

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

Technical Application Note



Disclaimer

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

Revision History

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

1 Table of Contents

2	INT	ENDED AUDIENCE	5
3	DOC	CUMENT OVERVIEW	5
4	ABC	DUT SPECTRALINK	5
	4.1	DECT Servers	5
	4.2	S SERIES HANDSETS	5
5	INT	RODUCTION	6
	5.1	AUDIENCE	6
	5.2	REQUIREMENTS	6
	5.3	ARCHITECTURE	6
6	ZOO	DM CONFIGURATION	7
	6.1	ADD DEVICE	7
	6.2	SIP ACCOUNT DETAILS	9
7	SPE	CTRALINK 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	CON	FIGURING THE SBC	17
9	NEV	V 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	- 77
	9.6.1	Divisional Interfaces	
	067	Physical Interfaces	22
	9.6.2 9.7	Physical Interfaces	22 23
	9.6.2 9.7 9.7 1	Physical Interfaces	22 23 23 23
	9.6.2 9.7 9.7.1 9.7.2	Physical Interfaces	22 23 23 23 23 23 24
	9.6.2 9.7 9.7.1 9.7.2 9.7.2	Physical Interfaces	22 23 23 23 23 24 25
	9.6.2 9.7 9.7.1 9.7.2 9.7.3 9.7.4	Physical Interfaces	22 23 23 23 23 24 25 25
	9.6.2 9.7 9.7.1 9.7.2 9.7.3 9.7.4 9.7.5	Physical Interfaces	22 23 23 23 23 24 25 25 26
	9.6.2 9.7 9.7.1 9.7.2 9.7.3 9.7.4 9.7.5 9.7.6	Physical Interfaces	22 23 23 24 25 25 26 27
	9.6.2 9.7 9.7.1 9.7.2 9.7.3 9.7.4 9.7.5 9.7.6 9.7.7	Physical Interfaces	22 23 23 24 25 25 26 27 28
	9.6.2 9.7 9.7.1 9.7.2 9.7.3 9.7.4 9.7.5 9.7.6 9.7.7 9.8	Physical Interfaces Network Interfaces SECURITY CONFIGURATION Certificate Records SBC End Entity Configuration Root CA and Intermediate Certificates Generate Certificate Signing Request Import Certificates to SBC. TLS Profile Media Security MEDIA CONFIGURATION	22 23 23 24 25 25 26 27 28 30
	9.6.2 9.7 9.7.1 9.7.2 9.7.3 9.7.4 9.7.5 9.7.6 9.7.7 9.8 9.8.1	Physical Interfaces Network Interfaces SECURITY CONFIGURATION Certificate Records SBC End Entity Configuration Root CA and Intermediate Certificates Generate Certificate Signing Request Import Certificates to SBC TLS Profile Media Security MEDIA CONFIGURATION Media Manager	22 23 23 23 24 25 25 26 27 28 30 30
	9.6.2 9.7 9.7.1 9.7.2 9.7.3 9.7.4 9.7.5 9.7.6 9.7.7 9.8 9.8.1 9.8.2	Physical Interfaces	22 23 23 24 25 25 26 27 28 30 30 31
	9.6.2 9.7 9.7.1 9.7.2 9.7.3 9.7.4 9.7.5 9.7.6 9.7.7 9.8 9.8.1 9.8.2 9.8.3	Physical Interfaces	22 23 23 23 24 25 25 26 27 28 30 30 31 32
	9.6.2 9.7 9.7.1 9.7.2 9.7.3 9.7.4 9.7.5 9.7.6 9.7.7 9.8 9.8.1 9.8.2 9.8.3 9.9	Physical Interfaces Network Interfaces SECURITY CONFIGURATION Certificate Records SBC End Entity Configuration Root CA and Intermediate Certificates Generate Certificate Signing Request Import Certificates to SBC TLS Profile Media Security MEDIA CONFIGURATION Media Manager Realm Config Steering Pools SIP CONFIGURATION	22 23 23 24 25 25 26 27 28 30 30 31 32 32

992 Sin Interface	33
9.9.3 Session Agents	
9.10 ROUTING CONFIGURATION	
9.11 Access Controls	
9.12 SAVE AND ACTIVATE	
9.12.1 Save Config	
9.12.2 Activate Config	
10 APPENDIX A	
10 APPENDIX A 10.1 ORACLE SBC DEPLOYED BEHIND NAT	37
 10 APPENDIX A	
 10 APPENDIX A	
 10 APPENDIX A 10.1 ORACLE SBC DEPLOYED BEHIND NAT 11 APPENDIX B 11.1 ACLI RUNNING CONFIGURATION 12 APPENDIX C 	

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 Spectralink 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

