

Oracle SBC integration with Cisco Webex Calling and Webex Contact Center (CC) as 3rd party Local Gateway (LGW).

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	Oracle SBC integration with Cisco Webex Calling as 3rd party Local Gateway (LGW)	30 th October 2022
1.1	Added Appendix B section to the document for the new feature which supports Cisco DTMF with OPUS codec	05 th January 2023
1.2	Added ACLI config of the SBC. Also added screenshots to import certs to the SBC. Added section w.r.t sip options ping in multitenancy setup ChangeContactHost sip manipulation changed for ACK method. SBC version changed to 9.x in the whole document to keep it uniform. Config added for Media optimization feature (is supported from 9.3.0 and	08 th November 2024

Added crypto attributes for SRTP which includes GCM ciphers.	
Added support for Cisco Webex Contact Center along with Cisco Webex Calling part.	
Sip-manips made uniform for sip-interface going towards cisco Webex side from PSTN (Both normal and multitenancy config)	

Table of Contents

1. INTENDED AUDIENCE	6
2. DOCUMENT OVERVIEW	6
2.1. CISCO WEBEX CALLING:	6
3. INTRODUCTION	
3.1. AUDIENCE	
3.2. REQUIREMENTS	7
3.3. Architecture	
4. CISCO WEBEX SIDE CONFIGURATION	
5. CONFIGURING THE SBC	
5.1. VALIDATED ORACLE SBC VERSION	
6 NEW SRC CONFIGURATION	12
6.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC	
6.2. CONFIGURE SBC USING WEB GUI	
6.3. CONFIGURE SYSTEM-CONFIG	
6.4. CONFIGURE PHYSICAL INTERFACE VALUES	
6.5. CONFIGURE NETWORK INTERFACE VALUES	19
6.6. ENABLE MEDIA MANAGER	
6.8. CONFIGURE REALMS	
6.9. CONFIGURING A CERTIFICATE FOR SBC	
6.11 CONFIGURE SIP INTERFACES	
6.12. CONFIGURE SESSION-AGENT	
6.13. CONFIGURE LOCAL-POLICY	
6.14. CONFIGURE STEERING-POOL	
6.15. CONFIGURE SDES PROFILE	
6.16. CONFIGURE MEDIA SECURITY PROFILE	
6.17. CONFIGURE MEDIA OPTIMIZATION (ICE-PROFILE)	
7. EXISTING SBC CONFIGURATION	
8. SBC SCALING	
9. ORACLE SBC INTEGRATION WITH CISCO WEBEX CONTACT CENTER	
9.1. ENABLE THE USERS WITH WEBEX CC LICENSE	
9.2. SYNCHRONIZE THE USERS WITH WEBEX CC TENANT.	
9.5. CONFIGURE THE SETTINGS IN VOICE TAB	
9.5. CONFIGURE THE MULTIMEDIA PROFILE TAB.	
9.6. CONFIGURE THE DESKTOP PROFILE TAB.	
9.7. CONFIGURE THE IDLE/WRAP-UP CODES TAB.	55
9.8. CONFIGURE THE SITES TAB	55
9.9. CONFIGURE THE SKILL DEFINITIONS TAB	
9.10. CONFIGURE THE CONTACT CENTER USERS TAB.	
APPENDIX A	58
CONFIGURE MULTI-TENANCY	
APPENDIX B	

10. CAVEAT	65
ISSUE 1: SIP OPTIONS PING FROM MULTIPLE REALMS TO GLOBAL SESSION AGENTS	65
ISSUE 2: VIDEO CALL ISSUES WHEN CALL COMES FROM CISCO CUCM TOWARDS CISCO WEBEX	65
11. ACLI RUNNING CONFIGURATION	66

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 along with Cisco Webex Calling and Cisco Webex Contact Center with 3rd Party Local Gateway.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between PSTN Trunk with Cisco Webex Calling Solution and Cisco Webex Contact Center. The solution contained within this document has been tested using Oracle Communication SBC with software version **OS 9.x version.**

Please find the related documentation links below:

2.1. Cisco Webex Calling:

Cisco Webex Calling is a cloud calling solution that delivers enterprise-grade calling, enabling you to replace your on-premises PBX network with a globally trusted cloud calling solution. This Webex Calling easily extends to a complete collaboration experience that includes market-leading calling, meetings, messaging, contact center, and integrated devices for all situations

Webex Calling Cloud service or in short "Webex Calling" supports "Bring Your Own PSTN" and Enterprise dialing using through what is termed as a Local Gateway that sits at the edge of the Customer's VoIP network. A local gateway is a SIP Session Border Controller that interworks with Webex Calling cloud service in specific ways & This Local gateway MUST operate specified conditions with Webex Calling. Local Gateway feature enables Webex Calling customers to continue using their existing PSTN service provider. **Oracle SBC works with Webex calling as 3rd party Local Gateway in Certificate based Trunking model.**

For additional information on Cisco Webex Calling and certificate-based trunking, please check the below links:

https://www.Webex.com/products/Webex-calling.html

https://help.Webex.com/en-us/article/n0xb944/Configure-Trunks,-Route-Groups,-and-Dial-Plans-for-Webex-Calling#Cisco_Reference.dita_20664899-b518-4f5d-bc92-88af4a5c6694

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 Webex Calling with 3rd party LGW feature using 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, SIP/RTP and TLS/SRTP are also necessary to complete the configuration and for troubleshooting, if necessary.

3.2. Requirements

• Fully functioning Cisco Webex Control Hub (Provisioned Webex Control Hub with necessary Webex Calling licenses/Subscription and also prepared Webex Calling environment)

https://help.webex.com/en-us/article/n4cprps/Prepare-Your-Environment-for-Webex-Calling

• Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 9.x version.

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
Revision 1	9.x

3.3. Architecture



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

- Phase 1 Configuring the Cisco Webex calling with 3rd party Local Gateway (LGW) feature for Oracle SBC.
- Phase 2 Configuring the Oracle SBC.
- Phase 3 Configuring the Cisco Webex Contact Center.

4. Cisco Webex Side Configuration

The configuration of Cisco Webex side is a mandatory prerequisite before starting the SBC configuration. The Webex admin should <u>Configure Trunks</u>, <u>Route Groups</u>, <u>and Dial Plans for Webex</u> Calling to create a trunk toward Oracle SBC. Once the configuration on Webex Control Hub is complete, the admin will be provided with destination (Webex Edge proxy) Address that need to be configured on the Oracle SBC.

Please login to **Webex Control Hub ----- Calling ------ Call routing** and you can check the created Trunk which actually connects to the SBC.

webex Contro	Q Search	h			4º 0 0
📋 Devices	0 11				
Co Apps	Calling				
Account	Numbers Locations Call	Routing Features PS	TN Orders Service Settin	ngs Client Settings	
🔅 Organization Settings					
	Trunk Route Group Dial Plans	Verify Call Routing Zone	Trusted Network Edge		
SERVICES	Trunk				
C Updates & Migrations	SIP trunks provide connectivity to a c These were previously accessed via	customer-owned PSTN service and the Local Gateway configuration pa	to an on-premises IP PBX deployi ge.	nent.	Add Trunk
○ Messaging					
📋 Meeting	Q Search				
𝗞 Calling	Name	Location	Trunk Type	In Use	
S Connected UC	cloudsbc	BurlingtonHQ	Certificate based	Yes	
		, - , ,			
Cracle					

Click on the trunk name to get more details about the configured trunk.

webex Contro	l Hub	Search			4º 0 c
Devices	Calling			cloudsbc //	Х
CO Apps	Calling				
Account	Numbers Locations	Call Routing Features	PSTN Orde	Trunk	
ôf Organization Settings				Details	
	Trunk Route Group Dia	I Plans Verify Call Routing	Zone Truste	Trunk Info	Manage >
SERVICES	Trunk				
C Updates & Migrations	SIP trunks provide connectivi These were previously acces	ity to a customer-owned PSTN sen sed via the Local Gateway configu	vice and to an on- ration page.	In Use	
○ Messaging				Calls to On-Premises Extensions	0 Locations $ ightarrow$
📋 Meeting	Q Search			Dial Plans	0 Dial Plans $ ight angle$
𝗞 Calling	Name	Location	Trunk	PSTN Connection	2 Locations 〉
S Connected UC	cloudsbc	BurlingtonHQ	Certifica	Poute Group	
🛆 Hybrid				Note Group	o noute croups /
Oracle					

Click on the Trunk Info to get the details which is the parameters used to connect to the Oracle SBC. The trunk status shows Online which means the Webex is able to establish a connection with Oracle SBC and the trunk type are defined as Certificate based and the FQDN is also defined.

webex Contro	l Hub	Q Search			 ↓ [®] ⑦s
ැබූ Settings	Calling			cloudsbc 🖉	Х
SERVICES	Numbers Locations	Call Routing Features	B PSTN Orde	Trunk > Details	
C Updates & Migrations	Trunk Douto Crown	Diel Diene Vorify Cell Deuting	Zeno Trueto	Status (i)	
	Trunk Route Group	Dial Plans Verify Call Routing	Zone Truste	Online	
£)	Trunk			Trunk Type	
Meeting	SIP trunks provide conne	ctivity to a customer-owned PSTN se	ervice and to an on-	Certificate based	
🗞 Calling	These were previously a	ccessed via the Local Gateway config	uration page.		
Nideest				Device	
	Q Search			Oracle ACME Session Border Controller	
S Connected UC					
→ Hybrid	Name	Location	Truck	FQDN	
	Name	Location	ITUIK	cloudsbc.cgbusolutionslab.com:5061	
Cracle	cloudsbc	BurlingtonHQ	Certific	Max concurrent calls	
				2000	

In the below screen, you can check the destination (Webex Edge proxy) Address which will be used as Session Agent in the Oracle SBC to connect to Cisco Webex side. As Cisco recommends using SRV based Webex Calling edge address, we will be using that as Session Agent in oracle SBC (This requirement is for now and may be changed in future). You can also check the created directory numbers and the locations in the same Calling page of Webex Control Hub.

Please note that Webex Calling Proxy Addresses given below is example addresses which are used for testing and these values will vary from region to region. For more information about the Webex Calling Proxy Addresses, please contact your Cisco team.

webex Contro	l Hub	Q Search		↓ [®] ⑦ CS
ర్టి Settings	Calling			Max concurrent calls
SERVICES	Numbers Location	s Call Routing Features	PSTN Orde	2000
C Updates & Migrations	Trunk Poute Group	Dial Dians Varify Call Pourting	Zone Truste	Webex Calling edge proxy address (FQDN) peering1.us.sipconnect.bcld.webex.com:5062
○ Messaging	Trunk		20110 114310	peering2.us.sipconnect.bcld.webex.com:5062 peering3.us.sipconnect.bcld.webex.com:5062
📋 Meeting	ITUTIK SIP trunks provide connectivity to a customer-owned PSTN service and to an on-			peering4.us.sipconnect.bcld.webex.com:5062
🗞 Calling	These were previously accessed via the Local Gateway configuration page.			Webex Calling edge proxy address (SRV)
D Vidcast				us01.sipconnect.bcld.webex.com
😂 Connected UC	Q Search			Dual Identity Support
🛆 Hybrid	Name Location Trunk		The Dual Identity Support setting Impacts the handling of the From header and P-Asserted-Identity (PAI) header when sending an initial SIP	
	cloudsbc	BurlingtonHQ	Certifica	INVITE to the trunk for an outbound call. When enabled, the From and PAI headers are treated independently and may differ. When disabled, the
Oracle				PAI header is set to the same value as the From header. Please refer to

With this, Cisco side configuration is complete.

5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Cisco Webex Calling and PSTN SIP Trunk. In this SBC config, Cisco Webex Calling side is secure (TLS/SRTP) and PSTN Side is unsecure (UDP or TCP/RTP).

5.1. Validated Oracle SBC version

Oracle conducted tests with SBC 9.x 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
- Oracle SBC on Public Cloud

6. New SBC configuration

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

6.1. 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

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
Initializ	zing /opt/ Cleaner
Starting	tLogCleaner task
Bringing	up shell
starting	aclimgr
bassword	secure mode is enabled
amin 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.

Password:
8
8 Only alphabetic (upper or lower case), numeric and punctuation
% characters are allowed in the password.
% Password must be 8 - 64 characters,
% and have 3 of the 4 following character classes :
8 - lower case alpha
% - upper case alpha
% - numerals
% - punctuation
8
Enter New Password:
Confirm New Password:
Password is acceptable.

