ORACLE

Deploying Oracle SBC with PCI-PAL

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.

1 Contents

2 Related Documentation

2.1 Oracle SBC

- Oracle® Enterprise Session Border Controller Web GUI User Guide
- Oracle® Enterprise Session Border Controller ACLI Configuration Guide
- Oracle® Enterprise Session Border Controller Release Notes

2.2 PCIPAL

- PCI-PAL Knowledge Center

3 About PCIPAL

PCI Pal Digital makes secure omnichannel payments possible for contact centers.

Merchants can take payments seamlessly with full visibility across multiple engagement channels, with flexible payment options to suit any customer.

What makes the solution stand out is no matter what channel the payment link is sent through or which method the customer chooses to pay by the contact center agent can follow any customer payment journey in real time.

Ensuring no drop off, and assisting the customer if needed, meaning a great customer and agent experience all around.

4 Revision History

Version	Date Revised	Description of Changes
1.0	05/17/2019	Initial Publication
2.0	09/19/2022	9.0 Certification Changes

5 Intended Audience

This document describes how to connect the Oracle SBC to PCI-PAL. This document is intended for IT or telephony professionals.

Note: To zoom in on screenshots of Web GUI configuration examples, press Ctrl and +.

6 Validated Oracle Versions

SCZ830m1p7, SCZ9.0.0

- AP 1100
- AP 3900
- AP 3950
- AP 4600
- AP 4900
- AP 6350
- AP 6300
- VME
- Public Cloud (OCI, Azure, AWS)

7 Infrastructure Requirements

The table below shows the list of infrastructure requirements for deploying the Oracle SBC with PCI-PAL.

Infrastructure Prerequisite
Oracle Session Border Controller (SBC)
Sip Trunks connected to the SBC
Public IP address for the SBC
Public Trusted Certificate for the SBC

Please note, SSM is required for TLS on Acme Packet 4600, 6100, 6300, and 6350. SSM is not required for TLS on Acme Packet 1100, 3900, 3950, 4900, and VME/VNF. VME/VNF deployments do require a traditional TLS/SRTP license key. For more information, please refer to the 9.0 Security Guide.

8 Architecture

Below shows the connection topology

There are multiple connections shows:

- Inbound to Contact Centre: PSTN to Oracle SBC, Oracle SBC to/from PCI-PAL and Oracle SBC to Contact Centre
- Outbound from Contact Centre: Contact Centre to Oracle SBC, Oracle SBC to/from PCI-PAL, Oracle SBC to PSTN

8.1 Figure 1: Normal Operation

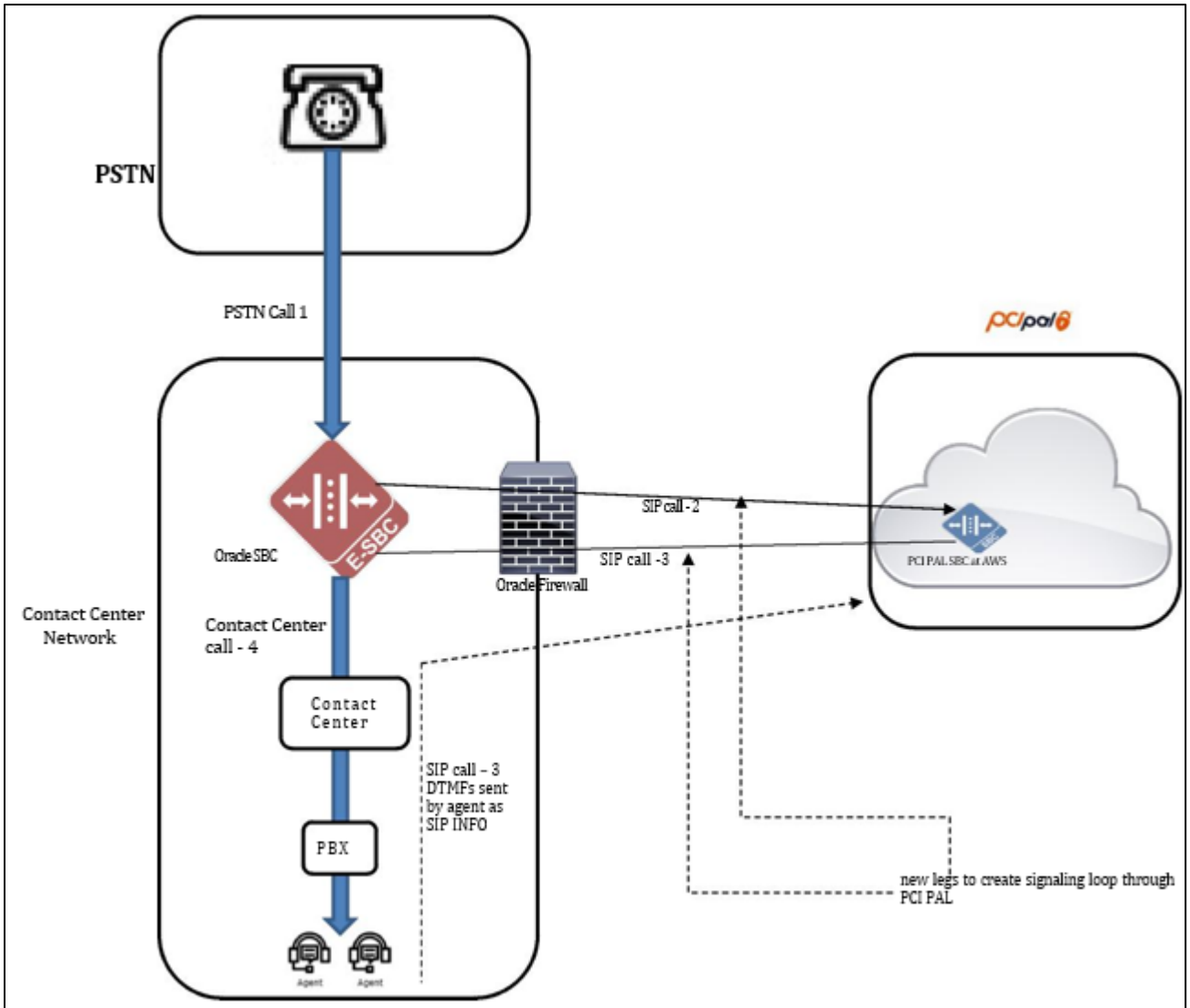


Figure 1. Normal Operation

8.2 Figure 2: During Payment

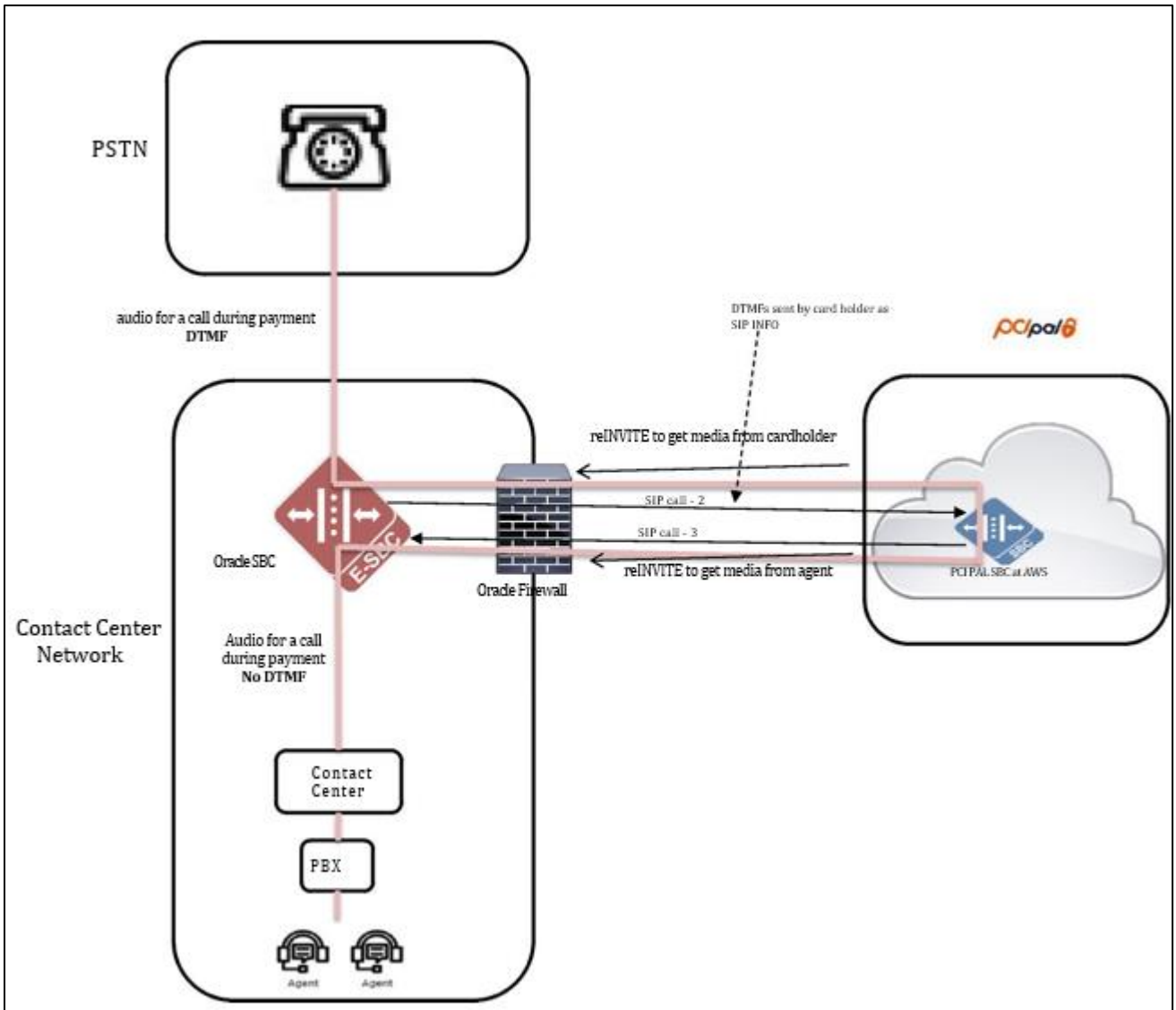


Figure 2. During Payment

9 Oracle SBC Configuration

This section provides step-by-step guidance on how to configure Oracle SBC for interworking with PCI-PAL There are two methods for configuring the OCSBC: ACLI or GUI.

