ORACLE

Oracle SBC with Spectralink Virtual/200/400/6500 IP-DECT Servers

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.

Revision History

Version	**Description of Changes**	**Date Revision Completed**
1.0	Initial Draft	12th December 2024

1 Table of Contents

2 INTENDED AUDIENCE 5

3 DOCUMENT OVERVIEW 5

4 ABOUT SPECTRALINK 5
4.1 DECT SERVERS 5
4.2 S SERIES HANDSETS 5

5 INTRODUCTION 6
5.1 AUDIENCE 6
5.2 REQUIREMENTS 6
5.3 ARCHITECTURE 6

6 ZOOM CONFIGURATION 7
6.1 ADD DEVICE 7
6.2 SIP ACCOUNT DETAILS 9

7 SPECTRALINK IP-DECT 9
7.1 CONFIGURATION OF IP-DECT SERVER 10
7.1.1 Basic Network Settings 10
7.1.2 Recommended Network Configuration 11
7.1.3 SIP Settings 11
7.1.4 Enable Feature Codes 13
7.1.5 Security Settings 14
7.1.6 Adding Users and Handsets 15

8 CONFIGURING THE SBC 17

9 NEW SBC CONFIGURATION 17
9.1 SETUP PRODUCT 17
9.2 SETUP ENTITLEMENTS 18
9.3 ENABLE MANAGEMENT GUI 19
9.4 CONFIGURE SBC USING WEB GUI 19
9.5 SYSTEM-CONFIG 21
9.5.1 NTP-Sync 21
9.6 NETWORKING CONFIGURATION 22
9.6.1 Physical Interfaces 22
9.6.2 Network Interfaces 23
9.7 SECURITY CONFIGURATION 23
9.7.1 Certificate Records 23
9.7.2 SBC End Entity Configuration 24
9.7.3 Root CA and Intermediate Certificates 25
9.7.4 Generate Certificate Signing Request 25
9.7.5 Import Certificates to SBC 26
9.7.6 TLS Profile 27
9.7.7 Media Security 28
9.8 MEDIA CONFIGURATION 30
9.8.1 Media Manager 30
9.8.2 Realm Config 31
9.8.3 Steering Pools 32
9.9 SIP CONFIGURATION 32
9.9.1 Sip-Config 32

9.9.2 Sip Interface 33
9.9.3 Session Agents 34
9.10 ROUTING CONFIGURATION 35
9.11 ACCESS CONTROLS 36
9.12 SAVE AND ACTIVATE 37
9.12.1 Save Config 37
9.12.2 Activate Config 37
10 APPENDIX A 37
10.1 ORACLE SBC DEPLOYED BEHIND NAT 37
11 APPENDIX B 38
11.1 ACLI RUNNING CONFIGURATION 38
12 APPENDIX C 41
12.1 FEATURES TESTED AND SUPPORTED 41

2 Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers, partners, and end users of the Oracle Enterprise Session Border Controller (SBC). It's assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform along with the Specrtalink IP-DECT servers.

3 Document Overview

The purpose of this Application Note is to guide user's on configuring Oracle SBC to work with Spectralink IP-DECT Server and DECT S Series Wireless Endpoints. This document covers a full operational configuration of the Oracle SBC deployed in an access environment with Spectralink IP-Dect and Zoom Phone Local Proxy as a registrar. The solution contained within this document has been tested using Oracle Communication SBC with **OS930p2**

4 About Spectralink

Spectralink is a leading global provider of enterprise mobility solutions, empowering businesses with seamless communication and collaboration in the digital age. Since their inception, they have been on a relentless journey to revolutionize the way organizations connect, communicate, and operate. Their commitment to innovation, reliability, and customer-centricity has earned the trust of countless enterprises across diverse industries, including healthcare, retail, manufacturing and more.

4.1 DECT Servers

Within the Spectralink DECT Server Series, customers will discover a selection of wireless server options tailored to businesses of various sizes. Spectralink servers offer flexibility and scalability, seamlessly aligning with your calling platforms, whether on-premises or hosted in the cloud. Embracing open standards, Spectralink DECT servers (integrate) with numerous third-party applications, and their adaptability can be fine-tuned to match your unique requirements.

4.2 S Series Handsets

S Series handsets are reliable, durable, and secure to support the daily demands of in-building deskless workforces. Loaded with features, S Series is designed to empower your teams with the right tools for more efficient communication and collaboration on the move. Available in three models to provide the right solution for workers across many industries.

For more information, please see the link below:

https://www.spectralink.com/

5 Introduction

5.1 Audience

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

5.2 Requirements

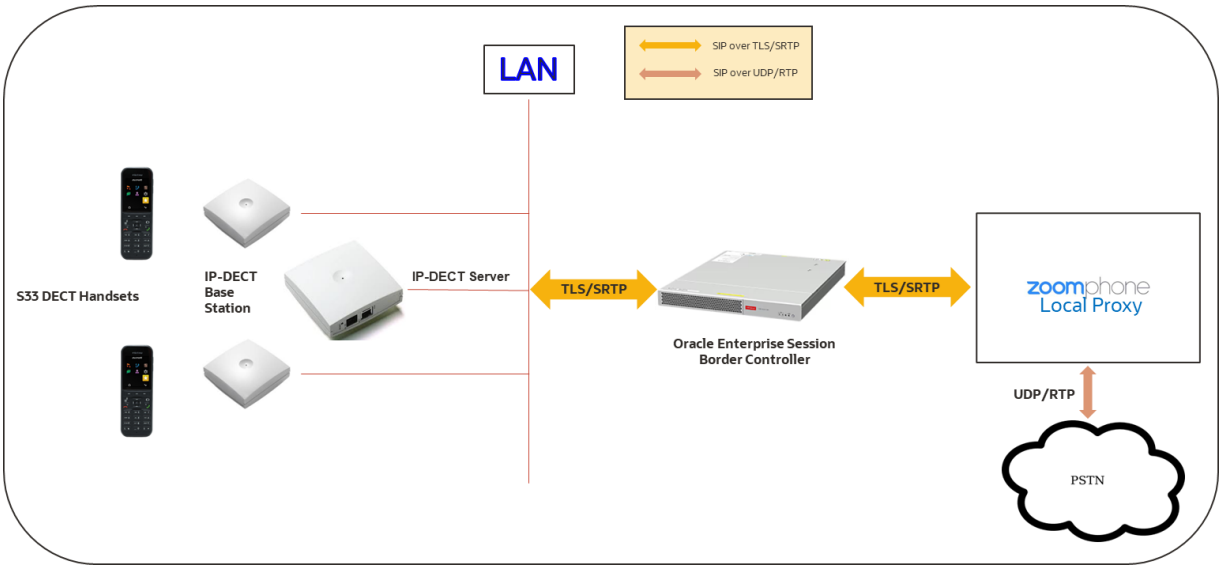
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 9.3.0 version.
- IP-DECT Server and Base station with S Series Wireless Endpoints
- Zoom Phone account: a valid Zoom Phone subscription is required to assign a Spectralink IP-DECT endpoint.
- Zoom approval for provisioning of Spectralink endpoints as Generic SIP devices. Administrators should contact their Zoom Account Executive to start an approval process.

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

Software Used	SBC Version	IP-DECT Server Version
Revision 1	9.3.0	PCS24Bb Build 126538

5.3 Architecture

Below figure illustrates the position of Spectralink IP-Dect Server, Base Stations and Endpoints in a Customer Network. In this scenario, Spectralink Endpoints are enabled with the Zoom Native Calling Plan. Oracle SBC, which is certified with Zoom Phone, is hosted in the Enterprise Network's premise DMZ and is used to steer the signaling and media from Spectralink towards the Zoom Cloud. Spectralink Wireless Endpoints in the Corporate premise register onto the Zoom Cloud through Oracle SBC which maintains a local cache of these registrations. Oracle SBC is configured to route all outbound calls to the Registrar (Zoom Cloud) which terminates it to the PSTN Network.



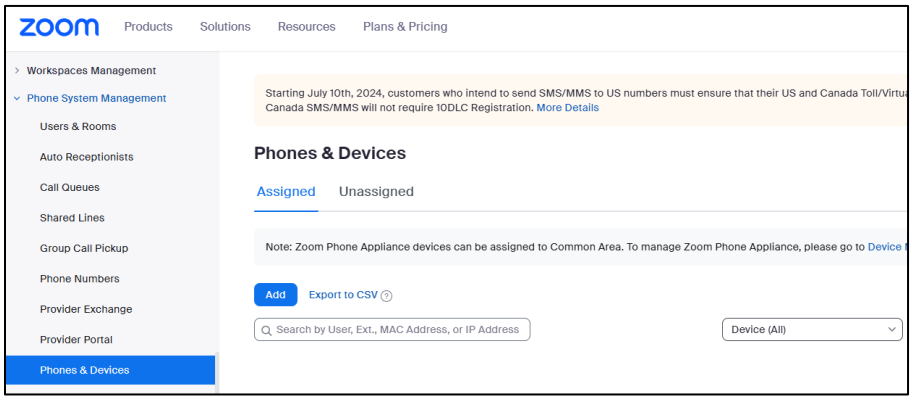
6 Zoom Configuration

This section provides instructions on how to configure 3rd Party SIP endpoints in Zoom Web Portal. For steps to configure Zoom Phone and enable Zoom's Local Proxy feature, please see the link below:

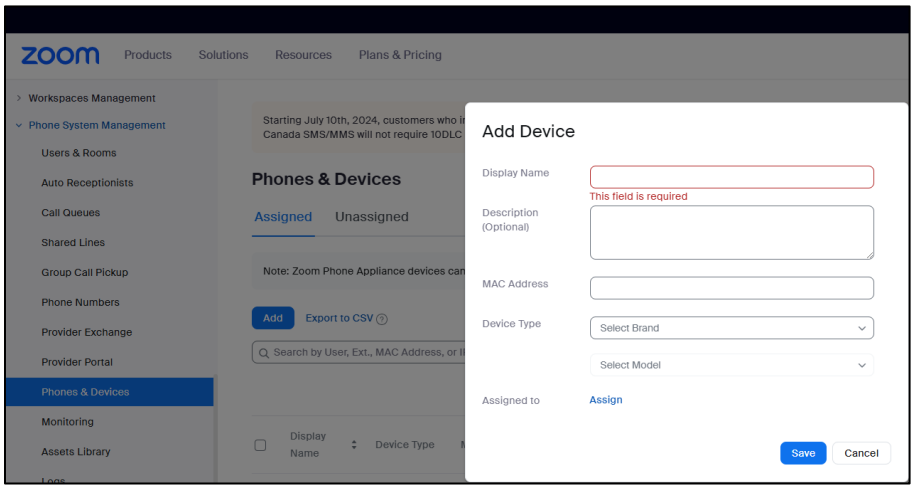
https://www.oracle.com/a/otn/docs/oracle-sbc-working-as-zoom-phone-local-proxy-vga1.0.pdf

6.1 Add Device

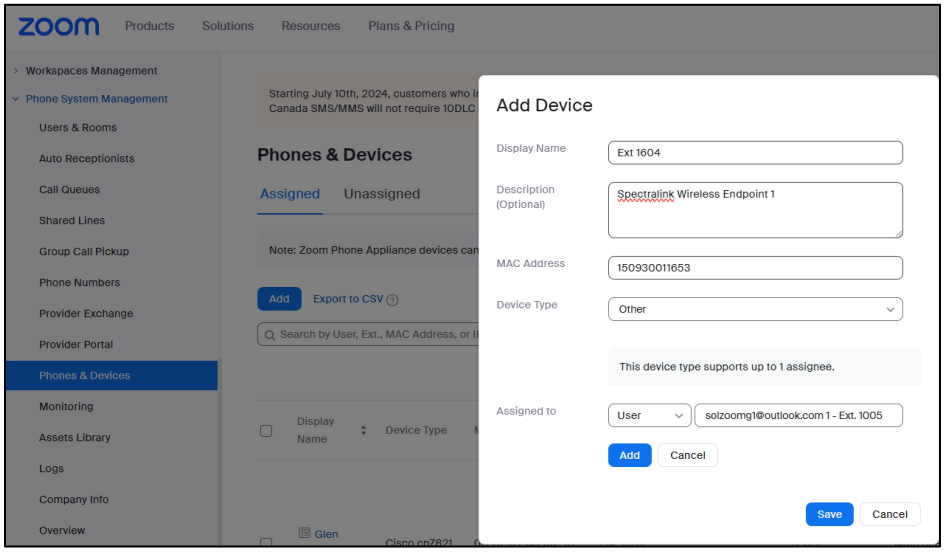
- Navigate to Phone System Management > Phone and Devices