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

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

```
SolutionsLab-vSBC-2(configure)# bootparam
 .' = clear field; '-' = go to previous field; q = quit
Boot File
                       : /boot/nnSCZ900p4.bz
IP Address
VLAN
Netmask
Gateway
Pv6 Address
IPv6 Gateway
Host IP
TP username
                       : vxftp
TP password
Flags
                      : 0x00000040
Target Name
                     : SolutionsLab-vSBC-2
Console Device
                     : COM1
Console Baudrate
Other
NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.
       ERROR
               : space in /boot
                                     (Percent Free: 18)
SolutionsLab-vSBC-2(configure)#
SolutionsLab-vSBC-2(configure)#
```

Note: There is no management IP configured by default.

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

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

SolutionsLab-vSBC-2# setup product
WARNING: Alteration of product alone or in conjunction with entitlement changes will not be complete until system reboot
Last Modified 2022-10-03 07:21:29
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. (The below screen is just an example and not actual config)

Last	Modified: 2022-02-23 18:18:18	Controller
1:	Session Capacity	: 9999
2:	Advanced	: enabled
3:	STIR/SHAKEN Client	
4 :	Admin Security	:
5:	Data Integrity (FIPS 140-2)	
6:	IPSec Trunking Sessions	: 0
7:	MSRP B2BUA Sessions	: 0
8:	SRTP Sessions	: 0
9:	Transcode Codec AMR	
10:	Transcode Codec AMR Capacity	: 0
11:	Transcode Codec AMRWB	
12:	Transcode Codec AMRWB Capacity	: 0
13:	Transcode Codec EVRC	
14:	Transcode Codec EVRC Capacity	: 0
15:	Transcode Codec EVRCB	
16:	Transcode Codec EVRCB Capacity	: 0
17:	Transcode Codec EVS	:
18:	Transcode Codec EVS Capacity	: 0
19:	Transcode Codec OPUS	: enabled
20.	Transcode Codec OPUS Capacity	· 2000
21.	Transcode Codec SILK	• enabled
21.	Transcode Codec SILK Capacity	• 2000
22:	Transcode codec SILK capacity	: 2000
Ente	r 1 – 22 to modify, d' to display, 's' t	to save, 'q' to exit. [s]: 1
Se	ssion Capacity (0-10000)	: 500
Ente	r 1 – 22 to modify, d' to display, 's' t	to save, 'q' to exit. [s]: 10
Tra	anscode Codec AMR Capacity (0-10000)	: 50
Ente	r 1 - 22 to modify, d' to display, 's' t	to save, 'q' to exit. [s]: 14
Tra	anscode Codec EVRC Capacity (0-10000)	: 40
Ente	r 1 – 22 to modify, d' to display, 's' t	to save, 'q' to exit. [s]: 🗌

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.

SolutionsLab-vSBC-2(http-server)# show	
http-server	
name	webserver
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	REST,GUI
http-file-upload-size	0
tls-profile	
auth-profile	
last-modified-by	webHTTP-admin@196.15.23.12:33336
last-modified-date	2022-07-07 17:34:44
SolutionsLab-vSBC-2(http-server)#	
SolutionsLab-vSBC-2(http-server)#	
SolutionsLab-vSBC-2 (http-server) #	

6.2. 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		Username	
Enterprise Session Border Controller		Password	Required
			Required
		SIGN IN	

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



Go to Configuration as shown below, to configure the SBC

ORACLE Enterprise Session Border Controller										
SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace Widgets Sy										
Configuration	View Configuration	n Q			Discard	😧 Verify	🖹 Save			
media-manager	▶	Configuration Objects								
security	•									
session-router	•	Name	Description							
sustem		access-control	Configure a static or dynamic access control list							
system	4	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://www.com/or	Configure on HTTD conver							
Show All		Displaying 1 - 11 of 40								

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

https://docs.oracle.com/en/industries/communications/enterprise-session-bordercontroller/9.3.0/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.

6.3. Configure system-config

Go to system->system-config

ORACLE Enterprise Session Border Controller								
SolutionsLab-vSBC-2 SCZ9.0.0 Pai	tch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets	System	
Configuration View Configuration	ion Q				Discard	🕸 Verify	B Save	
, host-route	Modify System Config					Show Cor	figuration	
http-client	Hostname	OracleSBC						
http-server	Description						I	
network-interface								
ntp-config								
phy-interface	Location							
redundancy-config	Mib System Contact							
snmp-community	Mib System Name							
spl-config	Mib System Location							
system-config	Acp TLS Profile	Ŧ						
Show All	OK	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/9.3.0/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.

6.4. Configure Physical Interface values

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

Please configure s0p0 for PSTN side and s1p0 for Cisco Webex side.

Parameter Name	PSTN Trunk side (s0p0)	Cisco Webex side (s1p0)
Slot	0	1
Port	0	0
Operation Mode	Media	Media

Please configure s0p0 interface as below.

ORACLE Enterprise Session Border Controller										
SolutionsLab-vSBC-2 SCZ9.0.0 Pat	Monitor and Trace	Widgets	System							
Configuration View Configuration	ion Q					Discard	😧 Verify	🖹 Sav		
, host-route	Modify Phy Interface									
http-client	Name	s0p0								
http-server	Operation Type	Media	v							
network-interface	Port	0	(Range: 05)							
ntp-config	Slot	0	(Range: 02)							
phy-interface	Virtual Mac									
redundancy-config	Admin State	✓ enable								
snmp-community	Auto Negotiation	✓ enable								
spl-config	Duplex Mode	FULL	v							
system-config	Speed	100	v							
Show All	OK	Back								

Please configure s1p0 interface as below

ORACLE Enterprise Session Border Controller										
SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4	4 (Build 343)	Dashboard	Configuration	Monitor and Trace	Widgets	System				
Configuration View Configuration	Q					Discard	😧 Verify	🖹 Save		
host-route	Modify Phy Interface									
http-client	Name	s1p0								
http-server (Operation Type	Media								
network-interface F	Port	0	(Range: 05)							
ntp-config S	Slot	1	(Range: 02)							
phy-interface	Virtual Mac									
redundancy-config	Admin State	✓ enable								
snmp-community	Auto Negotiation	✓ enable								
spl-config [Duplex Mode	FULL								
system-config	Speed	100								
Show All	OK	Back								

////

6.5. 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	PSTN Trunk Side Network Interface(s0p0)	Cisco Webex side Network Interface(s1p0)
Name	s0p0	S1p0
Host Name		
IP Address	155.212.214.90	10.1.3.4
Net Mask	255.255.255.0	255.255.255.0
Gateway	155.212.214.65	10.1.3.1

Please configure network interface s0p0 as below

ORACLE Enterprise Session Border Controller										
SolutionsLab-vSBC-2 SCZ9.0.0 Pat	ch 4 (Build 343)			D	ashboard	Configuration	Monitor and Trace	Widgets		
Configuration View Configuration	on Q						Discard	😧 Verify		
, host-route	Modify Network Interface									
http-client	Name	s0p0	•							
http-server	Sub Port Id	0		(Range: 04095)						
network-interface	Description									
ntp-config										
phy-interface										
redundancy-config	Hostname									
snmp-community	IP Address	155.212.214.90								
spl-config	Pri Utility Addr									
system-config	Sec Utility Addr									
Show All	OK	Back								

1177 2////

Similarly, configure network interface s1p0 as below

ORACLE Enterprise Session Border Controller										
SolutionsLab-vSBC-2 SCZ9.0.0 Pat	ich 4 (Build 343)			Dashboard	Configuration	Monitor and Trace	Widgets			
Configuration View Configuration	on Q					Discard	😧 Verify			
host-route	Modify Network Interface									
http-client	Name	s1p0	•							
http-server	Sub Port Id	0	(Range: 04095)							
network-interface	Description									
ntp-config										
phy-interface										
redundancy-config	Hostname									
snmp-community	IP Address	10.1.3.4								
snl-config	Pri Utility Addr									
system-config	Sec Utility Addr									
Show All	OK	Back								

ORACLE Enterprise Session Border Controller												
SolutionsLab-vSBC-2 SCZ9.0.0 Pate	ch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets						
Configuration View Configuration	n Q				Discard	😧 Verify						
session-router	Modify Network Interface											
system 🔻	DNS IP Primary	9.9.9.9	Add Upload									
traud-protection	DNS IP Backup1	8.8.8.8										
http_client	DNS IP Backup2	8.8.4.4										
http-server	DNS Domain	cgbusolutionslab.com										
	DNS Timeout	11	(Range: 04294967295)									
network-interface	DNS Max Ttl	86400	(Range: 302073600)									
ntp-config	Signaling Mtu	0	(Range: 0,5764096)									
phy-interface	HIP IP List											
redundancy-config	ICMD Addrocc											
Show All	OK	Back										

6.6. Enable media manager

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

Go to Media-Manager->Media-Manager

ORACLE	E Enterpris	e Session Border Controller					
SolutionsLab-vSBC-2	2 SCZ9.0.0 P	atch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configura	tion Q				Discard	😧 Verify
media-manager	•	Modify Media Manage	r				
codec-policy media-manager		State	✓ enable				
media-policy		Flow Time Limit	86400	(Range: 04294967295)			
realm-config		Initial Guard Timer	300	(Range: 04294967295)			
steering-pool		Subsq Guard Timer TCP Flow Time Limit	300 86400	(Range: 04294967295) (Range: 04294967295)			
security	•	TCP Initial Guard Timer	300	(Range: 04294967295)			
session-router	•	TCP Subsq Guard Timer	300	(Range: 04294967295)			
system	~	Hnt Rtcp	enable				
fraud-protection		Algd Log Level	NOTICE				
host-route		Mbcd I og I evel	107105				
Show All		ОК	Delete				

ORACL	E Enterpris	se Session Border Controller					i
SolutionsLab-vSB0	C-2 SCZ9.0.0 P	atch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configura	ation Q				Discard	😧 Verify
media-manager	Ψ.	Modify Media Manager					
codec-policy		Max Signaling Packets	0	(Range: 04294967295)			
media-manager		Max Untrusted Signaling	1	(Range: 0100)			
media-policy		Min Untrusted Signaling	1	(Range: 0100)			
roalm config		Dos Guard Window	5	(Range: 130)			
realm-coming		Untrusted Minor Threshold	0	(Range: 0100)			
steering-pool		Untrusted Major Threshold	0	(Range: 0100)			
security	•	Untrusted Critical Threshold	0	(Range: 0100)			
session-router	•	Trusted Minor Threshold	0	(Range: 0100)			
system	v	Trusted Major Threshold	0	(Range: 0100)			
, freed and a first		Trusted Critical Threshold	0	(Range: 0100)			
traud-protection		Arp Minor Threshold	0	(Range: 0100)			
host-route							
Show All		ОК	Delete				

-///

6.7. Enable sip-config

SIP config enables SIP handling in the SBC. To configure sip-config, Go to Session-Router->sip-config.

Also add the options to the sip-config as shown below. In options add max-udp-length =0.

