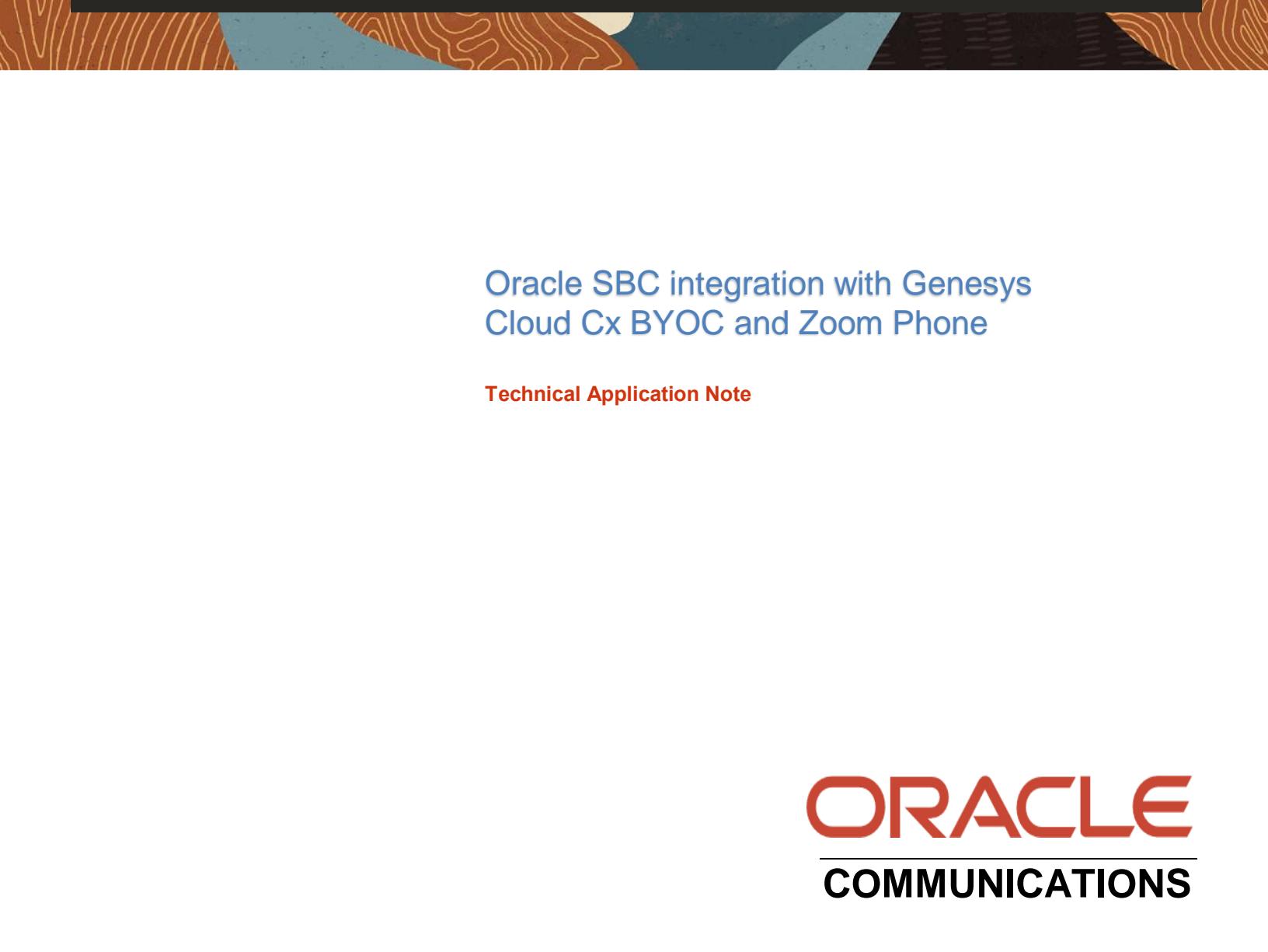


# ORACLE

Oracle SBC integration with Genesys  
Cloud Cx BYOC and Zoom Phone

Technical Application Note



**ORACLE**  
COMMUNICATIONS

## Disclaimer

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

## Revision History

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

<b>Version</b>	<b>Description of Changes</b>	<b>Date Revision Completed</b>
1.0	Oracle SBC integration with Genesys Cloud Cx and Zoom Phone BYOC	20 Aug 2021
1.1	Oracle Public IP Address masked	18 Nov 2021
1.2	Added Section Genesys Cloud Cx Configuration Assistant	03 Feb 2022
1.3	Rebranding of Genesys PureCloud to Genesys Cloud Cx	04 April 2025

## Table of Contents

<b>1 INTENDED AUDIENCE .....</b>	<b>5</b>
<b>2. DOCUMENT OVERVIEW .....</b>	<b>5</b>
2.1 ZOOM PHONE.....	5
2.2 GENESYS CLOUD CX.....	5
<b>3. VALIDATED ORACLE VERSIONS .....</b>	<b>5</b>
<b>4. ARCHITECTURE.....</b>	<b>6</b>
<b>5. CONFIGURE GENESYS CLOUD CX .....</b>	<b>7</b>
5.1 EXTERNAL TRUNK CONFIGURATION .....	7
5.1.1 Create a new External Trunk.....	7
5.1.2 Set Inbound SIP Termination Identifier.....	7
5.1.3 Set Outbound SIP Servers or Proxies .....	8
5.1.4 Set Calling Address .....	9
5.1.5 Set SIP Access Control.....	9
5.1.6 Enable E.164 format.....	9
5.2 SITE CONFIGURATION .....	10
5.2.1 Create a New Site.....	10
5.2.2 Number Plans & Classifications.....	11
5.2.3 Configure outbound route .....	12
5.2.4 Phone configuration.....	13
5.2.5 Simulate call.....	13
5.3 DID ASSIGNMENT.....	14
5.3.1 Create DID Range .....	14
5.3.2 Assign DID to User.....	15
5.4. ARCHITECT FLOW FOR INBOUND WELCOME PROMPT .....	15
<b>6. CONFIGURE ZOOM PHONE.....</b>	<b>16</b>
6.1 CREATE A ZOOM USER .....	16
6.2 ADD BYOC NUMBER.....	17
6.3 ASSIGN A CALLING PACKAGE TO USER .....	18
6.4 ASSIGN THE BYOC NUMBER TO A USER.....	19
<b>7. CONFIGURING THE SBC .....</b>	<b>20</b>
7.1 NEW SBC CONFIGURATION.....	20
7.1.1 Establishing a serial connection to the SBC .....	20
7.2.2 Configure SBC using Web GUI.....	24
7.2. CONFIGURE SYSTEM-CONFIG.....	25
7.3. CONFIGURE PHYSICAL INTERFACE VALUES .....	26
7.4. CONFIGURE NETWORK INTERFACE VALUES .....	28
7.5. ENABLE MEDIA MANAGER.....	29
7.6. CONFIGURE REALMS.....	30
7.7. SIP SECURITY CONFIGURATION .....	33
7.7.1 Configuring Certificates .....	33
7.7.1.1 End Entity Certificate .....	34
7.7.1.2 Import CA Certificate .....	38
7.8. TLS-PROFILE.....	38
7.9. CONFIGURE SIP INTERFACES .....	40
7.10. CONFIGURE SESSION-AGENT .....	41

7.11. CONFIGURE SESSION-AGENT GROUP .....	43
7.12. CONFIGURE LOCAL-POLICY .....	43
7.13. CONFIGURE STEERING-POOL .....	45
7.14. CONFIGURE ADDITIONAL PARAMETERS.....	46
7.14.1 SIP Manipulations .....	46
7.14.2 Enable Ping-response.....	47
7.15. MEDIA SECURITY CONFIGURATION.....	48
7.15.1 Configure sdes profile.....	48
7.15.2. Configure Media Security Profile.....	48
7.16 ACCESS CONTROL.....	50
7.17 SBC BEHIND NAT SPL CONFIGURATION .....	51
7.18 CAVEAT -OPUS TRANSCODING .....	52
<b>8. CONFIGURING THE ORACLE SBC THROUGH CONFIG ASSISTANT.....</b>	<b>53</b>
SECTION OVERVIEW AND REQUIREMENTS .....	53
INITIAL GUI ACCESS .....	53
CLOUD CX CONFIGURATION ASSISTANT.....	54
PAGE 1- CLOUD CX NETWORK .....	55
PAGE 2 - IMPORT DIGICERT TRUSTED CA CERTIFICATE FOR CLOUD CX.....	56
PAGE 3 - SBC CERTIFICATES FOR CLOUD CX SIDE .....	56
PAGE 4 – CLOUD CX SIDE TRANSCODING.....	57
PAGE 5 – PSTN SIP TRUNK NETWORK.....	58
PAGE 6 – PSTN SESSION AGENT.....	58
PAGE 7 - PSTN SIDE TRANSCODING.....	59
PAGE 8 – ADDITIONAL CONFIGURATION.....	59
REVIEW .....	60
DOWNLOAD AND/OR APPLY .....	62
CONFIGURATION ASSISTANT ACCESS .....	62
<b>9. TEST PLAN EXECUTED .....</b>	<b>62</b>

## 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 Cloud Cx and Zoom Phone.

## 2. Document Overview

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

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

You can follow our Application Note - <https://www-sites.oracle.com/a/otn/docs/oracle-sbc-with-genesys-cloud-cx-and-twilio-sip-trunkv0.3.pdf> as a reference to configure the Twilio SIP Trunk with Oracle SBC.

Related documentation can be found below –

### 2.1 Zoom Phone

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

### 2.2 Genesys Cloud Cx

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

<https://help.myCloud Cx.com/articles/about-byoc-cloud/>

## 3. Validated Oracle Versions

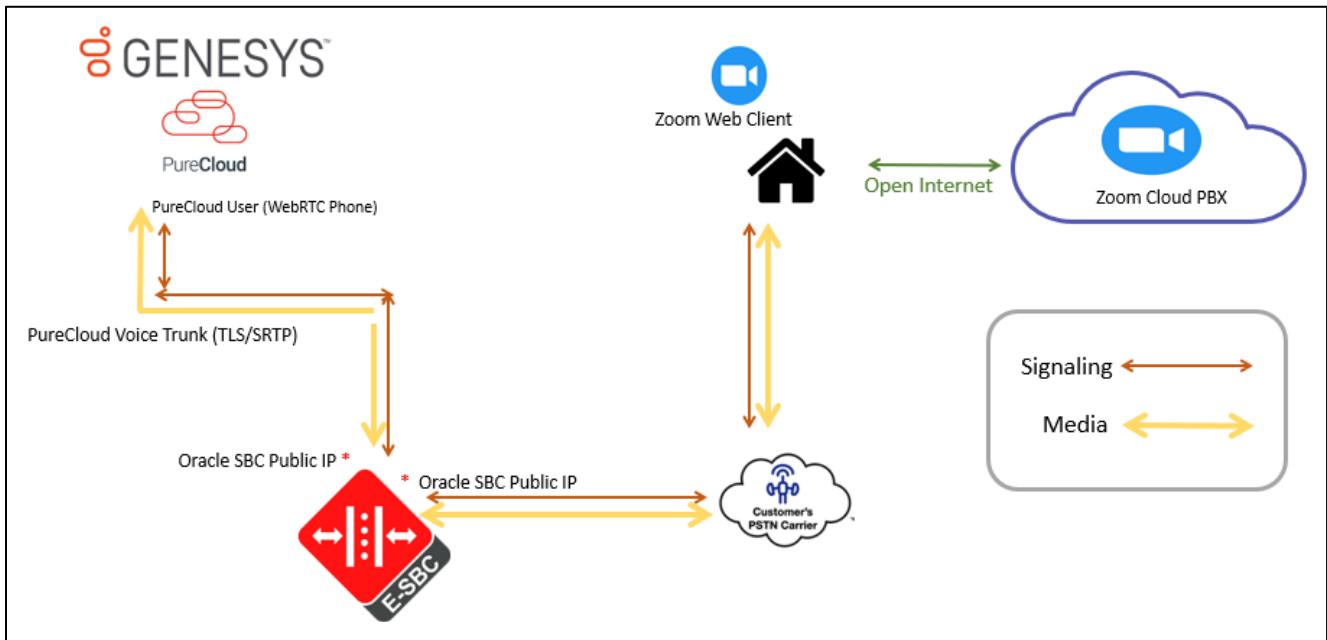
We have successfully conducted testing with the Oracle Communications SBC versions:  
SCZ840p5a

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

- AP 1100
- AP 3900
- AP 4600

- AP 6350
- AP 6300
- VME

## 4. Architecture.



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

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

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

Phase 1 – Configuring Genesys Cloud Cx

Phase 2 – Configuring Zoom Phone

Phase 3 – Configuring Oracle Session Border Controller.

Note IP Addresses, FQDN and configuration names and details given in this document are used for reference purposes only. These same details cannot be used in customer configurations. End users of this document can use the configuration details according to their network requirements. There are some public facing IPs (externally routable IPs) that we use for our testing are masked in this document for security reasons. You can configure any publicly routable IPs for these sections as per specific network architecture needs.

## 5. Configure Genesys Cloud Cx

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

**Note:** The document only includes the steps required on Genesys Cloud Cx 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 Cloud Cx configuration as per your requirement.

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

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

For the purpose of this Application note, the connection between Oracle SBC and Genesys Cloud Cx 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 Cloud Cx telephony connection option and facilitates point-to-point communication. We will configure Oracle Enterprise SBC as an external Trunk on the Cloud Cx Portal. Detailed steps to configure the external trunk can be found here-

<https://help.myCloud Cx.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 Cloud Cx. Here a vanity FQDN **byoc-voxai.byoc.myCloud Cx.com** is generated with the inbound sip termination identifier as byoc-voxai. This FQDN resolves to the following IP Addresses of the Cloud Cx AWS US Data Centers.

**Inbound SIP Termination Identifier:** byoc-voxai

**Ex:** INVITE <sip:+xxxxxxxxxx@byoc-voxai.byoc.myCloud Cx.com>

**Protocol:** TLS

Genesys Reference - <https://help.myCloud Cx.com/articles/tls-trunk-transport-protocol-specification/>

### ### Genesys Cloud IP List

IP Addresses	Load Balancer DNS Names
52.203.12.137	<a href="#">lb01.byoc.us-east-1.myCloud Cx.com</a>
54.82.241.192	<a href="#">lb02.byoc.us-east-1.myCloud Cx.com</a>
54.82.241.68	<a href="#">lb03.byoc.us-east-1.myCloud Cx.com</a>
54.82.188.43	<a href="#">lb04.byoc.us-east-1.myCloud Cx.com</a>

Topology

External Trunk Name

Metrics

Oracle BYOC POC

Trunks

Sites

Edge Groups

Edges

Phone Management

Trunk State ?

In Service

Certificate Authorities

DID Numbers

Extensions

Inbound / Termination

Inbound SIP Termination Identifier ?

byoc-voxai

DNIS Replacement Routing ?

Disabled

Status ? Operational

Type ? Generic BYOC Carrier

Metrics

Inbound Calls ? 0

Outbound Calls ? 0

QoS Mismatches ? 0

Protocol ?

TLS

Inbound Request-URI Reference

FQDN Method

INVITE sip:+xxxxxxxxxx@byoc-voxai.byoc.mypurecloud.com

TGRP Method ?

