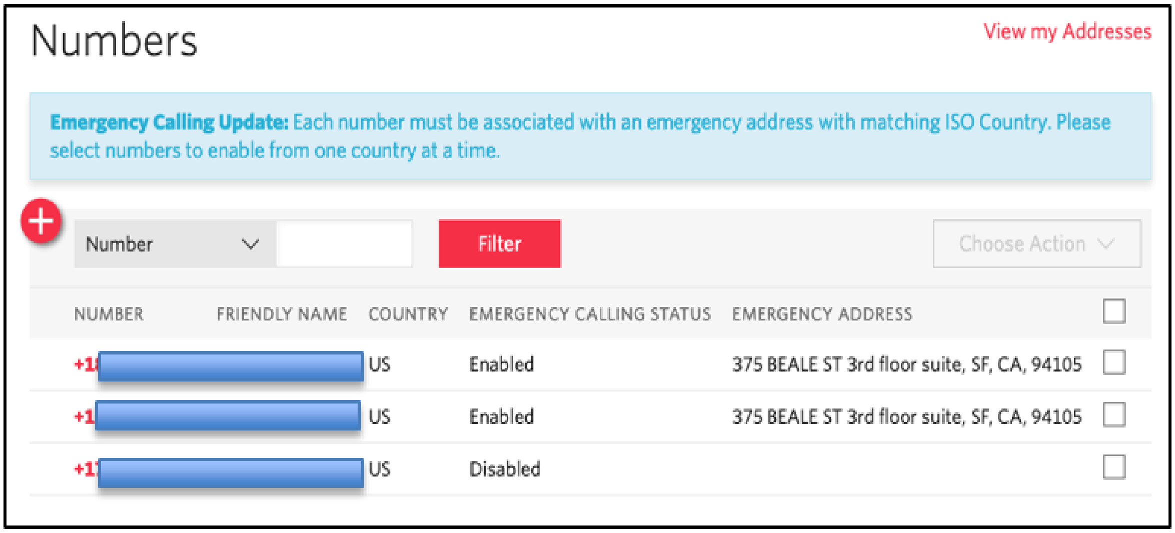
Show more about provisioning for high service availability

| 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

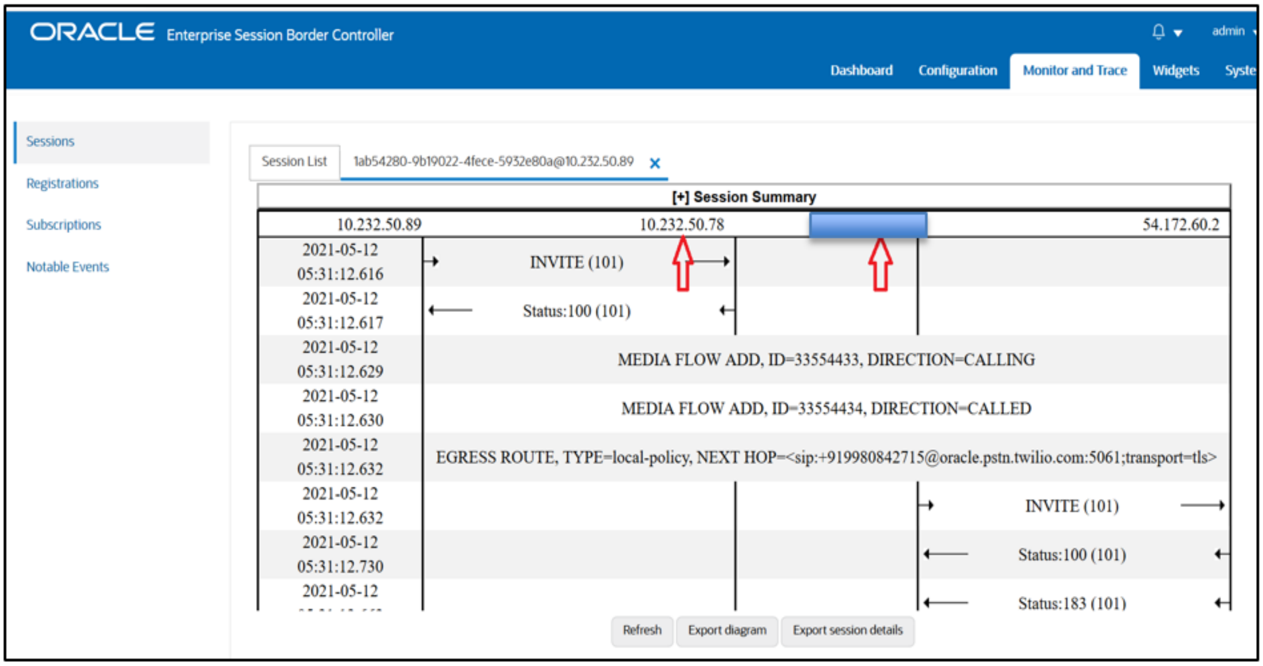
**Emergency Calling Update:** Each number must be associated with an emergency address with matching ISO Country. Please select numbers to enable from one country at a time.

