Oracle SBC integration with Genesys BYOC Cloud and Twilio Elastic Sip Trunking

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 BYOC Cloud and Twilio Elastic SIP Trunking Oracle Public IP Address Masked	26h May 2021
1.1	Oracle Public IP Address masked	18th Nov 2021
1.2	Added New Section - Configure Oracle SBC via Configuration Assistant	27 Jan 2022
1.4	Removed MAuth TLS and updated Cipher List Changed 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.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Genesys BYOC Cloud and Twilio Elastic Sip Trunk. The solution contained within this document has been tested using Oracle Communication SBC release **cz840p3b**.

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

Related documentation can be found below –

2.1. Twilio Elastic SIP Trunking

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

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

2.2. Genesys BYOC Cloud

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

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

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.

3. Introduction

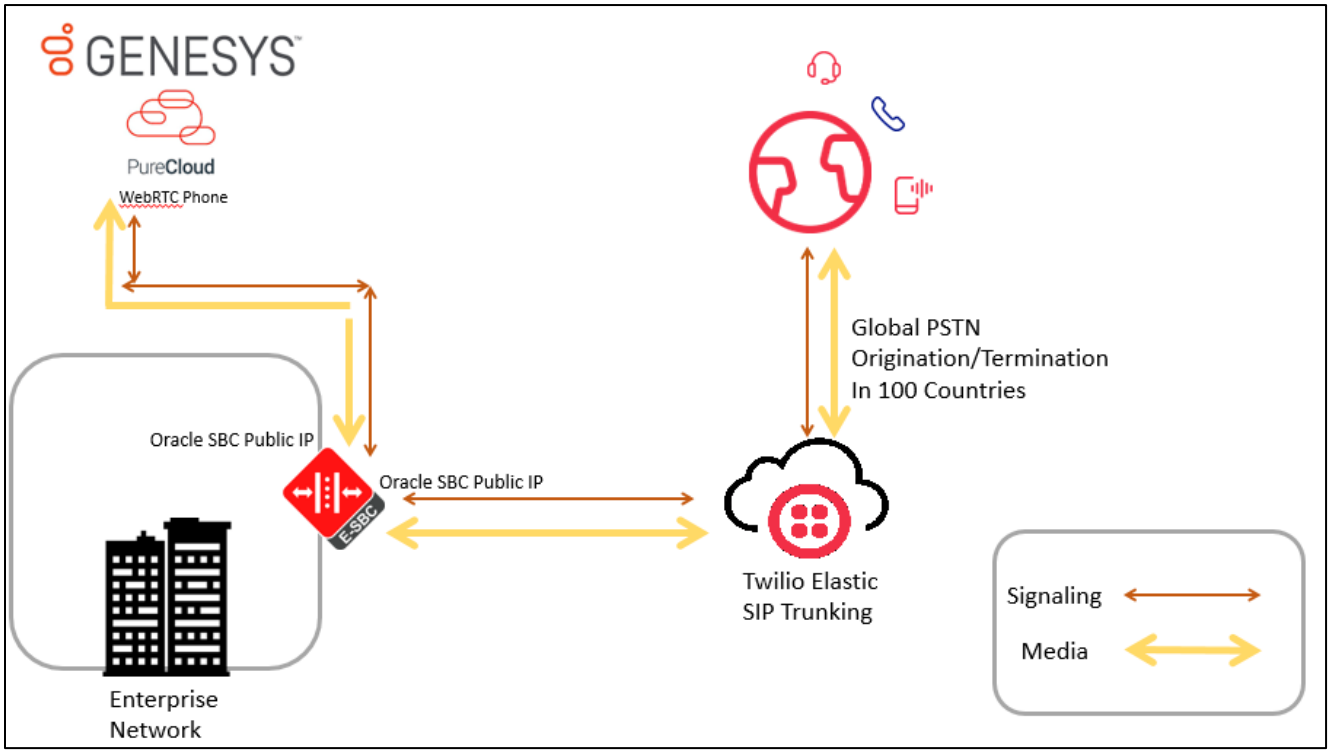
3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Genesys BYOC Cloud using Oracle Enterprise SBC. There will be steps that require navigating the Genesys BYOC Cloud configuration, Oracle SBC GUI interface. Understanding the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

3.2. Requirements

- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version
- Genesys Pure Cloud Solution with BYOC Cloud Setup.
- Twilio Elastic Sip Trunk and Twilio Direct Inward Dial numbers.

3.3. Architecture



Above figure illustrates the connection between Genesys BYOC Cloud, Oracle SBC and Twilio Elastic Sip Trunk. Both BYOC Cloud and Twilio Elastic Trunk are connected to the Oracle SBC Public FQDN /IP

In addition, SBC is used to steer the signaling, media to, and From the BYOC Cloud to Twilio SIP Trunk.

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

- Phase 1 – Configuring the Genesys BYOC Cloud
- Phase 2 – Configuring the Oracle SBC.
- Phase 3 – Configuring the Twilio Elastic SIP Trunk

4. Configure Genesys BYOC Cloud

The steps outlined below is the minimum required configuration to pair your SBC with Genesys BYOC Cloud. This is to be used as an example only, and we highly recommend you work with your Genesys representative to implement the correct configuration for your specific environment.

To implement BYOC Cloud BYOC, you use the Telephony Admin UI to create SIP trunks between the BYOC Cloud Media Tier resources in AWS and third party carriers or devices over the public Internet. The third-party carrier or device can be another cloud service or a device at the customer's premises. The Oracle Enterprise SBC will act as an intermediary between Twilio Elastic SIP Trunk and Genesys BYOC Cloud. The SBC is configured to broker calls as a back-to-back user agent (B2BUA) between the two systems. The Twilio DIDs are

assigned to users on BYOC Cloud System 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 as UDP.TLS and TCP Transport Protocol are also available as Transport Protocol on Genesys BYOC Cloud.

4.1 External Trunk Configuration

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

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

To configure the external Trunk Navigate to

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

4.1.1 Create a new External Trunk

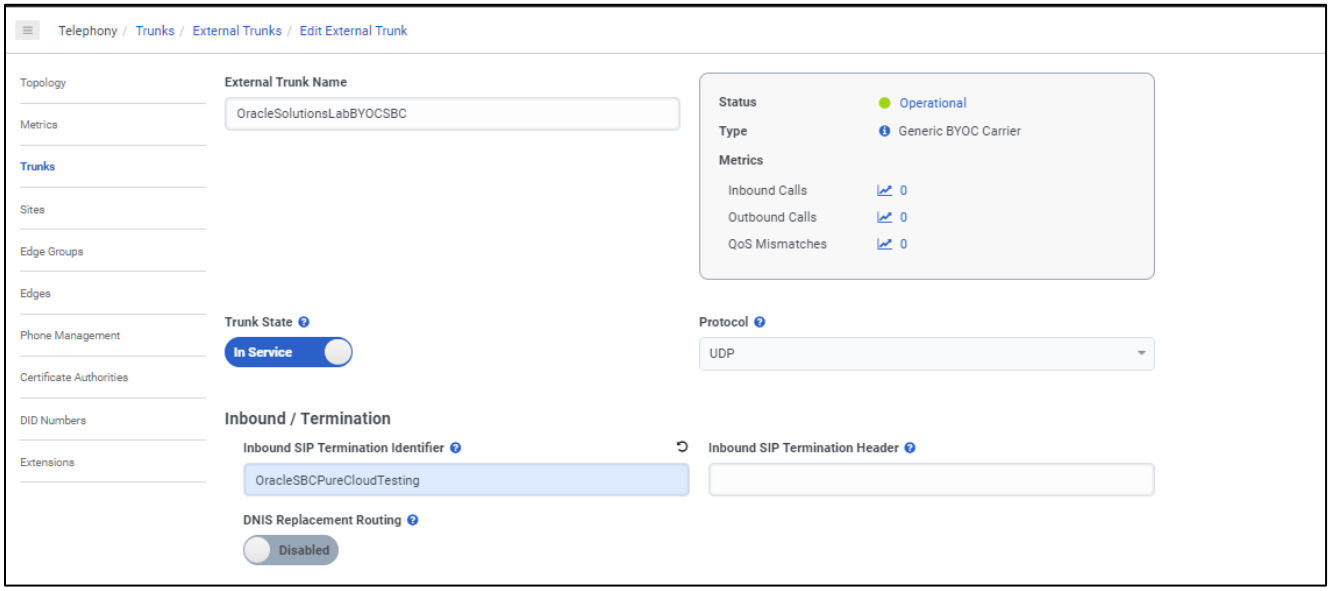
Type: BYOC Carrier Trunk

Protocol: UDP (TCP and TLS are also available)

4.1.2 Set Inbound SIP Termination Identifier

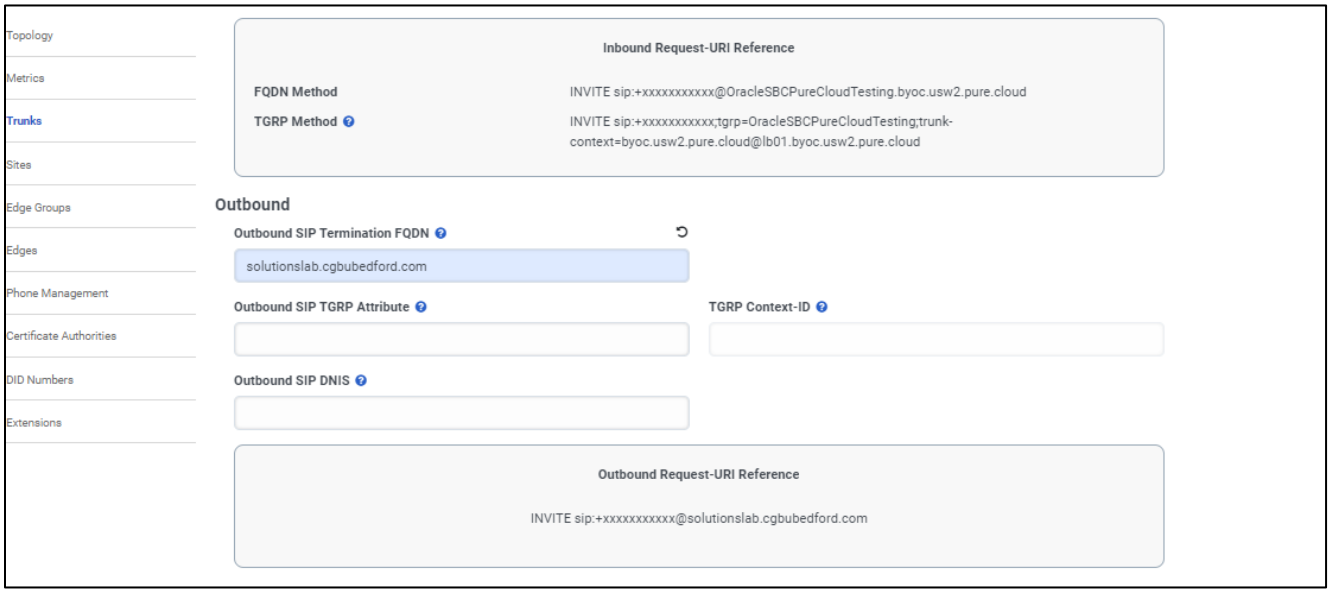
Inbound SIP Termination Identifier – is the DNS Name we will configure on the Oracle SBC and will be used to route calls towards BYOC Cloud . In this particular example, “OracleSBCPureCloudTesting” will generate the FQDN - OracleSBCPureCloudTesting.byoc.usw2.pure.cloud as shown in the example.

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



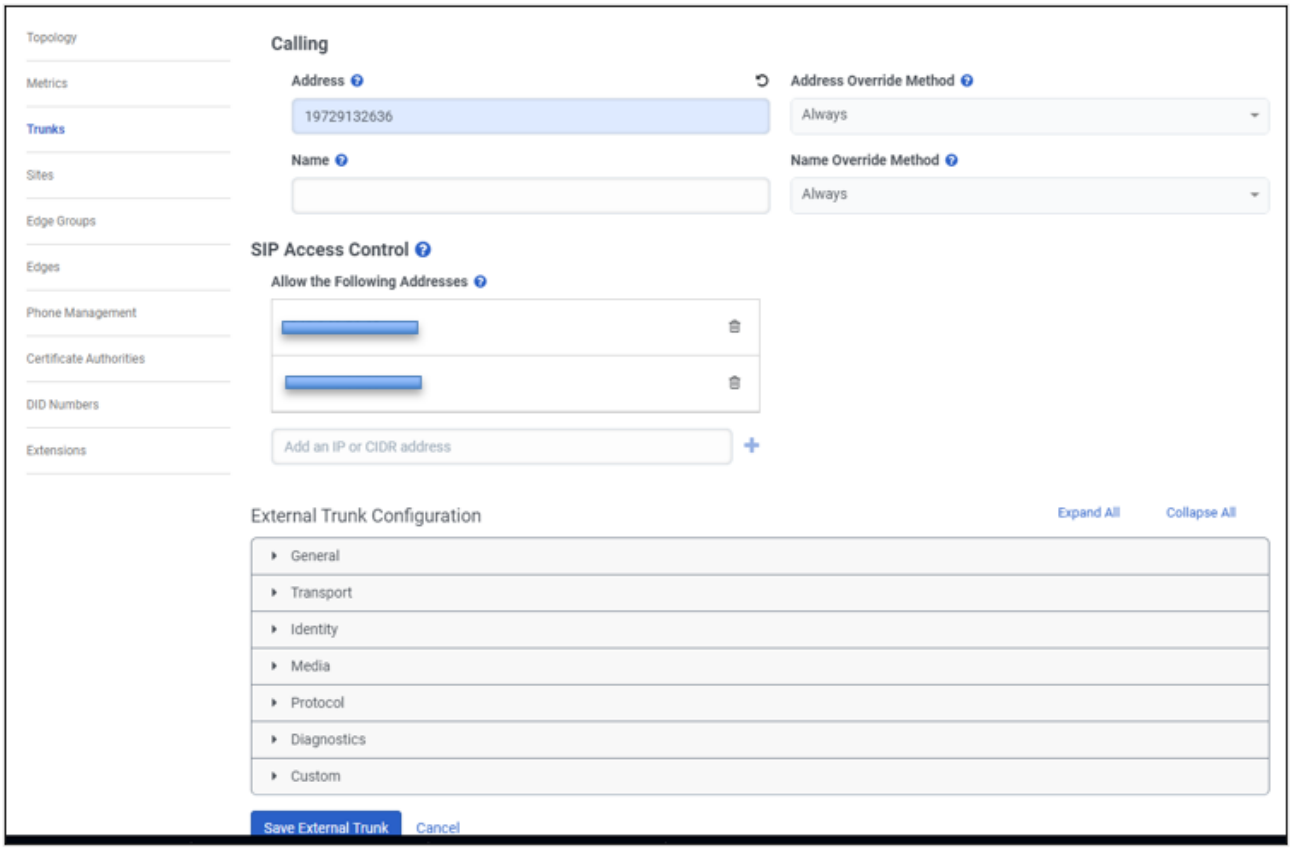
4.1.3 Set Outbound SIP Servers or Proxies

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



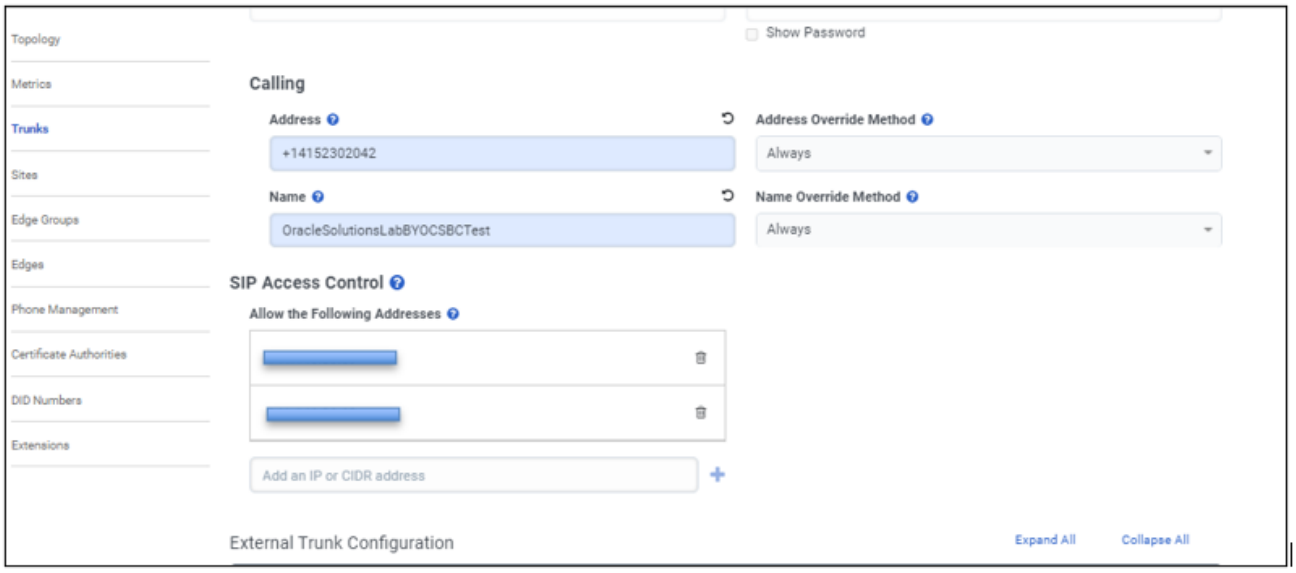
4.1.4 Set Calling Address

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



4.1.5 Set SIP Access Control

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



4.1.6 Enable E.164 format

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

4.2 Site Configuration.

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

Detailed steps to configure the Site can be found here-

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

4.2.1 Create a New Site

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

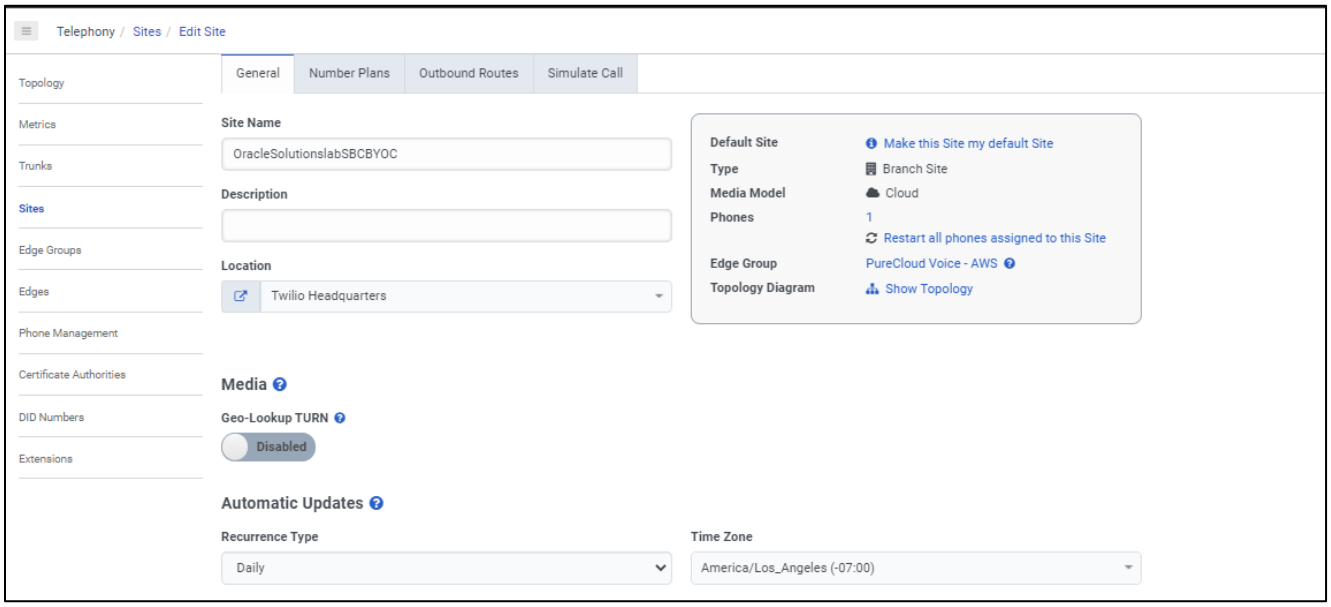
Type a name into the **Site Name** box.

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

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

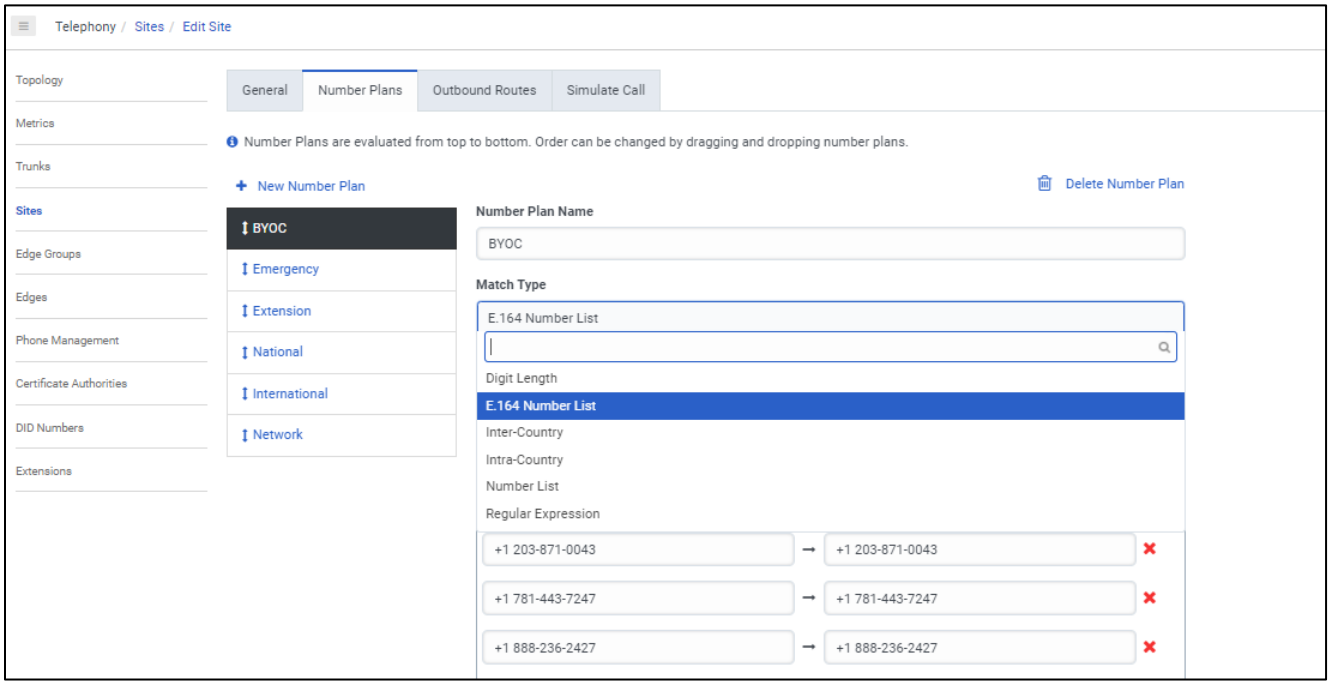
Under **Media Model**, select **Cloud**.

Click **Create Site**.



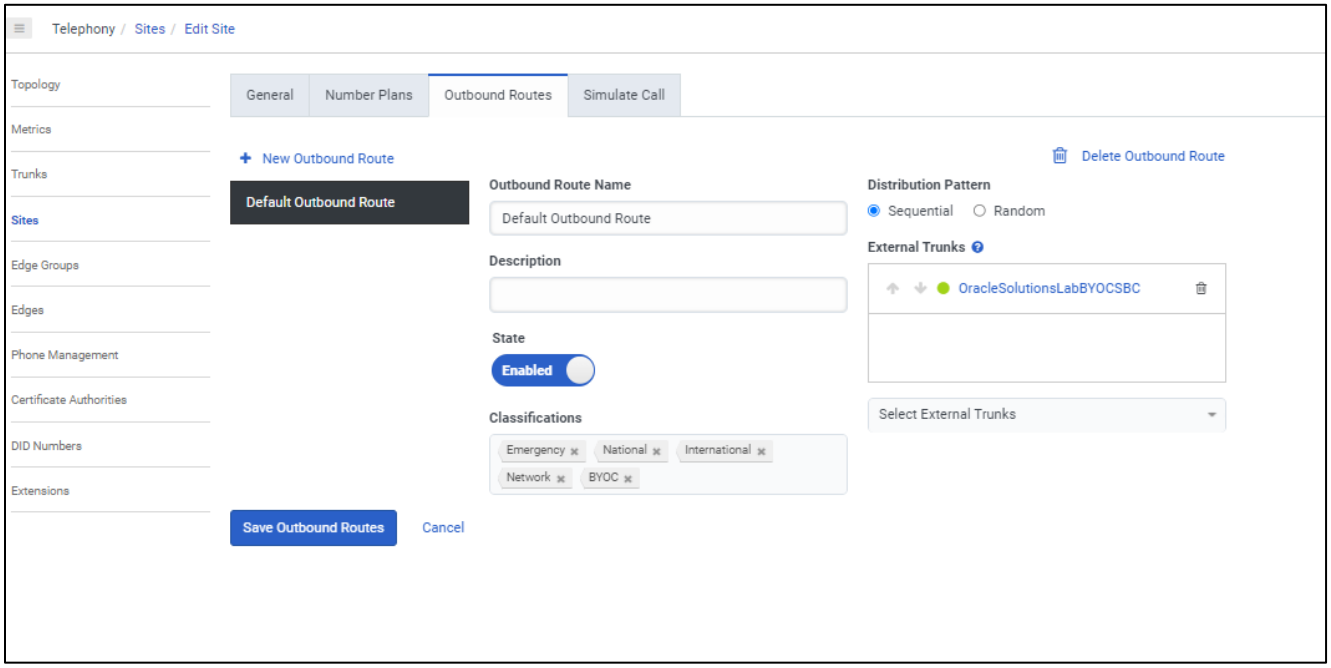
4.2.2 Number Plans & Classifications

BYOC 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.



