

# ORACLE

## Oracle Session Border Controller (SBC) integration with Five9 Cloud Contact Center

Technical Application Note



**ORACLE**  
**COMMUNICATIONS**

## **Disclaimer**

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

## **Version History**

<b>Version</b>	<b>Description of Changes</b>	<b>Date Revision Completed</b>
1.0	Oracle SBC and Five9 Cloud Contact Center Config	18 Nov 2021

## Table of Contents

<b>1. INTENDED AUDIENCE.....</b>	<b>4</b>
<b>2. DOCUMENT OVERVIEW .....</b>	<b>4</b>
2.1 ORACLE SBC.....	4
2.2 FIVE9 BYOC.....	4
<b>3. INTRODUCTION.....</b>	<b>5</b>
3.1 AUDIENCE .....	5
3.2 REQUIREMENTS .....	5
3.3 ARCHITECTURE .....	5
<b>4. CONFIGURING THE FIVE9 CLOUD CONTACT CENTER.....</b>	<b>6</b>
<b>5. CONFIGURING THE SBC.....</b>	<b>6</b>
5.1 VALIDATED ORACLE SBC VERSION .....	6
<b>6. NEW SBC CONFIGURATION .....</b>	<b>6</b>
6.1 ESTABLISHING A SERIAL CONNECTION TO THE SBC.....	6
6.2 CONFIGURE SBC USING WEB GUI.....	10
6.3 CONFIGURE SYSTEM-CONFIG .....	11
6.4 CONFIGURE PHYSICAL INTERFACE VALUES.....	12
6.5 CONFIGURE NETWORK INTERFACE VALUES .....	14
6.6 ENABLE MEDIA MANAGER.....	15
6.7 ENABLE SIP-CONFIG .....	16
6.8 CONFIGURE REALMS .....	17
6.9 CONFIGURING A CERTIFICATE FOR SBC.....	20
6.10 TLS-PROFILE .....	23
6.11 CONFIGURE SIP INTERFACES.....	23
6.12 CONFIGURE SESSION-AGENT .....	24
6.13 CONFIGURE SESSION-AGENT GROUP.....	26
6.14 CONFIGURE STEERING-POOL.....	27
6.15 CONFIGURE LOCAL-POLICY .....	27
6.16 CONFIGURE SDSE PROFILE.....	28
6.17 CONFIGURE MEDIA SECURITY PROFILE .....	29
6.18 ACCESS CONTROL.....	30
<b>7. EXISTING SBC CONFIGURATION .....</b>	<b>31</b>

## 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 (E-SBC). It is assumed that the reader is familiar with basic operations of the Oracle Communications Enterprise Session Border Controller platform along with Five9 and how SIP Trunking is implemented.

## 2. Document Overview

This Oracle technical application note outlines the configuration needed to set up the interworking between Oracle SBC and Five9 Cloud Contact Center Platform. The solution contained within this document has been tested using Oracle Communication 840. Our scope of this document is only limited to testing Oracle SBC with Five9 Cloud Contact Center Platform.

It should be noted that this application note focuses on the optimal configurations for the Oracle SBC in a Five9 BYOC Calling Environment. Many SBC applications may have additional configuration requirements that are specific to individual customer requirements. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

### **Related Documentation can be found below:**

#### 2.1 Oracle SBC

- [Oracle® Enterprise Session Border Controller ACLI Configuration Guide](#)
- [Oracle® Enterprise Session Border Controller Release Notes](#)
- [Oracle® Enterprise Session Border Controller Security Guide](#)

#### 2.2 Five9 BYOC

- [Five9® Contact Center Resources](#)
- [Five9® Softphone-Software](#)
- [Five9® Cloud Contact Center](#)
- [Five9® Cloud PBX](#)

**Please note that the IP address, FQDN and config name and its details given in this document is used as reference purpose only. The same details cannot be used in customer config and the end users can use the configuration details according to their network requirements.**

### 3. Introduction

#### 3.1 Audience

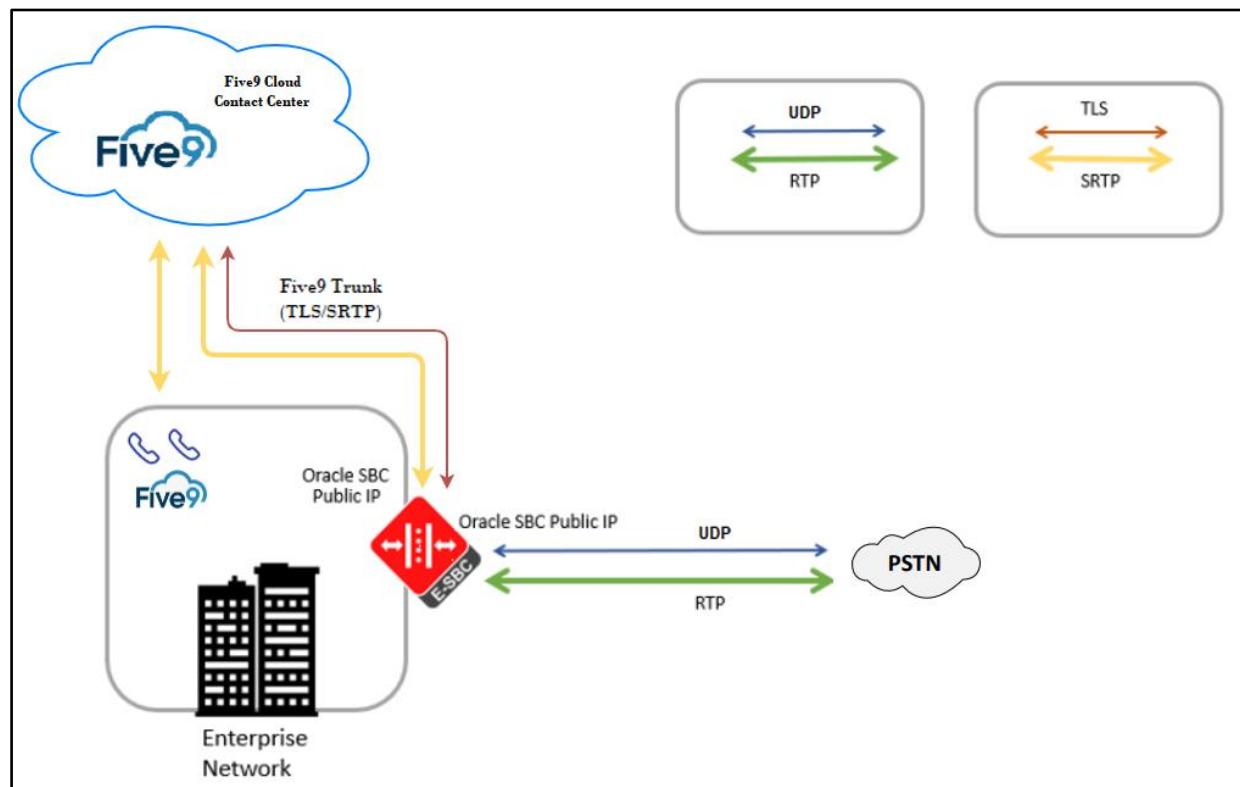
This is a technical document intended for telecommunications engineers with the purpose of configuring Five9 Cloud Contact Center Platform using Oracle Enterprise SBC. There will be steps that require navigating the Five9 Platform and Oracle SBC GUI interface. Having an understanding of the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

