Configuring the Oracle SBC to Microsoft Teams Direct Routing-Carrier Model

Technical Application Note

ORACLE

COMMUNICATIONS

Disclaimer

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

1 Contents

2 *Alert*:

Before Moving Forward in this Document, Please Read:

Due to planned upgrades to Microsoft Teams Direct Routing Platform, there are mandatory changes that are required to the Oracle Session Border Controller Configuration in some environments. If these changes are not implemented in the near future, there may be risk of call failures. Please See Important Information for more details:

Please reach out to your Oracle Account Team with any questions regarding this notification

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 Revision History

Version	Date Revised	Description of Changes
1.0	04/17/2019	Initial publication
1.1	10/09/2019	• Added GUI Configuration • Firmware Version 8.3 • Modified Due to changes in MSFT Concept of Hosting Model
1.2	03/26/2020	• Modified TLS Profile Config • Change LRT example • Added additional customer domain information
1.3	04/29/2020	• Added Alert • Add Important Information Section
1.4	06/08/2020	• Changed Running Config Output • Added Appendix C with Notes • Added notes regarding Sip Manipulation and new release
1.5	01/07/2022	• Removed Reference to sip-all fqdn

5 Intended Audience

This document describes how to connect 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 +.

6 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

7 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

8 Infrastructure Requirements

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

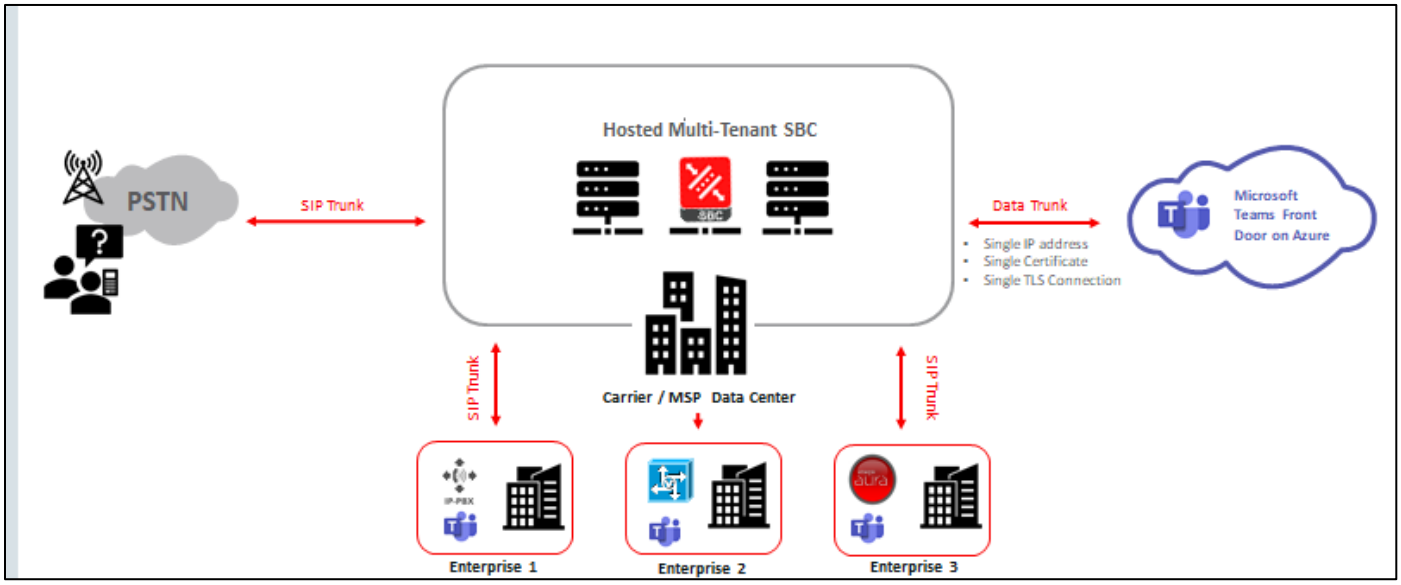
Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	**See Microsoft's Plan Direct Routing document**
SIP Trunks connected to the SBC	
Office 365 tenant	
Domains	
Public IP address for the SBC	
Fully Qualified Domain Name (FQDN) for the SBC	
Public DNS entry for the SBC	
Public 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	

9 Configuration

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

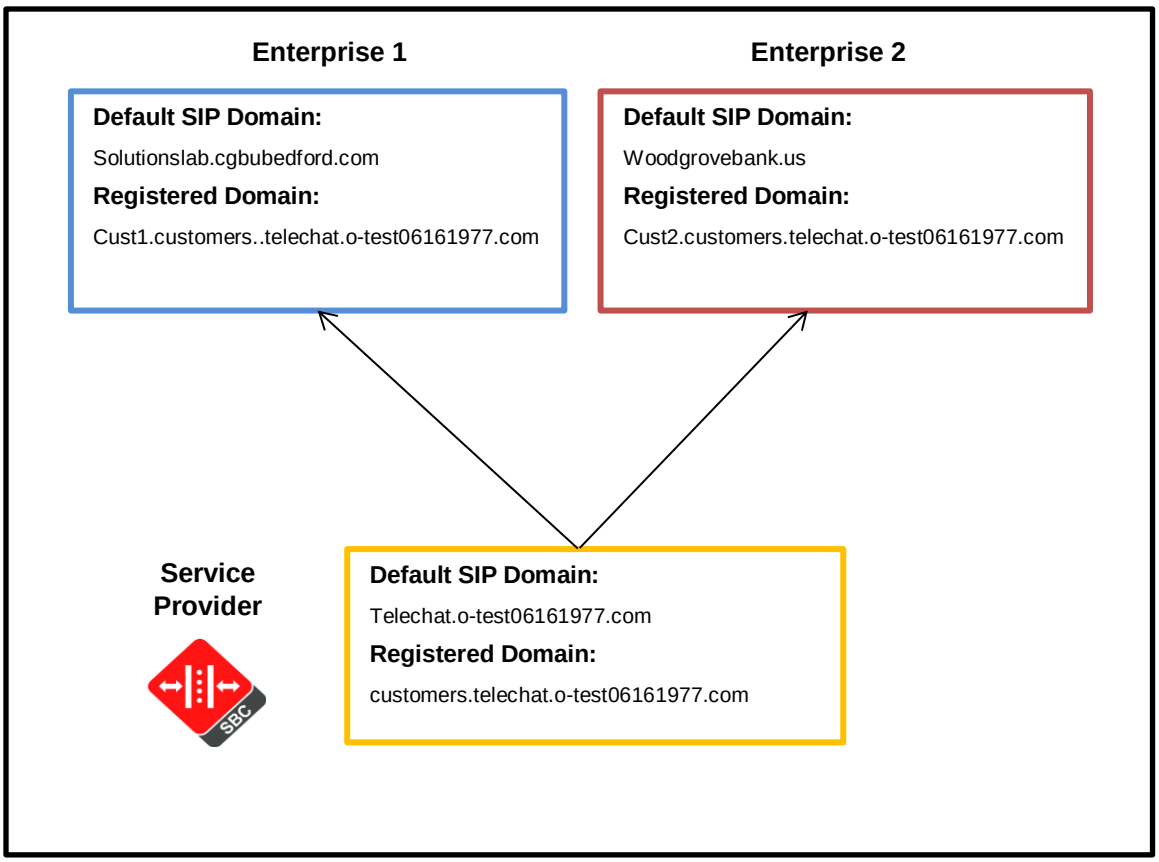
Below shows the connection topology example for MSFT Teams Carrier Model.
There are multiple connections shown:

- Teams Direct Routing Interface on the WAN
- Service provider Sip trunk terminating on the SBC



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

The below illustration and table are the Tenant Domain Structure used for this Application Note.



New Domain Name	Type	Registered Tenant	Certificate SAN for SBC	Tenant Default Domain	FQDN presented in Contact header when sending Calls
Customers.telechat.0-test06161977.com	Base	Carrier	*.cusotmers.telechat.o-test06161977.com	Telechat.o-test06161977.com	NA, this is a service tenant, no users
Sbc1.Customers.telechat.0-test06161977.com	Subdomain	Customer	*.cusotmers.telechat.o-test06161977.com	Solutionslab.cgbubedford.com	Sbc1.Customers.telechat.0-test06161977.com
Sbc2.Customers.telechat.0-test06161977.com	Subdomain	Customer	*.cusotmers.telechat.o-test06161977.com	Woodgrovebank.us	Sbc2.Customers.telechat.0-test06161977.co

9.1 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).

9.2 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:.

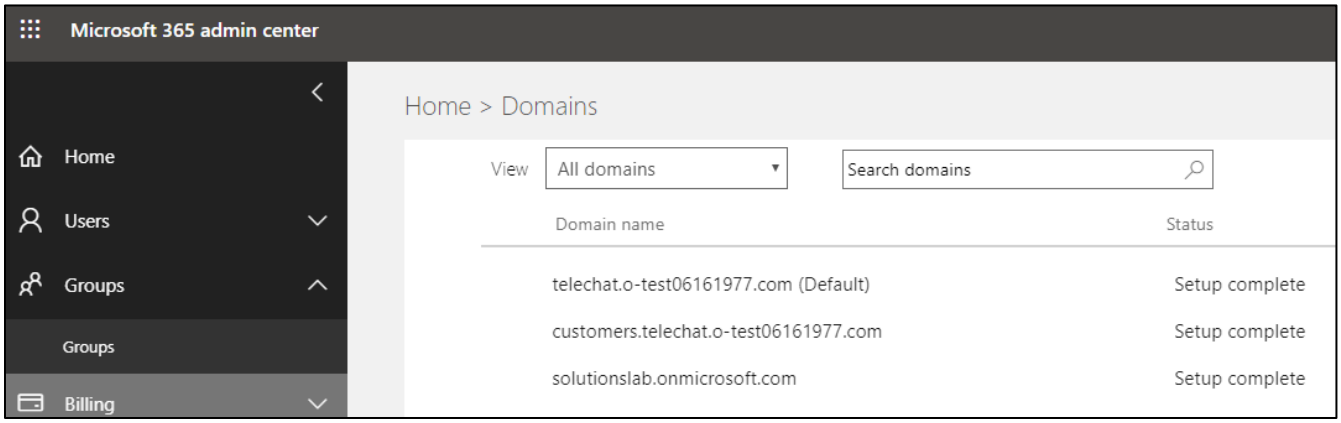
DNS Name	Can Be Used For SBC	Example of FQDN names
*.customers.adatum.biz	YES	**Valid FQDN:** • Sbc50.customers.adatum.biz • Sbc51.customer.adatum.biz • Ussbcsl5.customers.adataum.biz • Europe.customers.adatum.biz **Invalid FQDN:** • Sbc1.customers.europe.adatum.biz *(this would require registering domain name "Europe.adatum.biz")*
adatumbiz.onmicrosoft.com	NO	Using *.onmicrosoft.com domains is not supported for SBC names

9.3 SBC Domain Name in Carrier Tenant

Below is an example of registered DNS names in the Carrier Tenant:

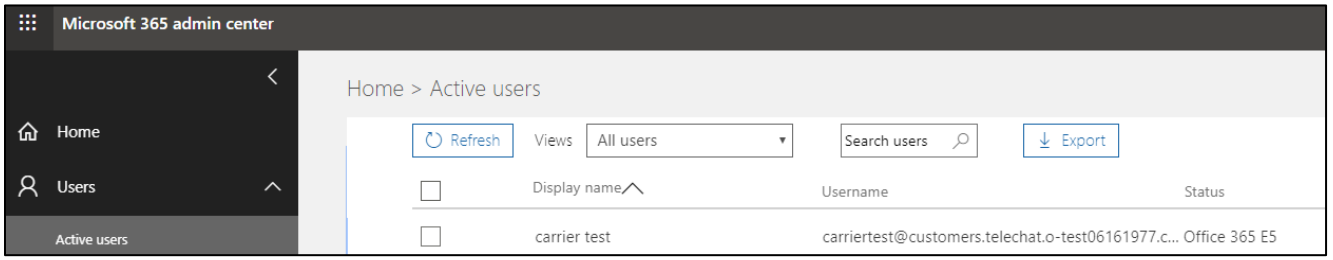
- Carrier Default Domain: **telechat.o-test06161977.com**
- Carrier Subdomain: **customers.telechat.o-test06161977.com**

  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.



After you have registered a domain name, you need to activate it by adding at least one licensed user with the SIP address matching the created base domain.

In the below example we have created the user carriertest@customers.telechat.o-test06161977.com in the carrier tenant to activate the carrier base domain:



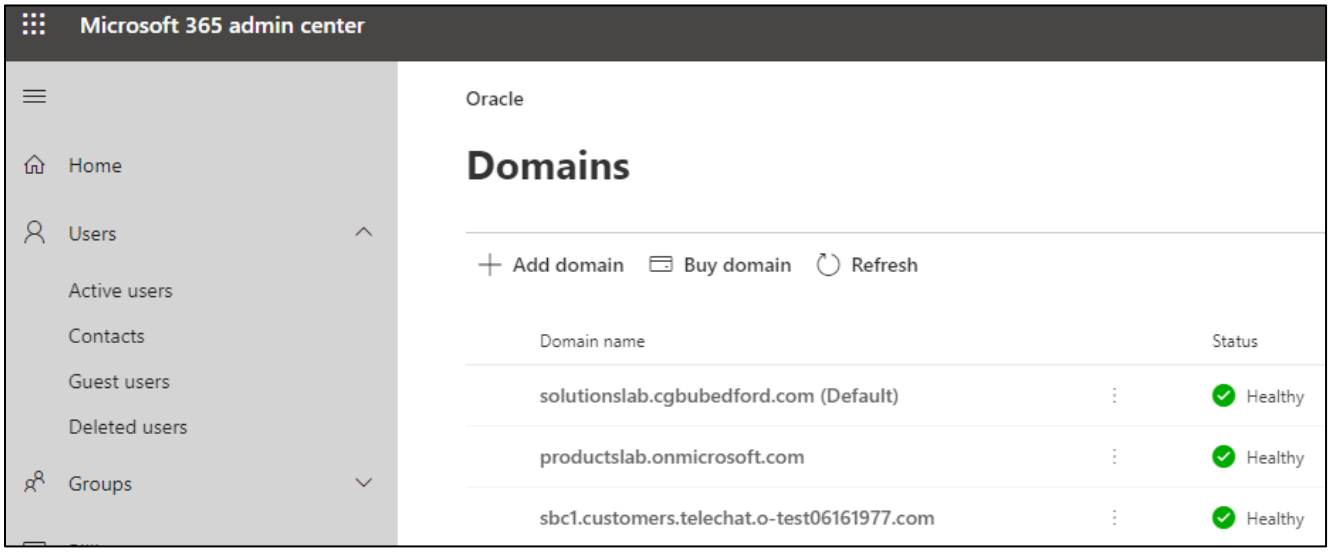
9.4 SBC Domain in Customer Tenant

For each customer tenant, you must register a subdomain that belongs to a carrier that points to a customer tenant.

In the below example:

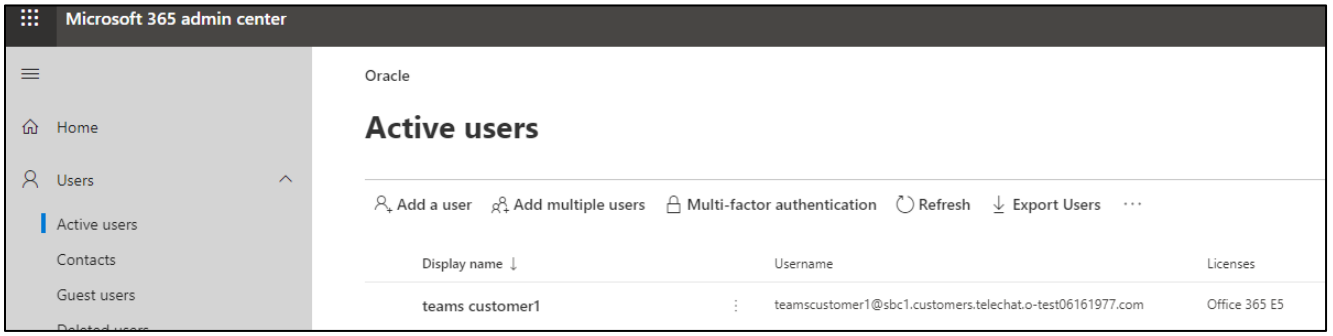
- Customer Tenant Default Domain: **solutionslab.cgbubedford.com**
- Carrier subdomain: **sbc1.customers.telechat.o-test06161977.com**

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.



Same as the carrier tenant above, once you register the domain, you must activate it by adding at least one licensed user with the SIP address matching the carrier subdomain in the customer tenant.

Below, we have added the user teamscustomer1@sbc1.customers.telechat.o-test06161977.com to activate the carrier subdomain in the customer tenant.



For the purposes of this example, the following IP address and FQDN's are used:

Note: all fqdn's listed below resolve to the same public IP address

FQDN Names	Public IP Address
customers.telechat.o-test06161977.com	**141.146.36.68**
sbc1.customers.telechat.o-test06161977.com	
sbc2.customers.telechat.o-test06161977.com	

10 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.

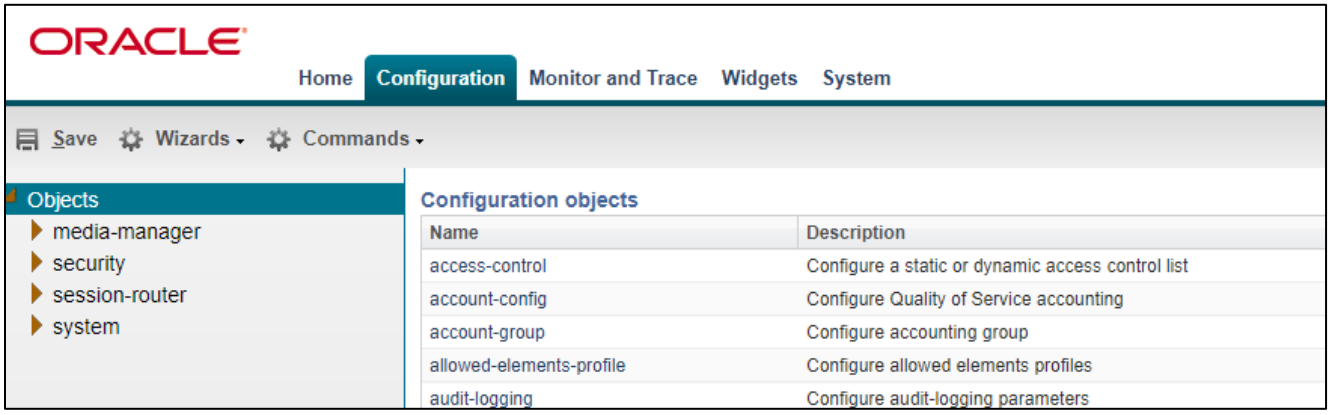
This guide assumes the OCSBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, web-server-config has been enabled for GUI access. If you require more information on how to install your SBC platform, please refer to the ACLI configuration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

Please note, the below configuration example assumes Media Bypass is enabled on the MSFT Teams Tenant. For differences in the OCSBC configuration for Non Media Bypass, please see Appendix A



10.1 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

10.1.1 System-Config

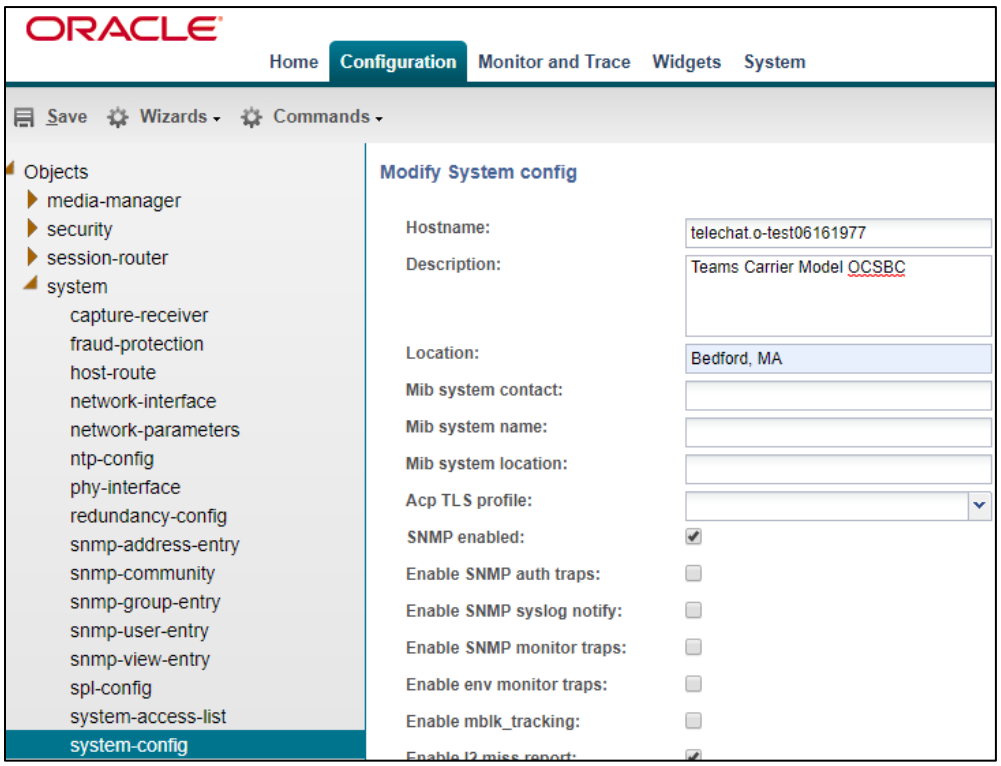
To configure system level functionality for the OCSBC, you must first enable the system-config

