Oracle SBC integration with Genesys PureCloud BYOC and Microsoft Teams Direct Routing

Technical Application Note

ORACLE
COMMUNICATIONS

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

As a best practice always follow the latest Application note available on the Oracle TechNet Website.
https://www.oracle.com/technical-resources/documentation/acme-packet.html

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with Genesys PureCloud and Microsoft Teams	07 July 2021
1.1	Oracle Public IP Addresses masked	18 Nov 2021
1.2	Removed sip-all FQDN Added New Access Control	12 Jan 2022
1.3	Added New Section PureCloud Configuration Assistant	27 Jan 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 Genesys PureCloud and Microsoft Teams Direct Routing.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Genesys PureCloud and Microsoft Teams. The Application note focuses on the steps required to create a SIP connection between PureCloud BYOC, Oracle SBC and Microsoft Teams through which voice communication is possible between PureCloud and MS Teams Direct Routing Users.

It should be noted that the SBC configuration provided in this guide focuses strictly on the Genesys PureCloud and Microsoft Teams related parameters. Microsoft Teams Direct Routing is the Microsoft’s BYOC so the calls To and From MS Teams to PureCloud are terminated via a carrier SIP Trunk. The steps required to configure the Carrier Trunk are specific to individual customers and are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

You can follow our Application Note - https://www.oracle.com/a/otn/docs/oracle-sbc-with-genesys-pure-cloud-and-twillio-sip-trunk.pdf as a reference to configure the Twilio SIP Trunk with Oracle SBC.

Related documentation can be found below –

2.1. 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

2.2. Genesys PureCloud

The Genesys PureCloud solution provides flexibility and interoperability to the PureCloud suite of voice services by allowing you to define SIP trunks between the PureCloud AWS-based Edge and Media Tier and third-party carriers over the public Internet.

https://help.mypurecloud.com/articles/about-byoc-cloud/

3. Requirements

- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version. The solution contained within this document has been tested using Oracle Communication SBC release **cz840p5a**.
- Genesys Pure Cloud BYOC (Cloud or Premise)
- Microsoft Teams Direct Routing

✓ *Tenant -Microsoft O365 Tenant with customer domain registered.*

✓ *License -Microsoft Phone System • Microsoft Teams + Skype for Business Plan 2 if included in Licensing Sku*

✓ *Oracle SBC FQDN and Public Trusted Certificates for Direct Routing.*

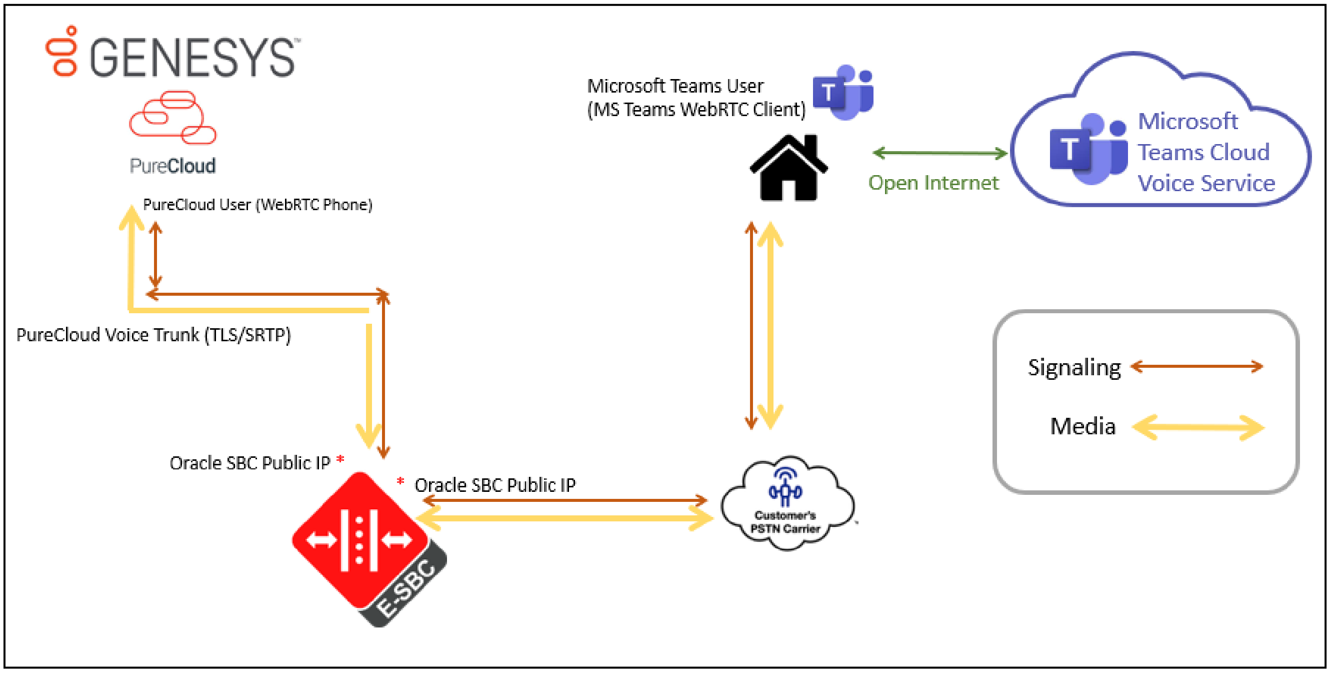
Follow Below Links for detailed MS Teams Direct Routing Requirements

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan
https://www.oracle.com/a/otn/docs/final_version_nonmedia_bypass-10-05-2021.pdf

Note: Microsoft Teams Direct Routing Supports multiple configuration models. Please choose appropriate model depending upon your specific requirement. Detailed information about Microsoft Teams Direct Models with Oracle SBC can be found under Microsoft Teams Subsection -

https://www.oracle.com/technical-resources/documentation/acme-packet.html

3.3. Architecture



Above figure illustrates the connection between Genesys PureCloud, Oracle SBC and Microsoft Teams Direct Routing. Both PureCloud and Microsoft Teams are connected to the Oracle SBC Public FQDN /IP

Oracle SBC which is certified with Microsoft Teams Direct Routing is used to steer the signaling, media to, and From the PureCloud to Microsoft Teams and vice versa. The Scenario represents a use-case where SBC is hosted in On Premise Network however the Oracle SBC can also be hosted in Public Cloud depending upon the use-case requirement.

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

Phase 1 – Configuring Genesys PureCloud

Phase 2 – Configuring Microsoft Teams Direct Routing

Phase 3 – Configuring Oracle Session Border Controller.

Note 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. You can configure any publicly routable IPs for these sections as per specific network architecture needs.

4. Configure Genesys PureCloud

The steps outlined below is the minimum required configuration to pair your SBC with Genesys PureCloud. work with your Genesys representative to implement the correct configuration for your specific environment.

Note: The document only includes the steps required on Genesys PureCloud to communicate with Oracle SBC as an External Trunk. Additional configuration may apply which may not be covered in this document. Please work with your Genesys representative for the most optimal Pure Cloud configuration as per your requirement.

To implement PureCloud BYOC with Oracle SBC, you use the Telephony Admin UI to create SIP trunks between the PureCloud Media Tier resources in AWS and the Oracle SBC. Oracle SBC connects to the PureCloud to Microsoft Teams over the Direct Routing based infrastructure.

The Oracle Enterprise SBC will act as an intermediary between Microsoft Teams and Genesys PureCloud. The SBC is configured to broker calls as a back-to-back user agent (B2BUA) between the two systems. The Carrier DIDs are assigned to users on PureCloud System and Microsoft Teams who can originate and accept the calls. These calls traverse through Oracle SBC with which we can implement several security and additional features as per our requirement.

For the purpose of this Application note, the connection between Oracle SBC and Genesys PureCloud is set over a Secure TLS 1.2 and SRTP based connection.

4.1 External Trunk Configuration

A trunk connects a communication service to a PureCloud telephony connection option and facilitates point-to-point communication. We will configure Oracle Enterprise SBC as an external Trunk on the PureCloud Portal. Detailed steps to configure the external trunk can be found here-

https://help.mypurecloud.com/articles/create-a-byoc-cloud-trunk/

To configure the external Trunk, Navigate to

Admin> Telephony>Trunks> **External Trunks** > **Create New.**

4.1.1 Create a new External Trunk

Type: BYOC Carrier Trunk

Protocol: TLS (TCP and UDP are also available)

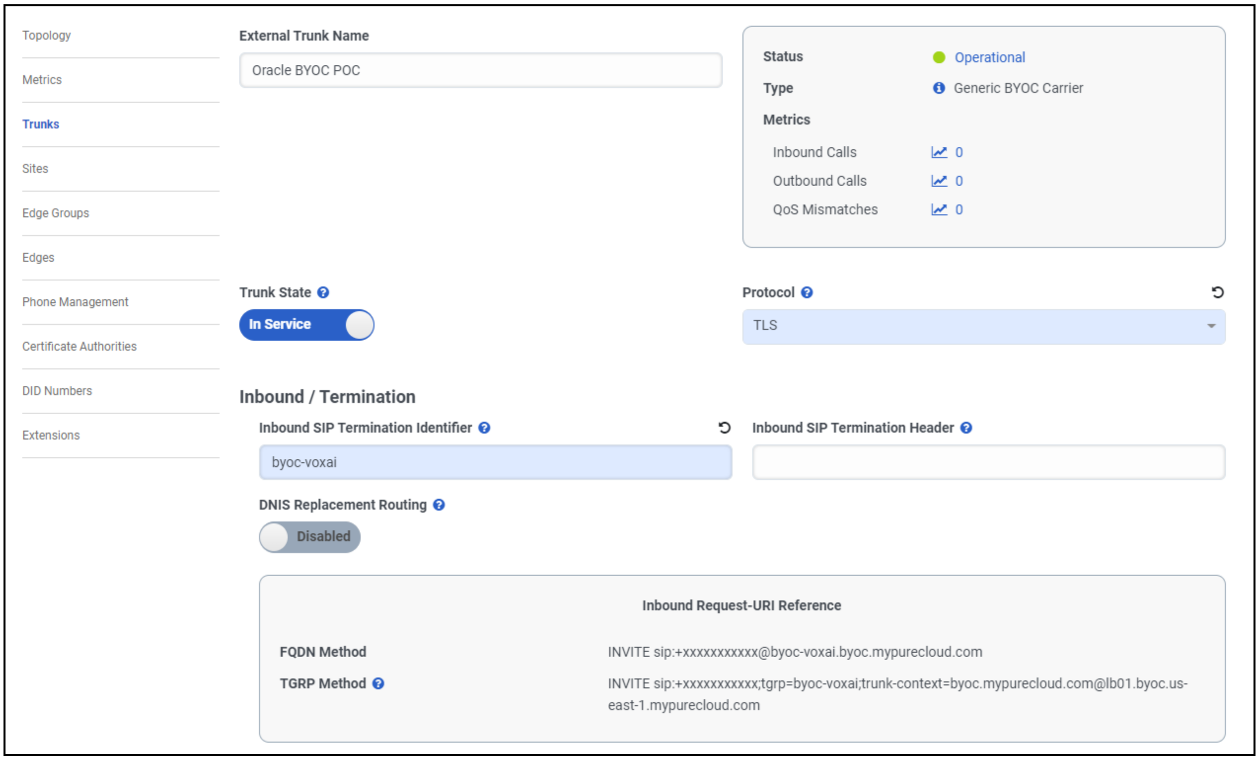
4.1.2 Set Inbound SIP Termination Identifier

Inbound SIP Termination Identifier – is the DNS Name we will configure on the Oracle SBC and will be used to route calls towards PureCloud. Here a vanity FQDN **byoc-voxai.byoc.mypurecloud.com** is generated with the inbound sip termination identifier as byoc-voxai. This FQDN resolves to the following IP Addresses of the PureCloud AWS US Data Centers.

Inbound SIP Termination Identifier: byoc-voxai
Ex: INVITE sip:+xxxxxxxxxxx@byoc-voxai.byoc.mypurecloud.com
Protocol: TLS
Genesys Reference - https://help.mypurecloud.com/articles/tls-trunk-transport-protocol-specification/

### Genesys Cloud IP List

IP Addresses	Load Balancer DNS Names
52.203.12.137	lb01.byoc.us-east-1.mypurecloud.com
54.82.241.192	lb02.byoc.us-east-1.mypurecloud.com
54.82.241.68	lb03.byoc.us-east-1.mypurecloud.com
54.82.188.43	lb04.byoc.us-east-1.mypurecloud.com



External Trunk Name: Oracle BYOC POC

Status: ● Operational
Type: Generic BYOC Carrier
Metrics
Inbound Calls: 0
Outbound Calls: 0
QoS Mismatches: 0

Trunk State: In Service

Protocol: TLS

Inbound / Termination

Inbound SIP Termination Identifier: byoc-voxai

Inbound SIP Termination Header:

DNIS Replacement Routing: Disabled

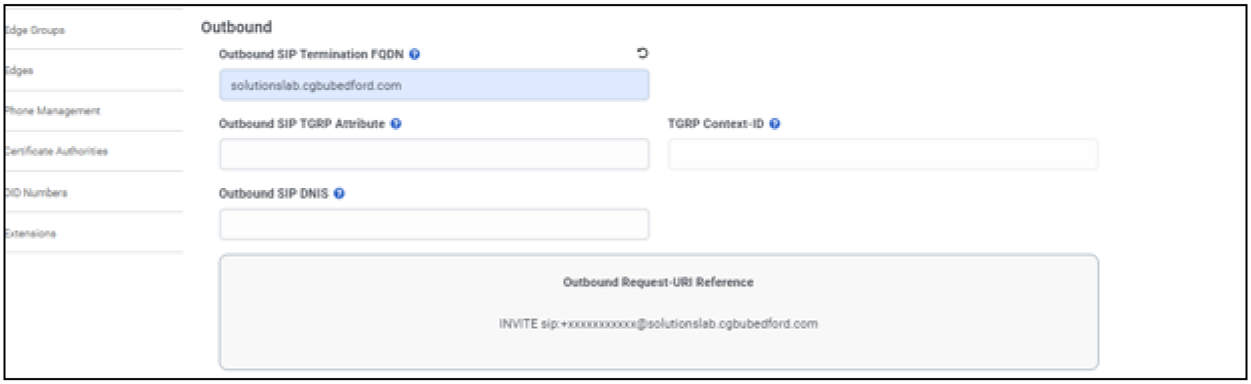
Inbound Request-URI Reference

FQDN Method: INVITE sip:+xxxxxxxxxxx@byoc-voxai.byoc.mypurecloud.com

TGRP Method: INVITE sip:+xxxxxxxxxxx;tgrp=byoc-voxai;trunk-context=byoc.mypurecloud.com@lb01.byoc.us-east-1.mypurecloud.com

4.1.3 Set Outbound SIP Servers or Proxies

Outbound SIP Termination FQDN is the Public FQDN of the Oracle SBC.



Outbound

Outbound SIP Termination FQDN: solutionslab.cgbubedford.com

Outbound SIP TGRP Attribute:

TGRP Context-ID:

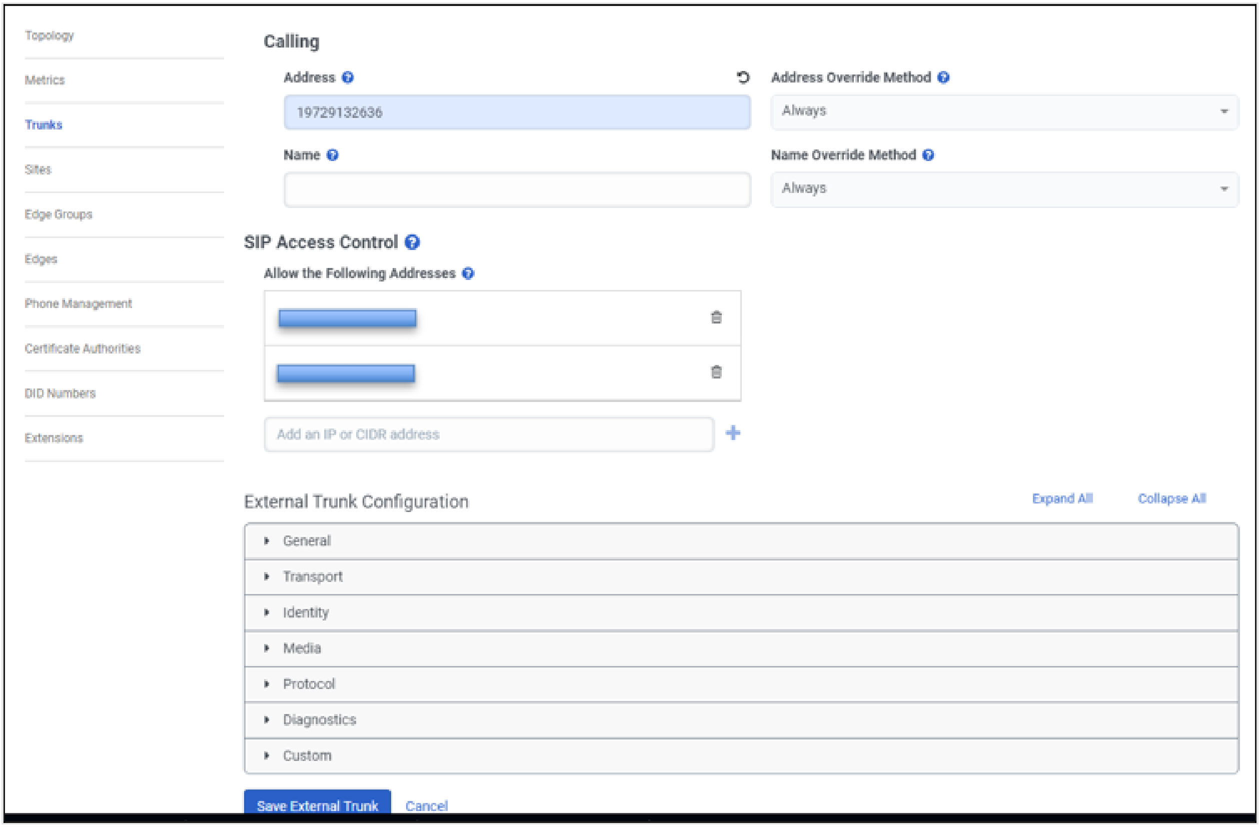
Outbound SIP DNIS:

Outbound Request-URI Reference

INVITE sip:+xxxxxxxxxxx@solutionslab.cgbubedford.com

4.1.4 Set Calling Address

The Calling Address is the default number used as an outbound ANI when a call is placed on the Trunk. In case a user has assigned the optionally DID that number can be used in place of the default number.



Calling

Address: 19729132636

Address Override Method: Always

Name:

Name Override Method: Always

SIP Access Control

Allow the Following Addresses

[redacted]

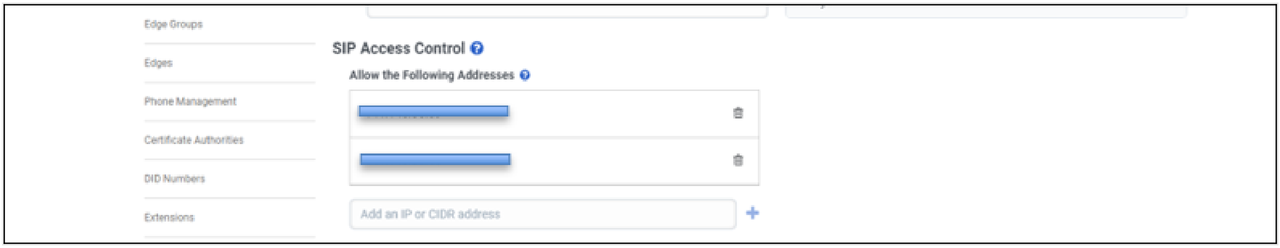
[redacted]

Add an IP or CIDR address +

External Trunk Configuration

4.1.5 Set SIP Access Control

Whitelist the Oracle SBC IP addresses under the SIP Access Control. (DNS name not supported)



SIP Access Control

Allow the Following Addresses

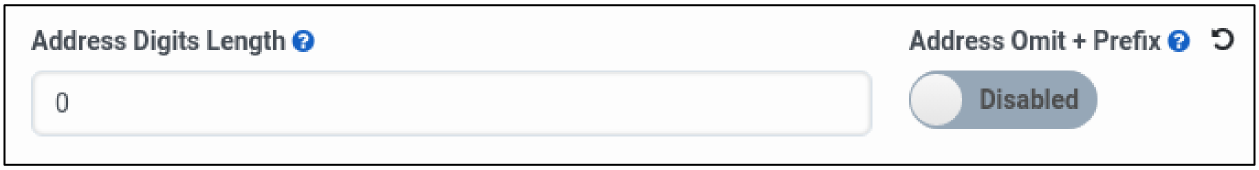
[redacted]

[redacted]

Add an IP or CIDR address

4.1.6 Enable E.164 format

By default, calls sent out of trunks do not include the "+" prefix, to enable E.164 number formatting disable omitting the "+". The settings can be found in the external trunk configuration, under the Identity Section. This setting is available for both inbound and outbound calls.



Address Digits Length: 0

Address Omit + Prefix: Disabled

4.2 Site Configuration.

A site is a list of rules for routing calls. Objects such as phones associated with a site share the same rules. When a user makes a call from a phone, the system looks up the site and the call type in order to route the call to the best outbound phone line, or endpoint. Phones that are associated with a site are usually located in the same general area and have the same general purpose. A site is used to link trunk with Pure Cloud Edge(s).

Detailed steps to configure the Site can be found here-

https://help.mypurecloud.com/articles/create-site-genesys-cloud-voice/

4.2.1 Create a New Site

To Create a site, Navigate to **Admin>Telephony>Sites> Create New**.

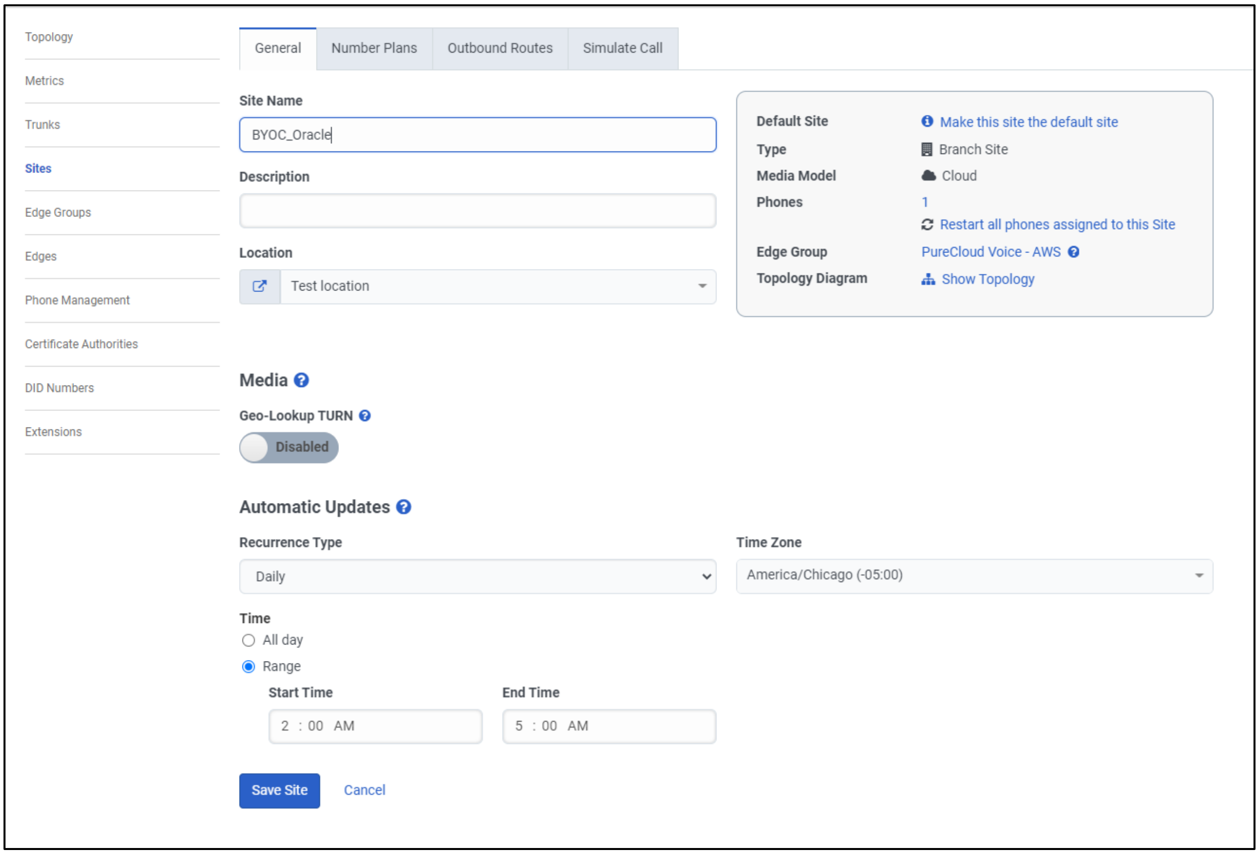
Type a name into the **Site Name** box.

From the **Location** list, select a location for your site.

From the **Time Zone** list, select your time zone.

Under **Media Model**, select **Cloud**.

Click **Create Site**.



Site Name: BYOC_Oracle

Description:

Location: Test location

Default Site	Make this site the default site
Type	Branch Site
Media Model	Cloud
Phones	1 Restart all phones assigned to this Site
Edge Group	PureCloud Voice - AWS
Topology Diagram	Show Topology

Media

Geo-Lookup TURN: Disabled

Automatic Updates

Recurrence Type: Daily

Time Zone: America/Chicago (-05:00)

Time

○ All day

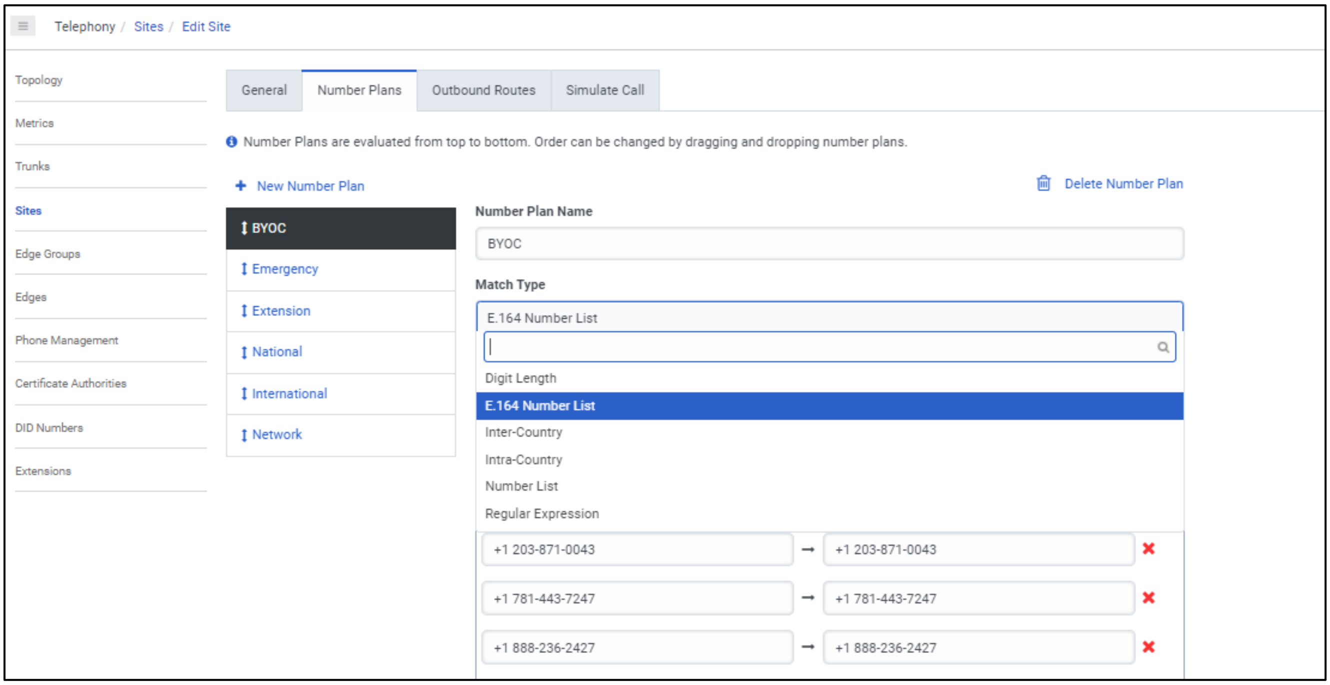
● Range

Start Time: 2 : 00 AM

End Time: 5 : 00 AM

4.2.2 Number Plans & Classifications

PureCloud provides a set of default number plans that work for most users. We can modify this numbering Plan as per our specific need. We have created a new Numbering Plan “BYOC” where we will define the Numbers that take the route associated with this trunk. You can assign specific numbers, a range or numbers or even use Regex for routing.



Number Plans are evaluated from top to bottom. Order can be changed by dragging and dropping number plans.

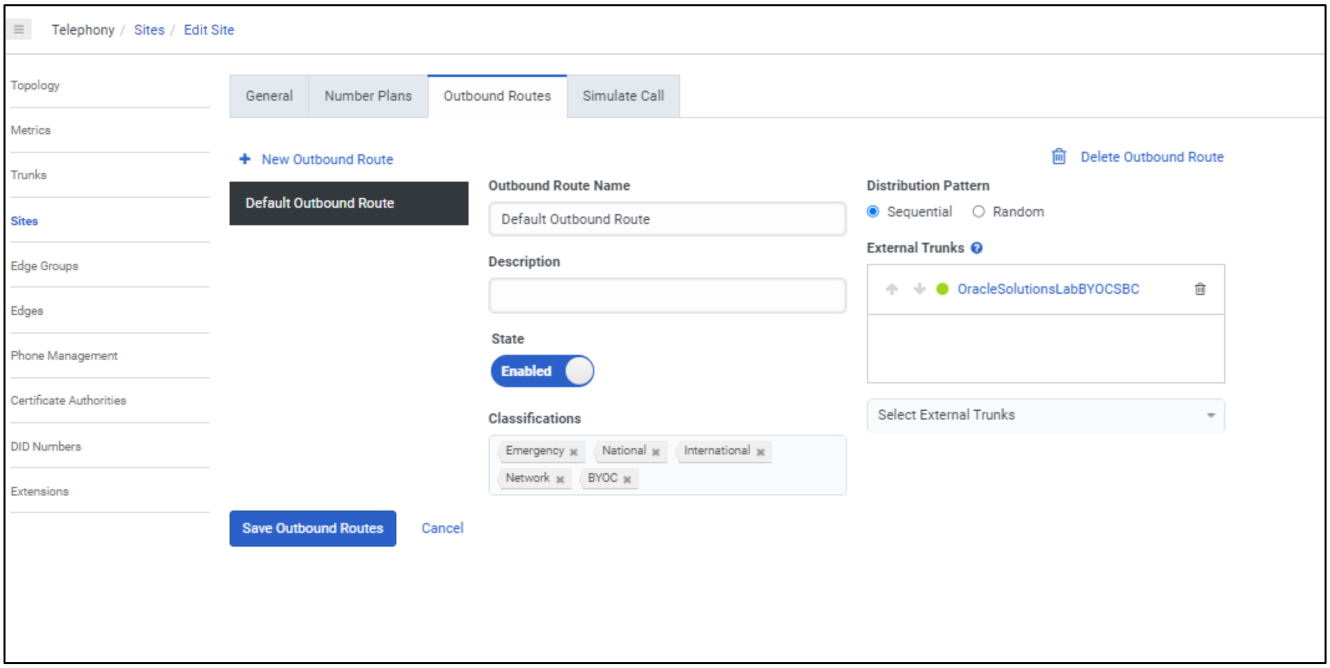
Number Plan Name: BYOC

Match Type: E.164 Number List

+1 203-871-0043	→	+1 203-871-0043
+1 781-443-7247	→	+1 781-443-7247
+1 888-236-2427	→	+1 888-236-2427

4.2.3 Configure outbound route

The Outbound route binds the numbering plans with the trunk. The classification created in numbering plan should be assigned to the Outbound Route associated with the external trunk.



Outbound Route Name: Default Outbound Route

Description:

State: Enabled

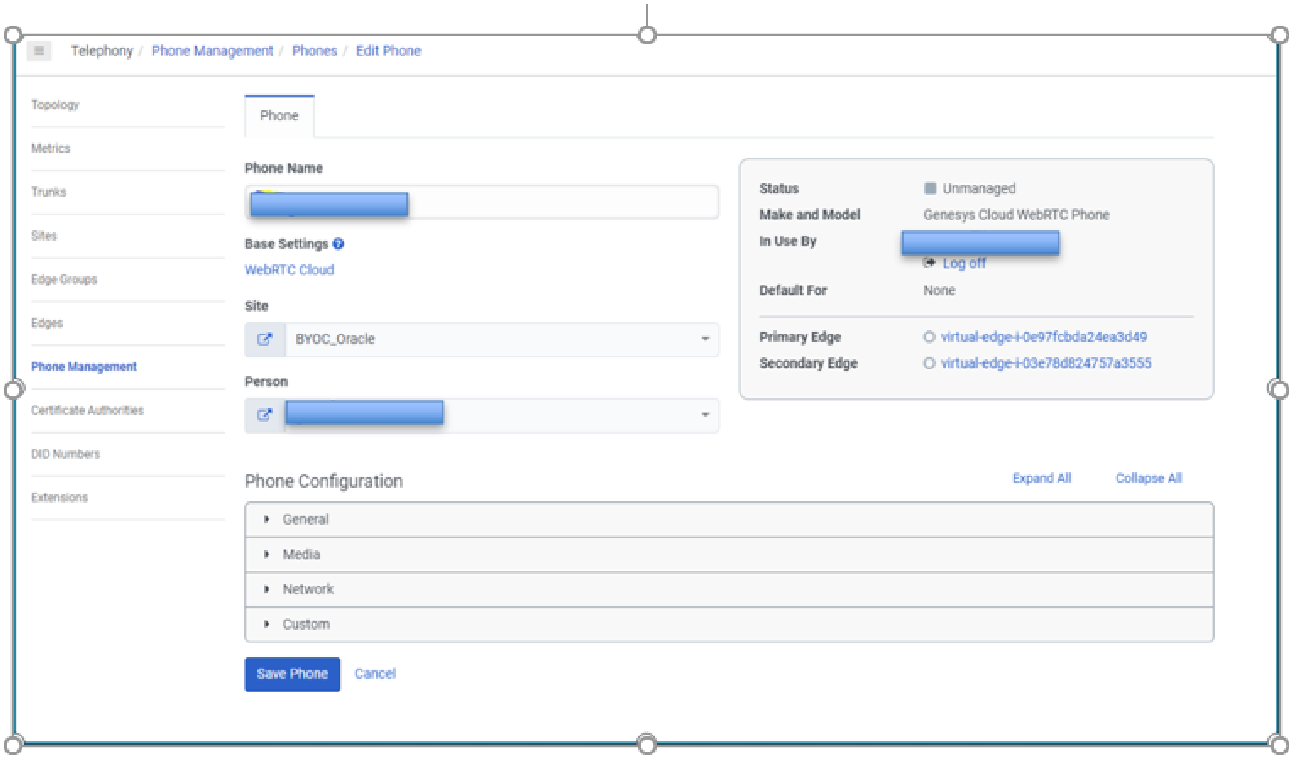
Classifications: Emergency, National, International, Network, BYOC

Distribution Pattern: ● Sequential ○ Random

External Trunks: OracleSolutionsLabBYOCSBC

4.2.4 Phone configuration

Below is an example of a WebRTC Phone configuration which will be used for calling purpose and is assigned to the Users. The WebRTC Phone is assigned to the Oracle BYOC Site.



