



Oracle SBC as a Local Gateway with Cisco Webex Calling and Contact Center

Technical Application Note



Disclaimer

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

Revision History

Version	Description of Changes	Date
1.0	<ul style="list-style-type: none">Oracle SBC integration with Cisco Webex Calling as 3rd party Local Gateway (LGW)	30 th October 2022
1.1	<ul style="list-style-type: none">Added Appendix B section to the document for the new feature which supports Cisco DTMF with OPUS codec	05 th January 2023
1.2	<ul style="list-style-type: none">Added ACLI and GUI Cert ImportAdded multitenancy monitoring.Added ACK method to Sip Manip.SBC version changed to 9.xIce Config for Media OptimizationIncluded GCM ciphers for SRTP.Added support for Cisco Webex Contact CenterModified Caveat to include software fix no available	08 th November 2024
1.3	<ul style="list-style-type: none">SBC v.9.3 Re-Certification Updates	

1 Table of Contents

1.	INTENDED AUDIENCE	5
2	VALIDATED ORACLE SBC VERSION.....	5
3	DOCUMENT OVERVIEW	5
4	CISCO WEBEX CALLING.....	5
5	INTRODUCTION.....	6
5.1	AUDIENCE.....	6
5.2	REQUIREMENTS	6
5.3	ARCHITECTURE.....	7
6	CISCO WEBEX CONFIGURATION.....	7
6.1	TRUNK CONFIGURATION	8
6.2	ROUTE GROUP	10
6.3	DIAL PLANS	11
6.4	WEBEX EDGE PROXY ADDRESS	12
7	CONFIGURING THE SBC	13
7.1	SYSTEM-CONFIG.....	14
7.1.1	NTP-Config.....	15
7.2	NETWORK CONFIGURATION	15
7.2.1	Physical Interfaces	16
7.2.2	Network Interfaces	16
7.3	SECURITY CONFIG	17
7.3.1	Certificate Records.....	17
7.3.2	TLS Profile.....	22
7.3.3	Media Security	22
7.3.4	Media Security Policy	23
7.4	TRANSCODING CONFIGURATION (OPTIONAL).....	25
7.4.1	Codec Policies	25
7.4.2	ICE Profile	25
7.5	MEDIA CONFIGURATION.....	26
7.5.1	Media Manager	26
7.5.2	Realm Config	27
7.5.3	Steering Pools.....	28
7.6	SIP CONFIGURATION	29
7.6.1	Sip-Config	29
7.6.2	Sip Manipulation.....	30
7.6.3	Sip Interface	33
7.6.4	Session Agents	34
7.7	ROUTING CONFIGURATION.....	34
7.8	SIP ACCESS CONTROLS.....	36
8	ORACLE SBC CONFIGURATION ASSISTANT	37
8.1	CISCO WEBEX CALLING CONFIGURATION ASSISTANT	37
9	VERIFY CONNECTIVITY	41
10	SBC SCALING.....	42
11	ORACLE SBC INTEGRATION WITH CISCO WEBEX CONTACT CENTER.....	43
11.1	ASSIGNING WEBEX CONTACT CENTER LICENSES TO USERS	44

11.2	SYNCHRONIZE USERS WITH THE WEBEX CONTACT CENTER TENANT.....	46
11.3	CONFIGURE SETTINGS IN THE SECURITY TAB.....	46
11.4	CONFIGURE SETTINGS IN THE VOICE TAB.....	47
11.5	CONFIGURE THE MULTIMEDIA PROFILE TAB.....	47
11.6	CONFIGURE THE DESKTOP PROFILE TAB.....	48
11.7	CONFIGURE THE IDLE/WRAP-UP CODES TAB.....	49
11.8	CONFIGURE THE SITES TAB.....	49
11.9	CONFIGURE THE SKILL DEFINITIONS TAB.....	50
11.10	CONFIGURE THE CONTACT CENTER USERS TAB.....	50
12	APPENDIX A	53
12.1	MULTI-TENANCY.....	53
12.1.1	Security Configuration.....	53
12.1.2	Additional Configuration Elements for Multitenancy	56
13	APPENDIX B	60
13.1	ORACLE SBC DEPLOYED BEHIND NAT.....	60
14	KNOWN ISSUES AND LIMITATIONS	61
14.1	SIP OPTIONS PING FROM MULTIPLE REALMS TO GLOBAL SESSION AGENTS.....	61
14.2	VIDEO CALL ISSUES WHEN CALLS ORIGINATE FROM CISCO CUCM TOWARDS CISCO WEBEX.....	61
14.3	ICE CANDIDATE PRIORITY ATTRIBUTE INTEROPERABILITY WITH CISCO MPP HANDPHONES	62
14.4	ONE-WAY AUDIO AFTER CALL TRANSFER WITH MEDIA OPTIMIZATION.....	63
15	ACLI RUNNING CONFIGURATION	64

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 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 3950
- A P4600
- AP 4900
- AP 6350
- AP 6400
- VME
- Oracle SBC on Public Cloud

3 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**.

4 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. 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 and 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.

5 Introduction

5.1 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.

5.2 Requirements

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

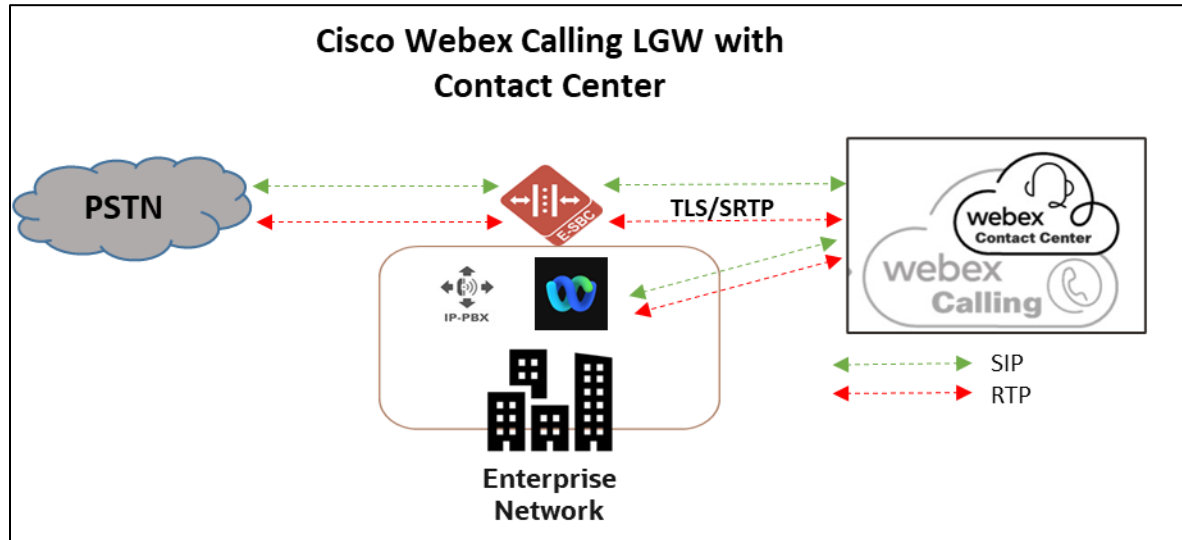
<https://help.webex.com/en-us/article/n4cprps/Prepare-Your-Environment-for-Webex-Calling>

- 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

5.3 Architecture



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

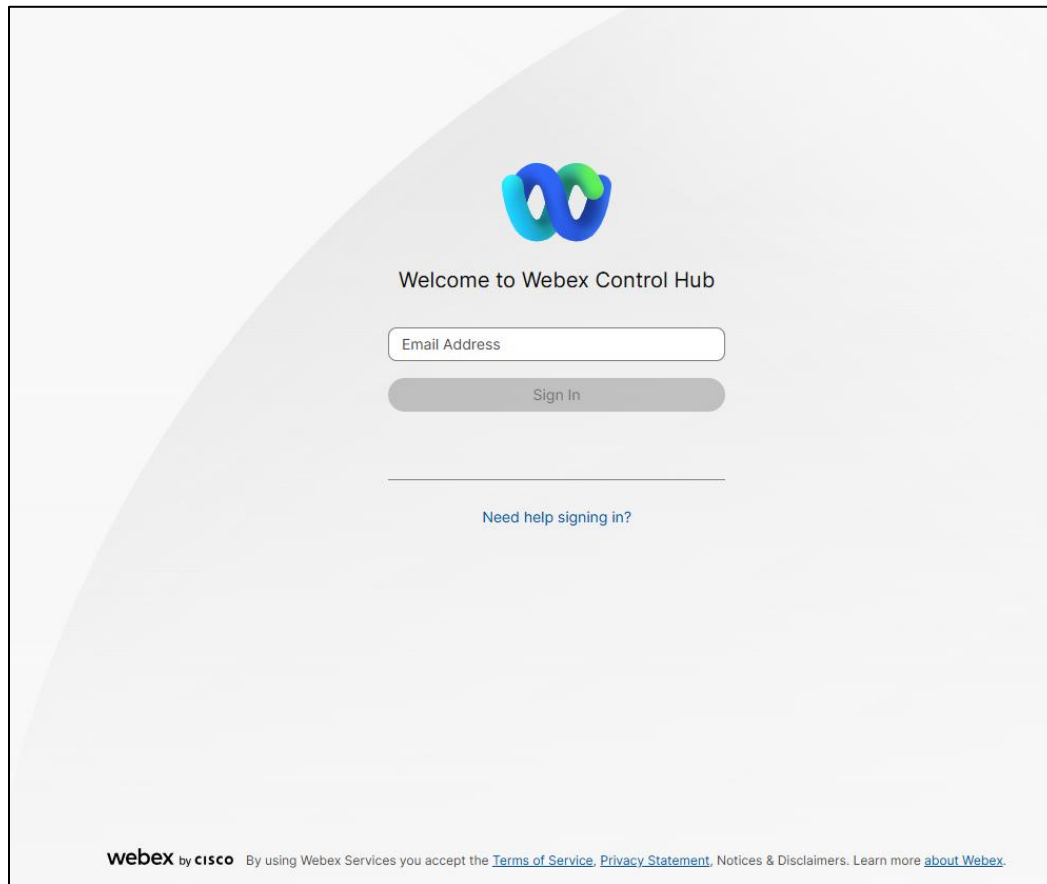
- Phase 1 – Configuring Cisco Webex Calling with for the Oracle SBC as a local gateway (LGW)
- Phase 2 – Configuration of the Oracle SBC.
- Phase 3 – Configuring the Cisco Webex Contact Center.

6 Cisco Webex Configuration

The configuration of Cisco Webex 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.

Login to **Webex Control Hub** with admin credentials.

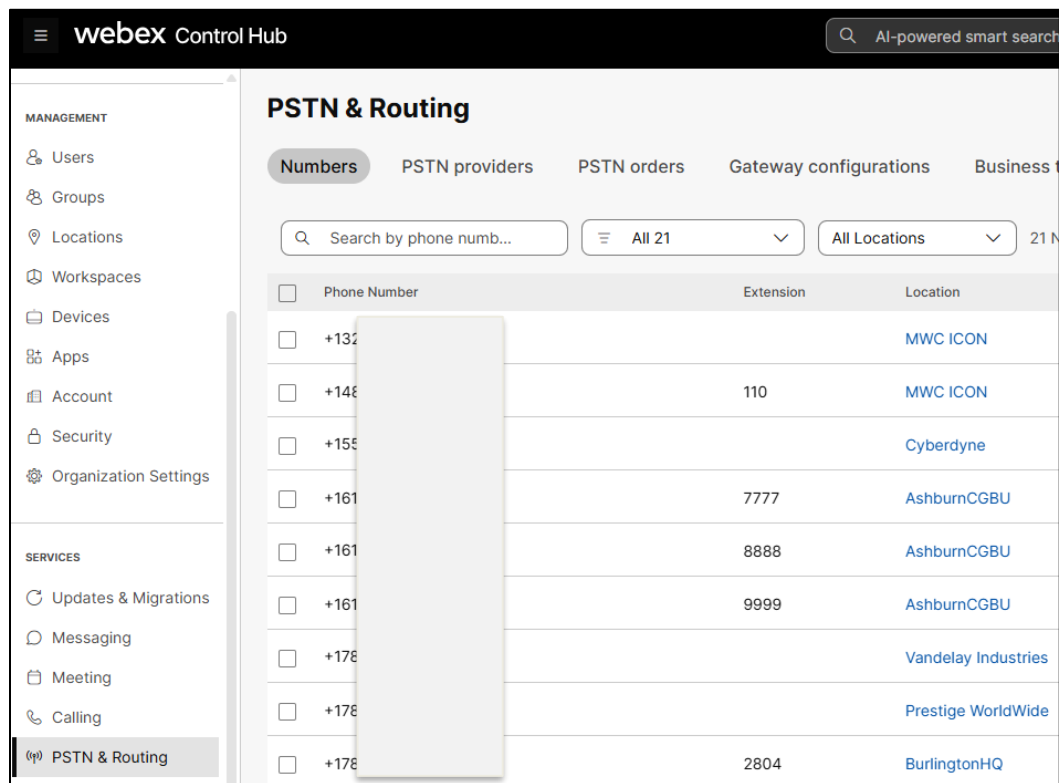
Note: This document assumes that you have already set up your Cisco account, configured your location, and registered the necessary FQDN(s) in the Cisco Control Hub. Please ensure all these prerequisites are completed before proceeding with the trunk configuration to connect to the Oracle SBC



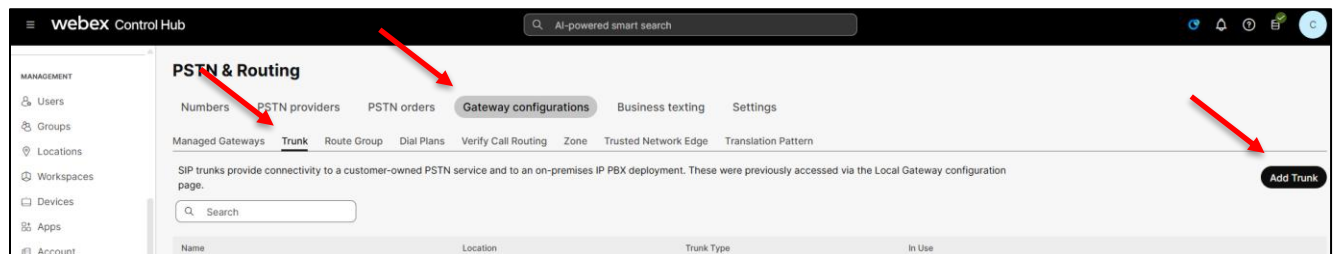
6.1 Trunk Configuration

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.

- In the left menu, select **PSTN & Routing** from the menu:



Next, at the top, click on Gateway configurations/Trunk, top right, click Add Trunk:



In the Add Trunk Configuration window, configure the following:

- Choose a Location from the drop down menu
- Name
- Trunk Type (Certificate Based)
- Select Oracle Session Border Controller for Device Type
- Select the radio button for FQDN
- Select your domain from the drop down menu
- Add the hostname
- Add Port
- Enter the Maximum number of concurrent Calls (must be in range <250, 6500>)

Add Trunk

Location
This location is where the trunk is physically connected. To create a new location, visit the [Locations](#) page.

BurlingtonHQ

Name
SolutionsLab

Trunk Type
Choose the right trunk type for this local gateway. [Learn more](#) on trunk type

Certificate based

Device Type
Oracle Session Border Controller

Enterprise Session Border Controller (SBC) Address
Select the type and enter an FQDN or SRV address for Webex Calling to reach out to your Enterprise SBC. You must have the domain for your SBC's FQDN/SRV [claimed or verified](#) before you can use this address. [Manage your domains](#)

☒ FQDN
☐ SRV

Hostname * Domain * Port *

testing cgbusolutionslab.com 5061

☒ Valid address

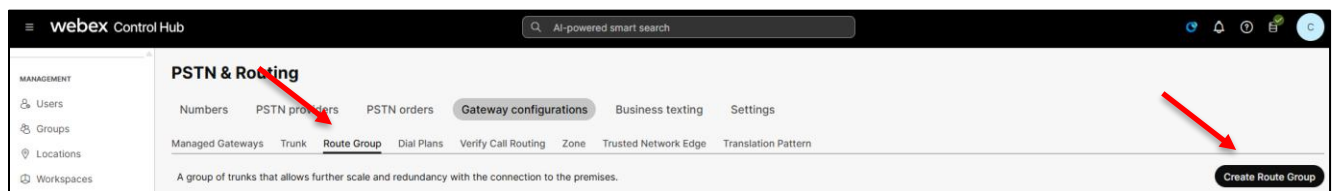
Cancel Save

- Click Save at the bottom

6.2 Route Group

A group of trunks that allows further scale and redundancy with the connection to the premises.

Under PSTN & Routing, select **Route Group** from the top menu, then select **Create Route Group**:



In the Create Route Group window, configure the following:

- Name
- Under Trunks, select the trunk we just added from the drop down menu
- Select a priority from the drop down menu (Priority 1 is highest)

Create Route Group

If you have a large number of locations or trunks, create a route group for load sharing and scale of connection to the premises.

