Oracle SBC integration with Genesys BYOC Cloud and Zoom Phone

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 BYOC Cloud and Zoom Phone BYOC	20 Aug 2021
1.1	Oracle Public IP Address masked	18 Nov 2021
1.2	Added Section Genesys BYOC Cloud Configuration Assistant	03 Feb 2022
1.3	Removed MAuth TLS and updated Cipher List Rebranded Genesys PureCloud to Genesys BYOC Cloud	19 Feb 2026

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 BYOC Cloud and Zoom Phone.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Genesys BYOC Cloud and Zoom Phone BYOC. The Application note focuses on the steps required to create a SIP connection between Genesys Cloud BYOC, Oracle SBC and Zoom Phone through which voice communication is possible between Genesys Cloud and Zoom Phone Users.

It should be noted that the SBC configuration provided in this guide focuses strictly on the Genesys BYOC Cloud and Zoom Phone related parameters. Calls between Zoom Phone and Genesys Cloud 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-cloud-cx-and-twillio-sip-trunkv0.3.pdf

as a reference to configure the Twilio SIP Trunk with Oracle SBC.

Related documentation can be found below –

2.1 Zoom Phone

- https://zoom.us/docs/doc/Zoom-Bring%20Your%20Own%20Carrier.pdf
- https://zoom.us/phonesystem
- https://zoom.us/zoom-phone-features

2.2 Genesys BYOC Cloud

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

https://help.myBYOC Cloud.com/articles/about-byoc-cloud/

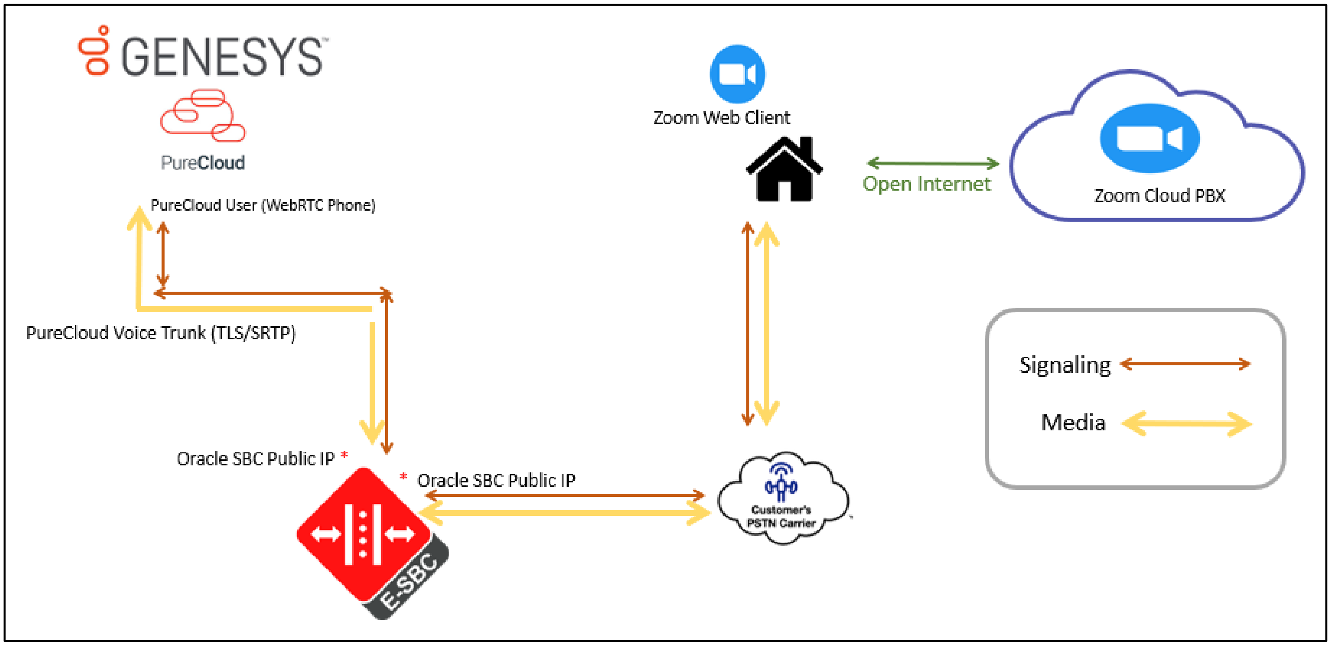
3. Validated Oracle Versions

We have successfully conducted testing with the Oracle Communications SBC versions:
SCZ840p5a

These software releases with the configuration listed below can run on any of the following products:

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

4. Architecture.



Above figure illustrates the connection between Genesys BYOC Cloud, Oracle SBC and Zoom Phone. Both Genesys Cloud and Zoom Phone are connected to the Oracle SBC Public FQDN /IP

Oracle SBC which is certified with Zoom Phone is used to steer the signaling, media to, and From the Genesys Cloud to Zoom Phone 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 BYOC Cloud

Phase 2 – Configuring Zoom Phone

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.

5. Configure Genesys BYOC Cloud

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

Note: The document only includes the steps required on Genesys BYOC Cloud 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 Genesys BYOC Cloudconfiguration as per your requirement.

To implement Genesys Cloud BYOC with Oracle SBC, you use the Telephony Admin UI to create SIP trunks between the Genesys Cloud Media Tier resources in AWS and the Oracle SBC. Oracle SBC connects to the Genesys Cloud to Zoom Phone over the based infrastructure.

The Oracle Enterprise SBC will act as an intermediary between Zoom Phone and Genesys BYOC Cloud. 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 Genesys Cloud System and Zoom Phone 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 BYOC Cloud is set over a Secure TLS 1.2 and SRTP based connection.

5.1 External Trunk Configuration

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

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

To configure the external Trunk, Navigate to

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

5.1.1 Create a new External Trunk

Type: BYOC Carrier Trunk

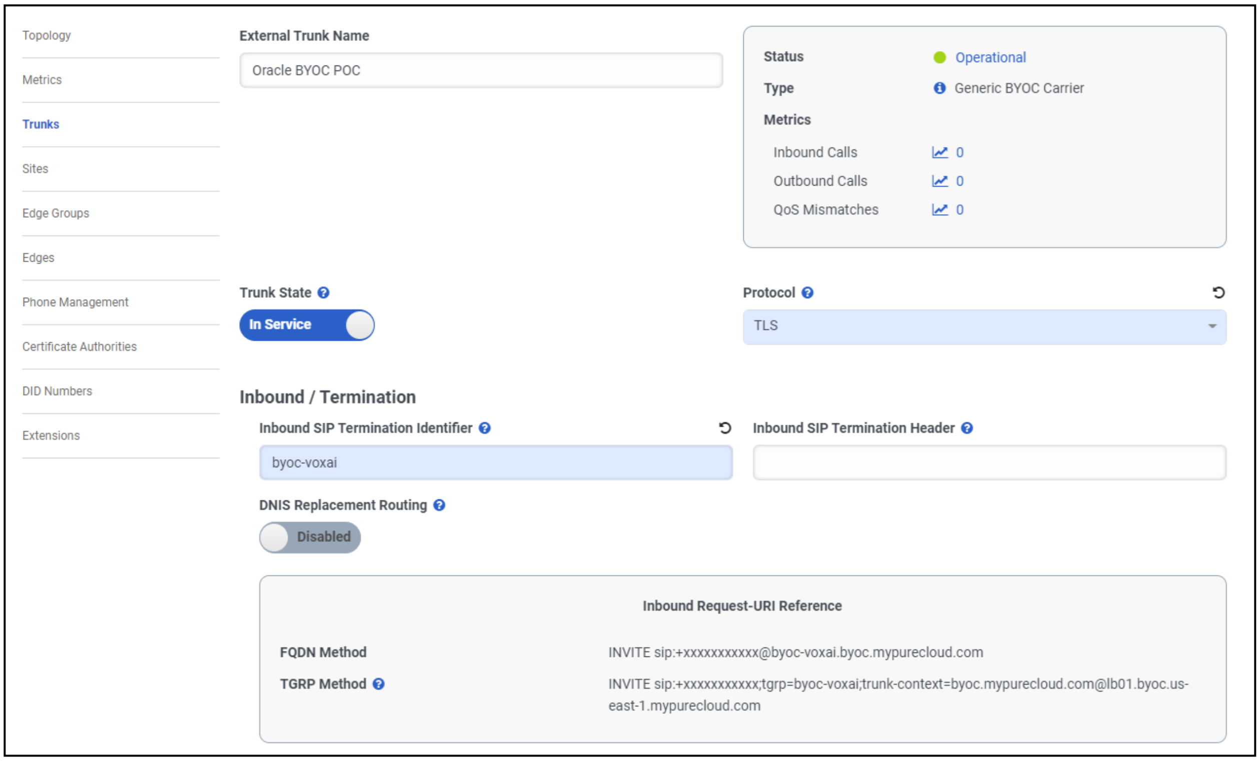
Protocol: TLS (TCP and UDP are also available)

5.1.2 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 BYOC Cloud. 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 Genesys Cloud 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.genesys.cloud/articles/byoc-cloud-public-sip-ip-addresses/

IP Addresses	Load Balancer DNS Names
52.203.12.137	lb01.voice.use1.pure.cloud
54.82.241.192	lb02.voice.use1.pure.cloud
54.82.241.68	lb03.voice.use1.pure.cloud
54.82.188.43	lb04.voice.use1.pure.cloud



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:

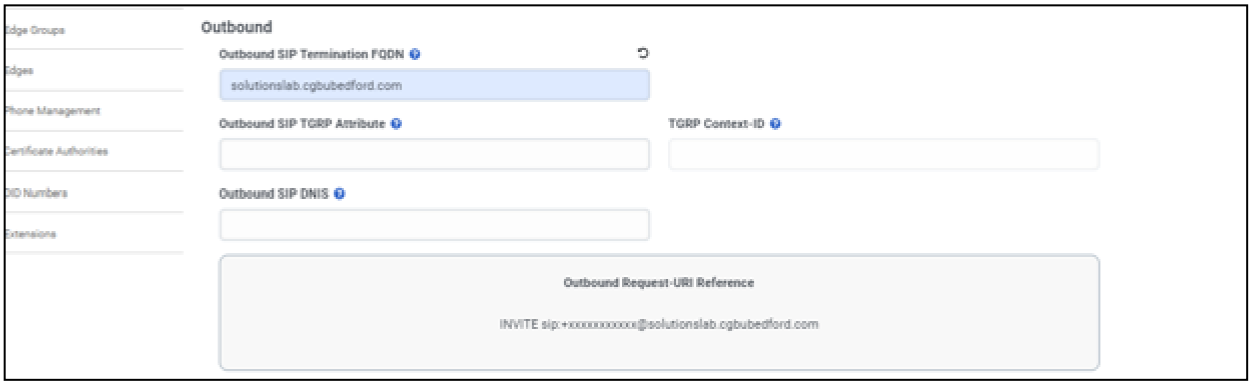
DNIS Replacement Routing: Disabled

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

5.1.3 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:

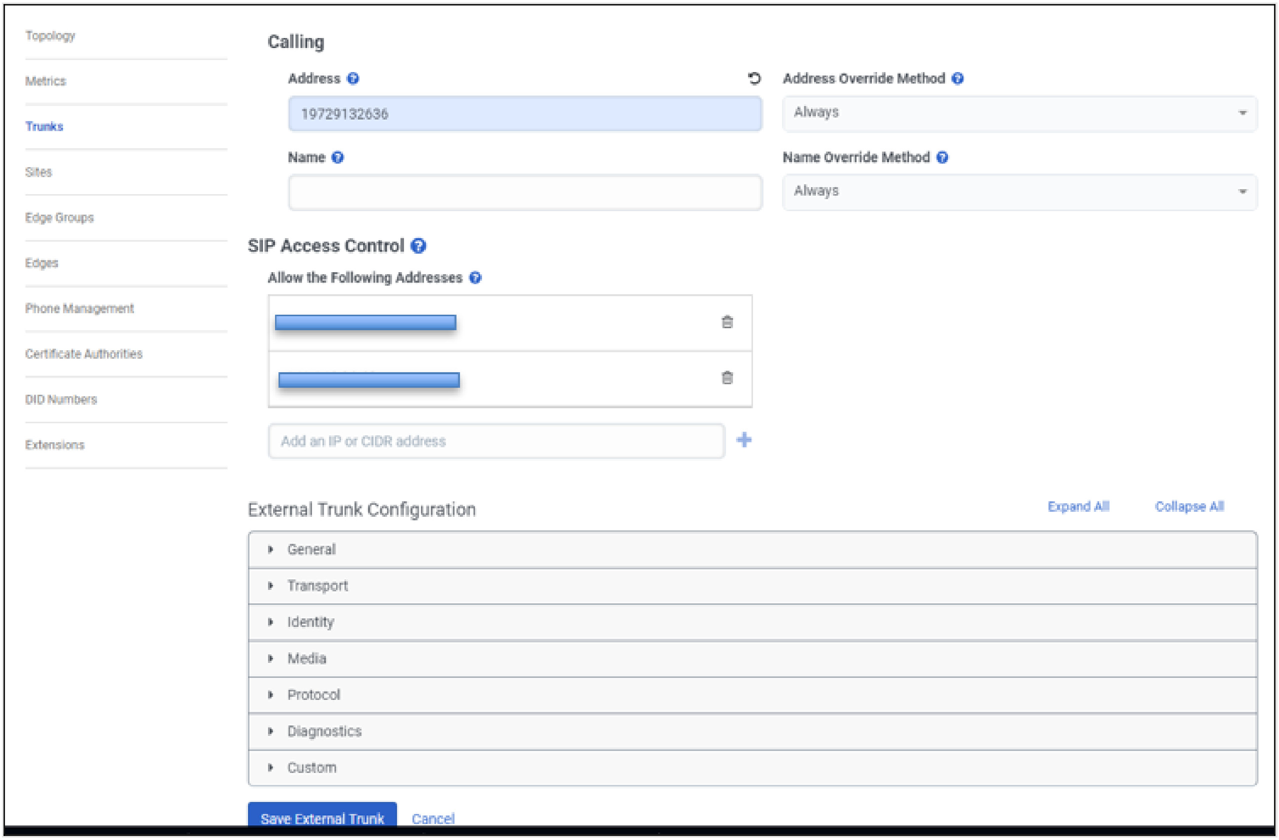
TGRP Context-ID:

Outbound SIP DNIS:

Outbound Request-URI Reference

INVITE sip:+xxxxxxxxxxx@solutionslab.cgbubedford.com

5.1.4 Set Calling Address



Calling

Address: 19729132636

Address Override Method: Always

Name:

Name Override Method: Always

SIP Access Control

Allow the Following Addresses

[redacted]

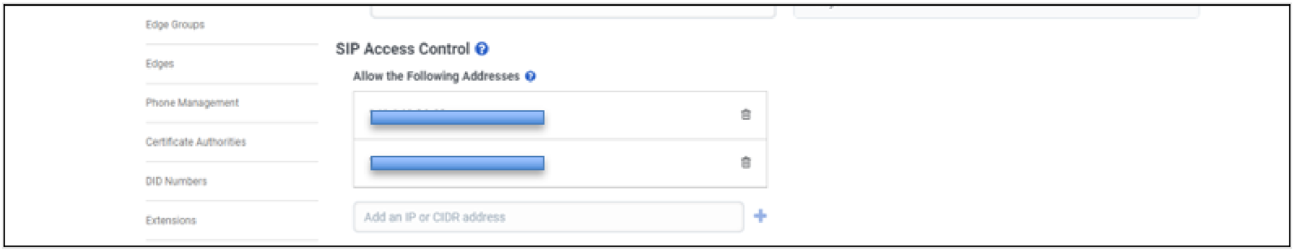
[redacted]

Add an IP or CIDR address

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.

5.1.5 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

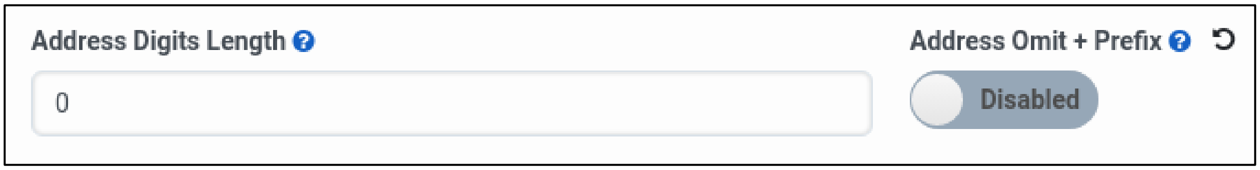
[redacted]

[redacted]

Add an IP or CIDR address

5.1.6 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

5.2 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 Genesys BYOC CloudEdge(s).

Detailed steps to configure the Site can be found here-

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

5.2.1 Create a New Site

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

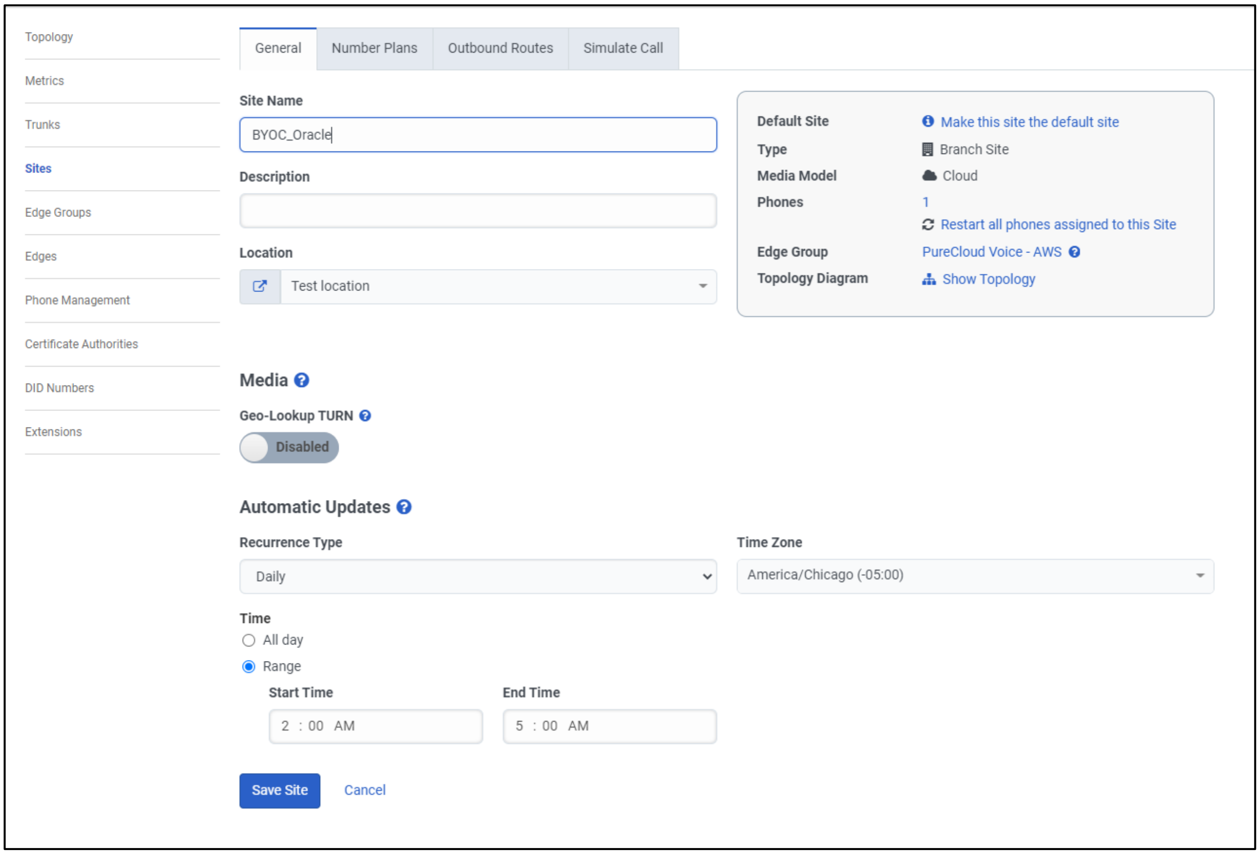
Type a name into the **Site Name** box.

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

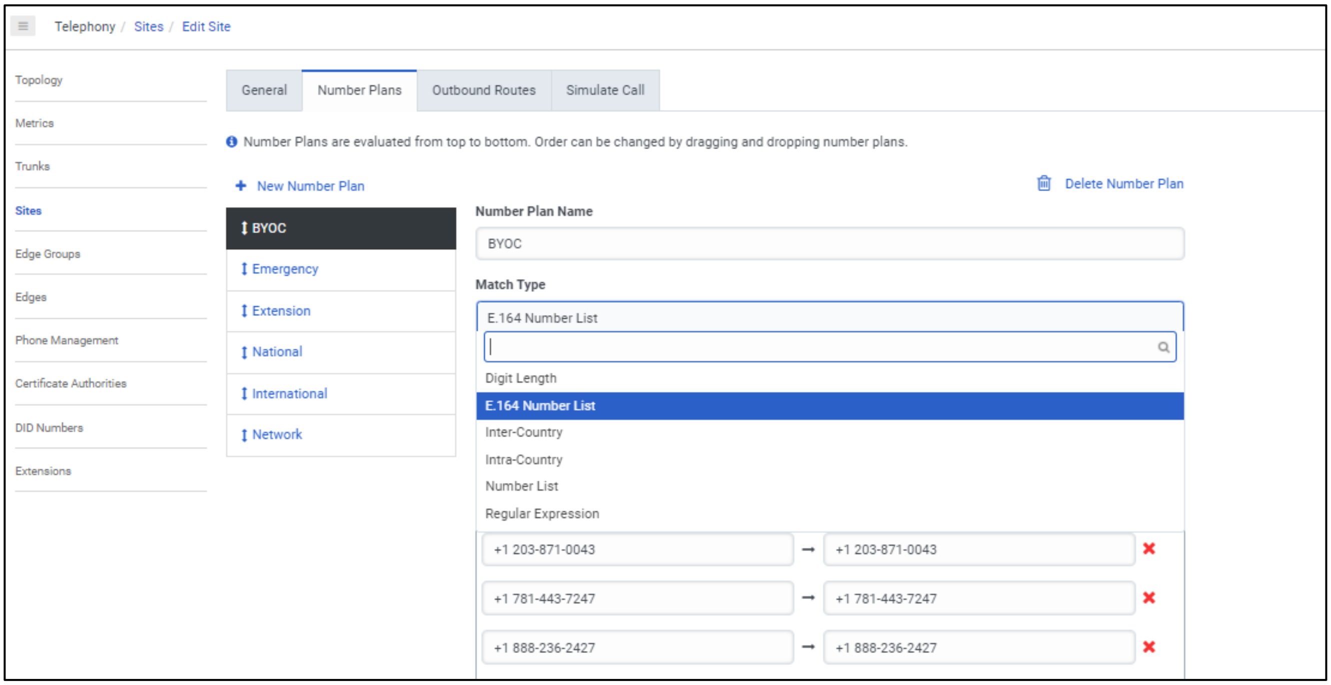
● Range

Start Time: 2 : 00 AM

End Time: 5 : 00 AM

5.2.2 Number Plans & Classifications

Genesys Cloud 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.

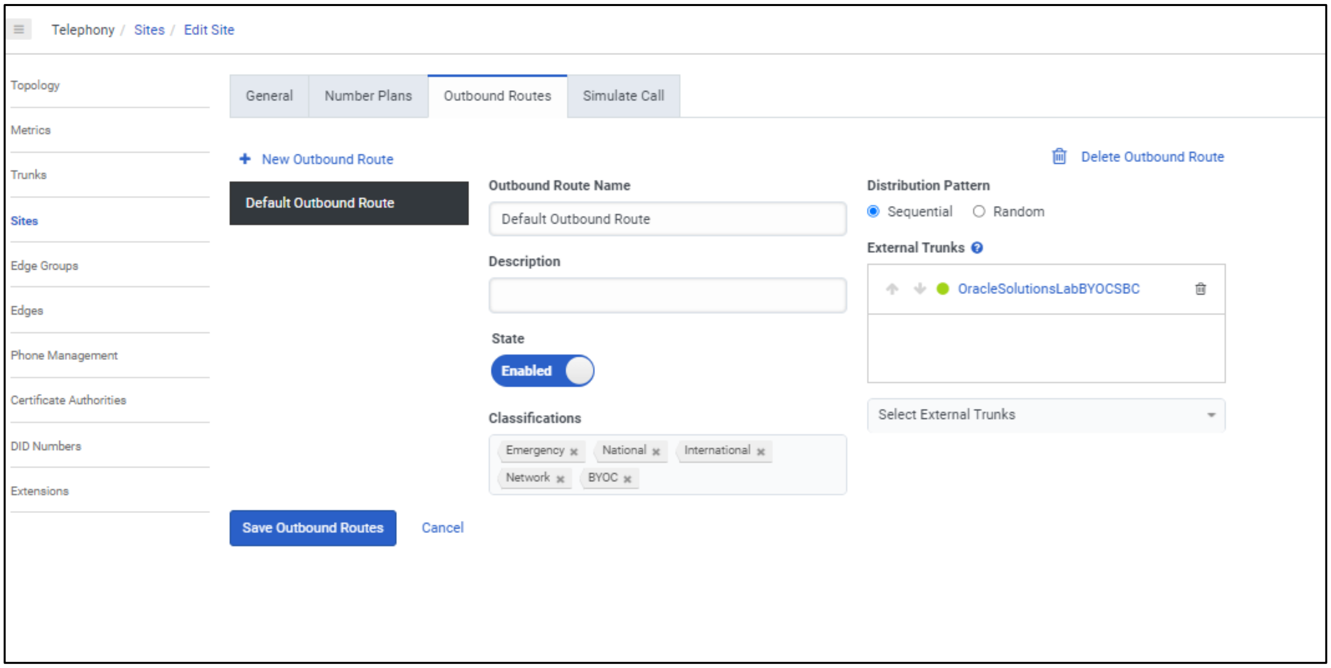
Number Plan Name: BYOC

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

5.2.3 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

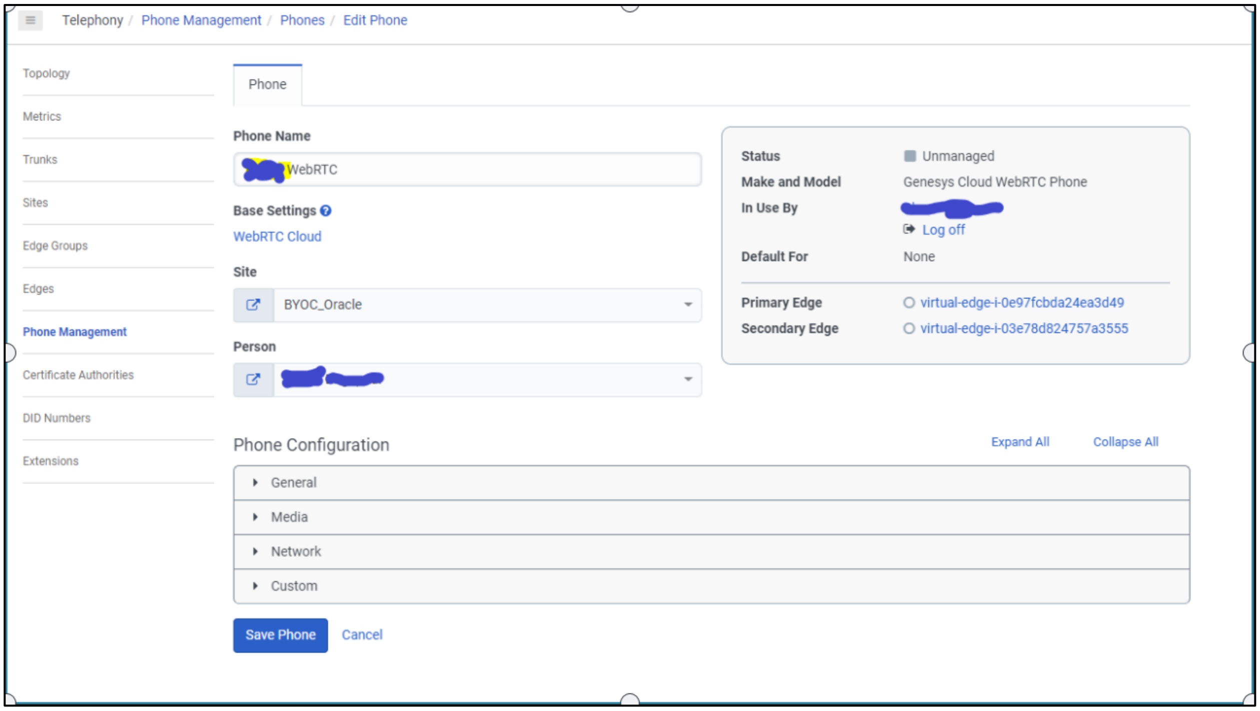
Classifications: Emergency, National, International, Network, BYOC

Distribution Pattern: ● Sequential ○ Random

External Trunks: OracleSolutionsLabBYOCSBC

5.2.4 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.



Phone Name: [redacted] WebRTC

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

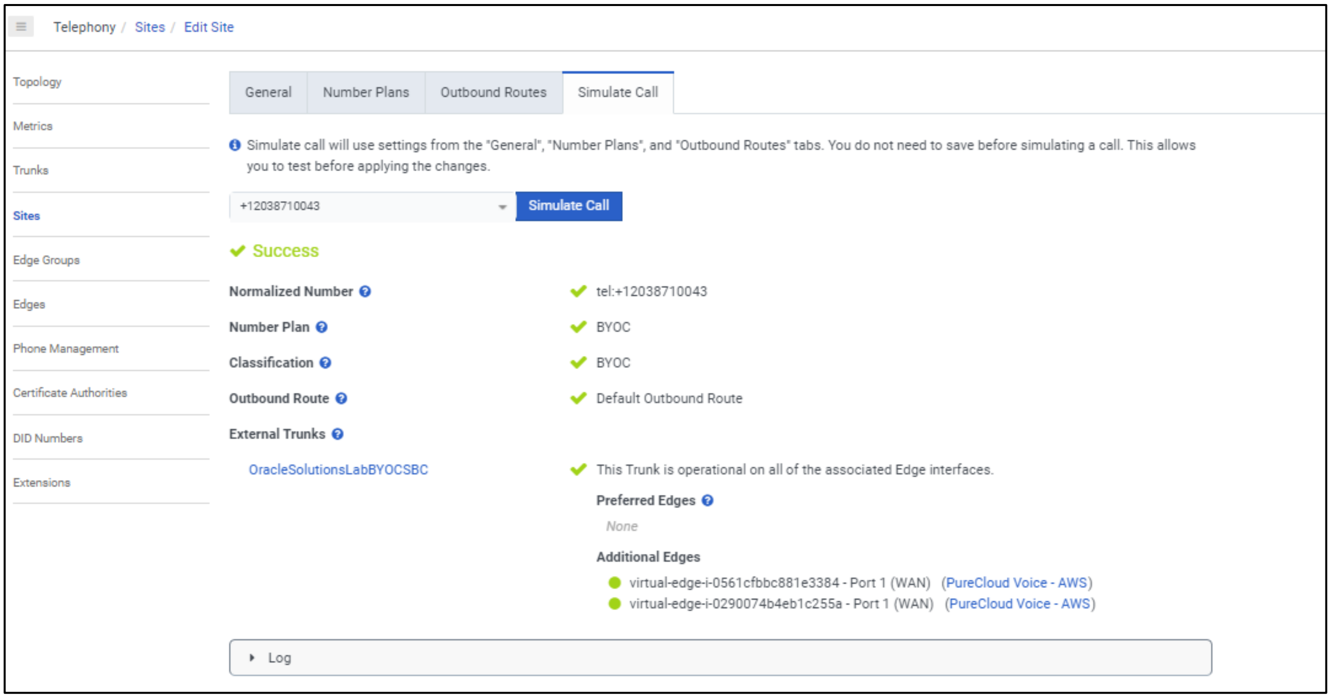
Secondary Edge: ○ virtual-edge-i-03e78d824757a3555

Phone Configuration

- General
- Media
- Network
- Custom

5.2.5 Simulate call

Genesys BYOC Cloud 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.



