Oracle Session Border Controller with Zoom Phone Local Survivability

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

1 DOCUMENT OVERVIEW 5
1.1 ORACLE SBC 5
1.2 ZOOM PHONE 5
1.3 REVISION HISTORY 5
1.4 VALIDATED ORACLE VERSIONS 5

2 SETTING UP ZOOM PHONE LOCAL SURVIVABILITY. 6
2.1 ZOOM PHONE LOCAL SURVIVABILITY (ZPLS) 6
2.2 ZOOM NODE OPERATION MODE 6
2.3 SUPPORTED ZOOM PHONE FUNCTIONALITY DURING ZPLS FAILOVER 7
2.4 SYSTEM REQUIREMENTS FOR ZPLS MODULE 7
2.5 DEPLOYING THE ZOOM PHONE SURVIVABILITY MODULE 7
2.6 DEPLOY VM FROM OVA FILE 8
2.7 CONFIGURE ZOOM NODE VM 8
2.8 TEST ZOOM NODE NETWORK CONNECTIVITY 11
2.9 REGISTER ZOOM NODE SERVER 12
2.10 ZOOM PHONE LOCAL SURVIVABILITY MODULE INSTALL 14
2.11 ZOOM PHONE SITE CONFIGURATION FOR LOCAL SURVIVABILITY 16
2.12 INTEGRATION ZOOM NODE WITH ORACLE SBC SESSION BORDER CONTROLLERS (SBC) 18

3 NETWORK DIAGRAM 20

4 CONFIGURING THE ORACLE SBC 21
4.1 GLOBAL CONFIGURATION ELEMENTS 22
4.1.1 System-Config 22
4.1.2 Media Manager 24
4.1.3 SIP Config 25
4.1.4 NTP Config 26

4.2 NETWORK CONFIGURATION 26
4.2.1 Physical Interfaces 27
4.2.2 Network Interfaces 27

4.3 SECURITY CONFIGURATION 28
4.3.1 Certificate Records 28
4.3.2 SBC End Entity Certificate 29
4.3.3 Root CA and Intermediate Certificates 31
4.3.4 Zoom Approved CA Vendors 31
4.3.5 Generate Certificate Signing Request 34
4.3.6 Import Certificates to SBC 35
4.3.7 TLS Profile 37

4.4 MEDIA SECURITY CONFIGURATION 39
4.4.1 Sdes-profile 39
4.4.2 Media Security Policy 40

4.5 MEDIA CONFIGURATION 42
4.5.1 Realm Config 42
4.5.2 Steering Pools 43
4.7 Session-Translation 45
4.8 SIP Interface 47
4.9 Session Agents 49
4.10 Routing Configuration 50
4.10.1 Calls from PSTN to Zoom 50

4.10.2 Route Calls from ZoomNode To PSTN: 51
5 ACLI RUNNING CONFIGURATION 52
6 SAMPLE CALL FLOW 63

1 Document Overview

Zoom Phone Local Survivability (ZPLS) aka Zoom Node is the Zoom's survivability solution of telephony services in order to provide an additional layer of protection to ensure business continuity. An outage can be the result of an internet service failure at a business location or a failure in multiple Zoom datacenters that prevent client devices from reaching Zoom Phone components. With ZPLS and Oracle SBC customers can get a seamless PSTN calling experience even when the Zoom Phones are not able to reach the Zoom Cloud.

This document focuses how to connect Oracle SBC to Zoom Phone Local Survivability only. Please follow our other Zoom Application Notes that focus on connecting **Oracle SBC with Zoom BYOC** and **Oracle SBC with Zoom Cloud Peering** depending upon your requirement to configure the Oracle SBC with Zoom Phone system offerings.

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 Phone

https://support.zoom.us/hc/en-us/articles/8427359971853-Zoom-Phone-Local-Survivability

1.3 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	18/11/22	• Initial publication

1.4 Validated Oracle Versions

We have successfully conducted call testing with the Oracle Communications SBC versions:SCZ9.0p4

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 (Release SCZ9.0.0 Only)
- AP4900 (Release SCZ9.0.0 Only)
- VME

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

2 Setting up Zoom Phone Local Survivability.

This section covers the steps required to configure ZPLS. Most of the content in this section is taken from Zoom's article https://support.zoom.us/hc/en-us/articles/8427359971853-Zoom-Phone-Local-Survivability which should be followed for detailed steps on how to configure the Zoom Node.

Disclaimer – The content of this section is subjected to change and Oracle does not guarantee it to be up to date. You should always follow latest Zoom configuration guide and contact your Zoom representative for Zoom side configuration.

2.1 Zoom Phone Local Survivability (ZPLS)

The Zoom Phone Local Survivability (ZPLS) module leverages the platform and OS provided by Zoom Node and is distributed as a Linux-based appliance that is spun up on an on-premises VMware ESXi host. Deploying the ZPLS module allows organizations to have an on-premise failover for their Zoom Phone system.

The ZPLS module does not affect the phone service during normal operations. Phone clients and devices in survivable Phone Sites register to the corresponding ZPLS module and are able to maintain a subset of Zoom Phone features when connectivity to Zoom Phone is lost. When connectivity to the Zoom Phone cloud returns, clients and devices re-register back to the cloud. During the outage neither the administrator nor the end user is required to take any action to enable survivability- the failover and fallback process is seamless and automatic.

2.2 Zoom Node Operation Mode

Zoom's survivability appliance is designed to typically serve as a backup plan in strategic locations that house a large number of employees in a single location or campus. During normal operations, Zoom Phone clients communicate with Zoom Phone data centers directly bypassing the ZPLS module. During an outage when the Zoom Client is unable to connect to the Zoom Phone data centers, supported clients and devices are able to register to an onsite ZPLS module in order to maintain internal dialing functionality and basic supplementary services. PSTN connectivity is maintained utilizing the Oracle SBC which is a trusted and certified with Zoom Phone System Network Function. When normal operations have been restored, clients register back to the cloud and the ZPLS module returns to an idle state.

2.3 Supported Zoom Phone functionality during ZPLS failover

As of today the following features are supported during failover.

- Internal Extension Dialing
- Dial By Name
- Contact Search/Calling (the client learns the first 25000 contacts)
- Dial From Call History (Call History in failover is uploaded to Zoom when service resumes)
- Inbound / Outbound PSTN (assumes Oracle SBC and survivable PSTN connectivity)
- Hold/Resume
- Mute/Unmute
- DTMF (RFC 2833)
- Consult Transfer
- Blind Transfer
- Call Park
- Adhoc 3-party Conference

2.4 System requirements for ZPLS module

The recommended specifications for the Zoom Phone Local Survivability module VM is as follows:

- **VM Platform**- VMware ESXi 6.7 or higher
- **Processor**- Intel(R) Xeon(R) CPU E5-2630 v4 or higher
- **Dedicated threads**- 8 or higher
- **Memory**- 16 GB or higher
- **Storage space**- 80 GB or higher
- **Network speed**- 4 Gbps or higher
- **For production deployments only 'Thick' provisioning is supported**

If you plan to choose a different configuration, contact your Zoom representative for assistance.

2.5 Deploying the Zoom Phone Survivability module.

1. Download Zoom Node OVA
2. Sign into the Zoom web portal.
3. In the navigation menu, click **Advanced** then **Zoom Node**.
4. Click **Add Servers**.
5. A new dialog box will appear.

6. Click **Download** to download the Node OVA file.
7. (Optional) Set the time for the **Code Expiration** in minutes.
8. Click **Generate**.
9. Click **Copy**, to copy the registration code, and save it to use later in section 2.9

2.6 Deploy VM from OVA File

1. Within the ESXI vCenter interface, select **Create/Register VM**.
2. Click **Deploy a virtual machine from an OVF or OVA file**.
3. Click **Next**.
4. Enter the name of the virtual machine, then click the blue pane, and select the Zoom Node OVA file.
5. Select the **datastore** that Zoom Node will be deployed to and click **Next**.
6. In the **Deployment options** window, select the network mappings (VLAN), disk provisioning (thin or thick provisioning, and other configuration options.
7. Click **Next**.
8. Review the deployment sections and click **Finish** to deploy the VM.
9. Once the deployment is completed successfully, power on the virtual machine and open the console of this virtual machine.

2.7 Configure Zoom Node VM

1. Start up the Zoom Node VM in vCenter.
2. In the Zoom Node VM, create a new password for the **zoom-setup** user, and save the password for future use in the TUI.

3. Once the password has been set, you will be prompted to modify the hostname for the server.

4. Type **Yes** and press the **Enter** key.
5. Enter the desired hostname and domain and press the **Enter** key.
6. Press any key to move to the main configuration menu.

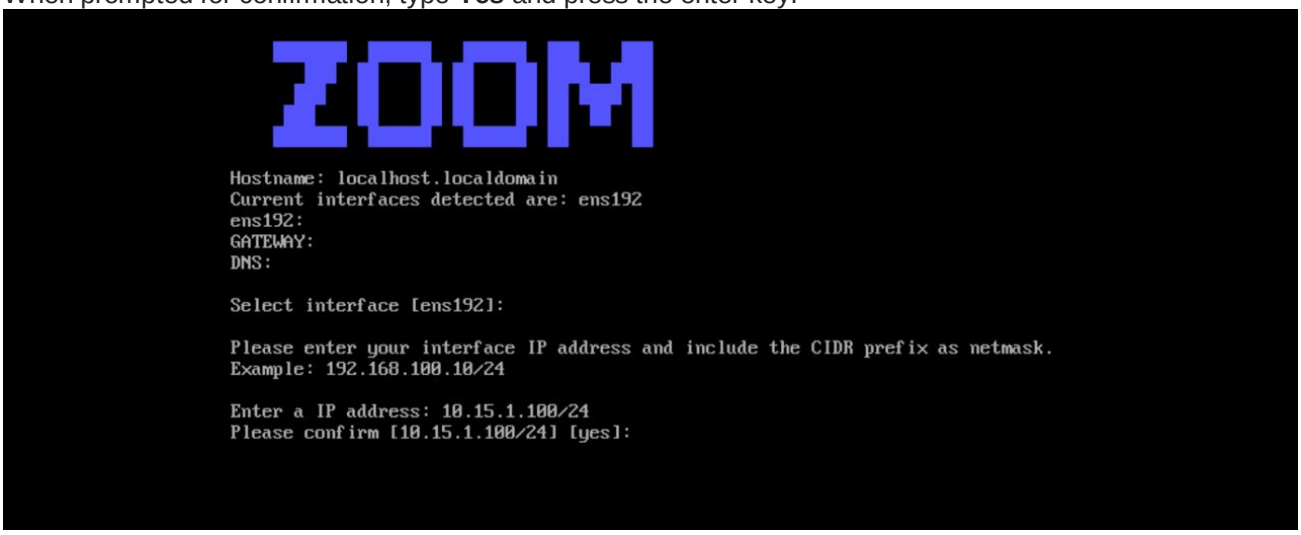
7. Configuring the network interfaces

In the main menu, press **1** to open the network configuration.
The following menu will be displayed.

1. Save the value for **Current interfaces detected are**, as that will be used for the IP address configuration.

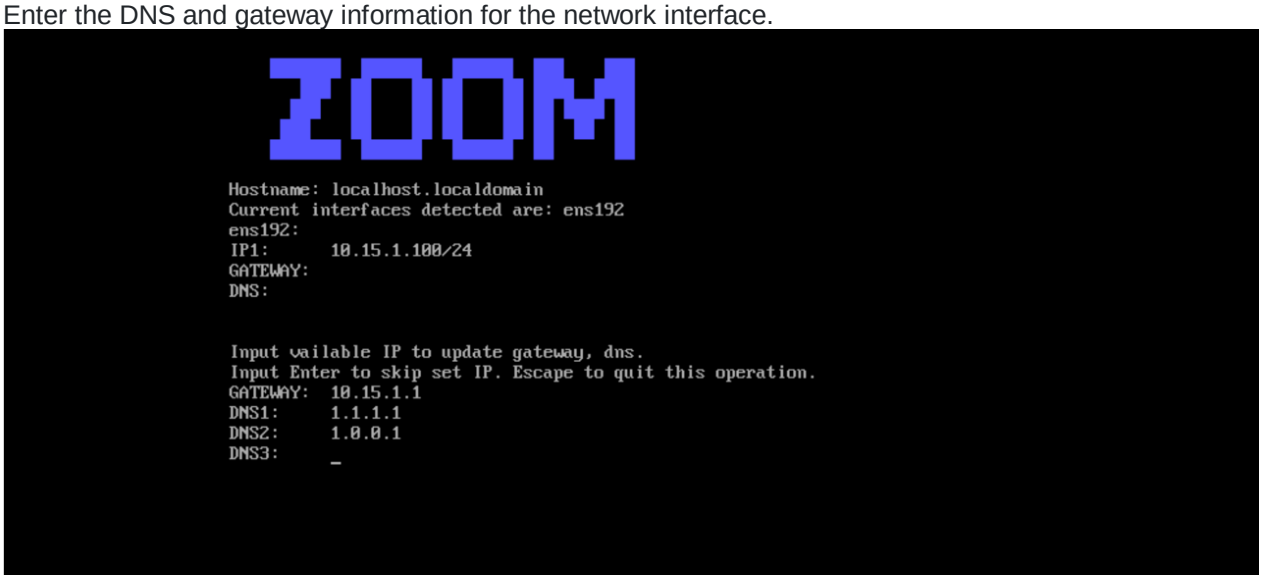
Note: If using DHCP for the subnet that the Node management server is deployed on, Zoom Node will automatically acquire an address. This address will be listed directly below the network interface name, as well as the **Gateway** and **DNS** addresses.

2. Press **1** to add the primary IP address.
3. Press the **Enter** (or manually type the name of the network interface), to choose the network interface for configuration.
4. Enter the IP address and subnet mask using CDIR notation without spacing (ex. 192.168.200.29/24).
5. Press **Enter** to accept the new address.
6. When prompted for confirmation, type **Yes** and press the enter key.

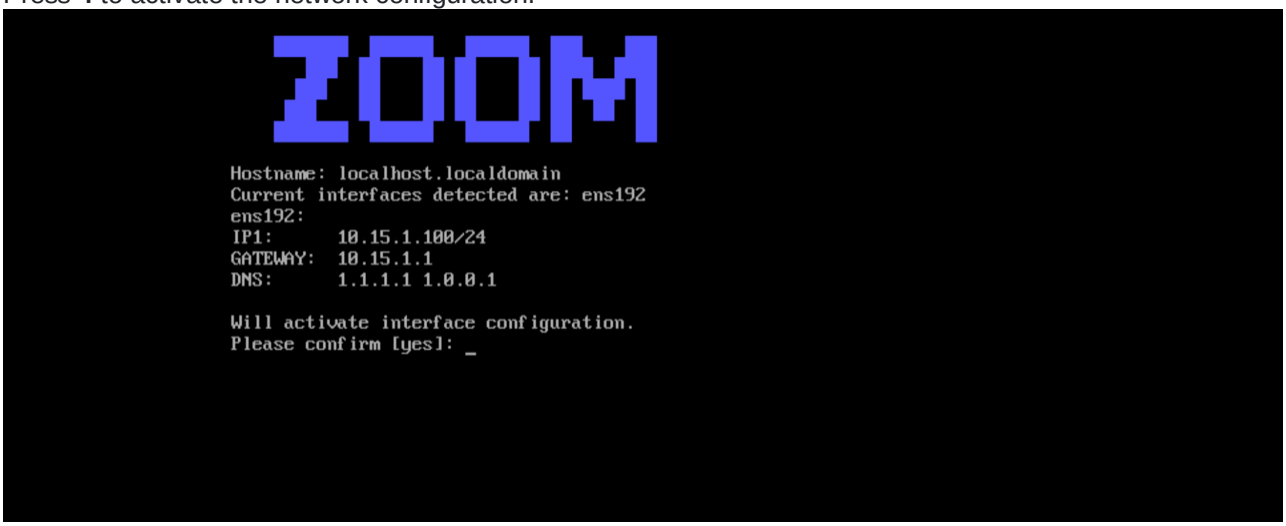


7. The new IP addresses will be listed with the rest of the network information.
8. (Optional) Press **3** to update the DNS and gateway information.
   Note: This step is only optional if utilizing DHCP for the subnet the server is deployed on.

9. Enter the DNS and gateway information for the network interface.



10. Press **Enter** to confirm the new changes.
11. Press **4** to activate the network configuration.



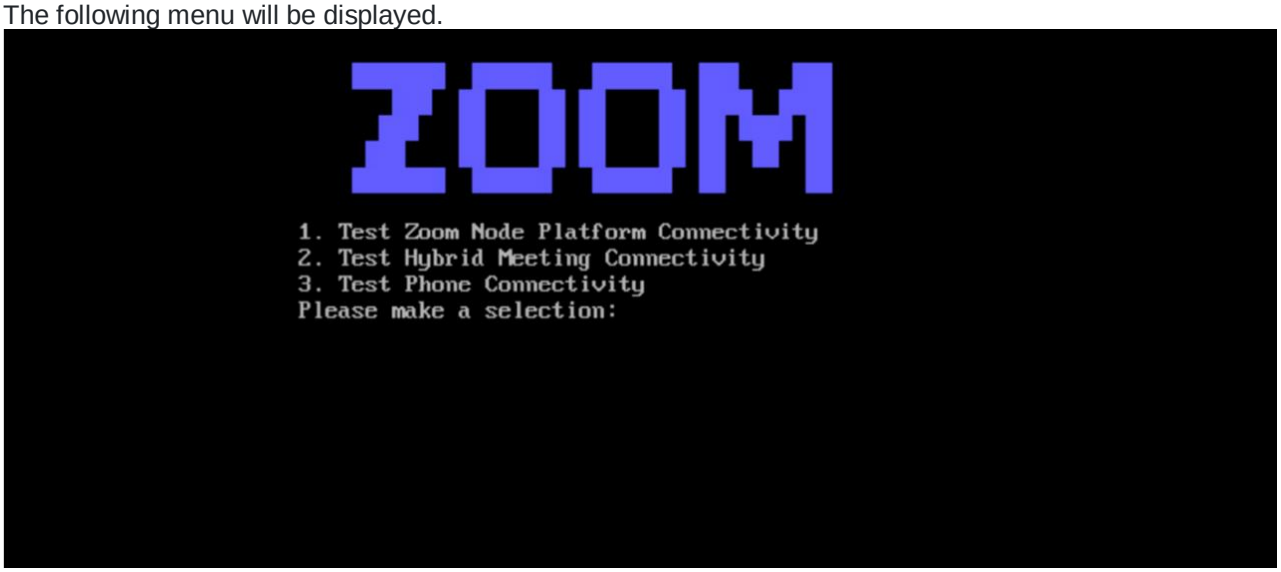
12. Under the network interface configuration menu, press **2**.
13. Press the **Enter** key to modify the suggested interface or type the name of the desired network interface and press **Enter** to modify it.
14. Type the IP address (in CDIR format), and press **Enter**.
15. Type **YES** to confirm you want to remove the address.

