# Configuring the Oracle SBC with Microsoft Teams Direct Routing Non-Media Bypass - Enterprise 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.

## Revision History

| Version | Description of Changes | Date Revision Completed |
|---|---|---|
| 1.0 | Added Web GUI | 12-09-2019 |
| 2.0 | • Added Missing sip-manipulation<br>• Added bug fixes ACMESOLU-106 | 21-10-2019 |
| 3.0 | • Modified Media Manger Options<br>• Added notes regarding new features in 830M1P8A<br>• Modified Appendix B<br>• Added Appendix D<br>• Add Alert and associated Important Info<br>• Added Config for E911 and Elin Gateway | 01-06-2020 |
| 4.0 | • Corrected spelling mistakes in media-manager config.<br>• Modified powershell screenshots with Microsoft latest update<br>• Removed media-profile config for CN | 19-02-2021 |
| 5.0 | • Corrected match value in SDP-line-rule | 10-05-2021 |
| 6.0 | • Modified Appendix C | 31-08-2021 |

# 1 *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 Appendix D/Important Note for more details:***

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

## Contents

# 2 Introduction

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

# 3 About Microsoft 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;
- Oracle Enterprise Session Border Controllers are Microsoft certified to work for Direct Routing. Additional information can be found at: https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers

## 3.1 Planning Direct Routing

If you are planning to configure direct routing with Oracle SBC, you must ensure that the following prerequisites are completed before proceeding further

- Tenant requirements
- Licensing and other requirements
- SBC domain names
- Public trusted certificate for the SBC
- SIP Signaling: FQDNs
- Transcoding Resources for the SBC (CN, RTCP, and Ringback)

### 3.1.1 Tenant Requirements

Make sure that you have a custom domain on your O365 tenant. Here we have created an account soladmin@solutionslab.onmicrosoft.com.

Likewise create an account, which is not the default domain created for your tenant. For more information https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#sbc-domain-names

### 3.1.2 Licensing Requirements

Make sure that the following license requirements are met by the Direct routing users. (ie the users must be assigned the following licenses in Office 365)

- Microsoft Phone System
- Microsoft Teams + Skype for Business Plan 2 if included in Licensing Sku

### 3.1.3 DNS Requirements

Create DNS records for domains in your network that resolve to your SBC.
Before you begin, make sure that you have the following per every SBC you want to pair:

- Public IP address
- FQDN name resolving to the Public IP address

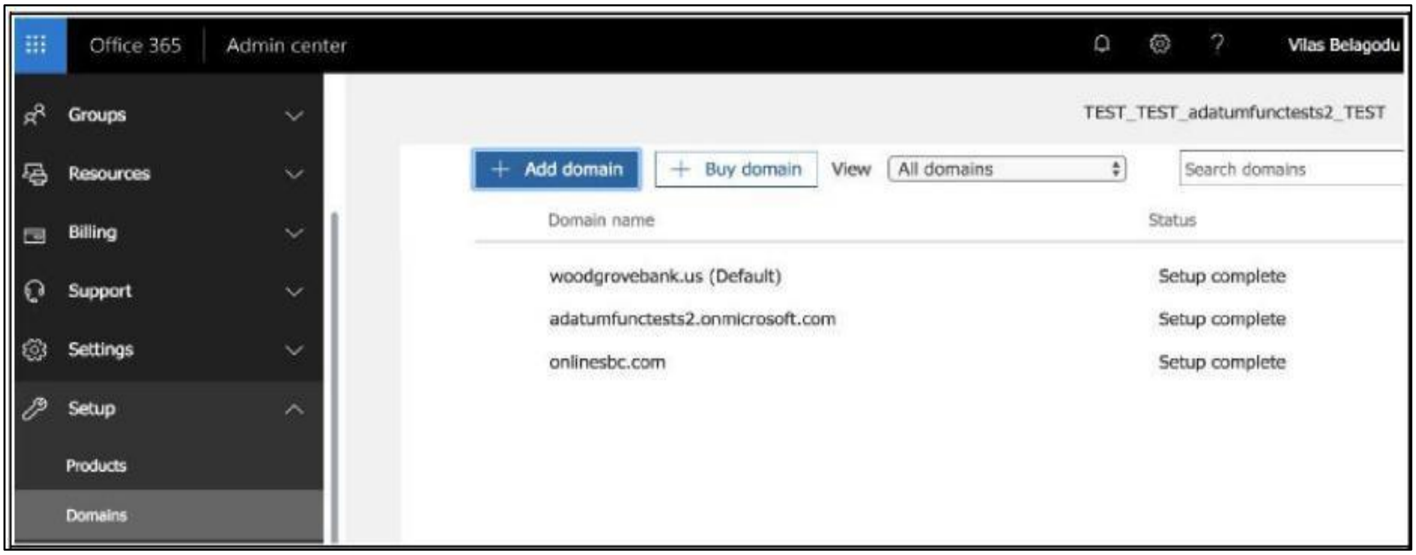
### 3.1.4 SBC Domain Names

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 FQDN | Examples of FQDN names |
|---|---|---|
| **woodgrovebank.us** | Yes | Valid names:<br>• sbc1.woodgrovebank.us;<br>• ussbcs15.woodgrovebank.us<br>• europe.woodgrovebank.us<br>Non-Valid name:<br>• sbc1.europe.woodgrovebank.us (requires registering domain name europe.atatum.biz in “Domains” first) |
| **woodgrovebankus.onmicrosoft.com** | No | Using *.onmicrosoft.com domains is not supported for SBC names |
| **hybrdvoice.org** | Yes | Valid names:<br>• sbc1. hybridvoice.org<br>• ussbcs15. hybridvoice.org<br>• europe. hybridvoice.org<br>Non-Valid name:<br>• sbc1.europe.hybridvoice.org (requires registering domain name europe. hybridvoice.org in “Domains” first) |

Please activate and register the domain of tenant.



| Domain name | Status |
|---|---|
| woodgrovebank.us (Default) | Setup complete |
| adatumfunctests2.onmicrosoft.com | Setup complete |
| onlinesbc.com | Setup complete |

In this document the following FQDN and IP is used as an example:

| Public IP | FQDN Name |
|---|---|
| 155.212.214.173 | Oracleesbc.woodgrovebank.us |

### 3.1.5 Public trusted certificate for the SBC

It is necessary to setup a public trusted certificate for direct routing. This certificate is used to establish TLS connection between Oracle SBC and MS Teams. The certificate needs to have the SBC FQDN in the subject, common name, or subject alternate name fields. For root certificate authorities used to generate SBC certificate refer to Microsoft documentation. https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

## 3.2 Configure Direct Routing

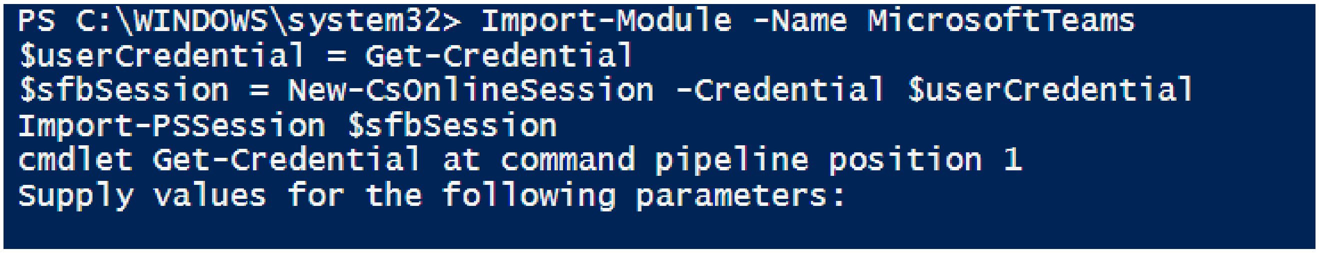
The SBC has to be paired with the Direct routing interface for direct routing to work. To achieve this, follow the below steps

### 3.2.1 Establish a remote PowerShell session to Skype for Business Online

The first step is to download Microsoft PowerShell .For more information and downloading the client, visit Microsoft's website [https://docs.microsoft.com/en-us/SkypeForBusiness/set-up-your-computer-for-windows-powershell/set-up-your-computer-for-windows-powershell](https://docs.microsoft.com/en-us/SkypeForBusiness/set-up-your-computer-for-windows-powershell/set-up-your-computer-for-windows-powershell).

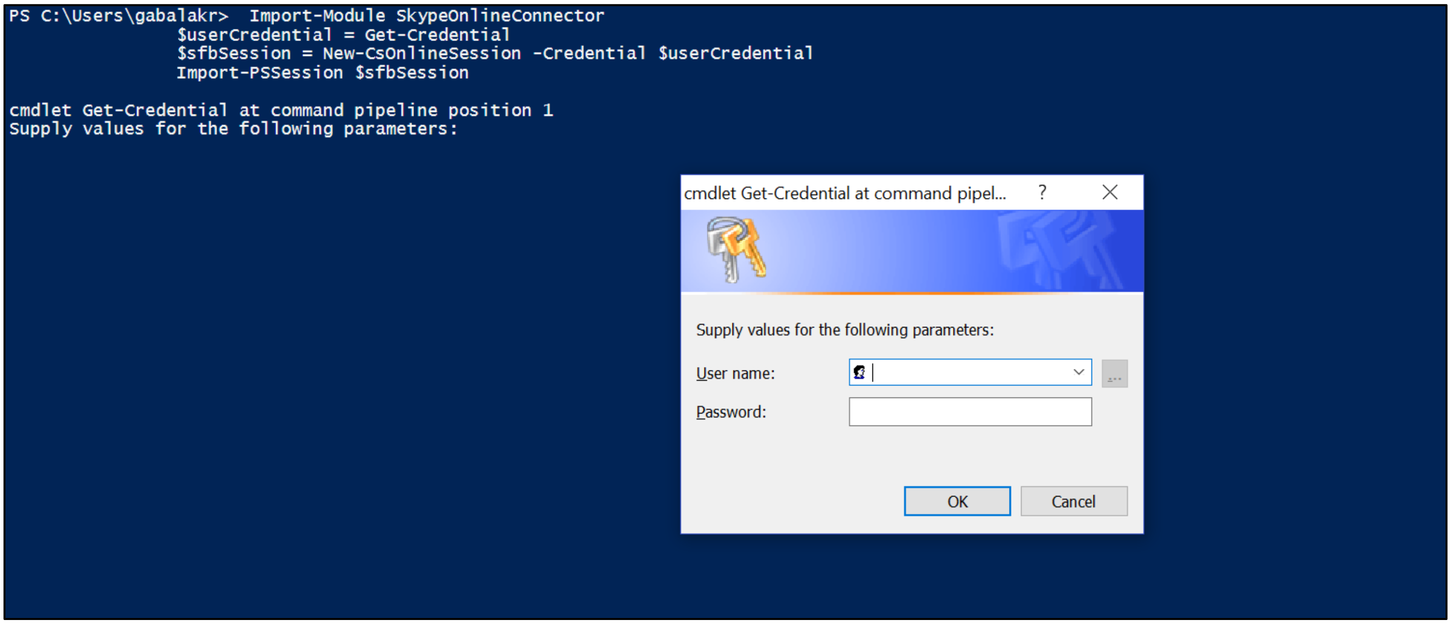
To establish a remote connection, follow the below steps

Open PowerShell and type in the below commands
Import-Module -Name MicrosoftTeams
$userCredential = Get-Credential
$sfbSession = New-CsOnlineSession -Credential $userCredential
Import-PSSession $sfbSession



```
PS C:\WINDOWS\system32> Import-Module -Name MicrosoftTeams
$userCredential = Get-Credential
$sfbSession = New-CsOnlineSession -Credential $userCredential
Import-PSSession $sfbSession
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
```

- PowerShell prompts for a username and password. Enter the tenant username and password. Tenants are used in pairing the SBC with the direct routing interface.



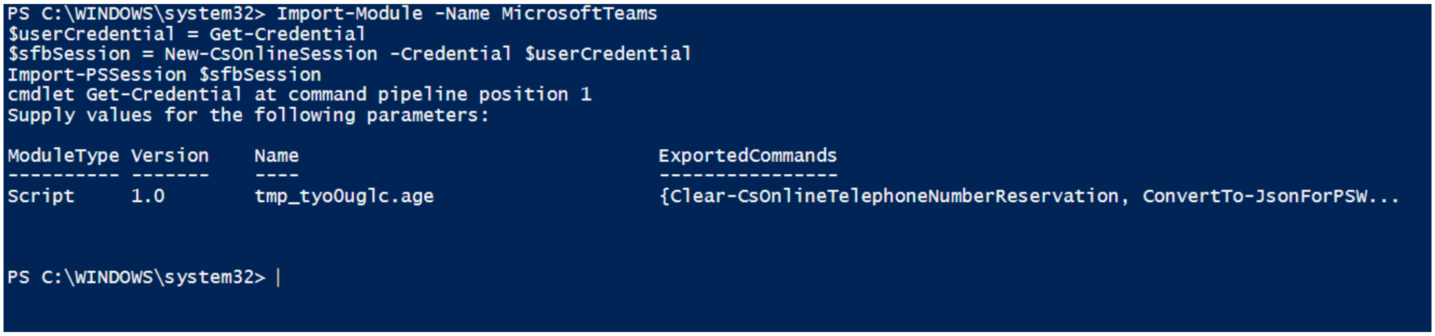
```
PS C:\Users\gabalakr>  Import-Module SkypeOnlineConnector
                $userCredential = Get-Credential
                $sfbSession = New-CsOnlineSession -Credential $userCredential
                Import-PSSession $sfbSession

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
```

cmdlet Get-Credential at command pipel...

Supply values for the following parameters:

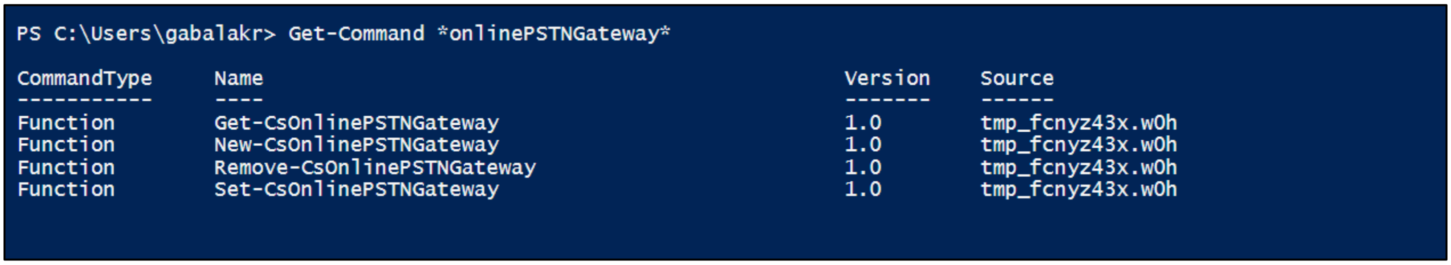
User name:

Password:



```
PS C:\WINDOWS\system32> Import-Module -Name MicrosoftTeams
$userCredential = Get-Credential
$sfbSession = New-CsOnlineSession -Credential $userCredential
Import-PSSession $sfbSession
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:

ModuleType Version    Name                             ExportedCommands
---------- -------    ----                             ----------------
Script     1.0        tmp_tyo0uglc.age                 {Clear-CsOnlineTelephoneNumberReservation, ConvertTo-JsonForPSW...


PS C:\WINDOWS\system32> |
```

- Now the remote connection is established. Check whether the remote connection is proper by using the below command
  “Get-Command *onlinePSTNGateway*”
  The command will return the four functions shown here that will let you manage the SBC.



```
PS C:\Users\gabalakr> Get-Command *onlinePSTNGateway*

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Get-CsOnlinePSTNGateway                            1.0        tmp_fcnyz43x.w0h
Function        New-CsOnlinePSTNGateway                            1.0        tmp_fcnyz43x.w0h
Function        Remove-CsOnlinePSTNGateway                         1.0        tmp_fcnyz43x.w0h
Function        Set-CsOnlinePSTNGateway                            1.0        tmp_fcnyz43x.w0h
```

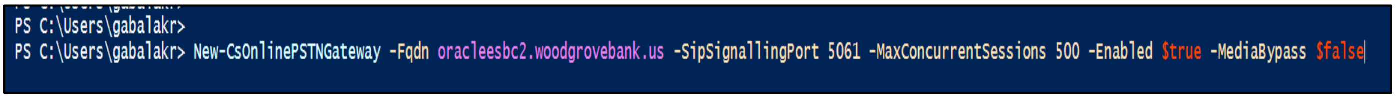
### 3.2.2 Pair the SBC to tenant

To pair SBC to the tenant, type the command as shown below. Here the FQDN used is oraclesbc.woodgrovebank.us

New-CsOnlinePSTNGateway -Fqdn <SBC FQDN> -SipSignalingPort <SBC SIP Port> -MaxConcurrentSessions <Max Concurrent Sessions the SBC can handle> -Enabled $true

For more information ,please visit the Microsoft documentation here:

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure#connect-to-skype-for-business-online-by-using-powershell

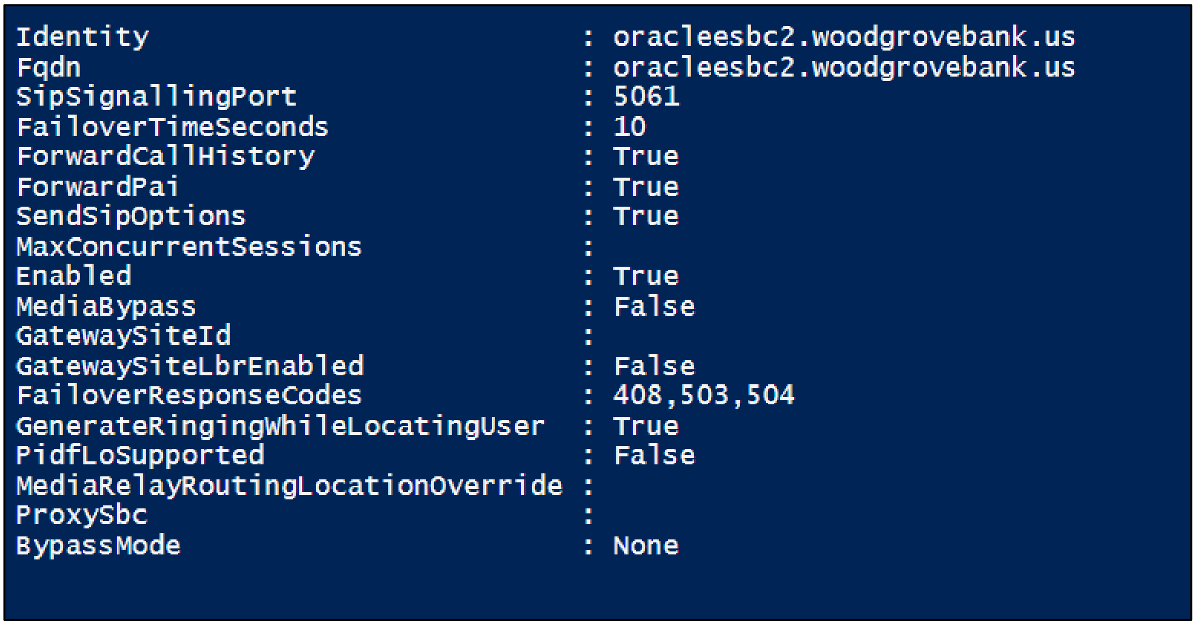


```
PS C:\Users\gabalakr>
PS C:\Users\gabalakr> New-CsOnlinePSTNGateway -Fqdn oracleesbc2.woodgrovebank.us -SipSignallingPort 5061 -MaxConcurrentSessions 500 -Enabled $true -MediaBypass $false
```

After pairing, we can check whether the SBC is present in the list of paired SBC’s by typing in the command:

Get-CsOnlinePSTNGateway -Identity oracleesbc2.woodgrovebank.us

The details of the gateway are listed when the above command is entered.
Verify whether the enabled parameter is set to true.
The OPTIONS ping from the SBC is now responded with 200OK.Once there are incoming options to the direct routing interface, it starts sending OPTIONS to the SBC.



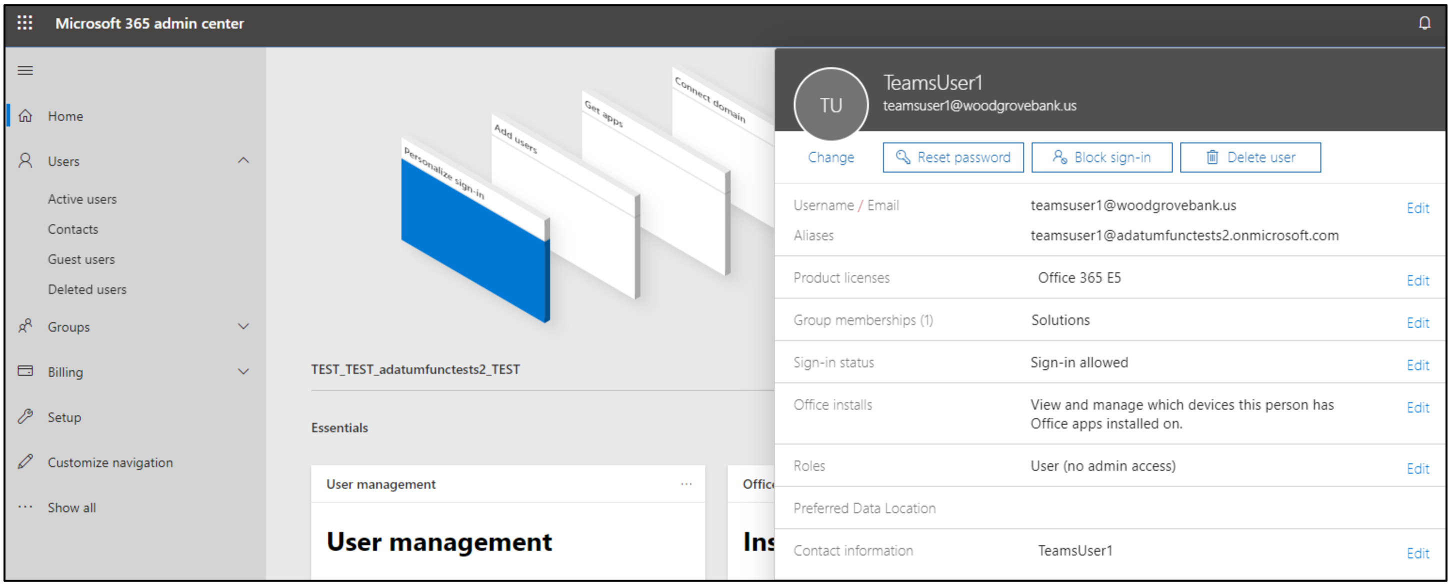
```
Identity                           : oracleesbc2.woodgrovebank.us
Fqdn                               : oracleesbc2.woodgrovebank.us
SipSignallingPort                  : 5061
FailoverTimeSeconds                : 10
ForwardCallHistory                 : True
ForwardPai                         : True
SendSipOptions                     : True
MaxConcurrentSessions              :
Enabled                            : True
MediaBypass                        : False
GatewaySiteId                      :
GatewaySiteLbrEnabled              : False
FailoverResponseCodes              : 408,503,504
GenerateRingingWhileLocatingUser   : True
PidfLoSupported                    : False
MediaRelayRoutingLocationOverride  :
ProxySbc                           :
BypassMode                         : None
```

### 3.2.3 Enable users for Direct Routing

To add users, create a user in Office 365 and assign a license. Here the following user is created: teamsuser1@woodgrovebank.us

Here the following license is added

- Office 365 Enterprise E5 (including SfB Plan2, Exchange Plan2, Teams, and Phone System)

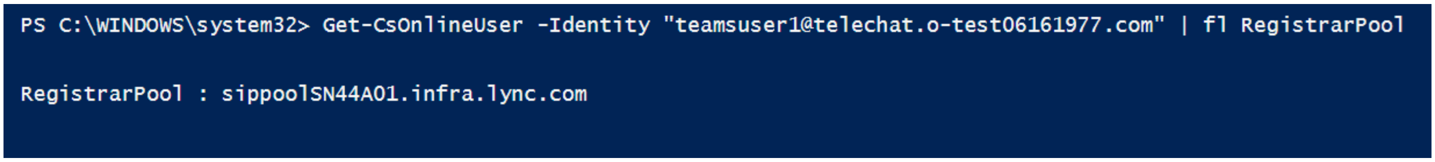


TeamsUser1
teamsuser1@woodgrovebank.us

| | |
|---|---|
| Username / Email | teamsuser1@woodgrovebank.us |
| Aliases | teamsuser1@adatumfunctests2.onmicrosoft.com |
| Product licenses | Office 365 E5 |
| Group memberships (1) | Solutions |
| Sign-in status | Sign-in allowed |
| Office installs | View and manage which devices this person has Office apps installed on. |
| Roles | User (no admin access) |
| Preferred Data Location | |
| Contact information | TeamsUser1 |

Verify whether the user is homed in Skype for business Online by issuing the below command in PowerShell

“Get-CsOnlineUser -Identity "<User name>" | fl RegistrarPool”
Here the “infra.lync.com” verifies that the user is homed.

