Configuring the Oracle SBC with Microsoft Azure Communication Services

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

1 Related Documentation

1.1 Oracle SBC

- Oracle® Enterprise Session Border Controller Configuration Guide
- Oracle® Enterprise Session Border Controller Release Notes
- Oracle® Enterprise Session Border Controller Security Guide
- Oracle® Enterprise Session Border Controller Web Gui User's Guide

1.2 Microsoft Azure Communication Services

- Direct Routing Telephony Concepts
- Azure Direct Routing Infrastructure Requirements
- Session Border Controllers and Voice Routing
- Azure Communication Services Overview
- Quickstart: Create and Manage Communication Services resources
- Quickstart: Build your own App
- Get Started with Web Calling Sample

2 Revision History

Version	Date Revised	Description of Changes
1.0	9/16/2021	Initial Release

3 Intended Audience

This document describes how to connect the Oracle SBC to Microsoft Azure Communication Services. This paper is intended for IT or telephony professionals.

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

4 Validated Oracle Versions

Microsoft has successfully conducted testing with the Oracle Communications SBC version:

SCZ840

This software release with the configuration outlined in this application note can run on any of the following products:

- AP 1100
- AP 3900
- AP 3950
- AP 4600
- AP 4900
- AP 6350
- AP 6300
- VME

5 About Azure Communication Services

Azure Communication Services allows you to easily add real-time voice, video, and telephone communication to your applications. Communication Services SDKs also allow you to add SMS functionality to your communications solutions. Azure Communication Services is identity agnostic; you have complete control over how end users are identified and authenticated. You can connect people to the communication data plane or services (bots).

Applications include:

- Business to Consumer (B2C). Business employees and services can interact with consumers using voice, video, and rich text chat in a custom browser or mobile application. An organization can send and receive SMS messages, or operate an interactive voice response system (IVR) using a phone number acquired through Azure. Integration with Microsoft Teams allows consumers to join Teams meetings hosted by employees; ideal for remote healthcare, banking, and product support scenarios where employees might already be familiar with Teams.

- Consumer to Consumer. Build engaging social spaces for consumer-to-consumer interaction with voice, video, and rich text chat. Any type of user interface can be built on Azure Communication Services SDKs. Complete application samples and UI assets are available to help you get started quickly.

5.1 Infrastructure Requirements

The table below shows the list of infrastructure prerequisites for deploying Direct Routing.

Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	**See Microsoft's Plan Direct Routing document**
SIP Trunks connected to the SBC	
Azure Subscription	
Communication Services Access Token	
Public IP address for the SBC	
Fully Qualified Domain Name (FQDN) for the SBC	
Public DNS entry for the SBC	
Public trusted certificate for the SBC	
Firewall IP addresses and ports for SIP Signaling and media	

5.2 SBC Domain Names

Customers without Office 365 can use any domain name for which they can obtain a public certificate.

The following table shows examples of DNS names registered for the tenant, whether the name can be used as an FQDN for the SBC, and examples of valid FQDN names:

DNS name	Can be used for SBC FQDN	Examples of FQDN names
contoso.com	Yes	**Valid names:** sbc1.contoso.com ssbcs15.contoso.com europe.contoso.com
contoso.onmicrosoft.com	No	Using *.onmicrosoft.com domains is not supported for SBC names

If you are an Office 365 customer, then the SBC domain name must not match registered in Domains of the Office 365 tenant. Below is the example of Office 365 and Azure Communication Service coexistence:

Domain registered in Office 365	Examples of SBC FQDN in Teams	Examples of SBC FQDN names in ACS
contoso.com (second level domain)	**sbc.contoso.com** (name in the second level domain)	**sbc.acs.contoso.com** (name in the third level domain) **sbc.fabrikam.com** (any name within different domain)
o365.contoso.com (third level domain)	**sbc.o365.contoso.com** (name in the third level domain)	**sbc.contoso.com** (name in the second level domain) **sbc.acs.o365.contoso.com** (name in the fourth level domain) **sbc.fabrikam.com** (any name within different domain)

SBC pairing works on an ACS resource level, meaning you can pair many SBCs to a single ACS resource, but you cannot pair a single SBC to more than one ACS resource.
Unique SBC FQDNs are required for pairing to different resources.

5.3 Public trusted certificate for the SBC

Microsoft recommends that you request the certificate for the SBC by generating a certification signing request (CSR). Instructions on generating a CSR for an Oracle SBC are provided in the Configuration section of this application note.

NOTE: Most Certificate Authorities (CAs) require the private key size to be at least 2048. Keep this in mind when generating the CSR.
The certificate needs to have the SBC FQDN as the common name (CN) or the subject alternative name (SAN) field. The certificate should be issued directly from a certification authority, not from an intermediate provider.

Alternatively, ACS SIP Interface supports a wildcard in the CN and/or SAN, and the wildcard needs to conform to standard RFC HTTP Over TLS. An example would be using *.contoso.com which would match the SBC FQDN sbc.contoso.com, but wouldn't match with sbc.test.contoso.com.

The certificate needs to be generated by one of the following root certificate authorities:

- AffirmTrust
- AddTrust External CA Root
- Baltimore CyberTrust Root*
- Buypass
- Cybertrust
- Class 3 Public Primary Certification Authority
- Comodo Secure Root CA
- Deutsche Telekom
- DigiCert Global Root CA
- DigiCert High Assurance EV Root CA
- Entrust

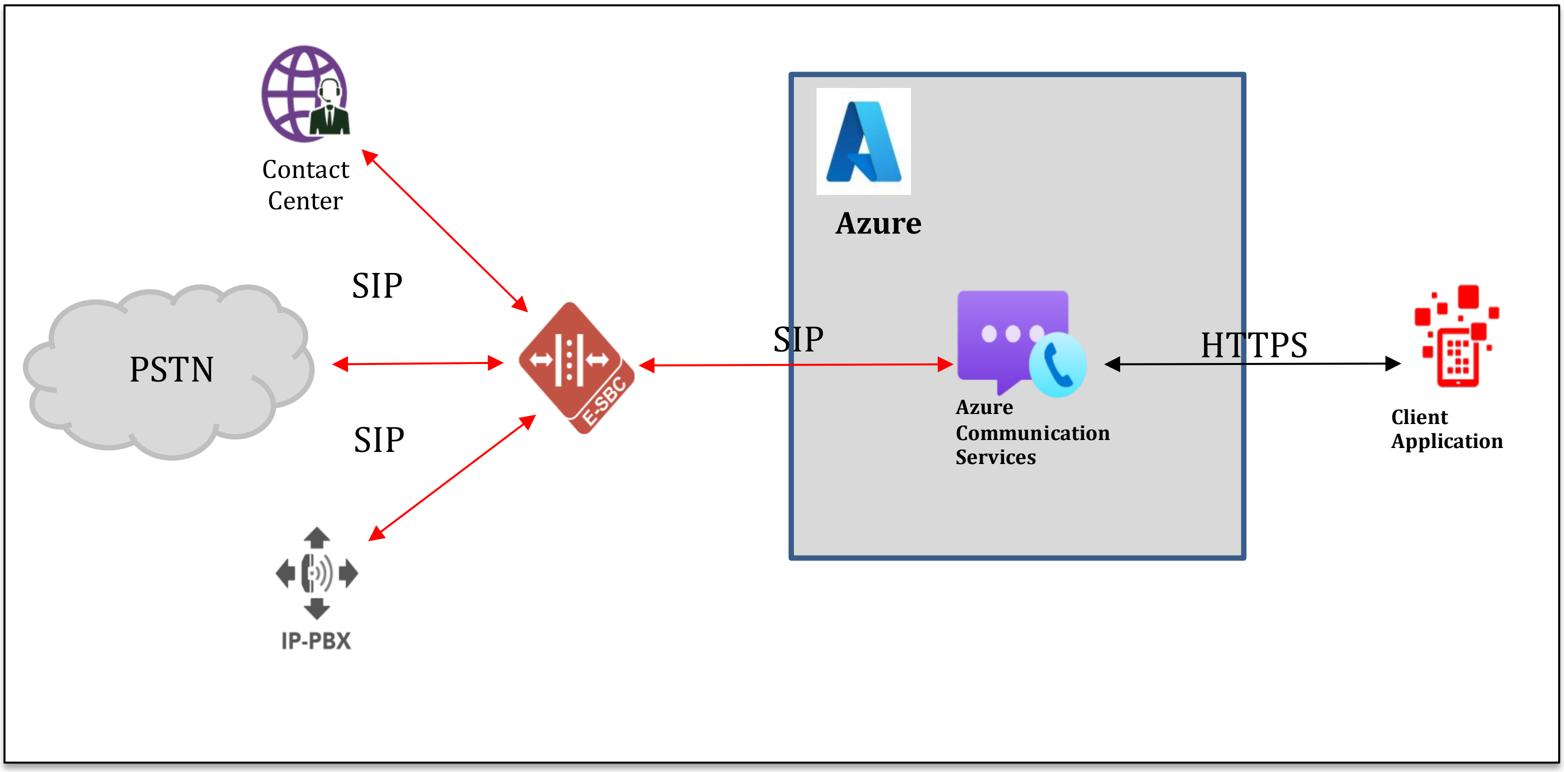
- GlobalSign
- Go Daddy
- GeoTrust
- Verisign, Inc.
- SSL.com
- Starfield
- Symantec Enterprise Mobile Root for Microsoft
- SwissSign
- Thawte Timestamping CA
- Trustwave
- TeliaSonera
- T-Systems International GmbH (Deutsche Telekom)
- QuoVadis

Microsoft is working on adding additional certification authorities based on customer requests.

6 Configuration

This chapter provides step by step guidance on how to configure the Oracle SBC for interworking with Microsoft Azure Communication Services.

Below shows the connection topology example for MSFT Azure Communication Services.



These instructions cover configuration steps between the Oracle SBC and Microsoft Azure Communications Services. The interconnection of other entities, such as connection of the SIP trunk, 3rd Party PBX and/or analog devices are not covered in this instruction. The details of such connection are available in other instructions produced by the vendors of retrospective components.

7 Azure Communication Services Direct Routing

Azure Communication Services supports a “SIP-Interface” option that allows you to connect, through Oracle’s certified session border controller, your legacy on-premises telephony and your carrier of choice to ACS. It provides PSTN calling capabilities to your ACS applications even if Azure Cloud Calling is not available in your country/region.

With this option:

- You connect your own supported Oracle SBC to Azure Communication Services without the need for additional on-premises software.
- You can use literally any telephony carrier with ACS.

- You can configure interoperability between your telephony equipment—such as a third-party PBX and analog devices—and ACS.

The cloud deployment and setup of Azure Communication Services is outside the scope of this document.

Please see Related Documentation for more information on the setup and configuration of Azure Communication Services

8 Oracle SBC Configuration

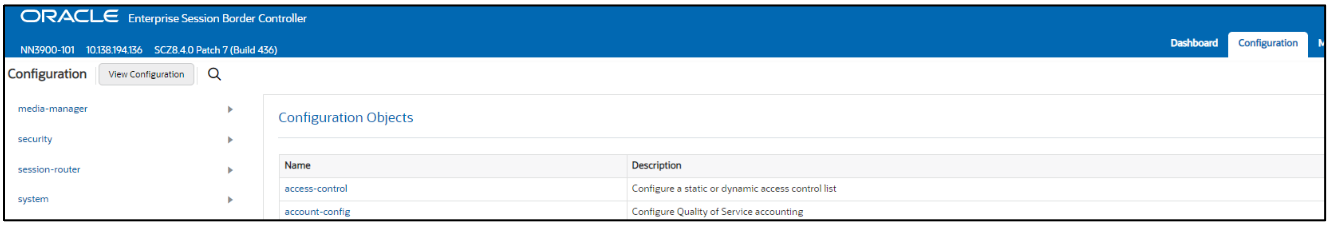
There are two methods for configuring the OCSBC, ACLI, or GUI.

For the purposes of this 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, 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 screen.



Name	Description
access-control	Configure a static or dynamic access control list
account-config	Configure Quality of Service accounting

Any configuration parameter not specifically listed below can remain at the OCSBC default value and does not require a change for connection to MSFT Teams Direct routing to function properly. Also, all FQDN, IP Address, SBC TLS certificates, or other network information outlined in this configuration example is only usable within the Oracle LAB, and cannot be added to any other configuration or SBC outside of that lab environment. This is for example purposes only.

8.1 Global Configuration Elements

Before you can configuration more granular parameters on the SBC, there are four global configuration elements that must be enabled to proceed.

- System-Config
- Ntp-config
- Media-manager-Config
- Sip-Config

8.1.1 System-Config

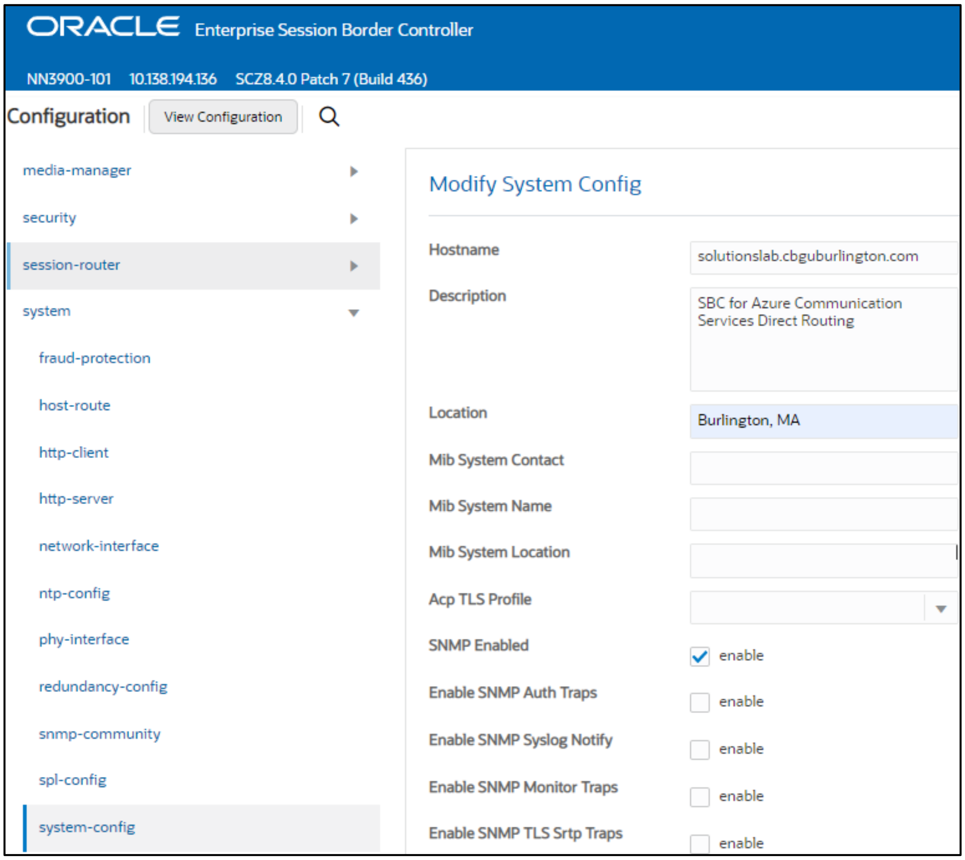
To configure system level functionality for the OCSBC, you must first enable the system-config

