

ORACLE

Oracle SBC integration with Zoom Phone Premise Peering (BYOC) and Twilio Elastic Sip Trunking

Technical Application Note



Disclaimer

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

Revision History

Revision	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with Zoom BYOC and Twilio Elastic SIP Trunking	26 th April 2021
1.1	Added new section for SBC config/Deployment Using Configuration Assistant Updated the certificate related information for Zoom (using DigiCert G2 and G3 root certificate as their primary Root Certificate for TLS negotiation)	10 th November 2023

Table of Contents

1. INTENDED AUDIENCE	5
2. DOCUMENT OVERVIEW	5
2.1. TWILIO ELASTIC SIP TRUNKING	5
2.2. ZOOM BYOC	5
3. INTRODUCTION	6
3.1. AUDIENCE	6
3.2. REQUIREMENTS.....	6
3.3. ARCHITECTURE	7
4. ZOOM PHONE CONFIGURATION	8
4.1. CREATE A ZOOM USER.	8
4.2. ADD BYOC NUMBER	8
4.3. ASSIGN THE BYOC NUMBER TO A USER	9
5. INFRASTRUCTURE REQUIREMENTS.	10
THE TABLE BELOW SHOWS THE LIST OF INFRASTRUCTURE PREREQUISITES FOR DEPLOYING ZOOM PREMISE PEERING.	10
6. CONFIGURING THE SBC	11
6.1. VALIDATED ORACLE SBC VERSION	11
7. NEW SBC CONFIGURATION	11
7.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC	11
7.2. CONFIGURE SBC USING WEB GUI	16
7.3. CONFIGURE SYSTEM-CONFIG	18
7.4. CONFIGURE PHYSICAL INTERFACE VALUES	19
7.5. CONFIGURE NETWORK INTERFACE VALUES	20
7.6. ENABLE MEDIA MANAGER	22
7.7. CONFIGURE REALMS.....	23
7.8. ENABLE SIP-CONFIG	26
7.9. CONFIGURING A CERTIFICATE FOR SBC	27
7.10. TLS-PROFILE	34
7.11. CONFIGURE SIP INTERFACES.....	35
7.12. CONFIGURE SESSION-AGENT.....	36
7.13. CONFIGURE LOCAL-POLICY	38
7.14. CONFIGURE STEERING-POOL.....	40
7.15. CONFIGURE SIP-MANIPULATION	41
7.16. CONFIGURE CODEC POLICY	43
7.17. CONFIGURE SDES PROFILE	44
7.18. CONFIGURE MEDIA SECURITY PROFILE	44
8. NEW SBC CONFIG/DEPLOYMENT USING CONFIGURATION ASSISTANT	45
8.1. SECTION OVERVIEW AND REQUIREMENTS	45
8.2. INITIAL GUI ACCESS.....	45
8.3. CONFIGURATION ASSISTANT TEMPLATE NAVIGATION.....	48
8.3.1. PAGE 1-ZOOM PHONE NETWORK	48
8.3.2. PAGE 2- IMPORT DIGICERT TRUSTED CA CERTIFICATE FOR MS TEAMS SIDE.	48
8.3.3. PAGE 3 - SBC CERTIFICATES FOR ZOOM SIDE	49
8.3.4. PAGE 4 - ZOOM DESTINATION.....	50
8.3.5. PAGE 5 - ZOOM SIDE TRANSCODING	51

8.3.6. PAGE 6 - TWILIO ELASTIC SIP TRUNK NETWORK	51
8.3.7. PAGE 7 - TWILIO SESSION AGENT.....	52
8.3.8. PAGE 8 - TWILIO SIDE TRANSCODING.....	52
8.3.9. PAGE 9 - IMPORT DIGI CERT ROOT CA CERTIFICATE FOR TWILIO SIDE	53
8.3.10. PAGE 10 - SBC CERTIFICATES FOR TEAMS SIDE.....	53
8.4. REVIEW	53
8.5. DOWNLOAD AND/OR APPLY	55
8.6. CONFIGURATION ASSISTANT ACCESS	56
9. EXISTING SBC CONFIGURATION	56
10. TWILIO ELASTIC SIP TRUNKING CONFIGURATION.....	57
10.1. CREATE AM IP-ACL RULE	57
10.2. CREATE A NEW TRUNK	58
10.3. ASSOCIATE PHONE NUMBERS ON YOUR TRUNK.....	62
11. VERIFICATION OF SAMPLE CALL FLOWS.....	63
APPENDIX A	65

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 Zoom Phone- Premise Peering - BYOC.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Twilio Elastic Sip Trunk with Zoom BYOC. The solution contained within this document has been tested using Oracle Communication SBC with **OS 840p3B version**.

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

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. Zoom BYOC

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

<https://zoom.us/phonesystem>

<https://zoom.us/zoom-phone-features>

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 Zoom BYOC Model using Oracle Enterprise SBC. There will be steps that require navigating the Zoom configuration, Oracle SBC GUI interface. Understanding the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP, TLS/SRTP are also necessary to complete the configuration and for troubleshooting, if necessary.

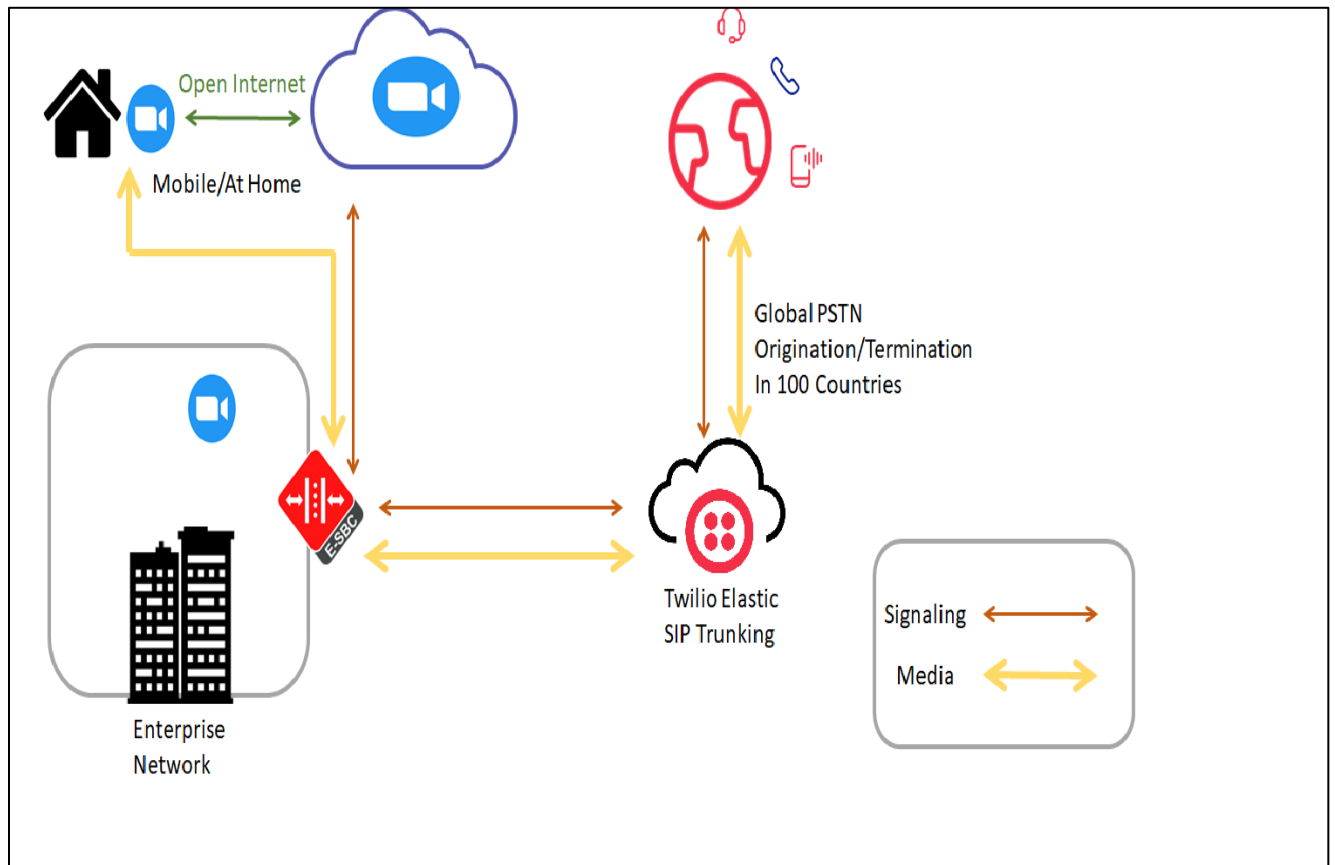
3.2. Requirements

- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version
- Zoom BYOC Model running Zoom Client.

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	Zoom Client version
Revision 1	8.4.0	Version: 5.2.0 (42619.0804)

3.3. Architecture



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

- Phase 1 – Configuring the Zoom Phone platform.
- Phase 2 – Configuring the Oracle SBC.
- Phase 3 – Configuring the Twilio Elastic SIP Trunk

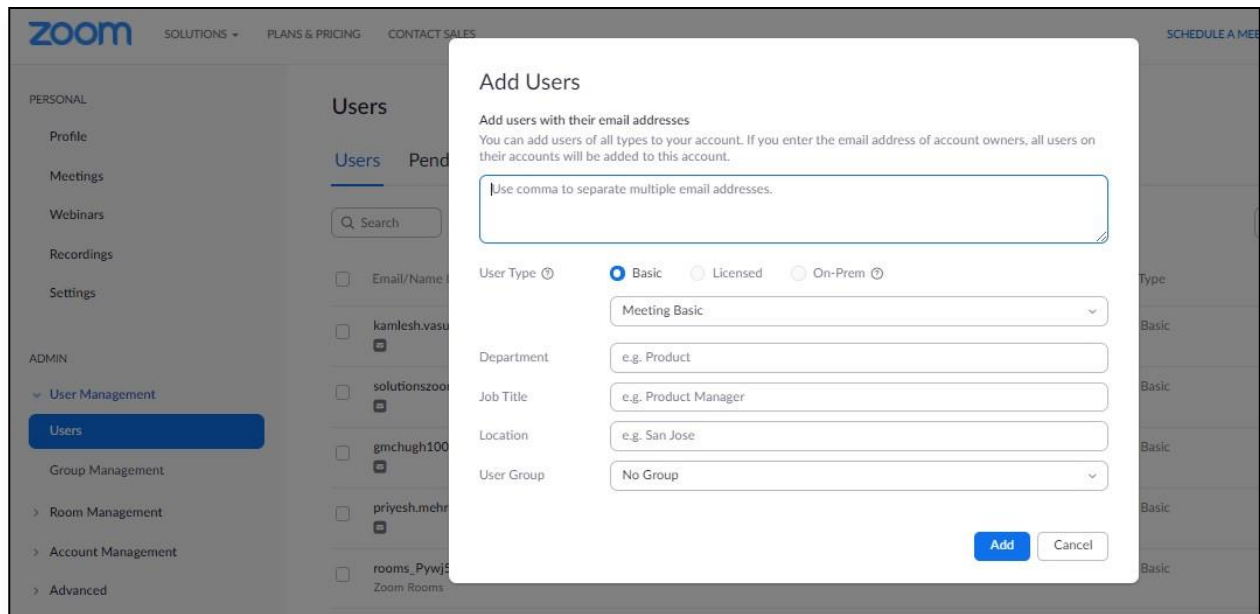
4. Zoom Phone configuration.

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

4.1. Create a Zoom User.

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

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

The image shows a screenshot of the Zoom Admin Portal interface. The main content area is titled 'Add Users'. It includes a search bar with the placeholder text 'Use comma to separate multiple email addresses.' Below this, there are several form fields: 'User Type' with radio buttons for 'Basic' (selected), 'Licensed', and 'On-Prem'; a dropdown menu for 'Meeting Basic'; 'Department' with the placeholder 'e.g. Product'; 'Job Title' with the placeholder 'e.g. Product Manager'; 'Location' with the placeholder 'e.g. San Jose'; and 'User Group' with a dropdown menu for 'No Group'. At the bottom right of the form are 'Add' and 'Cancel' buttons. The background shows the Zoom Admin Portal navigation menu with 'Users' selected under 'User Management'.

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

4.2. Add BYOC number

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

Select **Add** to add external phone numbers provided by Twilio Trunk into the Zoom portal.

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

Carrier –Choose BYOC

Numbers- Put the BYOC DID Number provided by Twilio Trunk.

SIP Group – Optional Parameter (Can be Left Blank) Acknowledge that the Phone Number belongs to your organization.

Click **Submit**.