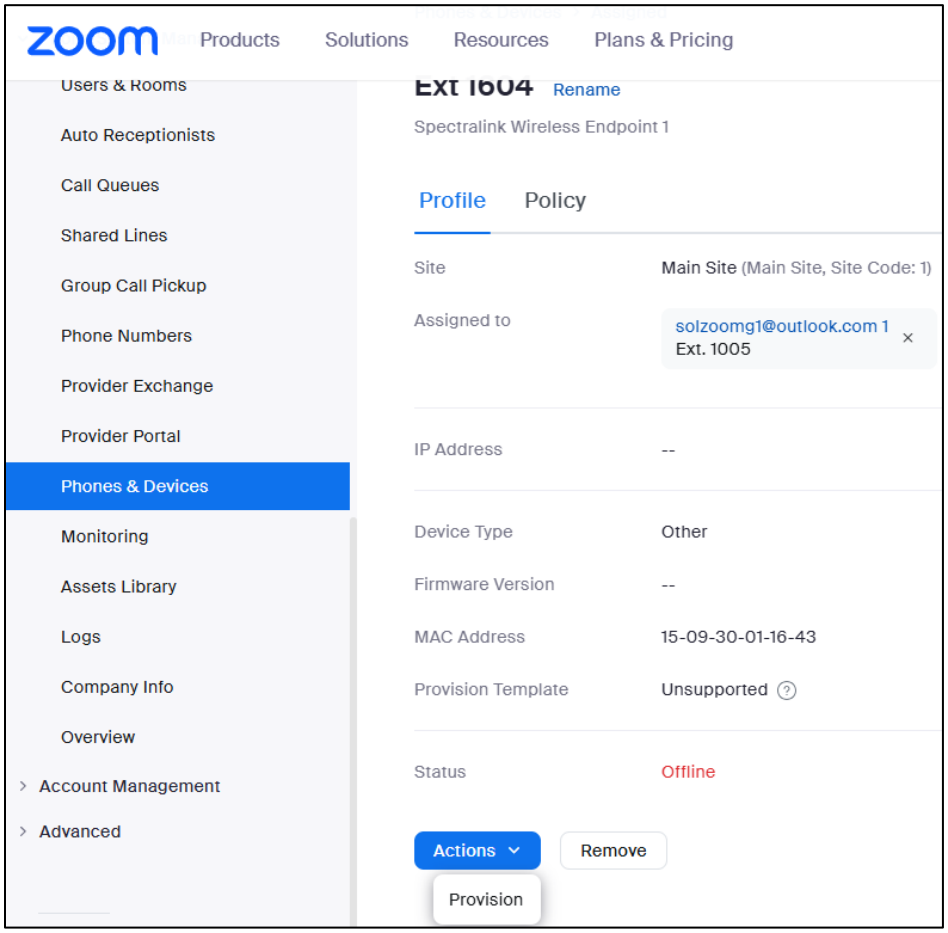
- Select Add

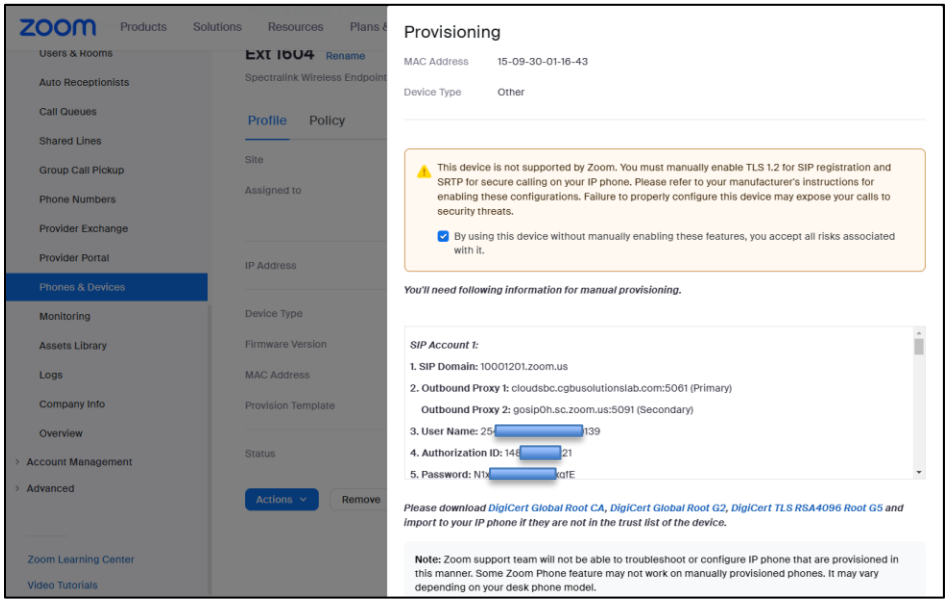


- Enter a Display Name to identify the phone.
- Choose Device type and select Other.
- Insert MAC Address **-** use Spectralink IPEI for individual handset – can be found on handset label or in IP-DECT Server Web portal.
- Enter the username or email of the phone user into the Assigned to field. If you have multiple sites, the phone will belong to the same site as the phone user.
- Click Save



- At the bottom of the Screen, Under Actions, Select Provision





6.2 Sip Account Details

Important – you will now see **SIP Account** details required to configure Spectralink IP-DECT Server and DECT Endpoint for the individual user.

SIP Account 1:

1. SIP Domain: 10001201.zoom.us

2. Outbound Proxy 1: cloudsbc.cgbusolutionslab.com:5061 (Primary)

Outbound Proxy 2: gosip0h.sc.zoom.us:5091 (Secondary)

3. User Name: 254[redacted]0139

4. Authorization ID: 14[redacted]1

5. Password: N1x[redacted]xqfE

Notice the two outbound proxies listed in the account details. The first is for the Oracle SBC, the second, Zoom Phone Local Proxy.

Repeat these steps for each Spectralink Wireless Endpoint you need to Register into Zoom Phone Local Proxy.

7 SpectraLink IP-DECT

This section provides instructions on how to configure Spectralink IP-DECT Server and DECT Endpoints

Before configuring the Spectralink IP-DECT Server, get the Zoom SIP settings for each handset. The SIP settings are configured on the Spectralink IP-DECT Server allowing handsets to register with Zoom Phone. Once the handset is registered, its able to make and receive calls.

Make sure to have followed the required steps in section 6 above or log in as an Administrator to your Zoom Online Account and retrieve the following:

- SIP Domain
- Outbound proxy
- Download available CA certificate for devices
- User credentials per device you wish to configure
    - User Name
    - Password
    - Authorization ID

Below is a description of how to configure the Spectralink IP-DECT Server and how to add users and handsets to the system.

It is assumed that you have installed and configured the Spectralink IP-DECT Server solution including deployment and administration of base stations before continuing the configuration outlined below.

You can access the web GUI Administration Page of the Spectralink IP-DECT Server by entering the IP address into a standard web browser, along with the username and password.

- Default username: **admin**
- Default password: **admin**

For configuration required to integrate Spectralink IP-DECT Server 200/400/6500 or Virtual IP-DECT Server One with Zoom Phone you will need information about IPEI of the handset and ARI of the server:

You can identify the unique ARI number on the server in the following ways:

- Spectralink IP-DECT Server 6500: See label on the bottom of the server.
- Spectralink IP-DECT Server 200/400: See label on the rear side of the server.
- Spectralink IP-DECT Server 200/400/6500 and Virtual IP-DECT Server One: From the management GUI: Administration Page→Status→Wireless Server.

You can identify the unique IPEI number on a handset in two ways:

- From the handset: Menu→Status→General
- See Label on the rear side of handset.

7.1 Configuration of IP-DECT Server

This section outlines the configuration needed for the Spectralink IP-DECT Server and Spectralink Wireless Endpoints.

7.1.1 Basic Network Settings

- From a DHCP server Using DHCP the device requests and obtains an available IP address from a DHCP server. The device also obtains other parameters such as the default gateway, subnet mask, DNS server, Time server and other IP parameters from the DHCP server.
- Entered manually through web GUI
  Administration Page→Configuration→General→General Configuration

Using network configuration, enter the IP-addresses and other networking parameters manually through the management GUI.

7.1.2 Recommended Network Configuration

Spectralink recommends the following when configuring the IP-DECT Server solution:

- Spectralink IP-DECT Server 200/400/6500 and Virtual IP-DECT Server One using a static IP address.

This is to avoid sudden change of the IP address which would temporarily affect all base stations and thus the entire installation.

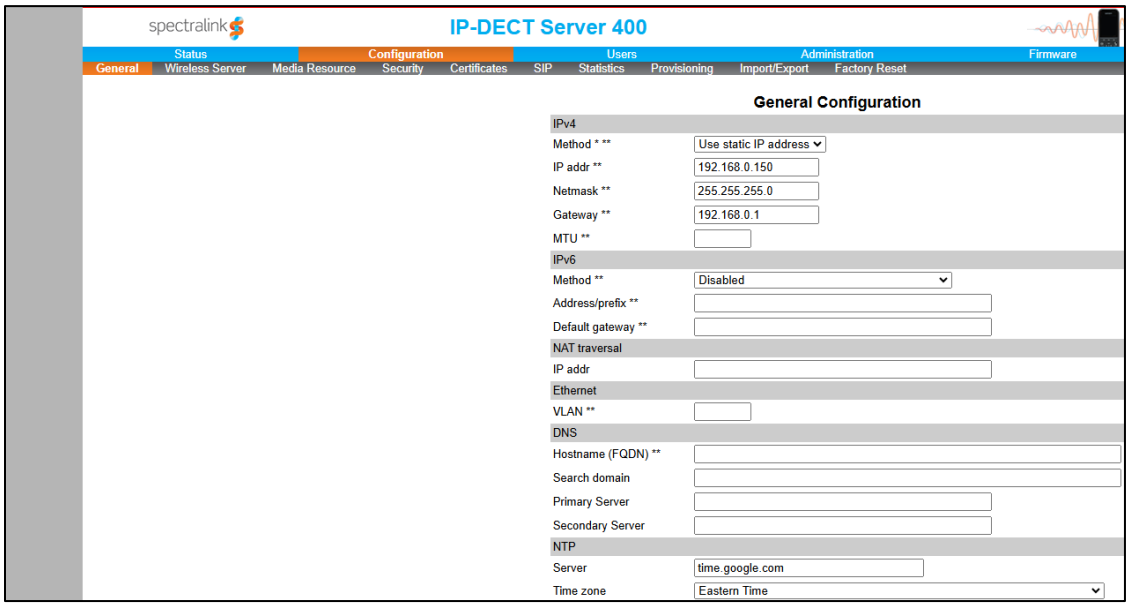
- Spectralink DECT Media Resources (optional module for more increased voice channels on Virtual IP-DECT Server) using a static IP address.

Like with the servers, this is to avoid sudden change of the IP address.

- Spectralink IP-DECT Base Stations using DHCP. This makes it easy to manage many base stations without having to keep track of all assigned IP addresses.

When the base stations are set up to DHCP, you can use UPnP to discover all the Wireless devices on the local network.

Spectralink IP-DECT Base Stations and Spectralink DECT Media Resources can be managed from the web GUI Administration Page of the Spectralink IP-DECT Server.



7.1.3 SIP Settings

The Spectralink IP-DECT Server requires some SIP settings to be adjusted to connect to Zoom Phone through the Oracle Session Border Controller

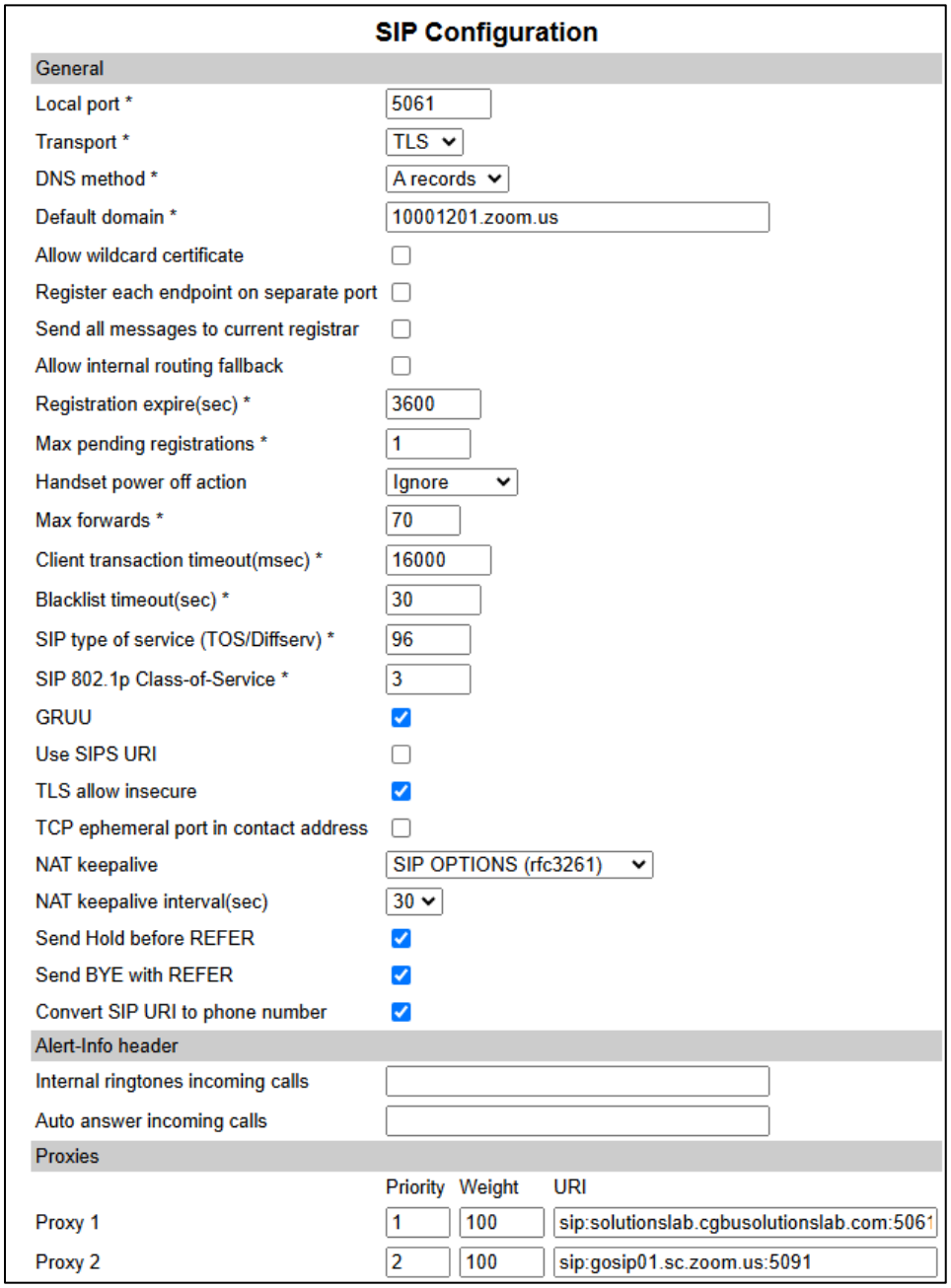
SIP settings not mentioned below should be left at their default values.