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

✓ 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

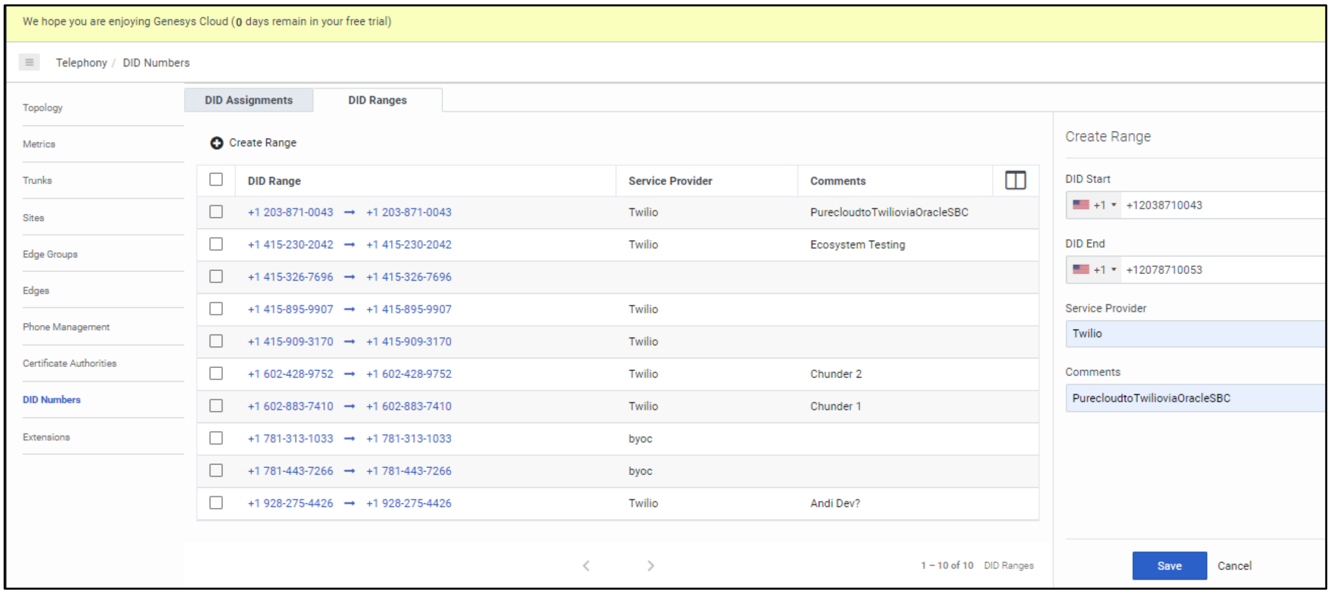
Additional Edges

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

5.3 DID Assignment

5.3.1 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

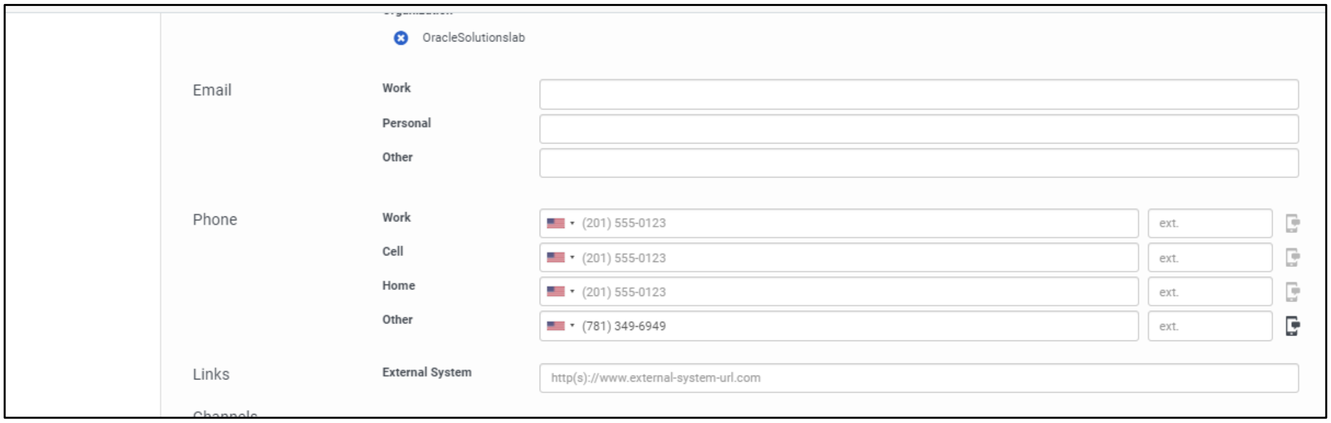
DID End: +1 +12078710053

Service Provider: Twilio

Comments: PurecloudtoTwilioviaOracleSBC

5.3.2 Assign DID to User.

On users' profile field, one of the DID can be assigned to Genesys Cloud 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 BYOC Cloud.

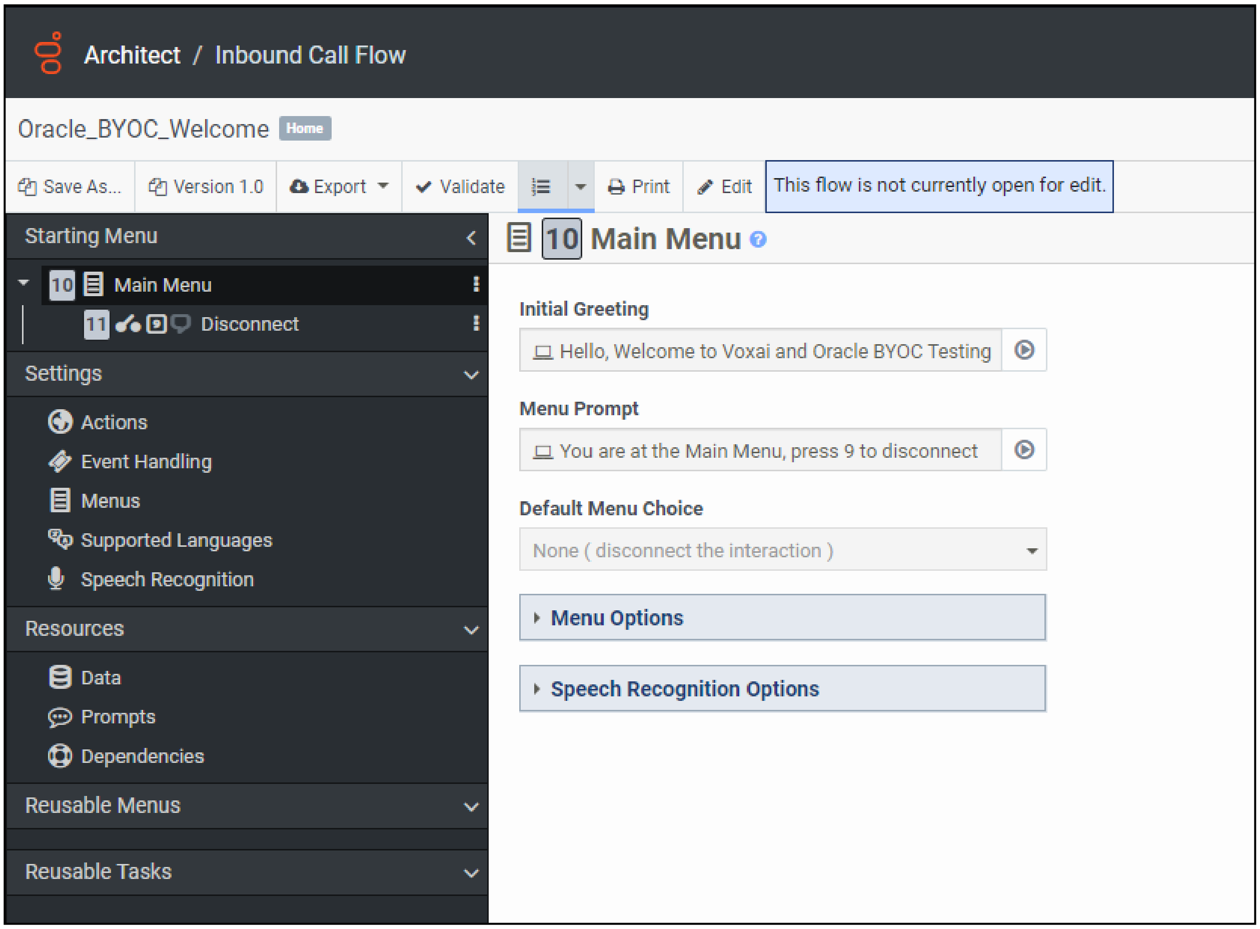


OracleSolutionslab

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	

5.4. 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 Zoom Phone to Genesys BYOC Cloud via Oracle SBC.



This flow is not currently open for edit.

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

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

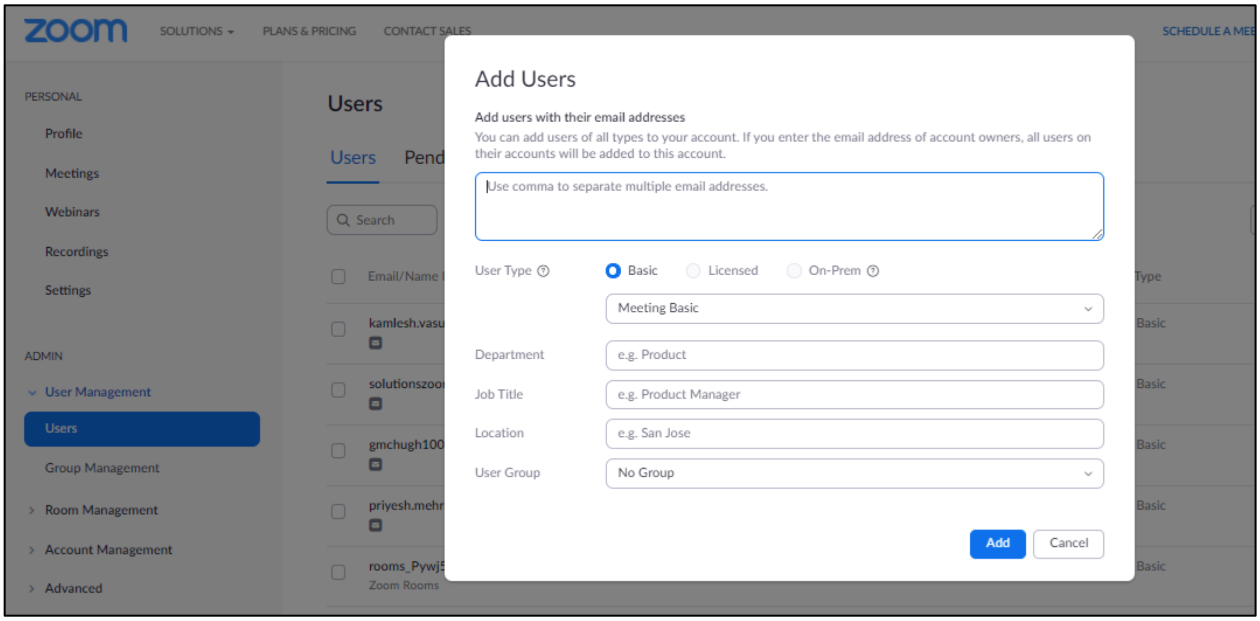
Default Menu Choice: None (disconnect the interaction)

6. Configure Zoom Phone

This Section describes the steps to configure BYOC Phone Numbers on the Zoom Admin Portal and assign the BYOC Number to a User. For detailed assistance with setting up and configuring your Zoom Phone System, please reach out to Zoom Sales: https://zoom.us/contactsales

6.1 Create a Zoom User

Navigate to **Admin>User Management > Users**.
Click Add to create new Zoom users. Provide the necessary details about the New User and Click on Add to Add the User.



Add Users

Add users with their email addresses

You can add users of all types to your account. If you enter the email address of account owners, all users on their accounts will be added to this account.

Use comma to separate multiple email addresses.

User Type: ● Basic ○ Licensed ○ On-Prem

Meeting Basic

Department: e.g. Product

Job Title: e.g. Product Manager

Location: e.g. San Jose

User Group: No Group

Once the New User is added it will start reflecting in **Admin >Users** Section on the Web portal.

6.2 Add BYOC Number

Navigate to **Phone Systems Management > Phone Numbers > BYOC**

Select **Add** to add external phone numbers provided by your carrier into the Zoom portal.

Site - Choose the relevant Site on which the Number needs to be added. For Example, Main Site.

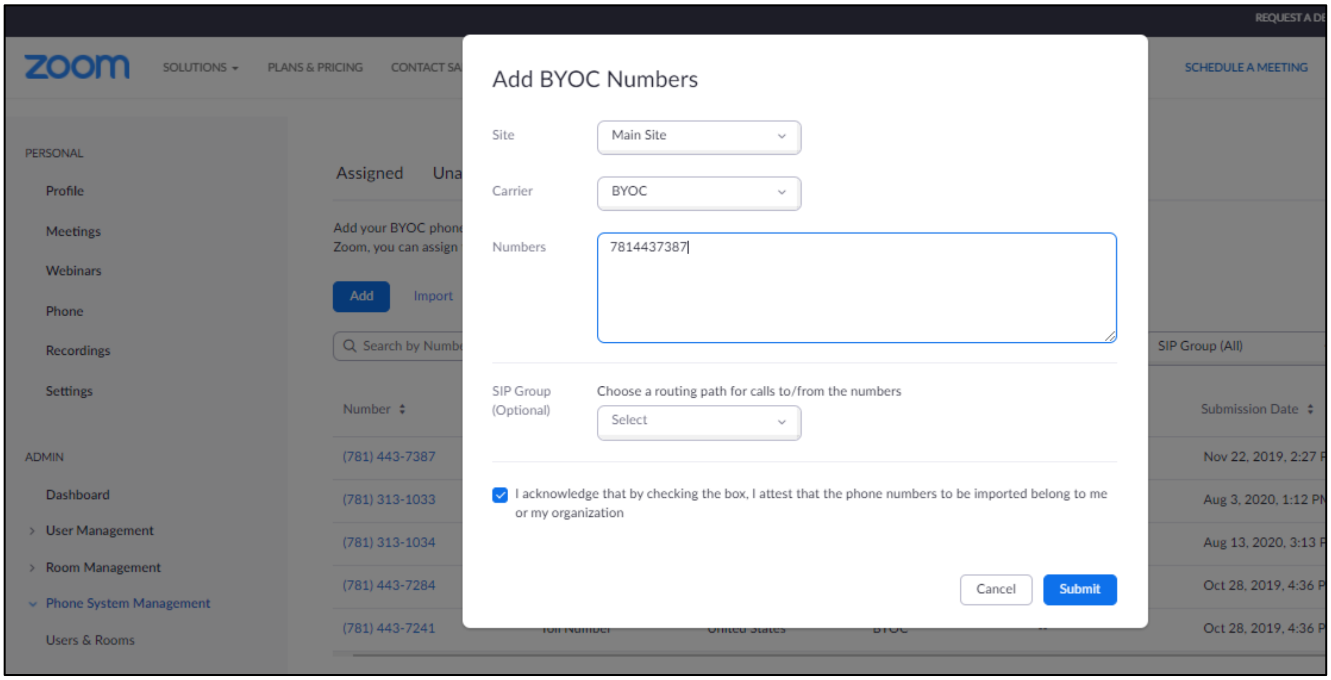
Carrier –Choose BYOC

Numbers- Put the BYOC DID Number provided by your Carrier.

SIP Group – Optional Parameter (Can be Left Blank)

Acknowledge that the Phone Number belongs to your organization.

Click **Submit**.



Number	Submission Date
(781) 443-7387	Nov 22, 2019, 2:27
(781) 313-1033	Aug 3, 2020, 1:12 PI
(781) 313-1034	Aug 13, 2020, 3:13
(781) 443-7284	Oct 28, 2019, 4:36
(781) 443-7241	Oct 28, 2019, 4:36

Add BYOC Numbers

Site: Main Site

Carrier: BYOC

Numbers: 7814437387

SIP Group (Optional): Choose a routing path for calls to/from the numbers — Select

☑ I acknowledge that by checking the box, I attest that the phone numbers to be imported belong to me or my organization

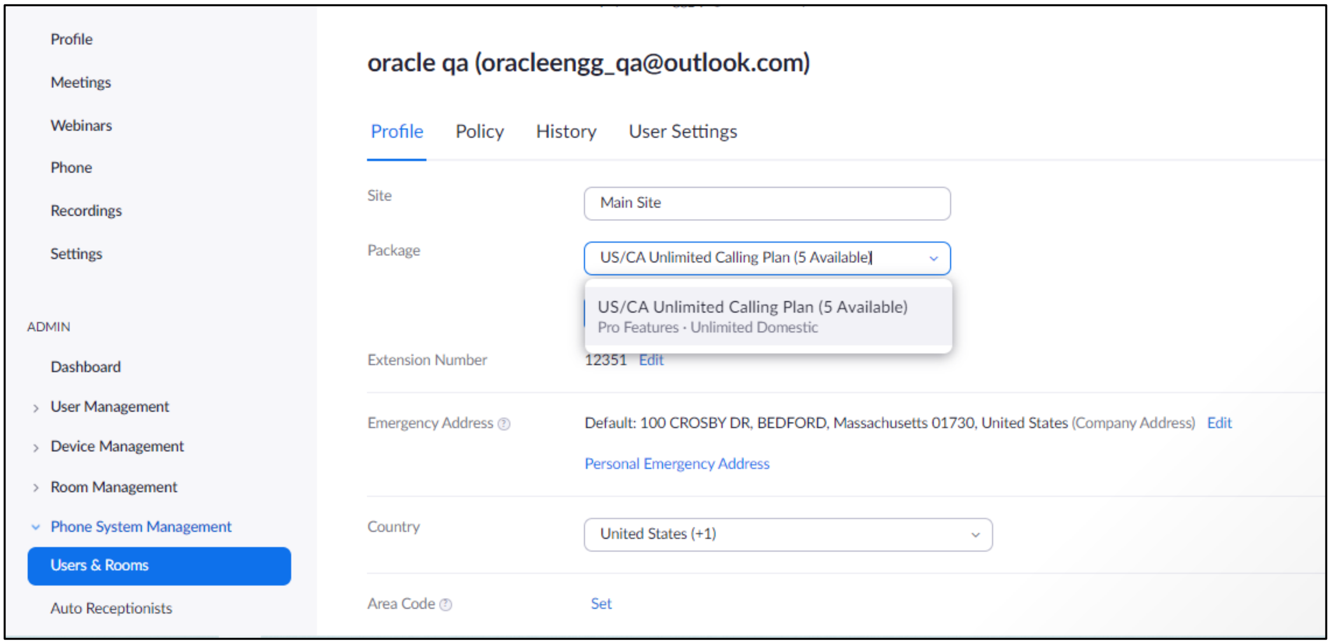
6.3 Assign a Calling Package to User

You may require adding a Calling package to the user before a Calling Number can be assigned to a User.

To assign a calling package

Navigate to **Users and Rooms > Package**

Choose the appropriate package and assign the package to the Respective User.



oracle qa (oracleengg_qa@outlook.com)

Site: Main Site

Package: US/CA Unlimited Calling Plan (5 Available)

US/CA Unlimited Calling Plan (5 Available)
Pro Features · Unlimited Domestic

Extension Number: 12351 Edit

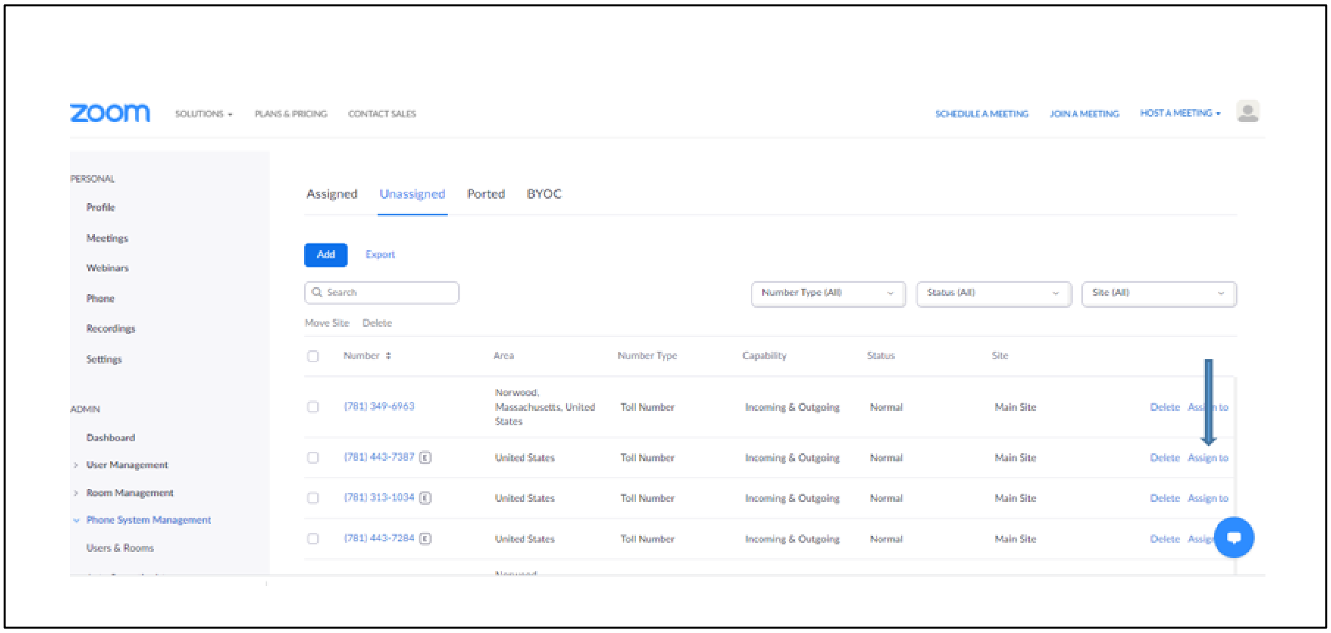
Emergency Address: Default: 100 CROSBY DR, BEDFORD, Massachusetts 01730, United States (Company Address) Edit
Personal Emergency Address

Country: United States (+1)

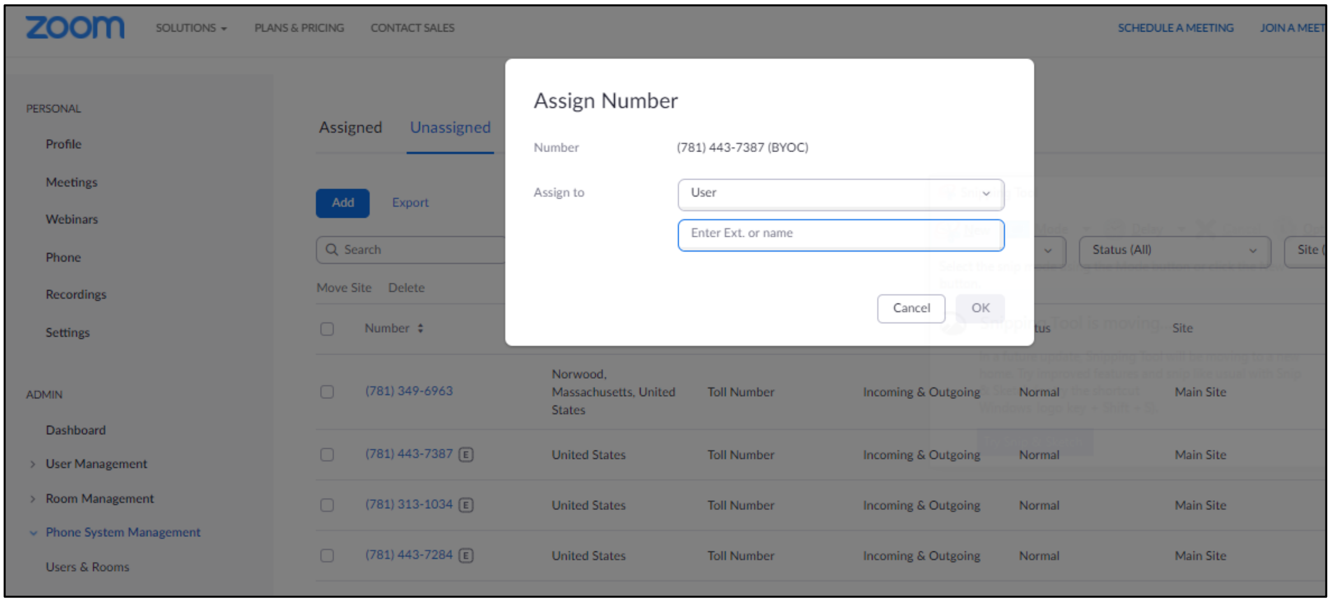
Area Code: Set

6.4 Assign the BYOC Number to a User

The BYOC Number will now be visible in the Unassigned Tab on the portal. Click on Assign to Tab to assign the Number to a User.



Number	Area	Number Type	Capability	Status	Site	
(781) 349-6963	Norwood, Massachusetts, United States	Toll Number	Incoming & Outgoing	Normal	Main Site	Delete Assign to
(781) 443-7387 E	United States	Toll Number	Incoming & Outgoing	Normal	Main Site	Delete Assign to
(781) 313-1034 E	United States	Toll Number	Incoming & Outgoing	Normal	Main Site	Delete Assign to
(781) 443-7284 E	United States	Toll Number	Incoming & Outgoing	Normal	Main Site	Delete Assign



Assign Number

Number (781) 443-7387 (BYOC)

Assign to User

Enter Ext. or name

Number	Area	Number Type	Capability	Status	Site
(781) 349-6963	Norwood, Massachusetts, United States	Toll Number	Incoming & Outgoing	Normal	Main Site
(781) 443-7387 E	United States	Toll Number	Incoming & Outgoing	Normal	Main Site
(781) 313-1034 E	United States	Toll Number	Incoming & Outgoing	Normal	Main Site
(781) 443-7284 E	United States	Toll Number	Incoming & Outgoing	Normal	Main Site

7. Configuring the SBC

This chapter provides systematic guidance on how to configure Oracle SBC for Genesys BYOC Cloud and Zoom Phone.

7.1 New SBC configuration

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

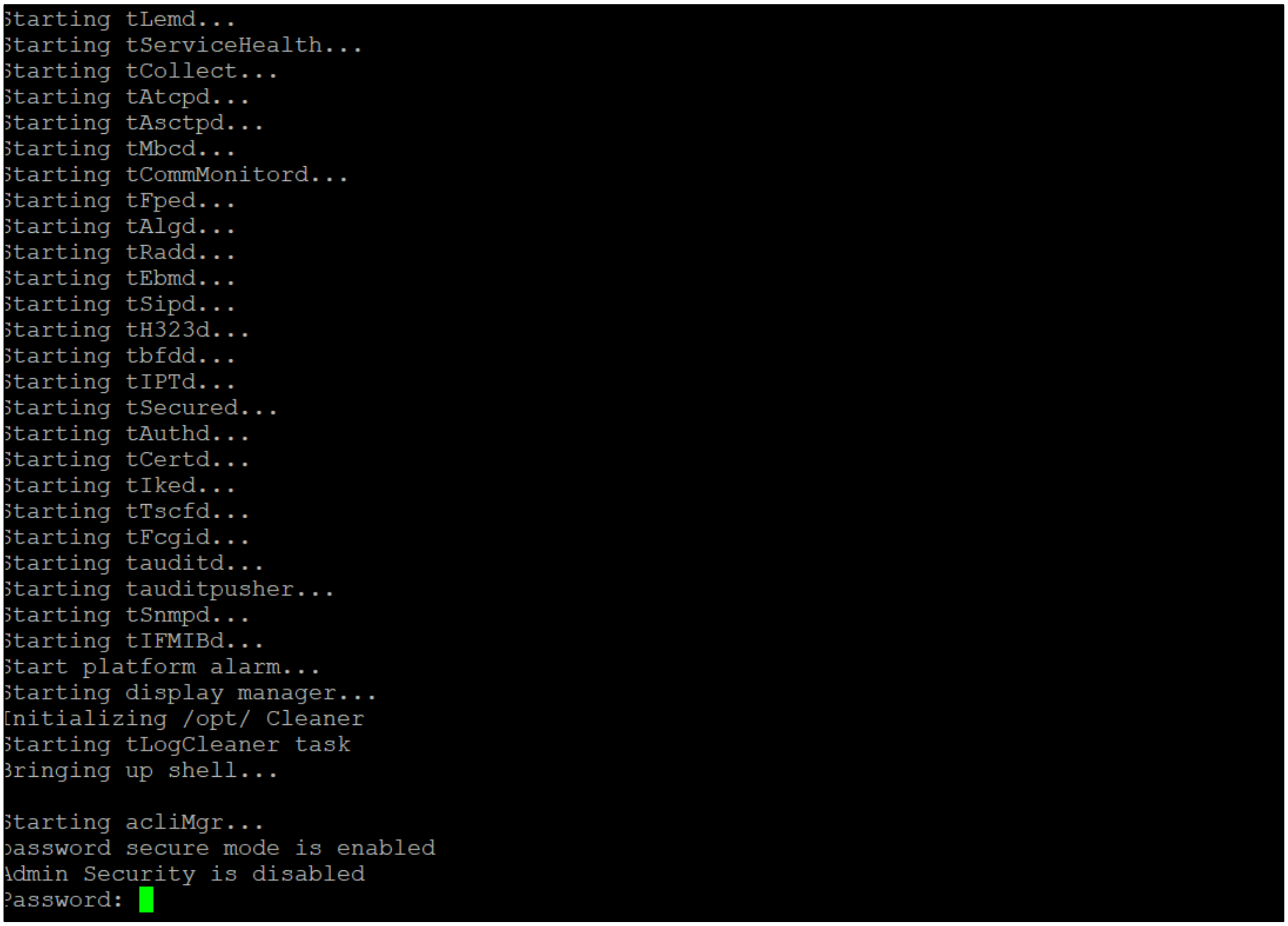
7.1.1 Establishing a serial connection to the SBC

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

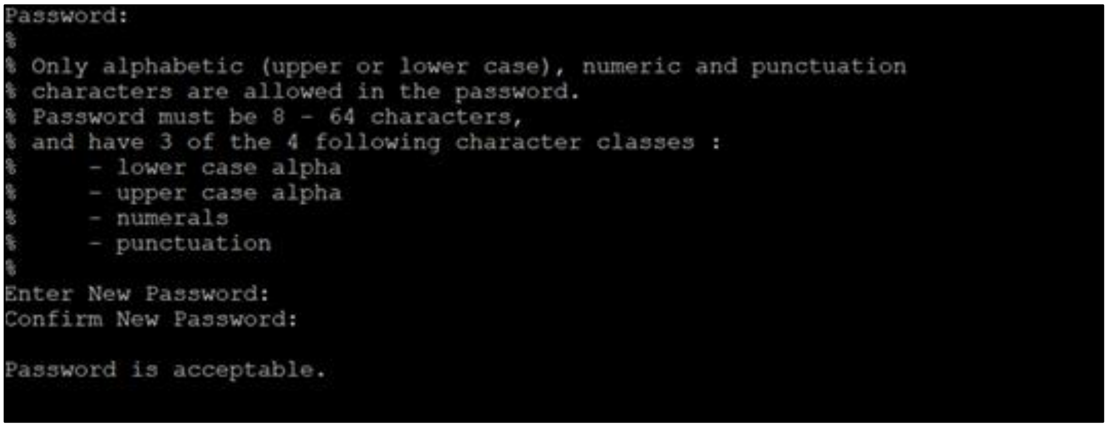
Power on the SBC and confirm that you see the following output from the boot-up sequence



```
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”.

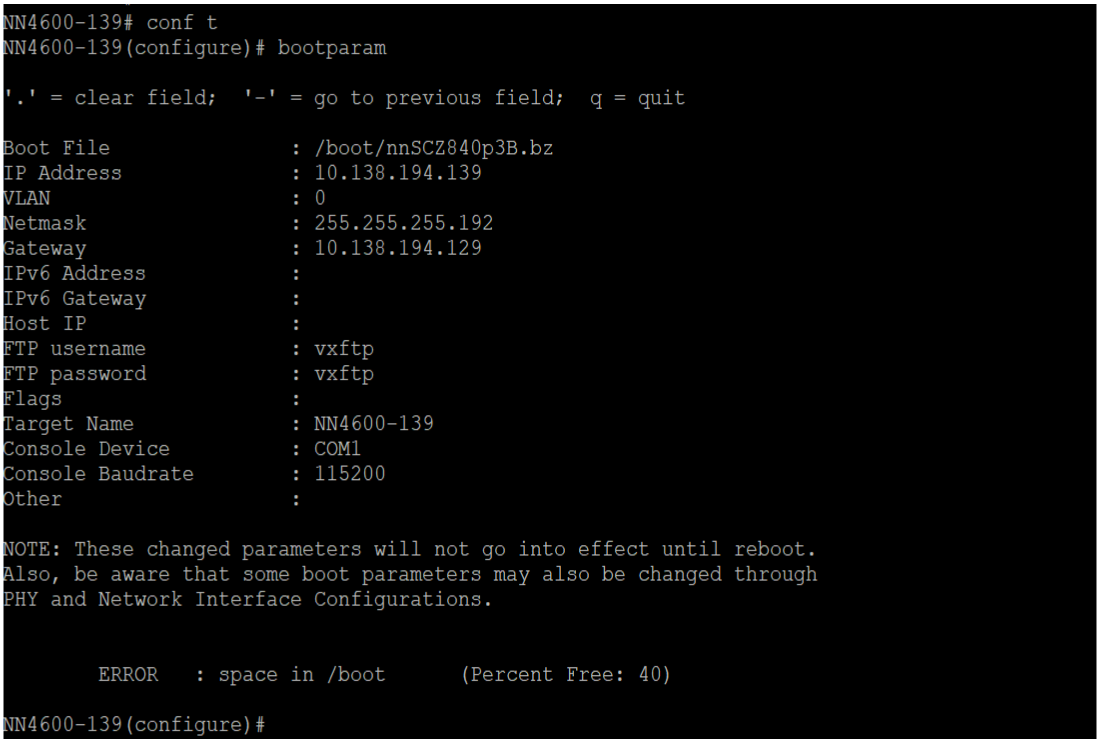
Both passwords must be changed according to the rules shown below.



```
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.