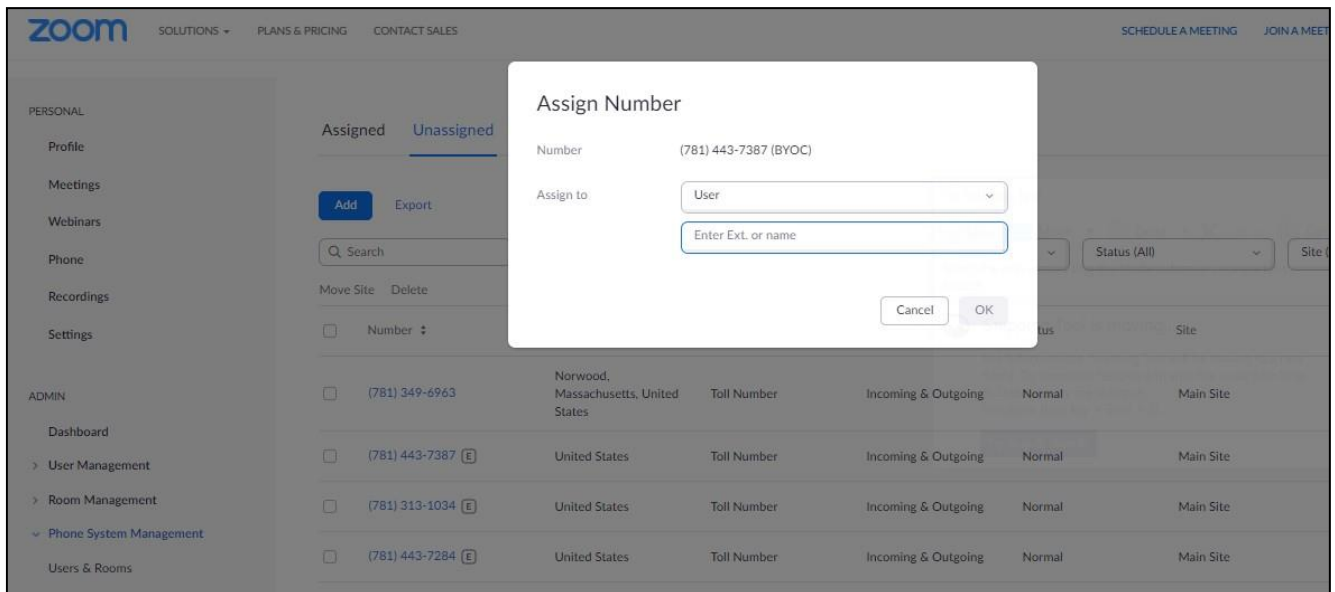
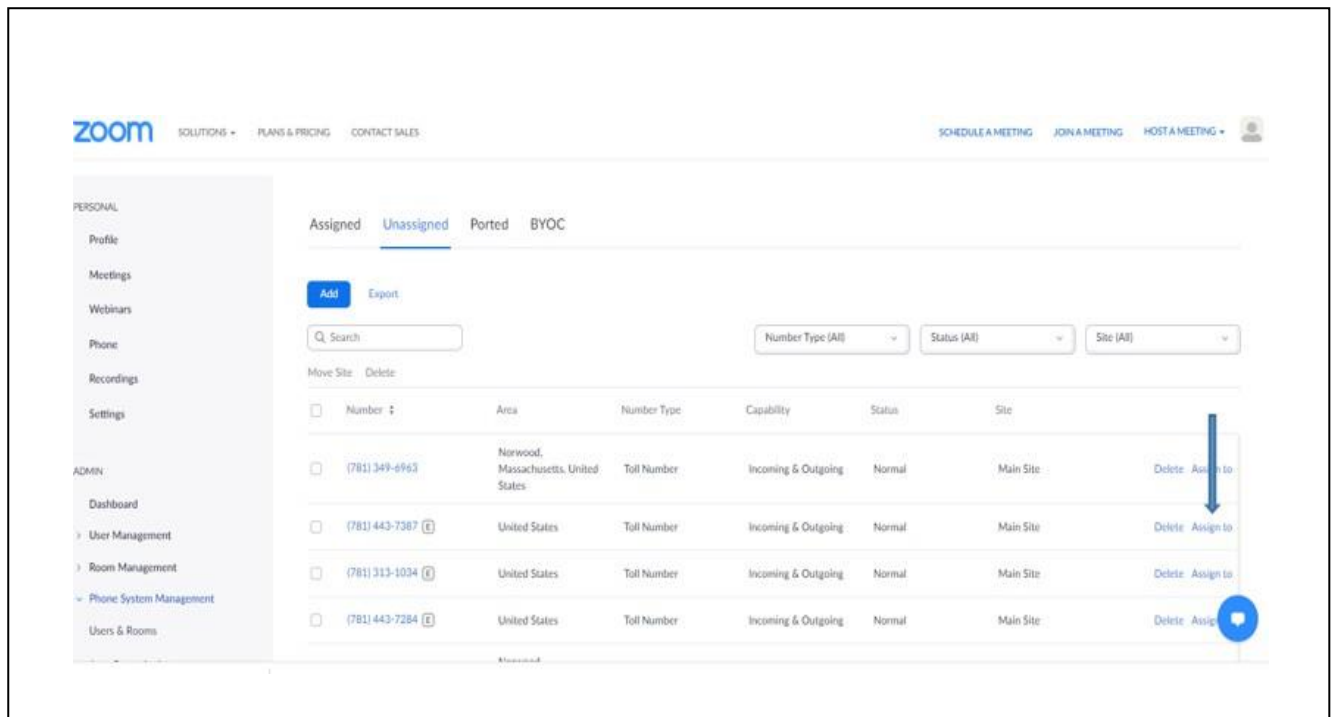
The screenshot shows the Zoom Admin Portal interface with a modal dialog box titled "Add BYOC Numbers". The dialog box contains the following fields and options:

- Site:** A dropdown menu with "Main Site" selected.
- Carrier:** A dropdown menu with "BYOC" selected.
- Numbers:** A text input field containing "7814437387".
- SIP Group (Optional):** A dropdown menu with "Select" selected, with the label "Choose a routing path for calls to/from the numbers" above it.
- Acknowledgment:** A checked checkbox with the text "I acknowledge that by checking the box, I attest that the phone numbers to be imported belong to me or my organization".
- Buttons:** "Cancel" and "Submit" buttons at the bottom right.

The background shows the Zoom Admin Portal navigation menu on the left and a table of assigned numbers in the center. The table has columns for "Number", "Site", "Carrier", and "BYOC".

4.3. Assign the BYOC number to a User

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



5. Infrastructure Requirements.

The table below shows the list of infrastructure prerequisites for deploying Zoom Premise Peering.

Session Border Controller (SBC)	See Zoom Documentation for More Details
SIP Trunks connected to the SBC	
Zoom Phone	
Public IP address for the SBC	
Public trusted certificate for the SBC	
Firewall ports for Zoom Voice signaling	
Firewall IP addresses and ports for Zoom Voice media	
Media Transport Profile	
Firewall ports for client media	

6. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Zoom BYOC and Twilio Elastic SIP Trunking. If the Oracle SBC being deployed is new, with no existing configuration, the simplest way to configure it to interface with Zoom Phone System is by utilizing the [Configuration Assistant](#) feature.

6.1. Validated Oracle SBC version

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

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

7. New SBC configuration

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

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

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

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

NN4600-139(configure)#
```

Note: There is no management IP configured by default.

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

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

```
NN4600-139#  
NN4600-139# setup product  
  
-----  
WARNING:  
Alteration of product alone or in conjunction with entitlement  
changes will not be complete until system reboot  
  
Last Modified 2020-04-30 22:38:15  
-----  
 1 : Product          : Enterprise Session Border Controller  
  
Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]: █
```

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

Save the changes and reboot the SBC.

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

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

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

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

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

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

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

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

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

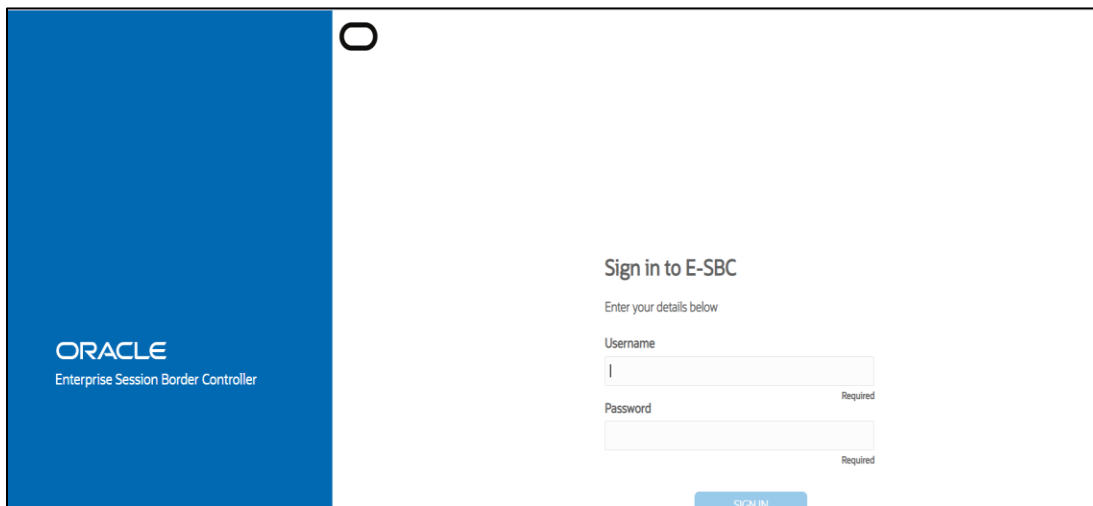
Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

