Oracle SBC integration with Teams Direct Routing 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 MS Teams DR and Twilio Elastic SIP Trunking	25th March 2021
1.1	Added new section for SBC config/Deployment Using Configuration Assistant	7th December 2021
1.2	Removed reference to sip-all FQDN from the app note document	12th January 2022
1.3	Since sip-all FQDN is removed, add the following two sections: Enable refer call xfer on realm Added RespondOptionsManip	22nd July 2022
1.4	Added DigiCert Global G2 Cert as root CA for Teams Changed certificate-record screenshots	5th Sep 2022
1.5	Added SIP access Control	13th Sep 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 Microsoft Teams Direct Routing Enterprise Model.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Twilio Elastic Sip Trunk with Microsoft Teams Direct Routing. The solution contained within this document has been tested using Oracle Communication SBC with **OS 840p3B version**.

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

Please find the related documentation links below:

2.1. Twilio Elastic SIP Trunking

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

Sign up for a free Twilio trial and learn more about configuring your Twilio Elastic SIP Trunk.

2.2. Microsoft Teams

Microsoft Phone System Direct Routing allows connection of a supported customer-provided Session Border Controller (SBC) to a Microsoft Phone System. Direct Routing enables using virtually any PSTN trunk with Microsoft Phone System and configuring interoperability between customer-owned telephony equipment, such as a third-party private branch exchange (PBX), analog devices, and Microsoft Phone System.

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

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

https://www.oracle.com/a/otn/docs/vzbwithsbcmsftteams-mb.pdf https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

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 Teams Direct Routing Enterprise Model using Oracle Enterprise SBC. There will be steps that require navigating the Teams 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.

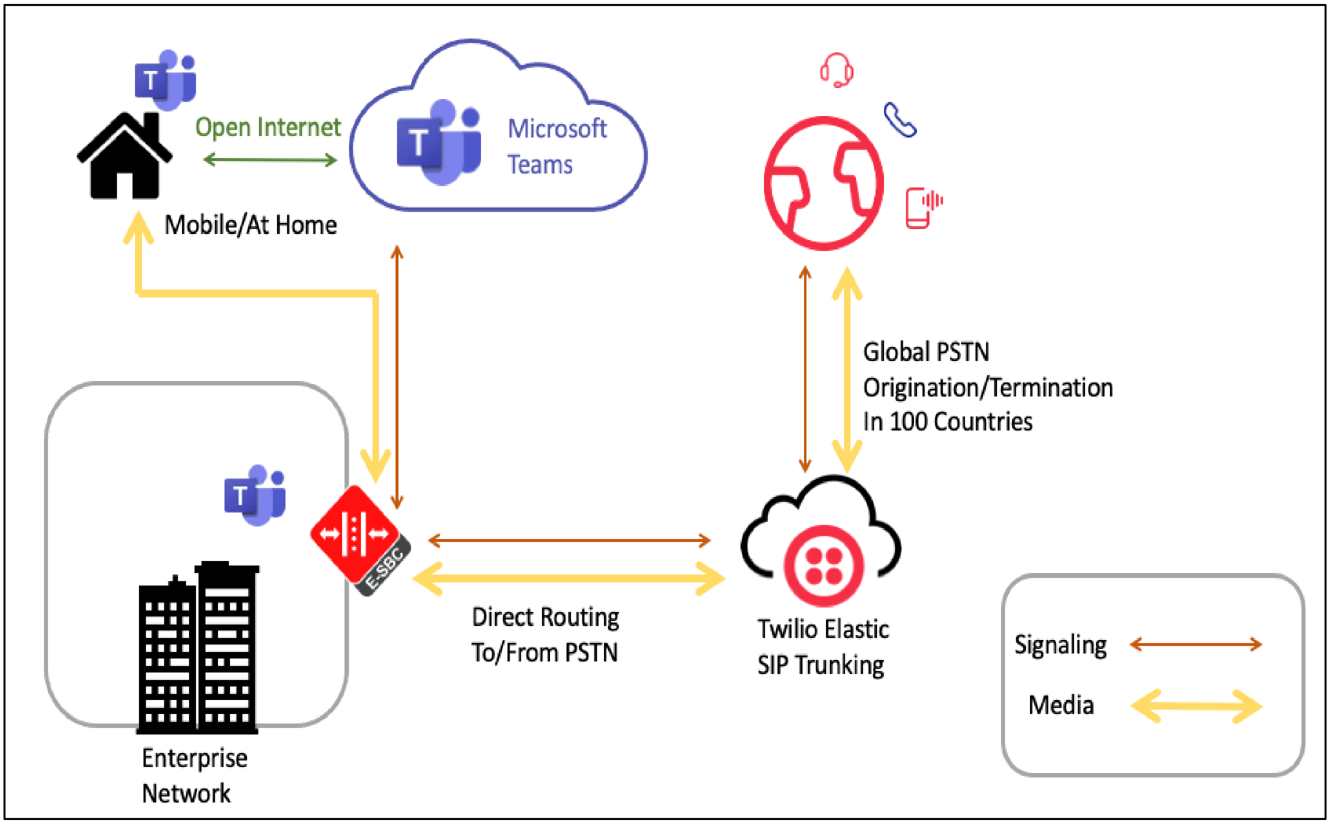
3.2. Requirements

- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version
- Teams Direct Routing Enterprise Model running Teams Client.

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

Software Used	SBC Version	Teams Client version
Revision 1	8.4.0	1.3.00.28779 (64-bit) (Windows) v.1416/1.0.0.2021010802 (Mobile)

3.3. Architecture


Open Internet
Microsoft Teams
Mobile/At Home
Global PSTN Origination/Termination In 100 Countries
E-SBC
Direct Routing To/From PSTN
Twilio Elastic SIP Trunking
Signaling
Media
Enterprise Network

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

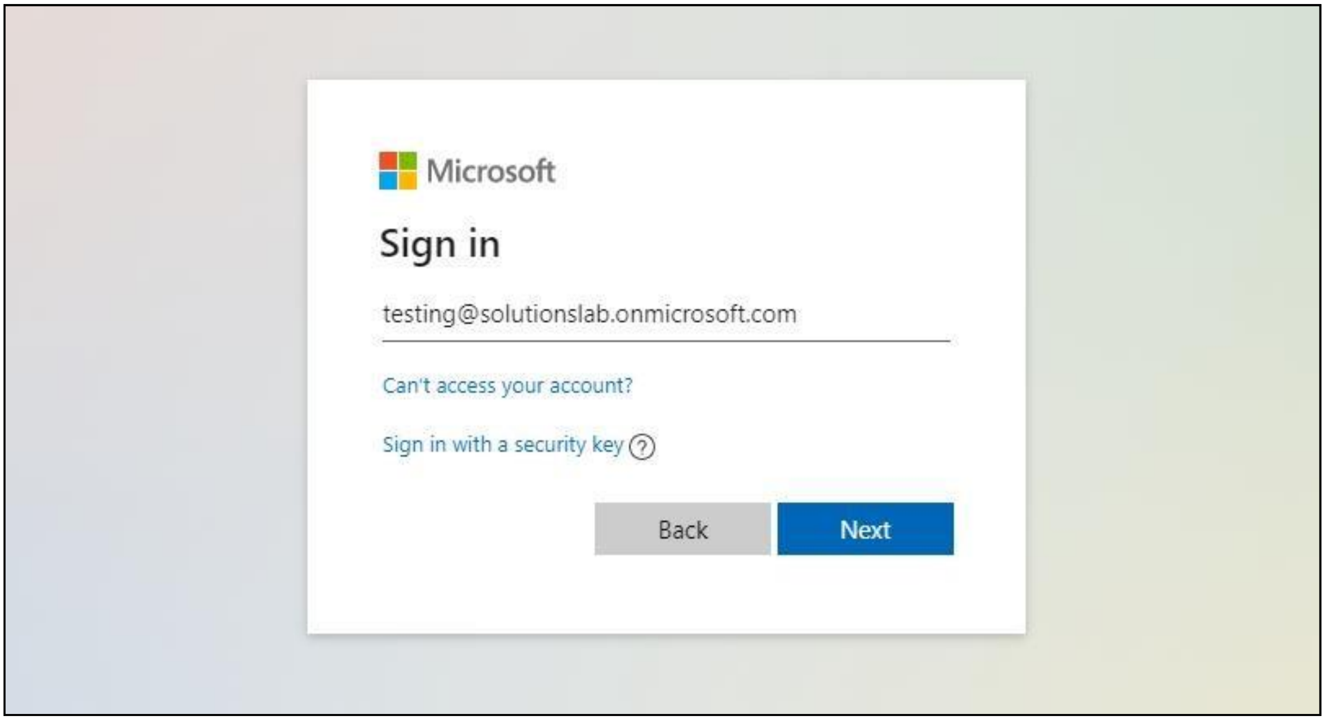
- Phase 1 – Configuring the Teams Direct Routing Enterprise Model.
- Phase 2 – Configuring the Oracle SBC.
- Phase 3 – Configuring the Twilio Elastic SIP Trunk

4. Configure Microsoft Teams Direct Routing

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

4.1. Access Teams Admin center

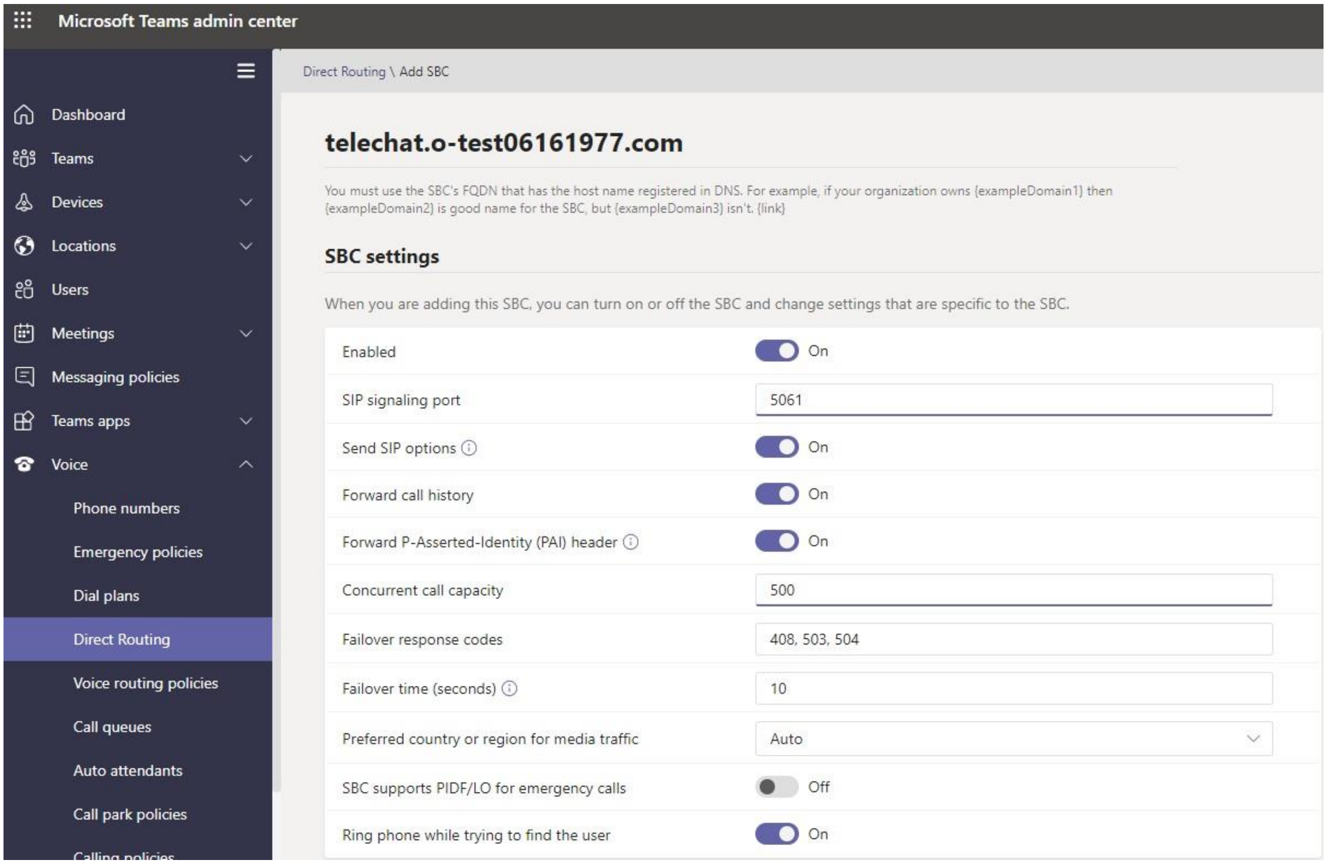
The first step is to access the Teams Admin Center with administrator admin credentials:



testing@solutionslab.onmicrosoft.com

4.2. Configure Online PSTN Gateway

Configuration Path: Voice/Direct Routing/SBC



telechat.o-test06161977.com

You must use the SBC's FQDN that has the host name registered in DNS. For example, if your organization owns {exampleDomain1} then {exampleDomain2} is good name for the SBC, but {exampleDomain3} isn't. {link}

SBC settings

When you are adding this SBC, you can turn on or off the SBC and change settings that are specific to the SBC.

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

Click Save at the bottom of the page

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

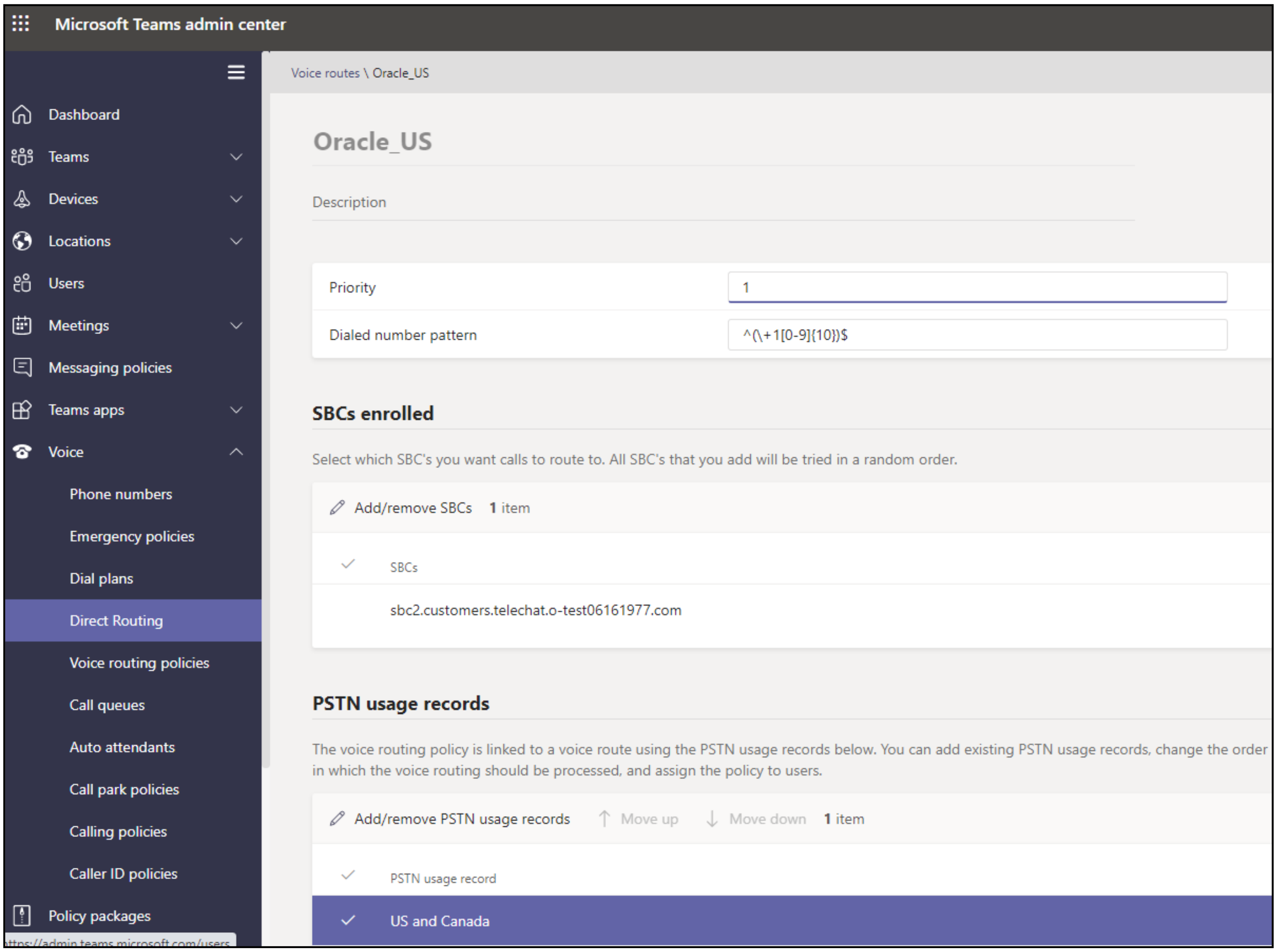
4.3. Configure Online PSTN Usage

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

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

4.4. Configure Online Voice Routes

Configuration Path: Voice/Direct Routing/Voice Routes



Oracle_US

Description

Priority: 1

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

SBCs enrolled

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

Add/remove SBCs 1 item

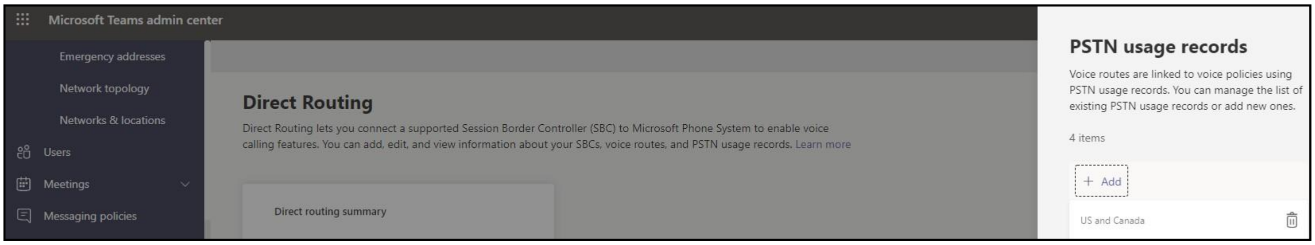
SBCs
sbc2.customers.telechat.o-test06161977.com

PSTN usage records

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

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

PSTN usage record
✓ US and Canada



Direct Routing

Direct Routing lets you connect a supported Session Border Controller (SBC) to Microsoft Phone System to enable voice calling features. You can add, edit, and view information about your SBCs, voice routes, and PSTN usage records. Learn more

PSTN usage records

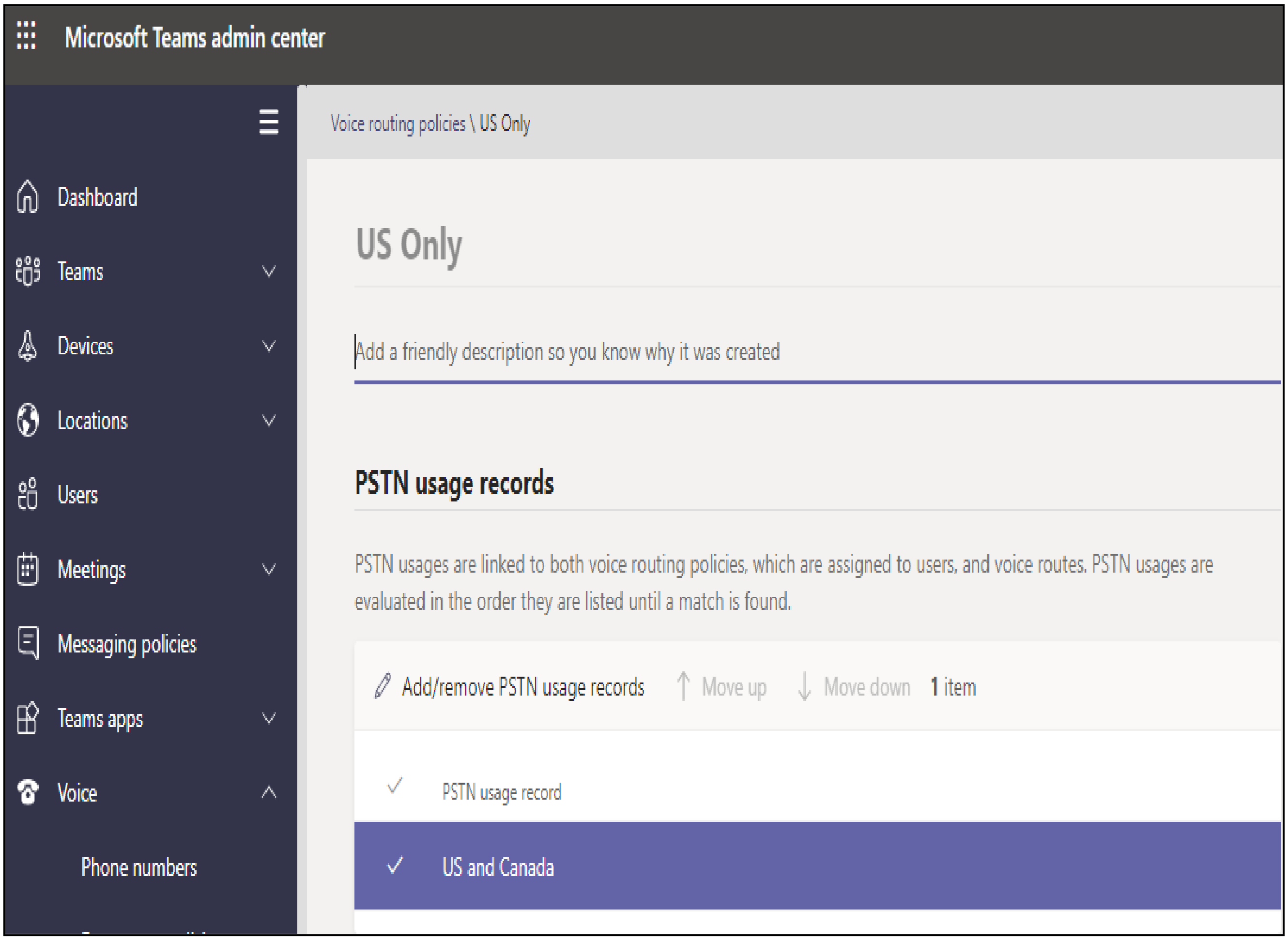
Voice routes are linked to voice policies using PSTN usage records. You can manage the list of existing PSTN usage records or add new ones.

4 items

US and Canada

4.5. Configure Online Voice Routing Policy

Configuration Path: Voice/Voice Routing Policies



Voice routing policies \ US Only

US Only

Add a friendly description so you know why it was created

PSTN usage records

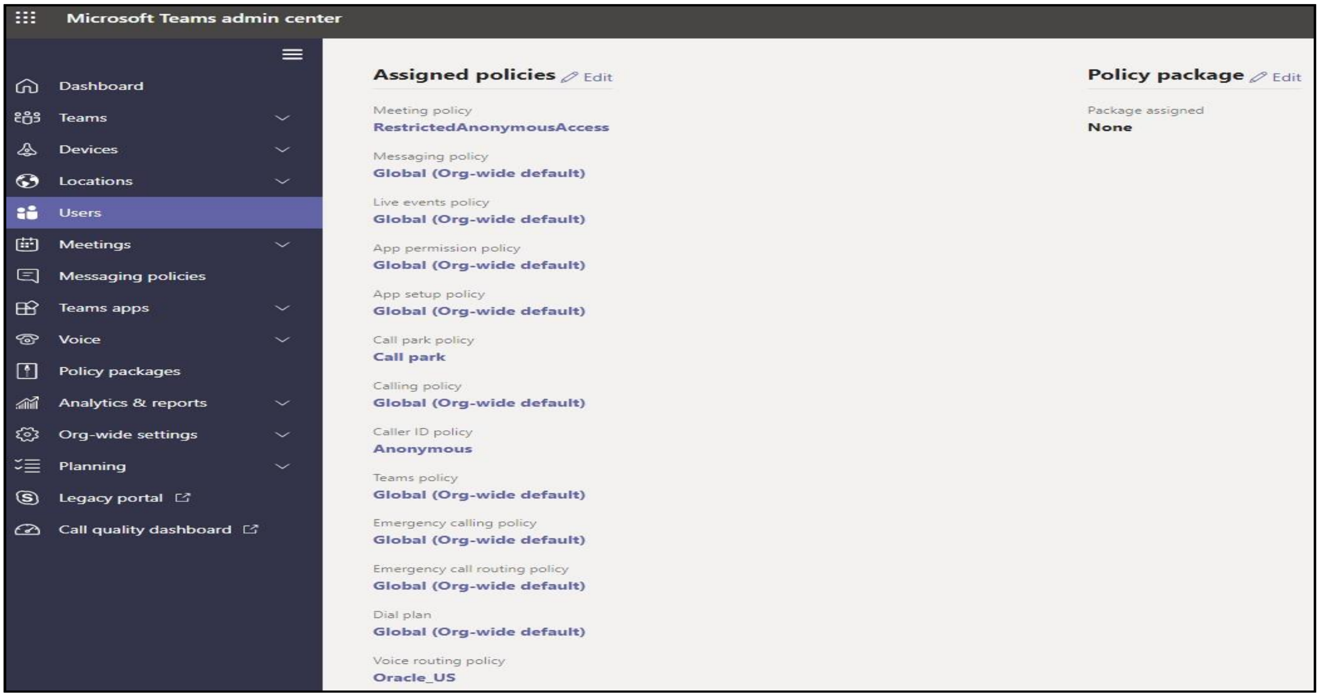
PSTN usages are linked to both voice routing policies, which are assigned to users, and voice routes. PSTN usages are evaluated in the order they are listed until a match is found.

✓	PSTN usage record
✓	US and Canada

4.6. Assign Voice Routing Policy to Users

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

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



Package assigned
None

Meeting policy
RestrictedAnonymousAccess

Messaging policy
Global (Org-wide default)

Live events policy
Global (Org-wide default)

App permission policy
Global (Org-wide default)

App setup policy
Global (Org-wide default)

Call park policy
Call park

Calling policy
Global (Org-wide default)

Caller ID policy
Anonymous

Teams policy
Global (Org-wide default)

Emergency calling policy
Global (Org-wide default)

Emergency call routing policy
Global (Org-wide default)

Dial plan
Global (Org-wide default)

Voice routing policy
Oracle_US

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

With this, Microsoft Teams Direct Routing config is complete.

5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Teams Direct Routing and Twilio Elastic SIP Trunking. If the Oracle SBC being deployed is new, with no existing configuration, the simplest way to configure it to interface with Microsoft Teams Direct Routing is by utilizing the Configuration Assistant feature.

5.1. Validated Oracle SBC version

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

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

6. New SBC configuration

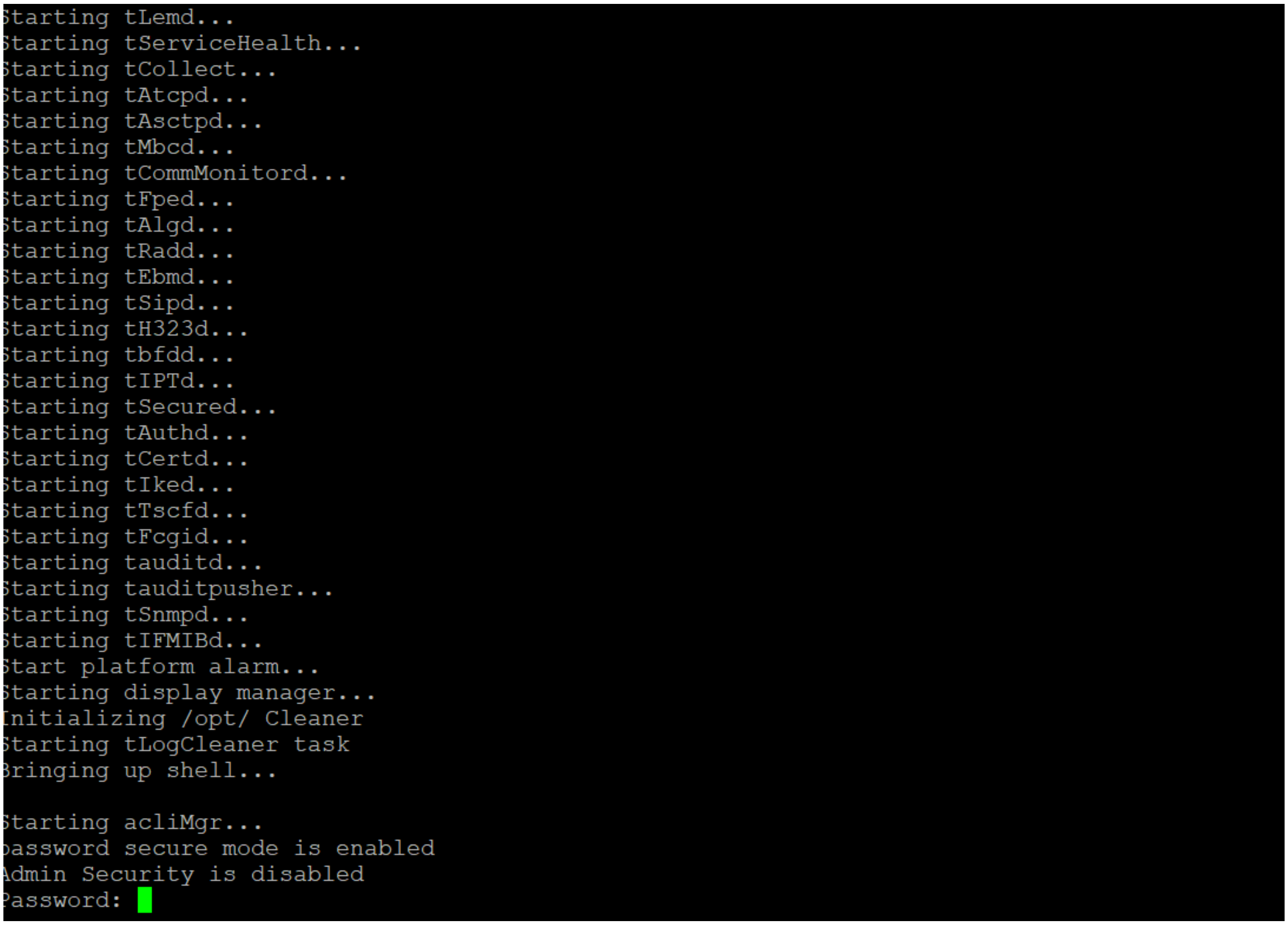
If the customer is looking to setup a new SBC from scratch, please follow the section below.

6.1. Establishing a serial connection to the SBC

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

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

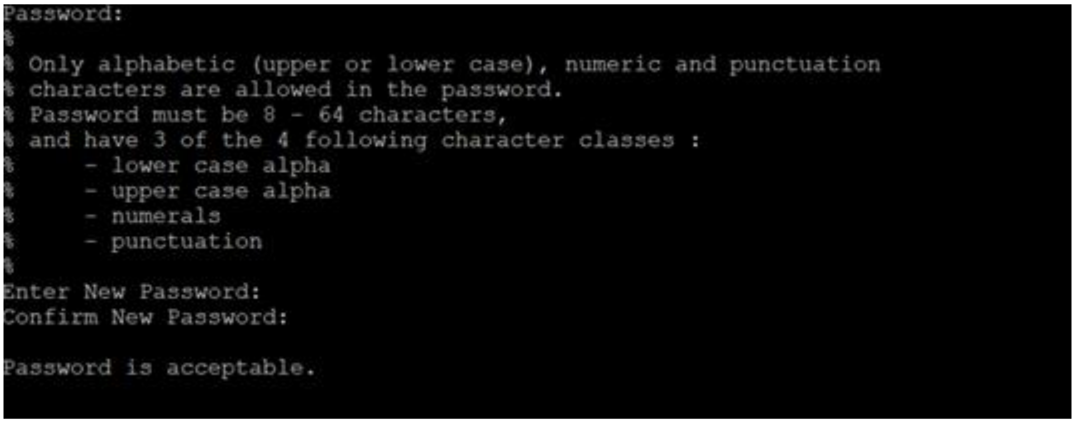
Power on the SBC and confirm that you see the following output from the boot-up sequence



```
Starting tLemd...
Starting tServiceHealth...
Starting tCollect...
Starting tAtcpd...
Starting tAsctpd...
Starting tMbcd...
Starting tCommMonitord...
Starting tFped...
Starting tAlgd...
Starting tRadd...
Starting tEbmd...
Starting tSipd...
Starting tH323d...
Starting tbfdd...
Starting tIPTd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tTscfd...
Starting tFcgid...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Starting tIFMIBd...
Start platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...

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

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

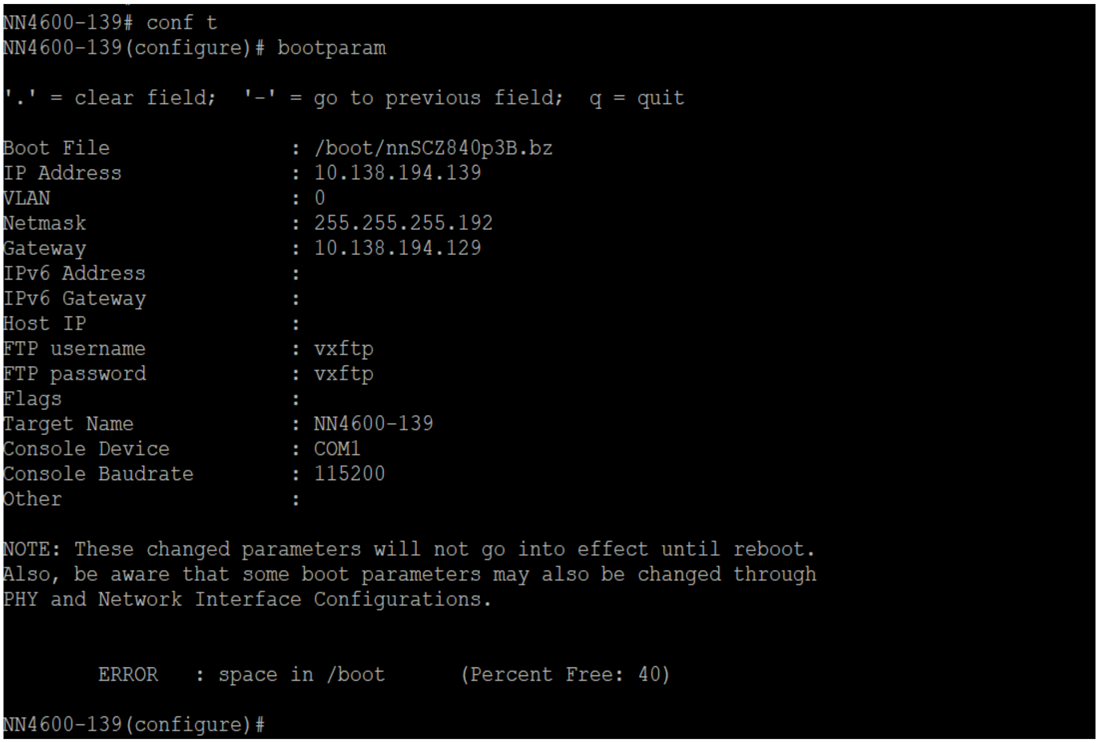
Both passwords have to be changed according to the rules shown below.



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

Password is acceptable.
```

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

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

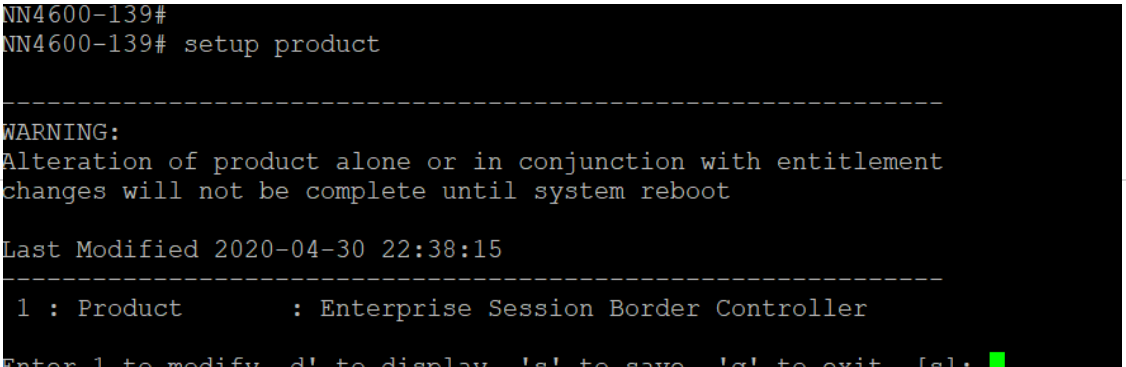


```
NN4600-139# conf t
NN4600-139(configure)# bootparam

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

Boot File                : /boot/nnSCZ840p3B.bz
IP Address               : 10.138.194.139
VLAN                     : 0
Netmask                  : 255.255.255.192
Gateway                  : 10.138.194.129
IPv6 Address             :
IPv6 Gateway             :
Host IP                  :
FTP username             : vxftp
FTP password             : vxftp
Flags                    :
Target Name              : NN4600-139
Console Device           : COM1
Console Baudrate         : 115200
Other                    :

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


        ERROR   : space in /boot      (Percent Free: 40)

NN4600-139(configure)#
```

Note: There is no management IP configured by default.