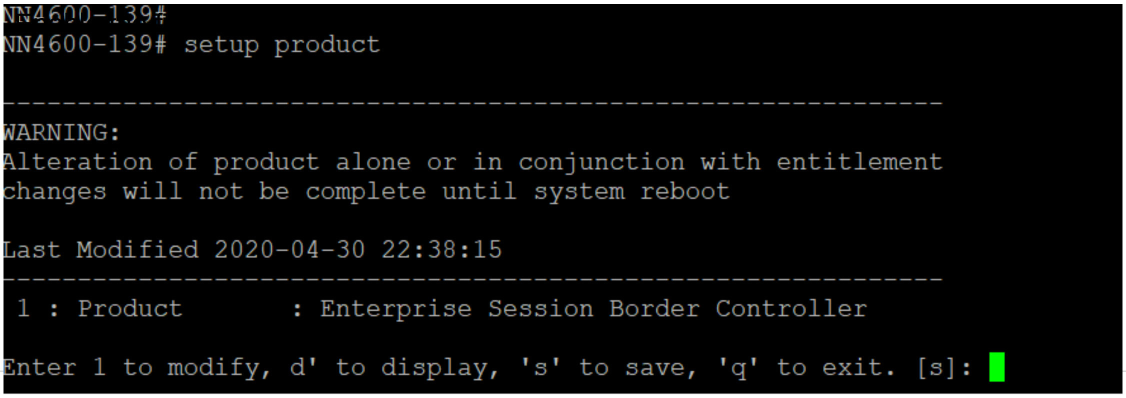


```
NN4600-139# conf t
NN4600-139(configure)# bootparam

'.' = 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.

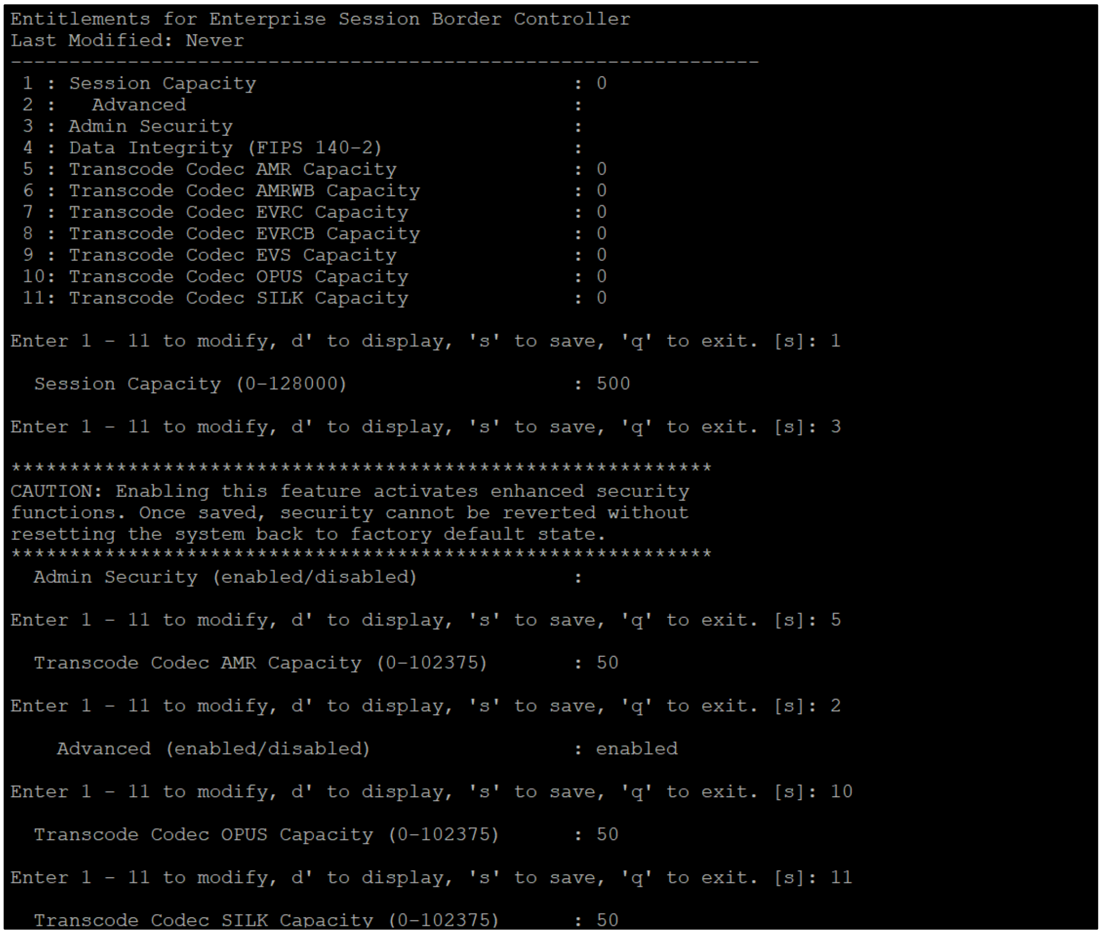
Setup product type to Enterprise Session Border Controller as shown below.

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

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

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

Save the changes and reboot the SBC.

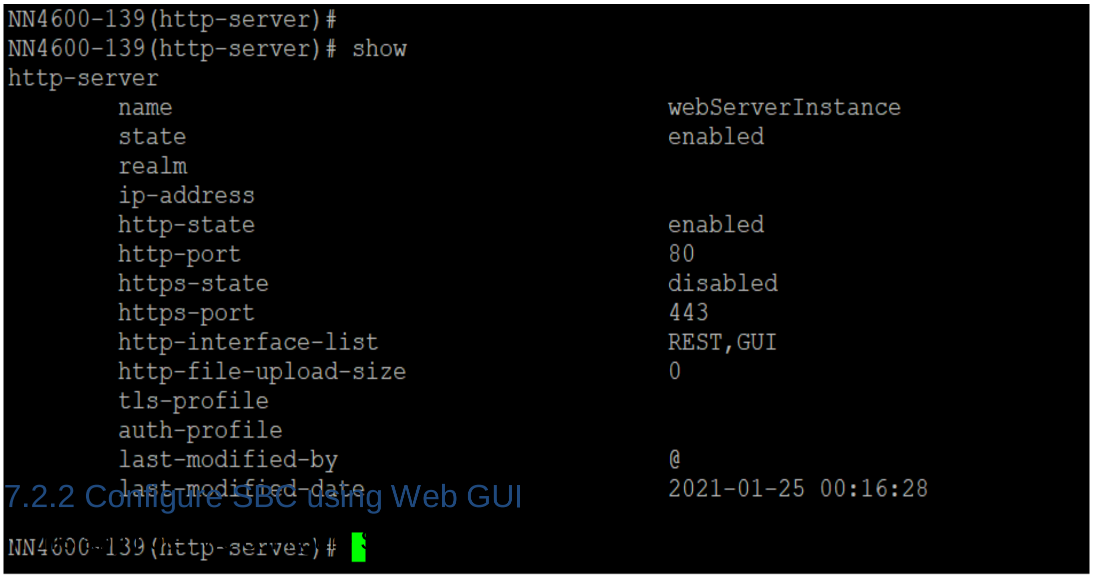


```
Entitlements for Enterprise Session Border Controller
Last Modified: Never
-----------------------------------------------------------------
 1 : Session Capacity                           : 0
 2 :   Advanced                                 :
 3 : Admin Security                             :
 4 :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

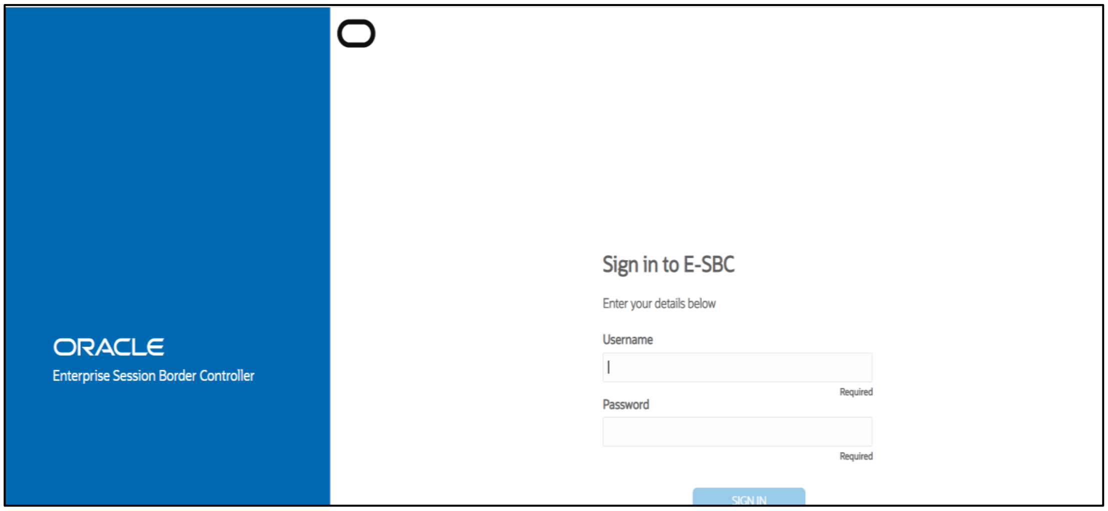
Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.



