



# ORACLE


Oracle Session Border Controller with Zoom Contact Center BYOC

**Technical Application Note**

**ORACLE**  

---

**COMMUNICATIONS**




## Disclaimer

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

## Contents

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>DOCUMENT OVERVIEW.....</b>                      | <b>5</b>  |
| 1.1      | ORACLE SBC.....                                    | 5         |
| 1.2      | ZOOM CONTACT CENTER.....                           | 5         |
| <b>2</b> | <b>REVISION HISTORY .....</b>                      | <b>5</b>  |
| <b>3</b> | <b>INTENDED AUDIENCE.....</b>                      | <b>5</b>  |
| 3.1      | VALIDATED ORACLE VERSIONS .....                    | 6         |
| <b>4</b> | <b>INFRASTRUCTURE REQUIREMENTS.....</b>            | <b>6</b>  |
| <b>5</b> | <b>ZOOM CONTACT CENTER BYOC CONFIGURATION.....</b> | <b>7</b>  |
| 5.1      | CREATE A ZOOM USER .....                           | 7         |
| 5.2      | ZOOM CONTACT CENTER USER.....                      | 7         |
| 5.3      | ZOOM CONTACT CENTER ROLE .....                     | 8         |
| 5.4      | QUEUES.....  | 9         |
| 5.5      | ADD THE ORACLE SESSION BORDER CONTROLLER.....      | 11        |
| 5.6      | ROUTE GROUP .....                                  | 12        |
| 5.7      | SIP GROUP.....                                     | 14        |
| 5.8      | ADD CONTACT CENTER BYOC NUMBER.....                | 14        |
| 5.9      | CONTACT CENTER FLOWS.....                          | 15        |
| <b>6</b> | <b>CONFIGURATION .....</b>                         | <b>16</b> |
| 6.1      | PREREQUISITES.....                                 | 17        |
| 6.2      | GLOBAL CONFIGURATION ELEMENTS .....                | 18        |
| 6.2.1    | System-Config.....                                 | 18        |
| 6.2.2    | Media Manager.....                                 | 19        |
| 6.2.3    | SIP Config.....                                    | 20        |
| 6.2.4    | NTP Config.....                                    | 22        |
| 6.3      | NETWORK CONFIGURATION .....                        | 22        |
| 6.3.1    | Physical Interfaces.....                           | 23        |
| 6.3.2    | Network Interfaces .....                           | 24        |
| 6.4      | SECURITY CONFIGURATION.....                        | 25        |
| 6.4.1    | Certificate Records.....                           | 25        |
| 6.4.2    | SBC End Entity Certificate .....                   | 26        |
| 6.4.3    | Root CA and Intermediate Certificates .....        | 28        |
| 6.4.4    | Zoom Approved CA Vendors.....                      | 28        |
| 6.4.5    | Generate Certificate Signing Request.....          | 31        |
| 6.4.6    | Import Certificates to SBC.....                    | 32        |
| 6.4.7    | TLS Profile.....                                   | 34        |
| 6.5      | MEDIA SECURITY CONFIGURATION .....                 | 36        |
| 6.5.1    | Sdes-profile .....                                 | 36        |
| 6.5.2    | Media Security Policy.....                         | 37        |
| 6.6      | MEDIA CONFIGURATION.....                           | 38        |
| 6.6.1    | Realm Config.....                                  | 39        |
| 6.6.2    | Steering Pools .....                               | 41        |
| 6.7      | SIP MODIFICATIONS.....                             | 43        |
| 6.7.1    | SIP Manipulations.....                             | 43        |
| 6.7.2    | Session-Translation .....                          | 50        |
| 6.8      | SIP INTERFACE.....                                 | 52        |



|           |  |           |
|-----------|--|-----------|
| 6.9       | SESSION AGENTS.....                    | 54        |
| 6.10      | ROUTING CONFIGURATION .....            | 57        |
| 6.10.1    | Local Policy Configuration.....        | 57        |
| 6.11      | ACCESS CONTROLS .....                  | 59        |
| 6.12      | SBC BEHIND NAT SPL CONFIGURATION ..... | 60        |
| <b>7.</b> | <b>ACLI RUNNING CONFIGURATION.....</b> | <b>62</b> |

## 1 Document Overview

Designed to increase productivity, Zoom Contact Center streamlines communication to foster a greater sense of collaboration between colleagues and augment the customer experience. Oracle Enterprise SBC protect critical, real-time communications for collaboration, unified communications (UC), and contact centers. Oracle Enterprise Session Border Controller (E-SBC) lets you interconnect SIP trunks, on-premises enterprise telephony, UCaaS, CCaaS, and any other SIP service with security, reliability, quality, and scalability and can be deployed in your own network, as well as in major public clouds.

This document focuses how to connect Oracle SBC to Zoom Contact Center to provide PSTN connectivity in a BYOC environment.

Related Documentation can be found below-

### 1.1 Oracle SBC

- [Oracle® Session Border Controller ACLI Configuration Guide](#)
- [Oracle® Session Border Controller Release Notes](#)
- [Oracle® Session Border Controller Security Guide](#)

### 1.2 Zoom Contact Center

- <https://explore.zoom.us/en/products/contactcenter/>
- <https://blog.zoom.us/introducing-zoom-contact-center/>
- <https://support.zoom.us/hc/en-us/categories/4423802887949-Zoom-Contact-Center-Support>

## 2 Revision History

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

| Version | Date Revised | Description of Changes  |
|---------|--------------|---|
| 1.0     | 06/12/2023   | <ul style="list-style-type: none"><li>• Initial publication</li></ul> |

## 3 Intended Audience

This document describes how to connect the Oracle SBC to Zoom Contact Center BYOC. This paper is intended for IT or telephony professionals.

*Note: To zoom in on screenshots of Web GUI configuration examples, press Ctrl and +.*

### 3.1 Validated Oracle Versions

We have successfully conducted call testing with the Oracle Communications SBC versions:SCZ9.2p3

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

- AP 1100
- AP 3900
- AP 4600
- AP 6350
- AP 6300
- AP3950
- AP4900
- VME
- Oracle SBC on Public Cloud

Please visit <https://docs.oracle.com/en/industries/communications/session-border-controller/index.html> for further information.

## 4 Infrastructure Requirements

The table below shows the list of infrastructure prerequisites for deploying Zoom Contact Center BYOC.

|   |  |
|---|--|
| Session Border Controller (SBC)                                   | <b>See <a href="#">Zoom Documentation</a> for More Details</b> |
| SIP Trunks connected to the SBC                                   |  |
| Zoom Contact Center License                                       |  |
| Public IP address for the SBC                                     |  |
| Public trusted certificate for the SBC (If TLS transport is used) |  |
| Firewall ports for Zoom Contact Center signaling                  |  |
| Firewall IP addresses and ports for Zoom Contact Center media     |  |
| Media Transport Profile   |  |
| Firewall ports for client media                                   |  |
|   |  |

## 5 Zoom Contact Center BYOC Configuration

This document only covers the steps required to configure Oracle SBC with Zoom Contact Center BYOC. There may be other components that are part of the Zoom Contact Center BYOC Setup which are not included in this document. The document focuses on the important configuration elements related to setting up the Zoom Contact Center environment. We have provided a reference to the Zoom configuration required in the Application Note however additional configuration elements may be required to be configured as per your respective implementation .Please refer the Zoom support articles or contact your Zoom representative for understanding of the implementation.

Please contact your Zoom Sales representative to procure the Zoom Contact Center access and License. For detailed assistance with setting up and configuring your Zoom Contact Center BYOC System please reach out to Zoom Sales: <https://zoom.us/contactsales>

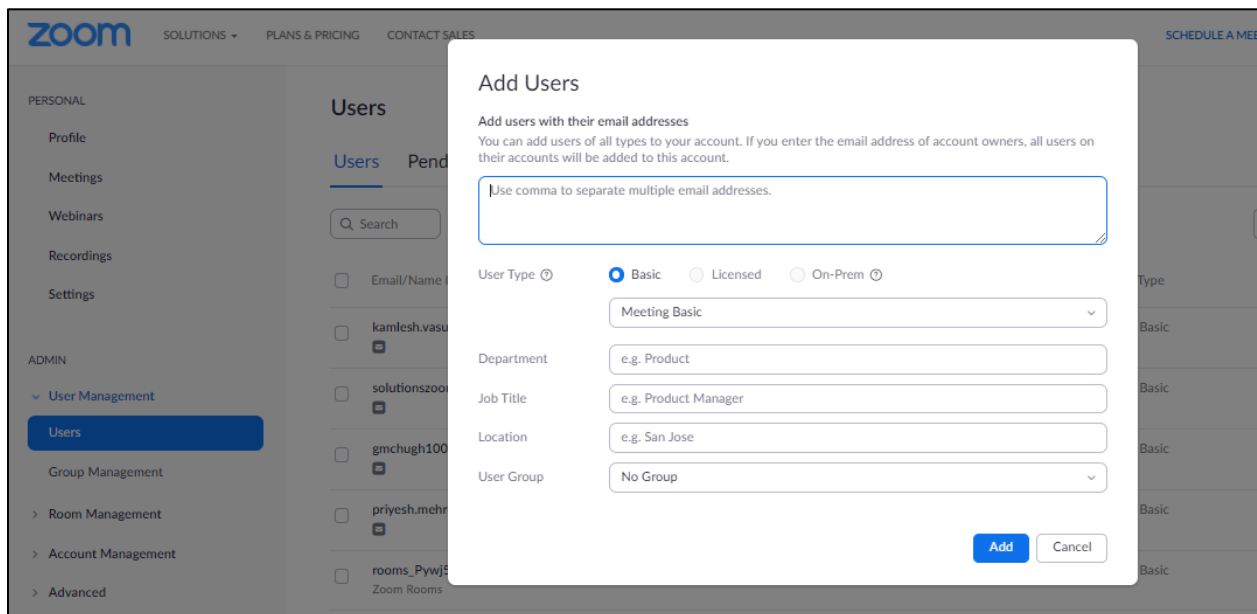
### 5.1 Create a Zoom User

Login to the Zoom Web Portal through your administrator credentials and

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 screenshot shows the Zoom Web Portal interface with the 'Add Users' dialog box open. The dialog box is titled 'Add Users' and contains the following fields and options:

- Add Users** (Title)
- Add users with their email addresses** (Instruction)
- You can add users of all types to your account. If you enter the email address of account owners, all users on their accounts will be added to this account.** (Note)
- Use comma to separate multiple email addresses.** (Text input field)
- User Type** (Dropdown menu): Basic (selected), Licensed, On-Prem
- Meeting Basic** (Dropdown menu)
- Department** (Text input field): e.g. Product
- Job Title** (Text input field): e.g. Product Manager
- Location** (Text input field): e.g. San Jose
- User Group** (Dropdown menu): No Group
- Add** (Button)
- Cancel** (Button)

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

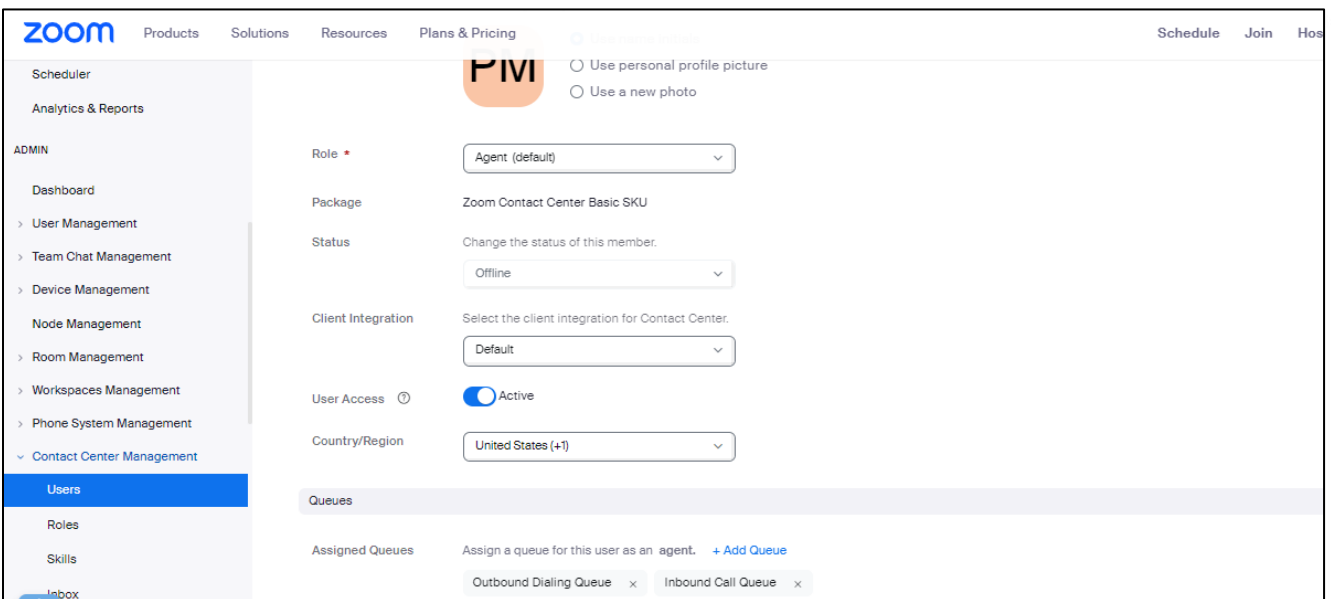
### 5.2 Zoom Contact Center user

Reference Zoom Article - <https://support.zoom.us/hc/en-us/articles/4423978411405-Managing-Zoom-Contact-Center-users->

Zoom Contact Center admins can assign or remove Zoom Contact Center licenses to existing Zoom users. You can add an existing user in the Zoom account to Zoom Contact Center.

1. Sign into the Zoom web portal.
2. In the navigation menu, click Contact Center Management then Users.
3. Click Add.
4. In the General section, specify the following required information:
  - User(s): Click Add, select the users to assign licenses to, then click Add.
  - Role: Select the role to assign to the user.
5. (Optional) Change the user's settings.  
Note: Some settings are only available after you've added the user, and you're changing user settings.
6. Click Save.  
Users will receive an email notification.

Below is an example of a sample Zoom Contact Center Agent created from Zoom Portal.



### 5.3 Zoom Contact Center Role

Zoom reference article - <https://support.zoom.us/hc/en-us/articles/4471054202253-Using-Zoom-Contact-Center-role-management>

There are three default roles that you can add members to. You can't delete these roles, but you can duplicate these roles to use as a starting point for a new custom role.



| Role Name  | Description   | Number of Members | Moc     |
|------------|---|-------------------|---------|
| Admin      | Admins have a wide range of permissions for accessing and managing Zoom Contact Center.                                   | 2                 | Can moc |
| Supervisor | Supervisors have some permissions for accessing and managing Zoom Contact Center.   | 0                 | Can moc |
| Agent      | Agents can access Zoom Contact Center engagement functions, but do not have permissions for managing Zoom Contact Center. | 3                 | Can moc |

Below example from Zoom Portal displays the 2 users are created with admin privileges and 3 Users are created as Agents in the test environment.

| Role Name  | Description   | Number of Members | Moc     |
|------------|---|-------------------|---------|
| Admin      | Admins have a wide range of permissions for accessing and managing Zoom Contact Center.                                   | 2                 | Can moc |
| Supervisor | Supervisors have some permissions for accessing and managing Zoom Contact Center.   | 0                 | Can moc |
| Agent      | Agents can access Zoom Contact Center engagement functions, but do not have permissions for managing Zoom Contact Center. | 3                 | Can moc |

**5.4 Queues.**

Zoom reference article – <https://support.zoom.us/hc/en-us/articles/4423986595085-Managing-Zoom-Contact-Center-queues>

Zoom Contact Center admins can create queues and add queue members. Queues determine the agents that calls are routed to. Queues also link to an existing routing profile to determine how calls are routed. After creating a queue, you can change queue settings.

To create a queue -

1. Sign into the Zoom web portal.
2. In the navigation menu, click **Contact Center Management** then **Queues**.
3. Click **Add**.
4. Enter the following information:

- **Name:** Enter a display name to help identify the queue.
- **Description (Optional):** Enter a description for the queue.
- **Channel:** Select the channel type for the queue. This corresponds to the flow channel and trigger type.
  - **Voice (Choose Voice for BYOC voice calls)**
- **Agents:** Click **Add** to add agents as queue members.

5. Click **Save**.

Below example shows the 2 voice channel queues we have created for the test environment.

**Queues**  
Create queues that define the consumers' engagement experience, including the agents and supervisors who engage with them.