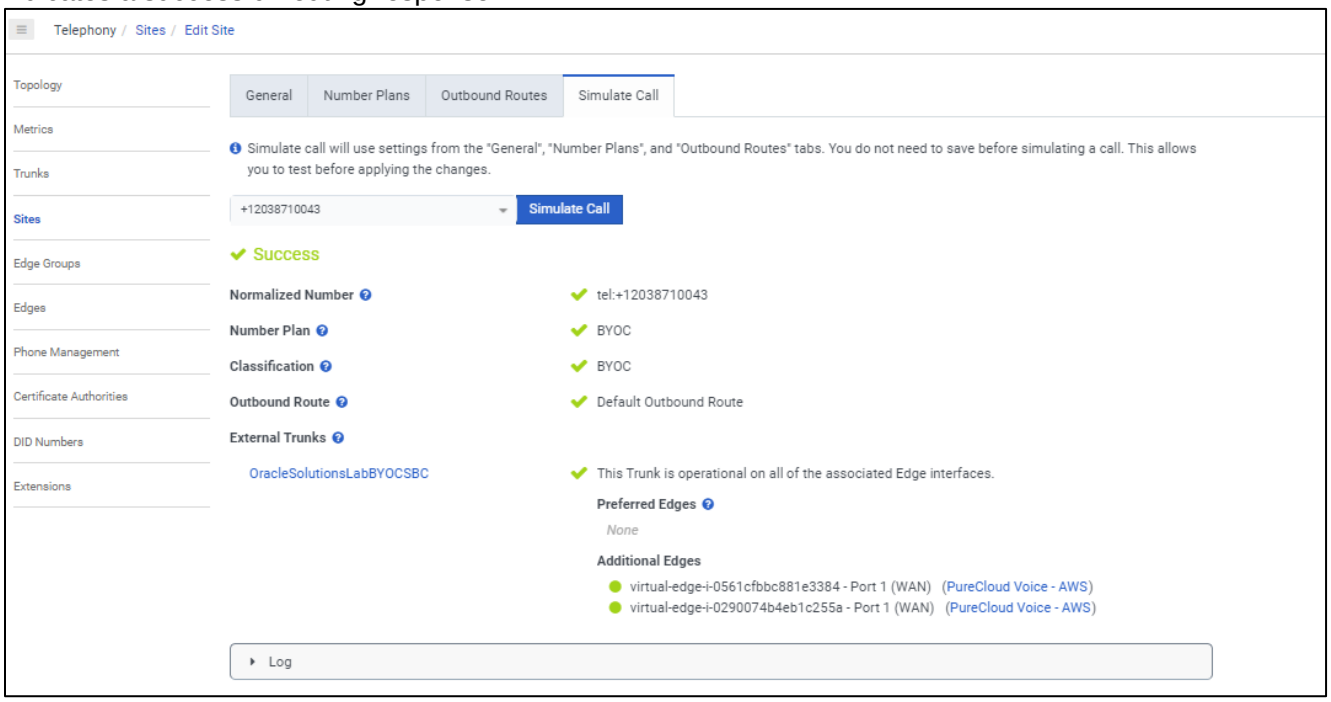
4.2.3 Configure outbound route

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



4.2.4 Simulate call

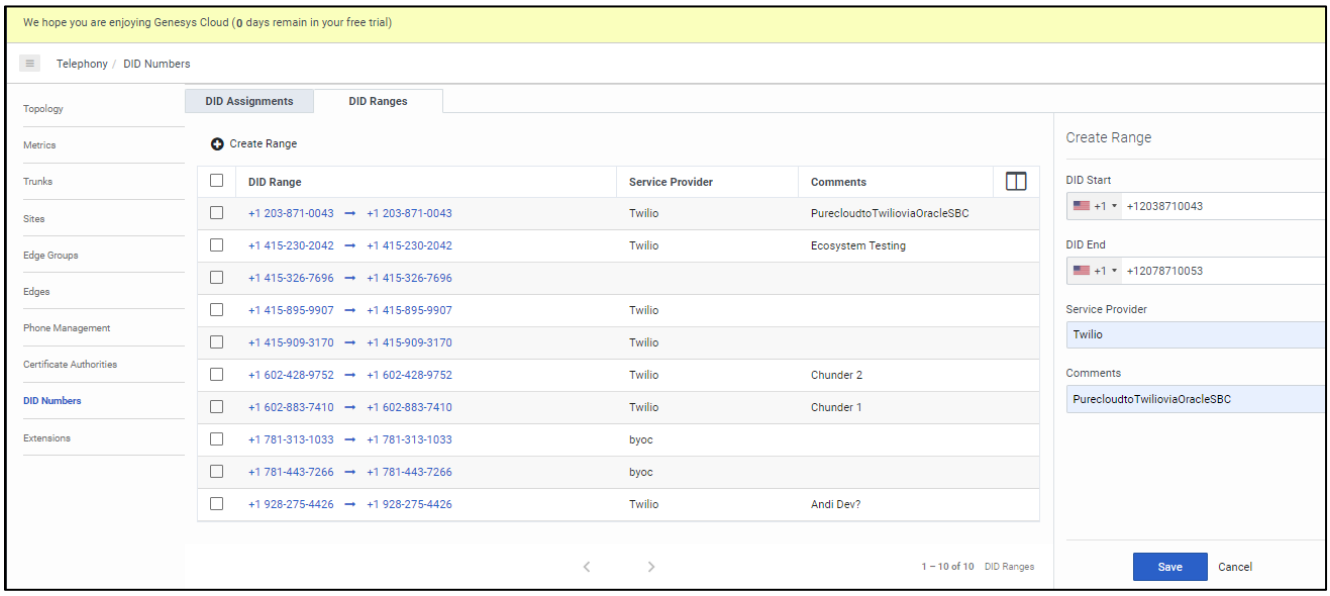
Genesys BYOC Cloud provides a neat feature to test and validate the routing of calls for troubleshooting purpose. Below is an example for a call to BYOC type number classification on this Site. Success indicates a successful routing response.



4.3 DID Assignment

4.3.1 Create DID Range

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



4.3.2 Assign DID to User.

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

5. Configuring the SBC

This chapter provides systematic guidance on how to configure Oracle SBC for Genesys BYOC Cloud and Twilio Elastic SIP Trunking.

5.1. Validated Oracle SBC version

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

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

6. New SBC configuration

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

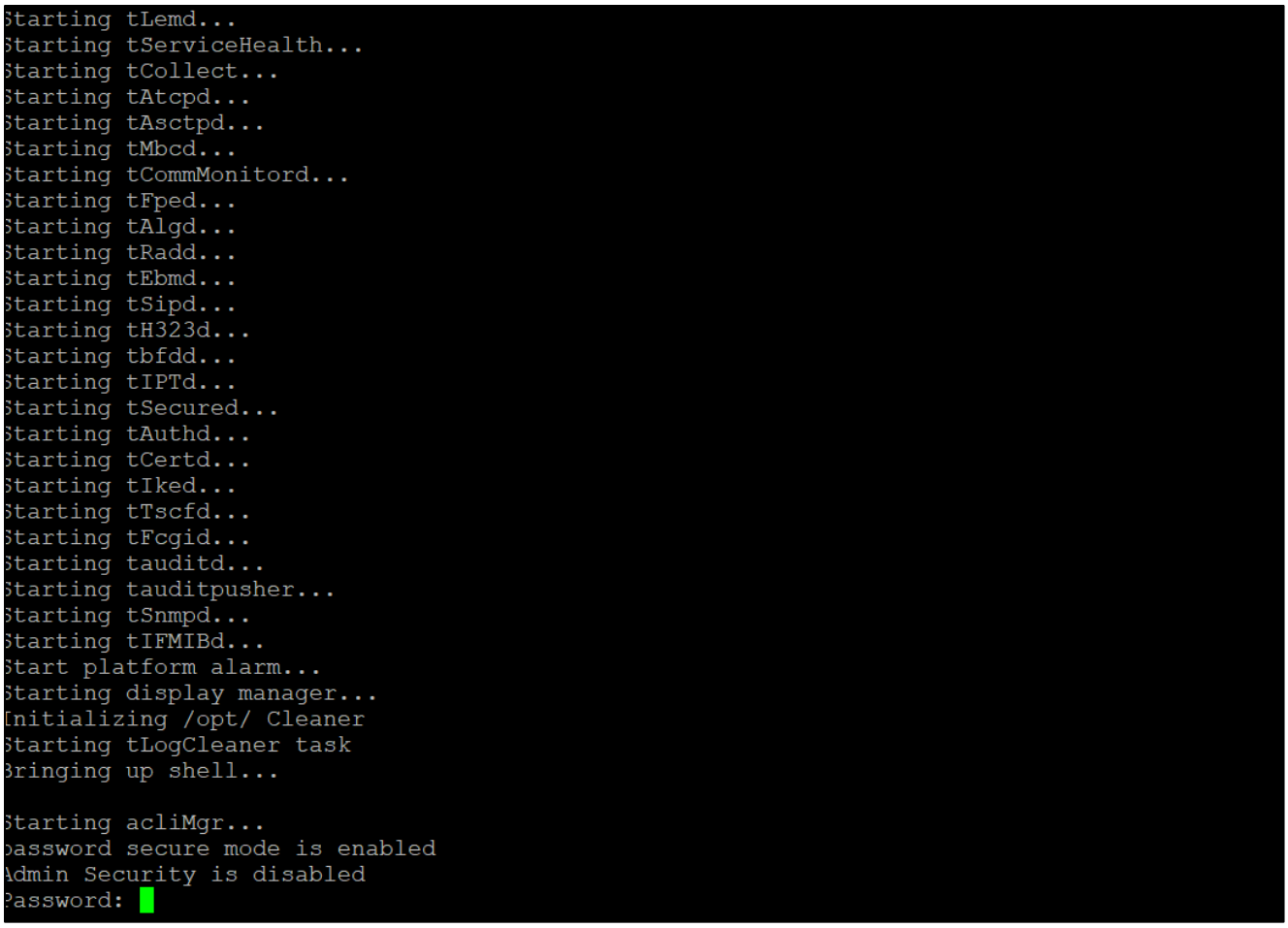
6.1. Establishing a serial connection to the SBC

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:

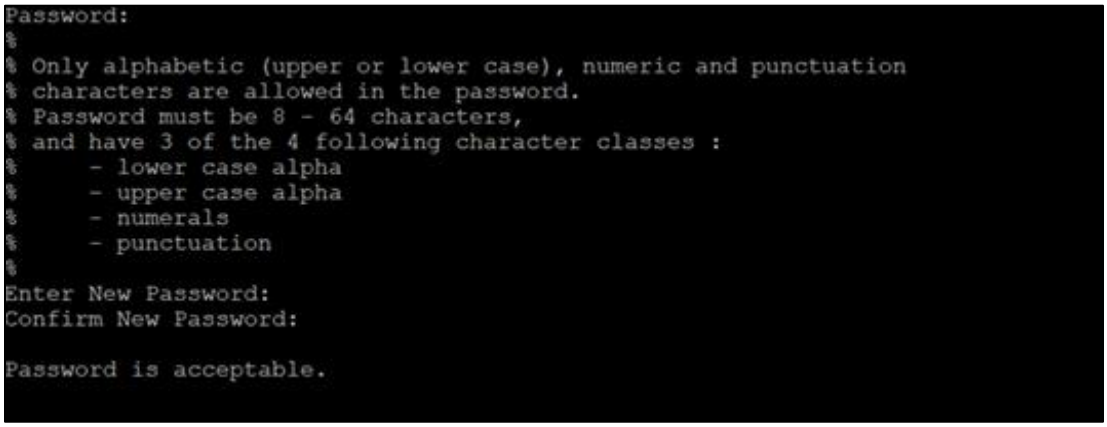
- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

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 have to 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.

