Oracle SBC integration with Genesys PureCloud BYOC 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 PureCloud and Zoom Phone BYOC	20 Aug 2021
1.1	Oracle Public IP Address masked	18 Nov 2021
1.2	Added Section Genesys PureCloud Configuration Assistant	03 Feb 2022

Table of Contents

1 Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of the Oracle Enterprise Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform along with Genesys PureCloud and Zoom Phone.

2. Document Overview

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

It should be noted that the SBC configuration provided in this guide focuses strictly on the Genesys PureCloud and Zoom Phone related parameters. Calls between Zoom Phone and PureCloud are terminated via a carrier SIP Trunk. The steps required to configure the Carrier Trunk are specific to individual customers and are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

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

Related documentation can be found below –

2.1 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 PureCloud

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

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

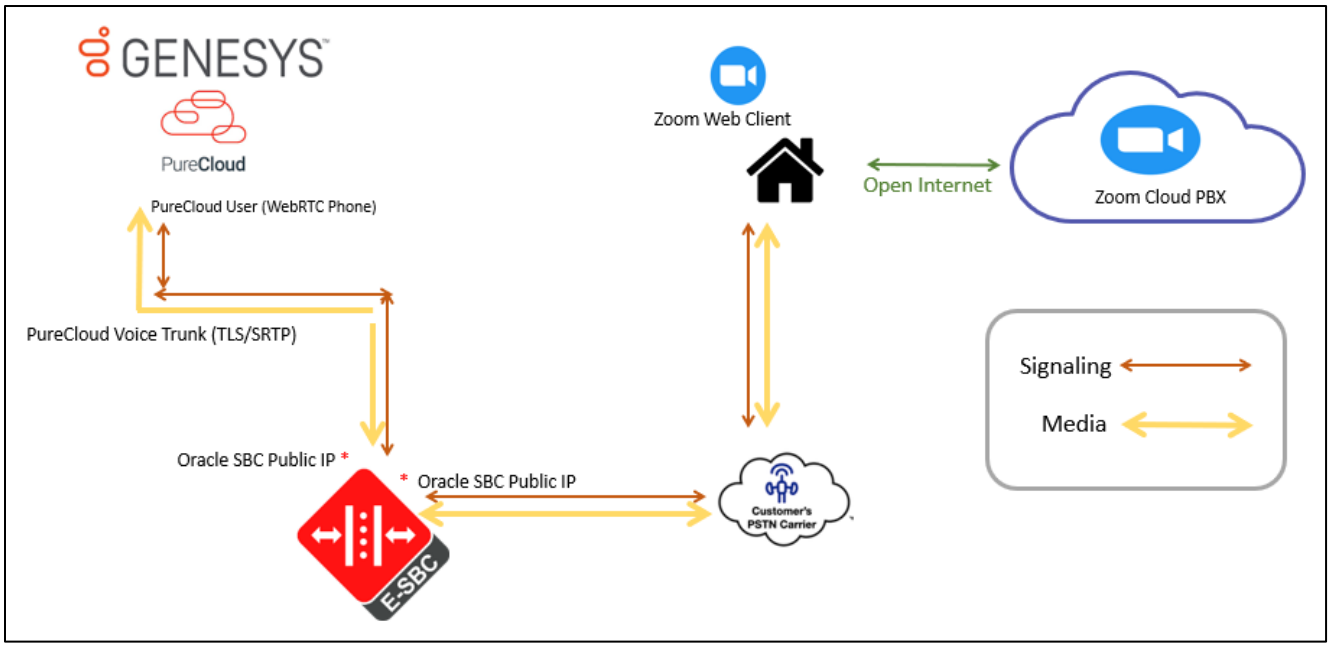
3. Validated Oracle Versions

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 PureCloud, Oracle SBC and Zoom Phone. Both PureCloud 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 PureCloud 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 PureCloud

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 PureCloud

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

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

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

The Oracle Enterprise SBC will act as an intermediary between Zoom Phone and Genesys PureCloud. The SBC is configured to broker calls as a back-to-back user agent (B2BUA) between the two systems. The Carrier DIDs are assigned to users on PureCloud System and 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 PureCloud 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 PureCloud telephony connection option and facilitates point-to-point communication. We will configure Oracle Enterprise SBC as an external Trunk on the PureCloud Portal. Detailed steps to configure the external trunk can be found here-

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

To configure the external Trunk, Navigate to

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

5.1.1 Create a new External Trunk

Type: BYOC Carrier Trunk

Protocol: TLS (TCP and UDP are also available)

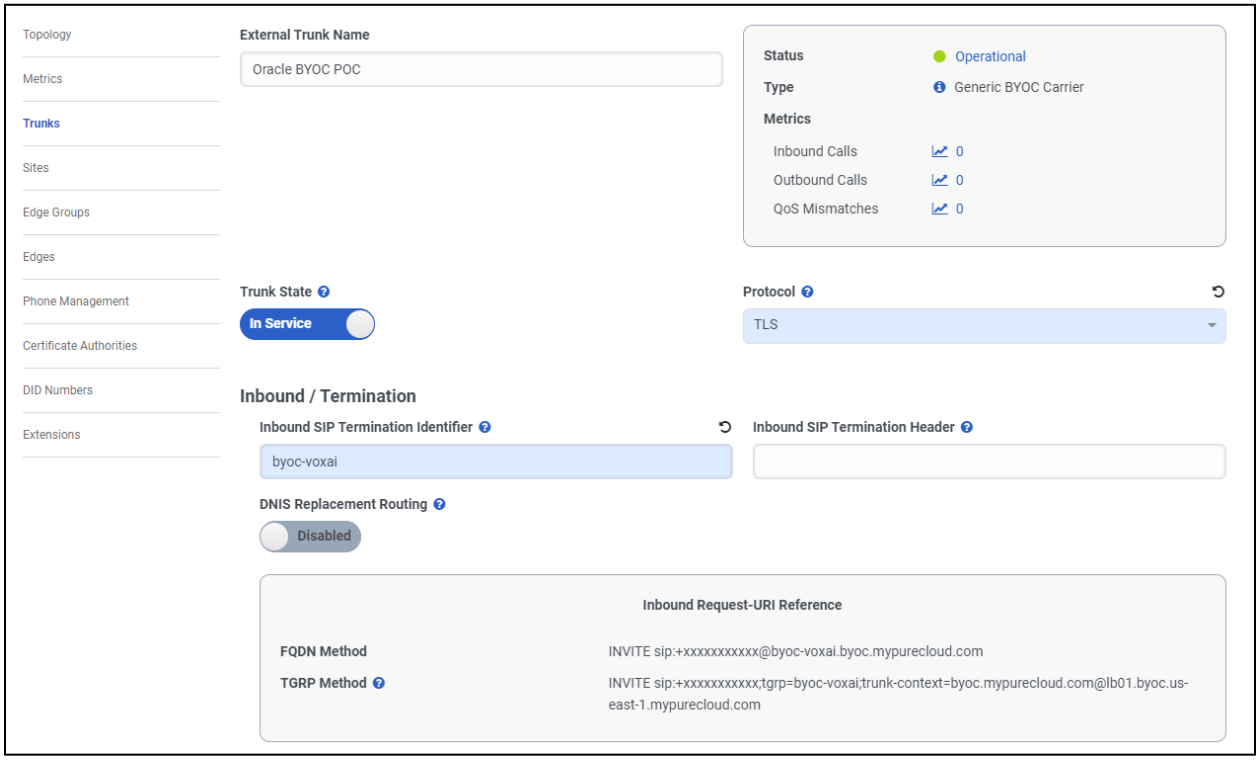
5.1.2 Set Inbound SIP Termination Identifier

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

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

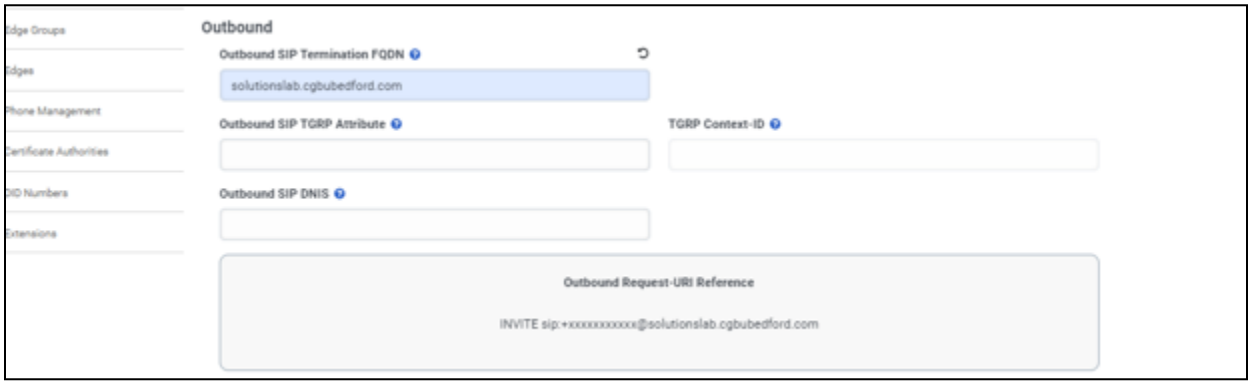
Genesys Cloud IP List

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

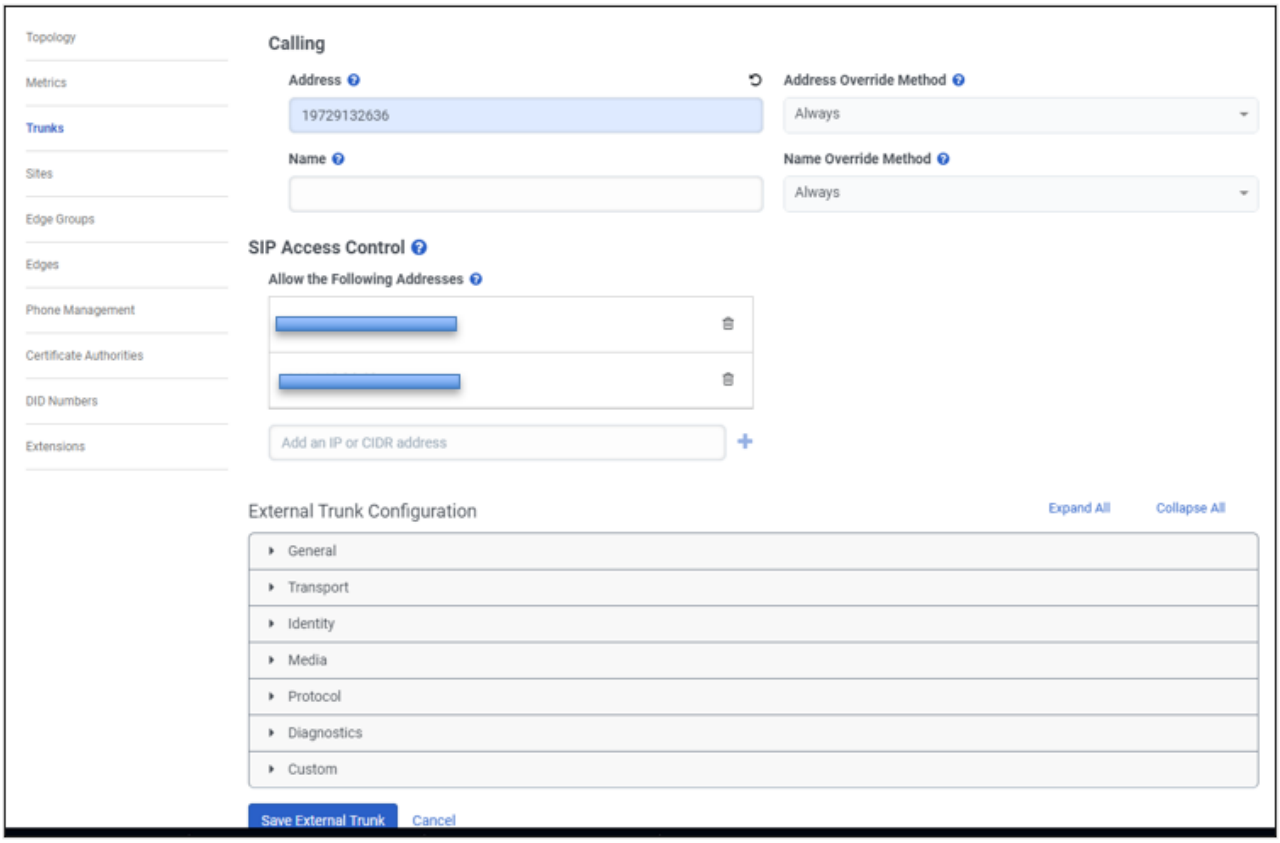


5.1.3 Set Outbound SIP Servers or Proxies

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



5.1.4 Set Calling Address



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

5.1.5 Set SIP Access Control

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

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.

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 Pure Cloud Edge(s).

Detailed steps to configure the Site can be found here-

https://help.mypurecloud.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**.

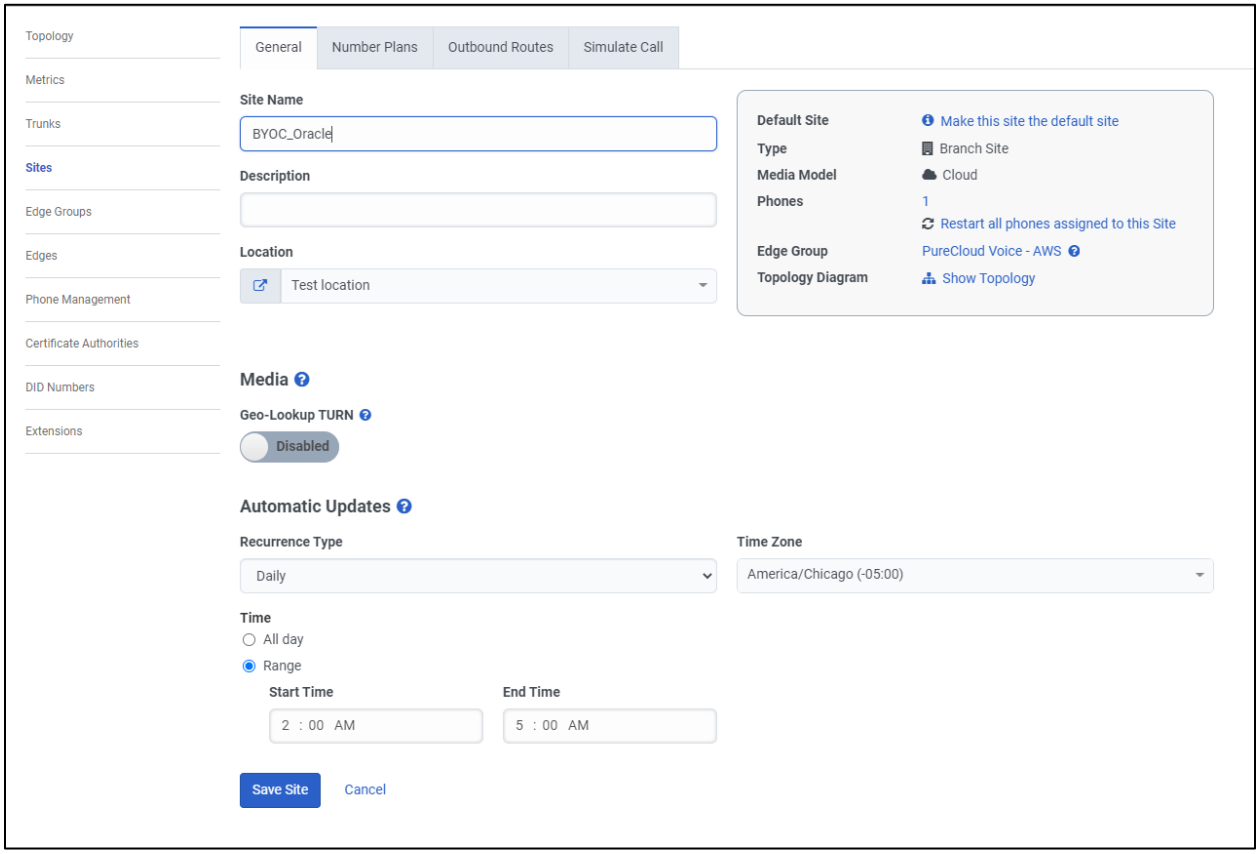
Type a name into the **Site Name** box.

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

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

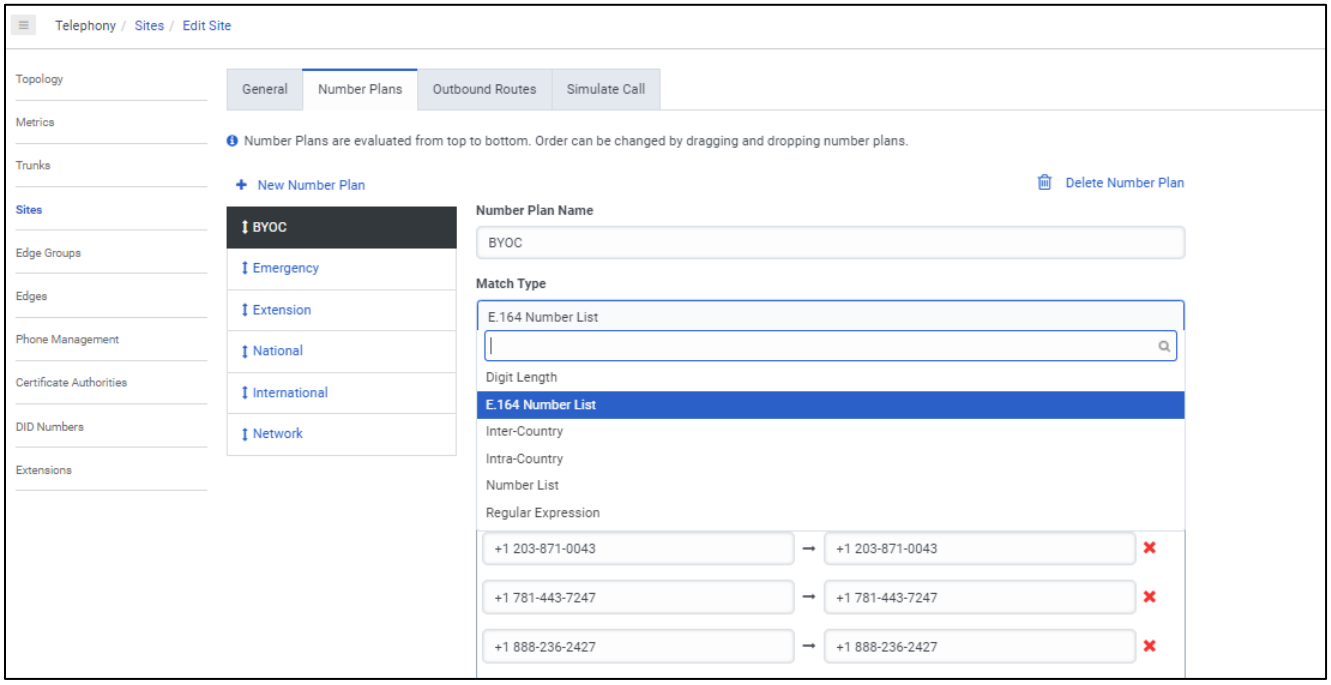
Under **Media Model**, select **Cloud**.

Click **Create Site**.



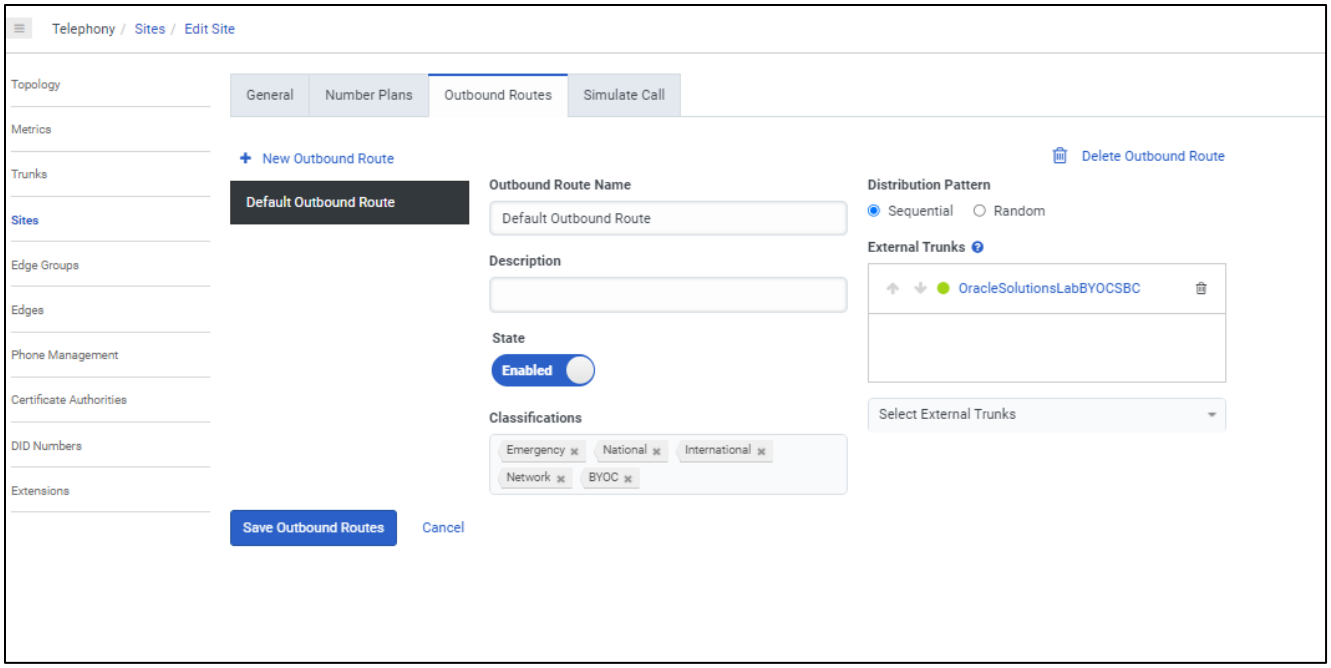
5.2.2 Number Plans & Classifications

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



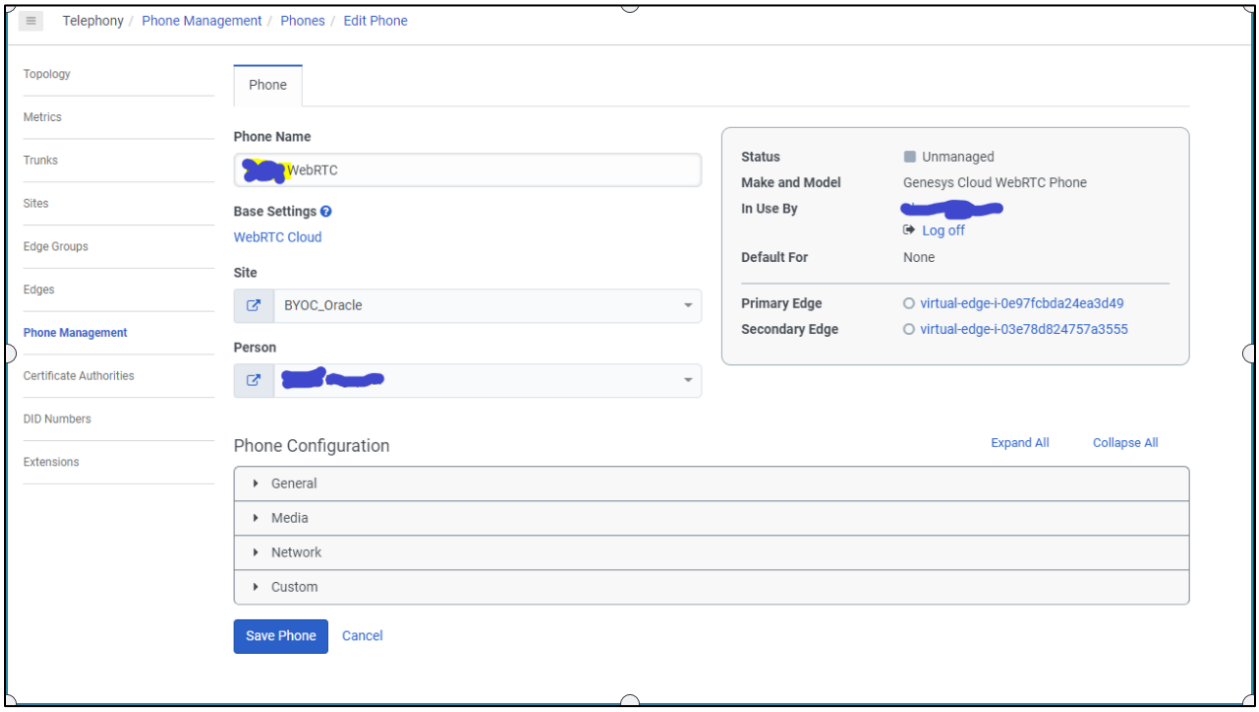
5.2.3 Configure outbound route

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.