Search by name:  Channel (All)

| <input type="checkbox"/> | Name ↕                 | Channel | Agents    | Supervisors | Modified by        | Last Modified ↕         | <input type="checkbox"/> |
|--------------------------|------------------------|---------|-----------|-------------|--------------------|-------------------------|--------------------------|
| <input type="checkbox"/> | Demo<br>Demo           | Voice   | 0 User(s) | 0 User(s)   | Oracle Partners... | 08/04/2023,<br>05:00 AM | <input type="checkbox"/> |
| <input type="checkbox"/> | Inbound Call Queue     | Voice   | 3 User(s) | 1 User(s)   | Oracle Partners... | 08/31/2023,<br>04:00 AM | <input type="checkbox"/> |
| <input type="checkbox"/> | Outbound Dialing Queue | Voice   | 3 User(s) | 1 User(s)   | Oracle Partners... | 08/31/2023,<br>03:43 AM | <input type="checkbox"/> |

**zoom** Products Solutions Resources Plans & Pricing Schedule Join

workspaces management  
Phone System Management  
Contact Center Management

- Users
- Roles
- Skills
- Inbox
- Queues**
- Phone Numbers
- Routing Profiles
- Dispositions
- Assets Library
- Waiting Rooms
- Flows
- Preferences

Queues > Inbound Call Queue

**Inbound Call Queue** ↗

[Profile](#) [Policy](#) [Channel Upgrades](#) [Survey](#)

Assigned Users

Assigned Users 3 Agents and 1 Supervisor [Manage](#)

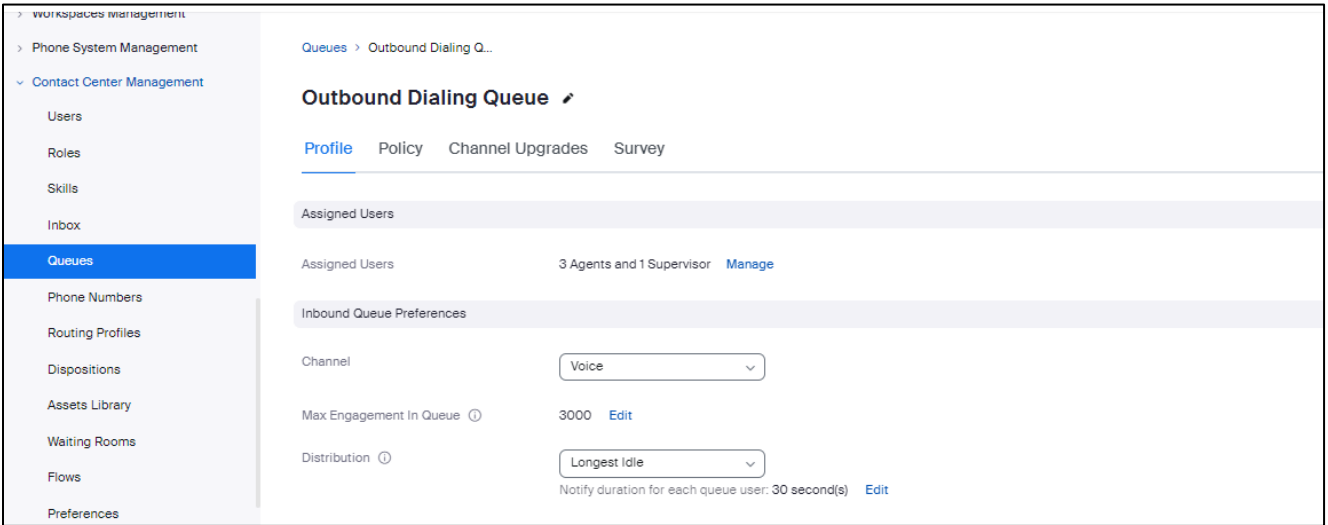
Inbound Queue Preferences

Channel

Max Engagement In Queue ⓘ 3000 [Edit](#)

Distribution ⓘ

Notify duration for each queue user: 30 second(s) [Edit](#)



## 5.5 Add the Oracle Session Border Controller.

You must add the Oracle SBCs Public IP onto the Zoom Portal that will establish the connectivity with Zoom Contact Center BYOC.

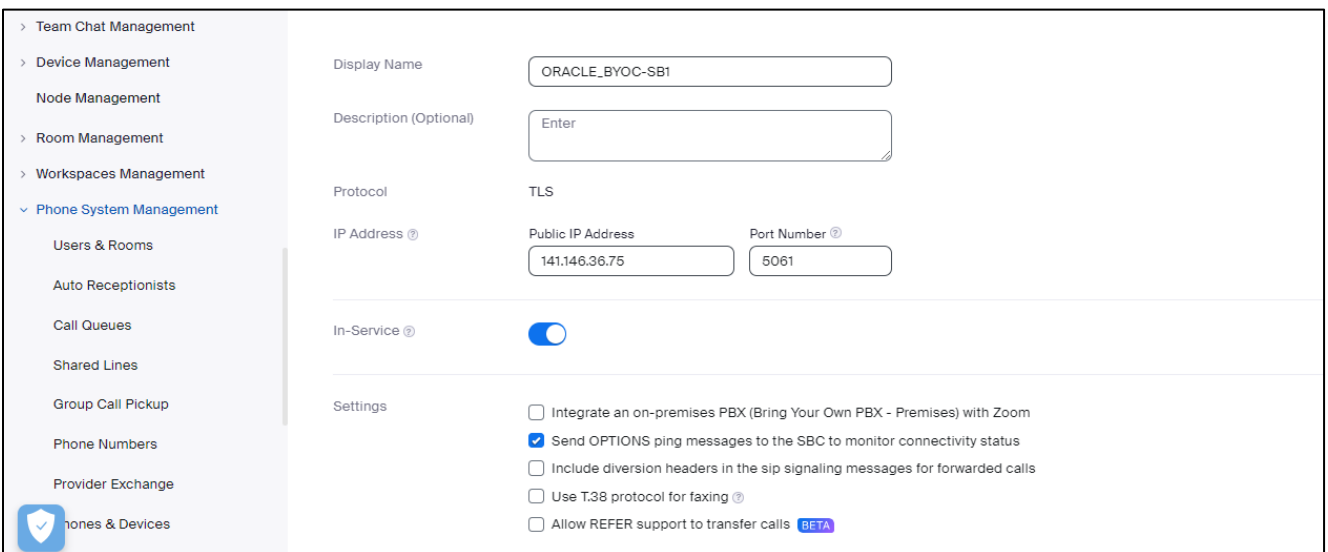
**Navigate to Phone System Management > Company info > Account settings > Session Border Controllers > Manage**

Enter the Oracle SBCs Public IP address and port

Enable below parameters.

Integrate an on-premises PBX (Bring Your Own PBX - Premises) with Zoom

Send OPTIONS ping messages to the SBC to monitor connectivity status



You can add more than one SBCs. Once the SBCs are added contact your Zoom representative to whitelist the IP and Port in their ACLs before you can start sending traffic and check the SIP connectivity through SIP OPTIONS once the transport is established.

## 5.6 Route Group

Route Groups are composed of one or more Session Border Controllers and assigned to SIP groups to determine the routing behavior for BYOC-P and BYOP-P calls. When a Route Group is assigned to a Region, calls are originated or terminated on the Zoom data centers that are part of that Region.

To create a route group.

**Navigate to Phone System Management > Company info > Account settings > Route Groups**

Click Add

Enter the Display Name

Type – BYOC-P

Region – Choose the appropriate region as per the geographic details of your implementation.

Distribution type – Can be sequential or Load Balancing.

Below is an example of Route Group from Zoom Admin Center.

The screenshot displays the 'Edit Route Group' modal in the Zoom Admin Center. The modal contains the following fields and options:

- Display Name:** ORACLE\_BYOP\_01
- Type:** BYOP-P
- Region:** US01 - US (SJ/DW/NY)
- Distribution:** Sequential
- Session Border Controllers:**

| Order | Session Border Controller         | Order          |
|-------|-----------------------------------|----------------|
| 1:    | ORACLE_BYOCP_02 (20.96.25.165:5)  | ↑ ↓ Add Delete |
| 2:    | ORACLE_BYOCP_01 (141.146.36.75:5) | ↑ ↓ Add Delete |
- Backup Route Group (Optional):** Select

The background interface shows the 'Phone System Management' section with a search bar and a list of regions: US Central (Colorado), US West (N. California), and US East (New York). A table of SIP Groups is partially visible on the right, showing columns for 'Type (All)', 'SIP Group', and 'Status'.


Once you add the Route Group Click on the Provision Button. It will take approximately 10 mins for the route group to provision and the state will change to In Progress and further completed once it is provisioned.

**Contact Center Route Group**

Region ⓘ : Sequential ⓘ :

US01 - US (SJ/DV/NY)

|                             |  |        |    |                           |                      |                     |
|-----------------------------|--|--------|----|---------------------------|----------------------|---------------------|
| - US West (N. California) ⓘ | ORACLE_BYOCP_...<br>(141.146.36.75:5061) | BYOC-P | -- | <a href="#">Provision</a> | <a href="#">Edit</a> | <a href="#">...</a> |
| - US Central (Colorado) ⓘ   | ORACLE_BYOCP_...<br>(141.146.36.75:5061) |        |    |                           |                      |                     |
| - US East (New York) ⓘ      | ORACLE_BYOCP_...<br>(141.146.36.75:5061) |        |    |                           |                      |                     |



| Display Name ⌵                | Session Border Controllers               | Type ⓘ | Backup Route Group | Provision Status | SIP Group            |                     |
|-------------------------------|--|--------|--------------------|------------------|----------------------|---------------------|
| <b>testRG</b>                 |  |        |                    |                  |                      |                     |
| Region ⓘ : Load Balancing ⓘ : |  |        |                    |                  |                      |                     |
| US01 - US (SJ/DV/NY)          |  |        |                    |                  |                      |                     |
| - US Central (Colorado) ⓘ     | ORACLE_BYOCP_...<br>(141.146.36.75:5061) | BYOC-P | --                 | In Progress ⓘ    | <a href="#">Edit</a> | <a href="#">...</a> |
| - US West (N. California) ⓘ   | ORACLE_BYOCP_...<br>(141.146.36.75:5061) |        |                    |                  |                      |                     |
| - US East (New York) ⓘ        | ORACLE_BYOCP_...<br>(141.146.36.75:5061) |        |                    |                  |                      |                     |

**ORACLE\_BYOP\_01**

Region ⓘ : Sequential ⓘ :

US01 - US (SJ/DV/NY)

|                             |  |        |    |             |                   |                      |                     |
|-----------------------------|--|--------|----|-------------|-------------------|----------------------|---------------------|
| - US Central (Colorado) ⓘ   | ORACLE_BYOCP_...<br>(20.96.25.165:5061)  | BYOP-P | -- | Completed ⓘ | ccsipgroup<br>SG1 | <a href="#">Edit</a> | <a href="#">...</a> |
| - US West (N. California) ⓘ | ORACLE_BYOCP_...<br>(141.146.36.75:5061) |        |    |             |                   |                      |                     |
| - US East (New York) ⓘ      | ORACLE_BYOCP_...<br>(141.146.36.75:5061) |        |    |             |                   |                      |                     |

## 5.7 SIP Group

Define SIP Groups and assign Route Groups to them, so as to route the calls placed by BYOC numbers. Any outgoing calls from the SIP Groups will be routed to the specific Route Groups.  
Creating SIP group is mandatory as you will require them while uploading BYOC Numbers.

To create a SIP group

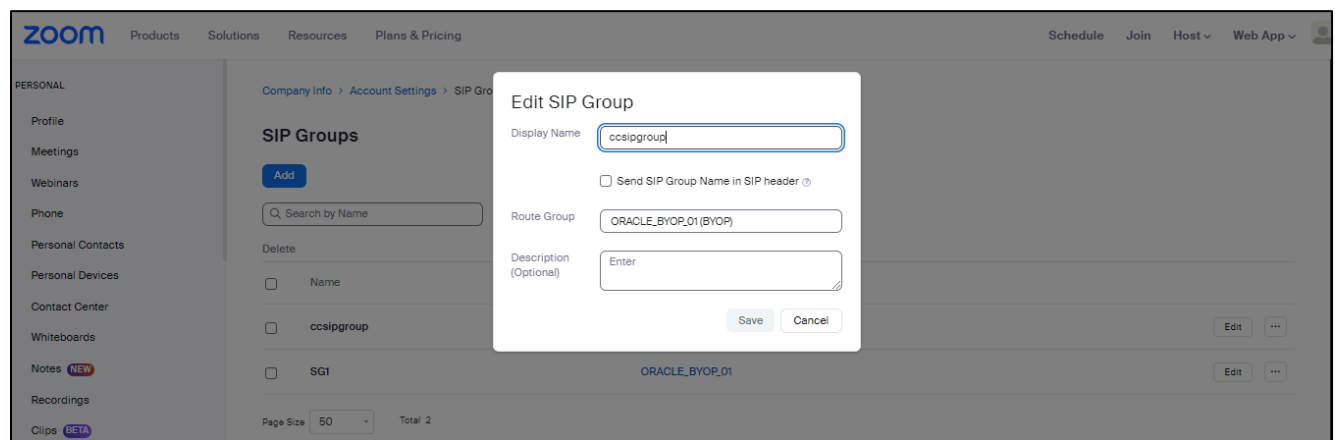
**Navigate to Phone System Management > Company info > Account settings > Sip Groups**

Enter Display Name

Select one of the previously created route group to bind the route group to the SIP Group.

Click Save

Below is an example from the Zoom Web Portal of the SIP Group.



## 5.8 Add Contact Center BYOC Number

You can add your phone numbers provided by your own carriers into Zoom. These numbers can act as entry point to a flow.

Reference article - <https://support.zoom.us/hc/en-us/articles/4471534794893-Managing-Zoom-Contact-Center-phone-numbers>

**Navigate to Contact Center Management > Phone Numbers.**

1. Choose BYOC Section to add the BYOC Number.

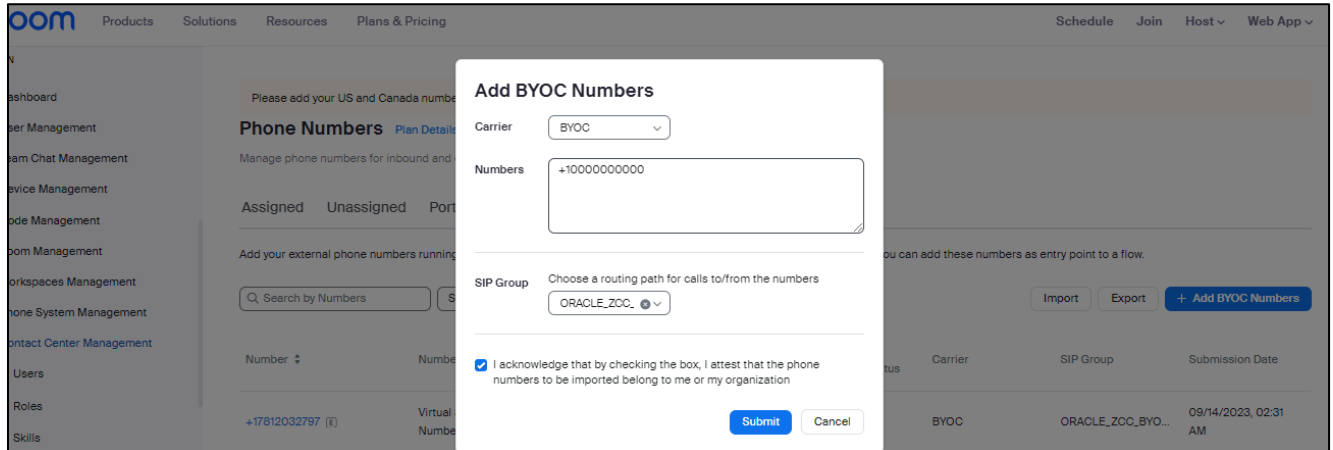
Click on Add BYOC Numbers

You can add the numbers individually or can upload a csv file as well.

Site – Chose a site for your implementation.

Carrier – BYOC

SIP Group – Choose the SIP Group created previously in Step 5.7



## 5.9 Contact Center Flows

The Zoom Contact Center flow editor is a graphical programming environment for creating and adjusting channel workflows.