Telephony / Phone Management / Phones / Edit Phone

Phone Name: [redacted]

Base Settings: WebRTC Cloud

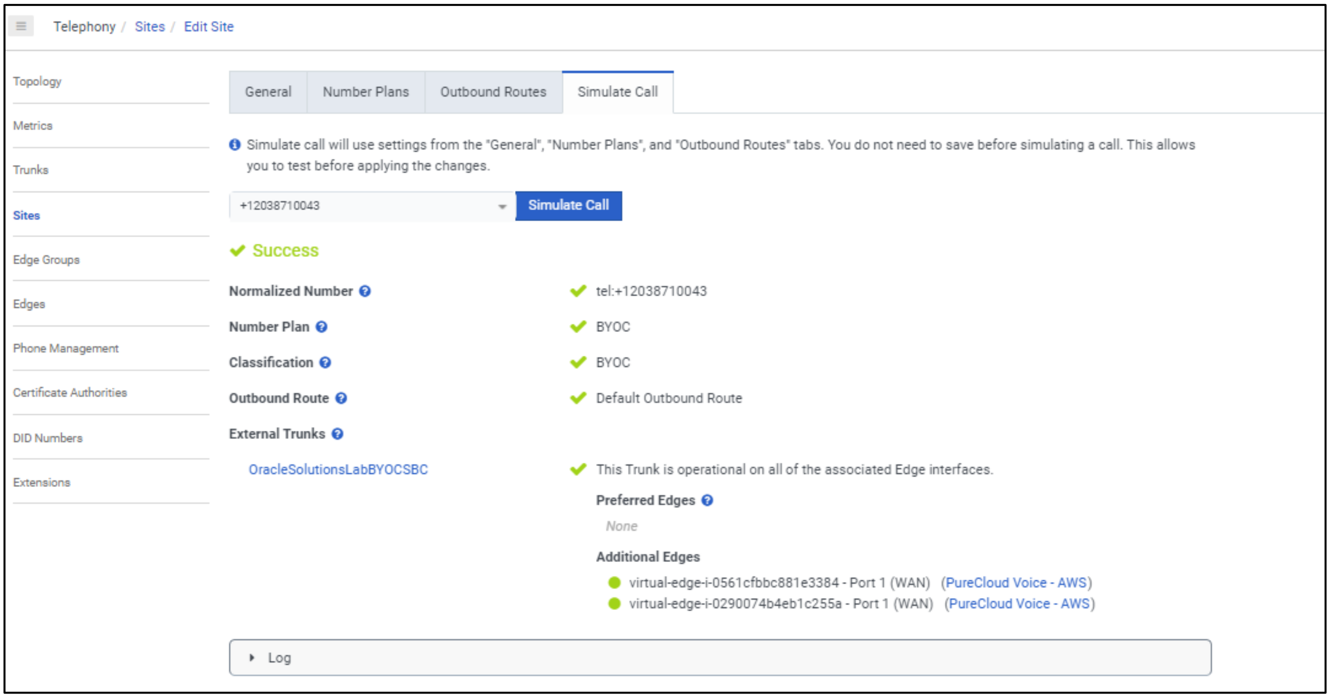
Site: BYOC_Oracle

Person: [redacted]

Status	Unmanaged
Make and Model	Genesys Cloud WebRTC Phone
In Use By	[redacted] Log off
Default For	None
Primary Edge	○ virtual-edge-i-0e97fcbda24ea3d49
Secondary Edge	○ virtual-edge-i-03e78d824757a3555

4.2.5 Simulate call

Genesys PureCloud provides a neat feature to test and validate the routing of calls for troubleshooting purpose. Below is an example for a call to BYOC type number classification on this Site. Success indicates a successful routing response.



Telephony / Sites / Edit Site

Simulate call will use settings from the "General", "Number Plans", and "Outbound Routes" tabs. You do not need to save before simulating a call. This allows you to test before applying the changes.

+12038710043 — Simulate Call

✓ Success

Normalized Number	✓ tel:+12038710043
Number Plan	✓ BYOC
Classification	✓ BYOC
Outbound Route	✓ Default Outbound Route
External Trunks	
OracleSolutionsLabBYOCSBC	✓ This Trunk is operational on all of the associated Edge interfaces.

Preferred Edges

None

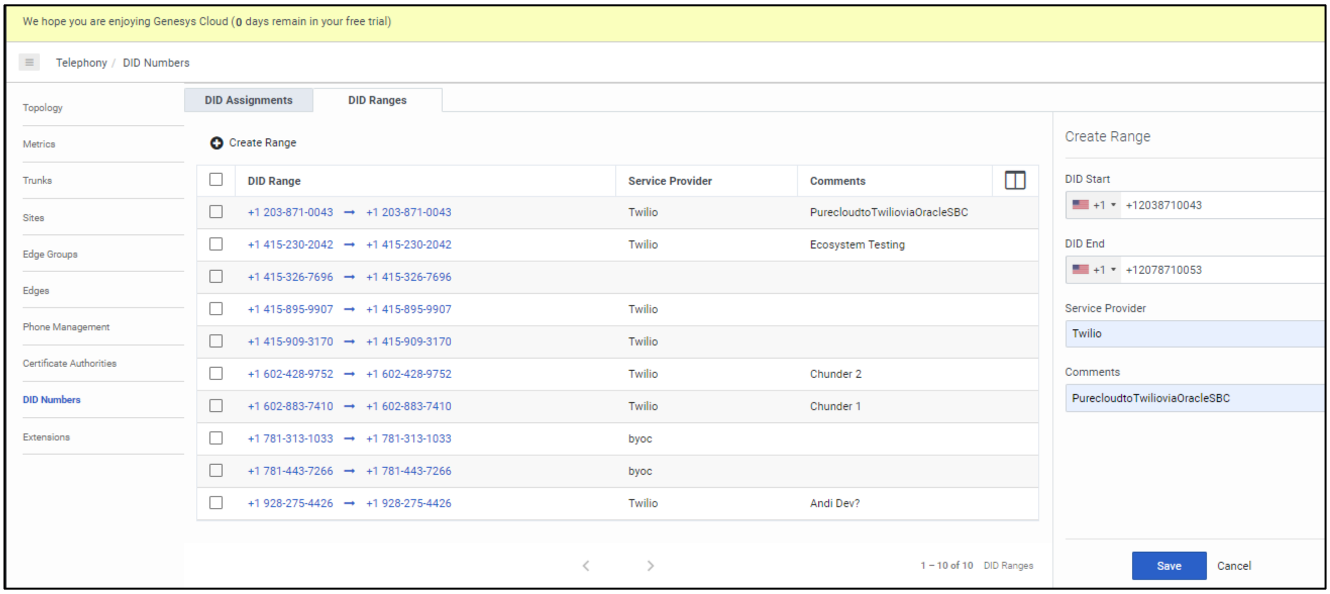
Additional Edges

● virtual-edge-i-0561cfbbc881e3384 - Port 1 (WAN) (PureCloud Voice - AWS)
● virtual-edge-i-0290074b4eb1c255a - Port 1 (WAN) (PureCloud Voice - AWS)

4.3 DID Assignment

4.3.1 Create DID Range

To create a New DID Range or Number Navigate to **Admin.**> **Telephony** > **DID Numbers**> **Create Range.** Provide the DID range and Service Provider name and Click Save



We hope you are enjoying Genesys Cloud (0 days remain in your free trial)

Telephony / DID Numbers

□	DID Range	Service Provider	Comments
□	+1 203-871-0043 → +1 203-871-0043	Twilio	PurecloudtoTwilioviaOracleSBC
□	+1 415-230-2042 → +1 415-230-2042	Twilio	Ecosystem Testing
□	+1 415-326-7696 → +1 415-326-7696		
□	+1 415-895-9907 → +1 415-895-9907	Twilio	
□	+1 415-909-3170 → +1 415-909-3170	Twilio	
□	+1 602-428-9752 → +1 602-428-9752	Twilio	Chunder 2
□	+1 602-883-7410 → +1 602-883-7410	Twilio	Chunder 1
□	+1 781-313-1033 → +1 781-313-1033	byoc	
□	+1 781-443-7266 → +1 781-443-7266	byoc	
□	+1 928-275-4426 → +1 928-275-4426	Twilio	Andi Dev?

1 – 10 of 10 DID Ranges

Create Range

DID Start: +1 +12038710043

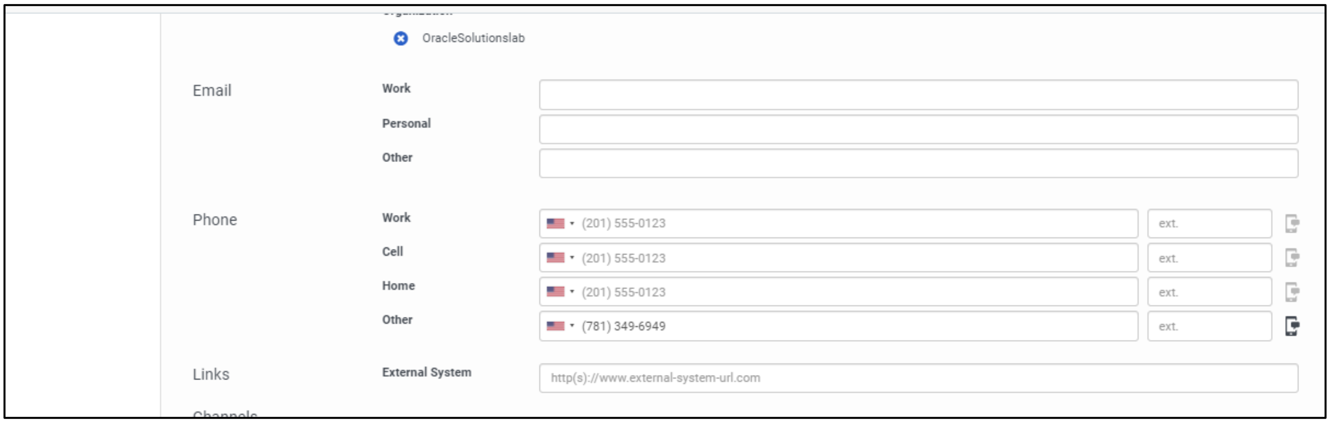
DID End: +1 +12078710053

Service Provider: Twilio

Comments: PurecloudtoTwilioviaOracleSBC

4.3.2 Assign DID to User.

On users' profile field, one of the DID can be assigned to PureCloud User as Other Number. The Oracle SBC is configured to send calls from external world to this DID number which will terminate to the user on PureCloud.



OracleSolutionslab

Email
Work:
Personal:
Other:

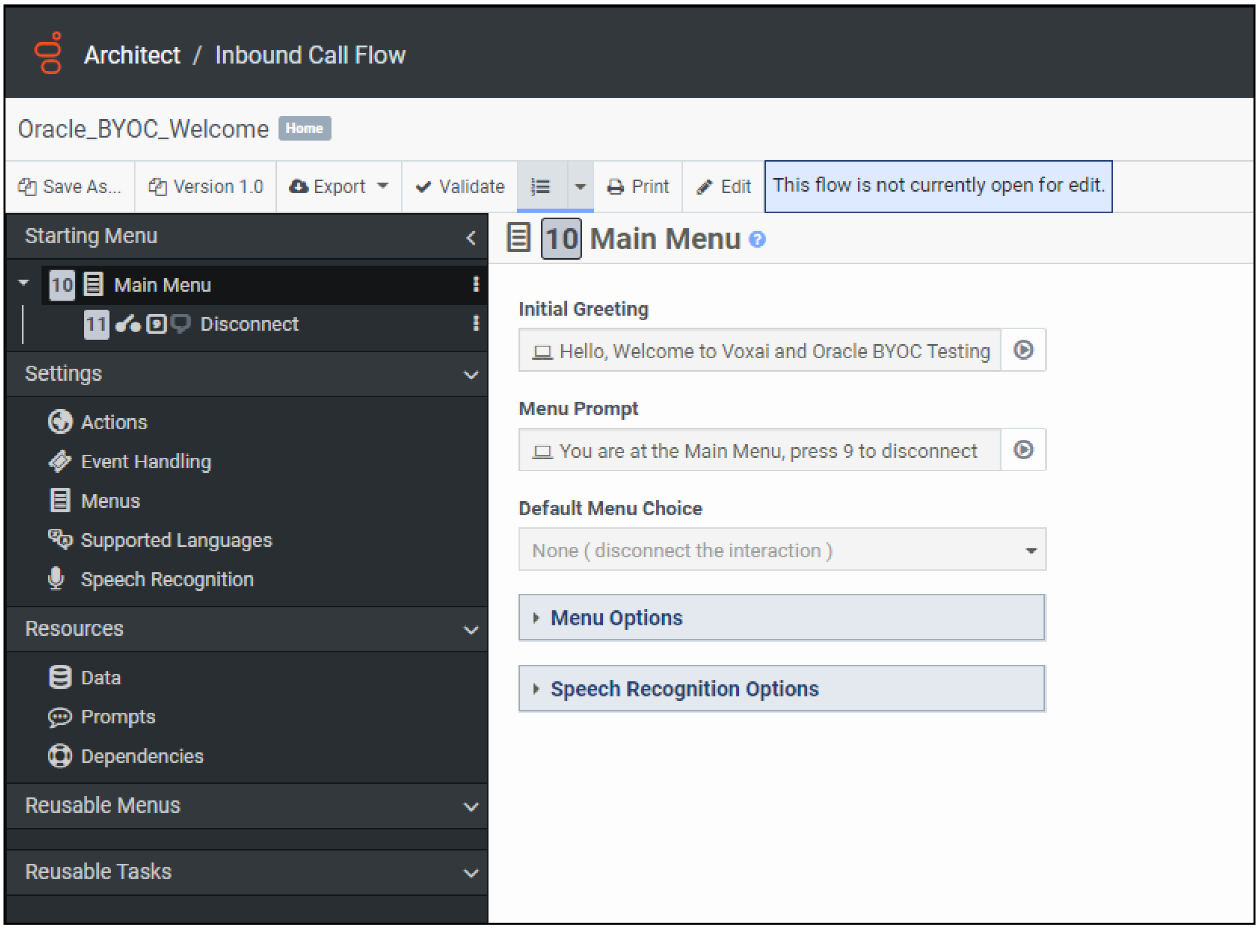
Phone
Work: (201) 555-0123 ext.
Cell: (201) 555-0123 ext.
Home: (201) 555-0123 ext.
Other: (781) 349-6949 ext.

Links
External System: http(s)://www.external-system-url.com

Channels

4.4. Architect flow for inbound welcome prompt

Below is an example for an Architect Flow for inbound Voice Prompt which will be used for inbound calls from Microsoft Teams to Genesys PureCloud via Oracle SBC.



Initial Greeting: Hello, Welcome to Voxai and Oracle BYOC Testing

Menu Prompt: You are at the Main Menu, press 9 to disconnect

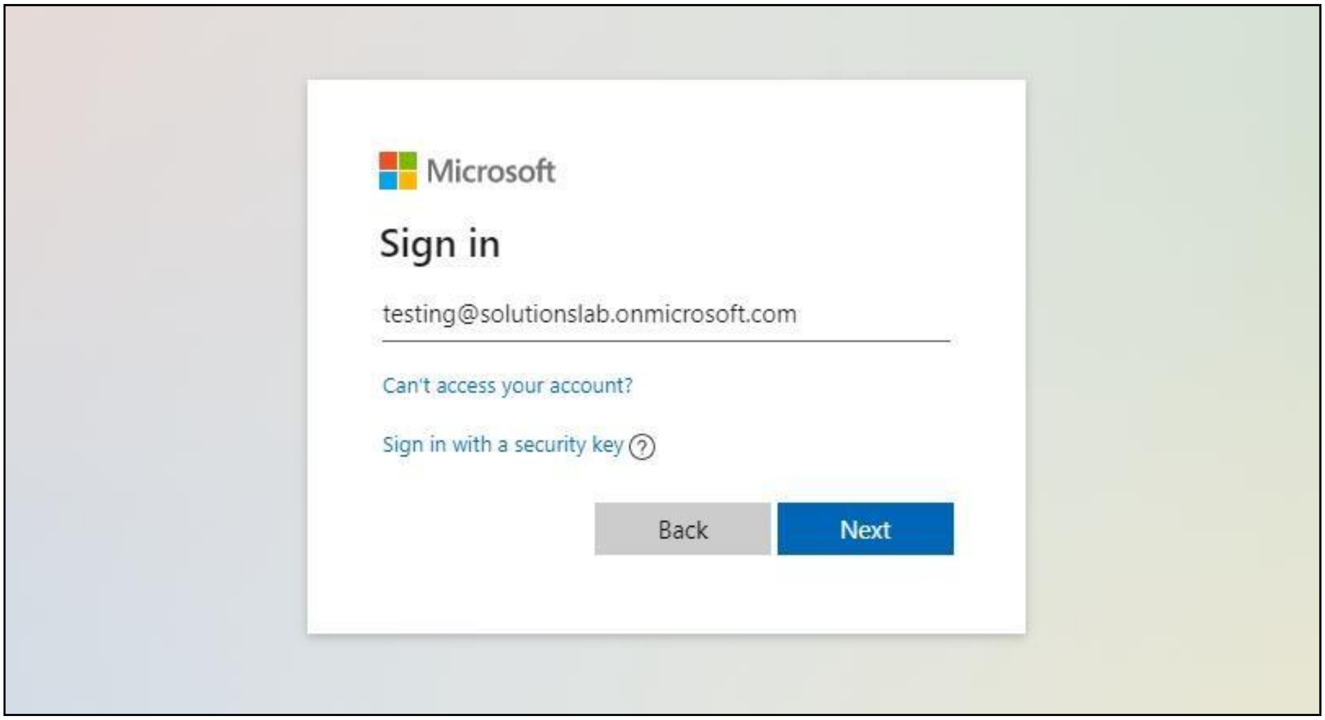
Default Menu Choice: None (disconnect the interaction)

5. 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.**

5.1. Access Teams Admin center

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



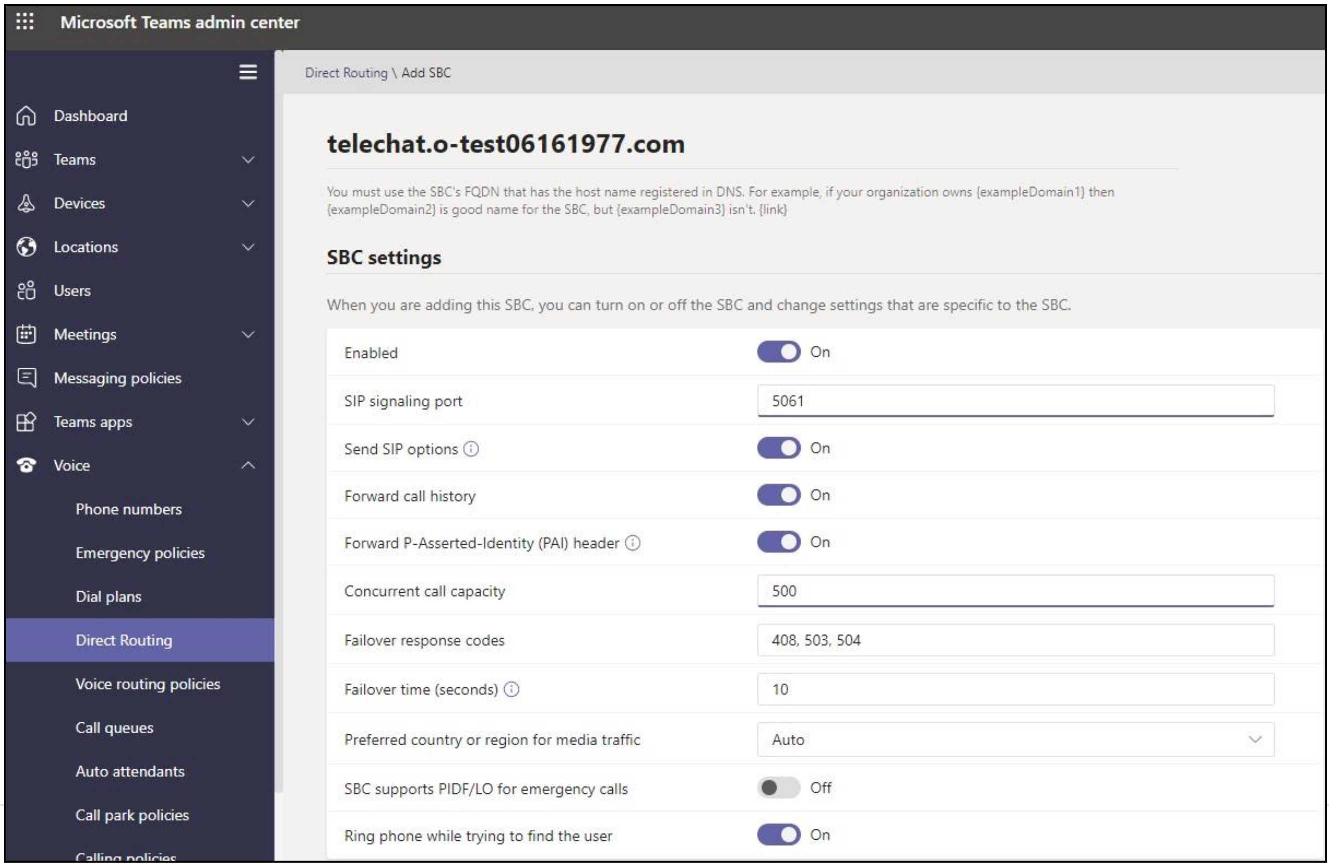
Microsoft

Sign in

testing@solutionslab.onmicrosoft.com

5.2. Configure Online PSTN Gateway

Configuration Path: Voice/Direct Routing/SBC



telechat.o-test06161977.com

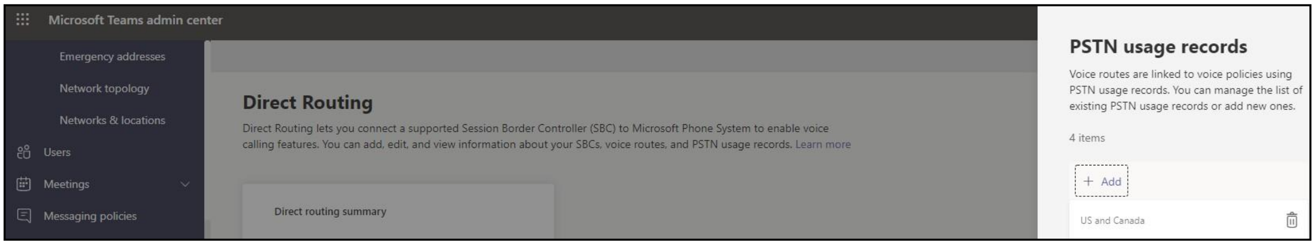
You must use the SBC's FQDN that has the host name registered in DNS. For example, if your organization owns {exampleDomain1} then {exampleDomain2} is good name for the SBC, but {exampleDomain3} isn't. {link}

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 Add, Type US and Canada, next, click Apply



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

Direct routing summary

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.

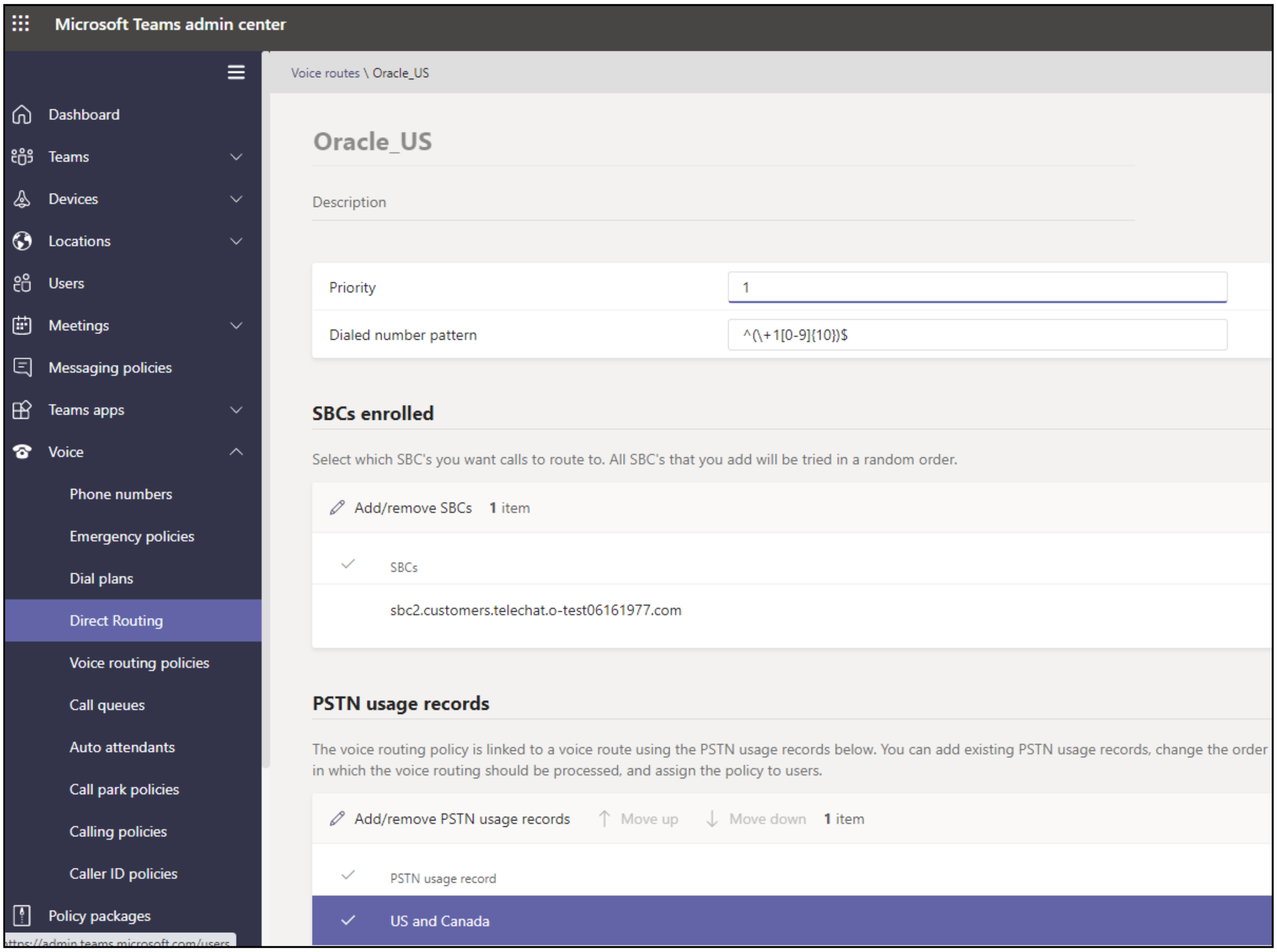
4 items

+ Add

US and Canada

5.4. Configure Online Voice Routes

Configuration Path: Voice/Direct Routing/Voice Routes



Voice routes \ Oracle_US

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

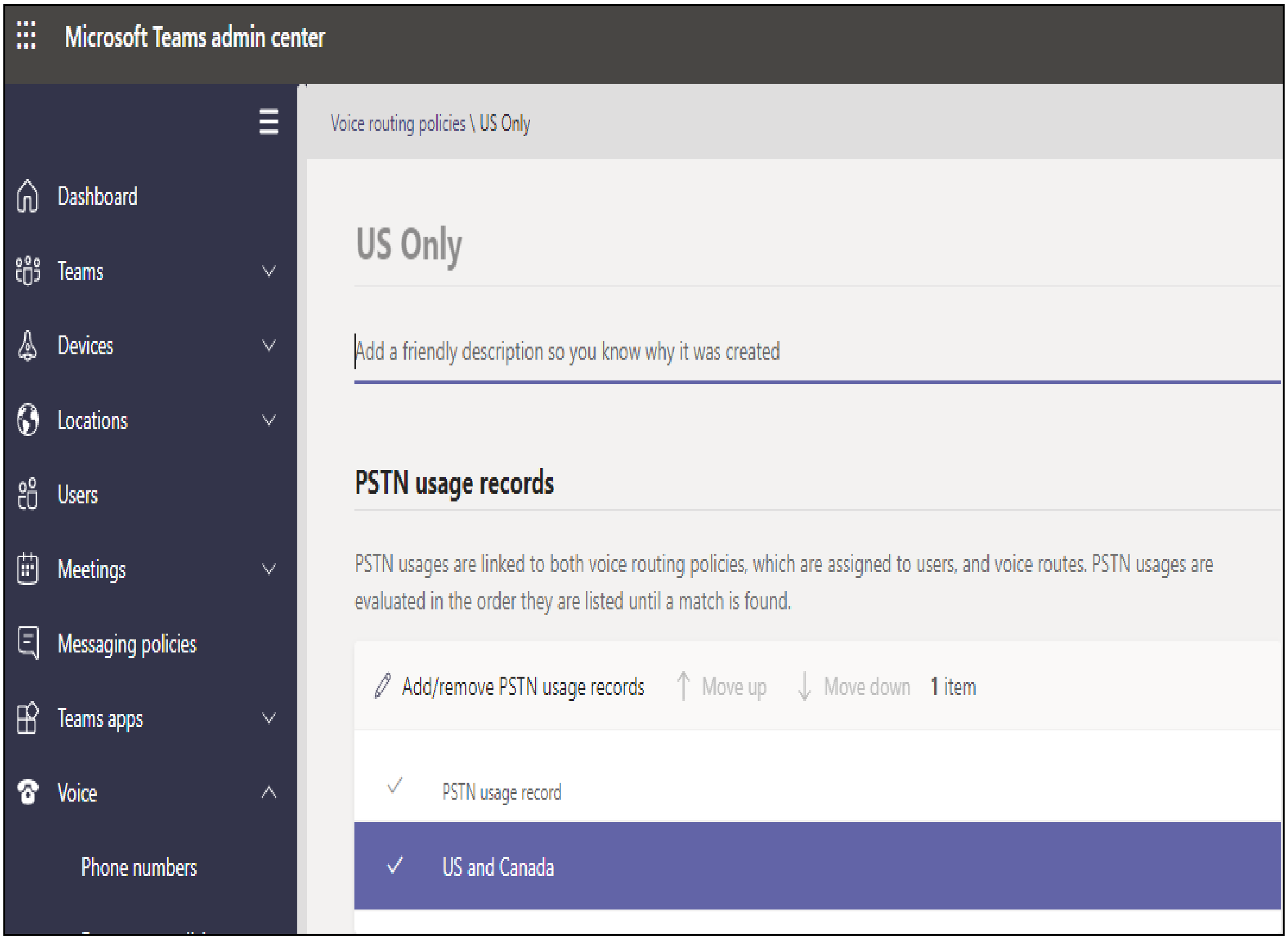
The voice routing policy is linked to a voice route using the PSTN usage records below. You can add existing PSTN usage records, change the order in which the voice routing should be processed, and assign the policy to users.

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

PSTN usage record
✓ US and Canada

5.5. Configure Online Voice Routing Policy

Configuration Path: Voice/Voice Routing Policies



US Only

Add a friendly description so you know why it was created

PSTN usage records

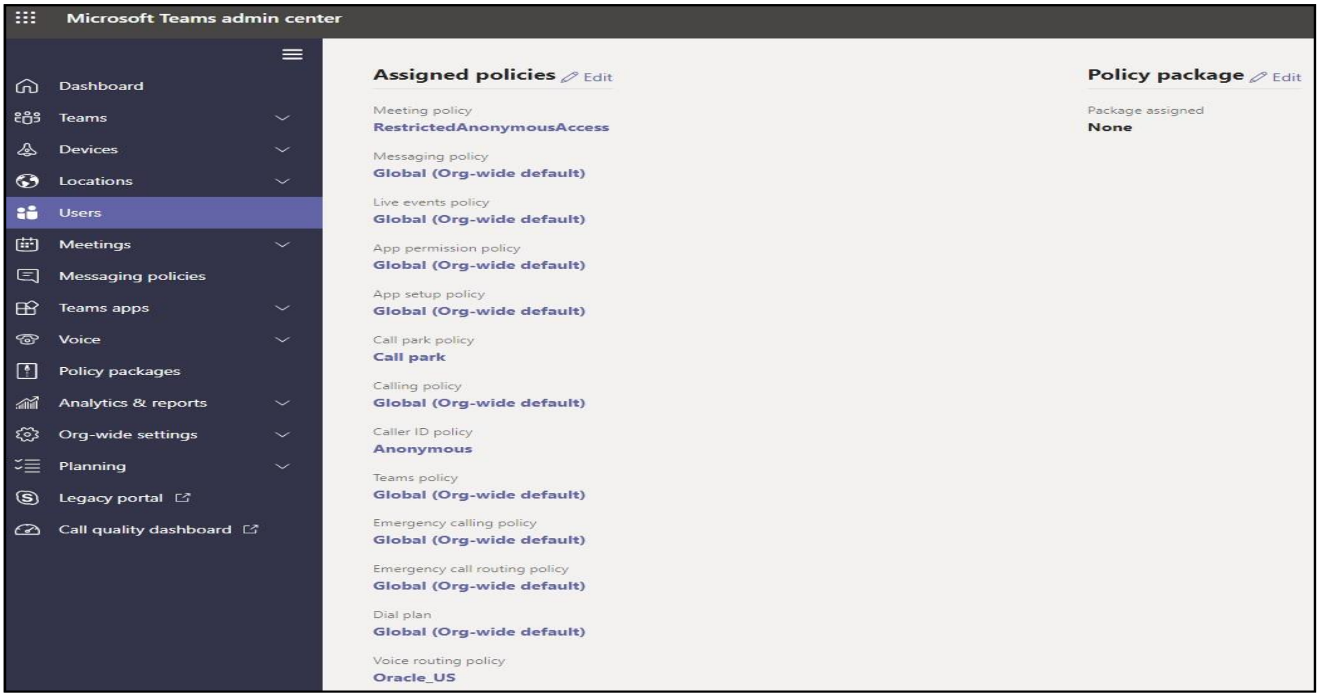
PSTN usages are linked to both voice routing policies, which are assigned to users, and voice routes. PSTN usages are evaluated in the order they are listed until a match is found.

✓	PSTN usage record
✓	US and Canada

5.6. 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:



Assigned policies

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

Policy package

Package assigned
None

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.

6. Configuring the SBC

This chapter provides systematic guidance on how to configure Oracle SBC for Genesys PureCloud and Microsoft Teams.