INVITE sip:+xxxxxxxxxx;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.

Edge Groups

Outbound

Outbound SIP Termination FQDN ?

solutionslab.cgbutherford.com

Edges

Outbound SIP TGRP Attribute ?

Phone Management

TGRP Context-ID ?

Certificate Authorities

Outbound SIP DNIS ?

DID Numbers

Extensions

Outbound Request-URI Reference

INVITE sip:+xxxxxxxxxx@solutionslab.cgbutherford.com

#### 5.1.4 Set Calling Address

Calling

Address: 19729132636

Address Override Method: Always

Name: (empty)

Name Override Method: Always

SIP Access Control

Allow the Following Addresses:

- (IP address 1)
- (IP address 2)

Add an IP or CIDR address

External Trunk Configuration

- General
- Transport
- Identity
- Media
- Protocol
- Diagnostics
- Custom

Save External Trunk Cancel

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:

- (IP address 1)
- (IP address 2)

Add an IP or CIDR address

Save External Trunk

#### 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.

<b>Address Digits Length</b> 	<b>Address Omit + Prefix</b>  
<input type="text" value="0"/>	<input checked="" type="radio"/> <b>Disabled</b>

## 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 Cloud Cx Edge(s).

Detailed steps to configure the Site can be found here-

<https://help.myCloud Cx.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**.

The screenshot shows the 'General' tab of the Cloud CX Topology configuration interface. The 'Site Name' is set to 'BYOC\_Oracle'. The 'Default Site' is selected, and there are options to make it the default site, branch site, or cloud site. The 'Phones' count is 1, and there is an option to restart all phones assigned to this site. The 'Edge Group' is 'PureCloud Voice - AWS', and there is a link to 'Show Topology'. The 'Media' section shows 'Geo-Lookup TURN' is disabled. The 'Automatic Updates' section shows a recurrence type of 'Daily' and a time zone of 'America/Chicago (-05:00)'. The 'Time' section shows 'Range' selected, with a start time of '2 : 00 AM' and an end time of '5 : 00 AM'. At the bottom are 'Save Site' and 'Cancel' buttons.

## 5.2.2 Number Plans & Classifications

Cloud Cx 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.

Topology

General Number Plans Outbound Routes Simulate Call

Metrics

Trunks

**Sites**

BYOC

Emergency

Extension

National

International

Network

Number Plan Name: BYOC

Match Type: E.164 Number List

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

**Delete Number Plan**

### 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.

Topology

General Number Plans Outbound Routes Simulate Call

Metrics

Trunks

**Sites**

Default Outbound Route

Outbound Route Name: Default Outbound Route

Distribution Pattern: Sequential

Description

External Trunks: OracleSolutionsLabBYOCSBC

State: Enabled

Classifications: Emergency, National, International, Network, BYOC

Select External Trunks

**Save Outbound Routes** Cancel

#### 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.

The screenshot shows the 'Edit Phone' page in the Genesys Cloud Cx interface. The left sidebar lists categories: Topology, Metrics, Trunks, Sites, Edge Groups, Edges, Phone Management (selected), Certificate Authorities, DID Numbers, and Extensions. The main area is titled 'Phone' and contains the following fields:

- Phone Name:** WebRTC
- Base Settings:** WebRTC Cloud
- Site:** BYOC\_Oracle
- Person:** [redacted]

On the right, a detailed view of the phone's status and configuration is shown:

<b>Status</b>	Unmanaged
<b>Make and Model</b>	Genesys Cloud WebRTC Phone
<b>In Use By</b>	[redacted] Log off
<b>Default For</b>	None
<b>Primary Edge</b>	<input type="radio"/> virtual-edge-i-0e97fcfda24ea3d49
<b>Secondary Edge</b>	<input type="radio"/> virtual-edge-i-03e78d824757a3555

Below this is the 'Phone Configuration' section, which is collapsed. It contains four expandable categories: General, Media, Network, and Custom. At the bottom are 'Save Phone' and 'Cancel' buttons.

#### 5.2.5 Simulate call

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

Telephony / Sites / Edit Site

Topology      General      Number Plans      Outbound Routes      Simulate Call

Metrics

Trunks

**Sites**      +12038710043      Simulate Call

Edge Groups

Normalized Number ✓

Number Plan ✓

Classification ✓

Outbound Route ✓

DID Numbers

External Trunks ✓

OracleSolutionsLabBYOCSBC

Extensions

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)

Log

## 5.3 DID Assignment

### 5.3.1 Create DID Range

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

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

Telephony / DID Numbers

Topology      DID Assignments      DID Ranges

**Create Range**

<input type="checkbox"/> DID Range	Service Provider	Comments	<span style="color: green;">✓</span>
<input type="checkbox"/> +1 203-871-0043 → +1 203-871-0043	Twilio	PurecloudtoTwilioviaOracleSBC	
<input type="checkbox"/> +1 415-230-2042 → +1 415-230-2042	Twilio	Ecosystem Testing	
<input type="checkbox"/> +1 415-326-7696 → +1 415-326-7696			
<input type="checkbox"/> +1 415-895-9907 → +1 415-895-9907	Twilio		
<input type="checkbox"/> +1 415-909-3170 → +1 415-909-3170	Twilio		
<input type="checkbox"/> +1 602-428-9752 → +1 602-428-9752	Twilio	Chunder 2	
<input type="checkbox"/> +1 602-883-7410 → +1 602-883-7410	Twilio	Chunder 1	
<input type="checkbox"/> +1 781-313-1033 → +1 781-313-1033	byoc		
<input type="checkbox"/> +1 781-443-7266 → +1 781-443-7266	byoc		
<input type="checkbox"/> +1 928-275-4426 → +1 928-275-4426	Twilio	Andi Dev?	

Create Range

DID Start ✓ +1 +12038710043

DID End ✓ +1 +12078710053

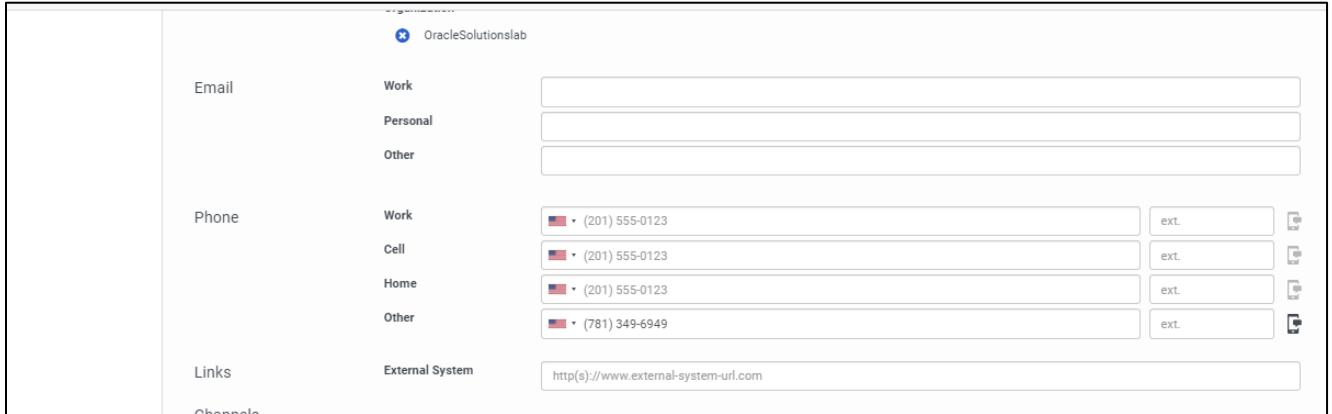
Service Provider ✓ Twilio

Comments ✓ PurecloudtoTwilioviaOracleSBC

Save Cancel

### 5.3.2 Assign DID to User.

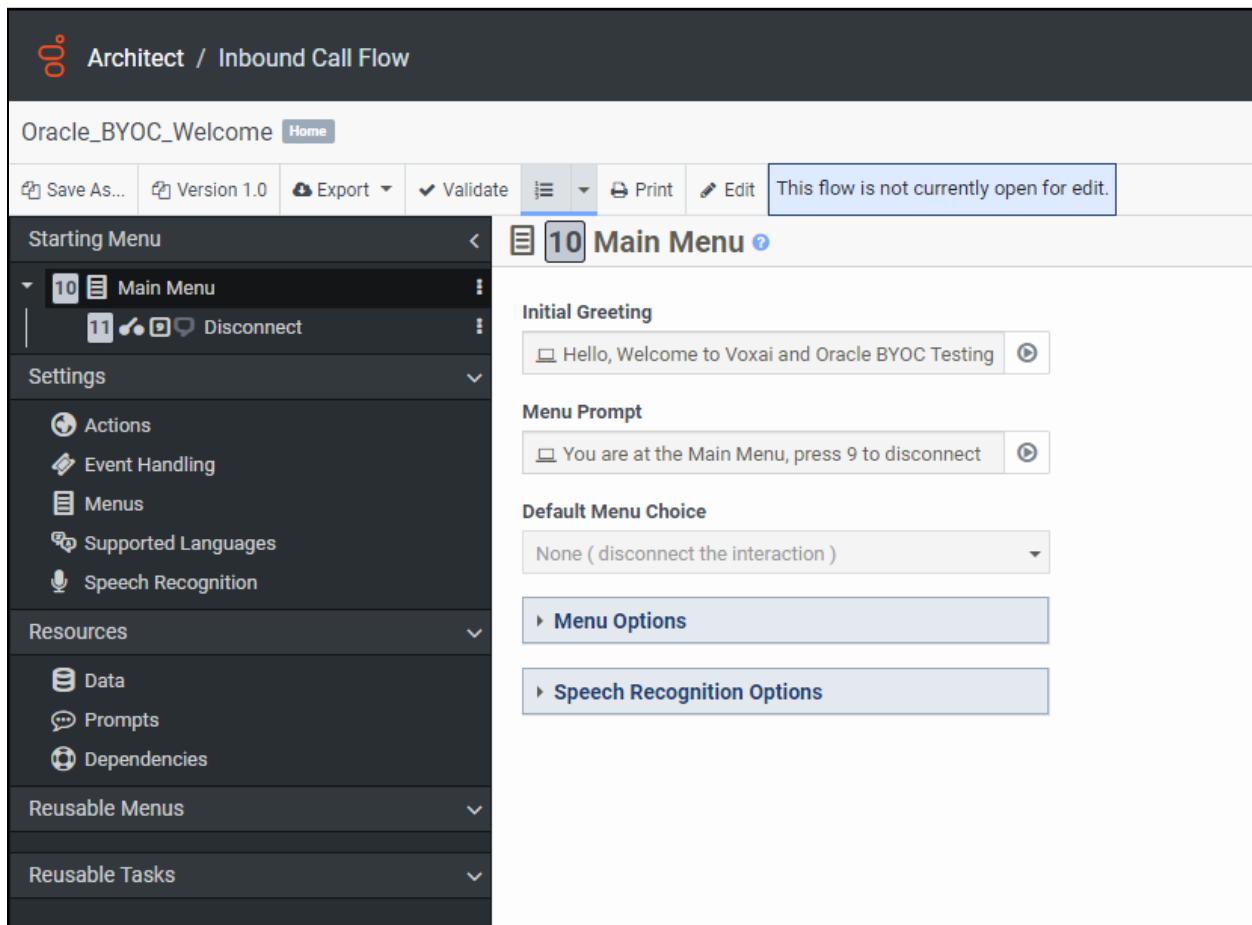
On users' profile field, one of the DID can be assigned to Cloud Cx User as Other Number. The Oracle SBC is configured to send calls from external world to this DID number which will terminate to the user on Cloud Cx.



The screenshot shows the Oracle Solutionslab user profile interface. The 'Email' section has three fields: 'Work' (empty), 'Personal' (empty), and 'Other' (empty). The 'Phone' section has four fields: 'Work' (US, (201) 555-0123, ext. empty, icon empty), 'Cell' (US, (201) 555-0123, ext. empty, icon empty), 'Home' (US, (201) 555-0123, ext. empty, icon empty), and 'Other' (US, (781) 349-6949, ext. empty, icon empty). The 'Links' section has one field: 'External System' (http://www.external-system-url.com). The 'Channels' section is partially visible at the bottom.

### 5.4. Architect flow for inbound welcome prompt

Below is an example for an Architect Flow for inbound Voice Prompt which will be used for inbound calls from Zoom Phone to Genesys Cloud Cx via Oracle SBC.



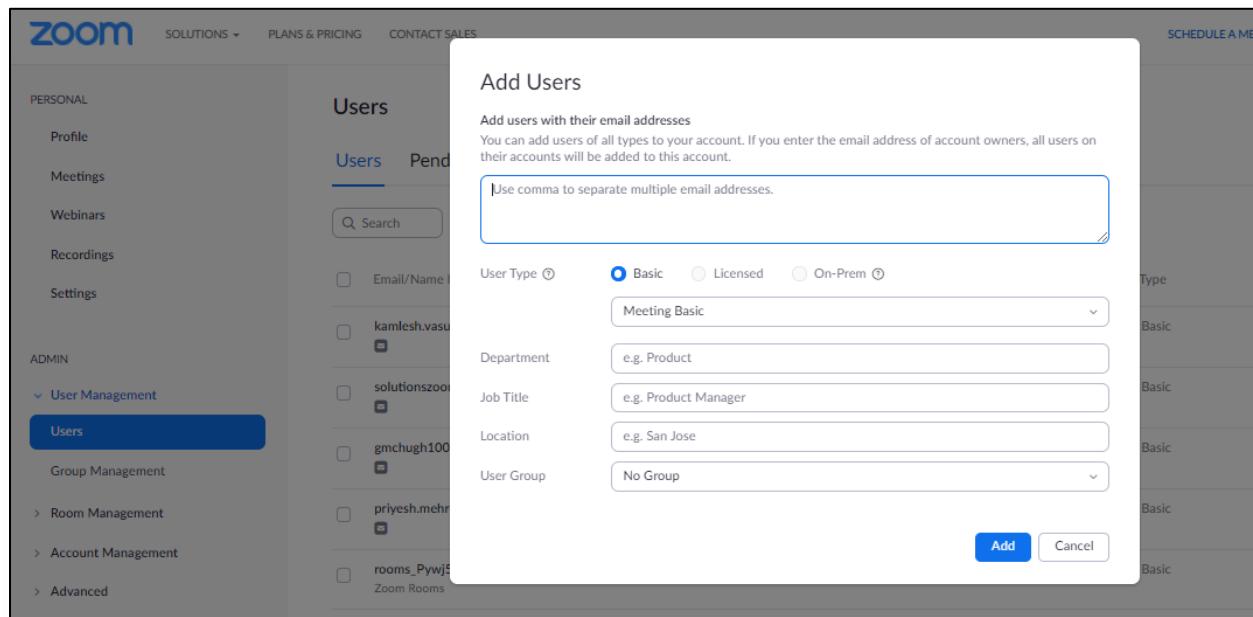
## 6. Configure Zoom Phone

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

### 6.1 Create a Zoom User

Navigate to **Admin>User Management > Users**.

Click Add to create new Zoom users. Provide the necessary details about the New User and Click on Add to Add the User.