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



Modify System Config

Hostname	solutionslab.cbguburlington.com
Description	SBC for Azure Communication Services Direct Routing
Location	Burlington, MA
Mib System Contact	
Mib System Name	
Mib System Location	
Acp TLS Profile	
SNMP Enabled	☑ enable
Enable SNMP Auth Traps	□ enable
Enable SNMP Syslog Notify	□ enable
Enable SNMP Monitor Traps	□ enable
Enable SNMP TLS Srtp Traps	□ enable

- Click OK at the bottom of the screen

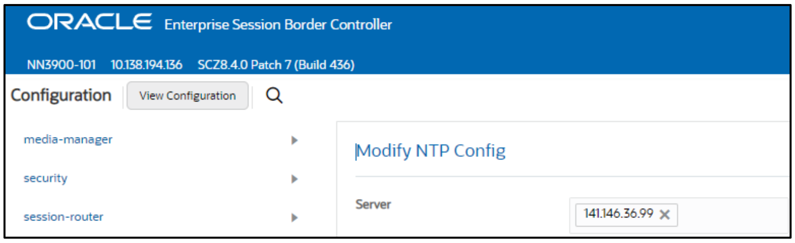
8.1.2 NTP Config

To enable NTP on the SBC:

GUI Path: system/ntp-config

ACLI Path: config t→system→ntp-config

- Add the IP address in the box for server


ORACLE Enterprise Session Border Controller
NN3900-101 10.138.194.136 SCZ8.4.0 Patch 7 (Build 436)
Configuration
View Configuration
media-manager
security
session-router

Modify NTP Config

Server: 141.146.36.99

- Click OK at the bottom

8.1.3 Media Manager

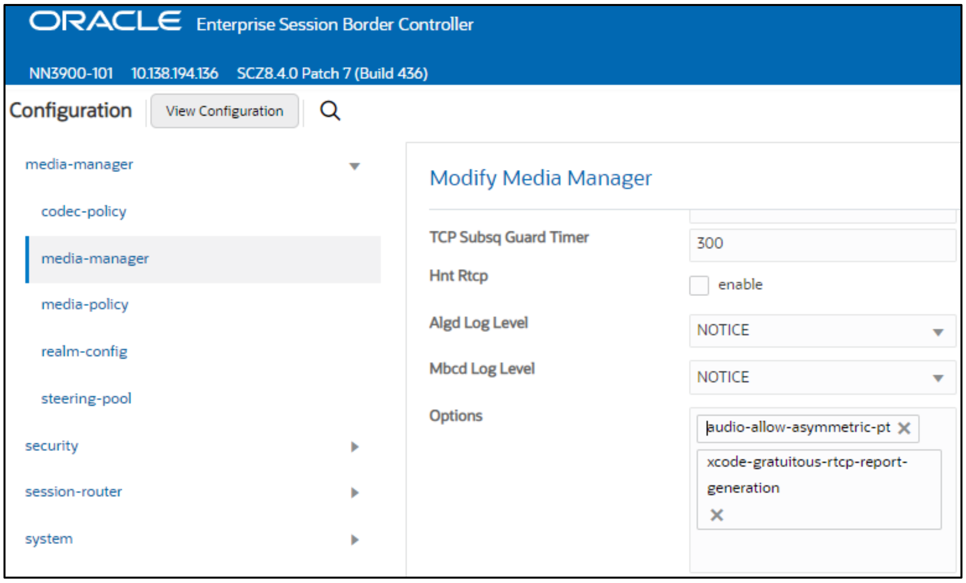
To configure media functionality on the SBC, you must first enabled the global media manager

GUI Path: media-manager/media-manager

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

The following options are recommeded for global media manager when interfacing with MSFT Teams Direct Routing

- Options: In the box next to options, add the string: audio-allow-asymmetric-pt
- Hit enter, then add: xcode-gratuitous-rtcp-report-generation (requires a reboot to take effect), hit enter again.



Modify Media Manager

TCP Subsq Guard Timer: 300

Hnt Rtcp: □ enable

Algd Log Level: NOTICE

Mbcd Log Level: NOTICE

Options: audio-allow-asymmetric-pt, xcode-gratuitous-rtcp-report-generation

- Click ok at the bottom

8.1.4 Sip Config

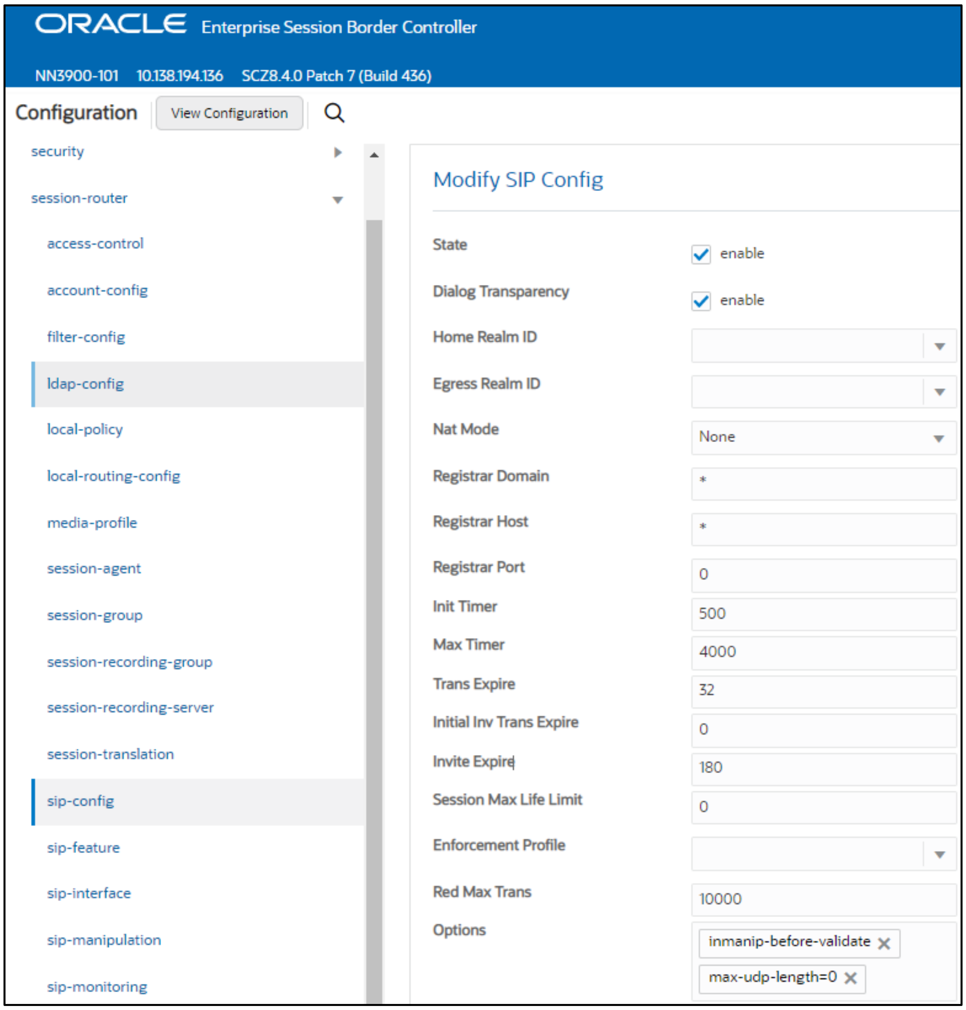
To enable sip related objects on the OCSBC, you must first configure the global Sip Config element:

GUI Path: session-router/sip-config

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

The following are recommended parameters under the global sip-config:

- Options: In the box next to options, add the string: inmanip-before-validate
- Hit enter, then add: max-udp-length=0, hit enter again



Modify SIP Config

State	☑ enable
Dialog Transparency	☑ enable
Home Realm ID	
Egress Realm ID	
Nat Mode	None
Registrar Domain	*
Registrar Host	*
Registrar Port	0
Init Timer	500
Max Timer	4000
Trans Expire	32
Initial Inv Trans Expire	0
Invite Expire	180
Session Max Life Limit	0
Enforcement Profile	
Red Max Trans	10000
Options	inmanip-before-validate ✕ max-udp-length=0 ✕

- Click OK at the bottom

8.2 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 MSFT Azure Communications Direct Routing, and the other to connect to PSTN Network.

8.2.1 Physical Interfaces

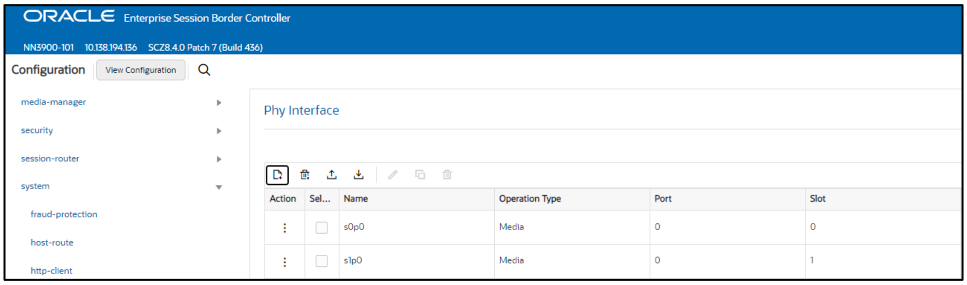
GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

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

Config Parameter	ACS Interface	PSTN
Name	s0p0	S1p0
Operation Type	Media	Media
Slot	0	1
Port	0	0

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



Action	Sel...	Name	Operation Type	Port	Slot
⋮	□	s0p0	Media	0	0
⋮	□	s1p0	Media	0	1

- Click OK at the bottom after entering config information for each.

8.2.2 Network Interfaces

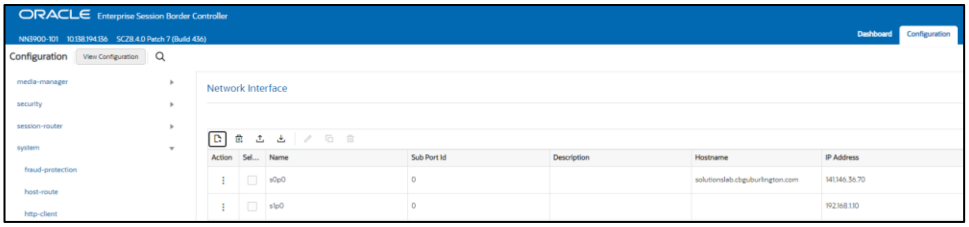
GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

- Click Add, use the following table as a configuration example: (hostname is optional)

Configuration Parameter	ACS Interface	PSTN
Name	s0p0	s1p0
Hostname	Solutionslab.cgbuburlington.com	
IP Address	141.146.36.70	192.168.1.10
Netmask	255.255.255.192	255.255.255.0
Gateway	141.146.36.65	192.168.1.1
DNS Primary IP	8.8.8.8	
DNS Domain	Solutionslab.cgbuburlington.com	

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



Action	Sel...	Name	Sub Port Id	Description	Hostname	IP Address
⋮	□	s0p0	0		solutionslab.cbguburlington.com	141.146.36.70
⋮	□	s1p0	0			192.168.1.10

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

8.3 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Microsoft Azure Communication Services Direct Routing

8.3.1 Certificate Records

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

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

GUI Path: security/certificate-record

ACLI Path: config t→security→certificate-record

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

- SBC Certificate (end-entity certificate)
- DigiCert RootCA Cert
- DigiCert Intermidiate Cert (this is optional – only required if your server certificate is signed by an intermediate)
- BaltimoreRoot CA Cert (Microsoft Presents the SBC a certficate signed by this authority)

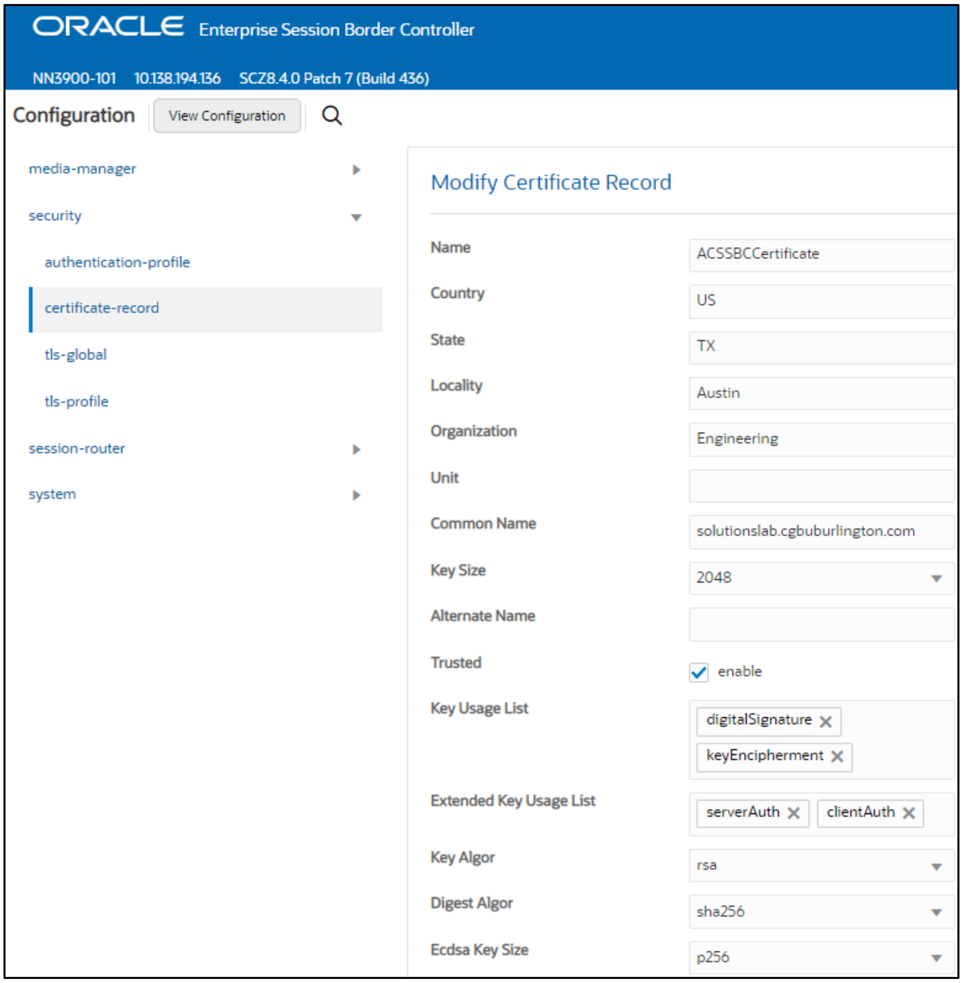
8.3.2 SBC End Entity Certificate

This is the certificate the SBC will present to Microsoft during the TLS handshake to establish a secure connection to Microsoft ACS Direct Routing.