To modify the SIP settings from the Administration Page:

- Click Configuration, and then click SIP.

Use the below table as an example to configure SIP Settings

Field	Setting
Local Port	5061
Transport	TLS
Default Domain	10001201.zoom.us (Zoom Domain)
Nat keepalive (OPTIONAL)	SIP OPTIONS (rfc3261)
NAT keepalive interval(sec) (Optional)	30
Proxy 1	sip:solutionslab.cgbusolutionslab.com:5061 (SBC)
Proxy 2	sip:gosip01.sc.zoom.us:5091 (ZPLP)



- Click Save at the bottom.

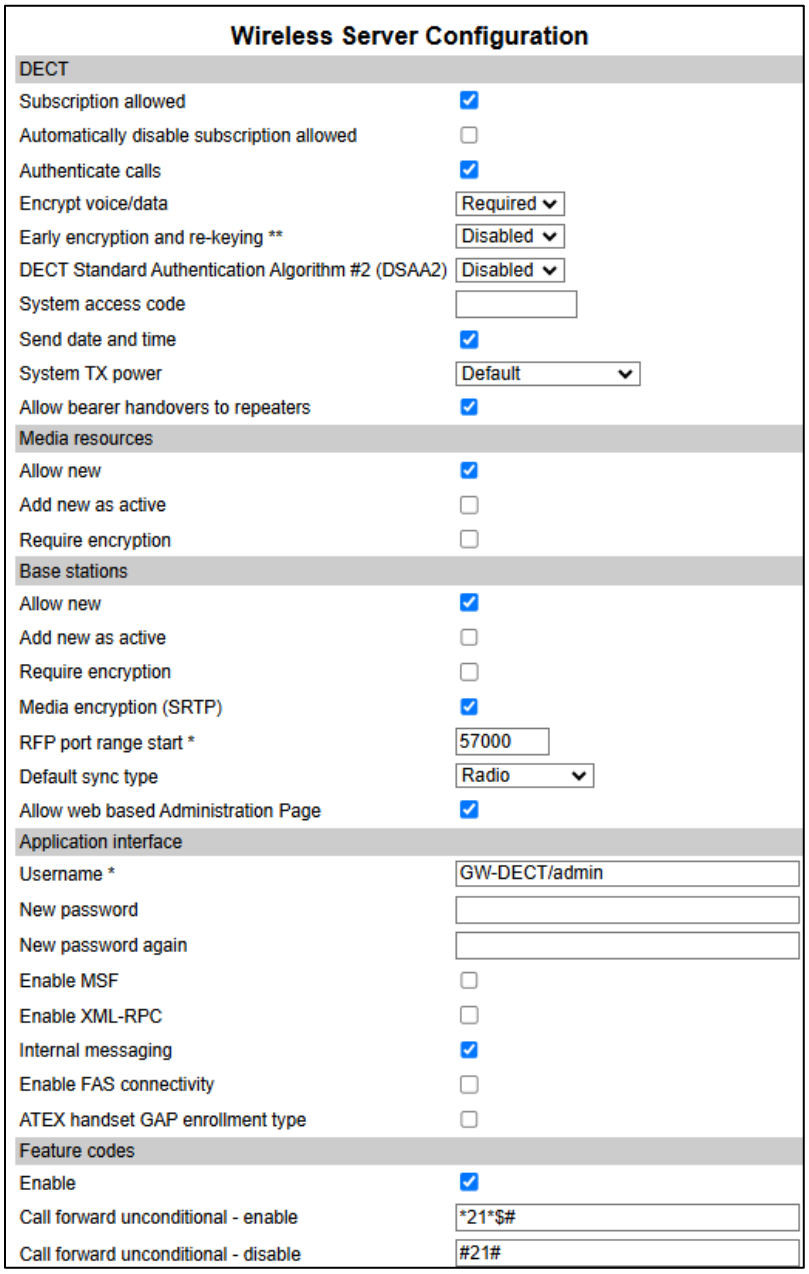
7.1.4 Enable Feature Codes

The feature, Call forward unconditional can be accessed by dialing special feature codes from the DECT handsets. To provide access to the this feature, feature codes must be enabled.

To Enable Feature Codes from the Management GUI:

Configuration→Wireless Server

Under Feature codes, check the box next to Enable.



Wireless Server Configuration

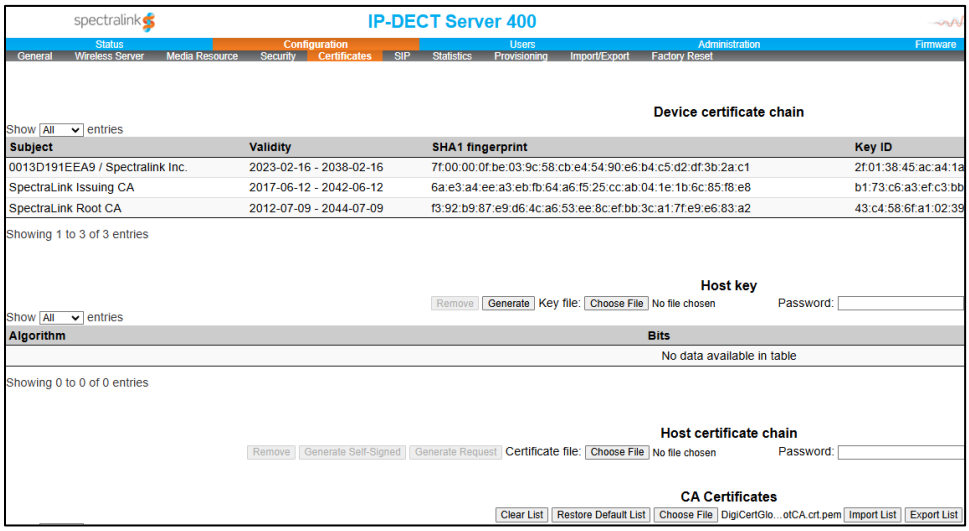
DECT	
Subscription allowed	☑
Automatically disable subscription allowed	☐
Authenticate calls	☑
Encrypt voice/data	Required
Early encryption and re-keying **	Disabled
DECT Standard Authentication Algorithm #2 (DSAA2)	Disabled
System access code	
Send date and time	☑
System TX power	Default
Allow bearer handovers to repeaters	☑
Media resources	
Allow new	☑
Add new as active	☐
Require encryption	☐
Base stations	
Allow new	☑
Add new as active	☐
Require encryption	☐
Media encryption (SRTP)	☑
RFP port range start *	57000
Default sync type	Radio
Allow web based Administration Page	☑
Application interface	
Username *	GW-DECT/admin
New password	
New password again	
Enable MSF	☐
Enable XML-RPC	☐
Internal messaging	☑
Enable FAS connectivity	☐
ATEX handset GAP enrollment type	☐
Feature codes	
Enable	☑
Call forward unconditional - enable	*21*$#
Call forward unconditional - disable	#21#

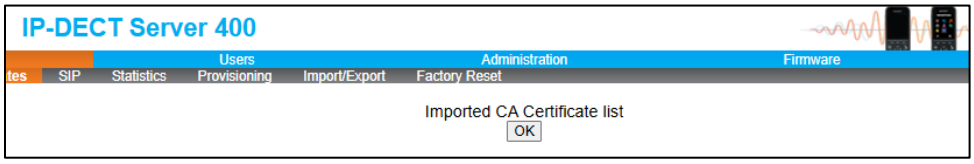
- Click Save at the bottom.

7.1.5 Security Settings

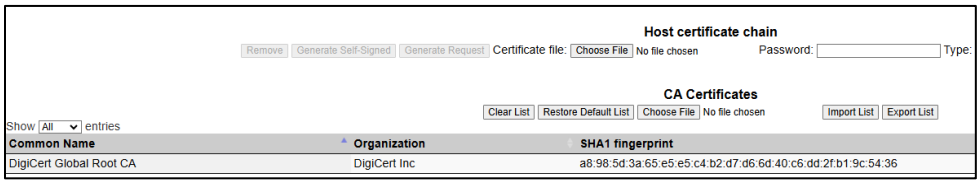
To Secure the connection between the SpectraLink IP-Dect Server and the Oracle SBC, we need to import the Root CA certificate used to sign the SBC's end entity certificate to the Servers trust store. In the Servers management GUI, under Configuration→Certificates

- Under CA Certificates, Click on Choose File
- Select the Root CA certificate used to sign the SBC's end entity certificate
- Click Import List
- Import CA Certification List, Click OK



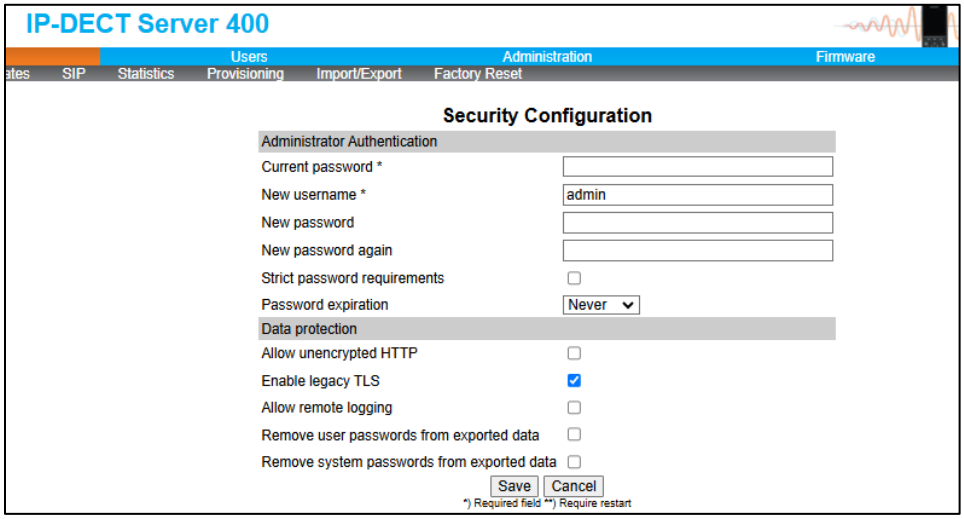


- Verify the Certificate was imported into the servers trust store:



Next, we'll enable Legacy TLS through the management GUI:

Configuration→Security

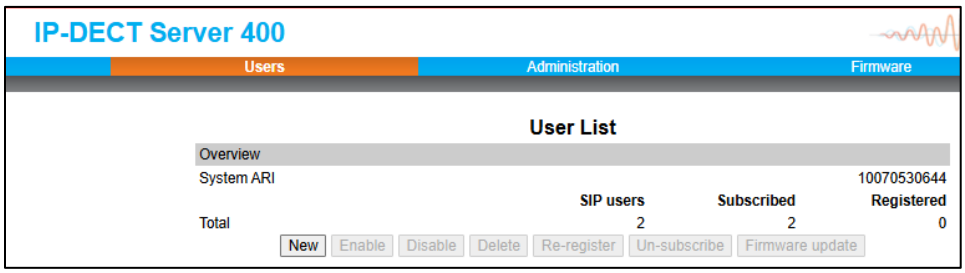


- Click Save and Reboot the server.

7.1.6 Adding Users and Handsets

Each individual handset/user must be added to the Spectralink IP-DECT Server and to Zoom Phone. This section describes how to add the handsets to the Spectralink IP-DECT Server.

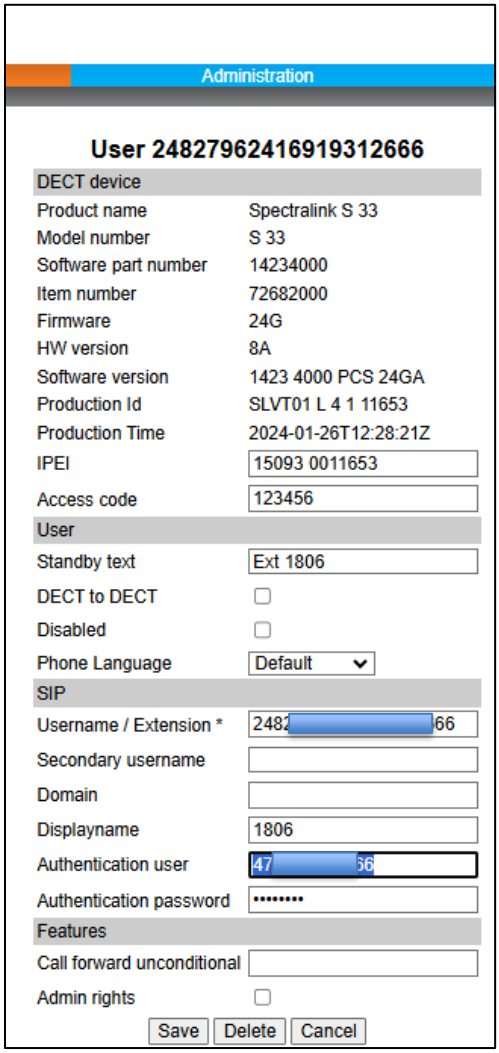
- From the Spectralink Management GUI, Click Users then Click New:



Use the table below as an example to configure each user endpoint that will access the IP DECT wireless system:

Note: To provision users, you will need the Username, Auth ID and Password from Zoom Provisioning.