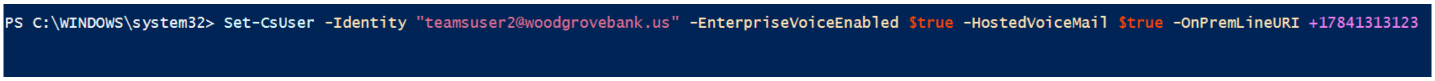


```
PS C:\WINDOWS\system32> Get-CsOnlineUser -Identity "teamsuser1@telechat.o-test06161977.com" | fl RegistrarPool

RegistrarPool : sippoolSN44A01.infra.lync.com
```

**Assign a phone number to the user**

After creating a user, a phone number and voice mail has to be assigned through Powershell. Enter the below command for assigning a phone number.

Set-CsUser -Identity "<User name>" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI tel:<E.164 phone number>



```
PS C:\WINDOWS\system32> Set-CsUser -Identity "teamsuser2@woodgrovebank.us" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI +17841313123
```

The phone number used has to be configured as a full E.164 phone number with country code.

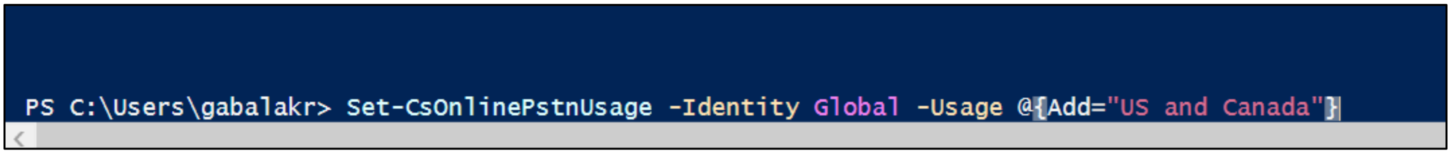
**Configure Voice Routing**

Voice Routing is performed by the direct routing Interface based on the following elements

- Voice Routing Policy
- PSTN Usages
- Voice Routes
- Online PSTN Gateway

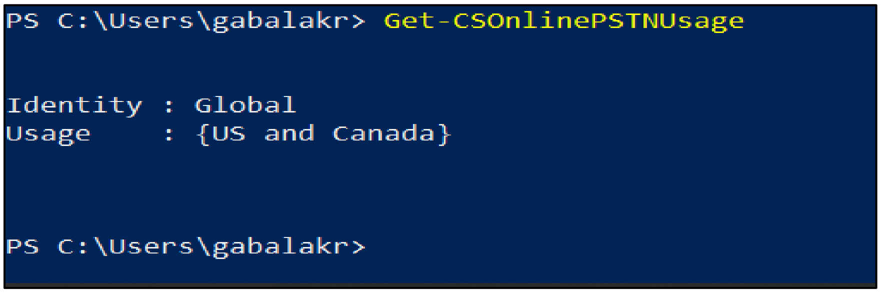
Here is an example to configure routes, PSTN usage, voice routing policy and assigning the policy to user.

1. Create the PSTN Usage "US and Canada".



```
PS C:\Users\gabalakr> Set-CsOnlinePstnUsage -Identity Global -Usage @{Add="US and Canada"}
```

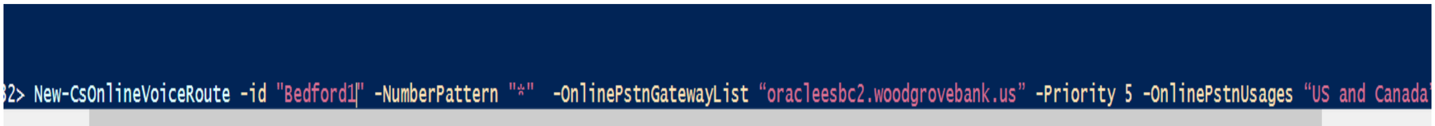
2. Verify this by executing the command below



```
PS C:\Users\gabalakr> Get-CSOnlinePSTNUsage


Identity : Global
Usage    : {US and Canada}



PS C:\Users\gabalakr>
```

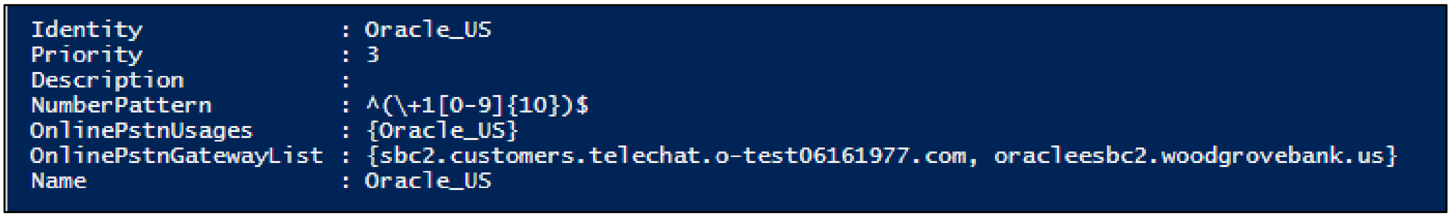
3. Configure voice route as shown below. Here all calls are routed to the same SBC.This is achieved by using -NumberPattern ".*"

New-CsOnlineVoiceRoute -id "$Routename" -NumberPattern "*"  -OnlinePstnGatewayList “oracleesbc2.woodgrovebank.us” -Priority 5 -OnlinePstnUsages “US and Canada”



```
32> New-CsOnlineVoiceRoute -id "Bedford1" -NumberPattern "*"  -OnlinePstnGatewayList “oracleesbc2.woodgrovebank.us” -Priority 5 -OnlinePstnUsages “US and Canada”
```

4.Verify the configuration by typing in the following command Get-CsOnlineVoiceRoute

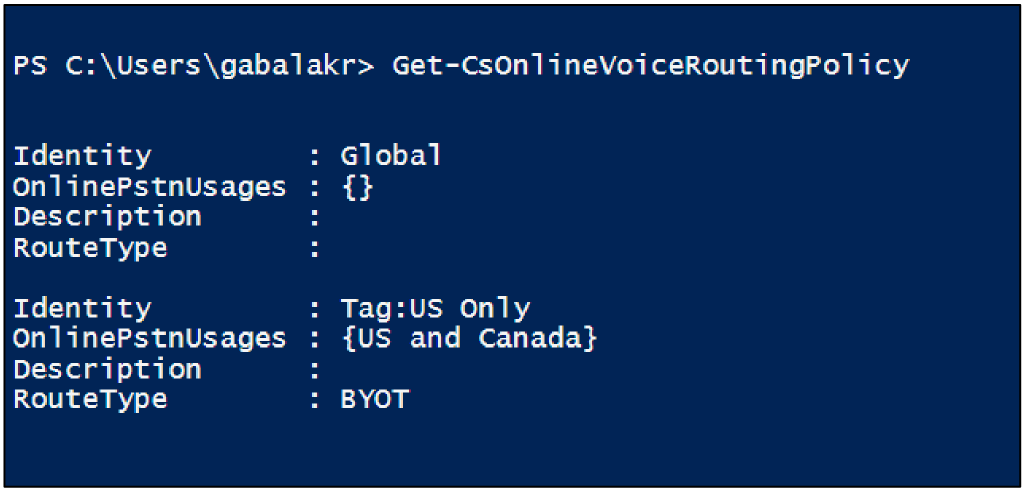


```
Identity                 : Oracle_US
Priority                 : 3
Description              :
NumberPattern            : ^(\+1[0-9]{10})$
OnlinePstnUsages         : {Oracle_US}
OnlinePstnGatewayList    : {sbc2.customers.telechat.o-test06161977.com, oracleesbc2.woodgrovebank.us}
Name                     : Oracle_US
```

5. Create a Voice Routing Policy "US Only" and add to the policy the PSTN Usage "US and Canada.".Use the following command

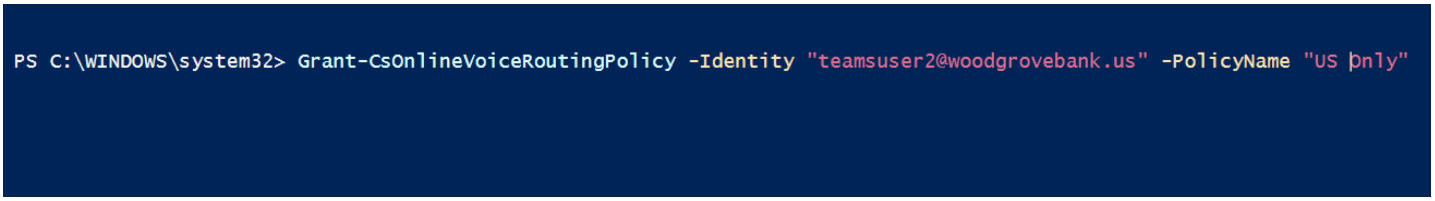
New-CsOnlineVoiceRoutingPolicy "US Only" -OnlinePstnUsages "US and Canada"

This can be verified through the following command.



```
PS C:\Users\gabalakr> Get-CsOnlineVoiceRoutingPolicy


Identity            : Global
OnlinePstnUsages : {}
Description         :
RouteType           :

Identity            : Tag:US Only
OnlinePstnUsages : {US and Canada}
Description         :
RouteType           : BYOT
```

6. Grant to user teamsuser1 a voice routing policy by using PowerShell



```
PS C:\WINDOWS\system32> Grant-CsOnlineVoiceRoutingPolicy -Identity "teamsuser2@woodgrovebank.us" -PolicyName "US Only"
```

7. Validate the same using the PowerShell command as shown below
   $GetUserDetails=Get-CsOnlineUser -Identity teamsuser2@woodgrovebank.us
   $GetUserVoiceRoutePolicy = $GetUserDetails.OnlineVoiceRoutingPolicy

## 3.3 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.

|  |  |  |  |
|---|---|---|---|
| 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 Crypto Suite | AES_CM_128_HMAC_SHA1_80, non-MKI | DTLS-SRTP is not supported |
|  | 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 | ICE-lite (RFC5245) – recommended,<br>• Client also has Transport Relays |  |
| Codecs | Audio codecs | • G711<br>• G722<br>• Silk (Teams clients)<br>• Opus (WebRTC clients) - Only if Media Bypass is used;<br>• G729 |  |
|  | Other codecs | • DTMF – Required<br>• Events 0-16<br>• CN<br>• Required narrowband and wideband<br>• RED – Not required<br>• Silence Suppression – Not required |  |

## 3.4 Requirements to SIP messages “Invite” and “Options”

Microsoft Teams Hybrid Voice Connectivity interface has requirements for the syntax of SIP messages.

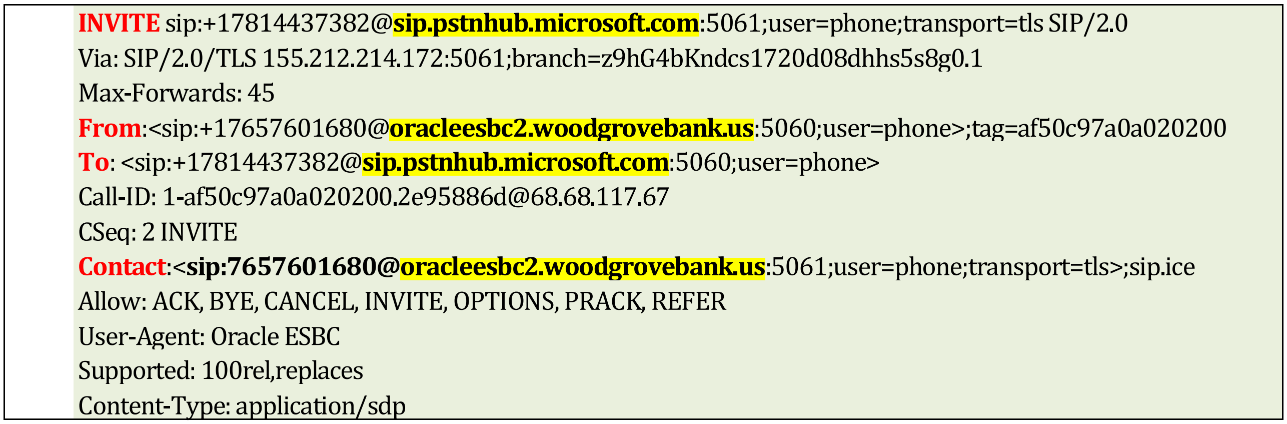
The section covers high-level requirements to SIP syntax of Invite and Options messages. The information can be used as a first step during troubleshooting when calls don’t go through. From our experience most of the issues are related to the wrong syntax of SIP messages.

**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

## 3.5 Requirements for “INVITE” messages syntax

Picture 1 Example of INVITE message



```
INVITE sip:+17814437382@sip.pstnhub.microsoft.com:5061;user=phone;transport=tls SIP/2.0
Via: SIP/2.0/TLS 155.212.214.172:5061;branch=z9hG4bKndcs1720d08dhhs5s8g0.1
Max-Forwards: 45
From:<sip:+17657601680@oracleesbc2.woodgrovebank.us:5060;user=phone>;tag=af50c97a0a020200
To: <sip:+17814437382@sip.pstnhub.microsoft.com:5060;user=phone>
Call-ID: 1-af50c97a0a020200.2e95886d@68.68.117.67
CSeq: 2 INVITE
Contact:<sip:7657601680@oracleesbc2.woodgrovebank.us:5061;user=phone;transport=tls>;sip.ice
Allow: ACK, BYE, CANCEL, INVITE, OPTIONS, PRACK, REFER
User-Agent: Oracle ESBC
Supported: 100rel,replaces
Content-Type: application/sdp
```

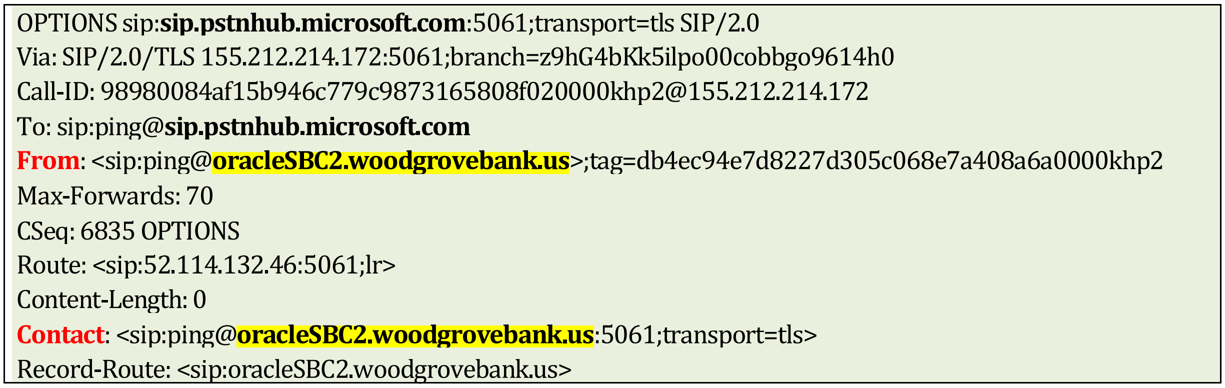
1. **Request-URI**
   The recommendation is to set the Global FQDN name of the direct routing, in URI hostname when sending calls to Hybrid Voice Connectivity interface.
   Syntax: INVITE sip: <phone number>@<Global FQDN > SIP/2.0
2. **From and To headers**
   **Must**: When placing calls to Teams Hybrid Voice Connectivity Interface “FROM” header MUST have SBC FQDN in URI hostname:
   Syntax: From:sip: <phone number>@<FQDN of the SBC>;tag=....
   If the parameter is not set correctly, the calls are rejected with “403 Forbidden” message.
   **Recommended**: When placing calls to Teams Hybrid Voice Connectivity Interface “To” header have SBC FQDN in URI hostname of the Syntax: To: INVITE sip: <phone number>@<FQDN of the SBC>
3. **Contact**

Must have the SBC FQDN for media negotiation. Syntax: Contact: <phone number>@<FQDN of the SBC>:<SBC Port>;<transport type>

The above requirements are automatically fulfilled in the referenced build of the software.

## 3.6 Requirements for “OPTIONS” messages syntax

Picture 2 Example of OPTIONS message



```
OPTIONS sip:sip.pstnhub.microsoft.com:5061;transport=tls SIP/2.0
Via: SIP/2.0/TLS 155.212.214.172:5061;branch=z9hG4bKk5ilpo00cobbgo9614h0
Call-ID: 98980084af15b946c779c9873165808f020000khp2@155.212.214.172
To: sip:ping@sip.pstnhub.microsoft.com
From: <sip:ping@oracleSBC2.woodgrovebank.us>;tag=db4ec94e7d8227d305c068e7a408a6a0000khp2
Max-Forwards: 70
CSeq: 6835 OPTIONS
Route: <sip:52.114.132.46:5061;lr>
Content-Length: 0
Contact: <sip:ping@oracleSBC2.woodgrovebank.us:5061;transport=tls>
Record-Route: <sip:oracleSBC2.woodgrovebank.us>
```

1. **From header**

   When sending OPTIONS to Teams Hybrid Voice Connectivity Interface “FROM” header MUST have SBC FQDN in URI hostname:

   Syntax: From: sip: <phone number>@<FQDN of the SBC>;tag=....

   If the parameter is not set correctly, the OPTIONS are rejected with “403 Forbidden” message.

2. **Contact.**

   When sending OPTIONS to Teams Hybrid Voice Connectivity 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, outbound OPTIONS won’t be sent by Teams

The above requirements are automatically fulfilled in the referenced build of the software.

## 3.7 Validated Oracle version

Oracle conducted tests with Oracle SBC SCZ8.3 software – this software with the configuration listed below can run on any of the following products:

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

Here Release SCZ830p7 is the software version used. Please upgrade to SCZ830p7 before configuring Oracle SBC for MS Teams.

# 4 Configuring the SBC

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

The Figure 1 below shows the connection topology example.

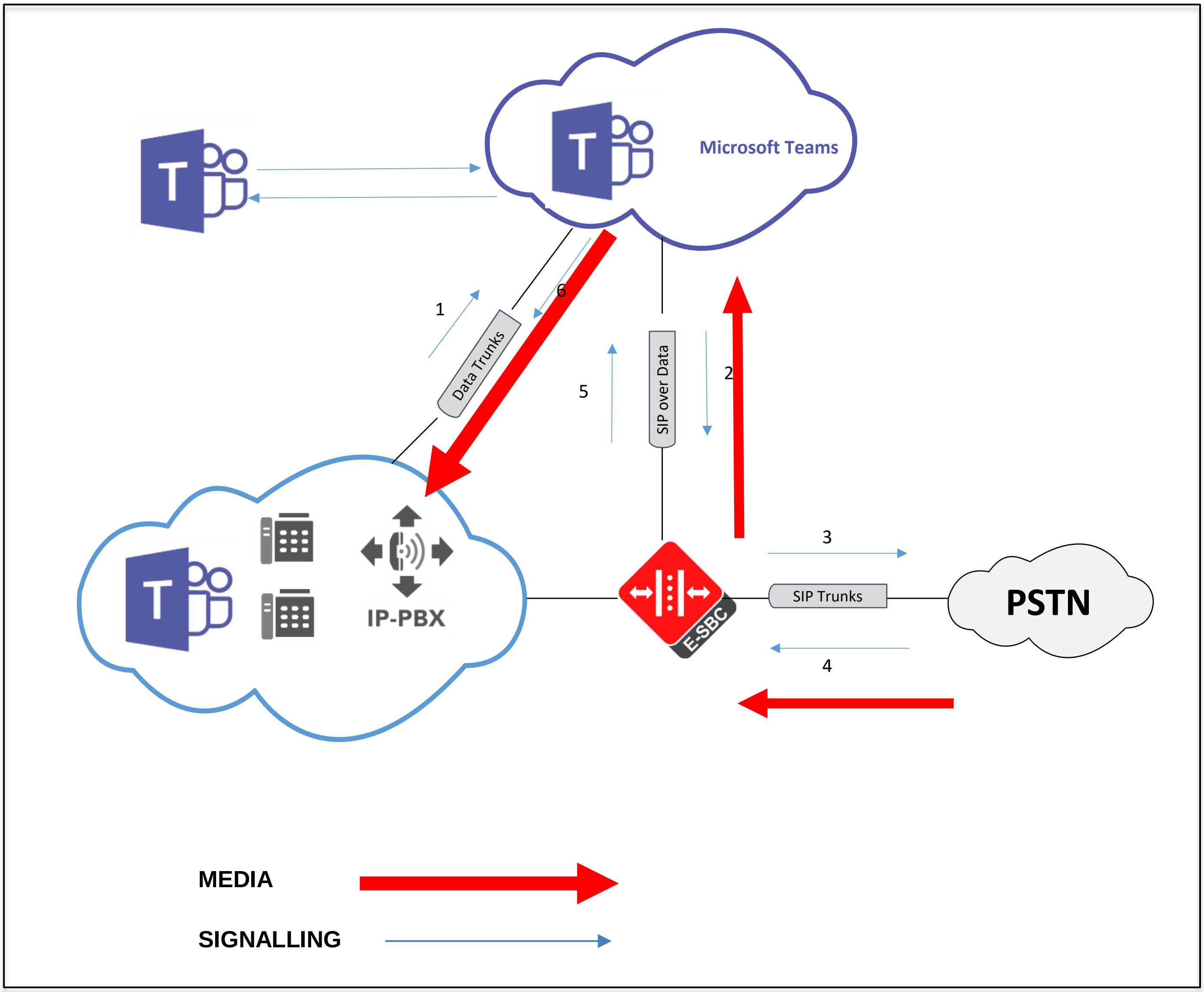


*Figure :1: Signaling & media flow with media-bypass disabled*

There are several connection entities on the picture:

- Enterprise network consisting of an IP-PBX and Teams client
- Microsoft Teams Direct Routing Interface on the WAN
- SIP trunk from a 3rd party provider on the WAN

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.

# 5 New SBC configuration

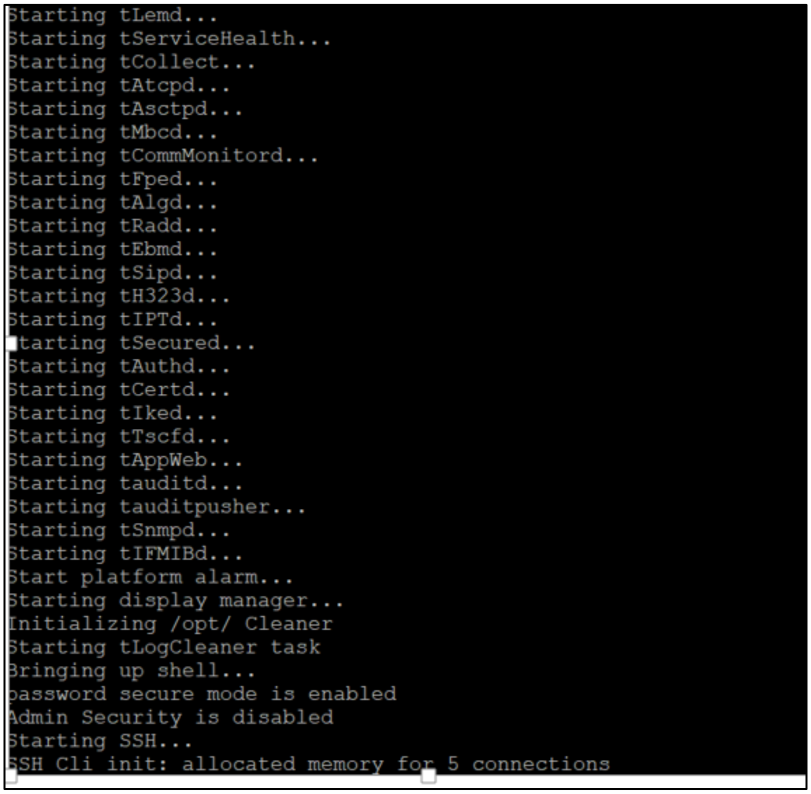
If the customer is looking to setup a new out of the box Oracle SBC with Microsoft teams, please follow the section below.