The common name of this certificate should contain the SBC’s FQDN.

To configure this certificate record:

- Click ADD, and configure as shown below:



Modify Certificate Record

Name	ACSSBCCertificate
Country	US
State	TX
Locality	Austin
Organization	Engineering
Unit	
Common Name	solutionslab.cgbuburlington.com
Key Size	2048
Alternate Name	
Trusted	☑ enable
Key Usage List	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth clientAuth
Key Algor	rsa
Digest Algor	sha256
Ecdsa Key Size	p256

- Click OK at the bottom
- Next, using this same procedure, configure certificate records for Root and Intermediate CA Certificates

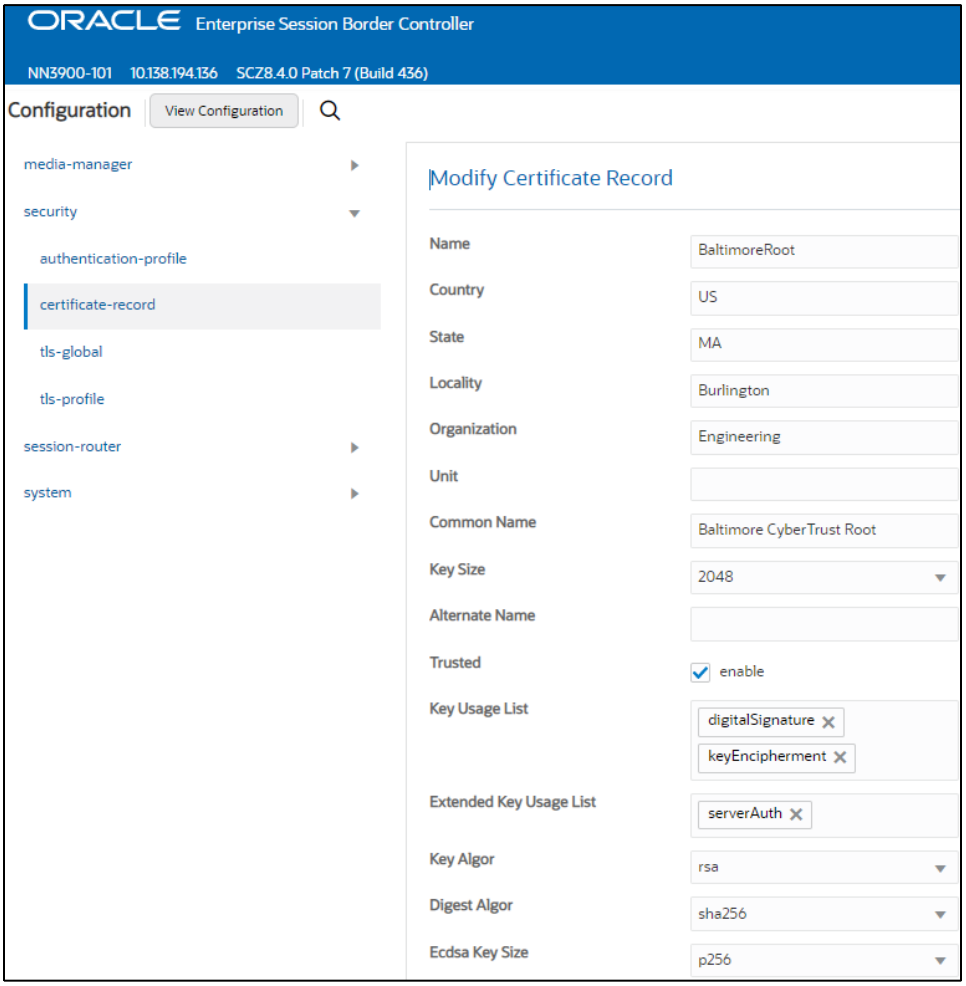
8.3.3 Root CA and Intermediate Certificates

8.3.3.1 Baltimore Root CA Certificate:

Microsoft presents a certificate to the SBC which is signed by Baltimore Cyber Baltimore CyberTrust Root. To trust this certificate, your SBC must have the certificate configured, imported and listed as a trusted CA certificate.

You can download this certificate here: https://cacert.omniroot.com/bc2025.pem

Please use the example below to configure this certificate on the Oracle SBC.



Modify Certificate Record

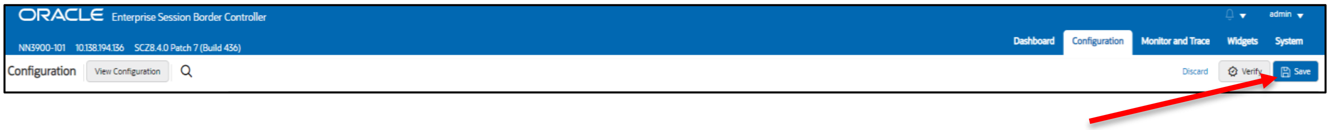
Name	BaltimoreRoot
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	
Common Name	Baltimore CyberTrust Root
Key Size	2048
Alternate Name	
Trusted	☑ enable
Key Usage List	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth
Key Algor	rsa
Digest Algor	sha256
Ecdsa Key Size	p256

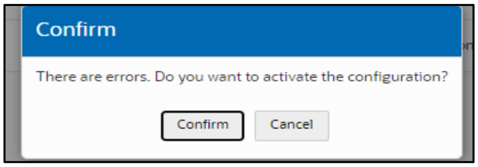
8.3.3.2 Digicert Root and Intermediate Certificates:

As part of this example configuration, you will see two more certificate records configured, DigiCertRoot and DigiCertIntermediate. This is the root and intermediate certificates used to sign our SBC certificate. As mentioned above, the intermediate certificate is optional, and only required if your server certificate is signed by an intermediate. Please see the table below as an example of how to create certificate records for the root (and intermediate if applicable) certificate provided to you by the Microsoft supported Certificate Authority you use to sign your SBC certificate.

Config Parameter	Digicert Intermediate	DigiCert Root CA
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

After you have created all of the required certificate records on the SBC, you will need to **save and activate** the configuration prior to moving on to the next step in the configuration process. You cannot generate a certificate signing request or import any certificates into the newly created certificate records without first saving and activating your configuration.



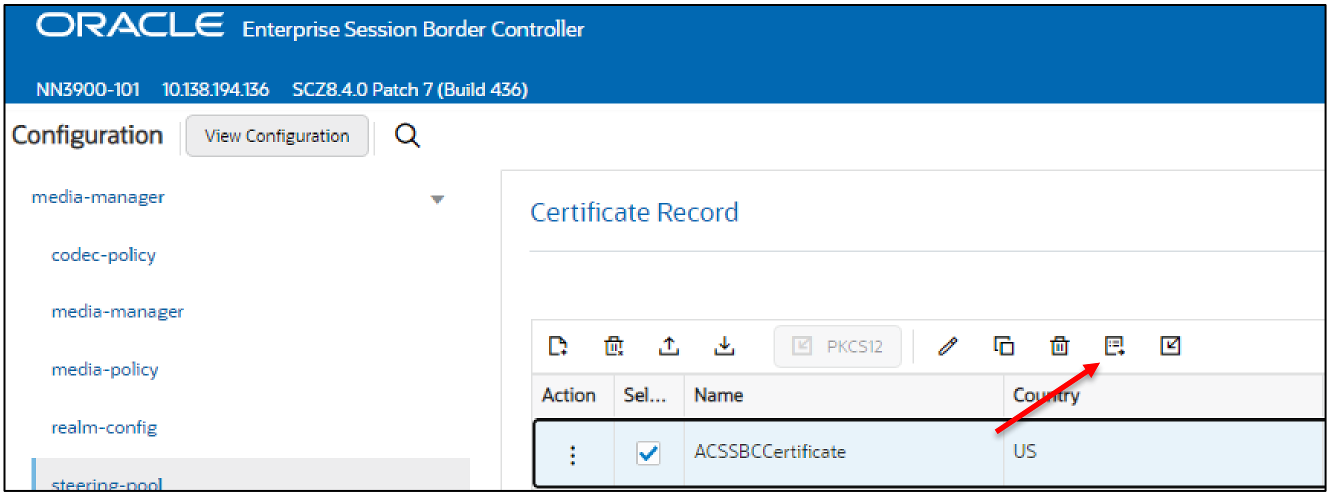


There are errors. Do you want to activate the configuration?

8.3.4 Generate Certificate Signing Request

Now that the SBC’s certificate has been configured, and you have saved and activated your configuration, it’s time to 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**.

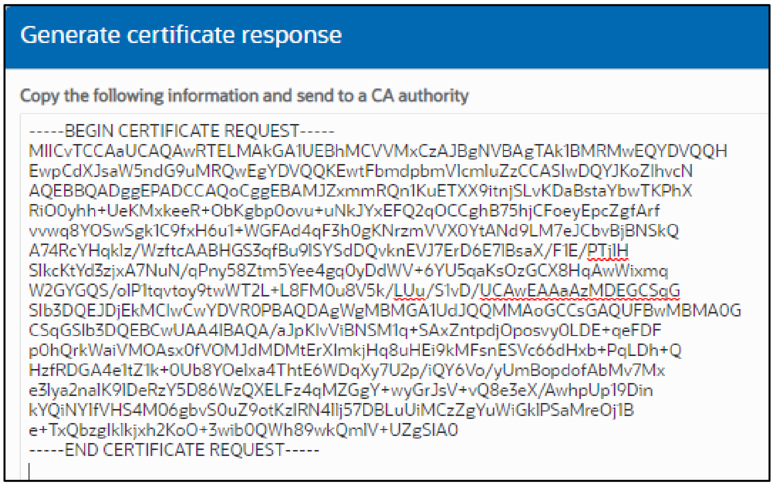
On the certificate record page in the OCSBC GUI, (security/certificate-record) select the SBC’s end entity certificate that was created above, and click the “generate” tab at the top:



NN3900-101 10.138.194.136 SCZ8.4.0 Patch 7 (Build 436)