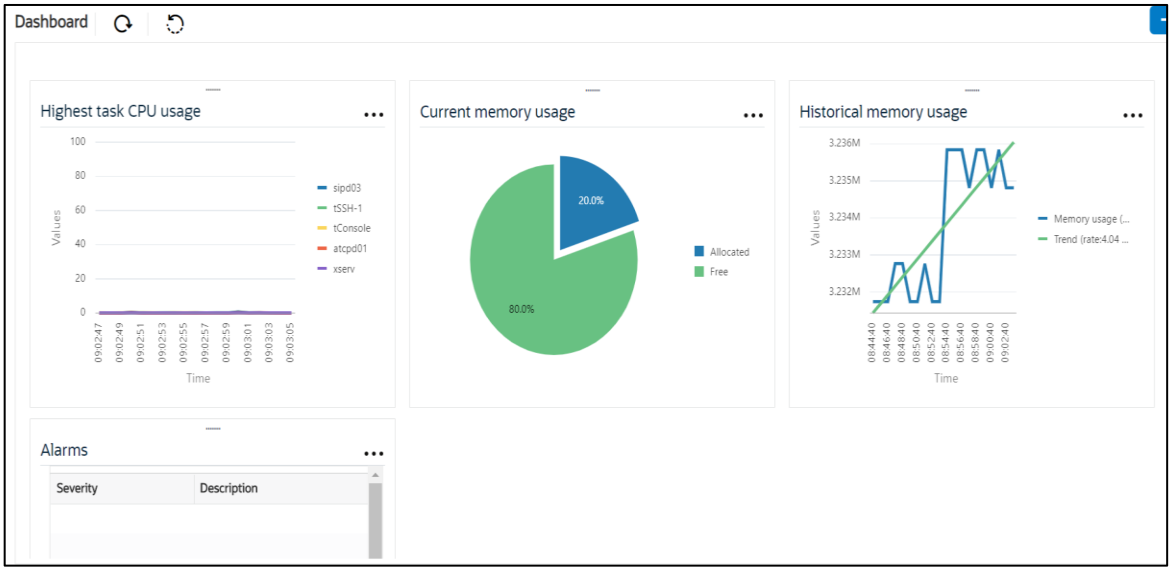
```
NN4600-139(http-server)#
NN4600-139(http-server)# show
http-server
        name                                    webServerInstance
        state                                   enabled
        realm
        ip-address
        http-state                              enabled
        http-port 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

7.2.2 Configure SBC using Web GUI

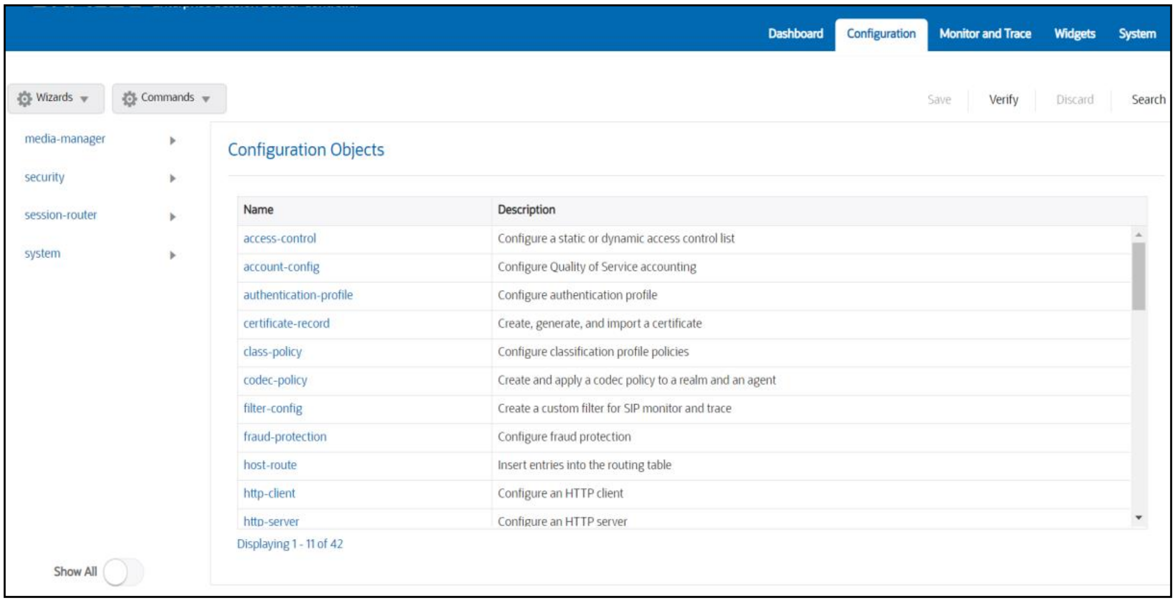
The Web GUI can be accessed through the URL http://<SBC_MGMT_IP>.



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.

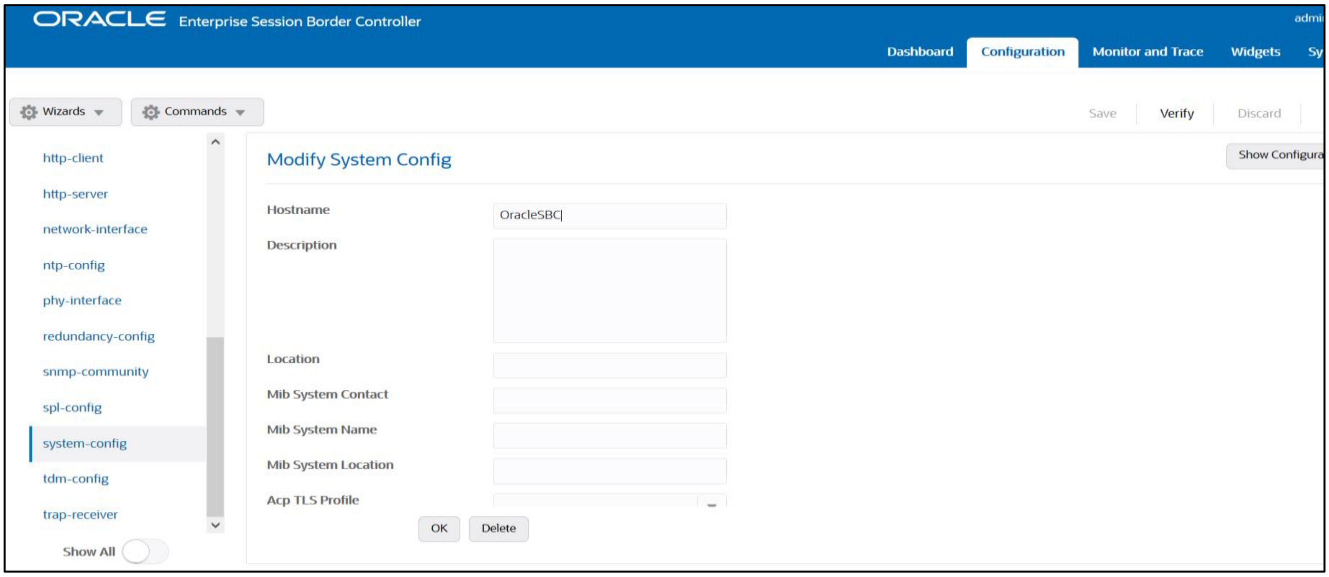
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf

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.

7.2. Configure system-config

Navigate to system->system-config



Modify System Config

Hostname: OracleSBC|

Description

Location

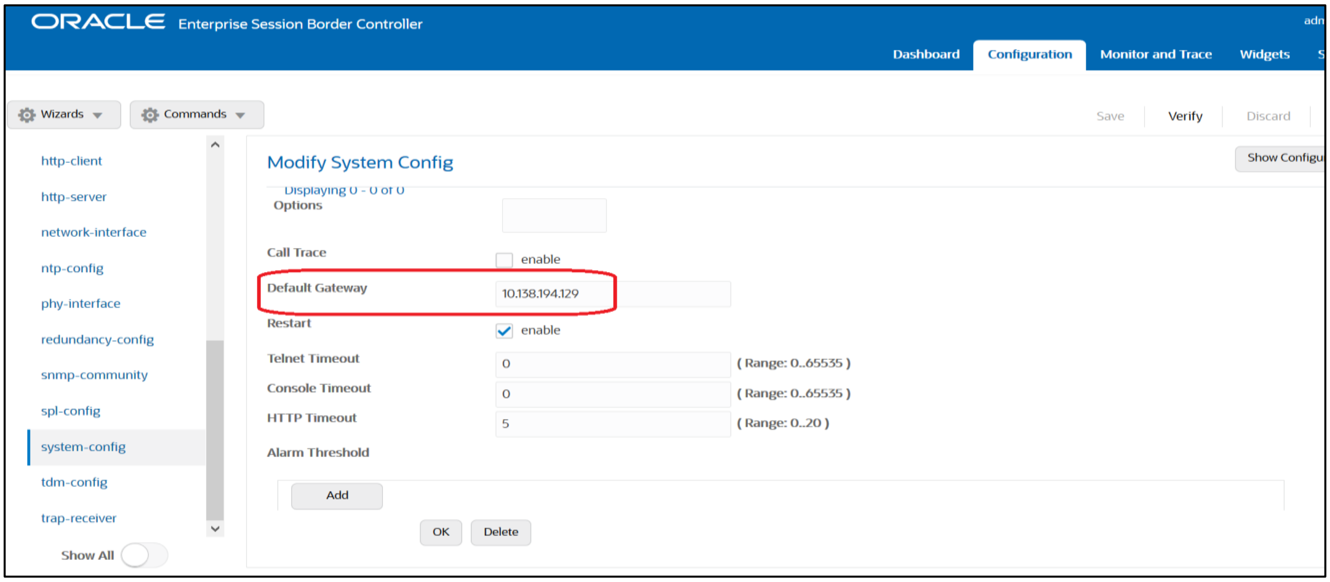
Mib System Contact

Mib System Name

Mib System Location

Acp TLS Profile

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



Modify System Config

Displaying 0 - 0 of 0

Options

Call Trace □ enable

Default Gateway 10.138.194.129

Restart ☑ enable

Telnet Timeout 0 (Range: 0..65535)

Console Timeout 0 (Range: 0..65535)

HTTP Timeout 5 (Range: 0..20)

Alarm Threshold

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

https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/releasenotes/esbc_scz840_releasenotes.pdf

The above step is needed only if any transcoding is used in the configuration.

If there is no transcoding involved, then the above step is not needed.

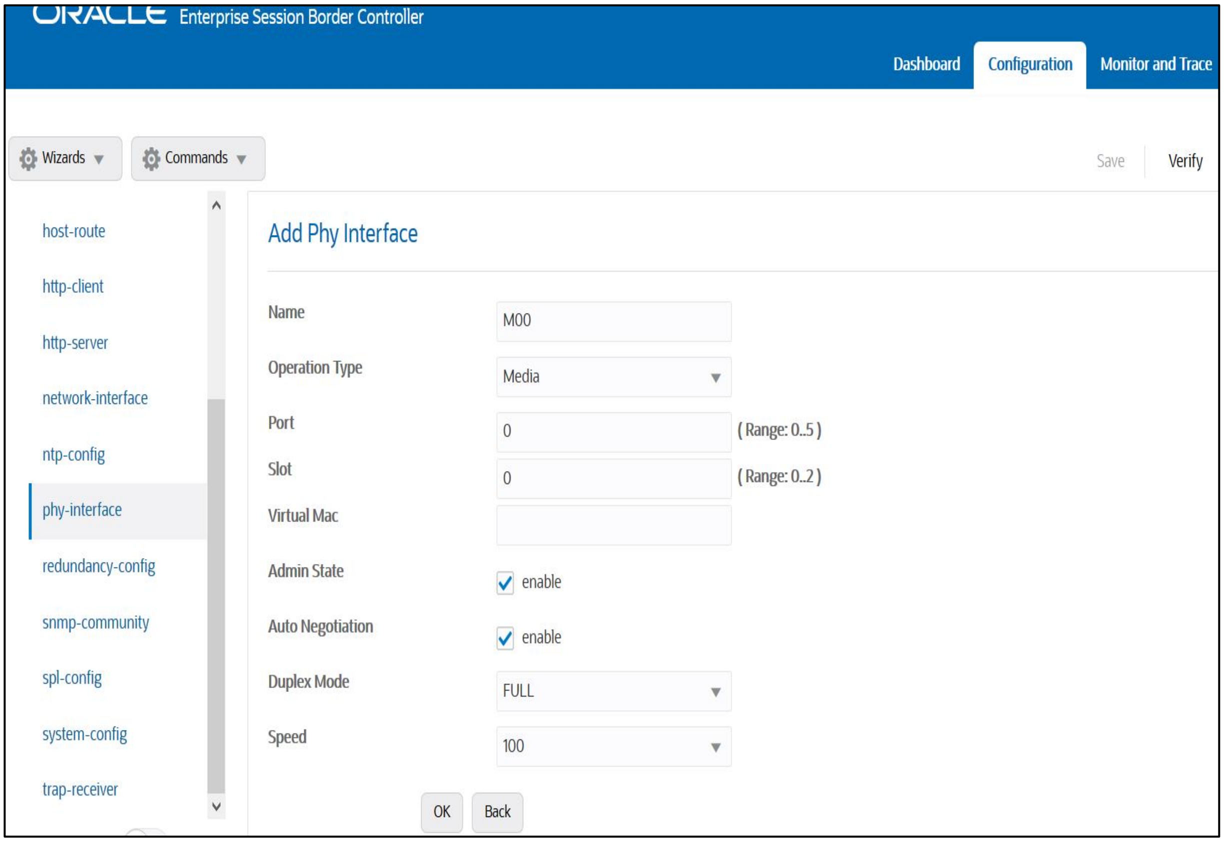
7.3. Configure Physical Interface values

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

Here we have configured, Network-interface M00 for Zoom Phone and M10 for BYOC Cloud.

Parameter Name	Zoom Phone (M00)	Genesys Cloud (M10)
Slot	0	1
Port	0	0
Operation Mode	Media	Media

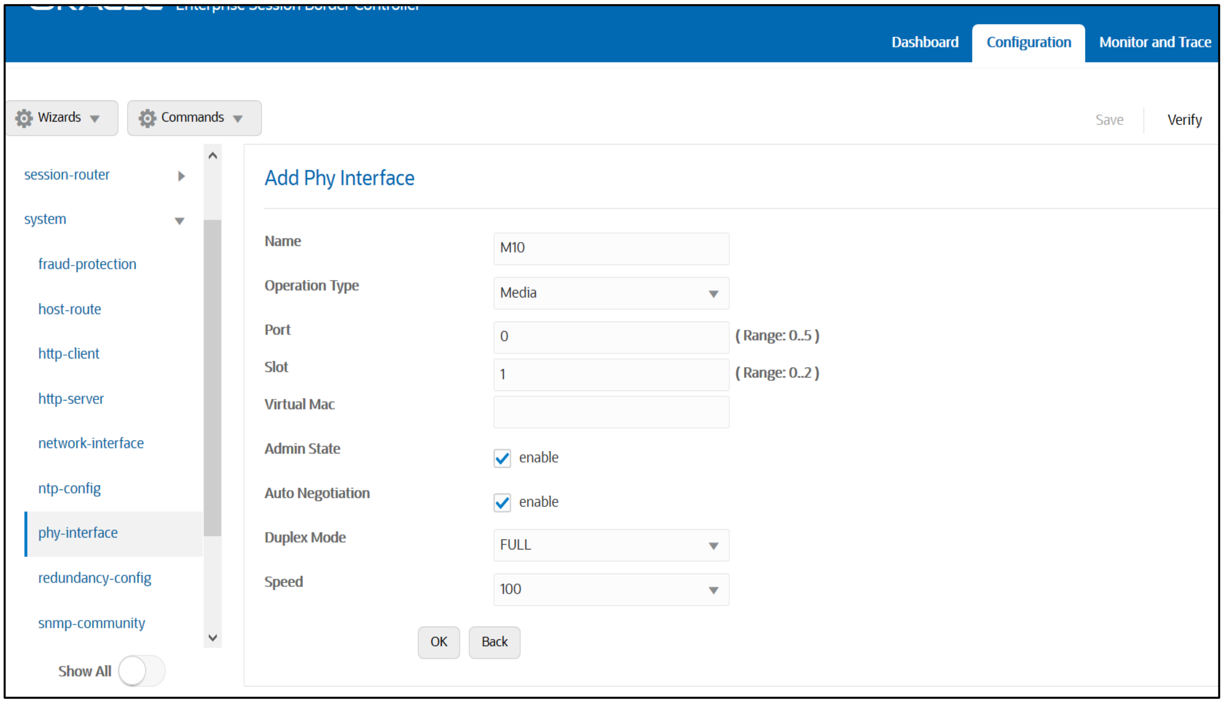
Configure **M00** interface as per example shared below.



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 per example shared 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	

7.4. 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.

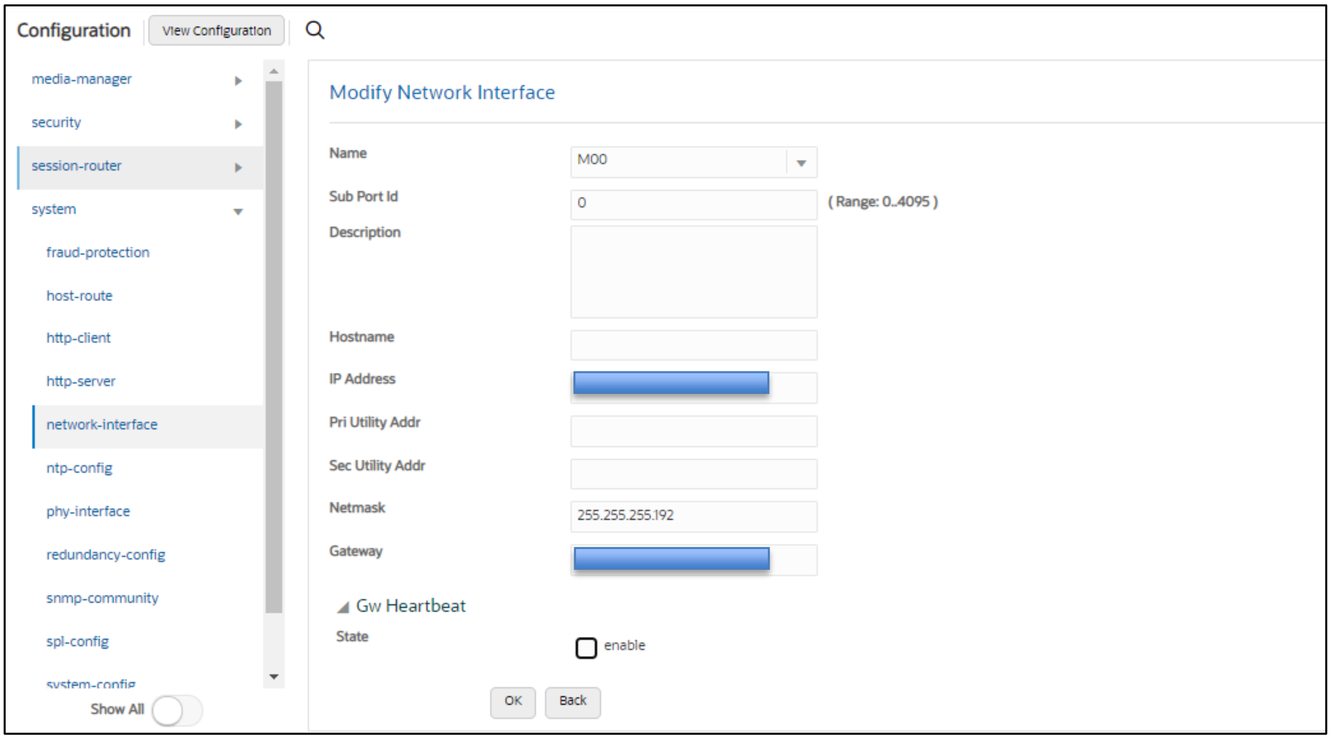
Note: The provided network IP addresses are given for example purpose only. In the real-world scenario

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	**Zoom Phone Network Interface**	**Genesys Cloud Network interface**
Name	M00	M10
Host Name	Domain (if applicable)	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
Dns-domain	Domain(if applicable)	solutionslab.cgbubedford.com

Configure network interface **M00** as below



Modify Network Interface

Name: M00

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

Description:

Hostname:

IP Address: [redacted]

Pri Utility Addr:

Sec Utility Addr:

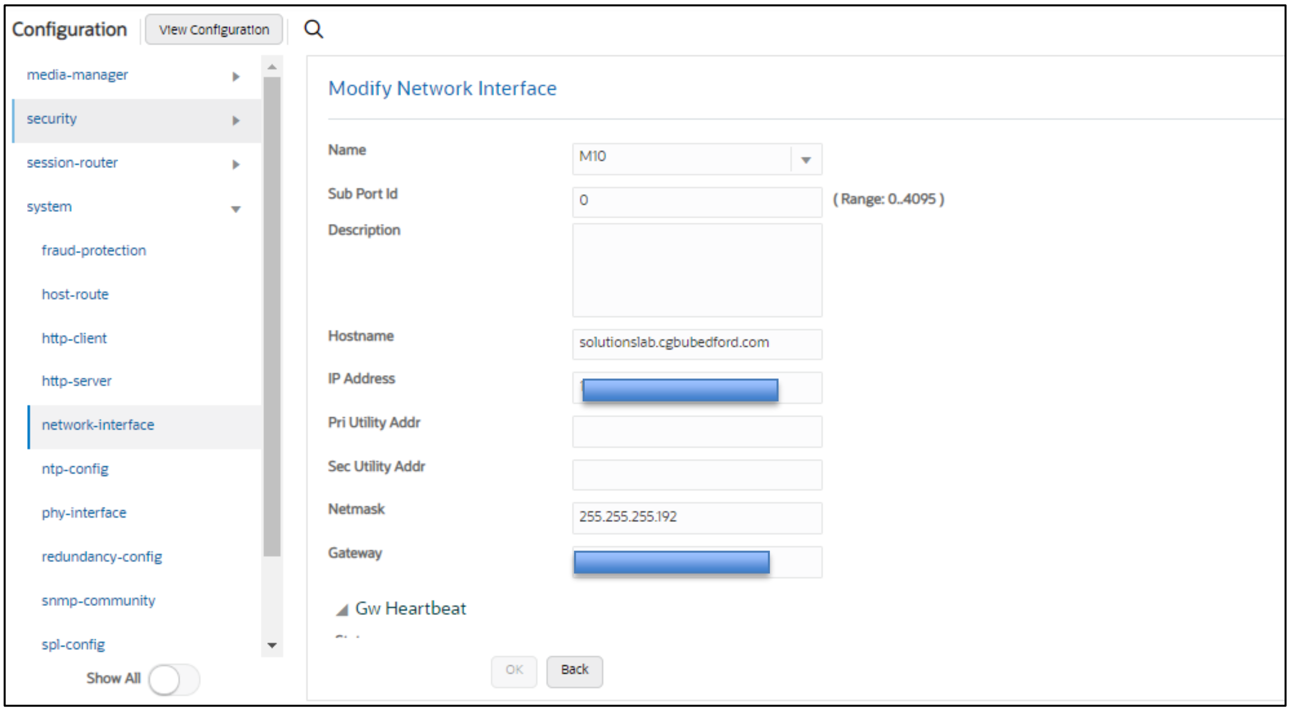
Netmask: 255.255.255.192

Gateway: [redacted]

Gw Heartbeat

State: □ enable

Similarly, configure network interface **M10** as below



Modify Network Interface

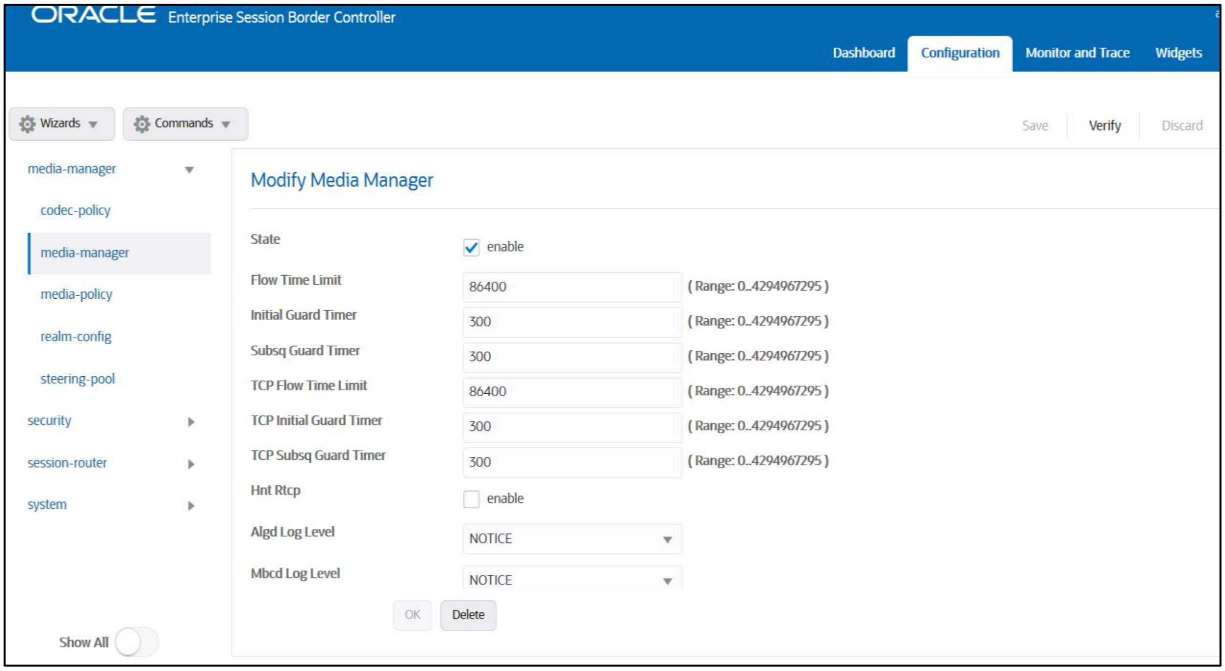
Name	M10	
Sub Port Id	0	(Range: 0..4095)
Description		
Hostname	solutionslab.cgbubedford.com	
IP Address	[redacted]	
Pri Utility Addr		
Sec Utility Addr		
Netmask	255.255.255.192	
Gateway	[redacted]	

7.5. Enable media manager

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

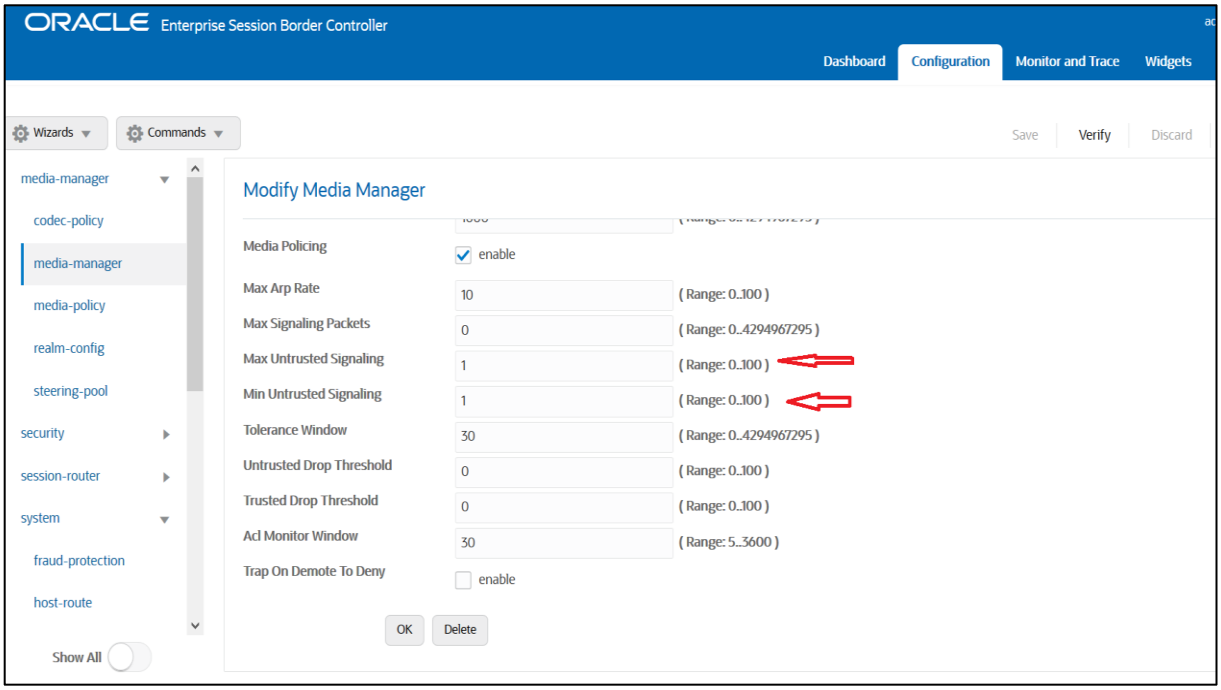
In addition to the above config, please set the max and min untrusted signaling values to one.

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	

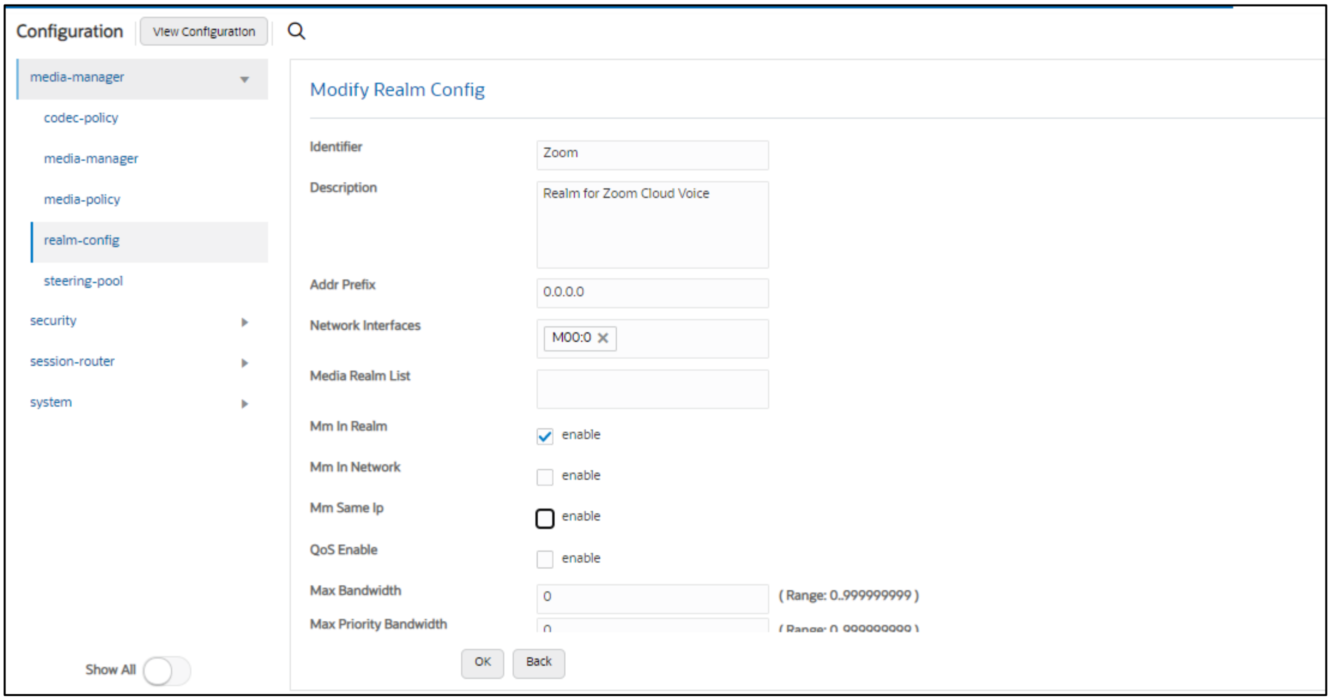
7.6. Configure Realms

Navigate to media-manager > realm-config

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:

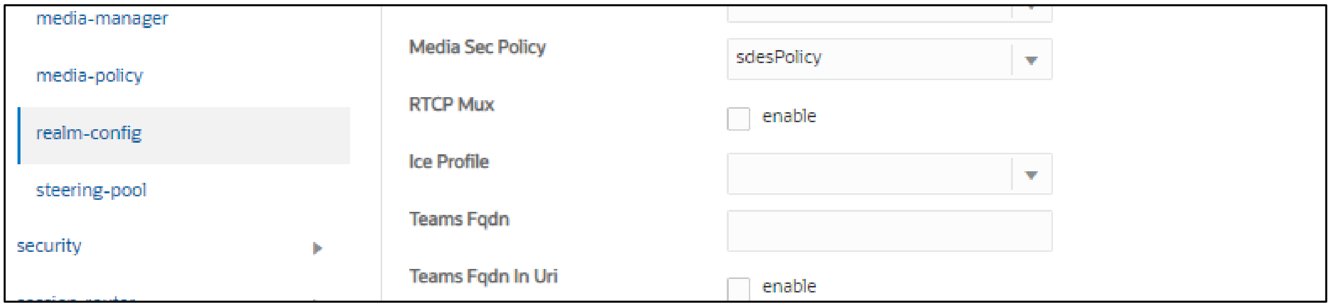
Config Parameter	Zoom Realm	GenesysCloud Realm
Identifier	Zoom	GenesysCloud
Network Interface	M00	M10
Mm in realm	☑	☑
Access Control Trust Level	High	High
Media Sec policy	sdespolicy	sdespolicy
RTCP mux	☑optional	

Realm for Zoom Phone –



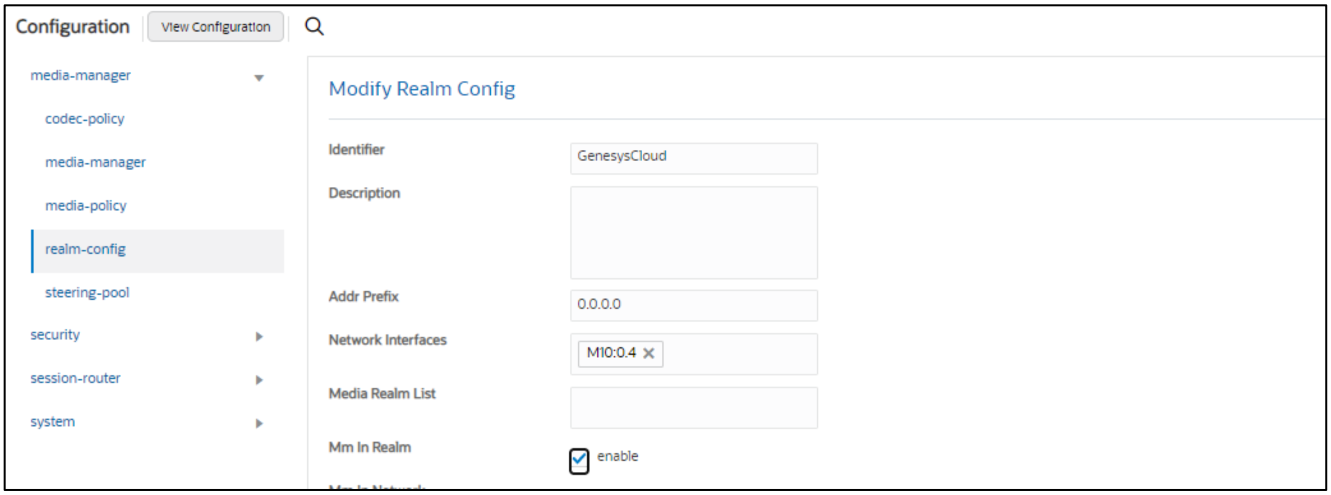
Modify Realm Config

Identifier	Zoom
Description	Realm for Zoom Cloud Voice
Addr Prefix	0.0.0.0
Network Interfaces	M00:0 ✕
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)



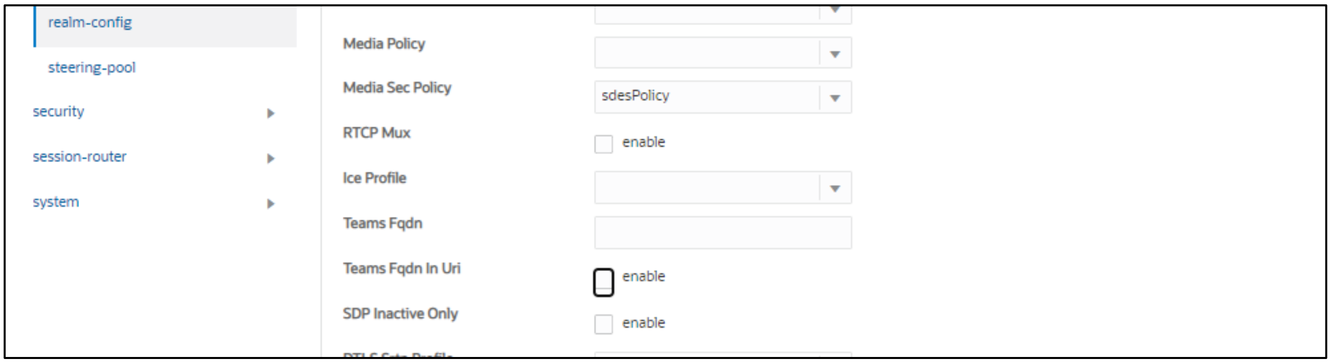
Media Sec Policy	sdesPolicy
RTCP Mux	□ enable
Ice Profile	
Teams Fqdn	
Teams Fqdn In Uri	□ enable

Realm for Genesys BYOC Cloud

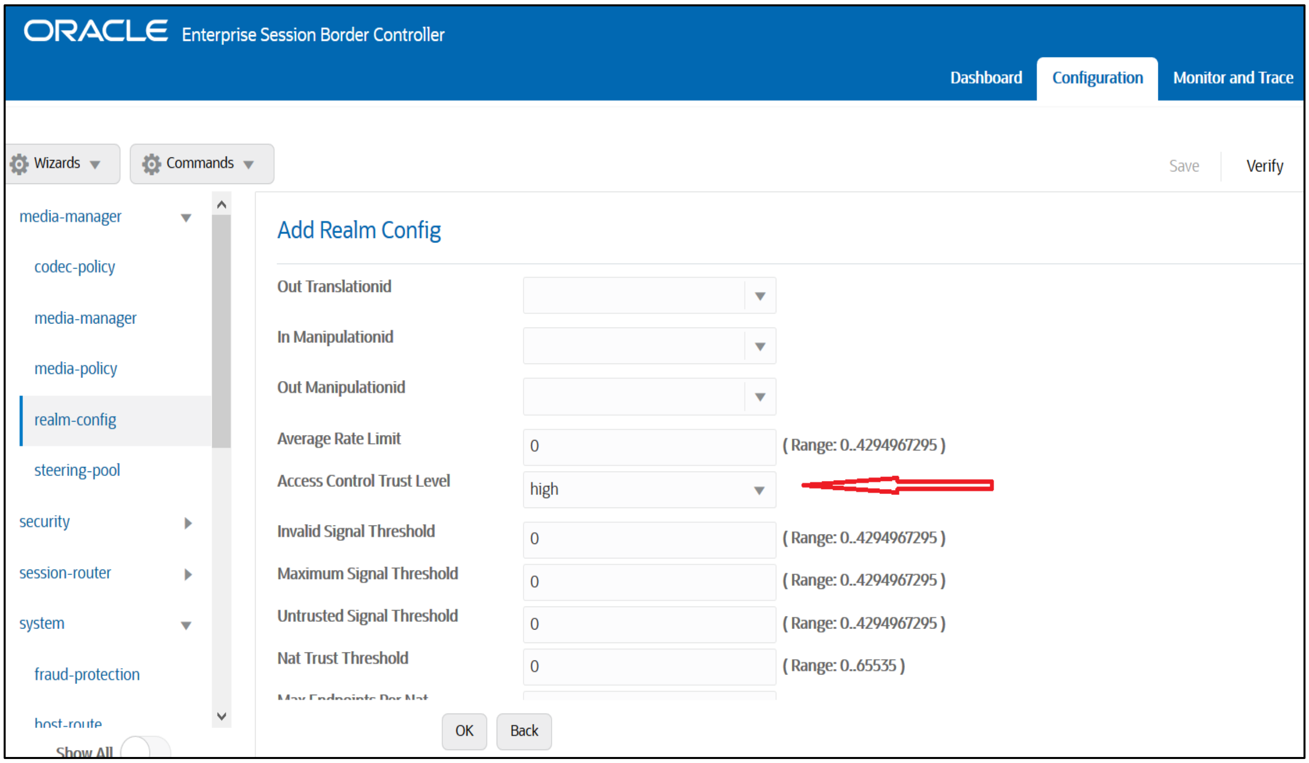


Modify Realm Config

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)

We have set Access Control Trust Level on the Reams to High as we have static access-control configured and this is a peering enviorment.

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

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

7.7. SIP Security Configuration

This section describes how to configure the SBC for TLS and SRTP communication for **Zoom Phone and BYOC Cloud**. It requires a certificate signed by one of the trusted Certificate Authorities.

The communication between the **Oracle SBC with Zoom Phone and Genesys BYOC Cloud 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.

7.7.1 Configuring Certificates for Zoom Phone

GUI Path: security/certificate-record

For the purposes of this application note, we'll create certificate records as below.

- **SBC Certificates (end-entity certificate) for Zoom Phone and Genesys BYOC Cloud**
- **DigiCert Root CA (SBC and Zoom Phone)**
- **DigiCert Intermidiate Cert (this is optional – only required if your server certificate is signed by an intermediate) (Not shown)**
- **DigiCert Global Root G2(Genesys BYOC Cloud and Zoom Phone)**
- **DigiCert Global Root G3(Genesys BYOC Cloud and Zoom Phone)**

These Certificates can be downloaded at below links –

- https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem
- https://www.digicert.com/kb/digicert-root-certificates.htm#intermediates

The follow certificates must be installed onto the SBC to trust the TLS Certificate provided by Zoom for TLS negotiation.DigiCert TLS Certificates can be downloaded at below Links.

- https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem
- https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem
- https://cacerts.digicert.com/DigiCertGlobalRootG3.crt.pem

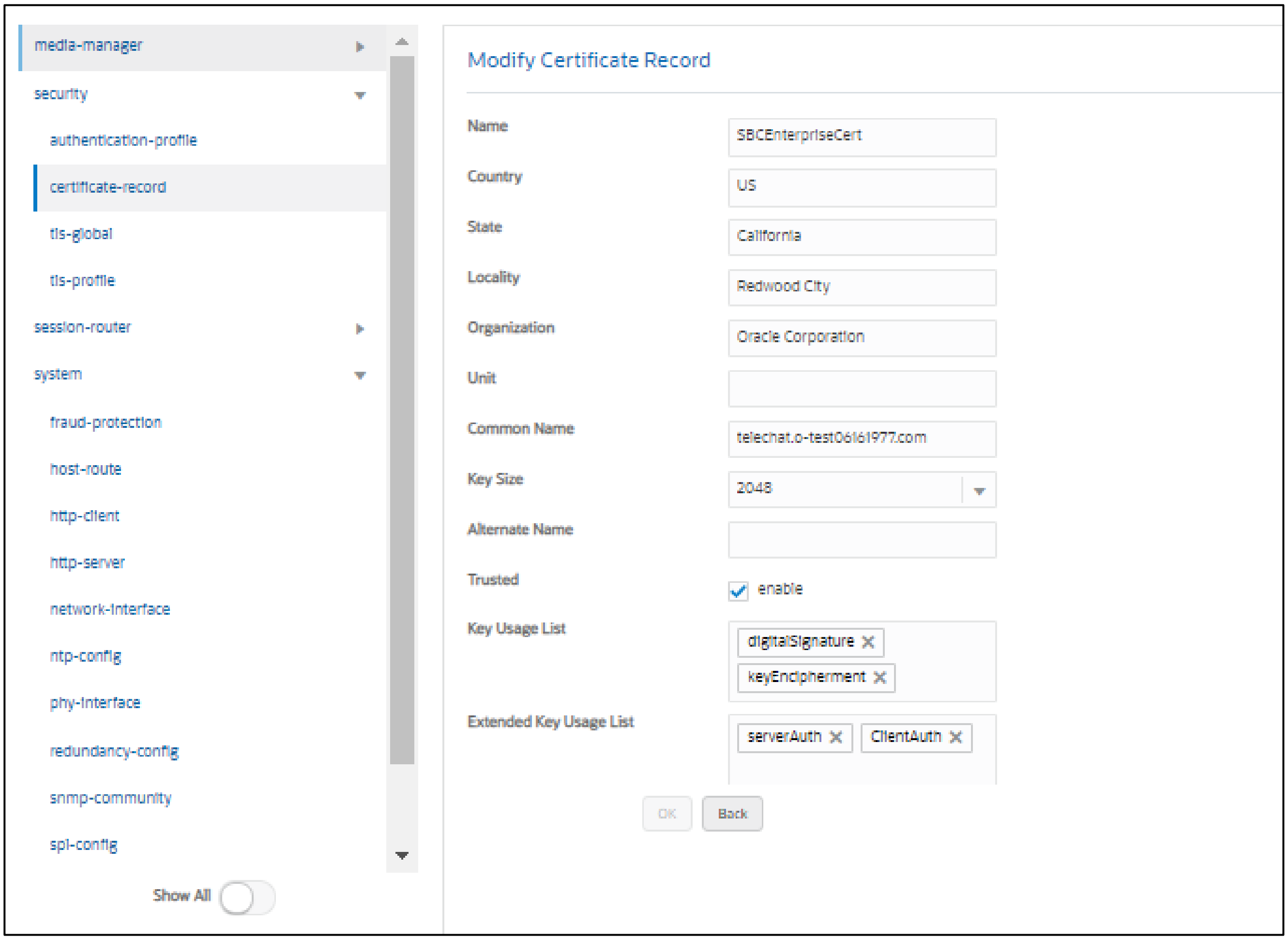
7.7.1.1 SBC End Entity Certificate for Zoom Phone

The SBC's end entity certificate is what is presented to Zoom Phone signed by your CA authority, in this example we are using Digicert as our signing authority. The certification must include a common name.
For this, we are using an fqdn as the common name.

- Common name: (**telechat.o-test06161977.com**)

To Configure the certificate record:

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



Modify Certificate Record

Name	SBCEnterpriseCert
Country	US
State	California
Locality	Redwood City
Organization	Oracle Corporation
Unit	
Common Name	telechat.o-test06161977.com
Key Size	2048
Alternate Name	
Trusted	☑ enable
Key Usage List	digitalSignature ✕ keyEncipherment ✕
Extended Key Usage List	serverAuth ✕ ClientAuth ✕

- Click OK at the bottom
- Next, using this same procedure, configure certificate records for Root CA and Intermediate Certificates

7.7.1.2 Root CA and Intermediate Certificates

The following, DigitCertRootGlobalRootCA and DigiCert SHA2 Secure Server CA are the root and intermediate CA certificates used to sign the SBC's end entity certificate.

To trust Zoom certificates, your SBC must have below DigiCert Global Root CA, DigiCert Global Root G2 and DigiCert Global Root G3 installed.

Note : Since both Oracle SBC and Zoom use DigiCert Global Root CA only one certificate record should be created for the DigiCert Global Root CA certificate.

Zoom Approved CA Vendors

Below is the list of Zoom approved CA Vendors. Oracle SBC Certificate can be signed by any of these Certificate Authorities.

Certificate Issuer Organization	Common Name or Certificate Name
Buypass AS-983163327	Buypass Class 2 Root CA
Buypass AS-983163327	Buypass Class 3 Root CA
Baltimore	Baltimore CyberTrust Root

Cybertrust, Inc	Cybertrust Global Root
DigiCert Inc	DigiCert Assured ID Root CA
DigiCert Inc	DigiCert Assured ID Root G2
DigiCert Inc	DigiCert Assured ID Root G3
DigiCert Inc	DigiCert Global Root CA
DigiCert Inc	DigiCert Global Root G2
DigiCert Inc	DigiCert Global Root G3
DigiCert Inc	DigiCert High Assurance EV Root CA
DigiCert Inc	DigiCert Trusted Root G4
GeoTrust Inc.	GeoTrust Global CA
GeoTrust Inc.	GeoTrust Primary Certification Authority
GeoTrust Inc.	GeoTrust Primary Certification Authority - G2
GeoTrust Inc.	GeoTrust Primary Certification Authority - G3
GeoTrust Inc.	GeoTrust Universal CA
GeoTrust Inc.	GeoTrust Universal CA 2
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G6
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G6
Thawte, Inc.	Thawte Primary Root CA
Thawte, Inc.	Thawte Primary Root CA - G2
Thawte, Inc.	Thawte Primary Root CA - G3

VeriSign, Inc.	VeriSign Class 1 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 2 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G4
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign, Inc.	VeriSign Universal Root Certification Authority
AffirmTrust	AffirmTrust Commercial
AffirmTrust	AffirmTrust Networking
AffirmTrust	AffirmTrust Premium
AffirmTrust	AffirmTrust Premium ECC
Entrust, Inc.	Entrust Root Certification Authority
Entrust, Inc.	Entrust Root Certification Authority - EC1
Entrust, Inc.	Entrust Root Certification Authority - G2
Entrust, Inc.	Entrust Root Certification Authority - G4
Entrust.net	Entrust.net Certification Authority (2048)
GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign nv-sa	GlobalSign Root CA
The GoDaddy Group, Inc.	Go Daddy Class 2 CA
GoDaddy.com, Inc.	Go Daddy Root Certificate Authority - G2
Starfield Technologies, Inc.	Starfield Class 2 CA
Starfield Technologies, Inc.	Starfield Root Certificate Authority - G2
QuoVadis Limited	QuoVadis Root CA 1 G3
QuoVadis Limited	QuoVadis Root CA 2
QuoVadis Limited	QuoVadis Root CA 2 G3
QuoVadis Limited	QuoVadis Root CA 3
QuoVadis Limited	QuoVadis Root CA 3 G3
QuoVadis Limited	QuoVadis Root Certification Authority
Comodo CA Limited	AAA Certificate Services
AddTrust AB	AddTrust Class 1 CA Root

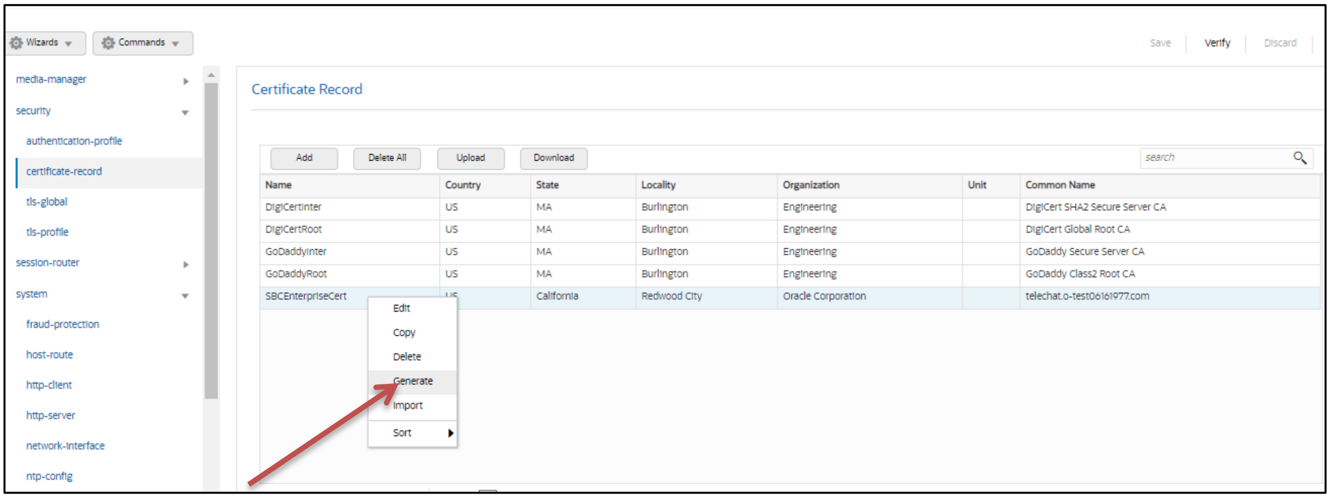
AddTrust AB	AddTrust External CA Root
COMODO CA Limited	COMODO Certification Authority
COMODO CA Limited	COMODO ECC Certification Authority
COMODO CA Limited	COMODO RSA Certification Authority
The USERTRUST Network	USERTrust ECC Certification Authority
The USERTRUST Network	USERTrust RSA Certification Authority
T-Systems Enterprise ServicesGmbH	T-TeleSec GlobalRoot Class 2
T-Systems Enterprise ServicesGmbH	T-TeleSec GlobalRoot Class 3

Generate Certificate Signing Request

Now that the SBC's certificate has been configured, create a certificate signing request for the SBC's end entity only.

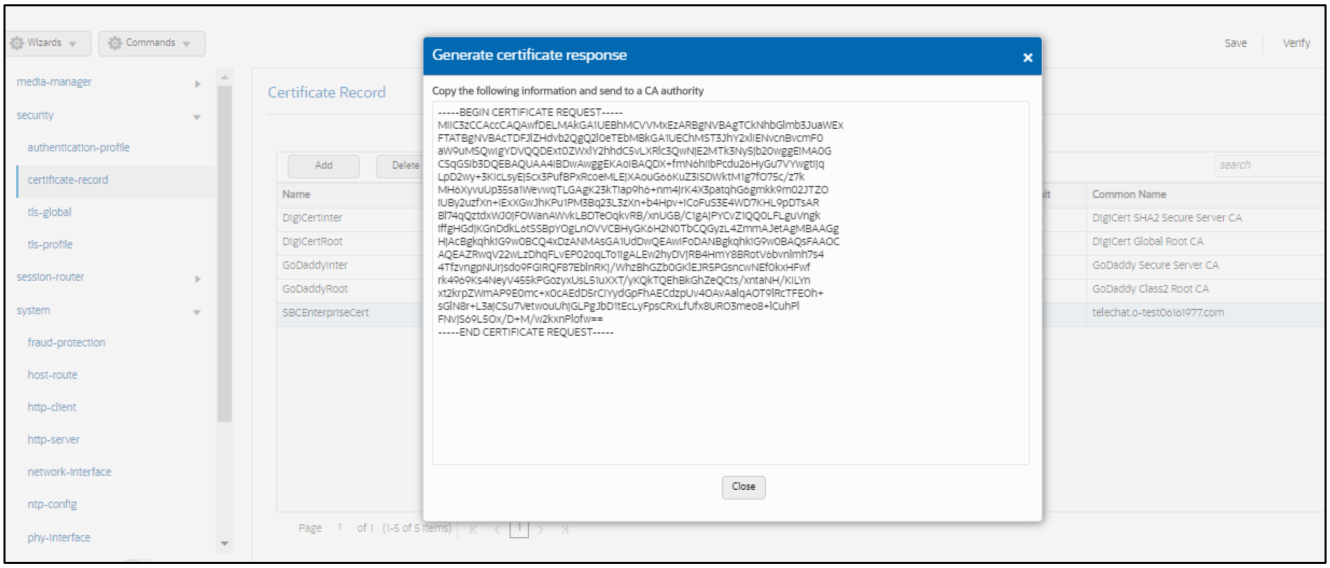
This is not required for any of the Root CA or intermidiate certificates that have been created.

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



Certificate Record

Name	Country	State	Locality	Organization	Unit	Common Name
DigiCertInter	US	MA	Burlington	Engineering		DigiCert SHA2 Secure Server CA
DigiCertRoot	US	MA	Burlington	Engineering		DigiCert Global Root CA
GoDaddyInter	US	MA	Burlington	Engineering		GoDaddy Secure Server CA
GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 Root CA
SBCEnterpriseCert	US	California	Redwood City	Oracle Corporation		telechat.o-test06161977.com



Generate certificate response

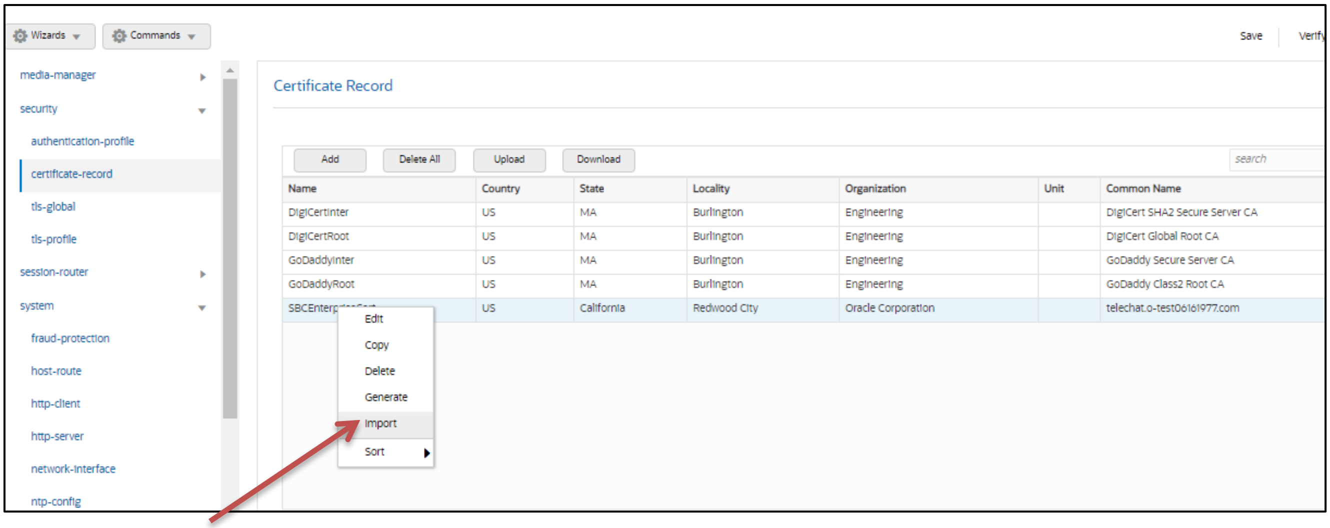
Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3zCCAccCAQAwfDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWEx
FTATBgNVBAcTDFJlZHdvb2QgQ2l0eTEbMBkGA1UEChMST3JhY2xlIENvcnBvcmF0
aW9uMSQwIgYDVQQDExt0ZWxlY2hhdC5vLXRlc3QwNjE2MTk3Ny5jb20wggEIMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDX+fmN6hI1bPcdu26HyGu7VYWgtIJq
LpD2wy+3KIcLsyEJ5cx3PufBPxRcoeMLEJXAouG66KuZ3ISDWktM1g7fO75c/z7k
MH6XyvuUp35sa1WevwqTLGAgK23kTIap9h6+nm4JrK4X3patqhG6gmkk9m02JTZO
1UBy2uzfXn+IExXGwJhKPu1PM3Bq23L3zXn+b4Hpv+1CoFuS3E4WD7KHL9pDTsAR
Bl74qQztdxWJ0JFOWanAWvkLBDTeOqkvRB/xnUGB/C1gAJPYCvZ1QQ0LFLguVngk
1ffgHGdJKGnDdkL6tSSBpYOgLnOVVCBHyGK6H2N0TbCQGyzL4ZmmAJetAgMBAAGg
HJAcBgkqhkiG9w0BCQ4xDzANMAsGA1UdDwQEAwIFoDANBgkqhkiG9w0BAQsFAAOC
AQEAZRwqV22wLzDhqFLvEP02oqLTo1IgALEw2hyDVJRB4HmY8BRotV6bvnlmh7s4
4TfzvngpNUrJsdo9FGIRQF87EblnRKJ/WhzBhGZb0GKlEJR5PGsncwNEf0kxHFwf
rk4969Ks4NeyV455kPGozyxUsL51uXXT/yKQkTQEhBkGhZeQCts/xntaNH/KILYn
xt2krpZWmAP9E0mc+x0cAEdD5rCIYydGpFhAECdzpUv4OAvAalqAOT9lRcTFEOh+
sGlN8r+L3aJCSu7VetwouUhJGLPgJbD1tEcLyFpsCRxLfUfx8URO3meo8+lCuhPl
FNvJS69L5Ox/D+M/w2kxnPlofw==
-----END CERTIFICATE REQUEST-----
```

