

ORACLE

Oracle SBC integration with Genesys Pure Engage 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

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with Genesys Pure Engage and Twilio Elastic Sip Trunking	04 th June 2021
1.1	Added new section for SBC config/Deployment Using Configuration Assistant	07 th January 2022

Table of Contents

1. INTENDED AUDIENCE	5
2. DOCUMENT OVERVIEW	5
2.1. TWILIO ELASTIC SIP TRUNKING	5
2.2. GENESYS PURE ENGAGE	5
3. INTRODUCTION	6
3.1. AUDIENCE	6
3.2. REQUIREMENTS	6
3.3. ARCHITECTURE.....	7
4. CONFIGURING THE GENESYS PURE ENGAGE	8
4.1. CONFIGURING A NEW DN.....	8
4.2. CONFIGURE A NEW TRUNK FOR SBC.....	10
5. CONFIGURING THE SBC	12
5.1. VALIDATED ORACLE SBC VERSION	12
6. NEW SBC CONFIGURATION	12
6.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC	12
6.2. CONFIGURE SBC USING WEB GUI	16
6.3. CONFIGURE SYSTEM-CONFIG.....	18
6.4. CONFIGURE PHYSICAL INTERFACE VALUES	19
6.5. CONFIGURE NETWORK INTERFACE VALUES	20
6.6. ENABLE MEDIA MANAGER.....	22
6.7. ENABLE SIP-CONFIG	23
6.8. CONFIGURE REALMS.....	24
6.9. CONFIGURING A CERTIFICATE FOR SBC	26
6.10. TLS-PROFILE.....	28
6.11. CONFIGURE SIP INTERFACES	29
6.12. CONFIGURE SESSION-AGENT	30
6.13. CONFIGURE LOCAL-POLICY	31
6.14. CONFIGURE STEERING-POOL	33
6.15. CONFIGURE PING RESPONSE	34
6.16. CONFIGURE SDES PROFILE.....	36
6.17. CONFIGURE MEDIA SECURITY PROFILE.....	36
6.18. CONFIGURE TRANSLATION RULES	37
6.19. CONFIGURE SESSION TRANSLATION RULES.....	38
7. SBC CONFIGURATION FOR GENESYS REMOTE WORKER.....	40
7.1. CONFIGURE REALMS.....	41
7.2. ENABLE MEDIA MANAGER.....	42
7.3. CONFIGURE SIP INTERFACES	43
7.4. CONFIGURE STEERING-POOL	44
7.5. CONFIGURE LOCAL-POLICY (OPTIONAL)	45
8. NEW SBC CONFIG/DEPLOYMENT USING CONFIGURATION ASSISTANT	46
8.1. SECTION OVERVIEW AND REQUIREMENTS	46
8.2. INITIAL GUI ACCESS.....	46
8.3. CONFIGURATION ASSISTANT TEMPLATE NAVIGATION	49
8.3.1. PAGE 1-GENESYS PUREENGAGE NETWORK.....	49
8.3.2. PAGE 2-GENESYS SESSION AGENT.....	49

8.3.3. PAGE 3 -GENESYS SIDE TRANSCODING.....	50
8.3.4. PAGE 4 - TWILIO ELASTIC SIP TRUNK NETWORK.....	51
8.3.5. PAGE 5 - TWILIO SESSION AGENT.....	51
8.3.6. PAGE 6 - TWILIO SIDE TRANSCODING.....	52
8.3.7. PAGE 7 - IMPORT DIGI CERT ROOT CA CERTIFICATE FOR TWILIO SIDE	52
8.3.8. PAGE 8 - SBC CERTIFICATES FOR TWILIO SIDE.....	53
8.4. REVIEW	54
8.5. DOWNLOAD AND/OR APPLY.....	56
8.6. CONFIGURATION ASSISTANT ACCESS	57
9. EXISTING SBC CONFIGURATION	57
10. TWILIO ELASTIC SIP TRUNKING CONFIGURATION.....	58
10.1. CREATE AN IP-ACL RULE.....	58
10.2. CREATE A NEW TRUNK	59
10.3. ASSOCIATE PHONE NUMBERS ON YOUR TRUNK	63
11. VERIFICATION OF SAMPLE CALL FLOWS.....	64
APPENDIX A	68

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 Pure Engage.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Twilio Elastic Sip Trunk with on premises Genesys Pure Engage. The solution contained within this document has been tested using Oracle Communication SBC with **OS840p5**

Please find the related documentation links 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 Pure Engage

SIP Server is the Genesys software component that provides an interface between your telephony hardware and the rest of the Genesys software components in your enterprise. It translates and keeps track of events and requests that come from and are sent to the telephony device. SIP Server is a TCP/IP-based server that can also act as a messaging interface between SIP Server clients. It is the critical point in allowing your Genesys solution to facilitate and track the contacts that flow through your enterprise and this reduces the cost and complexity of extending an enterprise's telephony system outside its network borders.

Genesys Pure Engage solution consists of the following components and the user should perform the configuration of the below servers.

Testing is performed as per below product release version.

- Genesys SIP Server, Version 8.1.1
- Genesys Media Control Platform, Version 9.0.013.61
- Genesys SIP Proxy Server, Version 8.1.100.76
- Genesys SIP Feature Server, Version 8.1.202.1
- Genesys Configuration Manager 8.1.1

The configuration of Genesys SIP Server, including Media Server, SIP Proxy, Configuration Manager and SIP Feature Server are out of scope of this document. Please note that the 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. The customers can configure any publicly routable IPs for these sections as per their network architecture needs.

3. Introduction

3.1. Audience

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

3.2. Requirements

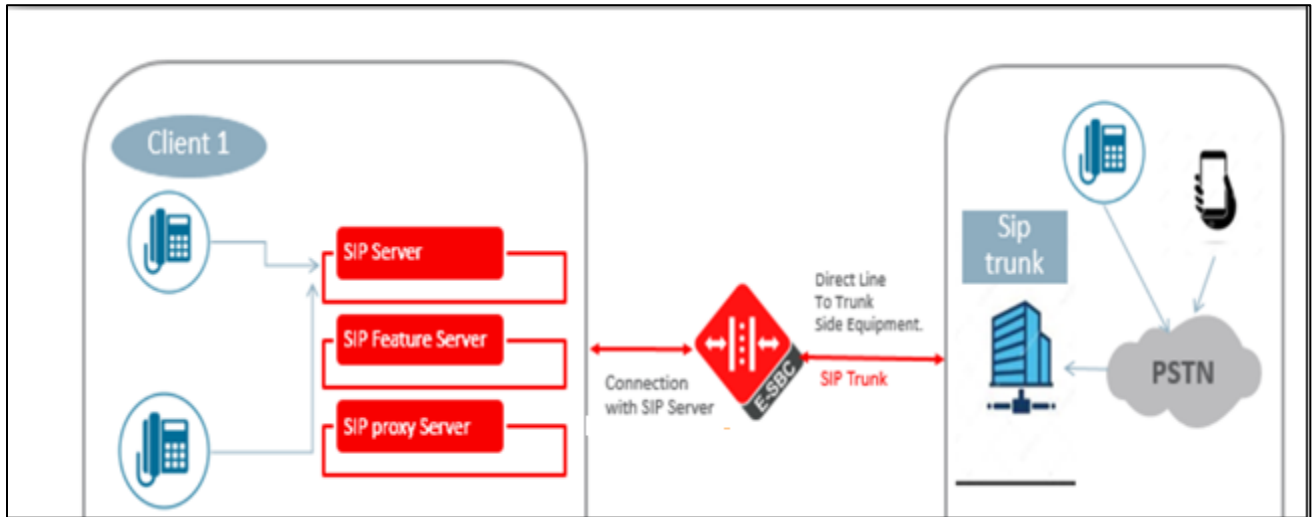
- Fully functioning Genesys SIP Server deployment, including Media Server, SIP Proxy and SIP Feature Server
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version

The below revision table explains the versions of the software used for each component:
This table is Revision 1 as of now:

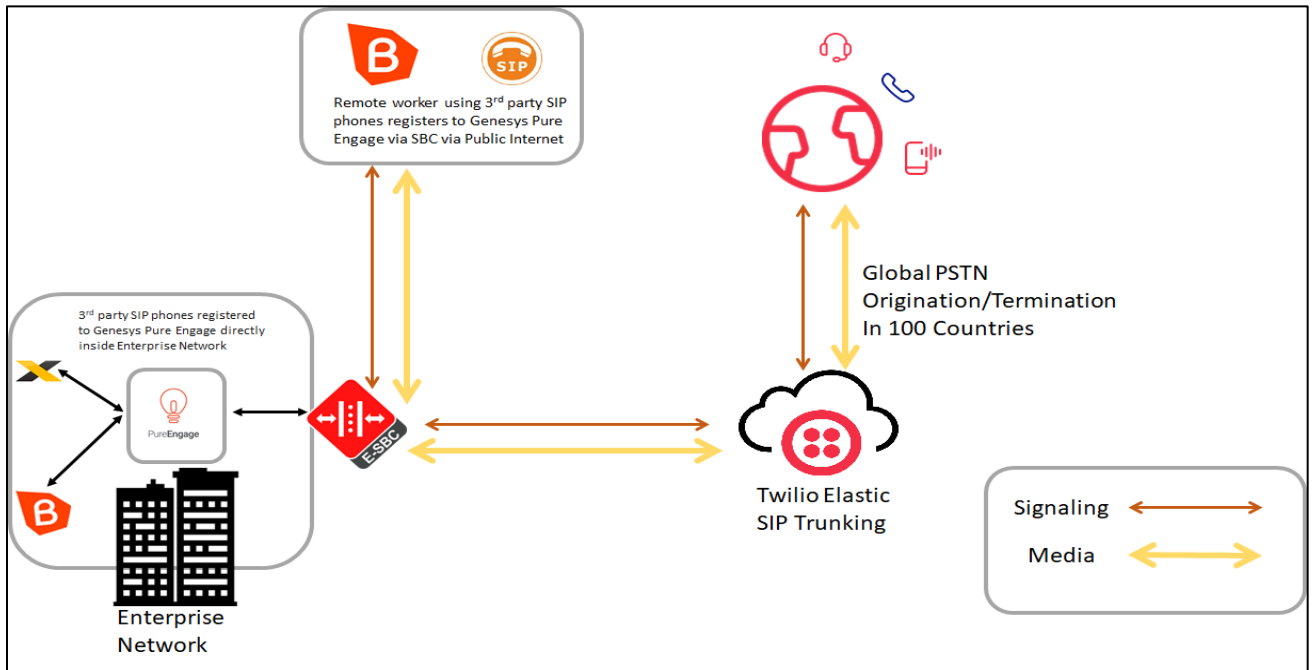
Software Used	SBC Version	Genesys Pure Engage
Revision 1	8.4.0	8.1.1

3.3. Architecture

The General architecture of Genesys Pure Engage with PSTN trunk is given below.



The lab setup used for the testing is given below specific to Genesys Pure Engage with Twilio SIP trunk.



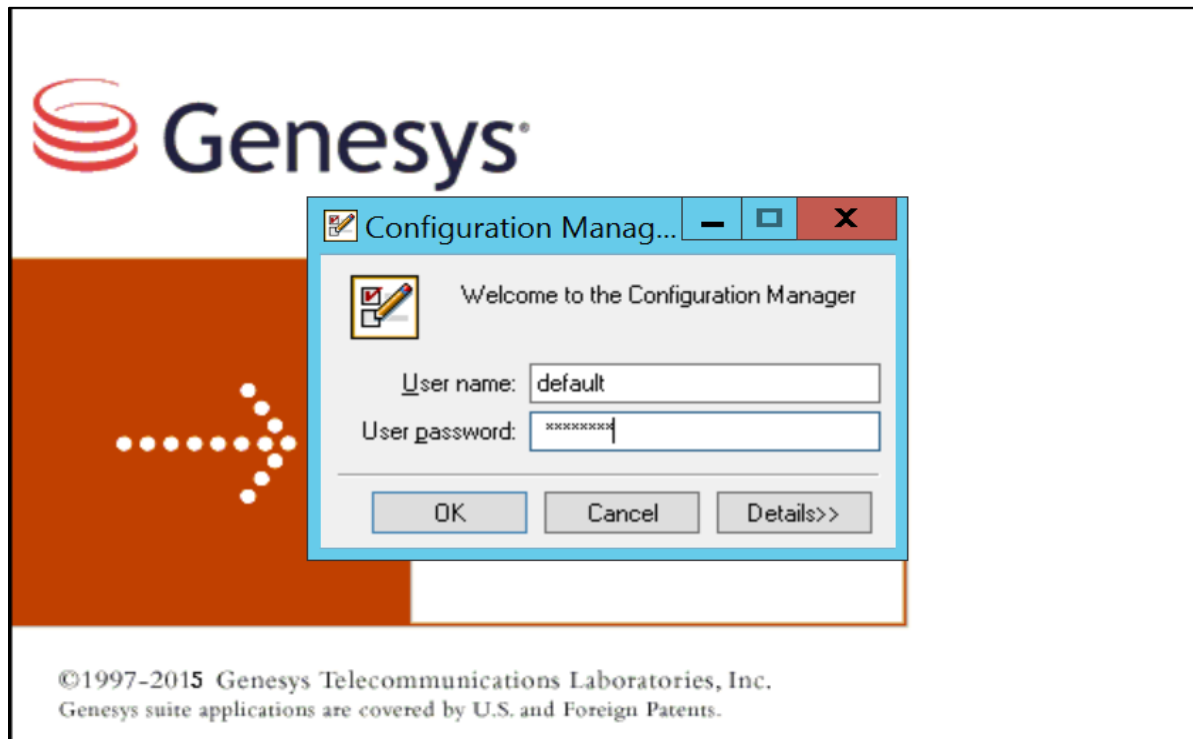
The configuration, validation and troubleshooting are the focuses of this document and will be described in three phases:

- Phase 1 – Configuring the Genesys Pure Engage for Oracle SBC.
- Phase 2 – Configuring the Oracle SBC.
- Phase 3 – Configuring the Twilio Elastic SIP Trunk

4. Configuring the Genesys Pure Engage

Please login to Genesys Configuration Manager GUI with proper login credentials (Username and password) as given below. After that, perform the steps below in the given order.

Note: The pre-requisite here is that user has done the basic config of Genesys Configuration Manager and knows the provisioning steps that's are given below.



4.1. Configuring a new DN

- 01) Go to Environment ----- Switches ----- Switch (SIP Switch) ----- DNs – Local DNs ----- Add New
- 02) Select Number as the DN or DID that needs to be assigned.
- 03) Select Type as “Extension” from the drop-down menu.
- 04) Leave other fields to Default values.
- 05) Click Apply and OK to save the DN.

You can follow the same procedure to add more DNs to the Genesys Configuration Manager.

Contents of /Configuration/Environments/Switches/Switch/DNs/Local DN

Number	Type	Switch	Alias
Enter text here	Enter text here	Enter te...	Enter te...
+17813131033	Extension	Switch	
+17813131034	Routing Point	Switch	
+17814437266	Extension	Switch	
+17814437285	Extension	Switch	
+17814437293	Extension	Switch	
100001	Extension	Switch	
100011	Extension	Switch	
100021	Extension	Switch	
100031	Extension	Switch	
100041	Extension	Switch	
1234567890	Extension	Switch	
16892203033	Extension	Switch	
17692105055	Extension	Switch	
17813131034	Routing Point	Switch	
17814437285	Routing Point	Switch	
17814437293	Extension	Switch	
18507904044	Extension	Switch	
9000	Routing Point	Switch	
9001	Routing Point	Switch	
9002	Routing Point	Switch	
911	Extension	Switch	
DMSML	Voice over IP Service	Switch	
DN	Trunk	Switch	
DN1	Trunk	Switch	

Context menu options: New, DN, Range of DNs, Folder, Filter..., View, Refresh, Cut, Copy, Paste, Properties.

Activate Windows
Go to System in Control Panel to activate Windows.

Contents of /Configuration/Environments/Switches/Switch/DNs/Local DN

Number	Type	Switch	Alias
Enter text here	Enter text here	Enter te...	Enter te...
+17813131033	Extension	Switch	
+17813131034	Routing P	Switch	
+17814437266	Extension	Switch	
+17814437285	Extension	Switch	
+17814437293	Extension	Switch	
100001	Extension	Switch	
100011	Extension	Switch	
100021	Extension	Switch	
100031	Extension	Switch	
100041	Extension	Switch	
1234567890	Extension	Switch	
16892203033	Extension	Switch	
17692105055	Extension	Switch	
17813131034	Routing P	Switch	
17814437285	Routing P	Switch	
17814437293	Extension	Switch	
18507904044	Extension	Switch	
9000	Routing P	Switch	
9001	Routing P	Switch	
9002	Routing P	Switch	
911	Extension	Switch	
DMSML	Voice over IP Service	Switch	
DN	Trunk	Switch	
DN1	Trunk	Switch	