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

## 6.2 Add BYOC Number

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

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

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

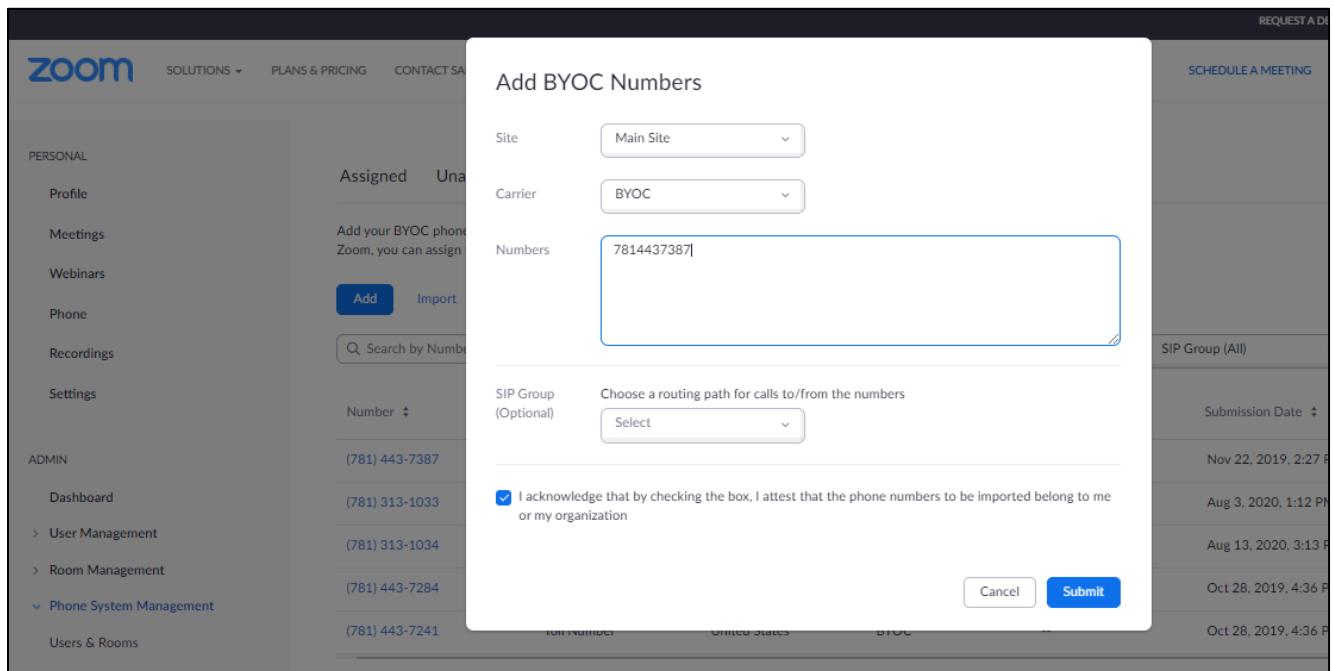
**Carrier** –Choose BYOC

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

**SIP Group** – Optional Parameter (Can be Left Blank)

Acknowledge that the Phone Number belongs to your organization.

Click **Submit**.



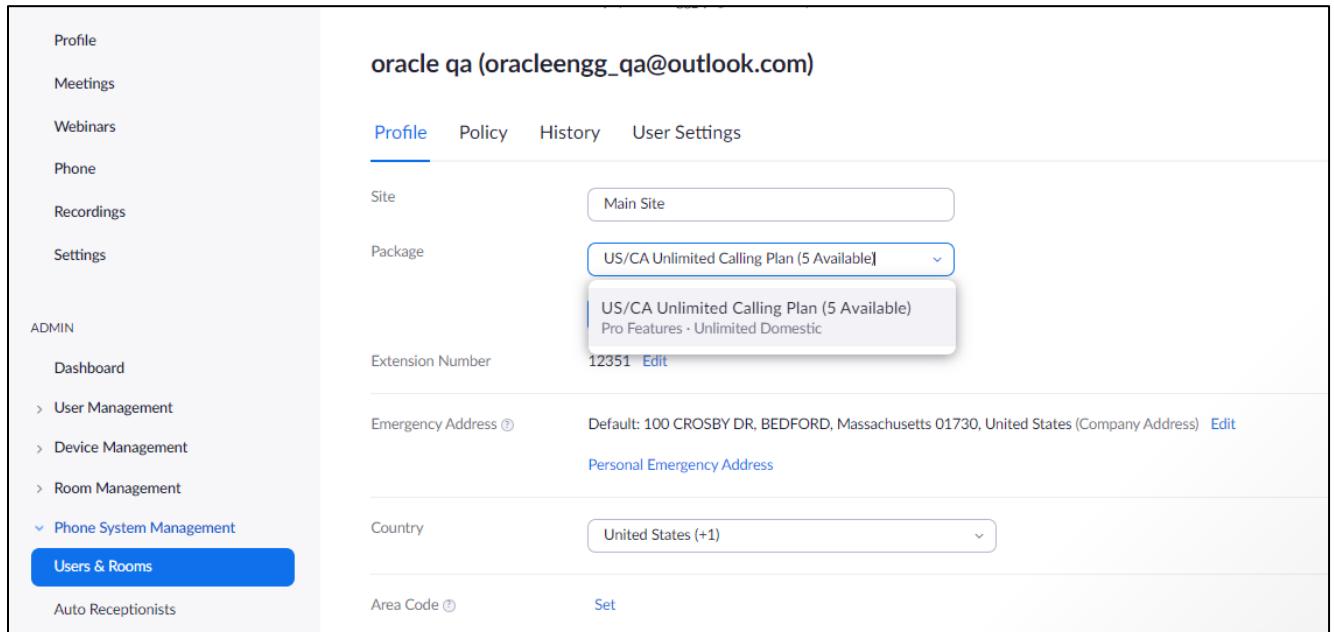
## 6.3 Assign a Calling Package to User

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

To assign a calling package

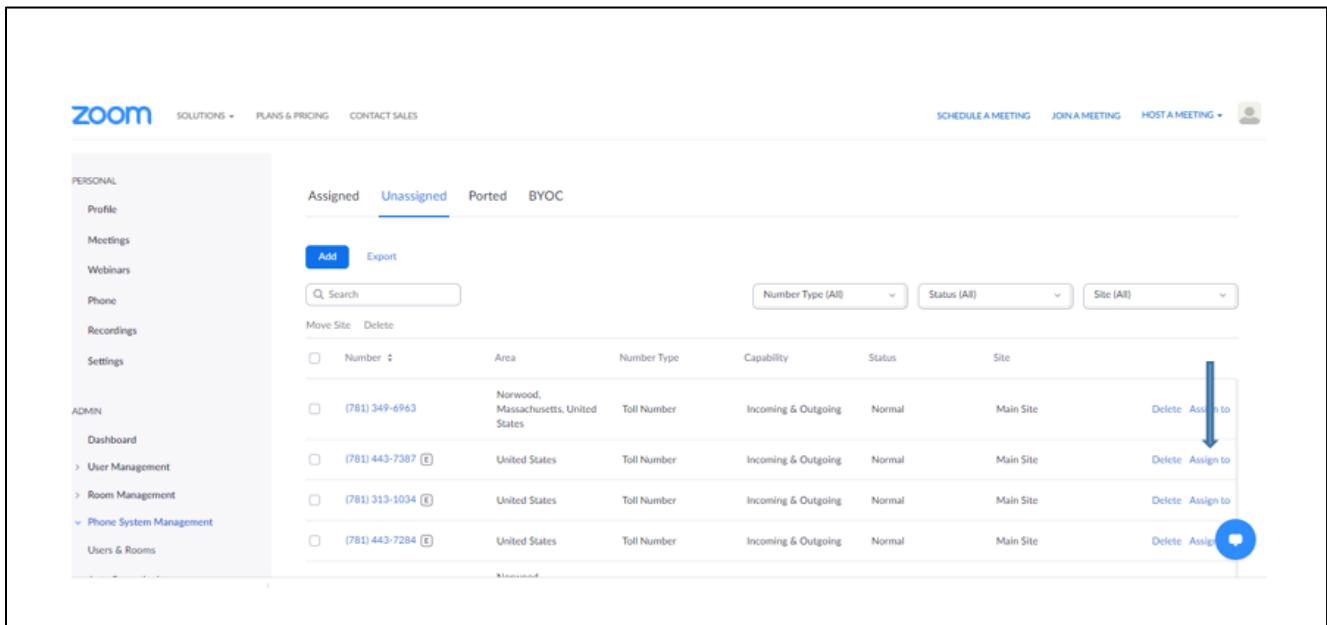
Navigate to **Users and Rooms > Package**

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

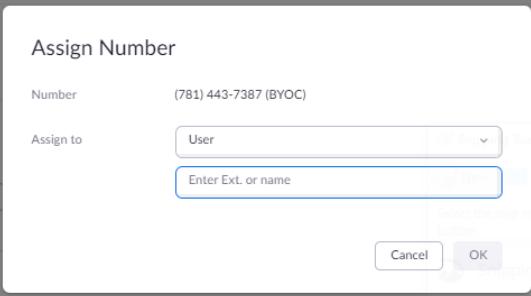


## 6.4 Assign the BYOC Number to a User

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



The screenshot shows the Zoom Phone System Management interface. The left sidebar includes sections for PERSONAL (Profile, Meetings, Webinars, Phone, Recordings, Settings) and ADMIN (Dashboard, User Management, Room Management, Phone System Management, Users & Rooms). The main content area has tabs for Assigned, Unassigned, Ported, and BYOC. The Unassigned tab is selected, showing a list of numbers. Each row in the list includes a checkbox, a number, an area, number type, capability, status, and site. To the right of the list, there are filters for Number Type (All), Status (All), and Site (All). At the bottom of the list, there is a 'Move Site' and 'Delete' button. To the right of the list, there are buttons for 'Delete' and 'Assign to'. A blue arrow points to the 'Assign to' button for a specific BYOC number.



The screenshot shows the 'Assign Number' dialog box. It has fields for 'Number' (set to '(781) 443-7387 (BYOC)') and 'Assign to' (set to 'User'). Below these are buttons for 'Cancel' and 'OK'. A blue arrow points to the 'OK' button. The background shows the Zoom Phone System Management interface with the Unassigned tab selected, displaying a list of numbers.

## 7. Configuring the SBC

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

### 7.1 New SBC configuration

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

#### 7.1.1 Establishing a serial connection to the SBC

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NN4600-139(configure)#

```

Note: There is no management IP configured by default.

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

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

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

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

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

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

Save the changes and reboot the SBC.

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

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 1
Session Capacity (0-128000) : 500

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 3
*****
CAUTION: Enabling this feature activates enhanced security
functions. Once saved, security cannot be reverted without
resetting the system back to factory default state.
*****
Admin Security (enabled/disabled) : :

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 5
Transcode Codec AMR Capacity (0-102375) : 50

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 2
Advanced (enabled/disabled) : enabled

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 10
Transcode Codec OPUS Capacity (0-102375) : 50

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 11
Transcode Codec SILK Capacity (0-102375) : 50
```