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)



- Click the OK at the bottom of the screen

10.1.2 Media Manager

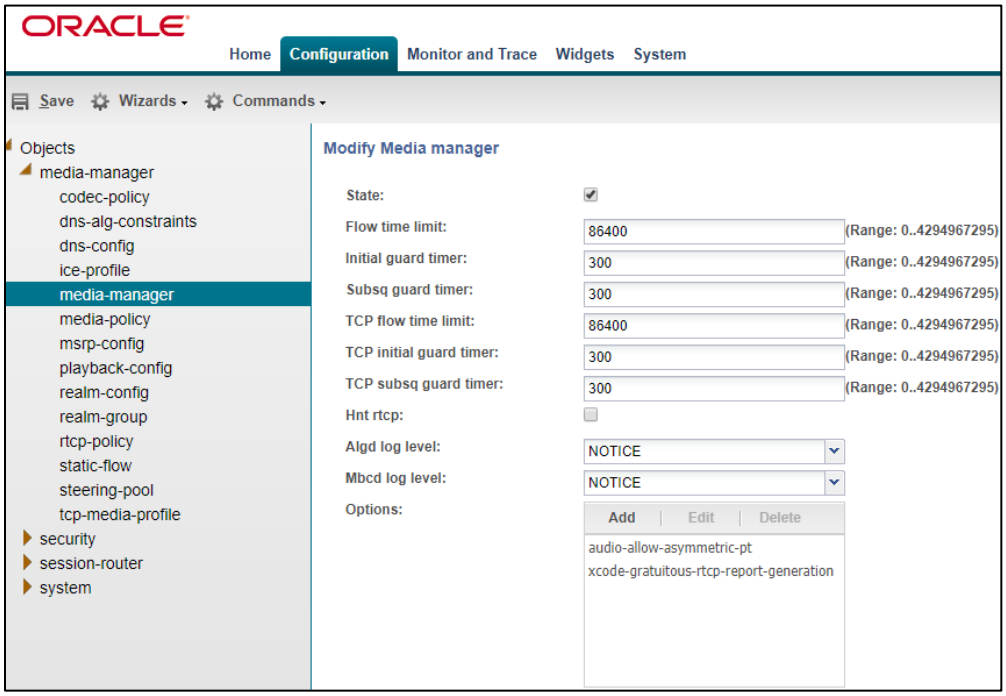
To configure media functionality on the SBC, you must first enabled the global media manager

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)
- Hit OK in the box



- Click OK at the bottom

10.1.3 Sip Config

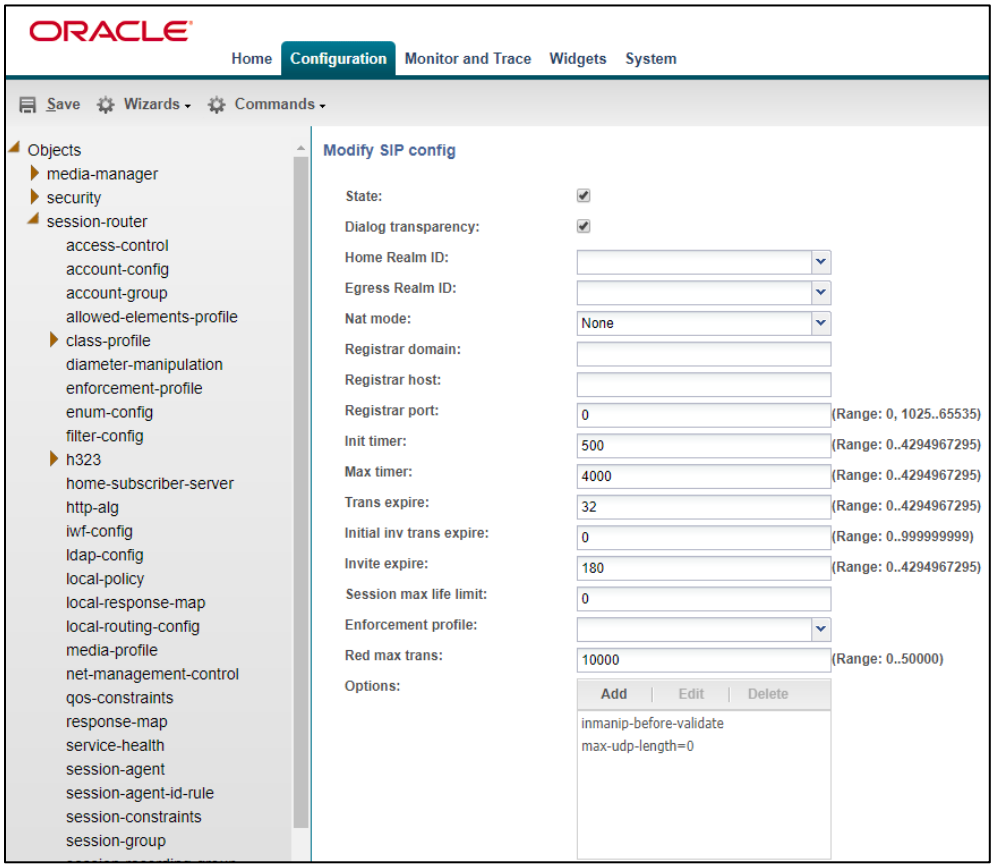
To enable sip related objects on the OCSBC, you must first configure the global Sip Config element:

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



- Click OK at the bottom

10.2 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 Teams Direct Routing, the other to connect to PSTN Network.

10.2.1 Physical Interfaces

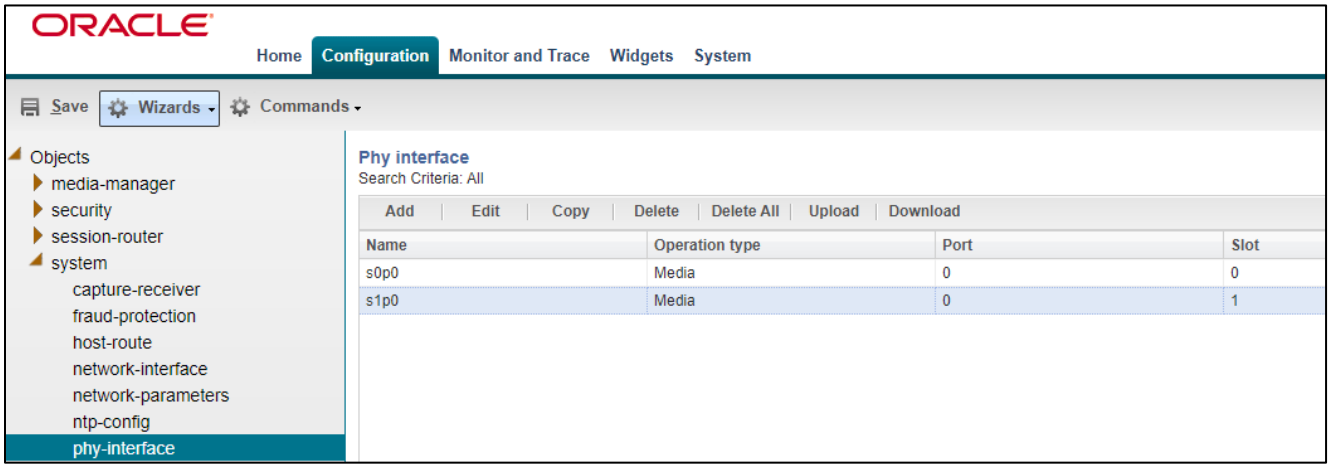
GUI Path: system/phy-interface

ACLI Path: config t→system→phy-interface

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

Config Parameter	Teams	PSTN
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



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

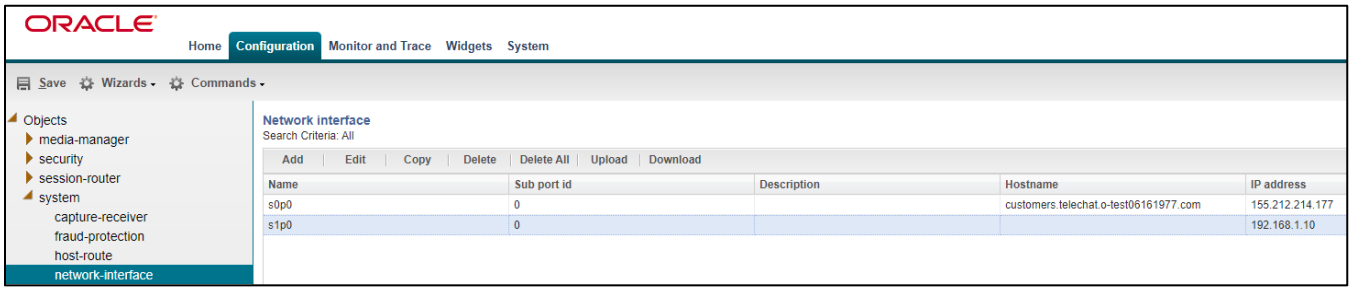
10.2.2 Network Interfaces

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
Name	s0p0	s1p0
Hostname	Carrier Base Domain	
IP Address	155.212.214.177	192.168.1.10
Netmask	255.255.255.0	255.255.255.0
Gateway	155.212.214.1	192.168.1.1
DNS Primary IP	8.8.8.8	
DNS Domain	Carrier Default Domain	



Please note: If running the latest GA release SCZ830m1p8A, hostname parameter in Network Interface is not mandatory, See Appendix C for additional details

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

10.3 Security Configuration

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

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

10.3.1 Certificate Records

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

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

GUI Path: security/certificate-record

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)

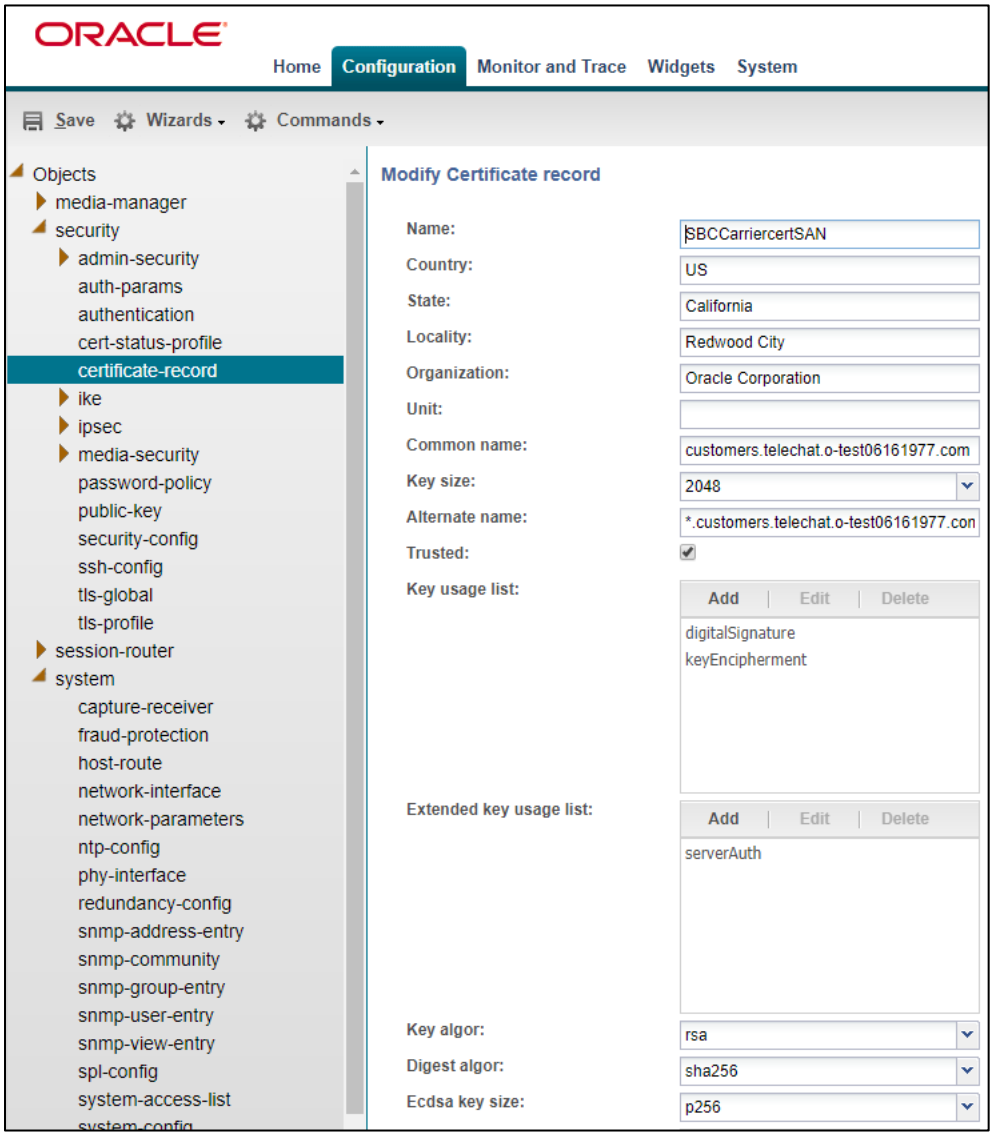
10.3.1.1 SBC End Entity Certificate

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

- Common name: Carrier Base Domain (**customers.telechat.o-test06161977.com**)
- Alternate Name: *.Carrier Base Domain (***.customers.telechat.o-test06161977.com**)

To Configure the certificate record:

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



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

10.3.1.2 Root CA and Intermediate Certificates

10.3.1.2.1 Digicert Root and Intermediate Certificates:

The following, DigitCertRoot and DigicertInter are the root and intermediate CA certificates used to sign the SBC's end entity certificate. As mentioned above, the intermediate certificate is optional, and only required if your server certificate is signed by an intermediate.

10.3.1.3 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://cacert.omniroot.com/bc2025.pem

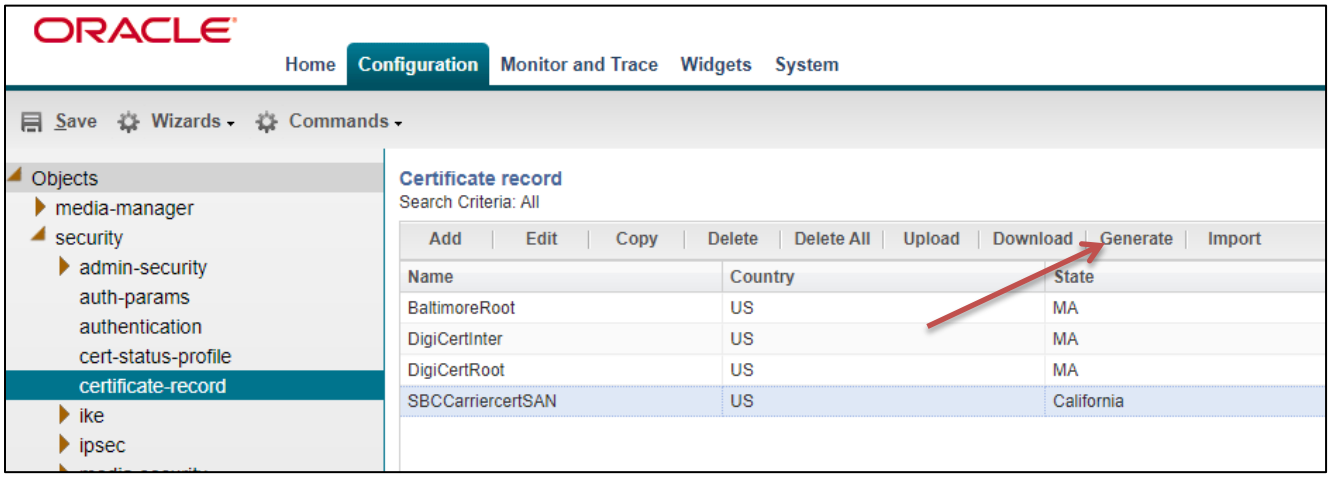
Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.

Config Parameter	Baltimore Root	Digicert Intermediate	DigiCert Root CA
Common Name	Baltimore CyberTrust Root	DigiCert SHA2 Secure Server CA	DigiCert Global Root CA
Key Size	2048	2048	2048
Key-Usage-List	digitalSignature keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth	serverAuth	serverAuth
Key algor	rsa	rsa	rsa
Digest-algor	Sha256	Sha256	Sha256

10.3.1.4 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**.

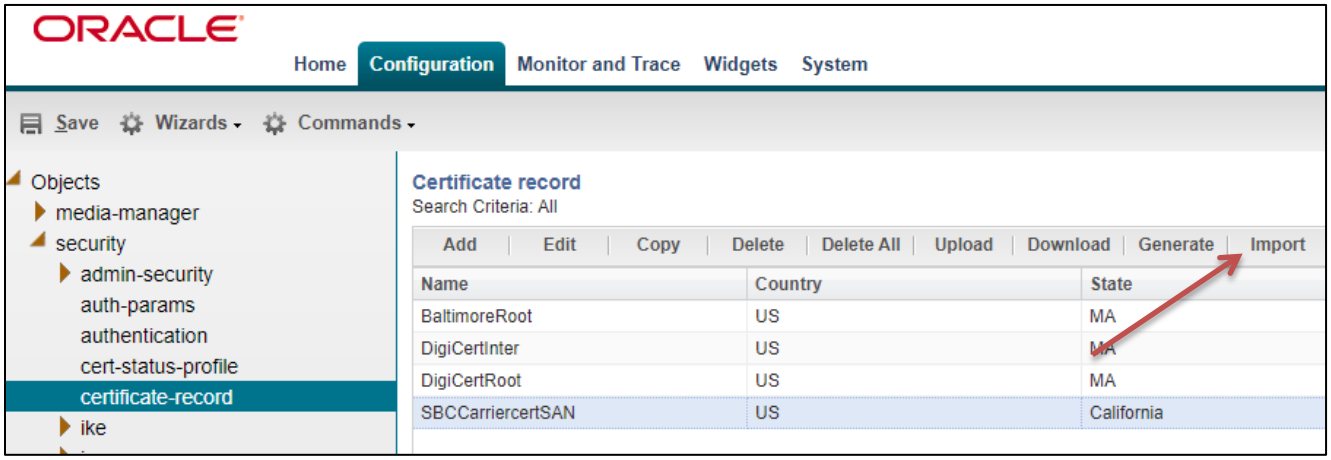
On the certificate record page in the OCSBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:

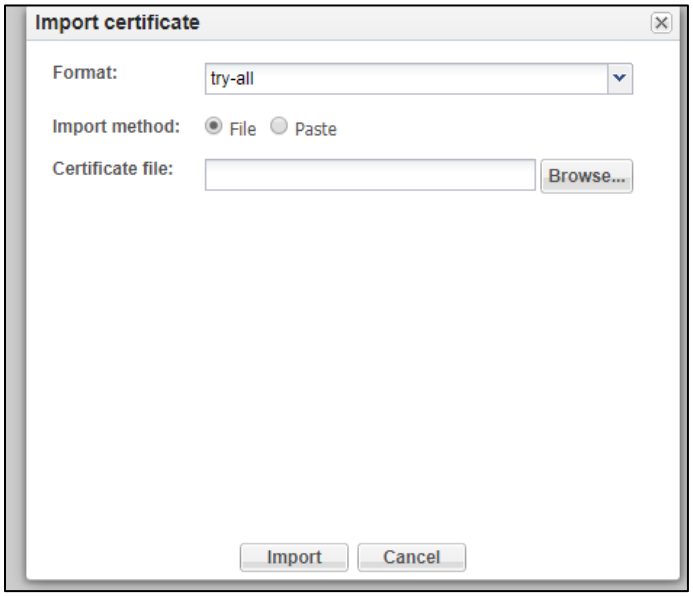


- copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, **a save and activate is required** before you can import the certificates to each certificate record created above.

10.3.1.5 Import Certificates to SBC

Once certificate signing request have been completed – import the signed certificate to the SBC.
Please note – all certificates including root and intermediate certificates are required to be imported to the SBC.
Once all certificates have been imported, issue **save/activate** from the WebGUI





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.