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

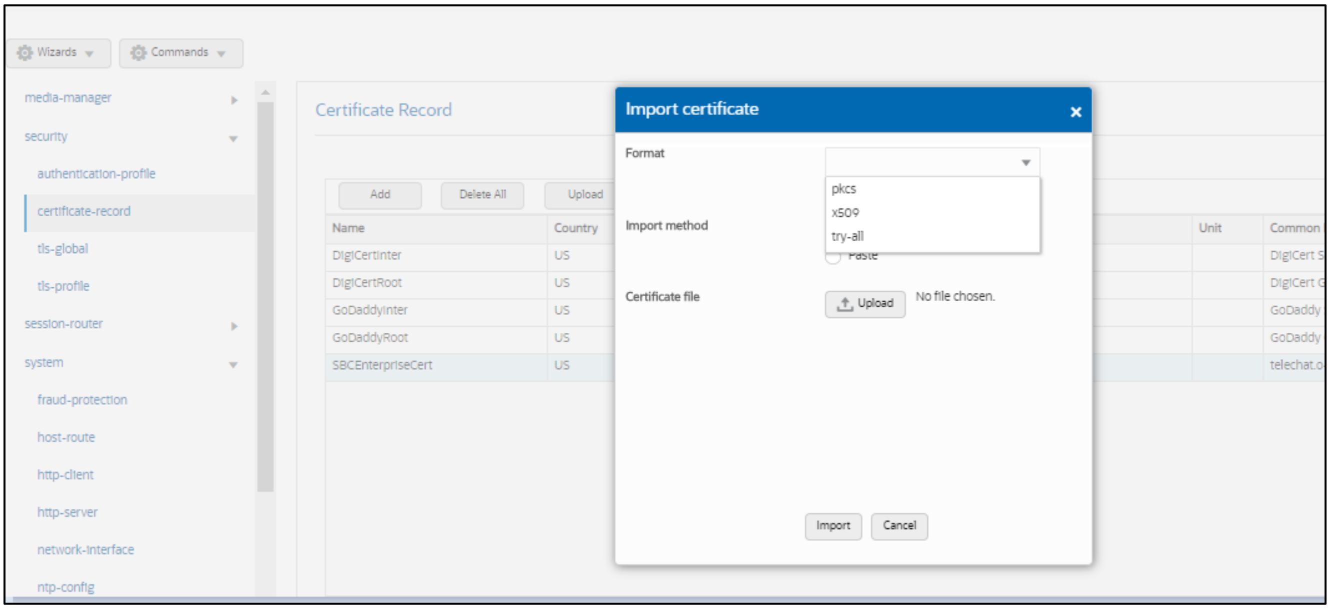
7.7.1.3 Import Certificates to SBC

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



Certificate Record

Name	Country	State	Locality	Organization	Unit	Common Name
DigiCertInter	US	MA	Burlington	Engineering		DigiCert SHA2 Secure Server CA
DigiCertRoot	US	MA	Burlington	Engineering		DigiCert Global Root CA
GoDaddyInter	US	MA	Burlington	Engineering		GoDaddy Secure Server CA
GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 Root CA
SBCEnterp	US	California	Redwood City	Oracle Corporation		telechat.o-test06161977.com



Import certificate

Format:
Import method: Paste
Certificate file: No file chosen.

Name	Country	Unit	Common
DigiCertInter	US		DigiCert S
DigiCertRoot	US		DigiCert G
GoDaddyInter	US		GoDaddy
GoDaddyRoot	US		GoDaddy
SBCEnterpriseCert	US		telechat.o

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

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

- DigiCertIntermediate
- DigiCertGlobalRootCA
- DigiCertGlobalRootG2
- DigiCertGlobalRootG3

At this stage, all required certificates have been imported.

7.7.2 Configuring Certificates for Genesys BYOC Cloud

Genesys BYOC Cloud supports TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by one of the trusted Certificate Authorities.

This section describes how to configure the SBC for TLS with Genesys BYOC Cloud. It requires a certificate signed by one of the trusted Certificate Authorities.

"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
ACLI Path: config t->security->certificate-record

For the purposes of this application note, we'll create certificate records as below.

- SBC Certificates (end-entity certificate)
- DigiCertEVRootCA (Genesys BYOC Cloud)

- DigiCert Global Root G2(Genesys BYOC Cloud)
- DigiCert Global Root G3(Genesys BYOC Cloud)

Supported CA for Genesys BYOC Cloud BYOC

Genesys BYOC Cloud signs the BYOC Cloud endpoints with X.509 certificates issued by DigiCert, a public Certificate Authority. The customer endpoints must trust the BYOC Cloud endpoints. Genesys 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 separated by region and uses certificates authorized by either DigiCert High Assurance EV Root CA or DigiCert Global Root G2/DigiCert Global Root G3. You can download the appropriate root public key certificate for your region from DigiCert.

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

https://help.genesys.cloud/announcements/client-authentication-eku-support-removed-from-genesys-cloud-certificate/

Note Genesys BYOC Cloud 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 Certificate (BYOC Cloud)**	**DigiCert High Assurance EV Root CA**	**DigiCert Global Root G2**	**DigiCert Global Root G3**
Name	SBCCert	DigiCert High Assurance EV Root CA	DigiCert Global Root G2	DigiCert Global Root G3
Common Name	solutionslab.cgbubedford.com	DigiCert High Assurance EV Root CA	DigiCert Global Root G2	DigiCert Global Root G3
Key Size	2048	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256	Sha256

7.7.2.1 End Entity Certificate

The SBC's end entity certificate is what is presented to BYOC Cloud signed by your CA authority, in this example we are using Digicert as our signing authority.

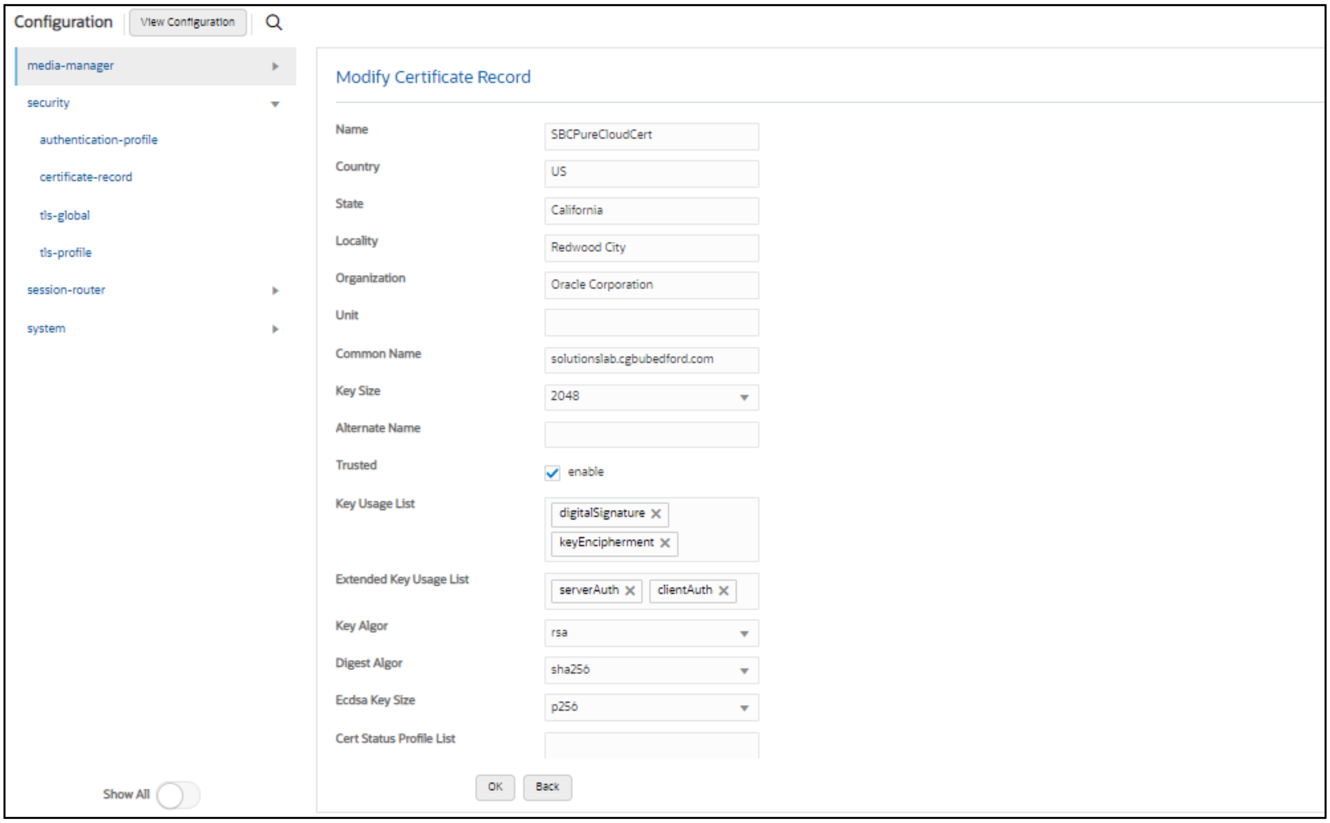
Here in this setup,We wil create two end entity certificates for BYOC Cloud.

- Common name: (**solutionslab.cgbubedford.com**) for BYOC Cloud

Step 1 Configure SBC Certificate Record

To Configure the certificate record:

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



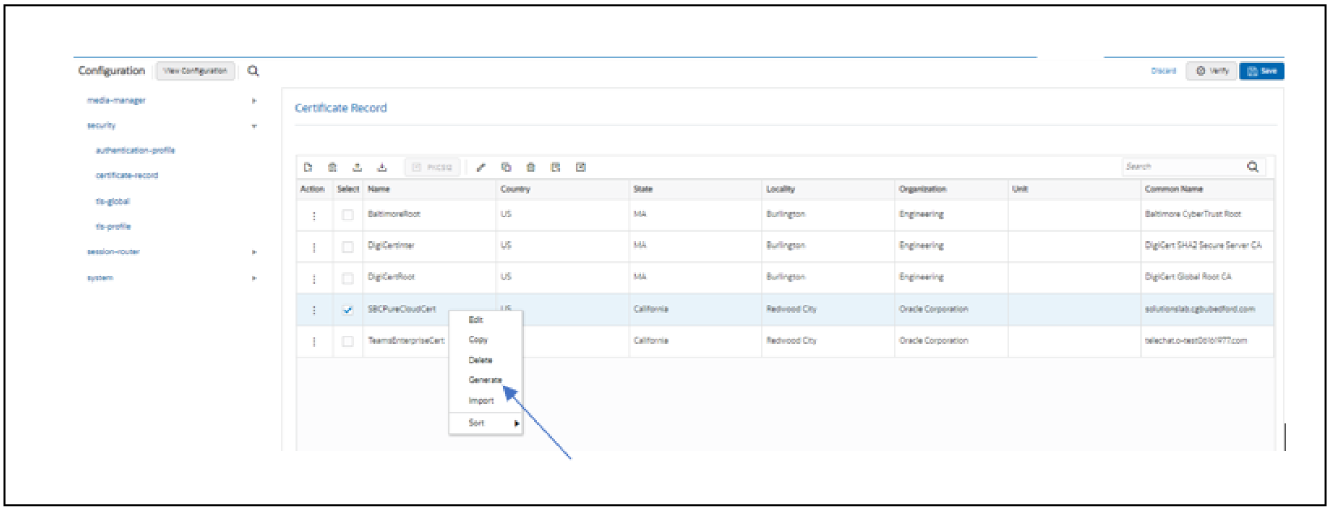
Modify Certificate Record

Name	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

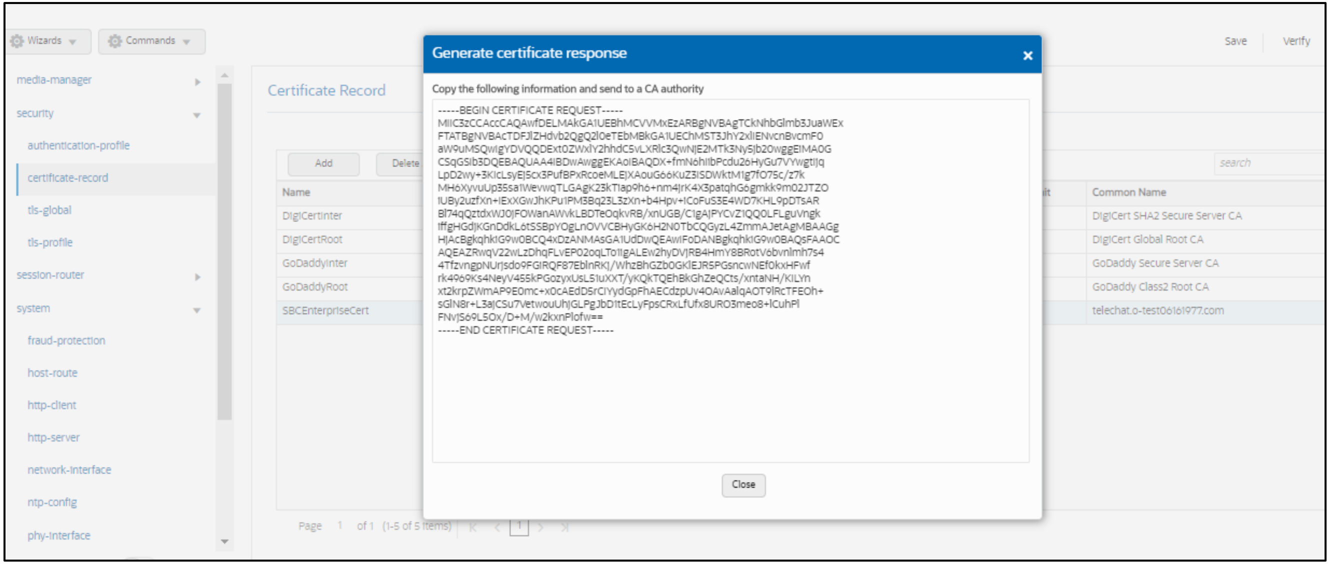
Please note – certificate signing request is only required to be executed for SBC Certificate – not for the root/intermediate certificates.

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



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
⋮	☑	SBCPureCloudCert	US	California	Redwood City	Oracle Corporation		solutionslab.cgbubedford.com
⋮	□	TeamsEnterpriseCert		California	Redwood City	Oracle Corporation		telechat.o-test06161977.com



Name	Common Name
DigiCertInter	DigiCert SHA2 Secure Server CA
DigiCertRoot	DigiCert Global Root CA
GoDaddyInter	GoDaddy Secure Server CA
GoDaddyRoot	GoDaddy Class2 Root CA
SBCEnterpriseCert	telechat.o-test06161977.com

Generate certificate response

Copy the following information and send to a CA authority

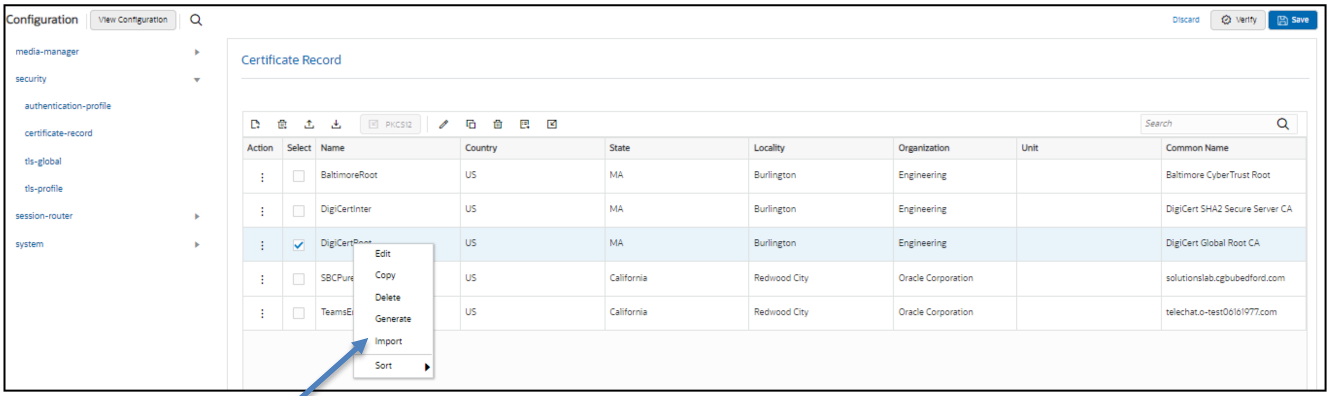
```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3zCCAccCAQAwfDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWEx
FTATBgNVBAcTDFJlZHdvb2QgQ2l0eTEbMBkGA1UEChMST3JhY2xlIENvcnBvcmF0
aW9uMSQwIgYDVQQDExt0ZWxlY2hhdC5vLXRlc3QwNjE2MTk3Ny5jb20wggEIMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDX+fmN6hI1bPcdu26HyGu7VYwgtIJq
LpD2wy+3KIcLsyEJ5cx3PufBPxRcoeMLEJXAouG66KuZ3ISDWktM1g7fO75c/z7k
MH6XyvuUp35sa1WevwqTLGAgK23kTIap9h6+nm4JrK4X3patqhG6gmkk9m02JTZO
1UBy2uzfXn+IExXGwJhKPu1PM3Bq23L3zXn+b4Hpv+ICoFuS3E4WD7KHL9pDTsAR
Bl74qQztdxWJ0JFOWanAWvkLBDTeOqkvRB/xnUGB/C1gAJPYCvZ1QQ0LFLguVngk
1ffgHGdJKGnDdkL6tSSBpYOgLnOVVCBHyGK6H2N0TbCQGyzL4ZmmAJetAgMBAAGg
HJAcBgkqhkiG9w0BCQ4xDzANMAsGA1UdDwQEAwIFoDANBgkqhkiG9w0BAQsFAAOC
AQEAZRwqV22wLzDhqFLvEP02oqLTo1IgALEw2hyDVJRB4HmY8BRotV6bvnlmh7s4
4TfzvngpNUrJsdo9FGIRQF87EblnRKJ/WhzBhGZb0GKlEJR5PGsncwNEf0kxHFwf
rk4969Ks4NeyV455kPGozyxUsL51uXXT/yKQkTQEhBkGhZeQCts/xntaNH/KILYn
xt2krpZWmAP9E0mc+x0cAEdD5rCIYydGpFhAECdzpUv4OAvAalqAOT9lRcTFEOh+
sGlN8r+L3aJCSu7VetwouUhJGLPgJbD1tEcLyFpsCRxLfUfx8URO3meo8+lCuhPl
FNvJS69L5Ox/D+M/w2kxnPlofw==
-----END CERTIFICATE REQUEST-----
```

- copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, **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

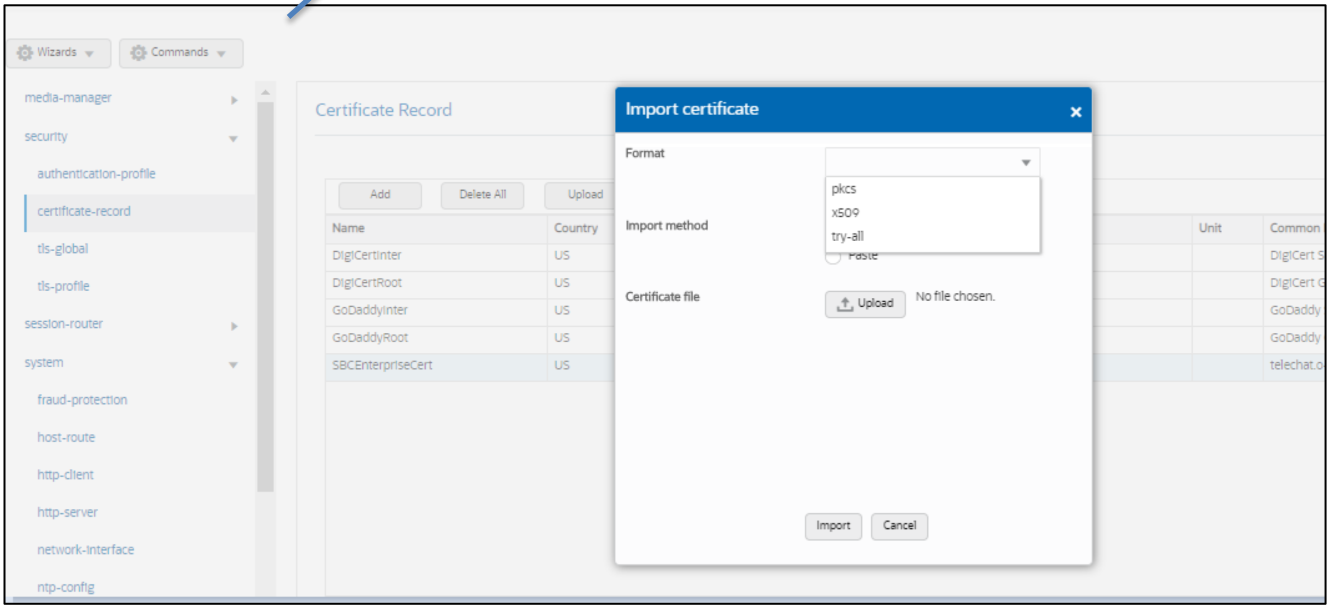
Once certificate signing request have been completed – import the signed certificate to the SBC.

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



Certificate Record

Name	Country	Unit	Common
DigiCertInter	US		DigiCert S
DigiCertRoot	US		DigiCert G
GoDaddyInter	US		GoDaddy
GoDaddyRoot	US		GoDaddy
SBCEnterpriseCert	US		telechat.o

Import certificate

Format: pkcs / x509 / try-all

Import method: ○ Paste

Certificate file: Upload No file chosen.

7.7.2.2 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

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

GUI Path: security/tls-profile

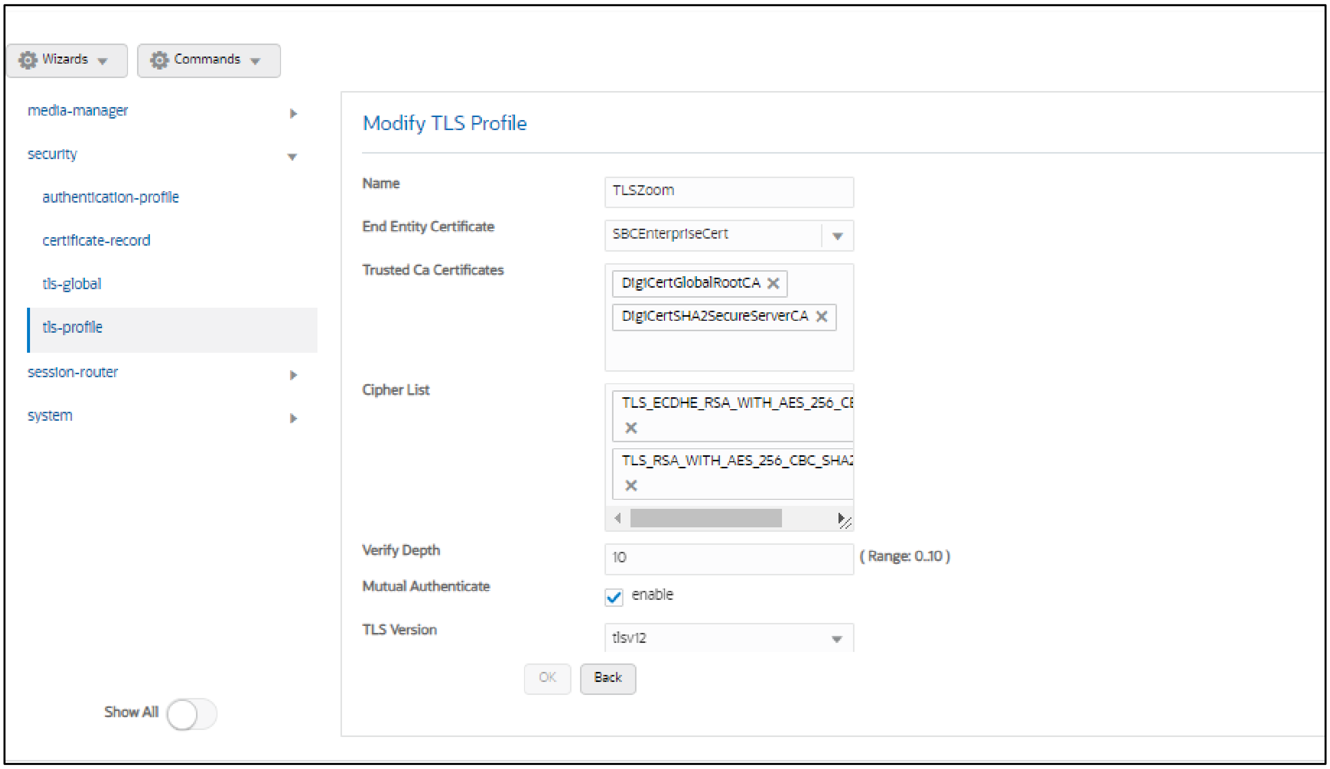
ACLI Path: config t→security→tls-profile

- Click Add, use the example below to configure.

7.8.1 TLS-Profile – Zoom Phone

Zoom supports the following signalling ciphers that need to be added to the TLS profile:

- TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA-384
- RSA-WITH-AES-256-CBC-SHA-256



Modify TLS Profile

Name: TLSZoom
End Entity Certificate: SBCEnterpriseCert
Trusted Ca Certificates: DigiCertGlobalRootCA, DigiCertSHA2SecureServerCA
Cipher List: TLS_ECDHE_RSA_WITH_AES_256_CE, TLS_RSA_WITH_AES_256_CBC_SHA2
Verify Depth: 10 (Range: 0..10)
Mutual Authenticate: ☑ enable
TLS Version: tlsv12

7.8.2 TLS-Profile - Genesys BYOC Cloud

Genesys Cloud BYOC only supports endpoints using the TLS version 1.2 protocol.

Supported TLS ciphers include:

Genesys Cloud supports below TLS ciphers-

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*

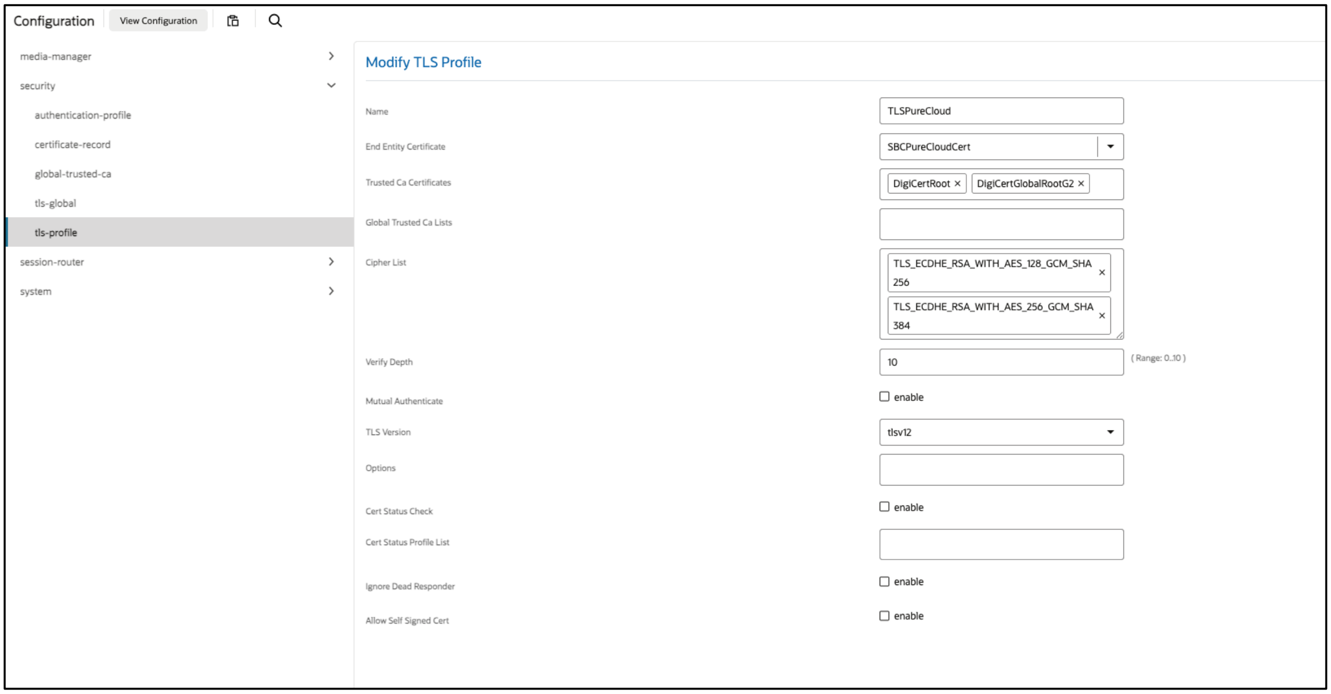
On March 24, 2025, Genesys announced that in a future release, Genesys Cloud will no longer support the following BYOC Cloud TLS ciphers.

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Between Oracle SBC and Genesys BYOC Cloud BYOC we have following common ciphers-

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS-only listeners are available on host port 5061.



Modify TLS Profile

Name: TLSPureCloud
End Entity Certificate: SBCPureCloudCert
Trusted Ca Certificates: DigiCertRoot × DigiCertGlobalRootG2 ×
Global Trusted Ca Lists:
Cipher List: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 × TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ×
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

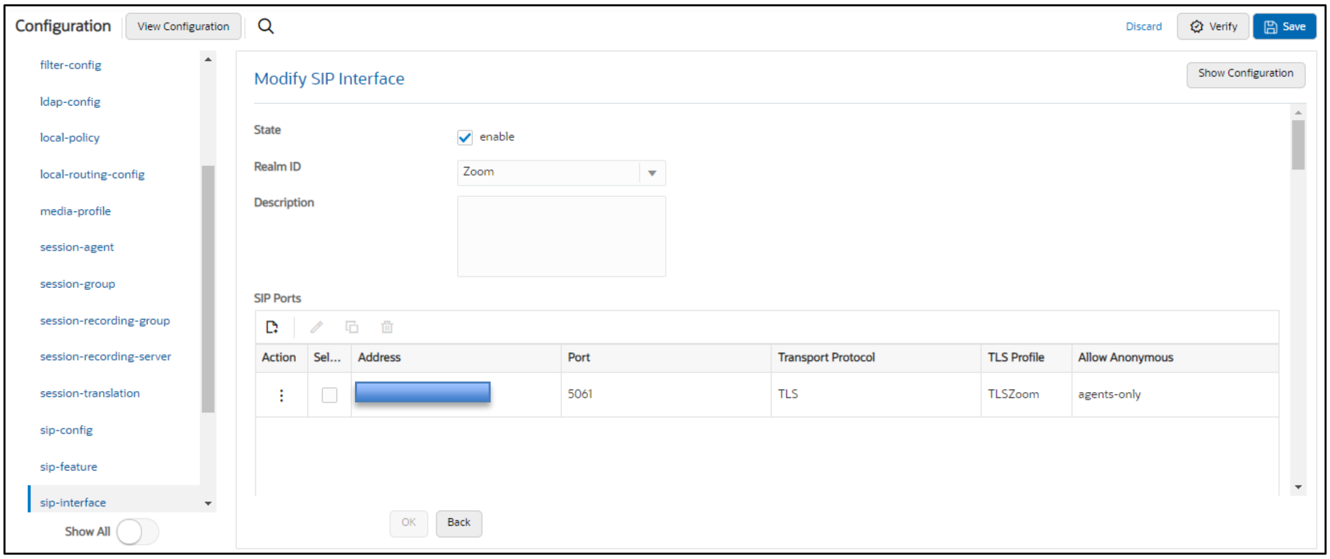
7.9. Configure SIP Interfaces

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

Please Configure sip-interface for the Genesys Cloud 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.

