Integration of Oracle SBC with Analog Devices and Microsoft Teams Direct Routing

Technical Application Note

Disclaimer

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

Contents

1 Revision History

Version	Date Revised	Description of Changes
1.0	04/17/2019	Initial publication
1.1	01/07/2022	Removed reference to sip-all FQDN
1.2	09/13/2022	Added Cert-record for DigiCert Global G2 Cert Added Access-Control
1.3	02/12/2024	Updated requirements for SBC’s end entity certificate
1.4	07/20/2024	Removed reference to ping-response parameter and added notes for using tls-global config in ACLI

2 Intended Audience

This document describes how to connect Analog Devices and the Oracle SBC to Microsoft Teams Direct Routing. This paper is intended for IT or telephony professionals.

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

3 Related Documentation

3.1 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
- https://docs.oracle.com/cd/F12246_01/doc/sbc_scz830_security.pdf

3.2 Microsoft Teams

- https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure
- https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants#create-a-trunk-and-provision-users
- https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

4 Validated Oracle Versions

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

SCZ830

Please visit https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers for further information.

These software releases with the configuration listed below can run on any of the following products:

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

5 About Teams Direct Routing

Microsoft Teams Direct Routing allows a customer provided SBC to connect to Microsoft Phone System. The customer provided SBC can be connected to almost any telephony trunk or interconnect 3rd party PSTN equipment. The scenario allows:

- Use virtually any PSTN trunk with Microsoft Phone System;
- Configure interoperability between customer-owned telephony equipment, such as 3rd party PBXs, analog devices, and Microsoft Phone System

6 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	
Office 365 tenant	
Domains	
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 ports for Direct Routing signaling	
Firewall IP addresses and ports for Direct Routing media	
Media Transport Profile	
Firewall ports for client media	

7 Configuration

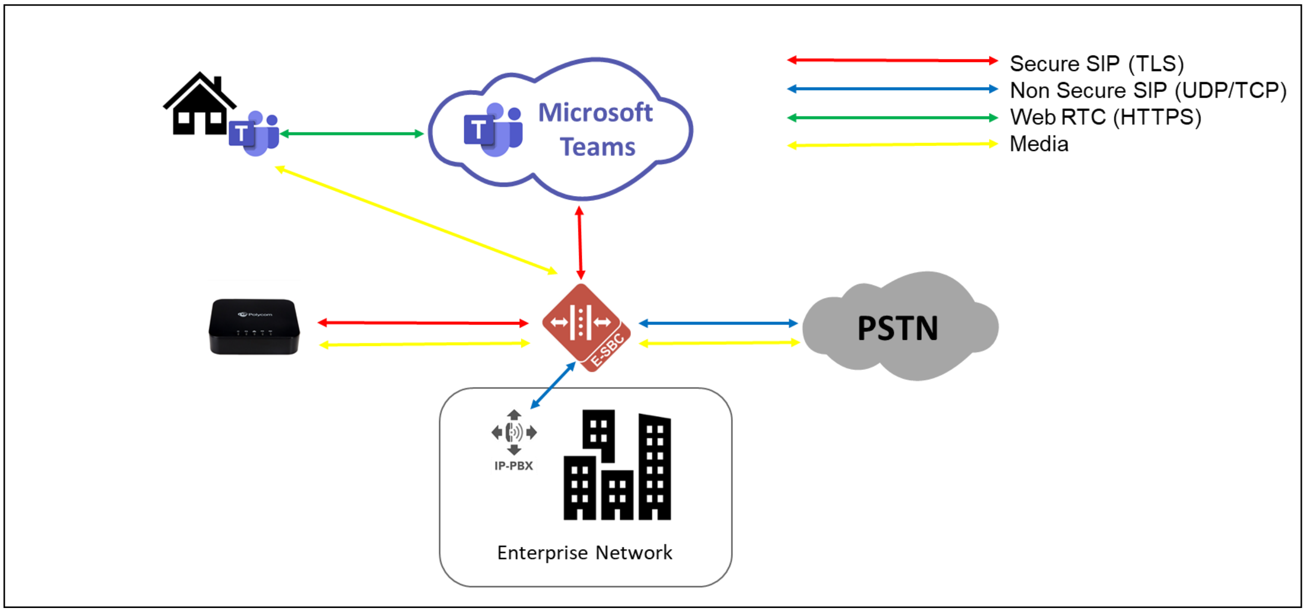
This chapter provides step-by-step guidance on how to configure Oracle SBC for interworking with Microsoft Teams Direct Routing Interface.

Below shows the connection topology example for MSFT Teams Carrier Model.
There are multiple connections shown:

- Teams Direct Routing Interface on the WAN
- Service provider Sip trunk terminating on the SBC
- Third Party ATA (Analog) device
- Third Party IP PBX (optional to use as registrar for ATA)

Note: Oracle did not implement a third party IP-PBX during the certification testing of analog devices with Microsoft Teams. The configuration outlined below demonstrates use of third party ATA (analog device) over secure transport direct to the Oracle SBC without registration or authentication.

Oracle SBC with Microsoft Teams Media Bypass and ATA Remote Worker



These instructions cover configuration steps for the Oracle SBC and Microsoft Teams Direct Routing Interface. The configuration 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.

7.1 Prerequisites

Before you begin, make sure that you have the following per every SBC you want to pair:

- Public IP address
- FQDN name for each registered subdomain representing individual tenants using the multitenant Direct Routing Trunk. Each FQDN must resolve to the Public IP address
- Public certificate, issued by one of the supported CAs (refer to Related Documentation for details about supported Certification Authorities).

7.2 About SBC Domain Name

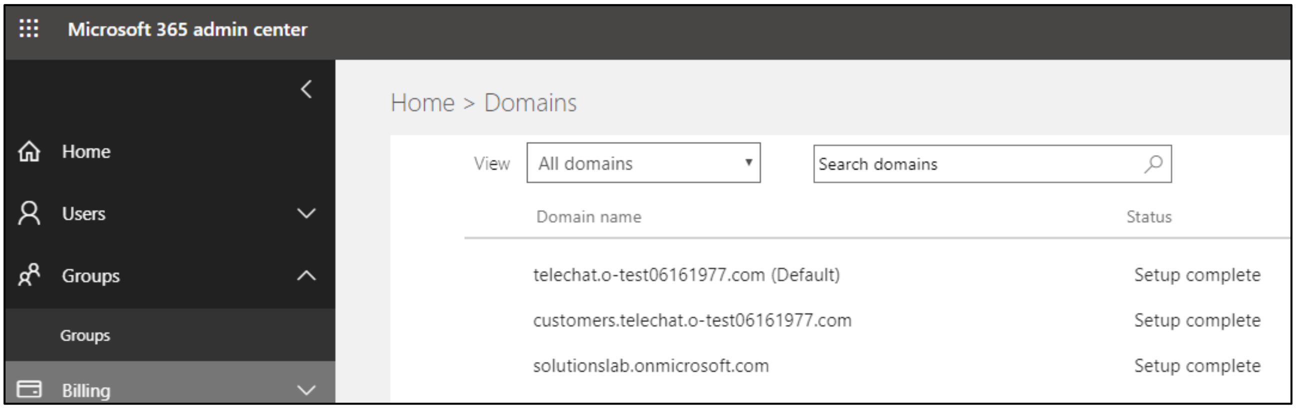
The SBC domain name must be from one of the names registered in “Domains” of the tenant. You cannot use the ***.onmicrosoft.com** tenant for the domain name. For example, on the picture below, the administrator registered the following DNS names for the tenant:.

DNS Name	Can Be Used For SBC	Example of FQDN names
telechat.o-test06161977.com	YES	**Valid FQDN:** • customers.telechat.o-test06161977.com • Sbc51. telechat.o-test06161977.com • Ussbc15. telechat.o-test06161977.com • Europe. telechat.o-test06161977.com **Invalid FQDN:** • Sbc1.europe.telechat.o-test06161977.com *(this would require registering domain name “Europe.adatum.biz”)*
solutionslab.onmicrosoft.com	NO	Using *.onmicrosoft.com domains is not supported for SBC names

Below is an example of registered DNS names in the customer tenant.

- **telechat.o-test06161977.com**

  Note: The above FQDN’s are examples only and not to be used outside of this document. Please use FQDN’s that are applicable to your environment.



Domain name	Status
telechat.o-test06161977.com (Default)	Setup complete
customers.telechat.o-test06161977.com	Setup complete
solutionslab.onmicrosoft.com	Setup complete

For the purposes of this example, the following IP address and FQDN is used:

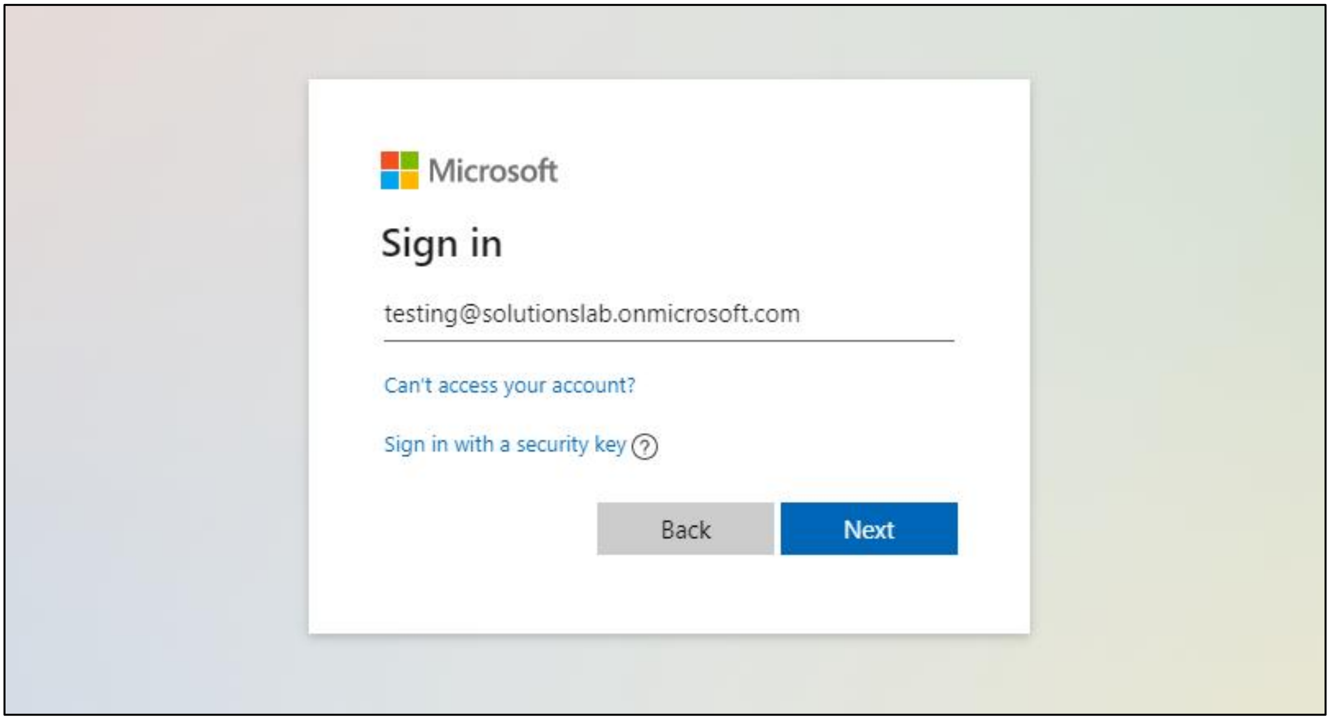
FQDN Names	Public IP Address
telechat.o-test06161977.com	141.146.36.68

8 Configure Direct Routing

The steps outlined below is the minimum required configuration to pair your SBC with Microsoft Teams Direct Routing Interface. This is to be used as an example only, and we highly recommend you work with your Microsoft Account representative to implement the correct configuration for your specific environment.

8.1.1 Access Teams Admin Center

The first step is to access the Teams Admin Center with administrator admin credentials:



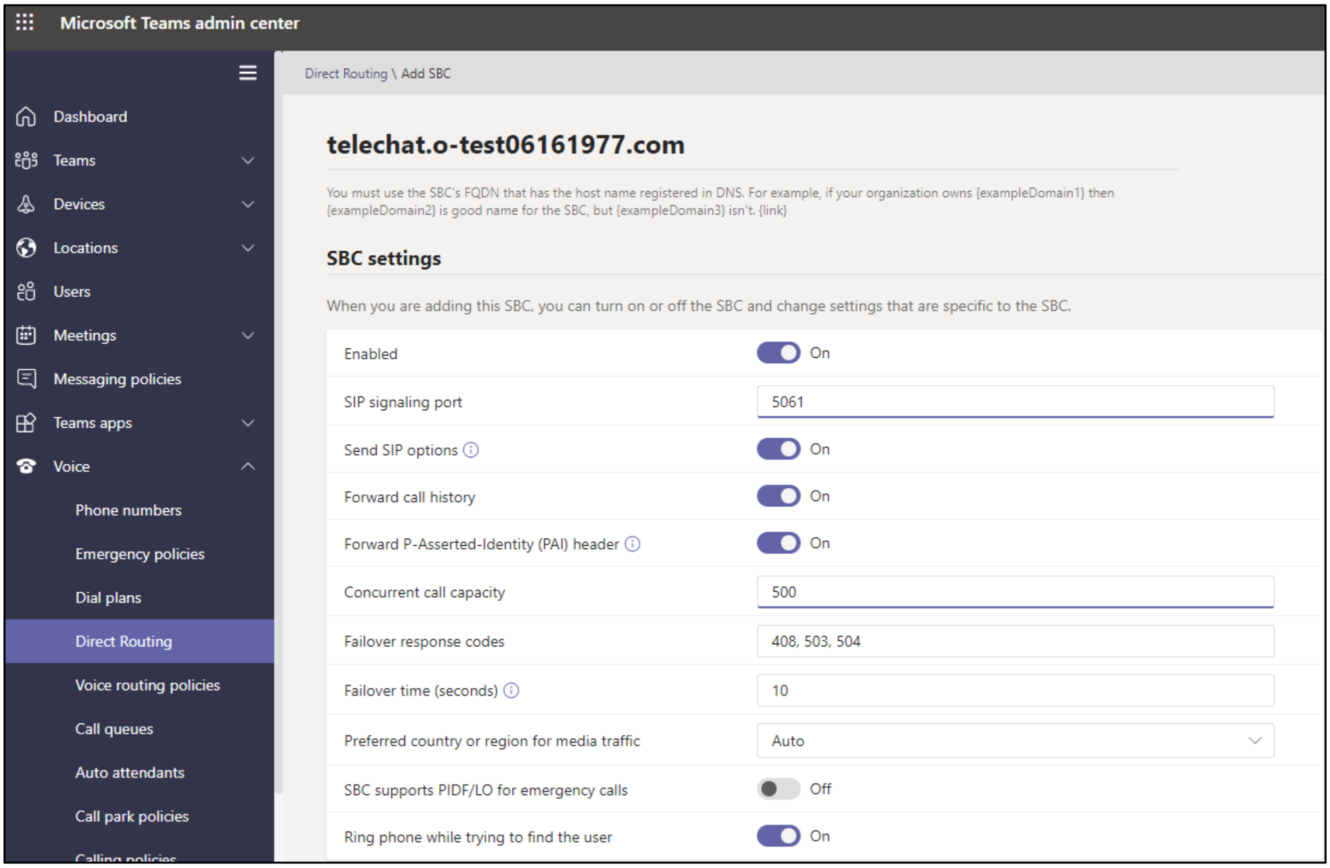
Microsoft

Sign in

testing@solutionslab.onmicrosoft.com

8.1.2 Configure Online PSTN Gateway

Configuration Path: Voice/Direct Routing/SBC



telechat.o-test06161977.com

You must use the SBC's FQDN that has the host name registered in DNS. For example, if your organization owns {exampleDomain1} then {exampleDomain2} is good name for the SBC, but {exampleDomain3} isn't. {link}

SBC settings

When you are adding this SBC, you can turn on or off the SBC and change settings that are specific to the SBC.

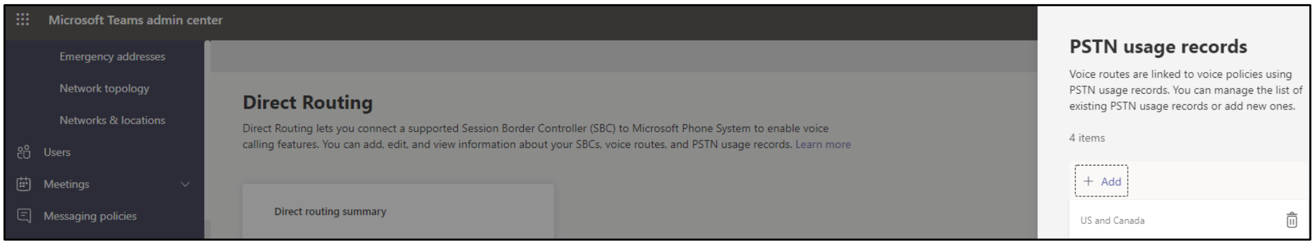
Enabled	On
SIP signaling port	5061
Send SIP options ⓘ	On
Forward call history	On
Forward P-Asserted-Identity (PAI) header ⓘ	On
Concurrent call capacity	500
Failover response codes	408, 503, 504
Failover time (seconds) ⓘ	10
Preferred country or region for media traffic	Auto
SBC supports PIDF/LO for emergency calls	Off
Ring phone while trying to find the user	On

- Click Save at the bottom of the page

8.1.3 Configure Online PSTN Usage

Configuration Path: Voice/Direct Routing/Manage PSTN usage Records (top right of screen)

Click Add, Type US and Canada, next, click Apply



Direct Routing

Direct Routing lets you connect a supported Session Border Controller (SBC) to Microsoft Phone System to enable voice calling features. You can add, edit, and view information about your SBCs, voice routes, and PSTN usage records. Learn more

PSTN usage records

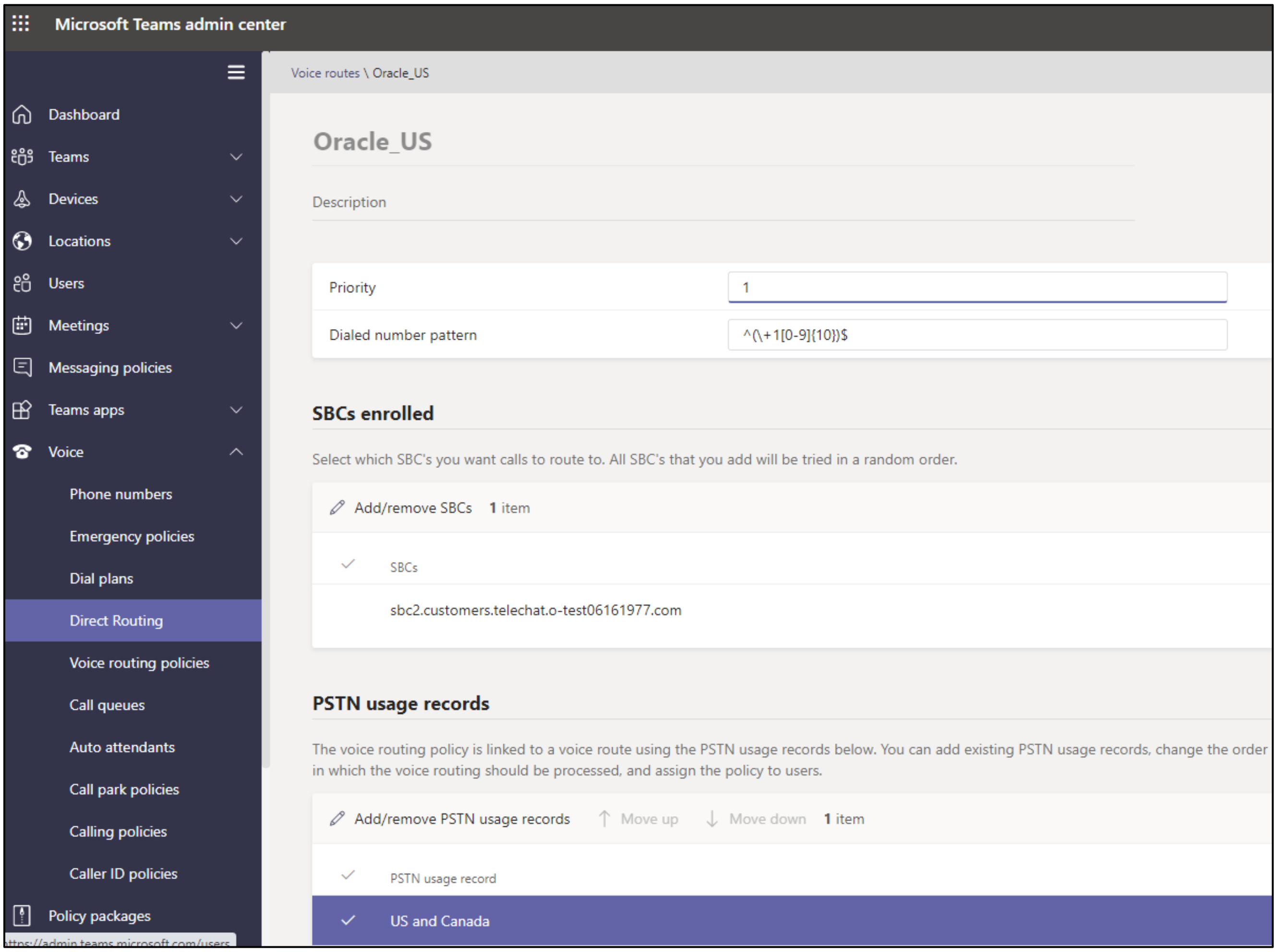
Voice routes are linked to voice policies using PSTN usage records. You can manage the list of existing PSTN usage records or add new ones.