Field	Setting
IPEI	15093 0011653
Username/Extension	248[redacted]66
Display Name	1806
Authentication User	47[redacted]66
Authentication Password	N1xl[redacted]xqfE



- Click Save at the bottom.

This concludes the minimum required configuration of Spectralink IP-DECT server. Now we'll move on to configuring the Oracle SBC as a local proxy.

8 Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC as a local proxy for Spectralink IP-DECT Server and Zoom phone.

Validated Oracle SBC version

Oracle conducted tests with Oracle SBC 9.3 software – this software with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6300
- AP 6350
- AP 3950
- AP 4900
- VME

9 New SBC configuration

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

As there are many ways to install the SBC (purpose-built appliance, VM, and public cloud deployment), please follow the link given below for the type of install base used to deploy the Oracle SBC.

https://docs.oracle.com/en/industries/communications/session-border-controller/9.3.0/installation/index.html

Once the SBC is installed and logged in, please follow the steps given below.

9.1 Setup product

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

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

```
NN4600-139# setup product

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

Last Modified 2023-02-07 15:50:20
---------------------------------------------------------------
 1 : Product       : Enterprise Session Border Controller

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

9.2 Setup Entitlements

Enable features for the ESBC using the "*setup entitlements*" command as shown below.

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

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Session Capacity (0-128000)                  : 500

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 3

***************************************************************
CAUTION: Enabling this feature activates enhanced security
functions. Once saved, security cannot be reverted without
resetting the system back to factory default state.
***************************************************************
  Admin Security (enabled/disabled)            :

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 5

  Transcode Codec AMR Capacity (0-102375)      : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2

    Advanced (enabled/disabled)                : enabled

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10

  Transcode Codec OPUS Capacity (0-102375)     : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 11

  Transcode Codec SILK Capacity (0-102375)     : 50
```

Save changes and reboot the SBC.

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

9.3 Enable Management GUI

ALCI Path: config t→system→http-server

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

```
http-server
        name                                    webServerInstance
        state                                   enabled
        realm
        ip-address
        http-state                              enabled
        http-port                               80
        HTTP-strict-transport-security-policy   disabled
        https-state                             disabled
        https-port                              443
        http-interface-list                     GUI
        http-file-upload-size                   0
        tls-profile
        auth-profile
        last-modified-by                        @
        last-modified-date                      2020-10-06 00:28:26
NN4600-139#
```

9.4 Configure SBC using Web GUI

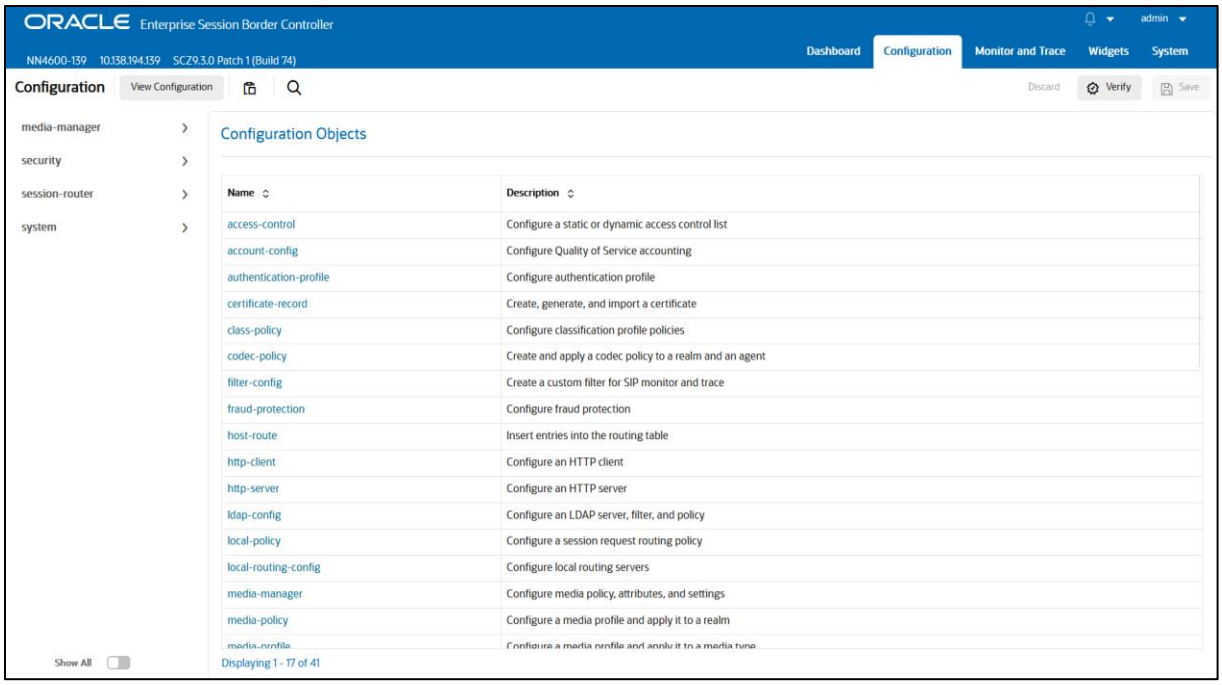
There are two methods for configuring the SBC, ACLI or GUI. For the purposes of this note, we'll be using the SBC GUI for all configuration examples. We will however provide the ACLI path to each element.

To access the SBC GUI, enter the management IP address into a web browser. When the login screen appears, enter the username and password to access the SBC.

Once you have access to the SBC GUI, at the top, click the Configuration Tab. This will bring up the SBC Configuration Objects List on the left-hand side of the screen.

Any configuration parameter not specifically listed below can remain at the SBC default value and does not require a change for the proper functionality.

Note: the configuration examples below were captured from a system running the latest GA software, 9.3.0



Refer to the SBC GUI User Guide for more information:

https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.3.0/webgui/web-gui-guide.pdf

Note: Expert Mode is used when adding or modifying the SBC configuration

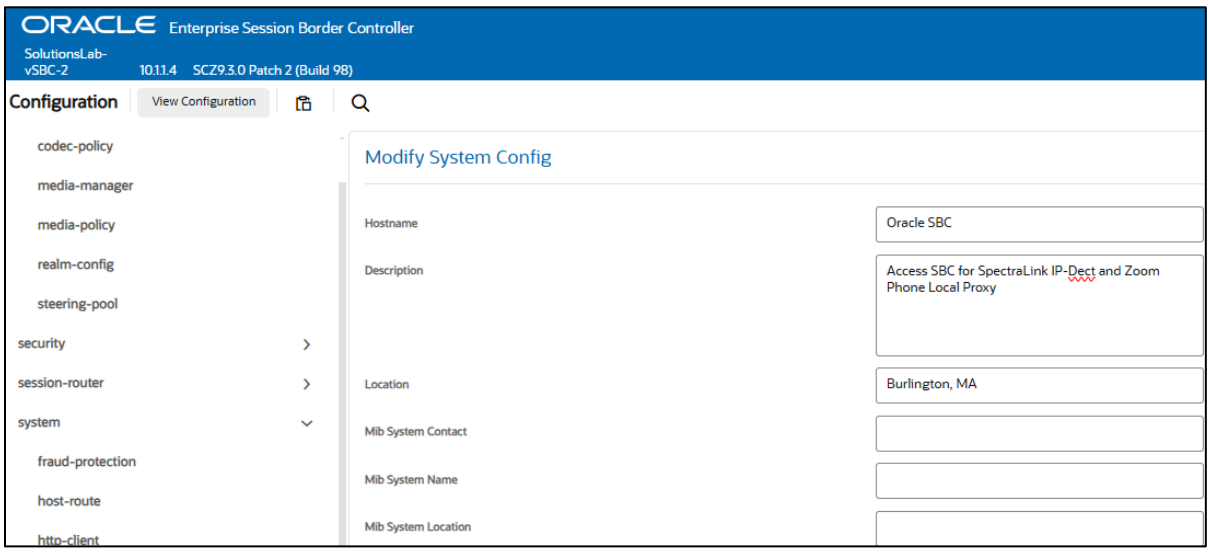
Tip: To make this configuration simpler, directly search the element to be configured from the Objects tab available.

9.5 System-Config

To enable system level functionality for the OCSBC, you must first enable the system-config

GUI Path: system/system-config

ACLI Path: config t→system→system-config



If media transcoding is required in your environment and the SBC is deployed as VME SBC or in a public cloud, you'll need to enable transcoding cores under the system config element. Please see the document below for more information:

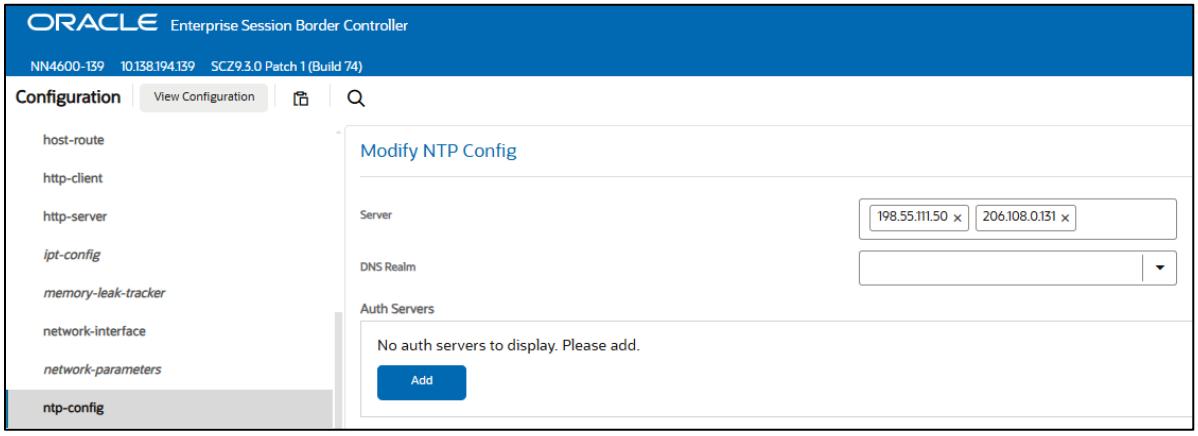
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.3.0/releasenotes/esbc-release-notes.pdf

9.5.1 NTP-Sync

You can use the following example to connect the Oracle SBC to any network time servers you have in your network. This is an optional configuration but recommended.

GUI Path: system/ntp-config

ACLI Path: config t→system→ntp-sync



- Select OK at the bottom

Now we'll move on configuring network connections on the SBC.

9.6 Networking 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 facing SpectraLink IP-Dect Server, the other for Zoom Phone.

9.6.1 Physical Interfaces

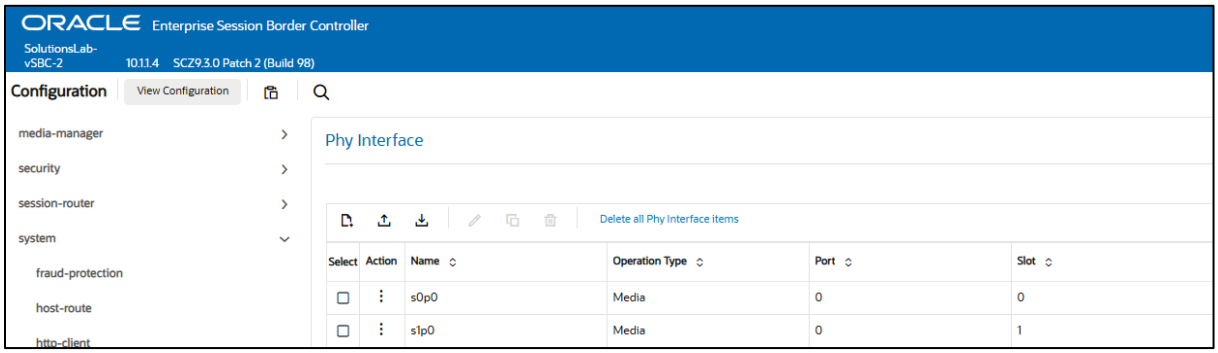
GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

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

Config Parameter	SL Endpoints	Zoom Proxy
Name	s0p0	S1p0
Operation Type	Media	Media
Slot	0	0
Port	0	1

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



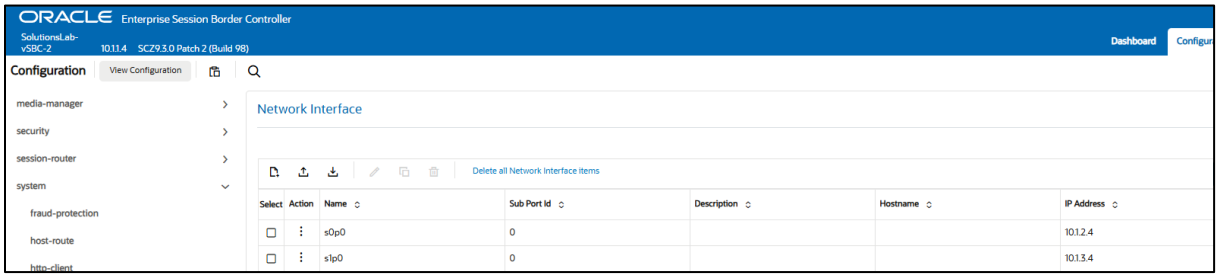
9.6.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

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

Config Parameter	SL Endpoints	Zoom Proxy
Name	s0p0	S1p0
IP Address	10.1.2.4	10.1.3.4
Netmask	255.255.255.0	255.255.255.0
Gateway	10.1.2.1	10.1.3.1
DNS IP Primary		8.8.8.8
DNS IP Backup1		8.8.4.4
DNS Domain		solutionslab.cgbuburlington.com



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

Next, we'll configure the necessary elements to secure the SIP and Media connections on the SBC.