6.1. Validated Oracle SBC version

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

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

6.2 New SBC configuration

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

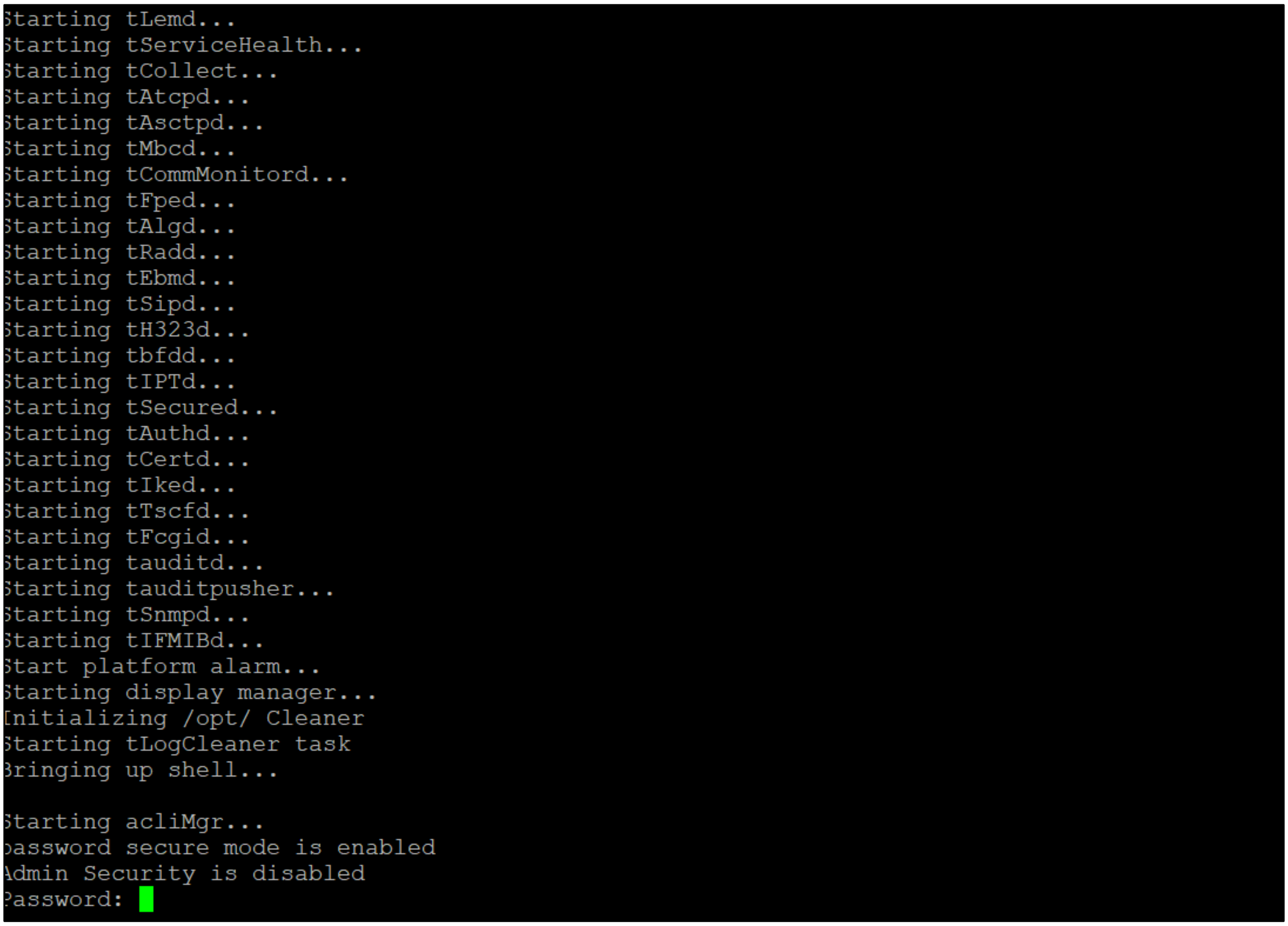
6.2.1 Establishing a serial connection to the SBC

Note: The below method is applicable to the SBCs running on Hardware Platforms. For VME and Cloud SBCs the method of configuration will be different to as shown below. Follow the appropriate documentation or contact your Oracle representative for details about how to configure the VME and Cloud SBC platforms.

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

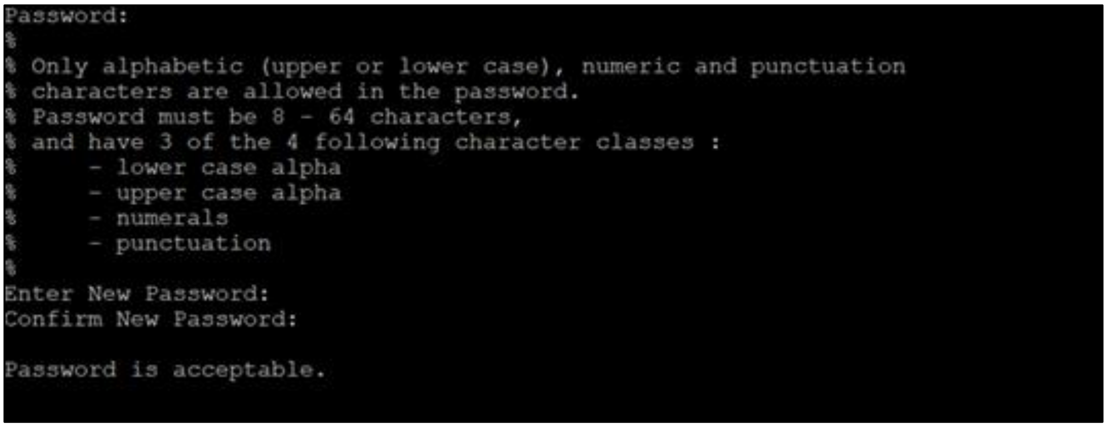
Power on the SBC and confirm that you see the following output from the boot-up sequence



```
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”.

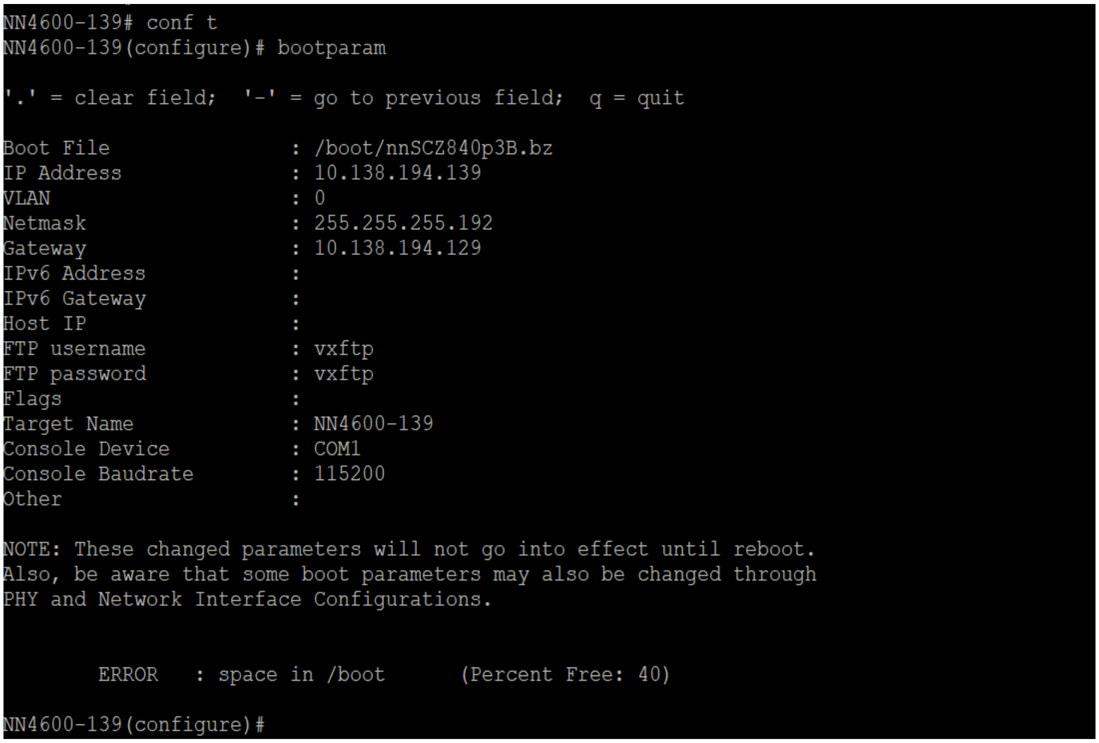
Both passwords must be changed according to the rules shown below.



```
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. Navigate to Configure terminal->bootparam.

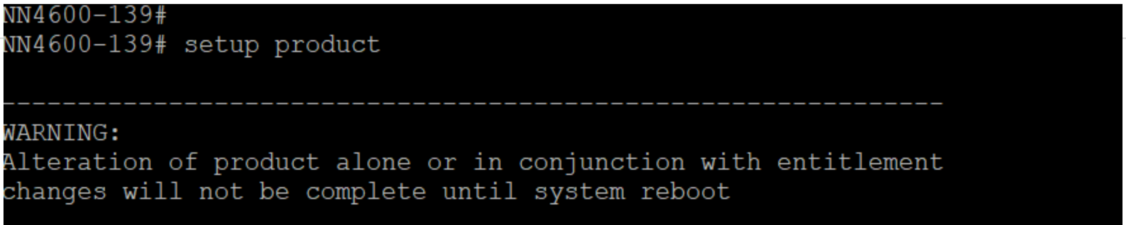


```
NN4600-139# conf t
NN4600-139(configure)# bootparam

'.' = 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.

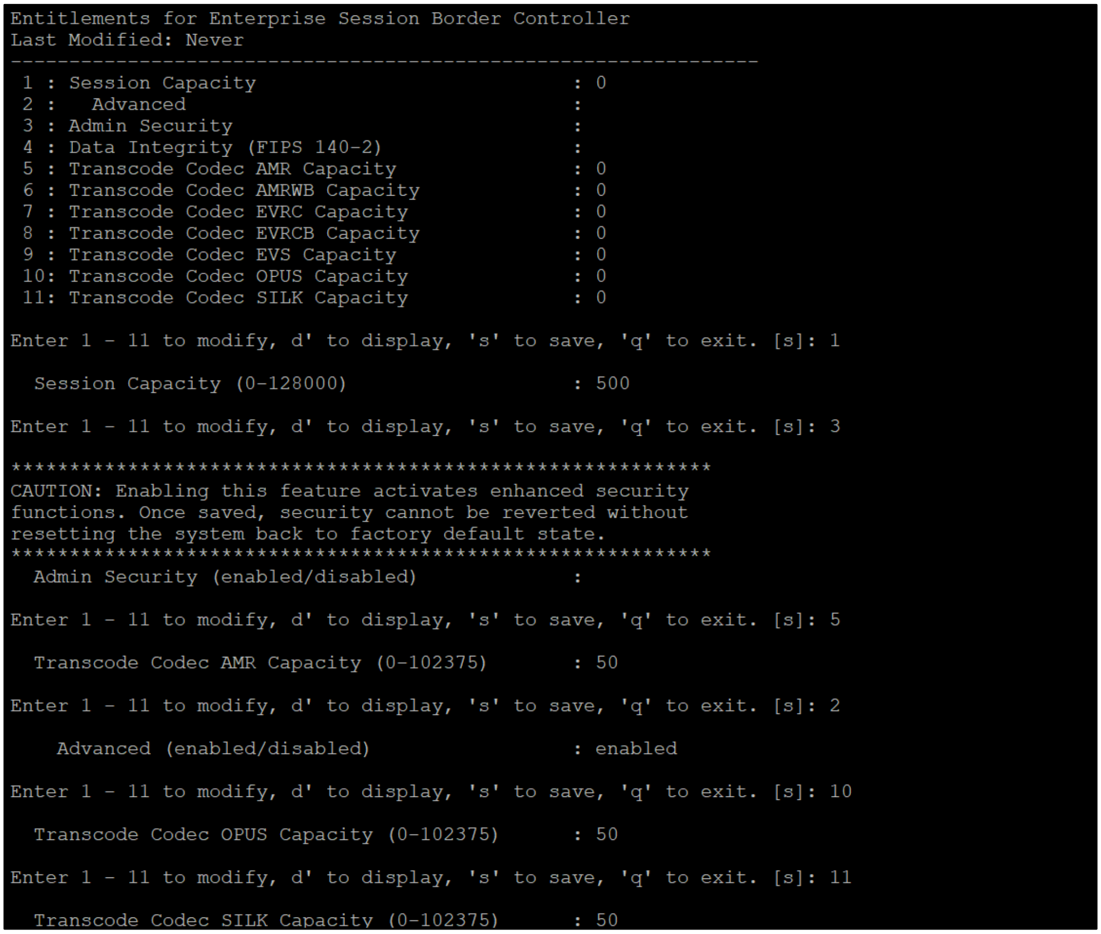
To configure product type, type in setup product in the terminal



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

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

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

Save the changes and reboot the SBC.

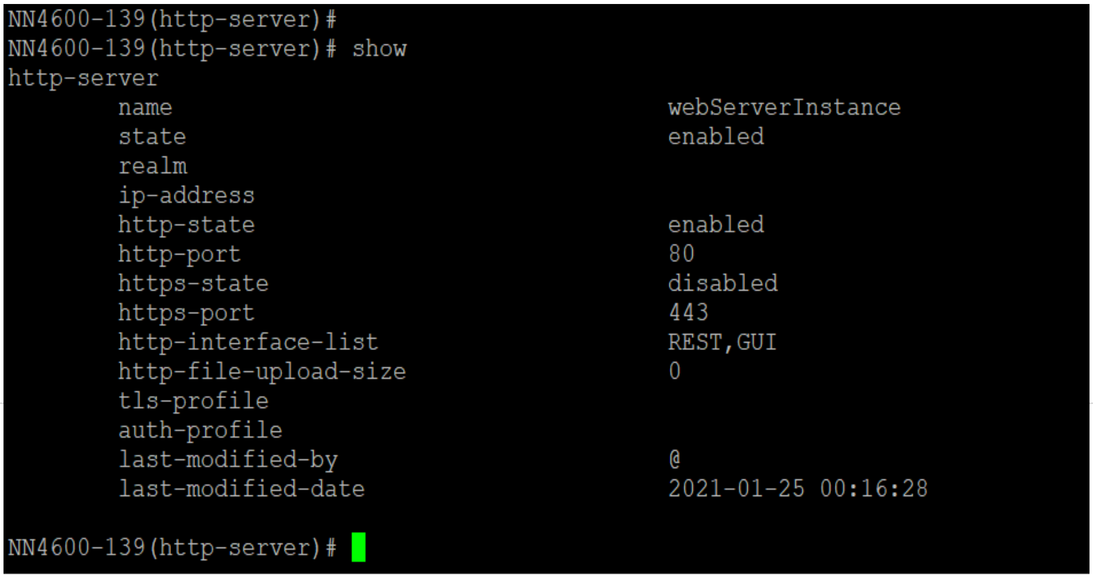


```
Entitlements for Enterprise Session Border Controller
Last Modified: Never
----------------------------------------------------------------
 1 : Session Capacity                           : 0
 2 :   Advanced                                 :
 3 : Admin Security                             :
 4 :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

Navigate to **configure terminal->system->http-server-config**.