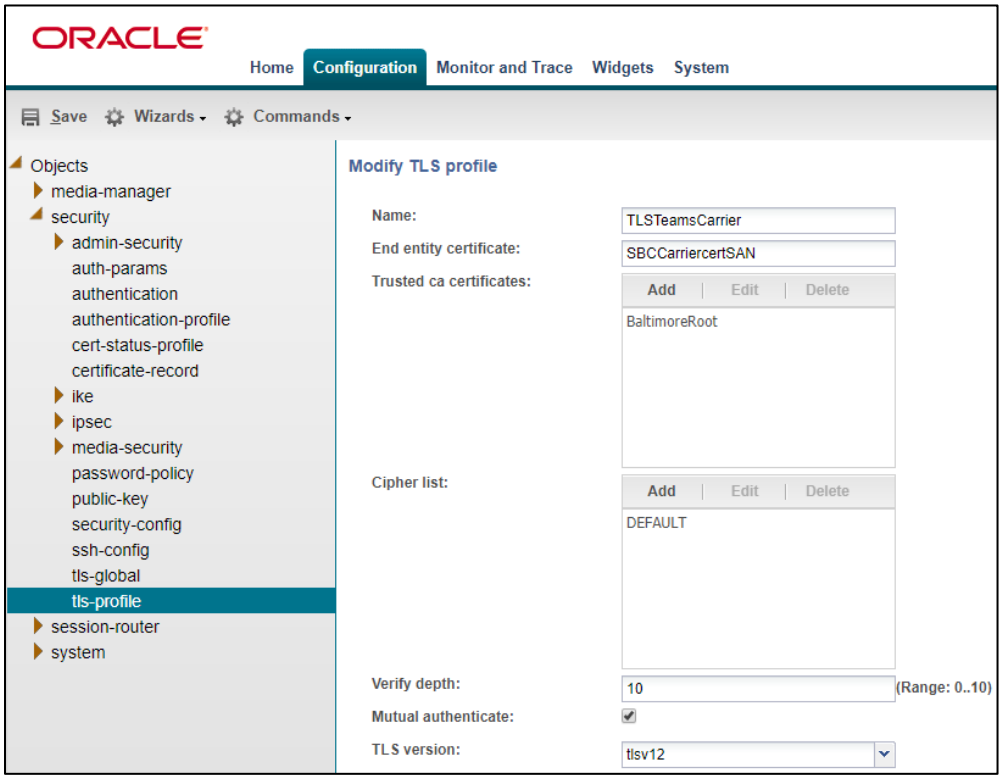
10.3.2 TLS Profile

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

GUI Path: security/tls-profile

ACLI Path: config t→security→tls-profile

- Click Add, use the example below to configure



- Click OK at the bottom

10.3.3 Media Security Configuration

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

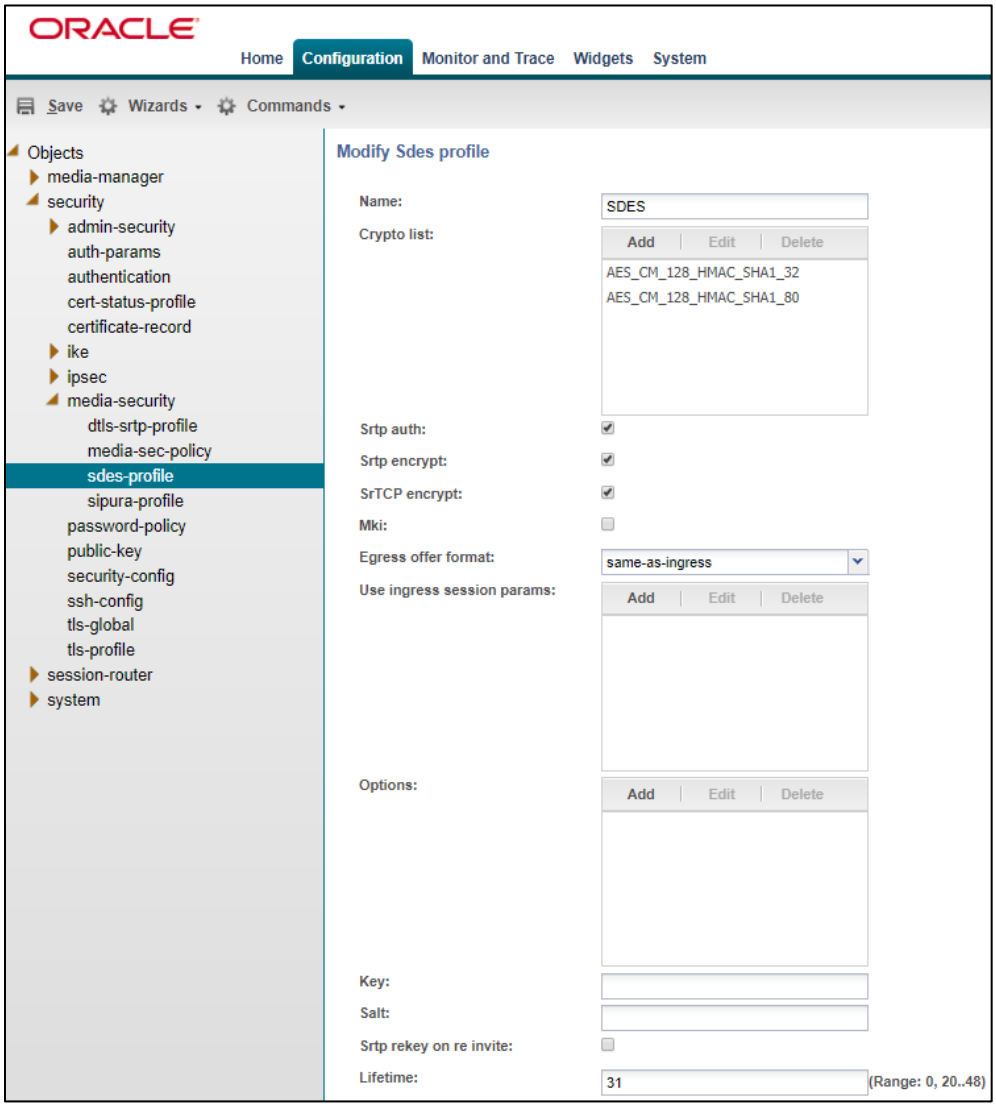
10.3.3.1 Sdes-profile

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



Note: The lifetime parameter set to a value of 31 is required for Microsoft Teams

- Click OK at the bottom

10.3.3.2 Media Security Policy

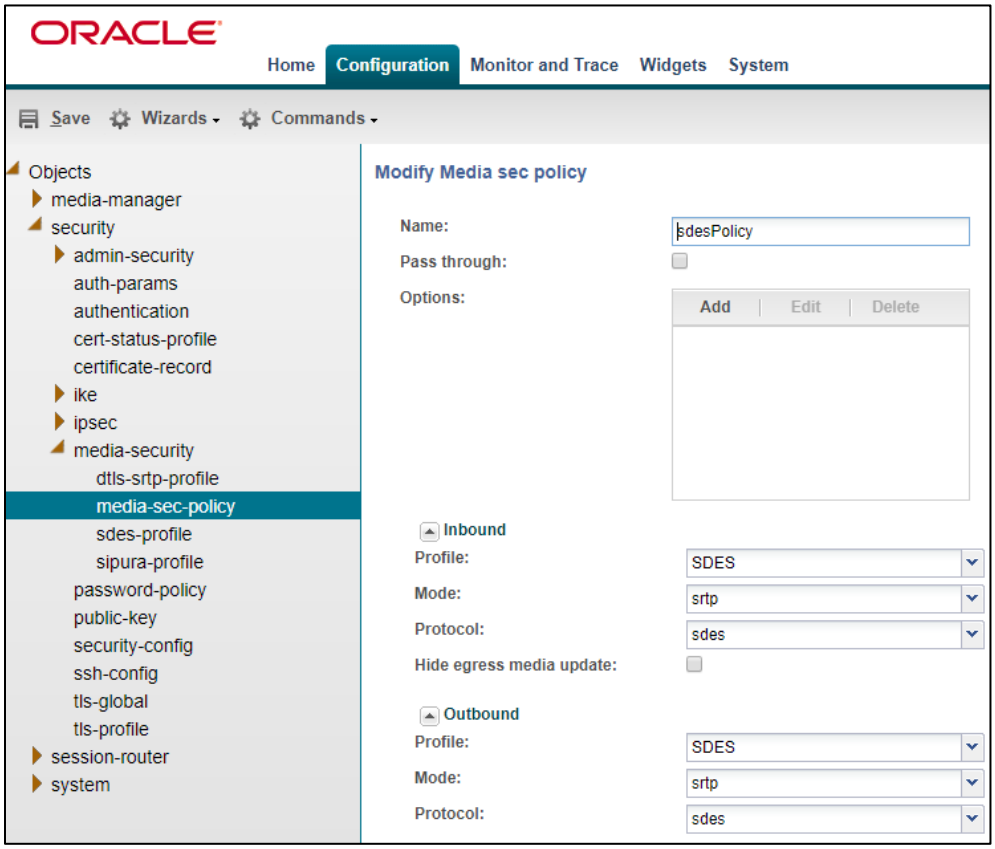
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them) and, if SRTP needs to be used, the sdes-profile that needs to be used

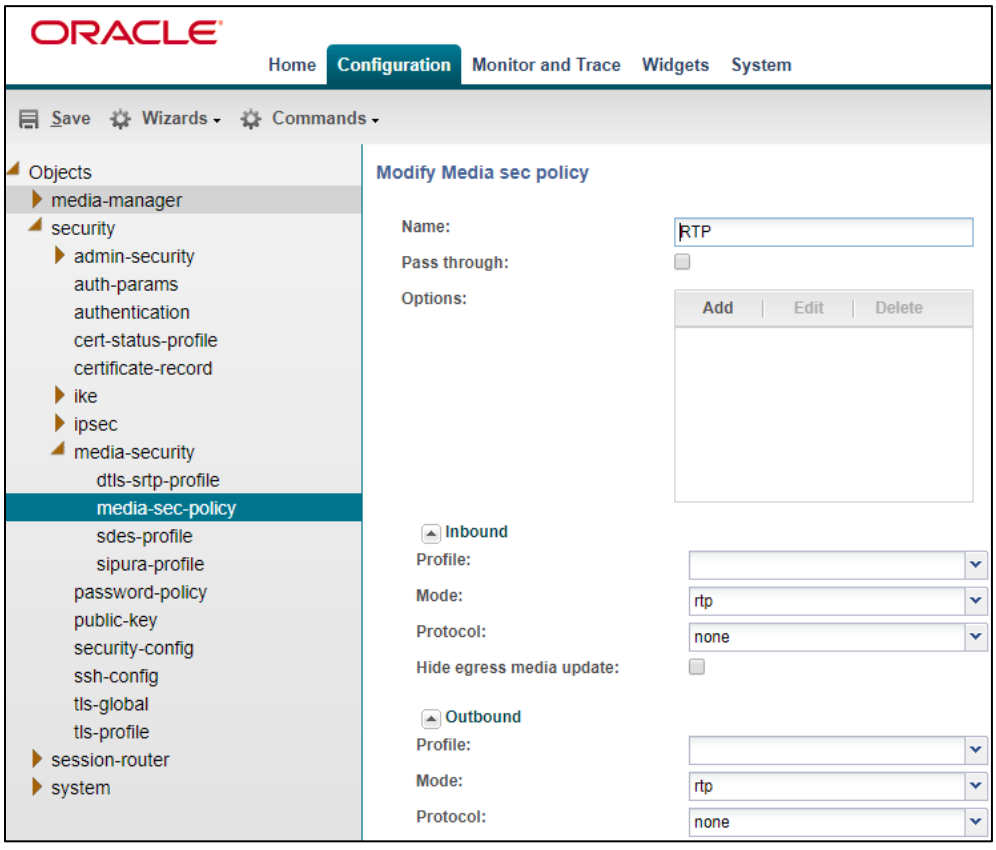
In this example, we are configuring two media security policies. One to secure and decrypt media toward Microsoft Teams, the other for non secure media facing PSTN.

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





- Click OK at the bottom of each when applicable

10.4 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.

10.4.1 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.

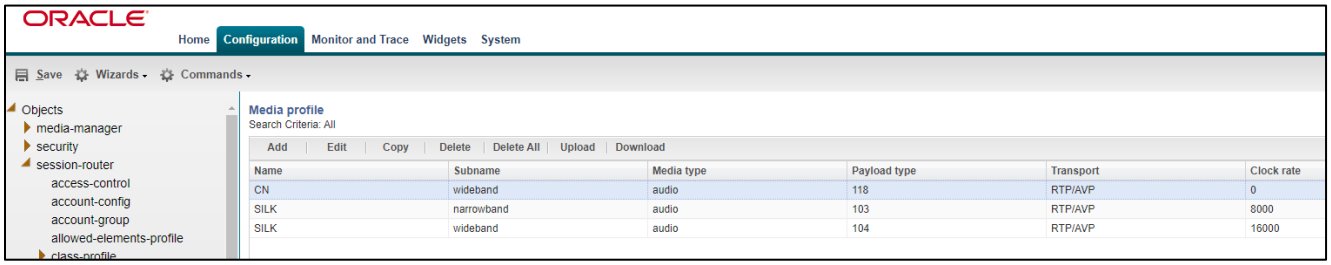
GUI Path: session-router/media-profile

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



- Click OK at the bottom of each when applicable

10.4.2 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

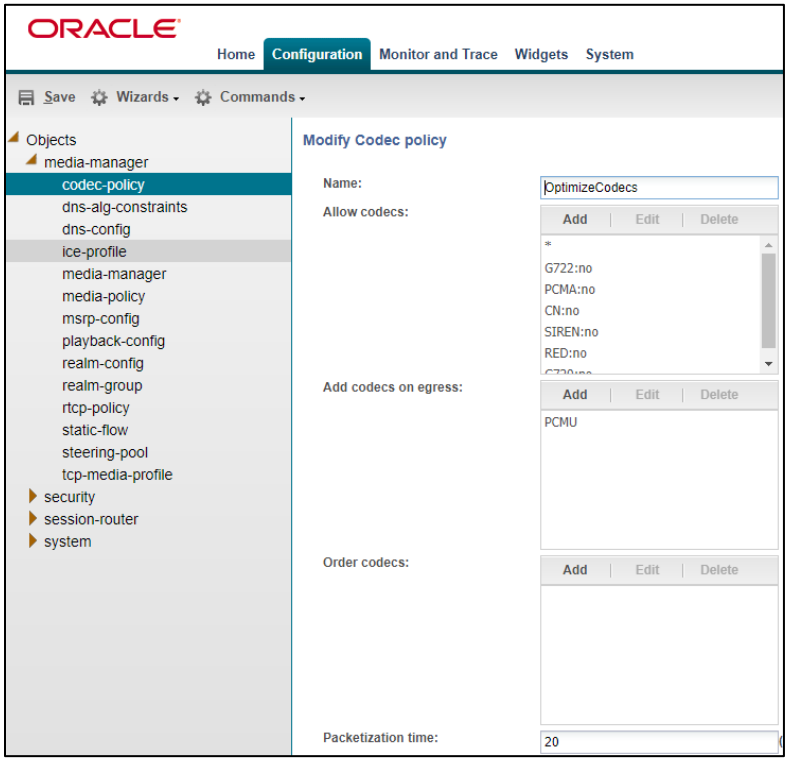
GUI Path: media-manager/codec-policy

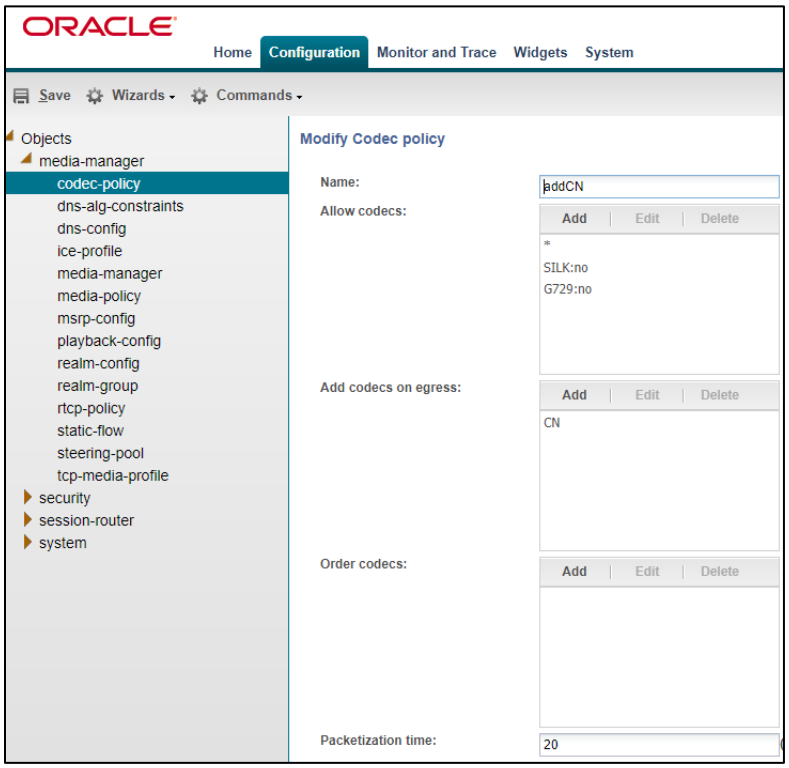
ACLI Path: config t→media-mangaer→codec-policy

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





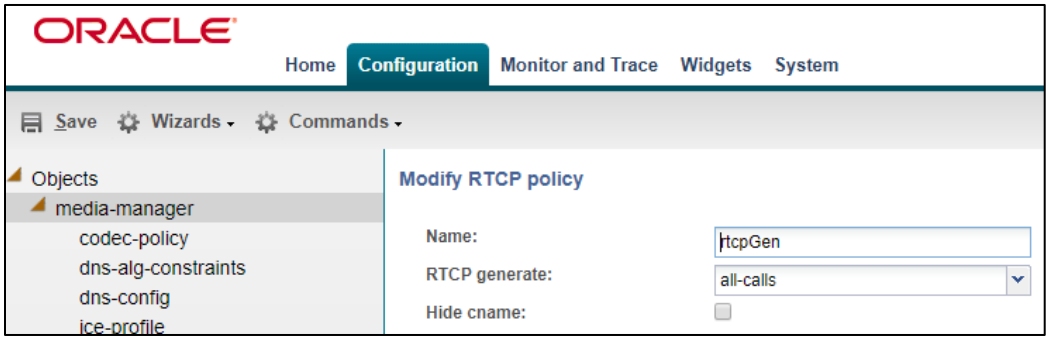
10.4.3 RTCP Policy

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



- Click OK at the bottom

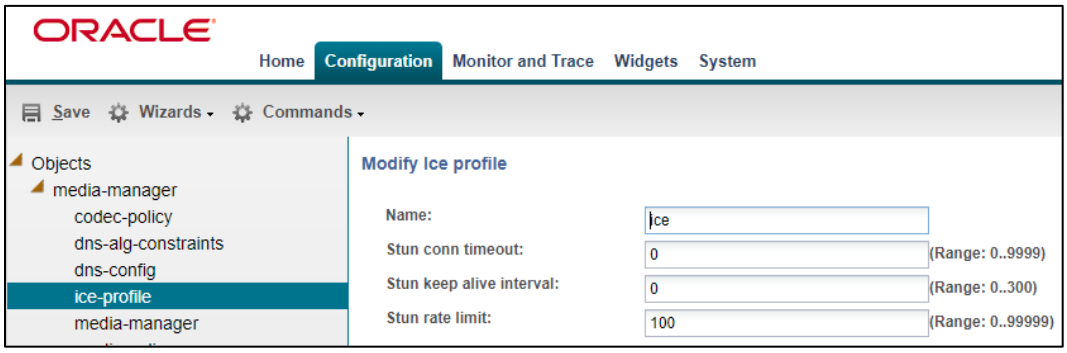
10.4.4 Ice Profile

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



- Click OK

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

10.5 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.

10.5.1 Realm Config

Nested Realm for Teams

Nested Realms is an OCSBC feature that supports hierarchical realm groups. One or more realms may be nested within a higher order realm. This allows the OCSBC to separate each tenant the Carrier Model OCSBC is servicing.

In this example we will create two realms facing MSFT Teams.

A parent realm for Teams and a child realm for a customer tenant. The parent realm will contain the carrier base domain, and the Tenant realm will contain the customer's carrier subdomain.

PSTN Realm

This is a standalone realm facing PSTN.