```
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) # █
```

7.2. Configure SBC using Web GUI

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

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



ORACLE
Enterprise Session Border Controller

Sign in to E-SBC

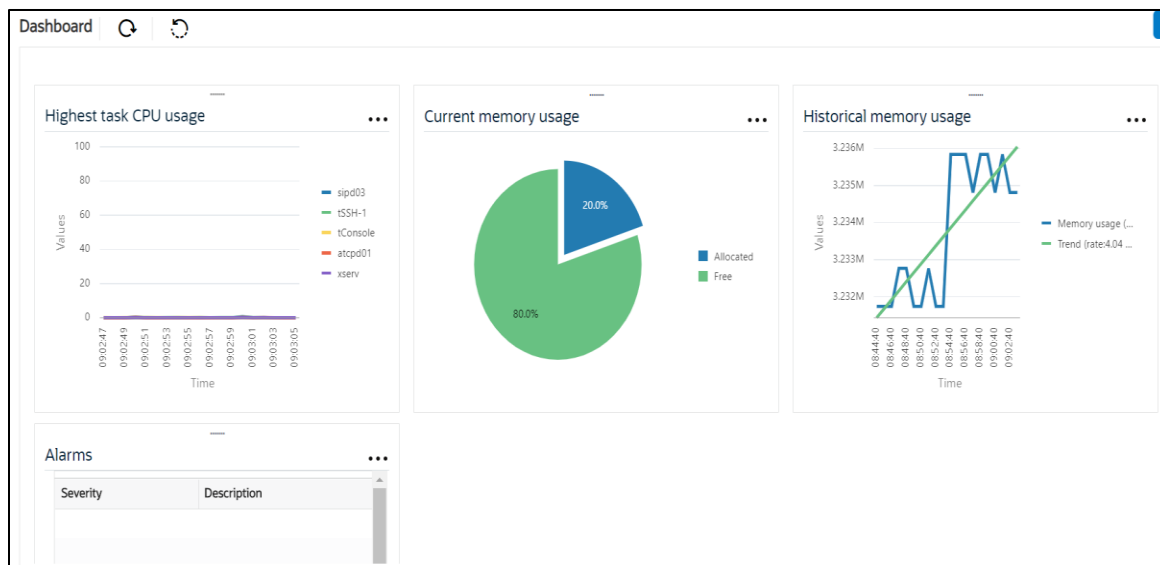
Enter your details below

Username Required

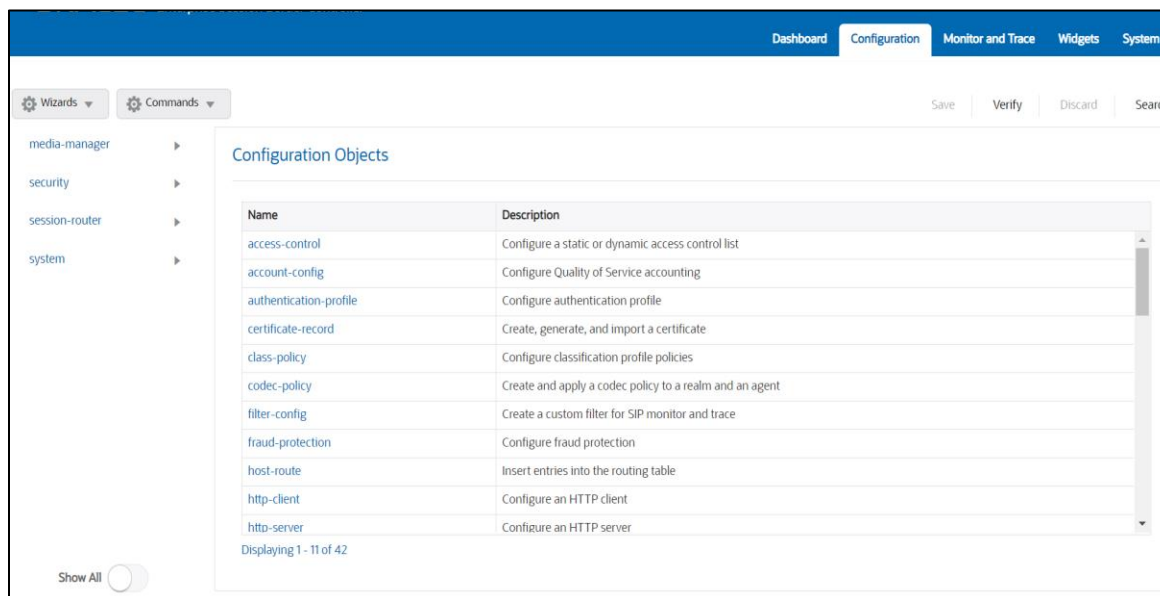
Password Required

SIGN IN

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.

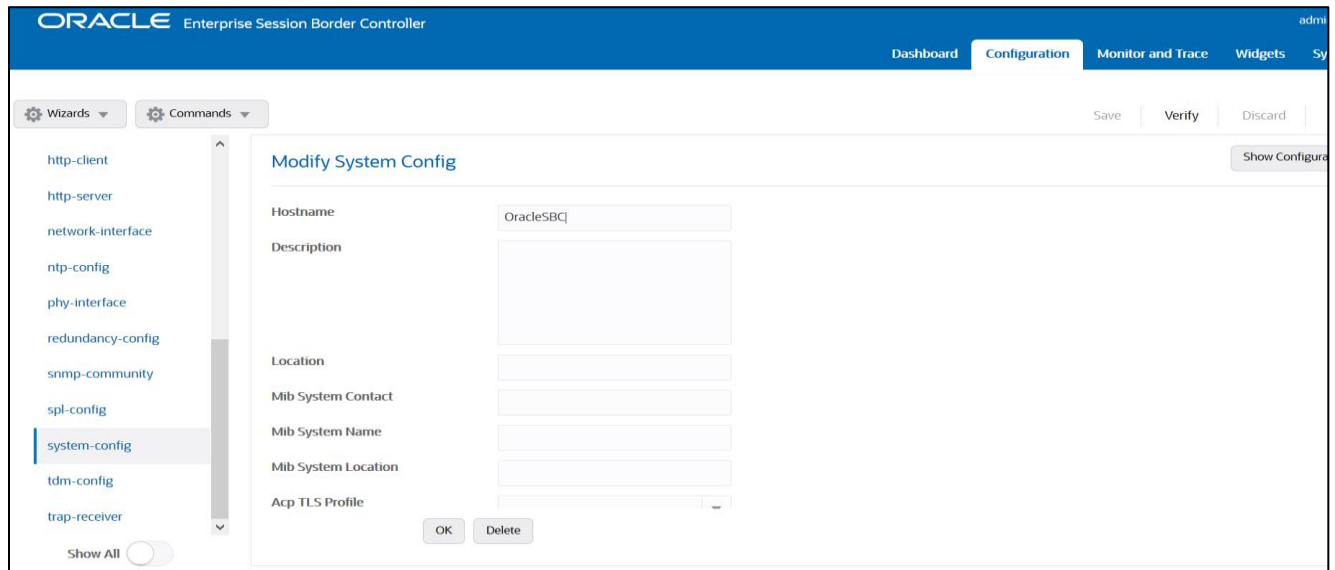
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf

The expert mode is used for configuration.

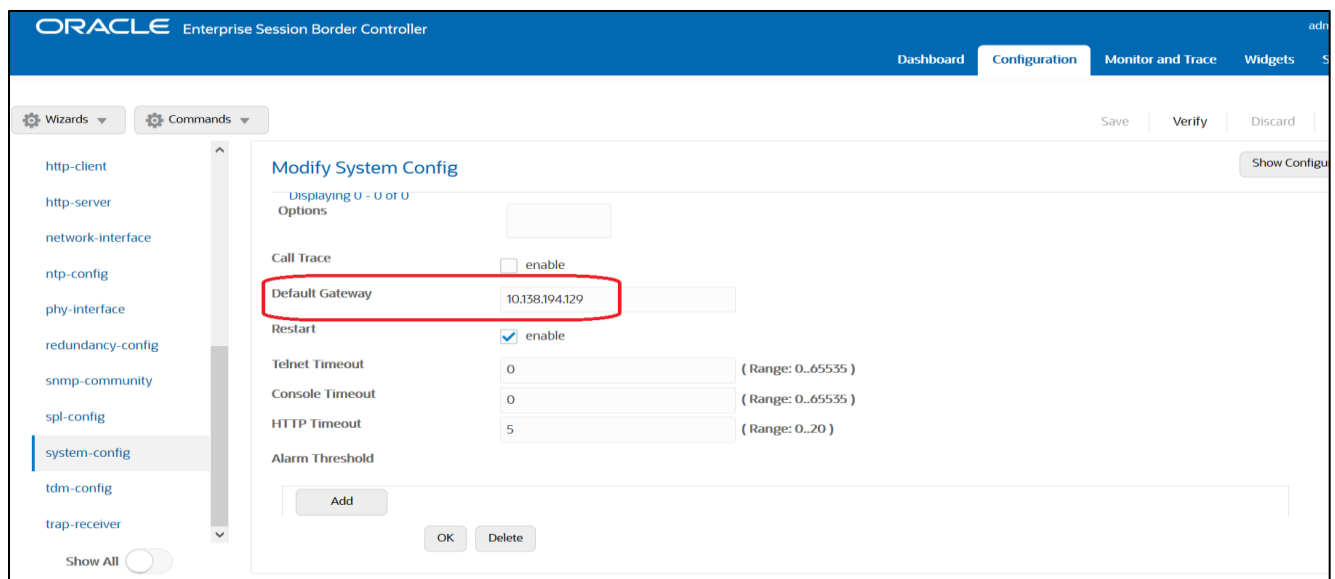
Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

7.3. Configure system-config

Go to system->system-config



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



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

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

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

7.4. Configure Physical Interface values

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

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

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

Please configure M00 interface as below.

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

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

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

Please configure M10 interface as below

7.5. 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	Zoom side network interface	Twilio side Network interface
Name	M00	M10
Host Name	customers.telechat.o-test06161977.com	
IP address	<input type="text"/>	155.212.214.102
Netmask	255.255.255.192	255.255.255.0
Gateway	<input type="text"/>	155.212.214.1

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', and 'Monitor and Trace'. The left sidebar lists various configuration categories, with 'network-interface' selected. The main content area is titled 'Add Network Interface' and contains the following fields:

- Name: M00
- Sub Port Id: 0 (Range: 0..4095)
- Description: (Empty text area)
- Hostname: customers.telechat.o-test061977.cor
- IP Address: (Empty text field)
- Pri Utility Addr: (Empty text field)
- Sec Utility Addr: (Empty text field)

Buttons for 'OK' and 'Back' are located at the bottom of the form. 'Save' and 'Verify' buttons are in the top right corner.

Similarly, configure network interface M10 as below

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

- Name: M10
- Sub Port Id: 0 (Range: 0..4095)
- Description: (Empty text area)
- Hostname: (Empty text field)
- IP Address: 155.212.214.102
- Pri Utility Addr: (Empty text field)
- Sec Utility Addr: (Empty text field)

Buttons for 'OK' and 'Back' are located at the bottom of the form. 'Save' and 'Verify' buttons are in the top right corner.

7.6. 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 'Configuration' tab is active, and the 'media-manager' configuration page is displayed. The 'State' checkbox is checked, indicating that the media manager is enabled. The following table lists the configuration parameters:

Parameter	Value	Range
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	

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, specifically the 'Media Policing' section of the 'media-manager' configuration page. The 'Media Policing' checkbox is checked, indicating that media policing is enabled. The following table lists the configuration parameters:

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

Red arrows point to the 'Max Untrusted Signaling' and 'Min Untrusted Signaling' fields, both of which are set to 1.

7.7. Configure Realms

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

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

Config Parameter	Zoom Side	Twilio Side
Identifier	Zoom	TwilioSipTrunk
Network Interface	M00	M10
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FQDN	Telechat.o-test06161977.com	
Media Sec policy	sdespolicy	sdespolicy
Access Control Trust Level	High	High
Codec-Policy	OptimizeCodecs	OptimizeCodecs

In the below case, Realm name is given as Zoom for Zoom 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 'Configuration' tab is active, and the 'realm-config' option is selected in the left-hand navigation menu. The 'Modify Realm Config' dialog is open, displaying the following configuration details:

- Identifier:** Zoom
- Description:** Realm for Zoom Cloud Voice
- Addr Prefix:** 0.0.0.0
- Network Interfaces:** M00:0
- Media Realm List:** (Empty field)
- Mm In Realm:** enable

Buttons for 'OK' and 'Back' are visible at the bottom of the dialog. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar lists various configuration categories like 'media-manager', 'codec-policy', 'media-policy', 'steering-pool', 'security', 'session-router', and 'system'.

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

Field Name	Value	Range
Average Rate Limit	0	(Range: 0..4294967295)
Access Control Trust Level	high	
Invalid Signal Threshold	0	(Range: 0..4294967295)
Maximum Signal Threshold	0	(Range: 0..4294967295)
Untrusted Signal Threshold	0	(Range: 0..4294967295)
Nat Trust Threshold	0	(Range: 0..65535)
Max Endpoints Per Nat	0	(Range: 0..65535)
Nat Invalid Message Threshold	0	(Range: 0..65535)
Wait Time For Invalid Register	0	(Range: 0,4..300)
Deny Period	30	(Range: 0..4294967295)

Buttons for 'OK' and 'Back' are located at the bottom of the form. A red arrow points to the 'Access Control Trust Level' dropdown menu.

Similarly, Realm name is given as TwilioSipTrunk for Twilio Elastic SIP Trunking side. Please set the Access Control Trust Level as high for this realm too.

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

Field Name	Value
Identifier	TwilioSipTrunk
Description	
Addr Prefix	0.0.0.0
Network Interfaces	M10:0.4 X
Media Realm List	
Mm In Realm	<input checked="" type="checkbox"/> enable

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

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace

Wizards Commands Save Verify

Add Realm Config

Out Translationid	<input type="text"/>	
In Manipulationid	<input type="text"/>	
Out Manipulationid	<input type="text"/>	
Average Rate Limit	<input type="text" value="0"/>	(Range: 0..4294967295)
