



Oracle SBC integration with Genesys  
Cloud Cx BYOC and Microsoft Teams  
Direct Routing

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.

## Revision History

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

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with Genesys Cloud Cx and Microsoft Teams	07 July 2021
1.1	Oracle Public IP Addresses masked	18 Nov 2021
1.2	Removed sip-all FQDN Added New Access Control	12 Jan 2022
1.3	Added New Section Cloud Cx Configuration Assistant	27 Jan 2022
1.4	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. MICROSOFT TEAMS.....	6
2.2. GENESYS CLOUD CX.....	6
<b>3. REQUIREMENTS .....</b>	<b>6</b>
3.3. ARCHITECTURE.....	7
<b>4. CONFIGURE GENESYS CLOUD CX .....</b>	<b>8</b>
4.1 EXTERNAL TRUNK CONFIGURATION .....	8
4.1.1 Create a new External Trunk.....	9
4.1.2 Set Inbound SIP Termination Identifier .....	9
4.1.3 Set Outbound SIP Servers or Proxies .....	10
4.1.4 Set Calling Address .....	10
4.1.5 Set SIP Access Control .....	10
4.1.6 Enable E.164 format.....	11
4.2 SITE CONFIGURATION .....	11
4.2.1 Create a New Site .....	11
4.2.2 Number Plans & Classifications.....	12
4.2.3 Configure outbound route .....	13
4.2.4 Phone configuration.....	13
4.2.5 Simulate call.....	14
4.3 DID ASSIGNMENT.....	15
4.3.1 Create DID Range .....	15
4.3.2 Assign DID to User. ....	15
4.4. ARCHITECT FLOW FOR INBOUND WELCOME PROMPT .....	16
<b>5. CONFIGURE MICROSOFT TEAMS DIRECT ROUTING .....</b>	<b>16</b>
5.1. ACCESS TEAMS ADMIN CENTER .....	16
5.2. CONFIGURE ONLINE PSTN GATEWAY .....	17
5.3. CONFIGURE ONLINE PSTN USAGE.....	17
5.4. CONFIGURE ONLINE VOICE ROUTES .....	18
5.5. CONFIGURE ONLINE VOICE ROUTING POLICY .....	18
5.6. ASSIGN VOICE ROUTING POLICY TO USERS.....	19
<b>6. CONFIGURING THE SBC .....</b>	<b>20</b>
6.1. VALIDATED ORACLE SBC VERSION .....	20
6.2 NEW SBC CONFIGURATION.....	21
6.2.1 Establishing a serial connection to the SBC .....	21
6.2.2 Configure SBC using Web GUI.....	24
6.3. CONFIGURE SYSTEM-CONFIG.....	25
6.4. CONFIGURE PHYSICAL INTERFACE VALUES .....	26
6.5. CONFIGURE NETWORK INTERFACE VALUES .....	28
6.6. ENABLE MEDIA MANAGER.....	29
6.7. CONFIGURE REALMS.....	30
6.8. SECURITY CONFIGURATION .....	34
6.8.1 Configuring Certificates .....	34
6.8.1.1 End Entity Certificate .....	35
6.8.1.2 Import CA Certificate .....	38
6.9. TLS-PROFILE.....	38

6.10. CONFIGURE SIP INTERFACES .....	40
6.11. CONFIGURE SESSION-AGENT .....	41
6.12. CONFIGURE SESSION-AGENT GROUP .....	43
6.13. CONFIGURE LOCAL-POLICY .....	43
6.13. CONFIGURE STEERING-POOL .....	46
6.14. CONFIGURE ADDITIONAL PARAMETERS.....	46
6.15. CONFIGURE MEDIA PROFILE AND CODEC POLICY .....	49
6.18. CONFIGURE ICE PROFILE .....	50
6.15. CONFIGURE SDES PROFILE.....	51
6.16. CONFIGURE MEDIA SECURITY PROFILE.....	51
6.17 CONFIGURE RTCP POLICY AND RTCP MUX .....	52
6.18 ACCESS CONTROL.....	53
<b>7. CONFIGURING THE ORACLE SBC THROUGH CONFIG ASSISTANT.....</b>	<b>55</b>
SECTION OVERVIEW AND REQUIREMENTS .....	55
INITIAL GUI ACCESS .....	56
CLOUD CX CONFIGURATION ASSISTANT.....	56
PAGE 1- CLOUD CX NETWORK .....	58
PAGE 2 - IMPORT DIGICERT TRUSTED CA CERTIFICATE FOR CLOUD CX.....	58
PAGE 3 - SBC CERTIFICATES FOR CLOUD CX SIDE .....	59
PAGE 4 – CLOUD CX SIDE TRANSCODING.....	60
PAGE 5 – PSTN SIP TRUNK NETWORK.....	61
PAGE 6 – PSTN SESSION AGENT.....	61
PAGE 7 - PSTN SIDE TRANSCODING.....	61
PAGE 8 – ADDITIONAL CONFIGURATION.....	62
REVIEW .....	63
DOWNLOAD AND/OR APPLY .....	64
CONFIGURATION ASSISTANT ACCESS .....	64
<b>8. TEST PLAN EXECUTED .....</b>	<b>64</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 Microsoft Teams Direct Routing.

## 2. Document Overview

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

It should be noted that the SBC configuration provided in this guide focuses strictly on the Genesys Cloud Cx and Microsoft Teams related parameters. Microsoft Teams Direct Routing is the Microsoft's BYOC so the calls To and From MS Teams to 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-twillio-sip-trunkv0.3.pdf> as a reference to configure the Twilio SIP Trunk with Oracle SBC.

Related documentation can be found below –

## 2.1. Microsoft Teams

Microsoft Phone System Direct Routing allows connection of a supported customer-provided Session Border Controller (SBC) to a Microsoft Phone System. Direct Routing enables using virtually any PSTN trunk with Microsoft Phone System and configuring interoperability between customer-owned telephony equipment, such as a third-party private branch exchange (PBX), analog devices, and Microsoft Phone System.

<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure>

<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants#create-a-trunk-and-provision-users>

<https://www.oracle.com/a/otn/docs/vzbwithsbcsfteams-mb.pdf>

<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc>

## 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.myCloudCx.com/articles/about-byoc-cloud/>

## 3. Requirements

- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version. The solution contained within this document has been tested using Oracle Communication SBC release **cz840p5a**.
- Genesys Cloud Cx BYOC (Cloud or Premise)
- Microsoft Teams Direct Routing
  - ✓ *Tenant -Microsoft O365 Tenant with customer domain registered.*
  - ✓ *License -Microsoft Phone System • Microsoft Teams + Skype for Business Plan 2 if included in Licensing Sku*
  - ✓ *Oracle SBC FQDN and Public Trusted Certificates for Direct Routing.*

Follow Below Links for detailed MS Teams Direct Routing Requirements

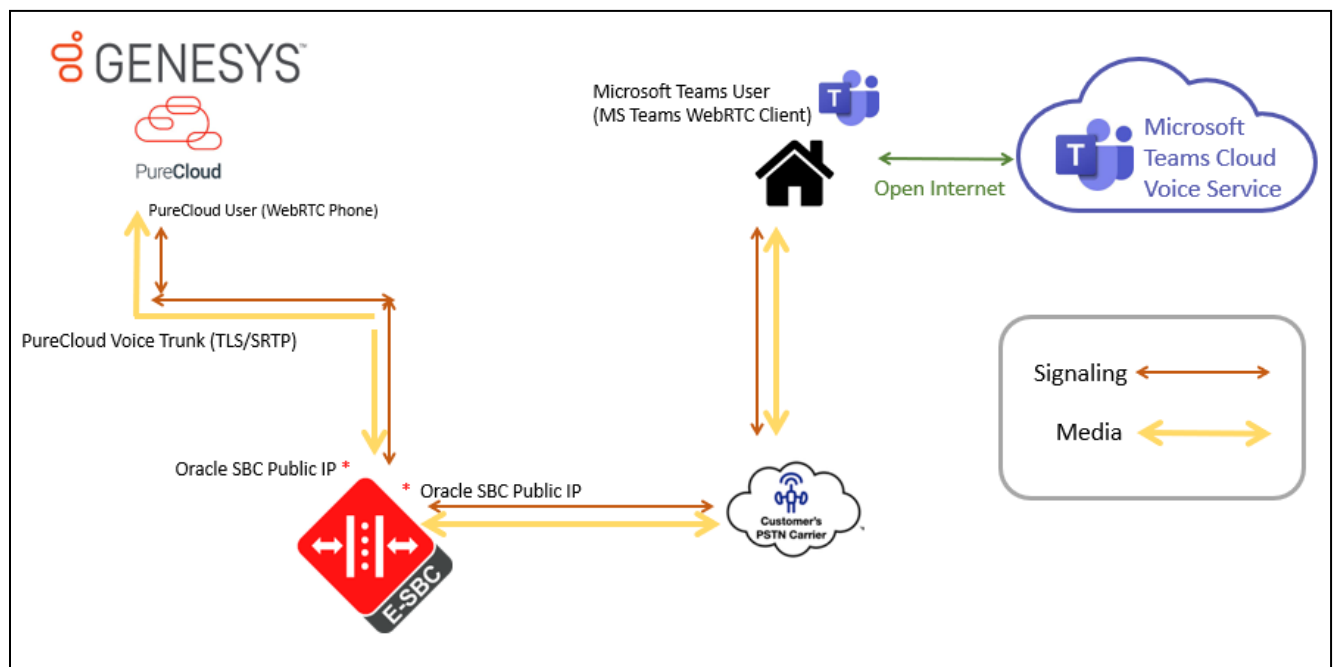
<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan>

[https://www.oracle.com/a/otn/docs/final\\_version\\_nonmedia\\_bypass-10-05-2021.pdf](https://www.oracle.com/a/otn/docs/final_version_nonmedia_bypass-10-05-2021.pdf)

Note: Microsoft Teams Direct Routing Supports multiple configuration models. Please choose appropriate model depending upon your specific requirement. Detailed information about Microsoft Teams Direct Models with Oracle SBC can be found under Microsoft Teams Subsection -

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

### 3.3. Architecture



Above figure illustrates the connection between Genesys Cloud Cx, Oracle SBC and Microsoft Teams Direct Routing. Both Cloud Cx and Microsoft Teams are connected to the Oracle SBC Public FQDN /IP

Oracle SBC which is certified with Microsoft Teams Direct Routing is used to steer the signaling, media to, and From the Cloud Cx to Microsoft Teams 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 Microsoft Teams Direct Routing

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.

## 4. 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 Microsoft Teams over the Direct Routing based infrastructure.

The Oracle Enterprise SBC will act as an intermediary between Microsoft Teams 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 DID's are assigned to users on Cloud Cx System and Microsoft Teams 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.

### 4.1 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.myCloudCx.com/articles/create-a-byoc-cloud-trunk/>

To configure the external Trunk, Navigate to

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



## 4.1.1 Create a new External Trunk

Type: BYOC Carrier Trunk

Protocol: TLS (TCP and UDP are also available)

## 4.1.2 Set Inbound SIP Termination Identifier

**Inbound SIP Termination Identifier** – is the DNS Name we will configure on the Oracle SBC and will be used to route calls towards 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](mailto: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="https://help.myCloud Cx.com/articles/tls-trunk-transport-protocol-specification/">lb01.byoc.us-east-1.myCloud Cx.com</a>
54.82.241.192	<a href="https://help.myCloud Cx.com/articles/tls-trunk-transport-protocol-specification/">lb02.byoc.us-east-1.myCloud Cx.com</a>
54.82.241.68	<a href="https://help.myCloud Cx.com/articles/tls-trunk-transport-protocol-specification/">lb03.byoc.us-east-1.myCloud Cx.com</a>
54.82.188.43	<a href="https://help.myCloud Cx.com/articles/tls-trunk-transport-protocol-specification/">lb04.byoc.us-east-1.myCloud Cx.com</a>

The screenshot shows the configuration interface for an External Trunk in Genesys Cloud. The left sidebar contains navigation links: Topology, Metrics, Trunks (selected), Sites, Edge Groups, Edges, Phone Management, Certificate Authorities, DID Numbers, and Extensions. The main content area is titled 'External Trunk Name' and shows 'Oracle BYOC POC'. Below this is a 'Trunk State' toggle set to 'In Service'. The 'Inbound / Termination' section includes an 'Inbound SIP Termination Identifier' field with the value 'byoc-voxai' and a 'DNS Replacement Routing' toggle set to 'Disabled'. To the right, the 'Status' is 'Operational', the 'Type' is 'Generic BYOC Carrier', and the 'Protocol' is 'TLS'. A 'Metrics' section shows 'Inbound Calls', 'Outbound Calls', and 'QoS Mismatches' all at 0. The 'Inbound SIP Termination Header' field is empty. At the bottom, an 'Inbound Request-URI Reference' section shows the 'FQDN Method' as 'INVITE sip:xxxxxxxxxx@byoc-voxai.byoc.mypurecloud.com' and the 'TGRP Method' as 'INVITE sip:xxxxxxxxxx;tgrp=byoc-voxai;trunk-context=byoc.mypurecloud.com@lb01.byoc.us-east-1.mypurecloud.com'.

Topology	External Trunk Name	Status
Metrics	Oracle BYOC POC	Operational
Trunks		Type
Sites		Generic BYOC Carrier
Edge Groups		Metrics
Edges		Inbound Calls 0
Phone Management	Trunk State	Outbound Calls 0
Certificate Authorities	In Service	QoS Mismatches 0
DID Numbers	Inbound / Termination	Protocol
Extensions	Inbound SIP Termination Identifier	TLS
	byoc-voxai	
	DNS Replacement Routing	
	Disabled	
	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

### 4.1.3 Set Outbound SIP Servers or Proxies

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

The screenshot shows the 'Outbound' configuration page. On the left is a sidebar with links: Edge Groups, Edges, Phone Management, Certificate Authorities, DID Numbers, and Extensions. The main content area has the following fields:

- Outbound SIP Termination FQDN**: A text input field containing 'solutionslab.cgbubedford.com'.
- Outbound SIP TGRP Attribute**: A text input field.
- TGRP Context-ID**: A text input field.
- Outbound SIP DNIS**: A text input field.
- Outbound Request-URI Reference**: A large text area containing the text 'INVITE sip:xxxxxxxxxx@solutionslab.cgbubedford.com'.

### 4.1.4 Set Calling Address

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

The screenshot shows the 'Calling' configuration page. On the left is a sidebar with links: Topology, Metrics, Trunks, Sites, Edge Groups, Edges, Phone Management, Certificate Authorities, DID Numbers, and Extensions. The main content area has the following sections:

- Calling**:
  - Address**: A text input field containing '19729132636'.
  - Name**: A text input field.
  - Address Override Method**: A dropdown menu with 'Always' selected.
  - Name Override Method**: A dropdown menu with 'Always' selected.
- SIP Access Control**:
  - Allow the Following Addresses**: A list of IP addresses with delete icons.
  - Add an IP or CIDR address**: A text input field with a plus icon.
- External Trunk Configuration**:
  - Expand All** and **Collapse All** buttons.
  - A list of expandable sections: General, Transport, Identity, Media, Protocol, Diagnostics, and Custom.