Certificate Record

Action	Sel...	Name	Country
⋮	☑	ACSSBCCertificate	US



Generate certificate response

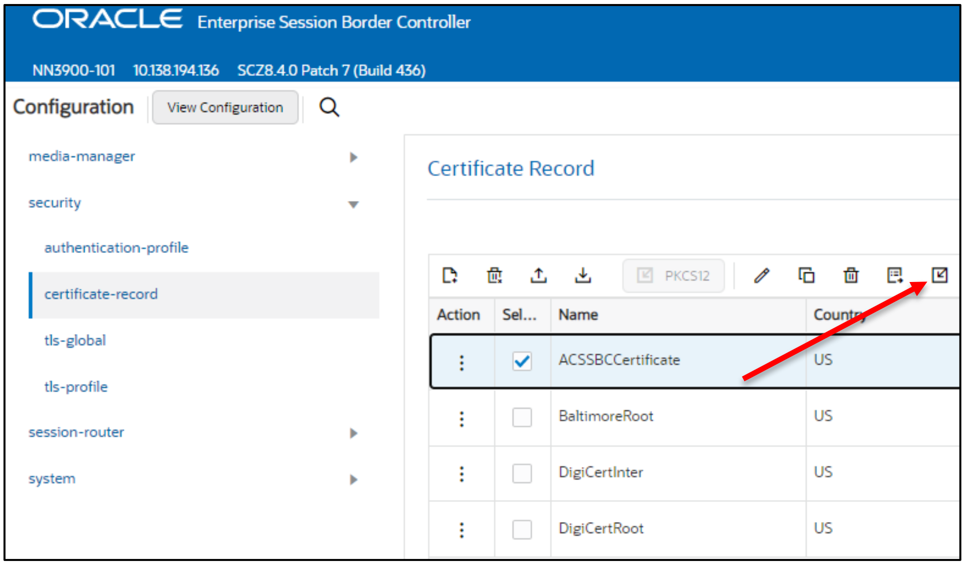
Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvTCCAaUCAQAwRTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMJZxmmRQn1KuETXX9itnjSLvKDaBstaYbwTKPhX
RiO0yhh+UeKMxkeeR+ObKgbp0ovu+uNkJYxEFQ2qOCCghB75hjCFoeyEpcZgfArf
vvwq8YOSwSgk1C9fxH6u1+WGFAd4qF3h0gKNrzmVVX0YtANd9LM7eJCbvBjBNSkQ
A74RcYHqklz/WzftcAABHGS3qfBu9ISYSdDQvknEVJ7ErD6E7IBsaX/F1E/PTjIH
SIkcKtYd3zjxA7NuN/qPny58Ztm5Yee4gq0yDdWV+6YU5qaKsOzGCX8HqAwWixmq
W2GYGQS/oIP1tqvtoy9twWT2L+L8FM0u8V5k/LUu/S1vD/UCAwEAAaAzMDEGCSqG
SIb3DQEJDjEkMCIwCwYDVR0PBAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0G
CSqGSIb3DQEBCwUAA4IBAQA/aJpKIvViBNSM1q+SAxZntpdjOposvy0LDE+qeFDF
p0hQrkWaiVMOAsx0fVOMJdMDMtErXImkjHq8uHEi9kMFsnESVc66dHxb+PqLDh+Q
HzfRDGA4e1tZ1k+0Ub8YOelxa4ThtE6WDqXy7U2p/iQY6Vo/yUmBopdofAbMv7Mx
e3lya2naIK9IDeRzY5D86WzQXELFz4qMZGgY+wyGrJsV+vQ8e3eX/AwhpUp19Din
kYQiNYIfVHS4M06gbvS0uZ9otKzIRN4Ilj57DBLuUiMCzZgYuWiGkIPSaMreOj1B
e+TxQbzgIkIkjxh2KoO+3wib0QWh89wkQmIV+UZgSIA0
-----END CERTIFICATE REQUEST-----
```

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

8.3.5 Import Certificates to SBC Certificate Records

- Once the 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 all certificates have been imported, issue save/activate from the WebGUI

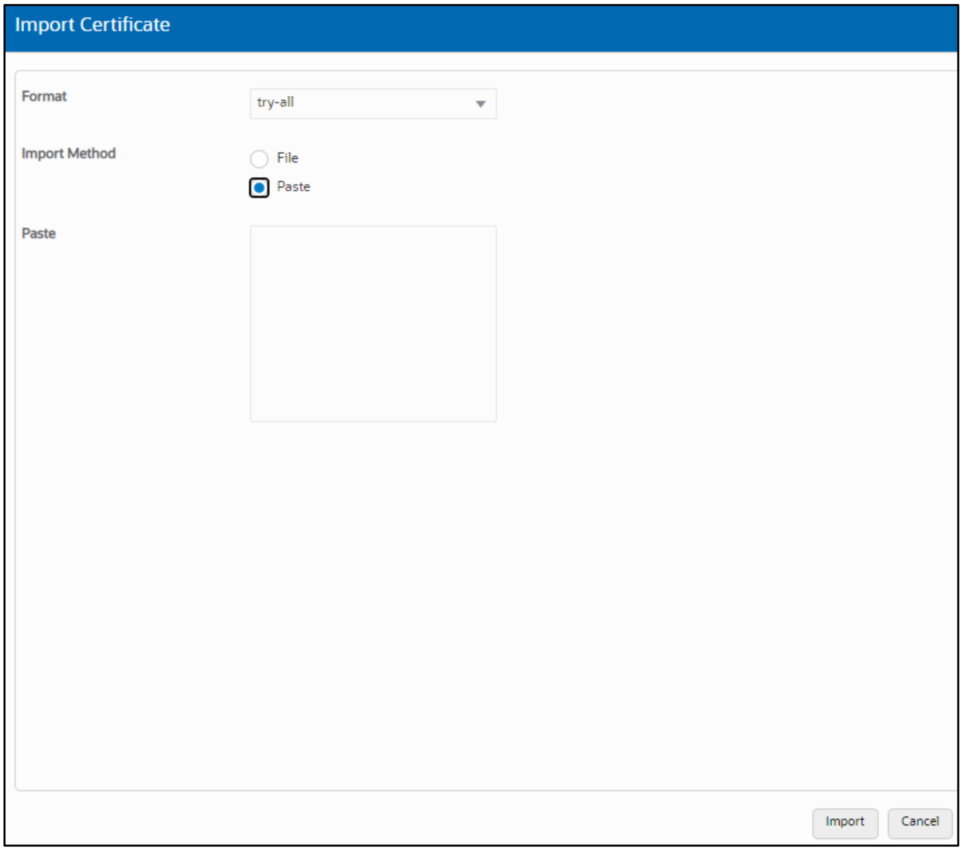


ORACLE Enterprise Session Border Controller

NN3900-101 10.138.194.136 SCZ8.4.0 Patch 7 (Build 436)

Certificate Record

Action	Sel...	Name	Country
⋮	☑	ACSSBCCertificate	US
⋮	□	BaltimoreRoot	US
⋮	□	DigiCertInter	US
⋮	□	DigiCertRoot	US



Import Certificate

Format: try-all

Import Method: ○ File ● Paste

Paste

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

- BaltimoreRoot
- DigiCertInter
- DigiCertRoot

At this stage, all required certificates have been imported.

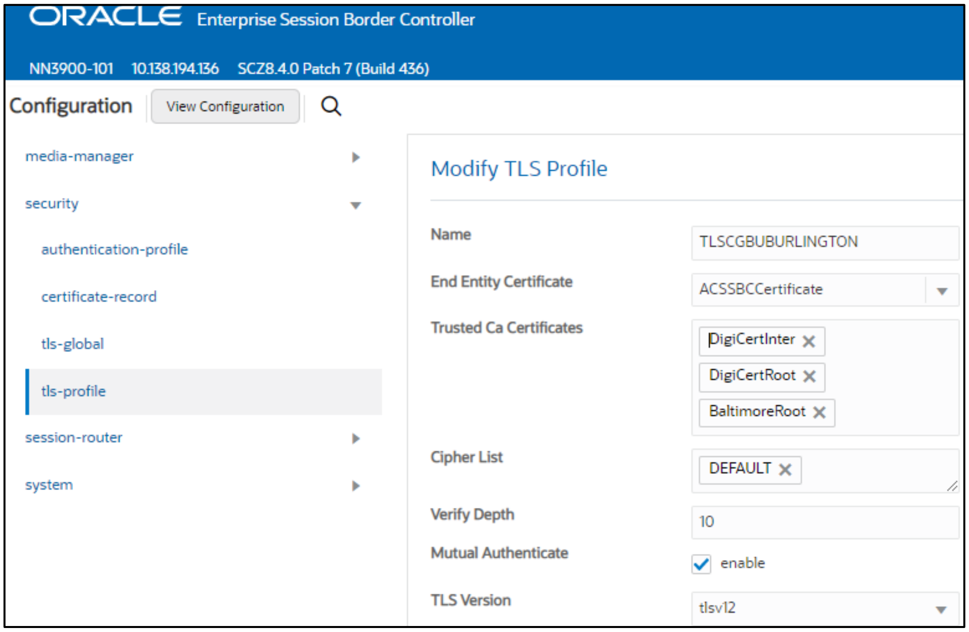
8.3.6 TLS Profile

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



Modify TLS Profile

Name: TLSCGBUBURLINGTON

End Entity Certificate: ACSSBCCertificate

Trusted Ca Certificates: DigiCertInter, DigiCertRoot, BaltimoreRoot

Cipher List: DEFAULT

Verify Depth: 10

Mutual Authenticate: ☑ enable

TLS Version: tlsv12

- As you can see in the example above, the tls-profile is where we assign the SBC end entity certificate, as well as the trusted CA certs that have been created and imported to the SBC.
- Once the tls profile config is in place, click OK at the bottom

8.4 Media Security Configuration

This section outlines how to configure support for media security (SRTP) between the OCSBC and Microsoft ACS Direct Routing.

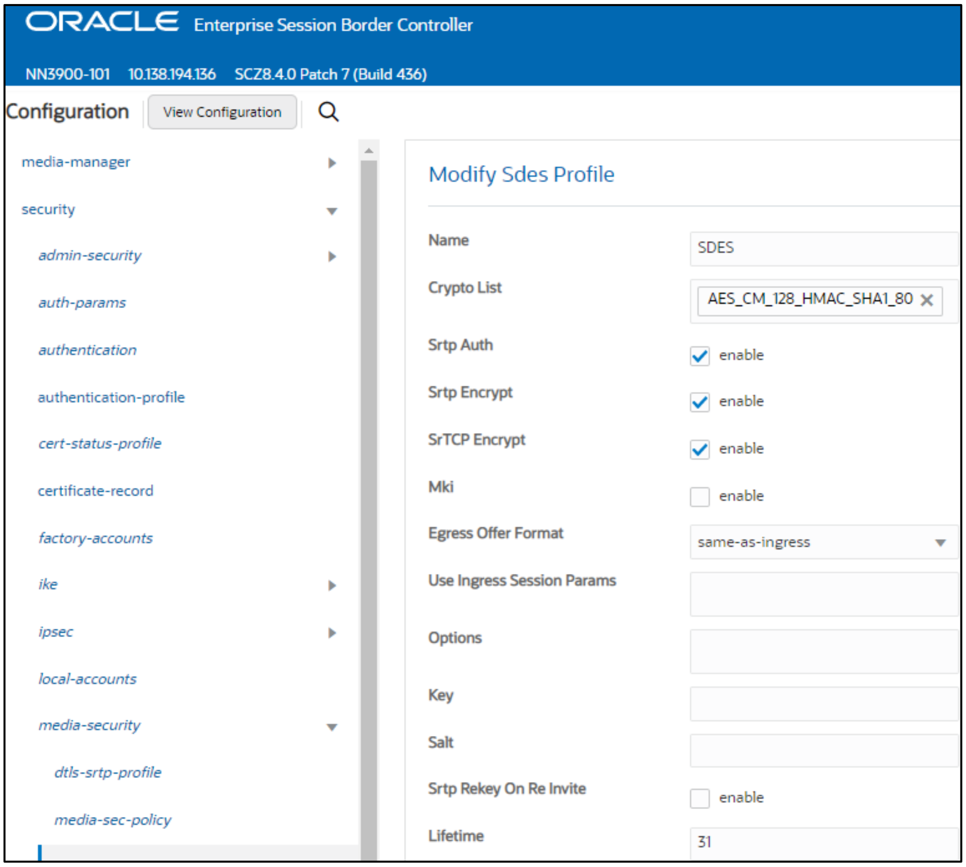
8.4.1 SDES-Profile

This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured. The only crypto-suite option supported by Microsoft is AES_CM_128_HMAC_SHA1_80 and must be included in the crypto list

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 (you may first have to toggle the "show all" button on the bottom left of the screen to see media secuirty configuration options)



Modify Sdes Profile

Name	SDES
Crypto List	AES_CM_128_HMAC_SHA1_80
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 Rekey On Re Invite	☐ enable
Lifetime	31

Note: The lifetime parameter set to a value of 31 is required for Microsoft ACS Direct Routing

- Click OK at the bottom

8.4.2 Media Security Policy

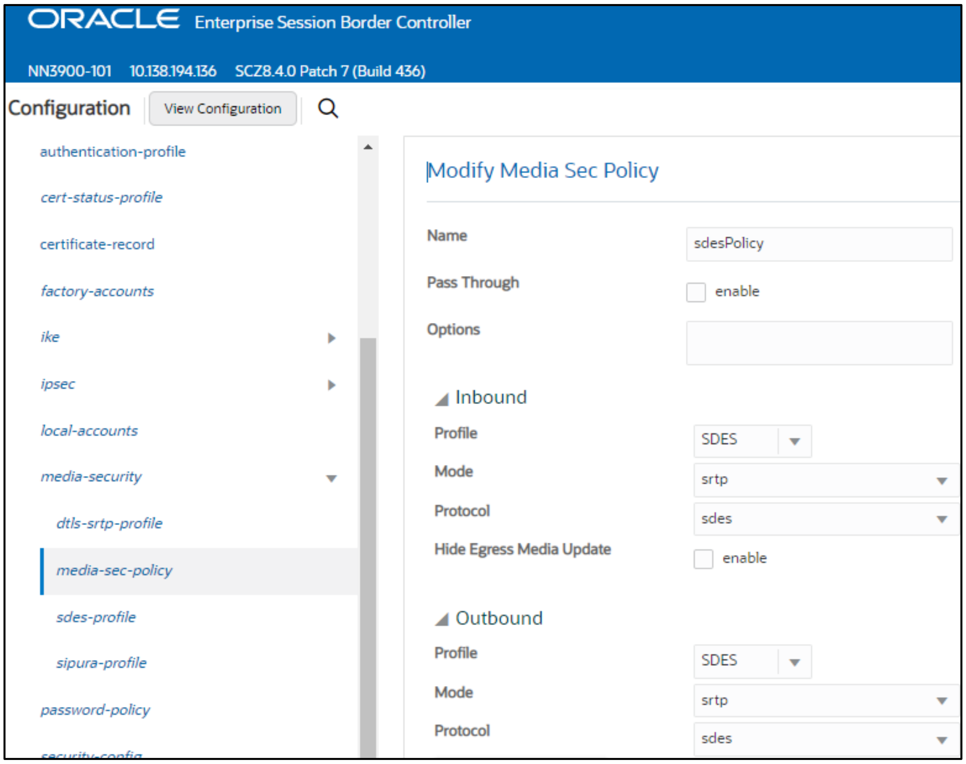
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or both) and, if SRTP needs to be used, the sdes-profile that will be used.

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

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



Modify Media Sec Policy

Name: sdesPolicy

Pass Through: □ enable

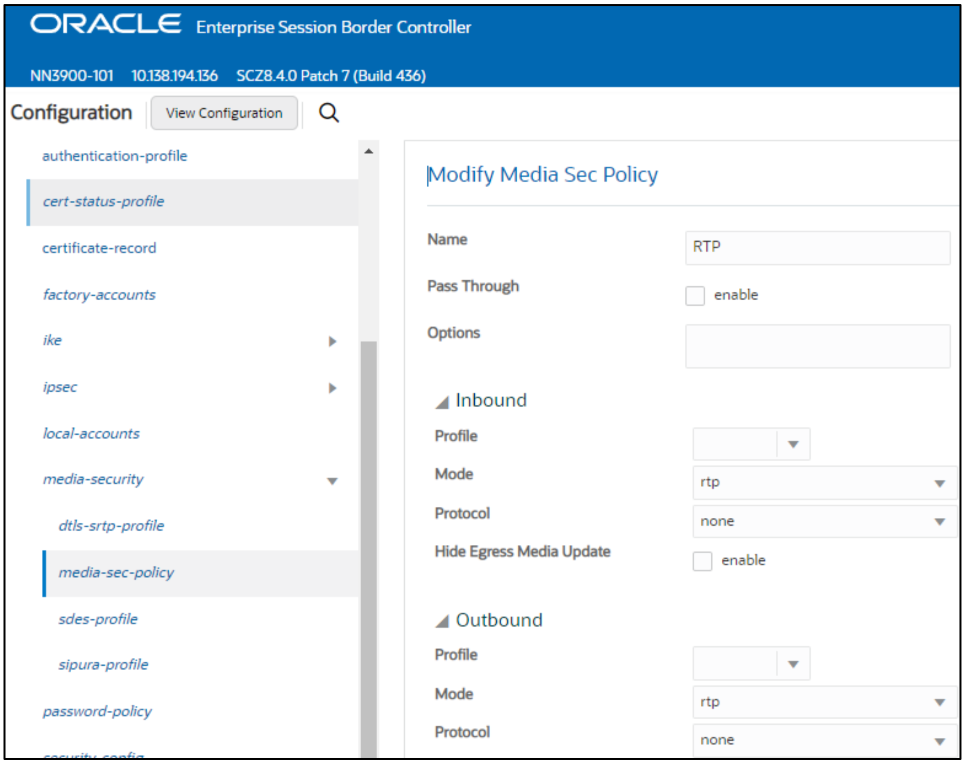
Options:

Inbound

- Profile: SDES
- Mode: srtp
- Protocol: sdes
- Hide Egress Media Update: □ enable

Outbound

- Profile: SDES
- Mode: srtp
- Protocol: sdes



Modify Media Sec Policy

Name: RTP

Pass Through: □ enable

Options:

Inbound

- Profile:
- Mode: rtp
- Protocol: none
- Hide Egress Media Update: □ enable

Outbound

- Profile:
- Mode: rtp
- Protocol: none

- Click OK at the bottom of each when applicable

8.5 Transcoding Configuration

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.

8.5.1 Codec Policies

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

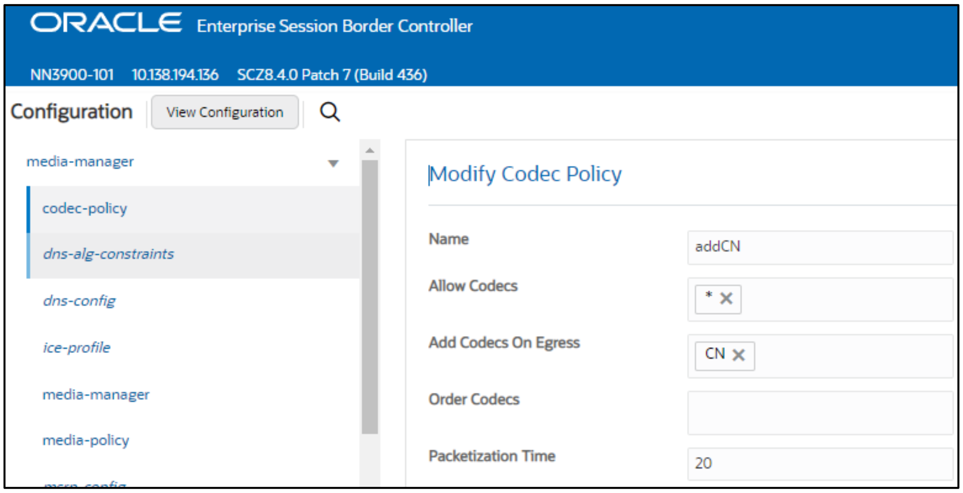
Note: This is an optional configuration. Only configure codec policies if deemed necessary in your environment

GUI Path: media-manager/codec-policy

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

We create the codec-policy, addCN, to allow the SBC to generate Comfort Noise packets towards Teams

- Click Add, and use the examples below to configure



Modify Codec Policy

Name: addCN

Allow Codecs: *

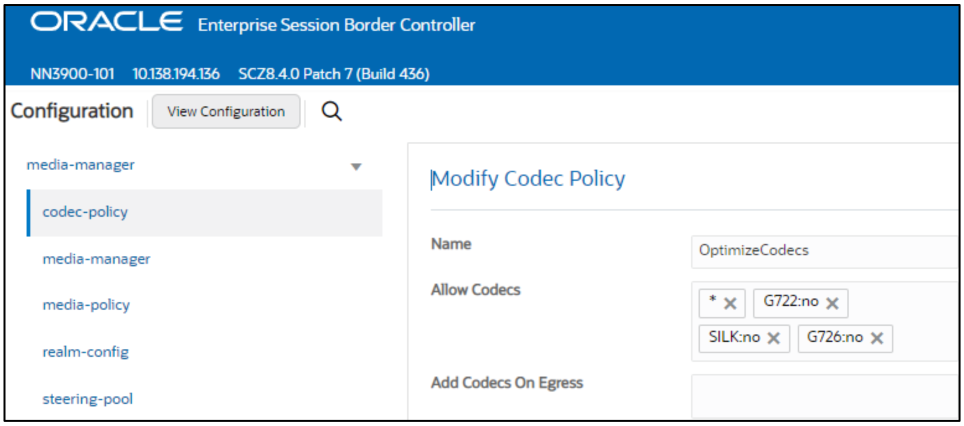
Add Codecs On Egress: CN

Order Codecs:

Packetization Time: 20

In some instances, SIP trunks may have issues with codec being offered by Microsoft teams. For this reason, we have created another codec policy, “OptimizeCodecs”, for the SIP trunk to remove the codecs that are not required or supported.

- Click Add and use the example below to configure if applicable in your environment.



Modify Codec Policy

Name	OptimizeCodecs
Allow Codecs	* ✕ G722:no ✕ SILK:no ✕ G726:no ✕
Add Codecs On Egress	

- Click OK at the bottom of each when applicable

8.5.2 Media Profiles

For different codecs and media types, you can setup customized media profiles that serve to police media values and define media bandwidth policies.

SILK & CN offered by Microsoft teams are using a payload type which is different usual, so to support this, we configure media profiles on the SBC.

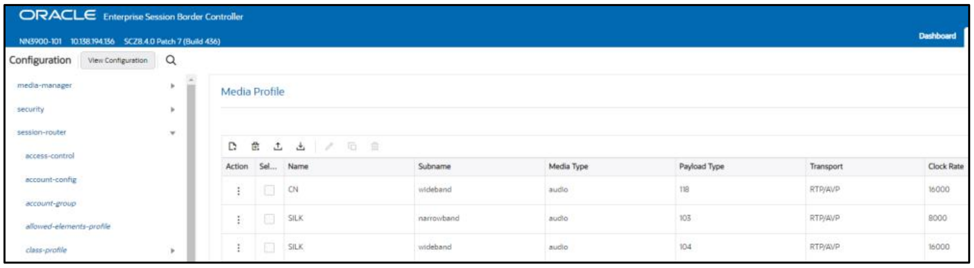
GUI Path: session-router/media-profile

ACLI Path: config t→session-router→media-profile

Configure three media profiles to support the following:

- Silk Wideband
- Silk Narrowband
- CN
- Click Add, then use the table below as an example to configure each:

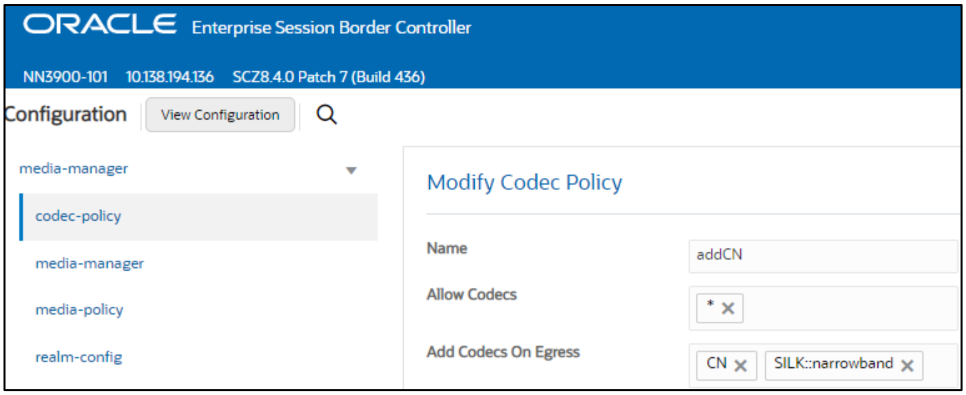
Parameters	Silk-1	Silk-2	CN
Subname	narrowband	wideband	wideband
Payload-Type	103	104	118
Clock-rate	8000	16000	0



Media Profile

Action	Sel...	Name	Subname	Media Type	Payload Type	Transport	Clock Rate
⋮	□	CN	wideband	audio	118	RTP/AVP	16000
⋮	□	SILK	narrowband	audio	103	RTP/AVP	8000
⋮	□	SILK	wideband	audio	104	RTP/AVP	16000

- Once media profiles are configured, then can then be added to the codec policy towards Microsoft. Please see the example below:



ORACLE Enterprise Session Border Controller
NN3900-101 10.138.194.136 SCZ8.4.0 Patch 7 (Build 436)
Configuration
View Configuration
media-manager
codec-policy
media-manager
media-policy
realm-config

Modify Codec Policy

Name: addCN

Allow Codecs: *

Add Codecs On Egress: CN, SILK::narrowband

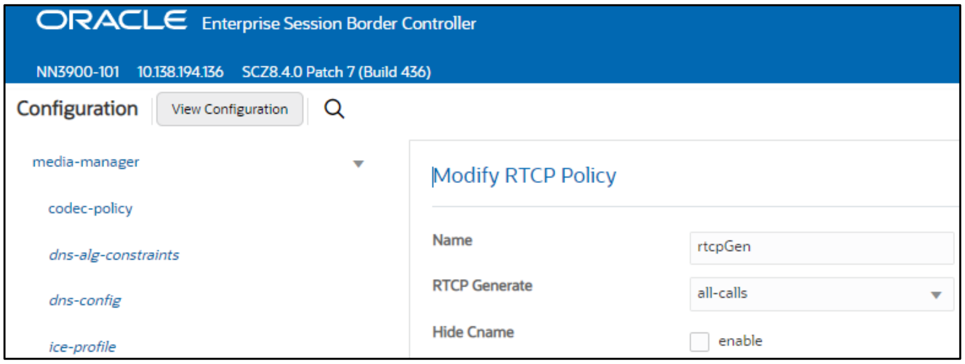
8.5.3 RTCP Policy

The following RTCP policy needs to be configured for the OCSBC to generate RTCP sender reports toward Microsoft Teams. The media manger options config, xcode-gratuitous-rtcp-report-generation, allows the SBC to generate receiver reports

GUI Path: media-manager/rtcp-policy

ACLI Path: config t→media-manger→rtcp-policy

- Click Add, use the example below as a configuration guide



ORACLE Enterprise Session Border Controller
NN3900-101 10.138.194.136 SCZ8.4.0 Patch 7 (Build 436)
Configuration
View Configuration
media-manager
codec-policy
dns-alg-constraints
dns-config
ice-profile

Modify RTCP Policy

Name: rtcpGen

RTCP Generate: all-calls

Hide Cname: □ enable

- Click OK at the bottom of the screen

8.6 Media Configuration

This section will guide you through the configuration of realms and steering pools, both of which are required for the SBC to handle signaling and media flows toward Microsoft ACS Direct Routing and PSTN.

8.6.1 Realm Config

Realms are a logical distinction representing routes (or groups of routes) reachable by the Oracle® Enterprise 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, which can reside in different VPNs.

In this example, we're creating two realms. One facing Microsoft ACS, the other facing PSTN.

GUI Path; media-manger/realm-config

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

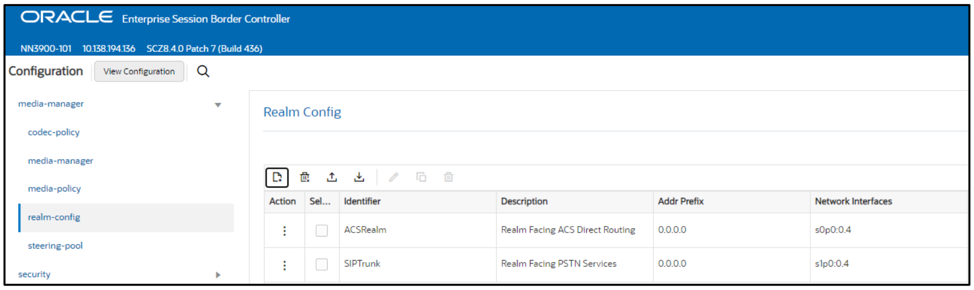
- Click Add, and use the following table as a configuration example for the three realms used in this configuration example

Config Parameter	ACS Realm	PSTN Realm
Identifier	ACSRealm	SIPTrunk
Network Interface	s0p0:0	s1p0:0
Mm in realm	☑	☑
Media Sec policy	sdespolicy	RTP
RTCP mux	☑	
Teams Fqdn	solutionslab.cgbuburlington.com	
Teams fqdn in uri	☑	
Sdp Inactive Only	☑	
Codec policy	addCN	OptimizeCodecs
RTCP policy	rtcpGen	
Access Control Trust Level	HIGH	HIGH

Teams FQDN field on the ACS facing realm must contain the SBC's FQDN. This is used by the SBC to properly format signaling messages the SBC sends to Microsoft.

Notice, the realm configuration is where we assign some of the elements configured earlier in this document, ie…

- Network interface
- Media security policy
- Codec policy
- Rtcp policy



Action	Sel...	Identifier	Description	Addr Prefix	Network Interfaces