Name

SolutionsLab

Trunks

You can add up to **10** trunks in a route group. The server considers available trunks at the highest priority first (1 being the highest) before it tries those with lower priority. Among those with the same priority, calls are distributed evenly in a load-balancing fashion.

Add Trunk

1 trunk added

Trunk Name	Priority
cloudsbc	1

Cancel

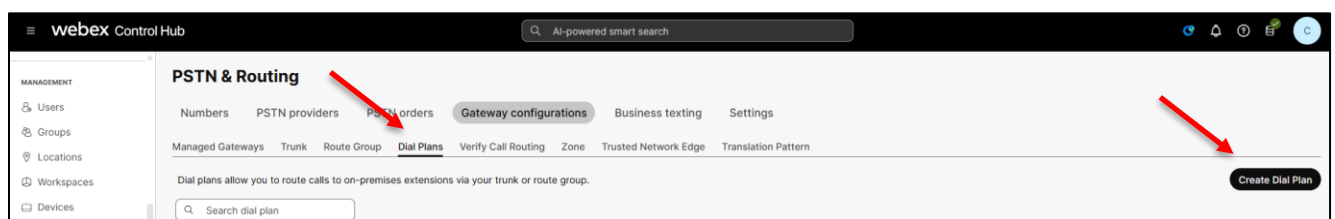
Save

Click Save at the bottom.

6.3 Dial Plans

Dial plans allow you to route calls to on-premises extensions via your trunk or route group.

Under PSTN & Routing, select **Dial Plans** from the top menu, then select **Create Dial Plan**:



In the Create Dial Plan window, configure the following:

- Name
- Routing Choice (you can select either Trunk or Route Group. In this example, we'll select the trunk)
- Enter a Dial pattern or import CSV (optional)

Create Dial Plan ✕

Create a dial plan to route internal calls to your PBX site. Calls are routed when they contain routing prefixes associated with the specified trunk or route group.

Name

SolutionsLab ✕

Routing Choice
When internal calls match with a pattern, calls will be routed to the specified trunk or route group.

cloudsbc ▼

Dial Patterns

A pattern can be a +E.164 prefix, a location dialing (ESN) prefix, or a SIP URI domain. A pattern needs to be unique. The longest match will be applied. Add up to 200 dial patterns at a time. To add more all at once, use CSV import.

Wildcards:

- "!" represents a sequence of one or more digits; only allowed with +E.164 prefixes. ⓘ
- "X" represents a single number (0-9). ⓘ
- A domain with a leading "*" indicates all sub-domains of that domain. For example, *.example.com.

[↑ Import CSV](#)

cgbuburlington.com ✕

Enter dial patterns separated by commas

1 dial pattern [Clear All](#)

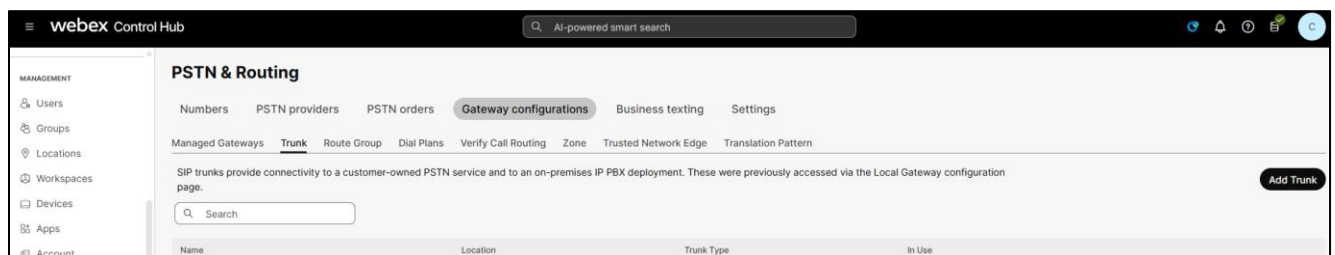
Cancel
Save

Click Save at the bottom.

6.4 Webex Edge Proxy Address

To view the destination (Webex Edge proxy) address, which will be used as the Session Agent in the Oracle SBC to connect to Cisco Webex:

Under PSTN & Routing, select Trunk from the top menu:



Next, click on the trunk created in [section 6.1](#)

cloudsbc

×

Trunk > Details

Status ⓘ

● Online

Trunk Type

Certificate based

Device

Oracle Session Border Controller

FQDN

cloudsbc.cgbusolutionslab.com:5061

Max concurrent calls

Webex Calling edge proxy address (FQDN)

peering1.us.sipconnect.bclid.webex.com:5062
peering2.us.sipconnect.bclid.webex.com:5062
peering3.us.sipconnect.bclid.webex.com:5062
peering4.us.sipconnect.bclid.webex.com:5062

Webex Calling edge proxy address (SRV)

us01.sipconnect.bclid.webex.com

Cisco recommends using SRV based Webex Calling edge address for connection your Oracle SBC as a local gateway.

Please note that Webex Calling Proxy Addresses given below are 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.

This concludes the minimum configuration required for the gateway. We'll now move on to configuring your Oracle SBC as a local gateway.

7 Configuring the SBC

This chapter provides step-by-step instructions for configuring the Oracle SBC for Cisco Webex Calling LGW. In this configuration, both signaling and media between the Oracle SBC and Cisco Webex are secured using TLS and SRTP. A generic example of configuring a non-secure PSTN service on the Oracle SBC is also included for illustration purposes only; however, it is not the primary focus of this chapter.

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

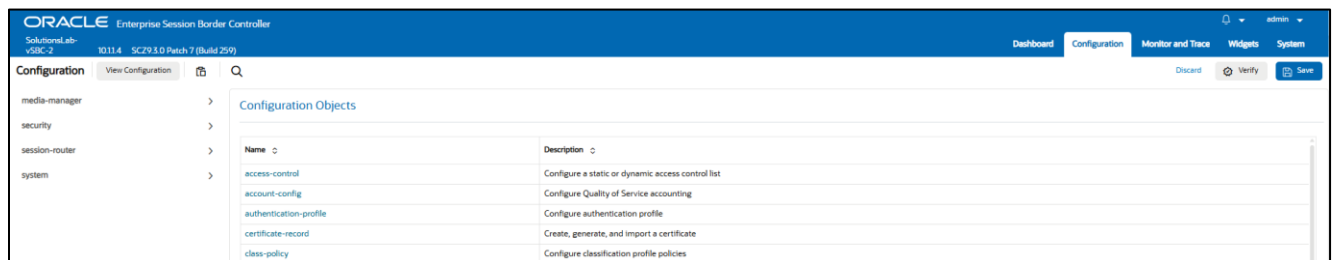
This guide assumes the Oracle SBC has been installed, the management interface has been configured, the product has been selected, and entitlements have been assigned. Additionally, web-server-config should be enabled for GUI access. If you need more information on installing your SBC platform, please refer to the [ACLI configuration guide](#).

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

Once you have access to the Oracle SBC GUI, click the **Configuration** tab at the top. This will display the Oracle SBC Configuration Objects List on the left-hand side of the screen.

Any configuration parameter not specifically listed below can remain at its Oracle SBC default value and does not require a change for the connection to Cisco Webex Calling to function properly.

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



Please refer to the Oracle SBC GUI Guide for more information.

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

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.

7.1 System-Config

To enable system level functionality for the Oracle SBC, you must first enable the system-config.

GUI Path: system/system-config

ACLI Path: config t→system→system-config

Note: The following parameters are optional but recommended for system config

- Hostname
- Description
- Location
- Default Gateway (recommended to be the same as management interface gateway)

- Transcoding Core (This field is only required if you have deployed a VME SBC)

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 10.11.4 SCZ9.3.0 Patch 7 (Build 259)

Configuration View Configuration

media-manager >

security >

session-router >

system >

fraud-protection >

host-route >

http-client >

http-server >

Modify System Config

Hostname OracleSBC-WebexLGW

Description

Location

Mib System Contact

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.

7.1.1 NTP-Config

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

GUI Path: system/ntp-config

ACLI Path: config t→system→ntp-sync

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 10.11.4 SCZ9.3.0 Patch 7 (Build 259)

Configuration View Configuration

media-manager >

security >

session-router >

system >

fraud-protection >

host-route >

Add NTP Config

This object has not been created. Start editing and click OK to add.

Server time-a-g.nist.gov x time-b-g.nist.gov x

DNS Realm CiscoWebexRealm

7.2 Network Configuration

To connect the SBC to network elements, we must configure both physical and network interfaces. For the purposes of this example, we will configure two physical interfaces, and two network interfaces. One to communicate with Cisco Webex Calling, the other to connect to PSTN Network. The slots and ports used in this example may be different from your network setup.

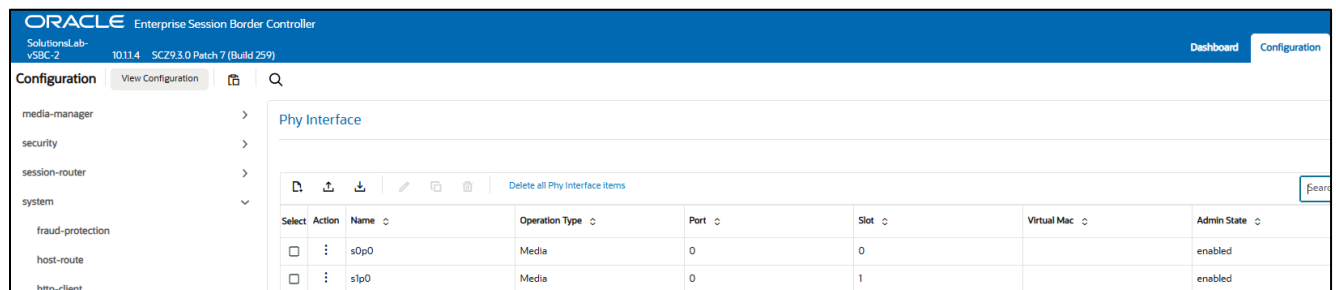
7.2.1 Physical Interfaces

GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

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

Config Parameter	PSTN	Cisco Webex
Name	s0p0	S1p0
Operation Type	Media	Media
Slot	0	1
Port	0	0



Select	Action	Name	Operation Type	Port	Slot	Virtual Mac	Admin State
<input type="checkbox"/>	⋮	s0p0	Media	0	0		enabled
<input type="checkbox"/>	⋮	s1p0	Media	0	1		enabled

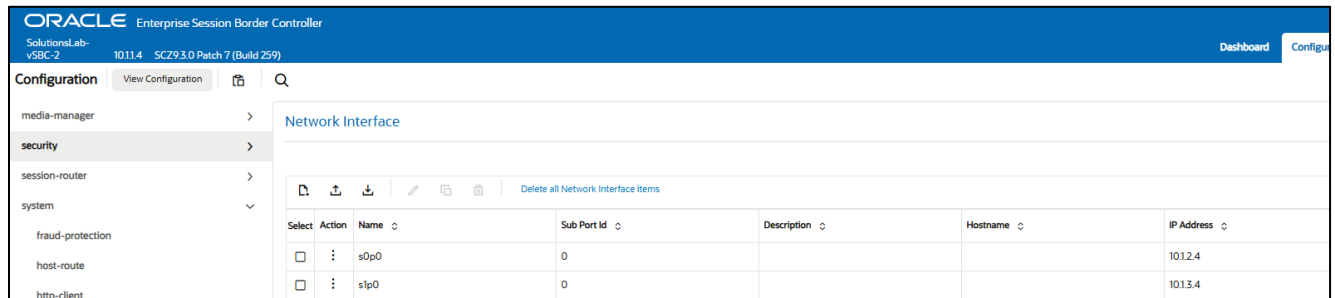
7.2.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

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

Configuration Parameter	PSTN	Cisco Webex
Name	s0p0	s1p0
IP Address	10.1.2.4	10.1.3.4
Netmask	255.255.255.0	255.255.255.0
Gateway	10.1.2.1	10.1.3.1
DNS Primary IP		8.8.8.8
DNS Domain		cgbusolutionslab.com



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

Next, we'll configure the necessary elements to secure signaling and media traffic between the Oracle SBC and Cisco Webex Calling.

7.3 Security Config

This section describes how to configure the SBC for both TLS and SRTP communication with Cisco Webex Calling.

Cisco Webex Calling supports TLS connections from SBCs for SIP signaling and uses SRTP for media traffic. It requires SBCs to present certificates signed by trusted Certificate Authorities. A list of Cisco's supported CA's can be found at:

[Cisco Webex Calling Supported Root Certificate Authorities](#)

7.3.1 Certificate Records

"Certificate-records" are configuration elements on Oracle SBC which capture information for a TLS certificate such as common-name, key-size, key-usage etc.

This section walks you through how to configure certificate records, create a certificate signing request, and import the necessary certificates into the SBC's configuration.

GUI Path: security/certificate-record

ACL Path: config t→security→certificate-record

For the purposes of this application note, we'll create three certificate records. They are as follows:

- SBC Certificate (end-entity certificate)
- GoDaddy Root Cert (Root CA used to sign the SBC's end entity certificate)
- IdentTrust Commercial Root CA (Cisco Webex Presents the SBC a certificate signed by this authority)

Note: The GoDaddy RootCA is only part of this example, as that is the Authority we used to sign our SBC certificate. You would replace this with the root and/or intermediate certificates used to sign the CSR generated from your SBC.

7.3.1.1 SBC End Entity Certificate

The SBC's end entity certificate is the certificate the SBC presents to Cisco to secure the connection. The only requirements when configuring this certificate is the common name must contain the SBC's FQDN and the **extended key usage list** must contain both **serverAuth** and **clientAuth**. In this example our common name will be **cloudsbc.cgbusolutionslab.com**. You must also give it a name. All other fields are optional, and can remain at default values.

To Configure the certificate record:

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

The screenshot shows a web form titled "Modify Certificate Record". The form contains the following fields and values:

Field	Value
Name	CloudSBC
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	
Common Name	cloudsbc.cgbusolutionslab.com
Key Size	2048
Alternate Name	
Trusted	<input checked="" type="checkbox"/> enable
Key Usage List	digitalSignature x keyEncipherment x
Extended Key Usage List	serverAuth x clientAuth x

- Click OK at the bottom

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

7.3.1.2 Root CA and Intermediate Certificates

7.3.1.2.1 Go Daddy Root

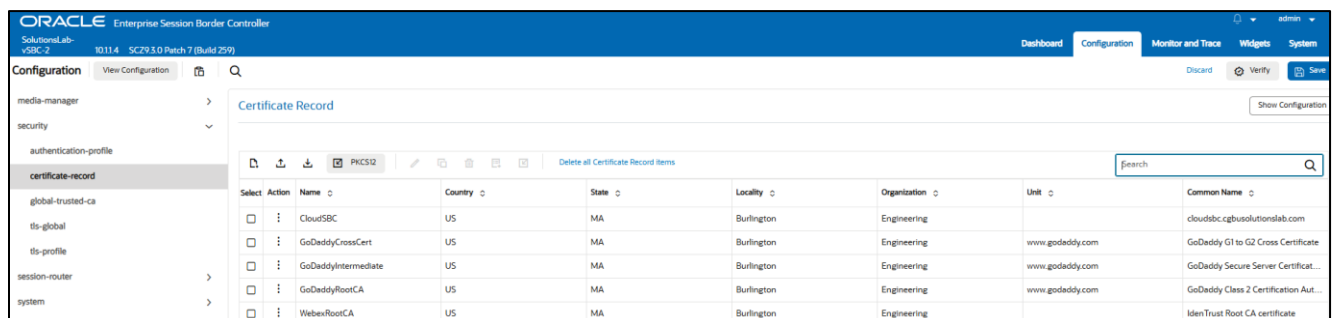
The following, GoDaddyRoot, is the root CA certificate used to sign the SBC's end entity certificate. As mentioned above, your root CA and/or intermediate certificate may differ. This is for example purposes only.

7.3.1.2.2 IdenTrust Commercial Root CA

Cisco presents a certificate to the SBC which is signed by IdenTrust Commercial Root CA. To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate. You can download this certificate here: [IdenTrust Commercial Root CA](#).

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

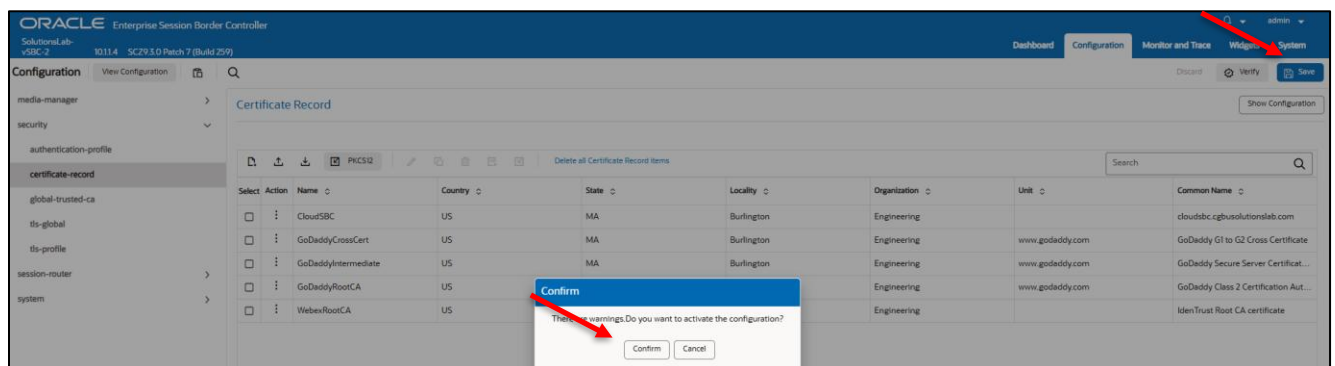
Config Parameter	GoDaddy Root	IdenTrust Commercial Root
Common Name	Go Daddy Class2 Root CA	IdenTrust Root CA Certificate
Key Size	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth
Key algor	rsa	rsa
Digest-algor	Sha256	Sha256



The screenshot shows the Oracle Enterprise Session Border Controller (SBC) Configuration page. The left sidebar shows the navigation menu with 'certificate-record' selected. The main area displays a table of certificate records.