4 items

US and Canada

8.1.5 Configure Online Voice Route

Configuration Path: Voice/Direct Routing/Voice Routes



Oracle_US

Description

Priority: 1

Dialed number pattern: ^(\+1[0-9]{10})$

SBCs enrolled

Select which SBC's you want calls to route to. All SBC's that you add will be tried in a random order.

SBCs
sbc2.customers.telechat.o-test06161977.com

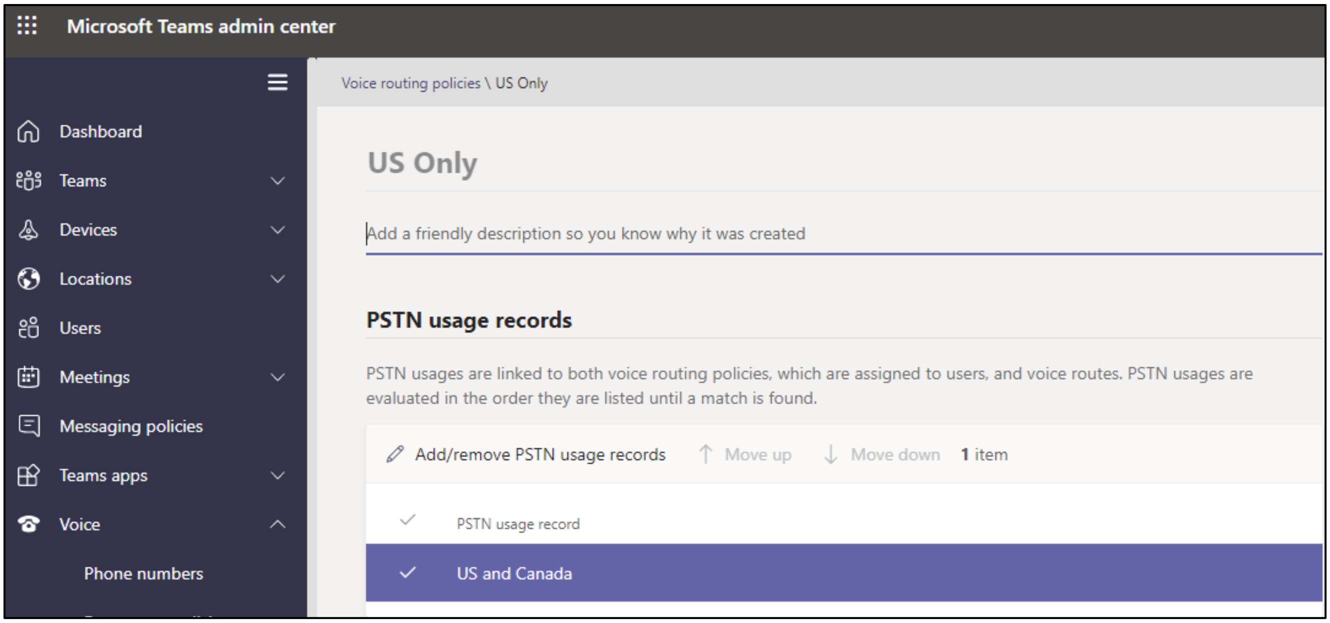
PSTN usage records

The voice routing policy is linked to a voice route using the PSTN usage records below. You can add existing PSTN usage records, change the order in which the voice routing should be processed, and assign the policy to users.

PSTN usage record
✓ US and Canada

8.1.6 Configure Voice Routing Policy

Configuration Path: Voice/Voice Routing Policies



US Only

Add a friendly description so you know why it was created

PSTN usage records

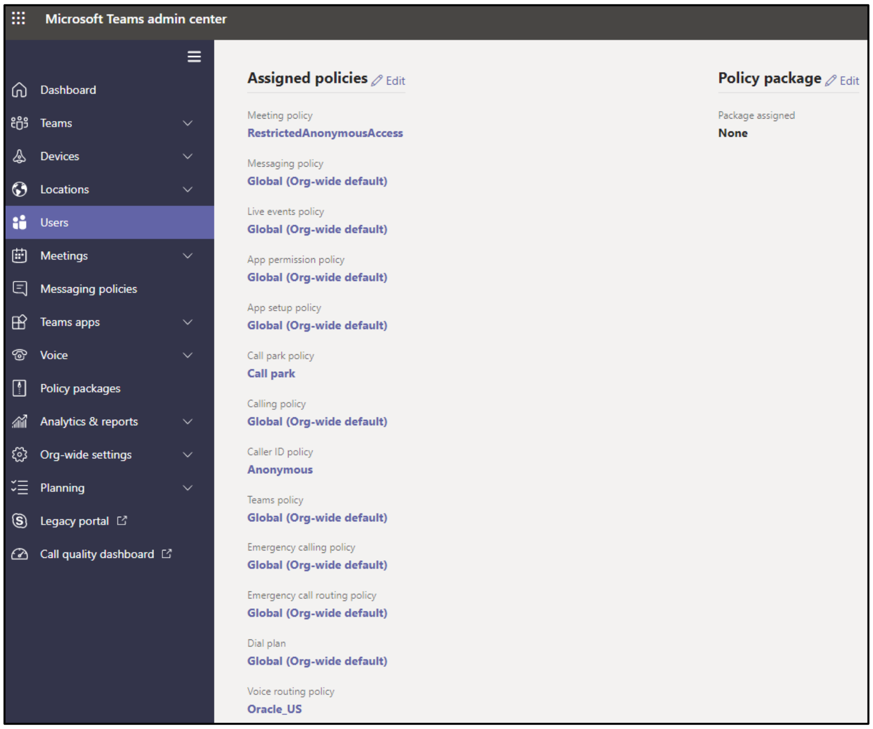
PSTN usages are linked to both voice routing policies, which are assigned to users, and voice routes. PSTN usages are evaluated in the order they are listed until a match is found.

✓	PSTN usage record
✓	US and Canada

8.1.7 Assign Voice Routing Policy to Users

Configuration Path: Users/Select the “User”/Policies

Next to Voice Routing Policy, Click Edit and Assign. In this example, we have selected Teamsuser1:



Assigned policies

Meeting policy
RestrictedAnonymousAccess

Messaging policy
Global (Org-wide default)

Live events policy
Global (Org-wide default)

App permission policy
Global (Org-wide default)

App setup policy
Global (Org-wide default)

Call park policy
Call park

Calling policy
Global (Org-wide default)

Caller ID policy
Anonymous

Teams policy
Global (Org-wide default)

Emergency calling policy
Global (Org-wide default)

Emergency call routing policy
Global (Org-wide default)

Dial plan
Global (Org-wide default)

Voice routing policy
Oracle_US

Policy package

Package assigned
None

For More Information about configuring Microsoft Teams to Connect to your SBC, Setting up users, or configuration voice routing, please refer to the Related Documentation Section of this guide.

9 Oracle SBC Configuration

There are two methods for configuing 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.

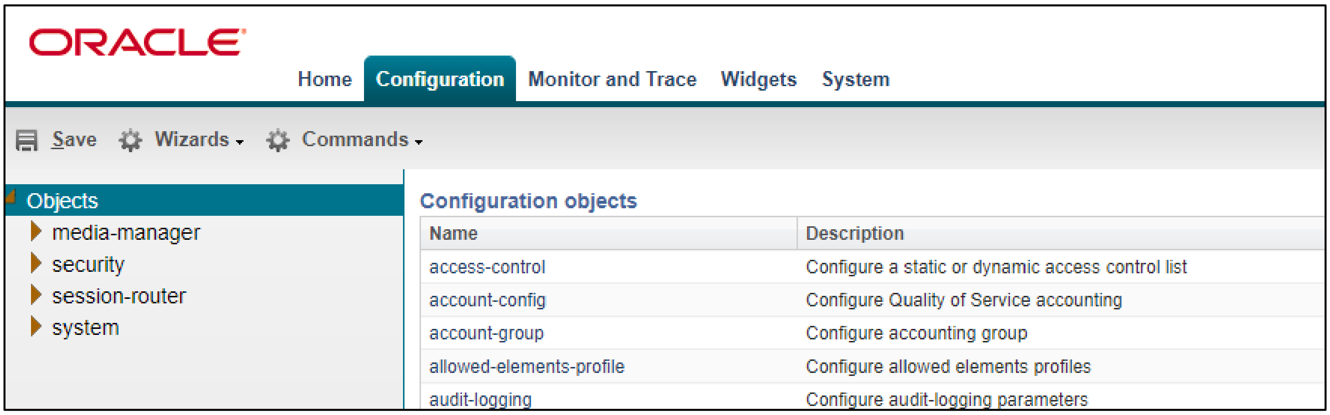
This guide assumes the OCSBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, web-server-config has been enabled for GUI access. If you require more information on how to install your SBC platform, please refer to the ACLI configuration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

To access the OCSBC GUI, enter the management IP address into a web brower.
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 for connection to MSFT Teams Direct routing or Analog device to function properly.

Please note, the below configuration example assumes Media Bypass is enabled on the MSFT Teams Tenant. This configuration example is based on the latest OCSBC software release, SCZ830M1P8A, which contains new parameters designed to simply the SBC's configuration for Microsoft Teams. If running a release prior to SCZ830m1p8A, please refer to Configuring the Oracle SBC with Microsoft Teams Direct Routing Media Bypass – Enterprise Model for instruction on how to configure.



Configuration objects

Name	Description
access-control	Configure a static or dynamic access control list
account-config	Configure Quality of Service accounting
account-group	Configure accounting group
allowed-elements-profile	Configure allowed elements profiles
audit-logging	Configure audit-logging parameters

9.1 Global Configuration Elements

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

- System-Config
- Media-manager-Config
- Sip-Config

9.1.1 System Config

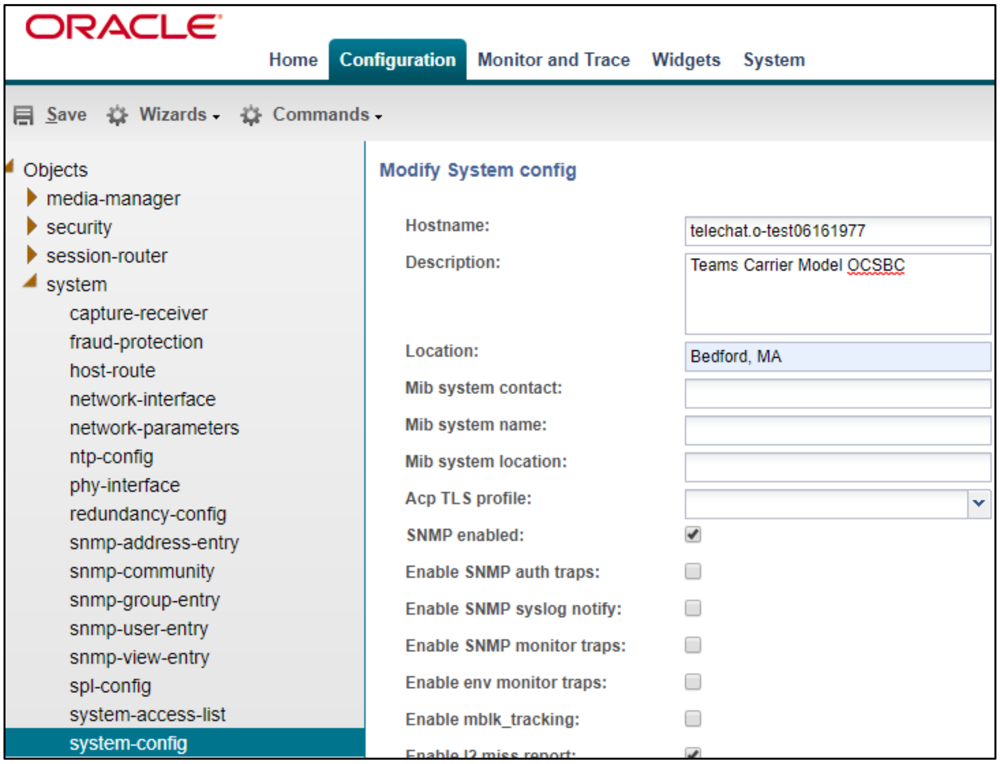
To configure system level functionality for the OCSBC, you must first enable the system-config

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



Modify System config

Hostname: telechat.o-test06161977
Description: Teams Carrier Model OCSBC
Location: Bedford, MA
Mib system contact:
Mib system name:
Mib system location:
Acp TLS profile:
SNMP enabled: ☑
Enable SNMP auth traps: □
Enable SNMP syslog notify: □
Enable SNMP monitor traps: □
Enable env monitor traps: □
Enable mblk_tracking: □
Enable l2 miss report: ☑

- Click the OK at the bottom of the screen

9.1.2 Media Manager

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

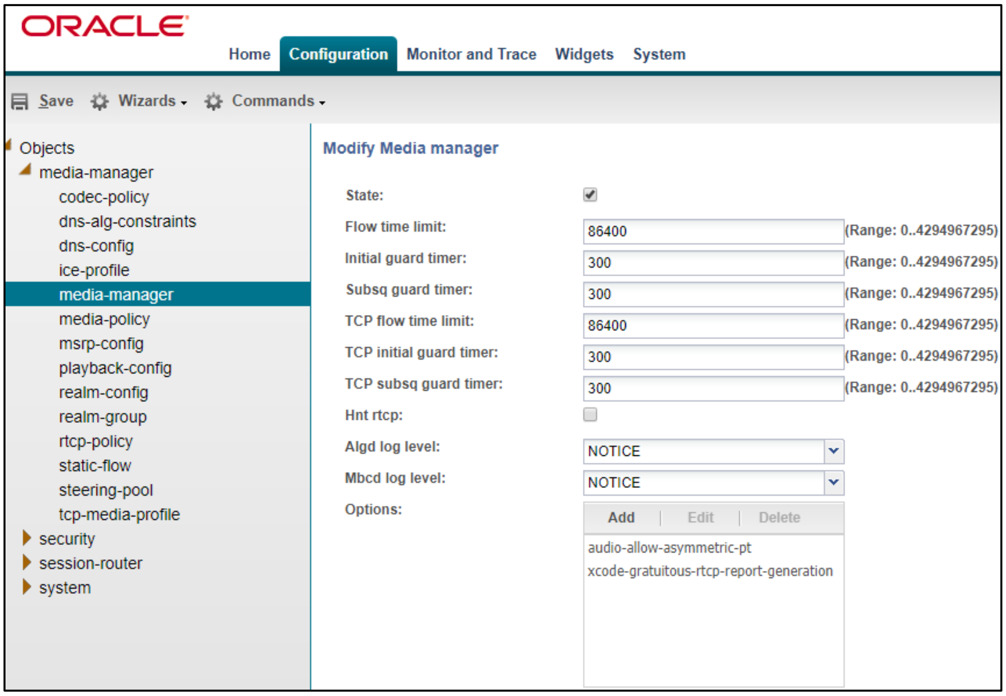
GUI Path: media-manager/media-manager

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: Click Add, in pop up box, enter the string: audio-allow-asymmetric-pt
- Click Apply/Add Another, then enter: xcode-gratuitous-rtcp-report-generation (requires a reboot to take effect)

- Max-Untrusted-Signalling=1
- Min-Untrusted-Signalling=1
- Hit OK in the box



Modify Media manager

State:	☑	
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:	☐	
Algd log level:	NOTICE	
Mbcd log level:	NOTICE	
Options:	audio-allow-asymmetric-pt xcode-gratuitous-rtcp-report-generation	