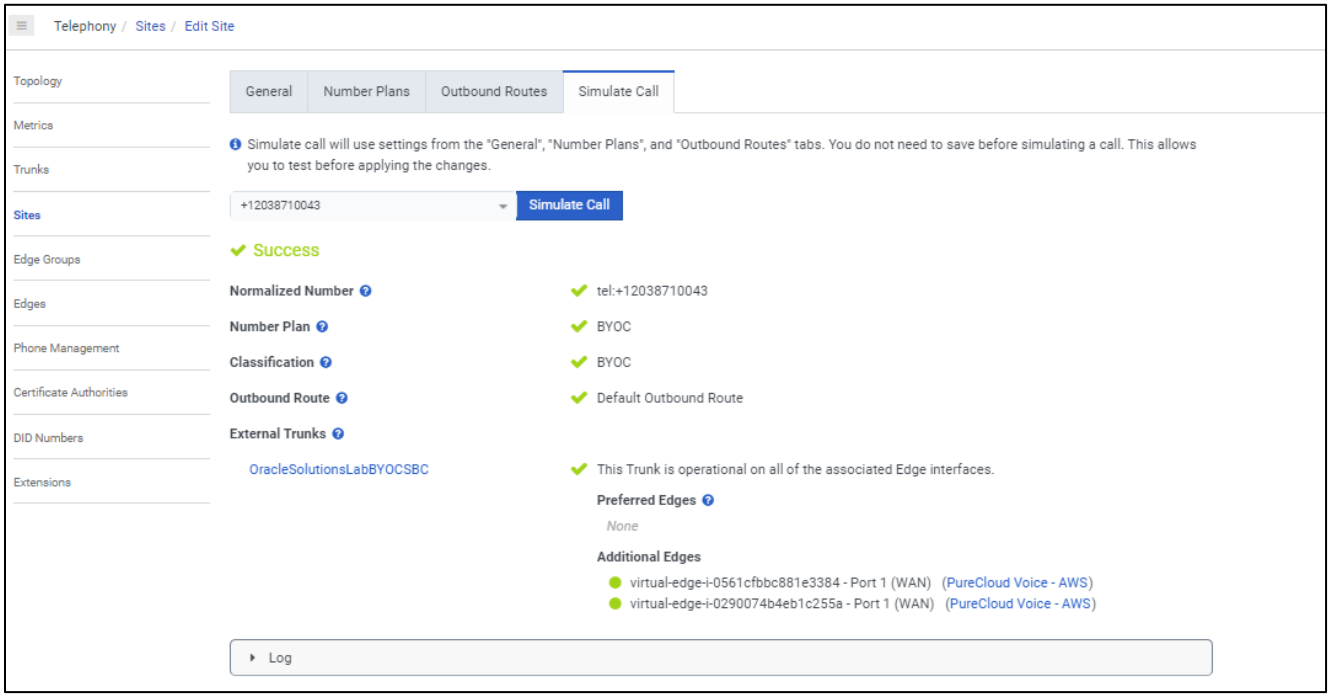
5.2.4 Phone configuration

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.



5.2.5 Simulate call

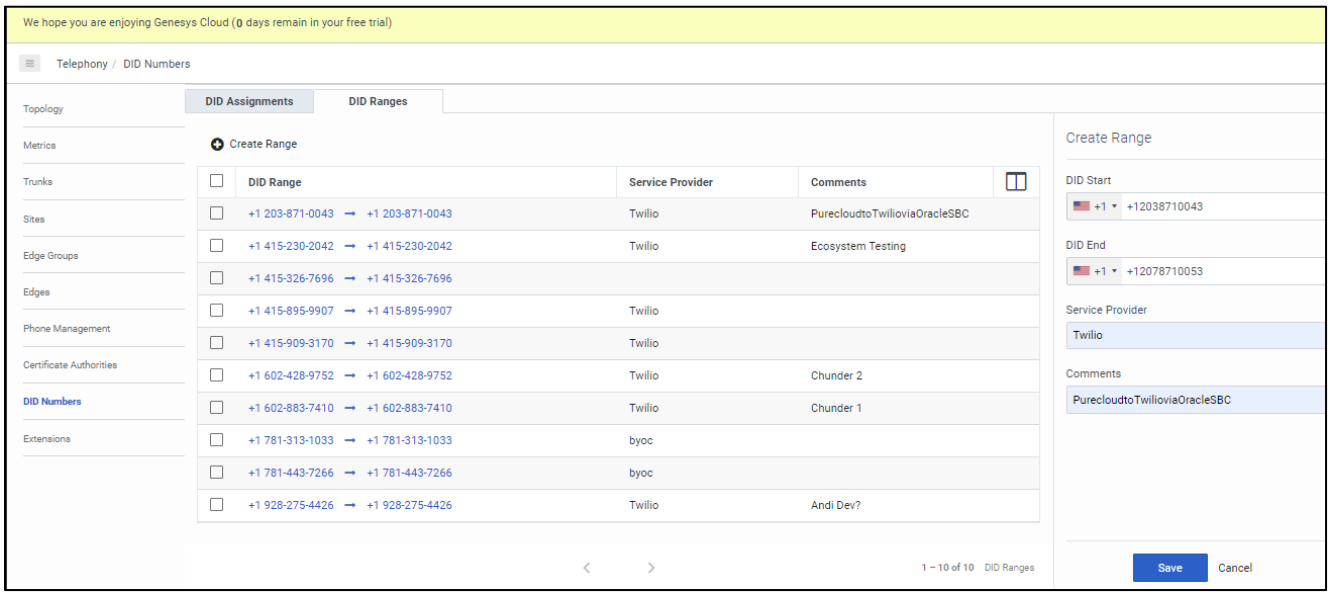
Genesys PureCloud provides a neat feature to test and validate the routing of calls for troubleshooting purpose. Below is an example for a call to BYOC type number classification on this Site. Success indicates a successful routing response.



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

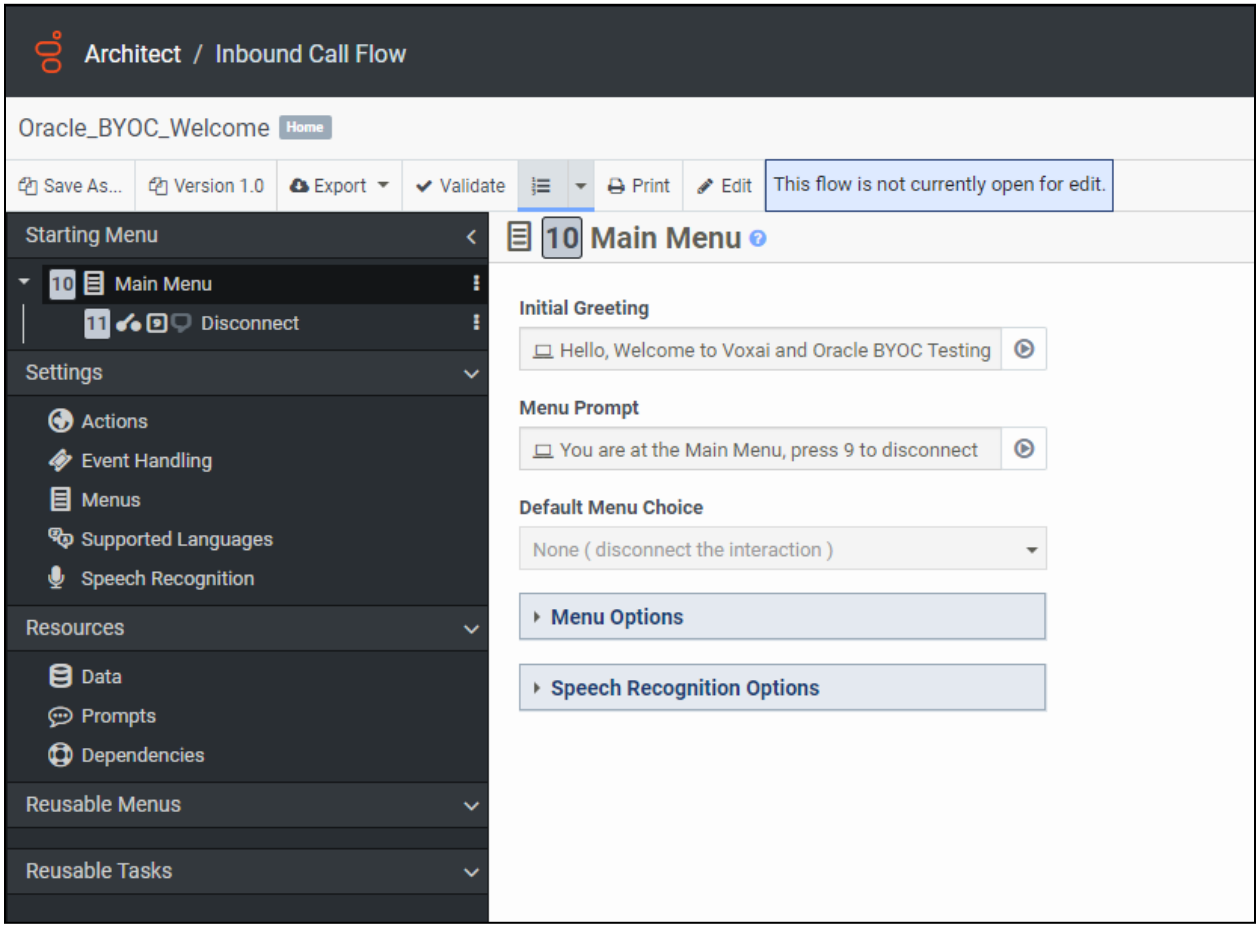


5.3.2 Assign DID to User.

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

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 PureCloud via Oracle SBC.

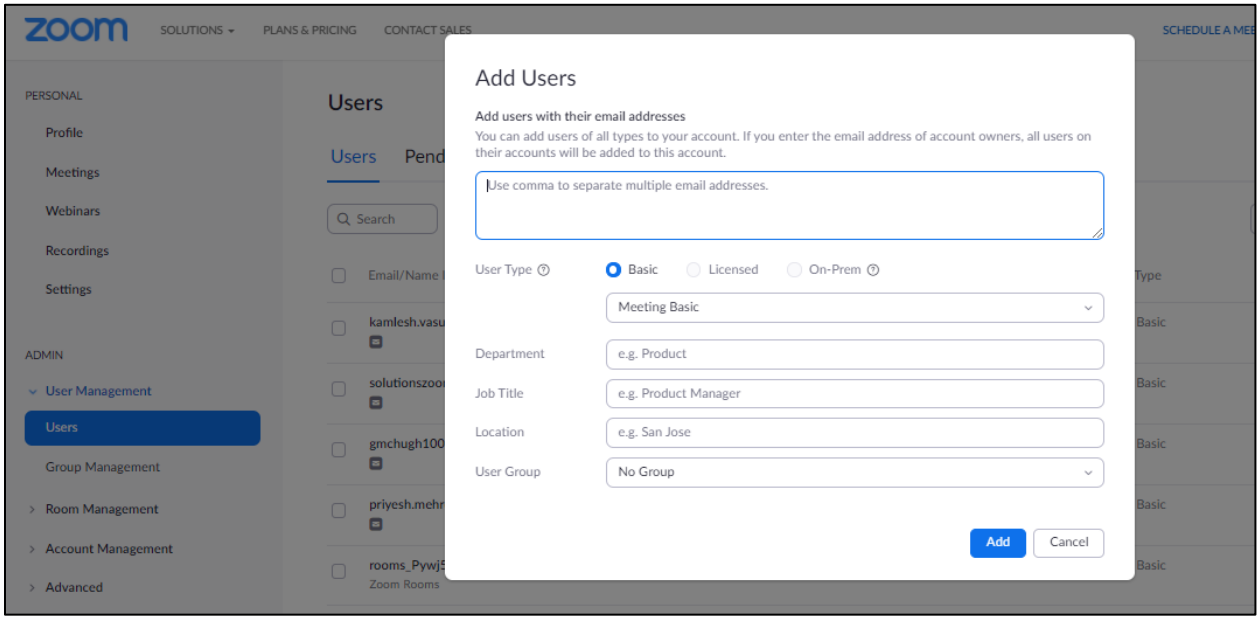


6. Configure Zoom Phone

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.



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.

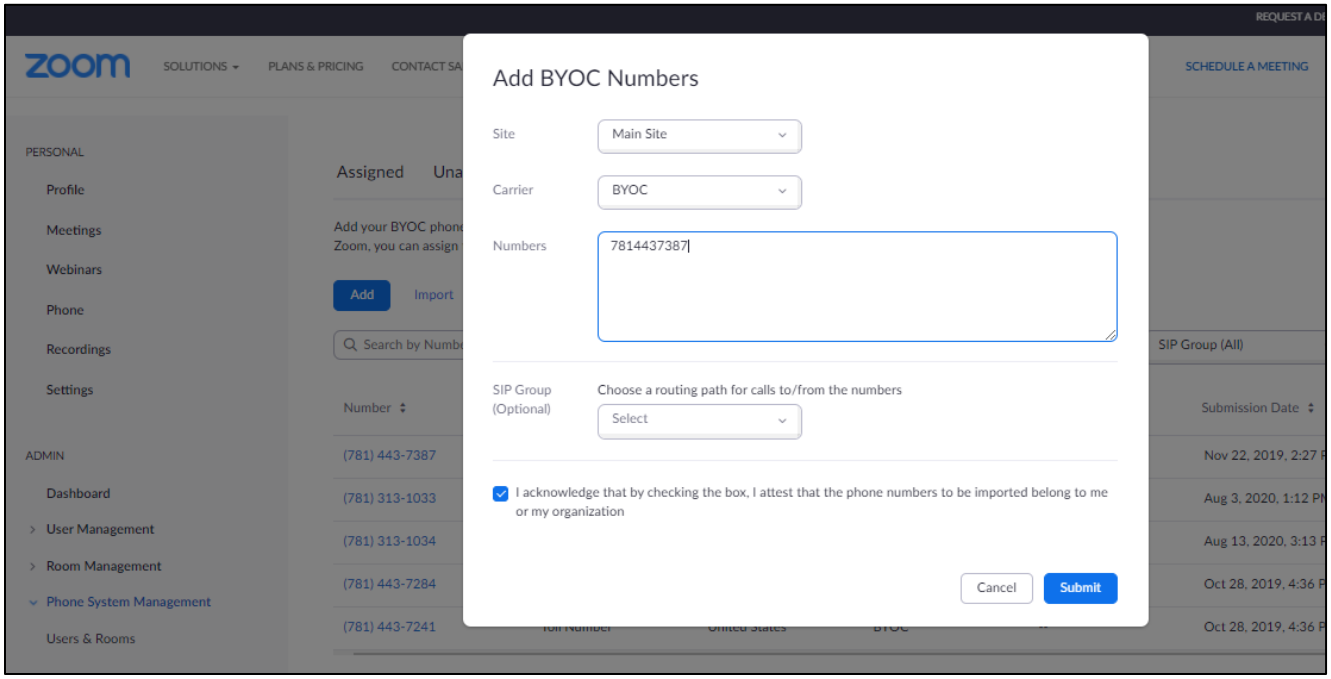
Carrier –Choose BYOC

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**.



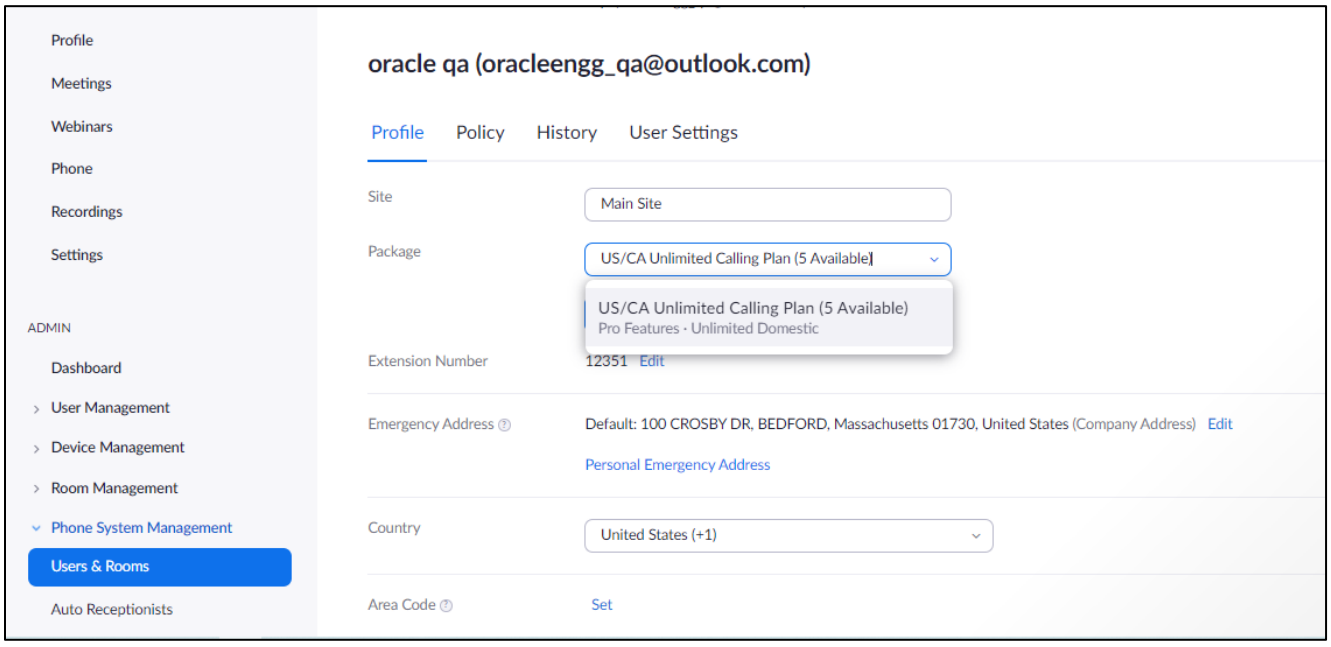
6.3 Assign a Calling Package to User

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

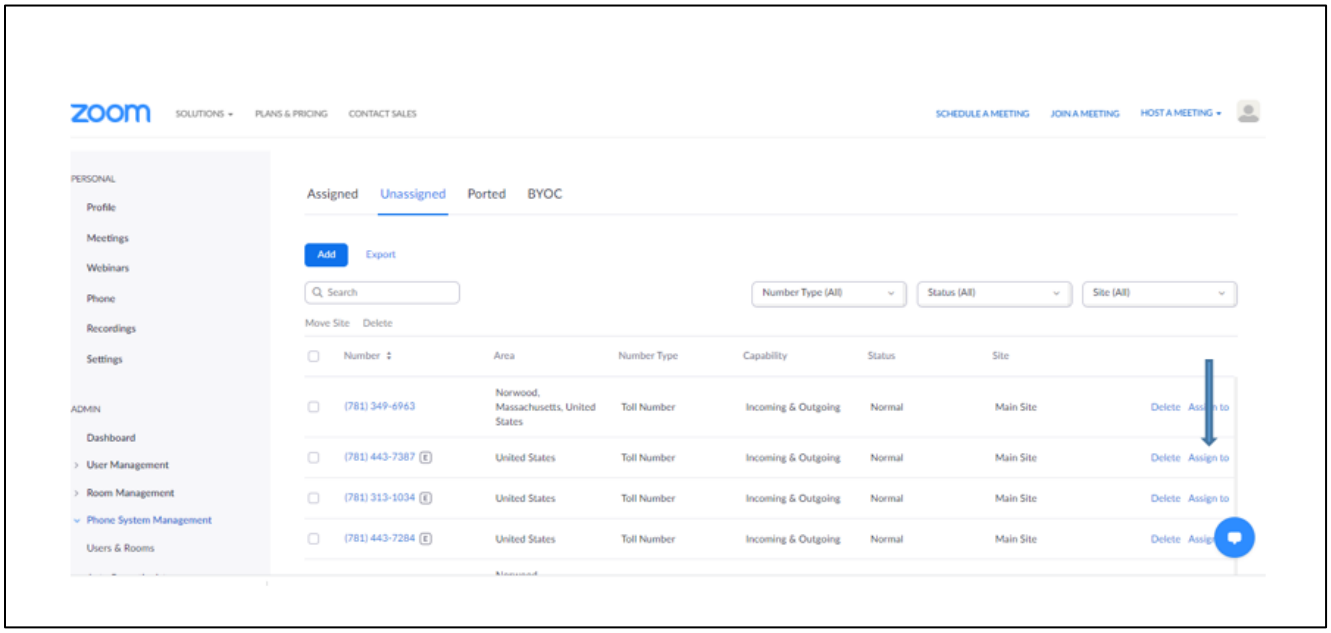
Navigate to **Users and Rooms > Package**

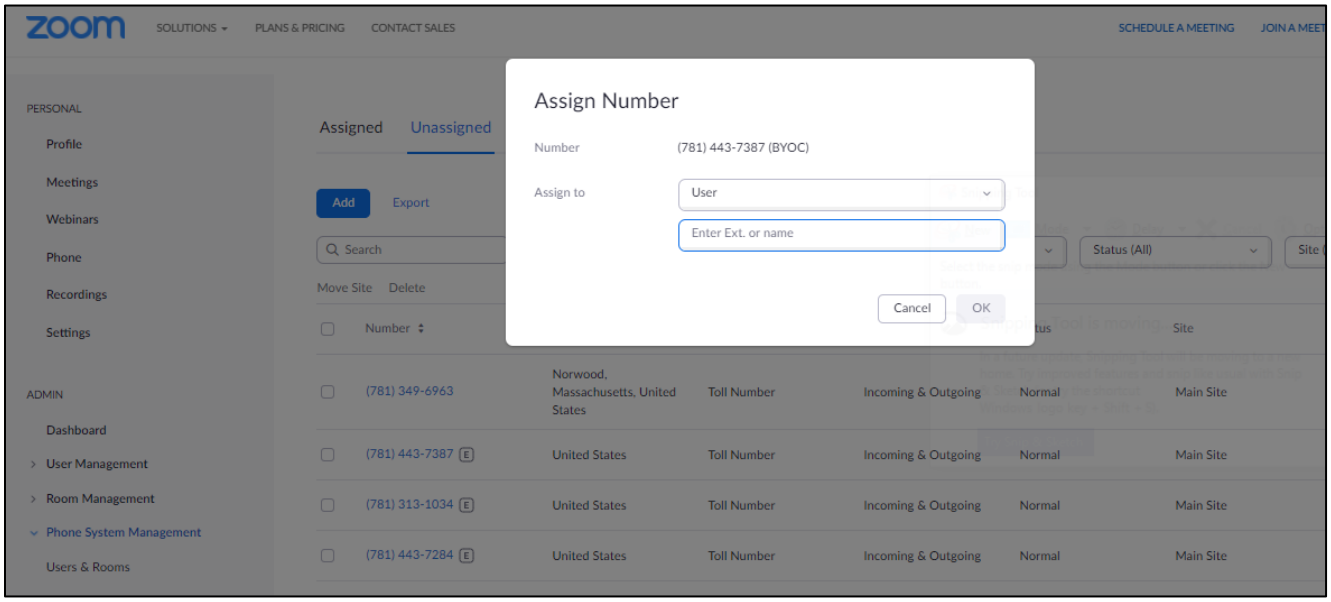
Choose the appropriate package and assign the package to the Respective User.



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.





7. Configuring the SBC

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

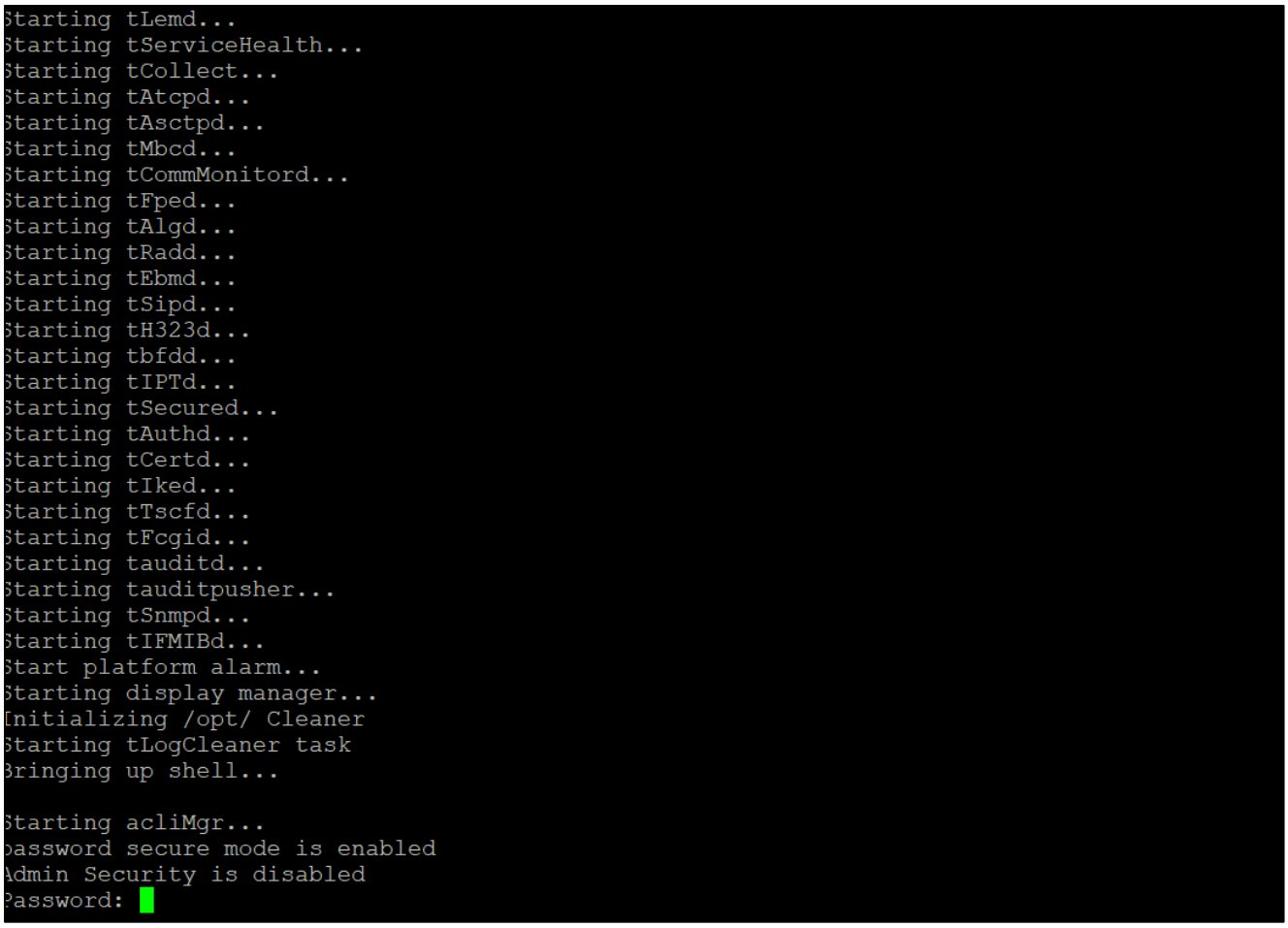
7.1.1 Establishing a serial connection to the SBC

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:

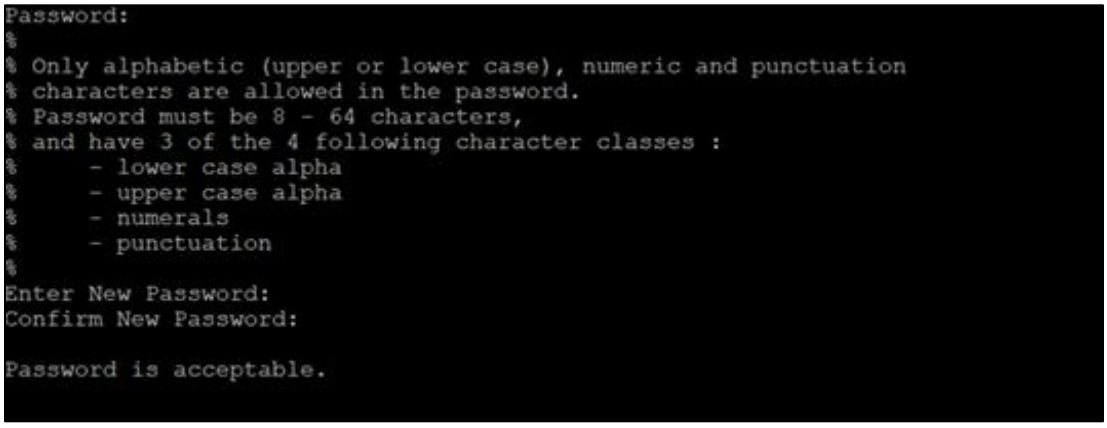
- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

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



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.