	Session Border Controller						a
SolutionsLab-vSBC-2 SCZ9.0.0 Pat	tch 4 (Build 343)			Dashboard	Configuration	Monitor and Trace	Widgets
Configuration View Configuration	on Q					Discard	😧 Verify
1 - Z							
local-routing-config	Modify SIP Config						
media-profile	State	✓ enable					
session-agent	Dialog Transparency	✓ enable					
session-group	Home Realm ID	CiscoWebexRealm	•				
session-recording-group	Egress Realm ID		T				
session-recording-server	Nat Mode	None					
session-translation	Registrar Domain	*					
sip-config	Registrar Host	*					
sip-feature	Registrar Port	5060		(Range: 0,102565535)			
sip-interface	Init Timer	500		(Range: 04294967295)			
Show All	ОК	Delete					

	Session Border Controller						ac
SolutionsLab-vSBC-2 SCZ9.0.0 Pat	ich 4 (Build 343)			Dashboard	Configuration	Monitor and Trace	Widgets S
Configuration View Configuration	on Q					Discard	😧 Verify
local-routing-config	Modify SIP Config						
media-profile	Invite Expire	180	(Range: 02147473)				
session-agent	Session Max Life Limit	0					
session-group	Enforcement Profile	v					
session-recording-group	Red Max Trans	10000	(Range: 050000)				
session-recording-server	Options	max-udp-length=0 🗙					
session-translation	SPL Options						
sip-config	SIP Message Len	4096	(Range: 065535)				
sip-feature	Enum Sag Match	enable					
sip-interface	Extra Method Stats	✓ enable					
Show All	OK	Delete					

6.8. 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	PSTN Side	Cisco Webex Side
Identifier	SIPTrunk	CiscoWebexRealm
Network Interface	S0p0	s1p0
Mm in realm		
trunk-context		cloudsbc.cgbusolutionslab.com
Media Sec policy	CiscoWebexSecurity	PSTNSide
Access Control Trust Level	High	High

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

ORACL	E Enterprise See	ssion Border Controller					a
SolutionsLab-vSBC	-2 SCZ9.0.0 Patch 4	(Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configuration	Q				Discard	😧 Verify
media-manager	•	Modify Realm Config					
codec-policy							
media-manager		Identifier	SIPTrunk				
media-policy		Description					
realm-config							
steering-pool		Addr Prefix	0.0.0.0				
security	•	Network Interfaces	s0p0:0.4 🗙				
session-router	►	Media Realm List					
system	•						
		Mm In Realm	✓ enable				
		Mm In Network	✓ enable				
		Mm Same Ip	✓ enable				
Show All		ОК	Back				

ORACL	E Enterprise Ses	ssion Border Controller							а
SolutionsLab-vSBC	-2 SCZ9.0.0 Patch 4	l (Build 343)				Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configuration	Q						Discard	😧 Verify
media-manager	Ψ.	Modify Realm Config							
codec-policy				٣					
media-manager		In Manipulationid		Ŧ					
media-policy		Out Manipulationid		Ŧ					
realm-config		Average Rate Limit	0		(Range: 04294967295)				
steering-pool		Access Control Trust Level	high	Ŧ					
security	•	Invalid Signal Threshold	0		(Range: 04294967295)				
cossion router		Maximum Signal Threshold	0		(Range: 04294967295)				
Session-router	<i>F</i>	Untrusted Signal Threshold	0		(Range: 04294967295)				
system	*	Nat Trust Threshold	0		(Range: 065535)				
fraud-protection		Max Endpoints Per Nat	0		(Range: 065535)				
host-route		Nat Invalid Message Threshold	0		(Range: 065535)				
http-client		Wait Time For Invalid Register	0		(Range: 0,4300)				
Show All		ОК	Back						

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

Please set the parameter trunk-context to cloudsbc.cgbusolutionslab.com (Please note that this parameter value given here is an example used for our testing purposes and the user can configure this value according to their environment). This value is configured as FQDN of SBC in the Cisco Webex Admin portal, and this will be used by Cisco Webex calling side to reach SBC when making calls.

ORACL	E Enterprise	e Session Border Controller					ā
SolutionsLab-vSB0	C-2 SCZ9.0.0 Pa	tch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configurati	tion Q				Discard	😧 Verify
media-manager	▼	Modify Realm Config					
codec-policy media-manager		Identifier	CiscoWebexRealm				
media-policy		Description					
realm-config							
steering-pool		Addr Prefix	0.0.0.0				
security	•	Network Interfaces	s1p0:0.4 🗙				
session-router	•	Media Realm List					
system	•	Mm In Realm	✓ enable				
		Mm In Network	- ··				
Show All		ОК	Back				

ORACL	E Enterprise	Session Border Controller						a
SolutionsLab-vSBC-	2 SCZ9.0.0 Pat	ich 4 (Build 343)			Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configurati	on Q					Discard	😧 Verify
media-manager	▼	Modify Realm Config						
codec-policy		Max Endpoints Per Nat	0		(Range: 065535)			
media-manager		Nat Invalid Message Threshold	0		(Range: 065535)			
media-policy		Wait Time For Invalid Register	0		(Range: 0,4300)			
realm-config		Deny Period	30		(Range: 04294967295)			
steering-pool		Session Max Life Limit	0					
		Untrust Cac Failure Threshold	0		(Range: 04294967295)			
security	•	Subscription Id Type	END_USER_NONE					
session-router	۱.	Trunk Context	cloudsbc.cgbusolutionslab.com					
system	•	Early Media Allow		Ŧ				
		Enforcement Profile		w				
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/9.3.0/security/securityguide.pdf

6.9. Configuring a certificate for SBC

This section describes how to configure the SBC for TLS and SRTP communication for Cisco Webex Calling. Cisco Webex calling side allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by the trusted Certificate Authorities like Go Daddy Root CA and also IdenTrust Root CA certificate as Cisco Webex has moved to a new Certificate Authority, IdenTrust Commercial Root CA from March 2021.

The links for Identrust certificate is given below:

https://help.Webex.com/en-us/article/WBX9000034330/New-Root-Certificate-Authority-for-Cisco-Webex-Services-from-March-2021

https://help.Webex.com/en-us/article/WBX9000008850/What-Root-Certificate-Authorities-are-Supportedfor-Calls-to-Cisco-Webex-Audio-and-Video-Platforms?

Though the links talks about Identrust certificates used by Cisco VCS and Expressway, we can still Download the Identrust root certificate and can upload it to the Oracle SBC with the steps given below.

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.

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.

- SBC 1 certificate-record assigned to SBC
- Root 1 certificate-record for root cert
- 2) Deploy the SBC and Root certificates on the SBC

Step 1 – Creating the certificate record

Go to security->Certificate Record and configure the SBC entity certificate for SBC as shown below.

Please note that the FQDN created on the Webex side must be the Common Name (CN) or Subject Alternative Name (SAN) of the certificate. As Cisco does an exact match and do not support wildcard certificates, each domain must be called out in CN or SAN of the certificate for validation.

ORACL	E Enterpris	e Session Border Controller					
SolutionsLab-vSBC-	2 SCZ9.0.0 P	atch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configura	tion Q				Discard	😧 Verify
media-manager	×	Modify Certificate Re	cord				
security	٣						
authentication-pro	ofile	Name	CloudSBCSolLab				
certificate-record		Country	US				
tls-global		State	МА				
tls-profile		Locality	Burlington				
session-router	•	Organization	Engineering				
system	•	Unit	SolutionsLab				
		Common Name	cloudsbc.cgbusolutionslab.com				
		Key Size	2048 💌				
		Alternate Name					
Show All		01	K Back				

ORACL	Enterprise	Session Border Controller					ac
SolutionsLab-vSB(C-2 SCZ9.0.0 Pate	ch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets S
Configuration	View Configuration	n Q				Discard	😧 Verify
media-manager	•	Modify Certificate Record	1				
security	•	Common Name	cloudsbc.cgbusolutionslab.com				
authentication-p	profile	Key Size	2048				
certificate-record	b	Alternate Name					
tls-global		Trusted	✓ enable				
tls-profile		Key Usage List	digitalSignature 🗙				
session-router	•		keyEncipherment X				
system	•	Extended Key Usage List	serverAuth x clientAuth x				
		Key Algor	rsa 💌				
		Digest Algor	sha256 💌				
Show All		OK	Back				

Create a Certificate record for Identrust Root CA in SBC as below:

ORACL	Enterprise	Session Border Controller					Û 🔺 🧯
SolutionsLab-vSBC	C-2 SCZ9.0.0 Pat	tch 4 (Build 343)		Dashbo	rd Configuration	Monitor and Trace	Widgets
Configuration	View Configurati	ion Q				Discard	😧 Verify
media-manager	Þ	Modify Certificate Reco	ord				
security authentication-p	▼ rofile	Name	WebexRootCA				
certificate-record		Country	US				
tls-global		State	MA				
tls-profile		Locality	Burlington				
session-router	F	Organization	Engineering				
system	•	Unit	Cisco Webex Calling				
		Common Name	IdenTrust Root CA certificate				
		Key Size	2048 💌				
		Alternate Name					
		Trusted	🖌 enable				
Show All	\bigcirc	OK	Back				

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

Config Parameter	Go Daddy Root	IdenTrust Root
Common Name	Go Daddy class2 Root CA	IdenTrusrt Root CA
Key Size	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth
Key algor	rsa	rsa
Digest-algor	Sha256	Sha256

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.

Configuration View	v Configu	ration	ß	Q						Discard	😧 Verify 🖺 Save
media-manager	>	Certi	ficate	Record							Show Configuration
security	~										
authentication-profile		D,	£		/ ि ₫	📑 🗹 Delete			Search		Q
certificate-record											~
tls-global		Select	Action	Name 🗘	Country 😂	State 🗘	Locality 🗘	Organization (0	Unit 🗘	Common Name 💲
tls-profile			÷	CGBUSolutionsLab	US	MA	Burlington	Engineering		SolutionsLab	cgbusolutionslab.com
session_router	`		:	CloudSBCSolLab	US	MA	Burlington	Engineering		SolutionsLab	cloudsbc.cgbusolutio
Session router			÷	GoDaddyCrossCert	US	МА	Burlington	Engineering		www.godaddy.com	GoDaddy G1 to G2 Cr
system	>		:	GoDaddyIntermediate	US	MA	Burlington	Engineering		www.godaddy.com	GoDaddy Secure Ser
				GoDaddyRootCA	US	МА	Burlington	Engineering		www.godaddy.com	GoDaddy Class 2 Cer
			÷	WebexRootCA	US	MA	Burlington	Engineering			IdenTrust Root CA ce

Copy the following information and send to a CA authority	
BEGIN CERTIFICATE REQUEST MIICvTCCAaUCAQAwRTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMR	
MwEQYDVQQH EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzCCASIwDQY	
JKoZlhvcN AQEBBQADggEPADCCAQoCggEBALzMG9rclE8r+f2nK1zIMcTJaLVdh+1WR	
+vWmKnn /nvifp7sKsUvFKX0bAjZU5SA5EpdHfYLC9G7jMz7dKJ0SUC0q6GkcFBKtvhBlf	
nU Js0vaSc3UMlc+jqy9G+2Fsd44mY/KMxPFQnMXECgT7RAyhKLj0zoxqi6dQ5zb	
HGJ2dAPkXqmwBwc2zx101bawk9W/sk2o2gKWl5B6rOw2lCblVyekn7SUEPB	
43NP43mvNQWbFffc3oCAzdqgWxvDzhQbvhu76nGJPnCGqxJoHR7dTD6GX	
gNFOWdLWEh00RCktAltTNeV4KdcGeYrYZlkvJZlHHpT/7mkCAwEAAaAzMD EGCSaG	

• 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

Configuration View C	Configur	ration	õ	Q							Discard	😧 Verify 🖺 Sa
media-manager	>	Certif	icate	Record								Show Configurati
security	~											
authentication-profile		D,	¢	1 R	PKCS12	∥ ⊡ ⊡	📮 🗹 Delete			Search		Q
certificate-record			I	Edit								_
tls-global		Select	ភេ	Codv		Country \$	State \$	Locality 💲	Organization	0	Unit ≎	Common Name 💲
tls-profile					insLab	US	МА	Burlington	Engineering		SolutionsLab	cgbusolutionslab.com
and provider			Ш	Delete	lLab	US	МА	Burlington	Engineering		SolutionsLab	cloudsbc.cgbusolutio.
session-router	>		E,	Generate	ssCert	US	МА	Burlington	Engineering		www.godaddy.com	GoDaddy G1 to G2 Cr.
system	>		Ľ	Import	ermediate	US	МА	Burlington	Engineering		www.godaddy.com	GoDaddy Secure Ser
			:	GoDaddyRo	otCA	US	MA	Burlington	Engineering		www.godaddy.com	GoDaddy Class 2 Cer.
			÷	WebexRoot	CA	US	МА	Burlington	Engineering			IdenTrust Root CA ce.

Configuration Vie	w Configu	ration	ĉ	Q							Discard	😧 Verify 🖺 Sa
media-manager	>	Certif	icate	Record								Show Configurat
security	~											
authentication-profile		n	ı	Edit	PKCS12	/ 6 前	🖳 🗹 Delete			Search	1	0
certificate-record			G	Conv								~
tls-global		Select	.u .a	Delete		Country 🗘	State 🗘	Locality 🗘	Organization	\$	Unit 🗘	Common Name 💲
tls-profile				Delete	nsLab	US	МА	Burlington	Engineering		SolutionsLab	cgbusolutionslab.com
session router			Ľ,	Generate	lLab	US	МА	Burlington	Engineering		SolutionsLab	cloudsbc.cgbusolutio
-			Ľ	Import 🥌	ssCert	US	МА	Burlington	Engineering		www.godaddy.com	GoDaddy G1 to G2 Cr
system	>		:	GoDaddyIn	termediate	US	МА	Burlington	Engineering		www.godaddy.com	GoDaddy Secure Ser.
			÷	GoDaddyRo	ootCA	US	МА	Burlington	Engineering		www.godaddy.com	GoDaddy Class 2 Cer
			:	WebexRoot	CA	US	МА	Burlington	Engineering			IdenTrust Root CA ce
Show All 20.69.252.200/#		Displayi	ng 1 - (6 of 6								

2///

ORACLE Enter	prise Session Border Controller		adm	
SolutionsLab- vSBC-2 10.1.1.4 SC	Import Certificate		×	stem
Configuration View Con			_	B Save
media-manager >	Format	try-all 🔹		iguration
security 🗸	Import Method	File		
authentication-profile		O Paste		0
certificate-record	Certificate File	↓ Upload No file selected.		~
tls-global				, com
tls-profile				plutio
session-router				52 Cr
system >				e Ser
		Import Cancel		2 Cer
			-	IA ce

Repeat these steps to import all the root and intermediate CA certificates into the SBC: At this stage all the required certificates have been imported to the SBC for Cisco Webex Calling.

