

Oracle SBC integration with Cisco Call Manager (CUCM) and Zoom Phone Premise Peering (BYOC)

**Technical Application Note** 



# Disclaimer

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

# **Revision History**

Revision	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with Cisco CUCM and Zoom Phone Premise Peering (BYOC)	22 <sup>nd</sup> May 2022
1.1	Updated the certificate related information for Zoom (using DigiCert G2 and G3 root certificate as their primary Root Certificate for TLS negotiation)	10 <sup>th</sup> November 2023

# **Table of Contents**

1. INTENDED AUDIENCE	
2 DOCUMENT OVERVIEW	4
2.1 ZOOM BYOC	4
2.2. CISCO CALL MANAGER (CISCO CUCM)	
	_
3. INTRODUCTION	
3.1. AUDIENCE	
3.2. KEQUIKEMENIS	
5.5. ARCHITECTURE	0
4. CONFIGURING THE CISCO CALL MANAGER (CISCO CUCM)	7
4.1. CONFIGURING A NEW SIP TRUNK	7
4.2. CONFIGURE A NEW ROUTE PATTERN	
4.3. END USER CONFIGURATION	
4.4. ADDING SIP PHONE IN CUCM	12
4.5. ASSOCIATING END USER TO PHONE	14
5. ZOOM PHONE CONFIGURATION	15
5.1. CREATE A ZOOM USER	15
5.2. ADD BYOC NUMBER	15
5.3. Assign the BYOC number to a User	16
6. INFRASTRUCTURE REQUIREMENTS	
7. CONFIGURING THE SBC	
7.1. VALIDATED ORACLE SBC VERSION	
8. NEW SBC CONFIGURATION	
8.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC	
8.2. CONFIGURE SBC USING WEB GUI	
8.3. CONFIGURE SYSTEM-CONFIG	
8.4. CONFIGURE PHYSICAL INTERFACE VALUES	
8.5. CONFIGURE NETWORK INTERFACE VALUES	
8.6. ENABLE MEDIA MANAGER	
8.7. CONFIGURE REALMS	
8.8. ENABLE SIP-CONFIG	
8.9. CONFIGURING A CERTIFICATE FOR SBC	
8.10. ILS-PROFILE.	
8.11. CONFIGURE SIP INTERFACES	
8.12. CONFIGURE SESSION-AGENT	
8.17. CONFIGURE LOCAL-POLICT	43
8 15 CONFIGURE PING RESPONSE	43 46
8 16 SBC CONFIG FOR CISCO OFFER LESS INVITE	40 47
8.17. CONFIGURE SDES PROFILE.	
8.18. CONFIGURE MEDIA SECURITY PROFILE	
9. EXISTING SBC CONFIGURATION	

# 1. Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of the Oracle Enterprise Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform, Cisco Call Manager (Cisco CUCM) along with Zoom Phone-Premise Peering - BYOC.

## 2. Document Overview

This Oracle technical application note outlines the configuration needed to set up the interworking between on premises Cisco CUCM using Oracle SBC and Zoom BYOC. The solution contained within this document has been tested using Oracle Communication SBC **900p3** version. Our scope of this document is testing the interoperability of Oracle SBC with CUCM and Zoom BYOC.

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

Please find the related documentation links below:

## 2.1. Zoom BYOC

https://Zoom.us/docs/doc/Zoom-Bring%20Your%20Own%20Carrier.pdf https://Zoom.us/phonesystem https://Zoom.us/Zoom-phone-features

### 2.2. Cisco Call Manager (Cisco CUCM)

Cisco Unified Call Manager provides industry-leading reliability, security, scalability, efficiency, and enterprise call and session management and is the core call control application of the collaboration portfolio.

It should be noted that while this application note focuses on the optimal configurations for the Oracle SBC in an enterprise Cisco CUCM 12.5 environment, the same SBC configuration model can also be used for other enterprise applications with a few tweaks to the configuration for required features.

In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the Cisco CUCM Server associated parameters. Many SBC applications may have additional configuration requirements that are specific to individual customer requirements. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

For additional information on CUCM 12.5, please visit

https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-version-12-5/index.html

Please note that the IP Addresses, FQDN and configuration names and details given in this document are used for reference purposes only. These same details cannot be used in customer configurations. End users of this document can use the configuration details according to their network requirements. There are some public facing IPs (externally routable IPs) that we use for our testing are masked in this document for security reasons. The customers can configure any publicly routable IPs for these sections as per their network architecture needs.

## 3. Introduction

#### 3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Cisco CUCM 12.5 version using Oracle Enterprise SBC and Zoom BYOC. There will be steps that require navigating the CUCM 12.5 server configuration, Oracle SBC GUI interface, understanding the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP, TLS/SRTP are also necessary to complete the configuration and for troubleshooting, if necessary.

#### 3.2. Requirements

- Fully functioning Cisco Call Manager (CUCM) 12.5 version.
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 9.0.0 version
- Zoom Phone subscription running Zoom Client.

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

Software Used	SBC Version	Cisco CUCM Version	Zoom Client version
Revision 1	9.0.0	12.5	Version: 5.10.6 (5263)

#### 3.3. Architecture



The PSTN part shown in the network architecture is not covered in this document (Out of scope for this document) and the end user can configure the PSTN part if they need it as per their requirements.

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

- Phase 1 Configuring the Cisco Unified Call Manager v12.5 for Oracle SBC.
- Phase 2 Configuring the Zoom BYOC.
- Phase 3 Configuring the Oracle SBC.

# 4. Configuring the Cisco Call Manager (Cisco CUCM)

Please login to Cisco CUCM admin web GUI with proper login credentials (Username and password). After that, perform the steps below in the given order.

← → C ▲ Not secure   10.232.50.89/ccmadmin/showHome.do	☆ <b>0</b> :
CISCO Unified CM Administration For Cisco Unified Communications Solutions	Navigation Cisco Unified CM Administration • Go
Cisco Unified CM Administration	Username admin Passward Login Reset
Copyright © 1999 - 2016 Cisco Systems, Inc. All rights reserved. This product contains cryptographic features and is subject to United States and local countr products does not imply third-party authority to import, export, distribute or use encryption. U.S. and local country laws. By using this product you agree to comply with applicable laws i product immediately.	y laws governing import, export, transfer and use. Delivery of Cisco cryptographic Importers, exporters, distributors and users are responsible for compliance with and regulations. If you are unable to comply with U.S. and local laws, return this
A summary of U.S. laws governing Cisco cryptographic products may be found at our Export	t Compliance Product Report web site.
For Cisco Technical Support please visit our Technical Support web site.	unications aracent polanentation web site.

## 4.1. Configuring a new SIP Trunk

01) Go to Device ----- Trunk ----- Add New

02) Select Trunk Type – SIP Trunk and then Click Next

03) In the Device Name field, enter the SIP Trunk name and optionally provide a description.

04) In the Device Pool drop-down list, select a device pool id created already else select Default

05) Enter the Destination Address and Destination Port of the SBC under SIP Information.

06) Select appropriate SIP profile and SIP trunk security profile from the dropdown menu.

07) Click Save

$\leftarrow \rightarrow C$	Not seare   10.232.50	).89/ccmadmin/trunl	kEdit.do?pi	rodt=95			☆	0	:
cisco For Cisco	Unified CM Ad	ministration Solutions		Navigation C admin S	i <mark>sco Unified CM Adm</mark> Gearch Documentat	inistratio	n About	•   Lo	Go gout
System ▼ Call Routin Help ▼	g 👻 Media Resources 👻	Advanced Features 🔻	Device 🔻	Application 👻	User Management	▼ Bulł	Adminis	tration	•
Trunk Configuration					Related Links: 🛽	Back To	Find/Lis	st 🔻	Go
Next									
– Status –									
i Status: Ready									
Trunk Information									
Trunk Type*	SIP Trunk		•						
Device Protocol*	SIP		•						
Trunk Service Type*	None(Default)		•						
Next indicates req	uired item.								

