



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

Technical Application Note



Disclaimer

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

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 Cloud Cx and Twilio Elastic SIP Trunking Oracle Public IP Address Masked	26 ^h May 2021
1.1	Oracle Public IP Address masked	18 th Nov 2021
1.2	Added New Section - Configure Oracle SBC via Configuration Assistant	27 Jan 2022
1.3	Rebranding of Genesys PureCloud to Genesys Cloud Cx	04 April 2025

Table of Contents

1. INTENDED AUDIENCE	4
2. DOCUMENT OVERVIEW	4
2.1. TWILIO ELASTIC SIP TRUNKING	4
2.2. GENESYS CLOUD CX	5
3. INTRODUCTION.....	5
3.1. AUDIENCE	5
3.2. REQUIREMENTS	5
3.3. ARCHITECTURE	6
4. CONFIGURE GENESYS CLOUD CX	6
4.1 EXTERNAL TRUNK CONFIGURATION	7
4.1.1 Create a new External Trunk.....	7
4.1.2 Set Inbound SIP Termination Identifier	7
4.1.3 Set Outbound SIP Servers or Proxies.....	8
4.1.4 Set Calling Address	8
4.1.5 Set SIP Access Control	9
4.1.6 Enable E.164 format.....	9
4.2 SITE CONFIGURATION	9
4.2.1 Create a New Site.....	9
4.2.2 Number Plans & Classifications.....	10
4.2.3 Configure outbound route	11
4.2.4 Simulate call.....	11
4.3 DID ASSIGNMENT	12
4.3.1 Create DID Range	12
4.3.2 Assign DID to User	12
5. CONFIGURING THE SBC	13
5.1. VALIDATED ORACLE SBC VERSION	13
6. NEW SBC CONFIGURATION	13
6.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC	13
6.2. CONFIGURE SBC USING WEB GUI	17
6.3. CONFIGURE SYSTEM-CONFIG	18
6.4. CONFIGURE PHYSICAL INTERFACE VALUES	19
6.5. CONFIGURE NETWORK INTERFACE VALUES	21
6.6. ENABLE MEDIA MANAGER	22
6.7. CONFIGURE REALMS.....	23
6.8. CONFIGURING A CERTIFICATE FOR SBC	25
6.9. TLS-PROFILE	29
6.10. CONFIGURE SIP INTERFACES.....	29
6.11. CONFIGURE SESSION-AGENT.....	30
6.12. CONFIGURE LOCAL-POLICY	31
6.13. CONFIGURE STEERING-POOL.....	32
6.14. ENABLE OPTIONS PING RESPONSE.	33
6.15. CONFIGURE SDES PROFILE	35
6.16. CONFIGURE MEDIA SECURITY PROFILE	35
6.17 ACCESS CONTROL.....	36
7. TWILIO ELASTIC SIP TRUNKING CONFIGURATION.....	37

7.1. CREATE AN IP-ACL RULE.....	37
7.2. CREATE A NEW TRUNK	38
7.3. ASSOCIATE PHONE NUMBERS ON YOUR TRUNK.....	42
CONFIGURING THE ORACLE SBC THROUGH CONFIG ASSISTANT	42
SECTION OVERVIEW AND REQUIREMENTS	42
INITIAL GUI ACCESS	43
CLOUD CX CONFIGURATION ASSISTANT.....	43
PAGE 1- CLOUD CX NETWORK	44
PAGE 2 - IMPORT DIGICERT TRUSTED CA CERTIFICATE FOR CLOUD CX.....	45
PAGE 3 - SBC CERTIFICATES FOR CLOUD CX SIDE	45
PAGE 4 – CLOUD CX SIDE TRANSCODING	47
PAGE 5 – TWILIO ELASTIC SIP TRUNK NETWORK	47
PAGE 6 – TWILIO SESSION AGENT	48
PAGE 7 - TWILIO SIDE TRANSCODING.....	48
PAGE 8 – IMPORT DIGI CERT ROOT CA CERTIFICATE FOR TWILIO SIDE	49
PAGE 9 – SBC CERTIFICATE FOR TWILIO	49
REVIEW	50
DOWNLOAD AND/OR APPLY	52
CONFIGURATION ASSISTANT ACCESS	52
9. TEST PLAN EXECUTED	52

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.

2. Document Overview

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

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

Related documentation can be found below –

2.1. Twilio Elastic SIP Trunking

[Twilio Elastic SIP Trunking](#) is a cloud-based solution that provides connectivity for IP-based communications infrastructure to connect to the PSTN for making and receiving telephone calls to the rest of the world via any

broadband internet connection. Twilio's Elastic SIP Trunking service automatically scales, up or down, to meet your traffic needs with unlimited capacity. In just minutes, you can deploy globally with Twilio's easy-to-use self-service tools without having to rely on slow providers.

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

2.2. Genesys 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/>

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

3. Introduction

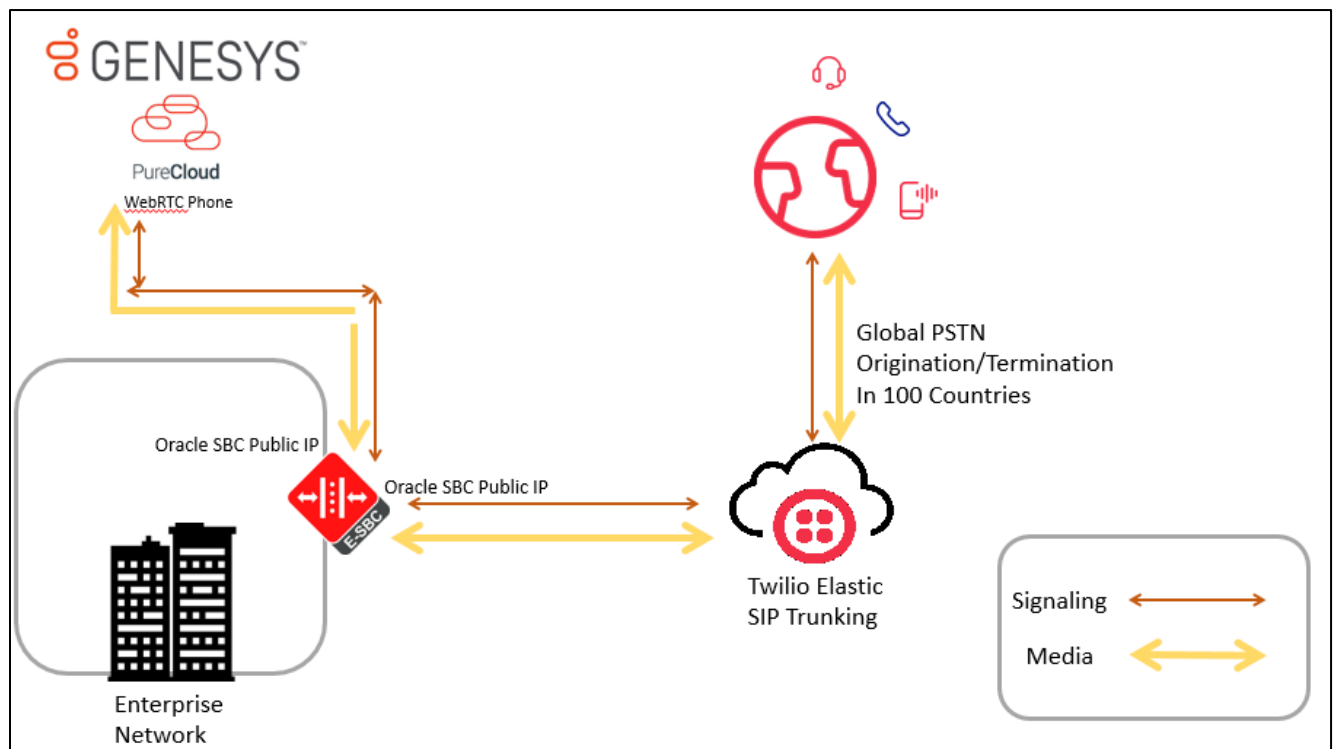
3.1. Audience

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

3.2. Requirements

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

3.3. Architecture



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

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

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

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

4. Configure Genesys Cloud Cx

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

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

users on Cloud Cx System who can originate and accept the calls. These calls traverse through Oracle SBC with which we can implement several security and additional features as per our requirement.

For the purpose of this Application note, the connection between Oracle SBC and Genesys Cloud Cx is set as UDP.TLS and TCP Transport Protocol are also available as Transport Protocol on Genesys Cloud Cx.

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: UDP (TCP and TLS are also available)

4.1.2 Set Inbound SIP Termination Identifier

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

The screenshot displays the 'Edit External Trunk' configuration page in the Oracle Cloud CX Portal. The breadcrumb trail at the top reads 'Telephony / Trunks / External Trunks / Edit External Trunk'. On the left, a sidebar menu lists various configuration areas: Topology, Metrics, Trunks (selected), Sites, Edge Groups, Edges, Phone Management, Certificate Authorities, DID Numbers, and Extensions. The main content area is divided into several sections. The 'External Trunk Name' field is set to 'OracleSolutionsLabBYOCSBC'. The 'Trunk State' is a toggle switch labeled 'In Service'. The 'Protocol' is set to 'UDP'. The 'Inbound / Termination' section includes the 'Inbound SIP Termination Identifier' set to 'OracleSBCCloudCxTesting' and the 'Inbound SIP Termination Header' field, which is currently empty. A 'DNIS Replacement Routing' toggle is shown as 'Disabled'. On the right side, a summary box displays the 'Status' as 'Operational' (green dot), the 'Type' as 'Generic BYOC Carrier', and 'Metrics' for 'Inbound Calls', 'Outbound Calls', and 'QoS Mismatches', all showing a count of 0.