6.10. 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 the Cisco Webex calling side:

ORACL	E Enterprise Ses	ssion Border Controller						
SolutionsLab-vSBC	-2 SC79.0.0 Patch 4	(Build 343)			Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configuration	Q					Discard	😟 Verify
media-manager	Þ	Modify TLS Profile						
authentication-p	vofile	Name End Entity Cortificate	TLSWebex					
certificate-record		Trusted Ca Certificates	CloudSBCSolLab					
tls-profile			WebexRootCA X GoDaddyIntermediate X					
session-router	►	Cipher List						
system	Þ	Verify Depth Mutual Authenticate TLS Version Options	10 enable tisvt2	(Range: 0.10)				
Show All		ОК	Back					

6.11. 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.

Please Configure sip-interface for the Cisco Webex Calling side as below:

- 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.
- Set user-agent parameter as Oracle/VM/9.0.0p4 (This can be the respective Oracle SBC Platform and version and these values can be updated accordingly)
- Set **initial-inv-trans-expire parameter value to 10** so the SBC will recurse on no response to SRV session agent

	e Session Border (Controller								admin 🔻
SolutionsLab-vSBC-2 SCZ9.0.0 Pa	atch 4 (Build 343)					Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration View Configurat	tion Q							Discard	😧 Verify	🖹 Save
session-group	Modify SIP	Interface							Show Cor	figuration
session-recording-group	State		✓ enable							
session-recording-server	Realm ID		CiscoWebexReal	m 🔻						
session-translation	Description									
sip-config										
sip-feature										
sip-interface	SIP Ports									
sip-manipulation	D:	6 8								
cip monitoring	Action Sele	ct Address	Port		Transport Protocol	TLS Profil	e Allow And	onymous Mu	lti Home Addrs	5
2h-monunk	: 🗆	10.1.3.4	5061		TLS	TLSWebex	agents-on	ly		
translation-rules										
Show All		OK	Back							

	Session Border Controller						Û ▲ a
SolutionsLab-vSBC-2 SCZ9.0.0 Pat	tch 4 (Build 343)			Dashboard	Configuration	Monitor and Trace	Widgets
Configuration View Configurati	on Q					Discard	🕸 Verify
session-group	Modify SIP Interface						Show Confi
session-recording-group							
session-recording-server	Displaying 1 - 1 of 1 Initial Inv Trans Expire	10		(Dange () 21/17/173)			
sip-config	Session Max Life Limit	0					
sip-feature	Proxy Mode		▼				
sip-interface	Redirect Action						
sip-manipulation	Nat Traversal	none	•				
sip-monitoring	Nat Interval	30		(Range: 04294967295)			
translation-rules Show All	TCP Nat Interval	Back		(Danne: N. 8208067205)			

		Session Border Controller						ė	
	SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace								
C	View Configuration	n Q					Discard	🕸 Verify	
	session-group	Modify SIP Interface						Show Conf	
	session-recording-group								
	session-recording-server	S8hr Profile		T					
	session-translation	Ringback Trigger	none	W					
	sip-config	Ringback File							
	sip-feature	Fax Continue Session	none	W					
	sip-interface	Npli Profile		W					
	sip-manipulation	Hist To Div For Cause 380	inherit	T					
	sip-monitoring	User Agent	Oracle/VM/9.0.0p4						
	translation-rules	Allow Diff2833 Clock Rate Mode	disabled						
	Show All	OK	lack						

We have some mandatory sip-manipulations that needs to be used with the Oracle SBC so that call flow between Cisco Webex and PSTN will be successful. The User can add these sip manipulations to the SBC using either GUI or CLI mode and is free to decide the way they want to add the sip manipulations. As per the request of Cisco, the FQDN of the SBC needs to be added to all sip messages toward Cisco Webex. Please assign the sip-manipulation as the out-manipulation ID in the Cisco Webex sip interface or Cisco Webex Session Agent as per customer need. The actual sip-manipulation is given under the sip-interface of the Multi-tenancy section of this App note to avoid redundancy.

ORACLE Enterprise Ses	sion Borde	r Contro	ller									Û 🔺	admin 🔻
SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4	(Build 343)							Dashboard	Configuration	Monitor and Tr	ace	Widgets	System
Configuration View Configuration	Q									Dis	card	😧 Verify	🖹 Save
session-agent	Modify	SIP In	terface									Show Con	figuration
session-group	Charles .												
session-recording-group	State			🗸 enabl	le								
session-recording-server	Realm ID			SIPTrunk	(•							
session-translation	Descripti	on											
sip-config													
sip-feature	CID Dorte												
sip-interface		/ [) 🗇										
sip-manipulation	Action	Select	Address		Port	T	Fransport Protocol	TLS Profile	Allow And	onymous	Multi H	ome Addrs	
sin-monitoring	:		155.212.214.90		5060	U	JDP		agents-on	ly			
translation_rulos	:		155.212.214.90		5060	T	ГСР		agents-on	ly			
system				- di									
Show All			OK	BCK									

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

We also have a sip-manipulation for PSTN side to remove DTG parameter which comes from Cisco side which will not be accepted by some of the sip trunks. So, we use the below manipulation to remove it. Please assign the below sip-manipulation as the out-manipulation ID in the PSTN sip interface. Please note that this sip-manipulation can be used according to the needs of the user as some of the sip trunks allow this parameter by default.

sip-manipulation name description split-headers join-headers	RemoveDTG
header-rule name header-name action comparison-type msg-type methods match-value new-value	StripDTG Request-URI manipulate case-sensitive request Invite



element-rule name parameter-name type action match-val-type comparison-type match-value new-value

stripdtg dtg header-param delete-element any case-sensitive

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

6.12. 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.

Go to session-router->Session-Agent and Configure the session-agents for the Cisco Webex side

- Host name to "**us01.sipconnect.bcld.Webex.com**", which is SRV based SA.
- When Using SRV as session agent, please make **port as 0** so that SRV will work properly.
- realm-id needs to match the realm created for the Cisco Webex side.
- transport set to "staticTLS"
- Please enable the parameters **ping all addresses, ping-response**,
- Please enable hidden option load-balance-dns-query and recurse-on-all
 - failures and set out-service-response-codes parameter to 408,503
- Please set ping method to OPTIONS and ping-interval duration in secs.
| | e Session Border Controller | | | | | a |
|----------------------------------|-----------------------------|--------------------------------|----------------------|---------------|-------------------|------------|
| SolutionsLab-vSBC-2 SCZ9.0.0 Pai | tch 4 (Build 343) | | Dashboard | Configuration | Monitor and Trace | Widgets |
| Configuration View Configurati | ion Q | | | | Discard | 😧 Verify |
| local-policy | Modify Session Agent | | | | | Show Confi |
| local-routing-config | | | | | | |
| media-profile | Hostname | us01.sipconnect.bcld.webex.com | | | | |
| session-agent | IP Address | | | | | |
| session-group | Port | 0 | (Range: 0,102565535) | | | |
| session-recording-group | State | ✓ enable | | | | |
| | App Protocol | SIP | | | | |
| session-recording-server | Арр Туре | | | | | |
| session-translation | | • | | | | |
| sin-config | Transport Method | StaticTLS 🔹 | | | | |
| Sip comb | Realm ID | CiscoWebexRealm | | | | |
| sip-feature | Føress Realm ID | | | | | |
| sip-interface | EBICOS REGIMED | T | | | | |
| Show All | OK | Back | | | | |

	Session Border Controller					Ų ▲ a
SolutionsLab-vSBC-2 SCZ9.0.0 Pat	tch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
Configuration View Configuration	on Q				Discard	😧 Verify
local-policy	Modify Session Agent					Show Confi
local-routing-config	Ping Interval	30	(Dange: 0, 4204067205)			
media-profile	Ping Send Mode	keep-alive	(Range, 04274901293)			
session-agent	Ping All Addresses	enable				
session-group	Ping In Service Response Codes					
session-recording-group	Options					
session-recording-server		recurse-on-all-failures X				
session-translation	SPL Options					
sip-config	Media Profiles					
sip-feature	In Translationid	v				
Show All	OK E	Back				

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

	ORACLE Enterprise S	Session Border Controller					a
	SolutionsLab-vSBC-2 SCZ9.0.0 Patc	.h 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
С	onfiguration View Configuration	n Q				Discard	😧 Verify
	local-policy	Modify Session Agent					Show Config
	local-routing-config						
	media-profile	Hostname	68.68.117.67				
	session-agent	IP Address	68.68.117.67				
	session-group	Port	5060	(Range: 0,102565535)			
	session-recording-group	State	✓ enable				
		App Protocol	SIP				
	session-recording-server	Арр Туре					
	session-translation	Transport Mathad	Y				
	sip-config	ITalisport Method	UDP .				
	in factors	Realm ID	SIPTrunk				
	sip-reature	Egress Realm ID					
	sip-interface						
	Show All	OK	3ack				

11/1/2/1/20

ORACLE Enterprise Session Border Controller										
SolutionsLab-vSBC-2 SCZ9.0.0 P	atch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets				
Configuration View Configura	tion Q				Discard	😧 Verify				
local-policy	Modify Session Agent					Show Confi				
local-routing-config		•								
media-profile	Redirect Action	v								
session-agent	Loose Routing	✓ enable								
session-group	Response Map	v								
session-recording-group	Ping Method	OPTIONS								
session-recording-server	Ping Interval	30	(Range: 04294967295)							
session-translation	Ping Send Mode	keep-alive 🔻								
sin-config	Ping All Addresses	✓ enable								
sip comp	Ping In Service Response Codes									
sip-teature	Options									
sip-interface 🔹										
Show All	OK	Back								

Please assign the below mandatory sip-manipulation as the out-manipulation ID in PSTN sip interface or PSTN Session Agent as per customer need.

11111

2///0

sip-manipulation	
name	ToPSTN
description	
split-headers	
join-headers	
header-rule	
name	StripDIG
header-name	Request-URI
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	Invite
match-value	
new-value	
element-rule	
name	stripdtg
parameter-name	dtg
type	header-param
action	delete-element
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	
header-rule	
name	DeleteXBroadworks
header-name	X-BroadWorks-Correlation-Info
action	delete
comparison-type	case-sensitive
msg-type	any
methods	BYE, INVITE, OPTIONS
match-value	
new-value	
header-rule	
name	DeleteSessionID
header-name	Session-ID
action	delete
comparison-type	case-sensitive
msg-type	any
methods	BYE INVITE OPTIONS
match-value	Dre,invire, or nono
new-value	
header-rule	
name	DeleteRecvInfo
header-name	Recv-Info
action	delete
comparison-type	case-sensitive
msg-type	any
methods	BYE,INVITE,OPTIONS

6.13. 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.