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.

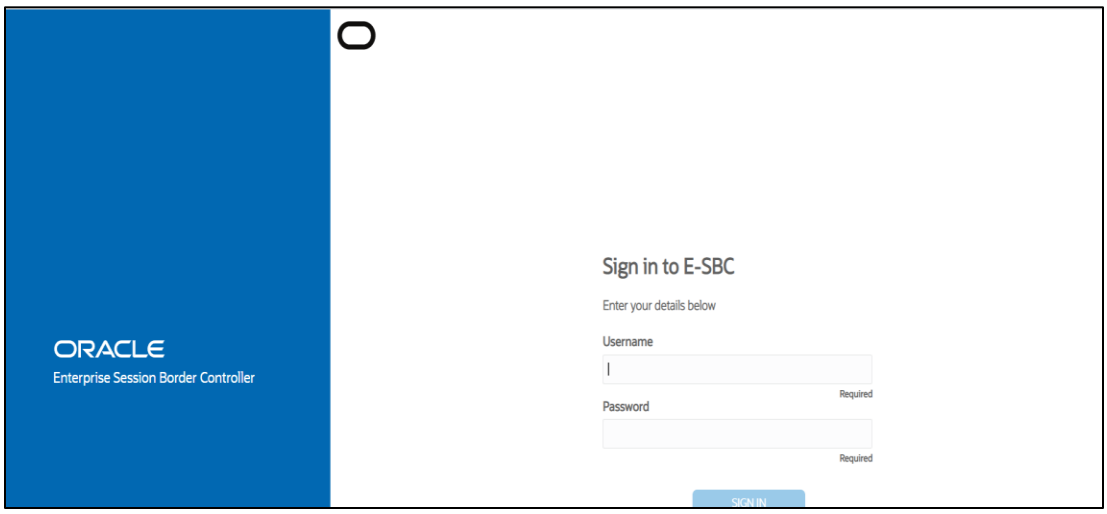
```
NN4600-139(http-server)#
NN4600-139(http-server)# show
http-server
        name                                webServerInstance
        state                               enabled
        realm
        ip-address
        http-state                          enabled
        http-port             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

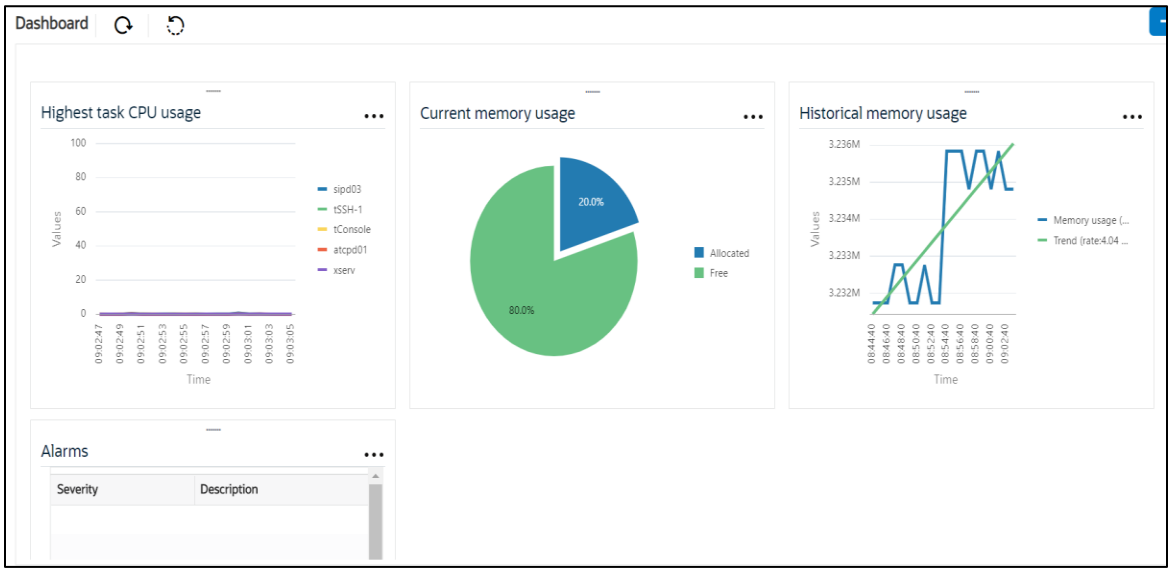
7.2.2 Configure SBC using Web GUI

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

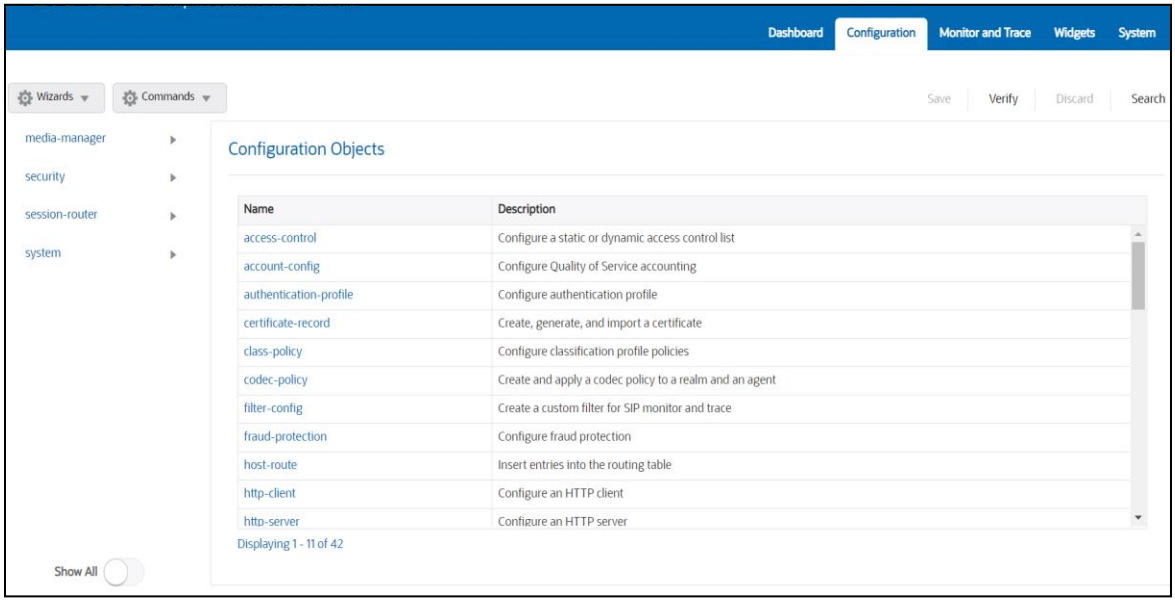
The Web GUI can be accessed through the URL http://<SBC_MGMT_IP>.



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



Navigate to Configuration as shown below, to configure the SBC.



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

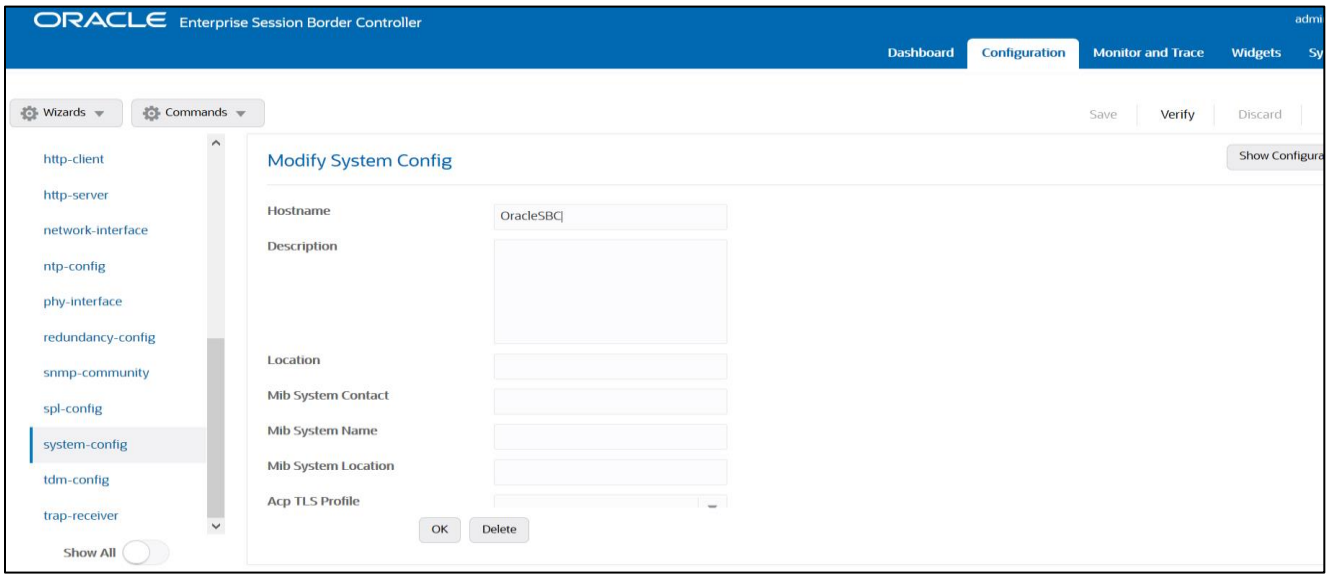
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf

The expert mode is used for configuration.

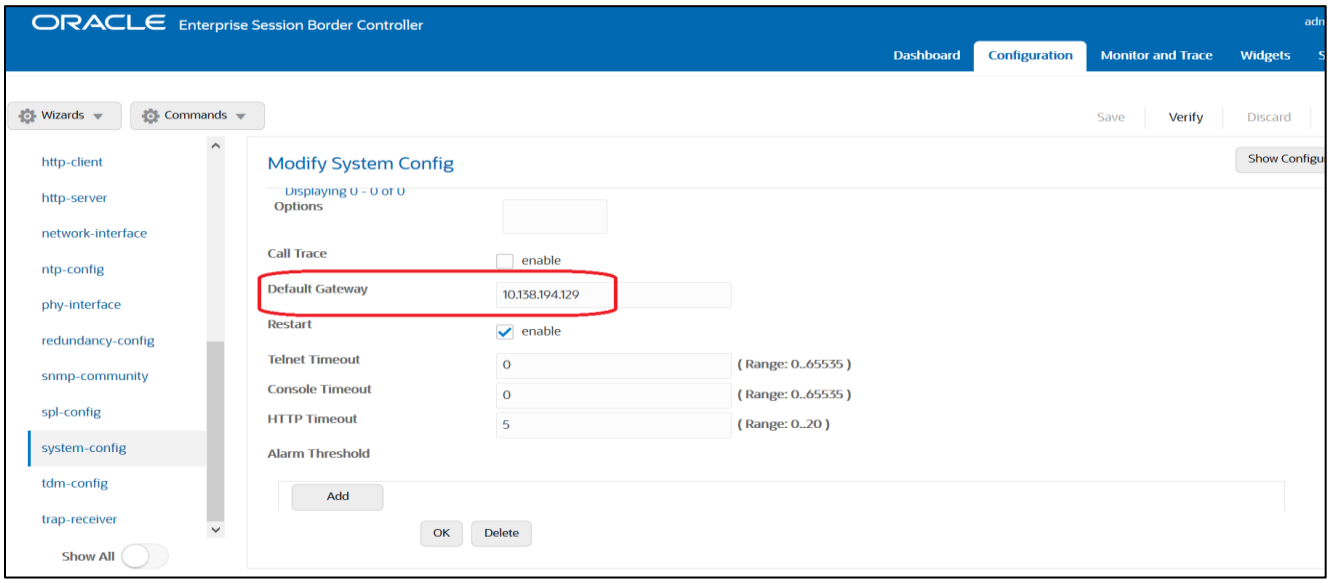
Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

7.2. Configure system-config

Navigate to system->system-config



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



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.

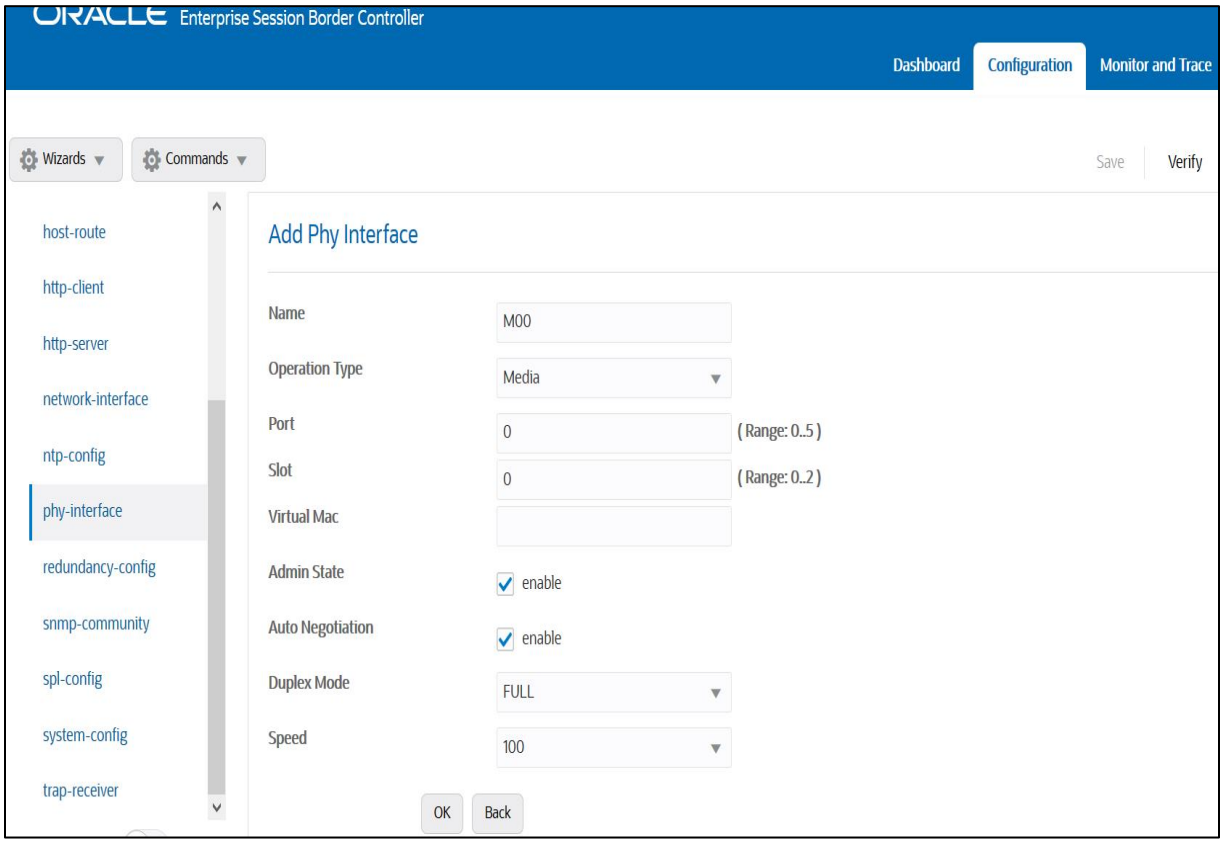
7.3. Configure Physical Interface values

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

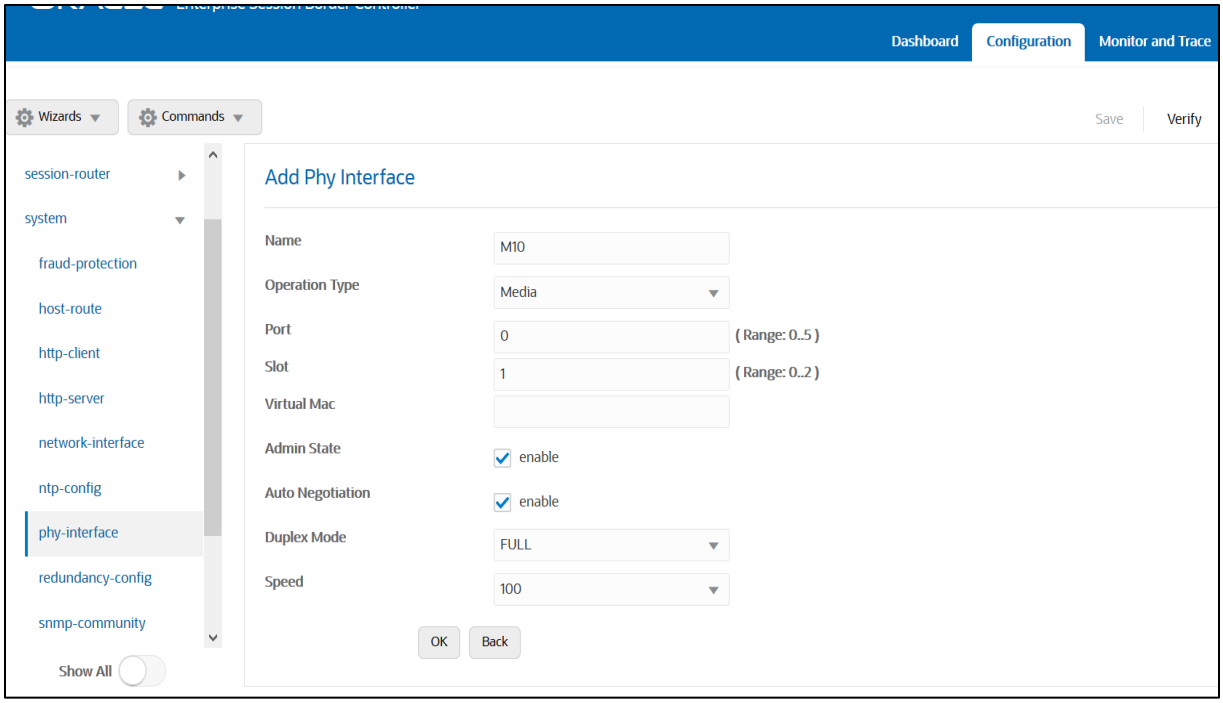
Here we have configured, Network-interface M00 for Zoom Phone and M10 for PureCloud.

Parameter Name	**Zoom Phone (M00)**	**PureCloud (M10)**
Slot	0	1
Port	0	0
Operation Mode	Media	Media

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



Configure **M10** interface as per example shared below -



7.4. Configure Network Interface values

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

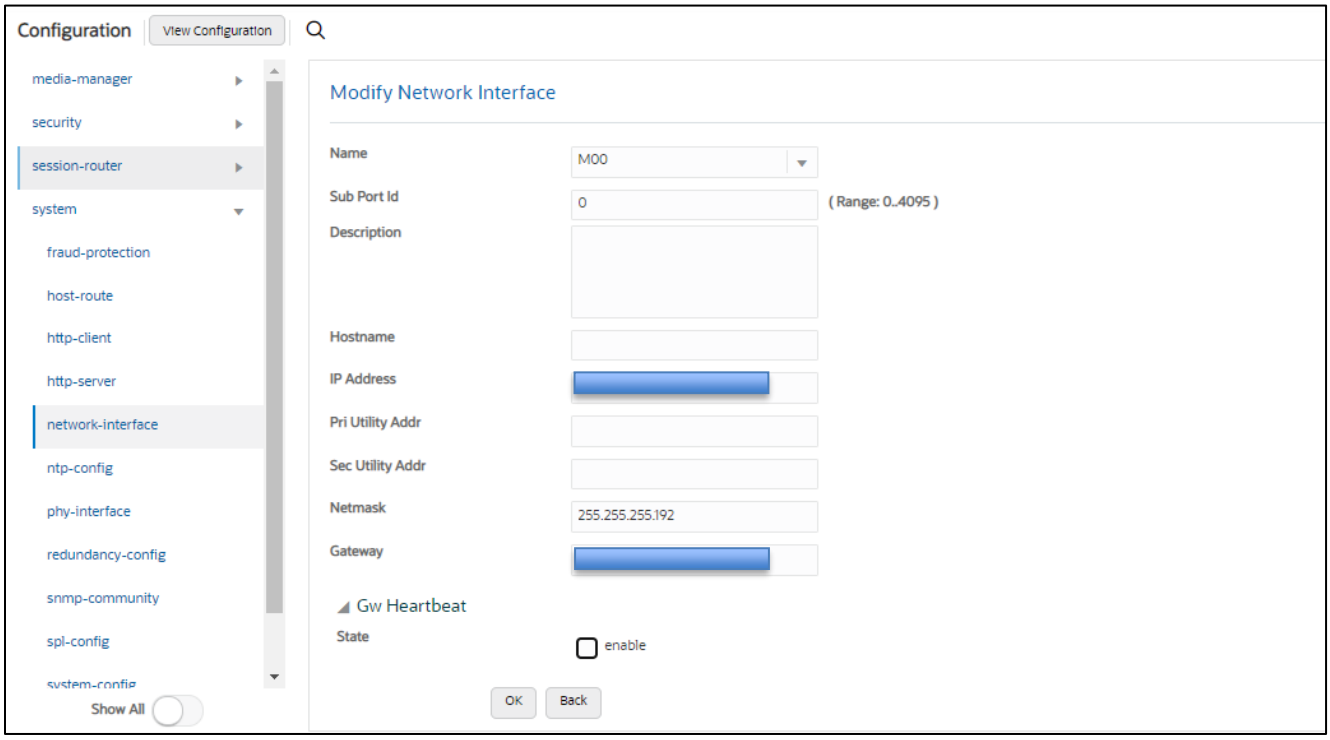
The table below lists the parameters, to be configured for both the interfaces.

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.

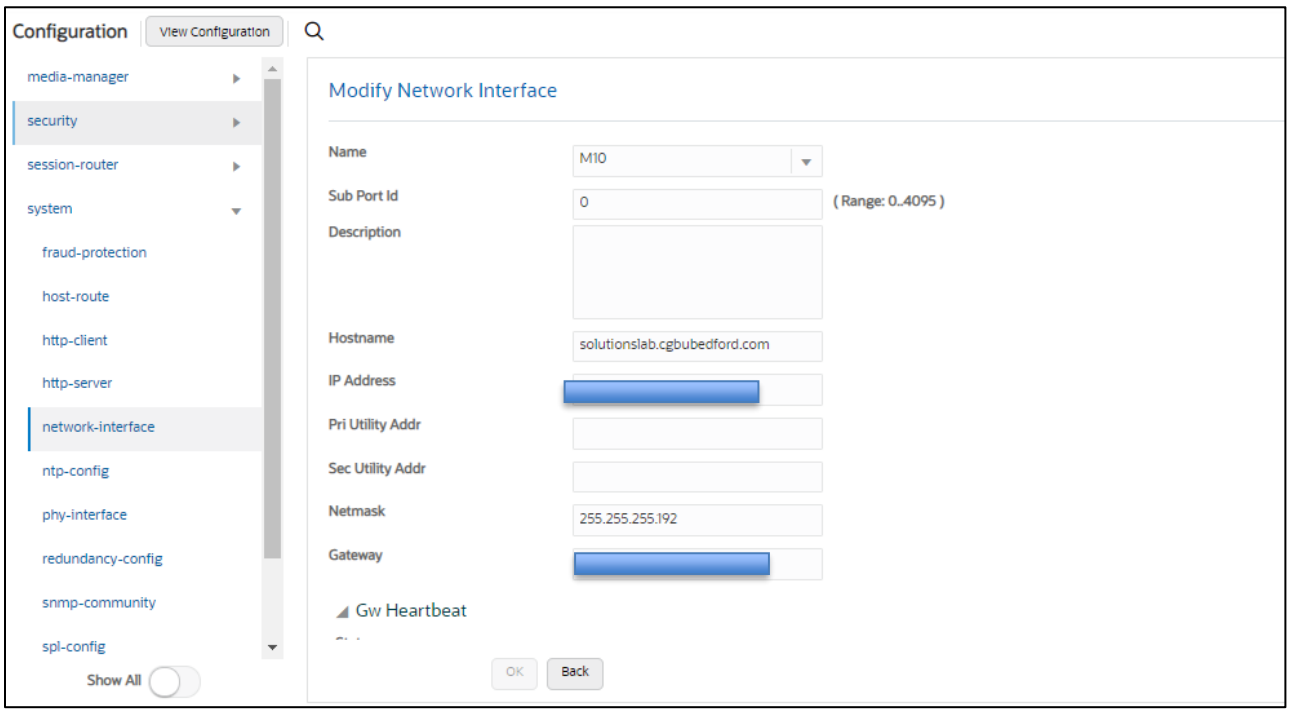
In this Setup we are using Google Public DNS to resolve the DNS names to IP Addresses.

Parameter Name	Zoom Phone Network Interface	PureCloud 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



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

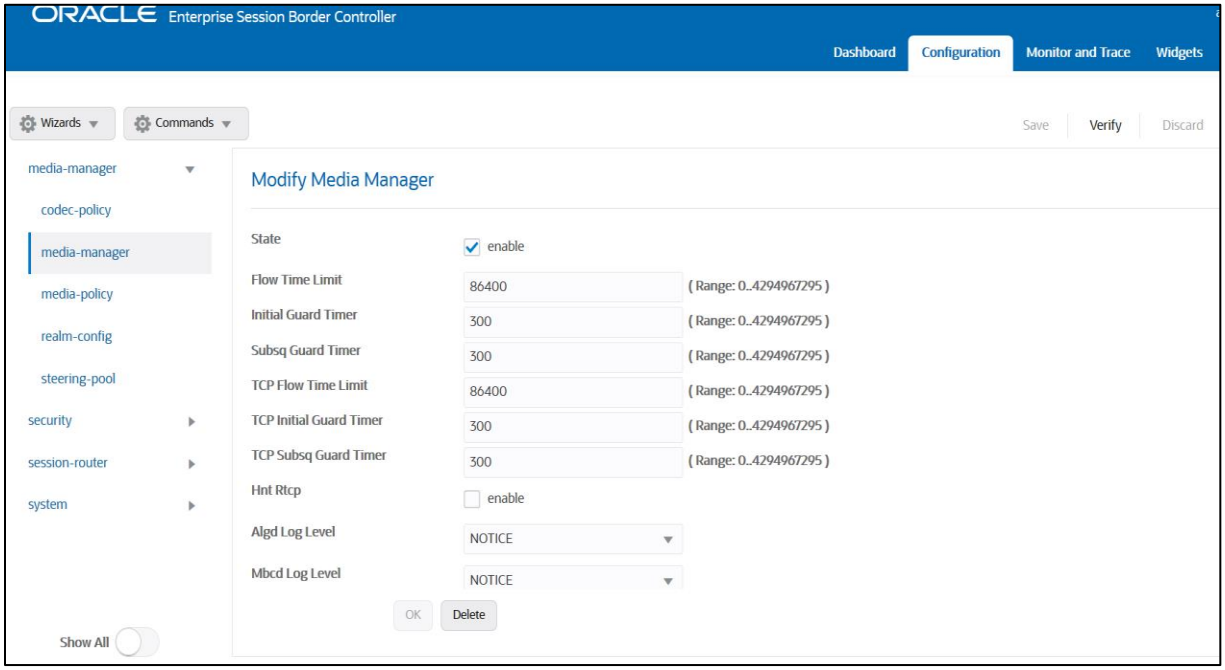


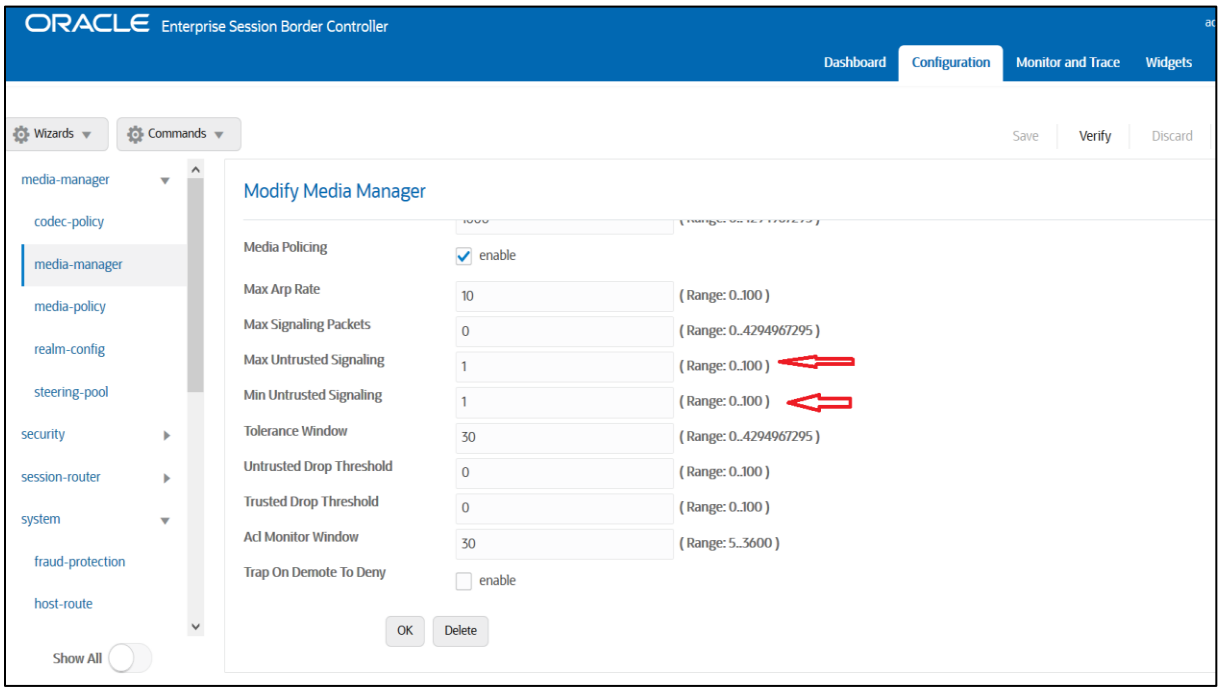
7.5. Enable media manager

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





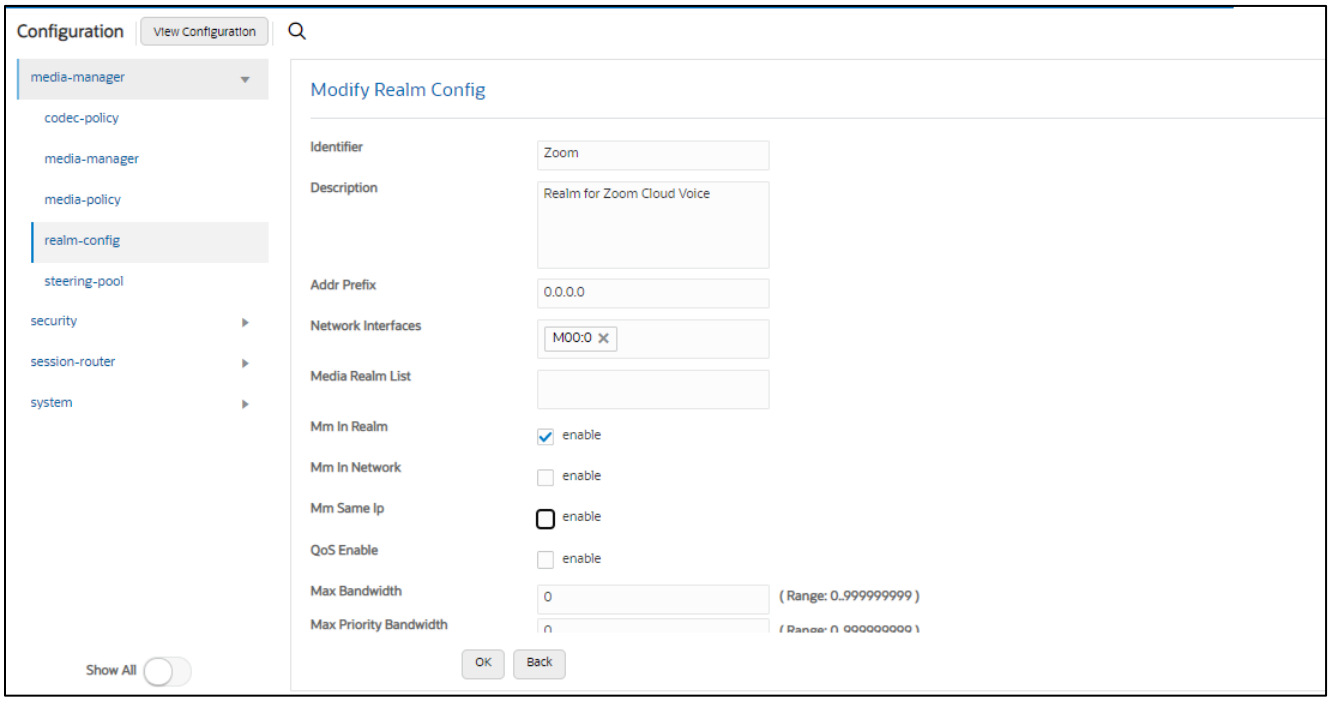
7.6. Configure Realms

Navigate to media-manager > realm-config

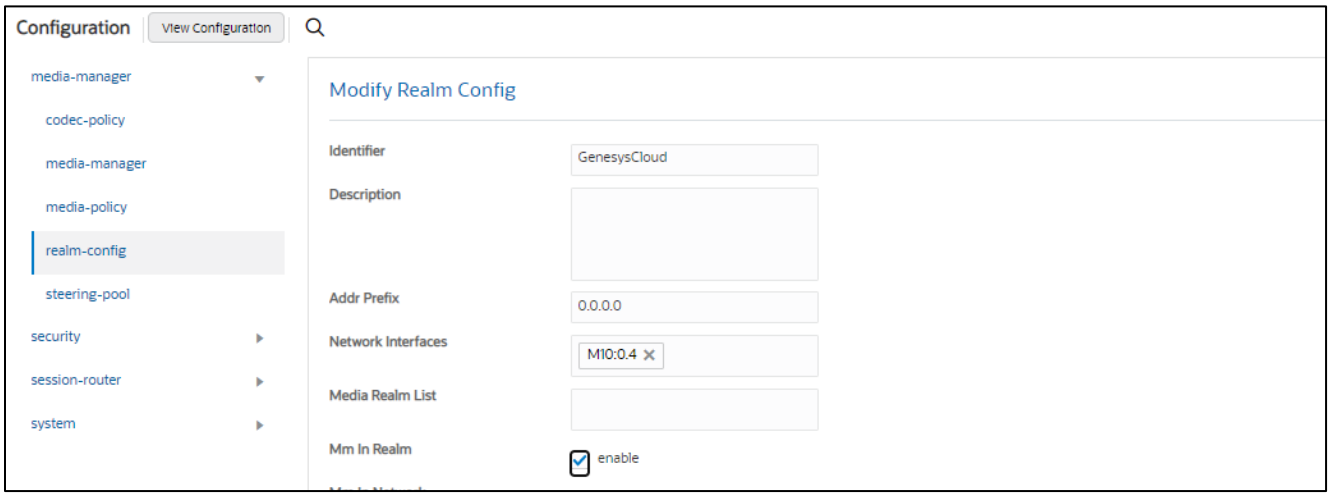
The name of the Realm can be any relevant name according to the user convenience. Use the following table as a configuration example for the three realms used in this configuration:

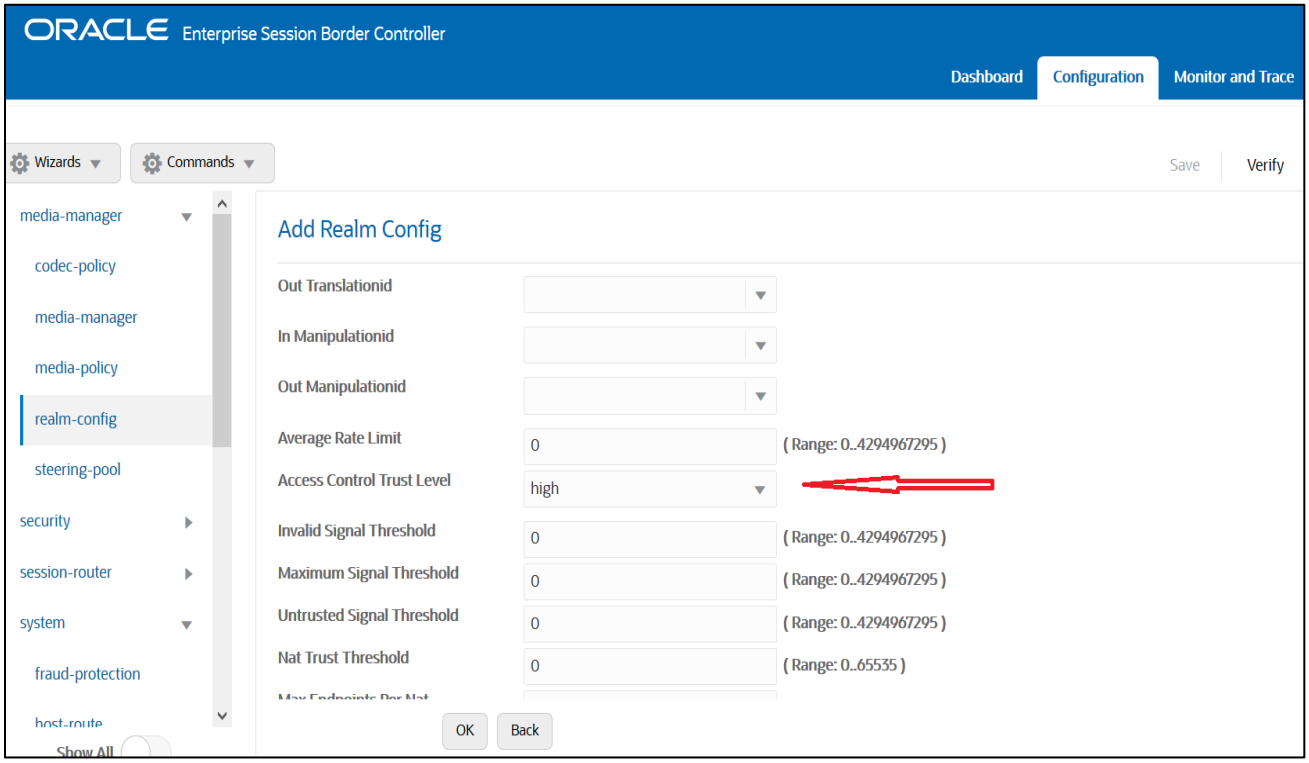
Config Parameter	Zoom Realm	GenesysCloud Realm
Identifier	Zoom	GenesysCloud
Network Interface	M00	M10
Mm in realm	☑	☑
Access Control Trust Level	High	High
Media Sec policy	sdespolicy	sdespolicy
RTCP mux	☑optional	

Realm for Zoom Phone –



Realm for Genesys PureCloud





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

7.7.1 Configuring Certificates

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

The communication between the **Oracle SBC with Zoom Phone and Genesys PureCloud is TLS/SRTP.**

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

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

GUI Path: security/certificate-record

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

- **SBC Certificates (end-entity certificate)**
- **DigiCert Root CA (SBC and Zoom Phone)**

- **DigiCert Intermidiate Cert (this is optional – only required if your server certificate is signed by an intermediate)**
- **DigiCertEVRootCA (Genesys PureCloud)**

Supported CAs for Zoom Phone.

https://support.zoom.us/hc/en-us/articles/360056087612-Zoom-Phone-certificate-update

Supported CA for Genesys PureCloud BYOC

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

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

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

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

Config Parameter	SBC Certificate1(Zoom)	SBC Certificate2(PureCloud)	DigiCertEV RootCA	DigiCert Root CA	DigiCert Intermediate
Name	SBCCert 1	SBCCert 2	PureCloudCert	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA
Common Name	**customers.telechat.o-test06161977.com**	**solutionslab.cgbubedford.com**	PureCloudCert	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA
Key Size	2048	2048	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256	Sha256	Sha256

7.7.1.1 End Entity Certificate

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

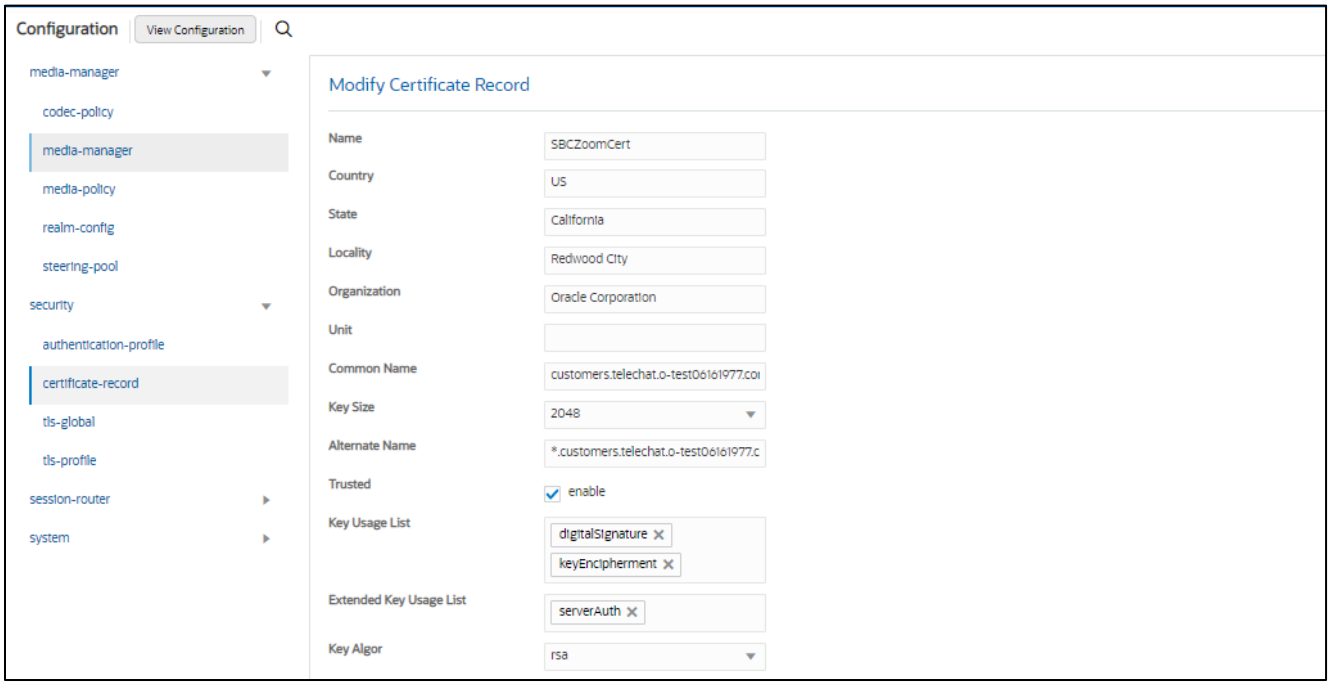
Here in this setup,We wil create two end entity certificates for PureCloud and Zoom Phone.

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

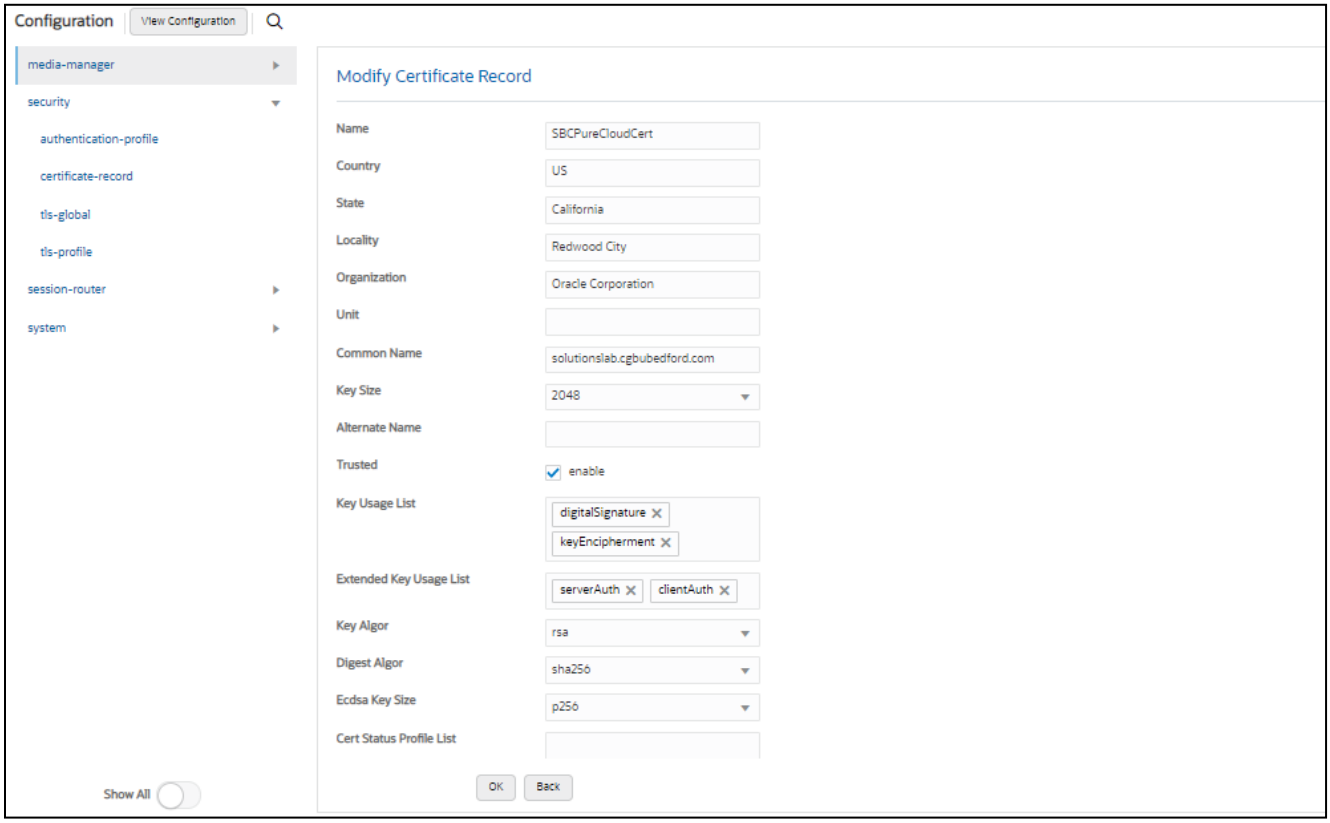
Step 1 Configure SBC Certificate Record

To Configure the certificate record:

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



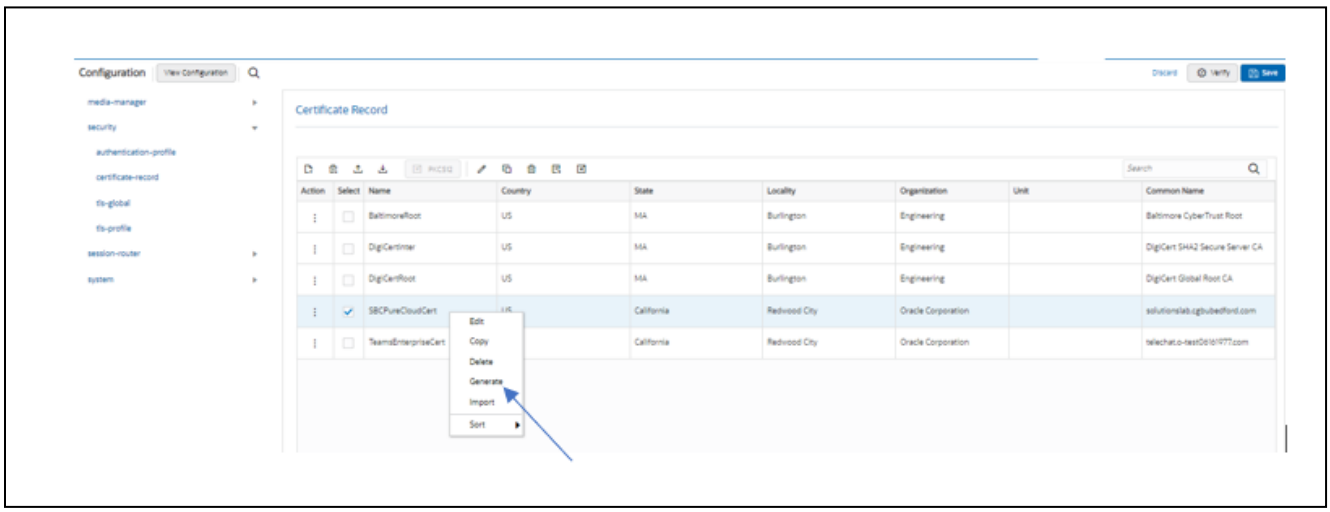
Similarly repeat the step to create another certificate record to present to Genesys PureCloud signed by your CA.

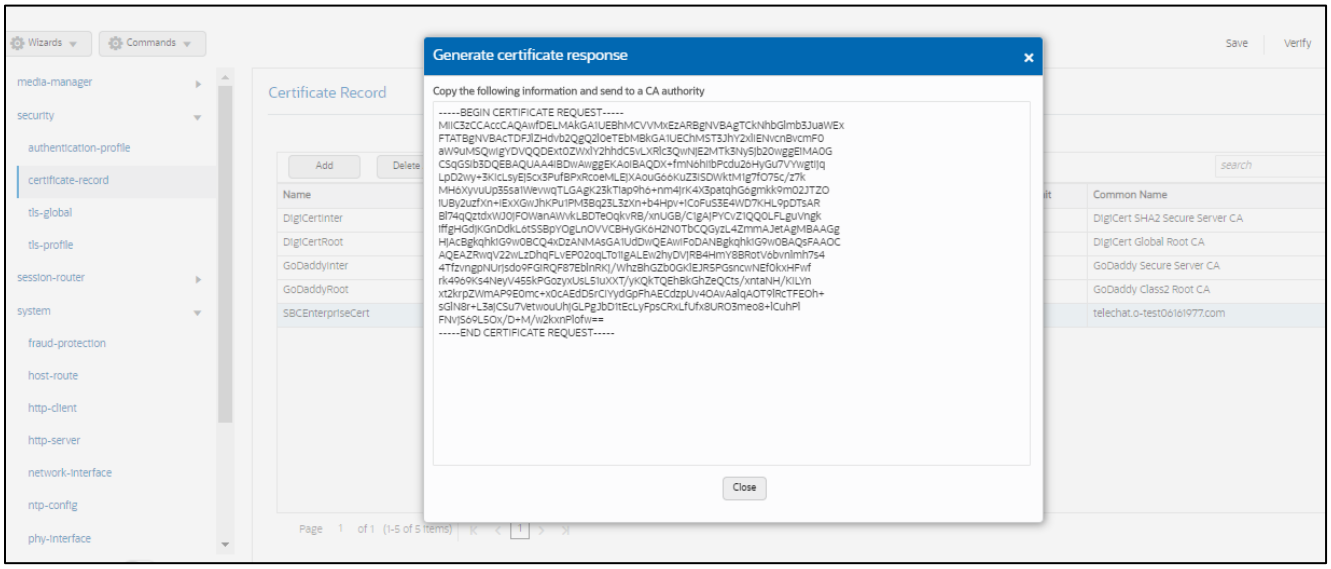


Step 2 – Generating a certificate signing request

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 both Certificate records -SBCZoomCert and SBCPureCloudCert.