Select	Action	Name	Country	State	Locality	Organization	Unit	Common Name
<input type="checkbox"/>		CloudSBC	US	MA	Burlington	Engineering		cloudsbc.cbusolutionslab.com
<input type="checkbox"/>		GoDaddyCrossCert	US	MA	Burlington	Engineering	www.godaddy.com	GoDaddy G1 to G2 Cross Certificate
<input type="checkbox"/>		GoDaddyIntermediate	US	MA	Burlington	Engineering	www.godaddy.com	GoDaddy Secure Server Certificat...
<input type="checkbox"/>		GoDaddyRootCA	US	MA	Burlington	Engineering	www.godaddy.com	GoDaddy Class 2 Certification Aut...
<input type="checkbox"/>		WebexRootCA	US	MA	Burlington	Engineering		IdenTrust Root CA certificate

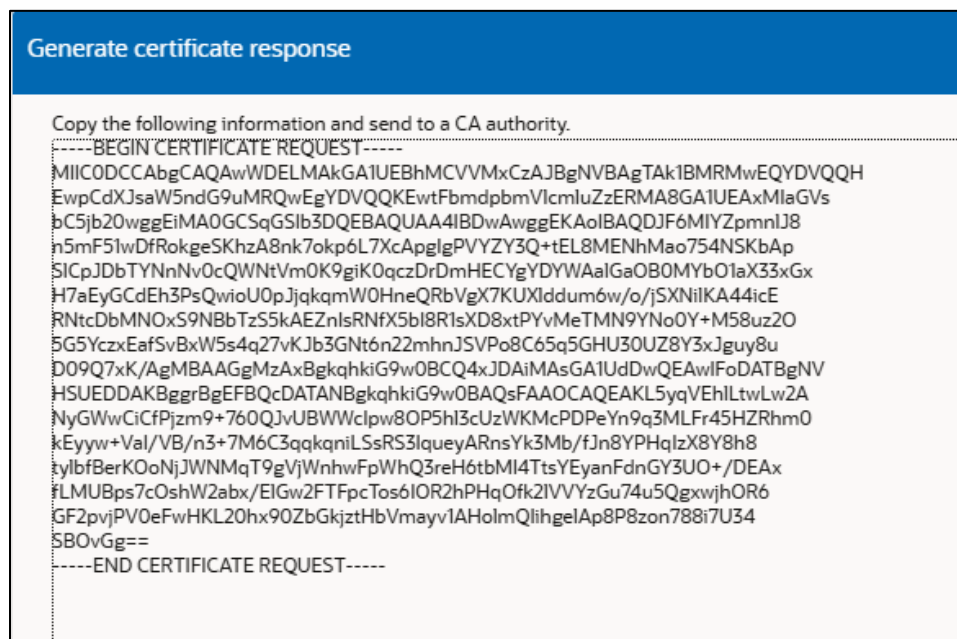
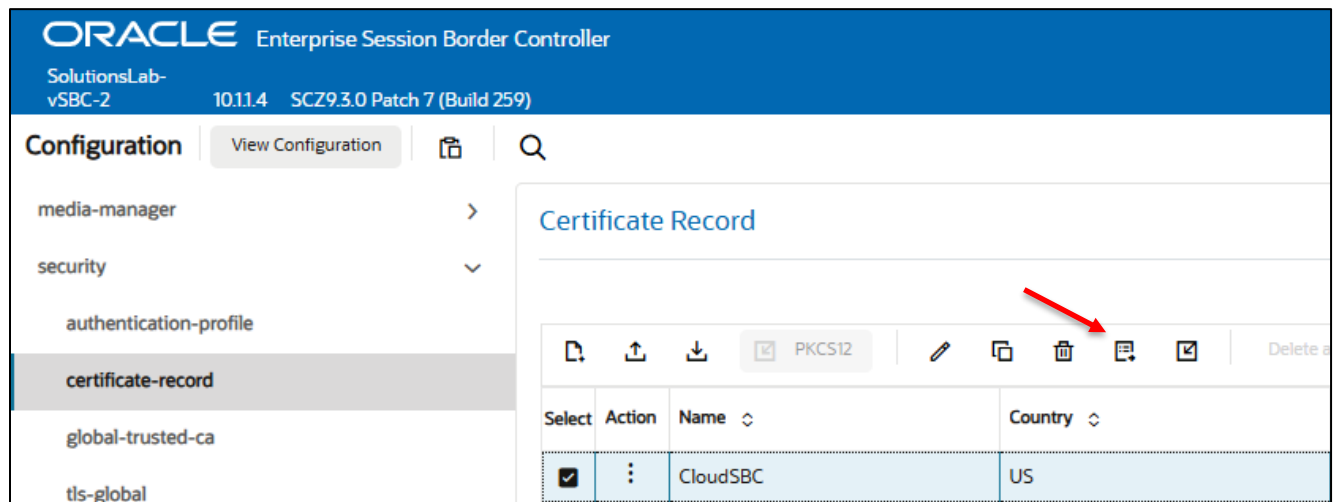
At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must **save and activate** the configuration of the SBC.



7.3.1.2.3 Generate Certificate Signing Request

Now that the SBC's certificate has been configured, create a certificate signing request for the SBC's end entity only. **This is not required for any of the Root CA or intermediate certificates that have been created.**

On the certificate record page in the Oracle SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:



Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.

Also note, **another save and activate is required** before you can import the certificates to each certificate record created above.

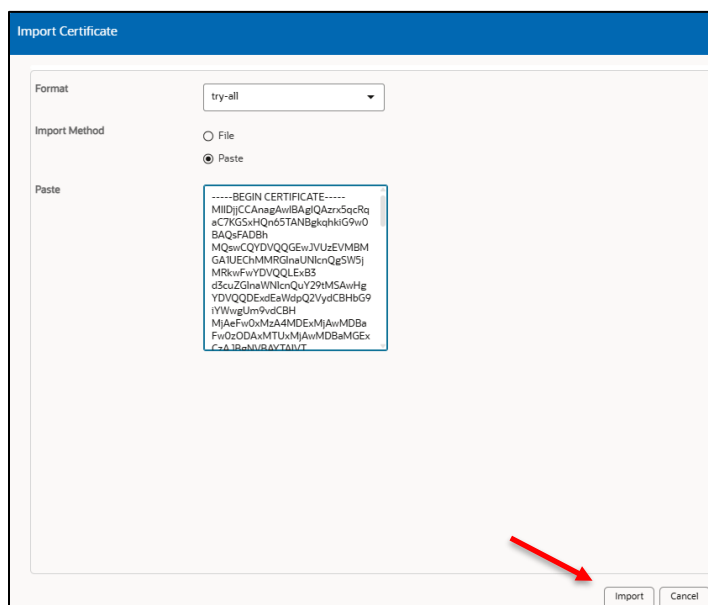
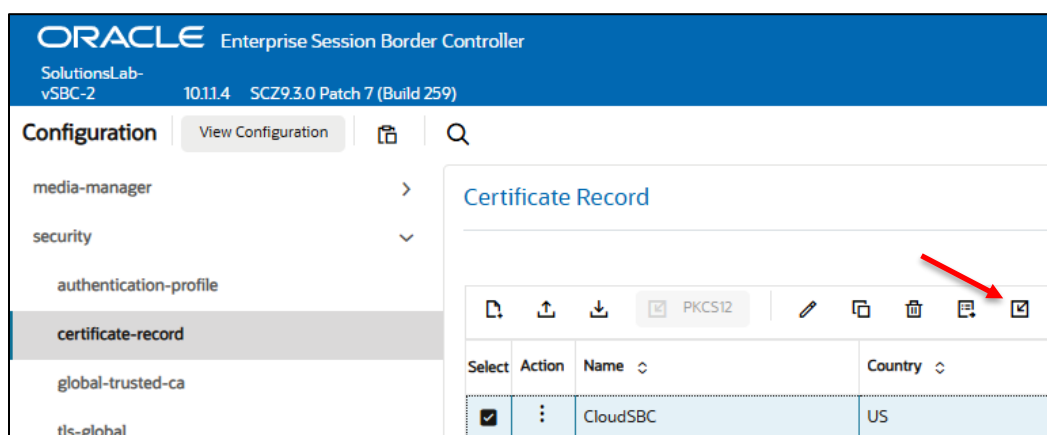
Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

7.3.1.2.4 Import Certificates to the SBC

Once certificate signing request has been completed – import the signed certificate to the SBC.

Please note – all certificates including root and intermediate certificates are required to be imported to the SBC.

Once all certificates have been imported, issue a third **save/activate** from the WebGUI to complete the configuration of certificates on the Oracle SBC.



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

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

7.3.2 TLS Profile

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

GUI Path: security/tls-profile

ACLI Path: config t→security→tls-profile

- Click Add, use the example below to configure

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The top header includes the Oracle logo and version information: SolutionsLab-vSBC-2, 10.11.4, SCZ9.3.0 Patch 7 (Build 259). The left sidebar is titled 'Configuration' and lists various settings: media-manager, security, authentication-profile, certificate-record, global-trusted-ca, tls-global, **tls-profile** (selected), session-router, and system. The main content area is titled 'Modify TLS Profile'. It contains several fields: 'Name' with the value 'TLSWebex', 'End Entity Certificate' with a dropdown menu showing 'CloudSBC', and 'Trusted Ca Certificates' with three buttons: 'GoDaddyRootCA x', 'WebexRootCA x', and 'GoDaddyIntermediate x'. Below these are two empty sections for 'Global Trusted Ca Lists' and 'Cert Status Profile List'.

- Select OK at the bottom

Next, we'll move to securing media between the SBC and Cisco Webex Calling

7.3.3 Media Security

This section outlines how to configure support for media security between the OCSBC and Cisco Webex Calling.

7.3.3.1 SDES Profile

This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured. Cisco Supports the following crypto's:

- AES_CM_256_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

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

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

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

- Click Add, and use the example below to configure

ORACLE Enterprise Session Border Controller
SolutionsLab-vSBC-2 10.11.4 SCZ9.3.0 Patch 7 (Build 259)

Configuration View Configuration

media-manager >
security >
admin-security >
auth-params
authentication
authentication-profile
cert-status-profile
certificate-record
factory-accounts
global-trusted-ca
local-accounts
media-security >
dts-srtP-profile
media-sec-policy
sdes-profile
sipura-profile
password-policy
security-config
ssh-config

Modify Sdes Profile

Name: CiscoSRTP

Crypto List: AES_CM_128_HMAC_SHA1_80 x AES_256_CM_HMAC_SHA1_80 x AES_CM_128_HMAC_SHA1_32 x AEAD_AES_256_GCM x

SrtP Auth: ☒ enable

SrtP Encrypt: ☒ enable

SrTCP Encrypt: ☒ enable

Mki: ☐ enable

Egress Offer Format: same-as-ingress

Use Ingress Session Params:

Options:

Key:

Salt:

SrtP Relay On Re Invite: ☒ enable

You may notice there is a fourth crypto in the list, AEAD_AES_256_GCM. This is only supported in Cisco for Government environments.

- Select OK at the bottom.

7.3.4 Media Security Policy

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

In this example, we are configuring two media security policies. One to secure and decrypt media toward Cisco Webex, the other for non-secure media facing PSTN.

GUI Path: security/media-security/media-sec-policy

ACL Path: config t→security→media-security→media-sec-policy

- Click Add, use the examples below to configure.

ORACLE Enterprise Session Border Controller
SolutionsLab-vSBC-2 10.11.4 SC29.3.0 Patch 7 (Build 259)

Configuration View Configuration

media-manager >
security >
 admin-security >
 auth-params
 authentication
 authentication-profile
 cert-status-profile
 certificate-record
 factory-accounts
 global-trusted-ca
 local-accounts
 media-security >
 dtls-srtp-profile
 media-sec-policy
 sdes-profile
 sipura-profile

Modify Media Sec Policy Entries

Name CiscoWebexSecurity

Pass Through ☐ enable

Options

Inbound

Profile CiscoSRTP

Mode srtp

Protocol sdes

Hide Egress Media Update ☐ enable

Outbound

Profile CiscoSRTP

Mode srtp

Protocol sdes

ORACLE Enterprise Session Border Controller
SolutionsLab-vSBC-2 10.11.4 SC29.3.0 Patch 7 (Build 259)

Configuration View Configuration

media-manager >
security >
 admin-security >
 auth-params
 authentication
 authentication-profile
 cert-status-profile
 certificate-record
 factory-accounts
 global-trusted-ca
 local-accounts
 media-security >
 dtls-srtp-profile
 media-sec-policy
 sdes-profile
 sipura-profile

Modify Media Sec Policy Entries

Name PSTNMediaSecurity

Pass Through ☐ enable

Options

Inbound

Profile

Mode rtp

Protocol none

Hide Egress Media Update ☐ enable

Outbound

Profile

Mode rtp

Protocol none

- Select OK at the bottom of each when finished.

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

7.4 Transcoding Configuration (Optional)

Transcoding is the ability to convert between media streams that are based upon disparate codecs. The OCSBC supports IP-to-IP transcoding for SIP sessions and can connect two voice streams that use different coding algorithms with one another.

7.4.1 Codec Policies

Codec policies are sets of rules that specify the manipulations to be performed on SDP offers allowing the Oracle SBC the ability to add, strip, and reorder codecs for SIP sessions.

GUI Path: media-manager/codec-policy

ACLI Path: config t→media-mangaer→codec-policy

Since some SIP Trunks may have issues with the codecs being offerened by Cisco Webex, you can create a codec policy to remove unwanted or unsupported codecs from the request/responses to your Sip Trunk provider.

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The left sidebar has a menu with 'media-manager' expanded, showing 'codec-policy' as the selected item. The main panel is titled 'Modify Codec Policy Entries'. It contains three fields: 'Name' with the value 'CiscoCodec', 'Allow Codecs' with a single asterisk '*' and a close button 'x', and 'Add Codecs On Egress' with two buttons labeled 'PCMU x' and 'PCMA x'.

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The left sidebar has a menu with 'media-manager' expanded, showing 'codec-policy' as the selected item. The main panel is titled 'Modify Codec Policy Entries'. It contains three fields: 'Name' with the value 'PSTN', 'Allow Codecs' with a list of codec buttons: 'opus:no x', 'SILK:no x', 'PCMU x', 'PCMA x', and 'G729 x', and 'Add Codecs On Egress' with three buttons labeled 'PCMU x', 'PCMA x', and 'G729 x'.

- Select OK at the bottom of each when finished

7.4.2 ICE Profile

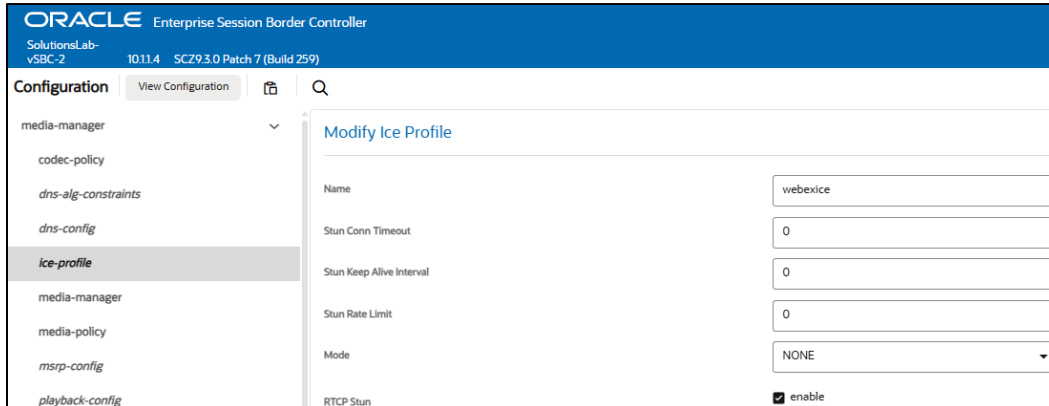
Interactive Connectivity Establishment - Session Traversal Utility for NAT (ICE STUN lite mode) enables an Advanced Media Termination client to perform connectivity checks and can provide several STUN servers to the browser. ICE STUN support requires configuring an ICE Profile.

The use of ICE is required only if using Cisco Webex Media Optimization Feature.

GUI Path: media-manager/ice-profile

ACL Path: config t→media-manger→ice-profile

- Click Add, use the example below as a guide to configure.



