Oracle SBC integration with Genesys PureCloud BYOC and Verizon Business IP Trunking

Technical Application Note

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Version 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 Verizon Business IP Trunk	09 Sep 2021
1.1	Oracle Public IP Address masked	18 Nov 2021
1.2	New Section added- 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 how SIP Trunking is implemented.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Genesys PureCloud and Verizon Business IP Trunk.

It should be noted that the SBC configuration provided in this guide focuses strictly on the Genesys PureCloud and Verizon Business IP 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 Verizon Business IP Trunking

https://www.verizon.com/business/products/voice-collaboration/voip/ip-trunking/

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/\

2.3 Oracle SBC

- Oracle® Enterprise Session Border Controller ACLI Configuration Guide
- Oracle® Enterprise Session Border Controller Release Notes
- Oracle® Enterprise Session Border Controller Security Guide

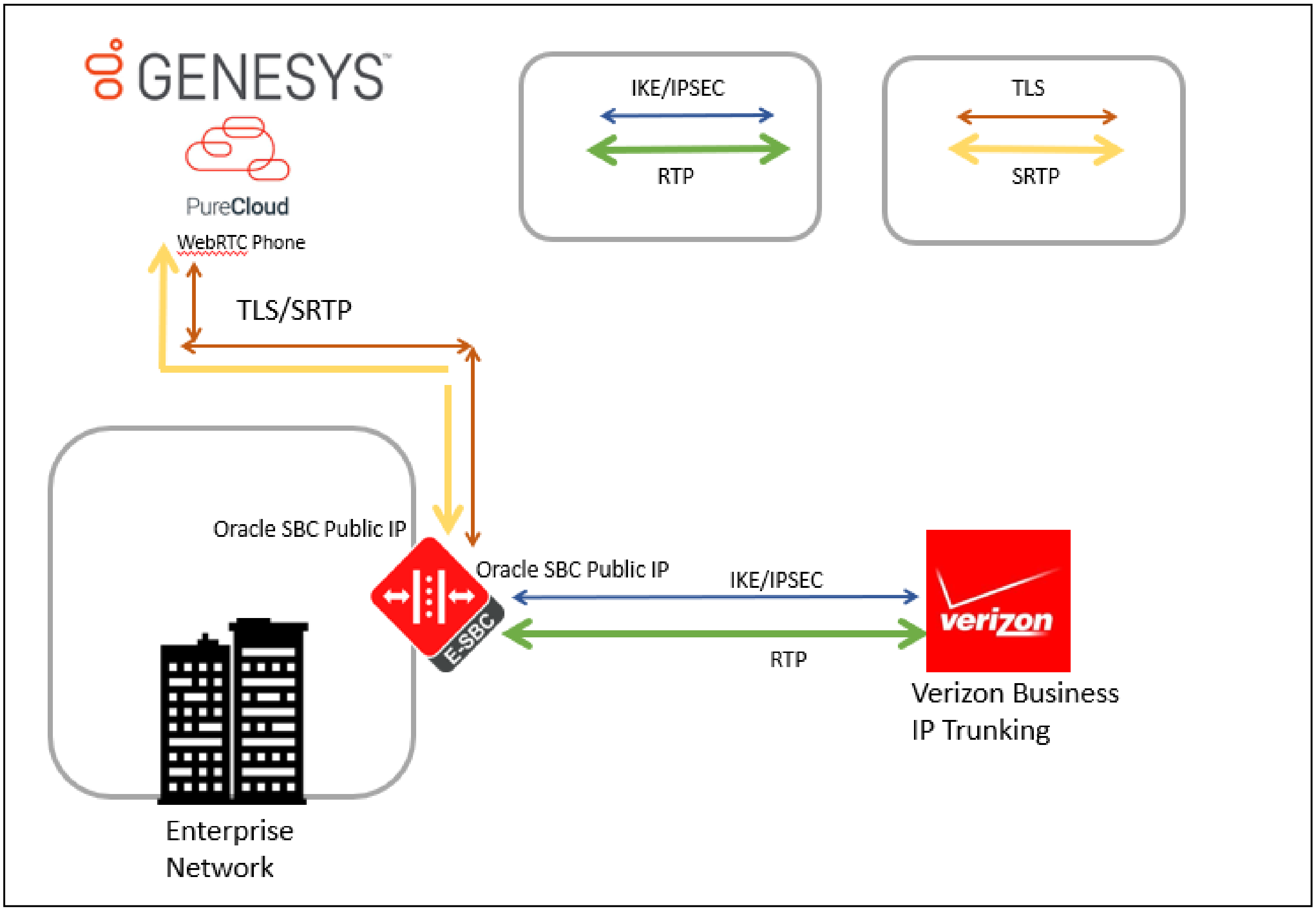
3. Validated Oracle Versions

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
- AP 3950
- AP 4900
- VME

4. Architecture.



Above figure illustrates the connection between Genesys PureCloud, Oracle SBC and Verizon Business IP Trunk. Both PureCloud and Verizon Trunk are connected to the Oracle SBC Public FQDN /IP. The connection between PureCloud and Oracle SBC is TLS/SRTP and between Verizon SIP Trunk and Oracle SBC is IPSEC/RTP. Oracle SBC is used to steer the signaling, media to, and From the PureCloud to Verizon SIP Trunk.

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

Phase 1 – Configuring Genesys PureCloud

Phase 2 – 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

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.

The Oracle Enterprise SBC will act as an intermediary between the Verizon Trunk and Genesys PureCloud. The SBC is configured to broker calls as a back-to-back user agent (B2BUA) between the two systems. The Verizon DIDs are assigned to users on PureCloud 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 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)

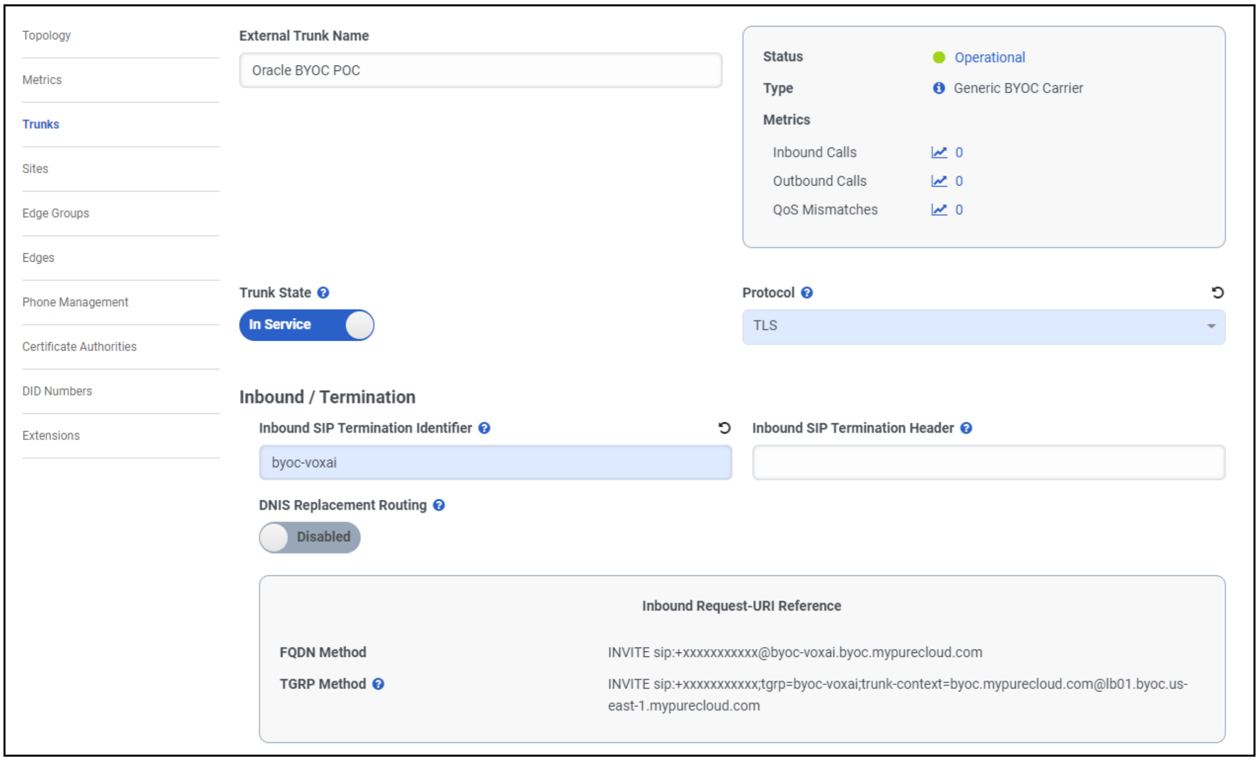
5.1.2 Set Inbound SIP Termination Identifier

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



External Trunk Name: Oracle BYOC POC

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

Trunk State: In Service

Protocol: TLS

Inbound / Termination

Inbound SIP Termination Identifier: byoc-voxai

Inbound SIP Termination Header:

DNIS Replacement Routing: Disabled

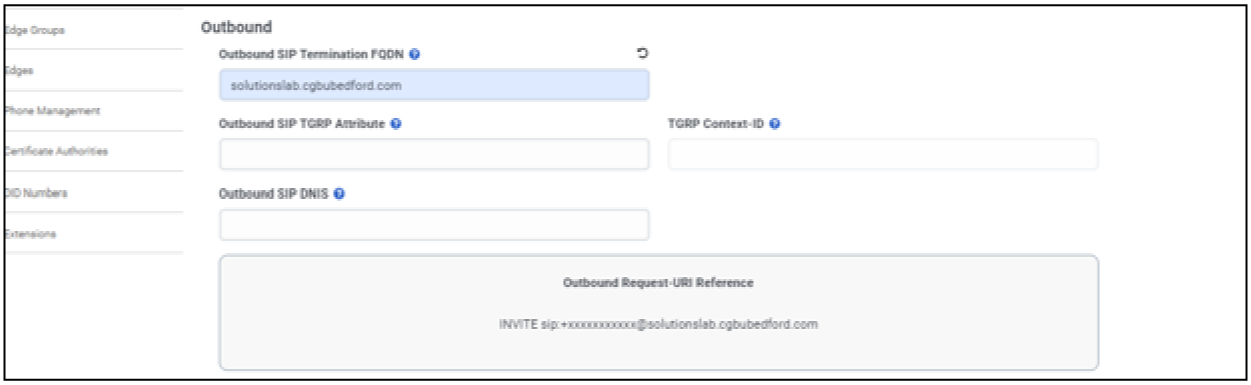
Inbound Request-URI Reference

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

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

5.1.3 Set Outbound SIP Servers or Proxies

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



Outbound

Outbound SIP Termination FQDN: solutionslab.cgbubedford.com

Outbound SIP TGRP Attribute:

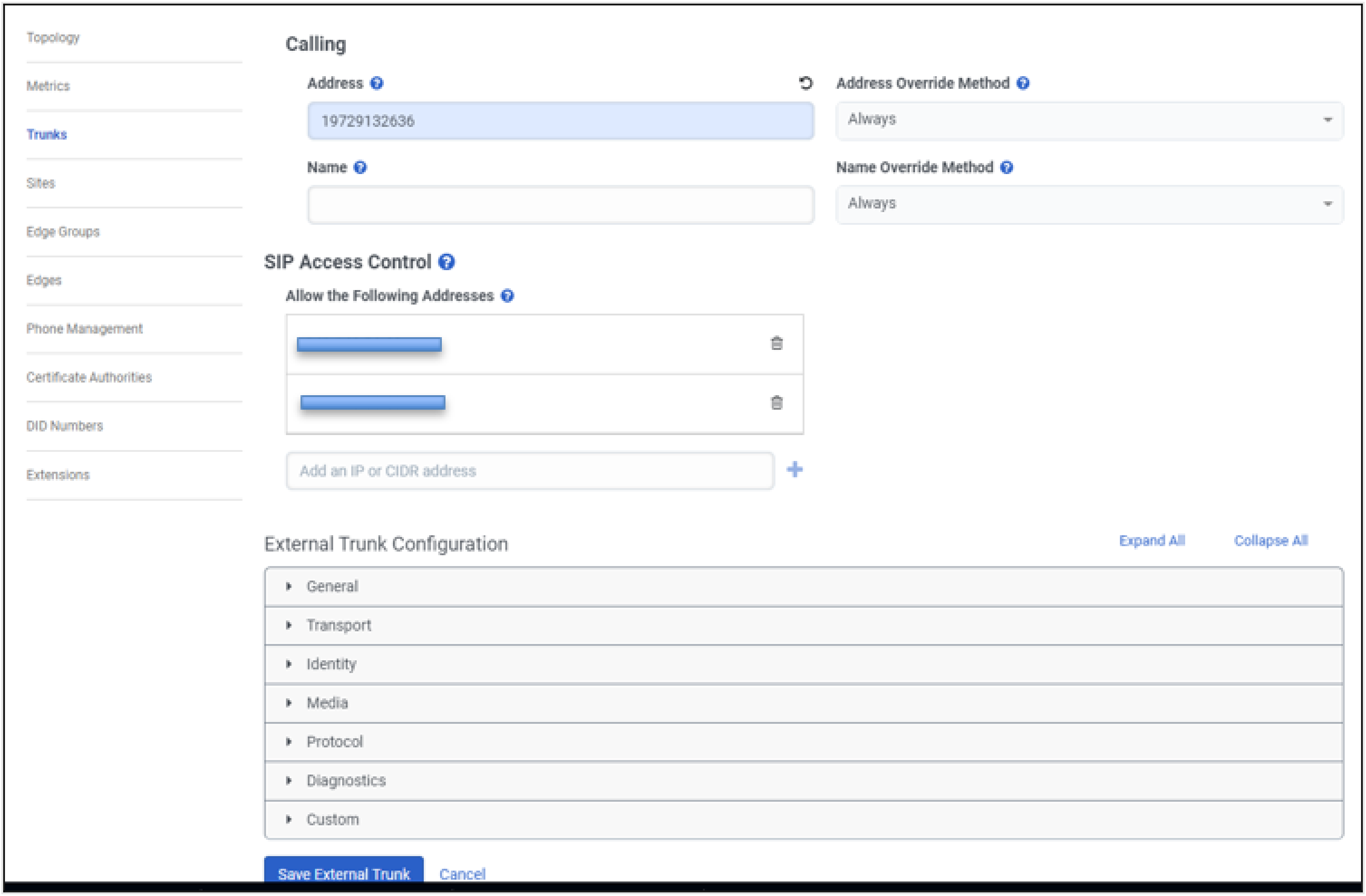
TGRP Context-ID:

Outbound SIP DNIS:

Outbound Request-URI Reference

INVITE sip:+xxxxxxxxxxx@solutionslab.cgbubedford.com

5.1.4 Set Calling Address



Calling

Address: 19729132636

Address Override Method: Always

Name:

Name Override Method: Always

SIP Access Control

Allow the Following Addresses

[redacted]

[redacted]

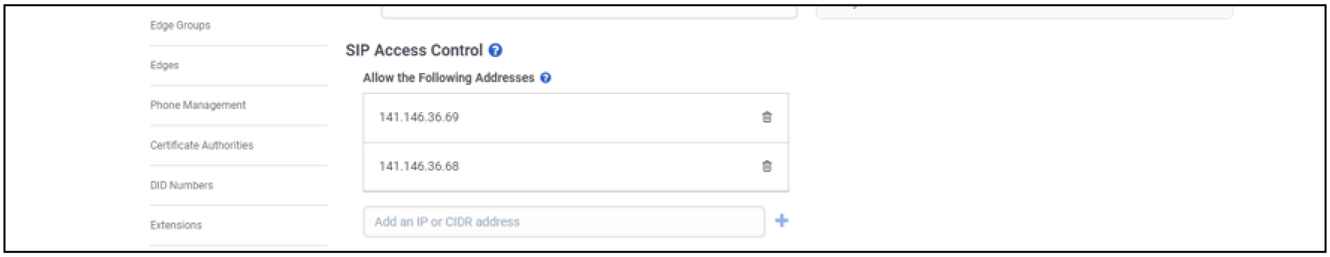
Add an IP or CIDR address

External Trunk Configuration

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

5.1.5 Set SIP Access Control

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



SIP Access Control

Allow the Following Addresses

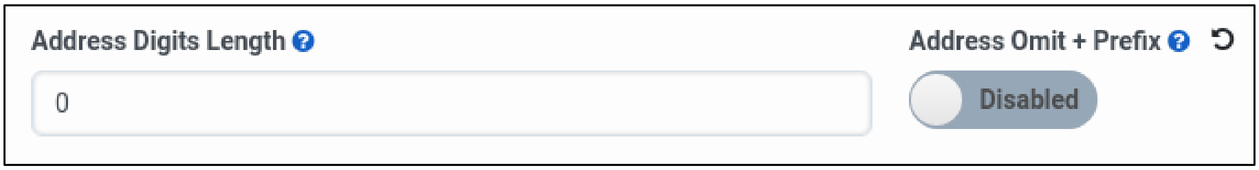
141.146.36.69

141.146.36.68

Add an IP or CIDR address

5.1.6 Enable E.164 format

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



Address Digits Length

0

Address Omit + Prefix

Disabled

5.2 Site Configuration.

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

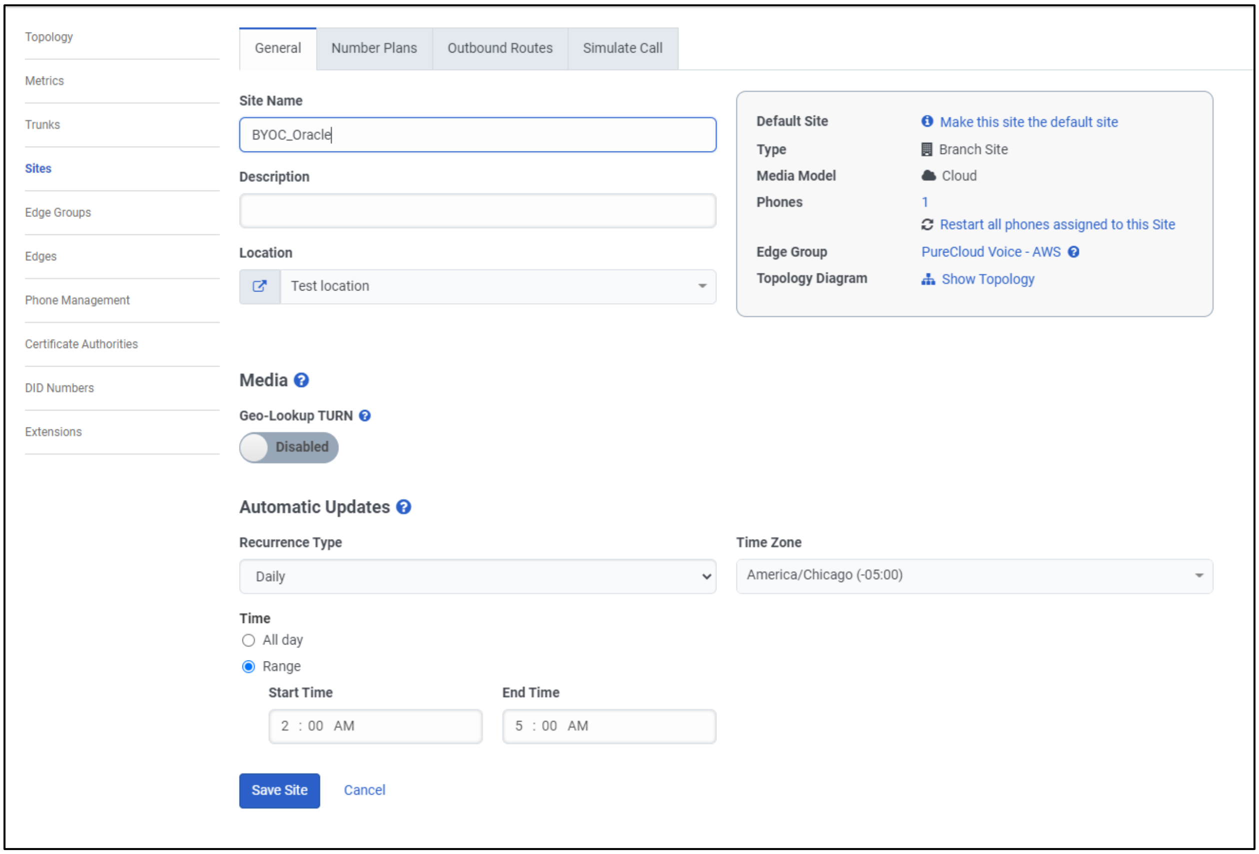
Type a name into the **Site Name** box.

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**.



Site Name: BYOC_Oracle

Description:

Location: Test location

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

Media

Geo-Lookup TURN: Disabled

Automatic Updates

Recurrence Type: Daily

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

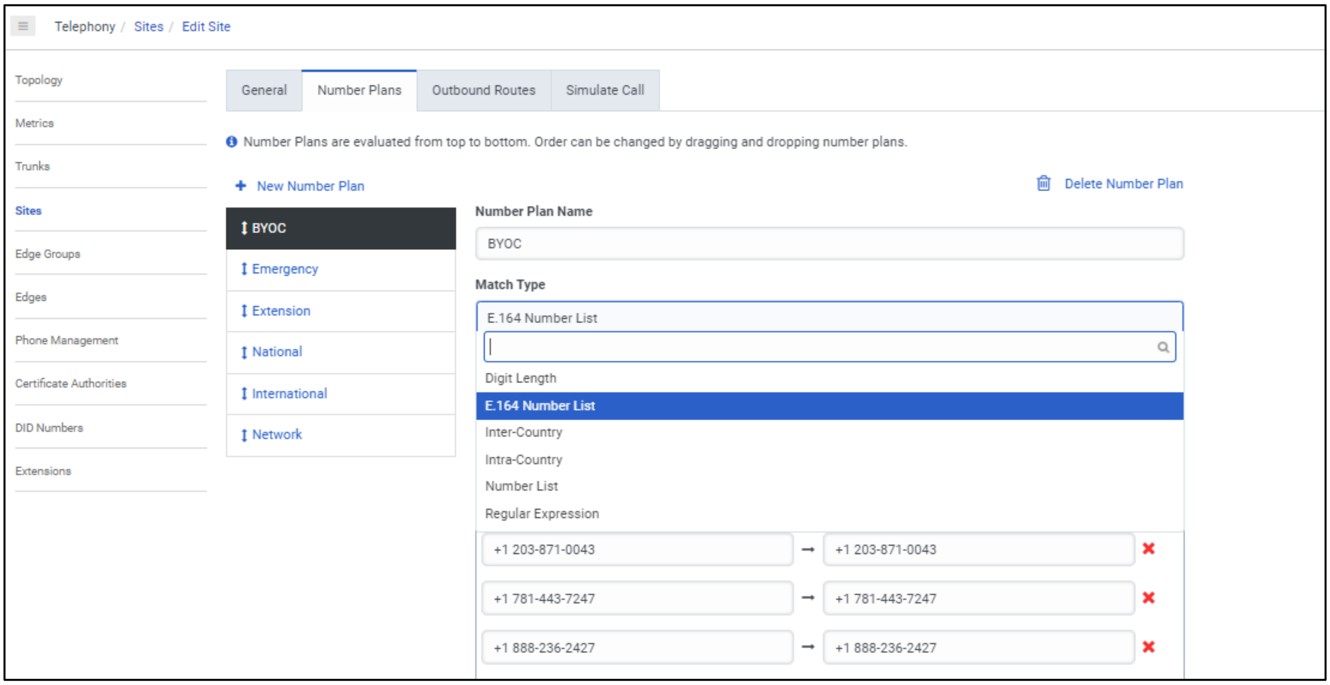
Time
○ All day
● Range

Start Time: 2 : 00 AM

End Time: 5 : 00 AM

5.2.2 Number Plans & Classifications

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



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

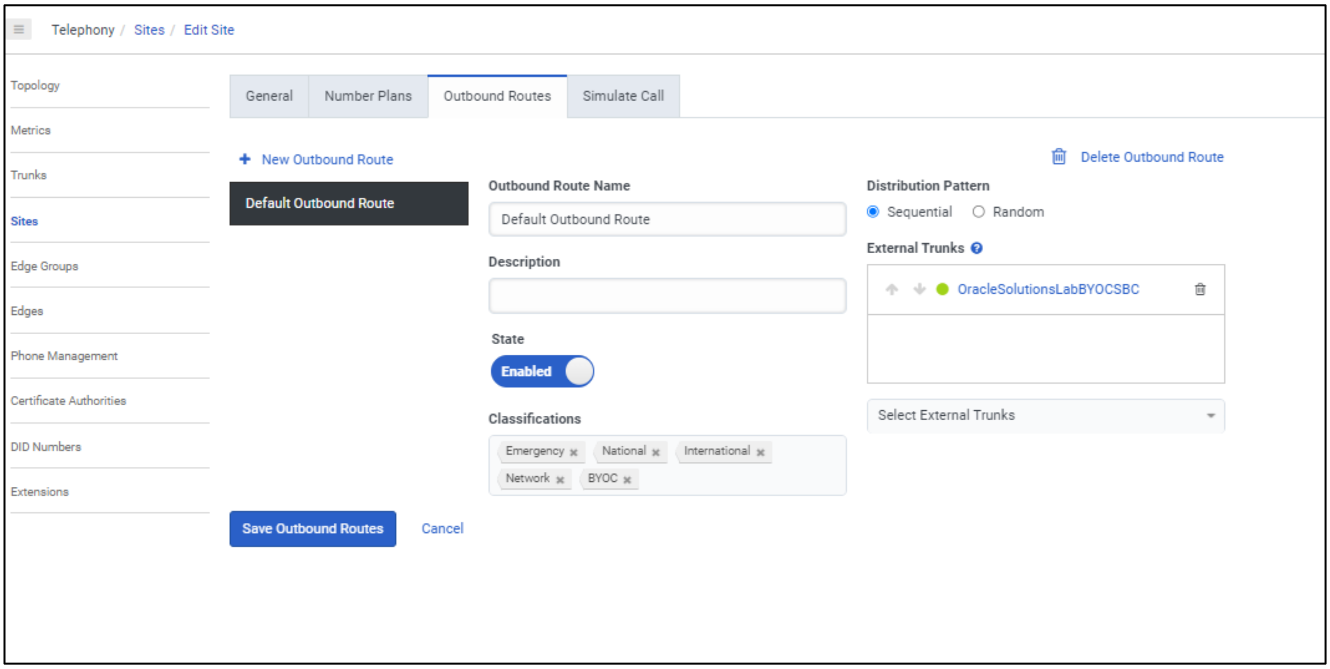
Number Plan Name: BYOC

Match Type: E.164 Number List

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

5.2.3 Configure outbound route

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



Outbound Route Name: Default Outbound Route

Description:

State: Enabled

Classifications: Emergency × National × International × Network × BYOC ×

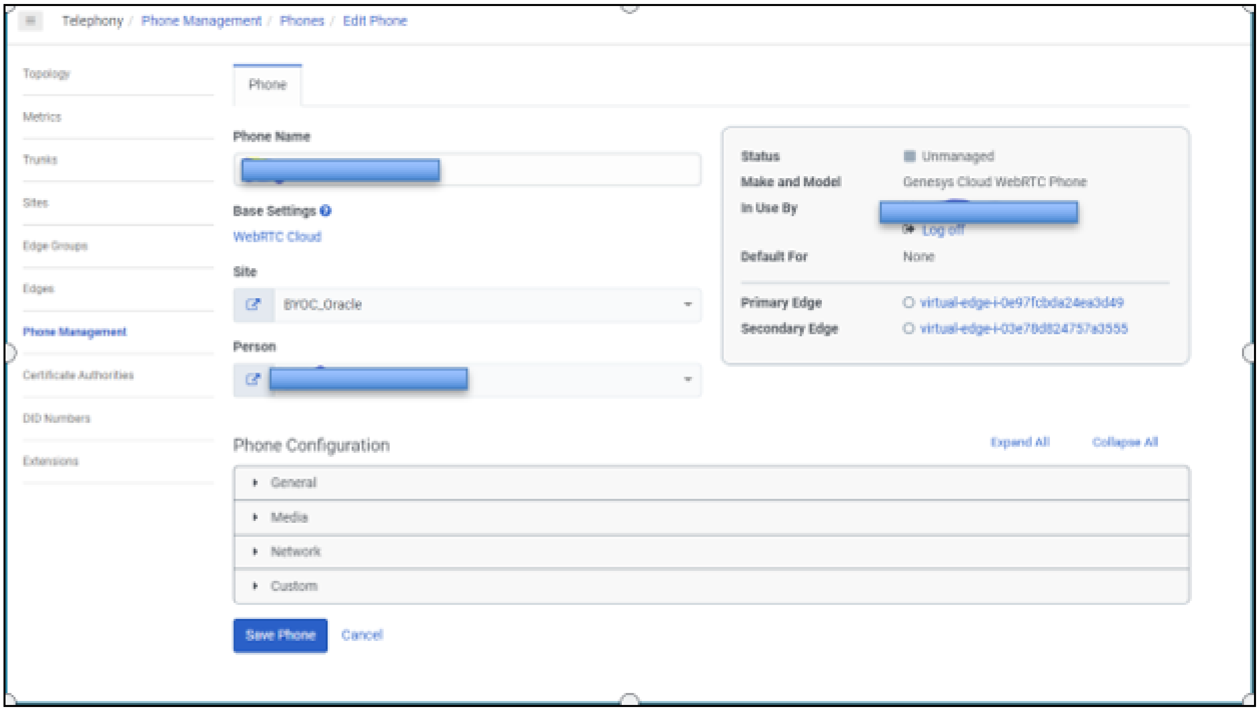
Distribution Pattern: ● Sequential ○ Random

External Trunks: ● OracleSolutionsLabBYOCSBC

Select External Trunks

5.2.4 Phone configuration

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



Phone Name: [redacted]

Base Settings: WebRTC Cloud

Site: BYOC_Oracle

Person: [redacted]

Status: Unmanaged

Make and Model: Genesys Cloud WebRTC Phone

In Use By: [redacted]
Log off

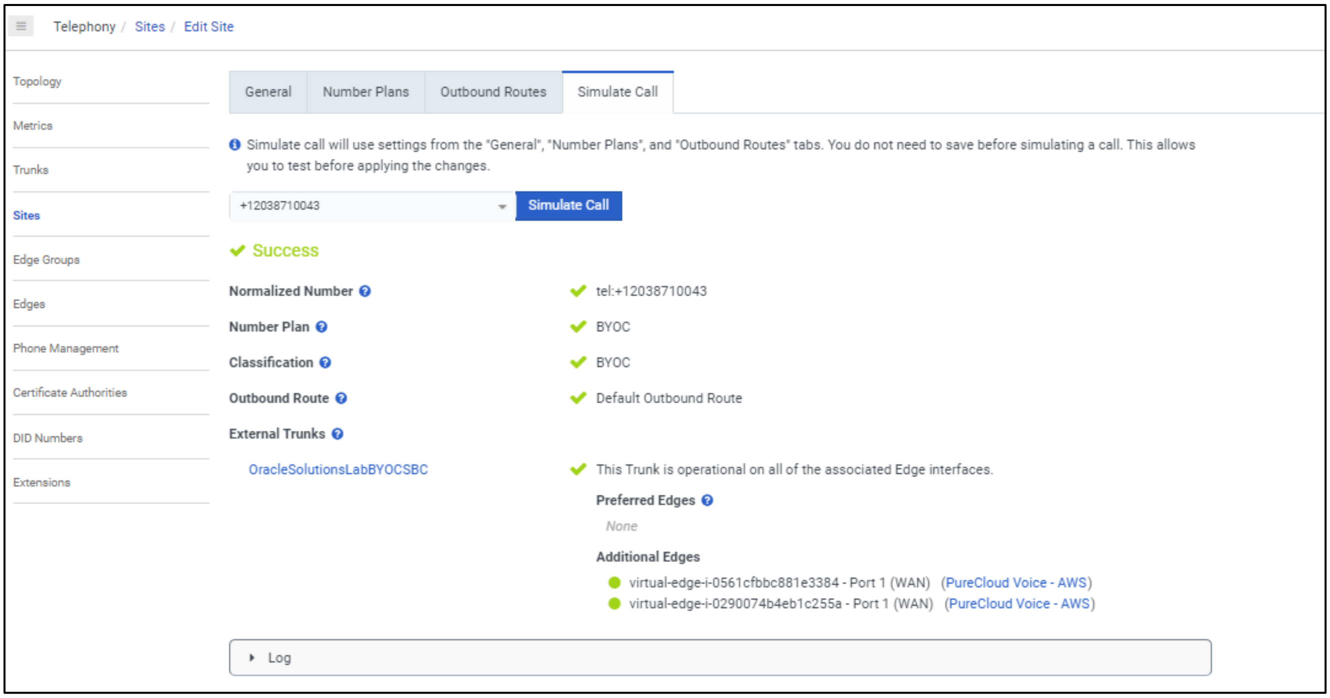
Default For: None

Primary Edge: ○ virtual-edge-i-0e97fcbda24ea3d49

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

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.