ZOOM Products S	olutions Resources Plans & Pricing
> Workspaces Management	
 Phone System Management 	Starting July 10th, 2024, customers who intend to send SMS/MMS to US numbers must ensure that their US and Canada Toll/Virte Canada SMS/MMS will not require 10DLC Registration. More Details
Users & Rooms	
Auto Receptionists	Phones & Devices
Call Queues	Assigned Unassigned
Shared Lines	
Group Call Pickup	Note: Zoom Phone Appliance devices can be assigned to Common Area. To manage Zoom Phone Appliance, please go to Device
Phone Numbers	
Provider Exchange	Add Export to CSV (2)
Provider Portal	Q Search by User, Ext., MAC Address, or IP Address
Phones & Devices	

Select Add

ZOOM Products Solu	utions Resources Plans & Pricing	
> Workspaces Management		
 Phone System Management 	Starting July 10th, 2024, customers who in Canada SMS/MMS will not require 10DLC	Add Device
Users & Rooms		
Auto Receptionists	Phones & Devices	Display Name This field is required
Call Queues	Assigned Unassigned	Description (Optional)
Shared Lines		(aprova)
Group Call Pickup	Note: Zoom Phone Appliance devices can	MAC Address
Phone Numbers	Add Export to CSV @	
Provider Exchange		Device Type Select Brand ~
Provider Portal	Q Search by User, Ext., MAC Address, or I	Select Model 🗸 🗸
Phones & Devices		Assigned to Assign
Monitoring	Display	
Assets Library	Name Clovice Type	Save Cancel
Loge		

- 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

ZOOM Products So	olutions Resources Plans & Pricing		
Workspaces Management Phone System Management Users & Rooms	Starting July 10th, 2024, customers who in Canada SMS/MMS will not require 10DLC	Add Device	
Auto Receptionists	Phones & Devices	Display Name	Ext 1604
Call Queues	Assigned Unassigned	Description (Optional)	Spectralink Wireless Endpoint 1
Shared Lines	Note: Zoom Phone Appliance devices can		
Phone Numbers		MAC Address	150930011653
Provider Exchange	Add Export to CSV ()	Device Type	Other v
Provider Portal Phones & Devices			This device type supports up to 1 assignee.
Monitoring	Distan	Assigned to	User v solzoomg1@outlook.com 1 - Ext. 1005
Assets Library	Name Device Type I		Add Cancel
Logs Company Info			
Overview	Glen Size 2700		Save Cancel

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

ZOOM Products Solution	ns Resources Plans	s & Pricing		
Users & Rooms	EXT IOU4 Rename	EXT IOU4 Rename		
Auto Receptionists	Spectralink Wireless Endpoi	int 1		
Call Queues	Profile Policy			
Shared Lines				
Group Call Pickup	Site	Main Site (Main Site, Site Code: 1)		
Phone Numbers	Assigned to	solzoomg1@outlook.com1 Ext. 1005		
Provider Exchange				
Provider Portal	IP Address			
Phones & Devices				
Monitoring	Device Type	Other		
Assets Library	Firmware Version			
Logs	MAC Address	15-09-30-01-16-43		
Company Info	Provision Template	Unsupported ?		
Overview				
> Account Management	Status	Offline		
> Advanced	Actions ~ Remove	e		
	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 0139
- 4. Authorization ID: 14
- 5. Password: N1x 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 <u>section 6</u> 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
 - o 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.

S	spectralink🕏			IP-DEC	TS	erver 400)		~~~~~
Conoral	Status Wireless Server	Media Resource	Configuration	Cortificator	ein	Users	Drovinio	Administration	Firmware
General	Wireless Server	Media Resource	Security	Certificates	JIP	Stausuus	FIUVISIO		
								General Configuration	
						IPv4			
						Method * **		Use static IP address V	
						IP addr **		192.168.0.150	
						Netmask **		255.255.255.0	
						Gateway **		192.168.0.1	
						MTU **			
						IPv6			
						Method **		Disabled	~
						Address/prefix **			
						Default gateway *	**		
						NAT traversal			
						IP addr			
						Ethernet			
						VLAN **			
						DNS			
						Hostname (FQDN	N) **		
						Search domain			
						Primary Server			
						Secondary Serve	r		
						NTP			
						Server		time.google.com]
						Time zone		Eastern Time	~

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)

2///0

111110

SIP Configuration					
General					
Local port *	5061				
Transport *	TLS V				
DNS method *	A records 🖌				
Default domain *	10001201.zoom.us				
Allow wildcard certificate					
Register each endpoint on separate port					
Send all messages to current registrar					
Allow internal routing fallback					
Registration expire(sec) *	3600				
Max pending registrations *	1				
Handset power off action	Ignore 🗸				
Max forwards *	70				
Client transaction timeout(msec) *	16000				
Blacklist timeout(sec) *	30				
SIP type of service (TOS/Diffserv) *	96				
SIP 802.1p Class-of-Service *	3				
GRUU					
Use SIPS URI					
TLS allow insecure					
TCP ephemeral port in contact address					
NAT keepalive	SIP OPTIONS (rfc3261) V				
NAT keepalive interval(sec)	30 🗸				
Send Hold before REFER					
Send BYE with REFER					
Convert SIP URI to phone number					
Alert-Info header					
Internal ringtones incoming calls					
Auto answer incoming calls					
Proxies					
Deves 1	Priority Weight URI				
Proxy 1	Image: sign sign sign sign sign sign sign sign				
Proxy 2	2 100 sip:gosip01.sc.zoom.us:5091				