The screenshot shows the Oracle Enterprise Session Border Controller GUI. The top header displays 'ORACLE Enterprise Session Border Controller' and 'SolutionsLab-vSBC-2 1011.4 SC29.3.0 Patch 7 (Build 259)'. The left sidebar lists configuration categories: media-manager, codec-policy, dns-alg-constraints, dns-config, ice-profile (selected), media-manager, media-policy, msrp-config, and playback-config. The main area is titled 'Modify Ice Profile' and contains the following fields:

Field	Value
Name	webexice
Stun Conn Timeout	0
Stun Keep Alive Interval	0
Stun Rate Limit	0
Mode	NONE
RTCP Stun	<input checked="" type="checkbox"/> enable

You must enable RTCP Stun on the ICE Profile for Cisco Media Optimization feature to be successful.

In some environments, it may be necessary to change the default values for Stun Conn Timeout, Stun Keep Alive Interval, and Stun Rate Limit to a value of 0 (zero).

- Select OK at the bottom.

This concludes the configuration for transcoding and Advanced Media Termination options on the SBC. We can now move to setup Media.

7.5 Media Configuration

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

7.5.1 Media Manager

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

GUI Path: media-manager/media-manager

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

ORACLE Enterprise Session Border Controller

Solutions Lab- vSBC-2 10.11.4 SC29.1.0 Patch 7 (Build 259)

Dashboard Configuration

Configuration View Configuration

media-manager

codecs-policy

media-manager

media-policy

realm-config

steering-pool

security

session-router

Modify Media Manager

State ☒ enable

Max Arp Rate 10 (Range: 0..100)

Max Signalling Packets 0 (Range: 0..4294967295)

Max Untrusted Signalling 100 (Range: 0..100)

Min Untrusted Signalling 30 (Range: 0..100)

- Click OK at the bottom.

7.5.2 Realm Config

Realms are a logical distinction representing routes (or groups of routes) reachable by the Oracle® Session Border Controller and what kinds of resources and special functions apply to those routes. Realms are used as a basis for determining ingress and egress associations to network interfaces.

GUI Path; media-manger/realm-config

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

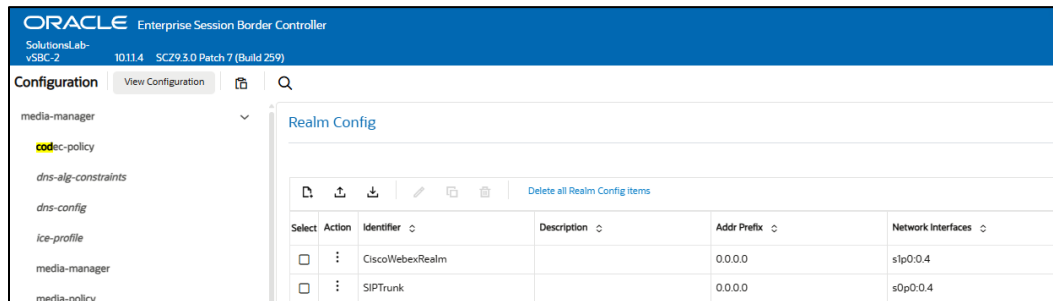
- Click Add and use the following table as a configuration example for the realms. The following parameters are all required unless mentioned as optional below.

Config Parameter	Cisco Webex	PSTN
Identifier	CiscoWebexRealm	SipTrunk
Network Interface	S1p0:0	S0p0:0
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Media Sec policy	CiscoWebexSecurity	PSTNMediaSecurity
ice profile	webexice (required for media opt only)	
Codec policy	CiscoCodec	PSTN
Trunk Context	Cloudsbc.cgbusolutionslab.com	
Access-control-trust-level	HIGH	HIGH

Also notice the realm configuration is where we assign some of the elements configured earlier in this document. IE...

- Network Interface
- Media Security Policy
- Ice Profile (optional, only required if using Media Opt)
- Codec Policy (optional)

Please also note the “trunk context” parameter. The value you set here should be the SBC’s FQDN, which was registered earlier in the Webex Control Hub. Later in this application note, this value will be used to adjust SIP header syntax to match Cisco Webex Calling requirements.



- Click OK at the bottom of each.

7.5.3 Steering Pools

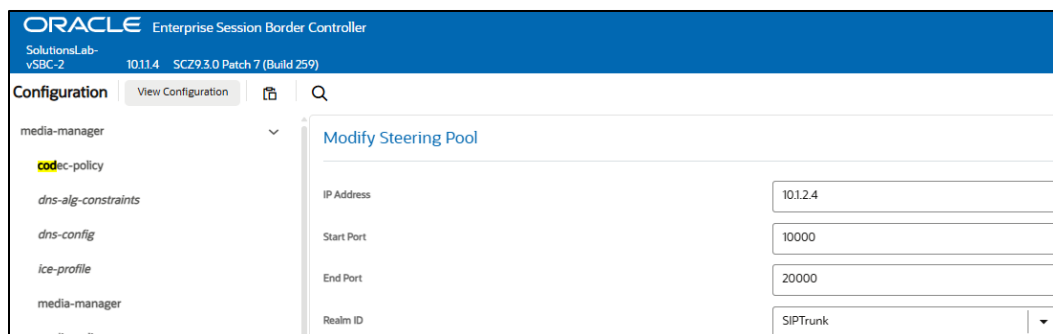
Steering pools define sets of ports that are used for steering media flows through the OCSBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

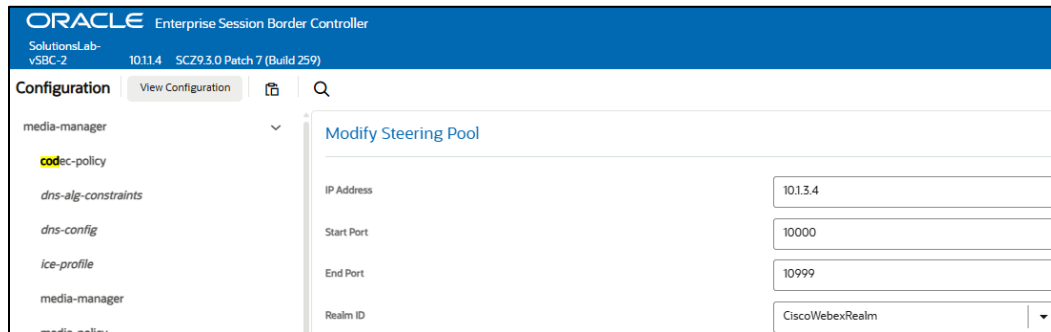
We configure one steering pool for PSTN. The other facing Cisco.

GUI Path: media-manger/steering-pool

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

- Click Add, and use the below examples to configure.





- Select OK at the bottom

We will now work through configuring what is needed for the SBC to handle SIP signaling.

7.6 Sip Configuration

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

7.6.1 Sip-Config

To enable sip related objects on the Oracle SBC, you must first configure the global Sip Config element:

GUI Path: session-router/sip-config

ACL Path: config t→session-router→sip-config

There are only two recommended changes/additions to the global Sip Config.

- Set the home realm ID parameter to CiscoWebexRealm, and add the following hidden option:
- **Max-udp-length=0**: Setting this option to zero (0) forces sipd to send fragmented UDP packets. Using this option, you override the default value of the maximum UDP datagram size (1500 bytes; sipd requires the use of SIP/TCP at 1300 bytes).

ORACLE Enterprise Session Border Controller
SolutionsLab-vSBC-2 10.11.4 SCZ9.3.0 Patch 7 (Build 259)

Configuration View Configuration

security >
session-router >
access-control
account-config
filter-config
ldap-config
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
sip-manipulation
sip-monitoring
translation-rules
system >

Modify SIP Config

Home Realm ID	CiscoWebexRealm
Egress Realm ID	
Nat Mode	None
Registrar Domain	*
Registrar Host	*
Registrar Port	5060
Init Timer	500
Max Timer	4000
Trans Expire	32
Initial Inv Trans Expire	0
Invite Expire	180
Session Max Life Limit	0
Enforcement Profile	
Emergency Dscp Profile	
Red Max Trans	10000
Options	max-udp-length=0 x

- Select OK at the bottom.

7.6.2 Sip Manipulation

To ensure that the SBC generates SIP messages conforming to Cisco Webex Calling requirements, create SIP manipulation rules to:

- Change the Contact header's host URI to the SBC's FQDN.
- Add a Contact header to SIP OPTIONS messages that includes the SBC's FQDN.
- Modify the Request URI host to use the Cisco Webex hostname.
- Change the P-Asserted-Identity (P-Asserted-ID) host part to the SBC's FQDN.

GUI Path: session router/sip manipulation

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

Click Add, and use the following example to configure:

While this can be configured via the GUI, we are using the ACLI output to provide an example config for ease of viewing.

```

sip-manipulation
  name CiscoOutManipulation
  header-rule
    name ChangeContactHost
    header-name Contact
    action manipulate
    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>"
  header-rule
    name changeToUser
    header-name To
    action manipulate
    msg-type request
    methods INVITE
    element-rule
      name changeTOhost
      type uri-host
      action replace
      new-value us01.sipconnect.bclld.webex.com
  header-rule
    name ChangePAI
    header-name P-Asserted-Identity
    action manipulate
    comparison-type pattern-rule
    methods INVITE
    element-rule
      name ChangePAI
      type uri-host
      action replace
      new-value $TRUNK_GROUP_CONTEXT

```

You'll notice that, in most of these header manipulation rules, the new values are set to **\$TRUNK_GROUP_CONTEXT**. This variable automatically uses the value configured in the realm parameter we set up earlier—which is the SBC's FQDN.

There is an additional, optional SIP manipulation that you can configure if needed. Some SIP trunk providers don't support certain SIP headers and header parameters that Cisco Webex Calling includes in its messages. To ensure smooth interoperability between your PSTN provider and Cisco, you may need to set up and apply the following SIP manipulation rule.

```

sip-manipulation
  name StripCiscoHeaders
  description Remove Cisco Headers to PSTN
  header-rule
    name DeleteLocationInfo
    header-name X-Cisco-Location-Info
    action delete
    methods BYE,INVITE,OPTIONS
  header-rule
    name DeleteRecvInfo
    header-name Recv-Info
    action delete
    methods BYE,INVITE,OPTIONS
  header-rule
    name DeleteSessionID
    header-name Session-ID
    action delete
    methods BYE,INVITE,OPTIONS
  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

```


7.6.3 Sip Interface

The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages

Configure two sip interfaces, one associated with PSTN Realm, and the other for Cisco.

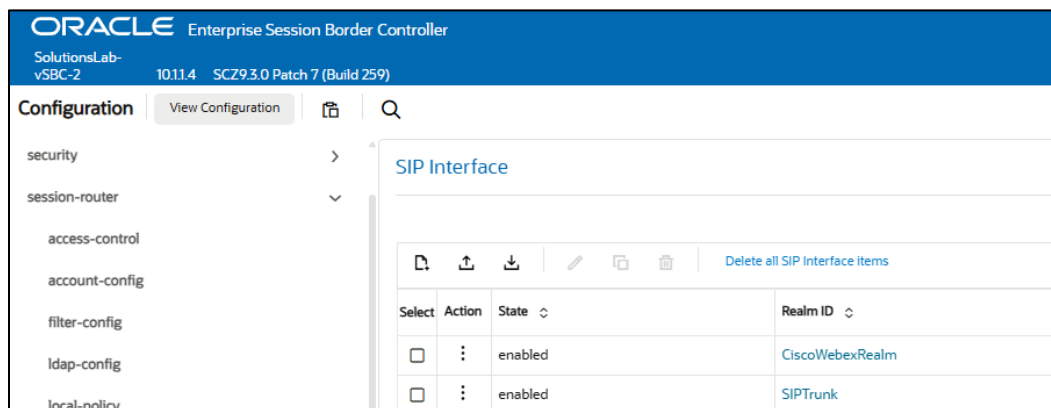
GUI Path: session-router/sip-interface

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

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

Config Parameter	SipTrunk	Cisco Webex
Realm ID	SipTrunk	CiscoWebexRealm
User Agent		Oracle/VM/9.3.0
Initial Inv Trans Expire		10
Out Manipulationid	StripCiscoHeaders	CiscoOutManipulation
Sip Port Config Parmeter	Sip Trunk	Cisco Webex
Address	10.1.2.4	10.1.3.4
Port	5060	5061
Transport protocol	UDP	TLS
TLS profile		TLSWebex
Allow anonymous	Agents-only	Agents-only

Here, you'll assign the TLS profile configured under the [Security](#) section of this guide and the sip-manipulations which ensures the SBC works smoothly with other systems. We also configure the User Agent parameter; this should reflect your specific Oracle SBC platform and software version of your SBC. Lastly, we adjust the Initial Invite Trans Expire value <Timer B> to ensure the SBC recurses properly when using Cisco's SRV agent.



- Select OK at the bottom of each when applicable.

7.6.4 Session Agents

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

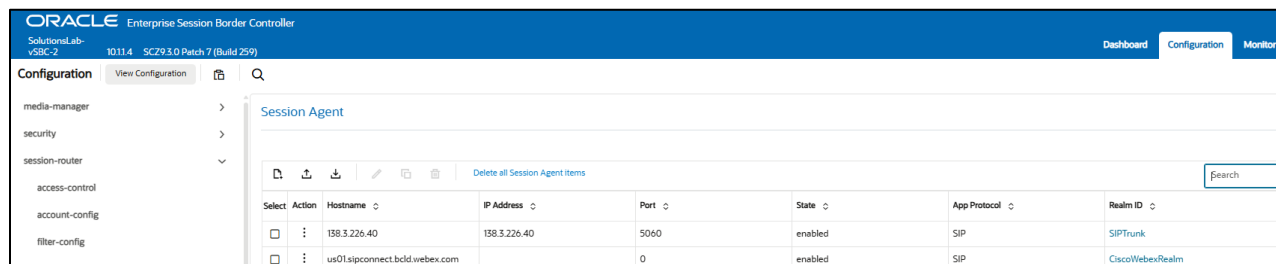
GUI Path: session-router/session-agent

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

In this example, we'll configure two session agents. The SRV agent for Cisco Webex Calling, and another for our Sip Trunk.

- Click Add, and use the table below to configure:

Config parameter	Session Agent 1	Session Agent 2
Hostname	us01.sipconnect.bcl.d.webex.com	138.3.226.40
IP Address		138.3.226.40
Port	0	5060
Transport method	StaticTLS	StaticTCP
Realm ID	CiscoWebexRealm	SipTrunk
Ping Method	OPTIONS	OPTIONS
Ping Interval	30	30
Ping Response	enabled	enabled
Ping All Addresses	<input checked="" type="checkbox"/>	



Select	Action	Hostname	IP Address	Port	State	App Protocol	Realm ID
<input type="checkbox"/>		138.3.226.40	138.3.226.40	5060	enabled	SIP	SipTrunk
<input type="checkbox"/>		us01.sipconnect.bcl.d.webex.com		0	enabled	SIP	CiscoWebexRealm

- Click OK at the bottom of each when applicable.

7.7 Routing Configuration

Now that a majority of the signaling, security and media configuration is in place, we can configure the SBC to route calls from one end of the network to the other. The SBC has multiple routing features that can be utilized, but for the purposes of this example configuration, we'll configure local policies to route calls from Cisco Webex Calling to our Sip trunk, and vice versa...

GUI Path: session-router/local-policy

ACLI Path: config t→session-router→local-policy

ORACLE Enterprise Session Border Controller
SolutionsLab-vSBC-2 10.11.4 SC29.3.0 Patch 7 (Build 259)

Configuration View Configuration

- media-manager
- security
- session-router
- access-control
- account-config
- filter-config
- ldap-config
- local-policy**
- local-routing-config
- media-profile
- session-agent
- session-group

Modify Local Policy Entries

From Address *

To Address *

Source Realm CiscoWebexRealm x

Description

Policy Priority none

Policy Attributes

After entering values for to and from address and source realm, click Add under policy attribute to configure the next hop destination.