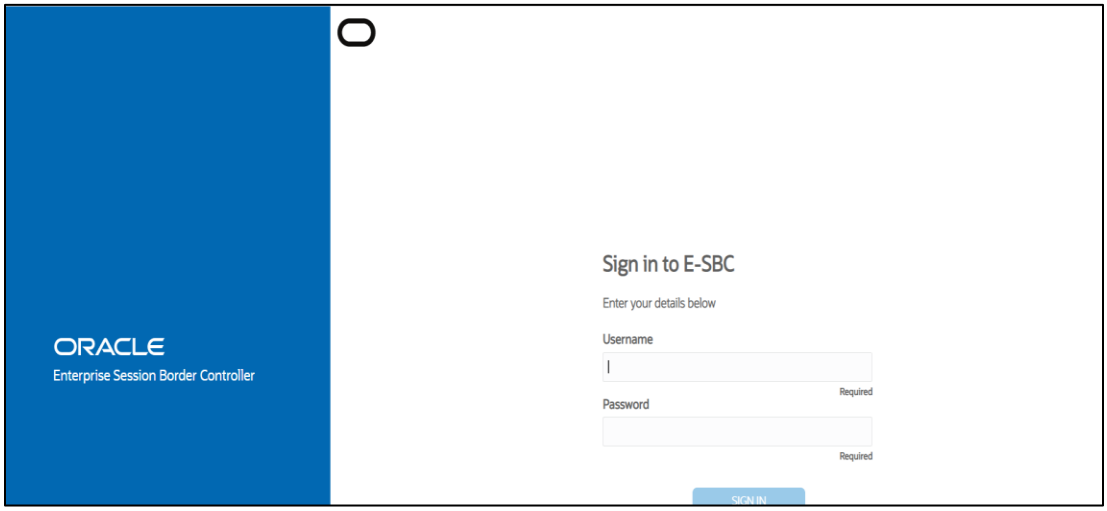
```
NN4600-139(http-server)#
NN4600-139(http-server)# show
http-server
        name                                webServerInstance
        state                               enabled
        realm
        ip-address
        http-state                          enabled
        http-port             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

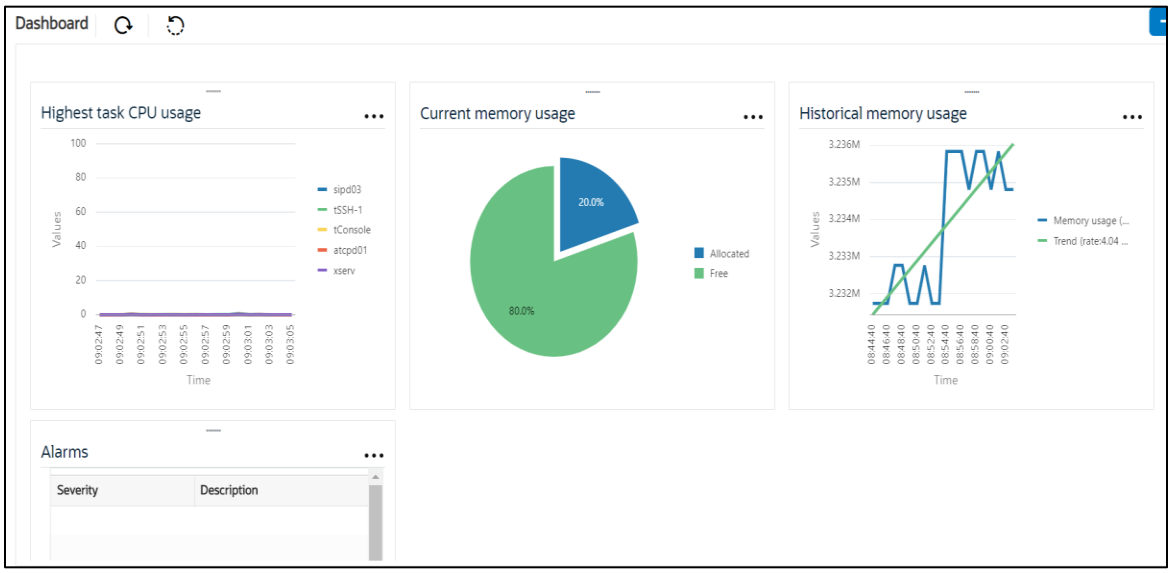
6.2. Configure SBC using Web GUI

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

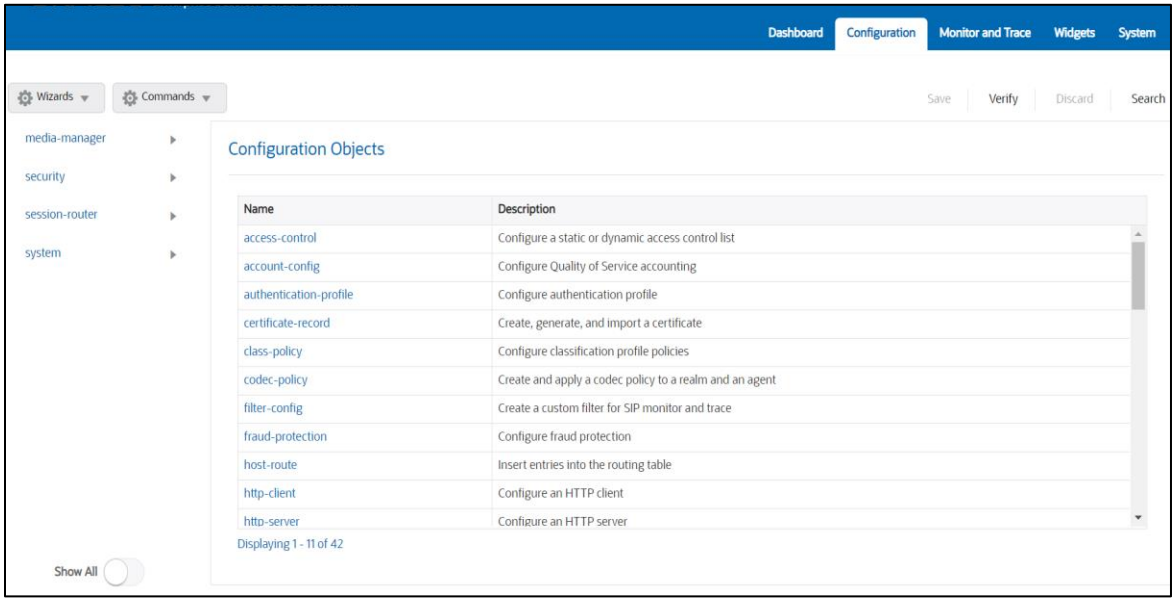
The Web GUI can be accessed through the URL http://<SBC_MGMT_IP>.



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



Navigate to Configuration as shown below, to configure the SBC



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

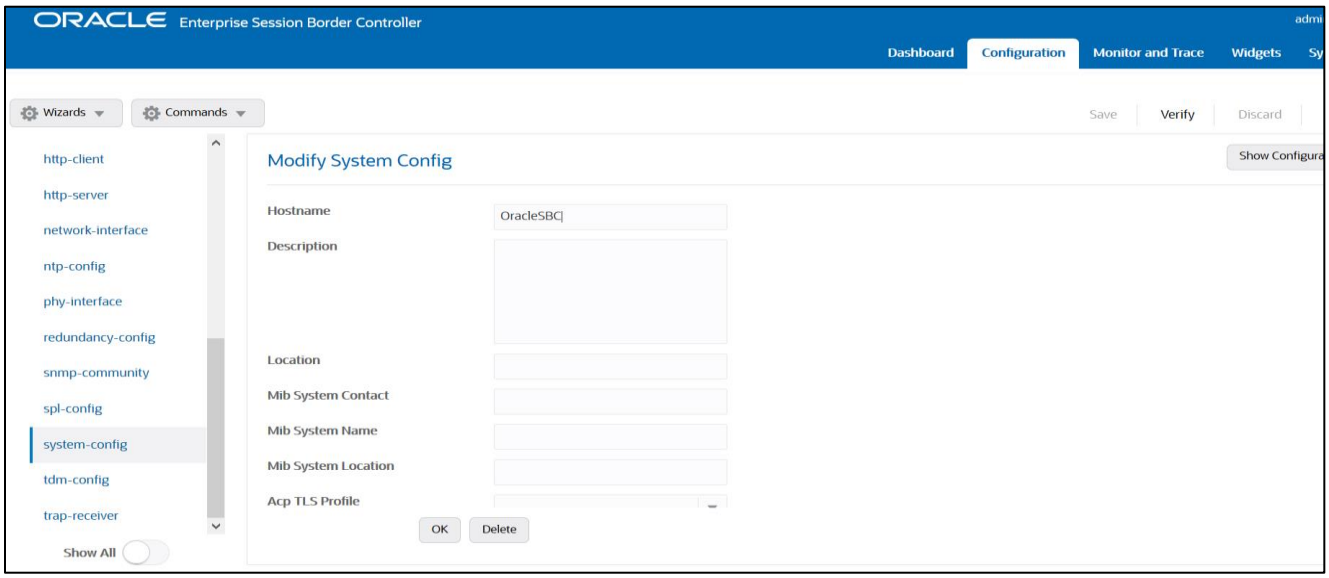
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf

The expert mode is used for configuration.

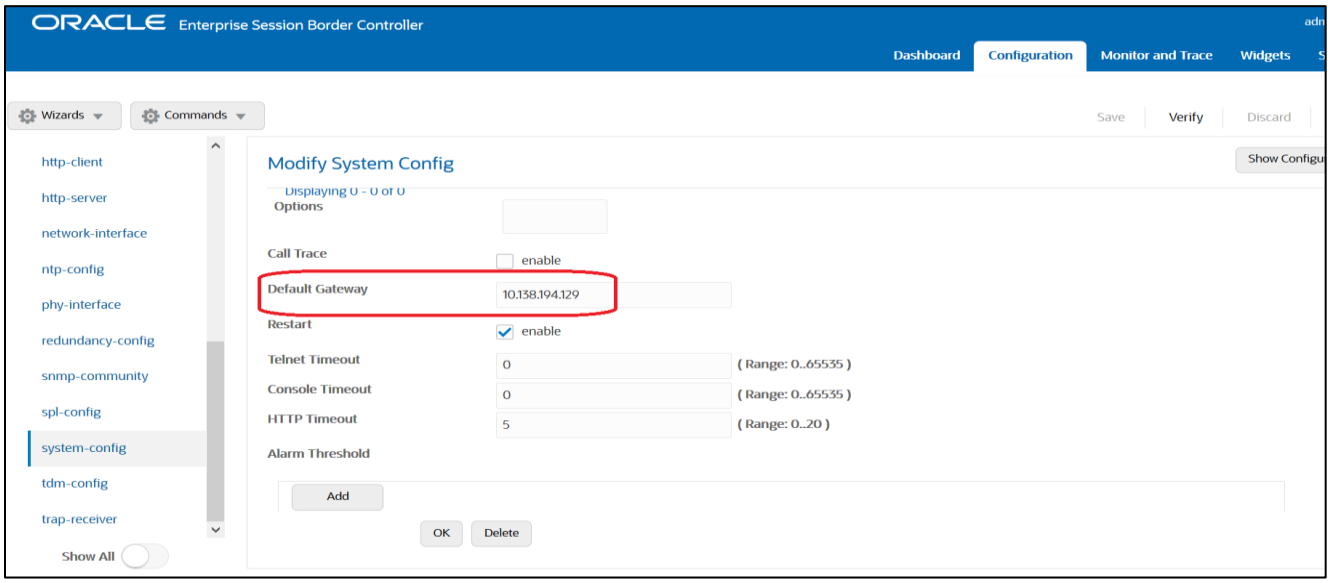
Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

6.3. 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.

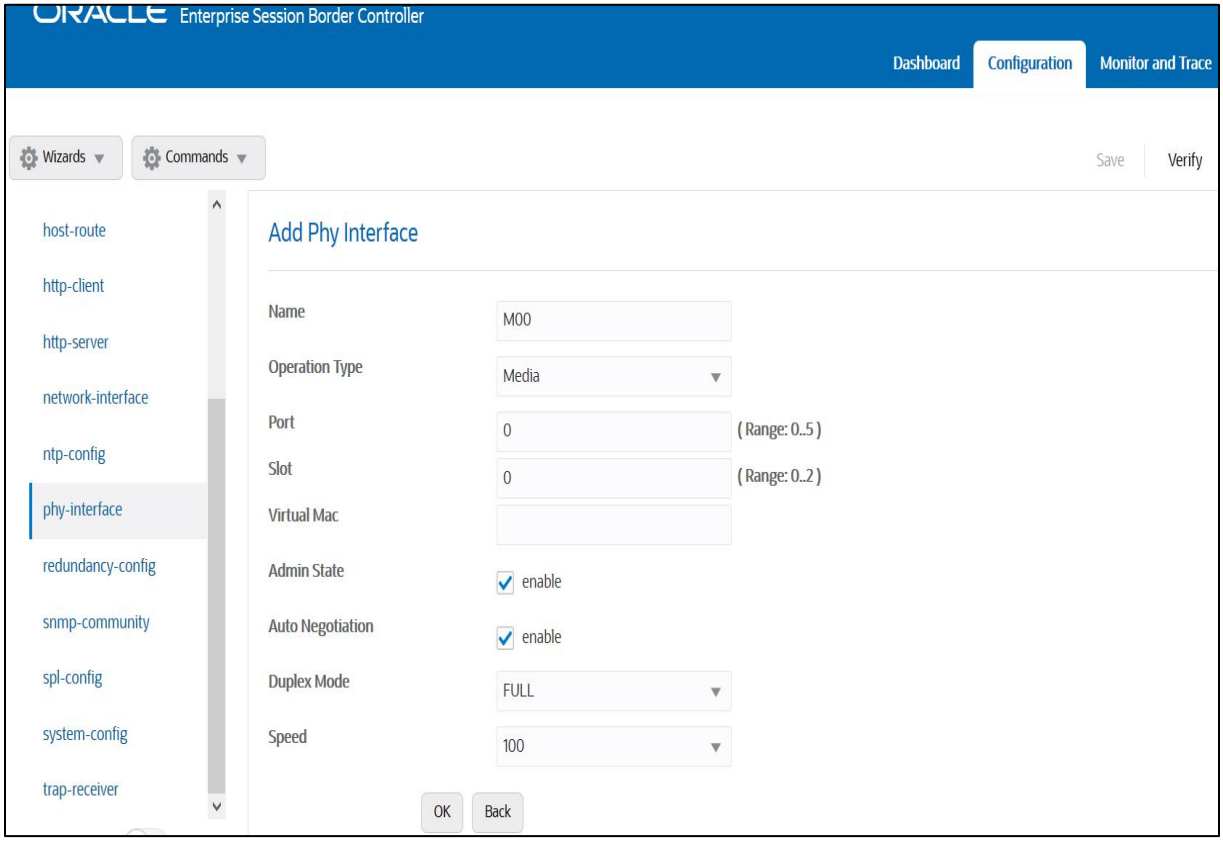
6.4. Configure Physical Interface values

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

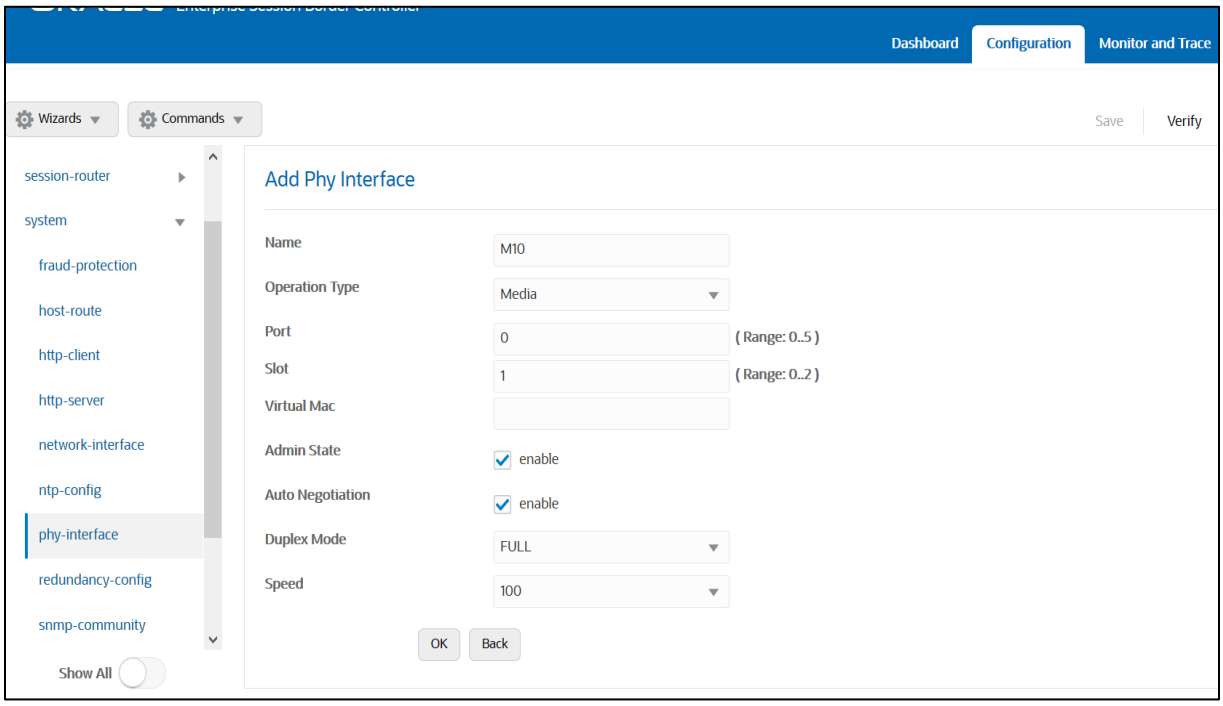
Here we have configured, Network-interface M00 for Twilio Elastic Sip Trunk and M10 for BYOC Cloud .

Parameter Name	**Twilio Elastic Sip Trunk (M00)**	**BYOC Cloud (M10)**
Slot	0	0
Port	0	1
Operation Mode	Media	Media

Please configure M00 interface as below.



Please configure M10 interface as below



6.5. Configure Network Interface values

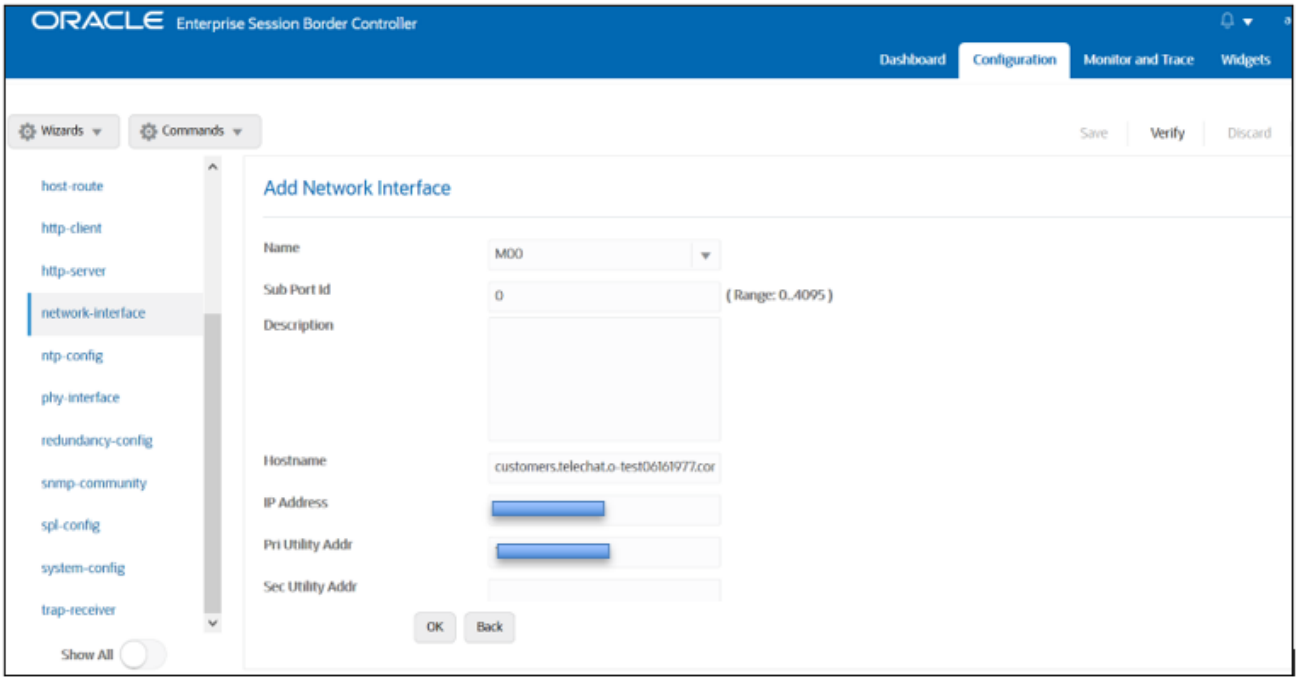
To configure network-interface, Navigate to system->Network-Interface. Configure interface

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

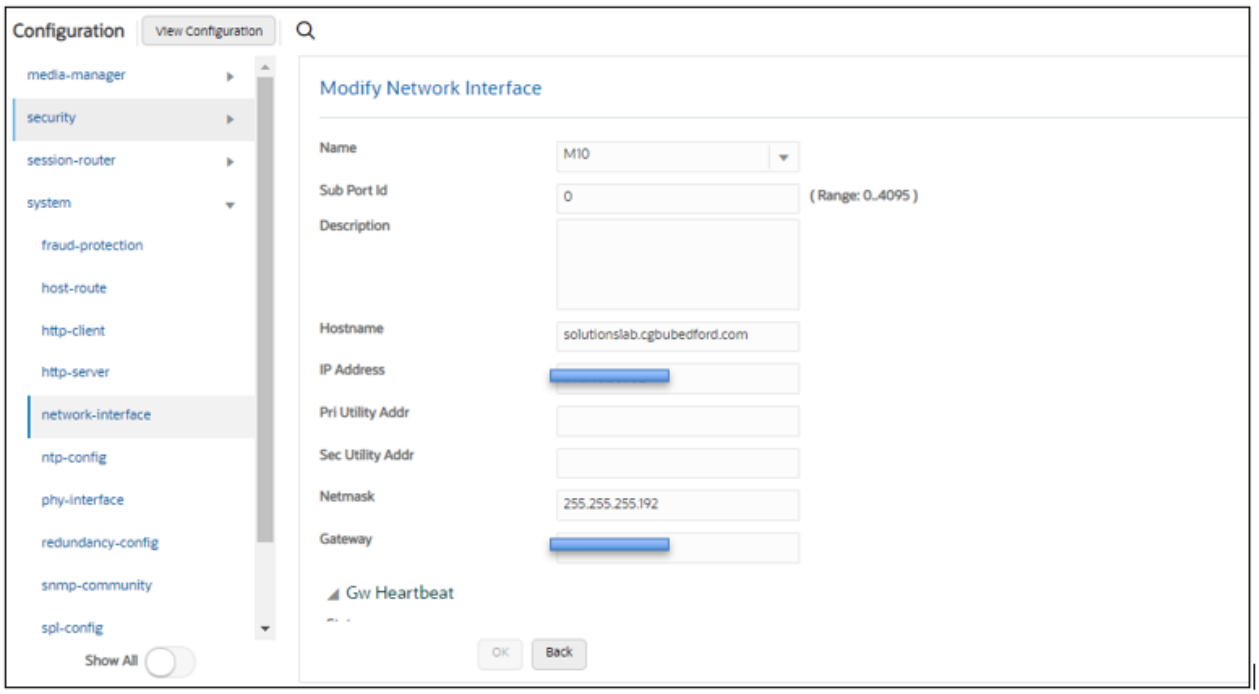
Note: The provided network IP addresses are given for example purpose only. In the real world scenario We cannot same networks on two network-interfaces hence make sure you use a different IP range for each Network-interface.

Parameter Name	Twilio Network interface	PureCloud Network interface
Name	M00	M10
Host Name	customers.telechat.o-test06161977.com	solutionslab.cgbubedford.com
IP address		
Netmask	255.255.255.192	255.255.255.192
Gateway		
dns-ip-primary	8.8.8.8	8.8.8.8
dns-ip-backup1	8.8.8.4	8.8.8.4
dns-domain	customers.telechat.o-test06161977.com	solutionslab.cgbubedford.com

Please configure network interface M00 as below



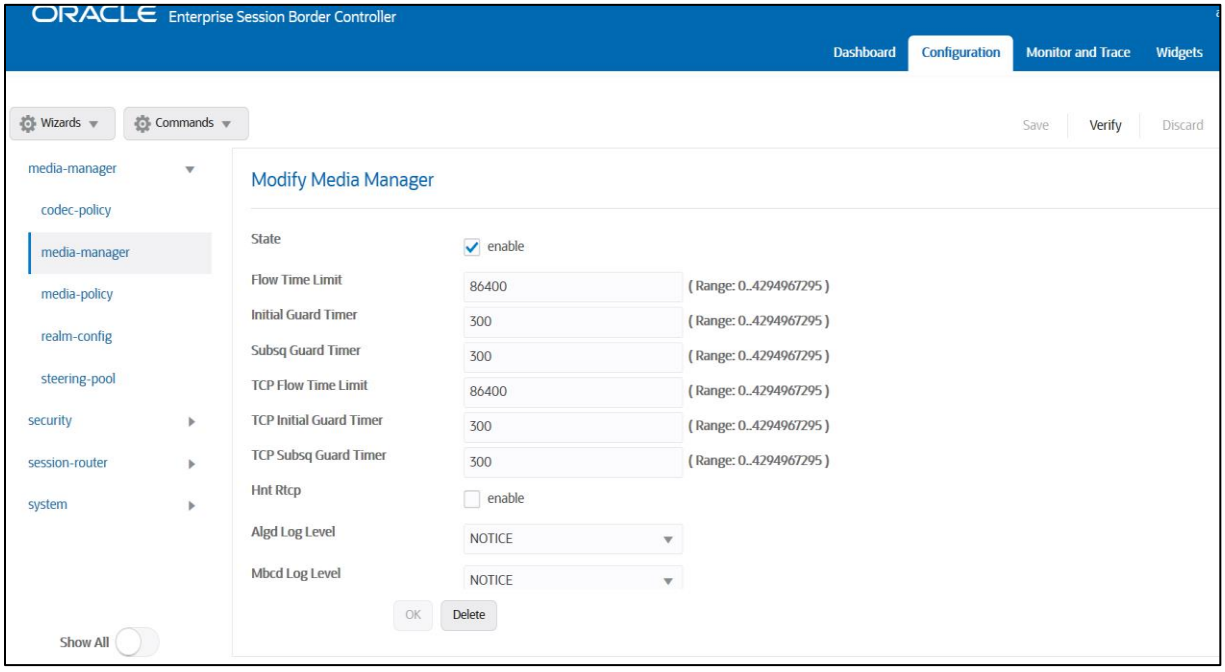
Similarly, configure network interface M10 as below

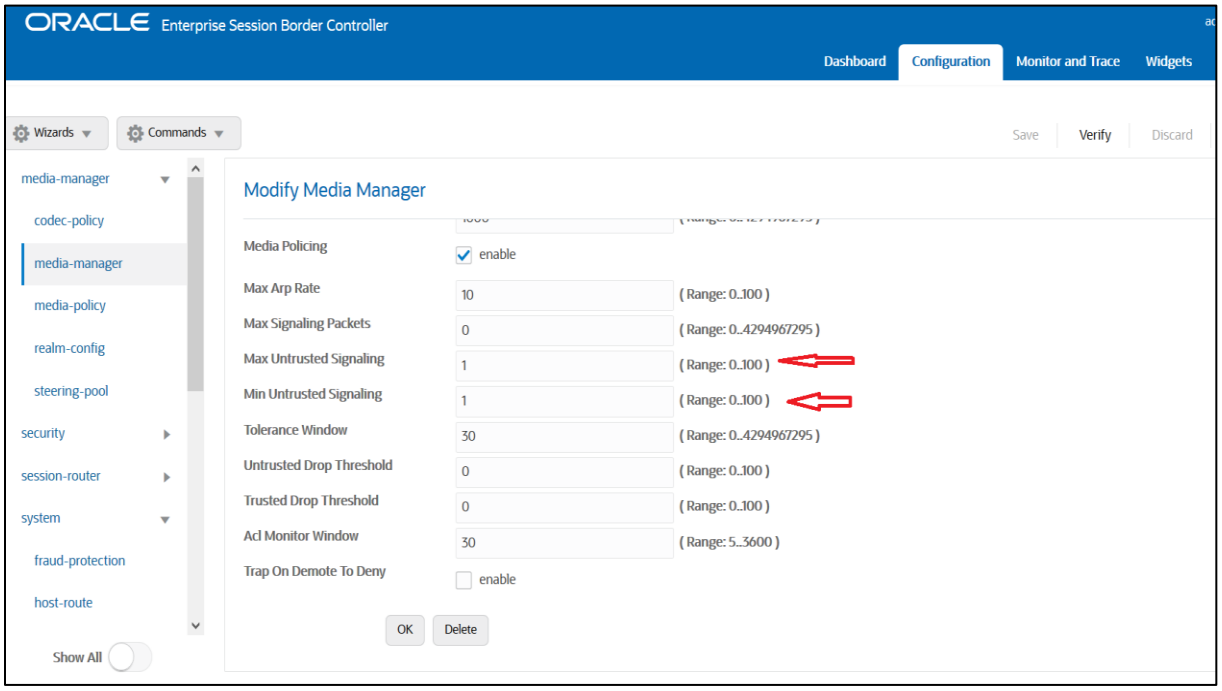


6.6. Enable media manager

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

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



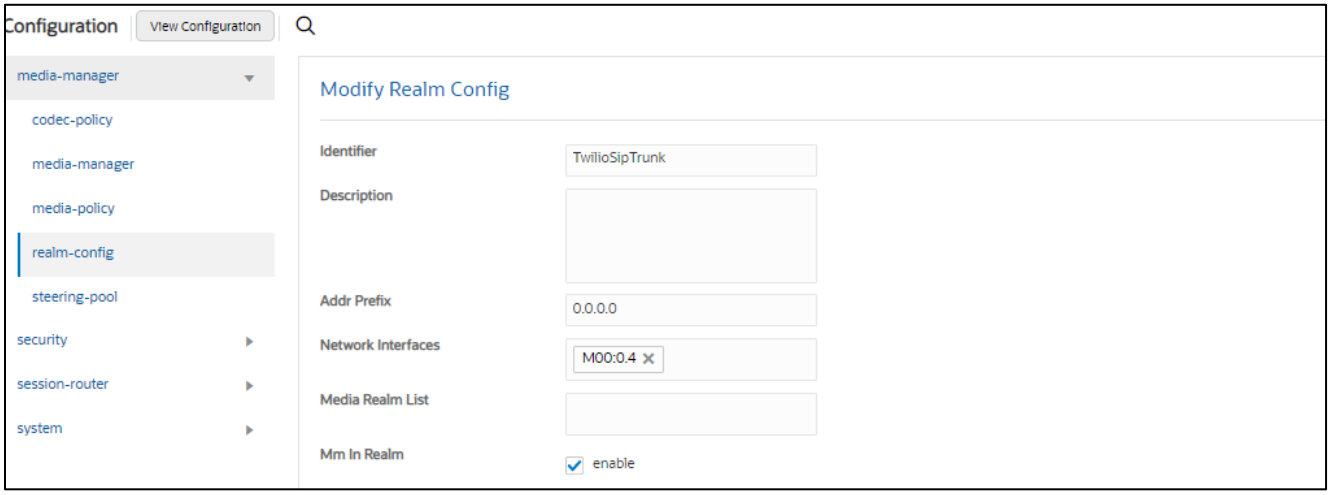


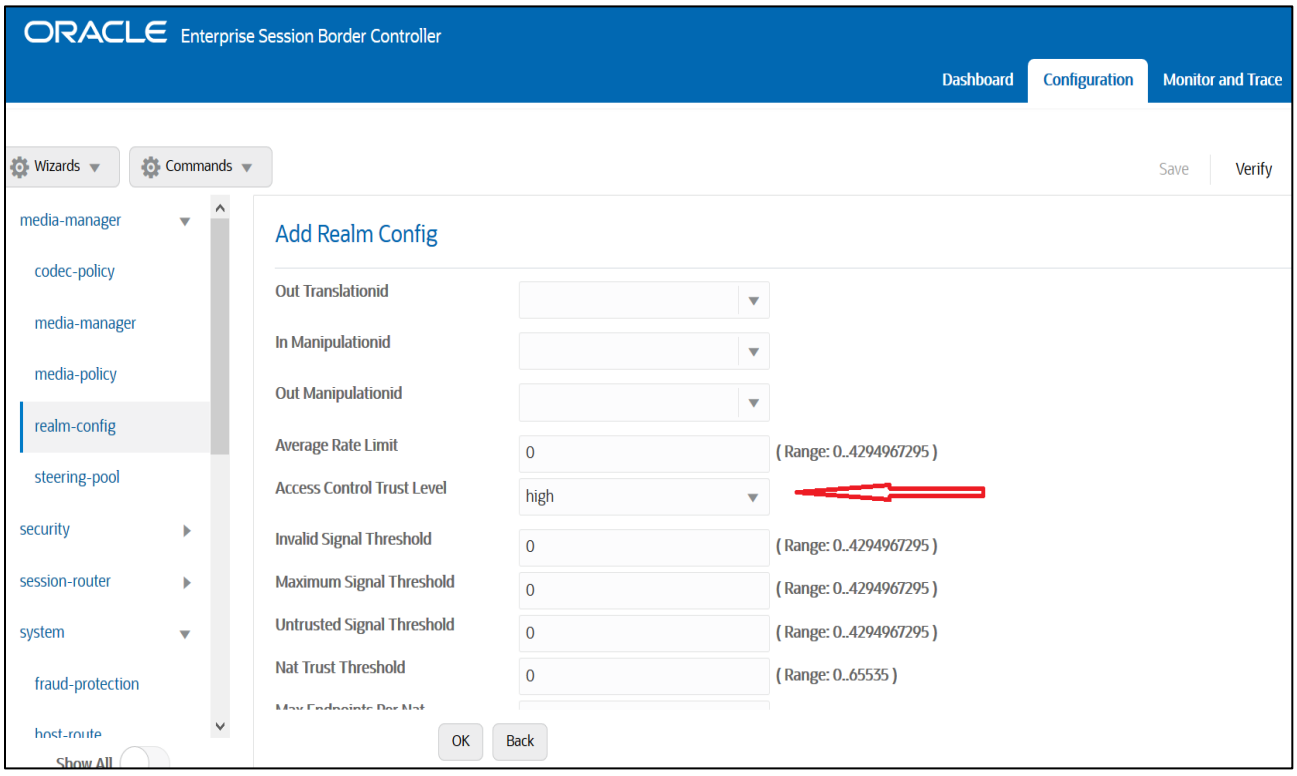
6.7. Configure Realms

Navigate to realm-config under media-manager and configure a realm as shown below
The name of the Realm can be any relevant name according to the user convenience.

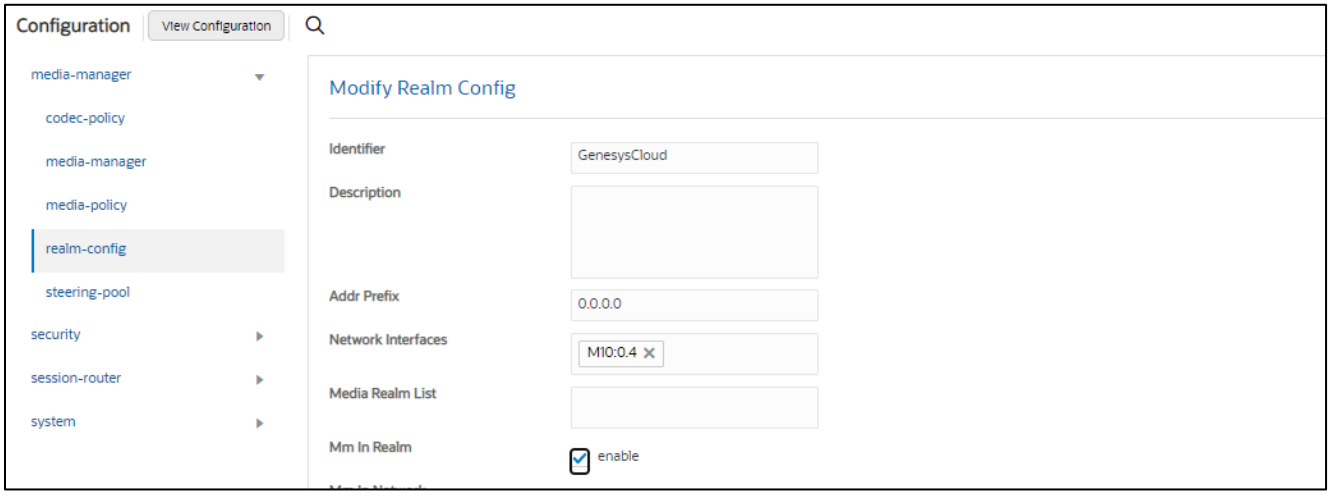