7.9.1 Sip-Interface for Zoom Phone



Modify SIP Interface

State ☑ enable

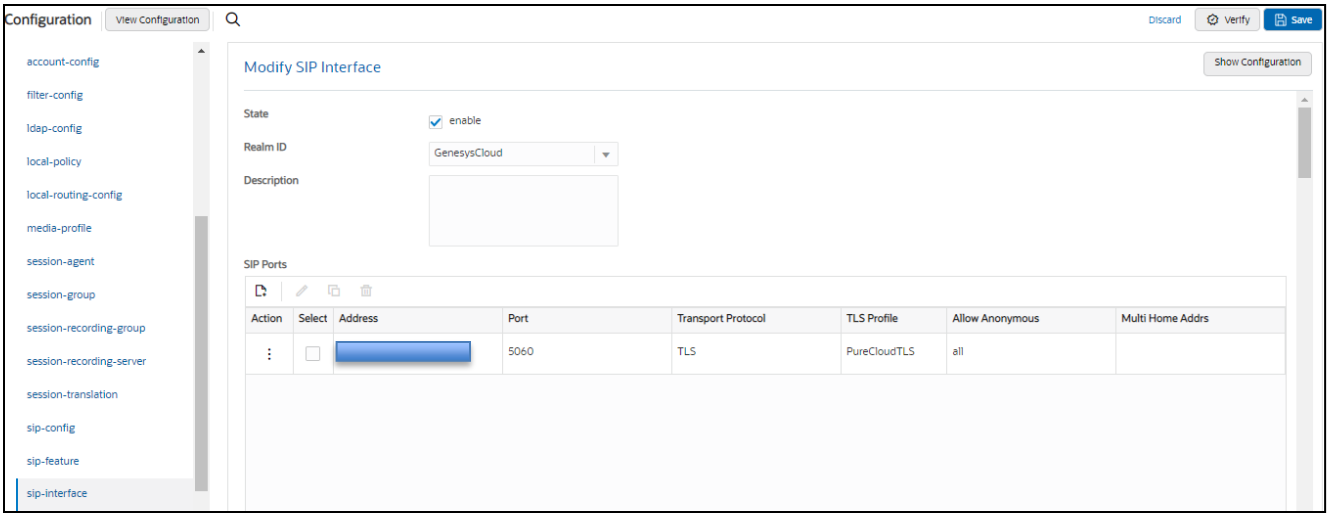
Realm ID Zoom

Description

SIP Ports

Action	Sel...	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous
⋮	□	[redacted]	5061	TLS	TLSZoom	agents-only

7.9.2 Sip-interface for Genesys BYOC Cloud



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.

7.10. Configure session-agent

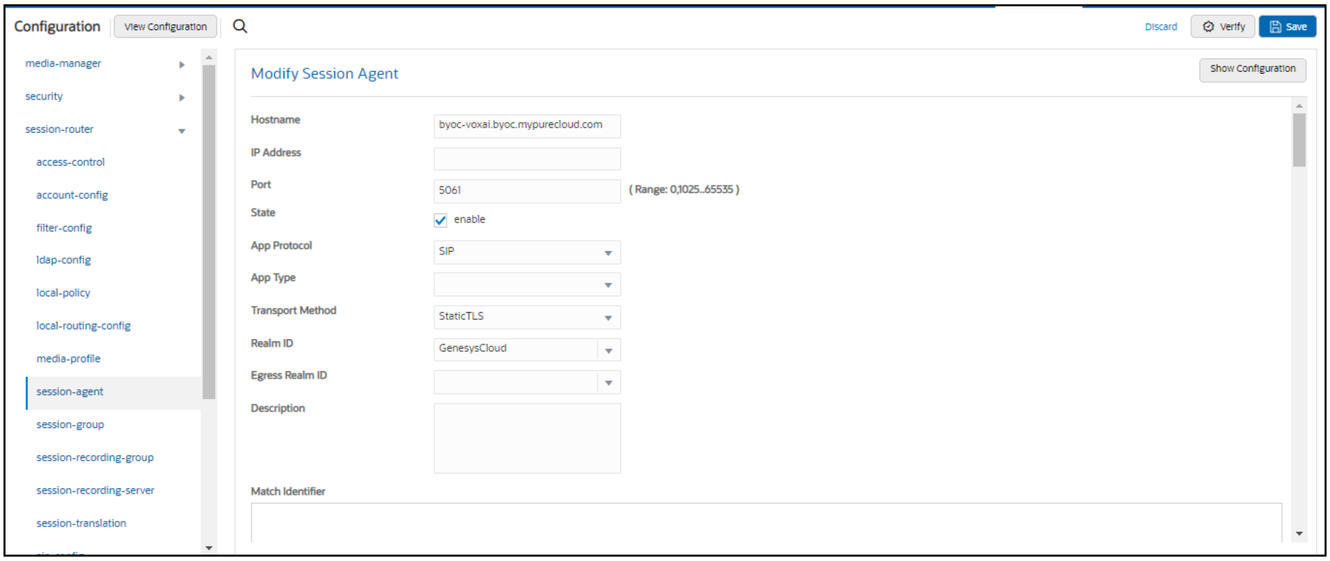
Session-agents are config elements, which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

Navigate to session-router->Session-Agent

Configure the session-agents for the Genesys BYOC Cloud

- Host name to “byoc-voxai.byoc.mypurecloud.com”
- port to 5061

- realm-id – needs to match the realm created for the Genesys BYOC 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

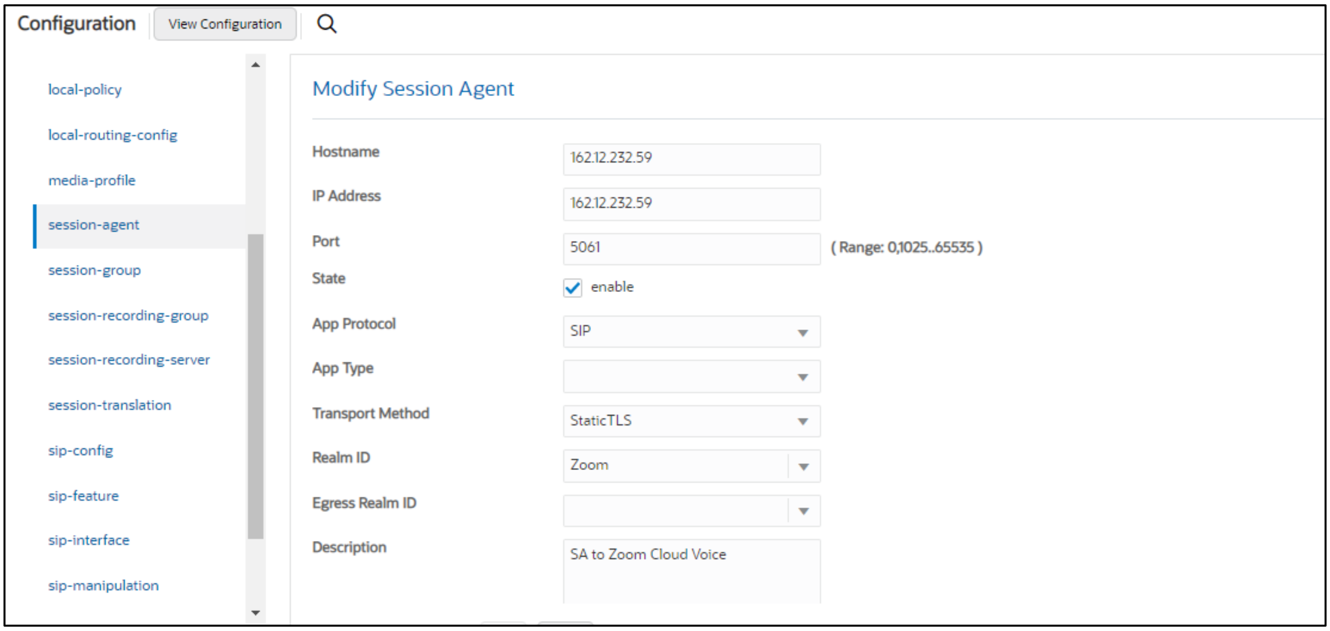
Egress Realm ID:

Description:

Match Identifier:

Configure the session-agents for Zoom.

Config parameter	Zoom 1	Zoom 2
Hostname	162.12.232.59	162.12.233.59
IP Address	162.12.232.59	162.12.233.59
Port	5061	5061
Transport method	StaticTLS	StaticTLS
Realm ID	Zoom	Zoom
Ping Method	OPTIONS	OPTIONS
Ping Interval	30	30
Ping Response	Enabled	Enabled



Modify Session Agent

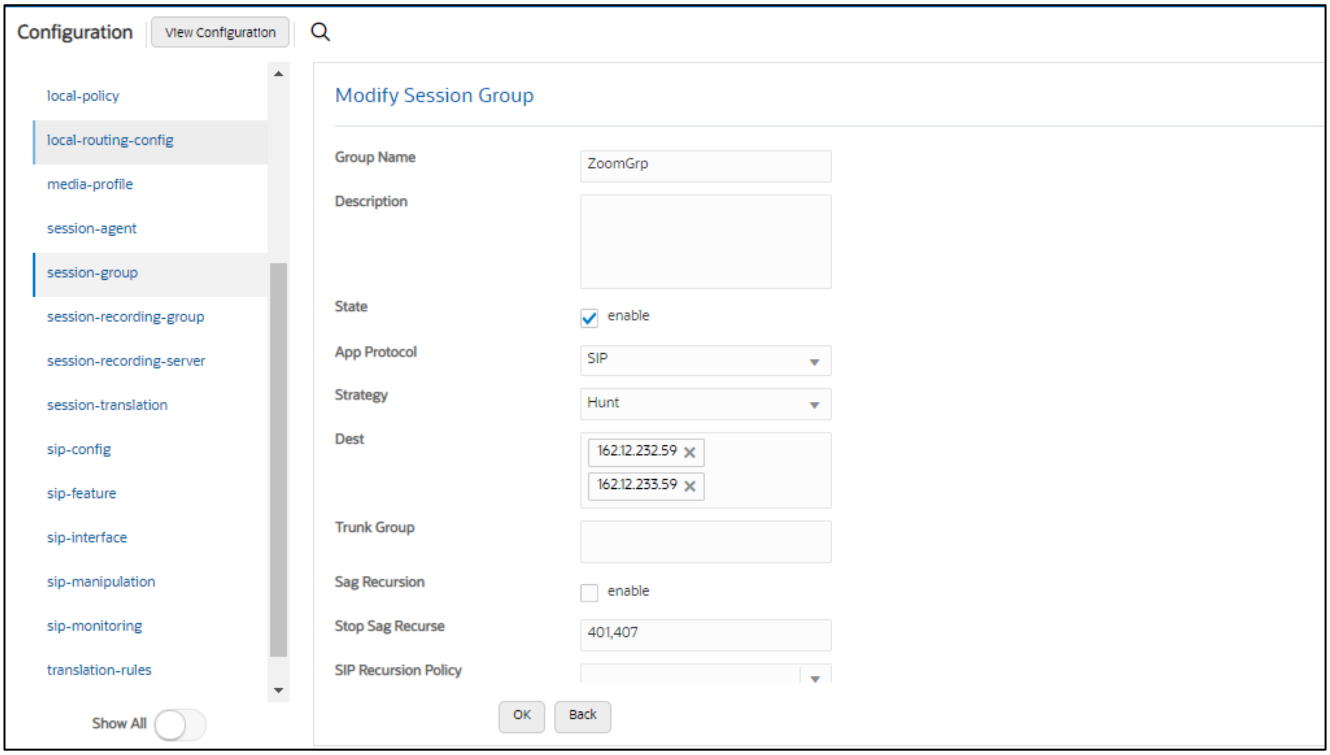
Hostname	162.12.232.59
IP Address	162.12.232.59
Port	5061 (Range: 0,1025..65535)
State	☑ enable
App Protocol	SIP
App Type	
Transport Method	StaticTLS
Realm ID	Zoom
Egress Realm ID	
Description	SA to Zoom Cloud Voice

Follow above step to create 1 more session-agent for Other Zoom Session-Agent 162.12.233.59

Note: The Session-Agent Ips/FQDNs might change depending upon your location and the BYOC Ips provided to you by Zoom. Please modify the configuration according to your specific need.

7.11. 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 Zoom Session Agents



Modify Session Group

Group Name: ZoomGrp

Description:

State: ☑ enable

App Protocol: SIP

Strategy: Hunt

Dest: 162.12.232.59, 162.12.233.59

Trunk Group:

Sag Recursion: ☐ enable

Stop Sag Recurse: 401,407

SIP Recursion Policy:

7.12. 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 Genesys Cloud to Zoom Phone –

Genesys BYOC Cloud → Oracle SBC → Carrier Trunk → Oracle SBC → Zoom Phone

Inbound calls from Zoom Phone to Genesys Cloud -

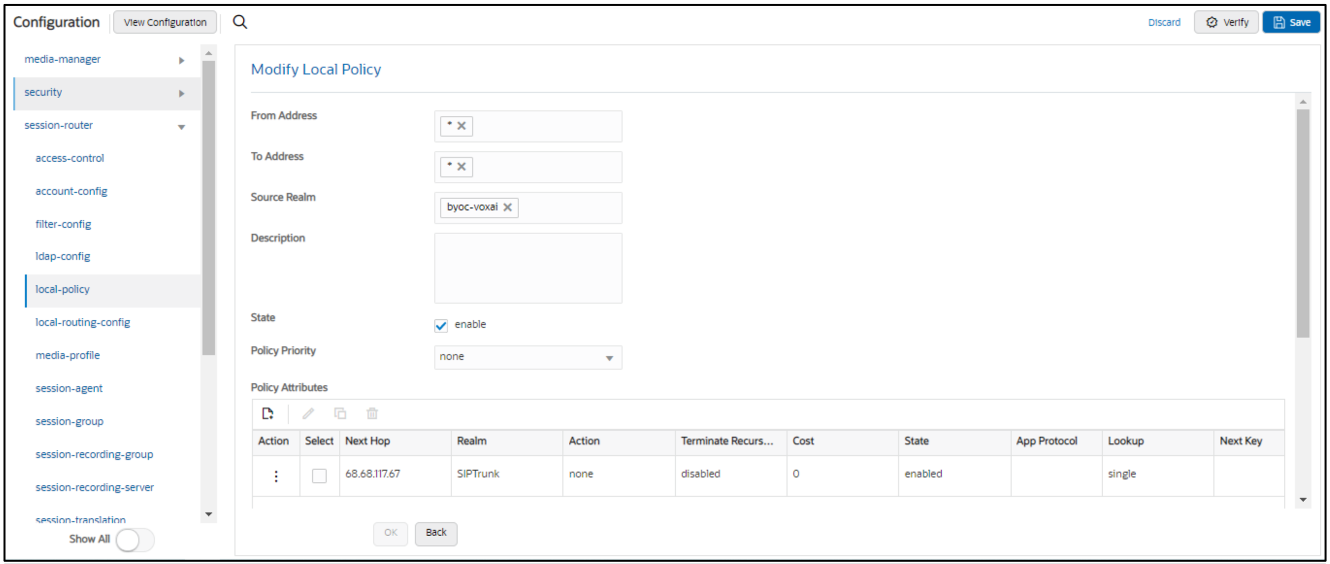
Zoom Phone→ Oracle SBC → Carrier Trunk → Oracle SBC → Genesys BYOC Cloud

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 BYOC Cloud and Twilio SIP Trunk Application Note can be found here –

https://www.oracle.com/a/otn/docs/oracle-sbc-with-genesys-cloud-cx-and-twillio-sip-trunkv0.3.pdf

Following **local-policy routes the calls from the Genesys BYOC Cloud** to Carrier and then the calls are routed from Carrier to Zoom Phone.



Modify Local Policy

From Address: * ✕

To Address: * ✕

Source Realm: byoc-voxai ✕

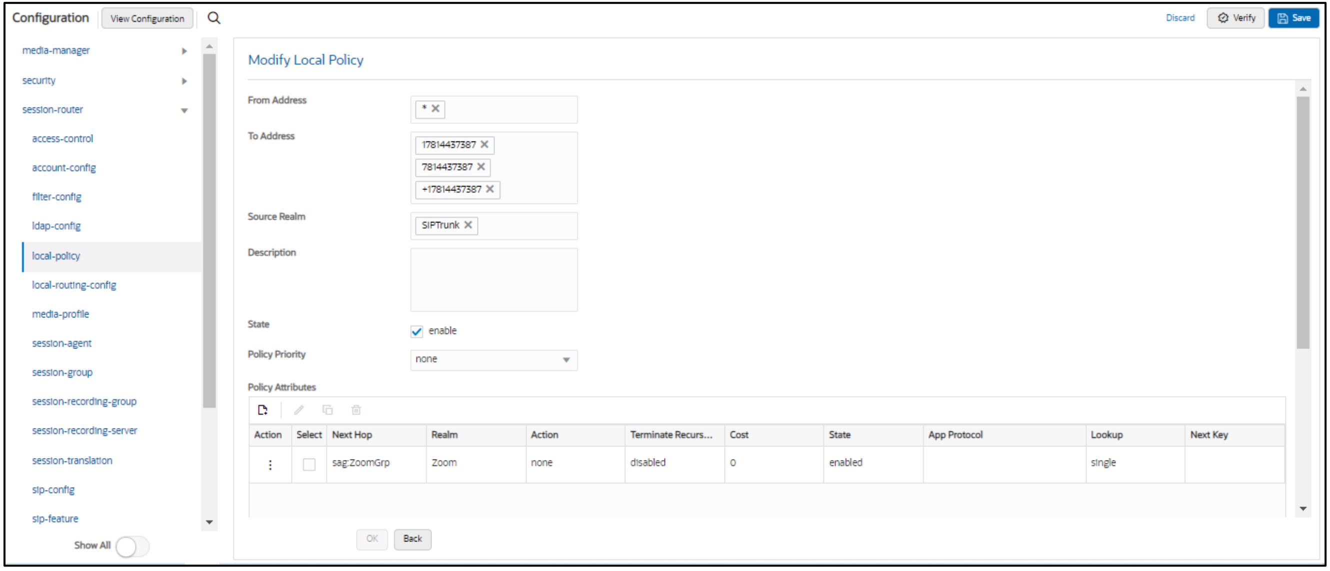
Description:

State: ☑ enable

Policy Priority: none

Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Recurs...	Cost	State	App Protocol	Lookup	Next Key
⋮	□	68.68.117.67	SIPTrunk	none	disabled	0	enabled		single	



Modify Local Policy

From Address: * ✕

To Address: 17814437387 ✕ 7814437387 ✕ +17814437387 ✕

Source Realm: SIPTrunk ✕

Description:

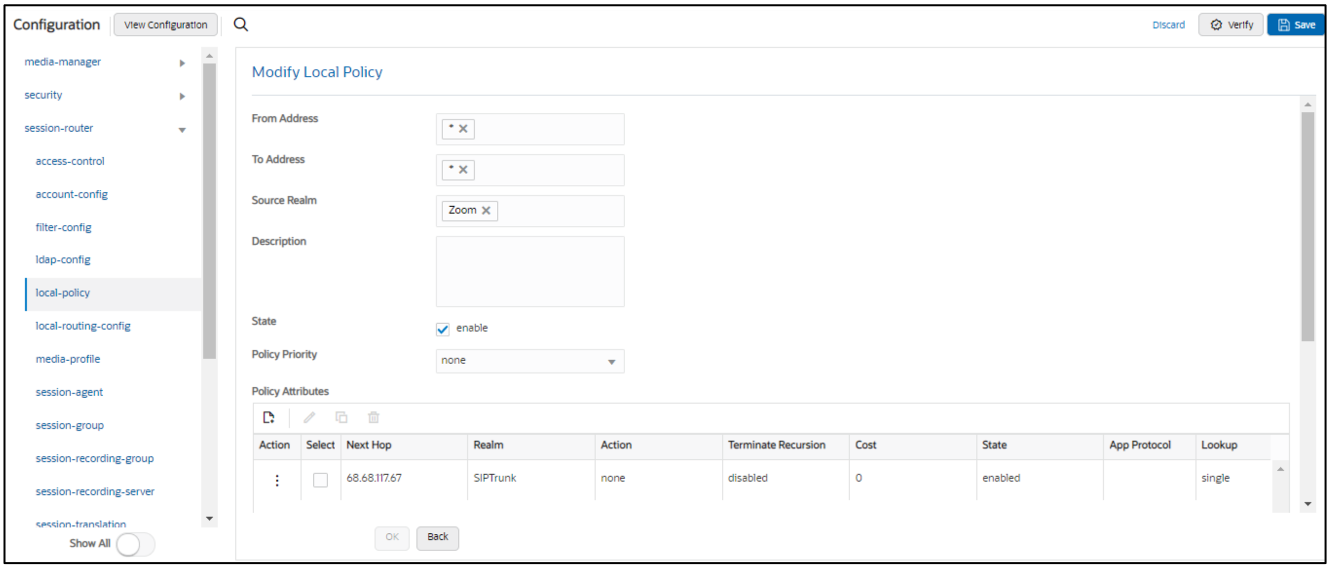
State: ☑ enable

Policy Priority: none

Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Recurs...	Cost	State	App Protocol	Lookup	Next Key
⋮	□	sag:ZoomGrp	Zoom	none	disabled	0	enabled		single	

Following **local-policy routes the calls from the Zoom Phone** to Carrier and then the calls are routed from Carrier to Genesys BYOC Cloud.



Modify Local Policy

From Address: *

To Address: *

Source Realm: Zoom

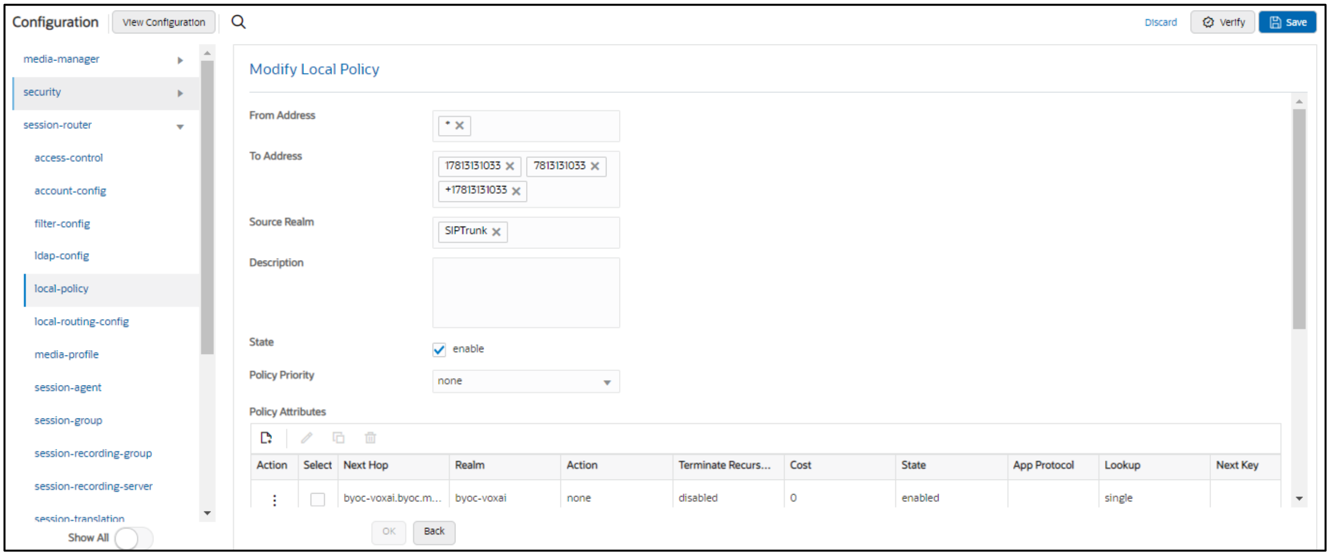
Description:

State: ☑ enable

Policy Priority: none

Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup
⋮	□	68.68.117.67	SIPTrunk	none	disabled	0	enabled		single



Modify Local Policy

From Address: *

To Address: 17813131033, 7813131033, +17813131033

Source Realm: SIPTrunk

Description:

State: ☑ enable

Policy Priority: none

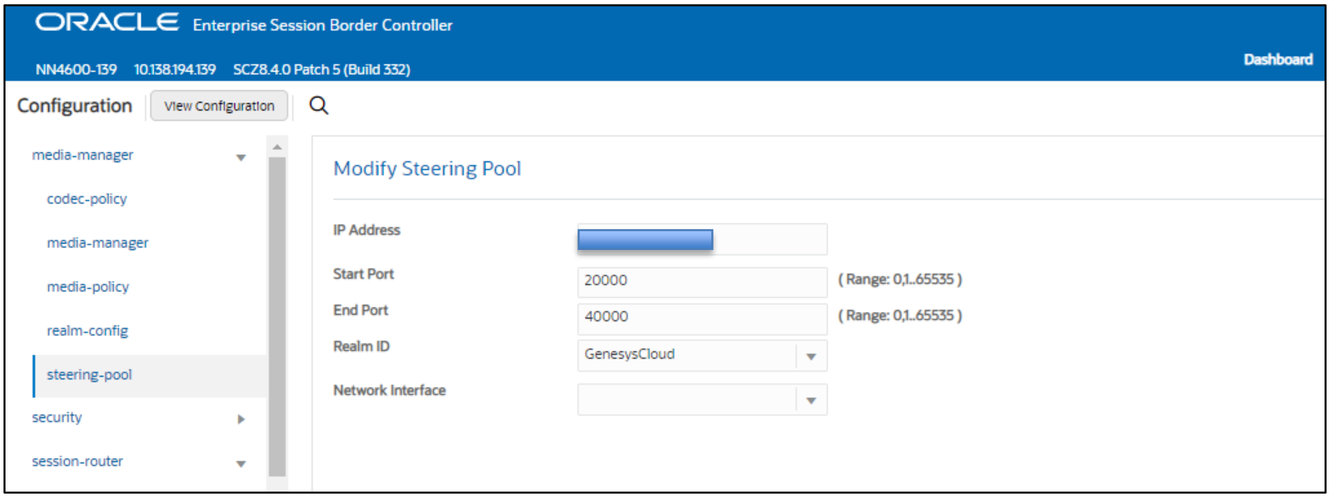
Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Recurs...	Cost	State	App Protocol	Lookup	Next Key
⋮	□	byoc-voxai.byoc.m...	byoc-voxai	none	disabled	0	enabled		single	

7.13. Configure steering-pool

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

Genesys Cloud Steering pool.



Modify Steering Pool

IP Address [redacted]

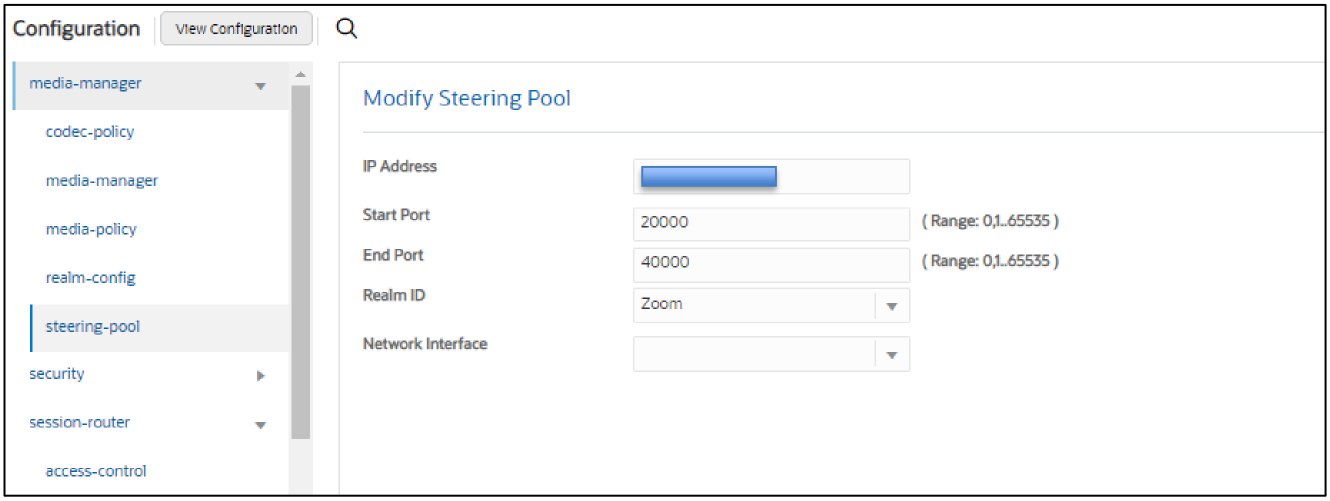
Start Port 20000 (Range: 0,1..65535)

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

Realm ID GenesysCloud

Network Interface

Zoom Phone Steering Pool



Modify Steering Pool

IP Address [redacted]

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

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

Realm ID Zoom

Network Interface

7.14. Configure additional Parameters

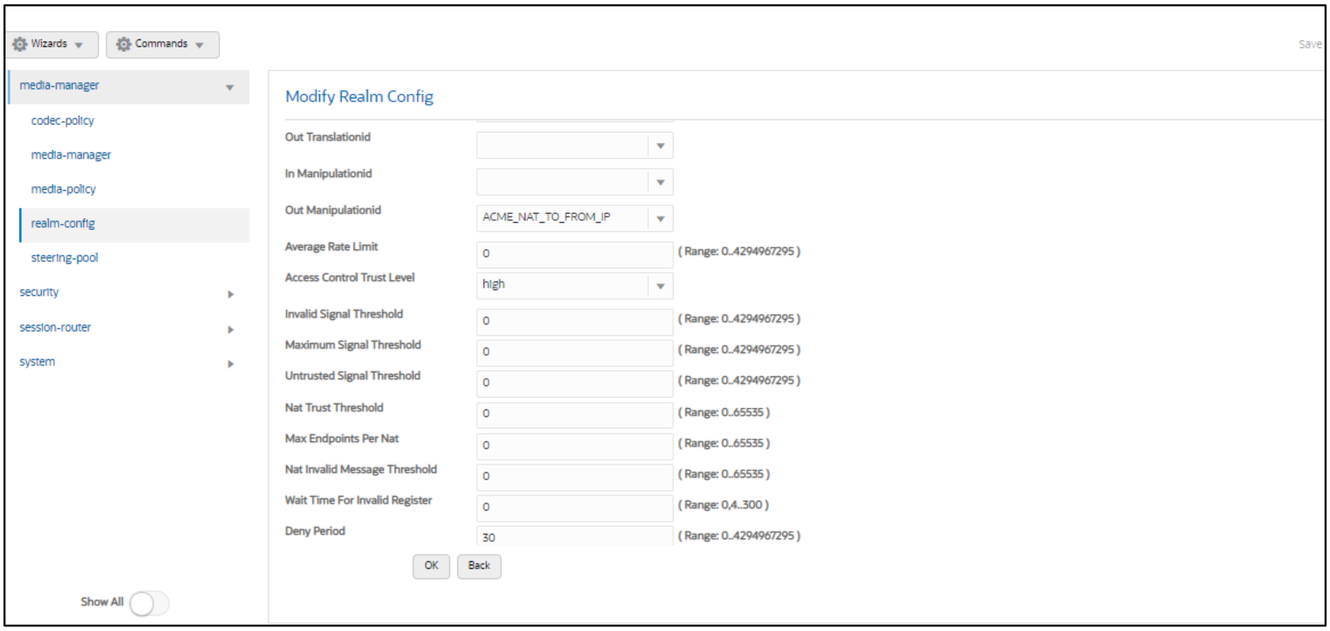
7.14.1 SIP Manipulations

For calls to be presented to Zoom Phone from the Oracle SBC, the Oracle SBC requires alterations to the SIP signaling natively created. To do this, we should use the prebuilt HMR ACME_NAT_TO_FROM_IP

The following SIP manipulation is applied as the out-manipulationId to the sip-interface created for Zoom and modifies packets generated by the Oracle SBC to Zoom Phone:

The manipulation performs the following modifications to SIP packets

1. Changes the host portion of From address with the SBC sip-interface IP Address.
2. Changes the host portion of To Header with Zoom IP Address.