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 'Trunks' configuration page. On the left is a sidebar with navigation links: Topology, Metrics, Trunks (selected), Sites, Edge Groups, Edges, Phone Management, Certificate Authorities, DID Numbers, and Extensions. The main content area is divided into two sections. The top section, 'Inbound Request-URI Reference', contains two rows: 'FQDN Method' with the value 'INVITE sip:+xxxxxxxxxx@OracleSBCPureCloudTesting.byoc.usw2.pure.cloud' and 'TGRP Method' with the value 'INVITE sip:+xxxxxxxxxx;tgrp=OracleSBCPureCloudTesting;trunk-context=byoc.usw2.pure.cloud@lb01.byoc.usw2.pure.cloud'. The bottom section, 'Outbound', contains three rows: 'Outbound SIP Termination FQDN' with the value 'solutionslab.cgbubedford.com', 'Outbound SIP TGRP Attribute' (empty), and 'TGRP Context-ID' (empty). Below these is an 'Outbound Request-URI Reference' section with the value '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 navigation links: Topology, Metrics, Trunks (selected), Sites, Edge Groups, Edges, Phone Management, Certificate Authorities, DID Numbers, and Extensions. The main content area is divided into several sections. The 'Calling' section contains 'Address' (19729132636), 'Name' (empty), 'Address Override Method' (Always), and 'Name Override Method' (Always). The 'SIP Access Control' section contains 'Allow the Following Addresses' with two empty input fields and a '+ Add an IP or CIDR address' button. The 'External Trunk Configuration' section contains 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)

The screenshot shows the 'SIP Access Control' configuration page. On the left is a sidebar with navigation links: Topology, Metrics, Trunks (selected), Sites, Edge Groups, Edges, Phone Management, Certificate Authorities, DID Numbers, and Extensions. The main content area is titled 'Calling' and includes a 'Show Password' checkbox. Below this, there are fields for 'Address' (containing '+14152302042') and 'Name' (containing 'OracleSolutionsLab8YOCSBCTest'). To the right of these fields are dropdown menus for 'Address Override Method' and 'Name Override Method', both set to 'Always'. Below these is the 'SIP Access Control' section, which has a sub-header 'Allow the Following Addresses'. It contains two empty input fields, each with a trash icon to its right. At the bottom of this section is a text input field labeled 'Add an IP or CIDR address' with a plus icon to its right. The page footer includes the text 'External Trunk Configuration' and two links: 'Expand All' and 'Collapse All'.

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.

The screenshot shows two settings in a row. The first is 'Address Digits Length' with a question mark icon and a text input field containing the value '0'. The second is 'Address Omit + Prefix' with a question mark icon and a refresh icon. It features a toggle switch that is currently in the 'Disabled' position, with the word 'Disabled' written inside the toggle.

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**.

The screenshot shows the 'Edit Site' configuration page in the Twilio console. The page has a sidebar on the left with navigation links: Topology, Metrics, Trunks, Sites (selected), Edge Groups, Edges, Phone Management, Certificate Authorities, DID Numbers, and Extensions. The main content area has tabs for General, Number Plans, Outbound Routes, and Simulate Call. The 'General' tab is active, showing the following fields:

- Site Name:** OracleSolutionslabSBCBYOC
- Description:** (empty text field)
- Location:** Twilio Headquarters (dropdown menu)
- Media:** Geo-Lookup TURN (toggle switch, currently Disabled)
- Automatic Updates:** Recurrence Type (Daily, dropdown menu)
- Time Zone:** America/Los_Angeles (-07:00) (dropdown menu)

On the right side, there is a summary box for the 'Default Site' with the following information:

- Make this Site my default Site** (link)
- Type:** Branch Site
- Media Model:** Cloud
- Phones:** 1
- Restart all phones assigned to this Site** (link)
- Edge Group:** PureCloud Voice - AWS (link)
- Topology Diagram:** Show Topology (link)

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.

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.

4.3 DID Assignment

4.3.1 Create DID Range

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

4.3.2 Assign DID to User.

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

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

5. Configuring the SBC

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

5.1. Validated Oracle SBC version

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

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

6. New SBC configuration

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

6.1. Establishing a serial connection to the SBC

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

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

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

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

```
$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
?assword: █
```

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

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

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

Password is acceptable.
```

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

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

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

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

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

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

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

NN4600-139(configure)#
```

Note: There is no management IP configured by default.

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

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

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

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

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

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**.

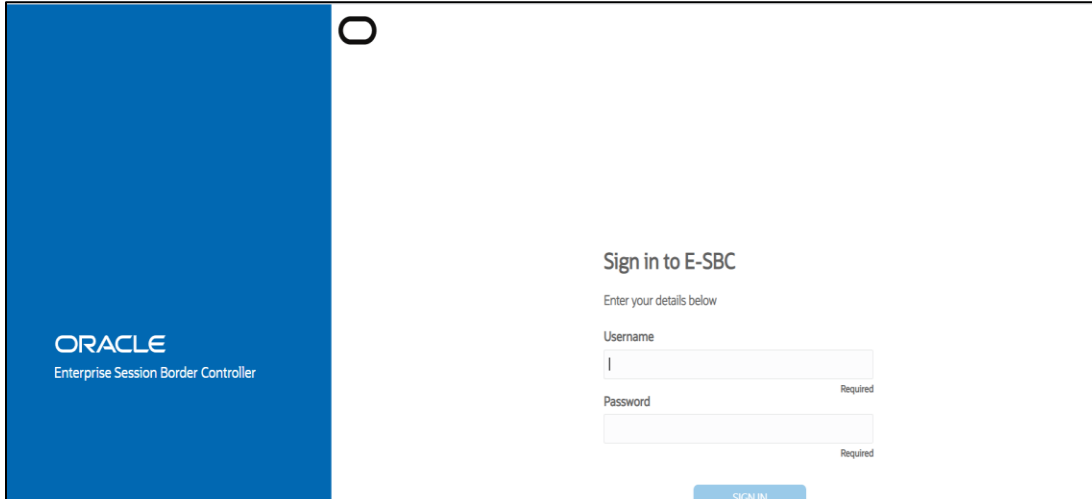
Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

```
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
```


6.2. Configure SBC using Web GUI

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

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



ORACLE
Enterprise Session Border Controller

Sign in to E-SBC

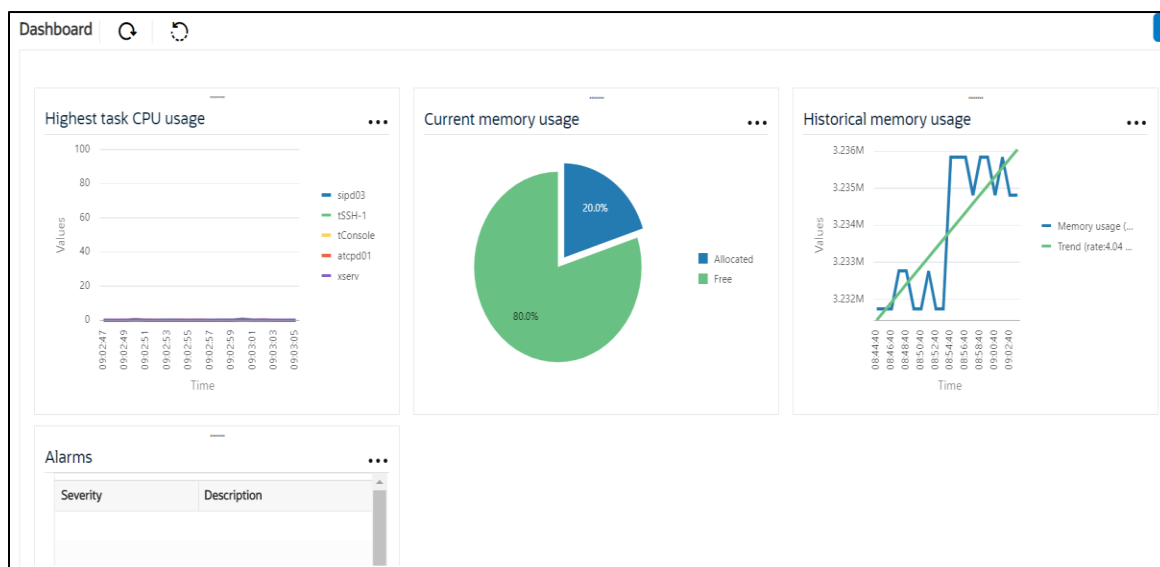
Enter your details below

Username

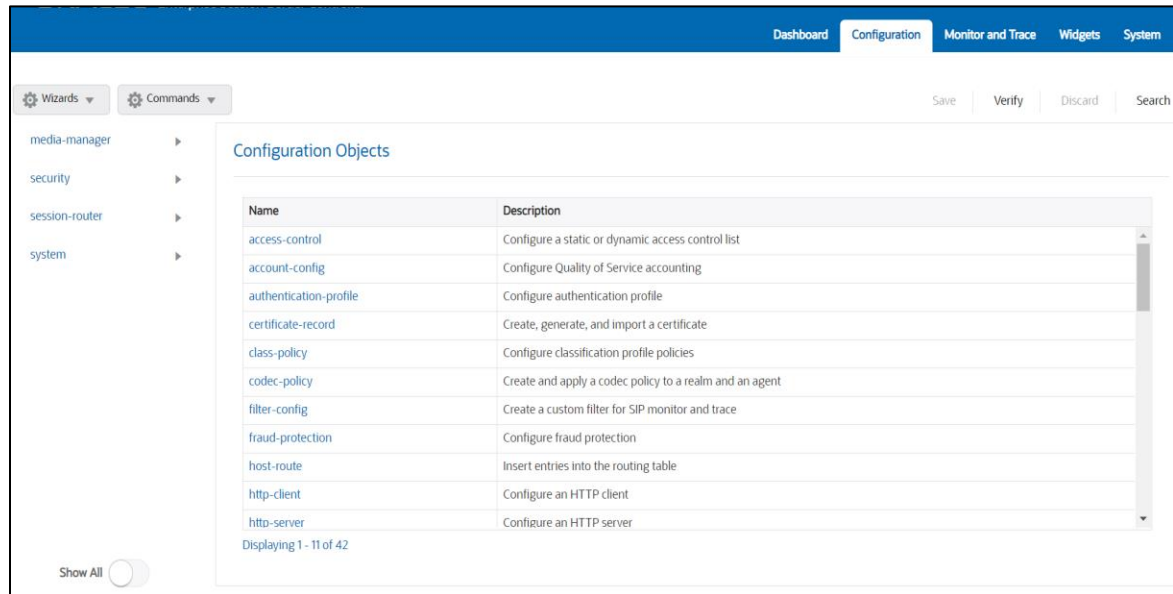
Password

SIGN IN

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



Navigate to Configuration as shown below, to configure the SBC



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

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

The expert mode is used for configuration.