Use the following table as a configuration example for the three realms used in this configuration:

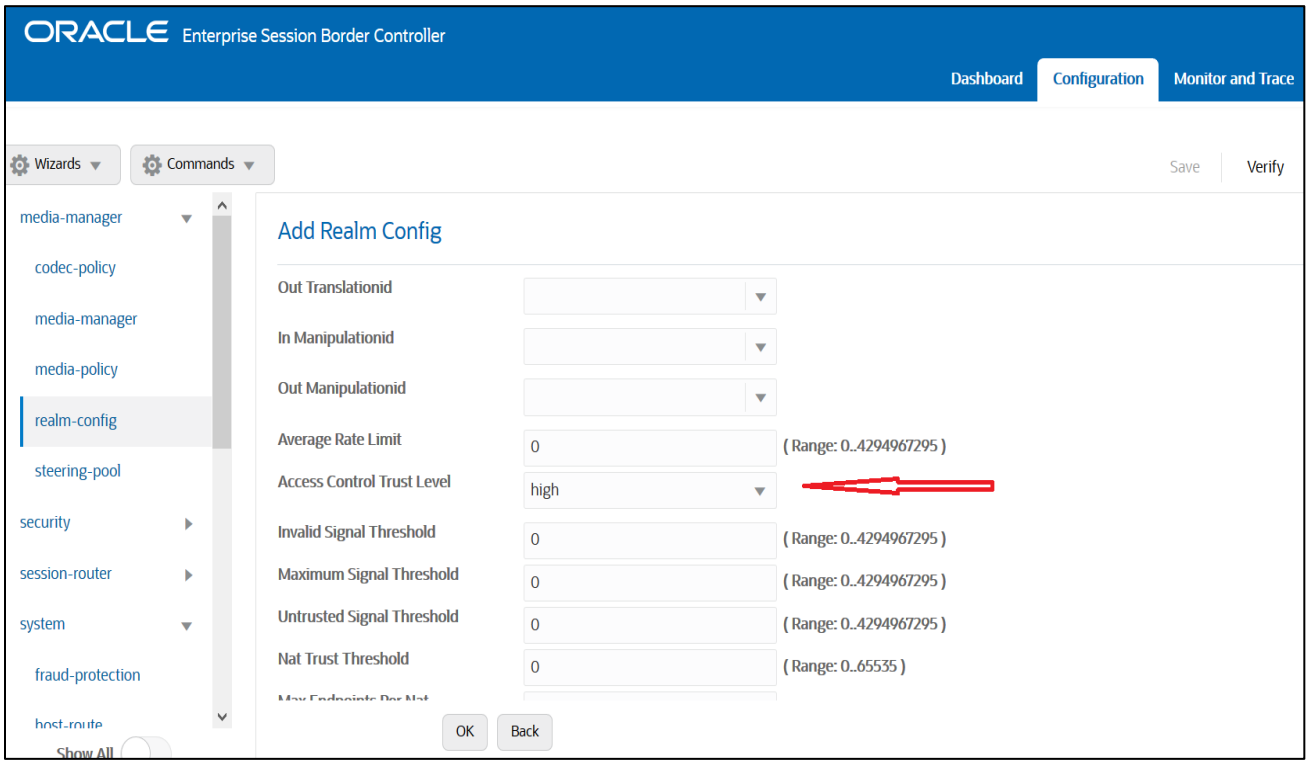
Config Parameter	Twilio Realm	GenesysCloud Realm
Identifier	TwilioSipTrunk	GenesysCloud
Network Interface	M00	M10
Mm in realm	☑	☑
Media Sec policy	sdespolicy	RTP
Access Control Trust Level	High	High





Create another realm for Genesys BYOC Cloud –





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

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

6.8. Security Configuration

This section describes how to configure the SBC for TLS and SRTP communication for Twilio Elastic SIP Trunking and Genesys BYOC Cloud.

6.8.1 Twilio Elastic SIP Trunk

Twilio Elastic SIP Trunking allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by one of the trusted Certificate Authorities. The process includes the following steps:

1) Create a certificate-record – "Certificate-record" are configuration elements on Oracle SBC, which captures information for a TLS certificate – such as common-name, key-size, key-usage etc.

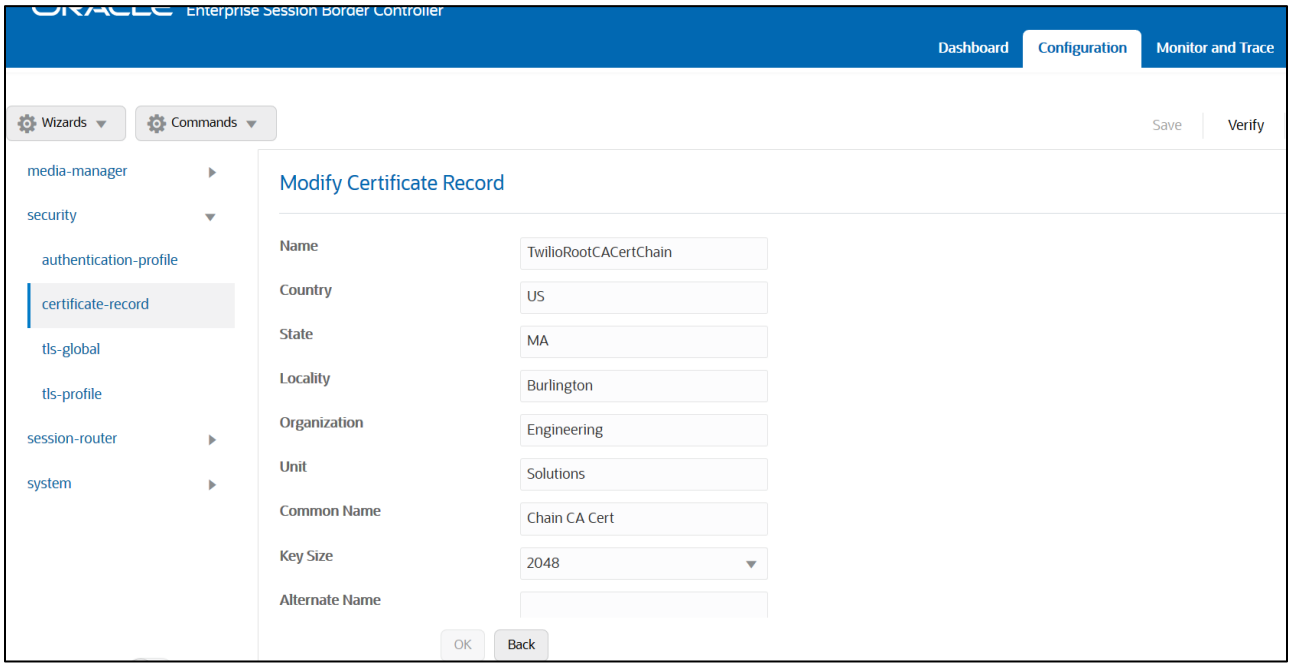
- SBC – 1 certificate-record assigned to SBC
- Root – 1 certificate-record for root cert

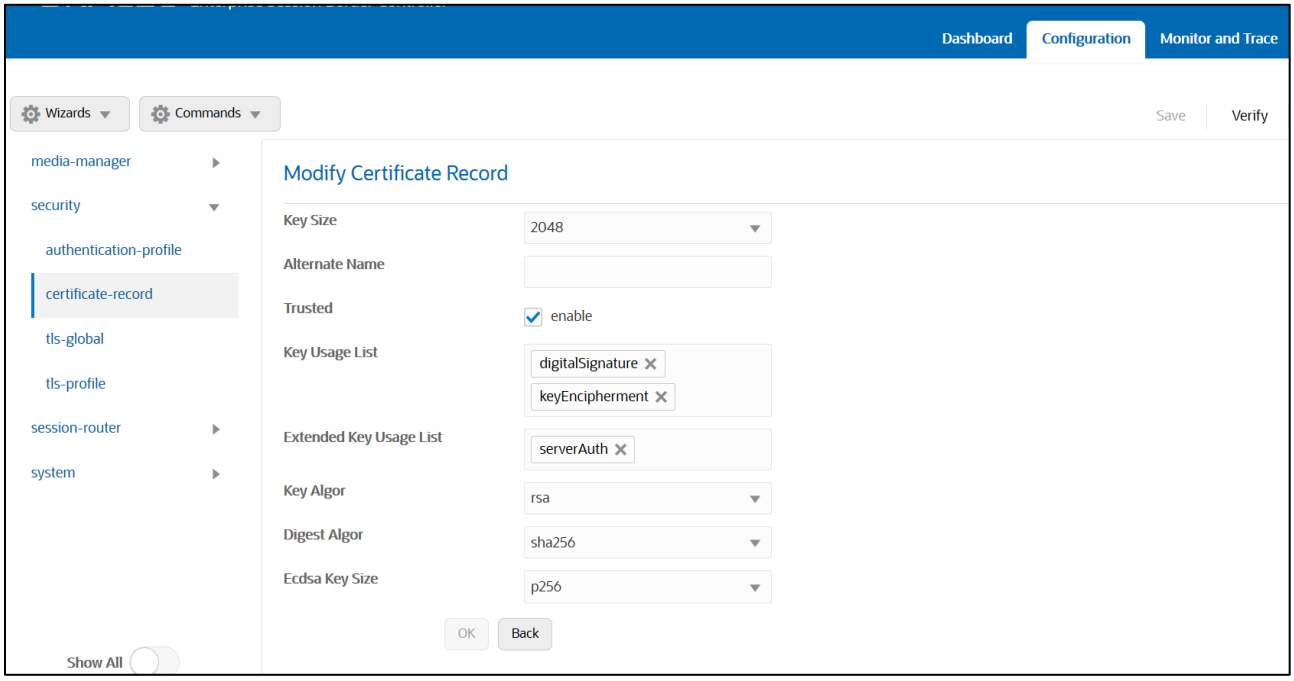
2) Deploy the SBC and Root certificates on the SBC

Step 1 – Creating the certificate record

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

https://www.twilio.com/docs/sip-trunking#rootCA





The table below specifies the parameters required for certificate configuration. Modify the configuration according to the certificates in your environment.

Config Parameter	Digicert Intermediate	DigiCert Root CA
Common Name	DigiCert SHA2 Secure Server CA	DigiCert Global Root CA
Key Size	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth
Key algor	rsa	rsa
Digest-algor	Sha256	Sha256

Step 2 – Generating a certificate signing request

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

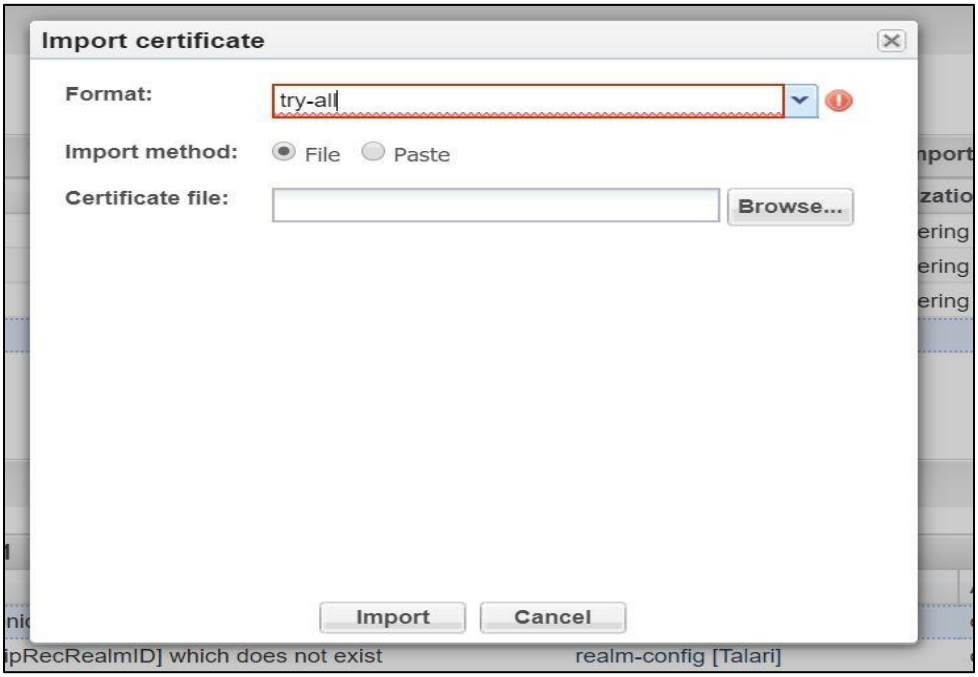
Please note – certificate signing request is only required to be executed for SBC Certificate – not for the root/intermediate certificates.

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

- Also, note that a save/activate is required

Step 3 – Deploy SBC & root certificates

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 done, issue save/activate from the WebGUI



Repeat these steps to import all the root and intermediate CA certificates into the SBC:
At this stage, all the required certificates have been imported to the SBC for Twilio Elastic SIP Trunk.

6.8.2 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.

6.8.2.1 Configuring Certificates

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

6.8.2.2 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.

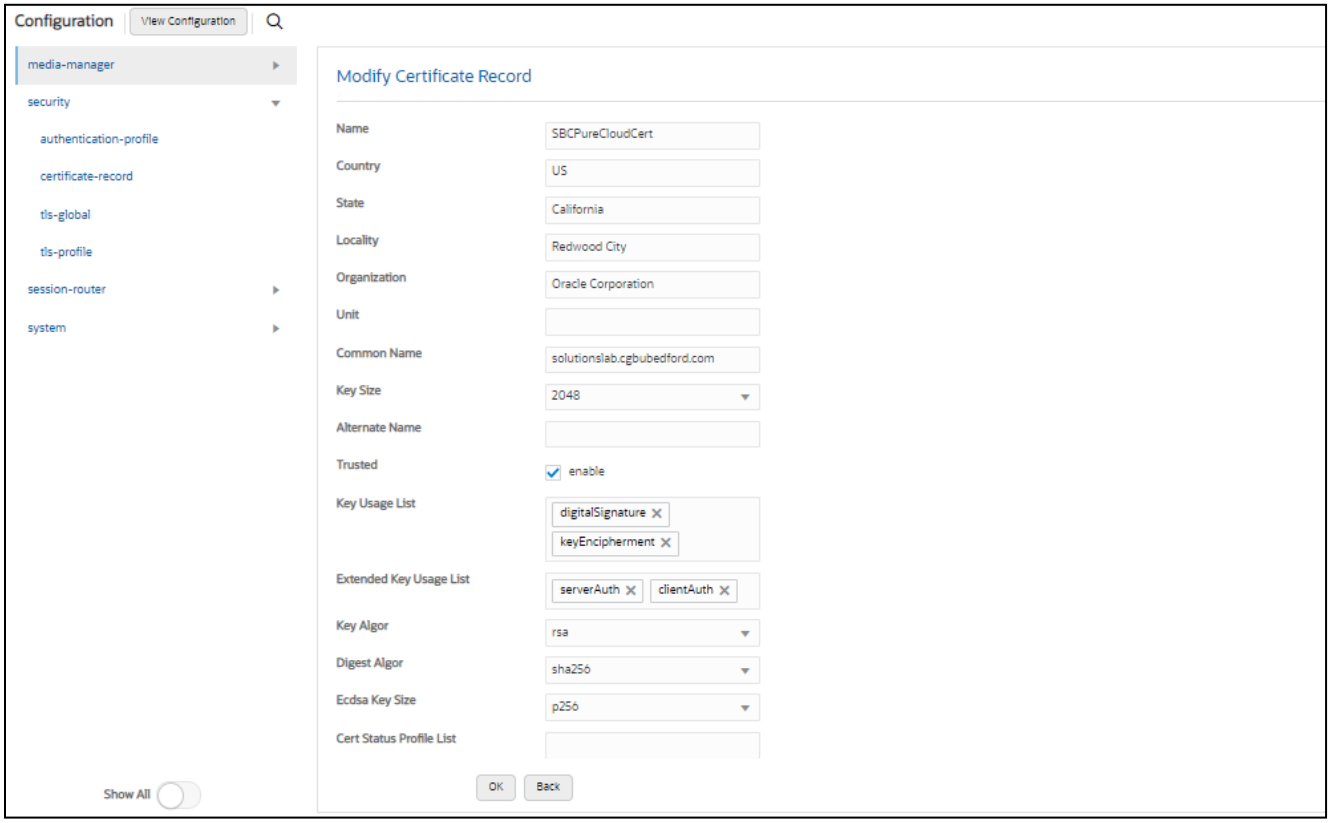
Here in this setup,We wil create two end entity certificates for BYOC Cloud.

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

Step 1 Configure SBC Certificate Record

To Configure the certificate record:

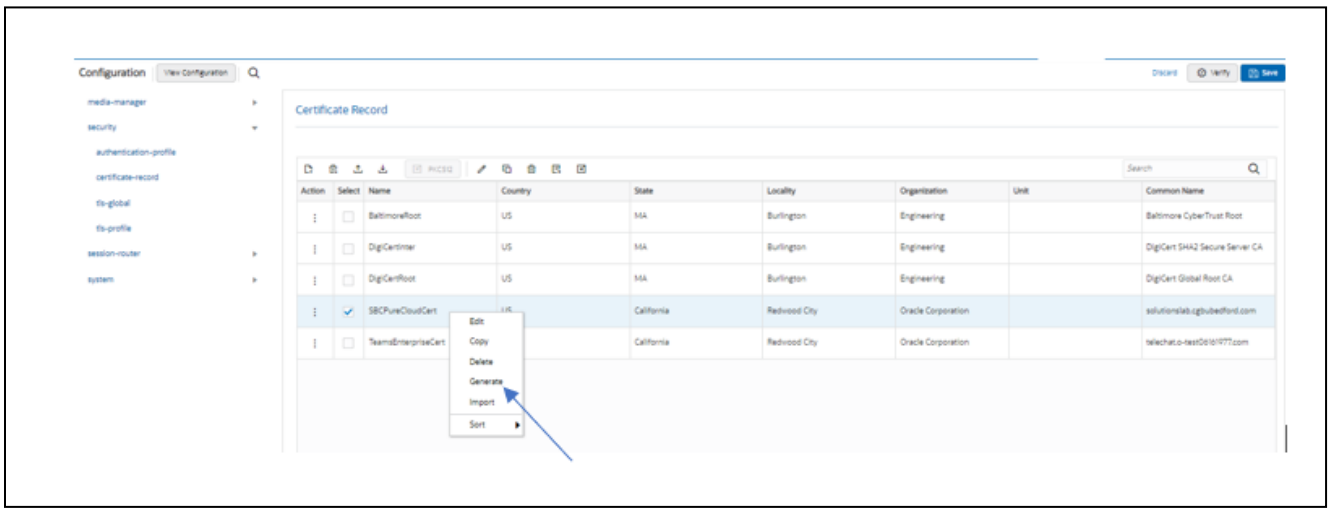
- Click Add, and configure the SBC certificate as shown below:

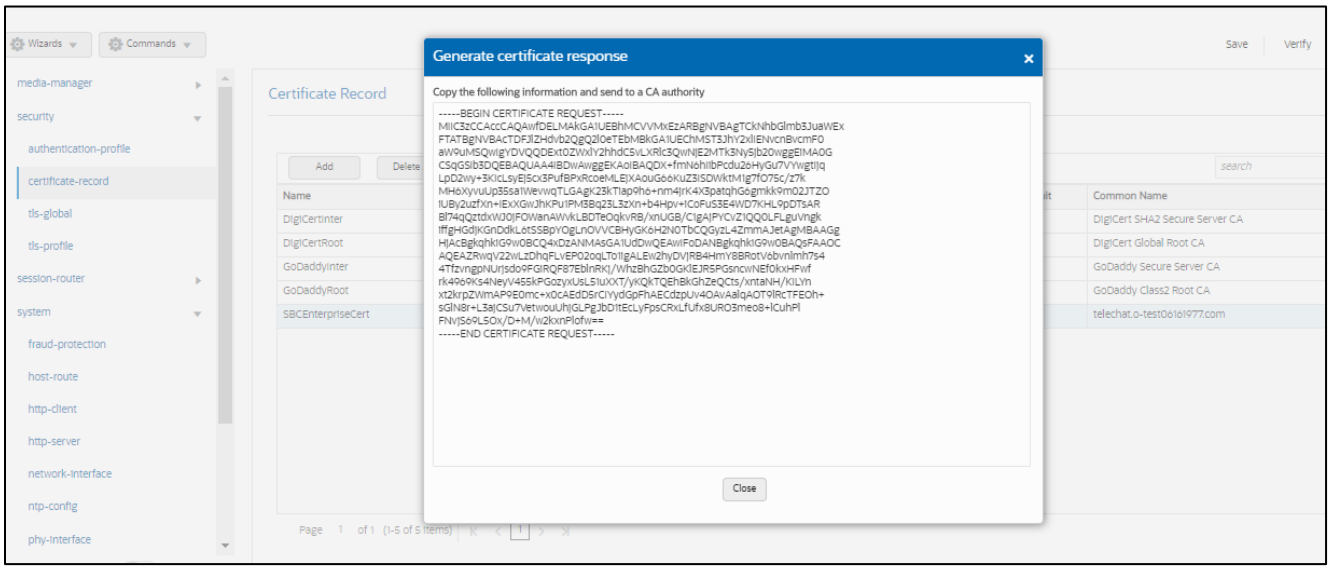