2.8 Test Zoom Node network connectivity

Once the network interfaces have been configured for the Zoom Node instance, network connectivity for the Node server should be tested to ensure proper function.

Note: Internet access is required on the Server to access reach Zoom Cloud System.

1. In the main menu, press **2** to open the connectivity test menu.
   The following menu will be displayed.



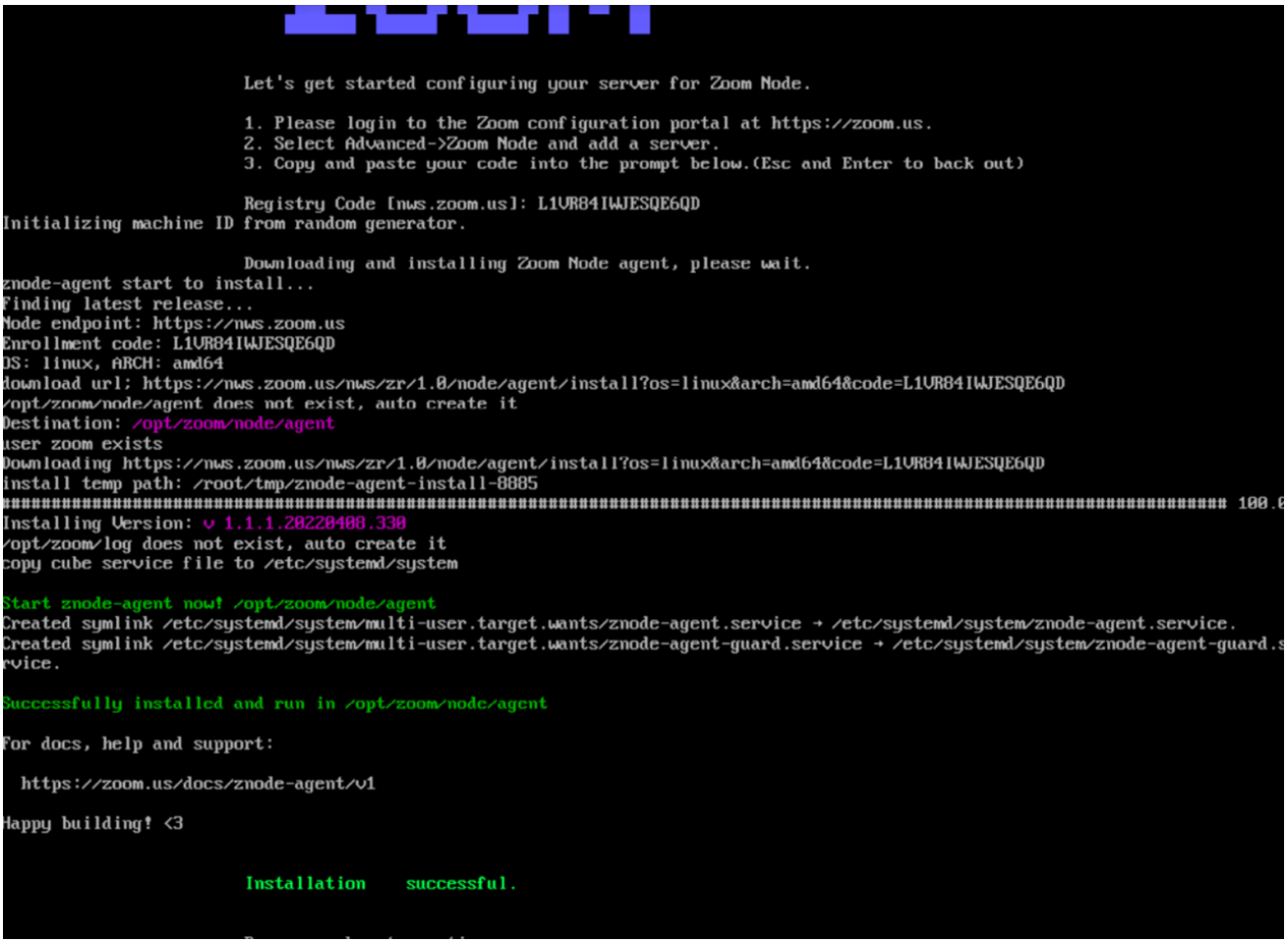
2. Press **1** to test connectivity for the Zoom Node platform.
3. Once the test finishes, the results for each service will be displayed.
4. (Optional) Press any key to return to the testing menu and test connectivity for the other modules.

2.9 Register Zoom Node server

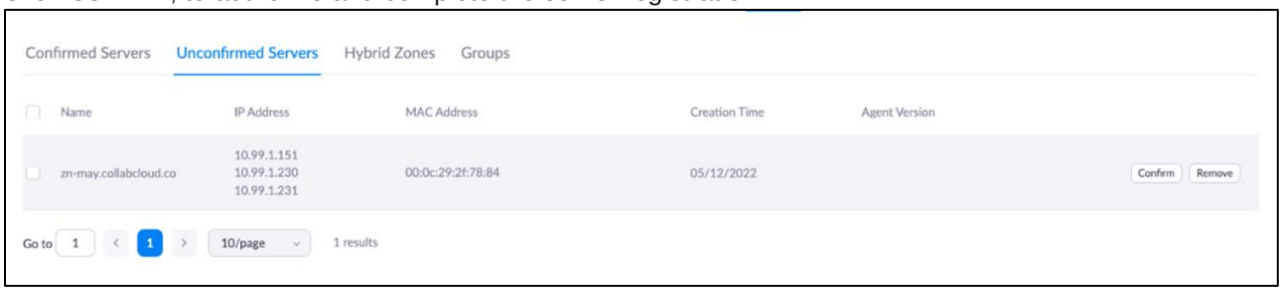
Once connectivity to the Zoom Cloud has been established and verified, the Zoom Node server is ready to be registered within the Zoom web portal.

1. In the main menu, press **3** to open the registration configuration.
   The following menu will be displayed.

2. Enter the registration code saved in Step 3 and press **Enter**.



3. Return to the Zoom web portal, and under the **Servers** tab, click **Unconfirmed Servers**.
4. The newly added server will be listed under **Unconfirmed Servers**.
5. Click **Confirm**, to authorize and complete the server registration.



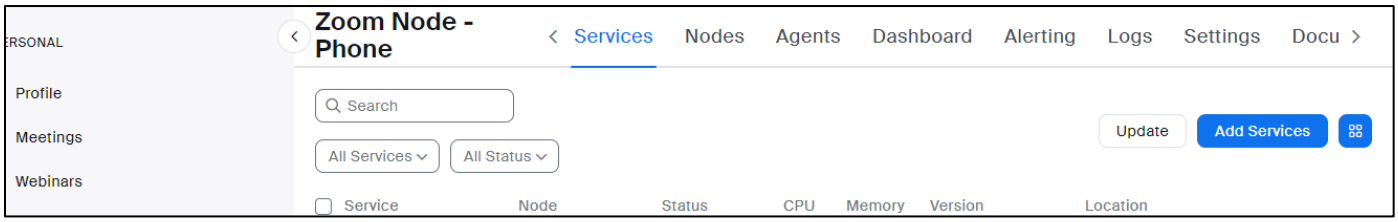
6. In the next window enter the following information:
    - **Description**: Description of the server.
    - **Location**: Location of the server, which should be listed in a way to easily filter in the **Servers** tab.
7. Click **Confirm**.
8. Click the **Confirmed Servers** tab to view the registered server.
9. Click the name of the server to view the server's properties.
   After 1-2 minutes, refresh the page to verify both the node and monitor agent are running.

The Zoom Node server is now ready to deploy services and modules.

2.10 Zoom Phone Local Survivability Module install

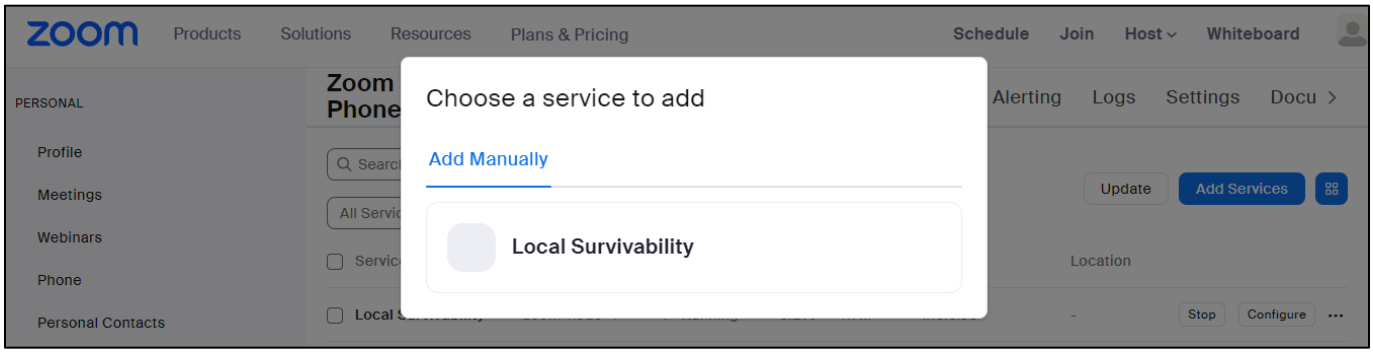
1. Navigate to **Advanced** > **Zoom Node** > **Zoom Node - Services**-

Select **Add Services** on the top right hand corner of the screen.

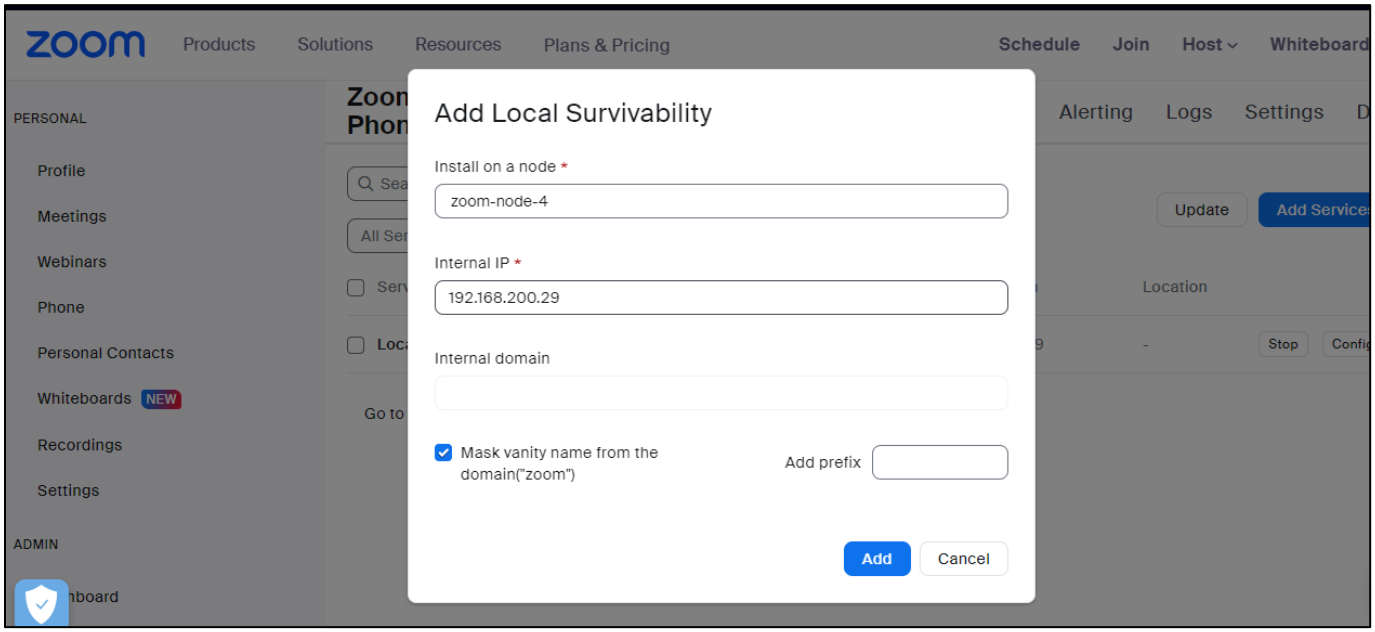


2. Select **Local Survivability** as the Service . Select the server where the Local Survivability Module needs to be installed and the Internal IP that will be used. Theremaining fields can be set as default. Click **Add**.

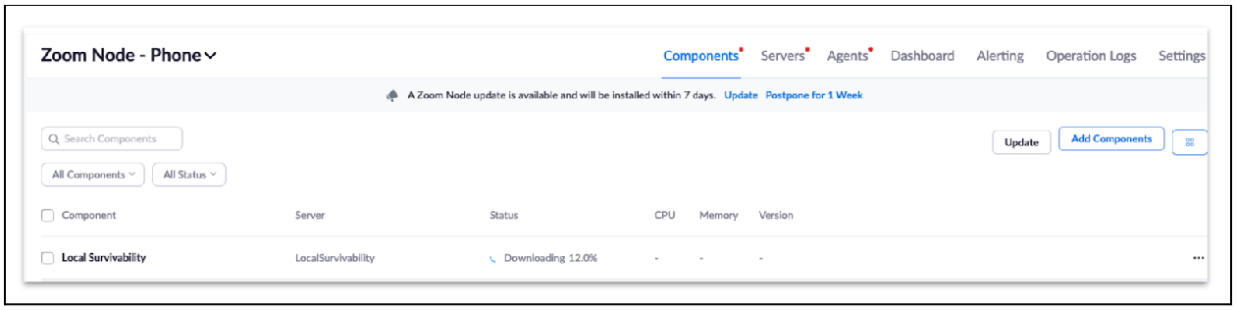
Note: If a prefix is added, it must be less than 10 characters.



Choose the Node and Internal IP. You can optionally mask the Vanity name from Domain.



The Survivability service will start deploying and once deployed it will start reflecting as below.

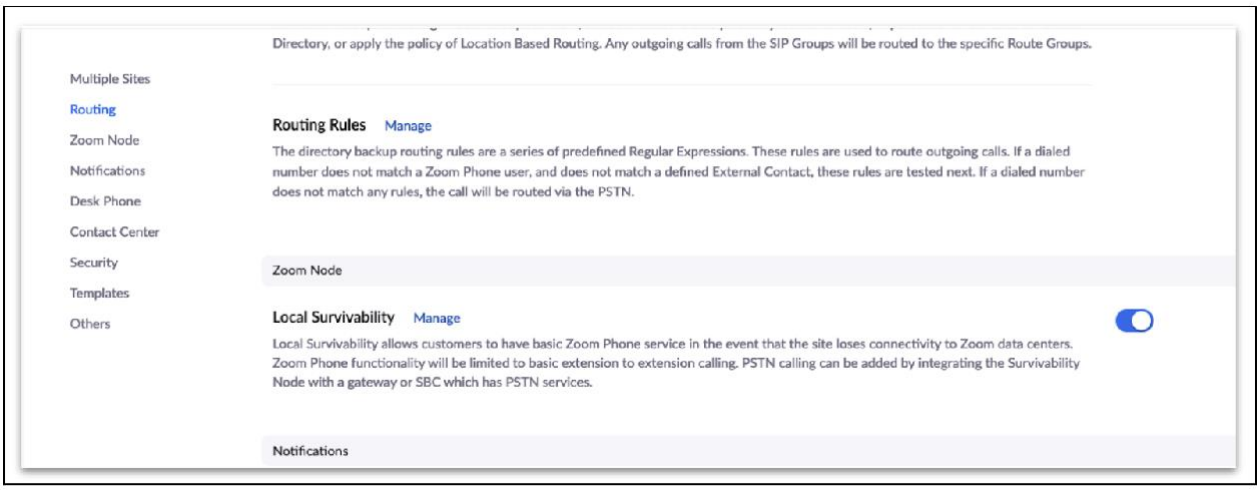


Once the module has finished installing, the Status will be Stopped. **DO NOT START MODULE UNTIL IT IS ASSIGNED TO A SITE**.

2.11 Zoom Phone Site Configuration for Local Survivability

After the Zoom Phone Local Survivability Module has been set up, this will be assigned to a site.By default all users in a Site will be assigned to this Local Survivability Module. Based on the hardware specification of the server, the maximum number of devices will be restricted to 2000 or 5000 devices. In future Zoom will add the capability to select which users and devices within a site are enabled for survivability.

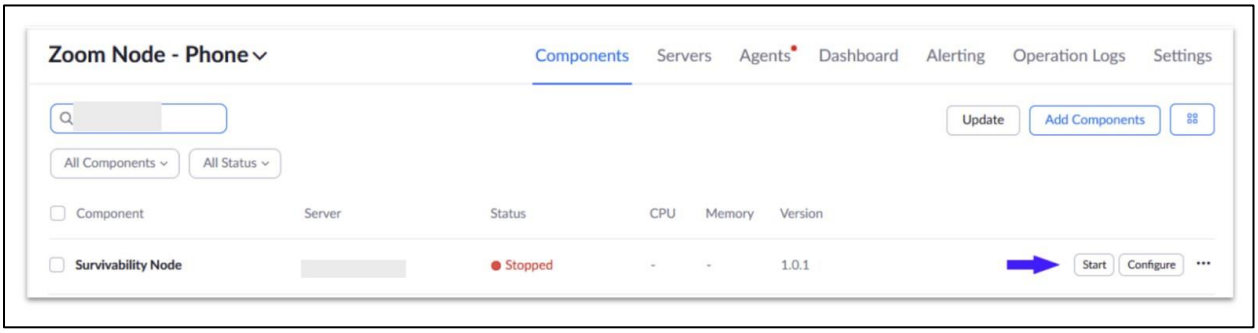
1. Navigate to **Phone System Management** > **Company Info** > **Account Settings** >**Zoom Node** and enable the **Local Survivability** option.