[•] 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 V				
Early encryption and re-keying **	Disabled V				
DECT Standard Authentication Algorithm #2 (DSAA2)	Disabled V				
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

spectralink💈	IP-DE	CT Server 400		
Status General Wireless Server Media Resource	Configuration Security Certificates SIP	Users Statistics Provisioning Import/Export	Administration Factory Reset	Firmware
			Device certificate	chain
Show All 🗸 entries				
Subject	Validity	SHA1 fingerprint		Key ID
0013D191EEA9 / Spectralink Inc.	2023-02-16 - 2038-02-16	7f:00:00:0f:be:03:9c:58:cb:e4:54:90:e6:	b4:c5:d2:df:3b:2a:c1	2f:01:38:45:ac:a4:1a
SpectraLink Issuing CA	2017-06-12 - 2042-06-12	6a:e3:a4:ee:a3:eb:fb:64:a6:f5:25:cc:ab:	04:1e:1b:6c:85:f8:e8	b1:73:c6:a3:ef:c3:bb
SpectraLink Root CA	2012-07-09 - 2044-07-09	f3:92:b9:87:e9:d6:4c:a6:53:ee:8c:ef:bb:	3c:a1:7f:e9:e6:83:a2	43:c4:58:6f:a1:02:39
Showing 1 to 3 of 3 entries				
			Host key	
Show All v entries		Remove Generate Key file: Choose File	No file chosen	Password:
Algorithm			Bits	
			No data available in	1 table
Chowing 0 to 0 of 0 optrion				
showing 0 to 0 of 0 entries				
			Host certificate	chain
	Remove Generate Self-Signed G	enerate Request Certificate file: Choose File	No file chosen	Password:
			CA Certificate	es
		Clear List Restore Default Lis	t Choose File DigiCertG	Inport List Export List

IF	P-DE(CT Serv	ver 400			
			Users		Administration	Firmware
tes	SIP	Statistics	Provisioning	Import/Export	Factory Reset	
					Imported CA Certificate list	

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

	emove Generate Self-Signed Generate Request	Host certificate chain Certificate file: Choose File No file chosen Password	I: Type:
Show All v entries	C	CA Certificates	Import List Export List
Common Name	Organization	SHA1 fingerprint	
DigiCert Global Root CA	DigiCert Inc	a8:98:5d:3a:65:e5:e5:c4:b2:d7:d6:6d:40:c6:	dd:2f:b1:9c:54:36

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

Configuration→Security

P-DECT Serv	ver 400		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
SIP Statistics	Users Admini Provisioning Import/Export Factory Reset	istration	Firmware
	Security Co	onfiguration	
	Administrator Authentication	Jinguration	
	Current password *		
	New username *	admin	
	New password		
	New password again		
	Strict password requirements		
	Password expiration	Never 🗸	
	Data protection		
	Allow unencrypted HTTP		
	Enable legacy TLS		
	Allow remote logging		
	Remove user passwords from exported data		
	Remove system passwords from exported da	ta 🗆	

- 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:

IP-DECT Ser	ver 400			m
	Users	Administration		Firmware
	Overview	User List		
	System ARI			10070530644
		SIP us	ers Subscrib	ed Registered
	Total New Enable	Disable Delete Re-register	2 Un-subscribe Firm	2 0 ware update

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 66
Display Name	1806
Authentication User	47 66
Authentication Password	N1xl kqfE

Admi	nistration
Lloor 2492706	2416010312666
	2410919312000
Product name	Spectralink S 33
Model number	S 33
Software part number	14234000
Item number	72682000
Firmware	24G
HW version	8A
Software version	1423 4000 PCS 24GA
Production Id	SLVT01 L 4 1 11653
Production Time	2024-01-26T12:28:21Z
IPEI	15093 0011653
Access code	123456
User	
Standby text	Ext 1806
DECT to DECT	
Disabled	
Phone Language	Default 🗸
SIP	
Username / Extension *	2482 66
Secondary username	
Domain	
Displayname	1806
Authentication user	47 b6
Authentication password	•••••
Features	
Call forward unconditional	
Admin rights	

• 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.