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

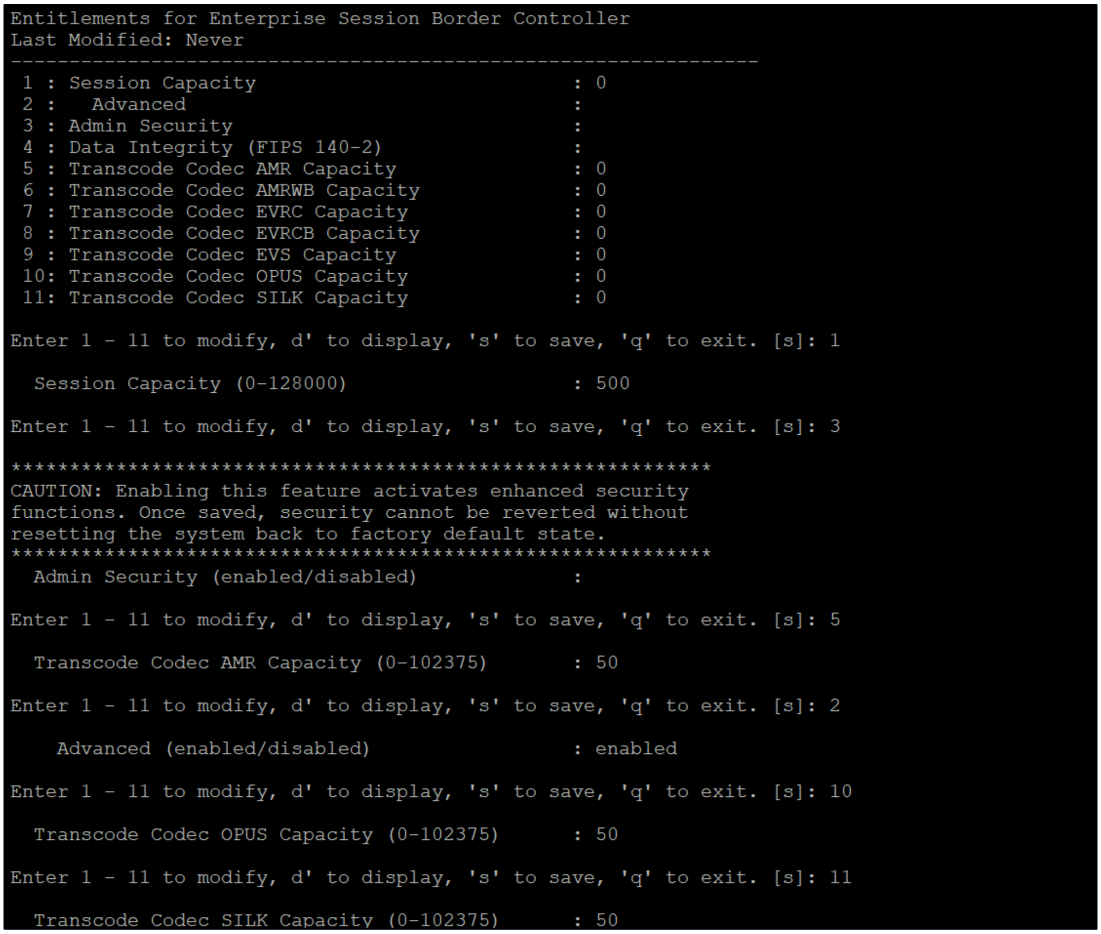
To configure product type, type in setup product in the terminal



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

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

Last Modified 2020-04-30 22:38:15
----------------------------------------------------------------
 1 : Product        : Enterprise Session Border Controller

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

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

Save the changes and reboot the SBC.

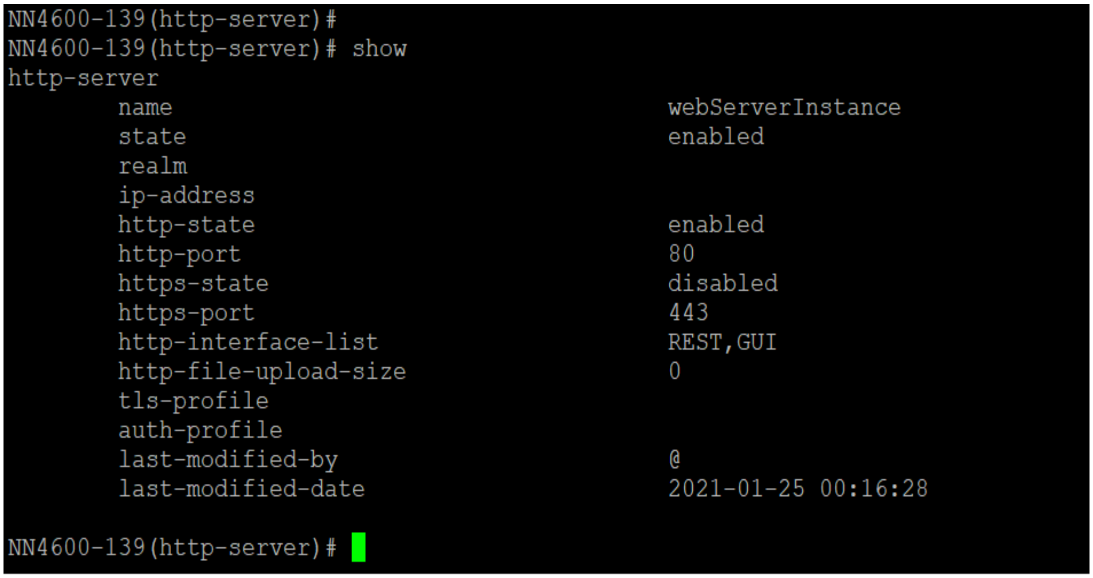


```
Entitlements for Enterprise Session Border Controller
Last Modified: Never
----------------------------------------------------------------
 1 : Session Capacity                             : 0
 2 :   Advanced                                   :
 3 : Admin Security                               :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

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Session Capacity (0-128000)                    : 500

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 3

************************************************************
CAUTION: Enabling this feature activates enhanced security
functions. Once saved, security cannot be reverted without
resetting the system back to factory default state.
************************************************************
  Admin Security (enabled/disabled)              :

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 5

  Transcode Codec AMR Capacity (0-102375)       : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2

    Advanced (enabled/disabled)                  : enabled

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10

  Transcode Codec OPUS Capacity (0-102375)      : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 11

  Transcode Codec SILK Capacity (0-102375)      : 50
```

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

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

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

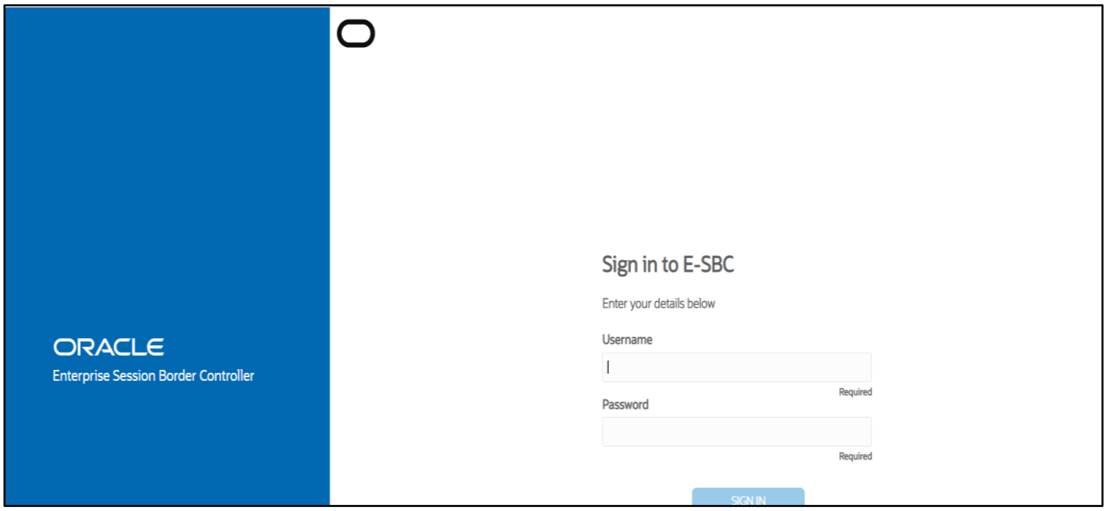


```
NN4600-139(http-server)#
NN4600-139(http-server)# show
http-server
        name                                webServerInstance
        state                               enabled
        realm
        ip-address
        http-state                          enabled
        http-port             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

NN4600-139(http-server)# 
```

6.2. Configure SBC using Web GUI

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

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



ORACLE
Enterprise Session Border Controller

Sign in to E-SBC

Enter your details below

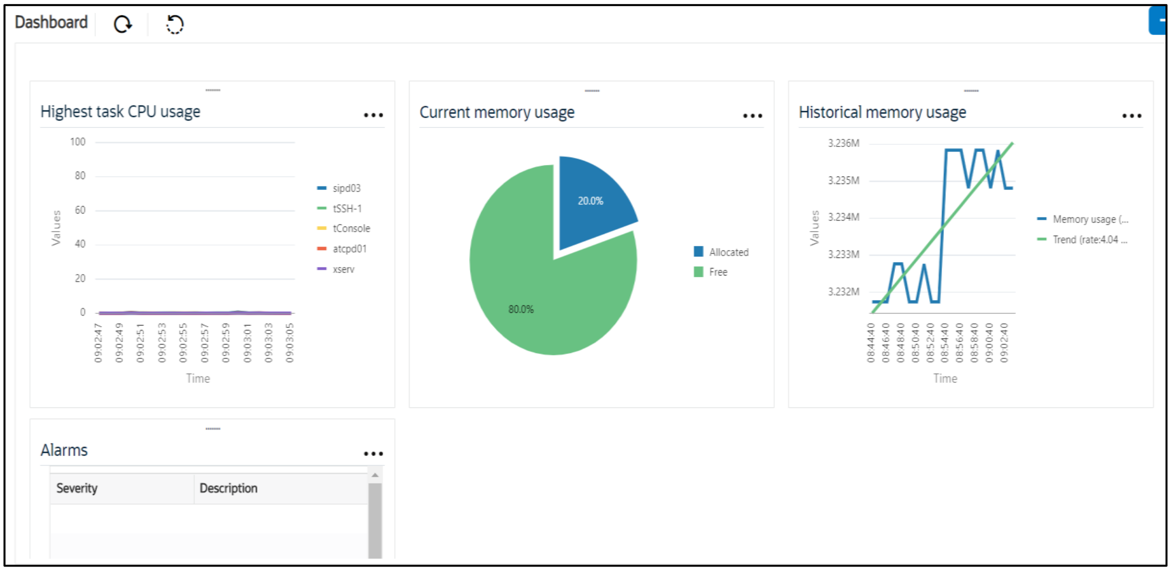
Username

Required

Password

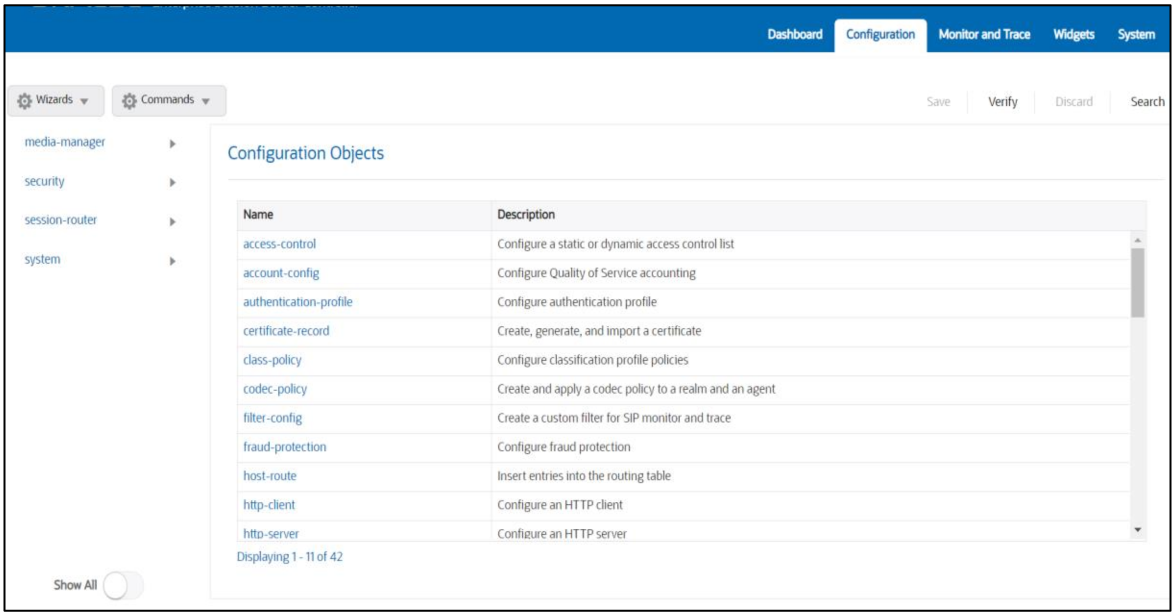
Required

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



Severity	Description

Go to Configuration as shown below, to configure the SBC



Configuration Objects

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

Displaying 1 - 11 of 42

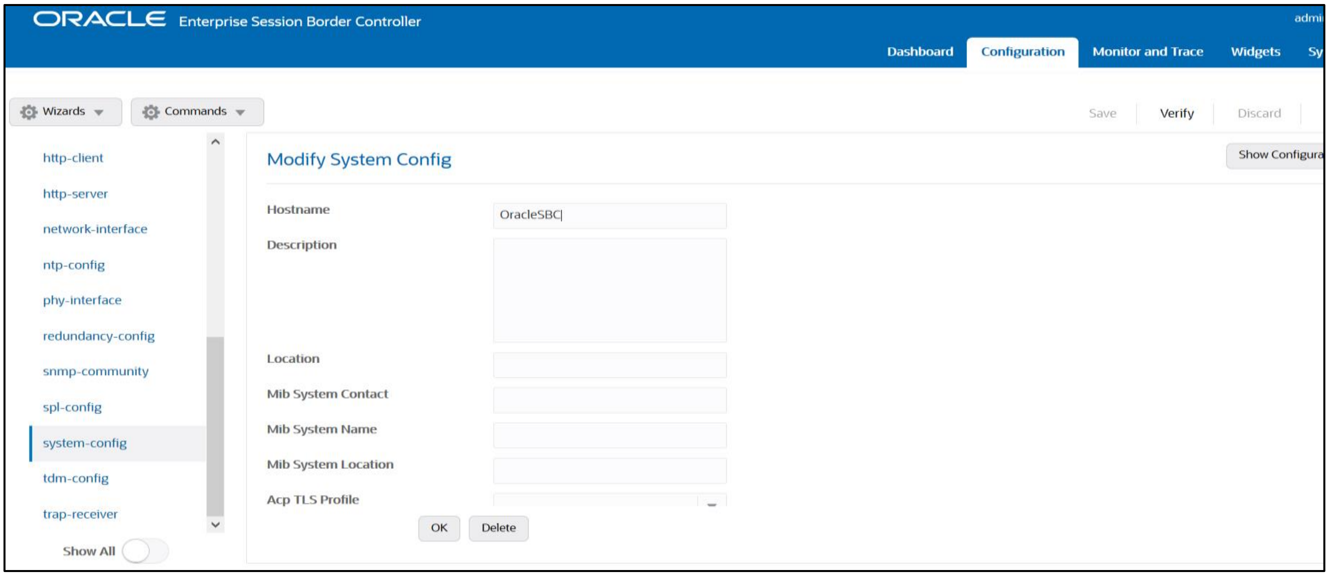
Kindly refer to the GUI User Guide given below for more information.

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

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

6.3. Configure system-config

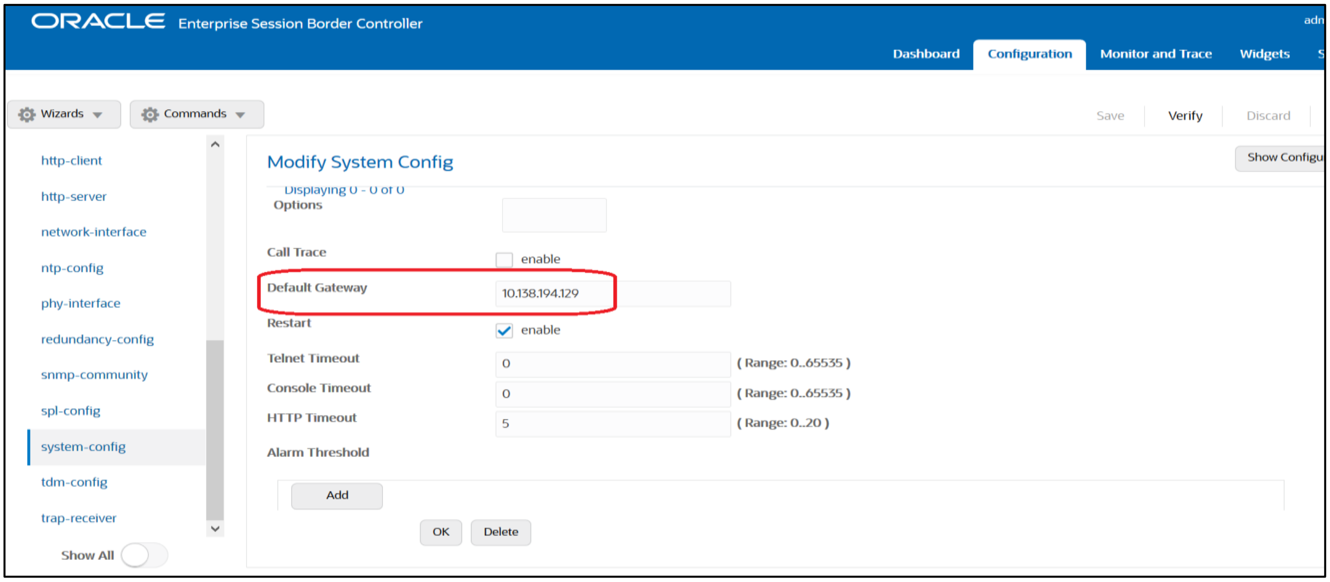
Go to system->system-config



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/8.4.0/releasenotes/esbc_scz840_releasenotes.pdf

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

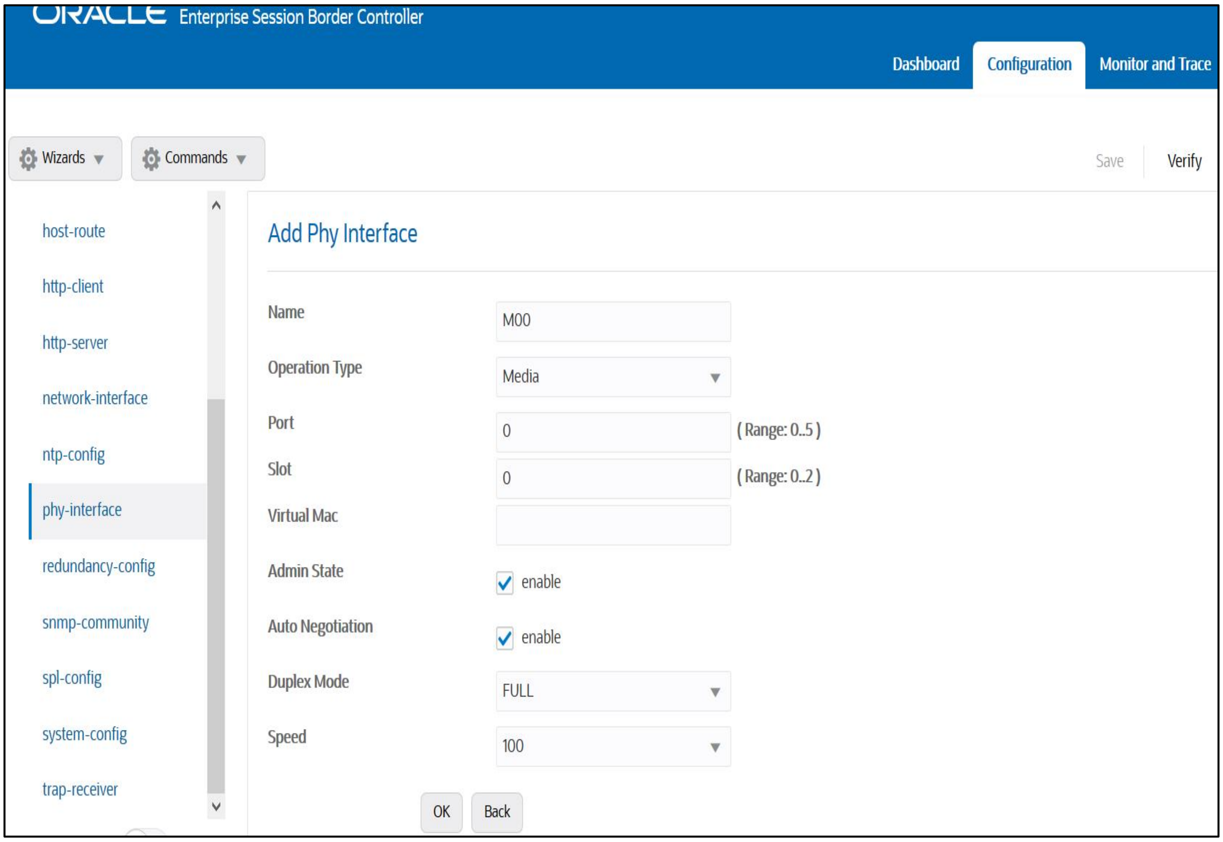
6.4. Configure Physical Interface values

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

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

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

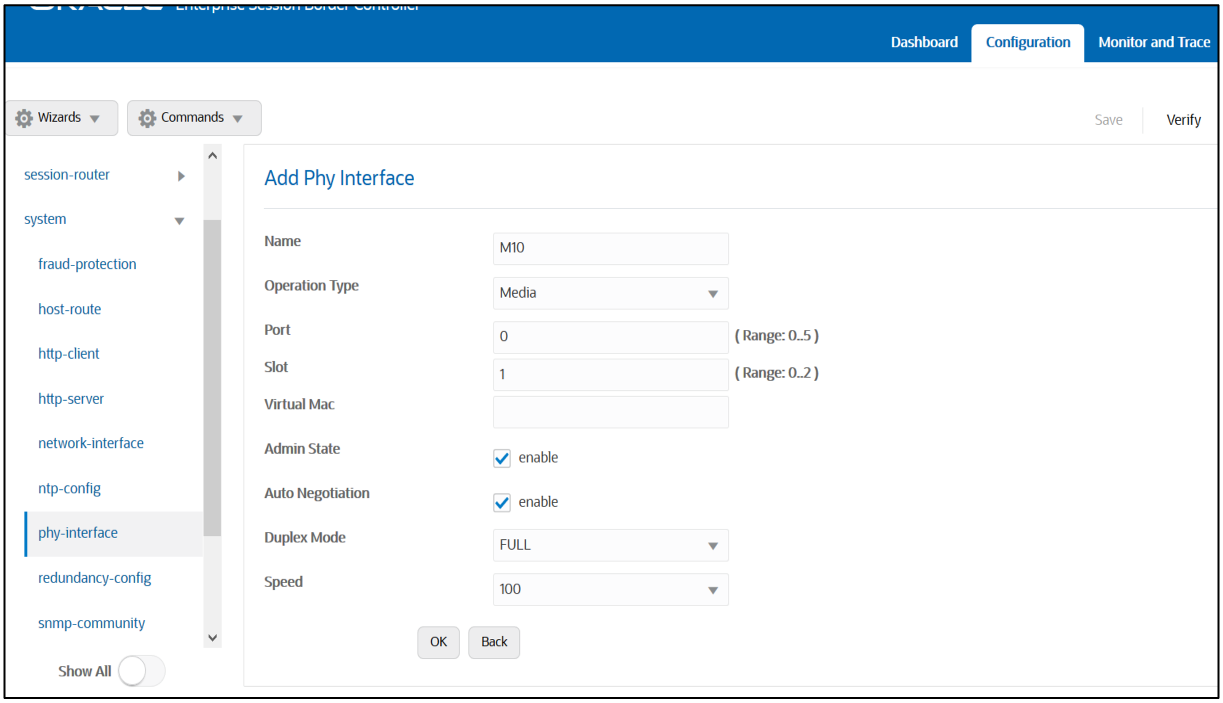
Please configure M00 interface as below.



Add Phy Interface

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

Please configure M10 interface as below



Add Phy Interface

Name: M10

Operation Type: Media

Port: 0 (Range: 0..5)

Slot: 1 (Range: 0..2)

Virtual Mac:

Admin State: ☑ enable

Auto Negotiation: ☑ enable

Duplex Mode: FULL

Speed: 100

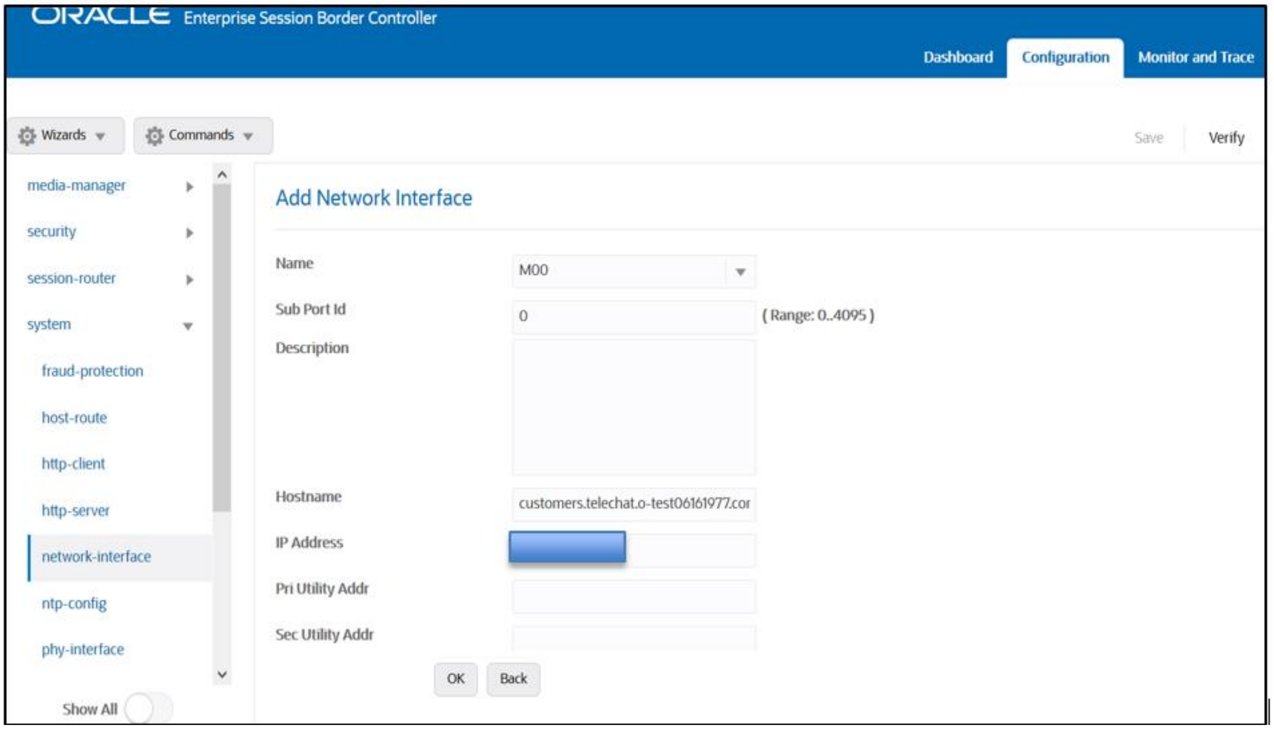
6.5. Configure Network Interface values

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

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

Parameter Name	Teams side network interface	Twilio side Network interface
Name	M00	M10
Host Name	customers.telechat.o-test06161977.com	
IP address	[redacted]	155.212.214.102
Netmask	255.255.255.192	255.255.255.0
Gateway	[redacted]	155.212.214.1

Please configure network interface M00 as below



Add Network Interface

Name: M00

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

Description:

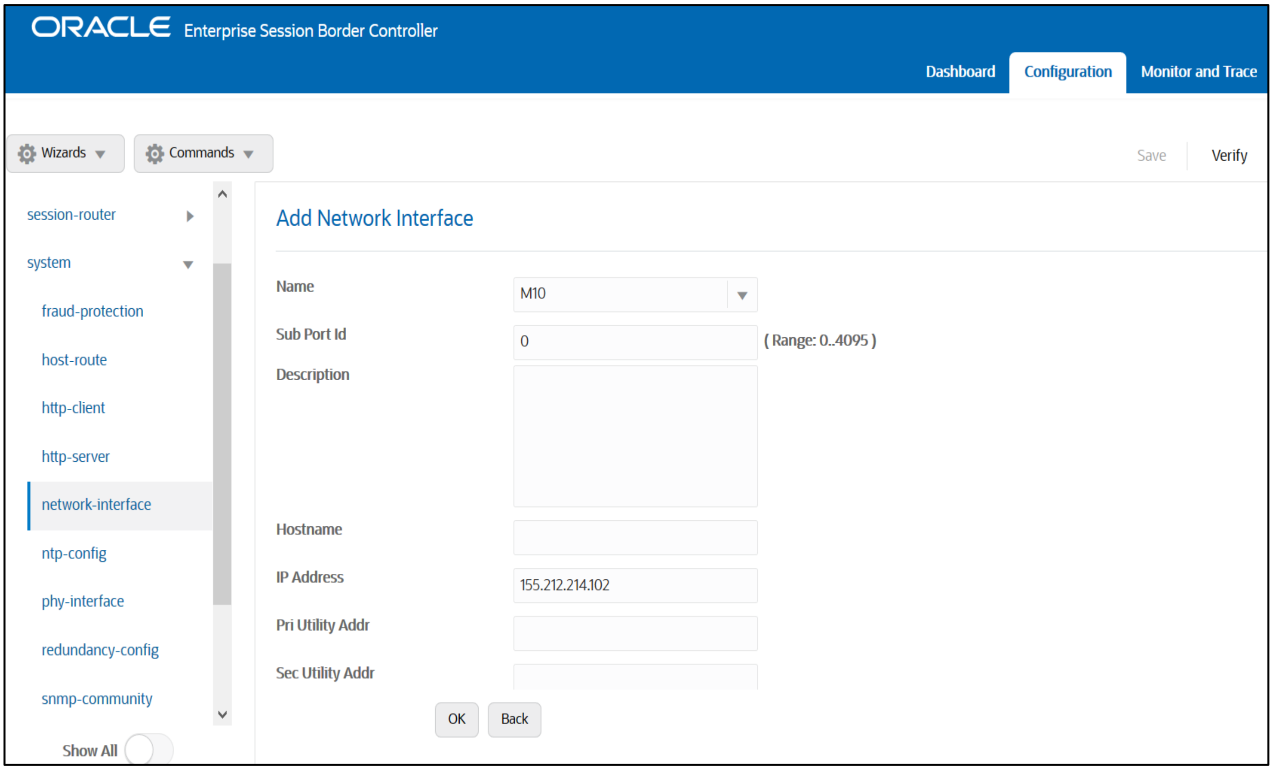
Hostname: customers.telechat.o-test06161977.cor

IP Address:

Pri Utility Addr:

Sec Utility Addr:

Similarly, configure network interface M10 as below



Add Network Interface

Name: M10

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

Description:

Hostname:

IP Address: 155.212.214.102

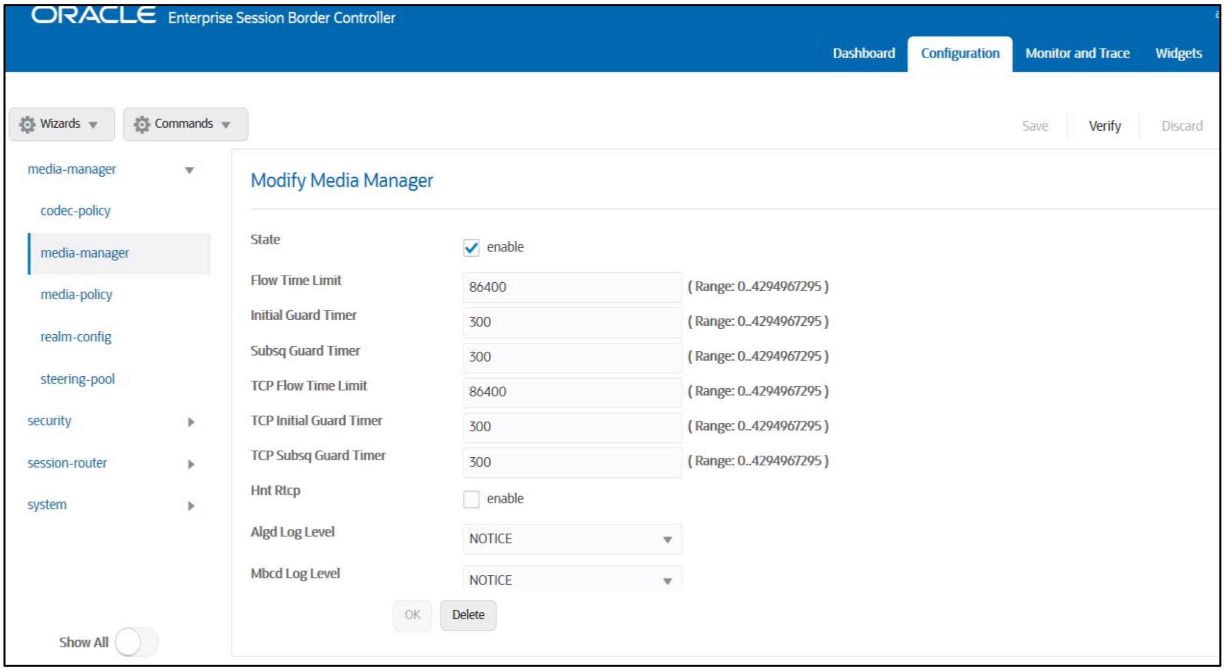
Pri Utility Addr:

Sec Utility Addr:

6.6. Enable media manager

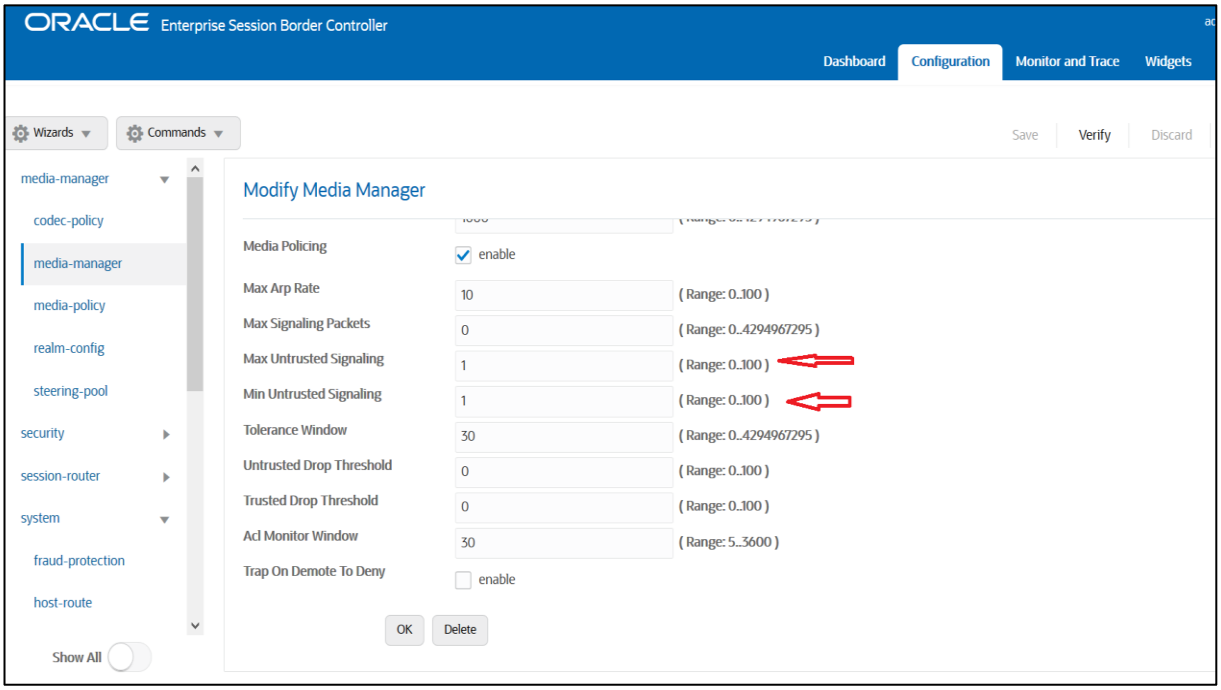
Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