Reference article - <https://support.zoom.us/hc/en-us/sections/4424229774861-Flow-Editor>

To create Flows Navigate to **Contact Center Management > Flows**

Add Flow

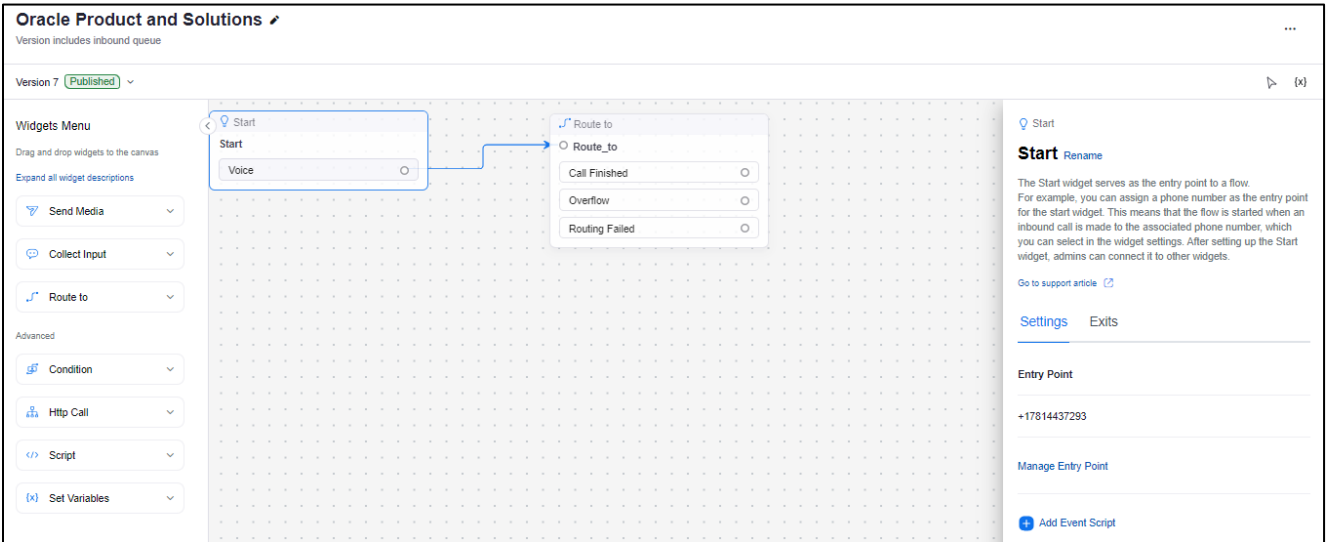
Create the appropriate flows as per your organization needs.

Below is an example of a sample inbound call flow that uses a BYOC number as an entry point. The customer is the below example dial the number to reach Zoom Contact center. These calls will be routed from the carrier trunk to Oracle SBC which will terminate it to the Zoom Contact Center Platform.

Please follow Zoom Support articles to create the flows according to your need.

Below article demonstrates how to manage a flow entry point to assign a BYOC number to the flow.

<https://support.zoom.us/hc/en-us/articles/4472948997133-Customizing-the-Start-widget>



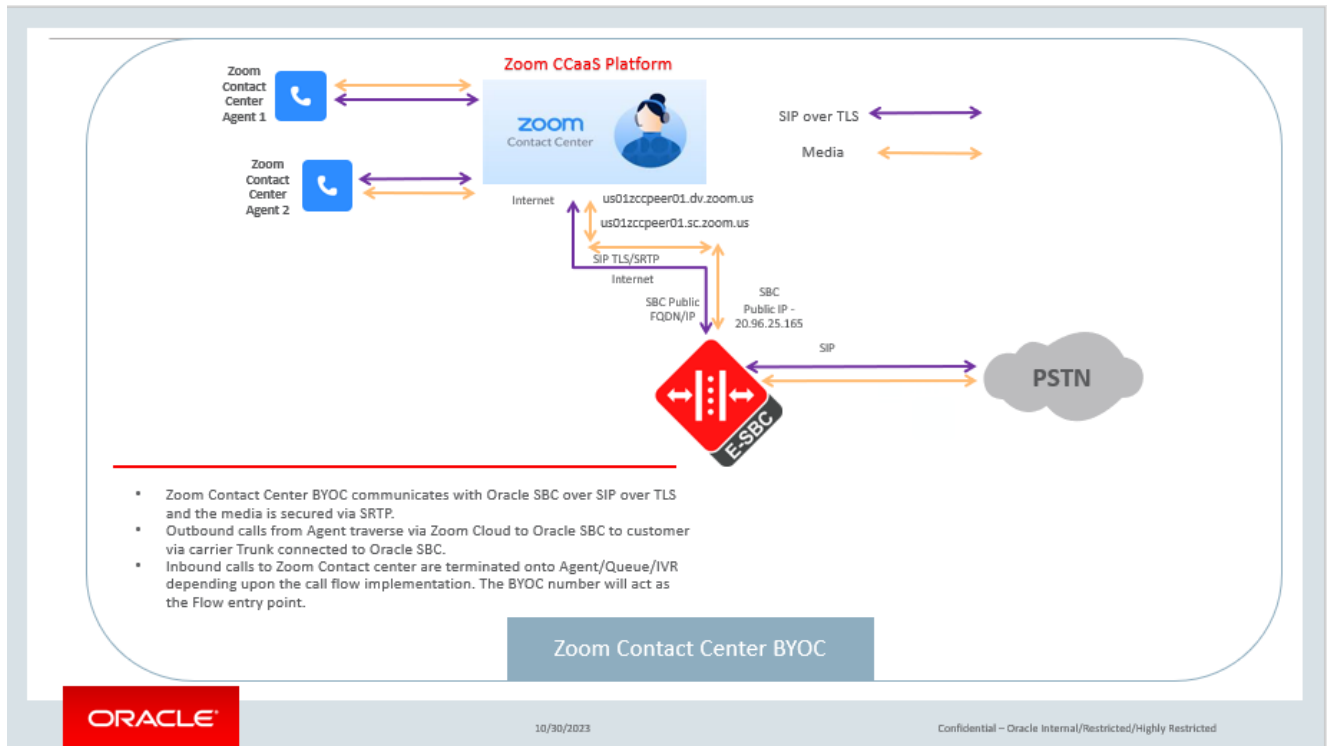
## 6 Configuration

This chapter provides step-by-step guidance on how to configure Oracle SBC for interworking with Zoom Contact Center BYOC.

All testing were performed in Oracle Labs. Below is an outline of the network setup used to conduct all testing between the Oracle SBC and Zoom Contact Center BYOC platform.

*These instructions cover configuration steps between the Oracle SBC and Zoom Contact Center BYOC. The complete interconnection of other entities, such as connection of the SIP trunk, 3rd Party PBX and/or analog devices are not fully covered in this instruction. The details of such connection are available in other instructions produced by the vendors of retrospective components.*





Above Figure illustrates how customers can utilize Oracle SBC to connect to provide PSTN connectivity to Zoom Contact Center Agents. PSTN Calls originating from Zoom Contact Center BYOC System are routed to customer's PSTN Trunk from Oracle SBC.

Inbound calls from PSTN to Zoom Contact Center are terminated to the Contact Center Flow entry Point from which the calls are routed for further treatment as per your organizational needs.

For the purpose of this application note the connection to Zoom Contact Center and Oracle SBC is TLS/SRTP.

## 6.1 Prerequisites

Before you begin, make sure that you have the following per every SBC you want to pair:

- Public IP address
- Public certificate issued by one of the supported CAs
- Zoom Public CA certificates to add to trust store of SBC

There are two methods for configuring the Oracle SBC, ACLI, or GUI. For the purposes of this note, we'll provide both ACLI and WebGUI examples.

This guide assumes the Oracle SBC has been installed, management interface has been configured, product selected and entitlements have been assigned. If you require more information on how to install your SBC platform, please refer to the [ACLI configuration guide](#).

Any configuration parameter not specifically listed below can remain at the ORACLE SBC default value and does not require a change for connection to Zoom Contact Center BYOC to function properly, however this should be noted as basic guidelines and there may be a need to implement additional Oracle SBC configuration parameters in your production setup.

Contact your Oracle Sales representative if you require assistance in configuring the Oracle SBC.

**Note:** All network parameters, ip addresses, hostnames etc..are specific to Oracle Labs, and cannot be used outside of the Oracle Lab enviroment. They are for example purposes only!!!

## 6.2 Global Configuration Elements

Before you can configuration more granular parameters on the SBC, there are four global configuration elements that must be enabled (nap optional) to proceed.

- System-Config
- Media-manager-Config
- SIP-Config
- Ntp-config

### 6.2.1 System-Config

To configure system level functionality for the ORACLE SBC, you must first enable the system-config

GUI Path: system/system-config

ACLI Path: config t→system→system-config

**Note:** *The following parameters are optional but recommended for system config*

- Hostname
- Description
- Location
- Default-gateway (*recommend using the management interface gateway for this global setting*)

- Click the OK at the bottom of the screen.

To configure system-config from ACLI –

ACLI Path: config t→system→system-config

```

system-config
hostname          oraclesbc.com
description       SBC for Zoom Cloud Voice
location          Burlington, MA
  
```

- Perform a save and activate configuration for changes to take effect.

### 6.2.2 Media Manager

To configure media functionality on the SBC, you must first enable the global media manager

GUI Path: media-manager/media-manager

ACL Path: config t→media-manager→media-manager-config

The following options are recommended for global media manager to help secure the SBC.

- Max-untrusted-signalling
- Min-untrusted-signalling

The values in both these fields are related to the SBC's security configuration. For more detailed security configuration options, please refer to the [SBC's Security Guide](#).

The screenshot shows the 'Modify Media Manager' configuration page in a GUI. On the left is a navigation menu with items like 'media-manager', 'codec-policy', 'media-policy', 'realm-config', 'steering-pool', 'security', 'session-router', and 'system'. The 'media-manager' item is selected. The main area contains the following configuration fields:

| 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                                     |                          |

At the bottom of the configuration area are 'OK' and 'Delete' buttons. A 'Show All' toggle is located at the bottom left of the main configuration area.

- Click OK at the bottom.

To enable media-manager from ACLI –

ACL Path: config t→media-manager→media-manager-config

```
media-manager
state          enabled
```

- Perform a save and activate configuration for changes to take effect.

### 6.2.3 SIP Config

To enable SIP related objects on the Oracle SBC, you must first configure the global SIP Config element:

GUI Path: session-router/SIP-config

ACL Path: config t→session-router→SIP-config

The following are recommended parameters under the global SIP-config:

- Options: Click Add, in pop up box, enter the string: **inmanip-before-validate**
- Click Apply/Add another, then enter: **max-udp-length=0**
- Press OK in box
- Home Realm ID (Optional)

Configuration View Configuration Q Discard Verify Save

### Modify SIP Config

|                     |                                     |                               |
|---------------------|-------------------------------------|-------------------------------|
| State               | <input checked="" type="checkbox"/> | enable                        |
| Dialog Transparency | <input checked="" type="checkbox"/> | enable                        |
| Home Realm ID       |                                     | Core_Zoom                     |
| Egress Realm ID     |                                     |                               |
| Nat Mode            |                                     | None                          |
| Registrar Domain    |                                     | *                             |
| Registrar Host      |                                     | *                             |
| Registrar Port      |                                     | 5060 ( Range: 0,1025..65535 ) |
| Init Timer          |                                     | 500 ( Range: 0..4294967295 )  |
| Max Timer           |                                     | 4000 ( Range: 0..4294967295 ) |
| Trans Expire        |                                     | 32 ( Range: 0..999999999 )    |

OK Delete

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

|                          |                                     |   |
|--------------------------|-------------------------------------|---|
| Red Max Trans            |                                     | 10000 ( Range: 0..50000 )                       |
| Options                  |                                     | inmanip-before-validate X<br>max-udp-length=0 X |
| SPL Options              |                                     |   |
| SIP Message Len          |                                     | 4096 ( Range: 0..65535 )                        |
| Enum Sag Match           | <input type="checkbox"/>            | enable  |
| Extra Method Stats       | <input checked="" type="checkbox"/> | enable  |
| Extra Enum Stats         | <input type="checkbox"/>            | enable  |
| Registration Cache Limit |                                     | 0 ( Range: 0..999999999 )                       |
| Register Use To For Lp   | <input type="checkbox"/>            | enable  |
| Refer Src Routing        | <input checked="" type="checkbox"/> | enable  |

OK Delete

- Click OK at the bottom

To configure sip config from ACLI.

ACL Path: config t→session-router→sip-config

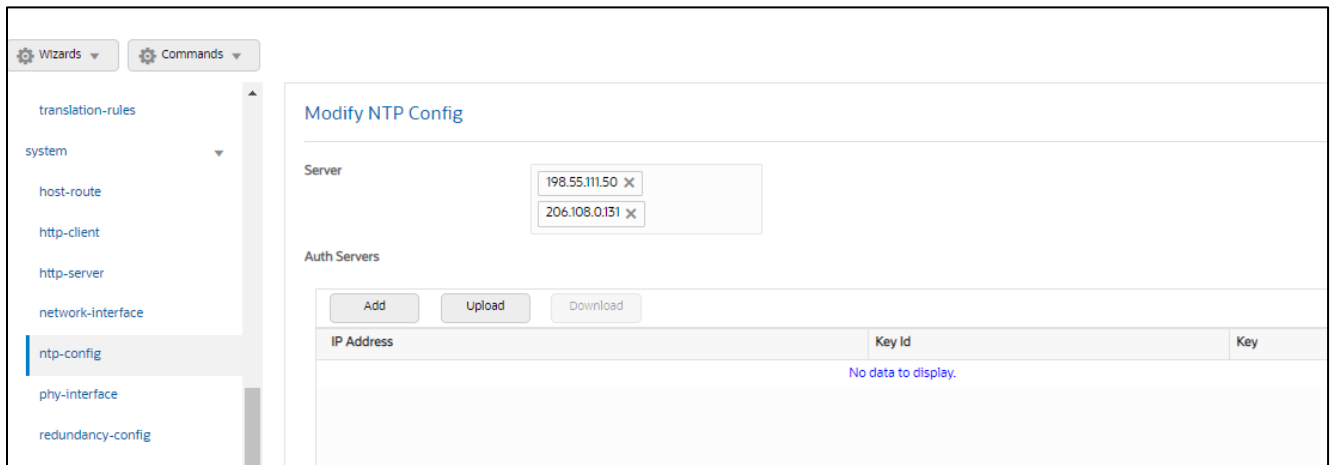
```
sip-config
  home-realm-id          Zoom
  options                max-udp-length=0
                        inmanip-before-validate
```

- Perform a save and activate configuration for changes to take effect.

### 6.2.4 NTP Config

GUI Path: system/ntp-config

ACL Path: config t→system→ntp-config



- Click OK at the bottom

To configure ntp-config from ACLI –

ACL Path: config t→system→ntp-sync

```
ntp-config
  server                216.239.35.0
```

- Perform a save and activate configuration for changes to take effect.

### 6.3 Network Configuration

To connect the SBC to network elements, we must configure both physical and network interfaces. For the purposes of this example, we will configure three physical interfaces, and three network interfaces. One to communicate with Zoom Cloud Voice, the other to connect to PSTN Networks.

**Note:** It is not required to have to PSTN terminations and just one Carrier trunk is required to route calls to and From Zoom Contact Center.

### 6.3.1 Physical Interfaces

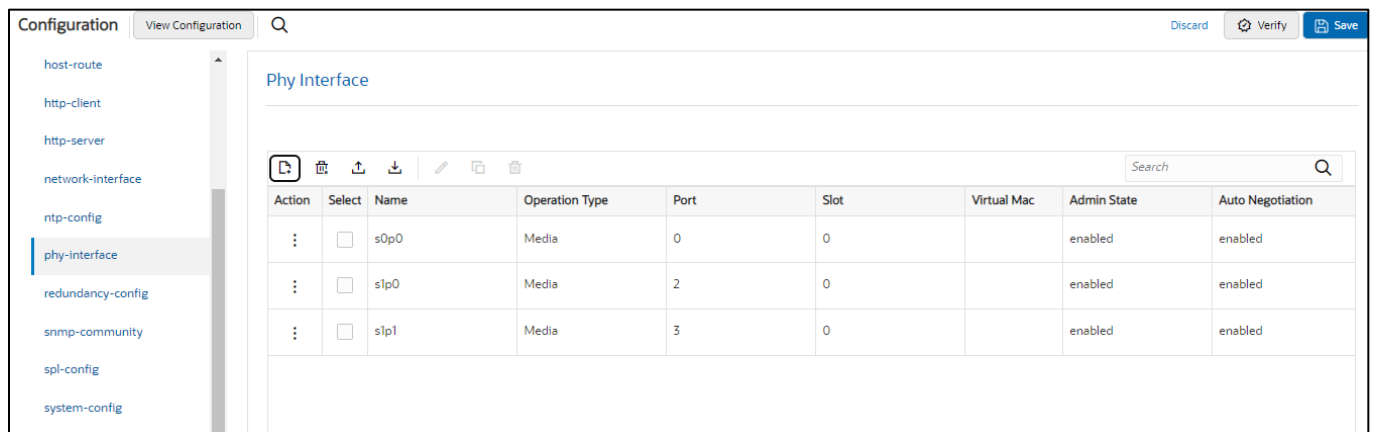
GUI Path: system/phy-interface

ACL Path: config t→system→phy-interface

- Click Add, use the following table as a configuration example:

| Config Parameter | Zoom  | PSTN1 | PSTN2 |
|------------------|-------|-------|-------|
| Name             | s0p0  | s1p0  | s1p1  |
| Operation Type   | Media | Media | Media |
| Slot             | 0     | 1     | 1     |
| Port             | 0     | 0     | 0     |

*Note: Physical interface names, slot and port may vary depending on environment*



- Click OK at the bottom of each after entering config information.