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

6.3. Configure system-config

Navigate to system->system-config

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
redundancy-config
snmp-community
spl-config
system-config
tdm-config
trap-receiver

Show All

Modify System Config

Hostname: OracleSBC

Description:

Location:

Mib System Contact:

Mib System Name:

Mib System Location:

Acp TLS Profile:

OK Delete

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

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
redundancy-config
snmp-community
spl-config
system-config
tdm-config
trap-receiver

Show All

Modify System Config

Displaying U - U or U 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/releases/esbc_scz840_releasenotes.pdf

The above step is needed only if any transcoding is used in the configuration.
If there is no transcoding involved, then the above step is not needed.

6.4. Configure Physical Interface values

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

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

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

Please configure M00 interface as below.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The 'Configuration' tab is active. On the left, there is a sidebar with a list of configuration options: 'host-route', 'http-client', 'http-server', 'network-interface', 'ntp-config', 'phy-interface' (highlighted), 'redundancy-config', 'snmp-community', 'spl-config', 'system-config', and 'trap-receiver'. The main area displays the 'Add Phy Interface' form for the M00 interface. The form fields are as follows:

Field	Value	Notes
Name	M00	
Operation Type	Media	
Port	0	(Range: 0..5)
Slot	0	(Range: 0..2)
Virtual Mac		
Admin State	<input checked="" type="checkbox"/> enable	
Auto Negotiation	<input checked="" type="checkbox"/> enable	
Duplex Mode	FULL	
Speed	100	

At the bottom of the form, there are 'OK' and 'Back' buttons. In the top right corner of the configuration area, there are 'Save' and 'Verify' buttons.

Please configure M10 interface as below

The screenshot shows the 'Enterprise Session Border Controller' configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration categories: 'session-router', 'system', 'fraud-protection', 'host-route', 'http-client', 'http-server', 'network-interface', 'ntp-config', 'phy-interface' (selected), 'redundancy-config', and 'snmp-community'. The main area is titled 'Add Phy Interface' and contains the following fields:

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

At the bottom of the form are 'OK' and 'Back' buttons. There are also 'Wizards' and 'Commands' tabs at the top left, and 'Save' and 'Verify' buttons at the top right.

6.5. Configure Network Interface values

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

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

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

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

Please configure network interface M00 as below

The screenshot shows the Oracle Enterprise Session Border Controller (ESBC) Configuration page. The left sidebar lists various configuration options, with 'network-interface' selected. The main area is titled 'Add Network Interface' and contains the following fields:

- Name: M00
- Sub Port Id: 0 (Range: 0..4095)
- Description: (Empty text area)
- Hostname: customers.telechat.o-test06161977.cor
- 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 navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'.

Similarly, configure network interface M10 as below

The screenshot shows the Oracle Enterprise Session Border Controller (ESBC) Configuration page. The left sidebar lists various configuration options, with 'network-interface' selected. The main area is titled 'Modify Network Interface' and contains the following fields:

- Name: M10
- Sub Port Id: 0 (Range: 0..4095)
- Description: (Empty text area)
- Hostname: solutionslab.cgbubedford.com
- IP Address: (Empty text field)
- Pri Utility Addr: (Empty text field)
- Sec Utility Addr: (Empty text field)
- Netmask: 255.255.255.192
- Gateway: (Empty text field)

At the bottom of the form are 'OK' and 'Back' buttons. The top navigation bar includes 'Configuration', 'View Configuration', and a search icon.

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

The screenshot shows the 'Modify Media Manager' configuration page in the Oracle Enterprise Session Border Controller. The left sidebar lists various configuration categories, with 'media-manager' selected. The main area contains the following settings:

Parameter	Value	Range
State	<input checked="" type="checkbox"/> enable	
Flow Time Limit	86400	(Range: 0..4294967295)
Initial Guard Timer	300	(Range: 0..4294967295)
Subsq Guard Timer	300	(Range: 0..4294967295)
TCP Flow Time Limit	86400	(Range: 0..4294967295)
TCP Initial Guard Timer	300	(Range: 0..4294967295)
TCP Subsq Guard Timer	300	(Range: 0..4294967295)
Hint Rtcp	<input type="checkbox"/> enable	
AlgId Log Level	NOTICE	
Mbcd Log Level	NOTICE	

Buttons at the bottom: OK, Delete, Save, Verify, Discard.

The screenshot shows the 'Modify Media Manager' configuration page with additional settings visible. The left sidebar is scrolled down to show 'media-manager' selected. The main area contains the following settings:

Parameter	Value	Range
Media Policing	<input checked="" type="checkbox"/> enable	
Max Arp Rate	10	(Range: 0..100)
Max Signaling Packets	0	(Range: 0..4294967295)
Max Untrusted Signaling	1	(Range: 0..100)
Min Untrusted Signaling	1	(Range: 0..100)
Tolerance Window	30	(Range: 0..4294967295)
Untrusted Drop Threshold	0	(Range: 0..100)
Trusted Drop Threshold	0	(Range: 0..100)
Acl Monitor Window	30	(Range: 5..3600)
Trap On Demote To Deny	<input type="checkbox"/> enable	

Buttons at the bottom: OK, Delete, Save, Verify, Discard.

6.7. Configure Realms

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

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

Config Parameter	Twilio Realm	GenesysCloud d Realm
Identifier	TwilioSipTrunk	GenesysCloud
Network Interface	M00	M10
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Media Sec policy	sdesppolicy	RTP
Access Control Trust Level	High	High

Configuration View Configuration Q

media-manager ▼

- codec-policy
- media-manager
- media-policy
- realm-config
- steering-pool

security ▶

session-router ▶

system ▶

Modify Realm Config

Identifier: TwilioSipTrunk

Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M00:0.4 ×

Media Realm List:

Mm In Realm: ☒ 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

Create another realm for Genesys Cloud Cx –

Configuration

View Configuration

Q

media-manager

codecs-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

Mrm In Realm

☒ enable

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace

Wizards

Commands

Save

Verify

media-manager

codecs-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 Node

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

6.8. Configuring a certificate for SBC

This section describes how to configure the SBC for TLS and SRTP communication for Twilio Elastic SIP Trunking. Twilio Elastic SIP Trunking allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by one of the trusted Certificate Authorities.

The process includes the following steps:

- 1) Create a certificate-record – “Certificate-record” are configuration elements on Oracle SBC, which captures information for a TLS certificate – such as common-name, key-size, key-usage etc.
 - SBC – 1 certificate-record assigned to SBC
 - Root – 1 certificate-record for root cert
- 2) Deploy the SBC and Root certificates on the SBC

Step 1 – Creating the certificate record

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

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

The screenshot shows the Oracle Enterprise Session Border Controller (SBC) Configuration page. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar shows a tree view with categories: 'media-manager', 'security', 'authentication-profile', 'certificate-record' (selected), 'tls-global', 'tls-profile', 'session-router', and 'system'. The main content area is titled 'Modify Certificate Record' and contains a form with the following fields:

Field	Value
Name	TwilioRootCACertChain
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	Solutions
Common Name	Chain CA Cert
Key Size	2048
Alternate Name	

At the bottom of the form are 'OK' and 'Back' buttons. In the top right corner of the configuration area are 'Save' and 'Verify' buttons.