Step 2 – Generating a certificate signing request

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.



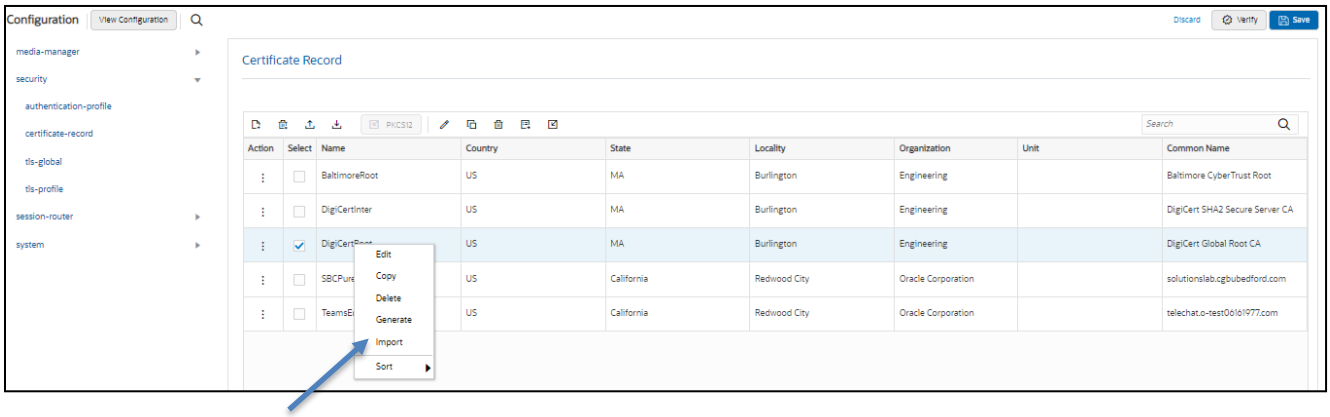


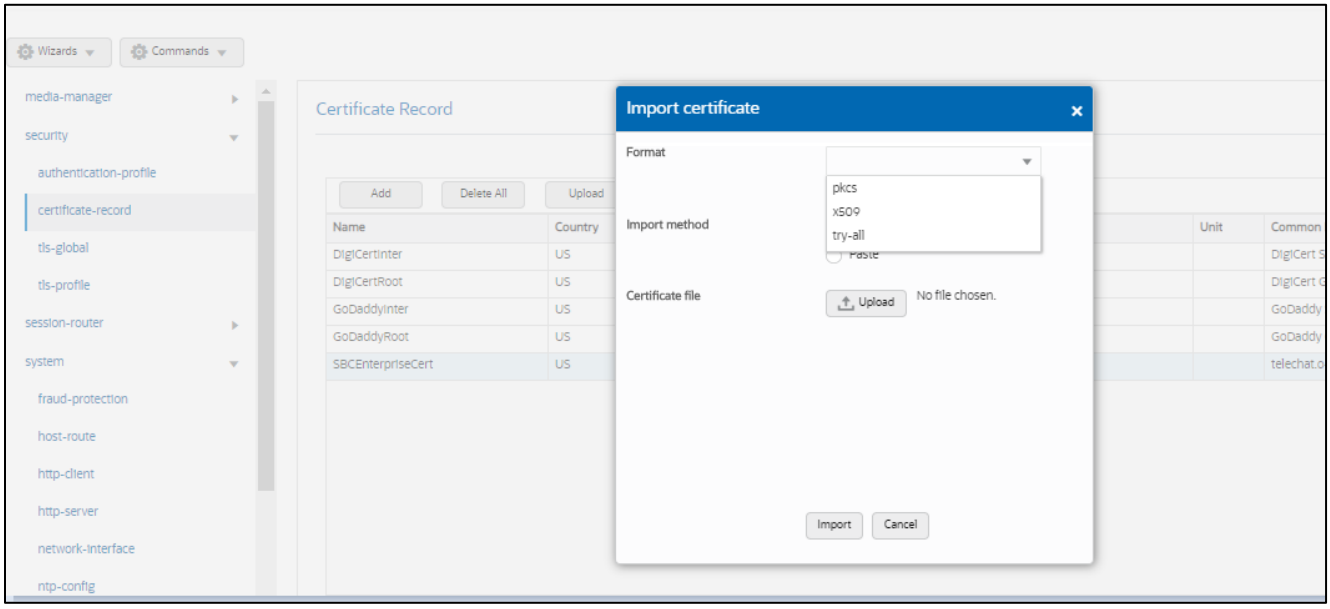
- copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, **a save and activate is required** before you can import the certificates to each certificate record created above.

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





6.8.2.3 Import CA Certificate

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

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

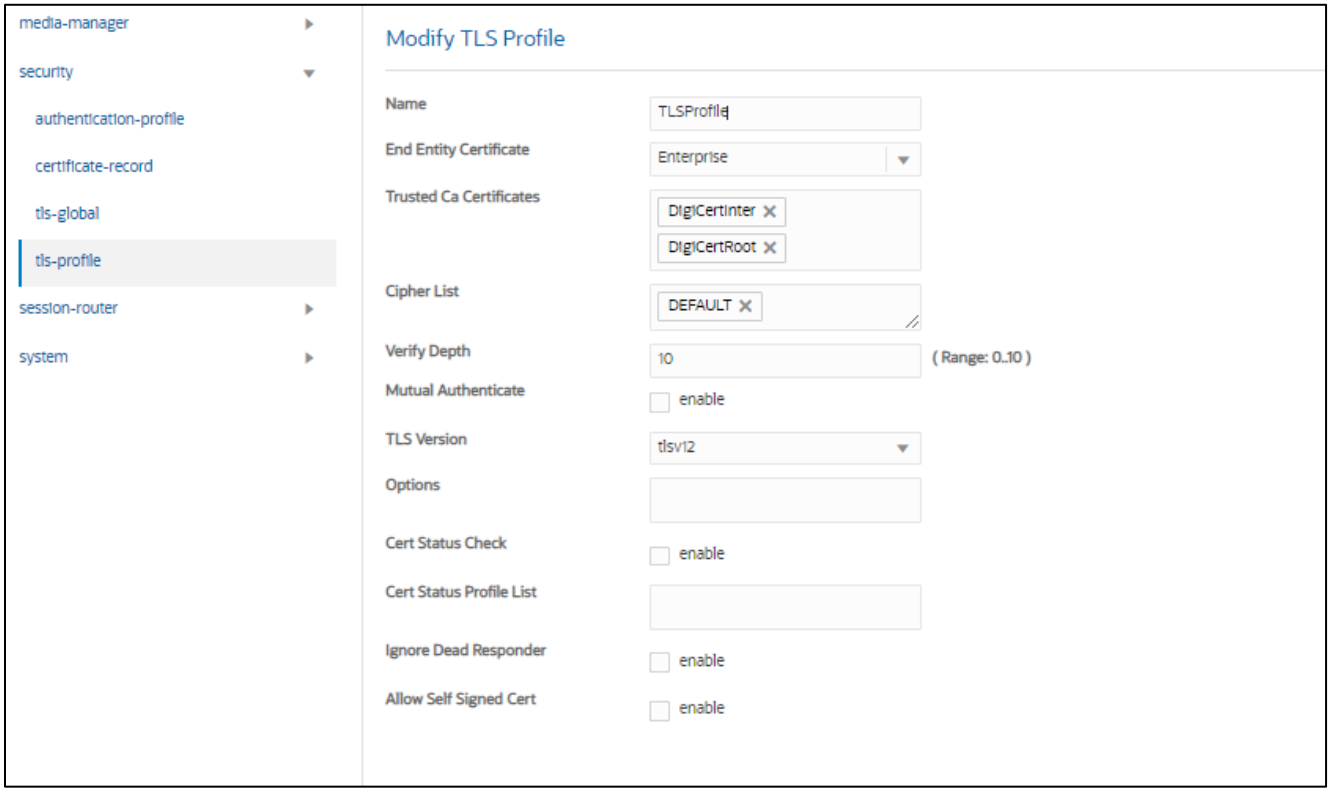
6.9. TLS-Profile

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

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

6.9.1 Twilio TLS Profile

The below is the TLS profile configured for the Twilio Elastic SIP Trunk :



6.9.2 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*

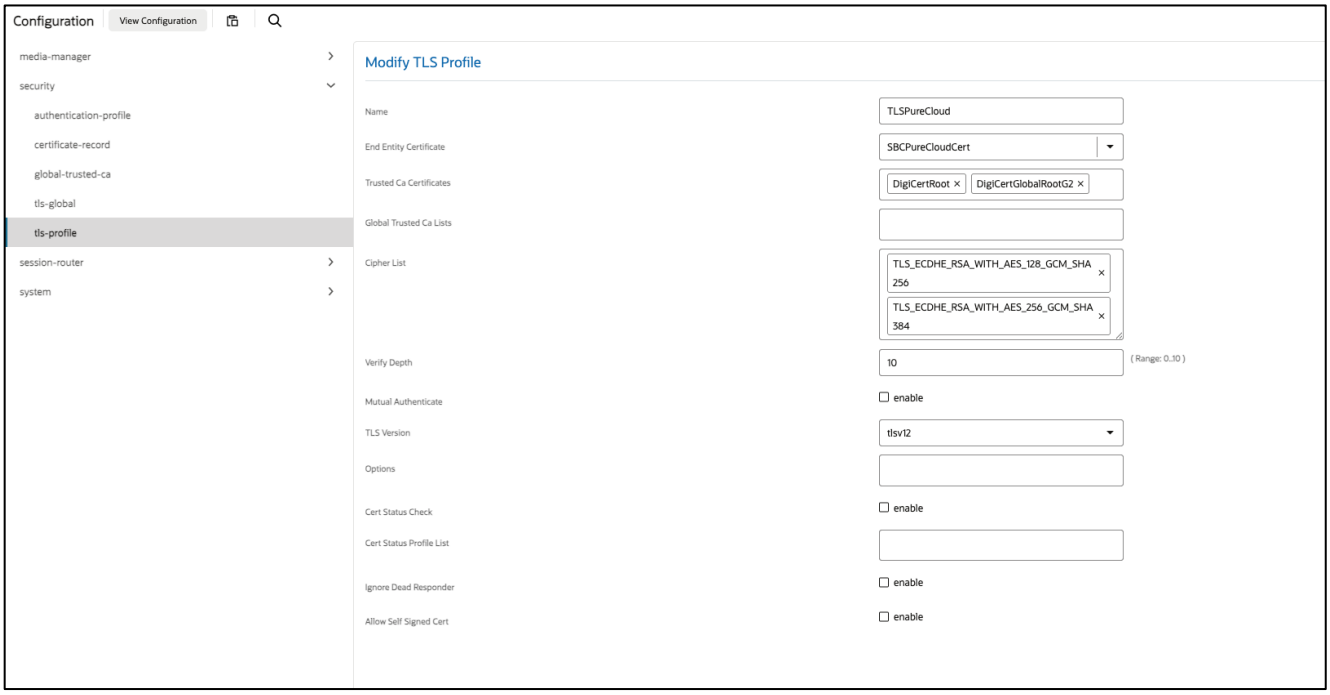
On March 24, 2025, Genesys announced that in a future release, Genesys Cloud will no longer support the following BYOC Cloud TLS ciphers.

- 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.

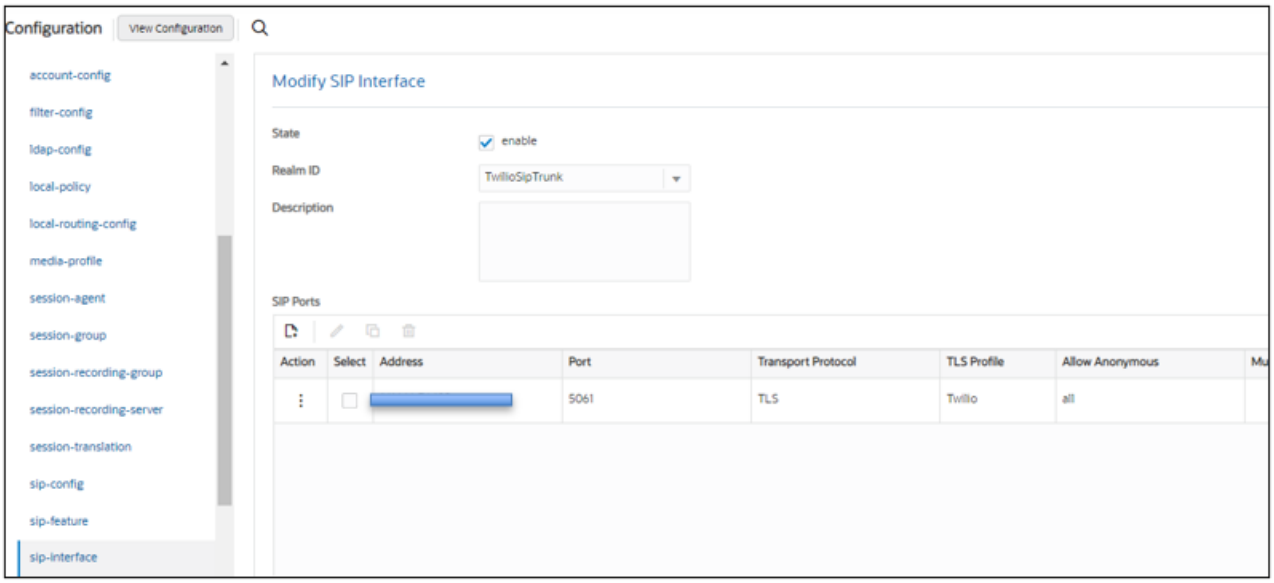


6.10. Configure SIP Interfaces

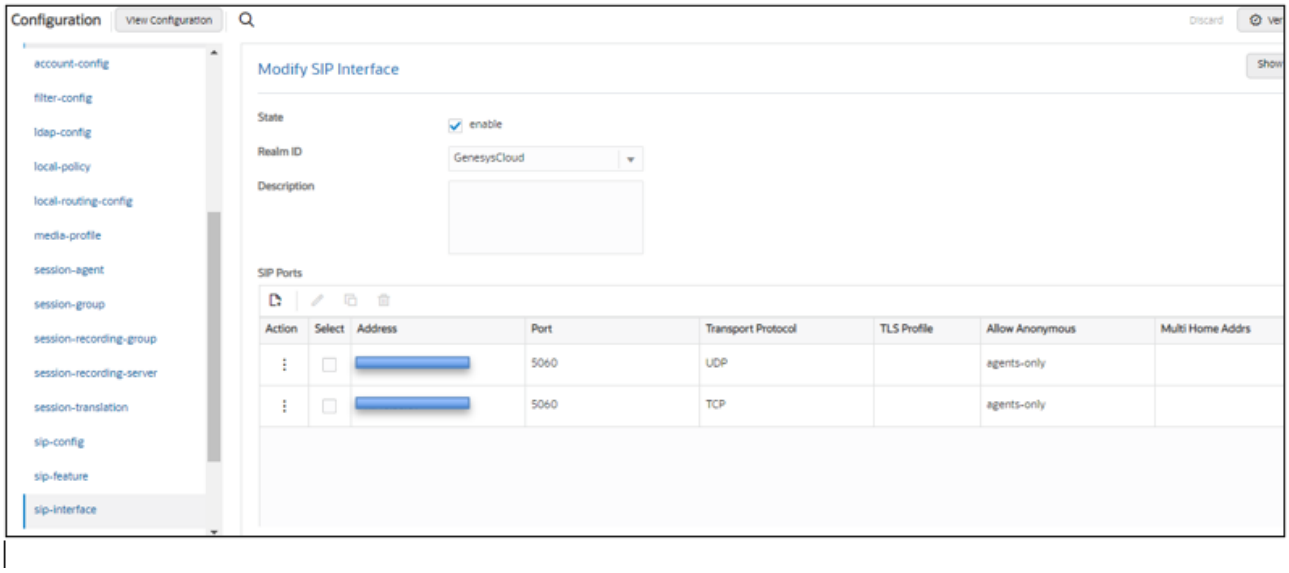
Navigate to sip-interface under session-router and configure the sip-interface as shown below. Please configure the below settings under the sip-interface.

Please Configure sip-interface for the Twilio Elastic SIP Trunk as below:

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



Similarly, Configure sip-interface for the BYOC Cloud as below:



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

6.11. Configure session-agent

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

Navigate to session-router->Session-Agent and Configure the session-agents for the Twilio Elastic SIP Trunk

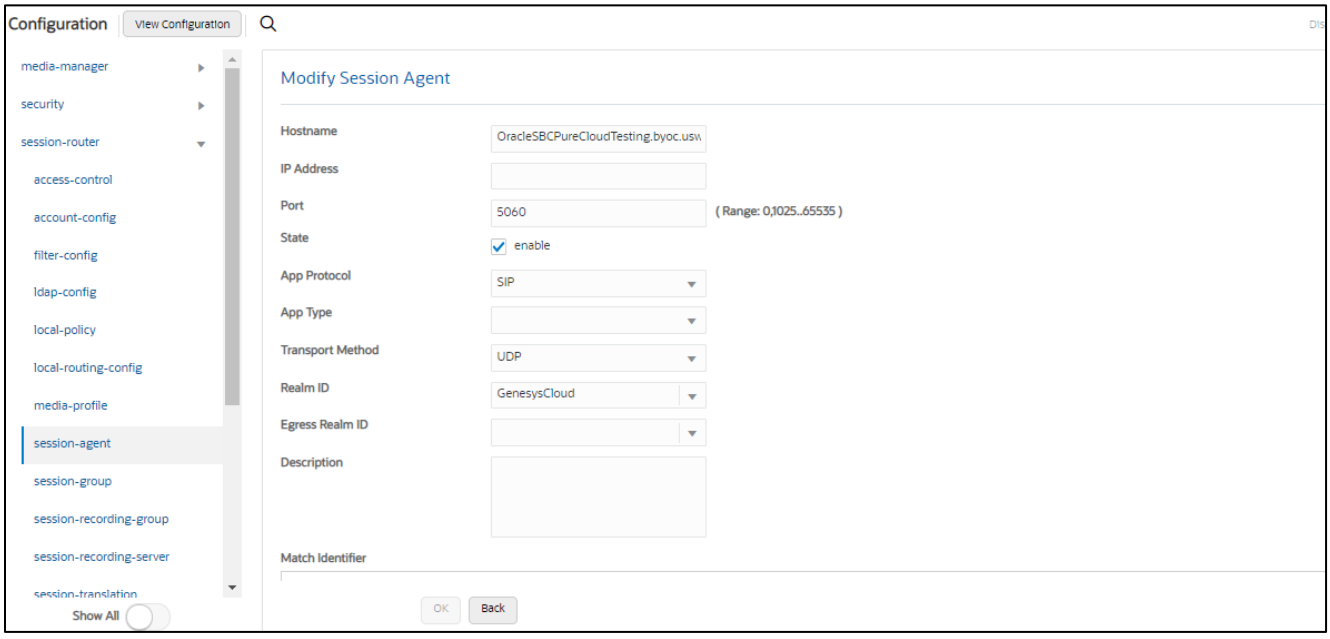
- Host name to “oracle.pstn.twilio.com”**, port to 5061
- realm-id – needs to match the realm created for the Twilio Elastic SIP Trunk
- transport set to “staticTLS”

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

- {example}.pstn.ashburn.twilio.com (North America Virginia)
- {example}.pstn.umatilla.twilio.com (North America Oregon)
- {example}.pstn.dublin.twilio.com (Europe Ireland)
- {example}.pstn.frankfurt.twilio.com (Europe Frankfurt)
- {example}.pstn.singapore.twilio.com (Asia Pacific Singapore)
- {example}.pstn.tokyo.twilio.com (Asia Pacific Tokyo)
- {example}.pstn.sao-paulo.twilio.com (South America São Paulo)
- {example}.pstn.sydney.twilio.com (Asia Pacific Sydney)

Click here for more information on Twilio Elastic SIP Trunking IP Address

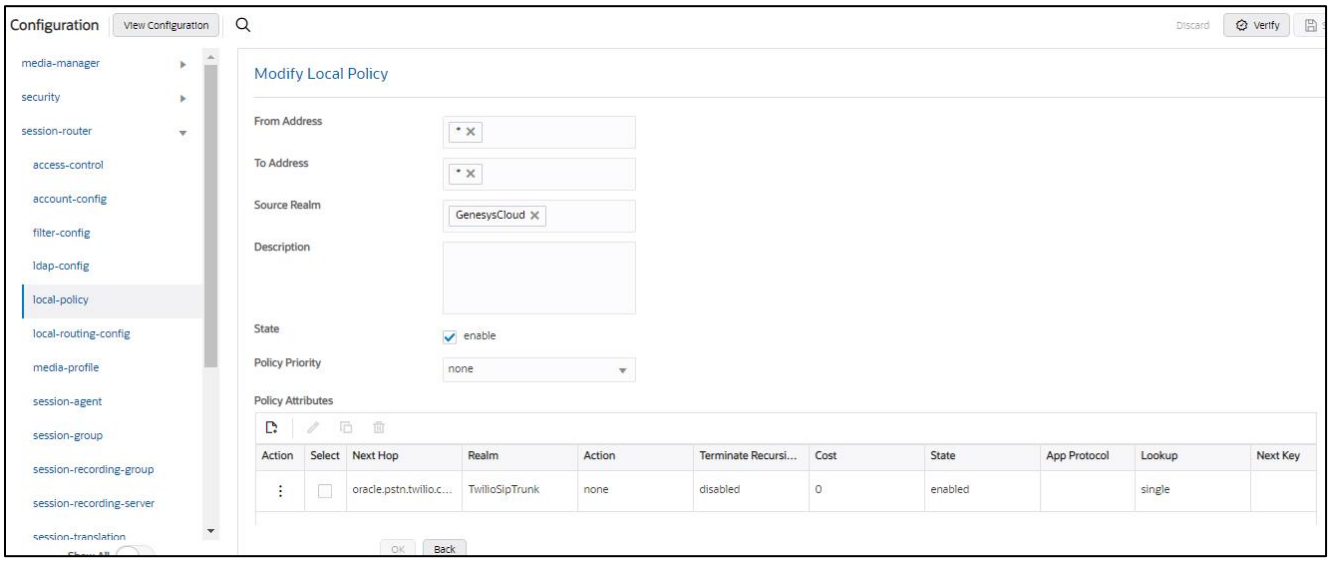
Similarly, configure the session-agents for the BYOC Cloud :



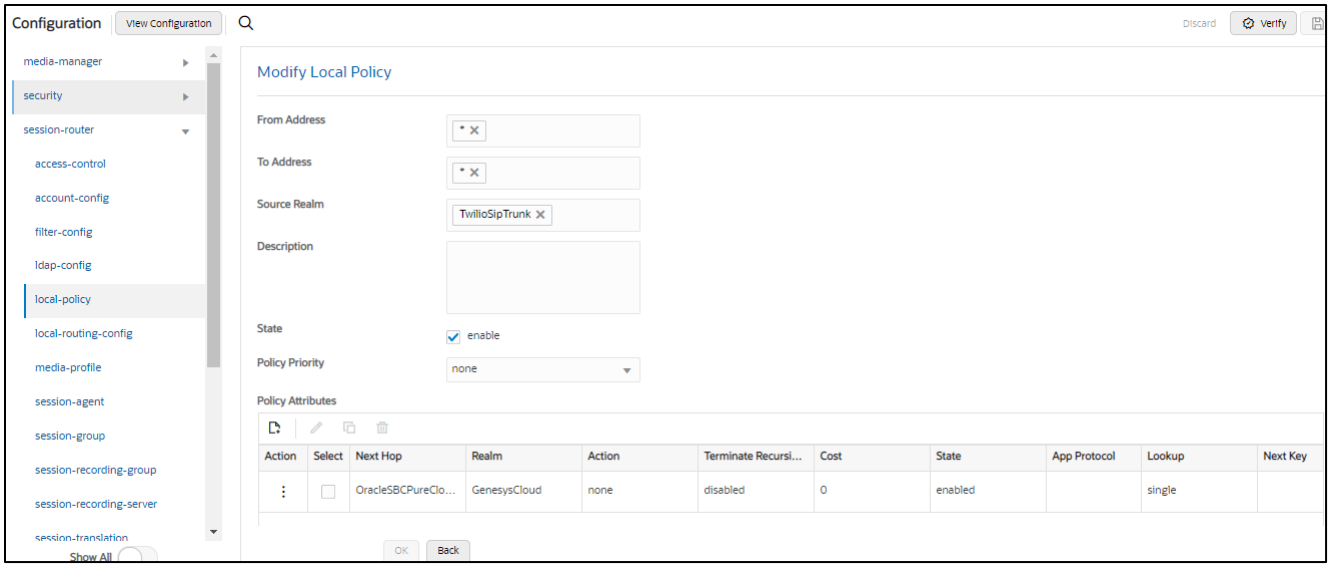
6.12. Configure local-policy

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.

To route the calls from BYOC Cloud to Twilo Sip Trunk, Use the below local –policy



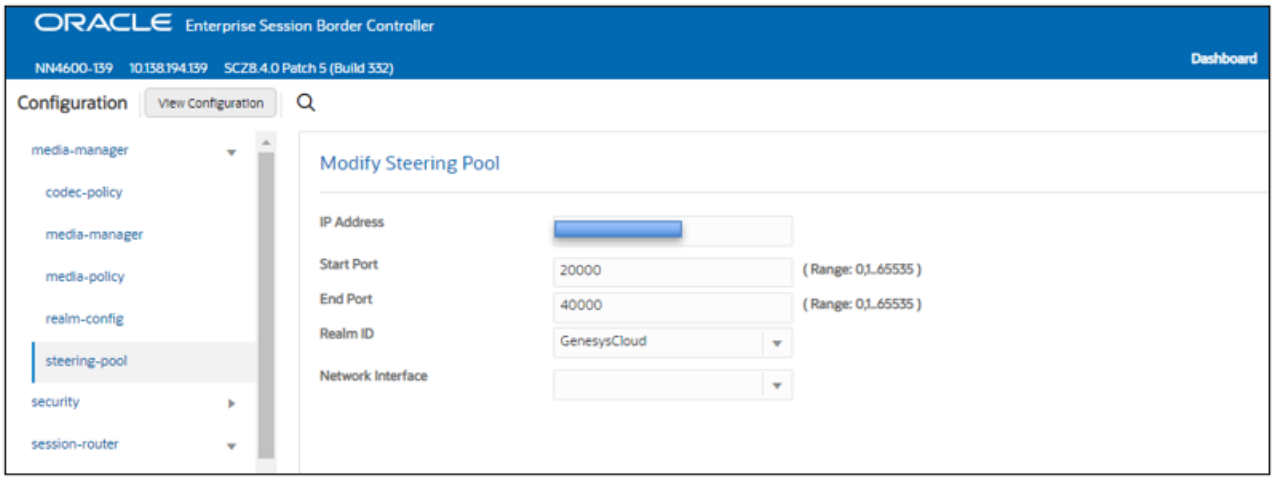
To route the calls from the Twilio Elastic SIP Trunk to BYOC Cloud , Use the below local –policy