Cisco Unified CM Administration			Navigation Cisco Unified CM Administration
CISCO For Cisco Unified Communications Solutions			admin   Search Documentation   About
System      Call Routing      Media Resources      Advanced Features      Dev	ice • Application • User Management • Bulk Adm	ninistration 🔻 Help 👻	
Trunk Configuration			Related Links: <b>Back To Find/List</b>
🔚 Save 🗙 Delete			
Product:	SIP Trunk		
Device Protocol:	SIP		
Trunk Service Type	None(Default)		
Device Name*	CUCM-SBC		
Description			
Device Pool*	Default	¥	
Common Device Configuration	< None >	<b>v</b>	
Call Classification*	Use System Default	¥	
Media Resource Group List	< None >	¥	
Location*	Hub_None	¥	
AAR Group	< None >	¥	
Tunneled Protocol*	None	¥	
QSIG Variant*	No Changes	$\checkmark$	
ASN.1 ROSE OID Encoding*	No Changes	$\vee$	
Packet Capture Mode*	None	¥	
Packet Capture Duration	0		
Media Termination Point Required			
Retry Video Call as Audio			
Path Deplacement Cupport			

aluda Cisco Unified CM	Administ	ration				Navigation Cisco Unifie	d CM Administratio	on v	
CISCO For Cisco Unified Communic	ISCO         For Cisco Unified Communications Solutions         admin         Search Documentation         About								
System - Call Routing - Media Resources	stem   Call Routing  Media Resources  Advanced Features  Device  Application  User Management  Buik Administration  Help								
Trunk Configuration	runk Configuration Related Links: Back To Find/List								
🔲 Save 🎽 Delete 💁 Reset 斗	Add New								
SIP Information									
Destination									
Destination Address is an SRV									
Destination Address		Destination Address IPv	6	Destination Port	Status	Status Reason	Durati	ion	
1* 10.232.50.78				5060	ир		Time Up: 0 da minut	y 0 hour 21 .es	
MTP Preferred Originating Codec*	711ulaw			1					
BLF Presence Group*	Standard Pres	ence aroup		]					
SIP Trunk Security Profile*	Non Secure S	IP Trunk Profile		]					
Rerouting Calling Search Space				]					
Out-Of-Dialog Refer Calling Search Space			-	]					
SUBSCRIBE Calling Search Space				]					
SIP Profile*	Standard Sin	Profile - Options Enabled ISP	-	View Details					
DTME Signaling Method*									
	KFC 2033		~						
Normalization Script									
Normalization Script < None >		¥							
Enable Trace									

////

#### 4.2. Configure a new Route Pattern

01) Go to Call Routing ------ Route/Hunt ------ Route Pattern and click Add New
02) Enter a Route Pattern according to the network requirements and calling plan.
03) From the Gateway/Route List drop-down list, select the created SIP Trunk device name.

04) Click Save. We can create other route patterns in the same way as shown below.

alada Cisco Unified CM Ad	ministration							Navigation Cisco Unified CM Administration 🗸 🗸
CISCO For Cisco Unified Communication	ns Solutions							admin Search Documentation About
System      Call Routing      Media Resources	Advanced Features 👻	Device 🔻	Application •	User Ma	nagement 🔻	Bulk Administration 👻	Help 🔻	
Route Pattern Configuration								Related Links: Back To Find/List 🗸
🔜 Save 🗶 Delete 🕒 Copy 🕂 Add N	lew							
Status								
(i) Status: Ready								
Pattern Definition								
Route Pattern*	1XXXXXXXXXX							
Route Partition	< None >			v				
Description	Route to SBC							
Numbering Plan	Not Selected			V				
Route Filter	< None >			V				
MLPP Precedence*	Default			¥				
Apply Call Blocking Percentage								
Resource Priority Namespace Network Domain	< None >			¥				
Route Class*	Default			~				
Gateway/Route List*	CUCM-SBC			~	( <u>Edit</u> )			
Route Option	Route this pattern							
	$\bigcirc$ Block this pattern	No Error		۷				

The route patterns that has been created is shown below:

սիսիս	Cisco Unified CM Administra	ation			Navigation Cisco Unified CM Ad	ministration 🗸			
CISCO	For Cisco Unified Communications Solutions				admin Search Docume	ntation About Log			
System -	Call Routing • Media Resources • Advanced Fea	itures • Device • Application • User Ma	anagement 🔻 Bulk Administra	ation • Help •					
Find and	List Route Patterns								
Add N	Add New 🔠 Select All 🔛 Clear All 💥 Delete Selected								
Status-									
<b>1</b> 2 red	cords found								
Route P	atterns (1 - 2 of 2)					Rows per Page 50			
Find Route	e Patterns where Pattern	✓ begins with ✓	Find Clear Filter	ф <b>—</b>					
	Pattern 📥	Description	Partition	Route Filter	Associated Device	Сору			
	<u>1XXXXXXXXXXX</u>	Route to SBC			CUCM-SBC	ß			
	<u>91XXXXXXXXXXX</u>	Route to SBC			CUCM-SBC	6			
Add Ne	w Select All Clear All Delete Selected								

1111111110

The created SIP trunk associated with the route pattern is shown below:

սիսիս	Cisco U	<b>Inified Cl</b>	M Adminis	stration	1							Navigation Cisco Unified CM Admini	stration 🗸 G
cisco	For Cisco U	nified Commu	nications Solut	ions								admin Search Documentati	ion About Logo
System 👻	Call Routing •	Media Resour	rces 🔻 Advance	ed Features 🔻	Device 🕶	Application - U	er Managem	ent 🔻 Bul	lk Adminis	tration 🔻	Help 🔻		
Find and	List Trunks												
Add N	Vew Eselect	t All 🔛 Clea	ar All 🙀 Dele	te Selected	Preset S	elected							
-Status													
<b>(i)</b> 4 rec	cords found												
Trunks	(1 - 4 of 4	)										,	Rows per Page 50 🗸
Find Trunk	s where Devic	e Name	v begin	is with		Find	Clear Fil	ter 🔒	_				
					Select item (	or enter search tex	t v						
		Name 🔺	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration	SIP Trunk Security Prof
		CUCM-			<u>Default</u>					SIP	Full Service	Time In Full Service: 9 days 16 hours	Non Secure SIP True
		CUCM- SBC			<u>Default</u>	<u>1XXXXXXXXXXXXXX</u>				SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 41 minutes	Non Secure SIP True Profile
		<u>CUCM-</u> <u>SBC</u>			<u>Default</u>	<u>91XXXXXXXXXXX</u>				SIP Trunk	Full Service	Time In Full Service: 0 day 0 hour 41 minutes	<u>Non Secure SIP Trui</u> <u>Profile</u>
		sbcce			<u>Default</u>					SIP Trunk	No Service	Time not in Full Service: 7 days 19 hours 33 minutes	Non Secure SIP True Profile
Add Ne	w Select All	Clear All	Delete Select	ted Reset	t Selected								

# 4.3. End User Configuration

- 01) Go to User Management ---- End User and click Add New
  02) Enter in your User ID, password, pin, and Last Name
  03) You must also enter in a password in the Digest Credentials and Confirm.
  04) Click Save (remember the User ID and Password and DN of the device)

ahaha	Cisco U	nified CM Ac	Iministration						Navigation Cisco Unified CM Administration
cisco	For Cisco Un	ified Communicatio	ons Solutions						admin Search Documentation About
System 👻	Call Routing •	Media Resources 🔻	Advanced Features 🔻	Device 🔻	Application •	User Management	Bulk Administration 👻	Help 🔻	
End User (	Configuration								Related Links: Back to Find List Users 🗸
Save	X Delete	Add New							
Status									
(i) Statu	is: Ready								
User Info	ormation ——								
User Statu	ıs	Enabled Local User	r						
User ID*		isrvoip1							
Password		•••••	•••••	•••••	Edit Cre	edential			
Confirm Pa	assword	•••••	•••••	•••••					
Self-Servic	ce User ID	18507904044							
PIN		•••••	•••••	•••••	Edit Cre	edential			
Confirm PI	IN	•••••	•••••	•••••					
Last name	*	isrvoip1							
Middle nan	me								
First name	e								
Display na	ame								
Title									
Directory l	URI								
Telephone	Number	18507904044							

1///

Cisco Un For Cisco Unit	ified CM Administration ied Communications Solutions		Navigation Cisco Unified CM Administration <b>Cisco Unified CM Administration</b> G admin Search Documentation About Logou
System + Call Routing +	Media Resources - Advanced Features - Devi	ce 👻 Application 👻 User Management 👻	▼ Bulk Administration ▼ Help ▼
End User Configuration			Related Links: Back to Find List Users 🔻 Go
📊 Save 🗙 Delete 🚽	Add New		
Home Number Mobile Number Pager Number Mail ID Manager User ID Department User Locale Associated PC/Site Code Digest Credentials	< None >	▼	
User Profile	Standard (Factory Default) User Profile	View Details	
User Rank*	1-Default User Rank	•	
Service Settings	ified CM IM and Presence (Configure IM and Pr ing information in presence(Requires Exchange	esence in the associated UC Service Profi Presence Gateway to be configured on C	ile) CUCM IM and Presence server)
UC Service Profile	Use System Default	View Details	

# 4.4. Adding SIP Phone in CUCM

- 01) Go to Device ---- Phone and click Add New
- 02) Select Third Party Sip Device (Basic) and click Next
- 03) Enter in a 12 digit MAC address (any dummy MAC address)
- 04) Enter the pertinent information for the SIP DEVICE settings it should mostly be configured the same as a standard phone on your system except for the following settings
  - a) in the owner user ID field select the user you created above
  - b) in the Device Security Profile field select the security profile you created above
  - c) in the Digest User field select the user you created above
- 05) Click Save.
- 06) Configure the line settings for the SIP device the line settings should match the line settings of your standard user's Cisco IP phones

There are no special attributes that we need to worry about on the line configuration.