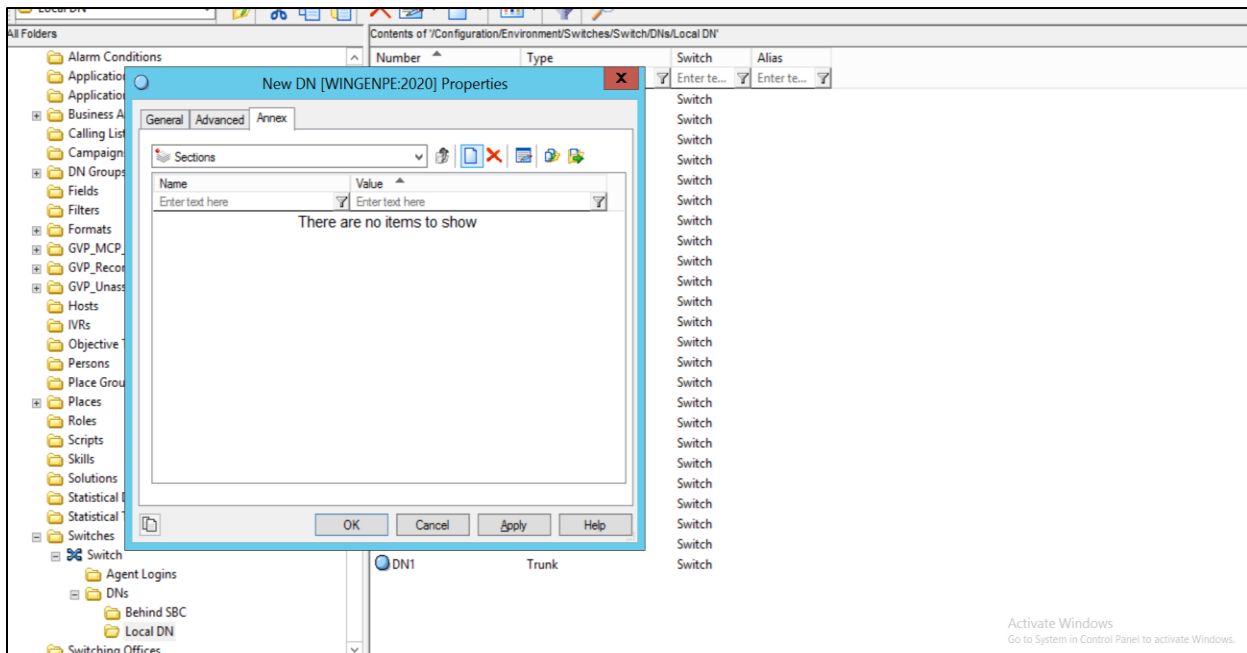
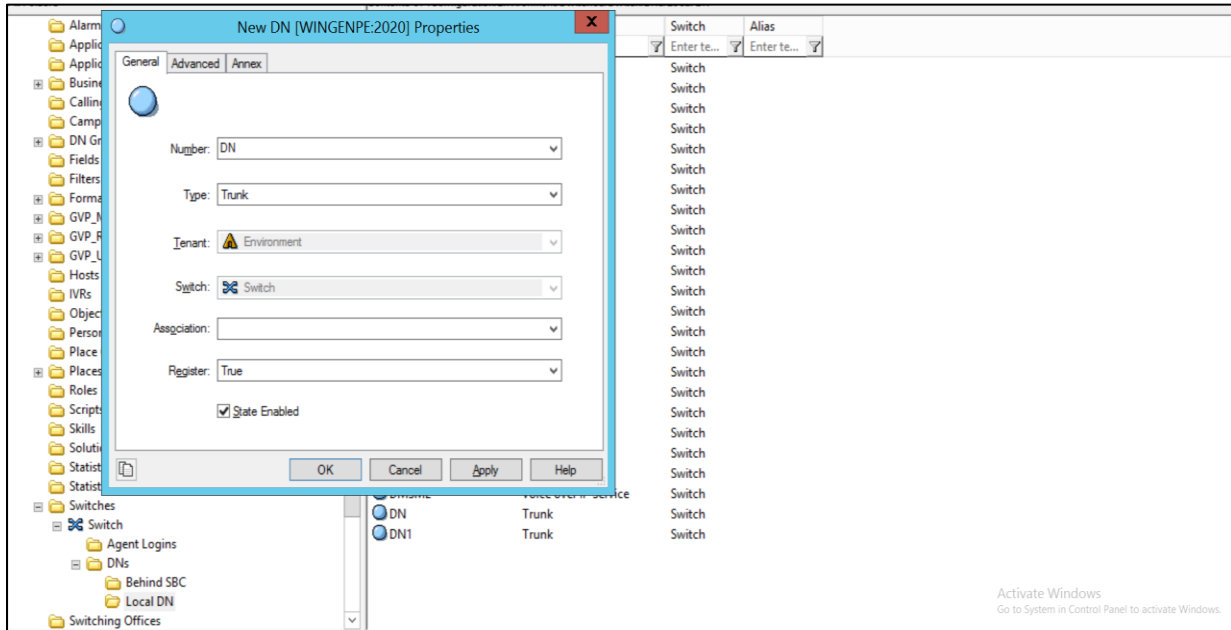
New DN [WINGENPE:2020] Properties dialog box:

- Number: 18507904044
- Type: Extension
- Tenant: Environment
- Switch: Switch
- Association: (empty)
- Register: True
- State Enabled

Activate Windows
Go to System in Control Panel to activate Windows.

4.2. Configure a new Trunk for SBC.

- 01) Go to Environment ----- Switches ----- Switch (SIP Switch) ---- DNs – Local DNs ---- Add New
- 02) Select Number as the DN (Default value)
- 03) Select Type as “Trunk” from the drop-down menu.
- 04) Click on Annex Tab and select Create New section/ option and give an appropriate name and click OK.
- 05) After Trunk name is created, select Create New section/ option again.
- 06) Add the following parameters given below and Click Apply and OK to save the Trunk configuration.
The important parameter is “Contact” where we give SBC inside SIP interface (Core side)



5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Genesys Pure Engage and Twilio Elastic SIP Trunking. **In this SBC config, Twilio Elastic SIP trunk side is secure (TLS/SRTP) and Genesys Pure Engage Side is unsecure (UDP or TCP/RTP).** If the Oracle SBC being deployed is new, with no existing configuration, the simplest way to configure it to interface with Genesys PureEngage is by utilizing the [Configuration Assistant](#) feature.

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.

Please note that the setup of VM and Cloud is different from hardware SBC and the steps below is to be used with hardware based SBC.

6.1. Establishing a serial connection to the SBC

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 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. Go to Configure terminal->bootparam.

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

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

Boot File           : /boot/nnSCZ840p5.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: 6)