9.7 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with IP-DECT server and Zoom Phone.

9.7.1 Certificate Records

"Certificate-records" are configuration elements on Oracle SBC which capture 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 four certificate records. They are as follows:

- SBC Certificate (end-entity certificate) for IP-DECT Server
- SBC Certificate (end-entity certificate) for Zoom Phone Local Proxy
- Digicert Global Root CA (Root CA used to sign the SBC's end entity certificates)
- DigiCert Global G2 Cert (Zoom Presents the SBC a certificate signed by this authority)

9.7.2 SBC End Entity Configuration

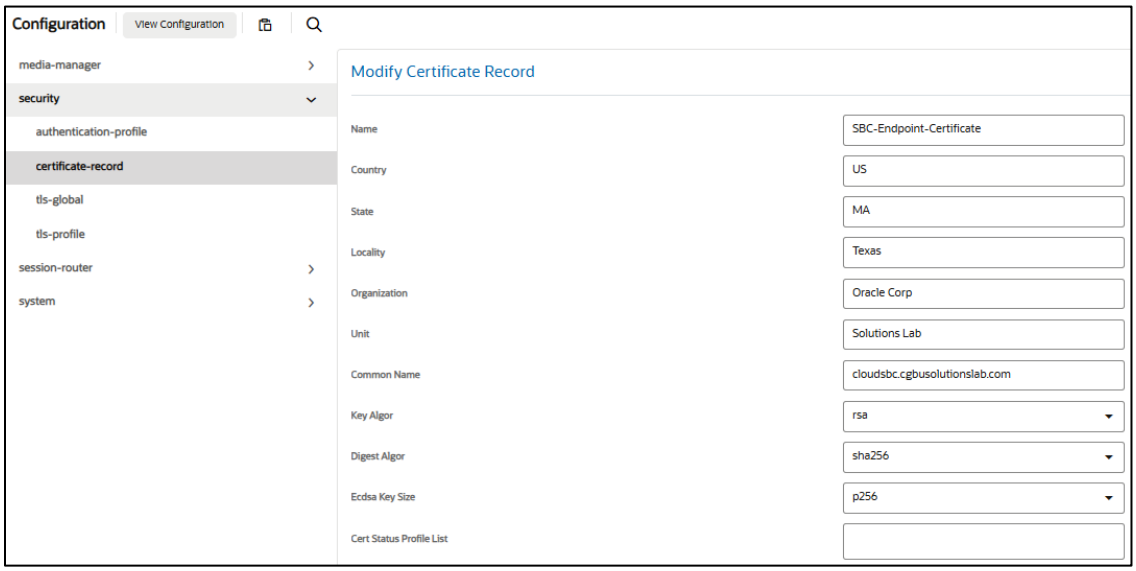
The SBC's end entity certificate is the certificate the SBC presents to Spectralink IP-DECT server and Zoom to secure the connection. The only requirements when configuring this certificate is the common name must contain the SBC's FQDN and the extended key usage list must contain both serverAuth and clientAuth. In this example our common names will be:

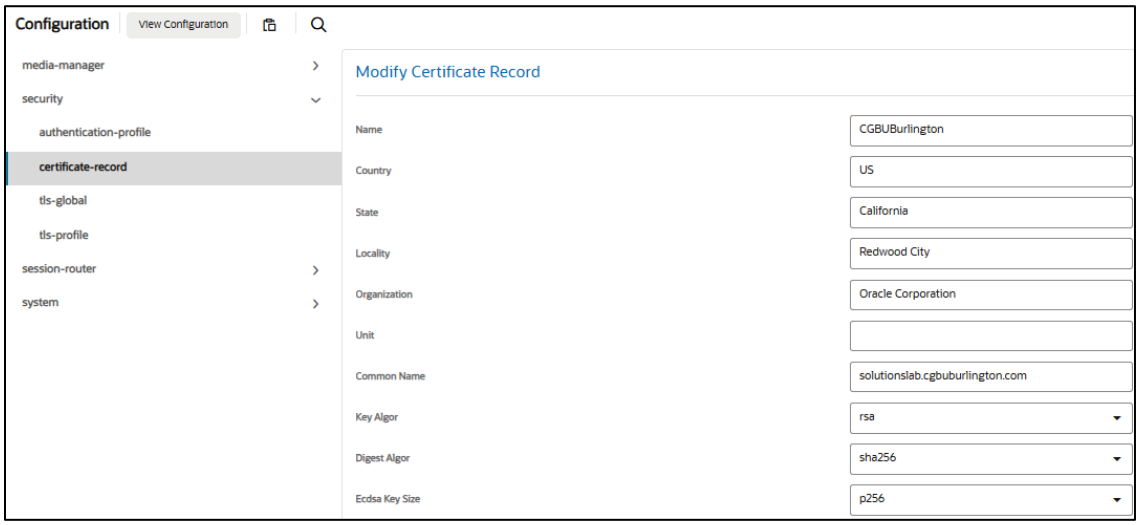
- Cloudsbc.cgbusolutionslab.com (Spectralink IP-DECT server)
- Solutionslab.cgbuburlington.com (Zoom

You must also give it a name. All other fields are optional and can remain at default values.

To Configure the certificate record:

Click Add and use the following example to configure the SBC certificate.





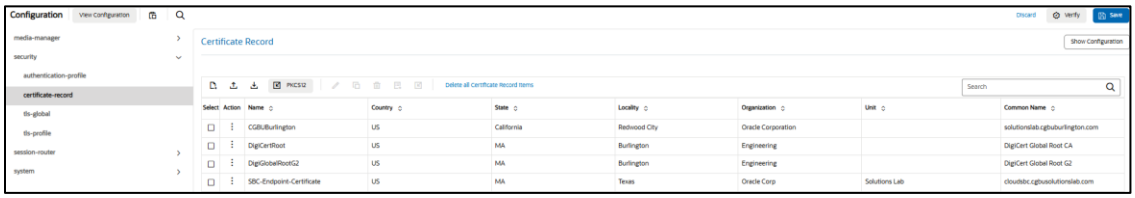
- Click OK at the bottom of each.

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

9.7.3 Root CA and Intermediate Certificates

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

Config Parameter	DigiCert Global Root CA	DigiCert Global Root G2
Common Name	DigiCert Global Root	DigiCert Global Root G2
Key Size	2048	2048
Key-Usage-List	digitalSignature keyEnchpherment	digitalSignature keyEnchpherment
Extended Key Usage List	serverAuth	serverAuth
Key algor	Rsa	Rsa
Digest-algor	Sha256	Sha256

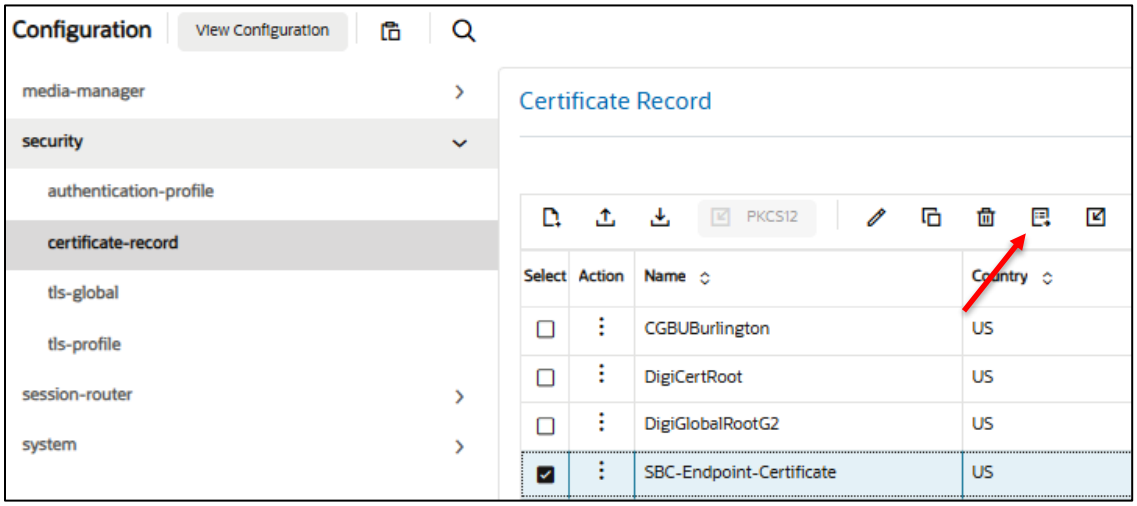


At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must save and activate the configuration of the SBC.

9.7.4 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:



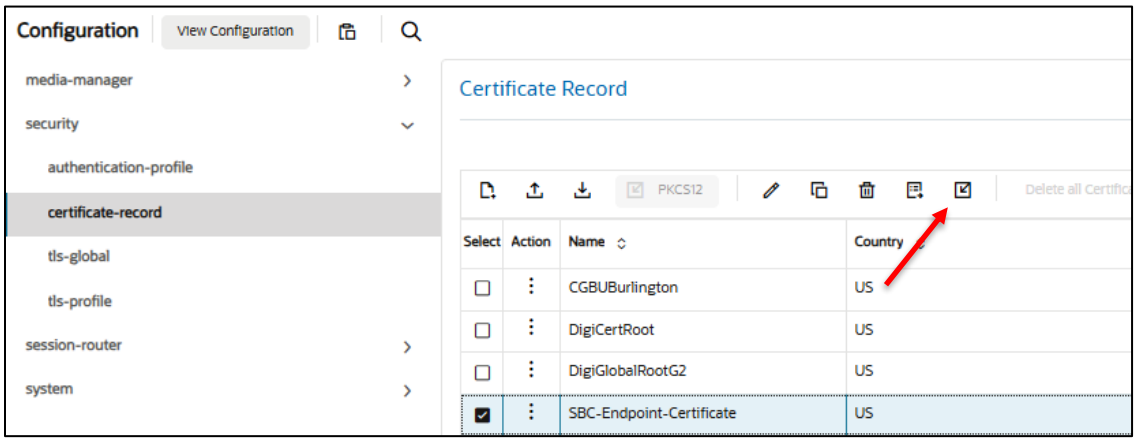
Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, another save and activate is required before you can import the certificates to each certificate record created above.

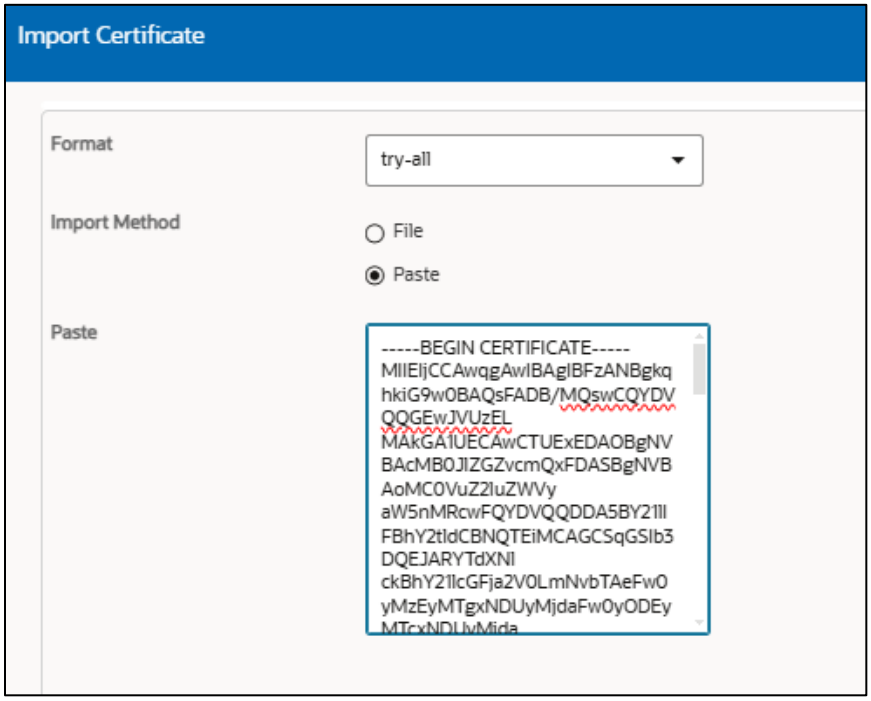
Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

9.7.5 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 a third save/activate from the WebGUI to complete the configuration of certificates on the Oracle SBC.





- Once pasted in the text box, select Import at the bottom, then save and activate your configuration.