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

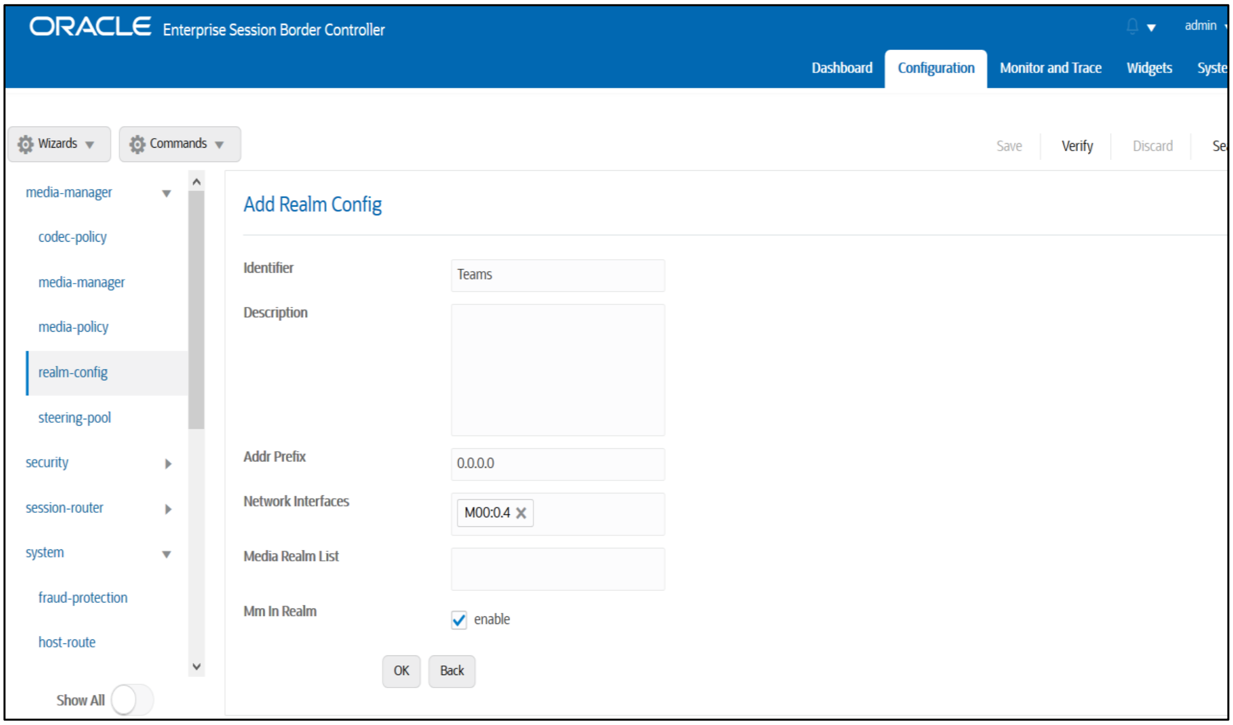
Navigate to realm-config under media-manager and configure a realm as shown below

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	Teams Side	Twilio Side
Identifier	Teams	TwilioSipTrunk
Network Interface	M00	M10
Mm in realm	☑	☑
Teams-FQDN	Telechat.o-test06161977.com	
Teams fqdn in uri	☑	
Sdp inactive only	☑	
Media Sec policy	sdespolicy	sdespolicy
RTCP mux	☑	
ice profile	ice	
Codec policy	addCN	OptimizeCodecs
RTCP policy	rtcpGen	
Access Control Trust Level	High	High
Pai-strip	Enabled	enabled
Refer Call Transfer	Enabled	

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



Add Realm Config

Identifier: Teams

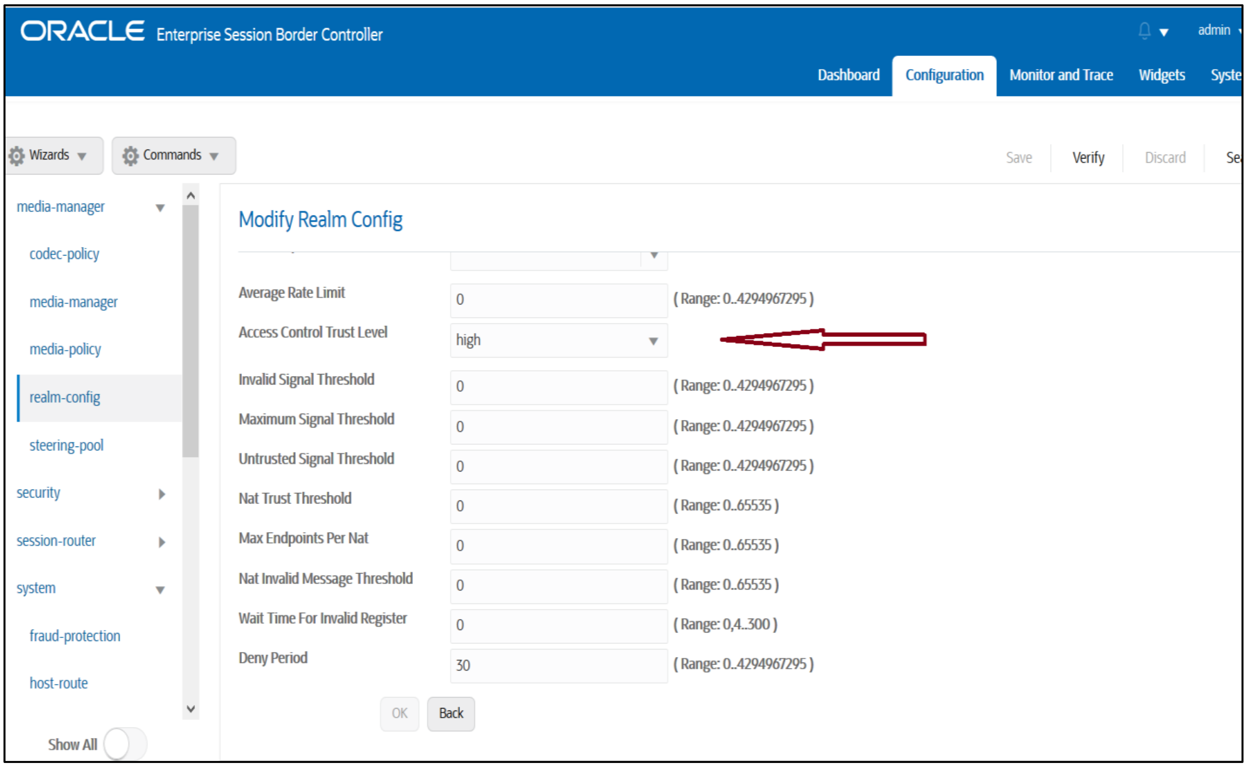
Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M00:0.4 ×

Media Realm List:

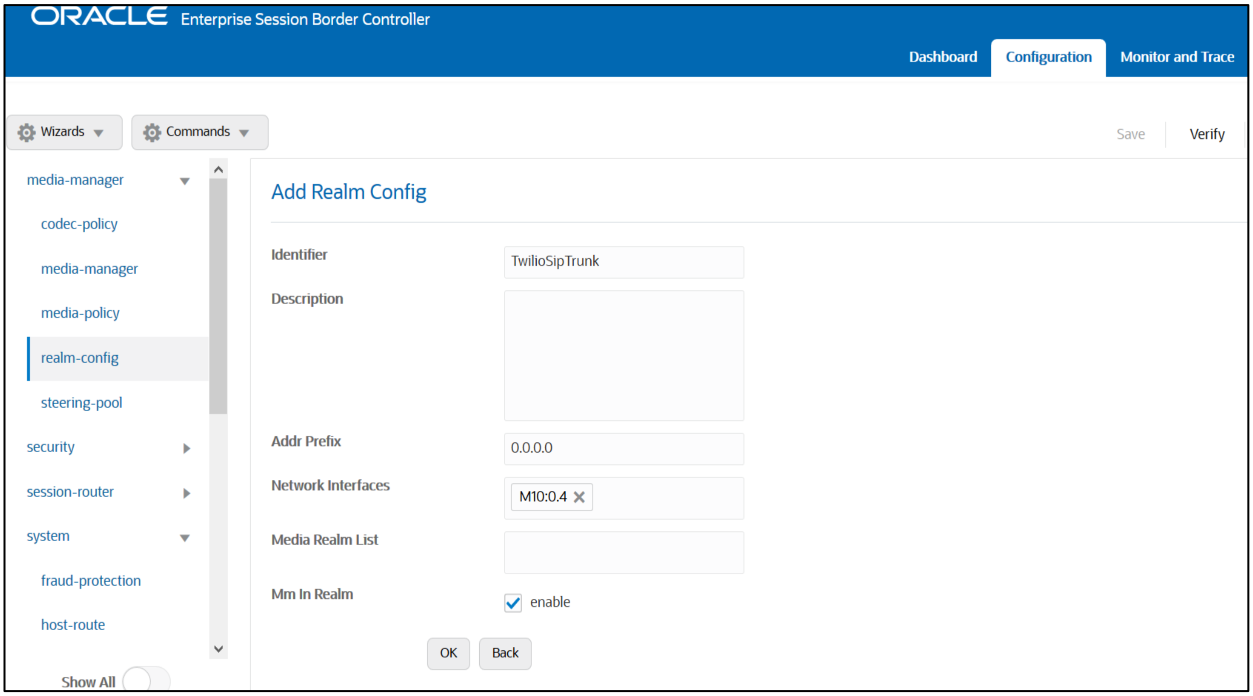
Mm In Realm: ☑ enable



Modify Realm Config

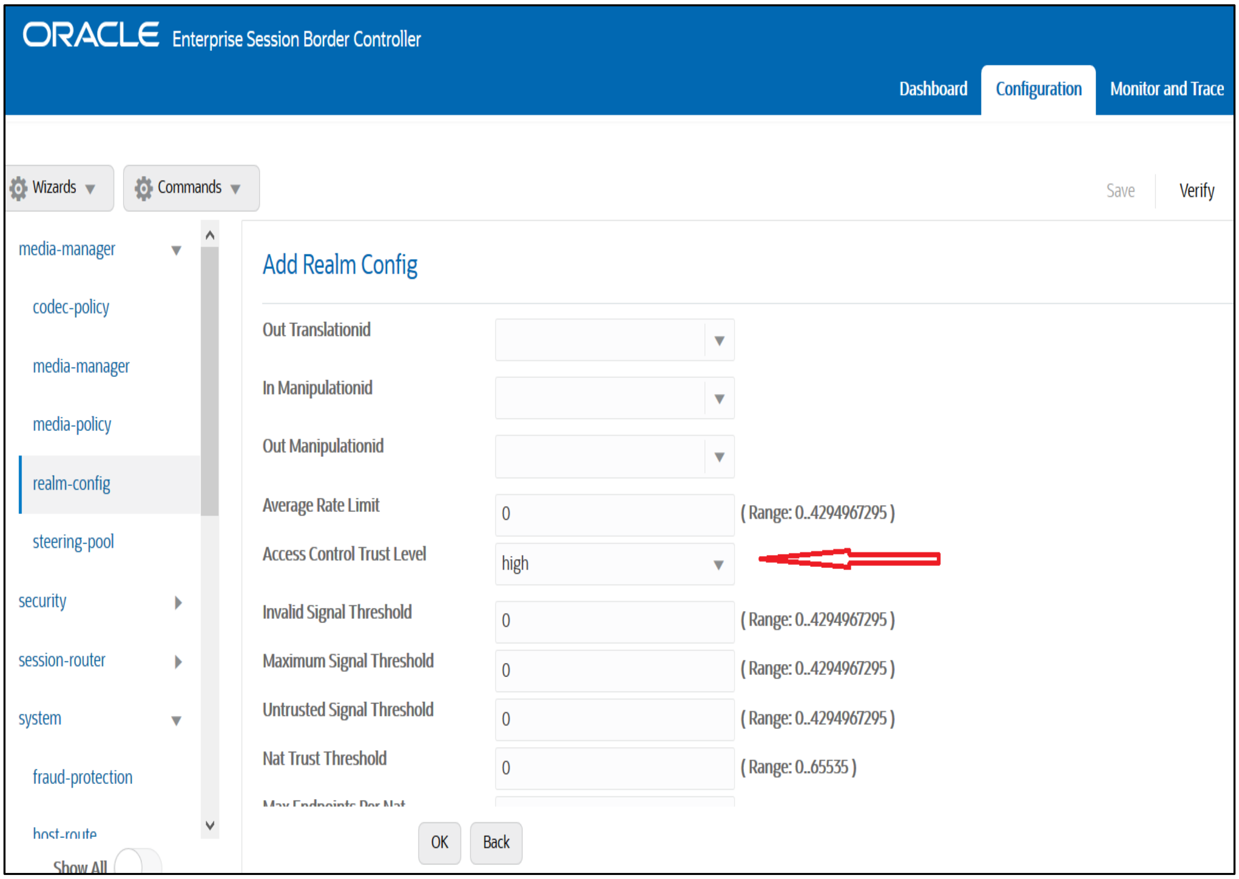
Average Rate Limit	0	(Range: 0..4294967295)
Access Control Trust Level	high	
Invalid Signal Threshold	0	(Range: 0..4294967295)
Maximum Signal Threshold	0	(Range: 0..4294967295)
Untrusted Signal Threshold	0	(Range: 0..4294967295)
Nat Trust Threshold	0	(Range: 0..65535)
Max Endpoints Per Nat	0	(Range: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

Similarly, Realm name is given as TwilioSipTrunk for Twilio Elastic SIP Trunking side. Please set the Access Control Trust Level as high for this realm too.



Add Realm Config

Identifier	TwilioSipTrunk
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		

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

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

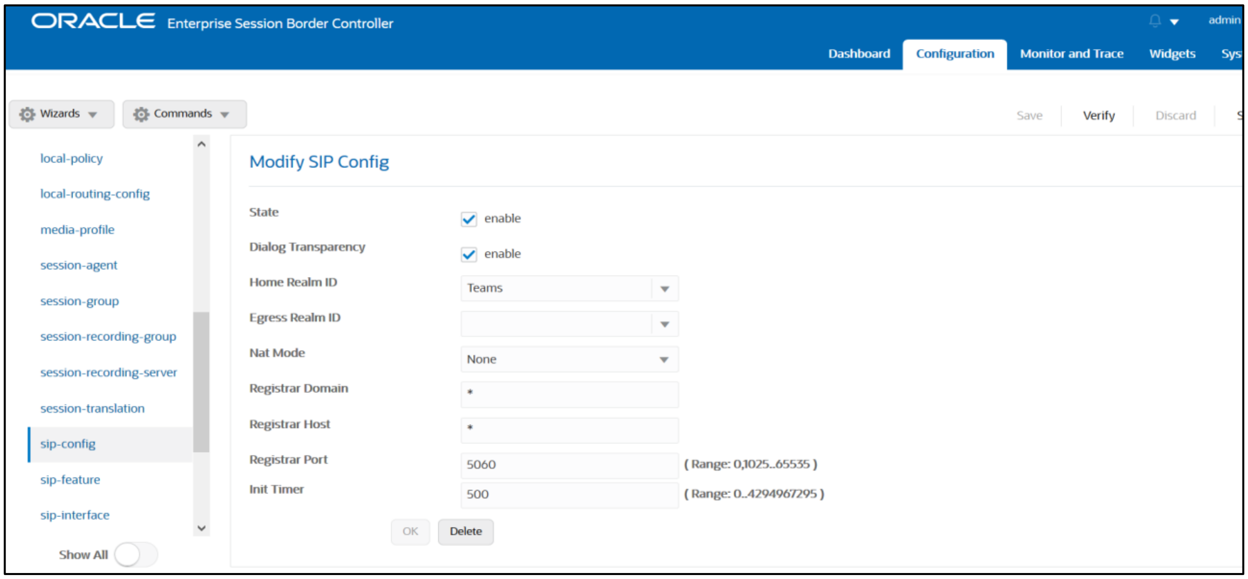
6.8. Enable sip-config

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

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

- add max-udp-length =0
- inmanip-before-validate

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



Modify SIP Config

State ☑ enable

Dialog Transparency ☑ enable

Home Realm ID: Teams

Egress Realm ID:

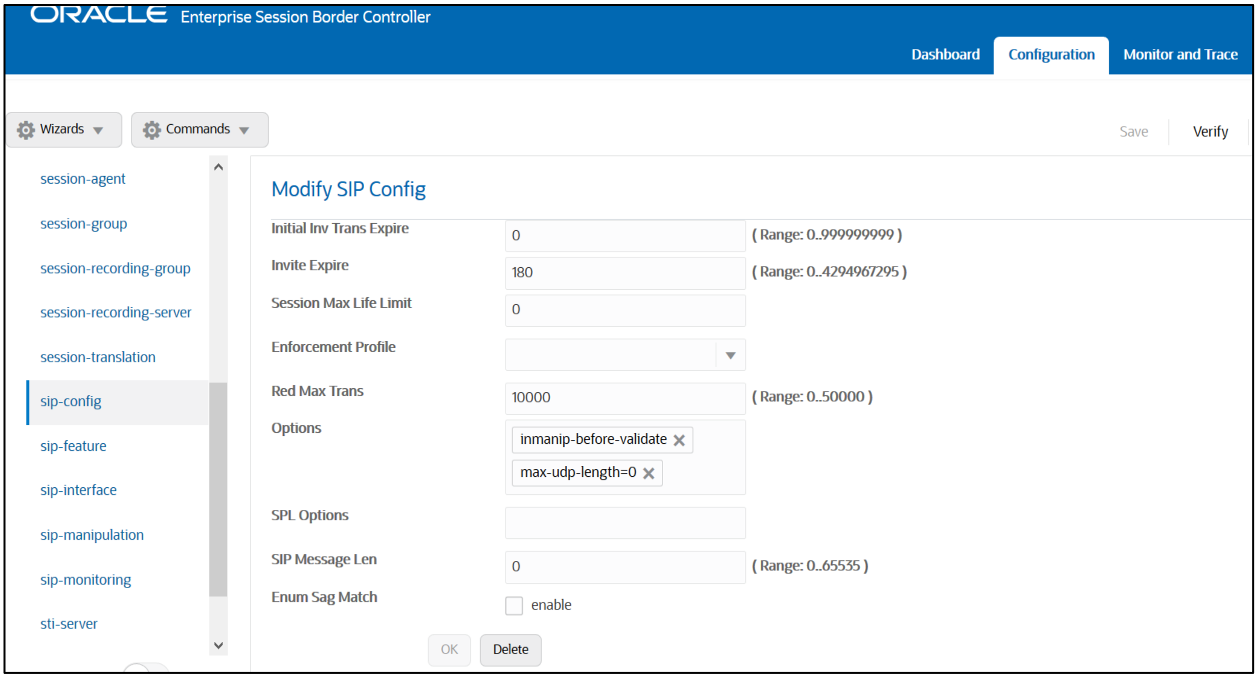
Nat Mode: None

Registrar Domain: *

Registrar Host: *

Registrar Port: 5060 (Range: 0,1025..65535)

Init Timer: 500 (Range: 0..4294967295)



Modify SIP Config

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: inmanip-before-validate ✕ max-udp-length=0 ✕

SPL Options:

SIP Message Len: 0 (Range: 0..65535)

Enum Sag Match □ enable

6.9. Configuring a certificate for SBC

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

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

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

For the purposes of this application note, we'll create these certificate records. They are as follows:

- SBC Certificate (end-entity certificate)
- GoDaddy Root Cert (Root CA used to sign the SBC's end entity certificate)
- BaltimoreRoot CA Cert (Microsoft Presents the SBC a certficate signed by this authority)
- DigiCert Global G2 Cert (Microsoft Presents the SBC a certficate signed by this authority)

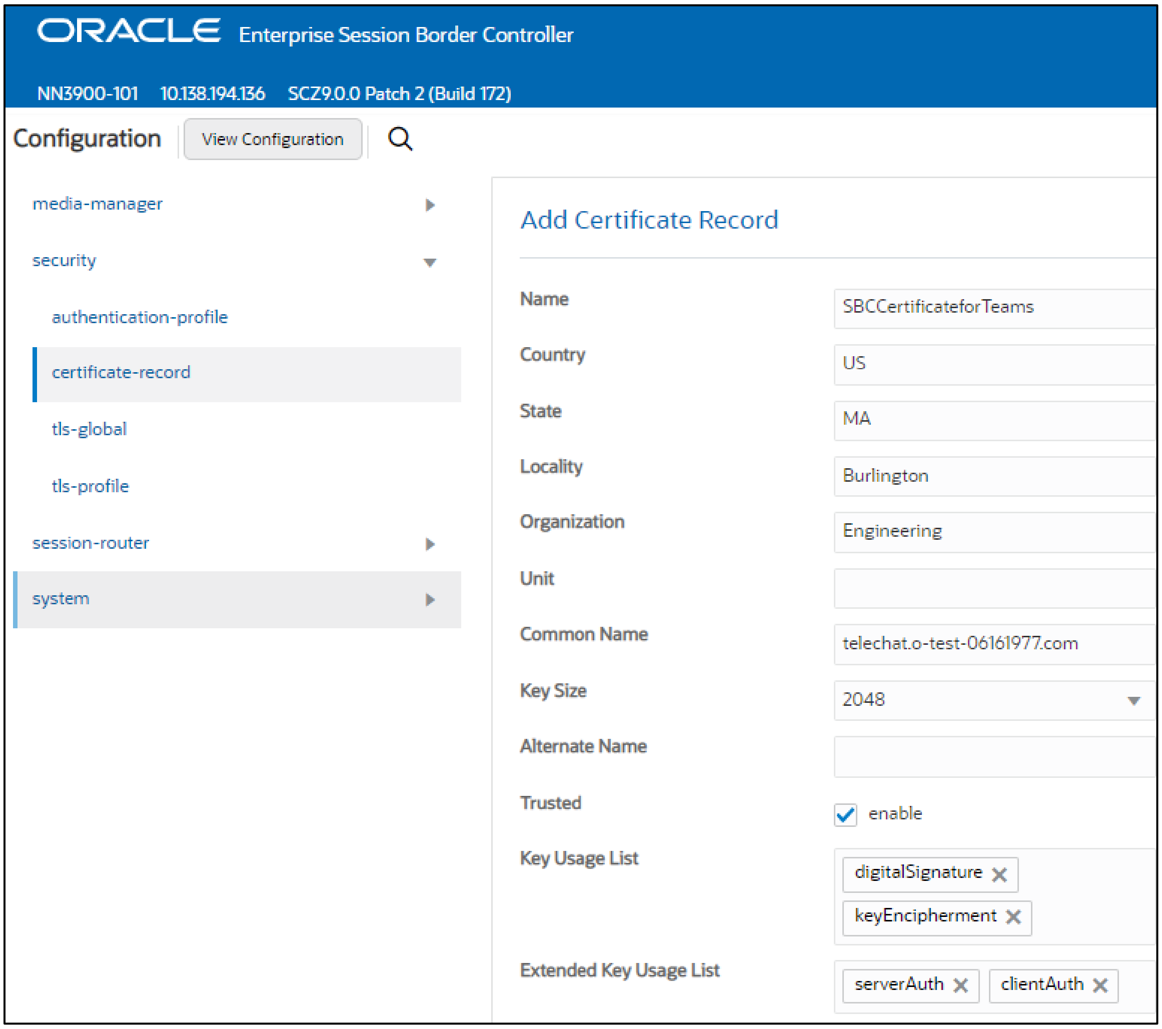
Note: The DigiCert RootCA is only part of this example, as that is the Authority we used to sign our SBC certificate. You would replace this with the root and/or intermediate certificates used to sign the CSR generated from your SBC.

SBC End Entity Certificate

The SBC's end entity certificate is the certificate the SBC presents to Microsoft to secure the connection. The only requirements when configuring this certificate is the common name must contain the SBC's FQDN. In this example our common name will be **telechat.o-test06161977.com.** You must also give it a name. All other fields are optional, and can remain at default values.

To Configure the certificate record:

Click Add, and use the following example to configure the SBC certificate



Add Certificate Record

Name	SBCCertificateforTeams
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	
Common Name	telechat.o-test-06161977.com
Key Size	2048
Alternate Name	
Trusted	☑ enable
Key Usage List	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth, clientAuth

- Click OK at the bottom

Next, using this same procedure, configure certificate records for the Root CA certificates

Root CA and Intermediate Certificates

- **Go Daddy Root**

The following, GoDaddyRoot, is the root CA certificate used to sign the SBC's end entity certificate. As mentioned above, your root CA and/or intermediate certificate may differ. This is for example purposes only.

- **DigiCert Global Root G2**

The DNS name of the Microsoft Teams Direct Routing interface is sip.pstnhub.microsoft.com. Microsoft presents a certificate to the SBC which is signed by DigiCert Global Root G2.To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate. You can download this certificate here: DigiCert Global Root G2

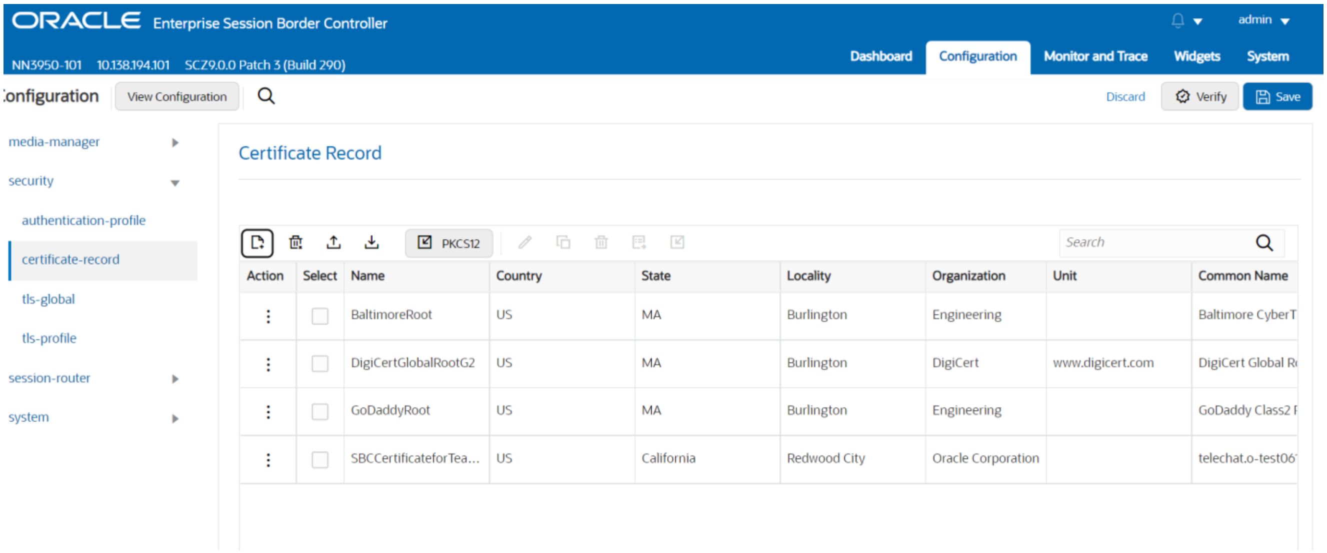
- **Baltimore Root**

The DNS name of the Microsoft Teams Direct Routing interface is sip.pstnhub.microsoft.com. Microsoft presents a certificate to the SBC which is signed by Baltimore Cyber Baltimore CyberTrust Root. To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate.

You can download this certificate here: https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt.pem

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

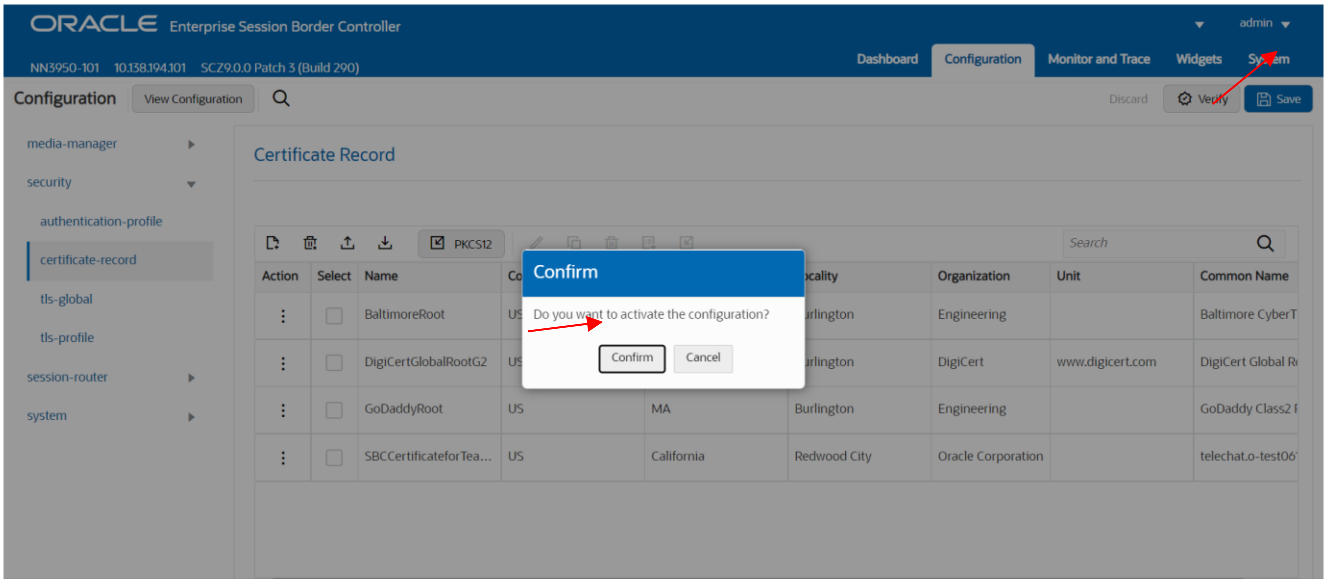
Config Parameter	Baltimore Root	GoDaddy Root	DigiCert Global Root G2
Common Name	Baltimore CyberTrust Root	Go Daddy Class2 Root CA	DigiCert Global Root G2
Key Size	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256



Certificate Record

Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
⋮	□	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberT
⋮	□	DigiCertGlobalRootG2	US	MA	Burlington	DigiCert	www.digicert.com	DigiCert Global R
⋮	□	GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 F
⋮	□	SBCCertificateforTea...	US	California	Redwood City	Oracle Corporation		telechat.o-test06

At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must **save and activate** the configuration of the SBC.



Certificate Record

Action	Select	Name	Co		ocality	Organization	Unit	Common Name
⋮	□	BaltimoreRoot	US		urlington	Engineering		Baltimore CyberT
⋮	□	DigiCertGlobalRootG2	US		urlington	DigiCert	www.digicert.com	DigiCert Global R
⋮	□	GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 I
⋮	□	SBCCertificateforTea...	US	California	Redwood City	Oracle Corporation		telechat.o-test06

Confirm

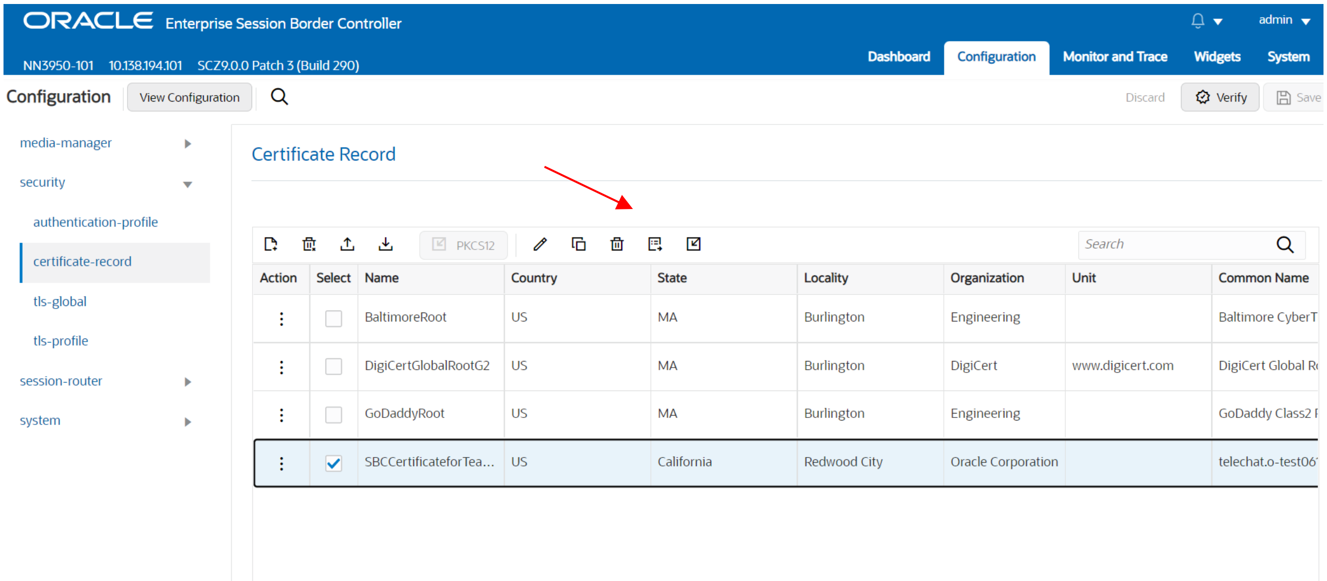
Do you want to activate the configuration?

Confirm Cancel

Generate Certificate Signing Request

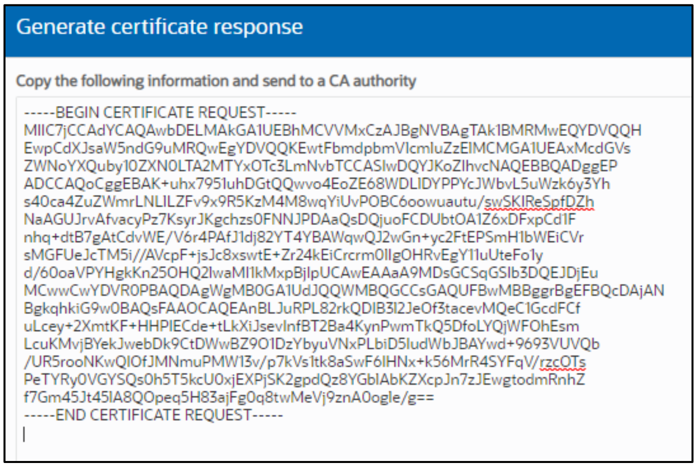
Now that the SBC's certificate has been configured, create a certificate signing request for the SBC's end entity only. **This is not required for any of the Root CA or intermidiate certificates that have been created**.