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

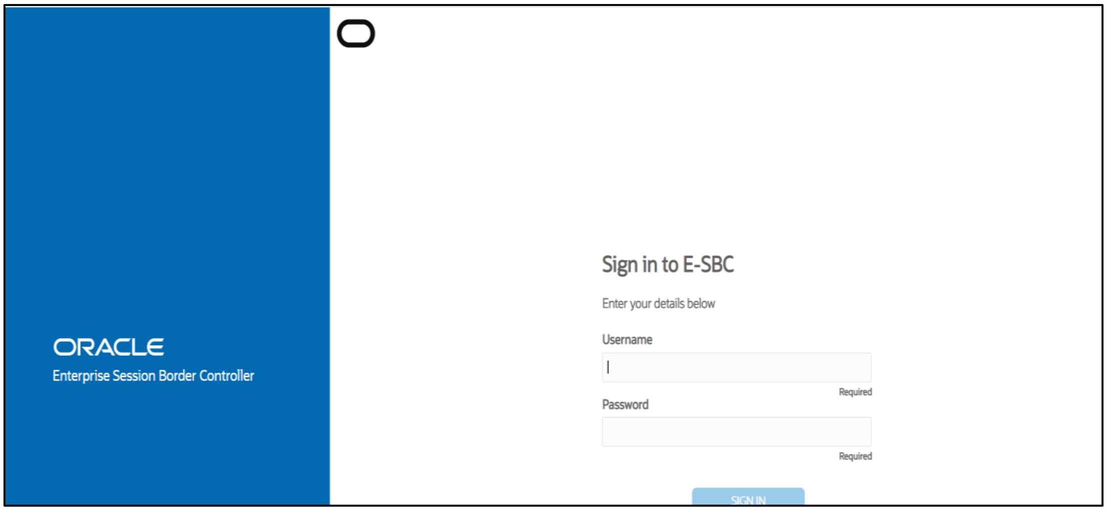


```
NN4600-139(http-server)#
NN4600-139(http-server)# show
http-server
        name                                    webServerInstance
        state                                   enabled
        realm
        ip-address
        http-state                              enabled
        http-port 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

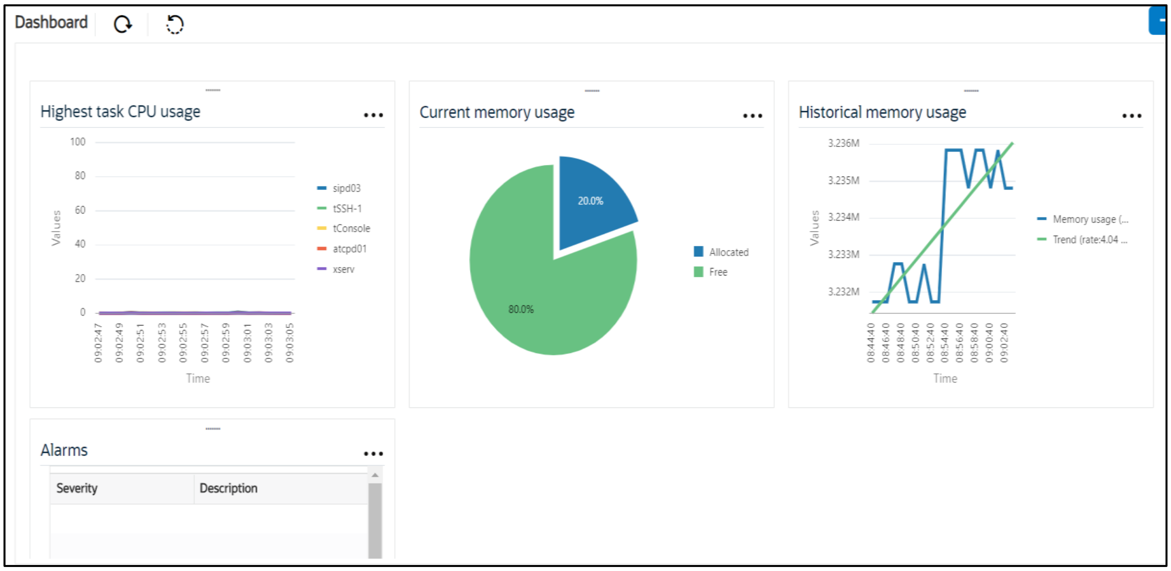
6.2.2 Configure SBC using Web GUI

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

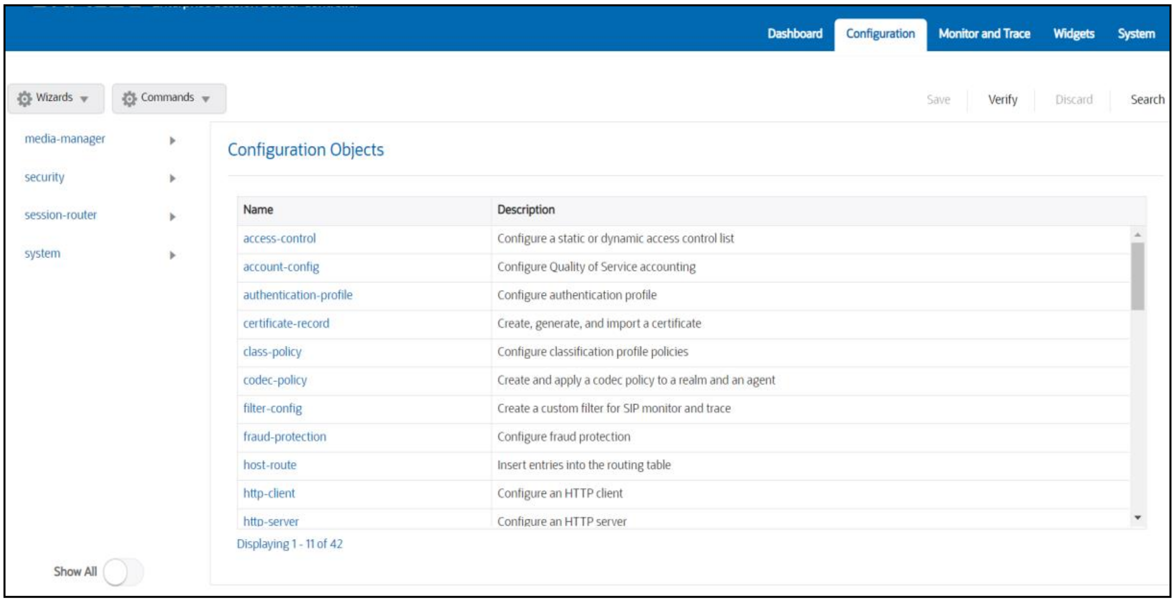
The Web GUI can be accessed through the URL http://<SBC_MGMT_IP>.



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



Navigate 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.

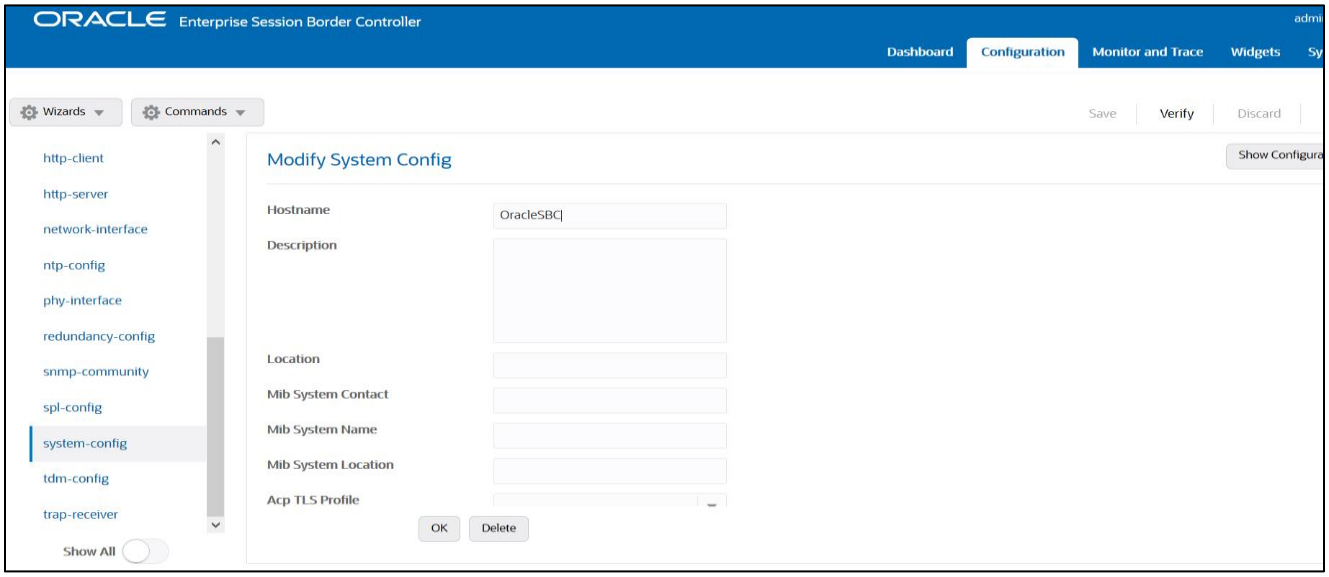
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf

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

Navigate to system->system-config



Modify System Config

Hostname: OracleSBC

Description:

Location:

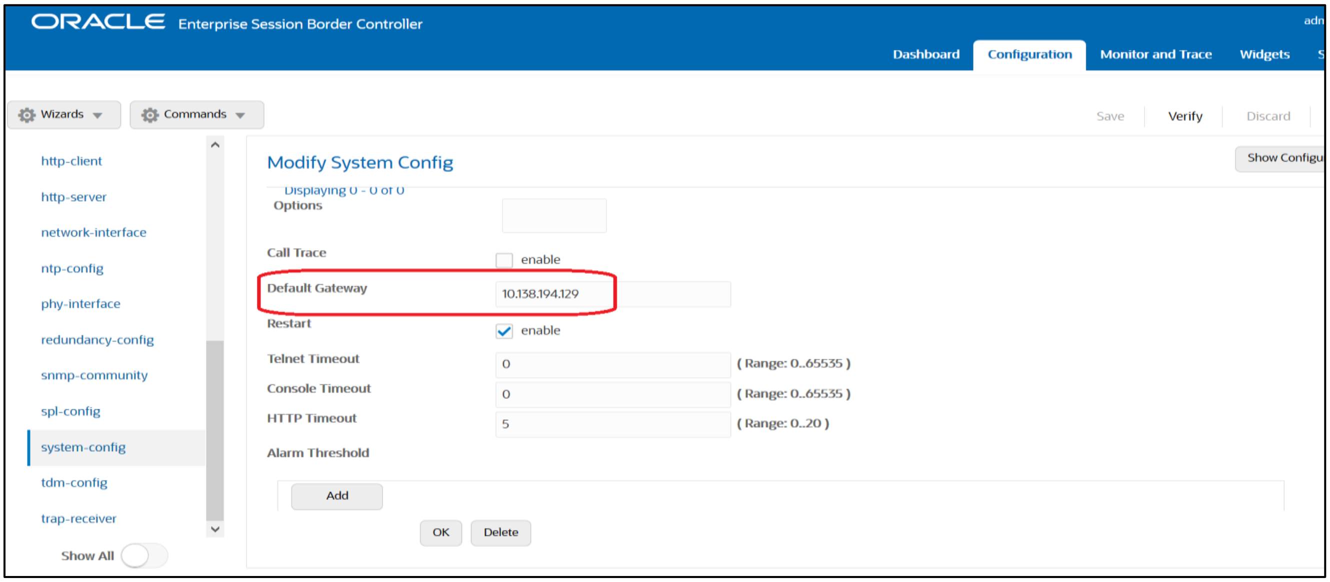
Mib System Contact:

Mib System Name:

Mib System Location:

Acp TLS Profile:

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



Modify System Config

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.

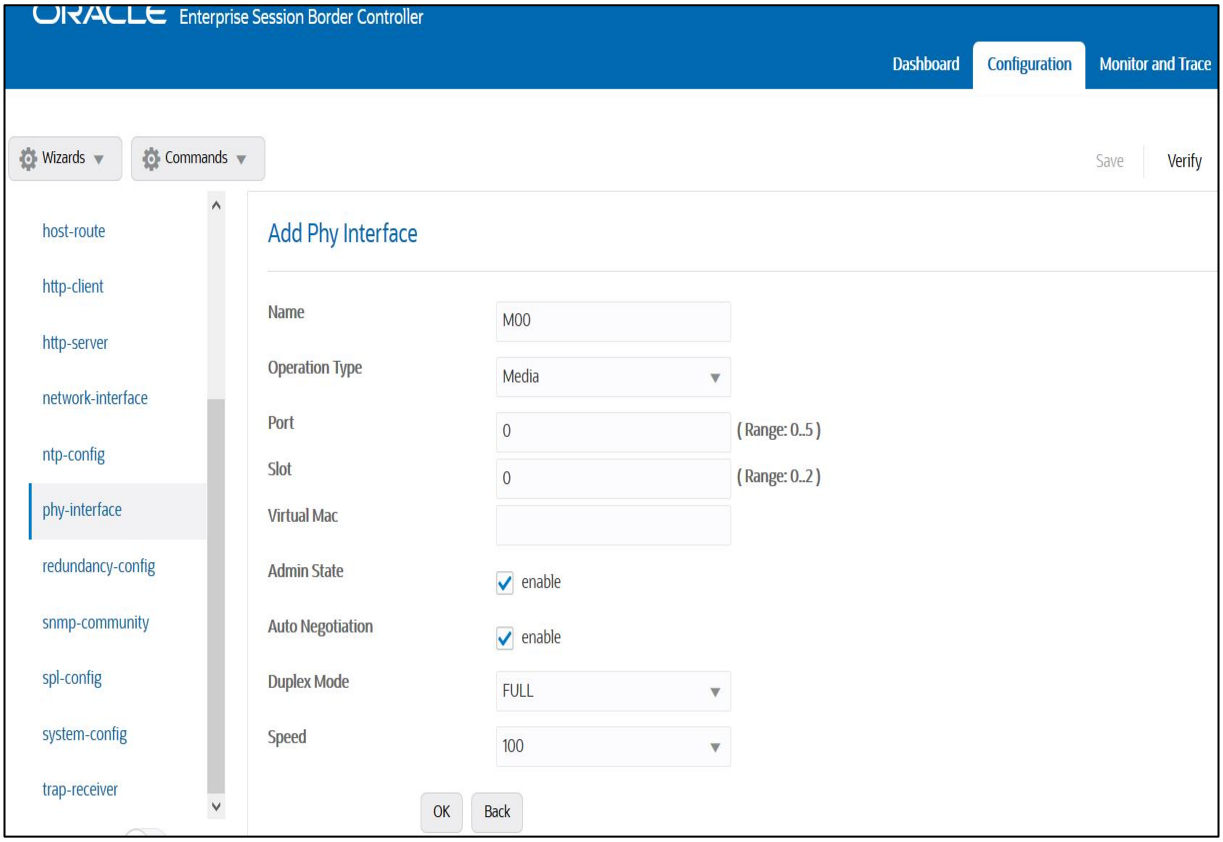
6.4. Configure Physical Interface values

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

Here we have configured, Network-interface M00 for Microsoft Teams and M10 for PureCloud.

Parameter Name	Microsoft Teams (M00)	PureCloud (M10)
Slot	0	1
Port	0	0
Operation Mode	Media	Media

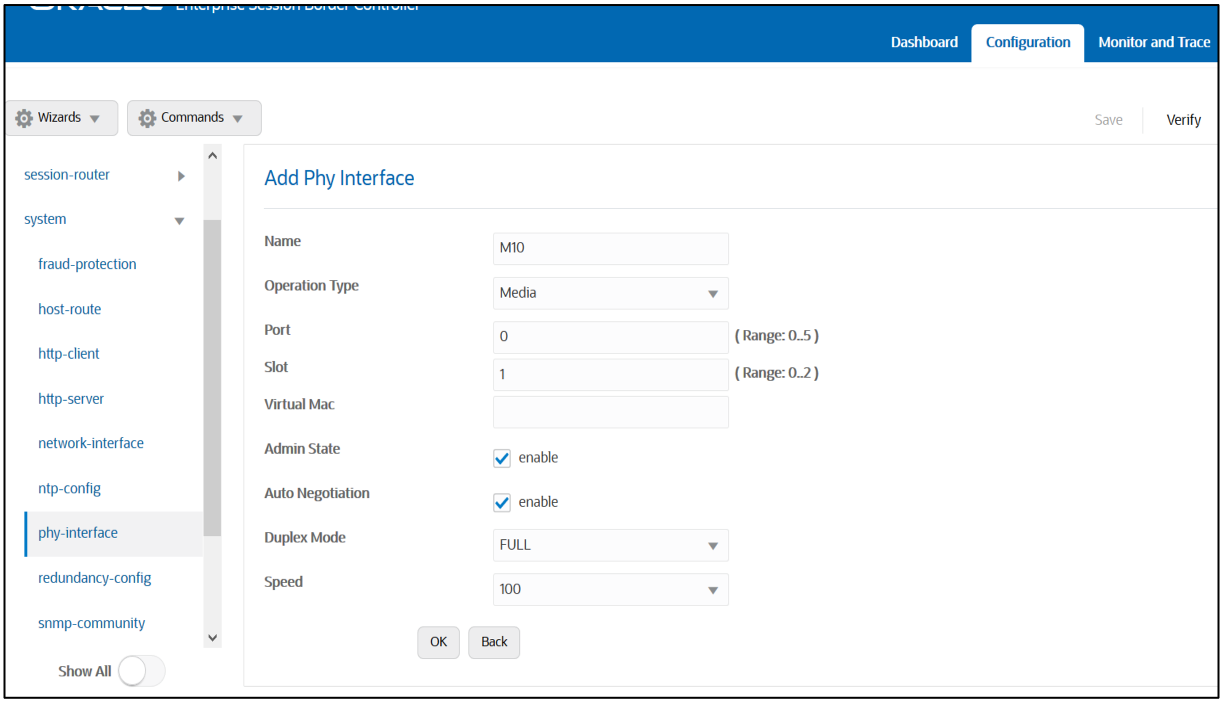
Configure M00 interface as below.



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	

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, Navigate to system->Network-Interface. Configure interface

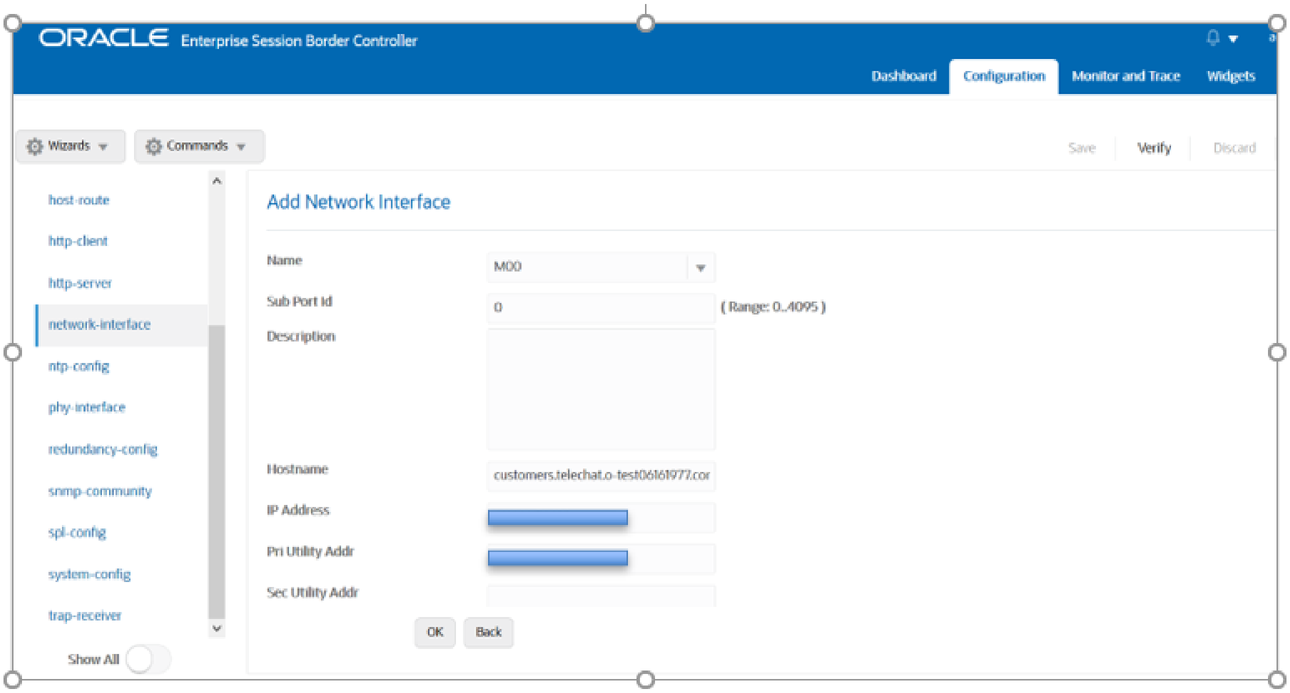
The table below lists the parameters, to be configured for both the interfaces.

Note: The provided network IP addresses are given for example purpose only. In the real-world scenario We cannot use same networks on two network-interfaces hence make sure you use a different IP range for each Network-interface.

In this Setup we are using Google Public DNS to resolve the DNS names to IP Addresses.

Parameter Name	Microsoft Teams Network Interface	PureCloud Network interface
Name	M00	M10
Host Name	customers.telechat.o-test06161977.com	solutionslab.cgbubedford.com
IP address	[redacted]	[redacted]
Netmask	255.255.255.192	255.255.255.192
Gateway	[redacted]	[redacted]
dns-ip-primary	8.8.8.8	8.8.8.8
dns-ip-backup1	8.8.8.4	8.8.8.4

Configure network interface M00 as below



Add Network Interface

Name: M00

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

Description:

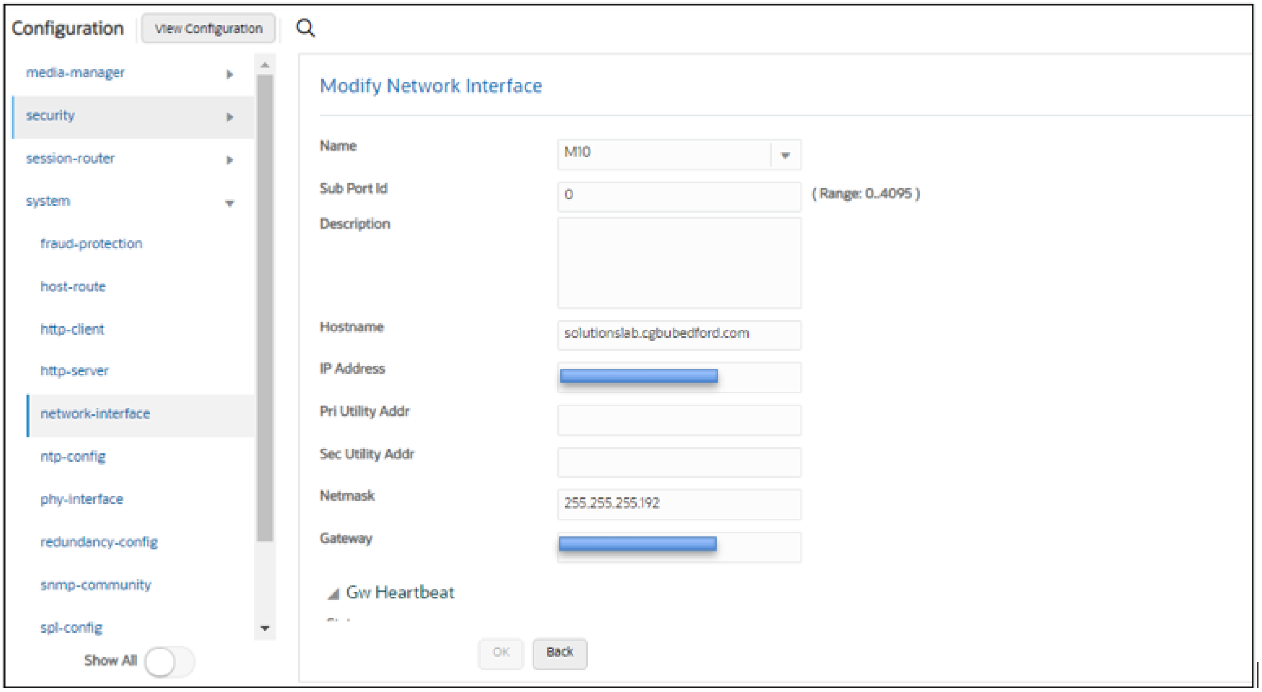
Hostname: customers.telechat.o-test06161977.cor

IP Address: [redacted]

Pri Utility Addr: [redacted]

Sec Utility Addr:

Similarly, configure network interface M10 as below



Modify Network Interface

Name: M10

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

Description:

Hostname: solutionslab.cgbubedford.com

IP Address: [redacted]

Pri Utility Addr:

Sec Utility Addr:

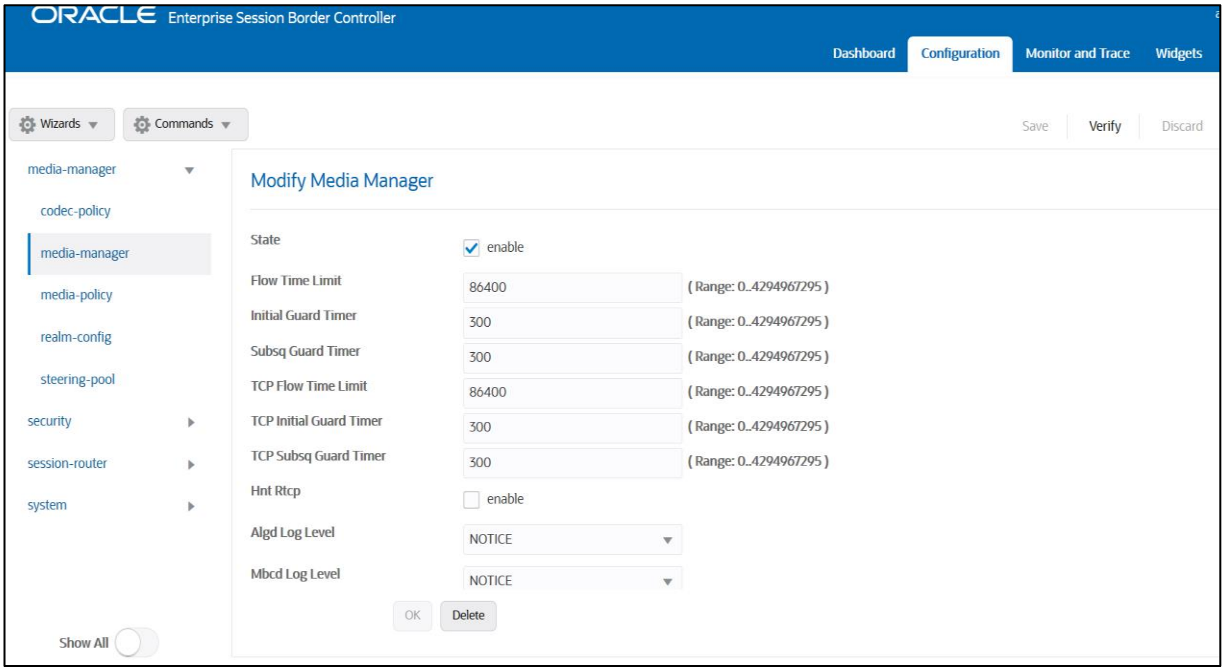
Netmask: 255.255.255.192

Gateway: [redacted]

6.6. Enable media manager

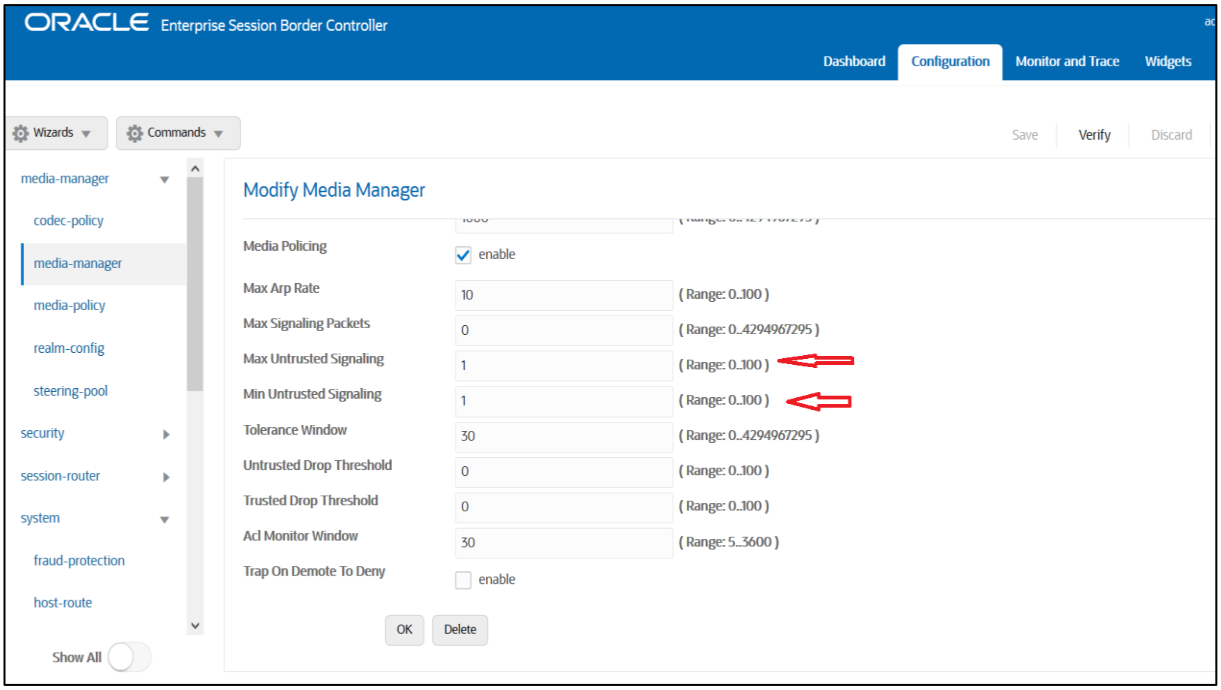
Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

In addition to the above config, please set the max and min untrusted signaling values to one.
Navigate 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

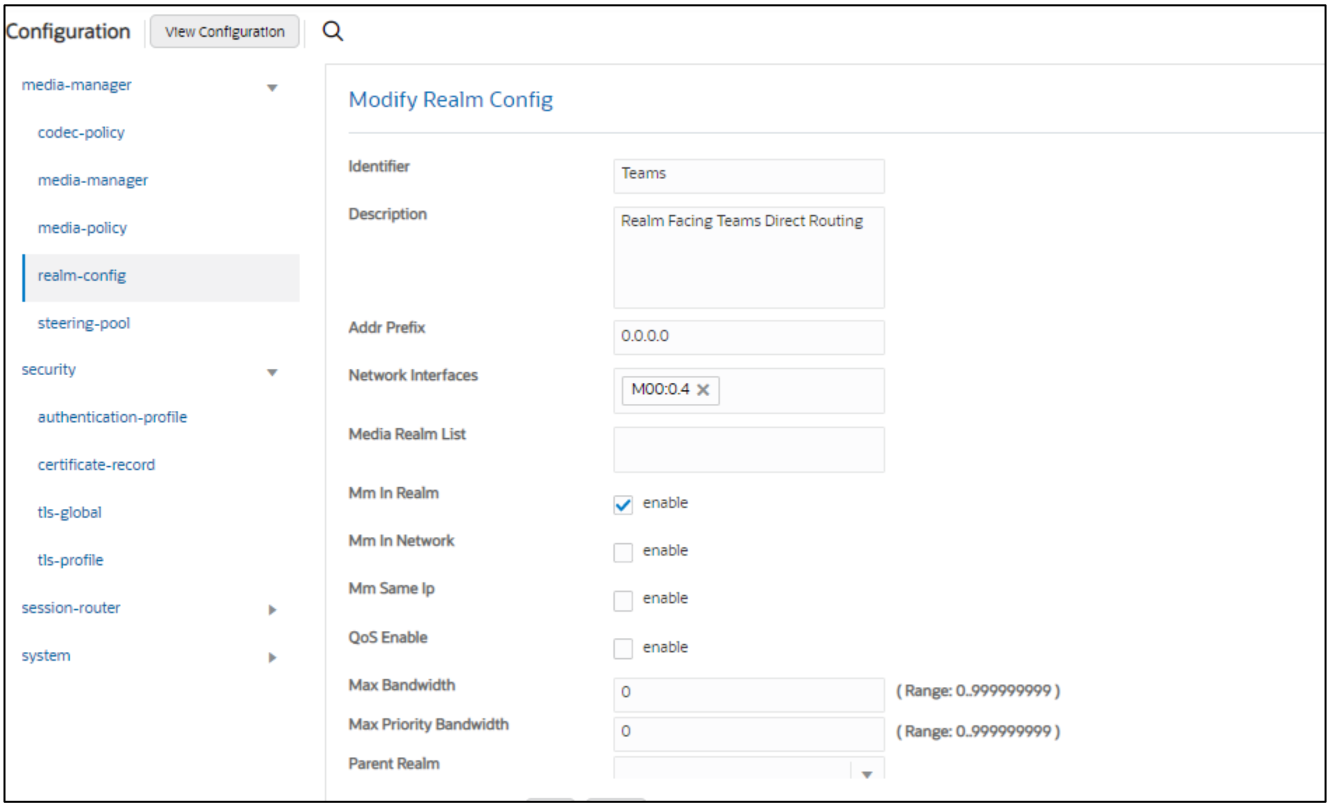
6.7. Configure Realms

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 three realms used in this configuration:

Config Parameter	Teams Side	GenesysCloud Realm
Identifier	Teams	GenesysCloud
Network Interface	M00	M10
Mm in realm	☑	☑
Teams-FQDN	Customers.Telechat.o-test06161977.com	
Teams fqdn in uri	☑	
Sdp inactive only	☑	
Media Sec policy	sdespolicy	sdespolicy
RTCP mux	☑	
ice profile	ice	
Codec policy	addCN	
RTCP policy	rtcpGen	
Access Control Trust Level	High	High
Pai-strip	enabled	
Media-policy		

Realm for Microsoft Teams –



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

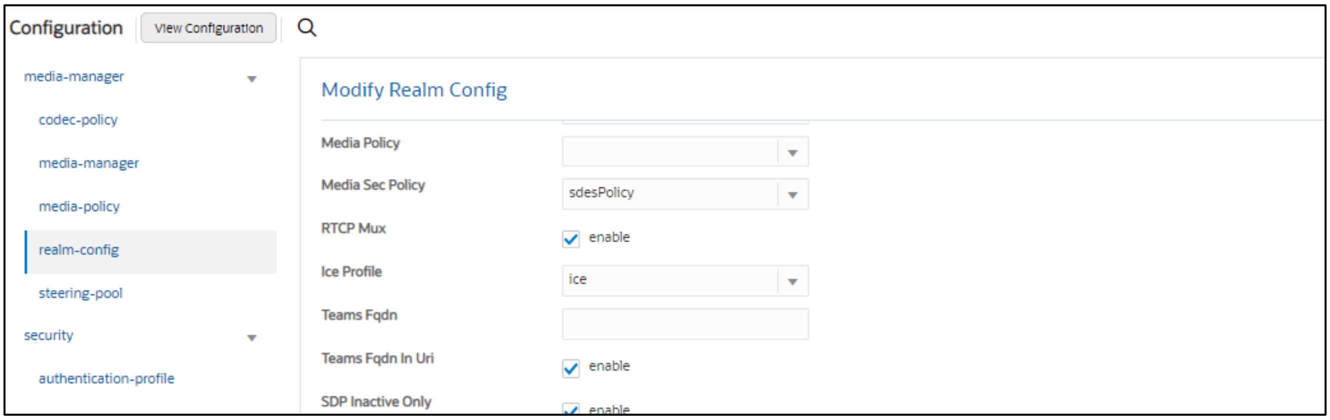
Mm Same Ip: □ enable

QoS Enable: □ enable

Max Bandwidth: 0 (Range: 0..999999999)

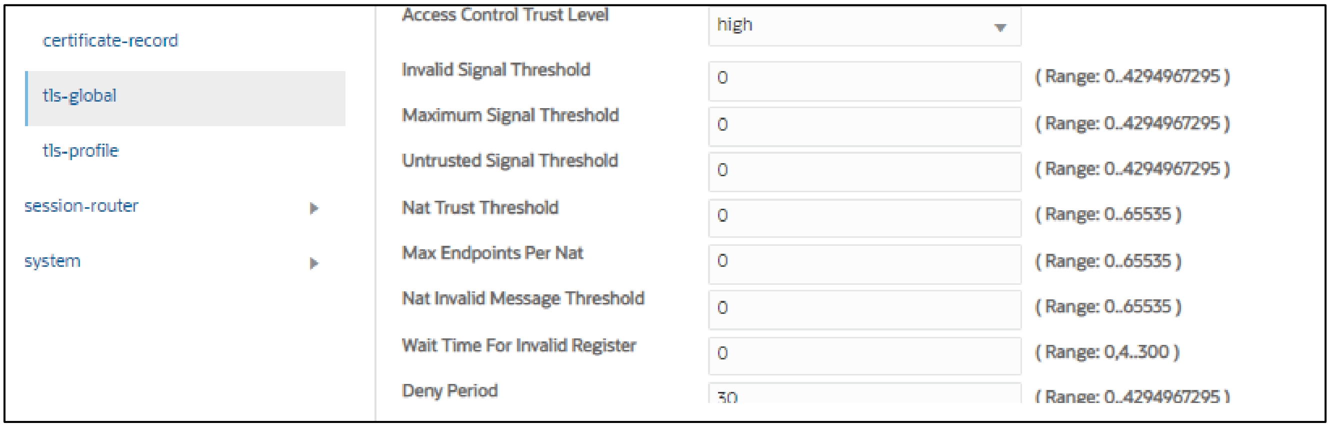
Max Priority Bandwidth: 0 (Range: 0..999999999)

Parent Realm:

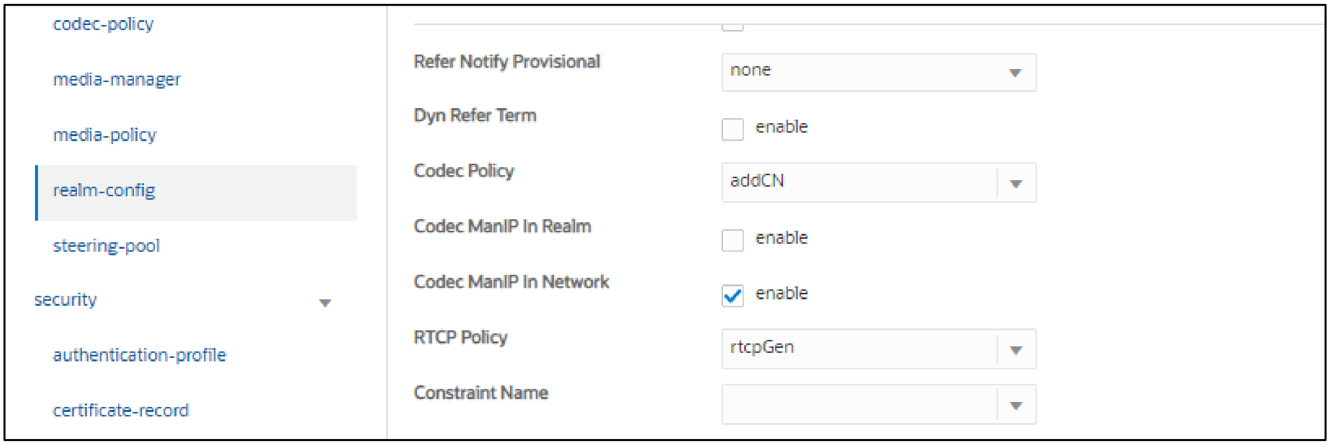


Modify Realm Config

Media Policy	
Media Sec Policy	sdesPolicy
RTCP Mux	☑ enable
Ice Profile	ice
Teams Fqdn	
Teams Fqdn In Uri	☑ enable
SDP Inactive Only	☑ enable

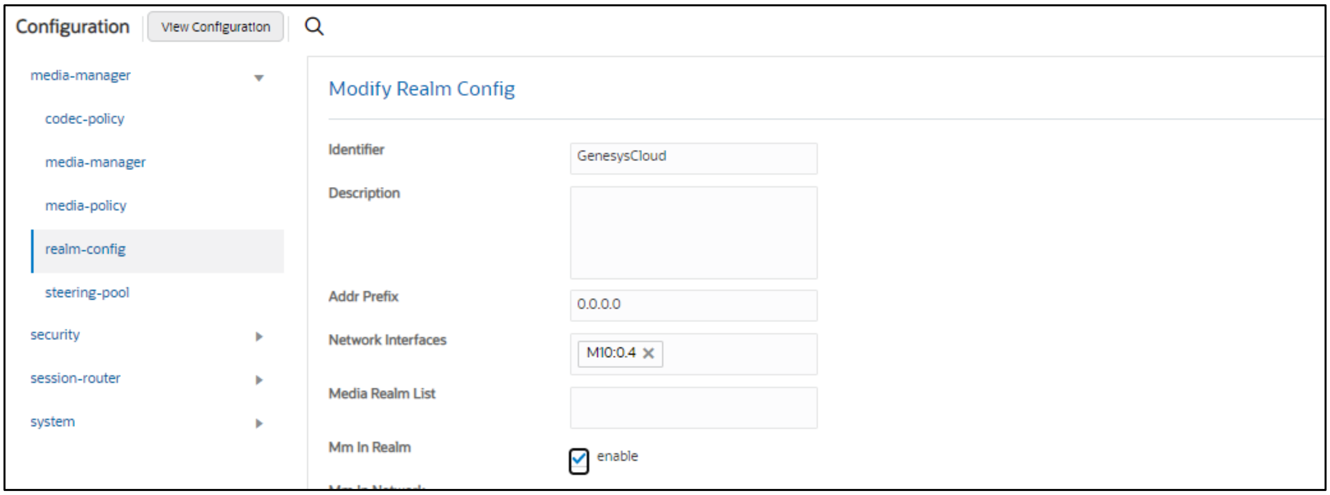


Access Control Trust Level	high	
Invalid Signal Threshold	0	(Range: 0..4294967295)
Maximum Signal Threshold	0	(Range: 0..4294967295)
Untrusted Signal Threshold	0	(Range: 0..4294967295)
Nat Trust Threshold	0	(Range: 0..65535)
Max Endpoints Per Nat	0	(Range: 0..65535)
Nat Invalid Message Threshold	0	(Range: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



Refer Notify Provisional	none
Dyn Refer Term	☐ enable
Codec Policy	addCN
Codec ManIP In Realm	☐ enable
Codec ManIP In Network	☑ enable
RTCP Policy	rtcpGen
Constraint Name	

Realm for Genesys PureCloud



Modify Realm Config

Identifier: GenesysCloud

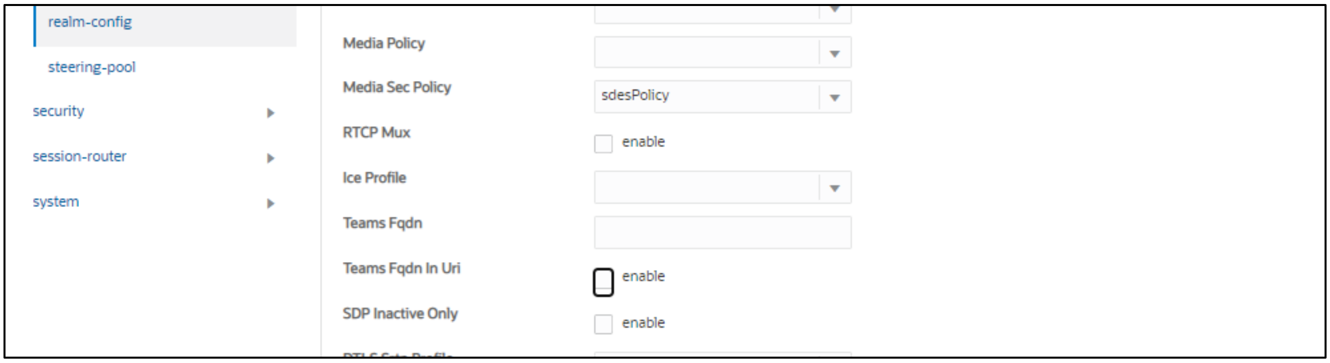
Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M10:0.4 ✕

Media Realm List:

Mm In Realm: ☑ enable



Media Policy:

Media Sec Policy: sdesPolicy

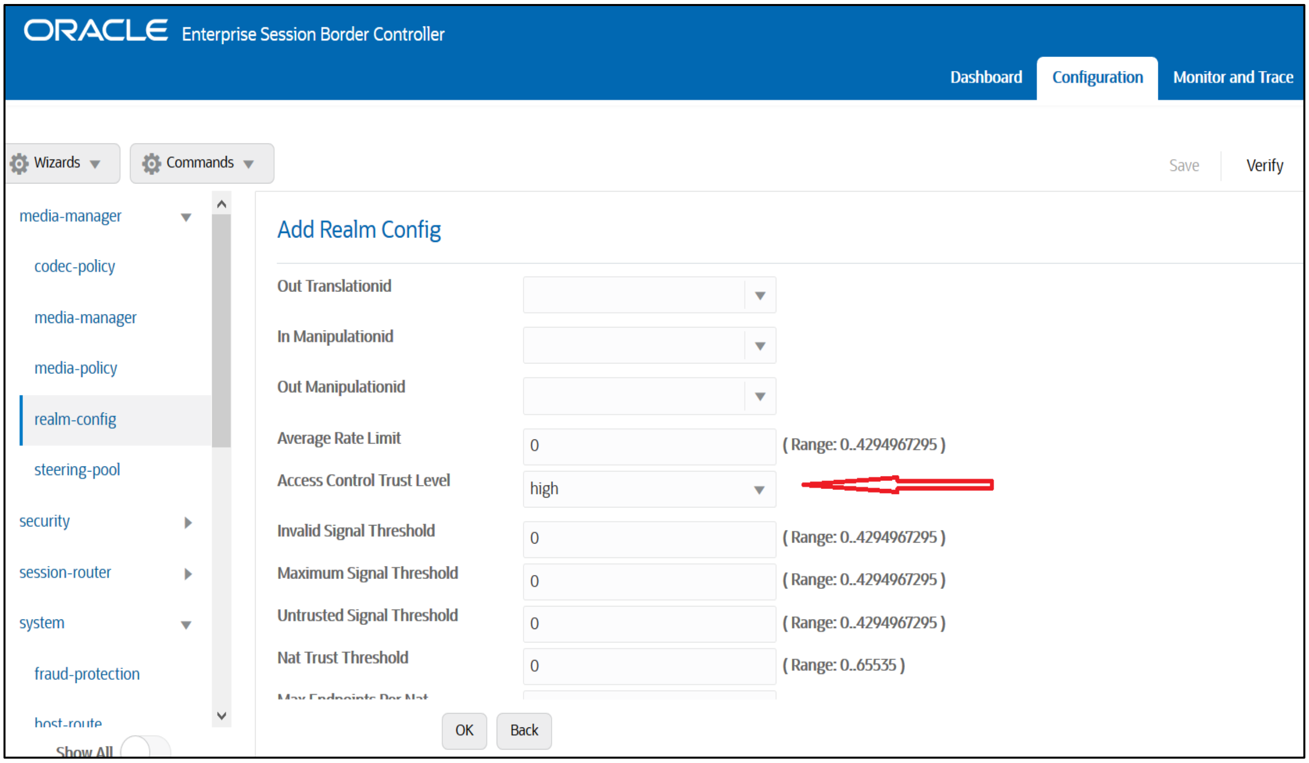
RTCP Mux: □ enable

Ice Profile:

Teams Fqdn:

Teams Fqdn In Uri: □ enable

SDP Inactive Only: □ enable



Add Realm Config

Out Translationid:

In Manipulationid:

Out Manipulationid:

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

Access Control Trust Level: high

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

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

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

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

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

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

6.8. Security Configuration

6.8.1 Configuring Certificates

This section describes how to configure the SBC for TLS and SRTP communication for Microsoft Teams and PureCloud BYOC. It requires a certificate signed by one of the trusted Certificate Authorities. The communication between the Oracle SBC with Microsoft Teams and Genesys PureCloud is TLS/SRTP.

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

This section walks you through how to configure certificate records, create a certificate signing request, and import the necessary certificates into the SBC’s configuration.

GUI Path: security/certificate-record

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

- **SBC Certificate (end-entity certificate)**
- **Baltimore Root -Required for Microsoft Teams**
- **DigiCert Root CA (SBC and Microsoft Teams)**
- **DigiCert Intermidiate Cert (this is optional – only required if your server certificate is signed by an intermediate)**
- **DigiCertEVRootCA (Genesys PureCloud)**

Supported CAs for Microsoft Teams.

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

Supported CA for Genesys PureCloud BYOC

Genesys Pure Cloud signs the BYOC Cloud endpoints with X.509 certificates issued by DigiCert, a public Certificate Authority. More specifically, the root certificate authority that signs the BYOC Cloud endpoints is the DigiCert High Assurance EV Root CA.

https://help.mypurecloud.com/articles/tls-trunk-transport-protocol-specification/