## 5.1 Establishing a serial connection to the SBC

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

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

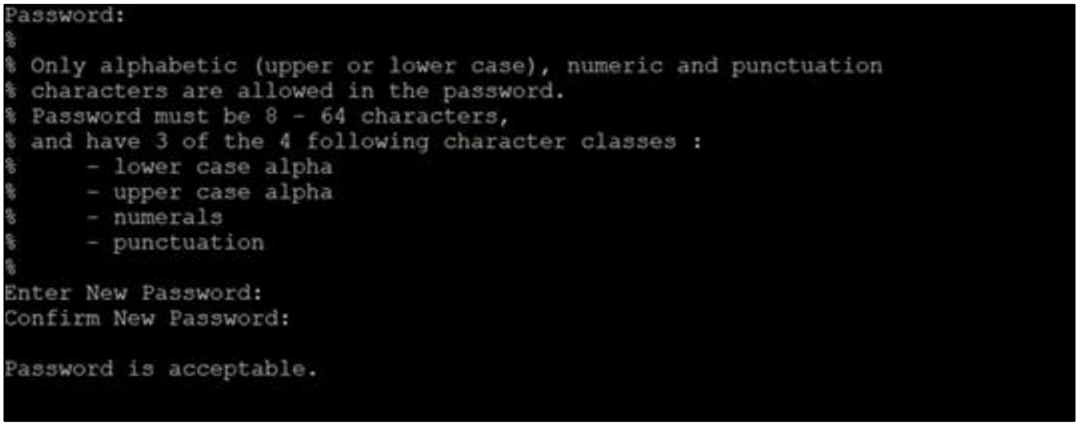
Power on the SBC and confirm that you see the following output from the boot-up sequence



```
Starting tLemd...
Starting tServiceHealth...
Starting tCollect...
Starting tAtcpd...
Starting tAsctpd...
Starting tMbcd...
Starting tCommMonitord...
Starting tFped...
Starting tAlgd...
Starting tRadd...
Starting tEbmd...
Starting tSipd...
Starting tH323d...
Starting tIPTd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tTscfd...
Starting tAppWeb...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Starting tIFMIBd...
Start platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...
password secure mode is enabled
Admin Security is disabled
Starting SSH...
SSH Cli init: allocated memory for 5 connections
```

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

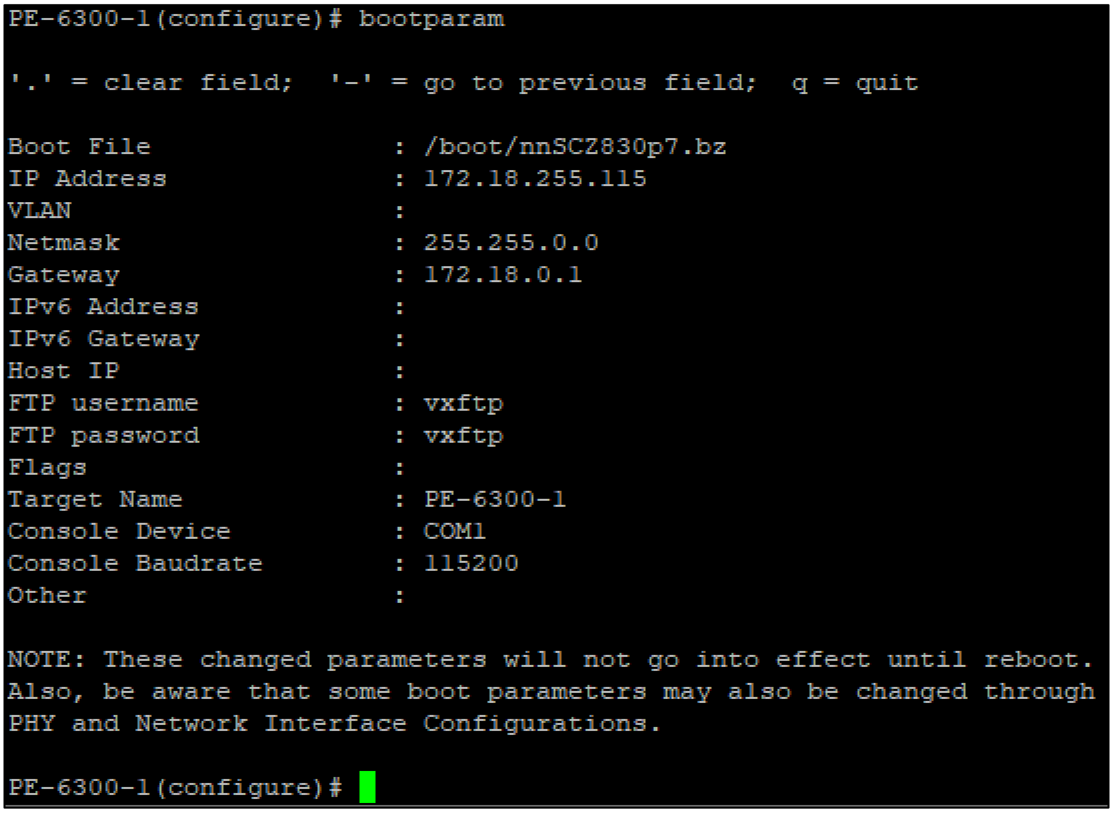
Both passwords have to be changed according to the rules shown below.



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

Password is acceptable.
```

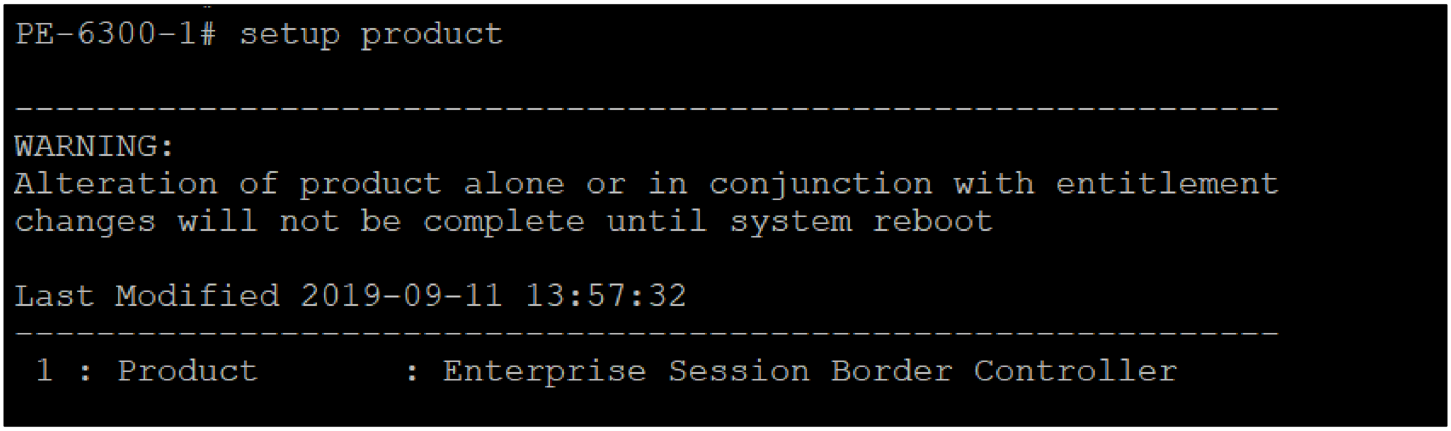
Now set the management IP of the SBC by setting the IP address in bootparam.to access bootparam. Go to Configure terminal->bootparam.

Note: There is no management IP configured by default.



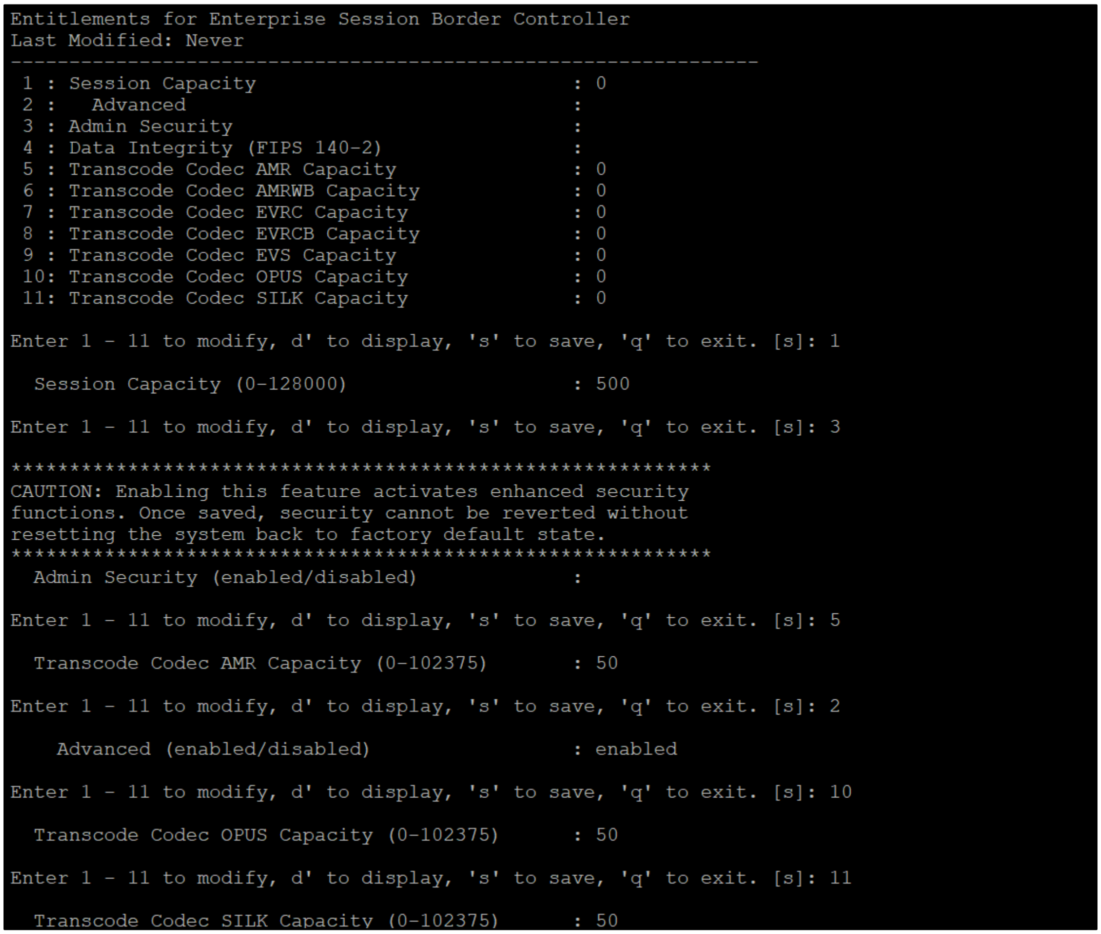
```
PE-6300-1(configure)# bootparam

'.' = clear field;  '-' = go to previous field;  q = quit

Boot File                : /boot/nnSCZ830p7.bz
IP Address               : 172.18.255.115
VLAN                     :
Netmask                  : 255.255.0.0
Gateway                  : 172.18.0.1
IPv6 Address             :
IPv6 Gateway             :
Host IP                  :
FTP username             : vxftp
FTP password             : vxftp
Flags                    :
Target Name              : PE-6300-1
Console Device           : COM1
Console Baudrate         : 115200
Other                    :

NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.

PE-6300-1(configure)#
```

Setup product type to Enterprise Session Border Controller as shown. To configure product type, type in setup product in the terminal.



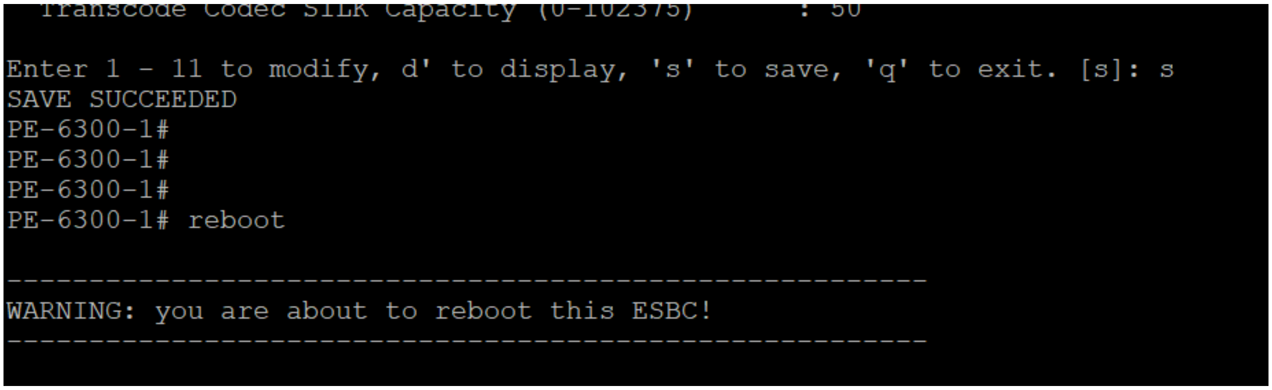
```
PE-6300-1# setup product

-------------------------------------------------------------
WARNING:
Alteration of product alone or in conjunction with entitlement
changes will not be complete until system reboot

Last Modified 2019-09-11 13:57:32
-------------------------------------------------------------
 1 : Product       : Enterprise Session Border Controller
```

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



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

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

  Session Capacity (0-128000)                     : 500

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 3

************************************************************
CAUTION: Enabling this feature activates enhanced security
functions. Once saved, security cannot be reverted without
resetting the system back to factory default state.
************************************************************
  Admin Security (enabled/disabled)               :

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

  Transcode Codec AMR Capacity (0-102375)         : 50

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

    Advanced (enabled/disabled)                   : enabled

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

  Transcode Codec OPUS Capacity (0-102375)        : 50

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

  Transcode Codec SILK Capacity (0-102375)        : 50
```

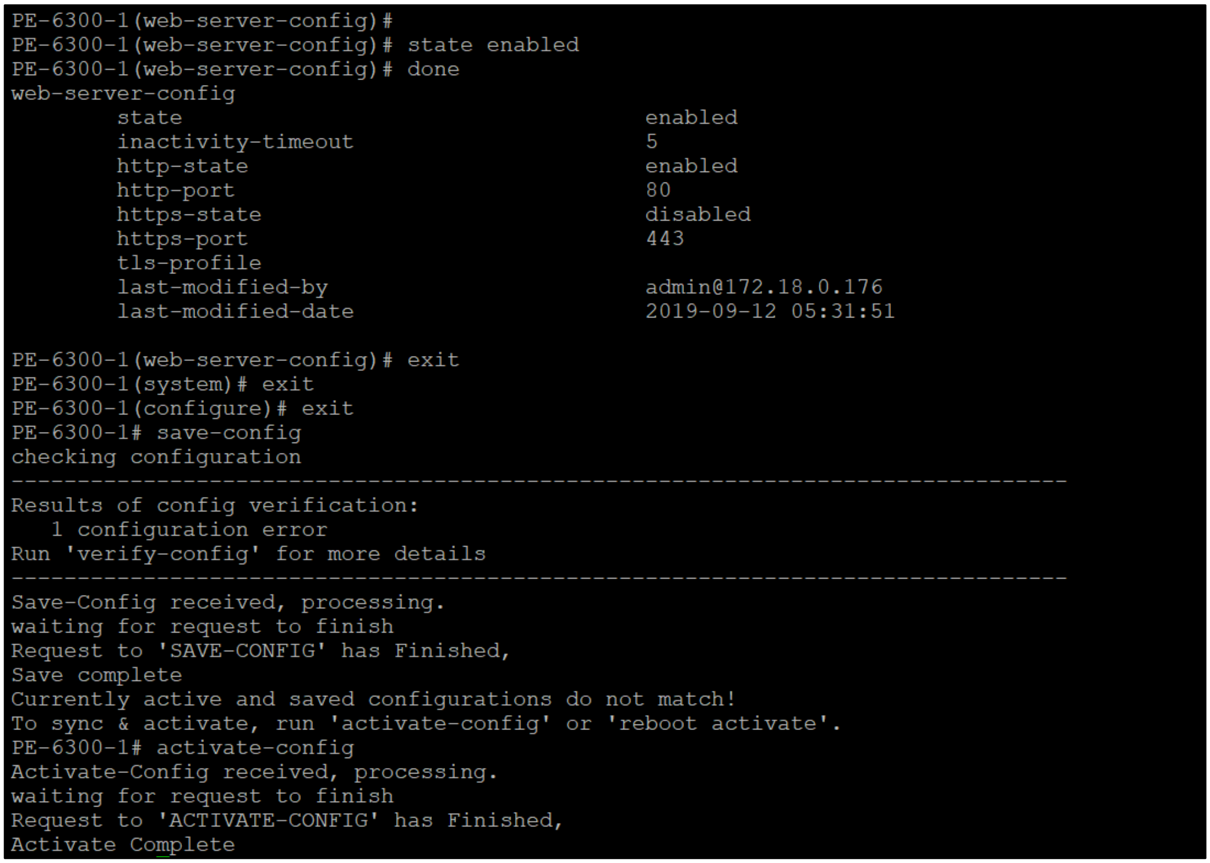
Save the changes and reboot the SBC.



```
 Transcode Codec SILK Capacity (0-102375)      : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
SAVE SUCCEEDED
PE-6300-1#
PE-6300-1#
PE-6300-1#
PE-6300-1# reboot

--------------------------------------------------------
WARNING: you are about to reboot this ESBC!
--------------------------------------------------------
```

When the SBC comes up after reboot, it is now ready for you to add a configuration.

Go to configure terminal->system->web-server-config. Enable the web-server-config to access the SBC using WebGUI. Save and activate the config.

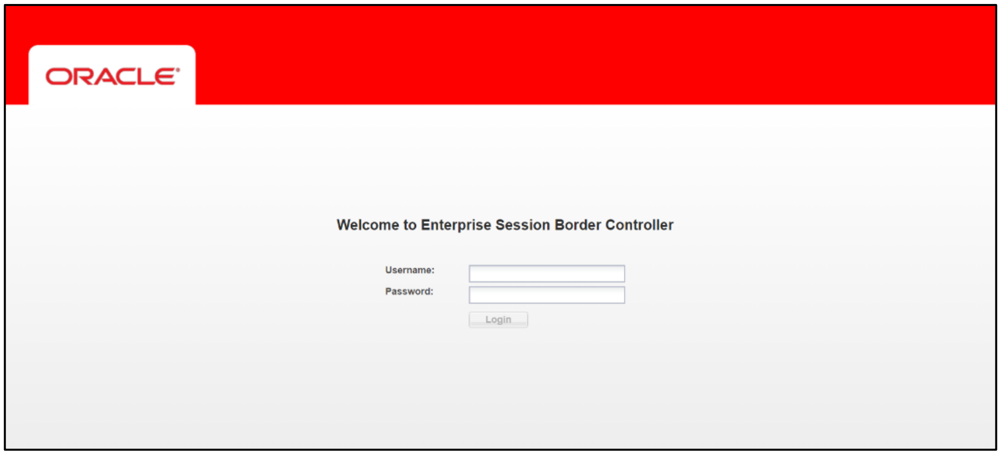


```
PE-6300-1(web-server-config)#
PE-6300-1(web-server-config)# state enabled
PE-6300-1(web-server-config)# done
web-server-config
        state                                   enabled
        inactivity-timeout                      5
        http-state                              enabled
        http-port                               80
        https-state                             disabled
        https-port                              443
        tls-profile
        last-modified-by                        admin@172.18.0.176
        last-modified-date                      2019-09-12 05:31:51

PE-6300-1(web-server-config)# exit
PE-6300-1(system)# exit
PE-6300-1(configure)# exit
PE-6300-1# save-config
checking configuration
--------------------------------------------------------------------------------
Results of config verification:
   1 configuration error
Run 'verify-config' for more details
--------------------------------------------------------------------------------
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
PE-6300-1# activate-config
Activate-Config received, processing.
waiting for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
```

## 5.2 Configure SBC using Web GUI

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

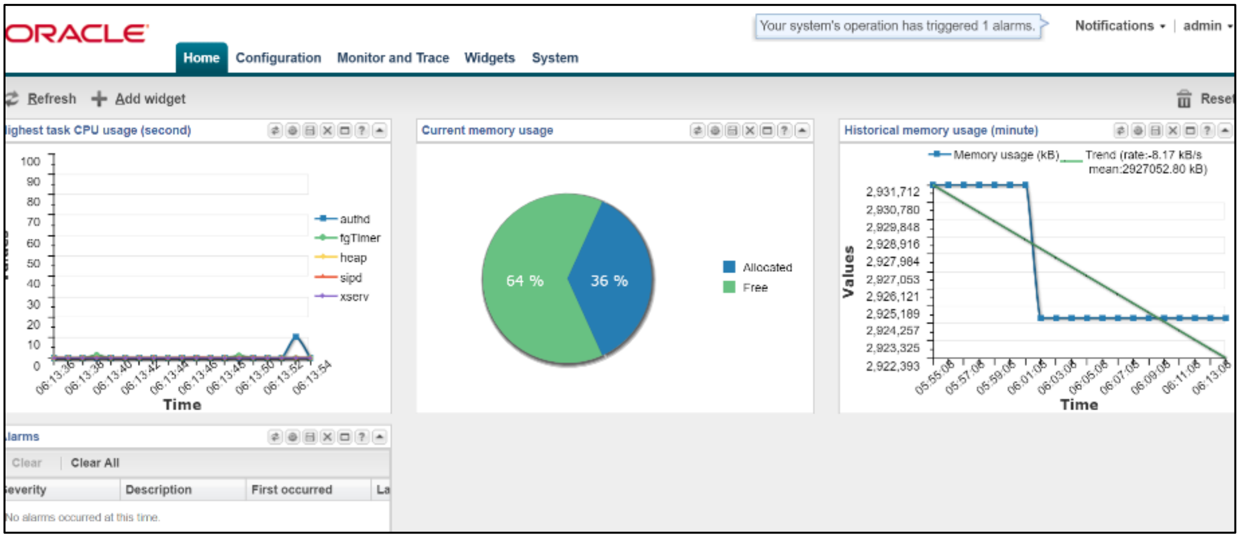
The WebGUI can be accessed through the url https://<SBC_MGMT_IP>. The username and password is the same as that of CLI.



Welcome to Enterprise Session Border Controller

Username:

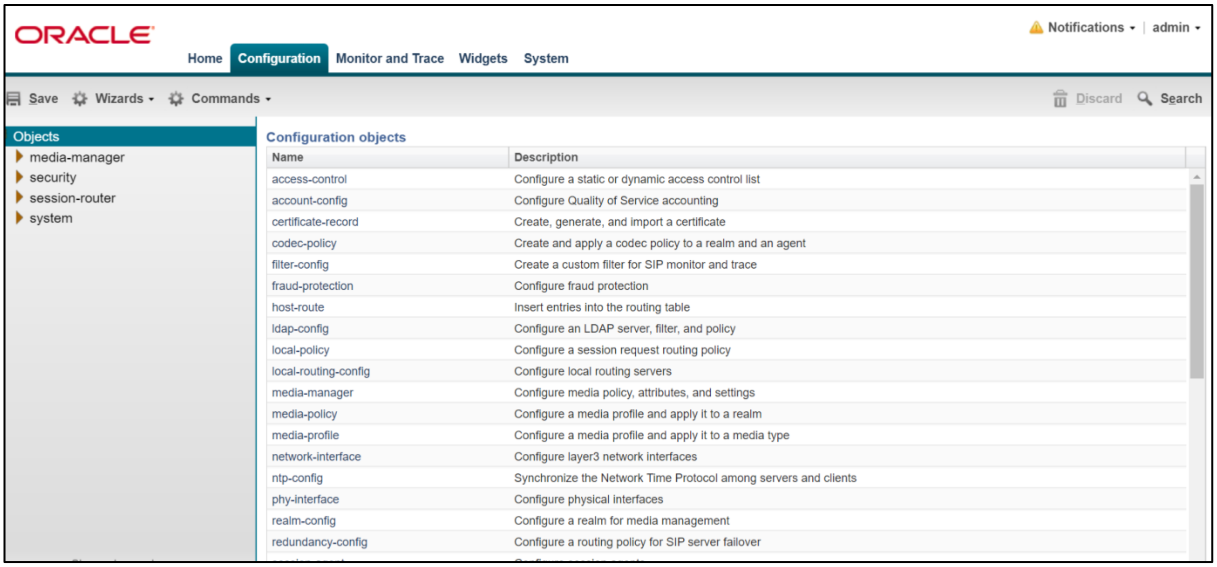
Password:



Your system's operation has triggered 1 alarms.

No alarms occurred at this time.