ORACLE Enterprise Session Border Controller
SolutionsLab-vSBC-2 10.11.4 SC29.3.0 Patch 7 (Build 259)

Configuration View Configuration

- media-manager
- security
- session-router
- access-control
- account-config

Modify Local policy / policy attribute

Next Hop 138.3.226.40

Realm SIPTrunk

Action replace-uri

Next, we'll setup routing from our SIP Trunk to Cisco Webex Calling:

ORACLE Enterprise Session Border Controller
SolutionsLab-vSBC-2 10.11.4 SC29.3.0 Patch 7 (Build 259)

Configuration View Configuration

- media-manager
- security
- session-router
- access-control
- account-config
- filter-config
- ldap-config
- local-policy**
- local-routing-config
- media-profile
- session-agent
- session-group

Modify Local Policy Entries

From Address *

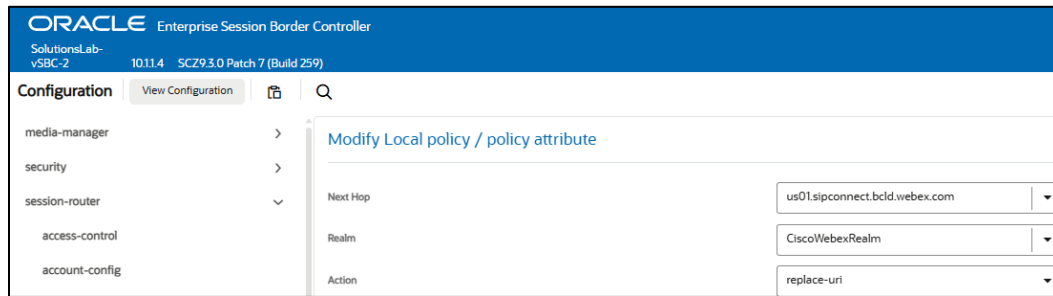
To Address *

Source Realm SIPTrunk x

Description

Policy Priority none

Policy Attributes



- Select OK when applicable on each screen

7.8 Sip Access Controls

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

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

<https://docs.oracle.com/en/industries/communications/session-border-controller/9.3.0/security/security-guide.pdf>

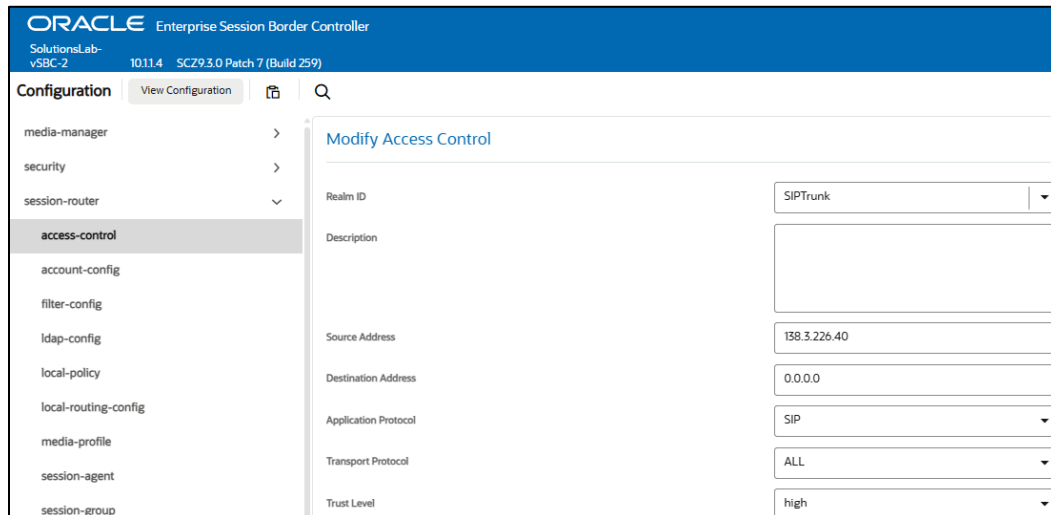
However. While some values are environment specific, there are some basic security parameters that can be implemented on the SBC that will help secure your setup.

1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high
2. Set the access control trust level on public facing [realms](#) to HIGH.

Use this example to create ACL's for all Cisco and PSTN IP's. This example can be followed for any of the public facing interfaces.

GUI Path: session-router/access-control

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



ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 10114 SCZ9.3.0 Patch 7 (Build 259)

Configuration View Configuration

- media-manager
- security
- session-router
- access-control**
- account-config
- filter-config
- ldap-config
- local-policy
- local-routing-config
- media-profile
- session-agent
- session-group

Modify Access Control

Realm ID	SIPTrunk
Description	
Source Address	138.3.226.40
Destination Address	0.0.0.0
Application Protocol	SIP
Transport Protocol	ALL
Trust Level	high

- Select OK at the bottom.

This concludes the required configuration of the SBC to act as a local gateway for Cisco Webex Calling.

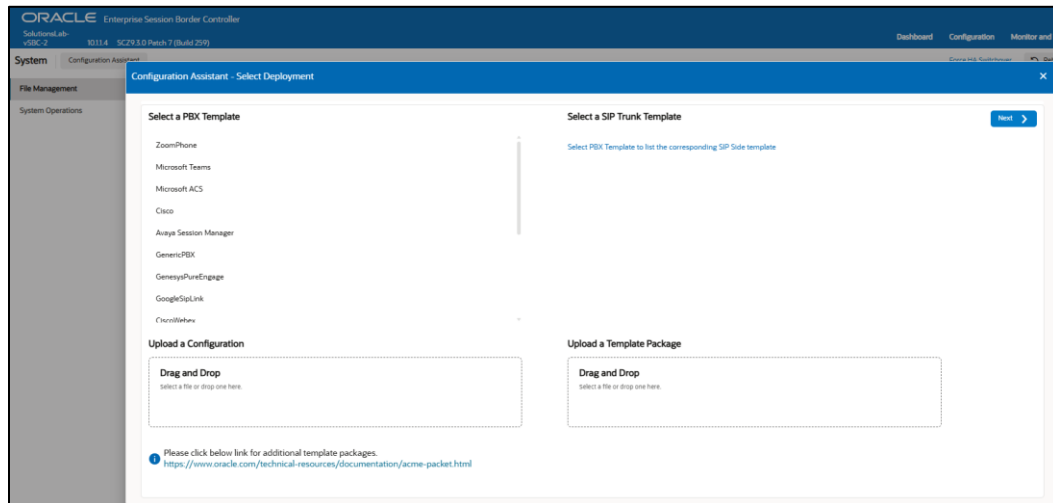
8 Oracle SBC Configuration Assistant

When you first log on to the Oracle SBC, the system requires you to set the configuration parameters necessary for basic operation. To help you set the initial configuration with minimal effort, the SBC provides the Configuration Assistant. The Configuration Assistant, which you can run from the Web GUI or the Acme Command Line Interface (ACLI), asks you questions and uses your answers to set parameters for managing and securing call traffic between the SBC and Cisco Webex Calling. You can use the Configuration Assistant for the initial set up to make to the basic configuration. See "[Configuration Assistant Operations](#)" in the Web GUI User Guide and "[Run Configuration Assistant](#)" in the ACLI Configuration Guide

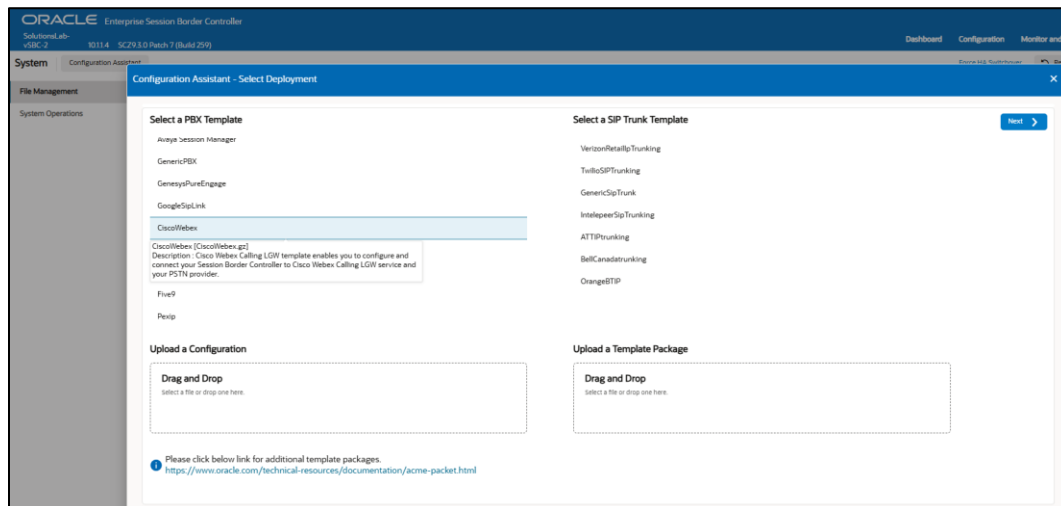
8.1 Cisco Webex Calling Configuration Assistant

The screenshots below are from an Oracle SBC GUI running 930p7.

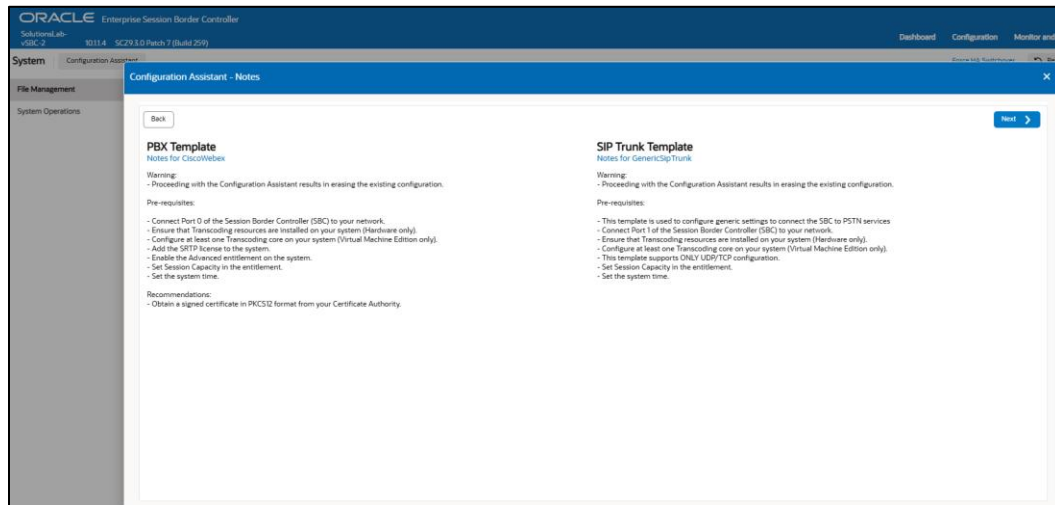
For a new SBC deployment, once access to the GUI is configured, you will see the following when logging in for the first time:



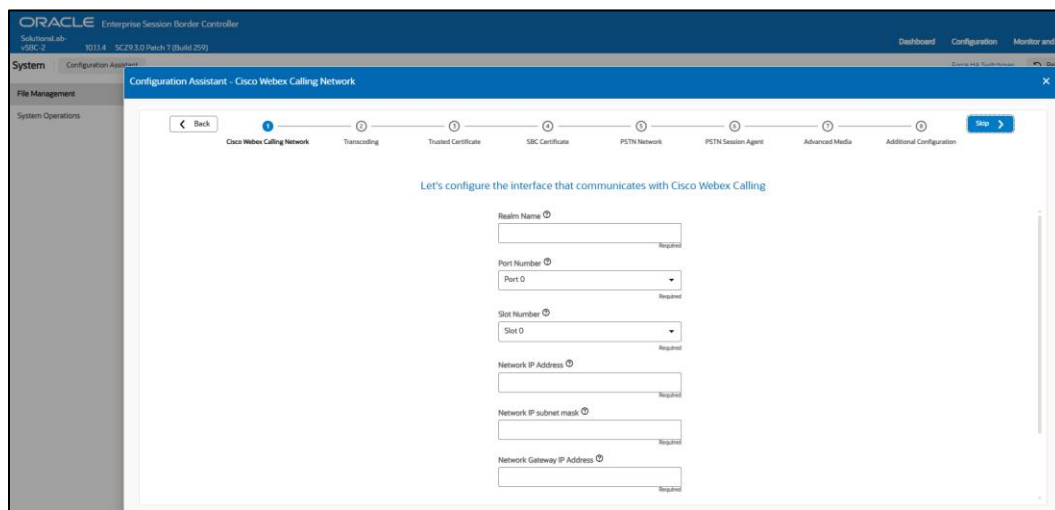
Under PBX template, we'll select Cisco Webex template. This brings up a list of available sip trunk templates.



Select a sip trunk template and click next at the top to access the Notes page. Pay close attention to the information here, as this is a list of warnings, pre-requisites, and recommendations:

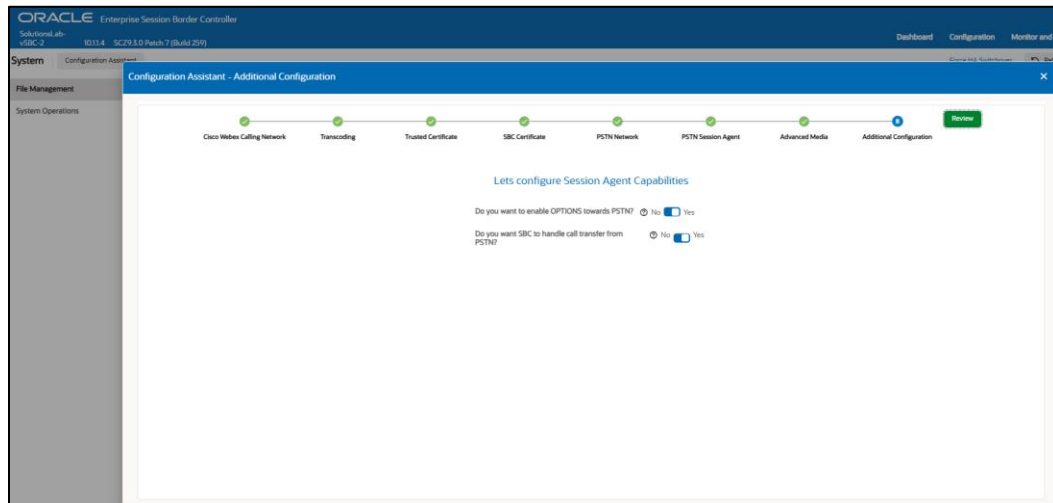


Clicking “Next” on the Notes page triggers the configuration assistant to do a system check. This ensures that all the system requirements for the platform and sip trunk you have selected have been met before proceeding to configuration pages. If they have not been met, you will be greeted by a page providing the opportunity to setup entitlements, add license keys, etc...before moving on to the configuration. Once all requirements for your selected templates have been satisfied, you can proceed to the configuration pages.



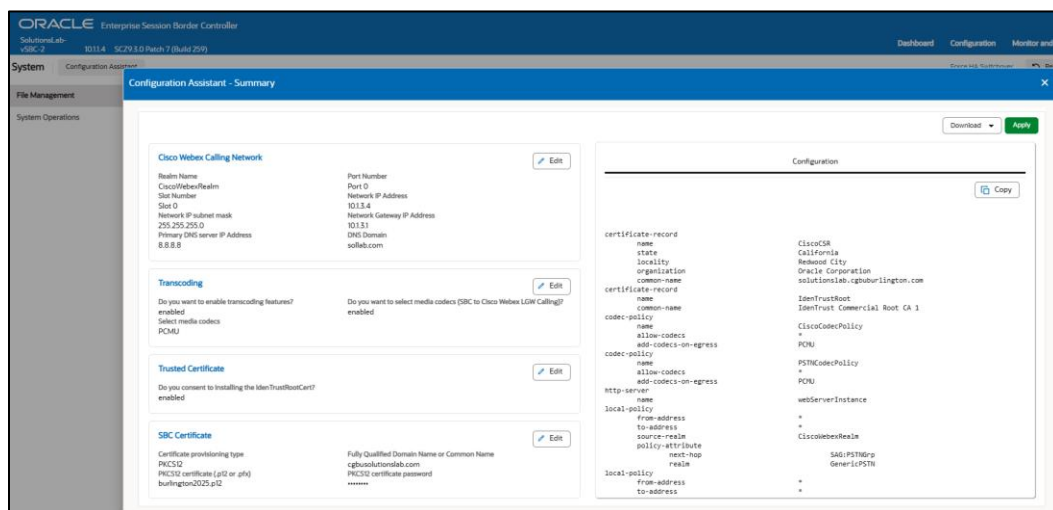
Follow the instructions on each page. Any field that is labeled required must contain an entry.

Once you have entered all information in required fields on all pages, select the option to Review in the top right of the screen:



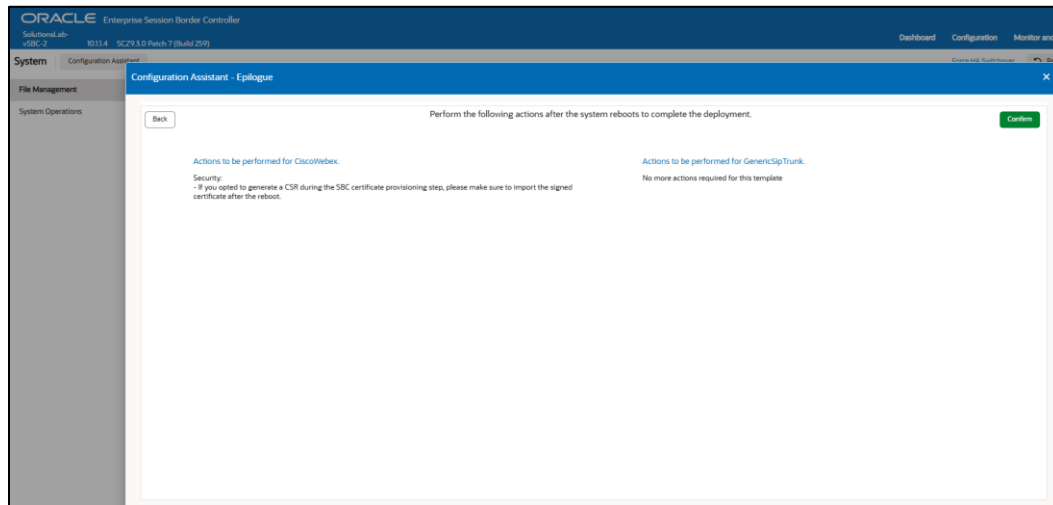
The left side of the review page contains all of the entries added on each page and allows for editing each page individually if necessary.