| NUMBER | FRIENDLY NAME | COUNTRY | EMERGENCY CALLING STATUS | EMERGENCY ADDRESS | ☐ |
|---|---|---|---|---|---|
| +1[redacted] | [redacted] | US | Enabled | 375 BEALE ST 3rd floor suite, SF, CA, 94105 | ☐ |
| +1[redacted] | [redacted] | US | Enabled | 375 BEALE ST 3rd floor suite, SF, CA, 94105 | ☐ |
| +1[redacted] | [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 Cisco Users

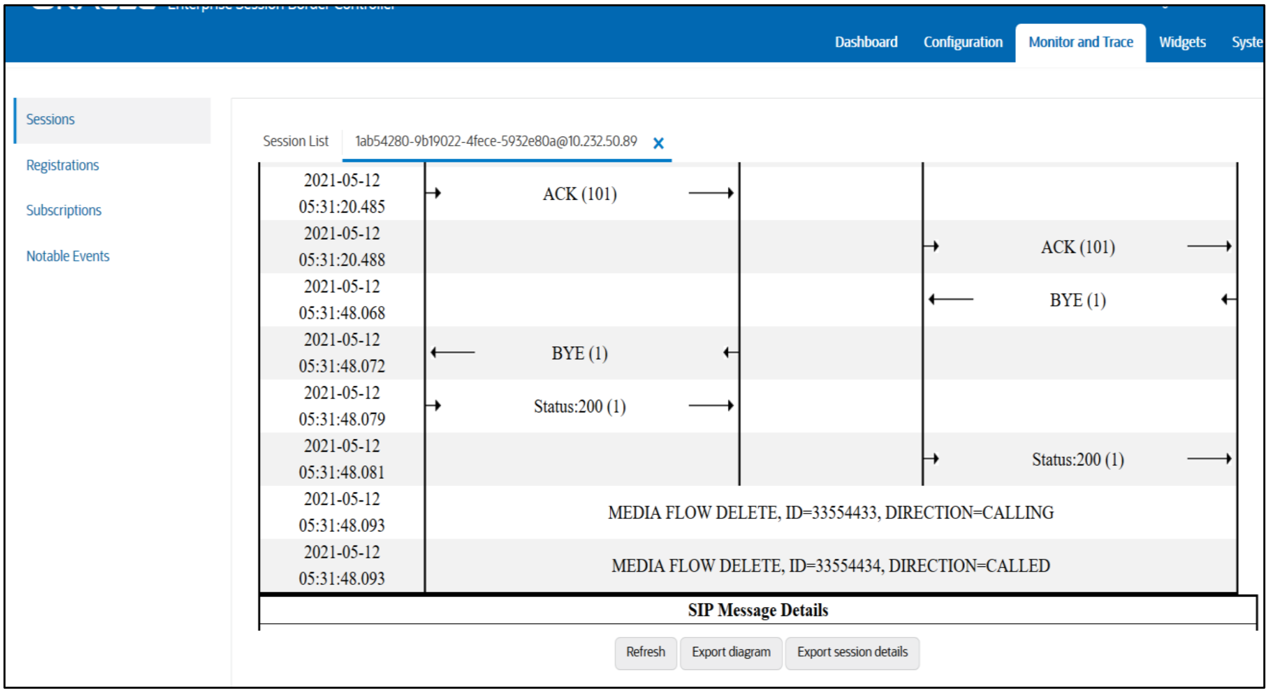
1. Make Call from Cisco user to the Twilio Elastic Sip Trunk and check the call flow. The calls flow from Cisco SIP Interface to Twilio Elastic SIP Trunking Interface and to Twilio Session Agent and the call reaches the PSTN user after that.