#### 3.2 Requirements

- Five9 Cloud Contact Center Platform
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version

#### 3.3 Architecture

This is a technical document intended for telecommunications engineers with the purpose of configuring Five9 Cloud Contact Center Platform using Oracle Enterprise SBC. There will be steps that require navigating the Five9 Platform and Oracle SBC GUI interface. Having an understanding of the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.





Above figure illustrates the connection between Five9, Oracle SBC and SIPTrunk. Both Five9 and SIPTrunk are connected to the Oracle SBC Public FQDN /IP. The connection between Five9 and Oracle SBC is TLS/SRTP and between SIPTrunk and Oracle SBC is UDP/RTP. Oracle SBC is used to steer the signaling, media to, and from the Five9 to SIPTrunk.

## 4. Configuring the Five9 Cloud Contact Center

Five9's "Bring your own carrier" (BYOC) enables users to dial out from a Five9-Cloud Contact Center to PSTN numbers such as landline phones, mobile phones and audio bridges, meaning that organizations no longer need a separate telephone in conference rooms. The customer selects and engages a telephony carrier and provides implementation details to their partner who then creates the necessary configuration. When a call is placed, the Five9 Service routes it out to the chosen carrier who then handles the call rest of the way.

**Note:** The document only includes the steps required to configure Oracle SBC. Additional configuration may apply which may not be covered in this document. Please work with your Five9 representative for the most optimal Five9 configuration as per your requirement.

## 5. Configuring the SBC

This chapter provides systematic guidance on how to configure Oracle SBC for interworking with Five9 Cloud Contact Center Platform and SIP Trunk.

### 5.1 Validated Oracle SBC version

All testing was completed using Oracle SBC 8.4 software – this software with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6300
- AP 6350
- VME
- AP 3950 (Supported Software – 9.0)
- AP 4900 (Supported Software – 9.0)

## 6. New SBC configuration

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

### 6.1 Establishing a serial connection to the SBC

**Note:** The below method is applicable to the SBCs running on Hardware Platforms. For VME and Cloud SBCs the method of configuration will be different to as shown below. Follow the appropriate documentation or contact your Oracle representative for details about how to configure the VME and Cloud SBC platforms.

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

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

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

```
>Starting tLemd...
>Starting tServiceHealth...
>Starting tCollect...
>Starting tAtcpd...
>Starting tAsctpd...
>Starting tMbcd...
>Starting tCommMonitord...
>Starting tFped...
>Starting tAlg...
>Starting tRadd...
>Starting tEbmd...
>Starting tSipd...
>Starting tH323d...
>Starting tbfd...
>Starting tIPTd...
>Starting tSecured...
>Starting tAuthd...
>Starting tCertd...
>Starting tIked...
>Starting tTscfd...
>Starting tFcgid...
>Starting tauditd...
>Starting tauditpusher...
>Starting tSnmpd...
>Starting tIFMIBd...
>Start platform alarm...
>Starting display manager...
>Initializing /opt/ Cleaner
>Starting tLogCleaner task
>Bringing up shell...

>Starting acliMgr...
>password secure mode is enabled
>Admin Security is disabled
>Password: [REDACTED]
```

Enter the default password to log in to the SBC. Note that the default SBC password is “acme” and the default super user password is “packet” for the Hardware and VME Platform.

**Follow the appropriate documentation or contact your Oracle representative for details about how to configure the Cloud SBC platforms.**

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

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

Password is acceptable.
```

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

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

```
OracleESBC#  
OracleESBC# con t  
OracleESBC(configure)# bootparam  
  
. = clear field; '-' = go to previous field; q = quit  
  
Boot File : /boot/nnSCZ840p8.bz  
IP Address : 10.138.194.139  
VLAN : 0  
Netmask : 255.255.255.192  
Gateway : 10.138.194.129  
IPv6 Address :  
IPv6 Gateway :  
Host IP :  
FTP username : vxftp  
FTP password : *****  
Flags :  
Target Name : OracleESBC  
Console Device : COM1  
Console Baudrate : 115200  
Other :  
  
NOTE: These changed parameters will not go into effect until reboot.  
Also, be aware that some boot parameters may also be changed through  
PHY and Network Interface Configurations.  
  
OracleESBC(configure)#[/pre>
```

Note: There is no management IP configured by default.

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

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

```
OracleESBC# setup product  
  
-----  
WARNING:  
Alteration of product alone or in conjunction with entitlement  
changes will not be complete until system reboot  
  
Last Modified 2021-11-16 16:15:17  
-----  
l : Product : Enterprise Session Border Controller  
  
Enter l to modify, d' to display, 's' to save, 'q' to exit. [s]:[/pre>
```

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

Save the changes and reboot the SBC.