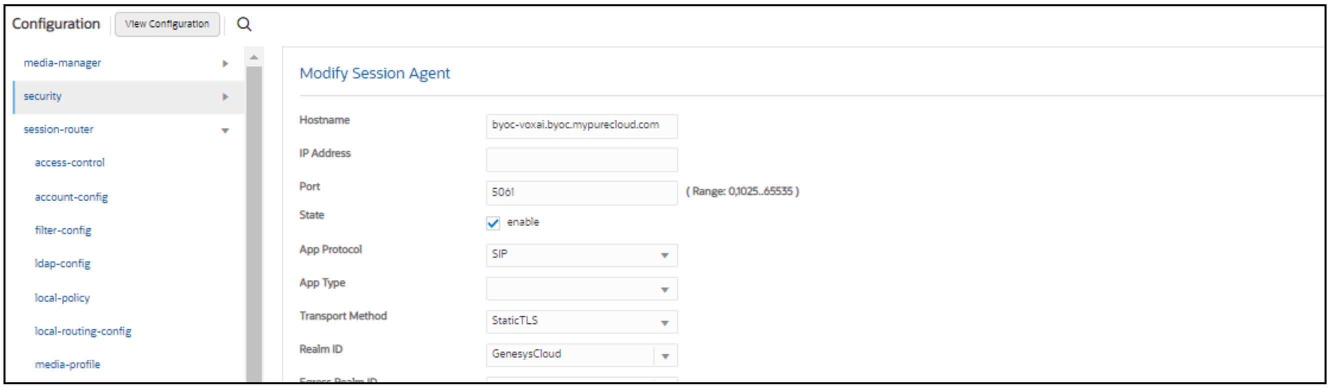


Modify Realm Config

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

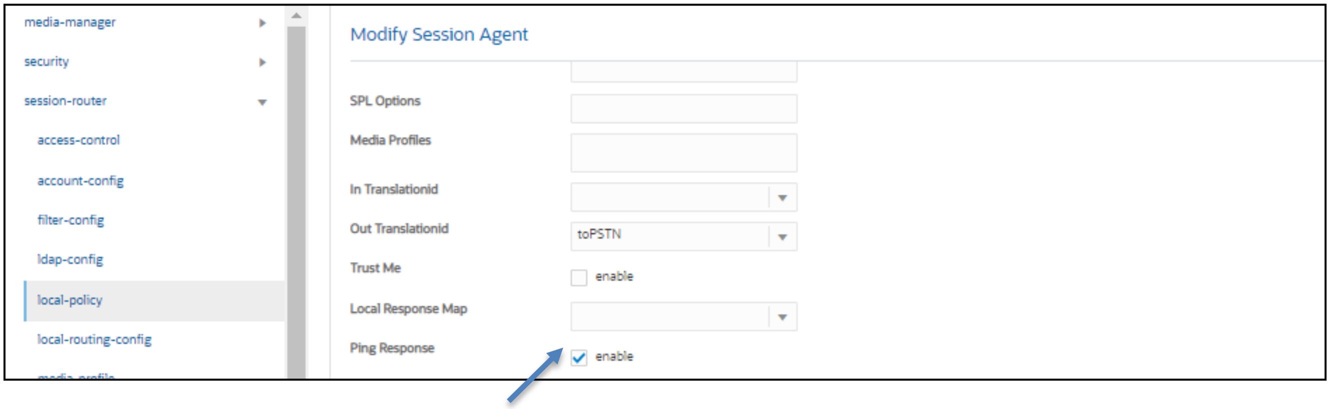
7.14.2 Enable Ping-response

The option is found under the **Session agent** configuration element and will be enabled on all session agents configured for Zoom Phone and Genesys BYOC Cloud .
Below is an example of the parameter **Ping response** enabled on Genesys Cloud Session-Agent. Similarly, the parameter should be enabled for other Zoom Phone 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

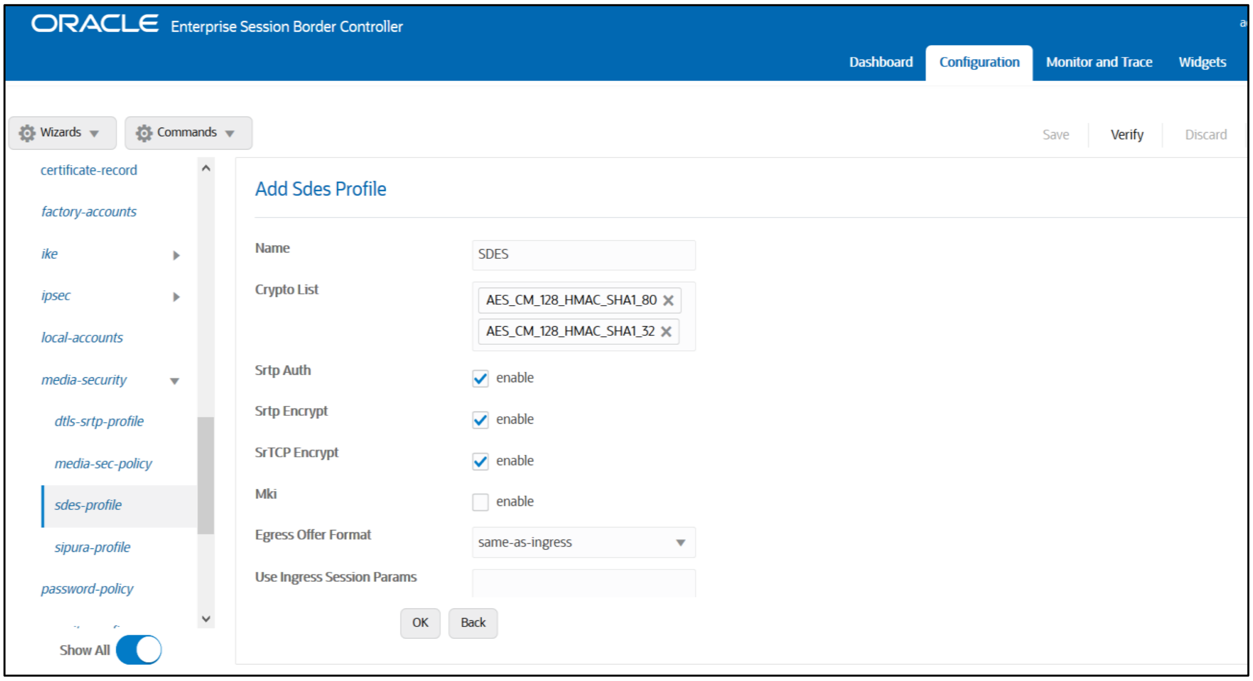
SPL Options	
Media Profiles	
In Translationid	
Out Translationid	toPSTN
Trust Me	□ enable
Local Response Map	
Ping Response	☑ enable

7.15. Media Security Configuration.

This section outlines how to configure support for media security between the ORACLE SBC Zoom Cloud Voice and Genesys BYOC Cloud.

7.15.1 Configure sdes profile

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

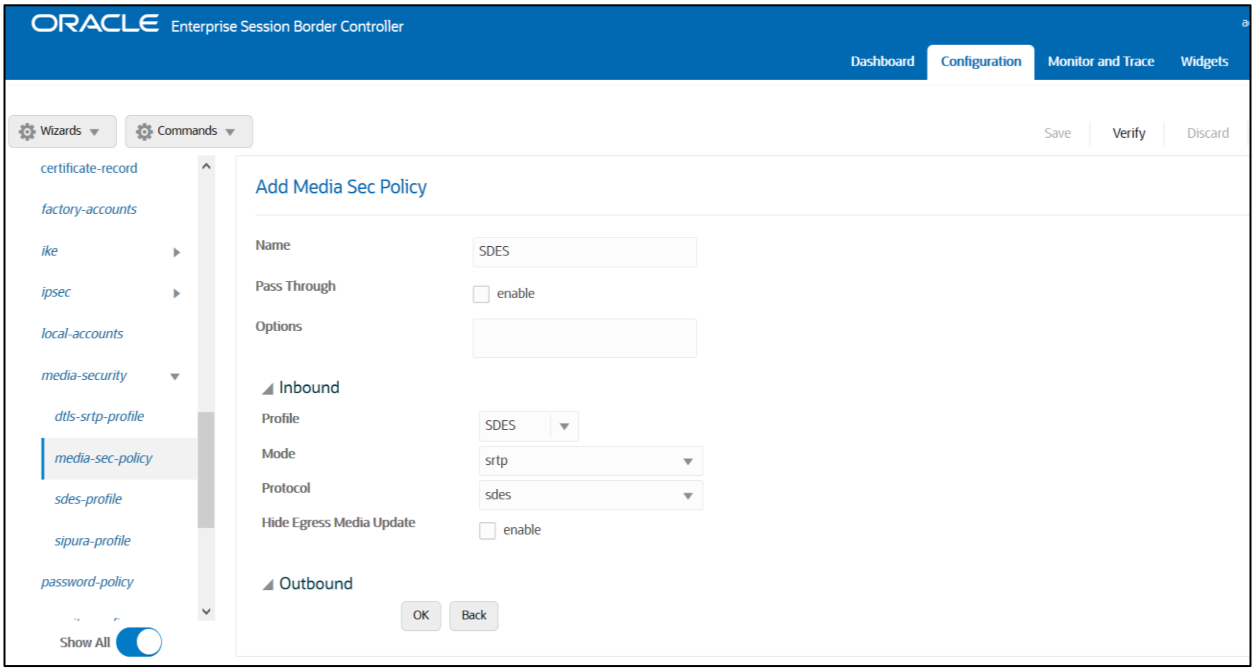
Egress Offer Format: same-as-ingress

Use Ingress Session Params:

7.15.2. Configure Media Security Profile

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 Genesys Cloud and Zoom Phone Realm.



Add Media Sec Policy

Name: SDES

Pass Through: □ enable

Options:

◢ Inbound

Profile: SDES

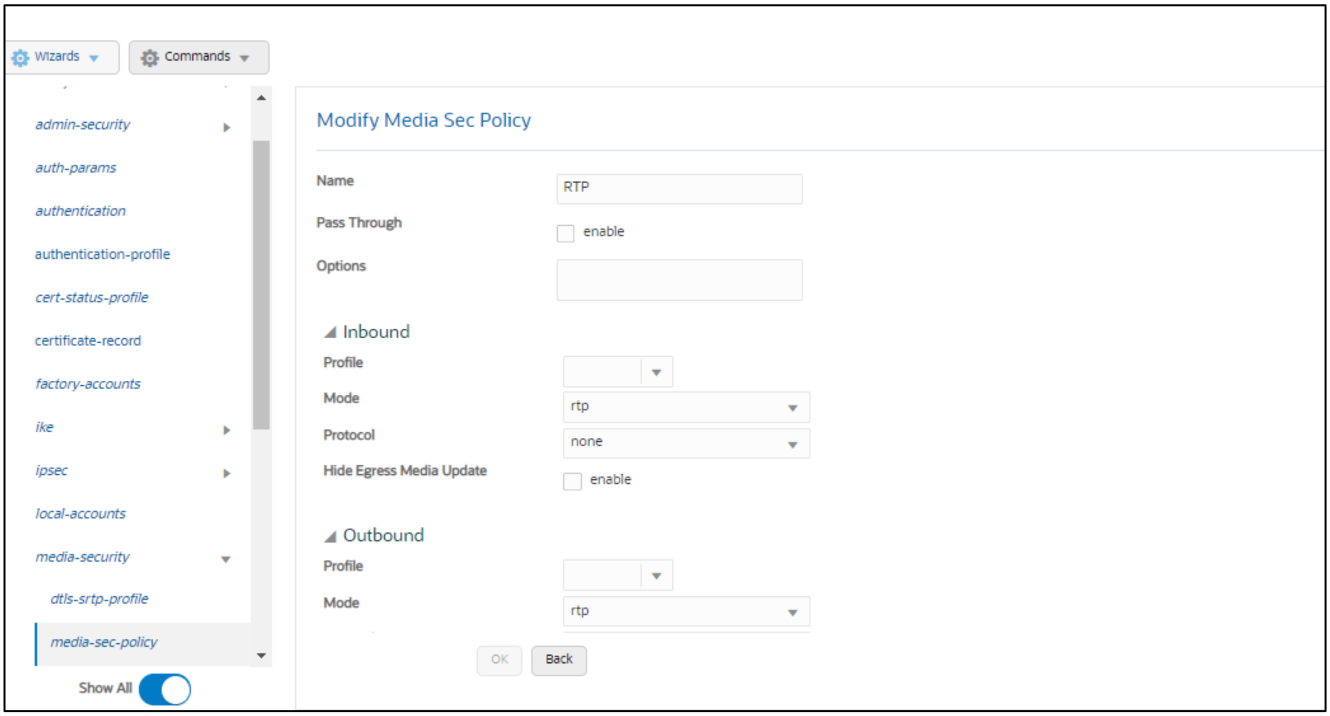
Mode: srtp

Protocol: sdes

Hide Egress Media Update: □ enable

◢ Outbound

Note- Both Zoom Phone and Genesys BYOC Cloud 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

7.16 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

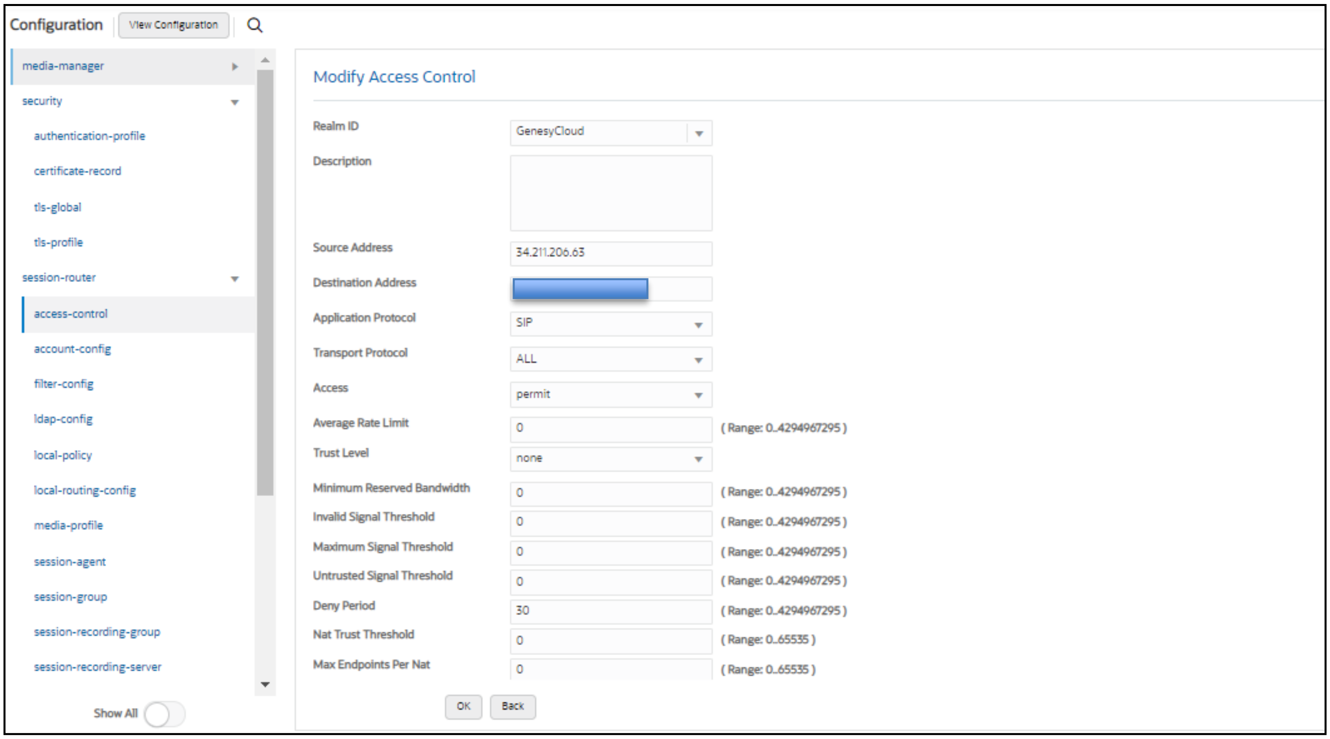
Please use the example below to configure access controls in your environment for both BYOC Cloud IP's, as well as SIP Trunk IP's (if applicable).

The IP for NAM region are -

IP Addresses	Load Balancer DNS Names
52.203.12.137	lb01.voice.use1.pure.cloud
54.82.241.192	lb02.voice.use1.pure.cloud
54.82.241.68	lb03.voice.use1.pure.cloud
54.82.188.43	lb04.voice.use1.pure.cloud

Complete IP details can be found below-
https://help.genesys.cloud/articles/byoc-cloud-public-sip-ip-addresses/

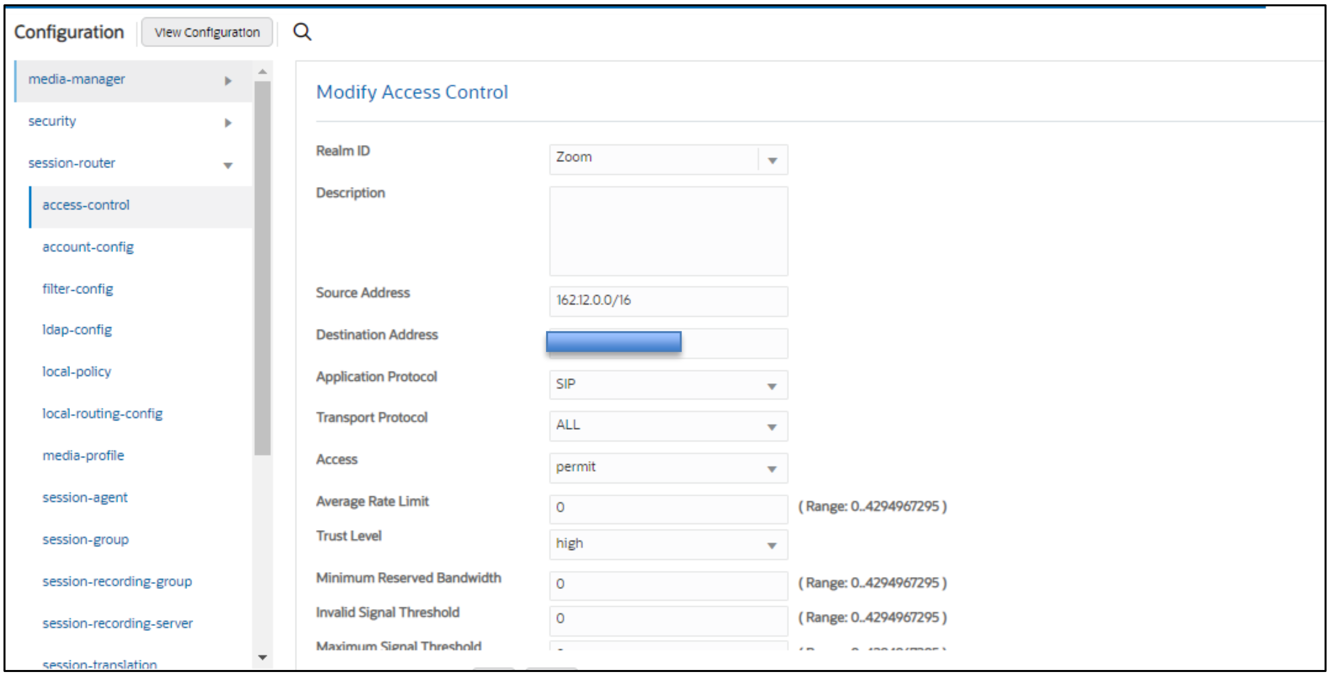
Configure access-control for each IP BYOC Cloud IP Address or Subnet as shown in the below example.



Modify Access Control

Realm ID	GenesyCloud	
Description		
Source Address	34.211.206.63	
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 Zoom Phone IP Addresses as shown in the below example.



Modify Access Control

Realm ID	Zoom	
Description		
Source Address	162.12.0.0/16	
Destination Address	[redacted]	
Application Protocol	SIP	
Transport Protocol	ALL	
Access	permit	
Average Rate Limit	0	(Range: 0..4294967295)
Trust Level	high	
Minimum Reserved Bandwidth	0	(Range: 0..4294967295)
Invalid Signal Threshold	0	(Range: 0..4294967295)
Maximum Signal Threshold		

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

7.17 SBC Behind NAT SPL configuration

This configuration is needed when your SBC is behind a NAT device. This is configured to avoid loss in voice path and SIP signaling.

The Support for SBC Behind NAT SPL plug-in changes information in SIP messages to hide the end point located inside the private network. The specific information that the Support for SBC Behind NAT SPL plug-in changes depends on the direction of the call.

For example, from the NAT device to the SBC or from the SBC to the NAT device.

Configure the Support for SBC Behind NAT SPL plug-in for each SIP interface that is connected to a NAT device. One public-private address pair is required for each SIP interface that uses the SPL plug-in, as follows.

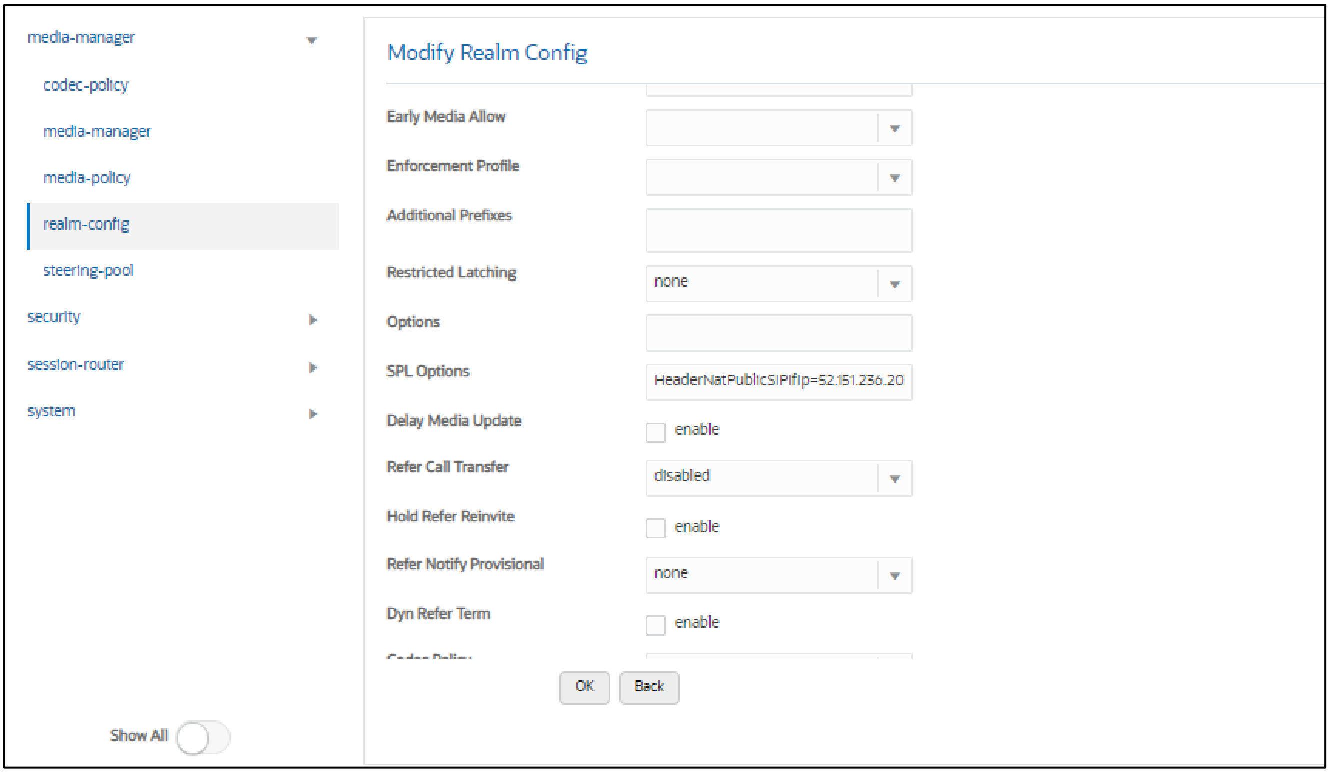
- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

Here is an example configuration with SBC Behind NAT SPL config. The SPL is applied to the Zoom side SIP interface.

To configure SBC Behind NAT SPL Plug in, go to session-router->SIP-interface->spl-options and input the following value, save, and activate.

HeaderNatPublicSIPIfIp=52.151.236.203,HeaderNatPrivateSIPIfIp=10.0.4.4

Here HeaderNatPublicSIPIfIp is the public interface ip and HeaderNatPrivateSIPIfIp is the private ip.



Modify Realm Config

Early Media Allow	
Enforcement Profile	
Additional Prefixes	
Restricted Latching	none
Options	
SPL Options	HeaderNatPublicSIPIfIp=52.151.236.20
Delay Media Update	□ enable
Refer Call Transfer	disabled
Hold Refer Reinvite	□ enable
Refer Notify Provisional	none
Dyn Refer Term	□ enable

This configuration would be applied to each SIP Interface in the ORACLE SBC configuration that was deployed behind a Nat Device.

7.18 Caveat -OPUS Transcoding

Opus is an audio codec developed by the IETF that supports constant and variable bitrate encoding from 6 kbit/s to 510 kbit/s and sampling rates from 8 kHz (with 4 kHz bandwidth) to 48 kHz (with 20 kHz bandwidth, where the entire hearing range of the human auditory system can be reproduced). It incorporates technology from both Skype's speech-oriented SILK codec and Xiph.Org's low-latency CELT codec. This feature adds the Opus codec as well as support for transrating, transcoding, and pooled transcoding. Opus can be adjusted seamlessly between high and low bit rates, and transitions internally between linear predictive coding at lower bit rates and transform coding at higher bit rates (as well as a hybrid for a short overlap). Opus has a very low algorithmic delay (26.5 ms by default), which is a necessity for use as part of a low audio latency communication link, which can permit natural conversation, networked music performances, or lip sync at live events. Opus permits trading-off quality or bit rate to achieve an even smaller algorithmic delay, down to 5 ms. Its delay is very low compared to well over 100 ms for popular music formats such as MP3, Ogg Vorbis, and HE-AAC; yet Opus performs very competitively with these formats in terms of quality across bit rates.

Zoom Phone fully support the use of OPUS, but advertises a static value of 40000 for max average bit rate Although the range for maxaveragebitrate is 6000 to 51000, only bit rates of 6000 to 30000 bps are transcodable by the DSP's on the Oracle SBC. A media profile configured with a value for maxaveragebitrate greater than 30000 is not transcodable and cannot be added on egress in the codec-policy element.

The Oracle SBC will however support the entire range of of maxaveragebitrate if negotiated between the parties of each call flow.

8. 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 BYOC Cloud. We will choose a Generic SIP Trunk on the other Side for Carrier Connectivity. We also have configuration Assistant for Zoom Phone related to Zoom Phone configuration. Please follow the latest Zoom Phone Application Note to get instructions on configuring Zoom Phone 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 Genesys Cloud 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

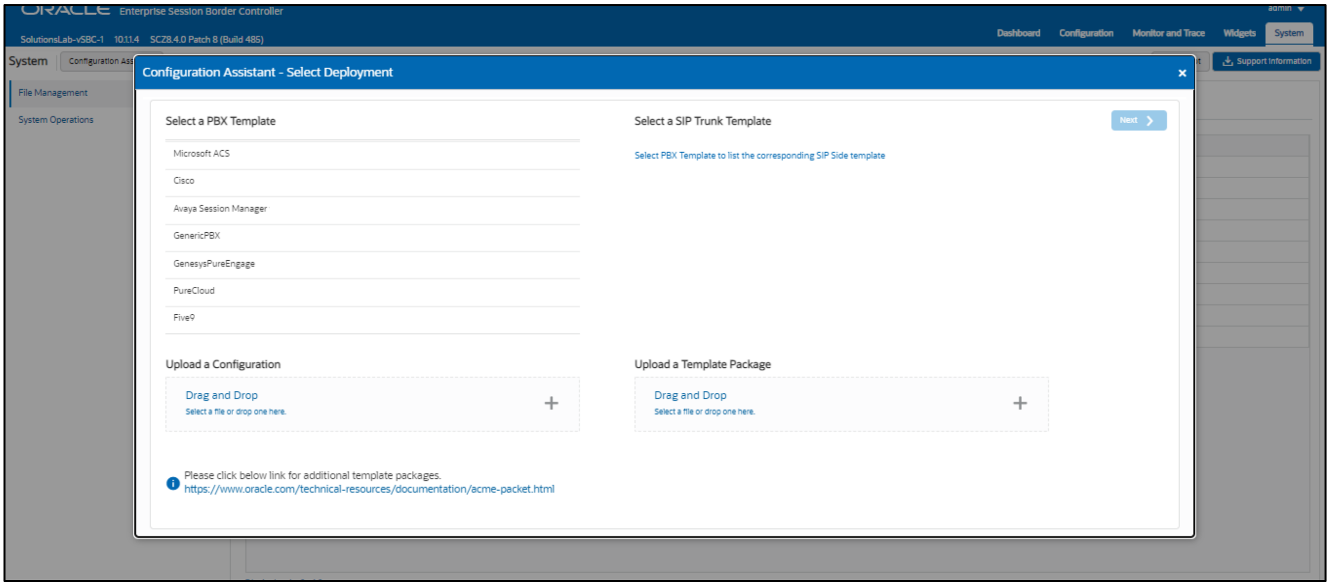
The Oracle SBC WebGui can be accessed by entering the following in your web browser.
http(s)://<SBC Management IP>.

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

Genesys Cloud 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

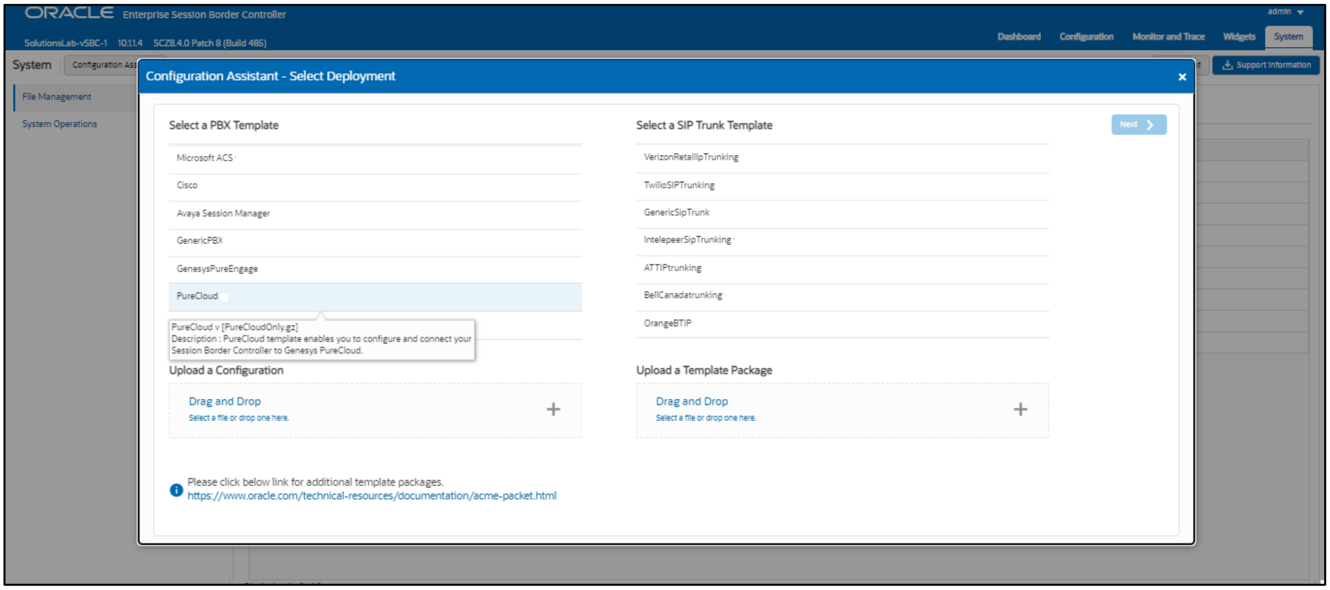
Drag and Drop
Select a file or drop one here.

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 Genesys Cloud 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

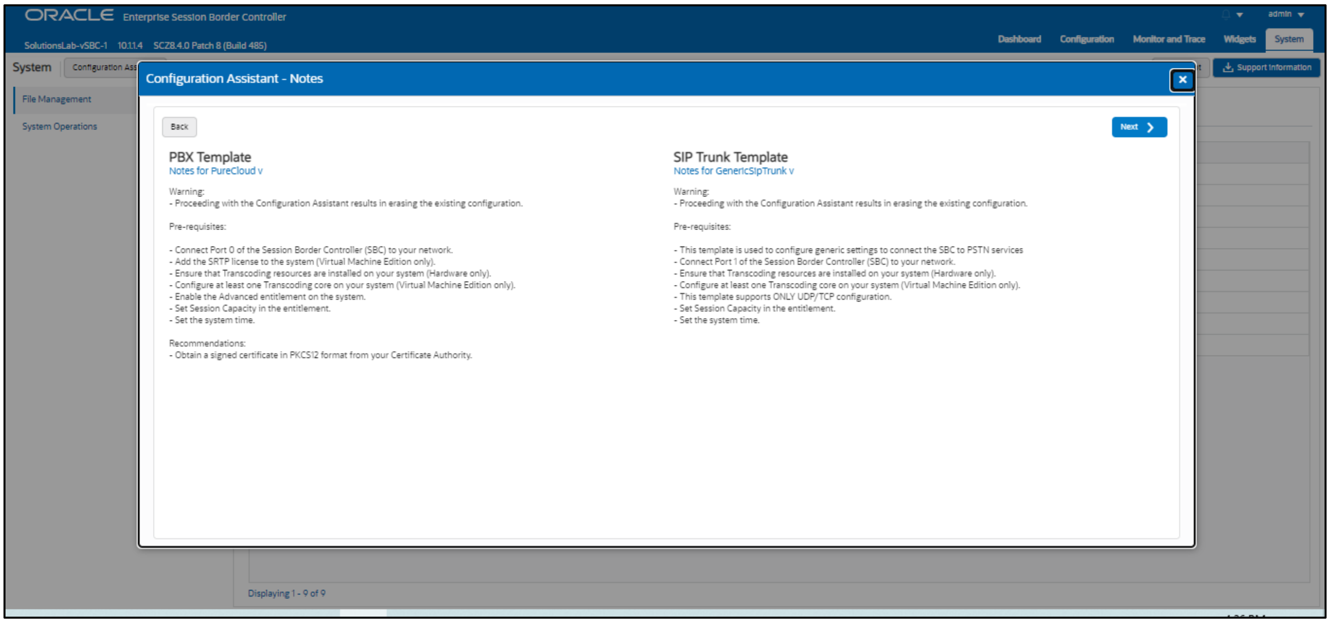
Drag and Drop
Select a file or drop one here.