[+] Session Summary

10.232.50.89 | 10.232.50.78 | 54.172.60.2

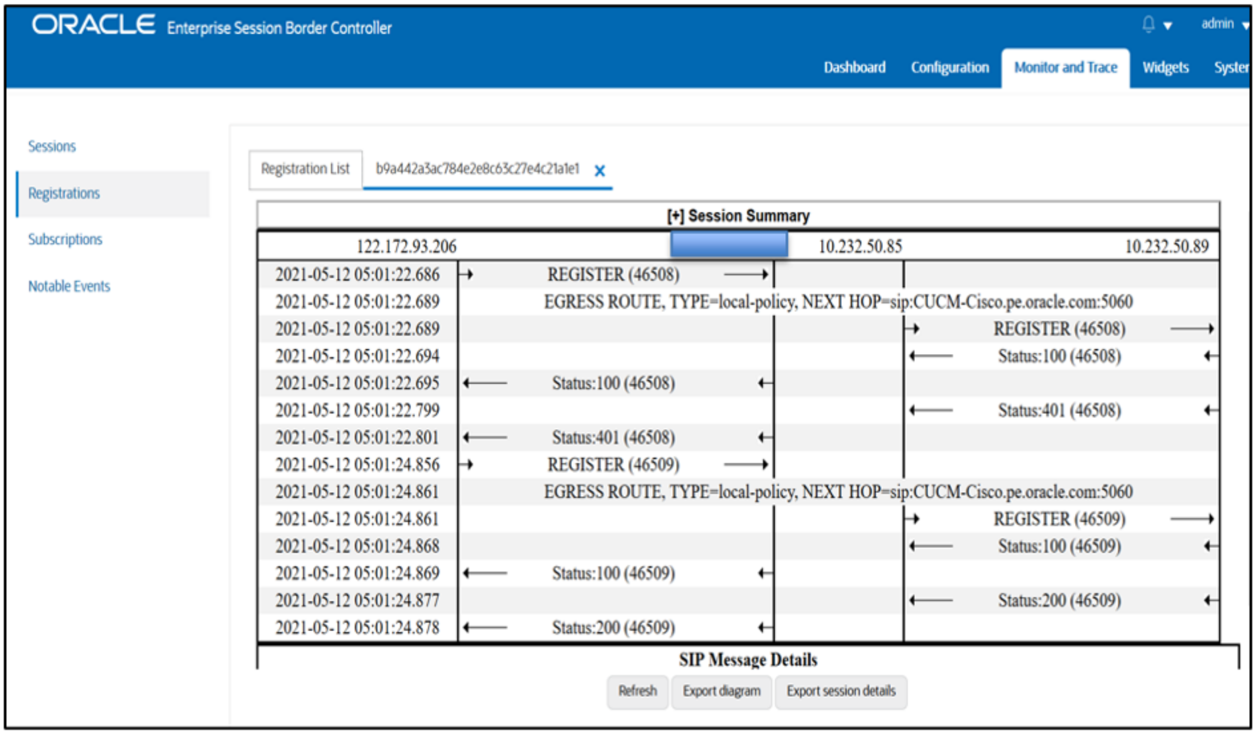
2021-05-12 05:31:12.616 INVITE (101) →
2021-05-12 05:31:12.617 ← Status:100 (101)
2021-05-12 05:31:12.629 MEDIA FLOW ADD, ID=33554433, DIRECTION=CALLING
2021-05-12 05:31:12.630 MEDIA FLOW ADD, ID=33554434, DIRECTION=CALLED
2021-05-12 05:31:12.632 EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:+919980842715@oracle.pstn.twilio.com:5061;transport=tls>
2021-05-12 05:31:12.632 INVITE (101) →
2021-05-12 05:31:12.730 ← Status:100 (101)
2021-05-12 ← Status:183 (101)



2021-05-12 05:31:20.485 ACK (101) →
2021-05-12 05:31:20.488 ACK (101) →
2021-05-12 05:31:48.068 ← BYE (1)
2021-05-12 05:31:48.072 ← BYE (1)
2021-05-12 05:31:48.079 Status:200 (1) →
2021-05-12 05:31:48.081 Status:200 (1) →
2021-05-12 05:31:48.093 MEDIA FLOW DELETE, ID=33554433, DIRECTION=CALLING
2021-05-12 05:31:48.093 MEDIA FLOW DELETE, ID=33554434, DIRECTION=CALLED