Cisco Unified CM Administ For Cisco Unified Communications Solutio	Cisco Unified CM Administration         Navigation         Cisco Unified CM Administration           Sco         For Cisco Unified Communications Solutions         admin         Search Documentation         About					
System  Call Routing  Media Resources  Advanced Features  Device  Application  User Management  Builk Administration  Help						
Phone Configuration Related Links: Back To Find/List						
📄 Save 🗶 Delete 📄 Copy 睯 Reset 🧷 Ap	oly Config 🕂 Add New					
Status						
i Status: Ready						
Association	Phone Type					
Modify Button Items	Product Type: Third-party SIP Device (Basic)					
1 <u>Ine [1] - 18507904044 (no partition)</u>	Device Protocol: SIP					
Unassigned Associated Items	Real-time Device Status					
2 •m: Line [2] - Add a new DN	Registration: Registered with Cisco	Unified Communications Manager CUCM-Cisco.pe.orad	cle.com			
ent - ent -	IPv4 Address: 10.232.50.2	IPv4 Address: 10.232.50.2				
	Active Load ID: None					
	Download Status: None					
	Device Information					
	Device is Active					
	A Device is not trusted					
	MAC Address*	00AABB11CCFF				
	Description	ISRVoip1				
	Device Pool*	Default	View Details			
	Common Device Configuration	< None >	View Details			
	Phone Button Template*	Third-narty SIP Device (Basic)	v			

ahaha	CISCO UNITICA CM Administr	ation		Navigatio	Cisco Unified CM Administra	tion	v
cisco	For Cisco Unified Communications Solutions	5		admi	n Search Documentation	About	
System -	Call Routing • Media Resources • Advanced Fe	eatures • Device • Application • User Ma	nagement • Bulk Administration • Help •				
Phone Co	nfiguration			Related Linl	ks: Back To Find/List		v
Save	🗙 Delete 📔 Copy 睯 Reset 🧷 Appl	y Config 🕂 Add New					
		Phone Button Template*	Third-party SIP Device (Basic)	~			
		Common Phone Profile*	Standard Common Phone Profile	View Det	ails		
		Calling Search Space	< None >	~			
		AAR Calling Search Space	< None >	~			
		Media Resource Group List	< None >	¥			
		Location*	Hub_None	~			
		AAR Group	< None >	~			
		Device Mobility Mode*	Default	View Cur	rent Device Mobility Settings		
		Owner	User      Anonymous (Public/Shared Space)				
		Owner User ID*	isrvoip1	~			
		Mobility User ID	< None >	¥			
		Use Trusted Relay Point*	Default	¥			
		Always Use Prime Line*	Default	~			
		Always Use Prime Line for Voice Message*	Default	¥			
		Geolocation	< None >	¥			
		□ Ignore Presentation Indicators (interna	I calls only)				
		✓ Logged Into Hunt Group					
		Remote Device					
						]	

Cisco Unified CM Administr Cisco Unified Communications Solution	ration s	Navigation Cisco Unified CM admin Search Docum	Administration entation   About	• Go Logout
ystem - Call Routing - Media Resources - Advanced F	eatures - Device - Application -	User Management 👻 Bulk Administration 👻 Help	•	
hone Configuration		Related Links: Back To Find/	List	▼ Go
📊 Save 🗶 Delete 🗋 Copy 🎦 Reset 🥒 App	V Config Add New  Remote Number  Calling Party Transformation CS  Use Device Pool Calling Party	S [ < None > y Transformation CSS (Device Mobility Related Infor	v mation)	
	Protocol Specific Information - BLF Presence Group* MTP Preferred Originating Codec* Device Security Profile* Rerouting Calling Search Space SUBSCRIBE Calling Search Space SIP Profile* Digest User Media Termination Point Requi Unattended Port Require DTMF Reception	Standard Presence group         711ulaw         Third-party SIP Device Basic - Standard SIP Non-         < None >         < None >         Standard Sip Profile - Options Enabled ISR         isrvoip1	▼ Se ▼ ▼ ▼ Yiew Details	
	MLPP and Confidential Access MLPP Domain Confidential Access Mode < Non Confidential Access Mode < Non	Level Information e > T e > T		

# 4.5. Associating End User to Phone

- 01) Go to User Management ----- End Users and search for the sip user you created above, once you find it, click on it
- 02) Scroll down to Device Association and click on the Device Association button
- 03) Locate and select the sip device you created above
- 04) Check the checkbox next to this device and click Save Selected/Changes
- 05) Click Go next to the Back to User related link near the upper right-hand corner
- 06) Click Save one more time on the End User Configuration screen.

End User Configuration	× +				-	
← → C ▲ Not	secure   10.232.50.89/ccmadmin/userEdi	t.do?key=d464a40a-663c-1	o7a0-dad8-ca576d745f9d	đ	☆	Θ
III Apps 🥥 AvayaSystem	mMan 🔥 AvayaCM 🔄 EOM 💽 ESBC	NTT-SBC				
alada Cisco Un	ified CM Administration		Navigation	Cisco Unified CM Administra	ation	• 0
CISCO For Cisco Unif	ied Communications Solutions		admin	Search Documentation	About	Logo
ystem + Call Routing +	Media Resources + Advanced Features + De	vice 👻 Application 👻 User I	Management 👻 Bulk Admini	stration - Help -		-
nd User Configuration			Rel	ated Links: Back to Find	List Use	s V G
🗍 Save 😽 Delete 🗐	a Add New					
Manager User ID						
Department						
User Locale	< None >	•				
Associated PC/Site Code						
Digest Credentials						
Confirm Digest Credentials						
User Profile	Standard (Factory Default) User Profile	View Details				
User Rank*	1-Default User Rank	•				
Service Settings						
A Home Cluster						
Enable User for Un	ified CM IM and Presence (Configure IM and I	Presence in the associated UC	Service Profile)			
Include meet	ing information in presence/Requires Exchange	e Presence Gateway to be co	infigured on CUCM IM and I	Presence server)		
UC Service Profile	Use System Default	View Details				
		and an and a second				
Device Information						
Controlled Devices	5112000002295352133	-	Devides Association			
			THE REPORT OF THE PARTY OF THE			

With these steps, the CUCM configuration is complete.

# 5. Zoom Phone configuration.

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

### 5.1. Create a Zoom User.

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

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

	5 PRICING CONTACT SAL	FS		SCHEDULE A MEE
PERSONAL Profile	Users Pend	Add Users Add users with th You can add users their accounts wil	reir email addresses s of all types to your account. If you enter the email address of account owners, all users on II be added to this account.	
Webinars	Q. Search	Use comma to :	separate multiple email addresses.	(
Recordings	Email/Name I	User Type 🕥	Basic Licensed On-Prem ③	Туре
ADMIN	C kamlesh.vasu	Department	e.g. Product	Basic
User Management	solutionszoo	Job Title	e.g. Product Manager	Basic
Group Management	gmchugh100	Location User Group	No Group	Basic
> Room Management	priyesh.mehr			Basic
Account Management     Advanced	Zoom Rooms		Add Cancer	Basic

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

### 5.2. Add BYOC number

Navigate to Phone Systems Management > Phone Numbers > BYOC

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

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

Carrier – Choose BYOC

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

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

Click Submit.

			REQUEST A D
ZOOM SOLUTIONS - PI	LANS & PRICING CONTACT SA	Add BYOC Numbers	SCHEDULE A MEETING
PERSONAL	Assigned Una	Site v	
Profile	Add your BYOC phone	Carrier BYOC ~	
Webinars	Zoom, you can assign	Numbers 7814437387	
Phone Recordings	Q. Search by Numbe		SIP Group (All)
Settings	Number ‡	SIP Group (Optional) Choose a routing path for calls to/from the numbers	Submission Date 💲
ADMIN	(781) 443-7387		Nov 22, 2019, 2:27 F
Dashboard	(781) 313-1033	I acknowledge that by checking the box, I attest that the phone numbers to be imported belong to me or my organization	Aug 3, 2020, 1:12 PM
<ul> <li>User Management</li> </ul>	(781) 313-1034		Aug 13, 2020, 3:13 F
Room Management     Phone System Management	(781) 443-7284	Cancel Submit	Oct 28, 2019, 4:36 P
Users & Rooms	(781) 443-7241	ION MAINDEN ONNEG SUILES DI OC M	Oct 28, 2019, 4:36 P

# 5.3. Assign the BYOC number to a User

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

ZOOTT SOLUTIONS -	PLANS & PRICING	CONTACT SALES					SCHEDULE A MEETING JOIN A ME	ETING HOST A MEETING +
PERSONAL Profile	Assi	gned Unassigned	Ported BYOC					
Meetings								
Webinars	Adk	Export						
Phone	Qs	earth			Number Type (All)	2	Status (Alt)	Site (All)
Recordings	Move	Site Delete						
Settings		Number \$	Area	Number Type	Capability	Status	Site	<b>1</b> 2
ADMIN		(781) 349-6963	Norwood, Massachusetts, United States	Toll Number	Incoming & Outgoing	Normal	Main Site	Delete Assem to
> User Management		(781) 443-7387 💽	United States	Toll Number	Incoming & Outgoing	Normal	Main Site	Delete Assign to
> Room Management		(781) 313-1034	United States	Toll Number	Incoming & Outgoing	Normal	Main Site	Delete: Assign to