```

Entitlements for Enterprise Session Border Controller
Last Modified: Never
-----
1 : Session Capacity : 0
2 : Advanced : :
3 : Admin Security : :
4 : Data Integrity (FIPS 140-2) : :
5 : Transcode Codec AMR Capacity : 0
6 : Transcode Codec AMRWB Capacity : 0
7 : Transcode Codec EVRC Capacity : 0
8 : Transcode Codec EVRCB Capacity : 0
9 : Transcode Codec EVS Capacity : 0
10: Transcode Codec OPUS Capacity : 0
11: Transcode Codec SILK Capacity : 0

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 1

Session Capacity (0-128000) : 500

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 3
*****
CAUTION: Enabling this feature activates enhanced security
functions. Once saved, security cannot be reverted without
resetting the system back to factory default state.
*****
Admin Security (enabled/disabled) : :

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 5

Transcode Codec AMR Capacity (0-102375) : 50

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 2

Advanced (enabled/disabled) : enabled

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 10

Transcode Codec OPUS Capacity (0-102375) : 50

Enter 1 - 11 to modify, 'd' to display, 's' to save, 'q' to exit. [s]: 11

Transcode Codec SILK Capacity (0-102375) : 50

```

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

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

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

```

OracleESBC(http-server)# show
http-server
      name                      webServerInstance
      state                     enabled
      realm
      ip-address
      http-state                enabled
      http-port                 80
      https-state               disabled
      https-port                443
      http-interface-list        []
      http-file-upload-size     0
      tls-profile
      auth-profile
      last-modified-by          admin@73.69.242.156
      last-modified-date         2021-11-16 16:19:41

```

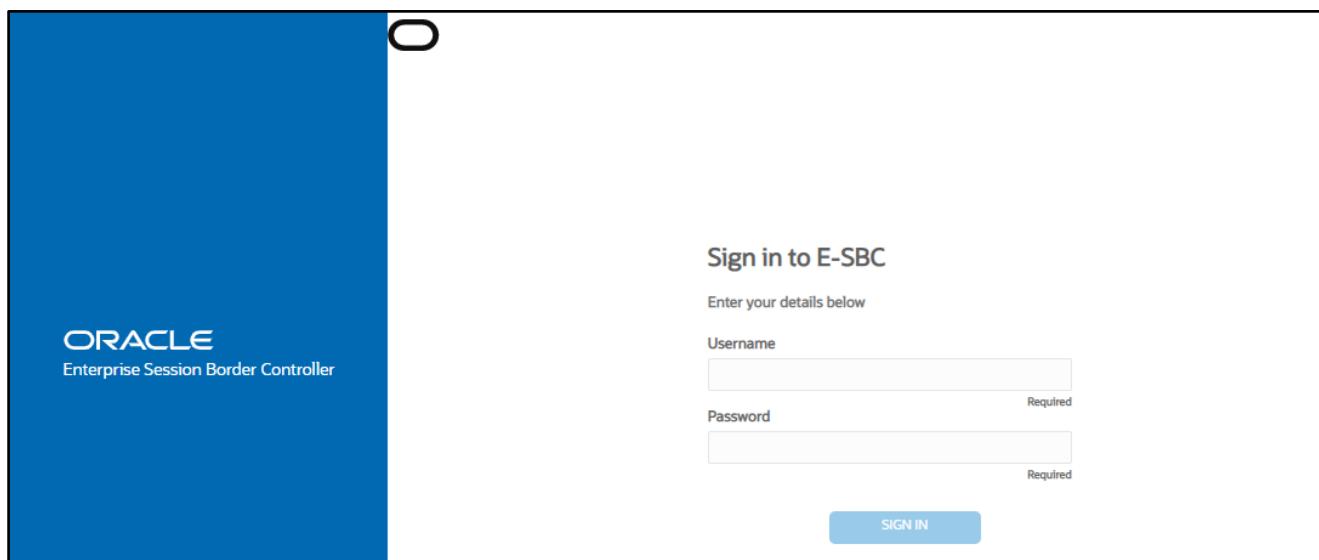
```
OracleESBC(http-server)#

```

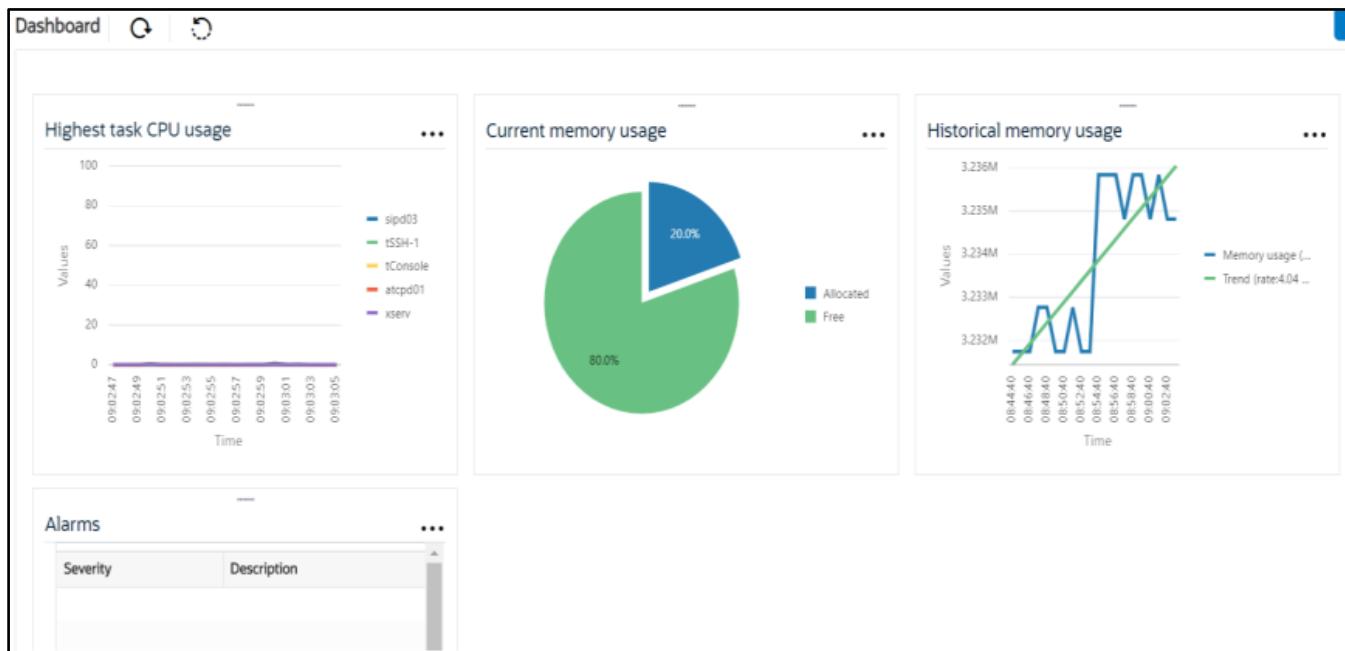
## 6.2 Configure SBC using Web GUI

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

The Web GUI can be accessed through the URL [http://<SBC\\_MGMT\\_IP>](http://<SBC_MGMT_IP>).



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



Navigate to Configuration as shown below, to configure the SBC.

The screenshot shows the Oracle Communications Session Border Controller (SC840) Configuration Objects page. The left sidebar has categories: media-manager, security, session-router, and system. The main area is titled "Configuration Objects" and lists various configuration objects with their descriptions:

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

At the bottom left, there is a "Show All" button and a status indicator. At the bottom right, it says "Displaying 1 - 9 of 40".

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

[https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc\\_scz840\\_webgui.pdf](https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf)

The expert mode is used for configuration.

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

## 6.3 Configure system-config

To configure system level functionality for the OCSBC, you must first enable the system-config

Navigate to 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 being the same as management interface gateway)

OracleESBC SCZB 4.0 Patch 8 (Build 485)

Configuration View Configuration Q

host-route  
http-client  
http-server  
network-interface  
ntp-config  
phy-interface  
redundancy-config  
snmp-community  
spl-config  
**system-config**  
trap-receiver

Add System Config

Hostname: OracleSBC  
Description:  
Location: Burlington, MA  
Mib System Contact:  
Mib System Name:  
Mib System Location:  
Acp TLS Profile:

OK Delete Show Configuration Discard Verify Save

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

OracleESBC SCZB 4.0 Patch 8 (Build 485)

Configuration View Configuration Q

fraud-protection  
host-route  
http-client  
http-server  
network-interface  
ntp-config  
phy-interface  
redundancy-config  
snmp-community  
spl-config  
**system-config**  
trap-receiver

Add System Config

Options:  
Call Trace:  enable  
**Default Gateway: 10.138.194.129**

Restart:  enable  
Telnet Timeout: 0 (Range: 0..65535)  
Console Timeout: 0 (Range: 0..65535)  
HTTP Timeout: 5 (Range: 0..20)

Alarm Threshold:

OK Delete Show Configuration Discard Verify Save

## 6.4 Configure Physical Interface values

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

ACLI Path: config t->system->phy-interface

Please configure phy-interface M00 for Five9 side and M10 for SIPTrunk side.

Parameter Name	Five9 (M00)	SIPTrunk (M10)
Slot	0	1
Port	0	0
Operation Mode	Media	Media

Configure **M00** interface as per example shared below.

OracleESBC SCZ8.4.0 Patch 8 (Build 485)

Configuration View Configuration Q

Add Phy Interface

Name	M00
Operation Type	Media
Port	0 (Range: 0..5)
Slot	0 (Range: 0..2)
Virtual Mac	
Admin State	<input checked="" type="checkbox"/> enable
Auto Negotiation	<input checked="" type="checkbox"/> enable
Duplex Mode	FULL
Speed	100
Wancom Health Score	50 (Range: 0..100)

OK Back

fraud-protection  
host-route  
http-client  
http-server  
network-interface  
ntp-config  
**phy-interface**  
redundancy-config  
snmp-community  
spl-config  
system-config  
trap-receiver

Show All

Configure **M10** interface as per example shared below.

OracleESBC SCZ8.4.0 Patch 8 (Build 485)

Configuration View Configuration Q

Add Phy Interface

Name	M10
Operation Type	Media
Port	0 (Range: 0..5)
Slot	1 (Range: 0..2)
Virtual Mac	
Admin State	<input checked="" type="checkbox"/> enable
Auto Negotiation	<input checked="" type="checkbox"/> enable
Duplex Mode	FULL
Speed	100
Wancom Health Score	50 (Range: 0..100)

OK Back

fraud-protection  
host-route  
http-client  
http-server  
network-interface  
ntp-config  
**phy-interface**  
redundancy-config  
snmp-community  