⋮	□	ACSRealm	Realm Facing ACS Direct Routing	0.0.0.0	s0p0:0.4
⋮	□	SIPTrunk	Realm Facing PSTN Services	0.0.0.0	s1p0:0.4

- Click OK at the bottom after configuring each realm.

8.6.2 Steering Pools

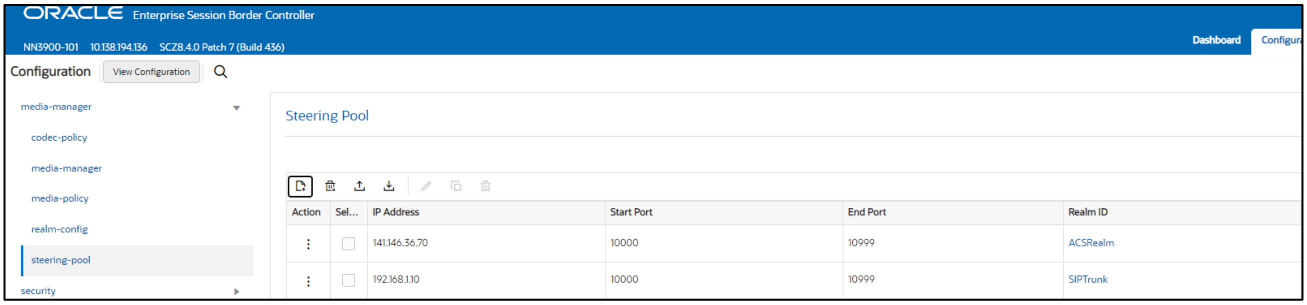
Steering pools define sets of ports that are used for steering media flows through the OCSBC.
These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We configure one steering pool for PSTN and another for Microsoft ACS.

GUI Path: media-manger/steering-pool

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

- Click Add, and use the below examples to configure



Action	Sel...	IP Address	Start Port	End Port	Realm ID
⋮	□	141.146.36.70	10000	10999	ACSRealm
⋮	□	192.168.1.10	10000	10999	SIPTrunk

- Click OK at the bottom after configuring each

8.7 Sip Configuration

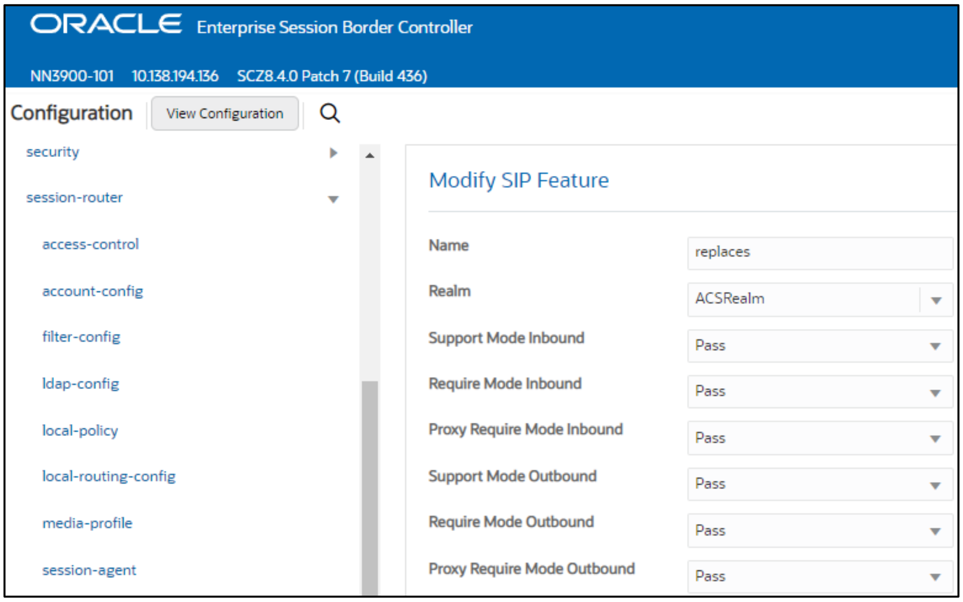
This section outlines the configuration parameters required for processing, modifying and securing sip signaling traffic.

8.7.1 Sip Feature

The following sip feature needs to be added to the Configuration of the SBC to enable support for the replaces header, allowing for successful consultative transfer. This applies to sip messages received by the SBC with replaces listed under the Supported header.

GUI Path: session-router/sip-feature

ALCI Path: config t→session-router→sip-feature



Modify SIP Feature

Name	replaces
Realm	ACSRealm
Support Mode Inbound	Pass
Require Mode Inbound	Pass
Proxy Require Mode Inbound	Pass
Support Mode Outbound	Pass
Require Mode Outbound	Pass
Proxy Require Mode Outbound	Pass

- Click ok at the bottom

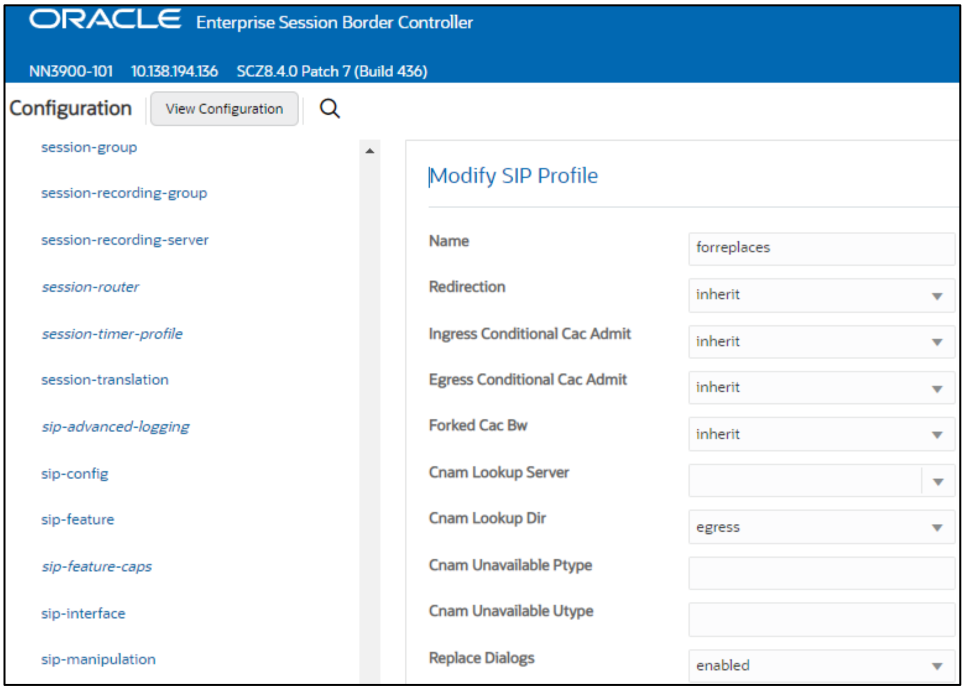
8.7.2 Sip Profile

A sip profile needs to be configured an assigned to the ACS sip interface. The sip profile allows the SBC to replace a dialog when it receives a request form MSFT with a replaces header.

GUI Path: session-router/sip-profile

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

- Click Add and use the example below to configure a sip profile on the SBC.



Modify SIP Profile

Name	forreplaces
Redirection	inherit
Ingress Conditional Cac Admit	inherit
Egress Conditional Cac Admit	inherit
Forked Cac Bw	inherit
Cnam Lookup Server	
Cnam Lookup Dir	egress
Cnam Unavailable Ptype	
Cnam Unavailable Utype	
Replace Dialogs	enabled

- Click OK at the bottom

8.7.3 Sip Interface

The SIP interface defines the transport addresses (IP address and port) upon which the OCSBC

Receives and sends SIP messages

Configure two sip interfaces, one associated with PSTN Realm, and the other will be for Microsoft ACS realm.

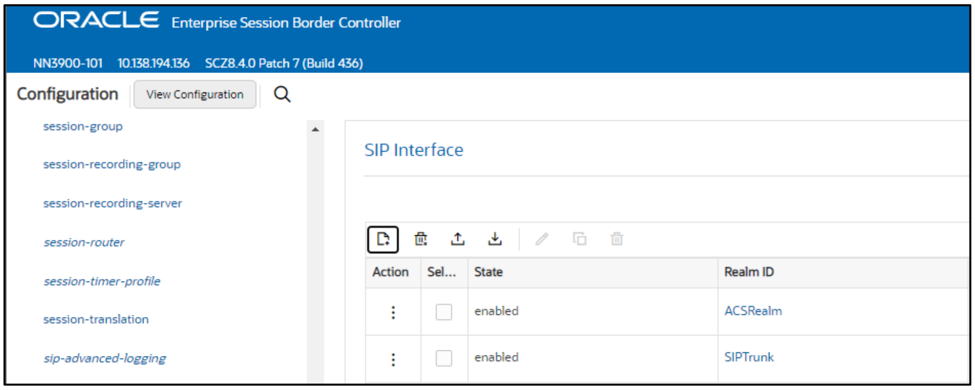
GUI Path: session-router/sip-interface

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

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

Config Parameter	SipTrunk	ACS
Realm ID	SipTrunk	ACSRealm
Sip profile		forreplaces
Sip Port Config Parmeter	**Sip Trunk**	**Teams**
Address	192.168.1.10	141.146.36.70
Port	5060	5061
Transport protocol	UDP	TLS
TLS profile		TLSCGBUBURLINGTON
Allow anonymous	agents-only	agents-only

- This is also where we are assigning two parameters configured earlier in the guide. TLSProfile to secure sip signaling between the OCSBC and Microsoft ACS, and the sip profile to allow the SBC to replace dialogs.



SIP Interface

Action	Sel...	State	Realm ID
⋮	□	enabled	ACSRealm
⋮	□	enabled	SIPTrunk

- Click OK at the bottom of each after they are configured.

8.7.4 Session Agents

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

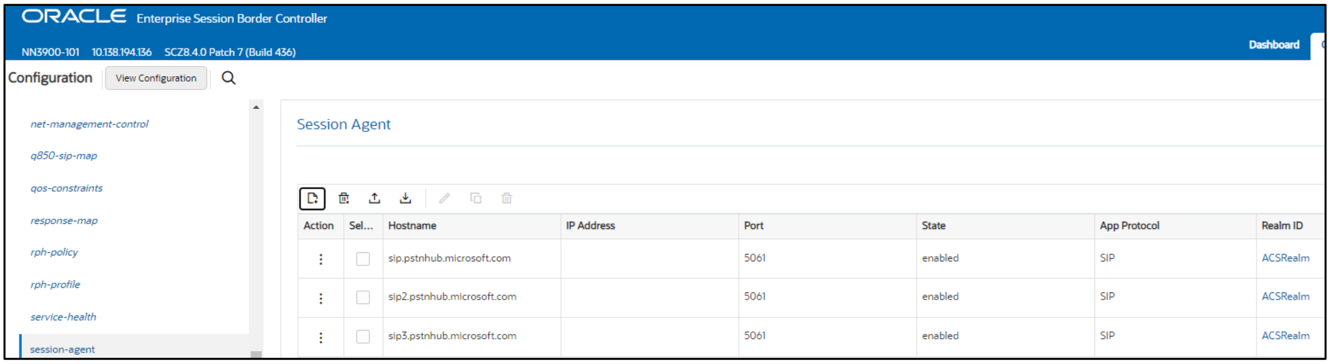
GUI Path: session-router/session-agent

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

You will need to configure three Session Agents for the Microsoft ACS Direct Routing Interface

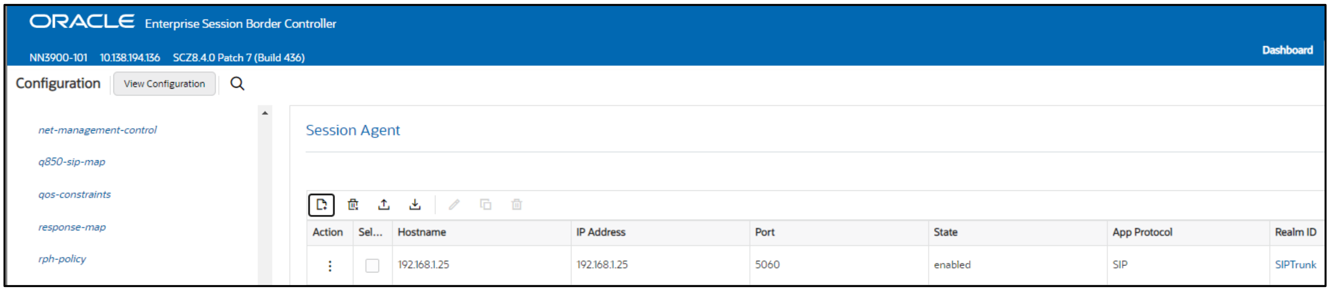
- Click Add, and use the table below to configure:

Config parameter	Session Agent 1	Session Agent 2	Session Agent 3
Hostname	sip.pstnhub.microsoft.com	sip2.pstnhub.microsoft.com	sip3.pstnhub.microsoft.com
Port	5061	5061	5061
Transport method	StaticTLS	StaticTLS	StaticTLS
Realm ID	ACSRealm	ACSRealm	ACSRealm
Ping Method	OPTIONS	OPTIONS	OPTIONS
Ping Interval	30	30	30
Refer Call Transfer	enabled	enabled	enabled
Ping Response	☑	☑	☑



Action	Sel...	Hostname	IP Address	Port	State	App Protocol	Realm ID
⋮	□	sip.pstnhub.microsoft.com		5061	enabled	SIP	ACSRealm
⋮	□	sip2.pstnhub.microsoft.com		5061	enabled	SIP	ACSRealm
⋮	□	sip3.pstnhub.microsoft.com		5061	enabled	SIP	ACSRealm

- In our example config, we have also configured another session agent for PSTN. This is the signaling IP or FQDN to send and receive calls to and from your carrier.



Action	Sel...	Hostname	IP Address	Port	State	App Protocol	Realm ID
⋮	□	192.168.1.25	192.168.1.25	5060	enabled	SIP	SIPTrunk

- Hit the OK tab at the bottom of each when applicable

8.7.5 Session Agent Group

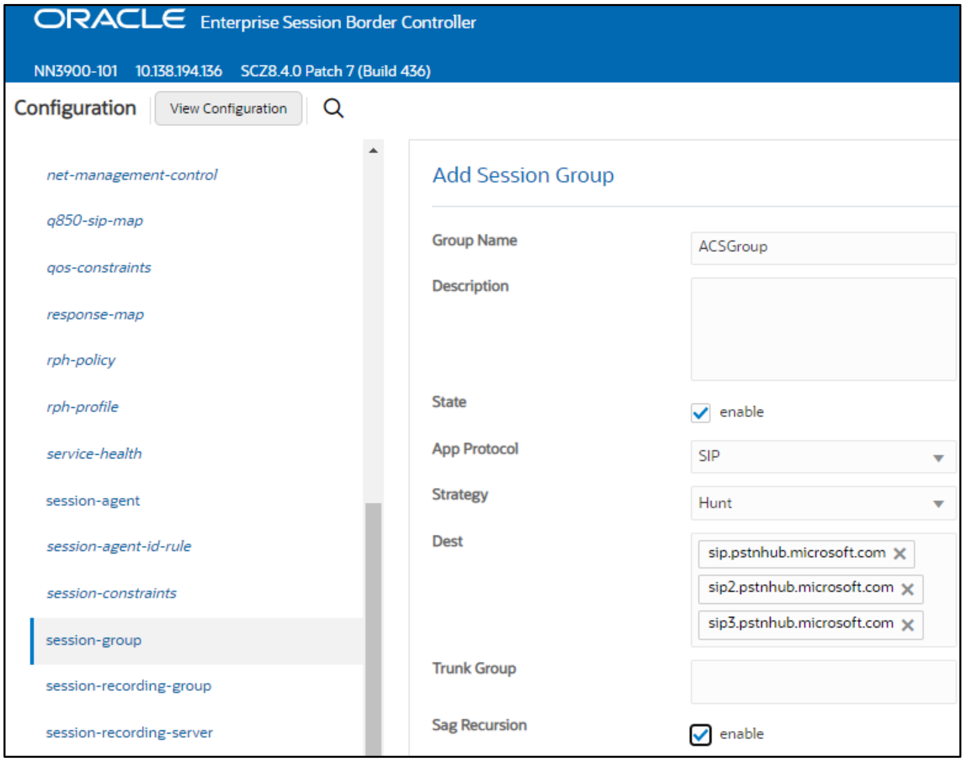
A session agent group allows the SBC to create a load balancing model:

All three session agents configured above for Microsoft ACS will be added to the group.

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:



Add Session Group

Group Name	ACSGroup
Description	
State	☑ enable
App Protocol	SIP
Strategy	Hunt
Dest	sip.pstnhub.microsoft.com sip2.pstnhub.microsoft.com sip3.pstnhub.microsoft.com
Trunk Group	
Sag Recursion	☑ enable

- Click OK at the bottom

8.7.6 Routing Configuration-Local Policy

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

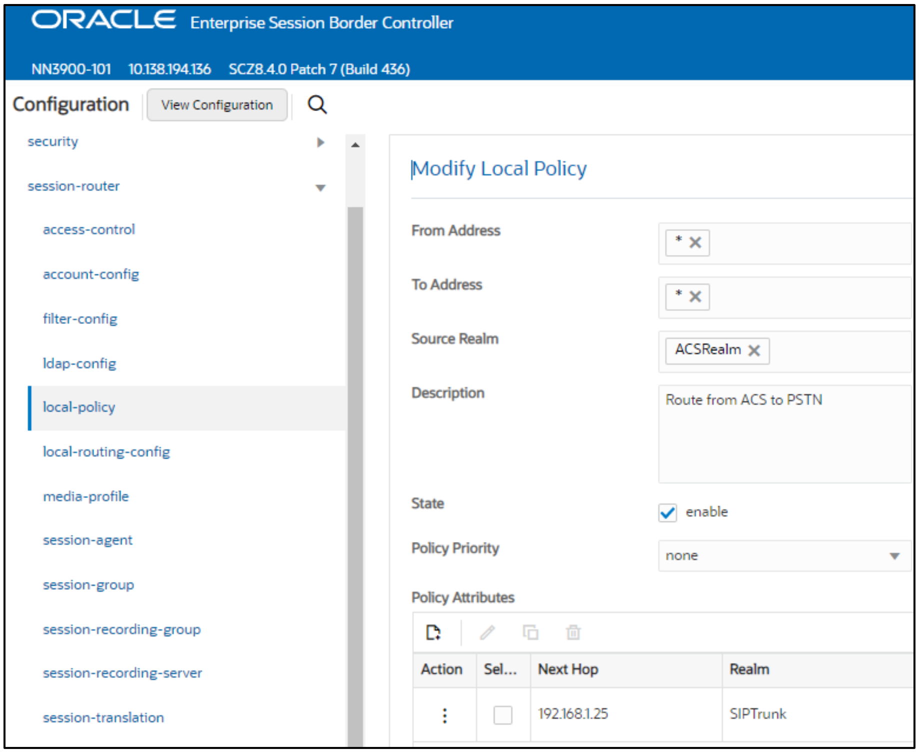
Below there are two local policies configured, one to route sip traffic from Microsoft ACS Direct Routing to PSTN, and the other to route sip traffic from PSTN to Microsoft ACS sip interface.

GUI Path: session-router/local-policy

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

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

Route from ACS to PSTN:



Modify Local Policy

From Address: *

To Address: *

Source Realm: ACSRealm

Description: Route from ACS to PSTN

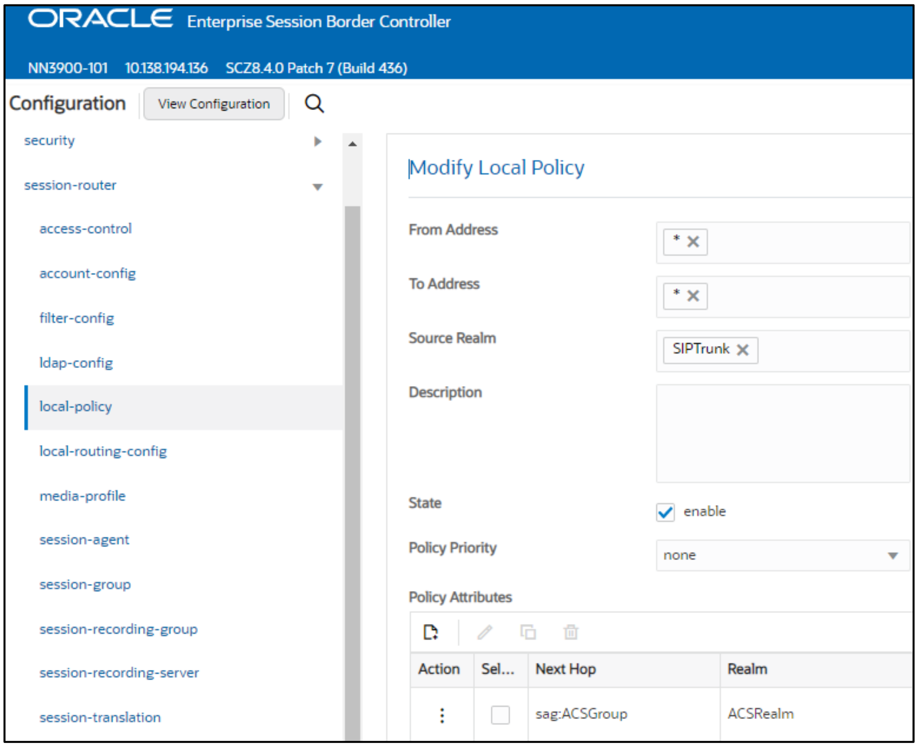
State: ☑ enable

Policy Priority: none

Policy Attributes

Action	Sel...	Next Hop	Realm
⋮	□	192.168.1.25	SIPTrunk

Route from PSTN to ACS:



Modify Local Policy

From Address: *

To Address: *

Source Realm: SIPTrunk

Description:

State: ☑ enable

Policy Priority: none

Policy Attributes

Action	Sel...	Next Hop	Realm
⋮	□	sag:ACSGroup	ACSRealm

- Notice here we utilize the session group and PSTN session agent configured earlier in this guide. They have now become the next hops for each realm for routing sip traffic.

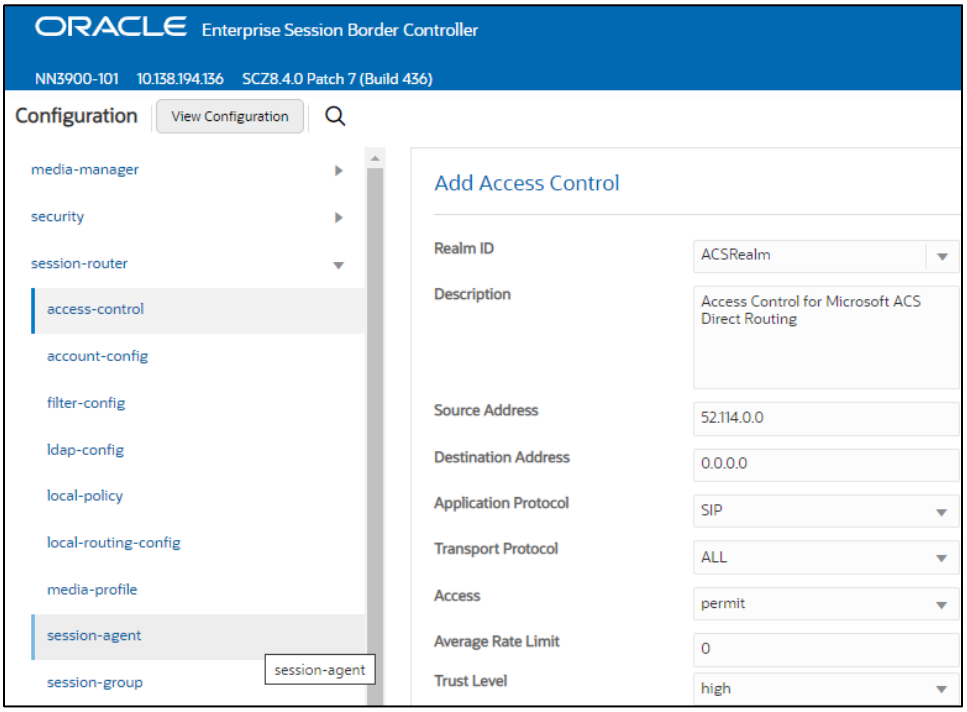
8.7.7 Access Control

As this configuration is a peering environment we would only want to allow layer 3 and layer 5 traffic from trusted sources. We can do this by configuring access controls on the SBC, and setting the trust level of the access control to the same trust level as the associated realm. This creates an implicit deny on the SBC, so only traffic from trusted IP addresses will be allowed.

GUI Path: session router/access-control

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

- Click add and use the examples below to configure.



Add Access Control

Realm ID	ACSRealm
Description	Access Control for Microsoft ACS Direct Routing
Source Address	52.114.0.0
Destination Address	0.0.0.0
Application Protocol	SIP
Transport Protocol	ALL
Access	permit
Average Rate Limit	0
Trust Level	high

- Click OK at the bottom

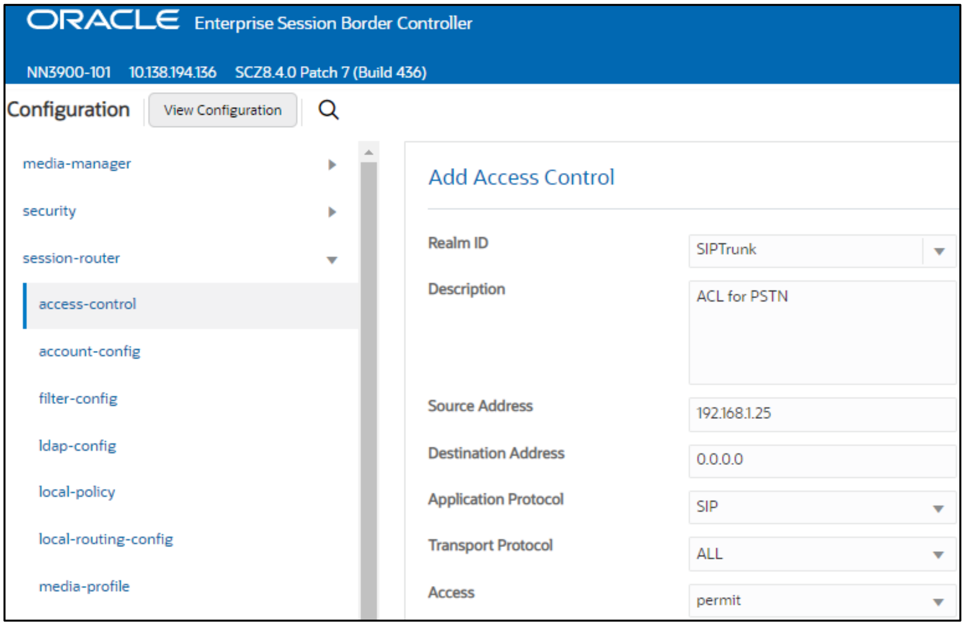
Notice in the ACL above, we are using a source address of 52.114.0.0. This creates a static permit entry on the SBC for the entire network. This is for example purposes only.

The Microsoft FQDN's configured earlier as session agents, – sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com and sip3.pstnhub.microsoft.com – will be resolved to one of the following IP addresses:

- 52.114.148.0
- 52.114.132.46
- 52.114.75.24
- 52.114.76.76
- 52.114.7.24
- 52.114.14.70
- 52.114.16.74
- 52.114.20.29

We recommend you configure an ACL on the SBC for each Microsoft IP address listed above.

Now we'll configure another ACL for the PSTN side of the SBC:



Add Access Control

Realm ID: SIPTrunk

Description: ACL for PSTN

Source Address: 192.168.1.25

Destination Address: 0.0.0.0

Application Protocol: SIP

Transport Protocol: ALL

Access: permit

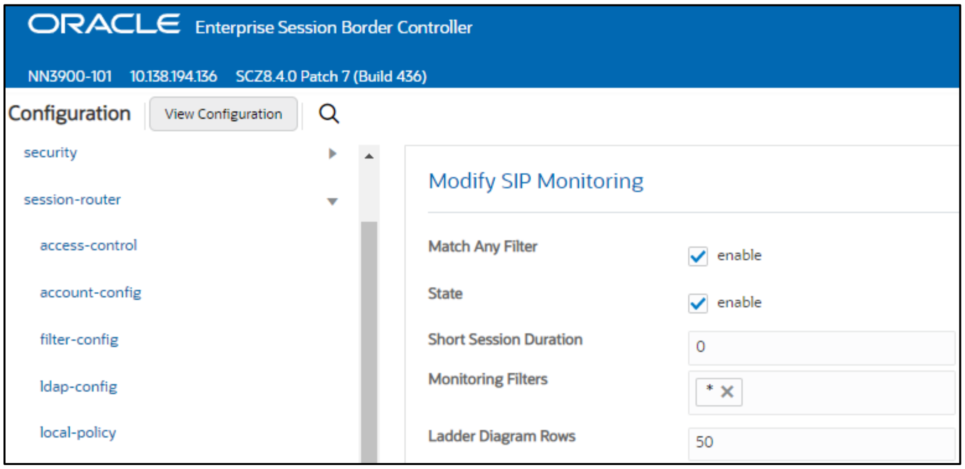
- Click OK at the bottom

8.7.8 Sip Monitoring

Sip monitoring configuration allows the SBC to capture calls and display them in the GUI under the Monitor and Trace Tab.

GUI Path: session router/sip monitoring

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



Modify SIP Monitoring

Match Any Filter: ☑ enable

State: ☑ enable

Short Session Duration: 0

Monitoring Filters: * ✕

Ladder Diagram Rows: 50

Click OK at the bottom

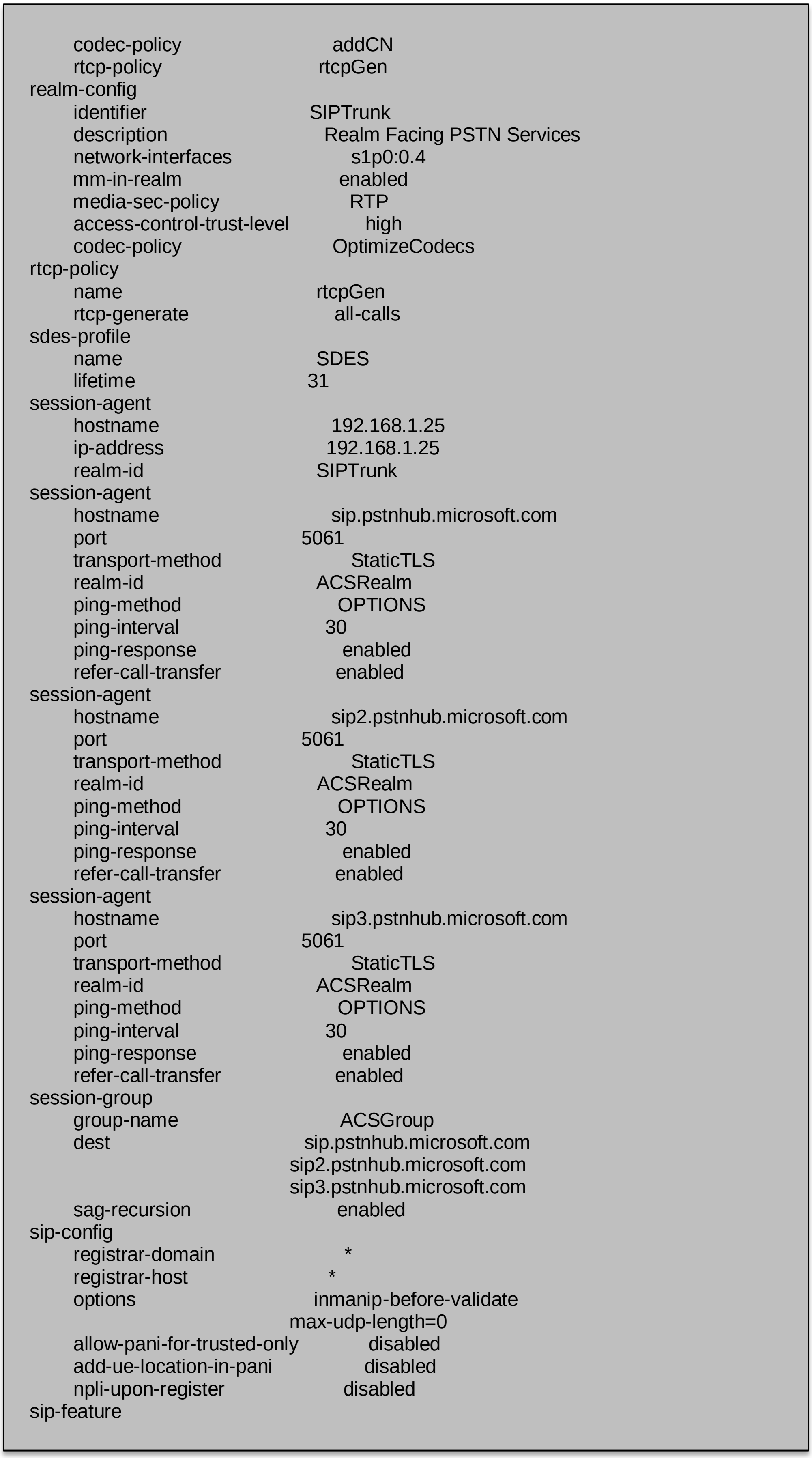
This concludes the SBC configuration via the GUI on the SBC. Save and activate the configuration. After that, we recommend you create a backup of your configuration as well.

9 ACLI Running Config

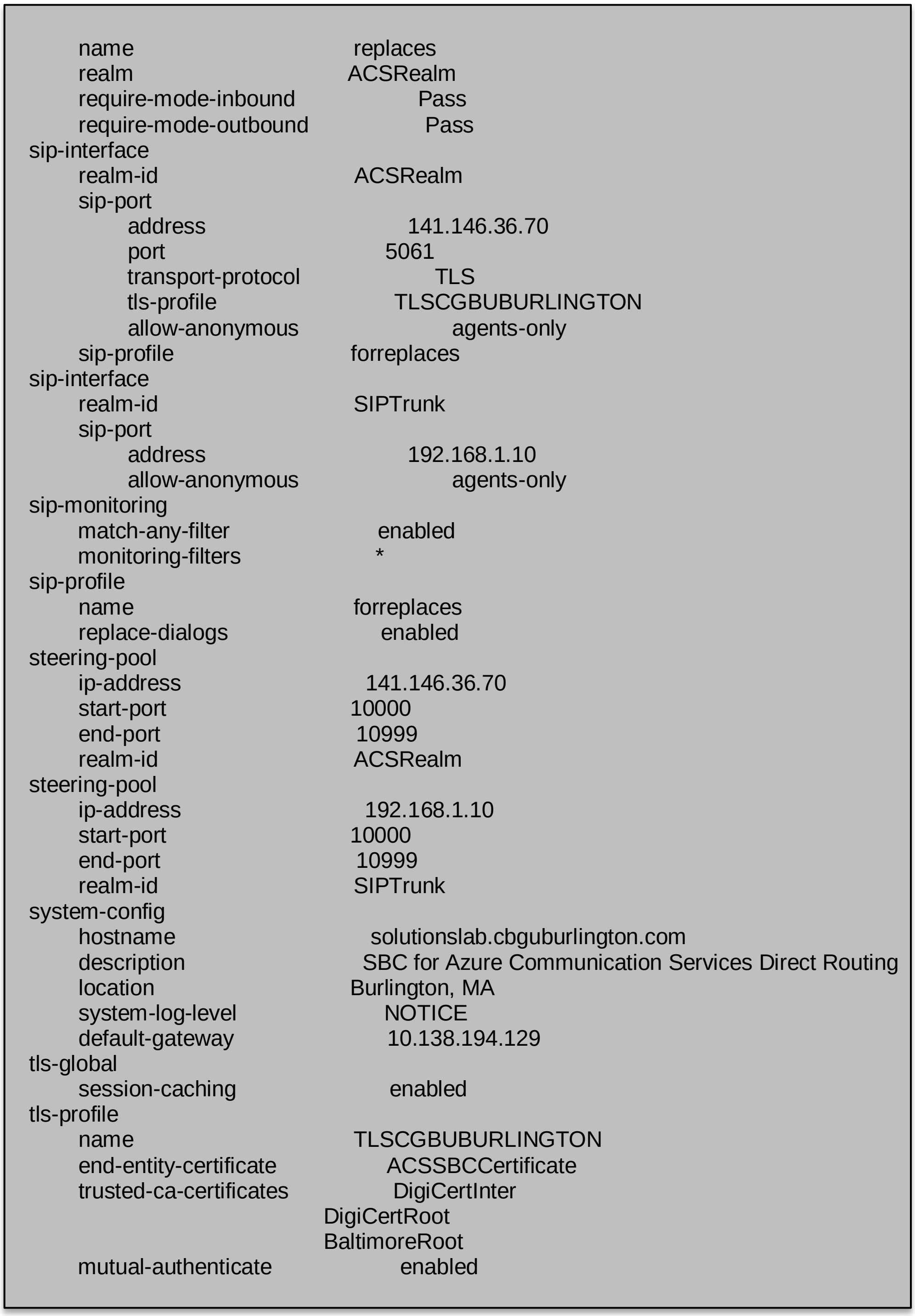
9.1 Show running config short

Below is the output for running the ACLI command, “show running-config short”