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



Configuration objects

| Name | Description |
|---|---|
| access-control | Configure a static or dynamic access control list |
| account-config | Configure Quality of Service accounting |
| certificate-record | Create, generate, and import a certificate |
| codec-policy | Create and apply a codec policy to a realm and an agent |
| filter-config | Create a custom filter for SIP monitor and trace |
| fraud-protection | Configure fraud protection |
| host-route | Insert entries into the routing table |
| ldap-config | Configure an LDAP server, filter, and policy |
| local-policy | Configure a session request routing policy |
| local-routing-config | Configure local routing servers |
| media-manager | Configure media policy, attributes, and settings |
| media-policy | Configure a media profile and apply it to a realm |
| media-profile | Configure a media profile and apply it to a media type |
| network-interface | Configure layer3 network interfaces |
| ntp-config | Synchronize the Network Time Protocol among servers and clients |
| phy-interface | Configure physical interfaces |
| realm-config | Configure a realm for media management |
| redundancy-config | Configure a routing policy for SIP server failover |

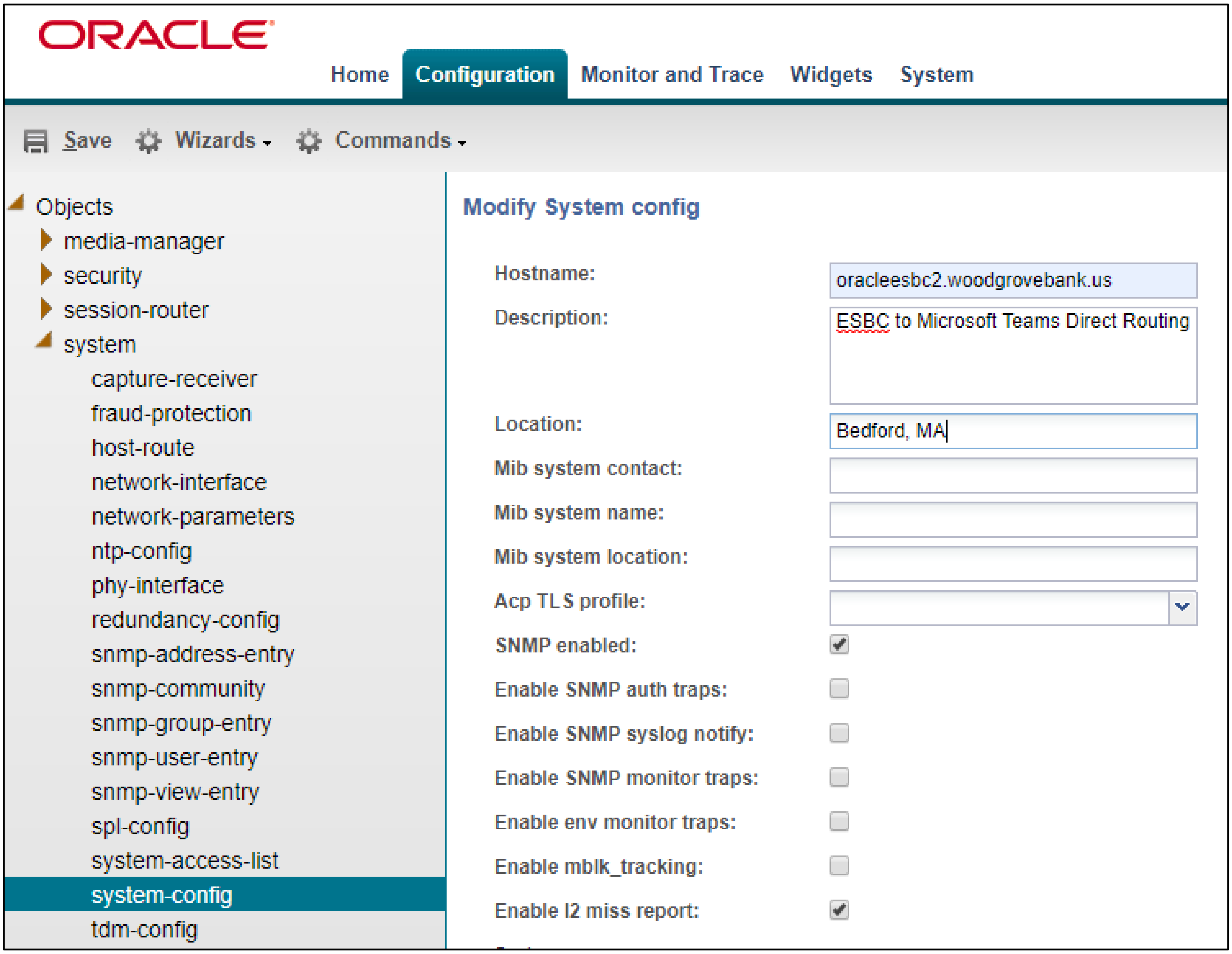
Kindly refer to the GUI User Guide [https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.3.0/webgui/esbc_scz830_webgui.pdf](https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.3.0/webgui/esbc_scz830_webgui.pdf) for more information.

The expert mode is used for configuration.

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

## 5.3 Configure system-config

Go to system->system-config



Modify System config

| | |
|---|---|
| Hostname: | oracleesbc2.woodgrovebank.us |
| Description: | ESBC to Microsoft Teams Direct Routing |
| 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: | ☑ |

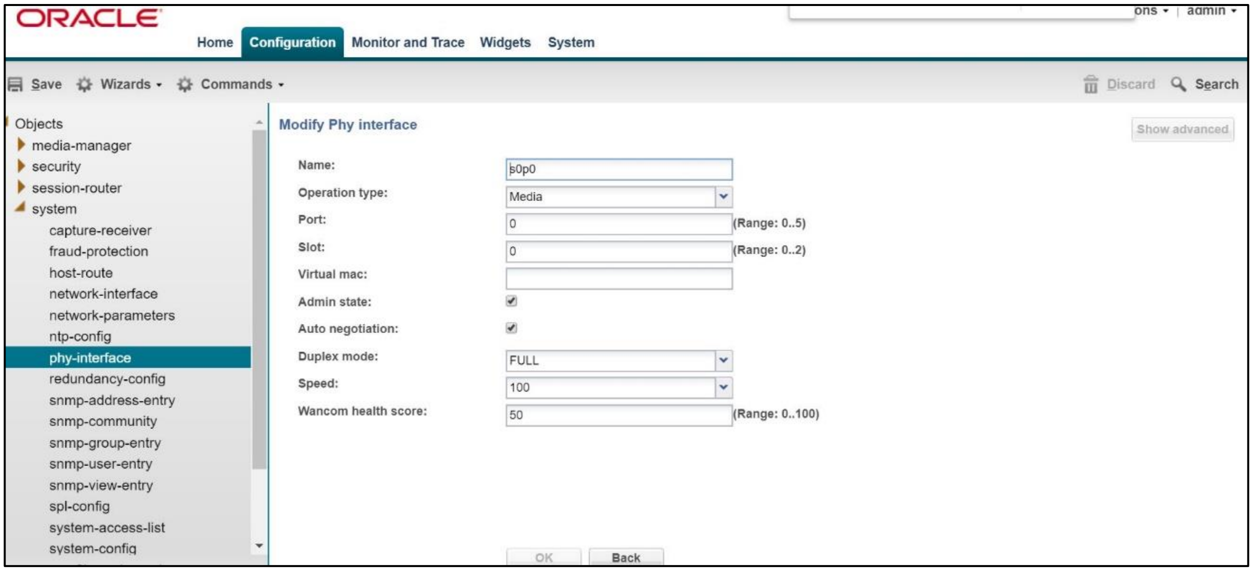
## 5.4 Configure Physical Interface values

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

You will first configure the slot 0, port 0 interface designated with the name s0p0. This will be the port plugged into your inside (connection to the PSTN gateway) interface. Teams is configured on the slot 0 port 1. Below is the screenshot for creating a phy-interface on s0p0

Create a similar interface for Teams as well from the WebGUI. The table below specifies the values for both teams and Trunk.

| Parameter Name | Trunk(s0p0) | MSTeams(s0p1) |
|---|---|---|
| Slot | 0 | 0 |
| Port | 0 | 1 |
| Operation Mode | Media | Media |



Modify Phy interface

| | | |
|---|---|---|
| Name: | s0p0 | |
| Operation type: | Media | |
| Port: | 0 | (Range: 0..5) |
| Slot: | 0 | (Range: 0..2) |
| Virtual mac: | | |
| Admin state: | ☑ | |
| Auto negotiation: | ☑ | |
| Duplex mode: | FULL | |
| Speed: | 100 | |
| Wancom health score: | 50 | (Range: 0..100) |

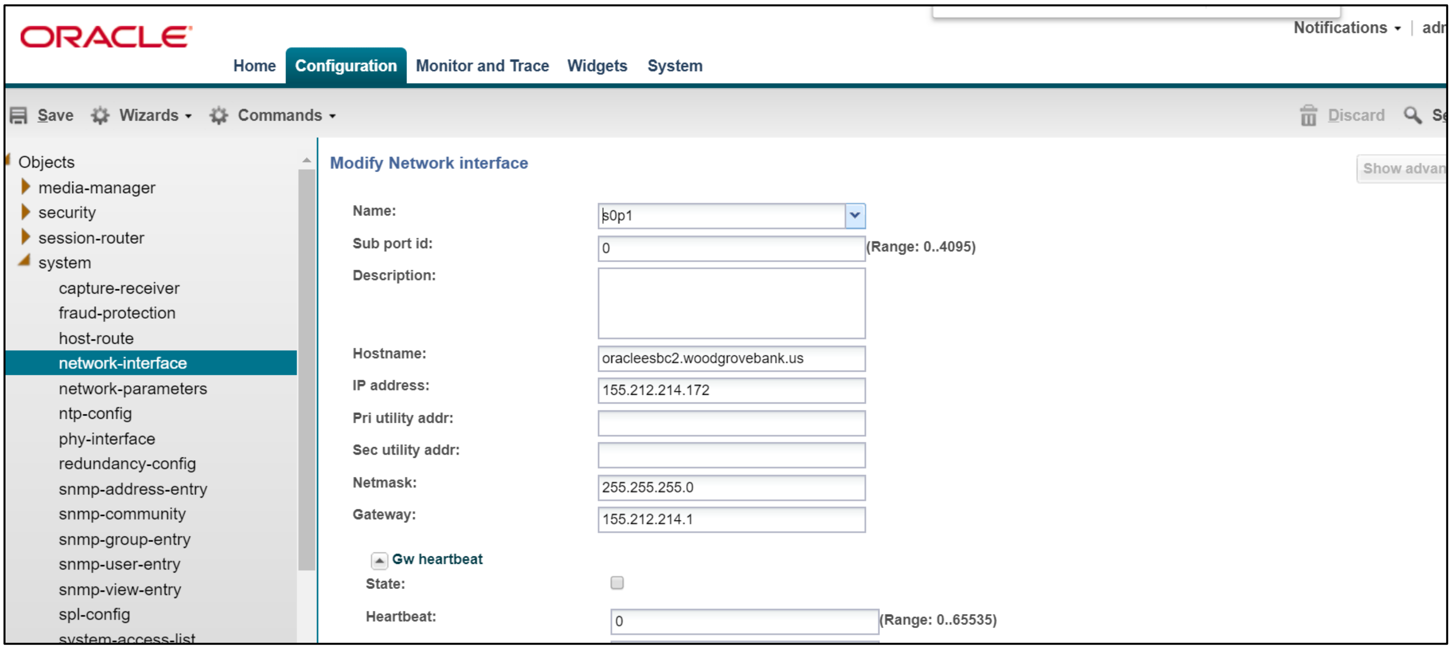
## 5.5 Configure Network Interface values

To configure network-interface, go to system->Network-Interface. Configure two interfaces, one for teams and one for PSTN trunk. Here,in the example the  Teams network interface is shown. Configure the PSTN interface in the same manner.

The table below lists the parameters, to be configured for both the interfaces. The same is modified as per  customer environment.

| Parameter Name | Teams Network Interface | PSTN trunk Network interface |
|---|---|---|
| Name | s0p1 | s0p0 |
| Host Name | oracleesbc2.woodgrovebank.us | |
| IP address | 155.212.214.172 | 192.65.72.196 |
| Netmask | 255.255.255.0 | 255.255.255.0 |
| Gateway | 155.212.214.1 | 192.65.72.1 |
| DNS-IP Primary | 8.8.8.8 | |
| DNS-domain | woodgrovebank.us | |

*Please note:  If running the GA release SCZ830m1p8A, hostname parameter in Network Interface is not mandatory, See Appendix D for additional details on how the hostname parameter is used with new features to help simplify your configuration by eliminating most, if not all required sip manipulations.*

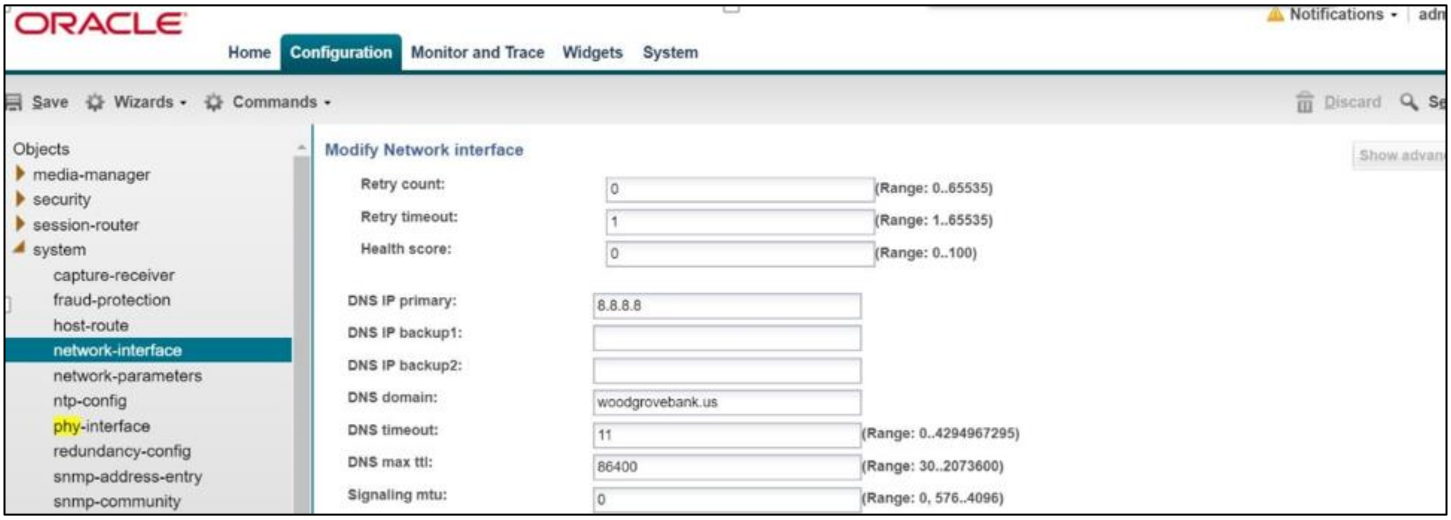


Modify Network interface

| | |
|---|---|
| Name: | s0p1 |
| Sub port id: | 0 (Range: 0..4095) |
| Description: | |
| Hostname: | oracleesbc2.woodgrovebank.us |
| IP address: | 155.212.214.172 |
| Pri utility addr: | |
| Sec utility addr: | |
| Netmask: | 255.255.255.0 |
| Gateway: | 155.212.214.1 |

Gw heartbeat

| | |
|---|---|
| State: | □ |
| Heartbeat: | 0 (Range: 0..65535) |



Modify Network interface

| | |
|---|---|
| Retry count: | 0 (Range: 0..65535) |
| Retry timeout: | 1 (Range: 1..65535) |
| Health score: | 0 (Range: 0..100) |
| DNS IP primary: | 8.8.8.8 |
| DNS IP backup1: | |
| DNS IP backup2: | |
| DNS domain: | woodgrovebank.us |
| DNS timeout: | 11 (Range: 0..4294967295) |
| DNS max ttl: | 86400 (Range: 30..2073600) |
| Signaling mtu: | 0 (Range: 0, 576..4096) |

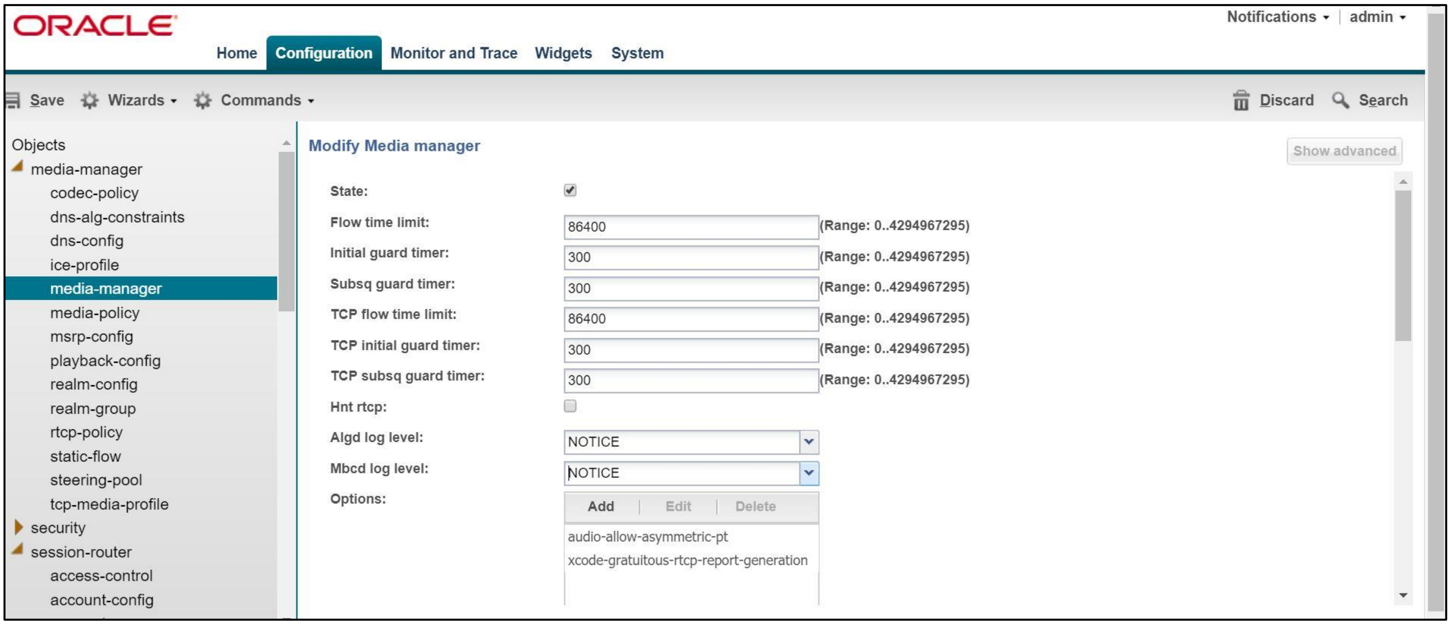
*Tip: Configure ICMP IP and HIP IP only on the PSTN side.It is not advisable to configure the ICMP ip and HIP ip on the teams facing side because of inherint risks.*

## 5.6 Enable media manager

Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager and configure the below option for generating rtcp reports.

- audio-allow-asymmetric-pt
- xcode-gratuitous-rtcp-report-generation (requires a reboot)

Go to Media-Manager->Media-Manager



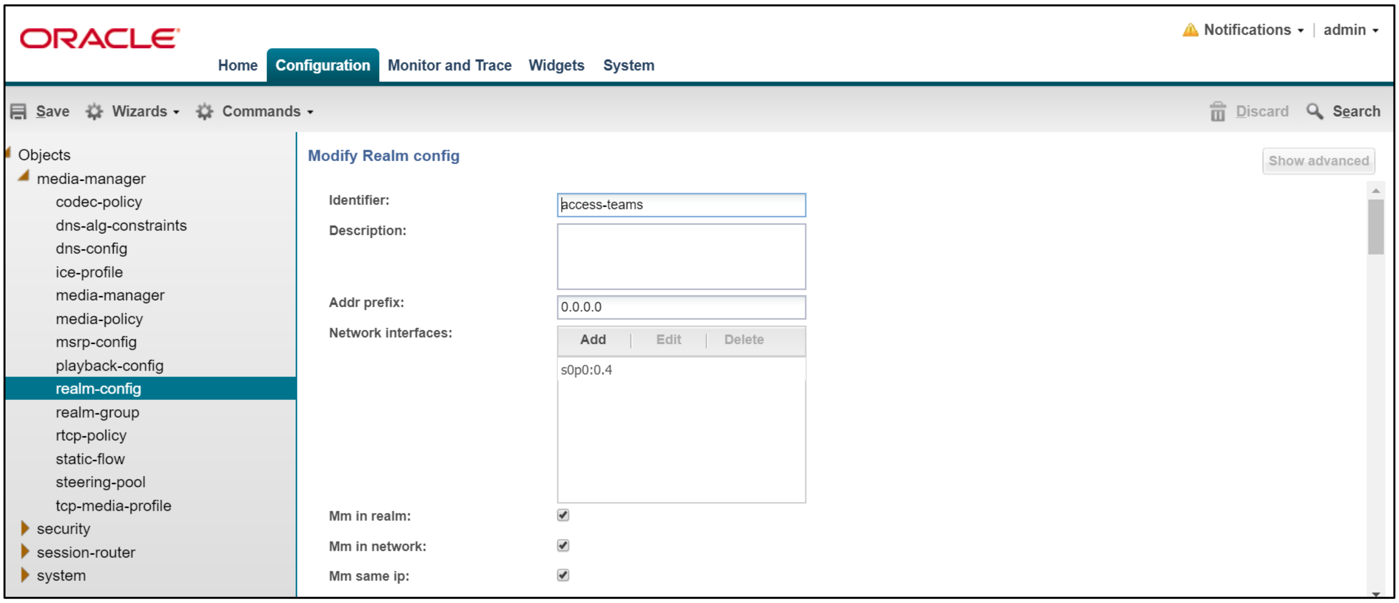
Modify Media manager

| | |
|---|---|
| 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<br>xcode-gratuitous-rtcp-report-generation |

## 5.7 Configure Realms

Navigate to realm-config under media-manager and configure a realm as shown below

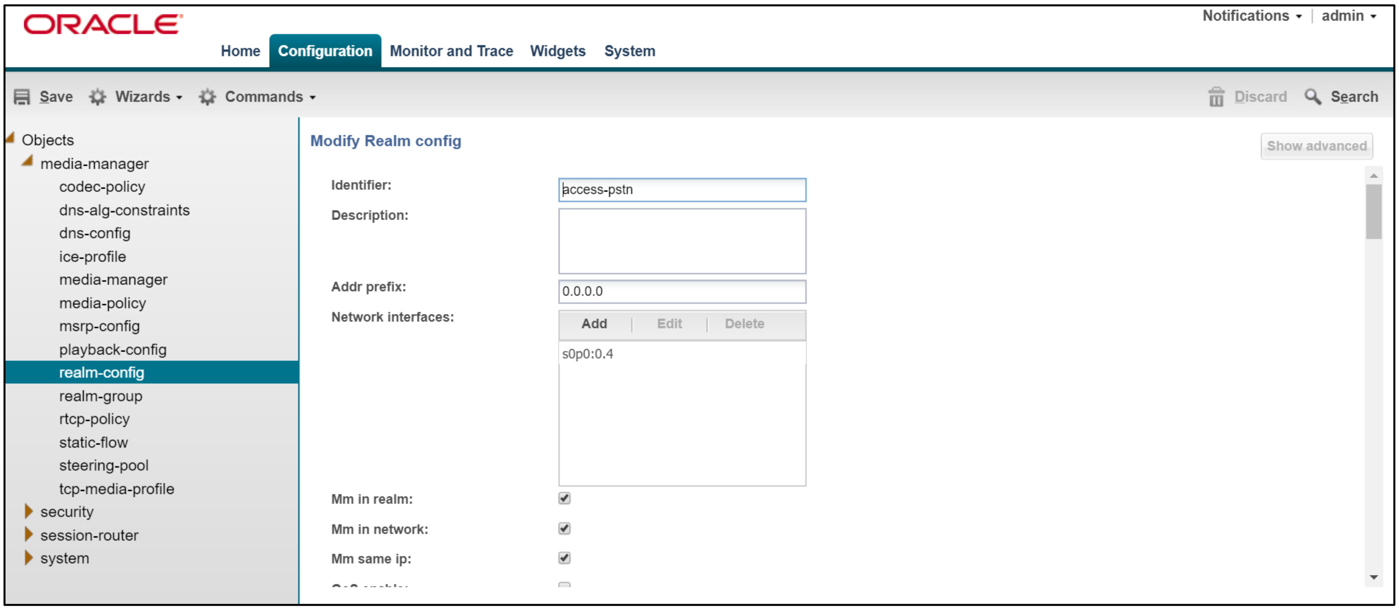
Configure realm for teams as shown below



Modify Realm config

| | |
|---|---|
| Identifier: | access-teams |
| Description: | |
| Addr prefix: | 0.0.0.0 |
| Network interfaces: | s0p0:0.4 |
| Mm in realm: | ☑ |
| Mm in network: | ☑ |
| Mm same ip: | ☑ |

Configure the realm, similarly for SIP Trunk



Modify Realm config

Identifier: access-pstn

Description:

Addr prefix: 0.0.0.0

Network interfaces: s0p0:0.4

Mm in realm: ☑

Mm in network: ☑

Mm same ip: ☑

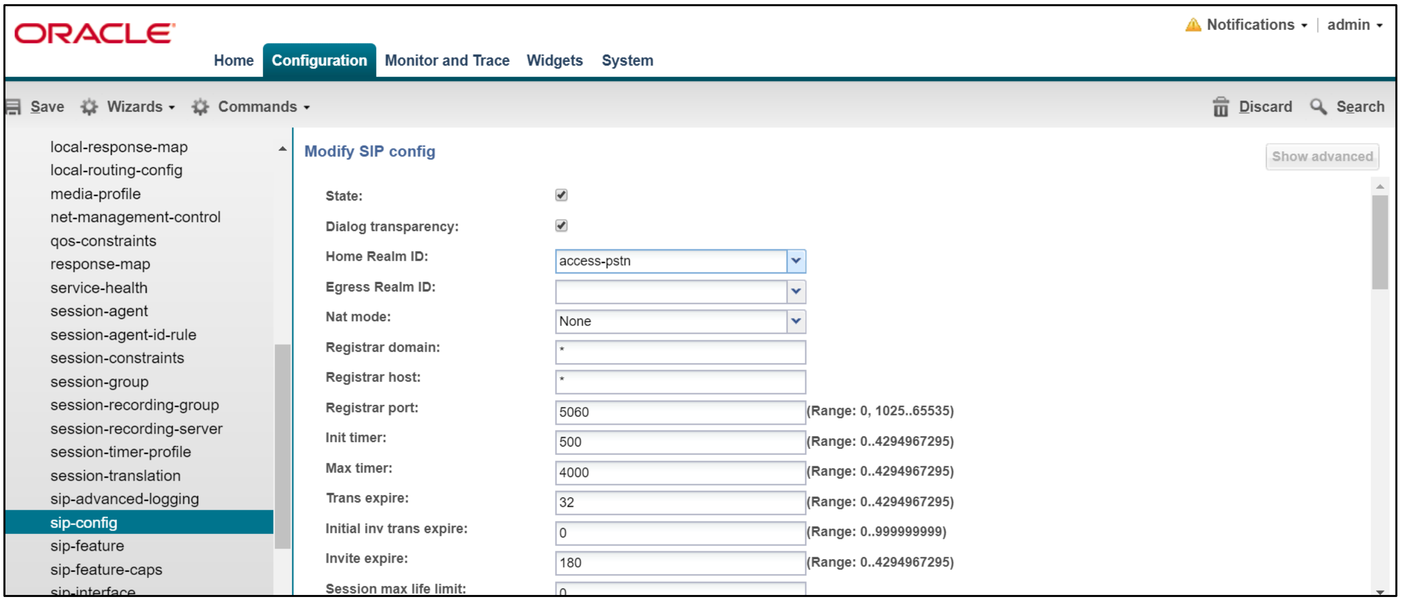
## 5.8 Enable sip-config

SIP config enables SIP handling in the SBC. Make sure the home realm-id, registrar-domain and registrar-host are configured. Also add the options to the sip-config as shown below.