NN4600-139(configure)#
NN4600-139(configure)#
```

Note: There is no management IP configured by default.

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

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

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

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

Last Modified 2020-04-30 22:38:15
-----

 1 : Product           : Enterprise Session Border Controller

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

Save the changes and reboot the SBC.

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

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

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

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

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

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

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

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

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

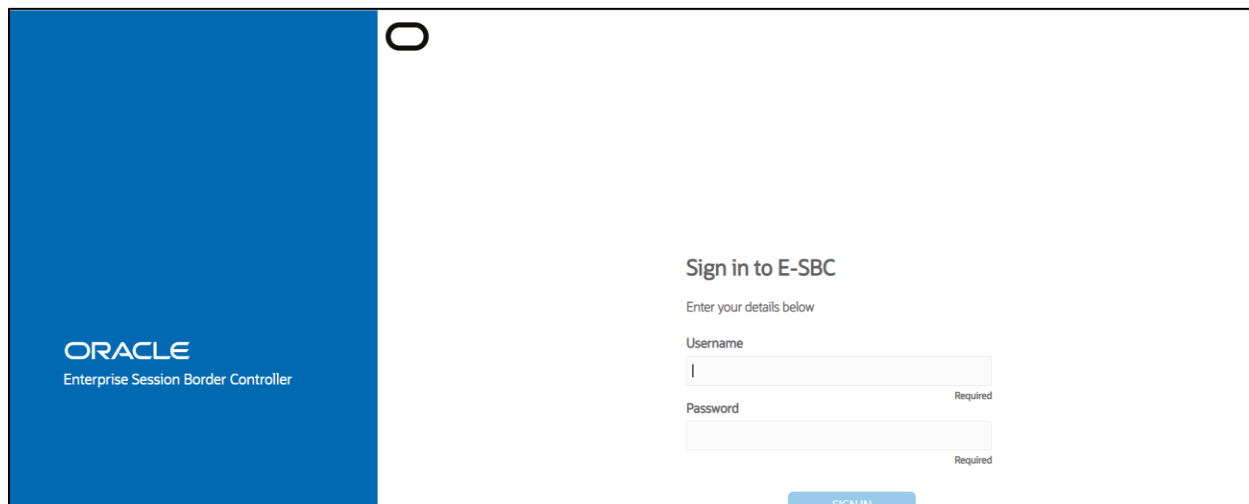
Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

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

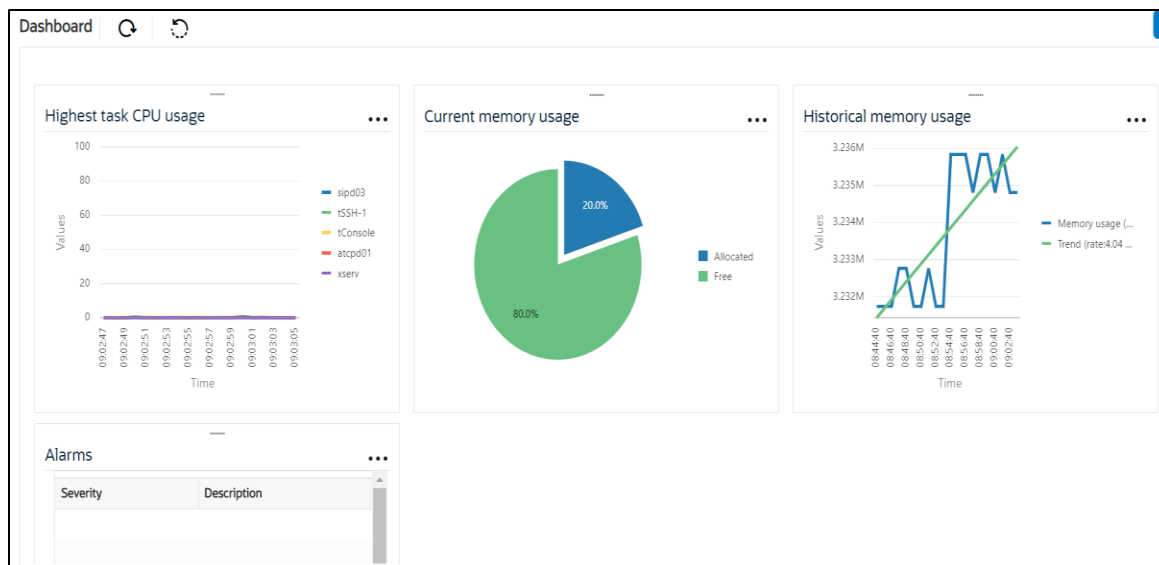
6.2. Configure SBC using Web GUI

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

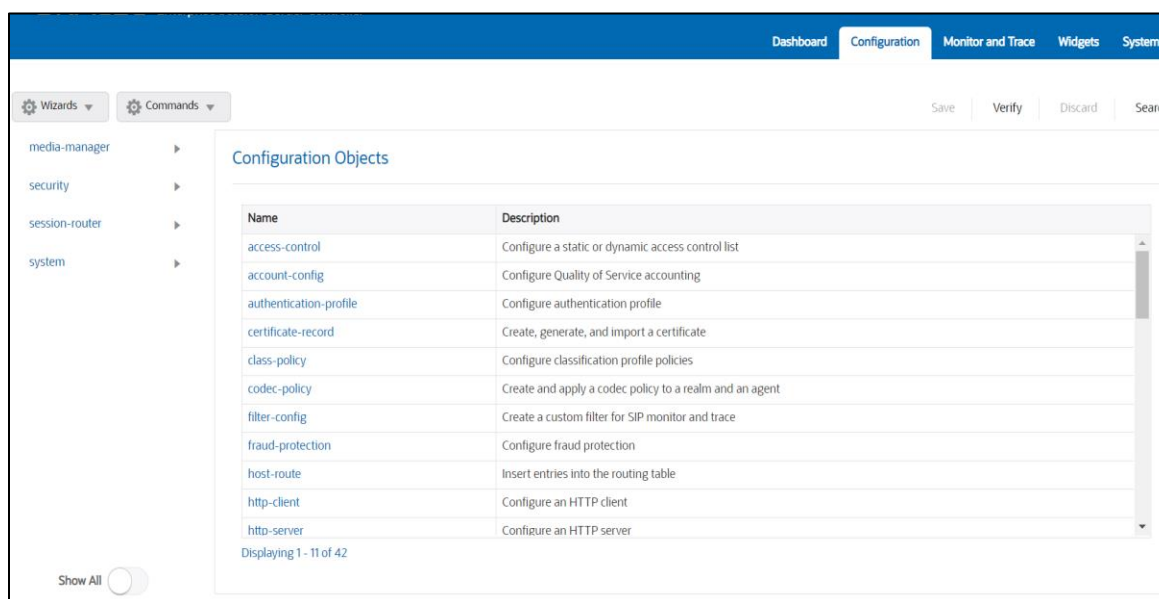
The Web GUI can be accessed through the url http://<SBC_MGMT_IP>.



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



Go 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

Go to system->system-config

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration categories, with 'system-config' selected. The main content area is titled 'Modify System Config' and contains the following fields:

- Hostname: Oracle SBC
- Description: (empty text area)
- Location: (empty text field)
- Mib System Contact: (empty text field)
- Mib System Name: (empty text field)
- Mib System Location: (empty text field)
- Acp TLS Profile: (dropdown menu)
- SNMP Enabled: enable

Buttons for 'OK' and 'Delete' are visible at the bottom of the form.

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

This screenshot shows the same 'Modify System Config' page, but with additional fields visible. The 'Default Gateway' field is highlighted with a red rectangle and contains the value '10.138.194.129'. Other fields include:

- Call Trace: enable
- Restart: enable
- Telnet Timeout: 0 (Range: 0..65535)
- Console Timeout: 0 (Range: 0..65535)
- HTTP Timeout: 5 (Range: 0..20)

An information icon and the message 'No alarm threshold to display. Please add.' are located at the bottom of the form area. 'OK' and 'Delete' buttons are also present.

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

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

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

6.4. Configure Physical Interface values

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

Please configure M00 for Twilio side and M10 for Genesys side.

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

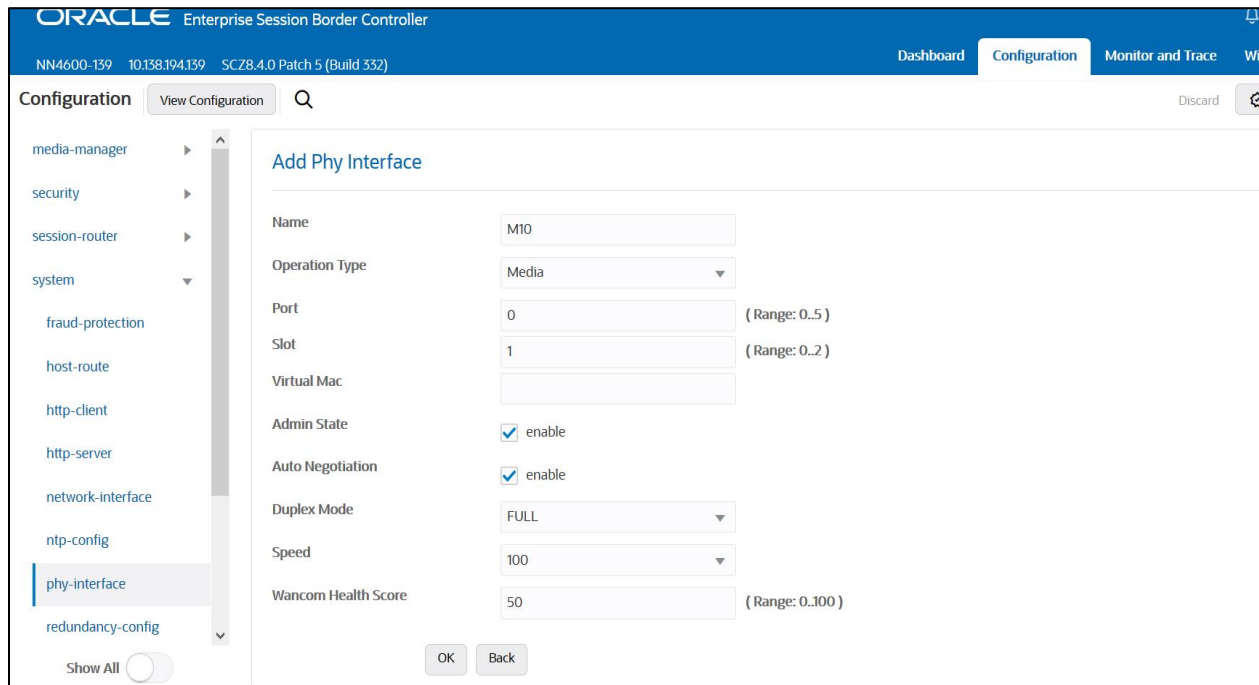
Please configure M00 interface as below.

The screenshot shows the Oracle Enterprise Session Border Controller configuration page for adding a physical interface. The interface is titled "Add Phy Interface" and includes the following fields and settings:

- Name:** M00
- Operation Type:** Media
- Port:** 0 (Range: 0..5)
- Slot:** 0 (Range: 0..2)
- Virtual Mac:** (empty field)
- Admin State:** enable
- Auto Negotiation:** enable
- Duplex Mode:** FULL
- Speed:** 100
- Wancom Health Score:** 50 (Range: 0..100)

At the bottom of the form, there are "OK" and "Back" buttons. The left sidebar shows the navigation menu with "phy-interface" selected.

Please configure M10 interface as below



6.5. Configure Network Interface values

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

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

Parameter Name	Twilio side Network interface	Genesys side Network interface
Name	M00	M10
Host Name		
IP address	<input type="text"/>	10.232.50.68
Netmask	255.255.255.192	255.255.255.0
Gateway	<input type="text"/>	10.232.50.1

Please configure network interface M00 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 'Configuration' tab is active. On the left, a sidebar lists various configuration categories, 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	
Hostname	
IP Address	
Pri Utility Addr	
Sec Utility Addr	
Netmask	255.255.255.192

Buttons for 'OK' and 'Back' are located at the bottom right of the form.

Similarly, configure network interface M10 as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for network interface M10. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'V'. The 'Configuration' tab is active. On the left, a sidebar lists various configuration categories, with 'network-interface' selected. The main area is titled 'Add Network Interface' and contains the following fields:

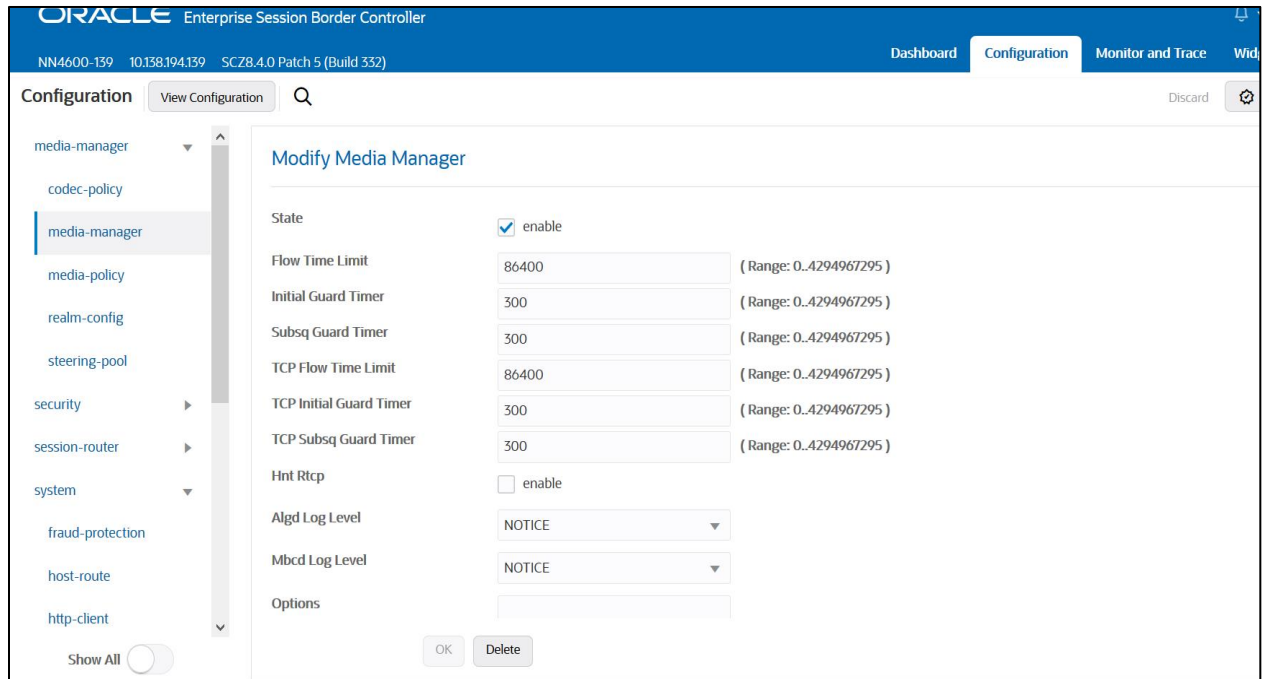
Name	M10
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	10.232.50.68
IP Address	10.232.50.68
Pri Utility Addr	
Sec Utility Addr	
Netmask	255.255.255.0

Buttons for 'OK' and 'Back' are located at the bottom right of the form.

6.6. Enable media manager

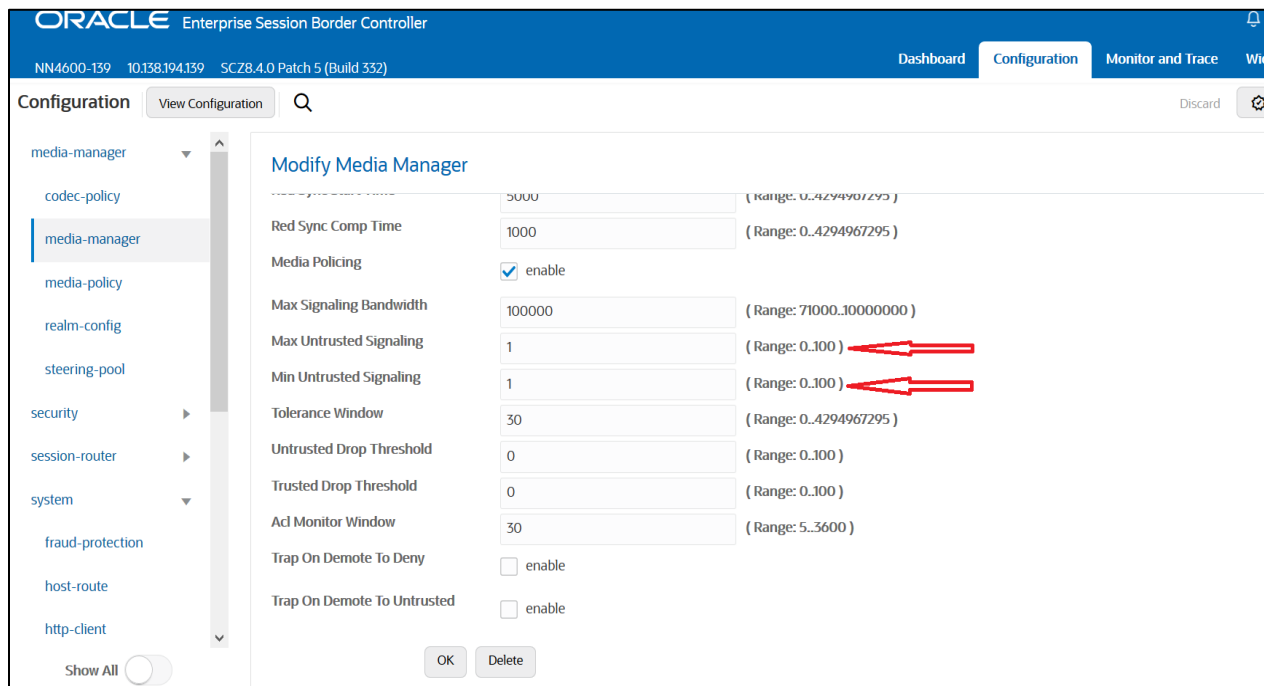
Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

In addition to the above config, please set the max and min untrusted signaling values to 1. Go to Media-Manager->Media-Manager



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'media-manager' selected. The main panel displays the 'Modify Media Manager' configuration page. The 'State' checkbox is checked, indicating the media manager is enabled. Other parameters are set to default values: Flow Time Limit (86400), Initial Guard Timer (300), Subsq Guard Timer (300), TCP Flow Time Limit (86400), TCP Initial Guard Timer (300), TCP Subsq Guard Timer (300), Hint Rtcp (disabled), Algd Log Level (NOTICE), and Mbcd Log Level (NOTICE). There are 'OK' and 'Delete' buttons at the bottom.

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	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	
Options		



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, specifically the 'Modify Media Manager' page. The 'Media Policing' checkbox is checked, indicating it is enabled. The 'Max Untrusted Signaling' and 'Min Untrusted Signaling' fields are both set to 1, with red arrows pointing to these values. Other parameters include: Red Sync Comp Time (5000), Media Policing (enabled), Max Signaling Bandwidth (100000), Tolerance Window (30), Untrusted Drop Threshold (0), Trusted Drop Threshold (0), and Acl Monitor Window (30). There are 'OK' and 'Delete' buttons at the bottom.

Parameter	Value	Range
Red Sync Comp Time	5000	(Range: 0..4294967295)
Media Policing	<input checked="" type="checkbox"/> enable	
Max Signaling Bandwidth	100000	(Range: 71000..10000000)
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	
Trap On Demote To Untrusted	<input type="checkbox"/> enable	

6.7. Enable sip-config

SIP config enables SIP handling in the SBC.

Make sure the home realm-id, registrar-domain and registrar-host are registrar-port are configured as below (The below example is specific to Genesys config that we have configured)

Also add the options to the sip-config as shown below.

To configure sip-config, Go to Session-Router->sip-config and in options, add the below

- add max-udp-length =0
- reg-cach-mode=from

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', version information (NN4600-139, 10.138.194.139, SCZ8.4.0 Patch 5 (Build 332)), and tabs for 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration categories, with 'sip-config' selected. The main area is titled 'Modify SIP Config' and contains the following fields:

State	<input checked="" type="checkbox"/> enable
Dialog Transparency	<input checked="" type="checkbox"/> enable
Home Realm ID	GenesysRealm
Egress Realm ID	
Nat Mode	None
Registrar Domain	*
Registrar Host	172.18.0.124
Registrar Port	4080 (Range: 0,1025..65535)
Init Timer	500 (Range: 0..4294967295)
Max Timer	4000 (Range: 0..4294967295)

Buttons for 'OK' and 'Delete' are visible at the bottom.

This screenshot shows the same 'Modify SIP Config' page but with more advanced options visible. The fields include:

Max Timer	4000 (Range: 0..4294967295)
Trans Expire	32 (Range: 0..4294967295)
Initial Inv Trans Expire	0 (Range: 0..999999999)
Invite Expire	180 (Range: 0..4294967295)
Session Max Life Limit	0
Enforcement Profile	
Red Max Trans	10000 (Range: 0..50000)
Options	max-udp-length=0 ✕ reg-cache-mode=from ✕
SPL Options	
SIP Message Len	4096 (Range: 0..65535)

Buttons for 'OK' and 'Delete' are visible at the bottom.

6.8. 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 two realms used in this configuration:

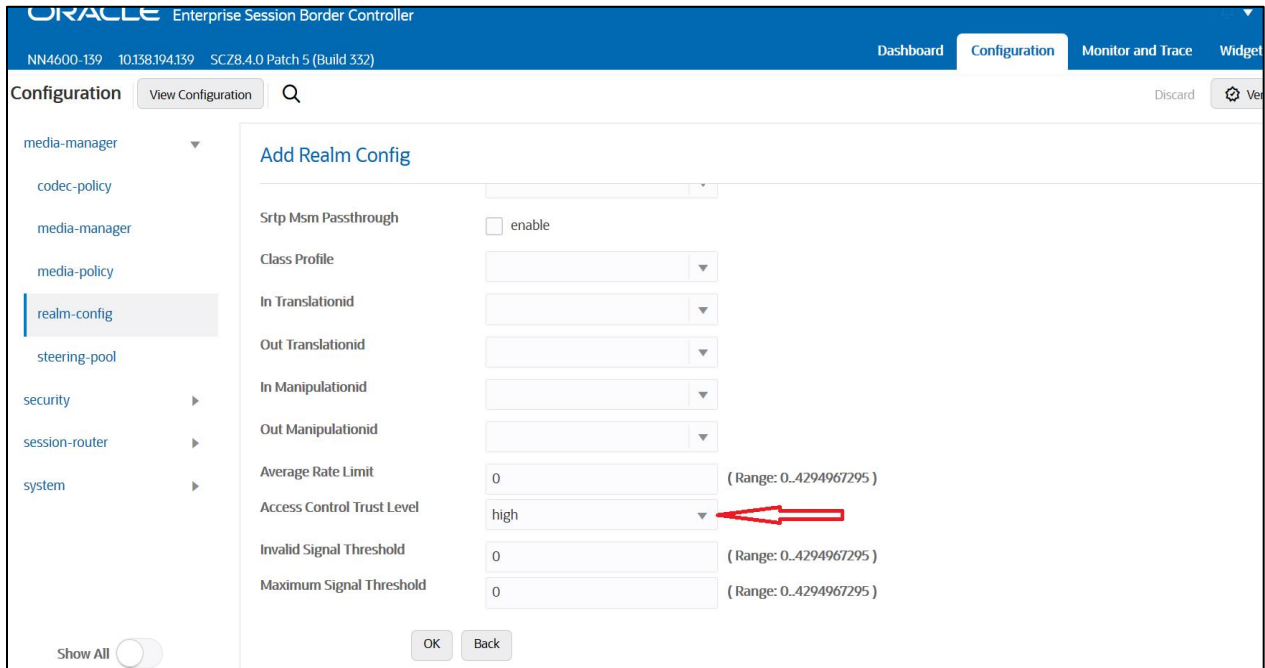
Config Parameter	Twilio Side	Genesys Side
Identifier	TwilioRealm	GenesysRealm
Network Interface	M00	M10
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FQDN		
Media Sec policy	sdespolicy	RTP
Access Control Trust Level	High	High

In the below case, Realm name is given as TwilioRealm for Twilio Elastic SIP Trunking Side
Please set the Access Control Trust Level as high for this realm

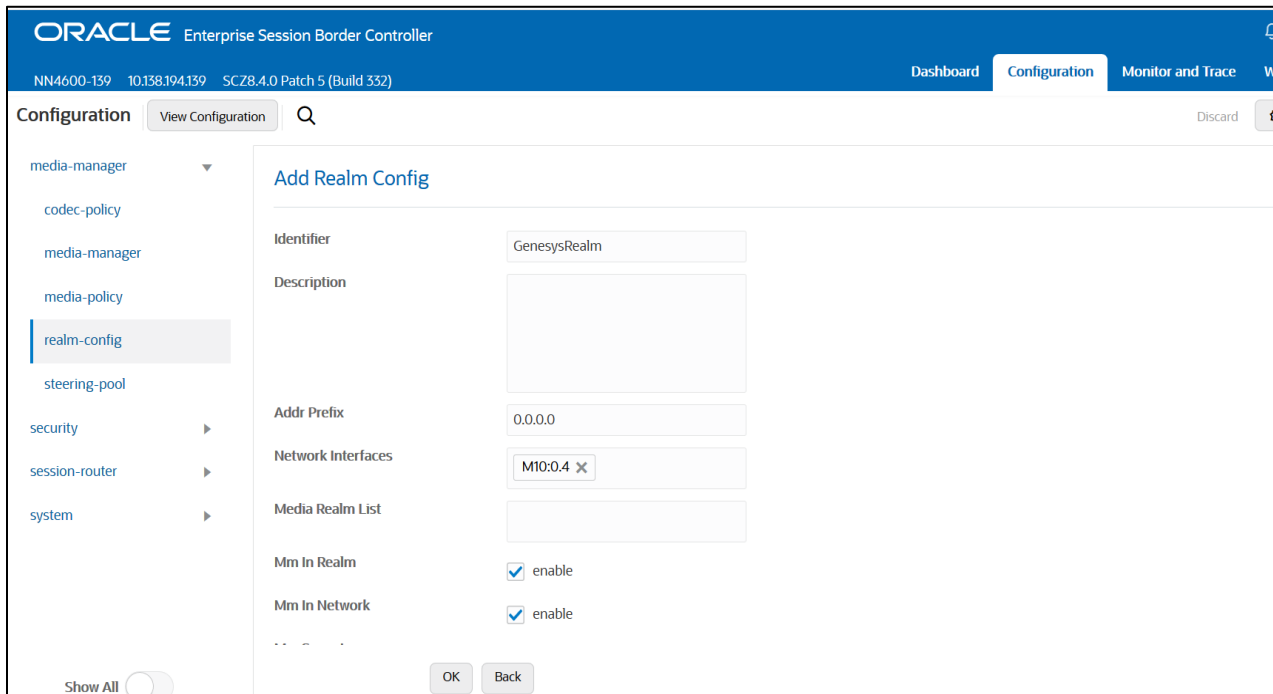