2. Select **Manage** and find the Local Survivability server that will be assigned to this site.

3. Select **Assign to** and select the appropriate site. Click **Save**

4. Navigate to **Advanced > Zoom Node > Zoom Node - Phone > Components**. Find theserver and click Start.



5. Navigate to **Phone System Management > Company Info > Sitename > Settings > Zoom Node and enable Local Survivability**

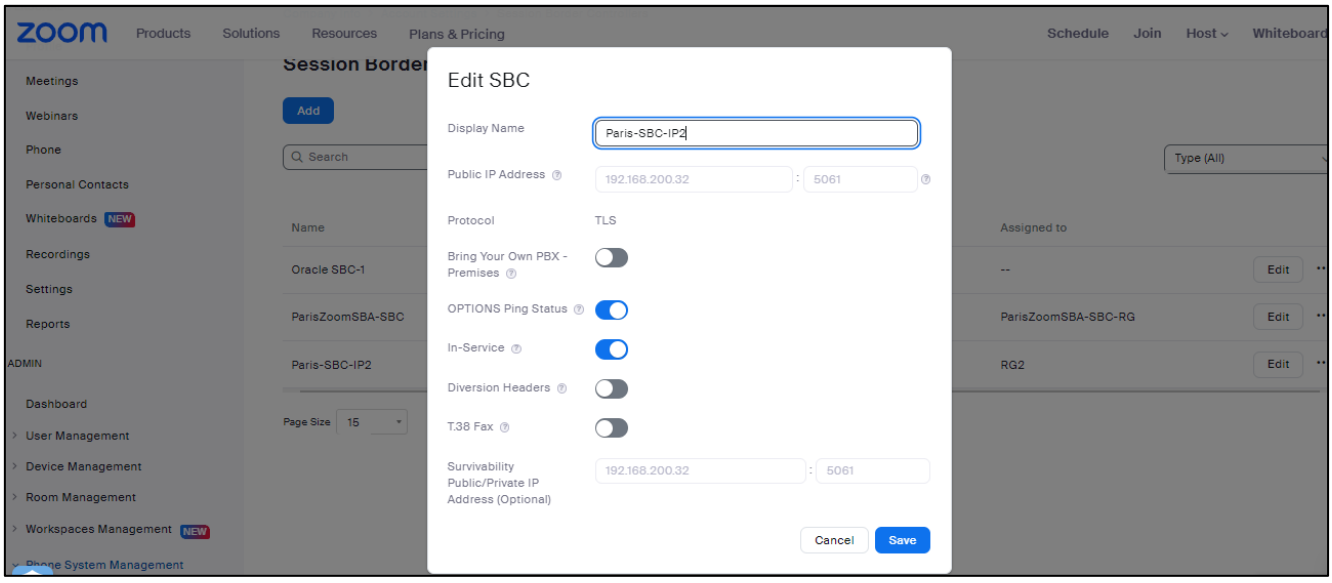
2.12 Integration Zoom Node with Oracle SBC Session Border Controllers (SBC)

Oracle SBC is required to connect to Zoom Node to provide PSTN connectivity functionality. To integrate Local Survivability module with our SBC over a SIP trunk, perform the following steps:

Add the SBC

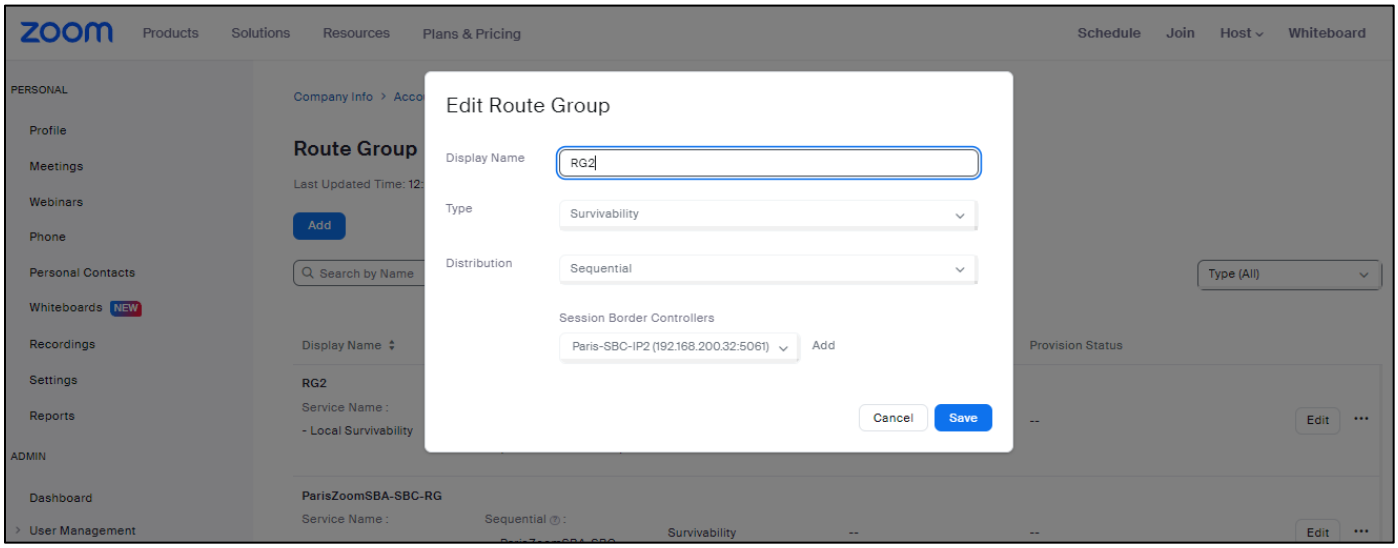
1. Add the SBC internal IP by navigating to **Company Info** > **Account Settings** > **Routing** > Session Border Controllers
2. Click **Manage** and select **Add**
3. Enter a **Display Name**
4. Enter **IP address**
5. Enable OPTIONS Ping Status
6. Mark In Service to bring the SBC in Service

Note: IP address should be reachable from the Local Survivability module directly. NAT is not recommended. Currently, only port 5061 is supported by Zoom Node thus ensure that the SBC communicates to Local Survivability over port 5061



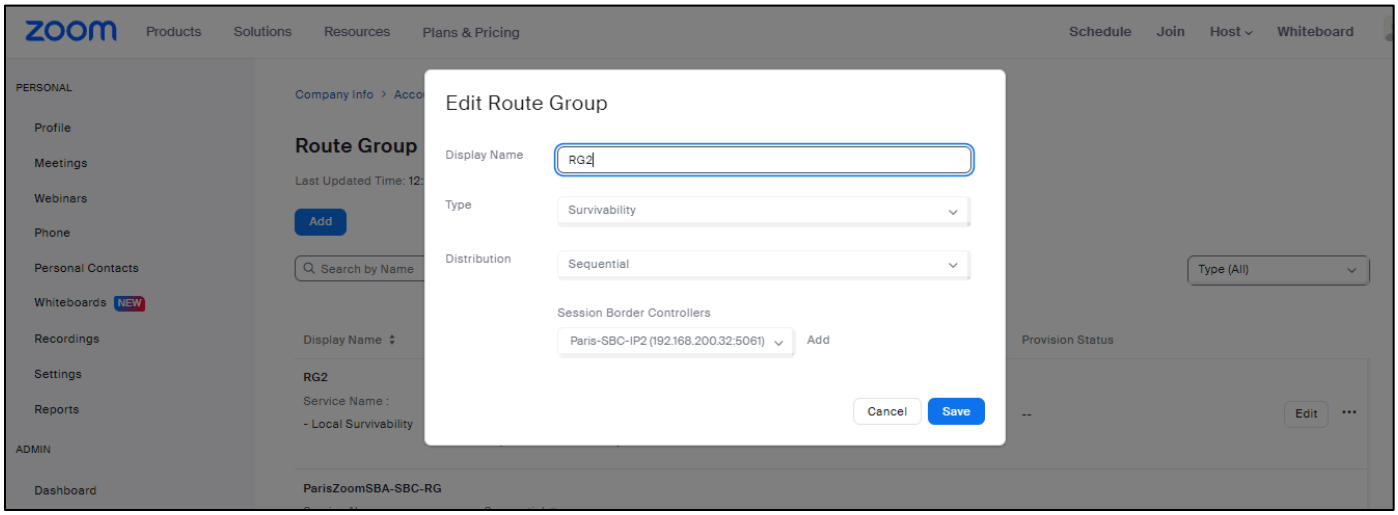
Assign this SBC to a Route group

1. Navigate to **Company Info** > **Account Settings** > **Route Groups**
2. Click **Add** and select **Or, add a new route group**
3. Enter a **Display Name** for the Route group
4. Change the Type to **Survivability**
5. Click on **Add** and select the **Session Border Controller** that was added in the previoussteps
6. Click **Save**



Assign this Route group to the Local Survivability Module

1. Navigate to **Company Info** > **Account Settings > Zoom Node** and click **Manage**
2. Select the server and click **"Assign to"** and select the Route Group that was created inthe previous steps.
3. Click Save



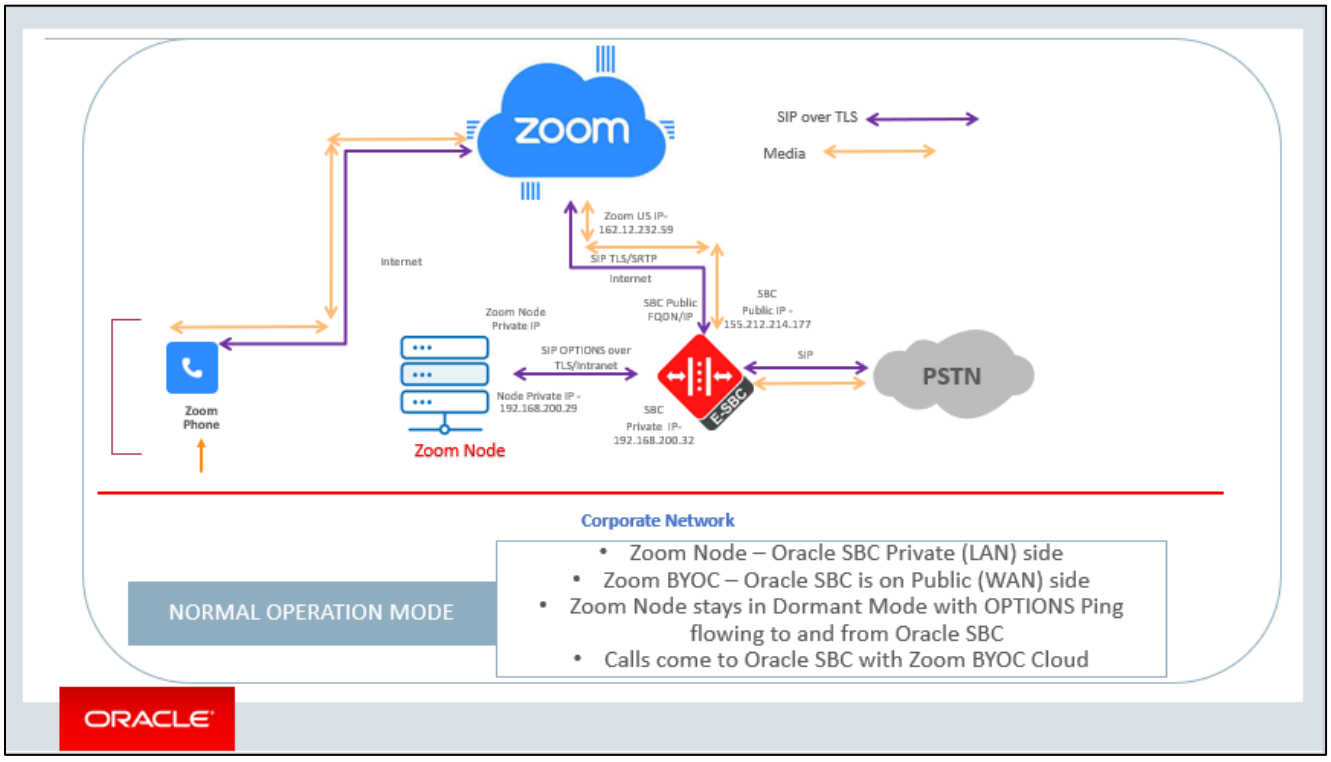
3 Network Diagram

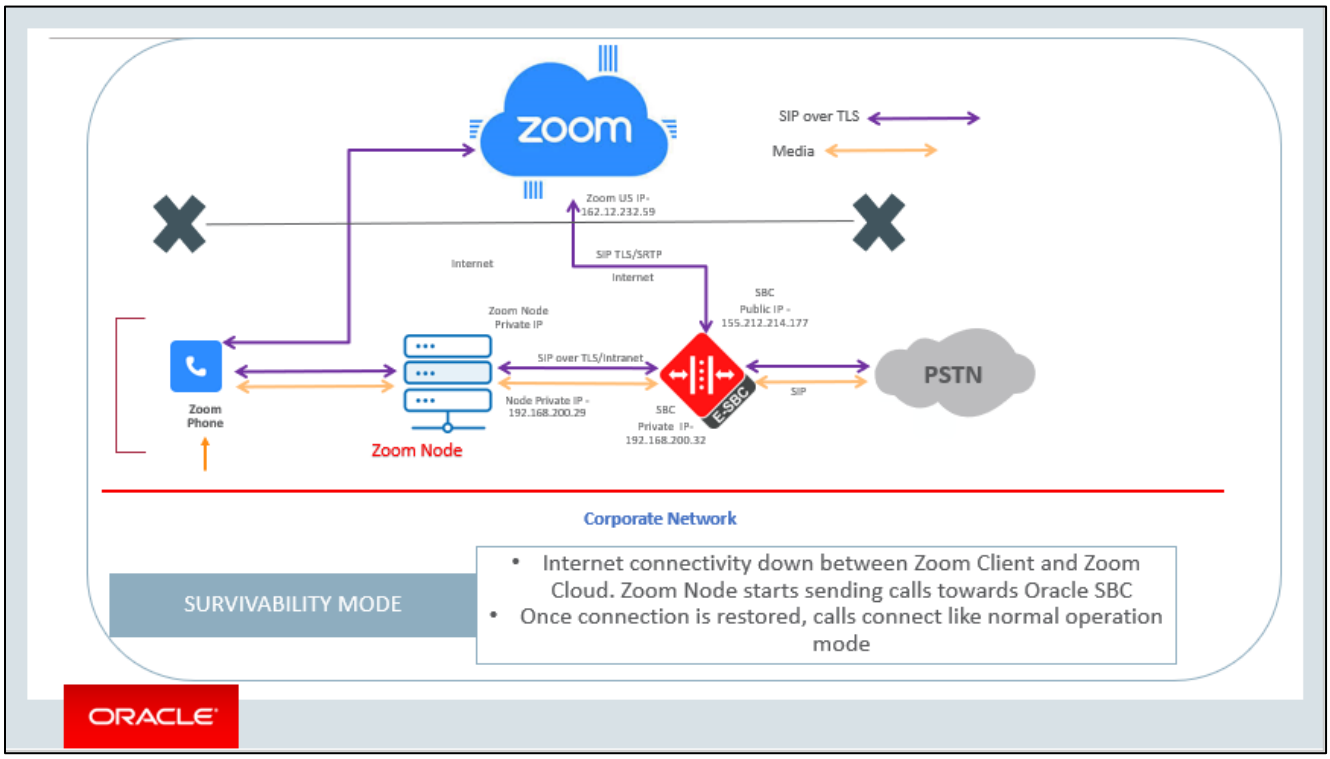
Zoom supported Clients and Devices maintain a keepalive mechanism (based on SIP OptionsPing) to the Zoom Phone cloud. In the event of an outage the client continues to send keepalive messages in order to detect the return of the cloud service and initiate resumption of normal operations.

Clients discover the appropriate failover ZPLS modulefrom the Zoom Phone platform during the bootup process since the ZPLS Module is added as the tertiary User Agent Server behind the primary and backup SIP zone.

In the event that a site is offline and the keepalive mechanism to the Zoom cloud has failed, supported clients and devices will register to the ZPLS module using SIP overTLS.

For Inbound and Outbound PSTN Connectivity Oracle SessionBorder Controller (SBC) that maintains operational PSTN Connectivity either through a legacy TDM/analog connection or SIP Trunk leveraging a cellular or alternate internet connection. The ZPLS module routes any foreign number that is not known locally to the SBC.





4 Configuring the Oracle SBC

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

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

These instructions cover configuration steps between the Oracle SBC and Zoom Node. 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.

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

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 Phone to function properly,however this should note should be treated 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!!!

IMPORTANT - Zoom Node is the Survivability Solution from Zoom ,which means Node only comes in the call flow when the Zoom clients are able to establish the connectivity with Zoom Cloud.Under normal circumstances Oracle SBC connects with Zoom Cloud IPs to send receive calls.

The current application note is a subset of Zoom BYOC application note and mainly focuses on steps required to connect Zoom Node with Oracle SBC.We have Another application Note Oracle SBC with Zoom BYOC that provides detailed instructions on how to connect Zoom BYOC with Oracle SBC.