Note: Both Genesys PureCloud and Microsoft Teams uses subject name validation to ensure that the remote endpoint identifies itself as the expected target. If a server certificate does not contain the name to which the client is connected as either the common name or the subject alternate name, the connection is refused.

Below Table 1 is for reference. Modify the configuration according to the certificates in your environment.

Config Parameter	SBC Certificate1(Teams)	SBC Certificate2(PureCloud)	Baltimore Root	DigiCertEV RootCA	DigiCert Root CA	DigiCert Intermediate
Name	SBCCert1	SBCCert2	Baltimore CyberTrust Root	PureCloudCert	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA

Common Name	**customers.telechat.o-test06161977.com**	**solutionslab.cgbubedford.com**	Baltimore CyberTrust Root	**P**ureCloudCert	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA
Key Size	2048	2048	2048	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256	Sha256	Sha256	Sha256

6.8.1.1 End Entity Certificate

The SBC’s end entity certificate is what is presented to PureCloud and Microsoft Teams signed by your CA authority, in this example we are using Digicert as our signing authority.

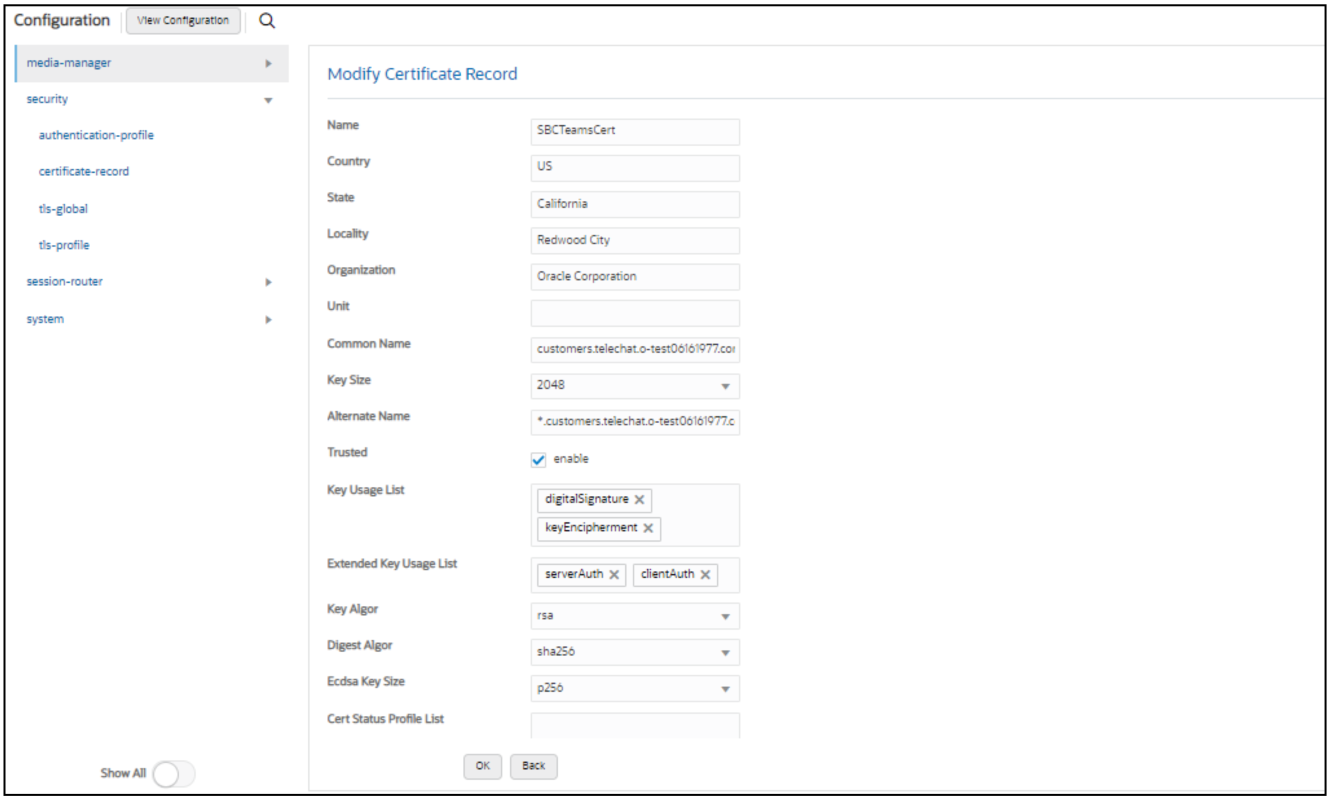
Here in this setup,We wil create two end entity certificates in this case as we are connecting to PureCloud and Microsoft Teams over different FQDN

- Common name: (**customers.telechat.o-test06161977.com**) for Microsoft Teams.
- Common name: (**solutionslab.cgbubedford.com**) for PureCloud..

Step 1 Configure SBC Certificate Record

To Configure the certificate record:

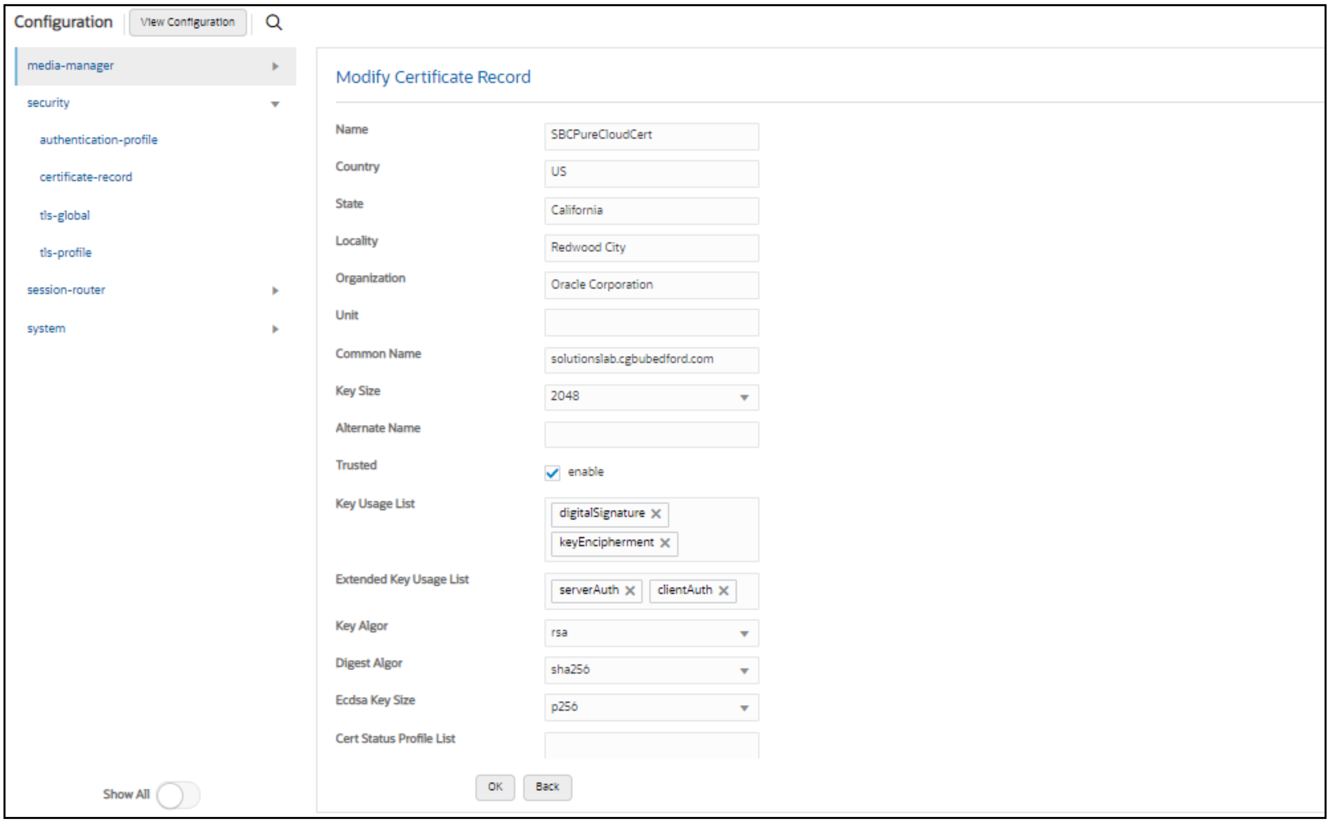
- Click Add, and configure the SBC certificate as shown below:



Modify Certificate Record

Name	SBCTeamsCert
Country	US
State	California
Locality	Redwood City
Organization	Oracle Corporation
Unit	
Common Name	customers.telechat.o-test06161977.cor
Key Size	2048
Alternate Name	*.customers.telechat.o-test06161977.c
Trusted	☑ enable
Key Usage List	digitalSignature ✕ keyEncipherment ✕
Extended Key Usage List	serverAuth ✕ clientAuth ✕
Key Algor	rsa
Digest Algor	sha256
Ecdsa Key Size	p256
Cert Status Profile List	

Similarly repeat the step to create another certificate record to present to Genesys PureCloud signed by your CA.



Modify Certificate Record

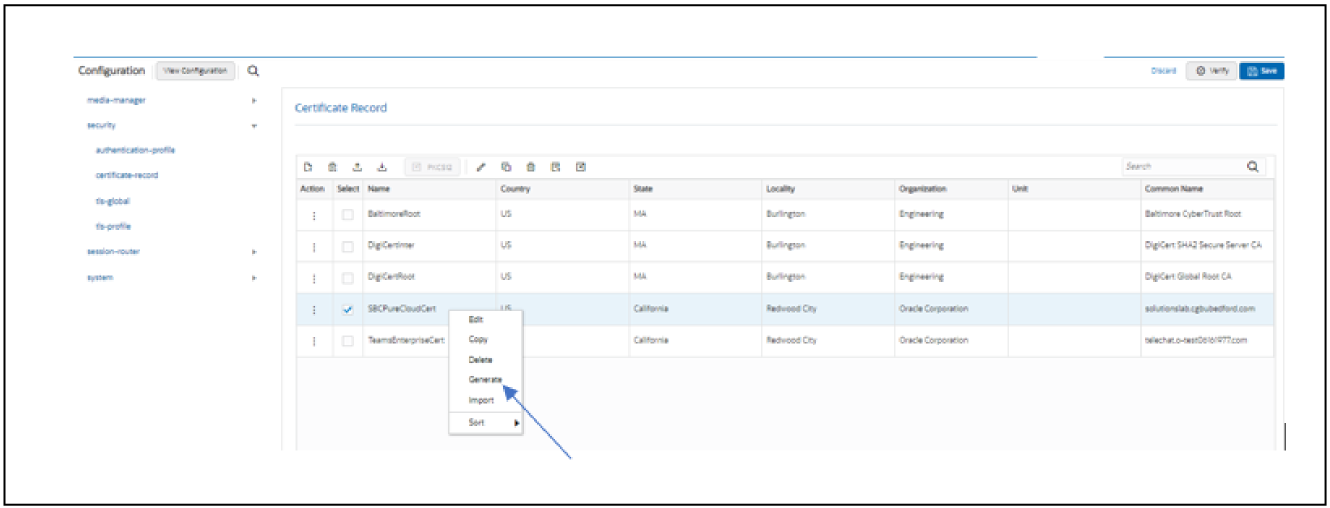
Name	SBCPureCloudCert
Country	US
State	California
Locality	Redwood City
Organization	Oracle Corporation
Unit	
Common Name	solutionslab.cgbubedford.com
Key Size	2048
Alternate Name	
Trusted	☑ enable
Key Usage List	digitalSignature ✕ keyEncipherment ✕
Extended Key Usage List	serverAuth ✕ clientAuth ✕
Key Algor	rsa
Digest Algor	sha256
Ecdsa Key Size	p256
Cert Status Profile List	

Step 2 – Generating a certificate signing request

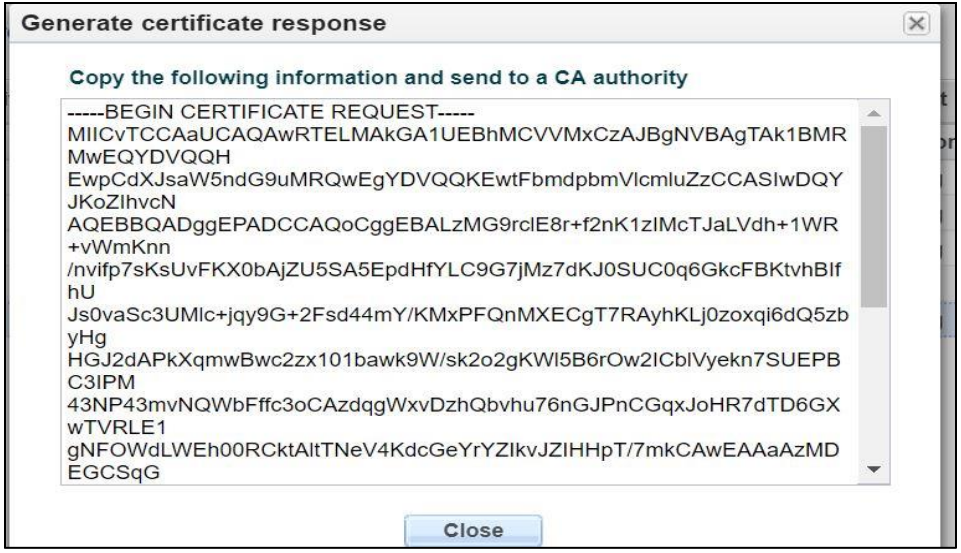
(Only required for the SBC's end entity certificate, and not for root CA certs)

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

- Select the certificate and generate certificate on clicking the "Generate" command.
- The Step must be performed for both Certificate records -SBCTeamsCert and SBCPureCloudCert
- Please copy/paste the text that is printed on the screen as shown below and upload to your CA server for signature.



Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
⋮	□	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberTrust Root
⋮	□	DigiCertInter	US	MA	Burlington	Engineering		DigiCert SHA2 Secure Server CA
⋮	□	DigiCertRoot	US	MA	Burlington	Engineering		DigiCert Global Root CA
⋮	☑	SBCPureCloudCert	US	California	Redwood City	Oracle Corporation		solutionslab.cgbubedford.com
⋮	□	TeamsEnterpriseCert		California	Redwood City	Oracle Corporation		telechat.o-test06161977.com



Copy the following information and send to a CA authority

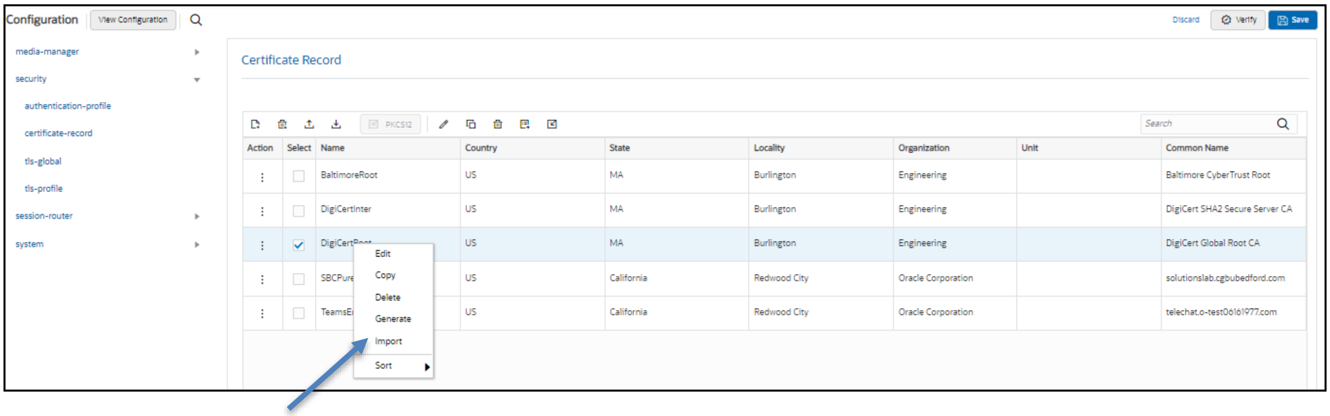
```
-----BEGIN CERTIFICATE REQUEST-----
MIICvTCCAaUCAQAwRTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMR
MwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzCCASIwDQY
JKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALzMG9rclE8r+f2nK1zIMcTJaLVdh+1WR
+vWmKnn
/nvifp7sKsUvFKX0bAjZU5SA5EpdHfYLC9G7jMz7dKJ0SUC0q6GkcFBKtvhBIf
hU
Js0vaSc3UMlc+jqy9G+2Fsd44mY/KMxPFQnMXECgT7RAyhKLj0zoxqi6dQ5zb
yHg
HGJ2dAPkXqmwBwc2zx101bawk9W/sk2o2gKWI5B6rOw2ICblVyekn7SUEPB
C3IPM
43NP43mvNQWbFffc3oCAzdqgWxvDzhQbvhu76nGJPnCGqxJoHR7dTD6GX
wTVRLE1
gNFOWdLWEh00RCktAltTNeV4KdcGeYrYZIkvJZIHHpT/7mkCAwEAAaAzMD
EGCSqG
```

- 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, **a save and activate is required** before you can import the certificates to each certificate record created above.

Step 3 Import Certificates to the SBC

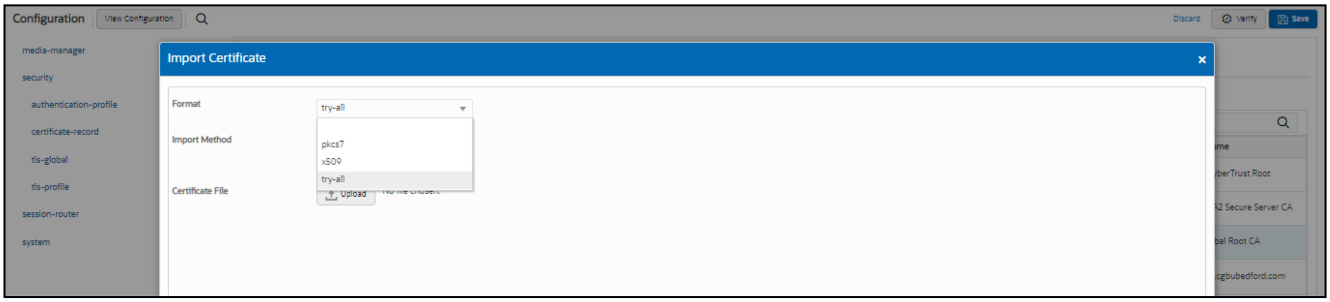
Once certificate signing request have been completed – import the signed certificate to the SBC.

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



Certificate Record

Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
⋮	□	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberTrust Root
⋮	□	DigiCertInter	US	MA	Burlington	Engineering		DigiCert SHA2 Secure Server CA
⋮	☑	DigiCertRoot	US	MA	Burlington	Engineering		DigiCert Global Root CA
⋮	□	SBCPure	US	California	Redwood City	Oracle Corporation		solutionslab.cgbubedford.com
⋮	□	TeamsE	US	California	Redwood City	Oracle Corporation		telechat.o-test06161977.com



Import Certificate

Format: try-all

Import Method

Certificate File: No file chosen.

6.8.1.2 Import CA Certificate

Repeat the steps provided Step 3 to import all the root and intermediate CA certificates into the SBC as mentioned in Table 1.

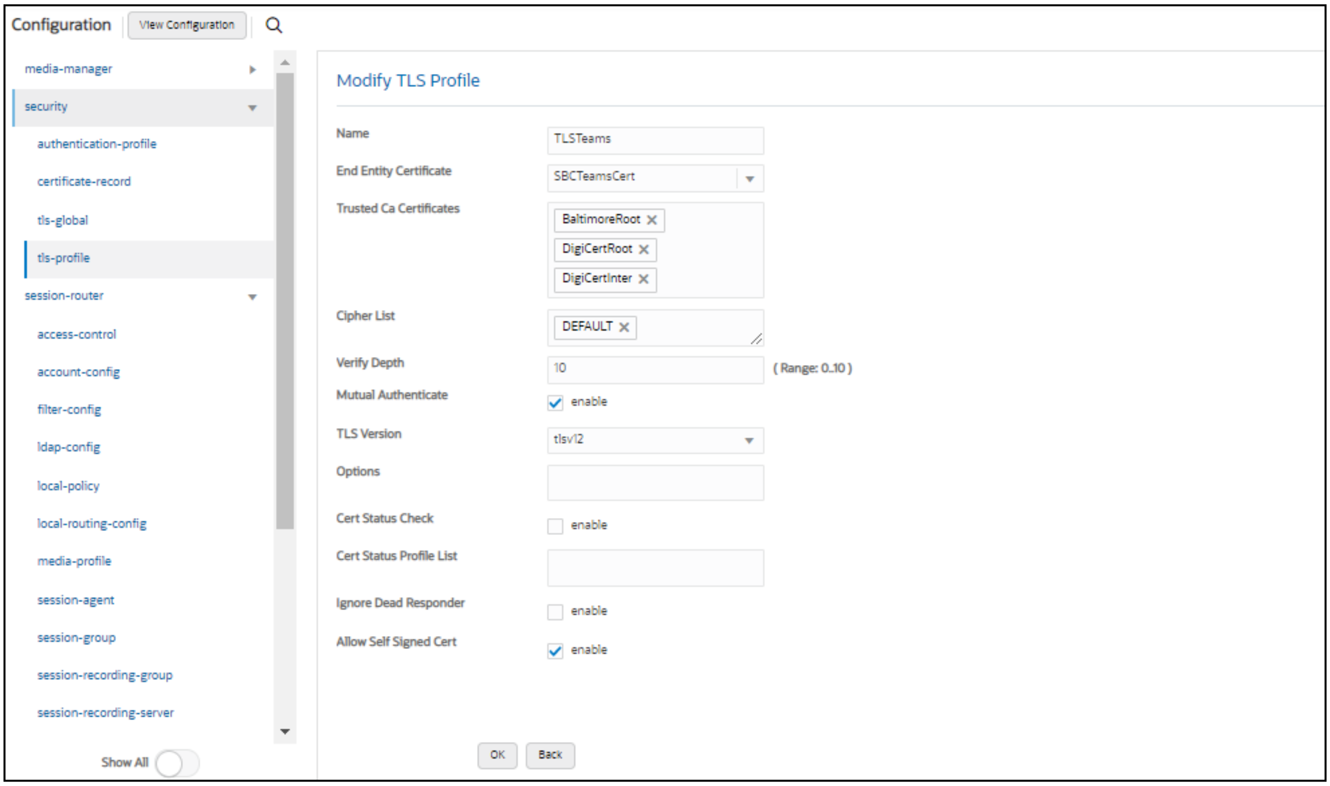
At this stage, all the required certificates SBC certificates have been imported to the SBC

6.9. TLS-Profile

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

Navigate to security-> TLS-profile config element and configure the tls-profile as shown below

TLS profile -Microsoft Teams.



Modify TLS Profile

Name: TLSTeams

End Entity Certificate: SBCTeamsCert

Trusted Ca Certificates: BaltimoreRoot ✕ DigiCertRoot ✕ DigiCertInter ✕

Cipher List: DEFAULT ✕

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

Mutual Authenticate: ☑ enable

TLS Version: tlsv12

Options:

Cert Status Check: □ enable

Cert Status Profile List:

Ignore Dead Responder: □ enable

Allow Self Signed Cert: ☑ enable

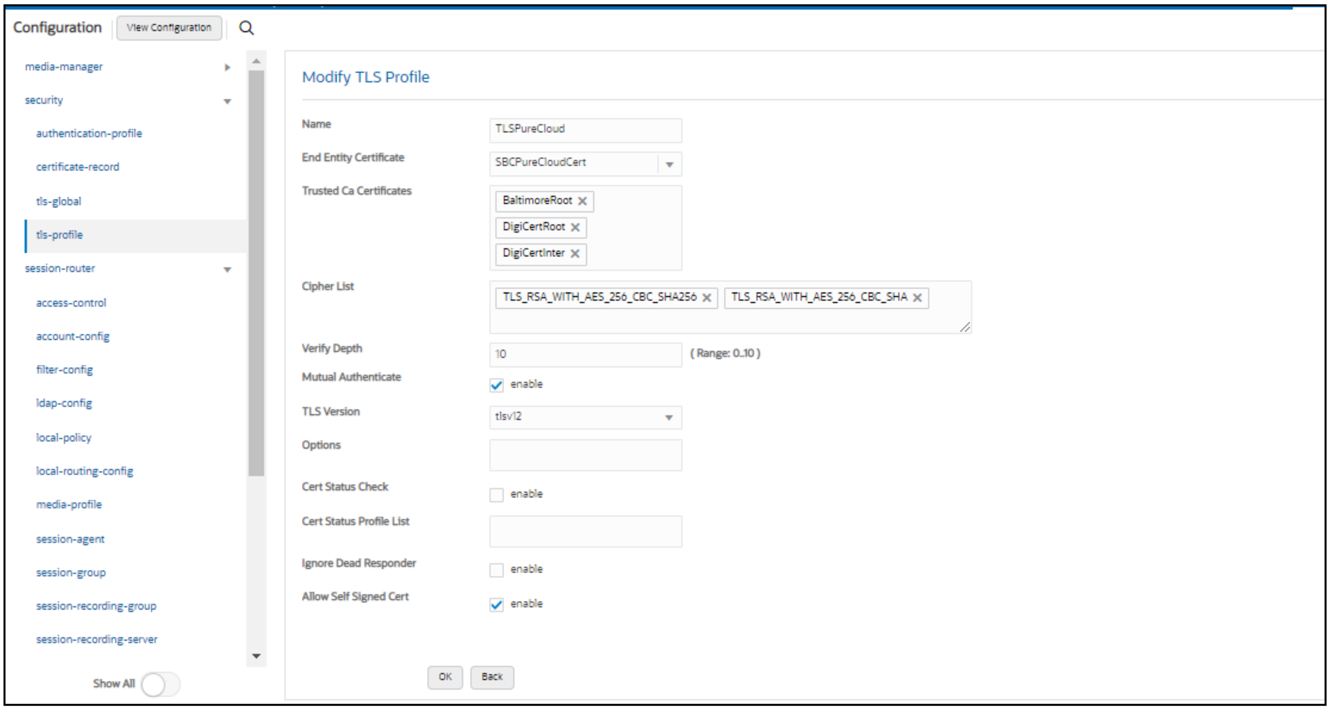
TLS-Profile - Genesys PureCloud

PureCloud BYOC only supports endpoints using the TLS version 1.2 protocol.

Supported TLS ciphers include:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256

TLS-only listeners are available on host port 5061.



Modify TLS Profile

Name	TLSPureCloud
End Entity Certificate	SBCPureCloudCert
Trusted Ca Certificates	BaltimoreRoot DigiCertRoot DigiCertInter
Cipher List	TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA
Verify Depth	10 (Range: 0..10)
Mutual Authenticate	☑ enable
TLS Version	tlsv12
Options	
Cert Status Check	□ enable
Cert Status Profile List	
Ignore Dead Responder	□ enable
Allow Self Signed Cert	☑ enable

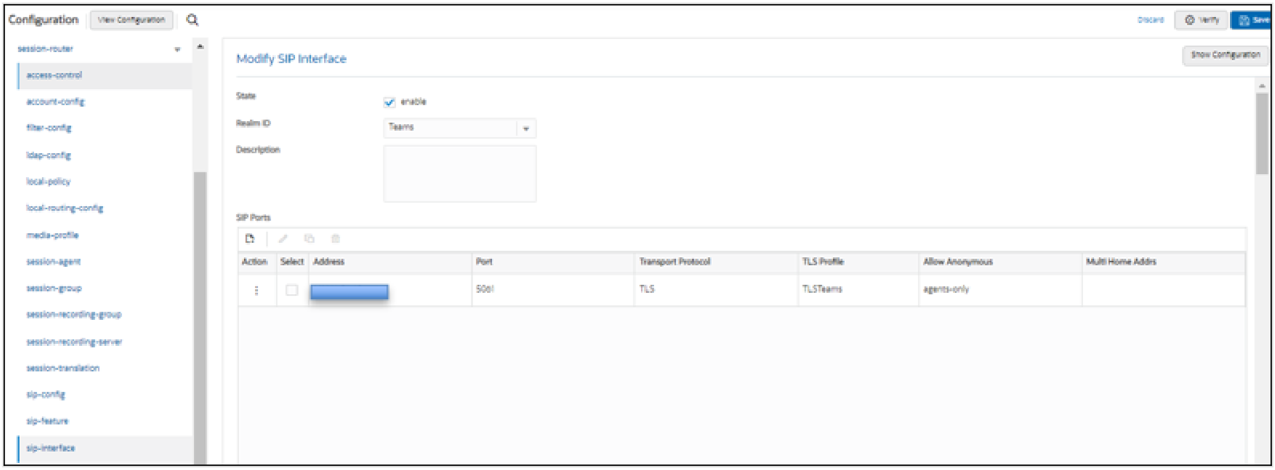
6.10. Configure SIP Interfaces

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

Please Configure sip-interface for the PureCloud as below-

- Tls-profile needs to match the name of the tls-profile previously created
- Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from the Session agents added to the SBC.

Sip-Interface for Microsoft Teams



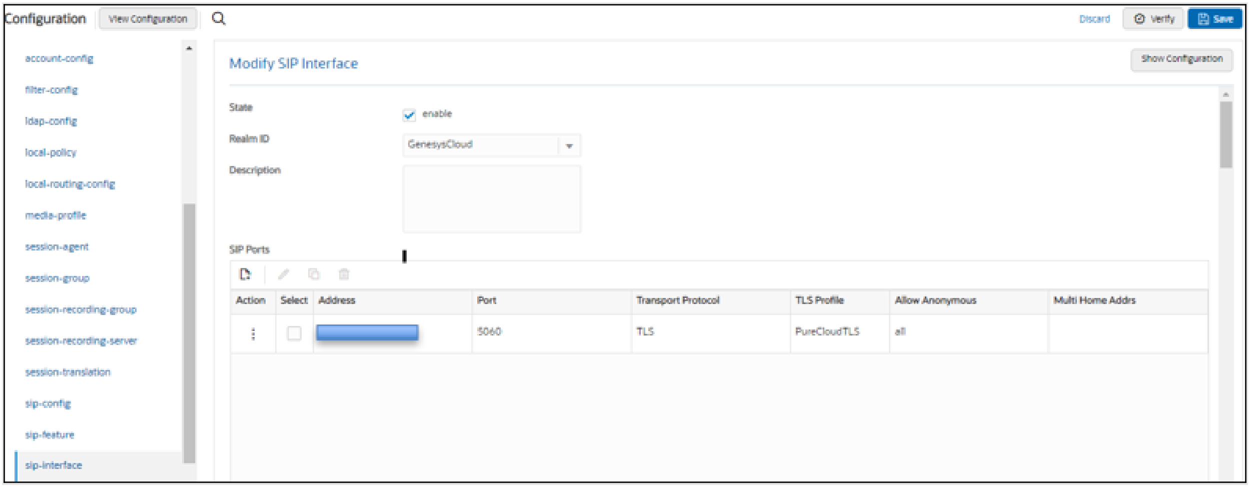
Modify SIP Interface

State	☑ enable
Realm ID	Teams
Description	

SIP Ports

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
⋮	□	[redacted]	5061	TLS	TLSTeams	agents-only	

Sip-interface for Genesys PureCloud



Modify SIP Interface

State ☑ enable

Realm ID GenesysCloud

Description

SIP Ports

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
⋮	□	[redacted]	5060	TLS	PureCloudTLS	all	