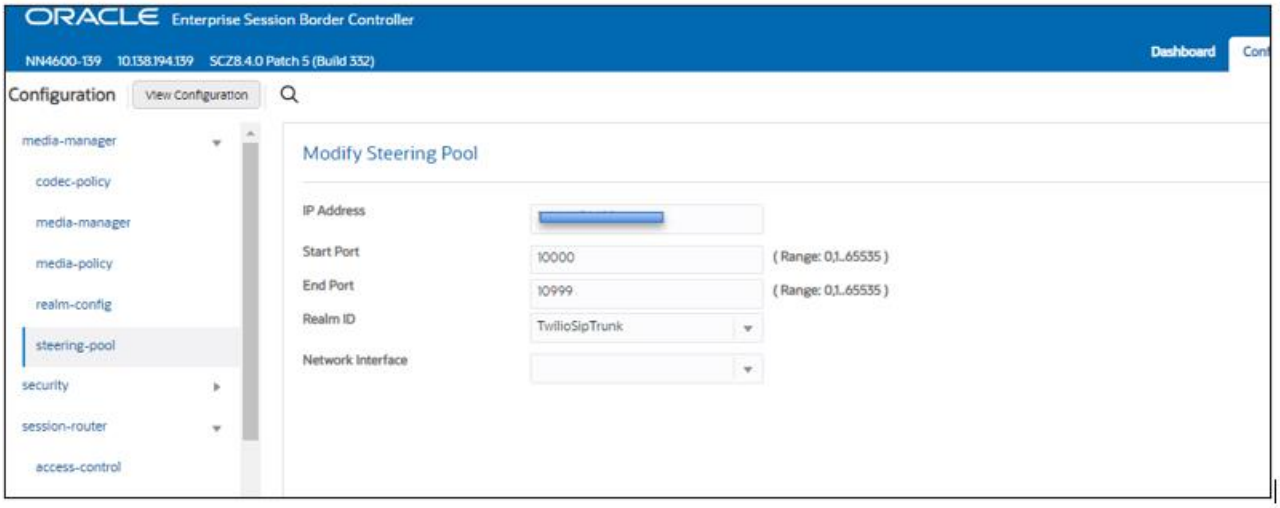
6.13. Configure steering-pool

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

BYOC Cloud Steering pool.



Twilio steering pool.



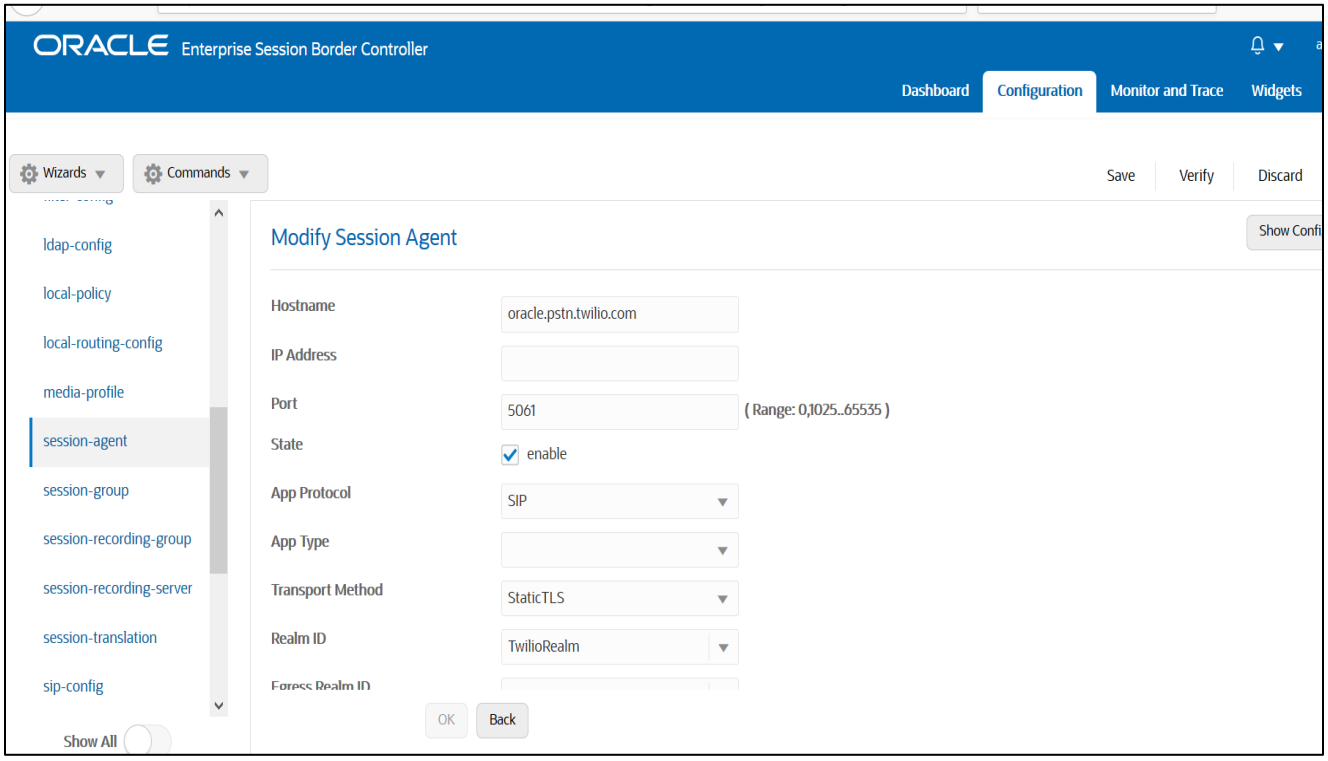
6.14. Enable OPTIONS Ping response.

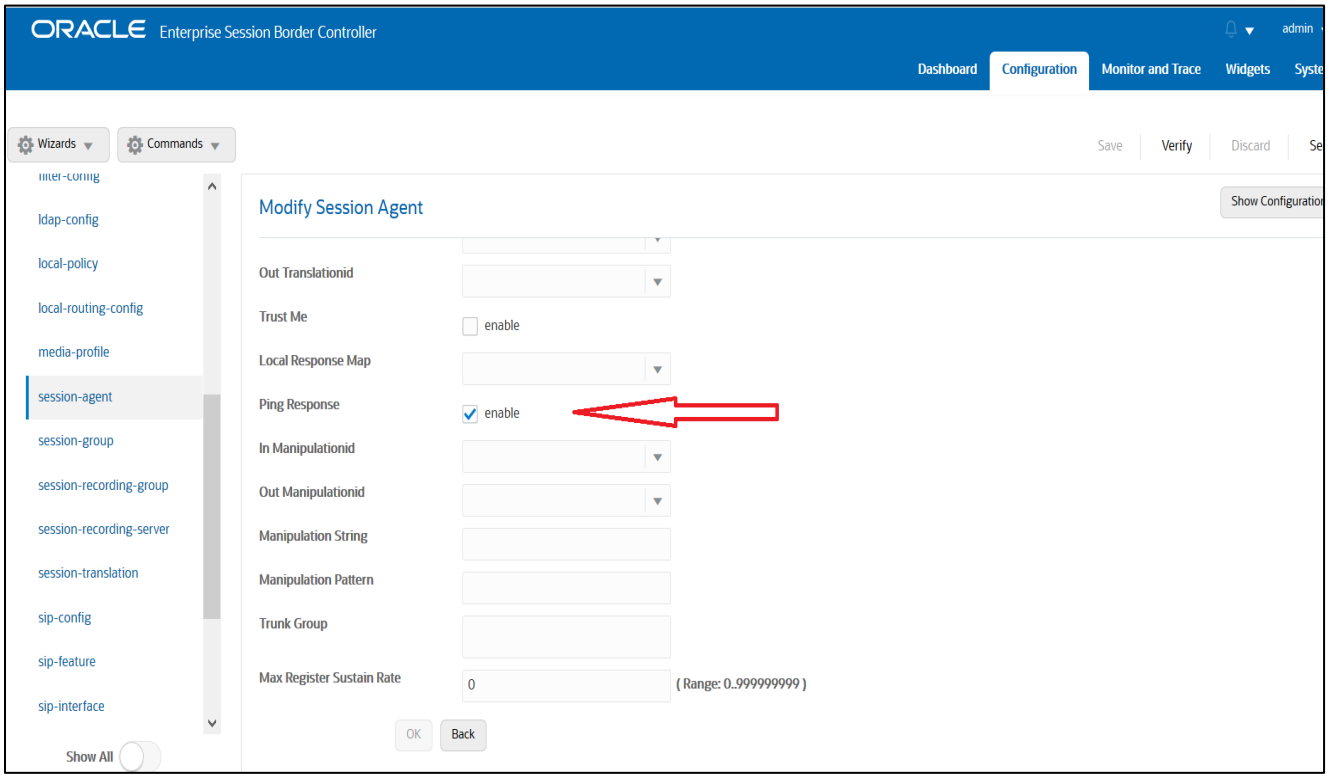
To simplify the ORACLE SBC sip manipulation, from GA Release SCZ830m1p7, there is a new parameter introduced under the **Session agent** configuration element.

The parameter name is **Ping response**.

Ping Response:

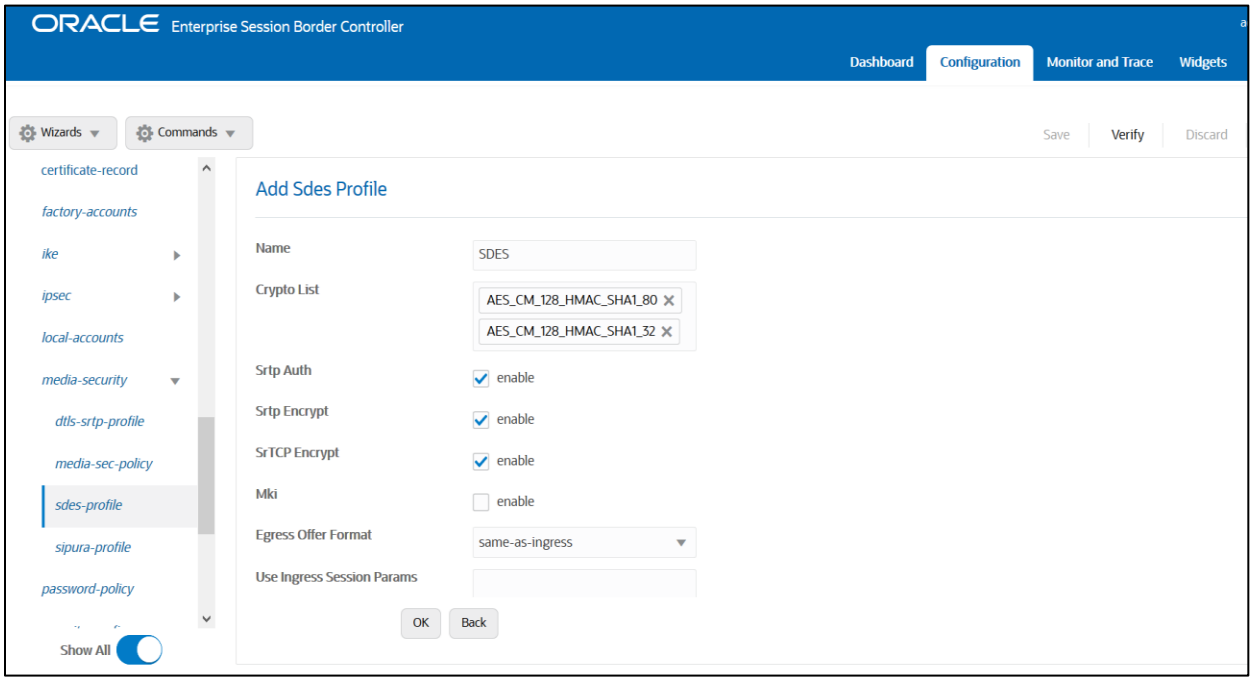
When this parameter is enabled, the SBC responds with a 200 OK to all Sip Options Pings it receives from trusted agents. This takes the place of the current Sip Manipulation, RepondOptions.


ORACLE Enterprise Session Border Controller
Dashboard
Configuration
Monitor and Trace
Widgets
Wizards
Commands
Save
Verify
Discard
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
Show All
Modify Session Agent
Hostname
oracle.pstn.twilio.com
IP Address
Port
5061
(Range: 0,1025..65535)
State
enable
App Protocol
SIP
App Type
Transport Method
StaticTLS
Realm ID
TwilioRealm
OK
Back


ORACLE Enterprise Session Border Controller
admin
Dashboard
Configuration
Monitor and Trace
Widgets
Wizards
Commands
Save
Verify
Discard
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
Show All
Modify Session Agent
Out Translationid
Trust Me
enable
Local Response Map
Ping Response
enable
In Manipulationid
Out Manipulationid
Manipulation String
Manipulation Pattern
Trunk Group
Max Register Sustain Rate
0
(Range: 0..999999999)
OK
Back

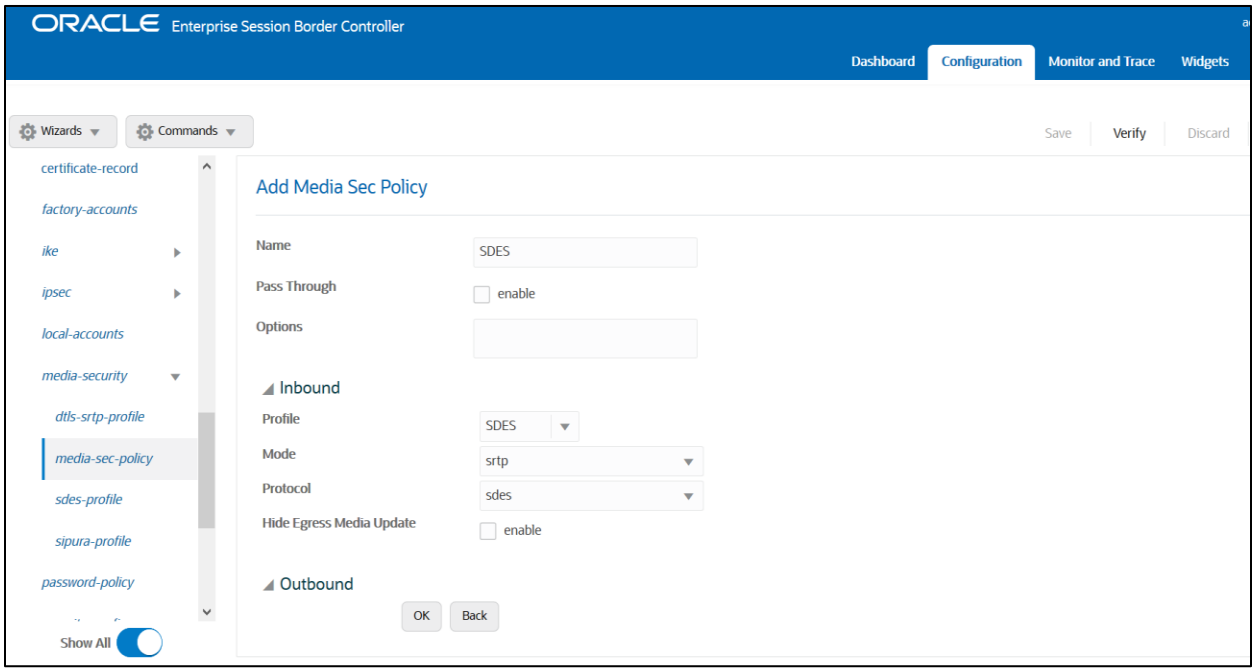
6.15. Configure sdes profile

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

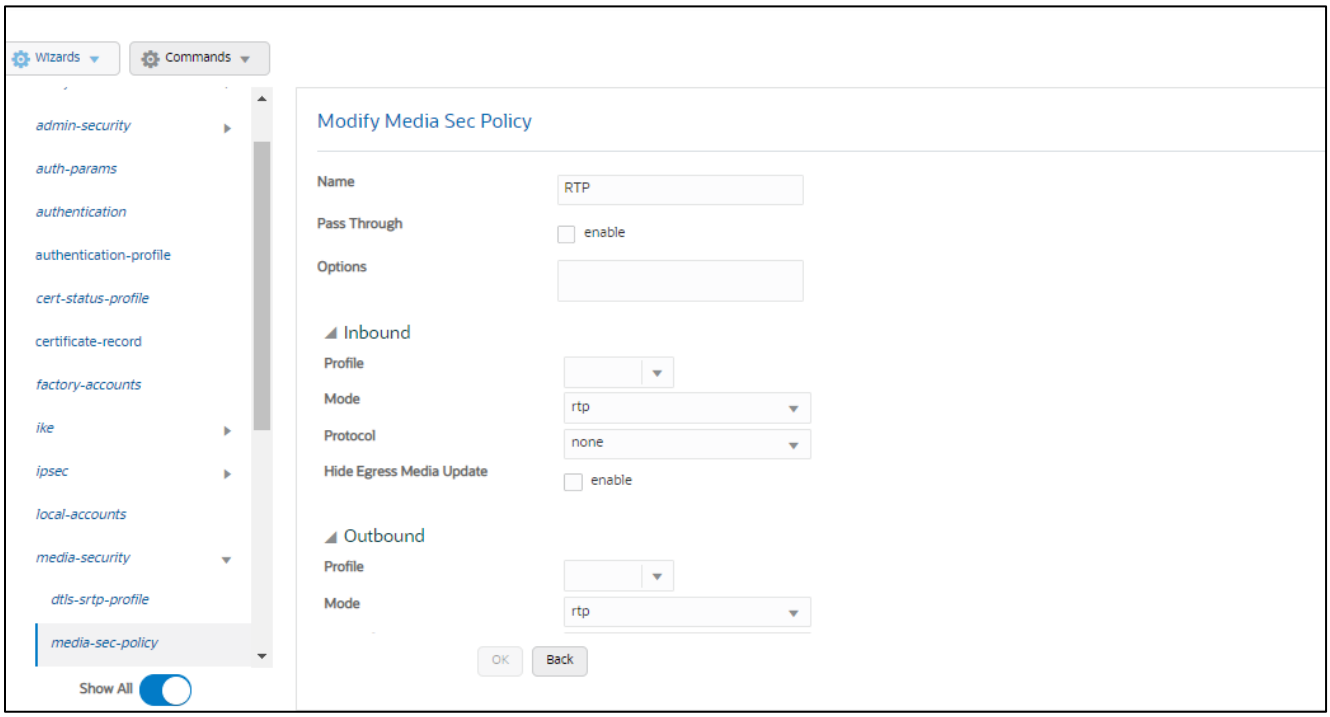


6.16. Configure Media Security Profile

Please Navigate to →Security → Media Security →media Sec policy and create the policy as below:
Create Media Sec policy with name SDES, which will have the sdes profile, created above.
Assign this media policy to Twilio Realm as it use TLS/SRTP.



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



6.17 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

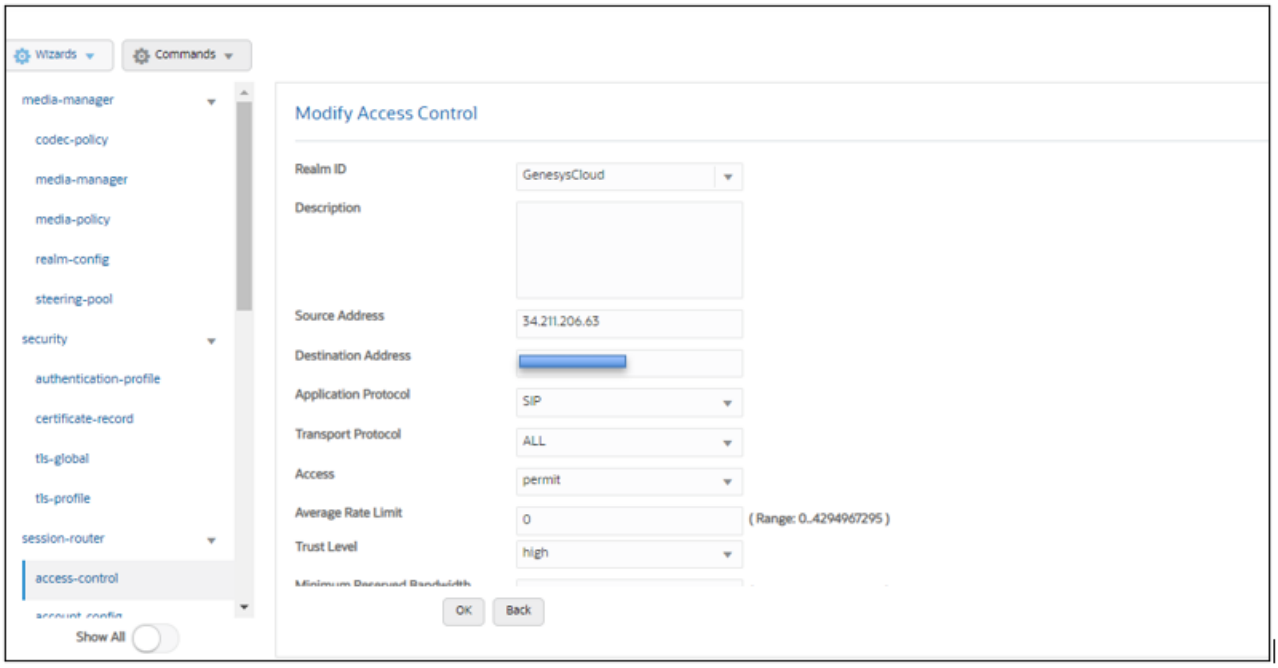
Please use the example below to configure access controls in your environment for both BYOC Cloud IP's, as well as SIP Trunk IP's (if applicable).

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/

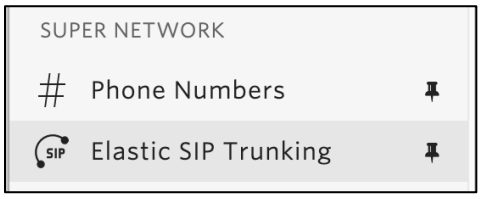
Configure access-control for each IP BYOC Cloud IP Address or Subnet as shown in the below example.



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.

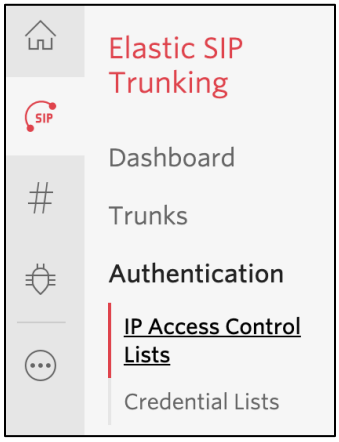
7. Twilio Elastic SIP Trunking Configuration

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

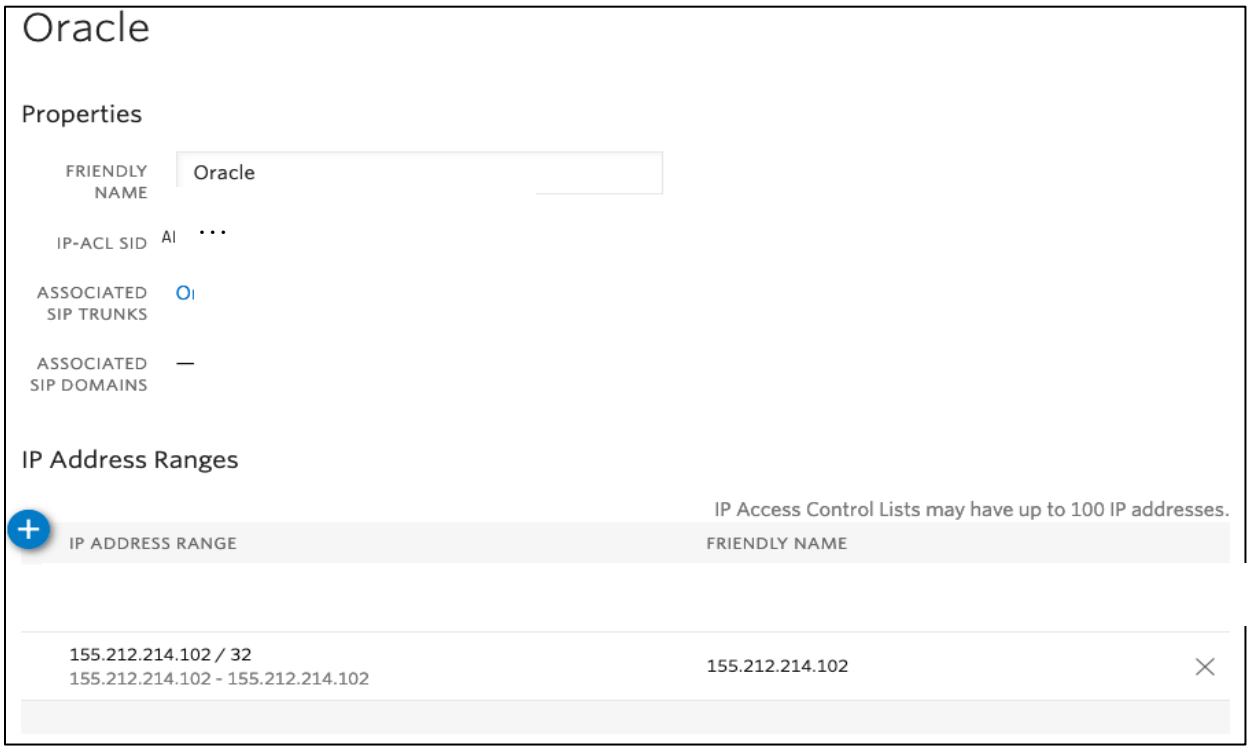


7.1. Create an IP-ACL rule

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



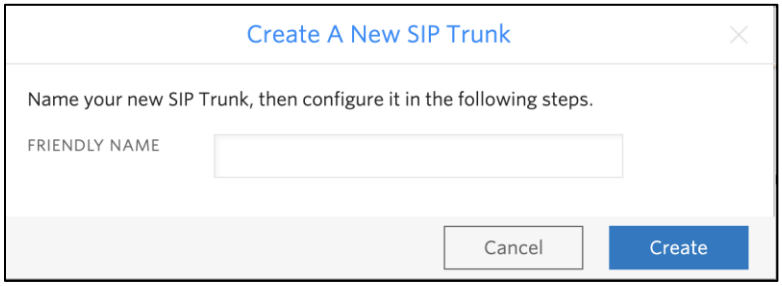
Create a new IP-ACL, for example call it "Oracle" and add your SBCs IP addresses.



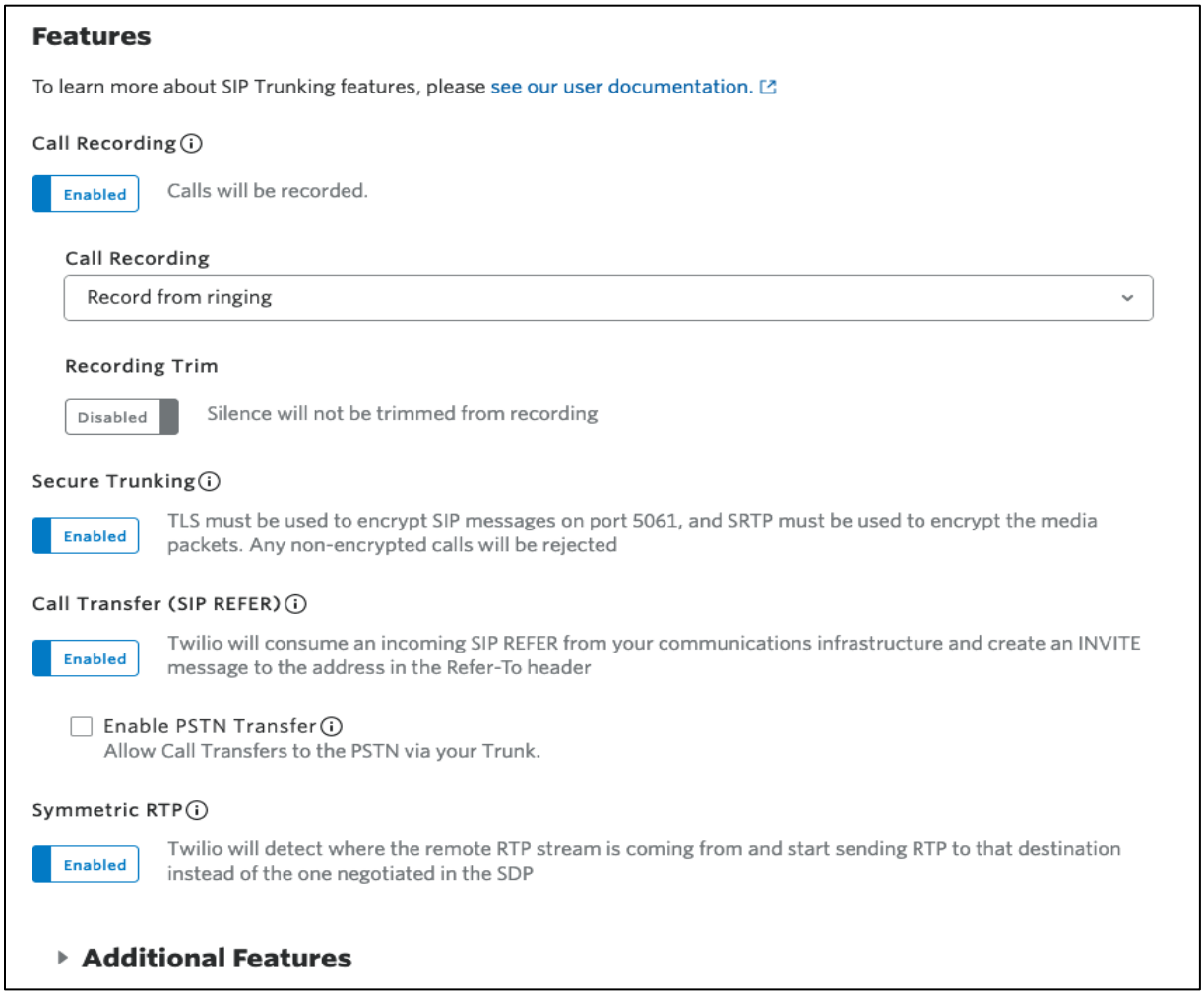
7.2. Create a new Trunk

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

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