ZOOM SOLUTIONS - PL	ANS & PRICING CONTACT SALES	2			SCHEDU	ILE A MEETING JOIN A MEET
PERSONAL Profile Meetings	Assigned Unassigned	Assign Number	781) 443-7387 (BYOC)			
Webinars Phone	Add Export	Assign to	User Enter Ext. or name		V Status (All)	
Recordings Settings	Move Site Delete	-		Cancel OK	tus Tooli is maxima	Site
ADMIN Dashboard	(781) 349-6963	Norwood. Massachusetts, United States	Toll Number	Incoming & Outgoing	Normal	Main Site
> User Management	(781) 443-7387 E	United States	Toll Number	Incoming & Outgoing	Normal	Main Site
Room Management     Denne System Management	(781) 313-1034 🗉	United States	Toll Number	Incoming & Outgoing	Normal	Main Site
Users & Rooms	(781) 443-7284 🕑	United States	Toll Number	Incoming & Outgoing	Normal	Main Site

2///8

# 6. Infrastructure Requirements.

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

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

# 7. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Cisco Call Manager (Cisco CUCM) and Zoom BYOC.

## 7.1. Validated Oracle SBC version

Oracle conducted tests with Oracle SBC 9.0 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 (Starting from SBC 9.0 version)
- AP 4900 (Starting from SBC 9.0 version)
- VME

# 8. New SBC configuration

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

#### 8.1. Establishing a serial connection to the SBC

Connect one end of a straight-through Ethernet cable to the front console port (which is active by default) on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB-9 adapter) to the DB-9 port on a workstation, running a terminal emulator application such as Putty. Start the terminal emulation application using the following settings:

- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

Please note that the above console connection procedure does not apply to VME or cloud deployments of SBC and can be applied only to hardware platforms.

Power on the SBC and confirm that you see the following output from the boot-up sequence

Starting	tLemd
Starting	tServiceHealth
Starting	tCollect
Starting	tAtcpd
Starting	tAsctpd
Starting	tMbcd
Starting	tCommMonitord
Starting	tFped
Starting	tAlgd
Starting	tRadd
Starting	tEbmd
Starting	tSipd
Starting	tH323d
Starting	tbfdd
Starting	tIPTd
Starting	tSecured
Starting	tAuthd
Starting	tCertd
Starting	tIked
Starting	tTscfd
Starting	tFcgid
Starting	tauditd
Starting	tauditpusher
Starting	tSnmpd
Starting	tIFMIBd
Start pla	atform alarm
Starting	display manager
[nitializ	zing /opt/ Cleaner
Starting	tLogCleaner task
Bringing	up shell
Starting	acliMgr
bassword	secure mode is enabled
Admin Sec	curity is disabled
assword:	

Enter the default password to log in to the SBC. Note that the default SBC password is "acme" and the default super user password is "packet".

Both passwords have to be changed according to the rules shown below.



Now set the management IP of the SBC by setting the IP address in bootparam.

To access bootparam. Go to Configure terminal->bootparam.

NN4600-139(configure)# bootparam			
<pre>'.' = clear field; '-'</pre>	go to previous field; q = quit		
Boot File	/boot/nnSCZ900p3.bz		
IP Address	10.138.194.139		
VLAN	0		
Netmask	255.255.255.192		
Gateway	10.138.194.129		
IPv6 Address			
IPv6 Gateway			
Host IP			
FTP username	vxftp		
FTP password	****		
Flags			
Target Name	NN4600-139		
Console Device	COM1		
Console Baudrate	115200		
Other			
NOTE: These changed para	eters will not go into effect until re	boot.	
Also, be aware that some	poot parameters may also be changed th	rough	
PHY and Network Interfac	Configurations.		

Note: There is no management IP configured by default.

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

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

NN3900-101# setup product WARNING: Alteration of product alone or in conjunction with entitlement changes will not be complete until system reboot Last Modified 2020-07-21 04:51:24 1 : Product : Enterprise Session Border Controller Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]:

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

Save the changes and reboot the SBC.

Entitlements for Enterprise Session Bord	der Controller
Last Modified: Never	
1 : Session Capacity	
2 : Advanced	
3 : Admin Security	
4 : Data Integrity (FIPS 140-2)	
5 : Transcode Codec AMR Capacity	
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
11: Humboode bouce bills oupdotey	
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 functions. Once saved, security cannot b resetting the system back to factory def ************************************	**************************************
Enter 1 - 11 to modify, d' to display,	's' to save, 'q' to exit. [s]: 5
Transcode Codec AMR Capacity (0-102375	5) : 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 (0-1023)	75) : 50
Enter 1 - 11 to modify, d' to display,	's' to save, 'q' to exit. [s]: 11
Transcode Codec SILK Capacity (0-1023)	75) <b>:</b> 50

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

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

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

NN3900-101(http-server)# show	
http-server	
name	webServerInstance
state	enabled
realm	
ip-address	
http-state	enabled
http-port	80
https-state	disabled
https-port	443
http-interface-list	GUI
http-file-upload-size	0
tls-profile	
auth-profile	
last-modified-by	0
last-modified-date	2020-10-06 00:28:26
NN3900-101(http-server)#	
NN3900-101(http-server)#	

# 8.2. Configure SBC using Web GUI

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

The Web GUI can be accessed through the url <u>http://<SBC\_MGMT\_IP</u>>.

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

The username and password is the same as that of CLI.

lighest task CPU usage	•••	Current memory usage		Historical memory usage	
100 80 60 40 20 0 157060 10806 1080600 1080600 1080600 1080600 1080600 10	<ul> <li>sipd03</li> <li>ISSH-1</li> <li>Console</li> <li>actod01</li> <li>xserv</li> </ul>	20.0%	Allocated Free	3,235M 3,235M 3,233M 3,233M 3,233M 3,233M 0,000	<ul> <li>Memory usage</li> <li>Trend (rate:4.04</li> </ul>

Go to Configuration as shown below, to configure the SBC

ORACL	E Enterprise S	ession Border Controller				Û 🗸	admin 🔻		
NN4600-139 10.1	38.194.139 SCZ9.0	.0 Patch 3 (Build 290)	Dashboard	Configuration	Monitor and Trace	Widgets	System		
Configuration	View Configuration	Q			Discard	😧 Verify	🖹 Save		
media-manager	•	Configuration Objects							
security	•								
session-router	•	Name	Description						
		access-control	Configure a static or dynamic access control list				^		
system	•	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				~		
Show All		Displaying 1 - 10 of 40							

Kindly refer to the GUI User Guide given below for more information.

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/9.0.0/webgui/web-gui-guide.pdf

The expert mode is used for configuration.

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

# 8.3. Configure system-config

Go to system->system-config

	e Session Border Controller					Û 🔺	admin 🔻
NN4600-139 10.138.194.139 SCZ9	9.0.0 Patch 3 (Build 290)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration View Configuration	ion Q				Discard	😧 Verify	🖹 Sav
host-route	Modify System Config					Show Co	nfiguration
http-client							~
http-server	Hostname	OracleSBC					- 1
network-interface	Description						
ntp-config							
phy-interface							
redundancy-config	Location						
snmp-community	Mib System Contact						
spl-config	Mib System Name						
system-config	Mib System Location						
trap-receiver	Acp TLS Profile	T					
Show All	ОК	Delete					

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

	se Session Border Controller						Û 🔺	admin 👻
NN4600-139 10.138.194.139 SCZ	29.0.0 Patch 3 (Build 290)		C	Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration View Configura	tion Q					Discard	😧 Verify	🖹 Save
host-route	Modify System Config						Show Cor	figuration
http-client								^
http-server	Options							
network-interface	Call Trace							
ntp-config	Default Catanan	enable						
phy-interface	Default Gateway	10.138.194.129						
redundancy-config	Restart	✓ enable						
spmp-community	Telnet Timeout	0	(Range: 065535)					- 1
	Console Timeout	0	( Range: 065535 )					
spi-config	HTTP Timeout	5	( Range: 020 )					
system-config	Alarm Threshold							_
trap-receiver								>
Show All	ОК	Delete						

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

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/9.0.0/releasenotes/esbc-release-notes.pdf The above step is needed only if any transcoding is used in the configuration. If there is no transcoding involved, then the above step is not needed.

# 8.4. Configure Physical Interface values

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

Please configure M00 for Zoom side and M01 for Cisco side.

Zoom BYOC (M00)	Cisco side (M01)
0	1
0	0
Media	Media
	Zoom BYOC (M00) 0 0 Media

Please configure M00 interface as below.

ORACL	ORACLE Enterprise Session Border Controller										
NN4600-139 10.1	38.194.139	SCZ9.0	.0 Patch 3 (Build 290)				Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Con	figuration	Q						Discard	😧 Verify	🖹 Save
media-manager	•	^	Modify Phy Interface								
security	►										^
session-router	►		Name	M00							
system	Ŧ		Operation Type	Media	•						
fraud-protection			Port	0		( Range: 05 )					
			Slot	0		(Range: 0)					
host-route			Virtual Mac								
http-client			Admin State	anable.							- 1
http-server			Auto Nogotistion	V enable							
network-interface	2		Auto negotiation	🗸 enable							
netton interact	-		Duplex Mode	FULL							
ntp-config			Speed	100	w						
phy-interface		~									~
Show All			ОК	Back							

Please configure M01 interface as below

ORACL	E Enterprise	Session Border Controller							admin 🔻
NN4600-139 10.	138.194.139 SCZ9.	0.0 Patch 3 (Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	n Q					Discard	😧 Verify	B Save
media-manager	*	Modify Phy Interface							
security									^
session-router	<b>→</b>	Name	M01						
system	Ŧ	Operation Type	Media	7					
fraud-protection		Port	1	(Range: 05)					
		Slot	0	(Range: 0)					
nost-route		Virtual Mac							
http-client		Admin State	🗸 enable						
http-server		Auto Negotiation							
network-interfac	e	nato negotiation	enable						
		Duplex Mode	FULL	7					
ntp-config		Speed	100	r					
phy-interface	~								×
Show All		ОК	Back						

# 8.5. Configure Network Interface values

To configure network-interface, go to system->Network-Interface. Configure interface

The table below lists the parameters, to be configured for both the interfaces.