- Please copy/paste the text that is printed on the screen as shown below and upload to your CA server for signature.



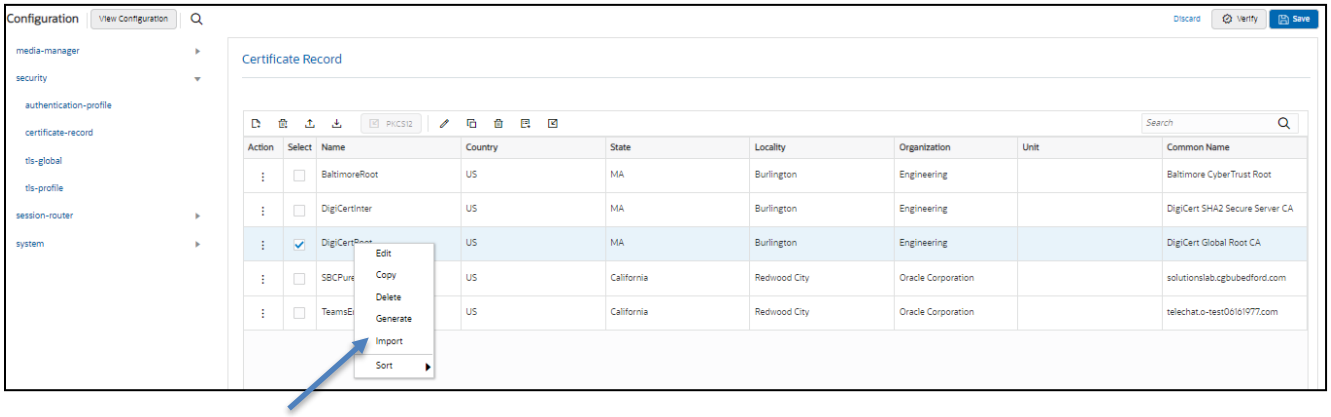


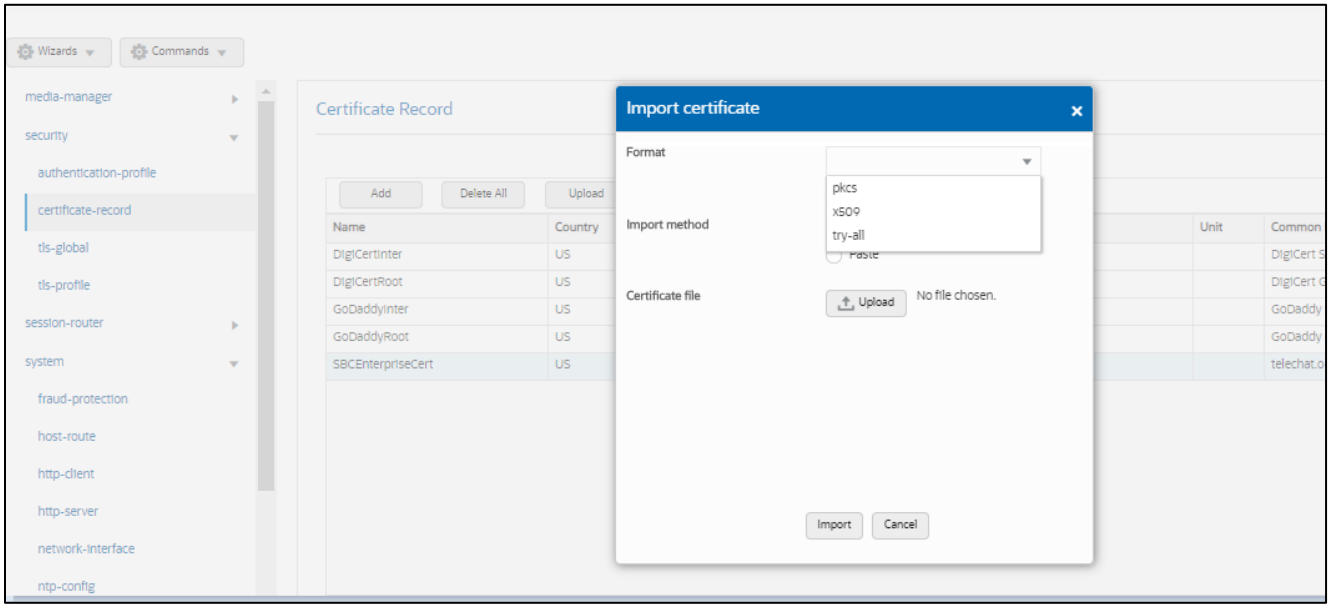
- copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, **a save and activate is required** before you can import the certificates to each certificate record created above.

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





7.7.1.2 Import CA Certificate

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

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

7.8. TLS-Profile

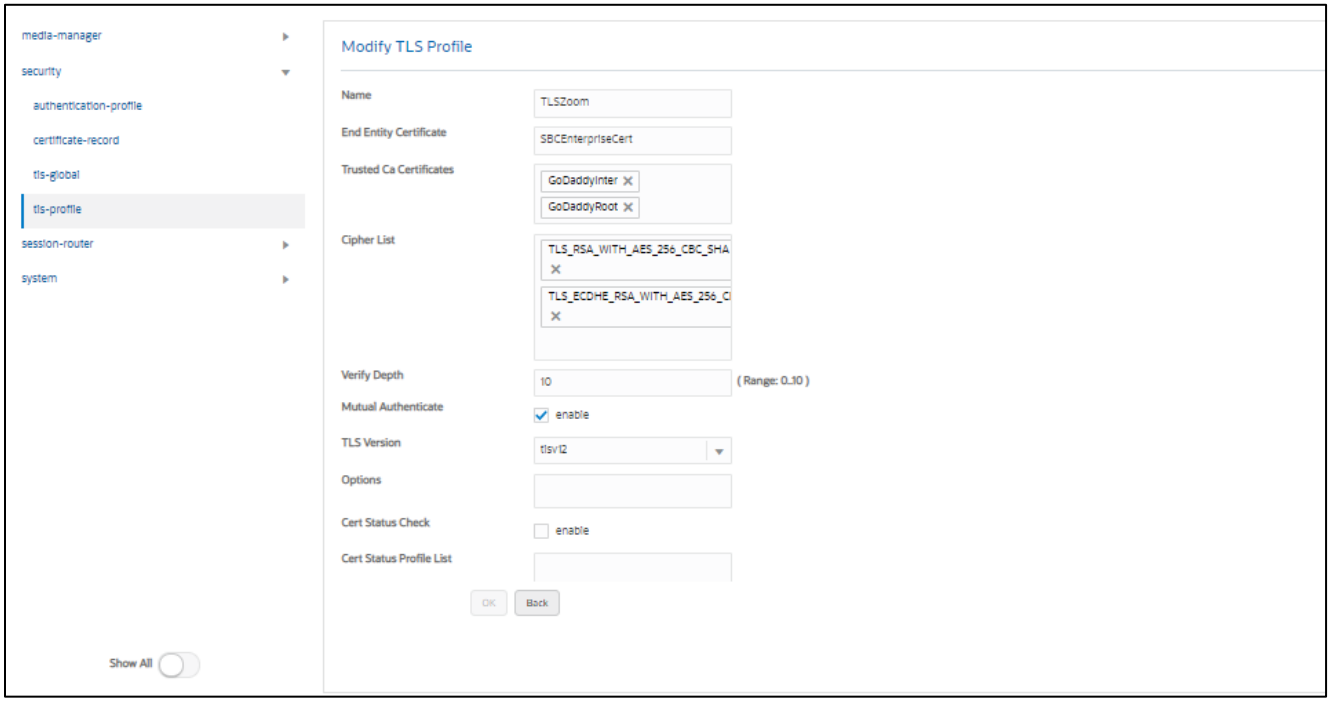
A TLS profile configuration on the SBC allows specific certificates to be assigned.

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

TLS profile -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



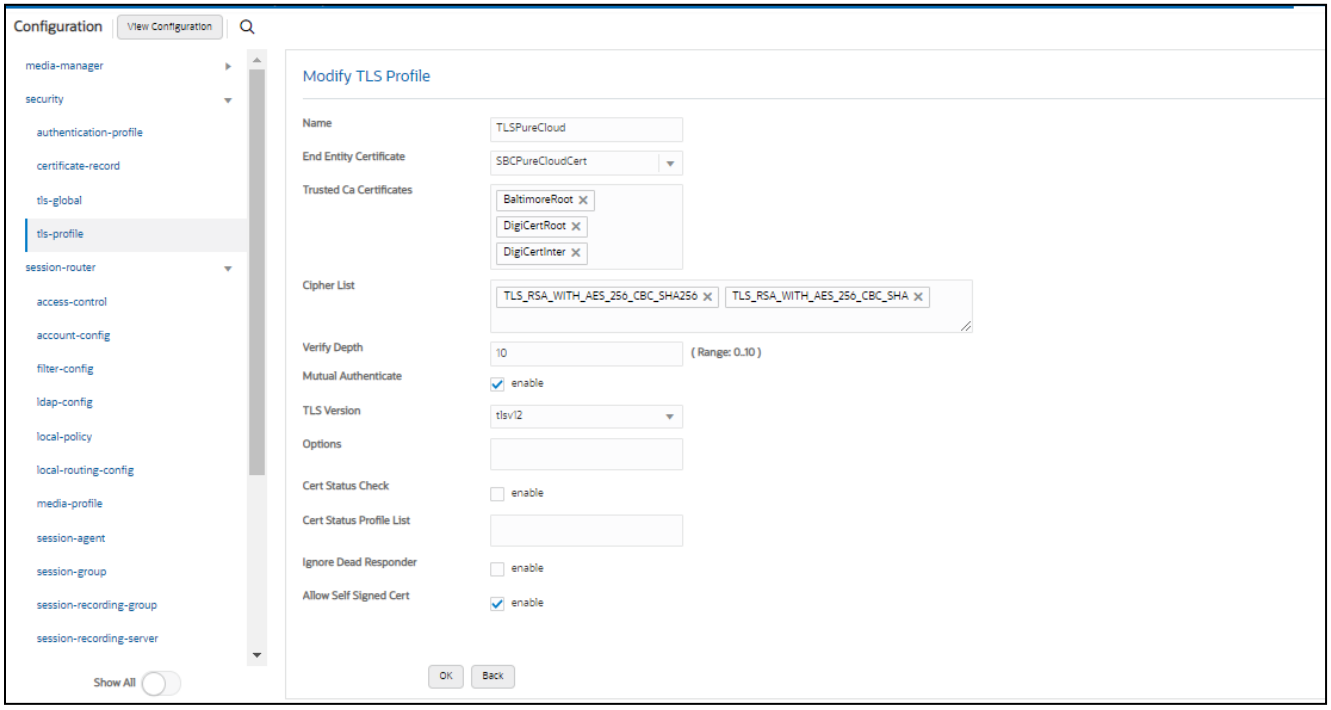
TLS-Profile - Genesys PureCloud

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

Supported TLS ciphers include:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256

TLS-only listeners are available on host port 5061.



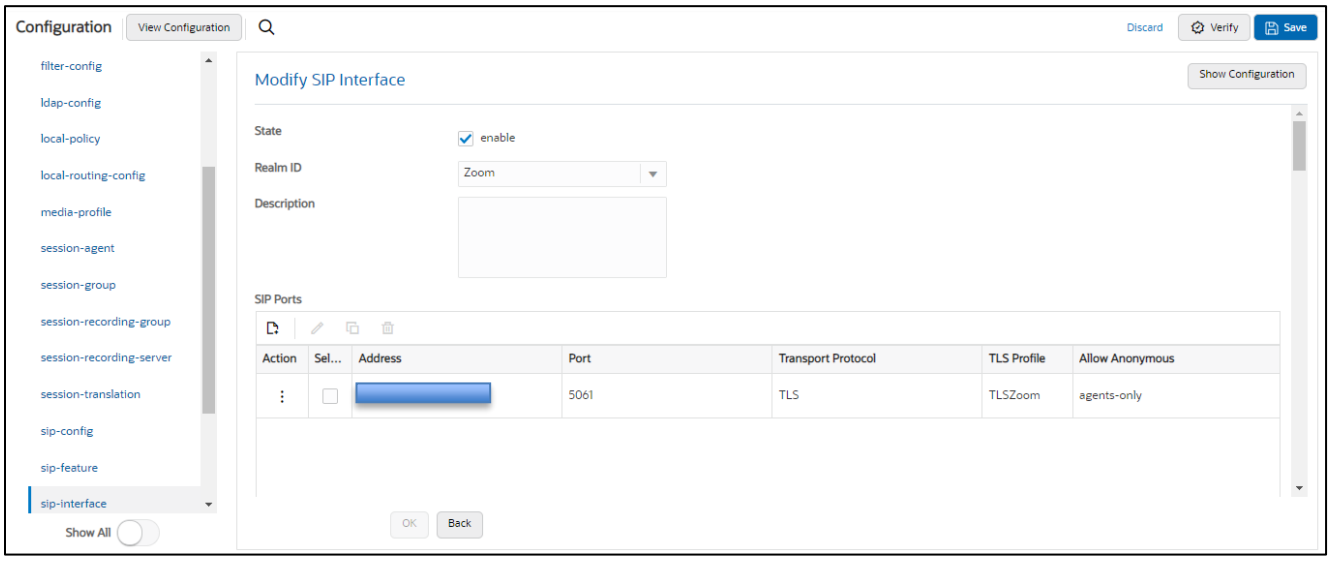
7.9. Configure SIP Interfaces

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

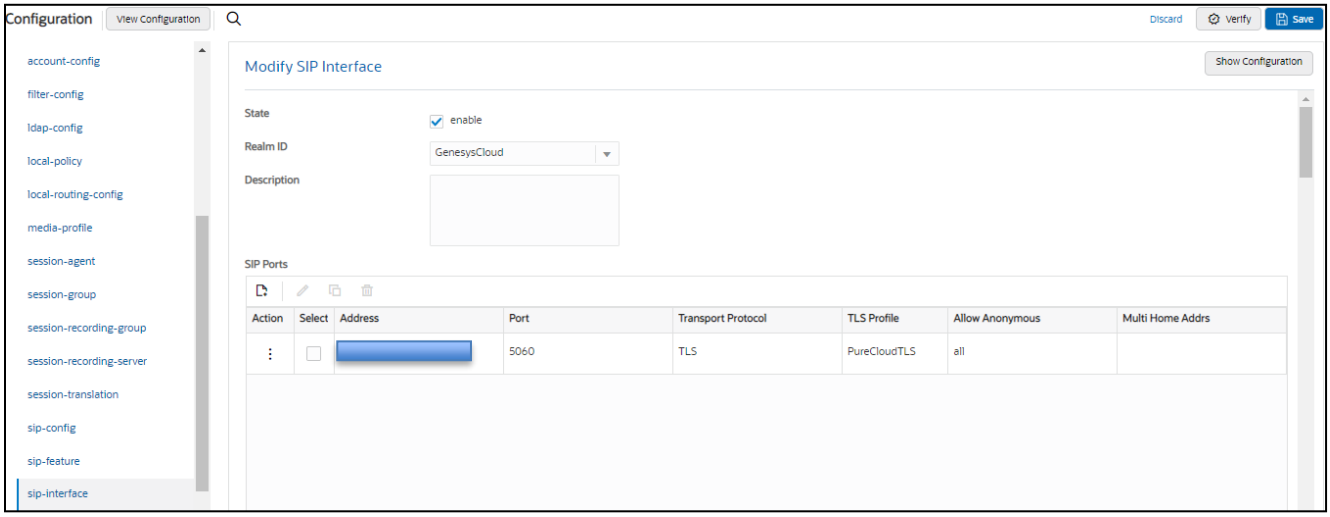
Please Configure sip-interface for the PureCloud as below-

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

Sip-Interface for Zoom Phone



Sip-interface for Genesys PureCloud



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

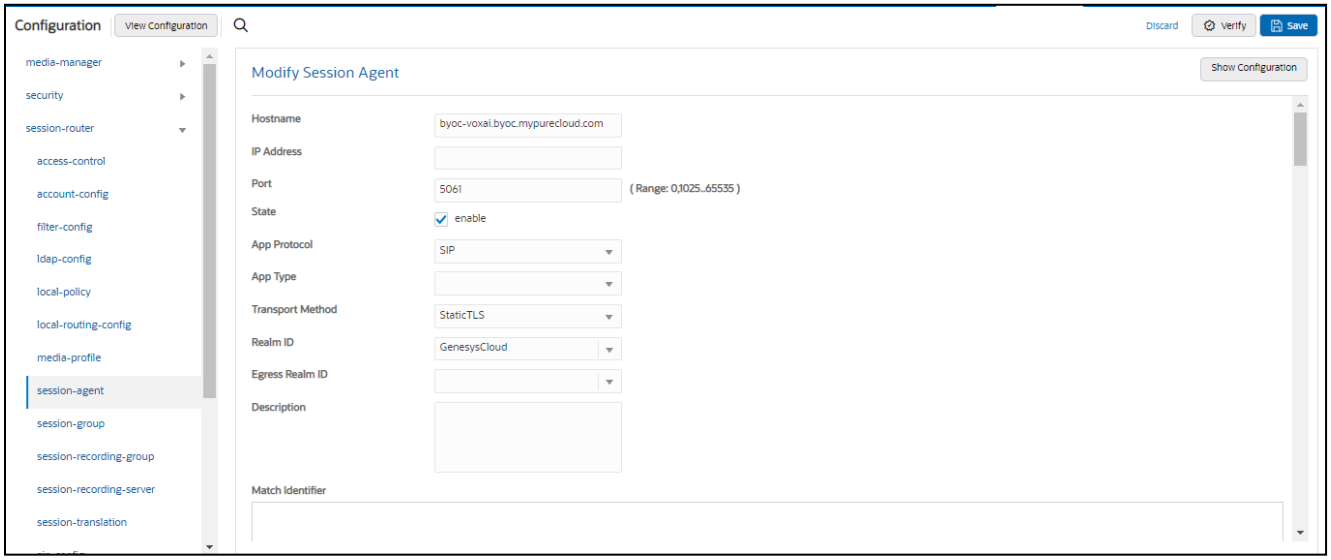
7.10. Configure session-agent

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

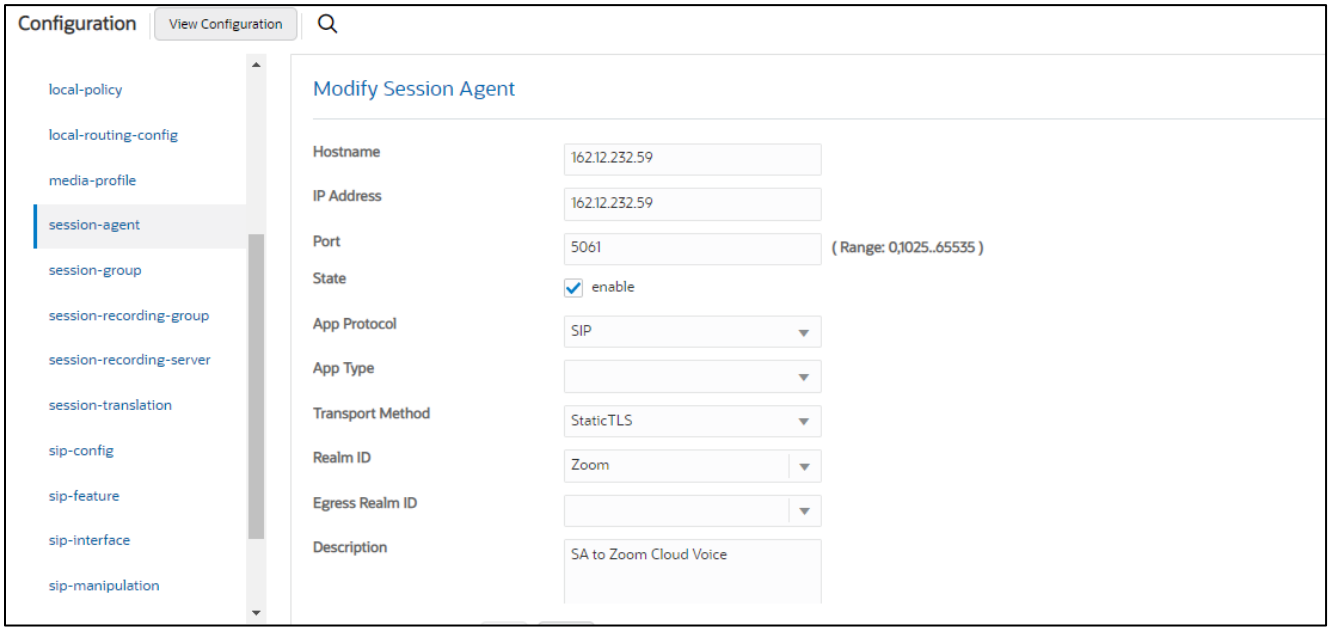
Configure the session-agents for the Genesys Pure Cloud

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



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

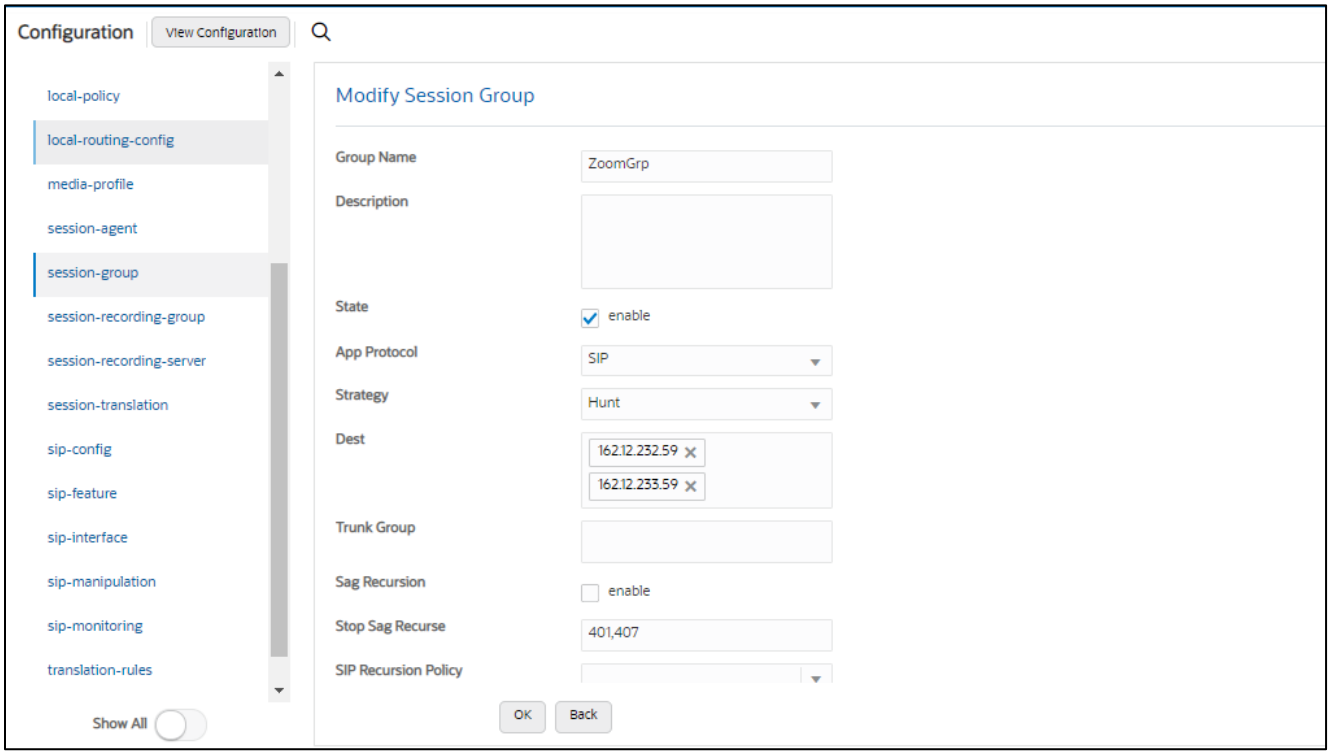


Follow above step to create 1 more session-agent for Other Zoom Session-Agent 162.12.233.59

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



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 PureCloud to Zoom Phone –

Genesys PureCloud → Oracle SBC → Carrier Trunk → Oracle SBC → Zoom Phone

Inbound calls from Zoom Phone to PureCloud -

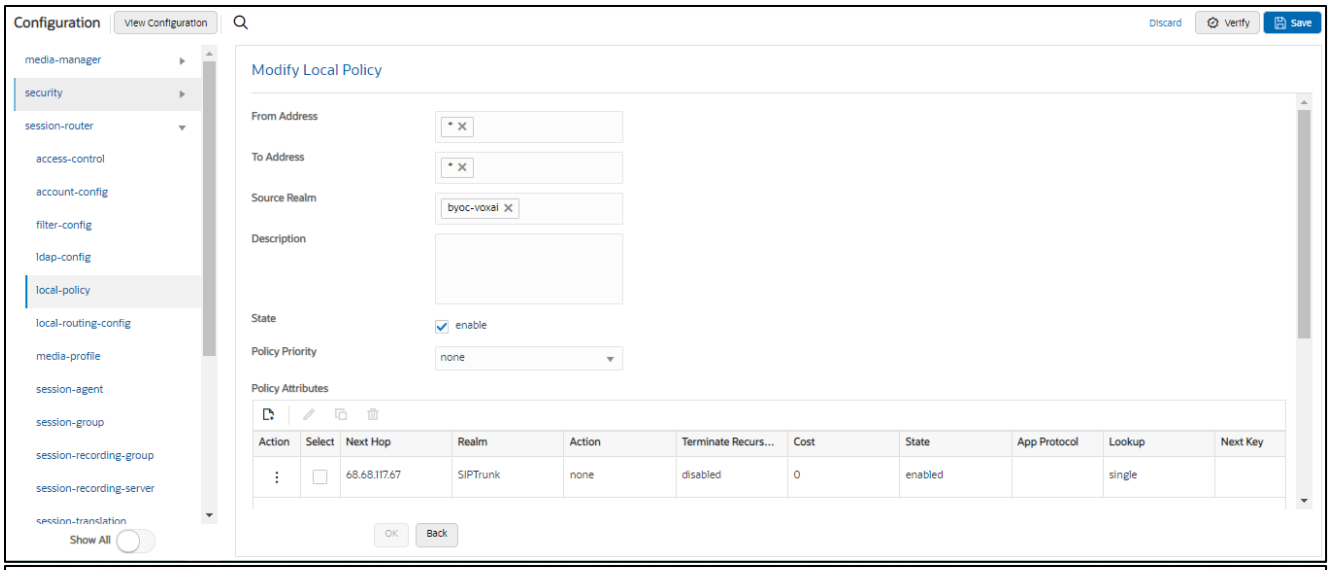
Zoom Phone→ Oracle SBC → Carrier Trunk → Oracle SBC → Genesys PureCloud

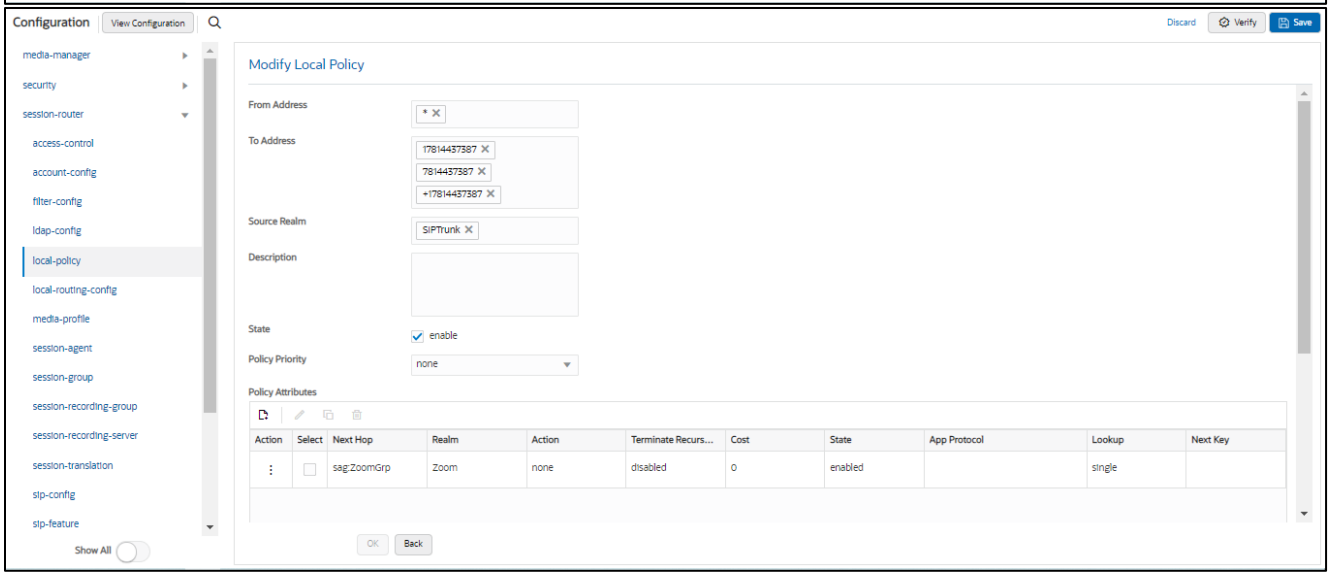
We have multiple application Notes available on the Oracle TechNet Page to configure the Oracle SBC with different PBXs and Twilio Elastic SIP Trunk.

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

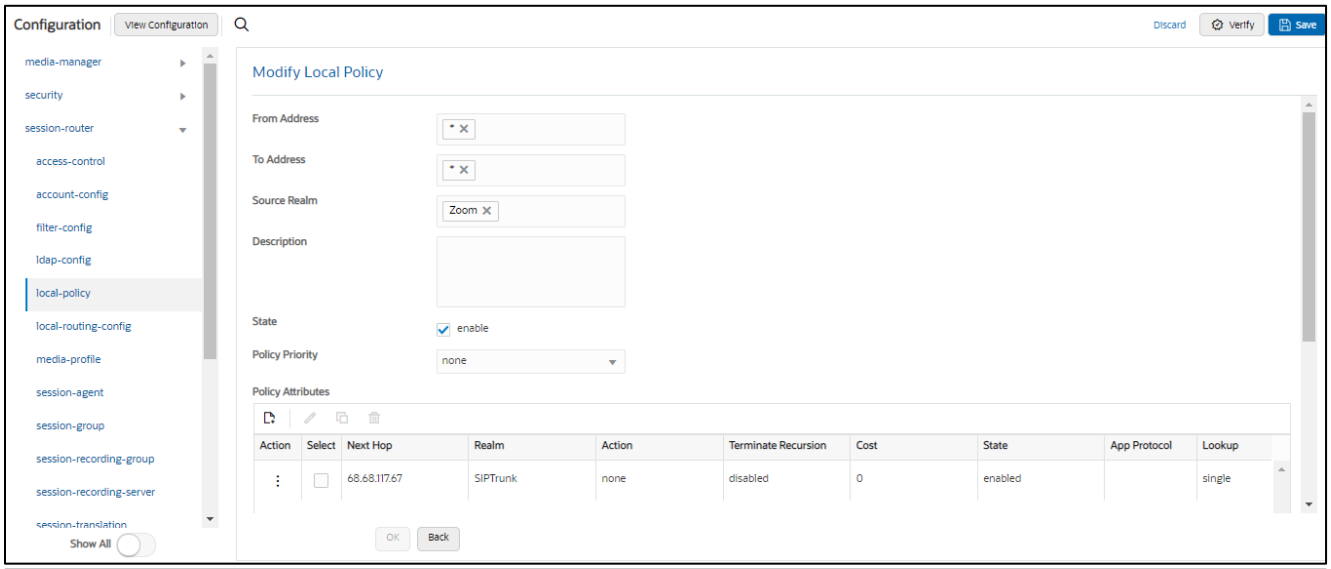
https://www.oracle.com/a/otn/docs/oracle-sbc-with-genesys-pure-cloud-and-twillio-sip-trunk.pdf