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

+12038710043 Simulate Call

✓ Success

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

Preferred Edges

None

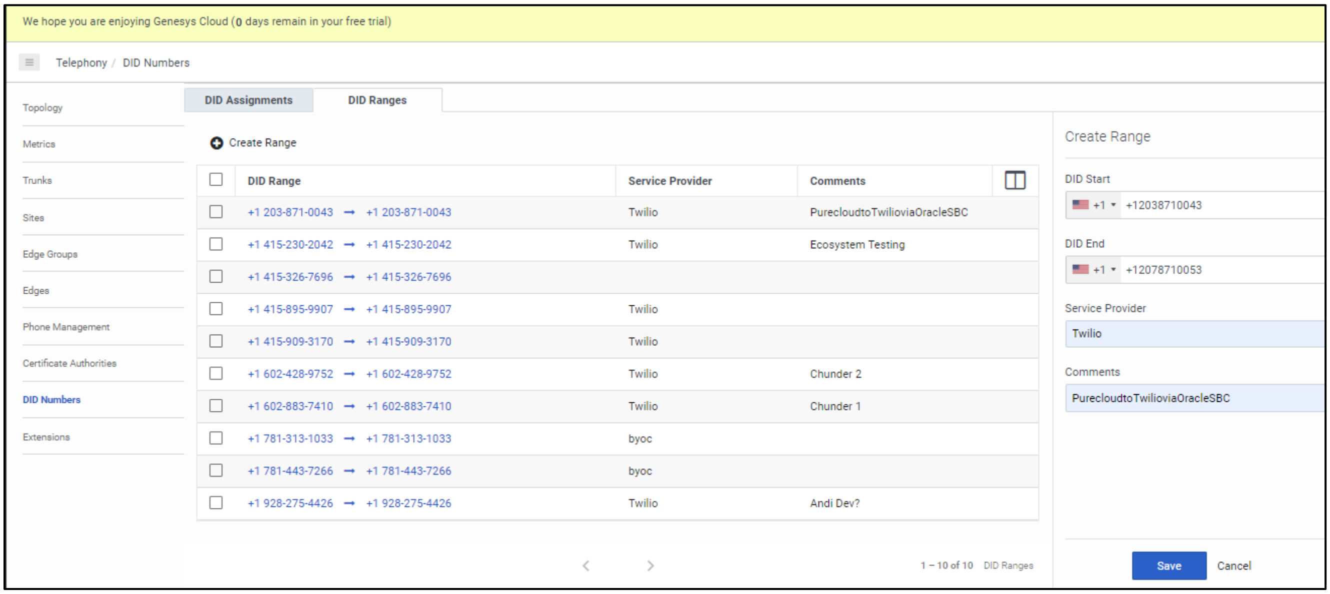
Additional Edges

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

5.3 DID Assignment

5.3.1 Create DID Range

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



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

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

1 – 10 of 10 DID Ranges

Create Range

DID Start: +1 +12038710043

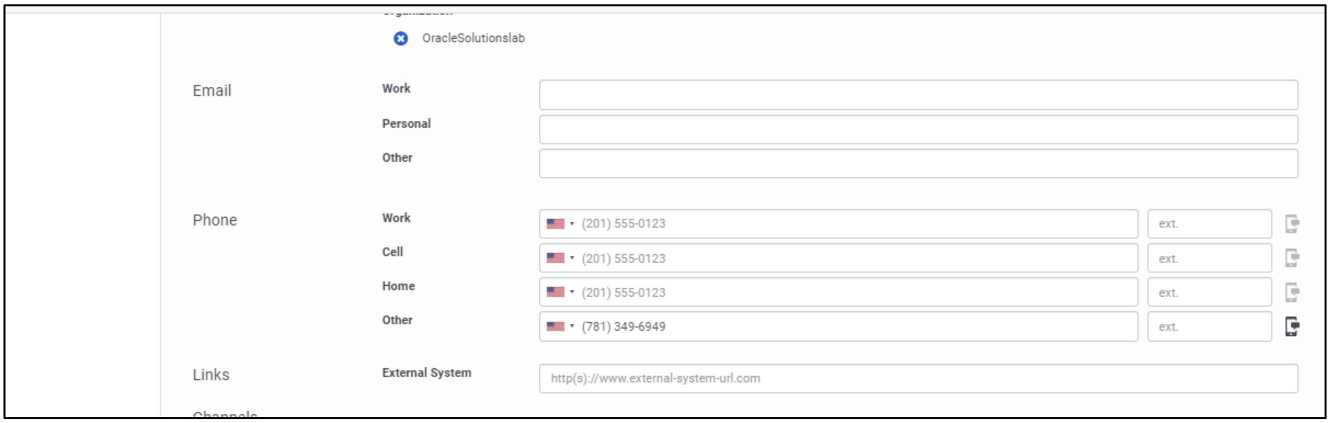
DID End: +1 +12078710053

Service Provider: Twilio

Comments: PurecloudtoTwilioviaOracleSBC

5.3.2 Assign DID to User

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

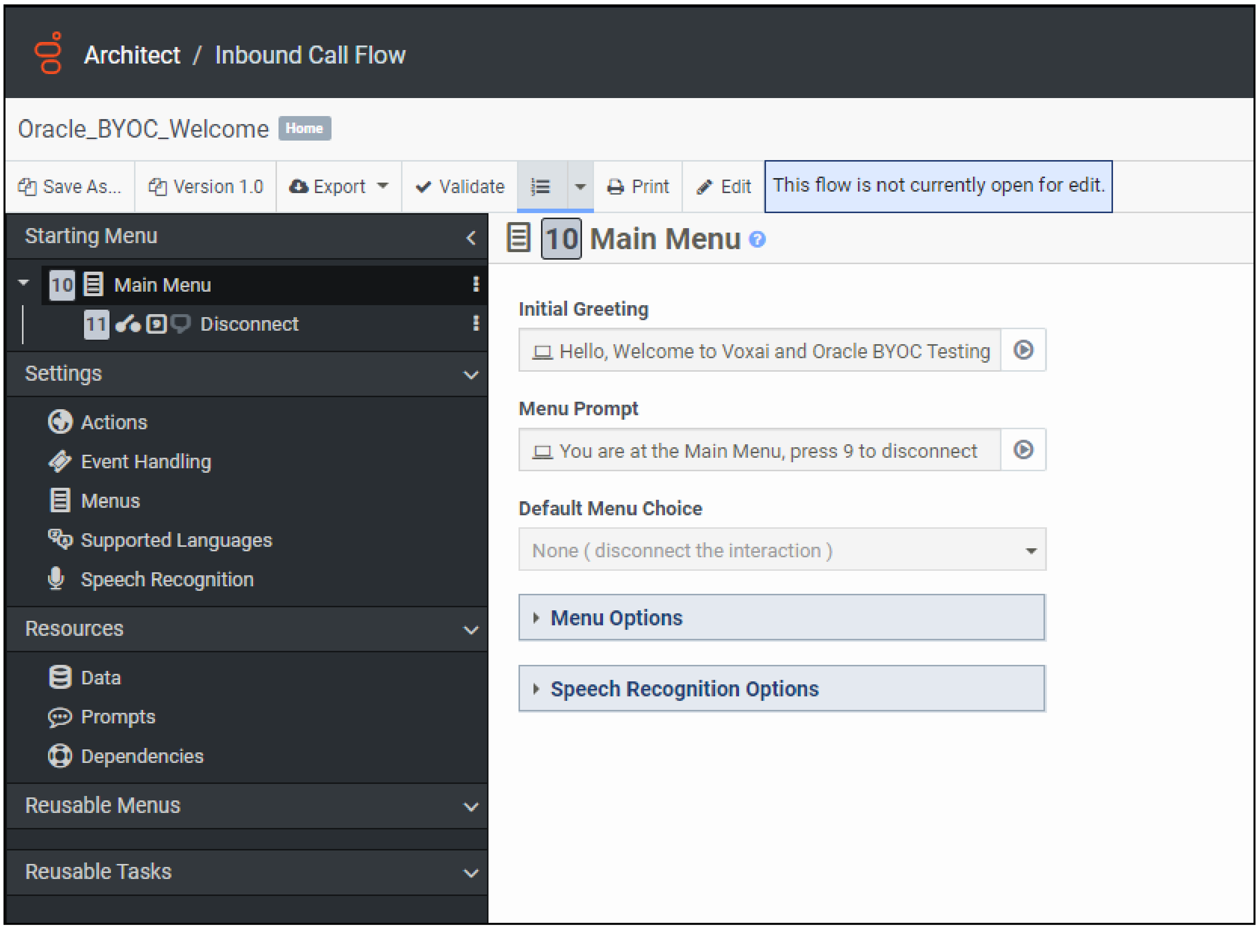

OracleSolutionslab

Email

Email	Work		
	Personal		
	Other		
Phone	Work	(201) 555-0123	ext.
	Cell	(201) 555-0123	ext.
	Home	(201) 555-0123	ext.
	Other	(781) 349-6949	ext.
Links	External System	http(s)://www.external-system-url.com	

5.4. Architect flow for inbound welcome prompt

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



This flow is not currently open for edit.

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

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

Default Menu Choice: None (disconnect the interaction)

6. Configuring the SBC

This chapter provides systematic guidance on how to configure Oracle SBC for Genesys PureCloud and Verizon IP Trunk.

6.1 New SBC configuration

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

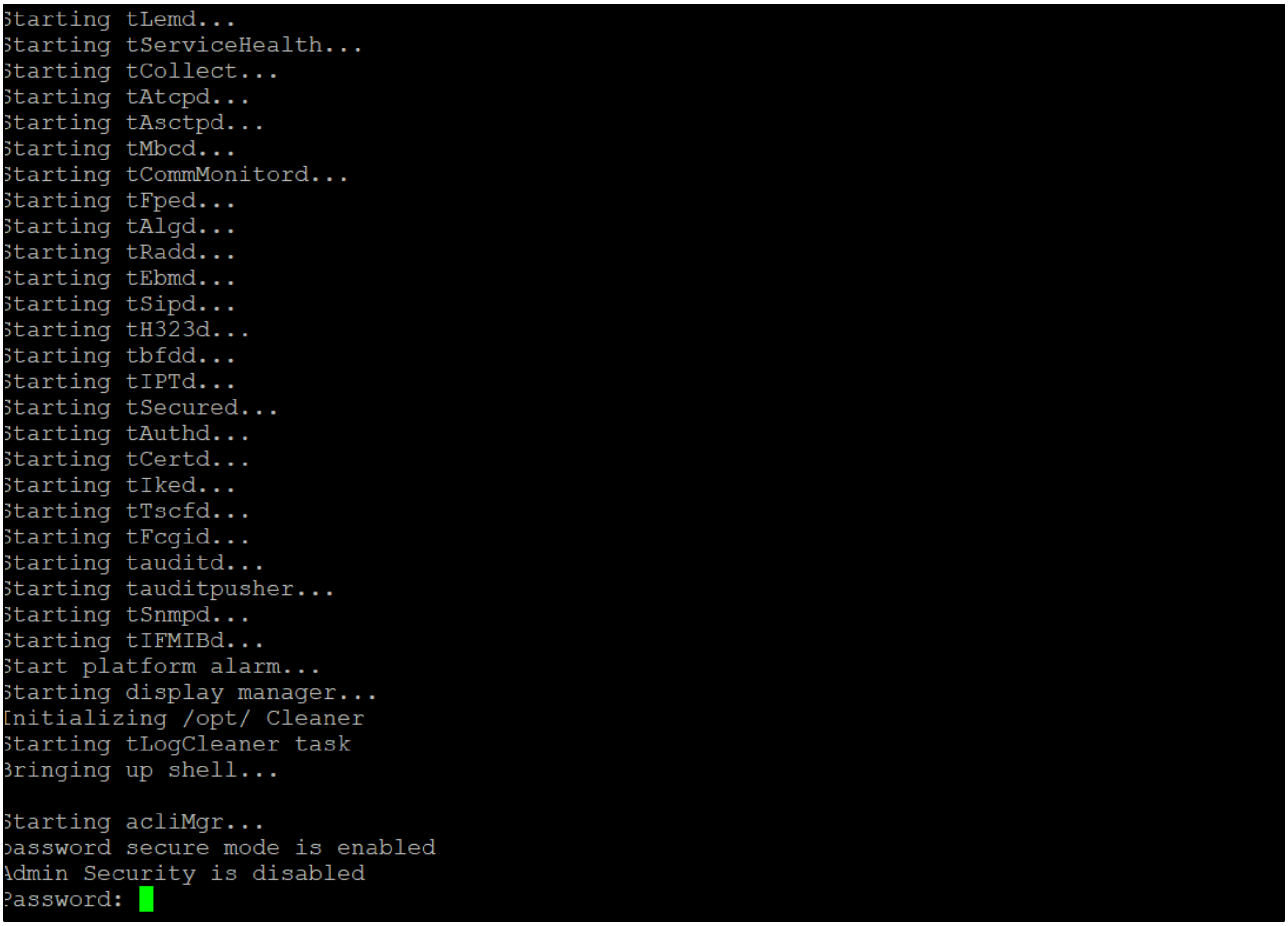
6.1.1 Establishing a serial connection to the SBC

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

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

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

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

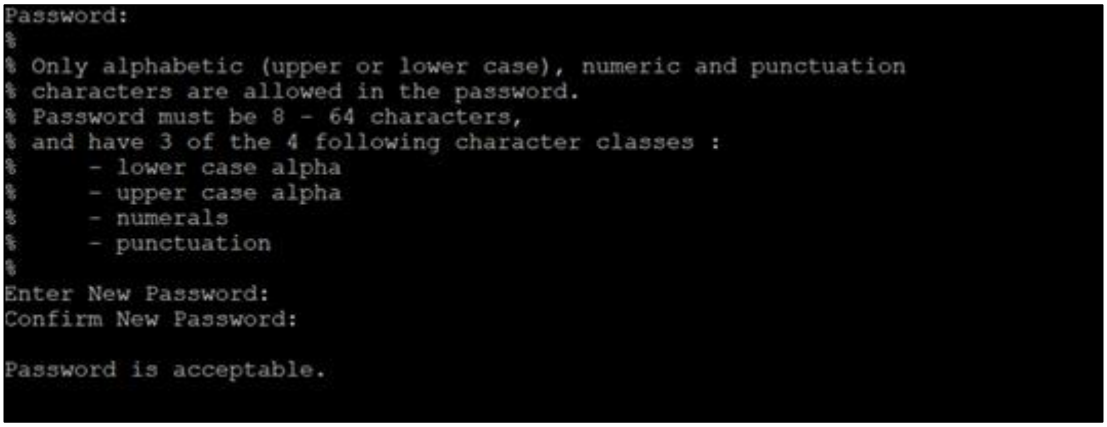


```
Starting tLemd...
Starting tServiceHealth...
Starting tCollect...
Starting tAtcpd...
Starting tAsctpd...
Starting tMbcd...
Starting tCommMonitord...
Starting tFped...
Starting tAlgd...
Starting tRadd...
Starting tEbmd...
Starting tSipd...
Starting tH323d...
Starting tbfdd...
Starting tIPTd...
Starting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

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

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

Follow the appropriate documentation or contact your Oracle representative for details about how to configure the Cloud SBC platforms.

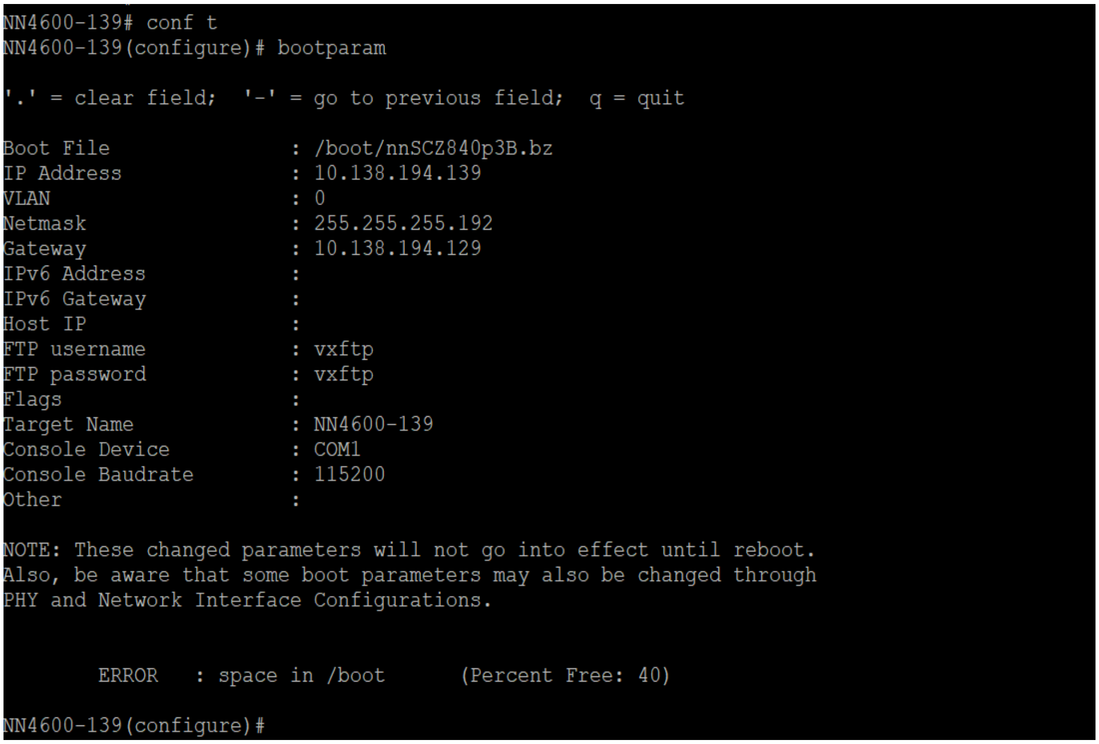
Both passwords must be changed according to the rules shown below.



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

Password is acceptable.
```

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

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

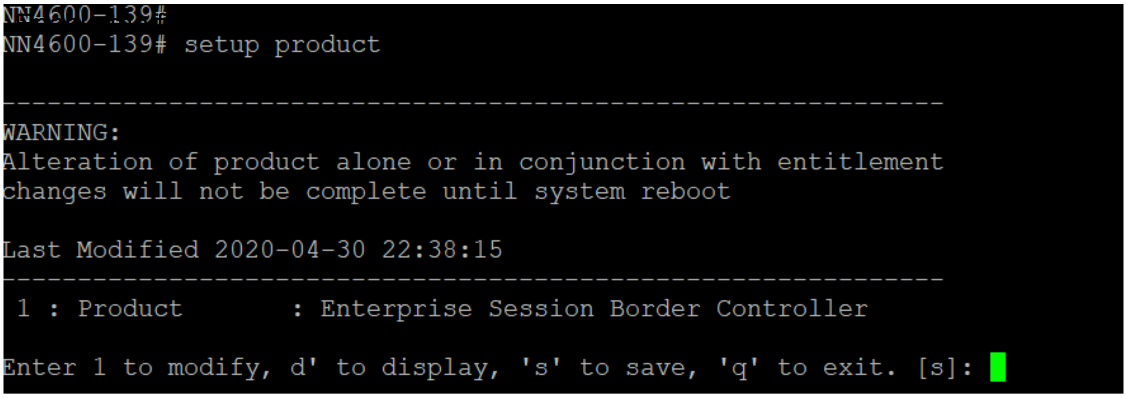


```
NN4600-139# conf t
NN4600-139(configure)# bootparam

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

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

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


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

NN4600-139(configure)#
```

Note: There is no management IP configured by default.

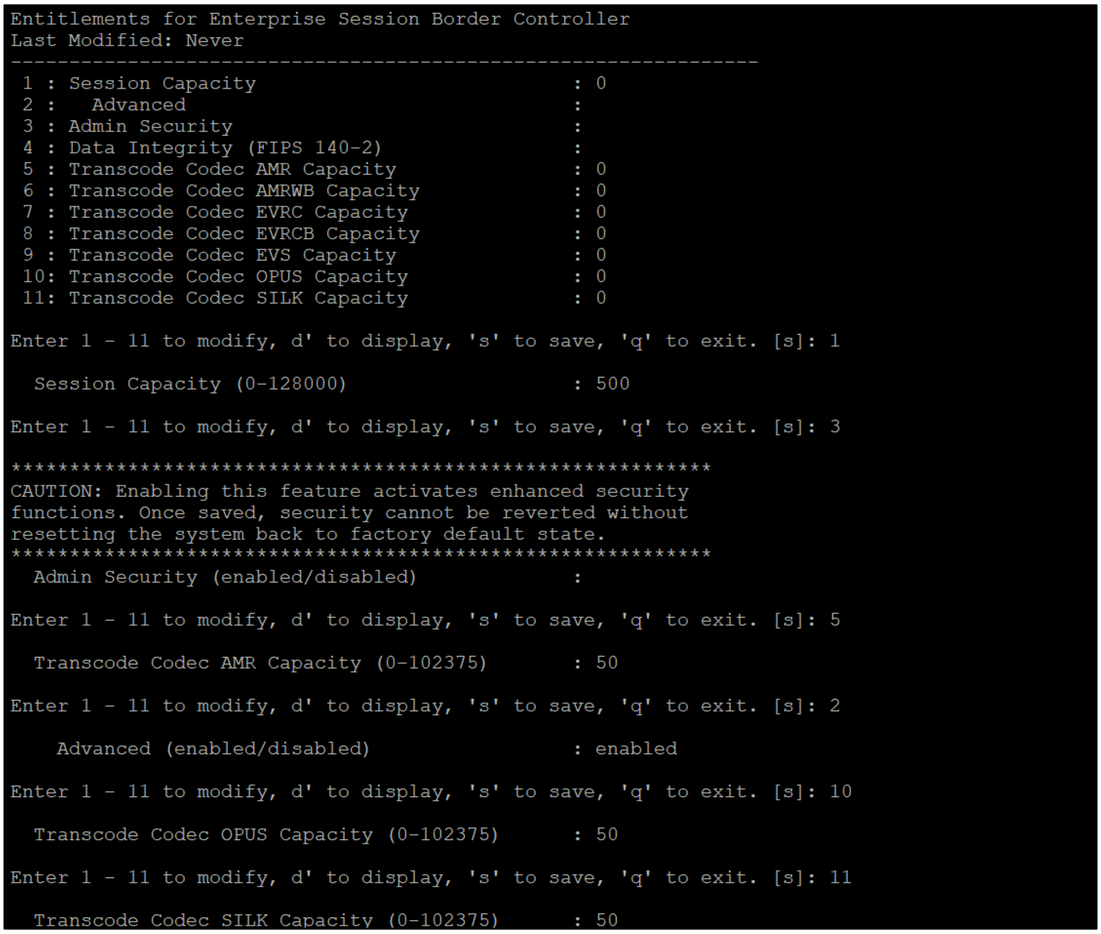
Setup product type to Enterprise Session Border Controller as shown below.

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



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

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

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

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

Save the changes and reboot the SBC.

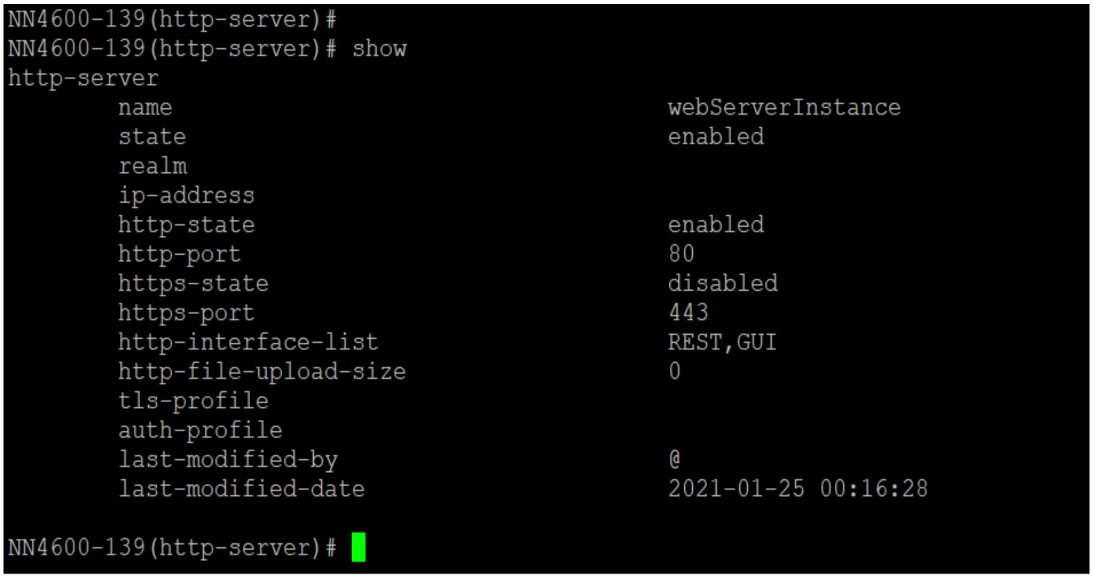


```
Entitlements for Enterprise Session Border Controller
Last Modified: Never
----------------------------------------------------------------
 1 : Session Capacity                          : 0
 2 :   Advanced                                :
 3 : Admin Security                            :
 4 : Data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

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

  Session Capacity (0-128000)                  : 500

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

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

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

  Transcode Codec AMR Capacity (0-102375)      : 50

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

    Advanced (enabled/disabled)                : enabled

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

  Transcode Codec OPUS Capacity (0-102375)     : 50

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

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

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

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

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

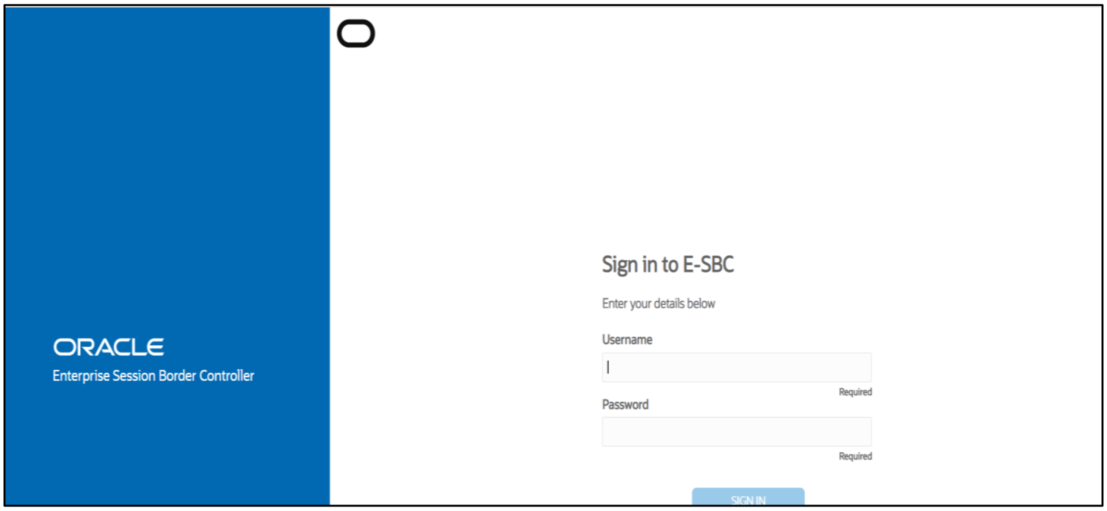


```
NN4600-139(http-server)#
NN4600-139(http-server)# show
http-server
        name                                    webServerInstance
        state                                   enabled
        realm
        ip-address
        http-state                              enabled
        http-port 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

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

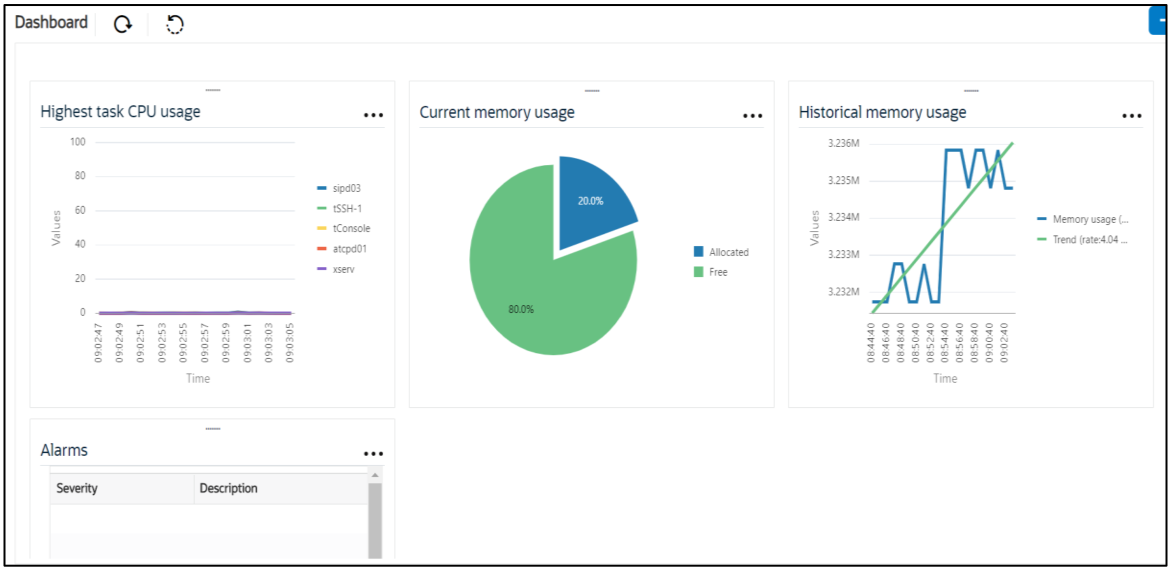
6.1.2 Configure SBC using Web GUI

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

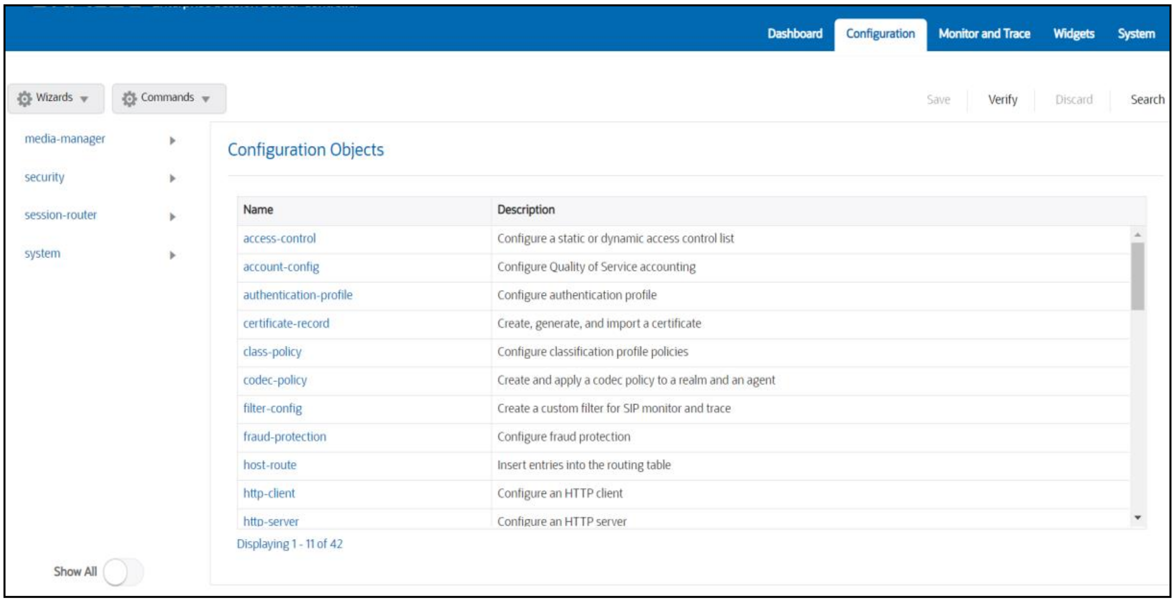
The Web GUI can be accessed through the URL http://<SBC_MGMT_IP>.



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



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



Configuration Objects

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

Displaying 1 - 11 of 42

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

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

The expert mode is used for configuration.

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

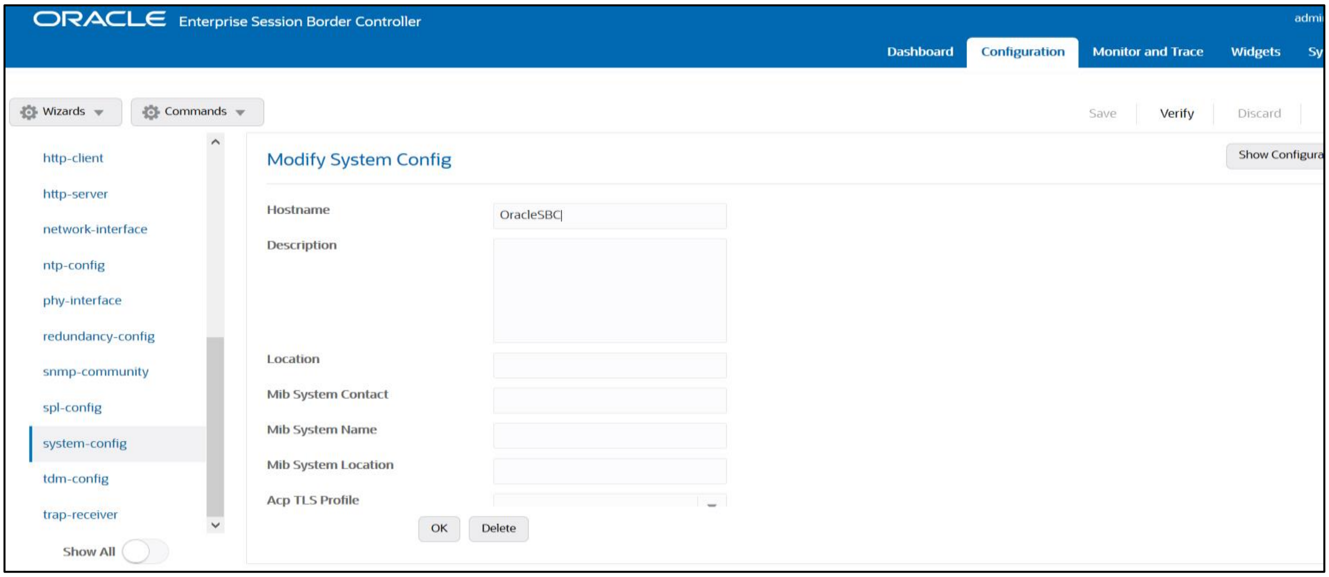
6.2. Configure system-config

To configure system level functionality for the OCSBC, you must first enable the system-config

Navigate to system->system-config
ACLI Path: config t->system->system-config

Note: The following parameters are optional but recommended for system config

- Hostname
- Description
- Location
- Default Gateway (recommended to be the same as management interface gateway)



Modify System Config

Hostname: OracleSBC|

Description:

Location:

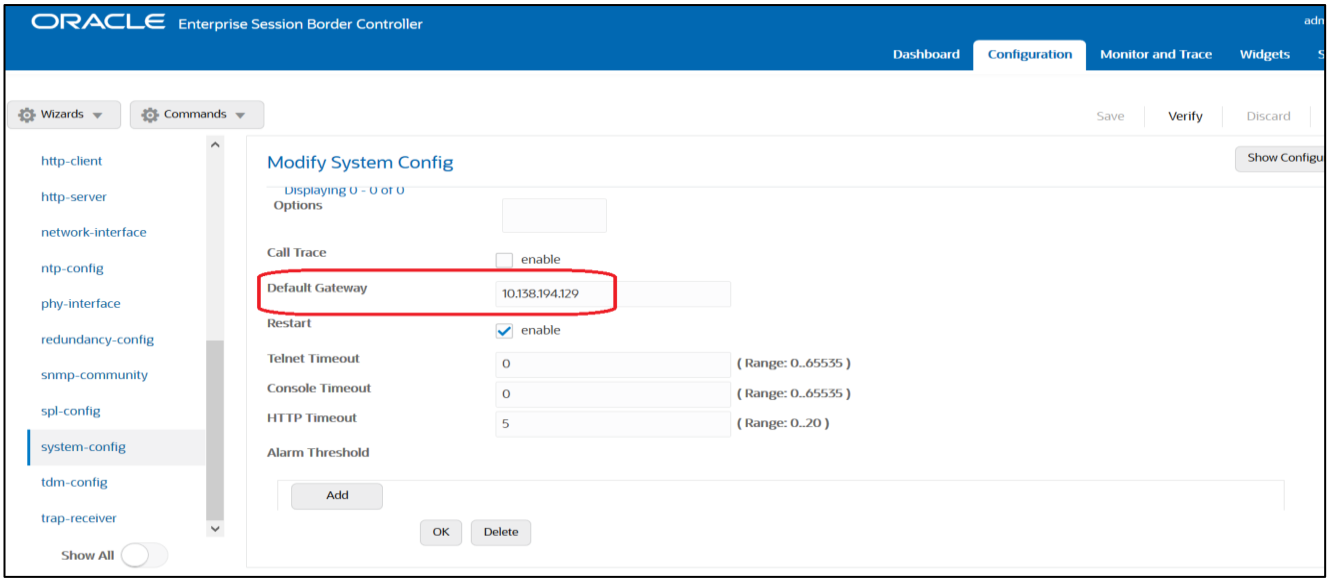
Mib System Contact:

Mib System Name:

Mib System Location:

Acp TLS Profile:

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



Modify System Config

Displaying 0 - 0 of 0

Options:

Call Trace: ☐ enable

Default Gateway: 10.138.194.129

Restart: ☑ enable

Telnet Timeout: 0 (Range: 0..65535)

Console Timeout: 0 (Range: 0..65535)

HTTP Timeout: 5 (Range: 0..20)

Alarm Threshold

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

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

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

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

6.3. Configure Physical Interface values

To configure physical Interface values,

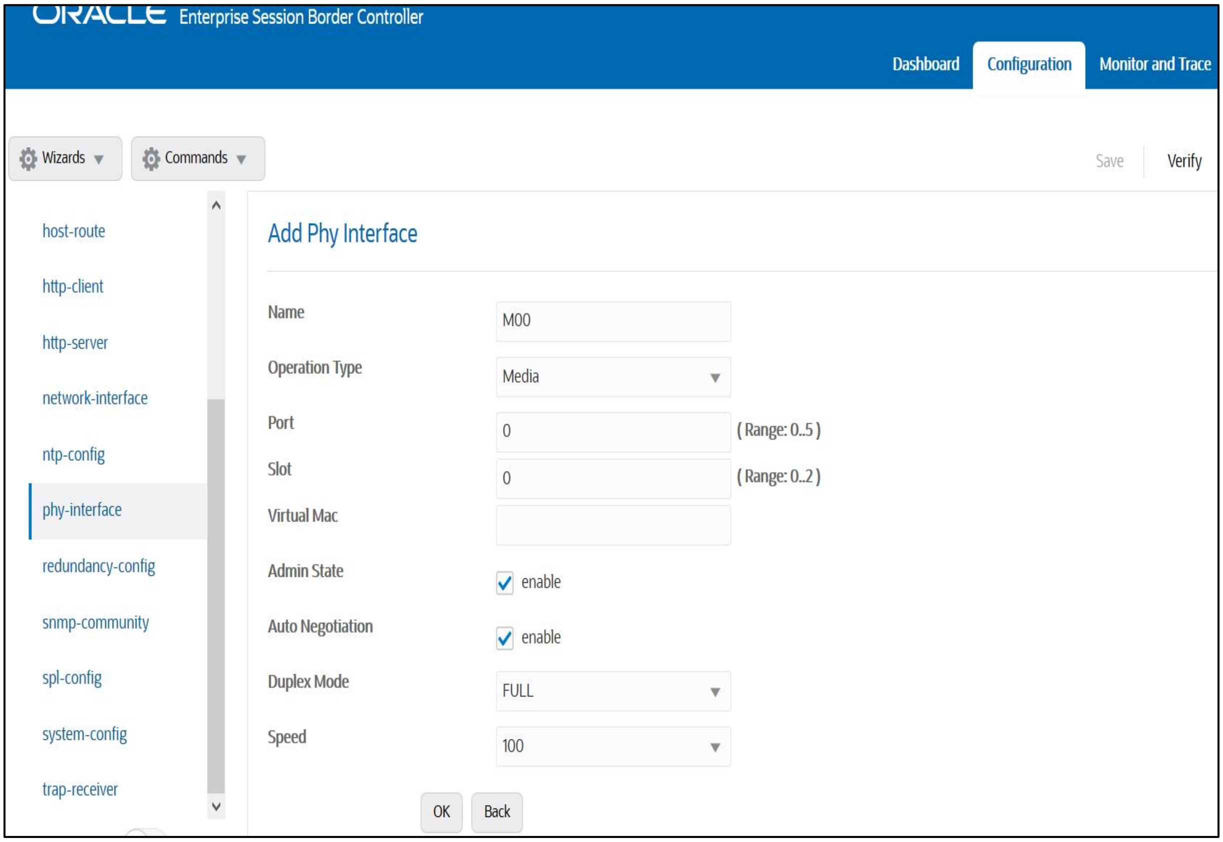
Navigate to System->phy-interface.