spl-config  
system-config  
trap-receiver

Show All

## 6.5 Configure Network Interface values

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

ACLI Path: config t->system->network-interface

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

**Note:** The provided network IP addresses are given for example purpose only.

In this Setup, we are using Google Public DNS to resolve the DNS names to IP Addresses.

Parameter Name	Five9	SIPTrunk
Name	M00	M10
Host Name	solutionslab.cgbubedford.com	
IP address	172.16.36.101	192.168.1.150
Netmask	255.255.255.192	255.255.255.0
Gateway	172.16.36.65	192.168.1.1
dns-ip-primary	6.6.6.6	
dns-ip-backup1	6.6.6.4	
Dns-domain	solutionslab.cgbubedford.com	

Configure network interface **M00** as below.

The screenshot shows the OracleESBC Configuration interface. The left sidebar is a tree view of configuration sections: media-manager, security, session-router, system (with sub-options like fraud-protection, host-route, http-client, http-server), network-interface (selected), ntp-config, phy-interface, redundancy-config, snmp-community, sntp-config, system-config, and trap-receiver. The main area is titled 'Add Network Interface' and contains the following fields for interface M00:

- Name: M00
- Sub Port Id: 0 (Range: 0..4095)
- Description: (empty)
- Hostname: solutionslab.cgbubedford.com
- IP Address: 172.16.36.101
- Pri Utility Addr: (empty)
- Sec Utility Addr: (empty)
- Netmask: 255.255.255.192
- Gateway: 172.16.36.65
- Gw Heartbeat:
  - State: enable (checkbox checked)
  - Heartbeat: 0 (Range: 0..65535)
  - Retry Count: 0 (Range: 0..65535)
  - Retry Timeout: 1 (Range: 1..65535)
  - Health Score: 0 (Range: 0..100)
- DNS IP Primary: 6.6.6.6
- DNS IP Backup1: 6.6.6.4
- DNS IP Backup2: (empty)
- DNS Domain: solutionslab.cgbubedford.com

At the bottom are 'OK' and 'Back' buttons.

Similarly, configure network interface **M10** as below.

OracleESBC SCZ8.4.0 Patch 8 (Build 485)

Configuration | View Configuration | Q

**Add Network Interface**

Name	M10
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	
IP Address	192.168.1.150
Pri Utility Addr	
Sec Utility Addr	
Netmask	255.255.255.0
Gateway	192.168.1.1

OK | Back

media-manager security session-router system fraud-protection host-route http-client http-server network-interface ntp-config phy-interface redundancy-config community Show All

## 6.6 Enable media manager

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

In addition to the above config, please set the max and min untrusted signaling values to 1.

Navigate to Media->Manager->Media-Manager

ACLI Path: config t->media-manager->media-manager-config

ORACLE Enterprise Session Border Controller

Dashboard | Configuration | Monitor and Trace | Widgets

**Modify Media Manager**

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

OK | Delete | Save | Verify | Discard

Wizards | Commands | media-manager | codec-policy | media-manager | media-policy | realm-config | steering-pool | security | session-router | system | Show All

## 6.7 Enable sip-config

SIP config enables SIP handling in the SBC.

Make sure the home realm-id, registrar-domain and registrar-host are configured.

Also, add the options to the sip-config as shown below.

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

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

OracleESBC SCZ8.4.0 Patch 8 (Build 485)

Dashboard Configuration Monitor

Configuration View Configuration Q

session-agent  
session-group  
session-recording-gr...  
session-recording-se...  
session-translation  
**sip-config**  
sip-feature  
sip-interface  
sip-manipulation  
sip-monitoring  
translation-rules  
system

Add SIP Config

Red Max Trans: 10000 (Range: 0..50000)  
 Options:    
 SPL Options:  
 SIP Message Len: 4096 (Range: 0..65535)  
 Enum Sag Match:  enable  
 Extra Method Stats:  enable  
 Extra Enum Stats:  enable  
 Registration Cache Limit: 0 (Range: 0.999999999)  
 Register Use To For Lp:  enable  
 Refer Src Routing:  enable

OK Delete

Show All

## 6.8 Configure Realms

Navigate to realm-config under media-manager and configure a realm as shown below.  
 ACLI Path: config t->media-manger->realm-config

The name of the Realm can be any relevant name according to the user convenience. Use the following table as a configuration example for the two realms used in this configuration:

Config Parameter	Five9 Realm	SIPTrunk Realm
Identifier	Five9	SIPTrunk
Network Interface	M00	M10
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access Control Trust Level	High	High
Media Sec policy	sdespolicy	RTP

In the below case, Realm name is given as Five9 for Five9 Side. Please set the Access Control Trust Level as high for this realm.

OracleESBC SCZ8.4.0 Patch 8 (Build 485)

Configuration View Configuration  Dashboard Configuration Monitor

**Add Realm Config**

Identifier: Five9  
Description: Realm for Five9

Addr Prefix: 0.0.0  
Network Interfaces: M00:0

Media Realm List:

Mm In Realm:  enable  
Mm In Network:  enable  
Mm Same Ip:  enable

Show All

realm-config steering-pool security session-router system

Media Policy:   
Media Sec Policy: sdesPolicy  
RTCP Mux:  enable  
Ice Profile:   
Teams Fqdn:   
Teams Fqdn In Uri:  enable  
SDP Inactive Only:  enable

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace

Wizards Commands Save Verify

**Add Realm Config**

Out Translationid:   
In Manipulationid:   
Out Manipulationid:   
Average Rate Limit: 0 (Range: 0..4294967295)  
Access Control Trust Level: high  (highlighted with red box)  
Invalid Signal Threshold: 0 (Range: 0..4294967295)  
Maximum Signal Threshold: 0 (Range: 0..4294967295)  
Untrusted Signal Threshold: 0 (Range: 0..4294967295)  
Nat Trust Threshold: 0 (Range: 0..65535)

Show All

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

OracleESBC SCZB4.0 Patch 8 (Build 485)

Configuration View Configuration Q Dashboard Configuration Monitor and Trace Discard

**Add Realm Config**

Identifier: SipTrunk

Description:

Addr Prefix: 0.0.0.0

Network Interfaces: M10:0 X

Media Realm List:

Mm In Realm:  enable

Mm In Network:  enable

Mm Same Ip:  enable

OK Back

Show All

Configuration View Configuration Q

**Modify Realm Config**

Parent Realm:

DNS Realm:

Media Policy:

Media Sec Policy: RTP

RTCP Mux:  enable

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Tra

Wizards Commands Save Verify

**Add Realm Config**

Out Translationid:

In Manipulationid:

Out Manipulationid:

Average Rate Limit: 0 (Range: 0..4294967295)

Access Control Trust Level: high

Invalid Signal Threshold: 0 (Range: 0..4294967295)

Maximum Signal Threshold: 0 (Range: 0..4294967295)

Untrusted Signal Threshold: 0 (Range: 0..4294967295)

Nat Trust Threshold: 0 (Range: 0..65535)

OK Back

We have set Access Control Trust Level on the Reams to High as we have static access-control configured and this is a peering environment.

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

[https://docs.oracle.com/en/industries/communications/session-border-controller/8.4.0/security/sbc\\_scz840\\_security.pdf](https://docs.oracle.com/en/industries/communications/session-border-controller/8.4.0/security/sbc_scz840_security.pdf)

## 6.9 Configuring a certificate for SBC

This section describes how to configure the SBC for both TLS and SRTP communication with **Five9**.

Five9 supports TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by one of the trusted Certificate Authorities.

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

GUI Path: security->certificate-record

ACLI Path: config t->security->certificate-record

The process includes the following steps:

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

### Step 1 – Creating the certificate record

Go to security->Certificate Record and configure the SBC entity certificate for SBC as shown below. We are creating this certificate for **Five9** Side. Five9 signs the BYOC Cloud endpoints with X.509 certificates issued by DigiCert, a public Certificate Authority.

The screenshot shows the Oracle SBC Configuration interface. The left sidebar shows a navigation tree with sections like media-manager, security, authentication-profile, certificate-record (which is selected and highlighted in blue), tls-global, tls-profile, session-router, and system. The main area is titled "Add Certificate Record" and contains the following fields:

- Name: SBCFive9Cert
- Country: US
- State: MA
- Locality: Burlington
- Organization: Engineering
- Unit: (empty)
- Common Name: solutionslab.cgbubedford.com
- Key Size: 2048
- Alternate Name: (empty)
- Trusted: checked
- Key Usage List: digitalSignature, keyEncipherment
- Extended Key Usage List: serverAuth, clientAuth
- Key Algor: rsa
- Digest Algor: sha256
- Ecdsa Key Size: p256
- Cert Status Profile List: (empty)
- Options: (empty)

At the bottom of the dialog are "OK" and "Back" buttons. A "Show All" button is also visible at the bottom left of the main window area.

Follow the same steps and create following intermediate and root certificates.

- DigiCert Root CA: This certificate is always required for Five9.
- DigiCert Intermediate Cert (this is optional – only required if your server certificate is signed by an intermediate)

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

Parameter	DigicertInter	DigiCertRoot
Common-name	DigiCert SHA2 Secure Server CA	DigiCert Global Root CA
Key-size	2048	2048
Key-usage-list	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended-key-usage-list	serverAuth	serverAuth
key-algor	rsa	rsa
digest-algor	sha256	sha256

## Step 2 – Generating a certificate signing request

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

- Select the certificate and generate certificate on clicking the “Generate” command.
- The Step must be performed for SBCFive9Cert.
- Please copy/paste the text that is printed on the screen as shown below and upload to your CA server for signature.

The screenshot shows the OracleESBC Configuration interface. The left sidebar navigation includes 'media-manager', 'security' (selected), 'authentication-profile', 'certificate-record' (selected), 'tls-global', 'tls-profile', 'session-router', and 'system'. The main area is titled 'Certificate Record' and displays a table of certificates. The table has columns: Action, Sel..., Name, Country, State, Locality, Organization, Unit, and Common Name. Three rows are listed:

- DigiCertInter: US, MA, Burlington, Engineering, DigiCert SHA2 Secure Server CA
- DigiCertRoot: US, MA, Burlington, Engineering, DigiCert Global Root CA
- SBCFive9Cert: US, MA, Burlington, Engineering, solutionslab.cgbutherford.com

A context menu is open over the third row (SBCFive9Cert), with options: Edit, Copy, Delete, **Generate** (highlighted in red), Import, and Sort. The top right of the interface has tabs for Dashboard, Configuration, Monitor and Trace, Widgets, System, Discard, Verify, and Save.

**Generate certificate response**

Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7CCAQAwBDELMAkGA1UEBhMCVVvMxCzAJBgNVBAgTAKIBMRMwEQYDVQQH
EwpCdJsaW5ndG9uMRQwEgYDVQQKewtFbmdpbmVlcmLuZzElMCMGAIUEAxMc29s
dXRpb25zbGFILmNnYnVzWRmb3jkLmNvbTCASlwDQYJKoZIhvnaQEBBQADgEP
ADCCAQoCggEBAPaXlVnGfTxmmofDsXlWAUFCaEuVtkzAdizDW5pBGaNsBzXR
w5xUrLknnYJro+4QuYihNvQKtfDvf3CHkg0PyhFX8zPCz7N9J7sDmultNOwy7cIT
m3nURx3nuq15O+FxL82VtEdxghlyb/3UyHgPxay7rVtviuDTku6LVqUorMQZ
4dQ1zd9nZWf5allkzs9gbn6r8COKHYNSh2grml0dcnxzp+BjN1pr+LF+8VwO
9KkMGYClakSNuBH3xH4HWsmcLNk8mVIIUvnZFGIusbOZZVr9Lxhgyz2914mY10
uLbcVSeAUknklw5WC2gPVIrn0j5lcCbsCAwEAAsA9MDsGCSoGS1b3DQEJDjEu
MCwwCwYDVROPBQAQDAgWgMB0GA1UdJQWMBQGCCsGAQUFBwMBBgrgEFBQcDAjAN
BgkqhkiG9w0BAQsFAAOCAQEAA9KxsAlqkqV0apuQCCm4McxyXBURF5SrnMROWi
nlyHdCN3me28ktzVhagYo0eSWMS9xQdGR8iA35/VovoEi6W89TwmImh5MKIIUO
zLmgPpTdJJQkyy/JUEBiqNIkdTFy05Ks4AI/5cK9dDFxaROLsL5HIIYFIG9bgP
EEjWhkUgeHPW0uPBGQKU8BxDRISeFxHs6e4GH7U4PjPMAszeeMbWx2yfjEL1Q5
try5poVquiPAjttj0dgU6wRwvifQj/OVx8mlgyuy7YwTDdYbkltg2U3RL8
nhHibDQ0cBnwVaQsosv2kZHxuVU85H8wFLE/vInCL+idQ=-
-----END CERTIFICATE REQUEST-----
```