Parameter Name	Zoom BYOC Network Interface(M00)	Cisco side Network Interface(M01)
Name	M00	M01
Host Name		
IP Address	155.212.214.120	10.232.50.79
Net Mask	255.255.255.0	255.255.255.0
Gateway	155.212.214.65	10.232.50.1

Please configure network interface M00 as below

ORACL	E Enterprise	Session Border Controller							admin 🔻
NN4600-139 10.1	38.194.139 SCZ9.	0.0 Patch 3 (Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuratio	n Q					Discard	😧 Verify	🖹 Save
media-manager	*	Modify Network Interface							
security	•								^
session-router		Name	M00	7					
system	Ŧ	Sub Port Id	0	(Range: 04095)					
fraud-protection		Description							
host-route									
http-client									
http-server		Hostname	155.212.214.120						
network-interfac	2	IP Address	155.212.214.120						
ntp-config		Pri Utility Addr							
ing coming		Sec Utility Addr							~
phy-interface	*	OK B	Bark						
Show All		UK D	duk .						

11/1/2///20

Similarly, configure network interface M01 as below

ORACL	E Enterprise S	Gession Border Controller								admin 🔻
NN4600-139 10.1	38.194.139 SCZ9.0	1.0 Patch 3 (Build 290)				Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	Q						Discard	😧 Verify	🖹 Save
media-manager	A	Modify Network Interface								
security	•									^
session-router	•	Name	M01	•						- 1
system	Ŧ	Sub Port Id	0		(Range: 04095)					
fraud-protection		Description								
host-route										
http-client										
http-server	- 1	Hostname	10.232.50.79							
network-interface	2	IP Address	10.232.50.79							
ntp-config		Pri Utility Addr								
nhu interface		Sec Utility Addr								~
Show All	<b>v</b>	OK	Back							

# 8.6. Enable media manager

Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

In addition to the above config, please set the max and min untrusted signaling values to 1. Go to Media-Manager->Media-Manager

ORACL	ORACLE Enterprise Session Border Controller								
NN4600-139 10.1	38.194.139 SCZ9.0	.0 Patch 3 (Build 290)		Dashboard	Configuration	Monitor and Trace	Widgets	Syster	
Configuration	View Configuration	Q				Discard	Ø Verify	Bs	
media-manager codec-policy	× ^	Modify Media Mana	ager						
media-manager		State	v enable						
media-policy		Flow Time Limit	86400	(Range: 04294967295)					
realm-config		Initial Guard Timer	300	(Range: 04294967295)					
steering-pool	- 11	TCP Flow Time Limit	300	(Range: 04294967295)					
security	÷	TCP Initial Guard Timer	300	(Range: 04294967295)					
session-router	<b>.</b>	TCP Subsq Guard Timer	300	(Range: 04294967295)					
system	Ŧ	Hnt Rtcp	enable						
fraud-protection		Algd Log Level	NOTICE 💌						
host-route	~	Mbcd Log Level	NOTICE						
Show All			OK Delete						

ORACL	ORACLE Enterprise Session Border Controller							
NN4600-139 10.1	138.194.139 SCZ9.0	0.0 Patch 3 (Build 290)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	n Q				Discard	😧 Verify	B Save
media-manager	*	Modify Media Manager						
codec-policy			enaple					^
media-manager		Max Signaling Bandwidth	100000	(Range: 7100010000000)				
media-policy		Max Untrusted Signaling	1	( Range: 0100				
realm_config		Min Untrusted Signaling	1	(Range: 0100)				
realiti-coning		Dos Guard Window	5	(Range: 130)				- 1
steering-pool		Untrusted Minor Threshold	0	(Range: 0100)				
security	•	Untrusted Major Threshold	0	(Range: 0100)				
session-router	•	Untrusted Critical Threshold	0	(Range: 0100)				
system	<b>.</b>	Trusted Minor Threshold	0	(Range: 0100)				
found another them		Trusted Major Threshold	0	(Range: 0100)				
traud-protection		Trusted Critical Threshold	0	(Range: 0100)				
host-route	~							·
Show All		ОК	Delete					

# 8.7. Configure Realms

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

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

Config Parameter	Zoom Side	Cisco Side
Identifier	ZoomRealm	CUCMRealm
Network Interface	M00	M01
Mm in realm		
FQDN		
Media Sec policy	sdespolicy	RTP
Access Control Trust Level	High	High

In the below case, Realm name is given as ZoomRealm for Zoom Side Please set the Access Control Trust Level as high for this realm

ORACL	ORACLE Enterprise Session Border Controller								
NN4600-139 10.1	38.194.139 SCZ9.0.0 I	Patch 3 (Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	Q					Discard	😧 Verify	Sav
media-manager	<b>T</b>	Add Realm Config							
codec-policy									^
media-manager		ldentifier	ZoomRealm						
media-policy		Description							
realm-config									
steering-pool									
security	+	Addr Prefix	0.0.0.0						
session-router	•	Network Interfaces	M00:0.4 ×						
system	v	Media Realm List							
fraud-protection		Mm In Realm	✓ enable						
host-route		Mm In Network	✓ enable						
http-client	~	Mm Same Ip	✓ enable						~
Show All	$\supset$	ОК	Back						

ORACL	E Enterprise Se	ssion Border Controller							admin 🔻
NN4600-139 10.1	38.194.139 SCZ9.0.0	Patch 3 (Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	Q					Discard	😧 Verify	E Save
media-manager	v ^	Add Realm Config							
codec-policy		In Manipulationid		Ψ.					^
media-manager		Out Manipulationid							
media-policy		Average Rate Limit	0		(Range: 04294967295)				
realm-config		Access Control Trust Level	high						
steering-pool		Invalid Signal Threshold	0		(Range: 04294967295)				
security	<b>→</b>	Maximum Signal Threshold	0		(Range: 04294967295)				
session-router	•	Untrusted Signal Threshold	0		(Range: 04294967295)				
system	v	Nat Trust Threshold	0		(Range: 065535)				
fraud-protection		Max Endpoints Per Nat	0		(Range: 065535)				
naud-protection		Nat Invalid Message Threshold	0		(Range: 065535)				
host-route		Wait Time For Invalid Register	0		( Range: 0,4300 )				
http-client		Deny Period	30		(Range: 04294967295)				~
Show All	<b>`</b>	ОК	Back						

2///8

Similarly, Realm name is given as CUCMRealm for Cisco side. Please set the Access Control Trust Level as high for this realm too.

ORACL	E Enterprise Ses	ssion Border Controller							admin 🔻
NN4600-139 10.	138.194.139 SCZ9.0.0	Patch 3 (Build 290)		I	Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	Q					Discard	😧 Verify	Save
media-manager	<b>v</b>	Add Realm Config							
codec-policy									^
media-manager		Identifier	CUCMRealm						
media-policy		Description							
realm-config									
steering-pool									
security	<b>→</b>	Addr Prefix	0.0.0.0						
session-router	•	Network Interfaces	M01:0.4 🗶						
system	Ŧ	Media Realm List							
fraud-protection		Mm In Realm	✓ enable						
host-route		Mm In Network	✓ enable						
http-client	*	Mm Same Ip	✓ enable						~
Show All		OK	Back						

ORACL	E Enterprise Se	ssion Border Controller							admin 🔻
NN4600-139 10.1	38.194.139 SCZ9.0.0	Patch 3 (Build 290)			Dashbo	ard Configura	tion Monitor and Trace	Widgets	System
Configuration	View Configuration	Q					Discard	😧 Verify	B Save
media-manager	*	Add Realm Config							
codec-policy		In Manipulationid							^
media-manager		Out Manipulationid							
media-policy		Average Rate Limit	0		(Range: 04294967295)				
realm-config		Access Control Trust Level	high	Ŧ					
steering-pool		Invalid Signal Threshold	0		(Range: 04294967295)				
security	•	Maximum Signal Threshold	0		(Range: 04294967295)				
session-router	•	Untrusted Signal Threshold	0		(Range: 04294967295)				
system		Nat Trust Threshold	0		(Range: 065535)				
fraud protection		Max Endpoints Per Nat	0		(Range: 065535)				
naud-protection		Nat Invalid Message Threshold	0		( Range: 065535 )				
host-route		Wait Time For Invalid Register	0		( Range: 0,4300 )				
http-client		Deny Period	30		(Range: 04294967295)				~
Show All	~	ОК	Back						

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

https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/security/security-guide.pdf

#### 8.8. Enable sip-config

SIP config enables SIP handling in the SBC. Make sure the home realm-id, registrar-domain and registrar-host are configured.

