



ORACLE

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

Technical Application Note

ORACLE

COMMUNICATIONS

Disclaimer

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

Revision History

Version	Description of Changes	Date Revision Completed
1.0	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 later)	08 th November 2024

	<p>Added crypto attributes for SRTP which includes GCM ciphers.</p> <p>Added support for Cisco Webex Contact Center along with Cisco Webex Calling part.</p>	
--	--	--

Table of Contents

1. INTENDED AUDIENCE	6
2. DOCUMENT OVERVIEW	6
2.1. CISCO WEBEX CALLING:.....	6
3. INTRODUCTION	7
3.1. AUDIENCE	7
3.2. REQUIREMENTS	7
3.3. ARCHITECTURE.....	8
4. CISCO WEBEX SIDE CONFIGURATION	8
5. CONFIGURING THE SBC	11
5.1. VALIDATED ORACLE SBC VERSION	11
6. NEW SBC CONFIGURATION.....	12
6.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC	12
6.2. CONFIGURE SBC USING WEB GUI	15
6.3. CONFIGURE SYSTEM-CONFIG.....	17
6.4. CONFIGURE PHYSICAL INTERFACE VALUES	18
6.5. CONFIGURE NETWORK INTERFACE VALUES	19
6.6. ENABLE MEDIA MANAGER.....	21
6.8. CONFIGURE REALMS.....	24
6.9. CONFIGURING A CERTIFICATE FOR SBC	26
6.10. TLS-PROFILE.....	32
6.11. CONFIGURE SIP INTERFACES	32
6.12. CONFIGURE SESSION-AGENT	37
6.13. CONFIGURE LOCAL-POLICY	41
6.14. CONFIGURE STEERING-POOL	43
6.15. CONFIGURE SDES PROFILE.....	44
6.16. CONFIGURE MEDIA SECURITY PROFILE.....	45
6.17. CONFIGURE MEDIA OPTIMIZATION (ICE-PROFILE).....	46
7. EXISTING SBC CONFIGURATION	48
8. SBC SCALING.....	48
9. ORACLE SBC INTEGRATION WITH CISCO WEBEX CONTACT CENTER.....	49
9.1. ENABLE THE USERS WITH WEBEX CC LICENSE	50
9.2. SYNCHRONIZE THE USERS WITH WEBEX CC TENANT.....	52
9.3. CONFIGURE THE SETTINGS IN SECURITY TAB.	53
9.4. CONFIGURE THE SETTINGS IN VOICE TAB.....	54
9.5. CONFIGURE THE MULTIMEDIA PROFILE TAB.	54
9.6. CONFIGURE THE DESKTOP PROFILE TAB.	55
9.7. CONFIGURE THE IDLE/WRAP-UP CODES TAB.	56
9.8. CONFIGURE THE SITES TAB.....	56
9.9. CONFIGURE THE SKILL DEFINITIONS TAB.....	57
9.10. CONFIGURE THE CONTACT CENTER USERS TAB.....	57
APPENDIX A	59
CONFIGURE MULTI-TENANCY	59
APPENDIX B	66



10. CAVEAT.....	66
ISSUE 1: SIP OPTIONS PING FROM MULTIPLE REALMS TO GLOBAL SESSION AGENTS.	66
ISSUE 2: VIDEO CALL ISSUES WHEN CALL COMES FROM CISCO CUCM TOWARDS CISCO WEBEX.....	66
11. ACLI RUNNING CONFIGURATION.....	67

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)

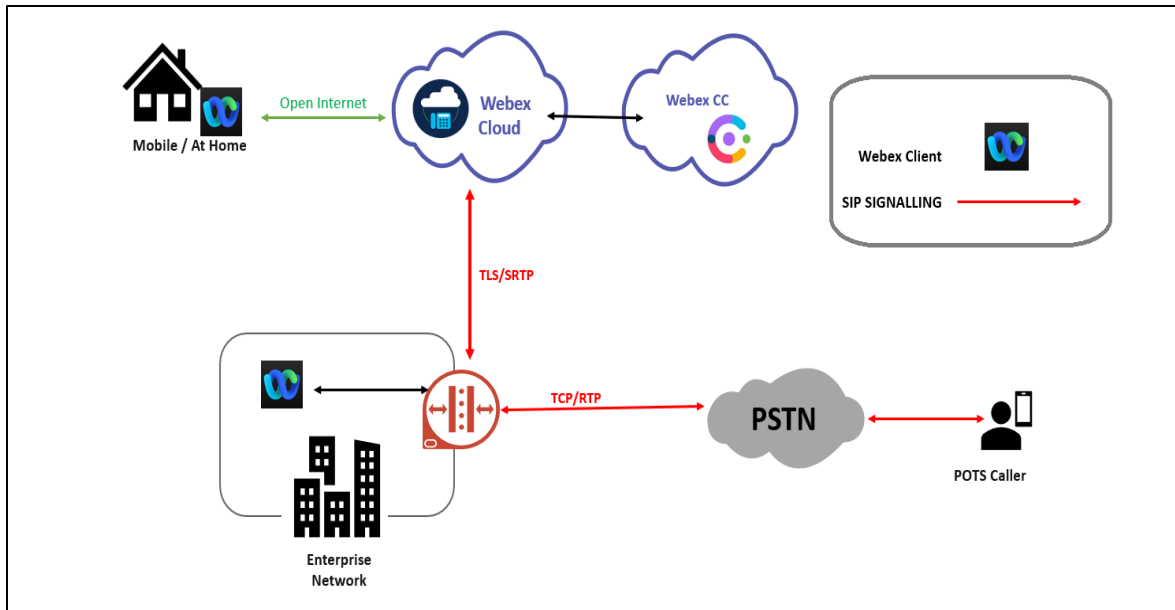
<https://help.webex.com/en-us/article/n4cprps/Prepare-Your-Environment-for-Webex-Calling>

- 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 [Configure Trunks, Route Groups, and Dial Plans for Webex 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 Control Hub 🔔 ? C

- Devices
- Apps
- Account
- Organization Settings

Calling

Numbers Locations **Call Routing** Features PSTN Orders Service Settings Client Settings

Trunk Route Group Dial Plans Verify Call Routing Zone Trusted Network Edge

Trunk

SIP trunks provide connectivity to a customer-owned PSTN service and to an on-premises IP PBX deployment. These were previously accessed via the Local Gateway configuration page. [Add Trunk](#)

Name	Location	Trunk Type	In Use
cloudsbc	BurlingtonHQ	Certificate based	Yes

- Updates & Migrations
- Messaging
- Meeting
- Calling**
- Connected UC
- Hybrid
- Oracle

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

webex Control Hub 🔔 ? C

- Devices
- Apps
- Account
- Organization Settings

Calling

Numbers Locations **Call Routing** Features PSTN Orders

Trunk Route Group Dial Plans Verify Call Routing Zone Trusted Network Edge

Trunk

SIP trunks provide connectivity to a customer-owned PSTN service and to an on-premises IP PBX deployment. These were previously accessed via the Local Gateway configuration page.

Name	Location	Trunk Type
cloudsbc	BurlingtonHQ	Certificate based

cloudsbc ✎ ✕

Trunk

Details

Trunk Info Manage >

In Use

Calls to On-Premises Extensions 0 Locations >

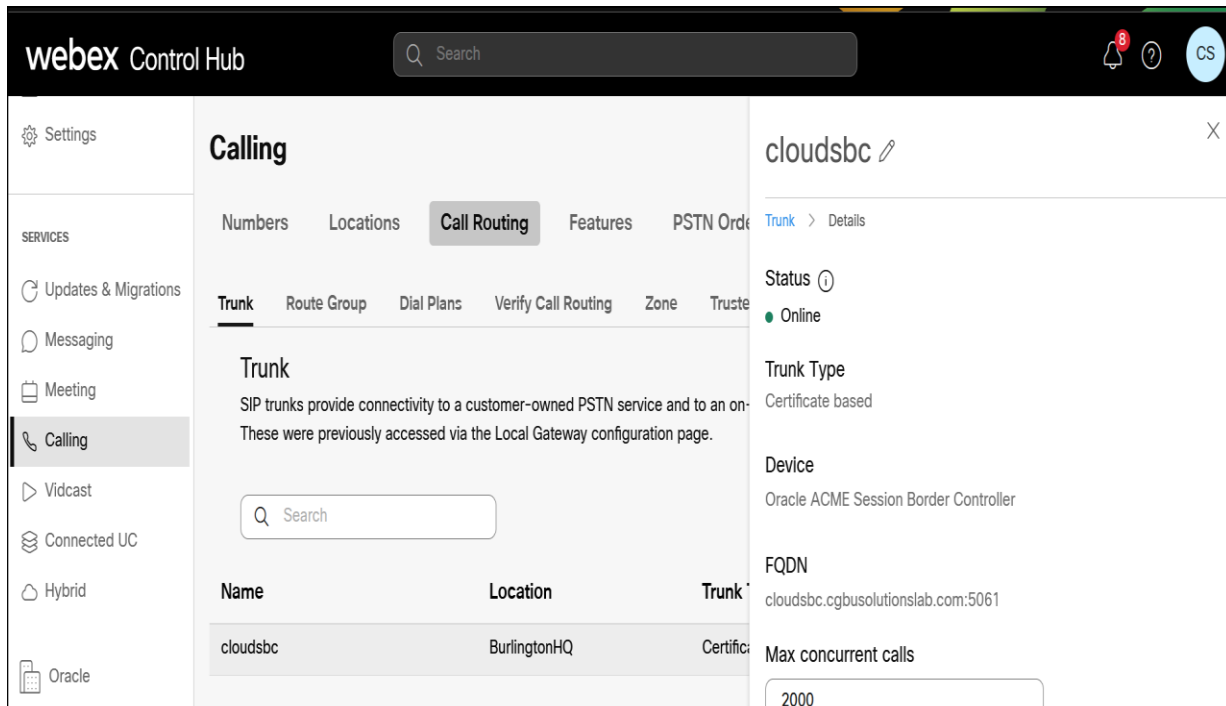
Dial Plans 0 Dial Plans >

PSTN Connection 2 Locations >

Route Group 0 Route Groups >

- Updates & Migrations
- Messaging
- Meeting
- Calling**
- Connected UC
- Hybrid
- 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.



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.

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 platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...

Starting acliMgr...
password secure mode is enabled
Admin Security is disabled
Password: █
```

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:
%
% 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 :
%   - lower case alpha
%   - upper case alpha
%   - numerals
%   - punctuation
%
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             :
IPv6 Address        :
IPv6 Gateway        :
Host IP             :
FTP username        : vxftp
FTP password        :
Flags               : 0x00000040
Target Name         : SolutionsLab-vSBC-2
Console Device      : COM1
Console Baudrate    : 115200
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)

```
-----
Entitlements for Enterprise Session Border Controller
Last Modified: 2022-02-23 18:18:18
-----

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
22: Transcode Codec SILK Capacity : 2000

Enter 1 - 22 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1
  Session Capacity (0-10000)          : 500

Enter 1 - 22 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10
  Transcode Codec AMR Capacity (0-10000) : 50

Enter 1 - 22 to modify, d' to display, 's' to save, 'q' to exit. [s]: 14
  Transcode Codec EVRC Capacity (0-10000) : 40

Enter 1 - 22 to modify, d' to display, 's' 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.

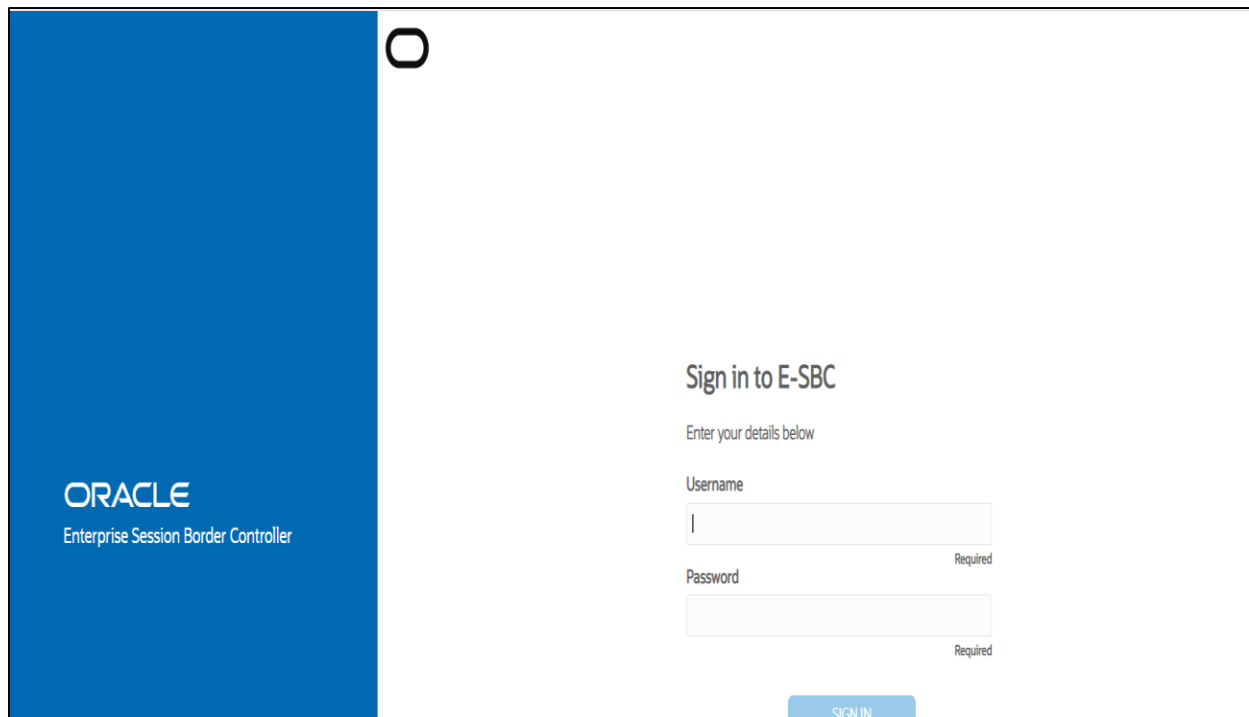
```
SolutionsLab-vSBC-2(http-server)# show
http-server
  name                webserver
  state                enabled
  realm
  ip-address
  http-state          enabled
  http-port            80
  HTTP-strict-transport-security-policy disabled
  https-state         disabled
  https-port          443
  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)#
```

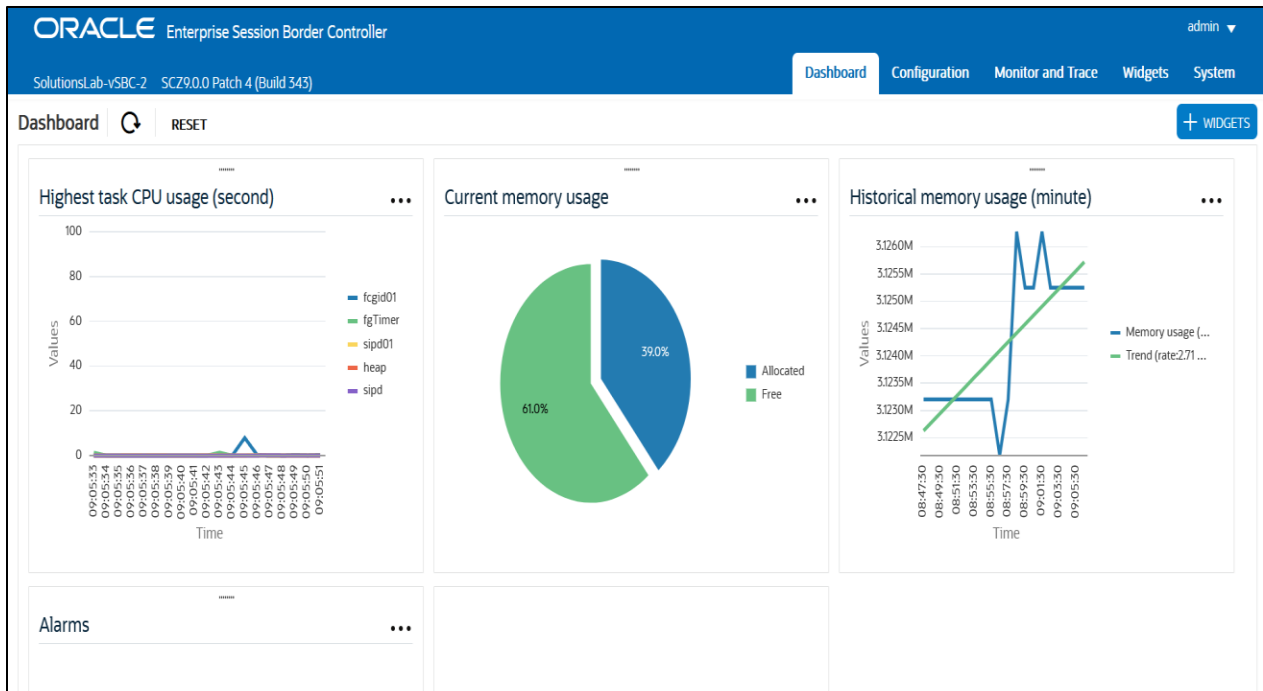
6.2. Configure SBC using Web GUI

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

The Web GUI can be accessed through the url http://<SBC_MGMT_IP>.