ACLI Path: config t->system->phy-interface

Here we have configured, phy-interface M00 for Verizon Trunk and M10 for PureCloud.

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

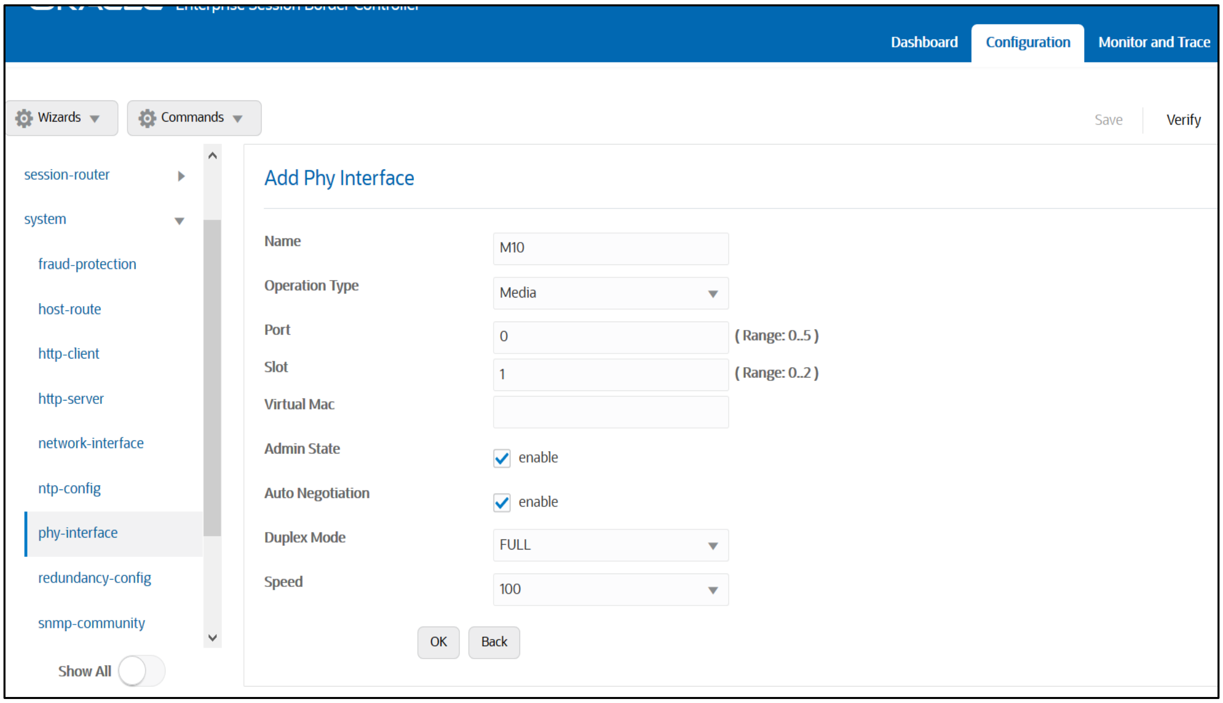
Configure **M00** interface as per example shared below.



Add Phy Interface

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

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



Add Phy Interface

Name	M10	
Operation Type	Media	
Port	0	(Range: 0..5)
Slot	1	(Range: 0..2)
Virtual Mac		
Admin State	☑ enable	
Auto Negotiation	☑ enable	
Duplex Mode	FULL	
Speed	100	

6.3. Configure Network Interface values

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

ACLI Path: config t->system->network-interface

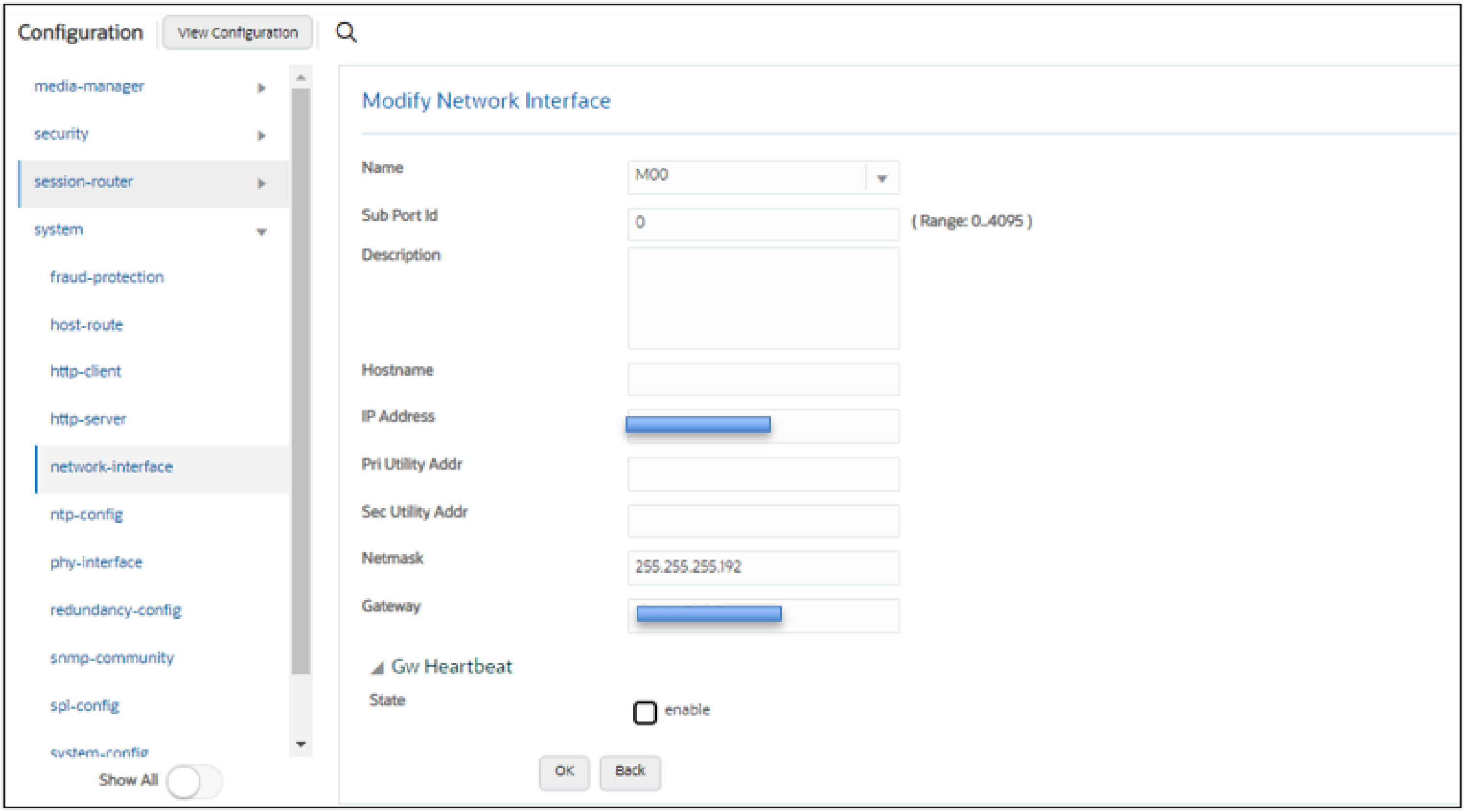
The table below lists the parameters, to be configured for both the interfaces.

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	Verizon	PureCloud Network interface
Name	M00	M10
Host Name		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
dns-ip-backup1		8.8.8.4
Dns-domain		solutionslab.cgbubedford.com

Configure network interface **M00** as below

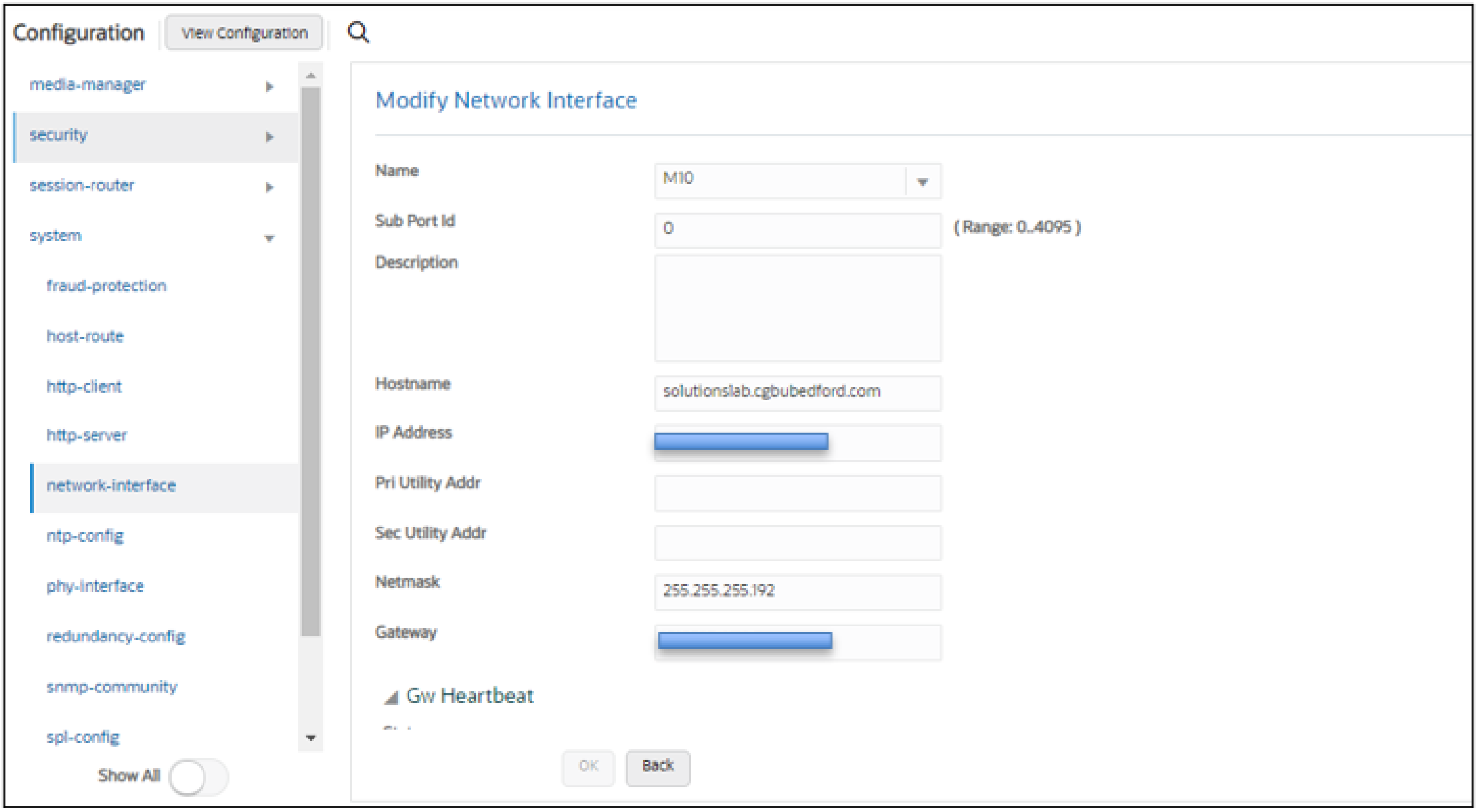


Modify Network Interface

Name: M00
Sub Port Id: 0 (Range: 0..4095)
Description:
Hostname:
IP Address: [redacted]
Pri Utility Addr:
Sec Utility Addr:
Netmask: 255.255.255.192
Gateway: [redacted]

Gw Heartbeat
State: □ enable

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



Modify Network Interface

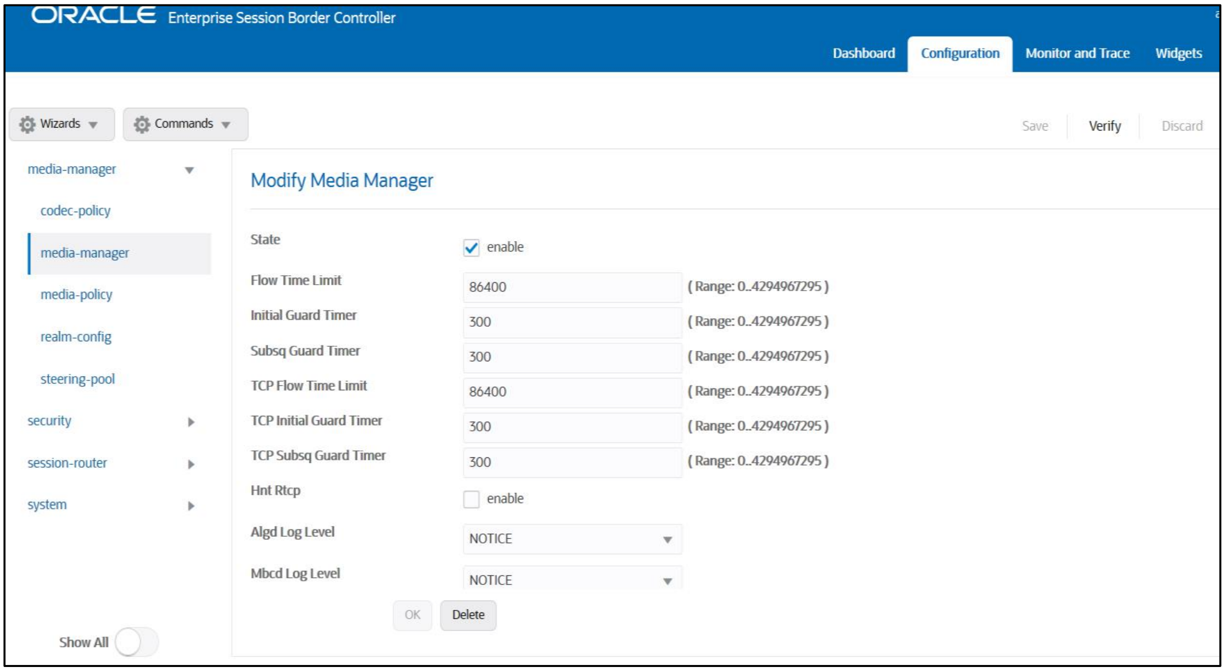
Name: M10
Sub Port Id: 0 (Range: 0..4095)
Description:
Hostname: solutionslab.cgbubedford.com
IP Address: [redacted]
Pri Utility Addr:
Sec Utility Addr:
Netmask: 255.255.255.192
Gateway: [redacted]

Gw Heartbeat

6.4. Enable media manager

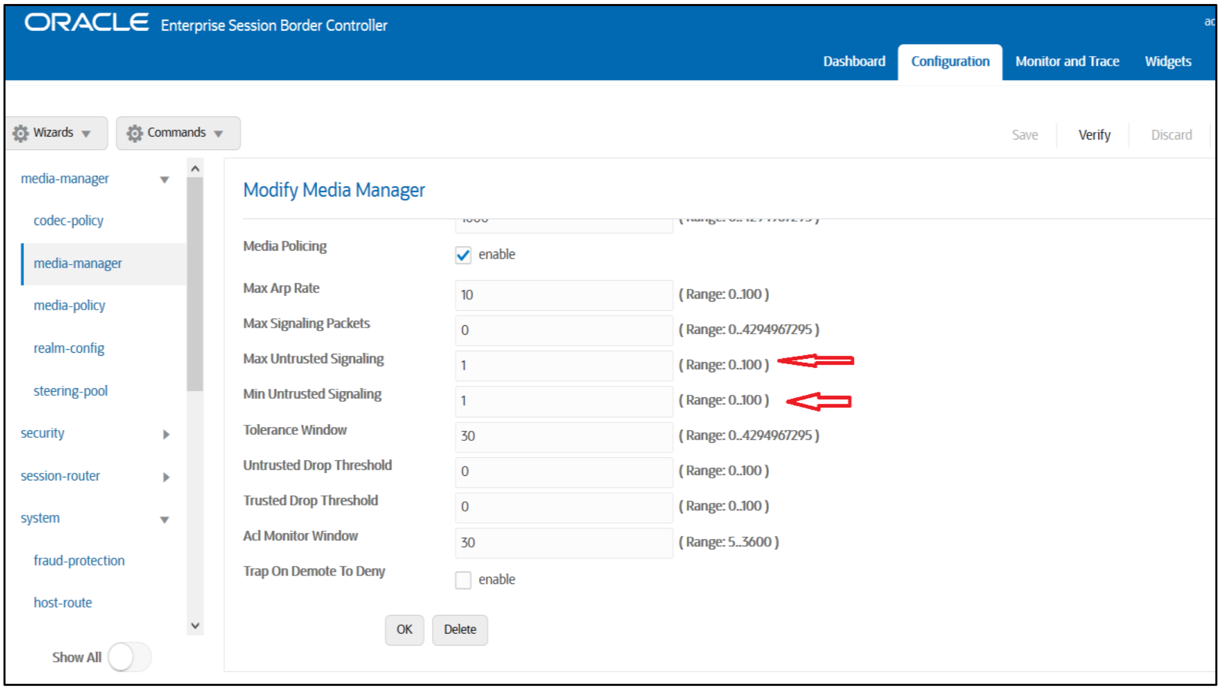
Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below. In addition to the above config, please set the max and min untrusted signaling values to one.

Navigate to Media->Manager->Media-Manager
ACLI Path: config t->media-manager->media-manager-config



Modify Media Manager

State	☑ enable	
Flow Time Limit	86400	(Range: 0..4294967295)
Initial Guard Timer	300	(Range: 0..4294967295)
Subsq Guard Timer	300	(Range: 0..4294967295)
TCP Flow Time Limit	86400	(Range: 0..4294967295)
TCP Initial Guard Timer	300	(Range: 0..4294967295)
TCP Subsq Guard Timer	300	(Range: 0..4294967295)
Hnt Rtcp	□ enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	



Modify Media Manager

Media Policing	☑ enable	
Max Arp Rate	10	(Range: 0..100)
Max Signaling Packets	0	(Range: 0..4294967295)
Max Untrusted Signaling	1	(Range: 0..100)
Min Untrusted Signaling	1	(Range: 0..100)
Tolerance Window	30	(Range: 0..4294967295)
Untrusted Drop Threshold	0	(Range: 0..100)
Trusted Drop Threshold	0	(Range: 0..100)
Acl Monitor Window	30	(Range: 5..3600)
Trap On Demote To Deny	□ enable	

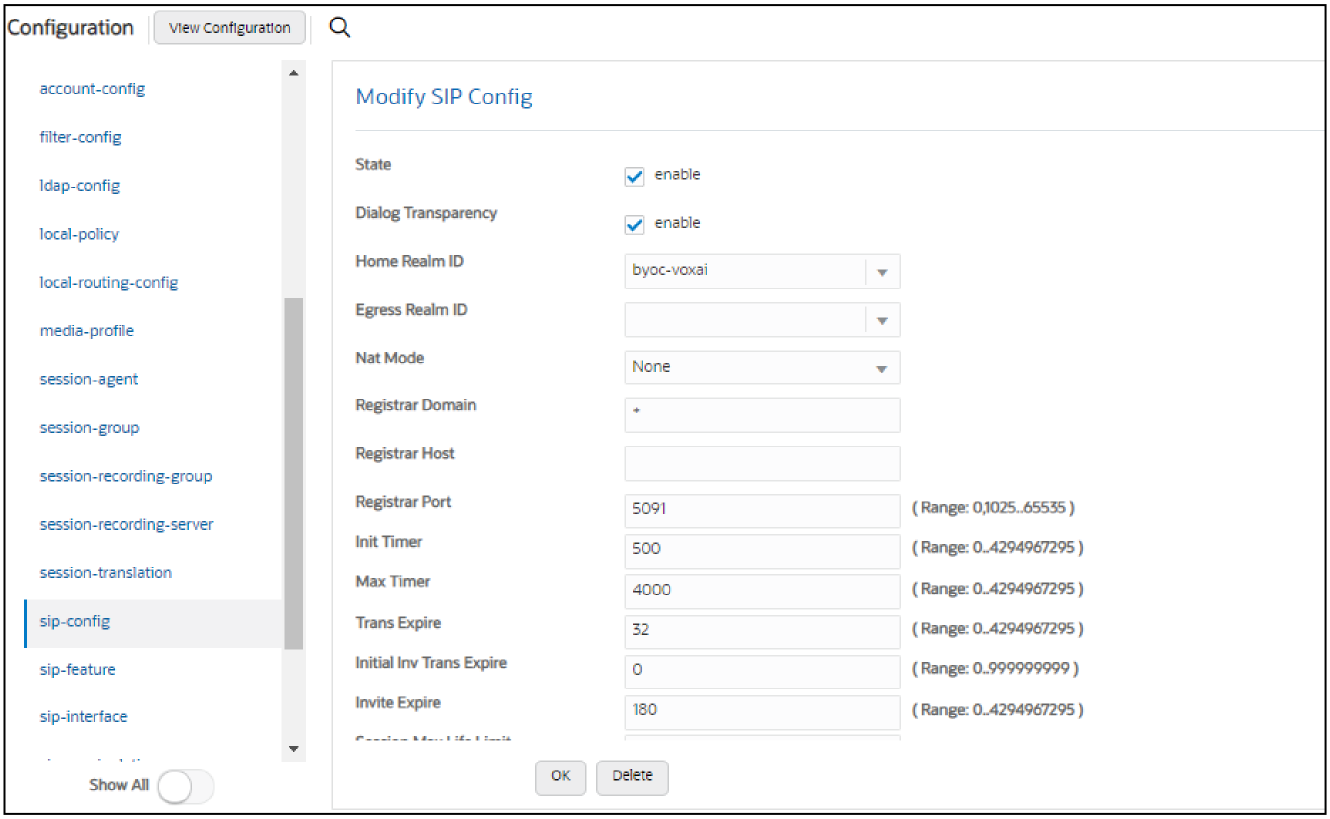
6.5. Enable sip-config

SIP config enables SIP handling in the SBC.

To configure sip-config, Navigate to Session-Router->sip-config
ACLI Path: config t->session-router->sip-config

Add the below options in the sip-config options

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



Modify SIP Config

State ☑ enable

Dialog Transparency ☑ enable

Home Realm ID byoc-voxai

Egress Realm ID

Nat Mode None

Registrar Domain *

Registrar Host

Registrar Port 5091 (Range: 0,1025..65535)

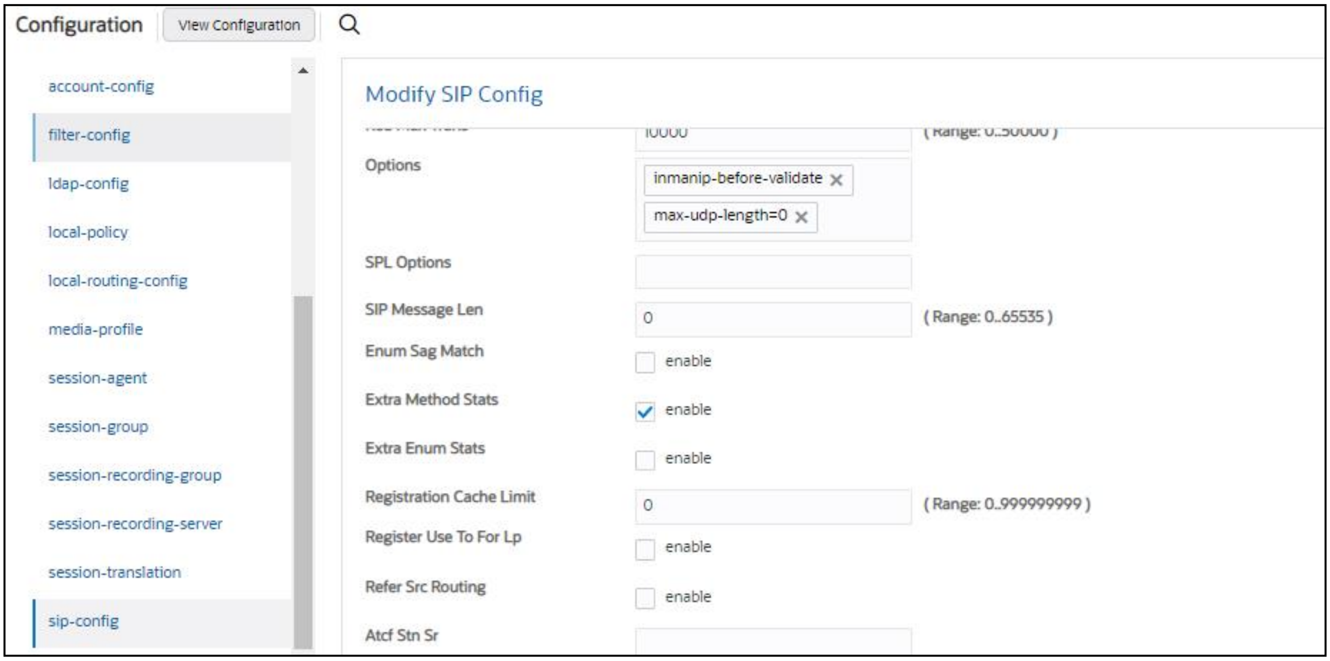
Init Timer 500 (Range: 0..4294967295)

Max Timer 4000 (Range: 0..4294967295)

Trans Expire 32 (Range: 0..4294967295)

Initial Inv Trans Expire 0 (Range: 0..999999999)

Invite Expire 180 (Range: 0..4294967295)



Modify SIP Config

10000 (Range: 0..50000)

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

SPL Options

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

Enum Sag Match □ enable

Extra Method Stats ☑ enable

Extra Enum Stats □ enable

Registration Cache Limit 0 (Range: 0..999999999)

Register Use To For Lp □ enable

Refer Src Routing □ enable

Atcf Stn Sr

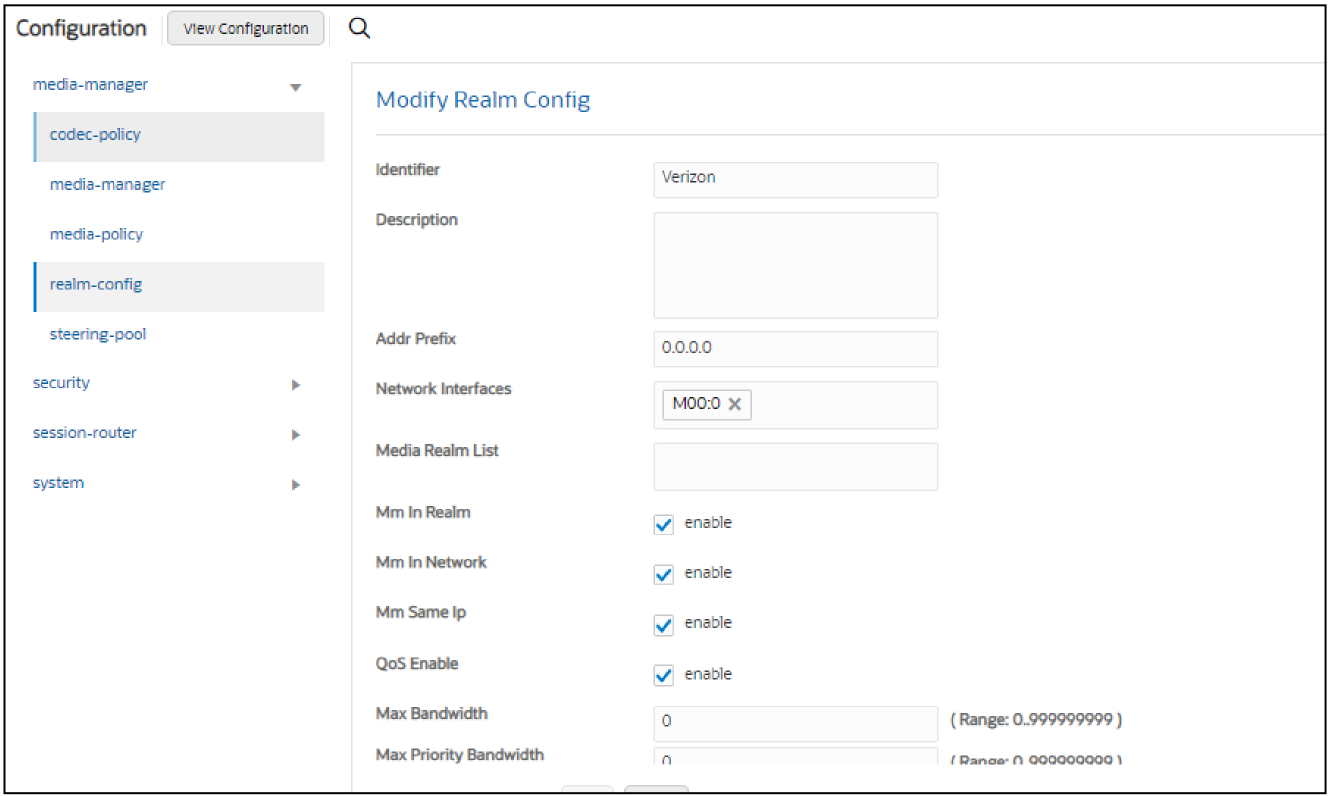
6.6. Configure Realms

Navigate to media-manager -> realm-config
ACLI Path: config t->media-manger->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:

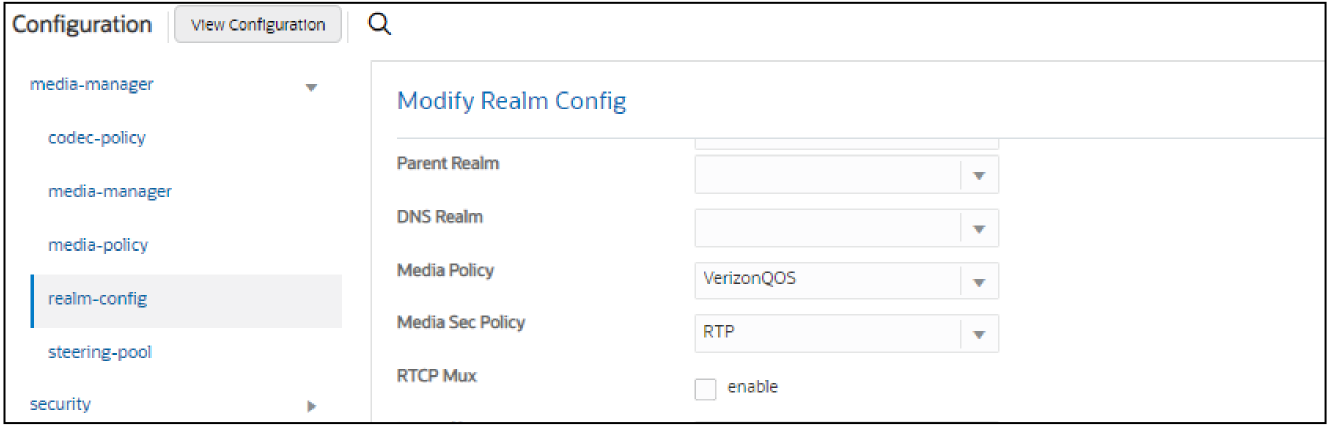
Config Parameter	Verizon	Pure Cloud Realm
Identifier	Verizon	GenesysCloud
Network Interface	M00	M10
Mm in realm	☑	☑
Access Control Trust Level	High	High
Media Sec policy	RTP	sdespolicy
Codec Policy	OptimizeCodecs	
Media Policy	VerizonQOS	

Configure Realm for Verizon Trunk as below -



Modify Realm Config

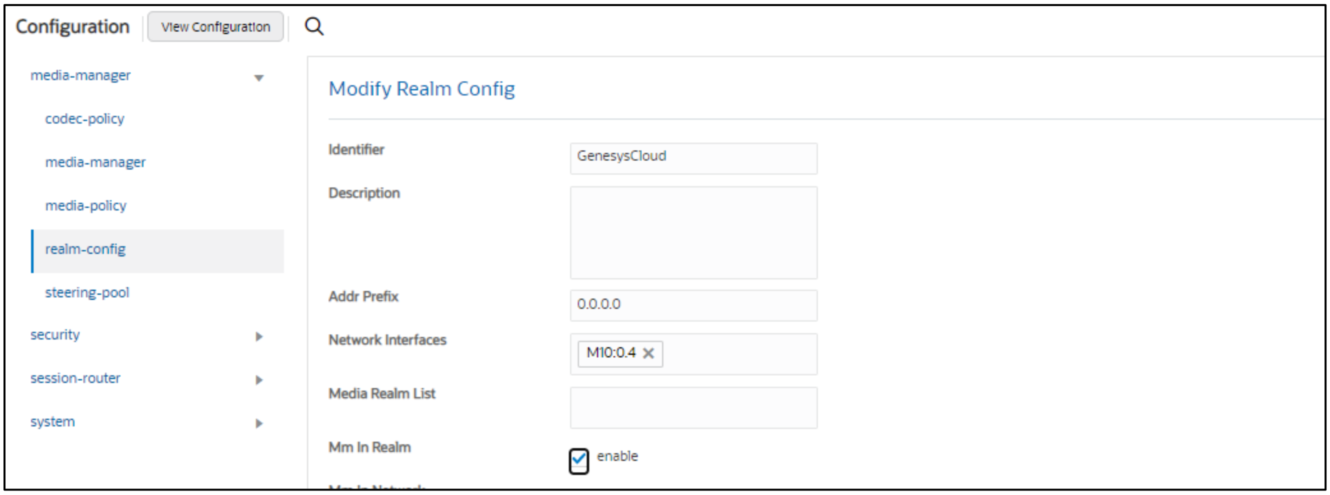
Identifier	Verizon
Description	
Addr Prefix	0.0.0.0
Network Interfaces	M00:0 ✕
Media Realm List	
Mm In Realm	☑ enable
Mm In Network	☑ enable
Mm Same Ip	☑ enable
QoS Enable	☑ enable
Max Bandwidth	0 (Range: 0..999999999)
Max Priority Bandwidth	0 (Range: 0..999999999)