9.1.3 Sip Config

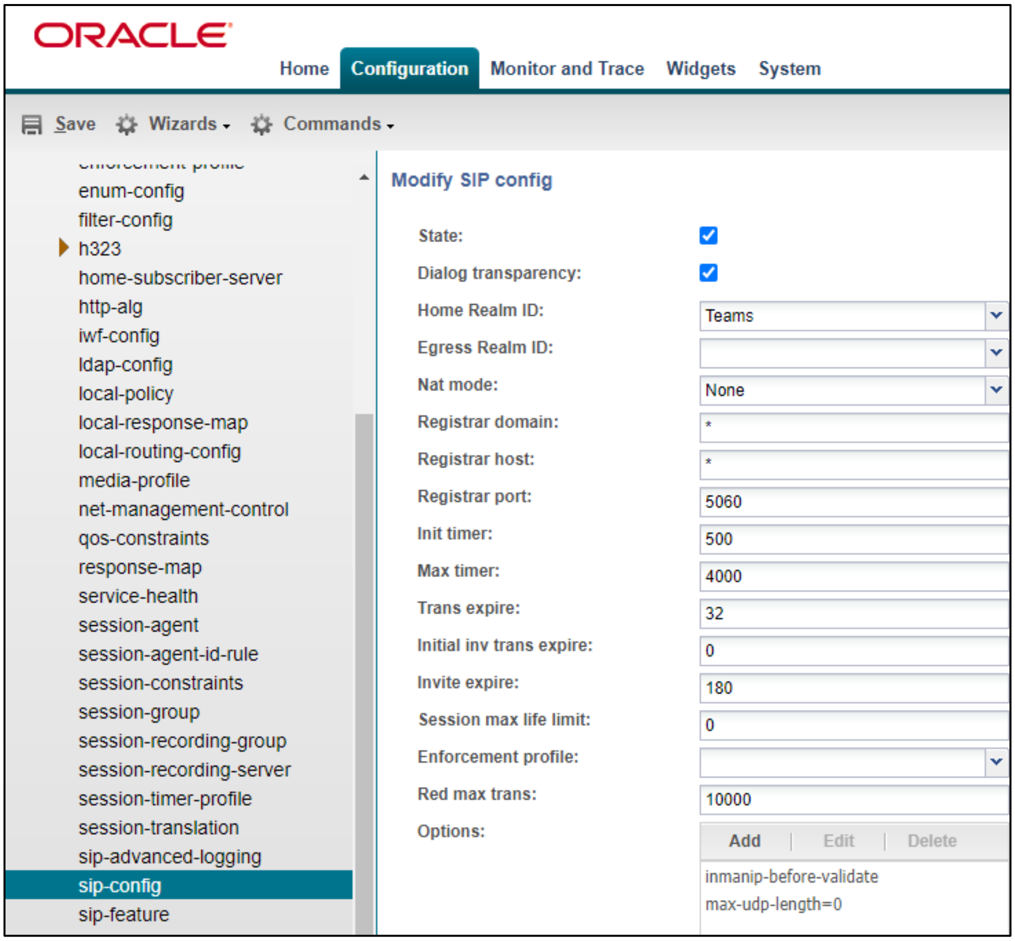
To enable sip related objects on the OCSBC, you must first configure the global Sip Config element:

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: Click Add, in pop up box, enter the string: inmanip-before-validate
- Click Apply/Add another, then enter: max-udp-length=0
- Press OK in box



Modify SIP config

State:	☑
Dialog transparency:	☑
Home Realm ID:	Teams
Egress Realm ID:	
Nat mode:	None
Registrar domain:	*
Registrar host:	*
Registrar port:	5060
Init timer:	500
Max timer:	4000
Trans expire:	32
Initial inv trans expire:	0
Invite expire:	180
Session max life limit:	0
Enforcement profile:	
Red max trans:	10000
Options:	inmanip-before-validate max-udp-length=0

Note: If using the SBC in an access environment to register ATA with IP-PBX, please check the Oracle SBC Configuration guide regarding proper setting for home realm, registrar-host, and registrar-port.

- Click OK at the bottom

9.2 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 three physical interfaces, and three network interfaces. One to communicate with MSFT Teams Direct Routing, one to connect to PSTN Network, and a third to communicate with the Analog Device

9.2.1 Physical Interfaces

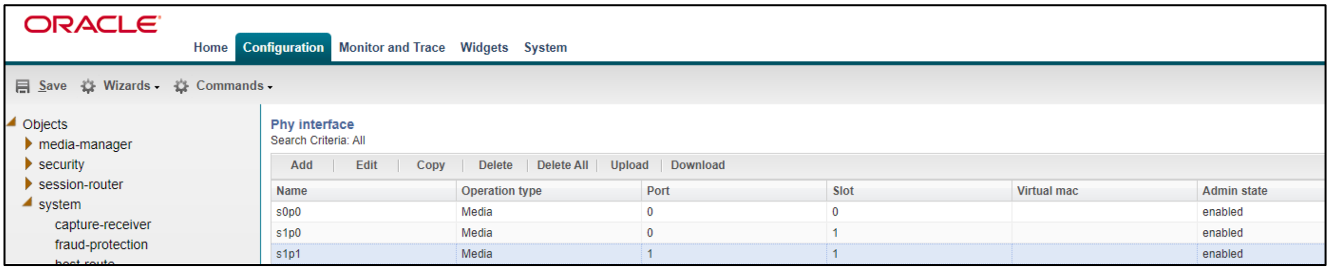
GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

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

Config Parameter	Teams	PSTN	ATA
Name	s0p0	S1p0	S1p1
Operation Type	Media	Media	Media
Slot	0	1	1
Port	0	0	1

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



Phy interface
Search Criteria: All

Name	Operation type	Port	Slot	Virtual mac	Admin state
s0p0	Media	0	0		enabled
s1p0	Media	0	1		enabled
s1p1	Media	1	1		enabled

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

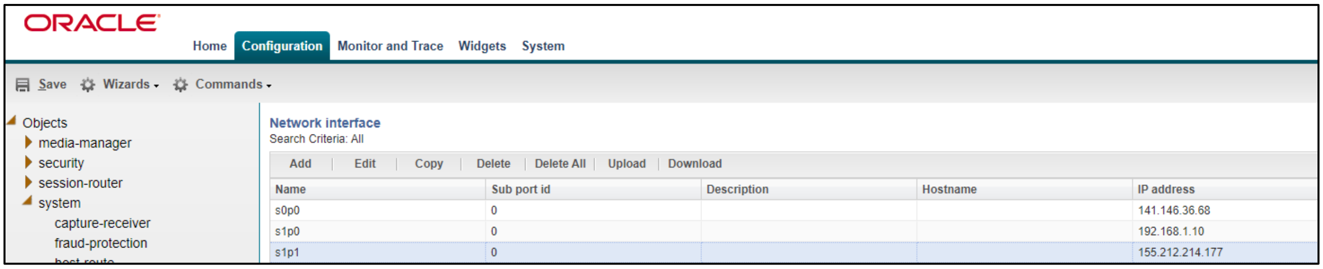
9.2.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

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

Configuration Parameter	Teams	PSTN	ATA
Name	s0p0	s1p0	S1p0
Hostname	(Optional)		
IP Address	141.146.36.68	192.168.1.10	155.212.214.177
Netmask	255.255.255.192	255.255.255.0	255.255.255.0
Gateway	141.146.36.65	192.168.1.1	155.212.214.1
DNS Primary IP	8.8.8.8		
DNS Domain	Carrier Default Domain		



Network interface
Search Criteria: All

Name	Sub port id	Description	Hostname	IP address
s0p0	0			141.146.36.68
s1p0	0			192.168.1.10
s1p1	0			155.212.214.177

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

9.3 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Teams Direct Routing and ATA interfaces

Microsoft Teams Direct Routing only allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by one fo the trusted Cerificate Authorities. A list of currently supported Certificate Authrities can be found at:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

9.3.1 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)
- GoDaddy Root Cert (Root CA used to sign the SBC's end entity certificate)
- BaltimoreRoot CA Cert (Microsoft Presents the SBC a certficate signed by this authority)
- DigiCert Global G2 Cert (Microsoft Presents the SBC a certficate signed by this authority)

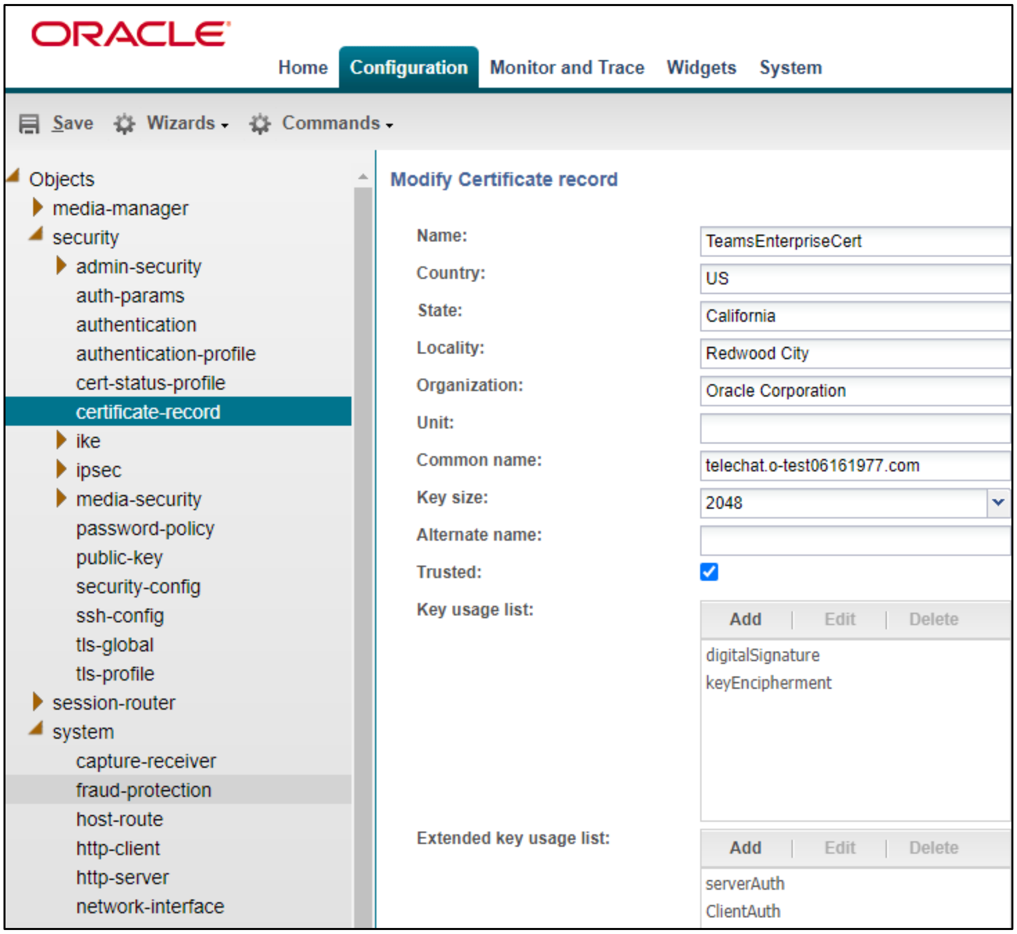
9.3.2 SBC End Entity Certificate

The SBC's end entity certificate is based on the domain structure outlined in the Configuration section of this document. This certificate record must include the following:

- Common name: SBC Domain Name (**telechat.o-test06161977.com**)
- Extended Key Usage List: serverAuth clientAuth

To Configure the certificate record:

- Click Add, and configure the SBC certificate as shown below:



Modify Certificate record

Name:	TeamsEnterpriseCert
Country:	US
State:	California
Locality:	Redwood City
Organization:	Oracle Corporation
Unit:	
Common name:	telechat.o-test06161977.com
Key size:	2048
Alternate name:	
Trusted:	☑
Key usage list:	digitalSignature keyEncipherment
Extended key usage list:	serverAuth ClientAuth

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

9.3.2.1 Root CA and Intermediate Certificates

9.3.2.1.1 Go Daddy Root

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

9.3.2.1.2 DigiCert Global Root G2

The DNS name of the Microsoft Teams Direct Routing interface is sip.pstnhub.microsoft.com. Microsoft presents a certificate to the SBC which is signed by DigiCert Global Root G2.To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate. You can download this certificate here: DigiCert Global Root G2

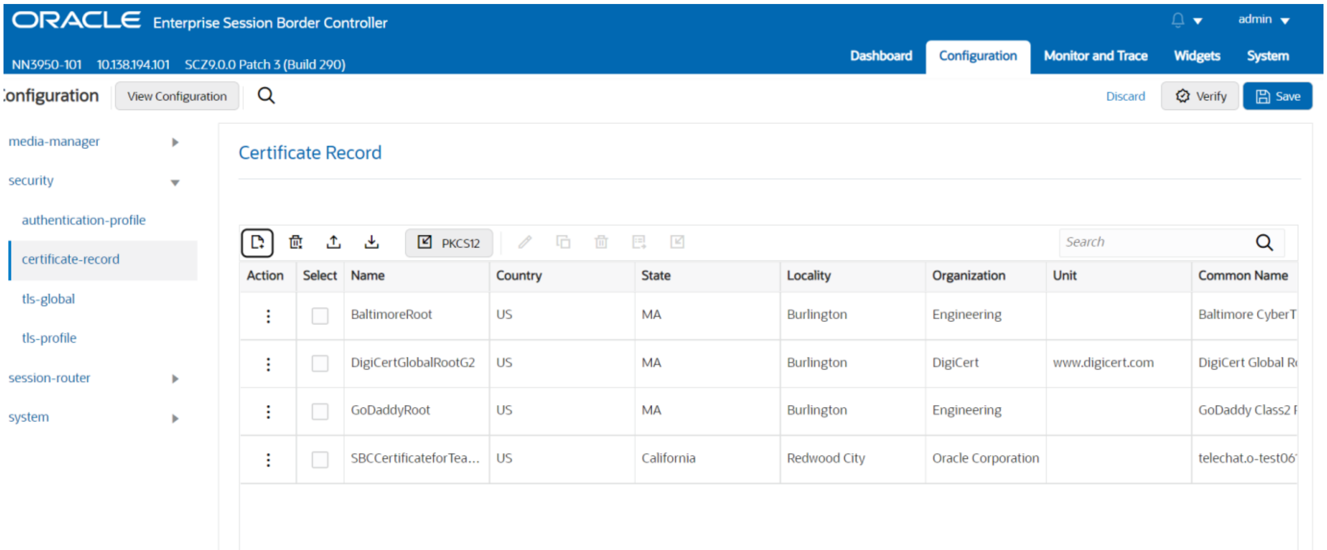
9.3.2.1.3 Baltimore Root

The DNS name of the Microsoft Teams Direct Routing interface is sip.pstnhub.microsoft.com. 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 listed as a trusted ca certificate.

You can download this certificate here: https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt.pem

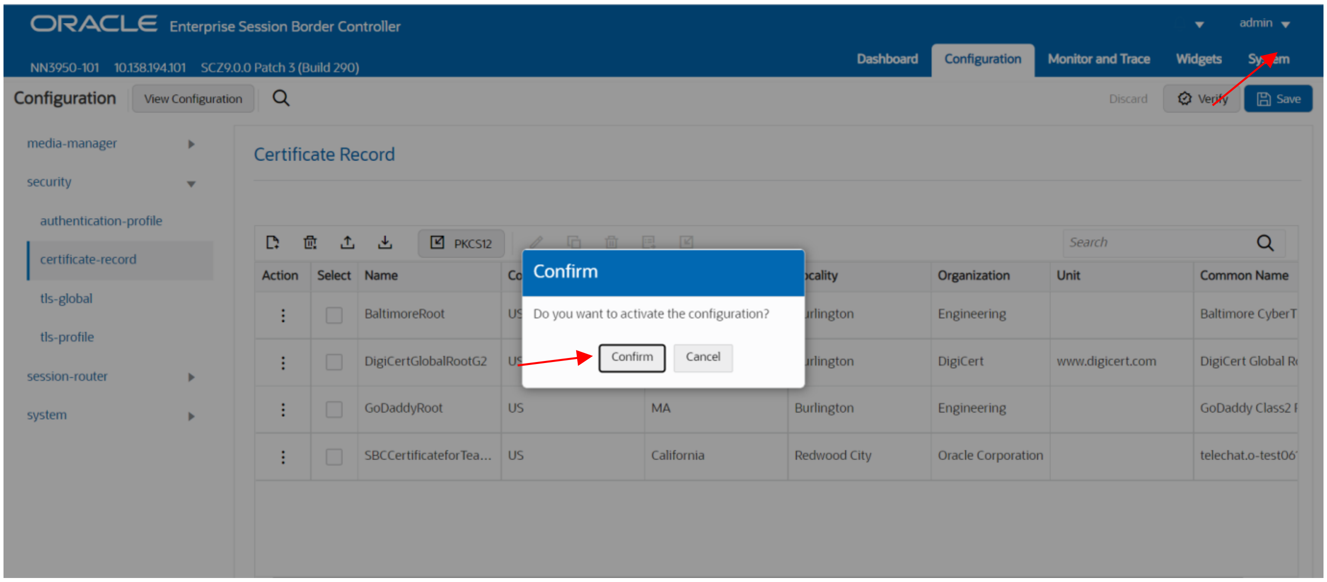
Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

Config Parameter	**Baltimore Root**	**GoDaddy Root**	DigiCert Global Root G2
Common Name	Baltimore CyberTrust Root	Go Daddy Class2 Root CA	DigiCert Global Root G2
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



Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
⋮	□	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberT
⋮	□	DigiCertGlobalRootG2	US	MA	Burlington	DigiCert	www.digicert.com	DigiCert Global R
⋮	□	GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 F
⋮	□	SBCCertificateforTea...	US	California	Redwood City	Oracle Corporation		telechat.o-test06

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.



Certificate Record

Action	Select	Name	Co		ocality	Organization	Unit	Common Name
⋮	□	BaltimoreRoot	US		rlington	Engineering		Baltimore CyberT
⋮	□	DigiCertGlobalRootG2	US		rlington	DigiCert	www.digicert.com	DigiCert Global R
⋮	□	GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 F
⋮	□	SBCCertificateforTea...	US	California	Redwood City	Oracle Corporation		telechat.o-test06

Confirm

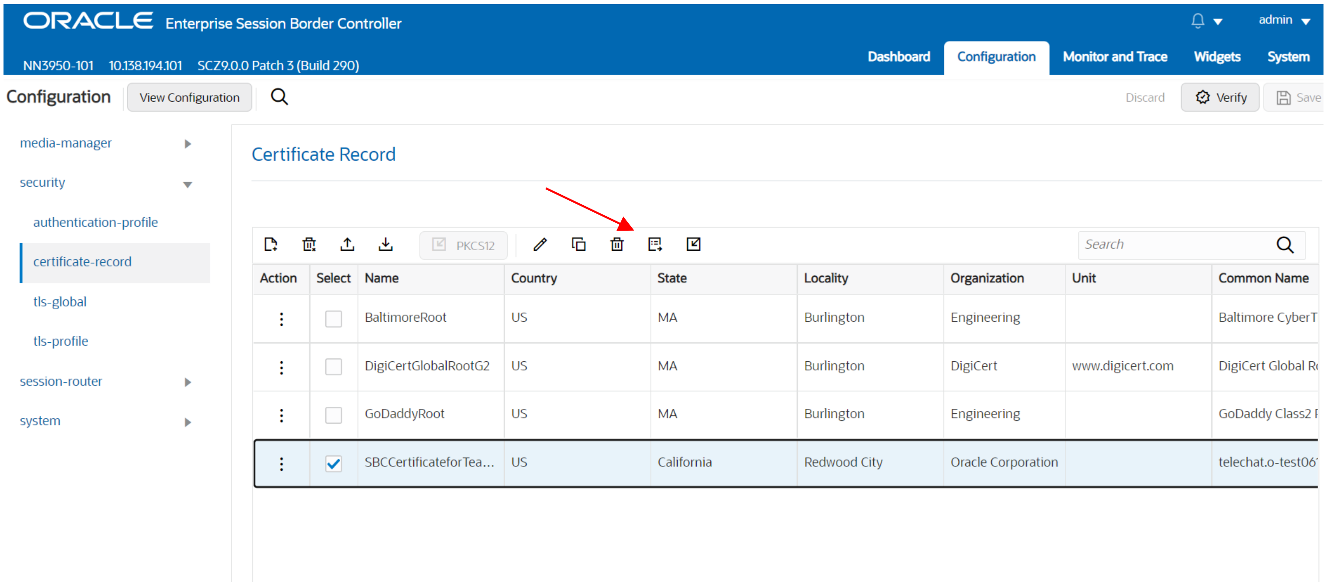
Do you want to activate the configuration?