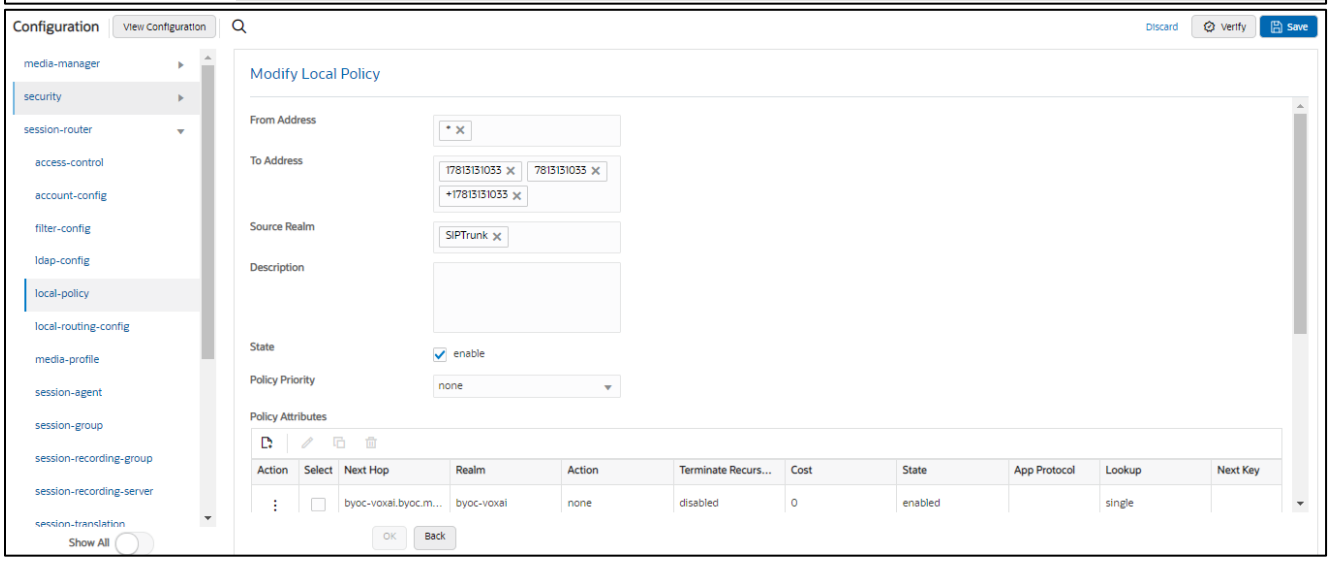
Following **local-policy routes the calls from the Genesys PureCloud** to Carrier and then the calls are routed from Carrier to Zoom Phone.





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

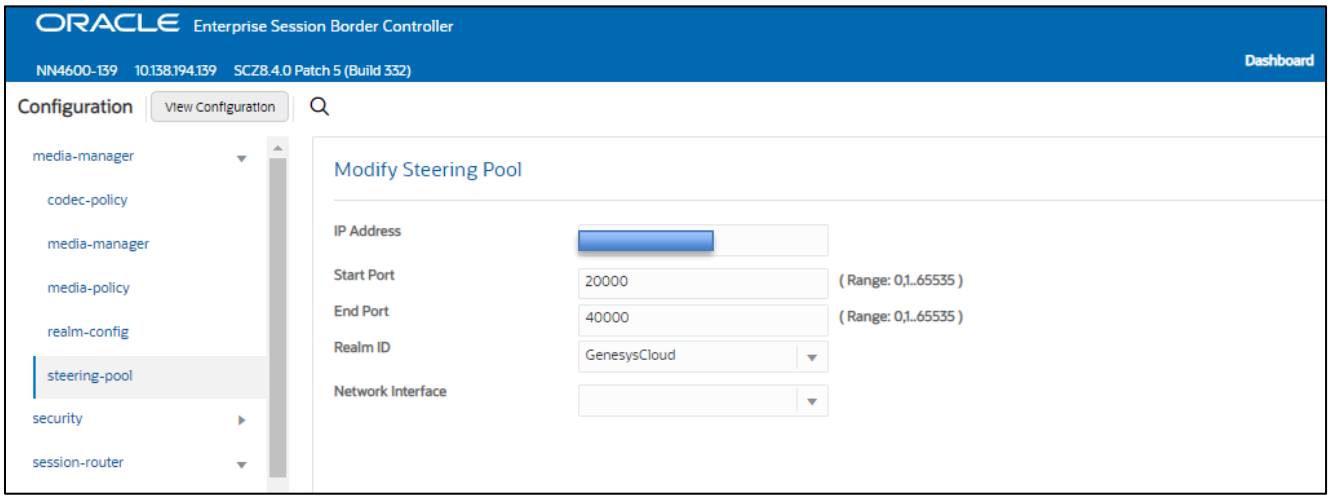




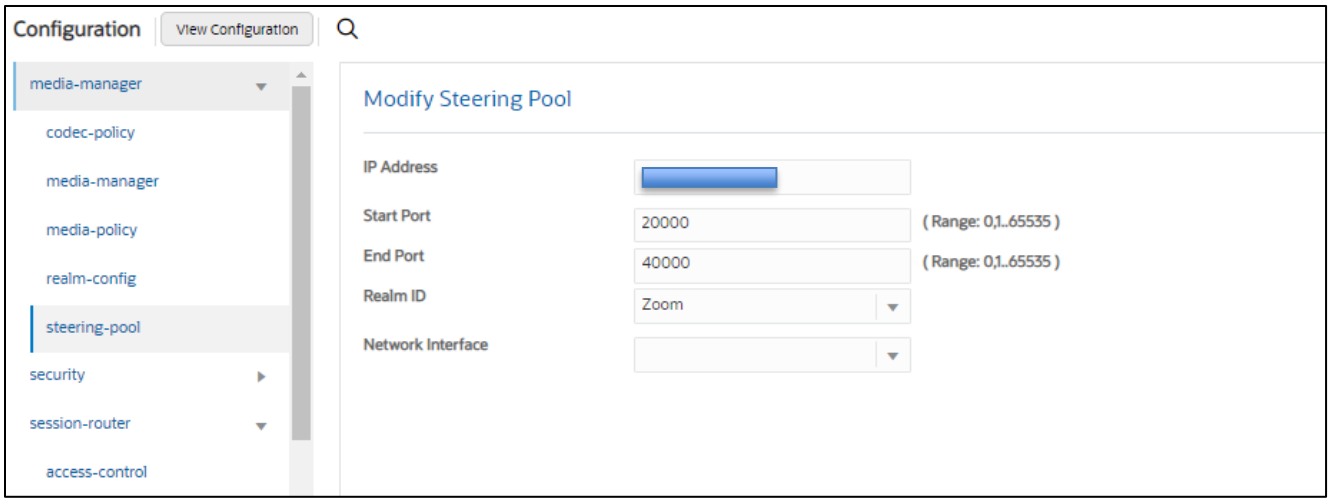
7.13. Configure steering-pool

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

PureCloud Steering pool.



Zoom Phone Steering Pool



7.14. Configure additional Parameters

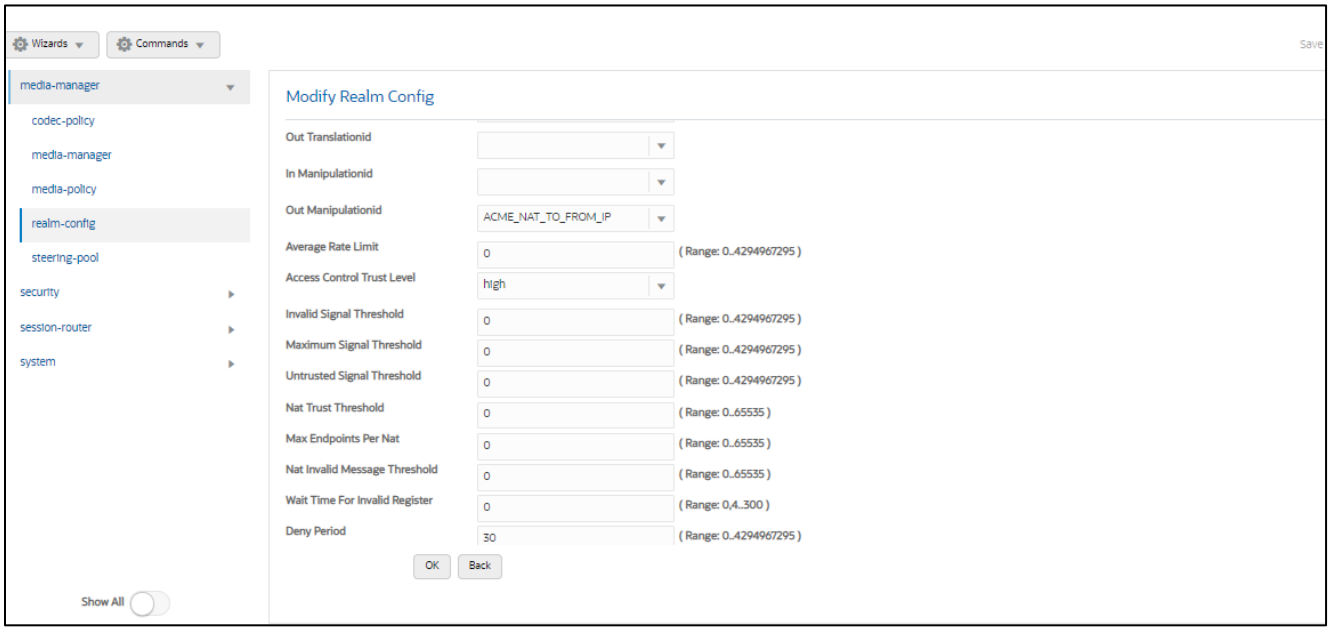
7.14.1 SIP Manipulations

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:

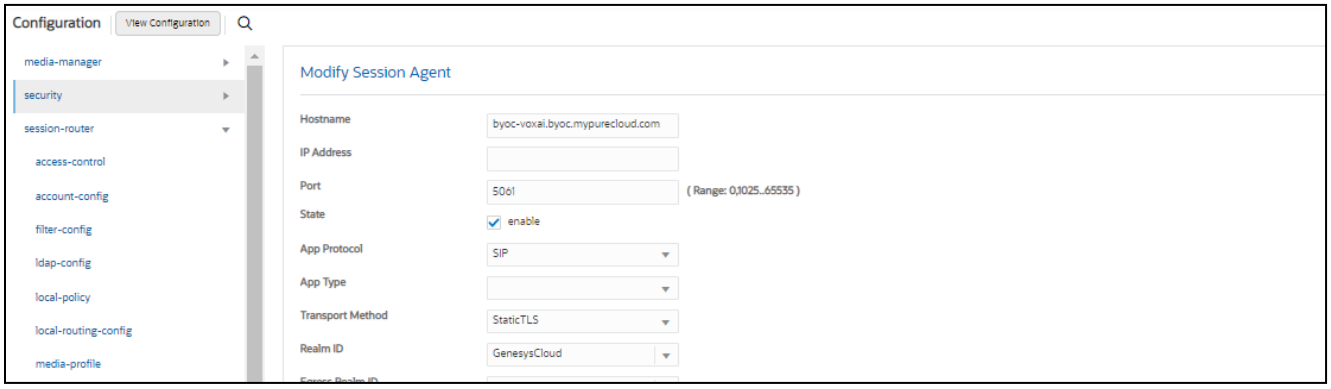
The manipulation performs the following modifications to SIP packets

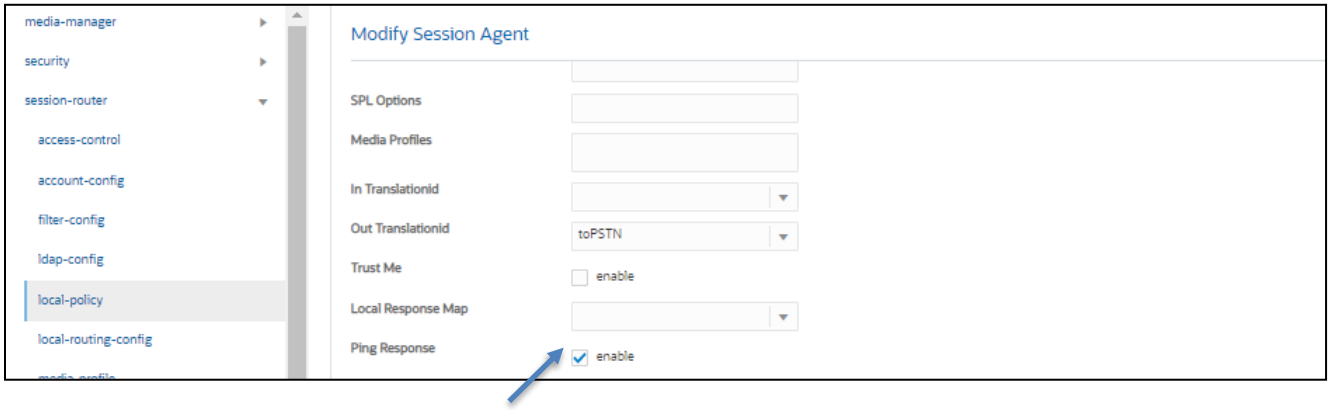
1. Changes the host portion of From address with the SBC sip-interface IP Address.
2. Changes the host portion of To Header with Zoom IP Address.



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 PureCloud .
Below is an example of the parameter **Ping response** enabled on PureCloud Session-Agent. Similarly, the parameter should be enabled for other Zoom Phone Session-Agents.



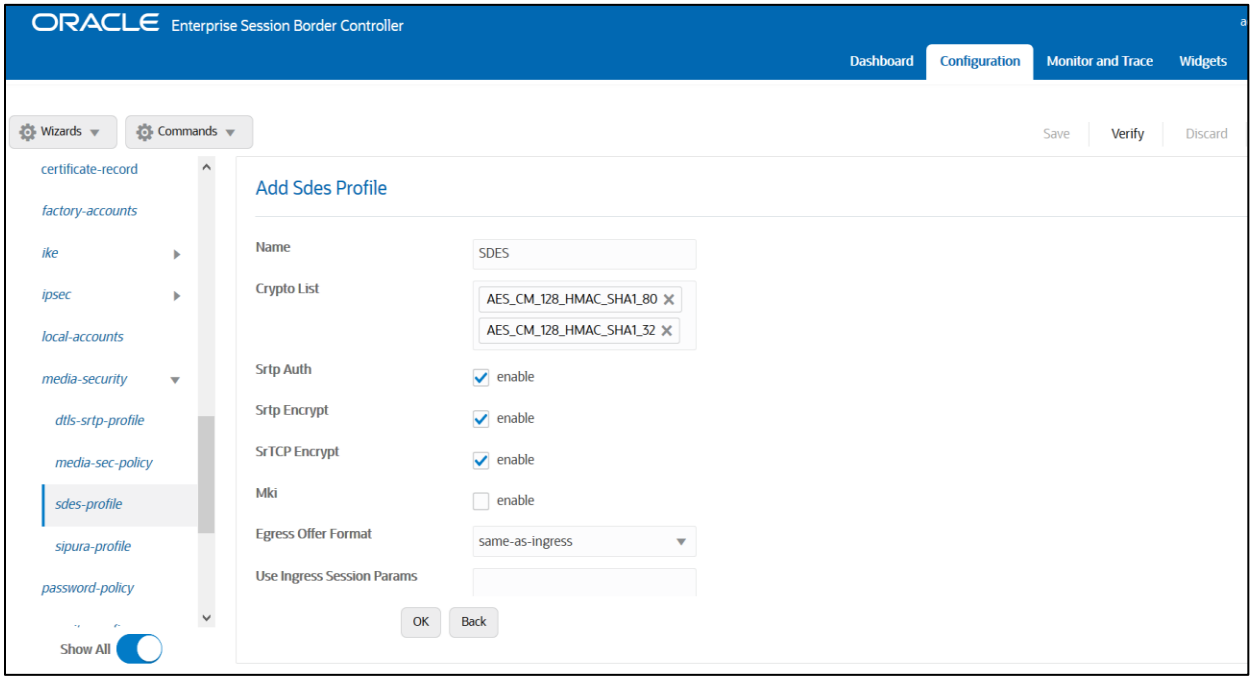


7.15. Media Security Configuration.

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

7.15.1 Configure sdes profile

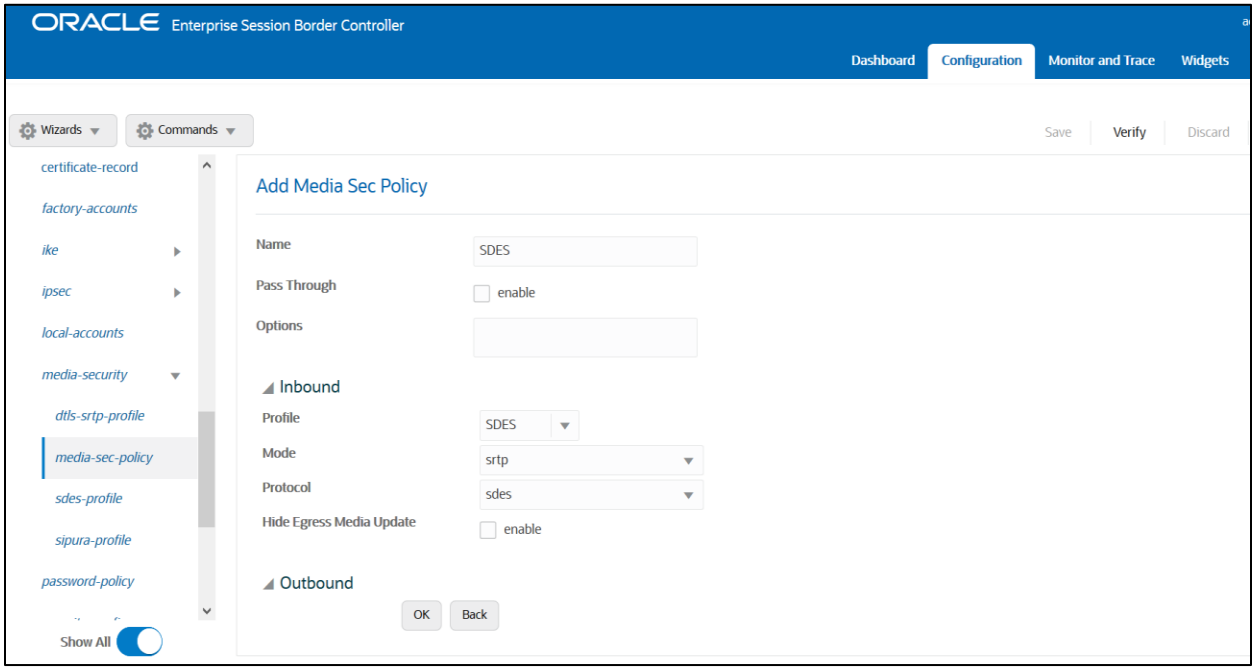
Navigate to →Security → Media Security →sdes profile and create the policy as below.



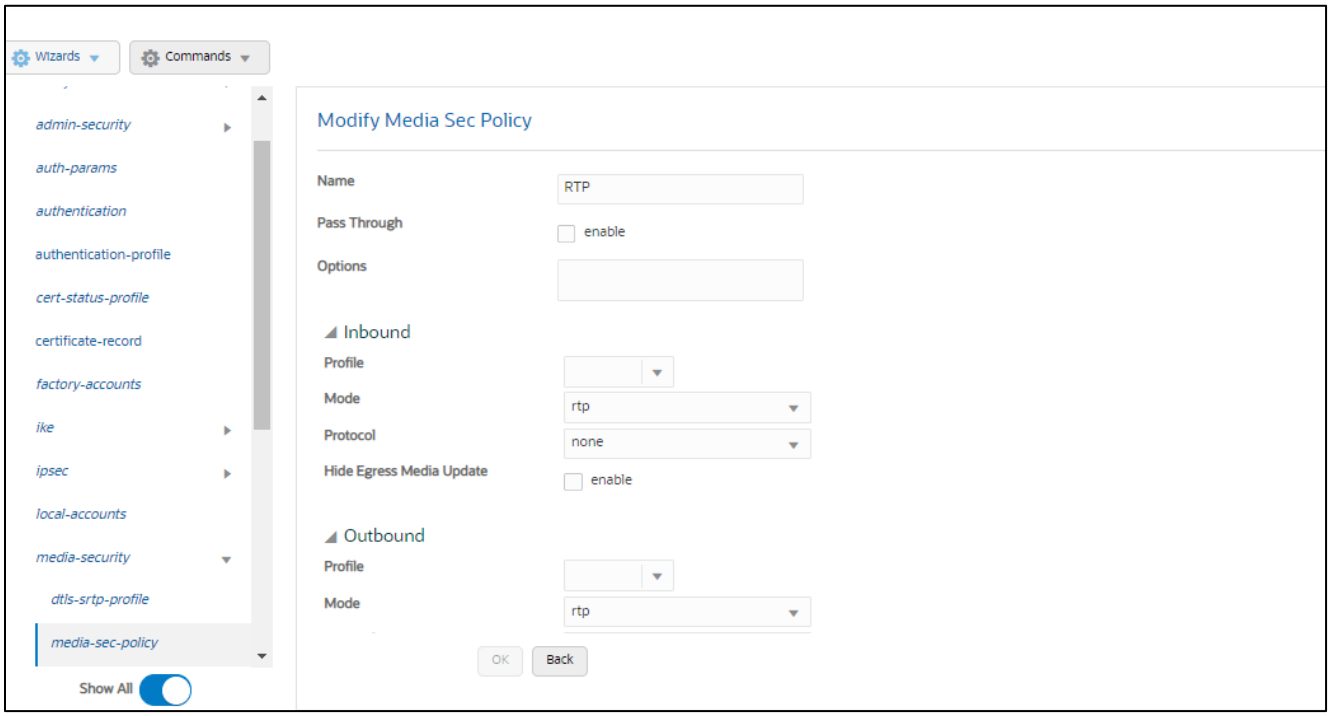
7.15.2. Configure Media Security Profile

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 PureCloud and Zoom Phone Realm.



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



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

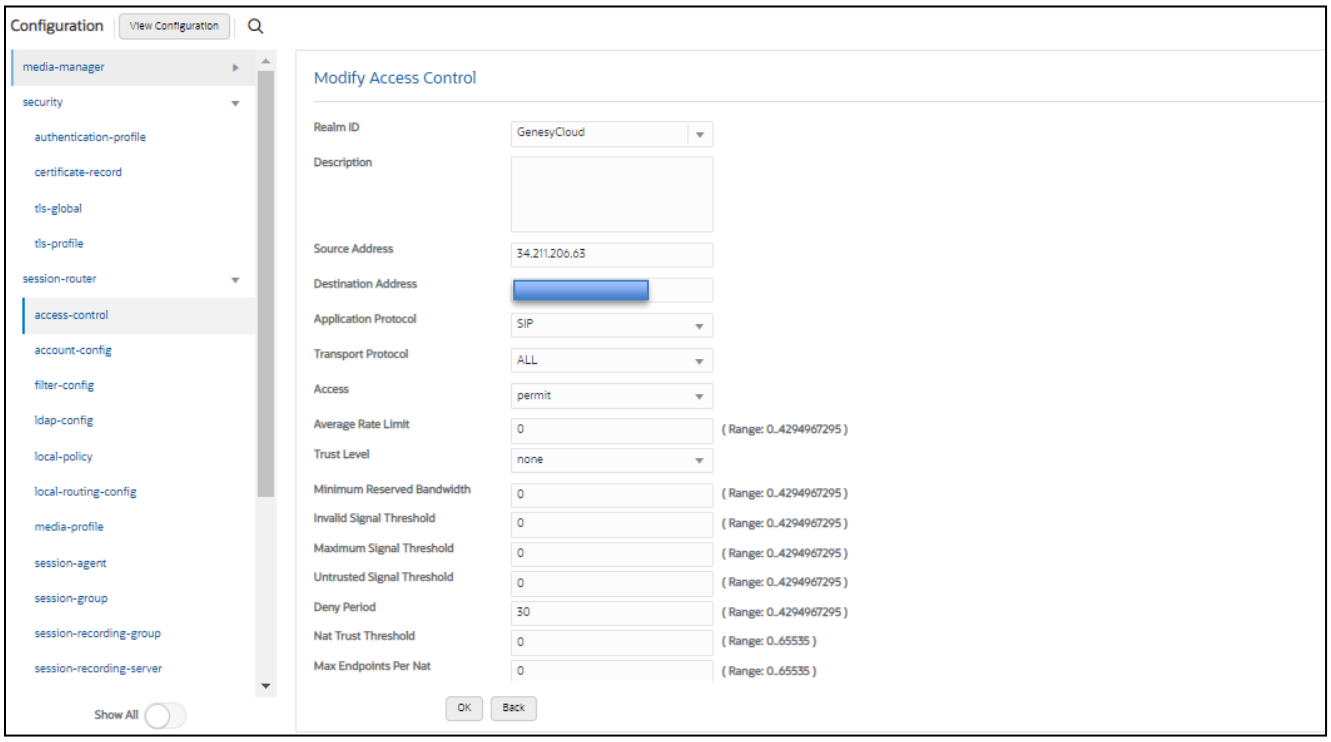
GUI Path: session-router/access-control

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

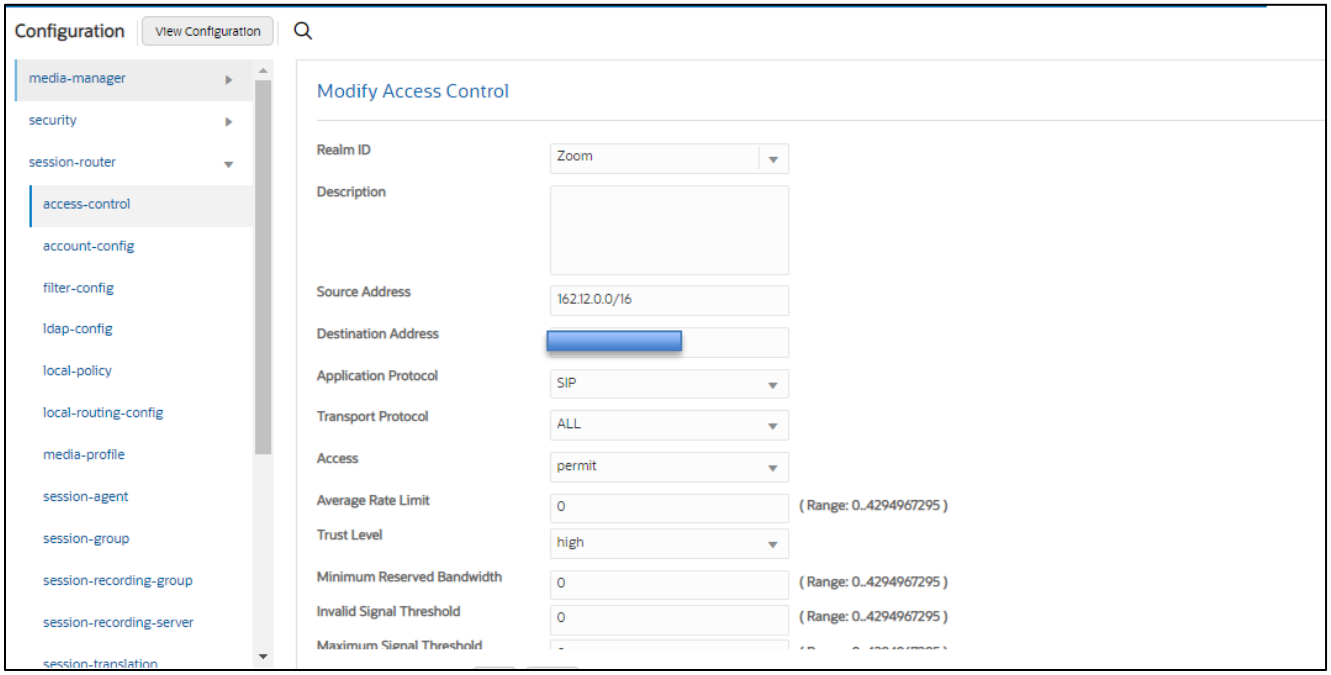
byoc.mypurecloud.com resolves to the following load balancer IP Addresses

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

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



Similarly create ACL entries for each Zoom Phone IP Addresses as shown in the below example.



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.

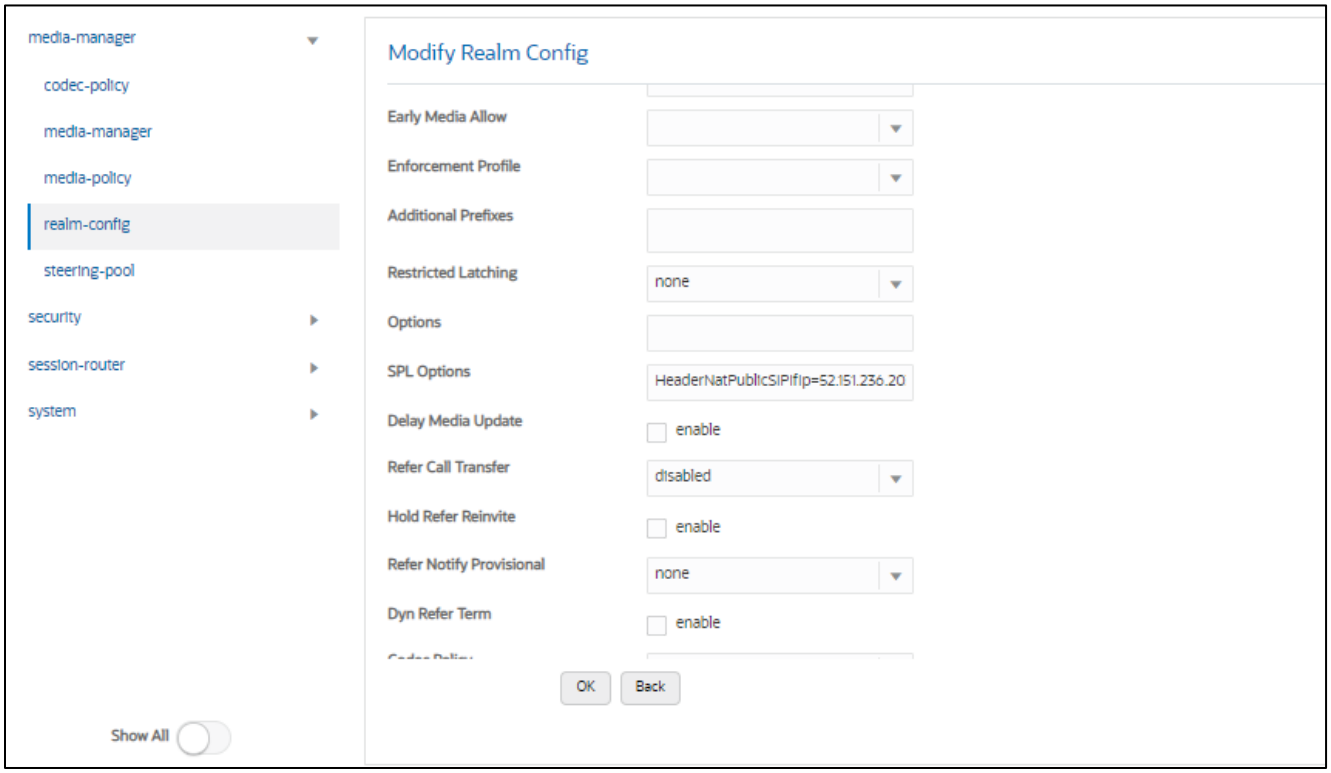
- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

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.



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 PureCloud. 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 PureCloud supported CA to sign certificate once CSR is generated by the SBC.

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

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

Initial GUI Access

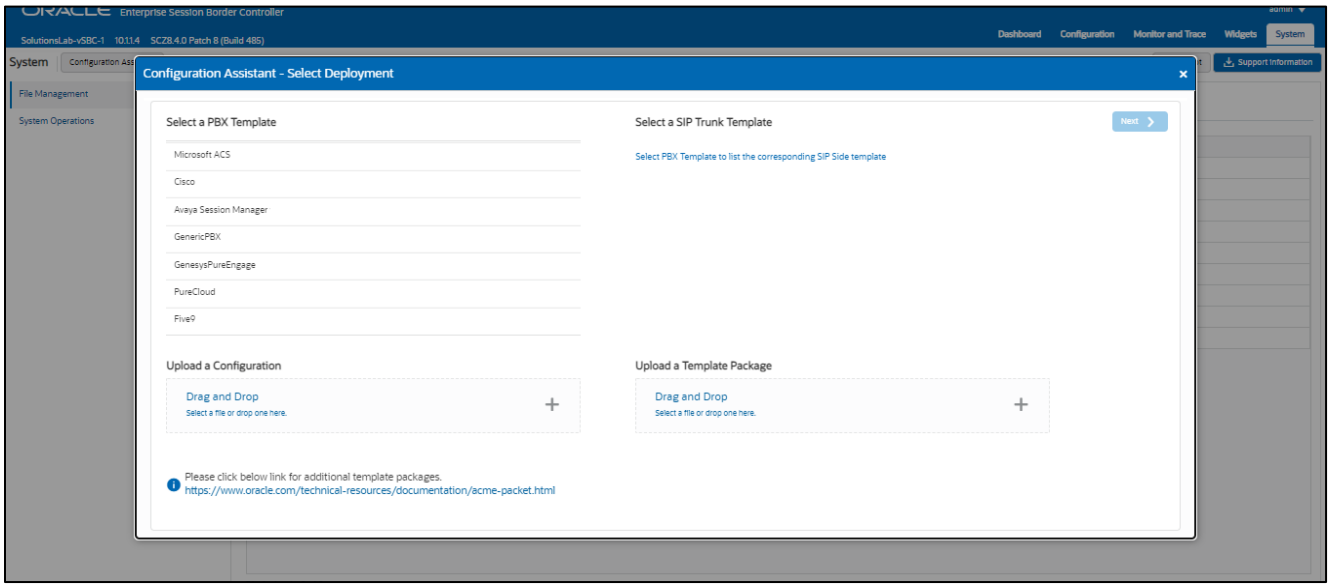