2///8

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-bordercontroller/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



9.2 Setup Entitlements

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



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

	0
ORACLE Enterprise Session Border Controller	Sign in to E-SBC Enter your details below Username Brequired Password Brequired SIGN IN

ORACLE	E Enterprise Ses	sion Border Controller						admin 👻
NN4600-139 10.13	58.194.139 SCZ9.3.0	Patch 1 (Build 74)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	ā Q				Discard	Ø Verify	Save
media-manager	>	Configuration Objects						
security	>							
session-router	>	Name 🗘	Description 😂					
system	>	access-control	Configure a static or dynamic access control list					
		account-config	Configure Quality of Service accounting					
		authentication-profile	Configure authentication profile					
		certificate-record	Create, generate, and import a certificate					
		class-policy	Configure classification profile policies					
		codec-policy	Create and apply a codec policy to a realm and an agent					
		filter-config	Create a custom filter for SIP monitor and trace					
		fraud-protection	Configure fraud protection					
		host-route	Insert entries into the routing table					
		http-client	Configure an HTTP client					
		http-server	Configure an HTTP server					
		Idap-config	Configure an LDAP server, filter, and policy					
		local-policy	Configure a session request routing policy					
		local-routing-config	Configure local routing servers					
		media-manager	Configure media policy, attributes, and settings					
		media-policy	Configure a media profile and apply it to a realm					
There are a second and a		merlia-nrofile	Configure a media profile and apply it to a media type					
Show All		Displaying 1 - 17 of 41						

Refer to the SBC GUI User Guide for more information:

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/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

SolutionsLab- ySBC-2 10.11.4 SC29.3.0 Patch 2 (Build 98)						
Configuration View Configuration	ពិ	۹				
codec-policy		Modify System Config				
media-manager						
media-policy		Hostname	Oracle SBC			
realm-config		Description	Access SBC for SpectraLink IP-Dect and Zoom			
steering-pool			Phone Local Proxy			
security	>					
session-router	>	Location	Burlington, MA			
system	~	Mib System Contact				
fraud-protection						
host-route		Mib System Name				
http-client		Mib System Location				

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-bordercontroller/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

ORACLE Enterprise Session Border Controller							
NN4600-139 10.138.194.139 SCZ9.3.0 Patch 1 (Build 74)							
Configuration View Configuration	Q						
host-route	Modify NTP Config						
http-client							
http-server	Server	[198.55.111.50 x] 206.108.0.131 x]					
ipt-config	DNS Realm						
memory-leak-tracker	Auth Servers						
network-interface	No auth servers to display. Please add.						
network-parameters	Add						
ntp-config							

• 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

ORACLE Enterprise Session Border Controller									
SolutionsLab- vSBC-2 10.1.1.4 SCZ9.3.0 Patch 2 (Build 98)									
Configuration View Configuration (B) Q									
media-manager >	Phy	Phy Interface							
security >									
session-router >				A faith and the faith fa					
system 🗸	L. T. 🕹 // L 🔟 Delete all PMy interface items								
fraud-protection	Select	Action	Name 🗘	Operation Type 💲	Port 🗘	Slot 🗘			
host-route		:	s0p0	Media	0	0			
http-client		:	s1p0	Media	0	1			

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

ORACL	Enterprise Sessi	ion Borde	Controll	er						
SolutionsLab- vSBC-2	10.1.1.4 SCZ9.3.0 Patc	h 2 (Build 9	8)						Dashboard	Configur
Configuration	View Configuration	ដ	Q							
media-manager		>	Netv	vork Ir	nterface					
security		>								
session-router		>	D	D. 슈, 크, 🖉 🗇 🍵 Delete al Network Interface items						
system		~								
fraud-protection			Select	Action	Name 😄	Sub Port Id 😄	Description 🗘	Hostname 😄	IP Address 😄	
host-route				- 1	s0p0	0			10.1.2.4	
http-client				- 8	s1p0	0			10.1.3.4	

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.

Configuration View Configuration		
media-manager	Modify Certificate Record	
security		
authentication-profile	Name	SBC-Endpoint-Certificate
certificate-record	Country	US
tls-global	State	МА
tis-profile	Locality	Texas
system	Organization	Oracle Corp
	Unit	Solutions Lab
	Common Name	cloudsbc.cgbusolutionslab.com
	Key Algor	rsa 🗸
	Digest Algor	sha256 👻
	Ecdsa Key Size	p256 🗸
	Cert Status Profile List	

Configuration View Configuration	Q							
media-manager	>	Modify Certificate Record						
security	~							
authentication-profile		Name	CGBUBurlington					
certificate-record		Country	US					
tls-global		State	California					
tls-profile		Locality	Redwood City					
session-router	>							
system	>	Organization	Oracle Corporation					
		Unit						
		Common Name	solutionslab.cgbuburlington.com					
		Key Algor	rsa 🗸					
		Digest Algor	sha256 🗸					
		Ecdsa Key Size	p256 •					

• 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	digitalSignature
	keyEnchpherment	keyEnchpherment
Extended Key Usage List	serverAuth	serverAuth
Key algor	Rsa	Rsa
Digest-algor	Sha256	Sha256