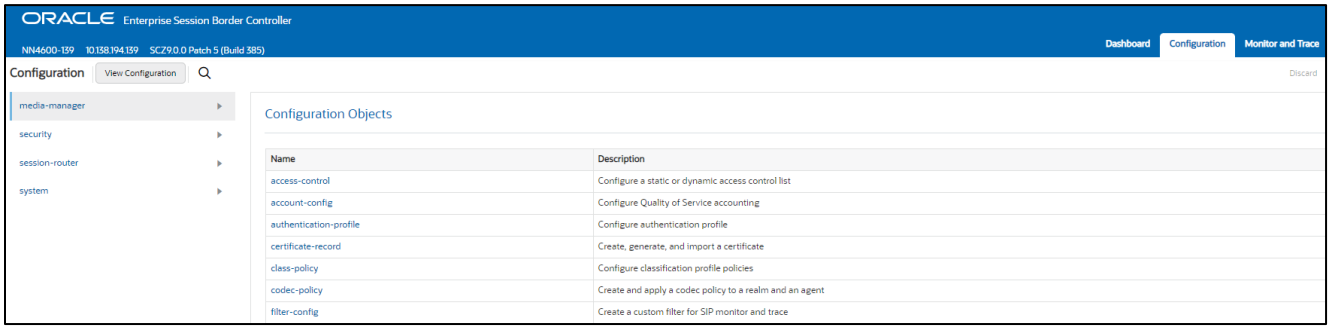
For the purposes of this app note, we'll be using the OCSBC GUI for all configuration examples. We will however provide the ACLI path to each element.

This guide assumes the OCSBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, web-server-config or http-server has been enabled for GUI access. If you require more information on how to install your SBC platform, please refer to the ACLI Configuration Guide.

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

Once you have accessed the OCSBC, at the top, click the Configuration Tab. This will bring up the OCSBC Configuration Objects List on the left-hand side of the screen.

Any configuration parameter not specifically listed below can remain at the OCSBC default value and does not require a change.



9.1.1 System-Config

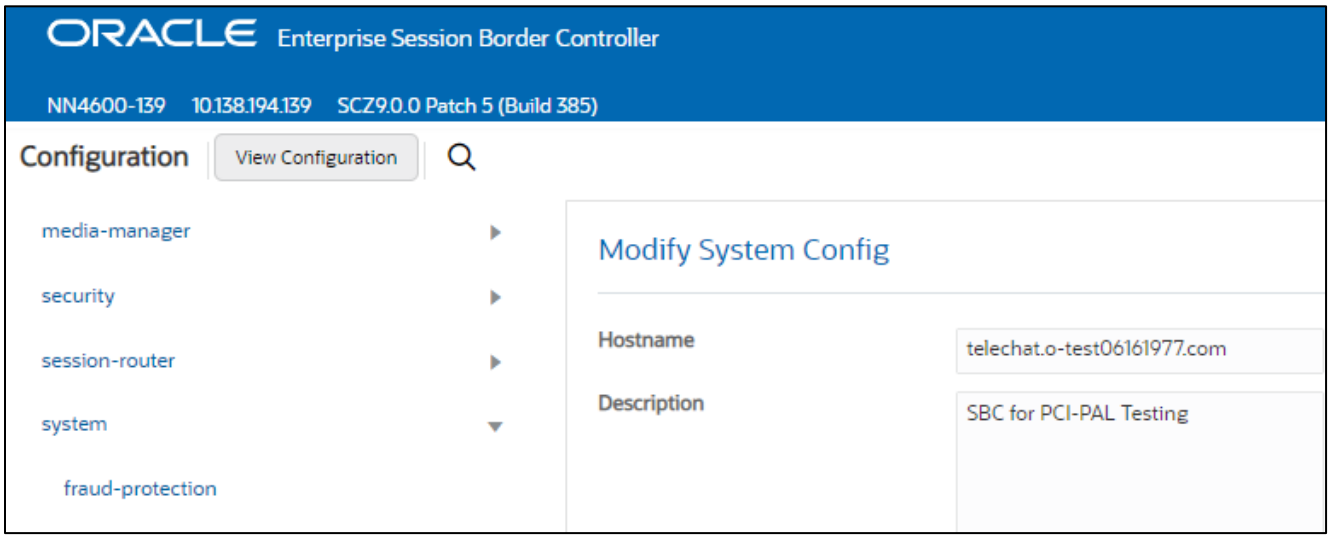
To configure system level functionality for the OCSBC, you must first enable the system-config

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



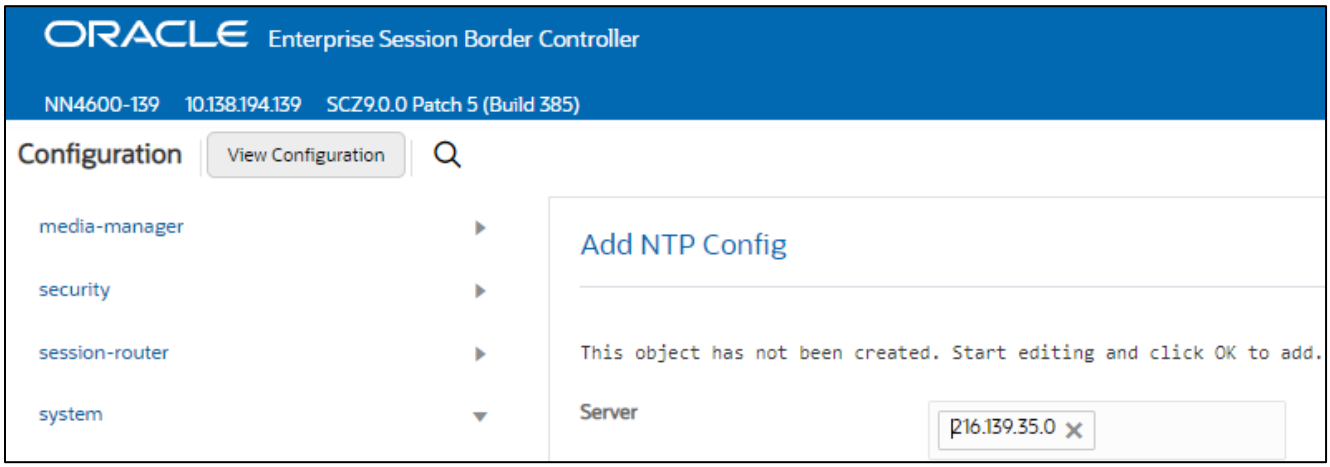
- Click the OK at the bottom of the screen

9.2 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



- Click OK at the bottom

9.3 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 three physical interfaces, and three network interfaces. One to communicate with Contact Center Platform, the others to connect to PSTN and PCI-PAL. The slots and ports used in this example may be different from your network setup.

9.3.1 Physical Interfaces

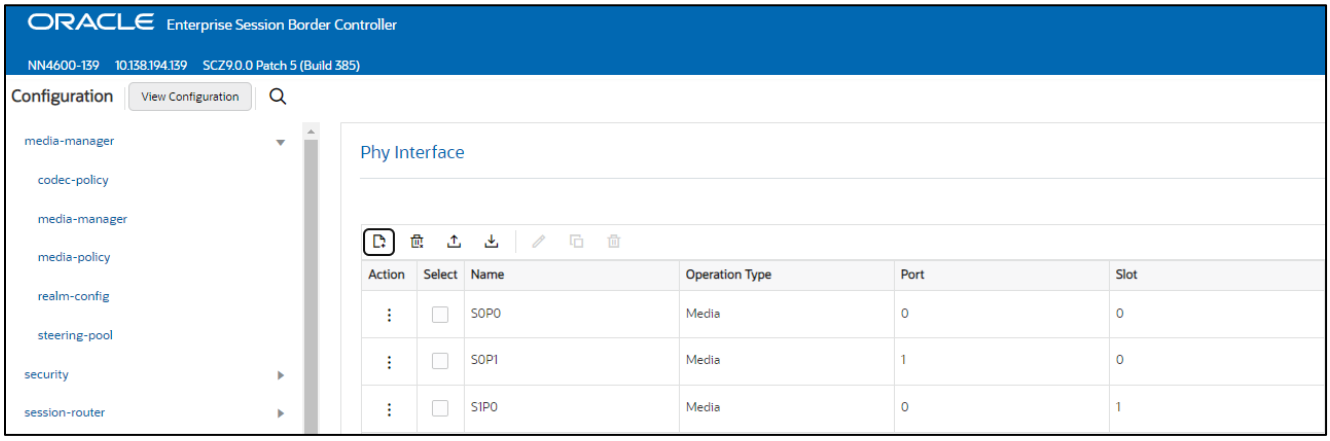
GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

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

Config Parameter	PSTN	Contact Centre	PCIPAL
Name	s0p0	S0p1	S1p0
Operation Type	Media	Media	
Slot	0	0	1
Port	0	1	0