The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar shows a tree view with 'realm-config' selected under 'media-manager'. The main content area displays the 'Add Realm Config' form with the following fields:

- Identifier: TwilioRealm
- Description: (empty text area)
- Addr Prefix: 0.0.0.0
- Network Interfaces: M00:0.4
- Media Realm List: (empty list)
- Mm In Realm: enable
- Mm In Network: enable

At the bottom of the form are 'OK' and 'Back' buttons. A 'Show All' toggle is visible in the bottom left corner.



Similarly, Realm name is given as GenesysRealm for Genesys side.
Please set the Access Control Trust Level as high for this realm too.
We can use the same realm for Genesys Remote worker config too (Discussed in later part)



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

6.9. 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 displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Wid'. The main content area is titled 'Add Certificate Record' and contains the following fields:

Name	DigiCertRoot
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	Solutions
Common Name	Chain CA Certs
Key Size	2048
Alternate Name	
Trusted	<input checked="" type="checkbox"/> enable

At the bottom of the form are 'OK' and 'Back' buttons. A 'Show All' toggle is visible in the bottom left corner of the configuration area.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', version information (NN4600-139, 10.138.194.139, SC78.4.0 Patch 5 (Build 332)), and tabs for 'Dashboard', 'Configuration', and 'Monitor and Trace'. The 'Configuration' tab is active, and the 'certificate-record' option is selected in the left-hand navigation menu. The main content area is titled 'Add Certificate Record' and contains the following configuration fields:

- Key Size: 2048
- Alternate Name: (empty)
- Trusted: enable
- Key Usage List: digitalSignature, keyEncipherment
- Extended Key Usage List: serverAuth
- Key Algor: rsa
- Digest Algor: sha256
- Ecdsa Key Size: p256
- Cert Status Profile List: (empty)

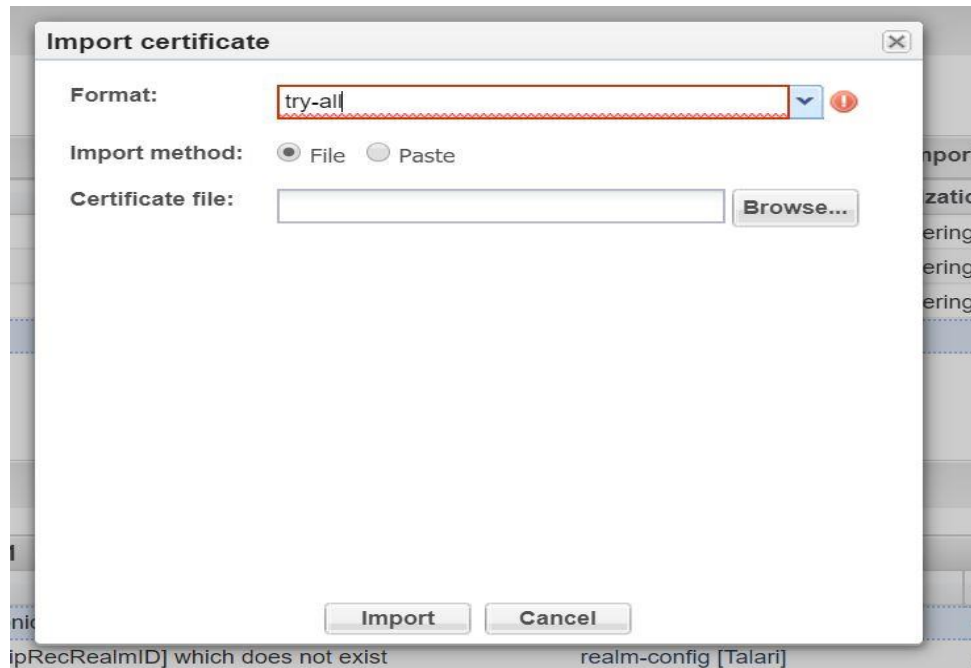
At the bottom of the configuration area, there are 'OK' and 'Back' buttons, and a 'Show All' toggle switch.

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

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

Step 2 – Deploy SBC & root certificates

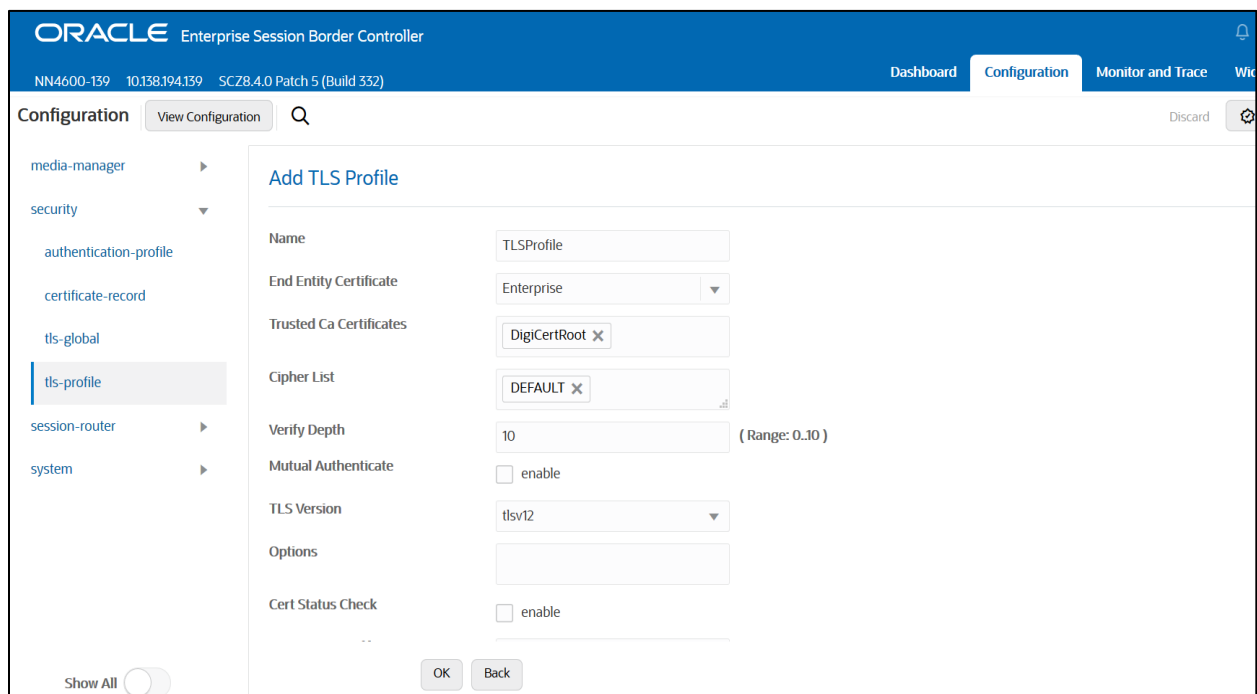
Once certificate record has been created – import the signed certificate to the SBC. Please note – all certificates including root certificates are required to be imported to the SBC. Once done, issue save/activate from the WebGUI



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

6.10. TLS-Profile

A TLS profile configuration on the SBC allows for specific certificates to be assigned. Go 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 side:



6.11. Configure SIP Interfaces

Navigate to sip-interface under session-router and configure the sip-interface as shown below. Please Configure sip-interface for the Twilio Elastic SIP Trunk side with below settings:

- 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 Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'sip-interface' selected. The main area is titled 'Modify SIP Interface'. The 'State' is set to 'enable'. The 'Realm ID' is 'TwilioRealm'. The 'SIP Ports' table contains one entry:

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

Similarly, Please Configure sip-interface for the Genesys side as below:

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for the Genesys side. The left sidebar lists various configuration categories, with 'sip-interface' selected. The main area is titled 'Modify SIP Interface'. The 'State' is set to 'enable'. The 'Realm ID' is 'GenesysRealm'. The 'SIP Ports' table contains two entries:

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
⋮	<input type="checkbox"/>	10.232.50.68	5060	UDP		agents-only	
⋮	<input type="checkbox"/>	10.232.50.68	5060	TCP		agents-only	

Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address. **Like Realm, We can use the same sip-interface for Genesys Remote worker config too (Discussed in later part)**

6.12. 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.

Go 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”

The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', system information (NN4600-139, 10.138.194.139, SCZ8.4.0 Patch 5 (Build 332)), and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Wid'. The 'Configuration' tab is active, showing a search bar and a 'View Configuration' button. A left sidebar lists various configuration categories, with 'session-agent' selected. The main area is titled 'Add Session Agent' and contains the following fields:

Hostname	oracle.pstn.twilio.com
IP Address	
Port	5061 (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
App Protocol	SIP
App Type	
Transport Method	StaticTLS
Realm ID	TwilioRealm
Egress Realm ID	
Description	

At the bottom of the form are 'OK' and 'Back' buttons, and a 'Show All' toggle switch.

****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 Genesys Side 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 left sidebar lists various configuration categories, with 'session-agent' selected. The main content area is titled 'Add Session Agent' and contains the following fields:

- Hostname: 172.18.0.124
- IP Address: 172.18.0.124
- Port: 4080 (Range: 0,1025..65535)
- State: enable
- App Protocol: SIP
- App Type: (empty dropdown)
- Transport Method: UDP+TCP
- Realm ID: GenesysRealm
- Egress Realm ID: (empty dropdown)
- Description: (empty text area)

Buttons for 'OK' and 'Back' are located at the bottom of the form.

6.13. Configure local-policy

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

To route the calls from Genesys side to Twilio side, Use the below local –policy

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

- From Address: * X
- To Address: * X
- Source Realm: GenesysRealm X
- Description: (empty text area)
- State: enable
- Policy Priority: none
- Policy Attributes: (empty text area)

Buttons for 'OK' and 'Back' are located at the bottom of the form.

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

- Source Realm: GenesysRealm
- Description: (empty text area)
- State: enable
- Policy Priority: none
- Policy Attributes: A table with columns for Action, Select, Next Hop, Realm, Action, Terminate Re..., Cost, State, App Protocol, Lookup, and Next Hop.

Action	Select	Next Hop	Realm	Action	Terminate Re...	Cost	State	App Protocol	Lookup	Next Hop
:	<input type="checkbox"/>	oracle.pstn.twil...	TwilioRealm	replace-uri	disabled	0	enabled		single	

Buttons for 'OK' and 'Back' are located at the bottom of the configuration area.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for 'Add Local Policy'. The left sidebar is the same as in the previous screenshot, with 'local-policy' selected. The main area is titled 'Add Local Policy' and contains the following fields:

- From Address: *
- To Address: *
- Source Realm: TwilioRealm
- Description: (empty text area)
- State: enable
- Policy Priority: none
- Policy Attributes: (empty table)

Buttons for 'OK' and 'Back' are located at the bottom of the configuration area.

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 'local-policy' selected. The main content area is titled 'Modify Local Policy' and contains the following fields:

- Source Realm: TwilioRealm
- Description: (empty text area)
- State: enable
- Policy Priority: none
- Policy Attributes: A table with columns for Action, Select, Next Hop, Realm, Action, Terminate Re..., Cost, State, App Protocol, and Lookup.

Action	Select	Next Hop	Realm	Action	Terminate Re...	Cost	State	App Protocol	Lookup
:	<input type="checkbox"/>	172.18.0.124	GenesysRealm	none	disabled	0	enabled		single

Buttons for 'OK' and 'Back' are located at the bottom of the configuration area.

6.14. Configure steering-pool

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

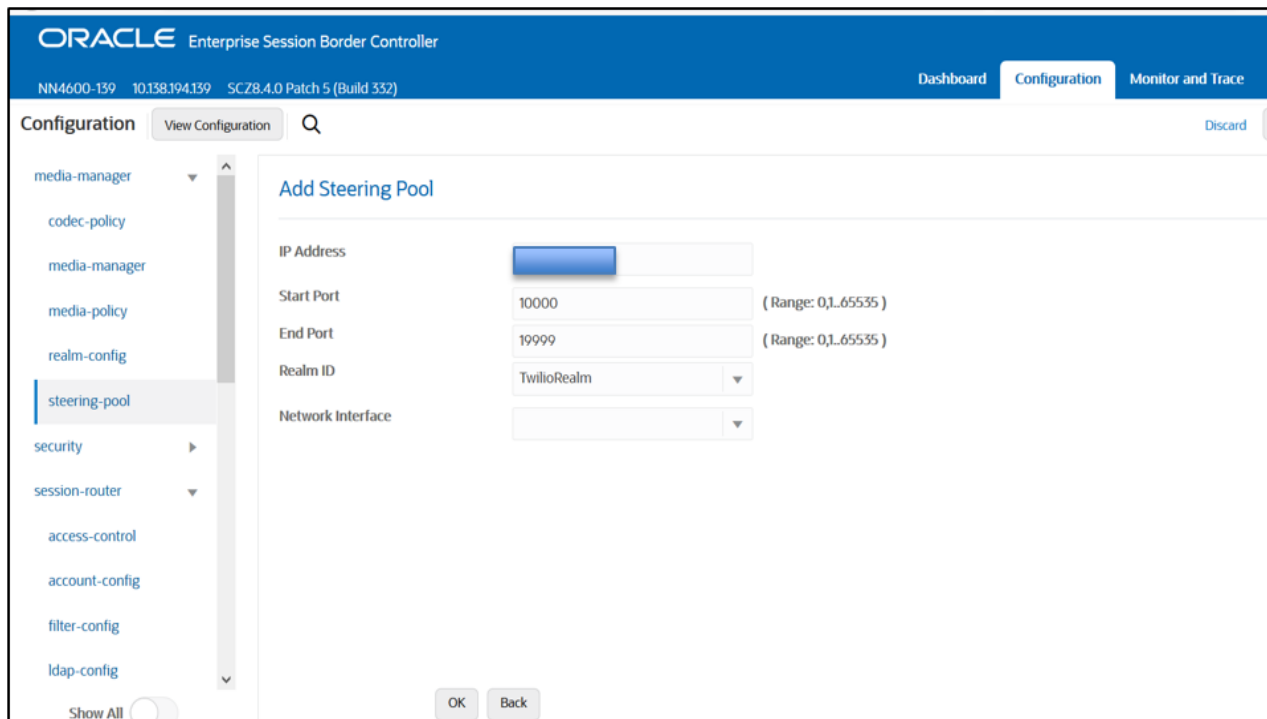
Genesys side steering pool.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for adding a steering pool. The left sidebar has 'steering-pool' selected. The main content area is titled 'Add Steering Pool' and contains the following fields:

- IP Address: 10.232.50.68
- Start Port: 20000 (Range: 0,1..65535)
- End Port: 29999 (Range: 0,1..65535)
- Realm ID: GenesysRealm
- Network Interface: (empty dropdown)

Buttons for 'OK' and 'Back' are located at the bottom of the configuration area.

Twilio side steering pool.



6.15. Configure Ping Response

To simplify the ORACLE SBC configuration, 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

NN4600-139 10.138.194.139 SCZ8.4.0 Patch 5 (Build 332) Dashboard Configuration Monitor and Trace Wid

Configuration View Configuration Q Discard

local-routing-confng
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring

Show All

Add Session Agent

Hostname: oracle.pstn.twilio.com

IP Address: []

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

State: enable

App Protocol: SIP

App Type: []

Transport Method: StaticTLS

Realm ID: TwilioRealm

Egress Realm ID: []

Description: []

OK Back

ORACLE Enterprise Session Border Controller

NN4600-139 10.138.194.139 SCZ8.4.0 Patch 5 (Build 332) Dashboard Configuration Monitor and Trace Wid

Configuration View Configuration Q Discard

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