The Oracle SBC WebGui can be accessed by entering the following in your web browser.
http(s)://<SBC Management IP>.

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

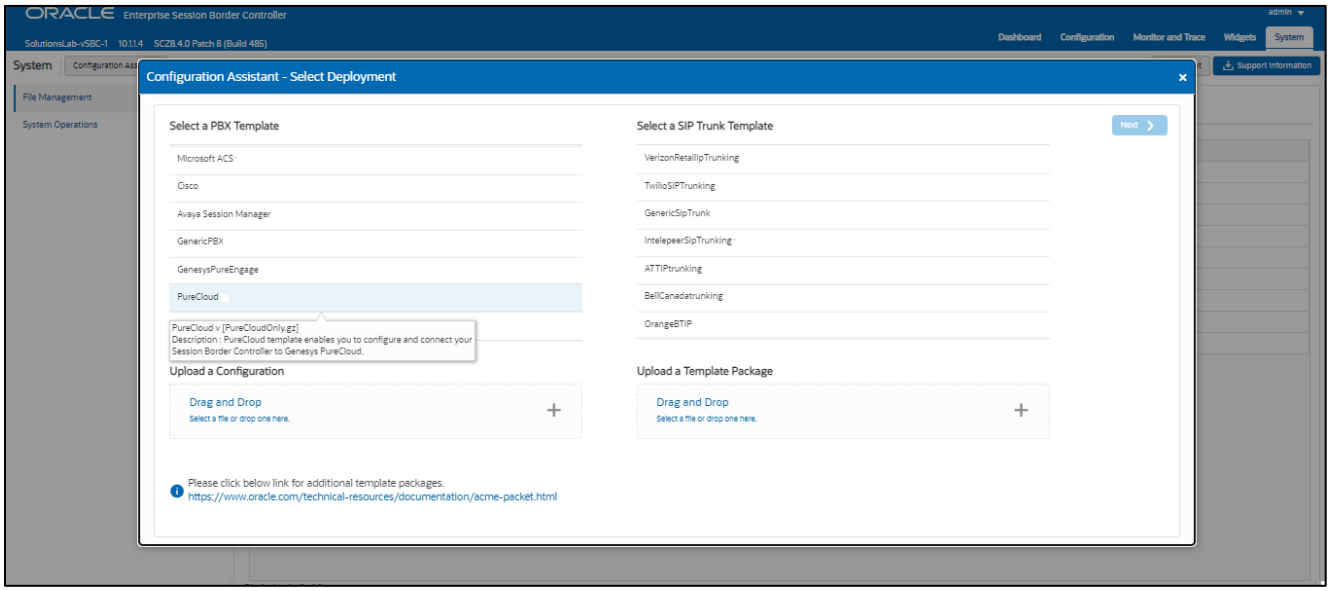
If there is no configuration on the SBC, the configuration assistant will show immediately upon login to the SBC GUI as shown below

PureCloud Configuration Assistant

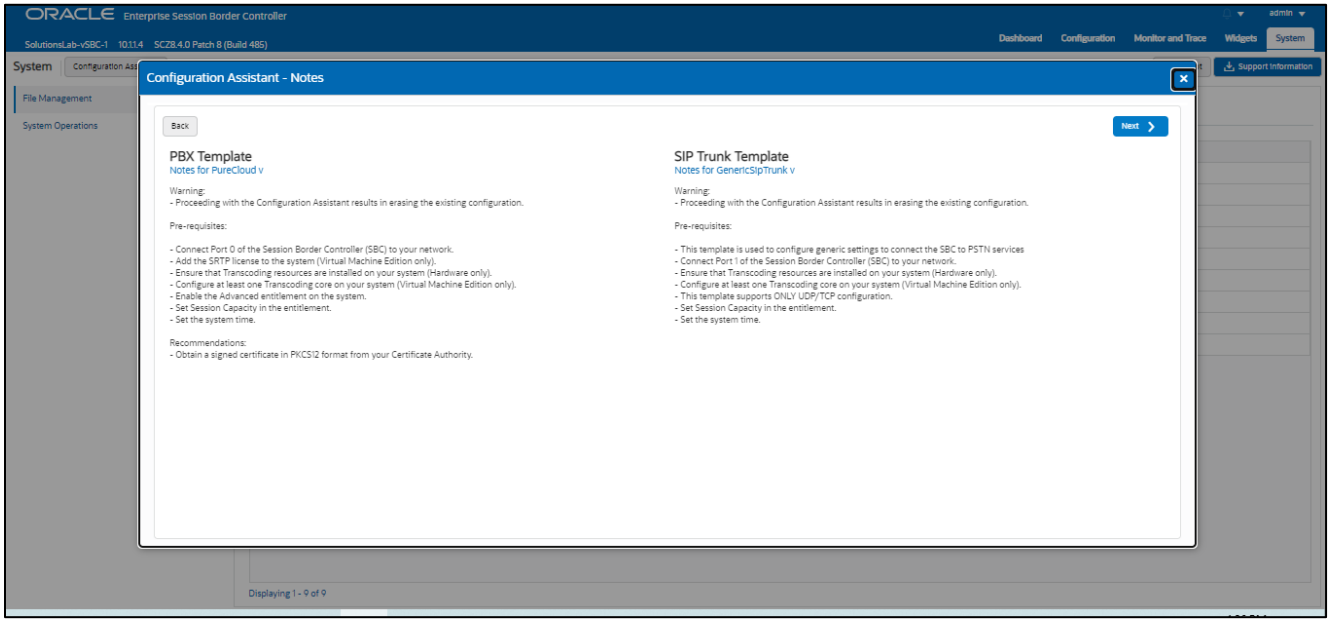
For a new SBC deployment, once access to the GUI is configured, you will see the following when logging in for the first time:



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



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:



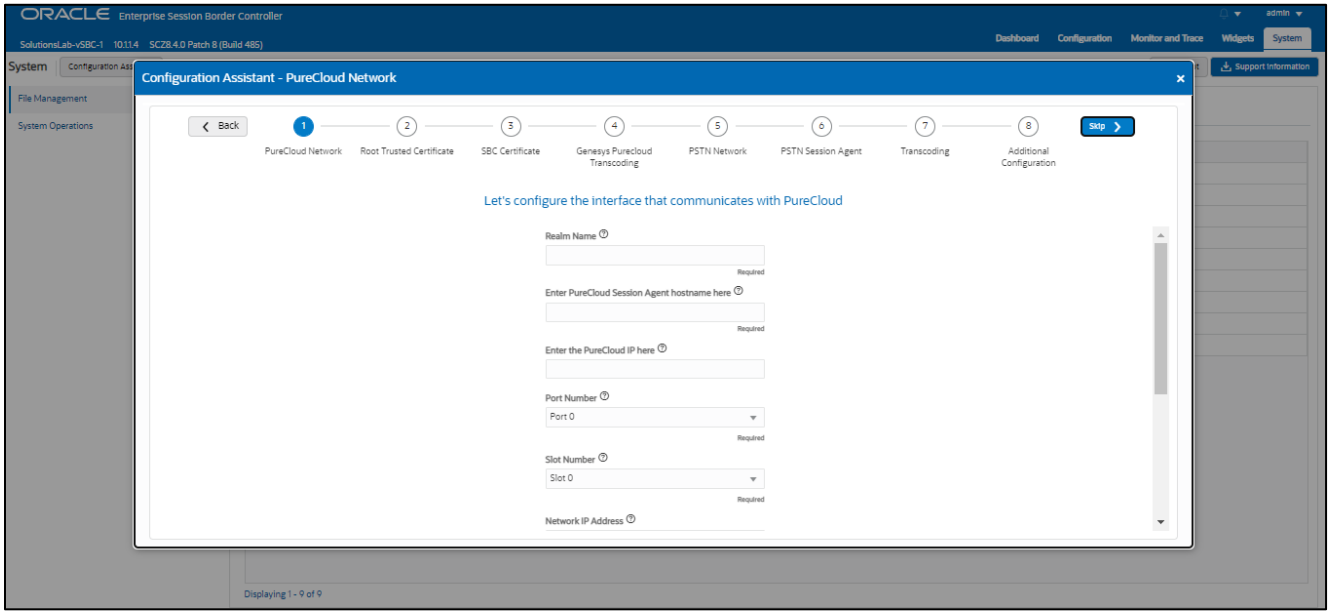
Clicking “Next” on the Notes page triggers the configuration assistant to do a system check. This ensures that all of the system requirements for the platform and sip trunk you have selected have been met before proceeding to configuration pages. If they have not been met, you will be greeted by a page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

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

Page 1- PureCloud Network

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

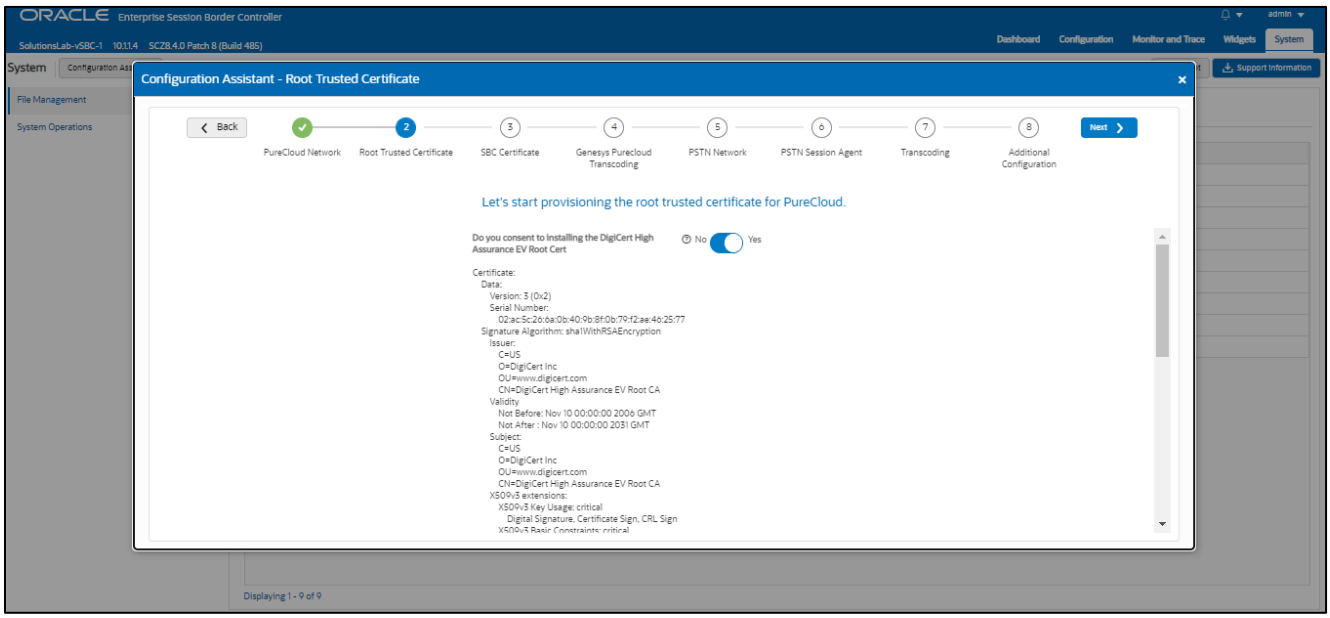
Next to each field is a help icon. If you hover over the icon, you will be provided with a description or definition of each filed. Also, pay close attention to which fields are listed as “required”.



Page 2 - Import DigiCert Trusted CA Certificate for PureCloud

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

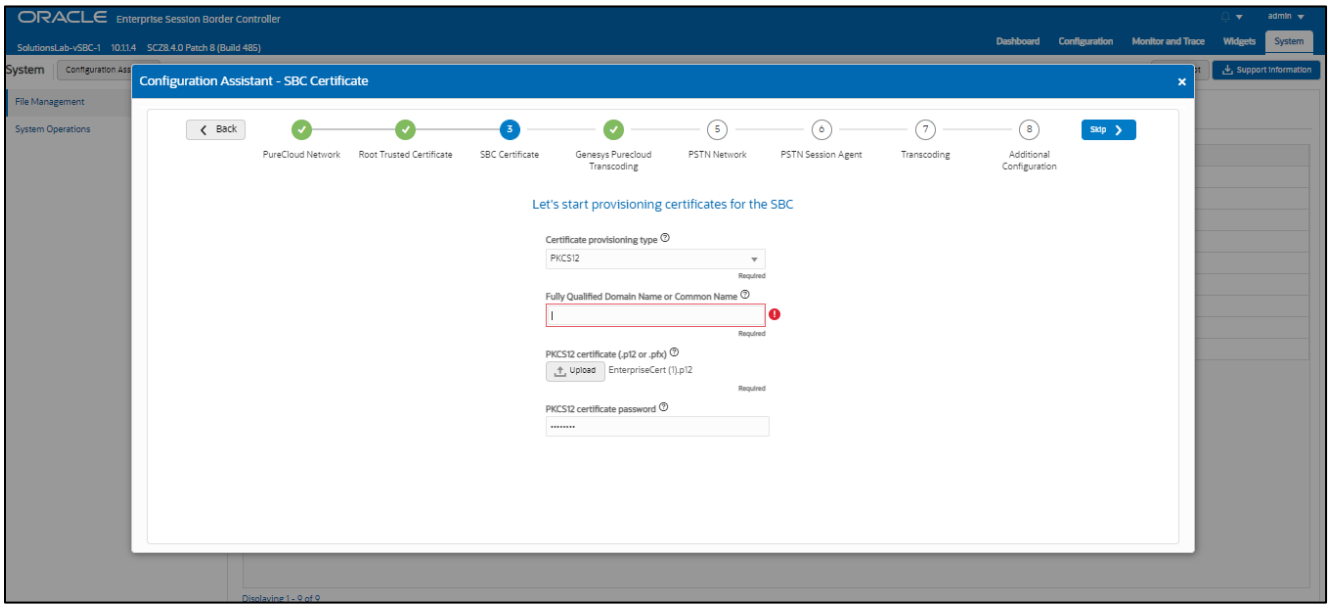
Importing the PureCloud Root CA certs is enabled by default.



Page 3 - SBC Certificates for PureCloud side

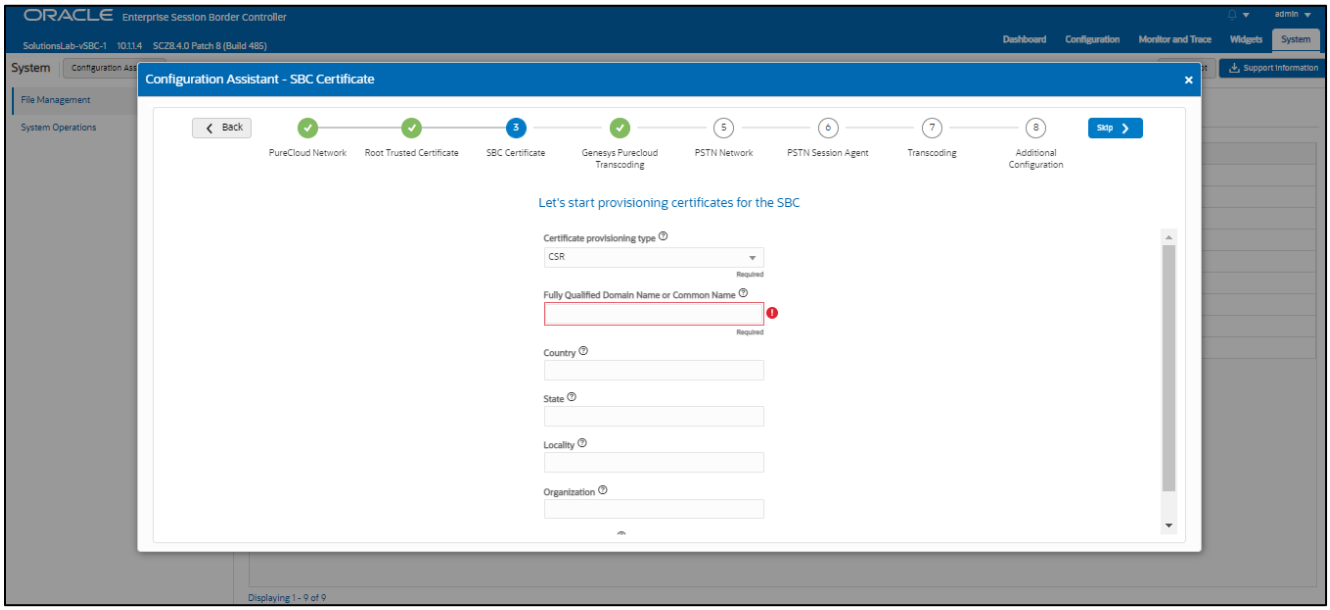
By default, the SBC is set to import a certificate in PKCS12 format. This is the simplest and recommended way to add a certificate to the Oracle SBC. Using this method, you will add the SBC's hostname under "FQDN or

Common Name” field, upload a certificate signed from one of the PureCloud Supported CA Vendors, and enter the certificates password.



Certificate Signing Request (CSR)

The alternative to importing a PKCS12 certificate to the SBC is to configure a certificate and generate a certificate signing request that you will have signed by a PureCloud supported CA. Same as PKCS12, you will enter the SBC’s hostname under “FQDN or Common Name” and “Country” field (required) and answer the remaining question presented on this page (optional).

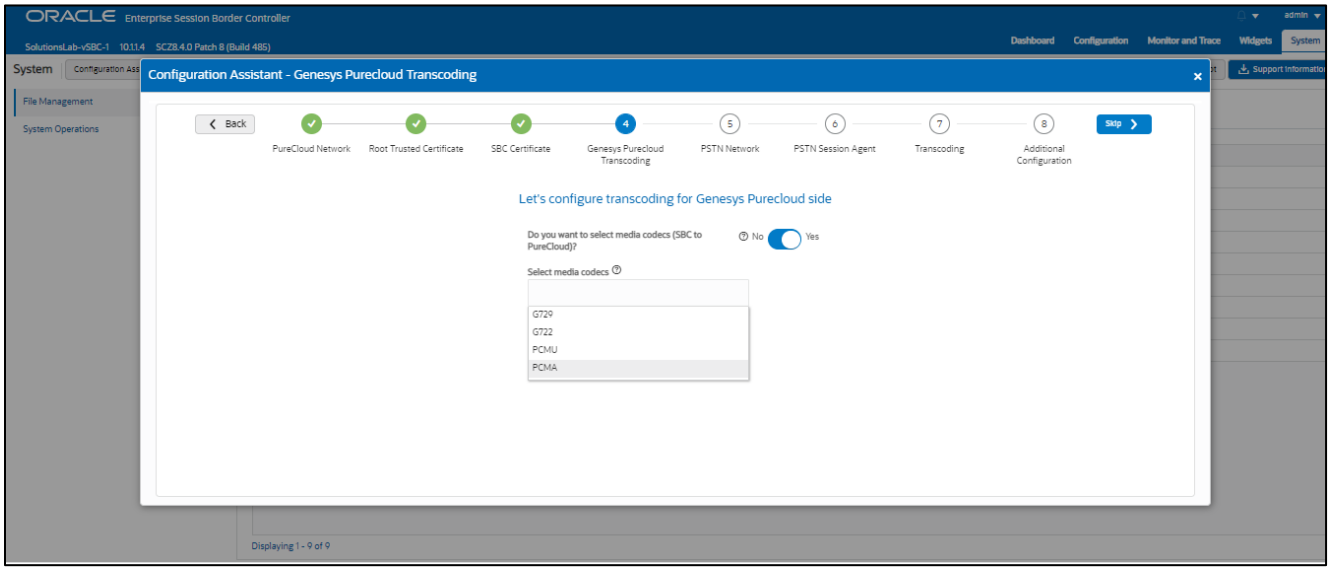


Page 4 – PureCloud side Transcoding

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

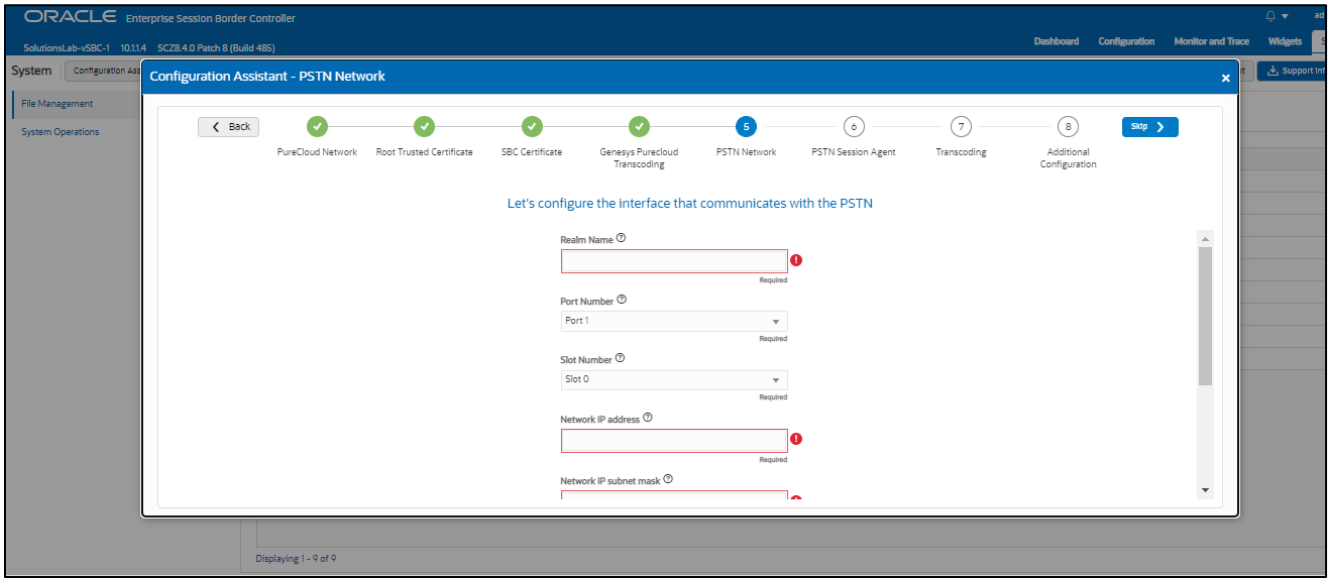