Dashboard
Configuration
Monitor and Trace

Wizards
Commands
Save
Verify

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

Modify Certificate Record

Key Size: 2048
Alternate Name:
Trusted: ☒ enable
Key Usage List: digitalSignature keyEncipherment
Extended Key Usage List: serverAuth
Key Algor: rsa
Digest Algor: sha256
Ecdsa Key Size: p256

OK
Back

Show All

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

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

Step 2 – Generating a certificate signing request

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

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

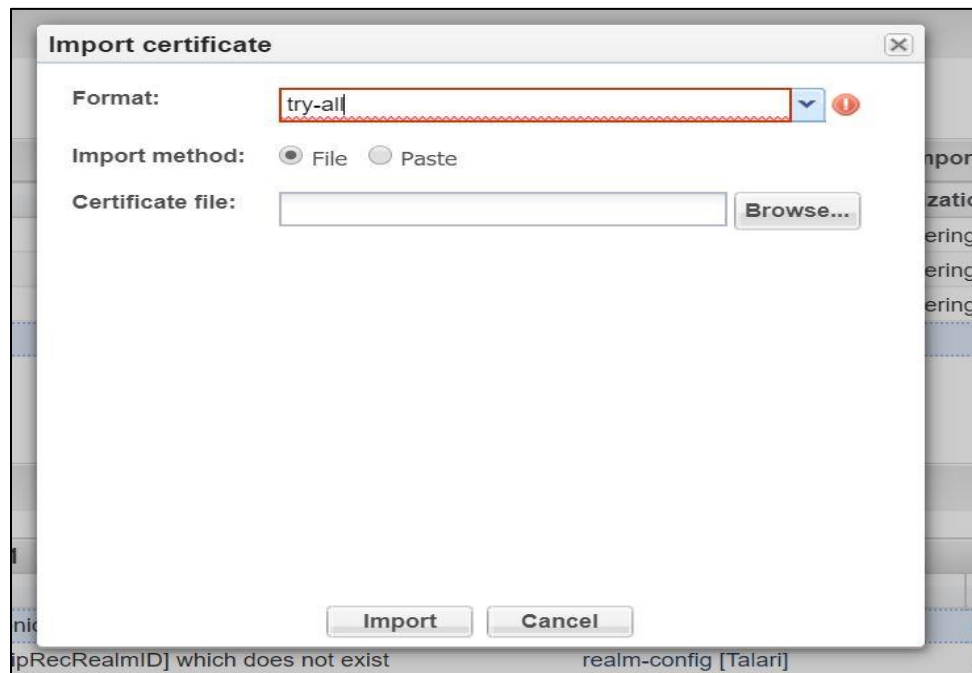
- Select the certificate and generate certificate on clicking the “Generate” command.
- Please copy/paste the text that is printed on the screen as shown below and upload to your CA server for signature.



- Also, note that a save/activate is required

Step 3 – Deploy SBC & root certificates

Once certificate signing request have been completed – import the signed certificate to the SBC. Please note – all certificates including root and intermediate certificates are required to be imported to the SBC. Once done, issue save/activate from the WebGUI



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

6.9. 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

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

6.10. Configure SIP Interfaces

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

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

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

The screenshot shows the 'Modify SIP Interface' configuration page. On the left is a sidebar with a list of configuration categories: 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, and sip-interface (which is highlighted). The main area is titled 'Modify SIP Interface'. It includes a 'State' section with a checked 'enable' checkbox. Below this is a 'Realm ID' dropdown menu set to 'TwilioSipTrunk' and a 'Description' text area. The 'SIP Ports' section contains a table with columns: Action, Select, Address, Port, Transport Protocol, TLS Profile, Allow Anonymous, and Multi Home Addrs. One port is configured with Port 5061, Transport Protocol TLS, TLS Profile Twilio, and Allow Anonymous set to all.

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
⋮	<input type="checkbox"/>		5061	TLS	Twilio	all	

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

The screenshot shows the 'Modify SIP Interface' configuration page for GenesysCloud. The sidebar is the same as the previous screenshot. The main area is titled 'Modify SIP Interface'. It includes a 'State' section with a checked 'enable' checkbox. Below this is a 'Realm ID' dropdown menu set to 'GenesysCloud' and a 'Description' text area. The 'SIP Ports' section contains a table with columns: Action, Select, Address, Port, Transport Protocol, TLS Profile, Allow Anonymous, and Multi Home Addrs. Two ports are configured, both with Port 5060 and Allow Anonymous set to agents-only. The first port uses Transport Protocol UDP, and the second uses TCP.

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
⋮	<input type="checkbox"/>		5060	UDP		agents-only	
⋮	<input type="checkbox"/>		5060	TCP		agents-only	

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

6.11. Configure session-agent

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

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

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

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

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

[Click here for more information on Twilio Elastic SIP Trunking IP Address](#)

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

The screenshot shows the 'Modify Session Agent' configuration interface. On the left, a sidebar lists various configuration categories, with 'session-agent' currently selected. The main panel contains several input fields and dropdown menus for configuring a session agent. The fields include: Hostname (set to 'OracleSBCPureCloudTesting.byoc.usw'), IP Address (empty), Port (set to '5060' with a range note '(Range: 0,1025..65535)'), State (checked 'enable'), App Protocol (set to 'SIP'), App Type (empty), Transport Method (set to 'UDP'), Realm ID (set to 'GenesysCloud'), Egress Realm ID (empty), and a Description text area. At the bottom, there is a 'Match Identifier' field and 'OK' and 'Back' buttons.

6.12. Configure local-policy

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

To route the calls from Cloud Cx to Twilio Sip Trunk, Use the below local –policy

ConfigurationView ConfigurationQ

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

DiscardVerify

Modify Local Policy

From Address

* X

To Address

* X

Source Realm

GenesysCloud X

Description

State

☒ enable

Policy Priority

none

Policy Attributes

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

OKBack

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

ConfigurationView ConfigurationQ

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

DiscardVerify

Modify Local Policy

From Address

* X

To Address

* X

Source Realm

TwilioSipTrunk X

Description

State

☒ enable

Policy Priority

none

Policy Attributes

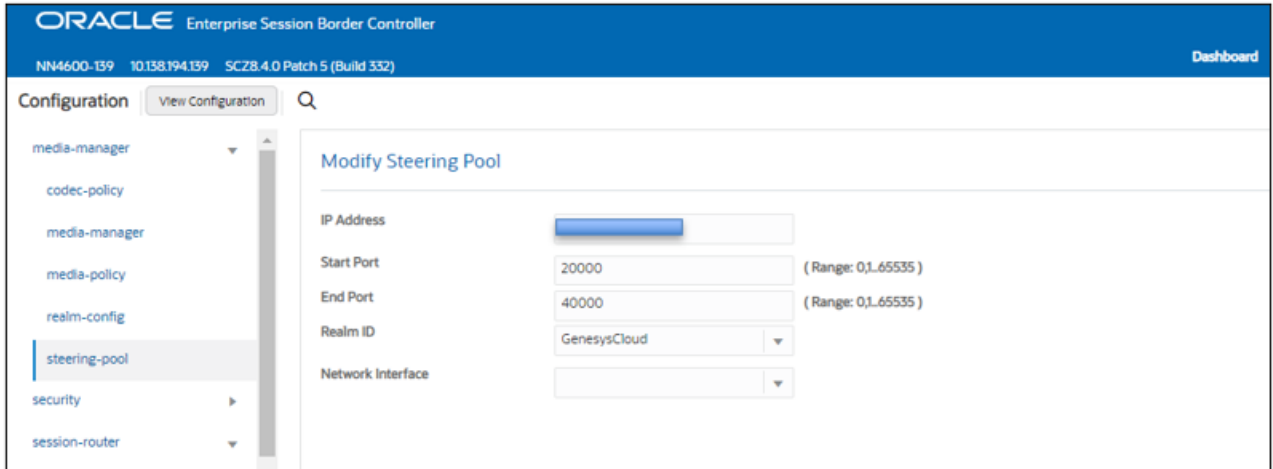
Action	Select	Next Hop	Realm	Action	Terminate Recursi...	Cost	State	App Protocol	Lookup	Next Key
:	<input type="checkbox"/>	OracleSBCPureClo...	GenesysCloud	none	disabled	0	enabled		single	

OKBack

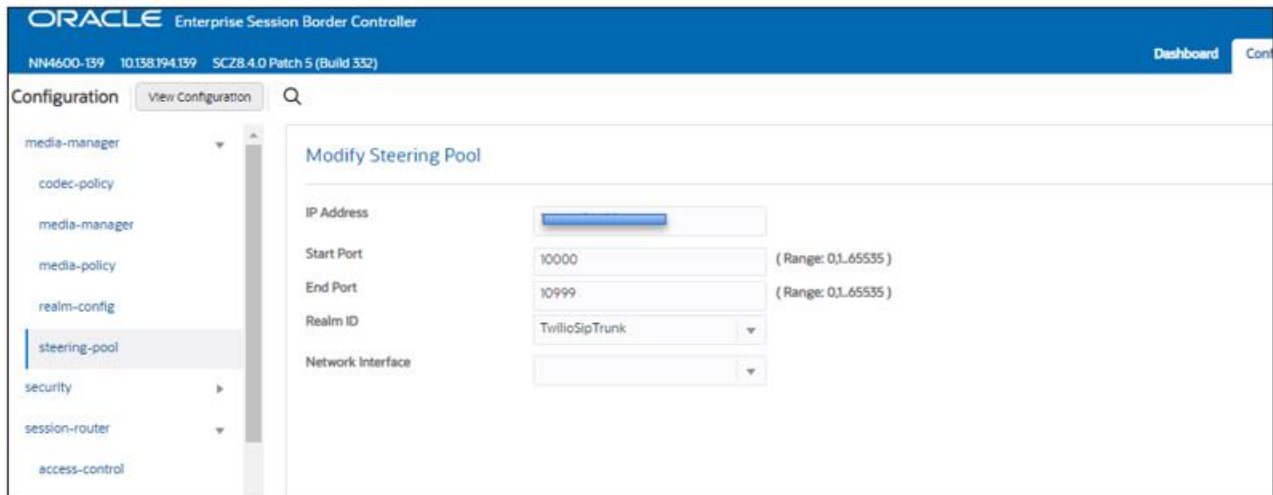
6.13. Configure steering-pool

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

Cloud Cx Steering pool.



Twilio steering pool.



6.14. Enable OPTIONS Ping response.

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

The parameter name is **Ping response**.