GUI Path; media-manger/realm-config

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

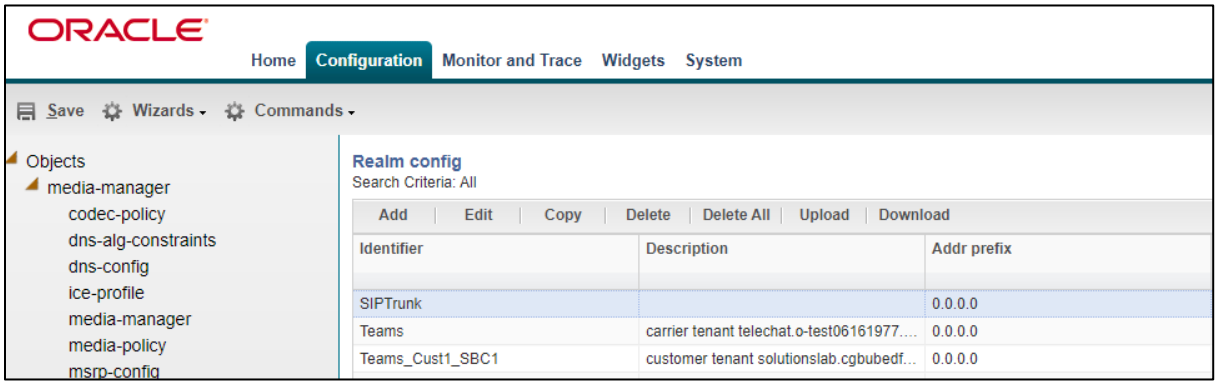
- Click Add, and use the following table as a configuration example for the three realms used in this configuration example

Config Parameter	Teams Realm	Tenant Realm	PSTN Realm
Identifier	Teams	Teams_Cust1_SBC1	SIPTrunk
Network Interface	s0p0:0	s0p0:0	s1p0:0
Mm in realm	☑	☑	☑
Parent Realm		Teams	
Media Sec policy	sdespolicy	sdespolicy	RTP
RTCP mux	☑	☑	
ice profile	ice	ice	
Codec policy	addCN	addCN	OptimizeCodecs
RTCP policy	rtcpGen	rtcpGen	
Trunk Context	(carrier base domain)	(tenant/carrier subdomain)	

Note: The Trunk-Context parameter is currently not available in the OCSBC GUI. This parameter must be added through the OCSBC ACLI and is required. The domains added to this parameter in each of the MSFT Realms are used as host-uri's in SIP messages. If you are running the latest GA release, SCZ830M1P8A, this parameter is no longer required. Please see Appendix C for more details

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

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



10.5.2 Steering Pools

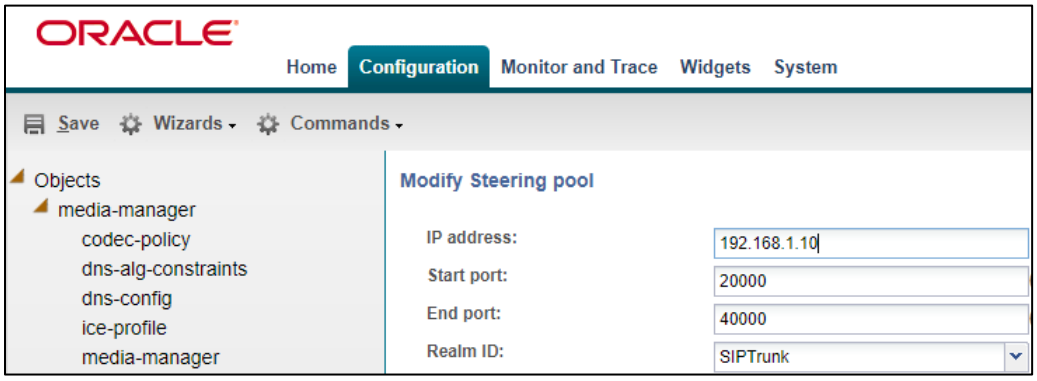
Steering pools define sets of ports that are used for steering media flows through the OCSBC.
These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

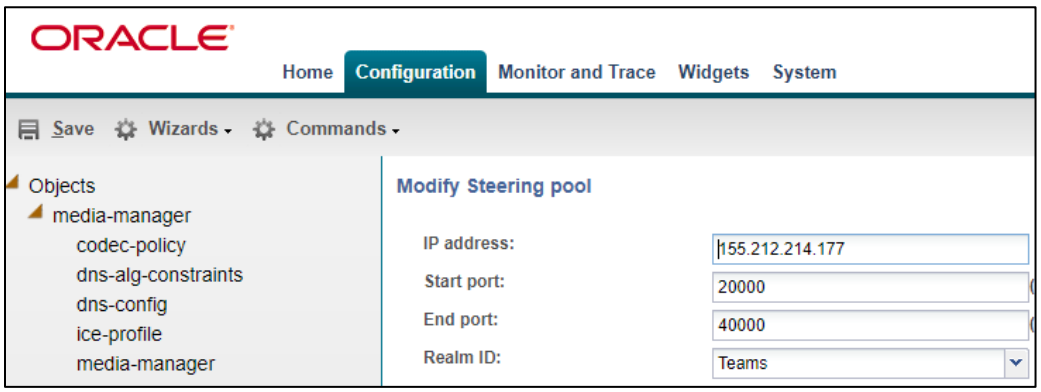
We configure one steering pool for PSTN. The other will be shared by all parent and child realms facing Teams.

GUI Path: media-manger/steering-pool

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

- Click Add, and use the below examples to configure





10.6 Sip Configuration

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

10.6.1 Sip Manipulations

For calls to be presented to Microsoft Teams or Sip Trunk from the OCSBC, the OCSBC requires alterations to the SIP signaling natively created. To do this, we must configure a series of sip manipulations in order to preset signaling packets that are acceptable to the MSFT Direct Routing Interface.

GUI Path: session-router/sip-manipulation

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

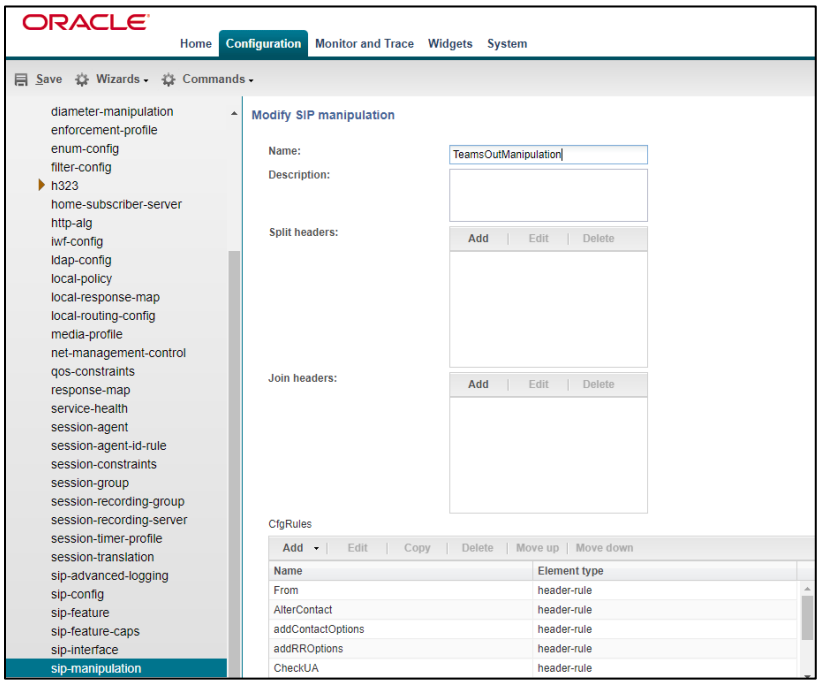
Note: If running the latest GA release, SCZ830m1p8A, please see Appendix C prior to configuring sip manipulations in your OCSBC

10.6.1.1 TeamsOutManip

The following sip manipulation is applied as an outmanipulationID and modifies signaling packets generated by the OCSBC destined for Teams.

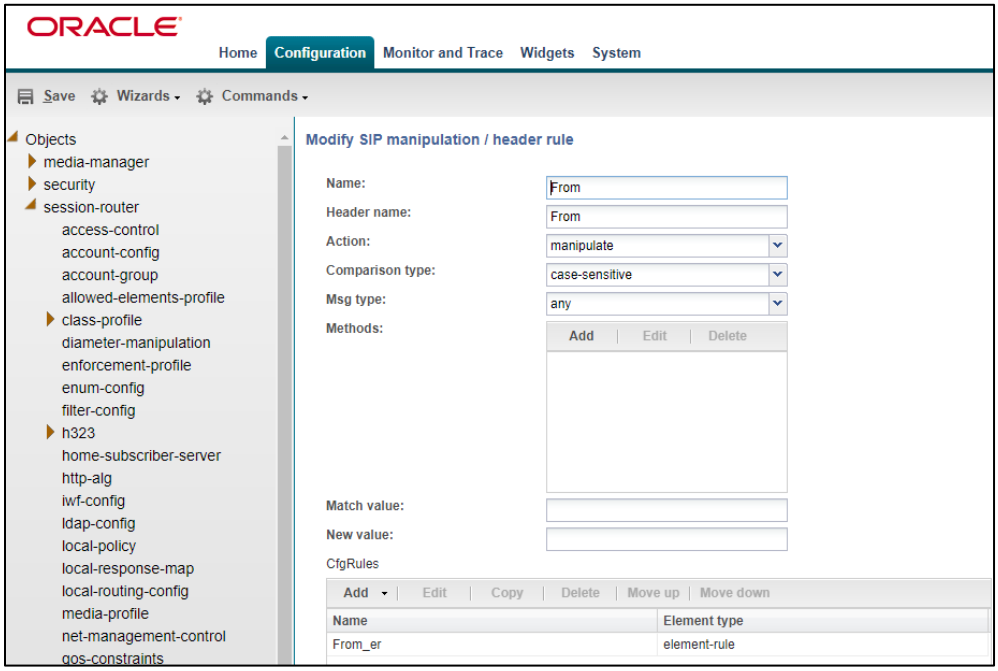
This manipulation performs the following modifications to SIP Packets:

- **Change_from_ip_fqdn**– changes the From header according to MSFT requirements
- **Alter_contact**-changes the contact header as per MSFT Teams requirements
- **Adduseragent/ModifyUA** – adds the SBC information in the User-Agent header,if the User-agent is not present already or modify if User-Agent header is present
- **Addcontactheaderinoptions** – Add a new Contact header to OPTIONS message
- **Recordroute** – Add a new Record-Route header to OPTIONS message

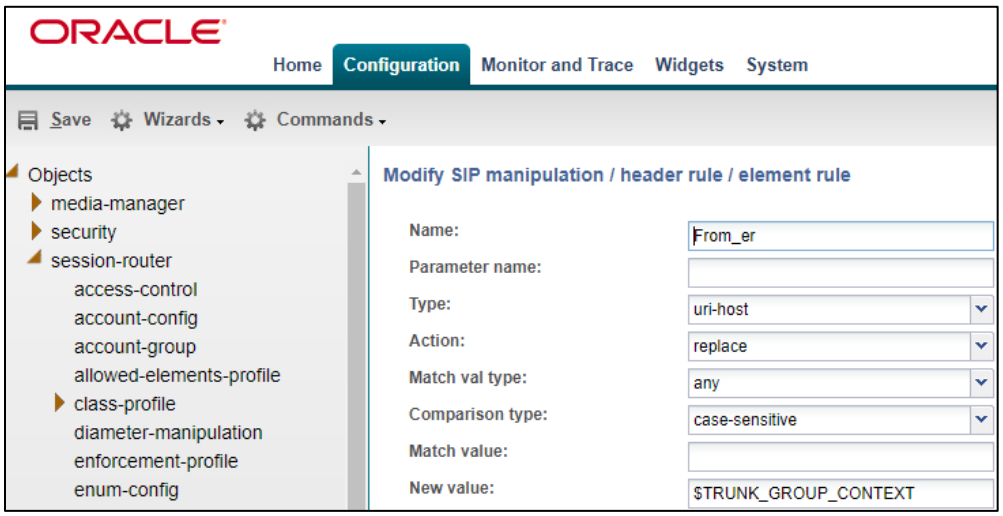


Change_From_IP_FQDN

Header Rule:

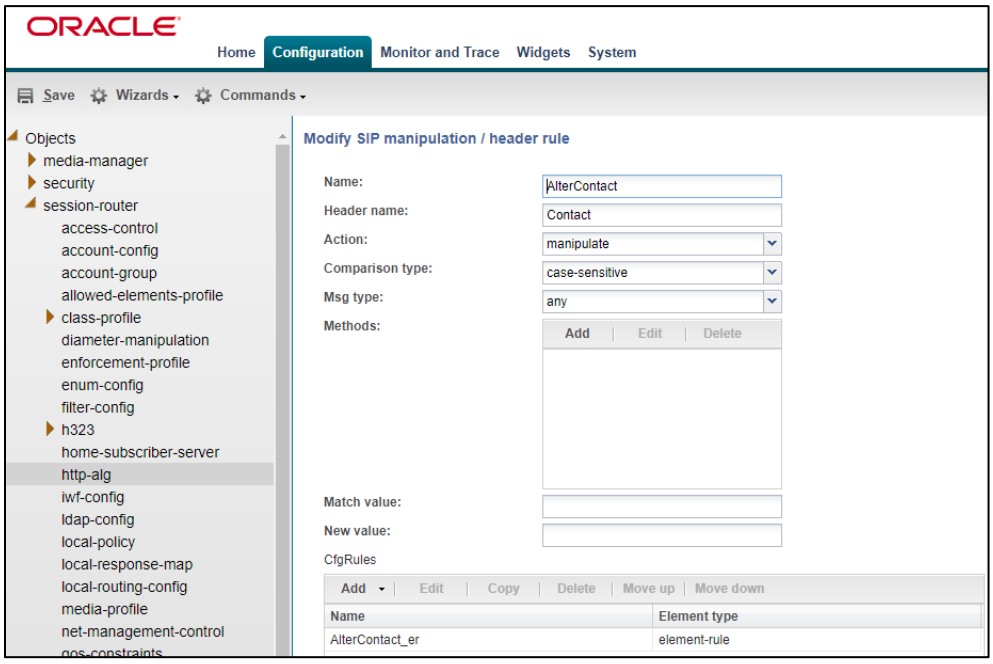


Element Rule:

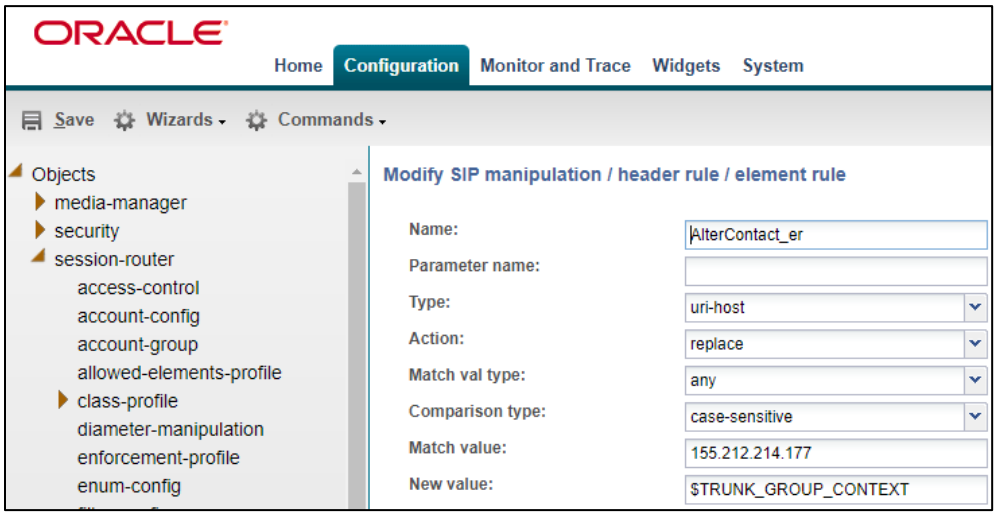


Alter Contact:

Header Rule:



Element Rule:

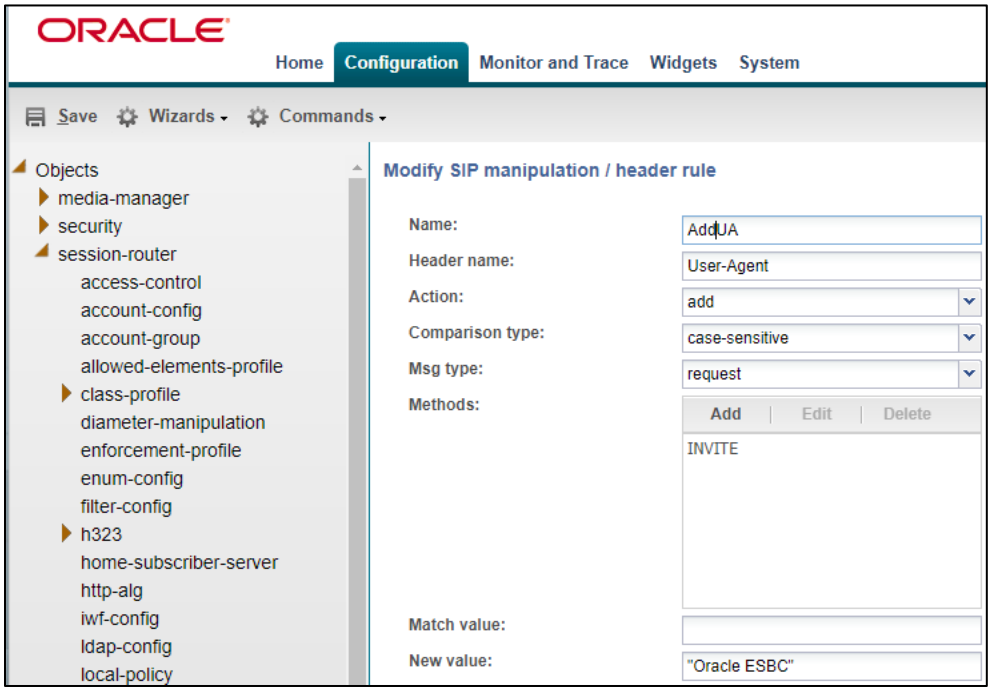


Notice in the above manipulations configurations the value, $TRUNK_GROUP_CONTEXT.
This is instructing the SBC to use the FQDN from the trunk-context parameter configured in each “Teams Realm”, which was added under Realm-Config previously in this document.