Modify Realm Config

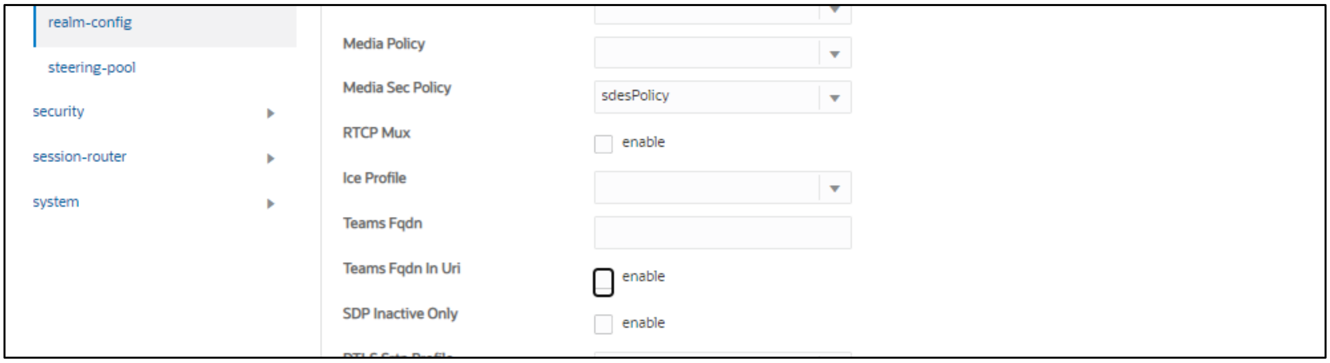
Parent Realm	
DNS Realm	
Media Policy	VerizonQOS
Media Sec Policy	RTP
RTCP Mux	□ enable

Configure Realm for Genesys PureCloud as below -



Modify Realm Config

Identifier	GenesysCloud
Description	
Addr Prefix	0.0.0.0
Network Interfaces	M10:0.4 ✕
Media Realm List	
Mm In Realm	☑ enable



Media Policy

Media Sec Policy: sdesPolicy

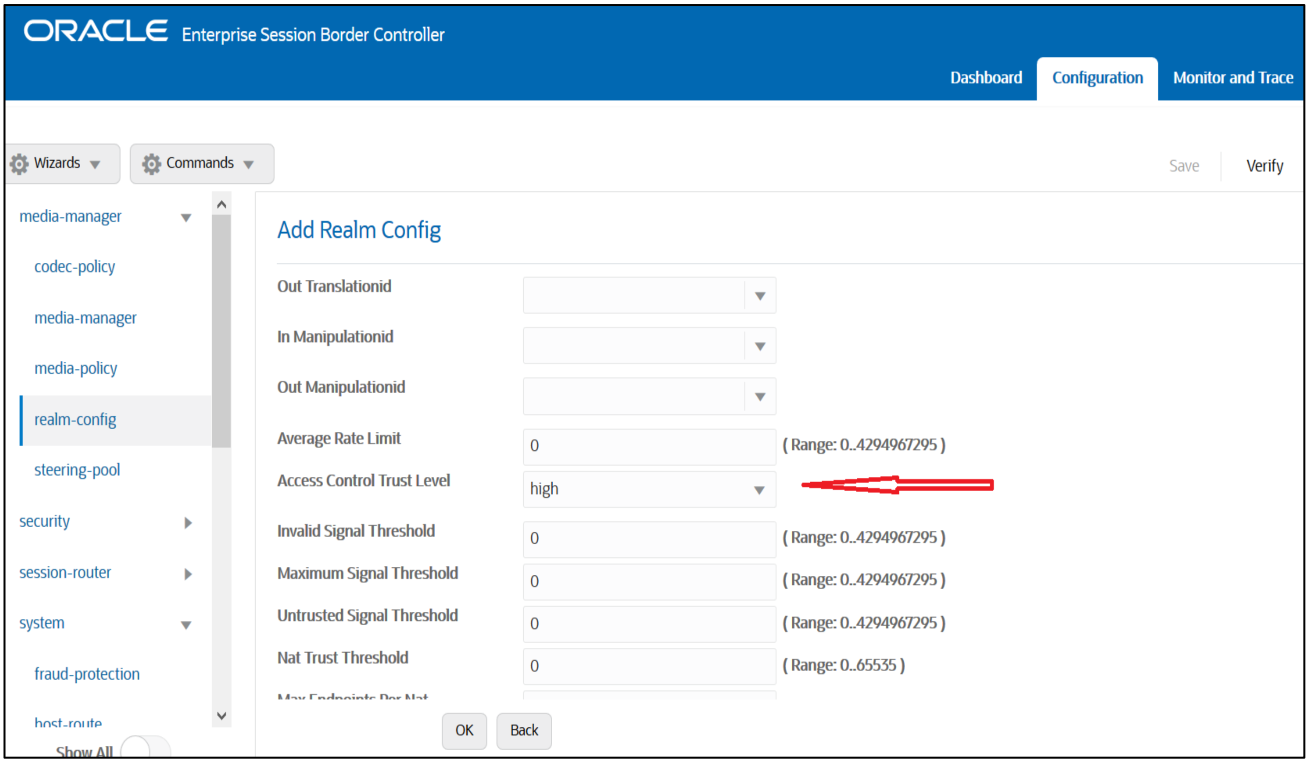
RTCP Mux: □ enable

Ice Profile

Teams Fqdn

Teams Fqdn In Uri: □ enable

SDP Inactive Only: □ enable



Add Realm Config

Out Translationid

In Manipulationid

Out Manipulationid

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

Access Control Trust Level: high

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

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

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

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

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

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

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

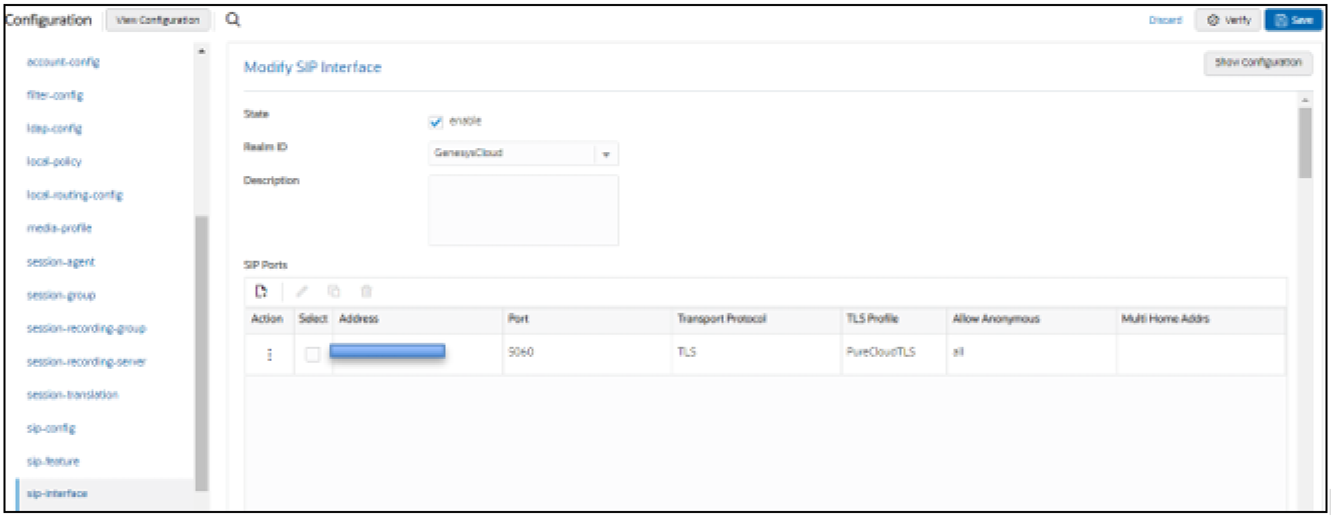
6.7. Configure SIP Interfaces

Navigate to session-router-> sip-interface and configure the sip-interface as shown below.
ACLI Path: config t->session-router->sip-interface

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.

Configure sip-interface for Genesys PureCloud and Verizon Business Trunk as below -



Modify SIP Interface

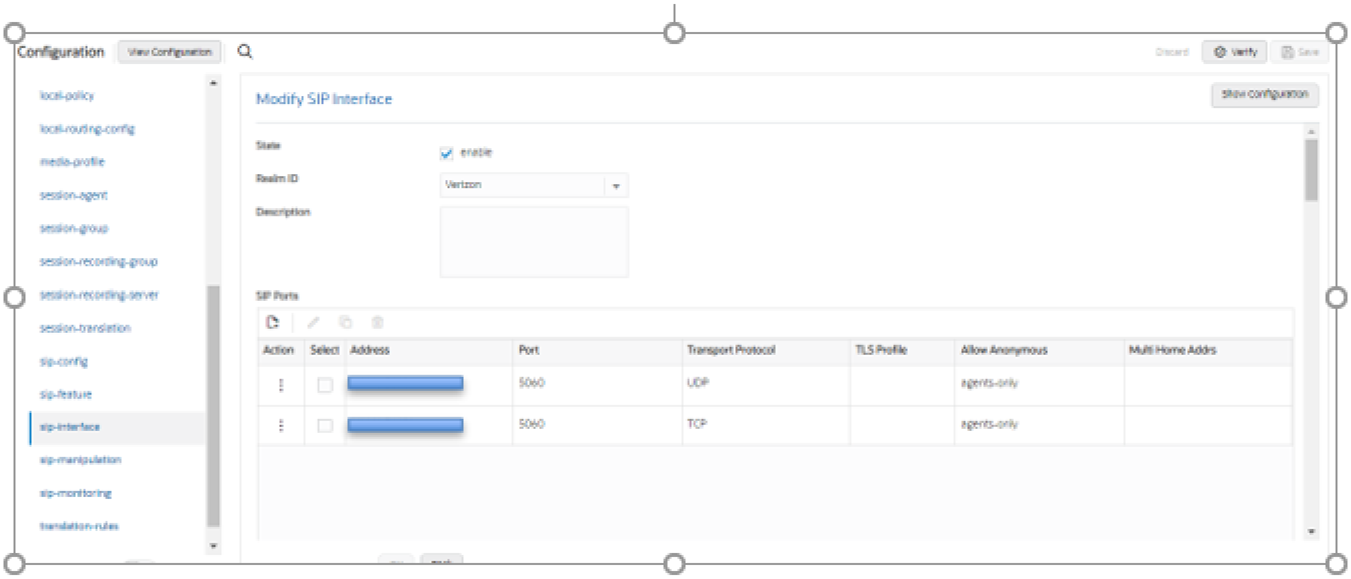
State ☑ enable

Realm ID GenesysCloud

Description

SIP Ports

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



Modify SIP Interface

State ☑ enable

Realm ID Verizon

Description

SIP Ports

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
⋮	□	[redacted]	5060	UDP		agents-only	
⋮	□	[redacted]	5060	TCP		agents-only	

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

6.8. Configure session-agent

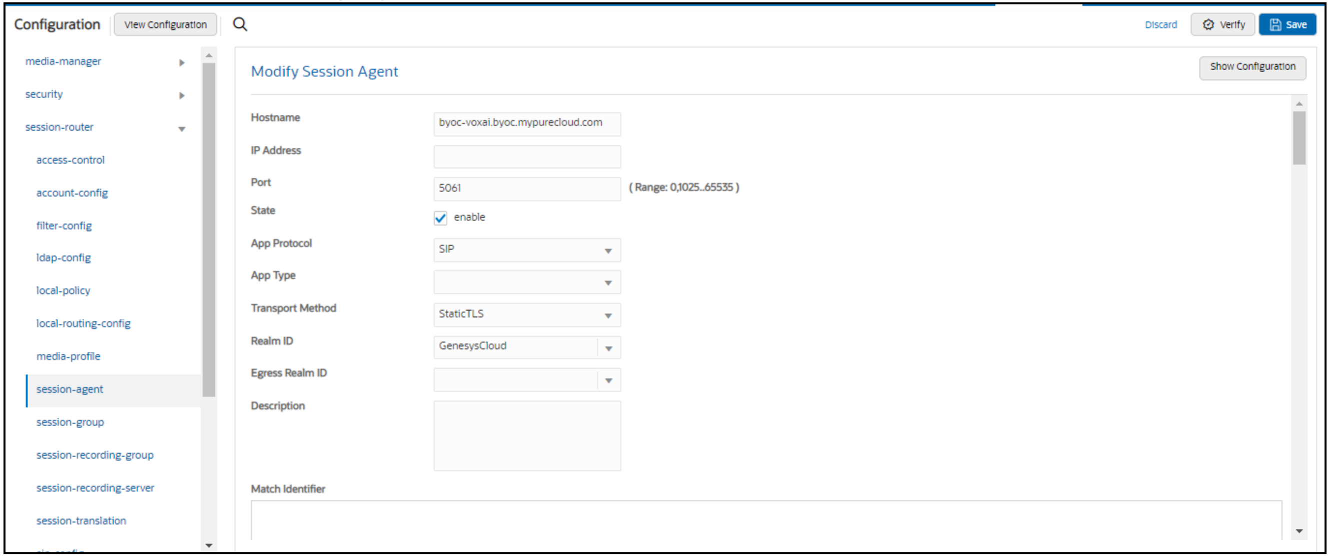
Session-agents are config elements, which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

Navigate to session-router->Session-Agent
ACLI Path: config t->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 PureCloud to check health
- ping-interval to 30 sec



Modify Session Agent

Hostname: byoc-voxai.byoc.mypurecloud.com

IP Address:

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

State: ☑ enable

App Protocol: SIP

App Type:

Transport Method: StaticTLS

Realm ID: GenesysCloud

Egress Realm ID:

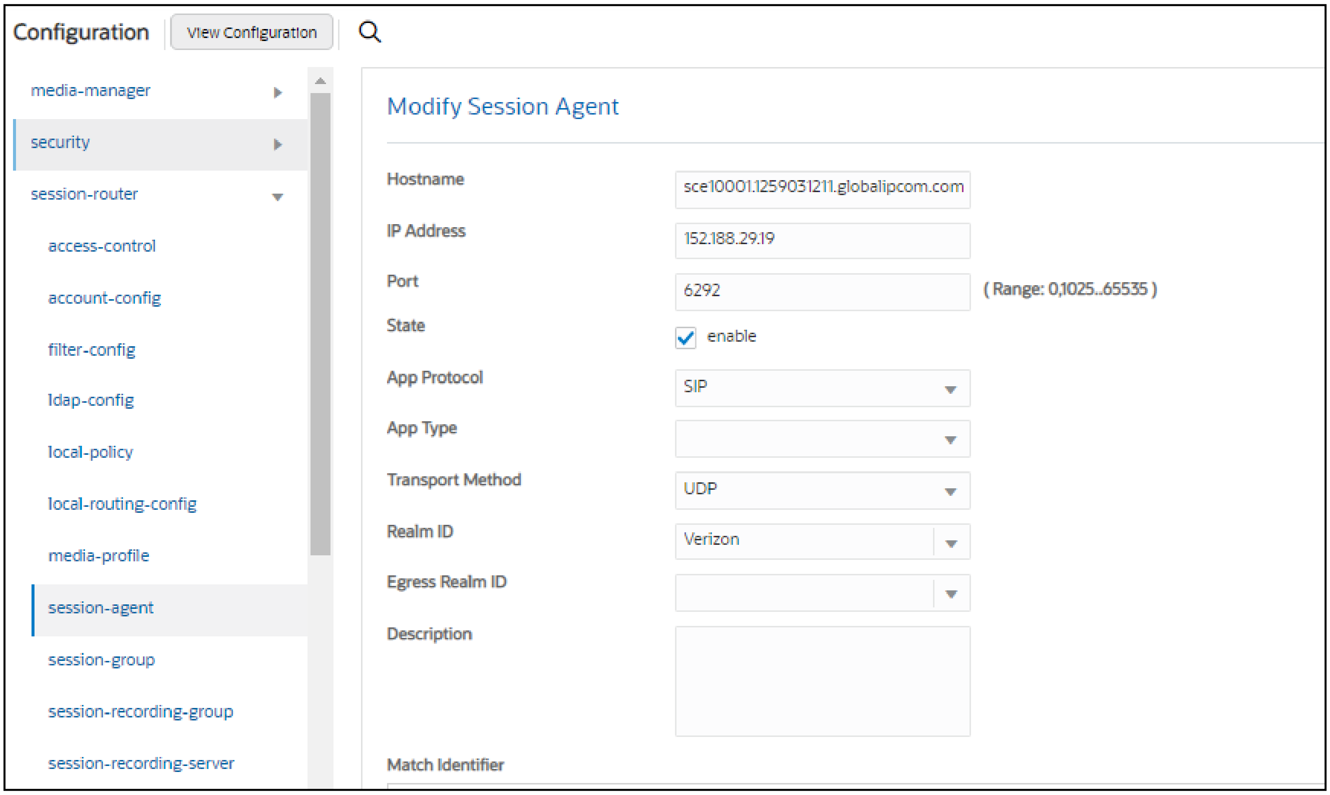
Description:

Match Identifier:

Configure the session-agents for the Verizon Business Trunk as below Table.

Config Parameter	Verizon 1	Verizon2
Hostname	<Verizon FQDN 1>	<Verizon FQDN 2>
IP-Address	<IPV4 Address>	<IPV4 Address>
Port	5201	6292
Transport method	UDP	UDP
Realm ID Verizon	Verizon	
Ping Method	OPTIONS	OPTIONS
Ping Interval	30	30
Refer Call Transfer	enabled	enabled
Ping Response	☑	☑

Verizon Session Agent 1



Modify Session Agent

Hostname: sce10001.1259031211.globalipcom.com

IP Address: 152.188.29.19

Port: 6292 (Range: 0,1025..65535)

State: ☑ enable

App Protocol: SIP

App Type:

Transport Method: UDP

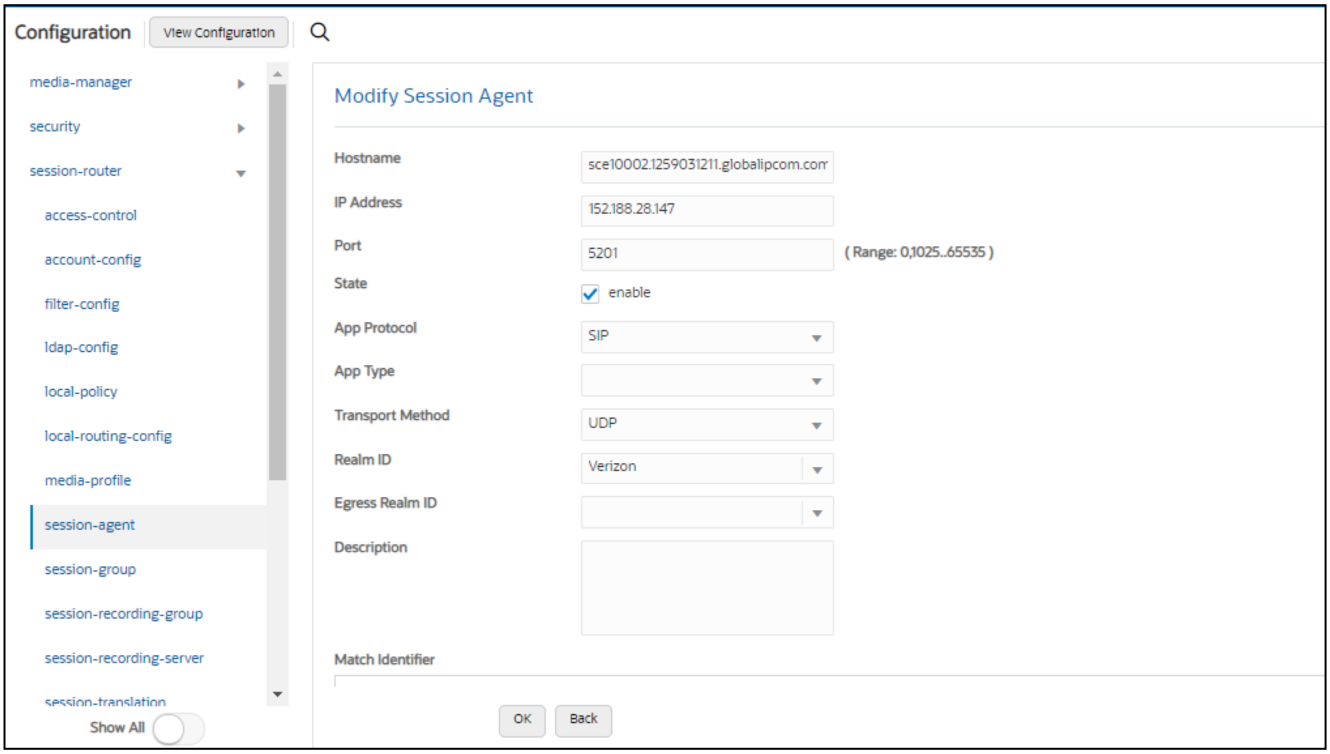
Realm ID: Verizon

Egress Realm ID:

Description:

Match Identifier

Verizon Session Agent 2



Modify Session Agent

Hostname: sce10002.1259031211.globalipcom.com

IP Address: 152.188.28.147

Port: 5201 (Range: 0,1025..65535)

State: ☑ enable

App Protocol: SIP

App Type:

Transport Method: UDP

Realm ID: Verizon

Egress Realm ID:

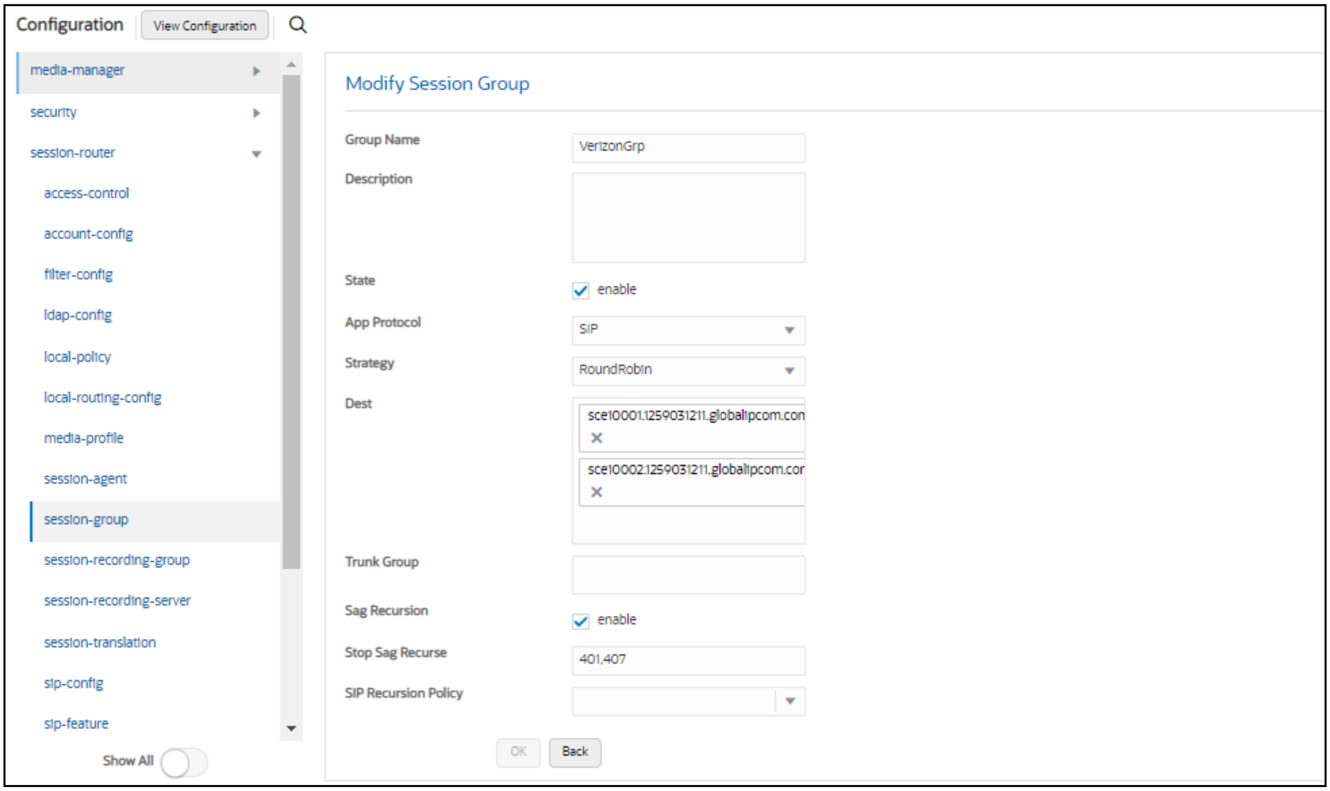
Description:

Match Identifier

6.9. Configure session-agent group

A session agent group allows the SBC to create a load balancing model.
Navigate to Session-Router->Session-Group.
ACLI Path: config t->session-router->session-group

Please configure the following group for Verizon Session Agents



Modify Session Group

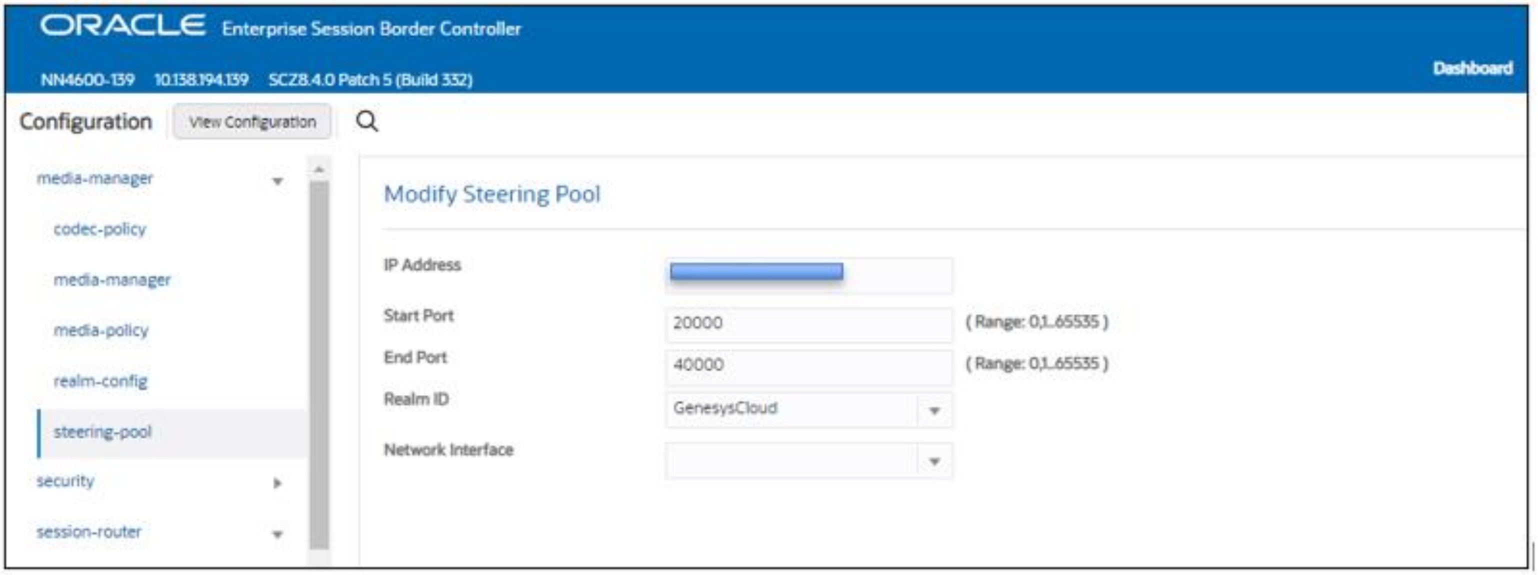
Group Name	VerizonGrp
Description	
State	☑ enable
App Protocol	SIP
Strategy	RoundRobin
Dest	sce10001.1259031211.globalipcom.con sce10002.1259031211.globalipcom.cor
Trunk Group	
Sag Recursion	☑ enable
Stop Sag Recurse	401,407
SIP Recursion Policy	

6.10. Configure steering-pool

Steering-pool config allows configuration to assign IP address(s), ports & a realm. They define sets of ports that are used for steering media flows through the OCSBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

Navigate to GUI Path: media-manger->steering-pool
ACLI Path: config t->media-manger->steering-pool

Configure PureCloud Steering pool as below -



Modify Steering Pool

IP Address [redacted]

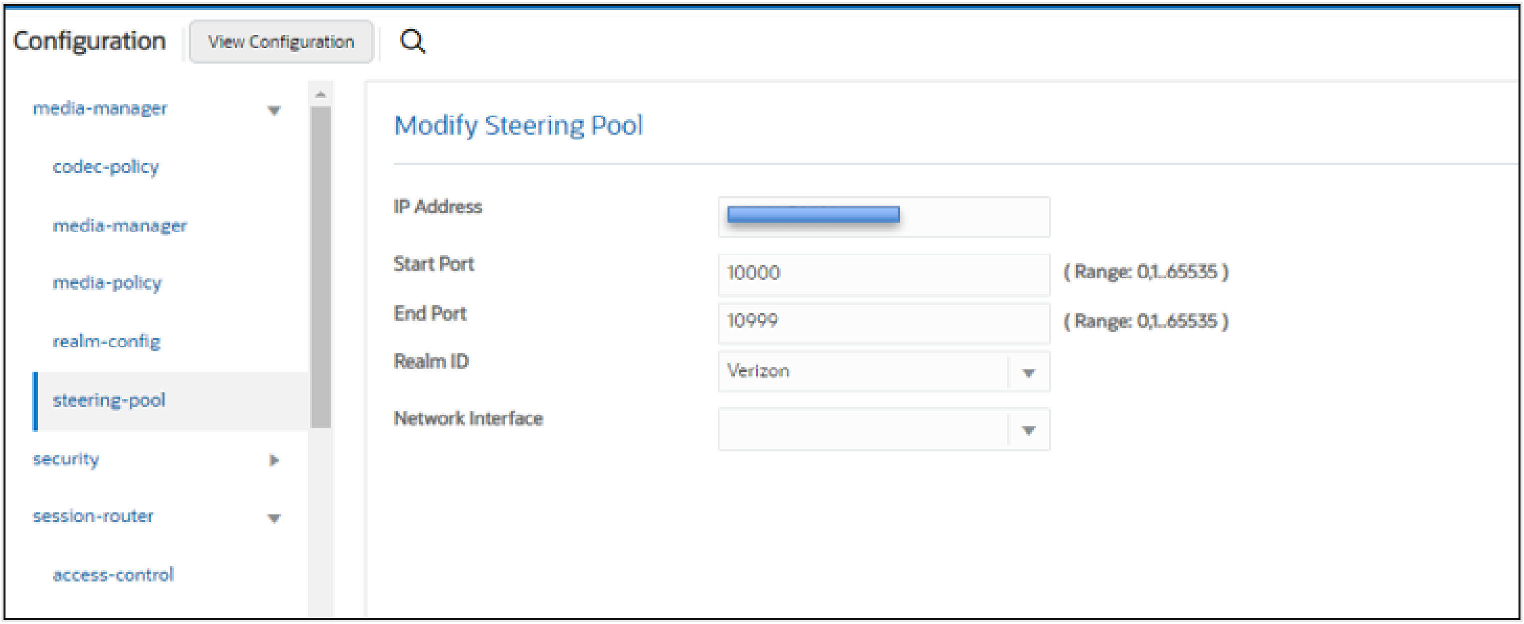
Start Port 20000 (Range: 0,1..65535)

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

Realm ID GenesysCloud

Network Interface

Configure Verizon Business Trunk Steering Pool as below -



Modify Steering Pool

IP Address [redacted]

Start Port 10000 (Range: 0,1..65535)

End Port 10999 (Range: 0,1..65535)

Realm ID Verizon

Network Interface

6.11. SIP Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Genesys Pure Cloud and and IKE/IPSEC to connect to Verizon Business IP Trunk

Genesys Purecloud 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. Similarly, Verizon Business requires a secure, IPSEC tunnel be established between the Oracle SBC and the VZB network. You must obtain the IPSEC Template from your Verizon Business account team before configuring IKE/IPSEC on the Oracle SBC.

6.11.1 Configuring Certificates

This section describes how to configure the SBC for TLS and SRTP communication for **PureCloud**. 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)
- DigiCert Root CA
- DigiCert Intermidiate Cert (this is optional – only required if your server certificate is signed by an intermediate)
- DigiCertEVRootCA (Genesys PureCloud)

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 Certificate(PureCloud)**	**DigiCertEV RootCA**	**DigiCert Root CA**	**DigiCert Intermediate**
Name	SBCCert	PureCloudCert	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA
Common Name	solutionslab.cgbubedford.com	PureCloudCert	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA
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

6.11.1.1 End Entity Certificate

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

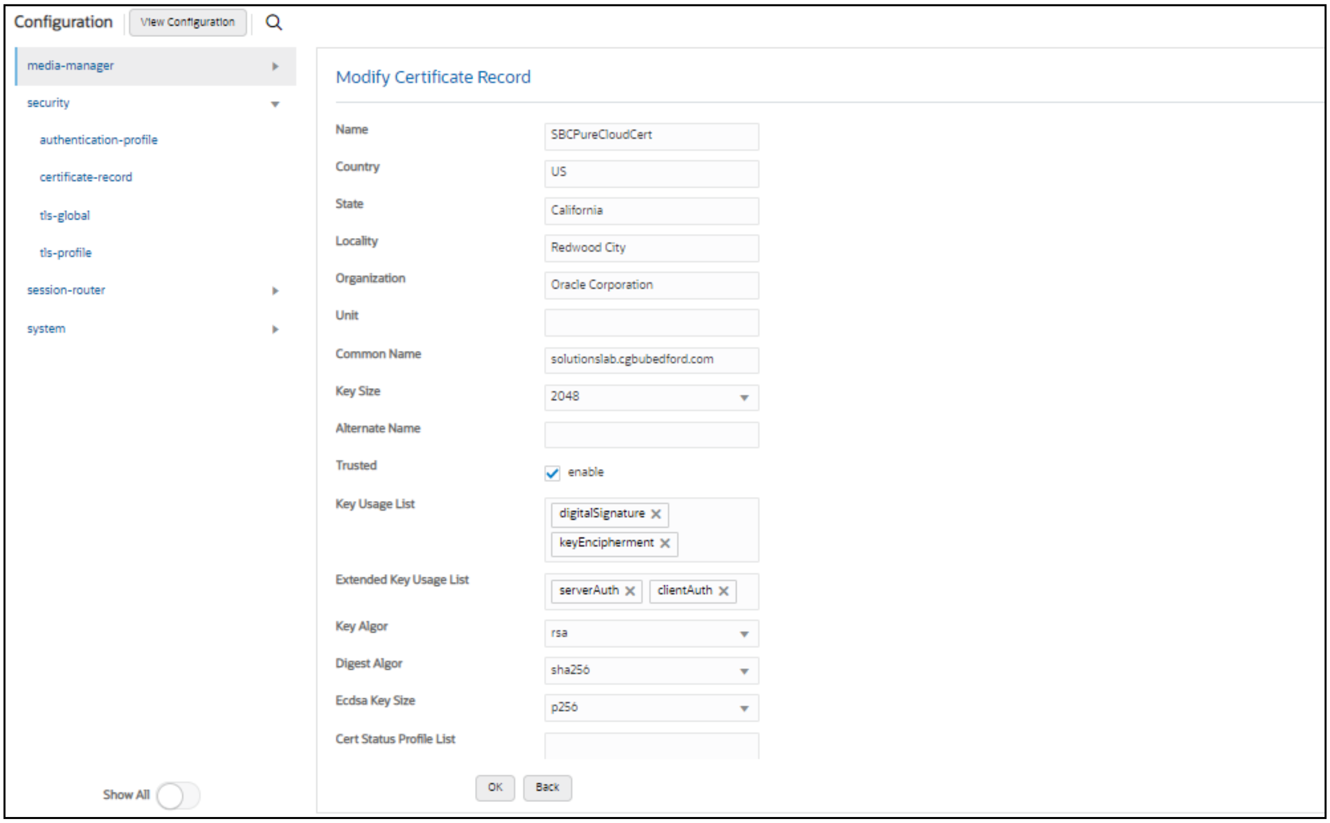
Here in this setup,We wil create two end entity certificates for PureCloud.