Confirm Cancel

9.3.2.2 Generate Certificate Signing Request

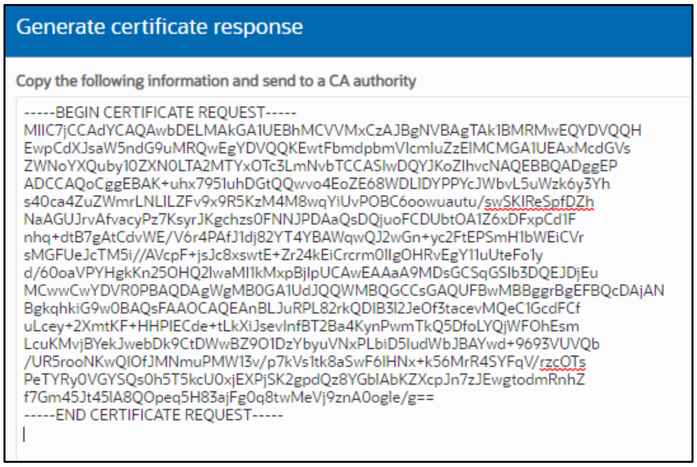
Now that the SBC's certificate has been configured, create a certificate signing request for the SBC's end entity only. **This is not required for any of the Root CA or intermidiate certificates that have been created**.

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:



Certificate Record

Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
⋮	□	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberT
⋮	□	DigiCertGlobalRootG2	US	MA	Burlington	DigiCert	www.digicert.com	DigiCert Global R
⋮	□	GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 F
⋮	☑	SBCCertificateforTea...	US	California	Redwood City	Oracle Corporation		telechat.o-test06



Generate certificate response

Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwbDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEIMCMGA1UEAxMcdGVs
ZWNoYXQuby10ZXN0LTA2MTYxOTc3LmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAK+uhx7951uhDGtQQwvo4EoZE68WDLIDYPPYcJWbvL5uWzk6y3Yh
s40ca4ZuZWmrLNLILZFv9x9R5KzM4M8wqYiUvPOBC6oowuautu/swSKIReSpfDZh
NaAGUJrvAfvacyPz7KsyrJKgchzs0FNNJPDAaQsDQjuoFCDUbtOA1Z6xDFxpCd1F
nhq+dtB7gAtCdvWE/V6r4PAfJ1dj82YT4YBAWqwQJ2wGn+yc2FtEPSmH1bWEiCVr
sMGFUeJcTM5i//AVcpF+jsJc8xswtE+Zr24kEiCrcrm0IlgOHRvEgY11uUteFo1y
d/60oaVPYHgkKn25OHQ2lwaMI1kMxpBjlpUCAwEAAaA9MDsGCSqGSIb3DQEJDjEu
MCwwCwYDVR0PBAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAN
BgkqhkiG9w0BAQsFAAOCAQEAnBLJuRPL82rkQDIB3I2JeOf3tacevMQeC1GcdFCf
uLcey+2XmtKF+HHPIECde+tLkXiJsevInfBT2Ba4KynPwmTkQ5DfoLYQjWFOhEsm
LcuKMvjBYekJwebDk9CtDWwBZ9O1DzYbyuVNxPLbiD5ludWbJBAYwd+9693VUVQb
/UR5rooNKwQIOfJMNmuPMW13v/p7kVs1tk8aSwF6IHNx+k56MrR4SYFqV/rzcOTs
PeTYRy0VGYSQs0h5T5kcU0xjEXPjSK2gpdQz8YGbIAbKZXcpJn7zJEwgtodmRnhZ
f7Gm45Jt45IA8QOpeq5H83ajFg0q8twMeVj9znA0ogle/g==
-----END CERTIFICATE REQUEST-----
```

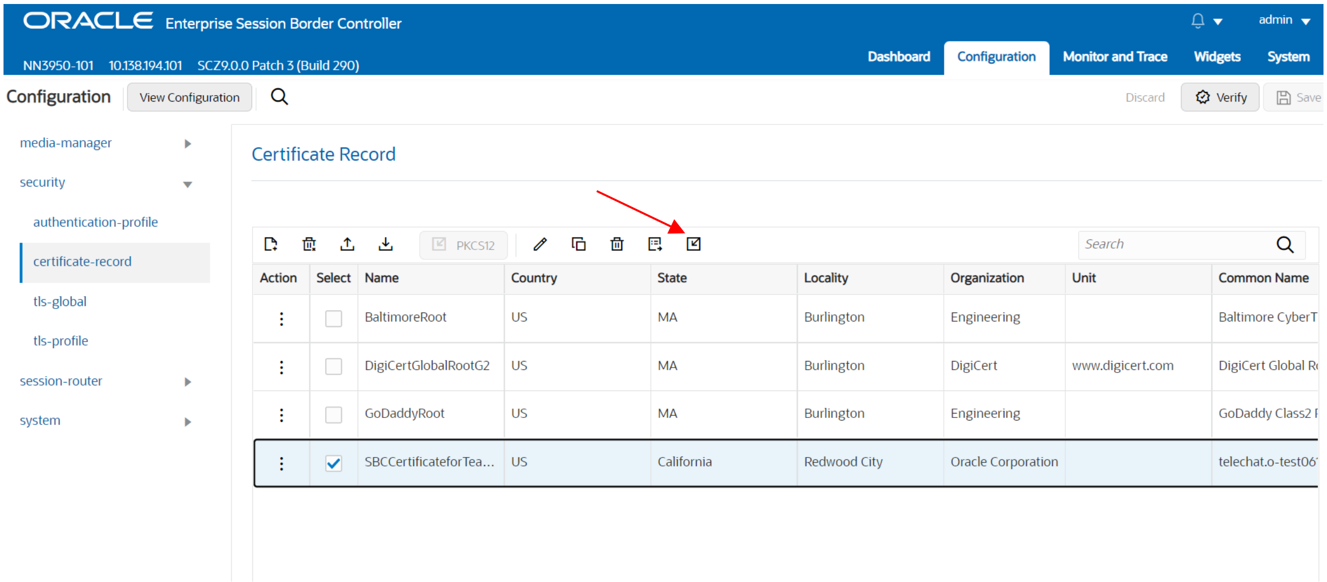
Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, at this point, **another save and activate is required** before you can import the certificates to each certificate record created above.

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

9.3.2.3 Import Certificates to SBC

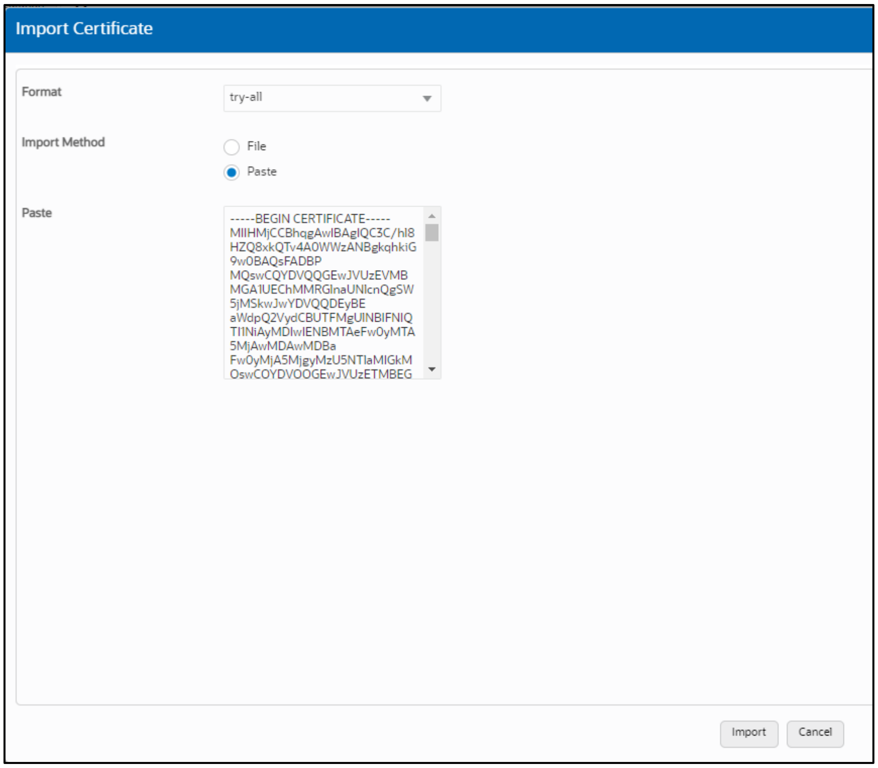
Once certificate signing request has been completed – import the signed certificate to the SBC.

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.



Certificate Record

Action	Select	Name	Country	State	Locality	Organization	Unit	Common Name
⋮	☐	BaltimoreRoot	US	MA	Burlington	Engineering		Baltimore CyberT
⋮	☐	DigiCertGlobalRootG2	US	MA	Burlington	DigiCert	www.digicert.com	DigiCert Global R
⋮	☐	GoDaddyRoot	US	MA	Burlington	Engineering		GoDaddy Class2 F
⋮	☑	SBCCertificateforTea...	US	California	Redwood City	Oracle Corporation		telechat.o-test06



Import Certificate

Format: try-all

Import Method: ○ File ● Paste

Paste:

```
-----BEGIN CERTIFICATE-----
MIIHMjCCBhqgAwIBAgIQC3C/hI8
HZQ8xkQTv4A0WWzANBgkqhkiG
9w0BAQsFADBP
MQswCQYDVQQGEwJVUzEVMB
MGA1UEChMMRGlnaUNlcnQgSW
5jMSkwJwYDVQQDEyBE
aWdpQ2VydCBUTFMgUlNBIFNIQ
TI1NiAyMDIwIENBMTAeFw0yMTA
5MjAwMDAwMDBa
Fw0yMjA5MjgyMzU5NTlaMIGkM
QswCQYDVQQGEwJVUzETMBEG
```

- 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:

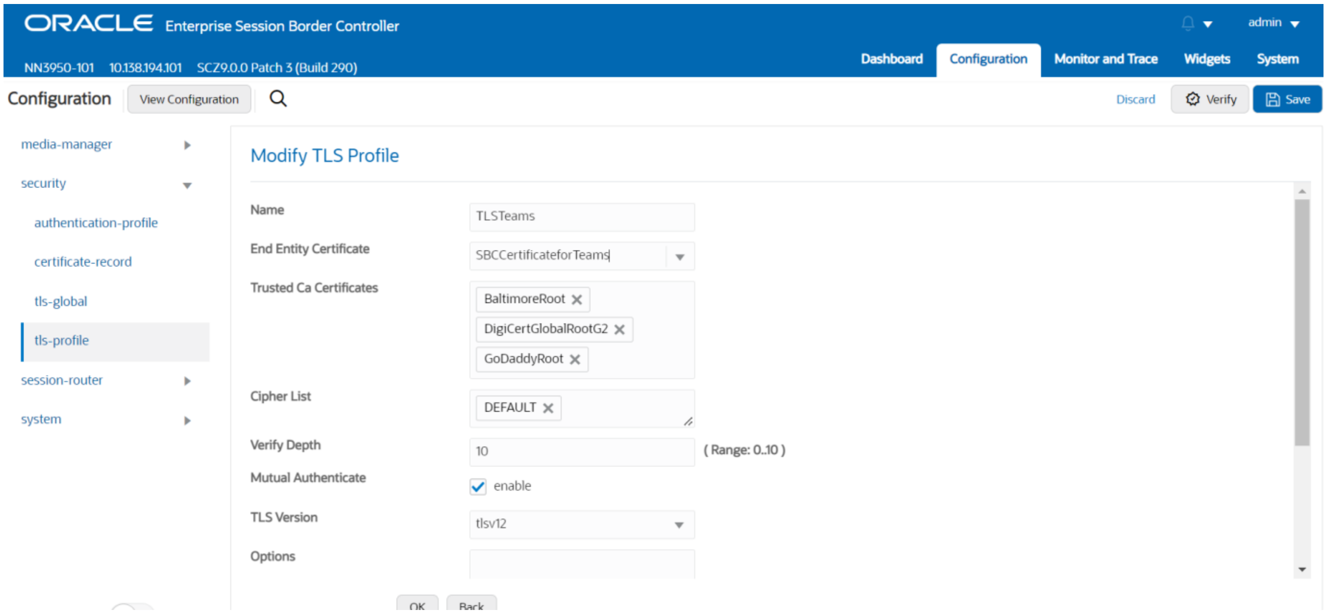
9.3.3 TLS Profile

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: TLSTeams

End Entity Certificate: SBCCertificateforTeams

Trusted Ca Certificates: BaltimoreRoot, DigiCertGlobalRootG2, GoDaddyRoot

Cipher List: DEFAULT

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

Mutual Authenticate: ☑ enable

TLS Version: tlsv12

Options:

- Select OK at the bottom

Next, we’ll move to securing media between the SBC and Microsoft Teams.

9.3.4 Media Security Configuration

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

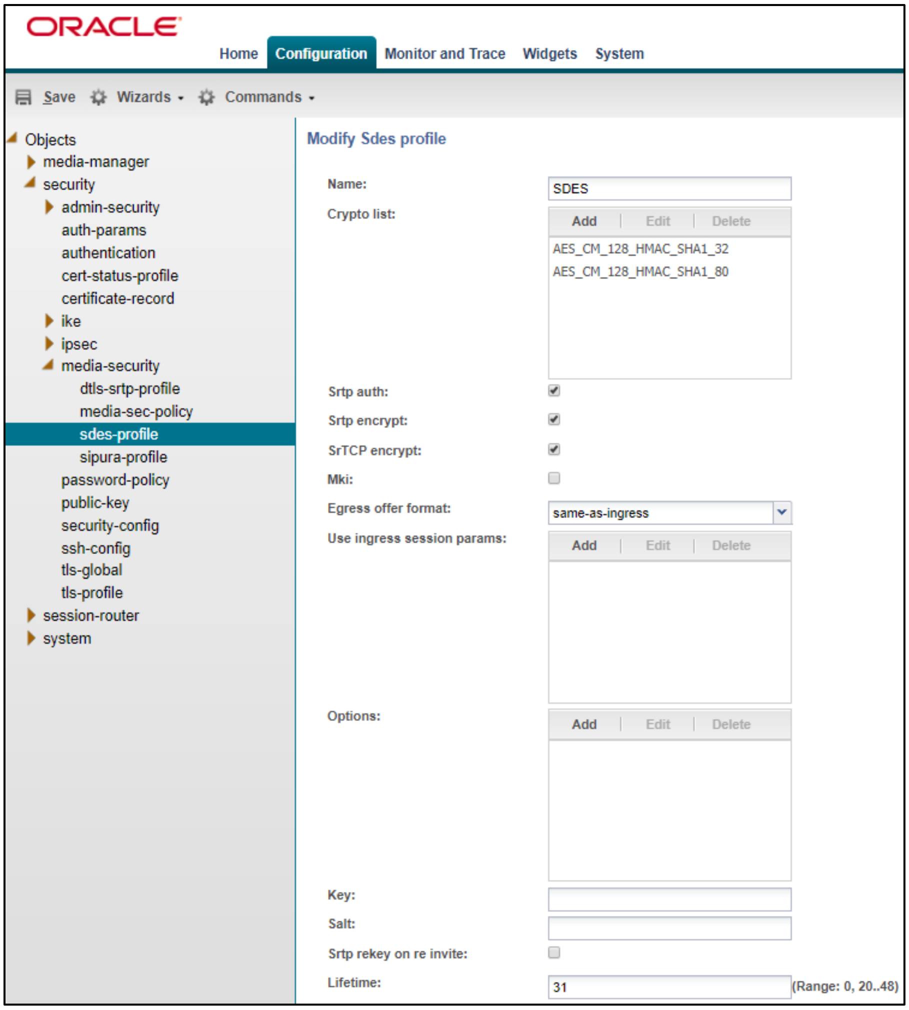
9.3.5 Sdes-profile

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



Modify Sdes profile

Name: SDES

Crypto list:
AES_CM_128_HMAC_SHA1_32
AES_CM_128_HMAC_SHA1_80

Srtp auth: ☑

Srtp encrypt: ☑

SrTCP encrypt: ☑

Mki: □

Egress offer format: same-as-ingress

Use ingress session params:

Options:

Key:

Salt:

Srtp rekey on re invite: □

Lifetime: 31 (Range: 0, 20..48)

Note: The lifetime parameter set to a value of 31 is required if utilizing Media Bypass on Microsoft Teams

- Click OK at the bottom

9.3.6 Media Security Policy

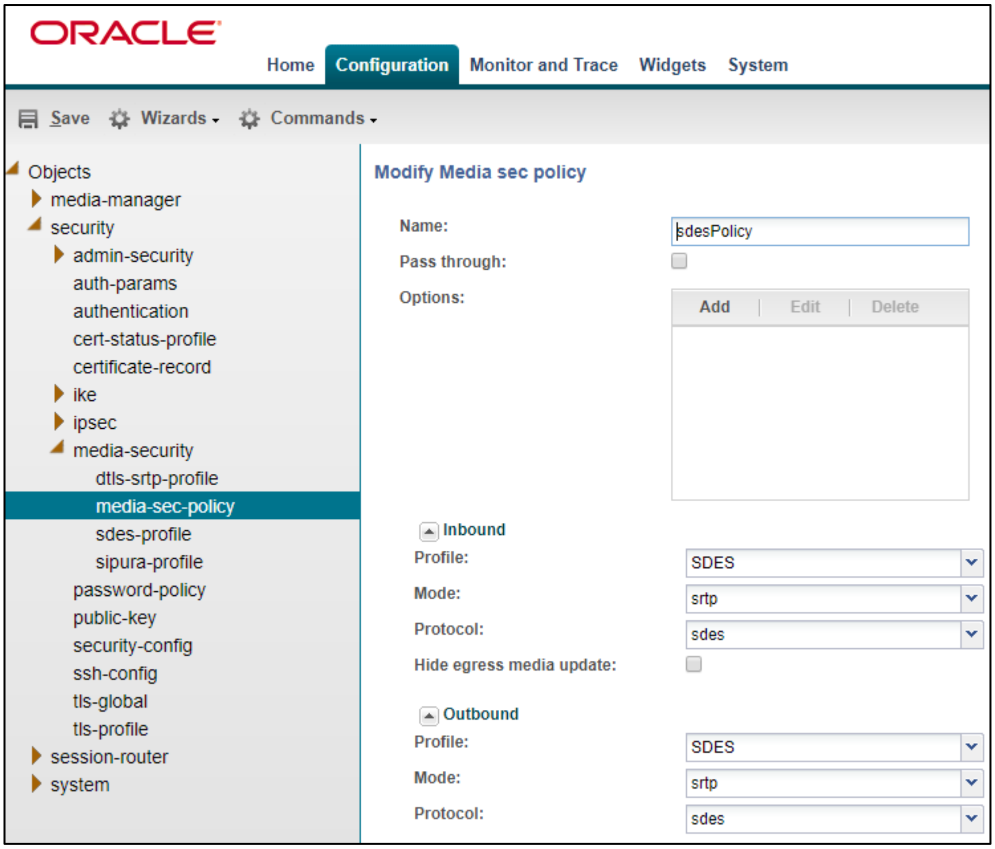
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them) and, if SRTP needs to be used, the sdes-profile that needs to be used

In this example, we are configuring two media security policies. One to secure and decrypt media toward Microsoft Teams, 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: □

Options:

Inbound

Profile: SDES

Mode: srtp

Protocol: sdes

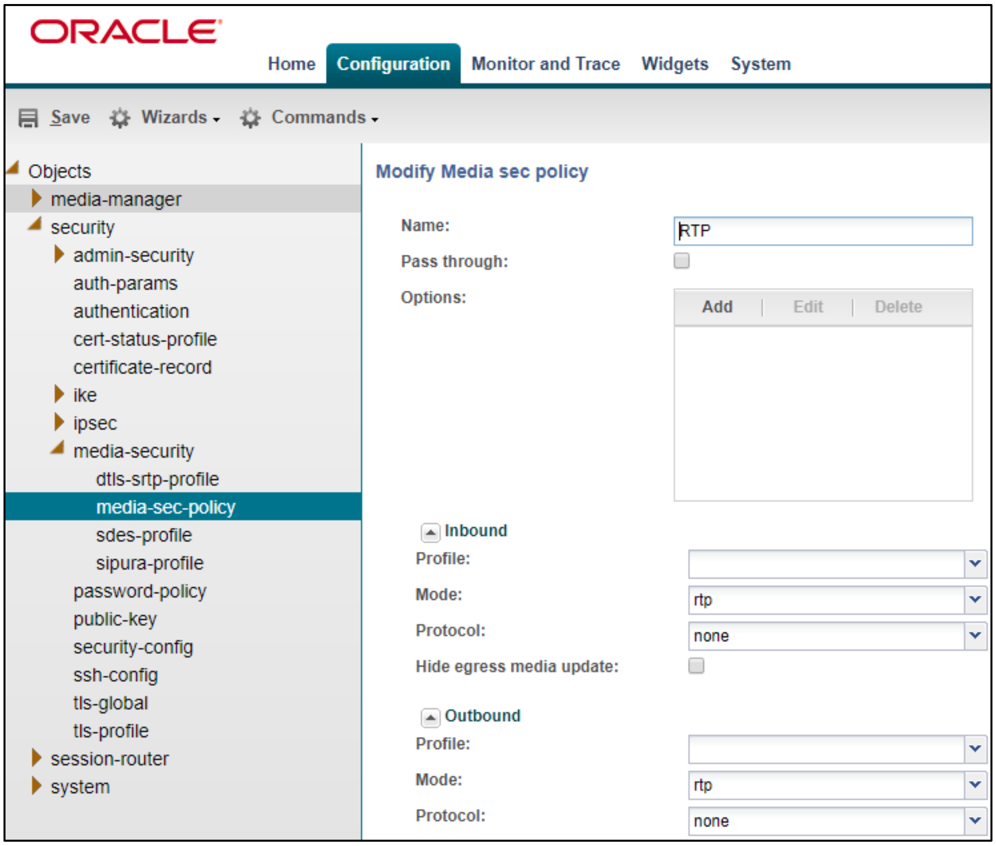
Hide egress media update: □

Outbound

Profile: SDES

Mode: srtp

Protocol: sdes



Modify Media sec policy

Name: RTP

Pass through: □

Options:

Inbound

Profile:

Mode: rtp

Protocol: none

Hide egress media update: □

Outbound

Profile:

Mode: rtp

Protocol: none

- Click OK at the bottom of each when applicable

9.4 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.

9.4.1 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.

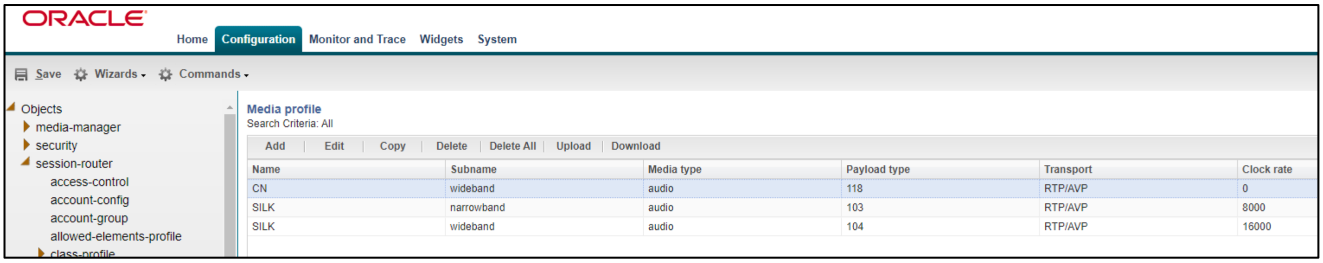
GUI Path: session-router/media-profile

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
Search Criteria: All

Name	Subname	Media type	Payload type	Transport	Clock rate
CN	wideband	audio	118	RTP/AVP	0
SILK	narrowband	audio	103	RTP/AVP	8000
SILK	wideband	audio	104	RTP/AVP	16000

- Click OK at the bottom of each when applicable

9.4.2 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

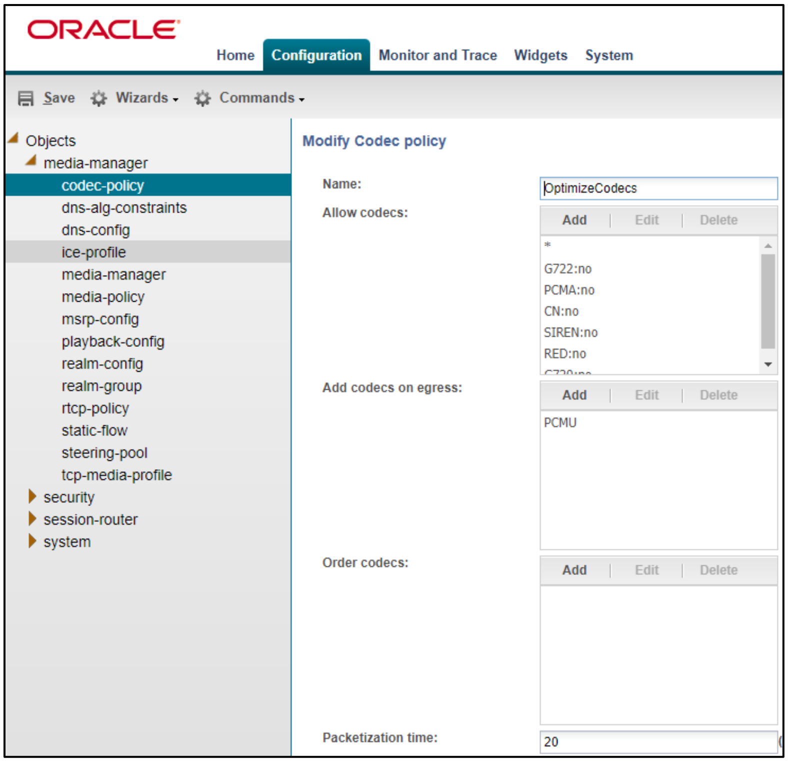
GUI Path: media-manager/codec-policy

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

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

Create another 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

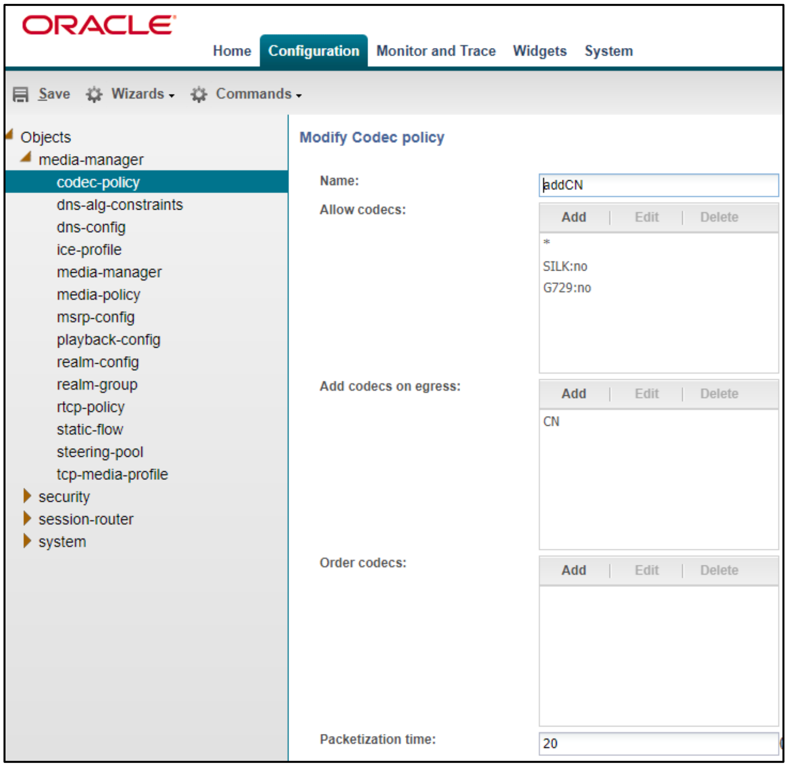
Name: OptimizeCodecs

Allow codecs:
*
G722:no
PCMA:no
CN:no
SIREN:no
RED:no

Add codecs on egress:
PCMU

Order codecs:

Packetization time: 20



Modify Codec policy

Name: addCN

Allow codecs:
*
SILK:no
G729:no

Add codecs on egress:
CN

Order codecs:

Packetization time: 20

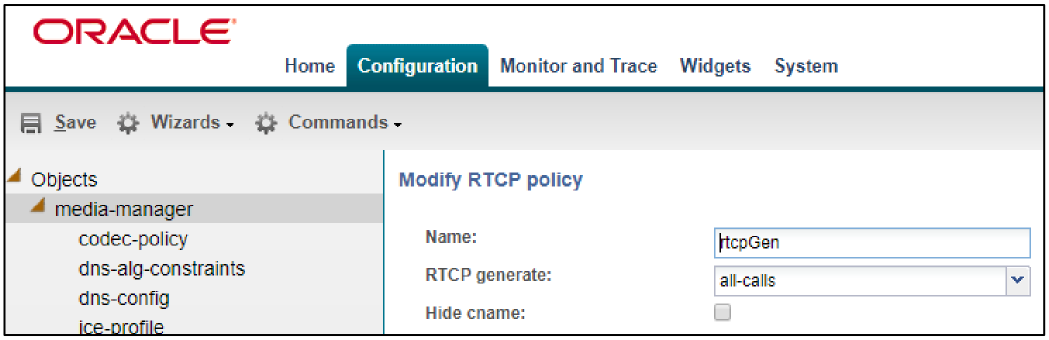
9.4.3 RTCP Policy

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



Modify RTCP policy

Name: rtcpGen

RTCP generate: all-calls

Hide cname: □

- Click OK at the bottom

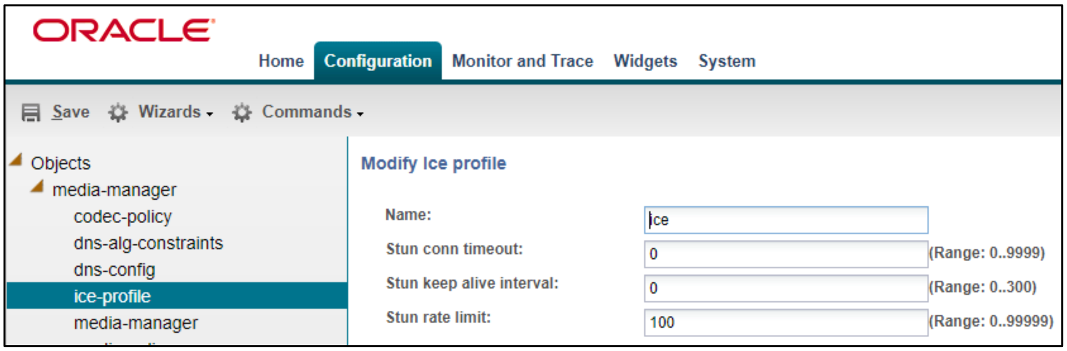
9.4.4 Ice Profile

SBC supports ICE-Lite. This configuration is required to support MSTeams media-bypass.

GUI Path: media-manager/ice-profile

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

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



Modify Ice profile

Name: Ice

Stun conn timeout: 0 (Range: 0..9999)

Stun keep alive interval: 0 (Range: 0..300)

Stun rate limit: 100 (Range: 0..99999)

- Click OK

Note: Ice Profile should not be configured for Non Media Bypass Environment with Microsoft Teams

9.5 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 Teams and PSTN.

9.5.1 Realm Config

In this example, we will configure a realm facing Microsoft Teams, A realm for PSTN Sip Trunk, and a third realm to interface with the ATA or analog device

GUI Path; media-manger/realm-config

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

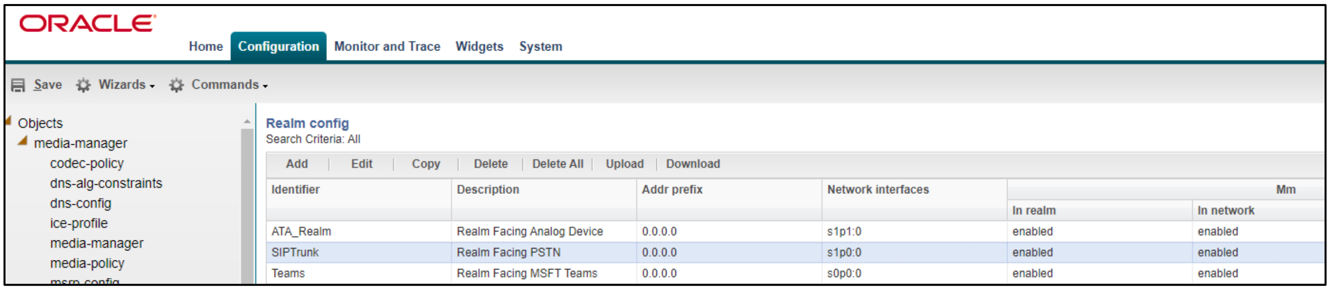
- Click Add, and use the following table as a configuration example for the three realms used in this configuration example

Config Parameter	Teams Realm	ATA	PSTN Realm
Identifier	Teams	ATA_Realm	SIPTrunk
Network Interface	s0p0:0	S1p1:0	s1p0:0
Mm in realm	☑	☑	☑
Teams-FQDN	Telechat.o-test06161977.com		
Teams fqdn in uri	☑		
Sdp inactive only	☑		
Media Sec policy	sdespolicy	sdespolicy	RTP
RTCP mux	☑		
ice profile	ice		
Codec policy	addCN	OptimizeCodecs	OptimizeCodecs
RTCP policy	rtcpGen		
Access Control Trust Level	High	High	High

The “Teams FQDN” Field is required to allow sip messages generated by the SBC to be formatted according to MSFT Teams Requirements. The SBC FQDN must be configured either in this realm parameter, or under the hostname field of the network interface.

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

- Network interface
- Media security policys
- Ice profile (Only required with Media Bypass set to enabled in Direct Routing Interface)
- Codec policys
- Rtcp policy



Realm config
Search Criteria: All

Identifier	Description	Addr prefix	Network interfaces	Mm	
				In realm	In network
ATA_Realm	Realm Facing Analog Device	0.0.0.0	s1p1:0	enabled	enabled
SIPTrunk	Realm Facing PSTN	0.0.0.0	s1p0:0	enabled	enabled
Teams	Realm Facing MSFT Teams	0.0.0.0	s0p0:0	enabled	enabled

9.5.2 Steering Pools

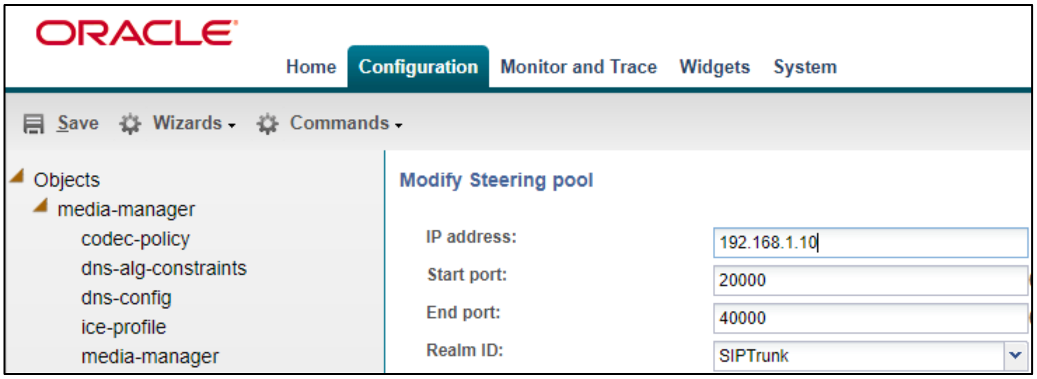
Steering pools define sets of ports that are used for steering media flows through the OCSBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We configure one steering pool for PSTN. The other will be shared by all parent and child realms facing Teams.

GUI Path: media-manger/steering-pool

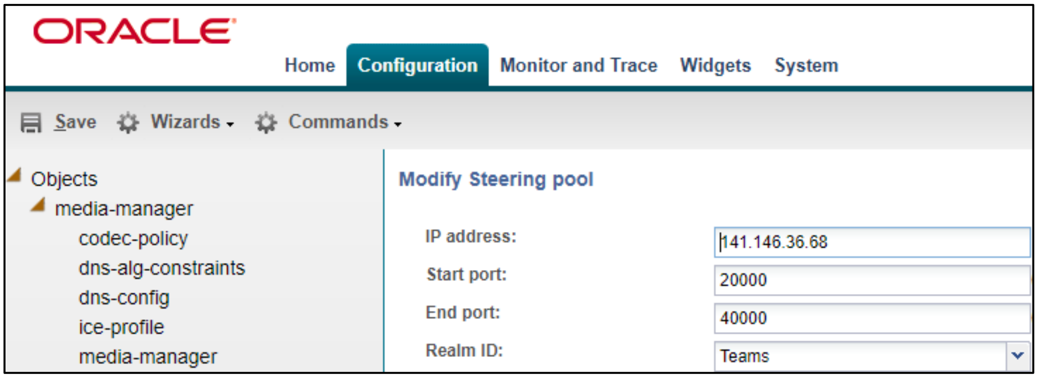
ACLI Path: config t→media-manger→steering-pool

- Click Add, and use the below examples to configure



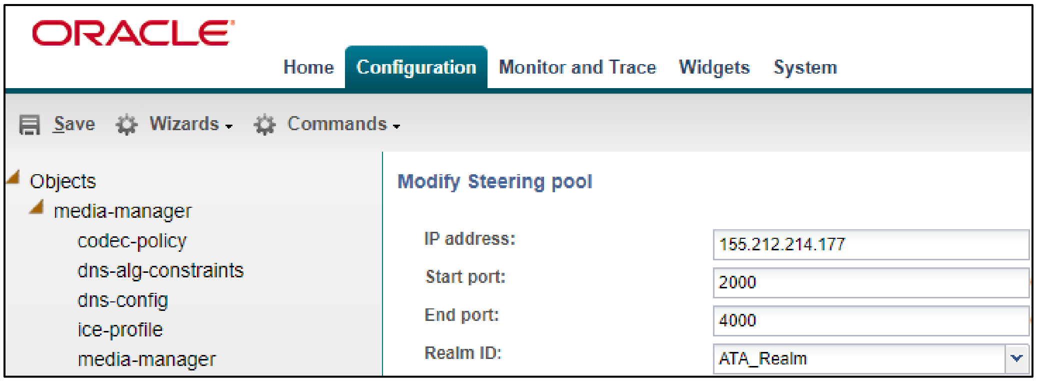
Modify Steering pool

IP address: 192.168.1.10
Start port: 20000
End port: 40000
Realm ID: SIPTrunk



Modify Steering pool

IP address: 141.146.36.68
Start port: 20000
End port: 40000
Realm ID: Teams



Modify Steering pool

IP address: 155.212.214.177
Start port: 2000
End port: 4000
Realm ID: ATA_Realm

9.6 Sip Configuration

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

9.6.1 SIP Profile

A sip profile needs to be configured and will be assigned to the Teams sip interface. This parameter is not currently available through the OCSBC GUI, and needs to be configured, and assigned through the OCSBC ACLI.

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

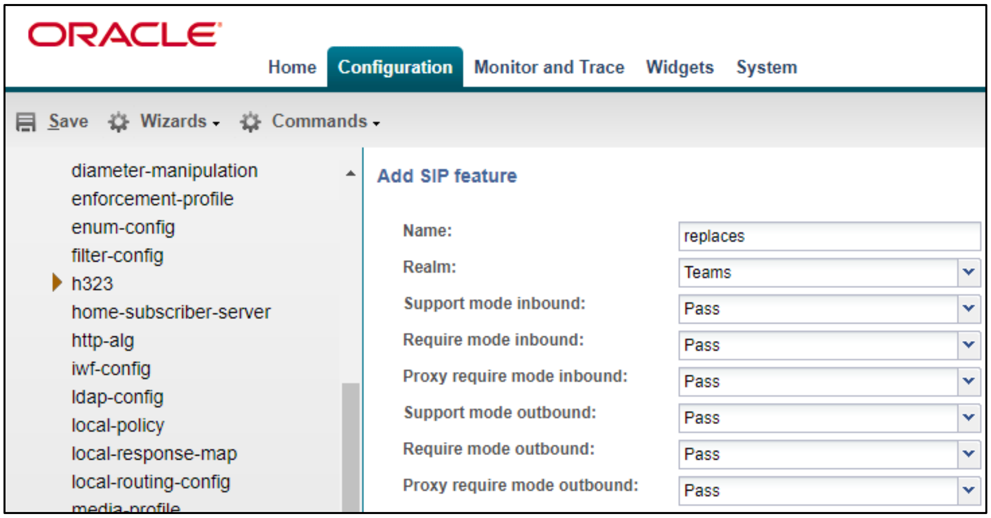
```
sip-profile
        name                              forreplace
        redirection                       inherit
        ingress-conditional-cac-admit      inherit
        egress-conditional-cac-admit       inherit
        forked-cac-bw                      inherit
        cnam-lookup-server
        cnam-lookup-dir                    egress
        cnam-unavailable-ptype
        cnam-unavailable-utype
        replace-dialogs                   enabled
```

9.6.2 Sip Feature

The following sip feature needs to be added to the Configuration of the SBC to enable support for the replaces, allowing for successful consultative transfer:

GUI Path: session-router/sip-feature

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



Add SIP feature

Name: replaces

Realm: Teams

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

9.6.3 Sip Interface

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

Configure three sip interfaces, one associated with PSTN Realm, One for Analog Device, and a third for Microsoft Teams direct routing.

GUI Path: session-router/sip-interface

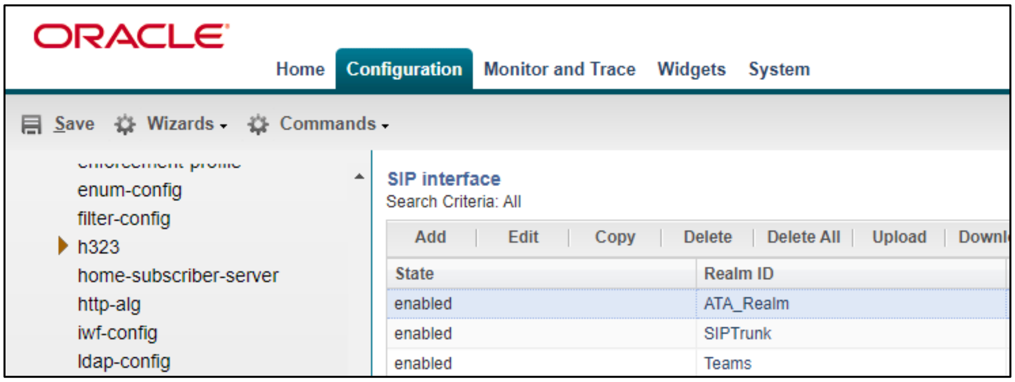
ACLI Path: config t→session-router→sip-interface

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

Config Parameter	SipTrunk	Teams	ATA
Realm ID	SipTrunk	Teams	ATA_Realm
Sip Proile		forreplace	
Sip Port Config Parmeter	**Sip Trunk**	**Teams**	
Address	192.168.1.10	141.146.36.68	155.212.214.177
Port	5060	5061	5061
Transport protocol	UDP	TLS	TLS
TLS profile		TLSTeams	TLSAnalog
Allow anonymous	agents-only	agents-only	Agents-only
in-manipulationid		RespondOptions	

Please note, this is also where we will be assigned some of the configuration elements configured earlier in this document, ie….

- Sip-Profile
- TLS Profile



SIP interface
Search Criteria: All

State	Realm ID
enabled	ATA_Realm
enabled	SIPTrunk
enabled	Teams

9.6.4 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

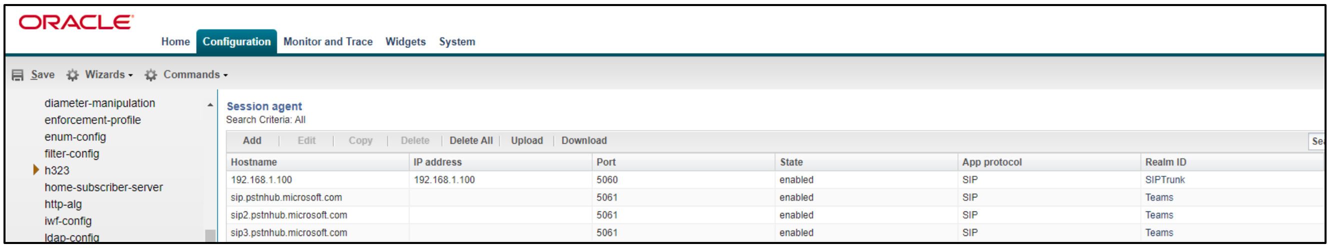
You will need to configure three Session Agents for the Microsoft Direct Routing Interface

- 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	Teams	Teams	Teams
Ping Method	OPTIONS	OPTIONS	OPTIONS
Ping Interval	30	30	30
Refer Call Transfer	enabled	enabled	enabled

You may need to configure additional session agents as well, for Sip Trunk and ATA. **This will vary widely based on individual environments and how the ATA is being deployed.** For the purposes of this example only…we will configure two additional session agents, one for SIPTrunk, and another for the Third Party Analog Device

Config parameter	Session Agent PSTN	Session Agent ATA
Hostname	68.68.117.67	155.212.214.170
IP-Address	68.68.117.67	155.212.214.170
Port	5060	5061
Transport method	UDP	StaticTLS
Realm ID	SIPTrunk	ATA_Realm
Ping Method	OPTIONS	OPTIONS
Ping Interval	30	30
Refer Call Transfer	enabled	enabled



Session agent
Search Criteria: All

Hostname	IP address	Port	State	App protocol	Realm ID
192.168.1.100	192.168.1.100	5060	enabled	SIP	SIPTrunk
sip.pstnhub.microsoft.com		5061	enabled	SIP	Teams
sip2.pstnhub.microsoft.com		5061	enabled	SIP	Teams
sip3.pstnhub.microsoft.com		5061	enabled	SIP	Teams

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

9.6.5 Session Agent Group

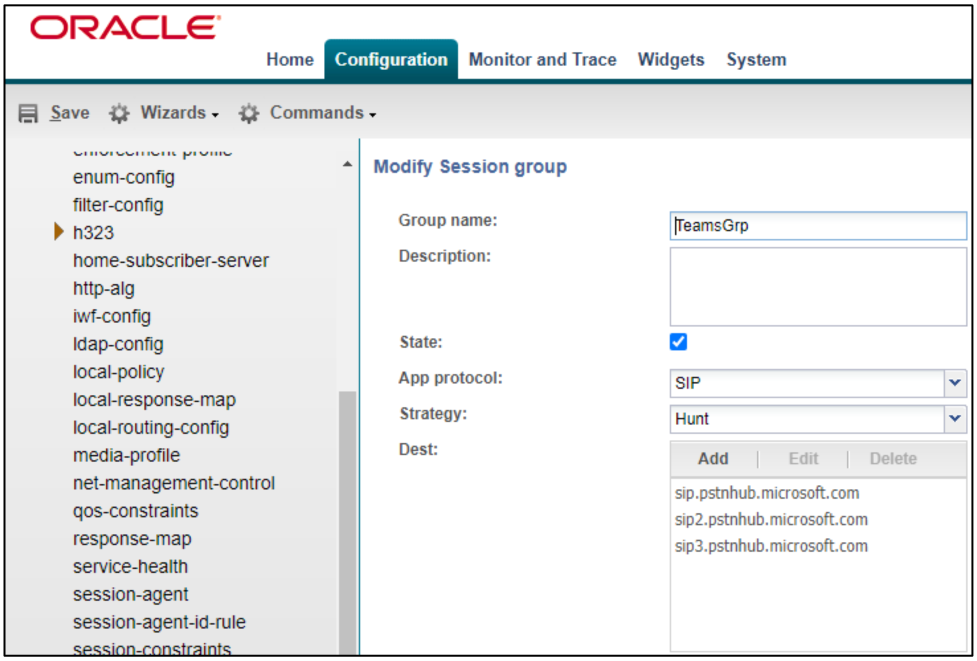
A session agent group allows the SBC to create a load balancing model:

All three Teams session agents configured above 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:



Modify Session group

Group name: TeamsGrp
Description:
State: ☑
App protocol: SIP
Strategy: Hunt
Dest:
sip.pstnhub.microsoft.com
sip2.pstnhub.microsoft.com
sip3.pstnhub.microsoft.com

- Click OK at the bottom

9.7 Routing Configuration

This section outlines how to configure the OCSBC to route Sip traffic to and from Microsoft Teams Direct Routing Interface, SIPTrunk, and Third Party Analog Device.

The OCSBC has multiple routing options that can be configured based on environment. Since we have only two DID's associated with the analog device, and two DID's assigned to Teams clients in this test environment, we utilized Local Policy Routing performing DID Separation via the TO (Request-URI) Address field in each local policy where applicable.

The DID assignments are as follows:

TeamsUser1: 17814437247

TeamsUser2: 17814437248

ATA Port 1: 17814437383

ATA Port 2: 17814437384

9.7.1 Local Policy Configuration

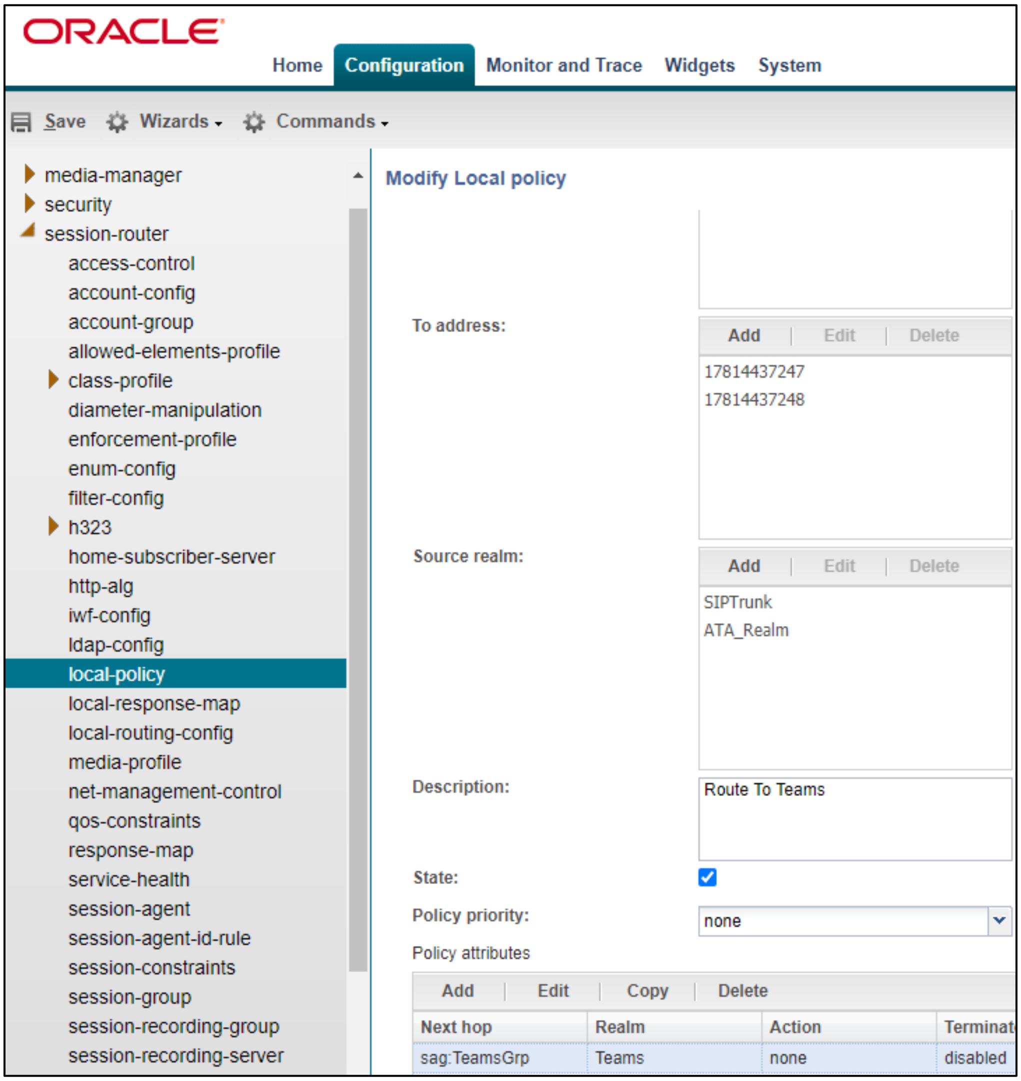
Local Policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria.

GUI Path: session-router/local-policy

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

Please note, the To Address field in local policy matches the Request URI in Sip Messages.

The following local policy routes calls from PSTN and from ATA to Microsoft Teams that match the To Address:



Modify Local policy

To address: 17814437247, 17814437248

Source realm: SIPTrunk, ATA_Realm

Description: Route To Teams

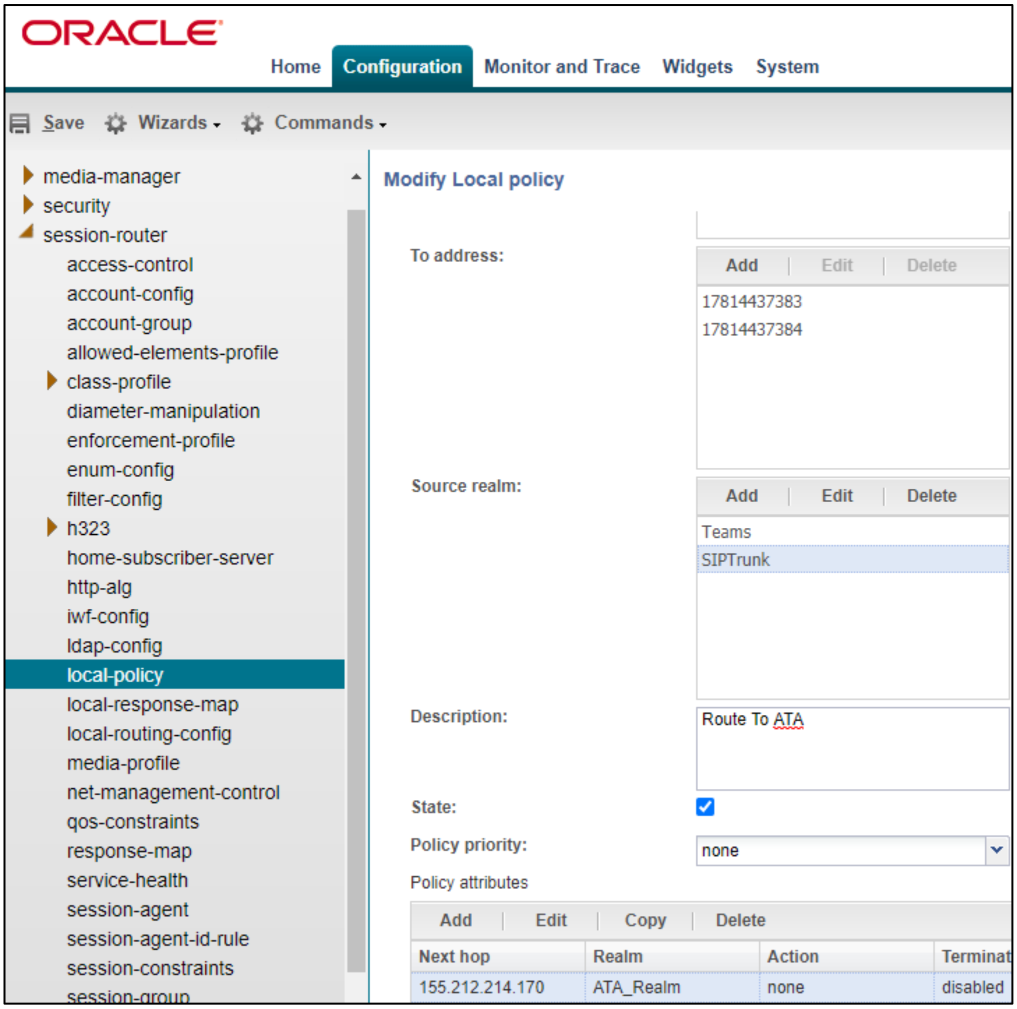
State: ☑

Policy priority: none

Policy attributes

Next hop	Realm	Action	Terminat
sag:TeamsGrp	Teams	none	disabled

The Following Routes Calls from PSTN and from MSFT Teams To ATA that match the To Address:



Modify Local policy

To address:
17814437383
17814437384

Source realm:
Teams
SIPTrunk

Description: Route To ATA

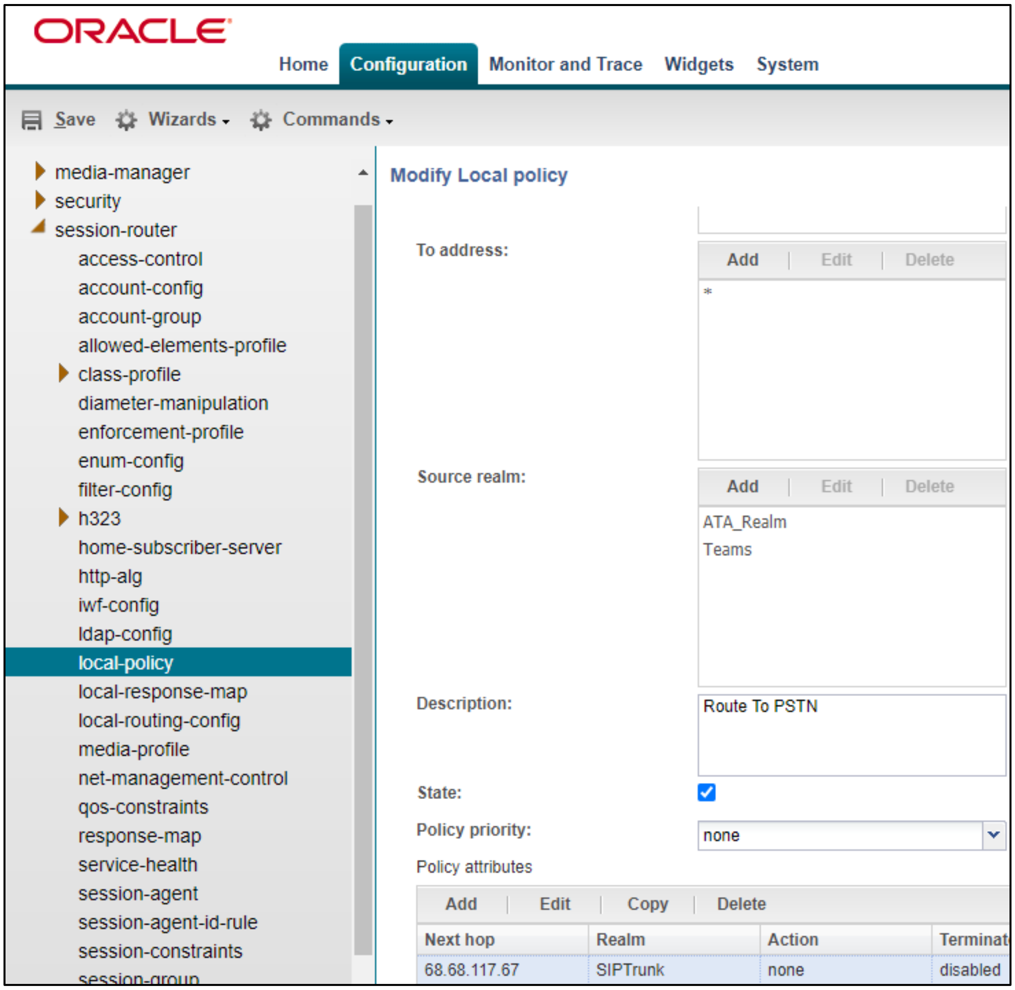
State: ☑

Policy priority: none

Policy attributes

Next hop	Realm	Action	Terminat
155.212.214.170	ATA_Realm	none	disabled

If the above configured local policies do not match the To Address Field, then the following policy will route all calls from either the Analog Device or From Teams to PSTN:



Modify Local policy

To address: *

Source realm: ATA_Realm, Teams

Description: Route To PSTN

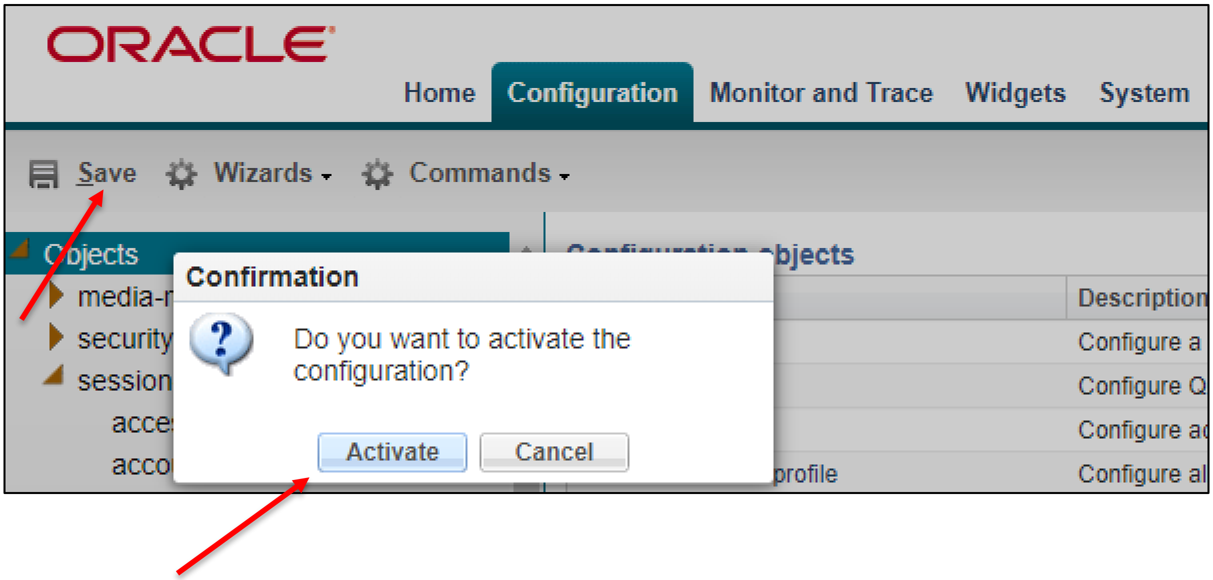
State: ☑

Policy priority: none

Policy attributes

Next hop	Realm	Action	Terminat
68.68.117.67	SIPTrunk	none	disabled

The SBC configuration is now complete. You can now save and activate the configuration.



Confirmation

Do you want to activate the configuration?

Move to verify the connection with Microsoft Direct Routing Interface

10 Verify Connectivity

10.1 OCSBC Options Ping

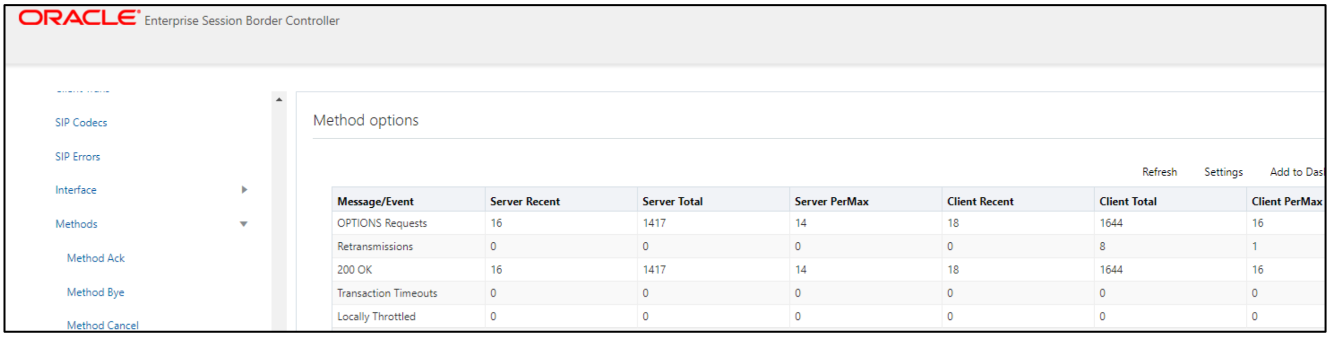
After you've paired the OCSBC with Direct Routing validate that the SBC can successfully exchange SIP Options with Microsoft Direct Routing. (Also verify with PSTN and ATA if applicable)

While in the OCSBC GUI, Utilize the "Widgets" to check for OPTIONS to and from the SBC.

- At the top, click "Wigits"

This brings up the Wigits menu on the left hand side of the screen

GUI Path: Signaling/SIP/Methods/OPTIONS



Method options

Message/Event	Server Recent	Server Total	Server PerMax	Client Recent	Client Total	Client PerMax
OPTIONS Requests	16	1417	14	18	1644	16
Retransmissions	0	0	0	0	8	1
200 OK	16	1417	14	18	1644	16
Transaction Timeouts	0	0	0	0	0	0
Locally Throttled	0	0	0	0	0	0

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

10.2 Microsoft SIP Tester Client

SIP Tester client is a sample PowerShell script that you can use to test Direct Routing Session Border Controller (SBC) connections in Microsoft Teams. This script tests basic functionality of a customer-paired Session Initiation Protocol (SIP) trunk with Direct Routing.

The script submits an SIP test to the test runner, waits for the result, and then presents it in a human-readable format. You can use this script to test the following scenarios:

- Outbound and inbound calls
- Simultaneous ring
- Media escalation
- Consultative transfer

Download the script and Documentation here:

Sip Tester Client script and documentation

11 Syntax Requirements for SIP Invite and SIP Options

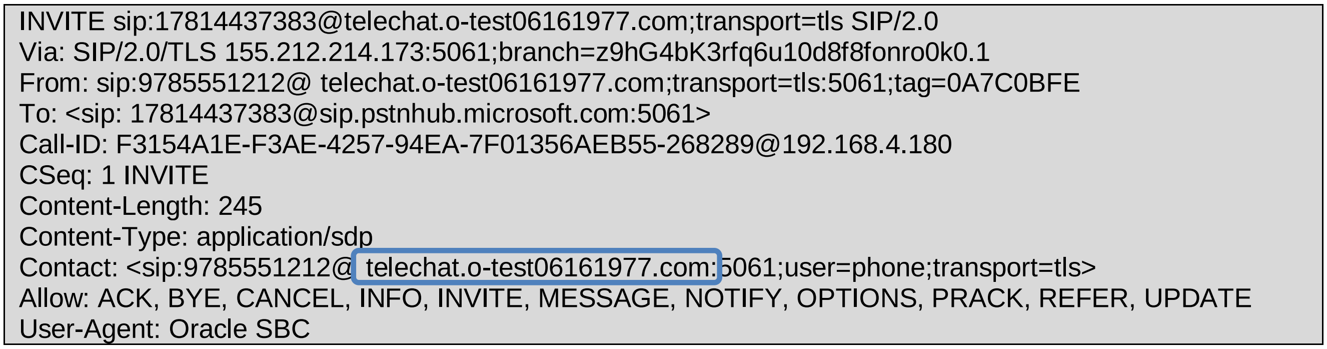
Microsoft Teams Hybrid Voice Connectivity interface has requirements for the syntax of SIP messages. This section covers high-level requirements to SIP syntax of Invite, Final Responses to Invite and Options messages. The information can be used as a first step during troubleshooting when calls don't go through. From our experience most of the issues are related to the wrong syntax of SIP messages.

11.1 Terminology

- Recommended – not required, but to simplify the troubleshooting, it is recommended to configure as in examples as follow
- Must – strict requirement, the system does not work without the configuration of these parameters

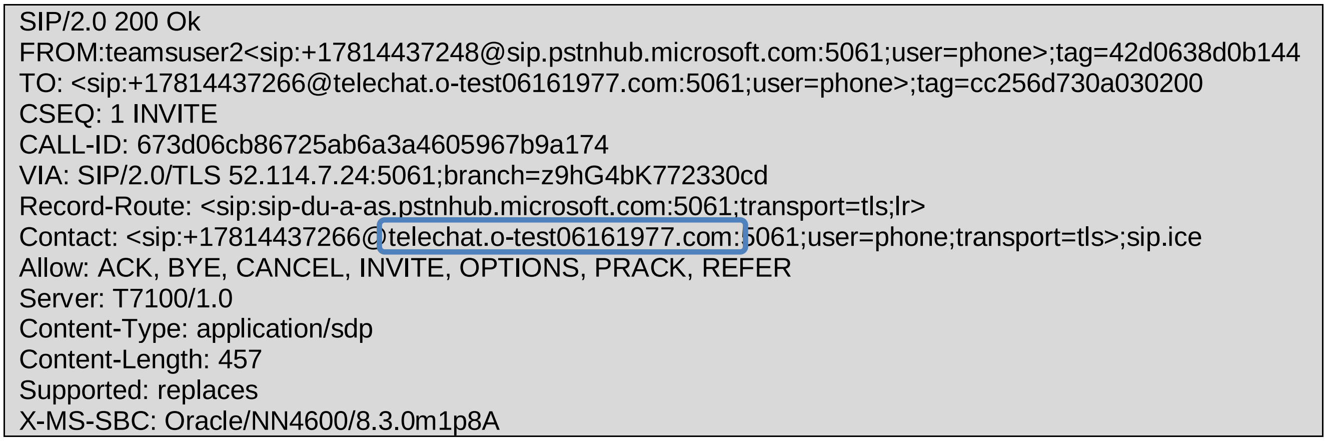
11.2 Requirements for Invite Messages

Picture 1 Example of INVITE message