///

	Session Border Controller					Û 🔺 🧯
SolutionsLab-vSBC-2 SCZ9.0.0 Pat	ch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
Configuration View Configuration	on Q				Discard	😧 Verify
local-policy	Modify Local Policy					
local-routing-config						
media-profile	From Address	* X				
session-agent	To Address	*×				
session-group	Source Realm	CiscoWebexRealm 🗙				
session-recording-group	Description					
session-recording-server						
session-translation						
sip-config	State	✓ enable				
sip-feature	Policy Priority	none 🔻				
sip-interface Show All	ОК	Back				

ORACLE Enterprise Session Border Controller									Û ▲ a		
SolutionsLab-vSBC-2 SCZ9.0.0 Pa	tch 4 (Build 3	43)						Dashboard	Configuration	Ionitor and Trace	Widgets
Configuration View Configuration	ion Q									Discard	😧 Verify
local-policy	Modify	/ Local	Policy								
local-routing-config	Source R	CiscoWebexRealm 🗙									
media-profile	Descript	ion									
session-agent											
session-group											
session-recording-group	State			 enable 							
session-recording-server	Policy Pr	iority		none		T					
session-translation	Policy At	tributes									
sip-config	D:	/ [
sip-feature	Action	Select	Next Hop	Realm	Action	Terminate	Cost	State	App Protocol	Lookup N	ext Key
cia interface	:		68.68.117.67	SIPTrunk	replace-uri	disabled	0	enabled		single	
Show All			ОК	Back							

To route the calls from the PSTN side to Cisco Webex side, Use the below local-policy

	Session Border Controller					û ▲ a
SolutionsLab-vSBC-2 SCZ9.0.0 Pat	ch 4 (Build 343)		Dashbo	ard Configuration	Monitor and Trace	Widgets
Configuration View Configuration	on Q				Discard	😧 Verify
local-policy	Modify Local Policy					
local-routing-config						
media-profile	From Address	* X				
session-agent	To Address	* X				
session-group	Source Realm	SIPTrunk 🗙				
session-recording-group	Description					
session-recording-server						
session-translation						
sip-config	State	✓ enable				
sip-feature	Policy Priority	none	7			
sip-interface	ОК	Back				

1111111

2///20

	Session Bo	order Co	ntroller								Ô ▲
SolutionsLab-vSBC-2 SCZ9.0.0 Pate	ch 4 (Build 3	43)					D	ashboard Co	onfiguration	Monitor and Trace	Widgets
Configuration View Configuration	on Q									Discard	🕸 Verify
local-policy	Modify	/ Local	Policy								
local-routing-config				SIPTrunk 🗙							
media-profile	Descripti	on									
session-agent											
session-group											
session-recording-group	State			🗸 enable							
session-recording-server	Policy Pri	iority		none		T					
session-translation	Policy At	tributes									
	D:	/ [
sip-config	Action	Select	Next Hop	Realm	Action	Terminate	Cost	State	App Protocol	Lookup N	lext Key
sip-feature	:		us01.sipconn	CiscoWebex	replace-uri	disabled	0	enabled		single	
sip-interface			ОК	Back							

6.14. Configure steering-pool

Steering-pool allows configuration to assign IP address(es), ports & a realm. The port configuration for Webex Calling as the media ports on LGW side is allowed/advertised from port 8000 to 48000 as per Cisco and the End user can define this port range on the Oracle SBC.

Cisco Webex side steering pool.

ORACL	ORACLE Enterprise Session Border Controller											
SolutionsLab-vSBC	-2 SCZ9.0.0 Pat	ch 4 (Build 343)			Dashboard	Configuration	Monitor and Trace	Widgets				
Configuration	View Configuration	on Q					Discard	😧 Verify				
media-manager	*	Modify Steering Pool										
media-manager		IP Address	10.1.3.4									
media-policy		Start Port	10000	(Range: 0,165535)								
realm-config		End Port	20000	(Range: 0,165535)								
		Realm ID	CiscoWebexRealm	•								
steering-pool		Network Interface		v								
security	•											
session-router	•											
system	•											
Show All		ОК В	Back									

PSTN side steering pool.

ORACL	Enterprise	Session Border Controller						6
SolutionsLab-vSBC	C-2 SCZ9.0.0 Pate	ch 4 (Build 343)			Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configuratio	n Q					Discard	😧 Verify
media-manager	▼	Modify Steering Pool						
media-manager		IP Address	155.212.214.90					
media-policy		Start Port	10000	(Range: 0,165535)				
realm-config		End Port	20000	(Range: 0,165535)				
steering-pool		Network Interface	SIPTrunk	v				
security	►							
session-router	►							
system	►							
Show All		ОК В	ack					

6.15. Configure sdes profile

Oracle SBC and Cisco Webex Calling Support the following ciphers for SRTP:

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

AEAD_AES_256_GCM (This cipher is applicable only for Webex for Government as it is FIPScompliant GCM ciphers)

	e Session Border Controller						admin 👻
SolutionsLab- vSBC-2 10.1.1.4 SCZ9.3	5.0 GA (Build 46)		Dashboard	Configuration	Monitor and Trace	Widgets	System
Configuration View Configur	ration 🖺 Q				Discard	😧 Verify	B Save
authentication	Add Sdes Profile				Show Advanced	Show	Configuration
authentication-profile							
cert-status-profile	Name	CiscoSRTP					
certificate-record	Crypto List	AEAD_AES_256_GCM ×					
factory-accounts	Srtp Auth	enable					
local-accounts		enable					
media-security 🗸	Srtp Encrypt	Chable					
dtls-srtp-profile	SrTCP Encrypt	enable					
media-sec-policy	Mki	enable					
sdes-profile	Egress Offer Format	same-as-ingress	•				
sipura-profile	Use Ingress Session Params						
password-policy	Ontions						
security-config	options -						
ssh-config	Кеу						
Show All	OK Back						

Add the below ciphers to the SDES profile as shown below.

AES_CM_256_HMAC_SHA1_80 AES_CM_128_HMAC_SHA1_80 AES_CM_128_HMAC_SHA1_32 (These 3 ciphers is applicable only for Cisco Webex Calling)

	e Session Border Controller					admin 🔫
SolutionsLab- vSBC-2 10.1.1.4 SCZ9.3	3.0 GA (Build 46)	Das	shboard Configuration	Monitor and Trace	Widgets	System
Configuration View Configu	ration 🗈 Q			Discard	😧 Verify	Save
authentication	Add Sdes Profile			Show Advanced	Show	Configuration
authentication-profile						
cert-status-profile	Name	CiscoSRTP				
certificate-record	Crypto List	AES_CM_128_HMAC_SHA1_80 x				
factory-accounts		AES_256_CM_HMAC_SHA1_80 ×				
local-accounts		AES_CM_128_HMAC_SHA1_32 ×				
media-security 🗸	Srtp Auth	enable				
dtls-srtp-profile	Srtp Encrypt	enable				
media-sec-policy	SrTCP Encrypt	✓ enable				
sdes-profile	Mki	enable				
sipura-profile		_				
password-policy	Egress Offer Format	same-as-ingress	•			
security-config	Use Ingress Session Params					
ssh-config	Options					
Show All	OK Back					

////

6.16. 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 CiscoWebexSecurity which will have the sdes profile created above. Assign this media policy to the Cisco Webex Realm

ORACL	E Enterprise Se	ssion Border Controller						a
SolutionsLab-vSBC	-2 SCZ9.0.0 Patch 4	4 (Build 343)			Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configuration	Q					Discard	😧 Verify
certificate-record		Modify Media Sec Policy						
ike	►	Name	CiscoWebexSecurity					
local-accounts		Pass Through	enable					
media-security	v	Options						
dtls-srtp-profil	le							
media-sec-poli	ïcy	▲ Inbound Profile	CisroSPTD =					
sdes-profile		Mode	srtp					
sipura-profile		Protocol	sdes					
password-policy		Hide Egress Media Update	enable					
security-config		Outbound						
ssh-config		Profile	CiscoSRTP 💌					
cch-kav Show All		OK	Back					

Similarly, Create Media Sec policy with name PSTNSide to convert srtp to rtp for the PSTN side. Assign this media policy to the PSTN Realm.

ORACL	E Enterprise Ses	sion Border Controller						a
SolutionsLab-vSBC-	2 SCZ9.0.0 Patch 4	(Build 343)			Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configuration	Q					Discard	😧 Verify
certificate-record								
factory-accounts		Modify Media Sec Policy						
ike	•	Name	PSTNSide					
local-accounts		Pass Through	enable					
media-security	•	Options						
dtls-srtp-profile								
madia cas poli		Inbound						
meula-sec-poin	- Y	Profile	v					
sdes-profile		Mode	rtp	7				
sipura-profile		Protocol	none	·				
password-policy		Hide Egress Media Update	enable					
security-config		Outbound						
ssh-config		Profile	v					
cch_kou								
Show All		OK	lack					

6.17. Configure Media Optimization (ICE-profile)

Please go to \rightarrow media-manager \rightarrow Select show all option \rightarrow ICE-profile and create a new profile as below:

Please enable the parameter **rtcp-stun** which is disabled by default.

This is the new parameter introduced in 9.3.0 release to support media optimization feature and this is supported from release 9.3 and later. Assign this profile to the Cisco Webex Realm.

Please note that this configuration is used only for media optimization feature.

	e Session Border Controller					admin 👻
SolutionsLab- vSBC-2 10.1.1.4 SCZ9.3	3.0 GA (Build 46)	Dash	board Configuration	Monitor and Trace	Widgets	System
Configuration View Configu	ration 🛅 Q			Discard	😧 Verify	Save
codec-policy	Modify Ice Profile			Show Advanced	Show	Configuration
dns-alg-constraints						
dns-config	Name	webexice]			
ice-profile	Stun Conn Timeout	0	(Range: 09999)			
media-manager	Stun Keep Alive Interval	10	(Range: 0300)			
media-policy	Stun Rate Limit	15	(Range: 099999)			
msrp-config						
playback-config	Mode	NONE				
realm-config	RTCP Stun	enable				
realm-group						
rtcp-policy						
static-flow						
steering-pool						
tcp-media-profile						
Show All	OK Back					

11/17/100

	e Session Border Controller						admin 👻
SolutionsLab- vSBC-2 10.1.1.4 SCZ9.3	5.0 GA (Build 46)		Dashb	oard Configuration	Monitor and Trace	Widgets	System
Configuration View Configur	ration 🖺 Q				Discard	Ø Verify	B Save
media-manager 🗸 🗸	Modify Realm Config				Show Advanced	Show	Configuration
codec-policy	0-5 5	enable					
dns-alg-constraints	QUS Enquie			(D			
dns-config	Max Bandwidth	0		(Range: 0.9999999999)			
ice-profile	Max Priority Bandwidth	0		(Range: 0999999999))			
media-manager	Parent Realm		•				
media-policy	DNS Realm		•				
msrp-config							
playback-config	Media Policy		•				
realm-config	Nsep Media Policy		•				
realm-group	Media Sec Policy	CiscoWebexSecurity	•				
rtcp-policy	RTCP Mux	enable					
static-flow	Ice Profile	webexice	•				
steering-pool	L			1			
Show All	OK Back						

With this, SBC configuration is complete.

7. Existing SBC configuration

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

- New realm-config
- Configuring a certificate for SBC Interface
- TLS-Profile
- <u>New sip-interface</u>
- New session-agent
- <u>New steering-pools</u>
- New local-policy
- SDES Profile
- Media-sec-Policy
- Media-Optimization

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

8 SBC Scaling

For SBC scaling, Oracle has released the below values recently and these values are derived based on certain conditions and the table is given below with the values of each platform. These values can be taken as reference and these values may differ when the users are using specific conditions like integrating with Cisco Webex with single tenancy, multi-tenancy, etc.

Feature	Virtualized SBC*	AP1100	AP3950	AP4900	AP6350
Form factor	Virtualized	1U System	1U System	1U System	3U System
System Architecture	Data Centre /COTS	Purpose Built	Purpose Built	Purpose Built	Purpose Built
Max. Media Sessions	60,000	360	10,000	40,000	160,000
Max. SRTP Call Legs	19,000	360	10,000	16,000	120,000
Max. SIPREC Sessions	19,000	180	7,500	12,000	40,000
Max. Transcoded Sessions (G711 <-> G729)	3,200**	360	6,500	6,500	58,000
Max. Calls Per Second	2,000	30	100	600	1,700
* VM configuration c ** Software transcod	lependent ling				

9. Oracle SBC integration with Cisco Webex Contact Center

Cisco Webex Contact Center is a Software-as-a-Service (SaaS) offering that provides the significant advantages of cloud delivery. Cisco Webex Contact Center is a cloud-based enterprise Contact Center solution that can help any organization unlock higher levels of agility, flexibility, scalability, innovation, and customer success.

Cisco Webex Contact Center gives you control over every incoming and outgoing interaction from a central point, regardless of organization, technology, or location. The voice processing is performed in the cloud, and we need to route calls in and out of the cloud. It knows which agents, teams, sites, and partners are available at any given time and sends each interaction to the agent with the best identified skills for handling an issue.