Access Control Trust Level	<input type="text" value="high"/>	
Invalid Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Maximum Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Untrusted Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Nat Trust Threshold	<input type="text" value="0"/>	(Range: 0..65535)
Max Endpoints Per Host	<input type="text"/>	

OK Back

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

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

7.8. Enable sip-config

SIP config enables SIP handling in the SBC.

Make sure the home realm-id, registrar-domain and registrar-host are 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

For more info, please refer to SBC security guide given in the above section.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active. The left sidebar lists various configuration categories, with 'sip-config' selected. The main area displays the 'Modify SIP Config' form with the following fields:

State	<input checked="" type="checkbox"/> enable
Dialog Transparency	<input checked="" type="checkbox"/> enable
Home Realm ID	Zoom
Egress Realm ID	
Nat Mode	None
Registrar Domain	*
Registrar Host	*
Registrar Port	5060 (Range: 0,1025..65535)
Init Timer	500 (Range: 0..4294967295)

Buttons: OK, Delete

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, continuing from the previous one. The 'Configuration' tab is active. The left sidebar lists various configuration categories, with 'sip-config' selected. The main area displays the 'Modify SIP Config' form with the following fields:

Invite Expires	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 X
SPL Options	
SIP Message Len	0 (Range: 0..65535)
Enum Sag Match	<input type="checkbox"/> enable
Extra Method Stats	<input checked="" type="checkbox"/> enable

Buttons: OK, Delete

7.9. Configuring a certificate for SBC

This section describes how to configure the SBC for both TLS and SRTP communication with Zoom and Twilio Elastic SIP Trunking.

Zoom 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

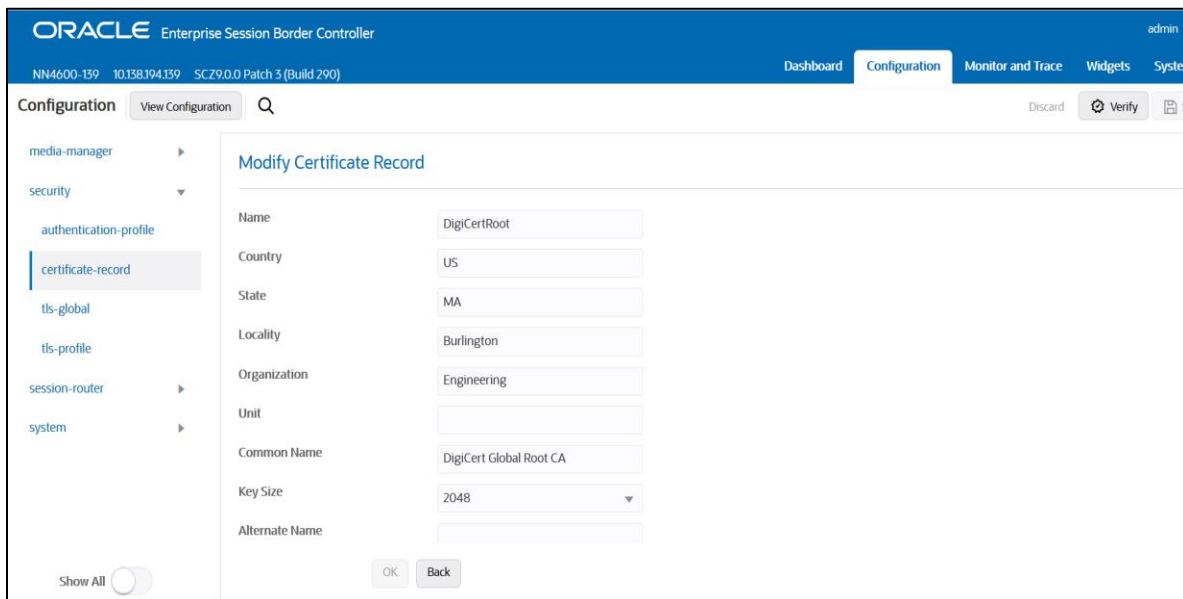
The following, DigiCert GlobalRootCA and DigiCert SHA2 Secure Server CA are the root and intermediate CA certificates used to sign the SBC's end entity certificate

To trust Zoom certificates, your SBC must have below DigiCert Global Root CA, DigiCert Global Root G2 and DigiCert Global Root G3 installed.

Note: Since both Oracle SBC and Zoom use DigiCert Global Root CA only one certificate record should be created for the DigiCert Global Root CA certificate.

Step 1 – Creating the certificate record

Go to security->Certificate Record and configure the SBC entity certificate for SBC as shown below. **We are creating this certificate for Zoom Side.** The certificate can be from any root which is supported by Zoom.



The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'admin', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the 'certificate-record' option is selected in the left-hand navigation menu. The main content area shows the 'Modify Certificate Record' form with the following fields:

Name	DigiCertRoot
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	
Common Name	DigiCert Global Root CA
Key Size	2048
Alternate Name	

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration page for 'Modify Certificate Record'. The interface includes a navigation menu on the left with categories like 'media-manager', 'security', 'authentication-profile', 'certificate-record', 'tls-global', 'tls-profile', 'session-router', and 'system'. The main configuration area contains the following fields:

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

Buttons for 'OK' and 'Back' are located at the bottom of the configuration area. A 'Show All' toggle is also present.

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

Config Parameter	Digicert Intermediate	DigiCert Root CA	DigiCertRootG2	DigiCertRootG3
Common Name	DigiCert SHA2 Secure Server CA	DigiCert Global Root CA	DigiCert Global RootG2	DigiCert Global RootG3
Key Size	2048	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignaturekey Encipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage list	serverAuth	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256	Sha256

Certificate Issuer Organization	Common Name or Certificate Name
Buypass AS-983163327	Buypass Class 2 Root CA
Buypass AS-983163327	Buypass Class 3 Root CA
Baltimore	Baltimore CyberTrust Root
Cybertrust, Inc	Cybertrust Global Root
DigiCert Inc	DigiCert Assured ID Root CA
DigiCert Inc	DigiCert Assured ID Root G2
DigiCert Inc	DigiCert Assured ID Root G3
DigiCert Inc	DigiCert Global Root CA
DigiCert Inc	DigiCert Global Root G2
DigiCert Inc	DigiCert Global Root G3
DigiCert Inc	DigiCert High Assurance EV Root CA
DigiCert Inc	DigiCert Trusted Root G4
GeoTrust Inc.	GeoTrust Global CA
GeoTrust Inc.	GeoTrust Primary Certification Authority
GeoTrust Inc.	GeoTrust Primary Certification Authority - G2
GeoTrust Inc.	GeoTrust Primary Certification Authority - G3
GeoTrust Inc.	GeoTrust Universal CA
GeoTrust Inc.	GeoTrust Universal CA 2
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G6
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G6
Thawte, Inc.	Thawte Primary Root CA
Thawte, Inc.	Thawte Primary Root CA - G2
Thawte, Inc.	Thawte Primary Root CA - G3
VeriSign, Inc.	VeriSign Class 1 Public Primary Certification Authority - G3

VeriSign, Inc.	VeriSign Class 2 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G4
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign, Inc.	VeriSign Universal Root Certification Authority
AffirmTrust	AffirmTrust Commercial
AffirmTrust	AffirmTrust Networking
AffirmTrust	AffirmTrust Premium
AffirmTrust	AffirmTrust Premium ECC
Entrust, Inc.	Entrust Root Certification Authority
Entrust, Inc.	Entrust Root Certification Authority - EC1
Entrust, Inc.	Entrust Root Certification Authority - G2
Entrust, Inc.	Entrust Root Certification Authority - G4
Entrust.net	Entrust.net Certification Authority (2048)
GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign nv-sa	GlobalSign Root CA
The GoDaddy Group, Inc.	Go Daddy Class 2 CA
GoDaddy.com, Inc.	Go Daddy Root Certificate Authority - G2