To configure phy-interface from ACLI –

ACL Path: config t→system→phy-interface

```

phy-interface
  name          s0p0
  operation-type Media
phy-interface
  name          s0p1
  operation-type Media
  port          1
phy-interface
  name          s1p0
  operation-type Media
  slot          1
  
```

- Perform a save and activate configuration for changes to take effect.

### 6.3.2 Network Interfaces

GUI Path: system/network-interface

ACL Path: config t→system→network-interface

- Click Add, use the following table as a configuration example:

| Configuration Parameter | Zoom                   | PSTN1        | PSTN2         |
|-------------------------|------------------------|--------------|---------------|
| Name                    | s0p0                   | s1p0         | s1p1          |
| Hostname                | Domain (if applicable) |              |               |
| IP Address              | 155.212.214.177        | 172.18.0.201 | 192.168.1.10  |
| Netmask                 | 255.255.255.0          | 255.255.0.0  | 255.255.255.0 |
| Gateway                 | 155.212.214.1          | 172.18.0.1   | 192.168.1.1   |
| DNS Primary IP          | 8.8.8.8                |              |               |
| DNS Domain              | Domain(if applicable)  |              |               |

The screenshot shows the 'Network Interface' configuration page in a GUI. On the left, a sidebar contains a tree view with 'network-interface' selected. The main area displays a table of network interfaces. The table has columns for Action, Select, Name, Sub Port Id, Description, Hostname, IP Address, and Pri Utility Addr. Three rows are visible, each with a colon in the Action column and a checkbox in the Select column. The IP addresses are 155.212.214.177, 172.18.0.201, and 192.168.1.10.

| Action | Select                   | Name | Sub Port Id | Description | Hostname | IP Address      | Pri Utility Addr |
|--------|--------------------------|------|-------------|-------------|----------|-----------------|------------------|
| :      | <input type="checkbox"/> | s0p0 | 0           |             |          | 155.212.214.177 |                  |
| :      | <input type="checkbox"/> | s1p0 | 0           |             |          | 172.18.0.201    |                  |
| :      | <input type="checkbox"/> | s1p1 | 0           |             |          | 192.168.1.10    |                  |

- Click OK at the bottom of each after entering config information



To configure network-interface from ACLI –

ACLI Path: config t→system→network-interface

```
network-interface
  name          s0p0
  ip-address    155.212.214.177
  netmask      255.255.255.192
  gateway      155.212.214.1
  dns-ip-primary 8.8.8.8
  dns-domain   telechat.o-test06161977.com
network-interface
  name          s1p0
  ip-address    172.18.0.201
  netmask      255.255.0.0
  gateway      172.18.0.1
network-interface
  name          s1p1
  ip-address    192.168.1.10
  netmask      255.255.255.0
  gateway      192.168.1.1
```

- Perform a save and activate configuration for changes to take effect.

## 6.4 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Zoom Contact Center BYOC Platform.

Zoom Contact Center BYOC allows UDP or TLS connections from SBC's for SIP traffic, and RTP or SRTP for media traffic. For our testing, the connection between the Oracle SBC and Zoom Contact Center BYOC platform was secured via TLS/SRTP.

This setup requires a certificate signed by one of the trusted Certificate Authorities.

### 6.4.1 Certificate Records

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

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

GUI Path: security/certificate-record

ACLI Path: config t→security→certificate-record

For the purposes of this application note, we'll create Five certificate records.They are as follows:

- SBC Certificate (end-entity certificate)
- DigiCertGlobalRootCA- In our setup SBC certificate is signed from DigiCertGlobalRootCA
- DigiCert Intermediate Cert (this is optional – only required if your server certificate is signed by an intermediate).In our setup we have DigiCert SHA2 Secure Server CA as the Intermediate CA.

These Certificates can be downloaded at below links –

- <https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem>
- <https://www.digicert.com/kb/digicert-root-certificates.htm#intermediates>

The follow certificates must be installed onto the SBC to trust the TLS Certificate provided by Zoom for TLS negotiation.DigiCert TLS Certificates can be downloaded at below Links.

- <https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem>
- <https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem>
- <https://cacerts.digicert.com/DigiCertGlobalRootG3.crt.pem>

#### 6.4.2 SBC End Entity Certificate

The SBC's end entity certificate is what is presented to Zoom Contact Center BYOC signed by your CA authority which is trusted by Zoom (Please see section 6.5.1 for detailed Zoom Supported CA Vendors), in this example we are using DigiCert as our signing authority. The certificate must include a common name. For this, we are using an fqdn as the common name.

- Common name: **(telechat.o-test06161977.com)**

To Configure the certificate record:

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

- Click OK at the bottom
- Next, using this same procedure, configure certificate records for Root CA and Intermediate Certificates

To configure certificate-record from ACLI –

ACLI Path: config t→security→certificate-record

```

certificate-record
  name          SBCEnterpriseCert
  state         California
  locality      Redwood City
  organization  Oracle Corporation
  unit          Oracle CGBU
  common-name   telechat.o-test06161977.com
  extended-key-usage-list  serverAuth
                                     ClientAuth

```

- Perform a save and activate configuration for changes to take effect.

- Next, using this same procedure, configure certificate records for the Root CA certificates

### 6.4.3 Root CA and Intermediate Certificates

The following, DigitCertRootGlobalRootCA 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.

Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

| Config Parameter        | Digicert Intermediate               | DigiCertGlobalRootCA                | DigiCertGlobalRootG2                | DigiCertGlobalRootG3                |
|-------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Common Name             | DigiCert SHA2 Secure Server CA      | DigiCert Global Root CA             | DigiCert Global Root G2             | DigiCert Global Root G3             |
| Key Size                | 2048                                | 2048                                | 2048                                | 2048                                |
| Key-Usage-List          | digitalSignature<br>keyEncipherment | digitalSignature<br>keyEncipherment | digitalSignature<br>keyEncipherment | digitalSignature<br>keyEncipherment |
| Extended Key Usage List | serverAuth                          | serverAuth                          | serverAuth                          | serverAuth                          |
| Key algor               | rsa                                 | rsa                                 | rsa                                 | rsa                                 |
| Digest-algor            | Sha256                              | Sha256                              | Sha256                              | Sha256                              |

### 6.4.4 Zoom Approved CA Vendors

Below is the list of Zoom approved CA Vendors. Oracle SBC Certificate can be signed by any of these Certificate Authorities.

| 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      |

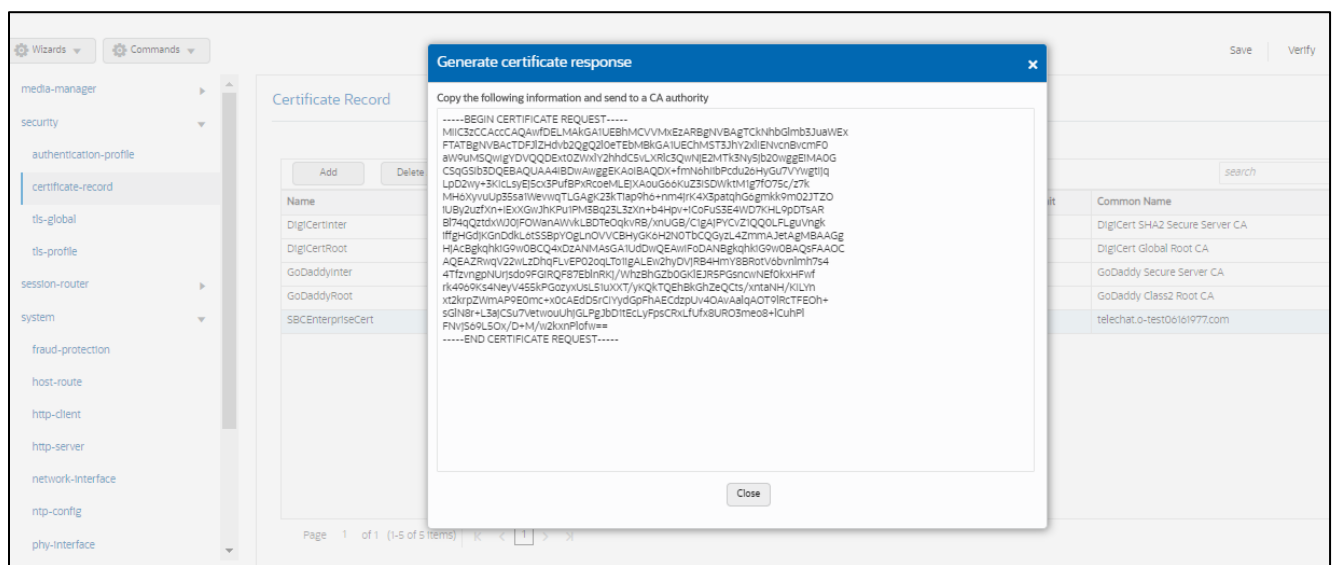
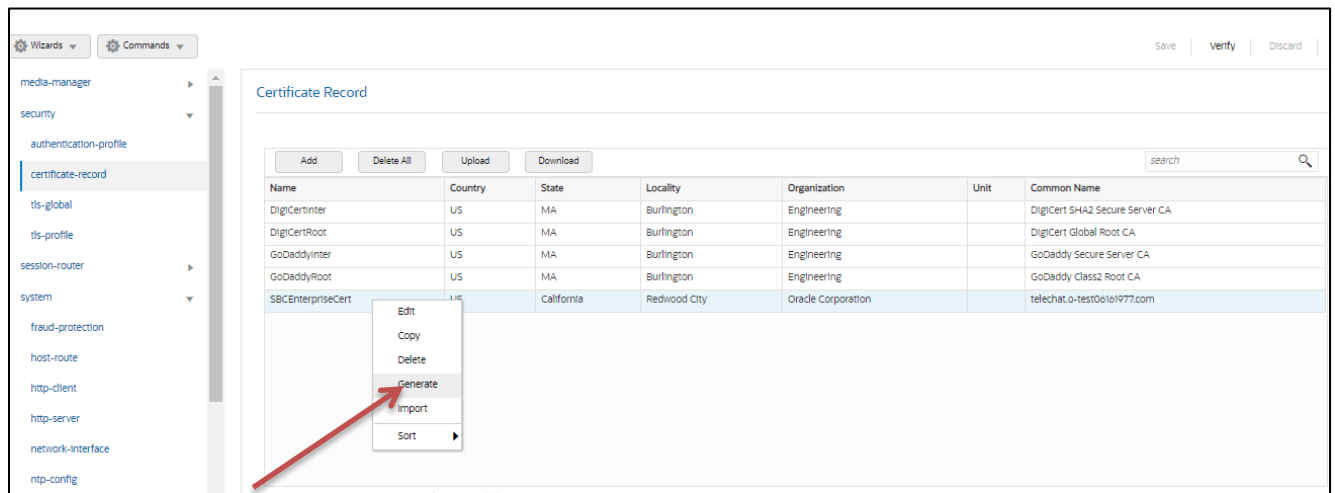
|                                    |                              |
|------------------------------------|------------------------------|
| T-Systems Enterprise Services GmbH | T-TeleSec GlobalRoot Class 2 |
| T-Systems Enterprise Services GmbH | T-TeleSec GlobalRoot Class 3 |

### 6.4.5 Generate Certificate Signing Request

Now that the SBC's certificate has been configured, create a certificate signing request for the SBC's end entity only.

**This is not required for any of the Root CA or intermediate certificates that have been created.**

On the certificate record page in the Oracle SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:



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

To Perform the Steps From ACLI use the below command –

#### **generate-certificate-request SBCEnterpriseCert**

This Step generates a text on Screen as shown below –

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC4zCCAcsCAQAawazELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAK1BMRMwEQYDVQQQ
HEwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbnVlcmlyZzEkMCIGA1UEAxMbdGVs
ZWN0eXQub3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3
MIIBCgKCAQEAr3AmjF15PclclwIB/kFExUGNHQHIbkJi28MDbcprO/KLXIHQysSnw
UWz34XLBfLQ6rS4MLyEMR8Nt8GGNSIWKiR431LsX7L+yGWvRjcBFP6DIHtH0Vuqm
ixVaUJpg5luPY6SvT1shyu26iLIBsLfem43tbKq5jz/jrvaUzyhICvAQ23c1oS5a
D4UiF2mNOuSqxvmkx50a3/BNYbKecLNOxvKQyyTMgffNpASbZuW+eMEUKI5iB+AB
/AAoZRP4bn4qlE3wn8pJsNm8Pjxy4hbz24ySgmaN9iXpP1FdRw0TemfCsNazZRuK
DsviWJfunZYTzRfDe5pJToMH4u1zt2fK1QIDAQABoDMwMQYJKoZlHvcNAQkOMSQw
IjALBgNVHQ8EBAMCBaAwEwYDVR0IBAwCgYIKwYBBQUHAWAwEwDQYJKoZlHvcNAQEL
BQADggEBADD5Y+u08LxmTMIJ2Rjc8cgPZocTqBDXN0tp27S4FuB/01ikBBdG3YV
Ffp7/Q8ZeFHHgU/rMzeF8Gpo9Cc6JUGGux3/ws8ZkgRBxsNIG276i7pFN1vCljEP
89AGxtryioRMc4kcdPpLJNQ10Qx1zKobHMTftGLDI6jN2pvn3zYHH8qA9V/1/yKa
3n0j33EuTrvTIQ5P4IgyVJqSBkd129T1gXY6O8JVFLCQefTrF4TLc6teNzxXMdPw
PHoPu9hM3scGOWOHQnODXOFeq2AxBQzAa0/Cjf7Bw3l3POmMclOawgDecZ8UjHpJ
IznX9/Gxg5X+S2QkHjNmPK+JuePqX4l=
-----END CERTIFICATE REQUEST-----
```

Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.

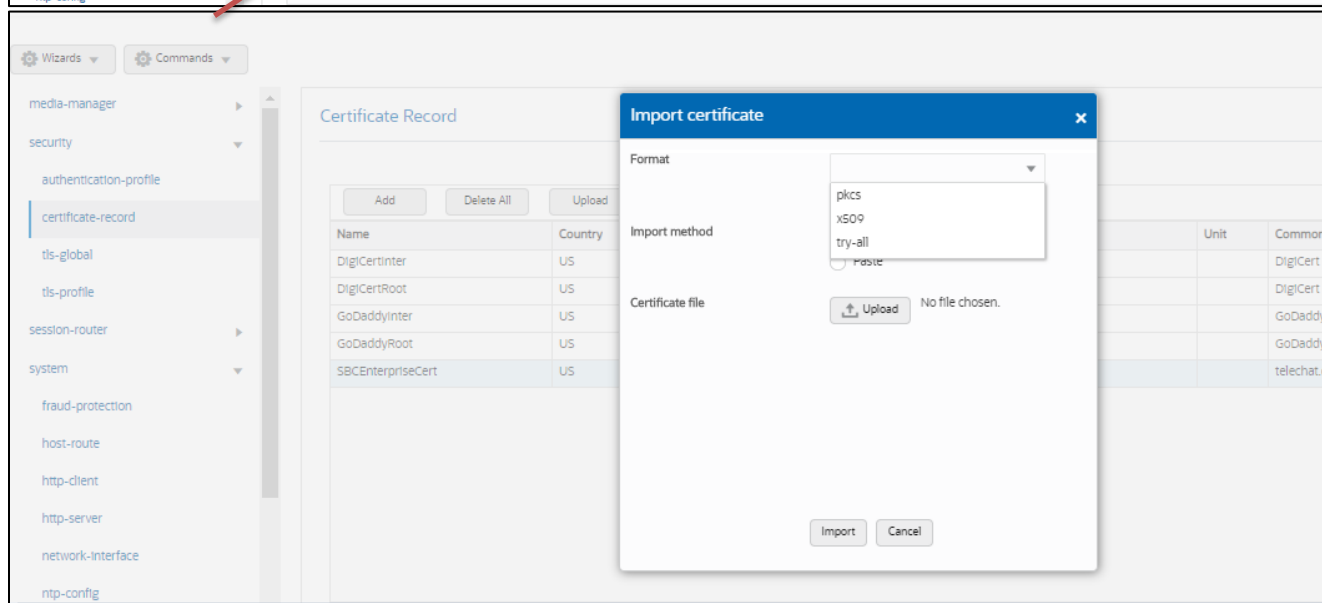
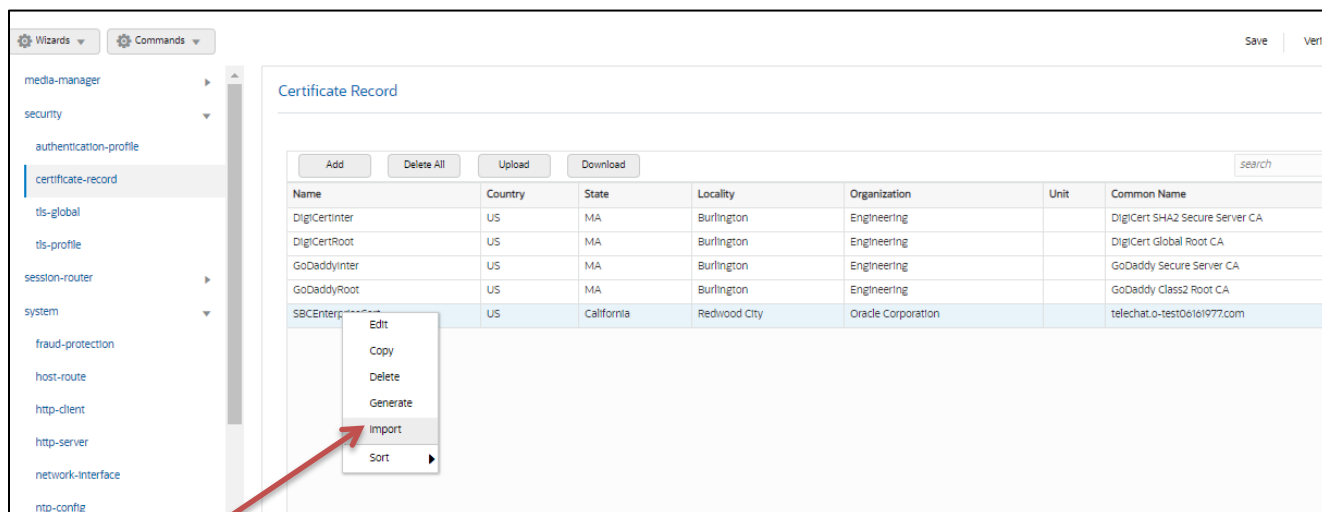
Also note, at this point, **another save and activate is required** before you can import the certificates to each certificate record created above.

Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

#### **6.4.6 Import Certificates to SBC**

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





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

- DigiCertIntermediate
- DigiCertGlobalRootCA
- DigiCertGlobalRootG2
- DigiCertGlobalRootG3

At this stage, all required certificates have been imported.

To import the certificate from ACLI follow below procedure -