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



Go to Configuration as shown below, to configure the SBC

Name	Description
access-control	Configure a static or dynamic access control list
account-config	Configure Quality of Service accounting
authentication-profile	Configure authentication profile
certificate-record	Create, generate, and import a certificate
class-policy	Configure classification profile policies
codec-policy	Create and apply a codec policy to a realm and an agent
filter-config	Create a custom filter for SIP monitor and trace
fraud-protection	Configure fraud protection
host-route	Insert entries into the routing table
http-client	Configure an HTTP client
http-server	Configure an HTTP server

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

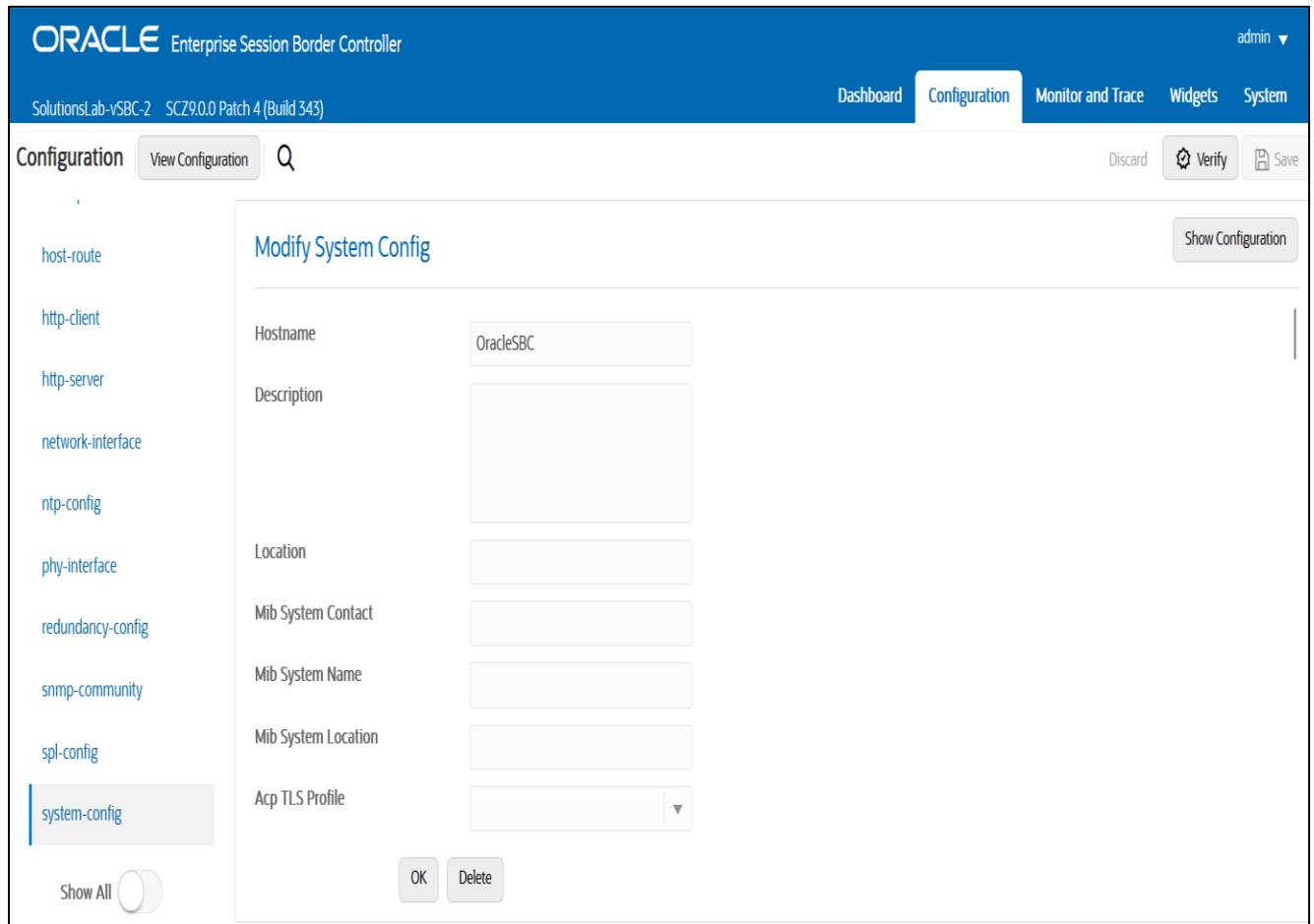
<https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.3.0/webgui/web-gui-guide.pdf>

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



The screenshot displays the Oracle Enterprise Session Border Controller (ESBC) configuration interface. The top navigation bar includes the Oracle logo, the product name 'Enterprise Session Border Controller', the user 'admin', and menu items for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' menu is active. Below the navigation bar, the page title is 'Configuration' with a search icon and a 'View Configuration' button. The main content area is titled 'Modify System Config' and contains a form with the following fields: 'Hostname' (text input with value 'OracleSBC'), 'Description' (text area), 'Location' (text input), 'Mib System Contact' (text input), 'Mib System Name' (text input), 'Mib System Location' (text input), and 'Acp TLS Profile' (dropdown menu). At the bottom of the form are 'OK' and 'Delete' buttons. A 'Show Configuration' button is located in the top right corner of the form area. On the left side, a sidebar lists various configuration objects: 'host-route', 'http-client', 'http-server', 'network-interface', 'ntp-config', 'phy-interface', 'redundancy-config', 'snmp-community', 'spl-config', and 'system-config' (which is highlighted). A 'Show All' toggle is located at the bottom left of the sidebar.

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

<https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/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

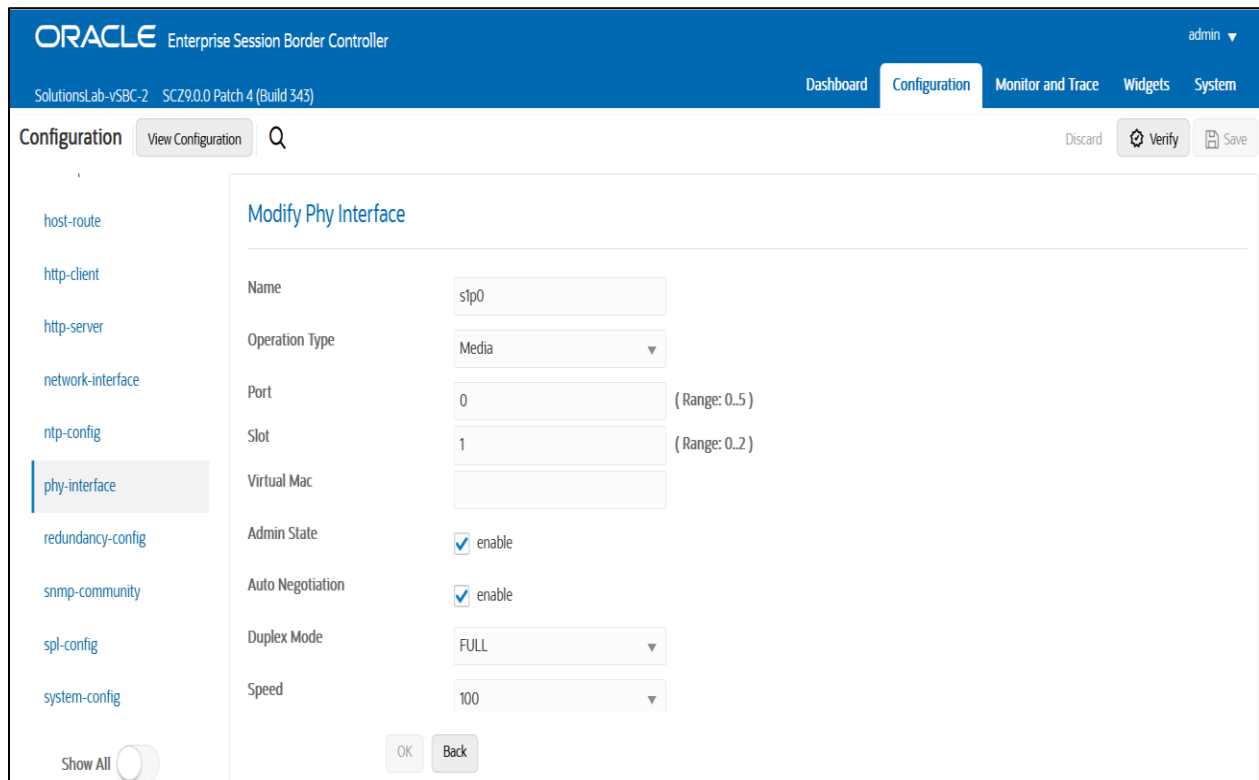
Please configure s0p0 interface as below.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'admin', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the 'phy-interface' option is selected in the left sidebar. The main content area is titled 'Modify Phy Interface' and contains the following configuration fields:

- Name: s0p0
- Operation Type: Media
- Port: 0 (Range: 0..5)
- Slot: 0 (Range: 0..2)
- Virtual Mac: (empty)
- Admin State: enable
- Auto Negotiation: enable
- Duplex Mode: FULL
- Speed: 100

At the bottom of the form, there are 'OK' and 'Back' buttons. The interface also includes a 'Show All' toggle and 'Discard', 'Verify', and 'Save' buttons in the top right corner.

Please configure s1p0 interface as below



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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' tab is active. On the left, a sidebar lists various configuration categories, with 'network-interface' selected. The main area is titled 'Modify Network Interface' and contains the following fields:

- Name: s0p0
- Sub Port Id: 0 (Range: 0..4095)
- Description: (empty text area)
- Hostname: (empty text field)
- IP Address: 155.212.214.90
- Pri Utility Addr: (empty text field)
- Sec Utility Addr: (empty text field)

At the bottom of the form are 'OK' and 'Back' buttons. A 'Show All' toggle is located at the bottom left of the sidebar.

Similarly, configure network interface s1p0 as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for network interface s1p0. The layout is identical to the previous screenshot, but with the following field values:

- Name: s1p0
- Sub Port Id: 0 (Range: 0..4095)
- Description: (empty text area)
- Hostname: (empty text field)
- IP Address: 10.1.3.4
- Pri Utility Addr: (empty text field)
- Sec Utility Addr: (empty text field)

'OK' and 'Back' buttons are present at the bottom of the form.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The current page is 'Configuration', with a search bar and 'View Configuration' button. The left sidebar shows a tree view with 'network-interface' selected. The main content area is titled 'Modify Network Interface' and contains the following configuration fields:

Field	Value	Range
DNS IP Primary	99.99	
DNS IP Backup1	8.8.8.8	
DNS IP Backup2	8.8.4.4	
DNS Domain	cgbusolutionslab.com	
DNS Timeout	11	(Range: 0..4294967295)
DNS Max TTL	86400	(Range: 30..2073600)
Signaling Mtu	0	(Range: 0,576..4096)
HIP IP List		
ICMP Address		

Buttons for 'Add', 'Upload', 'OK', and 'Back' are visible at the bottom of the configuration area.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for 'Modify Media Manager'. The top navigation bar is the same as in the previous screenshot. The left sidebar shows a tree view with 'media-manager' selected. The main content area is titled 'Modify Media Manager' and contains the following configuration fields:

Field	Value	Range
State	<input checked="" type="checkbox"/> enable	
Flow Time Limit	86400	(Range: 0..4294967295)
Initial Guard Timer	300	(Range: 0..4294967295)
Subsq Guard Timer	300	(Range: 0..4294967295)
TCP Flow Time Limit	86400	(Range: 0..4294967295)
TCP Initial Guard Timer	300	(Range: 0..4294967295)
TCP Subsq Guard Timer	300	(Range: 0..4294967295)
Hnt Rtcp	<input type="checkbox"/> enable	
Algd Log Level	NOTICE	
Mhcd Log Level		

Buttons for 'OK' and 'Delete' are visible at the bottom of the configuration area.

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343)

Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q Discard Verify

media-manager

codec-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

system

fraud-protection

host-route

Show All

Modify Media Manager

Max Signaling Packets	0	(Range: 0..4294967295)
Max Untrusted Signaling	1	(Range: 0..100)
Min Untrusted Signaling	1	(Range: 0..100)
Dos Guard Window	5	(Range: 1..30)
Untrusted Minor Threshold	0	(Range: 0..100)
Untrusted Major Threshold	0	(Range: 0..100)
Untrusted Critical Threshold	0	(Range: 0..100)
Trusted Minor Threshold	0	(Range: 0..100)
Trusted Major Threshold	0	(Range: 0..100)
Trusted Critical Threshold	0	(Range: 0..100)
Arp Minor Threshold	0	(Range: 0..100)

OK 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.

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q Discard Verify

local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface

Show All

Modify SIP Config

State	<input checked="" type="checkbox"/> enable
Dialog Transparency	<input checked="" type="checkbox"/> enable
Home Realm ID	CiscoWebexRealm
Egress Realm ID	
Nat Mode	None
Registrar Domain	*
Registrar Host	*
Registrar Port	5060 (Range: 0;1025..65535)
Init Timer	500 (Range: 0..4294967295)

OK Delete

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q Discard Verify

local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface

Show All

Modify SIP Config

Invite Expire	180 (Range: 0..2147473)
Session Max Life Limit	0
Enforcement Profile	
Red Max Trans	10000 (Range: 0..50000)
Options	max-udp-length=0 X
SPL Options	
SIP Message Len	4096 (Range: 0..65535)
Enum Sag Match	<input type="checkbox"/> enable
Extra Method Stats	<input checked="" type="checkbox"/> enable

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:

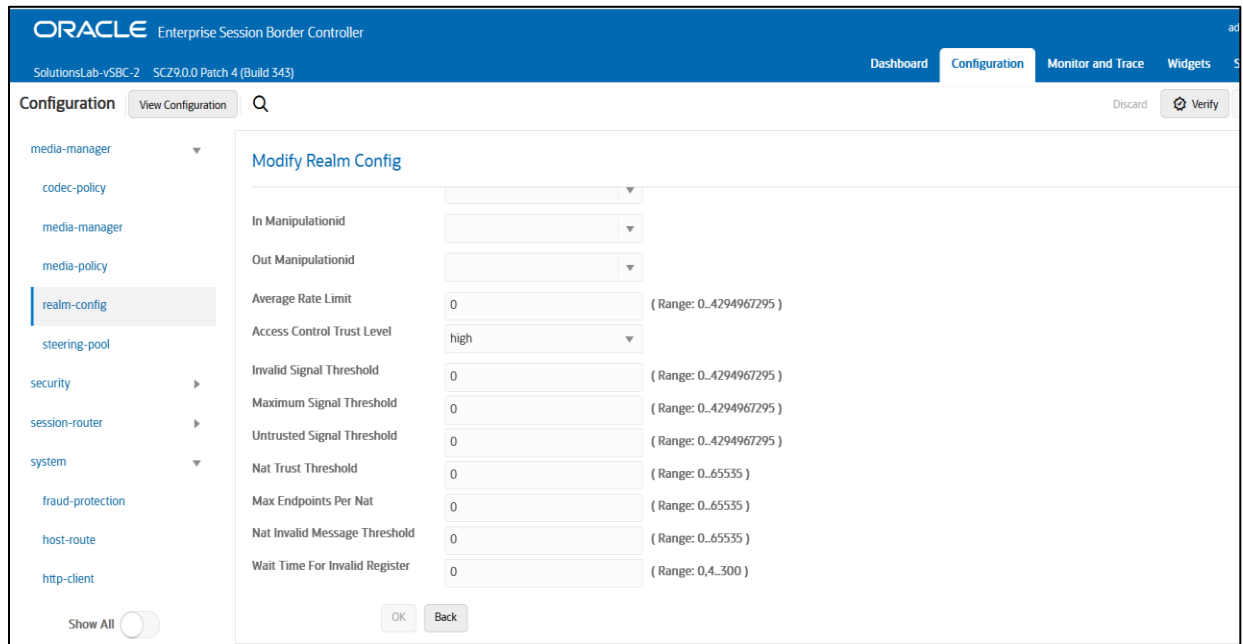
Config Parameter	PSTN Side	Cisco Webex Side
Identifier	SIPTrunk	CiscoWebexRealm
Network Interface	S0p0	s1p0
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
trunk-context		cloudsbc.cgbusolutionslab.com
Media Sec policy	CiscoWebexSecurity	PSTNSide
Access Control Trust 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

The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343)', and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' tab is active, and the left sidebar shows a tree view with 'realm-config' selected. The main content area is titled 'Modify Realm Config' and contains the following fields:

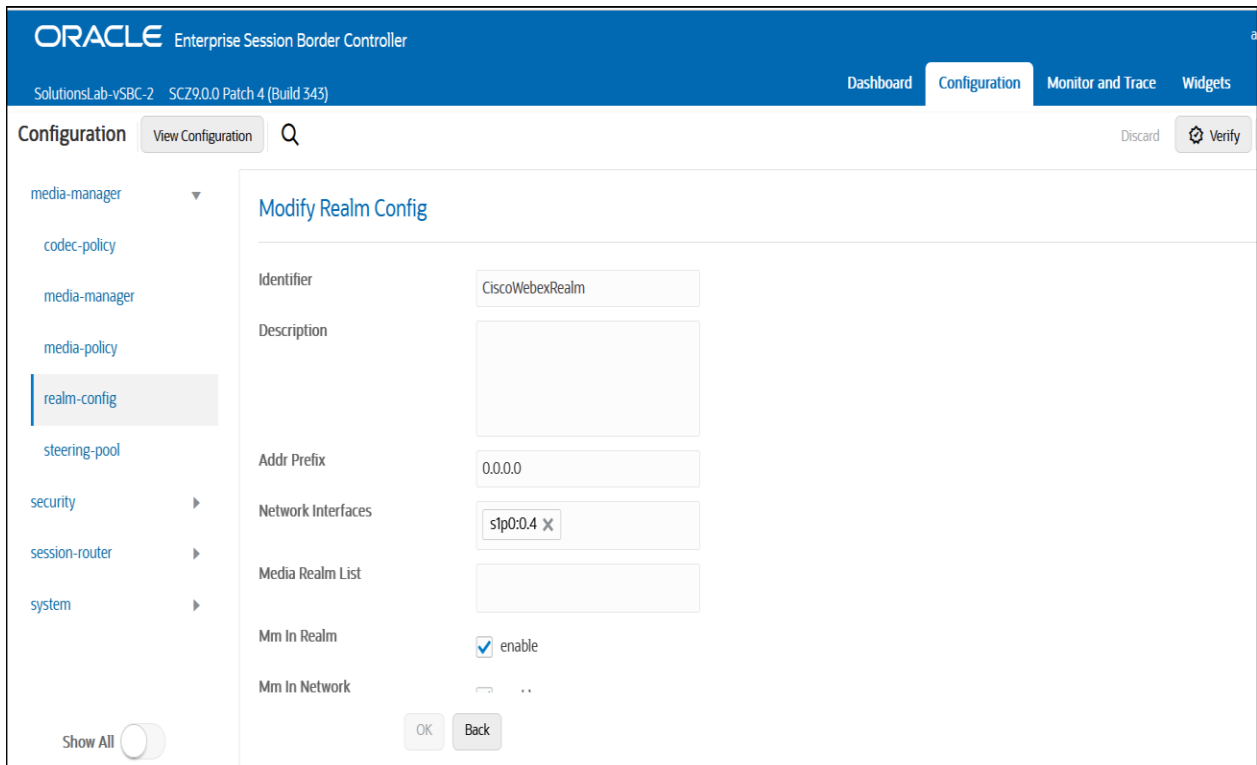
- Identifier: SIPTrunk
- Description: (empty text area)
- Addr Prefix: 0.0.0.0
- Network Interfaces: s0p0:0.4
- Media Realm List: (empty text area)
- Mm In Realm: enable
- Mm In Network: enable
- Mm Same Ip: enable

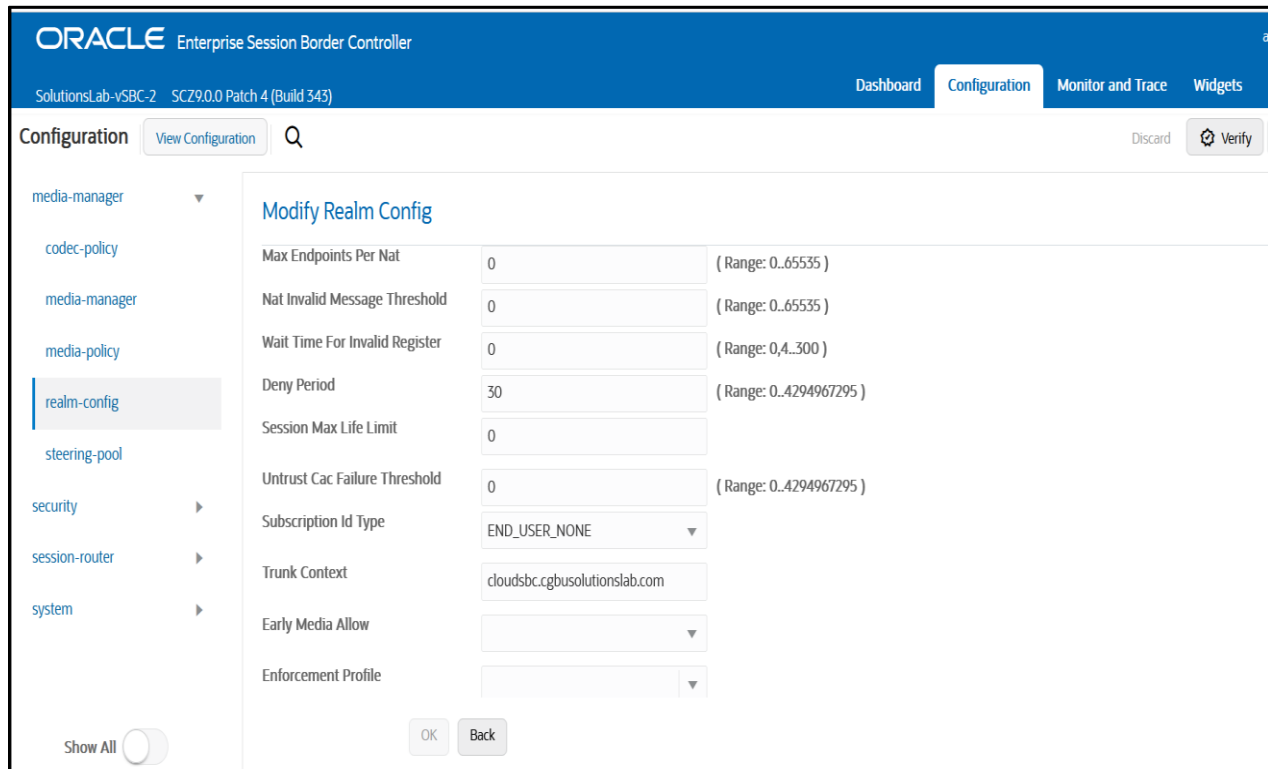
At the bottom of the configuration area, there are 'OK' and 'Back' buttons. A 'Show All' toggle is visible in the bottom left corner.



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.





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/security-guide.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-Supported-for-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.

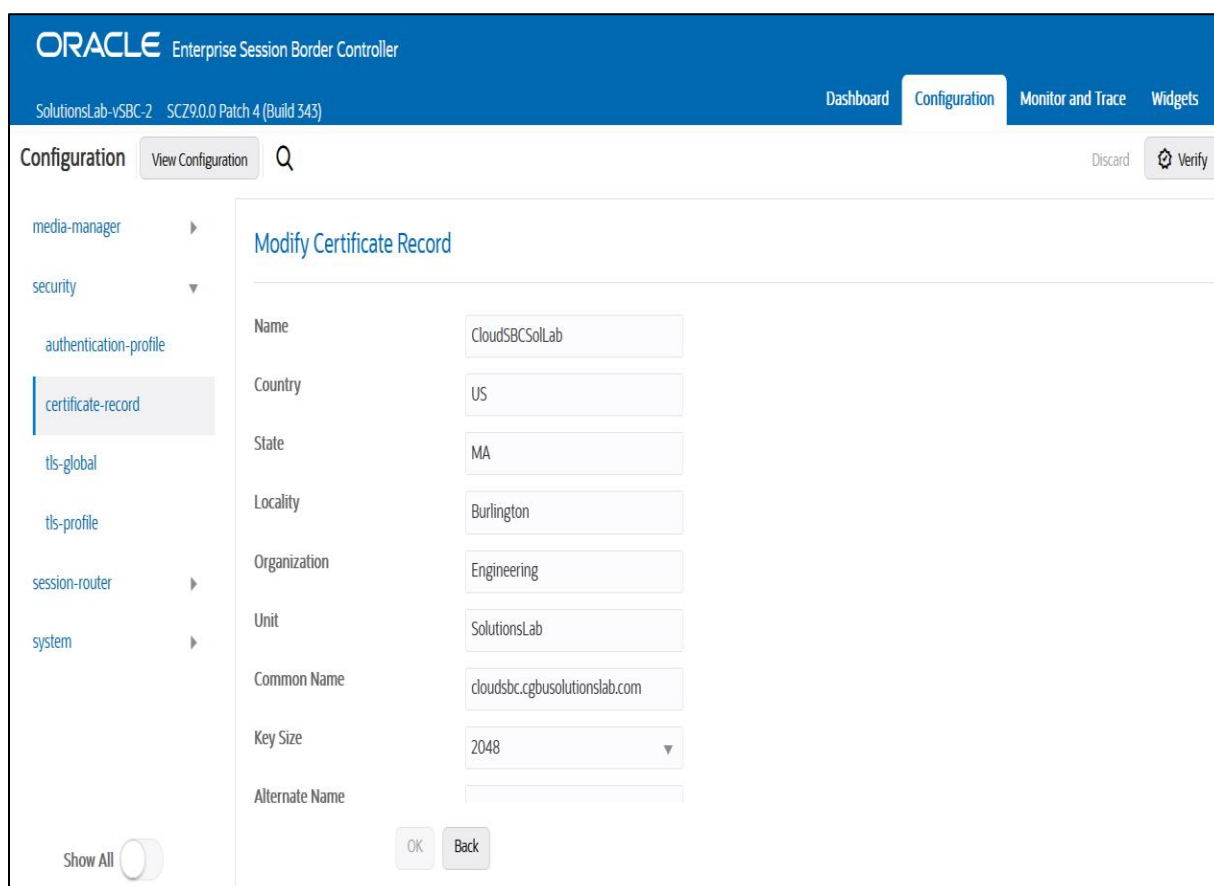
- SBC – 1 certificate-record assigned to SBC
- Root – 1 certificate-record for root cert

- 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.



The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes the Oracle logo, the product name 'Enterprise Session Border Controller', and the version 'SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343)'. The main navigation tabs are 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' tab is active, and the left sidebar shows a tree view with 'certificate-record' selected. The main content area is titled 'Modify Certificate Record' and contains the following fields:

Name	CloudSBCSolLab
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	SolutionsLab
Common Name	cloudsbc.cbusolutionslab.com
Key Size	2048
Alternate Name	

At the bottom of the form, there are 'Show All', 'OK', and 'Back' buttons.

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q Discard Verify

media-manager ▶ security ▼ authentication-profile certificate-record (selected) tls-global tls-profile session-router ▶ system ▶

Modify Certificate Record

Common Name: cloudsbc.cbusolutionslab.com

Key Size: 2048

Alternate Name:

Trusted: enable

Key Usage List: digitalSignature X, keyEncipherment X

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:

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q Discard Verify

media-manager ▶ security ▼ authentication-profile certificate-record (selected) tls-global tls-profile session-router ▶ system ▶

Modify Certificate Record

Name: WebexRootCA

Country: US

State: MA

Locality: Burlington

Organization: Engineering

Unit: Cisco Webex Calling

Common Name: IdenTrust Root CA certificate

Key Size: 2048

Alternate Name:

Trusted: enable

Show All 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	IdenTrusr 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.

The screenshot shows a configuration page for 'Certificate Record'. The interface includes a sidebar with navigation options like 'media-manager', 'security', 'authentication-profile', 'certificate-record', 'tls-global', 'tls-profile', 'session-router', and 'system'. The main area displays a table of certificate records with the following data:

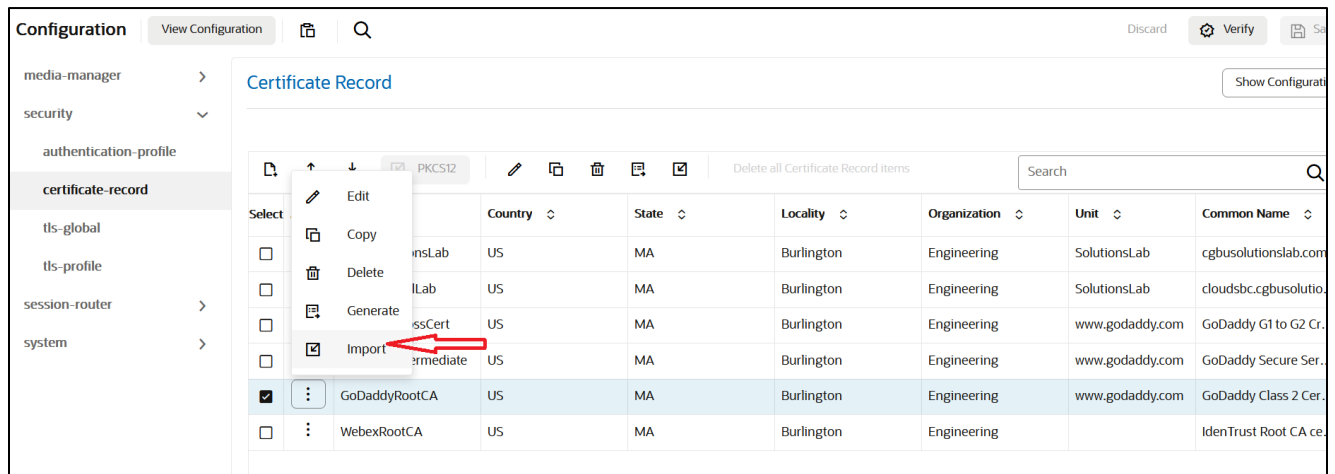
Select	Action	Name	Country	State	Locality	Organization	Unit	Common Name
<input type="checkbox"/>	⋮	CGBUSolutionsLab	US	MA	Burlington	Engineering	SolutionsLab	cgbusolutionslab.com
<input checked="" type="checkbox"/>	⋮	CloudSBCSolLab	US	MA	Burlington	Engineering	SolutionsLab	cloudsbc.cgbusolutio...
<input type="checkbox"/>	⋮	GoDaddyCrossCert	US	MA	Burlington	Engineering	www.godaddy.com	GoDaddy G1 to G2 Cr...
<input type="checkbox"/>	⋮	GoDaddyIntermediate	US	MA	Burlington	Engineering	www.godaddy.com	GoDaddy Secure Ser...
<input type="checkbox"/>	⋮	GoDaddyRootCA	US	MA	Burlington	Engineering	www.godaddy.com	GoDaddy Class 2 Cer...
<input type="checkbox"/>	⋮	WebexRootCA	US	MA	Burlington	Engineering		IdenTrust Root CA ce...

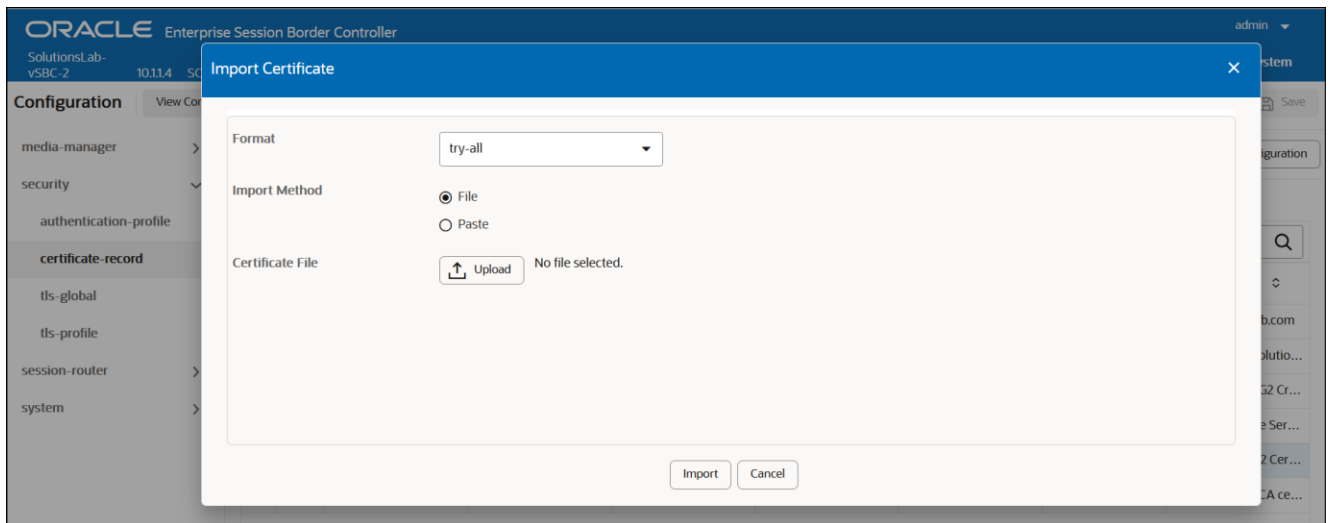
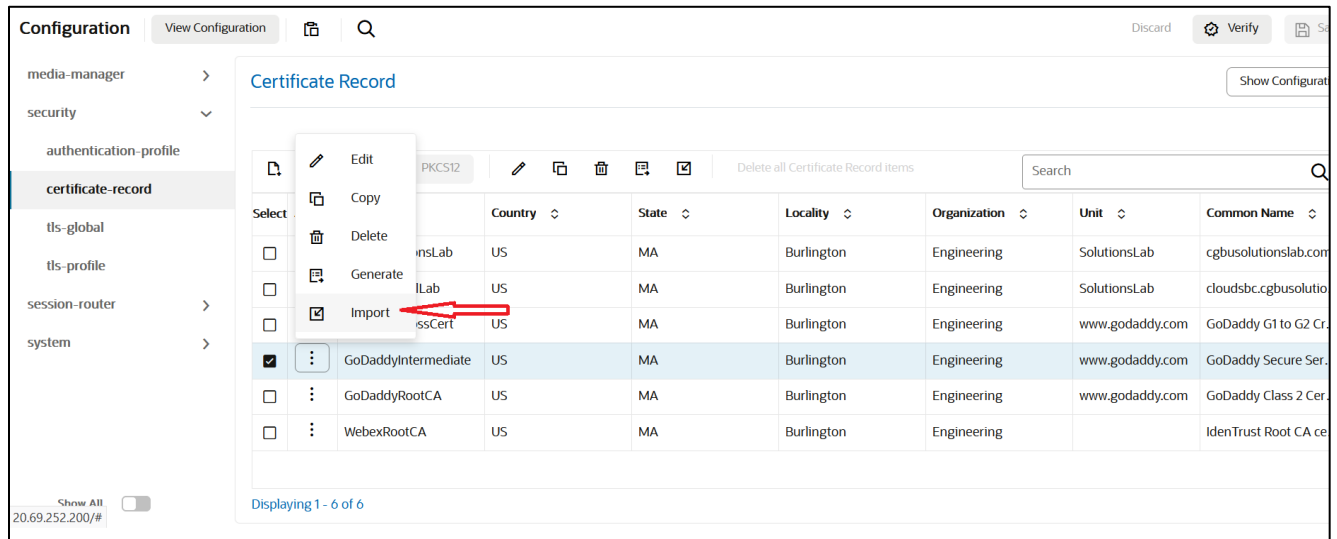