Starfield Technologies, Inc.	Starfield Class 2 CA
Starfield Technologies, Inc.	Starfield Root Certificate Authority - G2
QuoVadis Limited	QuoVadis Root CA 1 G3
QuoVadis Limited	QuoVadis Root CA 2
QuoVadis Limited	QuoVadis Root CA 2 G3
QuoVadis Limited	QuoVadis Root CA 3
QuoVadis Limited	QuoVadis Root CA 3 G3
QuoVadis Limited	QuoVadis Root Certification Authority
Comodo CA Limited	AAA Certificate Services

AddTrust AB	AddTrust Class 1 CA Root
AddTrust AB	AddTrust External CA Root
COMODO CA Limited	COMODO Certification Authority
COMODO CA Limited	COMODO ECC Certification Authority
COMODO CA Limited	COMODO RSA Certification Authority
The USERTRUST Network	USERTrust ECC Certification Authority
The USERTRUST Network	USERTrust RSA Certification Authority
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 2
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 3

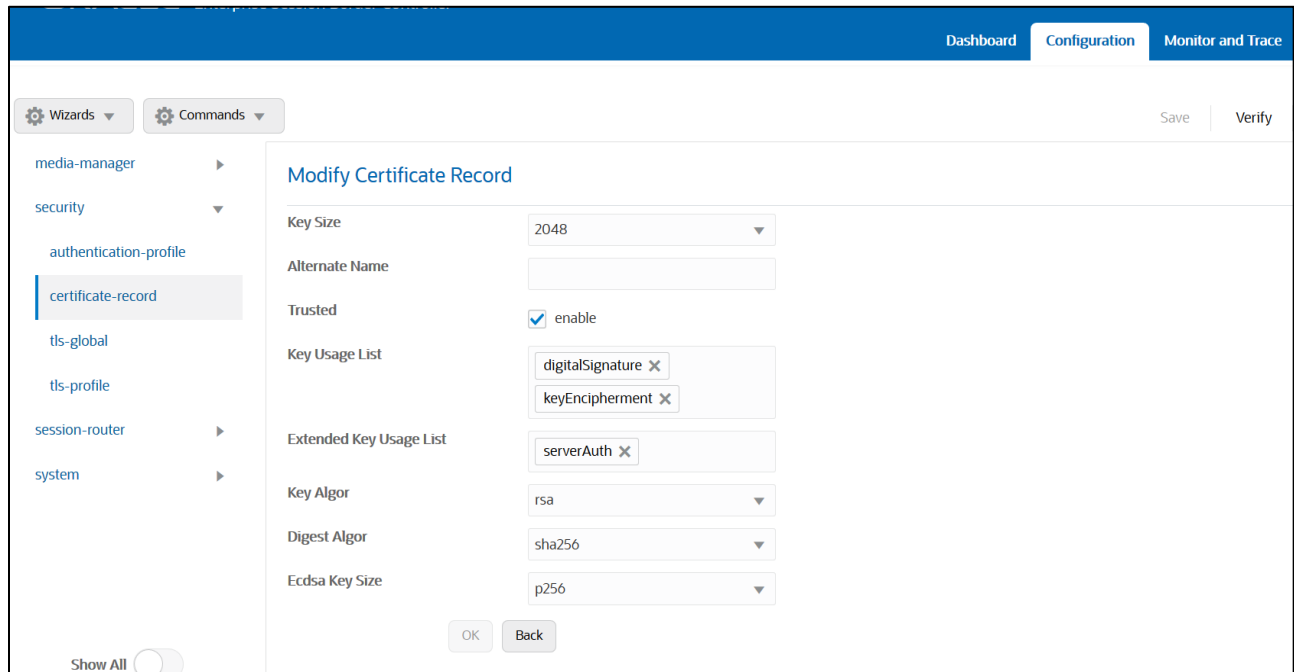
Similarly, Twilio Elastic SIP Trunking uses certificates from a CA (Certificate Authority) for establishing the TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It is important that you add the following root certificate to establish TLS connection from the link given below:

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar shows a tree view with 'certificate-record' selected. The main content area is titled 'Modify Certificate Record' and contains the following fields:

- Name: TwilioRootCACertChain
- Country: US
- State: MA
- Locality: Burlington
- Organization: Engineering
- Unit: Solutions
- Common Name: Chain CA Cert
- Key Size: 2048
- Alternate Name: (empty)

Buttons for 'OK' and 'Back' are located at the bottom of the form. 'Save' and 'Verify' buttons are also present in the top right corner of the configuration area.



Step 2 – Generating a certificate signing request

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

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

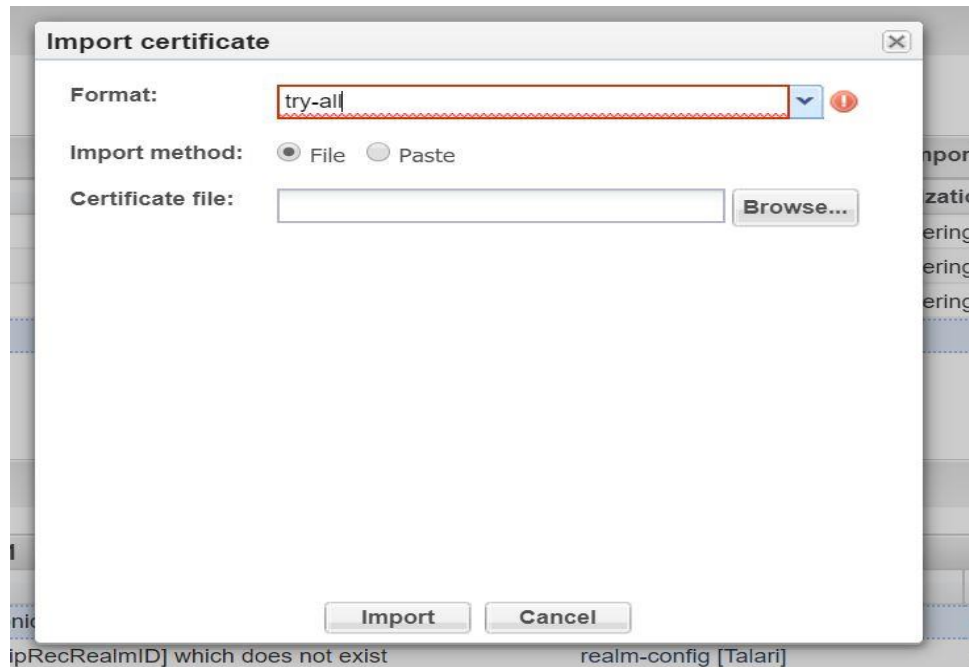
- Select the certificate and generate certificate on clicking the “Generate” command.
- Please copy/paste the text that gets printed on the screen as shown below and upload to your CA server for signature.



- Also, note that a save/activate is required

Step 3 – Deploy SBC & root certificates

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



Repeat these steps to import all the root and intermediate CA certificates into the SBC for Zoom Side:

- DigiCertIntermediate
- DigiCertGlobalRootCA
- DigiCertGlobalRootG2
- DigiCertGlobalRootG3

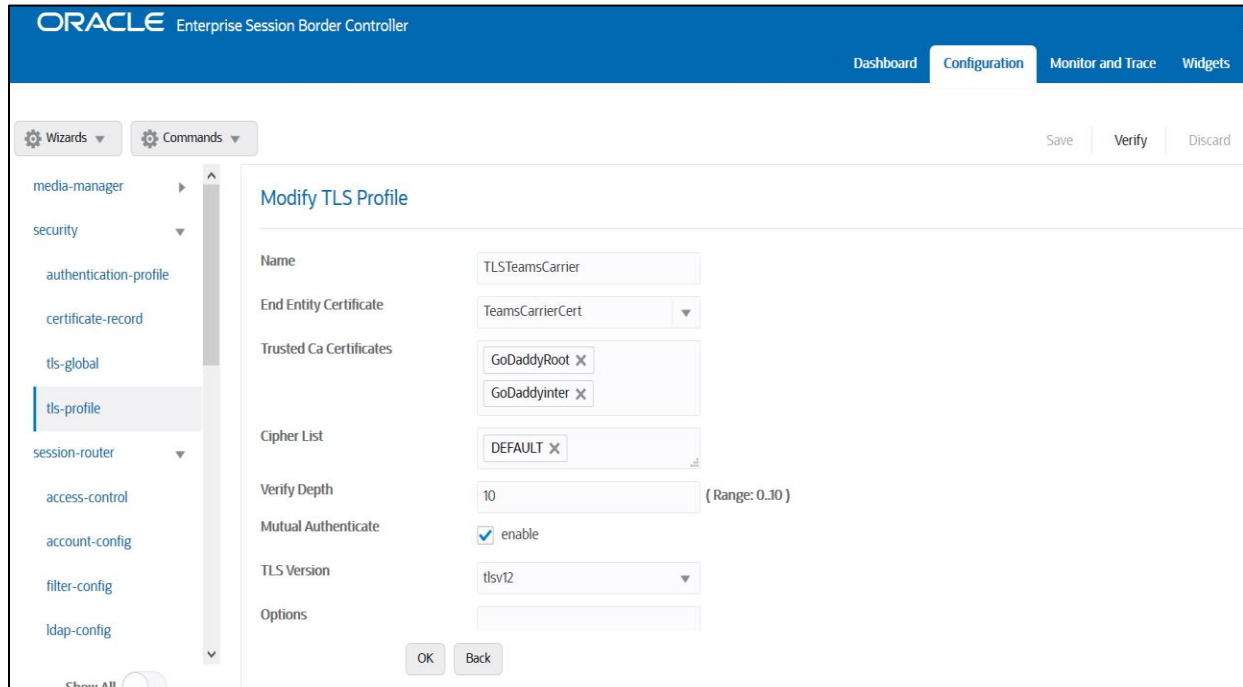
At this stage all the required certificates have been imported to the SBC for Zoom and the Twilio Elastic SIP Trunk.

7.10. 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 Zoom side.

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

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

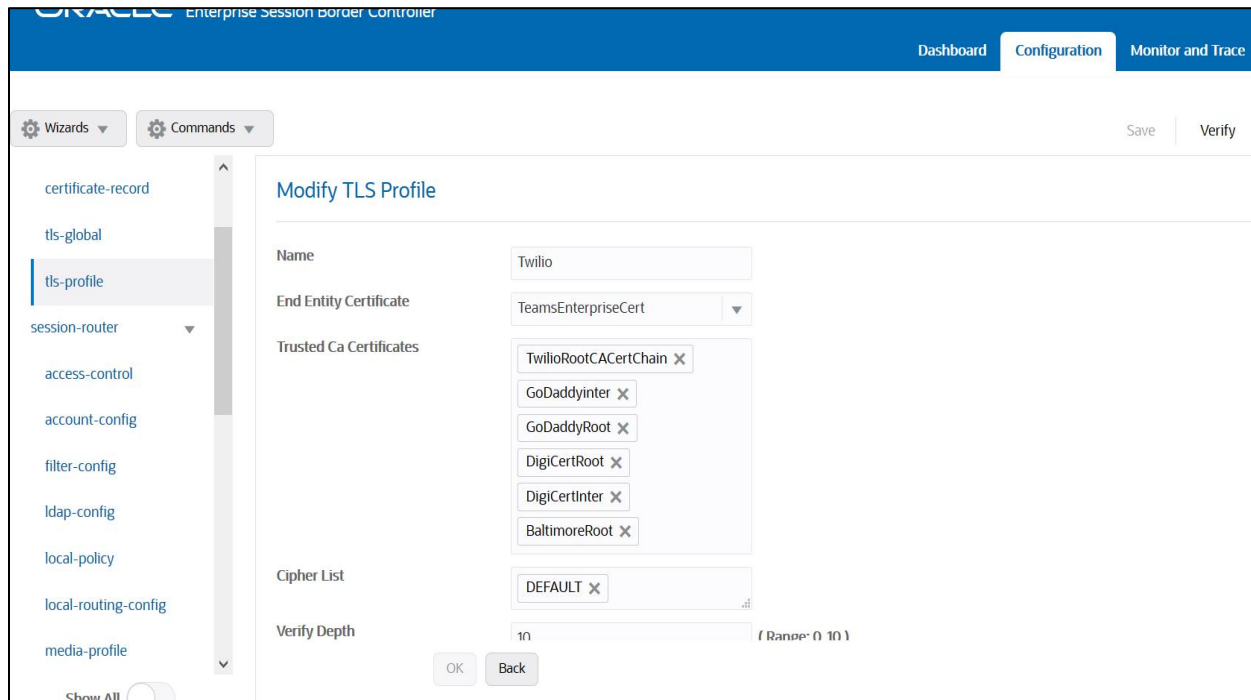


The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar shows a tree view with 'security' expanded to 'tls-profile'. The main content area is titled 'Modify TLS Profile' and contains the following fields:

Name	TLSTeamsCarrier
End Entity Certificate	TeamsCarrierCert
Trusted Ca Certificates	GoDaddyRoot X GoDaddyinter X
Cipher List	DEFAULT X
Verify Depth	10 (Range: 0-10)
Mutual Authenticate	<input checked="" type="checkbox"/> enable
TLS Version	tlsv12
Options	

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

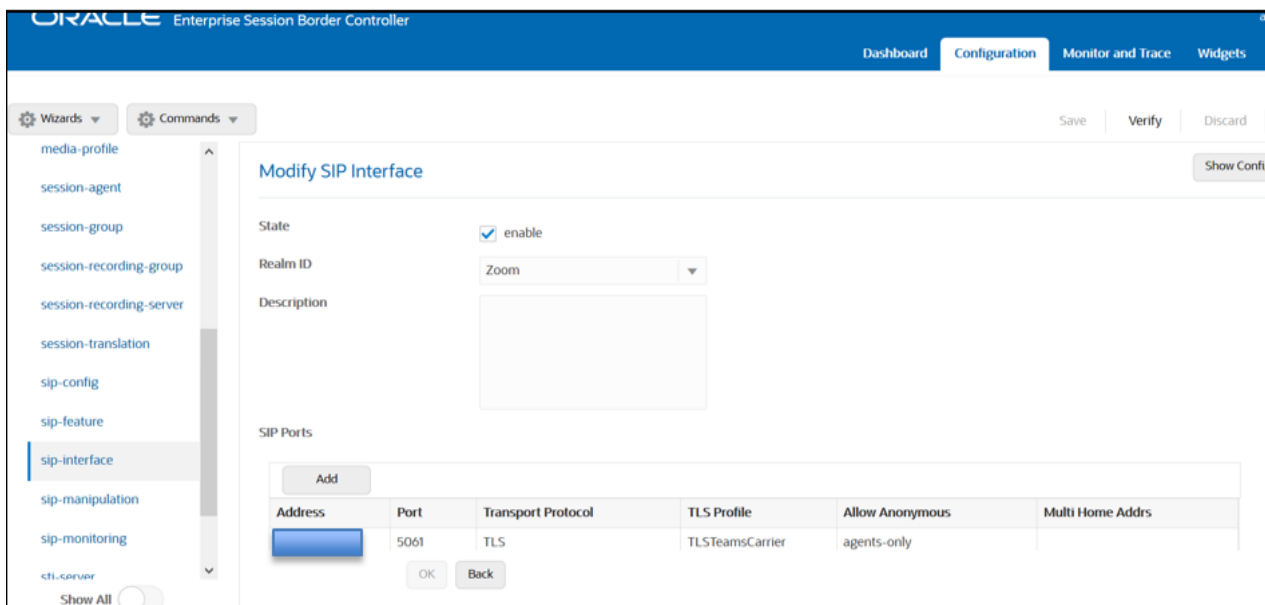
Similarly, configure the TLS profile shown below for the Twilio Elastic SIP Trunk side:



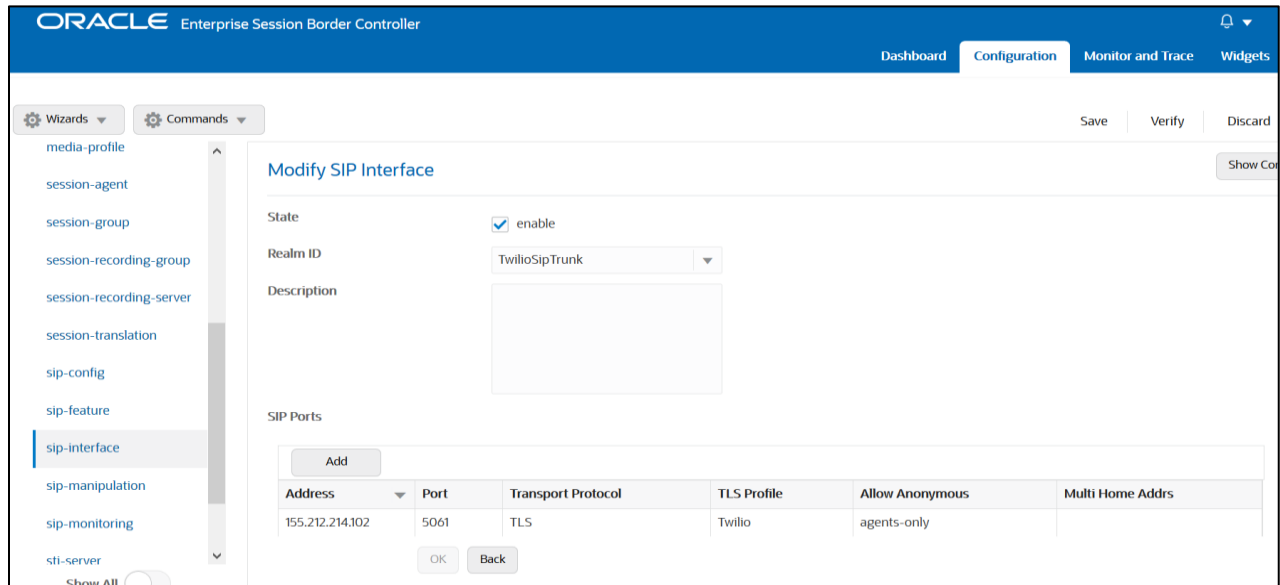
7.11. Configure SIP Interfaces

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

- 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. Below is the sip-interface Configured for Zoom side.



Similarly, Configure sip-interface for the Twilio Elastic SIP Trunk side as below:



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

7.12. 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.

Configure the session-agent for Zoom with the following parameters.
Go to session-router->Session-Agent.

- hostname and IP address as “ 162.12.232.59”
- port 5061
- realm-id – needs to match the realm created for Zoom
- transport set to “StaticTLS”
- ping-method –OPTIONS message
- ping-interval to 30 secs
-

The screenshot shows the Oracle Enterprise Session Border Controller 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 'Modify Session Agent' and contains the following fields:

- Hostname: 162.12.232.59
- IP Address: 162.12.232.59
- Port: 5061 (Range: 0,1025..65535)
- State: enable
- App Protocol: SIP
- App Type: (empty dropdown)
- Transport Method: StaticTLS
- Realm ID: Zoom
- Egress Realm ID: (empty dropdown)

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

Similarly, configure the session-agents for the Twilio Elastic SIP Trunk as below

- 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 shows the Oracle Enterprise Session Border Controller 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 'Modify Session Agent' and contains the following fields:

- Hostname: oracle.pstn.twilio.com
- IP Address: (empty)
- Port: 5061 (Range: 0,1025..65535)
- State: enable
- App Protocol: SIP
- App Type: (empty dropdown)
- Transport Method: StaticTLS
- Realm ID: TwilioSipTrunk
- Egress Realm ID: (empty dropdown)

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

****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](#)

7.13. Configure local-policy

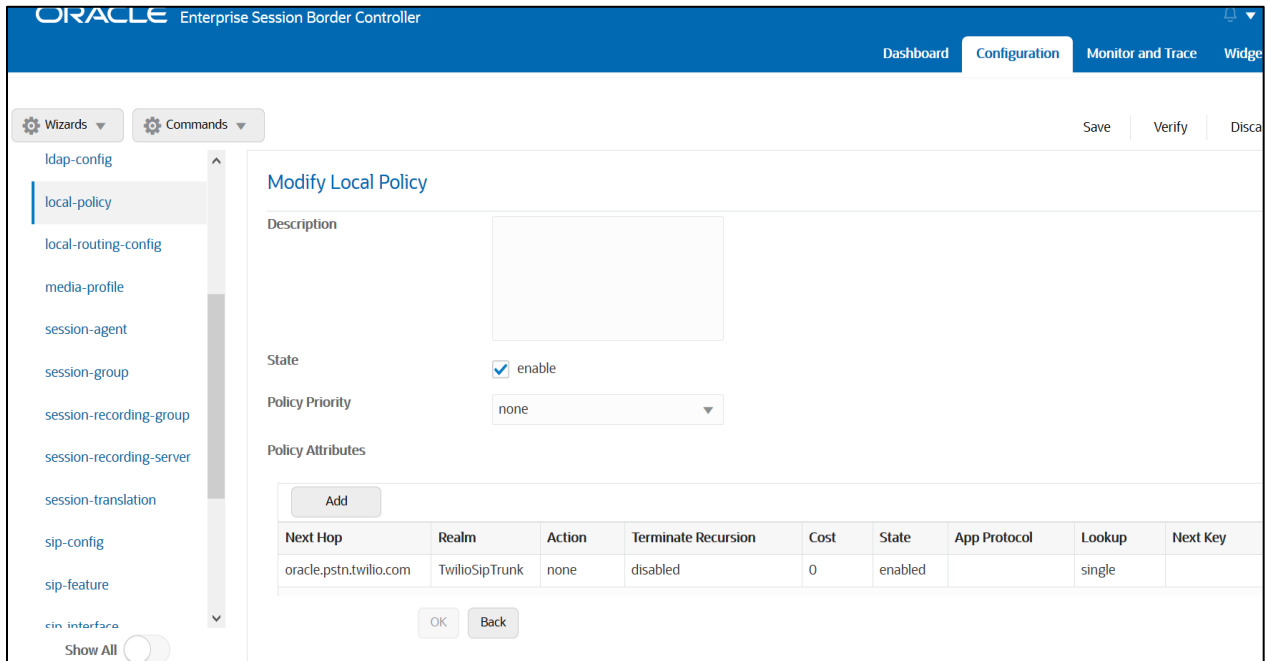
Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

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

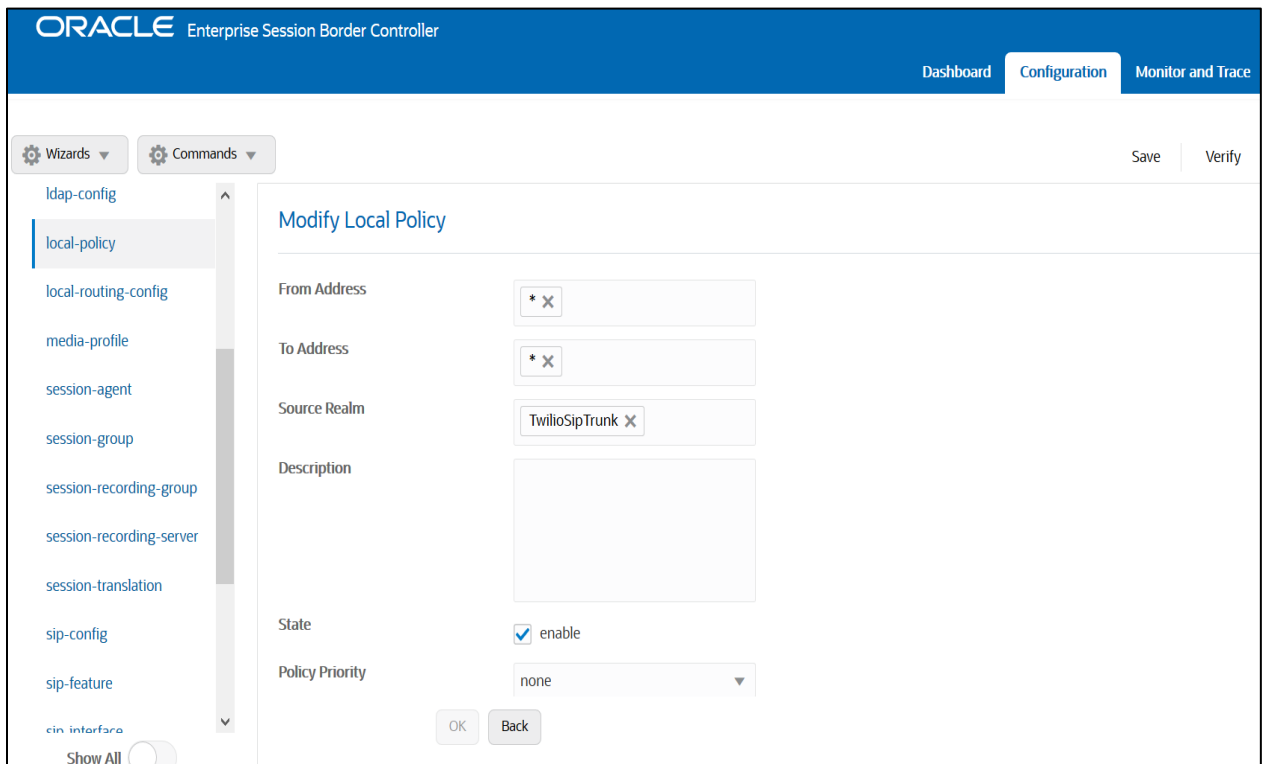
The screenshot displays the Oracle Enterprise Session Border Controller (SBC) configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar shows a tree view of configuration options, with 'local-policy' selected under the 'session-router' category. The main content area is titled 'Modify Local Policy' and contains the following fields:

- From Address:** A text input field with a placeholder '* x'.
- To Address:** A text input field with a placeholder '* x'.
- Source Realm:** A dropdown menu with 'Zoom' selected.
- Description:** A large empty text area.