AddUserAgent:

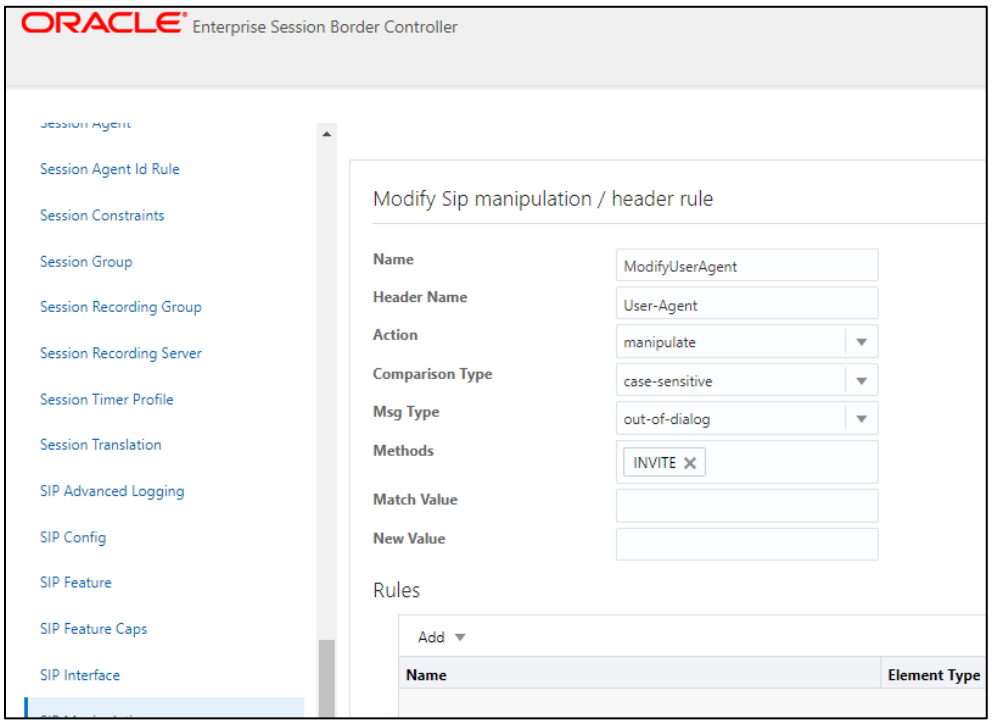
Header Rule:

Microsoft requires a User Agent header be included that contains SBC Information

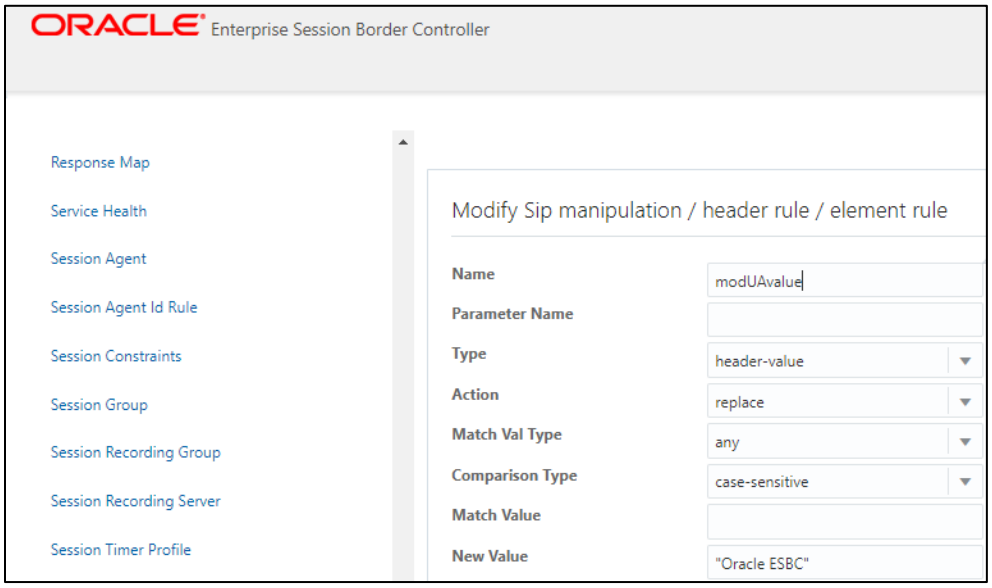


ModifyUserAgent

Header Rule:

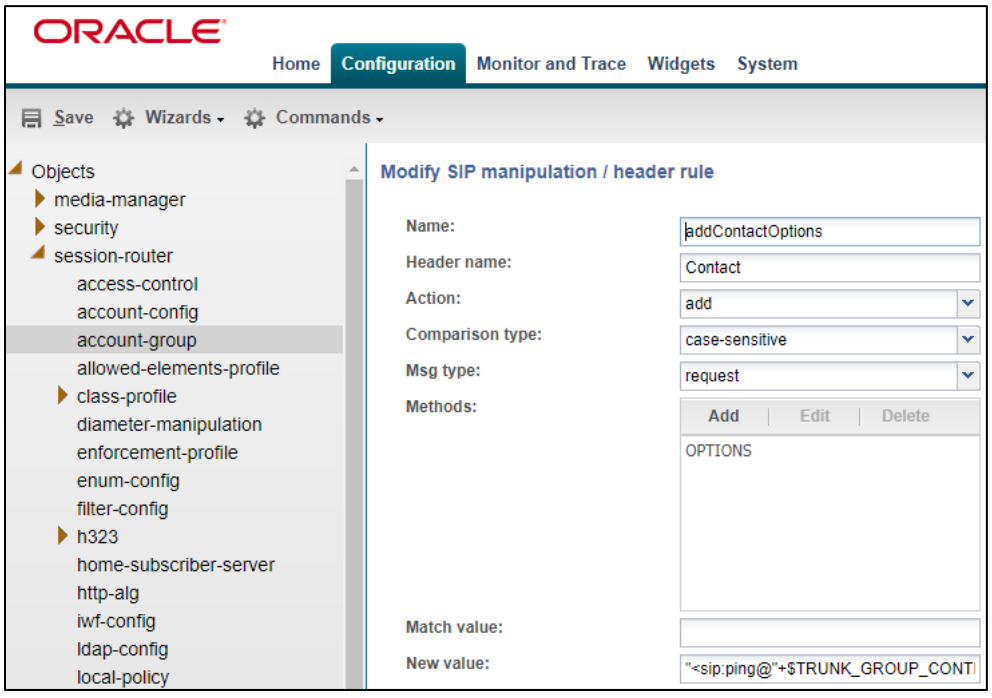


Element Rule:



AddContactHeaderOptions:

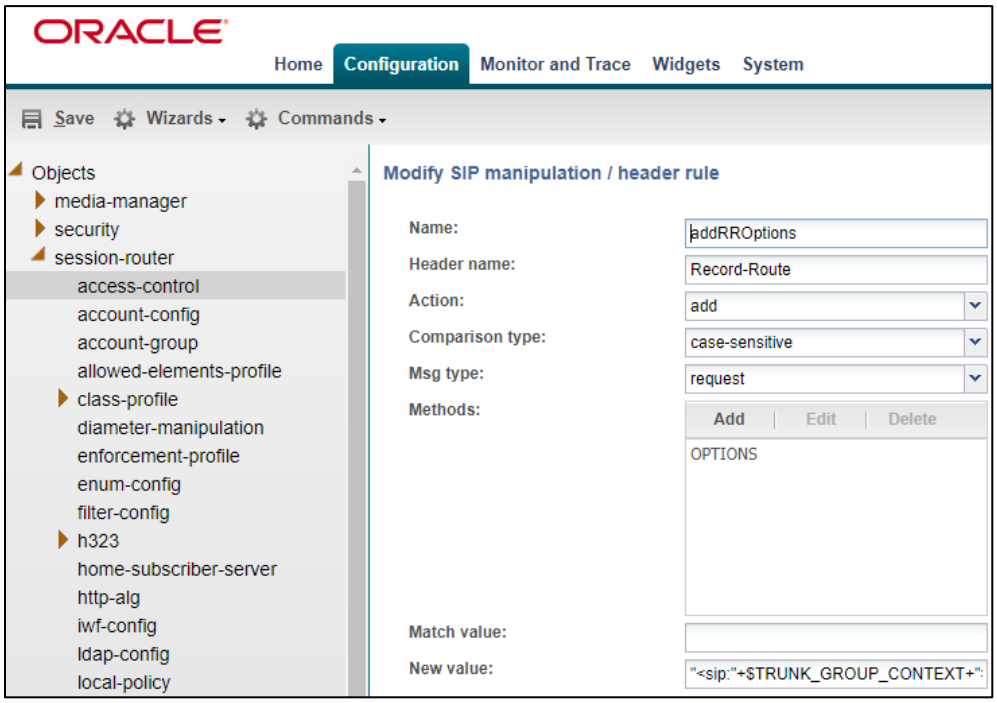
Header Rule:



New value: "<sip:ping@"+$TRUNK_GROUP_CONTEXT+":5061;transport=tls>"

RecordRoute

Header Rule:



New value: "<sip:"+$TRUNK_GROUP_CONTEXT+"

Additional Rules may be necessary if the Ringback feature is required to be enabled on the OCSBC in your environment. Please see Appendix B for further details.

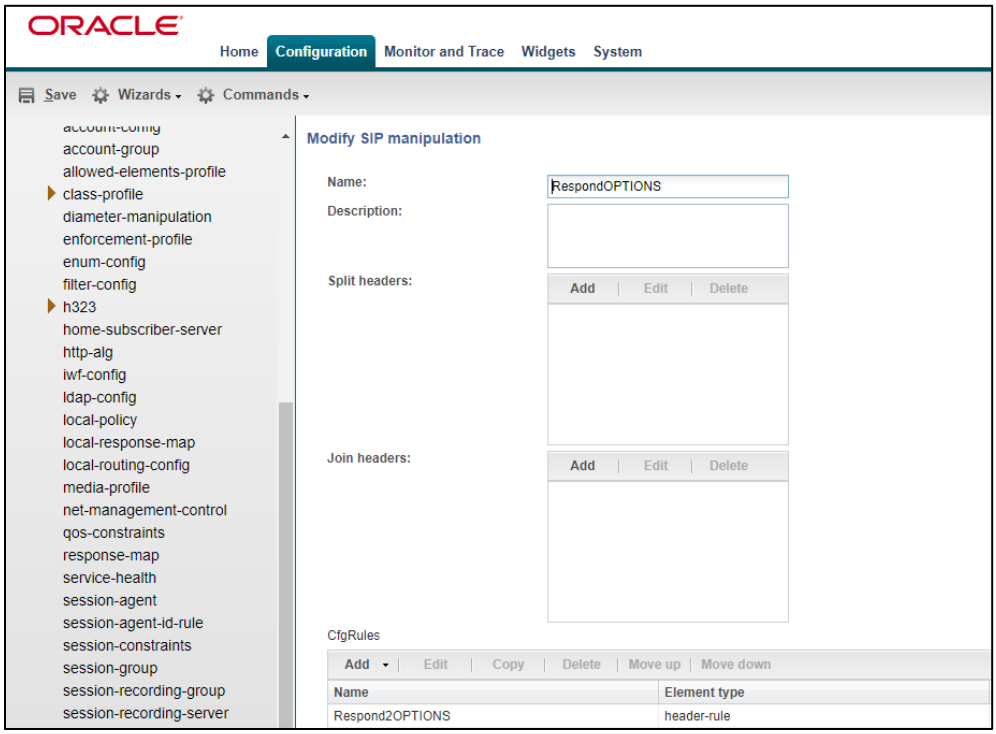
10.6.1.2 TeamsInManip

If you are running the latest GA release, SCZ830M1P8A, please see Appendix C before Configuring Manipulations

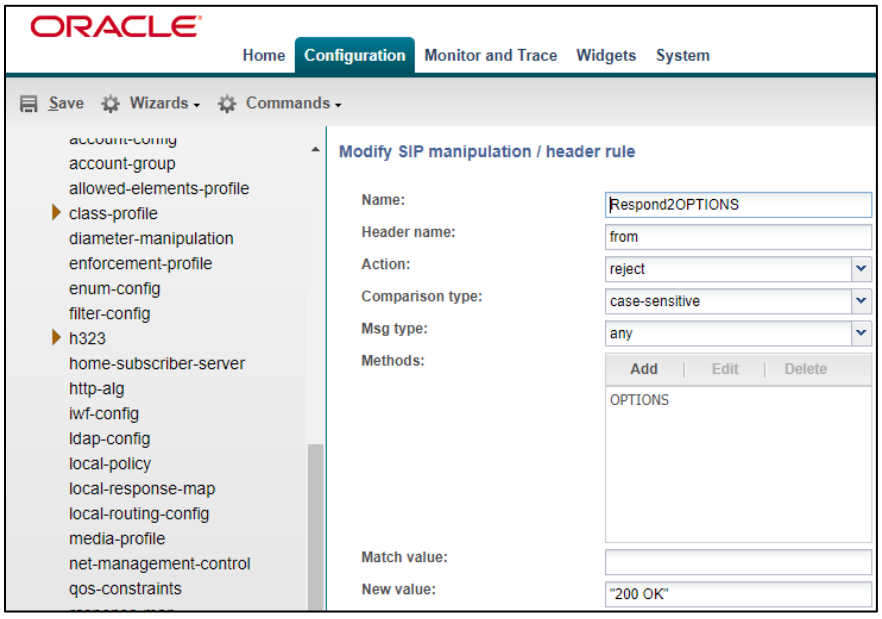
The following manipulation is configured to handle the SIP messages received inbound from Teams.

- **Respondoptions** – to handle the OPTIONS locally *(This sip-manipulation may also be configured and assigned as the in manipulation ID on the PSTN or Sip Trunk side to force the SBC to respond locally to OPTIONS requests being sent on Carrier Side)*

RespondOptions:



Header Rule:



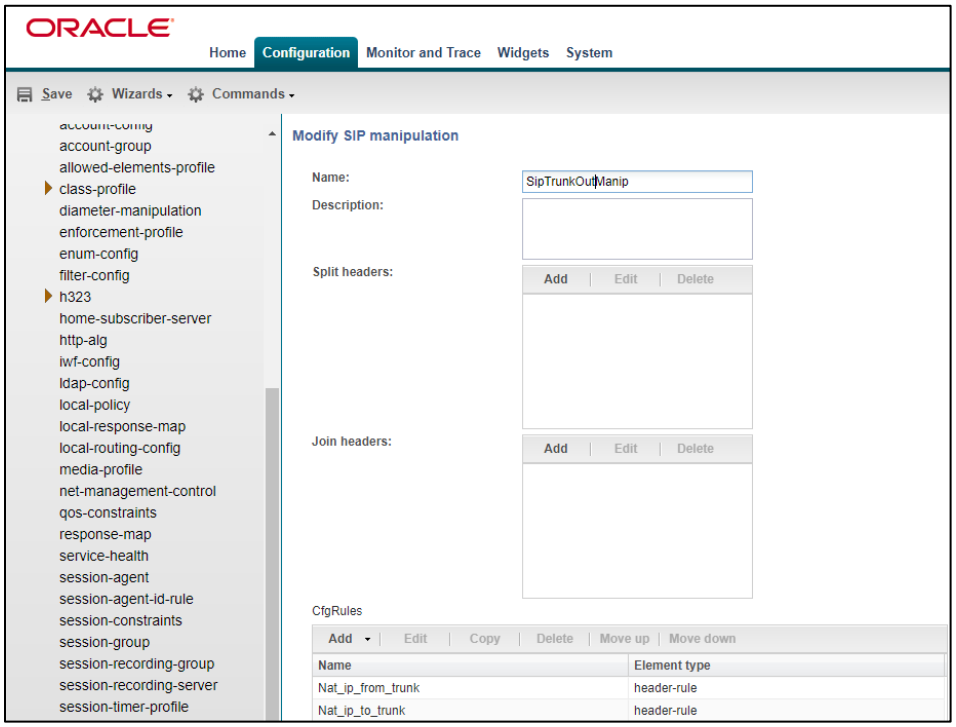
Additional Rules may be necessary if the Ringback feature is required to be enabled on the OCSBC in your environment. Please see Appendix B for further details.

Sip Trunk Manipulations:

SipTrunkOutManip

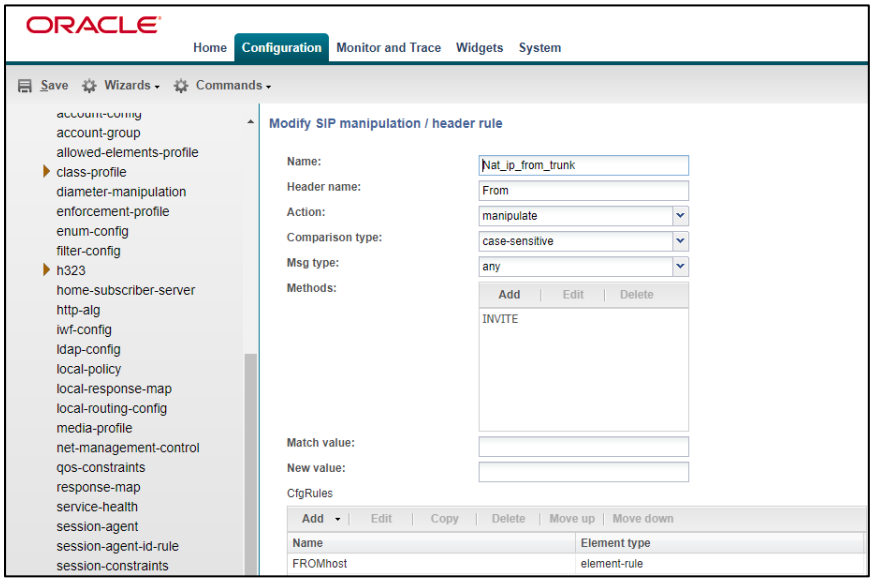
These manipulations are to be used on outgoing Sip Traffic from the SBC to the Sip Trunk.

- **Nat_ip_from_trunk**: replace the uri-host of the From header with the SBC's local ip.
- **Nat_ip_to_trunk**: replace the uri-host of the To header with the ip –address of the Trunk device

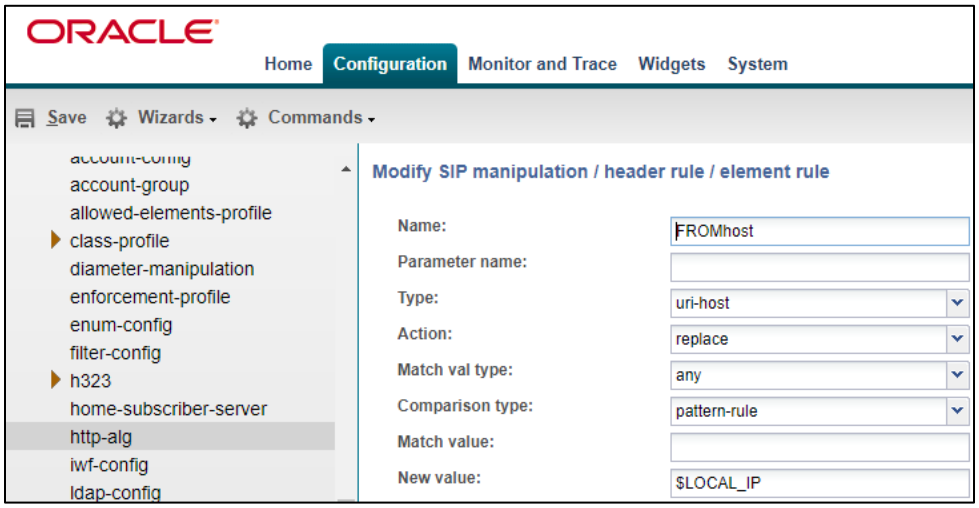


10.6.1.2.1 Nat_ip_from_trunk

Header Rule:

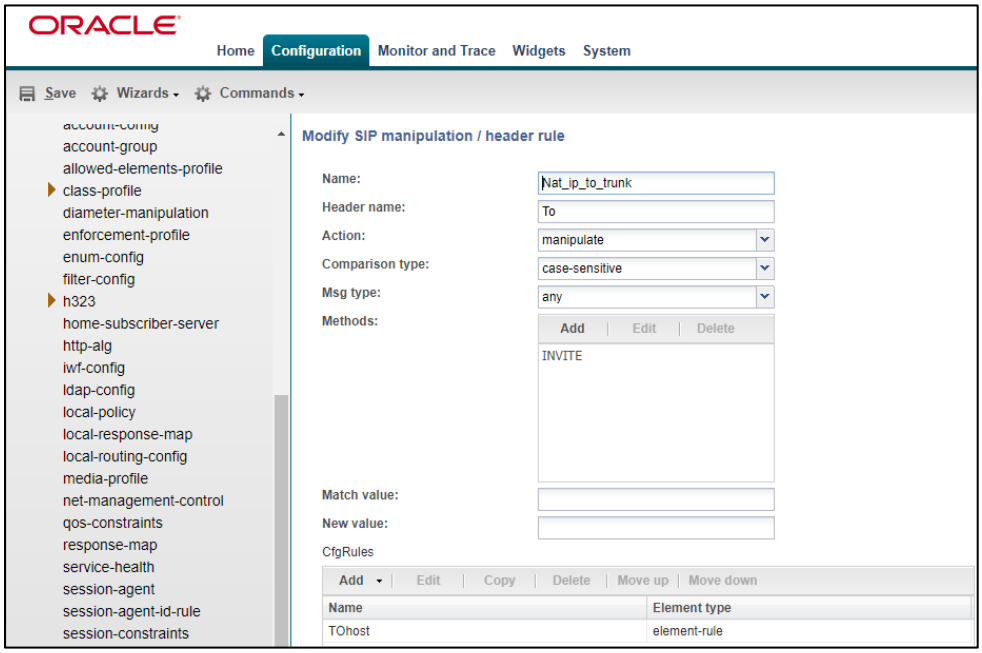


Element Rule:

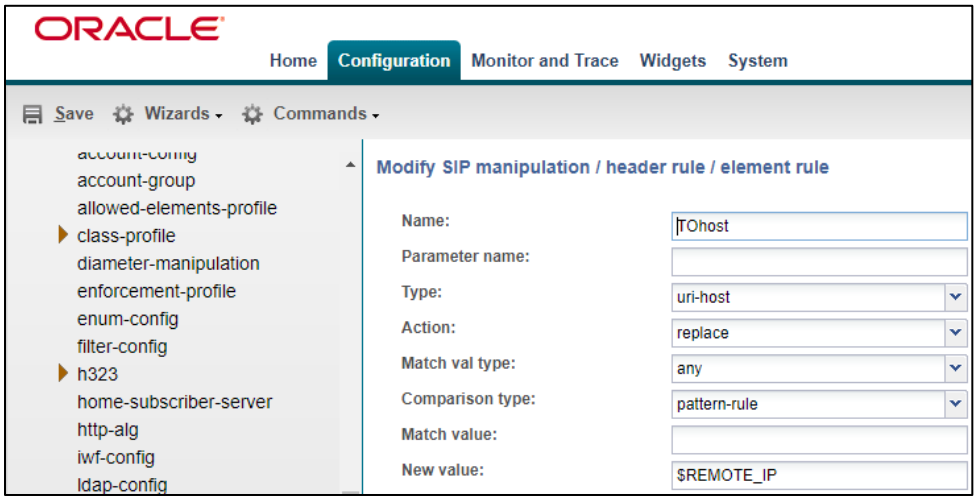


10.6.1.2.2 Nat_ip_to_trunk

Header Rule:



Element Rule:



10.6.2 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 shared by the Teams Nested Realms.