```
access-control
        realm-id                          SIPTrunk
        description                        ACL for PSTN
        source-address                        192.168.1.25
        application-protocol                  SIP
        trust-level                       high
access-control
        realm-id                          ACSRealm
        description                        Access Control for Microsoft ACS Direct Routing
        source-address                        52.114.0.0
        application-protocol                  SIP
        trust-level                       high
certificate-record
        name                              ACSSBCCertificate
        state                            TX
        locality                         Austin
        common-name                            solutionslab.cgbuburlington.com
        extended-key-usage-list                 serverAuth
                                       clientAuth
certificate-record
        name                              BaltimoreRoot
        common-name                            Baltimore CyberTrust Root
certificate-record
        name                              DigiCertInter
        common-name                            DigiCert SHA2 Secure Server CA
certificate-record
        name                              DigiCertRoot
        common-name                            DigiCert Global Root CA
codec-policy
        name                              OptimizeCodecs
        allow-codecs                        * G722:no SILK:no G726:no
codec-policy
        name                              addCN
        allow-codecs                        *
        add-codecs-on-egress                     CN
filter-config
        name                              all
        user                             *
http-server
        name                              webServerInstance
        http-interface-list                 GUI
local-policy
        from-address                        *
        to-address                        *
        source-realm                        ACSRealm
        description                        Route from ACS to PSTN
        policy-attribute
                next-hop                          192.168.1.25
                realm                           SIPTrunk
local-policy
        from-address                        *
        to-address                        *
        source-realm                    SIPTrunk
        policy-attribute
            next-hop                        sag:ACSGroup
            realm                           ACSRealm
    media-manager
        options                       audio-allow-asymmetric-pt
                                    xcode-gratuitous-rtcp-report-generation
    media-profile
        name                          SILK
        subname                         narrowband
        payload-type                    103
        clock-rate                    8000
    media-profile
        name                          SILK
        subname                         wideband
        payload-type                    104
        clock-rate                    16000
    media-sec-policy
        name                          RTP
    media-sec-policy
        name                          sdesPolicy
        inbound
            profile                         SDES
            mode                            srtp
            protocol                        sdes
        outbound
            profile                         SDES
            mode                            srtp
            protocol                        sdes
    network-interface
        name                          s0p0
        hostname                        solutionslab.cbguburlington.com
        ip-address                     141.146.36.70
        netmask                        255.255.255.192
        gateway                        141.146.36.65
        dns-ip-primary                   8.8.8.8
        dns-domain                       solutionslab.cgbuburlington.com
    network-interface
        name                          s1p0
        ip-address                     192.168.1.10
        netmask                        255.255.255.0
        gateway                        192.168.1.1
    ntp-config
        server                        141.146.36.99
    phy-interface
        name                          s0p0
        operation-type                  Media
    phy-interface
        name                          s1p0
        operation-type                  Media
        slot                        1
    realm-config
        identifier                    ACSRealm
        description                     Realm Facing ACS Direct Routing
        network-interfaces                 s0p0:0.4
        mm-in-realm                      enabled
        media-sec-policy                   sdesPolicy
        rtcp-mux                       enabled
        teams-fqdn                       solutionslab.cgbuburlington.com
        teams-fqdn-in-uri                  enabled
        sdp-inactive-only                  enabled
        access-control-trust-level            high
```