At the bottom are **Save External Trunk** and **Cancel** buttons.

### 4.1.5 Set SIP Access Control

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

#### 4.1.6 Enable E.164 format

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

### 4.2 Site Configuration.

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

#### 4.2.1 Create a New Site

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

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

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

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

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

Click **Create Site**.

Topology

Metrics

Trunks

Sites

Edge Groups

Edges

Phone Management

Certificate Authorities

DID Numbers

Extensions

General

Number Plans

Outbound Routes

Simulate Call

Site Name

BYOC\_Oracle

Description

Location

Test location

Media

Geo-Lookup TURN

Disabled

Automatic Updates

Recurrence Type

Daily

Time

All day

Range

Start Time

2 : 00 AM

End Time

5 : 00 AM

Time Zone

America/Chicago (-05:00)

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

Save Site

Cancel

## 4.2.2 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.



Telephony / Phone Management / Phones / Edit Phone

Topology

Metrics

Trunks

Sites

Edge Groups

Edges

**Phone Management**

Certificate Authorities

DID Numbers

Extensions

**Phone**

Phone Name

Base Settings

WebRTC Cloud

Site

BYOC\_Oracle

Person

Phone Configuration

General

Media

Network

Custom

Save Phone Cancel

Status

Unmanaged

Make and Model

Genesys Cloud WebRTC Phone

In Use By

Log off

Default For

None

Primary Edge

virtual-edge-i-0e97fcbda24ea3d49

Secondary Edge

virtual-edge-i-03e78d824757a3555

Expand All Collapse All

## 4.2.5 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

Metrics

Trunks

**Sites**

Edge Groups

Edges

Phone Management

Certificate Authorities

DID Numbers

Extensions

General Number Plans Outbound Routes **Simulate Call**

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)

Log

## 4.3 DID Assignment

### 4.3.1 Create DID Range

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

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

Telephony / DID Numbers

Topology

Metrics

Trunks

Sites

Edge Groups

Edges

Phone Management

Certificate Authorities

**DID Numbers**

Extensions

DID Assignments

DID Ranges

Create Range

<input type="checkbox"/>	DID Range	Service Provider	Comments	<input type="checkbox"/>
<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?	

1 - 10 of 10 DID Ranges

Create Range

DID Start

+1 → +12038710043

DID End

+1 → +12078710053

Service Provider

Twilio

Comments

PurecloudtoTwilioviaOracleSBC

Save Cancel

### 4.3.2 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.

OracleSolutionslab

Email

Work

Personal

Other

Phone

Work

Cell

Home

Other

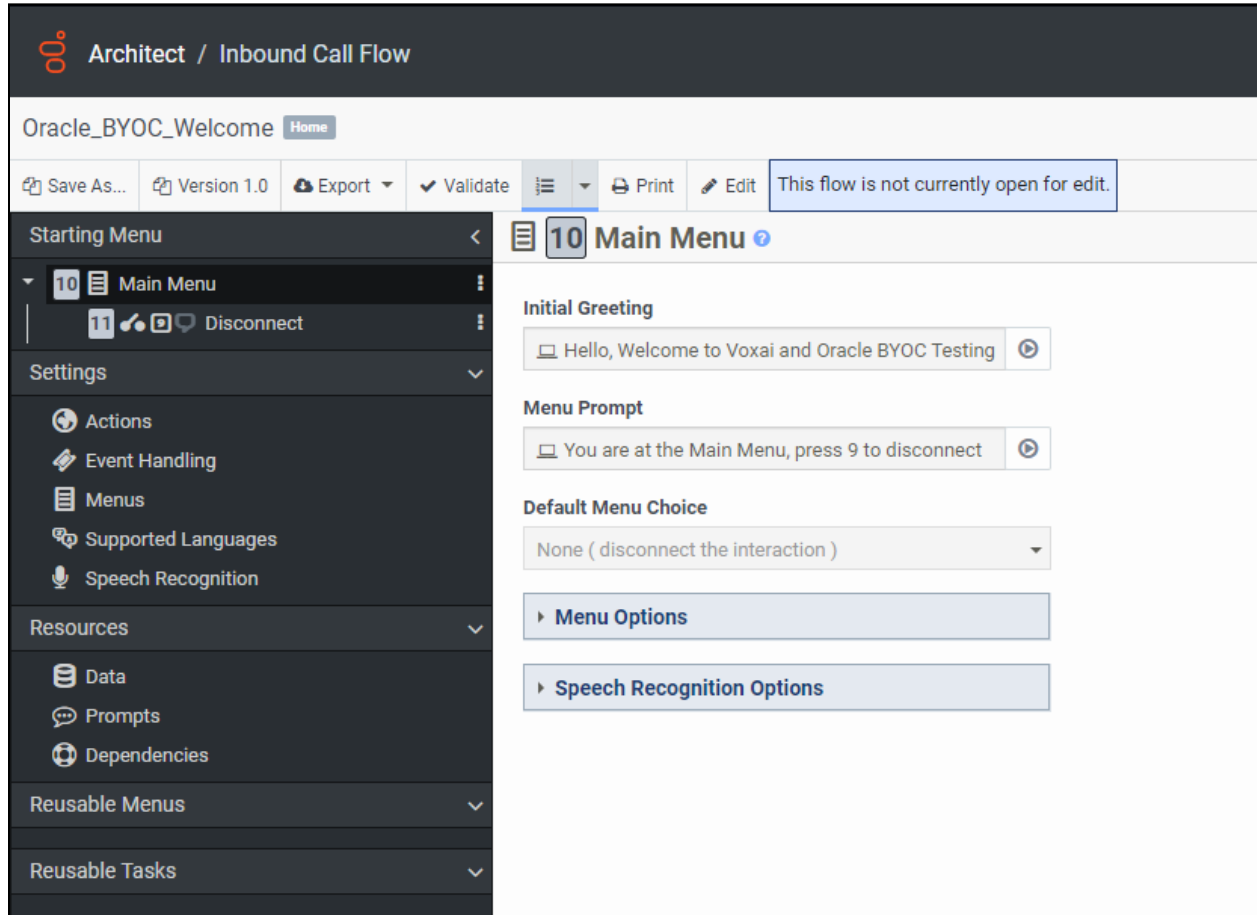
Links

External System

http(s)://www.external-system-url.com

## 4.4. 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 Microsoft Teams to Genesys Cloud Cx via Oracle SBC.



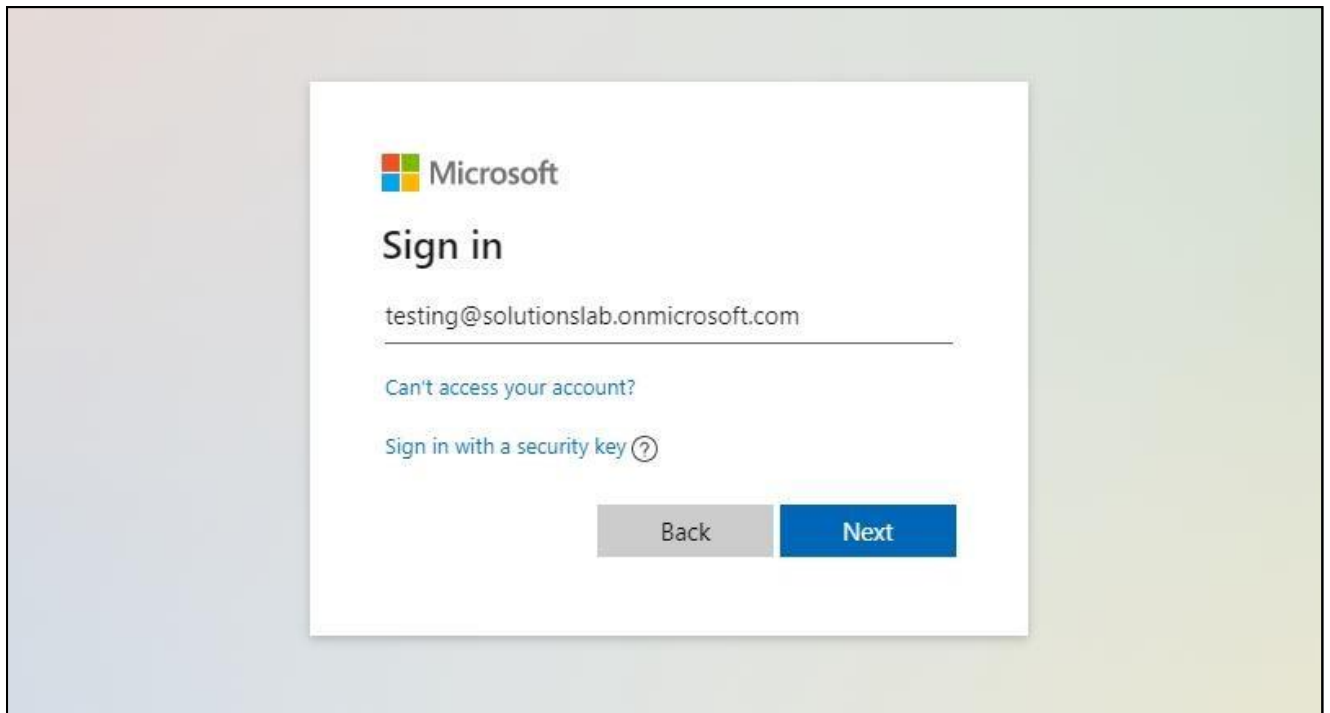
## 5. Configure Microsoft Teams Direct Routing

The steps outlined below is the minimum required configuration to pair your SBC with Microsoft Teams Direct Routing Interface. **This is to be used as an example only, and we highly recommend you work with your Microsoft Account representative to implement the correct configuration for your specific environment.**

### 5.1. Access Teams Admin center

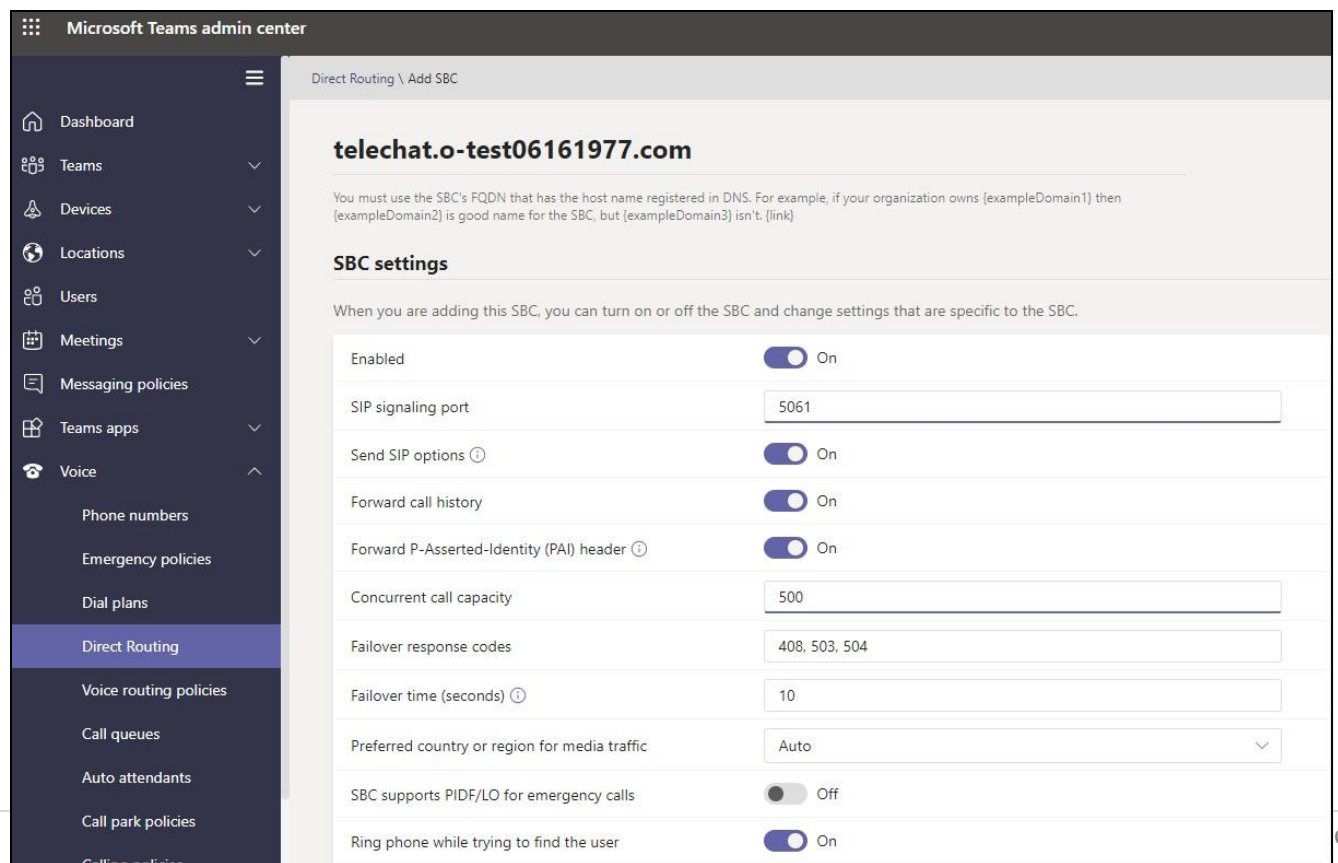
The first step is to access the Teams Admin Center with administrator admin credentials:



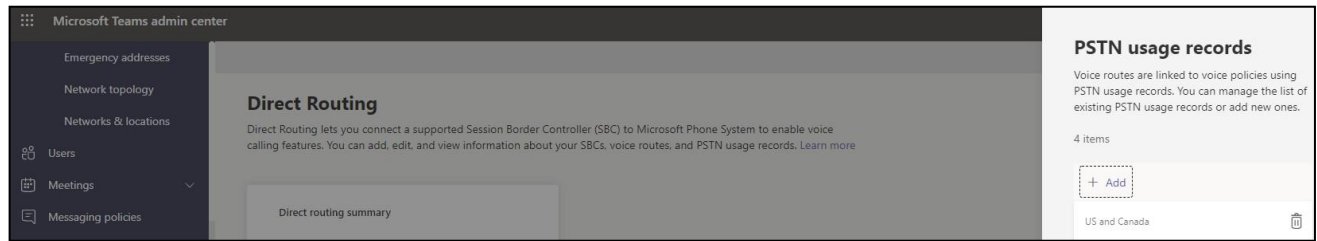


## 5.2. Configure Online PSTN Gateway

Configuration Path: Voice/Direct Routing/SBC

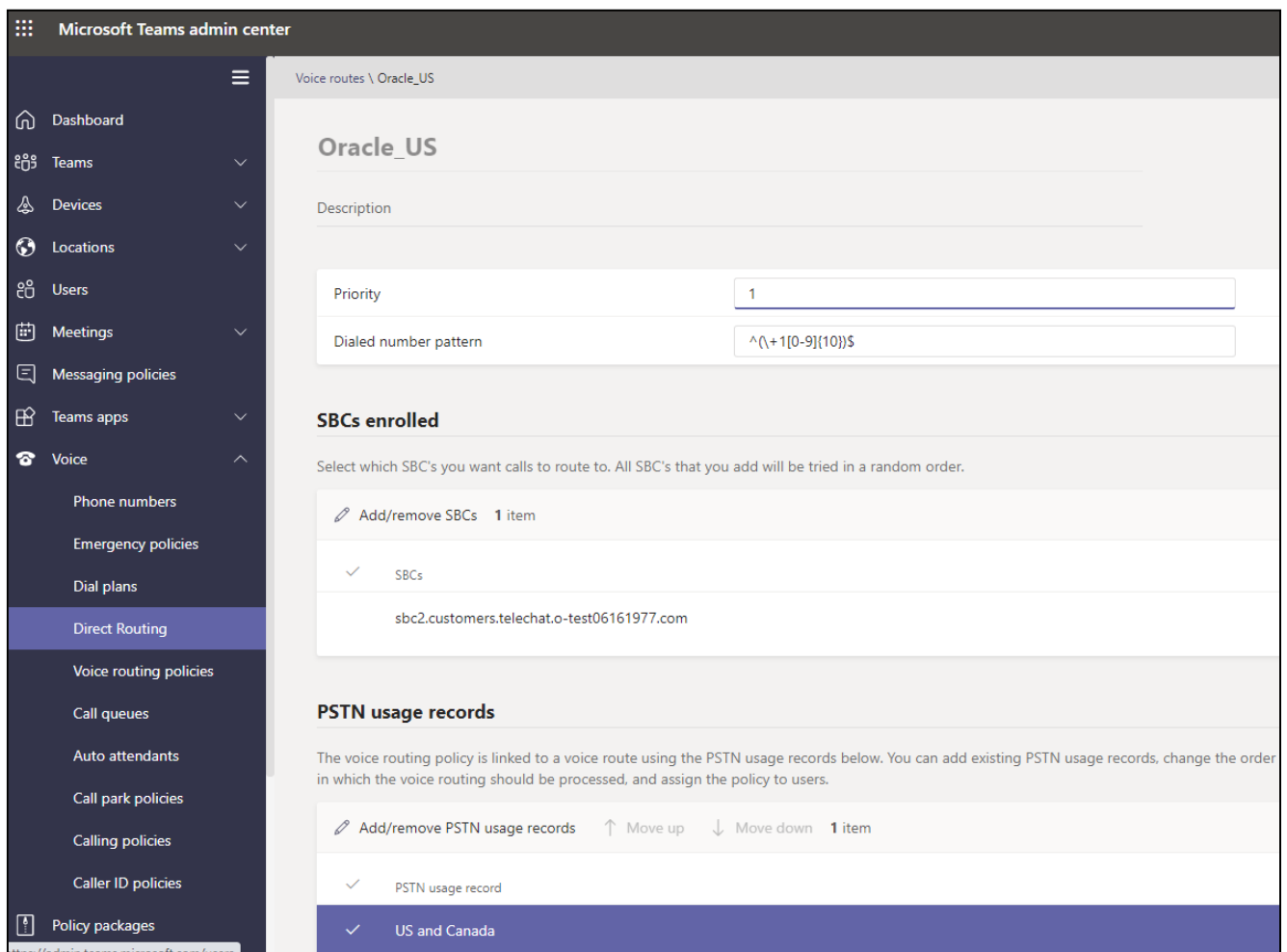


Click Add, Type US and Canada, next, click Apply



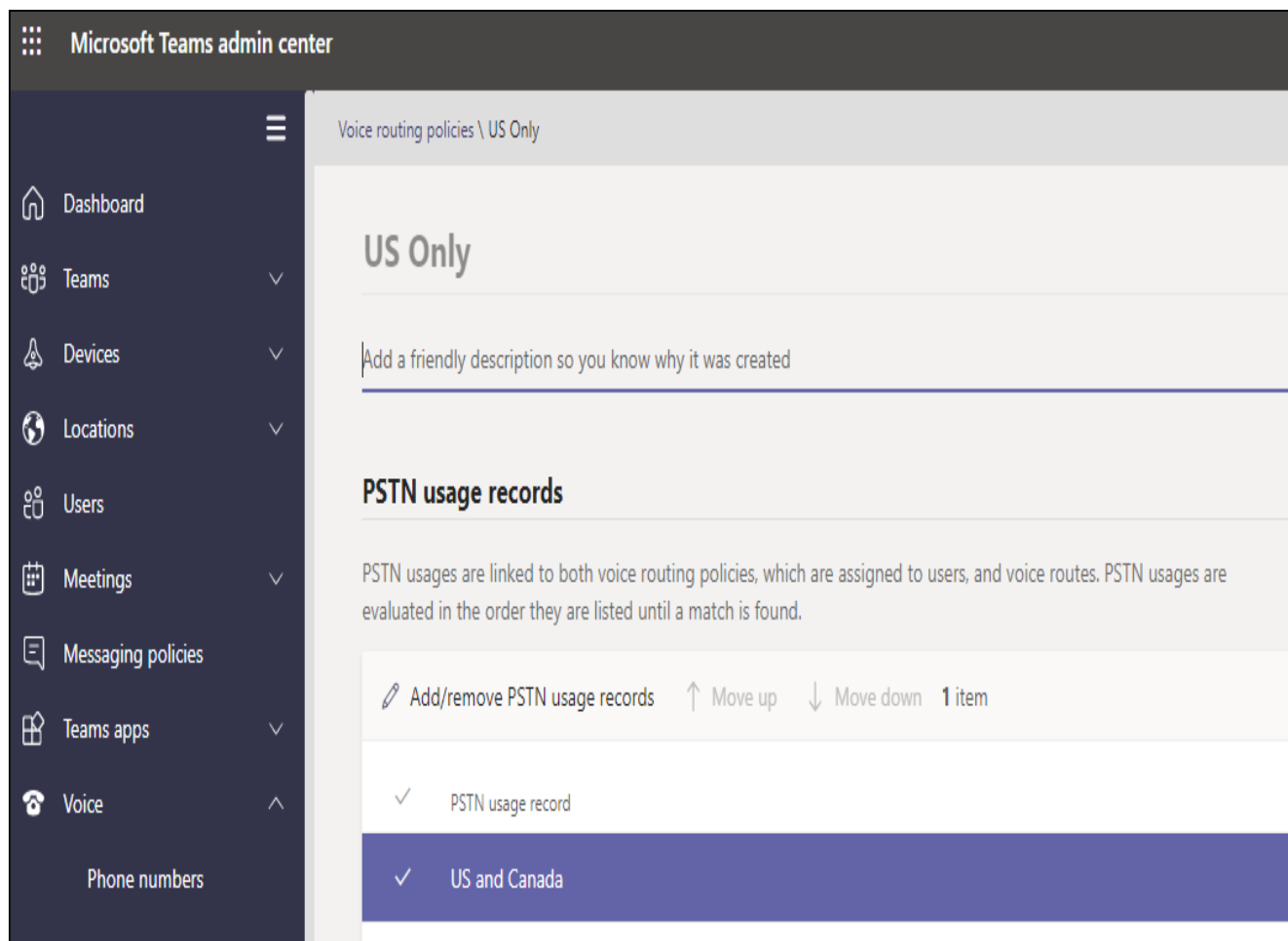
## 5.4. Configure Online Voice Routes

Configuration Path: Voice/Direct Routing/Voice Routes



## 5.5. Configure Online Voice Routing Policy

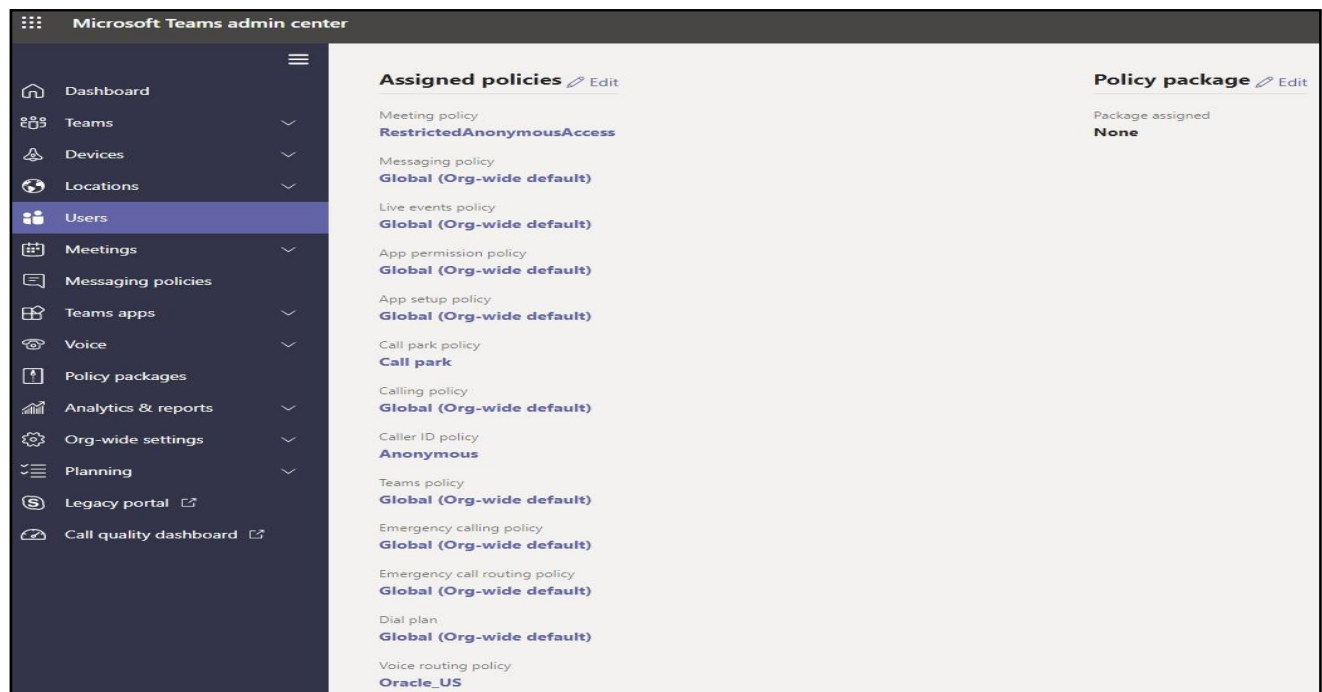
Configuration Path: Voice/Voice Routing Policies



## 5.6. Assign Voice Routing Policy to Users

Configuration Path: Users/Select the “User”/Policies

Next to Voice Routing Policy, Click Edit and Assign. In this example, we have selected Teamsuser1:



For More Information about configuring Microsoft Teams to Connect to your SBC, Setting up users, or configuration voice routing, please refer to the [Related Documentation](#) Section of this guide.

With this, Microsoft Teams Direct Routing config is complete.

## 6. Configuring the SBC

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

### 6.1. Validated Oracle SBC version

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

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

## 6.2 New SBC configuration

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

### 6.2.1 Establishing a serial connection to the SBC

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

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

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

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

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

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

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

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

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

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

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

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

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

Boot File           : /boot/nnsCZ840p3B.bz
IP Address          : 10.138.194.139
VLAN                : 0
Netmask             : 255.255.255.192
Gateway             : 10.138.194.129
IPv6 Address        :
IPv6 Gateway        :
Host IP             :
FTP username         : vxftp
FTP password        : vxftp
Flags               :
Target Name         : NN4600-139
Console Device      : COM1
Console Baudrate    : 115200
Other               :

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

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

NN4600-139(configure)#
```

Note: There is no management IP configured by default.

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

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

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

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

Enable the features for the ESBC using the setup entitlements command as shown

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)#
```