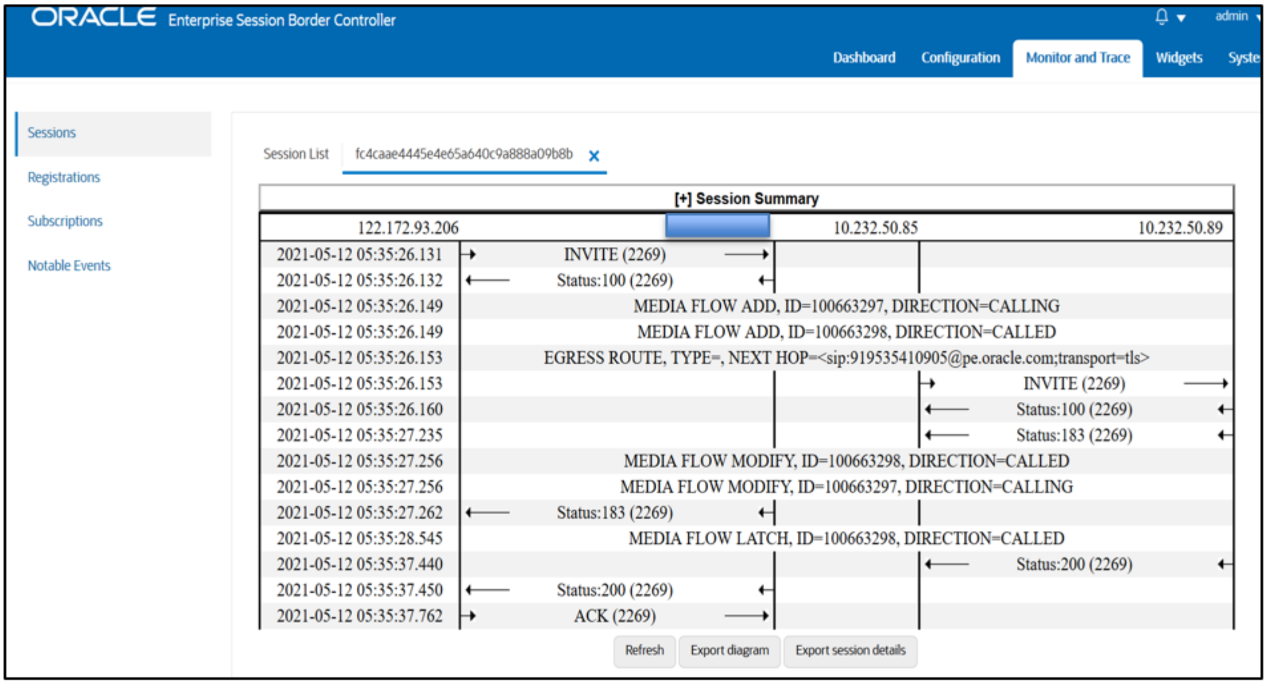
SIP Message Details

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

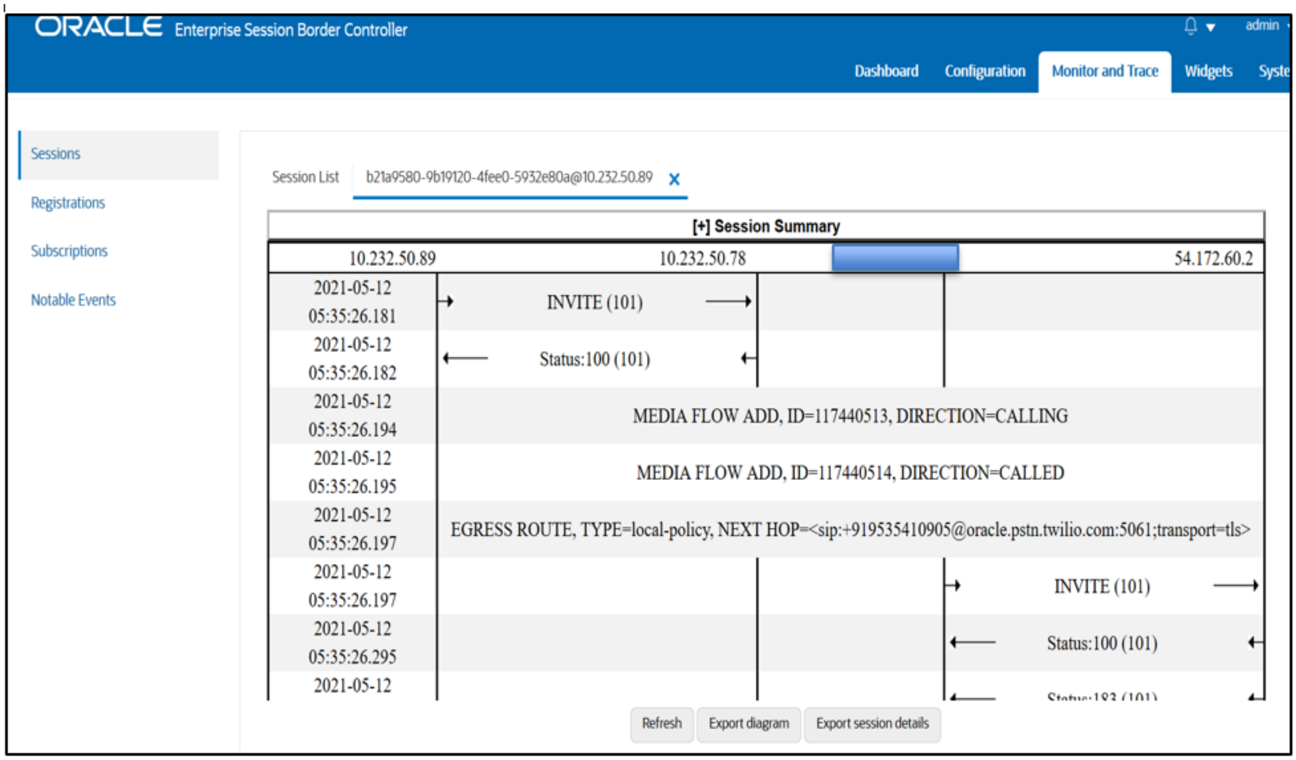


```
                          [+] Session Summary
                  122.172.93.206                10.232.50.85               10.232.50.89
2021-05-12 05:01:22.686 →   REGISTER (46508)     →|
2021-05-12 05:01:22.689     EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:CUCM-Cisco.pe.oracle.com:5060
2021-05-12 05:01:22.689                            |    →   REGISTER (46508)     →
2021-05-12 05:01:22.694                            |    ←   Status:100 (46508)   ←
2021-05-12 05:01:22.695 ←   Status:100 (46508)   ←|
2021-05-12 05:01:22.799                            |    ←   Status:401 (46508)   ←
2021-05-12 05:01:22.801 ←   Status:401 (46508)   ←|
2021-05-12 05:01:24.856 →   REGISTER (46509)     →|
2021-05-12 05:01:24.861     EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:CUCM-Cisco.pe.oracle.com:5060
2021-05-12 05:01:24.861                            |    →   REGISTER (46509)     →
2021-05-12 05:01:24.868                            |    ←   Status:100 (46509)   ←
2021-05-12 05:01:24.869 ←   Status:100 (46509)   ←|
2021-05-12 05:01:24.877                            |    ←   Status:200 (46509)   ←
2021-05-12 05:01:24.878 ←   Status:200 (46509)   ←|
                          SIP Message Details
```