- State:** A checkbox labeled 'enable' which is checked.
- Policy Priority:** A dropdown menu with 'none' selected.

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



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



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:

- Description:** A large empty text area.
- State:** A checkbox labeled 'enable' which is checked.
- Policy Priority:** A dropdown menu currently set to 'none'.
- Policy Attributes:** A table with an 'Add' button above it. The table has the following columns: Next Hop, Realm, Action, Terminate Recursion, Cost, State, App Protocol, Lookup, and Next Key. One row is visible with the following values: Next Hop: 162.12.232.59, Realm: Zoom, Action: none, Terminate Recursion: disabled, Cost: 0, State: enabled, App Protocol: (empty), Lookup: single, Next Key: (empty).

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

7.14. Configure steering-pool

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

Zoom side steering pool.

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

- IP Address:** A text input field with a blue highlight.
- Start Port:** A text input field containing '10000' with a range indicator '(Range: 1.65535)'.
- End Port:** A text input field containing '19999' with a range indicator '(Range: 1.65535)'.
- Realm ID:** A dropdown menu currently set to 'Zoom'.
- Network Interface:** A dropdown menu.

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

Twilio side steering pool.

The screenshot displays 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 'steering-pool' selected. The main content area is titled 'Add Steering Pool' and contains the following fields:

IP Address	<input type="text" value="155.212.214.102"/>
Start Port	<input type="text" value="20000"/> (Range: 1.65535)
End Port	<input type="text" value="29999"/> (Range: 1.65535)
Realm ID	<input type="text" value="TwilioSipTrunk"/>
Network Interface	<input type="text"/>

At the bottom of the form are 'OK' and 'Back' buttons. The interface also includes 'Wizards' and 'Commands' tabs, and 'Save' and 'Verify' buttons in the top right corner.

7.15. Configure sip-manipulation

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

Ping Response:

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

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace

Wizards Commands Save Verify

Modify Session Agent

Hostname: 162.12.232.59
IP Address: 162.12.232.59
Port: 5061 (Range: 0,1025..65535)
State: enable
App Protocol: SIP
App Type:
Transport Method: StaticTLS
Realm ID: Zoom
Egress Realm ID:
OK Back

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System admin

Wizards Commands Save Verify Discard Show Configuration

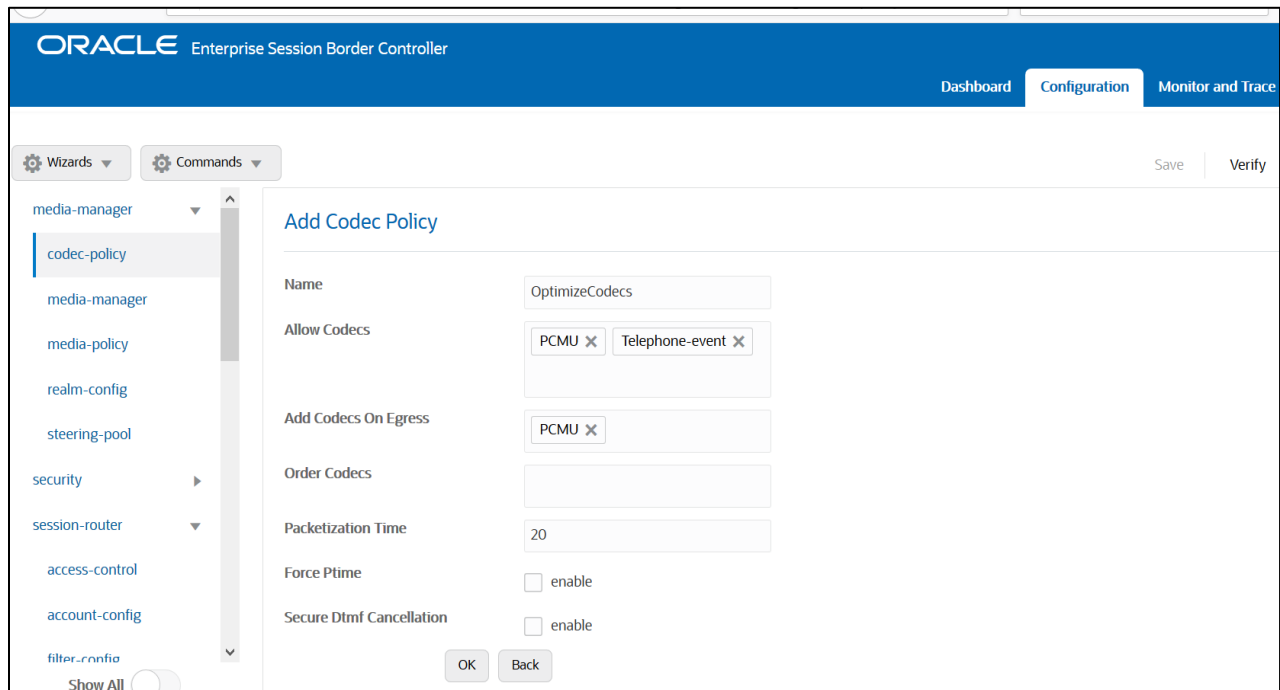
Modify Session Agent

Out Translationid:
Trust Me: enable
Local Response Map:
Ping Response: enable
In Manipulationid:
Out Manipulationid:
Manipulation String:
Manipulation Pattern:
Trunk Group:
Max Register Sustain Rate: 0 (Range: 0.999999999)
OK Back

7.16. Configure Codec Policy

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

Note: this is an optional config – configure codec policy only if deemed required
Go to media manager ----- codec policy



The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar shows a tree view with 'media-manager' selected, and 'codec-policy' highlighted. The main content area is titled 'Add Codec Policy' and contains the following fields:

- Name: OptimizeCodecs
- Allow Codecs: PCMU x Telephone-event x
- Add Codecs On Egress: PCMU x
- Order Codecs: (empty field)
- Packetization Time: 20
- Force Ptime: enable
- Secure Dtmf Cancellation: enable

Buttons for 'OK' and 'Back' are located at the bottom of the form. 'Save' and 'Verify' buttons are visible in the top right corner of the configuration area.

Assign this codec policy to both the Zoom and Twilio Realm.

7.17. 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)

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

7.18. 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 both the Zoom and Twilio Realm as they both 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: SDES
- Pass Through: enable
- Options: (empty)
- Inbound:
 - Profile: SDES
 - Mode: srtp
 - Protocol: sdes
 - Hide Egress Media Update: enable
- Outbound: (empty)

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

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 Zoom BYOC 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 access to Zoom supported CA to sign certificate once CSR is generated by the SBC. For Twilio side, list of supported CA's can be found [here](#)

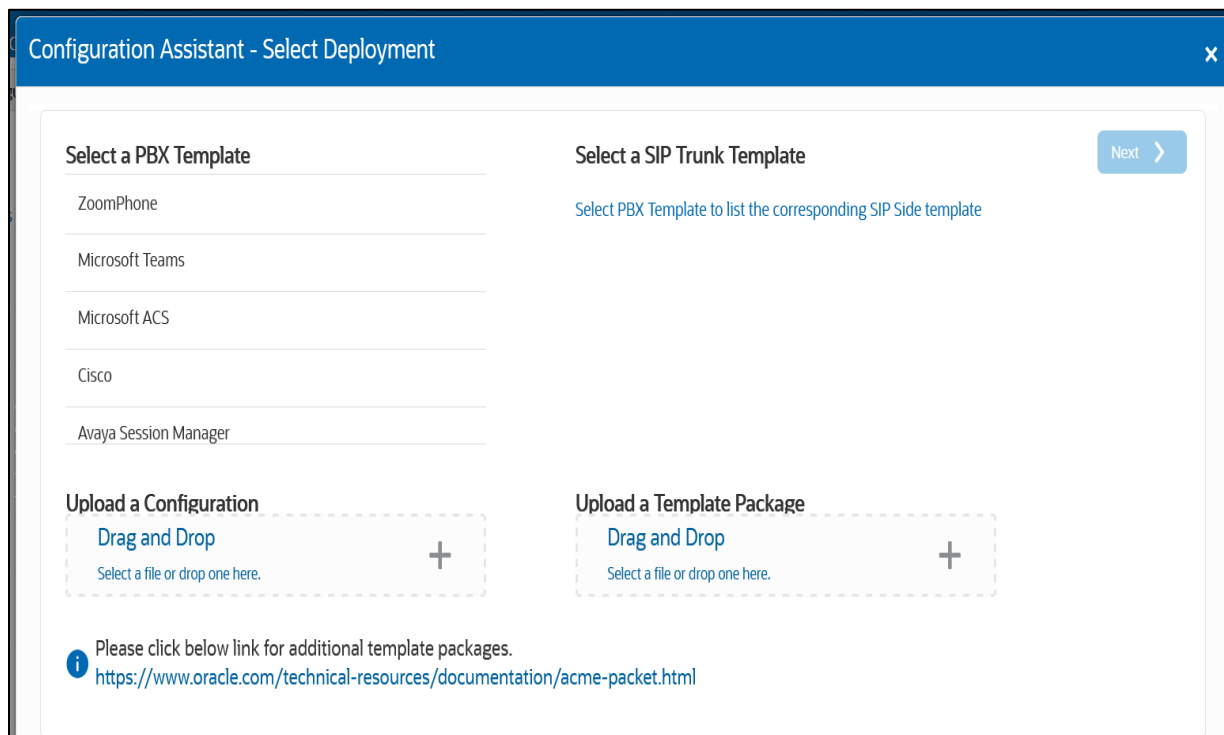
The following outline assumes you have established initial access to the SBC via console and completed the following steps:

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

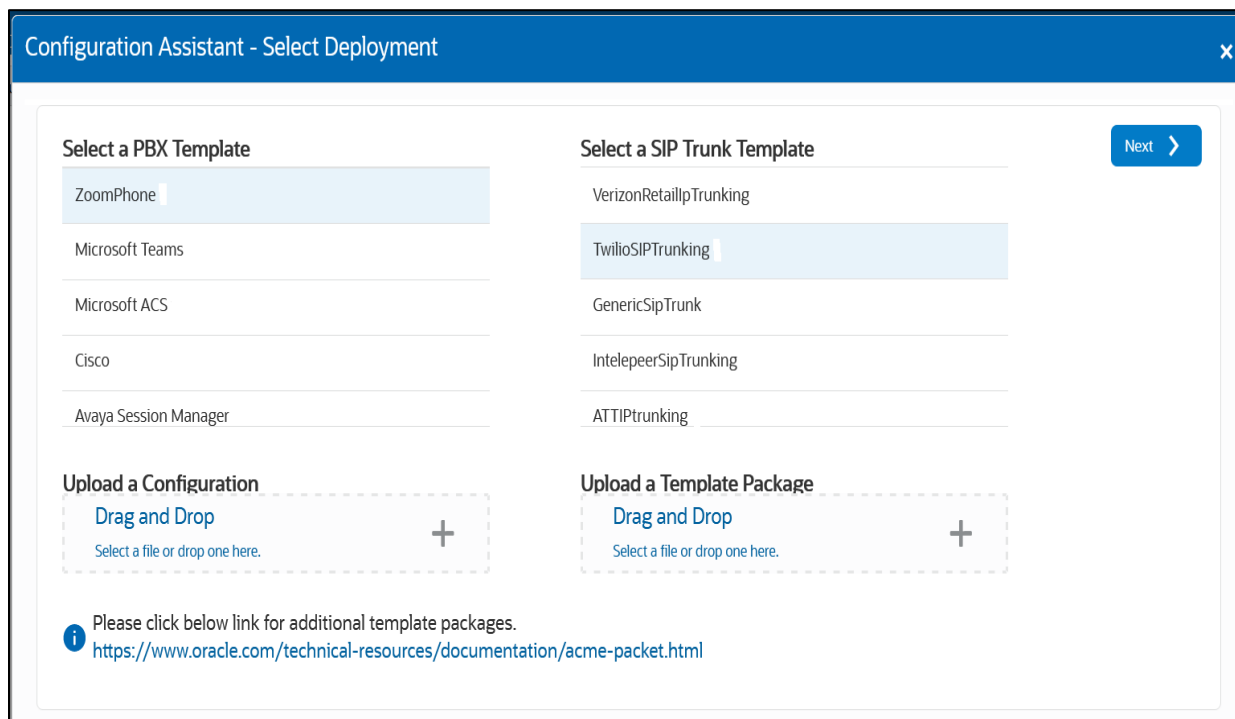
8.2. Initial GUI Access

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 ZoomPhone 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. The left column is for the "PBX Template" (Notes for ZoomPhone) and the right column is for the "SIP Trunk Template" (Notes for TwilioSIPTrunking). Both columns include a "Warning" section stating that proceeding with the Configuration Assistant will erase existing configuration, and a "Pre-requisites" section with a list of requirements such as connecting Port 0 or Port 1 of the SBC, installing SRTP licenses, and enabling advanced entitlements. A "Back" button is on the top left and a "Next" button is on the top right.

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 - Zoom Phone Network". At the top, there is a progress bar with 10 numbered steps. Step 1, "Zoom Phone Network", is currently selected and highlighted in blue. Other steps include "Root Trusted Certificate", "SBC Certificate", "Zoom Destination", "Transcodi...", "Twilio Elastic SIP Trunk", "Twilio Session Agent", "Transcodi...", "Root Trusted Certificate", and "SBC Certificate for Twilio". A "Skip" button is located at the end of the progress bar. Below the progress bar, the text reads "Let's configure the interface that communicates with Zoom Phone". There are three input fields: "Realm Name" (text input), "Port Number" (dropdown menu with "Port 0" selected), and "Slot Number" (dropdown menu with "Slot 0" selected). Each field has a "Required" label below it.