To configure sip-config,

Go to Session-Router->sip-config.

- In options add max-udp-length =0.



Modify SIP config

State: ☑

Dialog transparency: ☑

Home Realm ID: access-pstn

Egress Realm ID:

Nat mode: None

Registrar domain: *

Registrar host: *

Registrar port: 5060 (Range: 0, 1025..65535)

Init timer: 500 (Range: 0..4294967295)

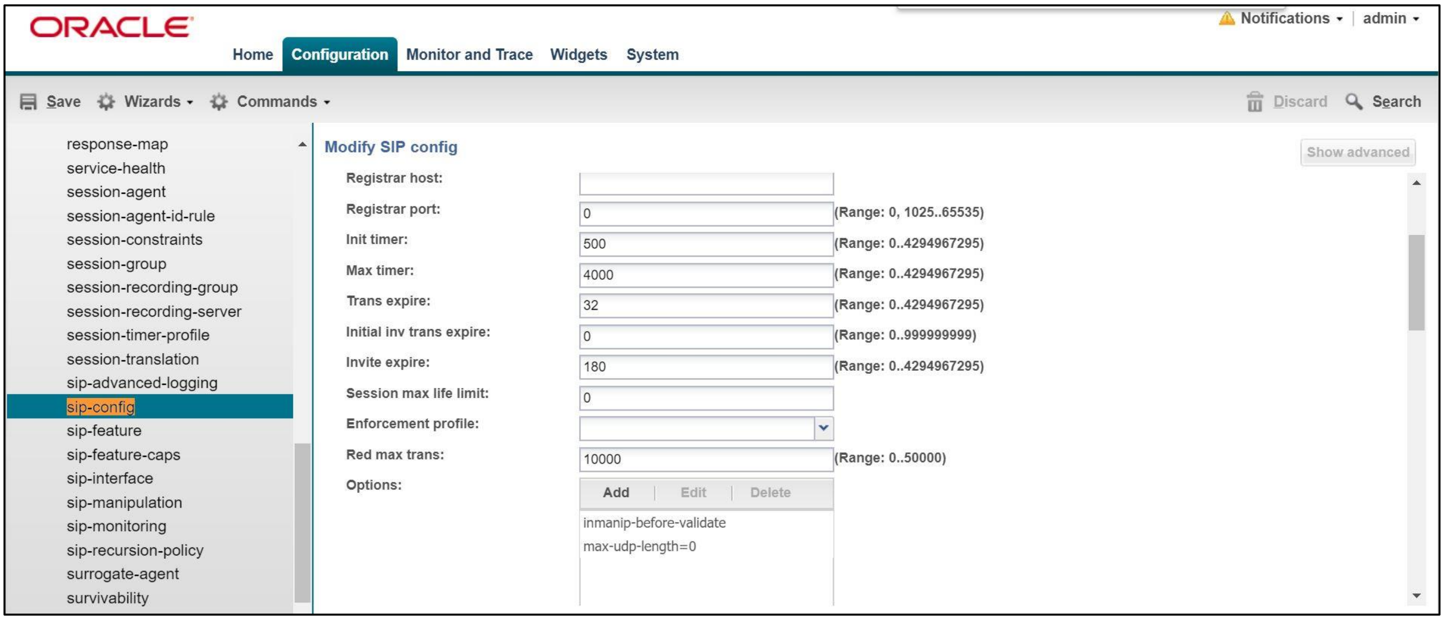
Max timer: 4000 (Range: 0..4294967295)

Trans expire: 32 (Range: 0..4294967295)

Initial inv trans expire: 0 (Range: 0..999999999)

Invite expire: 180 (Range: 0..4294967295)

Session max life limit: 0



Modify SIP config

| | | |
|---|---|---|
| Registrar host: | | |
| Registrar port: | 0 | (Range: 0, 1025..65535) |
| Init timer: | 500 | (Range: 0..4294967295) |
| Max timer: | 4000 | (Range: 0..4294967295) |
| Trans expire: | 32 | (Range: 0..4294967295) |
| Initial inv trans expire: | 0 | (Range: 0..999999999) |
| Invite expire: | 180 | (Range: 0..4294967295) |
| Session max life limit: | 0 | |
| Enforcement profile: | | |
| Red max trans: | 10000 | (Range: 0..50000) |
| Options: | inmanip-before-validate<br>max-udp-length=0 | |

## 5.9 Configuring a certificate for SBC Interface

Microsoft Teams Direct Routing Interface only allows TLS connections from SBCs for SIP traffic with a certificate signed by one of the trusted certification authorities.
The step below describes how to request a certificate for SBC External interface and configure it based on the example of DigiCert. The process includes the following steps:

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

The following certificate-records are required on the Oracle SBC in order for the SBC to connect with Microsoft Teams

- SBC – 1 certificate-record assigned to SBC
- Root – 1 certificate-record for root cert
- Intermediate – 1 certificate-record for intermediate (this is optional – only required if your server certificate is signed by an intermediate)

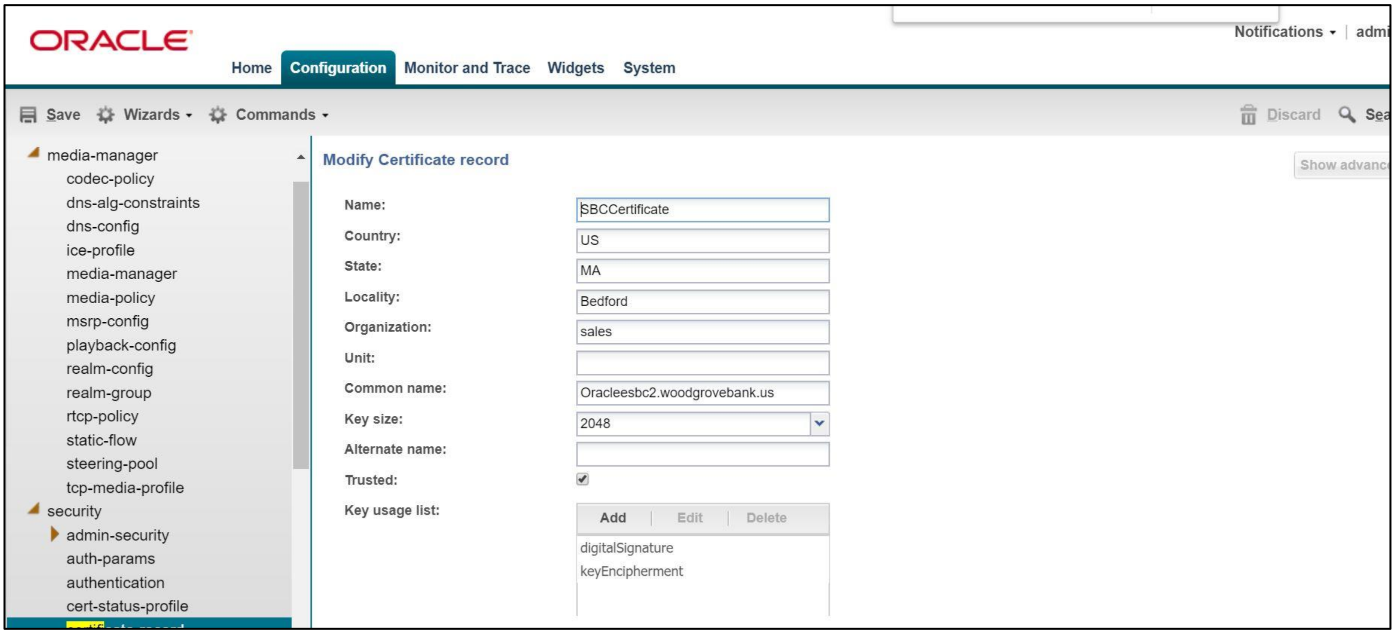
2. Generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority

3. Deploy the SBC and Root/Intermediary certificates on the SBC

## 5.10 SBC Certificate Creation

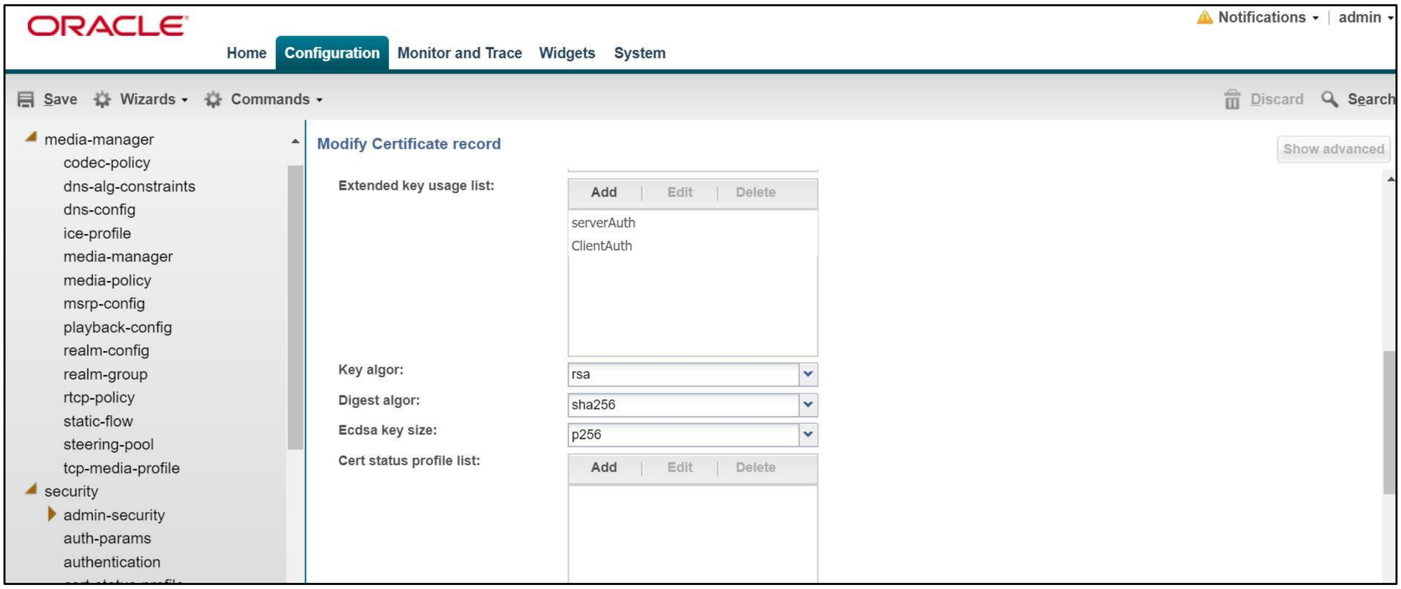
### 5.10.1 Step 1 – Creating the SBC certificate record

Go to security->Certificate Record and configure a certificate for SBC as shown below.



Modify Certificate record

Name: SBCCertificate
Country: US
State: MA
Locality: Bedford
Organization: sales
Unit:
Common name: Oracleesbc2.woodgrovebank.us
Key size: 2048
Alternate name:
Trusted: ☑
Key usage list: digitalSignature, keyEncipherment



Modify Certificate record

Extended key usage list: serverAuth, ClientAuth

Key algor: rsa

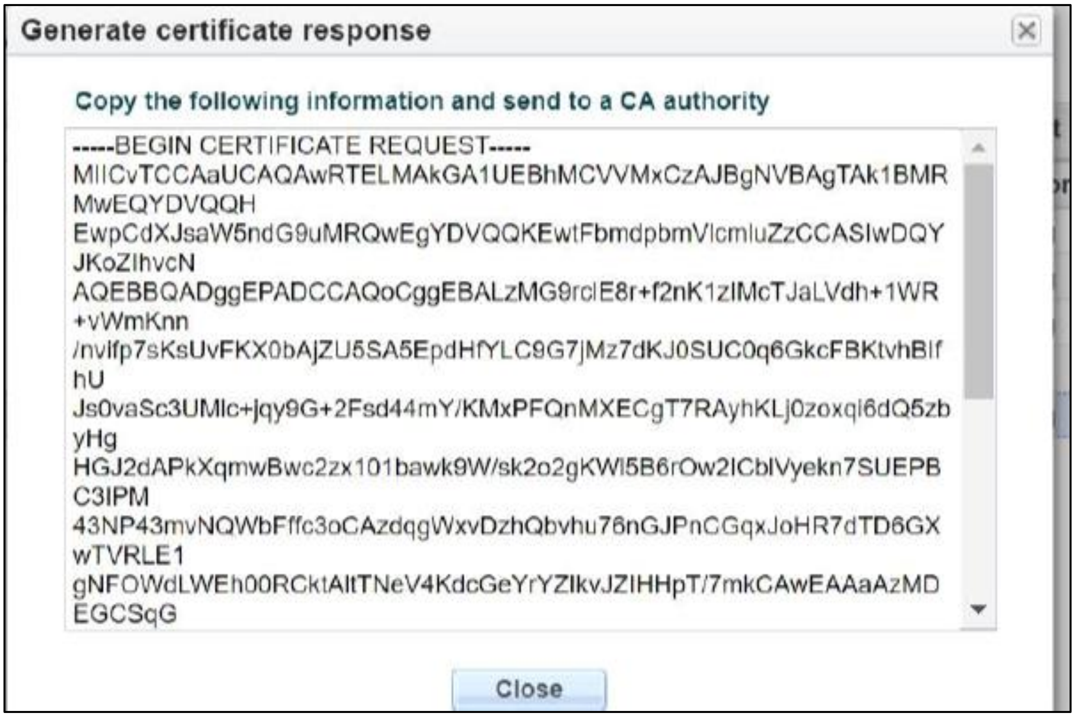
Digest algor: sha256

Ecdsa key size: p256

Cert status profile list:

### 5.10.2 Step 2 – Generating a certificate signing request for SBC certificate

- Select the certificate and generate certificate on clicking the "Generate" command.
- Please copy/paste the text that gets printed on the screen as shown below and upload to your CA server for signature.