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

Step 1 Configure SBC Certificate Record

To Configure the certificate record:

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



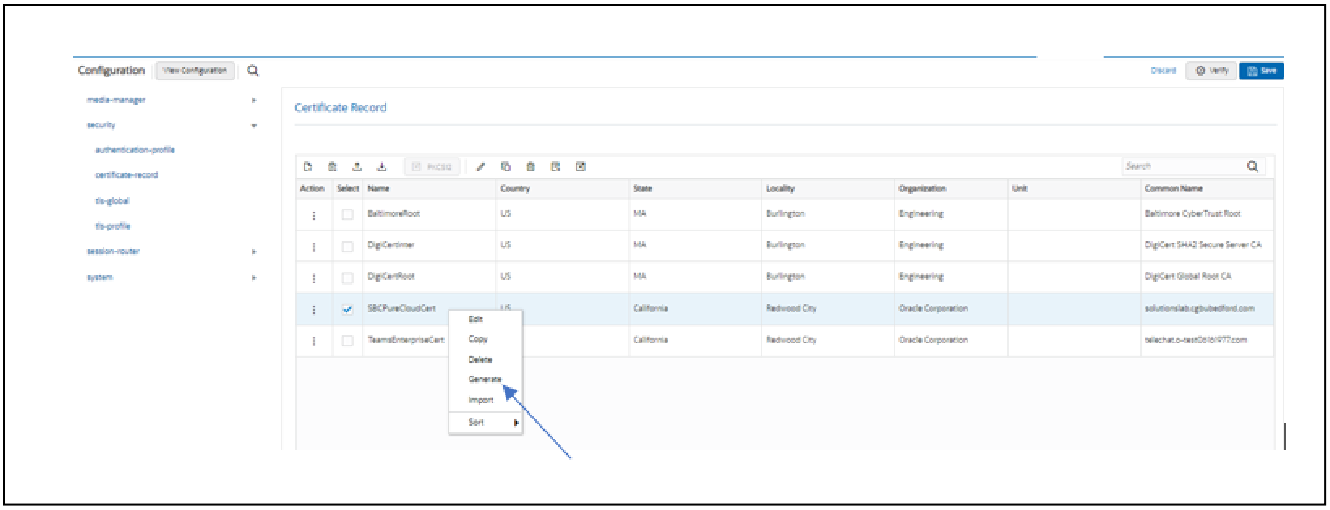
Modify Certificate Record

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

Step 2 – Generating a certificate signing request

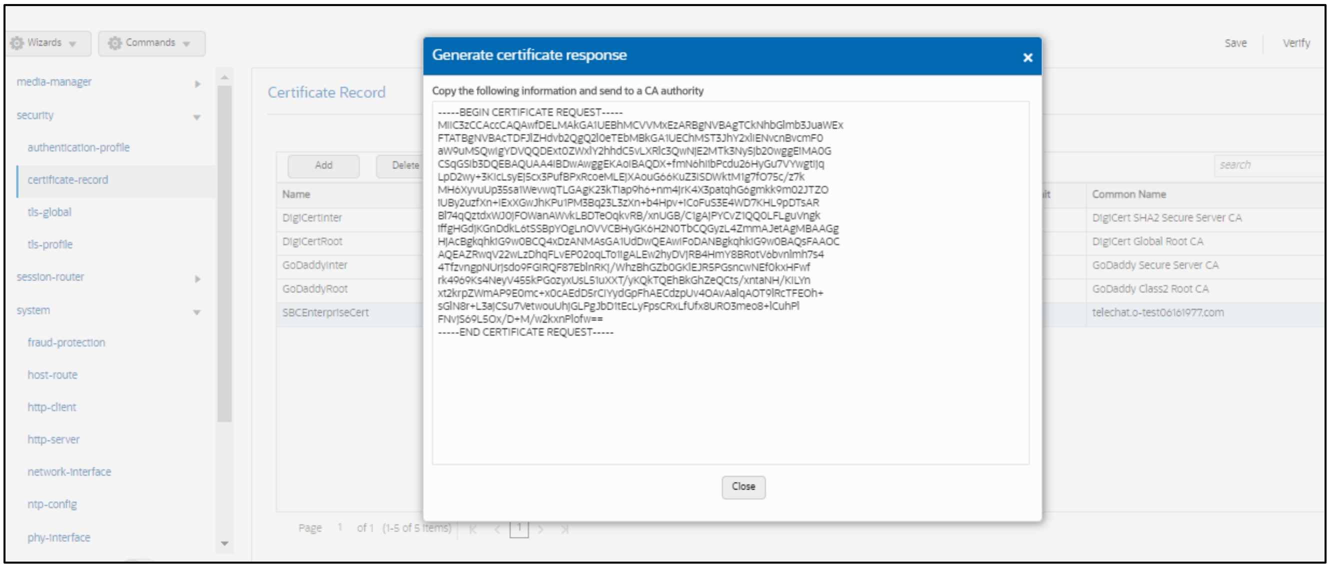
Please note – certificate signing request is only required to be executed for SBC Certificate – not for the root/intermediate certificates.

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



Certificate Record

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



Certificate Record

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

Generate certificate response

Copy the following information and send to a CA authority

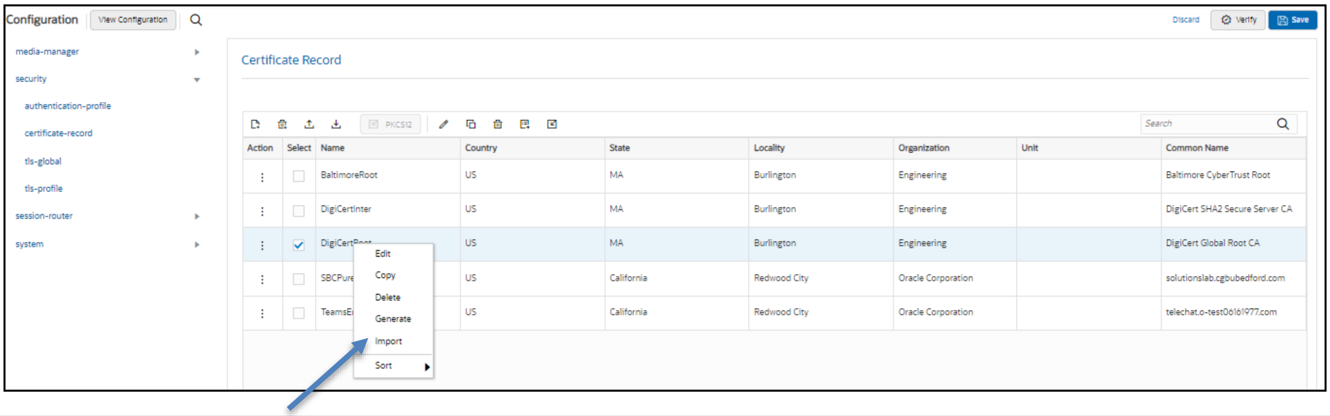
```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3zCCAccCAQAwfDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWEx
FTATBgNVBAcTDFJlZHdvb2QgQ2l0eTEbMBkGA1UEChMST3JhY2xlIENvcnBvcmF0
aW9uMSQwIgYDVQQDExt0ZWxlY2hhdC5vLXRlc3QwNjE2MTk3Ny5jb20wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDX+fmN6hI1bPcdu26HyGu7VYwgtIJq
LpD2wy+3KIcLsyEJ5cx3PufBPxRcoeMLEJXAouG66KuZ3ISDWktM1g7fO75c/z7k
MH6XyvuUp35sa1WevwqTLGAgK23kTIap9h6+nm4JrK4X3patqhG6gmkk9m02JTZO
1UBy2uzfXn+IExXGwJhKPu1PM3Bq23L3zXn+b4Hpv+lCoFuS3E4WD7KHL9pDTsAR
Bl74qQztdxWJ0JFOWanAWvkLBDTeOqkvRB/xnUGB/C1gAJPYCvZ1QQ0LFLguVngk
1ffgHGdJKGnDdkL6tSSBpYOgLnOVVCBHyGK6H2N0TbCQGyzL4ZmmAJetAgMBAAGg
HJAcBgkqhkiG9w0BCQ4xDzANMAsGA1UdDwQEAwIFoDANBgkqhkiG9w0BAQsFAAOC
AQEAZRwqV22wLzDhqFLvEP02oqLTo1IgALEw2hyDVJRB4HmY8BRotV6bvnlmh7s4
4TfzvngpNUrJsdo9FGIRQF87EblnRKJ/WhzBhGZb0GKlEJR5PGsncwNEf0kxHFwf
rk4969Ks4NeyV455kPGozyxUsL51uXXT/yKQkTQEhBkGhZeQCts/xntaNH/KILYn
xt2krpZWmAP9E0mc+x0cAEdD5rCIYydGpFhAECdzpUv4OAvAalqAOT9lRcTFEOh+
sGlN8r+L3aJCSu7VetwouUhJGLPgJbD1tEcLyFpsCRxLfUfx8URO3meo8+lCuhPl
FNvJS69L5Ox/D+M/w2kxnPlofw==
-----END CERTIFICATE REQUEST-----
```

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

Step 3 Import Certificates to the SBC

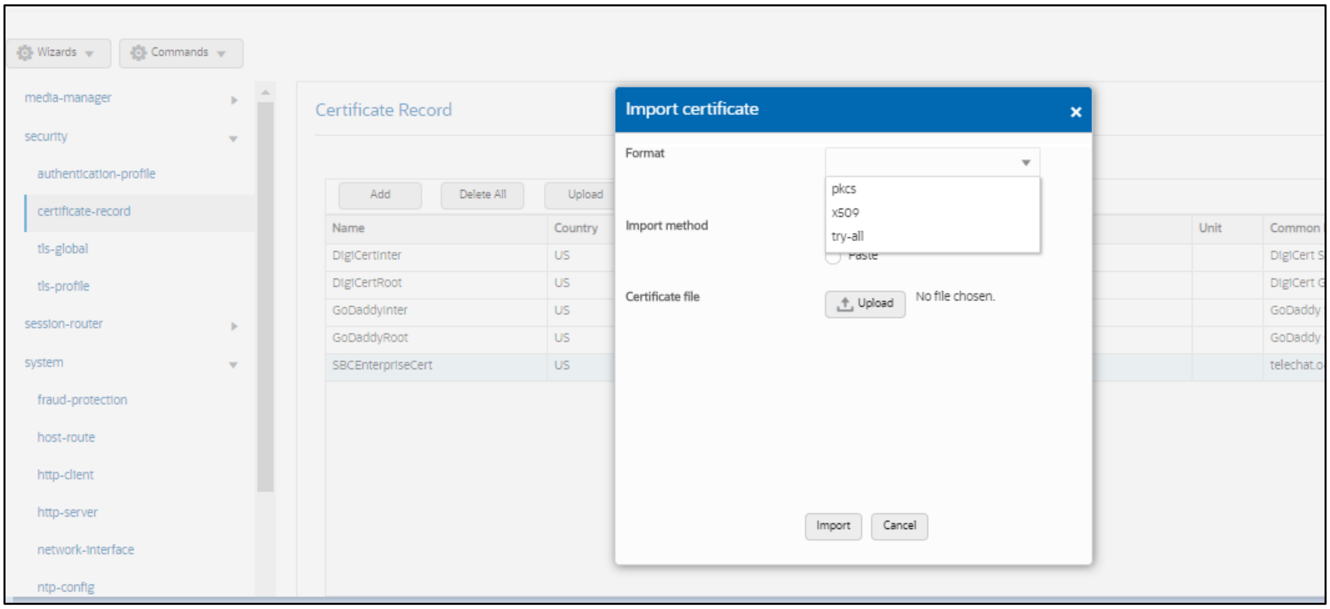
Once certificate signing request have been completed – import the signed certificate to the SBC.

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



Certificate Record

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



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

6.11.1.2 Import CA Certificate

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

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

6.11.2 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

ACLI Path: config t->security->tls-profile

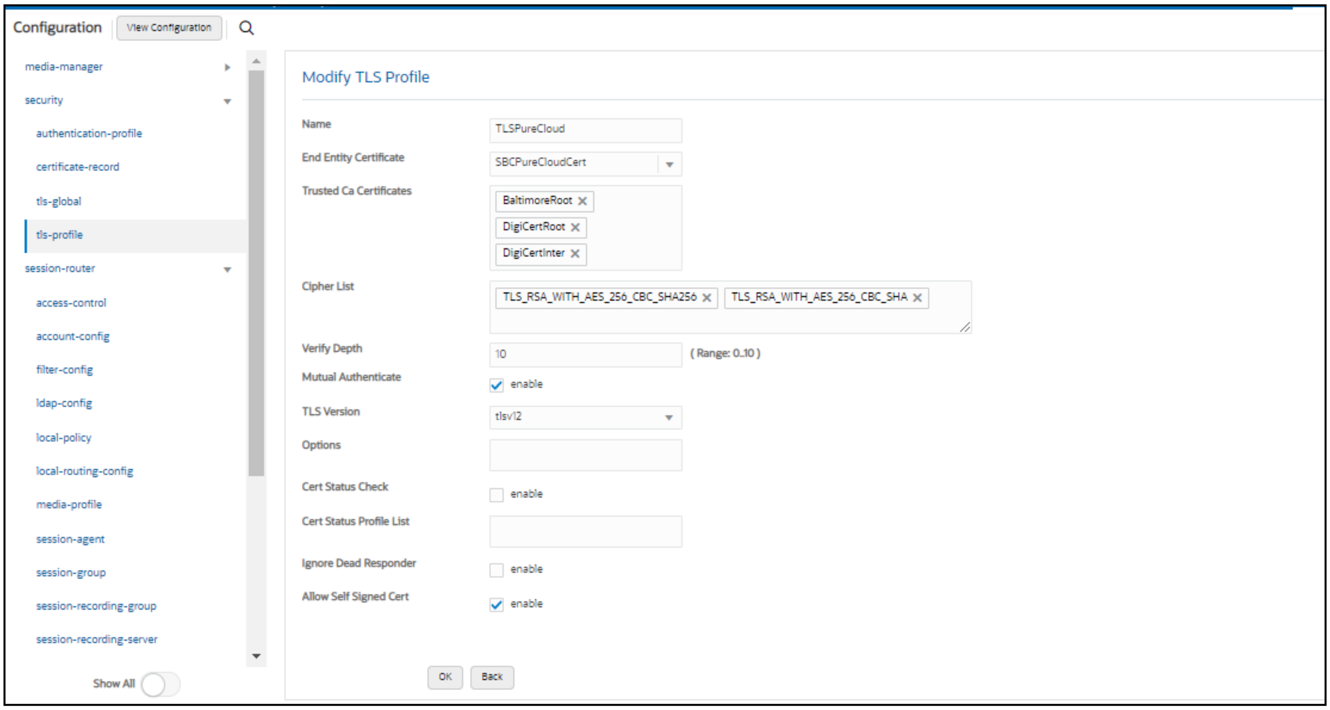
TLS-Profile - Genesys PureCloud

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

Supported TLS ciphers include:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256

TLS-only listeners are available on host port 5061.



Modify TLS Profile

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

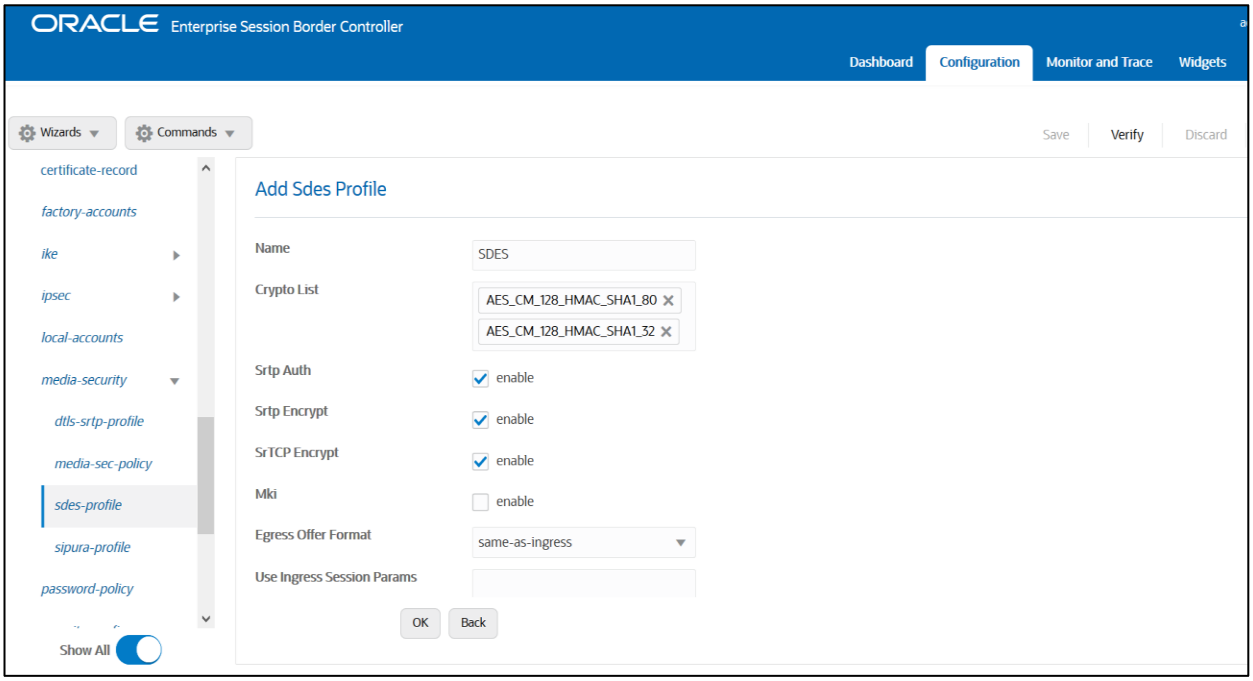
6.12. Media Security Configuration.

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

6.12.1 Configure sdes profile

This is the first element to be configured for media security, where the algorithm and the crypto’s to be used are configured.

Navigate to ->Security -> Media Security ->sdes profile and create the policy as below.
ACLI Path: config t->security->media-security->sdes-profile



Add Sdes Profile

Name: SDES
Crypto List: AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32
Srtp Auth: ☑ enable
Srtp Encrypt: ☑ enable
SrTCP Encrypt: ☑ enable
Mki: ☐ enable
Egress Offer Format: same-as-ingress
Use Ingress Session Params:

6.12.2. Configure Media Security Profile

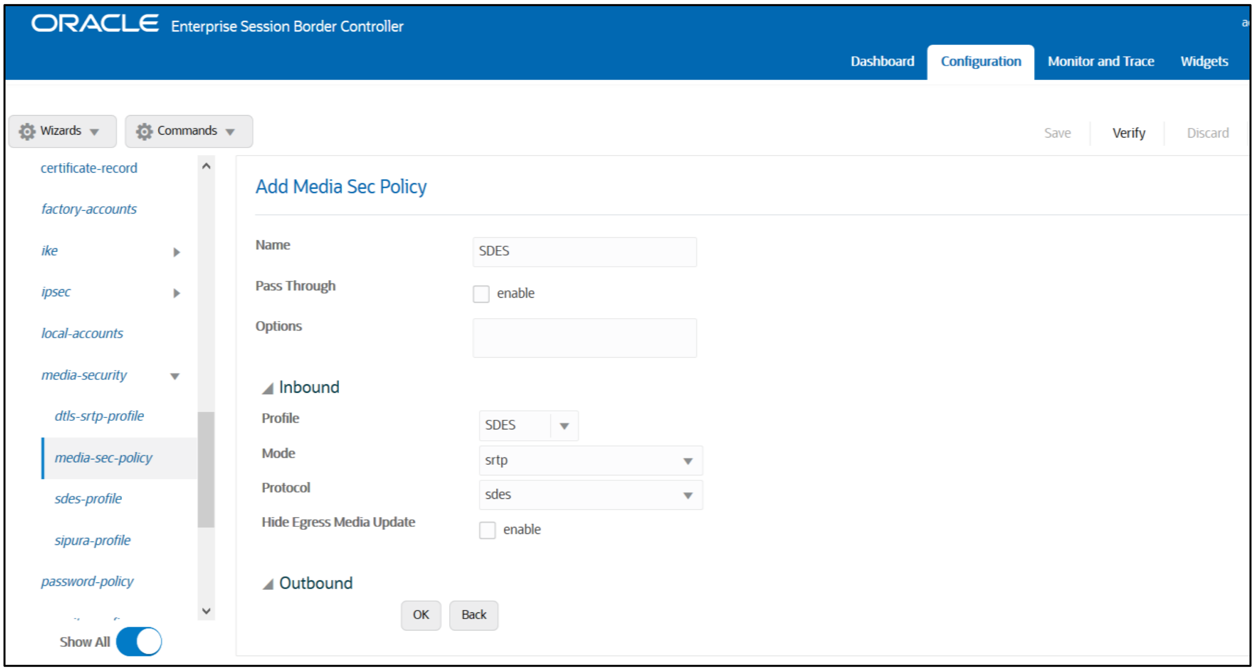
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them) and, if SRTP needs to be used, the sdes-profile that needs to be used

In this example, we are configuring two media security policies. One to secure and decrypt media toward Genesys PureCloud, the other for non-secure media facing Verizon Business Trunk.

Navigate to ->Security -> Media Security ->media Sec policy and create the policy as below:
ACLI Path: config t->security->media-security->media-sec-policy

Create Media Sec policy with name SDES, which will have the sdes profile, created above.

Assign this media policy to PureCloud Realm.



Add Media Sec Policy

Name: SDES

Pass Through: □ enable

Options:

Inbound

Profile: SDES

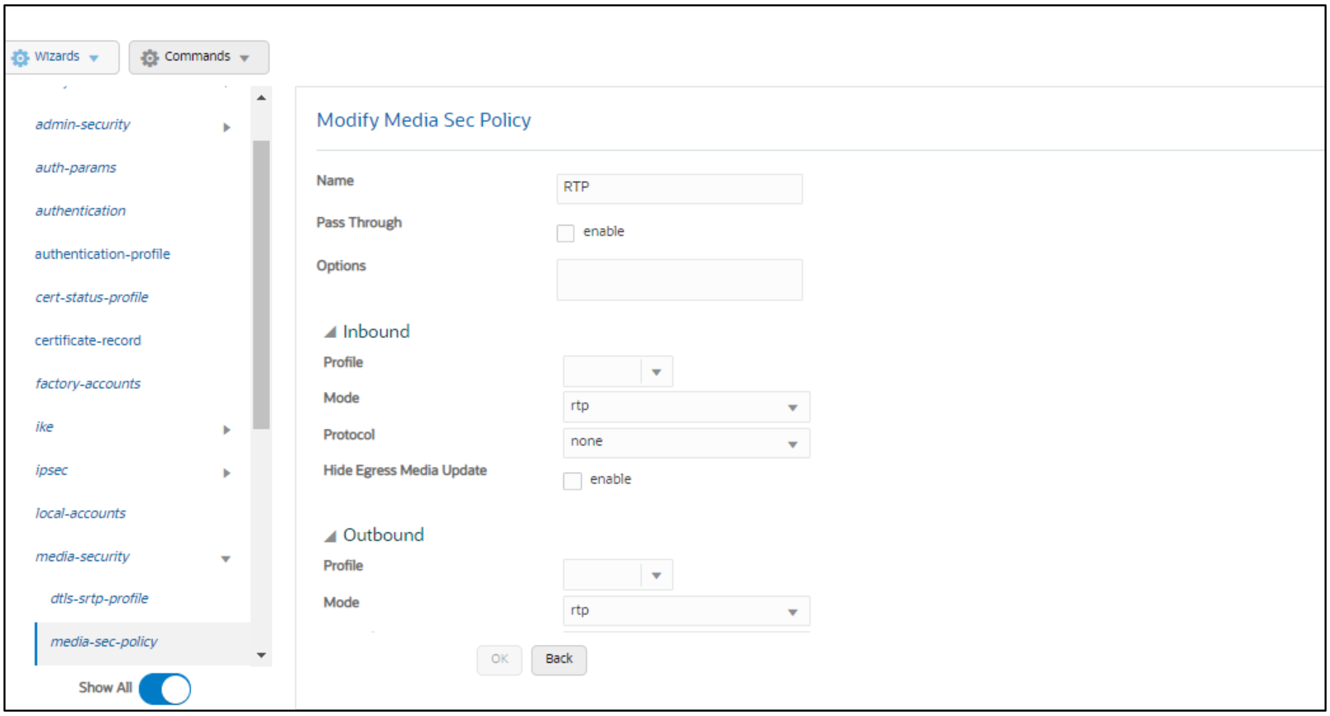
Mode: srtp

Protocol: sdes

Hide Egress Media Update: □ enable

Outbound

Create another Media Sec Policy RTP as shown below.This policy will be applied to the Verizon Ream facing the Verizon Business SIP Trunk.



Modify Media Sec Policy

Name: RTP

Pass Through: □ enable

Options:

Inbound

Profile:

Mode: rtp

Protocol: none

Hide Egress Media Update: □ enable

Outbound

Profile:

Mode: rtp

6.13 IKE/IPSEC Config

The configuration elements required for IKE are not available via the Oracle ESBC GUI and must be configured via ACLI.

Note : Verizon does not necessarily use IPSEC and IKE for Trunks and it could be UDP or TCP.IPSEC configuration is only required if the setup requires the Trunk to communicate over IPSEC.

Note: The examples provided will only display the parameters of each element that have been changed. All others can be left at default values unless required to be changed for your specific purposes:

6.13.1 IKE Config

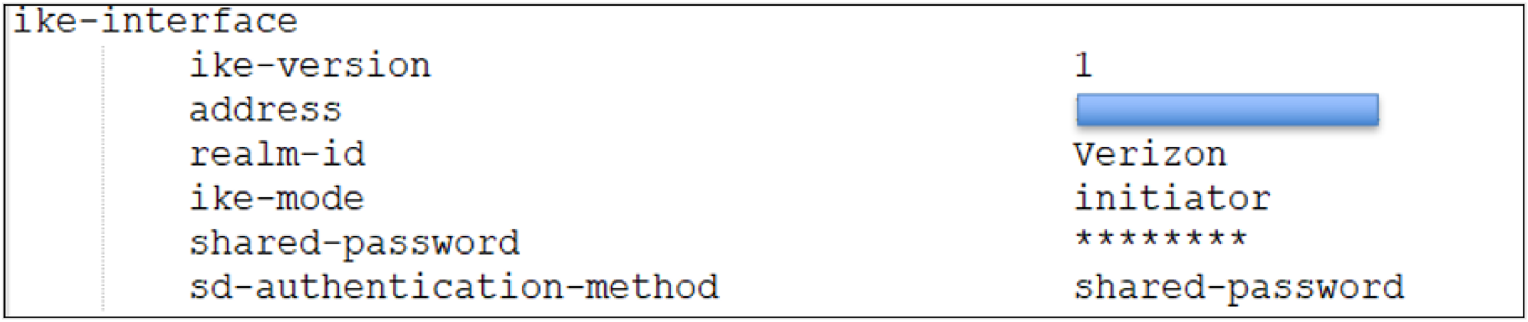
ACLI Path: config t->security->ike->ike-config

Type Select and use the below example to configure the global Ike configuration on the SBC.

```
ike-config
        ike-version                             1
        log-level                               NOTICE
        phase1-dh-mode                          dh-group2
        phase2-exchange-mode                    dh-group2
```

6.13.1.1 Ike Interface

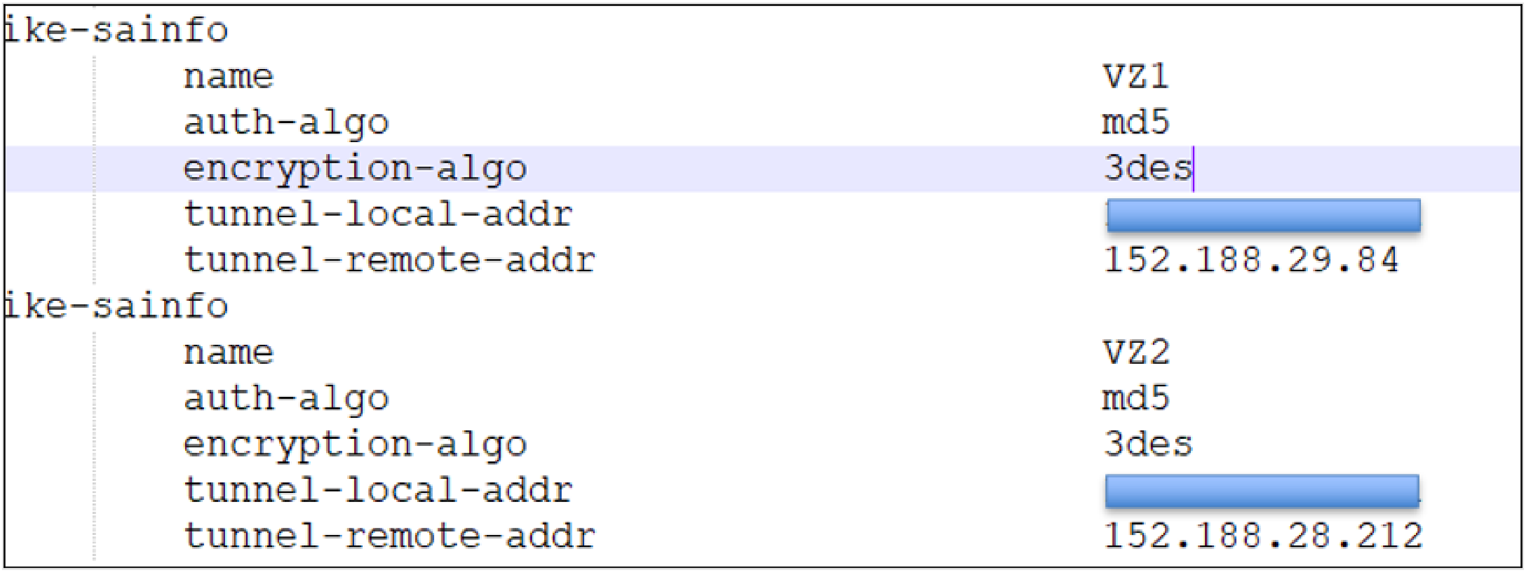
ACLI Path: config t->security->ike->ike-interface



```
ike-interface
        ike-version                              1
        address                                  [redacted]
        realm-id                                 Verizon
        ike-mode                                 initiator
        shared-password                          ********
        sd-authentication-method                 shared-password
```

6.13.1.2 Ike SaInfo

ACLI Path: config t->security->ike->ike-sainfo



```
ike-sainfo
        name                                     VZ1
        auth-algo                                md5
        encryption-algo                          3des
        tunnel-local-addr                        [redacted]
        tunnel-remote-addr                       152.188.29.84
ike-sainfo
        name                                     VZ2
        auth-algo                                md5
        encryption-algo                          3des
        tunnel-local-addr                        [redacted]
        tunnel-remote-addr                       152.188.28.212
```

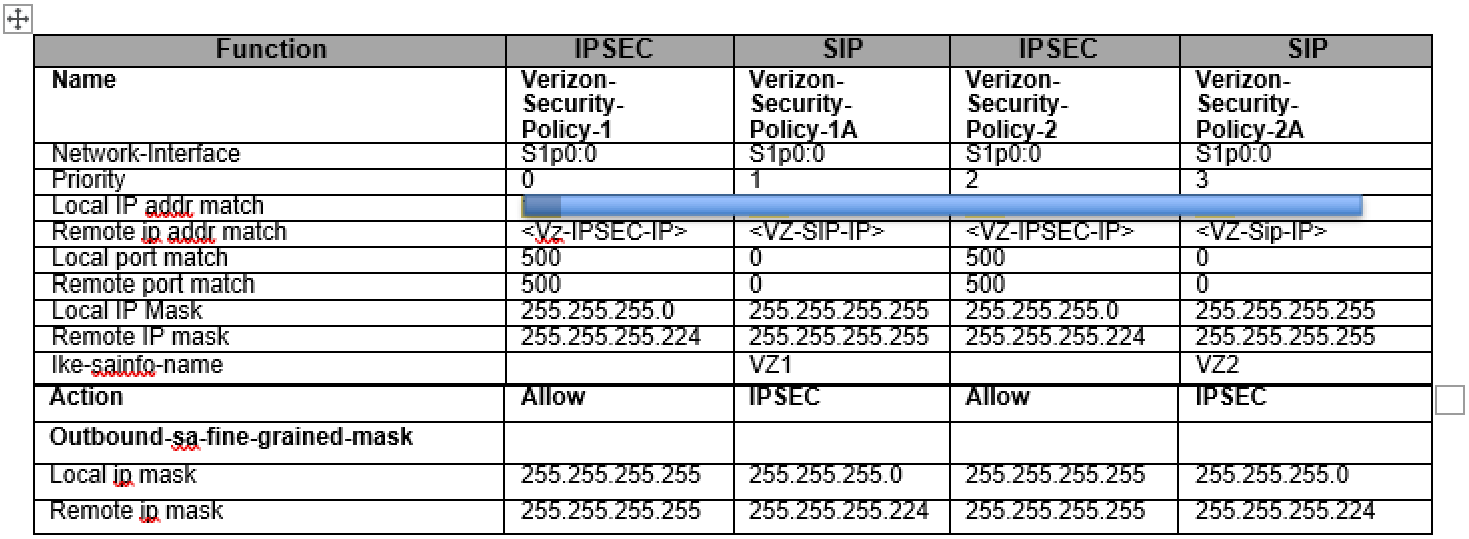
6.13.2 Security Policy

Security Policies are part of the IPSEC configuration on the SBC, and this is available through the GUI.