8.3. Configuration Assistant Template Navigation

8.3.1. Page 1-Zoom Phone Network

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

The screenshot shows a configuration window titled "Configuration Assistant - Zoom Phone Network". At the top, there is a progress bar with 10 steps: 1. Zoom Phone Network (active), 2. Root Trusted Certificate, 3. SBC Certificate, 4. Zoom Destination, 5. Transcodi..., 6. Twilio Elastic SIP Trunk, 7. Twilio Session Agent, 8. Transcodi..., 9. Root Trusted Certificate, and 10. SBC Certificate for Twilio. A "Back" button is on the left and a "Skip" button is on the right. Below the progress bar, the text reads "Let's configure the interface that communicates with Zoom Phone". There are three required fields: "Realm Name" (text input), "Port Number" (dropdown menu showing "Port 0"), and "Slot Number" (dropdown menu showing "Slot 0"). Each field has a help icon and a "Required" label.

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- Import DigiCert Trusted CA Certificate for MS Teams side.

Page 2 of this template is where the SBC will import the DigiCertRoot CA certificate, which Zoom uses to sign the certs it presents to the SBC during the TLS handshake. Importing the Zoom Root CA certs is enabled by default.

The screenshot shows a configuration window titled "Configuration Assistant - Root Trusted Certificate". The progress bar shows step 2, "Root Trusted Certificate", as active with a green checkmark. Step 1, "Zoom Phone Network", is completed. The text reads "Let's start provisioning the root trusted certificate for Zoom." Below this, the certificate details are displayed: "Serial Number: 08:3b:e0:56:90:42:46:b1:a1:75:6a:c9:59:91:c7:4a", "Signature Algorithm: sha1WithRSAEncryption", "Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA", "Validity: Not Before: Nov 10 00:00:00 2006 GMT, Not After : Nov 10 00:00:00 2031 GMT", and "Subject: C=US, O=DigiCert Inc, OU=www.digicert.com".

8.3.3. Page 3 - SBC Certificates for Zoom 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.

The screenshot shows the 'Configuration Assistant - SBC Certificate' window. At the top, a progress bar indicates the current step is 3, 'SBC Certificate', with previous steps 'Zoom Phone Network' and 'Root Trusted Certificate' completed. The main content area is titled 'Let's start provisioning certificates for the SBC'. It contains three required fields: 'Fully Qualified Domain Name or Common Name' (with a help icon), 'PKCS12 certificate (.p12 or .pfx)' (with an 'Upload' button and a help icon), and 'PKCS12 certificate password' (with a help icon). A 'Skip' button is located at the top right of the form area.

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).

The screenshot shows the 'Configuration Assistant - SBC Certificate' window. The progress bar indicates the current step is 3, 'SBC Certificate'. The main content area is titled 'Let's start provisioning certificates for the SBC'. It contains four required fields: 'Certificate provisioning type' (a dropdown menu with 'CSR' selected), 'Fully Qualified Domain Name or Common Name', 'Country', and 'State'. A 'Skip' button is located at the top right of the form area.

8.3.4. Page 4 - Zoom Destination

Page 4 of the template is where you will configure the Zoom Session Agent details where you will enter the next hop IP address and port for sip signaling to and from your Zoom Phone Network. Please fill the required fields and click Next.

Configuration Assistant - Zoom Destination

Back [✓] [✓] [✓] 4 5 6 7 8 9 10 Skip

Zoom Phone Network Root Trusted Certificate SBC Certificate Zoom Destination Transcodi... Twilio Elastic SIP Trunk Twilio Session Agent Transcodi... Root Trusted Certificate SBC Certificate for Twilio

Let's configure the Session Agent(s) for Zoom Cloud Voice

Zoom Session Agent hostname [?]

Required

Zoom Destination IP Address [?]

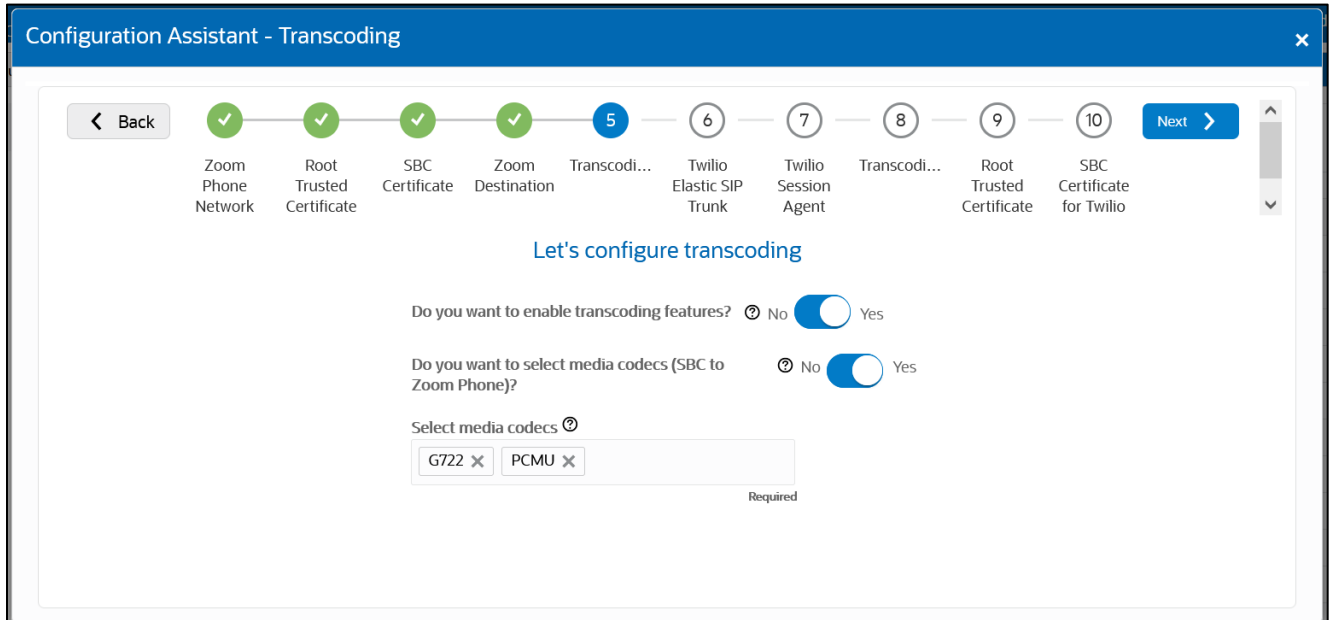
Zoom Destination Port [?]

Required

Did Zoom provide a second Hostname/IP? No Yes

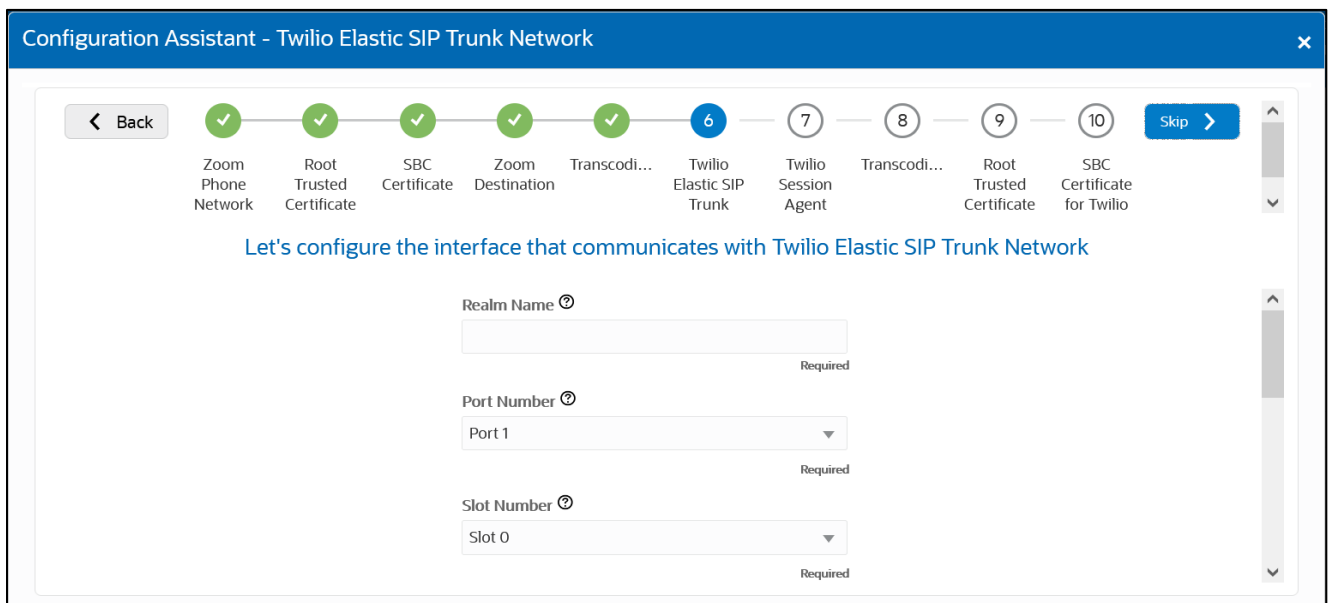
8.3.5. Page 5 - Zoom side Transcoding

Page 5 is where you will be able to configure transcoding between the SBC and Zoom side. 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 Zoom. 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.



8.3.6. Page 6 - Twilio Elastic SIP Trunk Network

Page 6 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.



8.3.7. Page 7 - Twilio Session Agent

Page 7 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.

Configuration Assistant - Twilio Session Agent

Progress: 1 Zoom Phone Network, 2 Root Trusted Certificate, 3 SBC Certificate, 4 Zoom Destination, 5 Transcodi..., 6 Twilio Elastic SIP Trunk, 7 Twilio Session Agent (Active), 8 Transcodi..., 9 Root Trusted Certificate, 10 SBC Certificate for Twilio. Skip >

Let's configure session agent for Twilio

Twilio Session Agent hostname [Ⓜ]

Required

Twilio Session Agent IP Address [Ⓜ]

Twilio Session Agent Port [Ⓜ]

Required

Do you have a second hostname / IP address for No Yes

8.3.8. Page 8 - Twilio side Transcoding

Page 8 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.

Configuration Assistant - Transcoding

Progress: 1 Zoom Phone Network, 2 Root Trusted Certificate, 3 SBC Certificate, 4 Zoom Destination, 5 Transcodi..., 6 Twilio Elastic SIP Trunk, 7 Twilio Session Agent, 8 Transcodi... (Active), 9 Root Trusted Certificate, 10 SBC Certificate for Twilio. Next >

Let's configure transcoding

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

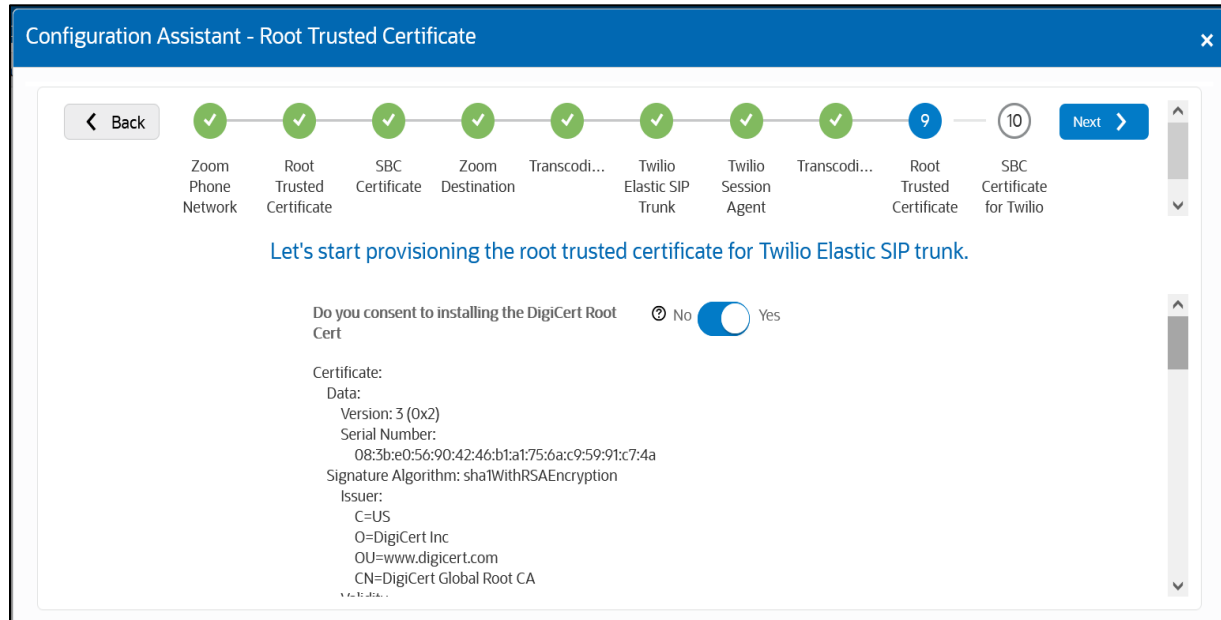
Do you want to select media codecs for your Twilio Elastic SIP trunk? [Ⓜ] No Yes

Select media codecs [Ⓜ]

Required

8.3.9. Page 9 - Import Digi Cert Root CA Certificate for Twilio Side

Page 9 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.

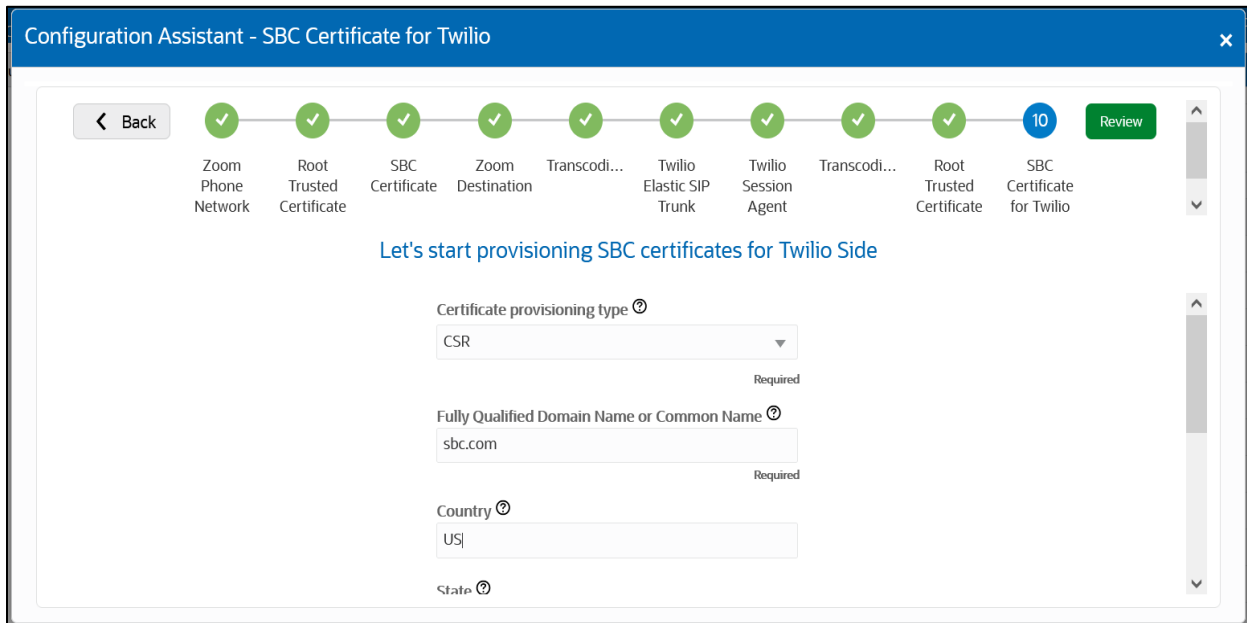


8.3.10. Page 10 - SBC Certificates for Teams side

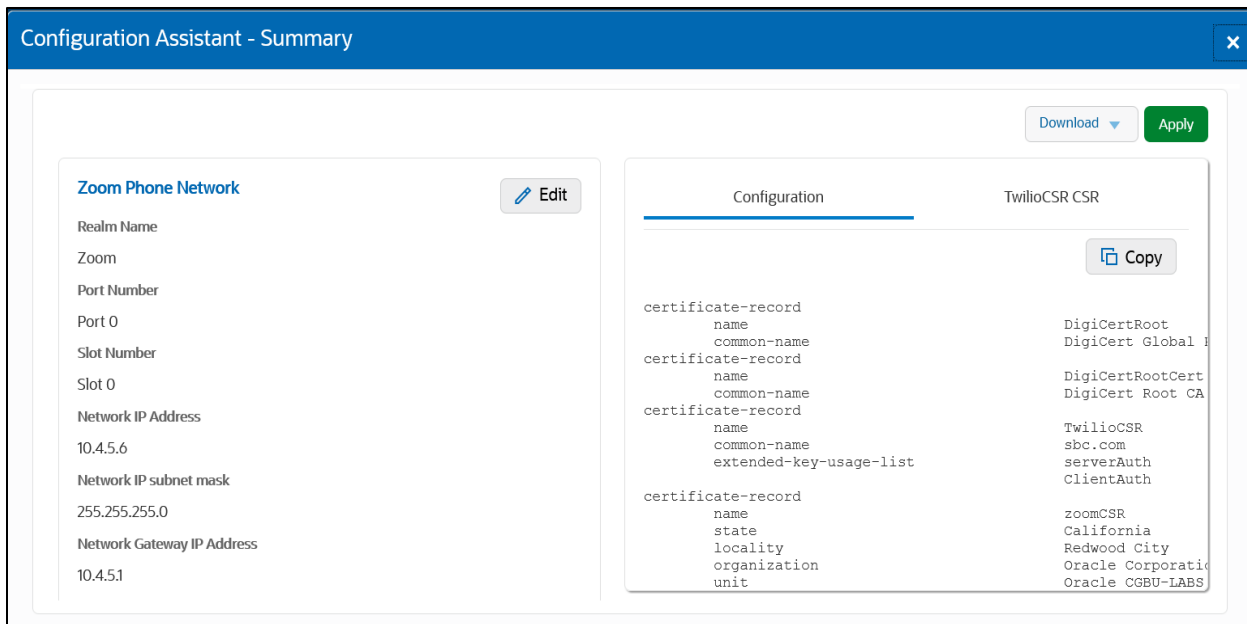
This page also follows the same procedure as page 3 and the screen also looks exactly similar to page 3. We can follow the same steps to import certificate for Twilio side too.