Also add the options to the sip-config as shown below. To configure sip-config, Go to Session-Router->sip-config and in options, add the below

- add max-udp-length =0
- inmanip-before-validate

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

ORACLE Enterprise Set	ssion Border Controller						admin 🔻
NN4600-139 10.138.194.139 SCZ9.0.0	) Patch 3 (Build 290)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration View Configuration	Q				Discard	😧 Verify	🖹 Save
session-agent	Modify SIP Config						
session-group		ISU	( канде: 04544401545 )				^
session-recording-group	Session Max Life Limit	0					
session-recording-server	Enforcement Profile	T					
session-translation	Red Max Trans	10000	(Range: 050000)				
sip-config	Options	inmanip-before-validate 🗙					
sip-feature		max-udp-length=0 🗙					
sip-interface	SPL Options						
sip-manipulation	SIP Message Len	4096	(Range: 065535)				
sip-monitoring	Enum Sag Match	enable					
	Extra Method Stats	✓ enable					~
translation-rules							
Show All	OK D	elete					

## 8.9. Configuring a certificate for SBC

This section describes how to configure the SBC for both TLS and SRTP communication with Zoom

Zoom allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by one of the trusted Certificate Authorities.

The process includes the following steps:

- 1) Create a certificate-record "Certificate-record" are configuration elements on Oracle SBC which captures information for a TLS certificate such as common-name, key-size, key-usage etc.
- SBC 1 certificate-record assigned to SBC
- Root 1 certificate-record for root cert
- 2) Deploy the SBC and Root certificates on the SBC

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

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

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

# Step 1 – Creating the certificate record

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

2///

ORACL	ORACLE Enterprise Session Border Controller admin								
NN4600-139 10.1	138.194.139 SCZ	9.0.0 Patch 3 (Build 290)		Dashboa	rd Configuration	Monitor and Trace	Widgets	Syster	
Configuration	View Configurat	ion Q				Discard	😧 Verify	E s	
media-manager	►	Modify Certificate Record							
security	•								
authentication-p	rofile	Name	DigiCertRoot						
certificate-record	I.	Country	US						
tls-global		State	MA						
tls-profile		Locality	Burlington						
session-router	►	Organization	Engineering						
system	►	Unit							
		Common Name	DigiCert Global Root CA						
		Key Size	2048 💌						
		Alternate Name							
Show All		OK	Back						

ORACL	E Enterprise	Session Border Controller								admin 🔻
NN4600-139 10.13	8.194.139 SCZ9	0.0 Patch 3 (Build 290)			Dash	nboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	n Q						Discard	😧 Verify	E Save
media-manager	Þ	Modify Certificate Record								
security	•	Alternate Name								^
authentication-pro	ofile	Trusted	✓ enable							
certificate-record		Key Usage List	digitalSignature 🗙							
tls-global			keyEncipherment 🗙							
tls-profile		Extended Key Usage List	serverAuth 🗙							- 1
session-router	•	Key Algor	rsa	Ŧ						
system	•	Digest Algor	sha256	Ŧ						
		Ecdsa Key Size	p256	v						
		Cert Status Profile List								
										v
Show All		ОК	Back							

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

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

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

Certificate Issuer Organization	Common Name or Certificate Name
Buypass AS-983163327	Buypass Class 2 Root CA
Buypass AS-983163327	Buypass Class 3 Root CA
Baltimore	Baltimore CyberTrust Root
Cybertrust, Inc	Cybertrust Global Root
DigiCert Inc	DigiCert Assured ID Root CA
DigiCert Inc	DigiCert Assured ID Root G2
DigiCert Inc	DigiCert Assured ID Root G3
DigiCert Inc	DigiCert Global Root CA
DigiCert Inc	DigiCert Global Root G2
DigiCert Inc	DigiCert Global Root G3
DigiCert Inc	DigiCert High Assurance EV Root CA
DigiCert Inc	DigiCert Trusted Root G4

GeoTrust Inc.	GeoTrust Global CA
GeoTrust Inc.	GeoTrust Primary Certification Authority
GeoTrust Inc.	GeoTrust Primary Certification Authority - G2
GeoTrust Inc.	GeoTrust Primary Certification Authority - G3
GeoTrust Inc.	GeoTrust Universal CA
GeoTrust Inc.	GeoTrust Universal CA 2
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G6
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G6
Thawte, Inc.	Thawte Primary Root CA
Thawte, Inc.	Thawte Primary Root CA - G2
Thawte, Inc.	Thawte Primary Root CA - G3
VeriSign, Inc.	VeriSign Class 1 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 2 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G4
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign, Inc.	VeriSign Universal Root Certification Authority
AffirmTrust	AffirmTrust Commercial
AffirmTrust	AffirmTrust Networking
AffirmTrust	AffirmTrust Premium
AffirmTrust	AffirmTrust Premium ECC
Entrust, Inc.	Entrust Root Certification Authority
Entrust, Inc.	Entrust Root Certification Authority - EC1
Entrust, Inc.	Entrust Root Certification Authority - G2
Entrust, Inc.	Entrust Root Certification Authority - G4
Entrust.net	Entrust.net Certification Authority (2048)
GlobalSign	GlobalSign

GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign nv-sa	GlobalSign Root CA
The GoDaddy Group, Inc.	Go Daddy Class 2 CA
GoDaddy.com, Inc.	Go Daddy Root Certificate Authority - G2
Starfield Technologies, Inc.	Starfield Class 2 CA
Starfield Technologies, Inc.	Starfield Root Certificate Authority - G2
QuoVadis Limited	QuoVadis Root CA 1 G3
QuoVadis Limited	QuoVadis Root CA 2
QuoVadis Limited	QuoVadis Root CA 2 G3
QuoVadis Limited	QuoVadis Root CA 3
QuoVadis Limited	QuoVadis Root CA 3 G3
QuoVadis Limited	QuoVadis Root Certification Authority
Comodo CA Limited	AAA Certificate Services
AddTrust AB	AddTrust Class 1 CA Root
AddTrust AB	AddTrust External CA Root
COMODO CA Limited	COMODO Certification Authority
COMODO CA Limited	COMODO ECC Certification Authority
COMODO CA Limited	COMODO RSA Certification Authority
The USERTRUST Network	USERTrust ECC Certification Authority
The USERTRUST Network	USERTrust RSA Certification Authority
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 2
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 3

## Step 2 – Generating a certificate signing request

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

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

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

Copy the following information and send to a CA authority	
BEGIN CERTIFICATE REQUEST MIICvTCCAaUCAQAwRTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMR MwEQYDVQQH EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzCCASIwDQY	
JKoZIhvcN AQEBBQADggEPADCCAQoCggEBALzMG9rclE8r+f2nK1zIMcTJaLVdh+1WR +vWmKnn (pwtfp2cKsLlvEKX0bAlZU5SA5EpdHfXLC9GZiMzZdK_I0SLC0g6GkcEBKtvbBlf	
hU JS0vaSc3UMlc+jqy9G+2Fsd44mY/KMxPFQnMXECgT7RAyhKLj0zoxqi6dQ5zb yHg	
HGJ2dAPkXqmwBwc2zx101bawk9W/sk2o2gKWI5B6rOw2ICblVyekn7SUEPB C3IPM 43NP43mvNQWbFffc3oCAzdqgWxvDzhQbvhu76nGJPnCGqxJoHR7dTD6GX	
gNFOWdLWEh00RCktAltTNeV4KdcGeYrYZlkvJZlHHpT/7mkCAwEAAaAzMD EGCSqG	•

• Also, note that a save/activate is required

### Step 3 – Deploy SBC & root certificates

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

Format:	and and	
offiliat.	try-all	<b>⊻</b> ⊍
Import method:	● File ○ Paste	
Certificate file:		Browse
	Import	

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

- DigiCertIntermediate
- DigiCertGlobalRootCA
- DigiCertGlobalRootG2
- DigiCertGlobalRootG3

#### At this stage all the required certificates have been imported to the SBC for Zoom.

#### 8.10. TLS-Profile

A TLS profile configuration on the SBC allows for specific certificates to be assigned. Go to security-> TLS-profile config element and configure the tls-profile as shown below The below is the TLS profile configured for Zoom side.

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

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

ORACL	E Enterprise	Session Border Controller						admin 🔻
NN4600-139 10.1	138.194.139 SCZ9	2.0.0 Patch 3 (Build 290)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	on Q				Discard	😧 Verify	🖹 Sat
media-manager	•	Modify TLS Profile						
security authentication-p	▼ rofile	Name	TLSTeams					Í
certificate-record		End Entity Certificate	Enterprise 💌					
tls-global		Trusted Ca Certificates	DigiCertInter 🗙					
tls-profile			DigiCertRoot ×					
session-router	•		GoDaddyInter 🗙					
system	•		GoDaddyRoot 🗙					
		Cipher List	DEFAULT X					
		Verify Depth	10	(Range: 010)				
		Mutual Authonticato	_					
Show All		ОК	Back					

## 8.11. Configure SIP Interfaces

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

- Tls-profile needs to match the name of the tls-profile previously created
- Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from the particular Session agents added to the SBC.