Note: Physical interface names, slot and port may vary depending on environment



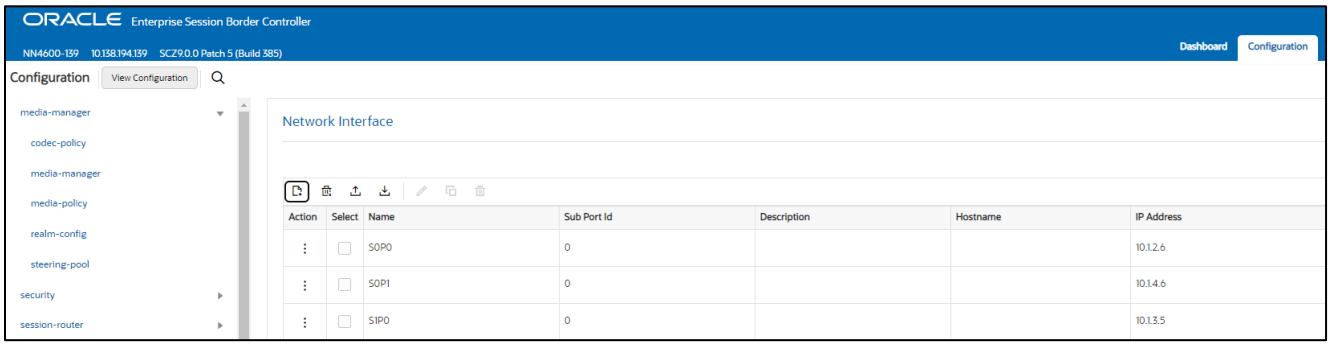
9.3.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

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

Configuration Parameter	PCIPAL	PSTN	Contact Centre
Name	s1p0	s0p0	s0p1
IP Address	10.1.3.4	10.1.2.4	10.1.4.4
Netmask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	10.1.3.1	10.1.2.1	10.1.4.1



- 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 PCIPAL.

9.4 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Contact Centre and PCI-PAL.

PCI-PAL allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by one of the trusted Certificate Authorities. Here is a list of PCI-PAL supported Certificate Authorities.

9.4.1 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

ACLI 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)
- DigiCertGlobalRoot (PCIPAL presents the SBC a certficate signed by this authority)

Note: The GoDaddy Root Cert 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.

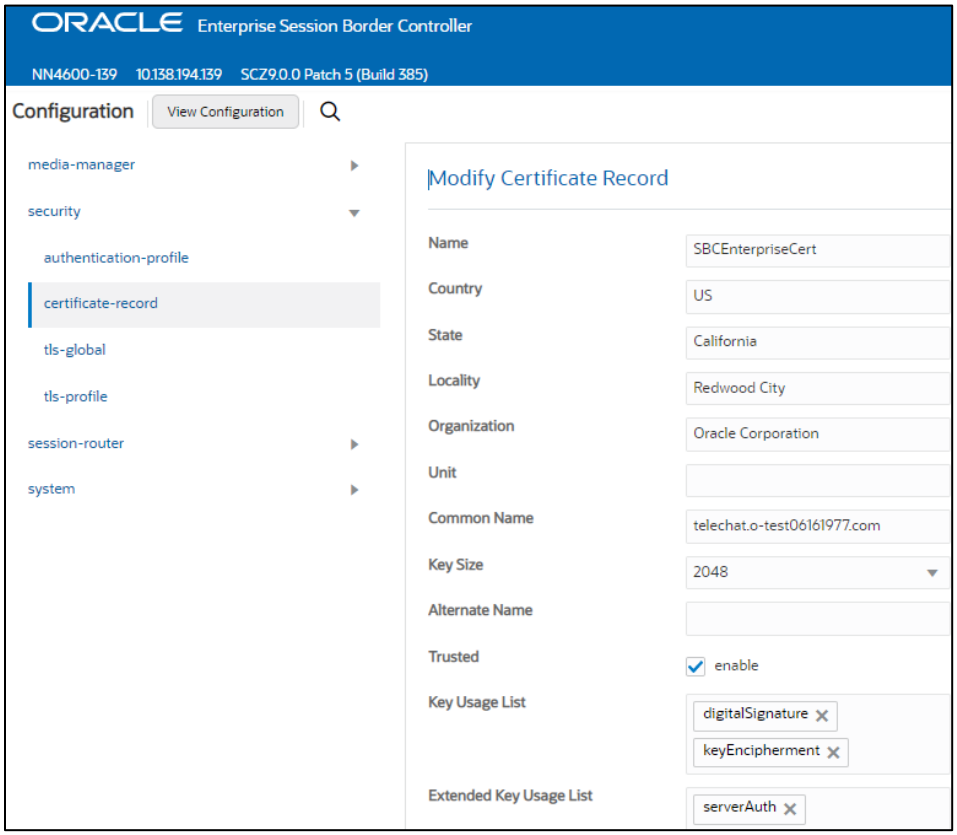
9.4.1.1 SBC End Entity Certificate

The SBC's end entity certificate is the certificate the SBC presents to PCI to secure the connection. The only requirements when configuring this certificate is the common name must contain the SBC's FQDN. In this

example our common name will be **telechat.o-test06161977.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



- Click OK at the bottom

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

9.4.1.2 Root CA and Intermediate Certificates

9.4.1.2.1 GoDaddy Root

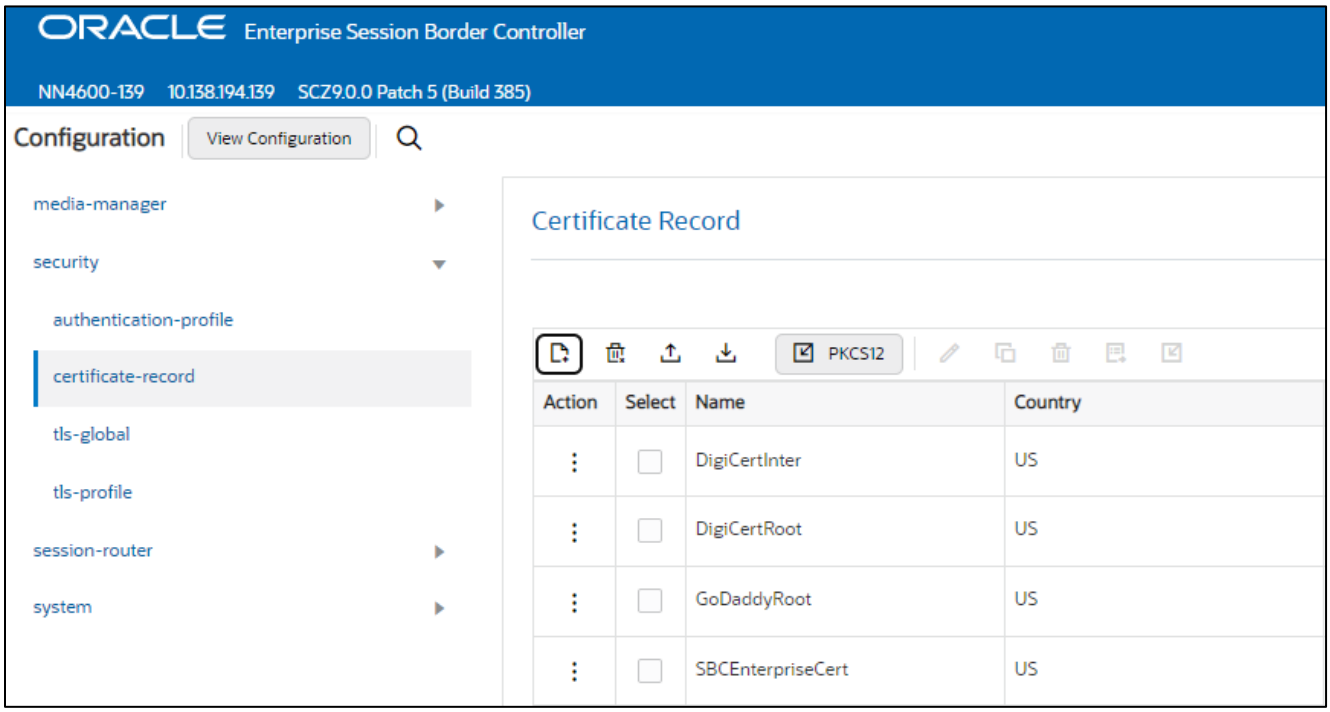
The following, GoDaddyRoot, is the root CA certificate used to sign the SBC's end entity certificate. As mentioned above, your root CA and/or intermediate certificate may differ. This is for example purposes only.

9.4.1.2.2 DigiCert Global Root and Intermediate Certificate

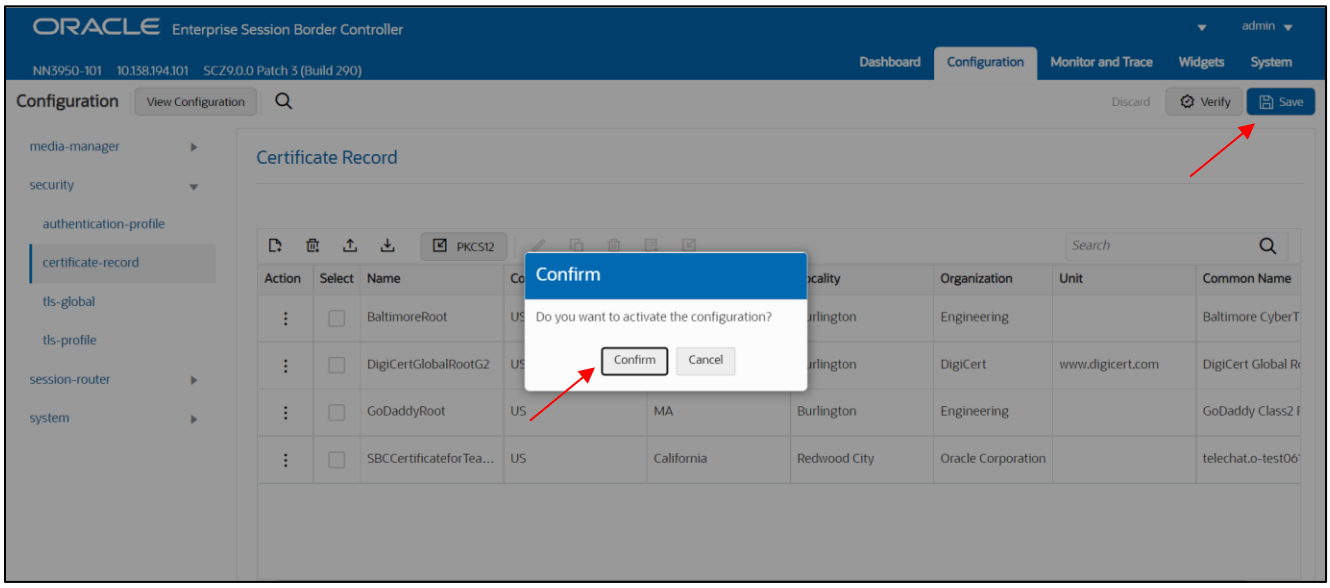
PCIPAL presents a certificate to the SBC which is signed by DigiCert Global Root and DigiCert Intermediate. To trust this certificate, your SBC must have the certificates listed as trusted ca certificates.