3. Make Call from Cisco 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 Cisco CUCM first and then reaches Twilio trunk user after that as given below.



```
                          [+] Session Summary
                  122.172.93.206                10.232.50.85               10.232.50.89
2021-05-12 05:35:26.131 →   INVITE (2269)        →|
2021-05-12 05:35:26.132 ←   Status:100 (2269)    ←|
2021-05-12 05:35:26.149         MEDIA FLOW ADD, ID=100663297, DIRECTION=CALLING
2021-05-12 05:35:26.149         MEDIA FLOW ADD, ID=100663298, DIRECTION=CALLED
2021-05-12 05:35:26.153     EGRESS ROUTE, TYPE=, NEXT HOP=<sip:919535410905@pe.oracle.com;transport=tls>
2021-05-12 05:35:26.153                            |    →   INVITE (2269)        →
2021-05-12 05:35:26.160                            |    ←   Status:100 (2269)    ←
2021-05-12 05:35:27.235                            |    ←   Status:183 (2269)    ←
2021-05-12 05:35:27.256         MEDIA FLOW MODIFY, ID=100663298, DIRECTION=CALLED
2021-05-12 05:35:27.256         MEDIA FLOW MODIFY, ID=100663297, DIRECTION=CALLING
2021-05-12 05:35:27.262 ←   Status:183 (2269)    ←|
2021-05-12 05:35:28.545         MEDIA FLOW LATCH, ID=100663298, DIRECTION=CALLED
2021-05-12 05:35:37.440                            |    ←   Status:200 (2269)    ←
2021-05-12 05:35:37.450 ←   Status:200 (2269)    ←|
2021-05-12 05:35:37.762 →   ACK (2269)           →|
```