```
        codec-policy                    addCN
        rtcp-policy                     rtcpGen
realm-config
        identifier                      SIPTrunk
        description                     Realm Facing PSTN Services
        network-interfaces              s1p0:0.4
        mm-in-realm                     enabled
        media-sec-policy                RTP
        access-control-trust-level      high
        codec-policy                    OptimizeCodecs
rtcp-policy
        name                            rtcpGen
        rtcp-generate                   all-calls
sdes-profile
        name                            SDES
        lifetime                        31
session-agent
        hostname                        192.168.1.25
        ip-address                      192.168.1.25
        realm-id                        SIPTrunk
session-agent
        hostname                        sip.pstnhub.microsoft.com
        port                            5061
        transport-method                StaticTLS
        realm-id                        ACSRealm
        ping-method                     OPTIONS
        ping-interval                   30
        ping-response                   enabled
        refer-call-transfer             enabled
session-agent
        hostname                        sip2.pstnhub.microsoft.com
        port                            5061
        transport-method                StaticTLS
        realm-id                        ACSRealm
        ping-method                     OPTIONS
        ping-interval                   30
        ping-response                   enabled
        refer-call-transfer             enabled
session-agent
        hostname                        sip3.pstnhub.microsoft.com
        port                            5061
        transport-method                StaticTLS
        realm-id                        ACSRealm
        ping-method                     OPTIONS
        ping-interval                   30
        ping-response                   enabled
        refer-call-transfer             enabled
session-group
        group-name                      ACSGroup
        dest                            sip.pstnhub.microsoft.com
                                        sip2.pstnhub.microsoft.com
                                        sip3.pstnhub.microsoft.com
        sag-recursion                   enabled
sip-config
        registrar-domain                *
        registrar-host                  *
        options                         inmanip-before-validate
                                        max-udp-length=0
        allow-pani-for-trusted-only     disabled
        add-ue-location-in-pani         disabled
        npli-upon-register              disabled
sip-feature
```