- Also, note that a **save/activate** is required

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

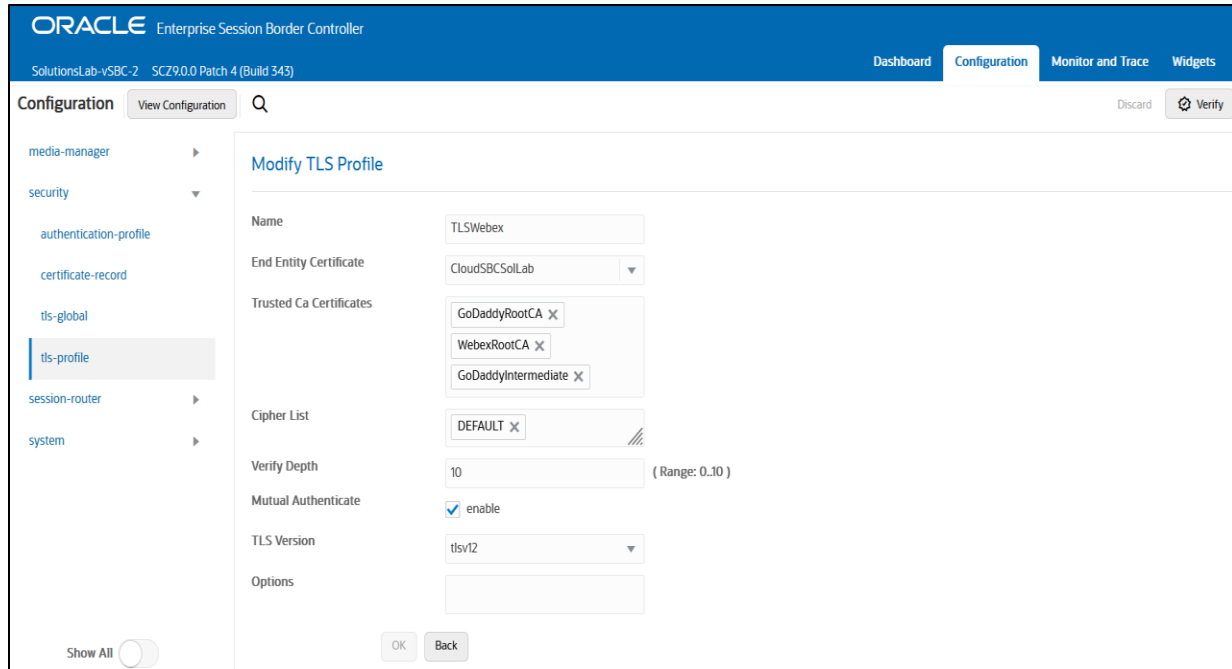




Repeat these steps to import all the root and intermediate CA certificates into the SBC:
At this stage all the required certificates have been imported to the SBC for Cisco Webex Calling.

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:



The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' tab is active, and the 'security' section is expanded to show 'tls-profile'. The 'Modify TLS Profile' form is visible, with the following settings:

- Name: TLSWebex
- End Entity Certificate: CloudSBCSolLab
- Trusted Ca Certificates: GoDaddyRootCA, WebexRootCA, GoDaddyIntermediate
- Cipher List: DEFAULT
- Verify Depth: 10 (Range: 0..10)
- Mutual Authenticate: enable
- TLS Version: tlsv12
- Options: (empty)

Buttons for 'OK' and 'Back' are located at the bottom of the form. A 'Show All' toggle is visible in the bottom left corner of the configuration area.

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

ORACLE Enterprise Session Border Controller admin ▾

SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace Widgets System

Configuration View Configuration Q Discard Verify Save

session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
translation-rules

Show All

Modify SIP Interface Show Configuration

State enable

Realm ID

Description

SIP Ports

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
⋮	<input type="checkbox"/>	10.1.3.4	5061	TLS	TLSWebex	agents-only	

OK Back

ORACLE Enterprise Session 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

session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface
sip-manipulation
sip-monitoring
translation-rules

Show All

Modify SIP Interface Show Conf

Displaying 1 - 1 of 1

Initial Inv Trans Expire (Range: 0..2147473)

Session Max Life Limit

Proxy Mode

Redirect Action

Nat Traversal

Nat Interval (Range: 0..4294967295)

TCP Nat Interval (Range: 0..4294967295)

OK Back

Configuration

View Configuration



Discard

Verify

- session-group
- session-recording-group
- session-recording-server
- session-translation
- sip-config
- sip-feature
- sip-interface**
- sip-manipulation
- sip-monitoring
- translation-rules

system

Show All

Modify SIP Interface

Show Conf

S8hr Profile	<input type="text"/>
Ringback Trigger	<input type="text" value="none"/>
Ringback File	<input type="text"/>
Fax Continue Session	<input type="text" value="none"/>
Npli Profile	<input type="text"/>
Hist To Div For Cause 380	<input type="text" value="inherit"/>
User Agent	<input type="text" value="Oracle/VM/9.0.0p4"/>
Allow Diff2833 Clock Rate Mode	<input type="text" value="disabled"/>

OK

Back

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 below sip-manipulation as the out-manipulation ID in the Cisco Webex sip interface or Cisco Webex Session Agent as per customer need.**

```

sip-manipulation
name
    header-rule
        name
        header-name
        action
        comparison-type
        msg-type
        methods
    element-rule
        name
        type
        action
        comparison-type
        match-value
        new-value
    element-rule
        name
        type
        action
        comparison-type
        match-value
        new-value
    header-rule
        name
        header-name
        action
        methods
        element-rule
            name
            type
            action
            new-value
    header-rule
        name
        header-name
        action
        msg-type
        methods
        new-value

```

ToCiscoWebex

```

addplus
Contact
manipulate
    pattern-rule
request
Invite

TenDigits
uri-user
replace
    pattern-rule
    ^[0-9]{10}$
    \+1+$ORIGINAL

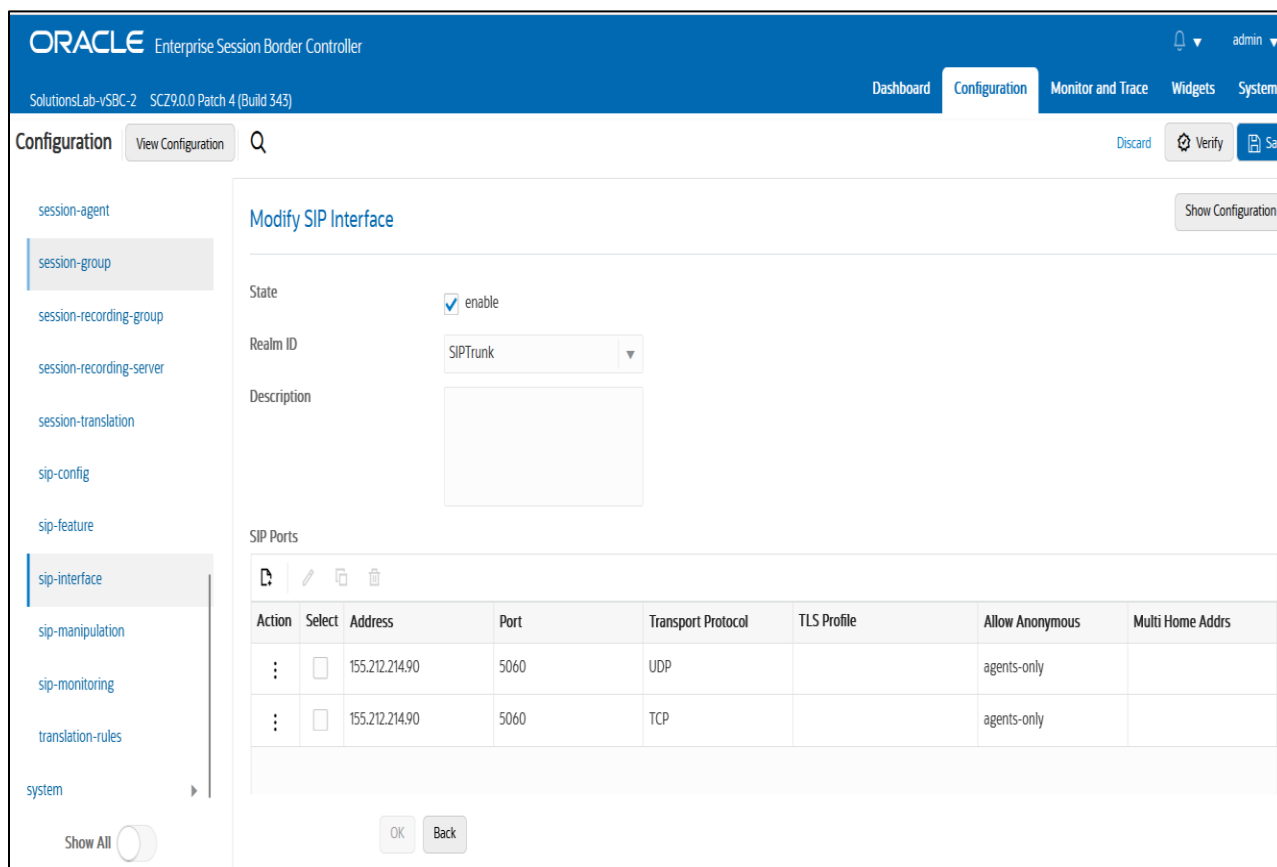
ElevenDigits
uri-user
replace
    pattern-rule
    ^[0-9]{11}$
    \++$ORIGINAL

ChangeContactHost
Contact
manipulate
    ACK,INVITE
    contacthost
    uri-host
    replace
    $TRUNK_GROUP_CONTEXT

AddContactOptions
Contact
add
request
OPTIONS
<sip:ping@"+$TRUNK_GROUP_CONTEXT+":5061;transport=tls>"

```

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                RemovedDTG
  description
  split-headers
  join-headers
  header-rule
    name              StripDTG
    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	

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.bclid.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.

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q Discard Verify

local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface

Show All

Modify Session Agent

Show Conf

Hostname: us01.sipconnect.bcl.d.webex.com

IP Address:

Port: 0 (Range: 0,1025..65535)

State: enable

App Protocol: SIP

App Type:

Transport Method: StaticTLS

Realm ID: CiscoWebexRealm

Egress Realm ID:

OK Back

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q Discard Verify

local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature

Show All

Modify Session Agent

Show Conf

Ping Interval: 30 (Range: 0..4294967295)

Ping Send Mode: keep-alive

Ping All Addresses: enable

Ping In Service Response Codes:

Options: recurse-on-all-failures X

SPL Options:

Media Profiles:

In Translationid:

OK Back

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The current page is 'Configuration', with a search bar and 'View Configuration' button. The left sidebar lists various configuration categories, with 'session-agent' selected. The main content area is titled 'Modify Session Agent' and contains the following fields:

Hostname	68.68.117.67
IP Address	68.68.117.67
Port	5060 (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
App Protocol	SIP
App Type	
Transport Method	UDP
Realm ID	SIPTrunk
Egress Realm ID	

Buttons for 'OK' and 'Back' are located at the bottom of the form.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, similar to the previous one. The top navigation bar and sidebar are the same. The main content area is titled 'Modify Session Agent' and contains the following fields:

Redirect Action	
Loose Routing	<input checked="" type="checkbox"/> enable
Response Map	
Ping Method	OPTIONS
Ping Interval	30 (Range: 0..4294967295)
Ping Send Mode	keep-alive
Ping All Addresses	<input checked="" type="checkbox"/> enable
Ping In Service Response Codes	
Options	

Buttons for 'OK' and 'Back' are located at the bottom of the form.

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

sip-manipulation	
name	ToPSTN
description	
split-headers	
join-headers	
header-rule	
name	StripDTG
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	
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.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is 'Modify Local Policy'. The configuration fields are as follows:

- From Address: * X
- To Address: * X
- Source Realm: CiscoWebexRealm X
- Description: (empty text area)
- State: enable
- Policy Priority: none

Buttons at the bottom include 'OK' and 'Back'. The left sidebar shows a list of configuration categories, with 'local-policy' selected.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, specifically the 'Policy Attributes' section. The configuration fields are as follows:

- Source Realm: CiscoWebexRealm X
- Description: (empty text area)
- State: enable
- Policy Priority: none

The 'Policy Attributes' section contains a table with the following data:

Action	Select	Next Hop	Realm	Action	Terminate ...	Cost	State	App Protocol	Lookup	Next Key
⋮	<input type="checkbox"/>	68.68.117.67	SIPTTrunk	replace-uri	disabled	0	enabled		single	

Buttons at the bottom include 'OK' and 'Back'. The left sidebar shows a list of configuration categories, with 'local-policy' selected.

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The page title is "Modify Local Policy". The configuration fields are as follows:

- From Address: * X
- To Address: * X
- Source Realm: SIPTrunk X
- Description: (empty text area)
- State: enable
- Policy Priority: none

Buttons at the bottom include "OK" and "Back".

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, similar to the first one, but with the "Policy Attributes" section expanded. The configuration fields are:

- Source Realm: SIPTrunk X
- Description: (empty text area)
- State: enable
- Policy Priority: none

The "Policy Attributes" section contains a table with the following data:

Action	Select	Next Hop	Realm	Action	Terminate ...	Cost	State	App Protocol	Lookup	Next Key
:	<input type="checkbox"/>	us01.sipconn...	CiscoWebex...	replace-uri	disabled	0	enabled		single	

Buttons at the bottom include "OK" and "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.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' tab is active. The left sidebar shows a tree view with 'steering-pool' selected. The main content area is titled 'Modify Steering Pool' and contains the following fields:

IP Address	101.3.4
Start Port	10000 (Range: 0,1..65535)
End Port	20000 (Range: 0,1..65535)
Realm ID	CiscoWebexRealm
Network Interface	

At the bottom, there are 'OK' and 'Back' buttons, and a 'Show All' toggle.

PSTN side steering pool.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' tab is active. The left sidebar shows a tree view with 'steering-pool' selected. The main content area is titled 'Modify Steering Pool' and contains the following fields:

IP Address	155.212.214.90
Start Port	10000 (Range: 0,1..65535)
End Port	20000 (Range: 0,1..65535)
Realm ID	SIPTrunk
Network Interface	

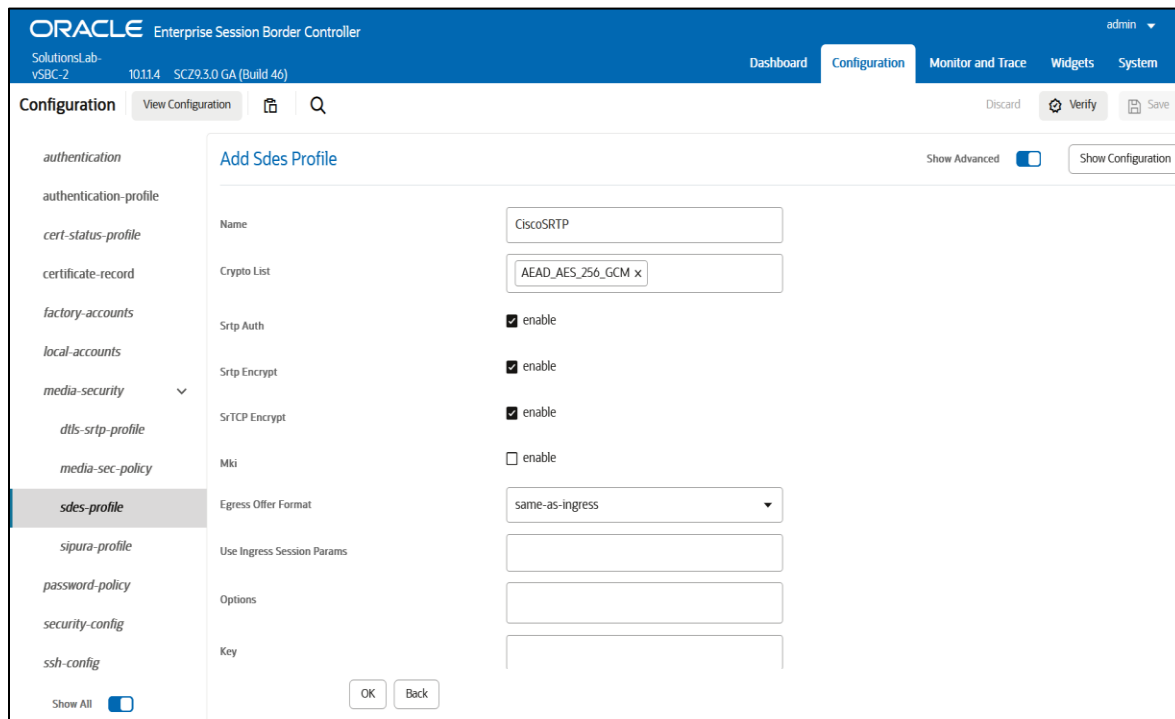
At the bottom, there are 'OK' and 'Back' buttons, and a 'Show All' toggle.