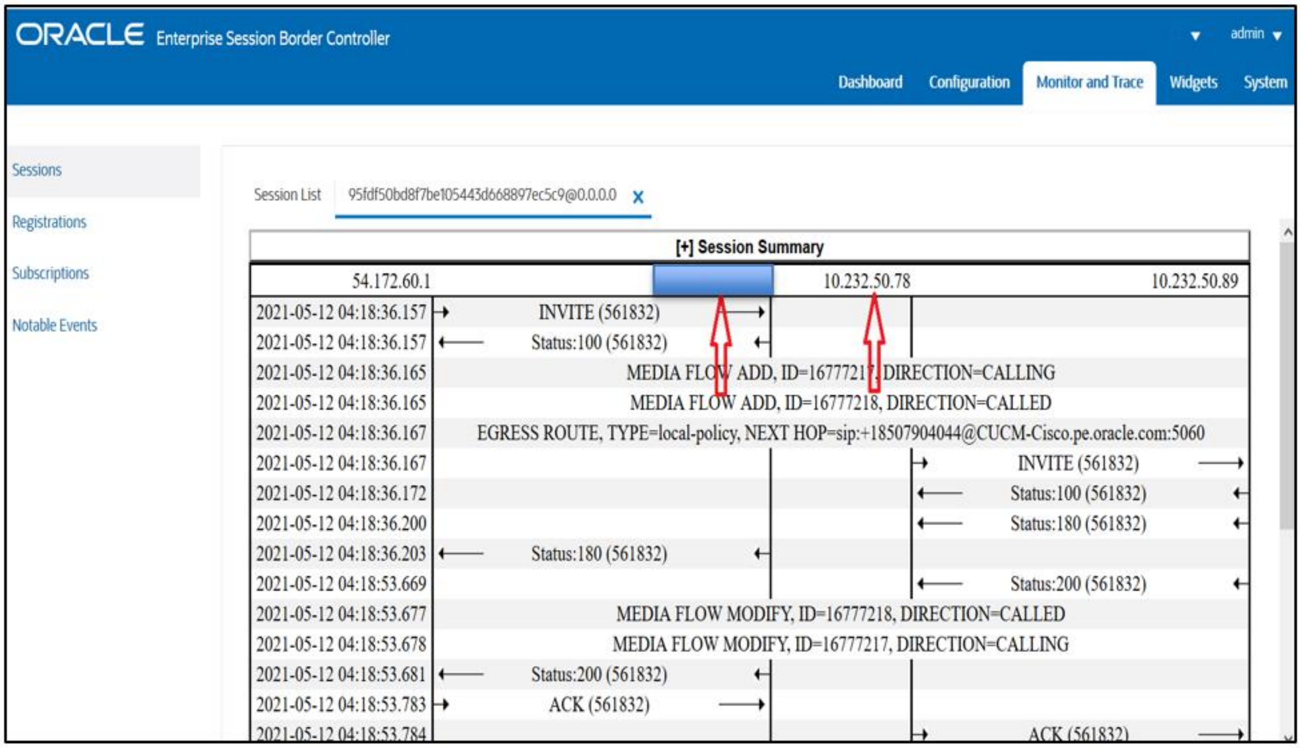


b21a9580-9b19120-4fee0-5932e80a@10.232.50.89

[+] Session Summary

| | 10.232.50.89 | 10.232.50.78 | 54.172.60.2 |
|---|---|---|---|
| 2021-05-12 05:35:26.181 | INVITE (101) → | | |
| 2021-05-12 05:35:26.182 | ← Status:100 (101) | | |
| 2021-05-12 05:35:26.194 | MEDIA FLOW ADD, ID=117440513, DIRECTION=CALLING | | |
| 2021-05-12 05:35:26.195 | MEDIA FLOW ADD, ID=117440514, DIRECTION=CALLED | | |
| 2021-05-12 05:35:26.197 | EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:+919535410905@oracle.pstn.twilio.com:5061;transport=tls> | | |
| 2021-05-12 05:35:26.197 | | | INVITE (101) → |
| 2021-05-12 05:35:26.295 | | | ← Status:100 (101) |
| 2021-05-12 | | | ← Status:183 (101) |