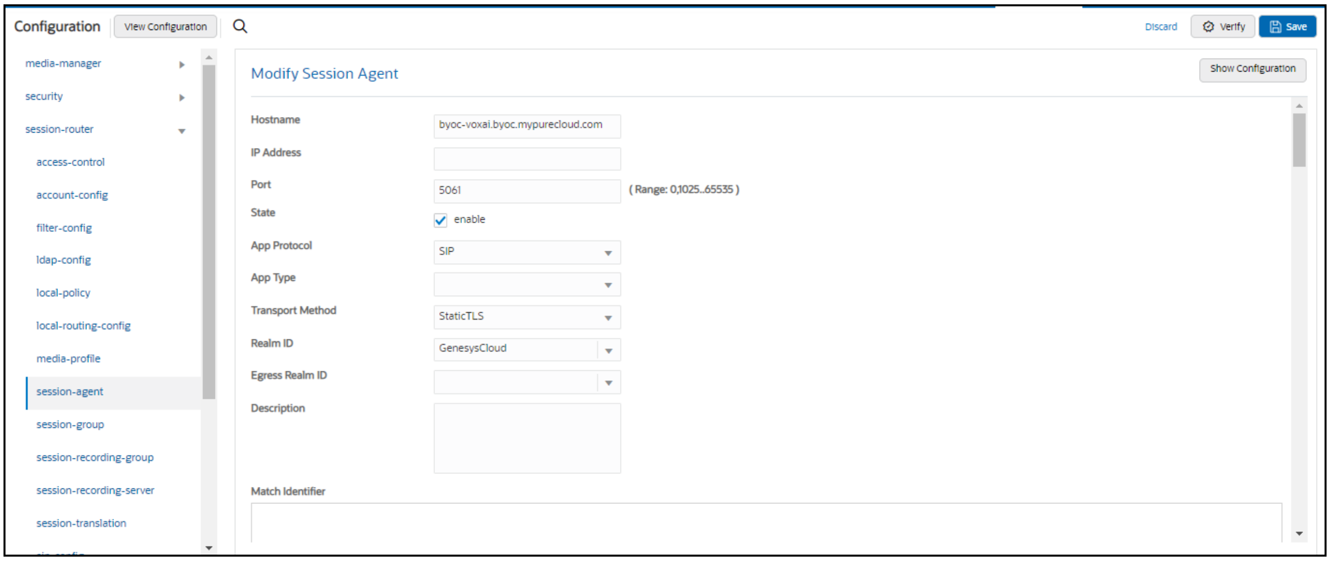
Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

6.11. Configure session-agent

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

Navigate to session-router->Session-Agent and **Configure the session-agents for the Genesys Pure Cloud**

- Host name to “byoc-voxai.byoc.mypurecloud.com”
- port to 5061
- realm-id – needs to match the realm created for the Genesys Pure Cloud
- transport set to “staticTLS”
- ping-method – send OPTIONS message to Microsoft to check health
- ping-interval to 30 secs

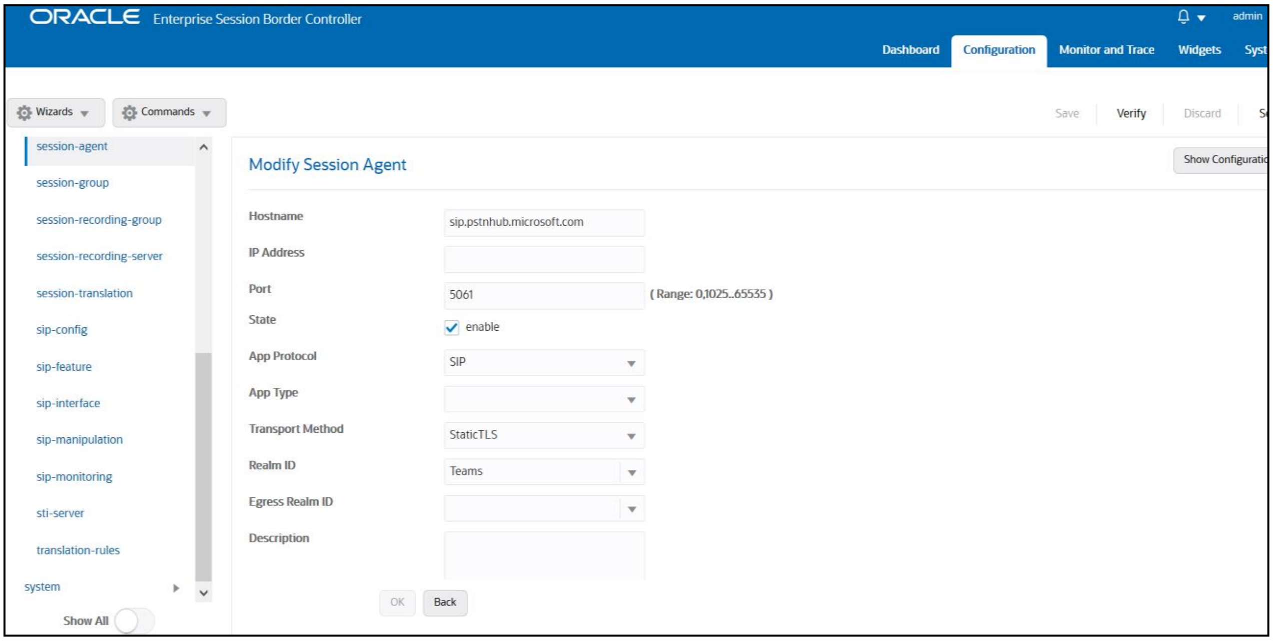


Modify Session Agent

Hostname: byoc-voxai.byoc.mypurecloud.com
IP Address:
Port: 5061 (Range: 0,1025..65535)
State: ☑ enable
App Protocol: SIP
App Type:
Transport Method: StaticTLS
Realm ID: GenesysCloud
Egress Realm ID:
Description:
Match Identifier:

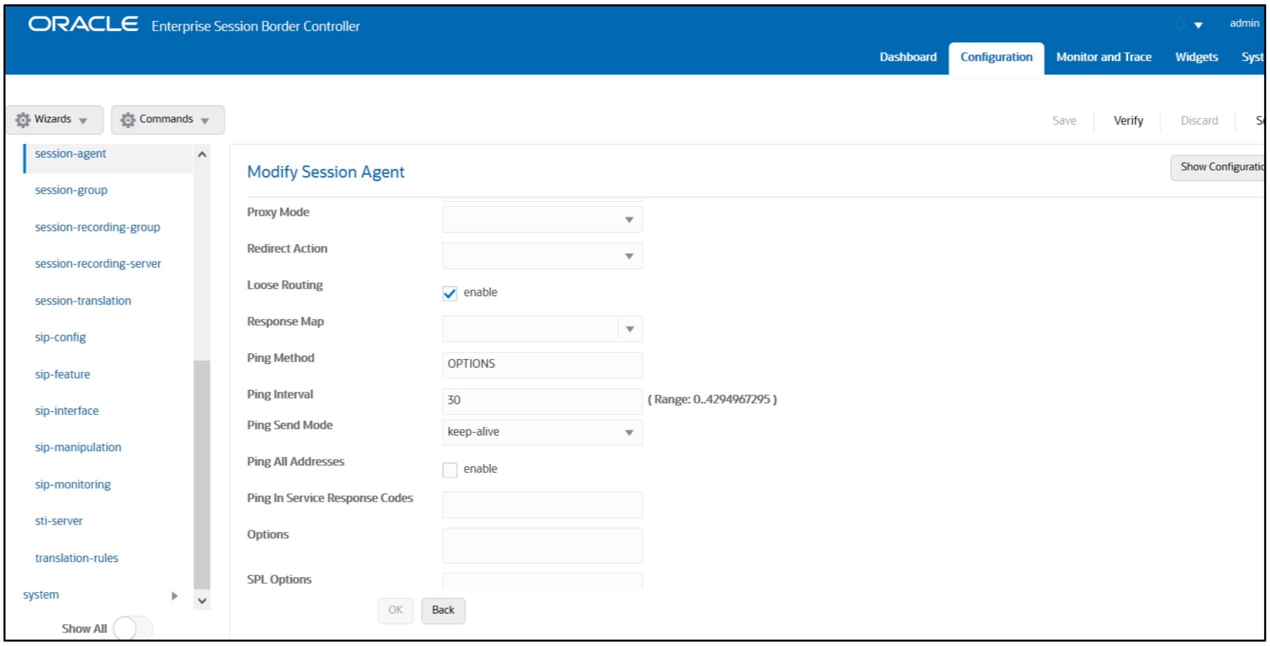
Configure the session-agent for Teams with the following parameters.
Go to session-router->Session-Agent.

- 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



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

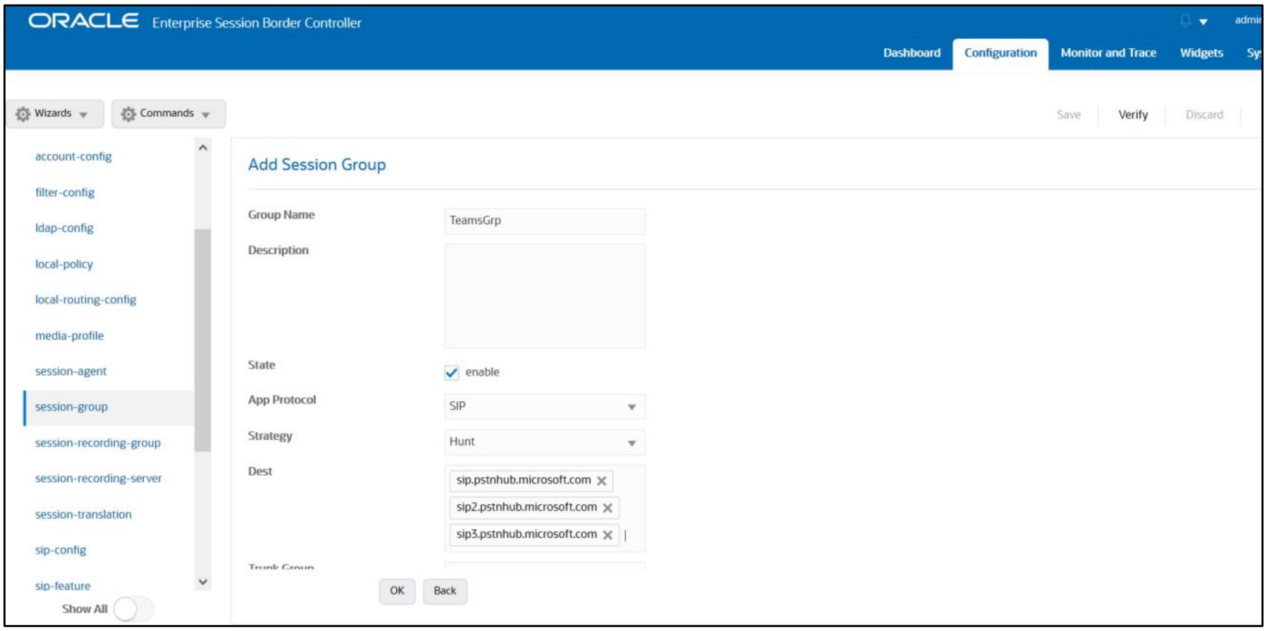
SPL Options

Follow above steps to create 2 more sessions for:

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

6.12. 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

6.13. Configure local-policy

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

Please note that in the below example calls are routed to Twilio Elastic SIP Trunk. Here Twilio Elastic SIP Trunk is the BYOC Carrier. The call flow in the setup is as below –

Inbound calls from PureCloud to Microsoft Teams –

Genesys PureCloud → Oracle SBC → Carrier Trunk (Twilio) → Oracle SBC SBC → MS Teams

Inbound calls from Microsoft Teams to PureCloud -

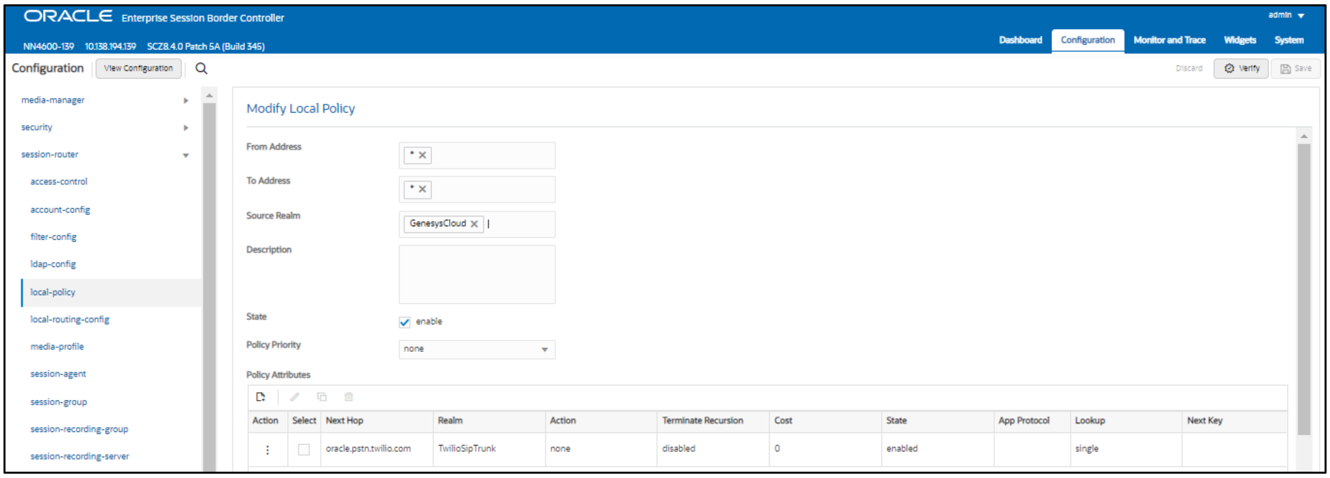
MS Teams→ Oracle SBC → Carrier Trunk (Twilio) → Oracle SBC SBC → Genesys PureCloud

We have multiple application Notes available on the Oracle Technet Page to configure the Oracle SBC with different PBXs and Twilio Elastic SIP Trunk.

Below is the Link to Oracle Technet Page
https://www.oracle.com/technical-resources/documentation/acme-packet.html
Oracle SBC interworking with Genesys PureCloud and Twilio SIP Trunk Application Note can be found here –

https://www.oracle.com/a/otn/docs/oracle-sbc-with-genesys-pure-cloud-and-twillio-sip-trunk.pdf

Following **local-policy routes the calls from the Genesys PureCloud** to Carrier and then the calls are routed from Carrier to Microsoft Teams.



Modify Local Policy

From Address: *

To Address: *

Source Realm: GenesysCloud

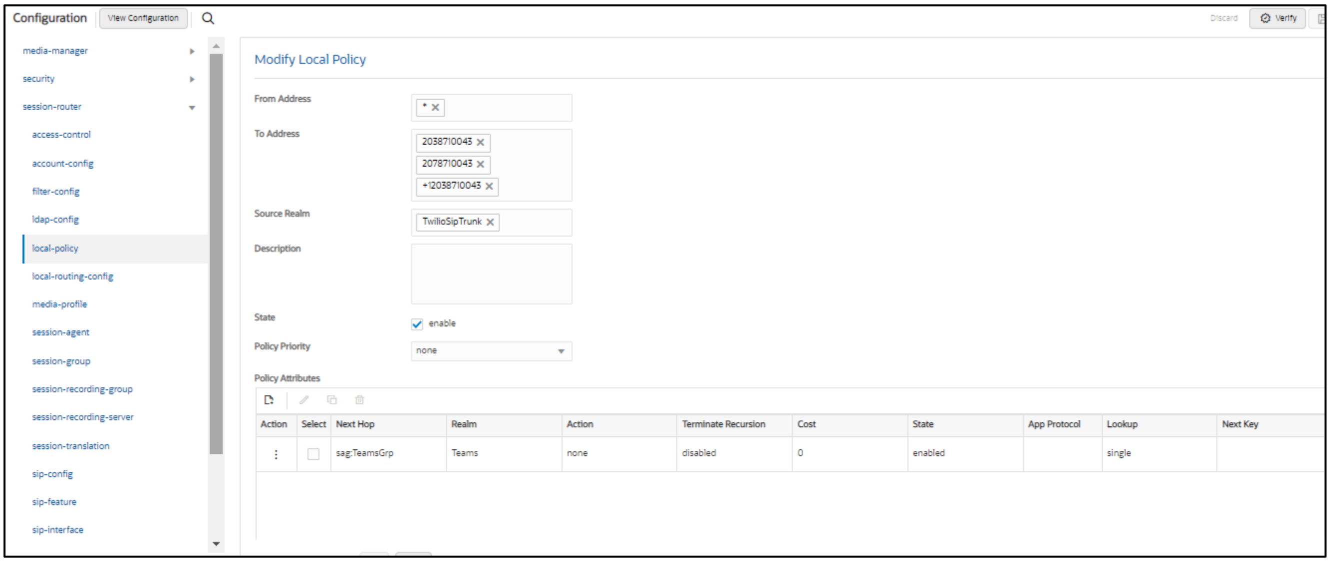
Description:

State: ☑ enable

Policy Priority: none

Policy Attributes

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



Modify Local Policy

From Address: * ✕

To Address: 2038710043 ✕
2078710043 ✕
+12038710043 ✕

Source Realm: TwilioSipTrunk ✕

Description:

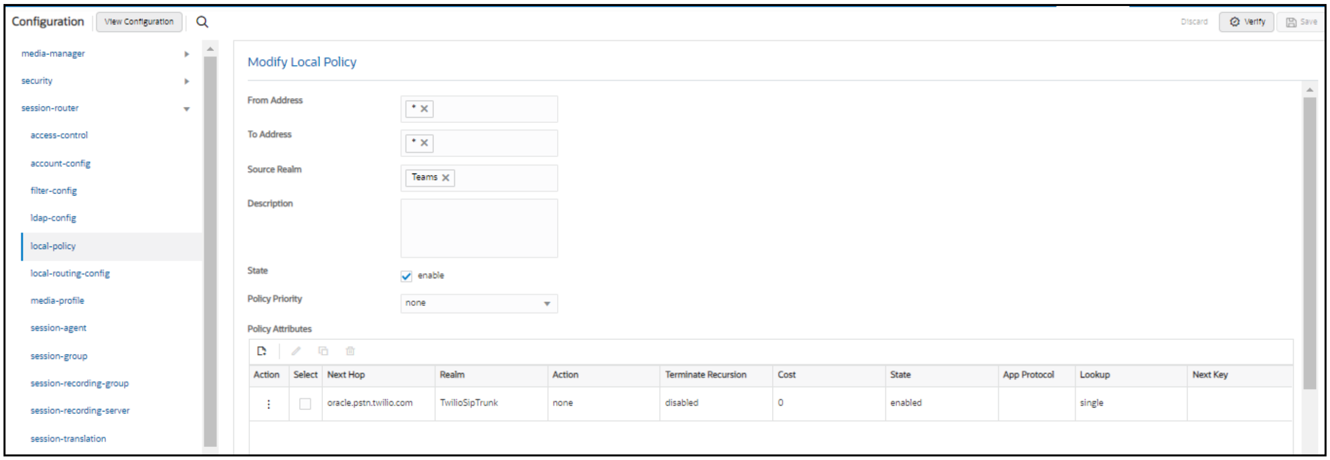
State: ☑ enable

Policy Priority: none

Policy Attributes

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

Following **local-policy routes the calls from the Microsoft Teams** to Carrier and then the calls are routed from Carrier to Genesys PureCloud.



Modify Local Policy

From Address: * ✕

To Address: * ✕

Source Realm: Teams ✕

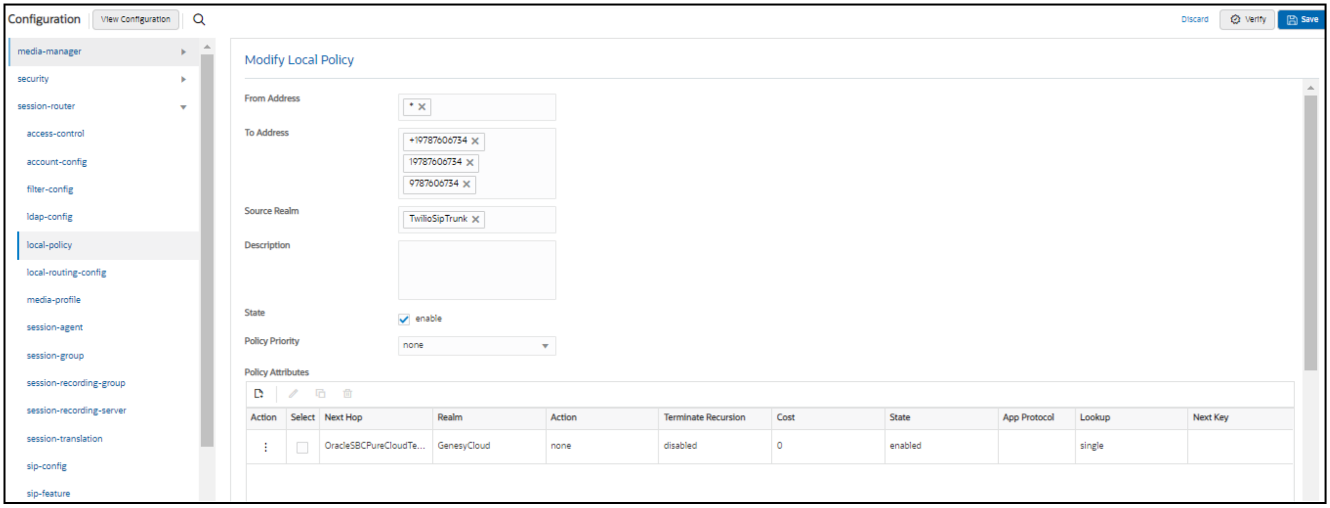
Description:

State: ☑ enable

Policy Priority: none

Policy Attributes

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



Modify Local Policy

From Address: * ✕

To Address: +19787606734 ✕
19787606734 ✕
9787606734 ✕

Source Realm: TwilioSipTrunk ✕

Description:

State: ☑ enable

Policy Priority: none

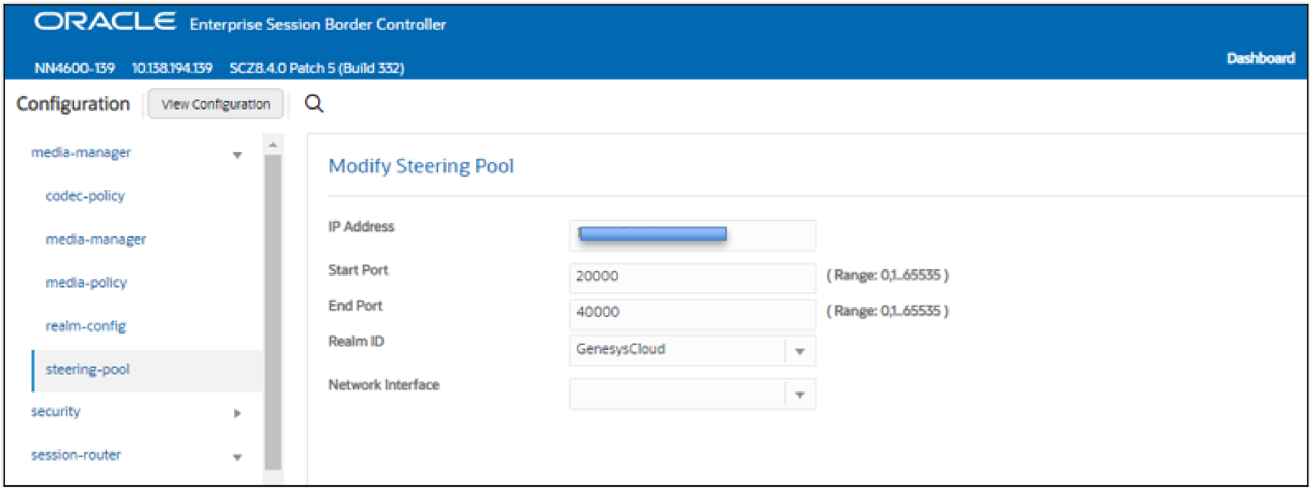
Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
⋮	□	OracleSBCPureCloudTe...	GenesyCloud	none	disabled	0	enabled		single	

6.13. Configure steering-pool

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

PureCloud Steering pool.



Modify Steering Pool

IP Address [redacted]

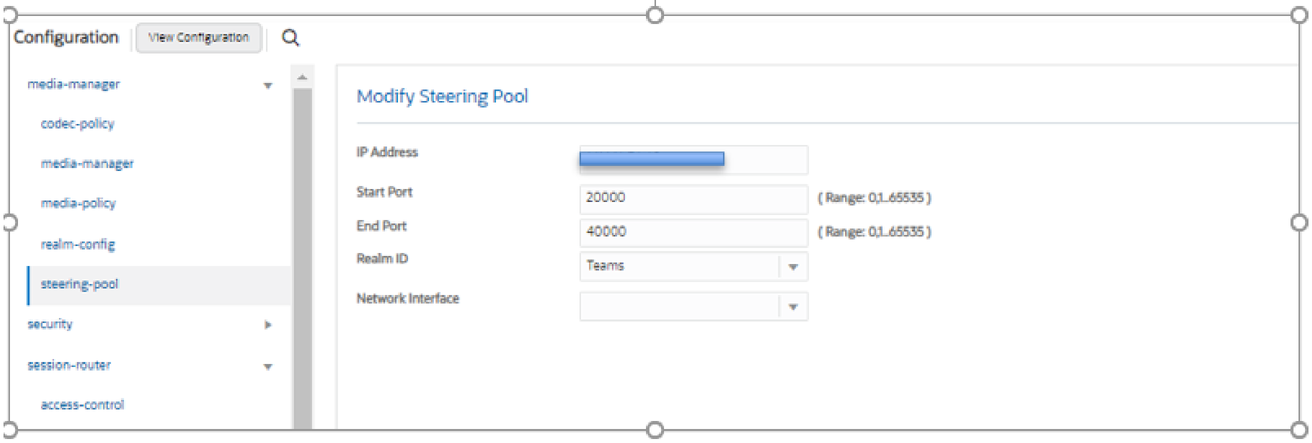
Start Port 20000 (Range: 0,1..65535)

End Port 40000 (Range: 0,1..65535)

Realm ID GenesysCloud

Network Interface

Microsoft Teams Steering Pool



Modify Steering Pool

IP Address [redacted]

Start Port 20000 (Range: 0,1..65535)

End Port 40000 (Range: 0,1..65535)

Realm ID Teams

Network Interface

6.14. Configure additional Parameters

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 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.

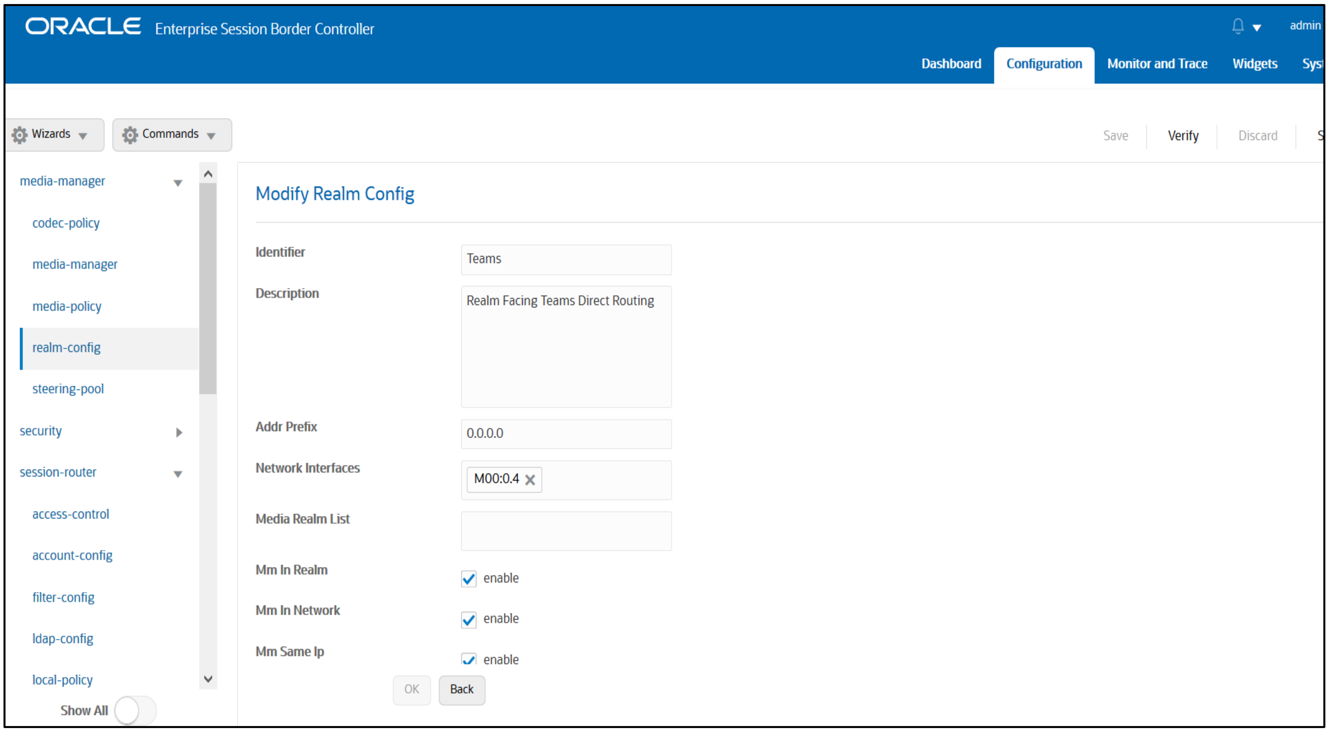
Teams FQDN in URI:

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

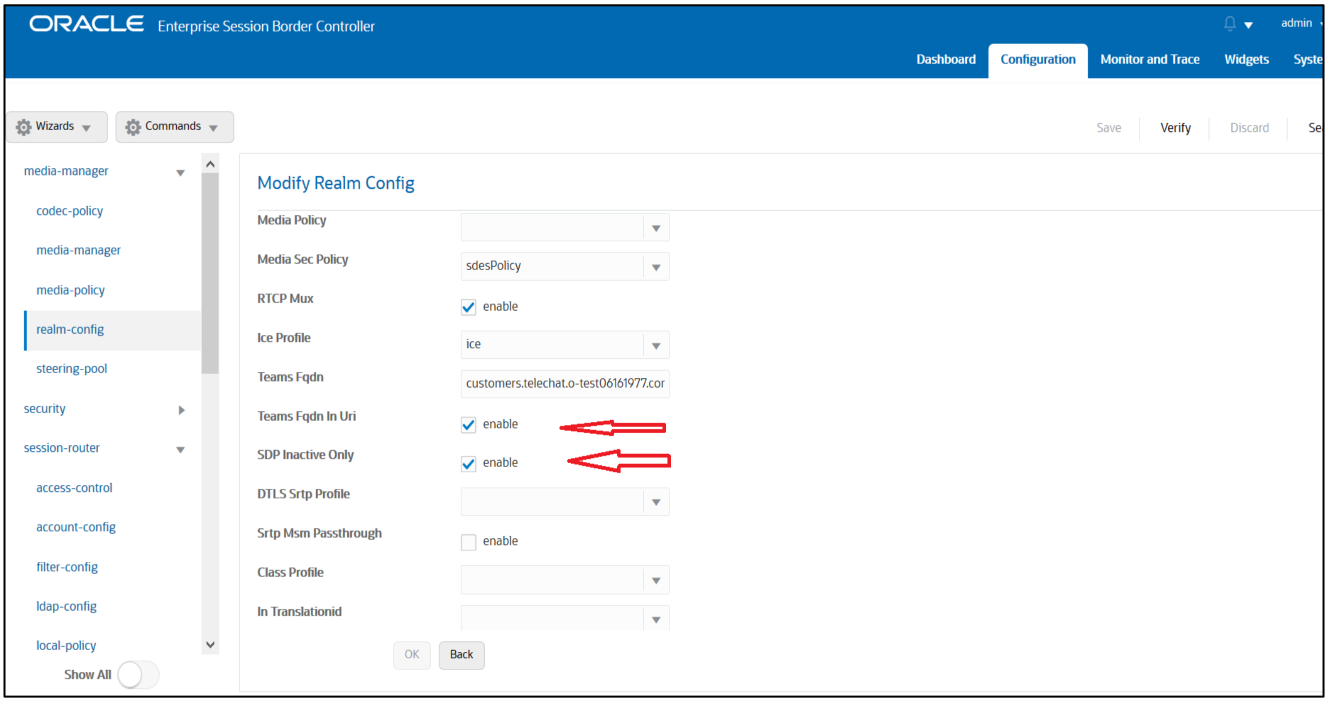
Network Interfaces: M00:0.4 ✕

Media Realm List:

Mm In Realm: ☑ enable

Mm In Network: ☑ enable

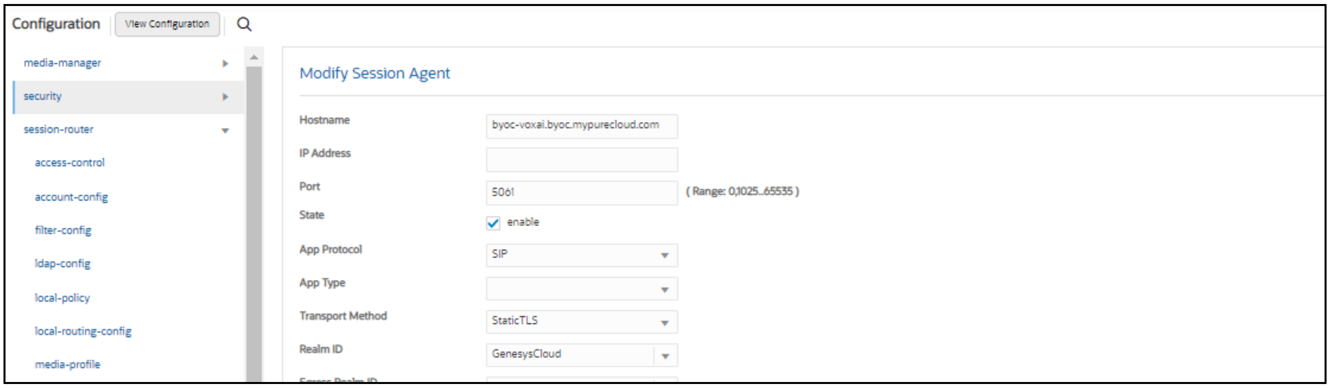
Mm Same Ip: ☑ enable



Modify Realm Config

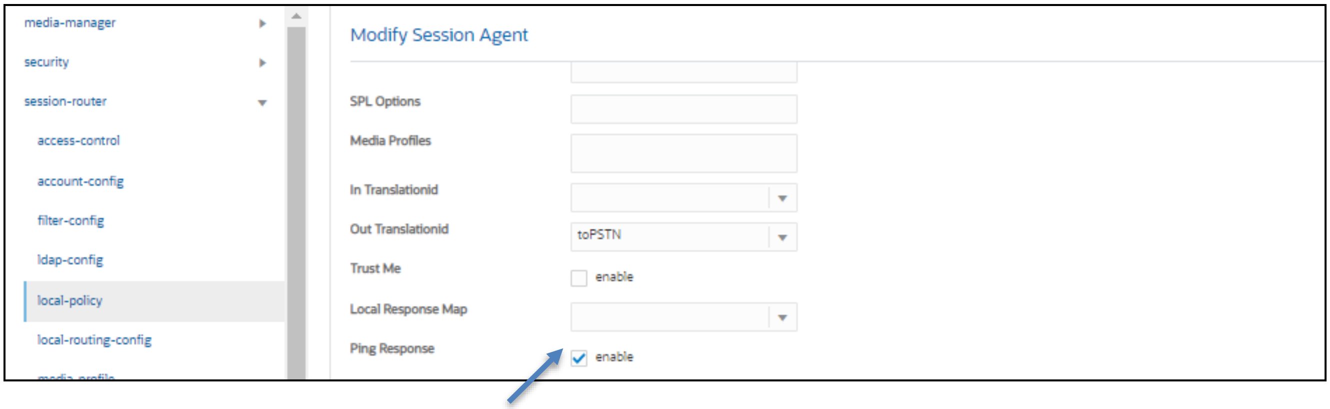
Media Policy	
Media Sec Policy	sdesPolicy
RTCP Mux	☑ enable
Ice Profile	ice
Teams Fqdn	customers.telechat.o-test06161977.cor
Teams Fqdn In Uri	☑ enable
SDP Inactive Only	☑ enable
DTLS Srtp Profile	
Srtp Msm Passthrough	□ enable
Class Profile	
In Translationid	

The third parameter is found under the **Session agent** configuration element and will be enabled on all session agents configured for Microsoft Teams and Genesys PureCloud .Below is an example of the parameter **Ping response** enabled on PureCloud Session-Agent. Similarly, the parameter should be enabled for other Microsoft Teams Session-Agents.



Modify Session Agent

Hostname	byoc-voxai.byoc.mypurecloud.com
IP Address	
Port	5061 (Range: 0,1025..65535)
State	☑ enable
App Protocol	SIP
App Type	
Transport Method	StaticTLS
Realm ID	GenesysCloud



Modify Session Agent

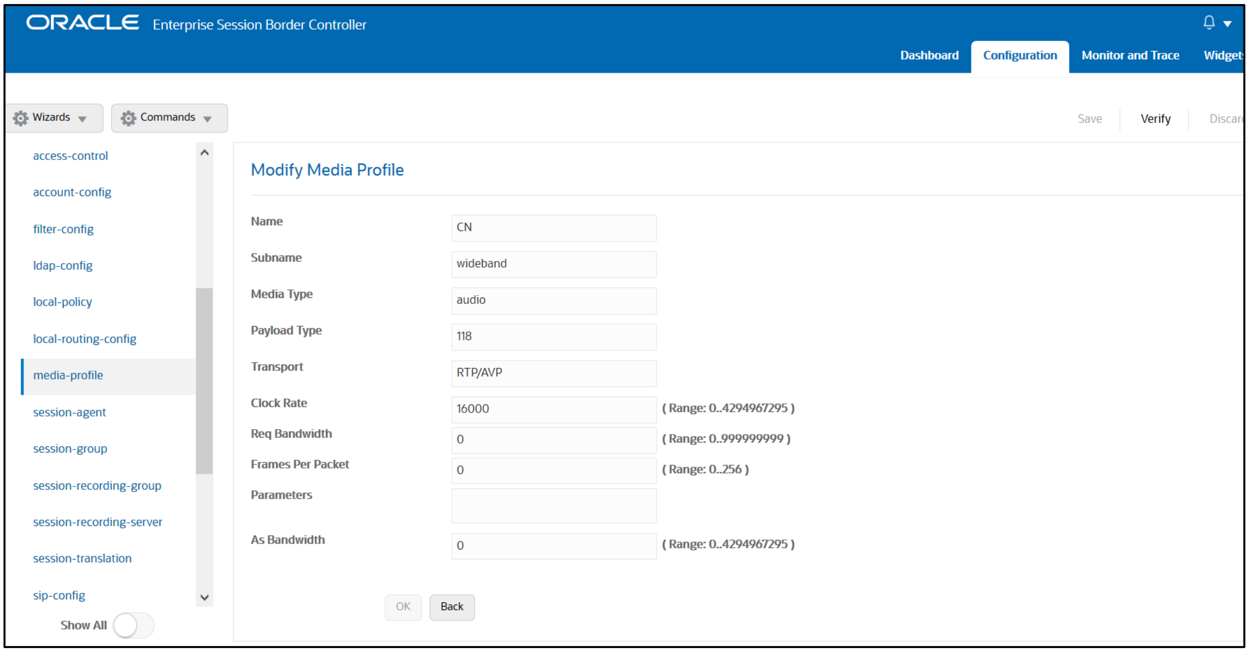
SPL Options	
Media Profiles	
In Translationid	
Out Translationid	toPSTN
Trust Me	□ enable
Local Response Map	
Ping Response	☑ enable

6.15. 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



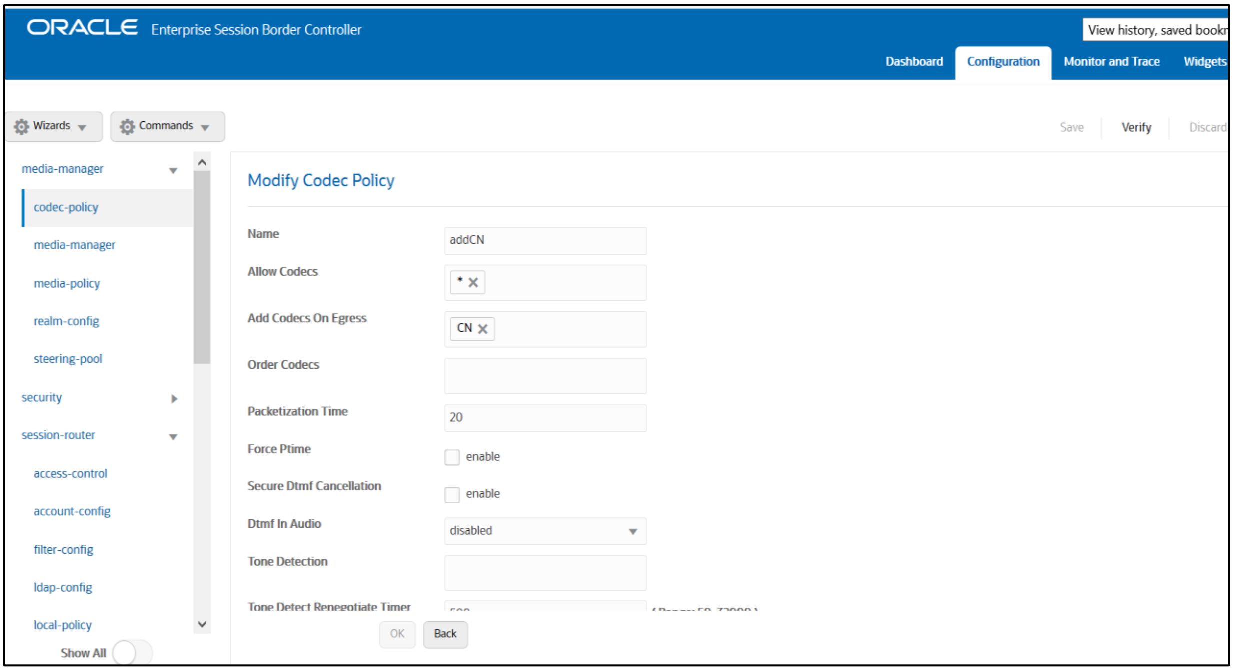
Modify Media Profile

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



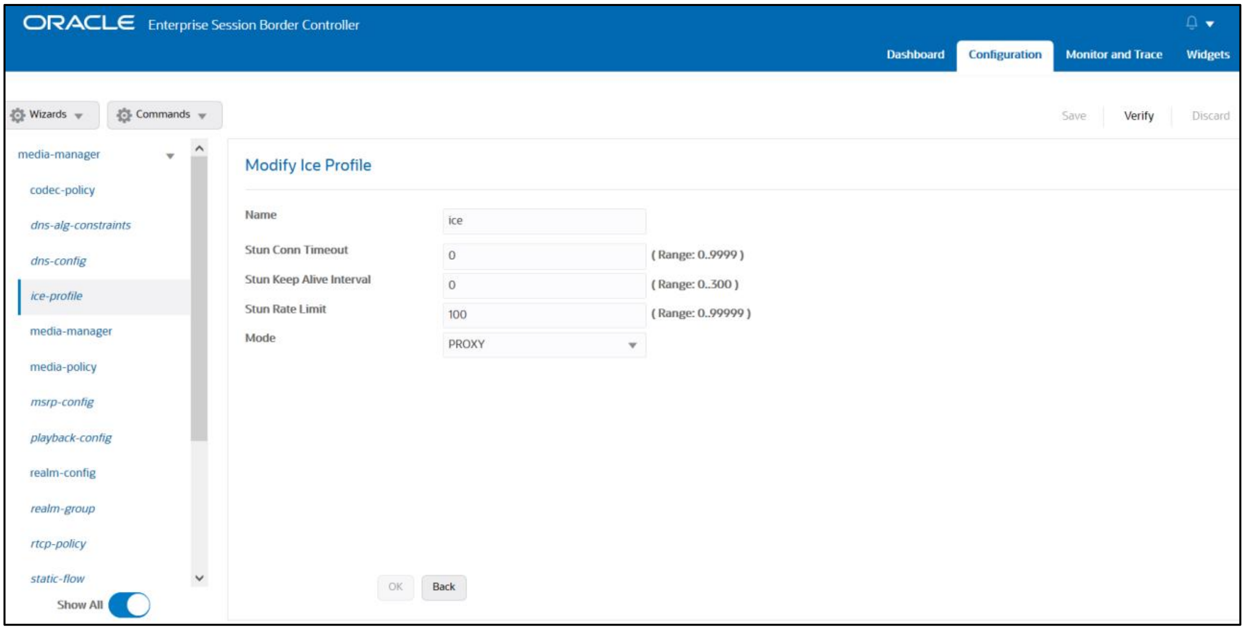
Modify Codec Policy

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.**

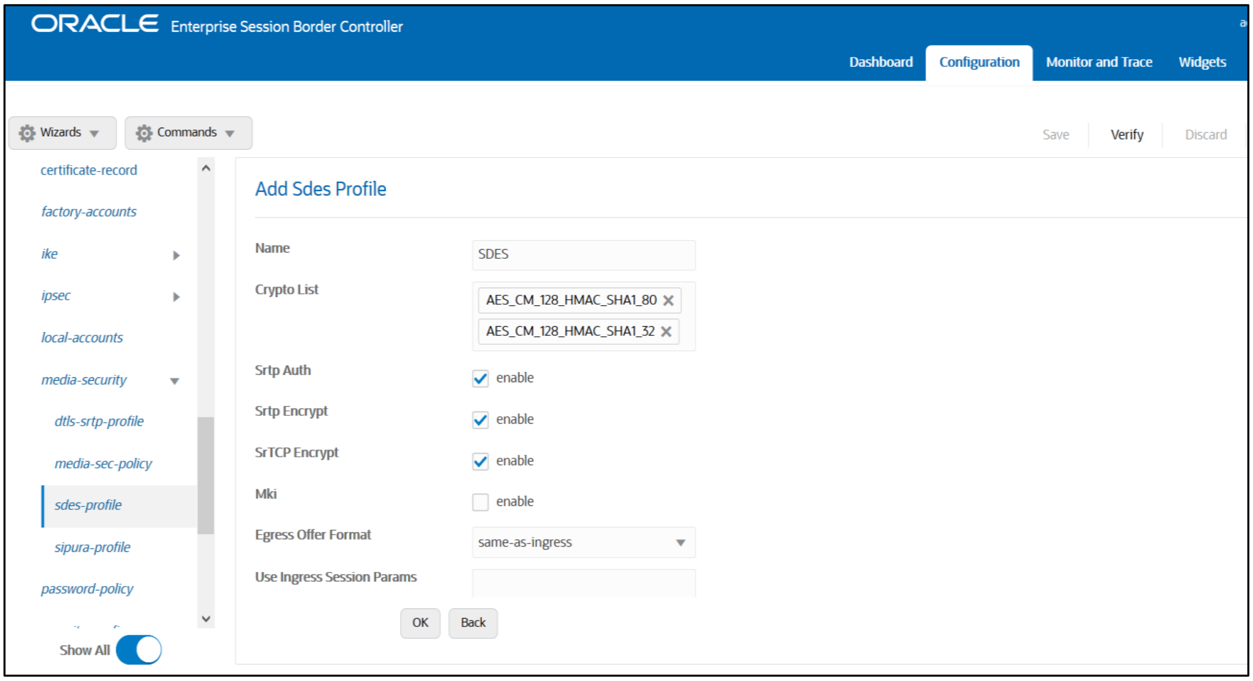


Modify Ice Profile

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	

6.15. Configure sdes profile

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

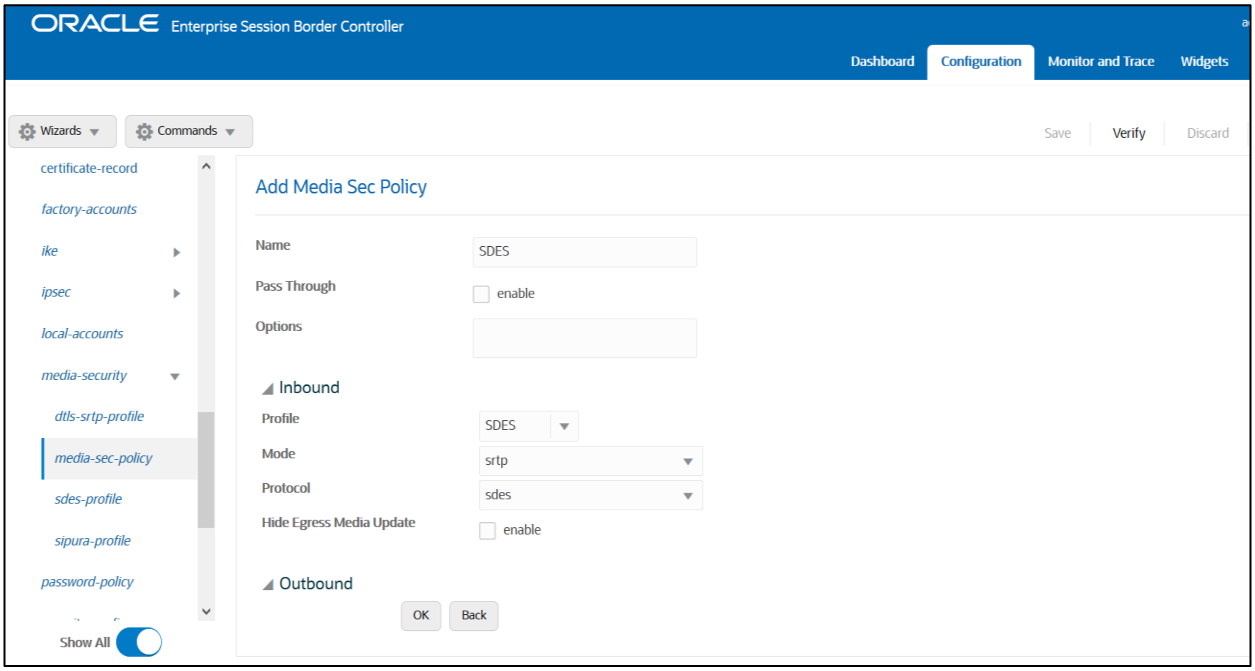


Add Sdes Profile

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	

6.16. Configure Media Security Profile

Please Navigate 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 PureCloud and Microsoft Teams Realm.



Add Media Sec Policy

Name: SDES

Pass Through: □ enable

Options:

Inbound

Profile: SDES

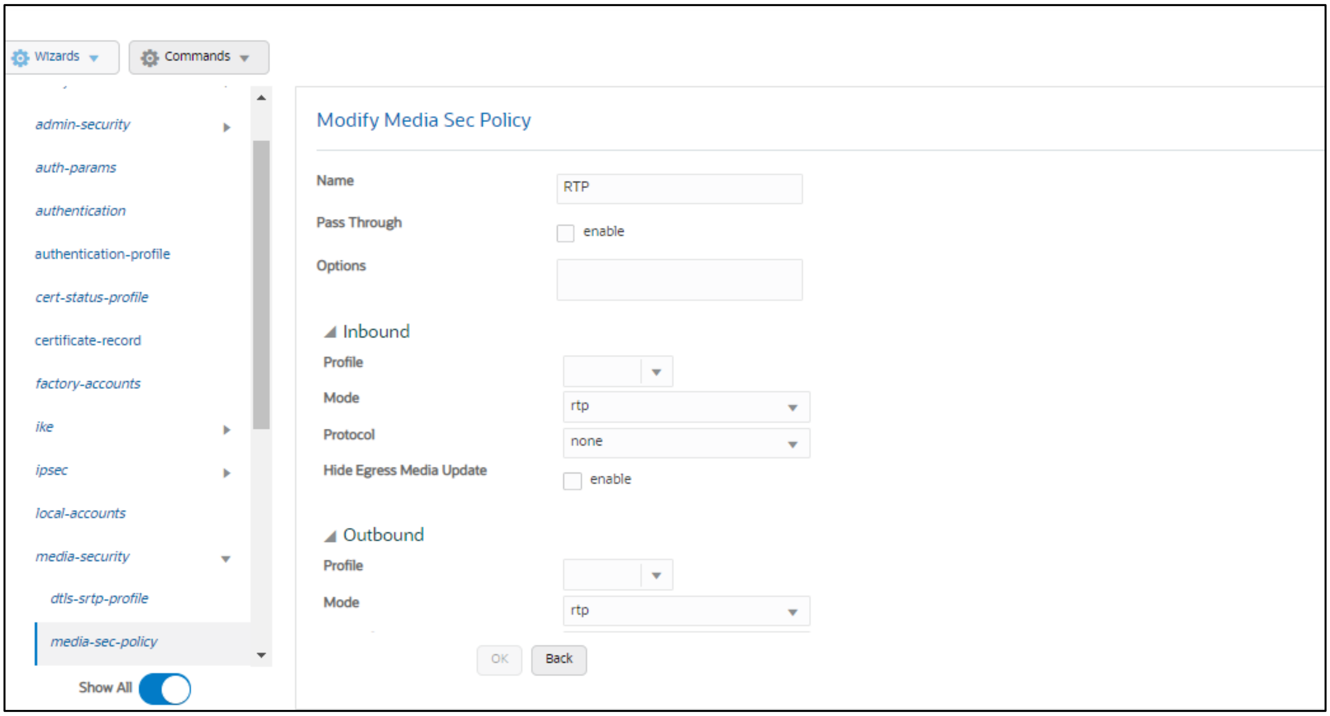
Mode: srtp

Protocol: sdes

Hide Egress Media Update: □ enable

Outbound

Note- Both Microsoft Teams and Genesys PureCloud in this setup require TLS SRTP to work. If any of your network component require RTP, another Media Sec policy as show below and named **RTP** ,to convert srtp to rtp can be created and applied to the appropriate realm as needed.



Modify Media Sec Policy

Name: RTP

Pass Through: □ enable

Options:

Inbound

Profile:

Mode: rtp

Protocol: none

Hide Egress Media Update: □ enable

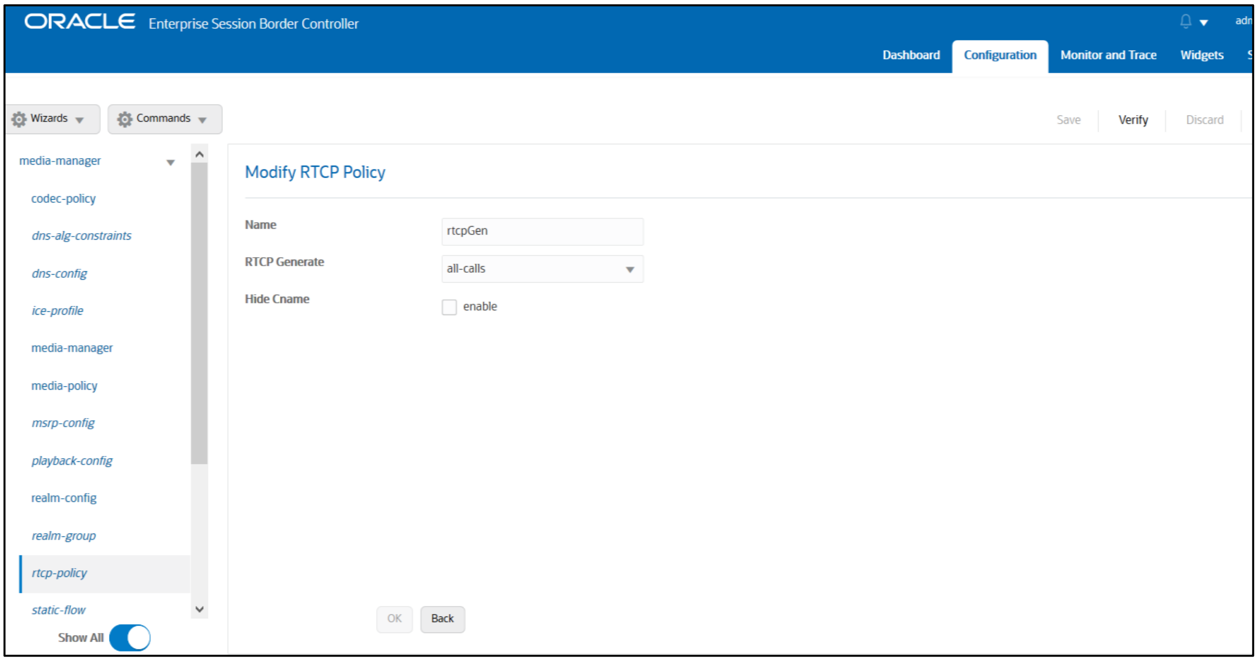
Outbound

Profile:

Mode: rtp

6.17 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

6.18 Access Control

To enhance the security of your Oracle Session Border Controller, we recommend configuration access controls to limit traffic to only trusted IP addresses on all public facing interfaces

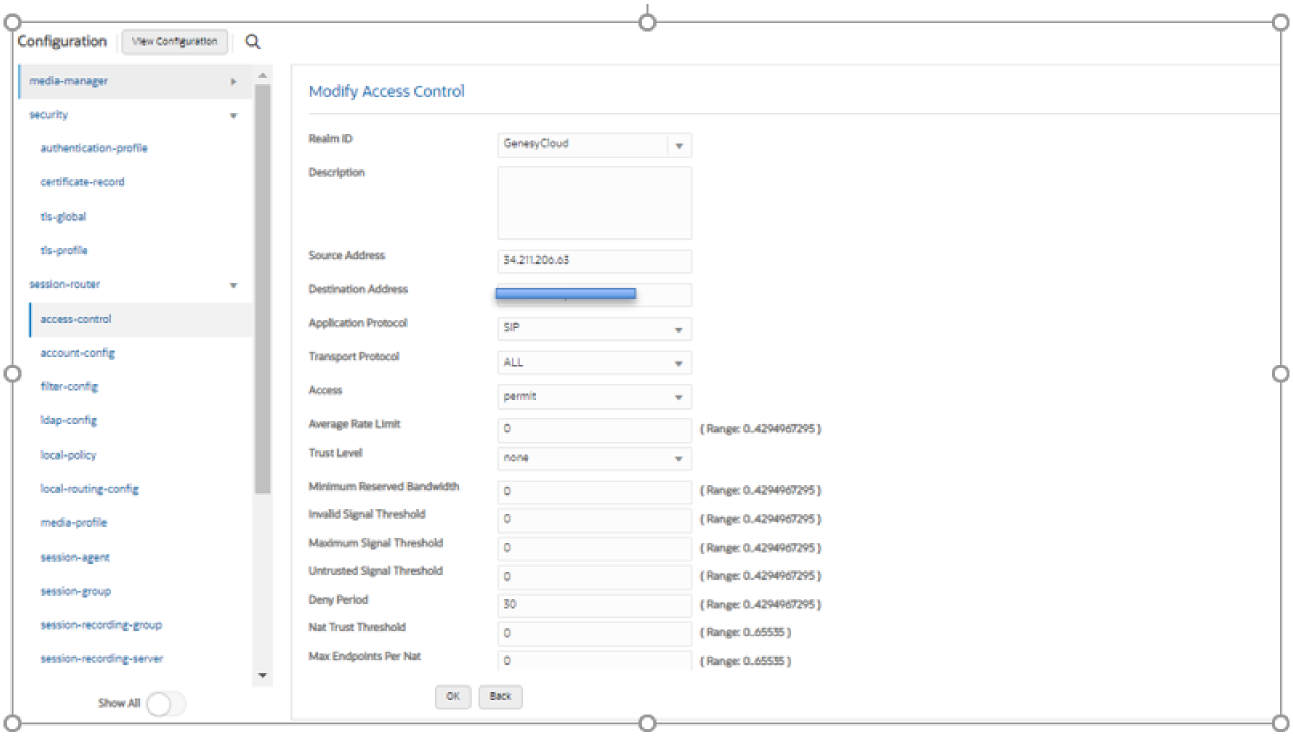
GUI Path: session-router/access-control