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

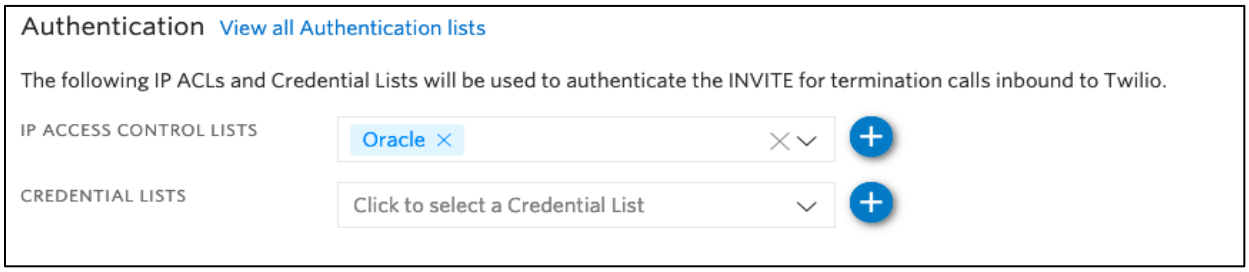


In the **Termination** section, select a Termination SIP URI.

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

Or

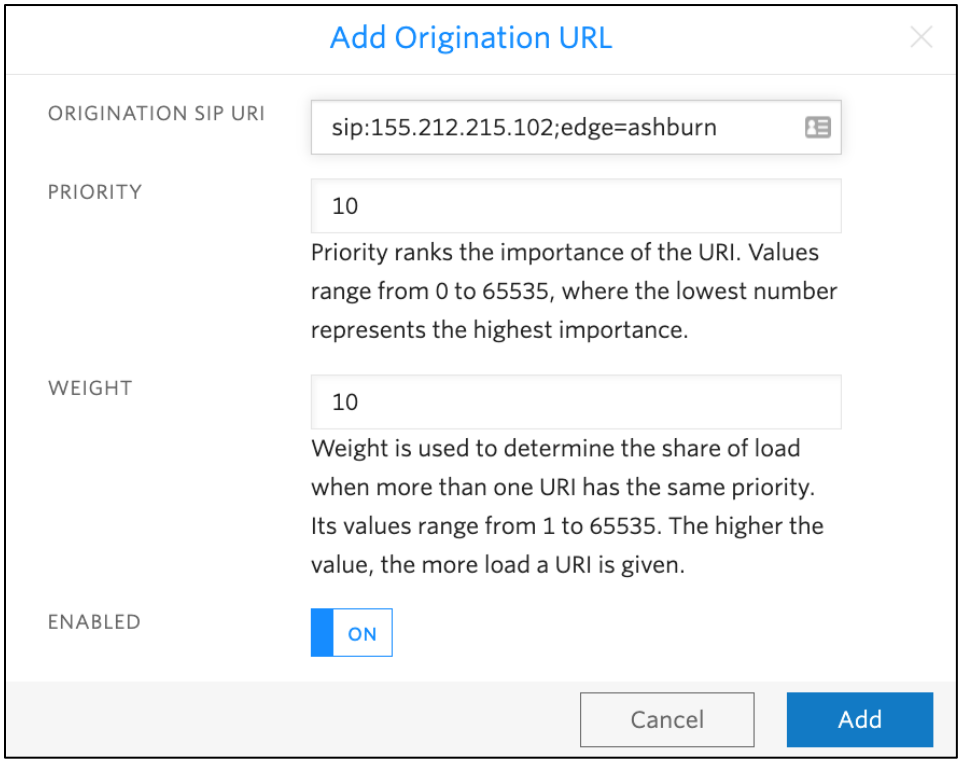
Assign the IP ACL ("Oracle") that you created in the previous step.



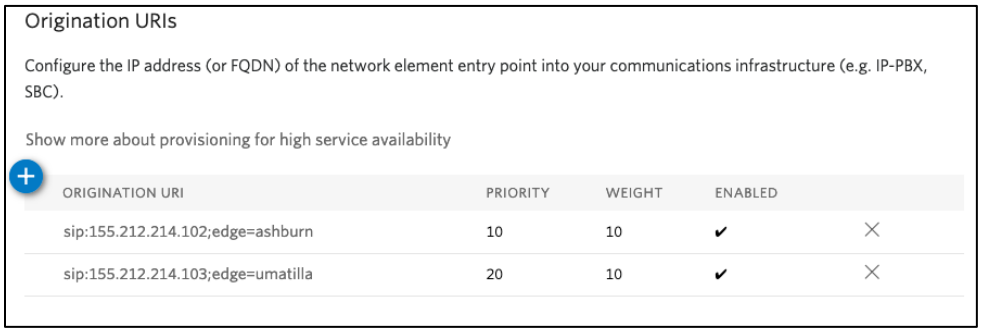
In the **Origination** section, we will need to add Origination URI's to route traffic towards your Oracle SBC. The recommended practice is to configure a redundant mesh per geographic region (in this context a

region is one of North America, Europe, etc.). In this case, we configure two Origination URIs, each egressing from a different Twilio Edge.

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



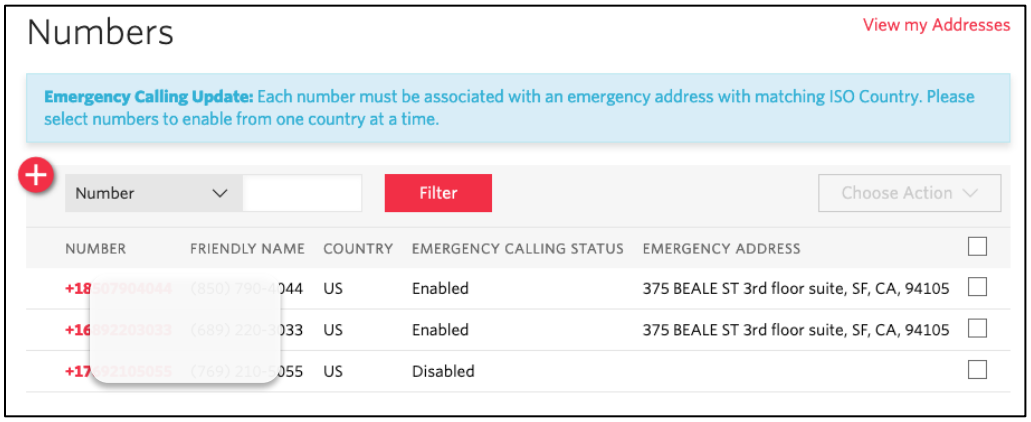
Continue to add the other Origination URIs, so you have the following configuration:



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

7.3. Associate Phone Numbers on your Trunk

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



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 and Twilio Elastic SIP Trunk.

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 BYOC 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

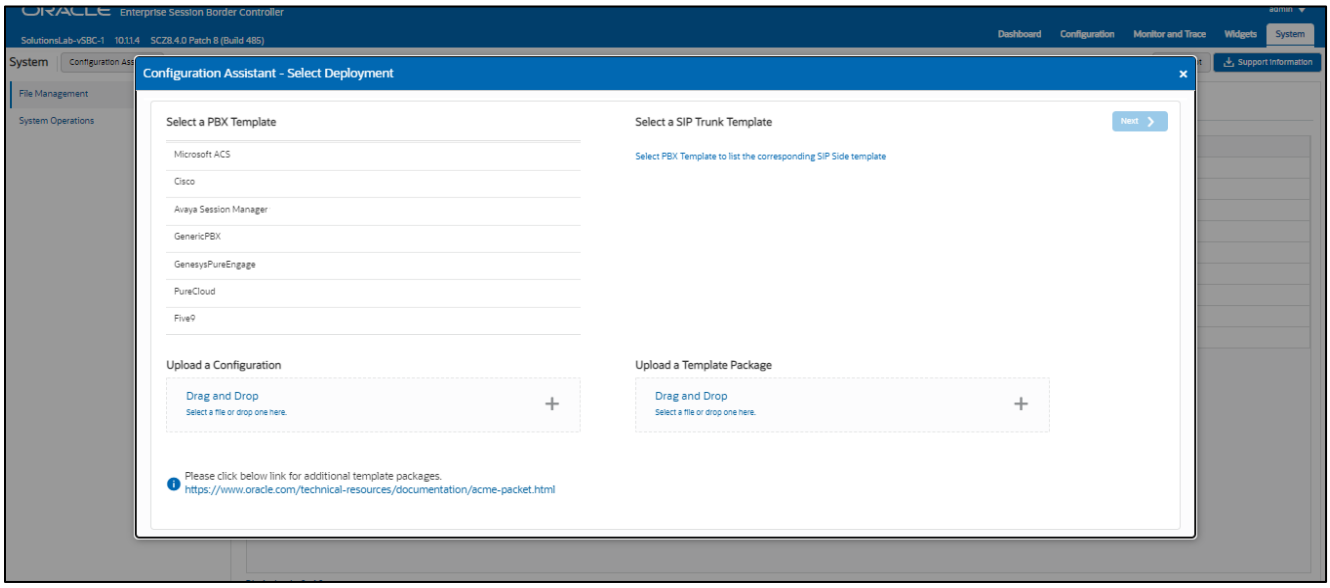
The Oracle SBC WebGui can be accessed by entering the following in your web browser.
http(s)://<SBC Management IP>.

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

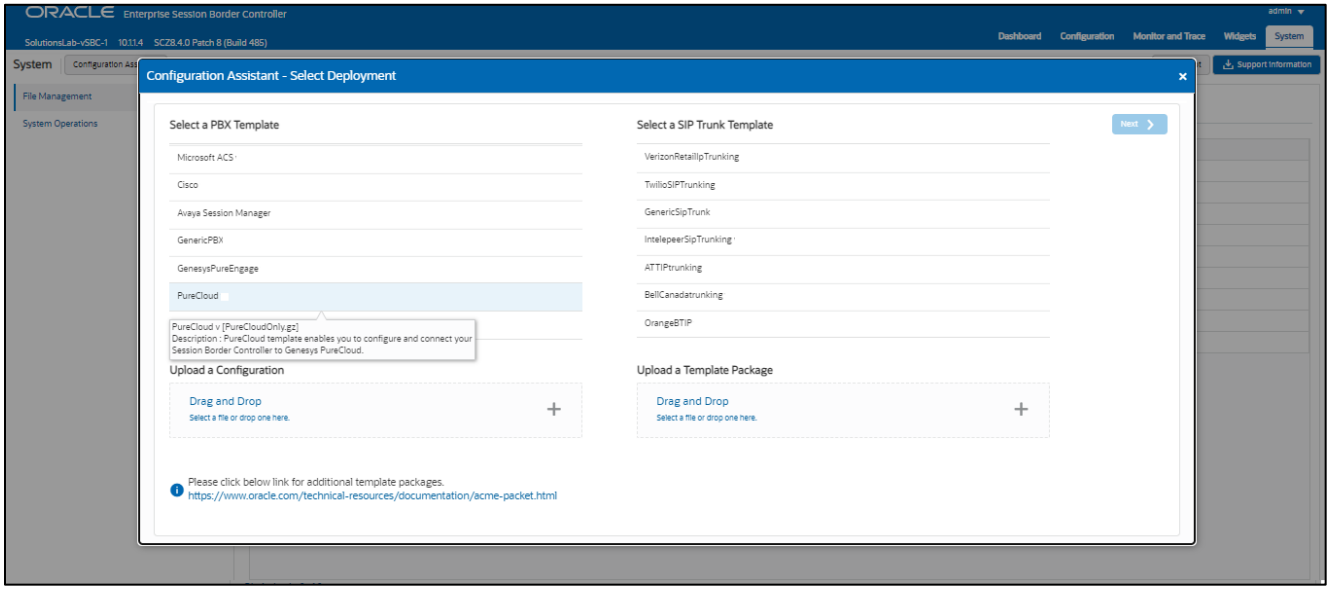
If there is no configuration on the SBC, the configuration assistant will show immediately upon login to the SBC GUI as shown below

BYOC Cloud Configuration Assistant

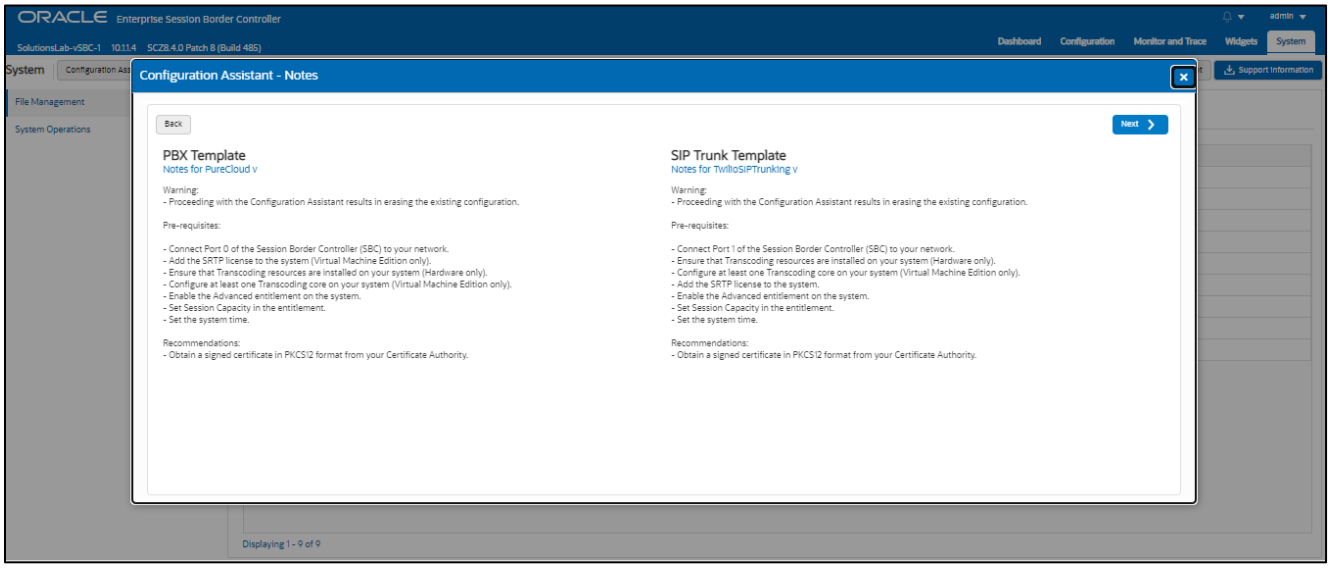
For a new SBC deployment, once access to the GUI is configured, you will see the following when logging in for the first time:



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



Select TwilioSIPTrunking 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:



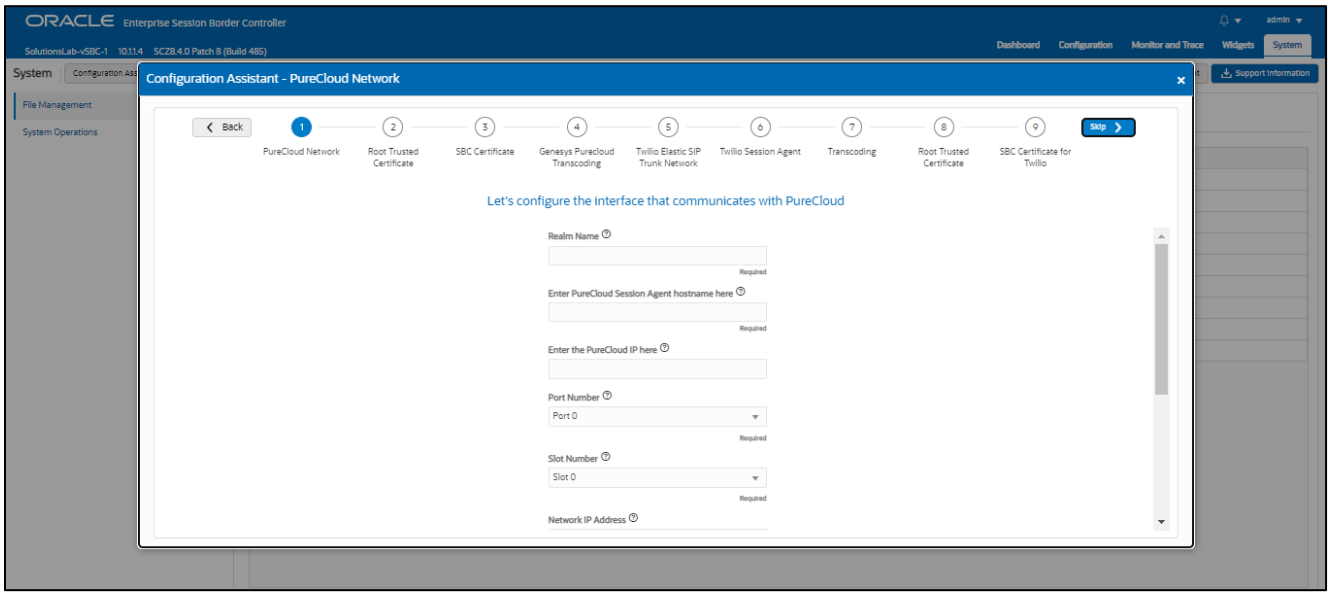
Clicking “Next” on the Notes page triggers the configuration assistant to do a system check. This ensures that all of the system requirements for the platform and sip trunk you have selected have been met before proceeding to configuration pages. If they have not been met, you will be greeted by a page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

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

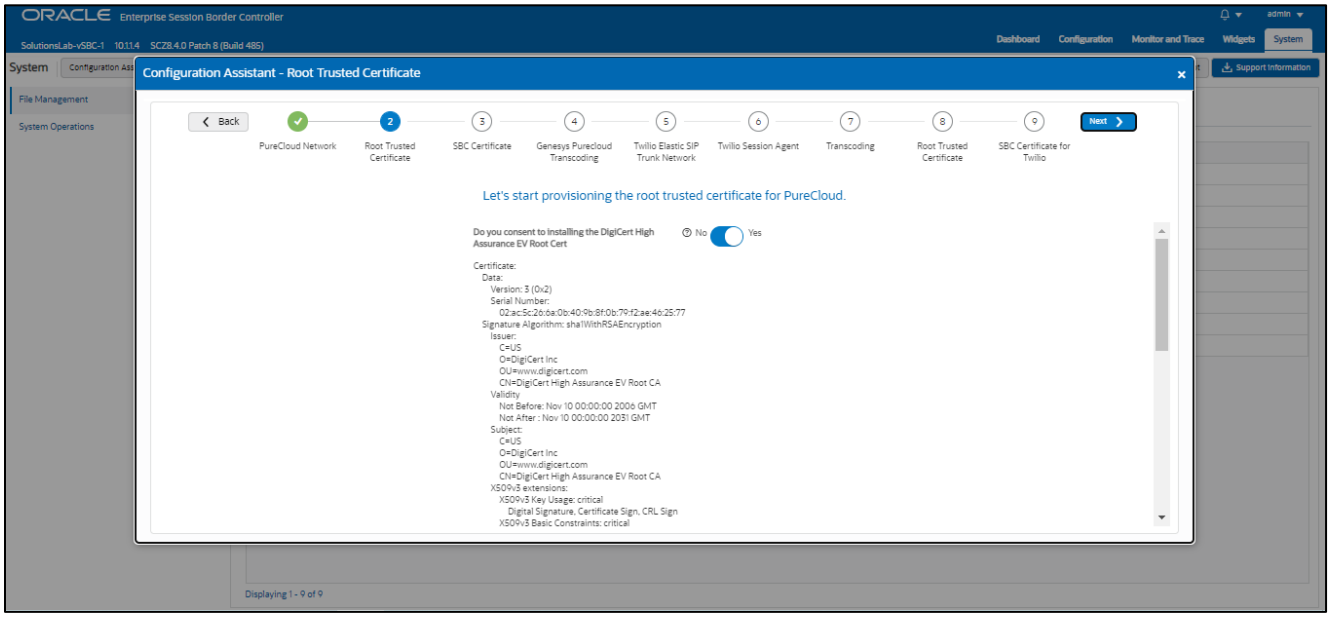
Next to each field is a help icon. If you hover over the icon, you will be provided with a description or definition of each filed. Also, pay close attention to which fields are listed as “required”.



Page 2 - Import DigiCert Trusted CA Certificate for BYOC Cloud

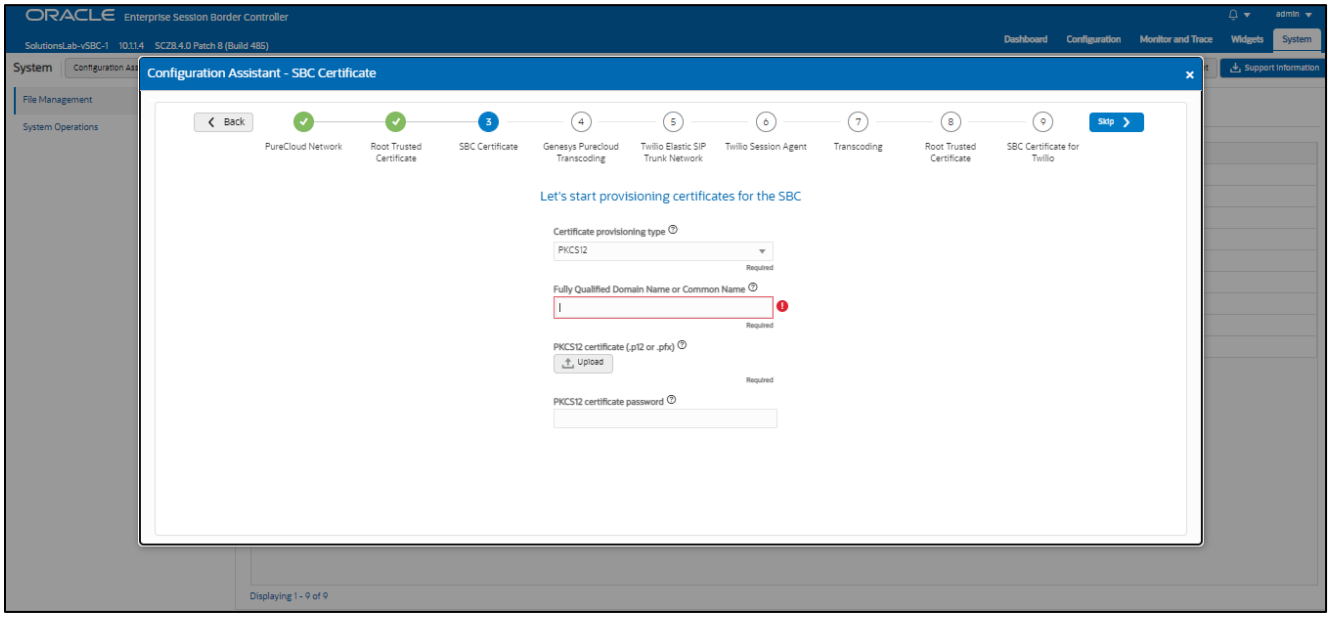
Page 2 of this template is where the SBC will import the **DigiCert High Assurance EV Root Cert CA** certificate, which BYOC Cloud uses to sign the certificates it presents to the SBC during the TLS handshake.

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



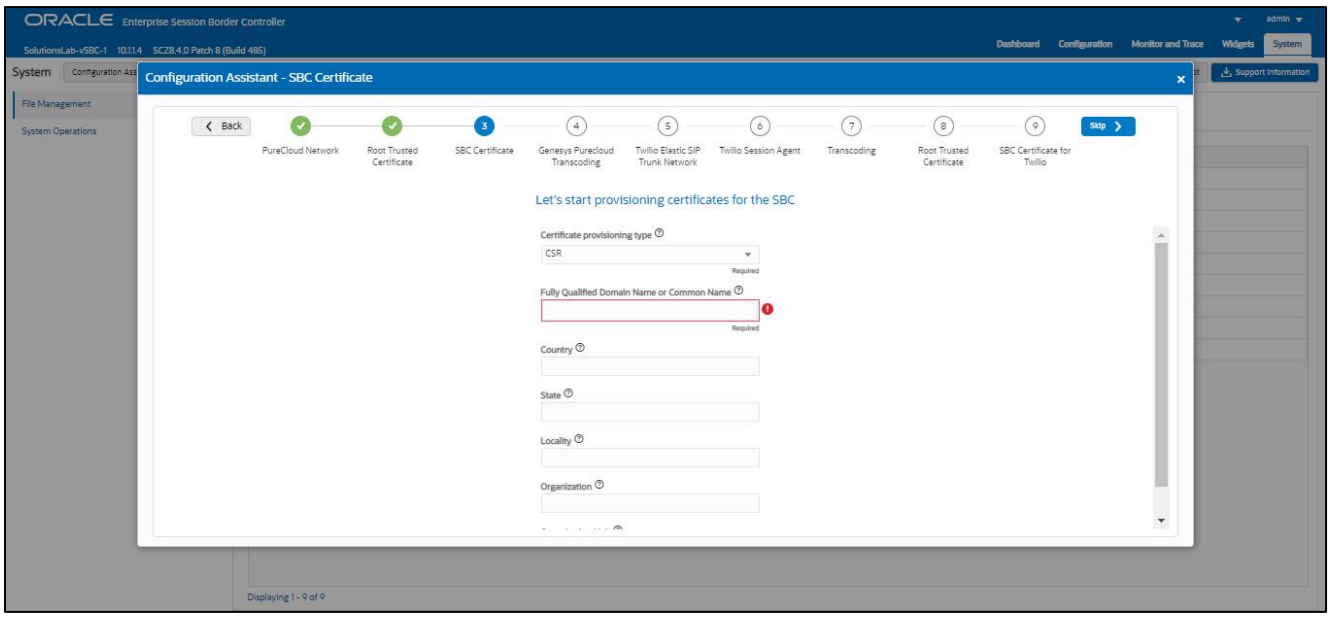