Add Session Agent

In Translationid: []

Out Translationid: []

Trust Me: enable

Local Response Map: []

Ping Response: enable

In Manipulationid: []

Out Manipulationid: []

Manipulation String: []

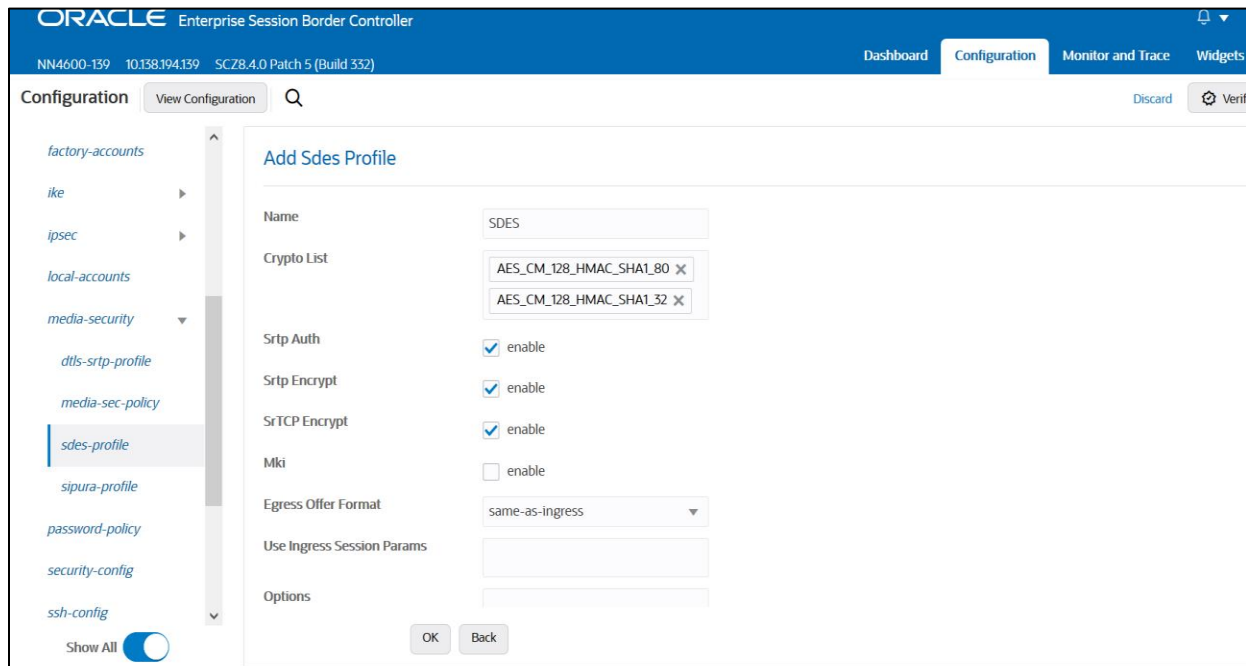
Manipulation Pattern: []

Trunk Group: []

OK Back

6.16. Configure sdes profile

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



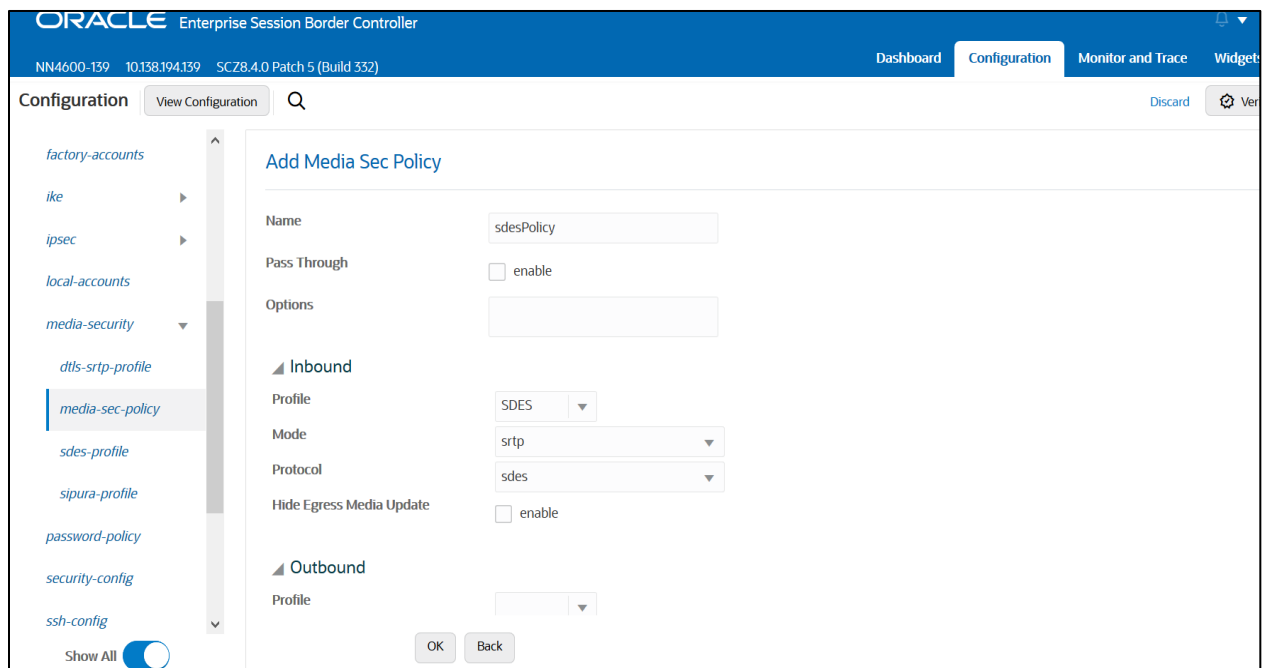
The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'media-security' expanded and 'sdes-profile' selected. The main content area is titled 'Add Sdes Profile' and contains the following fields:

- 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]
- Options: [Empty field]

Buttons for 'OK' and 'Back' are located at the bottom right of the form.

6.17. Configure Media Security Profile

Please go 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.

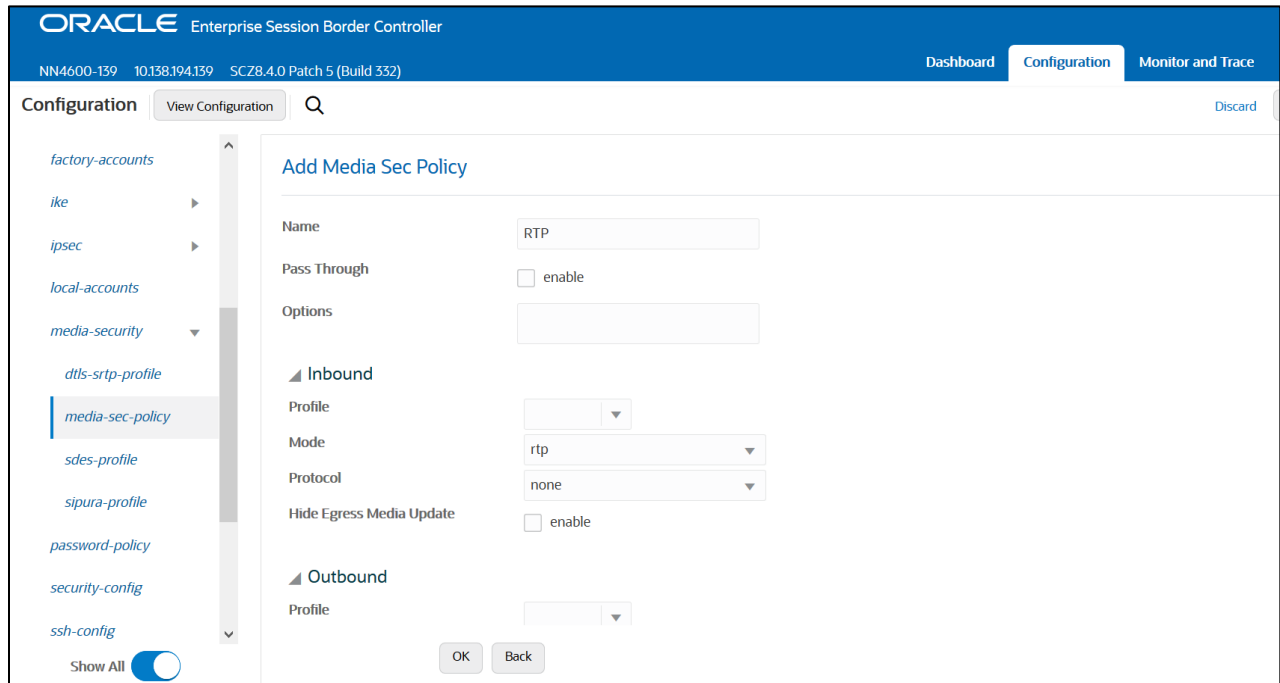


The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'media-security' expanded and 'media-sec-policy' selected. The main content area is titled 'Add Media Sec Policy' and contains the following fields:

- Name: sdesPolicy
- Pass Through: enable
- Options: [Empty field]
- Inbound**
 - Profile: SDES
 - Mode: srtp
 - Protocol: sdes
 - Hide Egress Media Update: enable
- Outbound**
 - Profile: [Empty field]

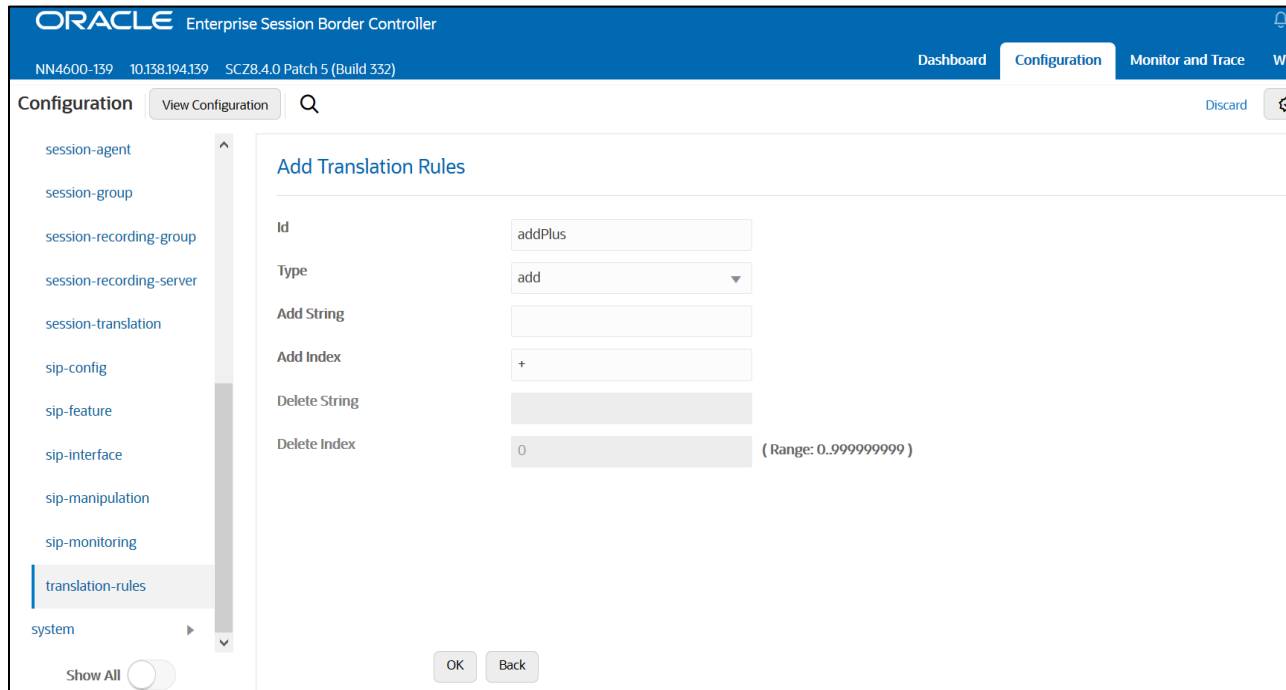
Buttons for 'OK' and 'Back' are located at the bottom right of the form.

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



6.18. Configure Translation Rules

The translation rules sub-element is where the actual translation rules are created. Go to Session router → translation-rules and create the below two rules.



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration categories, with 'translation-rules' selected. The main content area is titled 'Add Translation Rules' and contains the following fields:

- Id:** removeplus
- Type:** delete
- Add String:** (empty field)
- Add Index:** 0
- Delete String:** +
- Delete Index:** 0 (Range: 0..999999999)

Buttons for 'OK' and 'Back' are located at the bottom of the form.

6.19. Configure Session Translation Rules

A session translation defines how translation rules are applied to calling and called numbers. Go to Session Router → session-translation and configure the below translation rules.

Add the below translation rule to Genesys side.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for 'Add Session Translation'. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration categories, with 'session-translation' selected. The main content area is titled 'Add Session Translation' and contains the following fields:

- Id:** toGenesys
- Rules Calling:** removeplus X
- Rules Called:** removeplus X
- Rules Asserted Id:** (empty field)
- Rules Redirect:** (empty field)
- Rules Isup Cdpn:** (empty field)
- Rules Isup Cgpn:** (empty field)
- Rules Isup Gn:** (empty field)

Buttons for 'OK' and 'Back' are located at the bottom of the form.

Add the below translation rule to Twilio side as PSTN expects call with + sign.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', system information (NN4600-139, 10.138.194.139, SCZ8.4.0 Patch 5 (Build 332)), and tabs for 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration categories, with 'session-translation' selected. The main content area is titled 'Add Session Translation' and contains the following fields:

- Id:** toTwilio
- Rules Calling:** addPlus X
- Rules Called:** addPlus X
- Rules Asserted Id:** (empty)
- Rules Redirect:** (empty)
- Rules Isup Cdpn:** (empty)
- Rules Isup Cgpn:** (empty)
- Rules Isup Gn:** (empty)

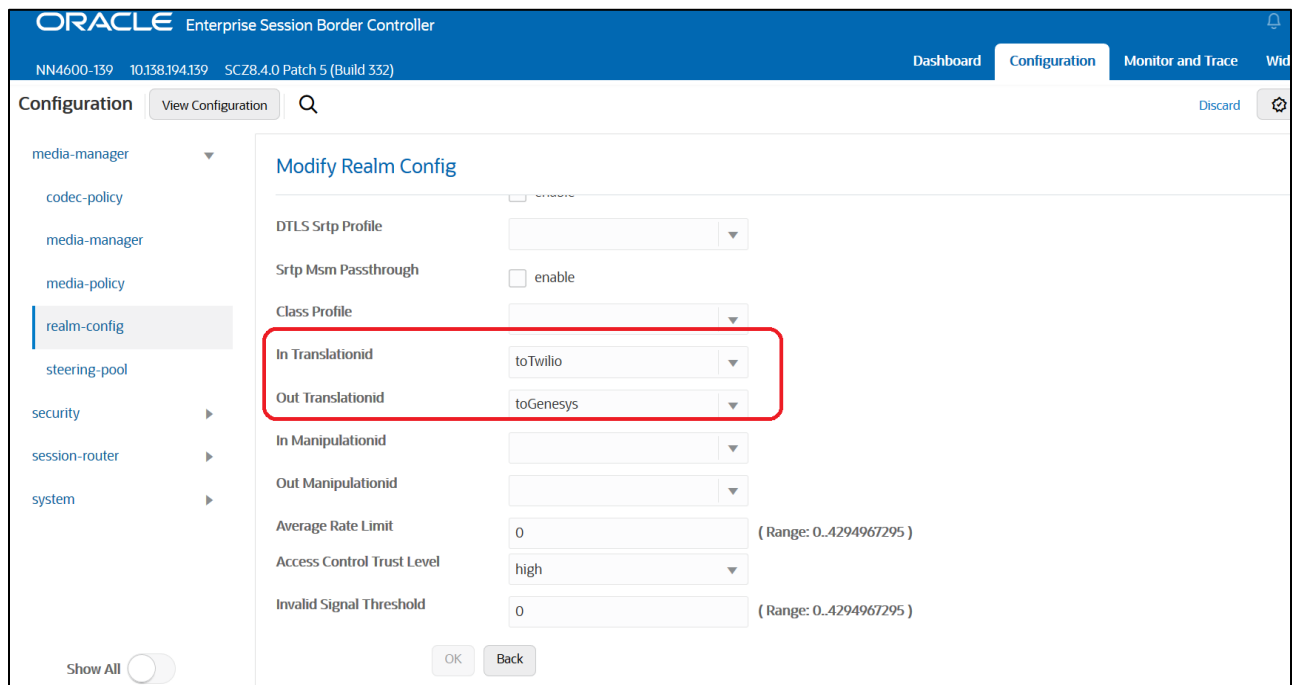
Buttons for 'OK' and 'Back' are located at the bottom right of the form.

Please add the above session translation rules to Genesys realm as shown below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for 'Modify Realm Config'. The top navigation bar is identical to the previous screenshot. The left sidebar shows 'realm-config' selected under the 'media-manager' category. The main content area is titled 'Modify Realm Config' and contains the following fields:

- Identifier:** GenesysRealm
- Description:** (empty)
- Addr Prefix:** 0.0.0.0
- Network Interfaces:** M10:0.4 X
- Media Realm List:** (empty)
- Mm In Realm:** enable
- Mm In Network:** enable

Buttons for 'OK' and 'Back' are located at the bottom right of the form.



With this, SBC configuration is complete

7. SBC configuration for Genesys Remote Worker

This section of Genesys Remote Worker configuration is included for Genesys remote endpoints that register through the Oracle SBC to the Genesys SIP Server. This would require additional configuration to be configured on the Oracle SBC along with the SIP trunking config as mentioned in the earlier description of the test bed. To complete the particular testing we have configured Genesys endpoints which will register to Genesys SIP server through the SBC. SBC will handle the calls based on the registration information present in the cache. **Please note that Genesys Remote worker Access side is secured (TLS/SRTP) and Genesys Core side is unsecured (UDP or TCP/RTP)**

In order to achieve the requirement we have made below configuration on the Oracle SBC

Access Realm for Genesys Remote worker

Steering Pool associated with the Realm for Genesys Remote worker

Sip-interface associated with the Realm for Genesys Remote worker

(Optional) A local-policy to route the registration requests from this Realm to the SIP Server.

Note -The local-policy element is optional as we can enable the Route to registrar parameter on the sip-interface config to route the requests to the Registrar.

The registrar host and port is configured in the sip-config element on the SBC. The remote endpoint sends register requests from Genesys Access Realm onto the SBC and then SBC registers these endpoints onto the Genesys Core Realm maintaining the registration cache in its database to route inbound calls to these endpoint. Below are the snippets from the Oracle SBC Web GUI for the Remote worker configuration.

7.1. 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.

In the below example, Realm name is given as GenesyspublicRealm for Genesys Access Side.
Please set the Access Control Trust Level as medium for this realm

The core realm is same GenesysRealm which we have configured already in earlier section.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration categories, with 'realm-config' under 'media-manager' selected. The main content area is titled 'Add Realm Config' and contains the following fields:

- Identifier: GenesyspublicRealm
- Description: (empty text area)
- Addr Prefix: 0.0.0.0
- Network Interfaces: M00:0.4
- Media Realm List: (empty text area)
- Mm In Realm: enable
- Mm In Network: enable

At the bottom of the form are 'OK' and 'Back' buttons, and a 'Show All' toggle is visible in the sidebar.

This screenshot shows the same 'Add Realm Config' page but with advanced settings expanded. The 'Access Control Trust Level' dropdown menu is highlighted with a red box and is set to 'medium'. Other advanced settings include:

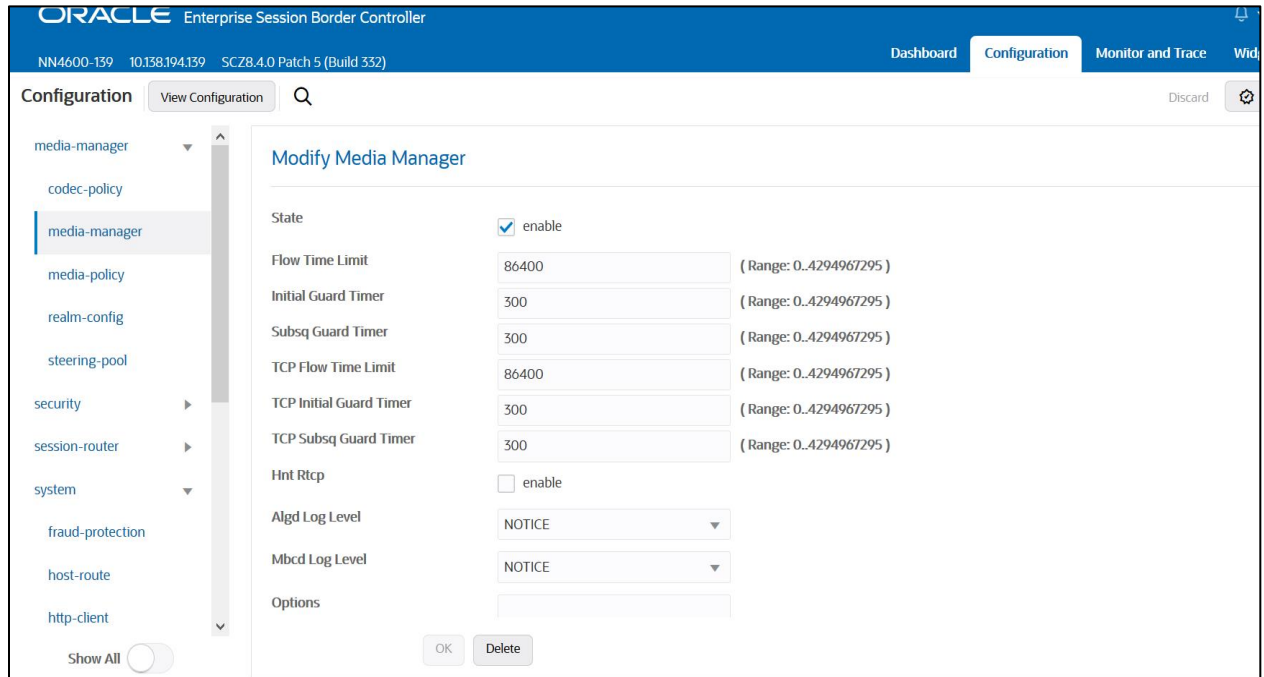
- In Translationid: (dropdown)
- Out Translationid: (dropdown)
- In Manipulationid: (dropdown)
- Out Manipulationid: (dropdown)
- Average Rate Limit: 0 (Range: 0..4294967295)
- Access Control Trust Level: medium (highlighted)
- Invalid Signal Threshold: 0 (Range: 0..4294967295)
- Maximum Signal Threshold: 0 (Range: 0..4294967295)
- Untrusted Signal Threshold: 0 (Range: 0..4294967295)
- Nat Trust Threshold: 0 (Range: 0..65535)
- Max Endpoints Per Nat: 0 (Range: 0..65535)

'OK' and 'Back' buttons are at the bottom, and the 'Show All' toggle is in the sidebar.

7.2. Enable media manager

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

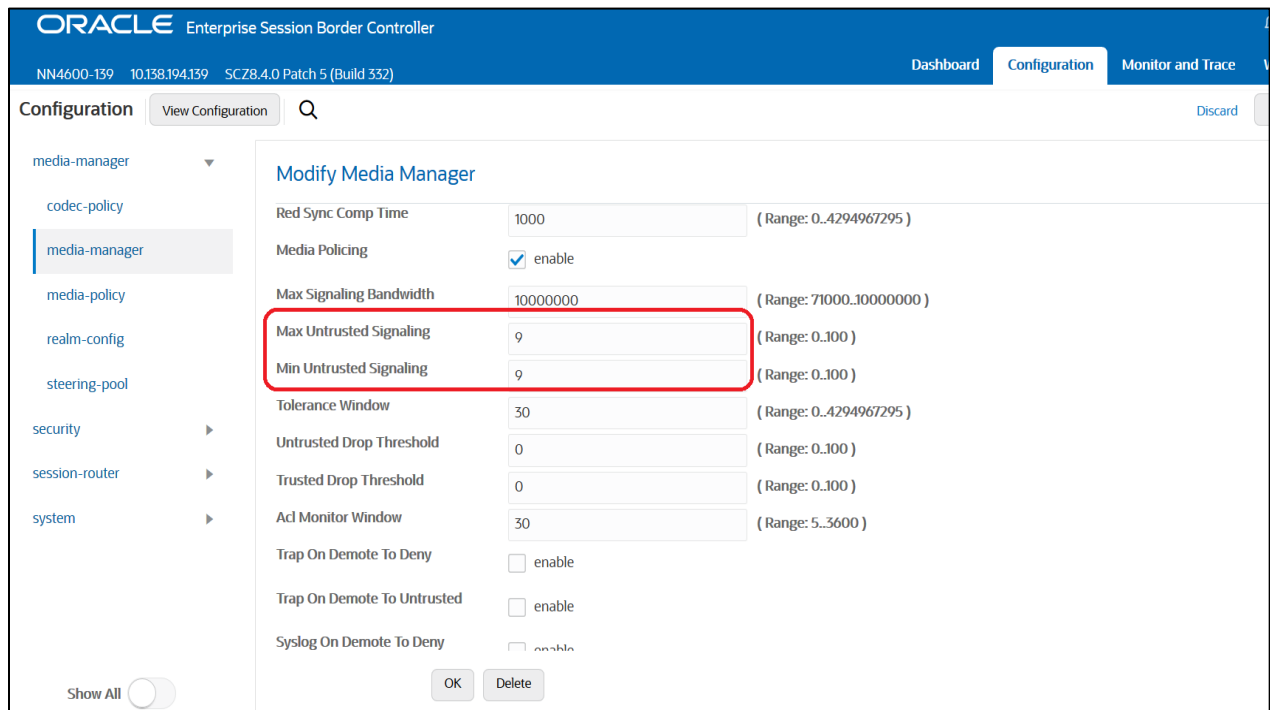
In addition to the above config, please set the max and min untrusted signaling values to 9 which takes care of Access Realm. Go to Media-Manager->Media-Manager



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Wid'. The left sidebar lists various configuration categories, with 'media-manager' selected. The main content area is titled 'Modify Media Manager' and 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)
Hnt Rtcp	<input type="checkbox"/> enable	
AlgD Log Level	NOTICE	
Mbcd Log Level	NOTICE	
Options		

Buttons for 'OK' and 'Delete' are visible at the bottom of the configuration area.



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, similar to the previous one. The left sidebar shows 'media-manager' selected. The main content area is titled 'Modify Media Manager' and contains the following settings:

Parameter	Value	Range
Red Sync Comp Time	1000	(Range: 0..4294967295)
Media Policing	<input checked="" type="checkbox"/> enable	
Max Signaling Bandwidth	10000000	(Range: 71000..10000000)
Max Untrusted Signaling	9	(Range: 0..100)
Min Untrusted Signaling	9	(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	
Trap On Demote To Untrusted	<input type="checkbox"/> enable	
Syslog On Demote To Deny	<input type="checkbox"/> enable	

The 'Max Untrusted Signaling' and 'Min Untrusted Signaling' fields are highlighted with a red box. Buttons for 'OK' and 'Delete' are visible at the bottom of the configuration area.