```
        name                              replaces
        realm                             ACSRealm
        require-mode-inbound                         Pass
        require-mode-outbound                        Pass
sip-interface
        realm-id                          ACSRealm
        sip-port
                address                          141.146.36.70
                port                          5061
                transport-protocol                   TLS
                tls-profile                     TLSCGBUBURLINGTON
                allow-anonymous                        agents-only
        sip-profile                       forreplaces
sip-interface
        realm-id                          SIPTrunk
        sip-port
                address                          192.168.1.10
                allow-anonymous                        agents-only
sip-monitoring
        match-any-filter                     enabled
        monitoring-filters                   *
sip-profile
        name                              forreplaces
        replace-dialogs                       enabled
steering-pool
        ip-address                         141.146.36.70
        start-port                        10000
        end-port                           10999
        realm-id                          ACSRealm
steering-pool
        ip-address                         192.168.1.10
        start-port                        10000
        end-port                           10999
        realm-id                          SIPTrunk
system-config
        hostname                            solutionslab.cbguburlington.com
        description                        SBC for Azure Communication Services Direct Routing
        location                          Burlington, MA
        system-log-level                      NOTICE
        default-gateway                        10.138.194.129
tls-global
        session-caching                        enabled
tls-profile
        name                              TLSCGBUBURLINGTON
        end-entity-certificate                 ACSSBCCertificate
        trusted-ca-certificates                 DigiCertInter
                                      DigiCertRoot
                                      BaltimoreRoot
        mutual-authenticate                     enabled
```

10 Appendix A

10.1 SBC Behind NAT SPL Configuration

This configuration is needed when your SBC is behind a NAT device. This SPL is configured to avoid any loss in signaling or media traffic when the SBC is deployed behind a nat device or in a public cloud.

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 the “Support for SBC Behind NAT SPL plug-in” changes depends on the direction of the call.

Ie.. 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.

- The private IP address must be the same as the SIP Interface and Steering Pool IP address, both of which much match in the SBC’s configuration.
- The public IP address must be the public IP address of the NAT device

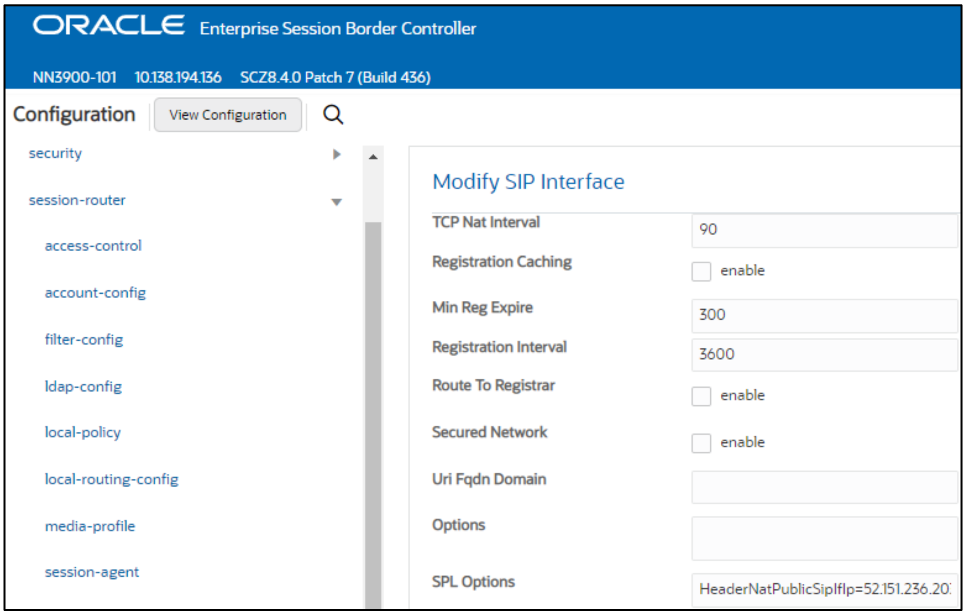
Here is an example configuration with SBC Behind NAT SPL config. The SPL is applied to the Microsoft ACS side SIP interface.

To configure SBC Behind NAT SPL Plug in, Go to:

session-router->sip-interface->spl-options and input the following value, save and activate. This is only an example:

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.0.4.4

Here HeaderNatPublicSipIfIp is the public ip of the nat device, and HeaderNatPrivateSipIfIp is the private ip configured on the SBC sip interface and steering pool



Modify SIP Interface

TCP Nat Interval: 90
Registration Caching: □ enable
Min Reg Expire: 300
Registration Interval: 3600
Route To Registrar: □ enable
Secured Network: □ enable
Uri Fqdn Domain:
Options:
SPL Options: HeaderNatPublicSipIfIp=52.151.236.20

11 Caveat

The OCSBC processes RTCP packets in two ways.

The first, as outlined in this application note, the Oracle SBC has the capability to use its own DSP resources to generate RTCP packets towards Microsoft ACS direct routing sip interface when PSTN does not have the ability to send RTCP.

The second, when both endpoints/agents involved in a call have the ability to send RTCP, the SBC will work as a pass-through by forwarding RTCP packets it receives unchanged to the other side.

When transcoding is enabled on the SBC, in some instances, the SBC will duplicate RTCP packets upon egress instead of just passing each individual packet through to the other side. If you experience this behavior, the resolution is to remove the codec polices from each realm. Once those transcoding (codec policies) are removed, the issue is resolved.

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/Oracle/

twitter.com/Oracle

oracle.com

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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services