4.1 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
-

4.1.1 System-Config

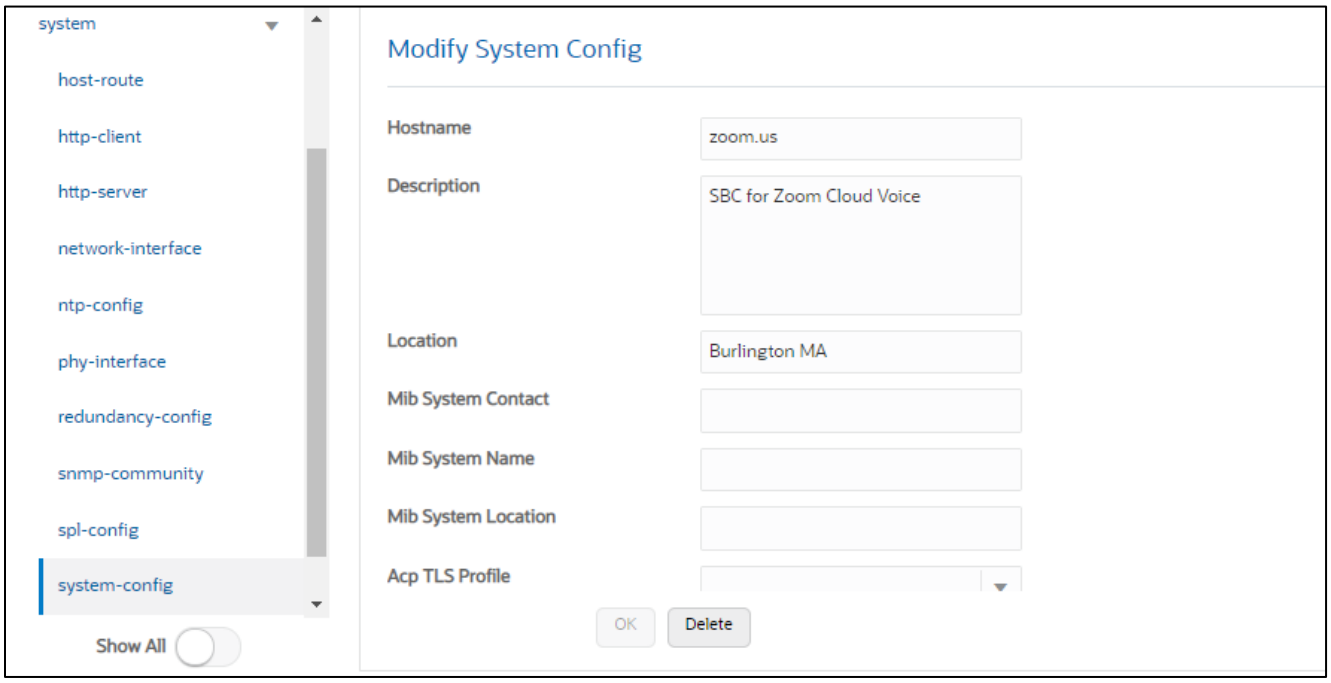
To configure system level functionality for the ORACLE SBC, you must first enable the system-config

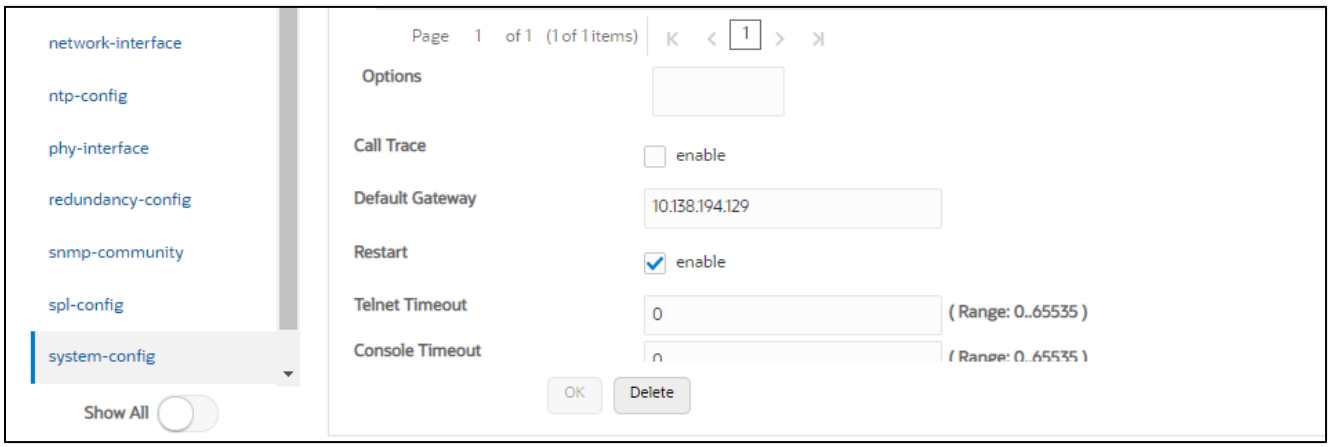
GUI Path: system/system-config

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.

4.1.2 Media Manager

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

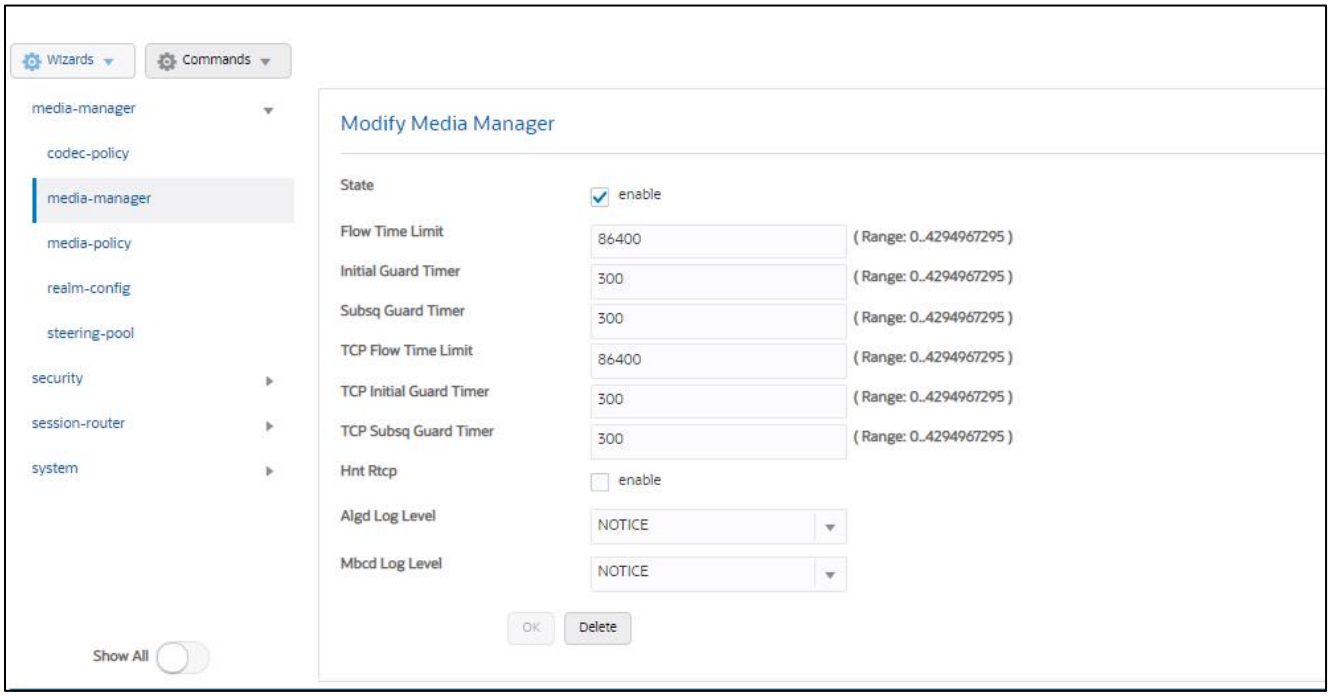
GUI Path: media-manager/media-manager

ACLI 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.



- Click OK at the bottom.

To enable media-manager from ACLI –

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

```
media-manager
    state                    enabled
```

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

4.1.3 SIP Config

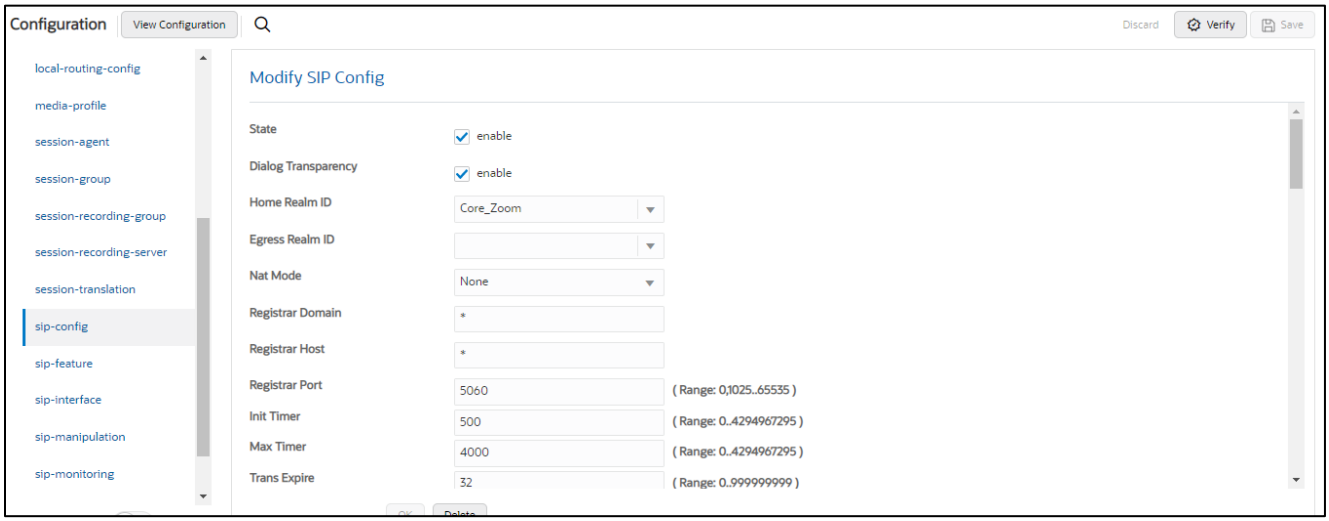
To enable SIP related objects on the Oracle SBC, you must first configure the global SIP Config element:

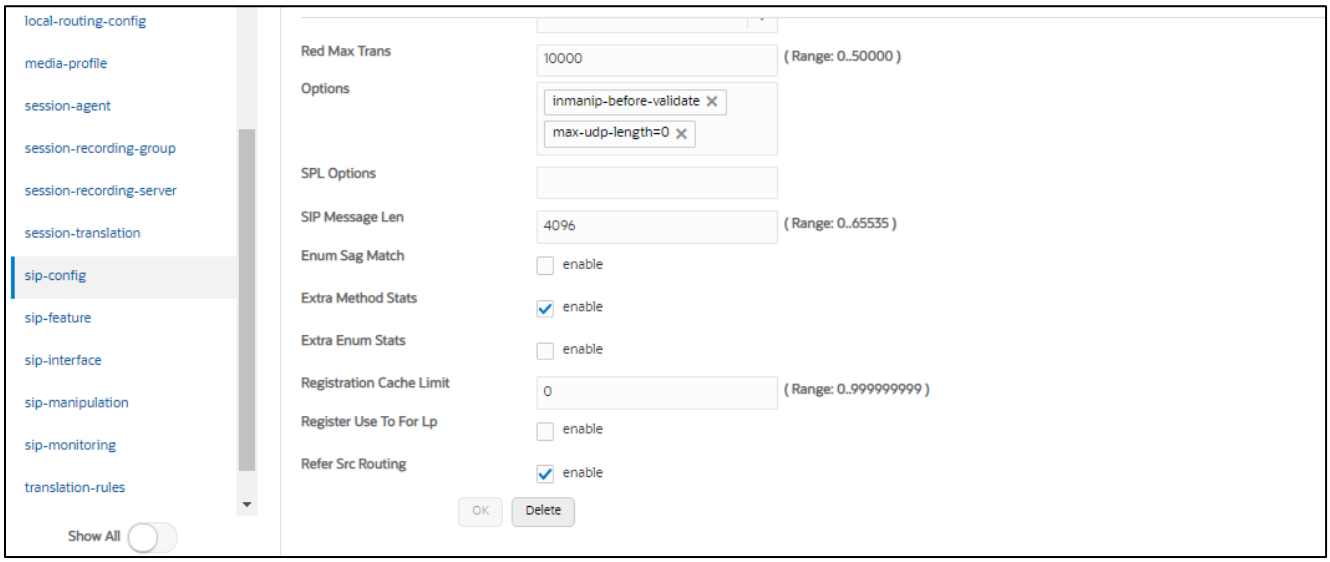
GUI Path: session-router/SIP-config

ACLI 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)





- Click OK at the bottom

To configure sip config from ACLI.

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

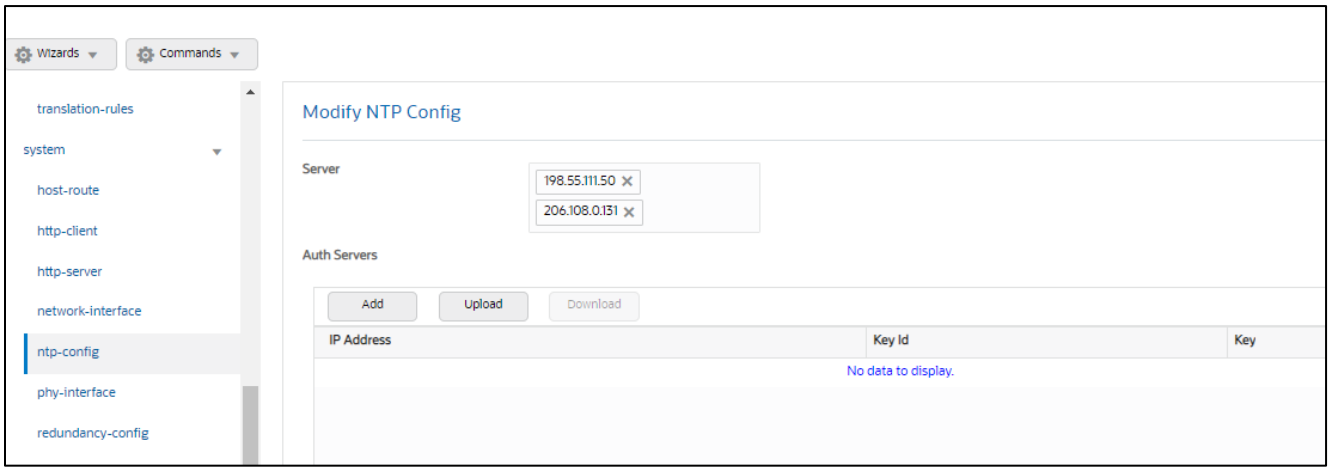
```
sip-config
      home-realm-id                Zoom
      options                      max-udp-length=0
                                     inmanip-before-validate
```

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

4.1.4 NTP Config

GUI Path: system/ntp-config

ACLI Path: config t→system→ntp-config



- Click OK at the bottom

To configure ntp-config from ACLI –

ACLI Path: config t→system→ntp-sync

```
ntp-config
      server                       216.239.35.0
```

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

4.2 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 two physical interfaces, and two network interfaces. One to communicate with Zoom Cloud Voice, the other to connect to PSTN Network.

4.2.1 Physical Interfaces

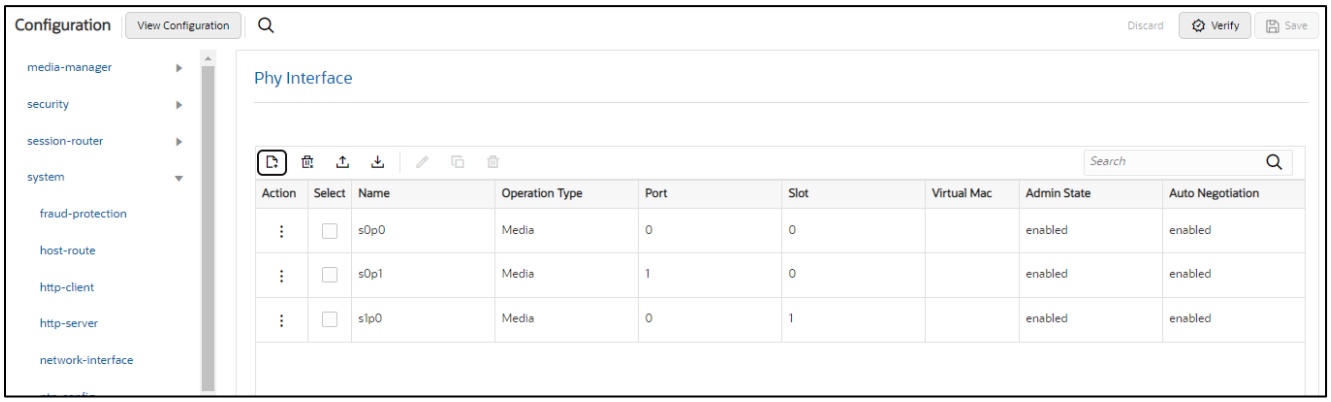
GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

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

Config Parameter	ZoomNode	PSTN1
Name	s0p1	s1p0
Operation Type	Media	Media
Slot	0	1
Port	0	0

Note: Physical interface names, slot and port may vary depending on environment.Interface s0p0 is created for communication with Zoom BYOC but this document only focuses on ZoomNode and PSTN connection so it can be ignored.