Ping Response:

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

ORACLE

Enterprise Session Border Controller

Dashboard

Configuration

Monitor and Trace

Widgets

Wizards

Commands

Save

Verify

Discard

session-agent

session-group

session-recording-group

session-recording-server

session-translation

sip-config

Show All

Modify Session Agent

Show Configuration

Hostname

oracle.pstn.twilio.com

IP Address

Port

5061

(Range: 0,1025..65535)

State

☒ enable

App Protocol

SIP

App Type

Transport Method

StaticTLS

Realm ID

TwilioRealm

Foreign Realm ID

OK

Back

ORACLE

Enterprise Session Border Controller

Dashboard

Configuration

Monitor and Trace

Widgets

System

Wizards

Commands

Save

Verify

Discard

Session

session-agent

session-group

session-recording-group

session-recording-server

session-translation

sip-config

sip-feature

sip-interface

Show All

Modify Session Agent

Show Configuration

Out Translationid

Trust Me

☐ enable

Local Response Map

Ping Response

☒ enable

In Manipulationid

Out Manipulationid

Manipulation String

Manipulation Pattern

Trunk Group

Max Register Sustain Rate

0

(Range: 0.999999999)

OK

Back

6.15. Configure sdes profile

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'media-security' expanded and 'sdes-profile' selected. The main panel is titled 'Add Sdes Profile'. It contains the following fields and options:

- 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 navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar also has 'Wizards' and 'Commands' tabs, and a 'Show All' toggle at the bottom.

6.16. Configure Media Security Profile

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

Assign this media policy to Twilio Realm as it use TLS/SRTP.

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

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

At the bottom of the form are 'OK' and 'Back' buttons. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar also has 'Wizards' and 'Commands' tabs, and a 'Show All' toggle at the bottom.

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

The screenshot shows the 'Modify Media Sec Policy' configuration page. The left sidebar contains a list of configuration items, with 'media-sec-policy' selected. The main panel displays the following configuration details:

- 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 main panel are 'OK' and 'Back' buttons.

6.17 Access Control

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

GUI Path: session-router/access-control

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

The Cloud Cx DNS Name - OracleSBCCloud CxTesting.byoc.usw2.pure.cloud resolves to the below IPs.

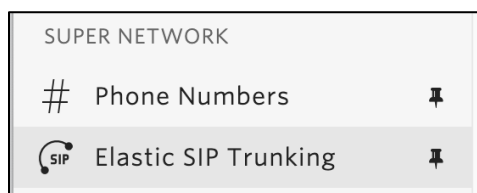
34.211.206.63
54.244.22.120
52.33.193.56
52.32.193.99

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

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

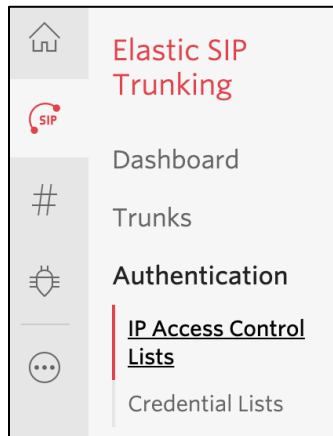
7. Twilio Elastic SIP Trunking Configuration

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



7.1. Create an IP-ACL rule

Click on [Authentication](#) in the left navigation, and then click on [IP Access Control Lists](#).



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

Oracle

Properties

FRIENDLY NAME

IP-ACL SID

AI

...

ASSOCIATED SIP TRUNKS

0

ASSOCIATED SIP DOMAINS

—

IP Address Ranges

+

IP Address Control Lists may have up to 100 IP addresses.

IP ADDRESS RANGE	FRIENDLY NAME
<div>155.212.214.102 / 32</div> <div>155.212.214.102 - 155.212.214.102</div>	<div>155.212.214.102</div> <div>×</div>

7.2. Create a new Trunk

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

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

Create A New SIP Trunk

×

Name your new SIP Trunk, then configure it in the following steps.

FRIENDLY NAME

Cancel

Create

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

Features

To learn more about SIP Trunking features, please [see our user documentation](#). [↗](#)

Call Recording ⓘ

Enabled

Calls will be recorded.

Call Recording

Record from ringing

Recording Trim

Disabled

Silence will not be trimmed from recording

Secure Trunking ⓘ

Enabled

TLS must be used to encrypt SIP messages on port 5061, and SRTP must be used to encrypt the media packets. Any non-encrypted calls will be rejected

Call Transfer (SIP REFER) ⓘ

Enabled

Twilio will consume an incoming SIP REFER from your communications infrastructure and create an INVITE message to the address in the Refer-To header

☐ **Enable PSTN Transfer** ⓘ

Allow Call Transfers to the PSTN via your Trunk.

Symmetric RTP ⓘ

Enabled

Twilio will detect where the remote RTP stream is coming from and start sending RTP to that destination instead of the one negotiated in the SDP

▶ **Additional Features**

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

Termination URI

Configure a SIP Domain Name to uniquely identify your Termination SIP URI for this Trunk. This URI will be used by your communications infrastructure to direct SIP traffic towards Twilio. Be sure to select a localized SIP URI to ensure your traffic takes the lowest latency path. If a localized version isn't selected, then your traffic will be sent to US1. [Learn more about Termination Settings](#)

TERMINATION SIP URI

oracle

.pstn.twilio.com

[Show Localized URIs](#)

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

NORTH AMERICA VIRGINIA	oracle.pstn.ashburn.twilio.com
NORTH AMERICA OREGON	oracle.pstn.umatilla.twilio.com
EUROPE DUBLIN	oracle.pstn.dublin.twilio.com
EUROPE FRANKFURT	oracle.pstn.frankfurt.twilio.com
SOUTH AMERICA SAO PAULO	oracle.pstn.sao-paulo.twilio.com
ASIA PACIFIC SINGAPORE	oracle.pstn.singapore.twilio.com
ASIA PACIFIC TOKYO	oracle.pstn.tokyo.twilio.com
ASIA PACIFIC SYDNEY	oracle.pstn.sydney.twilio.com

Or

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

Authentication [View all Authentication lists](#)

The following IP ACLs and Credential Lists will be used to authenticate the INVITE for termination calls inbound to Twilio.

IP ACCESS CONTROL LISTS

Oracle



CREDENTIAL LISTS

Click to select a Credential List



In the **Origination** section, we will need to add Origination URI's to route traffic towards your Oracle SBC. The recommended practice is to configure a redundant mesh per geographic region (in this context a region is one of North America, Europe, etc.). In this case, we configure two Origination URIs, each egressing from a different Twilio Edge.

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

Add Origination URL

ORIGINATION SIP URI

sip:155.212.215.102;edge=ashburn

PRIORITY

10

Priority ranks the importance of the URI. Values range from 0 to 65535, where the lowest number represents the highest importance.

WEIGHT

10

Weight is used to determine the share of load when more than one URI has the same priority. Its values range from 1 to 65535. The higher the value, the more load a URI is given.

ENABLED

ON

Cancel

Add

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

Origination URIs					
Configure the IP address (or FQDN) of the network element entry point into your communications infrastructure (e.g. IP-PBX, SBC).					
Show more about provisioning for high service availability					
+	ORIGINATION URI	PRIORITY	WEIGHT	ENABLED	
	sip:155.212.214.102;edge=ashburn	10	10	✓	×
	sip:155.212.214.103;edge=umatilla	20	10	✓	×

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

7.3. Associate Phone Numbers on your Trunk

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

Numbers

View my Addresses

Emergency Calling Update: Each number must be associated with an emergency address with matching ISO Country. Please select numbers to enable from one country at a time.

+

Number

Filter

Choose Action

NUMBER	FRIENDLY NAME	COUNTRY	EMERGENCY CALLING STATUS	EMERGENCY ADDRESS	
+18007904044	(850) 790-4044	US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	<input type="checkbox"/>
+16092203033	(609) 220-3033	US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	<input type="checkbox"/>
+1707100000	(707) 210-0000	US	Disabled		<input type="checkbox"/>

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 and Twilio Elastic SIP Trunk.

The pre-requisites are given below.

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

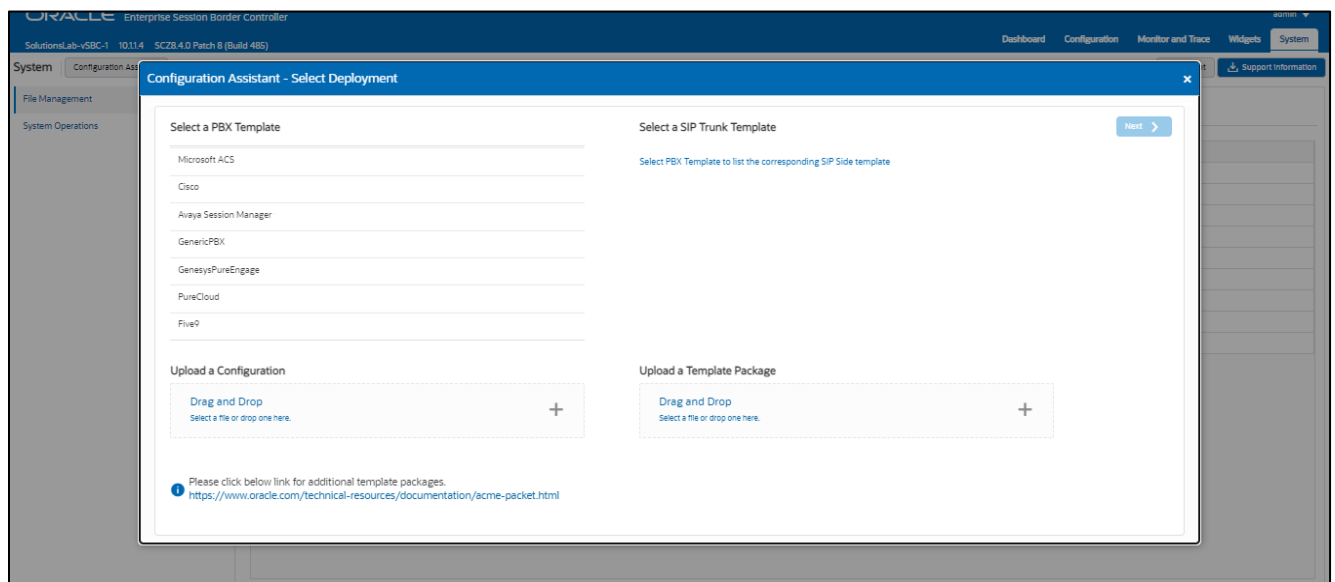
The Oracle SBC WebGui can be accessed by entering the following in your web browser.
`http(s)://<SBC Management IP>`.