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

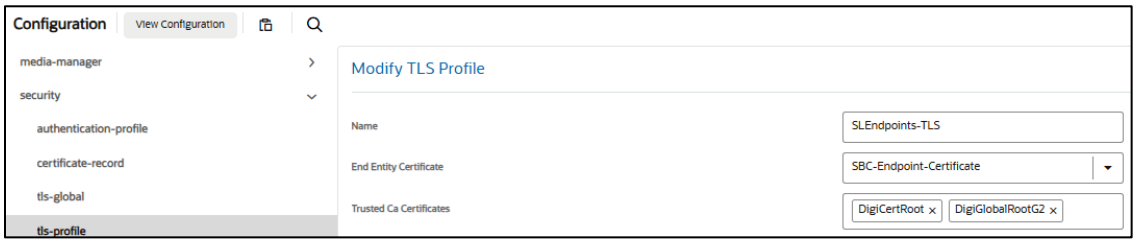
9.7.6 TLS Profile

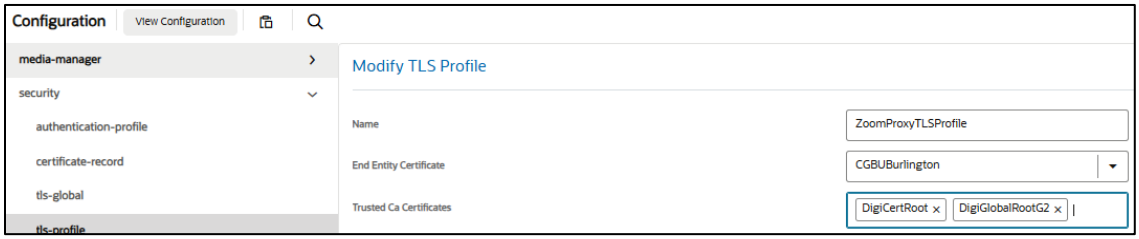
TLS profile configuration on the SBC allows for specific certificates to be assigned.

GUI Path: security/tls-profile

ACLI Path: config t→security→tls-profile

Click Add, use the examples below to configure:





- Select OK at the bottom

Next, we'll move to securing media between the SBC, IP-DECT Server and Zoom.

9.7.7 Media Security

This section outlines how to configure support for media security between the Oracle SBC, IP-DECT Server and Zoom.

9.7.7.1 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. The crypto-suite options supported Spectralink IP-DECT Server are:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

Zoom Supports the following cypto-suite:

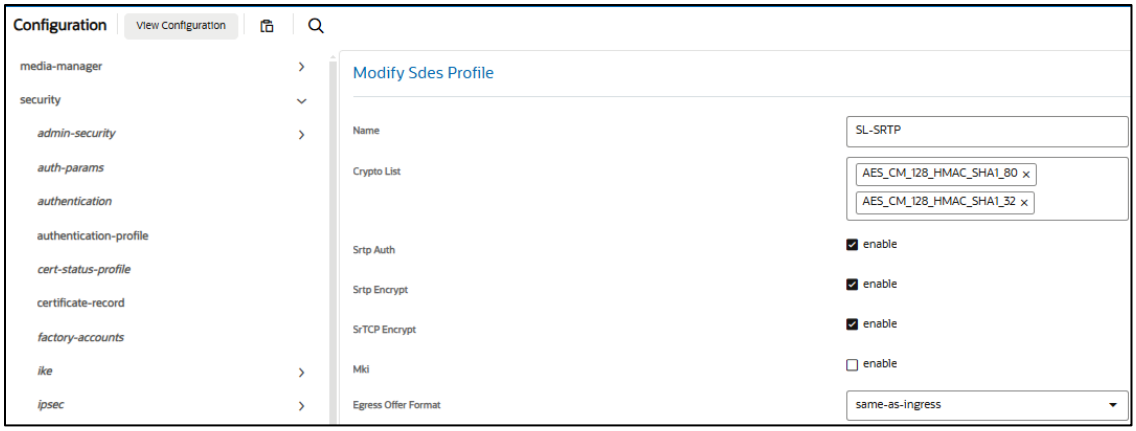
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- AES_256_CM_HMAC_SHA1_80
- AEAD_AES_256_GCM

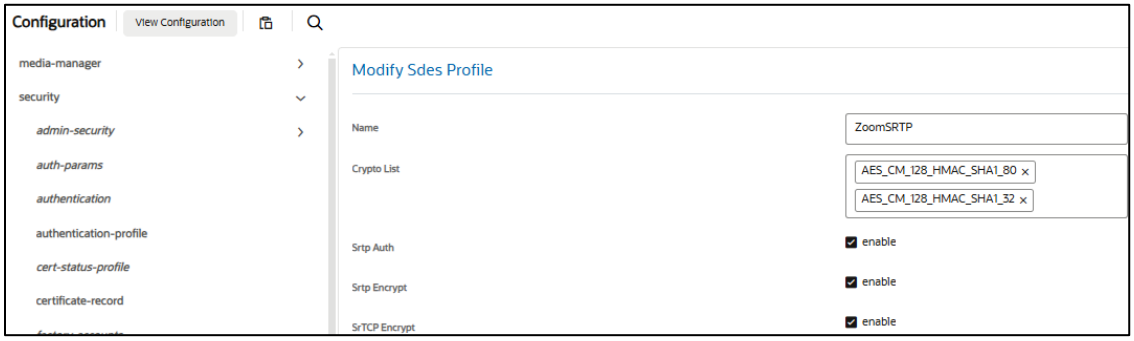
In the SBC's GUI, on the bottom left, you will need to enable the switch "Show All" to access the media security configuration elements.

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

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

- Click Add and use the example below to configure.





- Select OK at the bottom

9.7.7.2 Media Security Policy

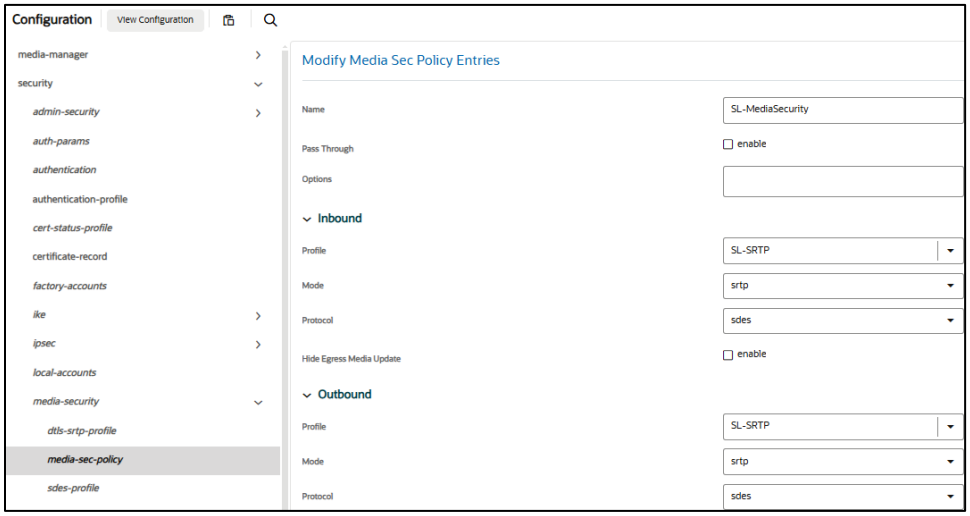
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any) and, if SRTP needs to be used, the sdes-profile that needs to be used.

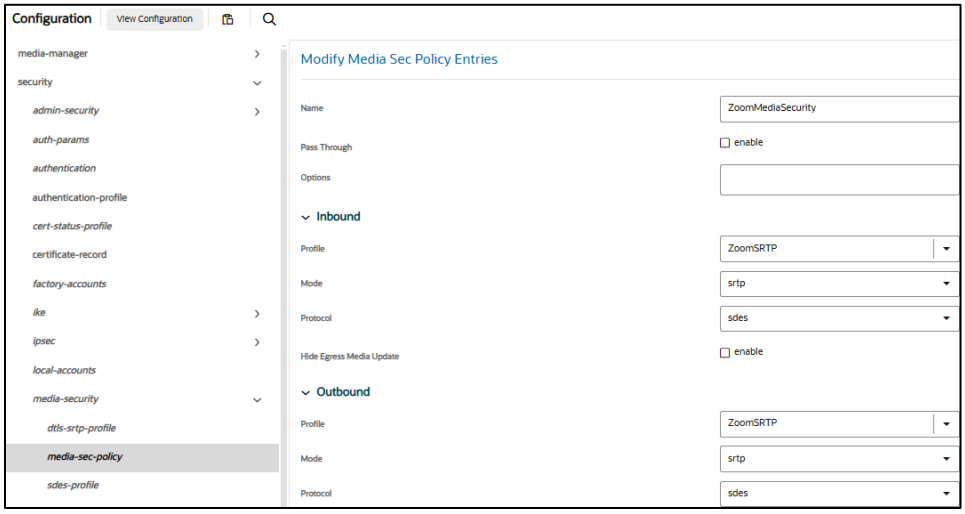
In this example, we are configuring two media security policies. One to secure and decrypt media toward IP-DECT Server, the other facing Zoom.

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.





- Select OK at the bottom of each when finished.

This completes the security configuration portion of the application note. We'll now move on to configuring media.

9.8 Media Configuration

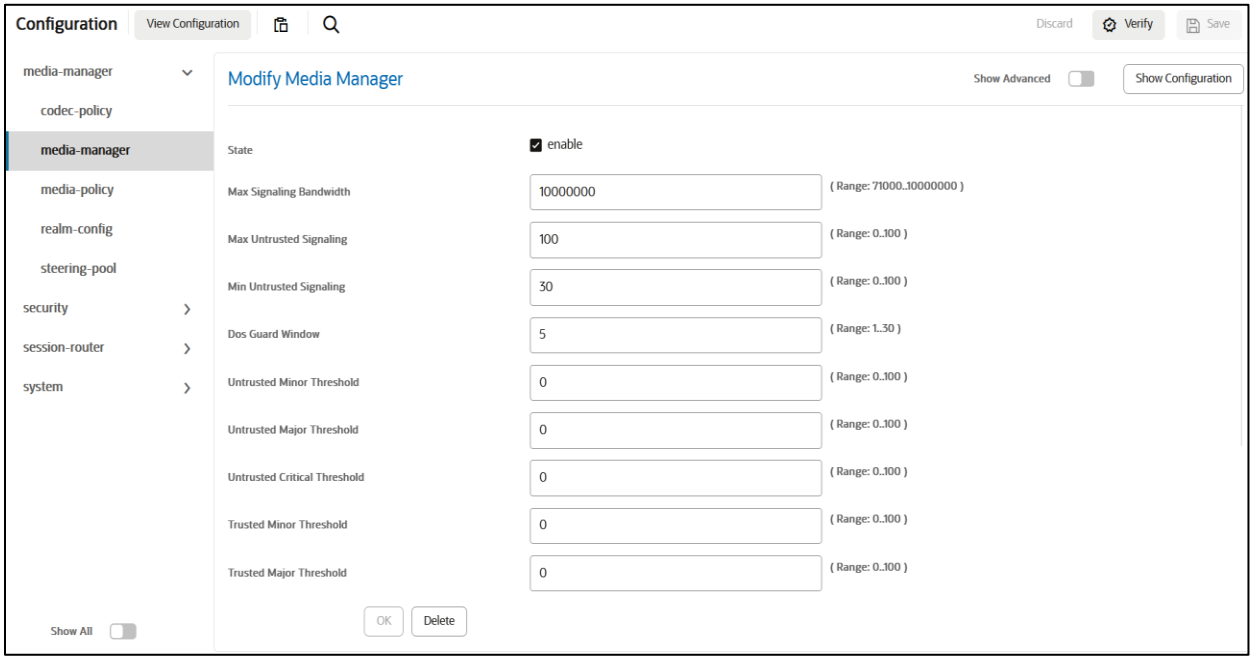
This section will guide you through the configuration of media manager, realms, and steering pools, all of which are required for the SBC to handle signaling and media flows through the SBC.

9.8.1 Media Manager

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

GUI Path: media-manager/media-manager

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



- Click OK at the bottom.

9.8.2 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.

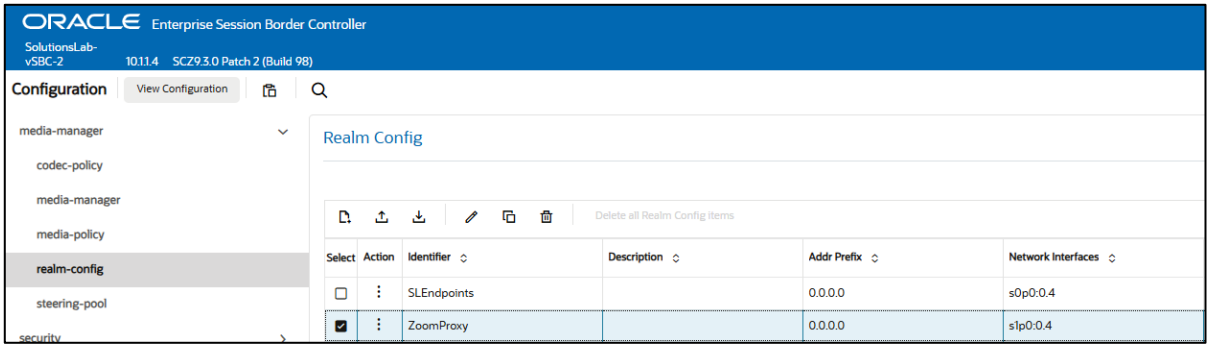
GUI Path; media-manger/realm-config

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

Click Add and use the following table as a configuration example for the realms. The following parameters are all required unless mentioned as optional below.