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

To configure phy-interface from ACLI –

ACLI Path: config t→system→phy-interface

```
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.

4.2.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

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

Configuration Parameter	ZoomNode	PSTN
Name	s0p1	s1p0
Hostname		
IP Address	192.168.200.32	192.168.1.10
Netmask	255.255.0.0	255.255.255.0
Gateway	192.168.200.1	192.168.1.1

- 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                    s0p1
        ip-address              192.168.200.32
        netmask                 255.255.0.0
        gateway                 192.168.200.1

network-interface
        name                    s1p0
        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.

4.3 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Zoom Node.The connection between the Oracle SBC and Zoom Phone platform is secured via TLS/SRTP.

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

4.3.1 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 Intermidiate 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

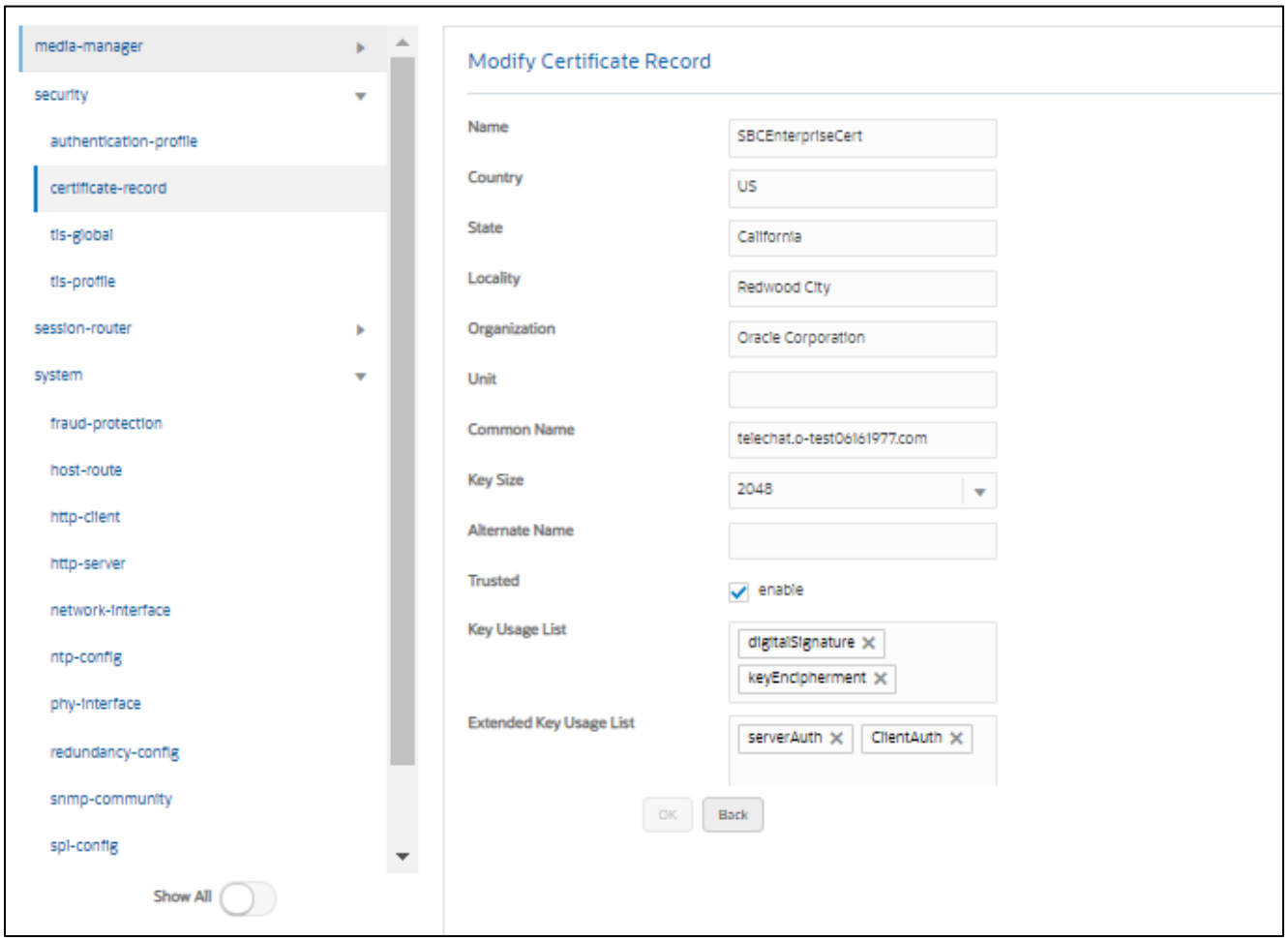
4.3.2 SBC End Entity Certificate

The SBC's end entity certificate is what is presented to Zoom Node 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 certification 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

4.3.3 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 keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256	Sha256

4.3.4 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

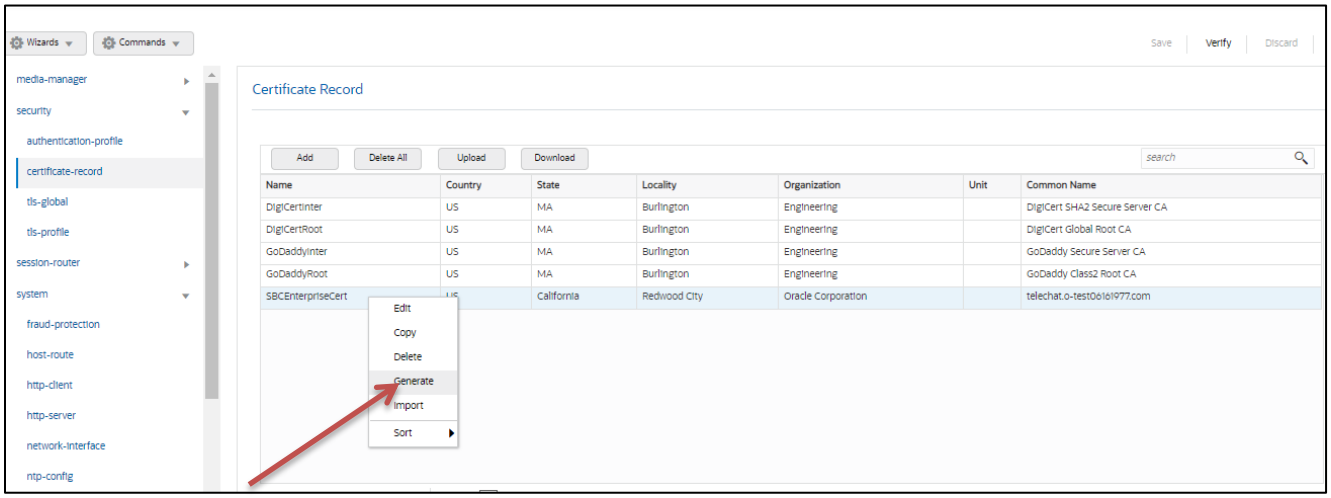
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 2
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 3

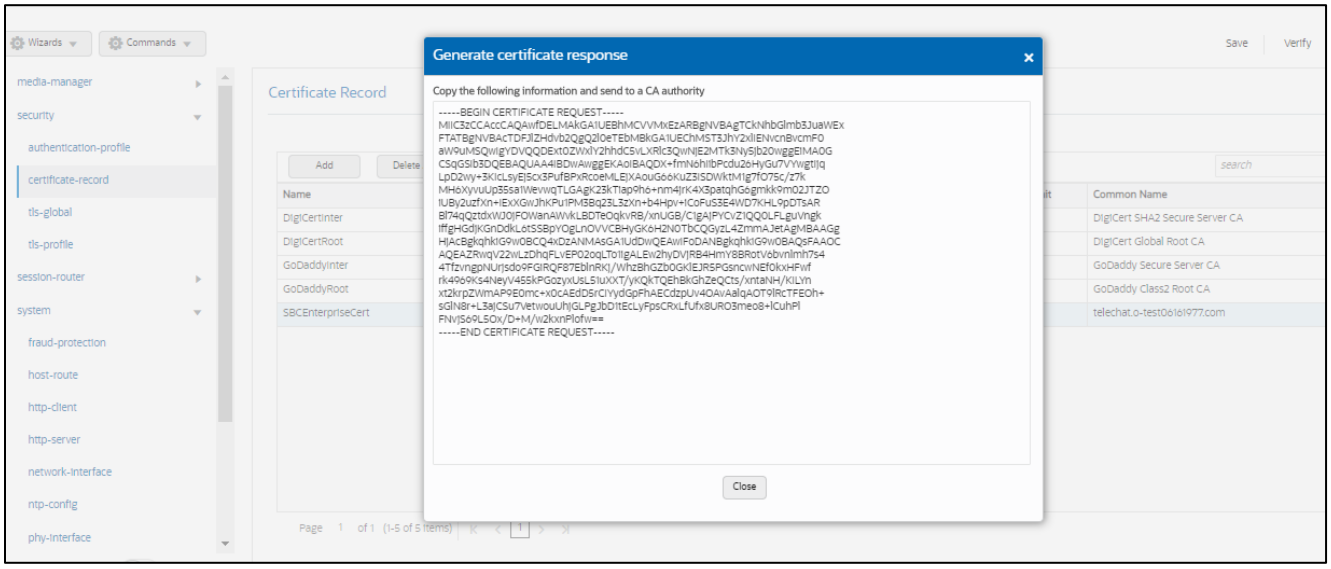
4.3.5 Generate Certificate Signing Request

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 intermidiate 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-----
MIIC4zCCAcsCAQAwazELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQ
HEwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEkMCIGA1UEAxMbdGVs
ZWNoYXQuby10ZXN0MDYxNjE5NzcuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAr3AmjF15PcIcWiB/kFExUGNHQHIbkJi28MDbcprO/KLXIHQysSnw
UWz34XLBfLQ6rS4MLyEMR8Nt8GGNSlWKiR431LsX7L+yGWvRjcBFP6DIHtH0Vuqm
ixVaUJpg5luPY6SvT1shyu26iLlBsLfem43tbKq5jz/jrvaUzyhlCvAQ23c1oS5a
D4UiF2mNOuSqxvmkx50a3/BNYbKecLNOxvKQyyTMgffNpASbZuW+eMEUKI5iB+AB
/AAoZRP4bn4qlE3wn8pJsNm8Pjxy4hbz24ySgmaN9iXpP1FdRw0TemfCsNazZRuK
DsviWJfunZYTzRfDe5pJToMH4u1zt2fK1QIDAQABoDMwMQYJKoZIhvcNAQkOMSQw
IjALBgNVHQ8EBAMCBaAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEL
BQADggEBADD5Y+u08LxmTMIsJ2Rjc8cgPZocTqBDXN0tp27S4FuB/01ikBBdG3YV
Ffp7/Q8ZeFHHgU/rMzeF8Gpo9Cc6JUGGux3/ws8ZkgRBxsNlG276i7pFN1vCIjEP
89AGxtryioRMc4kcdPpLJNQ10Qx1zKobHMTftGLDI6jN2pvn3zYHH8qA9V/1/yKa
3n0j33EuTrvTlQ5P4IgyVJqSBkdI29T1gXY6O8JVFLCQefTrF4TLc6teNzxXMdPw
PHoPu9hM3scGOWOHQnODXOFeq2AxBQzAa0/Cjf7Bw3l3POmMcIOawgDecZ8UjHpJ
lznX9/Gxg5X+S2QkHjNmPK+JuePqX4I=
-----END CERTIFICATE REQUEST-----

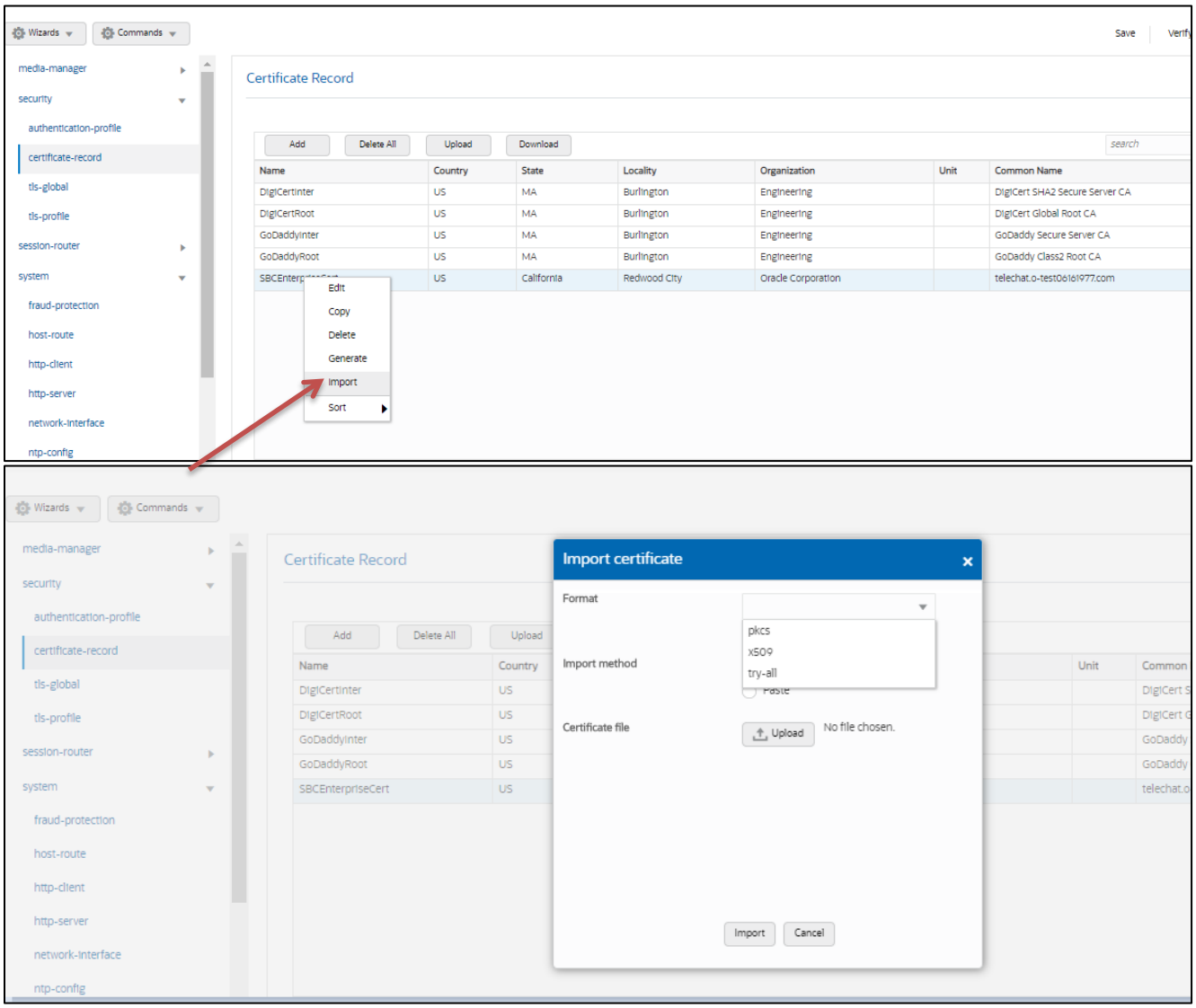
Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.

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.

4.3.6 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
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEkMCIGA1UEAxMbdGVs
ZWNoYXQuby10ZXN0MDYxNjE5NzcuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAr3AmjF15PcIcWiB/kFExUGNHQHIbkJi28MDbcprO/KLXIHQysSnw
UWz34XLBfLQ6rS4MLyEMR8Nt8GGNSlWKiR431LsX7L+yGWvRjcBFP6DIHtH0Vuqm
ixVaUJpg5luPY6SvT1shyu26iLlBsLfem43tbKq5jz/jrvaUzyhlCvAQ23c1oS5a
D4UiF2mNOuSqxvmkx50a3/BNYbKecLNOxvKQyyTMgffNpASbZuW+eMEUKI5iB+AB
/AAoZRP4bn4qlE3wn8pJsNm8Pjxy4hbz24ySgmaN9iXpP1FdRw0TemfCsNazZRuK
DsviWJfunZYTzRfDe5pJToMH4u1zt2fK1QIDAQABoDMwMQYJKoZIhvcNAQkOMSQw
IjALBgNVHQ8EBAMCBaAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEL
BQADggEBADD5Y+u08LxmTMIsJ2Rjc8cgPZocTqBDXN0tp27S4FuB/01ikBBdG3YV
Ffp7/Q8ZeFHHgU/rMzeF8Gpo9Cc6JUGGux3/ws8ZkgRBxsNlG276i7pFN1vCIjEP
89AGxtryioRMc4kcdPpLJNQ10Qx1zKobHMTftGLDI6jN2pvn3zYHH8qA9V/1/yKa
3n0j33EuTrvTlQ5P4IgyVJqSBkdI29T1gXY6O8JVFLCQefTrF4TLc6teNzxXMdPw
PHoPu9hM3scGOWOHQnODXOFeq2AxBQzAa0/Cjf7Bw3l3POmMcIOawgDecZ8UjHpJ
lznX9/Gxg5X+S2QkHjNmPK+JuePqX4I=
-----END CERTIFICATE REQUEST-----;

save and activate your configuration.

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

4.3.7 TLS Profile

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

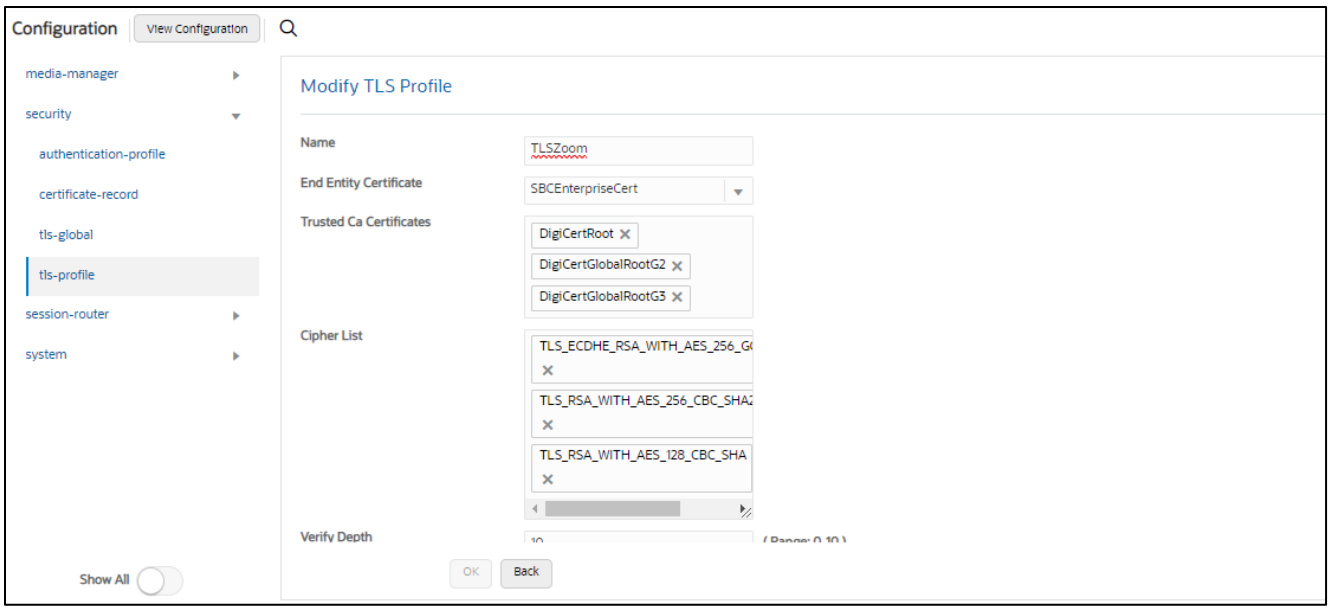
GUI Path: security/tls-profile

ACLI Path: config t→security→tls-profile

- Click Add, use the example below to configure

Zoom 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.

4.4 Media Security Configuration

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

4.4.1 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.

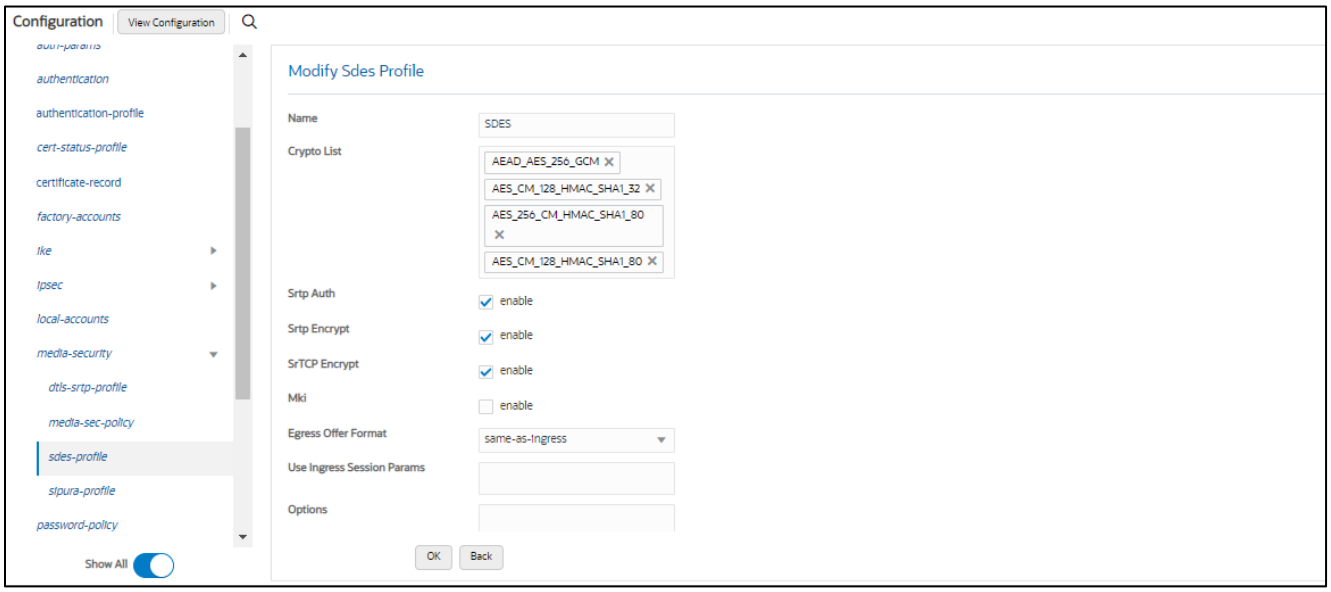
GUI Path: security/media-security/sdes-profile

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

Oracle SBC and Zoom Cloud Voice Support 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.



- Click OK at the bottom

To configure sdes-profile from ACLI –

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