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

Config Parameter	DigiCertRoot	GoDaddy Root	DigiCert Intermediate
Common Name	DigiCert Global Root CA	Go Daddy Class2 Root CA	DigiCert SHA2 Secure Server CA
Key Size	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256



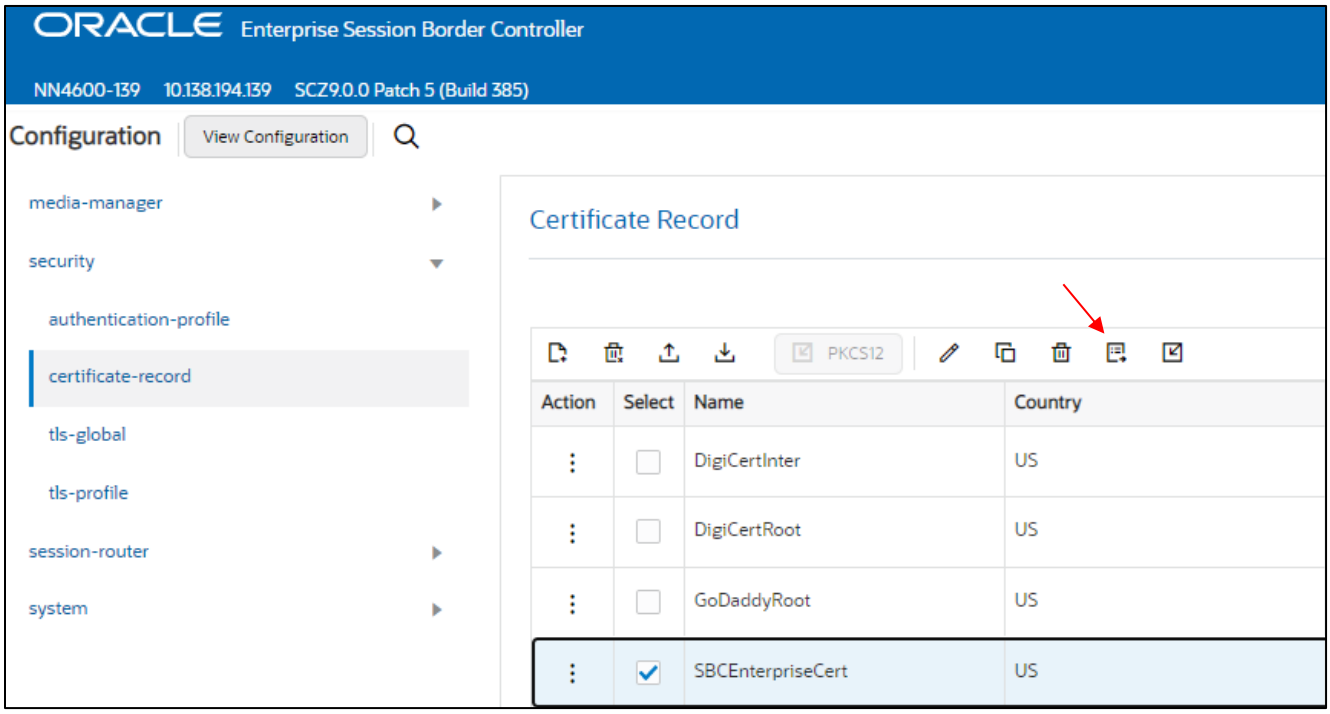
At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must **save and activate** the configuration of the SBC.

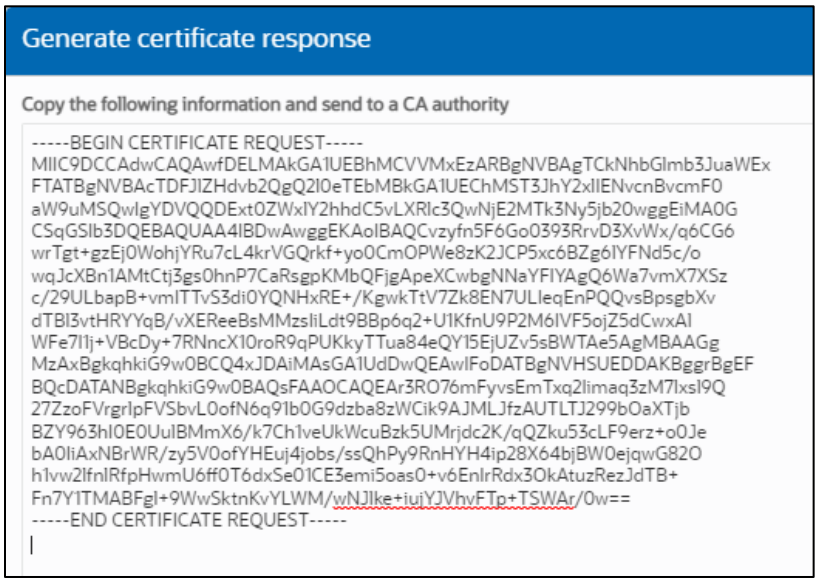


9.4.1.3 Generate Certificate Signing Request

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 intermidiate 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:





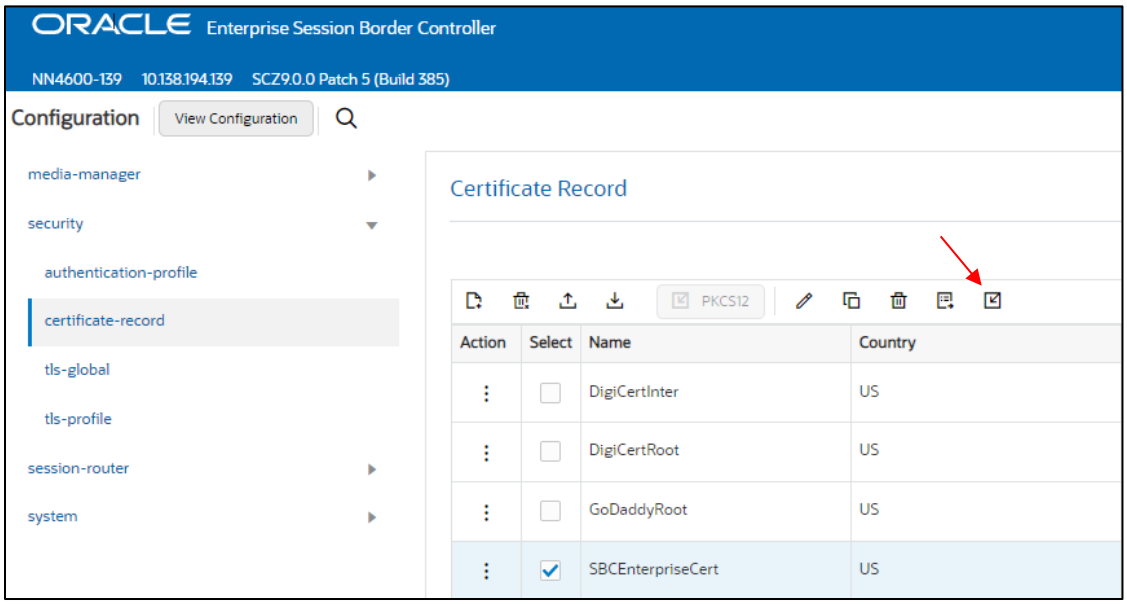
Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, at this point, **another save and activate is required** before you can import the certificates to each certificate record created above.