Once transcoding features is set to “yes”, you will then have an option to select additional media codecs you want included in offers/answers toward PureCloud. If you select yes to either question regarding media codecs, you will be presented with a required drop down.

You can select as many codecs from the list presented.



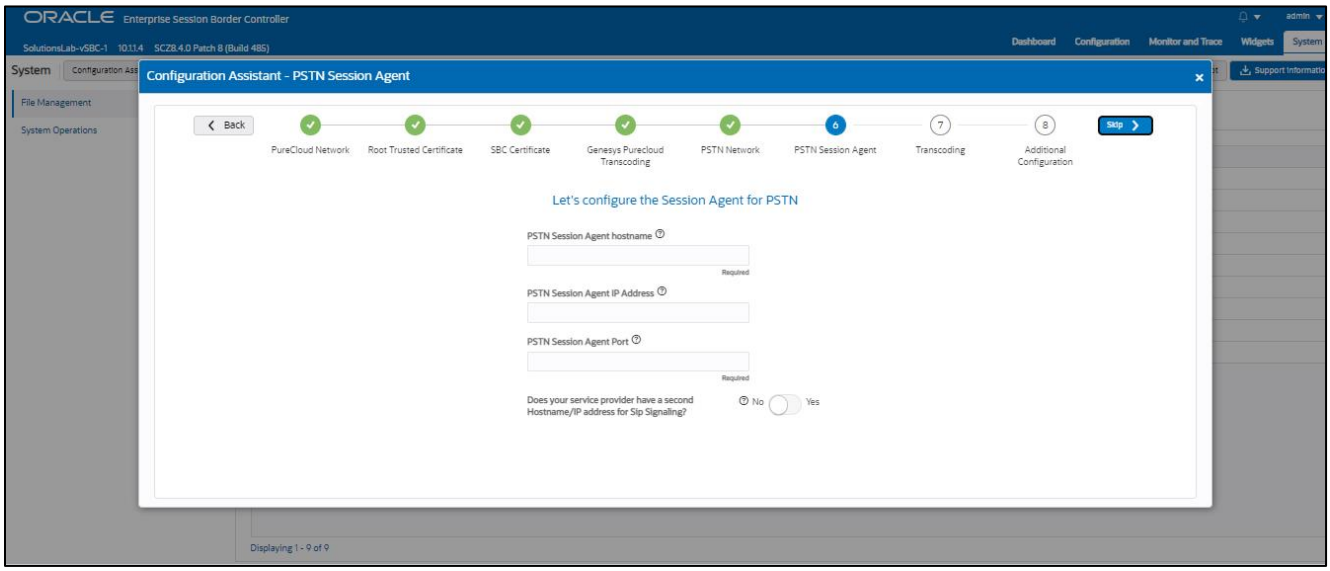
Page 5 – PSTN Sip Trunk Network

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.



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.

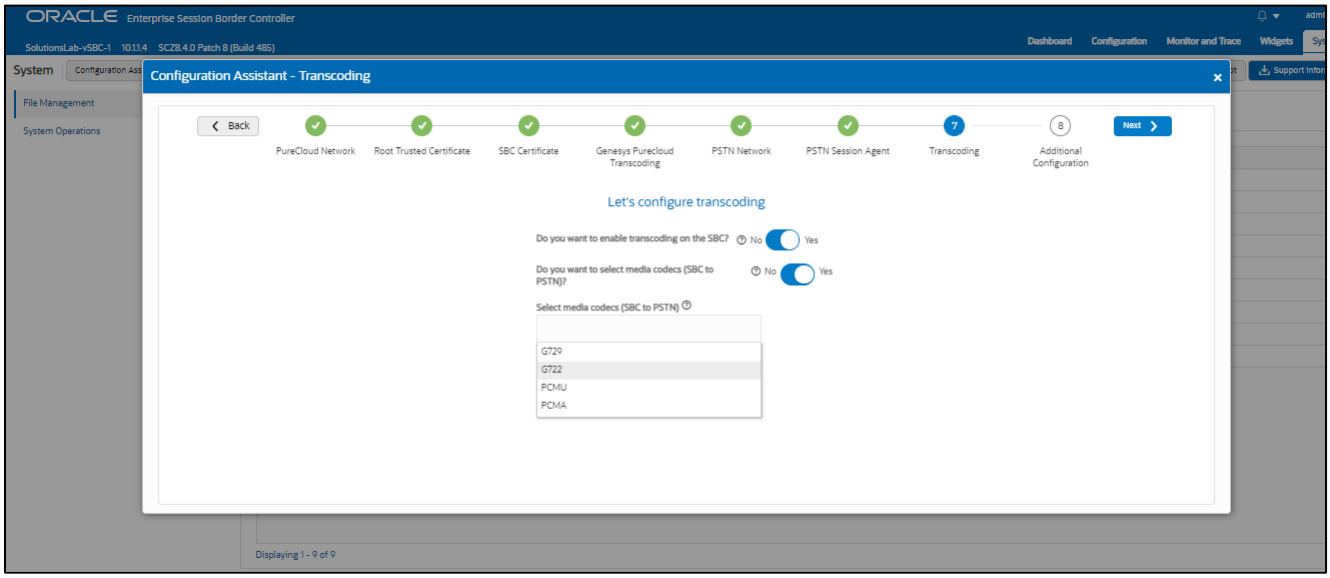


Please fill the required fields and click Next.

Page 7 - PSTN side Transcoding

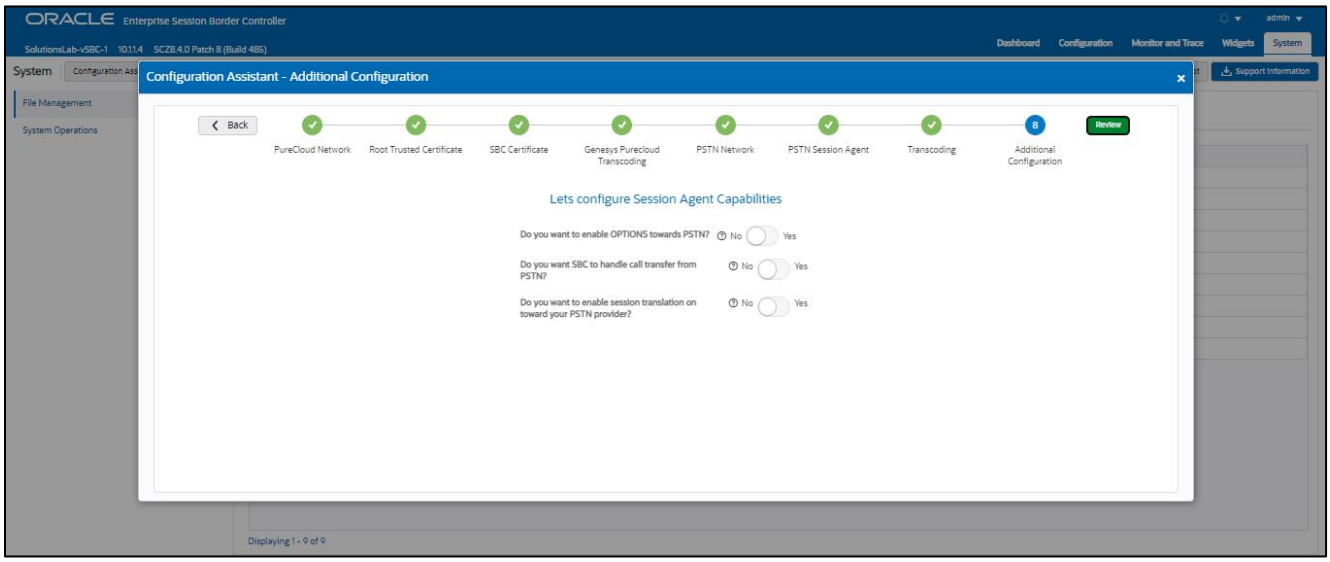
Page 7 is where you will be able to configure transcoding between the SBC and PSTN Trunk.

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.



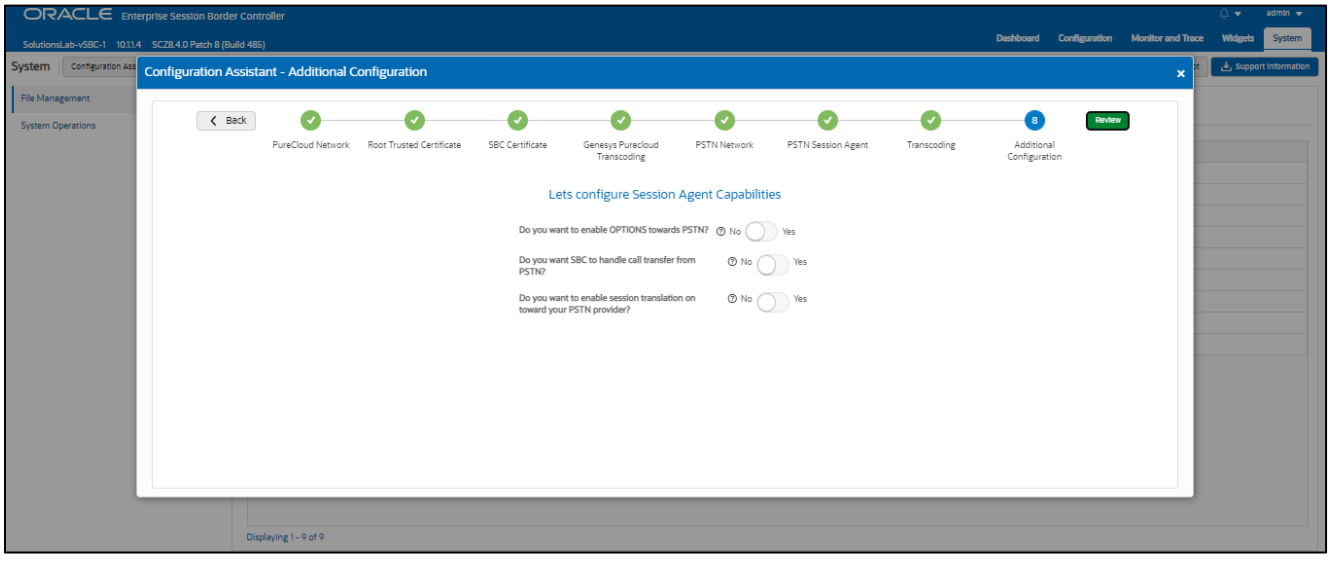
Page 8 – Additional Configuration

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



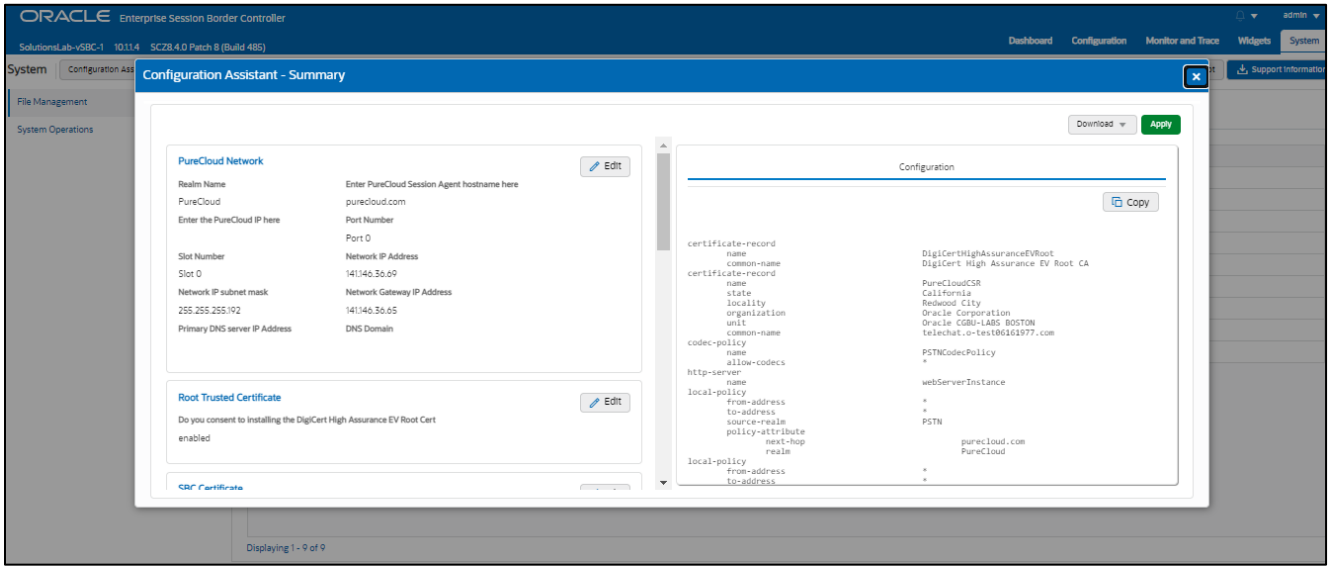
Review

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.



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.

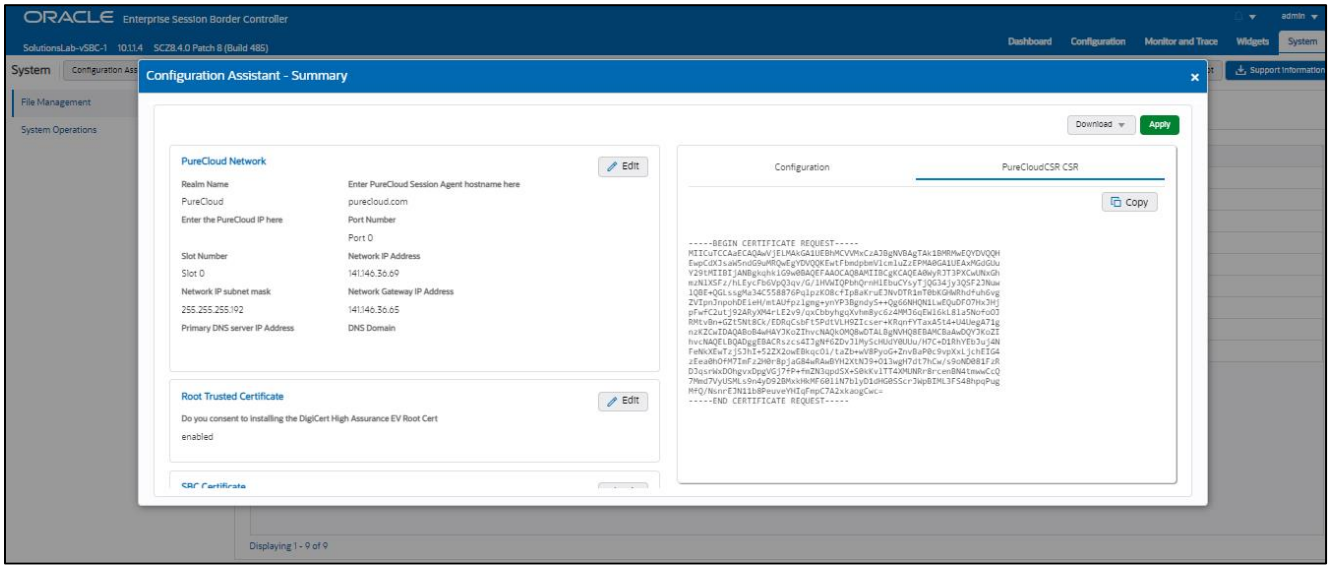
The right side displays the entire configuration created and when applicable, will also have a CSR tab that contains a certificate that can be signed by a CA authority.



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.



Click the copy button under the CSR and paste the output into a text file. Next, provide the txt file to your CA for signature. Once the certificate is signed by the CA, you will need to import that certificate into the SBC manually, either via ACLI or through the GUI.

Note: if you chose to import a certificate in PKCS12 format on page 3, the CSR tab will not be present under review.

Download and/or Apply

The template provides you with the ability to "Download" the config by clicking the "*Download*" tab on the top right. Next, click the "*Apply*" button on the top right, and you will see the following pop-up box appear.

Now you can click "*Confirm*" to confirm you want to apply the configuration to the SBC. The SBC will reboot. When it comes back up, the SBC will have a basic configuration in place for PureCloudPhone with Generic PSTN Sip Trunk.

Configuration Assistant Access

Upon initial login, if the Configuration Assistant Template does not immediately appear on the screen, you can access by clicking on the "*SYSTEM*" tab, top right of your screen. After that, click on the "*Configuration Assistant*" tab, top left. This allows end users to access the Configuration Assistance at any time through the SBC GUI.

9. Test Plan Executed

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

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

Oracle 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