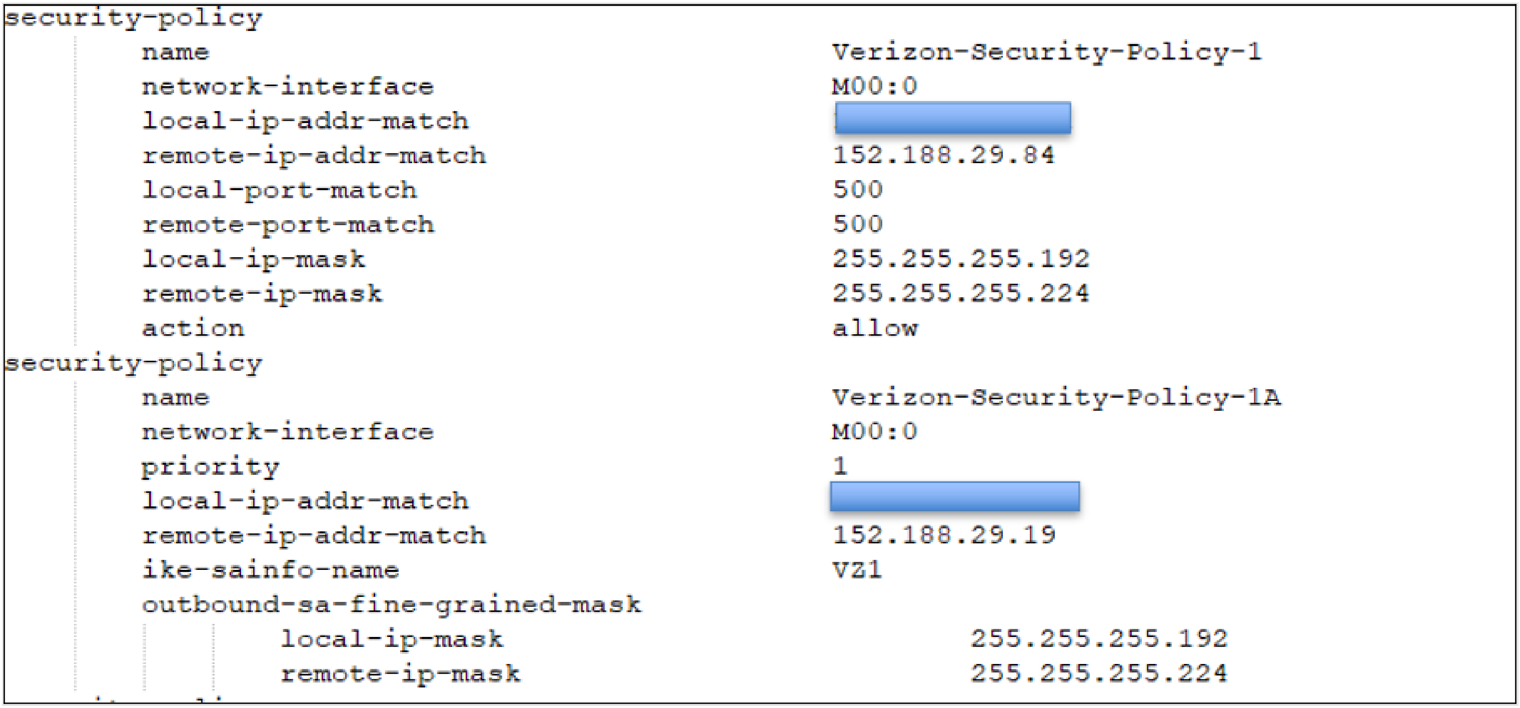
GUI Path: security/ipsec/security policy

ACLI Path: config t->security->ipsec->security-policy

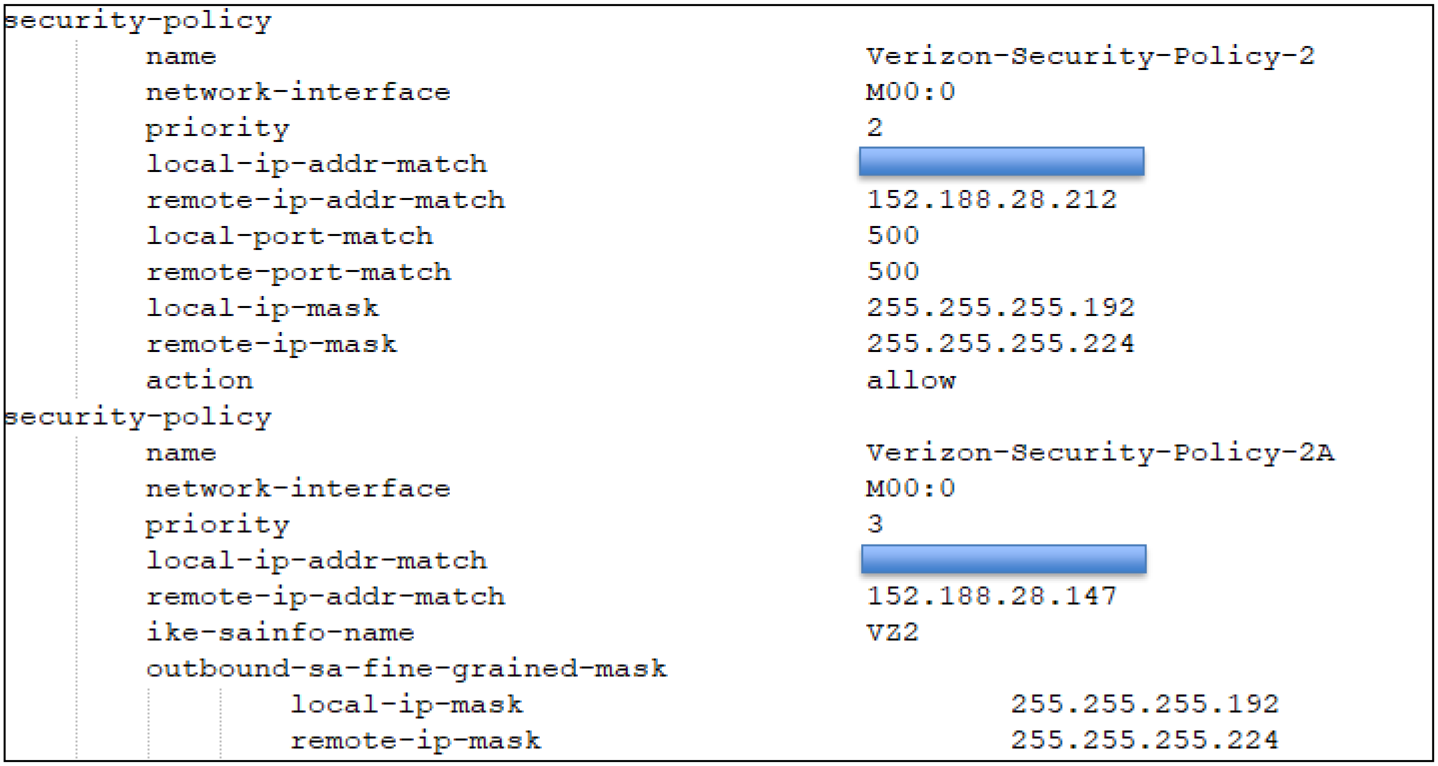
Use the below table as an example to configure security policies on the SBC toward Verizon Business:



Function	IPSEC	SIP	IPSEC	SIP
Name	**Verizon-Security-Policy-1**	**Verizon-Security-Policy-1A**	**Verizon-Security-Policy-2**	**Verizon-Security-Policy-2A**
Network-Interface	S1p0:0	S1p0:0	S1p0:0	S1p0:0
Priority	0	1	2	3
Local IP addr match	[redacted]	[redacted]	[redacted]	[redacted]
Remote ip addr match	<Vz-IPSEC-IP>	<VZ-SIP-IP>	<VZ-IPSEC-IP>	<VZ-Sip-IP>
Local port match	500	0	500	0
Remote port match	500	0	500	0
Local IP Mask	255.255.255.0	255.255.255.255	255.255.255.0	255.255.255.255
Remote IP mask	255.255.255.224	255.255.255.255	255.255.255.224	255.255.255.255
Ike-sainfo-name		VZ1		VZ2
Action	**Allow**	**IPSEC**	**Allow**	**IPSEC**
Outbound-sa-fine-grained-mask				
Local ip mask	255.255.255.255	255.255.255.0	255.255.255.255	255.255.255.0
Remote ip mask	255.255.255.255	255.255.255.224	255.255.255.255	255.255.255.224



```
security-policy
        name                                    Verizon-Security-Policy-1
        network-interface                       M00:0
        local-ip-addr-match                     [redacted]
        remote-ip-addr-match                    152.188.29.84
        local-port-match                        500
        remote-port-match                       500
        local-ip-mask                           255.255.255.192
        remote-ip-mask                          255.255.255.224
        action                                  allow
security-policy
        name                                    Verizon-Security-Policy-1A
        network-interface                       M00:0
        priority                                1
        local-ip-addr-match                     [redacted]
        remote-ip-addr-match                    152.188.29.19
        ike-sainfo-name                         VZ1
        outbound-sa-fine-grained-mask
                local-ip-mask                           255.255.255.192
                remote-ip-mask                          255.255.255.224
```



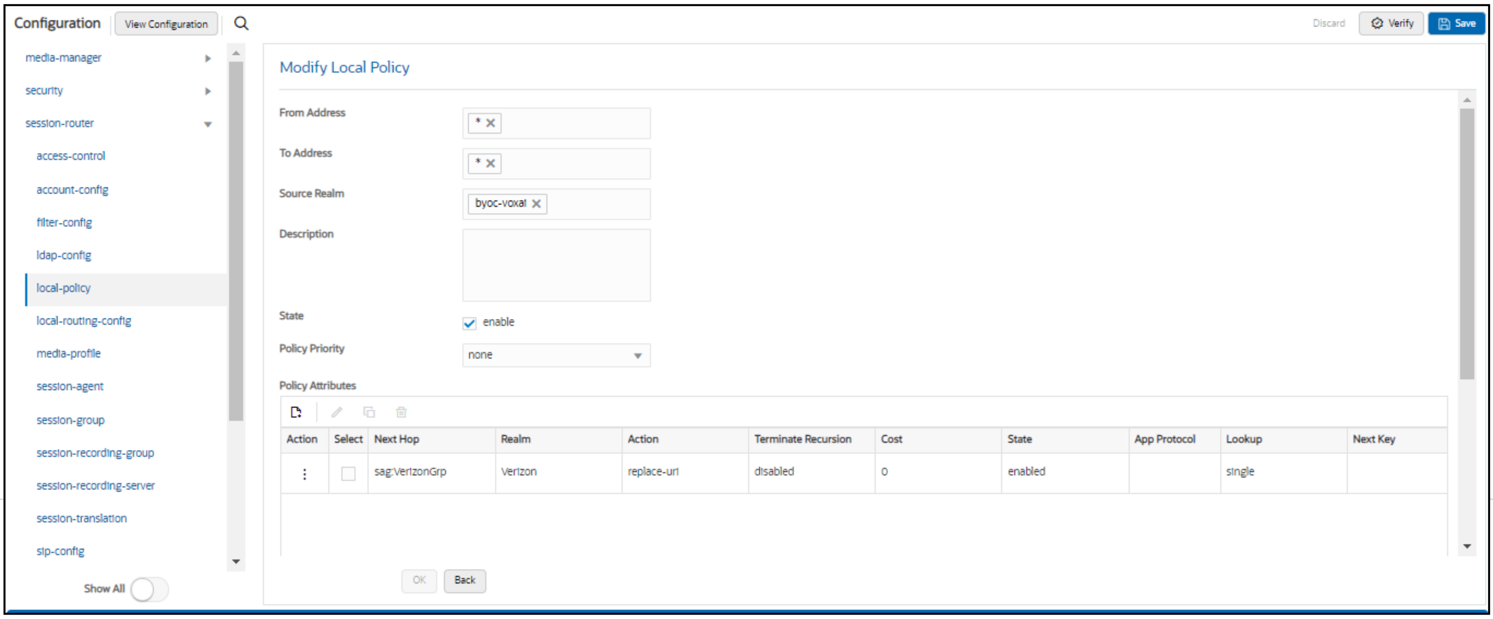
```
security-policy
        name                                    Verizon-Security-Policy-2
        network-interface                       M00:0
        priority                                2
        local-ip-addr-match                     [redacted]
        remote-ip-addr-match                    152.188.28.212
        local-port-match                        500
        remote-port-match                       500
        local-ip-mask                           255.255.255.192
        remote-ip-mask                          255.255.255.224
        action                                  allow
security-policy
        name                                    Verizon-Security-Policy-2A
        network-interface                       M00:0
        priority                                3
        local-ip-addr-match                     [redacted]
        remote-ip-addr-match                    152.188.28.147
        ike-sainfo-name                         VZ2
        outbound-sa-fine-grained-mask
                local-ip-mask                           255.255.255.192
                remote-ip-mask                          255.255.255.224
```

6.14. 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.
ACLI Path: config t->session-router->local-policy

Following local-policy routes the calls from Genesys PureCloud to Verizon Business IP Trunk which are then terminated towards PSTN.
Following local-policy routes the calls from Verizon Business Trunk which are then routed to Genesys PureCloud from the SBC.

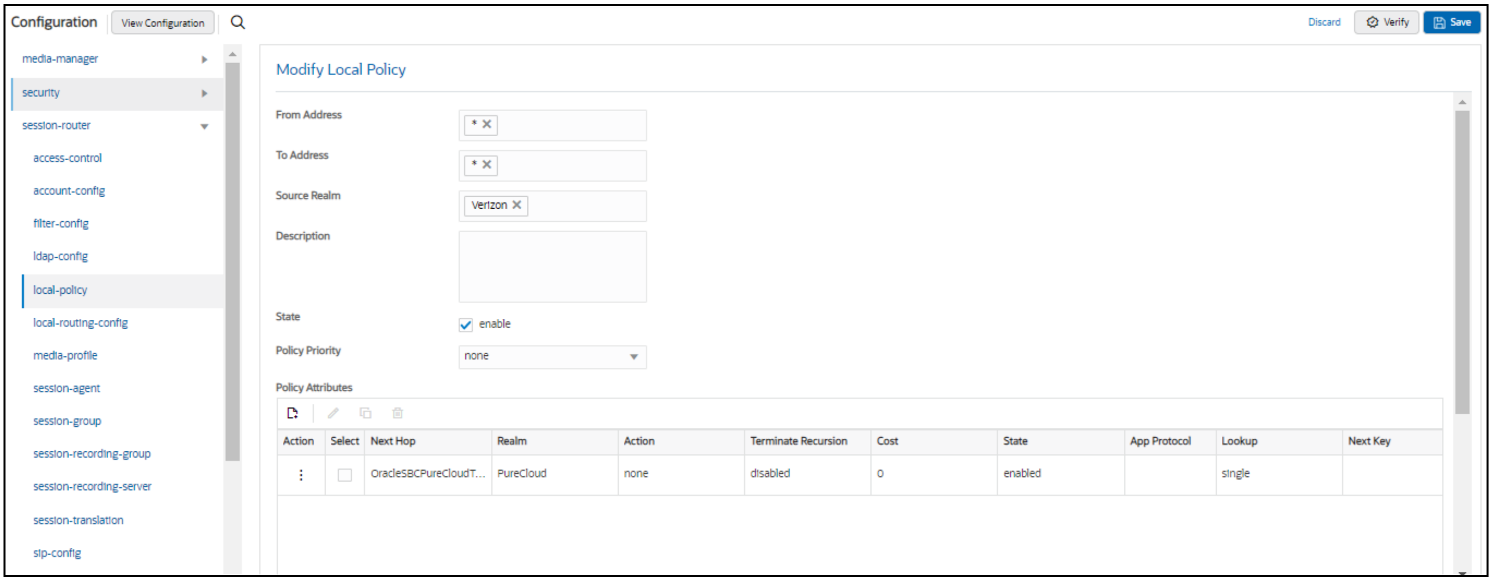


Modify Local Policy

From Address	*
To Address	*
Source Realm	byoc-voxai
Description	
State	☑ enable
Policy Priority	none

Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
⋮	□	sag:VerizonGrp	Verizon	replace-uri	disabled	0	enabled		single	



Modify Local Policy

From Address: *

To Address: *

Source Realm: Verizon

Description:

State: ☑ enable

Policy Priority: none

Policy Attributes

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

6.15. Codec Policies

Codec policies are sets of rules that specify the manipulations to be performed on SDP offers allowing the OCSBC the ability to add, strip, and reorder codecs for SIP sessions

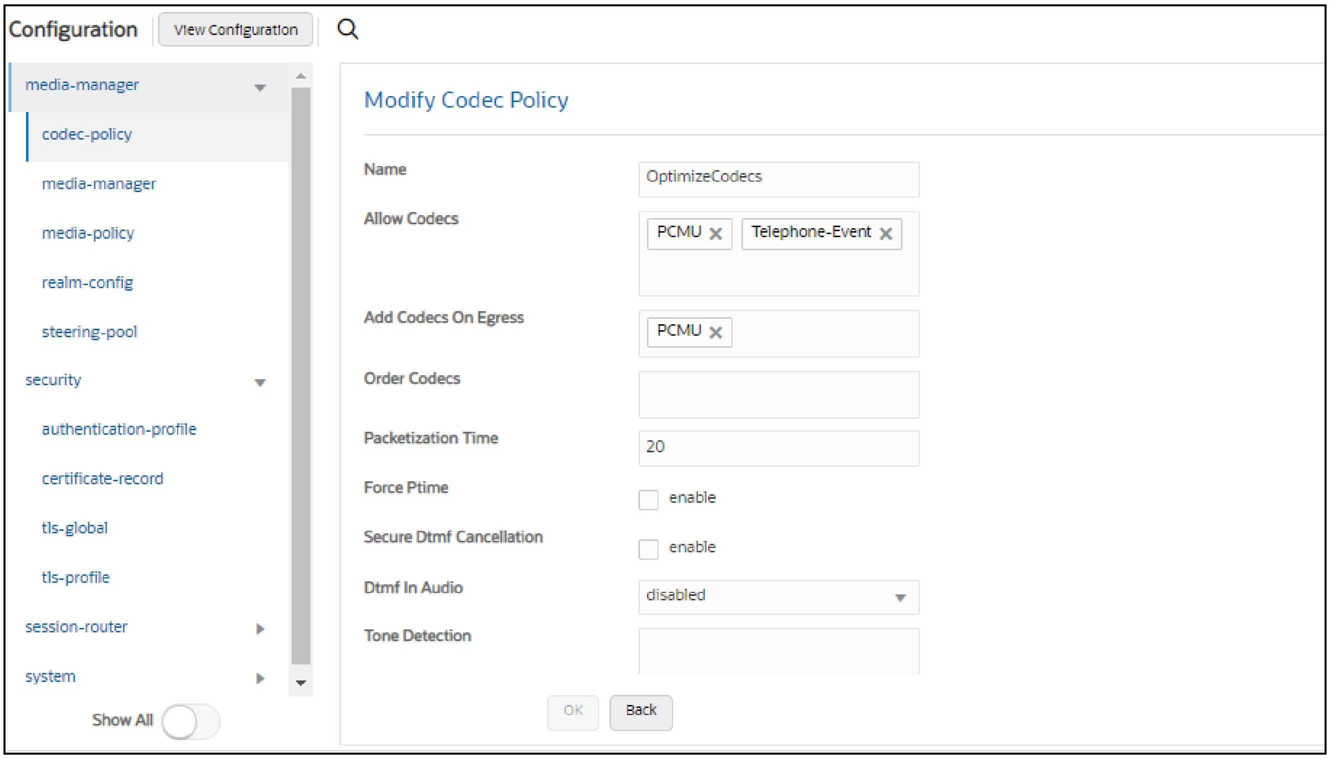
Note: This is an optional configuration. Only configure codec policies if deemed necessary in your environment

GUI Path: media-manager/codec-policy

ACLI Path: config t->media-manager->codec-policy

Some SIP trunks may have issues with codec being offered by Genesys PureCloud, specifically Verizon requested the SBC try to offer only one codec when possible. For this reason, we have created a codec policy “OptimizeCodecs” for the Verizon SIP trunk to remove the codecs that are not required or supported.

- Click Add, and use the examples below to configure



Modify Codec Policy

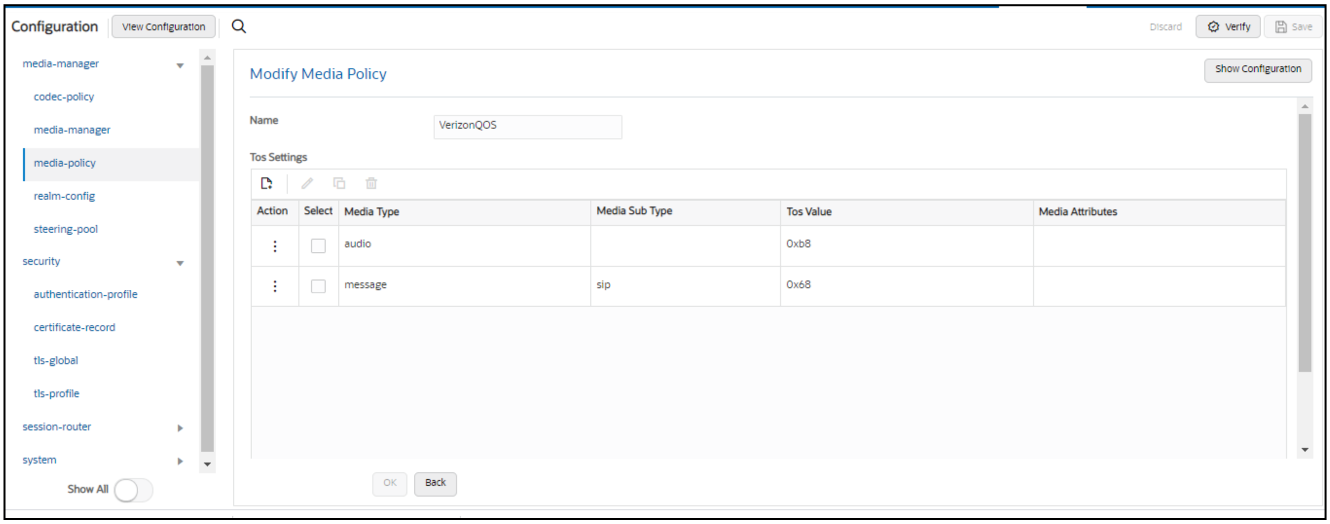
Name	OptimizeCodecs
Allow Codecs	PCMU ✕ Telephone-Event ✕
Add Codecs On Egress	PCMU ✕
Order Codecs	
Packetization Time	20
Force Ptime	□ enable
Secure Dtmf Cancellation	□ enable
Dtmf In Audio	disabled
Tone Detection	

6.16 QOS Marking

QoS marking allows you to apply a set of TOS/DiffServ mechanisms that enable you to provide better service for selected networks

GUI Path: media manager->media policy

ACLI Path: config t->media-manager->media-policy



Modify Media Policy

Name: VerizonQOS

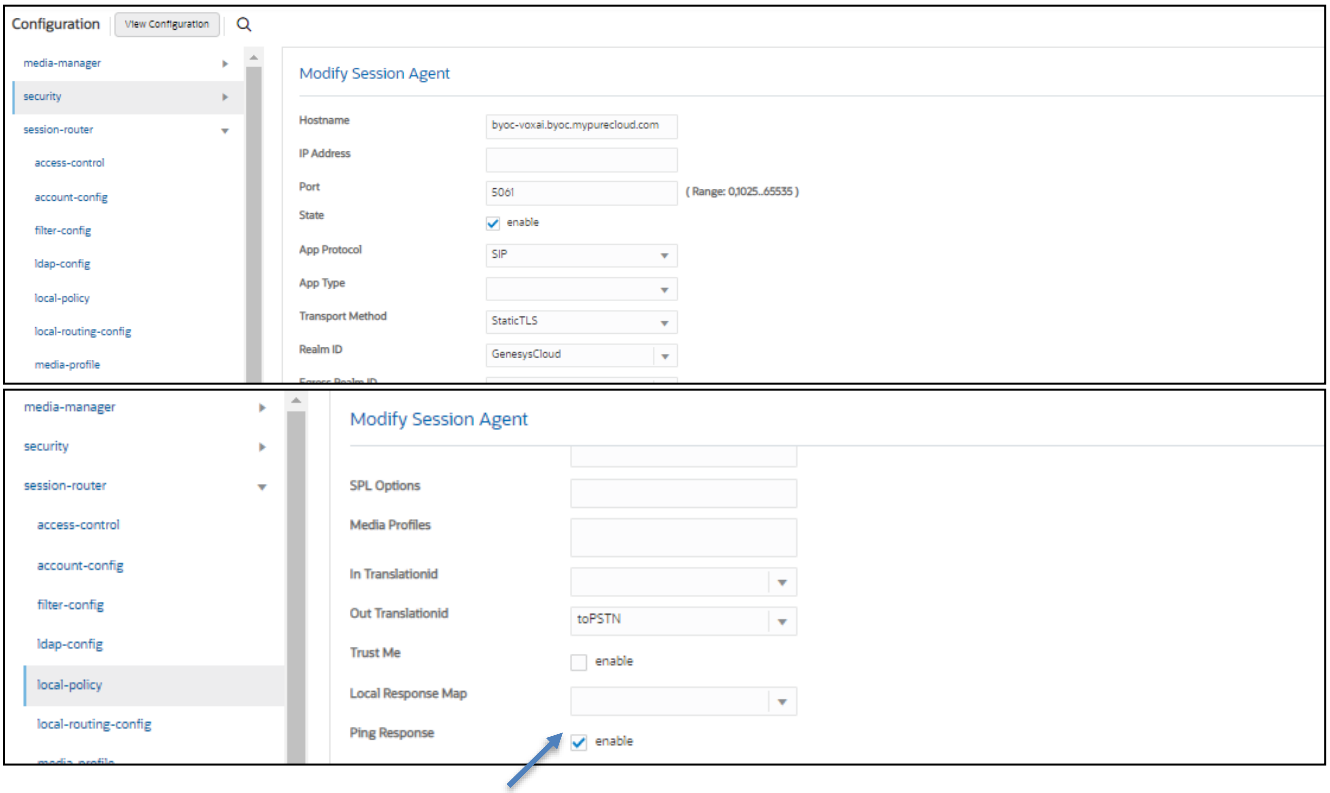
Tos Settings

Action	Select	Media Type	Media Sub Type	Tos Value	Media Attributes
⋮	□	audio		0xb8	
⋮	□	message	sip	0x68	

6.17. Enable Ping-response

The option is found under the **Session agent** configuration element and will be enabled on all session agents configured for Verizon Trunk and Genesys PureCloud .

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



Modify Session Agent

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

Modify Session Agent

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

6.18. Access Control

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

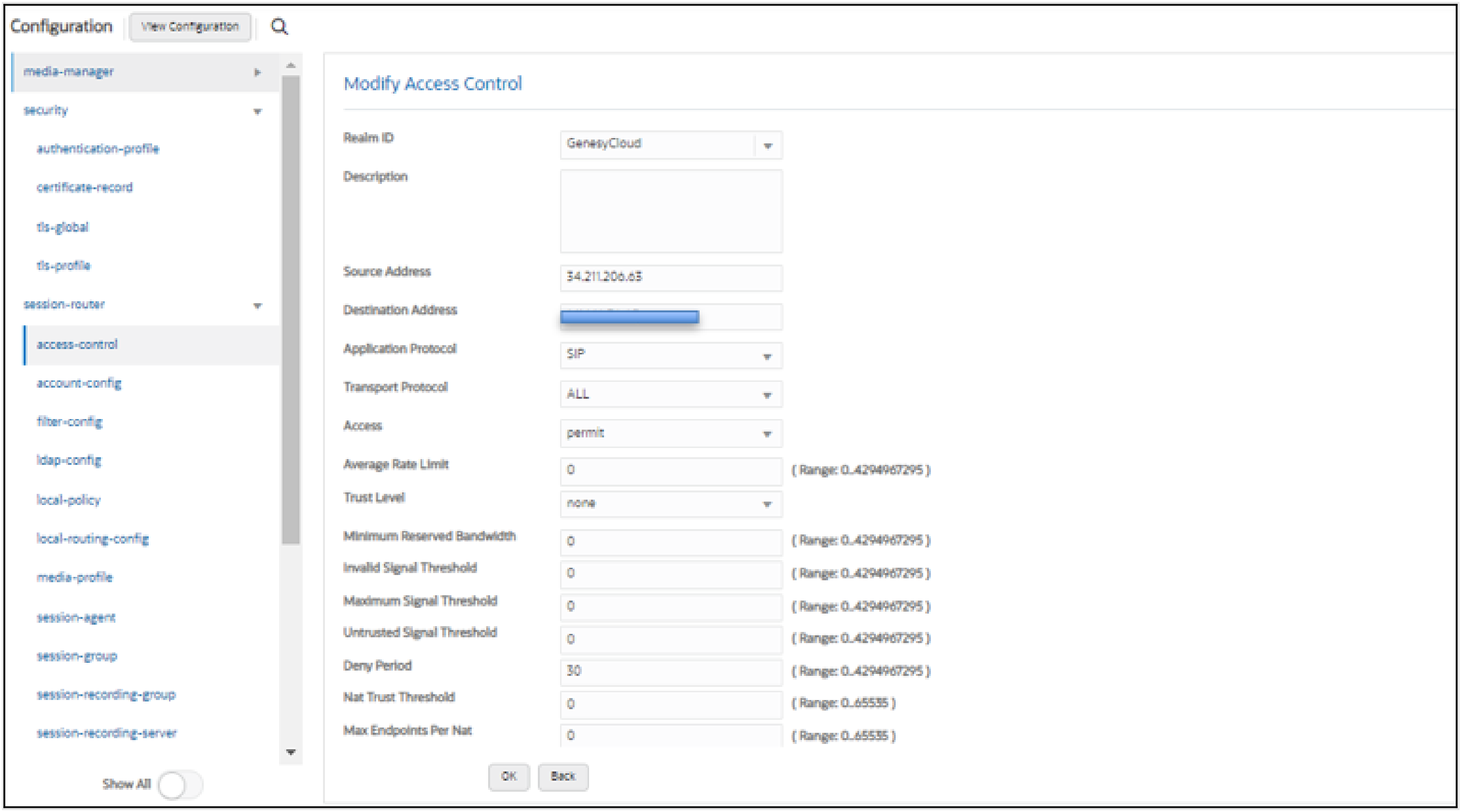
GUI Path: session-router/access-control

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

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

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

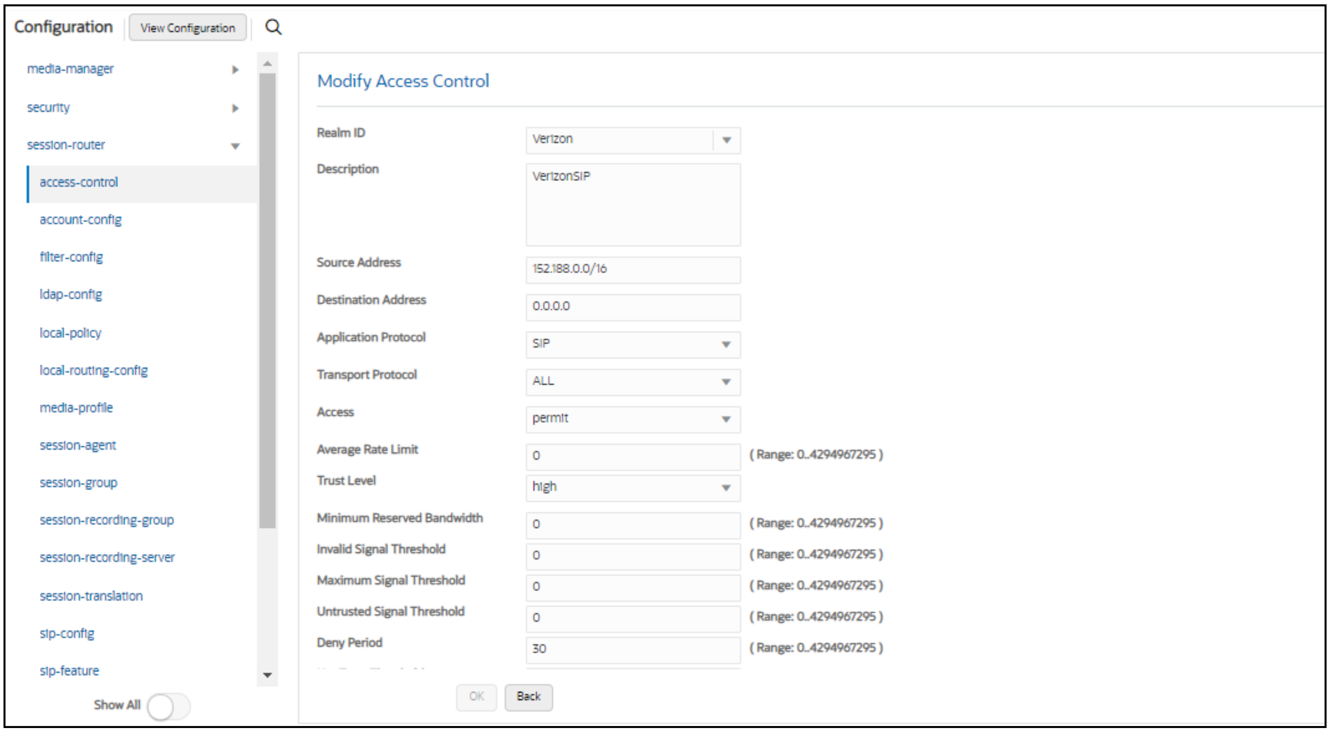
Configure access-control for each IP PureCloud IP Address as shown in the below example.



Modify Access Control

Realm ID	GenesysCloud	
Description		
Source Address	34.211.206.63	
Destination Address	[redacted]	
Application Protocol	SIP	
Transport Protocol	ALL	
Access	permit	
Average Rate Limit	0	(Range: 0..4294967295)
Trust Level	none	
Minimum Reserved Bandwidth	0	(Range: 0..4294967295)
Invalid Signal Threshold	0	(Range: 0..4294967295)
Maximum Signal Threshold	0	(Range: 0..4294967295)
Untrusted Signal Threshold	0	(Range: 0..4294967295)
Deny Period	30	(Range: 0..4294967295)
Nat Trust Threshold	0	(Range: 0..65535)
Max Endpoints Per Nat	0	(Range: 0..65535)

Similarly create ACL entries for each Verizon Trunk as shown in the below example.