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



ORACLE

Enterprise Session Border Controller



## Sign in to E-SBC

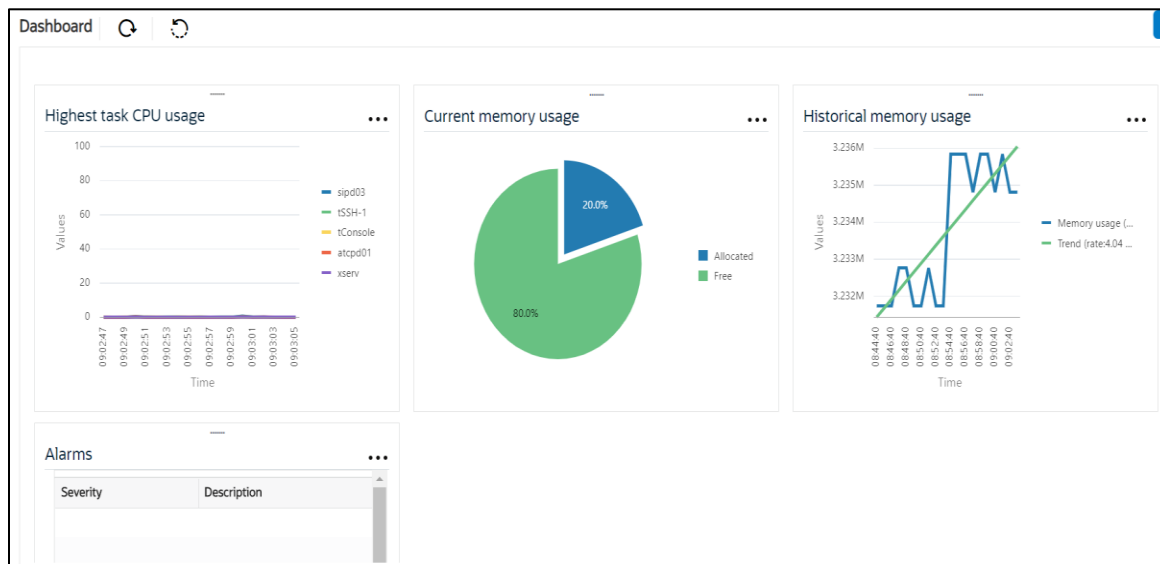
Enter your details below

Required

Required

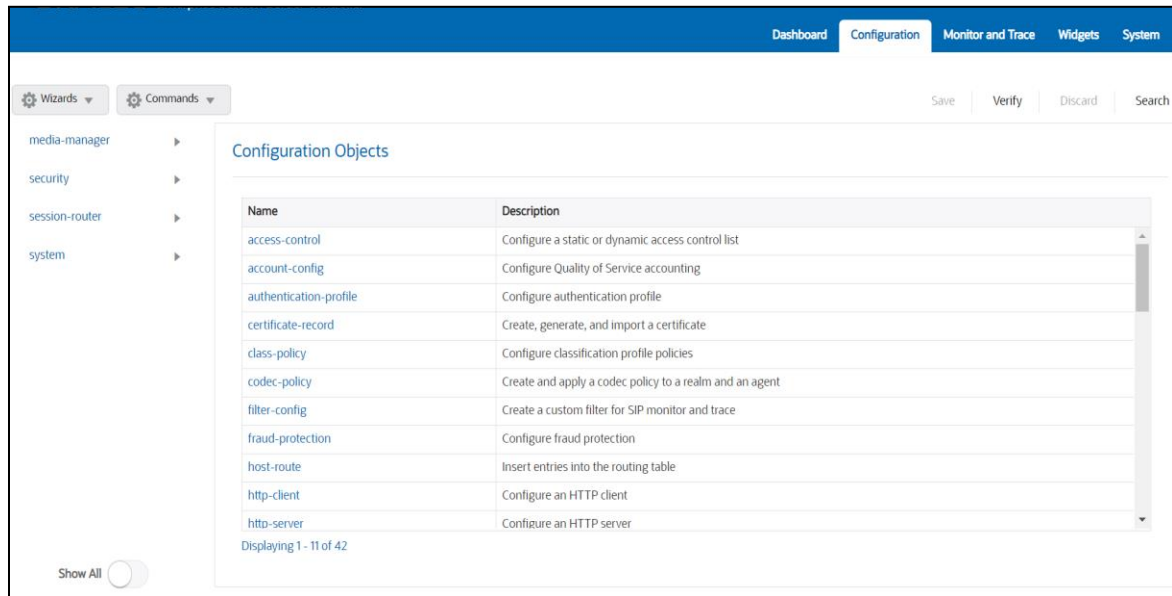
SIGN IN

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



Navigate to Configuration as shown below, to configure the SBC





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

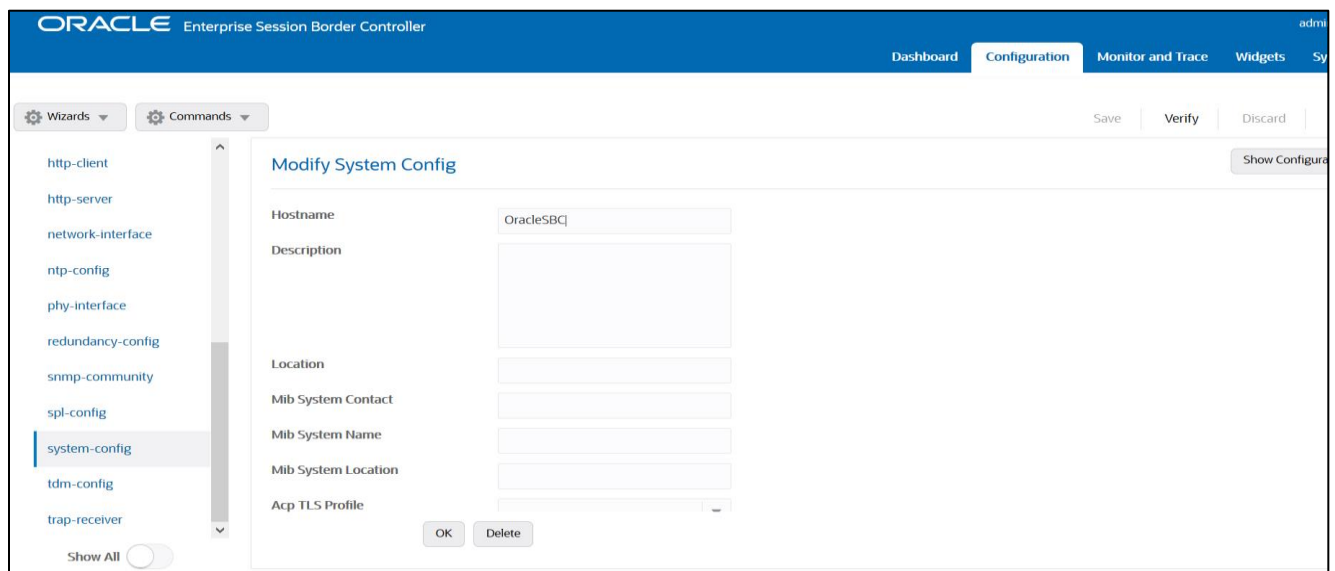
[https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc\\_scz840\\_webgui.pdf](https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf)

The expert mode is used for configuration.

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

### 6.3. Configure system-config

Navigate to system->system-config



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

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands

Save Verify Discard

http-client  
http-server  
network-interface  
ntp-config  
phy-interface  
phy-interface  
redundancy-config  
snmp-community  
spl-config  
system-config  
tdm-config  
trap-receiver

Show All

### 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

Add

OK Delete

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.

## 6.4. Configure Physical Interface values

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

Here we have configured, Network-interface M00 for Microsoft Teams and M10 for Cloud Cx.

Parameter Name	Microsoft Teams (M00)	Cloud Cx (M10)
Slot	0	1
Port	0	0
Operation Mode	Media	Media

Configure M00 interface as below.

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace

Wizards Commands Save Verify

host-route  
http-client  
http-server  
network-interface  
ntp-config  
**phy-interface**  
redundancy-config  
snmp-community  
spl-config  
system-config  
trap-receiver

### 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

OK Back

Configure M10 interface as below -

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace

Wizards Commands Save Verify

session-router  
system  
fraud-protection  
host-route  
http-client  
http-server  
network-interface  
ntp-config  
**phy-interface**  
redundancy-config  
snmp-community

Show All ☐

### 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

OK Back

## 6.5. Configure Network Interface values

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

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

**Note:** The provided network IP addresses are given for example purpose only. In the real-world scenario We cannot 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	Microsoft Teams Network Interface	PureCloud Network interface
Name	M00	M10
Host Name	customers.telechat.o-test06161977.com	solutionslab.cgbubedford.com
IP address		
Netmask	255.255.255.192	255.255.255.192
Gateway		
dns-ip-primary	8.8.8.8	8.8.8.8
dns-ip-backup1	8.8.8.4	8.8.8.4

Configure network interface M00 as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active. On the left, a sidebar lists various configuration options, with 'network-interface' selected. The main area is titled 'Add Network Interface'. It contains the following fields:

- Name:** M00
- Sub Port Id:** 0 (Range: 0..4095)
- Description:** (Empty text area)
- Hostname:** customers.telechat.o-test06161977.com
- IP Address:** (Empty text field)
- Pri Utility Addr:** (Empty text field)
- Sec Utility Addr:** (Empty text field)

At the bottom of the form are 'OK' and 'Back' buttons. The top of the interface shows the Oracle logo and navigation tabs: Dashboard, Configuration, Monitor and Trace, and Widgets.

Similarly, configure network interface M10 as below

The screenshot shows a web-based configuration interface for a network device. On the left, a sidebar titled 'Configuration' contains a list of menu items: media-manager, security, session-router, system, fraud-protection, host-route, http-client, http-server, network-interface (highlighted), ntp-config, phy-interface, redundancy-config, snmp-community, and spl-config. Below this list is a 'Show All' toggle switch. The main content area is titled 'Modify Network Interface'. It contains the following fields and controls:

- Name:** A dropdown menu with 'M10' selected.
- Sub Port Id:** A text input field containing '0', with a note '( Range: 0..4095 )' to its right.
- Description:** A large, empty text area.
- Hostname:** A text input field containing 'solutionslab.cgbubedford.com'.
- IP Address:** A text input field with a blue highlight bar.
- Pri Utility Addr:** An empty text input field.
- Sec Utility Addr:** An empty text input field.
- Netmask:** A text input field containing '255.255.255.192'.
- Gateway:** A text input field with a blue highlight bar.
- Gw Heartbeat:** A checkbox that is currently checked.
- Gw ...:** A checkbox that is currently unchecked.

At the bottom right of the main area are two buttons: 'OK' and 'Back'.

## 6.6. Enable media manager

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

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

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets

Wizards Commands Save Verify Discard

media-manager media-policy realm-config steering-pool security session-router system

### 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 )
Hnt 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-policy realm-config steering-pool security session-router system fraud-protection host-route

### 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 )
Ad Monitor Window	30	( Range: 5..3600 )
Trap On Demote To Deny	<input type="checkbox"/> enable	

OK Delete

Show All

## 6.7. Configure Realms

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

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

Config Parameter	Teams Side	GenesysCloud d Realm
Identifier	Teams	GenesysCloud
Network Interface	M00	M10
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Teams-FQDN	Customers.Telechat.o- test06161977.com	
Teams fqdn in uri	<input checked="" type="checkbox"/>	
Sdp inactive only	<input checked="" type="checkbox"/>	
Media Sec policy	sdespolicy	sdespolicy
RTCP mux	<input checked="" type="checkbox"/>	
ice profile	ice	
Codec policy	addCN	
RTCP policy	rtcpGen	
Access Control Trust Level	High	High
Pai-strip	enabled	
Media-policy		

## Realm for Microsoft Teams –

Configuration
View Configuration
Q

media-manager
▼
codec-policy
media-manager
media-policy
realm-config
steering-pool
security
▼
authentication-profile
certificate-record
tls-global
tls-profile
session-router
▶
system
▶

### Modify Realm Config

Identifier	Teams
Description	Realm Facing Teams Direct Routing
Addr Prefix	0.0.0.0
Network Interfaces	M00:0.4 ✕
Media Realm List	
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	0 ( Range: 0.999999999 )
Max Priority Bandwidth	0 ( Range: 0.999999999 )
Parent Realm	

Configuration
View Configuration
Q

media-manager
codecs-policy
media-manager
media-policy
realm-config
steering-pool
security
authentication-profile

### Modify Realm Config

Media Policy
Media Sec Policy
sdesPolicy
RTCP Mux
Ice Profile
ice
Teams Fqdn
Teams Fqdn In Uri
SDP Inactive Only

certificate-record
tls-global
tls-profile
session-router
system

### Access Control Trust Level

high
Invalid Signal Threshold
Maximum Signal Threshold
Untrusted Signal Threshold
Nat Trust Threshold
Max Endpoints Per Nat
Nat Invalid Message Threshold
Wait Time For Invalid Register
Deny Period

codecs-policy
media-manager
media-policy
realm-config
steering-pool
security
authentication-profile
certificate-record

### Refer Notify Provisional

none
Dyn Refer Term
Codec Policy
addCN
Codec ManIP In Realm
Codec ManIP In Network
RTCP Policy
rtcpGen
Constraint Name

## Realm for Genesys Cloud Cx



**Configuration** [View Configuration](#)

- media-manager
  - codec-policy
  - media-manager
  - media-policy
  - realm-config**
  - steering-pool
- security
- session-router
- system

### Modify Realm Config

Identifier: GenesysCloud

Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M10:0.4 ✕

Media Realm List:

Mm In Realm: ☒ enable

- realm-config**
- steering-pool
- security
- session-router
- system

Media Policy:

Media Sec Policy: sdesPolicy

RTCP Mux: ☐ enable

Ice Profile:

Teams Fqdn:

Teams Fqdn In Uri: ☐ enable

SDP Inactive Only: ☐ 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: 0 (Range: 0..4294967295)

Access Control Trust Level: **high** 

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

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

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

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

Max Endpoints Per Host:

OK Back

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)

## 6.8. Security Configuration

### 6.8.1 Configuring Certificates

This section describes how to configure the SBC for TLS and SRTP communication for Microsoft Teams and Cloud Cx BYOC. It requires a certificate signed by one of the trusted Certificate Authorities. The communication between the Oracle SBC with Microsoft Teams 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 below certificate records. They are as follows:

- **SBC Certificate (end-entity certificate)**
- **Baltimore Root -Required for Microsoft Teams**
- **DigiCert Root CA (SBC and Microsoft Teams)**
- **DigiCert Intermediate Cert (this is optional – only required if your server certificate is signed by an intermediate)**
- **DigiCertEVRotCA (Genesys Cloud Cx)**

#### Supported CAs for Microsoft Teams.

<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc>

#### 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.myCloudCx.com/articles/tls-trunk-transport-protocol-specification/>

**Note: Both Genesys Cloud Cx and Microsoft Teams 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( Teams)	SBC Certificate2( Cloud Cx)	Baltimore Root	DigiCertEV RootCA	DigiCert Root CA	DigiCert Intermediate
Name	SBCCert 1	SBCCert 2	Baltimore CyberTrust Root	<b>Cloud CxCert</b>	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA

Common Name	<b>customers.telechat.o-test06161977.com</b>	<b>solutionslab.cgbubedford.com</b>	Baltimore CyberTrust Root	<b>Cloud CxCert</b>	DigiCert Global Root CA	DigiCert SHA2 Secure Server CA
Key Size	2048	2048	2048	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256	Sha256	Sha256	Sha256

### 6.8.1.1 End Entity Certificate

The SBC's end entity certificate is what is presented to Cloud Cx and Microsoft Teams 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 in this case as we are connecting to Cloud Cx and Microsoft Teams over different FQDN

- Common name: (**customers.telechat.o-test06161977.com**) for Microsoft Teams.
- 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:

Configuration
View Configuration
Q

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

### Modify Certificate Record

NameSBCTeamsCert
CountryUS
StateCalifornia
LocalityRedwood City
OrganizationOracle Corporation
Unit
Common Namecustomers.telechat.o-test06161977.cor
Key Size2048
Alternate Name\*.customers.telechat.o-test06161977.c
Trusted☒ enable
Key Usage ListdigitalSignature keyEncipherment
Extended Key Usage ListserverAuth clientAuth
Key Algorrs
Digest Algorsha256
Ecdsa Key Sizep256
Cert Status Profile List

Show All
OK Back

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

NameSBCPureCloudCert
CountryUS
StateCalifornia
LocalityRedwood City
OrganizationOracle Corporation
Unit
Common Namesolutionslab.cgbubedford.com
Key Size2048
Alternate Name
Trusted☒ enable
Key Usage ListdigitalSignature keyEncipherment
Extended Key Usage ListserverAuth clientAuth
Key Algorrs
Digest Algorsha256
Ecdsa Key Sizep256
Cert Status Profile List