7.3. Configure SIP Interfaces

Navigate to sip-interface under session-router and configure the sip-interface as shown below. Please Configure sip-interface for the for Genesys Access side as below:

- Tls-profile needs to match the name of the tls-profile created earlier.
- Set allow-anonymous to Registered to ensure traffic to this sip-interface only comes from the registered user.
- Set NAT traversal to always for the remote workers to register.
- Enable Registration Caching and Route to Register

The screenshot shows the Oracle Enterprise Session Border Controller configuration page for a SIP Interface. The interface includes a navigation menu on the left with options like local-routing-config, media-profile, session-agent, session-group, session-recording-group, session-recording-server, session-translation, sip-config, sip-feature, sip-interface (selected), sip-manipulation, and sip-monitoring. The main content area is titled 'Modify SIP Interface' and contains the following configuration fields:

- State: enable
- Realm ID: GenesyspublicRealm
- Description: (Empty text area)

Below these fields is a table for SIP Ports:

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	M
⋮	<input type="checkbox"/>	[Redacted]	5061	TLS	TLSPProfile	registered	

At the bottom of the configuration area are 'OK' and 'Back' buttons.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'sip-interface' selected. The main panel is titled 'Modify SIP Interface' and contains several configuration fields:

- Proxy Mode: [Dropdown]
- Redirect Action: [Dropdown]
- Nat Traversal: **always** (indicated by a red arrow)
- Nat Interval: 30 (Range: 0..4294967295)
- TCP Nat Interval: 90 (Range: 0..4294967295)
- Registration Caching: **enable** (indicated by a red arrow)
- Min Reg Expire: 900 (Range: 0..999999999)
- Registration Interval: 3600 (Range: 0..4294967295)
- Route To Registrar: **enable** (indicated by a red arrow)
- Secured Network: enable
- Uri Fqdn Domain: [Text Field]

Buttons for 'OK' and 'Back' are located at the bottom of the configuration area.

The sip-interface created for Genesys side in earlier section can be used as Genesys Core side Interface. Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

7.4. Configure steering-pool

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

Genesys Access side steering pool.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for 'Add Steering Pool'. The left sidebar lists various configuration categories, with 'steering-pool' selected. The main panel is titled 'Add Steering Pool' and contains several configuration fields:

- IP Address: [Text Field]
- Start Port: 40000 (Range: 0,1..65535)
- End Port: 49999 (Range: 0,1..65535)
- Realm ID: GenesyspublicRealm (Dropdown)
- Network Interface: [Dropdown]

Buttons for 'OK' and 'Back' are located at the bottom of the configuration area.

7.5. Configure local-policy (Optional)

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

To route the calls from Genesys Access side to Core side and vice versa, Use the below local –policy

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'local-policy' selected under 'session-router'. The main content area is titled 'Add Local Policy' and contains the following fields:

- From Address:** A text input field with a clear button (X).
- To Address:** A text input field with a clear button (X).
- Source Realm:** A dropdown menu with 'GenesyspublicRealm' selected and a clear button (X).
- Description:** A large text area for entering a description.
- State:** A checkbox labeled 'enable' which is checked.
- Policy Priority:** A dropdown menu with 'none' selected.
- Policy Attributes:** A section for defining policy attributes.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for 'Modify Local Policy'. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Modify Local Policy' and contains the following fields:

- Source Realm:** A dropdown menu with 'GenesyspublicRealm' selected and a clear button (X).
- Description:** A large text area for entering a description.
- State:** A checkbox labeled 'enable' which is checked.
- Policy Priority:** A dropdown menu with 'none' selected.
- Policy Attributes:** A table for defining policy attributes.

Below the table are 'OK' and 'Back' buttons.

Action	Select	Next Hop	Realm	Action	Terminate Re...	Cost	State	App Protocol	Lookup
⋮	<input type="checkbox"/>	172.18.0.124	GenesysRealm	none	disabled	0	enabled	SIP	single

8. New SBC config/Deployment Using Configuration Assistant

When you first log on to the E-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 E-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.**

8.1. 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 PureEngage and Twilio Elastic SIP Trunking. The pre-requisite 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 CSR is generated by the SBC. For Twilio side, list of supported CA's can be found [here](#)

The following outline assumes you have established initial access to the SBC via console and completed the following steps:

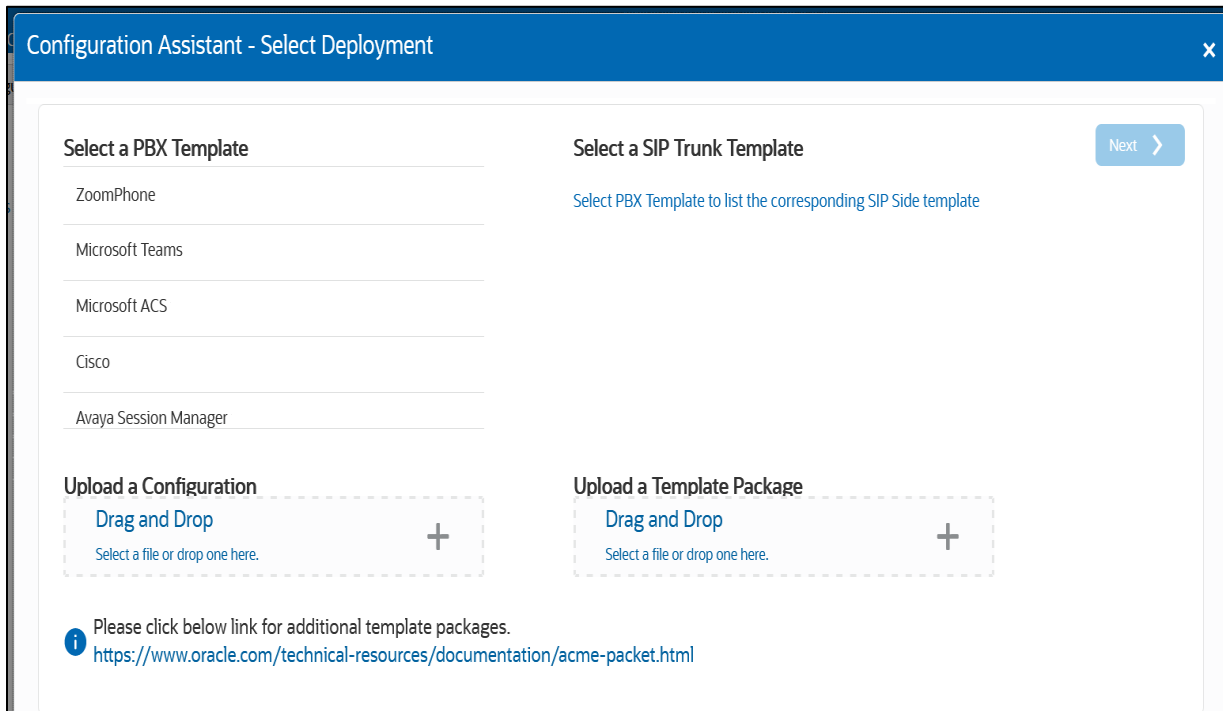
- Configured boot parameters for management access
- Setup Product
- Set Entitlements
- Configured HTTP-Server to establish access to SBC GUI

8.2. Initial GUI Access

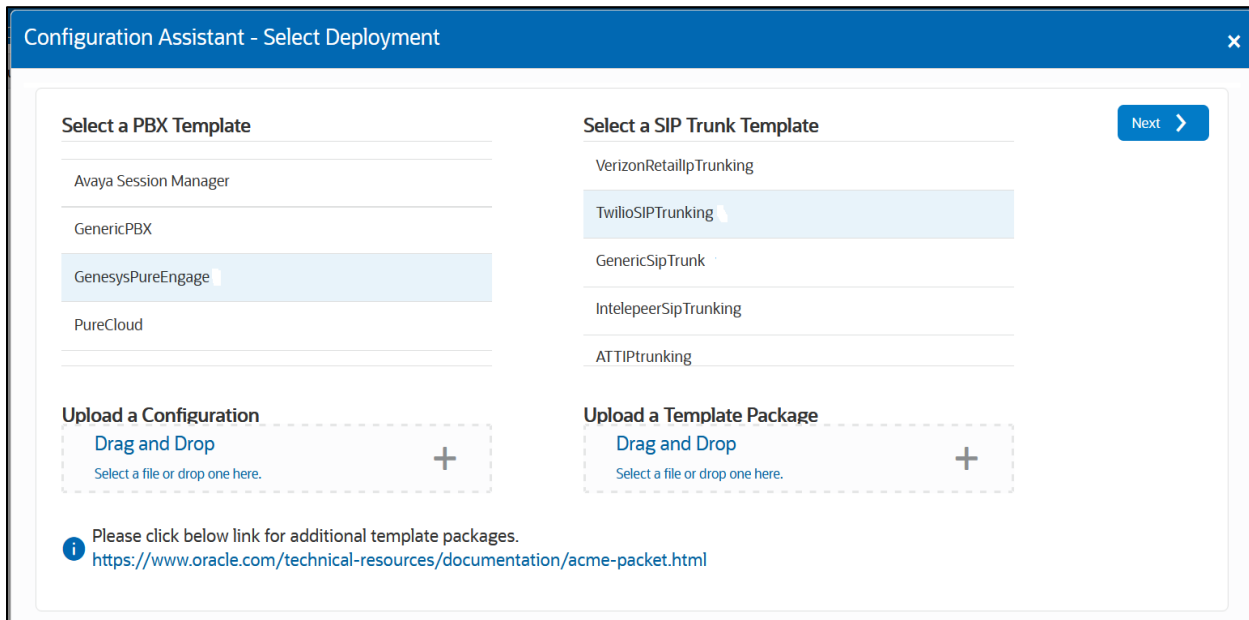
The Oracle SBC WebGui can be accessed by entering the following in your web browser:
`http(s)://<SBC Management IP>`.

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



As we can see, there are some templates of PBX populated in the template and we can select the PBX template that we want to use with our Twilio trunk and for this document, we have selected Genesys PureEngage template and once we select that, it asks us to select the SIP trunk template. After we select Twilio trunk template, the Next option would be enabled.



Click **Next**. The following “Notes” will be displayed related to pre-requisite

The screenshot shows a window titled "Configuration Assistant - Notes". It contains two columns of information:

- PBX Template**
Notes for GenesysPureEngage
Warning:
- Proceeding with the Configuration Assistant results in erasing the existing configuration.
Pre-requisites:
- Connect Port 0 of the Session Border Controller (SBC) to your network.
- Ensure that Transcoding resources are installed on your system (Hardware only).
- Configure at least one Transcoding core on your system (Virtual Machine Edition only).
- This template supports ONLY UDP/TCP configuration.
- Enable the Advanced entitlement on the system.
- Set Session Capacity in the entitlement.
- Set the system time.
- SIP Trunk Template**
Notes for TwilioSIPTrunking
Warning:
- Proceeding with the Configuration Assistant results in erasing the existing configuration.
Pre-requisites:
- Connect Port 1 of the Session Border Controller (SBC) to your network.
- Ensure that Transcoding resources are installed on your system (Hardware only).
- Configure at least one Transcoding core on your system (Virtual Machine Edition only).
- Add the SRTP license to the system.
- Enable the Advanced entitlement on the system.
- Set Session Capacity in the entitlement.
- Set the system time.

Click **Next** and we get the below screen where we need to enter the details for SBC configuration.

The screenshot shows a window titled "Configuration Assistant - Genesys PureEngage Network". It features a progress bar with 8 steps:

- Genesys PureEngage Network (Current step)
- Genesys Session Agent
- Transcoding
- Twilio Elastic SIP Trunk Network
- Twilio Session Agent
- Transcoding
- Root Trusted Certificate
- SBC Certificate for Twilio

Below the progress bar, the instruction reads: "Let's configure the interface that communicates with your Genesys Sip Server".

There are three required fields:

- Realm Name (Required)
- Port Number (Required, dropdown menu showing Port 0)
- Slot Number (Required, dropdown menu showing Slot 0)

8.3. Configuration Assistant Template Navigation

8.3.1. Page 1-Genesys PureEngage Network

Page 1 of the template is where you will configure the network information to connect to Genesys PureEngage Side

Configuration Assistant - Genesys PureEngage Network

1 — 2 — 3 — 4 — 5 — 6 — 7 — 8

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

Let's configure the interface that communicates with your Genesys Sip Server

Realm Name ⓘ
Required

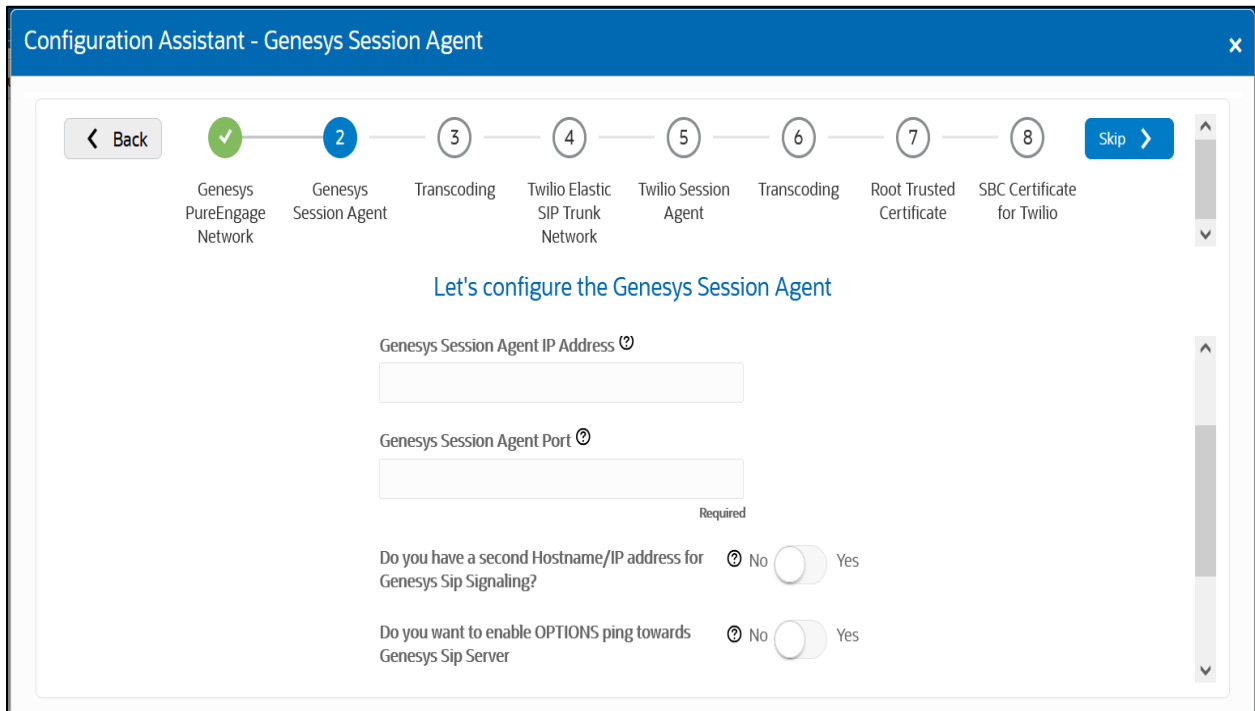
Port Number ⓘ
Port 0
Required

Slot Number ⓘ
Slot 0
Required

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”.

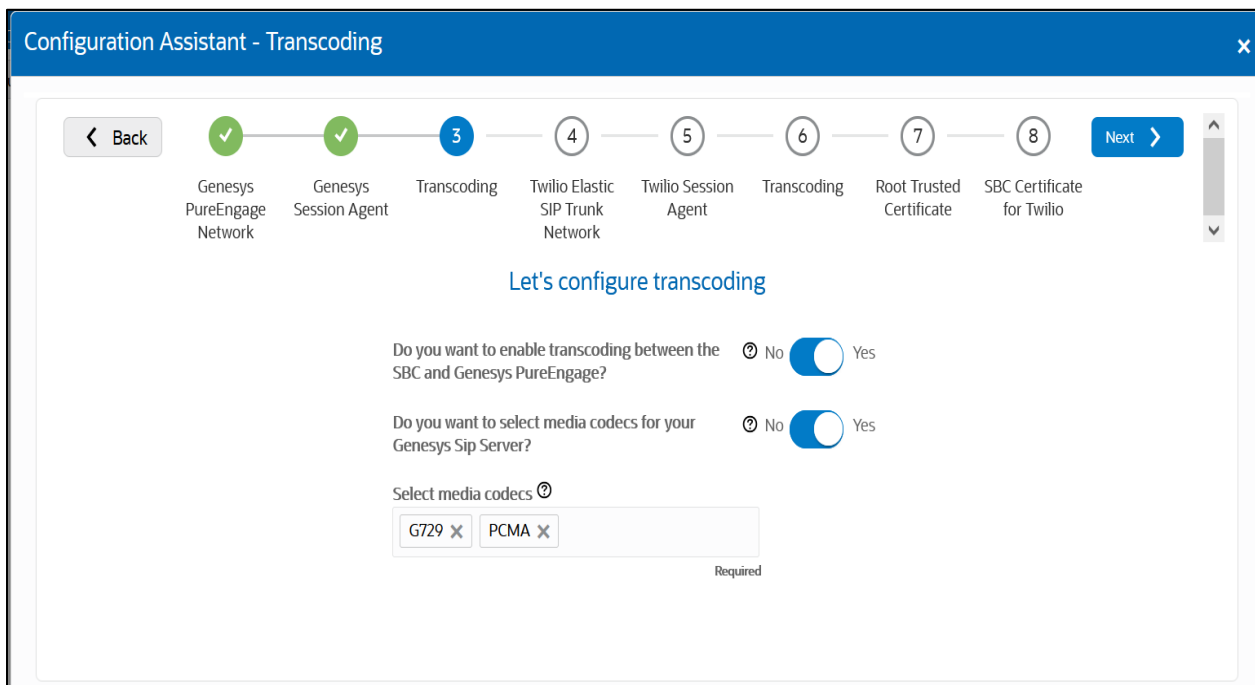
8.3.2. Page 2-Genesys Session agent

Page 2 of the template is where you will configure the Genesys PureEngage Session Agent details where you will enter the next hop IP address and port for sip signaling to and from your Genesys PureEngage Session Agent. Please fill the required fields and click Next.



8.3.3. Page 3 -Genesys side Transcoding

Page 3 is where you will be able to configure transcoding between the SBC and Genesys PureEngage. 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 Genesys Side. 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.



8.3.4. Page 4 - Twilio Elastic SIP Trunk Network

Page 4 of the template is where you will configure the network information to connect to Twilio Elastic SIP trunk Network. Please fill the required fields and Press Next.