Please use the example below to configure access controls in your environment for both PureCloud IP's, as well as SIP Trunk IP's (if applicable).

byoc.mypurecloud.com resolves to the following load balancer IP Addresses

52.203.12.137	lb01.byoc.us-east-1.mypurecloud.com
54.82.241.192	lb02.byoc.us-east-1.mypurecloud.com
54.82.241.68	lb03.byoc.us-east-1.mypurecloud.com
54.82.188.43	lb04.byoc.us-east-1.mypurecloud.com

Configure access-control for each IP PureCloud IP Address or Subnet as shown in the below example.



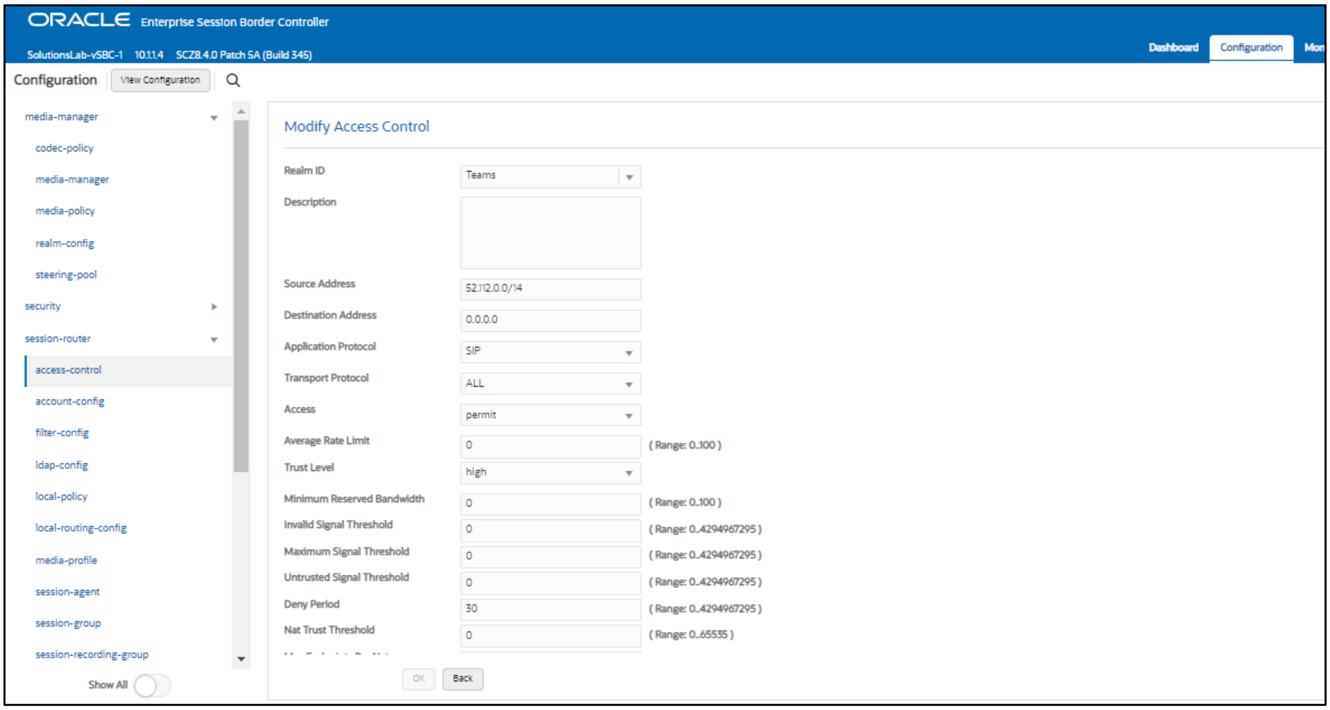
Modify Access Control

Realm ID: GenesyCloud
Description:
Source Address: 54.211.206.63
Destination Address: [redacted]
Application Protocol: SIP
Transport Protocol: ALL
Access: permit
Average Rate Limit: 0 (Range: 0..4294967295)
Trust Level: none
Minimum Reserved Bandwidth: 0 (Range: 0..4294967295)
Invalid Signal Threshold: 0 (Range: 0..4294967295)
Maximum Signal Threshold: 0 (Range: 0..4294967295)
Untrusted Signal Threshold: 0 (Range: 0..4294967295)
Deny Period: 30 (Range: 0..4294967295)
Nat Trust Threshold: 0 (Range: 0..65535)
Max Endpoints Per Nat: 0 (Range: 0..65535)

Similarly create ACL entries for each Microsoft Teams IP Addresses as shown in the below example. 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 t/session-router/access-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	(Range: 0..100)
Trust Level	high	
Minimum Reserved Bandwidth	0	(Range: 0..100)
Invalid Signal Threshold	0	(Range: 0..4294967295)
Maximum Signal Threshold	0	(Range: 0..4294967295)
Untrusted Signal Threshold	0	(Range: 0..4294967295)
Deny Period	30	(Range: 0..4294967295)
Nat Trust Threshold	0	(Range: 0..65535)

Notice the trust level on this ACL is set to high. When the trust level on an ACL is set to the same value of as the access control trust level of its associated realm, this create an implicit deny, so only traffic from IP addresses configured as ACL's with the same trust level will be allowed to send traffic to the SBC. For more information about trust level on ACL's and Realms, please see the SBC Security Guide, Page 3-10.

7. Configuring the Oracle SBC through Config Assistant

When you first log on to the Oracle 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 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.**

Configuration package is available starting in release nnSCZ840p7 and nnSCZ900p2.

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 Genesys PureCloud. We will choose a Generic SIP Trunk on the other Side for Carrier Connectivity. We also have configuration Assistant for Microsoft Teams related for Microsoft Teams related configuration. Please follow the latest Microsoft Teams Application Note to get instructions on configuring Microsoft Teams via Configuration Assistant Template.

The Application notes can be found at - https://www.oracle.com/technical-resources/documentation/acme-packet.html

The pre-requisites 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 PureCloud supported CA to sign certificate once CSR is generated by the SBC.

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

Initial GUI Access

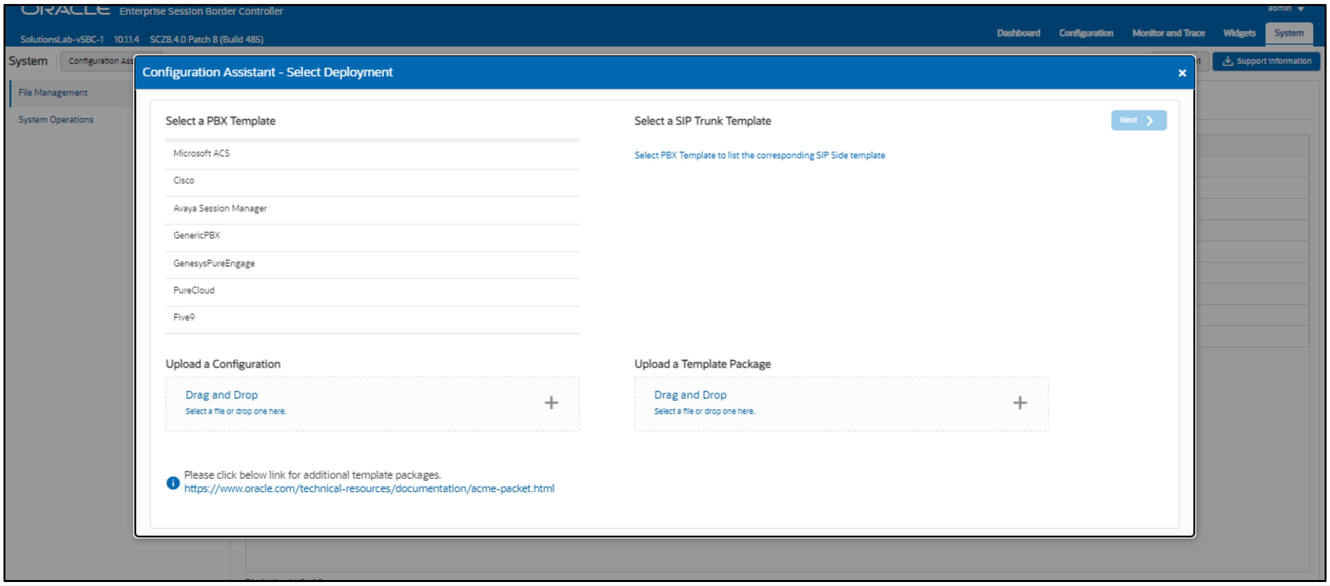
The Oracle SBC WebGui can be accessed by entering the following in your web browser. http(s)://<SBC Management IP>.

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

PureCloud Configuration Assistant

For a new SBC deployment, once access to the GUI is configured, you will see the following when logging in for the first time:



Configuration Assistant - Select Deployment

Select a PBX Template

- Microsoft ACS
- Cisco
- Avaya Session Manager
- GenericPBX
- GenesysPureEngage
- PureCloud
- Five9

Select a SIP Trunk Template

Select PBX Template to list the corresponding SIP Side template

Upload a Configuration

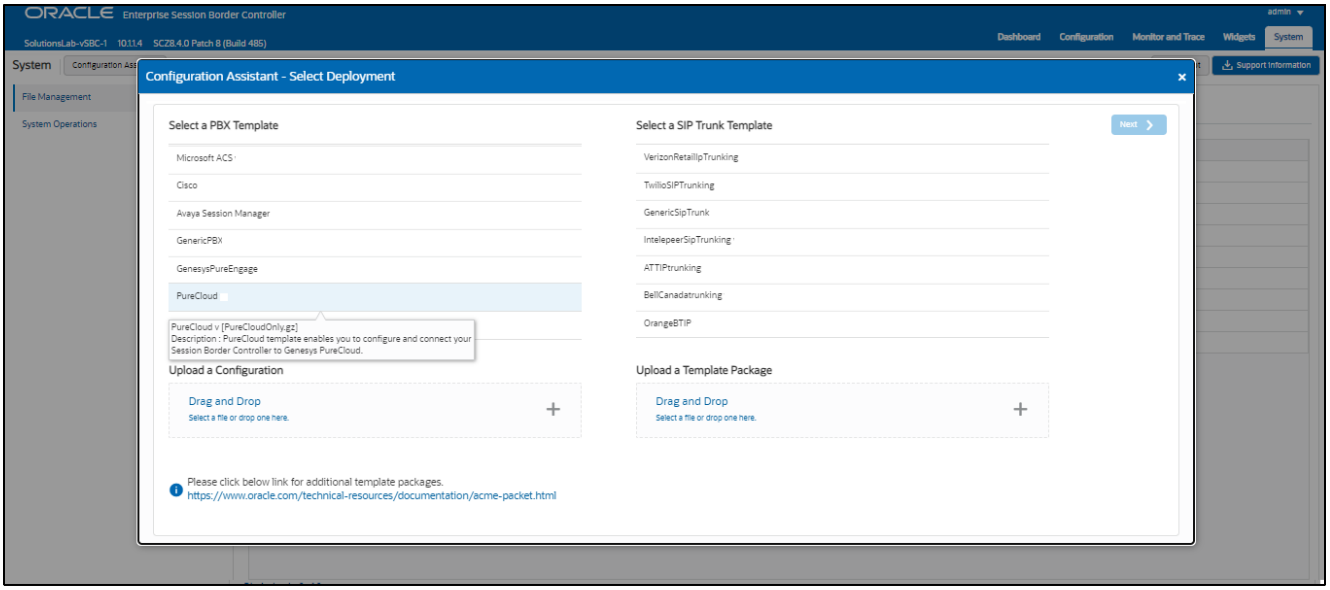
Drag and Drop
Select a file or drop one here.

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

Under PBX template, we’ll select PureCloud template. This brings up a list of available sip trunk templates.



Configuration Assistant - Select Deployment

Select a PBX Template

- Microsoft ACS
- Cisco
- Avaya Session Manager
- GenericPBX
- GenesysPureEngage
- PureCloud

PureCloud v [PureCloudOnly.gz]
Description : PureCloud template enables you to configure and connect your Session Border Controller to Genesys PureCloud.

Select a SIP Trunk Template

- VerizonRetailIpTrunking
- TwilioSIPTrunking
- GenericSipTrunk
- IntelepeerSipTrunking
- ATTIPtrunking
- BellCanadatrunking
- OrangeBTIP

Upload a Configuration

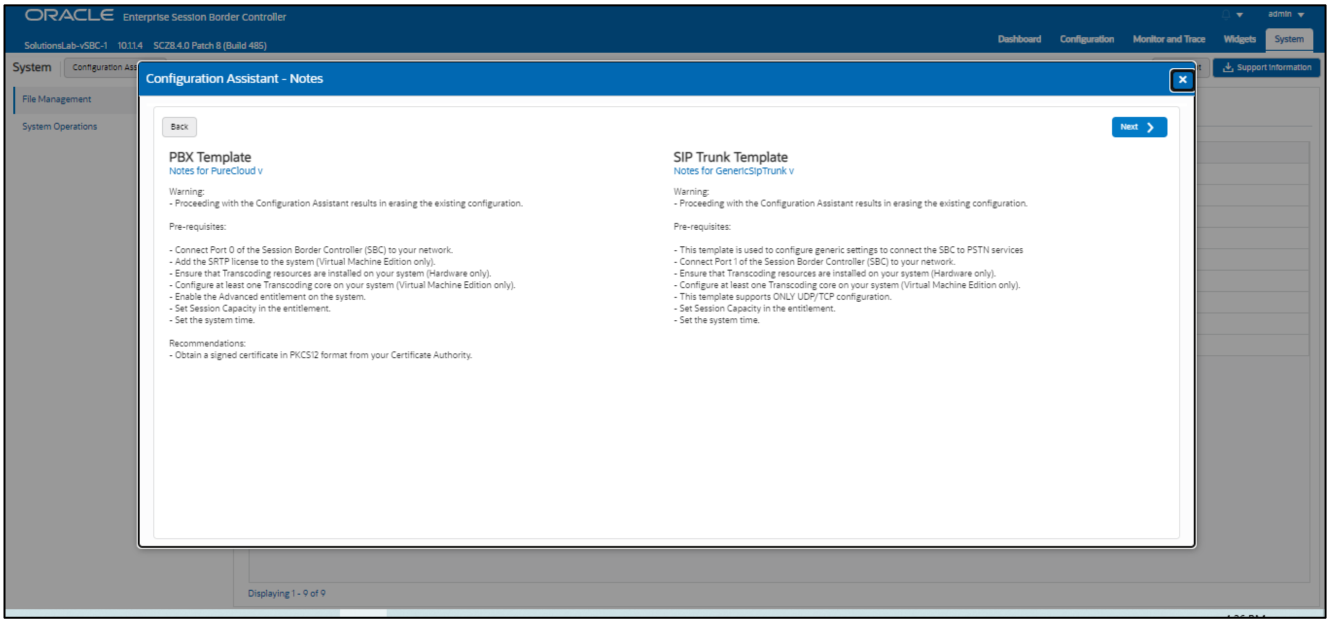
Drag and Drop
Select a file or drop one here.

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

Select a sip trunk template and click Next at the top to access the Notes page. Pay close attention to the information here, as this is a list of warnings, pre-requisites, and recommendations:



Configuration Assistant - Notes

PBX Template
Notes for PureCloud v

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

Recommendations:
- Obtain a signed certificate in PKCS12 format from your Certificate Authority.

SIP Trunk Template
Notes for GenericSipTrunk v

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

Pre-requisites:

- This template is used to configure generic settings to connect the SBC to PSTN services
- 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).
- This template supports ONLY UDP/TCP configuration.
- Set Session Capacity in the entitlement.
- Set the system time.

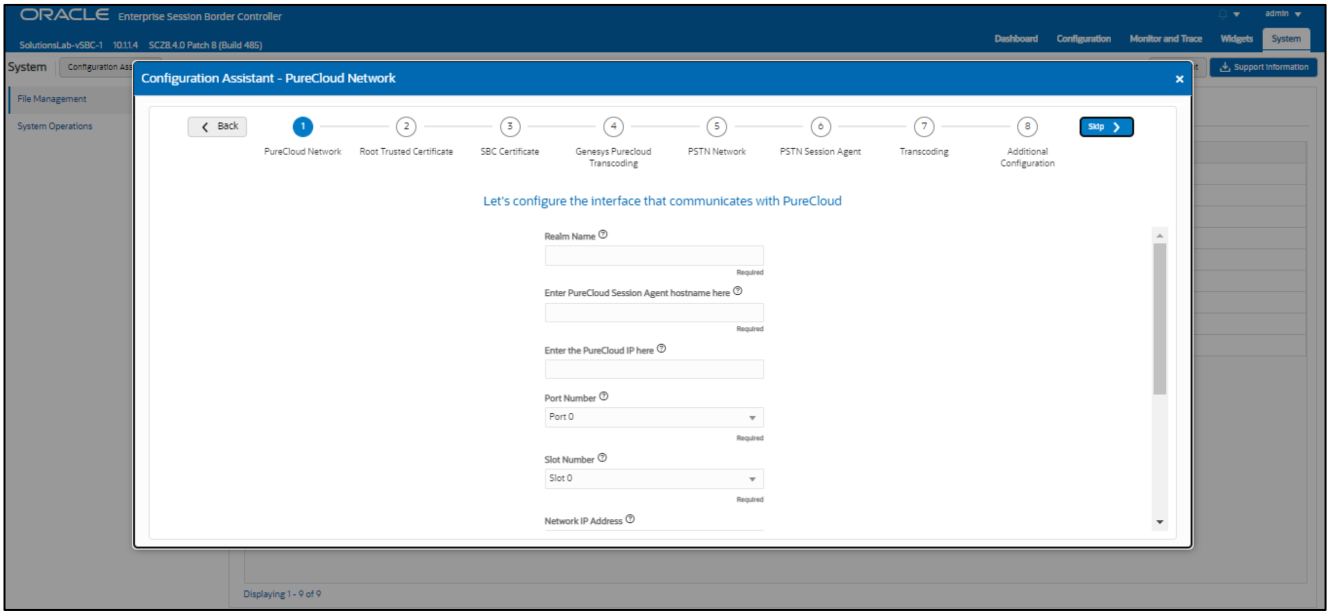
Clicking “Next” on the Notes page triggers the configuration assistant to do a system check. This ensures that all of the system requirements for the platform and sip trunk you have selected have been met before proceeding to configuration pages. If they have not been met, you will be greeted by a page providing the opportunity to setup entitlements, add license keys, etc. before moving on to the configuration.

Once all requirements for your selected templates have been satisfied, you can proceed to the configuration pages.

Page 1- PureCloud Network

Page 1 of the template is where you will configure the network information to connect to PureCloud Network.

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”.



Configuration Assistant - PureCloud Network

Let's configure the interface that communicates with PureCloud

Realm Name (Required)

Enter PureCloud Session Agent hostname here (Required)

Enter the PureCloud IP here

Port Number: Port 0 (Required)

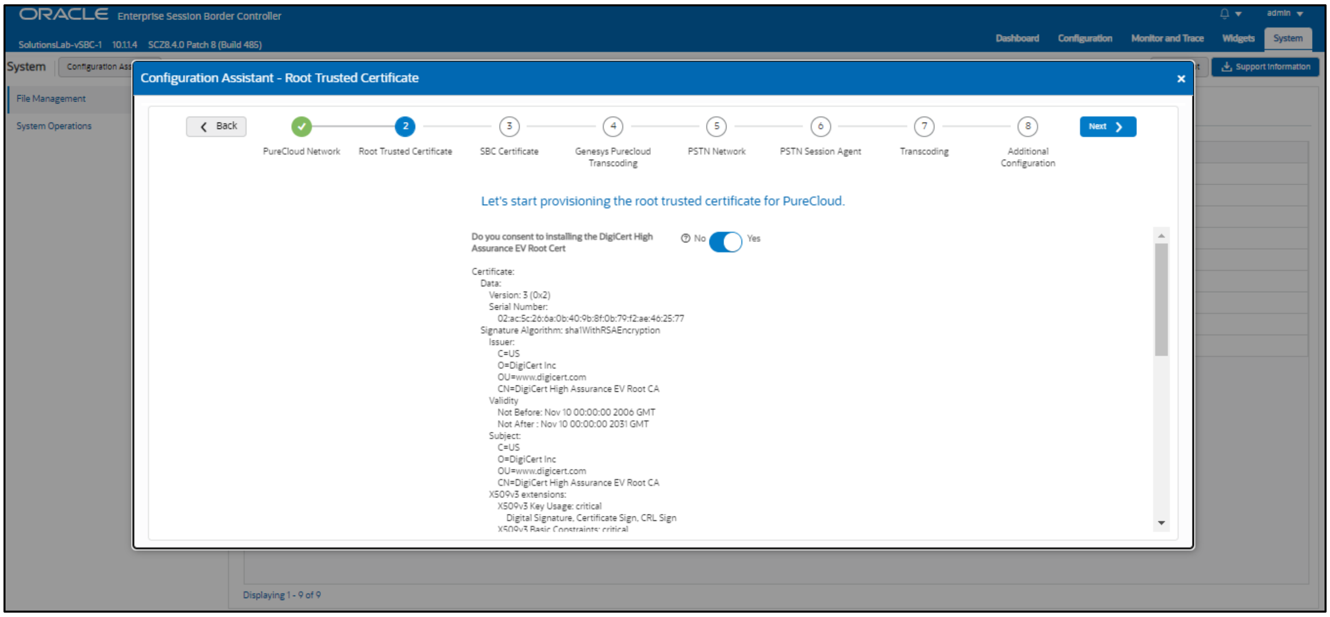
Slot Number: Slot 0 (Required)

Network IP Address

Page 2 - Import DigiCert Trusted CA Certificate for PureCloud

Page 2 of this template is where the SBC will import the **DigiCert High Assurance EV Root Cert CA** certificate, which PureCloud uses to sign the certificates it presents to the SBC during the TLS handshake.

Importing the PureCloud Root CA certs is enabled by default.



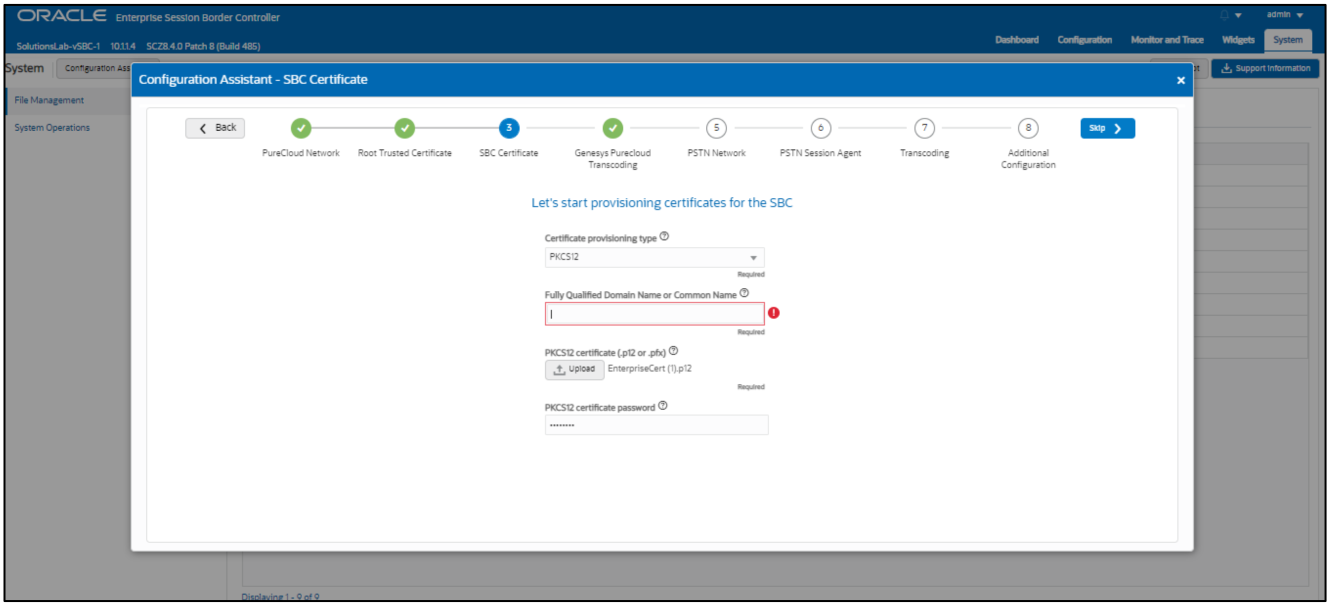
Let's start provisioning the root trusted certificate for PureCloud.

Do you consent to installing the DigiCert High Assurance EV Root Cert: No / Yes (toggle on)

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      02:ac:5c:26:6a:0b:40:9b:8f:0b:79:f2:ae:46:25:77
  Signature Algorithm: sha1WithRSAEncryption
    Issuer:
      C=US
      O=DigiCert Inc
      OU=www.digicert.com
      CN=DigiCert High Assurance EV Root CA
    Validity
      Not Before: Nov 10 00:00:00 2006 GMT
      Not After : Nov 10 00:00:00 2031 GMT
    Subject:
      C=US
      O=DigiCert Inc
      OU=www.digicert.com
      CN=DigiCert High Assurance EV Root CA
    X509v3 extensions:
      X509v3 Key Usage: critical
        Digital Signature, Certificate Sign, CRL Sign
      X509v3 Basic Constraints: critical
```