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

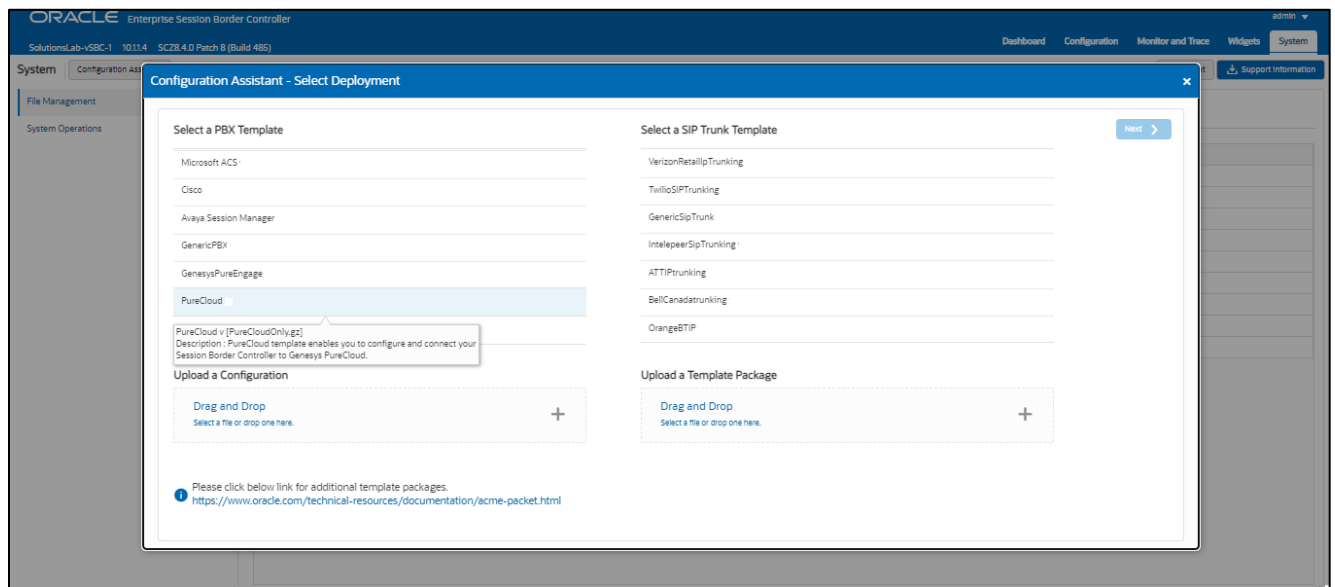
If there is no configuration on the SBC, the configuration assistant will show immediately upon login to the SBC GUI as shown below

Cloud Cx Configuration Assistant

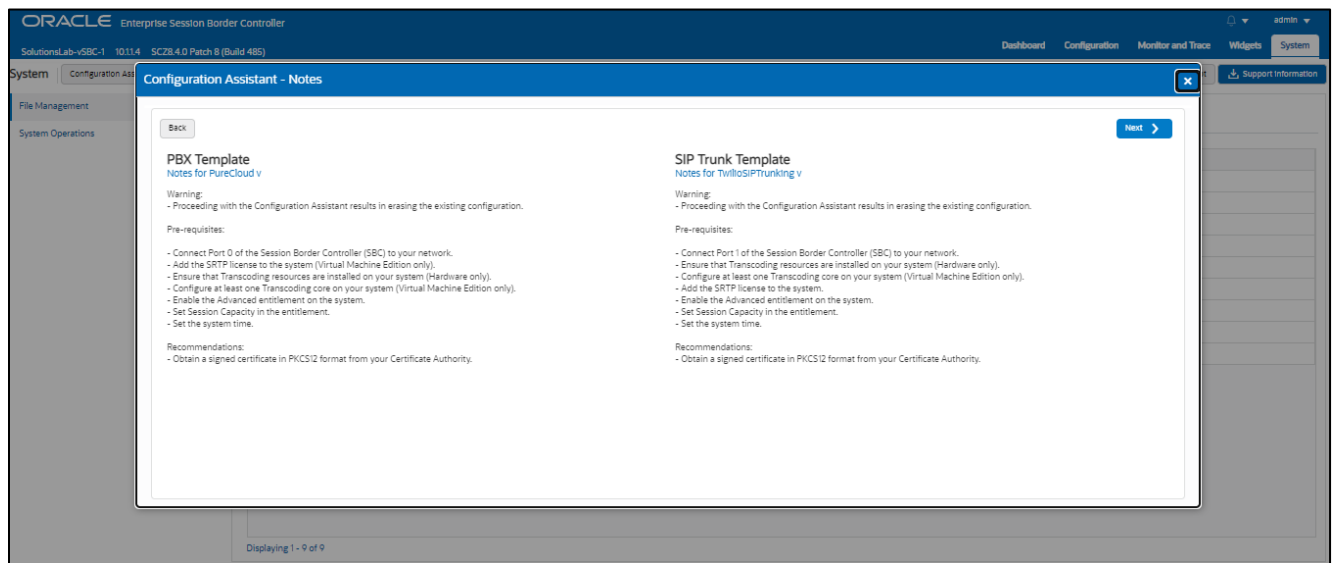
For a new SBC deployment, once access to the GUI is configured, you will see the following when logging in for the first time:



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



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



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

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

Page 1- 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”.

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-1 10.11.4 SC28.4.0 Patch 8 (Build 485)

Dashboard Configuration Monitor and Trace Widgets System

System Configuration Assistant

File Management System Operations

Configuration Assistant - PureCloud Network

1 2 3 4 5 6 7 8 9

Back Next

PureCloud Network Root Trusted Certificate SBC Certificate Genesys Purecloud Transcoding Twilio Elastic SIP Trunk Network Twilio Session Agent Root Trusted Certificate SBC Certificate for Twilio

Let's configure the interface that communicates with PureCloud

Realm Name Required

Enter PureCloud Session Agent hostname here Required

Enter the PureCloud IP here Required

Port Number Required

Slot Number Required

Network IP Address

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.

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-1 10.11.4 SC28.4.0 Patch 8 (Build 485)

Dashboard Configuration Monitor and Trace Widgets System

System Configuration Assistant

File Management System Operations

Configuration Assistant - Root Trusted Certificate

1 2 3 4 5 6 7 8 9

Back Next

PureCloud Network Root Trusted Certificate SBC Certificate Genesys Purecloud Transcoding Twilio Elastic SIP Trunk Network Twilio Session Agent Root Trusted Certificate SBC Certificate for Twilio

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

Do you consent to installing the DigiCert High Assurance EV Root Cert ☒ No ☒ Yes

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 02ac5c205a0b407b8f0b79f2ae4e2577

Signature Algorithm: sha1WithRSAEncryption

Issuer:

C=US

O=DigiCert Inc

OU=www.digicert.com

CN=DigiCert High Assurance EV Root CA

Validity:

Not Before: Nov 10 00:00:00 2006 GMT

Not After: Nov 10 00:00:00 2031 GMT

Subject:

C=US

O=DigiCert Inc

OU=www.digicert.com

CN=DigiCert High Assurance EV Root CA

X.509 extensions:

X.509v3 Key Usage: critical

Digital Signature, Certificate Sign, CRL Sign

X.509v3 Basic Constraints: critical

Displaying 1 - 9 of 9

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.

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-1 10.11.4 SC28.4.0 Patch 8 (Build 485)

Dashboard Configuration Monitor and Trace Widgets System

System Configuration Assistant

File Management System Operations

Configuration Assistant - SBC Certificate

Let's start provisioning certificates for the SBC

Certificate provisioning type

Fully Qualified Domain Name or Common Name

PKCS12 certificate (.p12 or .pfx)

PKCS12 certificate password

Displaying 1 - 9 of 9

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).