The screenshot shows a configuration assistant window titled "Configuration Assistant - Twilio Elastic SIP Trunk Network". At the top, a progress bar indicates the current step is 4, "Twilio Elastic SIP Trunk Network", which is highlighted with a blue circle. Steps 1-3 are marked with green checkmarks, and steps 5-8 are marked with grey circles. A "Back" button is on the left, and a "Skip" button is on the right. Below the progress bar, the instruction "Let's configure the interface that communicates with Twilio Elastic SIP Trunk Network" is displayed. The form contains three required fields: "Realm Name" (text input), "Port Number" (dropdown menu with "Port 1" selected), and "Slot Number" (dropdown menu with "Slot 0" selected). Each field has a "Required" label and a help icon.

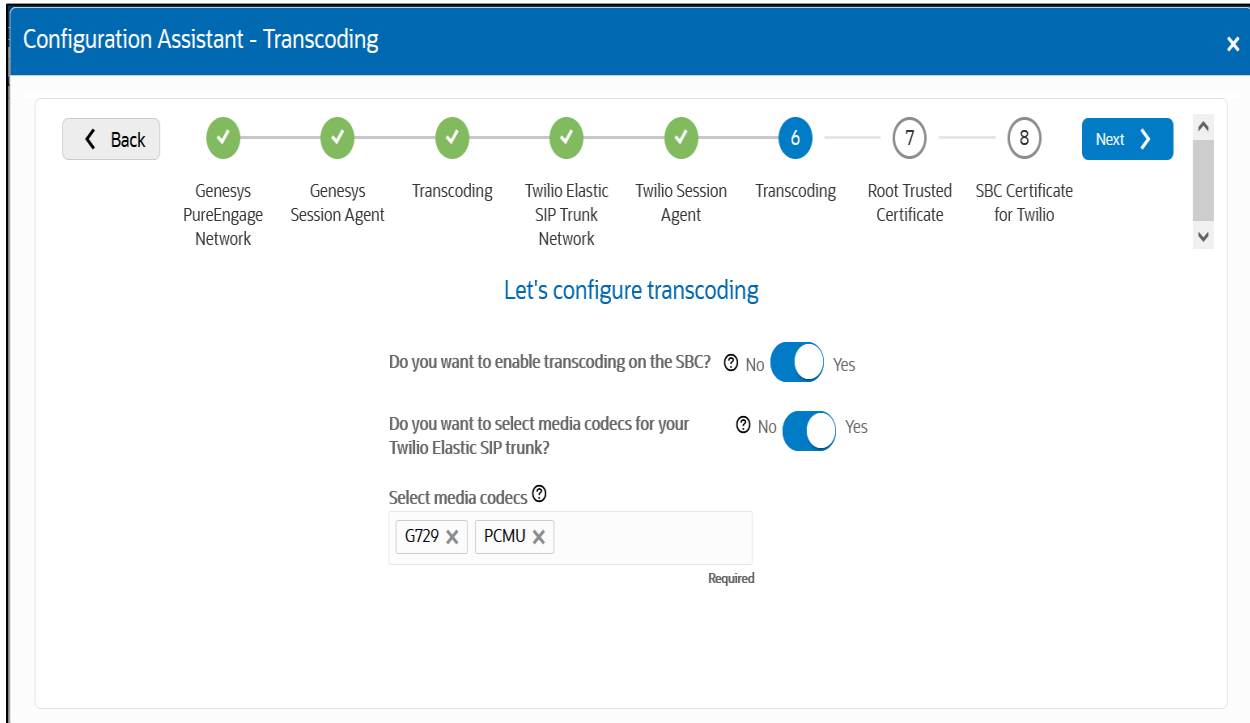
8.3.5. Page 5 - Twilio Session Agent

Page 5 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 Elastic SIP trunk. Please fill the required fields and click Next.

The screenshot shows a configuration assistant window titled "Configuration Assistant - Twilio Session Agent". The progress bar at the top indicates the current step is 5, "Twilio Session Agent", which is highlighted with a blue circle. Steps 1-4 are marked with green checkmarks, and steps 6-8 are marked with grey circles. A "Back" button is on the left, and a "Skip" button is on the right. Below the progress bar, the instruction "Let's configure session agent for Twilio" is displayed. The form contains three required fields: "Twilio Session Agent hostname" (text input), "Twilio Session Agent IP Address" (text input), and "Twilio Session Agent Port" (text input). Each field has a "Required" label and a help icon. At the bottom, there is a question: "Do you have a second hostname / IP address for" followed by radio buttons for "Yes" and "No".

8.3.6. Page 6 - Twilio side Transcoding

Page 6 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 toward 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.



8.3.7. Page 7 - Import Digi Cert Root CA Certificate for Twilio Side

Page 7 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.



8.3.8. Page 8 - SBC Certificates for Twilio side

PKCS12 Import

By default, the SBC is set to import a certificate in PKCS 12 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 from a supported CA, 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 supported CA

Same as PKCS12, you will enter the SBC's hostname under "FQDN or Common Name" and "Country" field (required) and answer the remaining question presented on this page (optional).

Configuration Assistant - SBC Certificate for Twilio

← Back

Genesys PureEngage Network ✓ Genesys Session Agent ✓ Transcoding ✓ Twilio Elastic SIP Trunk Network ✓ Twilio Session Agent ✓ Transcoding ✓ Root Trusted Certificate ✓ SBC Certificate for Twilio 8 Review

Let's start provisioning SBC certificates for Twilio Side

Certificate provisioning type ②
CSR Required

Fully Qualified Domain Name or Common Name ②
Required

Country ②
Required

State ②

8.4. 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.



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, “*TwilioCSR CSR*”.

On Page 8 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 as shown below.

The screenshot shows the 'Configuration Assistant - Summary' window. On the left, under 'Genesys PureEngage Network', there is an 'Edit' button and a list of configuration parameters:

- Realm Name: PureEngage
- Port Number: Port 0
- Slot Number: Slot 0
- Network IP Address: 10.232.50.70
- Network IP subnet mask: 255.255.255.0
- Network Gateway IP Address: 10.232.50.1

On the right, the 'Configuration' tab is active, showing a 'TwilioCSR CSR' configuration. A 'Copy' button is visible above a text area containing a long Base64-encoded CSR string. At the top right of the window, there are 'Download' and 'Apply' buttons.

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 a Twilio supported 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 8, the CSR tab will not be present under review.

8.5. Download and/or Apply

Now that the entries provided throughout the template have been reviewed, and the CSR has been copied into a text file (optional), 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.

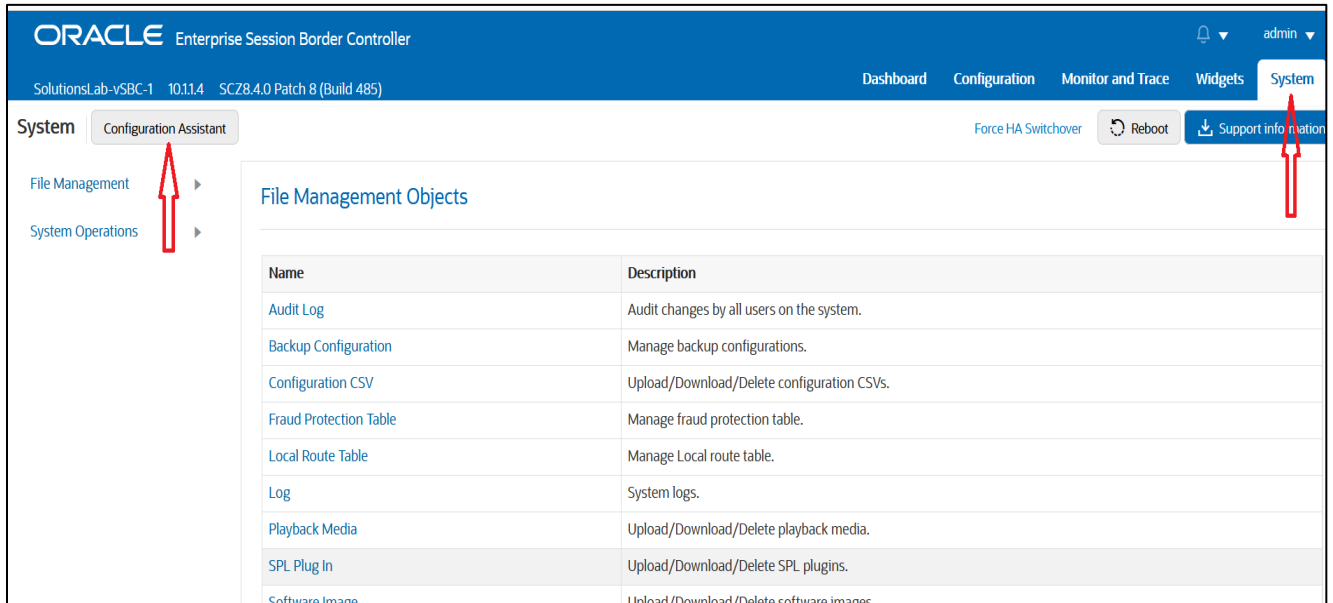
The screenshot shows the 'Configuration Assistant - Epilogue' window. It contains a 'Back' button on the left and a 'Confirm' button on the right. The main text reads: 'Perform the following actions after the system reboots to complete the deployment.' Below this, there are two columns of actions:

- Actions to be performed for GenesysPureEngage:** No more actions required for this template.
- Actions to be performed for TwilioSIPTrunking:** (The specific actions are not visible in the screenshot).

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 Genesys PureEngage with Twilio SIP trunking.

8.6. 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.



The screenshot displays the Oracle Enterprise Session Border Controller (SBC) GUI. The top navigation bar includes the Oracle logo, the product name 'Enterprise Session Border Controller', and the user 'admin'. Below this, the system information 'SolutionsLab-vSBC-1 10.11.14 SCZ8.4.0 Patch 8 (Build 485)' is shown. The main navigation tabs are 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'System' tab is selected, and the 'Configuration Assistant' sub-tab is active. A red arrow points to the 'Configuration Assistant' tab. Another red arrow points to the 'Support information' button in the top right corner of the main content area. The main content area displays 'File Management Objects' with a table listing various system components and their descriptions.

Name	Description
Audit Log	Audit changes by all users on the system.
Backup Configuration	Manage backup configurations.
Configuration CSV	Upload/Download/Delete configuration CSVs.
Fraud Protection Table	Manage fraud protection table.
Local Route Table	Manage Local route table.
Log	System logs.
Playback Media	Upload/Download/Delete playback media.
SPL Plug In	Upload/Download/Delete SPL plugins.
Software Image	Upload/Download/Delete software images.


9. Existing SBC configuration

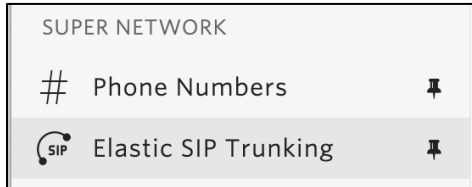
If the SBC being used is an existing SBC with functional configuration, following configuration elements are required:

- [New realm-config](#)
- [Configuring a certificate for SBC Interface](#)
- [TLS-Profile](#)
- [New sip-interface](#)
- [New session-agent](#)
- [New steering-pools](#)
- [New local-policy](#)
- [SDES Profile](#)
- [Media-sec-Policy](#)
- [New Translation Rules](#)
- [Session Translation Rules](#)

Please follow the steps mentioned in the above chapters to configure these elements.

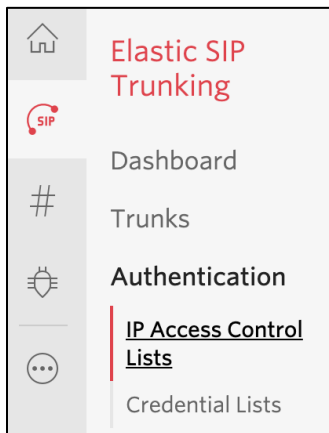
10. Twilio Elastic SIP Trunking Configuration

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



10.1. 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 All ...

ASSOCIATED SIP TRUNKS 0

ASSOCIATED SIP DOMAINS —

IP Address Ranges

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

IP ADDRESS RANGE	FRIENDLY NAME
155.212.214.102 / 32 155.212.214.102 - 155.212.214.102	155.212.214.102

10.2. 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

[Show Localized URIs](#)

Click on "Show localized URI's" and 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	<input type="text" value="Oracle x"/>	<input type="button" value="x"/>	<input type="button" value="v"/>	<input type="button" value="+"/>
CREDENTIAL LISTS	<input type="text" value="Click to select a Credential List"/>	<input type="button" value="v"/>	<input type="button" value="+"/>	

In the **Origination** section, we'll 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'll depict the configuration for North America:

Add Origination URL ✕

ORIGINATION SIP URI

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

WEIGHT
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

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'll route from Twilio's Umatilla edge.

10.3. 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.

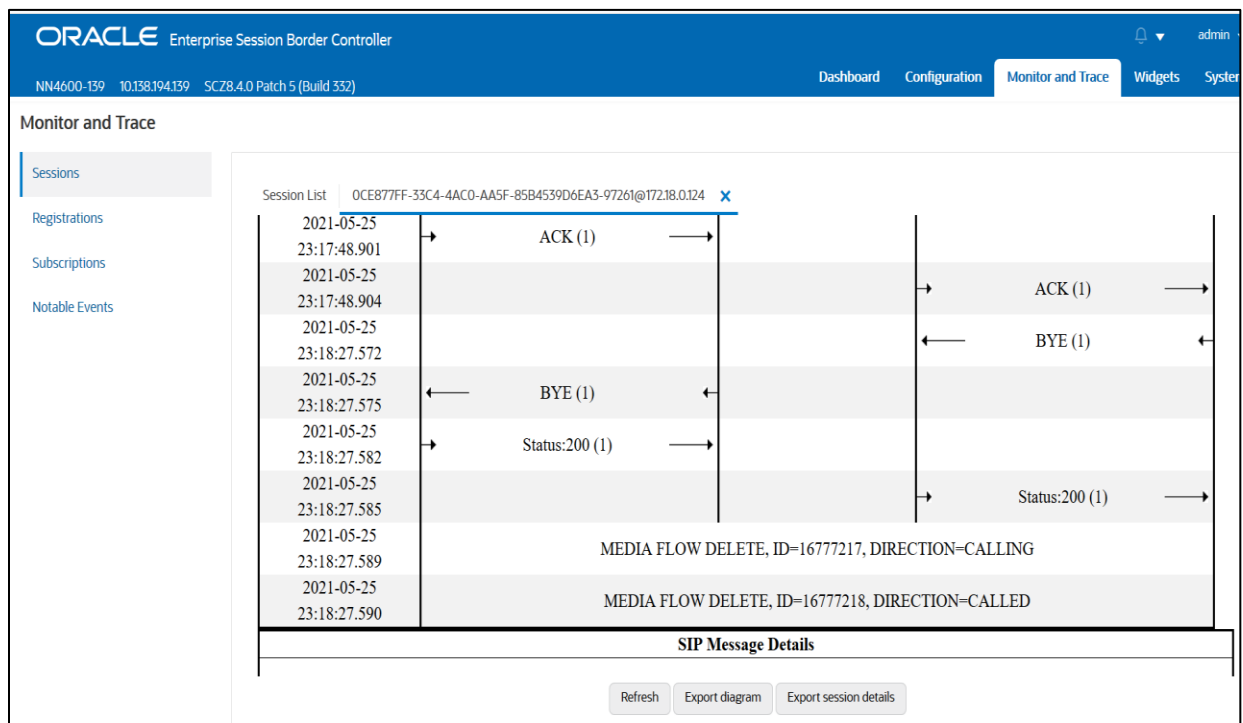
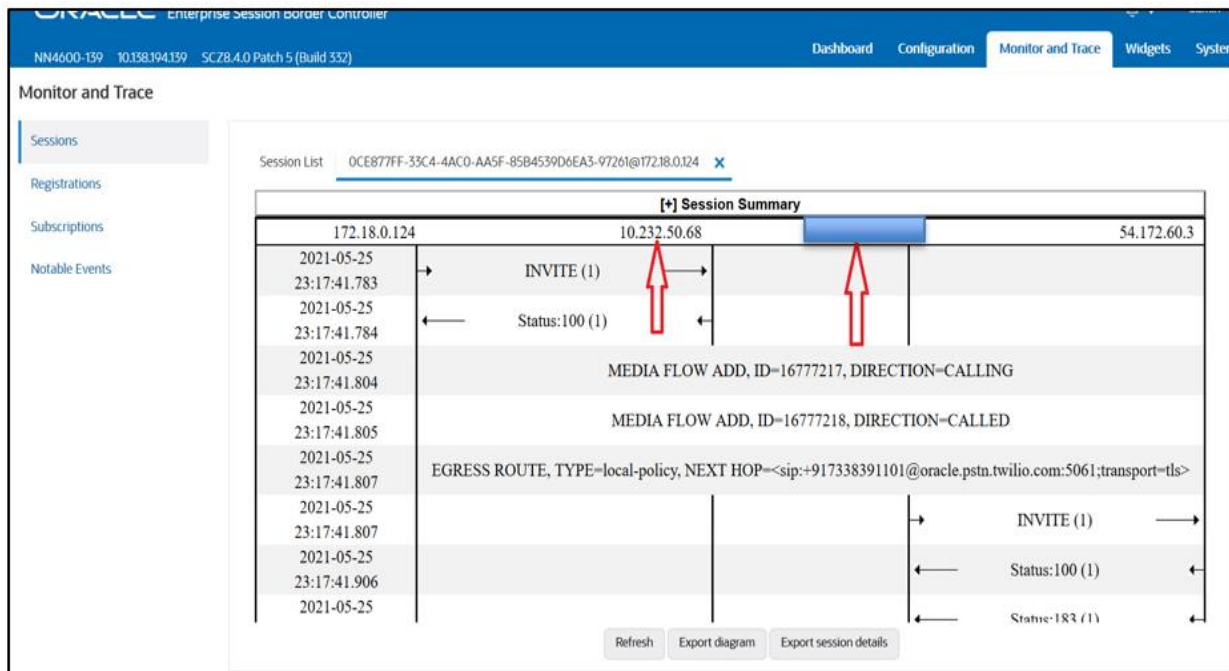
+ Number Filter Choose Action

NUMBER	FRIENDLY NAME	COUNTRY	EMERGENCY CALLING STATUS	EMERGENCY ADDRESS	<input type="checkbox"/>
+1 [redacted]		US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	<input type="checkbox"/>
+1 [redacted]		US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	<input type="checkbox"/>
+1 [redacted]		US	Disabled		<input type="checkbox"/>

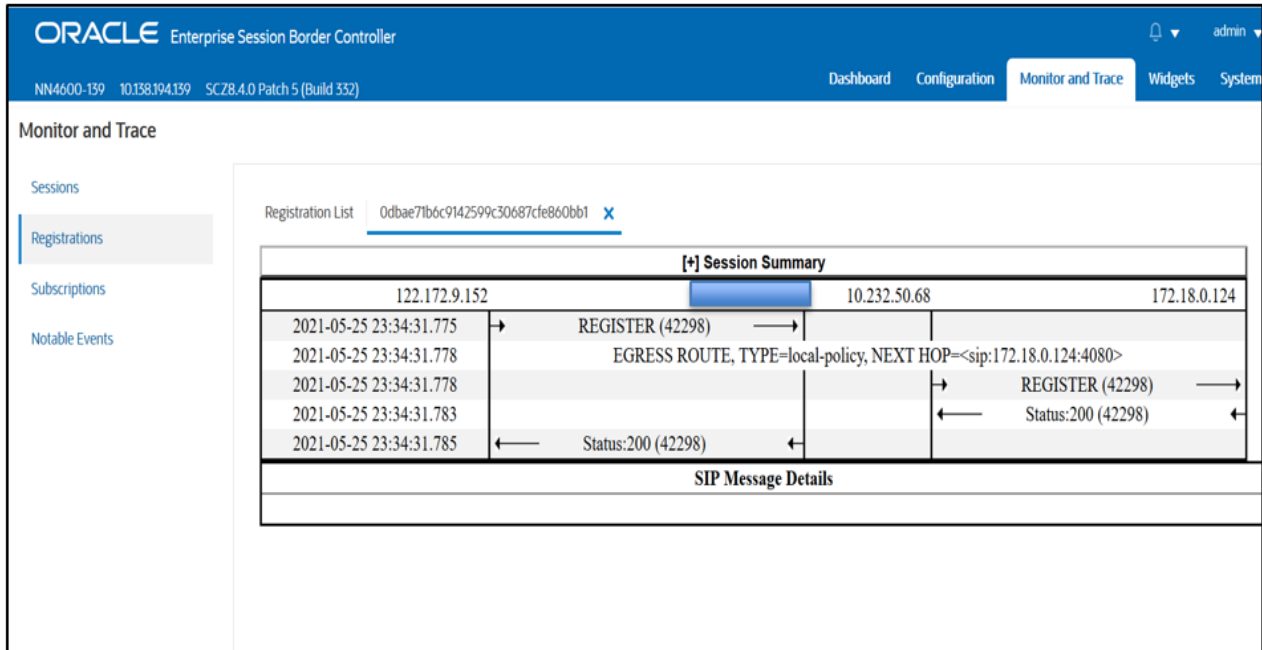
11. Verification of Sample Call flows

Once the configuration is complete, we can try making sample calls and can check the signaling path between Twilio Elastic Sip Trunk (PSTN Users) and Genesys Users

1. Make Call from Genesys user to the Twilio Elastic Sip Trunk and check the call flow. The calls flow from Genesys SIP Interface to Twilio Elastic SIP Trunking Interface and to Twilio Session Agent and the call reaches the PSTN user after that.



- When we register Genesys Remote Worker, we can see the registration happening through Oracle SBC to Pure Engage as given below.



ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

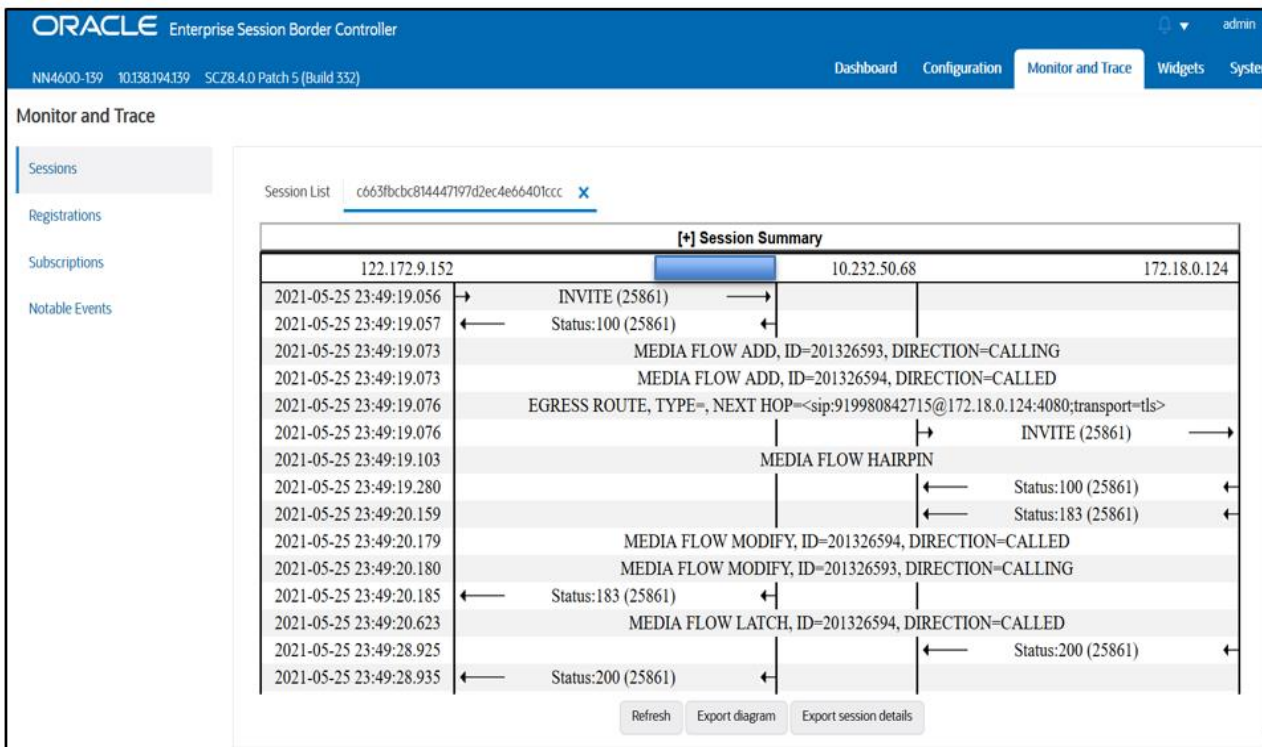
Monitor and Trace