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

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

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

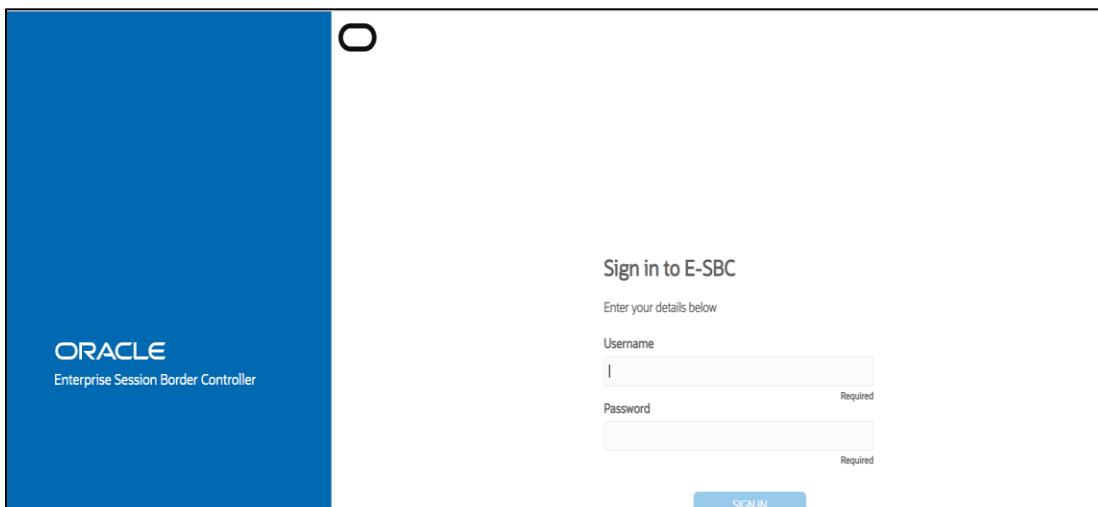
```
NN4600-139(http-server)#
NN4600-139(http-server)# show
http-server
  name                               webServerInstance
  state                             enabled
  realm
  ip-address
  http-state                         enabled
  http-port                          80
  https-state           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

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

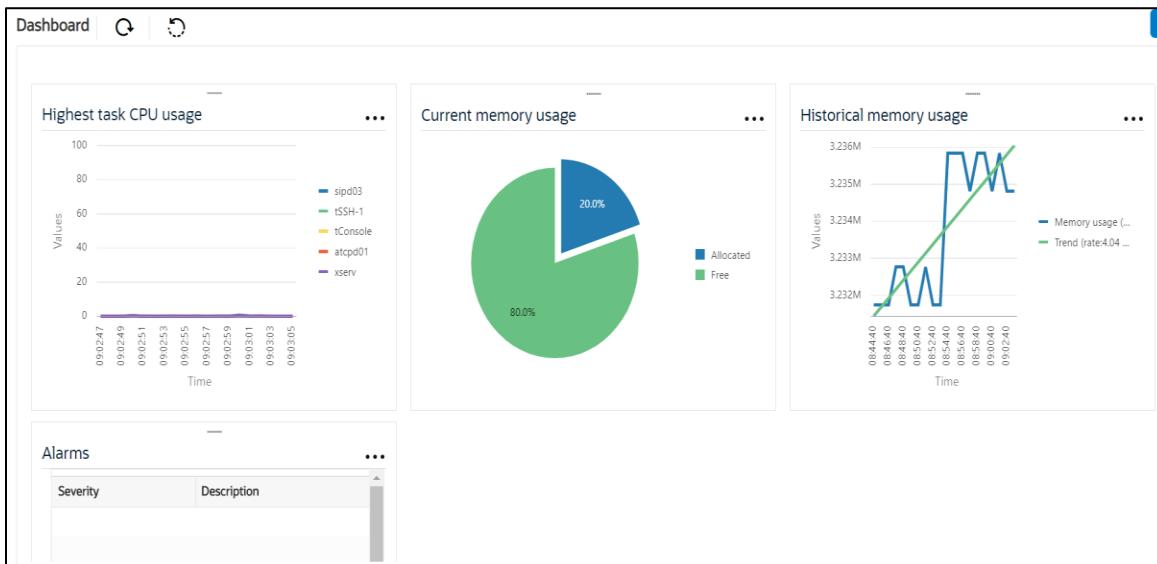
## 7.2.2 Configure SBC using Web GUI

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

The Web GUI can be accessed through the URL [http://<SBC\\_MGMT\\_IP>](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

Show All

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

The expert mode is used for configuration.

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

## 7.2. Configure system-config

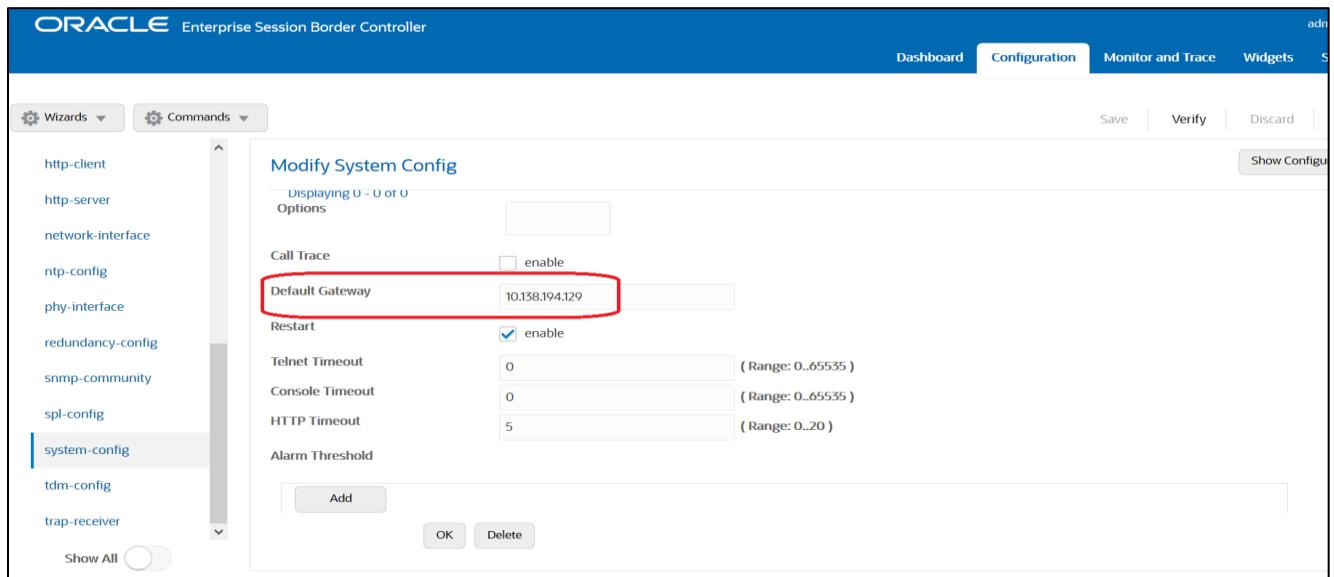
Navigate to system->system-config

Modify System Config

Hostname	OracleSBC
Description	
Location	
Mib System Contact	
Mib System Name	
Mib System Location	
Acp TLS Profile	

OK Delete

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



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

[https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/releasenotes/esbc\\_scz840\\_releasenotes.pdf](https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/releasenotes/esbc_scz840_releasenotes.pdf)

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

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

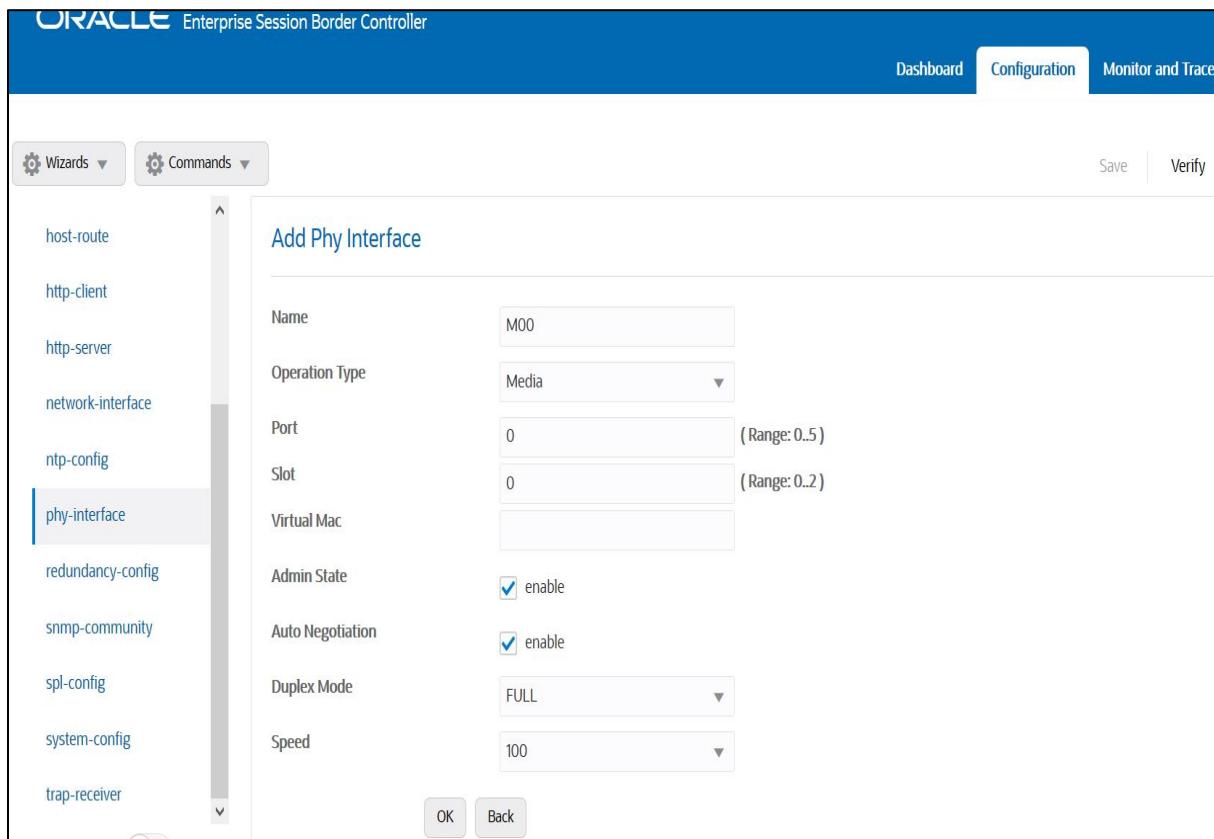
### 7.3. Configure Physical Interface values

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

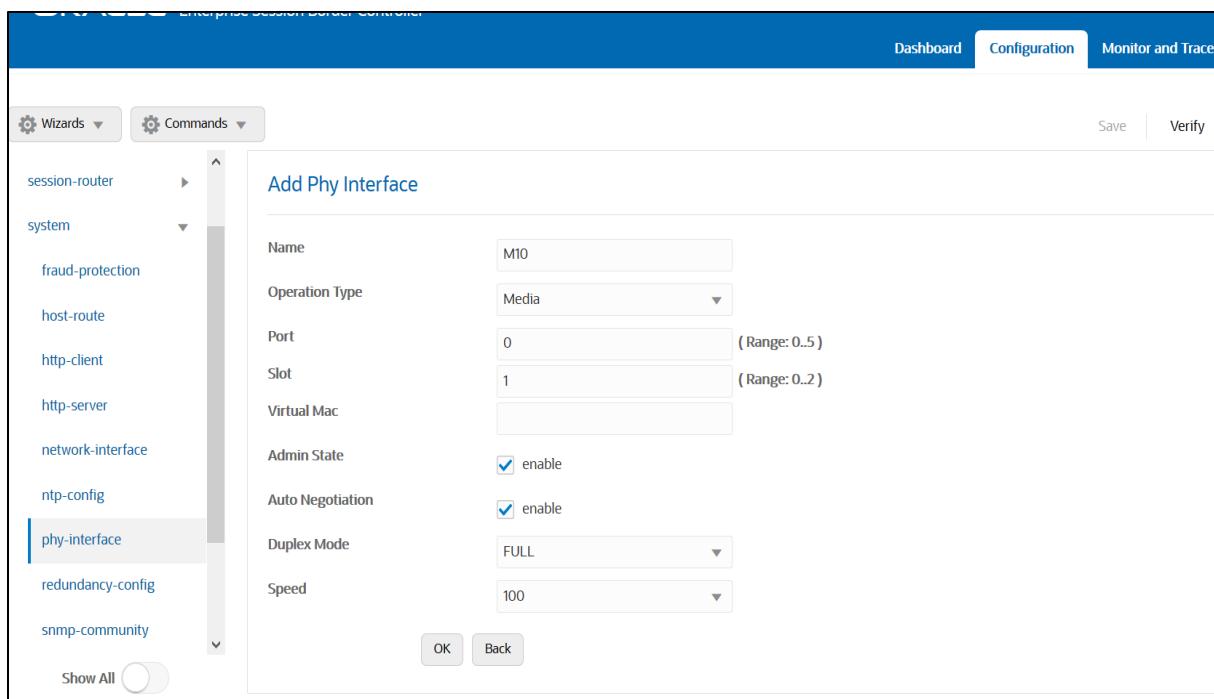
Here we have configured, Network-interface M00 for Zoom Phone and M10 for Cloud Cx.

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

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



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



## 7.4. Configure Network Interface values

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

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

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

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

Parameter Name	Zoom Phone Network Interface	Cloud Cx Network interface
Name	M00	M10
Host Name	Domain (if applicable)	solutionslab.cgbubedford.com
IP address	[REDACTED]	[REDACTED]
Netmask	255.255.255.192	255.255.255.192
Gateway	[REDACTED]	[REDACTED]
dns-ip-primary	8.8.8.8	8.8.8.8
dns-ip-backup1	8.8.8.4	8.8.8.4
Dns-domain	Domain(if applicable)	solutionslab.cgbubedford.com

Configure network interface **M00** as below

Configuration | View Configuration | Q

media-manager ▶

security ▶

session-router ▶

system ▶

fraud-protection

host-route

http-client

http-server ▶

network-interface ▶

ntp-config

phy-interface

redundancy-config

snmp-community

spi-config

system-config

Show All

Modify Network Interface

Name	M00	
Sub Port Id	0	(Range: 0..4095)
Description	[REDACTED]	
Hostname	[REDACTED]	
IP Address	[REDACTED]	
Pri Utility Addr	[REDACTED]	
Sec Utility Addr	[REDACTED]	
Netmask	255.255.255.192	
Gateway	[REDACTED]	
▲ Gw Heartbeat		
State	<input type="checkbox"/> enable	

OK Back

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

Configuration | View Configuration | Q

Modify Network Interface

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

OK | Back

## 7.5. Enable media manager

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

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

Navigate to Media-Manager->Media-Manager

ORACLE Enterprise Session Border Controller

Dashboard Configuration **Monitor and Trace** Widgets

Wizards Commands Save Verify Discard

media-manager > media-manager

Modify Media Manager

State	<input checked="" type="checkbox"/> 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)
Hint Rtcp	<input type="checkbox"/> enable
Algd Log Level	NOTICE
Mbcd Log Level	NOTICE

OK Delete

Show All

ORACLE Enterprise Session Border Controller

Dashboard Configuration **Monitor and Trace** Widgets

Wizards Commands Save Verify Discard

media-manager > media-manager

Modify Media Manager

Media Policing	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> enable

OK Delete

Show All

## 7.6. Configure Realms

Navigate to media-manager > realm-config

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

Config Parameter	Zoom Realm	GenesysCloud Realm
Identifier	Zoom	GenesysCloud
Network Interface	M00	M10
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access Control Trust Level	High	High
Media Sec policy	sdespolicy	sdespolicy
RTCP mux	<input checked="" type="checkbox"/> optional	

### Realm for Zoom Phone –

Configuration [View Configuration](#)  Q

media-manager

codec-policy

media-manager

media-policy

**realm-config**

steering-pool

security

session-router

system

[Show All](#)

**Modify Realm Config**

Identifier	<input type="text" value="Zoom"/>
Description	<input type="text" value="Realm for Zoom Cloud Voice"/>
Addr Prefix	<input type="text" value="0.0.0.0"/>
Network Interfaces	<input type="text" value="M00:0 X"/>
Media Realm List	<input type="text"/>
Mm In Realm	<input checked="" type="checkbox"/> enable
Mm In Network	<input type="checkbox"/> enable
Mm Same Ip	<input type="checkbox"/> enable
QoS Enable	<input type="checkbox"/> enable
Max Bandwidth	<input type="text" value="0"/> (Range: 0..9999999999)
Max Priority Bandwidth	<input type="text" value="0"/> (Range: 0..9999999999)

media-manager	Media Sec Policy	sdesPolicy
media-policy	RTCP Mux	<input type="checkbox"/> enable
realm-config	Ice Profile	
steering-pool	Teams Fqdn	
security	Teams Fqdn In Uri	<input type="checkbox"/> enable

## Realm for Genesys Cloud Cx

Configuration	<a href="#">View Configuration</a>	<input type="text"/> Q
media-manager	Identifier	GenesysCloud
codec-policy	Description	
media-manager	Addr Prefix	0.0.0
media-policy	Network Interfaces	M10:0.4
realm-config	Media Realm List	
steering-pool	Mm In Realm	<input checked="" type="checkbox"/> enable
security		
session-router		
system		

realm-config	Media Policy	
steering-pool	Media Sec Policy	sdesPolicy
security	RTCP Mux	<input type="checkbox"/> enable
session-router	Ice Profile	
system	Teams Fqdn	
	Teams Fqdn In Uri	<input type="checkbox"/> enable
	SDP Inactive Only	<input type="checkbox"/> enable

ORACLE Enterprise Session Border Controller

Dashboard Configuration **Monitor and Trace**

Wizards Commands Save Verify

media-manager

codec-policy

media-manager

media-policy

**realm-config**

steering-pool

security

session-router

system

fraud-protection

host-route

Add Realm Config

Out Translationid

In Manipulationid

Out Manipulationid

Average Rate Limit

Access Control Trust Level

Invalid Signal Threshold

Maximum Signal Threshold

Untrusted Signal Threshold

Nat Trust Threshold

OK Back

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

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

## 7.7. SIP Security Configuration

### 7.7.1 Configuring Certificates

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

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

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

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

GUI Path: security/certificate-record

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

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

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

### Supported CAs for Zoom Phone.

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

### Supported CA for Genesys Cloud Cx BYOC

Genesys Cloud Cx 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.myCloud Cx.com/articles/tls-trunk-transport-protocol-specification/>

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

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

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

#### 7.7.1.1 End Entity Certificate

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

Here in this setup, We will create two end entity certificates for Cloud Cx and Zoom Phone.

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

### Step 1 Configure SBC Certificate Record

To Configure the certificate record:

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

The screenshot shows the 'Modify Certificate Record' configuration page. The left sidebar lists various configuration categories: media-manager, codec-policy, media-policy, realm-config, steering-pool, security, authentication-profile, certificate-record, tls-global, tls-profile, session-router, and system. The 'certificate-record' category is currently selected. The main panel displays the following fields:

Name	SBCZoomCert
Country	US
State	California
Locality	Redwood City
Organization	Oracle Corporation
Unit	
Common Name	customers.telechat.o-test06161977.com
Key Size	2048
Alternate Name	*.customers.telechat.o-test06161977.c
Trusted	<input checked="" type="checkbox"/> enable
Key Usage List	<input type="checkbox"/> digitalSignature <input type="checkbox"/> keyEncipherment
Extended Key Usage List	<input type="checkbox"/> serverAuth
Key Algor	RSA

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

Configuration View Configuration Q

media-manager >

security >

authentication-profile

certificate-record

tls-global

tls-profile

session-router >

system >

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	<input checked="" type="checkbox"/> enable
Key Usage List	<input type="checkbox"/> digitalSignature <input type="checkbox"/> keyEncipherment
Extended Key Usage List	<input type="checkbox"/> serverAuth <input type="checkbox"/> clientAuth
Key Algor	rsa
Digest Algor	sha256
Ecdsa Key Size	p256
Cert Status Profile List	

Show All

OK Back

## Step 2 – Generating a certificate signing request

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

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

Configuration View Configuration Q

media-manager >

security >

authentication-profile

certificate-record

tls-global

tls-profile

session-router >

system >

Certificate Record

Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
		BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberTrust Root
		DigiCertRoot	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	US	California	Redwood City	Oracle Corporation		telechat-o-test0816977.com

Discard  Verify  Save

Search Q

Actions: Edit, Copy, Delete, Generate, Import, Sort

Generate certificate response

Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIICzCCAcQwggDgMA0GCSqGSIb3DQEBAQDwIBG4UEChMGT3A20iEVlvcBxrnFQ
FTAT8qBwAC7TnJzLzhdBzGQ2Q2iTE98kG4UEChMGT3A20iEVlvcBxrnFQ
aWVuhISQwggDgMA0GCSqGSIb3DQEBAQDwIBG4UEChMGT3A20iEVlvcBxrnFQ
CSqGSIb3DQEBAQDwIBG4UEChMGT3A20iEVlvcBxrnFQ
-----END CERTIFICATE REQUEST-----
```