```
import-certificate try-all SBCEnterpriseCert
```

The System will show a prompt as below -

**IMPORTANT:**

Please enter the certificate in the PEM format.

Terminate the certificate with ";" to exit.....

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIC4zCCAcsCAQAwazELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAK1BMRMwEQYDVQQH  
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmcluZzEkMCIGA1UEAxMbdGVs  
ZWN0eXQuby10ZXN0MDYxNjE5NzcuY29tMIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8A  
MIIBKgKCAQEAR3AmjF15PclcWiB/kFExUGNHQHlBkji28MDbcprO/KLXIHQysSnw  
UWz34XLBfLQ6rS4MLyEMR8Nt8GGNSIWkiR431LsX7L+yGWvRjcBFP6DIHtH0Vuqm  
ixVaUJpg5luPY6SvT1shyu26iLIBsLfem43tbKq5jz/jrvaUzyhICvAQ23c1oS5a  
D4UiF2mNOuSqxvmkx50a3/BNybKecLNOxvKQyyTMgffNpASbZuW+eMEUKI5iB+AB  
/AAoZRP4bn4qlE3wn8pJsNm8Pjxy4hbz24ySgmaN9iXpP1FdRw0TemfCsNazZRuK  
DsviWJfunZYTzRfDe5pJToMH4u1zt2fK1QIDAQABoDMwMQYJKoZIHvcNAQkOMSQw  
IjALBgNVHQ8EBAMCBaAwEwYDVR0IBAwWCgYIKwYBBQUHAWewDQYJKoZIHvcNAQEL  
BQADggEBADD5Y+u08LxmTMIJ2Rjc8cgPZocTqBDXN0tp27S4FuB/01ikBBdG3YV  
Ffp7/Q8ZeFHHgU/rMzeF8Gpo9Cc6JUGGux3/ws8ZkgRBxsNIG276i7pFN1vCIjEP  
89AGxtryioRmc4kcdPpLJNQ10Qx1zKobHMTftGLDI6jN2pvn3zYHH8qA9V/1/yKa  
3n0j33EuTrvTIQ5P4lgyVJqSBkdI29T1gXY6O8JVFLCQefTrF4TLc6teNzxXMdPw  
PHoPu9hM3scGOWOHQnODXOFeq2AxBQzAa0/Cjf7Bw3l3POmMclOawgDecZ8UjHpJ  
IznX9/Gxg5X+S2QkHjNmPK+JuePqX4l=
```

```
-----END CERTIFICATE REQUEST-----;
```

**save and activate** your configuration.

Repeat these steps to import all the root and intermediate CA certificates into the SBC.

#### 6.4.7 TLS Profile

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

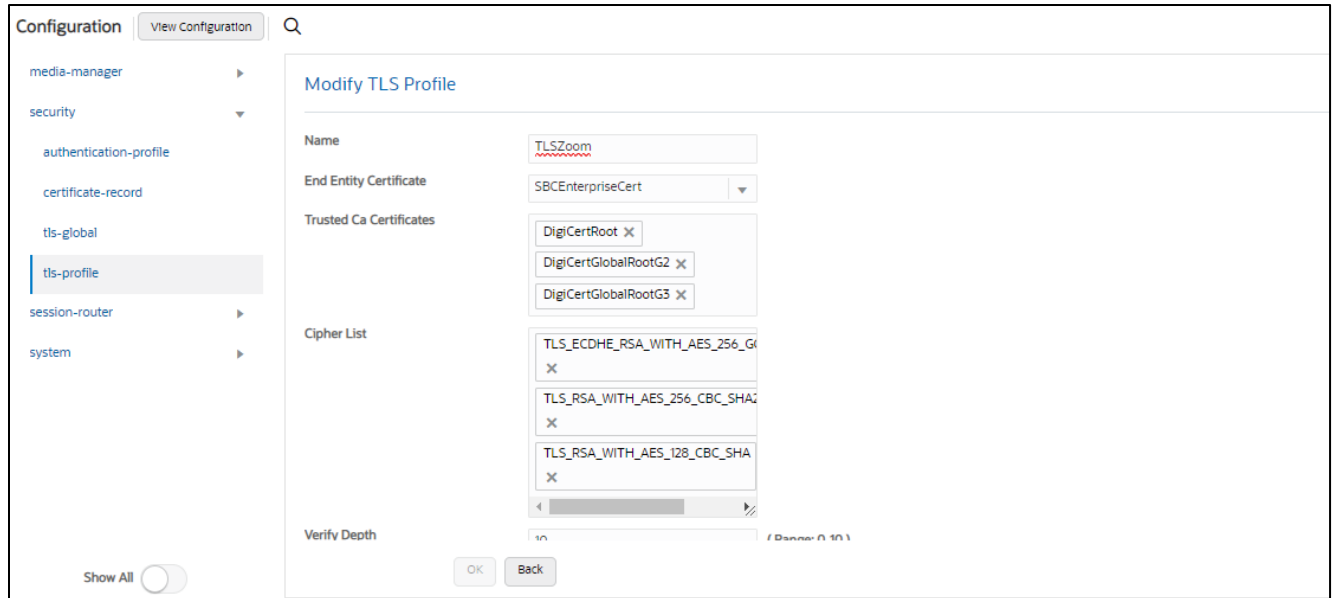
GUI Path: security/tls-profile

ACL Path: config t→security→tls-profile

- Click Add, use the example below to configure

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

**TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384**  
**TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256**  
**TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA**



- Click OK at the bottom

To configure tls-profile from ACLI –

ACLI Path: config t→security→tls-profile

|                         |                                       |
|-------------------------|---------------------------------------|
| tls-profile             |                                       |
| name                    | TLSZoom                               |
| end-entity-certificate  | SBCEnterpriseCert                     |
| trusted-ca-certificates | DigiCertRoot                          |
|                         | DigiCertGlobalRootG2                  |
|                         | DigiCertGlobalRootG3                  |
| cipher-list             | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 |
|                         | TLS_RSA_WITH_AES_256_CBC_SHA256       |
|                         | TLS_RSA_WITH_AES_128_CBC_SHA          |
| mutual-authenticate     | enabled                               |

- Perform a save and activate configuration for changes to take effect.

## 6.5 Media Security Configuration

This section outlines how to configure support for media security between the ORACLE SBC and Zoom Contact Center.

### 6.5.1 Sdes-profile

This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured.

GUI Path: security/media-security/sdes-profile

ACL Path: config t→security→media-security→sdes-profile

Oracle SBC and Zoom Contact center BYOC the following media ciphers for SRTP:

AEAD\_AES\_256\_GCM  
AES\_CM\_256\_HMAC\_SHA1\_80  
AES\_CM\_128\_HMAC\_SHA1\_80  
AES\_CM\_128\_HMAC\_SHA1\_32

Click Add, and use the example below to configure.

The screenshot displays the 'Modify Sdes Profile' configuration interface. On the left, a navigation pane lists various configuration categories, with 'sdes-profile' highlighted. The main area contains the following settings:

- Name:** SDES
- Crypto List:** AEAD\_AES\_256\_GCM, AES\_CM\_128\_HMAC\_SHA1\_32, AES\_256\_CM\_HMAC\_SHA1\_80, AES\_CM\_128\_HMAC\_SHA1\_80
- Srtp Auth:**  enable
- Srtp Encrypt:**  enable
- SRTP Encrypt:**  enable
- Mki:**  enable
- Egress Offer Format:** same-as-Ingress
- Use Ingress Session Params:** (empty field)
- Options:** (empty field)

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

- Click OK at the bottom

To configure sdes-profile from ACLI –

ACL Path: config t→security→media-security→sdes-profile

### sdes-profile

|             |   |
|-------------|---|
| name        | SDES  |
| crypto-list | AEAD_AES_256_GCM<br>AES_CM_128_HMAC_SHA1_32<br>AES_256_CM_HMAC_SHA1_80<br>AES_CM_128_HMAC_SHA1_80 |

- Perform a save and activate configuration for changes to take effect.

## 6.5.2 Media Security Policy

Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them) and, if SRTP needs to be used, the sdes-profile that needs to be used

In this example, we are configuring two media security policies. One to secure and decrypt media toward Zoom, the other for non-secure media facing PSTN.

These are named as sdesPolicy and RTP.

GUI Path: security/media-security/media-sec-policy

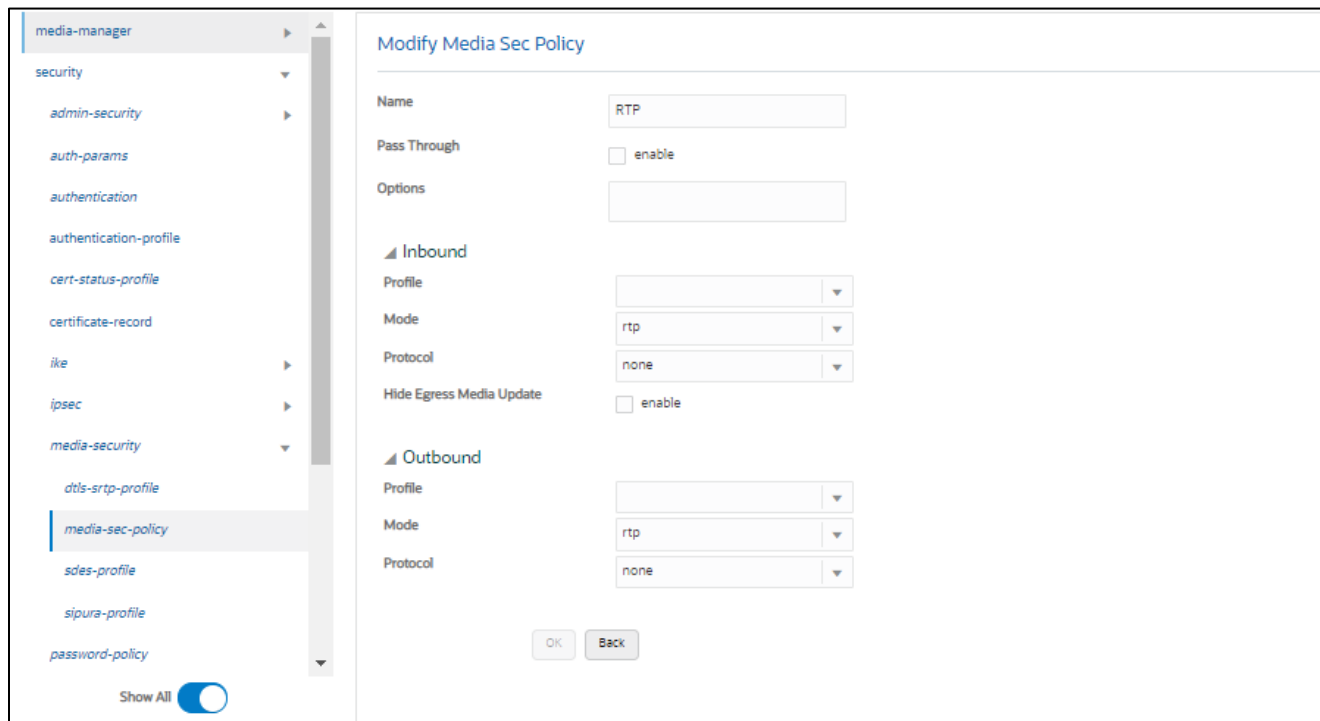
ACL Path: config t→security→media-security→media-sec-policy

- Click Add, use the examples below to configure

The screenshot displays the 'Modify Media Sec Policy' configuration interface. On the left, a navigation menu lists various configuration categories, with 'media-sec-policy' highlighted. The main configuration area is titled 'Modify Media Sec Policy' and contains the following settings:

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

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



To configure media security from ACLI.

ACLI Path: config t→security→media-security→media-sec-policy

```

media-sec-policy
  name RTP
media-sec-policy
  name sdesPolicy
  inbound
    profile SDES
    mode srtp
    protocol sdes
  outbound
    profile SDES
    mode srtp
    protocol sdes

```

- Perform a save and activate configuration for changes to take effect.

## 6.6 Media Configuration

This section will guide you through the configuration of realms and steering pools, both of which are required for the SBC to handle signaling and media flows toward Zoom and PSTN.

### 6.6.1 Realm Config

Realms are a logical distinction representing routes (or groups of routes) reachable by the Oracle Session Border Controller and what kinds of resources and special functions apply to those routes. Realms are used as a basis for determining ingress and egress associations to network interfaces.

#### Zoom Realm

This is a standalone realm facing Zoom Contact Center BYOC Platform

#### PSTN Realms

In the below example 1, Peer\_SIPTrunk1 represents the Sip realm for customer 1. Similarly another realm is created for Peer\_SIPTrunk2 which represents the Sip Trunk for customer 2. These realms are bound to different network interfaces (subnets) in this example.

GUI Path; media-manager/realm-config

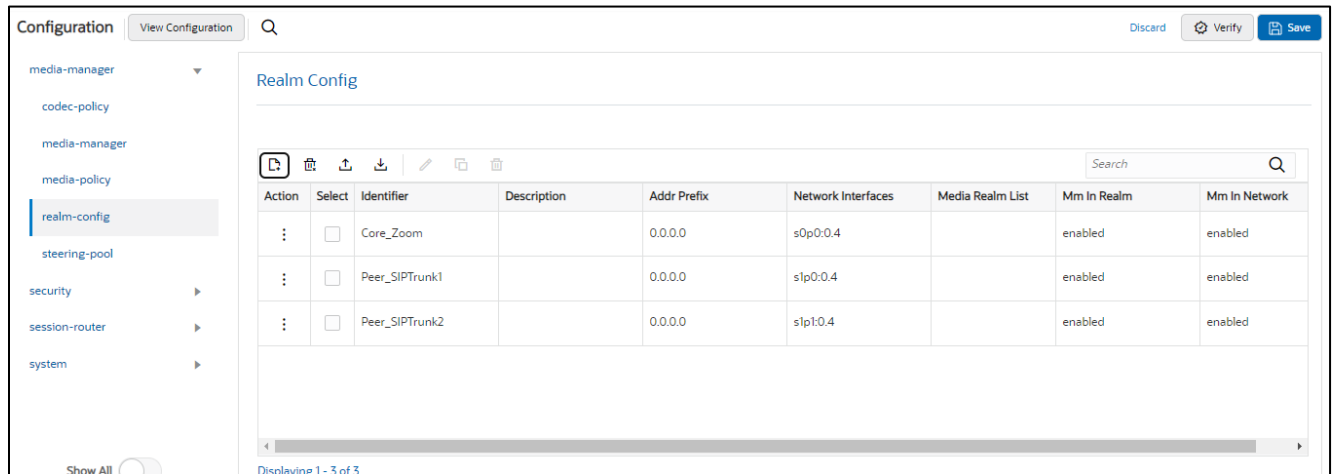
ACL Path: config t→media-manager→realm-config

- Click Add, and use the following table as a configuration example for the three realms used in this configuration example

| Config Parameter           | Zoom Contact Center BYOC            | PSTN Realm1                         | PSTN Realm2                         |
|----------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Identifier                 | Core_Zoom                           | Peer_SIPTrunk1                      | Peer_SIPTrunk2                      |
| Network Interface          | s0p0:0                              | s1p0:0                              | s1p1:0                              |
| Mm in realm                | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Access-control-trust-level | High                                | High                                | High                                |
| Media Sec policy           | sdespolicy                          | RTP                                 | RTP                                 |

Also notice, the realm configuration is where we assign some of the elements configured earlier in this document, i.e.