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

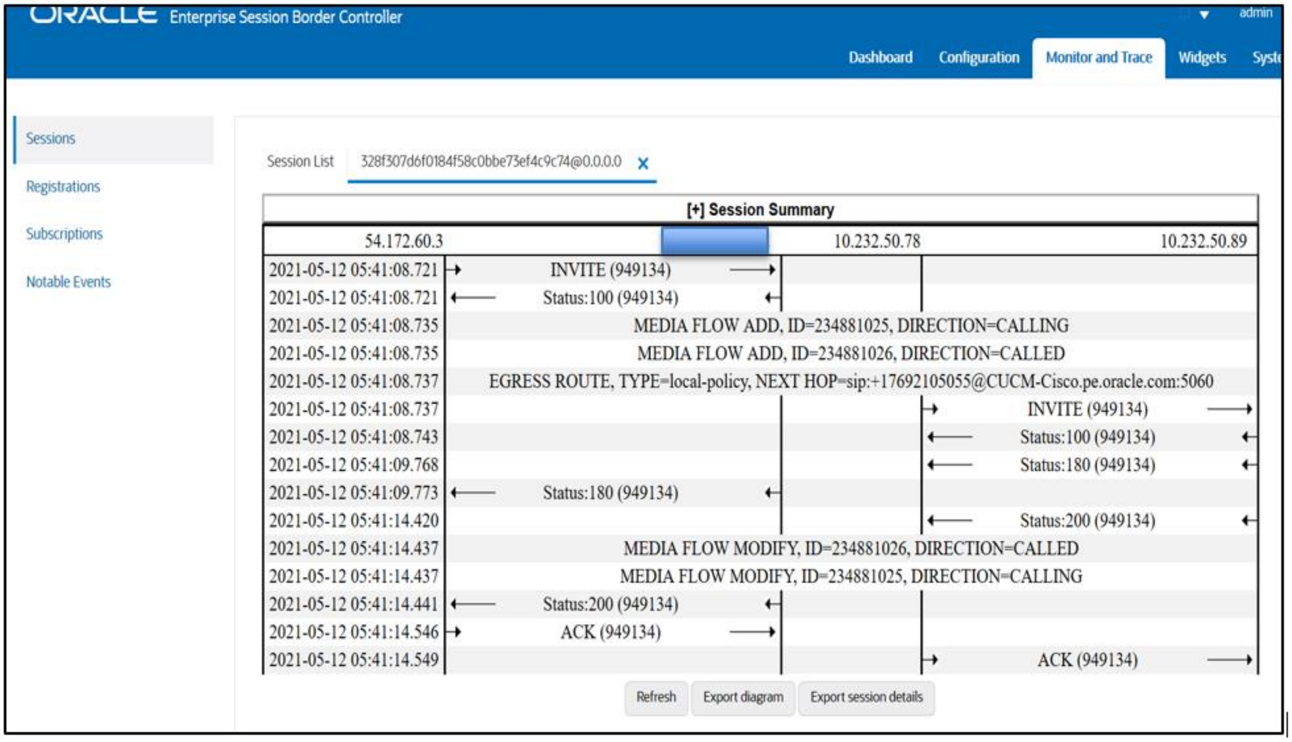


95fdf50bd8f7be105443d668897ec5c9@0.0.0.0

[+] Session Summary

| | 54.172.60.1 | 10.232.50.78 | 10.232.50.89 |
|---|---|---|---|
| 2021-05-12 04:18:36.157 | INVITE (561832) → | | |
| 2021-05-12 04:18:36.157 | ← Status:100 (561832) | | |
| 2021-05-12 04:18:36.165 | MEDIA FLOW ADD, ID=16777217, DIRECTION=CALLING | | |
| 2021-05-12 04:18:36.165 | MEDIA FLOW ADD, ID=16777218, DIRECTION=CALLED | | |
| 2021-05-12 04:18:36.167 | EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:+18507904044@CUCM-Cisco.pe.oracle.com:5060 | | |
| 2021-05-12 04:18:36.167 | | | INVITE (561832) → |
| 2021-05-12 04:18:36.172 | | | ← Status:100 (561832) |
| 2021-05-12 04:18:36.200 | | | ← Status:180 (561832) |
| 2021-05-12 04:18:36.203 | ← Status:180 (561832) | | |
| 2021-05-12 04:18:53.669 | | | ← Status:200 (561832) |
| 2021-05-12 04:18:53.677 | MEDIA FLOW MODIFY, ID=16777218, DIRECTION=CALLED | | |
| 2021-05-12 04:18:53.678 | MEDIA FLOW MODIFY, ID=16777217, DIRECTION=CALLING | | |
| 2021-05-12 04:18:53.681 | ← Status:200 (561832) | | |
| 2021-05-12 04:18:53.783 | ACK (561832) → | | |
| 2021-05-12 04:18:53.784 | | | ACK (561832) → |