Page 3 - SBC Certificates for BYOC Cloud side

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 BYOC Cloud 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 BYOC 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).

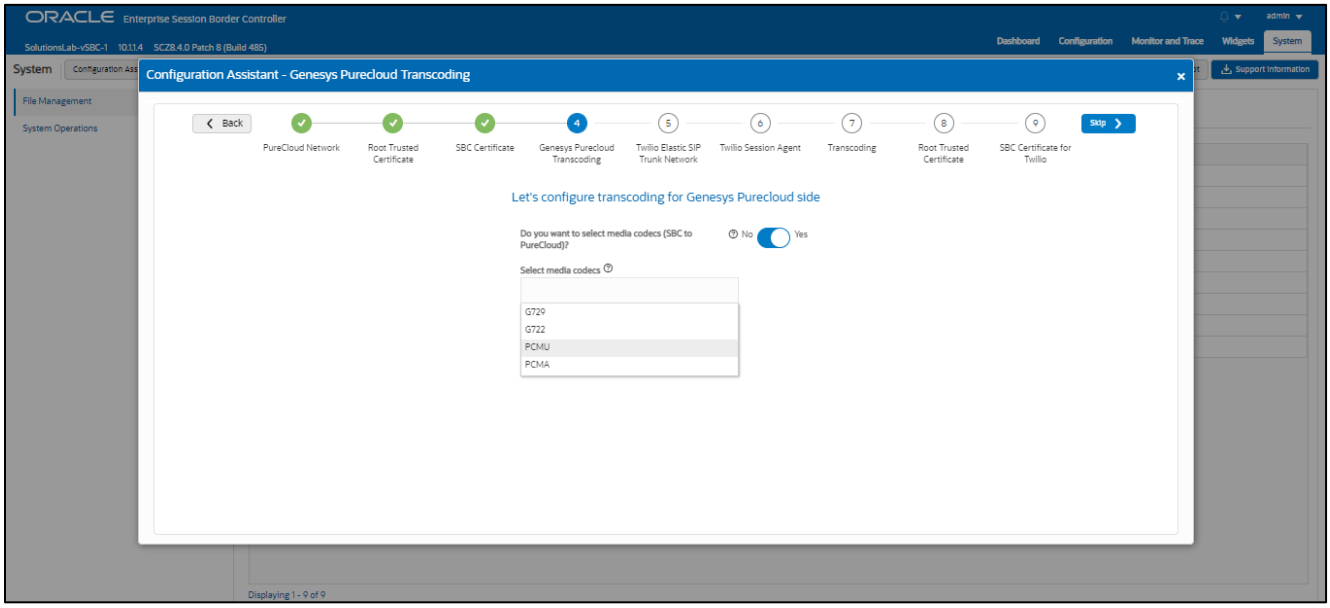


Page 4 – BYOC Cloud side Transcoding

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

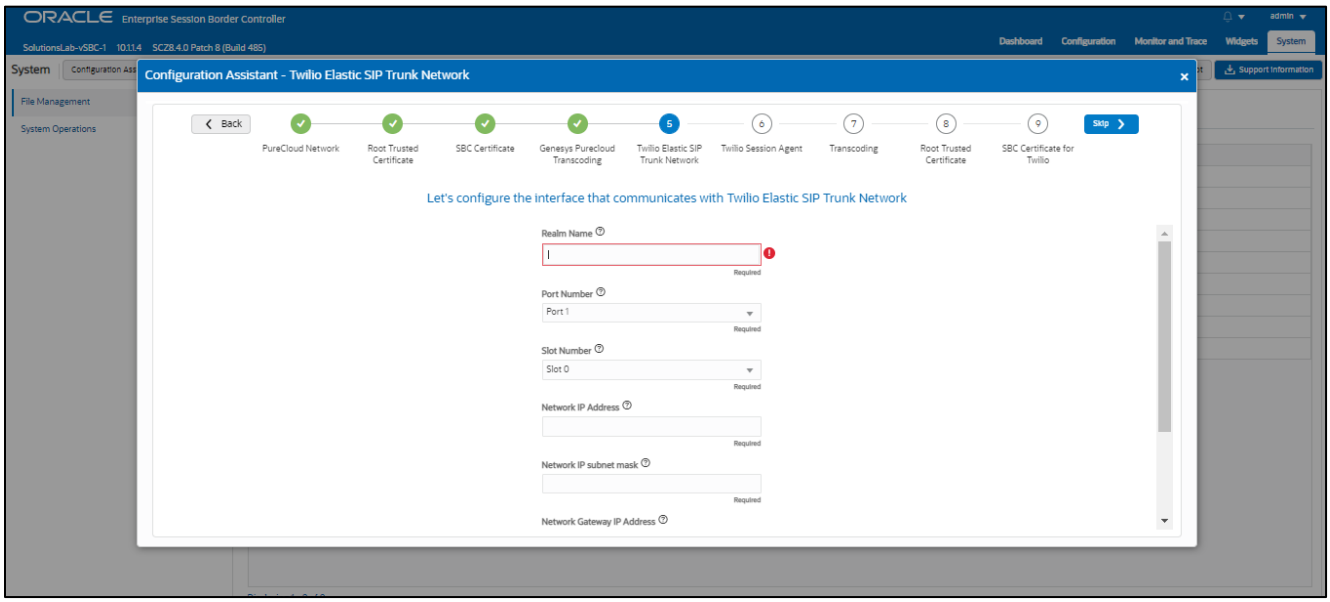
Once transcoding features is set to “yes”, you will then have an option to select additional media codecs you want included in offers/answers toward BYOC Cloud . If you select yes to either question regarding media codecs, you will be presented with a required drop down.

You can select as many codecs from the list presented.



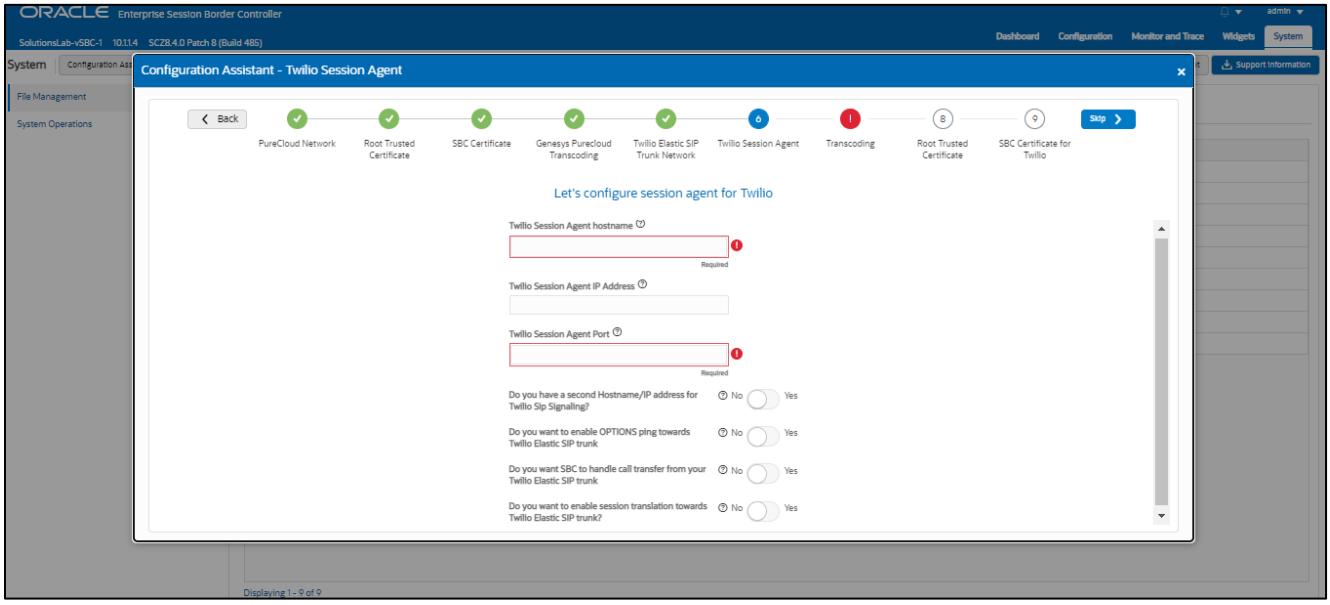
Page 5 – Twilio Elastic Sip Trunk Network

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



Page 6 – Twilio Session Agent

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

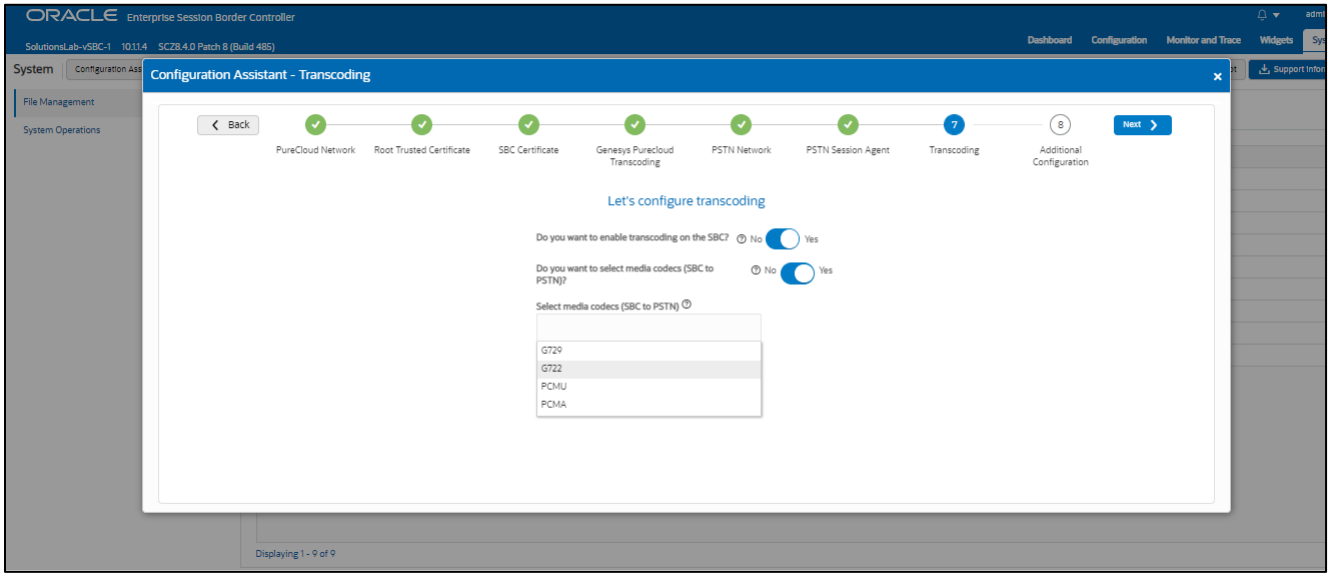


Please fill the required fields and click Next.

Page 7 - Twilio side Transcoding

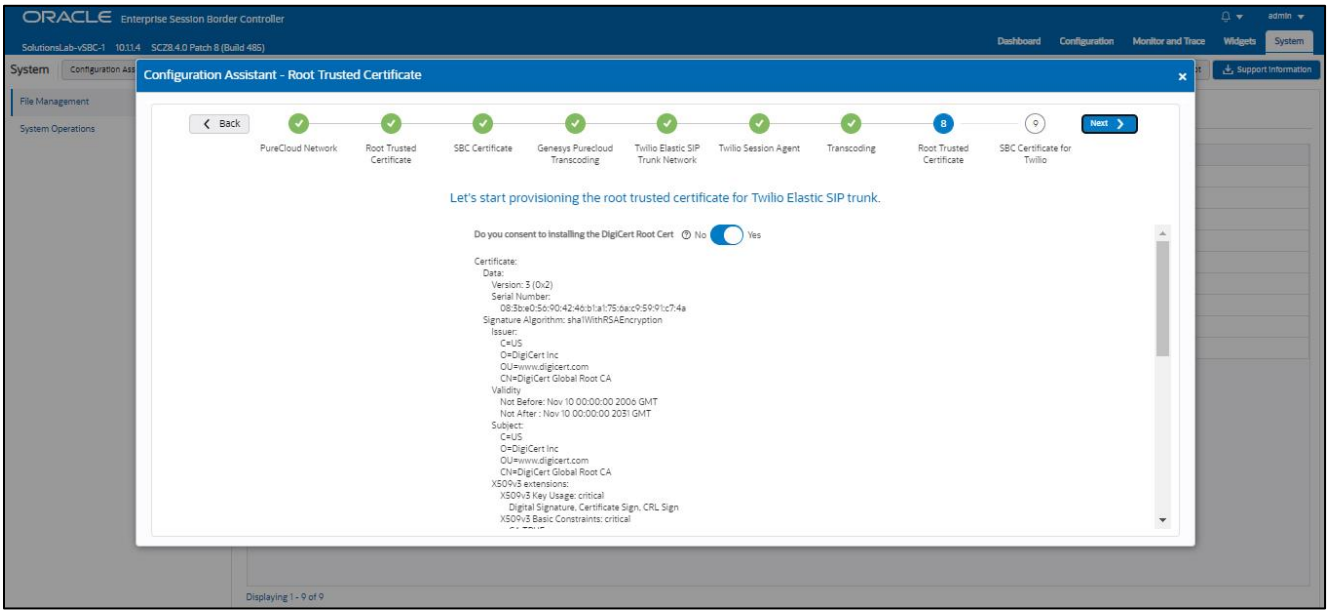
Page 7 is where you will be able to configure transcoding between the SBC and Twilio Trunk.

Once transcoding features is set to “yes”, you will then have an option to select additional media codecs you want included in offers/answers towards Twilio trunk. If you select yes to either question regarding media codecs, you will be presented with a required drop down. You can select as many codecs from the list presented.



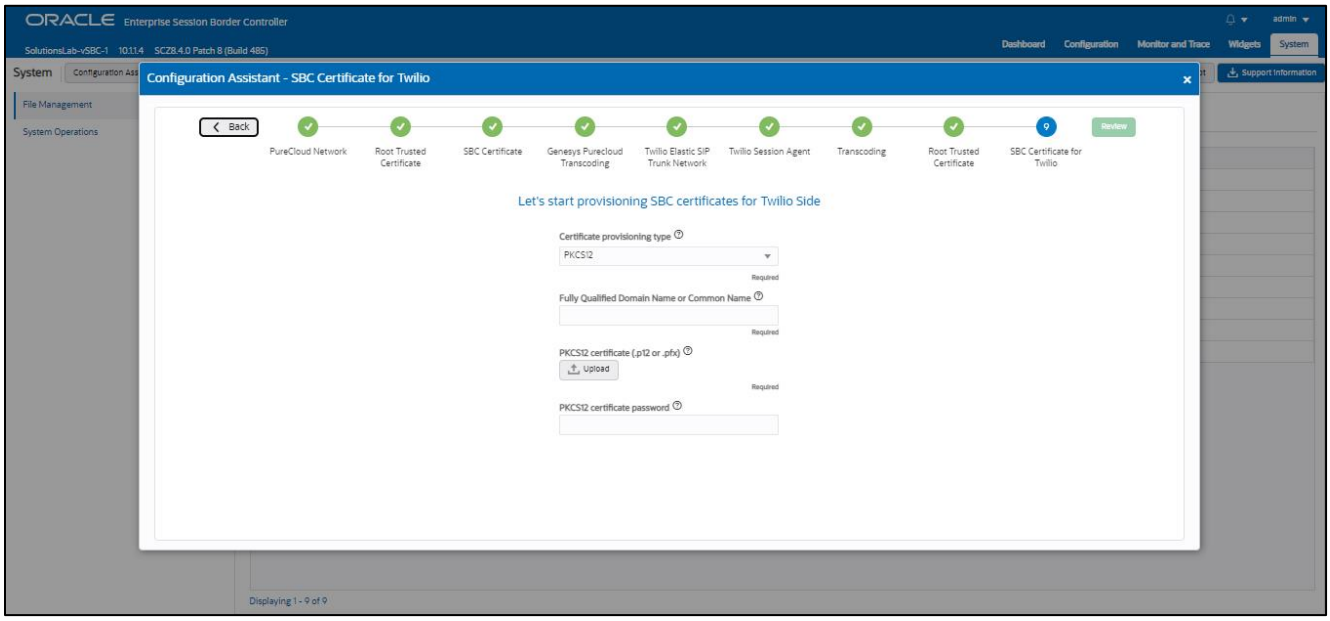
Page 8 – Import Digi Cert Root CA Certificate for Twilio Side

Page 8 of this template is where the SBC will import the DigiCert Root CA certificate, which Twilio uses to sign the certs it presents to the SBC during the TLS handshake. Importing the DigiCert Root CA certs is enabled by default.



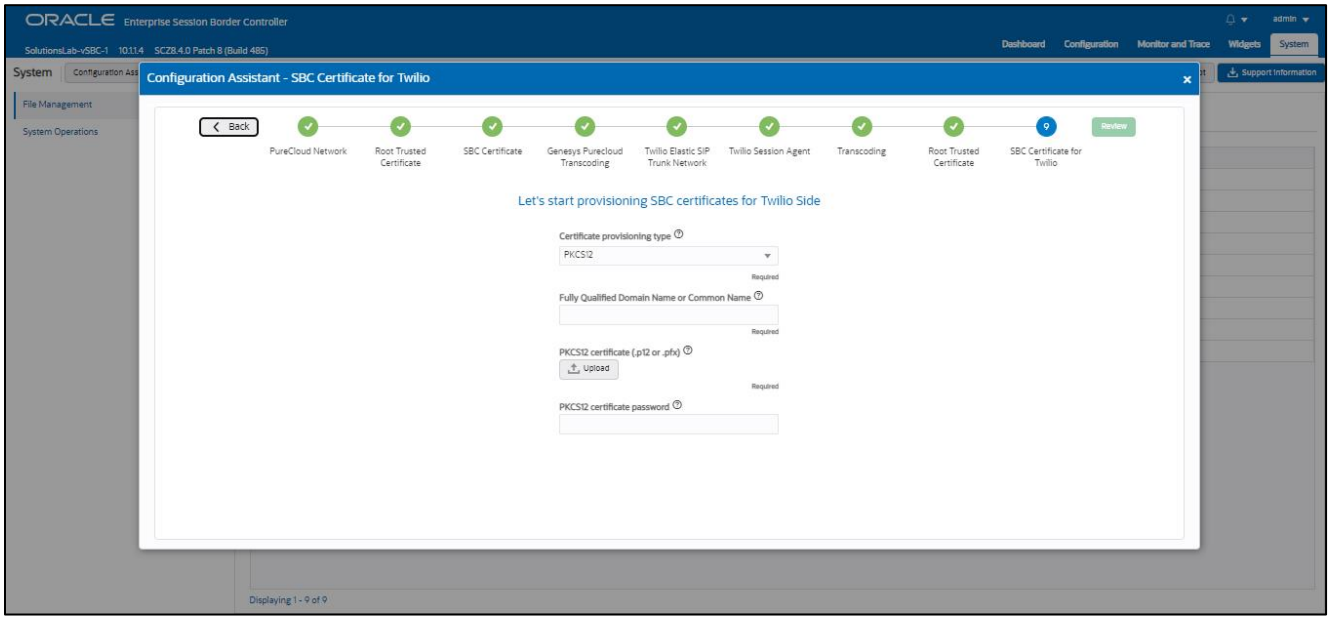
Page 9 – SBC Certificate for Twilio

Just like BYOC Cloud on Page 3,Page 9 of this template is where you provide the SBC Certificate for Twilio Side. You can either create a different SBC Certificate or reuse the SBC Certificate created for BYOC Cloud depending upon your specific requirement.



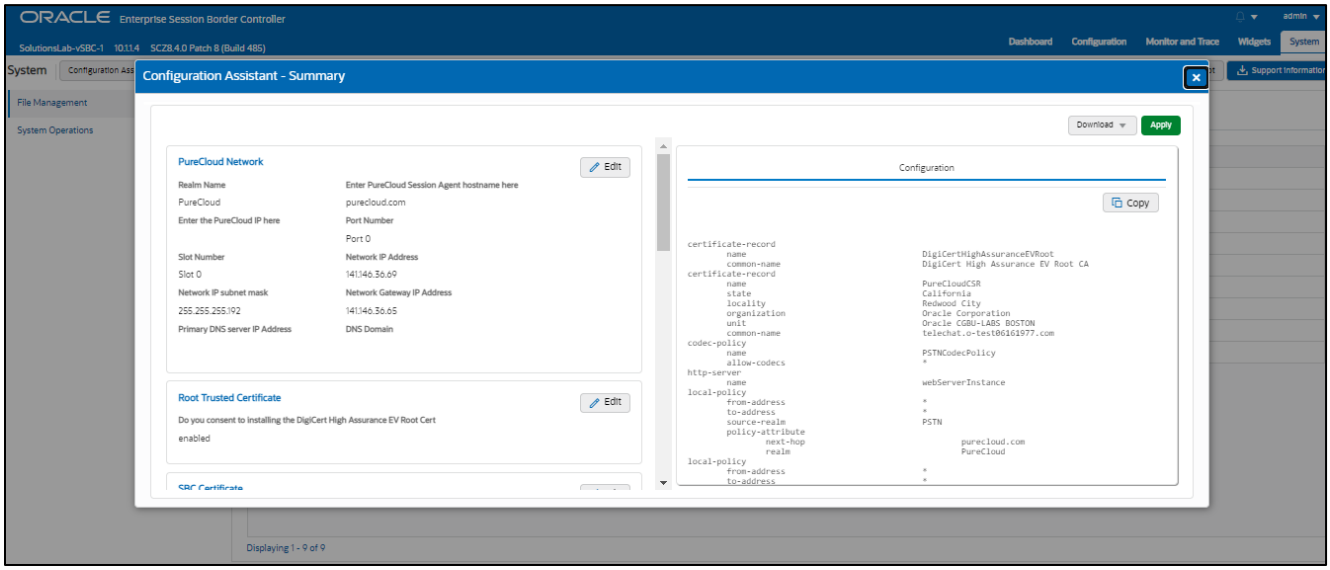
Review

At the end of the template, you will notice in the top right, a "*Review*" tab. If all 9 pages presented across the top are showing green, indicting there are no errors with the information entered, click on the "Review" tab.



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.

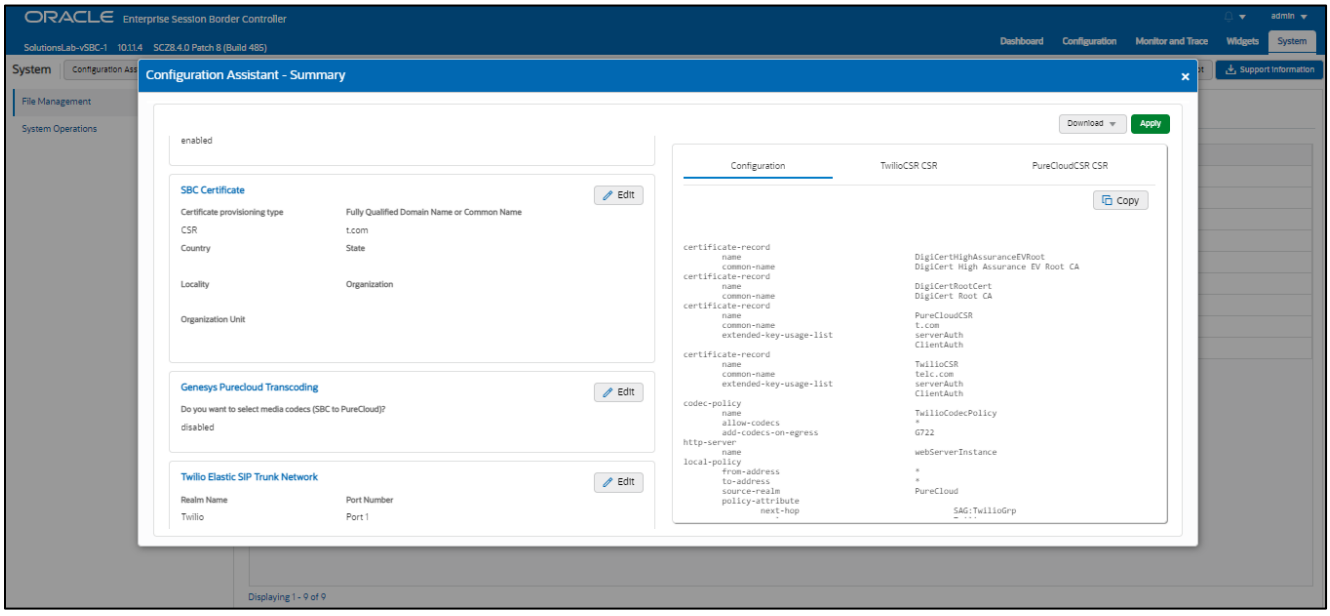
The right side displays the entire configuration created and when applicable, will also have a CSR tab that contains a certificate that can be signed by a CA authority.



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 and Page 9 of the template, if you chose CSR from the drop-down menu instead of PKCS, the SBC configures a certificate record and generates a certificate signing request for you.



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 Cloud Phone with Twilio 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