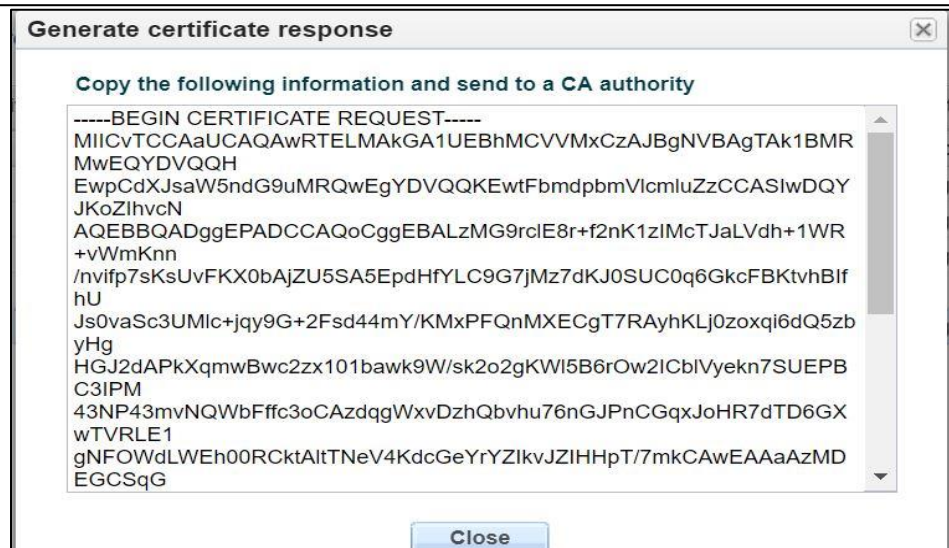
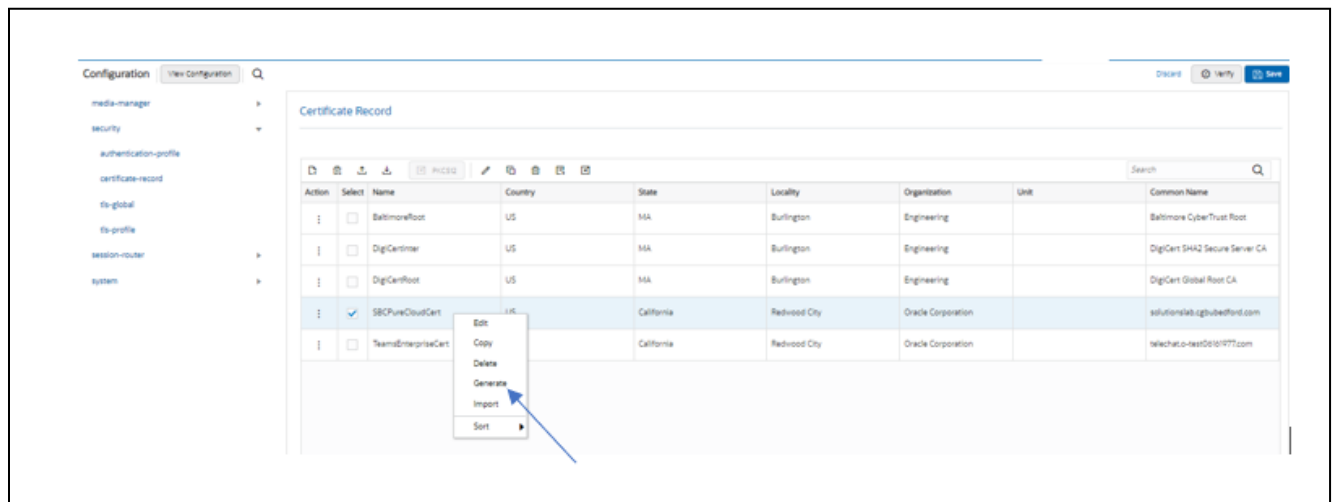
Show All
OK Back

## Step 2 – Generating a certificate signing request

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

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

- Select the certificate and generate certificate on clicking the “Generate” command.
- The Step must be performed for both Certificate records -SBCTeamsCert 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.

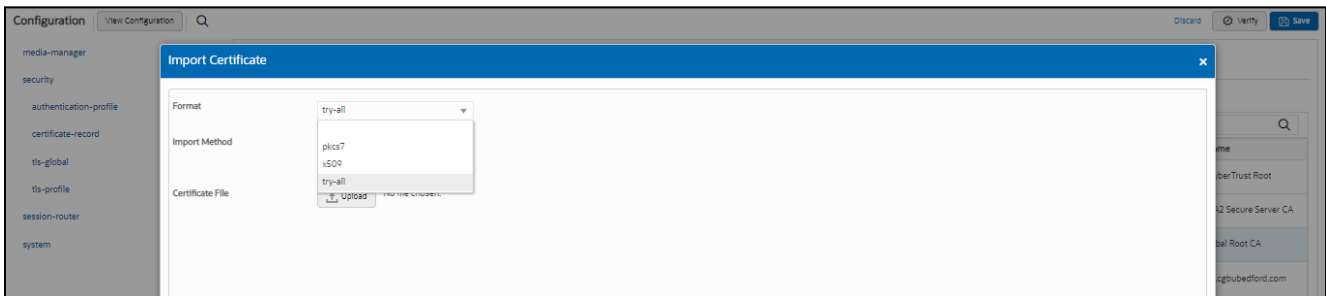
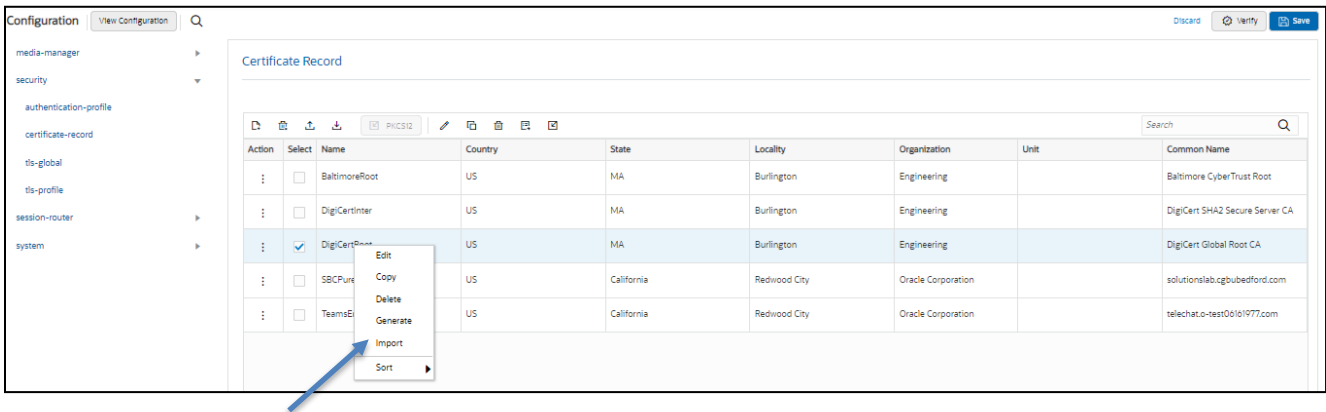


- copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, **a save and activate is required** before you can import the certificates to each certificate record created above.

### Step 3 Import Certificates to the SBC

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

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



#### 6.8.1.2 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

### 6.9. TLS-Profile

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

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

**TLS profile -Microsoft Teams.**

**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 TLS Profile

Name: TLSTeams

End Entity Certificate: SBCTeamsCert

Trusted Ca Certificates:
 

- BaltimoreRoot X
- DigiCertRoot X
- DigiCertInter X

Cipher List: DEFAULT X

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

OK Back

## 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.

**Configuration** View Configuration

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 TLS Profile

Name: TLSPureCloud

End Entity Certificate: SBCPureCloudCert

Trusted Ca Certificates: BaltimoreRoot X, DigiCertRoot X, DigiCertInter X

Cipher List: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 X, TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA X

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

OK Back

## 6.10. Configure SIP Interfaces

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

Please Configure sip-interface for the 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 Microsoft Teams

**Configuration** View Configuration

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  
session-translation  
sip-config  
sip-feature  
**sip-interface**

### Modify SIP Interface

State: ☒ enable

Realm ID: Teams

Description:

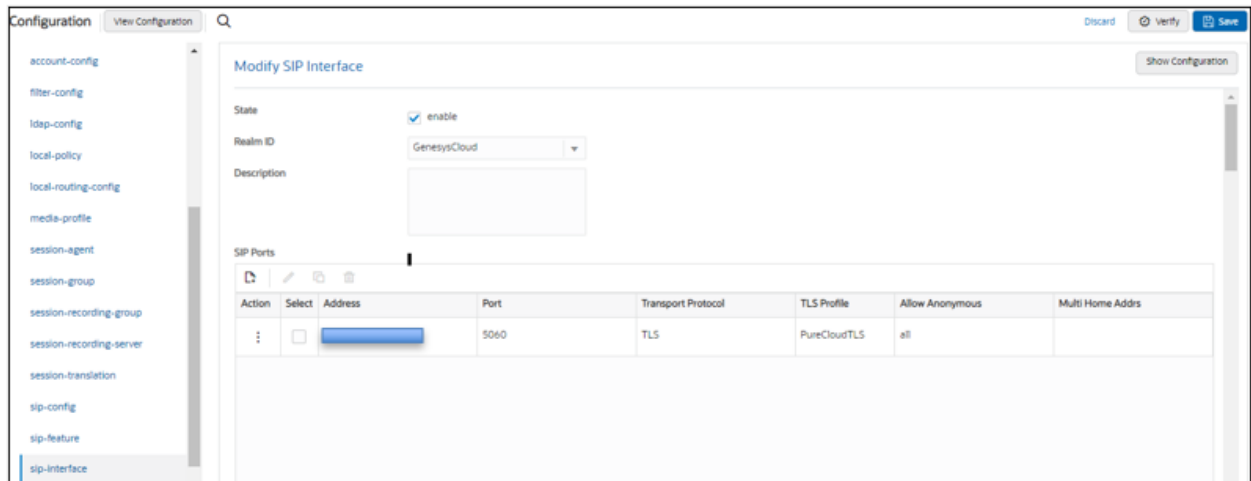
SIP Ports

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
	<input type="checkbox"/>	SIP	5061	TLS	TLSTeams	agents-only	

Show Configuration



## Sip-interface for Genesys Cloud Cx



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

### 6.11. Configure session-agent

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

Navigate to session-router->Session-Agent and **Configure the session-agents for the 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 Discard Verify Save

media-manager  
security  
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  
session-translation

**Modify Session Agent** Show Configuration

Hostname: byoc-voxa1.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-agent for Teams** with the following parameters.  
Go to session-router->Session-Agent.

- hostname to “sip.pstnhub.microsoft.com”
- port 5061
- realm-id – needs to match the realm created for Teams
- transport set to “StaticTLS”
- refer-call-transfer set to enabled
- ping-method – send OPTIONS message to Microsoft to check health
- ping-interval to 30 secs

**ORACLE** Enterprise Session Border Controller Dashboard Configuration Monitor and Trace Widgets Syst admin

Wizards Commands Save Verify Discard S

session-agent  
session-group  
session-recording-group  
session-recording-server  
session-translation  
sip-config  
sip-feature  
sip-interface  
sip-manipulation  
sip-monitoring  
sti-server  
translation-rules  
system Show All

**Modify Session Agent** Show Configuration

Hostname: sip.pstnhub.microsoft.com  
IP Address:   
Port: 5061 (Range: 0,1025..65535)  
State: ☒ enable  
App Protocol: SIP  
App Type:   
Transport Method: StaticTLS  
Realm ID: Teams  
Egress Realm ID:   
Description:   
OK Back

The screenshot shows the Oracle Enterprise Session Border Controller interface. The top navigation bar includes 'Dashboard', 'Configuration' (selected), 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration categories, with 'session-agent' selected. The main panel is titled 'Modify Session Agent' and contains the following fields:

- Proxy Mode: [Dropdown]
- Redirect Action: [Dropdown]
- Loose Routing: ☒ enable
- Response Map: [Dropdown]
- Ping Method: [Text: OPTIONS]
- Ping Interval: [Text: 30] (Range: 0..4294967295)
- Ping Send Mode: [Dropdown]
- Ping All Addresses: ☐ enable
- Ping In Service Response Codes: [Text]
- Options: [Text]
- SPL Options: [Text]

At the bottom of the main panel are 'OK' and 'Back' buttons. The left sidebar also has a 'Show All' button.

Follow above steps to create 2 more sessions for:

- sip2.pstnhub.microsoft.com
- sip3.pstnhub.microsoft.com

## 6.12. 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 Teams Session Agents

The screenshot shows the Oracle Enterprise Session Border Controller interface. The top navigation bar includes 'Dashboard', 'Configuration' (selected), 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration categories, with 'session-group' selected. The main panel is titled 'Add Session Group' and contains the following fields:

- Group Name: [Text: TeamsGrip]
- Description: [Text Area]
- State: ☒ enable
- App Protocol: [Dropdown: SIP]
- Strategy: [Dropdown: Hunt]
- Dest: [List of destinations: sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com, sip3.pstnhub.microsoft.com]

At the bottom of the main panel are 'OK' and 'Back' buttons. The left sidebar also has a 'Show All' button.

## 6.13. 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 Microsoft Teams –

Genesys Cloud Cx → Oracle SBC → Carrier Trunk (Twilio) → Oracle SBC SBC → MS Teams

Inbound calls from Microsoft Teams to Cloud Cx -

MS Teams→ Oracle SBC → Carrier Trunk (Twilio) → Oracle SBC 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-twillio-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 Microsoft Teams.

The screenshot displays the Oracle Enterprise Session Border Controller (SBC) configuration interface. The left sidebar shows the navigation menu with 'local-policy' selected. The main panel is titled 'Modify Local Policy' and contains the following fields:

- From Address: [Empty field with a dropdown arrow]
- To Address: [Empty field with a dropdown arrow]
- Source Realm: GenesysCloud X
- Description: [Empty text area]
- State: ☒ enable
- Policy Priority: none

Below these fields is a table for 'Policy Attributes' with the following columns: Action, Select, Next Hop, Realm, Action, Terminate Recursion, Cost, State, App Protocol, Lookup, and Next Key. The table contains one row with the following values:

Action	Select	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
:	<input type="checkbox"/>	oracle.pstn.twilio.com	TwilioSipTrunk	none	disabled	0	enabled		single	

Configuration View Configuration Q Discard Verify

media-manager
security
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
session-translation
sip-config
sip-feature
sip-interface

### Modify Local Policy

From Address
To Address
Source Realm
Description
State
Policy Priority

2038710043
2078710043
+12038710043

TwilioSipTrunk

☒ enable
none

Policy Attributes

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

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

Configuration View Configuration Q Discard Verify Save

media-manager
security
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
session-translation

### Modify Local Policy

From Address
To Address
Source Realm
Description
State
Policy Priority

Teams

☒ enable
none

Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
:	<input type="checkbox"/>	oracle.patn.twilio.com	TwilioSipTrunk	none	disabled	0	enabled		single	

Configuration View Configuration Q Discard Verify Save

media-manager
security
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
session-translation
sip-config
sip-feature

### Modify Local Policy

From Address
To Address
Source Realm
Description
State
Policy Priority

+19787606734
19787606734
9787606734

TwilioSipTrunk

☒ enable
none

Policy Attributes

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

## 6.13. Configure steering-pool

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

### Cloud Cx Steering pool.

The screenshot shows the ORACLE Enterprise Session Border Controller configuration interface. The top header displays the product name and version: NN4600-139, 10.138.194.139, SCZ8.4.0 Patch 5 (Build 332). The left sidebar lists configuration categories: media-manager, codec-policy, media-manager, media-policy, realm-config, steering-pool (selected), security, and session-router. The main panel is titled 'Modify Steering Pool' and contains the following fields:

Field	Value	Range
IP Address	[Empty]	
Start Port	20000	( Range: 0,1.65535 )
End Port	40000	( Range: 0,1.65535 )
Realm ID	GenesysCloud	
Network Interface	[Empty]	

### Microsoft Teams Steering Pool

This screenshot is identical to the one above, showing the 'Modify Steering Pool' configuration page. The only difference is the 'Realm ID' dropdown menu, which is now set to 'Teams' instead of 'GenesysCloud'.