The right side displays the entire configuration created and when applicable, will also have a CSR tab that contains a certificate that can be signed by a CA authority.

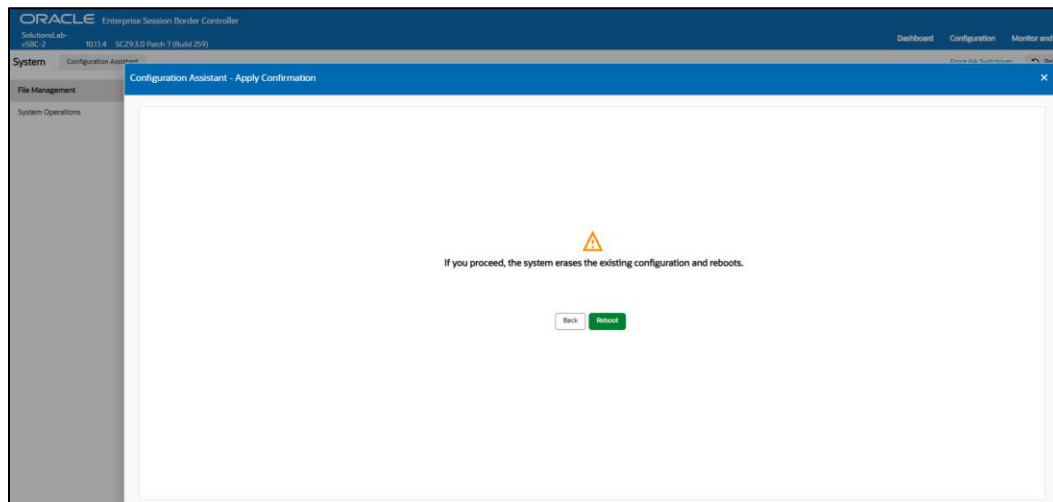


Once all the information has been reviewed and accepted, click Apply.

The SBC now presents the Epilogue.



Confirm, and then select reboot to apply the new configuration to the SBC.



When the SBC comes back up, you can verify connectivity between the SBC and Cisco WebEx Calling UCaaS platform.

9 Verify Connectivity

After you've paired the Oracle SBC with Cisco Webex Calling platform, validate that the SBC can successfully exchange SIP Options with Cisco Webex

While in the Oracle SBC GUI, Utilize the “Widgets” to check for OPTIONS to and from the SBC.

- At the top, click “Widgets.”

This brings up the Widgets menu on the left-hand side of the screen.

GUI Path: Signaling/SIP/Method/Method Option

Message/Event	Server Recent	Server Total	Server PerMax	Client Recent	Client Total	Client PerMax
OPTIONS Requests	20	2647	16	20	2644	16
Referencetions	0	0	0	0	0	0
200 OK	20	2647	16	20	2644	16
Transaction Timeouts	0	0	0	0	0	0
Locally Throttled	0	0	0	0	0	0

Looking at both the **Server Recent** and **Client Recent**, verify the counters are showing OPTIONS Requests and 200OK responses.

10 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

11 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>

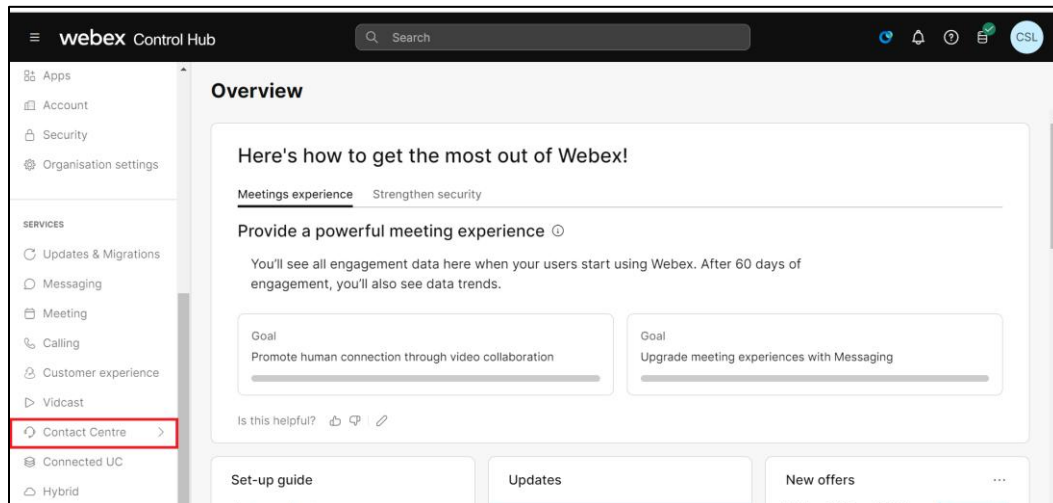
<https://help.webex.com/en-us/article/n5595zd/Webex-Contact-Center-Setup-and-Administration-Guide>

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, 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. **Additional configuration of Cisco Webex Contact Center may be necessary to meet specific customer requirements and ensure optimal operation. For advanced configuration needs, please consult your Cisco representative, as these topics are beyond the scope of this document.**

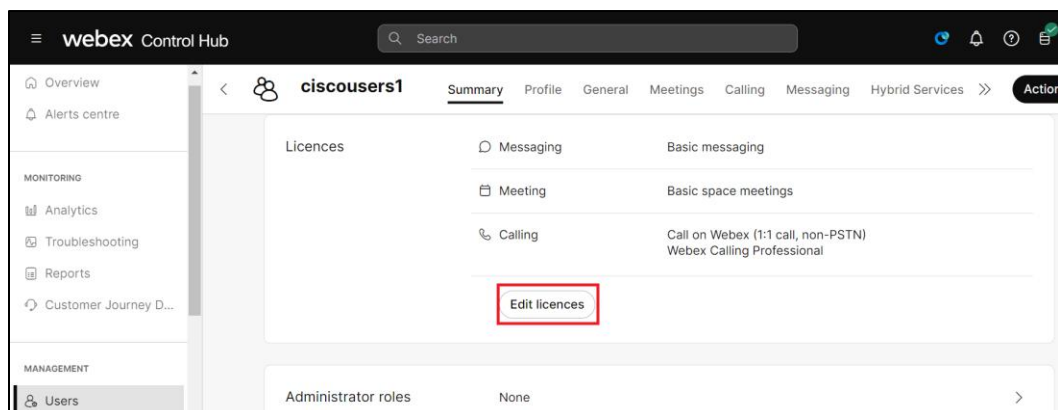
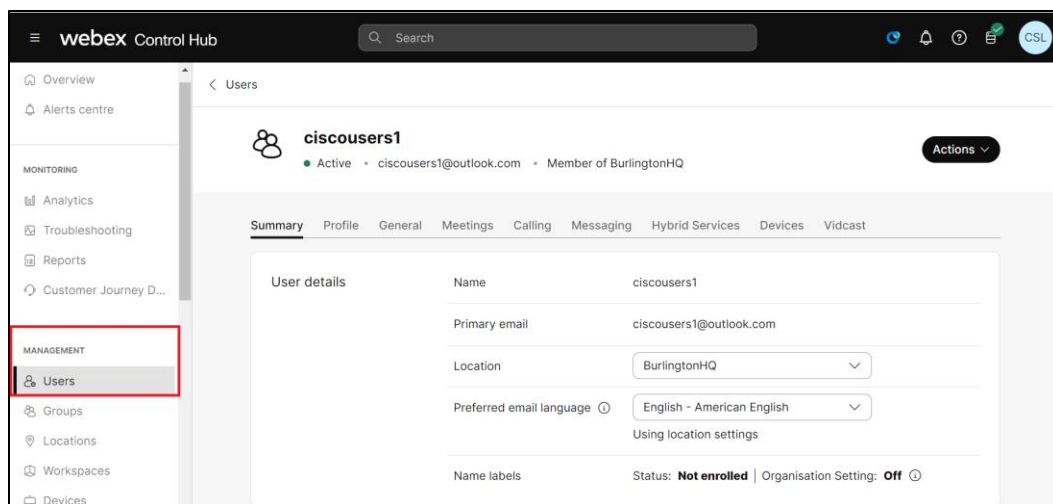
Webex admin page with Contact Center tab enabled:

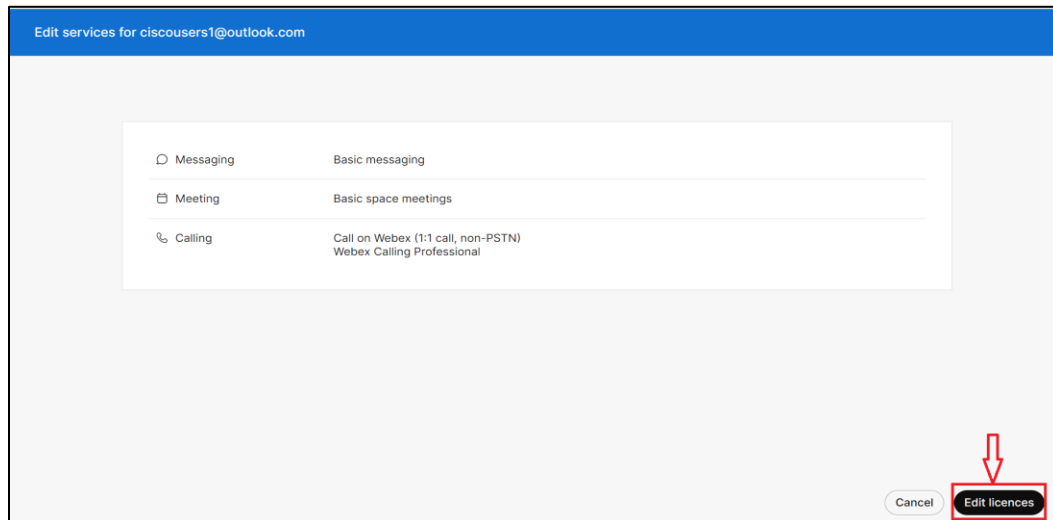


11.1 Assigning Webex Contact Center Licenses to Users

The first step is to assign the Webex Contact Center license to users.

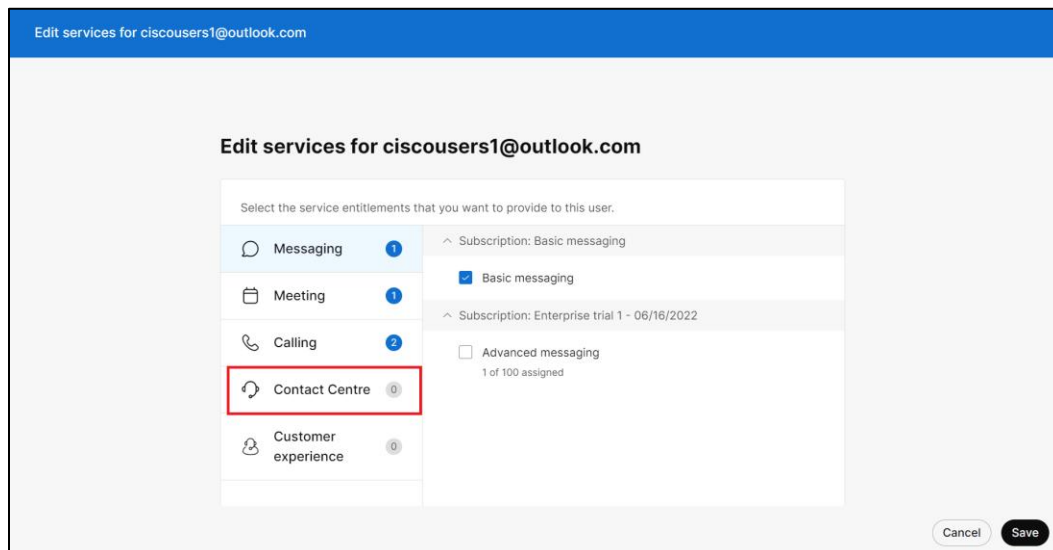
Log in to the **Cisco Webex Control Hub** portal and navigate to **Management > Users**. From there, enable the Webex CC license for the desired users as shown below.





Click on the **Contact Center** tab and choose the appropriate agent type: Standard Agent, Premium Agent, or Premium Agent with Supervisor role. Select the agent type that best fits your requirements. You can also designate an agent as an Admin for Webex Contact Center if needed.

After making your selections, click Save to apply the changes. Repeat this process for any additional users who will serve as agents in Webex Contact Center.



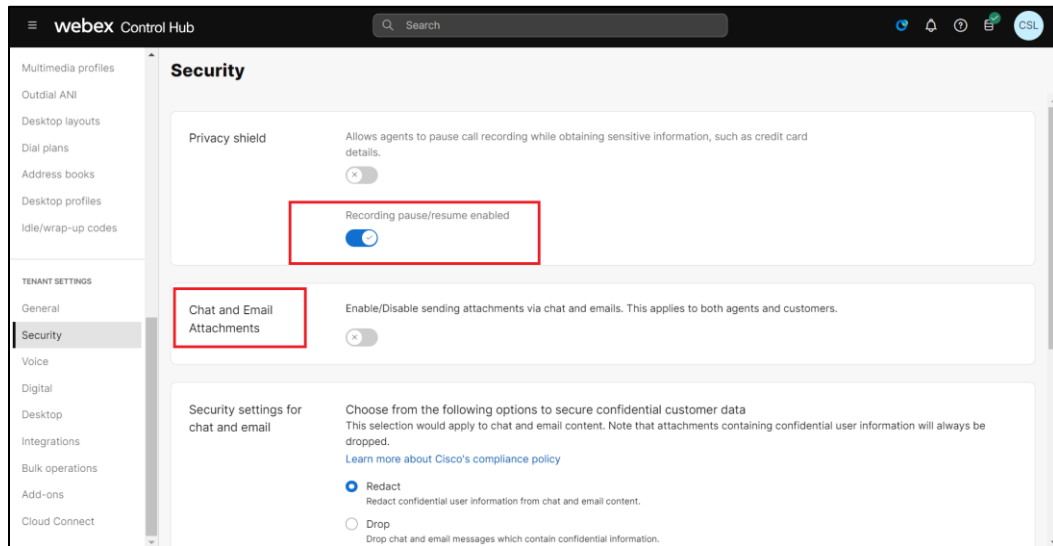
11.2 Synchronize Users with the Webex Contact Center Tenant

Navigate to **Cisco Webex Control Hub portal > Services > Contact Center > Tenant Settings > General**, and click on the **Synchronize Users** tab. This ensures that any recent changes to user accounts are reflected in the Cisco Webex Contact Center page. You can also update the time zone from this page; other settings can typically be left at their default values.

11.3 Configure Settings in the Security Tab.

Go to **Cisco Webex Control Hub portal > Services > Contact Center > Tenant Settings > Security** and configure the following settings:

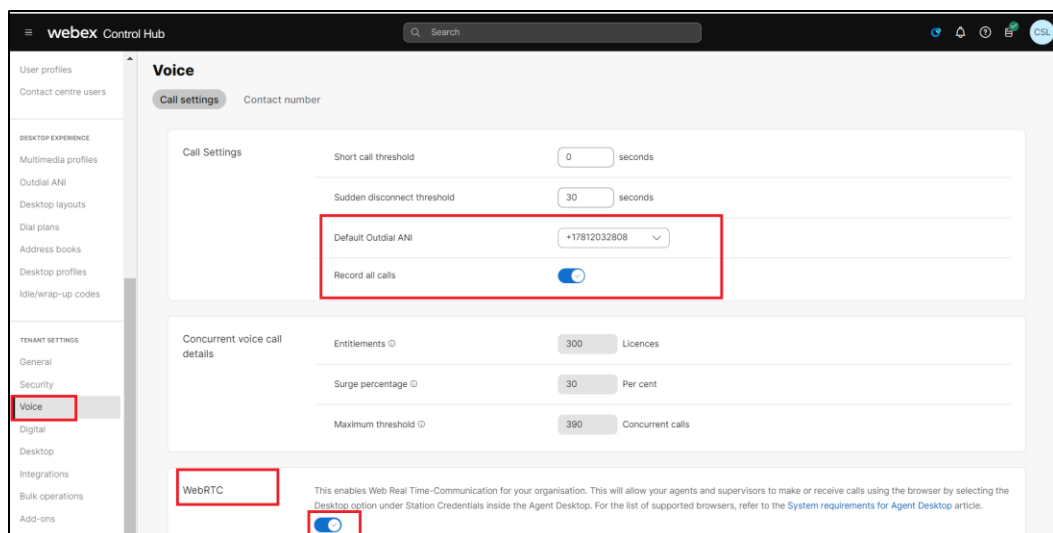
- Under the Privacy Shield tab, enable Recording Pause/Resume.
- Disable Chat, Email, and Attachments features, as this setup is focused solely on the Calling option.



11.4 Configure Settings in the Voice Tab.

Go to **Cisco Webex Control Hub portal > Services > Contact Center > Tenant Settings > Voice** and enter a DID for the default out-dial ANI. This number will be used for inbound calls to Webex Contact Center from external sources and will route callers to the IVR prompt.

Additionally, enable **WebRTC** to provide agents with access to the Webex Contact Center Agent Desktop option.