The Key advantages of Cisco Webex CC are listed below:

- Native cloud
- Omnichannel
- Skills-based routing
- Agent and expert collaboration etc

For additional information on Cisco Webex Contact Center, please check the below links:

https://help.webex.com/en-us/article/nee1mb6/Get-started-with-Webex-Contact-Center

https://help.webex.com/en-us/article/utqcm7/Webex-Contact-Center-Architecture

https://help.webex.com/en-us/article/n5595zd/Webex-Contact-Center-Setup-and-Administration-Guide

The Oracle SBC is fully certified to seamlessly integrate with Cisco Webex Contact Center. If your Oracle SBC is already configured for Cisco Webex Calling LGW SIP trunking, no additional SBC configuration is required. To leverage Cisco Webex Contact Center, customers simply need to obtain the necessary licenses. Once activated, the Contact Centre feature set will be accessible through the existing Cisco Webex admin portal.

While Cisco Webex Contact Center supports voice, email, and chat, this document will primarily focus on the voice integration between the Oracle SBC and Cisco Webex Contact Center.

Once Webex CC license is enabled, we will have additional tab for Contact center in Cisco Webex admin portal as shown below. After you click the tab, we will see options to configure Webex CC configuration in the next page. This App note focusses on the basic configuration of Cisco Webex contact center which can be configured on the Cisco Admin portal as shown below. More detailed configuration of Cisco Webex CC may be required based on the customer needs for the proper working of Webex contact center. For such configuration, please consult your Cisco representative which will be out of scope of this document. Webex admin page with Contact Center tab enabled:

≡ webex Control Hub	Q. Search	🕐 🗘 🕅 🗳 csu
Apps	Overview	
合 Security 豪 Organisation settings	Here's how to get the most out of Web Meetings experience Strengthen security	ex!
SERVICES C Updates & Migrations Messaging	Provide a powerful meeting experience You'll see all engagement data here when your users sta engagement, you'll also see data trends.	art using Webex. After 60 days of
Calling	Goal Promote human connection through video collaboration	Goal Upgrade meeting experiences with Messaging
Vidcast Contact Centre	Is this helpful? 👌 🖓 🖉	
 Connected UC Hybrid 	Set-up guide Updates	New offers

9.1. Enable the Users with Webex CC license

After The first step is to enable the Webex CC license for the users. Please login to **Cisco Webex control hub portal – Management ---- Users** and enable the license for the users that you wish to as shown below:

≡ webex Control Hub				😋 🗘 🕐 🗳 csl
	Users			
MONITORING	Ciscousers1 Active + ciscouse	rs1@outlook.com · Member of B	urlingtonHQ	Actions ~
In Analytics☑ Troubleshooting	Summary Profile General	Meetings Calling Messagi	ng Hybrid Services Devices Vidcast	
 Reports Customer Journey D 	User details	Name	ciscousers1	
MANAGEMENT		Primary email	ciscousers1@outlook.com	
<mark>දි, Users</mark> දී Groups		Preferred email language ()	English - American English V	
 Locations Workspaces 		Name labels	Using location settings Status: Not enrolled Organisation Setting	: Off 🛈
🖨 Devices				

≡ webex Control Hub	Q Sea	rch		C	¢ (୭ 🗳
 ⊖ Overview ↓ Alerts centre 	ළ ciscousers1	Summary Profile General	Meetings Calling Messaging	Hybrid Services	>>	Action
MONITORING	Licences	 Messaging Meeting 	Basic messaging Basic space meetings			
Analytics Troubleshooting Reports		& Calling	Call on Webex (1:1 call, non-PSTN Webex Calling Professional	4)		
Q Customer Journey D		Edit licences				
MANAGEMENT	Administrator roles	None				>

Edit services fo	r ciscousers1@outlook.	som	
	Ø Messaging	Basic messaging	
	🗎 Meeting	Basic space meetings	
	& Calling	Call on Webex (1:1 call, non-PSTN) Webex Calling Professional	
			Л
			Cancel Edit licences

Please click on Contact Center Tab and Enable the Agent type as shown below. The Agent types are Standard Agent, Premium Agent and Premium Agent with Supervisor role. Please select the appropriate agent as per your requirements and you can also select the Agent who can also be the Admin for the Webex CC.

Click Save to enable the changes made and you can do the same procedure for other users which can be the Agents for the Webex CC.

Edit services for cisco	users1@outlook.com	
	Edit services for ciscousers1@outlook.com	
	Select the service entitlements that you want to provide to this user. O Messaging Subscription: Basic messaging Subscription: Basic messaging 	
	Meeting Acceleration Meeting Acceleration Subscription: Enterprise trial 1 - 06/16/2022	
	Calling Calling Advanced messaging Contact Centre	
	Customer (0) experience	
		Cancel Save

////

Edit services for ciscousers1	@outlook.com		
	Edit services for cise Select the service entitlements Messaging 1 Meeting 1 Calling 2 Contact Centre 1 Customer 0 Customer 0	that you want to provide to this user. A Subscription: Enterprise trial 2 - 09/11/2024 E Licensed agent Standard Agent Premium Agent Premium agent – Supervisor role Administrator	
			Cancel Save

9.2. Synchronize the Users with Webex CC tenant.

Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- Tenant Settings** --- **General and click on Synchronize Users tab** so that the changes made to Users will be reflected in Cisco Webex CC page. We can also change the time zone from this page and other options can be left default in this page.

≡ webex Control Hub		Q Search	ତ ଠ ତ 🗳
Multimedia profiles Gel	neral		
Outdial ANI		Strategies.	
Desktop layouts		Go to the Webex Contact Centre	Management Portal
Dial plans			
Address books	and the late of the second	Van must aurebrezies Meheu use	re with Centest Centre liesees is order to successfully easies Centest Centre user avialiance
Desktop profiles	ynchronise Users	Fou must synchronise webex user	s with contact centre licences in order to successfully assign contact centre user privileges
Idle/wrap-up codes		Synchronise Users	
		Δ	
TENANT SETTINGS		U	
General	ervice Details	Country of operation	United States of America
Security		Tenant timezone	(OMT.05:00) America (Maus Vark -) (
Voice			(0M1-05-00) America/New_Tork
Digital			Changes to this field will only affect your voice channels and will not impact your digital channels, even if you have digital channels already set up.
Desktop			
Integrations		Platform details	Webex Contact Centre
Bulk operations		Disitel shannel	
Add-ons		Digital Channel	Webex Connect
Cloud Connect		Voice media platform	Real-time media service

9.3. Configure the settings in Security Tab.

Please go to Cisco Webex control hub portal – Services ---- Contact Center ---- Tenant Settings ---- Security and do the following settings.

- Enable the Recording Pause/Resume Enabled under Privacy shield tab
- Disable the Chat and Email and Attachments as we are dealing only with Calling option here.

	rol Hub	Q Search 🕐 🗘 🕐 🗳 🖙	SL
Multimedia profiles	Security		
Outdial ANI Desktop layouts			
Dial plans	Privacy shield	Allows agents to pause call recording while obtaining sensitive information, such as credit card details.	
Address books Desktop profiles	_	×	
Idle/wrap-up codes		Recording pause/resume enabled	
TENANT SETTINGS			
General	Chat and Email	Enable/Disable sending attachments via chat and emails. This applies to both agents and customers.	
Security	Attachments	×	
Voice			
Digital Desktop	Security settings for chat and email	Choose from the following options to secure confidential customer data This selection would apply to chat and email content. Note that attachments containing confidential user information will always be	
Integrations		dropped.	
Bulk operations		Redact	
Cloud Connect	2	Redact confidential user information from chat and email content. Drop Drop chat and email messages which contain confidential information.	

9.4. Configure the settings in Voice Tab.

Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- Tenant Settings** --- **Voice** and provide a DID for default out dial ANI. This is the default number which will be used to call Webex CC from outside and will reach the IVR prompt.

We also need to enable WebRTC so that we will get an Webex CC option of Agent Desktop.

webex Control Hul	b	Q Search		٢	¢ @ ₽ 😋
User profiles Contact centre users	Call settings Contact number	r			
DESKTOP EXPERIENCE Multimedia profiles	Call Settings	Short call threshold	0 seconds		
Outdial ANI Desktop layouts		Sudden disconnect threshold	30 seconds		
Dial plans Address books		Default Outdial ANI	+17812032808 ~		
Desktop profiles Idle/wrap-up codes		Record all calls			
TENANT SETTINGS	Concurrent voice call details	Entitlements O	300 Licences		
Security		Surge percentage ①	30 Per cent		
Voice		Maximum threshold ©	390 Concurrent calls		
Desktop Integrations	WebRTC	This enables Web Real Time-Communication for your or	ganisation. This will allow your agents and s	supervisors to make or receive calls using the browser by	selecting the
Add-ons		Desktop option under Station Credentials inside the Age	nt Desktop. For the list of supported brows	ers, refer to the System requirements for Agent Desktop	article.

9.5. Configure the Multimedia Profile Tab.

Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- Desktop Experience** --- **Multimedia Profile** and create a multimedia profile for the Agents. The configuration in this tab allows agents to handle multiple contacts in different channel types simultaneously. For our profile, we have selected the simultaneous calls as 1 and we do not deal with other options and hence the options are set to zero for those options.

= webex Cont	rol Hub		Q Sea	rch 🕐 🗘 🕐 🗳
USER MANAGEMENT	^ <	Helpdesk		54 💽 û
Sites				
Skill definitions		General	Name *	Helpdesk
Skill profiles			Description	
Teams			Description	Helpdesk Multimedia Profile
User profiles			Referenced by	You can access following link to see which other entitles are referenced.
Contact centre users				Reference list
DESKTOP EXPERIENCE				
Multimedia profiles		More Details	Select one from the following	options.
Outdial ANI			Blended	
Desktop layouts			 Blended real time 	
Dial plans			 Exclusive 	
Address books			This option allows agents to h	handle multiple contacts in different channel types simultaneously. Select the number of simultaneous contacts per channel type.
Desktop profiles				
Idle/wrap-up codes			Voice	
			Chat	
TENANT SETTINGS			GHA	0 ~
General			Email	
Security				
Voice			Social	0 ~
Digital				

9.6. Configure the Desktop Profile Tab.

Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- Desktop Experience** --- **Desktop Profile** and create a Desktop profile for the Agents as shown below:

1/18

= webex Control	l Hub	Q Se	earch	° ¢ 0 f
Skill profiles	< Desktop profiles			
User profiles Contact centre users	Agent-Profile ID: e1e100f5-c0c3-4212-a829-1	973c0bb93c16 - Last Modi	tiffed: September 17, 2024 18:57 pm	a 💽 Active
DESKTOP EXPERIENCE Multimedia profiles	General Idle/wrap-up co	odes Collaboration	Dial plans Voice channel options Agent statistics Desktop timeout	
Outdial ANI Desktop layouts	General	Name *	Agent-Profile	
Dial plans Address books		Description	Agent profile	
Desktop profiles Idle/wrap-up codes		Parent type	Tenant V	
		Screen pop-ups		
General		Last agent routing	8	
Security		Auto answer		
Digital Desktop		Referenced by	You can access following link to see which other entities are referenced.	
Integrations Bulk operations				

Please click Voice channel options and select the options as shown below.

= webex Control H	Hub	Q. Search	o 🗘 🕐 💕
Skill profiles	< Desktop profiles		
User profiles Contact centre users	Agent-Profile ID: e1e100f5-c0c3-4212-a829-973	:0bb93c16 · Last Modified: September 17, 2024 18:57 pm	a 💽 Active
DESKTOP EXPERIENCE Multimedia profiles	General Idle/wrap-up code	s Collaboration Dial plans Voice channel options Agent statistics Desktop timeout	
Outdial ANI Desktop layouts Dial plans Address books Desktop profiles Idle/wrap-up codes	Voice channel options	The One Voice option must always be selected. Agent DN Extension Desktop Validation for Agent DN Urrestricted fallow any value)	
TENANT SETTINGS		Provisioned DN (restrict the login DN to a provisioned agent DN) Validate using dial plans (select from list)	

9.7. Configure the Idle/Wrap-up codes Tab.

Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- Desktop Experience** --- Idle/Wrap-up codes and create a new profile for the Agents as shown below.

≡ webex Control	ol Hub	Q Search	
Teams	< Idle/wrap-up codes		
User profiles			
Contact centre users	Sale		
	ID: 4d58ff45-1246-430c-b42e-5	9441ae0b7156 • Last Modified	: September 11, 2024 23:58 pm
DESKTOP EXPERIENCE			
Multimedia profiles			
Outdial ANI	General	Name *	Cala
Desktop layouts			Sale
Dial plans		Description	Default wrap-up code
Address books			
Desktop profiles		Make it default	
Idle/wrap-up codes		Codo tupo *	
		code type	Default Wrapup Work Type 🗸
TENANT SETTINGS		Referenced by	There are no references available.
General		-	Reference list
Security			

9.8. Configure the Sites Tab.

Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- User Management** --- **Sites** and create a new site. Please assign the Multimedia profile which is created previously to the created site as shown below.