```
INVITE sip:17814437383@telechat.o-test06161977.com;transport=tls SIP/2.0
Via: SIP/2.0/TLS 155.212.214.173:5061;branch=z9hG4bK3rfq6u10d8f8fonro0k0.1
From: sip:9785551212@ telechat.o-test06161977.com;transport=tls:5061;tag=0A7C0BFE
To: <sip: 17814437383@sip.pstnhub.microsoft.com:5061>
Call-ID: F3154A1E-F3AE-4257-94EA-7F01356AEB55-268289@192.168.4.180
CSeq: 1 INVITE
Content-Length: 245
Content-Type: application/sdp
Contact: <sip:9785551212@ telechat.o-test06161977.com:5061;user=phone;transport=tls>
Allow: ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, REFER, UPDATE
User-Agent: Oracle SBC
```

Picture 2 Example of 200OK Response To Invite:



```
SIP/2.0 200 Ok
FROM:teamsuser2<sip:+17814437248@sip.pstnhub.microsoft.com:5061;user=phone>;tag=42d0638d0b144
TO: <sip:+17814437266@telechat.o-test06161977.com:5061;user=phone>;tag=cc256d730a030200
CSEQ: 1 INVITE
CALL-ID: 673d06cb86725ab6a3a4605967b9a174
VIA: SIP/2.0/TLS 52.114.7.24:5061;branch=z9hG4bK772330cd
Record-Route: <sip:sip-du-a-as.pstnhub.microsoft.com:5061;transport=tls;lr>
Contact: <sip:+17814437266@telechat.o-test06161977.com:5061;user=phone;transport=tls>;sip.ice
Allow: ACK, BYE, CANCEL, INVITE, OPTIONS, PRACK, REFER
Server: T7100/1.0
Content-Type: application/sdp
Content-Length: 457
Supported: replaces
X-MS-SBC: Oracle/NN4600/8.3.0m1p8A
```

11.2.1 Contact.Header

- Must have the FQDN sub-domain name of a specific Teams tenant for media negotiation.
- Syntax: Contact:: <phone number>@< subdomain FQDN >:<SBC Port>;<transport type>
- MSFT Direct Routing will reject calls if not configured correctly

11.3 Requirements for OPTIONS Messages

Picture 2 Example of OPTIONS message