6.15. Configure sdes profile

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

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

AEAD_AES_256_GCM (This cipher is applicable only for Webex for Government as it is FIPS-compliant GCM ciphers)



The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'admin', 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active, and the 'media-security' menu item is expanded to show 'sdes-profile'. The 'Add Sdes Profile' form is visible, with the following fields and values:

Field	Value
Name	CiscoSRTP
Crypto List	AEAD_AES_256_GCM x
Srtp Auth	<input checked="" type="checkbox"/> enable
Srtp Encrypt	<input checked="" type="checkbox"/> enable
SrTCP Encrypt	<input checked="" type="checkbox"/> enable
Mki	<input type="checkbox"/> enable
Egress Offer Format	same-as-ingress
Use Ingress Session Params	
Options	
Key	

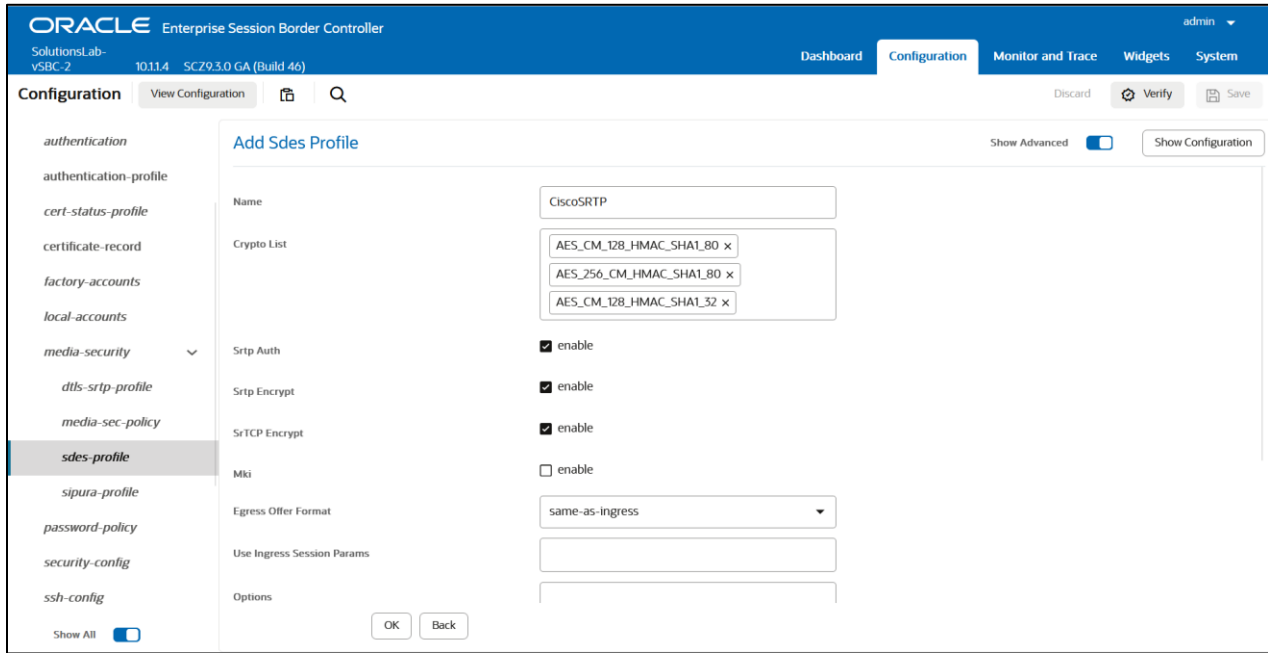
Buttons for 'OK' and 'Back' are located at the bottom of the form. The 'Show Advanced' toggle is turned on, and the 'Show Configuration' button is visible in the top right corner of the form area.

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

AES_CM_256_HMAC_SHA1_80

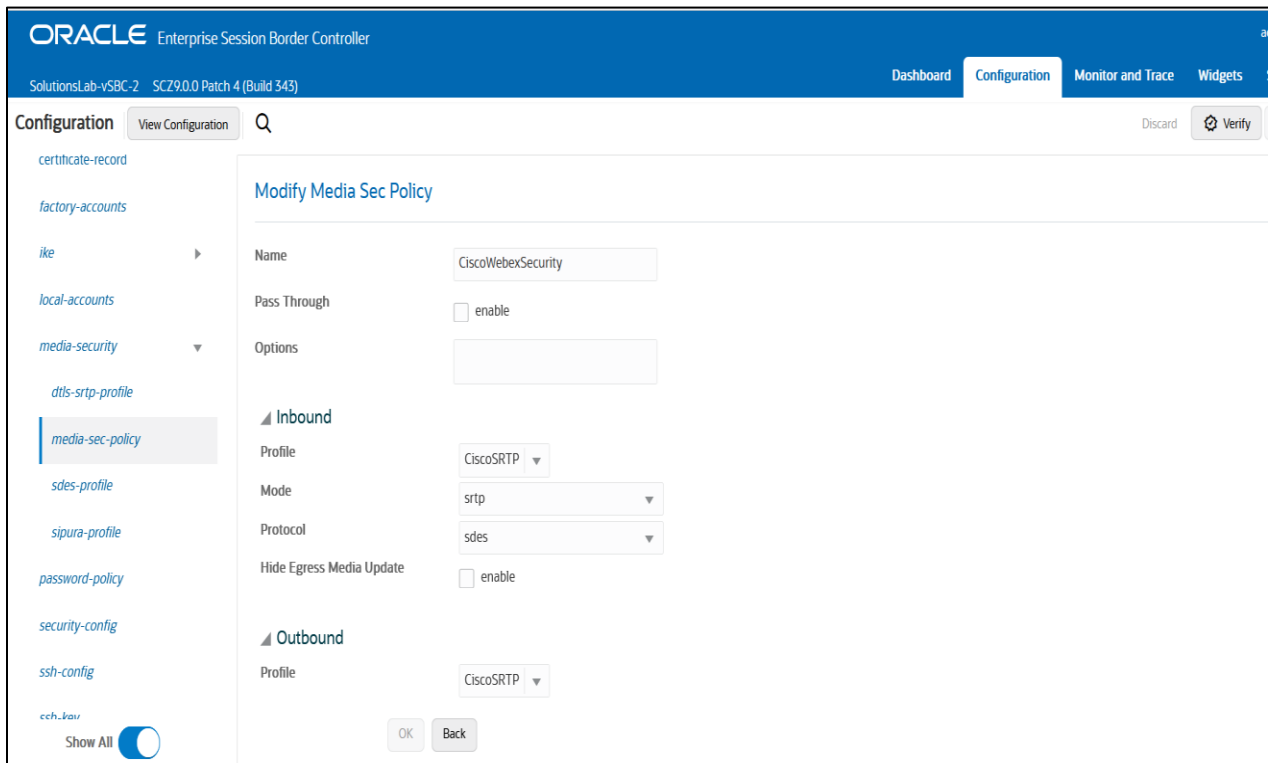
AES_CM_128_HMAC_SHA1_80

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

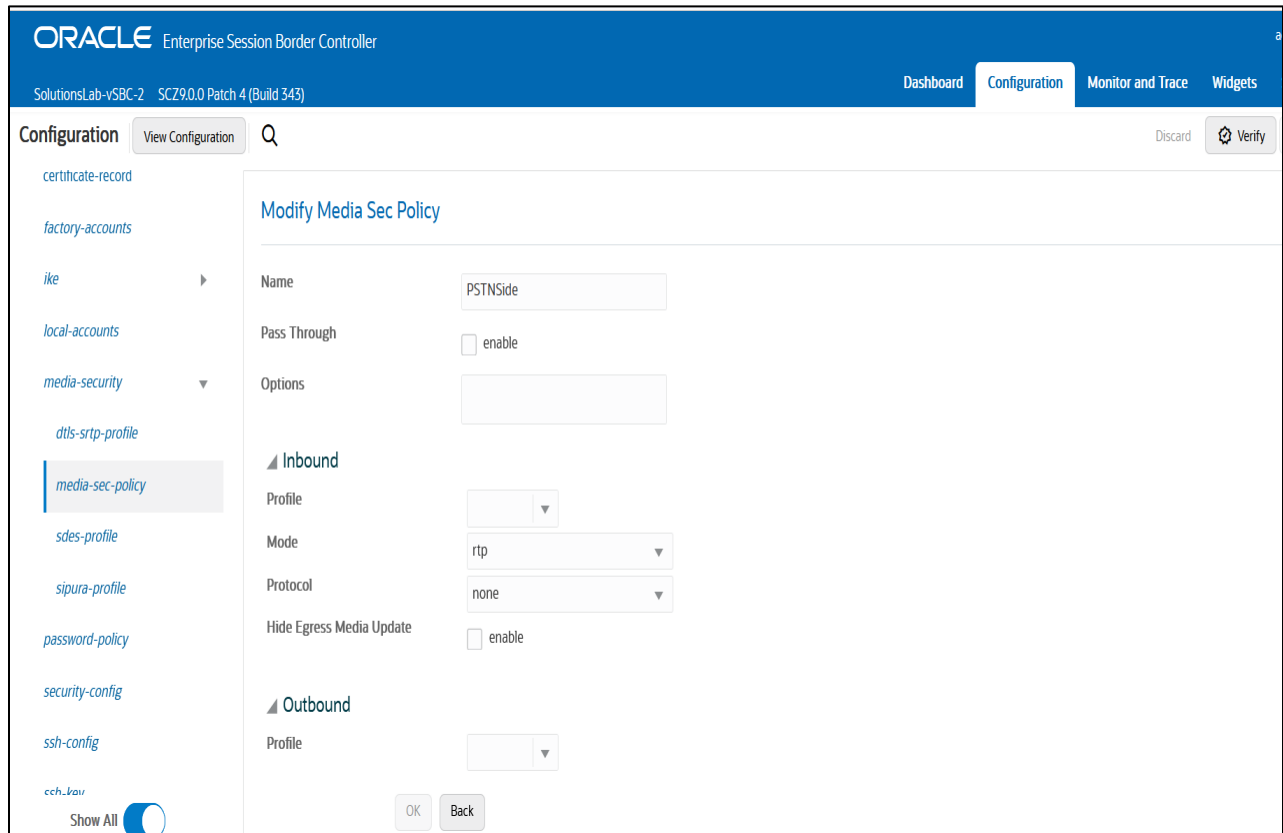


6.16. Configure Media Security Profile

Please go to → Security → Media Security → 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



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.



6.17. Configure Media Optimization (ICE-profile)

Please go to → media-manager → Select show all option → 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.

ORACLE Enterprise Session Border Controller
 SolutionsLab-vSBC-2 10.11.4 SCZ9.3.0 GA (Build 46) admin

Dashboard Configuration Monitor and Trace Widgets System

Configuration View Configuration [Search] Discard Verify Save

codec-policy
 dns-alg-constraints
 dns-config
ice-profile
 media-manager
 media-policy
 msrp-config
 playback-config
 realm-config
 realm-group
 rtc-policy
 static-flow
 steering-pool
 tcp-media-profile

Show All [Toggle]

Modify Ice Profile

Show Advanced [Toggle] Show Configuration

Name: webexice

Stun Conn Timeout: 0 (Range: 0..9999)

Stun Keep Alive Interval: 10 (Range: 0..300)

Stun Rate Limit: 15 (Range: 0..99999)

Mode: NONE

RTCP Stun: enable

OK Back

ORACLE Enterprise Session Border Controller
 SolutionsLab-vSBC-2 10.11.4 SCZ9.3.0 GA (Build 46) admin

Dashboard Configuration Monitor and Trace Widgets System

Configuration View Configuration [Search] Discard Verify Save

media-manager
 codec-policy
 dns-alg-constraints
 dns-config
 ice-profile
 media-manager
 media-policy
 msrp-config
 playback-config
realm-config
 realm-group
 rtc-policy
 static-flow
 steering-pool

Show All [Toggle]

Modify Realm Config

Show Advanced [Toggle] Show Configuration

QoS Enable: enable

Max Bandwidth: 0 (Range: 0..999999999)

Max Priority Bandwidth: 0 (Range: 0..999999999)

Parent Realm: [Dropdown]

DNS Realm: [Dropdown]

Media Policy: [Dropdown]

Nsep Media Policy: [Dropdown]

Media Sec Policy: CiscoWebexSecurity

RTCP Mux: enable

Ice Profile: webexice

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](#)
- [New sip-interface](#)
- [New session-agent](#)
- [New steering-pools](#)
- [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 dependent
 ** Software transcoding

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>

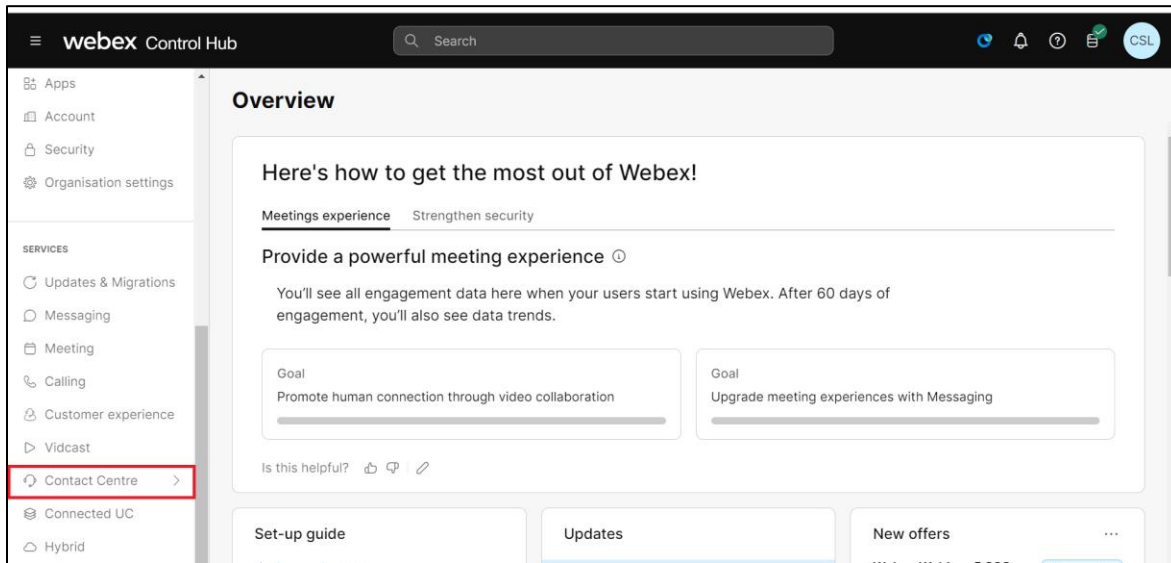
<https://help.webex.com/en-us/article/n5595zd/Webex-Contact-Center-Setup-and-Administration-Guide>

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.