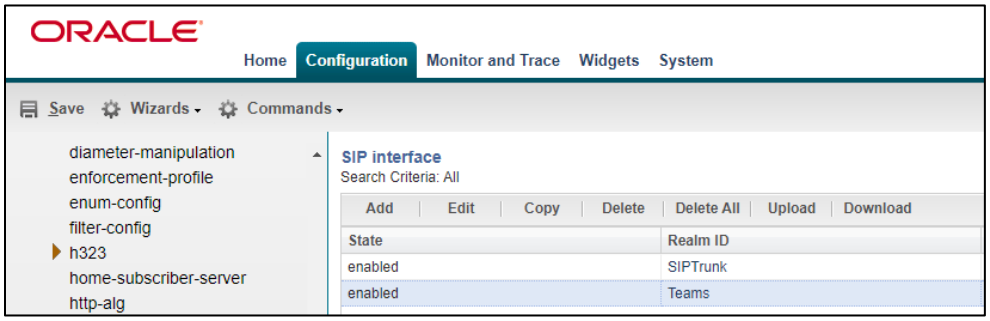
GUI Path: session-router/sip-interface

ACLI Path: config t→session-router→sip-interface
Click Add, and use the table below as an example to Configure:

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

- Sip-Manipulations
- TLS Profile

Config Parameter	SipTrunk	Teams
Realm ID	SipTrunk	Teams
Out manipulationid	SipTrunkOutManip	TeamsOutManip
In manipulationid		TeamsInManip
Sip Port Config Parmeter	**Sip Trunk**	**Teams**
Address	192.168.1.10	141.146.36.68
Port	5060	5061
Transport protocol	UDP	TLS
TLS profile		TLSTeamsCarrier
Allow anonymous	agents-only	agents-only



10.6.3 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.

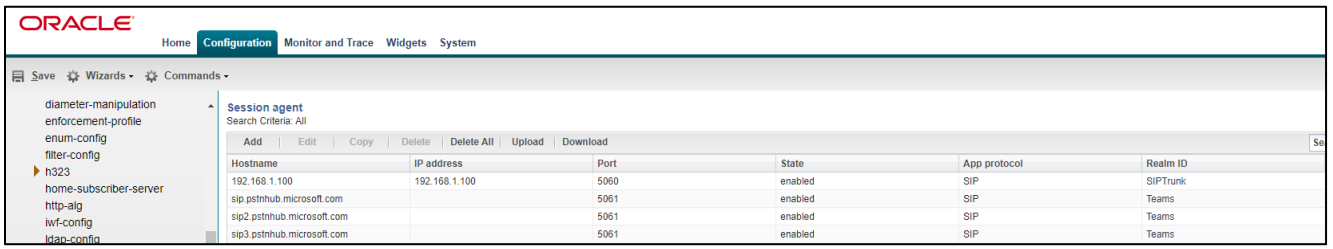
GUI Path: session-router/session-agent

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

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

- 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



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

10.6.4 Session Agent Group

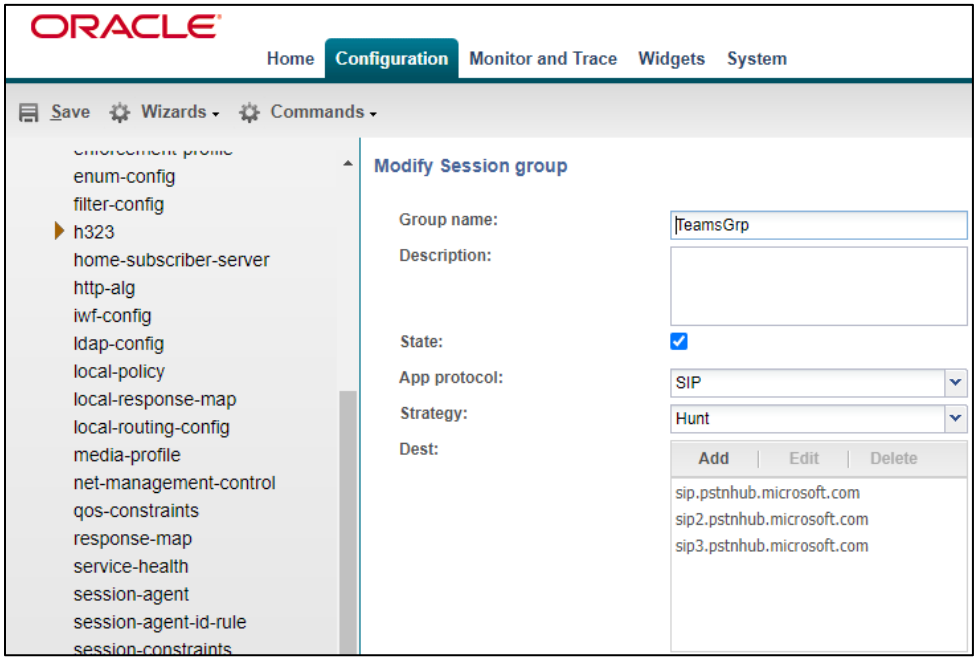
A session agent group allows the SBC to create a load balancing model:

All three 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:



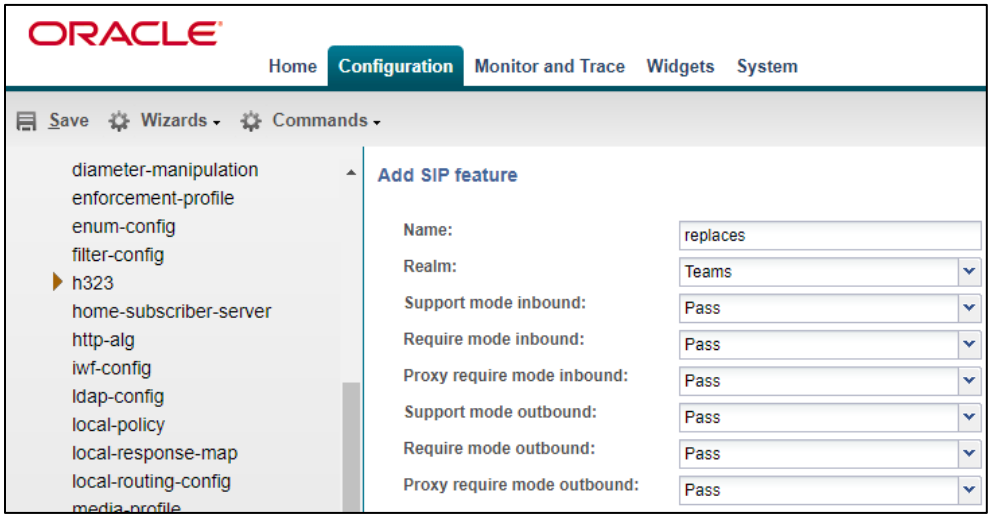
- Click OK at the bottom

10.6.5 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



10.6.6 SIP Profile

A sip profile needs to be configured and 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
```

10.7 Routing Configuration

This section outlines how to configure the OCSBC to route Sip traffic to and from Microsoft Teams Direct Routing Interface.

The OCSBC has multiple routing options that can be configured based on environment. For the purpose of this example configuration, we are utilizing the OCSBC's multistage local policy routing feature along with DID separation via local route table.

A routing stage signifies a re-evaluation of local policy based on the results of a local policy lookup. In the simplest, single stage case, the Session Border Controller performs a local policy lookup on a SIP message's Request URI. The result of that local policy lookup is a next hop FQDN, IP address, ENUM lookup, or LRT lookup; that result is where the Session Border Controller forwards the message. In the multistage routing model, that resultant next hop is used as the lookup key for a second local policy lookup

10.7.1 LRT

The OCSBC supports LRT, an XML document that contains either E164 telephone numbers or strings-to-SIP-URI mappings. An iLRT is configured and transferred from the development environment to the OCSBC /code/lrt directory. After installation and configuration, the LRT is available for SIP Request routing. For more information on creating and configuring LRT, please see the OCSBC 8.3 Configuration Guide, Chapter 8.

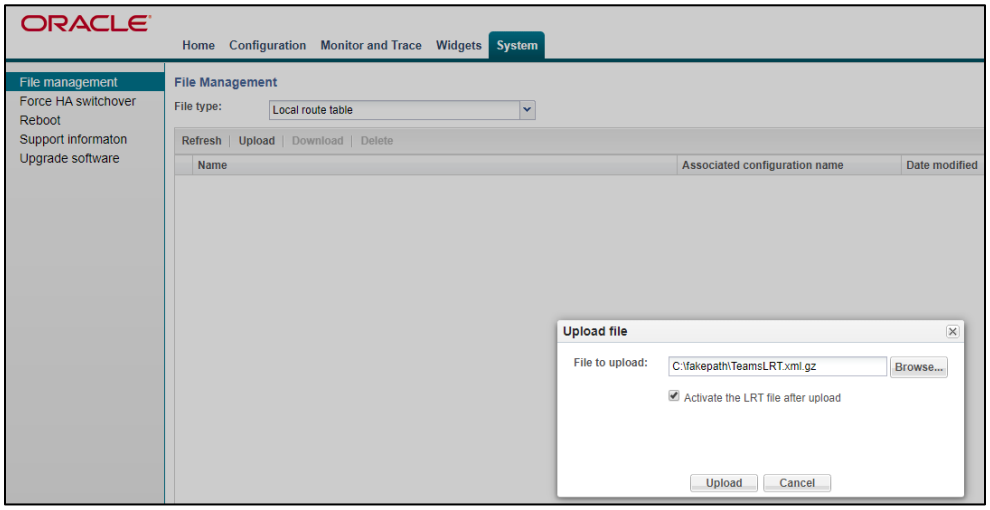
The following is an example Lrt file, once created, will be placed in the /code/lrt directory on the OCSBC

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<localRoutes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<!—Customer 1 Tenant: solutionslab.cgbubedford.com/sbc1.customers.telechat.o-test06161977.com -->
        <route>
                <user type="E164">17814437242</user>
                <next type="regex">!^.*!sip:\0@sbc1.customers.telechat.o-test06161977.com!</next>
</route>
        <route>
                <user type="E164">17814437247</user>
                <next type="regex">!^.*!sip:\0@sbc1.customers.telechat.o-test06161977.com!</next>
</route>
        <route>
                <user type="E164">17814437245</user>
                <next type="regex">!^.*!sip:\0@sbc1.customers.telechat.o-test06161977.com!</next>
</route>
<!-- Customer 2 Tenant – woodgrovebank.us/sbc2.customers.telechat.o-test06161977.com-->
        <route>
                <user type="E164">17814437243</user>
                <next type="regex">!^.*!sip:\0@sbc2.customers.telechat.o-test06161977.com!</next>
</route>
        <route>
                <user type="E164">17814437244</user>
                <next type="regex">!^.*!sip:\0@sbc2.customers.telechat.o-test06161977.com!</next>
</route>
        <route>
                <user type="E164">17814437388</user>
                <next type="regex">!^.*!sip:\0@sbc2.customers.telechat.o-test06161977.com!</next>
</route>
```

The LRT file, once created, can be copied to the /code/lrt directory of the SBC via SFTP to the management IP, or uploaded through the GUI:

10.7.2 GUI Upload of LRT File

- At the top, click on the System Tab
- File Type: Drop down, choose Local route table
- Click Upload
- Browse to select file to upload to SBC
- Check box “Activate LRT file after upload”
- Click Upload



10.7.3 Local Routing Config

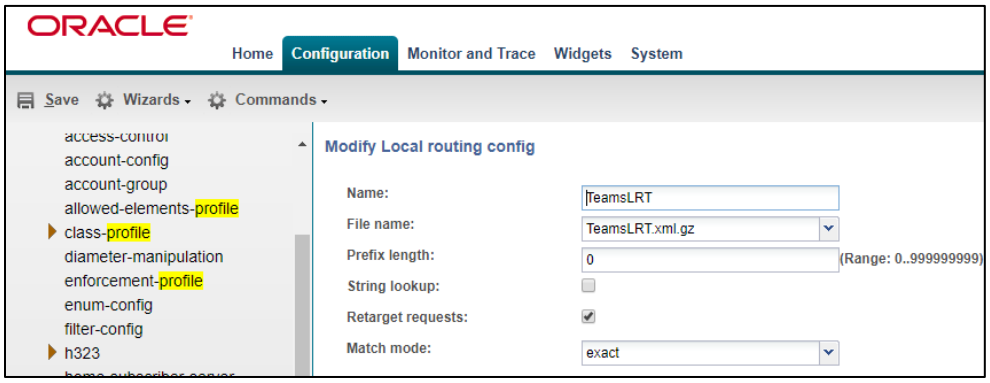
After moving the DID-range-based LRT to the /code/lrt directory on the OCSBC, use the following procedure to specify the file’s location, and the lookup method.

GUI Path: session-router/local-routing-config

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

Click Add, use the following as an example to configure

Note: the file name field below is the full name of the LRT file that has been placed in the /code/lrt directory on the OCSBC



- Click OK at the bottom

10.7.4 Session Router Config

Session router config allows for the SBC to perform multistage routing.

Currently, the session-router config element is not available through the OCGUI, and must be configured via OCSBC ACLI.

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

Use the following example to configure session router config:

```
session-router
      state                              enabled
      system-number-type                 Pots
      match-lp-src-parent-realm          disabled
      nested-realm-stats                 disabled
      reject-message-threshold           0
      reject-message-window              10
      force-report-trunk-info            disabled
      additional-lp-lookups              1
      max-routes-per-lookup              0
      total-lp-routes                    0
      multi-stage-src-realm-override     enabled
```

- Issue a “done” command, and back out of the config element by entering “exit” commands in the ACLI until you have exited configuration mode in the ACLI

10.7.5 Local Policy Configuration

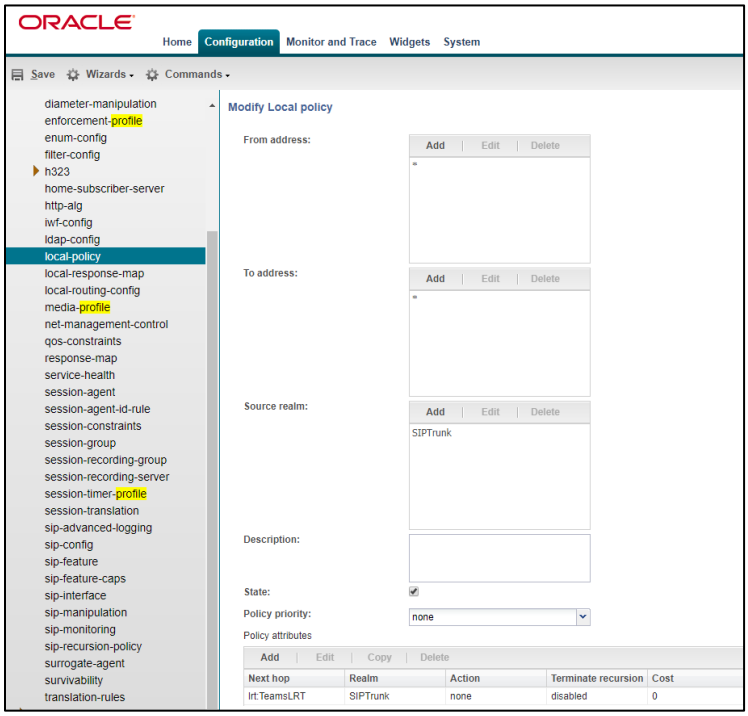
Local Policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria.

GUI Path: session-router/local-policy

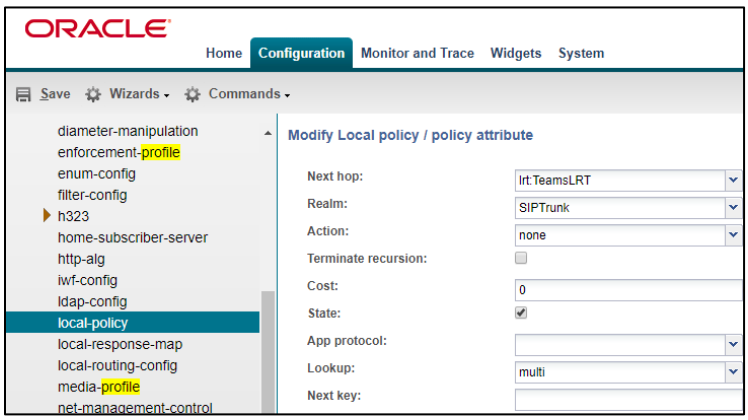
ACLI Path: config t→session-router→local-policy

In order to route Sip traffic to and from Microsoft Teams Direct Routing Interface, the following local-policies will need to be configured.

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

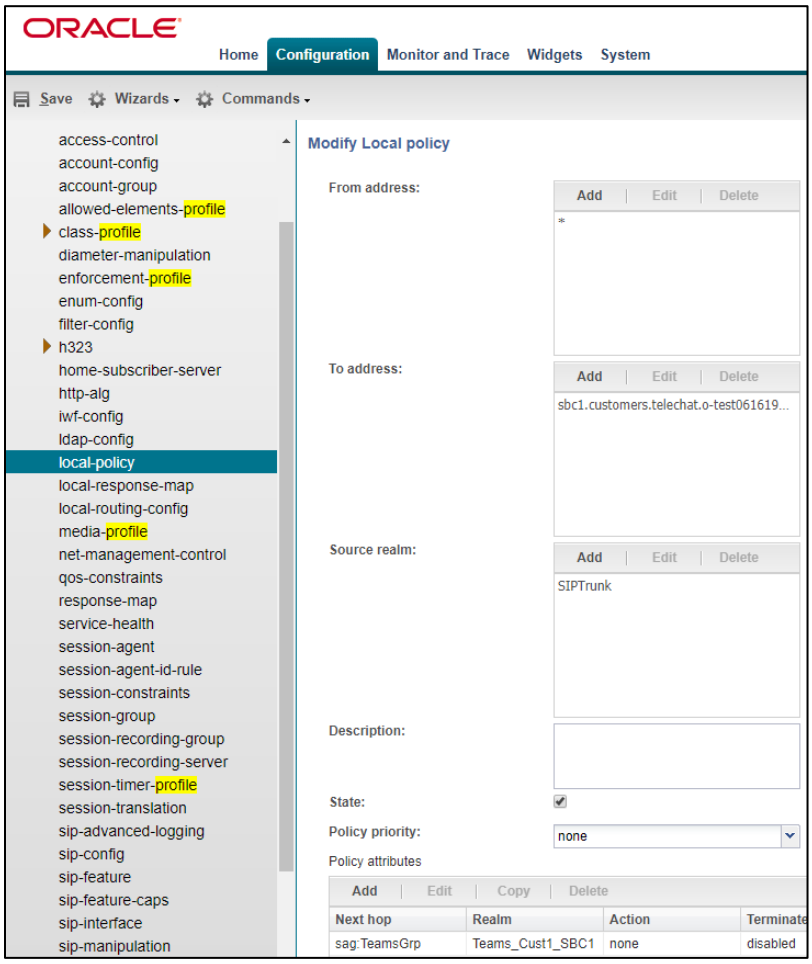


Policy Attribute:

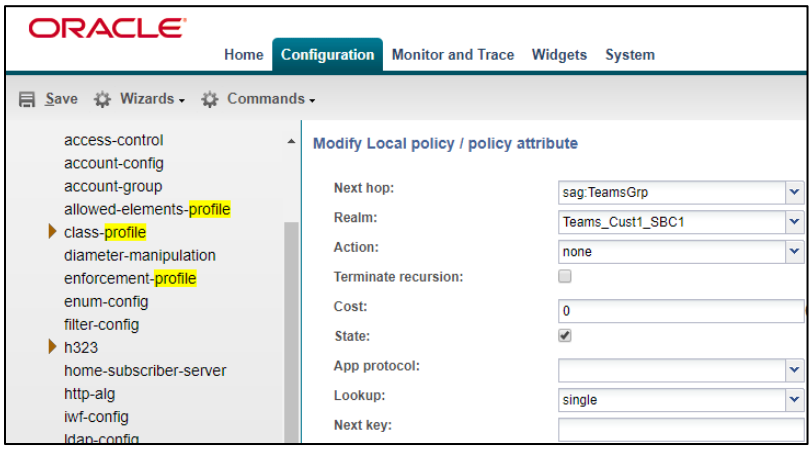


The above local policy utilizes the lrt /local-routing-config- outlined previously in this document. This is a way to identify the terminating tenant/subdomain when the core network (ie..SIPTrunk) does not identify the target in the Request-Uri host. When the target subdomain/tenant is identified in the Request-Uri host, the following local policies will route directly to Teams Group by to-address match.