- Network interface
- Media security policy



To configure realm-config from ACLI –

ACLI Path - config t→media-manger→realm-config

```

realm-config
  identifier          Core_Zoom
  network-interfaces  s0p0:0.4
  mm-in-realm        enabled
  media-sec-policy    sdesPolicy
  out-manipulationid ZoomOutManip
  access-control-trust-level  high
realm-config
  identifier          Peer_SIPTrunk1
  network-interfaces  s1p0:0.4
  mm-in-realm        enabled
  media-sec-policy    RTP
  access-control-trust-level  high
realm-config
  identifier          Peer_SIPTrunk2
  network-interfaces  s1p1:0.4
  mm-in-realm        enabled
  media-sec-policy    sdesPolicy
  access-control-trust-level  high

```

- Perform a save and activate configuration for changes to take effect.



## 6.6.2 Steering Pools

Steering pools define sets of ports that are used for steering media flows through the Oracle SBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We will configure one steering pool for both PSTN Trunks and one steering pool for Zoom Contact Center BYOC

GUI Path: media-manager/steering-pool

CLI Path: config t→media-manager→steering-pool

- Click Add, and use the below examples to configure

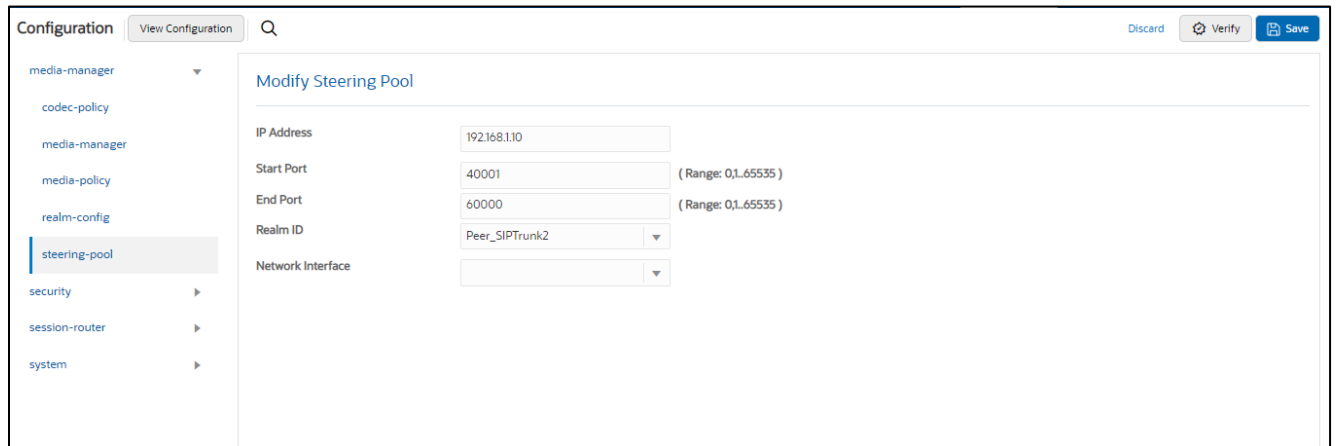
The screenshot shows the 'Modify Steering Pool' configuration page. The left sidebar contains a navigation menu with the following items: Wizards, Commands, media-manager (selected), codec-policy, media-manager, media-policy, realm-config, steering-pool (highlighted), security, session-router, and system. The main content area is titled 'Modify Steering Pool' and contains the following fields:

|                   |  |
|-------------------|--|
| IP Address        | <input type="text" value="155.212.214.177"/>         |
| Start Port        | <input type="text" value="20000"/> (Range: 1..65535) |
| End Port          | <input type="text" value="40000"/> (Range: 1..65535) |
| Realm ID          | <input type="text" value="Core_Zoom"/>               |
| Network Interface | <input type="text"/>                                 |

The screenshot shows the 'Modify Steering Pool' configuration page. The left sidebar contains a navigation menu with the following items: Configuration, View Configuration, media-manager (selected), codec-policy, media-manager, media-policy, realm-config, steering-pool (highlighted), security, session-router, and system. The main content area is titled 'Modify Steering Pool' and contains the following fields:

|                   |  |
|-------------------|--|
| IP Address        | <input type="text" value="172.18.0.201"/>            |
| Start Port        | <input type="text" value="20001"/> (Range: 0..65535) |
| End Port          | <input type="text" value="40000"/> (Range: 0..65535) |
| Realm ID          | <input type="text" value="Peer_SIPTrunk1"/>          |
| Network Interface | <input type="text"/>                                 |

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



To configure steering-pool from CLI

CLI Path: config t→media-manger→steering-pool

```

steering-pool
  ip-address      155.212.214.177
  start-port      10000
  end-port        20000
  realm-id        Core_Zoom
steering-pool
  ip-address      172.18.0.201
  start-port      20001
  end-port        40000
  realm-id        Peer_SIPTrunk1
steering-pool
  ip-address      192.168.1.10
  start-port      40001
  end-port        60000
  realm-id        Peer_SIPTrunk2

```

- Perform a save and activate configuration for changes to take effect.

## 6.7 SIP Modifications

This section outlines the configuration parameters required for processing, modifying, and securing SIP signaling traffic.

### 6.7.1 SIP Manipulations

In order to comply with the signaling message requirements of Carrier and Zoom we have applied following sip-manipulations towards Zoom Side.

**Note:** You may have to build sip-manipulations to cover the signaling requirement from Carrier Trunk.

#### 6.7.1.1 Manipulation towards Zoom Side

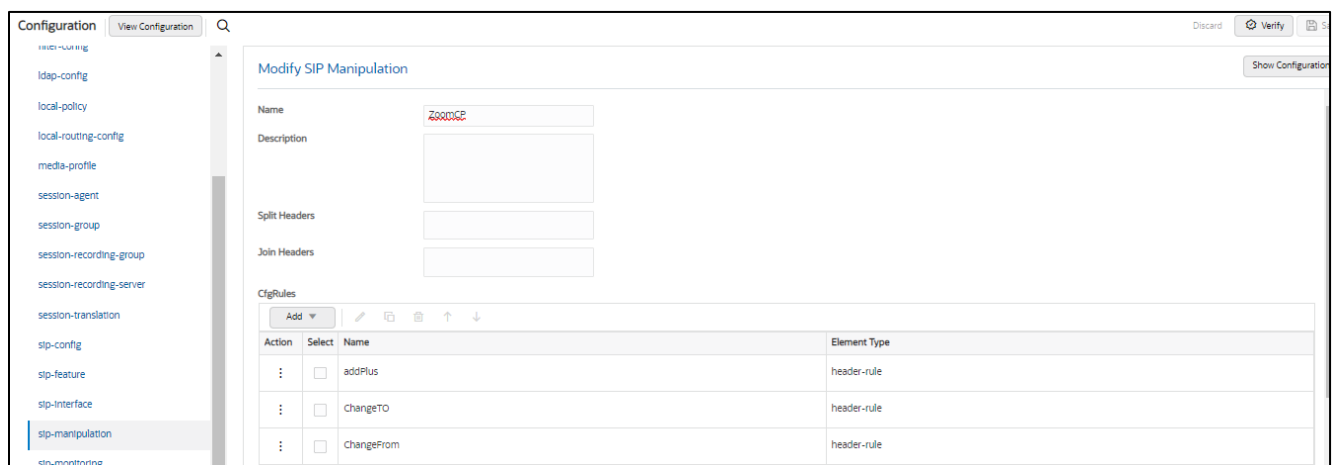
For calls to be presented to Zoom Contact Center BYOC the number must be in E.164 format for all SIP headers.

Besides, Options ping from Contact Center peering SBC to Zoom must be formatted as follows. The same formatting is to be followed for calls.

- The **“From”** header should have the IP address/FQDN of the Oracle SBC  
From: <sip:IPaddress/FQDN>
- The **“To”** header should contain the Zoom Contact Center BYOC IP address/FQDN  
To: <sip:IPaddressofZoomSBC>
- The **“Request URI”** header must contain the Zoom Contact Center BYOC IP address/FQDN
- The **“Contact”** header must have the IP address/FQDN of the Oracle SBC  
Contact: [sip:IPaddress/FQDN:PortNumber](#)

To achieve this we have created following Header manipulation rule on Oracle SBC.

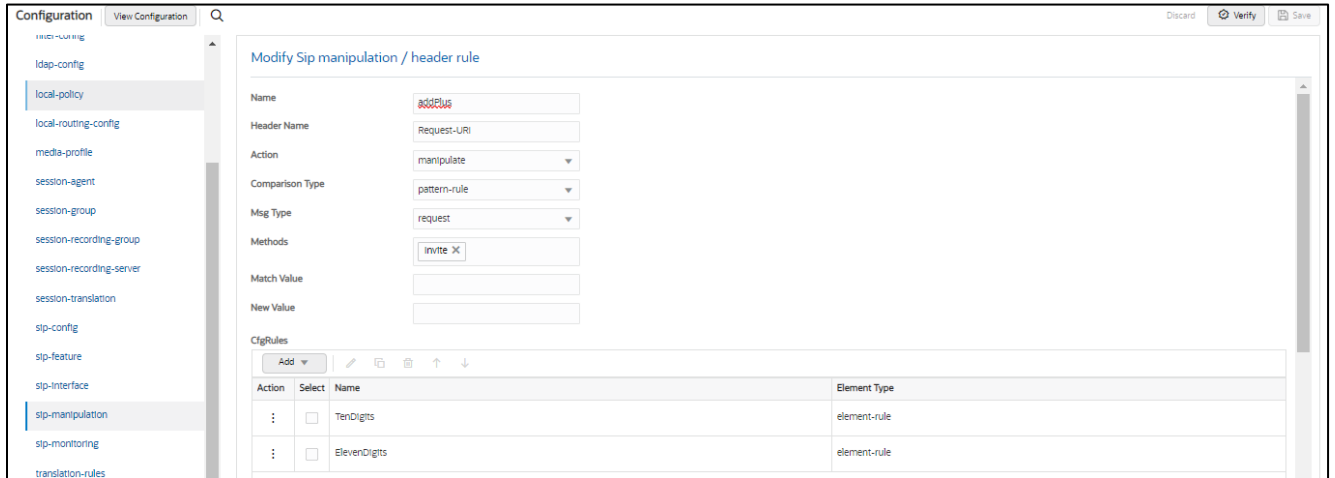
#### Sip-manipulation :



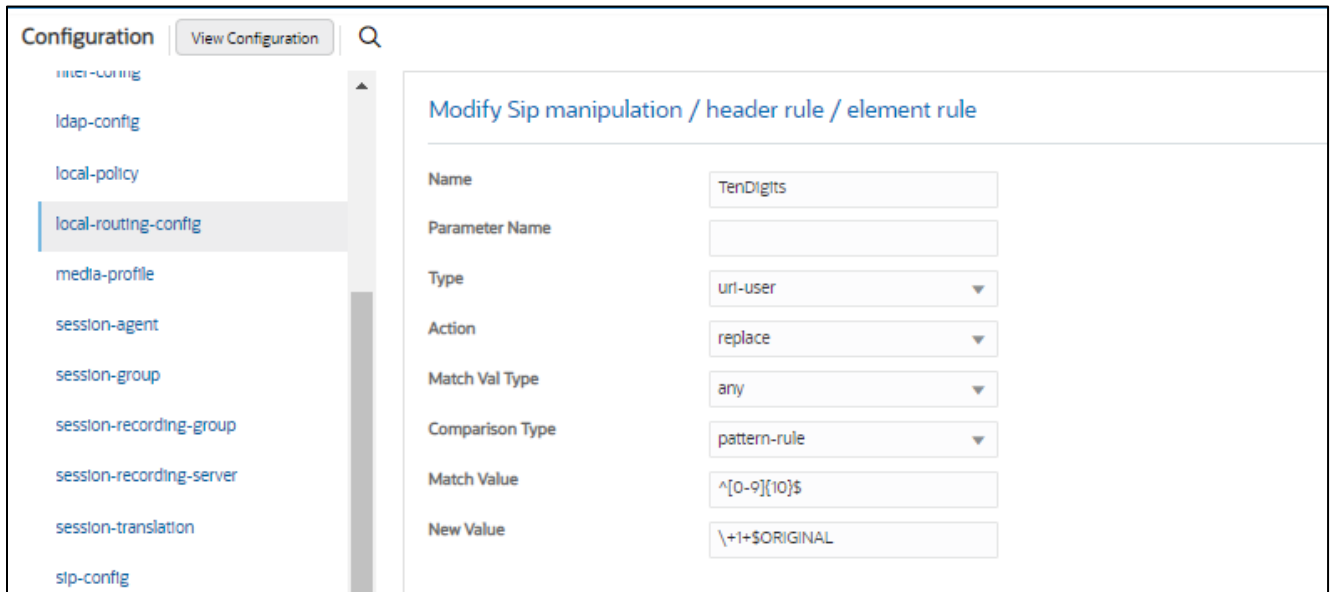
The screenshot shows the 'Modify SIP Manipulation' configuration page. The 'Name' field is set to 'ZoomSBC'. Below the 'Split Headers' and 'Join Headers' fields, there is a table for 'CfgRules'.

| Action | Select                   | Name       | Element Type |
|--------|--------------------------|------------|--------------|
| :      | <input type="checkbox"/> | addPlus    | header-rule  |
| :      | <input type="checkbox"/> | ChangeTO   | header-rule  |
| :      | <input type="checkbox"/> | ChangeFrom | header-rule  |

#### Header-rule #1



Element-rule # 1.1



Element-rule #1.2

Configuration View Configuration Q

local-routing

ldap-config

local-policy

local-routing-config

media-profile

session-agent

session-group

session-recording-group

session-recording-server

session-translation

sip-config

### Modify Sip manipulation / header rule / element rule

Name: ElevenDigits

Parameter Name:

Type: uri-user

Action: replace

Match Val Type: any

Comparison Type: pattern-rule

Match Value:  $^{[0-9]{11}}$$

New Value: \++\$ORIGINAL

## Header-rule #2

Configuration View Configuration Q Discard Verify Save

local-routing

ldap-config

local-policy

local-routing-config

media-profile

session-agent

session-group

session-recording-group

session-recording-server

session-translation

stp-config

stp-feature

stp-interface

stp-manipulation

stp-monitoring

translation-rules

system

### Modify Sip manipulation / header rule

Name: ~~ChangeToPort~~

Header Name: TO

Action: manipulate

Comparison Type: case-sensitive

Msg Type: request

Methods:

Match Value:

New Value:

CfgRules

| Action | Select                   | Name         | Element Type |
|--------|--------------------------|--------------|--------------|
| :      | <input type="checkbox"/> | changetohost | element-rule |
| :      | <input type="checkbox"/> | ChangeToPort | element-rule |

## Element-rule #2.1

Configuration View Configuration Q

[local-routing](#)  
[ldap-config](#)  
[local-policy](#)  
[local-routing-config](#)  
[media-profile](#)  
[session-agent](#)  
[session-group](#)  
[session-recording-group](#)  
[session-recording-server](#)  
[session-translation](#)  
[sip-config](#)  
[sip-feature](#)

### Modify Sip manipulation / header rule / element rule

|                 |   |
|-----------------|---|
| Name            | <input type="text" value="changetohost"/>   |
| Parameter Name  | <input type="text"/>                        |
| Type            | <input type="text" value="url-host"/>       |
| Action          | <input type="text" value="replace"/>        |
| Match Val Type  | <input type="text" value="any"/>            |
| Comparison Type | <input type="text" value="case-sensitive"/> |
| Match Value     | <input type="text"/>                        |
| New Value       | <input type="text" value="\$REMOTE_IP"/>    |