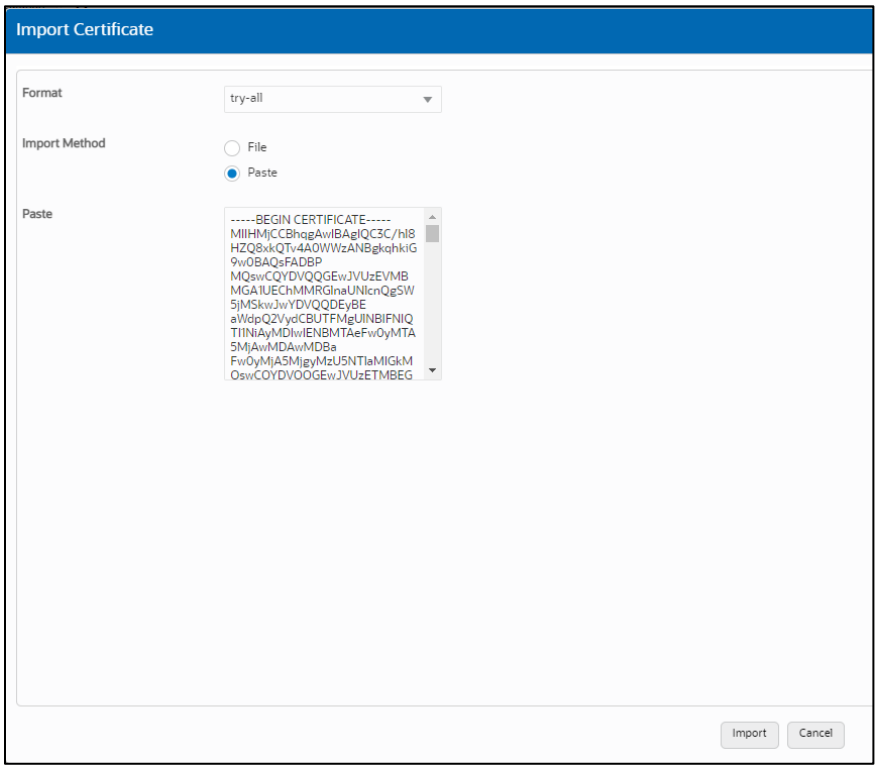
Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

9.4.1.4 Import Certificates to 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

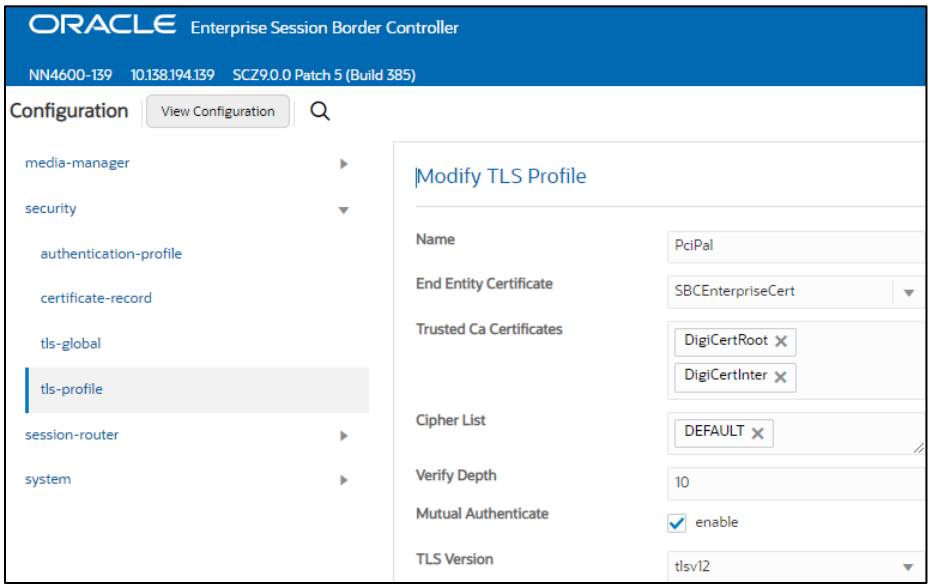
9.4.2 TLS Profile

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



- Click OK at the bottom

Next, we'll move to securing media between the SBC and PCIPAL.

9.4.3 Media Security

This section outlines how to configure support for media security between the OCSBC and Microsoft Teams Direct Routing.

9.4.3.1 SDES-Profile

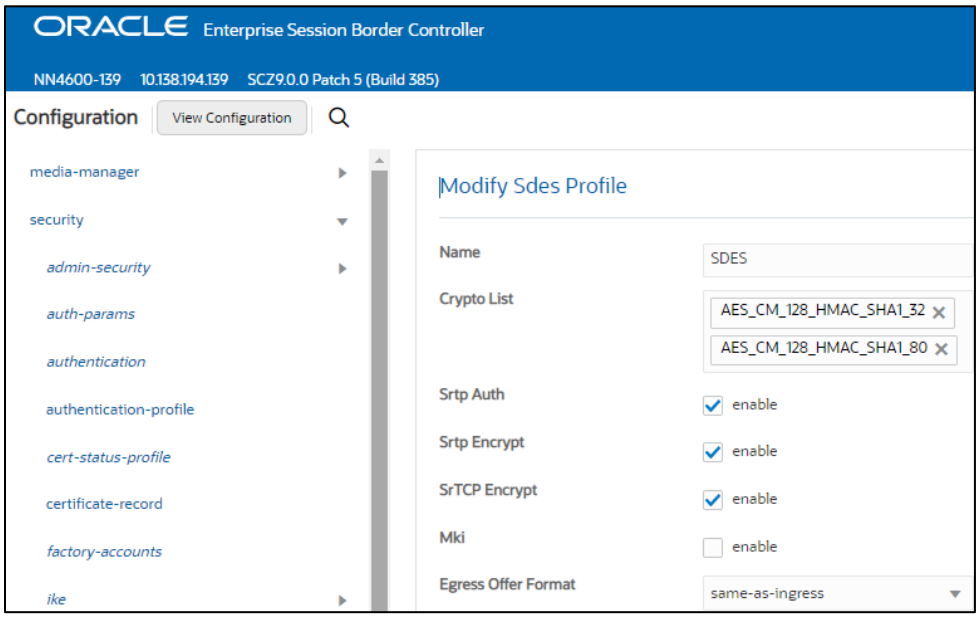
This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured.

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



- Select OK at the bottom

9.4.3.2 Media Security Policy

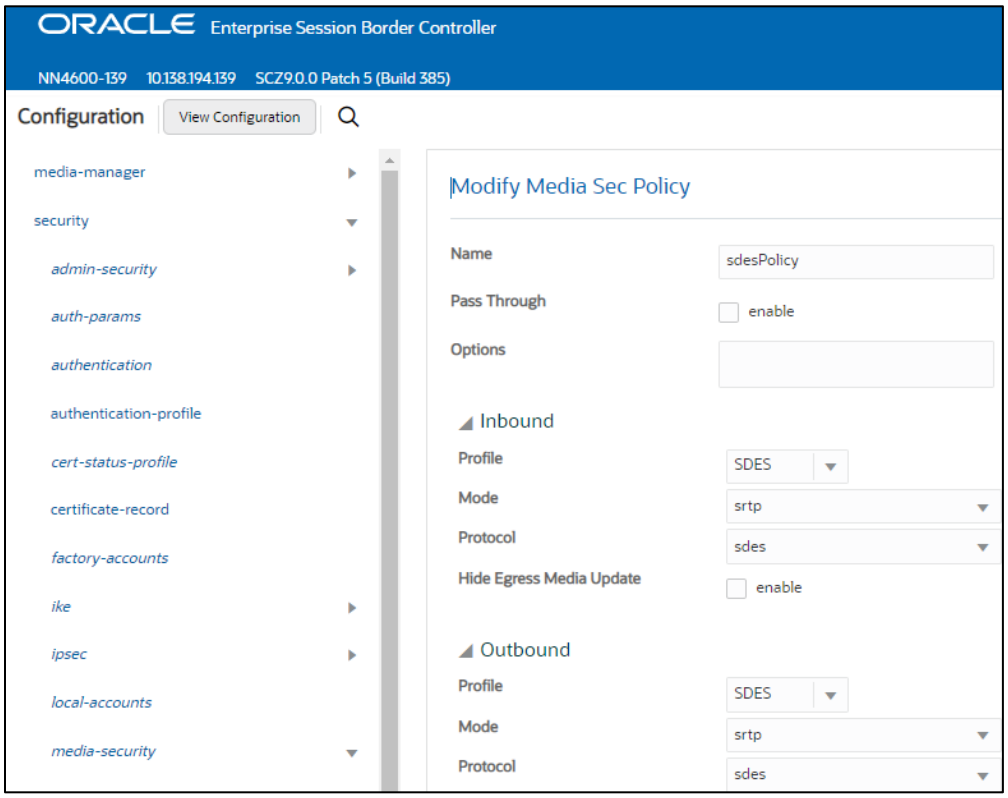
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any) and, if SRTP needs to be used, the sdes-profile that needs to be used

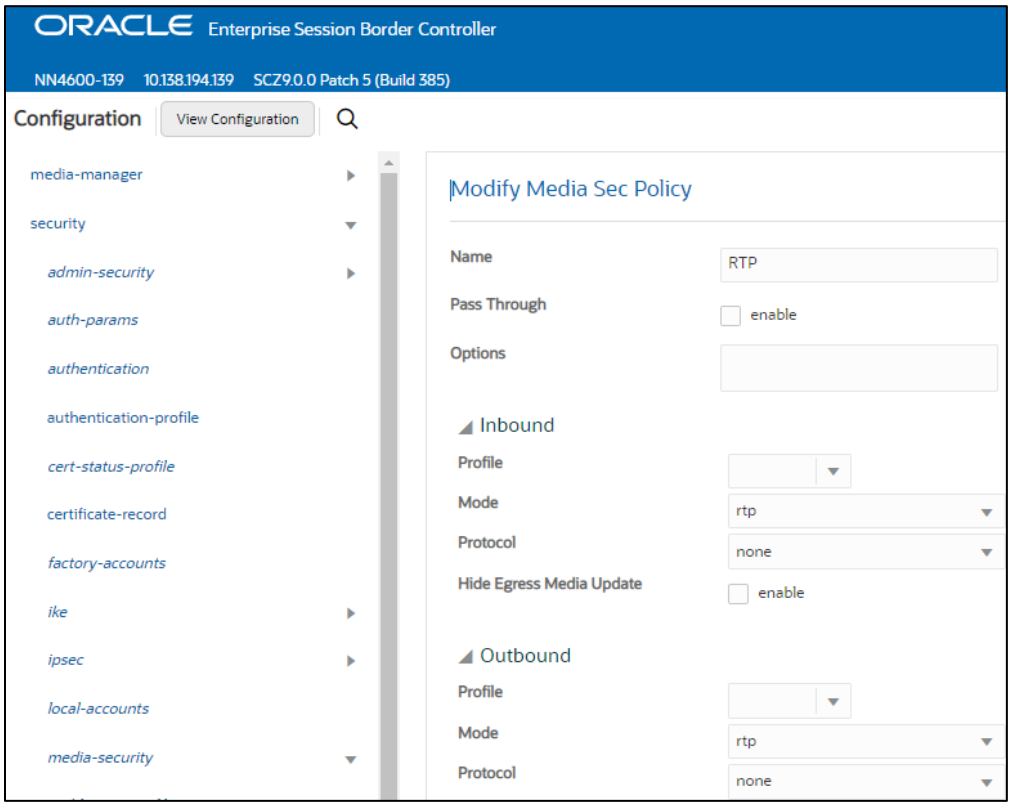
In this example, we are configuring two media security policies. One to secure and decrypt media toward PCIPAL, the other for non secure media facing PSTN and Contact Centre.