On the certificate record page in the Oracle SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:



Certificate Record

Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
⋮	□	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberT
⋮	□	DigiCertGlobalRootG2	US	MA	Burlington	DigiCert	www.digicert.com	DigiCert Global R
⋮	□	GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 I
⋮	☑	SBCCertificateforTea...	US	California	Redwood City	Oracle Corporation		telechat.o-test06



Generate certificate response

Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwbDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEIMCMGA1UEAxMcdGVs
ZWNoYXQuby10ZXN0LTA2MTYxOTc3LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAK+uhx7951uhDGtQQwvo4EoZE68WDLIDYPPYcJWbvL5uWzk6y3Yh
s40ca4ZuZWmrLNLILZFv9x9R5KzM4M8wqYiUvPOBC6oowuautu/swSKIReSpfDZh
NaAGUJrvAfvacyPz7KsyrJKgchzs0FNNJPDAaQsDQjuoFCDUbtOA1Z6xDFxpCd1F
nhq+dtB7gAtCdvWE/V6r4PAfJ1dj82YT4YBAWqwQJ2wGn+yc2FtEPSmH1bWEiCVr
sMGFUeJcTM5i//AVcpF+jsJc8xswtE+Zr24kEiCrcrm0IIgOHRvEgY11uUteFo1y
d/60oaVPYHgkKn25OHQ2lwaMI1kMxpBjlpUCAwEAAaA9MDsGCSqGSIb3DQEJDjEu
MCwwCwYDVR0PBAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAN
BgkqhkiG9w0BAQsFAAOCAQEAnBLJuRPL82rkQDIB3I2JeOf3tacevMQeC1GcdFCf
uLcey+2XmtKF+HHPIECde+tLkXiJsevInfBT2Ba4KynPwmTkQ5DfoLYQjWFOhEsm
LcuKMvjBYekJwebDk9CtDWwBZ9O1DzYbyuVNxPLbiD5ludWbJBAYwd+9693VUVQb
/UR5rooNKwQIOfJMNmuPMW13v/p7kVs1tk8aSwF6IHNx+k56MrR4SYFqV/rzcOTs
PeTYRy0VGYSQs0h5T5kcU0xjEXPjSK2gpdQz8YGbIAbKZXcpJn7zJEwgtodmRnhZ
f7Gm45Jt45IA8QOpeq5H83ajFg0q8twMeVj9znA0ogle/g==
-----END CERTIFICATE REQUEST-----
```

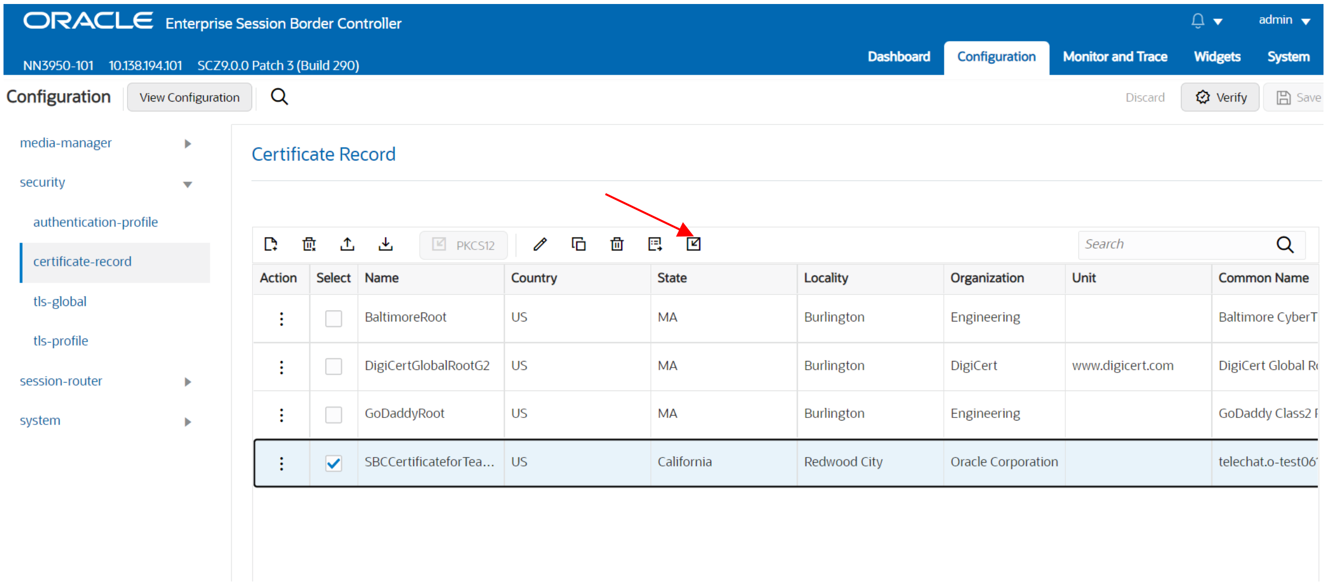
Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
Also note, at this point, **another save and activate is required** before you can import the certificates to each certificate record created above.

Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

Import Certificates to SBC

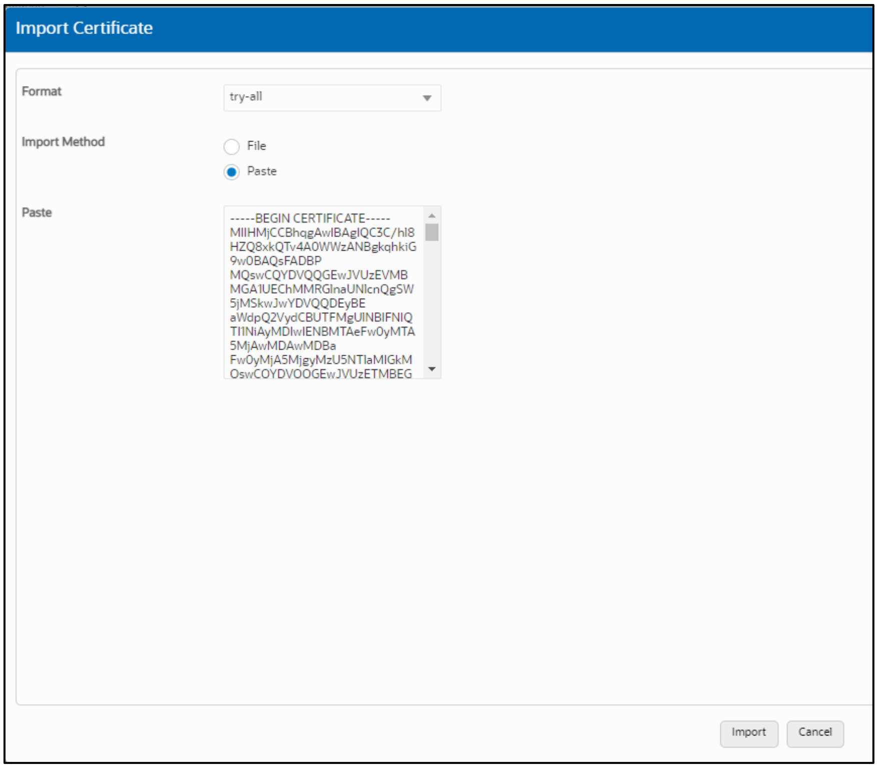
Once certificate signing request has been completed – import the signed certificate to the SBC.

Please note – all certificates including root and intermediate certificates are required to be imported to the SBC.
Once all certificates have been imported, issue a third **save/activate** from the WebGUI to complete the configuration of certificates on the Oracle SBC.



Certificate Record

Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
⋮	□	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberT
⋮	□	DigiCertGlobalRootG2	US	MA	Burlington	DigiCert	www.digicert.com	DigiCert Global R
⋮	□	GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 F
⋮	☑	SBCCertificateforTea...	US	California	Redwood City	Oracle Corporation		telechat.o-test06



Import Certificate

Format: try-all

Import Method: ○ File ● Paste

Paste:

```
-----BEGIN CERTIFICATE-----
MIIHMjCCBhqgAwIBAgIQC3C/hI8
HZQ8xkQTv4A0WWzANBgkqhkiG
9w0BAQsFADBP
MQswCQYDVQQGEwJVUzEVMB
MGA1UEChMMRGlnaUNlcnQgSW
5jMSkwJwYDVQQDEyBE
aWdpQ2VydCBUTFMgUlNBIFNIQ
TI1NiAyMDIwIENBMTAeFw0yMTA
5MjAwMDAwMDBa
Fw0yMjA5MjgyMzU5NTlaMIGkM
OswCOYDVOOGEwJVUzETMBEG
```

- Once pasted in the text box, select Import at the bottom, then **save and activate** your configuration.

Repeat these steps to import all the root and intermediate CA certificates into the SBC:

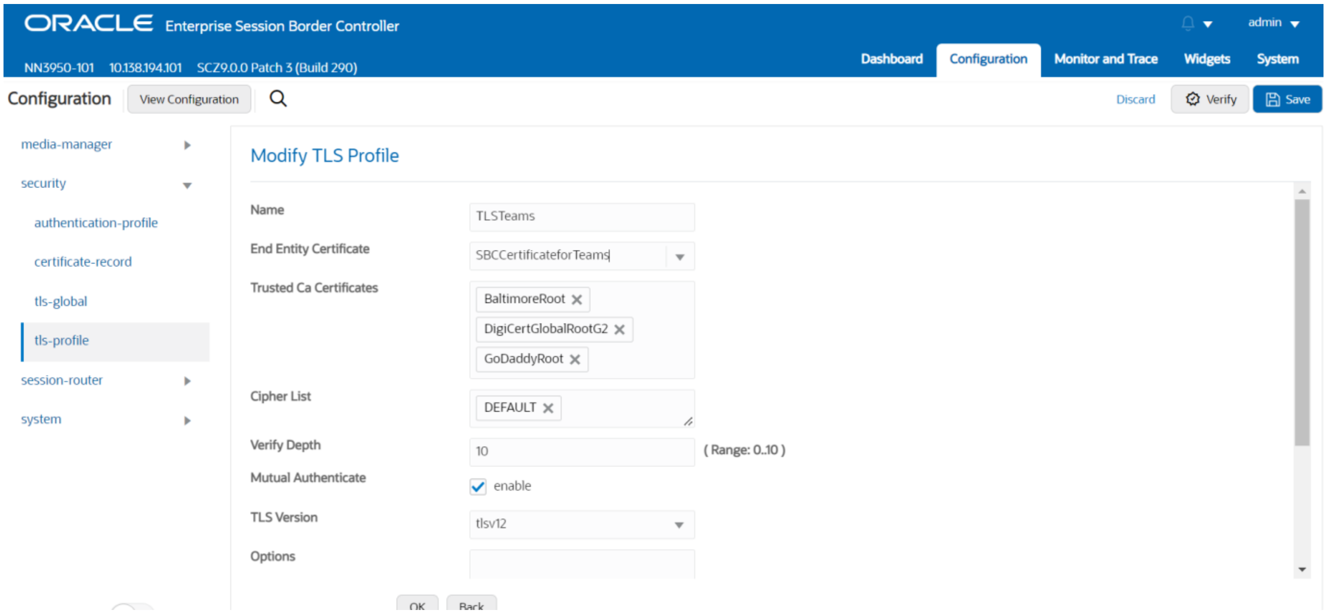
6.10.TLS Profile

TLS profile configuration on the SBC allows for specific certificates to be assigned.

GUI Path: security/tls-profile

ACLI Path: config t→security→tls-profile

- Click Add, use the example below to configure



Modify TLS Profile

Name: TLSTeams

End Entity Certificate: SBCCertificateforTeams

Trusted Ca Certificates: BaltimoreRoot, DigiCertGlobalRootG2, GoDaddyRoot

Cipher List: DEFAULT

Verify Depth: 10 (Range: 0..10)

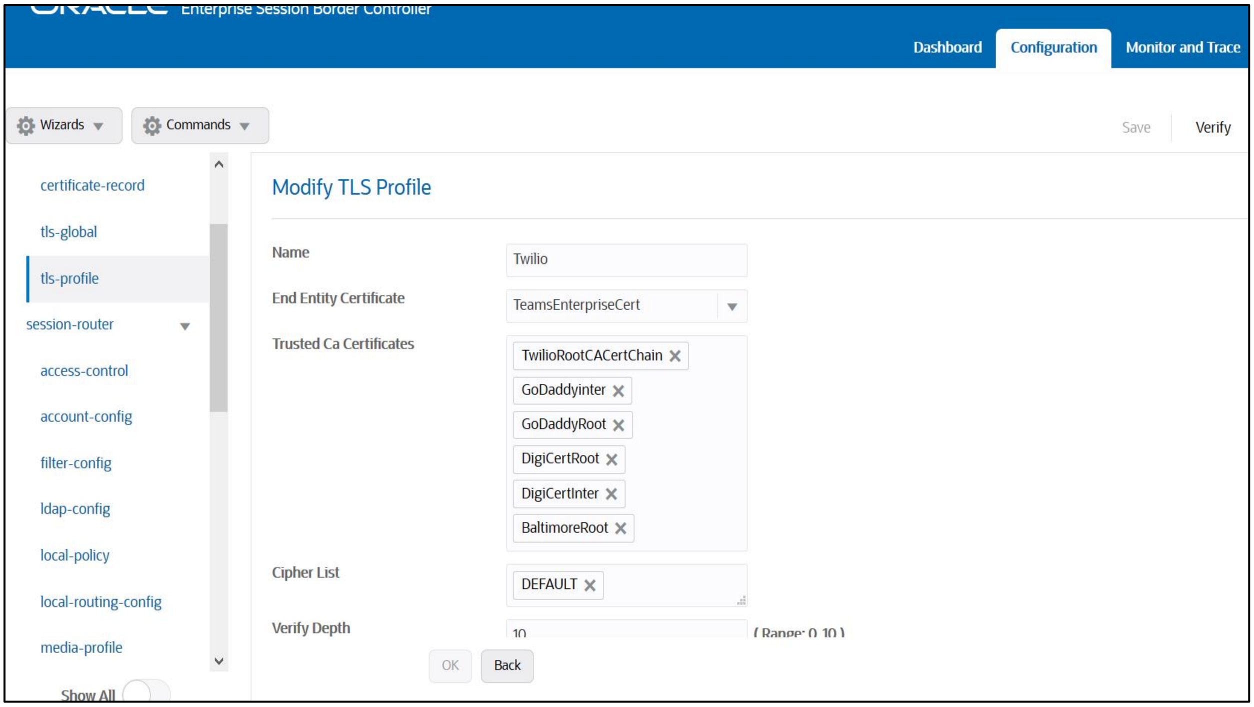
Mutual Authenticate: ☑ enable

TLS Version: tlsv12

Options:

- Select OK at the bottom

Similarly, configure the TLS profile shown below for the Twilio Elastic SIP Trunk side:



Modify TLS Profile

Name: Twilio

End Entity Certificate: TeamsEnterpriseCert

Trusted Ca Certificates: TwilioRootCACertChain, GoDaddyinter, GoDaddyRoot, DigiCertRoot, DigiCertInter, BaltimoreRoot

Cipher List: DEFAULT

Verify Depth: 10 (Range: 0..10)

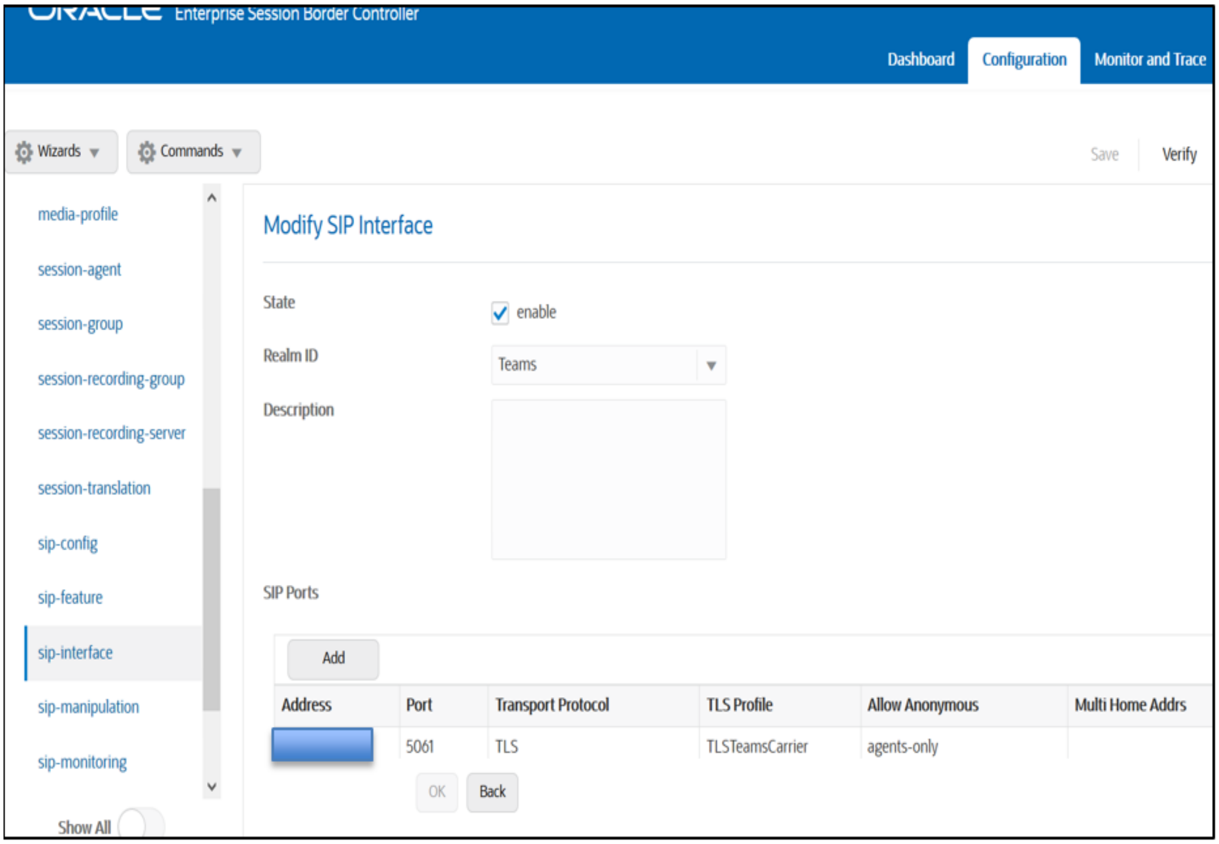
6.11. Configure SIP Interfaces

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

Please configure the below settings under the sip-interface.

- 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.

Below is the sip-interface Configured for Teams side.



Modify SIP Interface

State ☑ enable

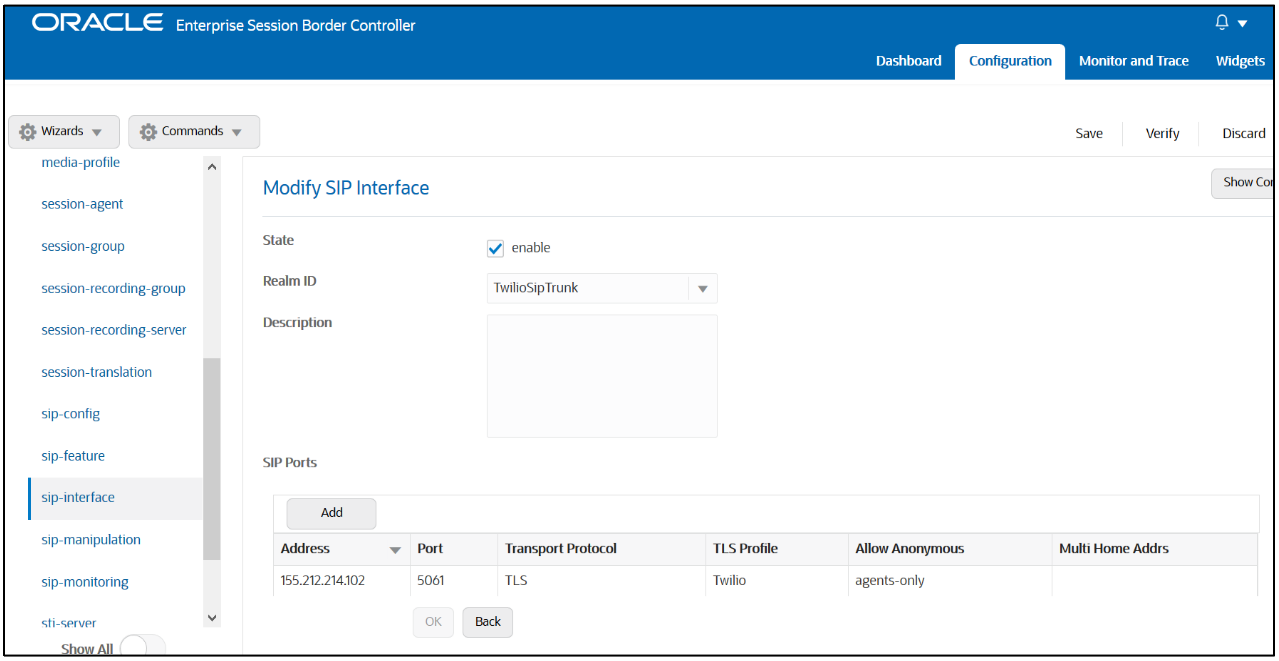
Realm ID: Teams

Description

SIP Ports

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

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



Modify SIP Interface

State ☑ enable

Realm ID TwilioSipTrunk

Description

SIP Ports

Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
155.212.214.102	5061	TLS	Twilio	agents-only	

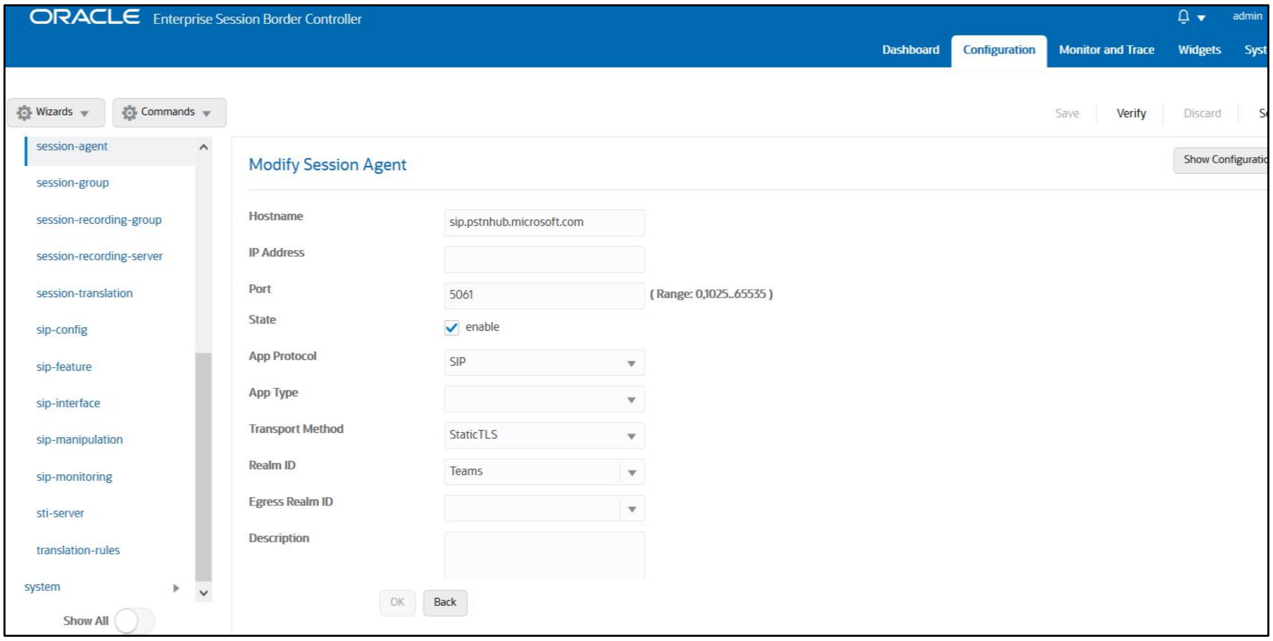
Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

6.12. Configure session-agent

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

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

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



Modify Session Agent

Hostname: sip.pstnhub.microsoft.com

IP Address:

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

State: ☑ enable

App Protocol: SIP

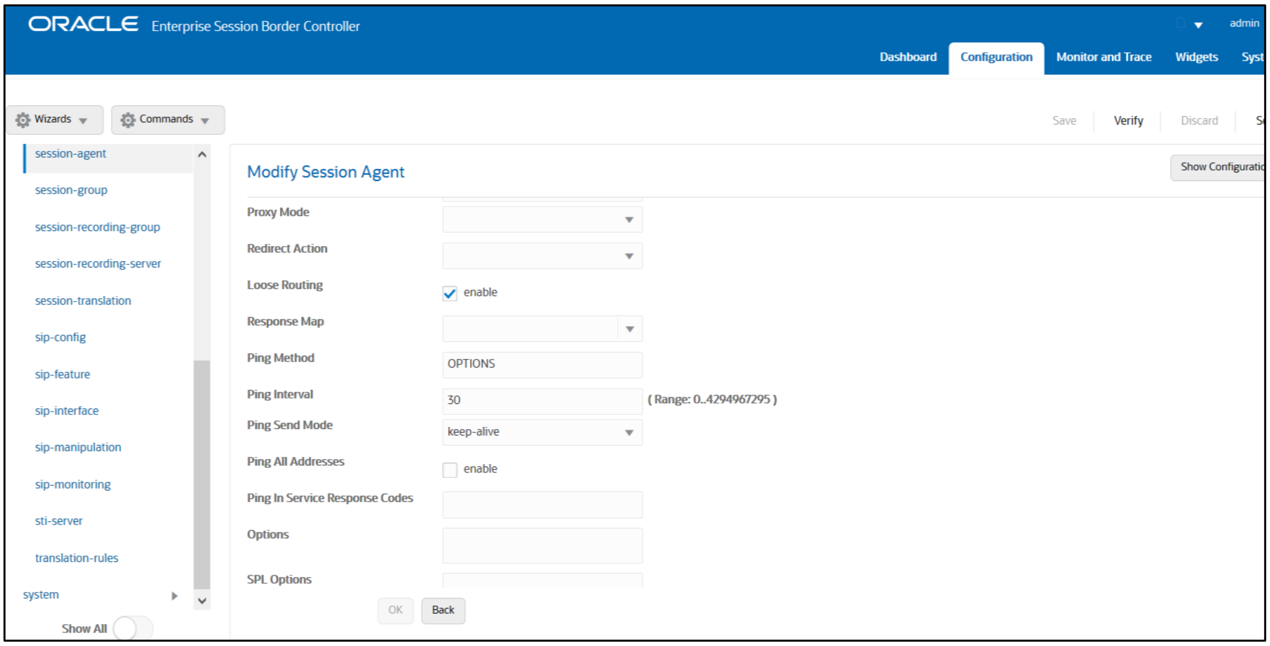
App Type:

Transport Method: StaticTLS

Realm ID: Teams

Egress Realm ID:

Description:



Modify Session Agent

Proxy Mode:

Redirect Action:

Loose Routing: ☑ enable

Response Map:

Ping Method: OPTIONS

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

Ping Send Mode: keep-alive

Ping All Addresses: ☐ enable

Ping In Service Response Codes:

Options:

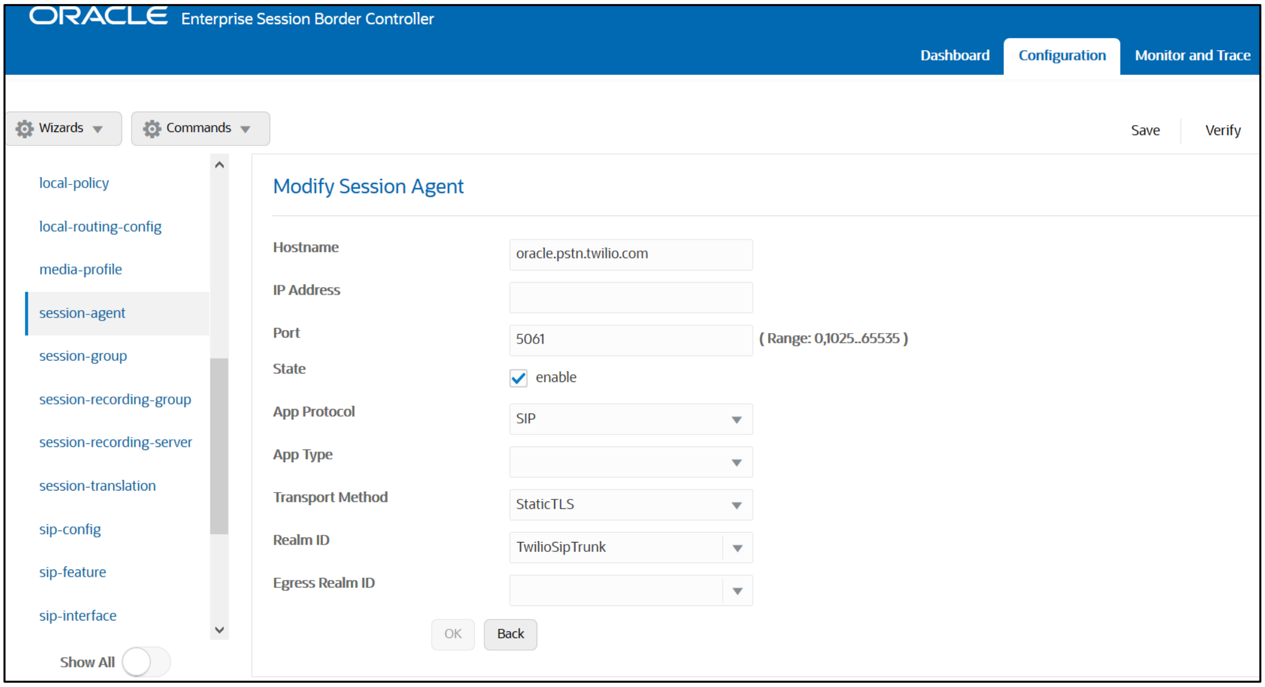
SPL Options:

Follow above steps to create 2 more sessions for:

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

Similarly, configure the session-agents for the Twilio Elastic SIP Trunk as below

- 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”



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	TwilioSipTrunk
Egress Realm ID	

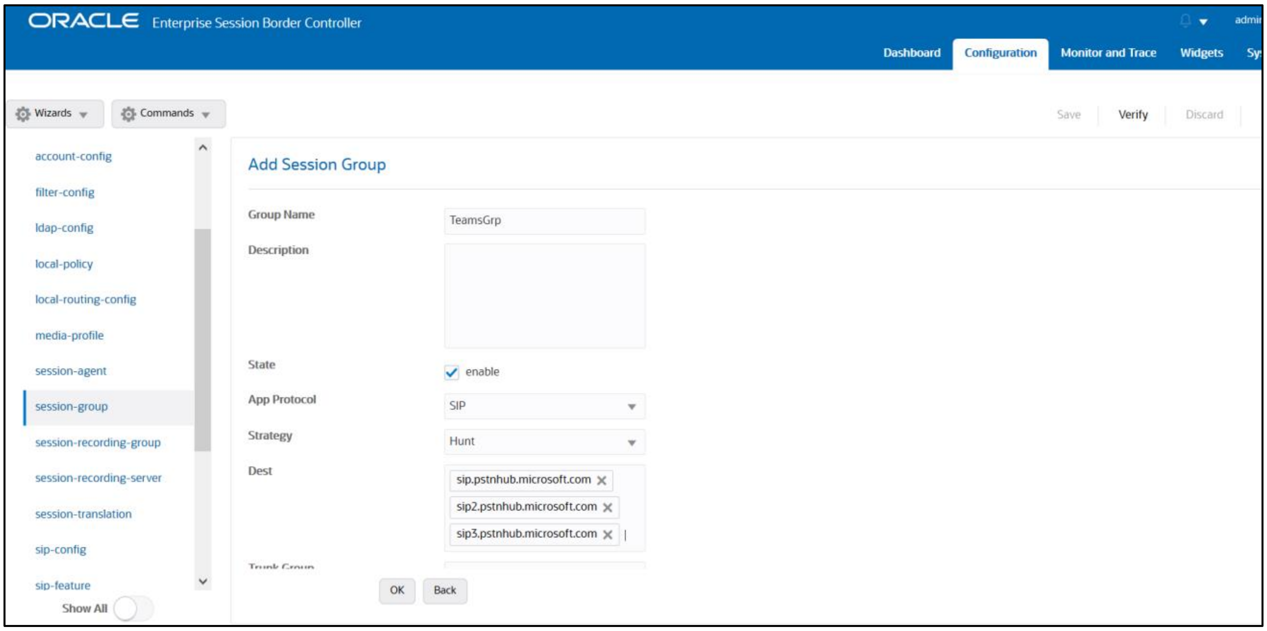
****NOTE: Connection to Twilio Elastic SIP Trunking is available in multiple geographic edge locations. If you wish to manually connect to a specific geographic edge location that is closest to the location of your communications infrastructure, you may do so by pointing your communications infrastructure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

6.13. Configure session-agent group

A session agent group allows the SBC to create a load balancing model.
Go to Session-Router->Session-Group. Please configure the following group for Teams Session Agents



Add Session Group

Group Name: TeamsGrp

Description:

State: ☑ enable

App Protocol: SIP

Strategy: Hunt

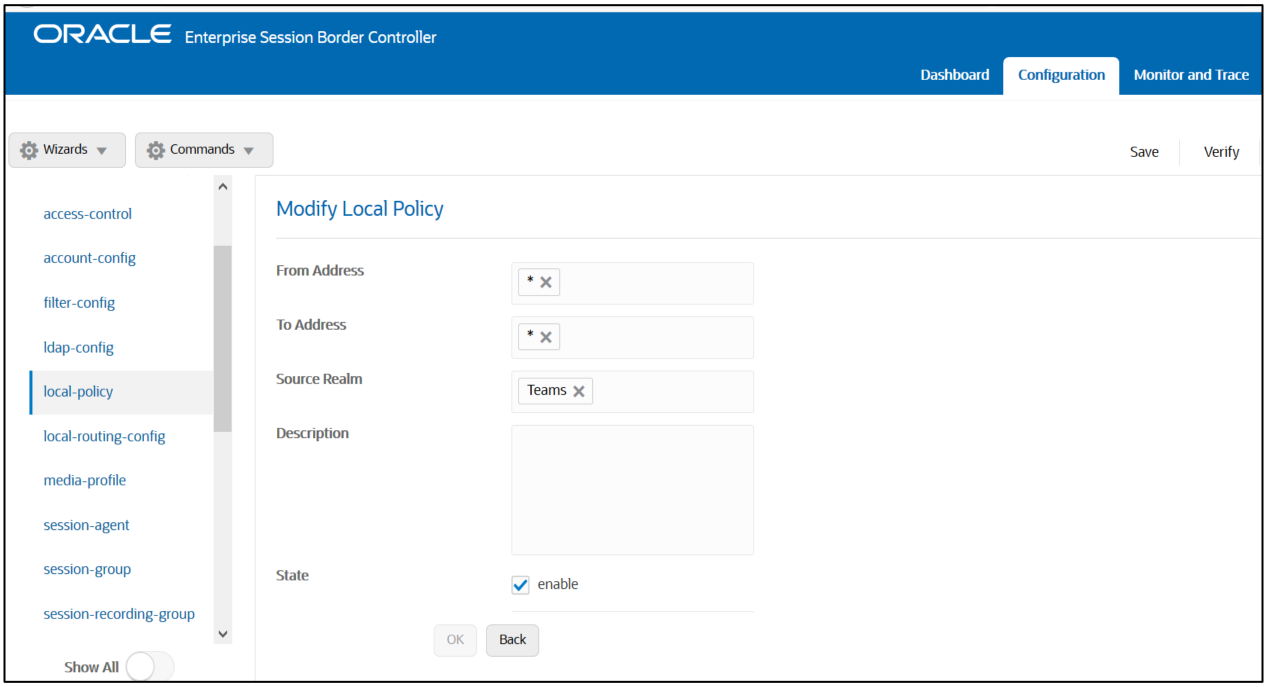
Dest: sip.pstnhub.microsoft.com
sip2.pstnhub.microsoft.com
sip3.pstnhub.microsoft.com

Trunk Group

6.14. 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 Teams side to Twilio side, Use the below local –policy



Modify Local Policy

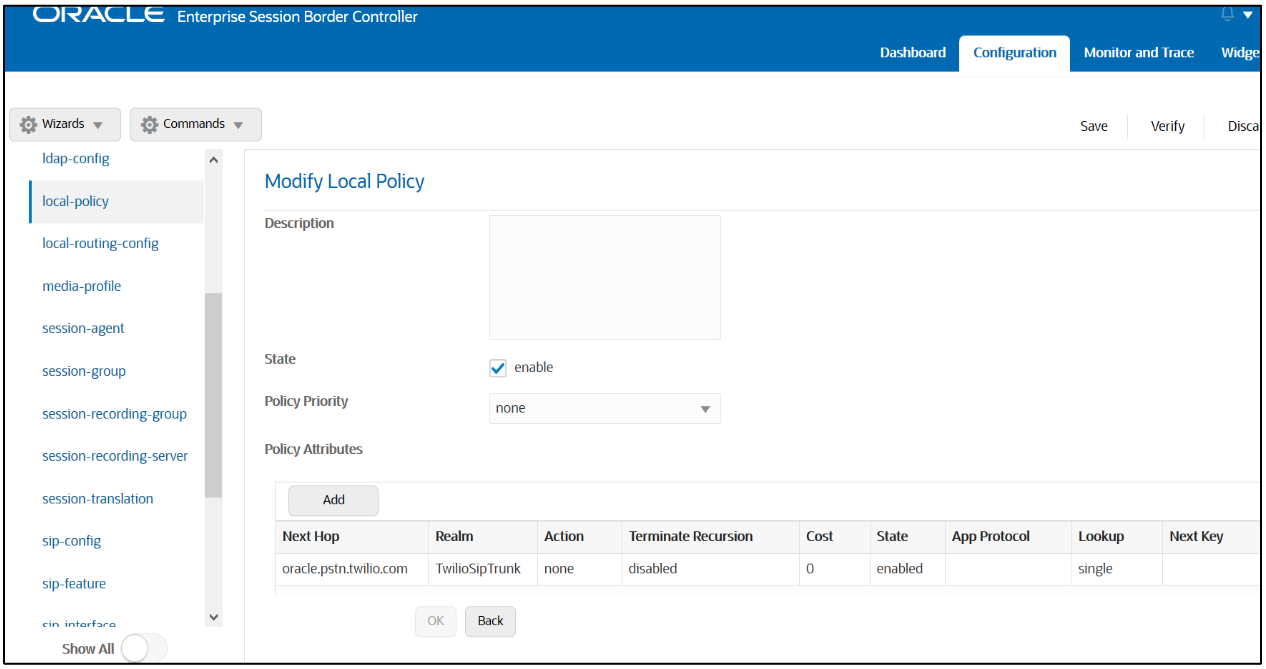
From Address: *

To Address: *

Source Realm: Teams

Description:

State: ☑ enable



Modify Local Policy

Description:

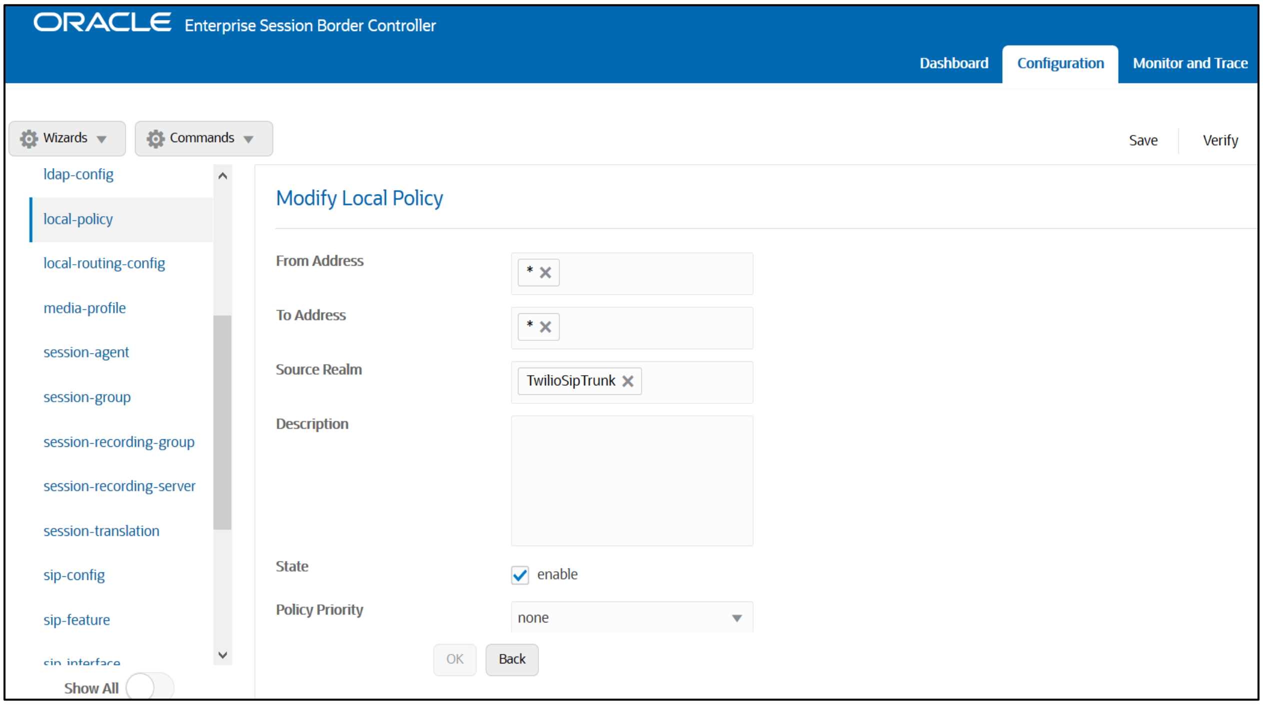
State: ☑ enable

Policy Priority: none

Policy Attributes

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

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



Modify Local Policy

From Address: *

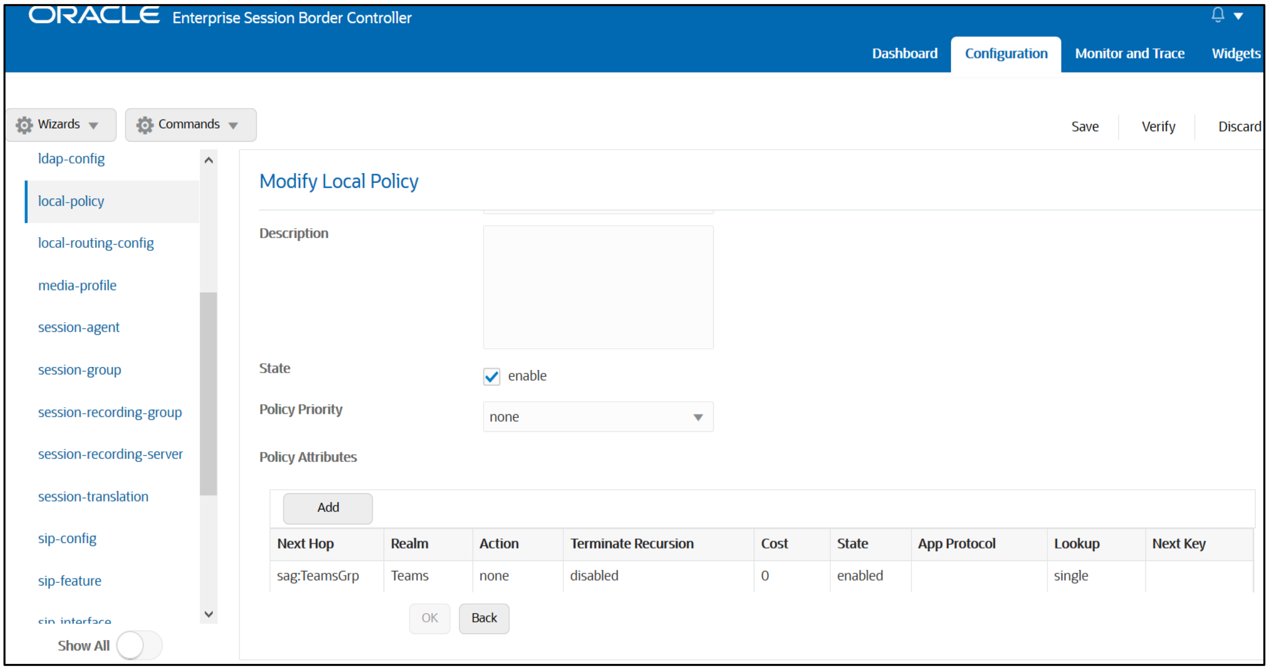
To Address: *

Source Realm: TwilioSipTrunk

Description:

State: ☑ enable

Policy Priority: none



Modify Local Policy

Description:

State: ☑ enable

Policy Priority: none

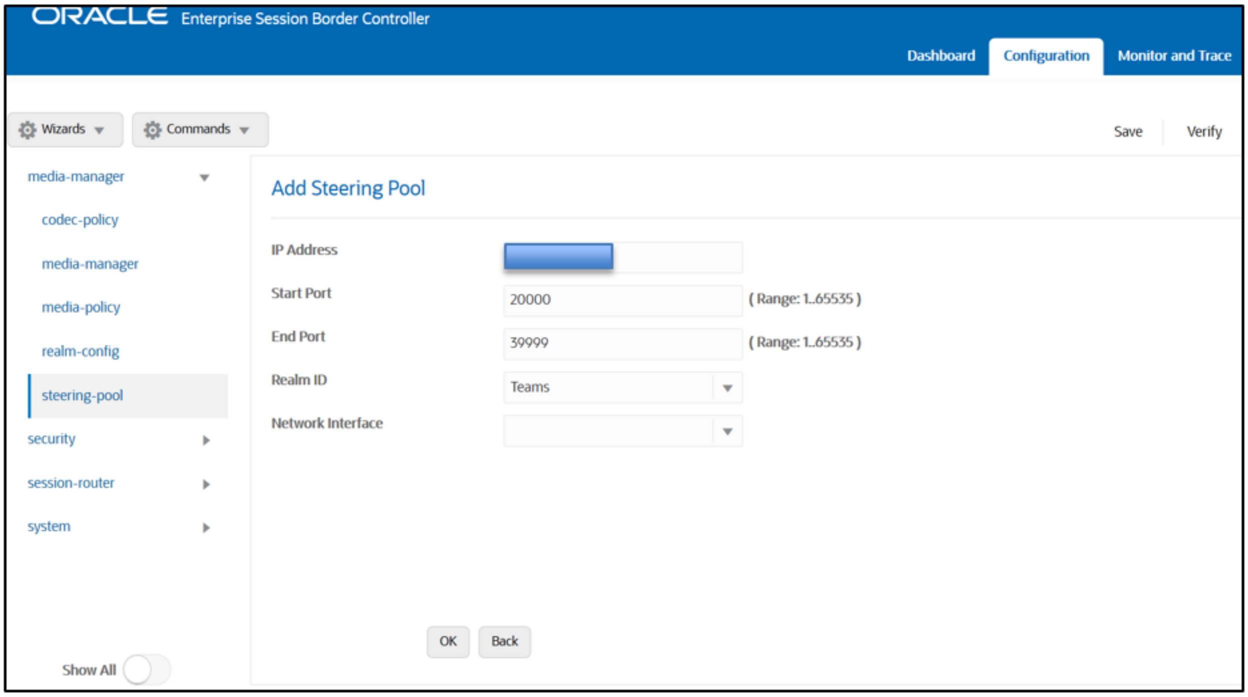
Policy Attributes

Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
sag:TeamsGrp	Teams	none	disabled	0	enabled		single	

6.15. Configure steering-pool

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

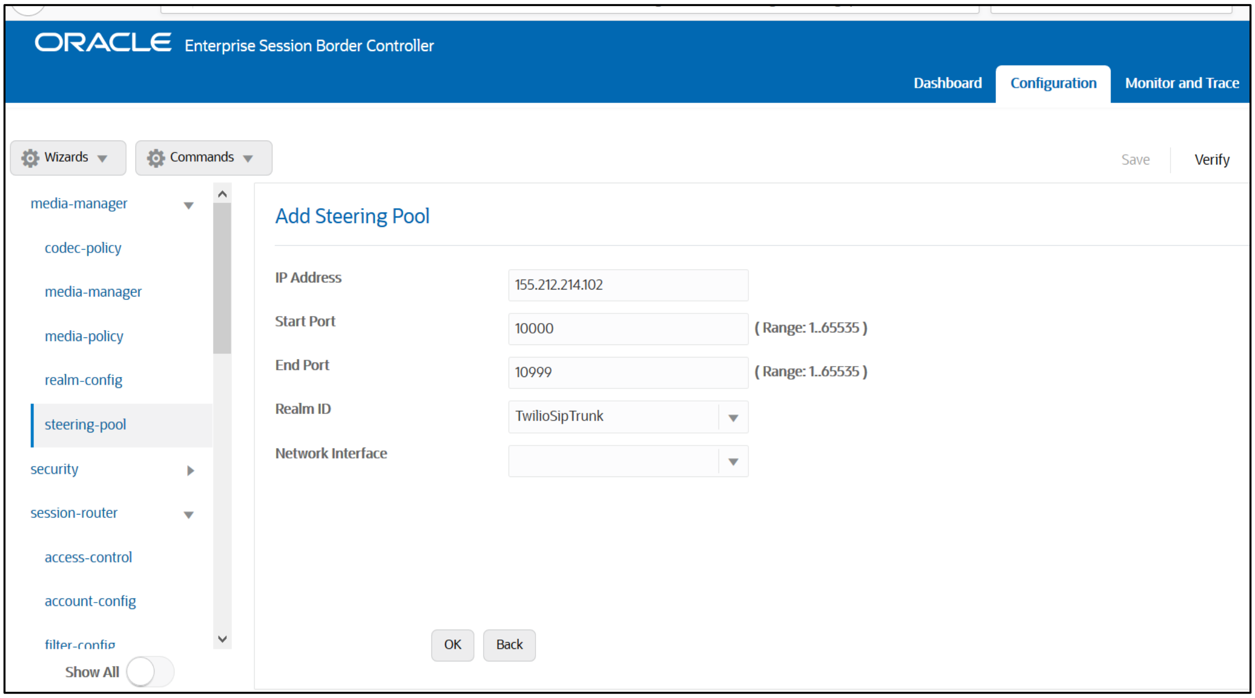
Teams side steering pool.



Add Steering Pool

IP Address
Start Port 20000 (Range: 1..65535)
End Port 39999 (Range: 1..65535)
Realm ID Teams
Network Interface

Twilio side steering pool.



Add Steering Pool

IP Address 155.212.214.102
Start Port 10000 (Range: 1..65535)
End Port 10999 (Range: 1..65535)
Realm ID TwilioSipTrunk
Network Interface

6.16. Configure sip-manipulation

To simplify the ORACLE SBC sip manipulation, from GA Release SCZ830m1p7 contains three additional SBC configuration parameters which are not found in prior releases.

The purpose of these three parameters is to replace the majority of the sip manipulation rules required to be configured in the ORACLE SBC in order to properly interface with Microsoft Teams Direct Routing.

The first two parameters are found under the **realm-config**, and would be enabled in realms facing Microsoft Teams.

They are **Teams FQDN in URI** and **SDP inactive only**.
The detailed description is given below for each config parameter.

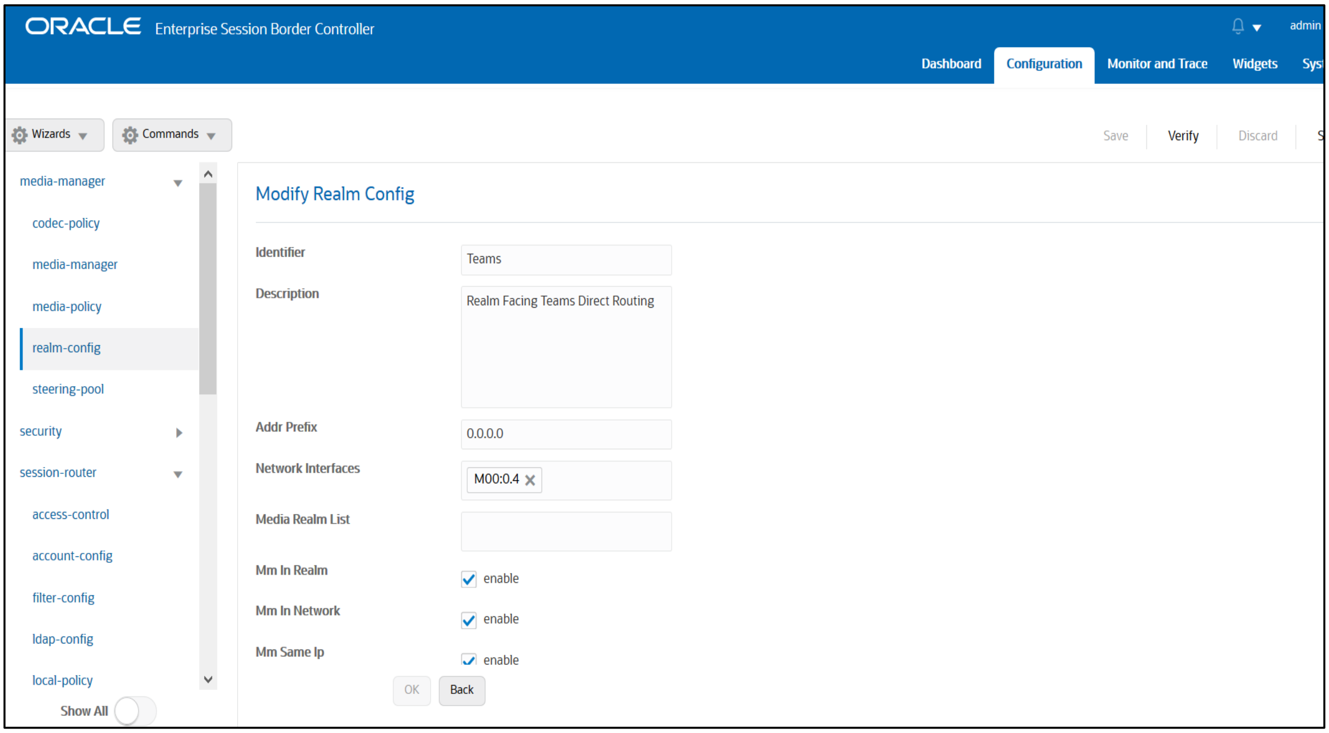
Teams FQDN in URI:

When enabled, this parameter takes the FQDN configured under hostname of the network interface, and inserts that into the Contact and FROM headers of Invites generated by the SBC towards Teams. This also adds a new “X-MS-SBC” Header to both Invite and OPTIONS Requests, which takes the place of the User-Agent header currently being added via Sip Manipulation. Lastly, SBC will add a Contact Header to outgoing SIP Options Pings, also containing the FQDN of the SBC listed under the hostname field of the network interface, and with the Contact Header added to OPTION Requests generated by the SBC, Record Route is no longer required.

SDP inactive only:

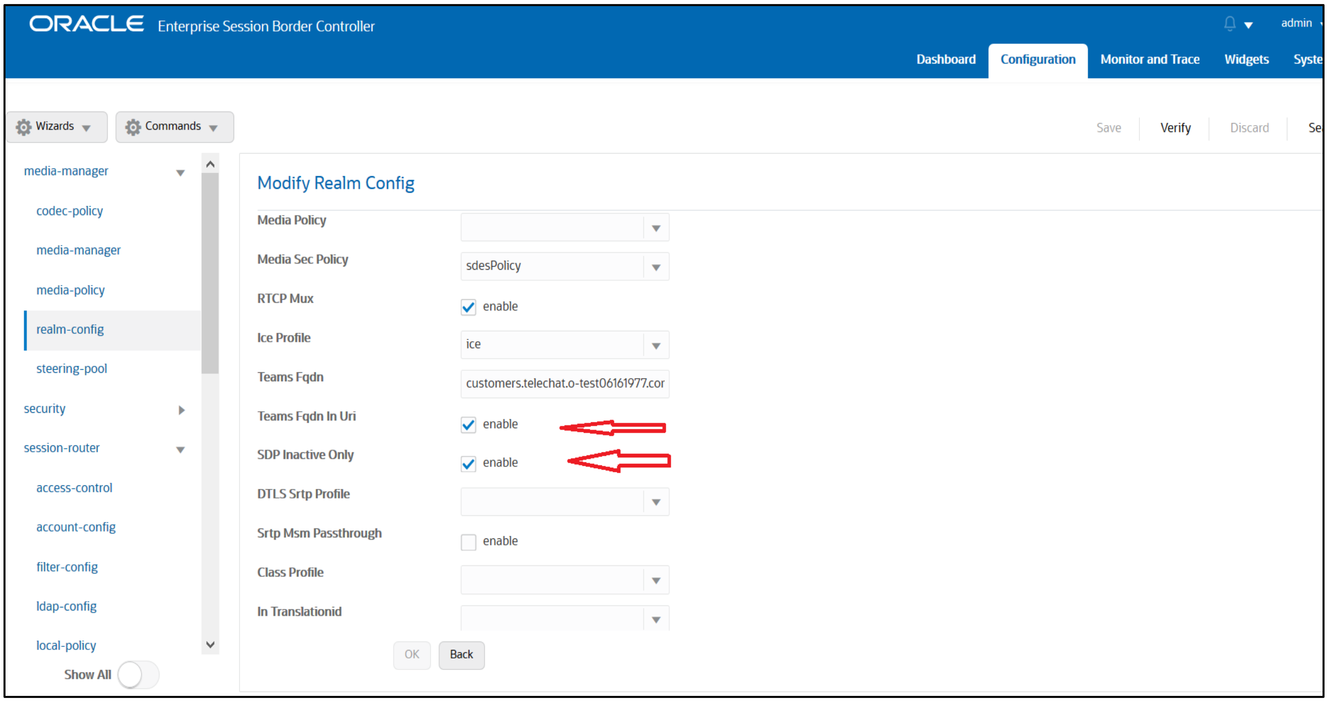
When enabled on Teams facing realm(s), this will modify the following SDP attributes in both requests and responses to and from Microsoft Teams

Message Type	Match Value	New Value
request	inactive	sendonly
reply	inactive	recvonly
request	sendonly	inactive
reply	recvonly	inactive



Modify Realm Config

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



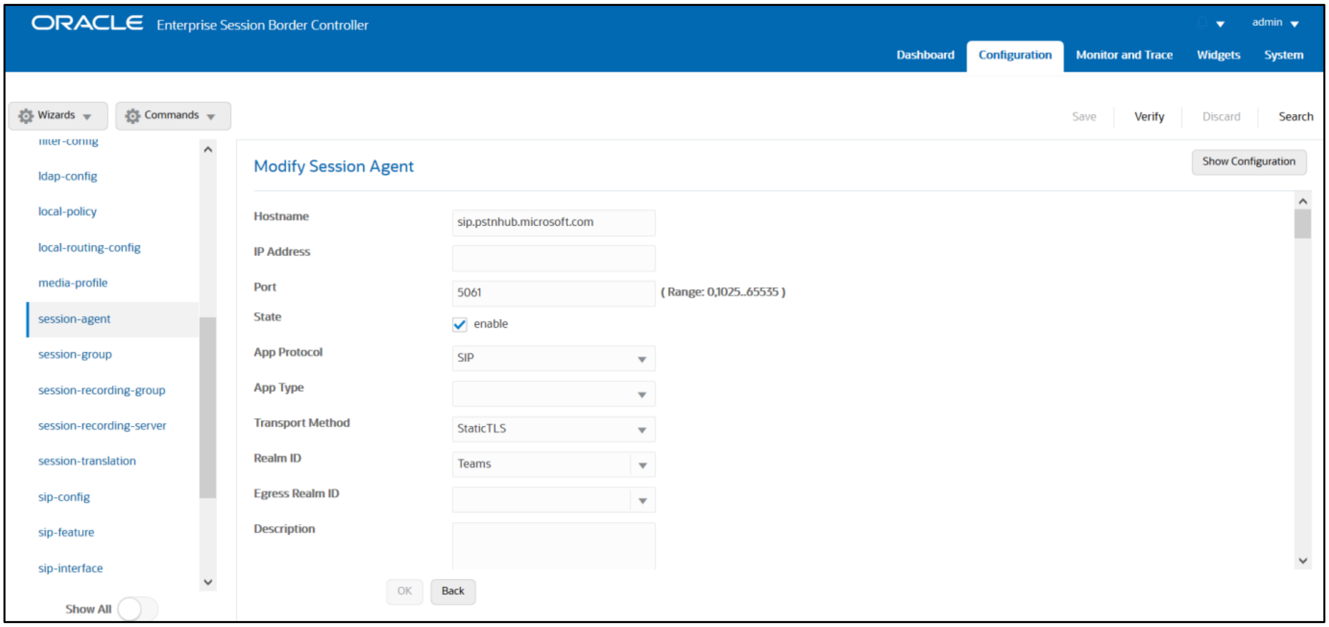
Modify Realm Config

Media Policy	
Media Sec Policy	sdesPolicy
RTCP Mux	☑ enable
Ice Profile	ice
Teams Fqdn	customers.telechat.o-test06161977.cor
Teams Fqdn In Uri	☑ enable
SDP Inactive Only	☑ enable
DTLS Srtp Profile	
Srtp Msm Passthrough	□ enable
Class Profile	
In Translationid	

The third parameter is found under the **Session agent** configuration element and will be enabled on all three session agents configured for Microsoft Teams. The parameter name is **Ping response**.

Ping Response:

When enabled, the SBC responds with a 200 OK to all Sip Options Pings it receives from trusted agents. This takes the place of the current Sip Manipulation, RespondOptions.



Modify Session Agent

Hostname: sip.pstnhub.microsoft.com

IP Address:

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

State: ☑ enable

App Protocol: SIP

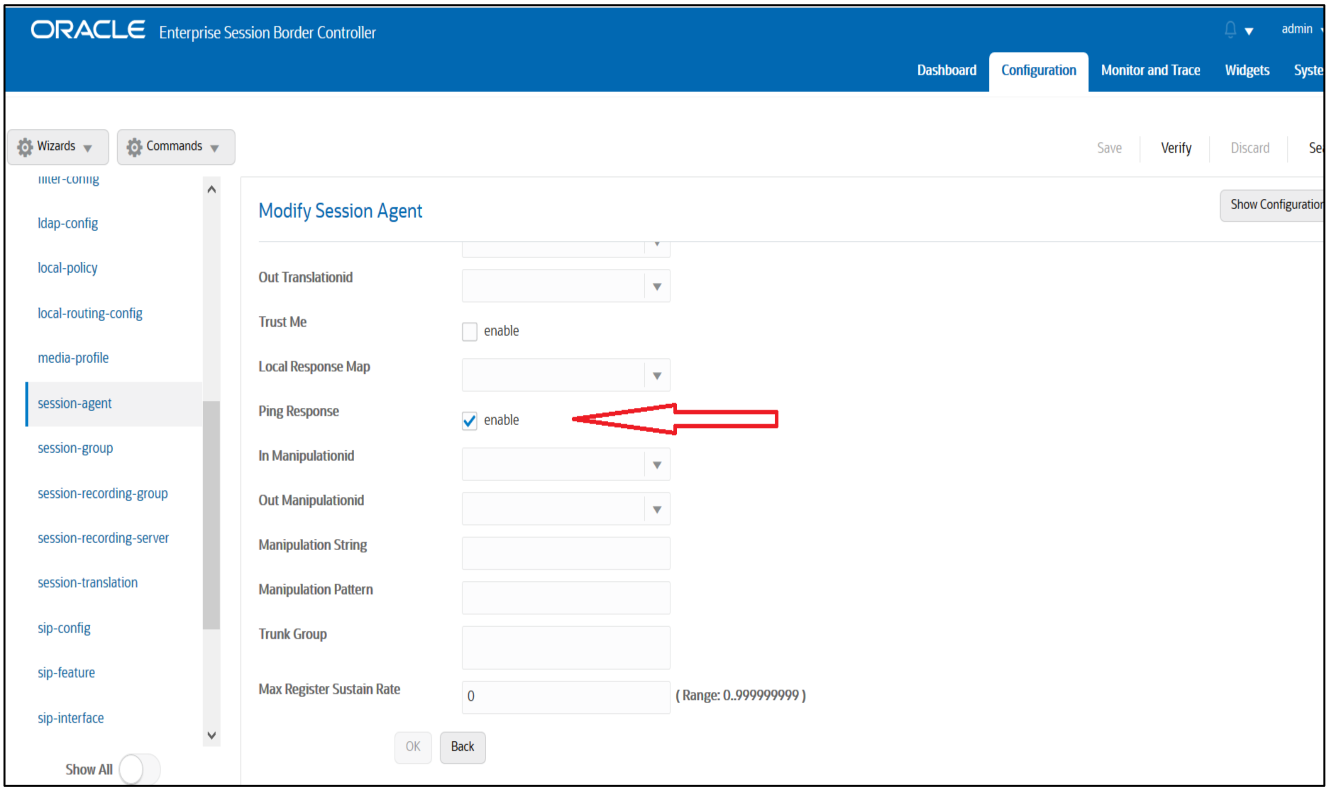
App Type:

Transport Method: StaticTLS

Realm ID: Teams

Egress Realm ID:

Description:



Modify Session Agent

Out Translationid:

Trust Me: □ enable

Local Response Map:

Ping Response: ☑ enable

In Manipulationid:

Out Manipulationid:

Manipulation String:

Manipulation Pattern:

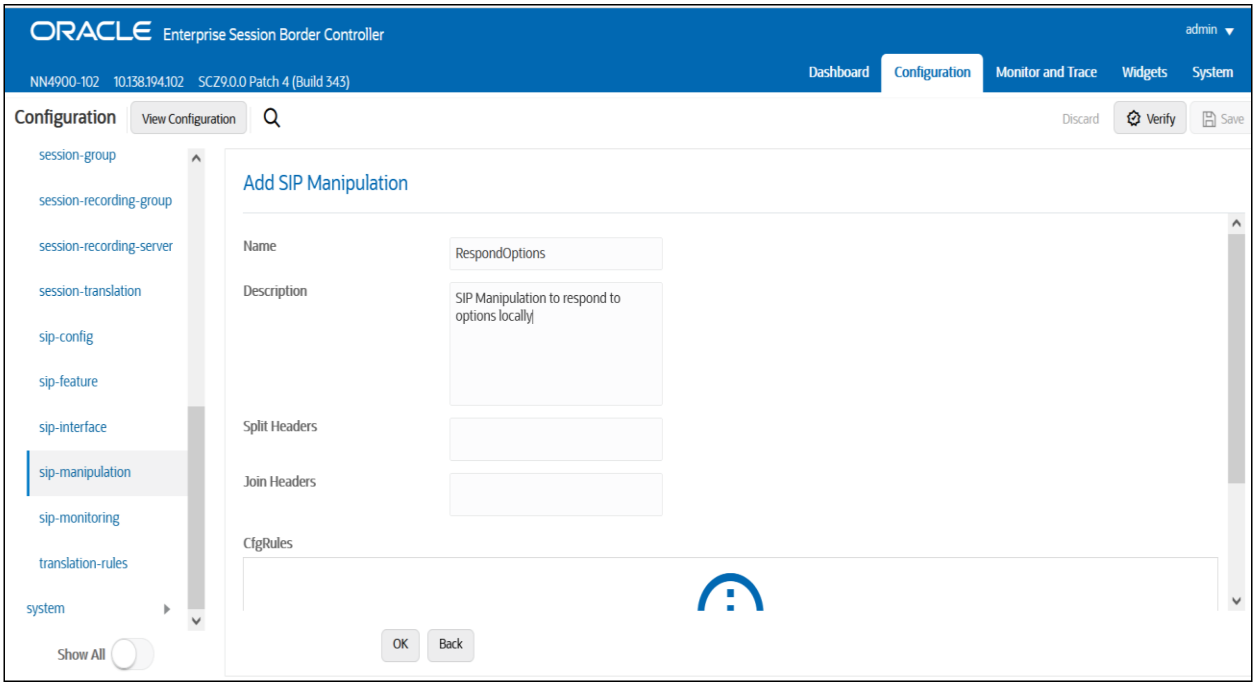
Trunk Group:

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

Respond to Options:

To ensure the SBC generates a 200OK response to SIP Options messages received from Teams, we'll configure the following sip-manipulation rule

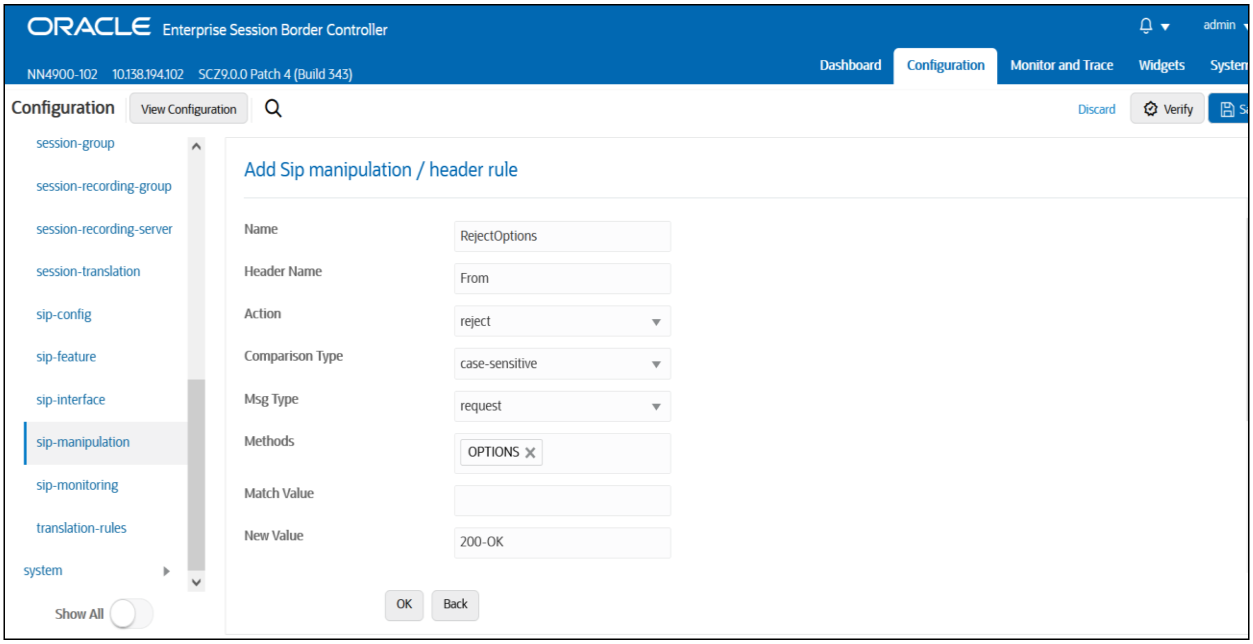
Go to GUI Path: session router/sip manipulation and add the following:



Add SIP Manipulation

Name	RespondOptions
Description	SIP Manipulation to respond to options locally
Split Headers	
Join Headers	
CfgRules	

Next, under CfgRules, select "header rule" in the "Add" drop down menu:



Add Sip manipulation / header rule

Name	RejectOptions
Header Name	From
Action	reject
Comparison Type	case-sensitive
Msg Type	request
Methods	OPTIONS
Match Value	
New Value	200-OK

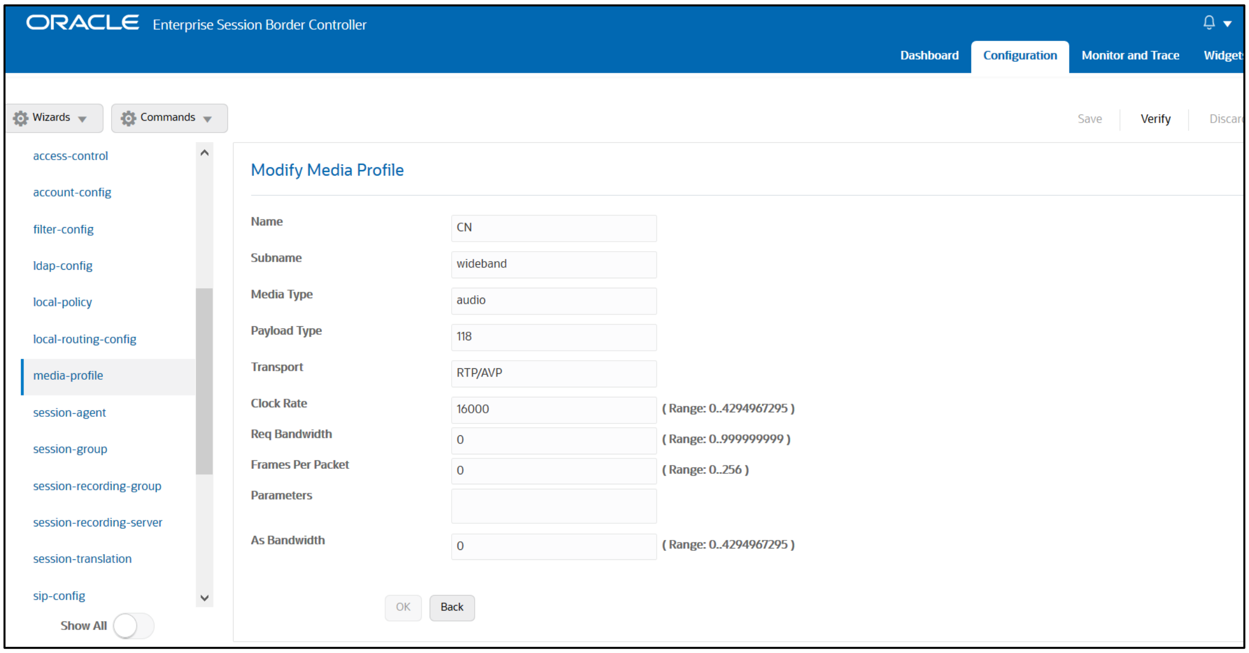
Click OK at the bottom when finished.

6.17. Configure Media Profile and Codec Policy

The Oracle Session Border Controller (SBC) uses codec policies to describe how to manipulate SDP messages as they cross the SBC. The SBC bases its decision to transcode a call on codec policy configuration and the SDP. Each codec policy specifies a set of rules to be used for determining what codecs are retained, removed, and how they are ordered within SDP.

Note: this is an optional config – configure codec policy only if deemed required

SILK & CN offered by Microsoft teams are using a payload type which is different than usual. Configure the media-profile as shown below,
Go to Session-Router->Media-profile



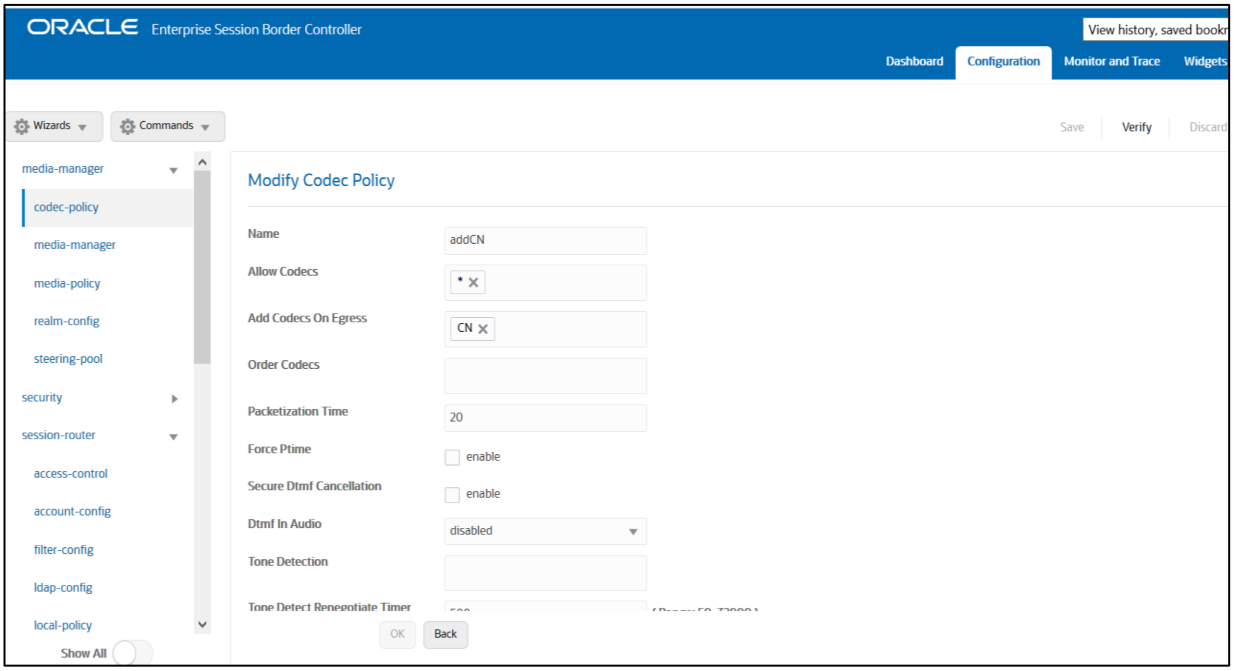
Modify Media Profile

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

Configure media profiles similarly, for silk codec also as given below.

Parameters	SILK-1	SILK-2
Subname	narrowband	wideband
Payload-Type	103	104
Clock-rate	8000	16000

After creating media profile, create codec-policy, addCN, to add comfort noise towards Teams.
Go to media manager ---- codec policy



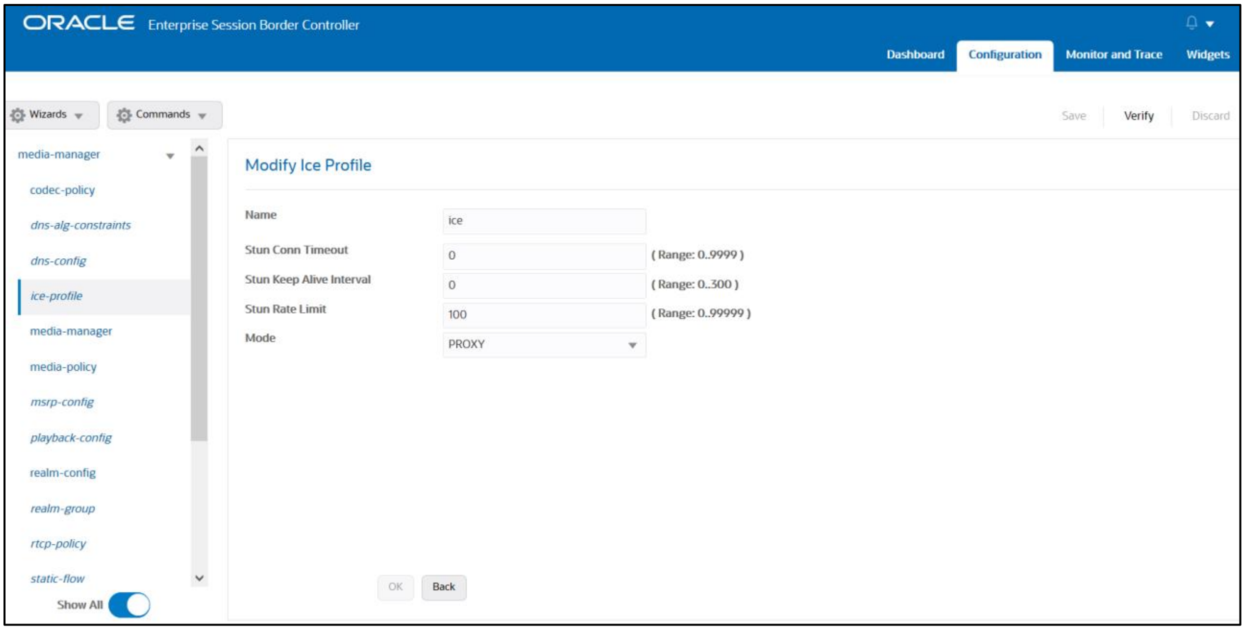
Modify Codec Policy

Name	addCN
Allow Codecs	* ✕
Add Codecs On Egress	CN ✕
Order Codecs	
Packetization Time	20
Force Ptime	□ enable
Secure Dtmf Cancellation	□ enable
Dtmf In Audio	disabled
Tone Detection	
Tone Detect Renegotiate Timer	

Apply this codec policy on the Teams realm

6.18. Configure ice profile

SBC supports ICE-Lite. This configuration is only required to support Teams media-bypass.
Configure the following ice profile and apply it on the realm towards Teams.
Go to media-manager->ice-profile. **Note: This config is required only for Media bypass model and its not needed for Non media bypass model.**

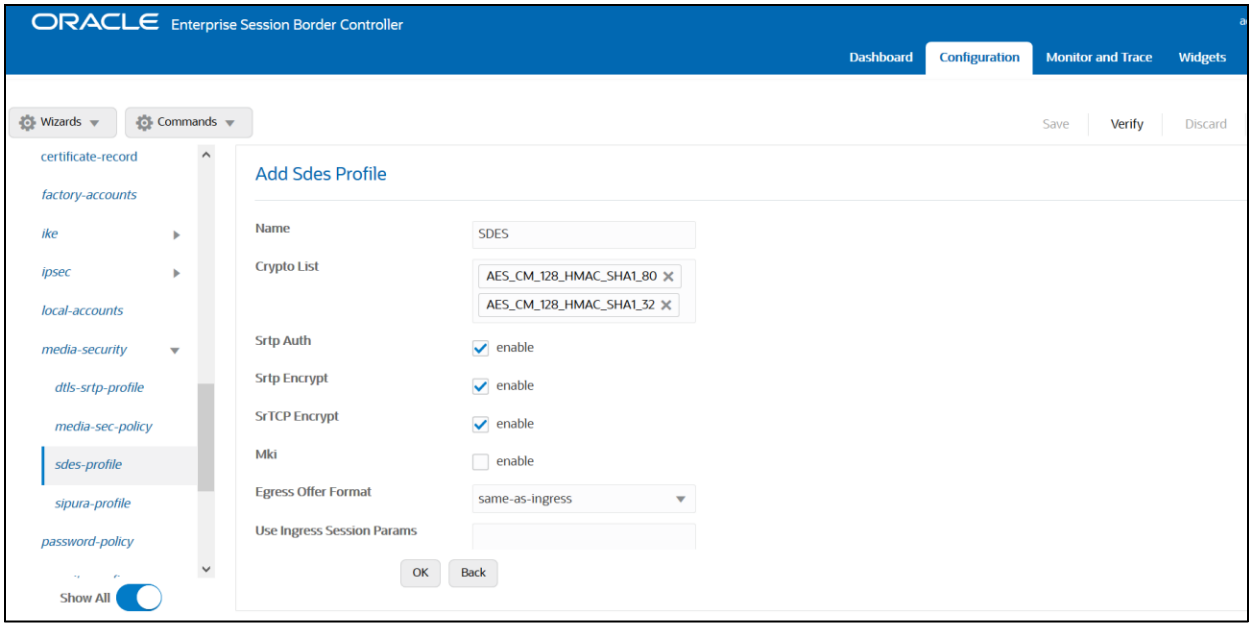


Modify Ice Profile

Name	ice	
Stun Conn Timeout	0	(Range: 0..9999)
Stun Keep Alive Interval	0	(Range: 0..300)
Stun Rate Limit	100	(Range: 0..99999)
Mode	PROXY	

6.19. 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

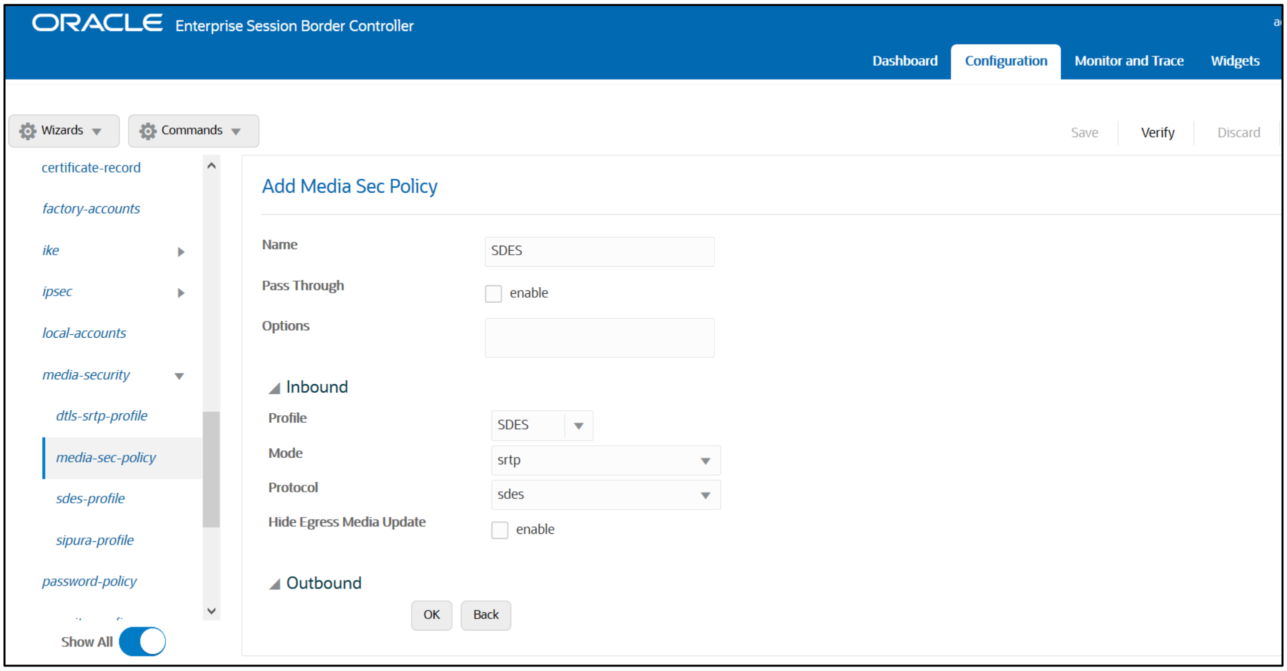
Mki: □ enable

Egress Offer Format: same-as-ingress

Use Ingress Session Params:

6.20. 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 both the Teams and Twilio Realm as they both use TLS/SRTP.



Add Media Sec Policy

Name: SDES

Pass Through: □ enable

Options:

Inbound

Profile: SDES

Mode: srtp

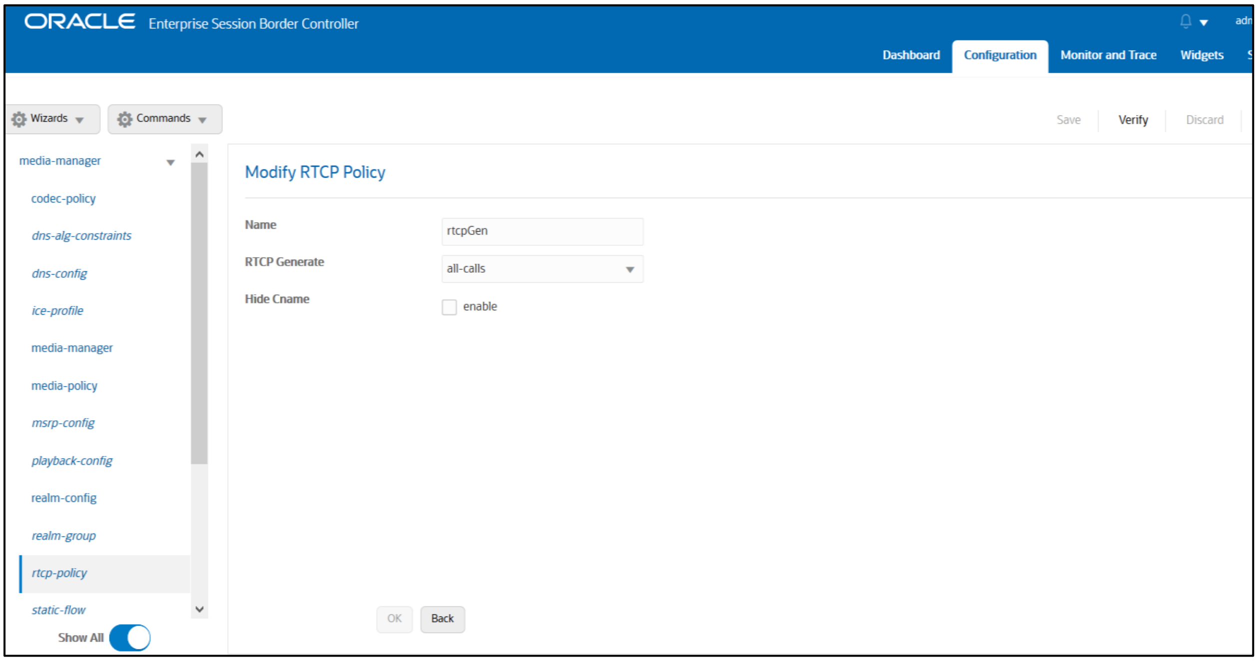
Protocol: sdes

Hide Egress Media Update: □ enable

Outbound

6.21. Configure RTCP Policy and RTCP Mux

The RTCP policy needs to be configured in order to generate RTCP reports towards Teams
Go to Media-manager->rtcp-policy to configure rtcp-policy.



Modify RTCP Policy

Name: rtcpGen

RTCP Generate: all-calls

Hide Cname: □ enable

Apply this RTCP policy on the Teams realm. Enable rtcp-mux also in the realm.
With this, SBC configuration is complete

7. 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.**

7.1. 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 Microsoft Teams Direct Routing 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 access to MSFT supported CA to sign certificate once CSR is generated by the SBC. A list of supported CA's can be found here. For Twilio side, list of supported CA's can be found here

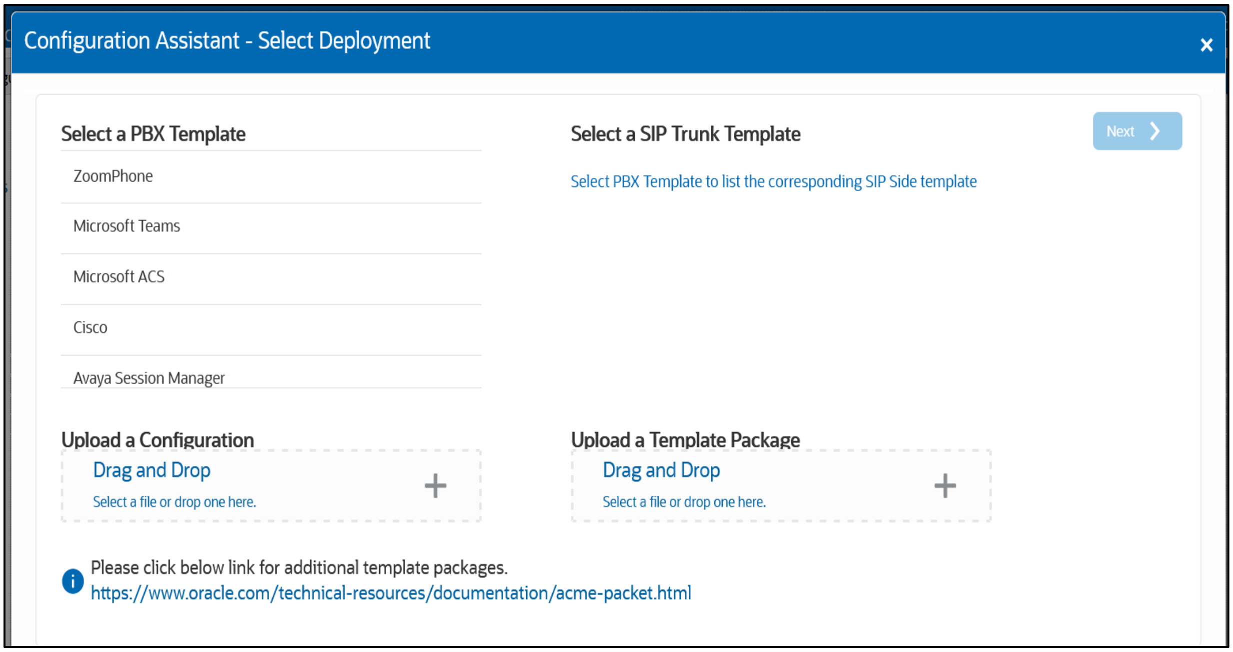
The following outline assumes you have established initial access to the SBC via console and completed the following steps:

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

7.2. Initial GUI Access

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

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



Configuration Assistant - Select Deployment

Select a PBX Template

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

Select a SIP Trunk Template

Select PBX Template to list the corresponding SIP Side template

Upload a Configuration

Drag and Drop

Select a file or drop one here.

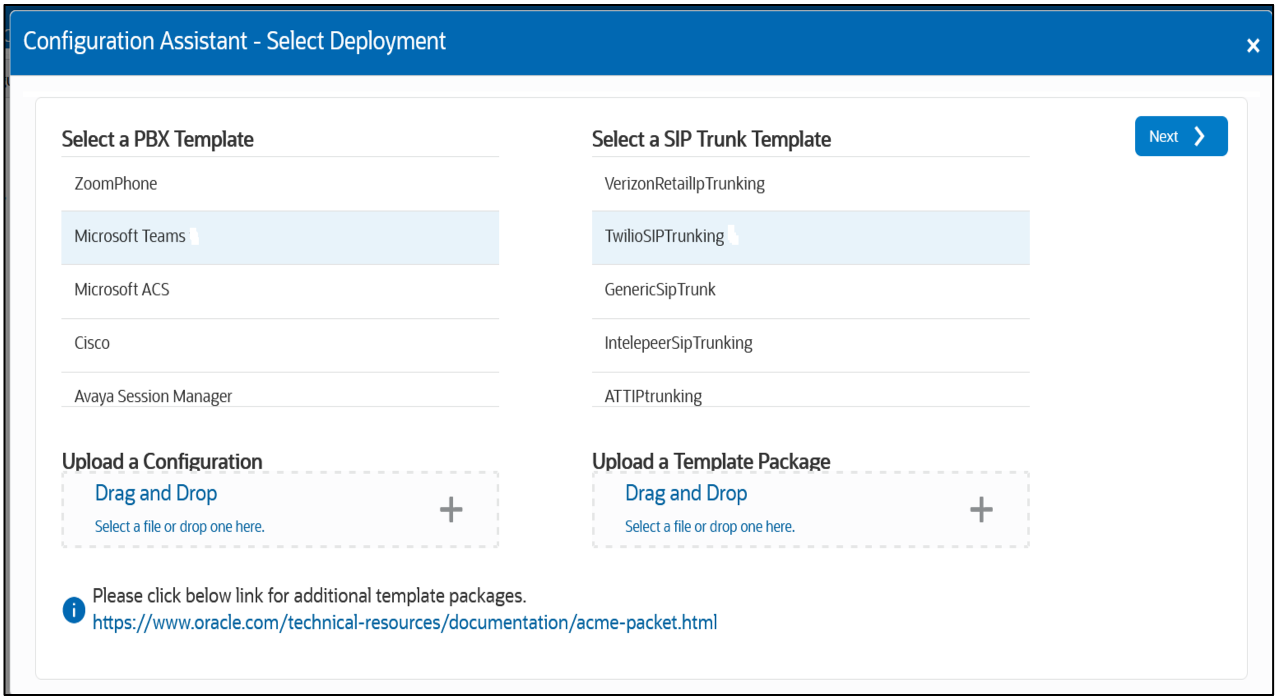
Upload a Template Package

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 MS Teams 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	Select a SIP Trunk Template
ZoomPhone	VerizonRetailIpTrunking
Microsoft Teams	TwilioSIPTrunking
Microsoft ACS	GenericSipTrunk
Cisco	IntelepeerSipTrunking
Avaya Session Manager	ATTIPtrunking

Upload a Configuration

Drag and Drop

Select a file or drop one here.

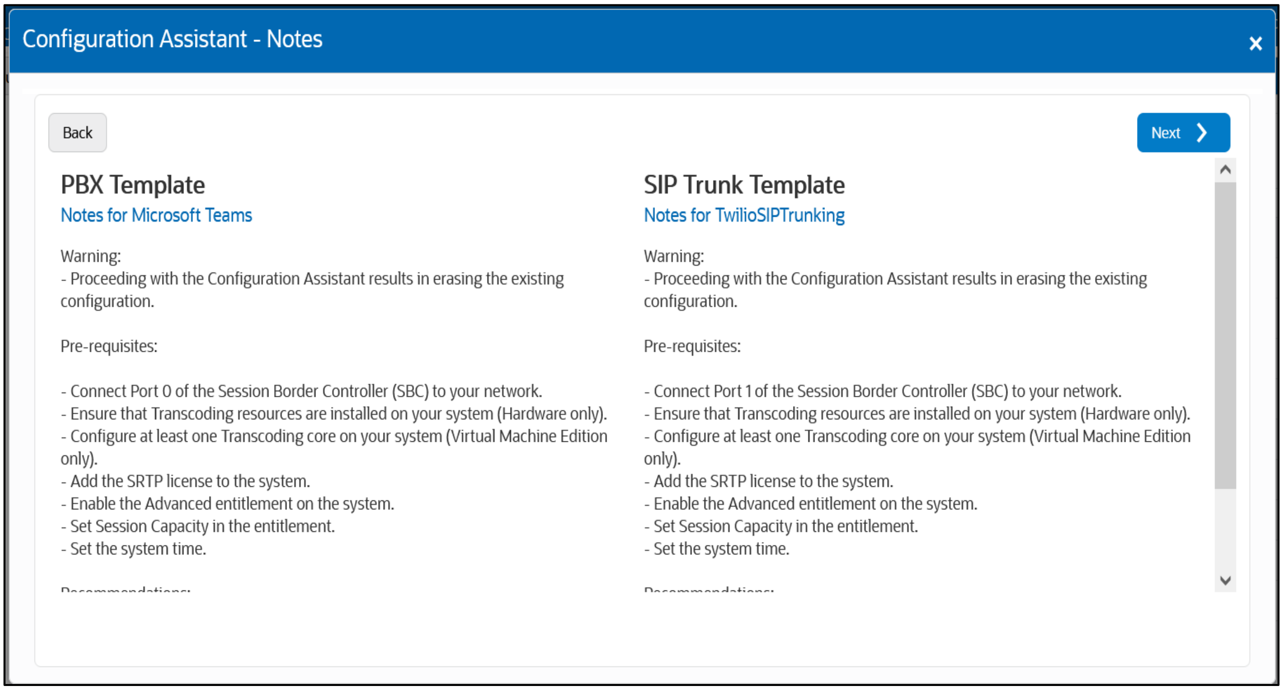
Upload a Template Package

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



Configuration Assistant - Notes

PBX Template

Notes for Microsoft Teams

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).
- 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:

SIP Trunk Template

Notes for TwilioSIPTrunking

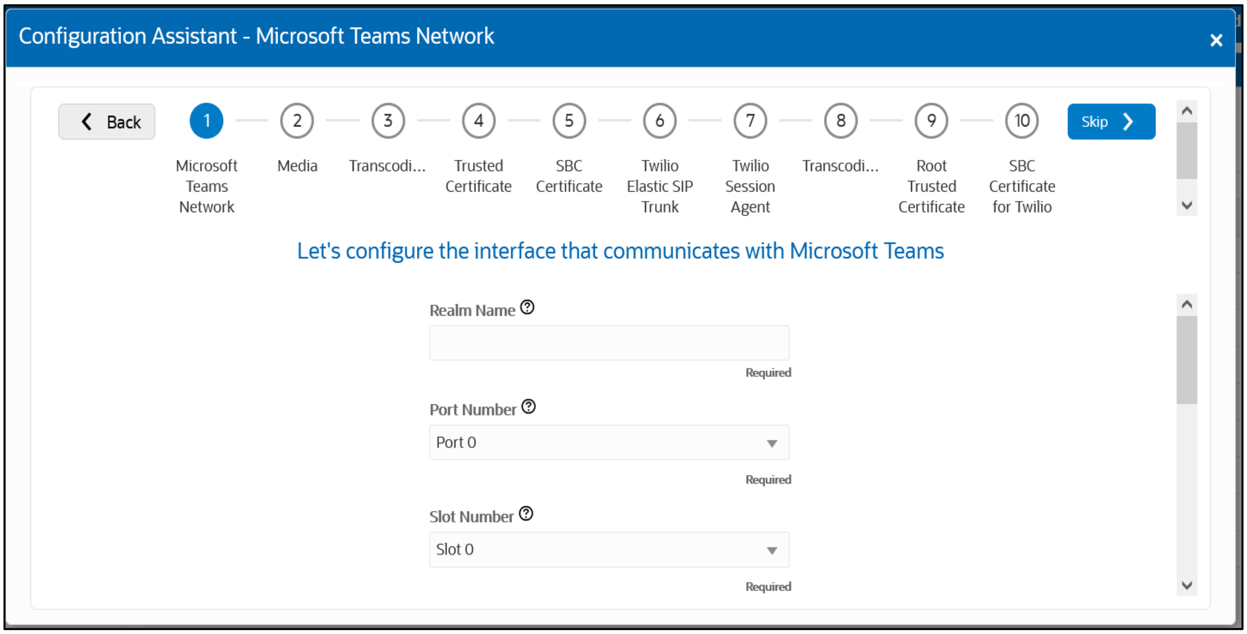
Warning:
- Proceeding with the Configuration Assistant results in erasing the existing configuration.

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 - Microsoft Teams Network
×
Back
1 Microsoft Teams Network
2 Media
3 Transcodi...
4 Trusted Certificate
5 SBC Certificate
6 Twilio Elastic SIP Trunk
7 Twilio Session Agent
8 Transcodi...
9 Root Trusted Certificate
10 SBC Certificate for Twilio
Skip

Let's configure the interface that communicates with Microsoft Teams

Realm Name
Required

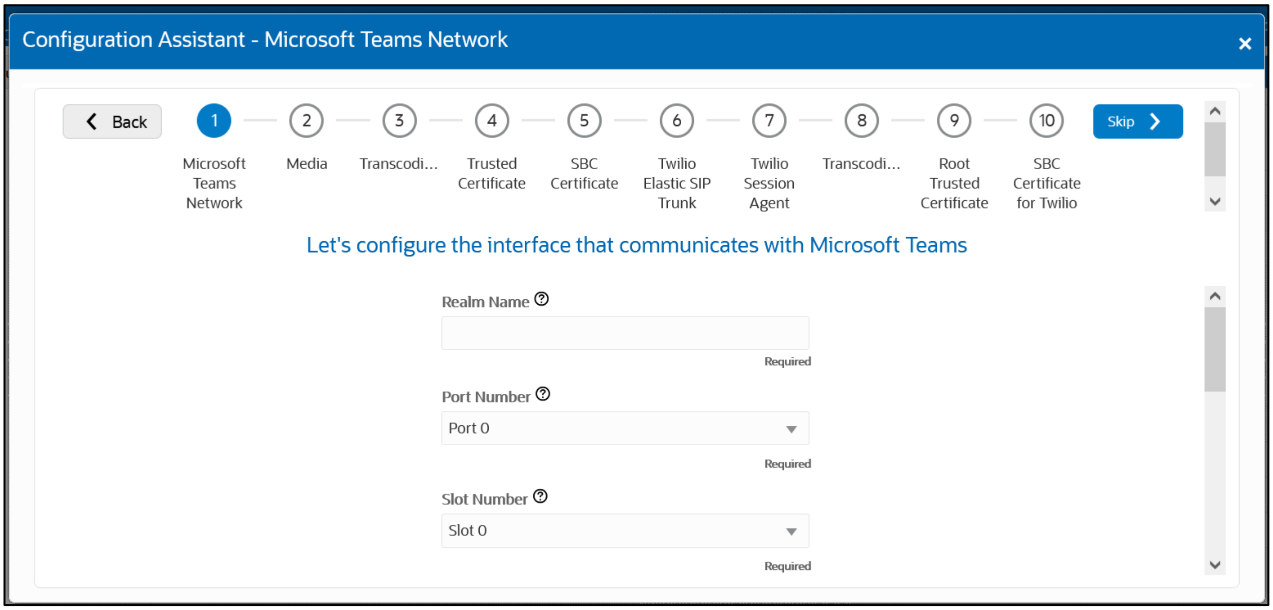
Port Number
Port 0
Required

Slot Number
Slot 0
Required

7.3. Configuration Assistant Template Navigation

7.3.1. Page 1-Microsoft Teams Network

Page 1 of the template is where you will configure the network information to connect Microsoft Teams Direct Routing.


Configuration Assistant - Microsoft Teams Network
×
Back
1 Microsoft Teams Network
2 Media
3 Transcodi...
4 Trusted Certificate
5 SBC Certificate
6 Twilio Elastic SIP Trunk
7 Twilio Session Agent
8 Transcodi...
9 Root Trusted Certificate
10 SBC Certificate for Twilio
Skip

Let's configure the interface that communicates with Microsoft Teams

Realm Name
Required

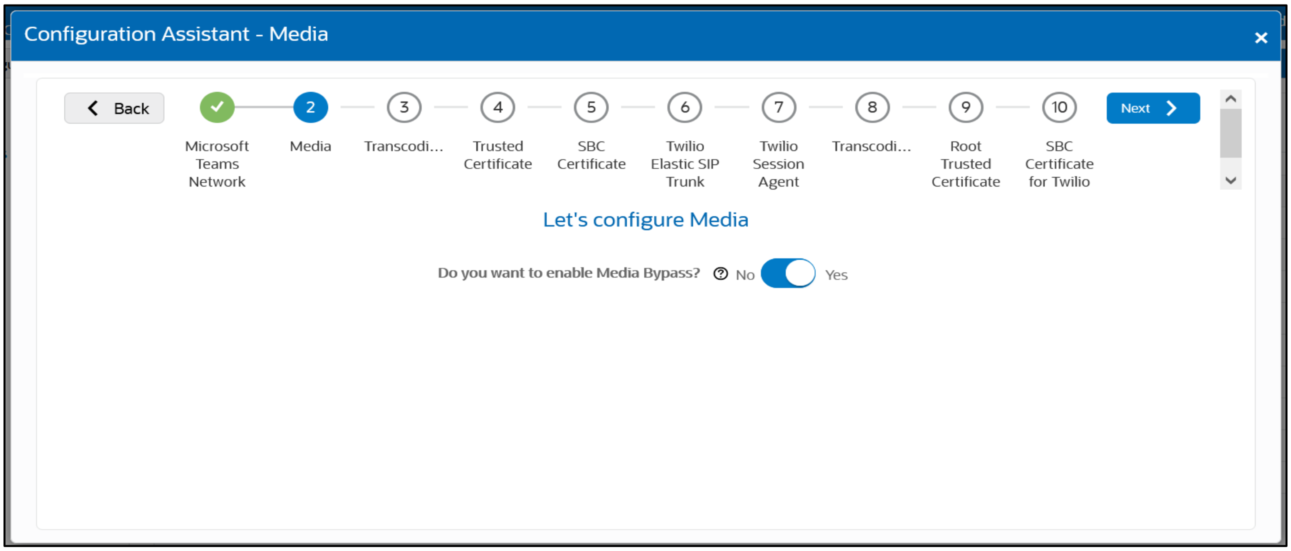
Port Number
Port 0
Required

Slot Number
Slot 0
Required

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

7.3.2. Page 2-Media

Page 2 of the template is where you configure the SBC for media bypass or non-media bypass. Your Teams side configures determines whether or not media will flow directly between the SBC and your Teams client, or from the SBC to a Microsoft Cloud media server. Please enable Media Bypass if you want to enable MS Teams Media bypass mode and click Next.



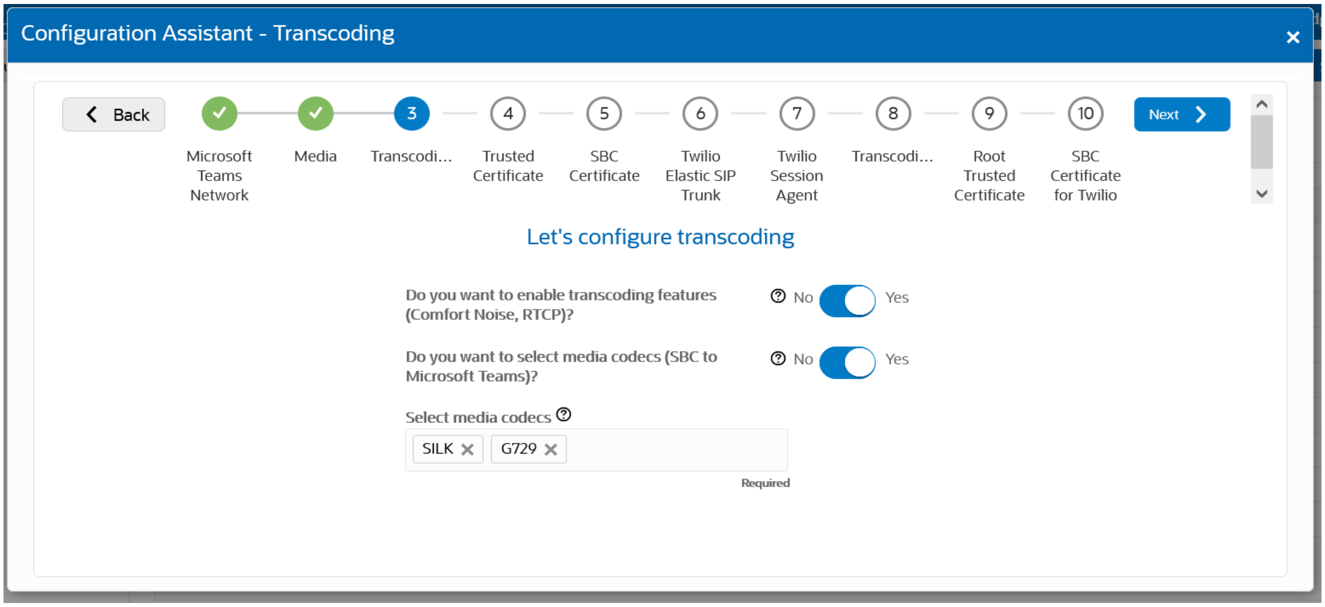
Configuration Assistant - Media

Let's configure Media

Do you want to enable Media Bypass? No [✓ Yes]

7.3.3. Page 3-MS Teams side Transcoding

Page 3 is where you will be able to configure transcoding between the SBC and Microsoft Teams. Just to note, Microsoft Teams requires the use of both Comfort Noise and RTCP on call flows. 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 Teams. 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 features (Comfort Noise, RTCP)? No / Yes: Yes

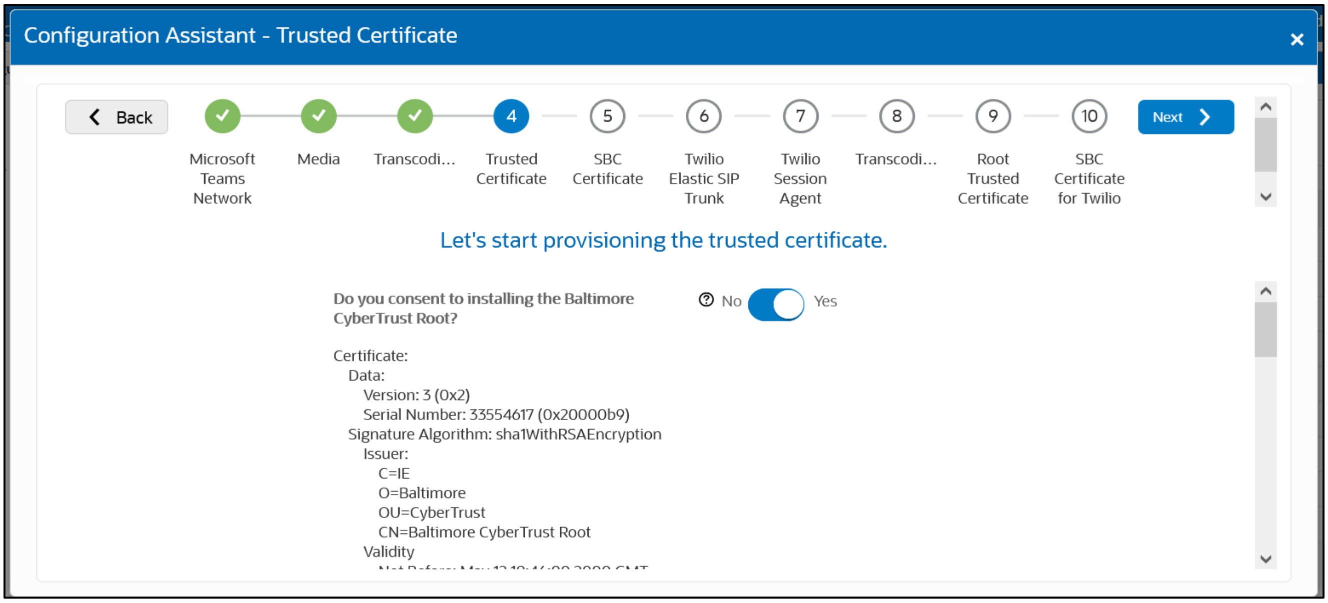
Do you want to select media codecs (SBC to Microsoft Teams)? No / Yes: Yes

Select media codecs: SILK ✕ G729 ✕

Required

7.3.4. Page 4 - Import Baltimore Root Trusted CA Certificate for MS Teams side.

Page 4 of this template is where the SBC will import the Baltimore Root CA certificate, which Microsoft uses to sign the certs it presents to the SBC during the TLS handshake. Importing the Baltimore Root CA certs is enabled by default.



Configuration Assistant - Trusted Certificate

Let's start provisioning the trusted certificate.

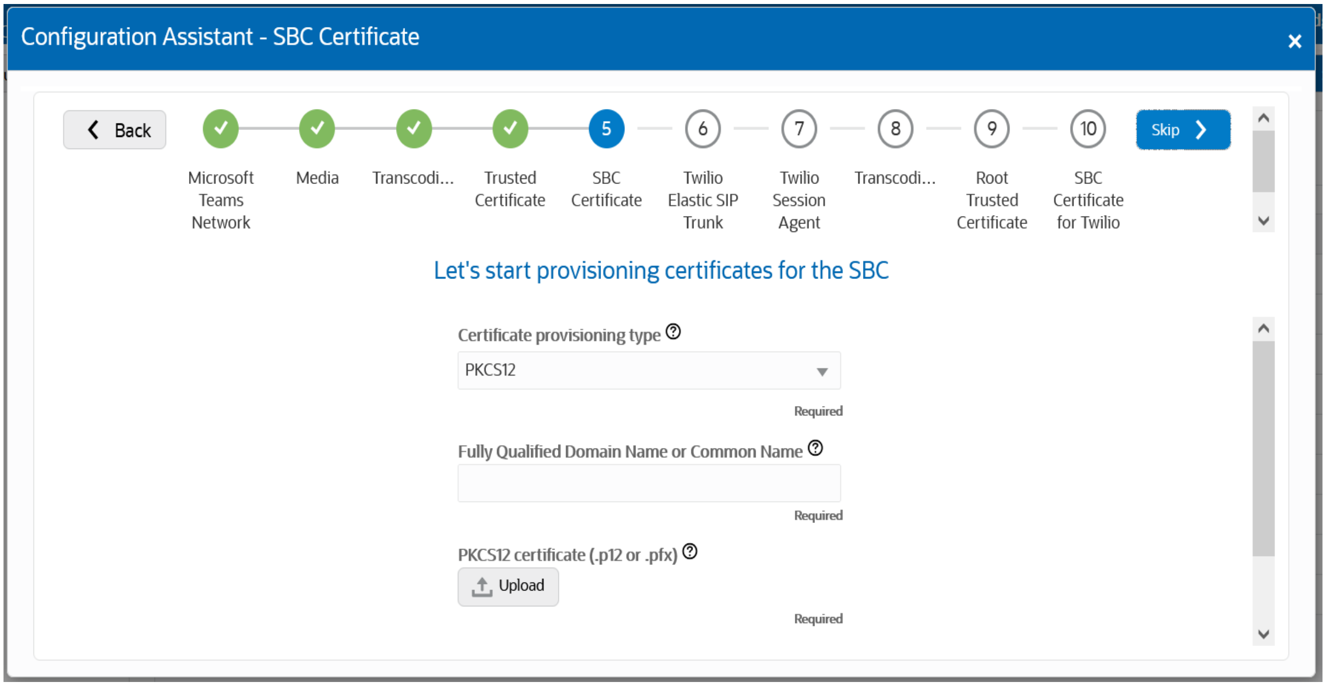
Do you consent to installing the Baltimore CyberTrust Root? No / Yes: Yes

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 33554617 (0x20000b9)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            C=IE
            O=Baltimore
            OU=CyberTrust
            CN=Baltimore CyberTrust Root
        Validity
```