### Element-rule #2.2

Configuration View Configuration Q

[local-routing](#)  
[ldap-config](#)  
[local-policy](#)  
[local-routing-config](#)  
[media-profile](#)  
[session-agent](#)  
[session-group](#)  
[session-recording-group](#)  
[session-recording-server](#)  
[session-translation](#)  
[sip-config](#)  
[sip-feature](#)

### Modify Sip manipulation / header rule / element rule

|                 |   |
|-----------------|---|
| Name            | <input type="text" value="ChangeToPort"/>   |
| Parameter Name  | <input type="text"/>                        |
| Type            | <input type="text" value="url-port"/>       |
| Action          | <input type="text" value="replace"/>        |
| Match Val Type  | <input type="text" value="any"/>            |
| Comparison Type | <input type="text" value="case-sensitive"/> |
| Match Value     | <input type="text"/>                        |
| New Value       | <input type="text" value="5061"/>           |

### Header-rule #3

Configuration View Configuration Q Discard Verify

Modify Sip manipulation / header rule

Name:

Header Name:

Action:

Comparison Type:

Msg Type:

Methods:

Match Value:

New Value:

CfgRules

| Action | Select                   | Name           | Element Type |
|--------|--------------------------|----------------|--------------|
| :      | <input type="checkbox"/> | ChangeFromHost | element-rule |
| :      | <input type="checkbox"/> | ChangeFromPort | element-rule |

### Element-rule #3.1

Configuration View Configuration Q

Modify Sip manipulation / header rule / element rule

Name:

Parameter Name:

Type:

Action:

Match Val Type:

Comparison Type:

Match Value:

New Value:

### Element-rule #3.2

Configuration View Configuration Q

- h3c-ctrl
- ldap-config
- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config

### Modify Sip manipulation / header rule / element rule

|                 |   |
|-----------------|---|
| Name            | <input type="text" value="ChangeFromPort"/> |
| Parameter Name  | <input type="text"/>                        |
| Type            | <input type="text" value="url-port"/>       |
| Action          | <input type="text" value="replace"/>        |
| Match Val Type  | <input type="text" value="any"/>            |
| Comparison Type | <input type="text" value="case-sensitive"/> |
| Match Value     | <input type="text"/>                        |
| New Value       | <input type="text" value="5061"/>           |

To configure the sip-manipulation from ACLI,

Navigate to config t→session-router→sip-manipulation



```

sip-manipulation
  name          ZoomCP
  header-rule
    name        addPlus
    header-name Request-URI
    action      manipulate
    comparison-type pattern-rule
    msg-type    request
    methods     Invite
    element-rule
      name      TenDigits
      type      uri-user
      action    replace
      comparison-type pattern-rule
      match-value ^[0-9]{10}$
      new-value  \+1+$ORIGINAL
    element-rule
      name      ElevenDigits
      type      uri-user
      action    replace
      comparison-type pattern-rule
      match-value ^[0-9]{11}$
      new-value  \++$ORIGINAL
  header-rule
    name        ChangeTO
    header-name TO
    action      manipulate
    msg-type    request
    methods     Invite
    element-rule
      name      changetohost
      type      uri-host
      action    replace
      new-value $REMOTE_IP
    element-rule
      name      ChangeToPort
      type      uri-port
      action    replace
      new-value 5061
  header-rule
    name        ChangeFrom
    header-name From
    action      manipulate
    msg-type    request
    methods     Invite
  element-rule
    name        ChangeFromHost
    type        uri-host
    action      replace
    new-value   20.96.25.165
    element-rule
      name      ChangeFromPort
      type      uri-port
      action    replace
      new-value 5061

```

### 6.7.1.2 Responding to Options Ping

The ping response parameter can be enabled on the Session Agents to locally respond to the OPTIONS ping sent towards SBC from Zoom and Carrier.

The screenshot shows the 'Modify Session Agent' configuration interface. The left sidebar lists various configuration categories, with 'session-agent' highlighted. The main configuration area includes the following fields and settings:

- SPL Options: [Empty text field]
- Media Profiles: [Empty text field]
- In Translationid: [Empty dropdown menu]
- Out Translationid: [Dropdown menu with 'addPlus' selected]
- Trust Me:  enable
- Local Response Map: [Empty dropdown menu]
- Ping Response:  enable
- In Manipulationid: [Dropdown menu with 'RespondOPTIONS' selected]
- Out Manipulationid: [Dropdown menu with 'ZoomManipulation' selected]
- Manipulation String: [Empty text field]
- Manipulation Pattern: [Empty text field]

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

To enable ping-response from ACLI-

```
SolutionsLab-vSBC-2(session-agent)# ping-response enabled
```

- Perform a save and activate configuration for changes to take effect.

### 6.7.2 Session-Translation

The following session-translation is created and applied as out-translationid on the Session-Agent towards Carriers. This session-translation is created to remove +1 when call is sent towards Carrier as Carrier in this case requires calls to be presented in 10 digit dial format.

GUI Path: session-router/session-translation

ACLI Path: config t → session-router → session-translation

- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- stp-config
- stp-feature
- stp-interface
- stp-manipulation
- stp-monitoring
- translation-rules
- system

Show All

### Modify Session Translation

|                   |   |
|-------------------|---|
| Id                | <input type="text" value="removeE164"/>   |
| Rules Calling     | <input type="text" value="removeplus1"/> <span style="font-size: 0.8em;">✕</span> |
| Rules Called      | <input type="text" value="removeplus1"/> <span style="font-size: 0.8em;">✕</span> |
| Rules Asserted Id | <input type="text" value="removeplus1"/> <span style="font-size: 0.8em;">✕</span> |
| Rules Redirect    | <input type="text"/>  |
| Rules Isup Cdpn   | <input type="text"/>  |
| Rules Isup Cgpn   | <input type="text"/>  |
| Rules Isup Gn     | <input type="text"/>  |
| Rules Isup Rdn    | <input type="text"/>  |
| Rules Isup Ocn    | <input type="text"/>  |

- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group
- session-recording-group
- session-recording-server
- session-translation
- stp-config
- stp-feature
- stp-interface
- stp-manipulation
- stp-monitoring
- translation-rules
- system

Show All

### Modify Translation Rules

|               |  |
|---------------|--|
| Id            | <input type="text" value="removeplus1"/>                             |
| Type          | <input type="text" value="delete"/>                                  |
| Add String    | <input type="text"/>   |
| Add Index     | <input type="text" value="0"/>                                       |
| Delete String | <input type="text" value="+1"/>                                      |
| Delete Index  | <input type="text" value="0"/> <small>( Range: 0..99999999 )</small> |

To configure session-translation from ACLI

```

session-translation
  id                removeE164
  rules-calling     removeplus1
  rules-called      removeplus1
  rules-asserted-id removeplus1
translation-rules
  id                removeplus1
  type              delete
  delete-string     +1

```

- Perform a save and activate configuration for changes to take effect.

## 6.8 SIP Interface

The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages

Configure two SIP interfaces, one associated with PSTN Realm, and the other for Zoom Contact Center BYOC.

GUI Path: session-router/SIP-interface

ACL Path: config t→session-router→sip-interface

Click Add, and use the table below as an example to Configure:

Please note, this is also where we will be assigned some of the configuration elements configured earlier in this document, i.e.

- TLS Profile
- Session-timer-profile
- SIP-Manipulations

Use the following as an example to configure SIP interfaces:

| Config Parameter   | Zoom      | SIPTrunk       | SIPTrunk       |
|--------------------|-----------|----------------|----------------|
| Realm ID           | Core_Zoom | Peer_SIPTrunk1 | Peer_SIPTrunk2 |
| Out manipulationid | ZoomCP    |                |                |

| SIP Port Config Parmeter | Zoom            | SIP Trunk    | SIP Trunk    |
|--------------------------|-----------------|--------------|--------------|
| Address                  | 155.212.214.177 | 172.18.0.201 | 192.168.1.10 |
| Port                     | 5061            | 5060         | 5060         |
| Transport protocol       | TLS             | UDP          | UDP          |
| TLS profile              | TLSZoom         |              |              |
| Allow anonymous          | agents-only     | agents-only  | agents-only  |

Configuration View Configuration Q Discard Verify Save

session-group  
 session-recording\_group  
 session-recording-server  
 session-translation  
 sip-config  
 sip-feature  
 sip-interface  
 sip-manipulation  
 sip-monitoring  
 translation-rules

Show All

### SIP Interface

Search

| Action | Select                   | State   | Realm ID       | Description | Carriers | Trans Expire | Initial Inv Trans Expire |
|--------|--------------------------|---------|----------------|-------------|----------|--------------|--------------------------|
| :      | <input type="checkbox"/> | enabled | Core_Zoom      |             |          |              | 0                        |
| :      | <input type="checkbox"/> | enabled | Peer_SIPTrunk1 |             |          |              | 0                        |
| :      | <input type="checkbox"/> | enabled | Peer_SIPTrunk2 |             |          |              | 0                        |

Displaying 1 - 3 of 3

```

sip-interface
  realm-id          Core_Zoom
  description       Interface for Zoom Phone
  sip-port
    address         155.212.214.177
    port            5061
    transport-protocol TLS
    tls-profile      TLSZoom
    allow-anonymous agents-only
  out-manipulationid ACME_NAT_TO_FROM_IP
  sip-profile        fireplaces
  session-timer-profile ZoomSessionTimer
sip-interface
  realm-id          Peer_SIPTrunk1
  sip-port
    address         172.18.0.201
    allow-anonymous agents-only
sip-interface
  realm-id          Peer_SIPTrunk2
  sip-port
    address         192.168.1.10
    allow-anonymous agents-only

```

## 6.9 Session Agents

Session Agents are configuration elements which are trusted agents that can both send and receive traffic from the ORACLE SBC with direct access to the trusted data path.

GUI Path: session-router/session-agent

ACLI Path: config t→session-router→session-agent

You will need to configure session agents for Zoom Contact Center BYOC and both Carrier SIP Trunks.

**Note:** In this configuration example we have used Zoom Contact Center BYOC Session Agents for North America Region. You will be required to configure Zoom Contact Center BYOC Session Agents as per your specific region.

Contact your Zoom representative for detailed list of Zoom IP Addresses.

- Click Add, and use the table below to configure:

| Config parameter | Zoom CC SA1              | Zoom CC SA2              | SIPTrunk1      | SIPTrunk2      |
|------------------|--------------------------|--------------------------|----------------|----------------|
| Hostname         | us01zccpeer01.sc.zoom.us | us01zccpeer01.dv.zoom.us | 172.18.0.210   | 192.168.1.20   |
| IP Address       | 204.80.108.250           | 50.239.204.250           | 172.18.0.210   | 192.168.1.20   |
| Port             | 5061                     | 5060                     | 5060           | 5060           |
| Transport method | StaticTLS                | UDP+TCP                  | UDP+TCP        | UDP+TCP        |
| Realm ID         | Core_Zoom                | Peer_SIPTrunk1           | Peer_SIPTrunk1 | Peer_SIPTrunk2 |
| Ping Method      | OPTIONS                  | OPTIONS                  | OPTIONS        | OPTIONS        |
| Ping Interval    | 30                       | 30                       | 30             | 30             |
| Ping Response    | Enabled                  | Enabled                  | Enabled        | Enabled        |

The screenshot shows a configuration page titled "Session Agent" with a table of configurations. The table has columns for Action, Select, Hostname, IP Address, Port, State, App Protocol, Realm ID, and Description. There are three rows of data, each with a colon in the Action column and a checkbox in the Select column.

| Action | Select                   | Hostname      | IP Address    | Port | State   | App Protocol | Realm ID       | Description |
|--------|--------------------------|---------------|---------------|------|---------|--------------|----------------|-------------|
| :      | <input type="checkbox"/> | 172.18.0.210  | 172.18.0.210  | 5060 | enabled | SIP          | Peer_SIPTrunk1 |             |
| :      | <input type="checkbox"/> | 192.168.1.20  | 192.168.1.10  | 5060 | enabled | SIP          | Peer_SIPTrunk2 |             |
| :      | <input type="checkbox"/> | 69174.108.135 | 69174.108.135 | 5061 | enabled | SIP          | Core_Zoom      |             |

- Hit the OK tab at the bottom of each when applicable

session-agent  
hostname us01zccpeer01.sc.zoom.us  
ip-address 204.80.108.250  
port 5061  
transport-method StaticTLS  
realm-id Core\_Zoom  
ping-method OPTIONS  
ping-interval 30  
ping-response enabled

session-agent  
hostname us01zccpeer01.dv.zoom.us  
ip-address 50.239.204.250  
port 5061  
transport-method StaticTLS  
realm-id Core\_Zoom  
ping-method OPTIONS  
ping-interval 30  
ping-response enabled

session-agent  
hostname 172.18.0.210  
ip-address 172.18.0.210  
transport-method UDP+TCP  
realm-id Peer\_SIPTrunk1  
ping-method OPTIONS  
ping-interval 30  
ping-response enabled

session-agent  
hostname 192.168.1.20  
ip-address 192.168.1.20  
transport-method UDP+TCP  
realm-id Peer\_SIPTrunk2  
ping-method OPTIONS  
ping-interval 30  
ping-response enabled



- Perform a save and activate configuration for changes to take effect.

## 6.10 Routing Configuration

This section outlines how to configure the Oracle SBC to route SIP traffic to and from PSTN Trunks and Zoom Contact Center BYOC Platform.

The Oracle SBC has multiple routing options that can be configured based on environment. For the purpose of this example configuration, we are utilizing the Oracle SBC's Local Policy Routing for all traffic to and from Zoom.

### 6.10.1 Local Policy Configuration

Local Policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria.

GUI Path: session-router/local-policy

ACL Path: config t→session-router→local-policy

**Note :** Having more than one PSTN Carrier terminated onto the SBC is optional as only one carrier trunk is required to terminate BYOC calls to and from Zoom Contact Center.

#### 6.12.1.1 Route Calls from Zoom To Customer 1:

Calls originating from Zoom Contact Center BYOC System are routed to carrier trunk for PSTN termination. Here in this example we DID 7692105055 belongs to Carrier 1 hence all calls originating from Zoom Contact Center BYOC System from DID 7692105055 are routed to Carrier 1 Sip Trunk i.e. 172.18.0.210 through realm Peer\_SIPTrunk1

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The main configuration area is titled 'Modify Local Policy'. It contains the following fields:

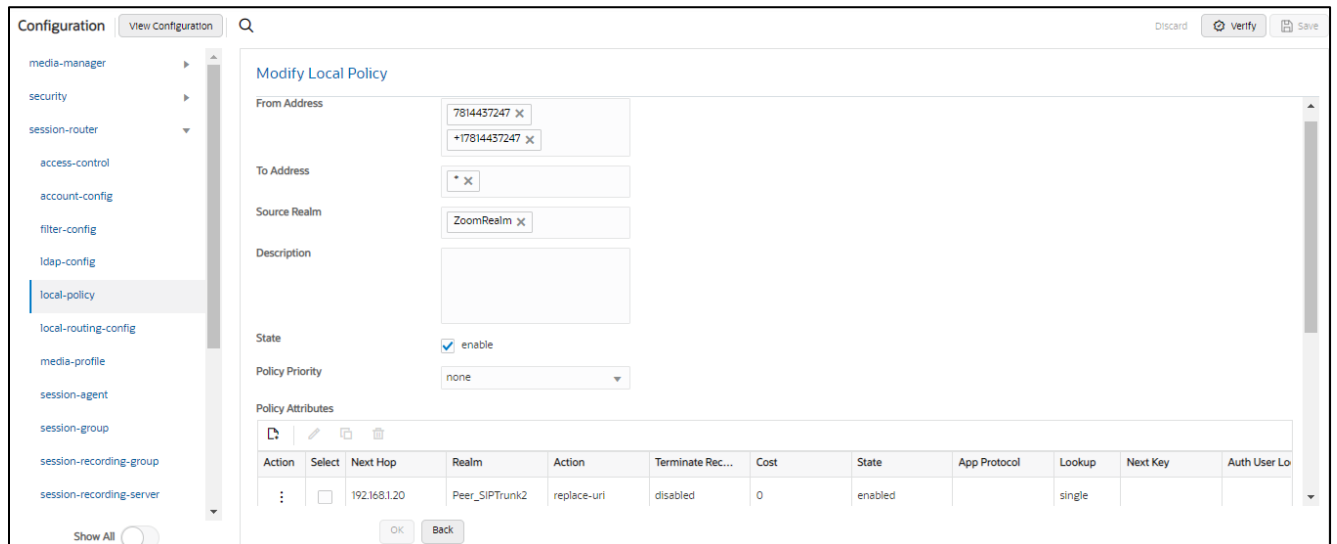
- From Address:** 7692105055 x, +17692105055 x
- To Address:** \* x
- Source Realm:** ZoomRealm x
- Description:** (empty)
- State:**  enable
- Policy Priority:** none