```
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
```

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

4.4.2 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

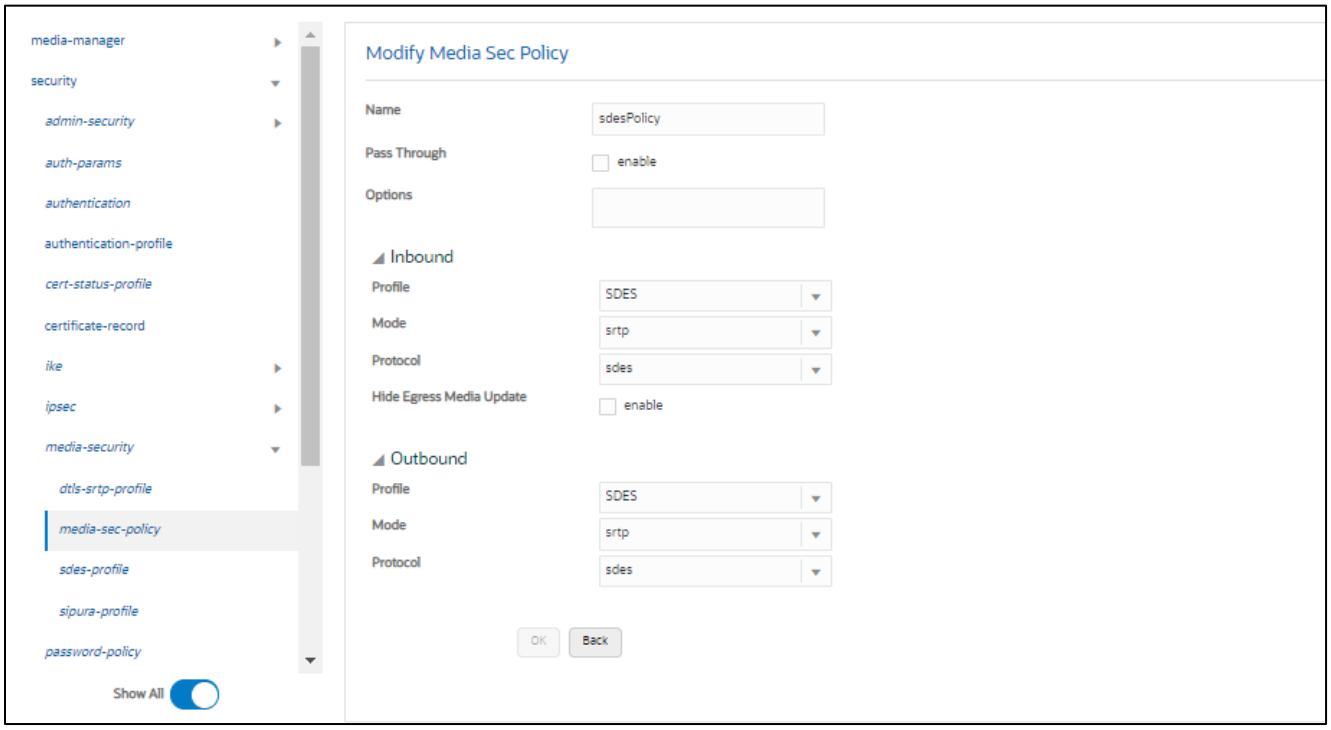
In this example, we are configuring two media security policies. One to secure and decrypt media toward Zoom, the other for non-secure media facing PSTN.

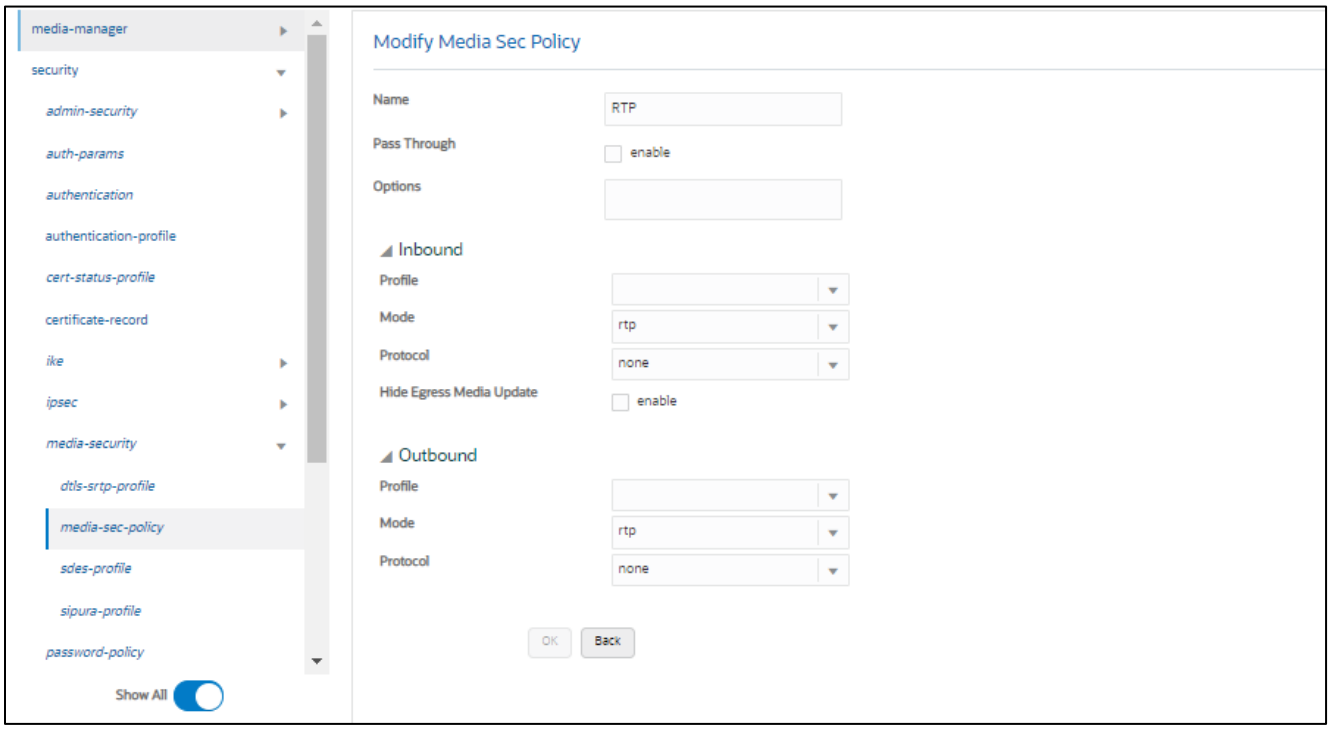
These are named as sdesPolicy and RTP.

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

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

- Click Add, use the examples below to configure





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.

4.5 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.

4.5.1 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.

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.

ZoomNode Realm

This is a standalone realm facing Zoom Node.

PSTN Realm

This is a standalone realm facing PSTN/SIP Trunk

GUI Path; media-manager/realm-config

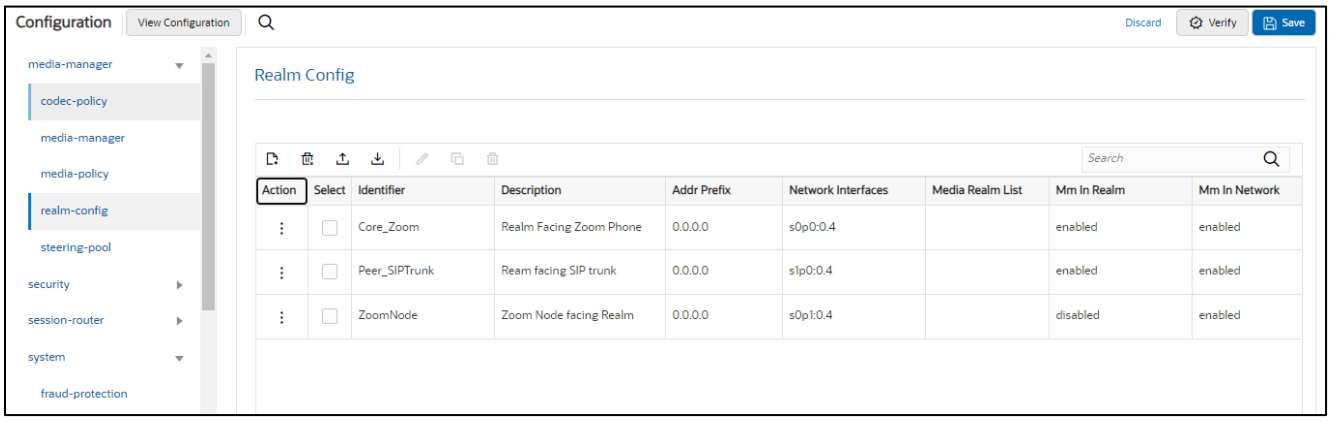
ACLI Path: config t→media-manager→realm-config

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

Config Parameter	Zoom Node	PSTN Realm
Identifier	ZoomNode	Peer_SIPTrunk
Network Interface	s0p1:0	s1p0:0
Mm in realm	☑	☑
Access-control-trust-level	High	High
Media Sec policy	sdespolicy	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                      Peer_SIPTrunk
        description                       Ream facing SIP trunk
        network-interfaces                  s1p0:0.4
        mm-in-realm                       enabled
        qos-enable                      enabled
        media-sec-policy                  RTP
        access-control-trust-level          high
        codec-policy                    OptimizeCodecs
        hide-egress-media-update              enabled
realm-config
        identifier                      ZoomNode
        description                       Zoom Node facing Realm
        network-interfaces                  s0p1:0.4
        media-sec-policy                  sdesPolicy
        access-control-trust-level          high
```

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

4.5.2 Steering Pools

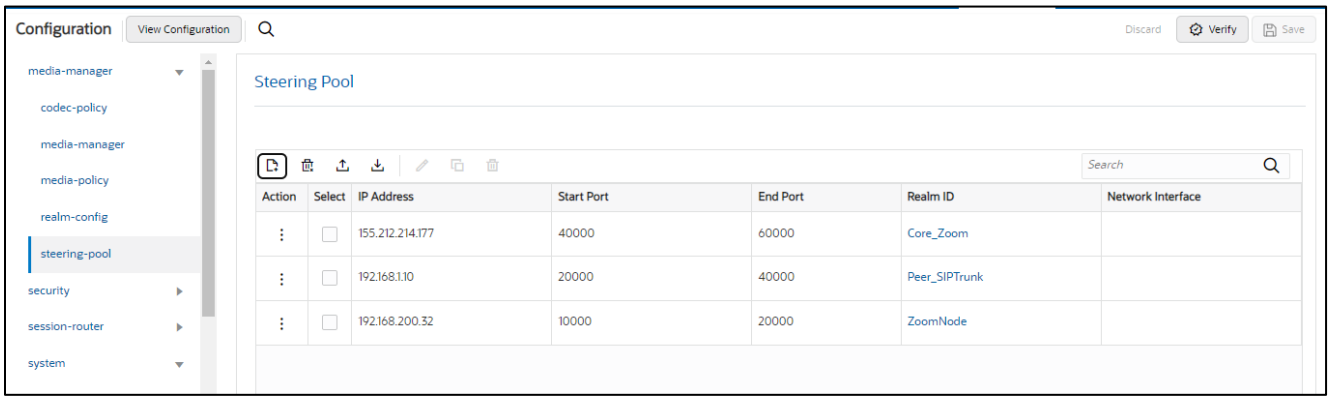
Steering pools define sets of ports that are used for steering media flows through the ORACLE SBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We configure one steering pool for PSTN and one steering pool for Zoom Phone

GUI Path: media-manager/steering-pool

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

- Click Add and use the below examples to configure.



To configure steering-pool from ACLI

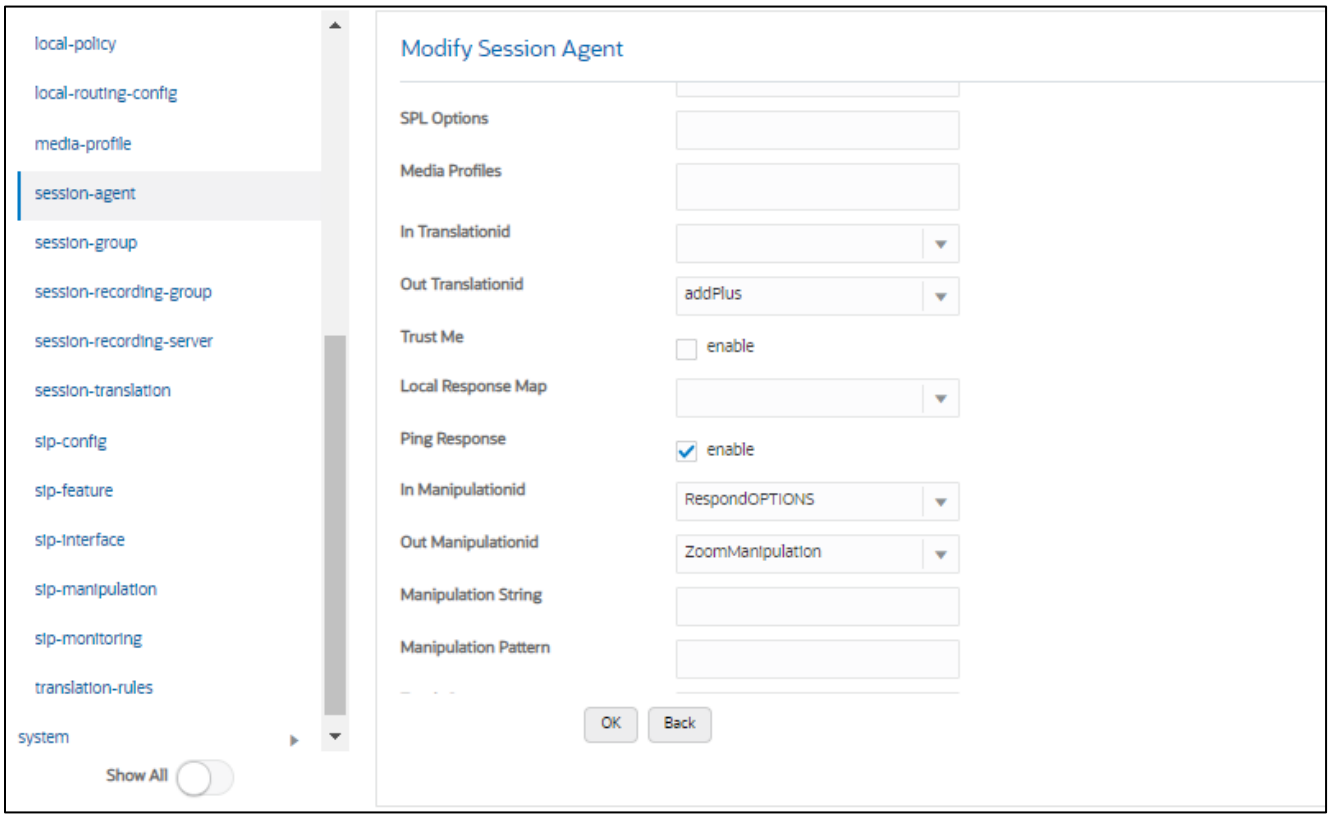
ACLI Path: config t→media-manger→steering-pool

```
steering-pool
        ip-address                  192.168.1.10
        start-port                 20000
        end-port                    40000
        realm-id                   Peer_SIPTrunk
steering-pool
        ip-address                  192.168.200.32
        start-port                 10000
        end-port                    20000
        realm-id                   ZoomNode
```

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

4.6 Responding to Options Ping

If running release SCZ830m1p7 or later, there is a new configuration parameters on the Session Agent Config element, called ping-response. When enabled on each agent, it will take that place of the following SIP-Manipulation.