Generate certificate response

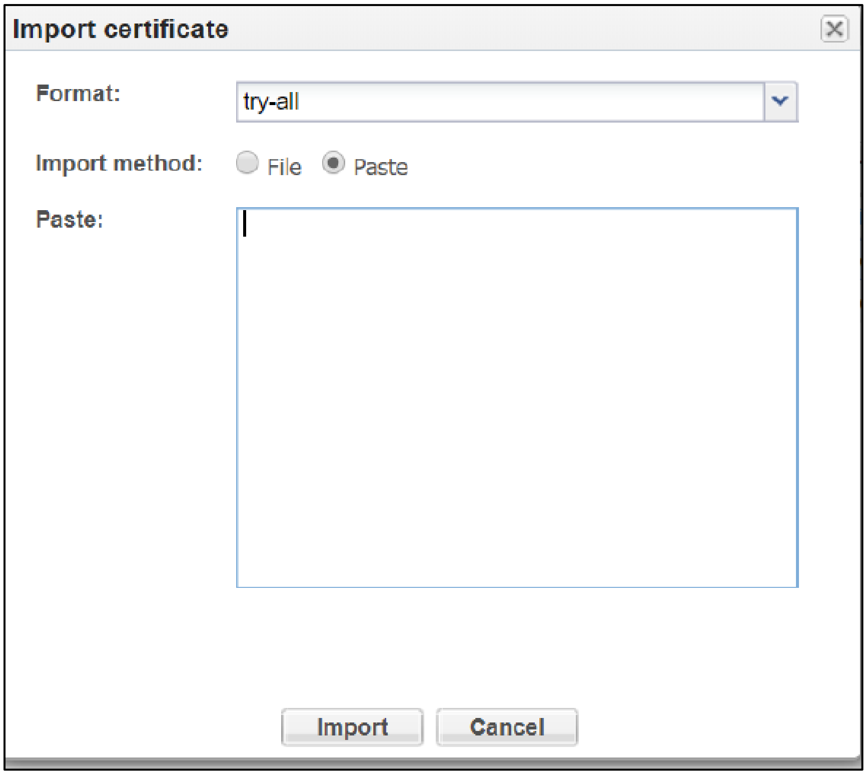
Copy the following information and send to a CA authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvTCCAaUCAQAwRTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1BMR
MwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzCCASIwDQY
JKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALzMG9rclE8r+f2nK1zIMcTJaLVdh+1WR
+vWmKnn
/nvlfp7sKsUvFKX0bAjZU5SA5EpdHfYLC9G7jMz7dKJ0SUC0q6GkcFBKtvhBIf
hU
Js0vaSc3UMIc+jqy9G+2Fsd44mY/KMxPFQnMXECgT7RAyhKLj0zoxqI6dQ5zb
yHg
HGJ2dAPkXqmwBwc2zx101bawk9W/sk2o2gKWI5B6rOw2ICblVyekn7SUEPB
C3IPM
43NP43mvNQWbFffc3oCAzdqgWxvDzhQbvhu76nGJPnCGqxJoHR7dTD6GX
wTVRLE1
gNFOWdLWEh00RCktAltTNeV4KdcGeYrYZIkvJZIHHpT/7mkCAwEAAaAzMD
EGCSqG
```

*Also, note that a save/activate is required*

### 5.10.3 Step 3 – Deploy the SBC certificate

Once certificate signing requests have been completed – import the signed certificate to the SBC.
Copy paste the certificate.
Once done, issue save/activate from the WebGUI



Import certificate

Format: try-all

Import method: ○ File ● Paste

Paste:

## 5.11 Root and Intermediate Certificates Creation

There are 3 more certificates that are required for direct routing.

-BaltimoreRoot: This certificate is always required for MS Teams.
This certificate can be downloaded from https://cacert.omniroot.com/bc2025.pem
The serial number of this certificate is 0x20000b9.
*Note :The certificate should be in .pem format.*

-DigiCertRoot

-DigiCertInter

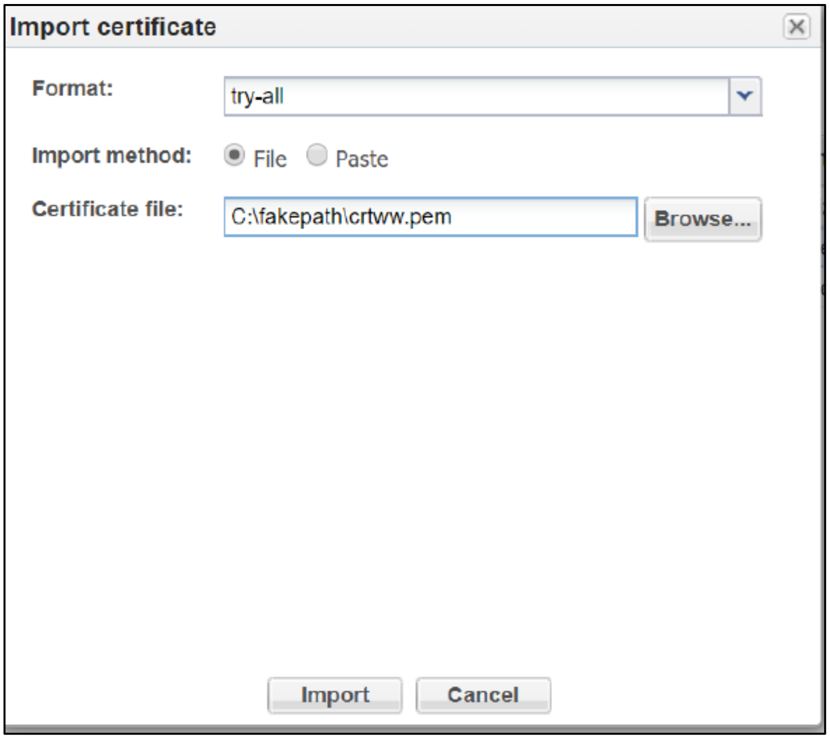
### 5.11.1 Step 1 - Creating the root and intermediate certificates on SBC

Go to security->Certificate Record and create the certificate with parameters as shown. . Modify the configuration according to the certificates in your environment.

| Parameter | DigicertInter | BaltimoreRoot | DigiCertRoot |
|---|---|---|---|
| Common-name | DigiCert SHA2 Secure Server CA | Baltimore CyberTrust Root | DigiCert Global Root CA |
| Key-size | 2048 | 2048 | 2048 |
| Key-usage-list | digitalSignature<br>keyEncipherment | digitalSignature<br>keyEncipherment | digitalSignature<br>keyEncipherment |
| Extended-key-usage-list | serverAuth | serverAuth | serverAuth |
| key-algor | rsa | rsa | rsa |
| digest-algor | sha256 | sha256 | sha256 |

### 5.11.2 Step 2 - Deploying the Root and Intermediate certificates on SBC

All the root and intermediate certificates have to imported to SBC.
The root and intermediate certificates can be imported into the SBC only in the .pem format.
Note: The BaltimoreRoot certificate downloaded in Step1 can be directly imported as shown.
Click on the certificate and select Import.
The below screen appears. Make sure your file is in .pem format and upload.



Import certificate

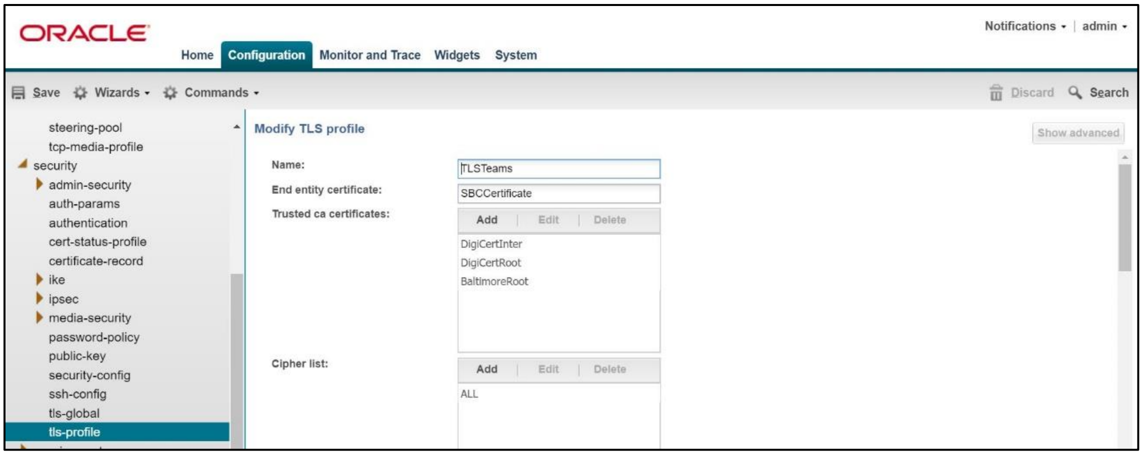
Format: try-all

Import method: ● File ○ Paste

Certificate file: C:\fakepath\crtww.pem

## 5.12 TLS-Profile

A TLS profile configuration on the SBC allows for specific certificates to be assigned. Go to security-> TLS-profile config element and configure the tls-profile as shown below



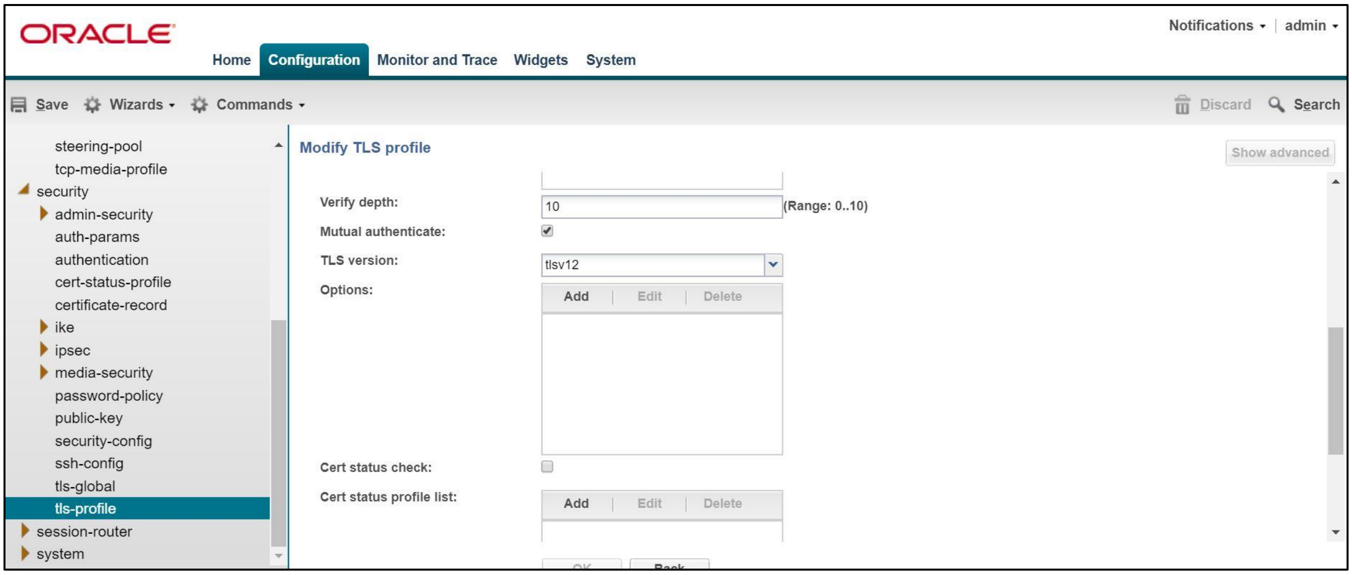
Modify TLS profile

Name: TLSTeams

End entity certificate: SBCCertificate

Trusted ca certificates:
DigiCertInter
DigiCertRoot
BaltimoreRoot

Cipher list:
ALL



Modify TLS profile

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

Mutual authenticate: ☑

TLS version: tlsv12

Options:

Cert status check: □

Cert status profile list:

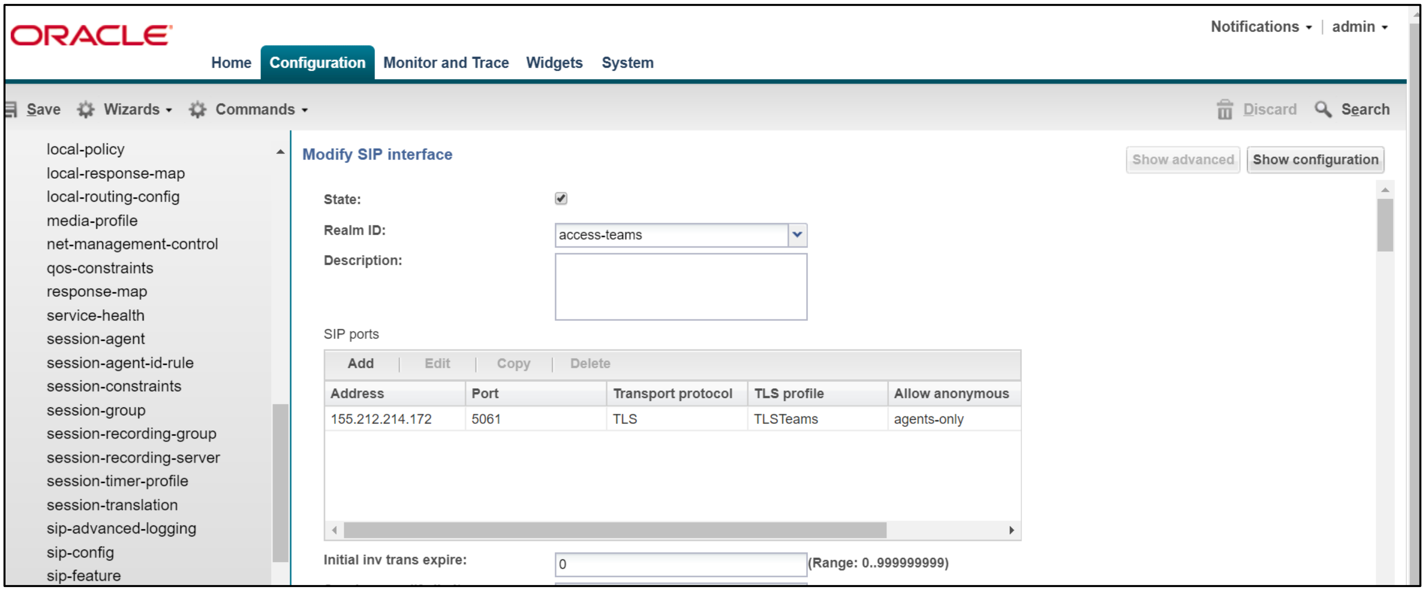
## 5.13 Creating a sip-interface to communicate with Microsoft Teams

Set the following configuration elements – ensure that the IP address allocated to the SIP interface is the FQDN resolvable address. i.e. if you issue command nslookup from another computer, “oracleesbc2.woodgrovebank.us” – it should resolve to 155.212.214.172.

Note that the IP should be publicly routable IP address. To configure sip-interface, Go to Session-Router->Sip-Interface.

Note:

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



Modify SIP interface

State: ☑

Realm ID: access-teams

Description:

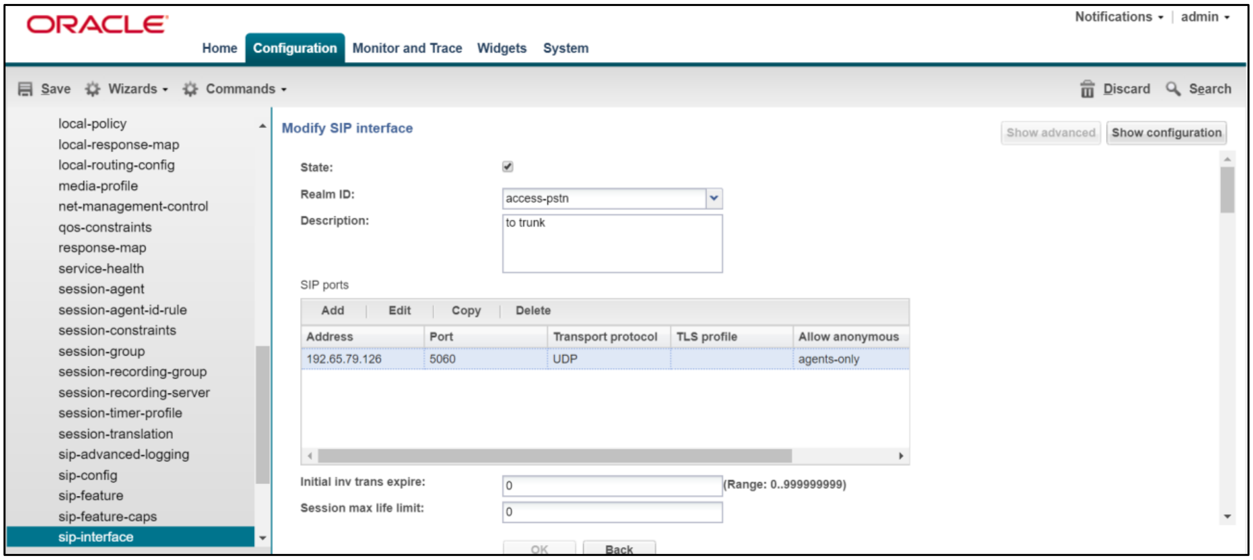
SIP ports

| Address | Port | Transport protocol | TLS profile | Allow anonymous |
|---|---|---|---|---|
| 155.212.214.172 | 5061 | TLS | TLSTeams | agents-only |

Initial inv trans expire: 0 (Range: 0..999999999)

## 5.14 Configure sip-interface to communicate with SIP Trunk

Similarly configure the sip-interface for sip-trunk, according to your environment.



Modify SIP interface

State: ☑

Realm ID: access-pstn

Description: to trunk

SIP ports

| Address | Port | Transport protocol | TLS profile | Allow anonymous |
|---|---|---|---|---|
| 192.65.79.126 | 5060 | UDP | | agents-only |

Initial inv trans expire: 0 (Range: 0..999999999)

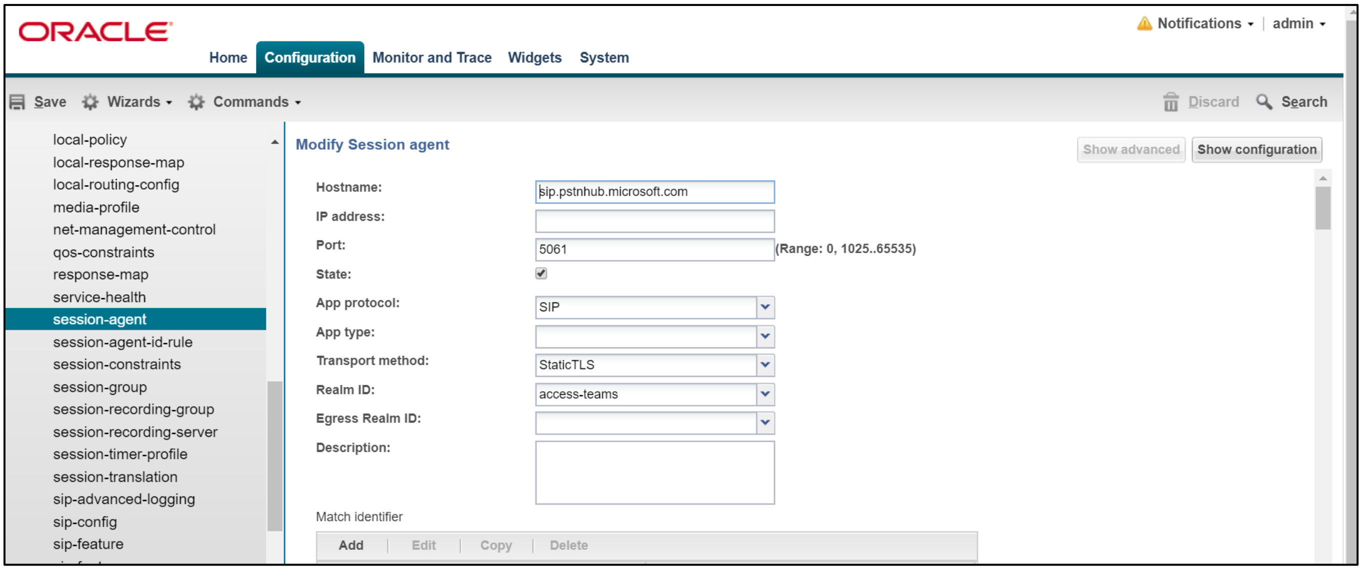
Session max life limit: 0

Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address. Now configure where the SBC sends the outbound traffic.

## 5.15 Configure session-agent

Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. Configure the session-agent for Teams with the following parameters. Go to session-router->Session-Agent.

- hostname to “sip.pstnhub.microsoft.com”
- port 5061
- realm-id – needs to match the realm created for teams – in this case – “Access-teams”