ORACL	E Enterprise S	ession Bo	order Co	ntroller								Û 🔺	admin 🔻
NN4600-139 10.1	138.194.139 SCZ9.0.	.0 Patch 3 (	(Build 290	))					Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	Q									Discard	😧 Verify	🖹 Sav
session-agent	^	Modify	/ SIP In	iterface								Show Co	nfiguration
session-group		State			🗸 enab	ole							^
session-recording	g-group	Realm ID			ZoomRe	ealm	v						
session-recording	g-server	Descripti	on										
session-translation	on												
sip-config	- 11												
sip-feature		SIP Ports											
sip-interface		Ľ\$	/ [	Ē									
sip-manipulation	n	Action	Select	Address		Port		Transport Protocol	TLS Profile	Allow Anor	nymous Mult	i Home Addrs	
sip-monitoring		:		155.212.214.120		5061		TLS	TLSTeams	agents-only	Į.		
Show All	~			ОК	Back								

2///8

Similarly, Please Configure sip-interface for the Cisco side as below:

ORACL	ORACLE Enterprise Session Border Controller										admin 🔻	
NN4600-139 10.	138.194.139 SCZ9.0.0	) Patch 3 (Buil	d 290)					Dashboa	rd Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	Q								Discard	😧 Verify	🖹 Save
session-agent	^	Modify	/ SIP Ir	nterface							Show Co	nfiguration
session-group		State			anabla							^
session-recordin	g-group	Realm ID		✓	ICMRealm	v						
session-recordin	g-server	Descripti	on									
session-translati	on											
sip-config												
sip-feature	- 1	CID Dorto										
sip-interface			/ [									
sip-manipulation	1	Action	Select	Address	Port		Transport Protocol	TLS Profile	Allow Anonymous	Multi Home	Addrs	
sip-monitoring		:		10.232.50.79	5060		UDP		agents-only			
translation-rules		:		10.232.50.79	5060		TCP		agents-only			
system	> v											~
Show All				OK Back	]							

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

## 8.12. Configure session-agent

Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

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

- hostname and IP address as "162.12.233.60"
- port 5061
- realm-id needs to match the realm created for Zoom
- transport set to "StaticTLS"
- ping-method –OPTIONS message
- ping-interval to 30 secs

ORACL	E Enter	prise Session Border Controller						Û 🔺	admin 🔻
NN4600-139 10.1	38.194.139	SCZ9.0.0 Patch 3 (Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Config	guration Q					Discard	😧 Verify	🖹 Save
media-manager	•	Modify Session Ag	ent					Show Co	nfiguration
security	- <b>- -</b>								^
session-router	Ŧ	Hostname	162.12.233.60						
access-control		IP Address	162.12.233.60						
account-config		Port	5061		(Range: 0,102565535)				
filter.config	- 1	State	🗹 enable						
Idan-config		App Protocol	SIP	Ŧ					
inter county		Арр Туре							
local-policy		Transport Mothod							
local-routing-con	fig	Tansport Method	StaticTLS						
	Ŭ	Realm ID	ZoomRealm						
media-profile		Egress Realm ID							
session-agent				Y					~
Show All			OK Back						

Similarly, configure the session-agents for the Cisco Side as below:

- Host name to FQDN of CUCM which is "CUCM-Cisco.pe.oracle.com" in our example. We can also give Cisco CUCM IP address if there is no host name configured.
- The same FQDN value should be configured in Cisco CUCM under System ---Enterprise Parameter ----Cluster FQDN.

ORACLE Enterprise Se	ession Border Controller					Û 🗸	admin 🔻
NN4600-139 10.138.194.139 SCZ9.0.0	0 Patch 3 (Build 290)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration View Configuration	Q				Discard	😧 Verify	🖹 Save
account-config	Modify Session Agent					Show Cor	nfiguration
filter-config	Hostname	CUCM-Cisco.pe.oracle.com					^
ldap-config	IP Address	10.232.50.89					
local-policy	Port	5060	(Range: 0,102565535)				
local-routing-config	State	✓ enable					
media-profile	App Protocol	SIP	•				
session-agent	Арр Туре		•				
session-group	Transport Method	UDP+TCP	•				
session-recording-group	Realm ID	CUCMRealm	•				
session-recording-server	Egress Realm ID		•				~
Show All	ОКВ	ack					

← → C A Nct secure   10.232.50.89/ccm adm	nin/serviceParamEd t.do?service=11&showall=false	e 🛱	Θ:
Cisco Unified CM Administrat	tion <sup>ns</sup>	Navigation Cisco Unifed CM Administration admin Search Docurrentation About	• Go Logout
System ▼ Call Roucing ▼ Media Resources ▼ Advanced Featur	res • Device • Application • User Management •	Bulk Administration 👻 Help 👻	
nterprise Parameters Configuration			
🔜 Save 🤣 Set to Default   🍟 Reset 🥖 Apply Config			
Syncing Mode for Enterprise Groups *	Differential Sync	▼ Differential Sync	-
Service Manager TCP ports parameters			
Service Manager TCP Server communication port number	8883	8888	
Service Manager TCP C ient communication port number	8889	8889	
CRS Application Parameters			
Auto Attendant Installed.*	false		
PCC Express Installed	Talse		
Clusterwide Domain Configuration			
Organization Top Level Domain	pe.oracle.com		
Cluster Fully Qualified Domain Name	CUCM-Cisco.pe.oracle.com		
Denial-of-Service Protection			
Denial-of-Service Protection *	True	▼ True	
TLS Handshake Timer			
TLS Handshake Timer *	60	60	
TLS Resumption Timer			
TLS Resumption Timer *	360)	3600	

# 8.13. Configure local-policy

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

1///

To fould the calls from Cisco side to 20011 side, use the below local $-policy$
---

ORACLE Enterprise	Session Border Controller					Û 🔺	admin 🔻
NN4600-139 10.138.194.139 SCZ9.	0.0 Patch 3 (Build 290)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration View Configuratio	n Q				Discard	😧 Verify	🖹 Save
account-config	Modify Local Policy						
filter-config	From Address	*x					^
ldap-config	To Address						
local-policy		* X					
local-routing-config	Source Realm	CUCMRealm 🗙					
media-profile	Description						
session-agent							
session-group							
session-recording-group	State	✓ enable					
session-recording-server	Policy Priority	none 🔻					~
Show All	ОК	Back					

	Session Bo	order Co	ntroller								Û 🗕	admin 🔻
NN4600-139 10.138.194.139 SCZ9	0.0.0 Patch 3 (	(Build 29(	))					Dashboard	Configuration	Monitor and Tra	ce Widgets	System
Configuration View Configuration	on Q									Disca	ard 😧 Verify	🖹 Save
account-config	Modify	/ Local	Policy									
filter-config												^
ldap-config												
local-policy	State			🗸 enable								- 1
local-routing-config	Policy Pri	iority		none		W						
media-profile	Policy At	tributes										
session-agent	D:	/ [										
session-group	Action	Select	Next Hop	Realm	Action	Terminate	Cost	State	App Protoco	ol Lookup	Next Key	Auth
session-recording-group	:		162.12.233.60	ZoomRealm	replace-uri	disabled	0	enabled		single		
session-recording-server												v
Show All			ОК	Back								

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

ORACL	E Enterp	rise Session Border Control	ler					admin 🔻
NN4600-139 10.1	38.194.139 S	CZ9.0.0 Patch 3 (Build 290)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configu	uration Q				Discard	😧 Verify	🖹 Save
media-manager	A	Modify Local Pol	icy					
security	•							^
session-router	Ŧ	From Address	* X					
access-control		To Address	* X					
account-config		Source Realm	ZoomRealm 🗙					
filter-config		Description						
Idap-config								
local-policy								
local-routing-con	fig	State	anakia					
media-profile		Policy Priority	enable					
session-agent	~	roncy money	none 💌					~
Show All			OK Back					

1111111

2///0

ORACL	E En	terprise	Session Bo	rder Co	ntroller								Û 🔺	admin	
NN4600-139 10.1	138.194.13	9 SCZ9.	.0.0 Patch 3 (	Build 29(	))				Dashboard	Configuration	Monitor and	Trace	Widgets	System	n
Configuration	View Co	onfiguratio	n Q								[	Discard	😧 Verify	🖪 s	ave
media-manager	•	^	Modify	/ Local	Policy										
security	►														^
session-router															
access-control															
account-config			State			🖌 enable									
filter-config		11	Policy Pri	ority		none	v								
ldap-config			Policy Att	ributes											
local-policy			D;	1	- II										
local routing cor	ofic		Action	Select	Next Hop	Realm	Action	Terminate Re	Cost	State	App Proto	Lookup	Ne	Aut	
iocal-routing-cor	шg		:		CUCM-Cisco.pe.orac	:l CUCMRealm	replace-uri	disabled	0	enabled		single			
media-profile															
session-agent		~													~
Show All					OK Bac	k									

# 8.14. Configure steering-pool

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

Cisco side steering pool.