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

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

- Click Add, use the examples below to configure





- 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.

9.5 Media Configuration

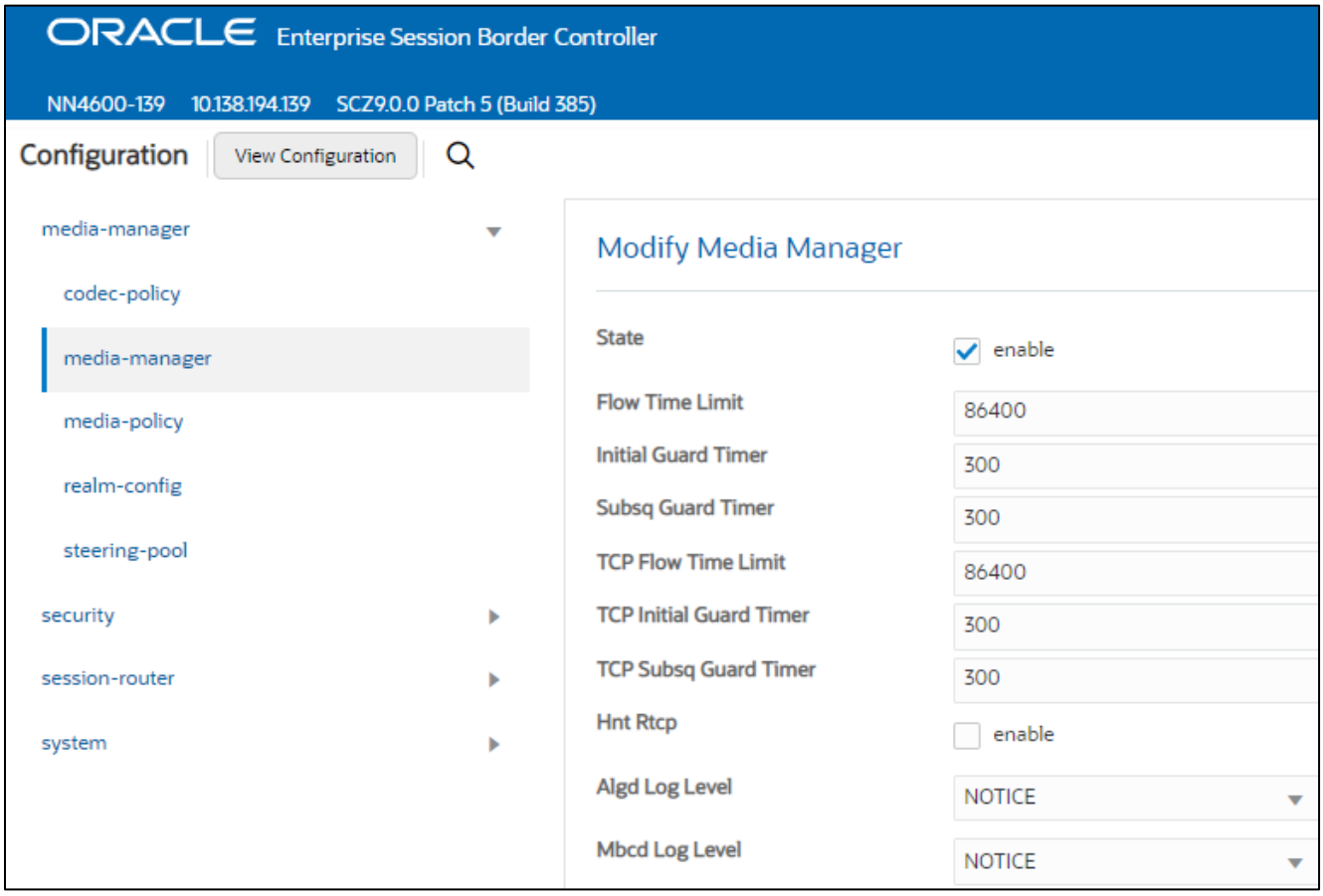
This section will guide you through the configuration of media manager, realms and steering pools, all of which are required for the SBC to handle signaling and media flows towards all agents and endpoints involved in call flows.

9.5.1 Media Manager

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

GUI Path: media-manager/media-manager

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



- Click OK at the bottom

9.5.2 Realm Config

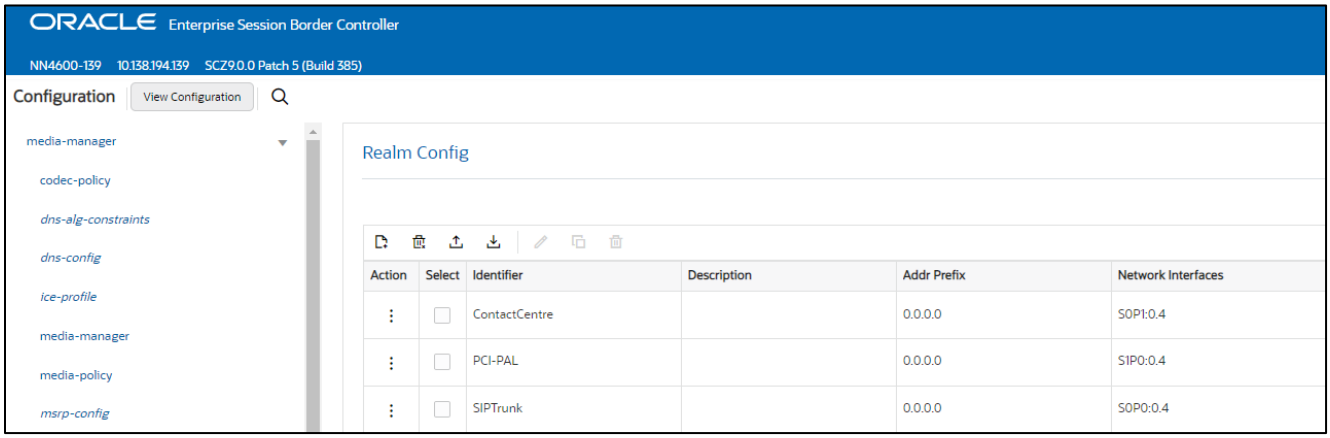
Realms are a logical distinction representing routes (or groups of routes) reachable by the Oracle® Session Border Controller and what kinds of resources and special functions apply to those routes. Realms are used as a basis for determining ingress and egress associations to network interfaces.
.
GUI 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	Contact Centre	PSTN Realm	PCIPAL
Identifier	ContactCentre	SipTrunk	PCIPAL
Network Interface	s0p1:0	s0p0:0	s1p0:0
Mm in realm	☑	☑	☑
Media Sec policy	RTP	RTP	sdesPolicy
Access-control-trust-level	HIGH	HIGH	HIGH

Notice the realm configuration is where we assign both the Network Interface and Media Security Policy configured earlier in this document.



- Click OK at the bottom to continue

9.5.3 Steering Pools

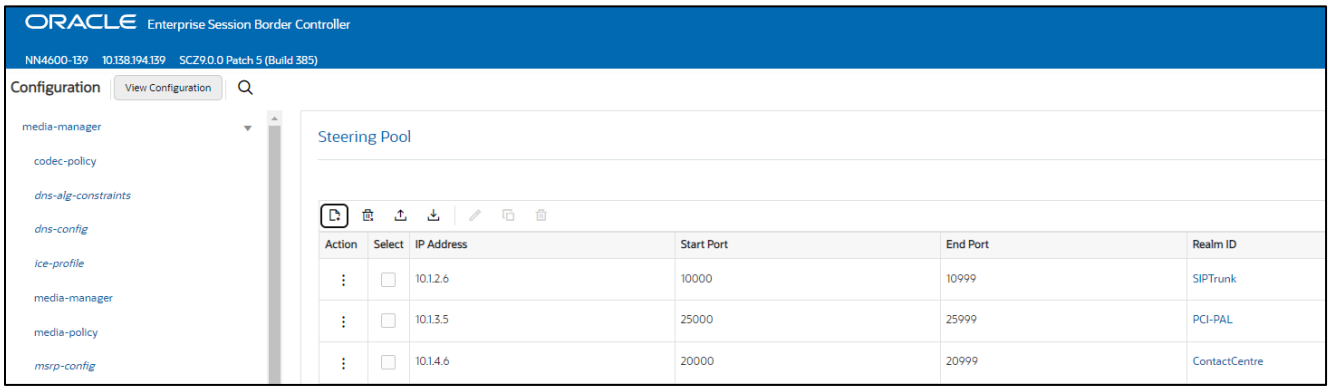
Steering pools define sets of ports that are used for steering media flows through the OCSBC.
These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We configure one steering pool for each Realm configured above