Modify Access Control

Realm ID	Verizon	
Description	VerizonSIP	
Source Address	152.188.0.0/16	
Destination Address	0.0.0.0	
Application Protocol	SIP	
Transport Protocol	ALL	
Access	permit	
Average Rate Limit	0	(Range: 0..4294967295)
Trust Level	high	
Minimum Reserved Bandwidth	0	(Range: 0..4294967295)
Invalid Signal Threshold	0	(Range: 0..4294967295)
Maximum Signal Threshold	0	(Range: 0..4294967295)
Untrusted Signal Threshold	0	(Range: 0..4294967295)
Deny Period	30	(Range: 0..4294967295)

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

6.19. 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

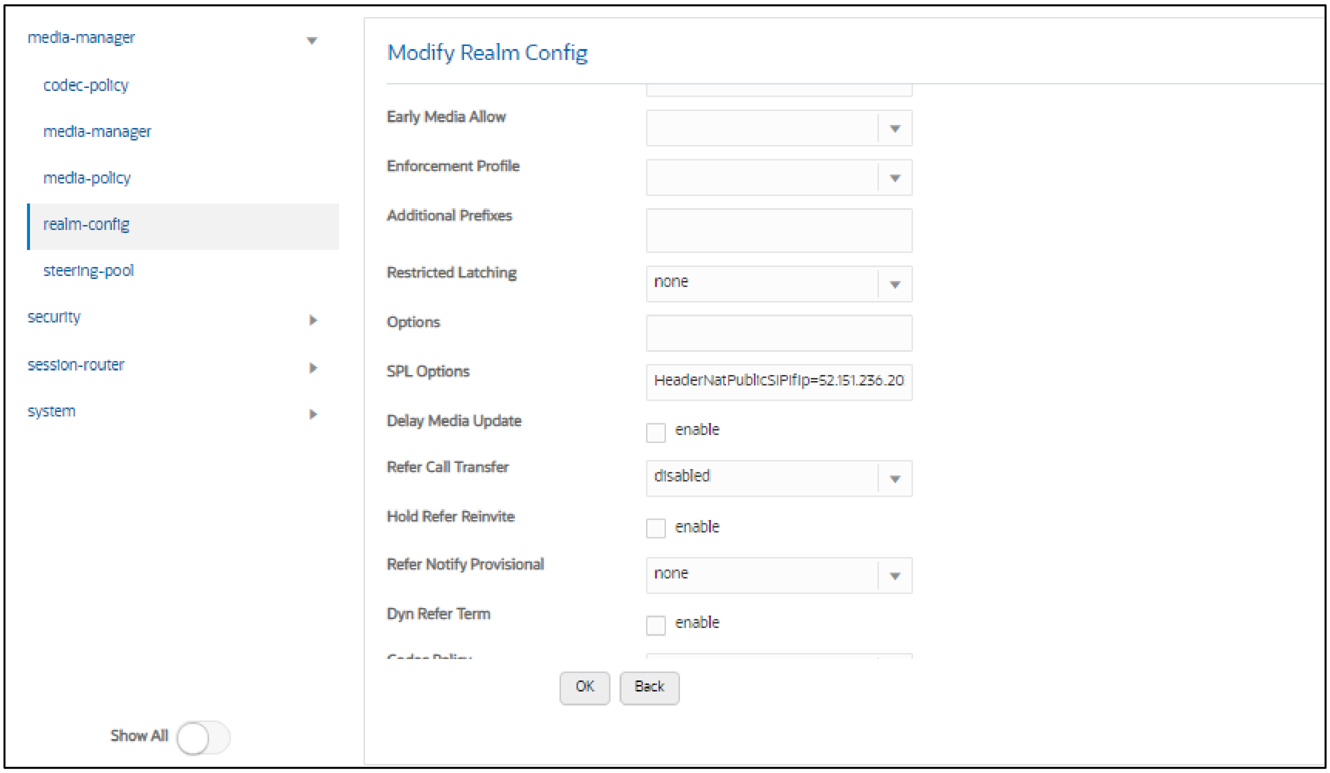
Here is an example configuration with SBC Behind NAT SPL config. The SPL is applied to the PureCloud side SIP interface.

To configure SBC Behind NAT SPL Plug in,

Navigate to session-router->SIP-interface->spl-options and input the following value, save, and activate.

HeaderNatPublicSIPIfIp=52.151.236.203,HeaderNatPrivateSIPIfIp=10.0.4.4

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



Modify Realm Config

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

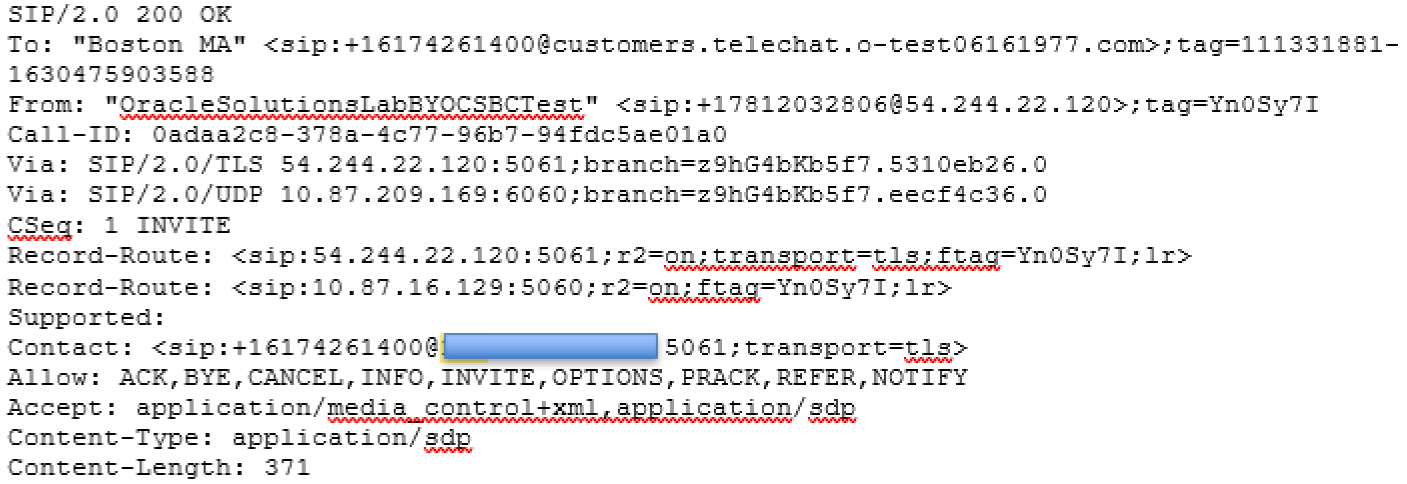
This configuration would be applied to each SIP Interface in the ORACLE SBC configuration that was deployed behind a Nat Device.

7. Syntax Examples

Picture 1 -Sample SIP INVITE from PureCloud to Oracle SBC

```
2021-09-01 02:00:43.658
INVITE sip:+16174261400@customers.telechat.o-test06161977.com:5061;transport=tls SIP/2.0
Record-Route: <sip:54.244.22.120:5061;r2=on;transport=tls;ftag=Yn0Sy7I;lr>
Record-Route: <sip:10.87.16.129:5060;r2=on;ftag=Yn0Sy7I;lr>
To: "Boston MA" <sip:+16174261400@customers.telechat.o-test06161977.com>
From: "OracleSolutionsLabBYOCSBCTest" <sip:+17812032806@54.244.22.120>;tag=Yn0Sy7I
Call-ID: 0adaa2c8-378a-4c77-96b7-94fdc5ae01a0
Via: SIP/2.0/TLS 54.244.22.120:5061;branch=z9hG4bKb5f7.5310eb26.0
Via: SIP/2.0/UDP 10.87.209.169:6060;branch=z9hG4bKb5f7.eecf4c36.0
CSeq: 1 INVITE
Max-Forwards: 67
Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, INFO
Supported: norefersub, timer
Accept: application/sdp, application/dtmf-relay
Contact: <sip:+17812032806@10.87.209.169:6060;did=42f.a8a5bde5>
x-inin-cnv: 238493bd-87d6-443e-a548-69b57deb5edd
x-pcv-domain: customers.telechat.o-test06161977.com
Content-Type: application/sdp
User-Agent: GENESYS-SIPSERVICE/1.0.0.4186
Content-Length: 357
```

Picture 2 – Sample 200 OK response to PureCloud .

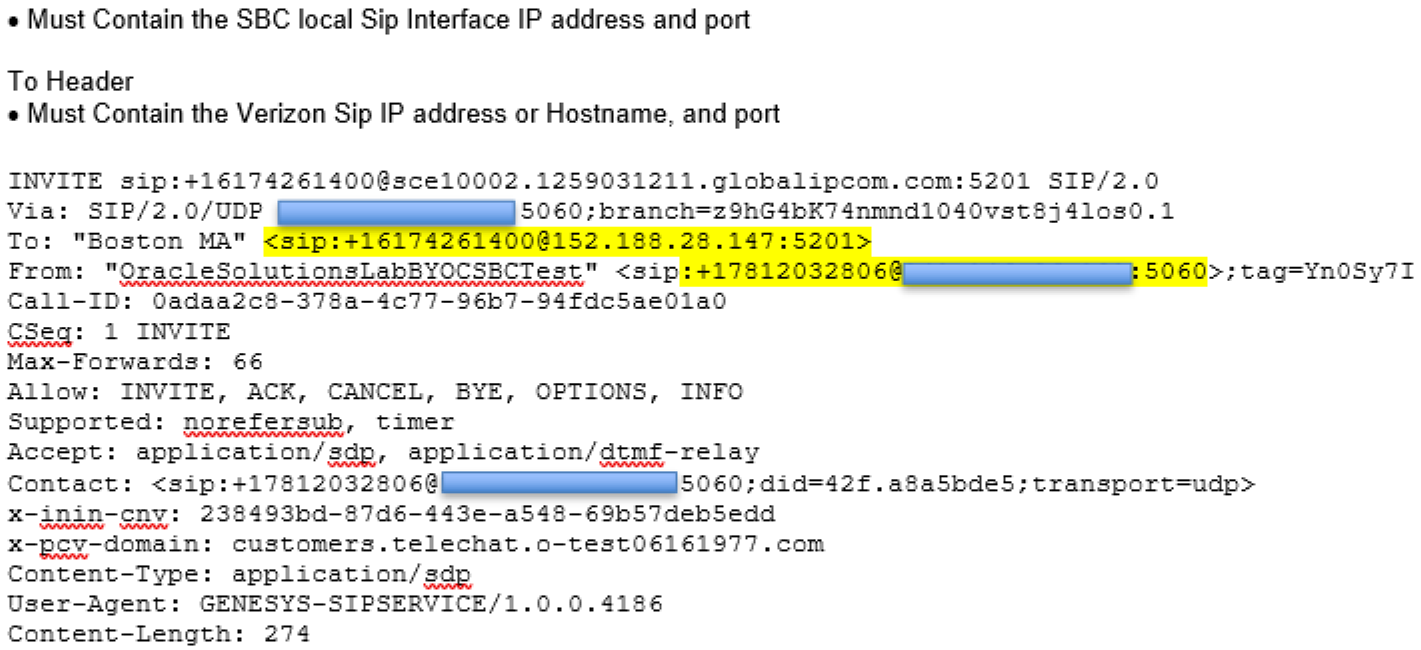


```
SIP/2.0 200 OK
To: "Boston MA" <sip:+16174261400@customers.telechat.o-test06161977.com>;tag=111331881-
1630475903588
From: "OracleSolutionsLabBYOCSBCTest" <sip:+17812032806@54.244.22.120>;tag=Yn0Sy7I
Call-ID: 0adaa2c8-378a-4c77-96b7-94fdc5ae01a0
Via: SIP/2.0/TLS 54.244.22.120:5061;branch=z9hG4bKb5f7.5310eb26.0
Via: SIP/2.0/UDP 10.87.209.169:6060;branch=z9hG4bKb5f7.eecf4c36.0
CSeq: 1 INVITE
Record-Route: <sip:54.244.22.120:5061;r2=on;transport=tls;ftag=Yn0Sy7I;lr>
Record-Route: <sip:10.87.16.129:5060;r2=on;ftag=Yn0Sy7I;lr>
Supported:
Contact: <sip:+16174261400@[redacted]5061;transport=tls>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Accept: application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 371
```

Picture 3- Sample SIP INVITE from Oracle SBC to VZB Trunk

From Header:

- Must contain a Verizon DID that is associated with the trunk group



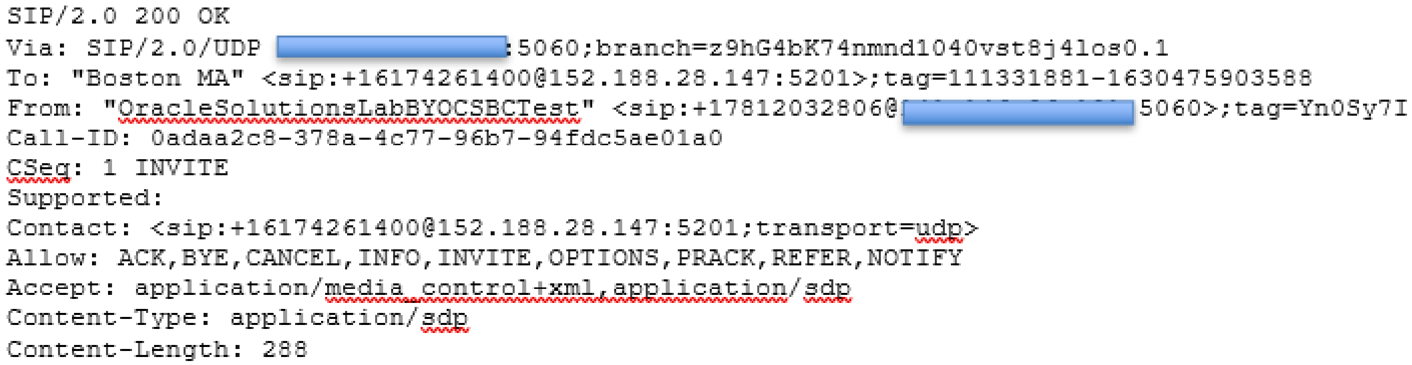
- Must Contain the SBC local Sip Interface IP address and port

To Header

- Must Contain the Verizon Sip IP address or Hostname, and port

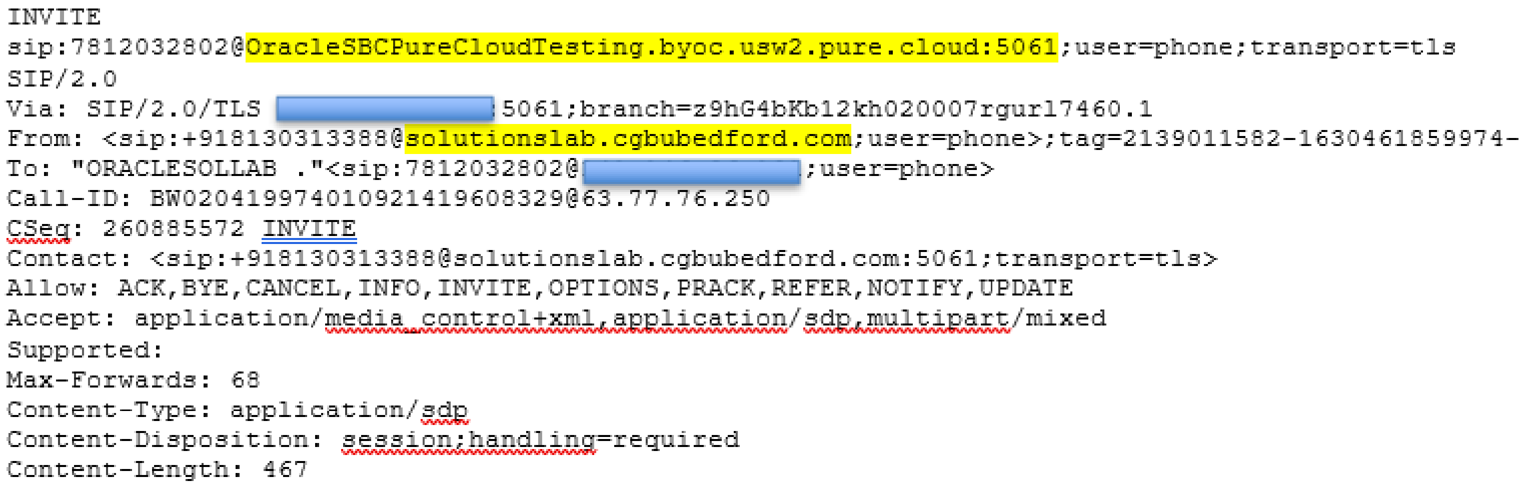
```
INVITE sip:+16174261400@sce10002.1259031211.globalipcom.com:5201 SIP/2.0
Via: SIP/2.0/UDP [redacted] 5060;branch=z9hG4bK74nmnd1040vst8j4los0.1
To: "Boston MA" <sip:+16174261400@152.188.28.147:5201>
From: "OracleSolutionsLabBYOCSBCTest" <sip:+17812032806@[redacted]:5060>;tag=Yn0Sy7I
Call-ID: 0adaa2c8-378a-4c77-96b7-94fdc5ae01a0
CSeq: 1 INVITE
Max-Forwards: 66
Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, INFO
Supported: norefersub, timer
Accept: application/sdp, application/dtmf-relay
Contact: <sip:+17812032806@[redacted]5060;did=42f.a8a5bde5;transport=udp>
x-inin-cnv: 238493bd-87d6-443e-a548-69b57deb5edd
x-pcv-domain: customers.telechat.o-test06161977.com
Content-Type: application/sdp
User-Agent: GENESYS-SIPSERVICE/1.0.0.4186
Content-Length: 274
```

Picture 4 – Sample 200 OK from Verizon Trunk to Oracle SBC



```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [redacted]:5060;branch=z9hG4bK74nmnd1040vst8j4los0.1
To: "Boston MA" <sip:+16174261400@152.188.28.147:5201>;tag=111331881-1630475903588
From: "OracleSolutionsLabBYOCSBCTest" <sip:+17812032806@[redacted]5060>;tag=Yn0Sy7I
Call-ID: 0adaa2c8-378a-4c77-96b7-94fdc5ae01a0
CSeq: 1 INVITE
Supported:
Contact: <sip:+16174261400@152.188.28.147:5201;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Accept: application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Length: 288
```

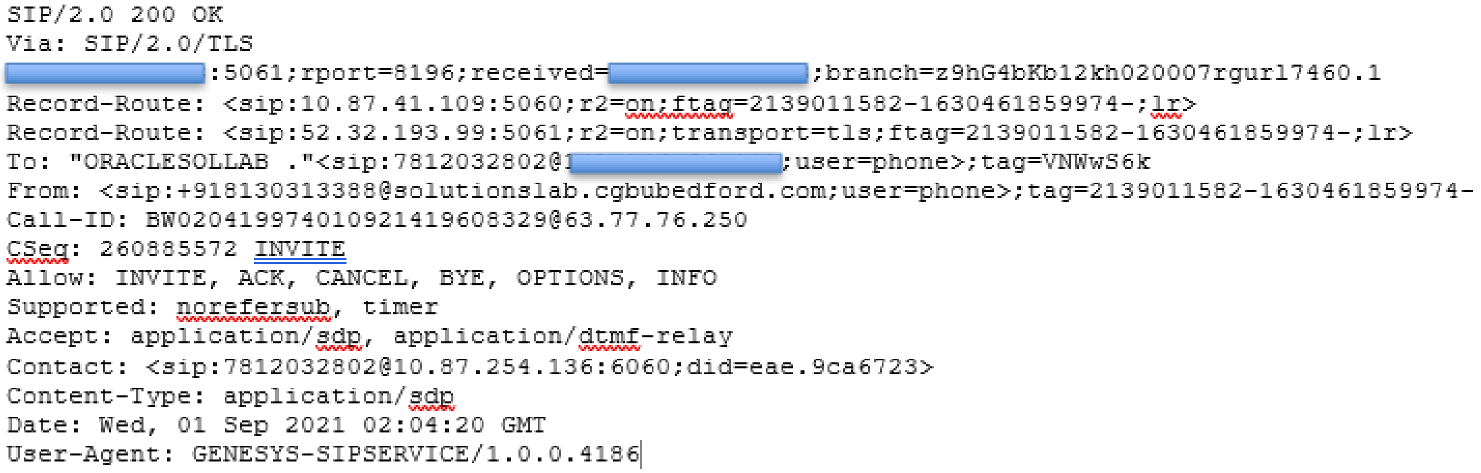
Picture 5- Sample SIP INVITE from Oracle SBC to PureCloud



```
INVITE
sip:7812032802@OracleSBCPureCloudTesting.byoc.usw2.pure.cloud:5061;user=phone;transport=tls
SIP/2.0
Via: SIP/2.0/TLS [redacted]5061;branch=z9hG4bKb12kh020007rgurl7460.1
From: <sip:+918130313388@solutionslab.cgbubedford.com;user=phone>;tag=2139011582-1630461859974-
To: "ORACLESOLLAB ."<sip:7812032802@[redacted];user=phone>
Call-ID: BW02041997401092141960832 9@63.77.76.250
CSeq: 260885572 INVITE
Contact: <sip:+918130313388@solutionslab.cgbubedford.com:5061;transport=tls>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: application/media_control+xml,application/sdp,multipart/mixed
Supported:
Max-Forwards: 68
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 467
```

```
X-MS-SBC: Oracle/NN4600/8.4.0p5A
```

Picture 6- Sample 200 OK from PureCloud to Oracle SBC



```
SIP/2.0 200 OK
Via: SIP/2.0/TLS
[redacted]:5061;rport=8196;received=[redacted];branch=z9hG4bKb12kh020007rgurl7460.1
Record-Route: <sip:10.87.41.109:5060;r2=on;ftag=2139011582-1630461859974-;lr>
Record-Route: <sip:52.32.193.99:5061;r2=on;transport=tls;ftag=2139011582-1630461859974-;lr>
To: "ORACLESOLLAB ."<sip:7812032802@[redacted];user=phone>;tag=VNWwS6k
From: <sip:+918130313388@solutionslab.cgbubedford.com;user=phone>;tag=2139011582-1630461859974-
Call-ID: BW020419974010921419608329@63.77.76.250
CSeq: 260885572 INVITE
Allow: INVITE, ACK, CANCEL, BYE, OPTIONS, INFO
Supported: norefersub, timer
Accept: application/sdp, application/dtmf-relay
Contact: <sip:7812032802@10.87.254.136:6060;did=eae.9ca6723>
Content-Type: application/sdp
Date: Wed, 01 Sep 2021 02:04:20 GMT
User-Agent: GENESYS-SIPSERVICE/1.0.0.4186
```

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 Verizon Retails IP Trunk on the other Side for Carrier Connectivity.

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

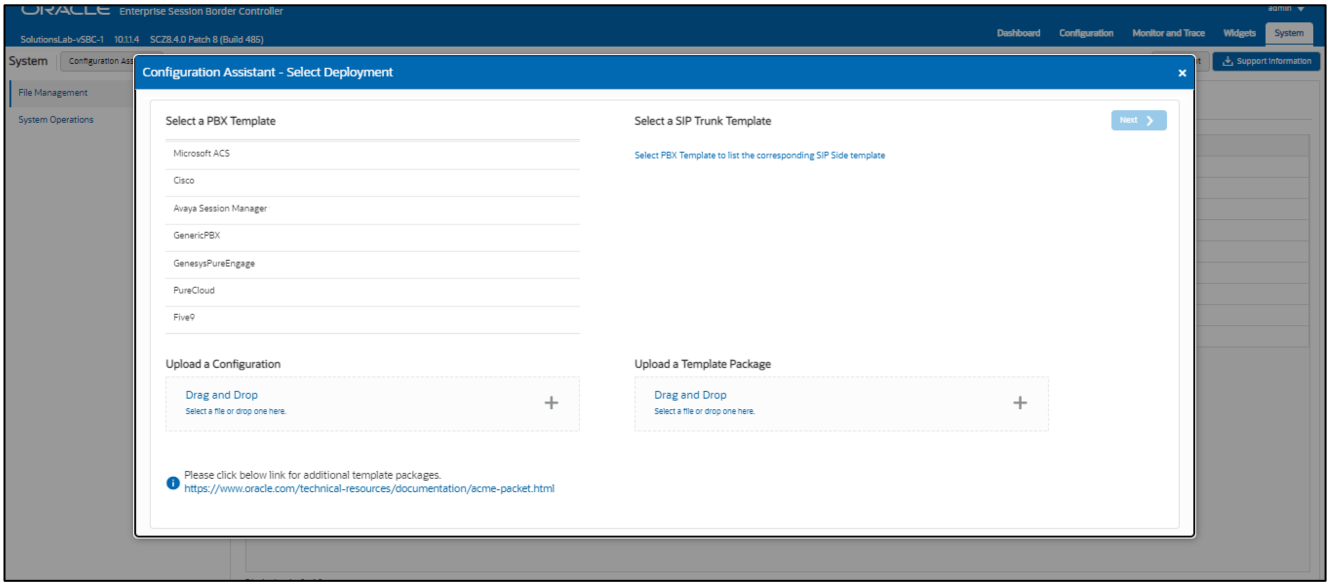
The Oracle SBC WebGui can be accessed by entering the following in your web browser.
http(s)://<SBC Management IP>.

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:

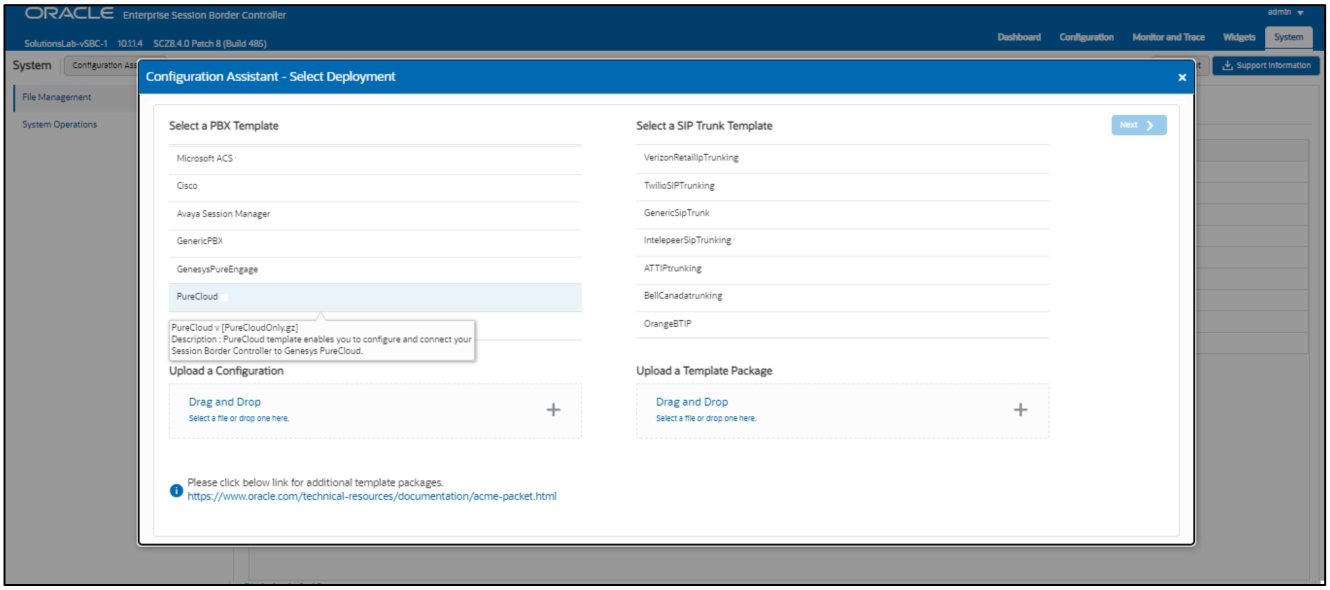


Select PBX Template to list the corresponding SIP Side template

Select a file or drop one here.

Please click below link for additional template packages.
https://www.oracle.com/technical-resources/documentation/acme-packet.html

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

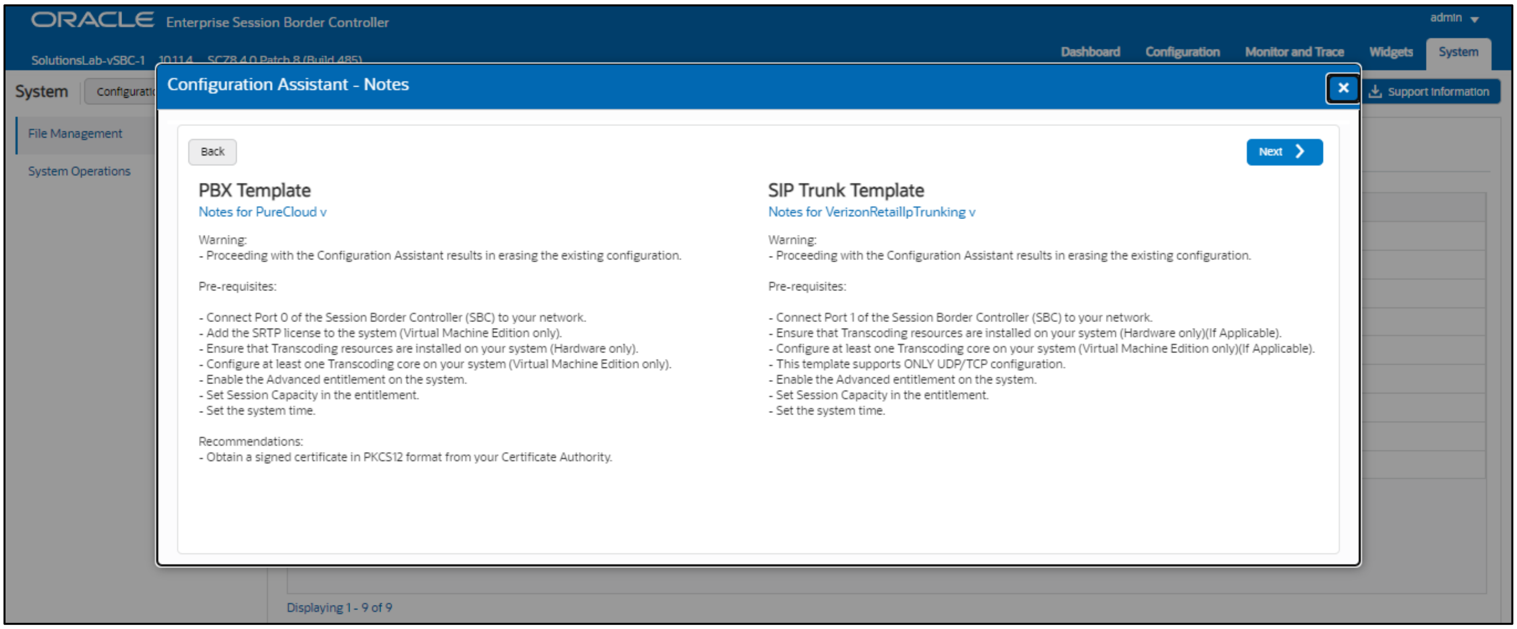


PureCloud v [PureCloudOnly.gz]
Description : PureCloud template enables you to configure and connect your Session Border Controller to Genesys PureCloud.

Select a file or drop one here.

Please click below link for additional template packages.
https://www.oracle.com/technical-resources/documentation/acme-packet.html

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



Configuration Assistant - Notes

PBX Template
Notes for PureCloud v

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

Pre-requisites:

- Connect Port 0 of the Session Border Controller (SBC) to your network.
- Add the SRTP license to the system (Virtual Machine Edition only).
- Ensure that Transcoding resources are installed on your system (Hardware only).
- Configure at least one Transcoding core on your system (Virtual Machine Edition only).
- Enable the Advanced entitlement on the system.
- Set Session Capacity in the entitlement.
- Set the system time.

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

SIP Trunk Template
Notes for VerizonRetailIpTrunking v

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

Pre-requisites:

- Connect Port 1 of the Session Border Controller (SBC) to your network.
- Ensure that Transcoding resources are installed on your system (Hardware only)(If Applicable).
- Configure at least one Transcoding core on your system (Virtual Machine Edition only)(If Applicable).
- This template supports ONLY UDP/TCP configuration.
- Enable the Advanced entitlement on the system.
- Set Session Capacity in the entitlement.
- Set the system time.

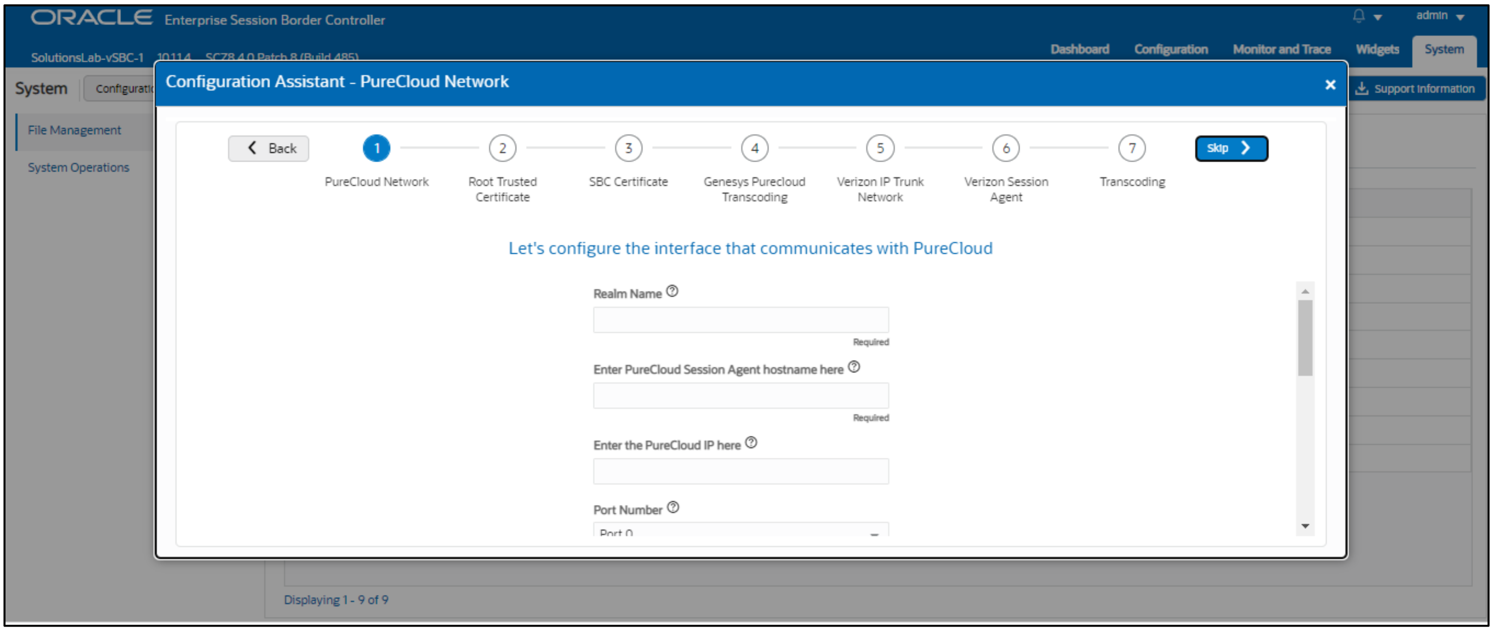
Clicking “Next” on the Notes page triggers the configuration assistant to do a system check. This ensures that all of the system requirements for the platform and sip trunk you have selected have been met before proceeding to configuration pages. If they have not been met, you will be greeted by a page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

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

Page 1- PureCloud Network

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

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



Configuration Assistant - PureCloud Network

Let's configure the interface that communicates with PureCloud

Realm Name

Required

Enter PureCloud Session Agent hostname here

Required

Enter the PureCloud IP here

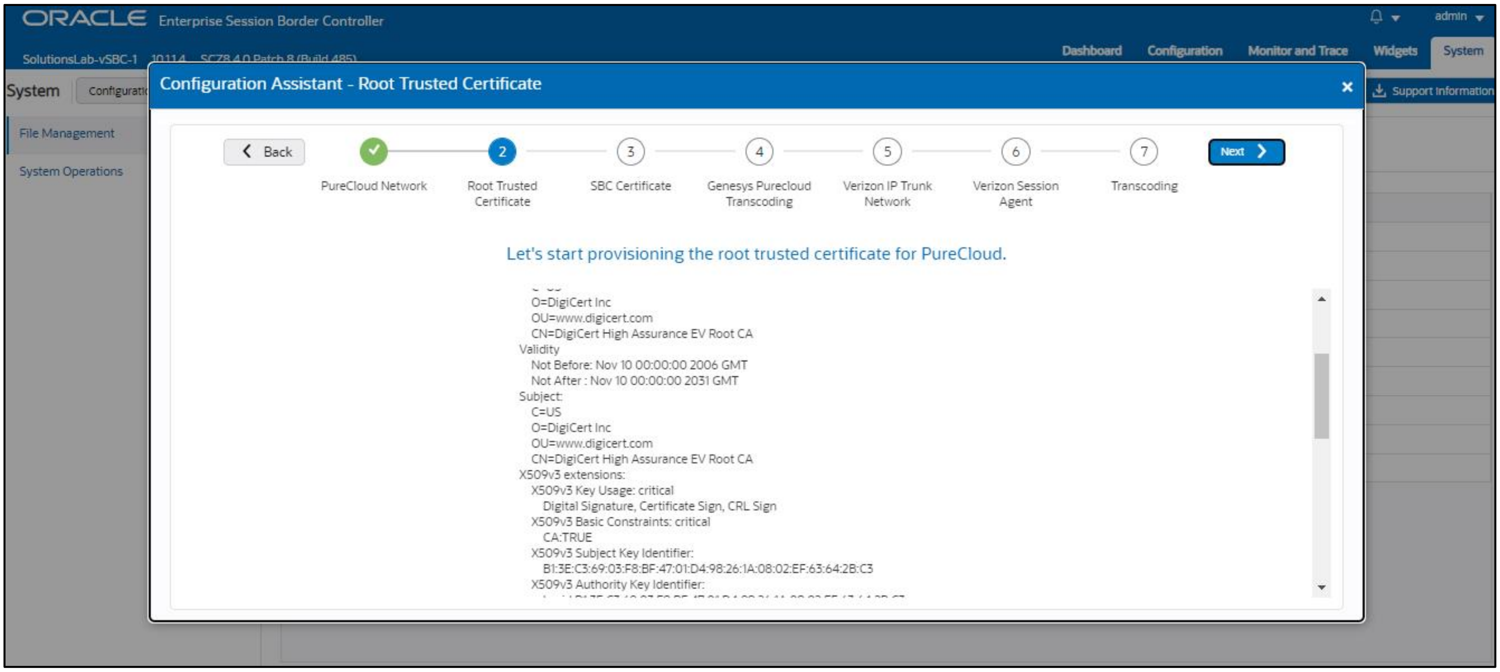
Port Number

Port 0

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.