8.4. Review

At the end of the template, you will notice in the top right, a “*Review*” tab. If all 10 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 3 or page 10 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. Also, if you choose CSR on both pages (pages 3 and 10), there will be two CSR's on the review page.

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 3 and 10, the CSR tab will not be present under review.

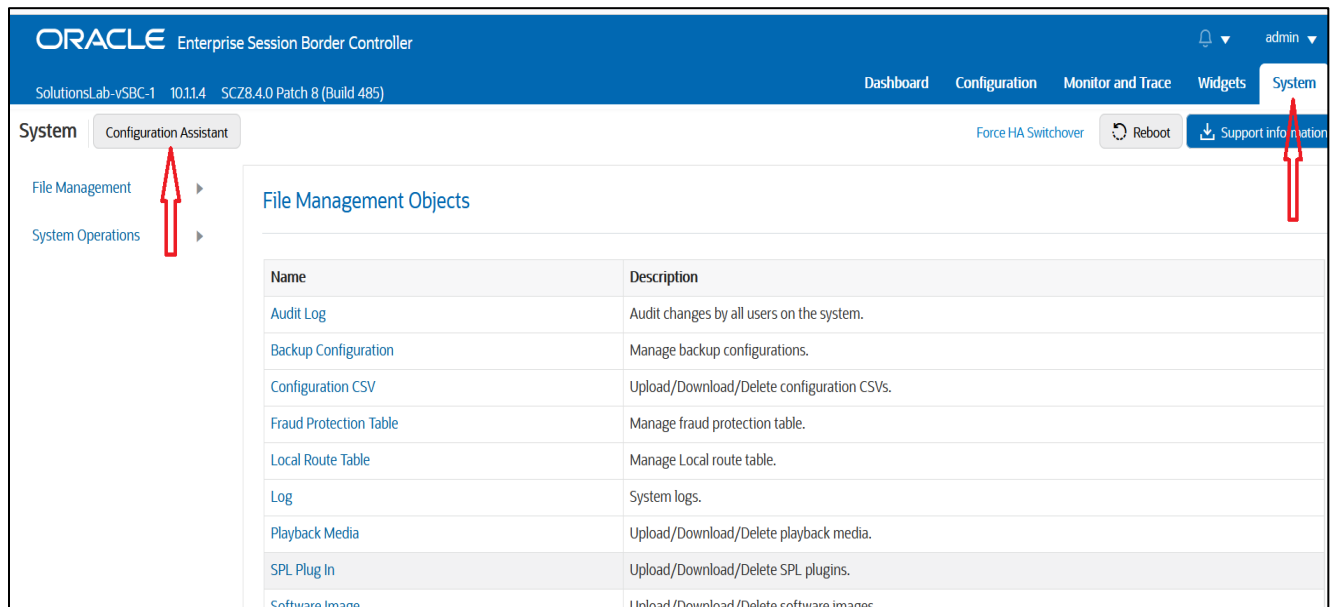
8.5. Download and/or Apply

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.

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 ZoomPhone 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.




9. Existing SBC configuration

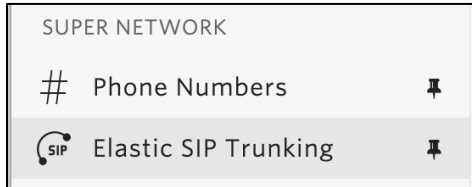
If the SBC being used is an existing SBC with functional configuration, following configuration elements are required:

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

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

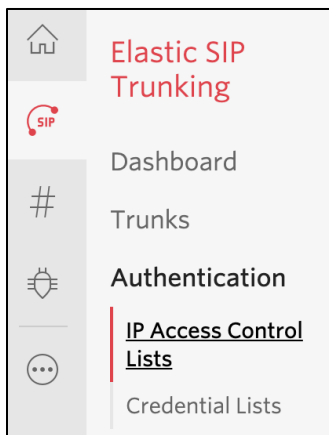
10. Twilio Elastic SIP Trunking Configuration

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 AI ...

ASSOCIATED SIP TRUNKS

ASSOCIATED SIP DOMAINS —

IP Address Ranges

+ IP ADDRESS RANGE FRIENDLY NAME

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

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

Features

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

Call Recording ⓘ

Enabled Calls will be recorded.

Call Recording

Record from ringing

Recording Trim

Disabled Silence will not be trimmed from recording

Secure Trunking ⓘ

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

Call Transfer (SIP REFER) ⓘ

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

Enable PSTN Transfer ⓘ
Allow Call Transfers to the PSTN via your Trunk.

Symmetric RTP ⓘ

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

▶ Additional Features

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

Termination URI

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

TERMINATION SIP URI

oracle

.pstn.twilio.com

[Show Localized URIs](#)

Click on "Show localized URI's" 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 ✕ +

CREDENTIAL LISTS +

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 ON

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

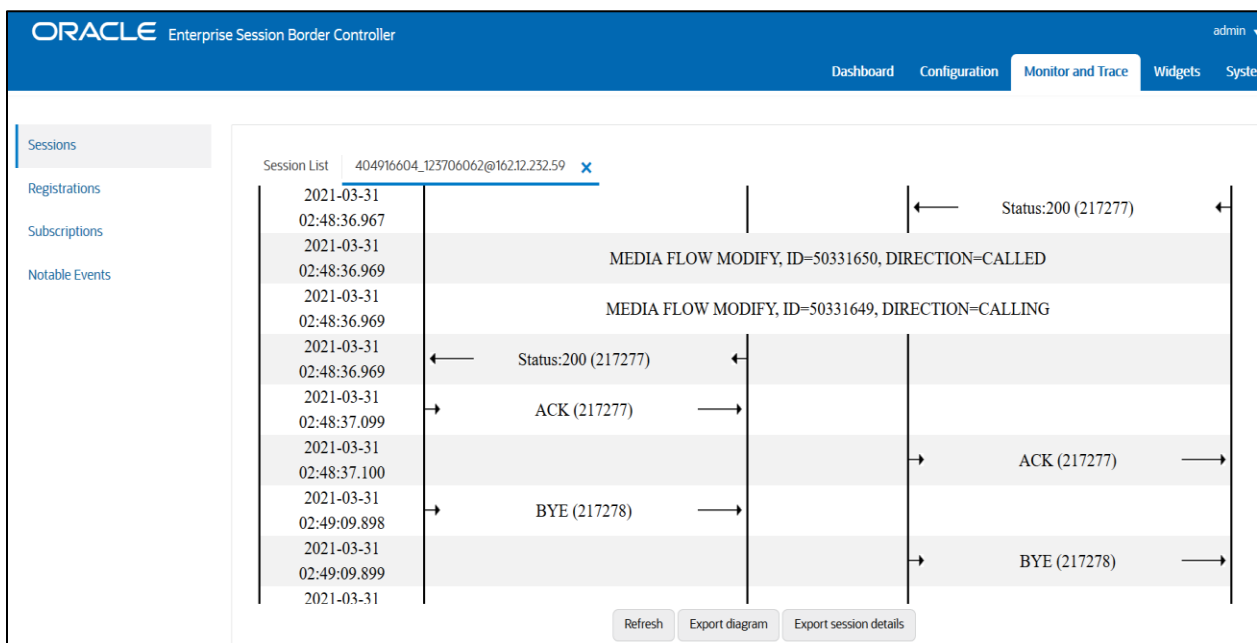
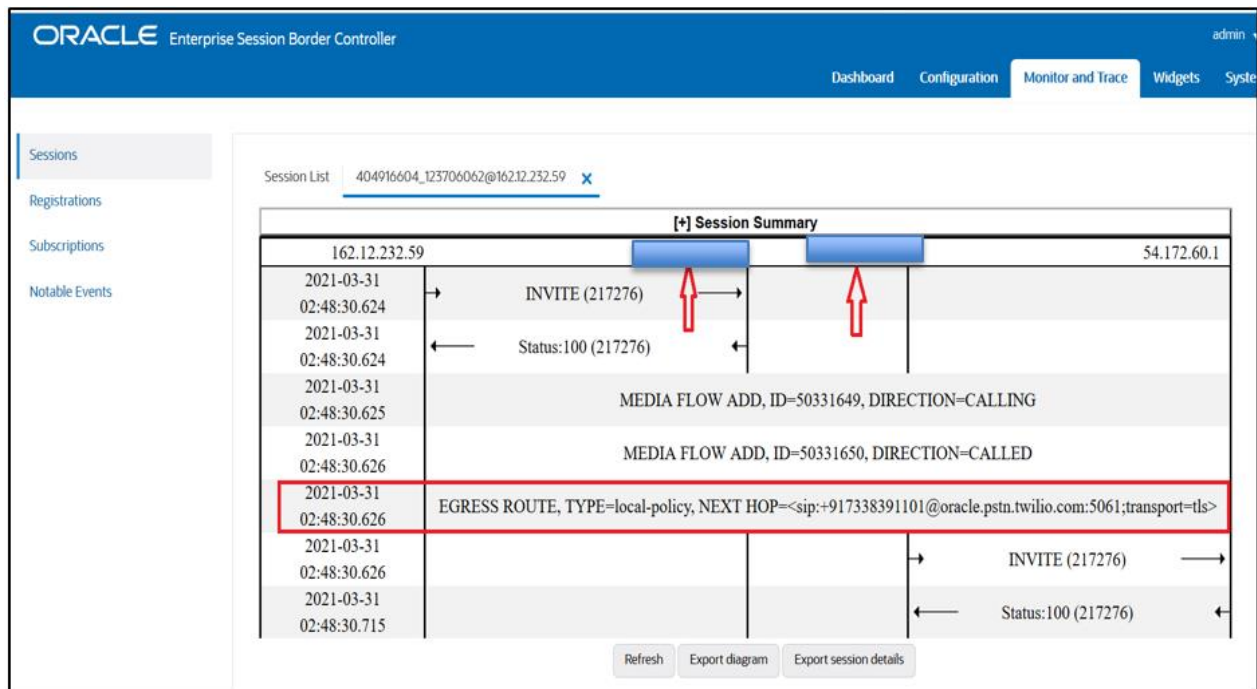
Choose Action

NUMBER	FRIENDLY NAME	COUNTRY	EMERGENCY CALLING STATUS	EMERGENCY ADDRESS	<input type="checkbox"/>
+18	[REDACTED]	4 US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	<input type="checkbox"/>
+10	[REDACTED]	3 US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	<input type="checkbox"/>
+17	[REDACTED]	5 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 Zoom Users. **For our testing, we used the single network interface for both Zoom and Twilio side as below.**

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



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

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Sessions

Registrations

Subscriptions

Notable Events

Session List [ad0a917a0264e5276c81e84taedb57f9@0.0.0.0](#)

[+] Session Summary

Time	Event	Direction
2021-03-31 03:12:26.270	INVITE (880210)	→
2021-03-31 03:12:26.270	Status:100 (880210)	←
2021-03-31 03:12:26.271	MEDIA FLOW ADD, ID=100663297, DIRECTION=CALLING	→
2021-03-31 03:12:26.271	MEDIA FLOW ADD, ID=100663298, DIRECTION=CALLED	←
2021-03-31 03:12:26.271	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:+18507904044@162.12.232.59:5061;transport=tls>	→
2021-03-31 03:12:26.271	INVITE (880210)	→
2021-03-31 03:12:26.368	Status:100 (880210)	←
2021-03-31 03:12:26.840	Status:180 (880210)	←
2021-03-31 03:12:26.841	Status:180 (880210)	←
2021-03-31 03:12:29.189	Status:200 (880210)	←
2021-03-31 03:12:29.190	MEDIA FLOW MODIFY, ID=100663298, DIRECTION=CALLED	←
2021-03-31 03:12:29.190	MEDIA FLOW MODIFY, ID=100663297, DIRECTION=CALLING	→
2021-03-31 03:12:29.190	Status:200 (880210)	←
2021-03-31 03:12:29.284	ACK (880210)	→

Refresh Export diagram Export session details

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Sessions

Registrations

Subscriptions

Notable Events

Session List [ad0a917a0264e5276c81e84taedb57f9@0.0.0.0](#)

Details for INVITE (880210)

2021-03-31 03:12:26.368	Status:100 (880210)	←
2021-03-31 03:12:26.840	Status:180 (880210)	←
2021-03-31 03:12:26.841	Status:180 (880210)	←
2021-03-31 03:12:29.189	Status:200 (880210)	←
2021-03-31 03:12:29.190	MEDIA FLOW MODIFY, ID=100663298, DIRECTION=CALLED	←
2021-03-31 03:12:29.190	MEDIA FLOW MODIFY, ID=100663297, DIRECTION=CALLING	→
2021-03-31 03:12:29.190	Status:200 (880210)	←
2021-03-31 03:12:29.284	ACK (880210)	→
2021-03-31 03:12:29.285	ACK (880210)	→
2021-03-31 03:13:06.676	BYE (299944)	←
2021-03-31 03:13:06.676	BYE (299944)	←
2021-03-31 03:13:06.781	Status:200 (299944)	→
2021-03-31 03:13:06.782	Status:200 (299944)	→
2021-03-31 03:13:06.782	MEDIA FLOW DELETE, ID=100663297, DIRECTION=CALLING	→
2021-03-31 03:13:06.782	MEDIA FLOW DELETE, ID=100663298, DIRECTION=CALLED	←

Refresh Export diagram Export session details

Appendix A




Following are the test cases that are executed as part of Zoom BYOC Model with the Twilio Elastic SIP Trunk (PSTN user).

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

16	Twilio Elastic SIP Trunk user makes outbound call to Zoom user and Zoom user makes a conference call by adding another Zoom/ PSTN user.	Pass
17	Zoom user calls an IVR number and navigates through the IVR menu after call connection	Pass
18	Zoom user calls into an external conference bridge and pastes a string of conference ID into Zoom which is recognized by Device and IVR	Pass
19	Zoom user mutes inbound call from Twilio Elastic SIP Trunk user and then unmutes	Pass
20	Zoom user mutes outbound call made to Twilio Elastic SIP Trunk user and then unmutes	Pass
21	Twilio Elastic SIP Trunk user mutes inbound call from Zoom user and then unmutes	Pass
22	Twilio Elastic SIP Trunk user mutes outbound call made to Zoom user user and then unmutes	Pass
23	Twilio Elastic SIP Trunk User disconnects outbound call to Zoom user before it is answered	Pass
24	Zoom 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