Registration List [Odbae71b6c9142599c30687cfe860bb1](#)

[+] Session Summary			
122.172.9.152		10.232.50.68	172.18.0.124
2021-05-25 23:34:31.775	→	REGISTER (42298)	→
2021-05-25 23:34:31.778		EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:172.18.0.124:4080>	
2021-05-25 23:34:31.783			← REGISTER (42298) →
2021-05-25 23:34:31.785	←	Status:200 (42298)	←

SIP Message Details

- Make Call from Genesys Remote user to the Twilio Elastic Sip Trunk user and check the call flow. Now, there will be 2 call legs (hair pinned call) as the call reaches Genesys first and then reaches Twilio trunk user after that as given below.



ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Monitor and Trace

Session List [c63fbc814447197d2ec4e66401ccc](#)

[+] Session Summary			
122.172.9.152		10.232.50.68	172.18.0.124
2021-05-25 23:49:19.056	→	INVITE (25861)	→
2021-05-25 23:49:19.057	←	Status:100 (25861)	←
2021-05-25 23:49:19.073		MEDIA FLOW ADD, ID=201326593, DIRECTION=CALLING	
2021-05-25 23:49:19.076		MEDIA FLOW ADD, ID=201326594, DIRECTION=CALLED	
2021-05-25 23:49:19.076		EGRESS ROUTE, TYPE=, NEXT HOP=<sip:919980842715@172.18.0.124:4080;transport=tls>	
2021-05-25 23:49:19.103			← INVITE (25861) →
2021-05-25 23:49:19.280			← Status:100 (25861) ←
2021-05-25 23:49:20.159			← Status:183 (25861) ←
2021-05-25 23:49:20.179		MEDIA FLOW MODIFY, ID=201326594, DIRECTION=CALLED	
2021-05-25 23:49:20.180		MEDIA FLOW MODIFY, ID=201326593, DIRECTION=CALLING	
2021-05-25 23:49:20.185	←	Status:183 (25861)	←
2021-05-25 23:49:20.623		MEDIA FLOW LATCH, ID=201326594, DIRECTION=CALLED	
2021-05-25 23:49:28.925			← Status:200 (25861) ←
2021-05-25 23:49:28.935	←	Status:200 (25861)	←

Refresh Export diagram Export session details

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

NN4600-139 10.138.194.139 SC28.4.0 Patch 5 (Build 332)

Monitor and Trace

Sessions

Registrations

Subscriptions

Notable Events

Session List [OCE877FF-33C4-4AC0-AA5F-85B4539D6EA3-97647@172.18.0.124](#)

[+] Session Summary			
172.18.0.124	10.232.50.68		54.172.60.3
2021-05-25 23:49:19.085	→ INVITE (1)	→	
2021-05-25 23:49:19.086	← Status:100 (1)	←	
2021-05-25 23:49:19.102	MEDIA FLOW ADD, ID=218103809, DIRECTION=CALLING		
2021-05-25 23:49:19.103	MEDIA FLOW HAIRPIN		
2021-05-25 23:49:19.103	MEDIA FLOW ADD, ID=218103810, DIRECTION=CALLED		
2021-05-25 23:49:19.106	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=< sip:+919980842715@oracle.pstn.twilio.com:5061;transport=tlsv>		
2021-05-25 23:49:19.106		→ INVITE (1)	→
2021-05-25 23:49:19.207		← Status:100 (1)	←
2021-05-25 23:49:20.120		← Status:183 (1)	←
2021-05-25 23:49:20.145	MEDIA FLOW MODIFY, ID=218103810, DIRECTION=CALLED		
2021-05-25 23:49:20.146	MEDIA FLOW MODIFY, ID=218103809, DIRECTION=CALLING		
2021-05-25 23:49:20.152	← Status:183 (1)	←	
2021-05-25 23:49:28.909		← Status:200 (1)	←
2021-05-25 23:49:28.918	← Status:200 (1)	←	
2021-05-25 23:49:29.254	→ ACK (1)	→	
2021-05-25 23:49:29.258		→ ACK (1)	→
2021-05-25 23:50:07.371		← BYE (1)	←
2021-05-25 23:50:07.375	← BYE (1)	←	

Refresh Export diagram Export session details

- Make Call from the Twilio Elastic Sip Trunk to Genesys User and check the call flow. The calls flow from Twilio Elastic SIP Trunking Interface to Genesys SIP Interface and the call reaches the Genesys user after that.

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

NN4600-139 10.138.194.139 SC28.4.0 Patch 5 (Build 332)

Monitor and Trace

Sessions

Registrations

Subscriptions

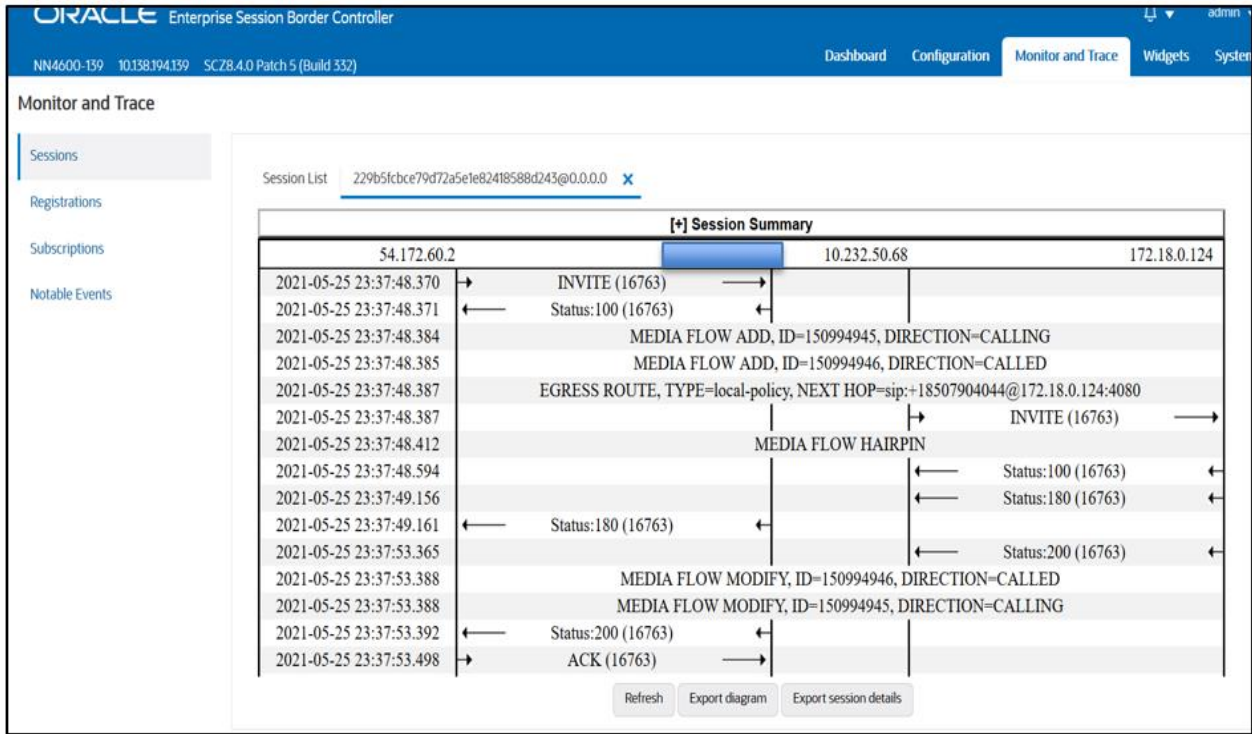
Notable Events

Session List [21bae2d99ee262ca3e17dcdee88da327@0.0.0.0](#)

[+] Session Summary			
54.172.60.2	10.232.50.68		172.18.0.124
2021-05-25 23:24:41.681	→ INVITE (347785)	→	
2021-05-25 23:24:41.681	← Status:100 (347785)	←	
2021-05-25 23:24:41.695	MEDIA FLOW ADD, ID=33554433, DIRECTION=CALLING		
2021-05-25 23:24:41.696	MEDIA FLOW ADD, ID=33554434, DIRECTION=CALLED		
2021-05-25 23:24:41.698	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:+17692105055@172.18.0.124:4080		
2021-05-25 23:24:41.698		→ INVITE (347785)	→
2021-05-25 23:24:41.748		← Status:180 (347785)	←
2021-05-25 23:24:41.752	← Status:180 (347785)	←	
2021-05-25 23:24:44.838		← Status:200 (347785)	←
2021-05-25 23:24:44.857	MEDIA FLOW MODIFY, ID=33554434, DIRECTION=CALLED		
2021-05-25 23:24:44.858	MEDIA FLOW MODIFY, ID=33554433, DIRECTION=CALLING		
2021-05-25 23:24:44.862	← Status:200 (347785)	←	
2021-05-25 23:24:44.967	→ ACK (347785)	→	
2021-05-25 23:24:44.970		→ ACK (347785)	→
2021-05-25 23:24:58.517	→ BYE (347786)	→	

Refresh Export diagram Export session details

- Make Call from Twilio Elastic Sip Trunk user to Genesys Remote user and check the call flow. Now, there will be 2 call legs (hair pinned call) as the call reaches Genesys first and then reaches Genesys Remote user after that as given below.



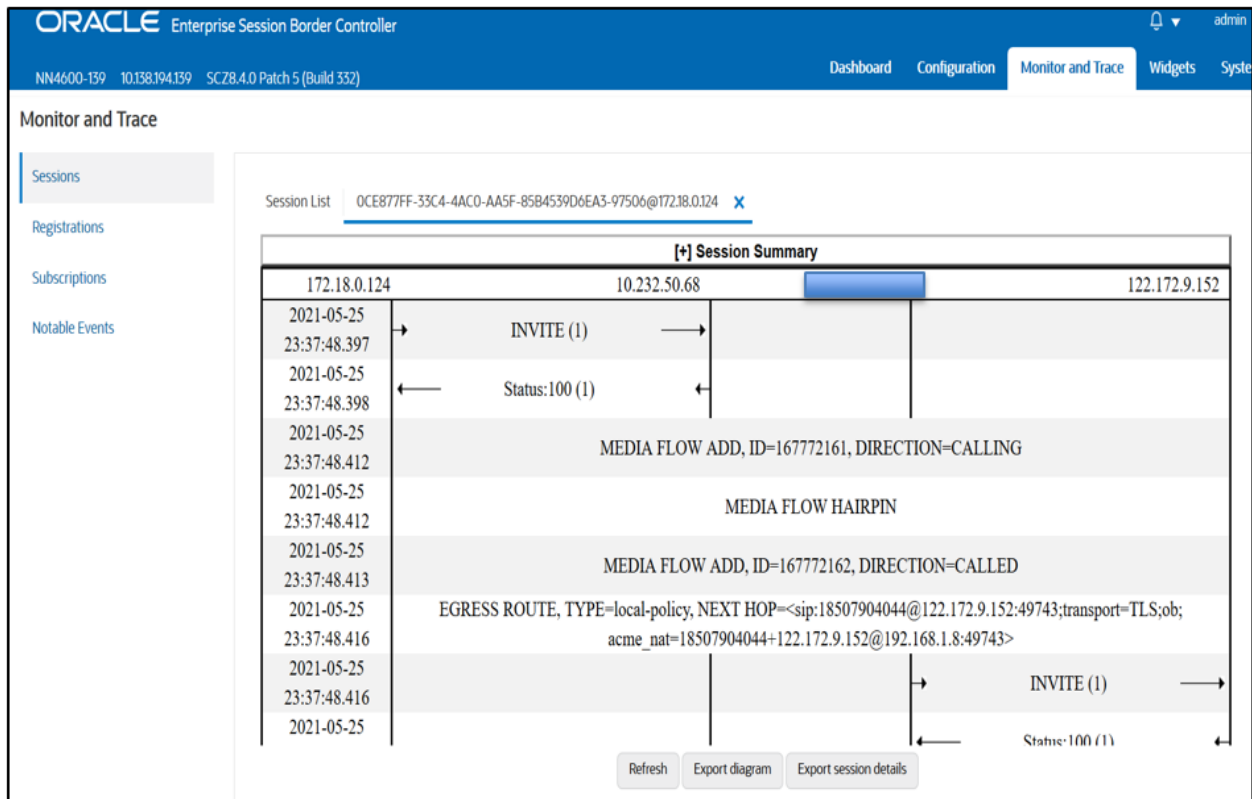
Oracle Enterprise Session Border Controller

Monitor and Trace

Session List: 229b5fcbce79d72a5e1e82418588d243@0.0.0.0

[+] Session Summary		
54.172.60.2	10.232.50.68	172.18.0.124
2021-05-25 23:37:48.370	→ INVITE (16763) →	
2021-05-25 23:37:48.371	← Status:100 (16763) ←	
2021-05-25 23:37:48.384	MEDIA FLOW ADD, ID=150994945, DIRECTION=CALLING	
2021-05-25 23:37:48.385	MEDIA FLOW ADD, ID=150994946, DIRECTION=CALLED	
2021-05-25 23:37:48.387	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:+18507904044@172.18.0.124:4080	
2021-05-25 23:37:48.387		→ INVITE (16763) →
2021-05-25 23:37:48.412	MEDIA FLOW HAIRPIN	
2021-05-25 23:37:48.594		← Status:100 (16763) ←
2021-05-25 23:37:49.156		← Status:180 (16763) ←
2021-05-25 23:37:49.161	← Status:180 (16763) ←	
2021-05-25 23:37:53.365		← Status:200 (16763) ←
2021-05-25 23:37:53.388	MEDIA FLOW MODIFY, ID=150994946, DIRECTION=CALLED	
2021-05-25 23:37:53.388	MEDIA FLOW MODIFY, ID=150994945, DIRECTION=CALLING	
2021-05-25 23:37:53.392	← Status:200 (16763) ←	
2021-05-25 23:37:53.498	→ ACK (16763) →	

Buttons: Refresh, Export diagram, Export session details



Oracle Enterprise Session Border Controller

Monitor and Trace

Session List: 0CE877FF-33C4-4AC0-AA5F-85B4539D6EA3-97506@172.18.0.124

[+] Session Summary		
172.18.0.124	10.232.50.68	122.172.9.152
2021-05-25 23:37:48.397	→ INVITE (1) →	
2021-05-25 23:37:48.398	← Status:100 (1) ←	
2021-05-25 23:37:48.412	MEDIA FLOW ADD, ID=167772161, DIRECTION=CALLING	
2021-05-25 23:37:48.412	MEDIA FLOW HAIRPIN	
2021-05-25 23:37:48.413	MEDIA FLOW ADD, ID=167772162, DIRECTION=CALLED	
2021-05-25 23:37:48.416	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:18507904044@122.172.9.152:49743;transport=TLS;ob;acme_nat=18507904044+122.172.9.152@192.168.1.8:49743>	
2021-05-25 23:37:48.416		→ INVITE (1) →
2021-05-25 23:37:48.416		← Status:100 (1) ←

Buttons: Refresh, Export diagram, Export session details

Appendix A





Following are the test cases that are executed between Genesys User with the Twilio Elastic SIP Trunk (PSTN user). **Please note that Genesys User here refers both Genesys User inside Enterprise network as well as Genesys Remote worker.**

Serial Number	Test Cases Executed	Result
1	Genesys user disconnects an inbound connected call	Pass
2	Genesys user disconnects an outbound connected call	Pass
3	Twilio Elastic SIP Trunk user disconnects an inbound connected call	Pass
4	Twilio Elastic SIP Trunk User disconnects an outbound connected call	Pass
5	Genesys user places inbound call from Twilio Elastic SIP Trunk user on hold and then resumes	Pass
6	Genesys user makes outbound call to Twilio Elastic SIP Trunk user and put that call on hold and then resumes	Pass
7	Twilio Elastic SIP Trunk user places inbound call from Genesys user on hold and then resumes	Pass
8	Twilio Elastic SIP Trunk user makes outbound call to Genesys user and put that call on hold and then resumes	Pass
9	Genesys user places inbound call from Twilio Elastic SIP Trunk user on hold for over 15/30 minutes and then resumes	Pass
10	Genesys user makes outbound call to Twilio Elastic SIP Trunk user and places the call on hold for over 15/30 minutes and then resumes	Pass
11	Inbound Twilio Elastic SIP Trunk call to Genesys blind transferred to second Genesys/ PSTN User	Pass
12	Outbound Twilio Elastic SIP Trunk call from Genesys user blind transferred to second Genesys/ PSTN User	Pass
13	Inbound Twilio Elastic SIP Trunk Call to Genesys consultatively transferred to Genesys/ PSTN User	Pass
14	Outbound Twilio Elastic SIP Trunk call from Genesys user consultatively transferred to Genesys/ PSTN User	Pass
15	Genesys user makes outbound call to Twilio Elastic SIP Trunk user and makes a conference call by adding another Genesys/ PSTN user.	Pass

16	Twilio Elastic SIP Trunk user makes outbound call to Genesys user and Genesys user makes a conference call by adding another Genesys/ PSTN user.	Pass
17	Genesys user mutes inbound call from Twilio Elastic SIP Trunk user and then unmutes	Pass
18	Genesys user mutes outbound call made to Twilio Elastic SIP Trunk user and then unmutes	Pass
19	Twilio Elastic SIP Trunk user mutes inbound call from Genesys user and then unmutes	Pass
20	Twilio Elastic SIP Trunk user mutes outbound call made to Genesys user and then unmutes	Pass
21	Twilio Elastic SIP Trunk User disconnects outbound call to Genesys user before it is answered	Pass
22	Genesys user disconnects outbound call to Twilio Elastic SIP Trunk user before it is answered	Pass

ORACLE

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