## 6.14. Configure additional Parameters

To simplify the ORACLE SBC sip manipulation, from GA Release SCZ830m1p7 contains three additional SBC configuration parameters which are not found in prior releases.

The purpose of these three parameters is to replace the majority of the sip manipulation rules required to be configured in the ORACLE SBC to properly interface with Microsoft Teams Direct Routing.

The first two parameters are found under the **realm-config** and would be enabled in realms facing Microsoft Teams.

They are **Teams FQDN in URI** and **SDP inactive only**.

The detailed description is given below for each config parameter.

## Teams FQDN in URI:

When enabled, this parameter takes the FQDN configured under hostname of the network interface and inserts that into the Contact and FROM headers of Invites generated by the SBC towards Teams. This also adds a new “X-MS-SBC” Header to both Invite and OPTIONS Requests, which takes the place of the User-Agent header currently being added via Sip Manipulation. Lastly, SBC will add a Contact Header to outgoing SIP Options Pings, also containing the FQDN of the SBC listed under the hostname field of the network interface, and with the Contact Header added to OPTION Requests generated by the SBC, Record Route is no longer required.

## SDP inactive only:

When enabled on Teams facing realm(s), this will modify the following SDP attributes in both requests and responses to and from Microsoft Teams

Message Type	Match Value	New Value
request	inactive	sendonly
reply	inactive	recvonly
request	sendonly	inactive
reply	recvonly	inactive

The screenshot shows the Oracle Enterprise Session Border Controller (ESBC) Configuration page. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'Sys'. The left sidebar lists various configuration categories: 'media-manager', 'codec-policy', 'media-manager', 'media-policy', 'realm-config' (selected), 'steering-pool', 'security', 'session-router', 'access-control', 'account-config', 'filter-config', 'ldap-config', and 'local-policy'. The main content area is titled 'Modify Realm Config' and contains the following fields:

- Identifier: Teams
- Description: Realm Facing Teams Direct Routing
- Addr Prefix: 0.0.0.0
- Network Interfaces: M00:0.4
- Media Realm List: (empty)
- Mm In Realm: ☒ enable
- Mm In Network: ☒ enable
- Mm Same Ip: ☒ enable

At the bottom of the form are 'OK' and 'Back' buttons. The top right of the configuration area has 'Save', 'Verify', and 'Discard' buttons.

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Wizards Commands

media-manager  
codec-policy  
media-manager  
media-policy  
**realm-config**  
steering-pool  
security  
session-router  
access-control  
account-config  
filter-config  
ldap-config  
local-policy

Show All

### Modify Realm Config

Media Policy

Media Sec Policy

RTCP Mux ☒ enable

Ice Profile

Teams Fqdn

Teams Fqdn In Uri ☒ enable

SDP Inactive Only ☒ enable

DTLS SrtP Profile

SrtP Msm Passthrough ☐ enable

Class Profile

In Translationid

OK Back

The third parameter is found under the **Session agent** configuration element and will be enabled on all session agents configured for Microsoft Teams 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 Microsoft Teams Session-Agents.

Configuration View Configuration

media-manager  
**security**  
session-router  
access-control  
account-config  
filter-config  
ldap-config  
local-policy  
local-routing-config  
media-profile

### Modify Session Agent

Hostname

IP Address

Port  ( Range: 0,3025..65535 )

State ☒ enable

App Protocol

App Type

Transport Method

Realm ID

---

### Modify Session Agent

SPL Options

Media Profiles

In Translationid

Out Translationid

Trust Me ☐ enable

Local Response Map

Ping Response ☒ enable



## 6.15. Configure Media Profile and Codec Policy

The Oracle Session Border Controller (SBC) uses codec policies to describe how to manipulate SDP messages as they cross the SBC. The SBC bases its decision to transcode a call on codec policy configuration and the SDP. Each codec policy specifies a set of rules to be used for determining what codecs are retained, removed, and how they are ordered within SDP.

Note: this is an optional config – configure codec policy only if deemed required

SILK & CN offered by Microsoft teams are using a payload type which is different than usual.  
Configure the media-profile as shown below,  
Go to Session-Router->Media-profile

The screenshot shows the Oracle Enterprise Session Border Controller (SBC) Configuration page. The left sidebar lists various configuration sections, with 'media-profile' selected. The main area is titled 'Modify Media Profile' and contains the following fields:

Field	Value	Range
Name	CN	
Subname	wideband	
Media Type	audio	
Payload Type	118	
Transport	RTP/AVP	
Clock Rate	16000	( Range: 0..4294967295 )
Req Bandwidth	0	( Range: 0..999999999 )
Frames Per Packet	0	( Range: 0..256 )
Parameters		
As Bandwidth	0	( Range: 0..4294967295 )

At the bottom of the form are 'OK' and 'Back' buttons. The left sidebar also includes a 'Show All' toggle.

Configure media profiles similarly, for silk codec also as given below.

Parameters	SILK-1	SILK-2
Subname	narrowband	wideband
Payload-Type	103	104
Clock-rate	8000	16000

After creating media profile, create codec-policy, addCN, to add comfort noise towards Teams.  
Go to media manager ---- codec policy

The screenshot shows the Oracle ESBC web interface. The left sidebar lists configuration categories: media-manager, codec-policy, media-manager, media-policy, realm-config, steering-pool, security, session-router, access-control, account-config, filter-config, ldap-config, and local-policy. The 'codec-policy' item is selected. The main panel is titled 'Modify Codec Policy' and contains the following fields:

- Name: addCN
- Allow Codecs: \* X
- Add Codecs On Egress: CN X
- Order Codecs: (empty)
- Packetization Time: 20
- Force Ptime: ☐ enable
- Secure Dtmf Cancellation: ☐ enable
- Dtmf In Audio: disabled
- Tone Detection: (empty)
- Tone Detect Reneegotiate Timer: (empty)

At the bottom of the form are 'OK' and 'Back' buttons. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'.

Apply this codec policy on the Teams realm

## 6.18. Configure ice profile

SBC supports ICE-Lite. This configuration is only required to support Teams media-bypass. Configure the following ice profile and apply it on the realm towards Teams.  
Go to media-manager->ice-profile. **Note: This config is required only for Media bypass model and its not needed for Non media bypass model.**

The screenshot shows the Oracle ESBC web interface. The left sidebar lists configuration categories: media-manager, codec-policy, dns-alg-constraints, dns-config, ice-profile, media-manager, media-policy, msrp-config, playback-config, realm-config, realm-group, rtcp-policy, and static-flow. The 'ice-profile' item is selected. The main panel is titled 'Modify Ice Profile' and contains the following fields:

- Name: ice
- Stun Conn Timeout: 0 (Range: 0..9999)
- Stun Keep Alive Interval: 0 (Range: 0..300)
- Stun Rate Limit: 100 (Range: 0..99999)
- Mode: PROXY

At the bottom of the form are 'OK' and 'Back' buttons. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'.

## 6.15. Configure sdes profile

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar lists various configuration categories, with 'media-security' expanded to show 'sdes-profile' selected. The main content area is titled 'Add Sdes Profile' and contains the following fields:

- 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:** (empty field)

At the bottom of the form are 'OK' and 'Back' buttons. The top right of the configuration area has 'Save', 'Verify', and 'Discard' buttons.

## 6.16. Configure Media Security Profile

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

**Assign this media policy to both Cloud Cx and Microsoft Teams Realm.**

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar lists various configuration categories, with 'media-sec-policy' selected. The main content area is titled 'Add Media Sec Policy' and contains the following fields:

- Name:** SDES
- Pass Through:** ☐ enable
- Options:** (empty text box)
- Inbound:**
  - Profile:** SDES
  - Mode:** srtp
  - Protocol:** sdes
  - Hide Egress Media Update:** ☐ enable
- Outbound:** (empty section)

At the bottom of the form are 'OK' and 'Back' buttons. The top right of the configuration area has 'Save', 'Verify', and 'Discard' buttons.

Note- Both Microsoft Teams 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.

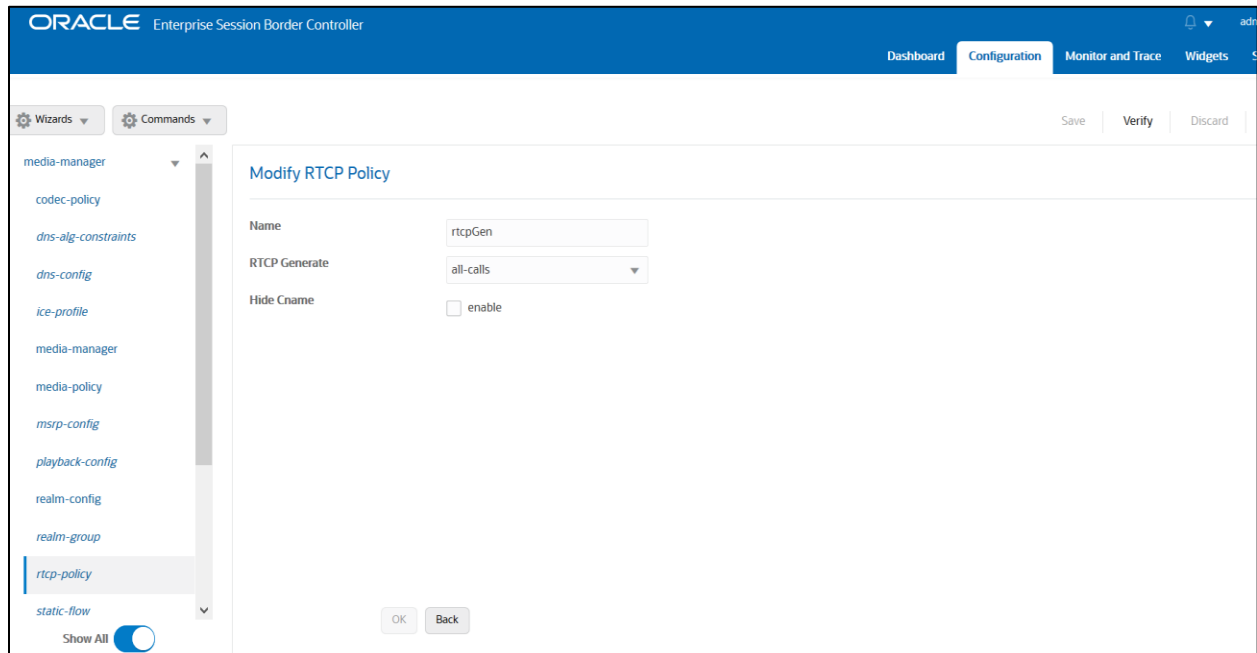
The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'media-sec-policy' selected. The main content area is titled 'Modify Media Sec Policy' and contains the following fields:

- Name:** RTP
- Pass Through:** ☐ enable
- Options:** (empty text box)
- Inbound:**
  - Profile:** (empty dropdown)
  - Mode:** rtp
  - Protocol:** none
  - Hide Egress Media Update:** ☐ enable
- Outbound:**
  - Profile:** (empty dropdown)
  - Mode:** rtp

At the bottom of the form are 'OK' and 'Back' buttons. The top right of the configuration area has 'Save', 'Verify', and 'Discard' buttons.

## 6.17 Configure RTCP Policy and RTCP Mux

The RTCP policy needs to be configured in order to generate RTCP reports towards Teams  
Go to Media-manager->rtcp-policy to configure rtcp-policy.



Apply this RTCP policy on the Teams realm. Enable rtcp-mux also in the realm.  
With this, SBC configuration is complete

## 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 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	<a href="https://lb01.byoc.us-east-1.myCloud Cx.com">lb01.byoc.us-east-1.myCloud Cx.com</a>
54.82.241.192	<a href="https://lb02.byoc.us-east-1.myCloud Cx.com">lb02.byoc.us-east-1.myCloud Cx.com</a>
54.82.241.68	<a href="https://lb03.byoc.us-east-1.myCloud Cx.com">lb03.byoc.us-east-1.myCloud Cx.com</a>
54.82.188.43	<a href="https://lb04.byoc.us-east-1.myCloud Cx.com">lb04.byoc.us-east-1.myCloud Cx.com</a>

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

**Configuration** View Configuration

- 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	GenesysCloud	
Description		
Source Address	34.211.200.63	
Destination Address		
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 Microsoft Teams IP Addresses as shown in the below example. Microsoft Teams has two subnets, 52.112.0.0/14 and 52.120.0.0/14 that must be allowed to send traffic to the SBC. Both must be configured as an access control on the Oracle SBC and associated with the realm facing Teams. Use this example to create ACL's for all MSFT Teams subnets. This example can be followed for any of the public facing interfaces, ie...SipTrunk, etc...

GUI Path: session-router/access-control

CLI Path: config t/session-router/access-control

Use this example to create ACL's for both MSFT Teams subnets, 52.112.0.0/14 and 52.120.0.0/14.