Common Name

- DigiCert SHA2 Secure Server CA
- DigiCert Global Root CA
- GoDaddy Secure Server CA
- GoDaddy Class2 Root CA
- telechat.o-test06101977.com

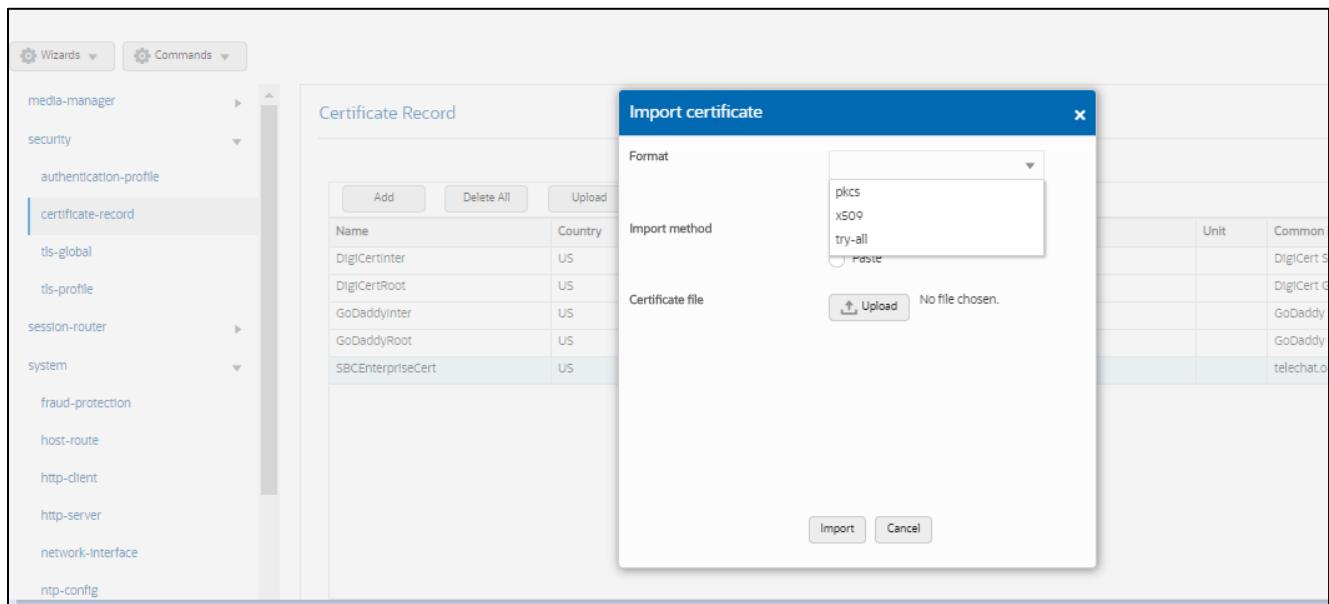
- copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, **a save and activate is required** before you can import the certificates to each certificate record created above.

### 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

Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
⋮	□	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberTrust Root
⋮	□	DigiCertRoot	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.cgbutherford.com
⋮	□	TeamsE	US	California	Redwood City	Oracle Corporation		telechat.o-test06101977.com



### 7.7.1.2 Import CA Certificate

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

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

## 7.8. TLS-Profile

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

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

### **TLS profile -Zoom Phone.**

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

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

media-manager  
security  
authentication-profile  
certificate-record  
tls-global  
tls-profile  
session-router  
system

Modify TLS Profile

Name: TLSZoom

End Entity Certificate: SBCEnterpriseCert

Trusted Ca Certificates: GoDaddyInter, GoDaddyRoot

Cipher List: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_C

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

Mutual Authenticate:  enable

TLS Version: tlsv12

Options:

Cert Status Check:  enable

Cert Status Profile List:

OK Back

Show All

## TLS-Profile - Genesys Cloud Cx

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

Supported TLS ciphers include:

- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256

TLS-only listeners are available on host port 5061.

## 7.9. Configure SIP Interfaces

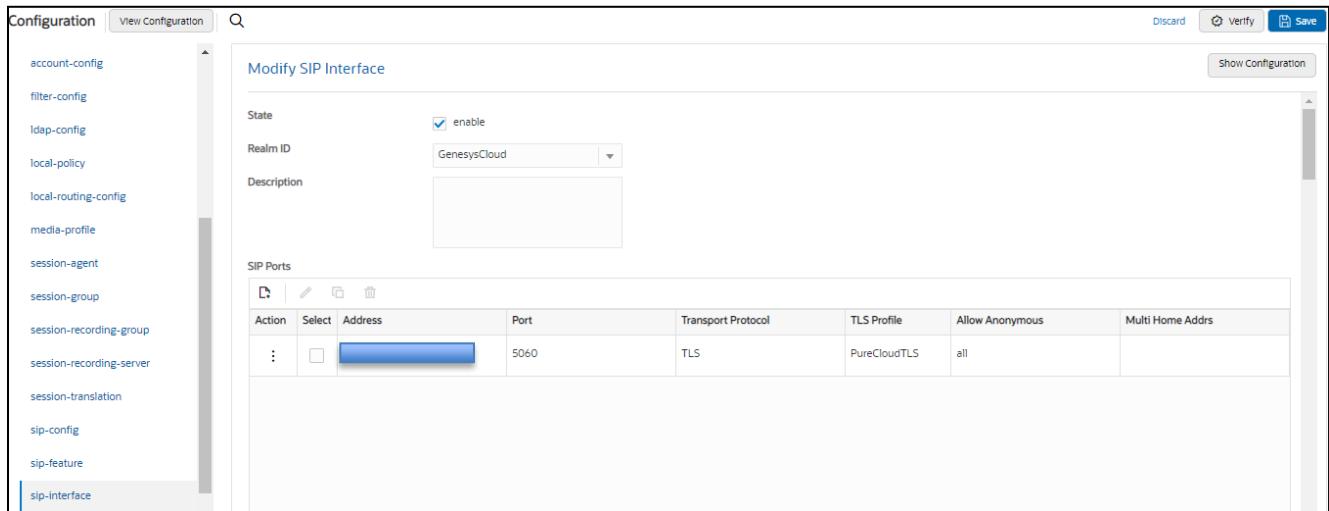
Navigate to session-router> sip-interface and configure the sip-interface as shown below.

Please Configure sip-interface for the Cloud Cx as below-

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

### Sip-Interface for Zoom Phone

### Sip-interface for Genesys Cloud Cx



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

## 7.10. Configure session-agent

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

Navigate to session-router->Session-Agent

### Configure the session-agents for the Genesys Cloud Cx

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

Configuration View Configuration Q

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:

Discard Verify Save Show Configuration

### Configure the session-agents for Zoom.

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

Configuration View Configuration Q

Modify Session Agent

Hostname: 162.12.232.59

IP Address: 162.12.232.59

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

State:  enable

App Protocol: SIP

App Type:

Transport Method: StaticTLS

Realm ID: Zoom

Egress Realm ID:

Description: SA to Zoom Cloud Voice

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

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

## 7.11. Configure session-agent group

A session agent group allows the SBC to create a load balancing model.

Go to Session-Router->Session-Group. Please configure the following group for Zoom Session Agents

Configuration | View Configuration | Q

local-policy

local-routing-config

media-profile

session-agent

session-group

session-recording-group

session-recording-server

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

sip-monitoring

translation-rules

Show All

Modify Session Group

Group Name: ZoomGrp

Description:

State:  enable

App Protocol: SIP

Strategy: Hunt

Dest: 162.12.232.59, 162.12.233.59

Trunk Group:

Sag Recursion:  enable

Stop Sag Recurse: 401.407

SIP Recursion Policy:

OK | Back

## 7.12. Configure local-policy

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

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

Inbound calls from Cloud Cx to Zoom Phone –

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

Inbound calls from Zoom Phone to Cloud Cx -

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

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

Below is the Link to Oracle TechNet Page

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

Oracle SBC interworking with Genesys Cloud Cx and Twilio SIP Trunk Application Note can be found here

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

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

**Modify Local Policy (Top Screenshot):**

Action	Select	Next Hop	Realm	Action	Terminate Recurs...	Cost	State	App Protocol	Lookup	Next Key
:	<input type="checkbox"/>	68.68.117.67	SIPTrunk	none	disabled	0	enabled		single	

**Modify Local Policy (Bottom Screenshot):**

Action	Select	Next Hop	Realm	Action	Terminate Recurs...	Cost	State	App Protocol	Lookup	Next Key
:	<input type="checkbox"/>	sag:ZoomGrp	Zoom	none	disabled	0	enabled		single	

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

[Configuration](#)

[View Configuration](#)

**Modify Local Policy**

From Address

To Address

Source Realm

Description

State

 enable

Policy Priority

**Policy Attributes**

Action	Select	Next Hop	Realm	Action	Terminate Recurs...	Cost	State	App Protocol	Lookup
:	<input type="checkbox"/>	68.68.117.67	SIPTrunk	none	disabled	0	enabled		single

**Modify Local Policy**

From Address

To Address

Source Realm

Description

State

 enable

Policy Priority

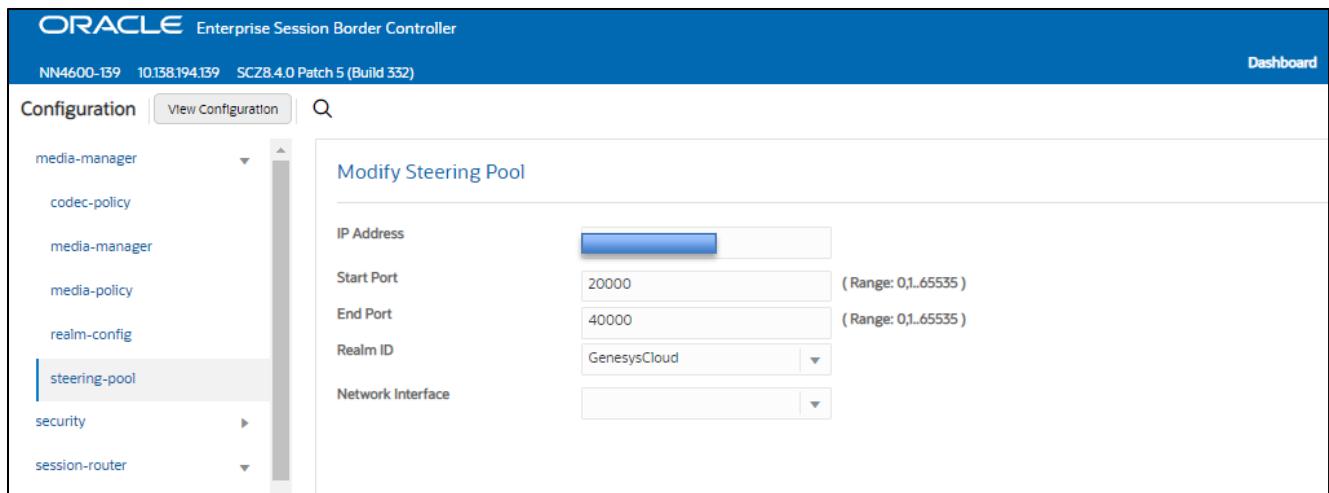
**Policy Attributes**

Action	Select	Next Hop	Realm	Action	Terminate Recurs...	Cost	State	App Protocol	Lookup	Next Key
:	<input type="checkbox"/>	byoc-voxal.byoc.m...	byoc-voxal	none	disabled	0	enabled		single	

## 7.13. Configure steering-pool

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

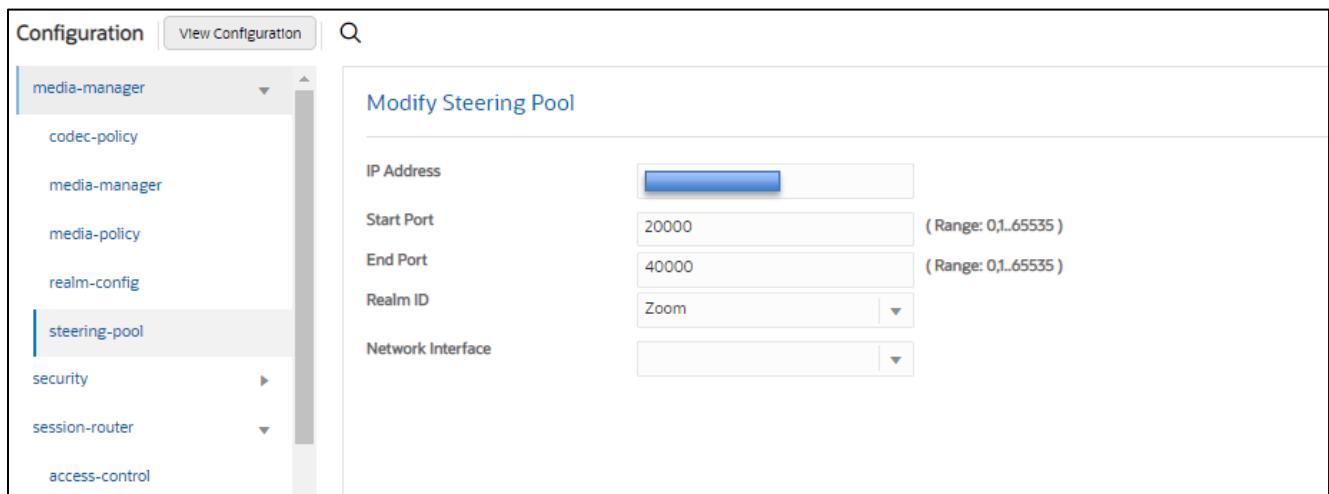
### Cloud Cx Steering pool.