≡ webex Control H	lub	Q. Sea	irch	⁰ \$ ⑦ ₫
Overview	< Sites			
customer experience Channels Queues	Corporate HQ ID: df1da79b-079a-4eb8	-bdad-9740a5b7c1b8 • Last Modil	lied: September 17, 2024 07-41 am	C C Active
Business Hours Audio prompts Flows Surveys	General	Name * Description	Corporate HQ Corporate HQ Site	
USER MANAGEMENT Sites Skill definitions Skill profiles		Multimedia profile *	Helpdesk Vou can access following link to see which other entities are referenced. Reference list	
Teams User profiles Contact centre users				

9.9. Configure the Skill Definitions Tab.

Please go to Cisco Webex control hub portal – Services ---- Contact Center ---- User Management --- Skill Definitions and create a new Skill profile as shown below.

≡ webex Contro	ol Hub	Q Search		<mark>0</mark> ¢ (2 💕
^	< Skill definitions				
CUSTOMER EXPERIENCE					
Channels	Helpdesk			ñ 🂽	Active
Queues	ID: e702fd7e-79b	I-4112-b359-705b9fa4076a • Last Modif	ïed: September 17, 2024 07:42 am		
Business Hours					
Audio prompts					
Flows	General	Name *	Helpdesk		
Surveys		Description	Helpdesk Skill		
USER MANAGEMENT		Type *	PROFICIENCY		
Sites		Service-level threshold ()	20 Seconds		
Skill definitions			30		
Skill profiles		Referenced by	There are no references available.		
Teams			Reference list		
User profiles					

9.10. Configure the Contact Center Users Tab.

Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- User Management** --- **Contact center users** and you will see the users that has Webex CC license enabled and synchronized with Webex CC listed here. We can go ahead and edit the users and can assign the profiles which we have created previously to the users as shown below.

■ webex Control Hub			♥ ↓ ⑦	
Surveys	cisco users1			ctive
USER MANAGEMENT	ID: de5c55e6-84d4-48e8-94	41a-9b2f7dea0081 🔹 Last Modi	fied: October 21, 2024 11:42 am	5070
Sites				
Skill definitions	General	First name	cisco	
Skill profiles				-
Teams		Last name	users1	
User profiles		Email	ciscousers1@outlook.com	
Contact centre users		User Profile *	Premium Agent U 🗸	
DESKTOP EXPERIENCE		Contact Centre *		
Multimedia profiles				-
Outdial ANI		Referenced by	You can access following link to see which other entities are referenced.	
Desktop layouts			Reference list	
Dial plans				
Address books				

≡ webex Control	ol Hub		Q. Search		o ¢	ĵ ₽
Surveys	< c	isco users1				
USER MANAGEMENT		Agent settings	Site *	Corporate HQ V		
Sites Skill definitions			Teams	Helpdesk ×		
Skill profiles Teams					~	
User profiles				1 Teams	Clear All	
Contact centre users			Desktop profile *	Agent-Profile V		
DESKTOP EXPERIENCE			Multimedia profile	Helpdesk V		
Multimedia profiles Outdial ANI			Skill profile	Helpdesk V		
Desktop layouts Dial plans			Default DN			
Address books Desktop profiles			External ID			

With this, the basic configuration steps of Webex CC are complete.

After the basic Cisco Webex CC configuration is complete, agent login can be performed using the below link.

https://desktop.wxcc-us1.cisco.com/

Agents of Cisco Webex CC mainly works in 3 modes after login which is shown below.

Saturon Credentials Select your telephony option () Dal Number Extension Desktop International Dialling Formal () () International Dialling Formal () () I	Statuon Crédéridais Select your telephony option ① Dial Number Setteration Desktop 2001 Desktop Cancel Cancel Submit	Station Credentials Select your telephony option ① Dial Number Extension ① Desktop allows to receive inbound calls and make outdial calls through the internet. Team Team_cpallou Ramember My Credentials Cance Submit
elect Dial Number for: PSTN based Agent On Premise Telephony	Select Extension for:Webex TelephonyWebex App	Select Desktop for: • WebRTC

< -	C C desktop.wxcc-us1.cisco.com		
©	Webex Contact Center		۵
G			
		Station Credentials	
		Select your telephony option (i)	
		 Dial Number Extension Desktop 	
		International Dialling Format ()	
	Al	Dial Number	
	1	Team	
	No tasks	(Helpdesk x	
		Remember My Credentials	
		Cancel Submit	

Following are the important test cases that have performed for Webex CC on top of the extensive test cases used for certifying the SBC with Cisco Webex LGW. We have tested the voice calls getting routed to the Agent using Oracle SBC and the below test cases are working fine for all the above 3 modes.

Test Case	Description
1	Basic Call w/ 2way Audio
2	Hold/Resume MOH from WxCC
3	Hold/Resume from ENT IP Phone
4	Mute/Unmute from ENT IP Phone
5	Consult Conference to a 2 nd Agent
6	Consult Transfer to a 2 nd Agent
7	Blind Transfer to a 2 nd Agent

Appendix A

Configure Multi-Tenancy

Multi-tenant configuration is primarily to host more than one trunk or locations on the given LGW or in the SBC. There are 2 types of configuration here which is given below:

- Different IP different FQDN
- Same IP different FQDN

These are optional configuration, and the customer can configure this configuration based on their needs.

The configuration steps and the screenshots for the 1st type is shared below

Add New Child Realm:

Add another realm to the configuration, identical to the CiscoWebexRealm. Add the trunk-context field which will now have the hostname of the new tenant which is created. You will also need to assign the CiscoWebexRealm as the parent-realm

ORACL	E Enterprise	e Session Border Controller					Û 🖌
SolutionsLab-vSBC	-2 SCZ9.0.0 Pai	tch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configurati	ion Q				Discard	😧 Verify
media-manager	Ŧ	Modify Realm Config					
media-manager		Identifier	Cisco_Tenant_2				
media-policy		Description					
realm-config							
steering-pool		Addr Prefix	0.0.0.0				
security	•	Network Interfaces	s1p0:0.4 🗙				
session-router	•	Media Realm List					
system	•						
		Mm In Realm	✓ enable				
Show All		OK	Back				

ORACL	E Enterprise	Session Border Controller						
SolutionsLab-vSB0	C-2 SCZ9.0.0 Pat	tch 4 (Build 343)			Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configurati	ion Q					Discard	😧 Verify
media-manager	•	Modify Realm Config						
codec-policy		Max Priority Bandwidth	0		(Range: 0999999999)			
media-manager		Parent Realm	CiscoWebexRealm	Ŧ				
media-policy		DNS Realm		v				
realm-config		Media Policy		v				
steering-pool		Media Sec Policy	CiscoWebexSecurity					
security	•	RTCP Mux	enable					
session-router	•	Ice Profile		v				
system	•	Teams Fqdn						
		Teams Fqdn In Uri	enable					
Show All		ОК	Back					

ORACL	E Enterprise	Session Border Controller					ė
SolutionsLab-vSBC	-2 SCZ9.0.0 Pat	ch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
Configuration	View Configuration	on Q				Discard	😧 Verify
media-manager	*	Modify Realm Config					
codec-policy		Deny Period	30	(Range: 04294967295)			
media-manager		Session Max Life Limit	0	, ,			
media-policy		Untrust Cac Failure Threshold	0	(Range: 04294967295)			
realm-config		Subscription Id Type	END_USER_NONE				
steering-pool		Trunk Context	vmsbc.cgbusolutionslab.com				
security	•	Early Media Allow					
session-router	•	Enforcement Profile					
system		Additional Prefixes					
system	r						
		Restricted Latching	none				
Show All		ОК	Back				

Add New SIP Interface for the child Realm

Please add a new sip-interface for the child realm.

Create a new tls-profile that includes the certificate for new tenant created above.

ORACLE Enterprise Session Border Controller							Û 🔺			
SolutionsLab-vSBC-2 SCZ9.0.0 Patc	SolutionsLab-ySBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace Wite								Widgets	
Configuration View Configuratio	n Q								Discard	😧 Verif
session-agent	Modify	/ SIP Ir	terface							Show C
session-group	C 1.1									
session-recording-group	State		✓ e	nable						
session-recording-server	Realm ID		Cisc	p_Tenant_2	•					
session-translation	Descripti	on								
sip-config										
sip-feature	SIP Ports									
sip-interface	D:	1	II							
sip-manipulation	Action	Select	Address	Port		Transport Protocol	TLS Profi	le	Allow Anonymous	Multi I
sin monitoring	:		10.1.5.4	5067		TLS	TLSWebe	x_MultiTenancy	agents-only	
ah-unununuR										1
Show All			OK Back							

The End user can use the below sip manipulation to change certain parameters when configuring multitenancy and the scenarios should work fine without any issues. **Please assign this as out-manipulation ID to the sip-interface created above**. The User can add these sip manipulations to the SBC using either GUI or CLI mode and is free to decide the way they want to add the sip manipulation.

sip-manipulation	
name	To_Webex
header-rule	
name	ChangePAI
header-name	P-Asserted-Identity
action	manipulate
comparison-type	pattern-rule
methods	INVITE
element-rule	
name	ChangePAI
type	uri-host
action	replace
new-value	<pre>\$TRUNK_GROUP_CONTEXT</pre>
header-rule	
name	ChangeToIP
header-name	ТО
action	manipulate
comparison-type	pattern-rule
msg-type	out-of-dialog
methods	INVITE

element-rule name ChangeTo type uri-host action replace new-value "us01.sipconnect.bcld.Webex.com" header-rule name ChangeContactHost header-name Contact manipulate action out-of-dialog msg-type methods INVITE, ACK element-rule name contacthost type uri-host action replace \$TRUNK_GROUP_CONTEXT new-value header-rule **AddContactOptions** name Contact header-name add action msg-type request methods **OPTIONS** new-value <sip:ping@"+\$TRUNK_GROUP_CONTEXT+":5061;transport=tls> header-rule ChangeFromIP name FROM header-name manipulate action out-of-dialog msg-type methods INVITE element-rule ChangeFrom name uri-host type action replace new-value **\$TRUNK_GROUP_CONTEXT** header-rule Addplus1Contact name header-name Contact manipulate action comparison-type pattern-rule element-rule Tendigits name type uri-user action replace comparison-type pattern-rule ^[0-9]{10}\$ match-value \+1+\$ORIGINAL new-value element-rule name ElevenDigits uri-user type action replace comparison-type pattern-rule ^[0-9]{11}\$ match-value \++\$ORIGINAL new-value

Add New Local Policy

Add new local policy which is matching on the DID's assigned to the users in the second tenant to properly route inbound calls as below:

////

	e Session Border Controller					Û 🔺
SolutionsLab-vSBC-2 SCZ9.0.0 Pat	tch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
Configuration View Configuration	ion Q				Discard	😧 Verify
ldap-config	Modify Local Policy					
local-policy						
local-routing-config	From Address	*X				
media-profile	To Address	17815551212 × 17815551213 ×				
session-agent						
session-group	Source Realm	SIPTrunk 🗙				
session-recording-group	Description					
session-recording-server						
session-translation						
sip-config	State	enable				

ORACLE Enterprise Ses	sion Borde	r Contro	ller									Û 🗕
SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4	(Build 343)								Dashboard	Configuration	Monitor and Trace	Widgets
Configuration View Configuration	Q										Discard	😧 Verify
Idap-config	Modify	/ Local	Policy									
local-policy	Source R	ealm		CIDTevels M								
local-routing-config				SIPTIUNK X								
media-profile	Descripti	on										
session-agent												
session-group	State			🗸 enable								
session-recording-group	Policy Pr	iority		none		v						
session-recording-server	Policy At	tributes										
session-translation												
sip-config	Action	Select	Next Hop	Realm	Action	Terminate	Cost	State	App Protoc	ol Lookup	Next Key	Auth U
sip-feature	:		us01.sipconn	Cisco_Tenant_2	replace-uri	disabled	0	enabled		single		
Show All			ОК	Back								

Finally, change the realm ID in the SRV session agent to * for multitenancy to work in both types. When making the above change, please make sure to add a home realm to the global sip config

	e Session Border Controller					a
SolutionsLab-vSBC-2 SCZ9.0.0 Pa	atch 4 (Build 343)		Dashboard	Configuration	Monitor and Trace	Widgets
Configuration View Configurat	ion Q				Discard	😧 Verify
ldap-config						
local-policy	Modify Session Agent					Show Config
local-routing-config	Hostname	us01.sipconnect.bcld.webex.com				
media-profile	IP Address					
session-agent	Port	0	(Range: 0,102565535)			
session-group	State	✓ enable				
session-recording-group	App Protocol	SIP	7			
session-recording-server	Арр Туре		7			
session-translation	Transport Method	StaticTLS	Ŧ			
sip-config	Realm ID	*	v			
sip-feature	Egress Realm ID		T			
Show All	ОК	Back				

With this, the SBC config for Multitenancy with Different IP different FQDN is complete.