- transport set to “StaticTLS”
- refer-call-transfer set to enabled
- ping-method – send OPTIONS message to Microsoft to check health
- ping-interval to 30 secs



Modify Session agent

Hostname: sip.pstnhub.microsoft.com

IP address:

Port: 5061 (Range: 0, 1025..65535)

State: ☑

App protocol: SIP

App type:

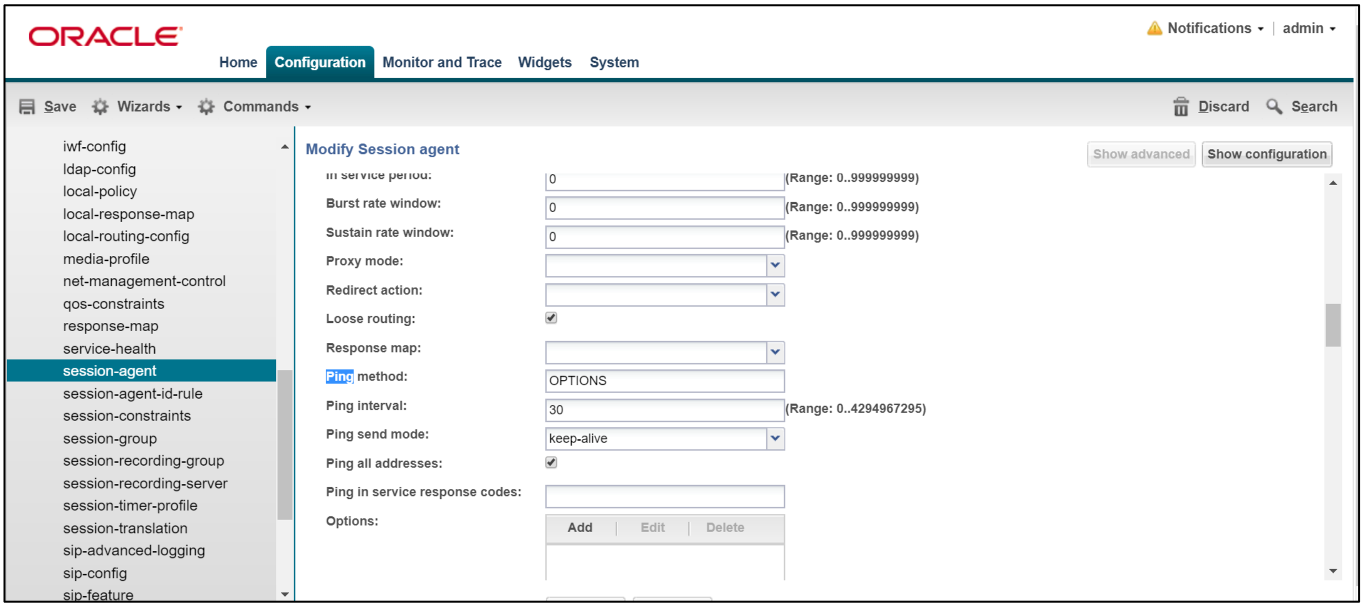
Transport method: StaticTLS

Realm ID: access-teams

Egress Realm ID:

Description:

Match identifier



Modify Session agent

In service period: 0 (Range: 0..999999999)

Burst rate window: 0 (Range: 0..999999999)

Sustain rate window: 0 (Range: 0..999999999)

Proxy mode:

Redirect action:

Loose routing: ☑

Response map:

Ping method: OPTIONS

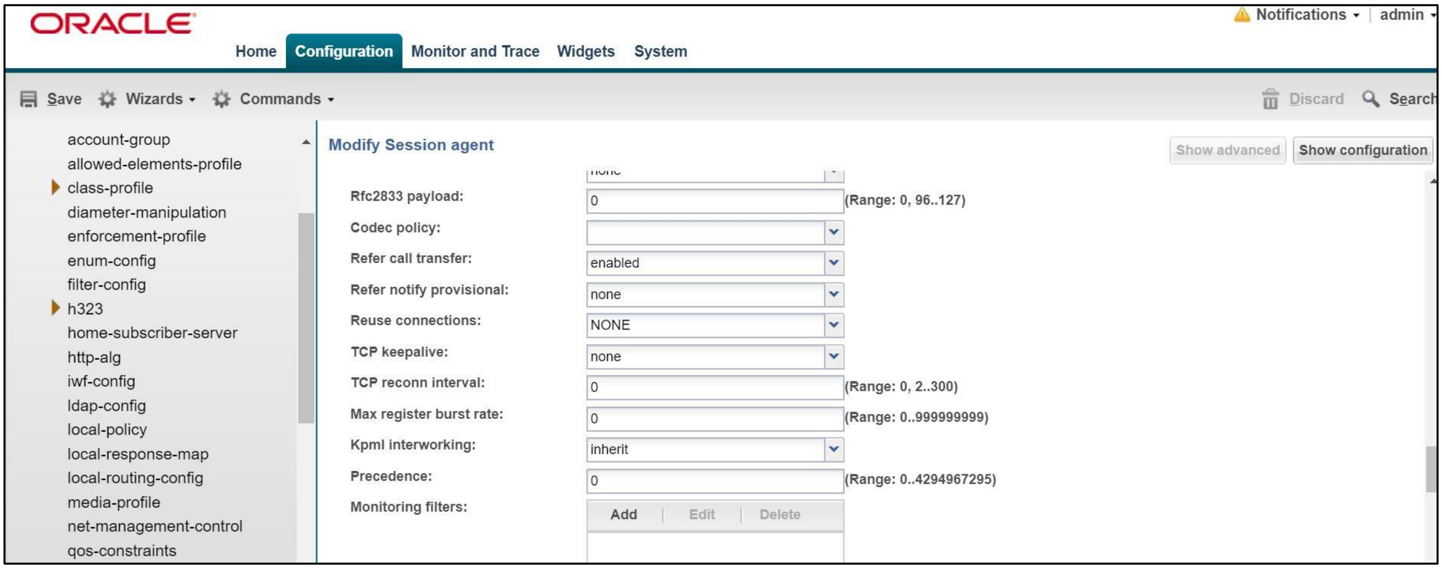
Ping interval: 30 (Range: 0..4294967295)

Ping send mode: keep-alive

Ping all addresses: ☑

Ping in service response codes:

Options:



- account-group
- allowed-elements-profile
- class-profile
- diameter-manipulation
- enforcement-profile
- 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

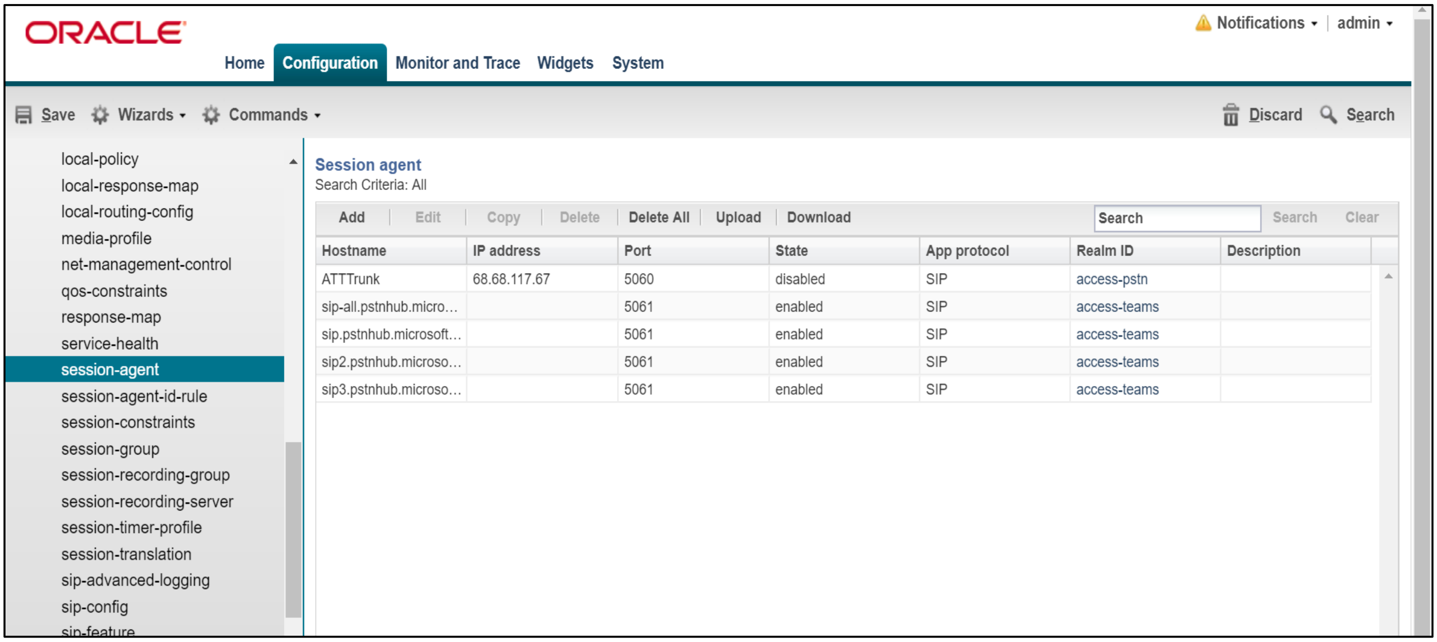
**Modify Session agent**

| | | |
|---|---|---|
| Rfc2833 payload: | 0 | (Range: 0, 96..127) |
| Codec policy: | | |
| Refer call transfer: | enabled | |
| Refer notify provisional: | none | |
| Reuse connections: | NONE | |
| TCP keepalive: | none | |
| TCP reconn interval: | 0 | (Range: 0, 2..300) |
| Max register burst rate: | 0 | (Range: 0..999999999) |
| Kpml interworking: | inherit | |
| Precedence: | 0 | (Range: 0..4294967295) |
| Monitoring filters: | Add Edit Delete | |

Follow above steps to create 2 more sessions for:

- sip2.pstnhub.microsoft.com
- sip3.pstnhub.microsoft.com
- sip-all.pstnhub.microsoft.com

*Note: Please note that all signaling SHOULD only point to sip/sip2/sip3.pstnhub.microsoft.com – no signaling shoulbe sent to sip-all.pstnhub.microsoft.com FQDN. The sip-all.pstnhub.microsoft.com FQDN is only used for longer DNS TTL value*



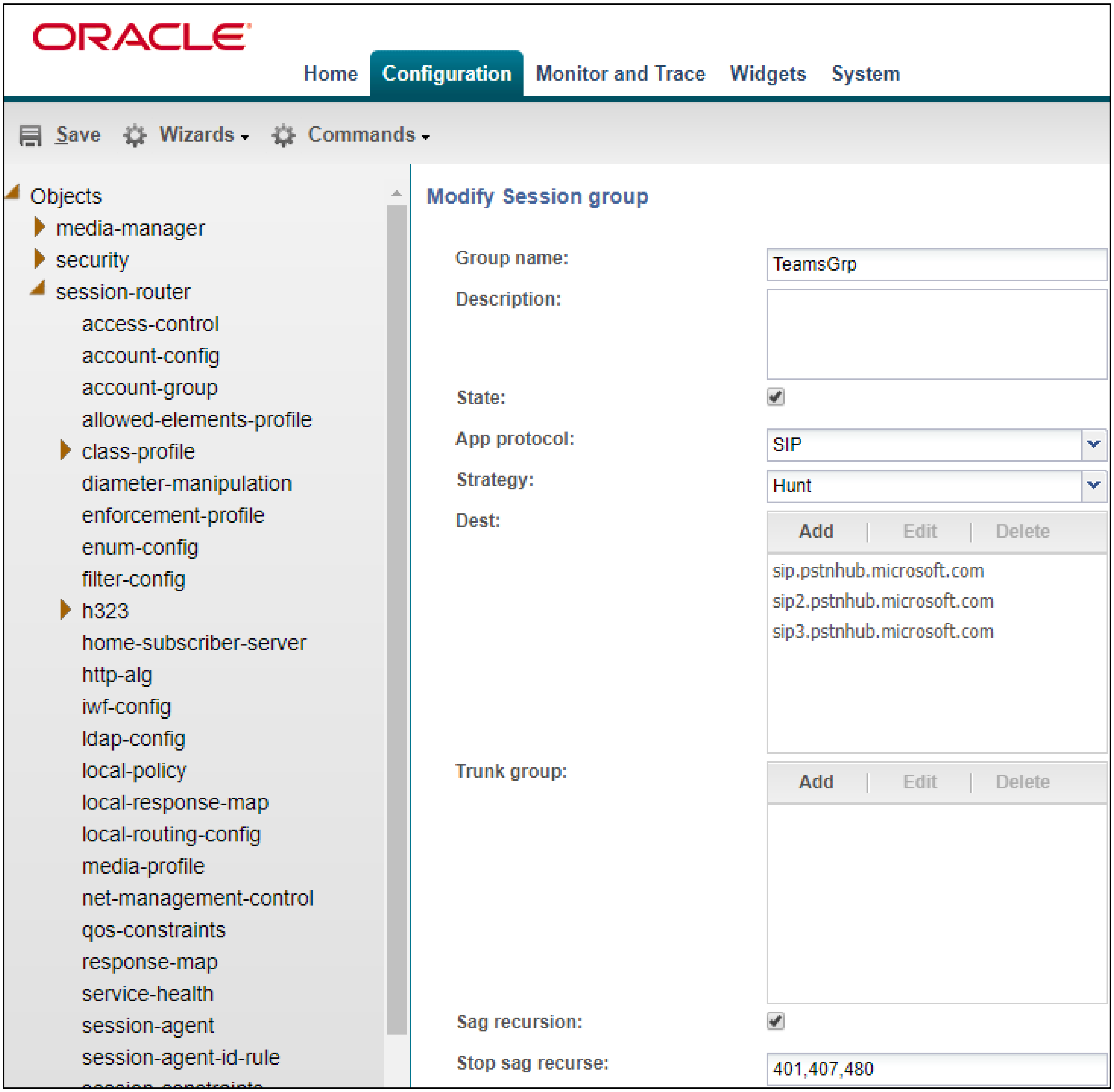
- local-policy
- local-response-map
- local-routing-config
- media-profile
- net-management-control
- qos-constraints
- response-map
- service-health
- session-agent
- session-agent-id-rule
- session-constraints
- session-group
- session-recording-group
- session-recording-server
- session-timer-profile
- session-translation
- sip-advanced-logging
- sip-config
- sip-feature

**Session agent**
Search Criteria: All

| Hostname | IP address | Port | State | App protocol | Realm ID | Description |
|---|---|---|---|---|---|---|
| ATTTrunk | 68.68.117.67 | 5060 | disabled | SIP | access-pstn | |
| sip-all.pstnhub.micro… | | 5061 | enabled | SIP | access-teams | |
| sip.pstnhub.microsoft… | | 5061 | enabled | SIP | access-teams | |
| sip2.pstnhub.microso… | | 5061 | enabled | SIP | access-teams | |
| sip3.pstnhub.microso… | | 5061 | enabled | SIP | access-teams | |

## 5.16 Create a Session Agent Group

A session agent group allows the SBC to create a load balancing model. Go to Session-Router->Session-Group.



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

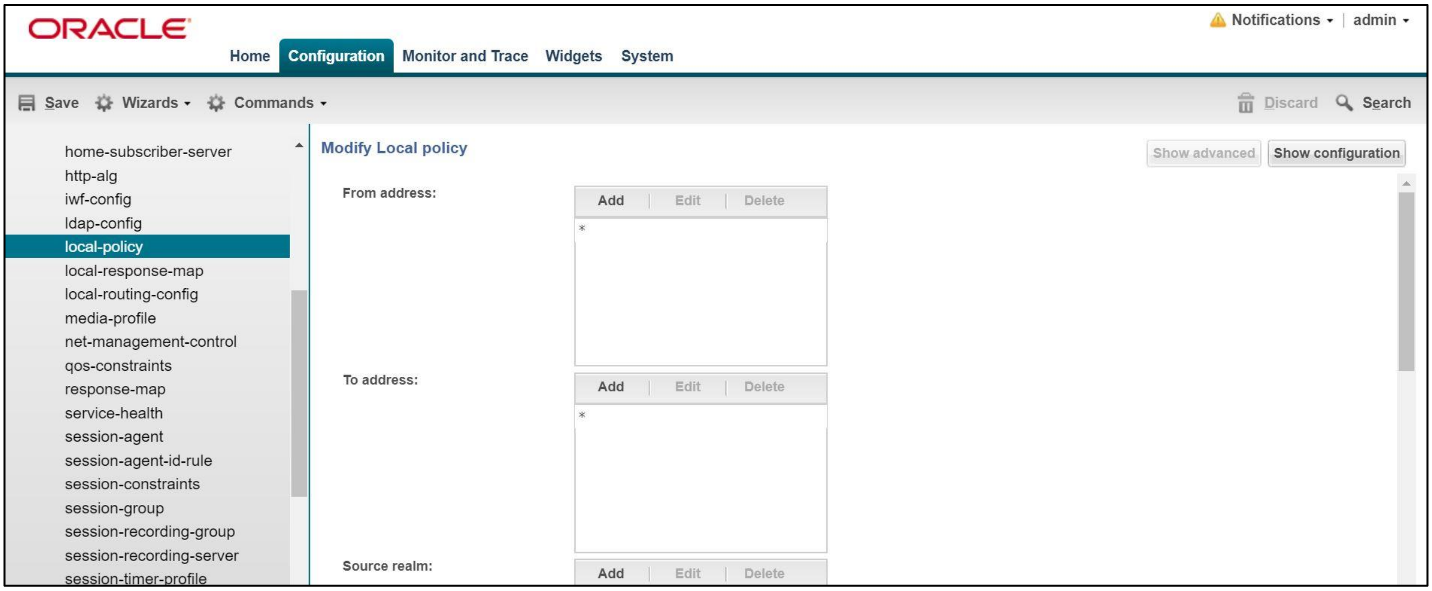
Trunk group:

Sag recursion: ☑

Stop sag recurse: 401,407,480

## 5.17 Configure local-policy

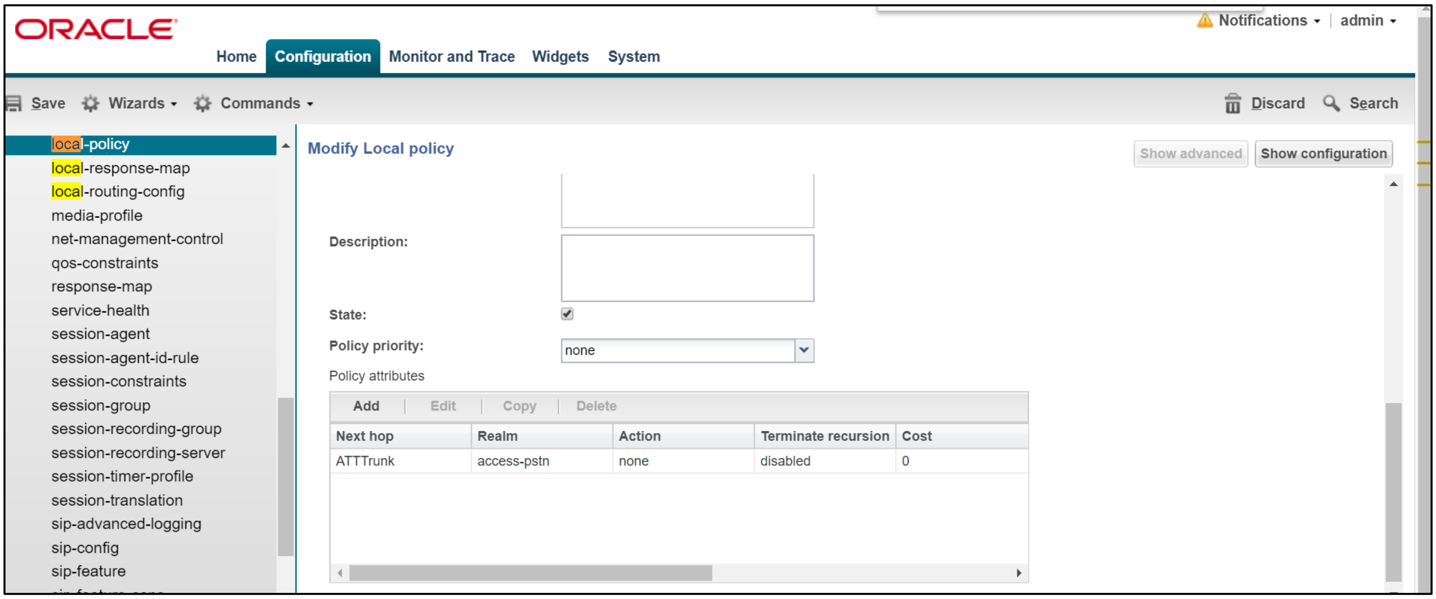
Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria.to configure local-policy, go to Session-Router->local-policy. In order for inbound calls from Teams to be routed to a SIP Trunk following config is required:



From address: *

To address: *

Source realm:



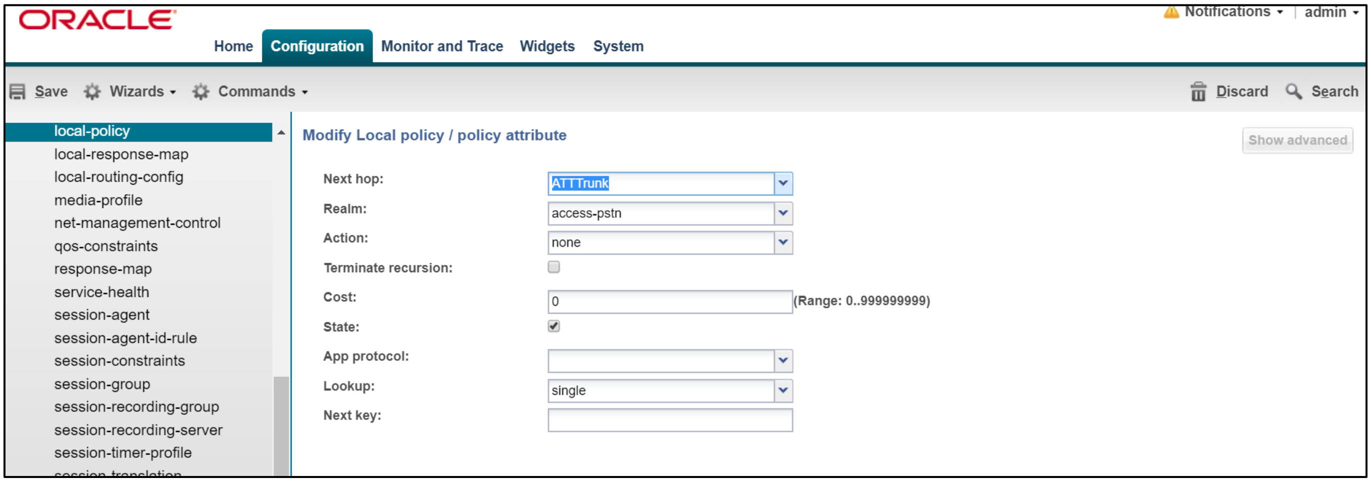
Description:

State: ☑

Policy priority: none

Policy attributes

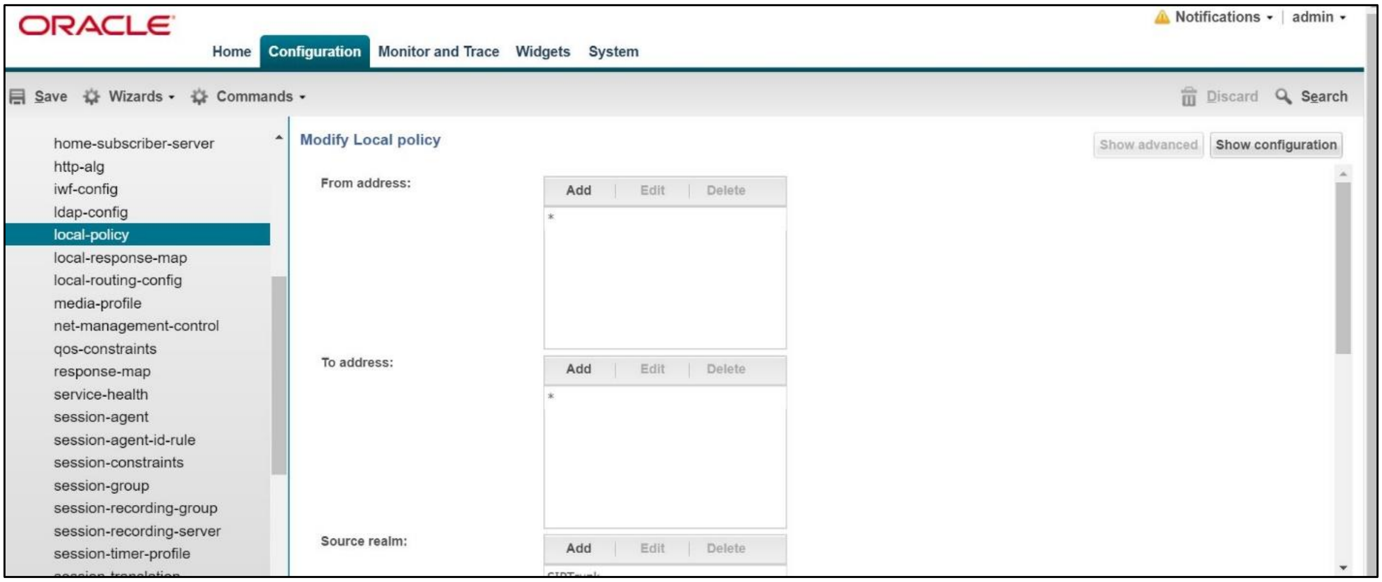
| Next hop | Realm | Action | Terminate recursion | Cost |
|---|---|---|---|---|
| ATTTrunk | access-pstn | none | disabled | 0 |



Modify Local policy / policy attribute

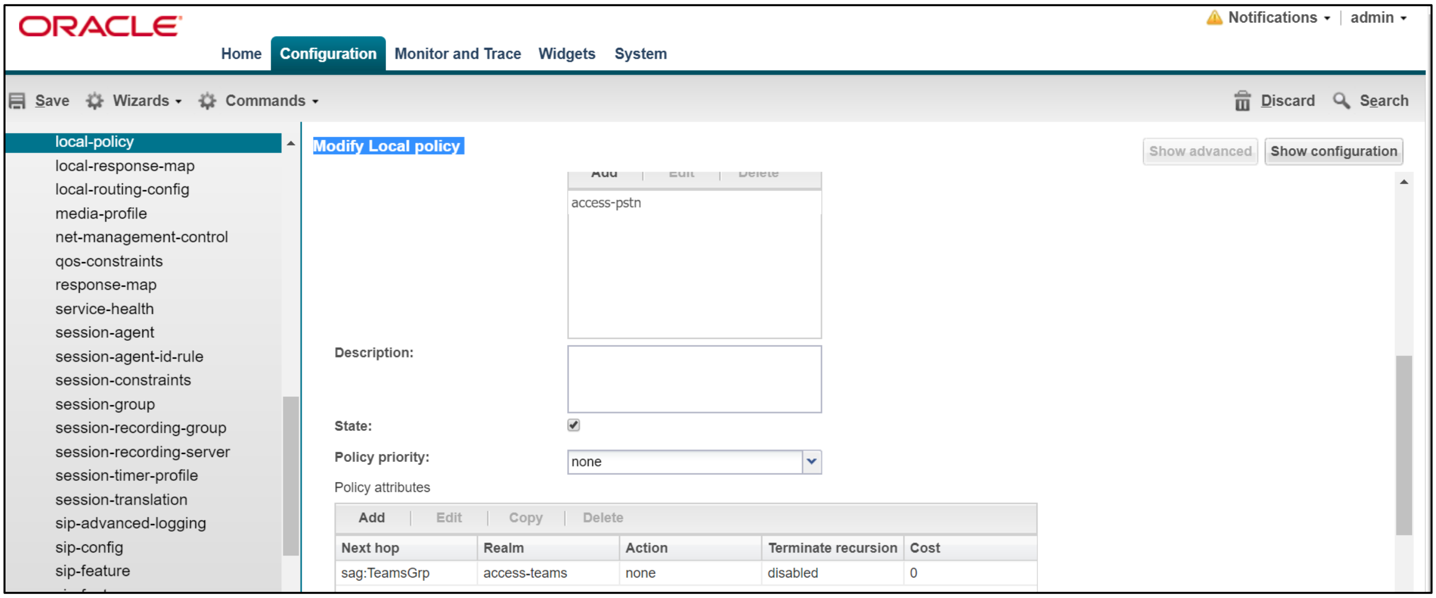
| | |
|---|---|
| Next hop: | ATTTrunk |
| Realm: | access-pstn |
| Action: | none |
| Terminate recursion: | ☐ |
| Cost: | 0 (Range: 0..999999999) |
| State: | ☑ |
| App protocol: | |
| Lookup: | single |
| Next key: | |

The above local policy config is allowing any DID from teams that lands on the SBC to be routed to ATT Trunk via realm access-pstn, where the next hop is the IP address of the ATT Trunk.
A second local policy is required to be configured to route outbound calls to Teams from access-pstn, configure it as follows:



Modify Local policy

| | |
|---|---|
| From address: | * |
| To address: | * |
| Source realm: | |



Modify Local policy

access-pstn

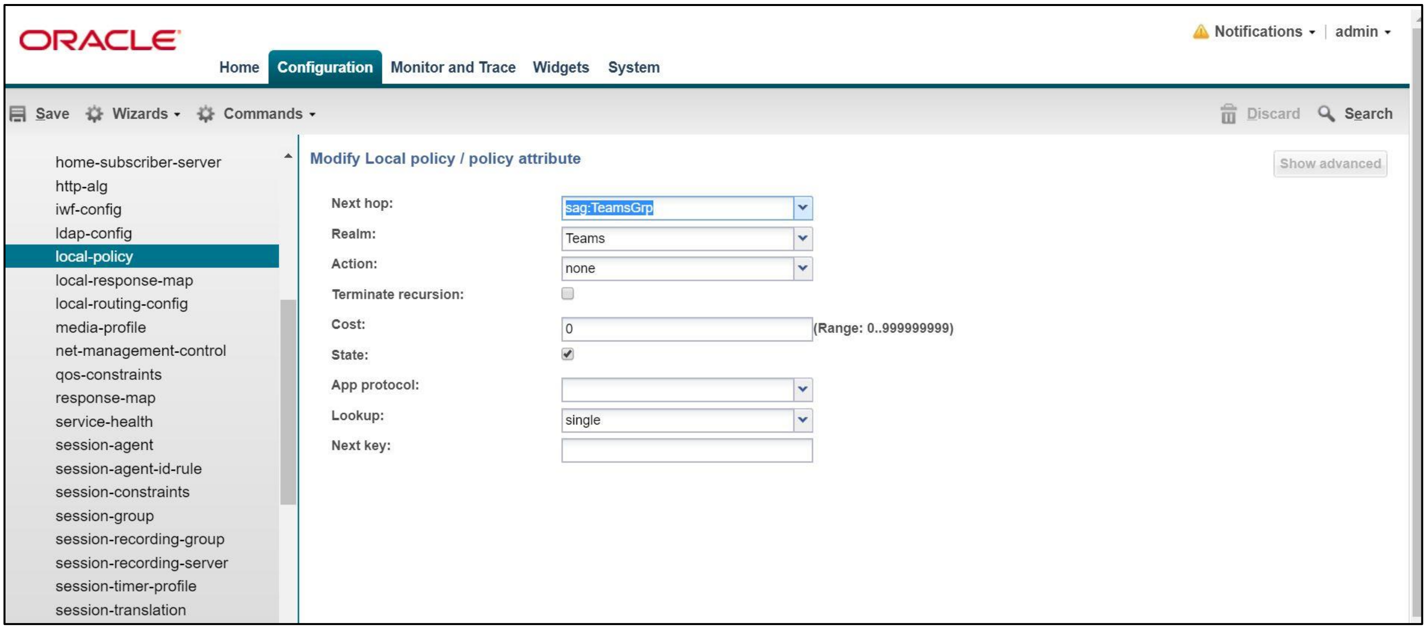
Description:

State: ☑

Policy priority: none

Policy attributes

| Next hop | Realm | Action | Terminate recursion | Cost |
|---|---|---|---|---|
| sag:TeamsGrp | access-teams | none | disabled | 0 |



Modify Local policy / policy attribute

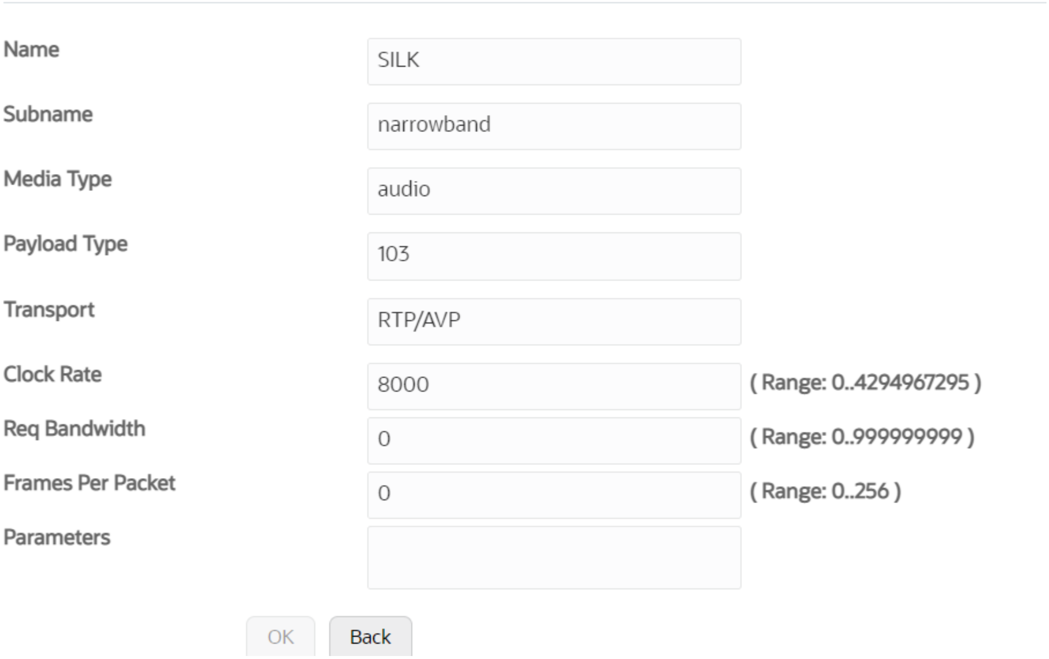
| | |
|---|---|
| Next hop: | sag:TeamsGrp |
| Realm: | Teams |
| Action: | none |
| Terminate recursion: | ☐ |
| Cost: | 0 (Range: 0..999999999) |
| State: | ☑ |
| App protocol: | |
| Lookup: | single |
| Next key: | |

The above local policy will route calls from Access-pstn to access-teams if they match the routing criteria.