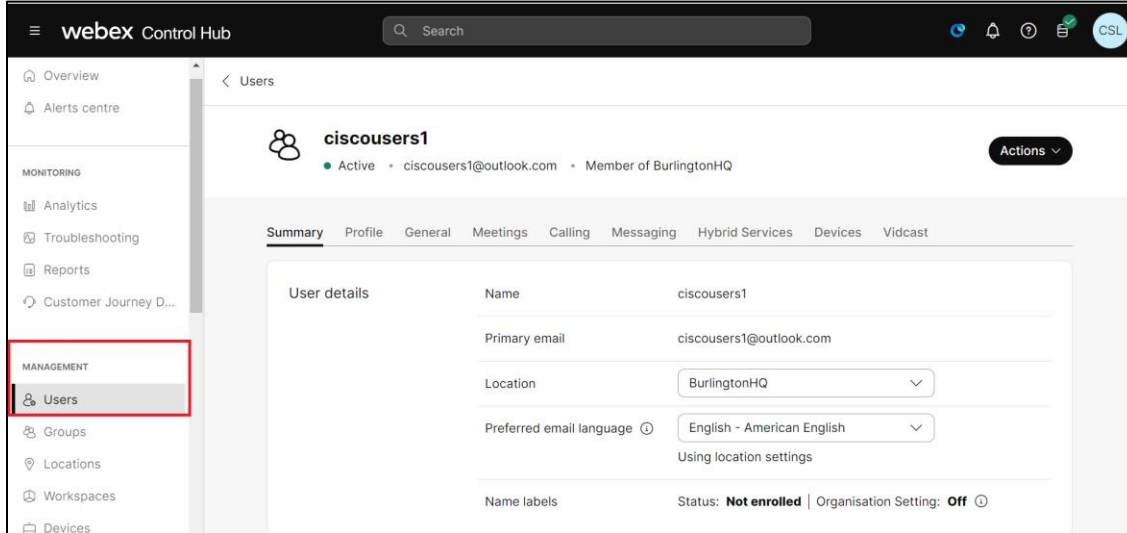
Once Webex CC license is enabled, we will have additional tab for Contact center in Cisco Webex admin portal as shown below. After you click the tab, we will see options to configure Webex CC configuration in the next page. This App note focusses on the basic configuration of Cisco Webex contact center 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.**

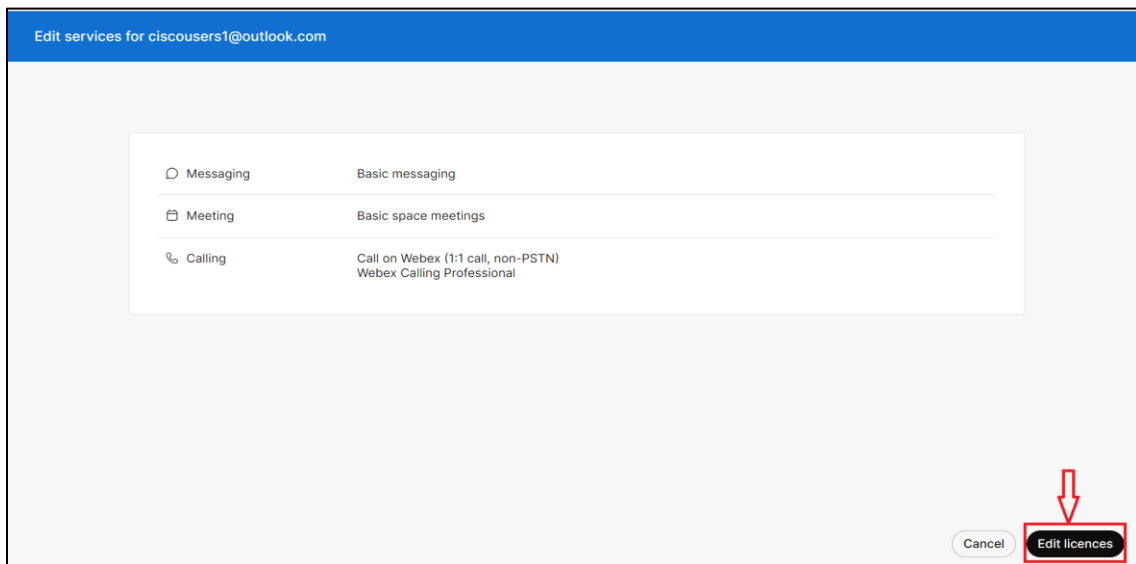
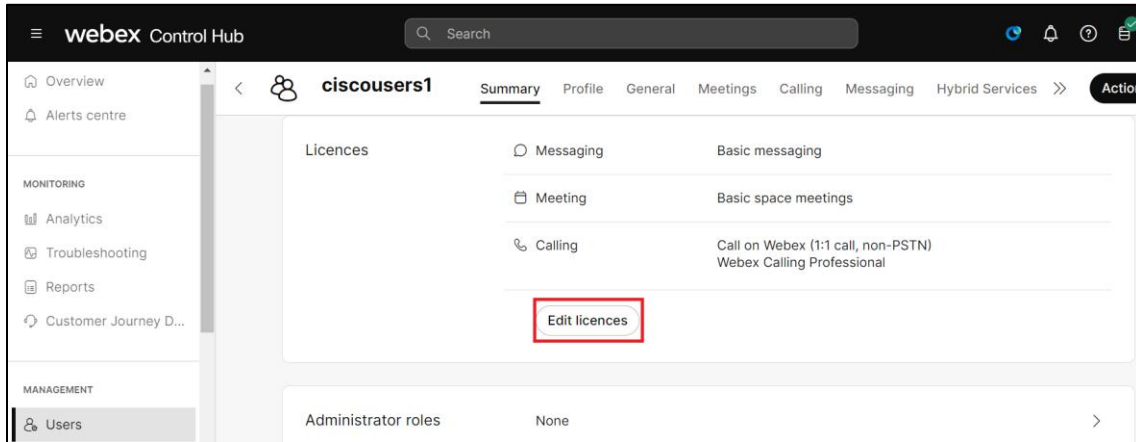
Webex admin page with Contact Center tab enabled:



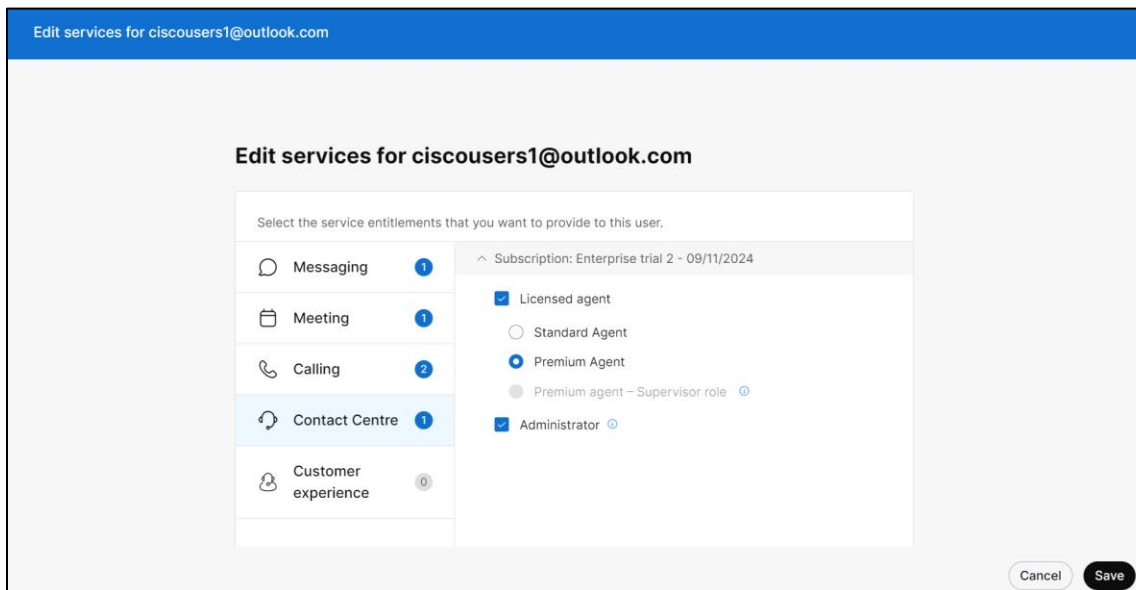
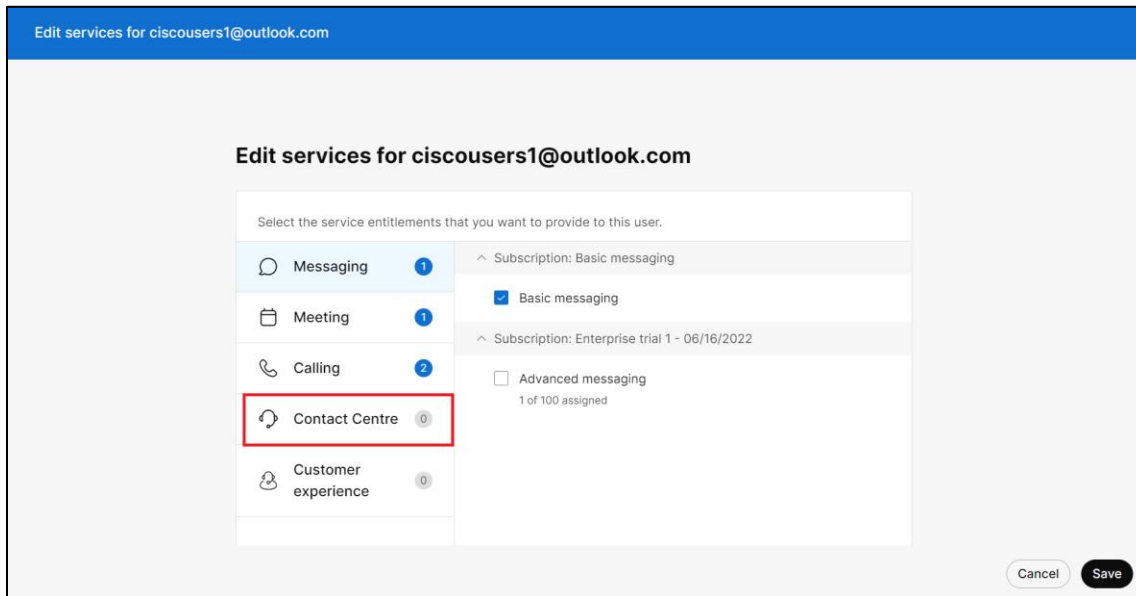
9.1. Enable the Users with Webex CC license

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:



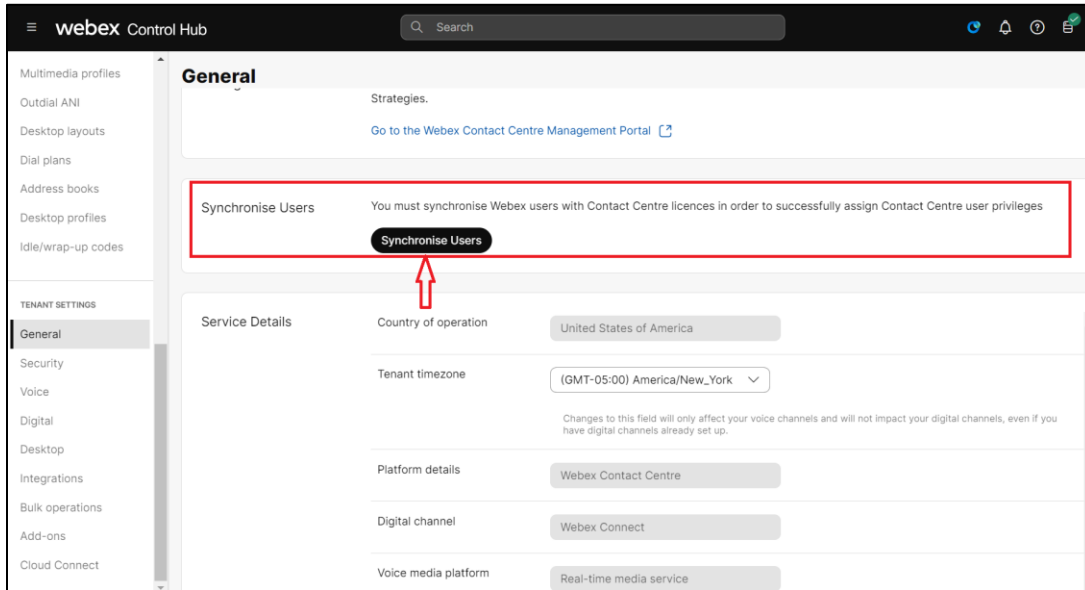


Please click on Contact Center Tab and Enable the Agent type as shown below.
The Agent types are Standard Agent, Premium Agent and Premium Agent with Supervisor role.
Please select the appropriate agent as per your requirements and you can also select the Agent who can also be the Admin for the Webex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



9.2. Synchronize the Users with Webex CC tenant.

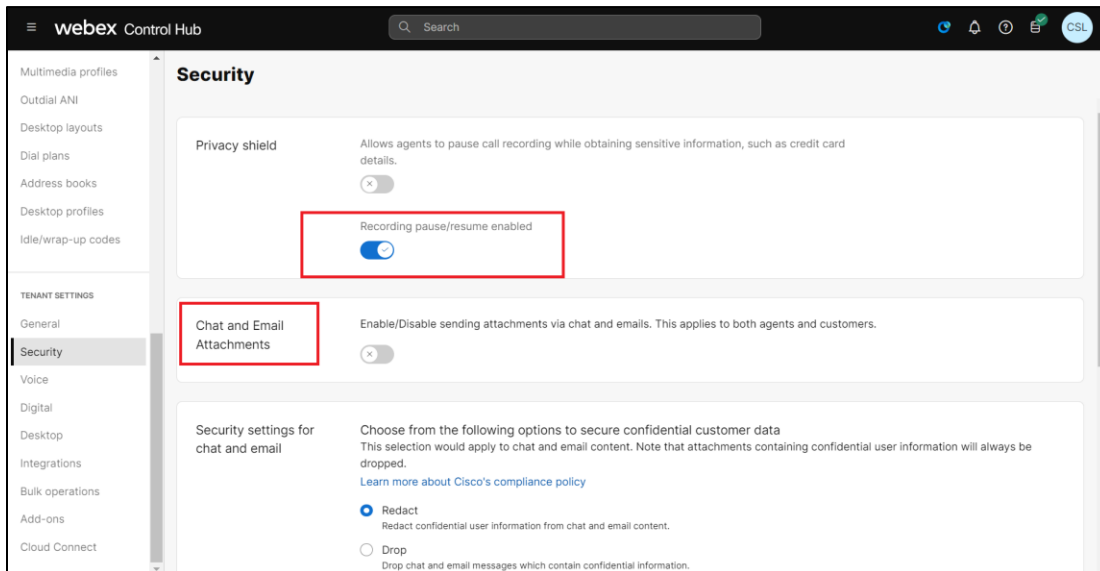
Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- Tenant Settings --- General** and click on **Synchronize Users** tab so that the changes made to Users will be reflected in Cisco Webex CC page. We can also change the time zone from this page and other options can be left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



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.

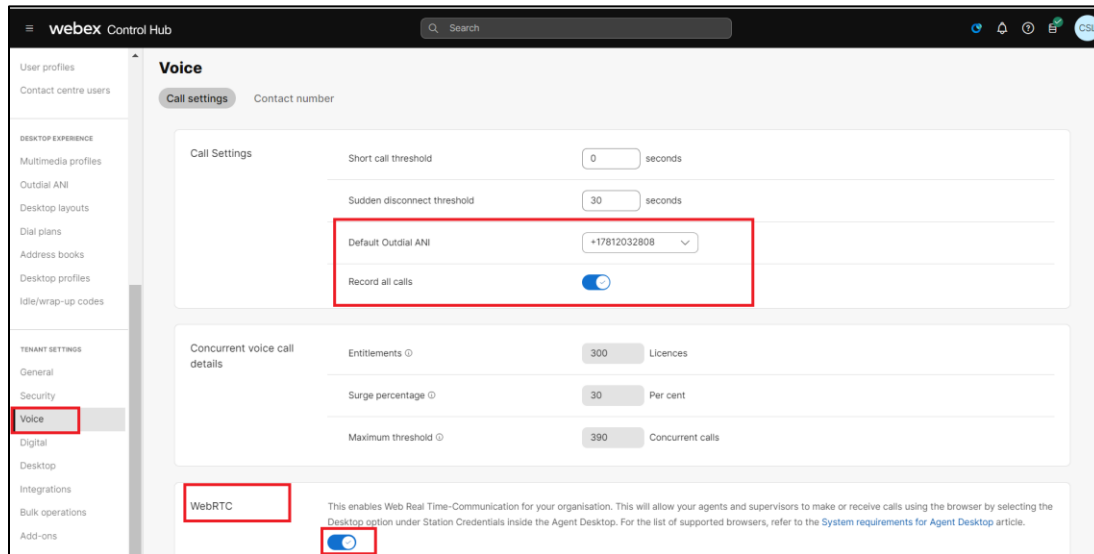
- Enable the Recording Pause/Resume Enabled under Privacy shield tab
- Disable the Chat and Email and Attachments as we are dealing only with Calling option here.