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

## 7. 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 Microsoft Teams related for Microsoft Teams related configuration. Please follow the latest Microsoft Teams Application Note to get instructions on configuring Microsoft Teams 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

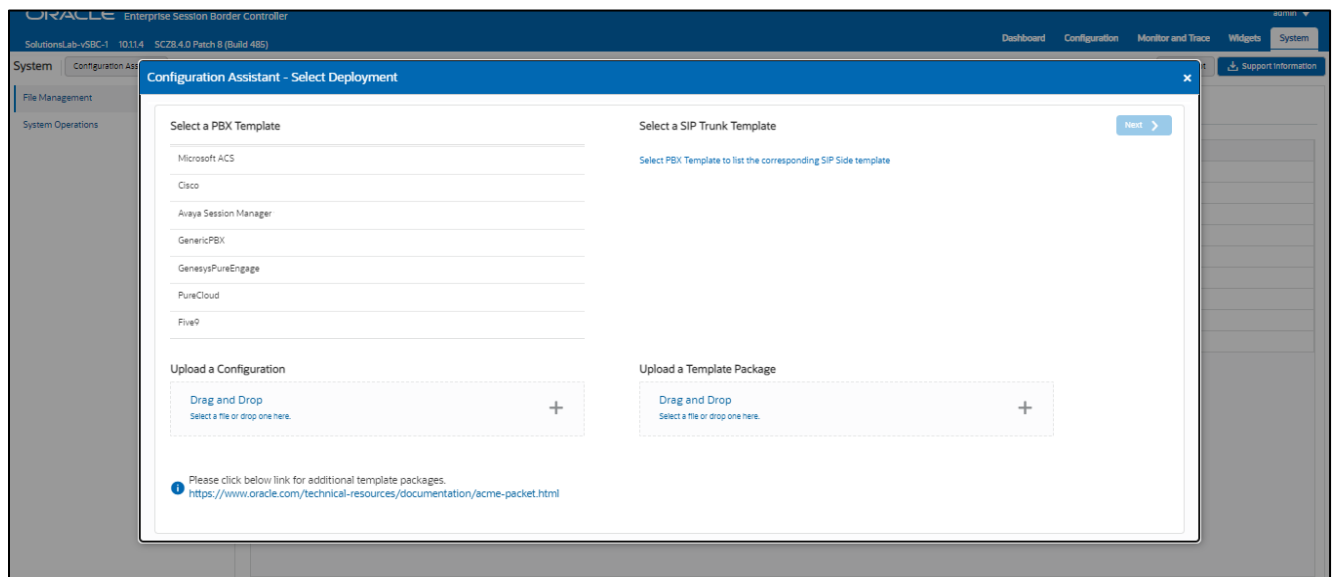
The Oracle SBC WebGui can be accessed by entering the following in your web browser.  
`http(s)://<SBC Management IP>.`

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

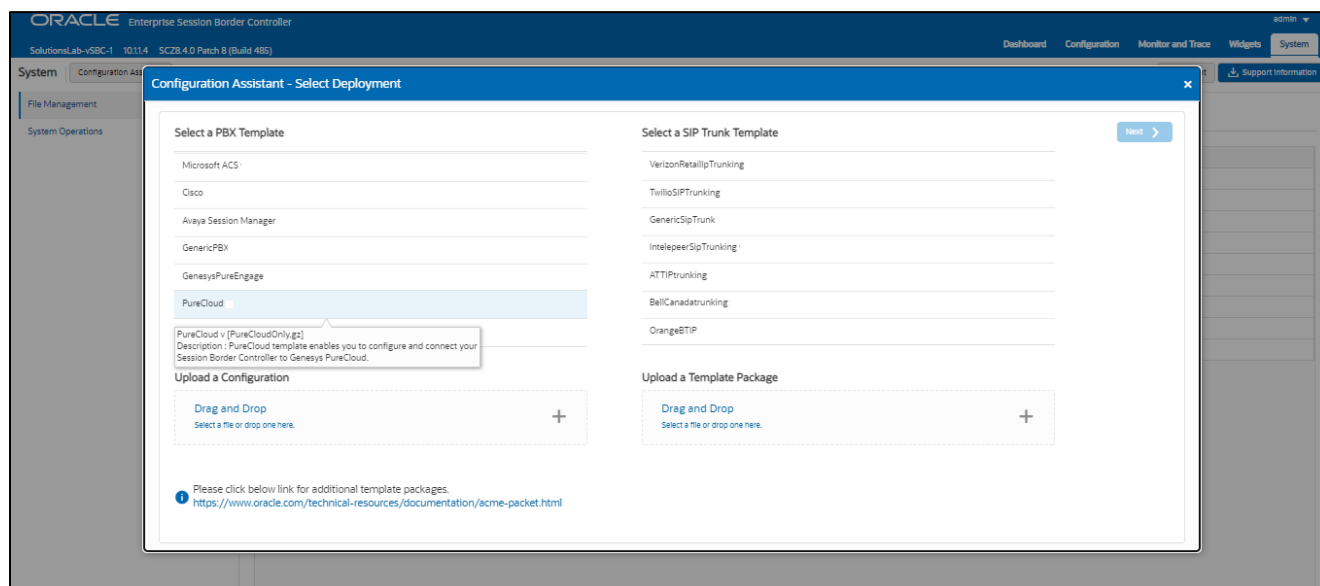
## Cloud Cx Configuration Assistant

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

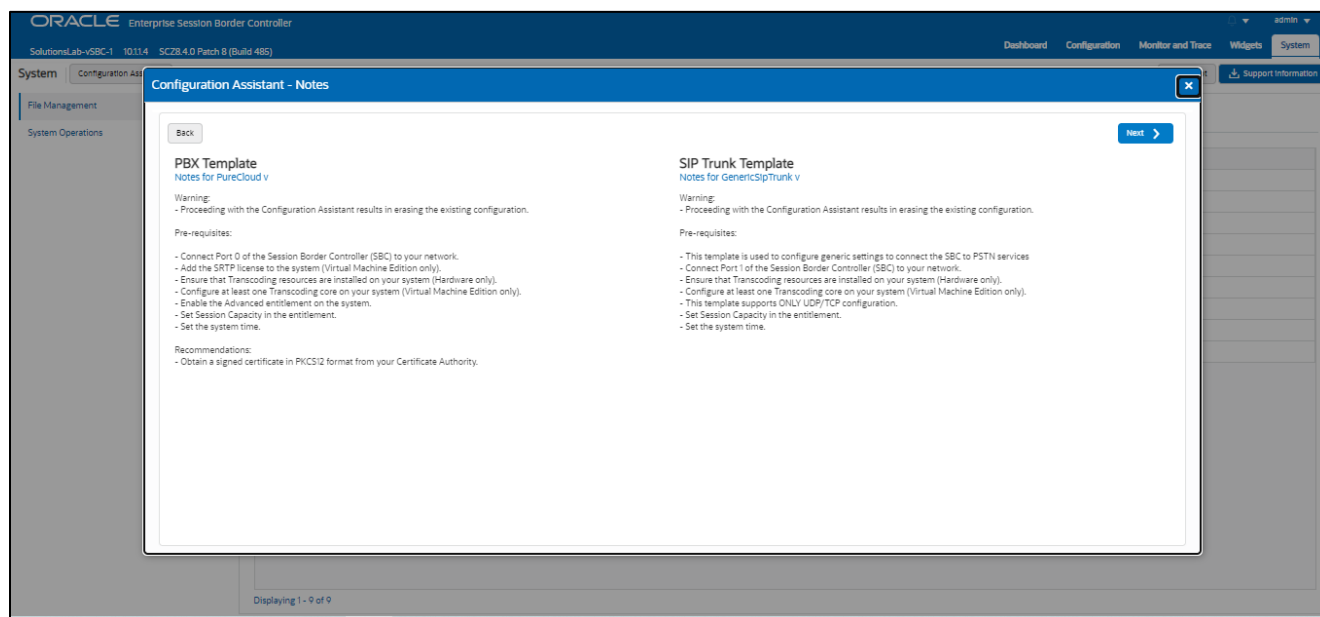




Under PBX template, we'll select Cloud Cx template. This brings up a list of available sip trunk templates.



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.

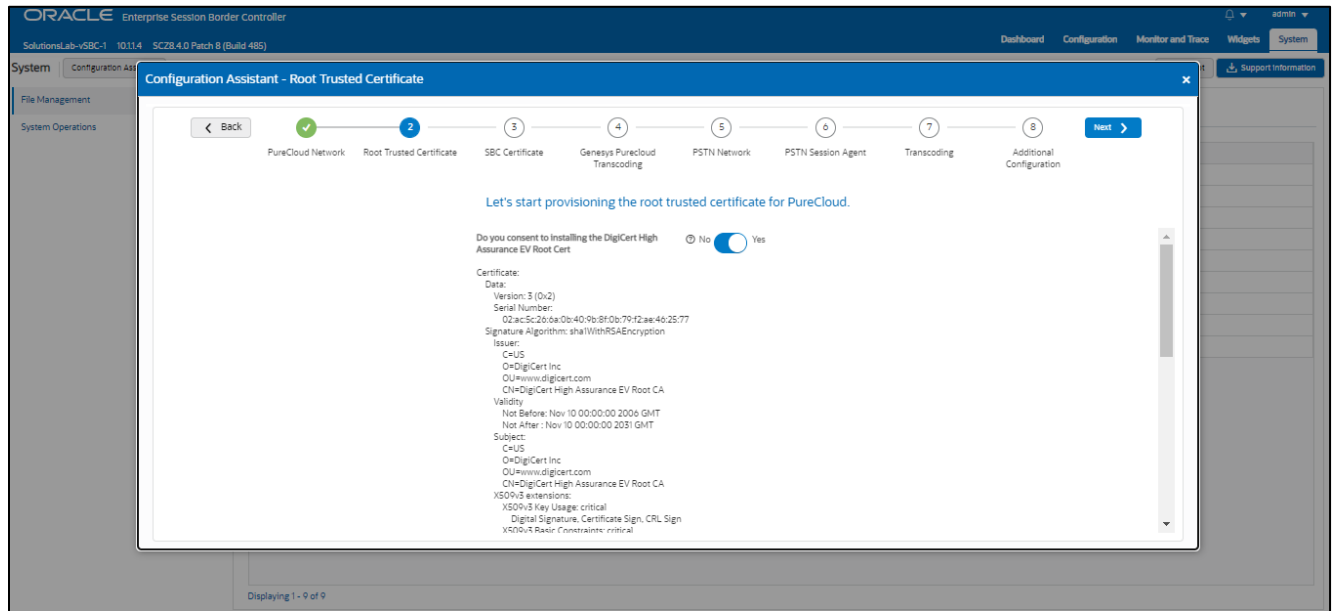
Next to each field is a help icon. If you hover over the icon, you will be provided with a description or definition of each field. Also, pay close attention to which fields are listed as “required”.

The screenshot shows the Oracle Enterprise Session Border Controller Configuration Assistant interface. The main window is titled "Configuration Assistant - PureCloud Network". It features a progress bar at the top with eight steps: 1. PureCloud Network (active), 2. Root Trusted Certificate, 3. SBC Certificate, 4. Genesys Purecloud Transcoding, 5. PSTN Network, 6. PSTN Session Agent, 7. Transcoding, and 8. Additional Configuration. Below the progress bar, the instruction "Let's configure the interface that communicates with PureCloud" is displayed. The form contains several fields, each with a help icon (i) and a "Required" label: "Realm Name" (text input), "Enter PureCloud Session Agent hostname here" (text input), "Enter the PureCloud IP here" (text input), "Port Number" (dropdown menu with "Port 0" selected), "Slot Number" (dropdown menu with "Slot 0" selected), and "Network IP Address" (text input). A "Skip" button is located at the top right of the form. The background shows the Oracle Enterprise Session Border Controller dashboard with various tabs like Dashboard, Configuration, Monitor and Trace, Widgets, and System.

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

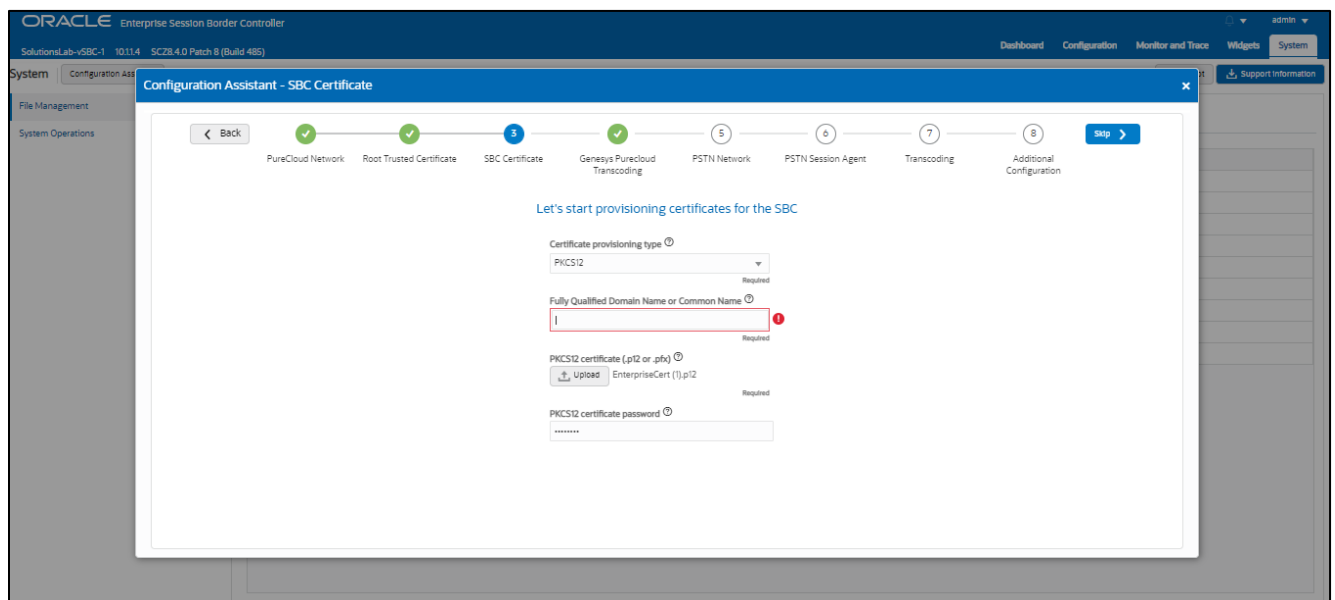
Page 2 of this template is where the SBC will import the **DigiCert High Assurance EV Root Cert CA** certificate, which Cloud Cx uses to sign the certificates it presents to the SBC during the TLS handshake.

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).

The screenshot shows the 'Configuration Assistant - SBC Certificate' window in the Oracle Enterprise Session Border Controller interface. The window has a progress bar at the top with steps: PureCloud Network, Root Trusted Certificate, SBC Certificate (current step), Genesys Purecloud Transcoding, PSTN Network, PSTN Session Agent, Transcoding, and Additional Configuration. The main content area is titled 'Let's start provisioning certificates for the SBC'. It contains a 'Certificate provisioning type' dropdown set to 'CSR'. Below it is a 'Fully Qualified Domain Name or Common Name' field with a red border and a red exclamation mark icon, indicating it is required. Other fields include 'Country', 'State', 'Locality', and 'Organization', all with red exclamation mark icons indicating they are required. The bottom of the window shows 'Displaying 1 - 9 of 9'.

## Page 4 – Cloud Cx side Transcoding

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.