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.

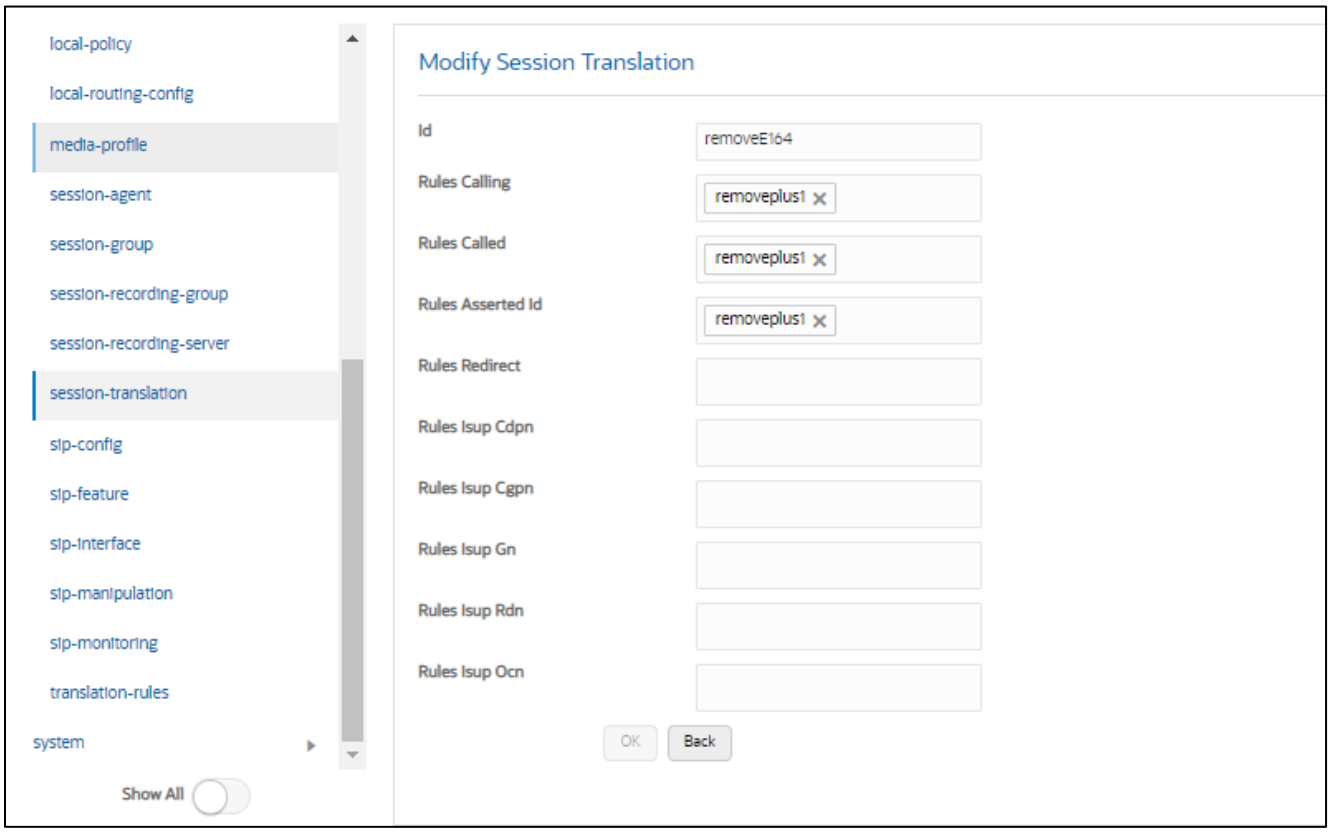
4.7 Session-Translation

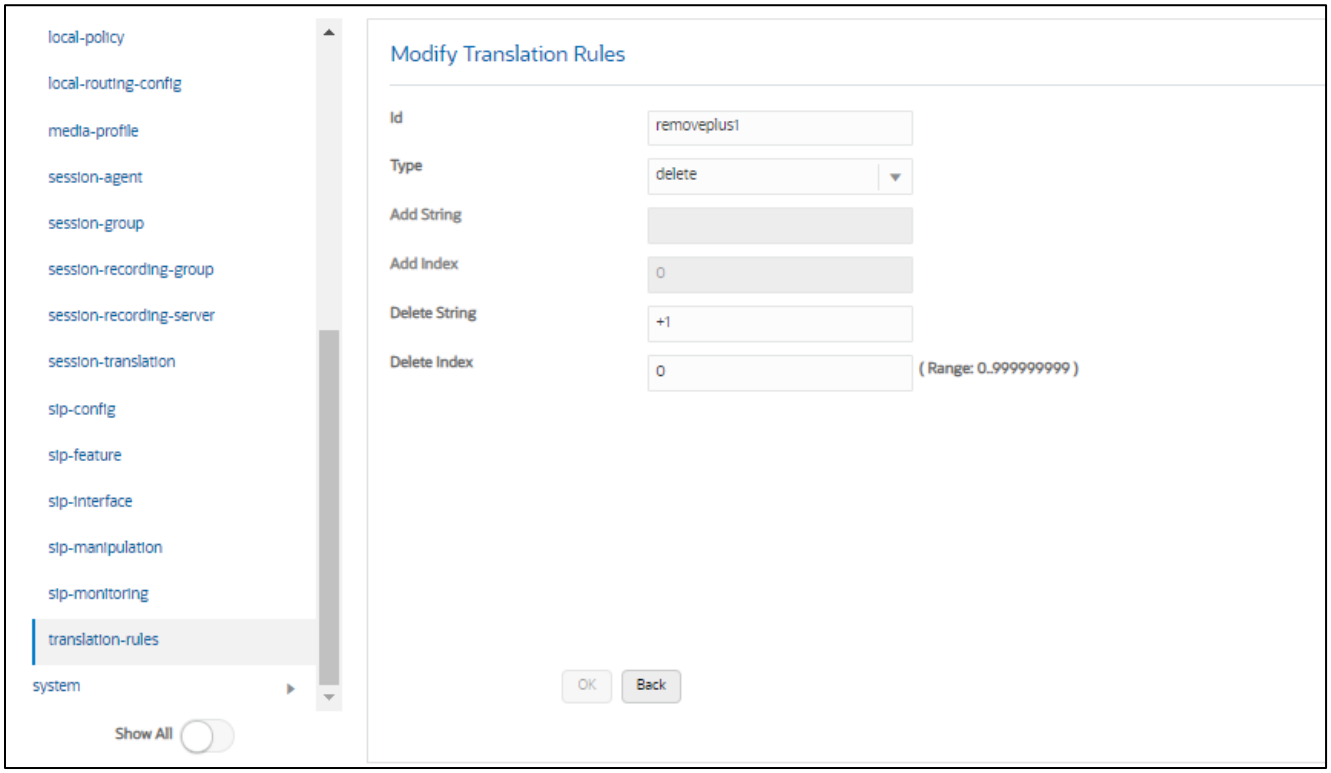
The following session-translation is created and applied as out-translational on the Session-Agent towards Carriers. This session-translation is created to remove +1 when call is sent towards Carrier as Carrier in this case requires calls to be presented in 10 digit dial format.

Note: This rule only applies to a US based Carrier and should only be implemented if needed.

GUI Path: session-router/session-translation

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





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.

4.8 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 Node.

GUI Path: session-router/SIP-interface

ACLI Path: config t→session-router→SIP-interface

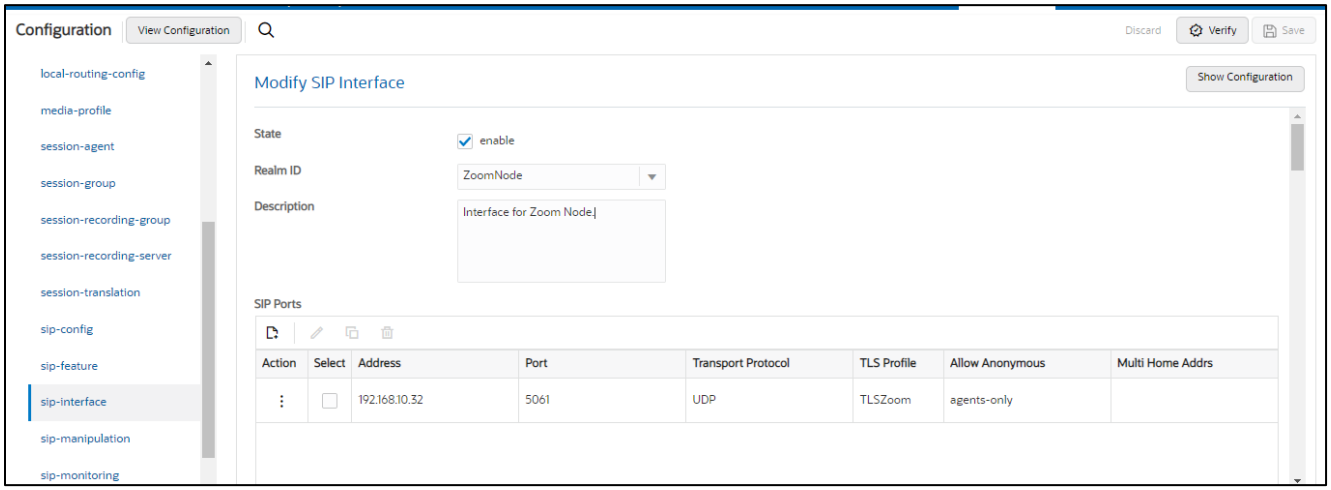
Click Add, and use the table below as an example to Configure:

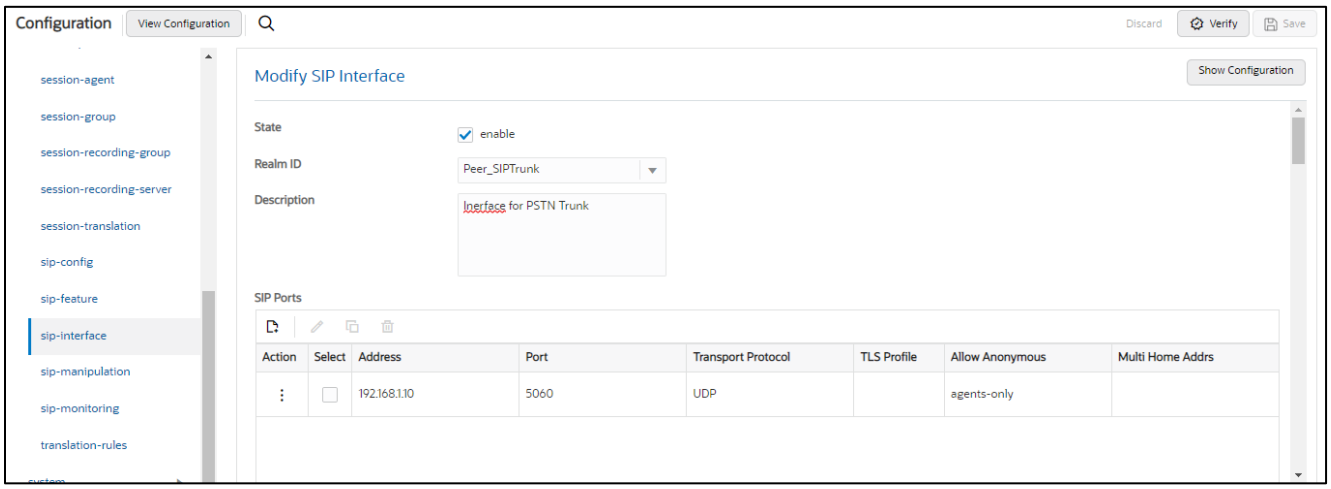
Please note, this is also where we will be assigned some of the configuration elements configured earlier in this document, ie….

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

Use the following as an example to configure SIP interfaces:

Config Parameter	SIPTrunk	Zoom
Realm ID	Peer_SIPTrunk	ZoomNode
SIP Port Config Parameter	SIP Trunk	Zoom
Address	192.168.1.10	192.168.1.32
Port	5060	5061
Transport protocol	UDP	TLS
TLS profile		TLSZoom
Allow anonymous	agents-only	agents-only





To configure sip-interface via ACLI.

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

```
sip-interface
        realm-id                        Peer_SIPTrunk
        description                      Inerface for PSTN Trunk
        sip-port
                address                         192.168.1.10
                allow-anonymous                 agents-only
sip-interface
        realm-id                        ZoomNode
        sip-port
                address                         192.168.10.32
                port                        5061
                tls-profile                  TLSZoom
                allow-anonymous                 agents-only
```

4.9 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 two session agents for Zoom Phone, and in our example, one for SIPTrunk.

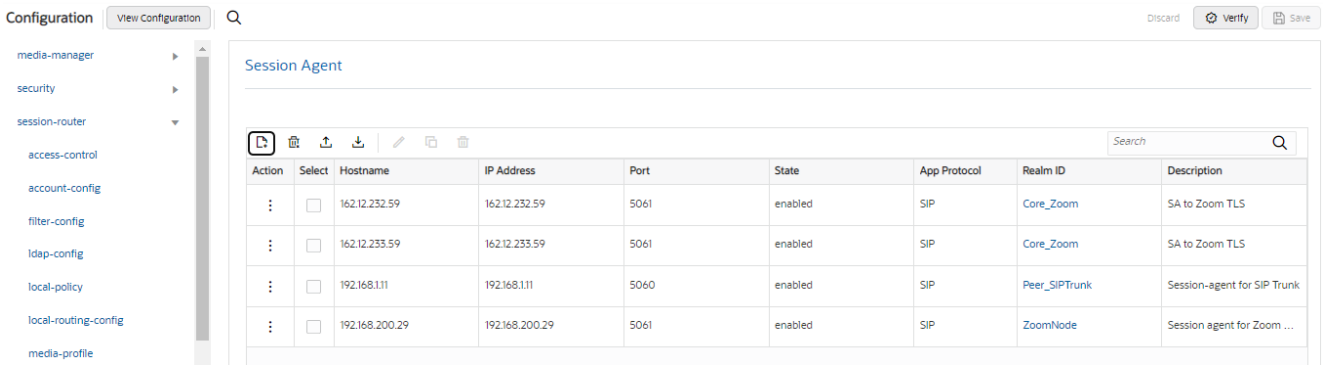
- Click Add, and use the table below to configure:

Config parameter	Zoom Node	SIPTrunk
Hostname	192.168.200.29	192.168.1.11
IP Address	192.168.200.29	192.168.1.11
Port	5061	5060
Transport method	StaticTLS	UDP+TCP
Realm ID	ZoomNode	Peer_SIPTrunk
Ping Method	OPTIONS	OPTIONS
Ping Interval	30	30
Ping Response	Enabled	Enabled

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

To configure session-agent via ACLI

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




```
session-agent
        hostname                    192.168.1.11
        ip-address                  192.168.1.11
        realm-id                   Peer_SIPTrunk
        description                 Session-agent for SIP Trunk
        ping-method                  OPTIONS
        ping-interval               60
        out-translationid            removeE164
        out-manipulationid             SIPTrunkManipulation
session-agent
        hostname                    192.168.200.29
        ip-address                  192.168.200.29
        port                       5061
        realm-id                    ZoomNode
        description                 Session agent for Zoom Node
        ping-method                  OPTIONS
        ping-interval               30
```

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

4.10 Routing Configuration

This section outlines how to configure the ORACLE SBC to route SIP traffic to and from PSTN and Zoom Phone 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.

4.10.1 Calls from PSTN to Zoom

Zoom Node is configured to accept calls in case of connectivity with Zoom Cloud System goes down, to achieve this Zoom Node is defined as an additional hop to the local-policy which is used to route calls from PSTN to Zoom Phone System.

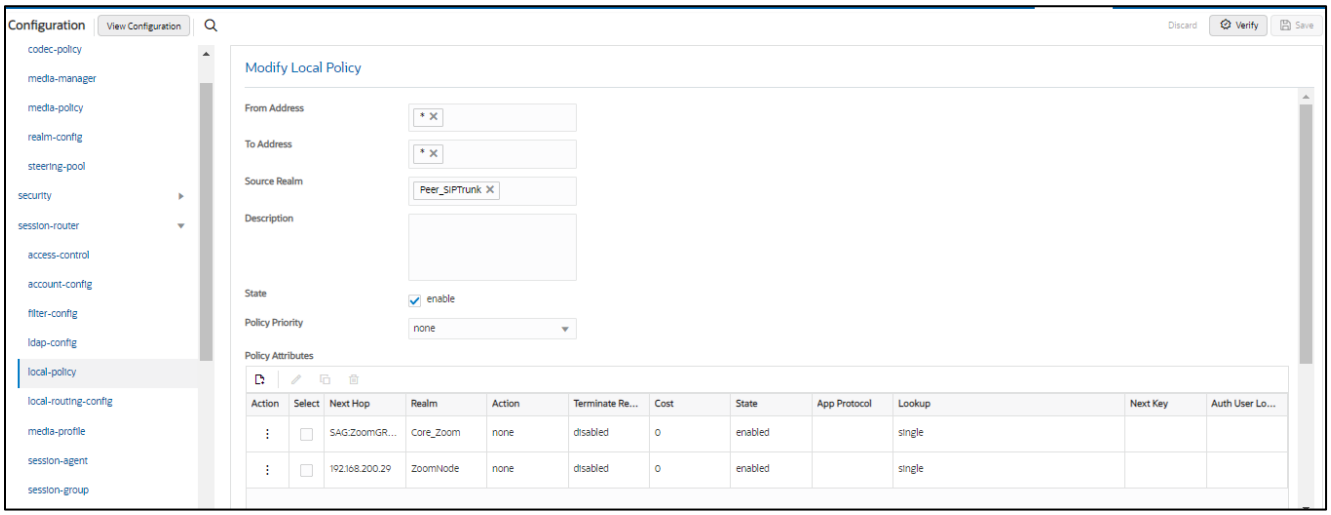
The existing local-policy routes the PSTN calls to the sag:ZoomGrp, which contains Zoom BYOC IPs.