9.4. Configure the settings in Voice Tab.

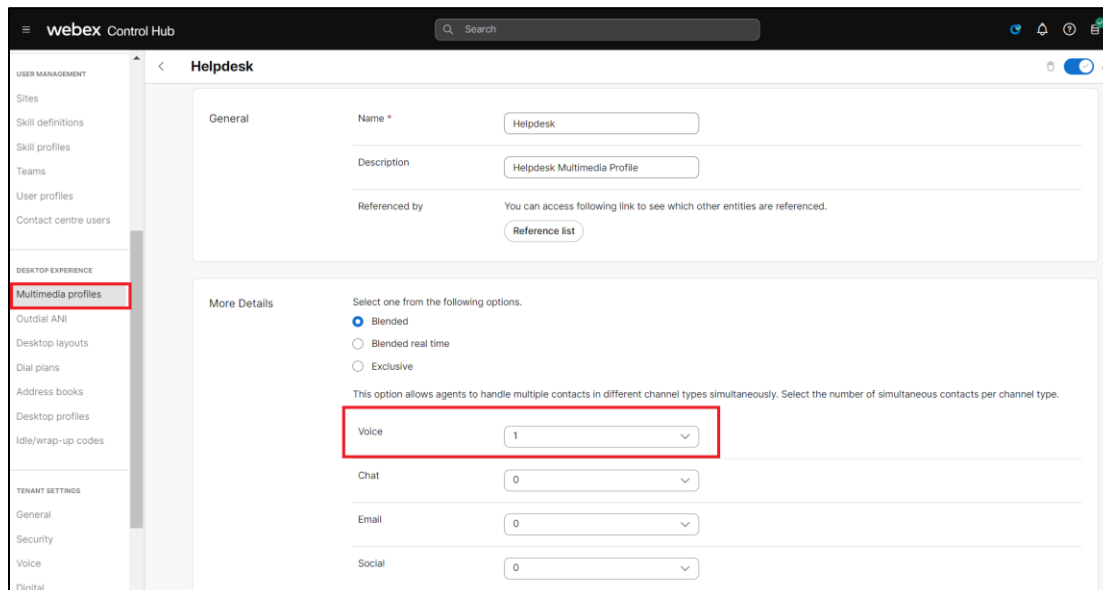
Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- Tenant Settings --- Voice** and provide a DID for default out dial ANI. This is the default number which will be used to call Webex CC from outside and will reach the IVR prompt.

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



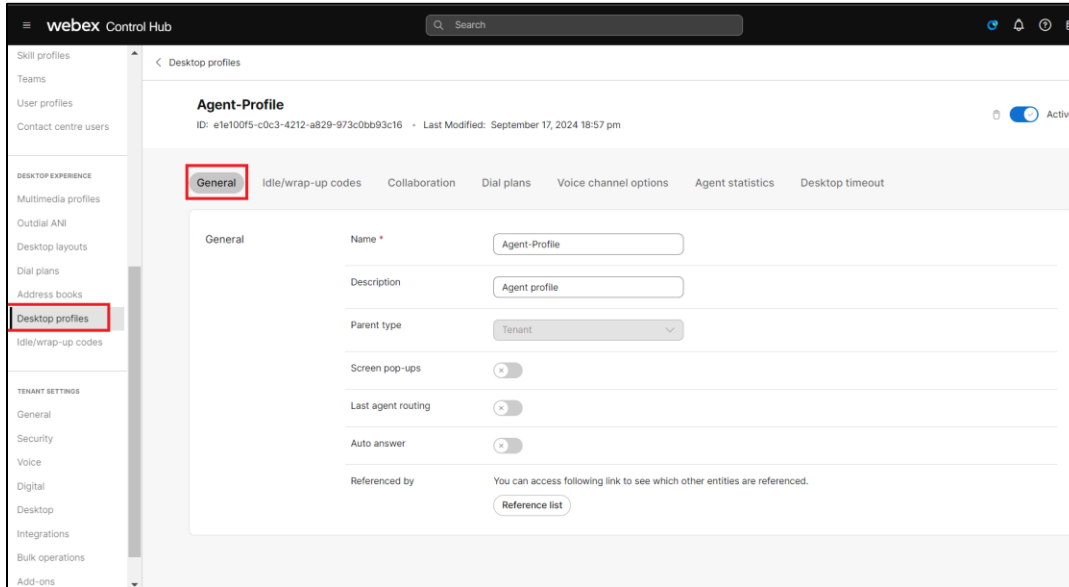
9.5. Configure the Multimedia Profile Tab.

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.

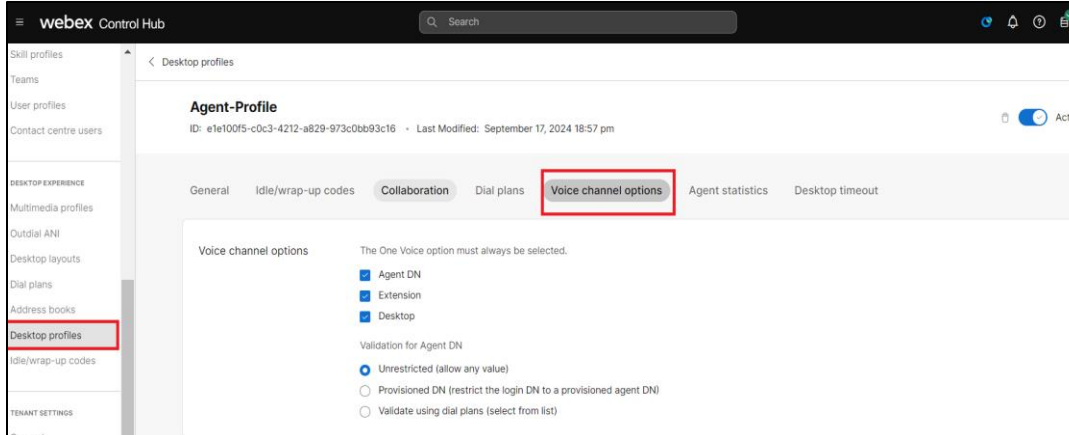


9.6. Configure the Desktop Profile Tab.

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:

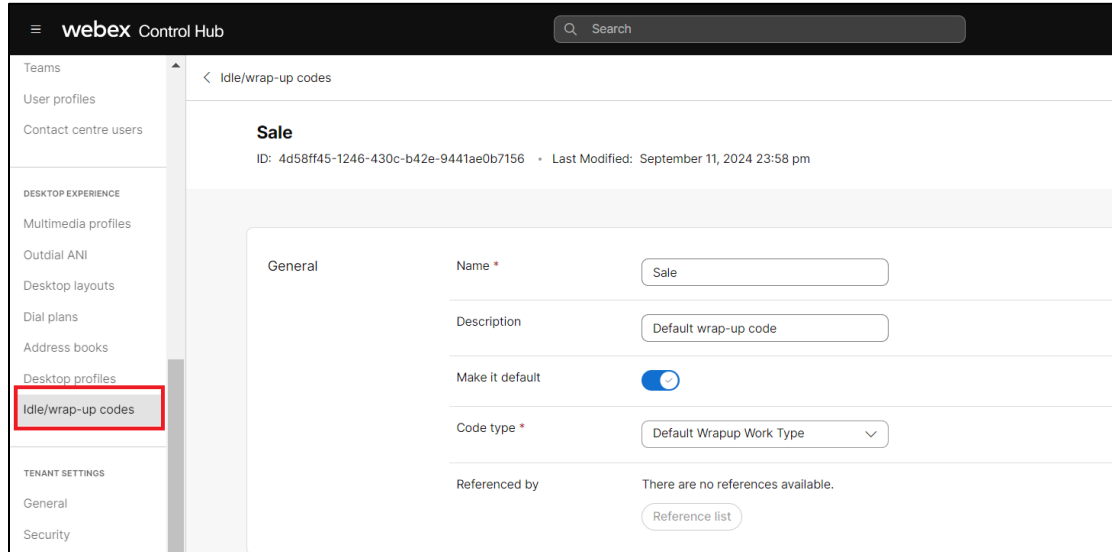


Please click Voice channel options and select the options as shown below.



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

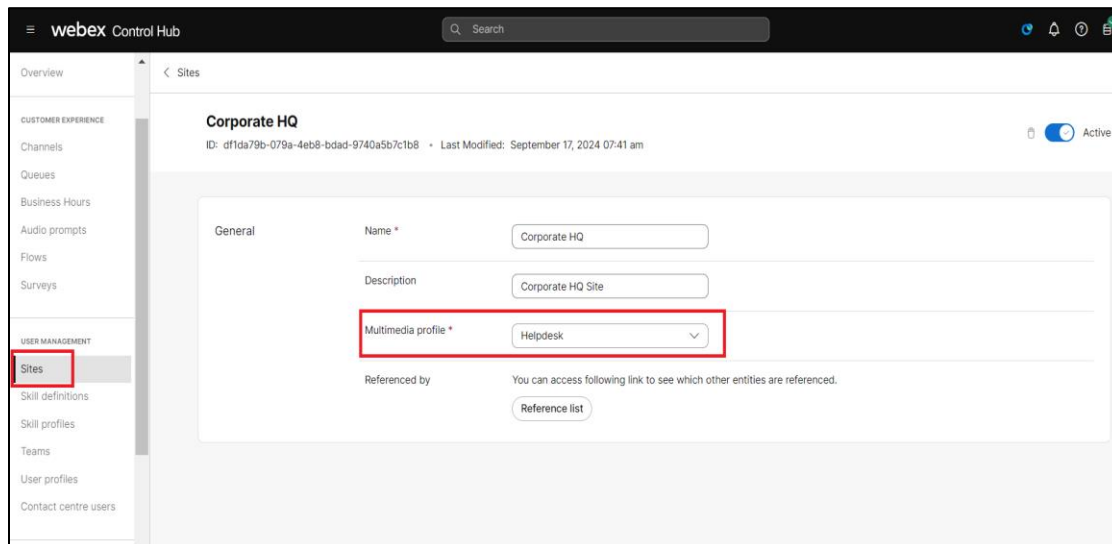
Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- Desktop Experience --- Idle/Wrap-up codes** and create a new profile for the Agents as shown below.



The screenshot shows the Cisco Webex Control Hub interface. The left sidebar is expanded to 'Desktop Experience' > 'Idle/wrap-up codes', which is highlighted with a red box. The main content area shows the configuration for a profile named 'Sale'. The 'Name' field is 'Sale', the 'Description' is 'Default wrap-up code', 'Make it default' is a checked toggle, and the 'Code type' is 'Default Wrapup Work Type'. The 'Referenced by' section indicates no references are available.

9.8. Configure the Sites Tab.

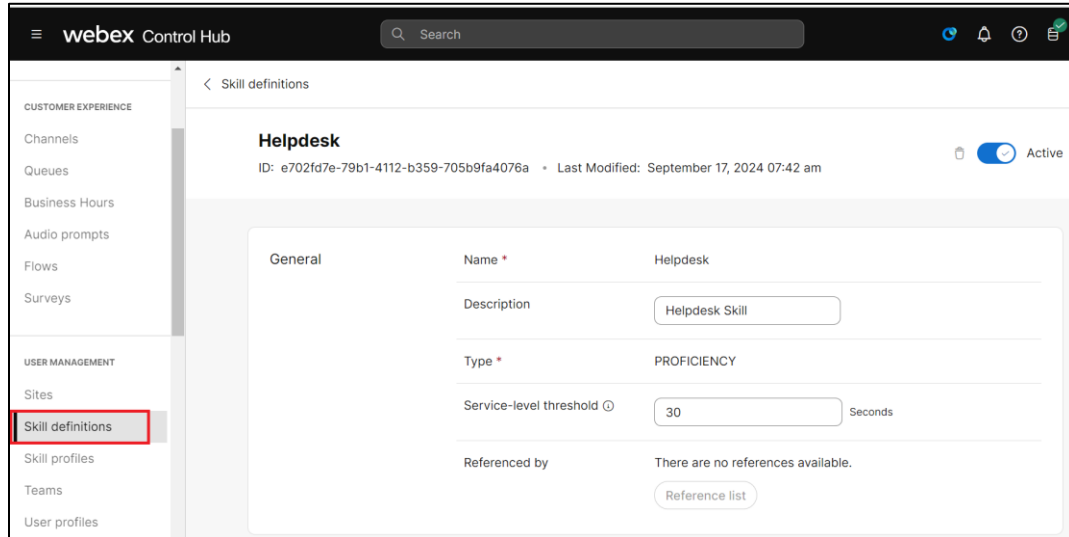
Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- User Management --- Sites** and create a new site. Please assign the Multimedia profile which is created previously to the created site as shown below.



The screenshot shows the Cisco Webex Control Hub interface. The left sidebar is expanded to 'User Management' > 'Sites', which is highlighted with a red box. The main content area shows the configuration for a site named 'Corporate HQ'. The 'Name' field is 'Corporate HQ', the 'Description' is 'Corporate HQ Site', and the 'Multimedia profile' is 'Helpdesk', which is highlighted with a red box. The 'Referenced by' section indicates that a link is available to see which other entities are referenced.

9.9. Configure the Skill Definitions Tab.

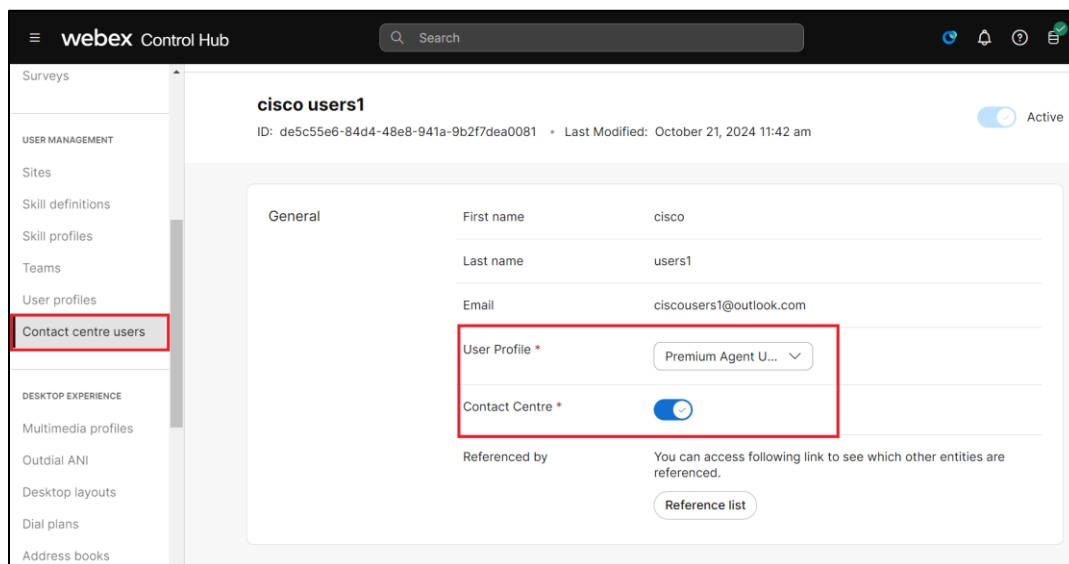
Please go to **Cisco Webex control hub portal – Services ---- Contact Center ---- User Management --- Skill Definitions** and create a new Skill profile as shown below.



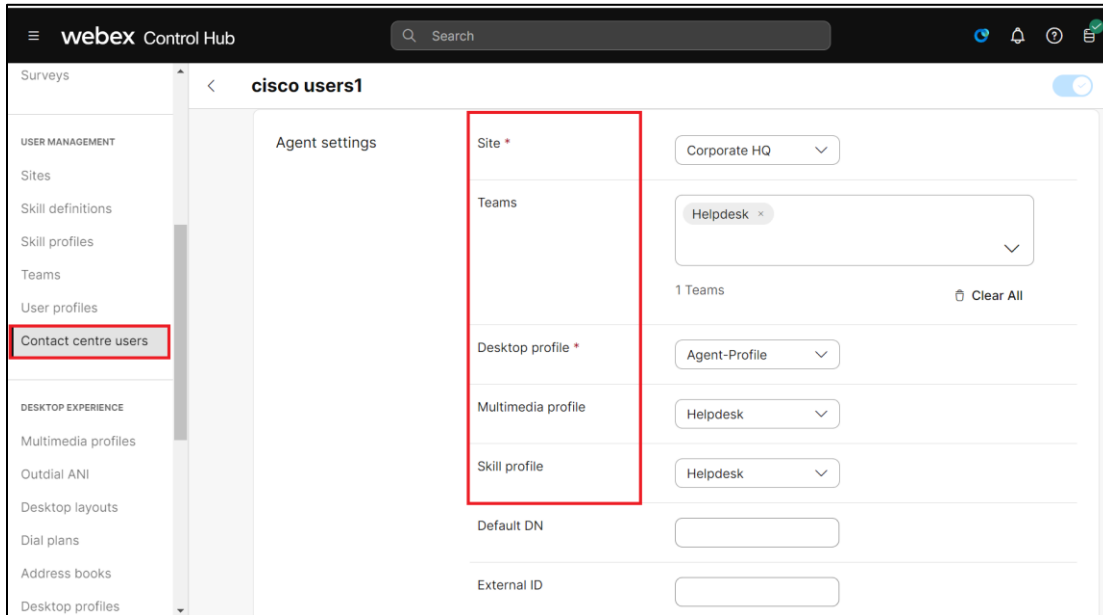
The screenshot shows the Cisco Webex Control Hub interface. The left sidebar is under 'USER MANAGEMENT' and 'Skill definitions' is highlighted with a red box. The main content area shows a 'Skill definitions' page for 'Helpdesk'. The 'Name' field is 'Helpdesk', 'Description' is 'Helpdesk Skill', 'Type' is 'PROFICIENCY', and 'Service-level threshold' is '30' seconds. The 'Referenced by' field shows 'There are no references available.' and a 'Reference list' button.

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.



The screenshot shows the Cisco Webex Control Hub interface. The left sidebar is under 'USER MANAGEMENT' and 'Contact centre users' is highlighted with a red box. The main content area shows a 'Contact centre users' page for 'cisco users1'. The 'First name' is 'cisco', 'Last name' is 'users1', and 'Email' is 'ciscousers1@outlook.com'. The 'User Profile' dropdown is set to 'Premium Agent U...' and the 'Contact Centre' toggle is turned on. The 'Referenced by' field shows 'You can access following link to see which other entities are referenced.' and a 'Reference list' button.