7.3.5. Page 5 - SBC Certificates for Teams 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 Microsoft support CA, and enter the certificates password.



Configuration Assistant - SBC Certificate

Let's start provisioning certificates for the SBC

Certificate provisioning type: PKCS12 (Required)

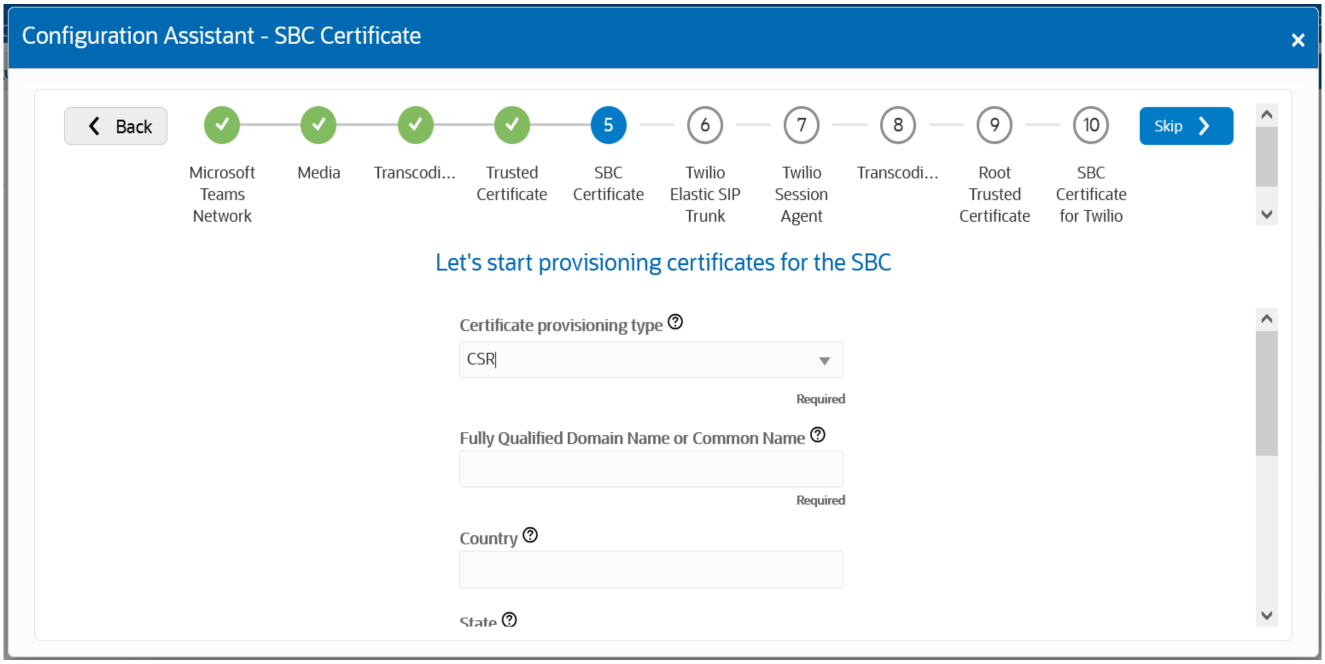
Fully Qualified Domain Name or Common Name: (Required)

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

Certificate Signing Request (CSR)

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

Let's start provisioning certificates for the SBC

Certificate provisioning type: CSR (Required)

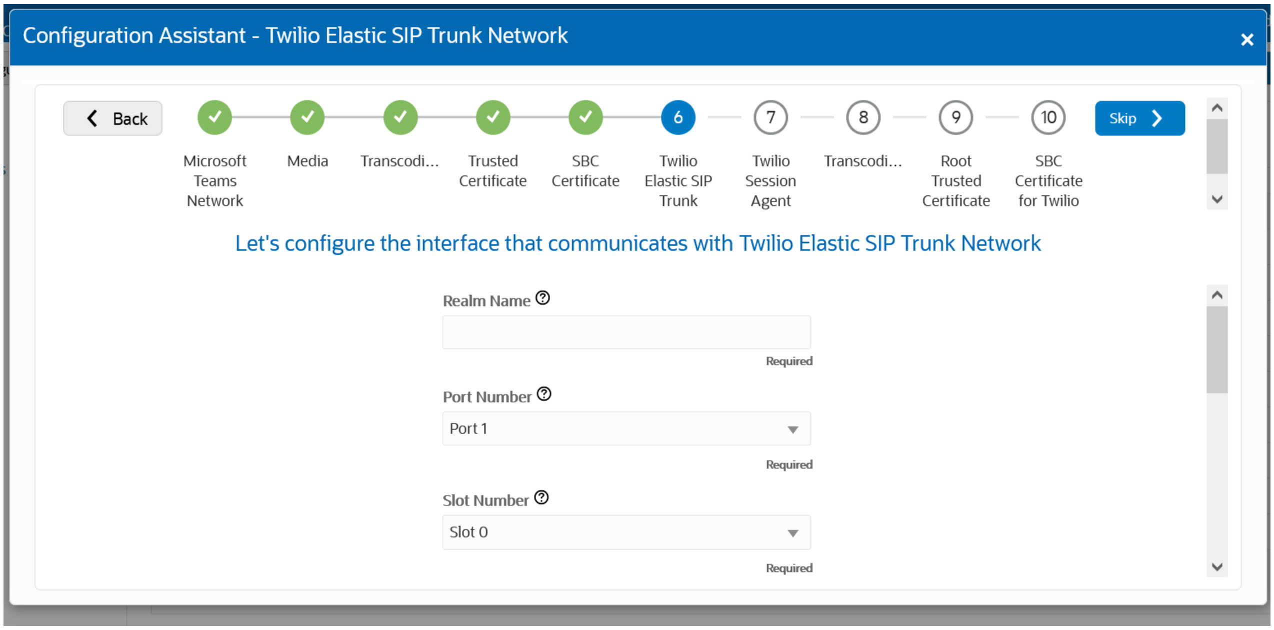
Fully Qualified Domain Name or Common Name: (Required)

Country:

State

7.3.6. Page 6 - Twilio Elastic SIP Trunk Network

Page 6 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.



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

Realm Name

Required

Port Number: Port 1

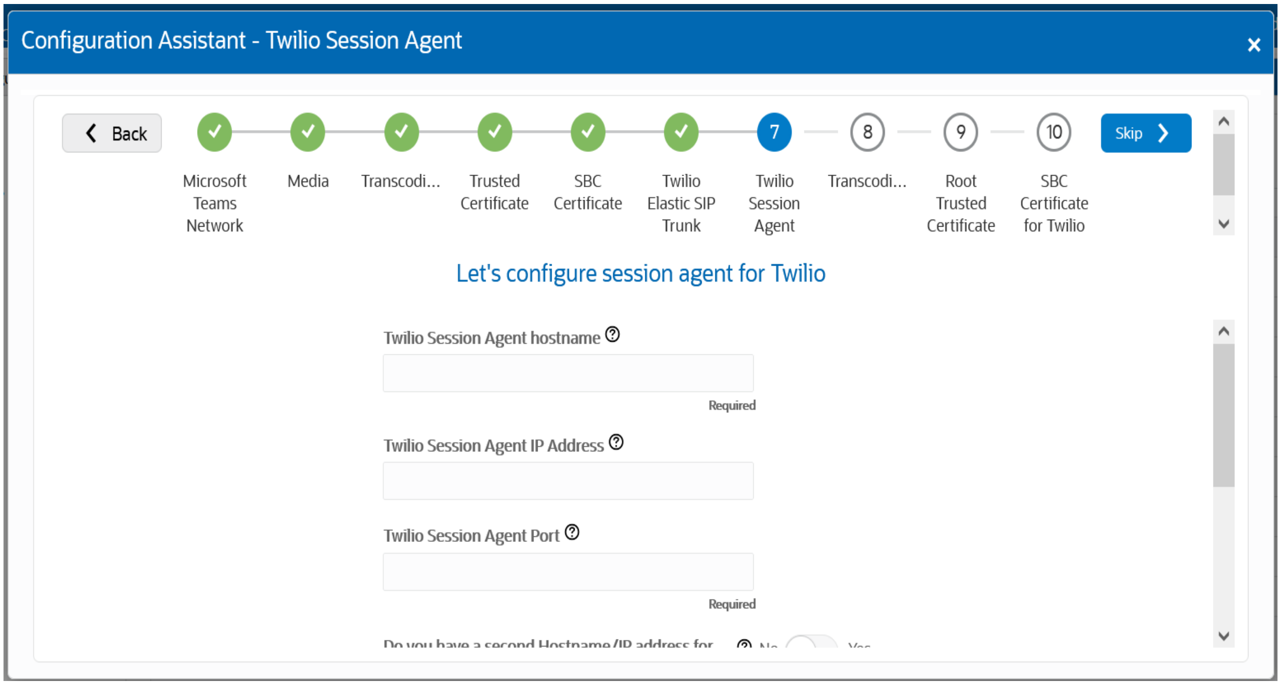
Required

Slot Number: Slot 0

Required

7.3.7. Page 7 - Twilio Session Agent

Page 7 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.



Let's configure session agent for Twilio

Twilio Session Agent hostname

Required

Twilio Session Agent IP Address

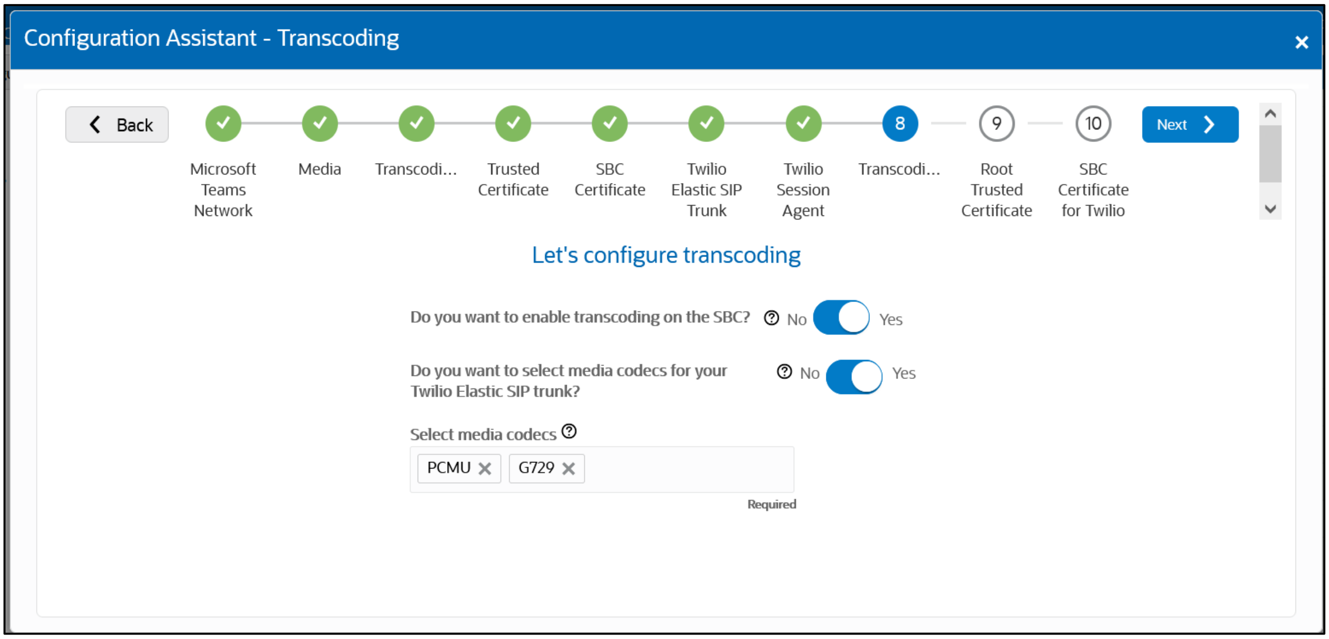
Twilio Session Agent Port

Required

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

7.3.8. Page 8 - Twilio side Transcoding

Page 8 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.



Let's configure transcoding

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

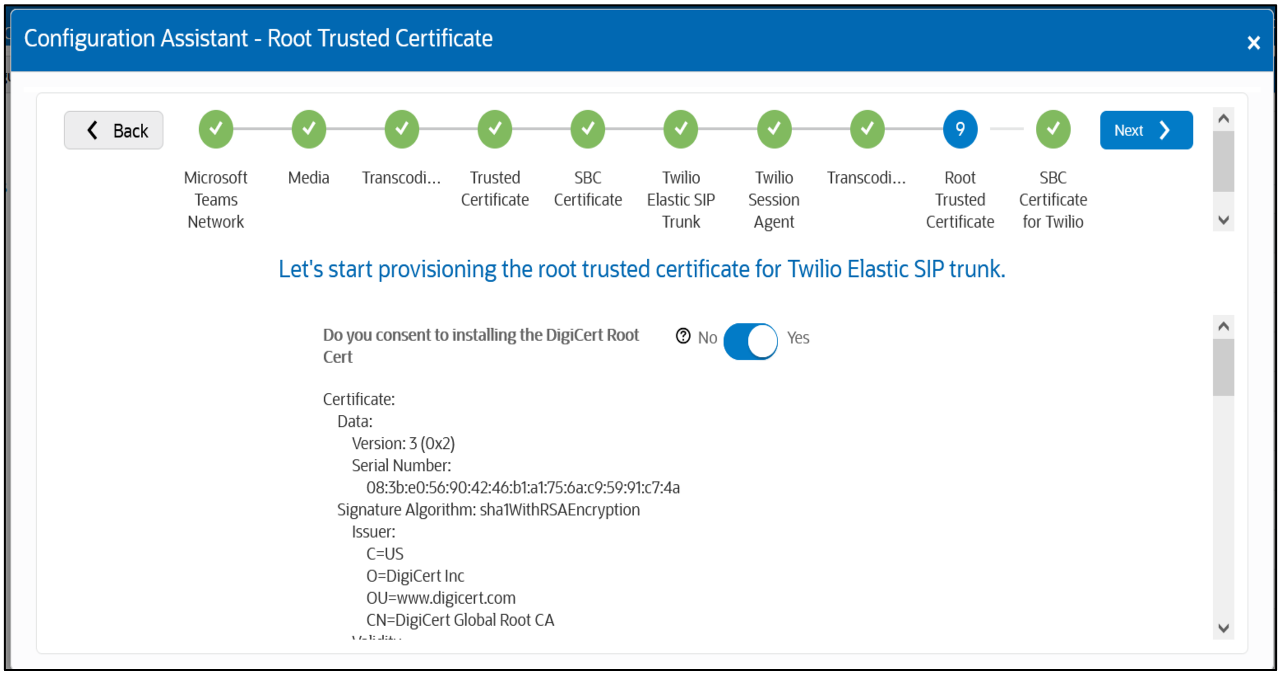
Do you want to select media codecs for your Twilio Elastic SIP trunk? No [✓ Yes]

Select media codecs: PCMU ✕ G729 ✕

Required

7.3.9. Page 9 - Import Digi Cert Root CA Certificate for Twilio Side

Page 9 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.



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

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

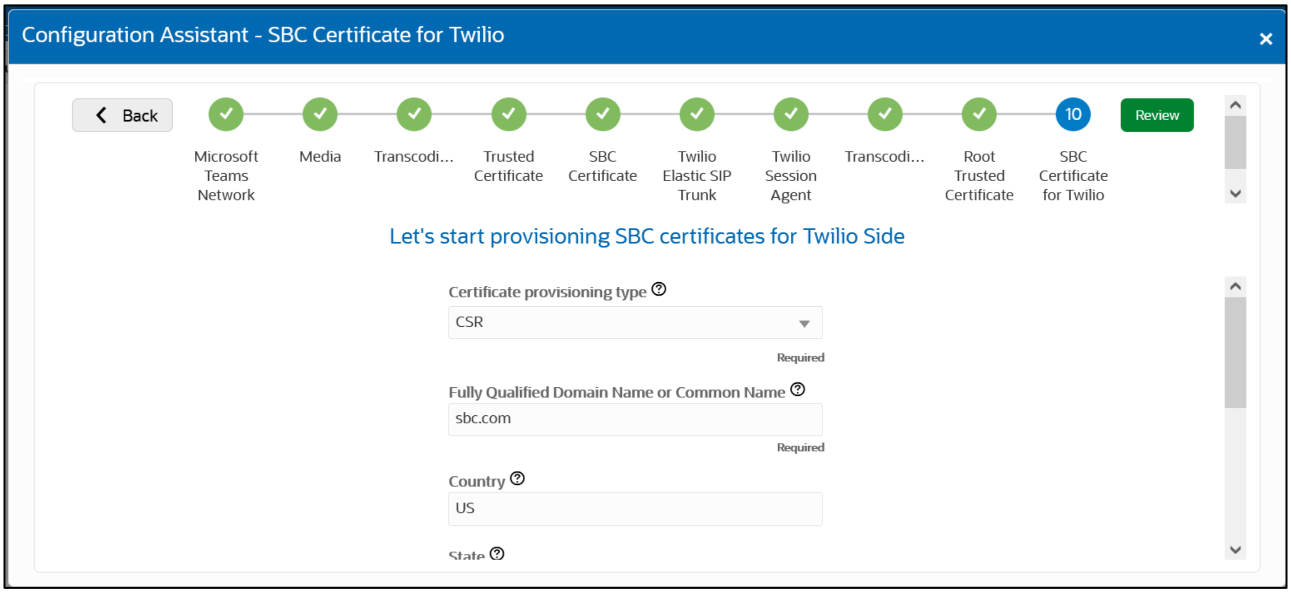
```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      08:3b:e0:56:90:42:46:b1:a1:75:6a:c9:59:91:c7:4a
  Signature Algorithm: sha1WithRSAEncryption
    Issuer:
      C=US
      O=DigiCert Inc
      OU=www.digicert.com
      CN=DigiCert Global Root CA
```

7.3.10. Page 10 - SBC Certificates for Teams side

This page also follows the same procedure as page 5 and the screen also looks exactly similar to page 5. We can follow the same steps to import certificate for Twilio side too.

7.4. Review

At the end of the template, you will notice in the top right, a “*Review*” tab. If all 10 pages presented across the top are showing green, indicting there are no errors with the information entered, click on the “Review” tab.



Let's start provisioning SBC certificates for Twilio Side

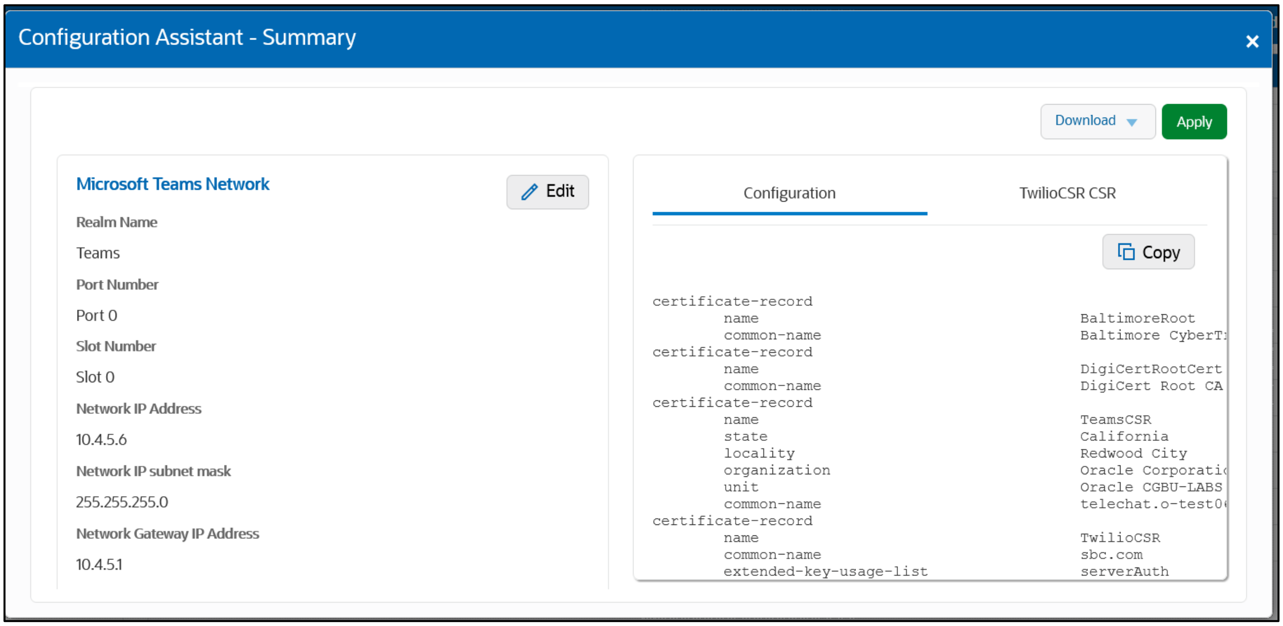
Certificate provisioning type ⓘ: CSR (Required)

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

Country ⓘ: US

State ⓘ

The screen looks like below after clicking the Review Tab.



Configuration Assistant - Summary

Microsoft Teams Network

Realm Name

Teams

Port Number

Port 0

Slot Number

Slot 0

Network IP Address

10.4.5.6

Network IP subnet mask

255.255.255.0

Network Gateway IP Address

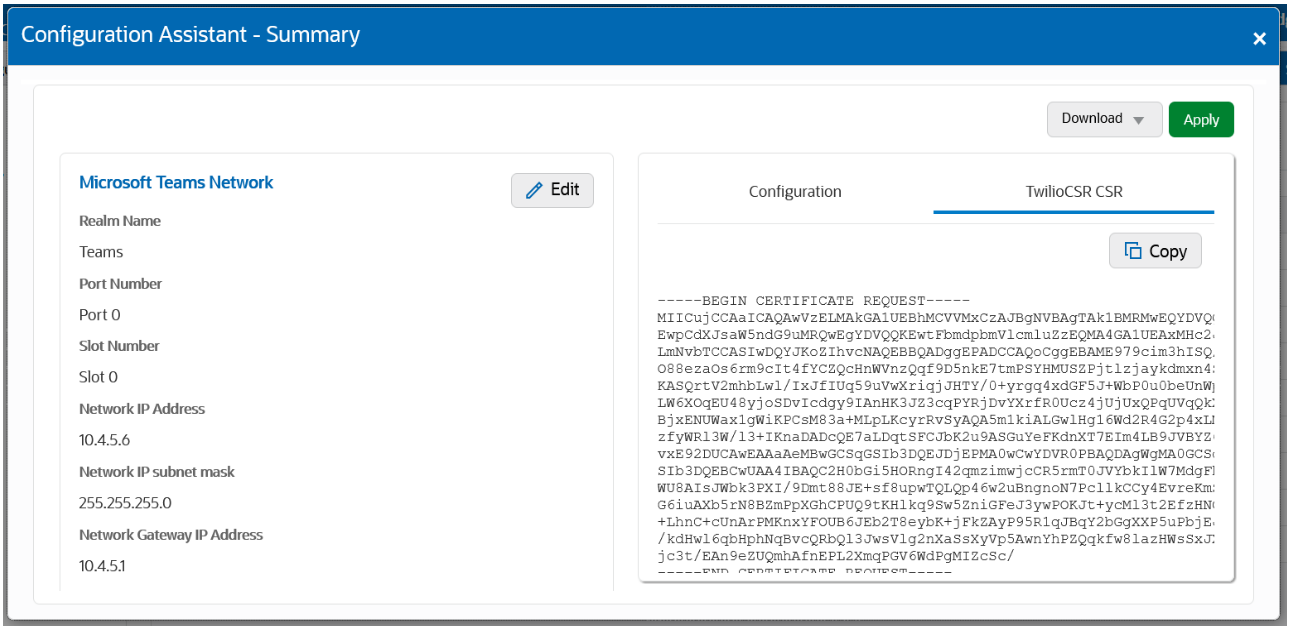
10.4.5.1

```
certificate-record
        name                                              BaltimoreRoot
        common-name                                       Baltimore CyberT
certificate-record
        name                                              DigiCertRootCert
        common-name                                       DigiCert Root CA
certificate-record
        name                                              TeamsCSR
        state                                             California
        locality                                          Redwood City
        organization                                      Oracle Corporati
        unit                                              Oracle CGBU-LABS
        common-name                                       telechat.o-test0
certificate-record
        name                                              TwilioCSR
        common-name                                       sbc.com
        extended-key-usage-list                           serverAuth
```

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 5 or page 10 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. Also, if you choose CSR on both pages (pages 5 and 10), there will be two CSR's on the review page.