Modify Steering Pool

IP Address	<input type="text"/>
Start Port	20000 (Range: 0..65535)
End Port	40000 (Range: 0..65535)
Realm ID	GenesysCloud
Network Interface	<input type="text"/>

### Zoom Phone Steering Pool



Modify Steering Pool

IP Address	<input type="text"/>
Start Port	20000 (Range: 0..65535)
End Port	40000 (Range: 0..65535)
Realm ID	Zoom
Network Interface	<input type="text"/>

## 7.14. Configure additional Parameters

### 7.14.1 SIP Manipulations

For calls to be presented to Zoom Phone from the Oracle SBC, the Oracle SBC requires alterations to the SIP signaling natively created. To do this, we should use the prebuilt HMR ACME\_NAT\_TO\_FROM\_IP

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

The manipulation performs the following modifications to SIP packets

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

## 7.14.2 Enable Ping-response

The option is found under the **Session agent** configuration element and will be enabled on all session agents configured for Zoom Phone and Genesys Cloud Cx .

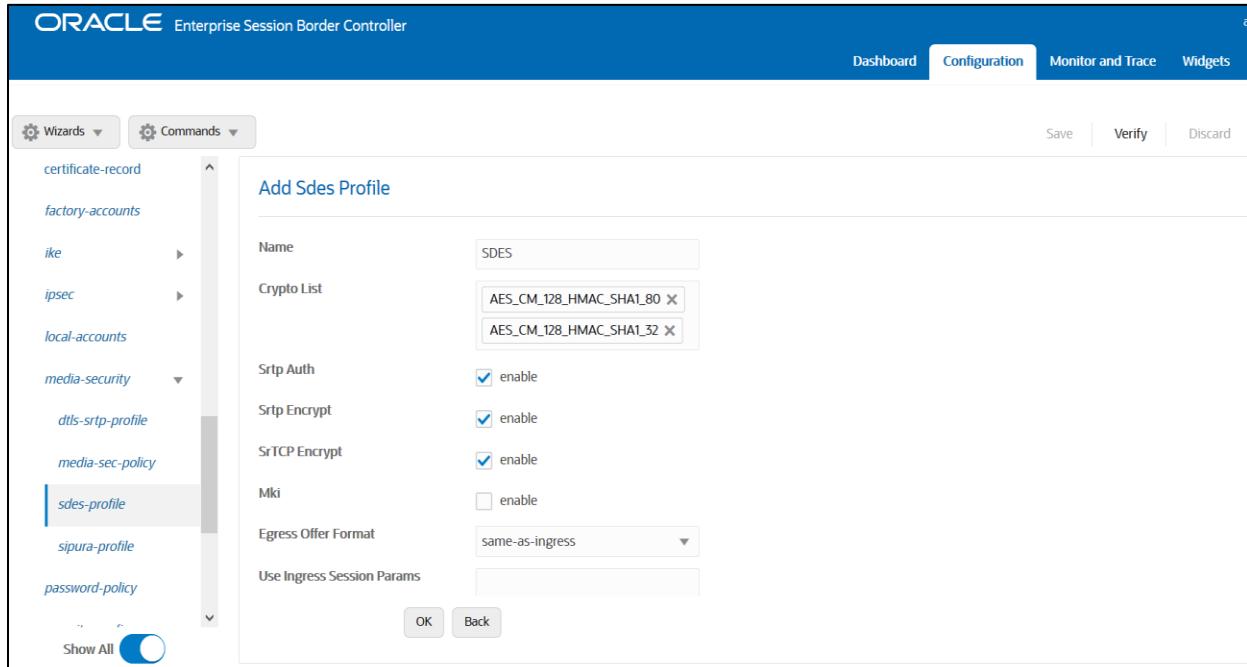
Below is an example of the parameter **Ping response** enabled on Cloud Cx Session-Agent. Similarly, the parameter should be enabled for other Zoom Phone Session-Agents.

## 7.15. Media Security Configuration.

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

### 7.15.1 Configure sdes profile

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



The screenshot shows the 'Add Sdes Profile' dialog in the ORACLE Enterprise Session Border Controller (ESBC) Configuration interface. The 'Name' field is set to 'SDES'. The 'Crypto List' contains two entries: 'AES\_CM\_128\_HMAC\_SHA1\_80' and 'AES\_CM\_128\_HMAC\_SHA1\_32'. The 'Srtp Auth', 'Srtp Encrypt', and 'SrTCP Encrypt' checkboxes are checked and set to 'enable'. The 'Mki' checkbox is unchecked and set to 'enable'. The 'Egress Offer Format' dropdown is set to 'same-as-ingress'. The 'Use Ingress Session Params' field is empty. At the bottom, there are 'OK' and 'Back' buttons.

### 7.15.2. Configure Media Security Profile

Navigate to →Security → Media Security →media Sec policy and create the policy as below:  
Create Media Sec policy with name SDES, which will have the sdes profile, created above.

**Assign this media policy to both Cloud Cx and Zoom Phone Realm.**

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

Add Media Sec Policy

Name: SDES

Pass Through:  enable

Options:

**Inbound**

Profile: SDES

Mode: srtp

Protocol: sdes

Hide Egress Media Update:  enable

**Outbound**

OK Back

certificate-record  
factory-accounts  
ike  
ipsec  
local-accounts  
media-security  
    dtls-srtp-profile  
        media-sec-policy  
        sdes-profile  
        sipura-profile  
    password-policy  
Show All

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

Wizards Commands

admin-security  
auth-params  
authentication  
authentication-profile  
cert-status-profile  
certificate-record  
factory-accounts  
ike  
ipsec  
local-accounts  
media-security  
    dtls-srtp-profile  
        media-sec-policy  
Show All

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

OK Back

## 7.16 Access Control

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

GUI Path: session-router/access-control

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

**byoc.myCloud Cx.com resolves to the following load balancer IP Addresses**

52.203.12.137 [lb01.byoc.us-east-1.myCloud Cx.com](#)  
54.82.241.192 [lb02.byoc.us-east-1.myCloud Cx.com](#)  
54.82.241.68 [lb03.byoc.us-east-1.myCloud Cx.com](#)  
54.82.188.43 [lb04.byoc.us-east-1.myCloud Cx.com](#)

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

Configuration | View Configuration | Q

media-manager >

security

authentication-profile

certificate-record

tls-global

tls-profile

session-router >

access-control

account-config

filter-config

ldap-config

local-policy

local-routing-config

media-profile

session-agent

session-group

session-recording-group

session-recording-server

Show All

Modify Access Control

Realm ID: GenesyCloud

Description: (redacted)

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)

OK | Back

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

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

## 7.17 SBC Behind NAT SPL configuration

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

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

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

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

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

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

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

HeaderNatPublicSIPIfIp=52.151.236.203,HeaderNatPrivateSIPIfIp=10.0.4.4

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

The configuration dialog is titled 'Modify Realm Config'. The left sidebar shows a tree structure with 'realm-config' selected. The main dialog contains the following configuration options:

- Early Media Allow: A dropdown menu.
- Enforcement Profile: A dropdown menu.
- Additional Prefixes: A text input field.
- Restricted Latching: A dropdown menu with 'none' selected.
- Options: A text input field.
- SPL Options: A text input field with the value 'HeaderNatPublicSIPfip=52.151.236.20'.
- Delay Media Update: A checkbox labeled 'enable'.
- Refer Call Transfer: A dropdown menu with 'disabled' selected.
- Hold Refer Reinvite: A checkbox labeled 'enable'.
- Refer Notify Provisional: A dropdown menu with 'none' selected.
- Dyn Refer Term: A checkbox labeled 'enable'.

At the bottom of the dialog are 'OK' and 'Back' buttons.

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

## 7.18 Caveat -OPUS Transcoding

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

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

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

## 8. Configuring the Oracle SBC through Config Assistant

When you first log on to the Oracle SBC, the system requires you to set the configuration parameters necessary for basic operation. To help you set the initial configuration with minimal effort, the SBC provides the Configuration Assistant.

The Configuration Assistant, which you can run from the Web GUI or the Acme Command Line Interface (ACLI), asks you questions and uses your answers to set parameters for managing and securing call traffic. You can use the Configuration Assistant for the initial set up to make to the basic configuration. Please check "Configuration Assistant Operations" in the [Web GUI User Guide](#) and "Configuration Assistant Workflow and Checklist" in the [ACLI Configuration Guide](#)

Please note, applying a configuration to the SBC via the Configuration Assistant will overwrite any existing configuration currently applied to the SBC. **We highly recommend this only be used for initial setup of the SBC. This feature is not recommended to be used to make changes to existing configurations.**

Configuration package is available starting in release nnSCZ840p7 and nnSCZ900p2.

### Section Overview and Requirements

This section describes how to use our Configuration Assistant feature as a quick and simple way to configure the Oracle SBC for integration with Genesys Cloud Cx. We will choose a Generic SIP Trunk on the other Side for Carrier Connectivity. We also have configuration Assistant for Zoom Phone related to Zoom Phone configuration. Please follow the latest Zoom Phone Application Note to get instructions on configuring Zoom Phone via Configuration Assistant Template.

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

The pre-requisites are given below.

- SBC running release SCZ840p7 or later which will have this template package by default added to the SBC code.
- TLS certificate for the SBC preferably in PKCS format, or access to Cloud Cx 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

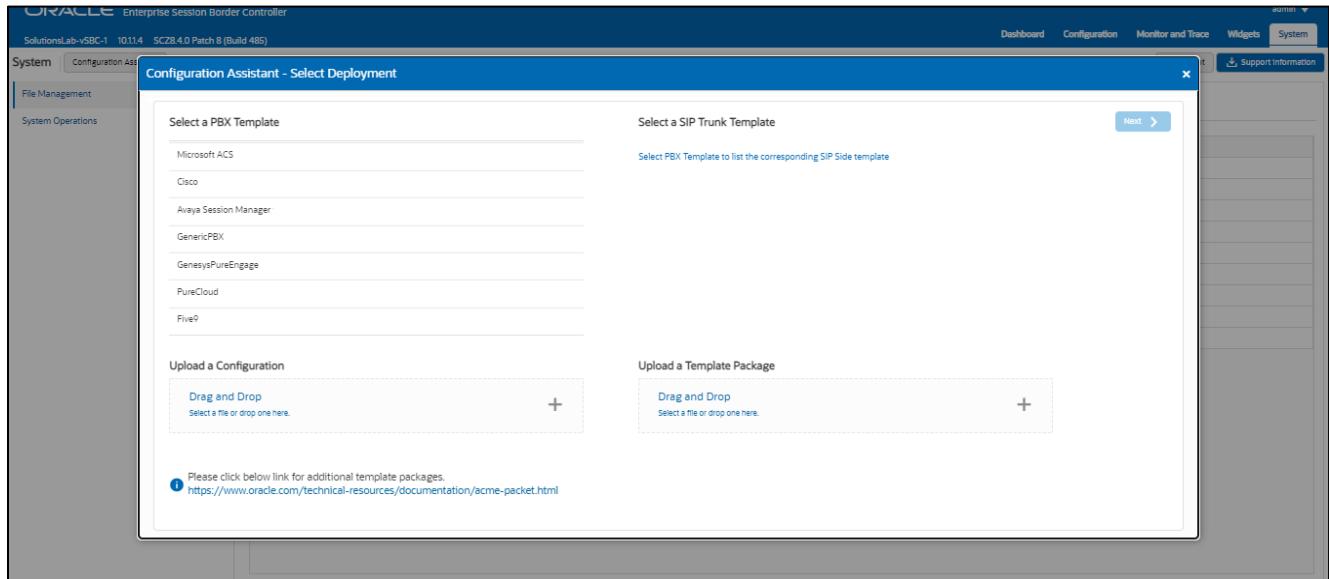
The Oracle SBC WebGui can be accessed by entering the following in your web browser.  
http(s)://<SBC Management IP>.

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

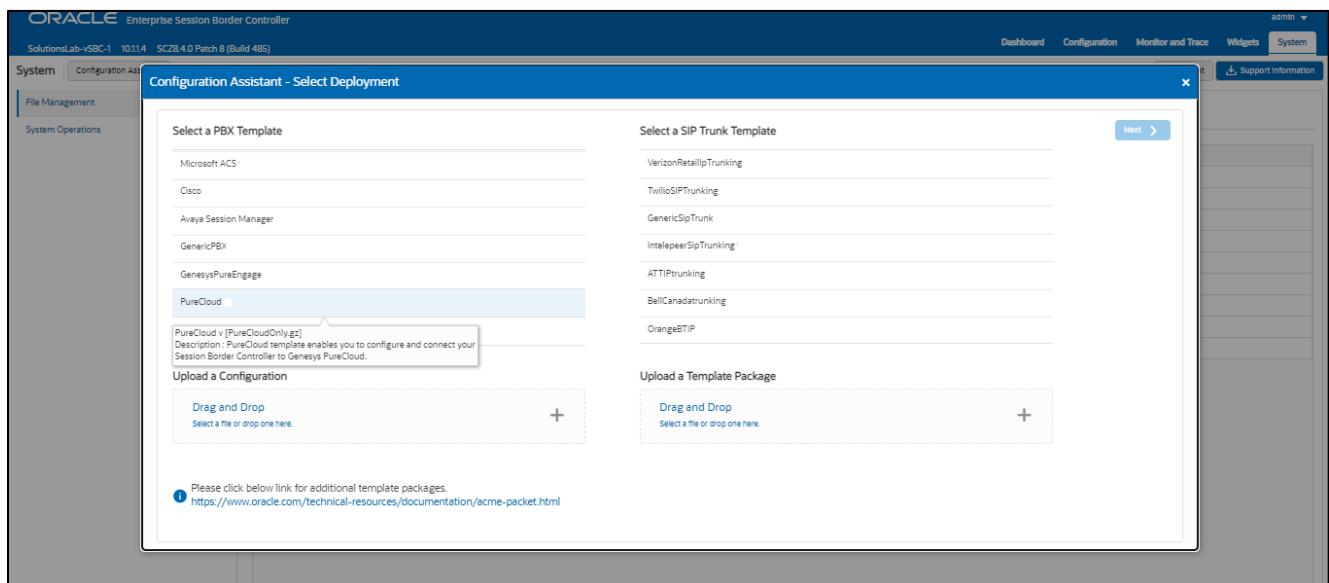
If there is no configuration on the SBC, the configuration assistant will show immediately upon login to the SBC GUI as shown below