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-1 10.11.4 SC28.4.0 Patch 8 (Build 485)

Dashboard Configuration Monitor and Trace Widgets System

System Configuration Assistant

File Management System Operations

Configuration Assistant - SBC Certificate

Let's start provisioning certificates for the SBC

Certificate provisioning type

Fully Qualified Domain Name or Common Name

Country

State

Locality

Organization

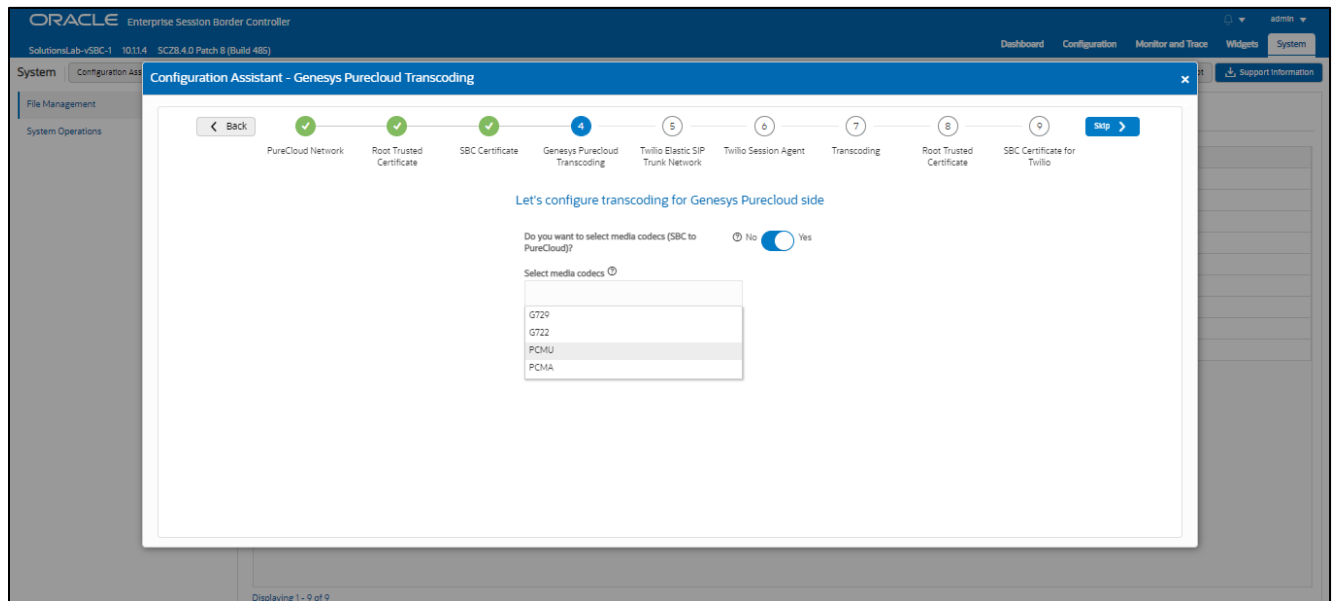
Displaying 1 - 9 of 9

Page 4 – Cloud Cx side Transcoding

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

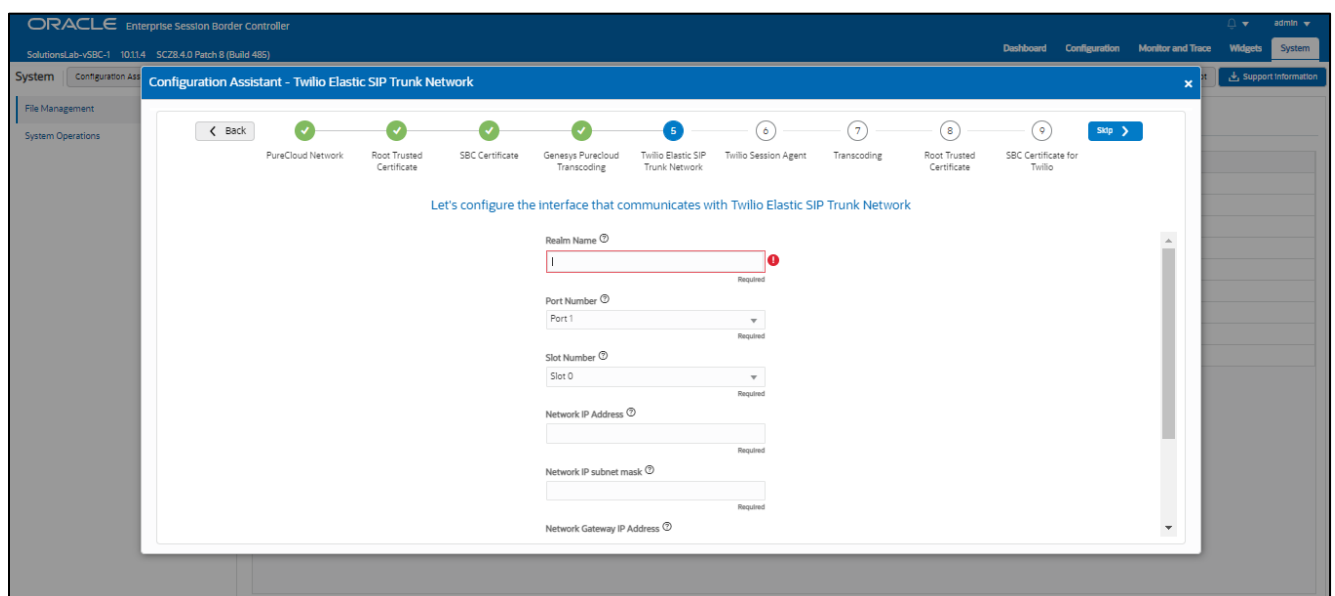
Once transcoding features is set to “yes”, you will then have an option to select additional media codecs you want included in offers/answers toward Cloud Cx. If you select yes to either question regarding media codecs, you will be presented with a required drop down.

You can select as many codecs from the list presented.



Page 5 – Twilio Elastic Sip Trunk Network

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



Page 6 – Twilio Session Agent

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

The screenshot shows the Oracle Enterprise Session Border Controller Configuration Assistant interface. The main window is titled "Configuration Assistant - Twilio Session Agent". At the top, there is a progress bar with steps: PureCloud Network, Root Trusted Certificate, SBC Certificate, Genesys Purecloud Transcoding, Twilio Elastic SIP Trunk Network, Twilio Session Agent (current step), Transcoding, Root Trusted Certificate, and SBC Certificate for Twilio. The "Twilio Session Agent" step is highlighted with a blue circle and a red exclamation mark, indicating it is the current step and has a required field. Below the progress bar, the text "Let's configure session agent for Twilio" is displayed. The form contains the following fields and options:

- Twilio Session Agent hostname (Required field, marked with a red exclamation mark)
- Twilio Session Agent IP Address
- Twilio Session Agent Port (Required field, marked with a red exclamation mark)
- Do you have a second Hostname/IP address for Twilio Sip Signaling? (Radio buttons: No, Yes)
- Do you want to enable OPTIONS ping towards Twilio Elastic SIP trunk? (Radio buttons: No, Yes)
- Do you want SBC to handle call transfer from your Twilio Elastic SIP trunk? (Radio buttons: No, Yes)
- Do you want to enable session translation towards Twilio Elastic SIP trunk? (Radio buttons: No, Yes)

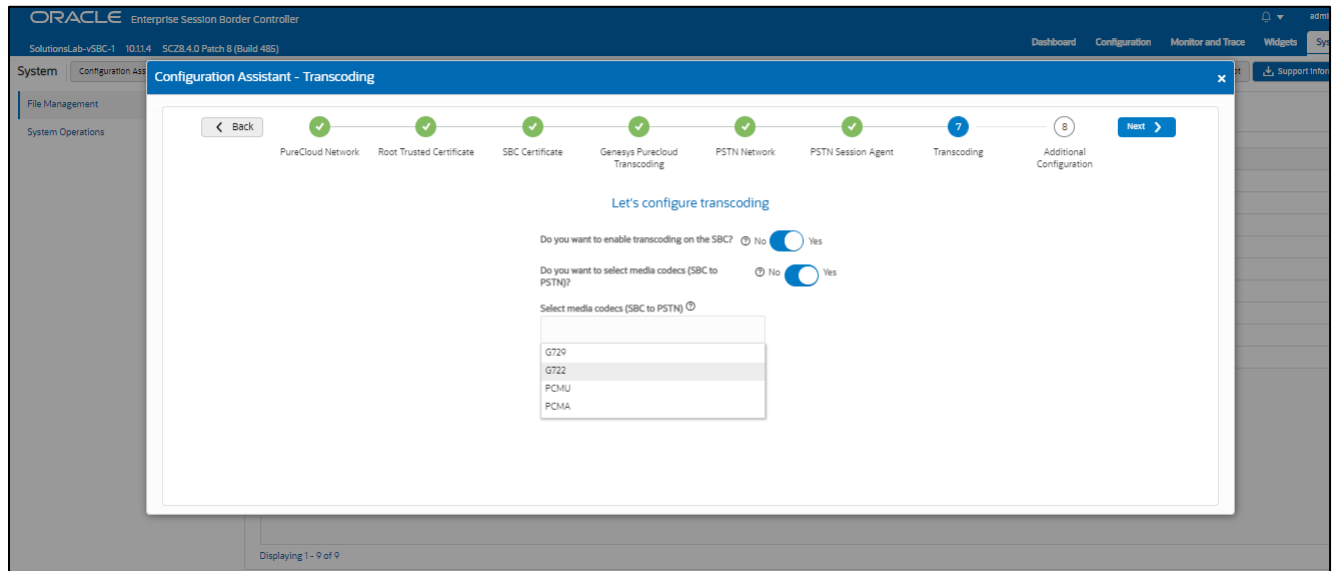
The bottom of the window shows "Displaying 1 - 2 of 2".

Please fill the required fields and click Next.