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:



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.

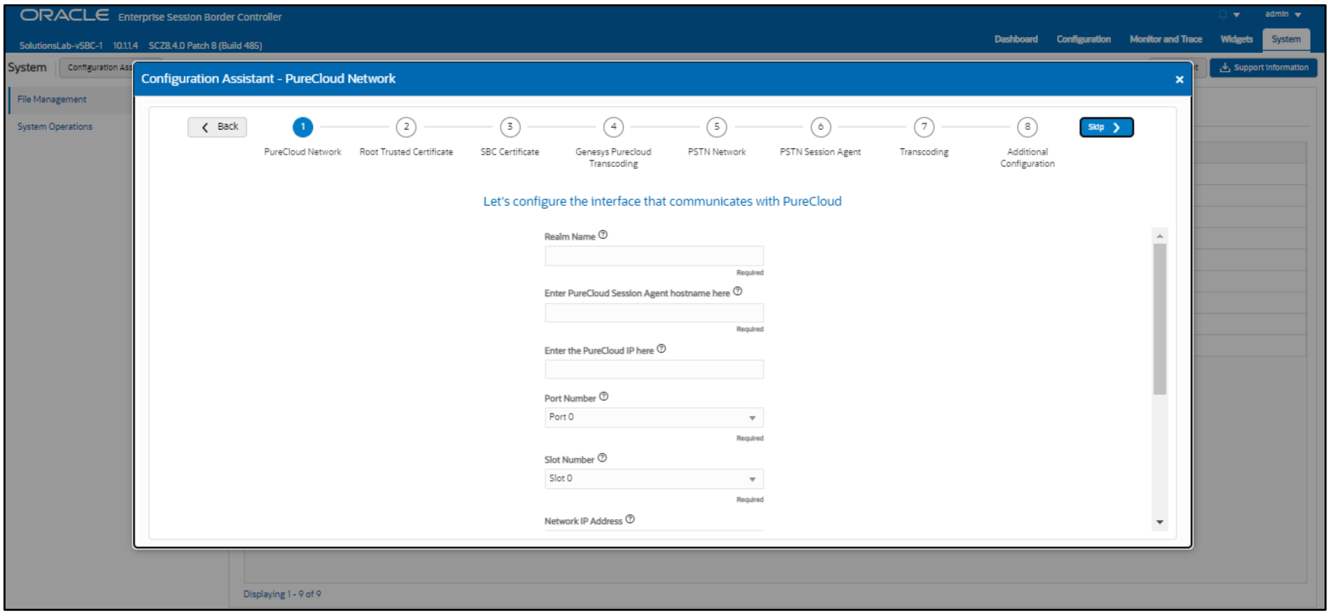
Clicking “Next” on the Notes page triggers the configuration assistant to do a system check. This ensures that all of the system requirements for the platform and sip trunk you have selected have been met before proceeding to configuration pages. If they have not been met, you will be greeted by a page 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- Genesys Cloud Network

Page 1 of the template is where you will configure the network information to connect to Genesys Cloud 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)

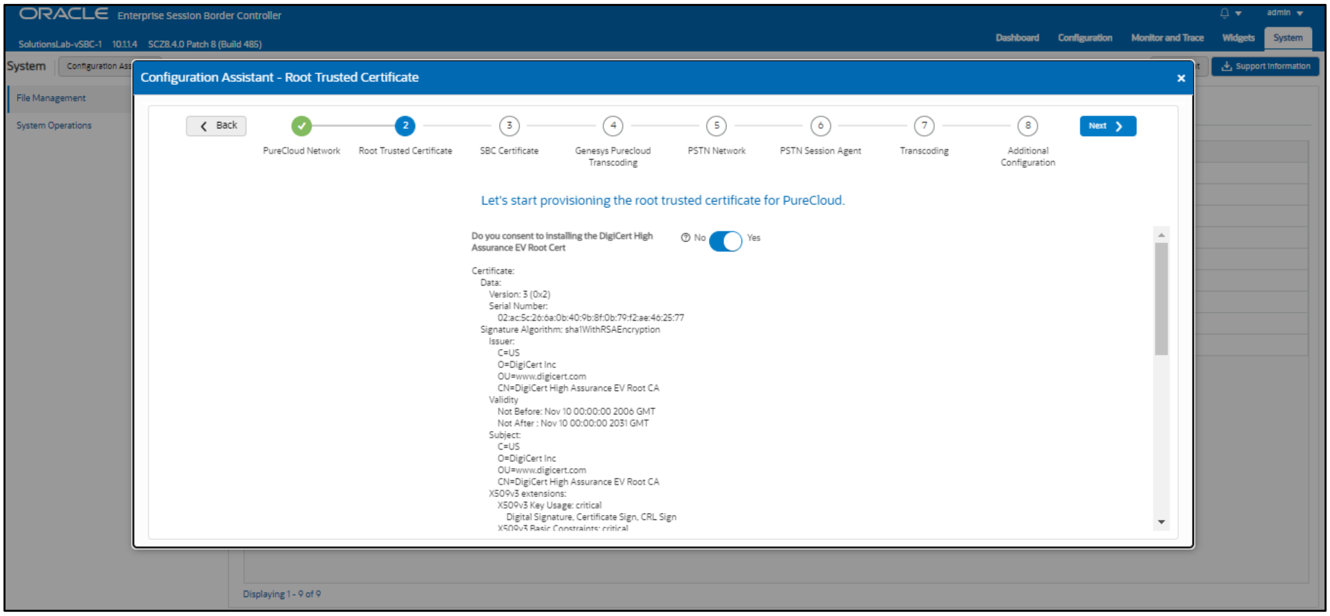
Slot Number: Slot 0 (Required)

Network IP Address

Page 2 - Import DigiCert Trusted CA Certificate for BYOC Cloud

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

Importing the Genesys Cloud Root CA certs is enabled by default.



Configuration Assistant - Root Trusted Certificate

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

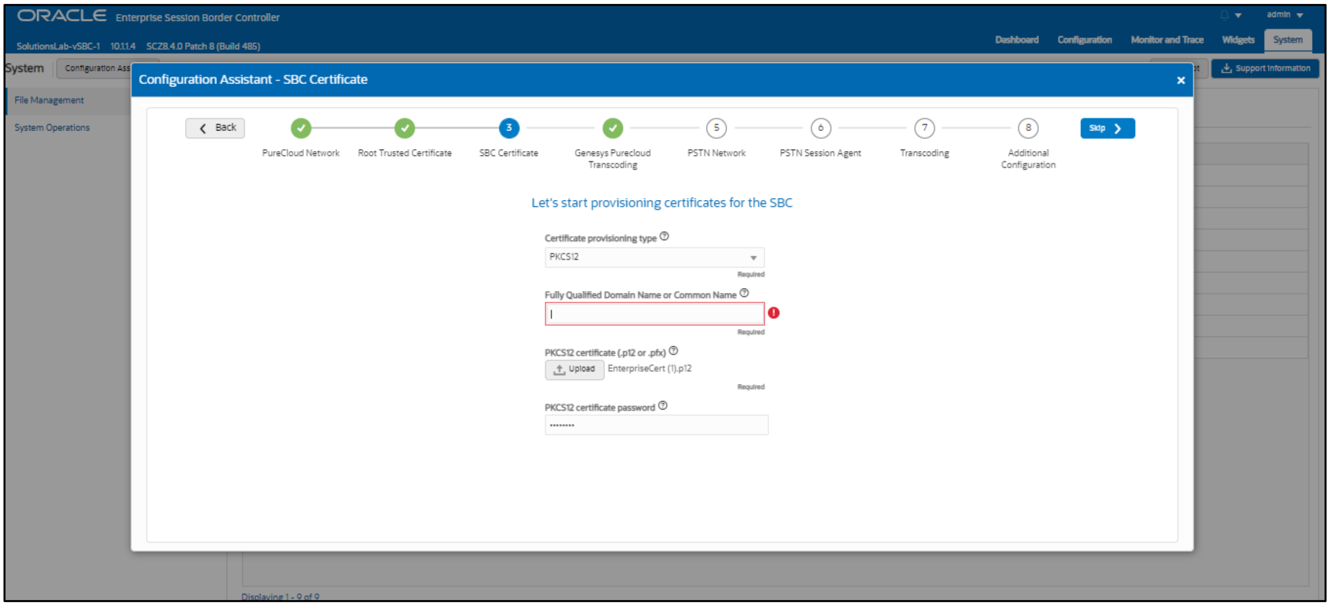
Do you consent to installing the DigiCert High Assurance EV Root Cert: No [✓ Yes]

```
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 Genesys Cloud 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 Genesys Cloud Supported CA Vendors, and enter the certificates password.



Configuration Assistant - SBC Certificate

Let's start provisioning certificates for the SBC

Certificate provisioning type: PKCS12 (Required)

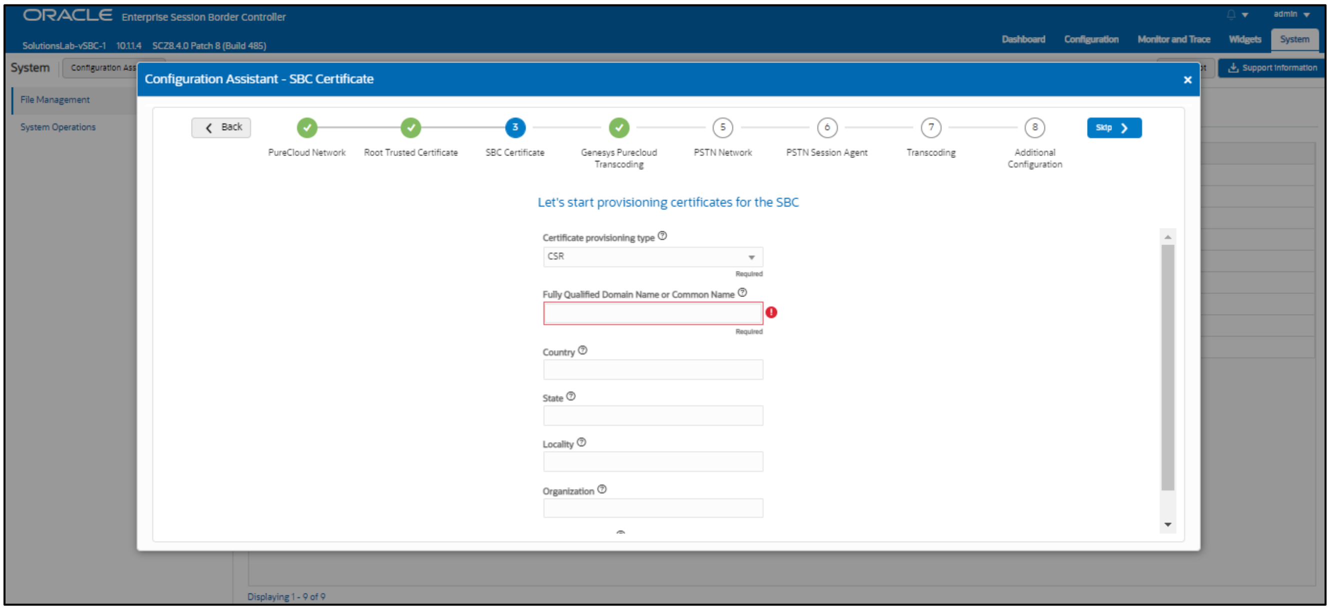
Fully Qualified Domain Name or Common Name: (Required)

PKCS12 certificate (.p12 or .pfx): Upload 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 Genesys Cloud 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

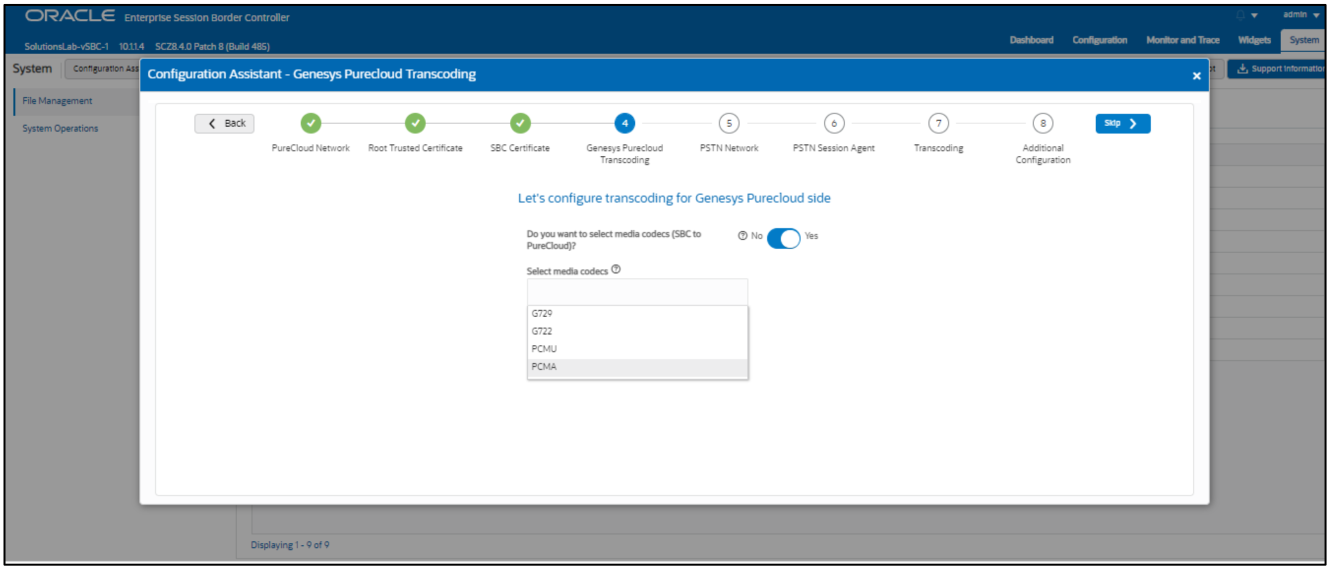
Locality

Organization

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

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 BYOC Cloud. 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

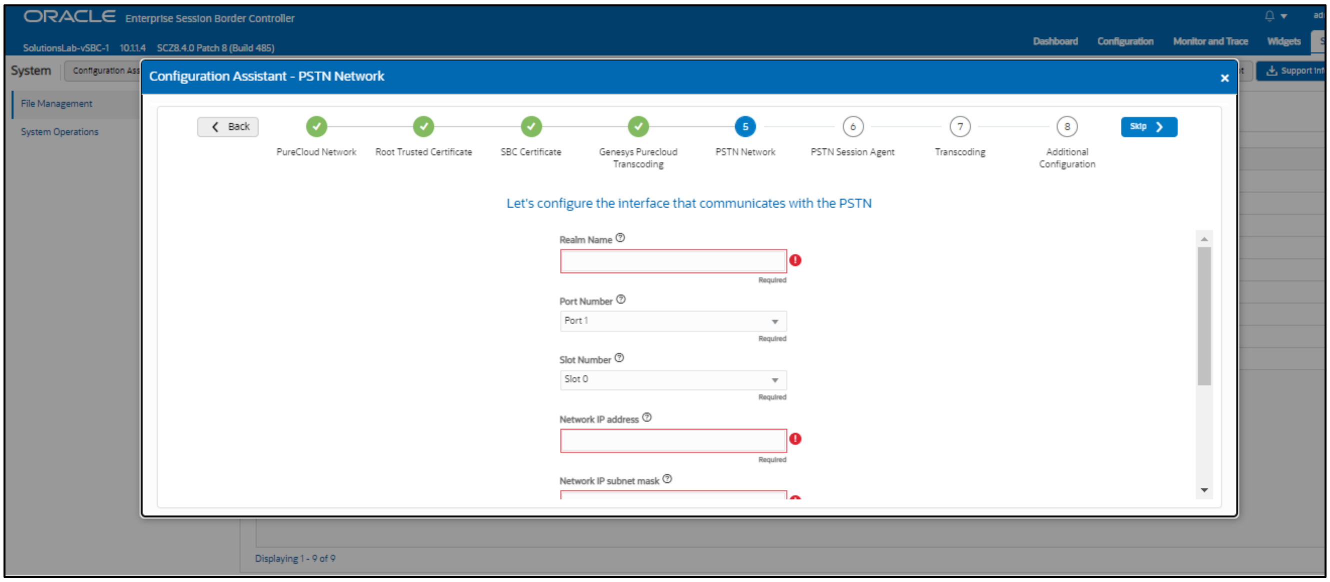
Do you want to select media codecs (SBC to PureCloud)? No / Yes

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)

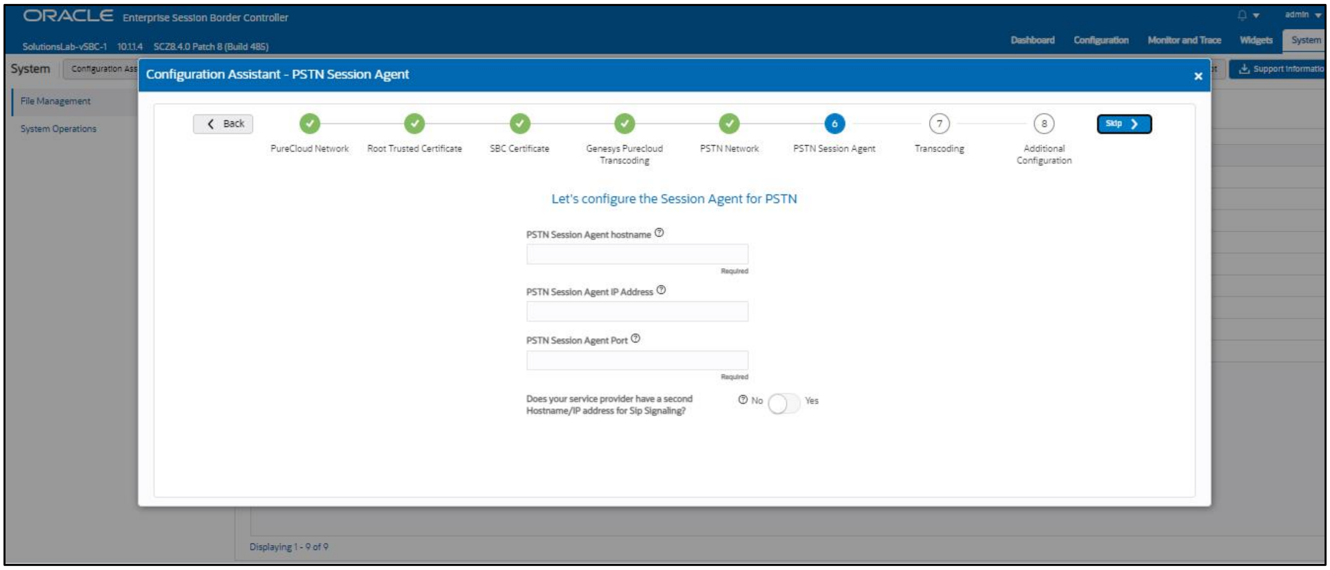
Slot Number: Slot 0 (Required)

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

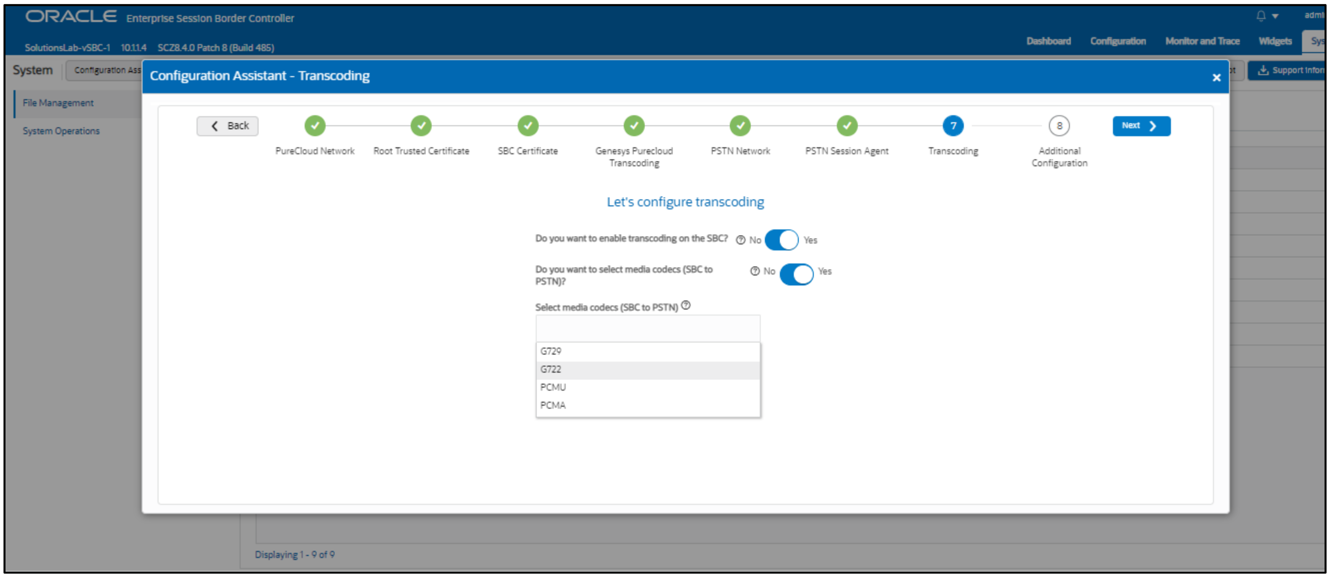
Does your service provider have a second Hostname/IP address for Sip Signaling? ⓘ [✓ No] Yes

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]

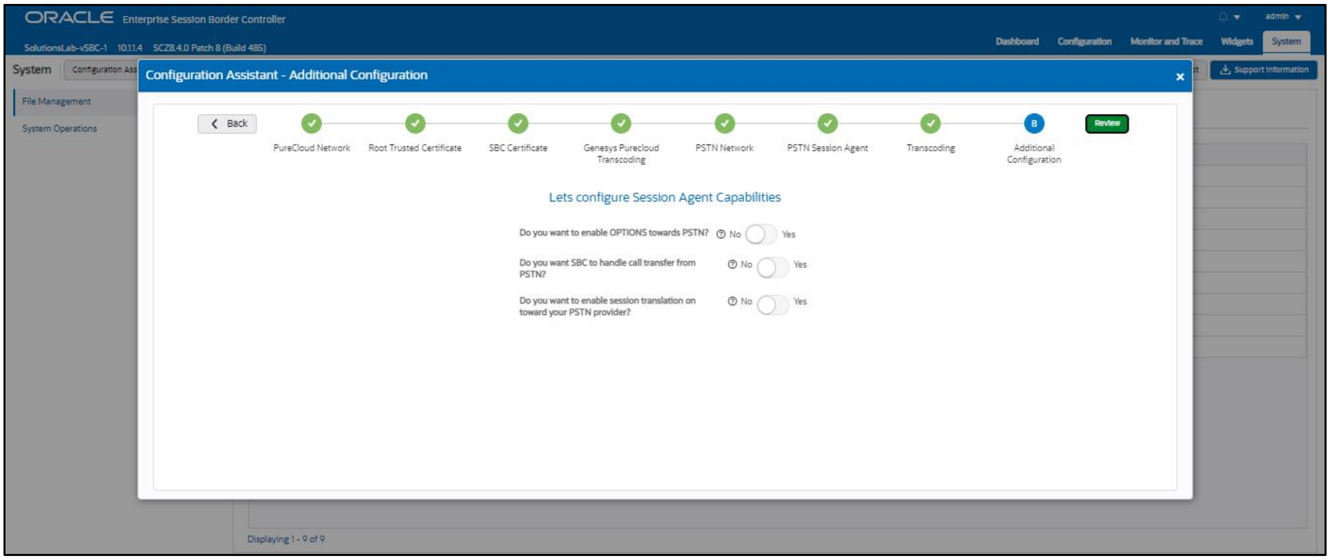
Do you want to select media codecs (SBC to PSTN)? ⓘ No [✓ Yes]

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

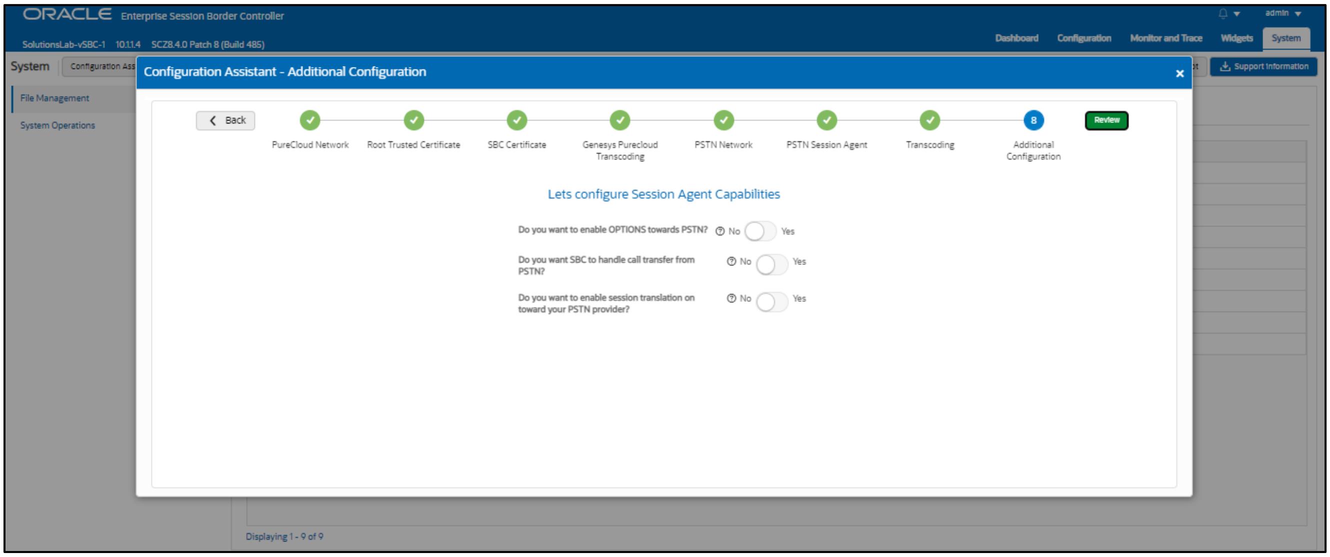
Do you want to enable OPTIONS towards PSTN? No ○ Yes

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

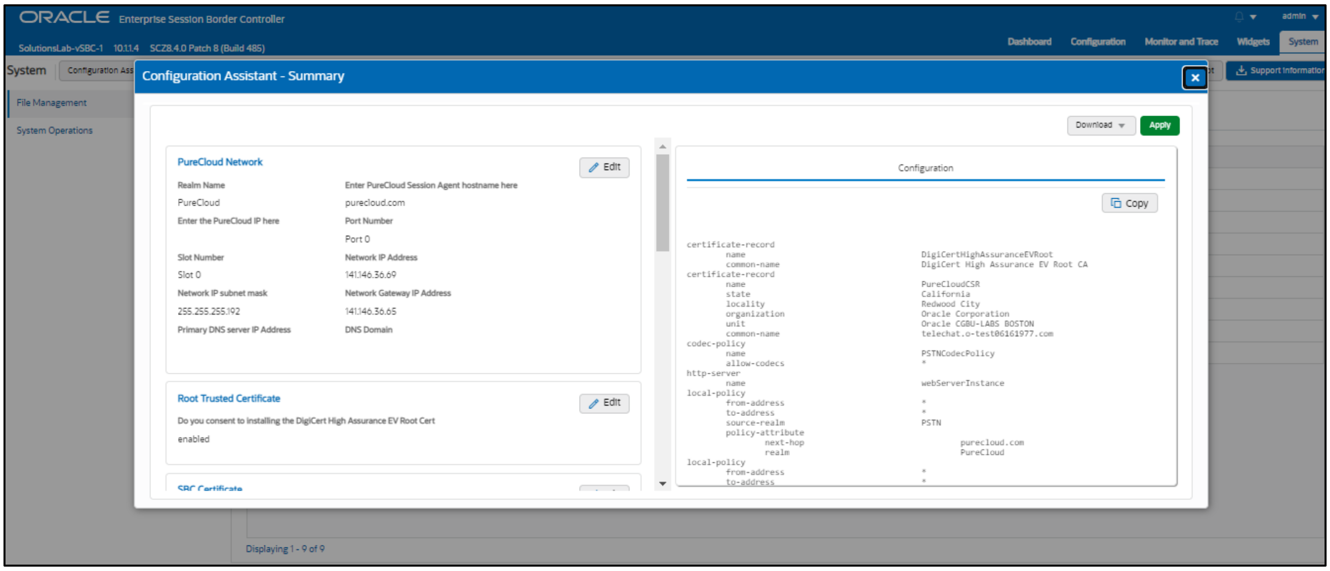
Do you want to enable OPTIONS towards PSTN? No ○ Yes

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.



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

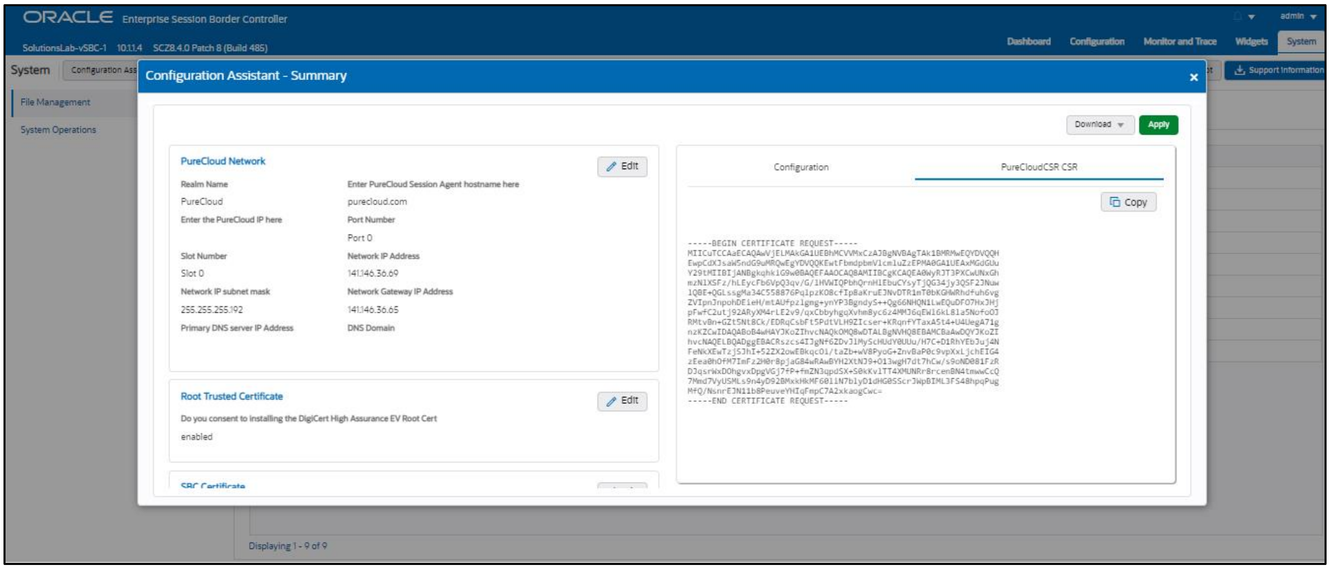
SBC Certificate

```
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.



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

```
-----BEGIN CERTIFICATE REQUEST-----
MIICuTCCAaECAQAwVjELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEPMA0GA1UEAxMGdGUu
Y29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0WyRJT3PXCwUNxGh
mzN1XSFz/hLEycFb6VpQ3qv/G/1HVWIQPbhQrnHlEbuCYsyTjQG34jy3QSF2JNuw
1Q8E+QGLssgMa34C558876Pq1pzKO8cfIp8aKruEJNvDTR1mT0bKGHWRhdfuh6vg
ZVIpnJnpohDEieH/mtAUfpz1gmg+ynYP3BgndyS++Qg66NHQN1LwEQuDFO7HxJHj
pFwfC2utj92ARyXM4rLE2v9/qxCbbyhgqXvhm8yc6z4MMJ6qEWl6kL81a5NofoOJ
RMtvBn+GZt5Nt8Ck/EDRqCsbFt5PdtVLH9ZIcser+KRqnfYTaxA5t4+U4UegA71g
nzKZCwIDAQABoB4wHAYJKoZIhvcNAQkOMQ8wDTALBgNVHQ8EBAMCBaAwDQYJKoZI
hvcNAQELBQADggEBACRszcs4IJgNf6ZDvJlMyScHUdY0UUu/H7C+D1RhYEbJuj4N
FeNkXEwTzjSJhI+52ZX2owE8kqcO1/taZb+wV8PyoG+ZnvBaP0c9vpXxLjchEIG4
zEea0hOfM7ImFz2H0r8pjaG84wRAwBYH2XtNJ9+O13wgH7dt7hCw/s9oND081FzR
DJqsrWxDOhgvxDpgVGj7fP+fmZN3qpdSX+S0kKvlTT4XMUNRr8rcenBN4tmwwCcQ
7Mmd7VyUSMLs9n4yD92BMxkHkMF60liN7b1yD1dHG0SScrJWpBIML3FS48hpqPug
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 BYOC CloudPhone 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.

9. Test Plan Executed

We have executed the following test plan to validate the interworking between Genesys BYOC Cloud 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 Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615