```
OPTIONS sip:sip.pstnhub.microsoft.com:5061;transport=tls SIP/2.0
Via: SIP/2.0/TLS 155.212.214.173:5061;branch=z9hG4bKumatcr30fod0o13gi060
Call-ID: 4cf0181d4d07a995bcc46b8cd42f9240020000sg52@155.212.214.173
To: sip:ping@sip.pstnhub.microsoft.com
From: <sip:ping@sip.pstnhub.microsoft.com>;tag=0b8d8daa0f6b1665b420aa417f5f4b18000sg52
Max-Forwards: 70
CSeq: 3723 OPTIONS
Route: <sip:52.114.14.70:5061;lr>
Content-Length: 0
Contact: <sip:ping@telechat.o-test06161977.com:5061;transport=tls>
Record-Route: <sip: customers.telechat.o-test06161977.com >
```

11.3.1 Contact Header

- When sending OPTIONS to the Direct Routing Interface Interface “Contact” header should have SBC FQDN in URI
- hostname along with Port & transport parameter set to TLS.
- Syntax: Contact: sip: <FQDN of the SBC:port;transport=tls>
- If the parameter is not set correctly, Teams Direct Routing Interface will not send SIP Options to the SBC

12 Microsoft Teams Direct Routing Interface characteristics

Table 1 contains the technical characteristics of the Direct Routing Interface. Microsoft, in most cases, uses RFC standards as a guide during the development. However, Microsoft does not guarantee interoperability with SBCs even if they support all the parameters in table 1 due to specifics of implementation of the standards by SBC vendors. Microsoft has a partnership with some SBC vendors and guarantees their device’s interoperability with the interface. All validated devices are listed on Microsoft’s site. Microsoft only supports the validated devices to connect to Direct Routing Interface. Oracle is one of the vendors who have a partnership with Microsoft.

Category	Parameter	Value	Comments
Ports and IP	SIP Interface FQDN	Refer to Microsoft documentation	
	IP Addresses range for SIP interfaces	Refer to Microsoft documentation	
	SIP Port	5061	
	IP Address range for Media	Refer to Microsoft documentation	
	Media port range on Media Processors	Refer to Microsoft documentation	
	Media Port range on the client	Refer to Microsoft documentation	
Transport and Security	SIP transport	TLS	
	Media Transport	SRTP	
	SRTP Security Context	DTLS, SIPS Note: DTLS is not supported until later time. Please configure SIPS at this moment. Once support of DTLS announced it will be the recommended context	https://tools.ietf.org/html/rfc5763
	Crypto Suite	AES_CM_128_HMAC_SHA1_80, non-MKI	
	Control protocol for media transport	SRTCP (SRTCP-Mux recommended)	Using RTCP mux helps reduce number of required ports
	Supported Certification Authorities	Refer to Microsoft documentation	
	Transport for Media Bypass (of configured)	ICE-lite (RFC5245) – recommended, · Client also has Transport Relays	
Codecs	Audio codecs	· G711 · Silk (Teams clients) · Opus (WebRTC clients) - Only if Media Bypass is used; · G729 · G722	
	Other codecs	· CN o Required narrowband and wideband · RED – Not required · DTMF – Required · Events 0-16 · Silence Suppression – Not required	

13 SIP Access Controls (Mandatory for MSFT Teams)

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

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

https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/security/security-guide.pdf

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

1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high

2. Set the access control trust level on public facing realms to HIGH

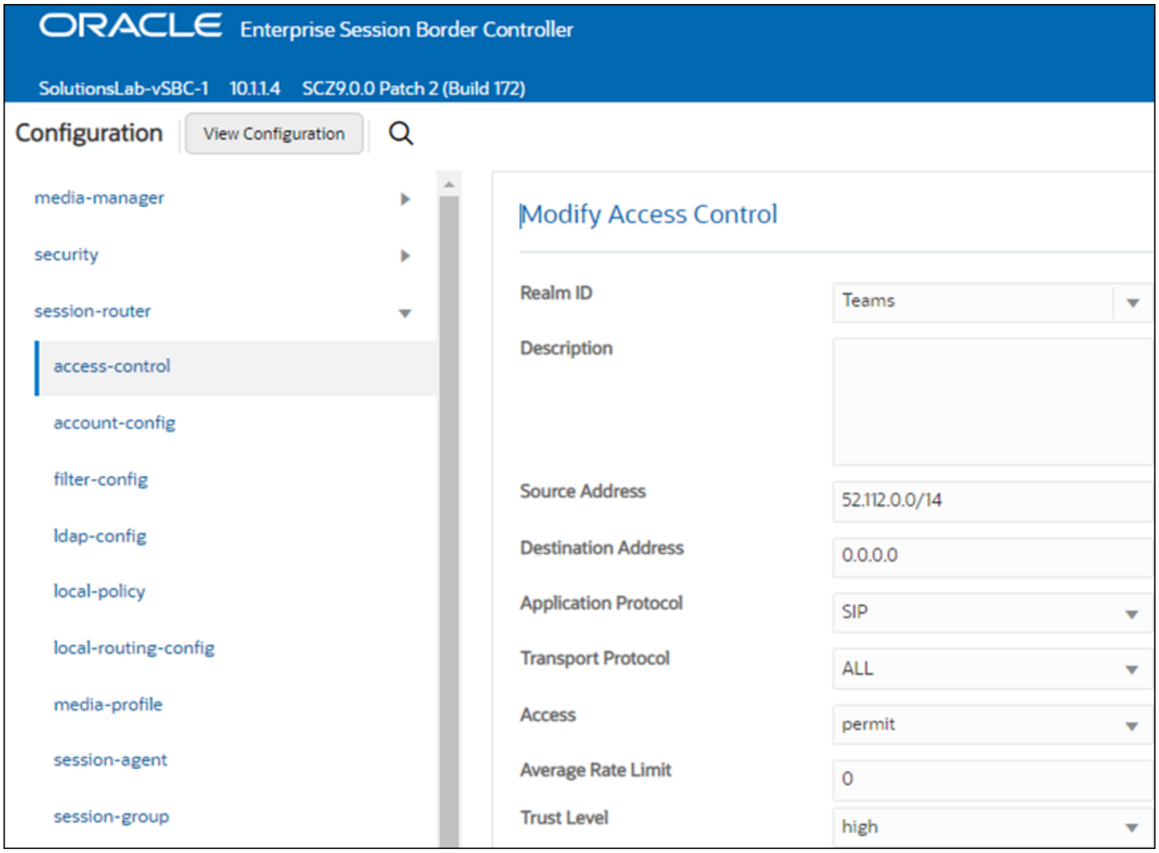
Microsoft Teams has two subnets, 52.112.0.0/14 and 52.120.0.0/14 that must be allowed to send traffic to the SBC. Both must be configured as an access control on the Oracle SBC and associated with the realm facing Teams.

Use this example to create ACL's for all MSFT Teams subnets. This example can be followed for any of the public facing interfaces, ie…SipTrunk, etc…

GUI Path: session-router/access-control

ACLI Path: config tàsession-routeràaccess-control

Use this example to create ACL's for both MSFT Teams subnets, 52.112.0.0/14 and 52.120.0.0/14.



Modify Access Control

Realm ID	Teams
Description	
Source Address	52.112.0.0/14
Destination Address	0.0.0.0
Application Protocol	SIP
Transport Protocol	ALL
Access	permit
Average Rate Limit	0
Trust Level	high

- Select OK at the bottom

This concludes the required configuration of the SBC to properly interface with Microsoft Teams Phone System Direct Routing.

14 Appendix A

14.1 SBC Behind NAT SPL configuration

This configuration is needed when your SBC is behind a NAT device. This is configured to avoid loss in voice path and SIP signaling.
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.

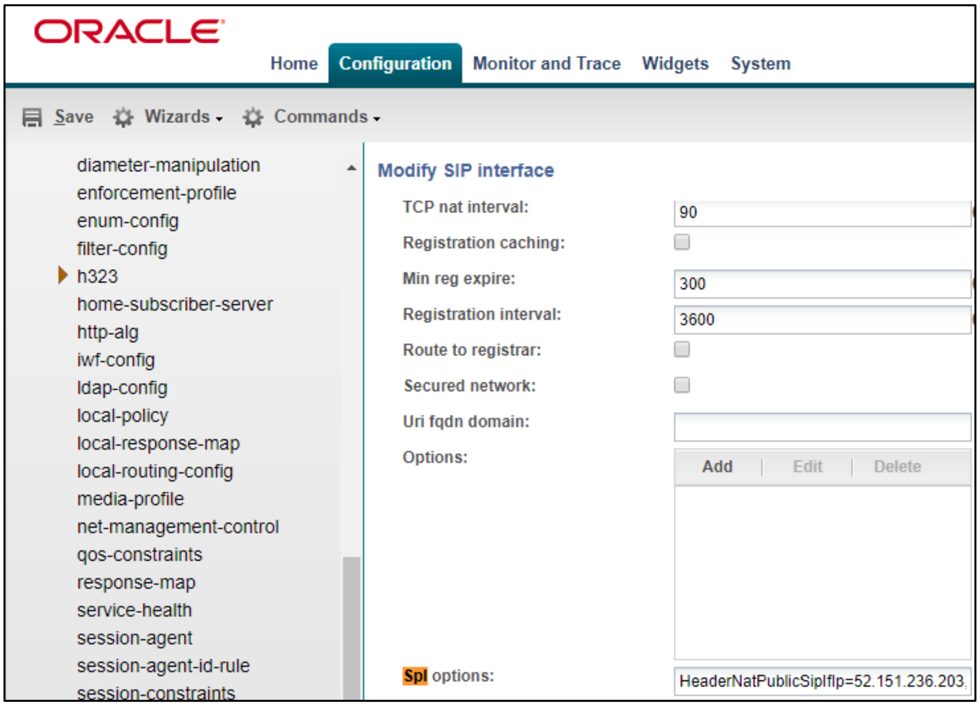
- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

Here is an example configuration with SBC Behind NAT SPL config. The SPL is applied to the Teams 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.

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.0.4.4

Here HeaderNatPublicSipIfIp is the public interface ip and HeaderNatPrivateSipIfIp is the private ip.



Modify SIP interface

TCP nat interval: 90

Registration caching: □

Min reg expire: 300

Registration interval: 3600

Route to registrar: □

Secured network: □

Uri fqdn domain:

Options:

Spl options: HeaderNatPublicSipIfIp=52.151.236.203,

- This configuration would be applied to each Sip Interface in the OCSBC configuration that was deployed behind a Nat Device

15 Caveats

15.1 No Audio-On-Hold

Microsoft has enabled the ability for the Direct Routing Interface to generate Music when a Teams Client parks or places a call on hold. Since this feature implementation, which currently cannot be disabled, some users have experienced no audio when trying to retrieve calls in which hold or park was initiated by a Microsoft Teams Client

This caveat has only been applicable to SBC's deployed as Virtual Machines, or VME SBC's.

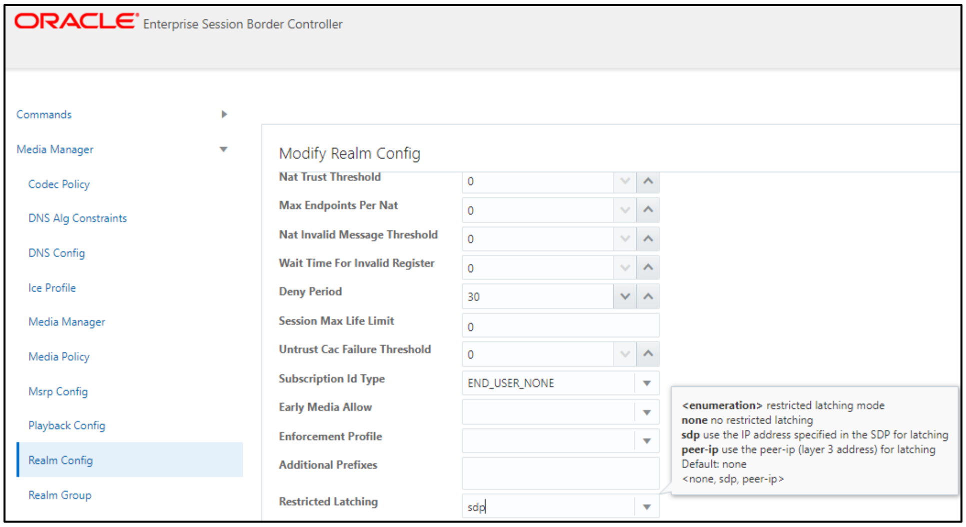
To correct this, Oracle recommends enabling Restricted Media Latching on realms configured for Microsoft Teams in the OCSBC.

The restricted media latching feature lets the Oracle® Session Border Controller latch only to media from a known source IP address, in order to learn and latch the dynamic UDP port number. The restricting IP addresses origin can be either the SDP information or the SIP message's Layer 3 (L3) IP address, depending on the configuration.

Deploying an OCSBC as a VME with Microsoft Direct routing, set this parameter to **SDP**.

GUI Path: media-manger/realm-config

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



Modify Realm Config

Nat Trust Threshold	0
Max Endpoints Per Nat	0
Nat Invalid Message Threshold	0
Wait Time For Invalid Register	0
Deny Period	30
Session Max Life Limit	0
Untrust Cac Failure Threshold	0
Subscription Id Type	END_USER_NONE
Early Media Allow	
Enforcement Profile	
Additional Prefixes	
Restricted Latching	sdp

<enumeration> restricted latching mode
none no restricted latching
sdp use the IP address specified in the SDP for latching
peer-ip use the peer-ip (layer 3 address) for latching
Default: none
<none, sdp, peer-ip>

- Click OK at the bottom
- Save and activate the configuration

16 Running Configuration

Below is the CLI output of show running config short. This only reflects parameters that have been modified from their default values.

```
show running-config short

access-control
        realm-id                                ATA_Realm
        source-address                                 155.212.214.170
        application-protocol                     SIP
        trust-level                             high
access-control
        realm-id                                Teams
        source-address                                 52.112.0.0/14
       destination-address                       141.146.36.68
        application-protocol                     SIP
        trust-level                             high
access-control
        realm-id                                SIPTrunk
        source-address                                 68.68.117.67
        application-protocol                     SIP
        trust-level                             high
certificate-record
        name                                   ATACert
        locality                              Bedford
        organization                               Oracle
        unit                                 Solutions
        common-name                                   proxysbc.com
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
certificate-record
        name                                   InernalCACert
        locality                              Bedford
        organization                               Oracle
        unit                                 Solutions
        common-name                                   solutionslab
certificate-record
        name                                   TeamsEnterpriseCert
        state                                 California
        locality                              Redwood City
        organization                               Oracle Corporation
        common-name                                   telechat.o-test06161977.com
        extended-key-usage-list                          serverAuth
                                           ClientAuth
codec-policy
        name                                   OptimizeCodecs
        allow-codecs                    * G722:no PCMA:no CN:no SIREN:no RED:no G729:no
        add-codecs-on-egress                PCMU
codec-policy
        name                            addCN
        allow-codecs                        *
        add-codecs-on-egress                CN
dtls-srtp-profile
        name                            TeamsDTLS
        tls-profile                     TLSTeams
        crypto-suite                      SRTP_AES128_CM_HMAC_SHA1_32
host-route
        dest-network                        8.8.0.0
        netmask                           255.255.0.0
        gateway                           141.146.36.65
ice-profile
        name                            ice
        stun-conn-timeout                      0
        stun-keep-alive-interval                0
local-policy
        from-address                         *
        to-address                         *
        source-realm                        ATA_Realm
                                        Teams
        policy-attribute
                next-hop                          68.68.117.67
                realm                           SIPTrunk
local-policy
        from-address                         *
        to-address                        17814437247
                                        17814437248
        source-realm                        ATA_Realm
                                        SIPTrunk
        policy-attribute
                next-hop                          SAG:TeamsGrp
                realm                           Teams
local-policy
        from-address                         *
        to-address                        17814437383
                                        17814437384
        source-realm                        SIPTrunk
                                        Teams
        policy-attribute
                next-hop                          155.212.214.170
                realm                           ATA_Realm
media-manager
        options                          audio-allow-asymmetric-pt
                                        xcode-gratuitous-rtcp-report-generation
        max-untrusted-signaling              1
        min-untrusted-signaling              1
media-profile
        name                            CN
        subname                           wideband
        payload-type                        118
        clock-rate                        16000
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
        ip-address                        141.146.36.68
        netmask                          255.255.255.192
        gateway                          141.146.36.65
        dns-ip-primary                       8.8.8.8
        dns-ip-backup1                        8.8.4.4
        dns-domain                          telechat.o-test06161977.com
        hip-ip-list                     141.146.36.100
        icmp-address                         141.146.36.100
network-interface
        name                            s1p0
        ip-address                        192.168.1.10
        netmask                          255.255.255.0
        gateway                          192.168.1.1
network-interface
        name                            s1p1
        ip-address                        155.212.214.177
        netmask                          255.255.255.0
        gateway                          155.212.214.1
phy-interface
        name                            s0p0
        operation-type                       Media
phy-interface
        name                            s1p0
        operation-type                       Media
        slot                          1
phy-interface
        name                            s1p1
        operation-type                       Media
        port                           1
        slot                          1
realm-config
        identifier                      ATA_Realm
        network-interfaces                  s1p1:0
        mm-in-realm                         enabled
        media-sec-policy                    sdesPolicy
        access-control-trust-level          high
        codec-policy                        OptimizeCodecs
realm-config
        identifier                          SIPTrunk
        network-interfaces                  s1p0:0
        mm-in-realm                         enabled
        qos-enable                          enabled
        media-sec-policy                    RTP
        access-control-trust-level          high
        codec-policy                        OptimizeCodecs
realm-config
        identifier                          Teams
        description                         Realm Facing Teams Direct Routing
        network-interfaces                  s0p0:0
        mm-in-realm                         enabled
        qos-enable                          enabled
        media-sec-policy                    sdesPolicy
        rtcp-mux                            enabled
        ice-profile                         ice
        teams-fqdn                          telechat.o-test16161977.com
        teams-fqdn-in-uri                   enabled
        sdp-inactive-only                   enabled
        access-control-trust-level          high
        codec-policy                        addCN
        rtcp-policy                         rtcpGen
rtcp-policy
        name                                rtcpGen
        rtcp-generate                       all-calls
sdes-profile
        name                                SDES
        crypto-list                         AES_CM_128_HMAC_SHA1_32
                                        AES_CM_128_HMAC_SHA1_80
        lifetime                            31
session-agent
        hostname                            155.212.214.170
        ip-address                          155.212.214.170
        port                                5061
        transport-method                    StaticTLS
        realm-id                            ATA_Realm
        ping-method                         OPTIONS
        ping-interval                       30
        reuse-connections                   TCP
session-agent
        hostname                            68.68.117.67
        ip-address                          68.68.117.67
        realm-id                            SIPTrunk
        ping-method                         OPTIONS
        ping-interval                       30
session-agent
        hostname                            sip.pstnhub.microsoft.com
        port                                5061
        transport-method                    StaticTLS
        realm-id                        Teams
        ping-method                         OPTIONS
        ping-interval                     30
        refer-call-transfer                 enabled
session-agent
        hostname                          sip2.pstnhub.microsoft.com
        port                         5061
        transport-method                      StaticTLS
        realm-id                        Teams
        ping-method                         OPTIONS
        ping-interval                     30
        refer-call-transfer                 enabled
session-agent
        hostname                          sip3.pstnhub.microsoft.com
        port                         5061
        transport-method                      StaticTLS
        realm-id                        Teams
        ping-method                         OPTIONS
        ping-interval                     30
        refer-call-transfer                 enabled
session-group
        group-name                          TeamsGrp
        dest                          sip.pstnhub.microsoft.com
                                    sip2.pstnhub.microsoft.com
                                    sip3.pstnhub.microsoft.com
        sag-recursion                       enabled
        stop-sag-recurse                      401,407,480
sip-config
        home-realm-id                        Teams
        registrar-domain                      *
        registrar-host                     *
        registrar-port                    5060
        options                         inmanip-before-validate
                                    max-udp-length=0
        sip-message-len                       0
        extra-method-stats                     enabled
sip-feature
        name                            replaces
        realm                          Teams
        require-mode-inbound                   Pass
        require-mode-outbound                   Pass
sip-interface
        realm-id                        ATA_Realm
        sip-port
                address                         155.212.214.177
                port                         5061
                transport-protocol                  TLS
                tls-profile                    TLSAnalog
                allow-anonymous                       agents-only
        nat-traversal                     rport
sip-interface
        realm-id                        SIPTrunk
        sip-port
                address                         192.168.1.10
                allow-anonymous                       agents-only
```

```
    secured-network                  enabled
sip-interface
    realm-id                      Teams
    sip-port
        address                       141.146.36.68
        port                        5061
        transport-protocol                TLS
        tls-profile                  TLSTeams
        allow-anonymous              agents-only
        in-manipulationid            RespondOptions
    options                       100rel-interworking
    sip-profile                   forreplaces
sip-monitoring
    monitoring-filters               *
sip-profile
    name                          forreplaces
    replace-dialogs                  enabled
steering-pool
    ip-address                      141.146.36.68
    start-port                    20000
    end-port                       40000
    realm-id                      Teams
steering-pool
    ip-address                      155.212.214.177
    start-port                    20000
    end-port                       40000
    realm-id                      ATA_Realm
steering-pool
    ip-address                      192.168.1.10
    start-port                    20000
    end-port                       40000
    realm-id                      SIPTrunk
system-config
    hostname                        telechat.o-test06161977.com
    description                     SBC for Analog and Teams
    location                      Burlington, MA
    system-log-level                  NOTICE
    comm-monitor
    default-gateway                   10.138.194.129
    source-routing                   enabled
    snmp-agent-mode                     v1v2
tls-global
    session-caching                   enabled
tls-profile
    name                          TLSAnalog
    end-entity-certificate            ATACert
    trusted-ca-certificates            InernalCACert
    cipher-list                    ALL
    options                       ignore-root-ca=yes
```

```
tls-profile
        name                                    TLSTeams
        end-entity-certificate                          TeamsEnterpriseCert
        trusted-ca-certificates                          BaltimoreRoot
                                                         DigiCertGlobalRootG2
        mutual-authenticate                              enabled
web-server-config
```

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