[Close](#)

- Also note, at this point, **a save and activate is required** before you can import the certificates to each certificate record created above.

## Step 3 – Deploy SBC & root/intermediate certificates

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

Please note – all certificates including root and intermediate certificates are required to be imported to the SBC. Once done, issue **save/activate** from the WebGUI

Action	Sel...	Name	Country	State	Locality	Organization	Unit	Common Name
⋮	□	DigiCertinter	US	MA	Burlington	Engineering		DigiCert SHA2 Secu...
⋮	□	DigiCertRoot	US	MA	Burlington	Engineering		DigiCert Global Roo...
⋮	✓	SBCFive9Cert	US	MA	Burlington	Engineering		solutionslab.cgbube...

**Import Certificate**

Format: try-all

Import Method: File (radio button selected)

Certificate File: No file chosen.

[Import](#) [Cancel](#)

Repeat the steps for the following certificates:

- DigiCertInter
- DigiCertRoot.

**At this stage, all the required certificates have been imported to the SBC for Five9.**

## 6.10 TLS-Profile

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

Go to security-> TLS-profile config element and configure the tls-profile as shown below.

ACLI Path: config t->security->tls-profile

The below is the TLS profile configured for Five9 side.

OracleESBC SCZ8.4.0 Patch 8 (Build 485)

Configuration View Configuration Q

Dashboard Configuration Monitor and Trace Widgets System

Discard Verify Save

Add TLS Profile

Name: TLSFive9

End Entity Certificate: SBCFive9Cert

Trusted Ca Certificates: DigiCertRoot, DigiCertInter

Cipher List: DEFAULT

Verify Depth: 10 (Range: 0..10)

Mutual Authenticate: enable

TLS Version: t1sv12

Options: (empty)

Show All OK Back

## 6.11 Configure SIP Interfaces

Navigate to sip-interface under session-router and configure the sip-interface as shown below.  
ACLI Path: config t->session-router->sip-interface

Please configure the below settings under the sip-interface.

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

Below is the sip-interface Configured for Five9 side.

The screenshot shows the OracleESBC Configuration interface. On the left, there's a navigation tree with items like media-manager, security, session-router, access-control, account-config, filter-config, ldap-config, local-policy, local-routing-config, media-profile, session-agent, and session-group. The 'Configuration' tab is selected. In the main area, there's a 'Modify SIP Interface' form. It has fields for 'State' (checked 'enable'), 'Realm ID' (set to 'Five9'), and 'Description'. Below that is a 'SIP Ports' table:

Action	Sel...	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addrs
⋮	□	172.16.36.101	5061	TLS	TLSFive9	all	

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

This screenshot shows the same configuration interface as above, but with a different 'Realm ID' setting. The 'Modify SIP Interface' form now has 'Realm ID' set to 'SIPTrunk'. The 'SIP Ports' table shows two entries:

Action	Sel...	Address	Port	Transport Protocol	Allow Anonymous	Multi Home Addrs
⋮	□	192.168.1.150	5060	UDP	all	
⋮	□	192.168.1.150	5060	TCP	all	

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

## 6.12 Configure session-agent

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

Navigate to session-router->Session-Agent

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

Configure two session-agents for Five9 with following parameters.