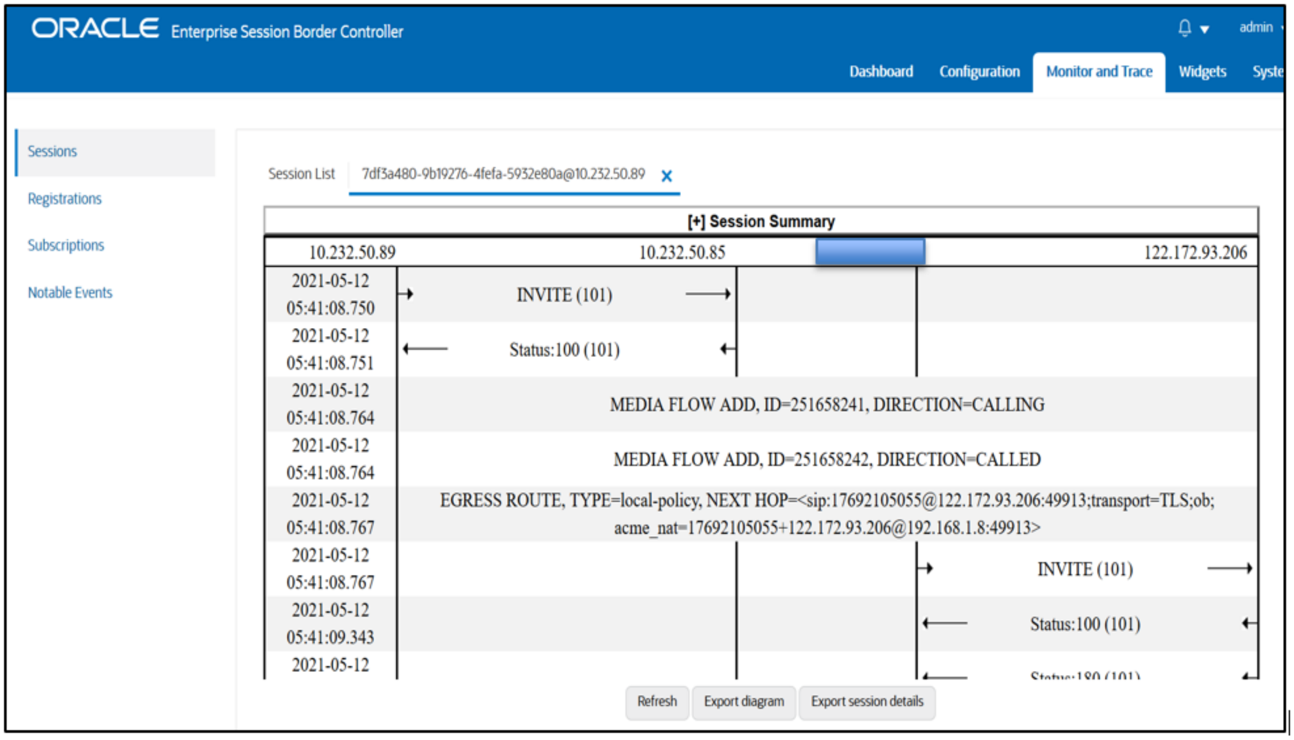
5. Make Call from Twilio Elastic Sip Trunk user to Cisco Remote user and check the call flow. Now, there will be 2 call legs (hair pinned call) as the call reaches Cisco CUCM first and then reaches Cisco Remote user after that as given below.



Session List 328f307d6f0184f58c0bbe73ef4c9c74@0.0.0.0

[+] Session Summary

```
                         54.172.60.3                10.232.50.78                10.232.50.89
2021-05-12 05:41:08.721  → INVITE (949134) →
2021-05-12 05:41:08.721  ← Status:100 (949134) ←
2021-05-12 05:41:08.735  MEDIA FLOW ADD, ID=234881025, DIRECTION=CALLING
2021-05-12 05:41:08.735  MEDIA FLOW ADD, ID=234881026, DIRECTION=CALLED
2021-05-12 05:41:08.737  EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:+17692105055@CUCM-Cisco.pe.oracle.com:5060
2021-05-12 05:41:08.737                                               → INVITE (949134) →
2021-05-12 05:41:08.743                                               ← Status:100 (949134) ←
2021-05-12 05:41:09.768                                               ← Status:180 (949134) ←
2021-05-12 05:41:09.773  ← Status:180 (949134) ←
2021-05-12 05:41:14.420                                               ← Status:200 (949134) ←
2021-05-12 05:41:14.437  MEDIA FLOW MODIFY, ID=234881026, DIRECTION=CALLED
2021-05-12 05:41:14.437  MEDIA FLOW MODIFY, ID=234881025, DIRECTION=CALLING
2021-05-12 05:41:14.441  ← Status:200 (949134) ←
2021-05-12 05:41:14.546  → ACK (949134) →
2021-05-12 05:41:14.549                                               → ACK (949134) →
```



Session List 7df3a480-9b19276-4fefa-5932e80a@10.232.50.89

[+] Session Summary

```
                         10.232.50.89          10.232.50.85                122.172.93.206
2021-05-12 05:41:08.750  → INVITE (101) →
2021-05-12 05:41:08.751  ← Status:100 (101) ←
2021-05-12 05:41:08.764  MEDIA FLOW ADD, ID=251658241, DIRECTION=CALLING
2021-05-12 05:41:08.764  MEDIA FLOW ADD, ID=251658242, DIRECTION=CALLED
2021-05-12 05:41:08.767  EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:17692105055@122.172.93.206:49913;transport=TLS;ob;
                         acme_nat=17692105055+122.172.93.206@192.168.1.8:49913>
2021-05-12 05:41:08.767                                               → INVITE (101) →
2021-05-12 05:41:09.343                                               ← Status:100 (101) ←
2021-05-12                                                            ← Status:180 (101) ←
```

## Appendix A

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

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

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

ORACLE

**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