Page 3 - SBC Certificates for PureCloud side

By default, the SBC is set to import a certificate in PKCS12 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 signed from one of the PureCloud Supported CA Vendors, and enter the certificates password.



Let's start provisioning certificates for the SBC

Certificate provisioning type: PKCS12 (Required)

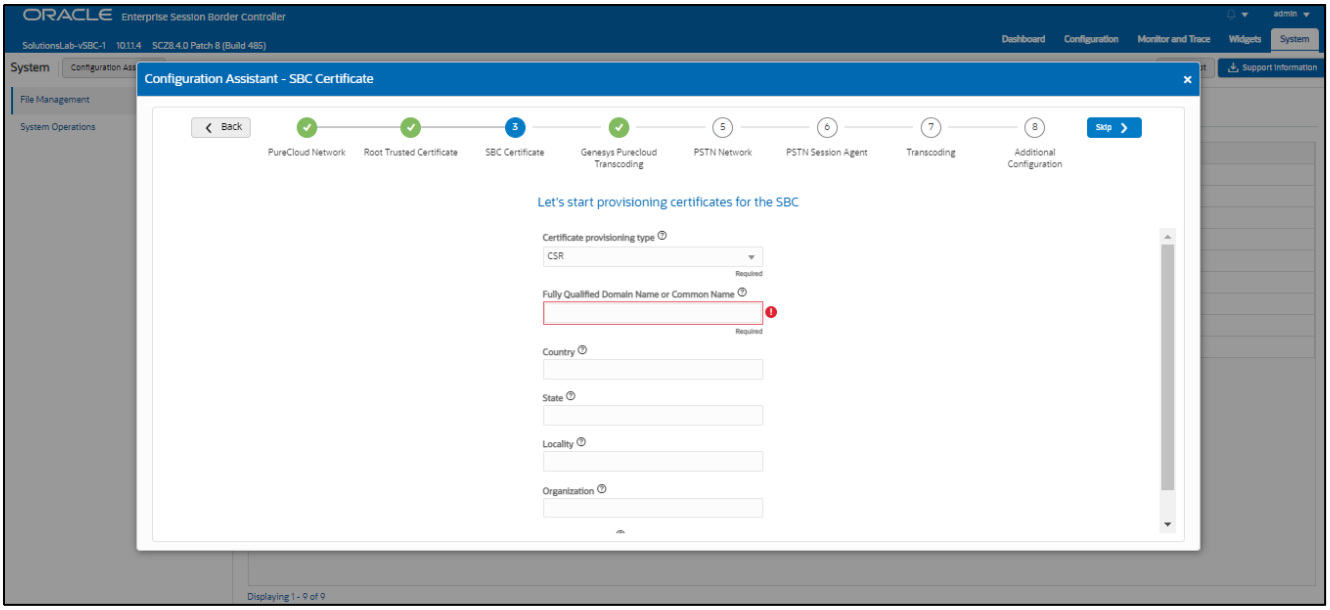
Fully Qualified Domain Name or Common Name: (Required)

PKCS12 certificate (.p12 or .pfx): EnterpriseCert (1).p12 (Required)

PKCS12 certificate password: ••••••••

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 PureCloud 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

Locality

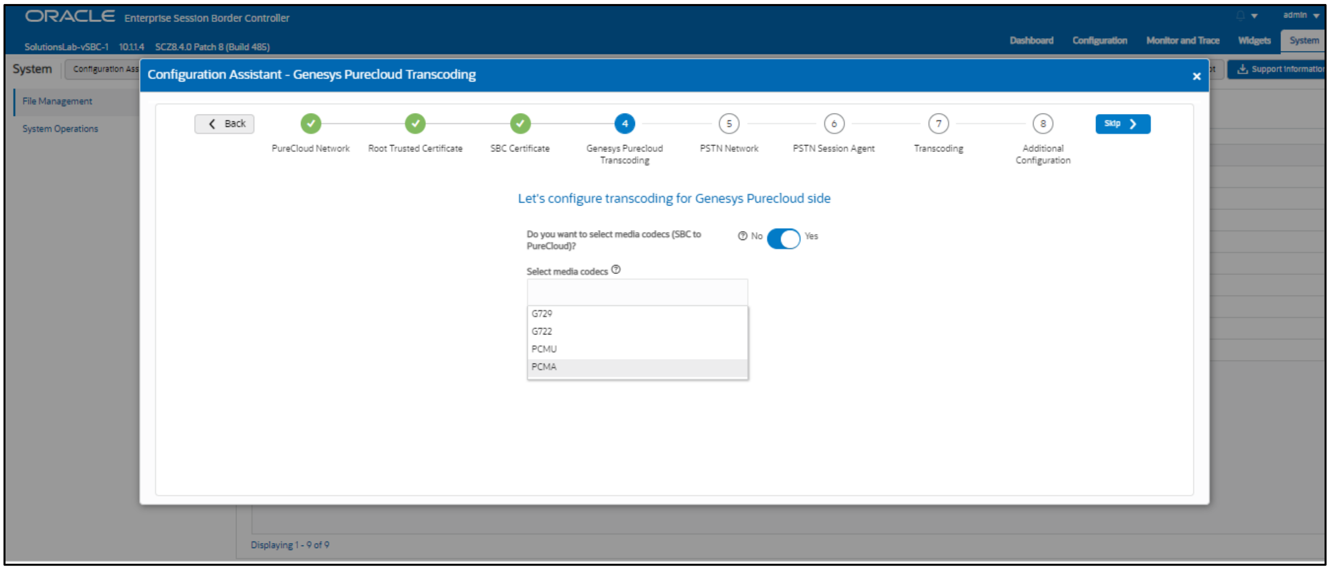
Organization

Page 4 – PureCloud side Transcoding

Page 4 is where you will be able to configure transcoding between the SBC and PureCloud.

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 PureCloud. 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 - Genesys Purecloud Transcoding

Let's configure transcoding for Genesys Purecloud side

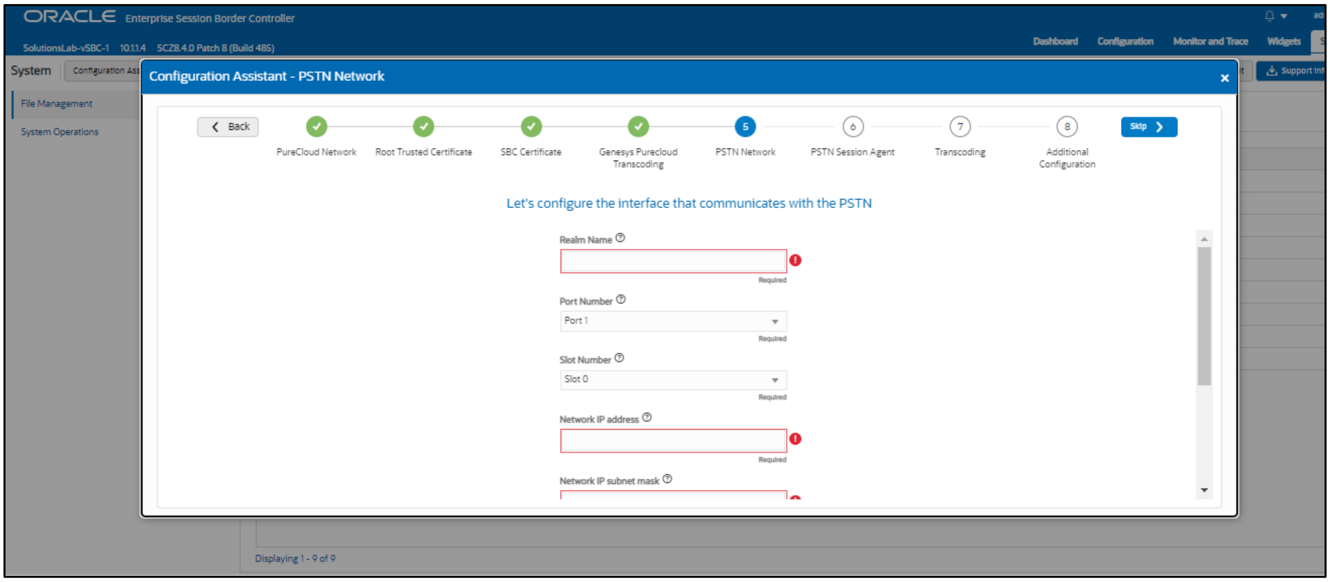
Do you want to select media codecs (SBC to PureCloud)? No [✓ Yes]

Select media codecs

G729
G722
PCMU
PCMA

Page 5 – PSTN Sip Trunk Network

Page 5 of the template is where you will configure the network information to connect to PSTN SIP trunk Network. Please fill the required fields and Press Next.



Configuration Assistant - PSTN Network

Let's configure the interface that communicates with the PSTN

Realm Name
Required

Port Number
Port 1
Required

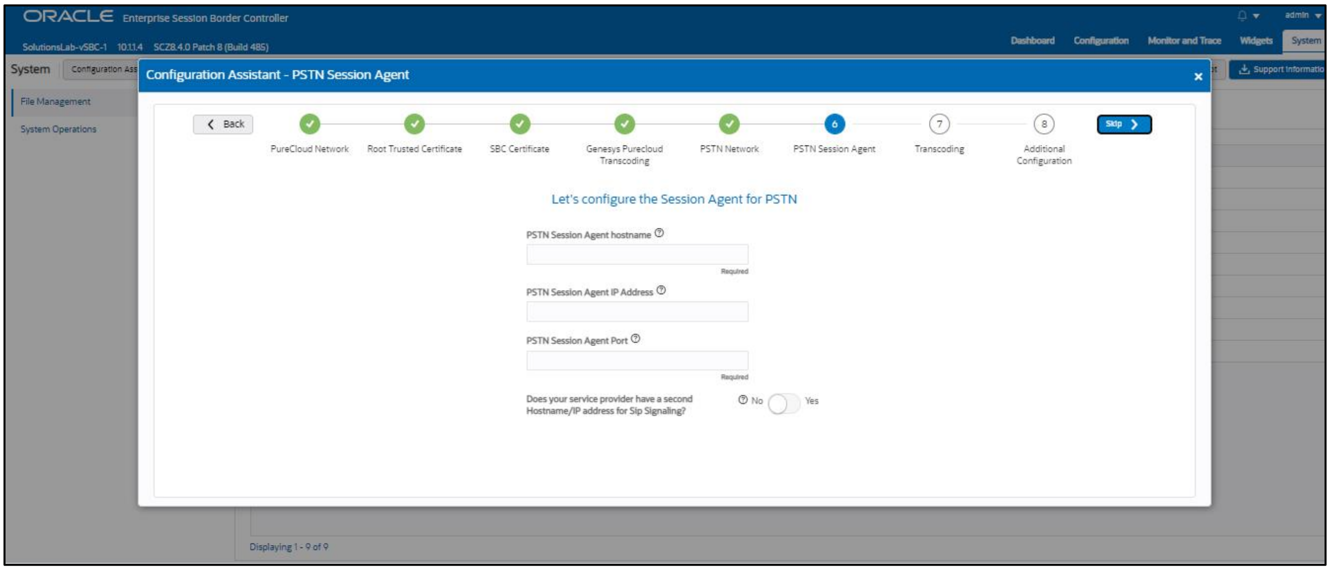
Slot Number
Slot 0
Required

Network IP address
Required

Network IP subnet mask

Page 6 – PSTN Session Agent

Page 6 of the template is where you will configure the PSTN Session Agent details where you will enter the next hop IP address and port for sip signaling to and from your PSTN SIP trunk.



Configuration Assistant - PSTN Session Agent

Let's configure the Session Agent for PSTN

PSTN Session Agent hostname
Required

PSTN Session Agent IP Address

PSTN Session Agent Port
Required

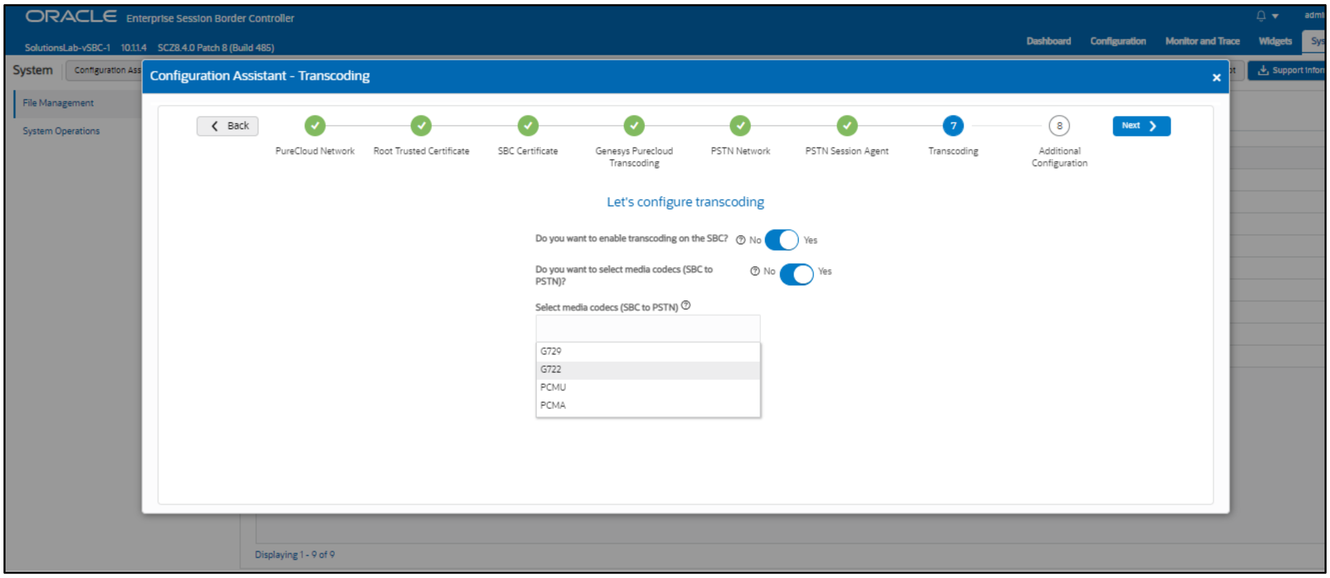
Does your service provider have a second Hostname/IP address for Sip Signaling? No Yes

Please fill the required fields and click Next.

Page 7 - PSTN side Transcoding

Page 7 is where you will be able to configure transcoding between the SBC and PSTN 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 towards PSTN trunk. If you select yes to either question regarding media codecs, you will be presented with a required drop down. You can select as many codecs from the list presented.



Configuration Assistant - Transcoding

Let's configure transcoding

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

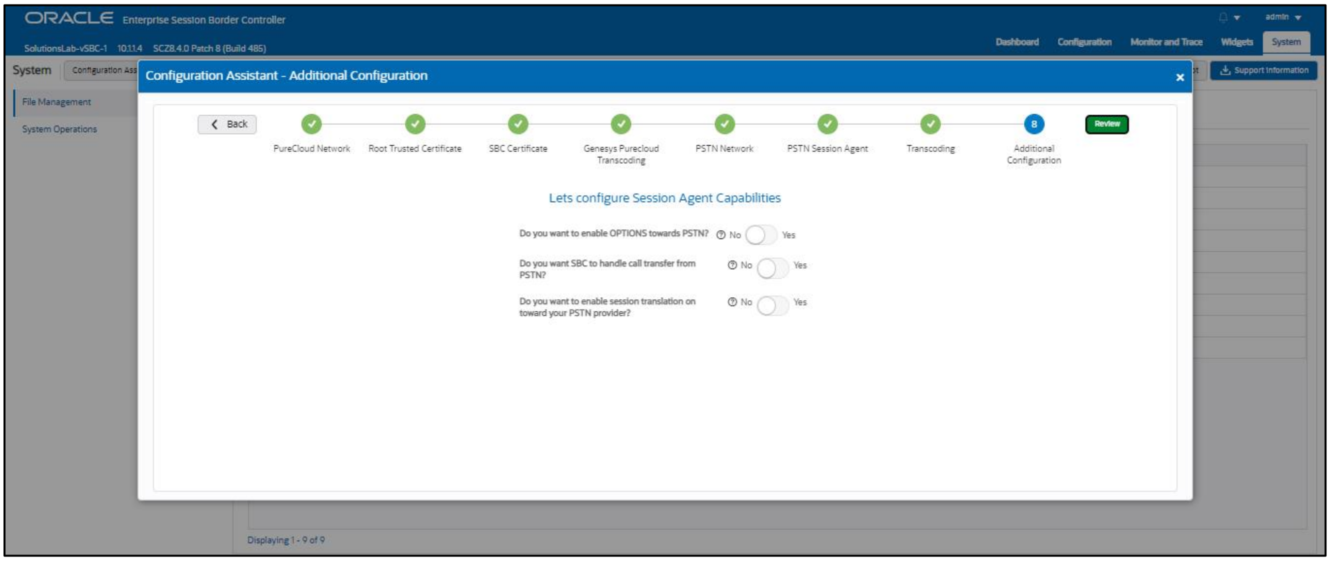
Do you want to select media codecs (SBC to PSTN)? No ● Yes

Select media codecs (SBC to PSTN)

G729
G722
PCMU
PCMA

Page 8 – Additional Configuration

Page 8 of this template is where you perform additional optional configuration. Hover over to the **?** to know more about each Option.



Configuration Assistant - Additional Configuration

Lets configure Session Agent Capabilities

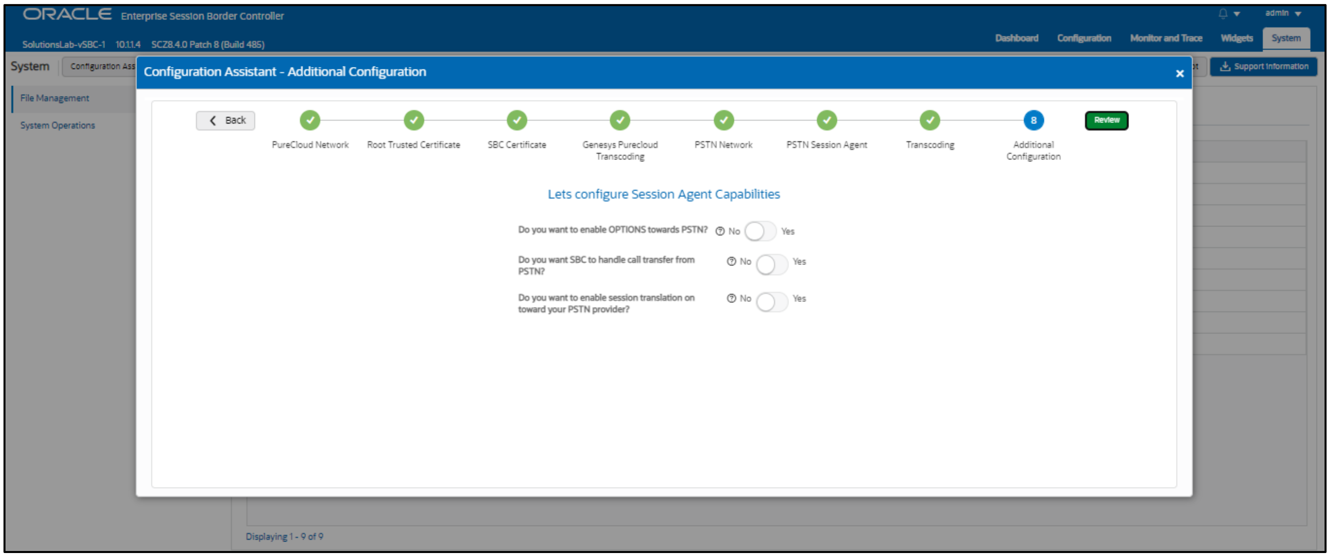
Do you want to enable OPTIONS towards PSTN? No ○ Yes

Do you want SBC to handle call transfer from PSTN? No ○ Yes

Do you want to enable session translation on toward your PSTN provider? No ○ Yes

Review

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



Configuration Assistant - Additional Configuration

Lets configure Session Agent Capabilities

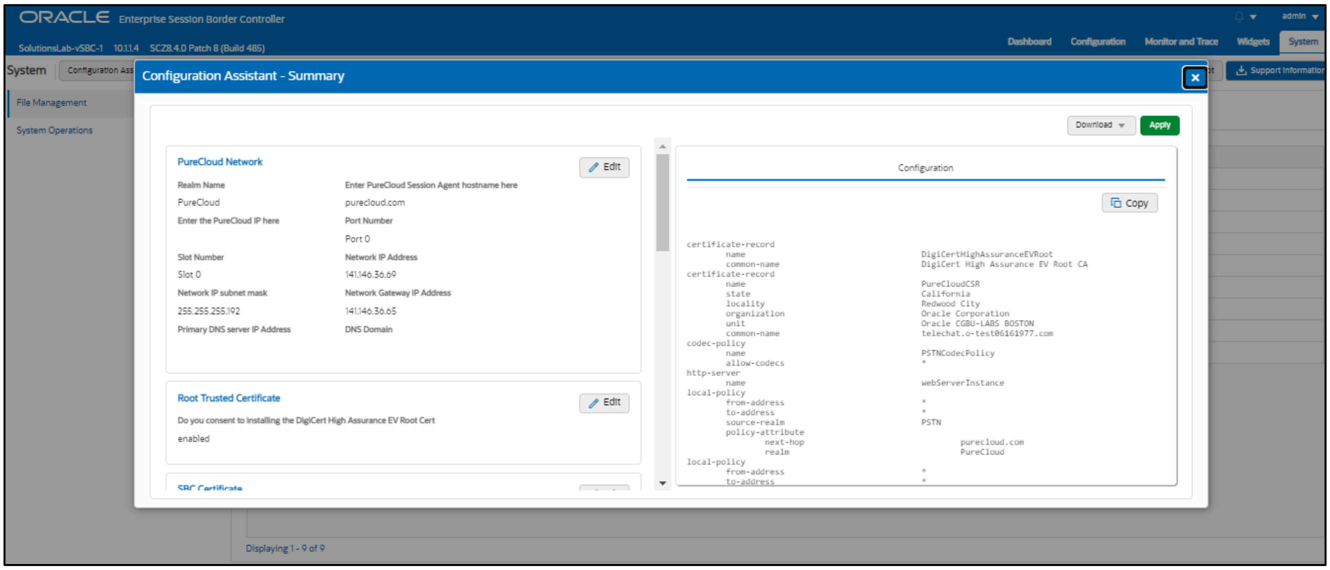
Do you want to enable OPTIONS towards PSTN? No ○ Yes

Do you want SBC to handle call transfer from PSTN? No ○ Yes

Do you want to enable session translation on toward your PSTN provider? No ○ Yes

The screen looks like below after clicking the Review Tab. The left side of the review page contains all of the entries added on each page and allows for editing each page individually if necessary.

The right side displays the entire configuration created and when applicable, will also have a CSR tab that contains a certificate that can be signed by a CA authority.



Configuration Assistant - Summary

PureCloud Network

Realm Name	Enter PureCloud Session Agent hostname here
PureCloud	purecloud.com
Enter the PureCloud IP here	Port Number
	Port 0
Slot Number	Network IP Address
Slot 0	141.146.36.69
Network IP subnet mask	Network Gateway IP Address
255.255.255.192	141.146.36.65
Primary DNS server IP Address	DNS Domain

Root Trusted Certificate

Do you consent to installing the DigiCert High Assurance EV Root Cert

enabled

SBC Certificate

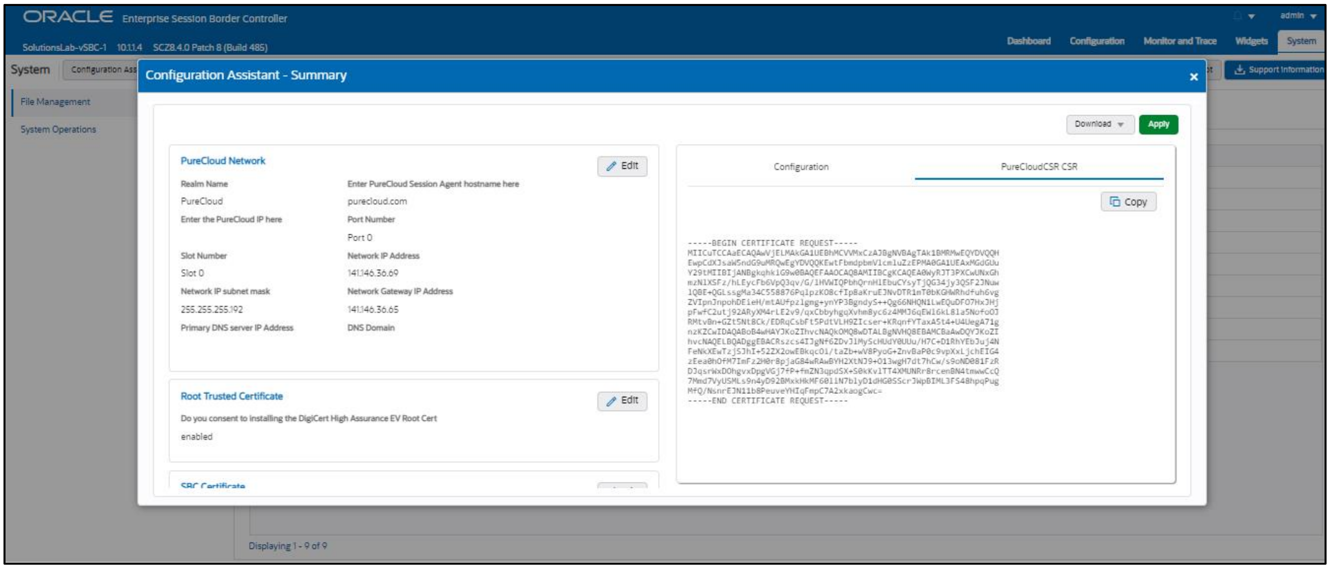
Configuration

```
certificate-record
        name                                    DigiCertHighAssuranceEVRoot
        common-name                             DigiCert High Assurance EV Root CA
certificate-record
        name                                    PureCloudCSR
        state                                   California
        locality                                Redwood City
        organization                            Oracle Corporation
        unit                                    Oracle CGBU-LABS BOSTON
        common-name                             telechat.o-test06161977.com
codec-policy
        name                                    PSTNCodecPolicy
        allow-codecs                            *
http-server
        name                                    webServerInstance
local-policy
        from-address                            *
        to-address                              *
        source-realm                            PSTN
        policy-attribute
                next-hop                                purecloud.com
                realm                                   PureCloud
local-policy
        from-address                            *
        to-address                              *
```

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, “*CSR*”.

On Page 3 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.



Configuration Assistant - Summary

PureCloud Network

Realm Name: PureCloud
Enter PureCloud Session Agent hostname here: purecloud.com
Enter the PureCloud IP here
Port Number: Port 0
Slot Number: Slot 0
Network IP Address: 141.146.36.69
Network IP subnet mask: 255.255.255.192
Network Gateway IP Address: 141.146.36.65
Primary DNS server IP Address
DNS Domain

Root Trusted Certificate

Do you consent to installing the DigiCert High Assurance EV Root Cert: enabled

SBC Certificate

```
-----BEGIN CERTIFICATE REQUEST-----
MIICuTCCAaECAQAwVjELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEPMA0GA1UEAxMGdGUu
Y29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0WyRJT3PXCwUNxGh
mzN1XSFz/hLEycFb6VpQ3qv/G/1HVWIQPbhQrnH1EbuCYsyTjQG34jy3QSF2JNuw
1QBE+QGLssgMa34C558876Pq1pzKO8cfIp8aKruEJNvDTR1mT0bKGHWRhdfuh6vg
ZVIpnJnpohDEieH/mtAUfpz1gmg+ynYP3BgndyS++Qg66NHQN1LwEQuDFO7HxJHj
pFwfC2utj92ARyXM4rLE2v9/qxCbbyhgqXvhm8yc6z4MMJ6qEWl6kL81a5NofoOJ
RMtvBn+GZtSNt8Ck/EDRqCsbFt5PdtVLH9ZIcser+KRqnfYTaxA5t4+U4UegA71g
nzKZCwIDAQABoB4wHAYJKoZIhvcNAQkOMQ8wDTALBgNVHQ8EBAMCBaAwDQYJKoZI
hvcNAQELBQADggEBACRszcs4IJgNf6ZDvJ1MySCHUdY0UUu/H7C+D1RhYEbJuj4N
FeNkXEwTzjSJhI+52ZX2owE8kqcO1/taZb+wV8PyoG+ZnvBaP0c9vpXxLjchEIG4
zEea0hOfM7ImFz2H0r8pjaG84wRAwBYH2XtNJ9+O13wgH7dt7hCw/s9oND081FzR
DJqsrWxDOhgvxDpgVGj7fP+fmZN3qpdSX+S0kKv1TT4XMUNRr8rcen8N4tmwwCcQ
7Mmd7VyUSMLs9n4yD92BMxkHkMF601lN7blyD1dHG0SScrJWpBIML3FS48hpqPug
MfQ/NsnrEJN11b8PeuveYHIqFmpC7A2xkaogCwc=
-----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 the 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 3, the CSR tab will not be present under review.

Download and/or Apply

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.

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 PureCloudPhone with Generic PSTN Sip Trunk.

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.

8. Test Plan Executed

We have executed the following test plan to validate the interworking between Genesys PureCloud and Twilio SIP Trunk via Oracle SBC.

Test	Description	Pass	Fail
Outbound Local	Place an outbound call to a local number	YES	
Outbound Long-Distance	Place an outbound call to a long-distance number	YES	
Outbound International	Place an outbound call to an international number (if applicable)	YES	
Outbound Toll-Free	Place an outbound call to a toll-free number	YES	
Inbound	Place an inbound call to the range of numbers pointed to your system	YES	
Hold	Place an outbound call to any number, place call on hold for 1 minute, take call off hold	YES	
Transfer Call	Place a call, transfer the call, ensure both parties connect successfully	YES	
Call Forward	Enable call forward on phone, place call to phone, confirm call forwards successfully	YES	
Conference	Create a conference call with 3 or more people on the same call	YES	
DTMF	Call 1-800-COMCAST, confirm DTMF is received	YES	
Outbound Duration	Place outbound call, keep it connected for 10+ minutes	YES	
Inbound Duration	Place inbound call, keep it connected for 10+ minutes	YES	

ORACLE

CONNECT WITH US

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

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services