GUI Path: media-manger/steering-pool

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

- Click Add, and use the below example to configure



- Click OK at the bottom of each

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

9.6 Sip Configuration

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

9.6.1 Sip Config

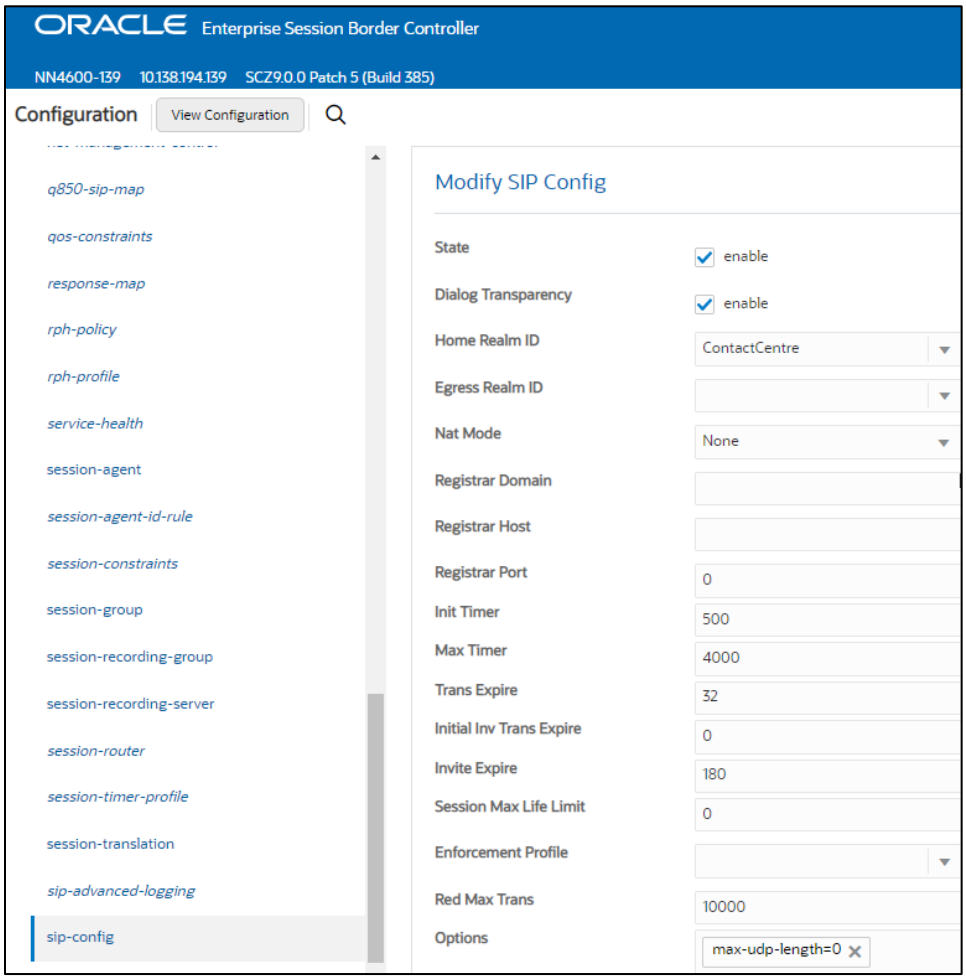
To enable sip related objects on the Oracle SBC, you must first configure the global Sip Config element:

GUI Path: session-router/sip-config

ACLI 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 ContactCentre,
  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).



- Click OK at the bottom

9.6.2 Sip Interface

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

Configure three sip interfaces, one for each realm configured previously in the document.

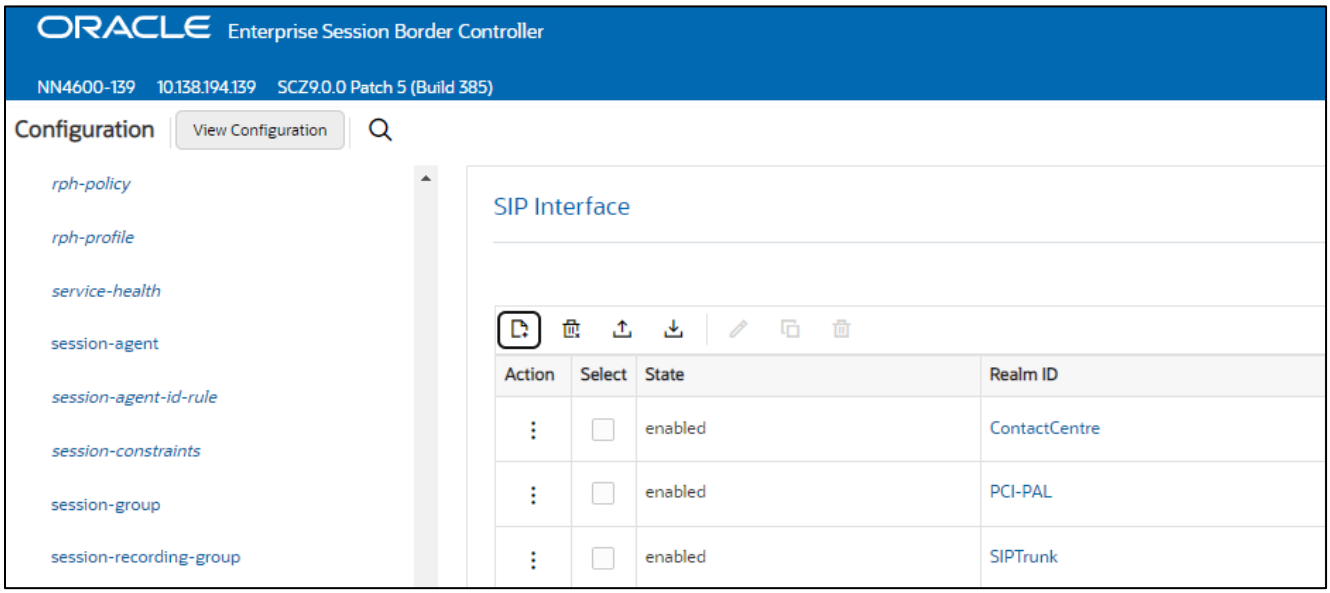
GUI Path: session-router/sip-interface

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

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

Note: For payment processing to work correctly, the RFC 2833 Mode on PCI-PAL Sip Interface must be set to dual.

Config Parameter	Contact Centre	PSTN	PCIPAL
Realm ID	ContactCentre	SIPTrunk	PCI-PAL
Rfc2833 payload	101	101	101
Rfc2833 mode	transparent	transparent	dual
Sip Port Config Parameter	**ContactCentre**	**SIPTrunk**	
Address	10.1.4.6	10.1.2.6	10.1.3.5
Port	5060	5060	5061
Transport protocol	UDP	UDP	TLS
TLS profile			PciPal
Allow anonymous	agents-only	agents-only	agents-only



- Select OK at the bottom of each when applicable

9.6.3 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.

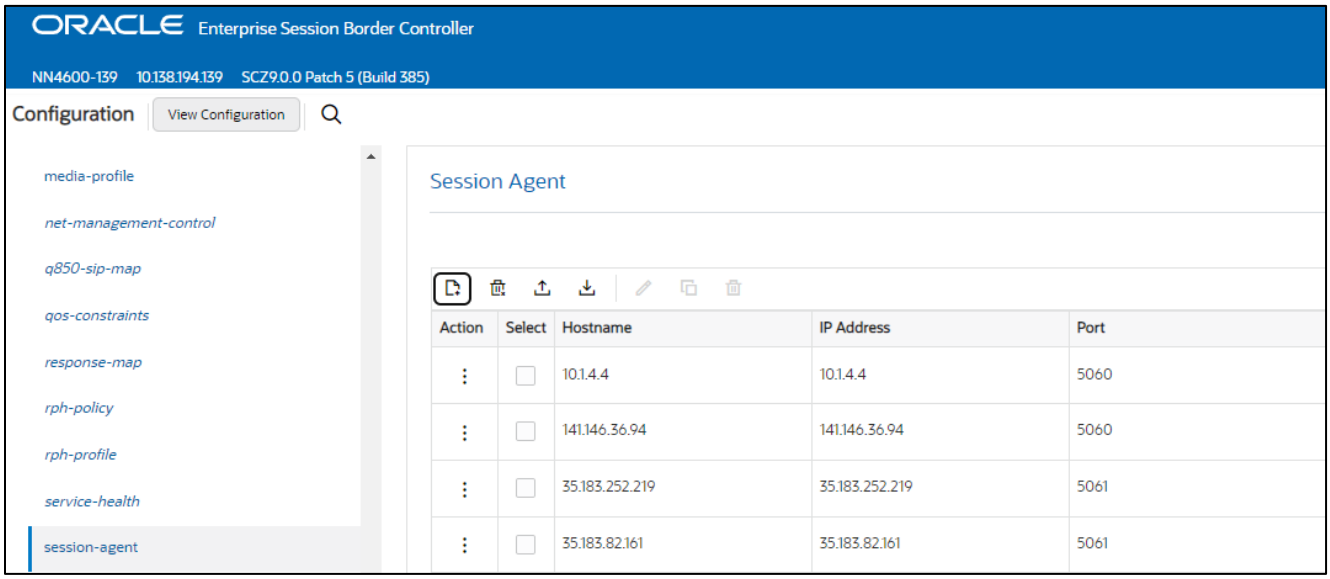
GUI Path: session-router/session-agent

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

For the purposes of this example, we'll configure four session agents. Two for PCIPAL, one for PSTN, and one for our Contact Centre.