Configuration Assistant - Summary

Microsoft Teams Network

Realm Name

Teams

Port Number

Port 0

Slot Number

Slot 0

Network IP Address

10.4.5.6

Network IP subnet mask

255.255.255.0

Network Gateway IP Address

10.4.5.1

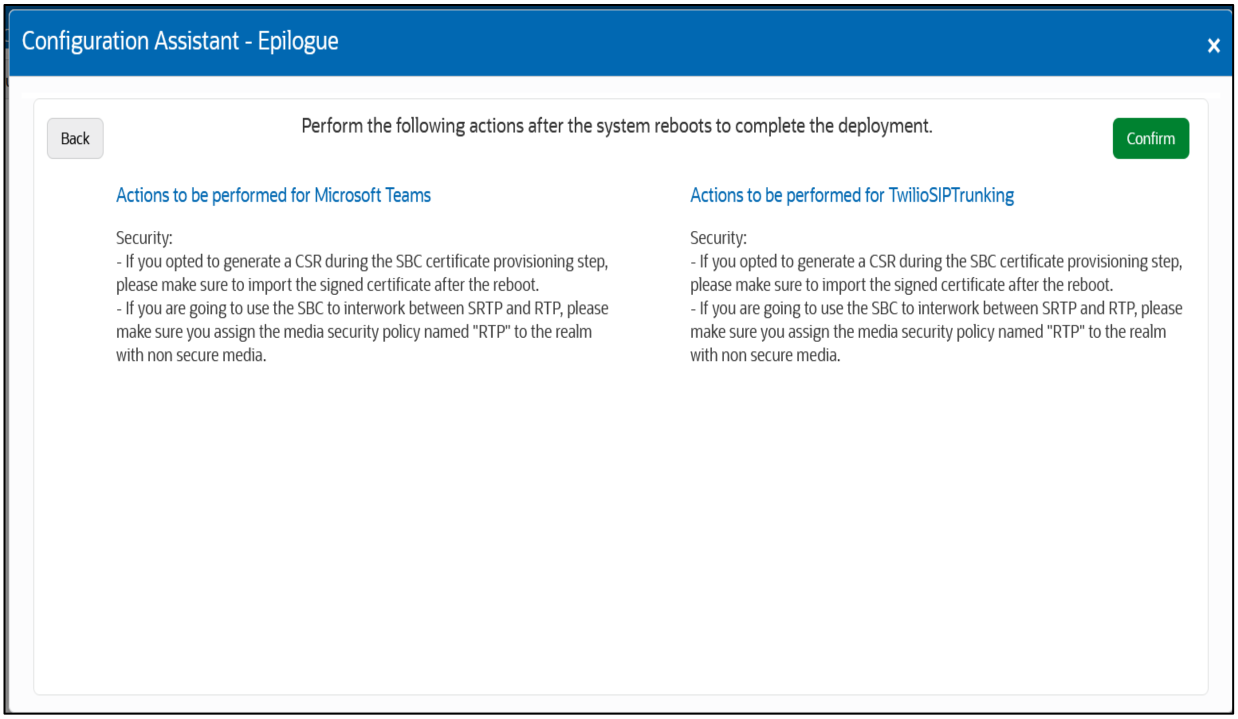
```
-----BEGIN CERTIFICATE REQUEST-----
MIICujCCAaICAQAwVzELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQ
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEQMA4GA1UEAxMHc2
LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAME979cim3hISQ
O88ezaOs6rm9cIt4fYCZQcHnWVnzQqf9D5nkE7tmPSYHMUSZPjtlzjaykdmxn4
KASQrtV2mhbLwl/IxJfIUq59uVwXriqjJHTY/0+yrgq4xdGF5J+WbP0u0beUnW
LW6XOqEU48yjoSDvIcdgy9IAnHK3JZ3cqPYRjDvYXrfR0Ucz4jUjUxQPqUVqQk
BjxENUWax1gWiKPCsM83a+MLpLKcyrRvSyAQA5m1kiALGwlHg16Wd2R4G2p4xL
zfyWRl3W/l3+IKnaDADcQE7aLDqtSFCJbK2u9ASGuYeFKdnXT7EIm4LB9JVBYZ
vxE92DUCAwEAAaAeMBwGCSqGSIb3DQEJDjEPMA0wCwYDVR0PBAQDAgWgMA0GCS
SIb3DQEBCwUAA4IBAQC2H0bGi5HORngI42qmzimwjcCR5rmT0JVYbkIlW7MdgF
WU8AIsJWbk3PXI/9Dmt88JE+sf8upwTQLQp46w2uBngnoN7PcllkCCy4EvreKm
G6iuAXb5rN8BZmPpXGhCPUQ9tKHlkq9Sw5ZniGFeJ3ywPOKJt+ycMl3t2EfzHN
+LhnC+cUnArPMKnxYFOUB6JEb2T8eybK+jFkZAyP95R1qJBqY2bGgXXP5uPbjE
/kdHwl6qbHphNqBvcQRbQl3JwsVlg2nXaSsXyVp5AwnYhPZQqkfw8lazHWsSxJ
jc3t/EAn9eZUQmhAfnEPL2XmqPGV6WdPgMIZcSc/
-----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 Microsoft or 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 5 and 10, the CSR tab will not be present under review.

7.5. 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.



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

Actions to be performed for Microsoft Teams

Security:
- If you opted to generate a CSR during the SBC certificate provisioning step, please make sure to import the signed certificate after the reboot.
- If you are going to use the SBC to interwork between SRTP and RTP, please make sure you assign the media security policy named "RTP" to the realm with non secure media.

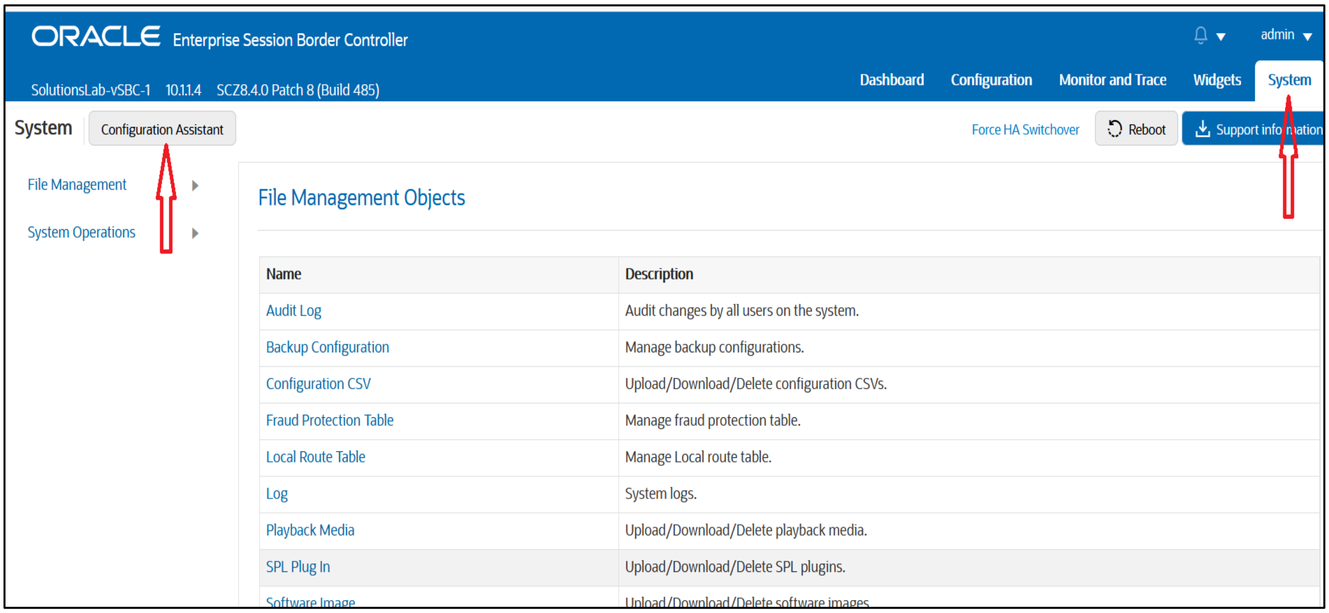
Actions to be performed for TwilioSIPTrunking

Security:
- If you opted to generate a CSR during the SBC certificate provisioning step, please make sure to import the signed certificate after the reboot.
- If you are going to use the SBC to interwork between SRTP and RTP, please make sure you assign the media security policy named "RTP" to the realm with non secure media.

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 Microsoft Teams Direct Routing with Twilio SIP trunking.

7.6. 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.

8. Existing SBC configuration

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

- New realm-config
- Configuring a certificate for SBC Interface
- TLS-Profile
- New sip-interface
- New session-agent
- New session-agent group
- New steering-pools
- New local-policy
- New sip-manipulation
- New media-profile and codec-policy
- ICE profile
- SDES Profile
- Media-sec-Policy
- RTCP Policy and RTP Mux

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

9.SIP Access Controls

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

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

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

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

1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high

2. Set the access control trust level on public facing realms to HIGH

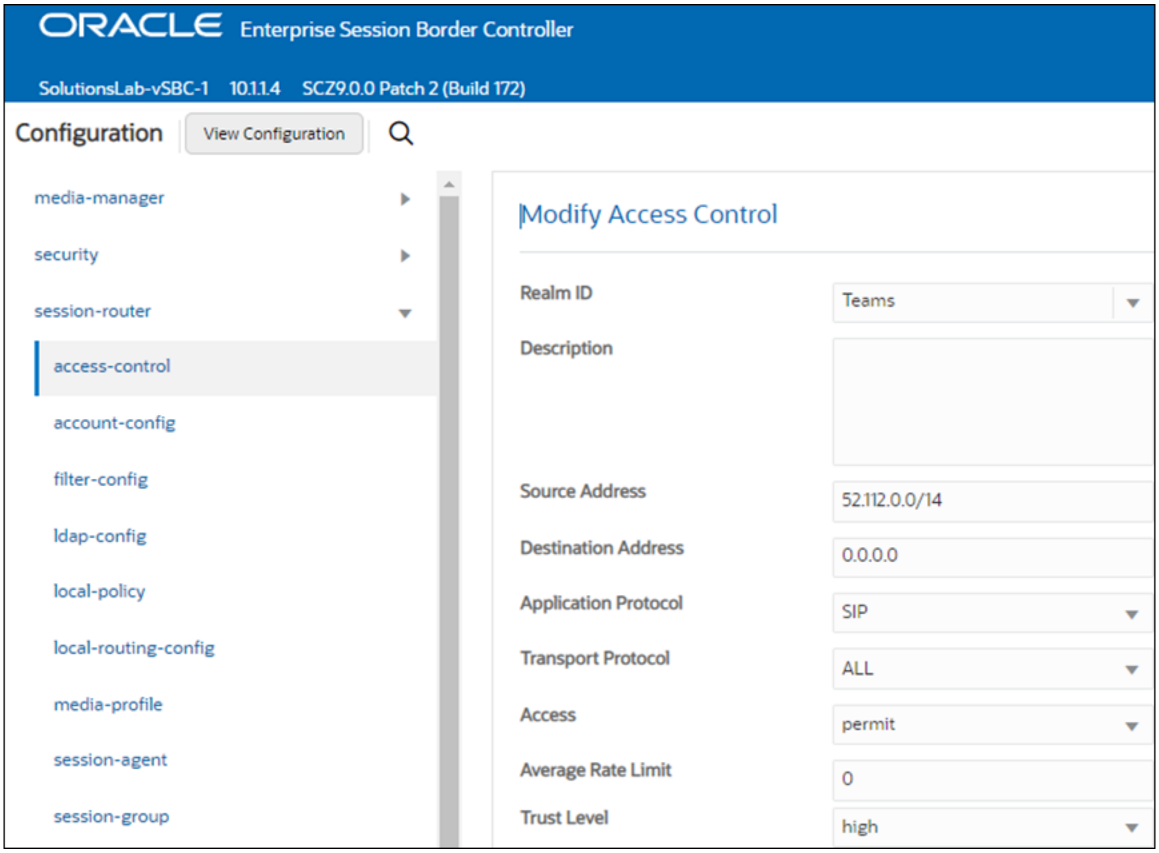
Microsoft Teams has two subnets, 52.112.0.0/14 and 52.120.0.0/14 that must be allowed to send traffic to the SBC. Both must be configured as an access control on the Oracle SBC and associated with the realm facing Teams.

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

GUI Path: session-router/access-control

ACLI Path: config tàsession-routeràaccess-control

Use this example to create ACL's for both MSFT Teams subnets, 52.112.0.0/14 and 52.120.0.0/14.



Modify Access Control

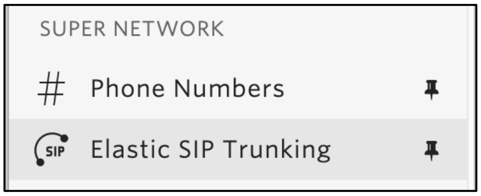
Realm ID	Teams
Description	
Source Address	52.112.0.0/14
Destination Address	0.0.0.0
Application Protocol	SIP
Transport Protocol	ALL
Access	permit
Average Rate Limit	0
Trust Level	high

- Select OK at the bottom

This concludes the required configuration of the SBC to properly interface with Microsoft Teams Phone System Direct Routing.

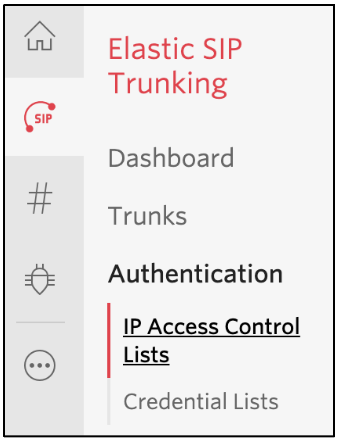
10. Twilio Elastic SIP Trunking Configuration

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

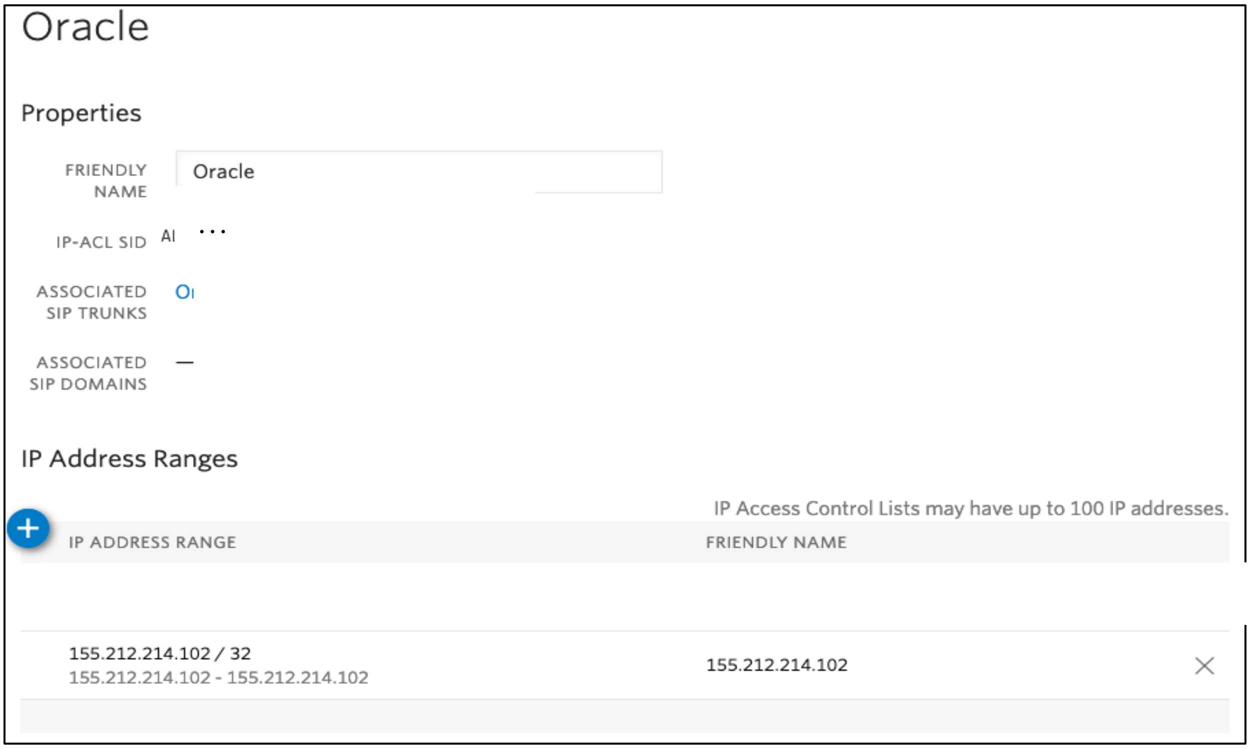


10.1. Create am IP-ACL rule

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	O
ASSOCIATED SIP DOMAINS	—

IP Address Ranges

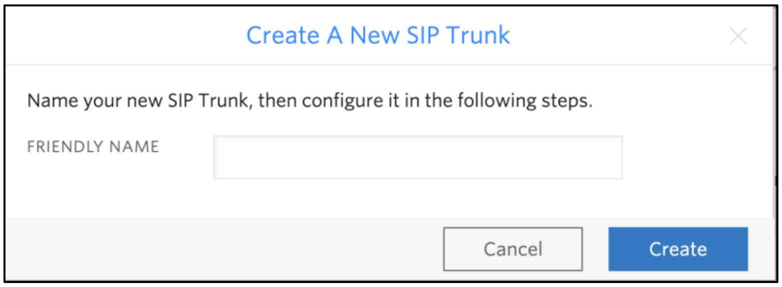
IP Access Control Lists may have up to 100 IP addresses.

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

10.2. Create a new Trunk

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

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

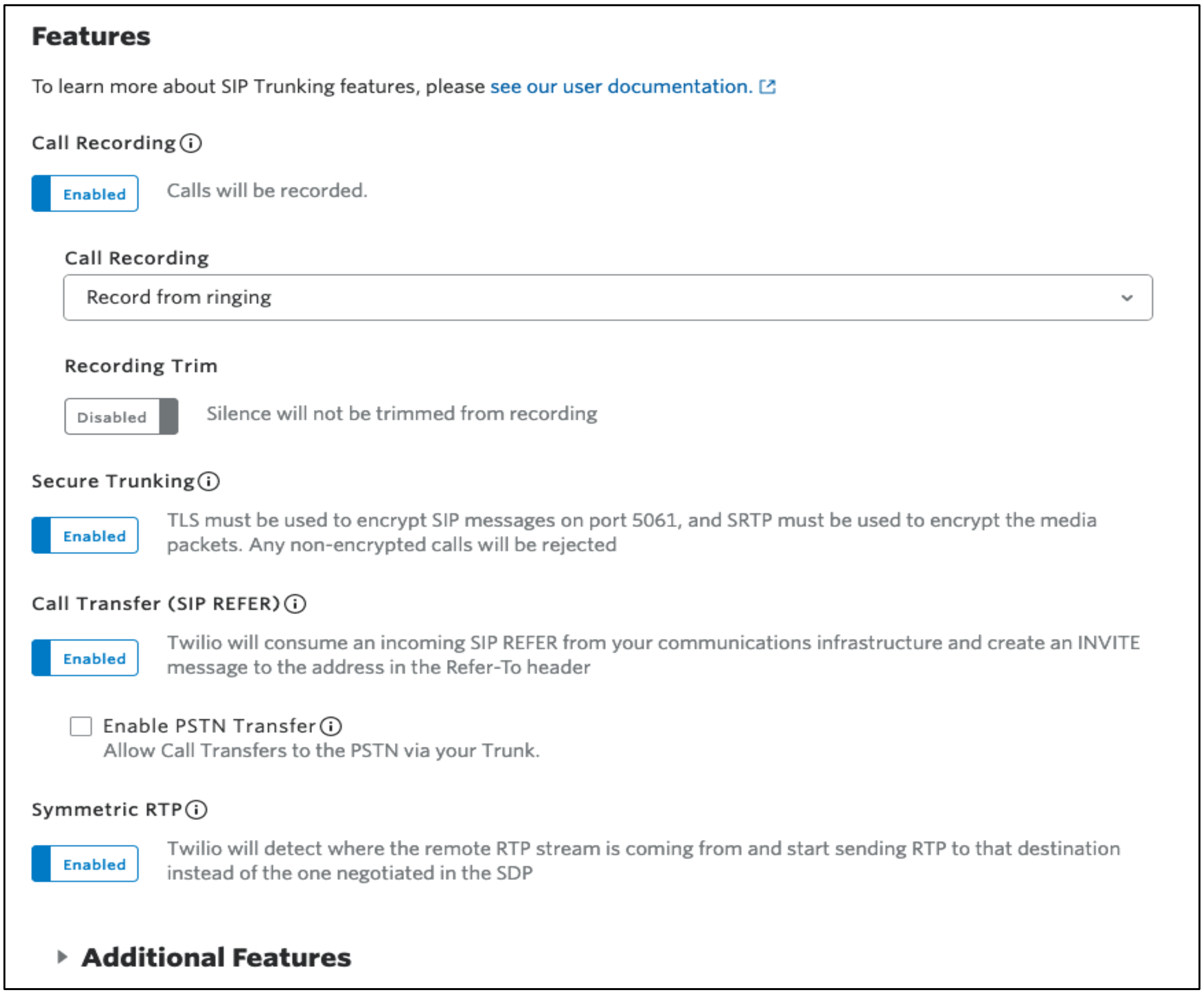


Create A New SIP Trunk

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

FRIENDLY NAME

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



Features

To learn more about SIP Trunking features, please see our user documentation.

Call Recording ⓘ

Enabled — Calls will be recorded.

Call Recording: Record from ringing

Recording Trim

Disabled — Silence will not be trimmed from recording

Secure Trunking ⓘ

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

Call Transfer (SIP REFER) ⓘ

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

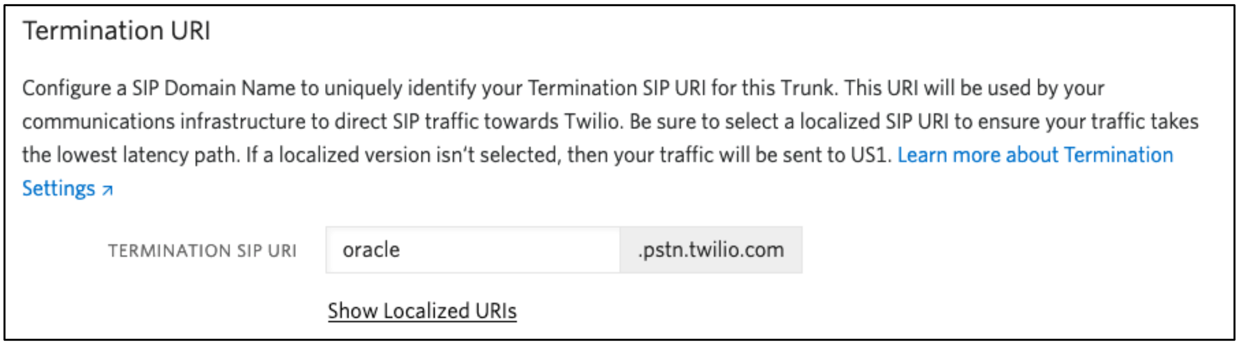
□ Enable PSTN Transfer ⓘ
Allow Call Transfers to the PSTN via your Trunk.

Symmetric RTP ⓘ

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

▸ **Additional Features**

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



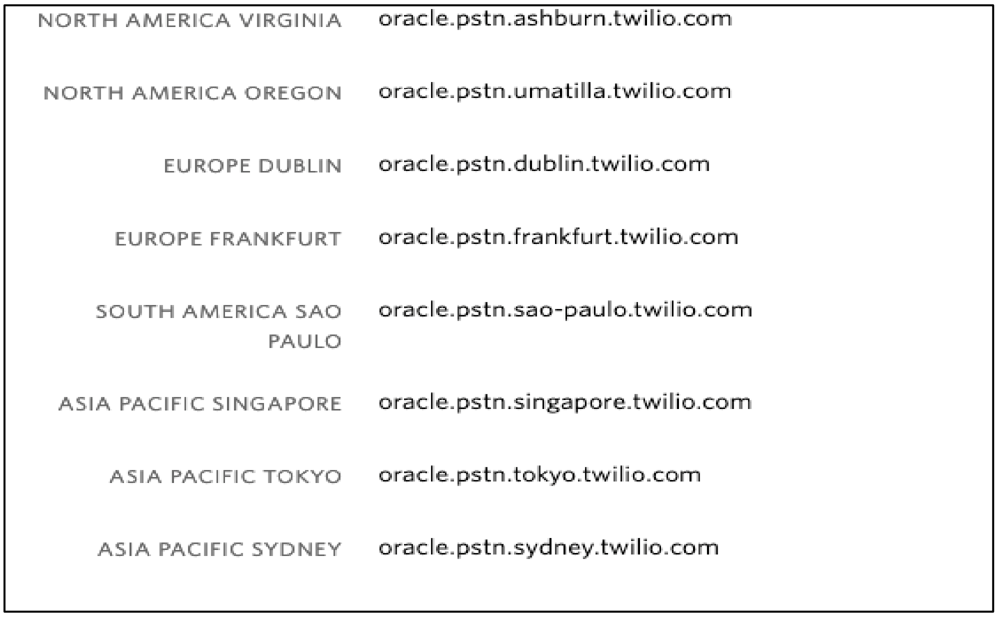
Termination URI

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

TERMINATION SIP URI: oracle .pstn.twilio.com

Show Localized URIs

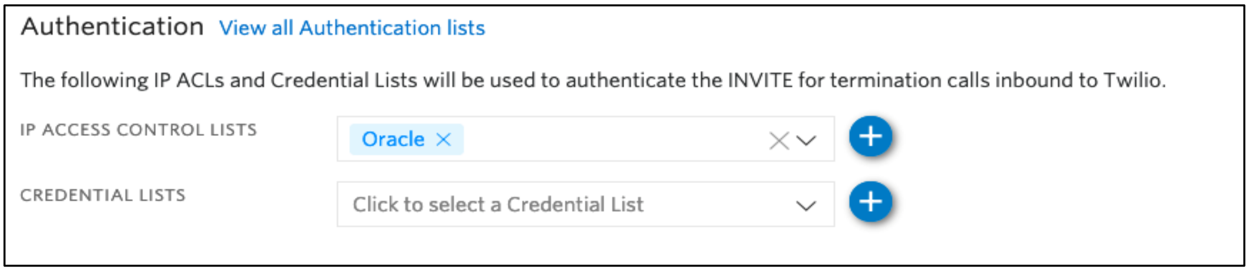
Click on "Show localized URI's" and copy and paste this information as you will use this on your SBC to configure your Trunk.



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

or

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



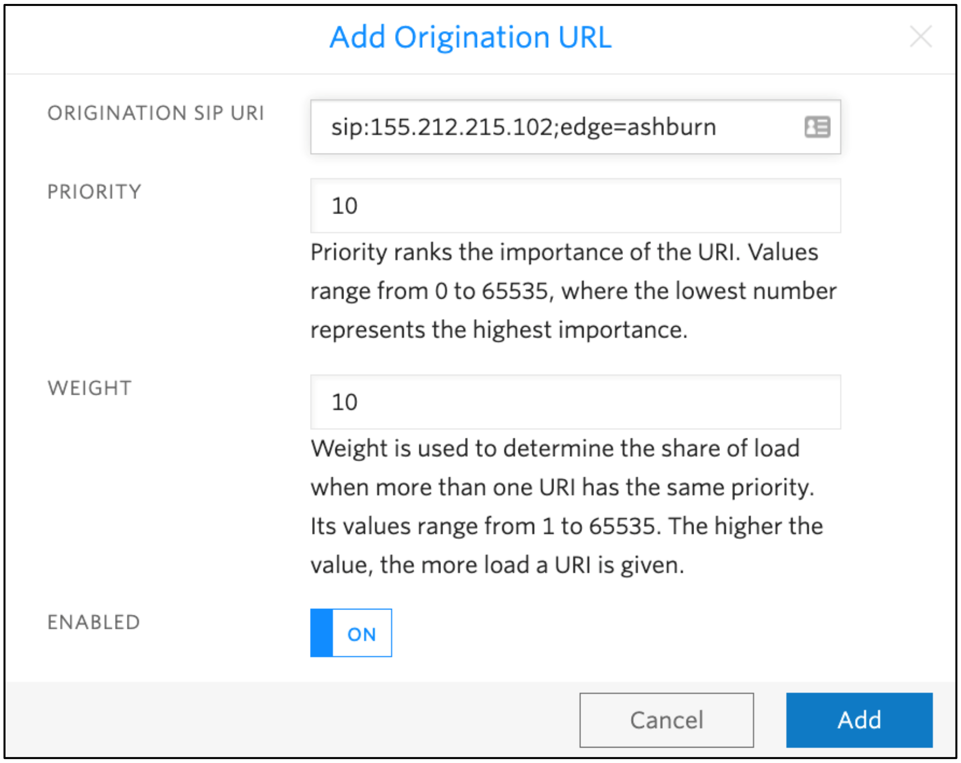
Authentication

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

IP ACCESS CONTROL LISTS	Oracle ✕
CREDENTIAL LISTS	Click to select a Credential List

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

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



Add Origination URL

ORIGINATION SIP URI: sip:155.212.215.102;edge=ashburn

PRIORITY: 10

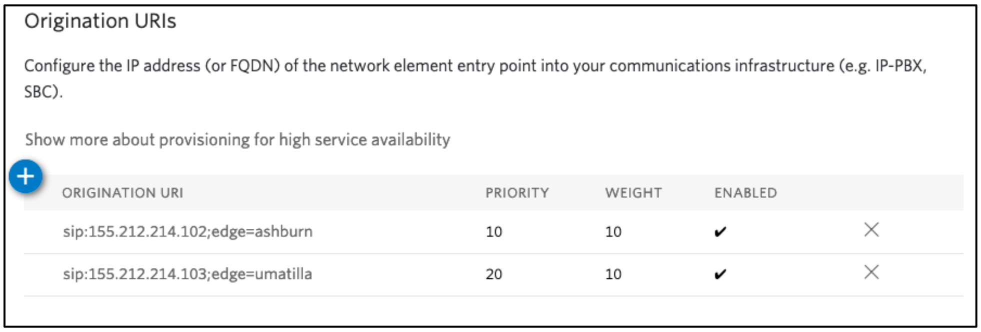
Priority ranks the importance of the URI. Values range from 0 to 65535, where the lowest number represents the highest importance.

WEIGHT: 10

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

ENABLED: ON

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



Origination URIs

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

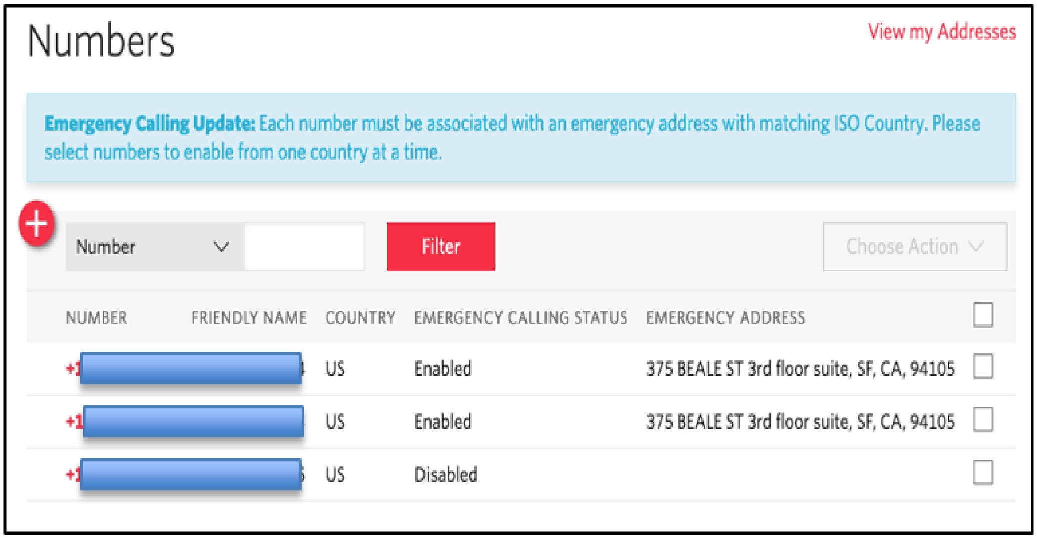
Show more about provisioning for high service availability

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

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

10.3. Associate Phone Numbers on your Trunk

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



Numbers

View my Addresses

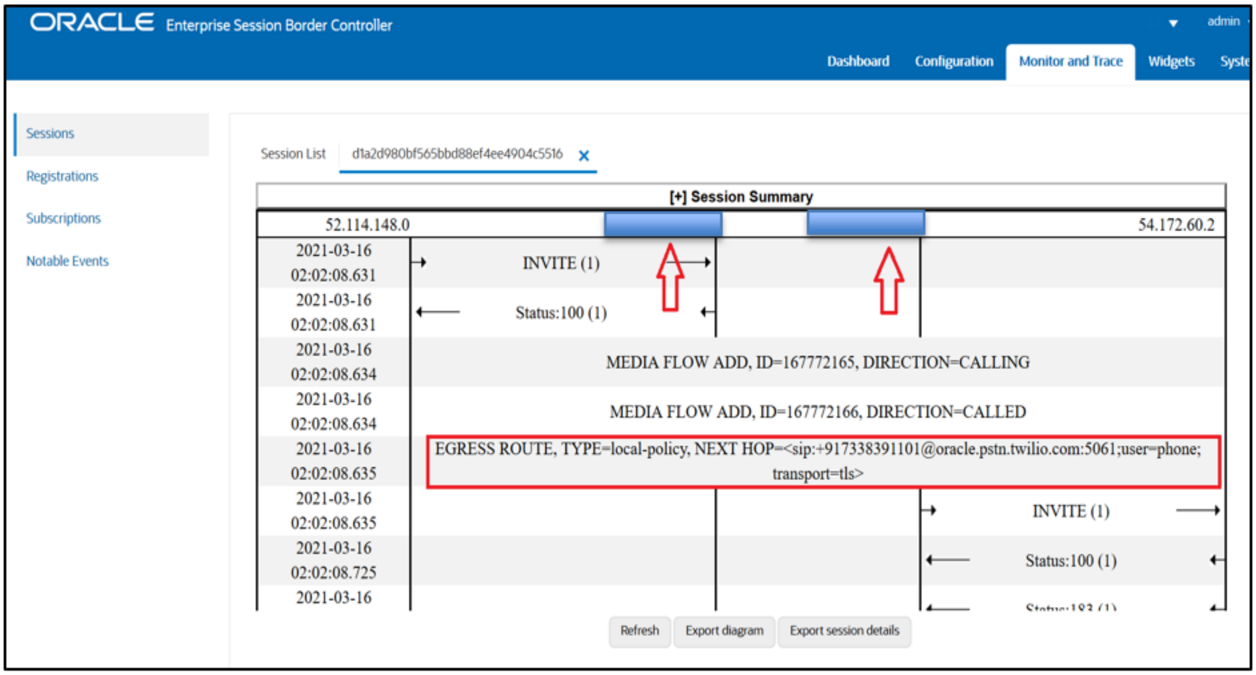
Emergency Calling Update: Each number must be associated with an emergency address with matching ISO Country. Please select numbers to enable from one country at a time.

NUMBER	FRIENDLY NAME	COUNTRY	EMERGENCY CALLING STATUS	EMERGENCY ADDRESS	□
+1[redacted]	[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		□

10. Verification of Sample Call flows

Once the configuration is complete, we can try making sample calls and can check the signaling path between Twilio Elastic Sip Trunk (PSTN Users) and Teams Users. **For our testing, we used the single network interface for both Teams and Twilio side as below.**

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



[+] Session Summary

52.114.148.0 — 54.172.60.2

2021-03-16 02:02:08.631 INVIDE (1)

2021-03-16 02:02:08.631 Status:100 (1)

2021-03-16 02:02:08.634 MEDIA FLOW ADD, ID=167772165, DIRECTION=CALLING

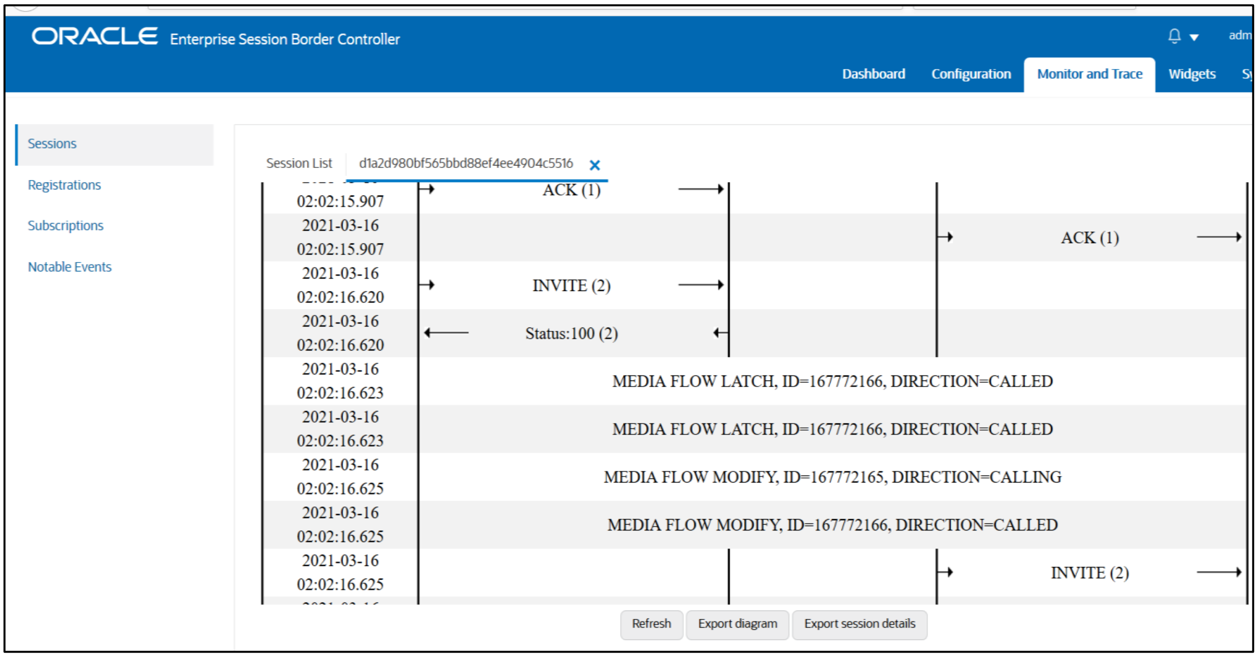
2021-03-16 02:02:08.634 MEDIA FLOW ADD, ID=167772166, DIRECTION=CALLED

2021-03-16 02:02:08.635 EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:+917338391101@oracle.pstn.twilio.com:5061;user=phone;transport=tls>

2021-03-16 02:02:08.635 INVITE (1)

2021-03-16 02:02:08.725 Status:100 (1)

2021-03-16 Status:183 (1)



02:02:15.907 ACK (1)

2021-03-16 02:02:15.907 ACK (1)

2021-03-16 02:02:16.620 INVITE (2)

2021-03-16 02:02:16.620 Status:100 (2)

2021-03-16 02:02:16.623 MEDIA FLOW LATCH, ID=167772166, DIRECTION=CALLED

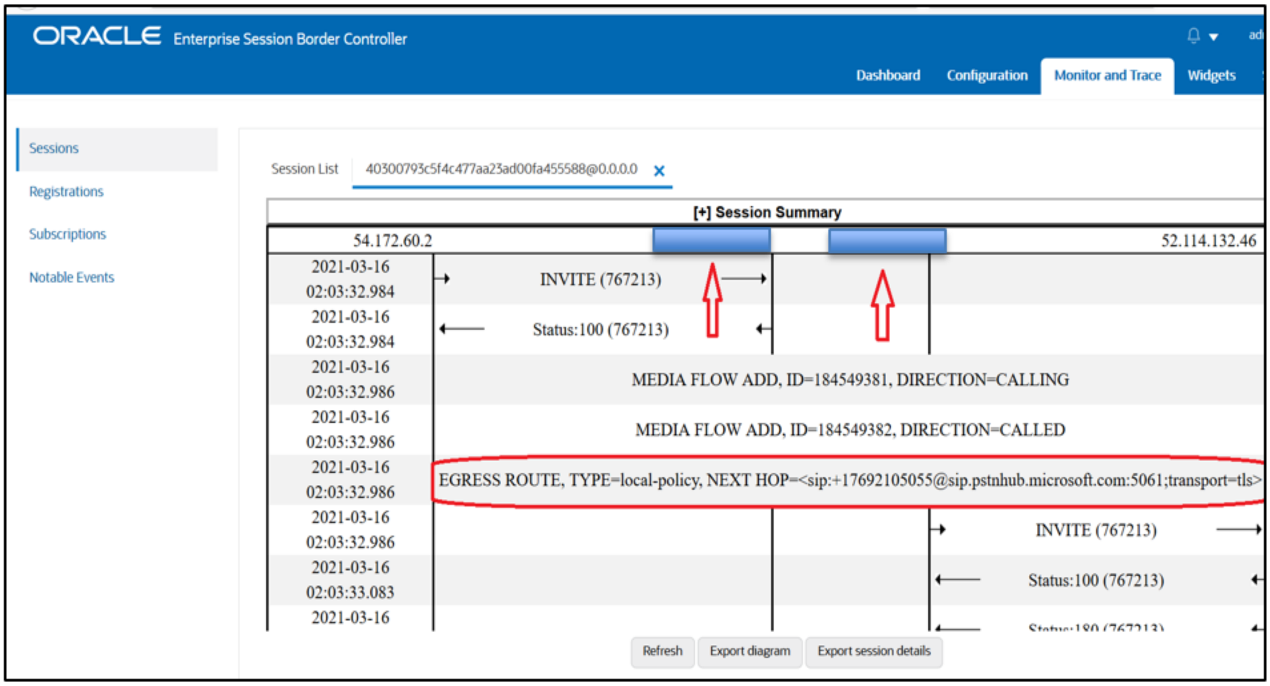
2021-03-16 02:02:16.623 MEDIA FLOW LATCH, ID=167772166, DIRECTION=CALLED

2021-03-16 02:02:16.625 MEDIA FLOW MODIFY, ID=167772165, DIRECTION=CALLING

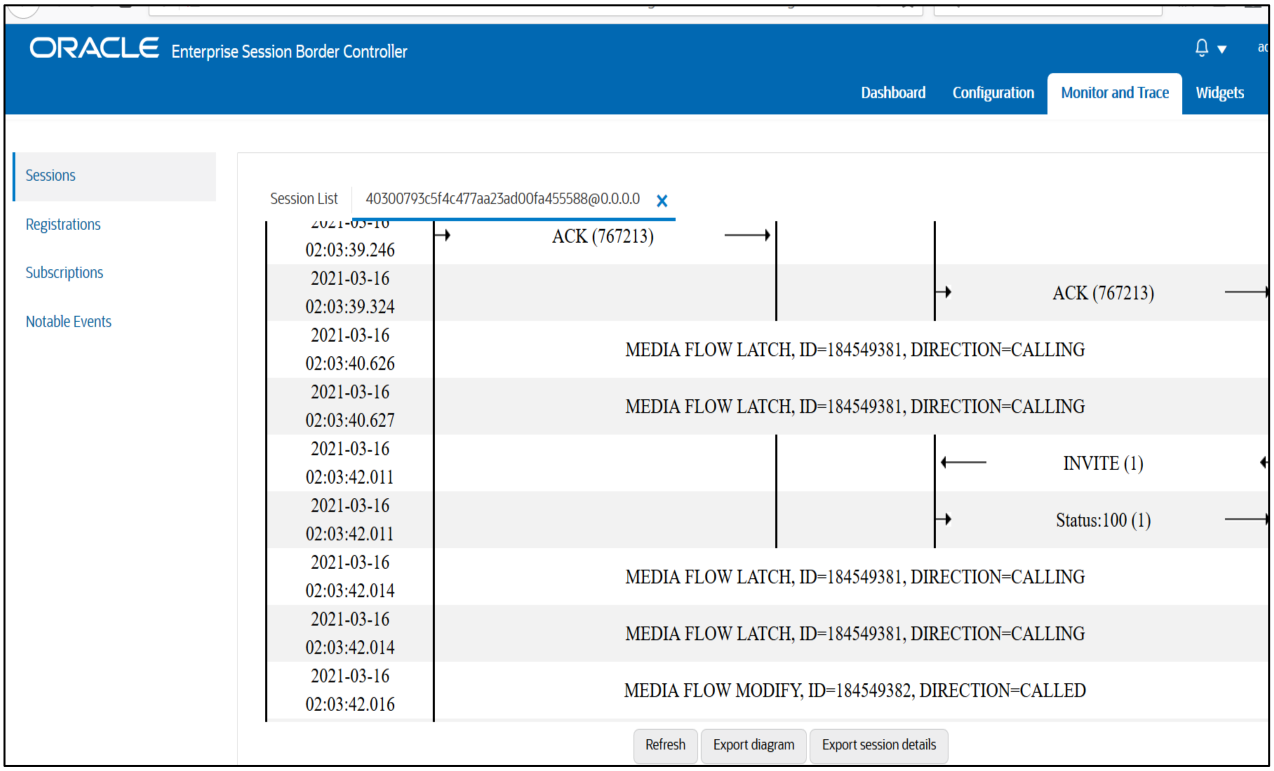
2021-03-16 02:02:16.625 MEDIA FLOW MODIFY, ID=167772166, DIRECTION=CALLED

2021-03-16 02:02:16.625 INVITE (2)

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



```
54.172.60.2                                                                 52.114.132.46
2021-03-16 02:03:32.984  INVITE (767213)
2021-03-16 02:03:32.984  Status:100 (767213)
2021-03-16 02:03:32.986  MEDIA FLOW ADD, ID=184549381, DIRECTION=CALLING
2021-03-16 02:03:32.986  MEDIA FLOW ADD, ID=184549382, DIRECTION=CALLED
2021-03-16 02:03:32.986  EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:+17692105055@sip.pstnhub.microsoft.com:5061;transport=tls>
2021-03-16 02:03:32.986  INVITE (767213)
2021-03-16 02:03:33.083  Status:100 (767213)
2021-03-16               Status:180 (767213)
```



```
2021-03-16 02:03:39.246  ACK (767213)
2021-03-16 02:03:39.324  ACK (767213)
2021-03-16 02:03:40.626  MEDIA FLOW LATCH, ID=184549381, DIRECTION=CALLING
2021-03-16 02:03:40.627  MEDIA FLOW LATCH, ID=184549381, DIRECTION=CALLING
2021-03-16 02:03:42.011  INVITE (1)
2021-03-16 02:03:42.011  Status:100 (1)
2021-03-16 02:03:42.014  MEDIA FLOW LATCH, ID=184549381, DIRECTION=CALLING
2021-03-16 02:03:42.014  MEDIA FLOW LATCH, ID=184549381, DIRECTION=CALLING
2021-03-16 02:03:42.016  MEDIA FLOW MODIFY, ID=184549382, DIRECTION=CALLED
```

Appendix A

Following are the test cases that are executed as part of Teams Direct Routing Enterprise Model with the Twilio Elastic SIP Trunk (PSTN user).

Serial Number	Test Cases Executed	Result
1	Device supports ptime of 20 ms for an inbound call to Twilio Elastic SIP Trunk user	Pass
2	Device sends its own FQDN in the contact header	Pass
3	Twilio Elastic SIP Trunk user accepts call from Teams user where the user's calling line identity is set to anonymous	Pass
4	Teams user places inbound call from Twilio Elastic SIP Trunk user on hold and then resumes	Pass
5	Teams user places outbound call to Twilio Elastic SIP Trunk user on hold and then resumes	Pass
6	Teams user places inbound call from Twilio Elastic SIP Trunk user on hold for over 15/30 minutes and then resumes	Pass
7	Teams 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
8	Inbound Twilio Elastic SIP Trunk call to Teams blind transferred to second Teams User	Pass
9	Outbound Twilio Elastic SIP Trunk call from Teams user blind transferred to second Teams User	Pass
10	Inbound Twilio Elastic SIP Trunk Call to Teams consultatively transferred to Teams User	Pass
11	Outbound Twilio Elastic SIP Trunk call from Teams user consultatively transferred to Teams User	Pass
12	Twilio Elastic SIP Trunk user calls Teams user that simultaneously rings second TEAMS/PSTN user and second user answers	Pass
13	Twilio Elastic SIP Trunk user calls Teams user that is forwarded to second PSTN/TEAMS user	Pass
14	Teams user makes outbound call to Twilio Elastic SIP Trunk user and makes a conference call by adding another Teams user.	Pass
15	Twilio Elastic SIP Trunk user makes outbound call to Teams user and Teams user makes a conference call by adding another Teams user.	Pass

16	Teams user calls an IVR number and navigates through the IVR menu after call connection	Pass
17	Teams user calls into an external conference bridge and pastes a string of conference ID into Teams which is recognized by Device and IVR	Pass
18	Device sends comfort noise packets to Direct Routing interface when Twilio Elastic SIP Trunk user mutes an outbound call	Pass
19	Device sends comfort noise packets to Direct Routing interface when Twilio Elastic SIP Trunk user mutes an inbound call	Pass
20	Teams user mutes inbound call from Twilio Elastic SIP Trunk user and then unmutes	Pass
21	Teams user mutes outbound call made to Twilio Elastic SIP Trunk user and then unmutes	Pass
22	Twilio Elastic SIP Trunk user mutes inbound call from Teams user user and then unmutes	Pass
23	Twilio Elastic SIP Trunk user mutes outbound call made to Teams user user and then unmutes	Pass
24	Twilio Elastic SIP Trunk User disconnects outbound call to Teams user before it is answered	Pass
25	Teams user disconnects outbound call to Twilio Elastic SIP Trunk user before it is answered	Pass
26	Twilio Elastic SIP Trunk user disconnects an inbound connected call	Pass
27	Twilio Elastic SIP Trunk User disconnects an outbound connected call	Pass
28	Teams user disconnects an inbound connected call	Pass
29	Teams user disconnects an outbound connected call	Pass
30	Device must indicate support for SRTCP multiplexing by including the a=rtcp-mux attribute in the offer	Pass
31	Device must respond with a=rtcp-mux attribute in the SDP response if the offer contains the same attribute	Pass
32	SBC sends the X-MS-SBC header in Options and the Invite messages towards the Teams user	Pass

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