## Cloud Cx Configuration Assistant

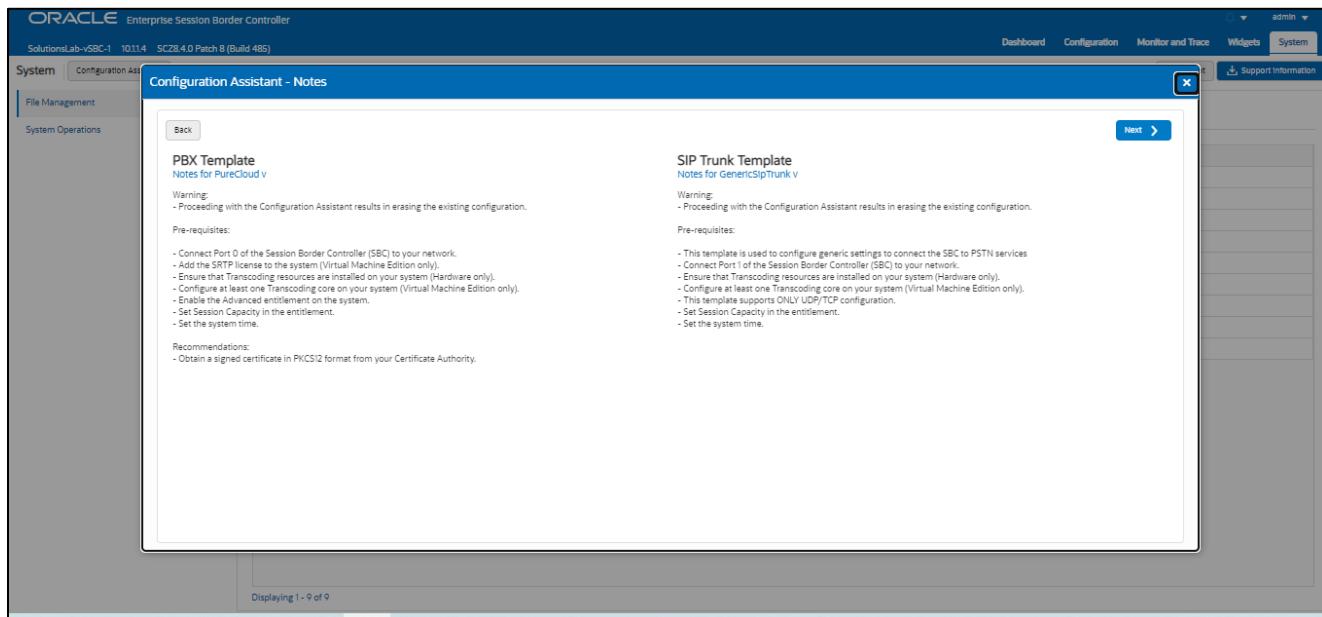
For a new SBC deployment, once access to the GUI is configured, you will see the following when logging in for the first time:



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



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



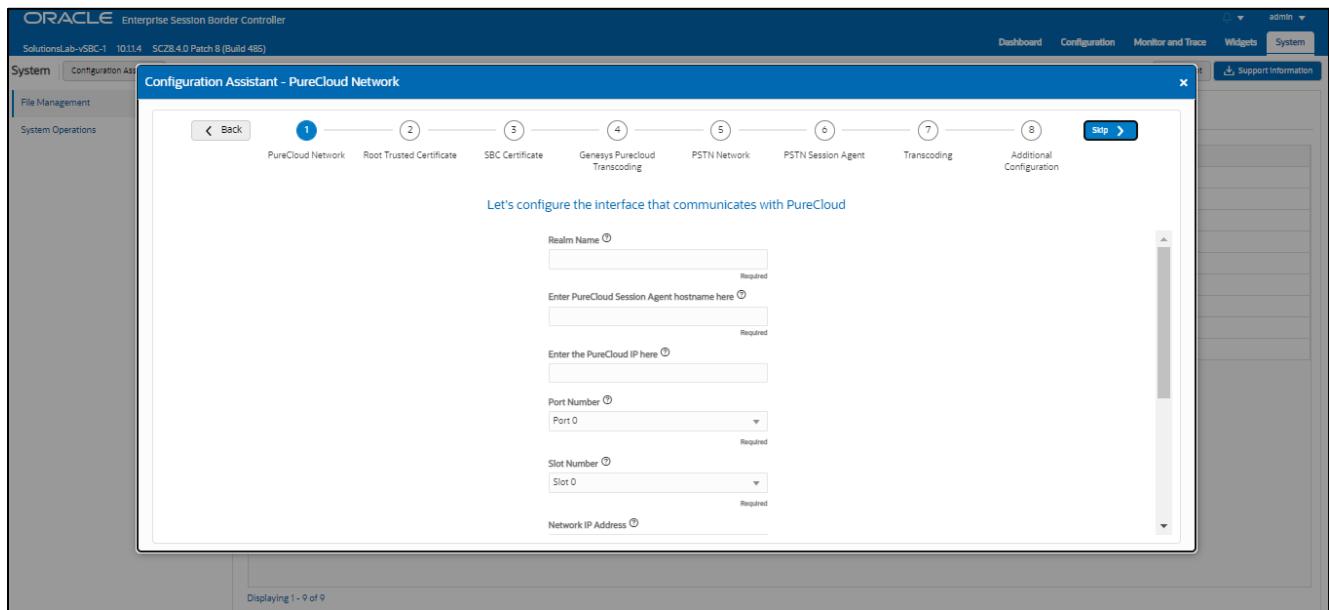
Clicking “Next” on the Notes page triggers the configuration assistant to do a system check. This ensures that all of the system requirements for the platform and sip trunk you have selected have been met before proceeding to configuration pages. If they have not been met, you will be greeted by a page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

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

## Page 1- Cloud Cx Network

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

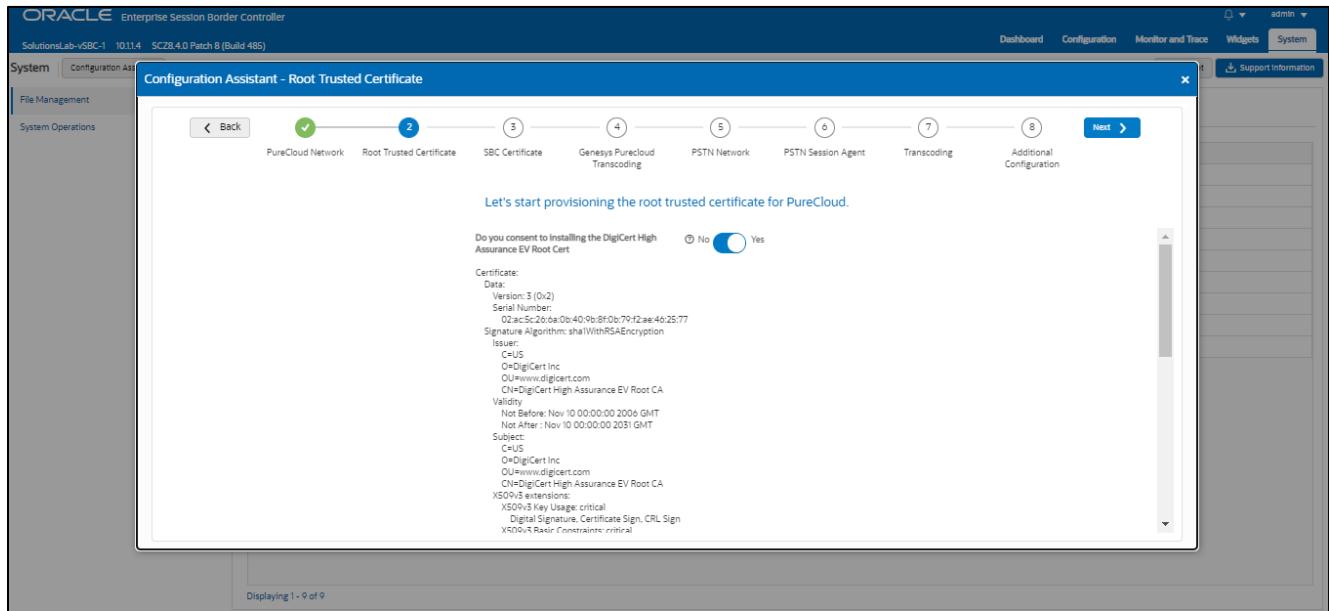
Next to each field is a help icon. If you hover over the icon, you will be provided with a description or definition of each field. Also, pay close attention to which fields are listed as “required”.



## Page 2 - Import DigiCert Trusted CA Certificate for Cloud Cx

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

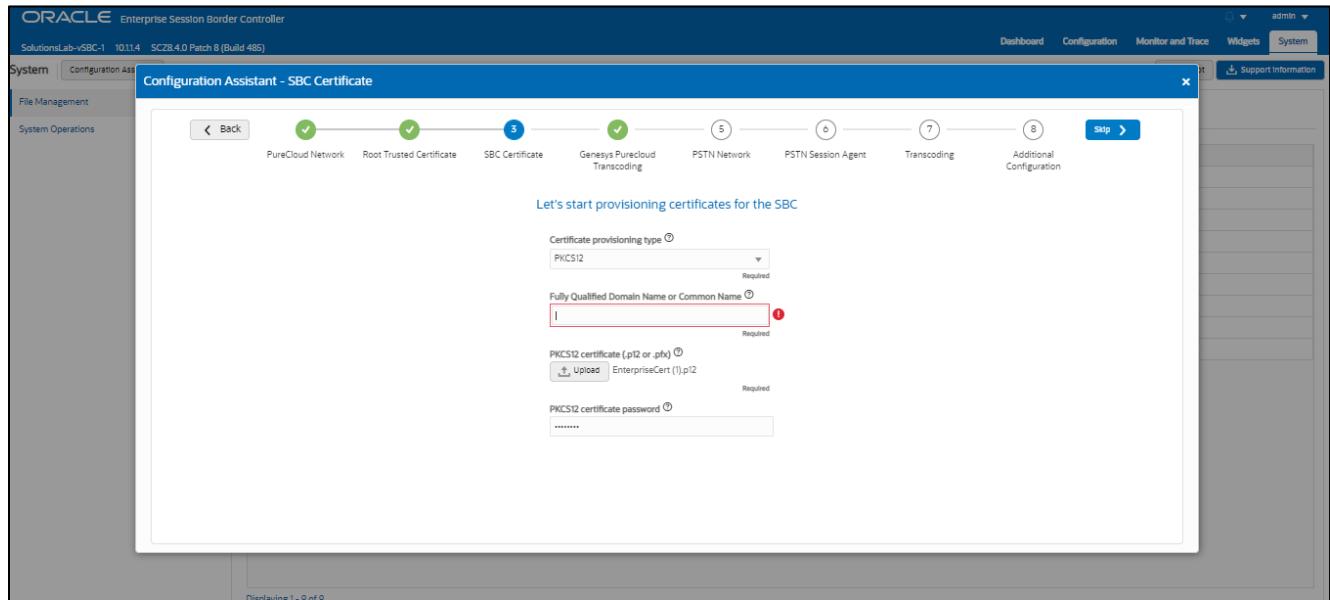
Importing the Cloud Cx Root CA certs is enabled by default.



## Page 3 - SBC Certificates for Cloud Cx side

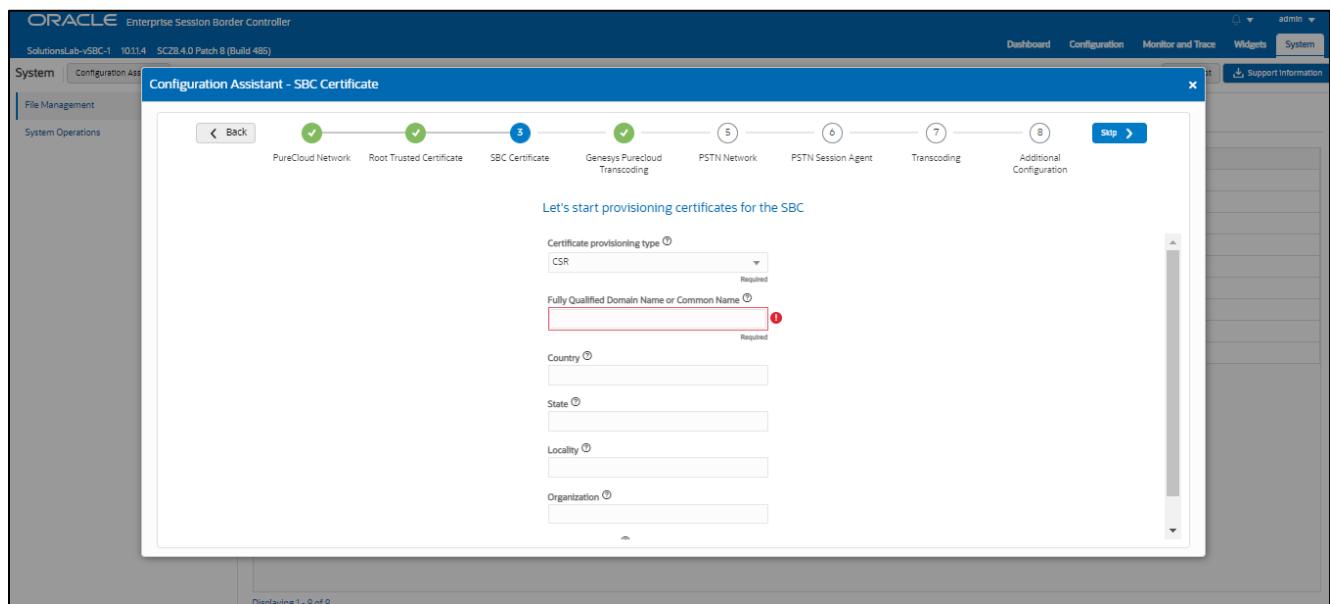
By default, the SBC is set to import a certificate in PKCS12 format. This is the simplest and recommended way to add a certificate to the Oracle SBC. Using this method, you will add the SBC's hostname under "FQDN or

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



### Certificate Signing Request (CSR)

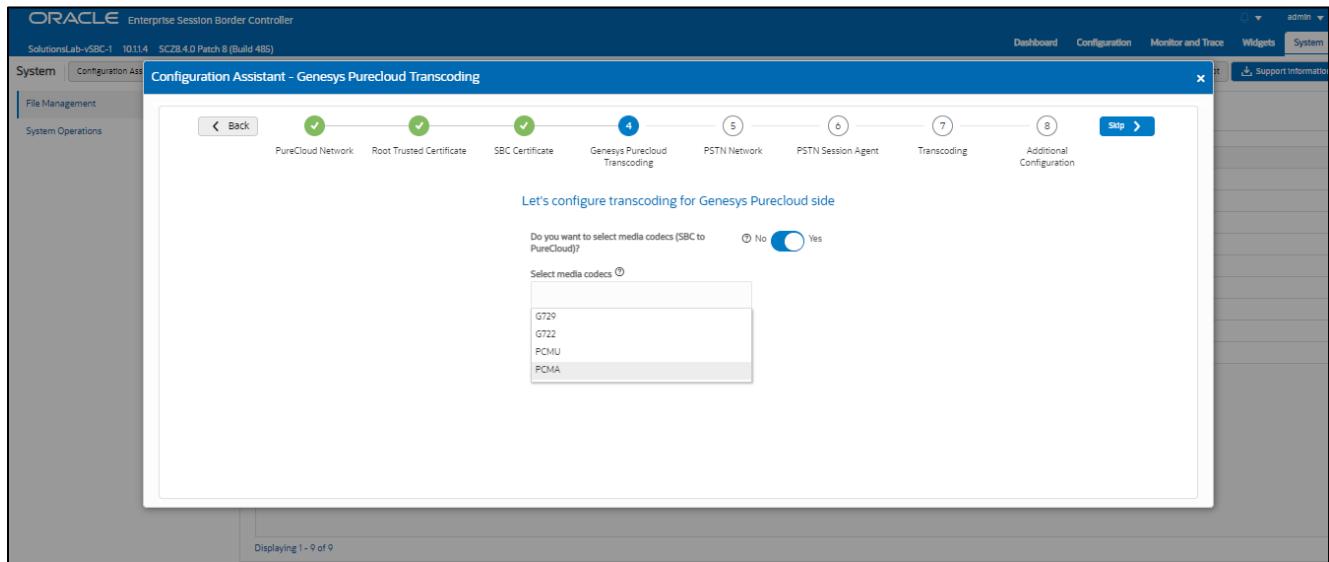
The alternative to importing a PKCS12 certificate to the SBC is to configure a certificate and generate a certificate signing request that you will have signed by a Cloud Cx supported CA. Same as PKCS12, you will enter the SBC's hostname under "FQDN or Common Name" and "Country" field (required) and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