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

Config parameter	Session Agent 1	Session Agent 2	Session Agent 3	Session Agent 4
Hostname	10.1.4.4	141.146.36.94	35.183.252.219	35.183.82.161
IP Address	10.1.4.4	141.146.36.94	35.183.252.219	35.183.82.161
Port	5060	5060	5061	5061
Transport method	UDP	UDP	StaticTLS	Static TLS
Realm ID	ContactCentre	SIPTrunk	PCI-PAL	PCI-PAL
Ping Method	OPTIONS	OPTIONS	OPTIONS	OPTIONS
Ping Interval	30	30	30	30
Refer Call Transfer	enabled	enabled	enabled	enabled
Ping Response	☑	☑	☑	☑



- Select OK at the bottom of each when applicable

9.6.4 Session Group

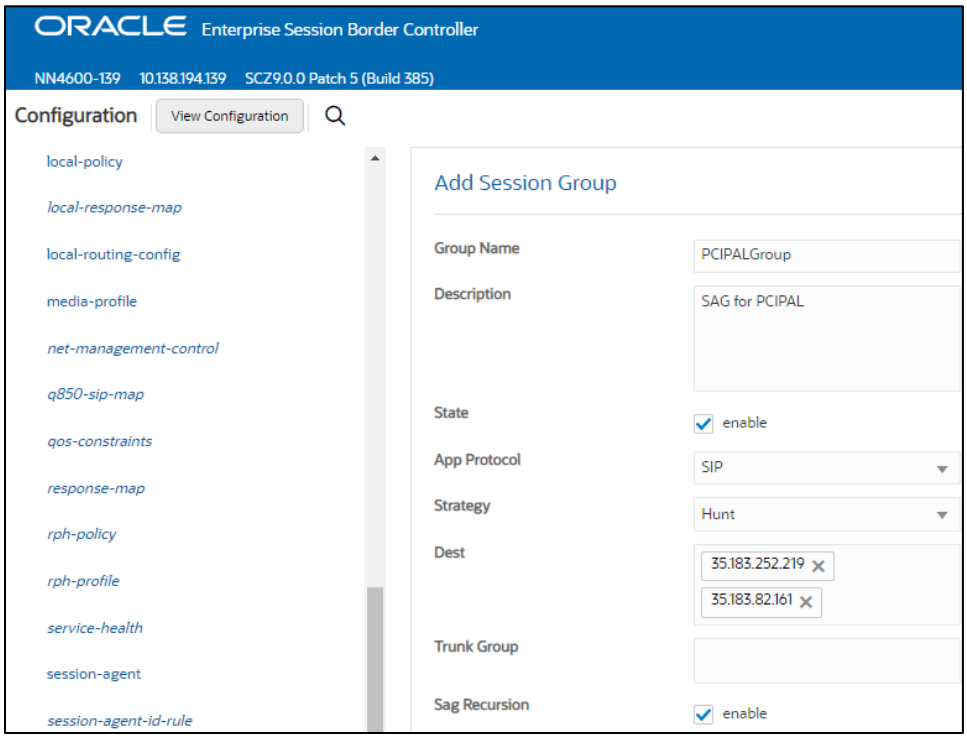
A session agent group allows the SBC to create a load balancing model:

Both PCIPAL session agents configured above will be added to the group. The session agents listed under destination must be in this order, and the strategy must be set to HUNT.

GUI Path: session-router/session-group

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

- Click Add, and use the following as an example to configure:



9.7 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 to and from PCIPAL, SIPTrunk, and Contact Centre.

GUI Path: session-router/local-policy

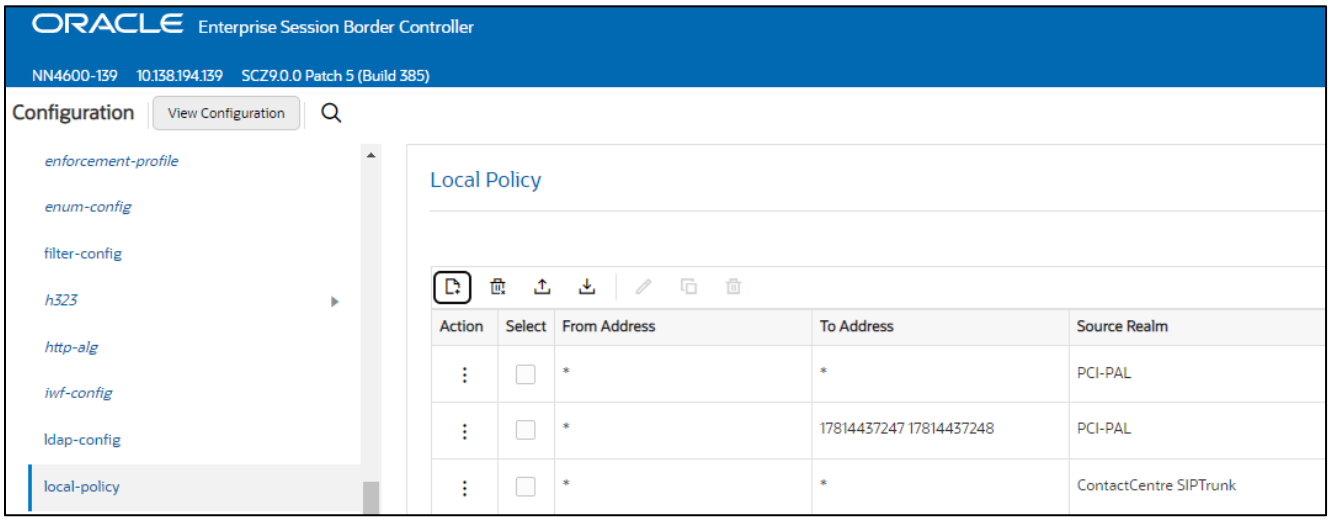
ACLI Path: config t→session-router→local-policy

We'll create three local policies for the purposes of this example.

1. Routes all calls from both SIPTrunk and ContactCentre to PCI-PAL Session Group.
2. Routes traffic from PCI-PAL to SIP Trunk
3. Routes calls matching the to-address of local policy (RURI) to Contact Centre

Use the table below as an example to configure local policy routing in your environment

Config Parameter	Policy 1	Policy 2	Policy 3
Source Realm	ContactCentre SipTrunk	PCI-PAL	PCI-PAL
From Address	*	*	*
To Address	*	*	17814437247 17814437248
Policy Attribute Config			
Next Hop	Sag:PCIPALGroup	10.1.2.6	10.1.4.4
Realm ID	PCI-PAL	SIPTrunk	ContactCentre
action	replace-uri	replace-uri	replace-uri



- Click OK at the bottom of each when applicable.

Save and activate your configuration.

This concludes the configuration of the SBC to interwork with PCIPAL.

10 Appendix A

10.1 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 the 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 PCIPAL side SIP interface.

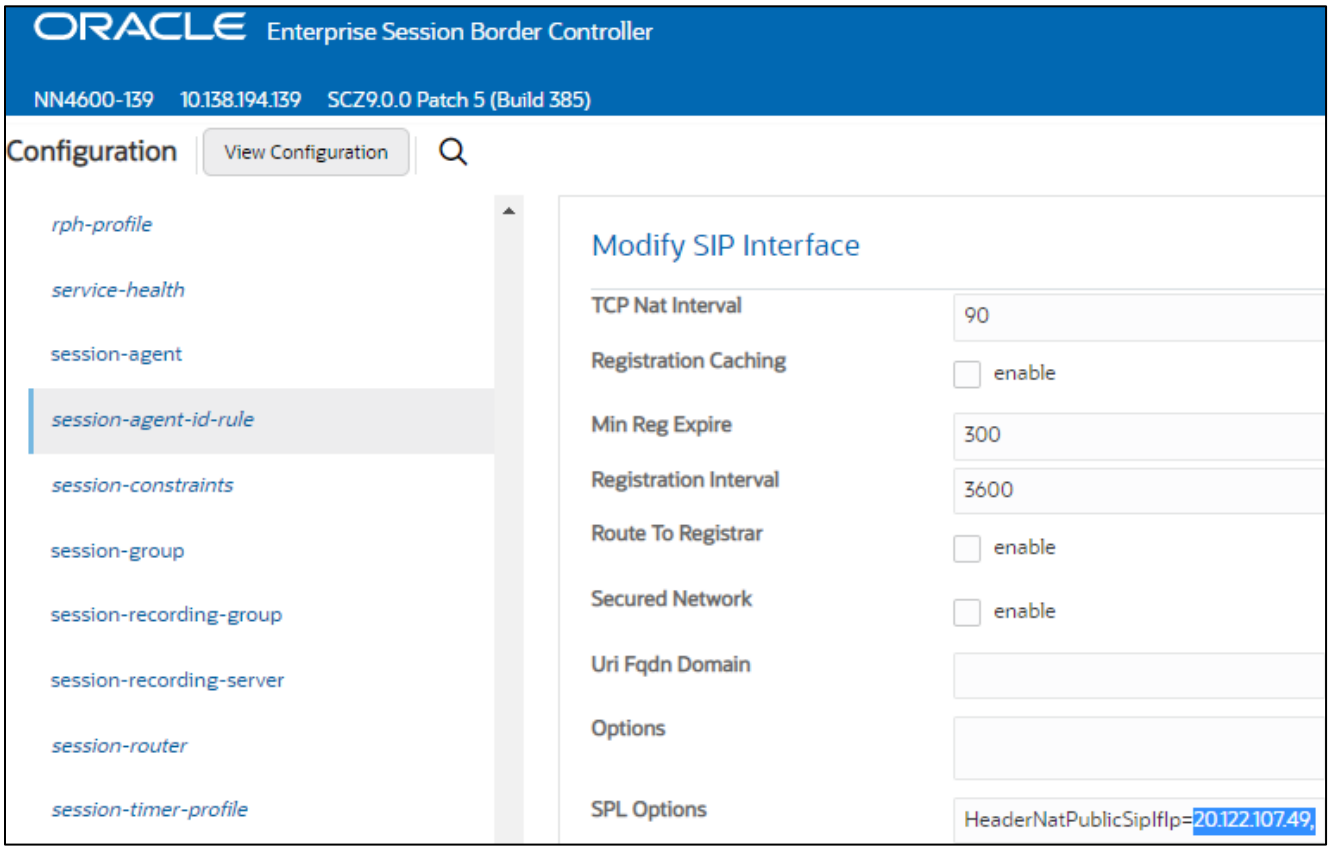
GUI Path: session-router/sip-interface

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

HeaderNatPublicSipIfIp= 20.122.107.49,HeaderNatPrivateSipIfIp=10.1.3.5

HeaderNatPublicSipIfIp is the public interface ip

HeaderNatPrivateSipIfIp is the private ip.



As mentioned above, you will need to apply these options to every sip interface on the SBC that is connected through a NAT.

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