11.5 Configure the Multimedia Profile Tab.

Go to **Cisco Webex Control Hub portal > Services > Contact Center > Desktop Experience > Multimedia Profile** and create a multimedia profile for the agents. This configuration allows agents to manage multiple contact types across various channels simultaneously. For this setup, set the number of simultaneous calls to 1 and leave the other channel options at zero, as they are not required for our use case.

webex Control Hub

Helpdesk

General

Name * Helpdesk

Description Helpdesk Multimedia Profile

Referenced by You can access following link to see which other entities are referenced.
Reference list

More Details

Select one from the following options.

☒ Blended

☐ Blended real time

☐ Exclusive

This option allows agents to handle multiple contacts in different channel types simultaneously. Select the number of simultaneous contacts per channel type.

Voice	1
Chat	0
Email	0
Social	0

11.6 Configure the Desktop Profile Tab.

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.

webex Control Hub

Desktop profiles

Agent-Profile

ID: e1e100f5-c0c3-4212-a829-973c0bb93c16 · Last Modified: September 17, 2024 18:57 pm

General Idle/wrap-up codes Collaboration Dial plans Voice channel options Agent statistics Desktop timeout

General

Name * Agent-Profile

Description Agent profile

Parent type Tenant

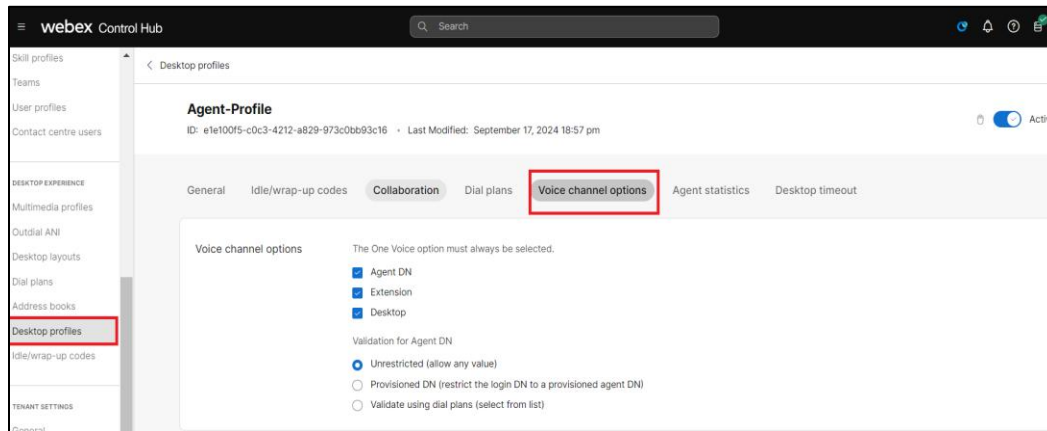
Screen pop-ups

Last agent routing

Auto answer

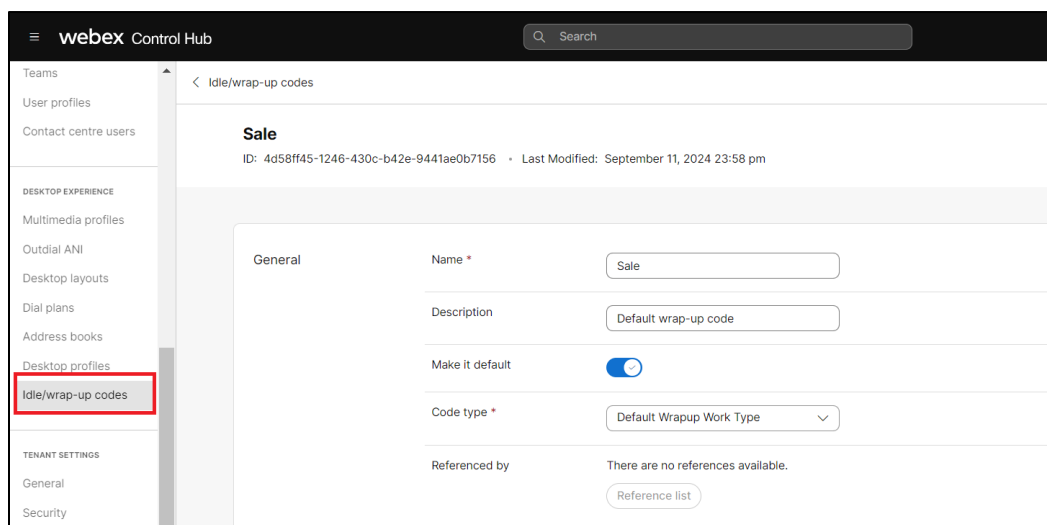
Referenced by You can access following link to see which other entities are referenced.
Reference list

Click on **Voice Channel Options** and select the configurations as indicated below.



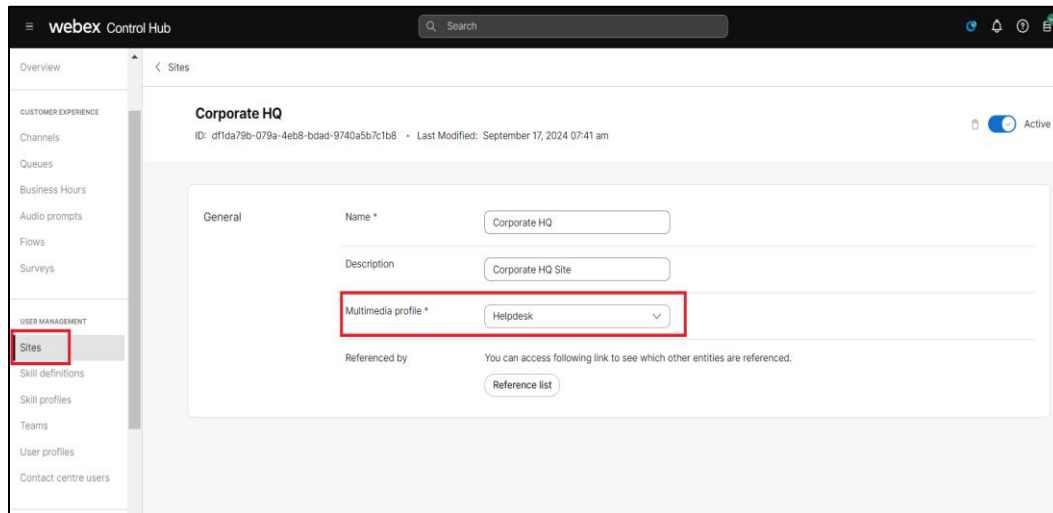
11.7 Configure the Idle/Wrap-up Codes Tab.

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.



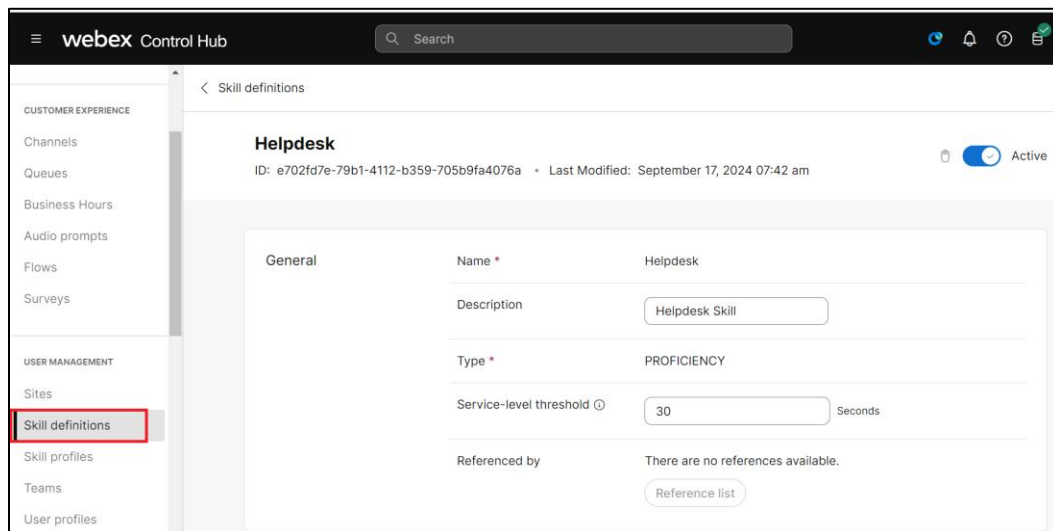
11.8 Configure the Sites Tab.

Go to **Cisco Webex Control Hub portal > Services > Contact Center > User Management > Sites** and create a new site. Assign the previously created Multimedia Profile to this site as shown below.



11.9 Configure the Skill Definitions Tab.

Go to **Cisco Webex Control Hub portal > Services > Contact Center > User Management > Skill Definitions** and create a new skill profile as shown below.



11.10 Configure the Contact Center Users Tab.

Go to **Cisco Webex Control Hub portal > Services > Contact Center > User Management > Contact Center Users**. Here you will see the users who have been assigned a Webex CC license and synchronized with Webex Contact Center. You can edit these users and assign the previously created profiles as shown below.

webex Control Hub

Search

Surveys

USER MANAGEMENT

Sites

Skill definitions

Skill profiles

Teams

User profiles

Contact centre users

DESKTOP EXPERIENCE

Multimedia profiles

Outdial ANI

Desktop layouts

Dial plans

Address books

cisco users1

ID: de5c55e6-84d4-48e8-941a-9b2f7dea0081 • Last Modified: October 21, 2024 11:42 am

Active

General

First name: cisco

Last name: users1

Email: ciscousers1@outlook.com

User Profile *: Premium Agent U...

Contact Centre *: ☒

Referenced by: You can access following link to see which other entities are referenced. [Reference list](#)

webex Control Hub

Search

Surveys

USER MANAGEMENT

Sites

Skill definitions

Skill profiles

Teams

User profiles

Contact centre users

DESKTOP EXPERIENCE

Multimedia profiles

Outdial ANI

Desktop layouts

Dial plans

Address books

Desktop profiles

cisco users1

Agent settings

Site *: Corporate HQ

Teams: Helpdesk

1 Teams [Clear All](#)

Desktop profile *: Agent-Profile

Multimedia profile: Helpdesk

Skill profile: Helpdesk

Default DN:

External ID:

With these steps, the basic configuration of Webex Contact Center is complete.
After completing the initial configuration, agents can log in using the link provided below.

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

After logging in, agents in Cisco Webex Contact Center typically operate in one of three modes, as shown below.

Station Credentials

Select your telephony option ⓘ

☒ Dial Number
 ☐ Extension
 ☐ Desktop

☒ International Dialling Format ⓘ

+1 ⓘ Enter Dial Number

Team

Team_cpalsau ⓘ

☒ Remember My Credentials

Cancel Submit

Select Dial Number for:

- PSTN based Agent
- On Premise Telephony

Station Credentials

Select your telephony option ⓘ

☐ Dial Number
 ☒ Extension
 ☐ Desktop

2001 ⓘ

Enter your calling extension number provided by the administrator.

Team

Team_cpalsau ⓘ

☒ Remember My Credentials

Cancel Submit

Select Extension for:

- Webex Telephony
- Webex App

Station Credentials

Select your telephony option ⓘ

☐ Dial Number
 ☐ Extension
 ☒ Desktop

Desktop allows to receive inbound calls and make outdial calls through the Internet.

Team

Team_cpalsau ⓘ

☒ Remember My Credentials

Cancel Submit

Select Desktop for:

- WebRTC

desktop.wxcc-us1.cisco.com

Webex Contact Center

Home

No tasks

Station Credentials

Select your telephony option ⓘ

☒ Dial Number
 ☐ Extension
 ☐ Desktop

☐ International Dialling Format ⓘ

Dial Number

Team

Helpdesk ⓘ

☐ Remember My Credentials

Cancel Submit

The following are key test cases performed for Webex Contact Center, in addition to the comprehensive tests conducted during the SBC certification with Cisco Webex LGW. We have verified that voice calls are successfully routed to the agent using Oracle SBC, and the test cases listed below have passed for all three agent 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

12 Appendix A

12.1 Multi-Tenancy

This section describes the requirement for the Oracle SBC to support multi-tenancy. Multi-tenancy essentially means configuring an Oracle SBC for hosting multiple trunks for the same customer or multiple customers.

Cisco Webex Calling has 4 models for multitenancy. They are as follows:

- Model 1: Trunk address is an FQDN, Unique IP address per trunk, same listen port.
- Model 2: Trunk address is an FQDN, shared IP on the Oracle SBC but different listen ports.
- Model 3: Trunk address is an SRV, Unique IP address per trunk, same listen port.
- Model 4: Trunk address is an SRV, shared IP address per trunk, different listen port.

The following configuration applies to all four deployment models described below. We are highlighting this requirement up front to ensure consistent configuration across all scenarios.

12.1.1 Security Configuration

To support multitenancy in a Webex Calling environment, the TLS configuration on the Oracle SBC must include the IP address or FQDN for each trunk as either a Common Name (CN) or Subject Alternative Name (SAN) in the SBC's end-entity certificate. This certificate, which is presented by the Oracle SBC to Cisco to secure the trunk, ensures proper authentication and connectivity for all configured trunks.

12.1.1.1 Certificate Record

You can create a separate TLS certificate to secure each FQDN or IP address or use a single certificate that includes all necessary FQDNs and IPs in the CN or SAN fields. Each environment may have unique requirements; however, for the purposes of this example, we will illustrate using a single certificate with the CN/SAN method to support multiple trunks.

GUI Path: security/certificate-record

ACL Path: config t→security→certificate-record

Use the following example to configure a certificate record to support your multitenant environment.

ORACLE Enterprise Session Border Controller

SolutionsLab-vSBC-2 1011.4 SCZ9.3.0 Patch 7 (Build 259)

Configuration View Configuration

media-manager >

security >

authentication-profile >

certificate-record

global-trusted-ca >

tls-global >

tls-profile >

session-router >

system >

Modify Certificate Record

Name CloudSBC

Country US

State MA

Locality Burlington

Organization Engineering

Unit

Common Name cloudsbc.cgbusolutionslab.com

Key Size 2048

Alternate Name DNS:cisco2.cgbusolutionslab.com

Please notice, when adding an alternate name to the SBC's end entity certificate, you must use the following format for each type of entry:

- IP:<IP Address> Example→ IP:10.2.2.2
- DNS:<FQDN> Example→ DNS:bar.example.com

Each entry must be comma separated.

Save and active your config.

Next, following the steps outlined previously in the [Security chapter](#) of this document that outlines the procedure to generate a CSR and imported your signed certificate.

12.1.1.2 Sip Manipulation

To ensure that the SBC generates SIP messages conforming to Cisco Webex Calling requirements across both Realms in this multitenancy example, create SIP manipulation rules to:

- Change the Contact header's host URI to the SBC's FQDN.
- Add a Contact header to SIP OPTIONS messages that includes the SBC's FQDN and Port.
- Modify the From URI host to the SBC's FQDN
- Change the P-Asserted-Identity (P-Asserted-ID) host part to the SBC's FQDN.
- Modify the To URI Host to the Cisco Webex Calling hostname

GUI Path: session router/sip manipulation

ACL Path: config t→session-router→sip-manipulation

Click Add, and use the following example to configure:

While this can be configured via the GUI, we are using the ACLI output to provide an example config for ease of viewing.

```

sip-manipulation
  name To_Webex
  header-rule
    name AddContactInOptions
    header-name Contact
    action add
    msg-type request
    methods OPTION
    new-value "sip:ping@"+$TRUNK_GROUP_CONTEXT+":."+$TRUNK_GROUP+";transport=tls"
  header-rule
    name ChangeContactHost
    header-name Contact
    action manipulate
    msg-type out-of-dialog
    methods INVITE
    element-rule
      name contacthost
      type uri-host
      action replace
      new-value $TRUNK_GROUP_CONTEXT
  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 ChangeFromIP
    header-name FROM
    action manipulate
    msg-type out-of-dialog
    methods INVITE
    element-rule
      name ChangeFrom
      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 out-of-dialog
    methods INVITE
    element-rule
      name ChangeTo
      type uri-host
      action replace
      new-value $MANIP_STRING

```

12.1.2 Additional Configuration Elements for Multitenancy

The following example assumes the foundational configuration steps outlined earlier in this document and builds upon them to demonstrate multitenancy-specific elements.

12.1.2.1 Realm Config

Nested Realm for Webex

Nested Realms is an Oracle SBC feature that supports hierarchical realm groups, allowing one or more realms to be nested within a higher-order (parent) realm. This structure enables the Oracle SBC to logically separate each tenant in a multitenancy environment.

In this example, we will create an additional realm for interfacing with Cisco Webex. The configuration will consist of a parent realm and a child realm, with each realm containing the FQDN for the respective tenant serviced by the Oracle SBC.

GUI Path: media-manger/realm-config

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

- Click Add and use the following table as a configuration example for the two realms used in this configuration example.

Config Parameter	Parent Realm	Child Realm
Identifier	CiscoWebexRealm	CiscoCust1
Network Interface	S1p0:0	S1p0:0
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Media Sec policy	CiscoWebexSecurity	CiscoWebexSecurity
Codec policy	CiscoCodec	CiscoCodec
Trunk Context	Cloudsbc.cgbusolutionslab.com	Cisco2.cgbusolutionslab.com
Access-control-trust-level	HIGH	HIGH
Parent Realm		CiscoWebexRealm

Please also note the “trunk context” parameter. The value you set here should be the SBC’s FQDN for each interface, which was registered earlier in the Webex Control Hub. Previously in this chapter, this value is used to adjust SIP header syntax to match Cisco Webex Calling requirements.