Config Parameter	SL Endpoints	Zoom Proxy
Identifier	SLEndpoints	ZoomProxy
Network Interface	s0p0	s0p1
MM in Realm	☑	☑
Media Sec Policy	SL-MediaSecurity	ZoomMediaSecurity
Access Control trust level	low	High

Notice, this is where we assign the media security policy configured earlier in the Media Security section of this guide.



- Select OK at the bottom of each.

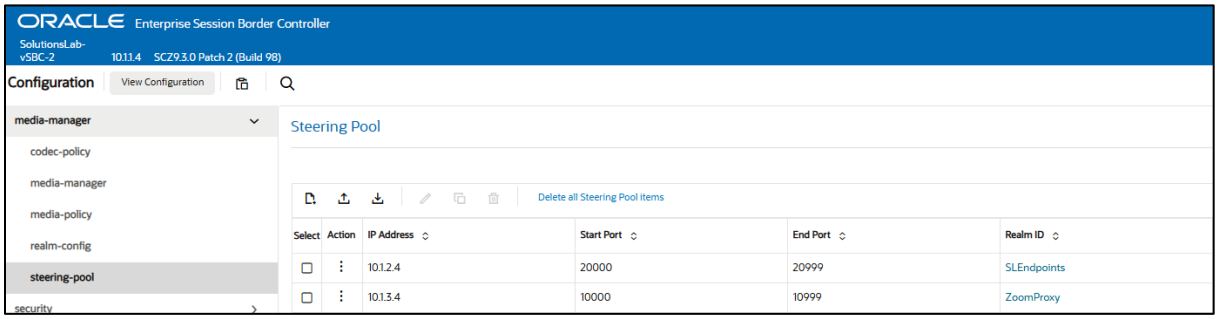
9.8.3 Steering Pools

Steering pools define sets of ports that are used for steering media flows through the OCSBC. 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 each configured realm:

GUI Path: media-manger/steering-pool

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

- Click Add and use the below examples to configure.



- Select OK at the bottom of each.

We'll now work through configuring what is needed for the SBC to handle SIP Signaling.

9.9 Sip Configuration

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

9.9.1 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

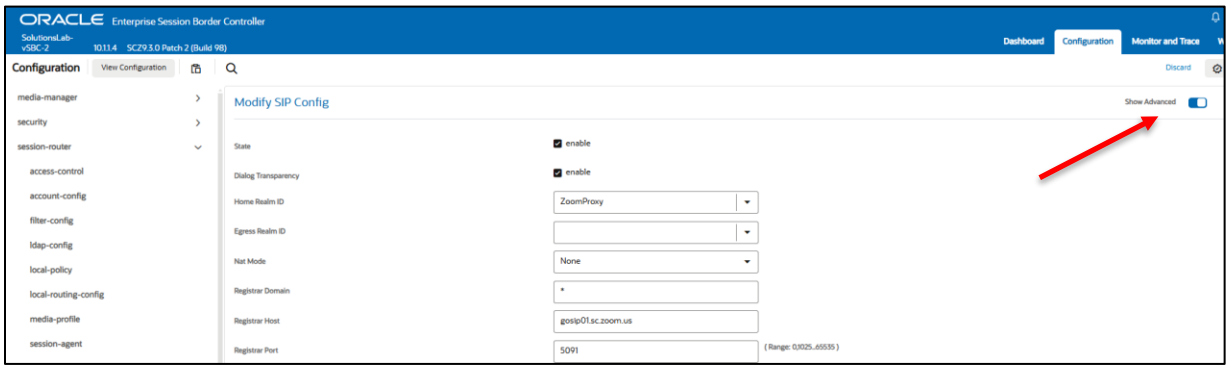
In the Global Sip config, we'll configure the following parameters:

- *Home Realm ID*: represents the internal default realm or network for the Oracle SBC and is where the Oracle SBC's SIP proxy is located.
- *Registrar Domain*: the domain name for identifying which requests for which Hosted NAT Traversal (HNT) or registration caching applies. An asterisk "*" is used to indicate any domain
- *Registrar Host*: the hostname or IP address of the SIP registrar for the HNT and registration caching function.
- *Registrar Port*: the port number of the SIP registrar server
- *Options: reg-cache-mode*: Affects how the userinfo part of Contact address is constructed with registration caching. *From*: userinfo from the From header is copied to the userinfo of the forwarded Contact header

Please use the table as an example to configure the global SIP-Config:

Config Parameter	Value
Home Realm ID	ZoomProxy
Registrar Domain	*
Registrar Host	Gosip01.sc.zoom.us
Registrar Port	5091
Options	Reg-cache-mode=from

Note: toggle show advanced to expose the "Option" parameter



- Select OK at the bottom.

9.9.2 Sip Interface

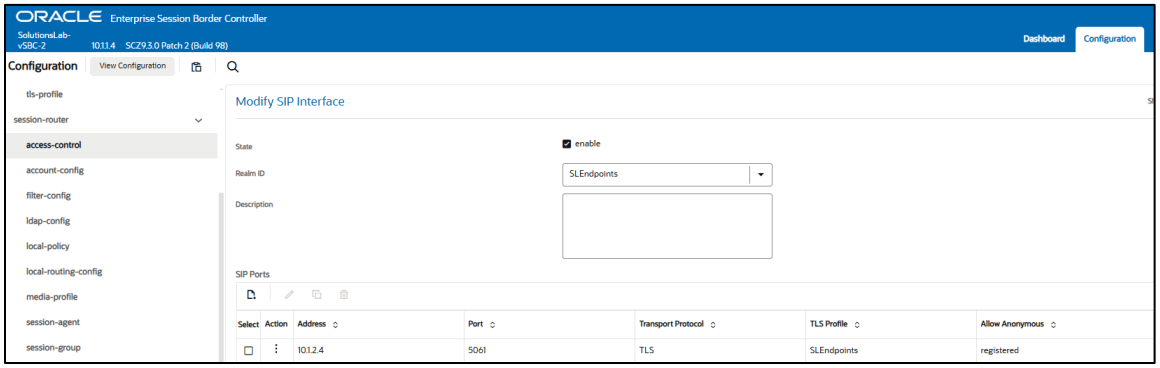
The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages. Configure two sip interfaces, one facing Spectralink IP-DECT server, one associated with Zoom Phone Local Proxy.

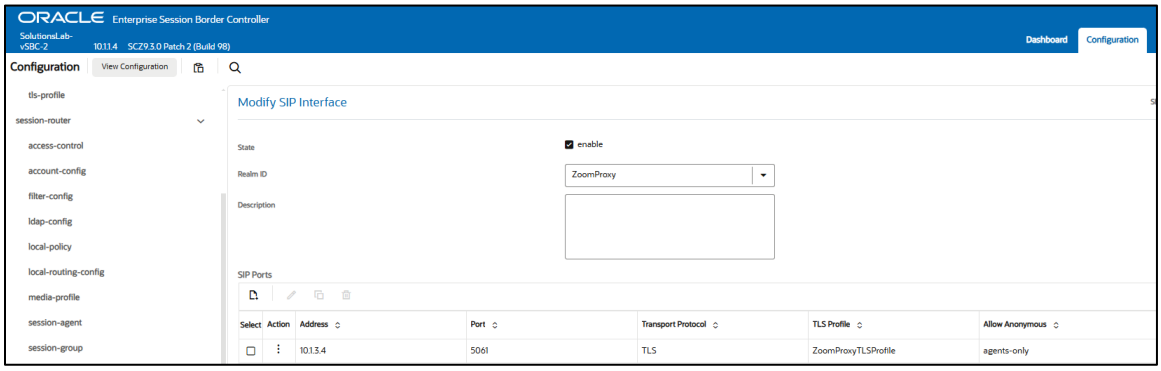
GUI Path: session-router/sip-interface

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

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

Config Parameter	SL Endpoints	Zoom Proxy
Realm ID	SLEndpoints	ZoomProxy
Nat Traversal	always	
Registration Caching	☑	
Route to Registrar	☑	
Sip Port Config Parameter	**SL Endpoints**	**Zoom Proxy**
Address	10.1.2.4	10.1.3.4
Port	5061	5061
Transport	TLS	TLS
TLS Profile	SLEndpoints-TLS	ZoomProxyTLSProfile
Allow Anonymous	registered	agents-only





Notice this is where we assign the TLS profiles configured in the security section of this document.

- Select OK at the bottom of each when applicable.

9.9.3 Session Agents

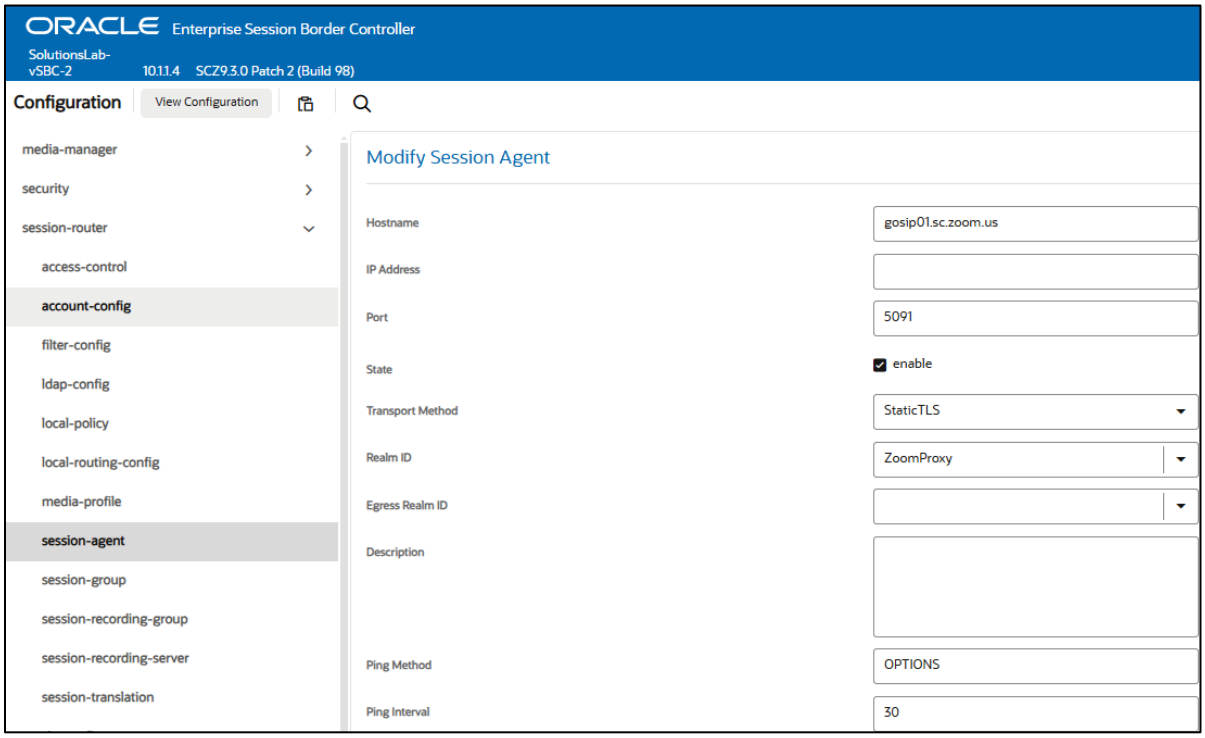
Session Agents are configuration elements which are trusted agents that can both send and receive traffic from the Oracle SBC with direct access to the trusted data path.

GUI Path: session-router/session-agent

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

In this configuration example, we'll configure a single Session Agent for Zoom Phone Local Proxy.

- Click Add, and use the following example to configure the session agent:



- Select OK at the bottom.

9.10 Routing Configuration

Now that we've established the foundational system, signaling, security, and media configurations, let's delve into routing SIP traffic through the SBC. This will enable us to route calls seamlessly across the network.

Leveraging SBC Routing Features

While the SBC offers a variety of routing features, for our current access environment configuration, we'll primarily rely on the Global SIP config and SIP interface parameters. These parameters, as detailed earlier, are already in place.

Global SIP Configuration

In the Global SIP config, we've ensured that the registrar host, port, and home realm ID align with the Zoom Proxy Session Agent, our designated registrar. This alignment is crucial for efficient routing.

SIP Interface Configuration

For SL Endpoints, we've enabled the "route to registrar" parameter on the SIP interface. This directive instructs the interface to forward Register Requests from endpoints to the host and port specified in the Global SIP config. By simplifying routing in this manner, we streamline the SBC's configuration process.

Routing Traffic from Registrar to Endpoints

The SBC leverages its registration cache to facilitate this routing. Once an endpoint receives a 200 OK response from the registrar, the SBC caches the endpoint's information locally. Subsequently, when the SBC

receives a packet from the registrar, it performs a cache lookup to identify the target endpoint. Upon matching the endpoint, the SBC forwards the packet to the appropriate destination based on the cached information.

9.11 Access Controls

The Oracle Session Border Controller (SBC) family of products are designed to increase security when deploying Voice over IP (VoIP) or Unified Communications (UC) solutions. Properly configured, Oracle's SBC family helps protect IT assets, safeguard confidential information, and mitigate risks—all while ensuring the high service levels which users expect from the corporate phone system and the public telephone network.

Please note, DDOS values are specific to platform and environment. For more detailed information please refer to the Oracle Communications SBC Security Guide.

https://docs.oracle.com/en/industries/communications/session-border-controller/9.3.0/security/index.html

However. While some values are environment specific, there are some basic security parameters that can be implemented on the SBC that will help secure your setup.