For multitenancy with same IP which is the 2nd type, the user **just has to remove the second sip interface that was configured for the new tenant**. Leave the local policy that was configured earlier for 1st type, and that should work since the calls will egress over the same IP but using a child realm as next hop.

Also, leave the session agent with * as the realm ID as shown in the above screenshot.

For this model, please create a single certificate with 2 SAN entries using the parameter -----→ alternate-name.

The details of this parameter is given below with an example:

-->The alternate name of the certificate holder which can be expressed as an IP address, DNS host, or email address. Configure this parameter using the following syntax to express each of these 3 forms.

ORACLESBC(certificate-record)# alternate-name

IP:10.2.2.2, IP:10.3.3.3, DNS:bar.example.com, DNS:foo.example.com

(Note each entry is comma separated)

Appendix B

As Cisco doesn't support any other clock rate other than 8K for DTMF and if the customer wants to use OPUS codec(48K) with Cisco WebEx Calling, there is a new feature added to the SBC 9.1p2 version or higher which will solve this problem. The feature name is **Separate Clock Rates for Audio and Telephone Events** and this feature is applied only when using OPUS codec with Cisco WebEx Calling.

If the customer is using SBC version other than 9.1p2 or higher, (For Ex, SBC 9.0 or 8.4 versions etc) then they may face DTMF issue as the feature is not available in those releases. For more information about this feature, please check the given <u>link</u> with the feature name given above.

10 Caveat

Issue 1: SIP OPTIONS ping from multiple Realms to global session agents.

Cisco requires SBC vendors to send SIP OPTION ping (keepalives) from all realms in multi-tenant UCaaS environment that contains the FQDN of each trunk to monitor the connection health between the SBC and customer tenant.

The Oracle SBC has a limitation of the above requirement as of now and the SBC can only successfully monitor a single customer tenant based on the current behavior of SIP OPTIONS ping. SBC still will respond locally to all OPTIONS sent from Cisco to the SBC on all trunks in a multitenancy environment, and our testing showed no interruption in calling service due to this limitation.

Oracle Engineering is working on an enhancement request to create the ability for the SBC to send SIP OPTIONS ping (keepalives) from multiple Realms to global session agents. This enhancement will be available in future SBC release (exact release not identified as of now) and this app note will be updated accordingly once the release is available. There are some workarounds that have been successful in customer environments. Please reach out to your account team to discuss what available options may be best suited for your particular environment.

Issue 2: Video Call issues when call comes from Cisco CUCM towards Cisco WebEx.

Some of the customer was having issues with establishing video between on prem CUCM and Webex Calling while using Oracle SBC as LGW and this issue happens because of how video starts or is handled. This issue is resolved after removing the below headers from the SDP video attribute coming from Cisco CUCM side and going towards Cisco WebEx side.

a=rtcp-fb:* nack pli a=rtcp-fb:* ccm fir a=rtcp-fb:* ccm tmmbr

We have created the below sip-manipulation which will remove these headers and this sip-manipulation needs to be applied towards Cisco WebEx side.

mime-sdp-rule	
name	Changealine
msg-type	any
methods	Invite
action	manipulate
comparison-type	pattern-rule
match-value	
new-value	
sdp-media-rule	
name	deleteattributes
media-type	video
action	manipulate
comparison-type	pattern-rule
match-value	
new-value	
sdp-line-rule	
name	deletertcp
type	a
action	delete
comparison-type	pattern-rule
match-value	(rtcp)(.*)
new-value	

11_ 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.

certificate-record	
name	CGBUSolutionsLab
unit	SolutionsLab
common-name	cgbusolutionslab.com
extended-key-usage-lis	t serverAuth
	clientAuth
certificate-record	
name	CloudSBCSolLab
unit	SolutionsLab
common-name	cloudsbc.cgbusolutionslab.com
extended-key-usage-lis	t serverAuth
	ClientAuth
certificate-record	CoDoddy Oraco Cort
name	
	www.goddddy.com
common-name	Gobaddy GT to G2 Cross Certificate
certificate-record	CoDoddulatormodiato
	Gobaddymiermediale
common-name	GoDaddy Secure Server Certificate - 62
certificate-record	Gobaddy Secure Server Certificate - 62
name	GoDaddyRootCA
unit	www.godaddy.com
common-name	GoDaddy Class 2 Certification Authority Root Certificate
certificate-record	
name	WebexRootCA
common-name	IdenTrust Root CA certificate
http-server	
name	webserver
local-policy	
from-address	*
to-address	*
source-realm	CiscoWebexRealm
policy-attribute	
next-hop	68.68.117.67
realm	SIPTrunk
action	replace-uri
local-policy	
from-address	*
to-address	
source-realm	SIPTrunk
policy-attribute	up01 sincerneet held webey som
realm	CiscoWebeyRealm
action	
action	replace-un

7/11/1/1772/1100

media-manager	
media-sec-policy	
name	CiscoWebexSecurity
inbound	
profile	CiscoSRTP
mode	srtp
protocol	sdes
outbound	
profile	CiscoSRTP
mode	srtp
protocol	sdes
media-sec-policy	DOTNO: I
name	PSINSide
network-interface	
name	SUPU
ip-address	155.212.214.90
netmask	255.255.255.0
gateway	155.212.214.65
network-interface	-1-0
name	stpu 10.1.2.4
ip-address	10.1.3.4
neumask	200.200.200.0
dag in primary	
dno in bookun1	
dns in backup?	
dns. domain	0.0.4.4 cabusolutionslab.com
uns-uomain phy interface	Cybusolulionsiab.com
phy-interface	c0n0
operation-type	Media
nhy-interface	Media
name	s1n0
operation-type	Media
slot	1
realm-config	•
identifier	CiscoWebexRealm
network-interfaces	s1p0:0.4
mm-in-realm	enabled
media-sec-policy	CiscoWebexSecurity
access-control-trust-level	high
trunk-context	cloudsbc.cgbusolutionslab.com
ice-profile	webexice
realm-config	
identifier	SIPTrunk
network-interfaces	s0p0:0.4
mm-in-realm	enabled
media-sec-policy	PSTNSide

sdes-profile	
name	CiscoSRTP
crypto-list	AES_CM_128_HMAC_SHA1_80
	AES_256_CM_HMAC_SHA1_80
	AES_CM_128_HMAC_SHA1_32
	AEAD_AES_256_GCM
srtp-rekey-on-re-invite	enabled
session-agent	
hostname	68.68.117.67
ip-address	68.68.117.67
realm-id	SIPTrunk
ping-method	OPTIONS
ping-interval	3U anoblad
ping-response	enabled
bostnamo	us01 sinceppent held webey com
nort	Ω
transport-method	StaticTLS
realm-id	CiscoWebexRealm
ping-method	OPTIONS
ping-interval	30
ping-all-addresses	enabled
ping-response	enabled
sip-config	
home-realm-id	CiscoWebexRealm
registrar-domain	*
registrar-host	*
registrar-port	5060
options	max-udp-length=0
extra-method-stats	enabled
sip-intenace realm-id	CiscoWebeyRealm
sip-port	CIGCOVEDEXICEAITI
address	10.1.3.4
port	5061
transport-protocol	TLS
tls-profile	TLSWebex
allow-anonymous	agents-only
spl-options	
HeaderNatPublicSipIfIp=20.9	6.25.165,HeaderNatPrivateSipIfIp=10.1.3.4
out-manipulationid	ToCiscoWebex
user-agent	Oracle/VM/9.0.0p4
sip-interface	CIDTruck
realm-la	SIFITUNK
sip-poit addross	155 212 214 00
aduress	agents-only
anow-anonymous	agents-only

sip-port		
address	155.212.214.90	
transport-protocol	TCP	
allow-anonymous	agents-only	
out-manipulationid	ToPSTN	
sip-monitoring		
match-any-filter	enabled	
monitoring-filters	*	
ladder-diagram-rows	500	
steering-pool		
ip-address	10.1.3.4	
start-port	10000	
end-port	20000	
realm-id	CiscoWebexRealm	
steering-pool		
ip-address	155.212.214.90	
start-port	10000	
end-port	20000	
realm-id	SIPTrunk	
system-config		
transcoding-cores	1	
tls-profile		
name	TLSWebex	
end-entity-certificate	CloudSBCSolLab	
trusted-ca-certificates	GoDaddyRootCA	
	WebexRootCA	
	GoDaddyIntermediate	
mutual-authenticate	enabled	
sip-manipulation		
name	Io_Webex	
header-rule		
name	Addplus1Contact	
header-name	Contact	
action	manipulate	
comparison-type	pattern-rule	
msg-type	request	
methods	Invite	
element-rule	TURNIC	
name	TenDigits	
type	uri-user	
action		
comparison-ty		
match-value		
	(+T+DORIGINAL	
element-rule	ElevenDigite	
hame		
type		
companson-ty		
match-value	- το- είται το	

2/11/1/1/1/1/2/1/1505

new-value	\++\$ORIGINAL
header-rule	
name	ChangeContactHost
header-name	Contact
action	manipulate
msg-type	out-of-dialog
methods	ACK.INVITĚ
element-rule	
name	contacthost
type	uri-host
action	replace
new-value	STRUNK GROUP CONTEXT
header-rule	
name	AddContactOptions
header-name	Contact
action	add
msa-type	request
mothods	OPTIONS
neurous	OF HONS
header rule	
neader-rule	ChangeTelD
hanne	
	TU moninulato
comparison-type	pattern-rule
msg-type	out-of-dialog
methods	INVITE
element-rule	
name	ChangeTo
type	uri-host
action	replace
new-value	"us01.sipconnect.bcld.Webex.com"
header-rule	
name	ChangePAI
header-name	P-Asserted-Identity
action	manipulate
comparison-type	pattern-rule
methods	INVITE
element-rule	
name	ChangePAI
type	uri-host
action	replace
new-value	\$TRUNK_GROUP_CONTEXT

header-rule ChangeFromIP name FROM header-name manipulate action msg-type methods INVITE element-rule name type action new-value sip-manipulation RemoveDTG name description split-headers join-headers header-rule StripDTG name header-name action manipulate comparison-type case-sensitive msg-type request methods Invite match-value new-value element-rule name parameter-name dtg type action match-val-type any comparison-type match-value new-value

out-of-dialog ChangeFrom uri-host replace **\$TRUNK_GROUP_CONTEXT Request-URI**

1111122

7/11

stripdtg header-param delete-element case-sensitive
header-rule name header-name action comparison-type msg-type methods match-value new-value header-rule name header-name action comparison-type msg-type methods match-value new-value header-rule name header-name action comparison-type msg-type methods mime-sdp-rule name msg-type methods action comparison-type match-value new-value sdp-media-rule name media-type action comparison-type match-value new-value

DeleteXBroadworks X-BroadWorks-Correlation-Info delete case-sensitive any BYE,INVITE,OPTIONS -///)

DeleteSessionID Session-ID delete case-sensitive any BYE,INVITE,OPTIONS

DeleteRecvInfo Recv-Info delete case-sensitive any BYE,INVITE,OPTIONS

Changealine any Invite manipulate pattern-rule

> deleteattributes video manipulate pattern-rule

sdp-line-rule name type action comparison- match-value new-value	deletertcp a delete etype pattern-rule (rtcp)(.*)
name	ToPSTN
description split-headers join-headers header-rule	
name	StripDTG
header-name	Request-URI
action	manipulate
companson-type	case-sensitive
methods	Invite
match-value new-value	
element-rule	
name	stripdtg
parameter-name	uly boader param
action	delete-element
match-val-type	any
comparison-type match-value	case-sensitive
new-value	
ice-profile	
name stup.copp.timoout	webexice
stun-keen-alive-interval	10
stun-rate-limit	15
mode	NONE
rtcp-stun	enabled



CONNECT WITH US

blogs.oracle.com
facebook.com/oracle
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.

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