Select	Action	Identifier	Description	Addr Prefix	Network Interfaces	Media Realm List	Mm In Realm
<input type="checkbox"/>	:	CiscoCust1	Child Realm for Multitenancy	0.0.0.0	s1p0:0.4		enabled
<input type="checkbox"/>	:	CiscoWebexRealm		0.0.0.0	s1p0:0.4		enabled

12.1.2.2 Sip Interface

The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages.

Configure two sip interfaces facing Cisco Webex, one for each tenant the SBC is servicing. Please pay close attention to the differences between Models 1 and 3, and models 2 and 4.

GUI Path: session-router/sip-interface

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

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

Config Parameter	CiscoWebexRealm	CiscoCust1
Realm ID	CiscoWebexRealm	CiscoCust1
User Agent	Oracle/VM/9.3.0	Oracle/VM/9.3.0
Initial Inv Trans Expire	10	10
Out Manipulationid	To_Webex	To_Webex
Sip Port Config Parmeter	Models 1 and 3	
Address	10.1.2.4	10.1.2.5
Port	5061	5061
Transport protocol	TLS	TLS
TLS profile	TLSWebex	TLSWebex
Allow anonymous	Agents-only	Agents-only
Sip Port Config Parameter	Models 2 and 4	
Address	10.1.2.4	10.1.2.4
Port	5061	5062
Transport protocol	TLS	TLS
TLS profile	TLSWebex	TLSWebex
Allow anonymous	Agents-only	Agents-only

ORACLE

Enterprise Session Border Controller

SolutionsLab-vSBC-2

10.11.4 SCZ9.3.0 Patch 7 (Build 259)

Configuration

View Configuration

Q

security

session-router

access-control

account-config

filter-config

ldap-config

local-policy

SIP Interface

Delete all SIP Interface items

Select	Action	State	Realm ID	Description
<input type="checkbox"/>	<div></div>	enabled	CiscoCust1	
<input type="checkbox"/>	<div></div>	enabled	CiscoWebexRealm	

12.1.2.3 Session Agent

Session Agents are configuration elements which are trusted agents that can both send and receive traffic from the Oracle SBC with direct access to the trusted data path. In Cisco multitenancy environments, we set up two SRV session agents that interface with Cisco Webex Calling.

GUI Path: session-router/session-agent

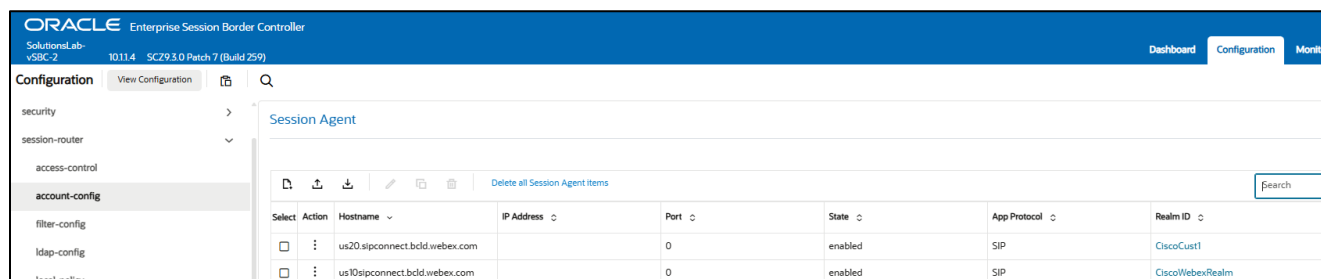
ACL Path: config t→session-router→session-agent

- Click Add, and use the table below to configure:

Config parameter	Session Agent 1	Session Agent 2
Hostname	us10.sipconnect.bclld.webex.com	us20.sipconnect.bclld.webex.com
Port	0	0
Transport method	StaticTLS	StaticTLS
Realm ID	CiscoWebexRealm	CiscoCust1
Ping Method	OPTIONS	OPTIONS
Ping Interval	30	30
Ping Response	enabled	enabled
Ping All Addresses	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Manipulation-string	us10.sipconnect.bclld.webex.com	us20.sipconnect.bclld.webex.com
Models 1 and 3		
Trunk-group	5061	5061
Models 2 and 4		
Trunk-group	5061	5062

Notice, for session agent configuration, the only difference between the models lies in the trunk group parameter, which specifies the SIP port for each interface according to the model.

Note: When deployed to support Cisco Webex multitenancy, the SBC has a limitation where it will only send SIP OPTIONS messages from a single realm to a global session agent. This can impact environments requiring OPTIONS from multiple realms to monitor the health of each trunk. Please see [SIP OPTIONS ping from multiple Realms to global session agents](#) under [Known Issues and Limitations](#) chapter for more information.



Select	Action	Hostname	IP Address	Port	State	App Protocol	Realm ID
<input type="checkbox"/>		us20.sipconnect.bclld.webex.com		0	enabled	SIP	CiscoCust1
<input type="checkbox"/>		us10.sipconnect.bclld.webex.com		0	enabled	SIP	CiscoWebexRealm

12.1.2.4 Routing Configuration

Next, we will create a new routing policy to direct traffic from the PSTN to the appropriate child tenant. For simplicity, the local policy will use the TO address field for DID separation and route calls to the child realm configured in the previous step.

GUI Path: session-router/local-policy

ACL Path: config t→session-router→local-policy

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The left sidebar lists configuration categories: security, session-router, access-control, account-config, filter-config, ldap-config, local-policy (selected), local-routing-config, media-profile, and session-agent. The main panel is titled 'Add Local Policy Entries'. It contains fields for 'From Address' (with a placeholder '* x'), 'To Address' (with two input boxes containing '17815551212 x' and '17815551213 x'), 'Source Realm' (with a dropdown showing 'SIPTrunk x'), 'Description' (with the text 'Route from PSTN to Cisco Webex Child Realm'), and 'Policy Priority' (with a dropdown showing 'none').

After entering values for to and from address and source realm, click Add under policy attribute to configure the next hop destination.

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The left sidebar lists configuration categories: media-manager, security, session-router, access-control, and account-config. The main panel is titled 'Modify Local policy / policy attribute'. It contains fields for 'Next Hop' (with a dropdown showing 'us10sipconnect.bcid.webex.com'), 'Realm' (with a dropdown showing 'CiscoWebexRealm'), and 'Action' (with a dropdown showing 'replace-uri').

- Select OK when applicable on each screen.

Save and Active your config.

This completes the basic configuration necessary to support Cisco Webex Calling multitenancy across all four models specified by Cisco.

13 Appendix B

13.1 Oracle SBC deployed behind NAT

The Support for SBC Behind NAT SPL plug-in changes information in SIP messages to hide the end point located inside the private network.

The specific information that the Support for SBC Behind NAT SPL plug-in changes depends on the direction of the call, for example, from the NAT device to the SBC or from the SBC to the NAT device.

Configure Support for SBC Behind NAT SPL plug-in for each SIP interface that is connected to a NAT device. One public-private address pair is required for each SIP interface that uses the SPL plug-in, as follows.

- The private IP address must be the same IP as configured on both the SIP Interface and Steering Pool
- The public IP address must be the public IP address of the NAT device.

Here is an example configuration with SBC Behind NAT SPL config.

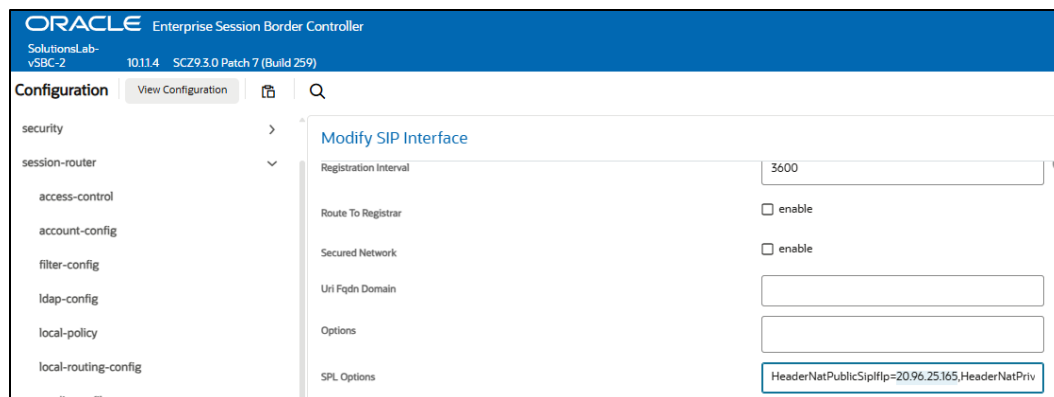
The SPL is applied to the Webex side SIP interface.

GUI Path: session-router/sip-interface

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

HeaderNatPublicSipIfIp=20.96.25.165,HeaderNatPrivateSipIfIp=10.1.3.4

- HeaderNatPublicSipIfIp is the public interface ip
- HeaderNatPrivateSipIfIp is the private ip.



You will need to apply these options to every sip interface on the SBC that is connected through a NAT.

14 Known Issues and Limitations

14.1 SIP OPTIONS ping from multiple Realms to global session agents.

When deployed to support Cisco Webex multitenancy, the SBC has a limitation where it will only send SIP OPTIONS messages from a single realm to a global session agent. This can impact environments requiring OPTIONS from multiple realms to monitor the health of each trunk.

For customers running SBC versions prior to 10.0, workarounds are available, please refer to [OCSBC-SIP OPTIONS monitoring in Multi-Tenant environments](#) BCP guide for more details. However, this limitation is fully resolved starting with SBC release 10.0, which introduces a new configuration feature that enables SIP OPTIONS pings from multiple realms to global session agents. Please see **SIP Pings from Multiple Realms to Global SAs** section under the **Session Routing and Load Balancing** chapter of the [ESBC Configuration Guide](#) for detailed information.

14.2 Video Call Issues When Calls Originate from Cisco CUCM Towards Cisco Webex

Some customers experienced issues establishing video calls between on-premises CUCM and Webex Calling when using Oracle SBC as the Local Gateway (LGW). This problem is related to how video negotiation is handled between the systems.

The issue is resolved by removing the following headers from the SDP video attribute in messages sent from Cisco CUCM to Cisco Webex:

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

We have created the SIP manipulation mime-rule below to remove these headers. This SIP manipulation must be applied to traffic directed towards the Cisco Webex. This would be added to the [CiscoOutManipulation](#) configured early in this document.

```

mime-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

```

14.3 ICE Candidate Priority Attribute Interoperability with Cisco MPP Handphones

When using Cisco MPP hardphones with Webex media optimization, the Oracle SBC may assign a priority value on the candidate line attributes in the SDP, leading to interoperability or ICE negotiation issues with Cisco Webex Calling. This issue is specific to deployments with Cisco MPP hardphones. It can be resolved by applying the SIP manipulation below to adjust the priority value of each host candidate. This modification should be added to the [CiscoOutManipulation](#) rule configured earlier in this document. The issue is permanently fixed in SBC software release 10.0p4.

```

mime-sdp-rule
  name          modpriorityhost
  methods       Invite
  action        manipulate
  sdp-media-rule
    name          modecandidatepriority
    media-type    audio
    action        manipulate
    comparison-type pattern-rule
  sdp-line-rule
    name          modrtcp
    type          a
    action        replace
    comparison-type pattern-rule
    match-value   (candidate.*)(659136)(.*)
    new-value     $1+2130706431+$3
  sdp-line-rule
    name          modrtcp
    type          a
    action        replace
    comparison-type pattern-rule
    match-value   (candidate.*)(659134)(.*)
    new-value     $1+2130706430+$3

```

14.4 One-Way Audio After Call Transfer with Media Optimization

When using media optimization, inbound calls to Cisco Webex Calling may experience one-way audio following a call transfer. The only known workaround at this time is for the transferee to place the call on hold and then resume it, which restores two-way audio. A permanent resolution for this issue is currently under investigation by both Oracle and Cisco development teams.

15 ACLI Running Configuration

Below is a complete output of the running configuration used to create this application note. This output includes all the configuration elements used in our examples, including some of the optional configuration features outlined throughout this document. Be aware this configuration does not include multitenancy configuration and 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.

```
access-control
  realm-id          SipTrunk
  source-address    138.3.226.40
  application-protocol SIP
  trust-level       high
certificate-record
  name              CloudSBC
  common-name       cloudsbc.cgbusolutionslab.com
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
codec-policy
  name              CiscoCodec
  allow-codecs      PCMU Telephone-Event
  add-codecs-on-egress PCMU Telephone-Event
codec-policy
  name              PSTN
  allow-codecs      *
  add-codecs-on-egress PCMU
http-server
  name              webserver
ice-profile
  name              webexice
  stun-conn-timeout 0
  stun-keep-alive-interval 0
  stun-rate-limit   0
  rtcp-stun         enabled
local-policy
  from-address      *
  to-address         *
```



```

source-realm CiscoWebexRealm
policy-attribute
  next-hop 138.3.226.40
  realm SipTrunk
  action replace-uri
local-policy
  from-address *
  to-address *
  source-realm SipTrunk
  policy-attribute
    next-hop us01.sipconnect.bcl.d.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 PSTN
network-interface
  name s0p0
  ip-address 10.1.2.4
  netmask 255.255.255.0
  gateway 10.1.2.1
network-interface
  name s1p0
  ip-address 10.1.3.4
  netmask 255.255.255.0
  gateway 10.1.3.1
  dns-ip-primary 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
  ice-profile         webexice
  access-control-trust-level  high
  trunk-context       cloudsbc.cgbusolutionslab.com
  codec-policy        CiscoCodec
  rtcp-policy         CiscoRTCP
realm-config
  identifier          SipTrunk
  network-interfaces  s0p0:0.4
  mm-in-realm         enabled
  media-sec-policy    PSTN
  access-control-trust-level  high
rtcp-policy
  name               CiscoRTCP
  rtcp-generate       all-calls
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            138.3.226.40
  ip-address           138.3.226.40
  transport-method     StaticTCP
  realm-id             SipTrunk
  ping-interval        30
  ping-response        enabled
  reuse-connections    TCP
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

```

```

sip-interface
  realm-id          CiscoWebexRealm
  sip-port
    address         10.1.3.4
    port            5061
    transport-protocol TLS
    tls-profile      TLSWebex
    allow-anonymous  agents-only
  out-manipulationid CiscoOutManipulation
  user-agent        Oracle/VM/9.3.0
sip-interface
  realm-id          SipTrunk
  sip-port
    address         10.1.2.4
    transport-protocol TCP
    allow-anonymous  agents-only
  sip-port
    address         10.1.2.4
    allow-anonymous  agents-only
  options           reuse-connections=latest
  out-manipulationid StripCiscoHeaders
sip-manipulation
  name              CiscoOutManipulation
  header-rule
    name            ChangeContactHost
    header-name      Contact
    action           manipulate
    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>"
  header-rule
    name            changeToUser
    header-name      To
    action           manipulate
    msg-type         request
    methods          INVITE

```

```

element-rule
  name      changeTOhost
  type      uri-host
  action    replace
  new-value us01.sipconnect.bclld.webex.com

header-rule
  name      ChangePAI
  header-name P-Asserted-Identity
  action    manipulate
  comparison-type pattern-rule
  methods   INVITE
  element-rule
    name      ChangePAI
    type      uri-host
    action    replace
    new-value $TRUNK_GROUP_CONTEXT

mime-sdp-rule
  name      modpriorityhost
  methods   Invite
  action    manipulate
  sdp-media-rule
    name      modecandidatepriority
    media-type audio
    action    manipulate
    comparison-type pattern-rule
    sdp-line-rule
      name      modrtsp
      type      a
      action    replace
      comparison-type pattern-rule
      match-value (candidate.*)(659136)(.*)
      new-value  $1+2130706431+$3
      sdp-line-rule
        name      modrtcp
        type      a
        action    replace
        comparison-type pattern-rule
        match-value (candidate.*)(659134)(.*)
        new-value  $1+2130706430+$3

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          StripCiscoHeaders
  description    Remove Cisco Headers to PSTN
  header-rule
    name        DeleteLocationInfo
    header-name  X-Cisco-Location-Info
    action      delete
    methods     BYE,INVITE,OPTIONS
  header-rule
    name        DeleteRecvInfo
    header-name  Recv-Info
    action      delete
    methods     BYE,INVITE,OPTIONS
  header-rule
    name        DeleteSessionID
    header-name  Session-ID
    action      delete
    methods     BYE,INVITE,OPTIONS
  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

```

sip-monitoring	
match-any-filter	enabled
monitoring-filters	*
steering-pool	
ip-address	10.1.2.4
start-port	10000
end-port	20000
realm-id	SipTrunk
steering-pool	
ip-address	10.1.3.4
start-port	10000
end-port	10999
realm-id	CiscoWebexRealm
system-config	
transcoding-cores	1
tls-profile	
name	TLSWebex
end-entity-certificate	CloudSBC
trusted-ca-certificates	GoDaddyRootCA
	WebexRootCA
	GoDaddyIntermediate
tls-version	tlsv12

ORACLE

CONNECT WITH US



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 © 2025, 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