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

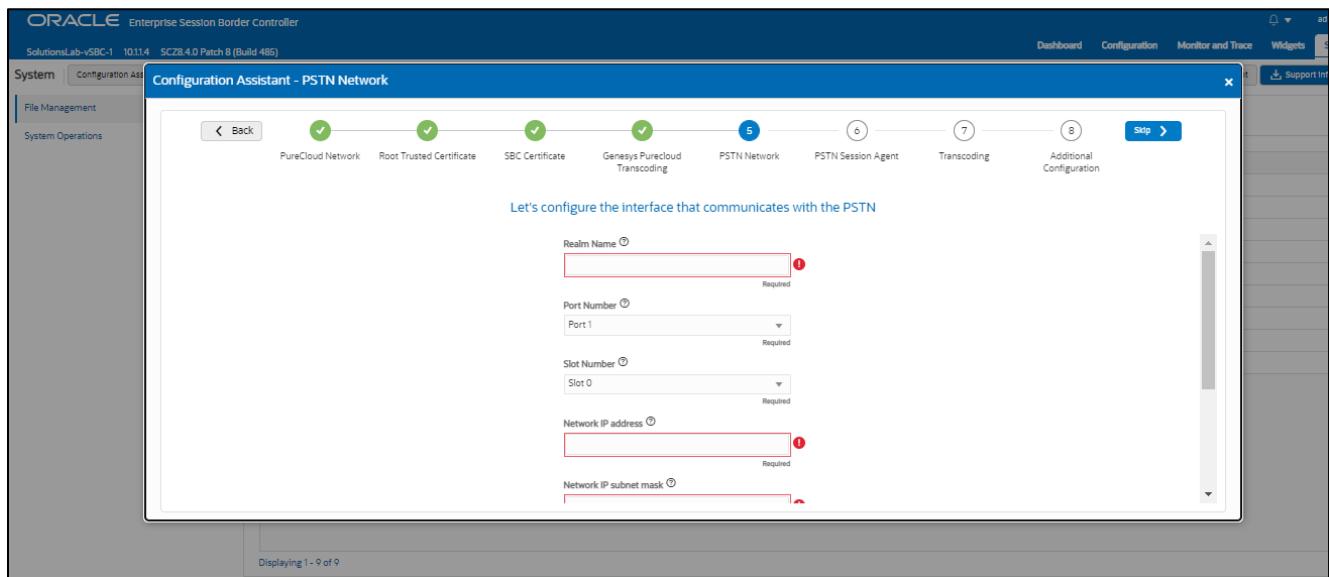
Once transcoding features is set to “yes”, you will then have an option to select additional media codecs you want included in offers/answers toward Cloud Cx. If you select yes to either question regarding media codecs, you will be presented with a required drop down.

You can select as many codecs from the list presented.



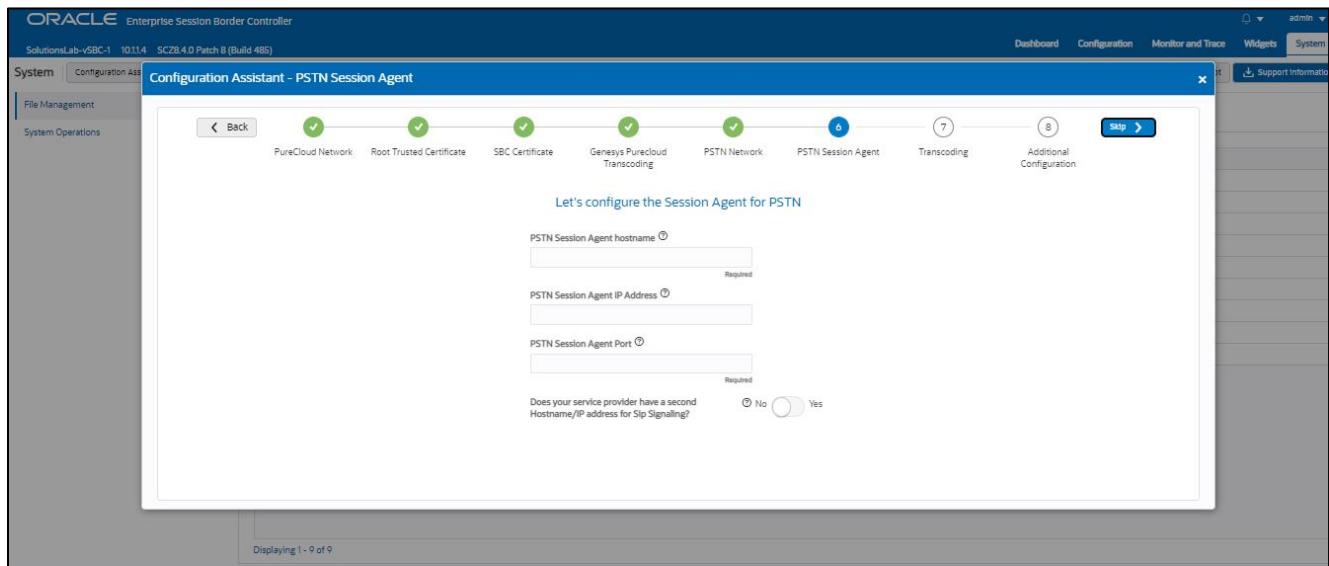
## Page 5 – PSTN Sip Trunk Network

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



## Page 6 – PSTN Session Agent

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

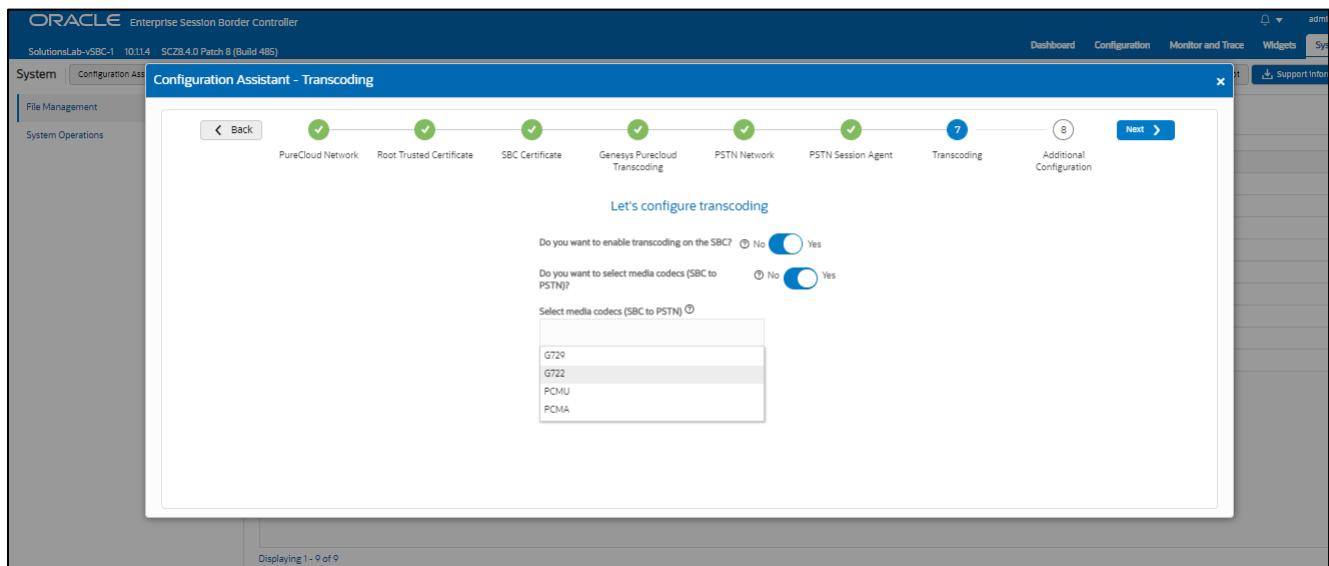


Please fill the required fields and click Next.

## Page 7 - PSTN side Transcoding

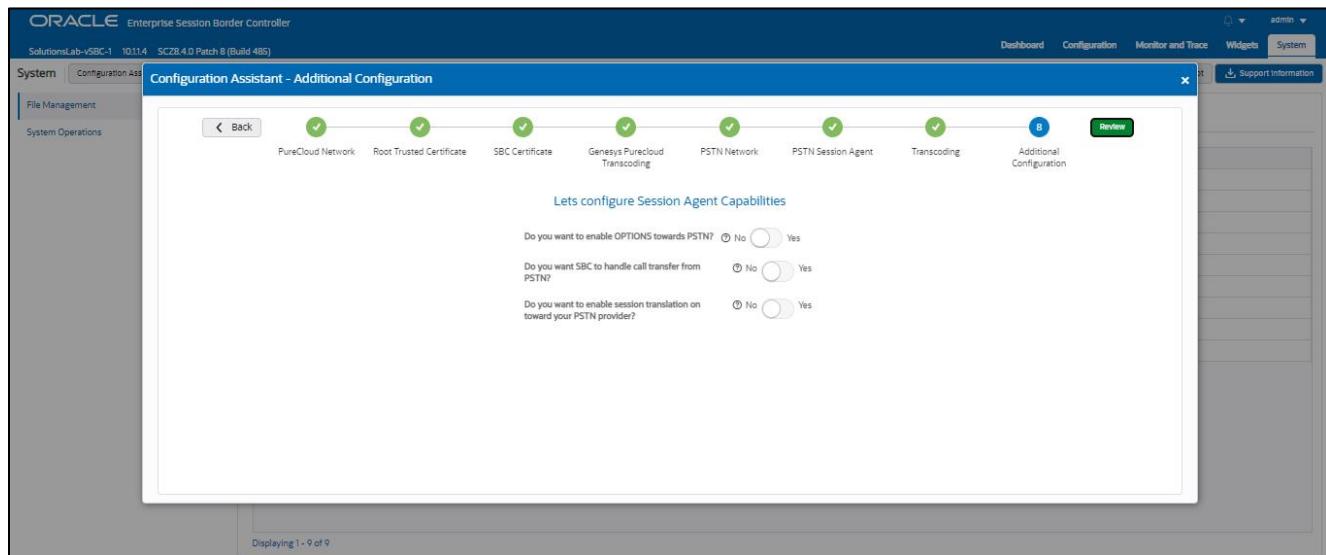
Page 7 is where you will be able to configure transcoding between the SBC and PSTN Trunk.

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



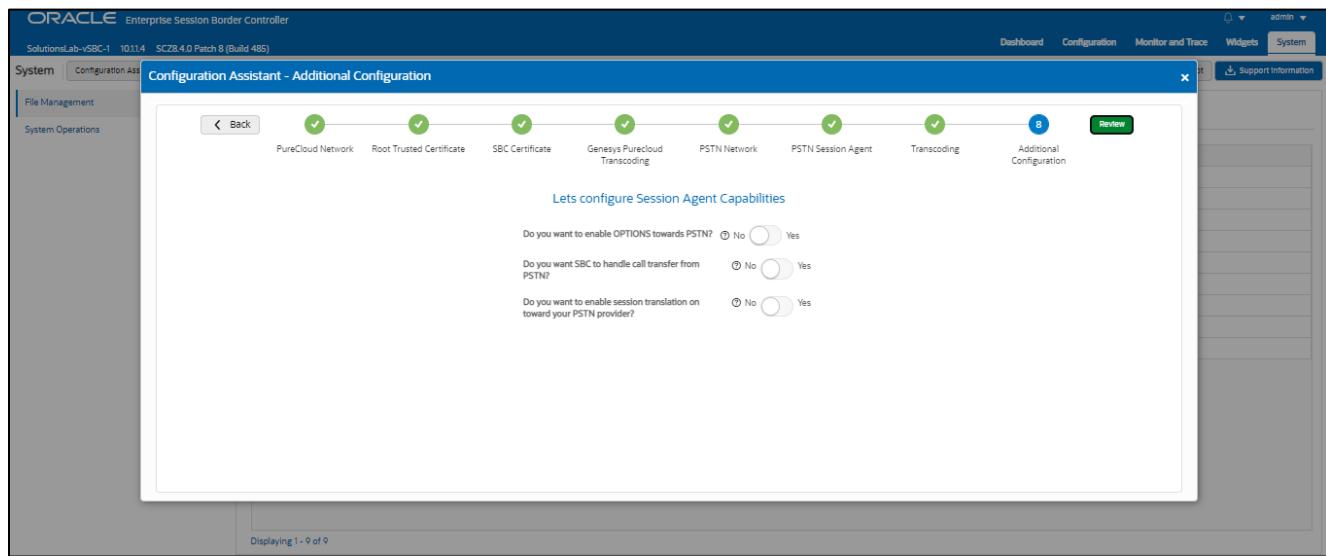
## Page 8 – Additional Configuration

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



## Review

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



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

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

The screenshot shows the Oracle Enterprise Session Border Controller (SBC) Configuration Assistant - Summary page. On the left, there are two main sections: 'PureCloud Network' and 'Root Trusted Certificate'. The 'PureCloud Network' section contains fields for Realm Name (purecloud), PureCloud (purecloud.com), Enter the PureCloud IP here (Port 0), Slot Number (Slot 0, Network IP Address 141.146.36.09, Network IP subnet mask 255.255.255.192, Primary DNS server IP Address DNS Domain), and a 'Edit' button. The 'Root Trusted Certificate' section asks if consent is given to install the DigiCert High Assurance EV Root Cert, with an 'Edit' button. On the right, there is a 'Configuration' tab showing detailed ACLI output for a certificate record named 'PureCloudCSR' with various attributes like common-name, state, organization, and unit. Below it is a 'CSR Certificate' tab. At the bottom, a note says 'Displaying 1 - 9 of 9'.

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.

This screenshot is similar to the previous one but shows a 'CSR Certificate' tab instead of a 'Configuration' tab. The left side has the same 'PureCloud Network' and 'Root Trusted Certificate' sections. The right side shows the 'CSR Certificate' tab with detailed ACLI output for a certificate record named 'PureCloudCSR CSR'. The output starts with '-----BEGIN CERTIFICATE REQUEST-----' and ends with '-----END CERTIFICATE REQUEST-----'. The text is a long string of hex and ASCII characters.

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 Cloud CxPhone 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 Cloud Cx and Twilio SIP Trunk via Oracle SBC.

Test	Description	Pas s	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	



CONNECT WITH US



[blogs.oracle.com/oracle](http://blogs.oracle.com/oracle)



[facebook.com/Oracle/](http://facebook.com/Oracle/)



[twitter.com/Oracle](http://twitter.com/Oracle)



[oracle.com](http://oracle.com)

**Oracle Corporation, World Headquarters**

500 Oracle Parkway  
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**

Phone: +1.650.506.7000  
Fax: +1.650.506.7200

**Integrated Cloud Applications & Platform Services**

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

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

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