- Call from Sip Trunk to Customer 1 Tenant:

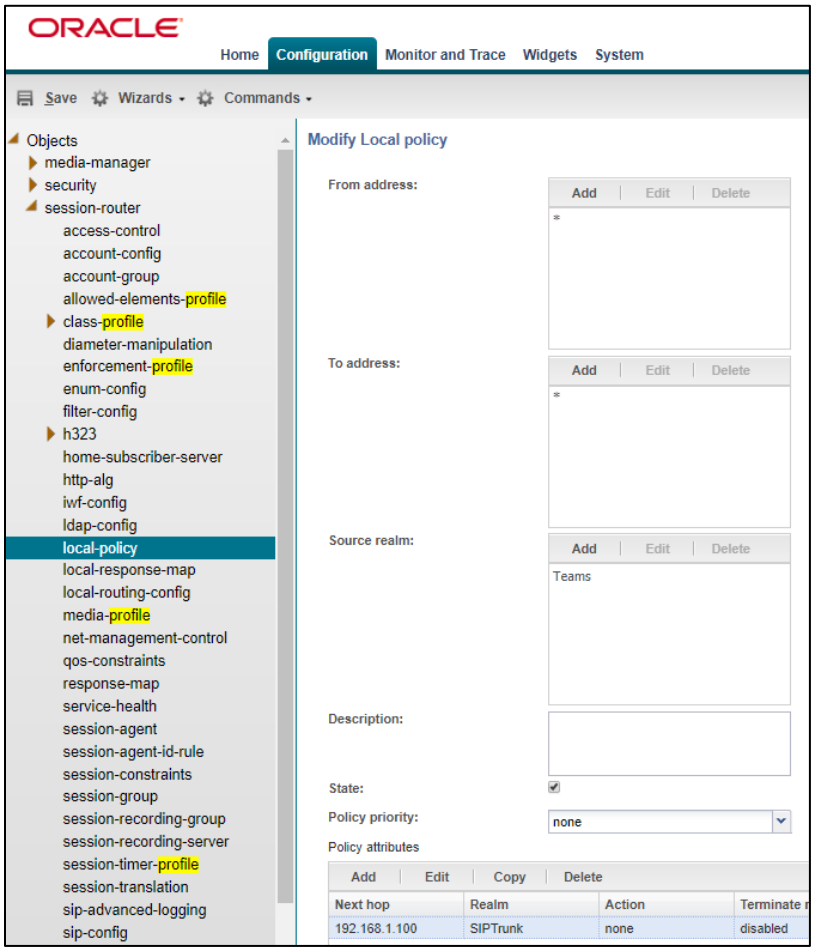


Policy Attribute:

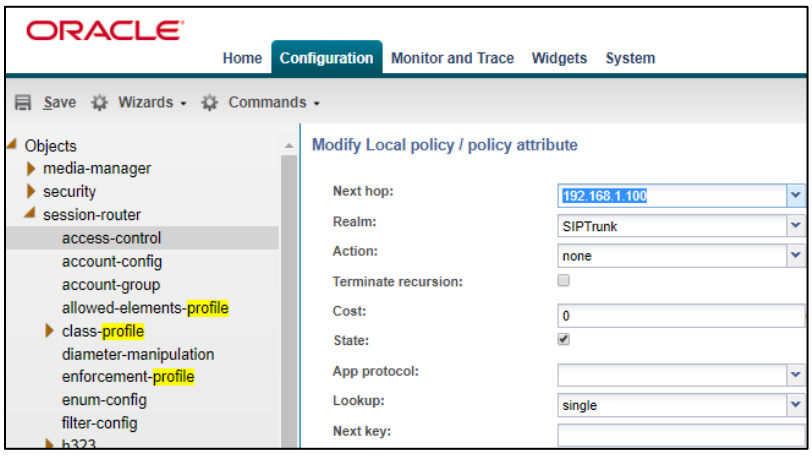


Using the above examples, continue for each customer tenant being hosted by this OCSBC.

The following local policy config is allowing any DID from teams that land on the SBC to be routed to SIP Trunk.



Policy Attribute:



- Click OK at the bottom of each when applicable:
- Save and Activate your configuration!

The SBC configuration is now complete. Move to verify the connection with Microsoft Direct Routing Interface.

11 Verify Connectivity

11.1 OCSBC Options Ping

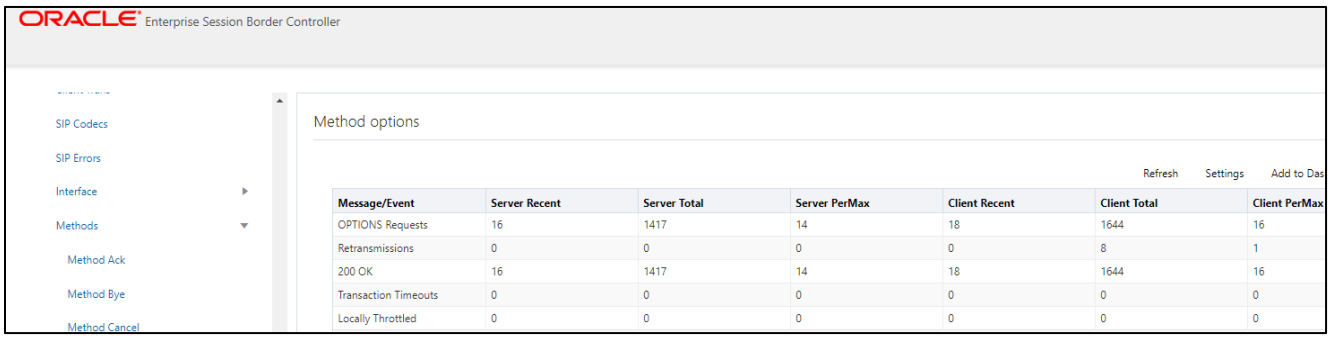
After you've paired the OCSBC with Direct Routing using the New-CsOnlinePSTNGateway PowerShell command, validate that the SBC can successfully exchange SIP Options with Microsoft Direct Routing.

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



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.

11.2 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

12 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 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.

12.1 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

12.2 Requirements for Invite Messages

Picture 1 Example of INVITE message

```
INVITE sip:17814437383@sbc1.customers.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@ sbc1.customers.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@ sbc1.customers.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
```

12.2.1 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

12.3 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@customers.telechat.o-test06161977.com:5061;transport=tls>
Record-Route: <sip: customers.telechat.o-test06161977.com >
```

12.3.1 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

12.4 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 Name	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 Appendix A

13.1 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.

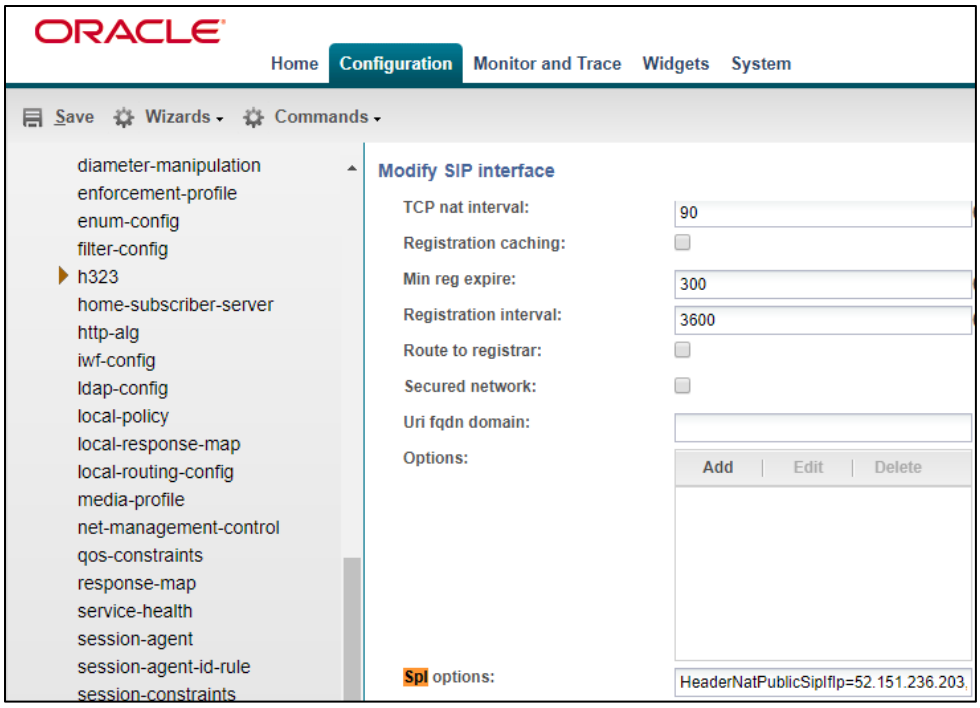
- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

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.



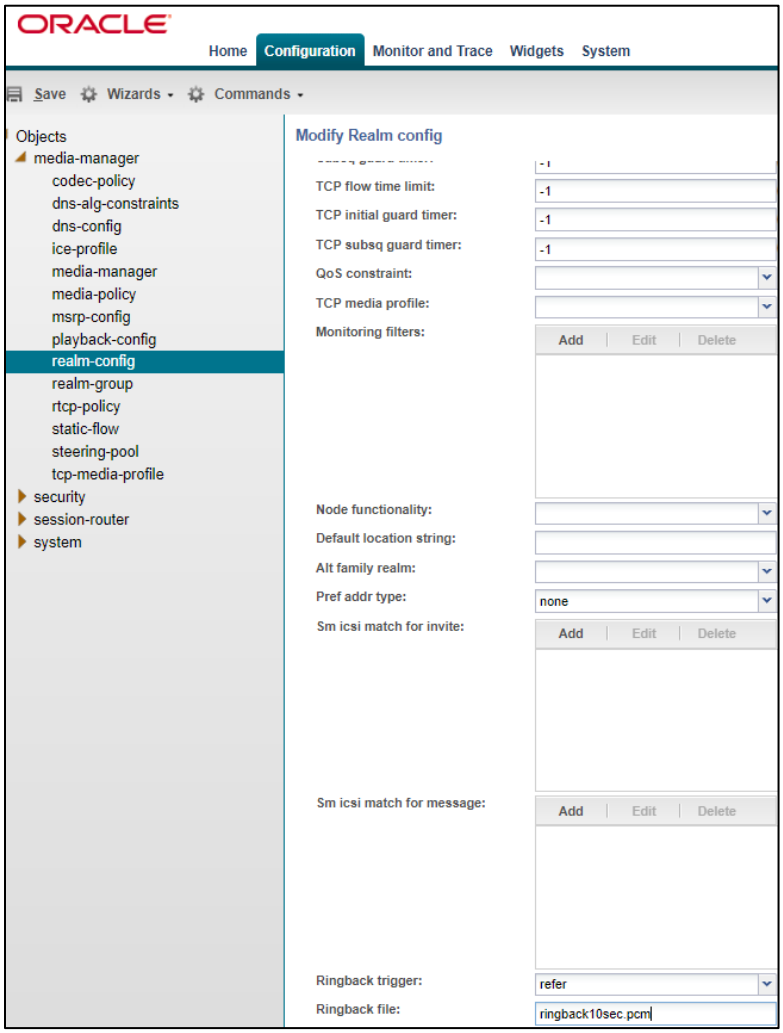
- This configuration would be applied to each Sip Interface in the OCSBC configuration that was deployed behind a Nat Device

14 Appendix B

14.1 SBC Ringback Configuration

14.1.1 Ringback on Transfers

During a call transfer, the calling party does not hear a ring back tone during the process of transfer. We utilize the local playback feature of the SBC to play ring back tone during transfers. The ringback tone is triggered on receiving SIP REFER. You must upload a media playback file to /code/media on the SBC. This file must be in raw media binary format. This ringback trigger and ringback file to be played is configured on the realm facing the trunk.



In addition to the ringback trigger configuration above, SDP manipulations are needed in order to play the ringback tone towards the PSTN caller. The INVITE MS Teams sends to the SBC to initiate the transfer contains the SDP attribute, a=inactive which is forwarded to the trunk. As a result of which, the SBC cannot play the ring back tone to the original PSTN caller (while call is being transferred). A sendonly attribute is required by the calling party to be able to hear ringback.

Note: If running latest GA release, SCZ830m1p8A, please see Appendix C prior to configuring Sip manipulations

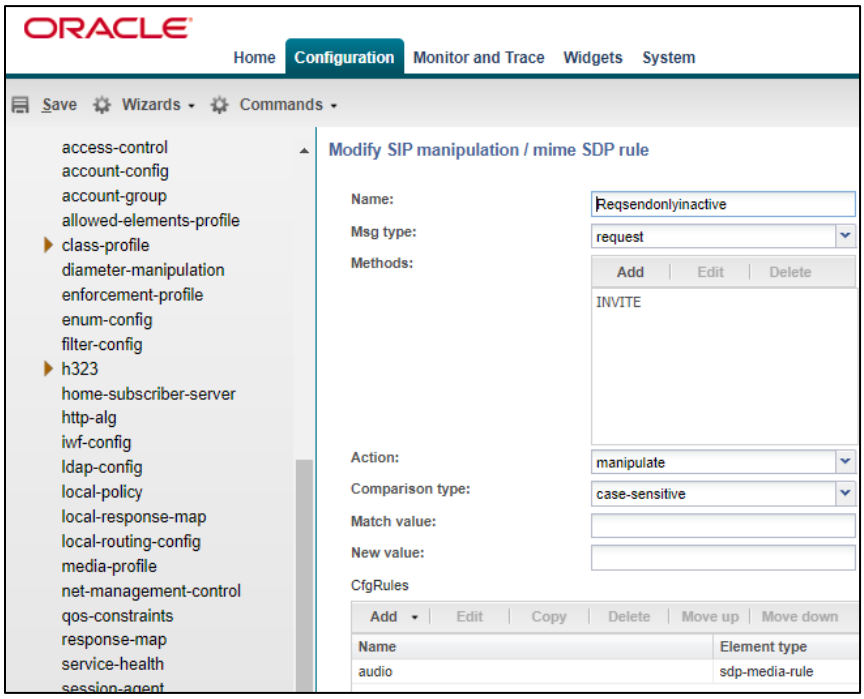
The SBC is able to signal appropriately towards the SIP trunk by changing the a=inactive SDP attribute in the INVITE to a=sendonly towards PSTN. We configure sdp-mime rule under the sip-manipulation Teamsinmanip to change a=inactive to sendonly in the INVITE received from Teams.(Here the MsgType is Request).Similarly we configure the msgtype as Reply and convert the a=inactive to a=recvonly ,so that inactive is not sent towards PSTN.

The 200 OK response received from the trunk contains a=recvonly in the SDP. Since Teams is expecting an a=inactive in the 200 OK for the INVITE, we configure the following sdp-mime-rule under the sip-manipulation – Teamsoutmanip, to convert the a=recvonly to a=inactive in the 200 OK being sent to Teams for the msgtype "Request". Here also we change the a=recvonly to a=inactive for the msgtype "reply" so that recvonly is not sent towards Teams.

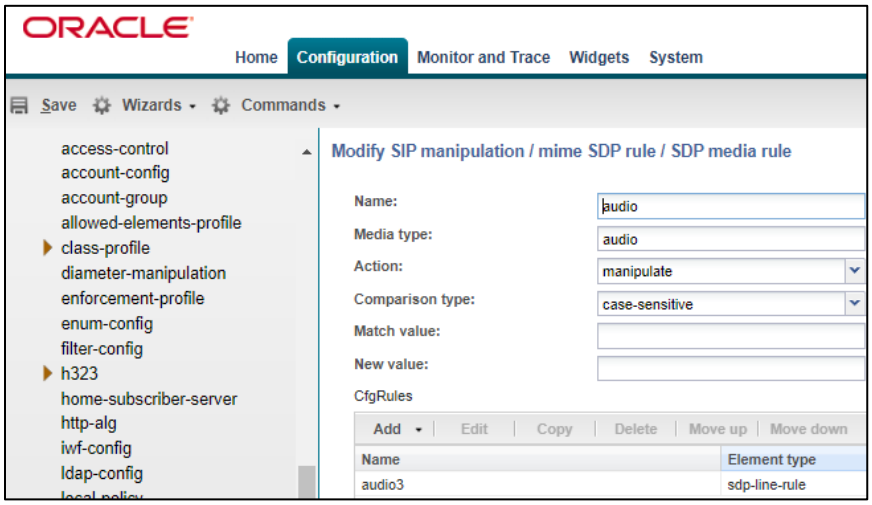
Manipulation	Msg Type	Match-Value	New-Value
Teamsinmanip	request	inactive	sendonly
Teamsinmanip	reply	inactive	recvonly
Teamsoutmanip	request	sendonly	inactive
Teamsoutmanip	reply	recvonly	inactive

Use the below example to configure the necessary mime and sdp rules, changing the msg-type, match and new values based on the information provided above. This example is configured under Teamsoutmanip:

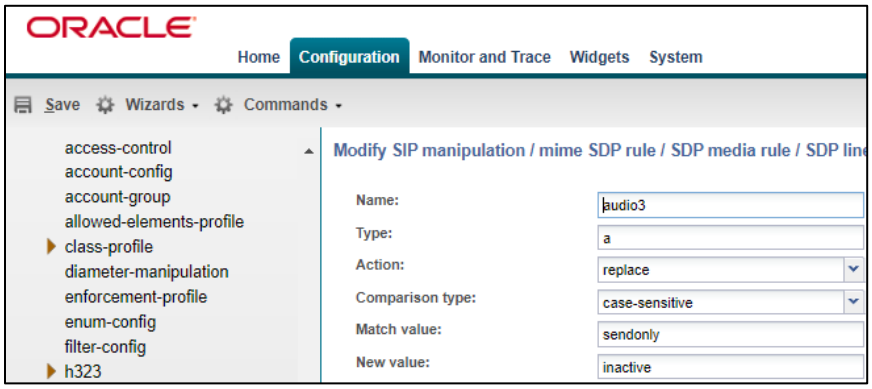
Mime-sdp-rule: Reqsendonlyinactive



Sdp-media-rule:audio



Sip-line-rule: audio3



15 Appendix C

15.1 Sip Manipulation Replacement

To simplify the OCSBC configuration, the latest OCSBC GA Release, SCZ830m1p8A, (available for download through My Oracle Support Portal, https://support.oracle.com/portal/, or via Oracle Software Delivery Cloud (https://edelivery.oracle.com/), contains four additional SBC configuration parameters not found in prior releases.

The purpose of these four parameters is to replace all of the Sip Manipulation rules required to be configured in the OCSBC in order to properly interface with Microsoft Teams Direct Routing.

15.2 Teams Facing Realms

The first three parameters are found under the realm-config, and would be enabled in Realms facing Microsoft Teams. They are:

- **Teams-FQDN**
- **Teams FQDN in URI**
- **SDP inactive only**

15.2.1 Teams FQDN

This is where you will add the SBC's FQDN required to interface with Microsoft Teams Direct routing interface.

Please note, for Carrier or Hosting Model configuration, this configuration parameters negates the need for the FQDN to be added to the Trunk Context Field of any realm facing Microsoft Teams.

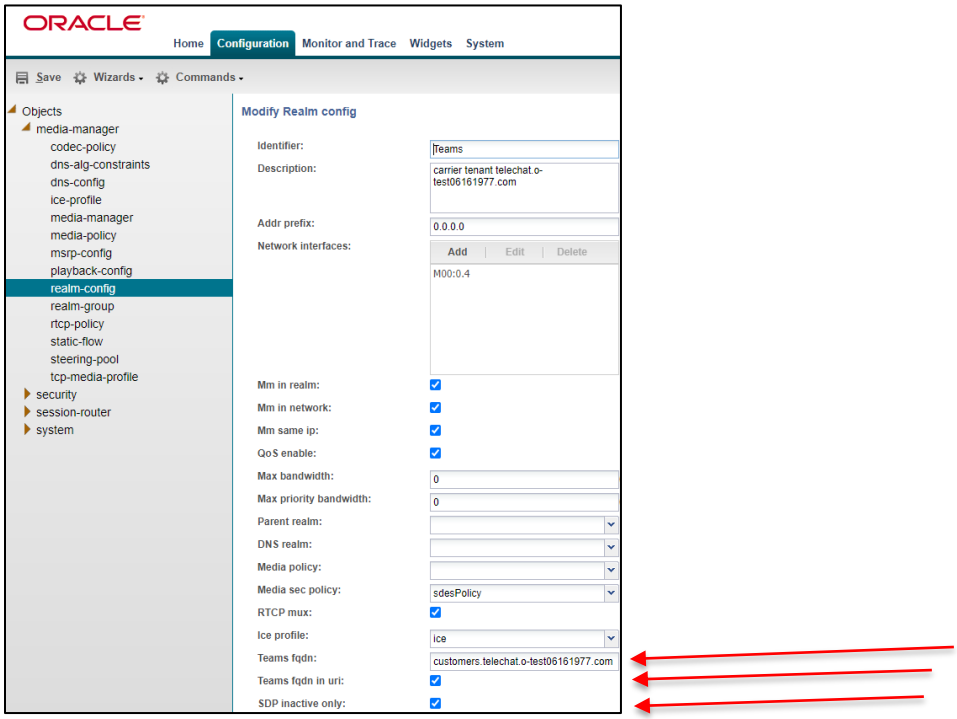
15.2.2 Teams FQDN in URI

When enabled, this parameter takes the FQDN configured under Teams FQDN field of the realm, and inserts that into the Contact and FROM headers of Invites generated by the SBC towards Teams. This also adds a new "X-MS-SBC" Header to both Invite and OPTIONS Requests, which takes the place of the User-Agent header currently being added via Sip Manipulation. Next, allows the SBC will add a Contact Header to outgoing SIP Options Pings, also containing the FQDN of the SBC listed under the hostname field of the network interface. Lastly, in order to satisfy the Microsoft Teams requirement outlined in the Important Information Section of this document, SBC will present the FQDN in the host URI of the Contact Header in all final responses sent to Microsoft Teams.

15.2.3 SDP inactive only

When enabled on Teams facing realm(s), this will modify the following SDP attributes in both requests and responses to and from Microsoft Teams:

Message Type	Match Value	New Value
request	inactive	sendonly
reply	inactive	recvonly
request	sendonly	inactive
reply	recvonly	inactive



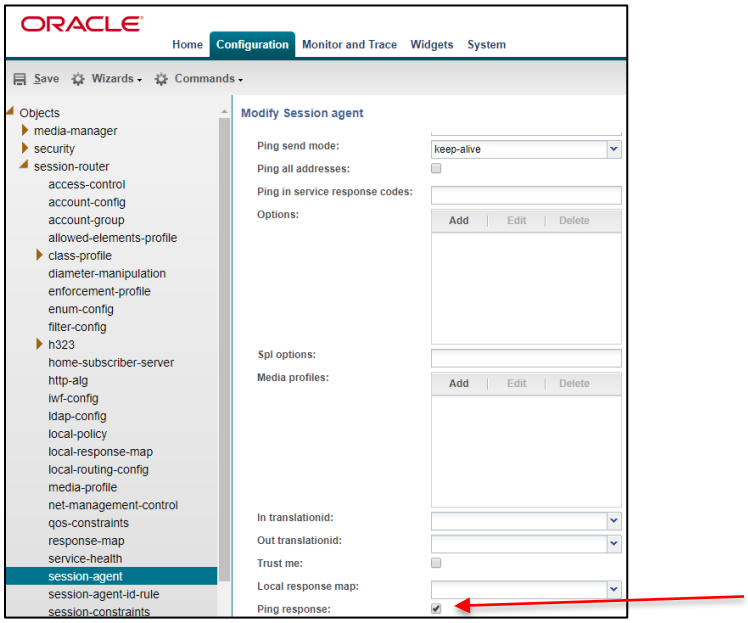
15.3 Teams Session Agents

The third parameter is found under the session agent configuration element and will be enabled on all three session agents configured for microsoft teams. Its called

- **ping response**

15.3.1 Ping Response

When enabled, the SBC responds with a 200OK to all Sip Options Pings it receives from trusted agents. This takes the place of the current Sip Manipulation, RepondOptions.



15.4 Carrier or Hosting Model

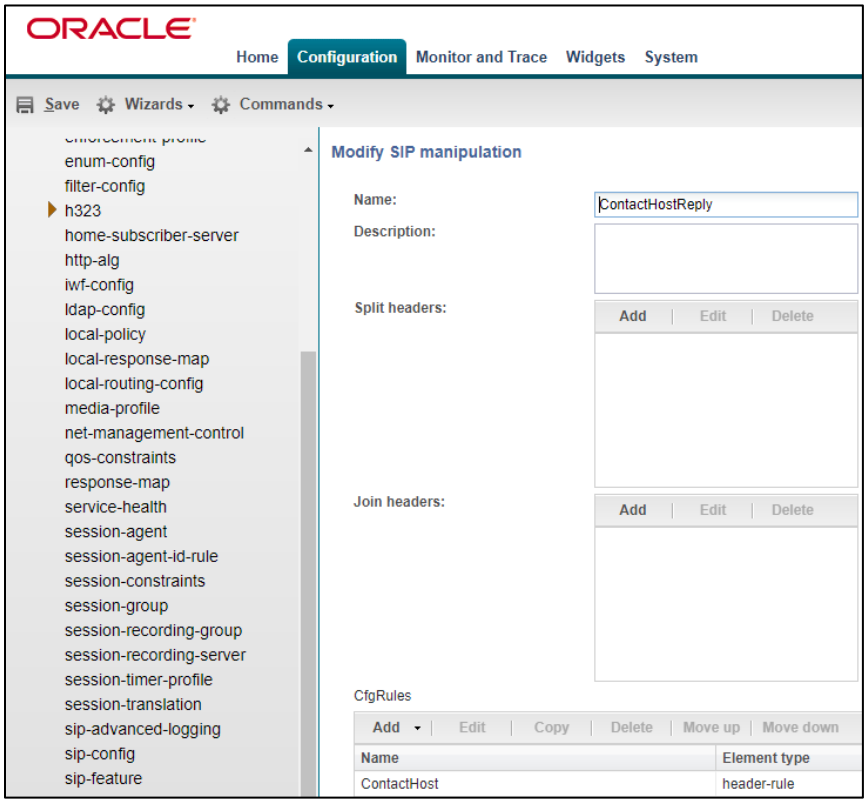
In some environments, it may be desirable to include the Customers FQDN as the Contact URI of all responses generated by the SBC toward Microsoft Teams. By default, the SBC will always add the FQDN of the realm associated with the signaling or sip interface. In a nested realms configuration, as outlined in this document, that is always the Parent or Carrier Realm. If you wish to use customers FQDNs the following Sip Manipulation will have to be added to the Oracle SBC's configuration.

ContactHostReply:

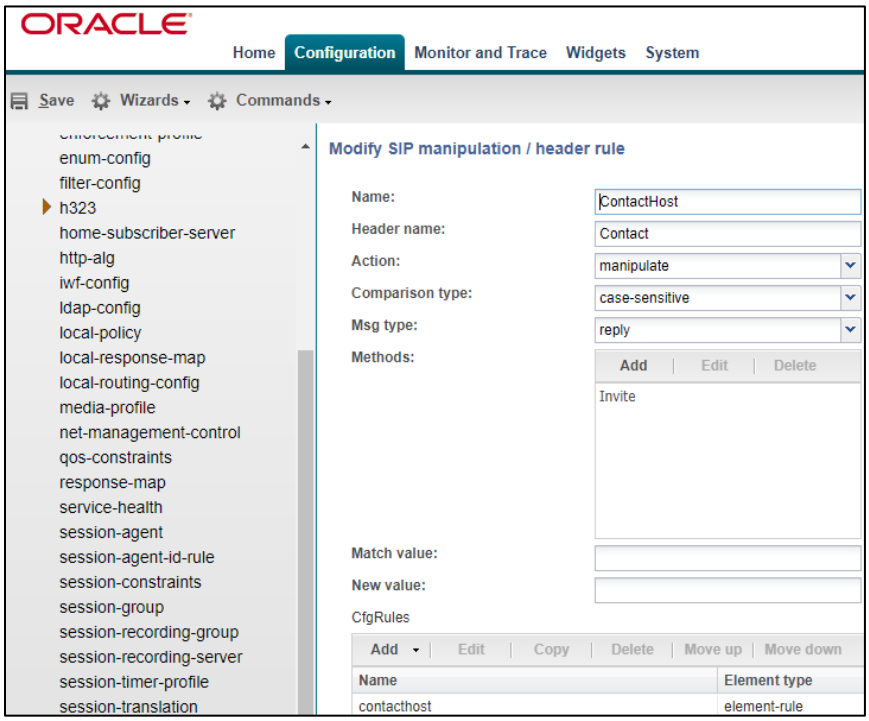
This manipulation will replace the host part of the Contact Header with the host part of the To Header. In a Teams environment, this is always the FQDN of the customer tenant.

GUI Path: session router/sip-manipulation

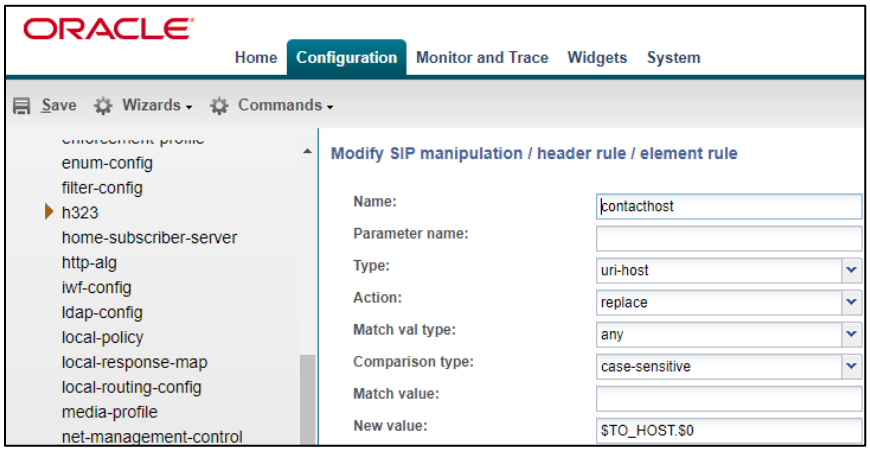
ACLI Path: config t→session-router→sip-manipulation


ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
enum-config
filter-config
h323
home-subscriber-server
http-alg
iwf-config
ldap-config
local-policy
local-response-map
local-routing-config
media-profile
net-management-control
qos-constraints
response-map
service-health
session-agent
session-agent-id-rule
session-constraints
session-group
session-recording-group
session-recording-server
session-timer-profile
session-translation
sip-advanced-logging
sip-config
sip-feature
Modify SIP manipulation
Name:
ContactHostReply
Description:
Split headers:
Add
Edit
Delete
Join headers:
Add
Edit
Delete
CfgRules
Add
Edit
Copy
Delete
Move up
Move down
Name
Element type
ContactHost
header-rule

Header Rule:


ORACLE
Home
Configuration
Monitor and Trace
Widgets
System
Save
Wizards
Commands
enum-config
filter-config
h323
home-subscriber-server
http-alg
iwf-config
ldap-config
local-policy
local-response-map
local-routing-config
media-profile
net-management-control
qos-constraints
response-map
service-health
session-agent
session-agent-id-rule
session-constraints
session-group
session-recording-group
session-recording-server
session-timer-profile
session-translation
Modify SIP manipulation / header rule
Name:
ContactHost
Header name:
Contact
Action:
manipulate
Comparison type:
case-sensitive
Msg type:
reply
Methods:
Add
Edit
Delete
Invite
Match value:
New value:
CfgRules
Add
Edit
Copy
Delete
Move up
Move down
Name
Element type
contacthost
element-rule

Element Rule:



This manipulation will be assigned as the out-manipulation ID of the Teams Sip Interface:

16 Important Information

Due to planned upgrades to Microsoft Teams Direct Routing, it is now a requirement for SBC's to present their FQDN in the host URI of the Contact Header in all final responses sent to Microsoft Teams. In order to accommodate this, changes to the configuration of your SBC may be needed. By default, the SBC add's the sip interface IP address to the host-uri of the Contact header in all responses. In order to change the host part of the Contact header from IP to FQDN, we'll utilize the Oracle SBC's sip-manipulation feature.

You should already have a TeamsOutManipulation that contains a header rule, Alter_contact, which modifies the host part of the Contact header in Requests and Responses toward Microsoft Teams. In some cases, a simple change may be needed to this header rule to ensure we are meeting this new requirement. Please make sure the **Msg type** in this rule is set to **ANY** as outlined in the Sip Manipulation Configuration Section of this note. This allows the SBC to modify the Contact Host in both requests and responses, satisfying this change.

Please note, if you are running the latest GA release, SCZ830M1P8A, sip manipulations are no longer required. Please see Appendix C for further Details.

17 Caveats

17.1 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.

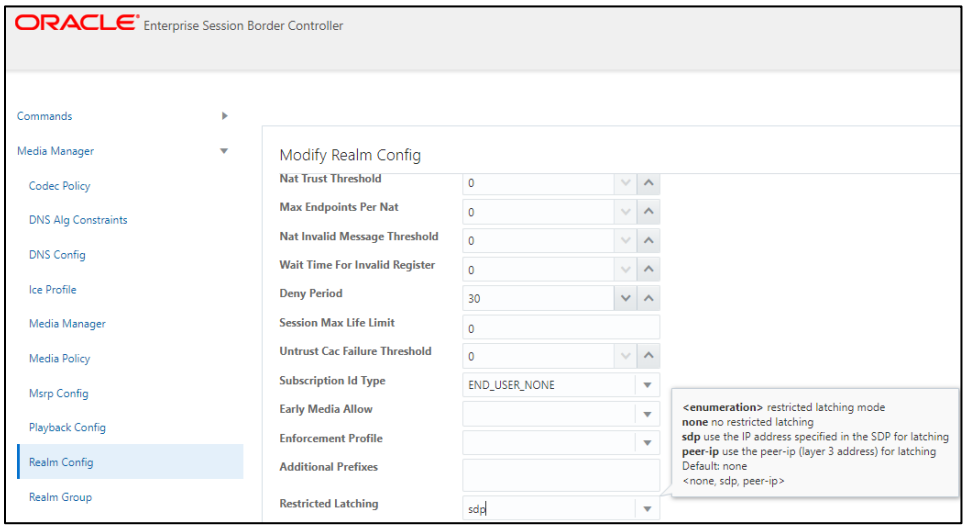
To correct this, Oracle recommends enabling Restricted Media Latching on realms configured for Microsoft Teams in the OCSBC.

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



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

18 ACLI Running Configuration

18.1 Show running-config short

The following is output from the SBC's ACLI, collected by running the command

"show running-config short"

The output below only displays configuration parameters that have been modified from their default values, and is based on the release SCZ830M1P8A