- hostname and IP address both same as “162.213.103.36 / 208.69.30.39”
- port to 5061
- realm-id – needs to match the realm created for Five9
- transport set to “staticTLS”
- ping-method – send OPTIONS message to Five9 to check health
- ping-interval to 30 sec

## Five9 Session Agent 1

OracleESBC SCZ8.4.0 Patch 8 (Build 485)

Configuration View Configuration  Discard Verify Save

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

Add Session Agent

Hostname	162.213.103.36
IP Address	162.213.103.36
Port	5061 (Range: 0;1025..65535)
State	<input checked="" type="checkbox"/> enable
App Protocol	SIP
App Type	
Transport Method	StaticTLS
Realm ID	Five9
Egress Realm ID	

Show All

## Five9 Session Agent 2

OracleESBC SCZ8.4.0 Patch 8 (Build 485)

Configuration View Configuration  Discard Verify Save

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

Add Session Agent

Hostname	208.69.30.39
IP Address	208.69.30.39
Port	5061 (Range: 0;1025..65535)
State	<input checked="" type="checkbox"/> enable
App Protocol	SIP
App Type	
Transport Method	StaticTLS
Realm ID	Five9
Egress Realm ID	

Show All

Similarly, Configure the session-agent for SIPTRUNK. Go to session-router->Session-Agent.

- Host name and IP address of SIP Trunk.
- port 5060
- realm-id – needs to match the realm created for SIPTRUNK.
- transport set to “UDP”

## 6.13 Configure session-agent group

A session agent group allows the SBC to create a load-balancing model.  
 Navigate to Session-Router->Session-Group.  
 ACLI Path: config t->session-router->session-group

Please configure the following group for Five9 Session Agents.

## 6.14 Configure steering-pool

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

Navigate to GUI Path: media-manger->steering-pool  
ACLI Path: config t->media-manger->steering-pool

Five9 side Steering pool.

OracleESBC SCZ8.4.0 Patch 8 (Build 485)

Configuration View Configuration Q

media-manager

codec-policy

media-manager

media-policy

realm-config

**steering-pool**

security

session-router

system

Add Steering Pool

IP Address: 172.16.36.101

Start Port: 20000 (Range: 0..65535)

End Port: 40000 (Range: 0..65535)

Realm ID: Five9

Network Interface: [dropdown]

SIPTrunk side Steering pool.

OracleESBC SCZ8.4.0 Patch 8 (Build 485)

Configuration View Configuration Q

media-manager

codec-policy

media-manager

media-policy

realm-config

**steering-pool**

security

session-router

Add Steering Pool

IP Address: 192.168.1.150

Start Port: 20000 (Range: 0..65535)

End Port: 40000 (Range: 0..65535)

Realm ID: Five9

Network Interface: [dropdown]

## 6.15 Configure local-policy

Local policy config allows the SBC to route calls from one end of the network to the other based on routing criteria.

To configure local-policy, Navigate to Session-Router->local-policy  
ACLI Path: config t->session-router->local-policy

To route the calls from Five9 side to SIPTrunk side, Use the below local-policy.

To route the calls from the SIPTrunk side to Five9 side, Use the below local-policy.

## 6.16 Configure 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.

Configure Security -> Media Security ->sdes profile and create the policy as below.  
 ACLI Path: config t->security->media-security->sdes-profile

## 6.17 Configure Media Security Profile

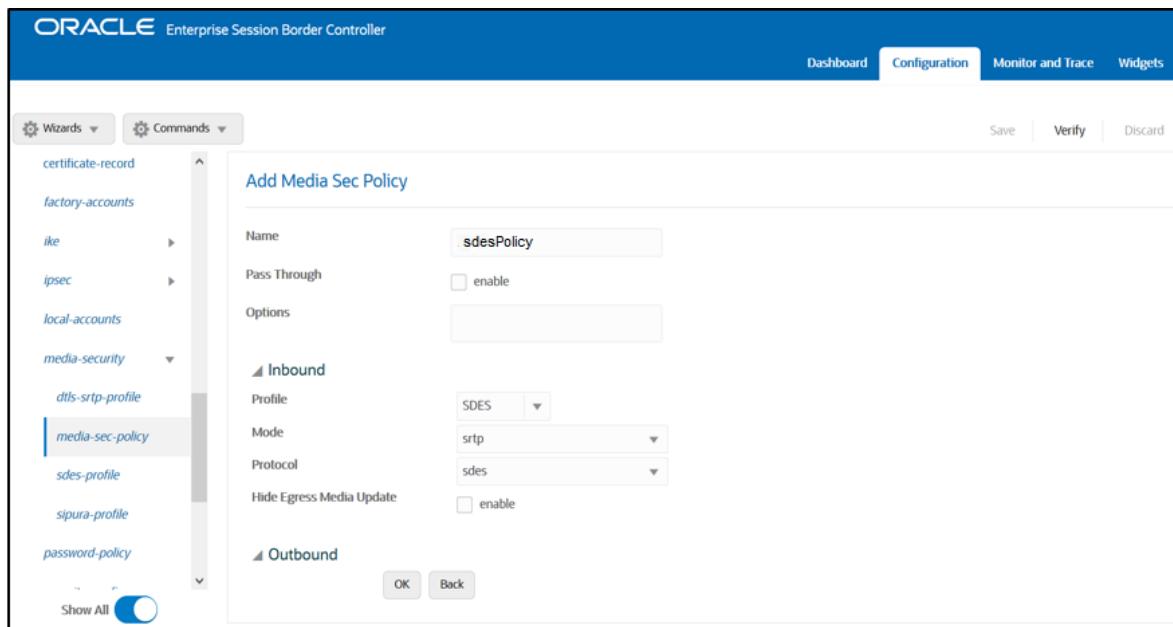
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them).

In this example, we are configuring two media security policies. One to secure and decrypt media toward Five9, the other for non-secure media facing SIPTrunk.