Configuration View Configuration	6	Q										Discard	@ verify	🕼 Sere
media-manager		>	Certi	ficate	Record								Show C	onfiguration
security		~												
authentication-profile			D	đ.	.+ 🕅 PKC512 / 🗅	1 E R Delete all Certific	ate Record Items				Search			0
certificate-record														~
tis-global			Select	Action	Name O	Country 0	State 0	Locality o	Organization 0	Unit o		Common Name	0	
tis-profile				1	CGBUBurlington	US	California	Redwood City	Oracle Corporation			solutionslab.cgbu	uburlington.co	¥m.
session-router				1	DigiCertRoot	US	MA	Burlington	Engineering			DigiCert Global R	loot CA	
		1		3	DigiGlobalRootG2	us	MA	Burlington	Engineering			DigiCert Global R	loot G2	
SADIGUL		<i>′</i>		8	SBC-Endpoint-Certificate	US	ма	Texas	Oracle Corp	Solutions Lab		cloudsbc.cgbusol	lutionslab.com	

At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must <u>save and activate</u> 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:

Configuration View Configuration	ð Q		
media-manager	>	Certificate Record	
security	~		
authentication-profile			
certificate-record		다. 소 보 🗹 PKCS12 / 다 🛱 🖳 🗹	1
tls-global		Select Action Name \Diamond Country \Diamond	
tls-profile		CGBUBurlington US	
session-router	>	DigiCertRoot US	
system	>	DigiGlobalRootG2 US	
		SBC-Endpoint-Certificate US	



Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, another <u>save and activate</u> 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 <u>save/activate</u> from the WebGUI to complete the configuration of certificates on the Oracle SBC.

Configuration View Configuration	Q				
media-manager	>	Certi	ificate	Record	
security	~				
authentication-profile		D	*		🖶 🖂 🔽 Delate all Certific
certificate-record		L.	<u>ت</u>		
tls-global		Select	Action	Name 😄	Country
tls-profile			:	CGBUBurlington	US
session-router	\$:	DigiCertRoot	US
sustem			:	DigiGlobalRootG2	US
aystern	1		:	SBC-Endpoint-Certificate	US

Format	try-all 👻
mport Method	⊖ File
	Paste
Paste	BEGIN CERTIFICATE MIIEIjCCAwqgAwlBAgIBFzANBgkq hkiG9w0BAQsFADB/MQswCQYDV QQGEwJVUZEL MAKGA1UECAwCTUExEDAOBgNV BAcMB0JIZGZvcmQxFDASBgNVB AoMC0VuZ2luZWVy aW5nMRcwFQYDVQQDDA5BY21II FBhY2tldCBNQTEiMCAGCSqGSIb3 DQEJARYTdXNI ckBhY21lcGFja2V0LmNvbTAeFw0 vMZEvMTgxNDUvMidaFw0v0DEv

• 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:

Configuration View Configuration	Q		
media-manager	>	Modify TLS Profile	
security	~		
authentication-profile		Name	SLEndpoints-TLS
certificate-record		End Entity Certificate	SBC-Endpoint-Certificate
tis-global		Trusted Ca Certificates	DigiCertRoot x DigiGlobalRootG2 x
tls-profile			
	-		

Configuration View Configuration		
media-manager	Modify TLS Profile	
security ~		
authentication-profile	Name	ZoomProxyTLSProfile
certificate-record	End Entity Certificate	CGBUBurlington +
tis-global	Trusted Ca Certificates	DigiCertRoot x DigiGlobalRootG2 x
tls-profile		

• 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.

Configuration View Configuration	Q				
media-manager	>	Modify Sdes Profile			
security	~				
admin-security	>	Name	SL-SRTP		
auth-params		Crypto List	AES_CM_128_HMAC_SHA1_80 x		
authentication			AES_CM_128_HMAC_SHA1_32 x		
authentication-profile		Srto Auth	✓ enable		
cert-status-profile			2 enable		
certificate-record		Srtp Encrypt	e choic		
factory-accounts		SrTCP Encrypt	enable		
ike	>	Mki	🗌 enable		
ipsec	>	Egress Offer Format	same-as-ingress 💌		

Configuration View Configuration	r Q		
media-manager	>	Modify Sdes Profile	
security	~		
admin-security	>	Name	ZoomSRTP
auth-params		Crypto List	AES_CM_128_HMAC_SHA1_80 ×
authentication			AES_CM_128_HMAC_SHA1_32 ×
authentication-profile		Srtp Auth	enable
cert-status-profile			🗖 enable
certificate-record		Srtp Encrypt	
		SrTCP Encrypt	enable

- 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.

Configuration View Configuration	Q			
media-manager	`	Modify Media Sec Policy Entries		
security	~			
admin-security	>	Name	SL-MediaSecurity	
auth-params		Pass Through	enable	
authentication		Options		
authentication-profile				
cert-status-profile		~ Inbound		
certificate-record		Profile	SL-SRTP	•
factory-accounts		Mode	srtp	•
ike	>	Protocol	sdes	•
ipsec	>			
local-accounts		Hide Egress Media Update		
media-security	~	✓ Outbound		
dtls-srtp-profile		Profile	SL-SRTP	•
media-sec-policy		Mode	srtp	•
sdes-profile		Protocol	sdes	•