ORACL	E Enterprise	Session Border Controller							admin 👻
NN4600-139 10.1	38.194.139 SCZ9.	0.0 Patch 3 (Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuratio	n Q					Discard	😧 Verify	B Save
media-manager	Ŧ	Modify Steering Pool							
codec-policy media-manager		IP Address	10.232.50.79						
media-policy		Start Port	25000	(Range: 0,165535)					
realm-config		End Port	29999	(Range: 0,165535)					
steering-pool		Realm ID	CUCMRealm	v					
security	•	Network Interface		v					
security									
session-router	4								
system	►								
Show All		OK	lack						

////

## Zoom side steering pool.

ORACL	Enterprise	Session Border Controller								admin 🔻
NN4600-139 10	.138.194.139 SCZ9	.0.0 Patch 3 (Build 290)				Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	on Q						Discard	😧 Verify	B Save
media-manager codec-policy	٣	Modify Steering Pool								
media-manager		IP Address	155.212.214.120							
media-policy		Start Port	40001		(Range: 0,165535)					
realm-config		End Port	50000		( Range: 0,165535 )					
steering-pool		Realm ID Network Interface	ZoomRealm	•						
security	►			•						
session-router	►									
system	•									
Show All		ОК	Back							

# 8.15. Configure Ping Response

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

#### Ping Response:

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

ORACL	E Enterprise	Session Border Controller					Û 🔺	admin 🔻
NN4600-139 10.1	38.194.139 SCZ9.	0.0 Patch 3 (Build 290)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configuration	n Q				Discard	😧 Verify	🖹 Save
media-manager	•	Modify Session Agent					Show Co	nfiguration
security	•							^
session-router	v	Hostname	162.12.233.60					
access-control		IP Address	162.12.233.60					
account-config		Port	5061	(Range: 0,102565535)				
filter-config	- 11	State	✓ enable					
Idan config		App Protocol	SIP					
iudp-coning		Арр Туре						
local-policy		Transport Mathod						
local-routing-con	fig	Transport Method	StaticTLS					
media profile		Realm ID	ZoomRealm	r				
media-pronie		Egress Realm ID		7				J
session-agent	~							
Show All		OK	Back					

ORACLE Enterprise Set	ssion Border Controller							admin 🔻
NN4600-139 10.138.194.139 SCZ9.0.0	Patch 3 (Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration View Configuration	Q					Discard	😧 Verify	B Save
media-profile	Modify Session Agent						Show Con	figuration
session-agent	Out Translationid		v					^
session-group	Trust Me	enable						
session-recording-group	Local Response Map		v					
session-recording-server	Ping Response	✓ enable						
session-translation	In Manipulationid		•					1
sip-config	Out Manipulationid		•					
sip-feature	Manipulation String							
sip-interface	Manipulation Pattern							
sip-manipulation	Trunk Group							
sin-monitoring  Show All	OK	Back						v

### 8.16. SBC config for Cisco Offer less INVITE

When CUCM sends INVITE without SDP towards SBC and in that case, SBC needs to send out INVITE with SDP towards Zoom and vice versa. To do that, please set the parameter "Add SDP Invite" as both under Zoom sip interface as highlighted below. When this option is enabled, codecs have to be configured under the parameter "Add SDP profiles". The configured codecs is also shown below.

Note: this is an optional config – configure this only if CUCM sends offer less INVITE towards SBC.

	Session Border Co	ontroller						Û 🔺	admin 🔻
NN4600-139 10.138.194.139 SCZ9.	0.0 Patch 3 (Build 29	0)		ſ	Dashboard Co	onfiguration N	Monitor and Trace	Widgets	System
Configuration View Configuration	n Q						Discard	😧 Verify	🖹 Save
media-profile	Modify SIP I	nterface						Show Cor	nfiguration
session-agent	State								^
session-group	Doolm ID	ena	Die						
session-recording-group	Realifitio	CUCMF	Realm						
session-recording-server	Description								
session-translation									
sip-config									
nin fankum	SIP Ports								
sip-reature	D: //								
sip-interface	Action Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonym	ious Multi	Home Addrs	
sip-manipulation	: 🗆	10.232.50.79	5060	UDP		agents-only			
sio-monitoring V Show All		OK Back							v

	e Session Border Controller						Û 🔺	admin 🔻
NN4600-139 10.138.194.139 SCZ	9.0.0 Patch 3 (Build 290)			Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration View Configurat	ion Q					Discard	😧 Verify	🖹 Save
nedia-profile	Modify SIP Interface						Show Cor	nfiguration
session-agent	TCP Keepalive	none	,					^
session-group	Add SDP Invite	both						
session-recording-group	Add SDP In Msg							
session-recording-server	D Farly Media Header							
session-translation	P Early Media Header	disabled	7					
sip-config	P Early Media Direction							
sip-feature	Add SDP Profiles	PCMU X PCMA X						
sip-interface		G729 🗙 G722 🗙						
sip-manipulation	Add SDP Profiles In Msg							
sio-monitorine V Show All	OK	Back						v

# 8.17. Configure sdes profile

Please go to  $\rightarrow$ Security  $\rightarrow$  Media Security  $\rightarrow$ sdes profile and create the policy as below.

ORACL	E Er	nterprise	Session Border Controller					Û 🔺	admin 🔻
NN4600-139 10.1	58.194.13	59 SCZ9.	0.0 Patch 3 (Build 290)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View C	onfiguratio	n Q				Discard	😧 Verify	B Save
factory-accounts		^	Modify Sdes Profile						
ike	Þ								^
ipsec	►		Name	SDES					
local-accounts			Crypto List	AES_CM_128_HMAC_SHA1_32 🗙					
media-security	Ŧ			AES_CM_128_HMAC_SHA1_80 🗙					
dtls-srtp-profile	9		Srtp Auth	✓ enable					
media-sec-poli	cy		Srtp Encrypt	✓ enable					
sdes-profile			SrTCP Encrypt	✓ enable					
sipura-profile		1.	Mki	enable					
password-policy			Egress Offer Format	same-as-ingress v					
security-config		~	Use Ingress Session Params						~
Show All	$\cap$		ОК	Back					

# 8.18. Configure Media Security Profile

Please go to  $\rightarrow$ Security  $\rightarrow$  Media Security  $\rightarrow$ media Sec policy and create the policy as below: Create Media Sec policy with name SDES which will have the sdes profile created above. **Assign this media policy to Zoom side as it uses TLS/SRTP**.

ORACL	E Ente	rprise S	Session Border Controller							Û 🔺	admin 🔻
NN4600-139 10.1	38.194.139	SCZ9.(	0.0 Patch 3 (Build 290)			Dashbo	bard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Conf	iguratior	n Q						Discard	Verify	🕒 Save
factory-accounts		^	Modify Media Sec Policy								
ike	•										^
ipsec	•		Name	sdesPolicy							
local-accounts			Pass Through	enable							
media-security	•		Options								
dtls-srtp-profil	e		Inbound								
media-sec-pol	icy		Profile	SDES 💌							
sdes-profile			Mode	srtp	v						
sipura-profile			Protocol	sdes	Ŧ						
password-policy			Hide Egress Media Update	enable							
security-config		~	∡ Outhound								*
Show All	0		OK	ack							

Similarly, Create Media Sec policy with name RTP to convert srtp to rtp for the CUCM side. Assign this media policy to the CUCM side as this will use only TCP/UDP

ORACL	E Enterp	rise Session Border Controller					Û 🗕	admin 🔻
NN4600-139 10.1	38.194.139 S	6CZ9.0.0 Patch 3 (Build 290)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration	View Configu	uration Q				Discard	😧 Verify	B Save
factory-accounts	^	Modify Media Sec Policy						
ike ipsec	> >	Name	RTP					^
local-accounts		Pass Through	enable					- 1
media-security	Ŧ	Options						
dtls-srtp-profil	e	Inbound						- 1
media-sec-pol	icy	Profile	T					- 1
sdes-profile		Mode	rtp 👻					
sipura-profile		Protocol	none 🔻					
password-policy		Hide Egress Media Update	enable					
security-config	~	⊿ Outhound						~
Show All	$\bigcirc$	ОК	Back					

With this, SBC configuration is complete

# 9. Existing SBC configuration

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

- <u>New realm-config</u>
- New SBC Certificate
- New TLS Profile
- New sip-interface
- New session-agent
- New steering-pools
- New local-policy
- New Media Security Profile

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

# Appendix A

Following are the test cases that are executed between Cisco User with the Zoom (ZOOM user). Please note that Cisco User here refers both Cisco User inside Enterprise network as well as Cisco Remote worker.

Z///X

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

17	Cisco user mutes inbound call from Zoom user and then unmutes	Pass
18	Cisco user mutes outbound call made to Zoom user and then unmutes	Pass
19	Zoom user mutes inbound call from Cisco user and then unmutes	Pass
20	Zoom user mutes outbound call made to Cisco user and then unmutes	Pass
21	Zoom User disconnects outbound call to Cisco user before it is answered	Pass
22	Cisco user disconnects outbound call to Zoom user before it is answered	Pass



CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/Oracle/

twitter.com/Oracle

oracle.com

Oracle Corporation, World Headquarters 500 Oracle Parkway

Redwood Shores, CA 94065, USA

Worldwide Inquiries Phone: +1.650.506.7000 Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

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