Below these fields is a table for 'Policy Attributes':

| Action | Select                   | Next Hop     | Realm          | Action      | Terminate Re... | Cost | State   | App Protocol | Lookup | Next Key | Auth User Lo... |
|--------|--------------------------|--------------|----------------|-------------|-----------------|------|---------|--------------|--------|----------|-----------------|
| :      | <input type="checkbox"/> | 172.18.0.210 | Peer_SIPTrunk1 | replace-uri | disabled        | 0    | enabled |              | single |          |                 |

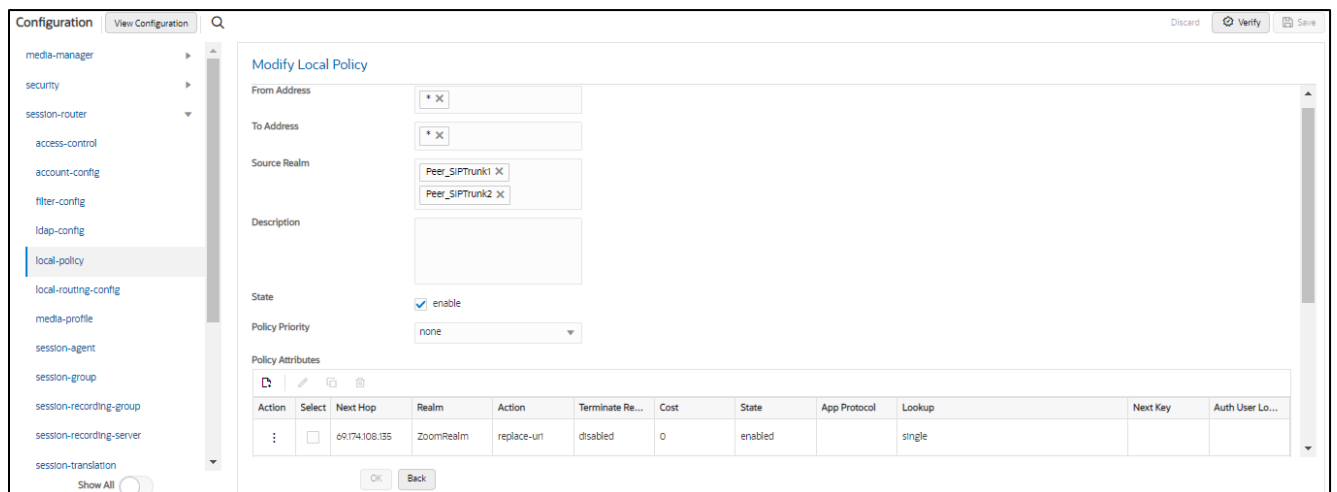
#### 6.12.1.2 Route Calls from Zoom To Customer 2:

Similarly, in below example DID 7814437247 belongs to Carrier2 hence all calls originating from Zoom Contact Center BYOC System from DID 7814437247 are routed to Carrier 2 Sip Trunk i.e. 192.168.1.20 through realm Peer\_SIPTrunk2



### 6.12.1.3 Route Calls from Sip Trunks to Zoom:

Below local policies route all the Calls from Peer\_SIPTrunk1 and Peer\_SIPTrunk2 to Zoom Contact Center BYOC System. The calls with terminate onto the Zoom Contact Flow that has an entry point with the DID.



To configure local-policy from CLI

```

local-policy
  from-address      7692105055
                   +17692105055
  to-address        *
  source-realm      Core_Zoom
  policy-attribute
    next-hop        172.18.0.210
    realm            Peer_SIPTrunk1
    action           replace-uri
local-policy
  from-address      7814437247
                   +17814437247
  to-address        *
  source-realm      Core_Zoom
  policy-attribute
    next-hop        192.168.1.20
    realm            Peer_SIPTrunk2
    action           replace-uri
local-policy
  from-address      *
  to-address        *
  source-realm      Peer_SIPTrunk1 Peer_SIPTrunk2

  policy-attribute
    next-hop        162.12.233.60
    realm            Core_Zoom
    action           replace-uri

```

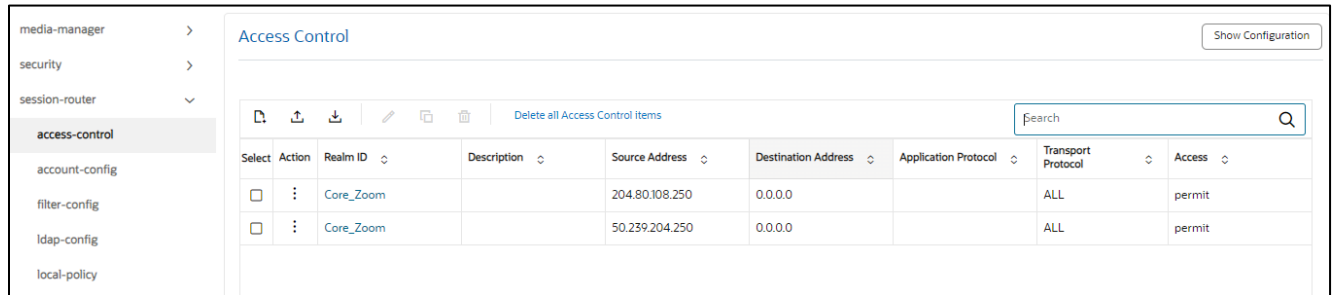
## 6.11 Access Controls

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

GUI Path: session-router/access-control

ACLI Path: config t→session-router→access-control

Please use the example below to configure access controls in your environment for rest of the Zoom IP's, as well as SIPTrunk IP's (if applicable).



- Click OK at the bottom

Save and activate your configuration.

To configure access-control from ACLI, Navigate to -

config t → session-router → access-control

```

access-control
  realm-id          Core_Zoom
  source-address    204.80.108.250
  application-protocol SIP
  trust-level       high
access-control
  realm-id          Core_Zoom
  source-address    50.239.204.250
  application-protocol SIP
  trust-level       high
  
```

Similarly create access controls for Sip Trunks if required.

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

## 6.12 SBC Behind NAT SPL configuration

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

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

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

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

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

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

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

HeaderNatPublicSIPIfIp=52.151.236.203,HeaderNatPrivateSIPIfIp=10.0.4.4,Here 52.151.236.203 is an example value and should be your public IP address.

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

The screenshot shows the 'Modify Realm Config' page in a management console. The left sidebar contains a navigation menu with the following items: media-manager, codec-policy, media-manager, media-policy, realm-config (highlighted), steering-pool, security, session-router, and system. The main content area is titled 'Modify Realm Config' and contains the following configuration options:

- Early Media Allow: [Dropdown menu]
- Enforcement Profile: [Dropdown menu]
- Additional Prefixes: [Text input field]
- Restricted Latching: [Dropdown menu with value 'none']
- Options: [Text input field]
- SPL Options: [Text input field with value 'HeaderNatPublicSIPIfIp=52.151.236.20']
- Delay Media Update: [Checkbox 'enable']
- Refer Call Transfer: [Dropdown menu with value 'disabled']
- Hold Refer Reinvite: [Checkbox 'enable']
- Refer Notify Provisional: [Dropdown menu with value 'none']
- Dyn Refer Term: [Checkbox 'enable']
- Codecs Policy: [Text input field]

At the bottom of the configuration area, there are two buttons: 'OK' and 'Back'. A 'Show All' toggle is located at the bottom left of the sidebar.

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

## 7. ACLI Running Configuration

```
access-control
  access-control
    realm-id          Core_Zoom
    source-address    204.80.108.250
    trust-level       high
access-control
  access-control
    realm-id          Core_Zoom
    source-address    50.239.204.250
    trust-level       high
access-control
  access-control
    realm-id          Peer_SIPTrunk1
    source-address    172.18.0.210
    destination-address 172.18.0.201
    application-protocol SIP
    trust-level       high
access-control
  access-control
    realm-id          Peer_SIPTrunk2
    source-address    192.168.1.20
    destination-address 192.168.1.10
    application-protocol SIP
    trust-level       high
certificate-record
  name                DigiCertGlobalRootCA
  common-name          DigiCertGlobalRootCA
certificate-record
  name                DigiCertGlobalRootG2
  common-name          DigiCertGlobalRootG2
certificate-record
  name                DigiCertGlobalRootG3
  common-name          DigiCertGlobalRootG3
certificate-record
  name                DigiCertInter
  common-name          DigiCert SHA2 Secure Server CAcertificate-record
certificate-record
  name                SBCEnterpriseCert
  state                California
```

```

locality                Redwood City
organization            Oracle Corporation
unit                   Oracle CGBU
common-name             telechat.o-test06161977.com
extended-key-usage-list serverAuth
                        ClientAuth
codec-policy
  name                  OptimizeCodecs
  allow-codecs          * G722:no PCMA:no CN:no SIREN:no RED:no G729:no
  add-codecs-on-egress PCMU
filter-config
  name                  all
  user                  *
local-policy
  from-address          7692105055
                        +17692105055
  to-address            *
  source-realm          Core_Zoom
  policy-attribute
    next-hop            172.18.0.210
    realm               Peer_SIPTrunk1
    action               replace-uri
local-policy
  from-address          7814437247
                        +17814437247
  to-address            *
  source-realm          Core_Zoom
  policy-attribute
    next-hop            192.168.1.20
    realm               Peer_SIPTrunk2
    action               replace-uri
local-policy
  from-address          *
  to-address            *
  source-realm          Peer_SIPTrunk1
  policy-attribute
    next-hop            162.12.233.60

```

|                         |                                 |
|-------------------------|---------------------------------|
| realm                   | Core_Zoom                       |
| action                  | replace-uri                     |
| local-policy            |                                 |
| from-address            | *                               |
| to-address              | *                               |
| source-realm            | Peer_SIPTrunk2                  |
| policy-attribute        |                                 |
| next-hop                | 162.12.233.60                   |
| realm                   | Core_Zoom                       |
| action                  | replace-uri                     |
| media-manager           |                                 |
| max-untrusted-signaling | 1                               |
| min-untrusted-signaling | 1                               |
| media-sec-policy        |                                 |
| name                    | RTP                             |
| media-sec-policy        |                                 |
| name                    | sdesPolicy                      |
| inbound                 |                                 |
| profile                 | SDES                            |
| mode                    | srtplib                         |
| protocol                | sdes                            |
| outbound                |                                 |
| profile                 | SDES                            |
| mode                    | srtplib                         |
| protocol                | sdes                            |
| network-interface       |                                 |
| name                    | s0p0                            |
| ip-address              | 155.212.214.177                 |
| netmask                 | 255.255.255.192                 |
| gateway                 | 155.212.214.1                   |
| dns-ip-primary          | 8.8.8.8                         |
| dns-domain              | solutionslab.cgbuburlington.com |
| network-interface       |                                 |
| name                    | s1p0                            |
| ip-address              | 172.18.0.201                    |
| netmask                 | 255.255.0.0                     |
| gateway                 | 172.18.0.1                      |



```

network-interface
  name          s1p1
  ip-address    192.168.1.10
  netmask      255.255.255.0
  gateway      192.168.1.1
ntp-config
  server        198.55.111.50
               206.108.0.131
phy-interface
  name          s0p0
  operation-type Media
phy-interface
  name          s1p0
  operation-type Media
  port          2
phy-interface
  name          s1p1
  operation-type Media
  port          3
realm-config
  identifier    Core_Zoom
  network-interfaces s0p0:0.4
  mm-in-realm  enabled
  media-sec-policy sdesPolicy
  out-manipulationid ZoomOutManip
  access-control-trust-level high
realm-config
  identifier    Peer_SIPTrunk1
  network-interfaces s1p0:0.4
  mm-in-realm  enabled
  media-sec-policy RTP
  access-control-trust-level high
realm-config
  identifier    Peer_SIPTrunk2
  network-interfaces s1p1:0.4
  mm-in-realm  enabled
  media-sec-policy sdesPolicy

```

```

    access-control-trust-level      high
sdes-profile
  name                            SDES
  crypto-list                      AEAD_AES_256_GCM
                                  AES_CM_128_HMAC_SHA1_32
                                  AES_256_CM_HMAC_SHA1_80
                                  AES_CM_128_HMAC_SHA1_80
session-agent
  hostname                        us01zccpeer01.sc.zoom.us
  ip-address                      204.80.108.250
  port                            5061
  transport-method                StaticTLS
  realm-id                        Core_Zoom
  ping-method                     OPTIONS
  ping-interval                   30
  ping-response                   enabled
session-agent
  hostname                        us01zccpeer01.dv.zoom.us
  ip-address                      50.239.204.250
  port                            5061
  transport-method                StaticTLS
  realm-id                        Core_Zoom
  ping-method                     OPTIONS
  ping-interval                   30
  ping-response                   enabled
session-agent
  hostname                        172.18.0.210
  ip-address                      172.18.0.210
  transport-method                UDP+TCP
  realm-id                        Peer_SIPTrunk1
  ping-method                     OPTIONS
  ping-interval                   30
  ping-response                   enabled
  rfc2833-mode                    preferred
  rfc2833-payload                 101
session-agent
  hostname                        192.168.1.20

```

```

ip-address          192.168.1.20
transport-method    UDP+TCP
realm-id            Peer_SIPTrunk2
ping-method         OPTIONS
ping-interval       30
ping-response       enabled
session-translation
  id                addPlus
  rules-calling     addPlus
  rules-called      addPlus
session-translation
  id                removeE164
  rules-calling     removeplus1
  rules-called      removeplus1
  rules-asserted-id removeplus1
SIP-config
  home-realm-id     Core_Zoom
  registrar-domain  *
  registrar-host    *
  registrar-port    5060
  options           inmanip-before-validate
                   max-udp-length=0
  extra-method-stats enabled
sip-interface
  realm-id          Core_Zoom
  description       Inerface for Zoom Contact Center BYOC
  sip-port
    address         155.212.214.177
    port            5061
    transport-protocol TLS
    tls-profile     TLSZoom
    allow-anonymous agents-only
  out-manipulationid ACME_NAT_TO_FROM_IP
  sip-profile        forreplaces
  session-timer-profile ZoomSessionTimer
sip-interface
  realm-id          Peer_SIPTrunk1

```

```

sip-port
  address          172.18.0.201
  allow-anonymous  agents-only
sip-interface
  realm-id        Peer_SIPTrunk2
  sip-port
    address       192.168.1.10
    allow-anonymous agents-only
sip-manipulation
  name            RespondOPTIONS
  header-rule
    name          Respond2OPTIONS
    header-name   from
    action        reject
    methods       OPTIONS
    new-value     "200 OK"

SIP-monitoring
  match-any-filter  enabled
  monitoring-filters *

steering-pool
  ip-address       155.212.214.177
  start-port       10000
  end-port         20000
  realm-id        Core_Zoom

steering-pool
  ip-address       172.18.0.201
  start-port       20001
  end-port         40000
  realm-id        Peer_SIPTrunk1

steering-pool
  ip-address       192.168.1.10
  start-port       40001
  end-port         60000
  realm-id        Peer_SIPTrunk2

system-config
  hostname         zoom.us

```

|                         |                                       |
|-------------------------|---------------------------------------|
| description             | SBC for Zoom Contact Center BYOC      |
| location                | Burlington,MA                         |
| system-log-level        | NOTICE                                |
| default-gateway         | 10.138.194.129                        |
| source-routing          | enabled                               |
| snmp-agent-mode         | v1v2                                  |
| tls-global              |                                       |
| session-caching         | enabled                               |
| tls-profile             |                                       |
| name                    | TLSZoom                               |
| end-entity-certificate  | SBCEnterpriseCert                     |
| trusted-ca-certificates | DigiCertRoot                          |
|                         | DigiCertGlobalRootG2                  |
|                         | DigiCertGlobalRootG3                  |
| cipher-list             | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 |
|                         | TLS_RSA_WITH_AES_256_CBC_SHA256       |
|                         | TLS_RSA_WITH_AES_128_CBC_SHA          |
| mutual-authenticate     | enabled                               |
| translation-rules       |                                       |
| id                      | addPlus                               |
| type                    | add                                   |
| add-string              | +1                                    |
| translation-rules       |                                       |
| id                      | removeplus1                           |
| type                    | delete                                |
| delete-string           | +1                                    |
| web-server-config       |                                       |
| http-interface-list     | GU                                    |



CONNECT WITH US

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

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

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

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

**Oracle Corporation, World Headquarters**

500 Oracle Parkway  
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**

Phone: +1.650.506.7000  
Fax: +1.650.506.7200

**Integrated Cloud Applications & Platform Services**

Copyright © 2023, 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