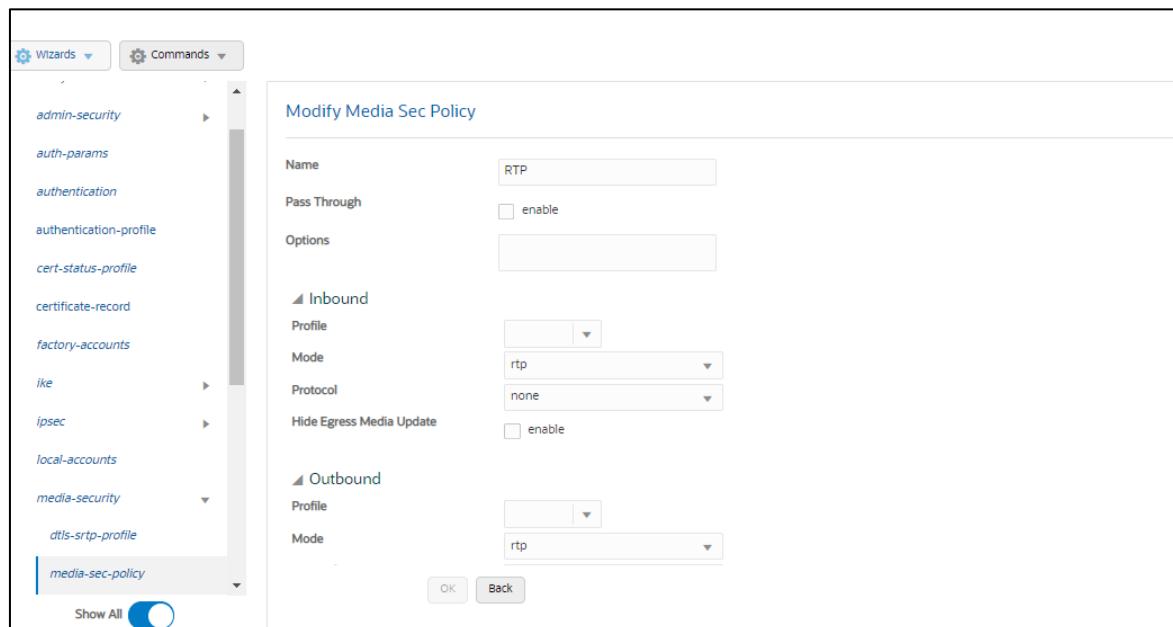
Navigate to config t->Security -> Media Security ->media Sec policy and create the policy as below:  
ACLI Path: config t->security->media-security->media-sec-policy

Create Media Sec policy with name sdesPolicy, which will have the sdes profile, created above.

**Assign this media policy to Five9 Realm.**



Similarly, Create Media Sec policy with name RTP to convert srtp to rtp for the SIPTRUNK (if the call is encrypted from Five9) which will use only TCP/UDP as transport protocol. Assign this media policy to the SIPTrunk Realm.



## 6.18 Access Control

To enhance the security of your Oracle Session Border Controller, we recommend configuration access controls to limit traffic to only trusted IP addresses on all public facing interfaces

GUI Path: session-router/access-control

Please use the example below to configure access controls in your environment for both Five9 IP's, as well as SIP Trunk IP's (if applicable).

OracleSBC SC28.4.0 Patch 8 (Build 485)

Configuration View Configuration Q

Add Access Control

Realm ID	Five9
Description	Site-1
Source Address	162.213.103.36
Destination Address	0.0.0.0
Application Protocol	SIP
Transport Protocol	ALL
Access	permit
Average Rate Limit	0 (Range: 0..100)
Trust Level	high
Minimum Reserved Bandwidth	0 (Range: 0..100)
Invalid Signal Threshold	0 (Range: 0..4294967295)
Maximum Signal Threshold	0 (Range: 0..4294967295)
Untrusted Signal Threshold	0 (Range: 0..4294967295)
Deny Period	30 (Range: 0..4294967295)
Nat Trust Threshold	0 (Range: 0..65535)
Max Endpoints Per Nat	0 (Range: 0..65535)
Nat Invalid Message Threshold	0 (Range: 0..65535)
Cac Failure Threshold	0 (Range: 0..4294967295)
Untrust Cac Failure Threshold	0 (Range: 0..4294967295)

Show All OK Back

OracleSBC SC28.4.0 Patch 8 (Build 485)

Configuration View Configuration Q

Add Access Control

Realm ID	Five9
Description	Site-2
Source Address	208.69.30.39
Destination Address	0.0.0.0
Application Protocol	SIP
Transport Protocol	ALL
Access	permit
Average Rate Limit	0 (Range: 0..100)
Trust Level	high
Minimum Reserved Bandwidth	0 (Range: 0..100)
Invalid Signal Threshold	0 (Range: 0..4294967295)
Maximum Signal Threshold	0 (Range: 0..4294967295)
Untrusted Signal Threshold	0 (Range: 0..4294967295)
Deny Period	30 (Range: 0..4294967295)
Nat Trust Threshold	0 (Range: 0..65535)
Max Endpoints Per Nat	0 (Range: 0..65535)
Nat Invalid Message Threshold	0 (Range: 0..65535)
Cac Failure Threshold	0 (Range: 0..4294967295)
Untrust Cac Failure Threshold	0 (Range: 0..4294967295)

Show All OK Back

Notice the trust level on this ACL is set to high. When the trust level on an ACL is set to the same value of as the access control trust level of its associated realm, this creates an implicit deny, so only traffic from IP addresses configured as ACL's with the same trust level will be allowed to send traffic to the SBC. For more information about trust level on ACL's and Realms, please see the [SBC Security Guide, Page 3-10](#)

## 7. Existing SBC configuration

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

- [New realm-config](#)
- [Configuring a certificate for SBC Interface](#)
- [TLS-Profile](#)
- [New sip-interface](#)
- [New session-agent](#)
- [New session-group](#)
- [New steering-pools](#)
- [New local-policy](#)
- [SDES Profile](#)
- [Media-Sec-Policy](#)
- [Access Control](#)

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



**Oracle Corporation, World Headquarters**  
500 Oracle Parkway  
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200

### CONNECT WITH US

- [blogs.oracle.com/oracle](#)
- [facebook.com/Oracle/](#)
- [twitter.com/Oracle](#)
- [oracle.com](#)

### Integrated Cloud Applications & Platform Services

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

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

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