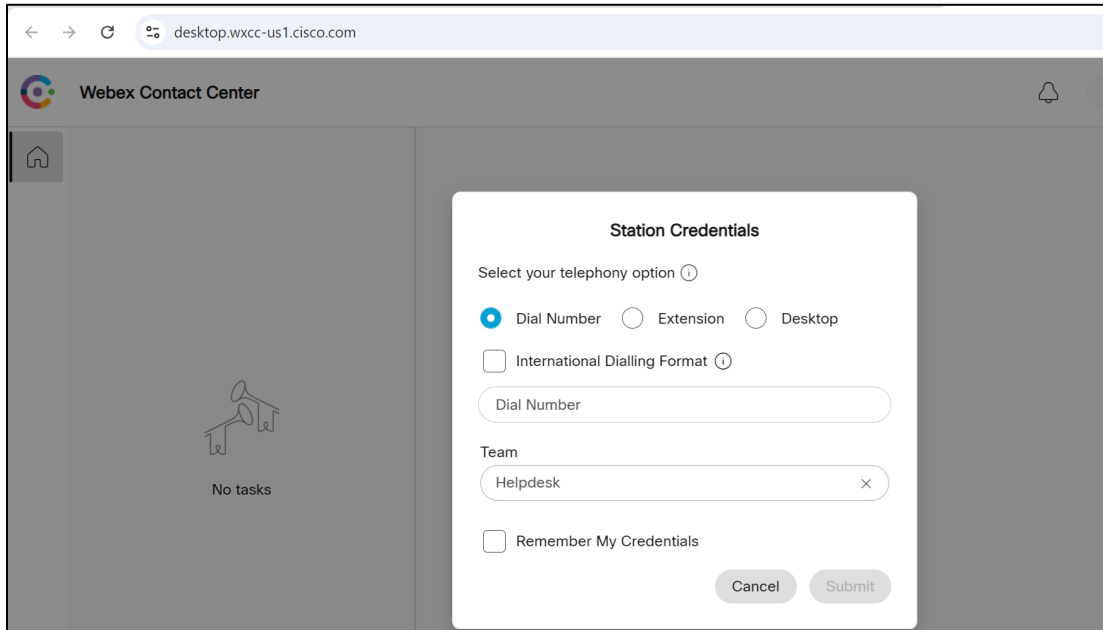


With this, the basic configuration steps of Webex CC are complete. After the basic Cisco Webex CC configuration is complete, agent login can be performed using the below link.

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

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

<p>Select Dial Number for:</p> <ul style="list-style-type: none"> • PSTN based Agent • On Premise Telephony 	<p>Select Extension for:</p> <ul style="list-style-type: none"> • Webex Telephony • Webex App 	<p>Select Desktop for:</p> <ul style="list-style-type: none"> • WebRTC



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

The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes the Oracle logo, the product name 'Enterprise Session Border Controller', and version information 'SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343)'. The main navigation menu contains 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' section is active, showing a search bar and 'View Configuration' and 'Verify' buttons. The left sidebar lists various configuration categories: 'media-manager', 'codec-policy', 'media-manager', 'media-policy', 'realm-config' (highlighted), 'steering-pool', 'security', 'session-router', and 'system'. The main content area is titled 'Modify Realm Config' and contains the following fields:

- Identifier: Cisco_Tenant_2
- Description: (empty text area)
- Addr Prefix: 0.0.0.0
- Network Interfaces: sip0:0.4
- Media Realm List: (empty text area)
- Mm In Realm: enable

At the bottom of the form are 'OK' and 'Back' buttons. A 'Show All' button is visible in the bottom left corner of the configuration area.

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q Discard Verify

media-manager ▼

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security ▶

session-router ▶

system ▶

Show All

Modify Realm Config

Max Priority Bandwidth	0	(Range: 0..999999999)
Parent Realm	CiscoWebexRealm	▼
DNS Realm		▼
Media Policy		▼
Media Sec Policy	CiscoWebexSecurity	▼
RTCP Mux	<input type="checkbox"/>	enable
Ice Profile		▼
Teams Fqdn		
Teams Fqdn In Uri	<input type="checkbox"/>	enable

OK Back

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 SCZ9.0.0 Patch 4 (Build 343) Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q Discard Verify

media-manager ▼

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security ▶

session-router ▶

system ▶

Show All

Modify Realm Config

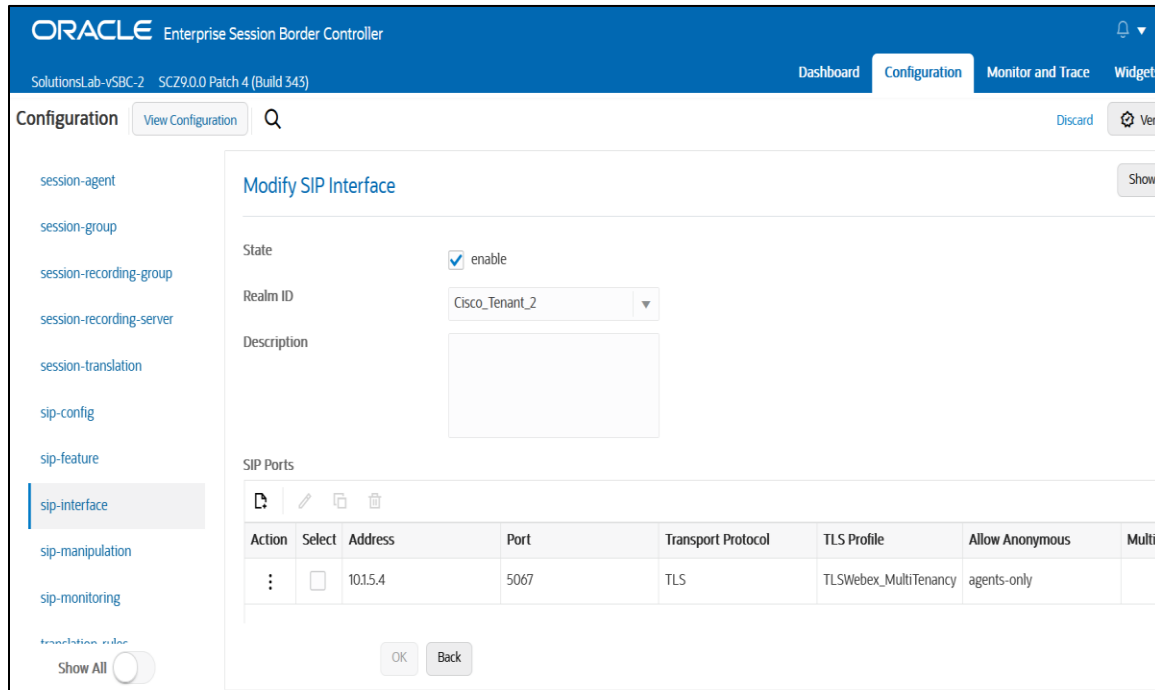
Deny Period	30	(Range: 0..4294967295)
Session Max Life Limit	0	
Untrust Cac Failure Threshold	0	(Range: 0..4294967295)
Subscription Id Type	END_USER_NONE	▼
Trunk Context	vmsbc.cbusolutionslab.com	
Early Media Allow		▼
Enforcement Profile		▼
Additional Prefixes		
Restricted Latching	none	▼

OK 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.



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 $TRUNK_GROUP_CONTEXT
  header-rule
    name ChangeToIP
    header-name TO
    action manipulate
    comparison-type pattern-rule
    msg-type any
    methods INVITE
  
```

```

element-rule
    name          ChangeTo
    type          uri-host
    action        replace
    new-value     "us01.sipconnect.bclد.Webex.com"

header-rule
    name          ChangeContactHost
    header-name   Contact
    action        manipulate
    msg-type     any
    methods       INVITE, ACK
    element-rule
        name      contacthost
        type      uri-host
        action    replace
        new-value $TRUNK_GROUP_CONTEXT

header-rule
    name          AddContactOptions
    header-name   Contact
    action        add
    msg-type     request
    methods       OPTIONS
    new-value     <sip:ping@"+$TRUNK_GROUP_CONTEXT+":5061;transport=tlс>

header-rule
    name          ChangeFromIP
    header-name   FROM
    action        manipulate
    msg-type     any
    methods       INVITE
    element-rule
        name      ChangeFrom
        type      uri-host
        action    replace
        new-value $TRUNK_GROUP_CONTEXT

header-rule
    name          Addplus1Contact
    header-name   Contact
    action        manipulate
    comparison-type pattern-rule
    element-rule
        name      Tendigits
        type      uri-user
        action    replace
        comparison-type pattern-rule
        match-value ^[0-9]{10}$
        new-value  \+1+$ORIGINAL

element-rule
    name          ElevenDigits
    type          uri-user
    action        replace
    comparison-type pattern-rule
    match-value  ^[0-9]{11}$
    new-value    \++$ORIGINAL

```

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:

The screenshot shows the 'Modify Local Policy' configuration page in the Oracle Enterprise Session Border Controller. The page is titled 'Modify Local Policy' and includes the following fields:

- From Address:** * X
- To Address:** 17815551212 X, 17815551213 X
- Source Realm:** SIPTrunk X
- Description:** (Empty text area)
- State:** enable

The left sidebar shows a list of configuration categories, with 'local-policy' selected. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The page also features a search bar and 'Discard' and 'Verify' buttons.

The screenshot shows the 'Modify Local Policy' configuration page in the Oracle Enterprise Session Border Controller, displaying the 'Policy Attributes' section. The page is titled 'Modify Local Policy' and includes the following fields:

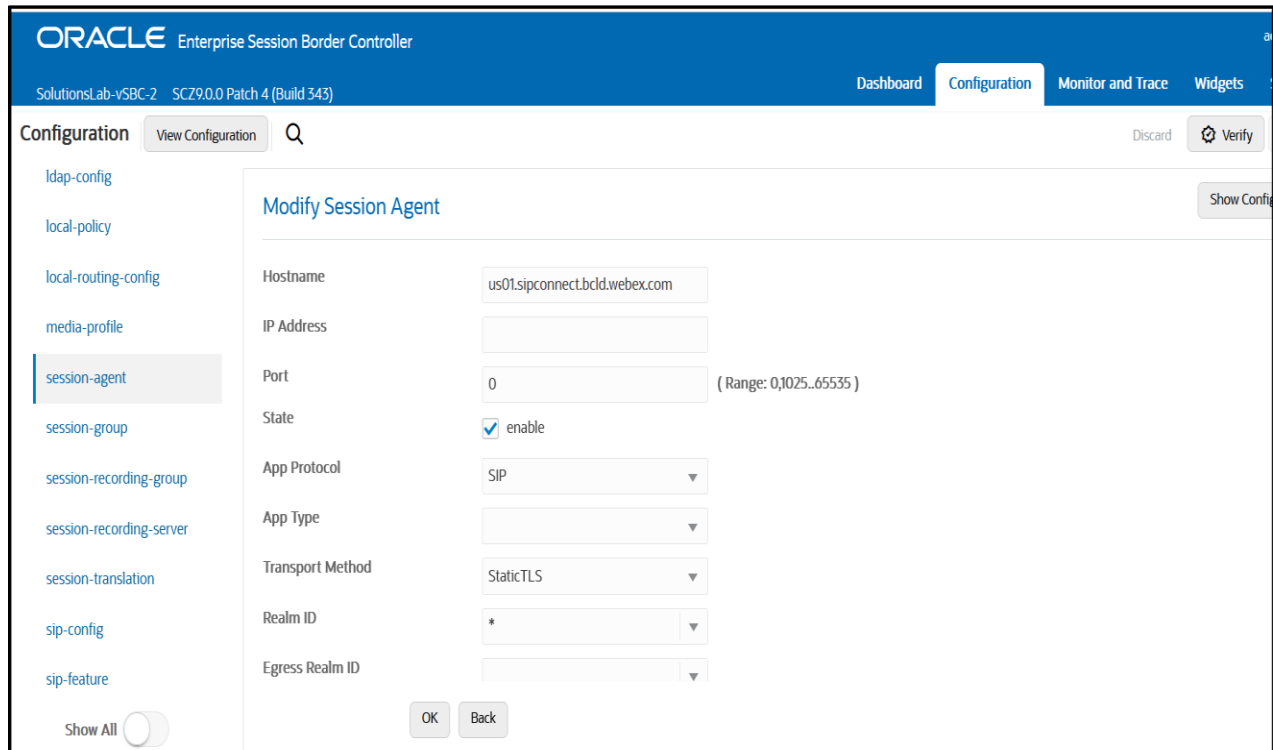
- Source Realm:** SIPTrunk X
- Description:** (Empty text area)
- State:** enable
- Policy Priority:** none

The 'Policy Attributes' section is a table with the following columns: Action, Select, Next Hop, Realm, Action, Terminate ..., Cost, State, App Protocol, Lookup, Next Key, and Auth Us. The table contains one row of data:

Action	Select	Next Hop	Realm	Action	Terminate ...	Cost	State	App Protocol	Lookup	Next Key	Auth Us
:	<input type="checkbox"/>	us01.sipconn...	Cisco_Tenant_2	replace-uri	disabled	0	enabled		single		

The bottom of the page includes a 'Show All' toggle and 'OK' and 'Back' buttons.

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**



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 [link](#) 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 tmmb
```

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

```

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-list
    serverAuth
    clientAuth

certificate-record
  name          CloudSBCSolLab
  unit          SolutionsLab
  common-name   cloudsbc.cgbusolutionslab.com
  extended-key-usage-list
    serverAuth
    clientAuth

certificate-record
  name          GoDaddyCrossCert
  unit          www.godaddy.com
  common-name   GoDaddy G1 to G2 Cross Certificate

certificate-record
  name          GoDaddyIntermediate
  unit          www.godaddy.com
  common-name   GoDaddy Secure Server Certificate - G2

certificate-record
  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
    next-hop    us01.sipconnect.bclld.webex.com
    realm       CiscoWebexRealm
    action      replace-uri

```

```

media-manager
media-sec-policy
  name          CiscoWebexSecurity
  inbound
    profile      CiscoSRTP
    mode         srtp
    protocol     sdes
  outbound
    profile      CiscoSRTP
    mode         srtp
    protocol     sdes
media-sec-policy
  name          PSTNSide
network-interface
  name          s0p0
  ip-address    155.212.214.90
  netmask       255.255.255.0
  gateway       155.212.214.65
network-interface
  name          s1p0
  ip-address    10.1.3.4
  netmask       255.255.255.0
  gateway       10.1.3.1
  dns-ip-primary 9.9.9.9
  dns-ip-backup1 8.8.8.8
  dns-ip-backup2 8.8.4.4
  dns-domain    cgbusolutionslab.com
phy-interface
  name          s0p0
  operation-type Media
phy-interface
  name          s1p0
  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 30
  ping-response enabled
session-agent
  hostname      us01.sipconnect.bcl.d.webex.com
  port          0
  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-interface
  realm-id      CiscoWebexRealm
  sip-port
    address     10.1.3.4
    port        5061
    transport-protocol  TLS
    tls-profile  TLSWebex
    allow-anonymous  agents-only
  spl-options
  HeaderNatPublicSipIfIp=20.96.25.165,HeaderNatPrivateSipIfIp=10.1.3.4
  out-manipulationid  ToCiscoWebex
  user-agent          Oracle/VM/9.0.0p4
sip-interface
  realm-id      SIPTrunk
  sip-port
    address     155.212.214.90
    allow-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              ToCiscoWebex
  header-rule
    name            addplus
    header-name     Contact
    action           manipulate
    comparison-type pattern-rule
    msg-type        request
    methods         Invite
    element-rule
      name          TenDigits
      type          uri-user
      action        replace
      comparison-type pattern-rule
      match-value   ^[0-9]{10}$
      new-value     \+1+${ORIGINAL}
    element-rule
      name          ElevenDigits
      type          uri-user
      action        replace
      comparison-type pattern-rule
      match-value   ^[0-9]{11}$

```

```

header-rule
  name          ChangeContactHost
  header-name   Contact
  action        manipulate
  msg-type      any
  methods       ACK,INVITE
  element-rule
    name        contacthost
    type        uri-host
    action      replace
    new-value   $TRUNK_GROUP_CONTEXT
header-rule
  name          AddContactOptions
  header-name   Contact
  action        add
  msg-type      request
  methods       OPTIONS
  new-value     <sip:ping@"+$TRUNK_GROUP_CONTEXT+":5061;transport=tls>"
sip-manipulation
  name          RemoveDTG
  description
  split-headers
  join-headers
  header-rule
    name        StripDTG
    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

```



```

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

sip-manipulation
  name          ToPSTN
  description
  split-headers
  join-headers
  header-rule
    name        StripDTG
    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
new-value

header-rule
name DeleteRecvInfo
header-name Recv-Info
action delete
comparison-type case-sensitive
msg-type any
methods BYE,INVITE,OPTIONS

ice-profile
name webexice
stun-conn-timeout 0
stun-keep-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