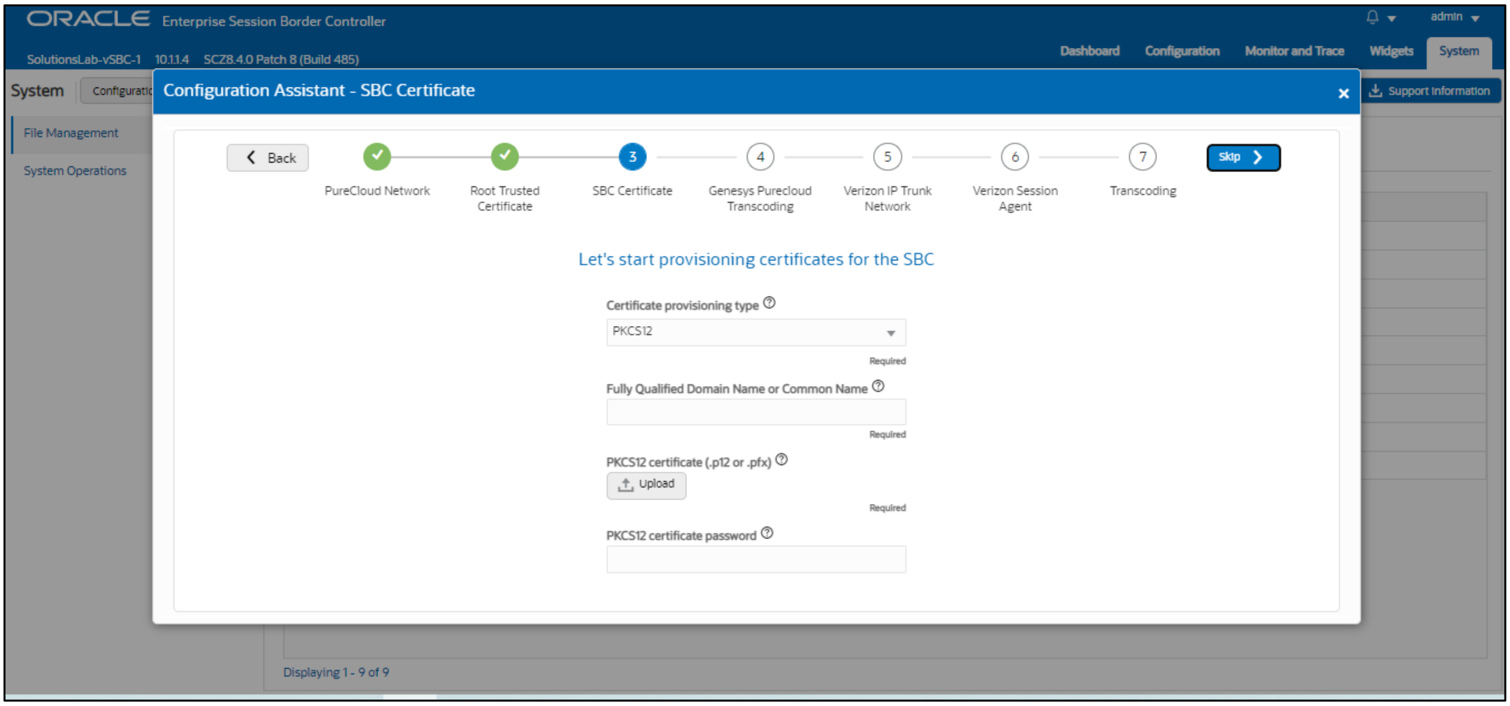
Configuration Assistant - Root Trusted Certificate

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

```
    O=DigiCert Inc
    OU=www.digicert.com
    CN=DigiCert High Assurance EV Root CA
  Validity
    Not Before: Nov 10 00:00:00 2006 GMT
    Not After : Nov 10 00:00:00 2031 GMT
  Subject:
    C=US
    O=DigiCert Inc
    OU=www.digicert.com
    CN=DigiCert High Assurance EV Root CA
  X509v3 extensions:
    X509v3 Key Usage: critical
      Digital Signature, Certificate Sign, CRL Sign
    X509v3 Basic Constraints: critical
      CA:TRUE
    X509v3 Subject Key Identifier:
      B1:3E:C3:69:03:F8:BF:47:01:D4:98:26:1A:08:02:EF:63:64:2B:C3
    X509v3 Authority Key Identifier:
```

Page 3 - SBC Certificates for PureCloud side

By default, the SBC is set to import a certificate in PKCS12 format. This is the simplest and recommended way to add a certificate to the Oracle SBC. Using this method, you will add the SBC's hostname under "FQDN or Common Name" field, upload a certificate signed from one of the PureCloud Supported CA Vendors, and enter the certificates password.



Let's start provisioning certificates for the SBC

Certificate provisioning type: PKCS12 (Required)

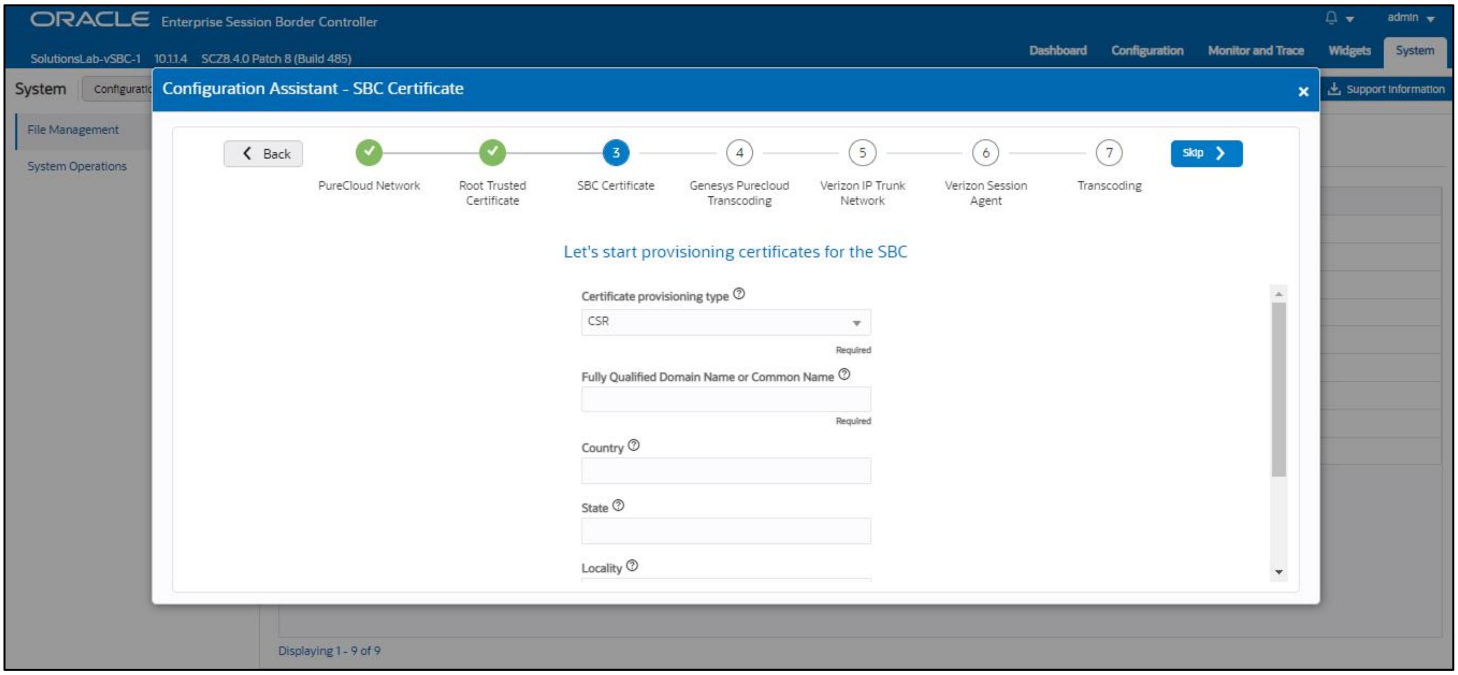
Fully Qualified Domain Name or Common Name (Required)

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

PKCS12 certificate password

Certificate Signing Request (CSR)

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



Configuration Assistant - SBC Certificate

Let's start provisioning certificates for the SBC

Certificate provisioning type: CSR (Required)

Fully Qualified Domain Name or Common Name (Required)

Country

State

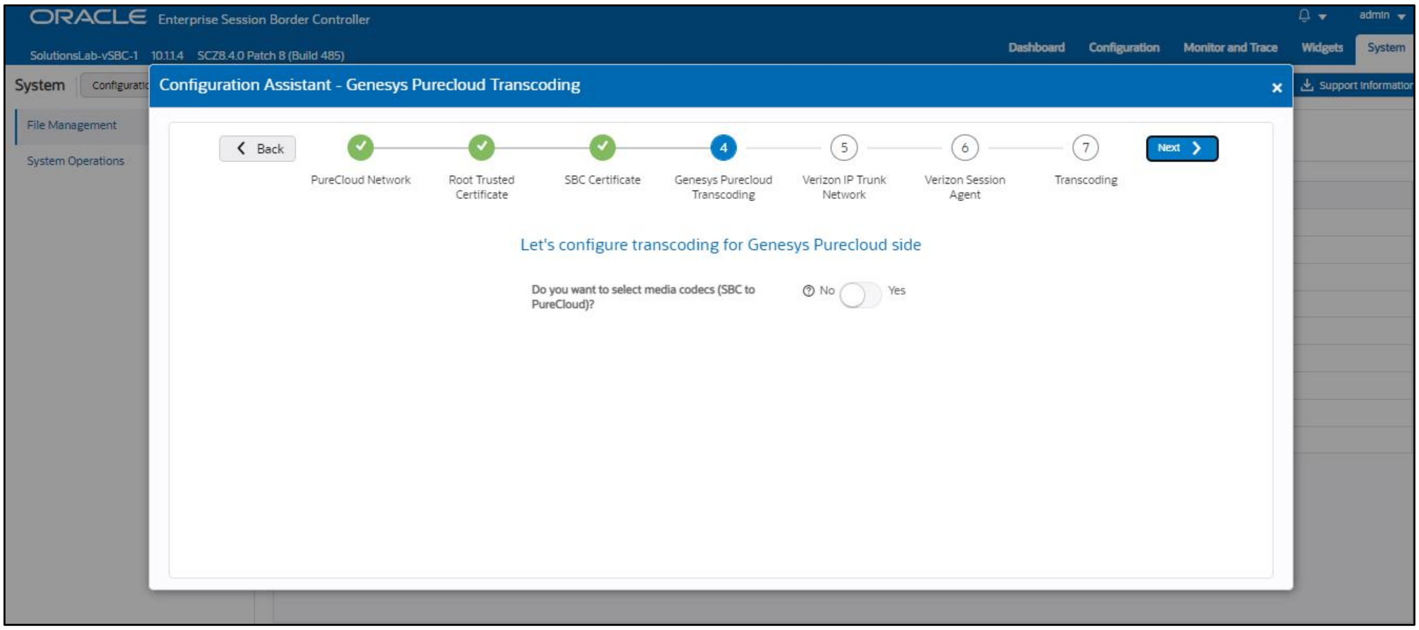
Locality

Page 4 – PureCloud side Transcoding

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

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

You can select as many codecs from the list presented.



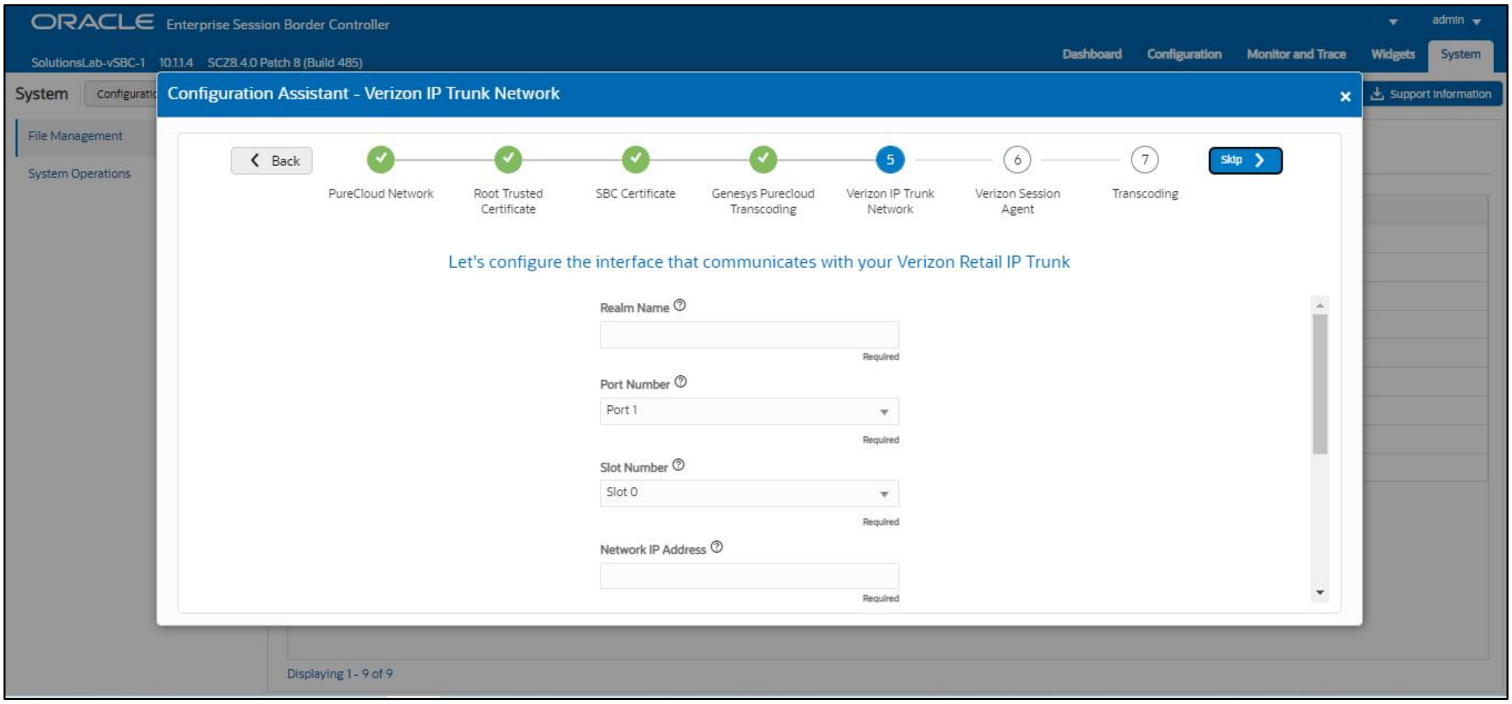
Configuration Assistant - Genesys Purecloud Transcoding

Let's configure transcoding for Genesys Purecloud side

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

Page 5 – Verizon Retail IP Trunk Network

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



Configuration Assistant - Verizon IP Trunk Network

Let's configure the interface that communicates with your Verizon Retail IP Trunk

Realm Name ⓘ

Required

Port Number ⓘ

Port 1

Required

Slot Number ⓘ

Slot 0

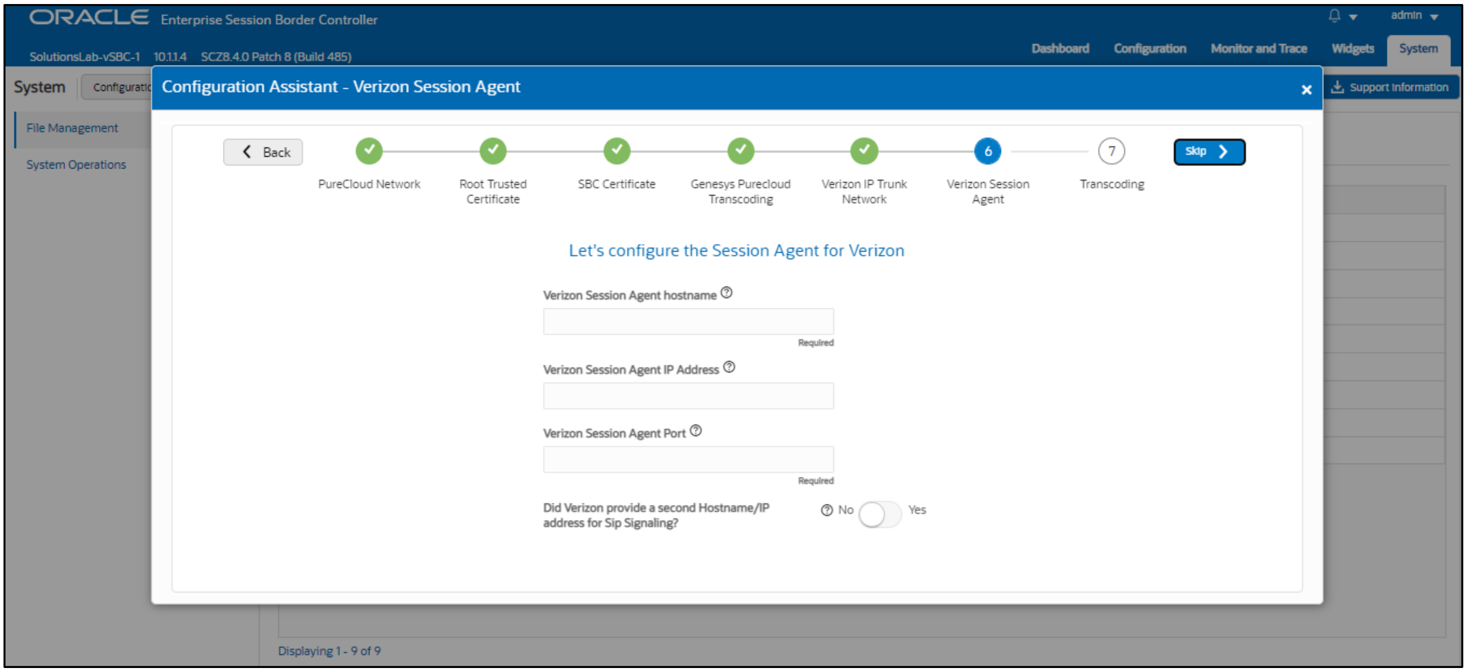
Required

Network IP Address ⓘ

Required

Page 6 – Verizon Retail IP Trunk Session Agent

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



Configuration Assistant - Verizon Session Agent

Let's configure the Session Agent for Verizon

Verizon Session Agent hostname ⓘ

Required

Verizon Session Agent IP Address ⓘ

Verizon Session Agent Port ⓘ

Required

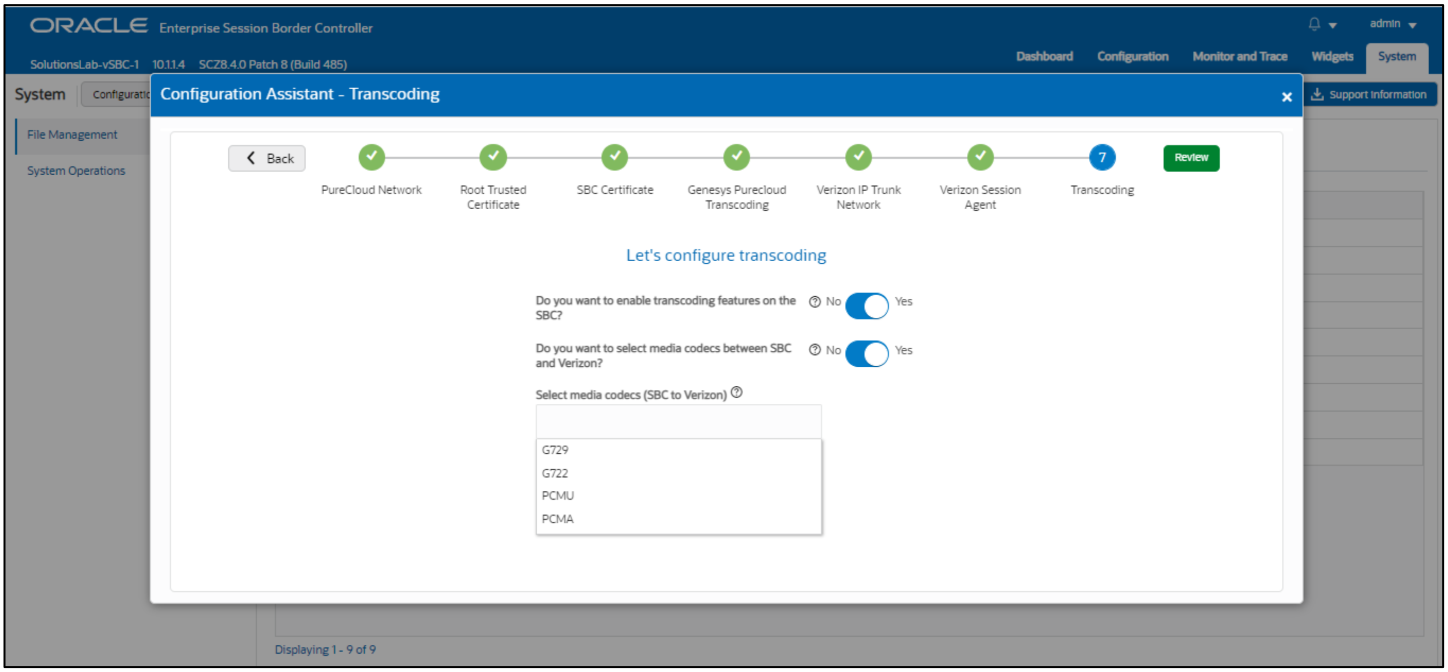
Did Verizon provide a second Hostname/IP address for Sip Signaling? ⓘ No ○ Yes

Please fill the required fields and click Next.

Page 7 - PSTN side Transcoding

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



Configuration Assistant - Transcoding

Let's configure transcoding

Do you want to enable transcoding features on the SBC? No / Yes: Yes

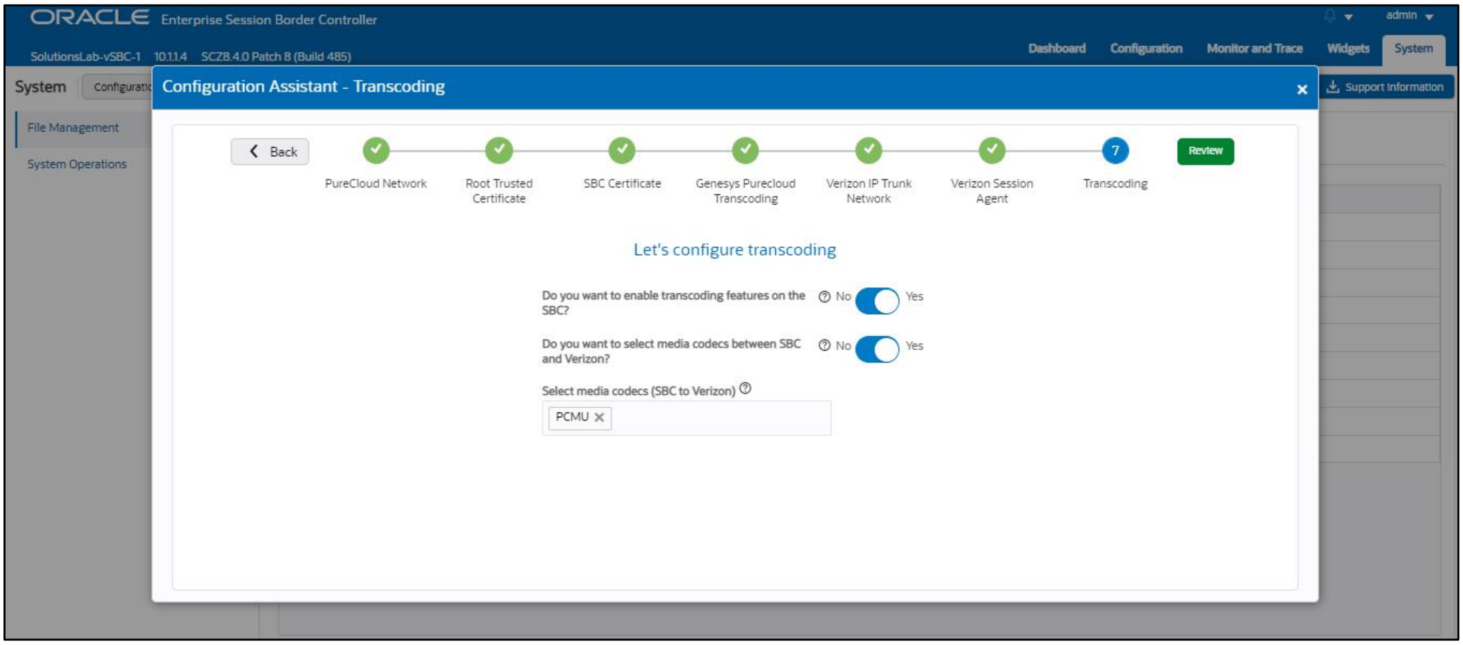
Do you want to select media codecs between SBC and Verizon? No / Yes: Yes

Select media codecs (SBC to Verizon)

G729
G722
PCMU
PCMA

Review

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



Configuration Assistant - Transcoding

Let's configure transcoding

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

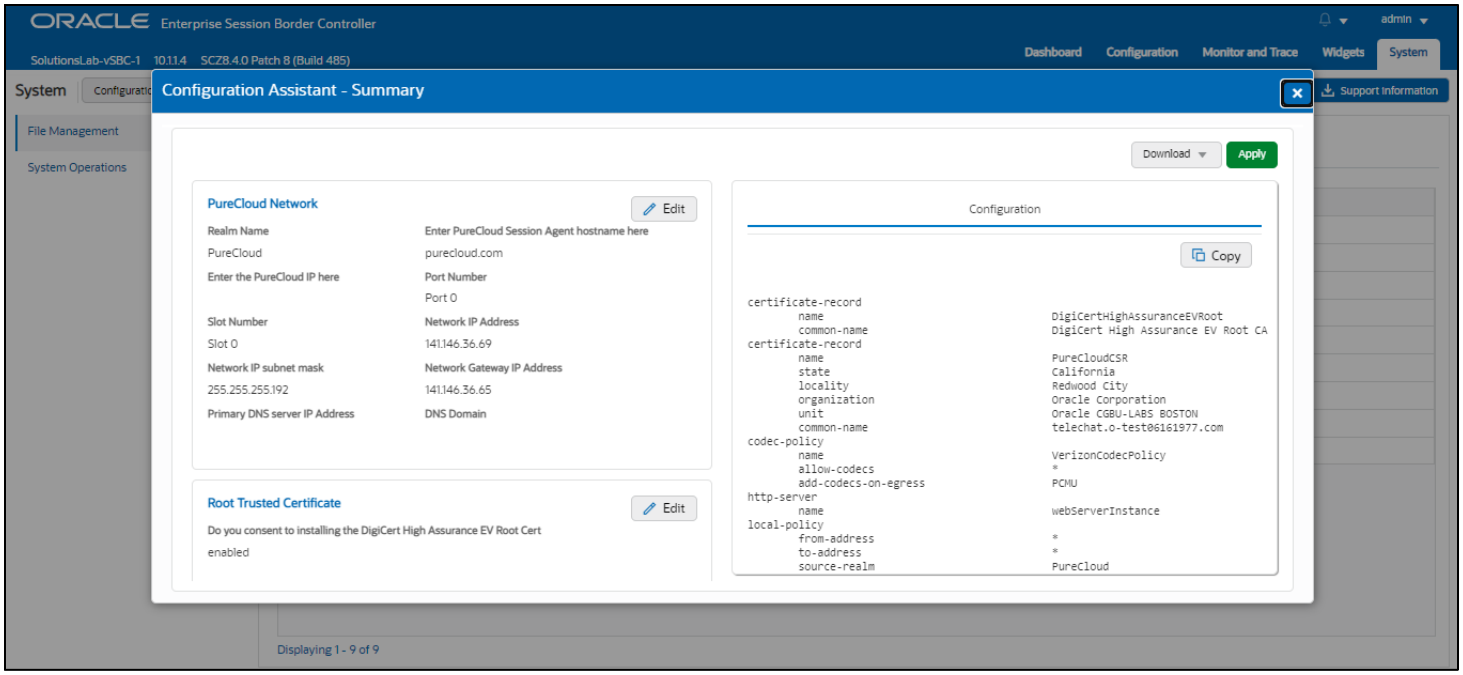
Do you want to select media codecs between SBC and Verizon? No [✓ Yes]

Select media codecs (SBC to Verizon)

PCMU ✕

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

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



Configuration Assistant - Summary

PureCloud Network

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

Root Trusted Certificate

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

enabled

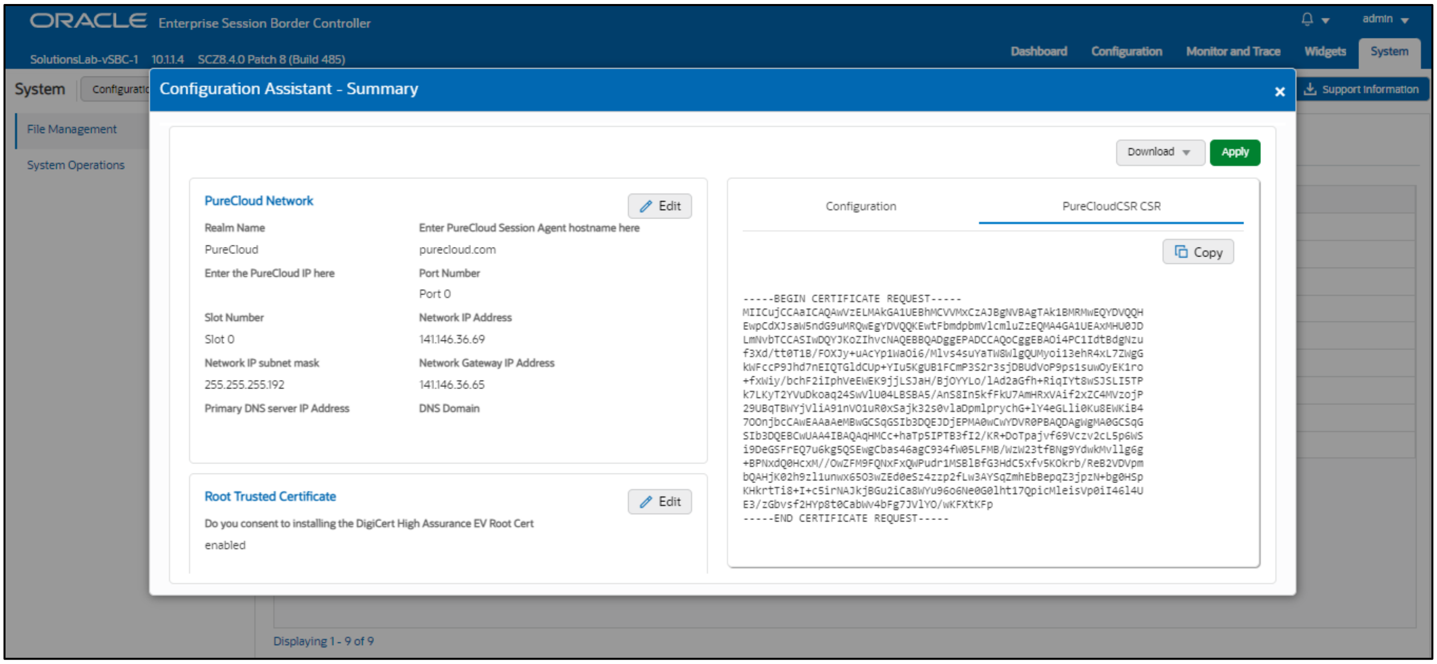
Configuration

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

On the left side of the review contains the entries for each page. Each page has an “*Edit*” tab that can be used to make changes to the information entered on that specific page without having to go through the entire template again.

On the right side of the review page, under the "*Configuration*" tab is the ACLI output from the SBC. This is the complete configuration of the SBC based on the information entered throughout the template. Also on the right side of the review page you may see another tab, "*CSR*".

On Page 3 of the template, if you chose CSR from the drop-down menu instead of PKCS, the SBC configures a certificate record and generates a certificate signing request for you.



Configuration Assistant - Summary

PureCloud Network

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

Root Trusted Certificate

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIICujCCAaICAQAwVzELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEQMA4GA1UEAxMHU0JD
LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOi4PC1IdtBdgNzu
f3Xd/tt0T1B/FOXJy+uAcYp1WaOi6/Mlvs4suYaTW8WlgQUMyoi13ehR4xL7ZWgG
kWFccP9Jhd7nEIQTGldCUp+YIu5KgUB1FCmP3S2r3sjDBUdVoP9ps1suwOyEK1ro
+fxWiy/bchF2iIphVeEWEK9jjLSJaH/BjOYYLo/lAd2aGfh+RiqIYt8wSJSLI5TP
k7LKyT2YVuDkoaq24SwVlU04LBSBA5/AnS8In5kfFkU7AmHRxVAif2xZC4MVzojP
29UBqTBWYjVliA91nVO1uR0xSajk32s0vlaDpmlprychG+lY4eGLli0Ku8EWKiB4
7OOnjbcCAwEAAaAeMBwGCSqGSIb3DQEJDjEPMA0wCwYDVR0PBAQDAgWgMA0GCSqG
SIb3DQEBCwUAA4IBAQAqHMCc+haTp5IPTB3fI2/KR+DoTpajvf69Vczv2cL5p6WS
i9DeGSFrEQ7u6kg5QSEwgCbas46agC934fW05LFMB/WzW23tfBNg9YdwkMvllg6g
+BPNxdQ0HcxM//OwZFM9FQNxFxQWPudr1MSBlBfG3HdC5xfv5KOkrb/ReB2VDVpm
bQAHjK02h9zl1unwx65O3wZEd0eSz4zzp2fLw3AYSqZmhEbBepqZ3jpzN+bg0HSp
KHkrtTi8+I+c5irNAJkjBGu2iCa8WYu96o6Ne0G0lht17QpicMleisVp0iI46l4U
E3/zGbvsf2HYp8t0CabWv4bFg7JVlYO/wKFXtKFp
-----END CERTIFICATE REQUEST-----
```

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

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

Download and/or Apply

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

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

Configuration Assistant Access

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

9. Test Plan Executed

We have executed the following test plan to validate the interworking between Genesys PureCloud and Verizon Business 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

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services