```
show running-config short

access-control
        realm-id                        Team
        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
        destination-address                   141.146.36.100
        application-protocol                  SIP
        trust-level                     high
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                            SBCCarriercertSAN
        state                           California
        locality                        Redwood City
        organization                        Oracle Corporation
        common-name                           customers.telechat.o-test06161977.com
        alternate-name                      *.customers.telechat.o-test06161977.com
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                        * SILK:no G729:no
        add-codecs-on-egress                  CN
codec-policy
        name                            addCNG729
        allow-codecs                        * SILK:no PCMU:no
        add-codecs-on-egress                  G729
codec-policy
        name                            audiotest
        allow-codecs                        * SILK:no G729:no
filter-config
        name                            all
        user                            *
ice-profile
```

```
        name                    ice
        stun-conn-timeout       0
        stun-keep-alive-interval 0
local-policy
        from-address            *
        to-address              *
        source-realm            SIPTrunk
        policy-attribute
                next-hop        lrt:TeamsLRT
                realm           SIPTrunk
                lookup          multi
local-policy
        from-address            *
        to-address              customers.telechat.o-test06161977.com
        source-realm            SIPTrunk
        policy-attribute
                next-hop        sag:TeamsGrp
                realm           Teams
local-policy
        from-address            *
        to-address              sbc1.customers.telechat.o-test06161977.com
        source-realm            SIPTrunk
        policy-attribute
                next-hop        sag:TeamsGrp
                realm           Teams_Cust1_SBC1
local-policy
        from-address            *
        to-address              sbc2.customers.telechat.o-test06161977.com
        source-realm            SIPTrunk
        policy-attribute
                next-hop        sag:TeamsGrp
                realm           Teams_Cust2_SBC2
local-policy
        from-address            *
        to-address              *
        source-realm            Teams
        policy-attribute
                next-hop        68.68.117.67
                realm           SIPTrunk
local-routing-config
        name                    TeamsLRT
        file-name               TeamsLRT.xml.gz
media-manager
        options                 audio-allow-asymmetric-pt
                                xcode-gratuitous-rtcp-report-generation
media-profile
        name                    CN
        subname                 wideband
        payload-type            118
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                    M00
        ip-address              141.146.36.100
        netmask                 255.255.255.192
        gateway                 141.146.36.65
        dns-ip-primary          8.8.8.8
        dns-domain              customers.telechat.o-test06161977.com
ntp-config
        server                  198.55.111.50
                                206.108.0.131
phy-interface
        name                    M00
        operation-type          Media
realm-config
        identifier              SIPTrunk
        network-interfaces      M00:0
        mm-in-realm             enabled
        qos-enable              enabled
        media-sec-policy        RTP
        access-control-trust-level      high
        codec-policy            OptimizeCodecs
        session-recording-required      enabled
        hide-egress-media-update        enabled
realm-config
        identifier              Teams
        description             carrier tenant telechat.o-test06161977.com
        network-interfaces      M00:0.4
        mm-in-realm             enabled
        qos-enable              enabled
        media-sec-policy        sdesPolicy
        rtcp-mux                enabled
        ice-profile             ice
        teams-fqdn              customers.telechat.o-test06161977.com
        teams-fqdn-in-uri       enabled
        sdp-inactive-only       enabled
        access-control-trust-level      high
        codec-policy            addCN
        rtcp-policy             rtcpGen
        session-recording-required      enabled
realm-config
        identifier              Teams_Cust1_SBC1
        description             customer tenant solutionslab.cgbubedford.com
        network-interfaces      M00:0.4
        mm-in-realm             enabled
        qos-enable              enabled
        parent-realm            Teams
        media-sec-policy        sdesPolicy
        rtcp-mux                enabled
        ice-profile             ice
        teams-fqdn              sbc1.customers.telechat.o-test06161977.com
        teams-fqdn-in-uri       enabled
        sdp-inactive-only       enabled
        codec-policy            addCN
        rtcp-policy             rtcpGen
realm-config
```

```
        identifier                Teams_Cust2_SBC2
        description                 customer tenant woodgrovebank.us
        network-interfaces              M00:0
        mm-in-realm                 enabled
        qos-enable                 enabled
        parent-realm                Teams
        media-sec-policy              sdesPolicy
        rtcp-mux                  enabled
        ice-profile               ice
        teams-fqdn                  sbc2.customers.telechat.o-test06161977.com
        teams-fqdn-in-uri             enabled
        sdp-inactive-only             enabled
        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                    68.68.117.67
        ip-address                 68.68.117.67
        realm-id                  SIPTrunk
        ping-method                 OPTIONS
        ping-interval              60
        ping-response                enabled
session-agent
        hostname                    sip.pstnhub.microsoft.com
        port                      5061
        transport-method                StaticTLS
        realm-id                  *
        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                  *
        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                  *
        ping-method                 OPTIONS
        ping-interval              30
        ping-response                enabled
        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
```

```
session-router
        match-lp-src-parent-realm             enabled
        additional-lp-lookups                 1
        multi-stage-src-realm-override        enabled
sip-config
        home-realm-id                         Teams
        registrar-domain                      *
        registrar-host                        *
        registrar-port                        5060
        options                               inmanip-before-validate
                                              max-udp-length=0
        extra-method-stats                    enabled
sip-feature
        name                                  replaces
        realm                                 Teams
        require-mode-inbound                  Pass
        require-mode-outbound                 Pass
sip-interface
        realm-id                              SIPTrunk
        description                           to trunk
        sip-port
                address                       141.146.36.100
                allow-anonymous               agents-only
        options                               100rel-interworking
        sip-ims-feature                       enabled
sip-interface
        realm-id                              Teams
        sip-port
                address                       141.146.36.68
                port                          5061
                transport-protocol            TLS
                tls-profile                   TLSTeamsCarrier
                allow-anonymous               agents-only
        out-manipulationid                    ContactHostReply
        sip-profile                           forreplaces
sip-manipulation
        name                                  ContactHostReply
        header-rule
                name                          ContactHost
                header-name                   Contact
                action                        manipulate
                msg-type                      reply
                methods                       Invite
                element-rule
                        name                  contacthost
                        type                  uri-host
                        action                replace
                        new-value             $TO_HOST.$0
sip-monitoring
        match-any-filter                      enabled
        monitoring-filters                    *
sip-profile
        name                                  forreplaces
        replace-dialogs                       enabled
steering-pool
        ip-address                            141.146.36.100
        start-port                            20000
        end-port                              40000
        realm-id                              SIPTrunk
steering-pool
        ip-address                            141.146.36.68
        start-port                            20000
        end-port                              40000
```

```
        realm-id                      Teams
system-config
        system-log-level                NOTICE
        default-gateway                 10.138.194.129
        source-routing                 enabled
        snmp-agent-mode                  v1v2
tls-global
        session-caching                 enabled
tls-profile
        name                          TLSTeamsCarrier
        end-entity-certificate              SBCCarriercertSAN
        trusted-ca-certificates              BaltimoreRoot
        mutual-authenticate                  enabled
web-server-config
        http-interface-list             GUI
```


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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/Oracle/
twitter.com/Oracle
oracle.com

Integrated Cloud Applications & Platform Services