Configuration 1 and a state			
Configuration View Configuration	të Q		
media-manager	> Î	Modify Media Sec Policy Entries	
security	~		
admin-security	>	Name	ZoomMediaSecurity
auth-params		Pass Through	enable
authentication		Options	
authentication-profile			
cert-status-profile		~ Inbound	
certificate-record		Profile	ZoomSRTP
factory-accounts		Mode	srtp 🗸
ike	>	Protocol	sdes 💌
ipsec	>	The Free Made Dates	enable
local-accounts		Hide Egress Media Update	
media-security	~	✓ Outbound	
dtls-srtp-profile		Profile	ZoomSRTP
media-sec-policy		Mode	srtp 🗸
sdes-profile		Protocol	sdes 🗸

• 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

Configuration	View Configu	ration 🛅 Q		Discard 😥 Verify 🖺 Save
media-manager codec-policy	~	Modify Media Manager		Show Advanced Show Configuration
media-manager		State	enable	
media-policy		Max Signaling Bandwidth	1000000	(Range: 7100010000000)
realm-config		Max Untrusted Signaling	100	(Range: 0.100)
steering-pool		Min Untrusted Signaling	30	(Range: 0.100)
security	>	Dos Guard Window	5	(Range: 1.30)
system	>	Untrusted Minor Threshold	0	(Range: 0.100)
		Untrusted Major Threshold	0	(Range: 0.100)
		Untrusted Critical Threshold	0	(Range: 0.100)
		Trusted Minor Threshold	0	(Range: 0.100)
		Trusted Major Threshold	0	(Range: 0.100)
Show All		OK Delete		L

• 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	\checkmark	\checkmark
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 <u>Media Security</u> section of this guide.

SolutionsLab- vSBC-2 10.1.1.4 SCZ9.3.0 Part	tch 2 (Build 98	3)					
Configuration View Configuration	Configuration View Configuration						
media-manager	~	Real	n Cor	ıfig			
codec-policy							
media-manager		D	<u>ث</u>	上 / 凸 面 □	elete all Realm Config items		
media-policy			-				
realm-config		Select	Action	Identifier 💠	Description 🗘	Addr Prefix 🗇	Network Interfaces \Diamond
steering-pool			:	SLEndpoints		0.0.0.0	s0p0:0.4
security			:	ZoomProxy		0.0.0.0	s1p0:0.4

• 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.

ORACL	ORACLE Enterprise Session Border Controller						
SolutionsLab- vSBC-2	10.1.1.4 SCZ9.3.0 Patch 2 (Build 9	B)					
Configuration	figuration View Configuration C Q						
media-manager	~	 Steering Pool 					
codec-policy							
media-manager		D	t.	.↓ / ⊡ ⊡ Delete	all Steering Pool items		
media-policy							
realm-config		Select	Action	IP Address 💠	Start Port 😄	End Port 💠	Realm ID 💲
steering-pool			÷	10.1.2.4	20000	20999	SLEndpoints
security	、 、		- 1	10.1.3.4	10000	10999	ZoomProxy

• 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

ORACL	.E Enterprise Sessi	ion Border	Controller		•
SolutionsLab- vSBC-2	10.11.4 SCZ9.3.0 Patc	h 2 (Build 9)	8)		Dashboard Configuration Monitor and Trace W
Configuration	View Configuration	ñ	Q		Discard
media-manager		>	Modify SIP Config		Show Advanced
security		>			
session-router		~	State	🗹 enable	
access-control			Dialog Transparency	enable	
account-config			Home Realm ID	ZoomProxy	
filter-config			Egress Realm ID		
Idap-config					
local-policy			Nat Mode	None •	
local-routing-cor	nfig		Registrar Domain	*	
media-profile			Registrar Host	gosip01.sc.zoom.us]
session-agent			Registrar Port	5091	(Range: 0,002565535)

• 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	\checkmark	
Route to Registrar	\checkmark	
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

	nterprise Sessio	n Border	Control	er							
SolutionsLab- vSBC-2 10.11.4	ab- 1011.4 SC2P3.0 Parks 2 (Suida 98)						Dashboard	Configuration			
Configuration View	Configuration	ĉ	Q								
tls-profile			Мос	lify SIF	Interface						5
session-router		~									
access-control			State				enable				
account-config			Realm	ID			SLEndpoints	•			
filter-config			Descrip	ption							
Idap-config											
local-policy											
local-routing-config			SIP Po	orts							
media-profile			D,	1	· · · ·						
session-agent			Select	Action	Address 0	Port o		Transport Protocol 🔅	TLS Profile 🔉	Allow Anonymous 😄	
session-group				1	10.1.2.4	5061		TLS	SLEndpoints	registered	

ORACLE Enterpres Session Border Controller								
SolutionsLab- vSBC-2 10.11.4 SCZ9.3.0 Patch 2 (Build S	28)						Dashboard	Configuration
Configuration View Configuration	Q							
tis-profile	Modify SI	P Interface						s
session-router 🗸 🗸								
access-control	State			enable				
account-config	Realm ID			ZoomProxy	-			
filter-config	Description							
Idap-config								
local-policy								
local-routing-config	SIP Ports							
media-profile	D.	/ 6 8						
session-agent	Select Action	Address 😄	Port 😄		Transport Protocol 💠	TLS Profile 👙	Allow Anonymous 🗘	
session-group	• ·	10.1.3.4	5061		TLS	ZoomProxyTLSProfile	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:

ORACLE Enterprise Session Border Controller				
vSBC-2 10.1.1.4 SCZ9.3.0 Patch 2	! (Build 98)		
Configuration View Configuration	ិ	۹		
media-manager	•	Modify Session Agent		
security	>			
session-router	~	Hostname	gosip01.sc.zoom.us	
access-control		IP Address		
account-config		Port	5091	
filter-config				
ldap-config		State		
local-policy		Transport Method	StaticTLS 🔹	
local-routing-config		Realm ID	ZoomProxy 🗸 🗸	
media-profile		Egress Realm ID		
session-agent		Description		
session-group				
session-recording-group				
session-recording-server		Ping Method	OPTIONS	
session-translation		Ping Interval	30	

• 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 <u>SIP config</u>, 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 <u>SIP interface</u>. 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:

ORACLE Enterprise Session Border Controller					
SolutionsLab- vSBC-2 10.1.1.4 SCZ9.3.0 Patch	2 (Build 9	8)			
Configuration View Configuration	ើ	۹			
media-manager	>	Modify Access Control			
security	>				
session-router	~	Realm ID	ZoomProxy	•	
access-control		Description			
account-config					
filter-config					
ldap-config		Source Address	192.204.13.4		
local-policy		Destination Address	0.0.0.0		
local-routing-config		Application Protocol	SIP	•	
media-profile					
session-agent		Transport Protocol	ALL	•	
session-group		Trust Level	high	•	

• Click OK at the bottom.

9.12 Save and Activate

9.12.1 Save Config

ORACLE Enterprise Session Border Cont	oller	û, ➡ admin ➡
NN4600-139 10.138.194.139 SC29.3.0 Petch 1 (Build 74)		Dashboard Configuration Monitor and Trace Widgets System
Configuration View Configuration C		Ctscard 🙆 Made 🔯 Save
media-manager >	Modify Account Config	Show Advanced Show Configuration

9.12.2 Activate Config

ORACLE Enterprise Session Border Controller					
NN4600-139 10.138.194.139 SCZ9.3.0 Patch 1 (Build 74)					
Configuration View Configuration	Configuration View Configuration fb Q				
media-manager >	Modify Account Config				
security >					
session-router 🗸	Strategy	Hunt 👻			
access-control	Protocol	RADIUS			
account-config	State	🖬 enable			
filter-config					
ldap-config	DNS Realm	•			
local-policy	Generate Start	Invite 👻			
local-routing-config	Generate Interim	Unsuccessful-Attempt x Egress-Invite x			
media-profile		Confirm			
session-agent	Generate Event	There are errors. Do you want to activate the configuration?			
session-group	File Output	Confirm Cancel			
session-recording-group	7.04				

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.

Configuration View Configuration	n Ĉ	٩	
media-manager	>	Modify SIP Interface	
security	>		L
session-router	~	Registration Interval	3600
access-control		Route To Registrar	🗌 enable
account-config		Secured Network	🗌 enable
filter-config		Lid Ende Domaio	
ldap-config			
local-policy		Options	
local-routing-config		SPL Options	HeaderNatPublicSipIfIp=20.96.25.165,HeaderNatPriv

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 access-control	-config short
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 SBC-Endpoint-Certificate name locality Texas organization Oracle Corp unit Solutions Lab cloudsbc.cgbusolutionslab.com common-name serverAuth extended-key-usage-list clientAuth http-server name webServerInstance WebServerInstance tls-profile media-manager max-signaling-bandwidth 4000000 9 max-untrusted-signaling min-untrusted-signaling 8 media-sec-policy name **TeamsMediaSecurity** inbound profile SL-SRTP mode srtp protocol sdes outbound SL-SRTP profile mode srtp protocol sdes media-sec-policy ZoomMediaSecurity name inbound ZoomSRTP profile 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 time.google.com server DNS-Realm ZoomProxy phy-interface s0p0 name operation-type Media phy-interface name s1p0 operation-type Media slot 1 realm-config identifier **SL-Endpoints** s0p0:0.4 network-interfaces