1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high

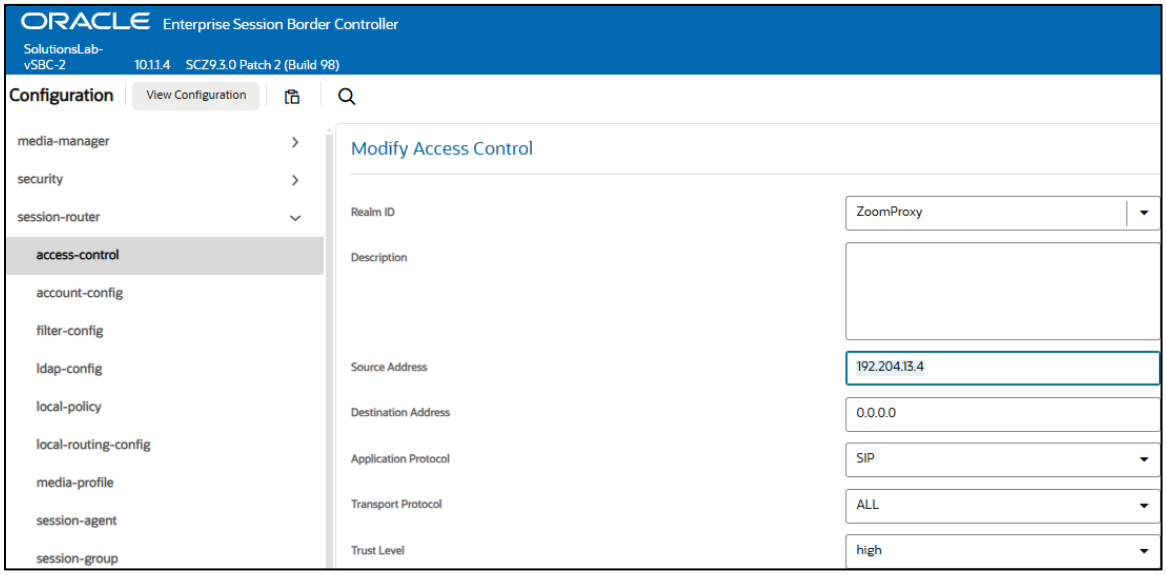
2. Set the access control trust level on public facing realms to HIGH

In this configuration example, Zoom Phone Local Proxy FQDN resolves to one IP address that must be allowed to send traffic to the SBC, 192.204.13.4. This must be configured as an access control on the Oracle SBC and associated with the realm facing Zoom

GUI Path: session-router/access-control

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

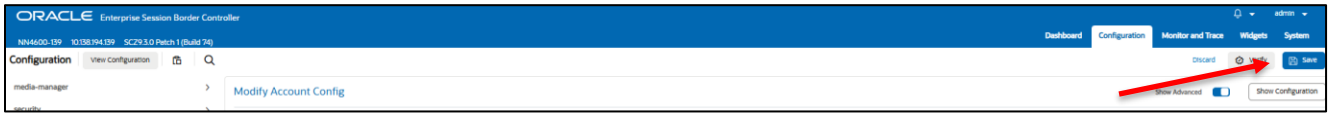
Click Add and use this example to create ACL for Zoom:



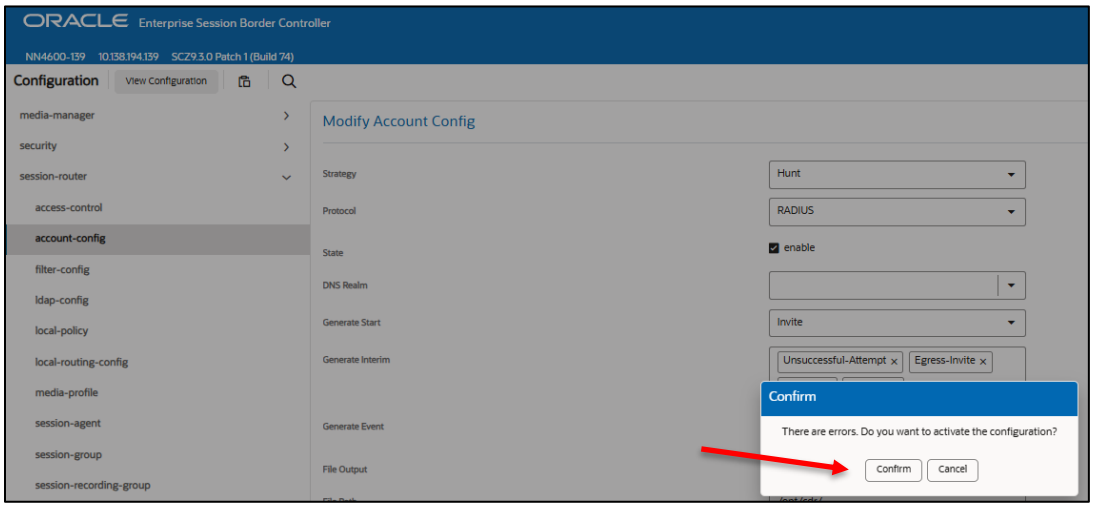
- Click OK at the bottom.

9.12 Save and Activate

9.12.1 Save Config



9.12.2 Activate Config



This concludes the minimum required configuration of the Oracle Session Border controller when deployed in an access environment to support Spectralink IP-DECT server with DECT Wireless endpoints, using Zoom Phone Local Proxy as a registrar.

10 Appendix A

10.1 Oracle SBC deployed behind NAT

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 IP as configured on both the SIP Interface and Steering Pool
- 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 SIP interface.

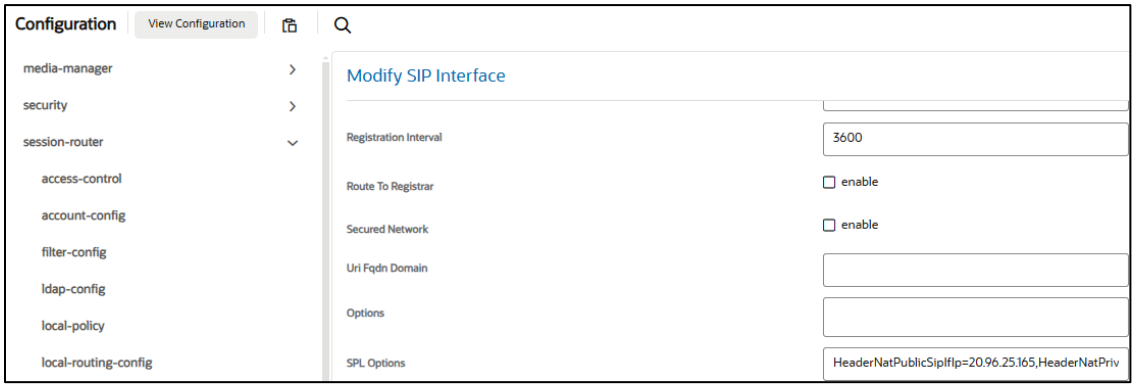
GUI Path: session-router/sip-interface

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

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.1.3.4

HeaderNatPublicSipIfIp is the public interface ip

HeaderNatPrivateSipIfIp is the private ip.



11 Appendix B

11.1 ACLI Running Configuration

Below is a complete output of the running configuration used to create this application note. This output includes all of the configuration elements used in our examples, including some of the optional configuration features outlined throughout this document. Be aware that not all parameters may be applicable to every Oracle SBC setup, so please take this into consideration if planning to copy and paste this output into your SBC.

```
Oracle-SBC# show running-config short
access-control
        realm-id                        ZoomProxy
        source-address                  192.204.13.4
        application-protocol            SIP
        trust-level                     high
certificate-record
        name                            CGBUBurlington
        state                           California
        locality                        Redwood City
        organization                    Oracle Corporation
        common-name                     solutionslab.cgbuburlington.com
certificate-record
        name                            DigiCertRoot
        common-name                     DigiCert Global Root CA
certificate-record
        name                            DigiGlobalRootG2
        common-name                     DigiCert Global Root G2
```

```
certificate-record
        name                            SBC-Endpoint-Certificate
        locality                        Texas
        organization                    Oracle Corp
        unit                            Solutions Lab
        common-name                     cloudsbc.cgbusolutionslab.com
        extended-key-usage-list         serverAuth
                                        clientAuth
http-server
        name                            webServerInstance
        tls-profile                     WebServerInstance
media-manager
        max-signaling-bandwidth         40000000
        max-untrusted-signaling         9
        min-untrusted-signaling         8
media-sec-policy
        name                            TeamsMediaSecurity
        inbound
                profile                 SL-SRTP
                mode                    srtp
                protocol                sdes
        outbound
                profile                 SL-SRTP
                mode                    srtp
                protocol                sdes
media-sec-policy
        name                            ZoomMediaSecurity
        inbound
                profile                 ZoomSRTP
                mode                    srtp
                protocol                sdes
        outbound
                profile                 ZoomSRTP
                mode                    srtp
                protocol                sdes
network-interface
        name                            s0p0
        ip-address                      10.1.2.4
        netmask                         255.255.255.0
        gateway                         10.1.2.1

network-interface
        name                            s1p0
        ip-address                      10.1.3.4
        netmask                         255.255.255.0
        gateway                         10.1.3.1
        dns-ip-primary                  8.8.8.8
        dns-ip-backup1                  8.8.4.4
        dns-ip-backup2                  9.9.9.9
        dns-domain                      solutionslab.cgbuburlington.com
ntp-config
        server                          time.google.com
        DNS-Realm                       ZoomProxy
phy-interface
        name                            s0p0
        operation-type                  Media
phy-interface
        name                            s1p0
        operation-type                  Media
        slot                            1
realm-config
        identifier                      SL-Endpoints
        network-interfaces              s0p0:0.4
```

```
        mm-in-realm                     enabled
        media-sec-policy                SL-MediaSecurity
        access-control-trust-level      low
        invalid-signal-threshold        5
        maximum-signal-threshold        4000
        untrusted-signal-threshold      25
realm-config
        identifier                      ZoomProxy
        network-interfaces              s1p0:0.4
        mm-in-realm                     enabled
        media-sec-policy                ZoomMediaSecurity
        access-control-trust-level      high
sdes-profile
        name                            SL-SRTP
        crypto-list                     AES_CM_128_HMAC_SHA1_80
                                        AES_CM_128_HMAC_SHA1_32
 sdes-profile
        name                            ZoomSRTP
                crypto-list             AES_CM_128_HMAC_SHA1_80
                                        AES_CM_128_HMAC_SHA1_32
session-agent
        hostname                        gosip01.sc.zoom.us
        port                            5091
        transport-method                StaticTLS
        realm-id                        ZoomProxy
        ping-method                     OPTIONS
        ping-interval                   30
        ping-response                   enabled
sip-config
        home-realm-id                   ZoomProxy
        registrar-domain                *
        registrar-host                  gosip01.sc.zoom.us
        registrar-port                  5091
        options                         max-udp-length=0
                                        reg-cache-mode=from
sip-interface
        realm-id                        SL-Endpoints
        sip-port
                address                 10.1.2.4
                port                    5061
                transport-protocol      TLS
                allow-anonymous         registered
        nat-traversal                   always
        registration-caching            enabled
        route-to-registrar              enabled
        secured-network                 enabled
        spl-options                     HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4
sip-interface
        realm-id                        ZoomProxy
        sip-port
                address                 10.1.3.4
                port                    5061
                transport-protocol      TLS
                tls-profile             ZoomProxyTLSProfile
                allow-anonymous         agents-only
        spl-options                     HeaderNatPublicSipIfIp=20.96.25.165,HeaderNatPrivateSipIfIp=10.1.3.4
sip-monitoring
        monitoring-filters              *
steering-pool
        ip-address                      10.1.2.4
        start-port                      20000
        end-port                        20999
        realm-id                        SL-Endpoints
```

```
steering-pool
        ip-address                    10.1.3.4
        start-port                    10000
        end-port                      10999
        realm-id                      ZoomProxy
system-config
        hostname                      Oracle SBC
        description
        location                      Burlington, MA
tls-profile
        name                          SLEndpoints-TLS
        end-entity-certificate        SBC-Endpoint-Certificate
        trusted-ca-certificates       DigiCertRoot
                                      DigiGlobalRootG2
        tls-version                   tlsv12
tls-profile
        name                          ZoomProxyTLSProfile
        end-entity-certificate        CGBUBurlington
        trusted-ca-certificates       DigiCertRoot
                                      DigiGlobalRootG2
        mutual-authenticate           enabled
        tls-version                   tlsv12
```

12 Appendix C

12.1 Features Tested and Supported

The following feature set was tested and is supported in this environment:

The following features are based on interoperability testing supported:

- Make and receive basic calls, local and PSTN
- Long duration calls (greater than 30 minutes)
- Handset-to-handset calling
- Check Voicemail
- Speed Dial
- Caller ID
- Call Hold and Retrieve
- Call Transfer (warm, blind)
- Three Party Conference (attend only)
- Call Forwarding
- Call Waiting
- Call Park/Retrieve
- Call Log
- Do Not Disturb (DND)
- Music on Hold (MOH)
- Long Duration Hold (greater than 30 minutes)
- DTMF
- Secure Voice - TLS 1.3 (Minimum 1.2 required)
- Call Queue (DECT endpoints assigned to queue)

Oracle Corporation, World Headquarters
2300 Oracle Way
Austin, TX 78741, USA

Worldwide Inquiries
Phone: +1.650.506.7000 or
Phone: +1.800.392.2999

ORACLE

CONNECT WITH US

blogs.oracle.com
facebook.com/oracle
twitter.com/oracle
oracle.com/

Integrated Cloud Applications & Platform Services