The screenshot shows the 'Configuration Assistant - Genesys Purecloud Transcoding' window in the Oracle Enterprise Session Border Controller interface. The window has a progress bar at the top with steps: PureCloud Network, Root Trusted Certificate, SBC Certificate, Genesys Purecloud Transcoding (current step), PSTN Network, PSTN Session Agent, Transcoding, and Additional Configuration. The main content area is titled 'Let's configure transcoding for Genesys Purecloud side'. It contains a question 'Do you want to select media codecs (SBC to PureCloud)?' with radio buttons for 'No' and 'Yes' (selected). Below the question is a 'Select media codecs' dropdown menu. The dropdown menu is open, showing a list of codecs: G729, G722, PCMU, and PCMA. The bottom of the window shows 'Displaying 1 - 9 of 9'.

## 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.

The screenshot shows the 'Configuration Assistant - PSTN Network' window in the Oracle Enterprise Session Border Controller. The progress bar at the top indicates the current step is 'PSTN Network' (step 5), with previous steps like 'PureCloud Network', 'Root Trusted Certificate', 'SBC Certificate', and 'Genesys Purecloud Transcoding' completed. The main area is titled 'Let's configure the interface that communicates with the PSTN' and contains the following required fields:

- Realm Name (Required)
- Port Number (Required) - Port 1 dropdown
- Slot Number (Required) - Slot 0 dropdown
- Network IP address (Required)
- Network IP subnet mask (Required)

At the bottom, it says 'Displaying 1 - 9 of 9'.

## 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.

The screenshot shows the 'Configuration Assistant - PSTN Session Agent' window. The progress bar indicates the current step is 'PSTN Session Agent' (step 6), with previous steps completed. The main area is titled 'Let's configure the Session Agent for PSTN' and contains the following fields:

- PSTN Session Agent hostname (Required)
- PSTN Session Agent IP Address (Required)
- PSTN Session Agent Port (Required)
- Does your service provider have a second Hostname/IP address for Sip Signalling? (Radio buttons: No, Yes)

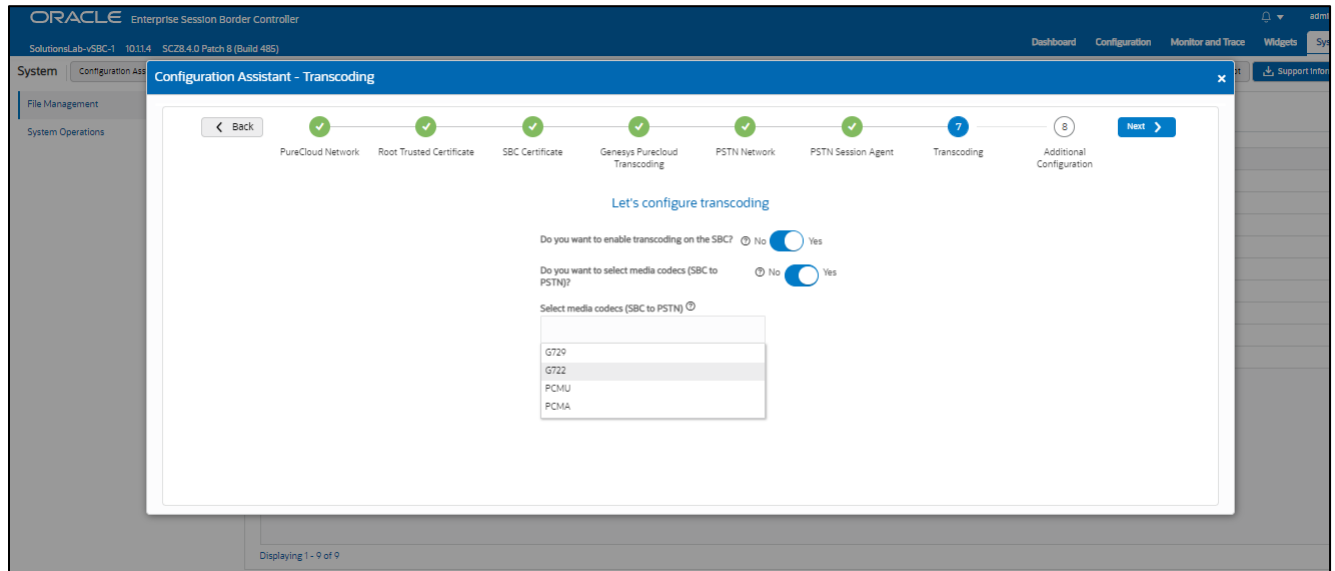
At the bottom, it says 'Displaying 1 - 9 of 9'.

Please fill the required fields and click Next.

## Page 7 - PSTN side Transcoding

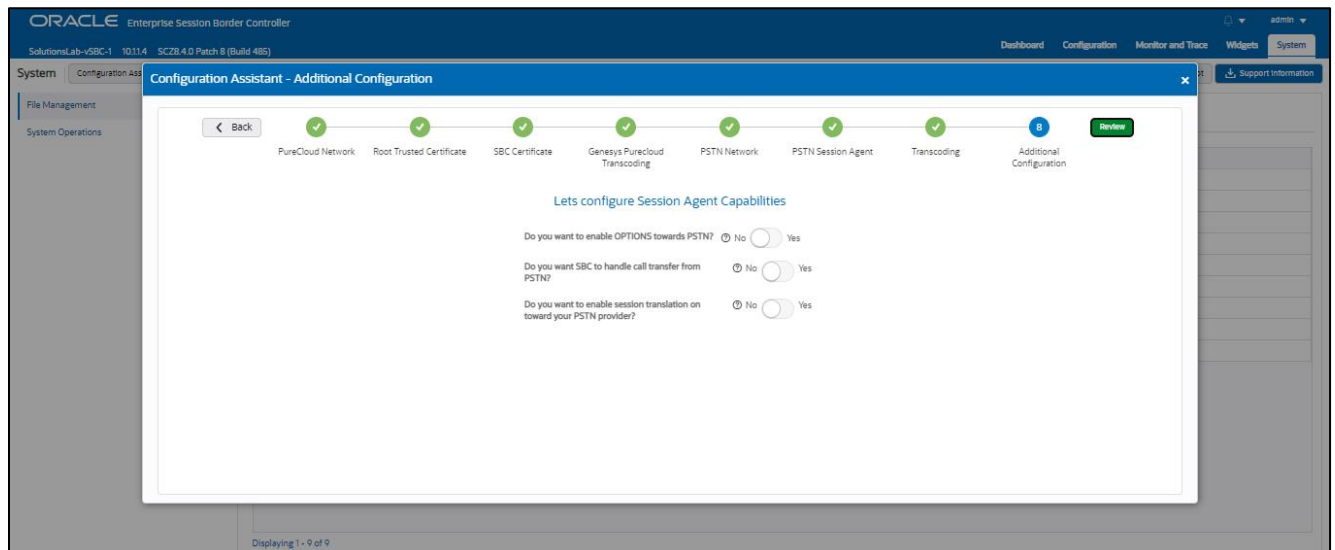
Page 7 is where you will be able to configure transcoding between the SBC and PSTN Trunk.

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.



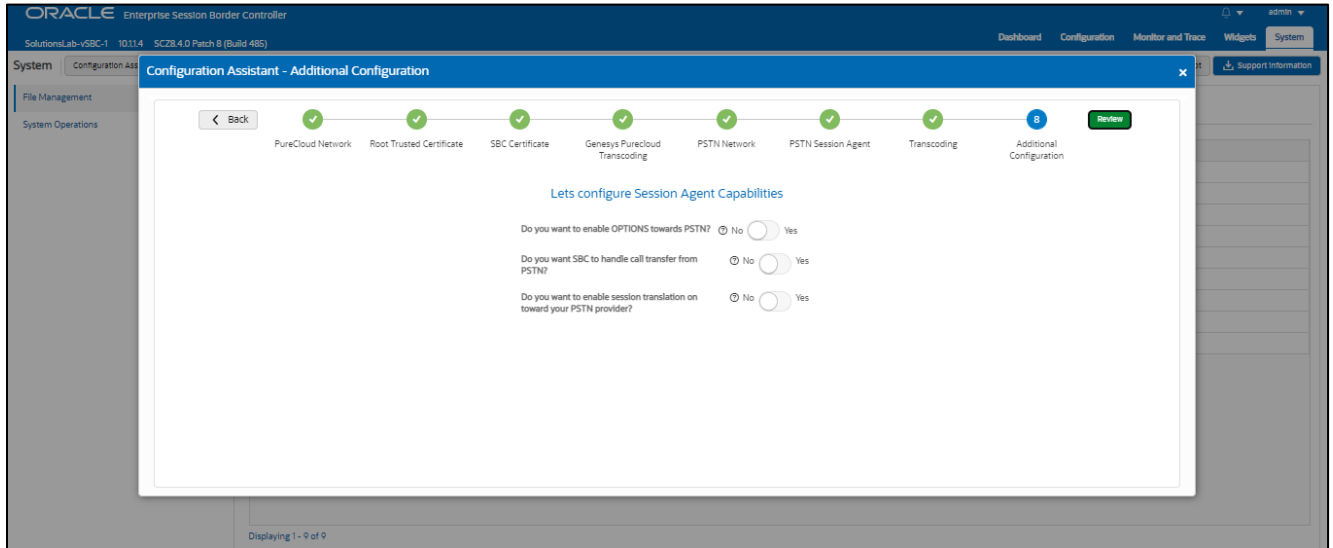
## Page 8 – Additional Configuration

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



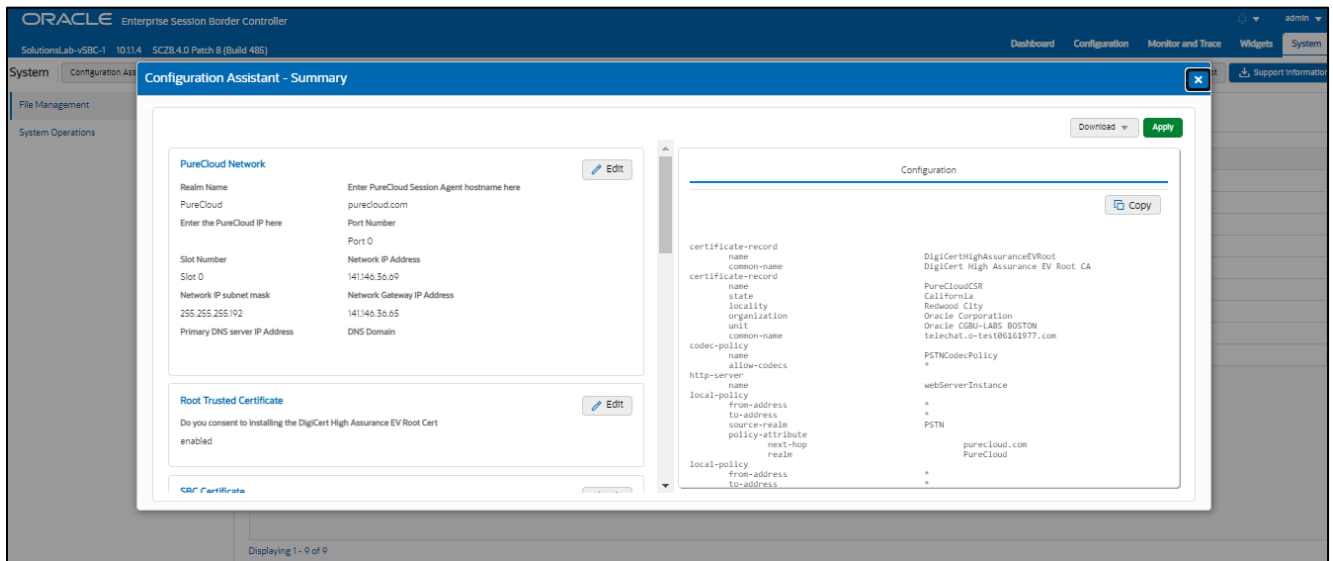
## Review

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.

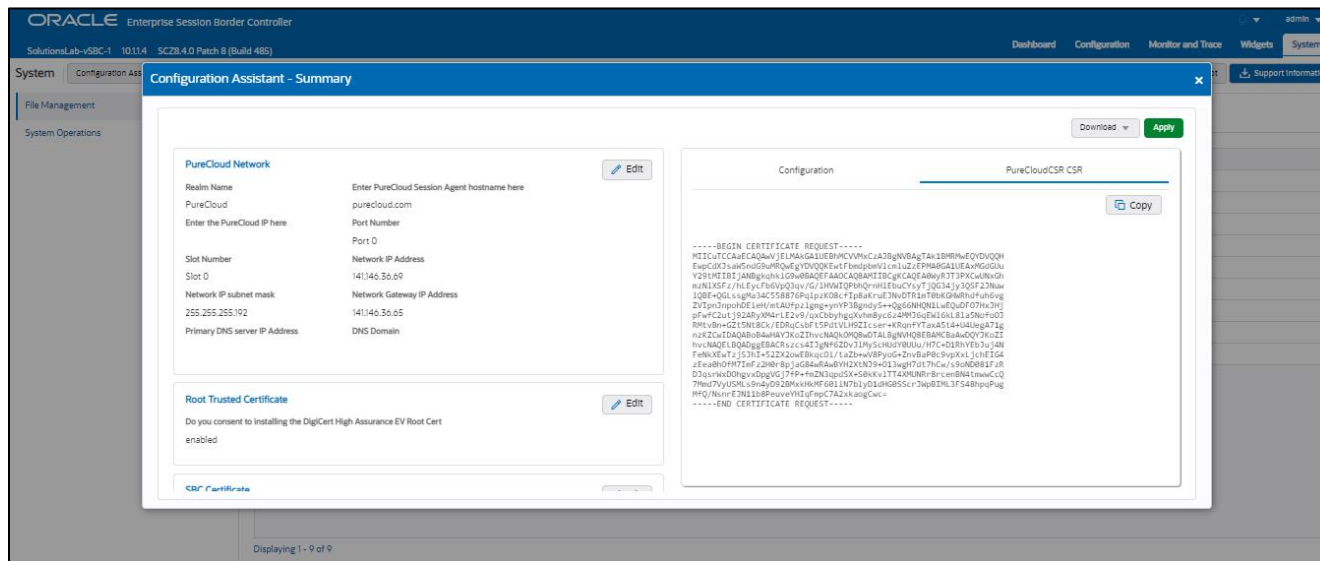
The right side displays the entire configuration created and when applicable, will also have a CSR tab that contains a certificate that can be signed by a CA authority.



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

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

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



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

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

### Download and/or Apply

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

Now you can click “**Confirm**” to confirm you want to apply the configuration to the SBC. The SBC will reboot. When it comes back up, the SBC will have a basic configuration in place for 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.

## 8. 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](https://blogs.oracle.com/oracle)

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

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

 [oracle.com](https://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