mm-in-realm	enabled
media-sec-policy	SL-MediaSecurity
access-control-trust-leve	l low
invalid-signal-threshold	5
maximum-signal-thresho	ld 4000
untrusted-signal-threshol	d 25
realm-config	20
identifier	ZoomProvy
network-interfaces	c100.0 4
mm in roolm	anabled
modio aco policy	ZoomModioSocurity
media-sec-policy	
access-controi-trust-ieve	i nign
sdes-prolle	
name	
crypto-list	
	AES_UM_128_HMAU_SHA1_32
sdes-profile	7 0070
name	
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	gosipu i.sc.zoom.us
registrar-host registrar-port	gosipu i.sc.zoom.us 5091
registrar-host registrar-port options	gosipu i.sc.zoom.us 5091 max-udp-length=0
registrar-host registrar-port options	gosipu i.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from
registrar-host registrar-port options sip-interface	gosipo i.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from
registrar-host registrar-port options sip-interface realm-id	gosipo i.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints
registrar-host registrar-port options sip-interface realm-id sip-port	gosipo i.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints
registrar-host registrar-port options sip-interface realm-id sip-port address	gosipo i.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4
registrar-host registrar-port options sip-interface realm-id sip-port address port	gosipo i.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol	gosipo I.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous	gosipo I.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal	gosipo I.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching	gosipo I.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar	gosipo I.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network	gosipo I.Sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled enabled enabled
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options	gosipo I.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled enabled HeaderNatPublicSipIflp=20.110.144.248,HeaderNatPrivateSipIflp=10.1.2.4
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface	gosipol.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id	gosipo I.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port	gosipoli.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address	gosipol.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address port	gosipol.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4 5061
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address port transport-protocol	gosipol.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4 5061 TLS
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address port transport-protocol tls-profile	gosipoli.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4 5061 TLS ZoomProxyTLSProfile
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address port transport-protocol tls-profile allow-anonymous	gosipoli.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4 5061 TLS ZoomProxyTLSProfile agents-only
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address port transport-protocol tls-profile allow-anonymous spl-options	gosipo 1.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled headerNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4 5061 TLS ZoomProxyTLSProfile agents-only HeaderNatPublicSipIfIp=20.96.25.165 HeaderNatPrivateSipIfIp=10.1.3.4
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address port transport-protocol tls-profile allow-anonymous spl-options	gosipul.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4 5061 TLS ZoomProxyTLSProfile agents-only HeaderNatPublicSipIfIp=20.96.25.165,HeaderNatPrivateSipIfIp=10.1.3.4
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address port transport-protocol tls-profile allow-anonymous spl-options sip-monitoring monitoring-filters	gosipul.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4 5061 TLS ZoomProxyTLSProfile agents-only HeaderNatPublicSipIfIp=20.96.25.165,HeaderNatPrivateSipIfIp=10.1.3.4 *
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address port transport-protocol tls-profile allow-anonymous spl-options sip-monitoring monitoring-filters	gusipul.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4 5061 TLS ZoomProxyTLSProfile agents-only HeaderNatPublicSipIfIp=20.96.25.165,HeaderNatPrivateSipIfIp=10.1.3.4
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address port transport-protocol tls-profile allow-anonymous spl-options sip-monitoring monitoring-filters steering-pool ip-address	gospon.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4 5061 TLS ZoomProxyTLSProfile agents-only HeaderNatPublicSipIfIp=20.96.25.165,HeaderNatPrivateSipIfIp=10.1.3.4 * 10.1.2.4
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address port transport-protocol tls-profile allow-anonymous spl-options sip-monitoring monitoring-filters steering-pool ip-address start-port	gospon.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4 5061 TLS ZoomProxyTLSProfile agents-only HeaderNatPublicSipIfIp=20.96.25.165,HeaderNatPrivateSipIfIp=10.1.3.4 * 10.1.2.4 20000
registrar-host registrar-port options sip-interface realm-id sip-port address port transport-protocol allow-anonymous nat-traversal registration-caching route-to-registrar secured-network spl-options sip-interface realm-id sip-port address port transport-protocol tls-profile allow-anonymous spl-options sip-monitoring monitoring-filters steering-pool ip-address start-port end-port	gosipul.sc.zoom.us 5091 max-udp-length=0 reg-cache-mode=from SL-Endpoints 10.1.2.4 5061 TLS registered always enabled enabled enabled HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4 ZoomProxy 10.1.3.4 5061 TLS ZoomProxyTLSProfile agents-only HeaderNatPublicSipIfIp=20.96.25.165,HeaderNatPrivateSipIfIp=10.1.3.4 * 10.1.2.4 20000

////

11110

steering-pool ip-address start-port end-port realm-id	10.1.3.4 10000 10999 ZoomProxy
system-config	
hostname description	Oracle SBC
location	Burlington, MA
tls-profile	
name	SLEndpoints-TLS
end-entity-certificate trusted-ca-certificates	SBC-Endpoint-Certificate DigiCertRoot DigiGlobalRootG2
tls-version	tlsv12
tls-profile	
name end-entity-certificate trusted-ca-certificates	ZoomProxyTLSProfile CGBUBurlington DigiCertRoot DigiGlobalRootG2
mutual-authenticate	enabled
tls-version	tisv12

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)



CONNECT WITH US



X twitter.com/oracle

oracle.com/

Oracle Corporation, World Headquarters 2300 Oracle Way Austin, TX 78741, USA Worldwide Inquiries Phone: +1.650.506.7000 or Phone: +1.800.392.2999

Integrated Cloud Applications & Platform Services

Copyright © 2024, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

111172

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615