Page 7 - Twilio side Transcoding

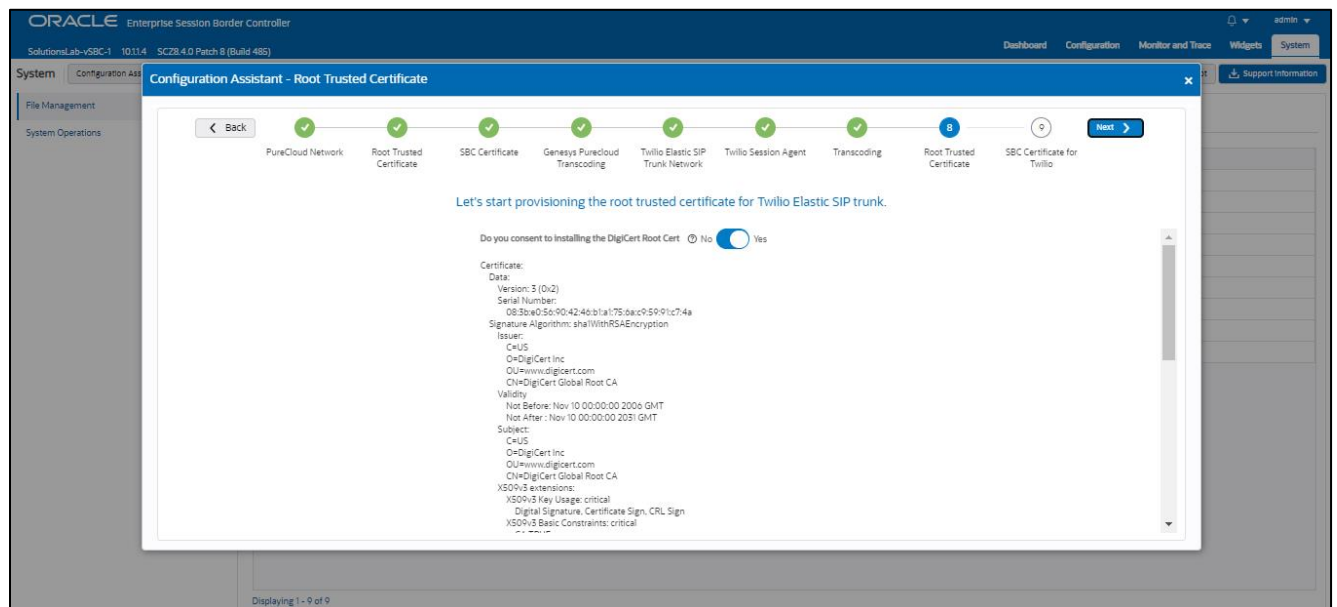
Page 7 is where you will be able to configure transcoding between the SBC and Twilio Trunk.

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



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

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



Page 9 – SBC Certificate for Twilio

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

ORACLE Enterprise Session Border Controller

SolutionsLab-VSBC-1 10.11.4 SC28.4.0 Patch 8 (Build 485)

Dashboard Configuration Monitor and Trace Widgets System

System Configuration Assistant

File Management System Operations

Configuration Assistant - SBC Certificate for Twilio

Back

PureCloud Network Root Trusted Certificate SBC Certificate Genesys Purecloud Transcoding Twilio Elastic SIP Trunk Network Twilio Session Agent Transcoding Root Trusted Certificate SBC Certificate for Twilio Review

Let's start provisioning SBC certificates for Twilio Side

Certificate provisioning type [?]

PKCS12

Required

Fully Qualified Domain Name or Common Name [?]

Required

PKCS12 certificate (.p12 or .pfx) [?]

upload

Required

PKCS12 certificate password [?]

Required

Displaying 1 - 9 of 9

Review

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

ORACLE Enterprise Session Border Controller

SolutionsLab-VSBC-1 10.11.4 SC28.4.0 Patch 8 (Build 485)

Dashboard Configuration Monitor and Trace Widgets System

System Configuration Assistant

File Management System Operations

Configuration Assistant - SBC Certificate for Twilio

Back

PureCloud Network Root Trusted Certificate SBC Certificate Genesys Purecloud Transcoding Twilio Elastic SIP Trunk Network Twilio Session Agent Transcoding Root Trusted Certificate SBC Certificate for Twilio Review

Let's start provisioning SBC certificates for Twilio Side

Certificate provisioning type [?]

PKCS12

Required

Fully Qualified Domain Name or Common Name [?]

Required

PKCS12 certificate (.p12 or .pfx) [?]

upload

Required

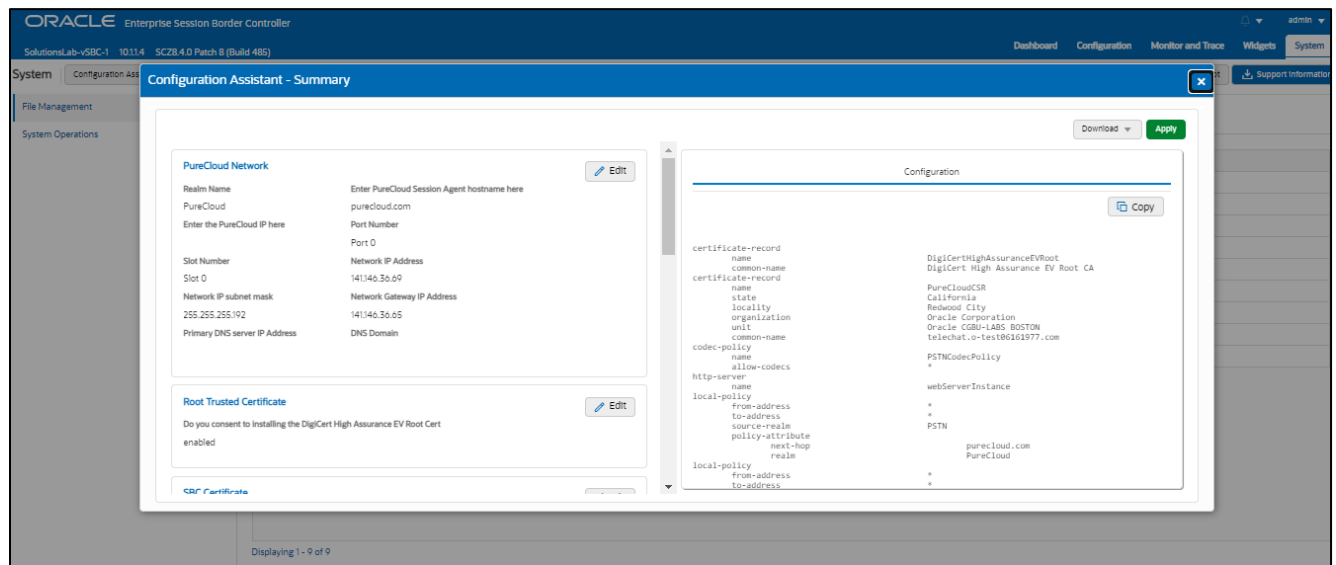
PKCS12 certificate password [?]

Required

Displaying 1 - 9 of 9

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

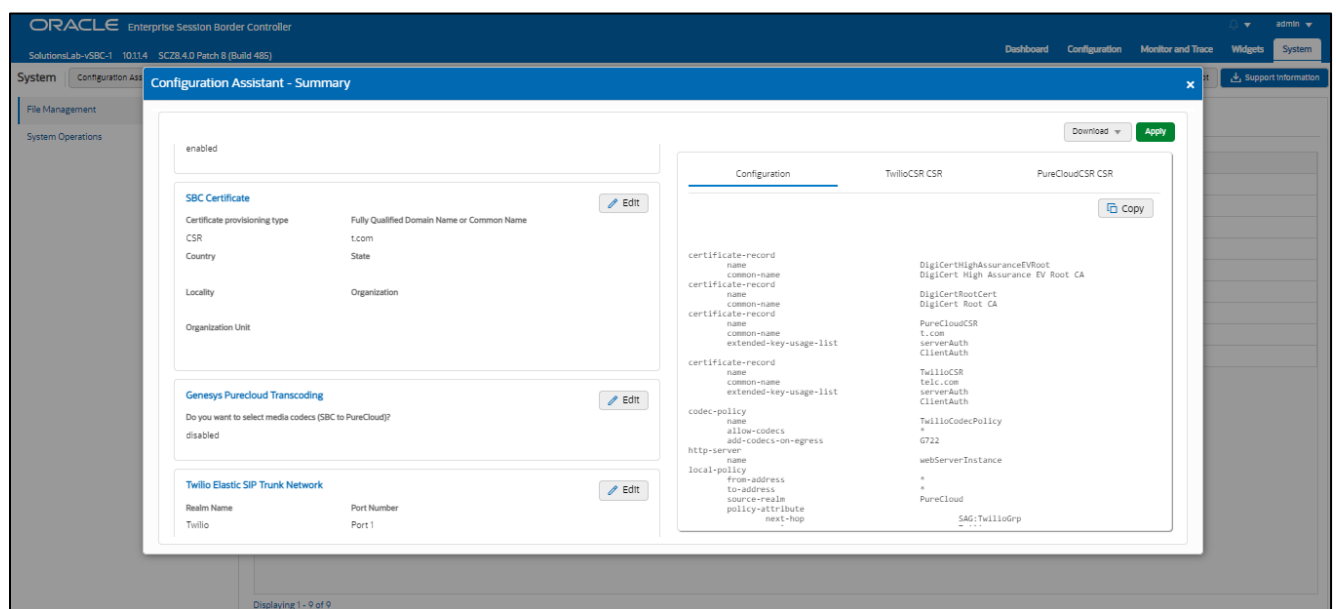
The right side displays the entire configuration created and when applicable, will also have a CSR tab that contains a certificate that can be signed by a CA authority.



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

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

On Page 3 and Page 9 of the template, if you chose CSR from the drop-down menu instead of PKCS, the SBC configures a certificate record and generates a certificate signing request for you.



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

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

Download and/or Apply

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

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

Configuration Assistant Access

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

9. Test Plan Executed

We have executed the following test plan to validate the interworking between Genesys 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

 facebook.com/Oracle/

 twitter.com/Oracle

 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