This local-policy is modified with Zoom Node Session-Agent “192.168.200.29” defined as an additional next hop. Below is the snippet of the modified local-policy. After trying Zoom Phone System hops, the call is connected via Zoom Node.

Terminate recursion parameter should be disabled on the local-policy for SBC to try all the hops.

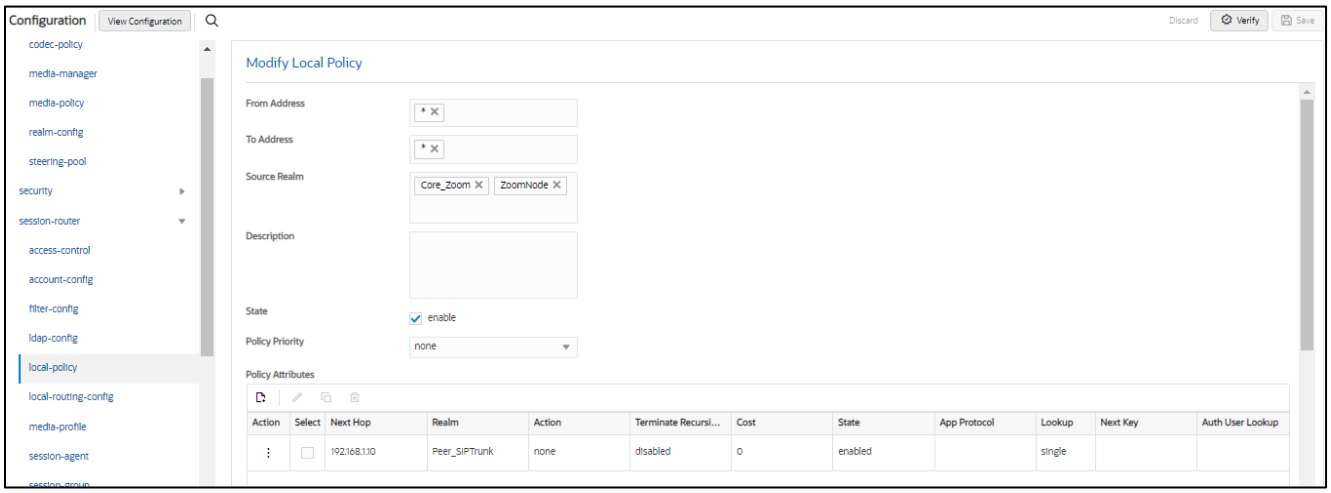
GUI Path: session-router/local-policy

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



4.10.2 Route Calls from ZoomNode To PSTN:

In order to route SIP traffic to and from Zoom Phone Platform, the source realm of the ZoomNode is added as an additional realm to the local policy which routes calls from both ZoomNode and Core_Zoom realm to Carrier Trunk.



- Click OK at the bottom of each when applicable.

```
local-policy
        from-address                *
        to-address                  *
        source-realm                  Core_Zoom
                                    ZoomNode
        policy-attribute
              next-hop                  192.168.1.10
              realm                   Peer_SIPTrunk
local-policy
        from-address                *
        to-address                  *
        source-realm                  Peer_SIPTrunk
        policy-attribute
              next-hop                  SAG:ZoomGRPTLS
              realm                   Core_Zoom
        policy-attribute
              next-hop                  192.168.200.29
              realm                   ZoomNode
```

5 ACLI Running Configuration

```
access-control
        realm-id                    Core_Zoom
        source-address                162.12.0.0/16
        destination-address            155.212.214.177
        application-protocol          SIP
        trust-level                 high
```

```
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
        realm-id                        Peer_SIPTrunk2
        source-address                      192.168.1.20
        destination-address                 192.168.1.10
        application-protocol                SIP
        trust-level                     high
capture-receiver
        address                         192.168.1.158
        network-interface                   M10:0
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             *
        to-address              *
        source-realm              Peer_SIPTrunk
        policy-attribute
                next-hop                SAG:ZoomGRPTLS
                realm                 Core_Zoom
        policy-attribute
                next-hop                192.168.200.29
                realm                 ZoomNode
media-manager
        max-untrusted-signaling          1
        min-untrusted-signaling          1
media-profile
        name                    CN
        subname                   wideband
        payload-type              118
media-sec-policy
        name                    RTP
media-sec-policy
        name                    sdesPolicy
        inbound
                profile             SDES
                mode                srtp
                protocol            sdes
        outbound
                profile             SDES
                mode                srtp
                protocol            sdes
network-interface
        name                    s0p0
```

```
        ip-address                      155.212.214.177
        netmask                         255.255.255.0
        gateway                         155.212.214.1
        dns-ip-primary                   8.8.8.8
        dns-domain                      customers.telechat.o-test06161977.com
        hip-ip-list                   155.212.214.177
        icmp-address                     155.212.214.177
network-interface
        name                           s0p1
        ip-address                      192.168.200.32
        netmask                         255.255.0.0
        gateway                         192.168.200.1
network-interface
        name                           s1p0
        ip-address                      192.168.1.10
        netmask                         255.255.255.0
        gateway                         192.168.1.1
        hip-ip-list                   192.168.1.10
        icmp-address                     192.168.1.10
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
        description                       Realm Facing Zoom Phone
        network-interfaces                s0p0:0.4
```

```
        mm-in-realm                   enabled
        media-sec-policy              sdesPolicy
        access-control-trust-level    high
        refer-call-transfer           enabled
        codec-policy                  audiotest
realm-config
        identifier                    Peer_SIPTrunk
        description                   Ream facing SIP trunk
        network-interfaces            s1p0:0.4
        mm-in-realm                   enabled
        qos-enable                    enabled
        media-sec-policy              RTP
        access-control-trust-level    high
        codec-policy                  OptimizeCodecs
        hide-egress-media-update      enabled
realm-config
        identifier                    ZoomNode
        description                   Zoom Node facing Realm
        network-interfaces            s0p1:0.4
        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                      162.12.232.59
        ip-address                    162.12.232.59
        port                          5061
        transport-method              StaticTLS
        realm-id                      Core_Zoom
        description                   SA to Zoom TLS
        ping-method                   OPTIONS
        ping-interval                 30
        out-translationid             addPlus
```

```
        in-manipulationid               RespondOPTIONS
        out-manipulationid              ZoomManipulation
session-agent
        hostname                        162.12.233.59
        ip-address                      162.12.233.59
        port                            5061
        transport-method                StaticTLS
        realm-id                        Core_Zoom
        description                     SA to Zoom TLS
        ping-method                     OPTIONS
        ping-interval                   30
        out-translationid               addPlus
        in-manipulationid               RespondOPTIONS
        out-manipulationid              ZoomManipulation
session-agent
        hostname                        192.168.1.11
        ip-address                      192.168.1.11
        realm-id                        Peer_SIPTrunk
        description                     Session-agent for SIP Trunk
        ping-method                     OPTIONS
        ping-interval                   60
        out-translationid               removeE164
        out-manipulationid              SIPTrunkManipulation
session-agent
        hostname                        192.168.200.29
        ip-address                      192.168.200.29
        port                            5061
        realm-id                        ZoomNode
        description                     Session agent for Zoom Node
        ping-method                     OPTIONS
        ping-interval                   30
        ping-response                   enabled
session-timer-profile
        name                            ZoomSessionTimer
        session-expires                 900
        force-reinvite                  enabled
        response-refresher              uac
```

```
session-translation
        id                      addPlus
        rules-calling           addPlus
        rules-called            addPlus
session-translation
        id                      removeE164
        rules-calling           removeplus1
        rules-called            removeplus1
        rules-asserted-id       removeplus1
session-group
        group-name              ZoomGRPTLS
        dest                    162.12.233.59
                                162.12.232.59
        sag-recursion           enabled
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 Phone
        sip-port
                address         155.212.214.177
                port            5061
                transport-protocol      TLS
                tls-profile     TLSZoom
                allow-anonymous         agents-only
        in-manipulationid       RespondOPTIONS
        out-manipulationid      ZoomE164
        sip-profile             forreplaces
        session-timer-profile   ZoomSessionTimer
sip-interface
        realm-id                Peer_SIPTrunk
```

```
        description                    Interface for PSTN Trunk
        sip-port
            address                    192.168.1.10
            allow-anonymous                agents-only
    sip-interface
        realm-id                   ZoomNode
        sip-port
            address                    192.168.10.32
            port                   5061
            tls-profile                TLSZoom
            allow-anonymous                agents-only
    sip-manipulation
        name                       SIPTrunkManipulation
        description                Manipulations on SIP Trunk side
        header-rule
            name                   XTraceID
            header-name                X-Trace-ID[^]
            action                 delete
            msg-type                   request
            methods                    INVITE
        header-rule
            name                   XInstanceID
            header-name                X-Instance-ID[^]
            action                 delete
            msg-type                   request
            methods                    INVITE
        header-rule
            name                   XDMInfo
            header-name                X-DM-Info[^]
            action                 delete
            msg-type                   request
            methods                    INVITE
        header-rule
            name                   XCapability
            header-name                X-Capability[^]
            action                 delete
            msg-type                   request
```

```
        methods                 INVITE
    header-rule
        name                    xpublicip
        header-name                 X-PUBLIC-IP[^]
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    xorigcontact
        header-name                 X-ORIGINAL-CONTACT[^]
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    xorigcallid
        header-name                 X-ORIGINAL-CALLID[^]
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    xtocarrier
        header-name                 X-TO-CARRIER[^]
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    xFSSupport
        header-name                 X-FS-Support[^]
        action                  delete
        msg-type                request
        methods                 INVITE
    header-rule
        name                    callAcme
        header-name                 From
        action                  sip-manip
        msg-type                request
        new-value                ACME_NAT_TO_FROM_IP
```

```
        header-rule
            name                        changeAssertedIP
            header-name                 P-Asserted-Identity
            action                      manipulate
            comparison-type             pattern-rule
            msg-type                    request
            methods                     INVITE
            element-rule
                name                    changeIP
                type                    uri-host
                action                  replace
                comparison-type         pattern-rule
                new-value               $LOCAL_IP
SIP-monitoring
        match-any-filter            enabled
        monitoring-filters          *
SIP-profile
        name                        forreplaces
        replace-dialogs             enabled
steering-pool
        ip-address                  155.212.214.177
        start-port                  40000
        end-port                    60000
        realm-id                    Core_Zoom
steering-pool
        ip-address                  192.168.1.10
        start-port                  20000
        end-port                    40000
        realm-id                    Peer_SIPTrunk
steering-pool
        ip-address                  192.168.200.32
        start-port                  10000
        end-port                    20000
        realm-id                    ZoomNode
system-config
        hostname                    zoom.us
        description                 SBC for Zoom Phone
```

```
        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     GUI
```

6 Sample call flow

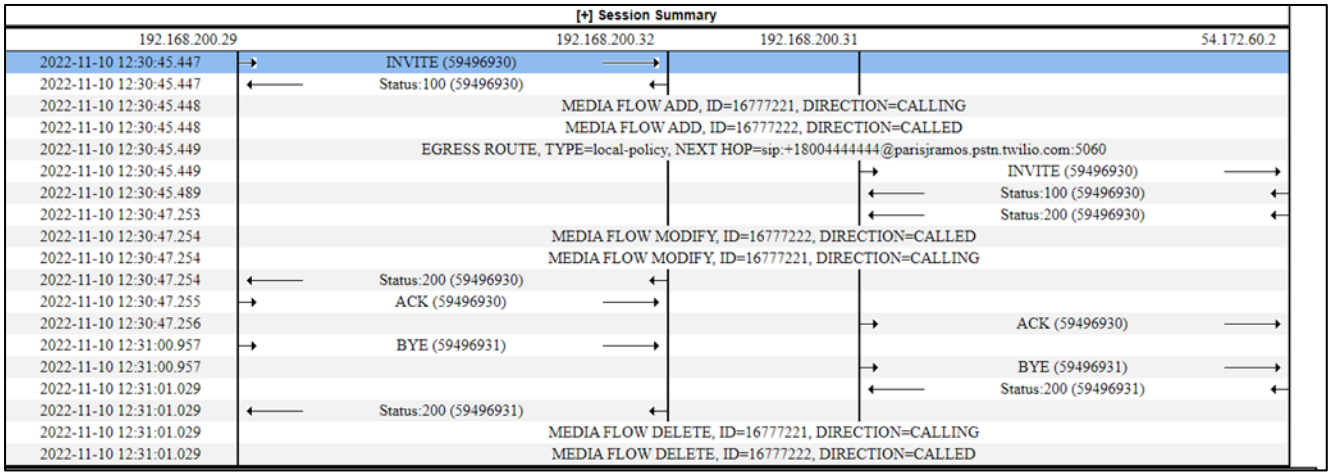
Following is a sample call flow for a call from Zoom Node towards Oracle SBC.

1.ZoomNode IP Address- 192.168.200.29

2.Oracle SBC IP Address -192.168.200.32

3.Oracle SBC IP address towards PSTN – 192.168.200.31

4.PSTN Trunk IP address – 54.170.60.2



Below Figure indicates the SIP and SDP Headers from Zoom Node in the SIP INVITE

```
INVITE sip:+18004444444@192.168.200.32:5061;transport=tls SIP/2.0
Via: SIP/2.0/TLS 192.168.200.29:5091;branch=z9hG4bKecS2m0ZjypvNr
Max-Forwards: 69
From: "19844644662" <sip:+19844644662@10001201.zoom.us>;tag=1gt6teBpDB57B
To: <sip:+18004444444@192.168.200.32:5061>
Call-ID: 40177d6e-dbc0-123b-cc8c-000c29d1f730
CSeq: 59496930 INVITE
Contact:
<sip:gw+bpXTdJ1tSau4a_XG0UqYGw@192.168.200.29:5091;transport=tls;gw=bpXTdJ1
tSau4a_XG0UqYGw>
User-Agent: Zoom PBX
Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, MESSAGE, INFO, UPDATE, REGISTER,
REFER, NOTIFY, PUBLISH, SUBSCRIBE
Supported: timer, outbound, path, replaces
Allow-Events: talk, hold, conference, presence, as-feature-event, dialog,
line-seize, call-info, sla, include-session-description, presence.winfo,
message-summary, sync-key, refer
Privacy: none
Content-Type: application/sdp
Content-Disposition: session
```

```
Content-Length: 1683
X-DM-Info: 192.168.1.123<9356,9358,21271>
X-Instance-ID: ZoomChat_pc_ALNTOzpmUqQdB
X-Capability: 187151
X-Trace-ID: aZ3v8l632F0UC502
Phone-Type: pstn
X-FS-Support: update_display,send_info
P-Asserted-Identity: "19844644662"sip:+19844644662@192.168.200.32:5061

v=0
o=FreeSWITCH 1668063757 1668063758 IN IP4 192.168.200.29
s=FreeSWITCH
c=IN IP4 192.168.200.29
t=0 0
m=audio 37688 RTP/SAVP 102 103 9 0 8 104 101
a=rtpmap:102 opus/48000/2
a=fmtp:102 useinbandfec=1; maxaveragebitrate=40000; maxplaybackrate=24000;
ptime=20; minptime=10; maxptime=40; stereo=1
a=rtpmap:103 opus/48000/2
a=fmtp:103 useinbandfec=1; maxaveragebitrate=40000; maxplaybackrate=24000;
ptime=20; minptime=10; maxptime=40
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:104 telephone-event/48000
a=fmtp:104 0-15
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtcp-mux
a=rtcp:37688 IN IP4 192.168.200.29
a=crypto:1 AEAD_AES_256_GCM_8
inline:QW5Dsugjq+U1soIVUK7DSB9GMLrIuMgF7iA7eAkbguCwVXwdbX6yqMj3/1M=
a=crypto:2 AEAD_AES_256_GCM
inline:imVBBHSol6uE1A9HX5JQDhVRCnnNZc/r9VsdKE4BHMOQ4K3I8+M5wOSU6vI=
a=crypto:3 AEAD_AES_128_GCM_8
inline:/Q/rEtU+N+amQPni4ryHOVVFVQiiMeUeL/DtOg==
a=crypto:4 AEAD_AES_128_GCM inline:WQKy7gw8HsjdKm+bBBFufsN7sY0R6AEYV9lr8g==
a=crypto:5 AES_256_CM_HMAC_SHA1_80
inline:N+p6ptiTcfyrkFFrHzkj5XC3qQIE/fJlgNwjCQWO/ORInKxorS6VazdxQsxVnA==
a=crypto:6 AES_192_CM_HMAC_SHA1_80
inline:FHI5GYX3fuhLXZPpd4PSwMe1Jjr9fC707F4ohrwc8KDrTi9vBUs=
a=crypto:7 AES_CM_128_HMAC_SHA1_80
inline:KQ/Vv+gQBt7eT7fKn5b3XHFEuH+WGxju7cNKLqWi
a=crypto:8 AES_256_CM_HMAC_SHA1_32
inline:JaztTNuLnR7csxGIB6okpxRXqiWaLwYGCsuDOc1OIU7gr/vNqgcipJhTffELuQ==
a=crypto:9 AES_192_CM_HMAC_SHA1_32
inline:thnxON67Z8NFofcL9HhiZD4YCk2YmTTmCPZu9nLQNnVNN+XFQn4=
a=crypto:10 AES_CM_128_HMAC_SHA1_32
inline:7rt82sPTNU0eBRpsHrFSNOgIsMkUfji3wFdcEyFl
a=crypto:11 AES_CM_128_NULL_AUTH
inline:kbKk0jYyiKjrCTcznIP1GXVaVjZ4jWui31OKG7PO
a=ptime:20
```

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/Oracle/

twitter.com/Oracle

oracle.com

Oracle Corporation, World Headquarters

500 Oracle Parkway

Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000

Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services