## 5.18 Configure Media Profile & Codec Policy

The Oracle® Session Border Controller (SBC) uses codec policies to describe how to manipulate SDP messages as they cross the SBC. The SBC bases its decision to transcode a call on codec policy configuration and the SDP. Each codec policy specifies a set of rules to be used for determining what codecs are retained, removed, and how they are ordered within SDP.

Note: this is an optional config – configure codec policy only if deemed required
Some SIP trunks may have issues with the codecs being offered by Microsoft teams, so following codec policy may be required in order for the calls to work flawlessly.
SILK offered by Microsoft teams is using a payload type which is different than usual. Configure the media-profile as shown below, go to Session-Router->Media-profile

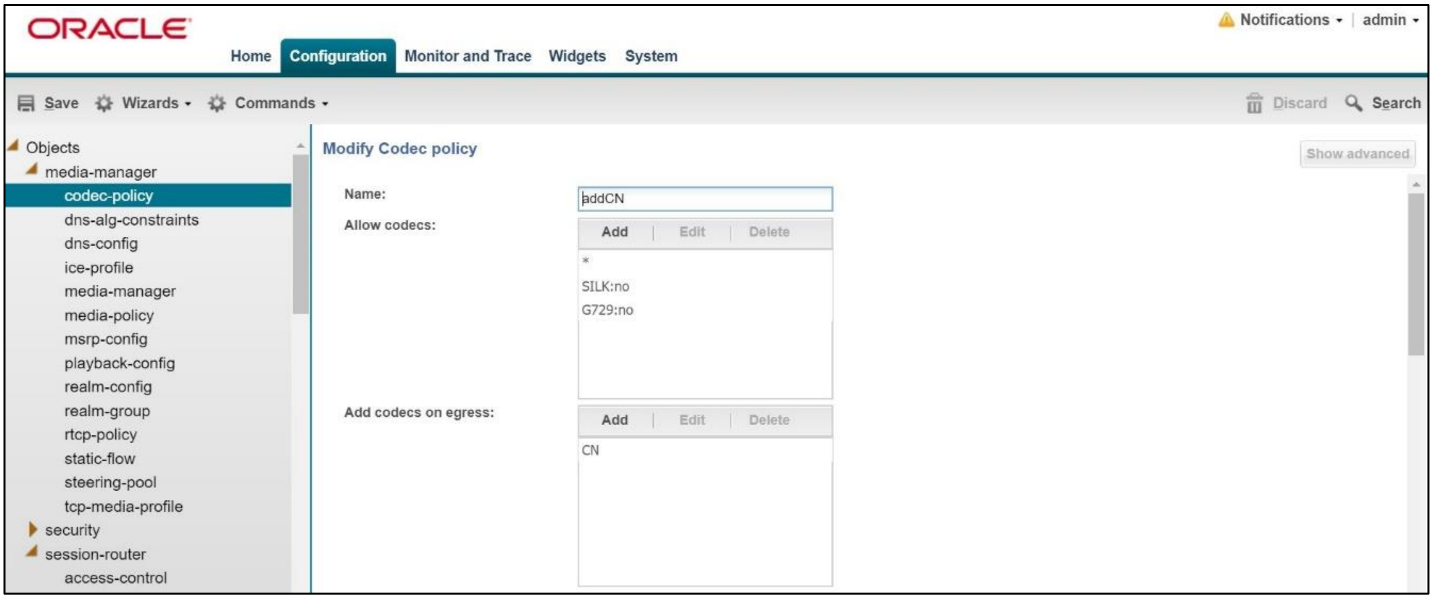


| | | |
|---|---|---|
| Name | SILK | |
| Subname | narrowband | |
| Media Type | audio | |
| Payload Type | 103 | |
| Transport | RTP/AVP | |
| Clock Rate | 8000 | ( Range: 0..4294967295 ) |
| Req Bandwidth | 0 | ( Range: 0..999999999 ) |
| Frames Per Packet | 0 | ( Range: 0..256 ) |
| Parameters | | |

Configure media profiles for SILK codec like shown below

| Parameters | SILK-1 | SILK-2 |
|---|---|---|
| Subname | narrowband | wideband |
| Payload-Type | 103 | 104 |
| Clock-rate | 8000 | 16000 |

Create a codec-policy addCN, to add comfort noise towards Teams and apply it on the realm for Teams, Access-teams.



Modify Codec policy

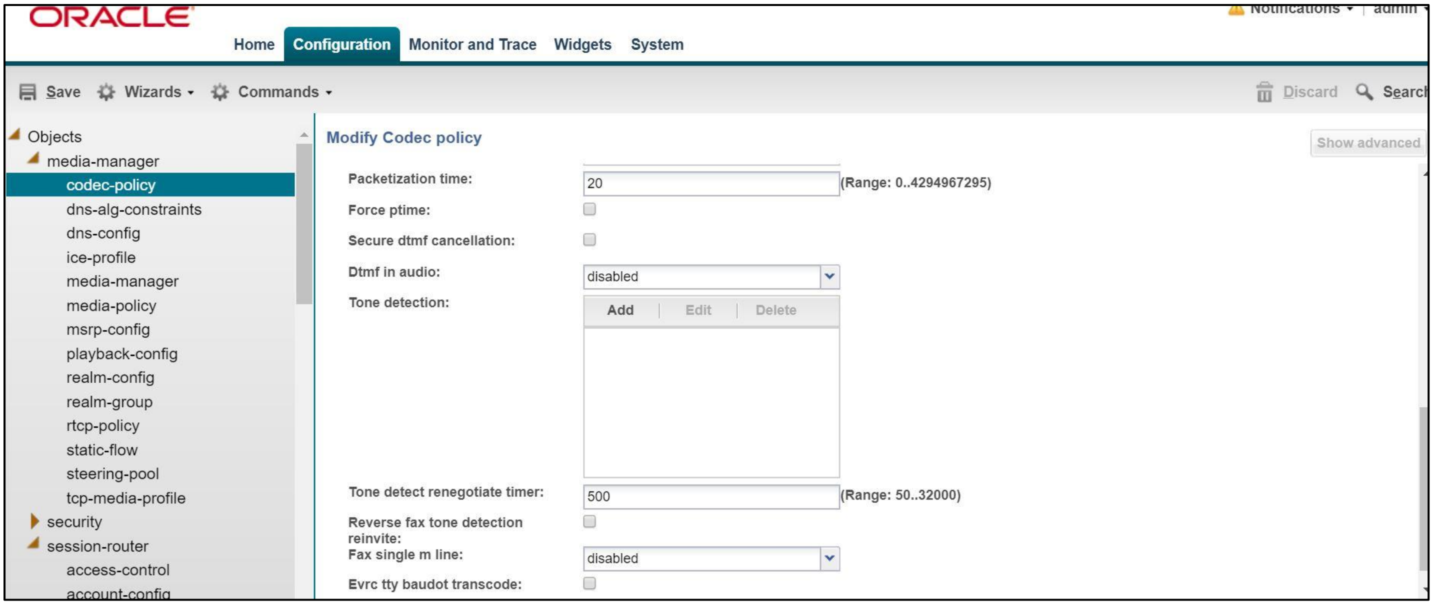
Name: addCN

Allow codecs:

*
SILK:no
G729:no

Add codecs on egress:

CN



Modify Codec policy

Packetization time: 20 (Range: 0..4294967295)

Force ptime: □

Secure dtmf cancellation: □

Dtmf in audio: disabled

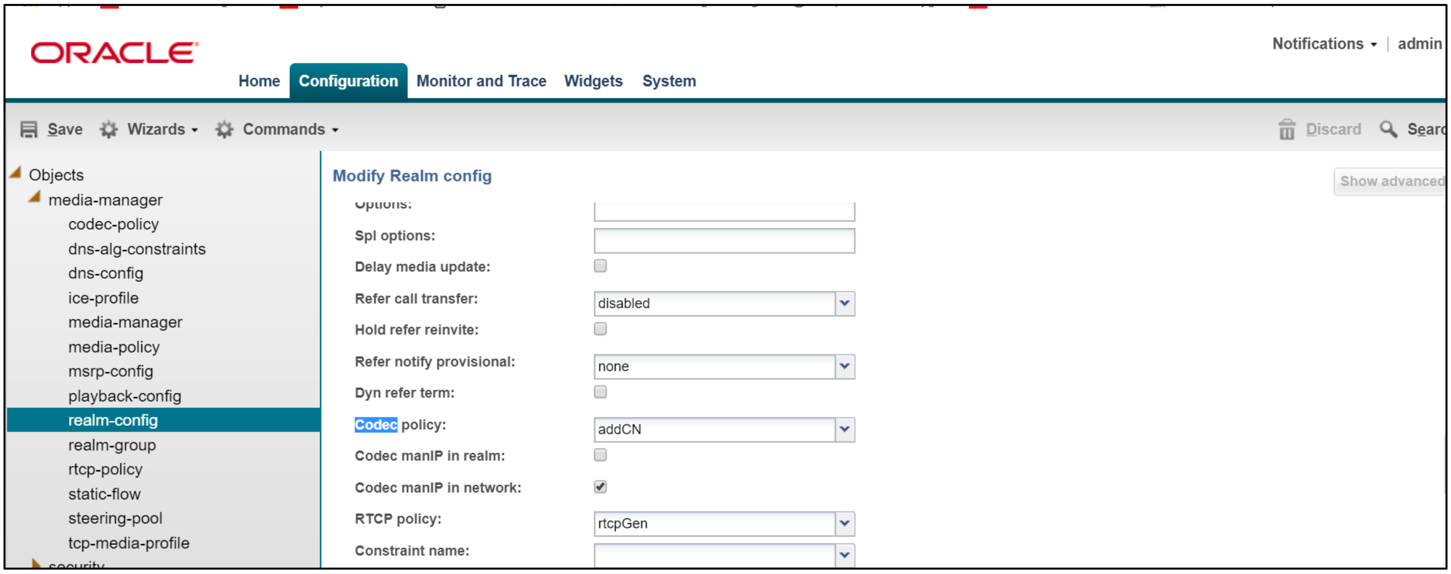
Tone detection:

Tone detect renegotiate timer: 500 (Range: 50..32000)

Reverse fax tone detection reinvite: □

Fax single m line: disabled

Evrc tty baudot transcode: □



Modify Realm config

Options:

Spl options:

Delay media update: □

Refer call transfer: disabled

Hold refer reinvite: □

Refer notify provisional: none

Dyn refer term: □

Codec policy: addCN

Codec manIP in realm: □

Codec manIP in network: ☑

RTCP policy: rtcpGen

Constraint name:

## 5.19 Configure sip-manipulations

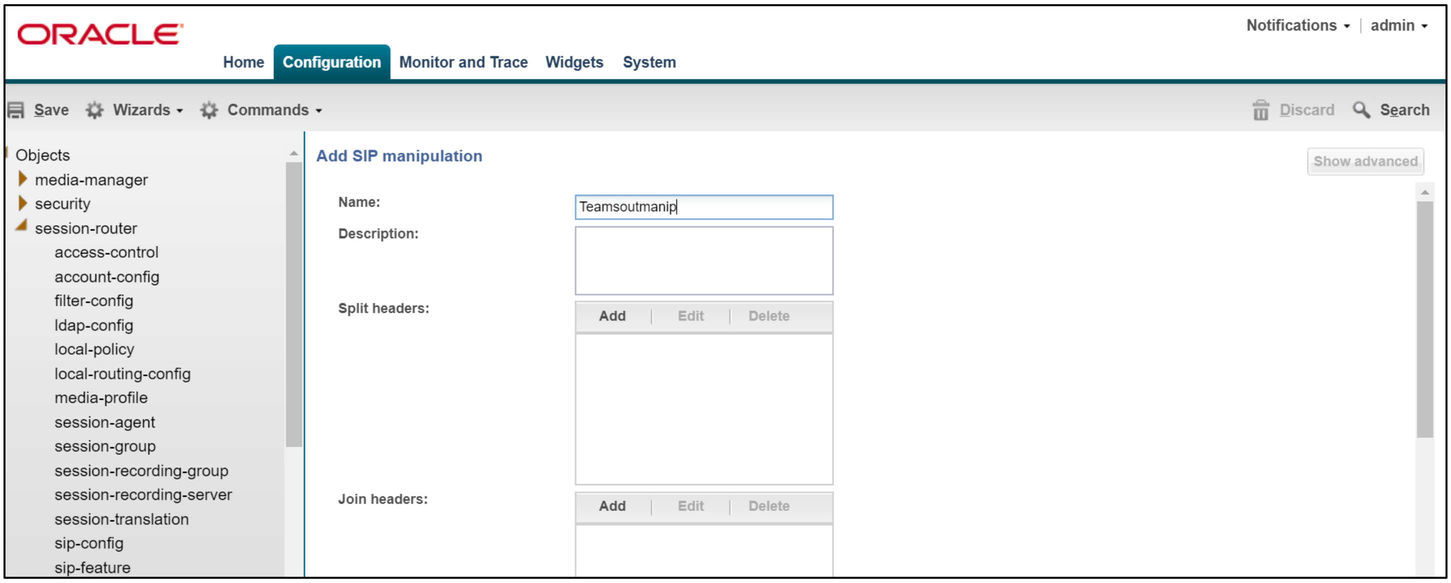
## 5.20 Teamsoutmanip

In order for calls to be presented to Microsoft teams or SIP trunk from the SBC – the SBC would require alterations to the SIP signaling natively created. Following are manipulations required on the SBC in order for to present signaling to Microsoft Teams:

- Countrycode– formats the Request-URI as per MS Teams standards
- Change_fromip_fqdn , Change_to_userandhost – changes the From and To header according to MS requirements
- Addcontactheaderinoptions – Add a new Contact header to OPTIONS message
- Recordroute – Add a new Record-Route header to OPTIONS message
- Alter_contact-changes the contact header as per MS Teams requirements
- Adduseragent – adds the SBC information in the User-Agent header,if the User-agent is not present already.
- Modifyuser – Modifies the SBC information in the User-Agent header,if the User-agent is present already.
- Reqsendonlytoinactive - Modifies the send only attribute of SDP to inactive in the request
- Replyrecvonlytoinactive - Modifies the recv only attribute of SDP to inactive in the reply

The following sip-manipulation called Teamsoutmanip is configured as out-manipulationid to make the changes mentioned above. To configure sip-manipulations, go to session-router->sip-manipulation

*Note: If running the GA release, SCZ830m1p8A, please see Appendix D prior to configuring sip manipulations in your Oracle SBC. This appendix outlines how new features added to the GA release will help simplify your configuration by eliminating the need for most, if not all required sip manipulations.*



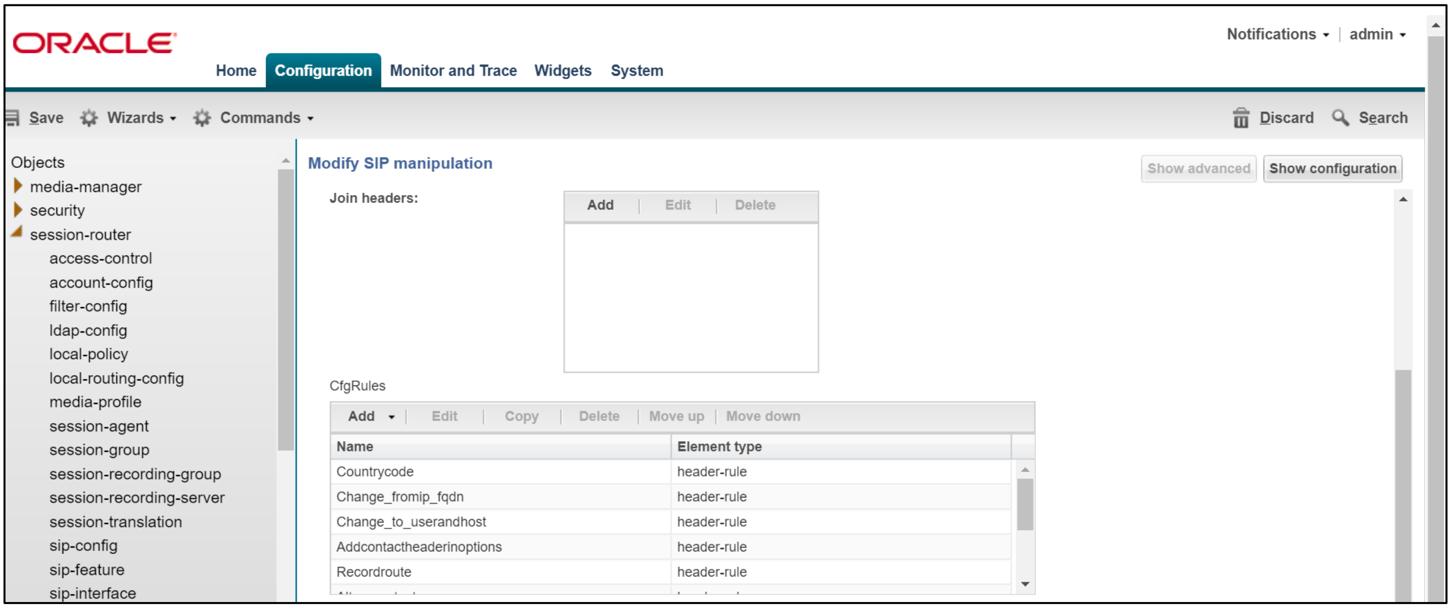
Add SIP manipulation

Name: Teamsoutmanip

Description:

Split headers:

Join headers:

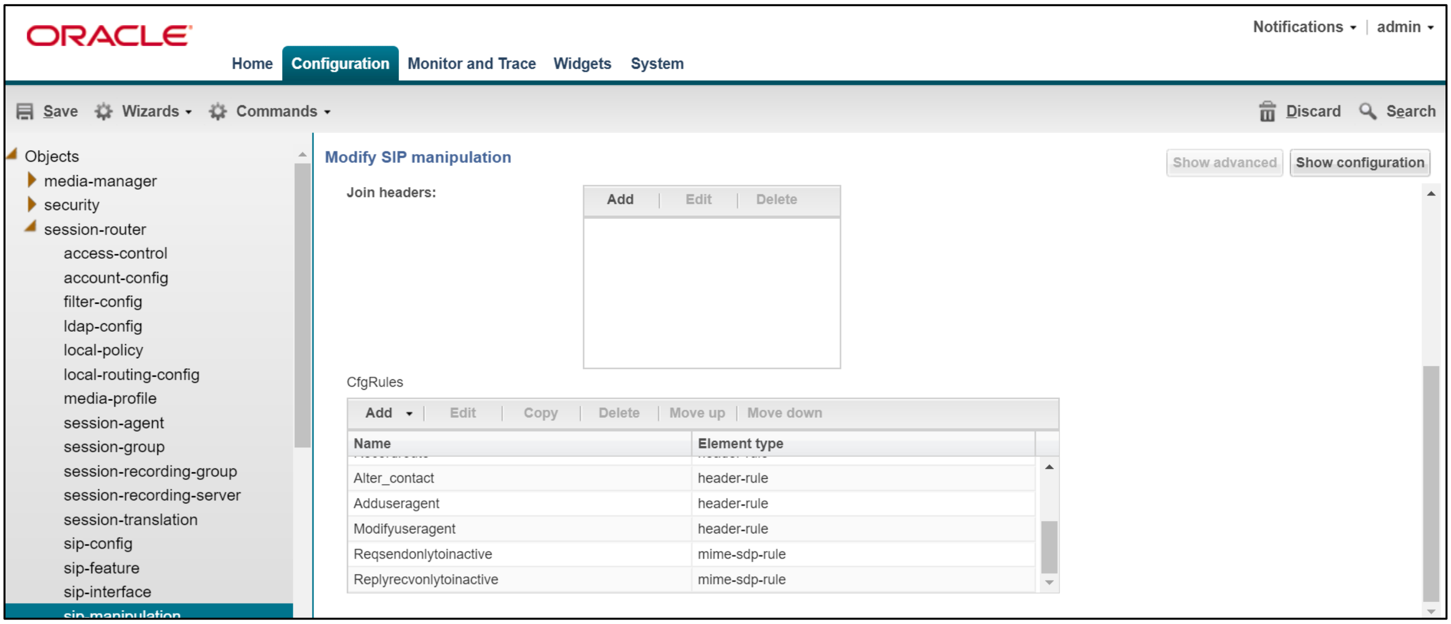


Modify SIP manipulation

Join headers:

CfgRules

| Name | Element type |
|---|---|
| Countrycode | header-rule |
| Change_fromip_fqdn | header-rule |
| Change_to_userandhost | header-rule |
| Addcontactheaderinoptions | header-rule |
| Recordroute | header-rule |



Modify SIP manipulation

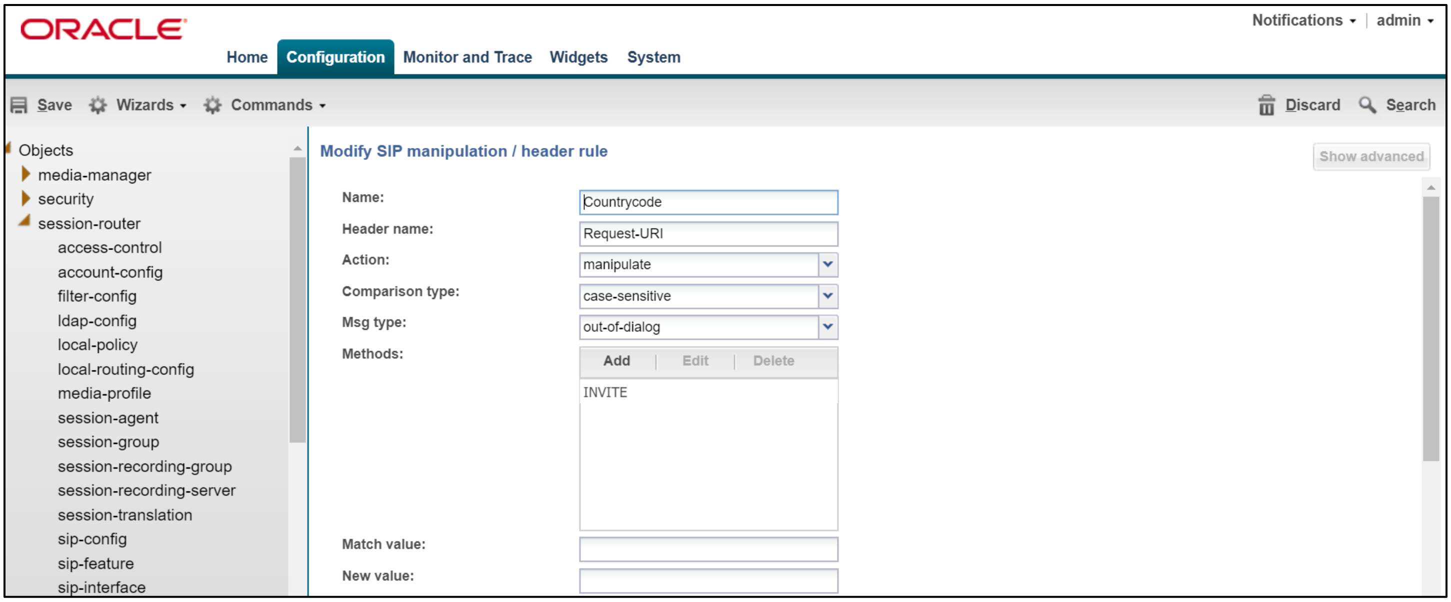
Join headers:

CfgRules

| Name | Element type |
|---|---|
| Alter_contact | header-rule |
| Adduseragent | header-rule |
| Modifyuseragent | header-rule |
| Reqsendonlytoinactive | mime-sdp-rule |
| Replyrecvonlytoinactive | mime-sdp-rule |

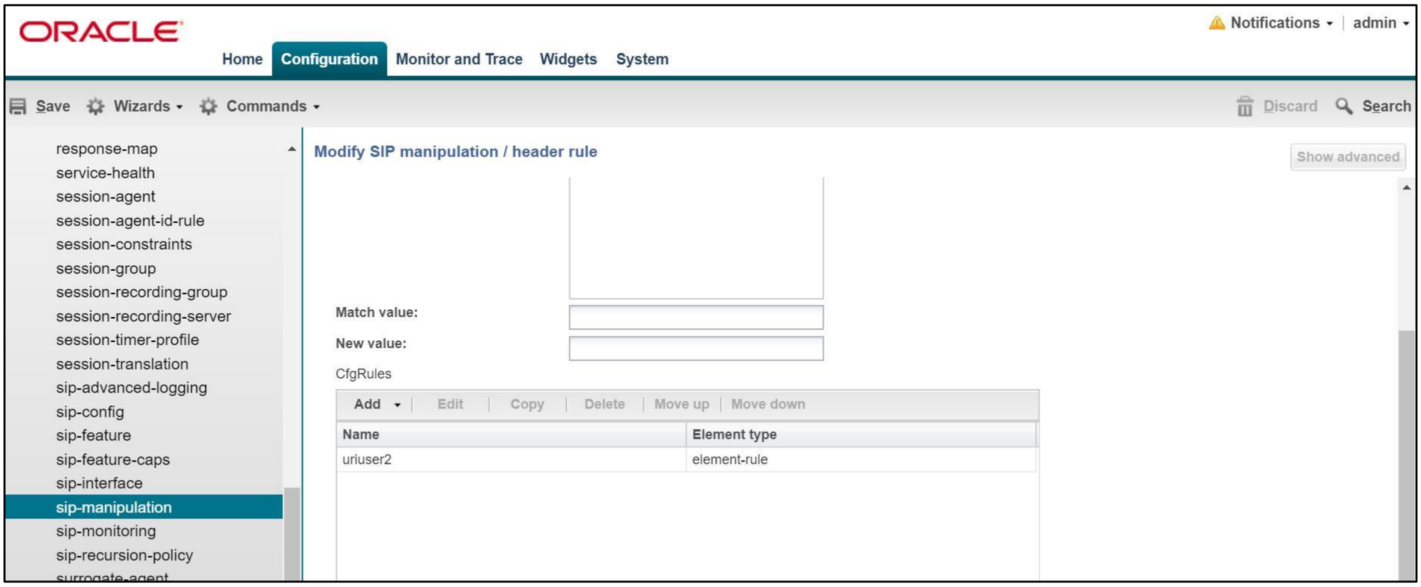
### 5.20.1 Countrycode Manipulation:

It is configured as a header rule in the sip-manipulation Teamsoutmanip shown above.



Modify SIP manipulation / header rule

| | |
|---|---|
| Name: | Countrycode |
| Header name: | Request-URI |
| Action: | manipulate |
| Comparison type: | case-sensitive |
| Msg type: | out-of-dialog |
| Methods: | INVITE |
| Match value: | |
| New value: | |

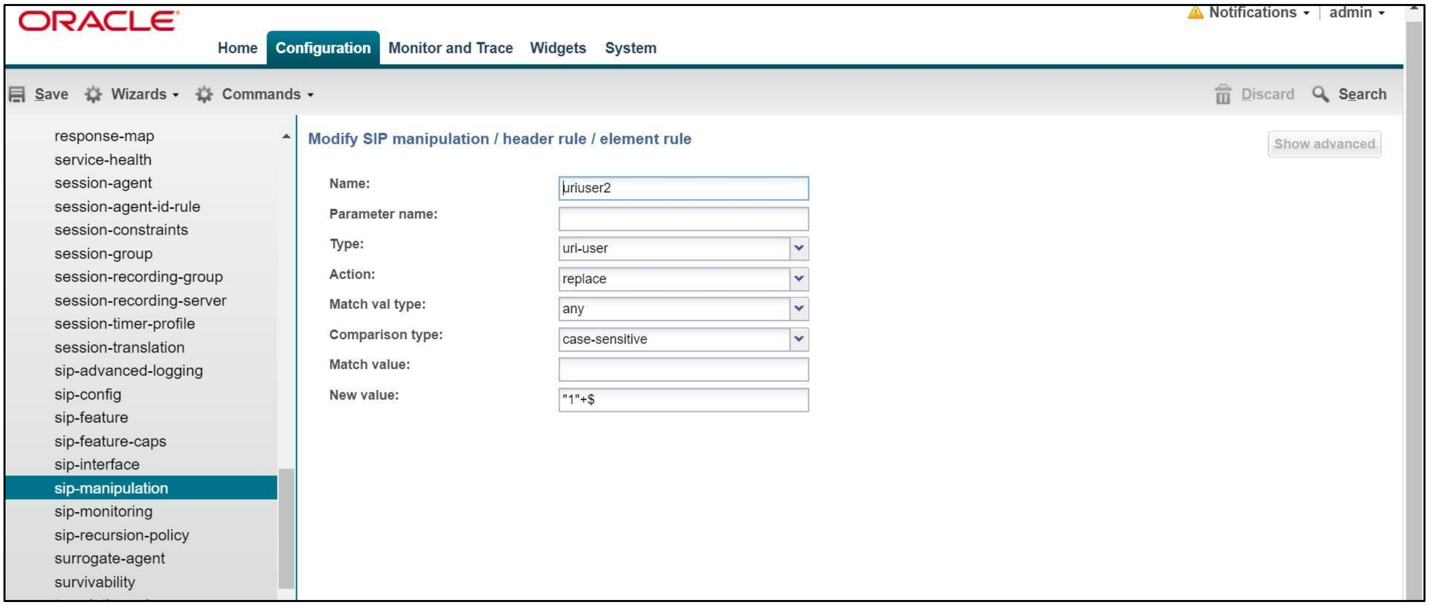


Modify SIP manipulation / header rule

| | |
|---|---|
| Match value: | |
| New value: | |

CfgRules

| Name | Element type |
|---|---|
| uriuser2 | element-rule |



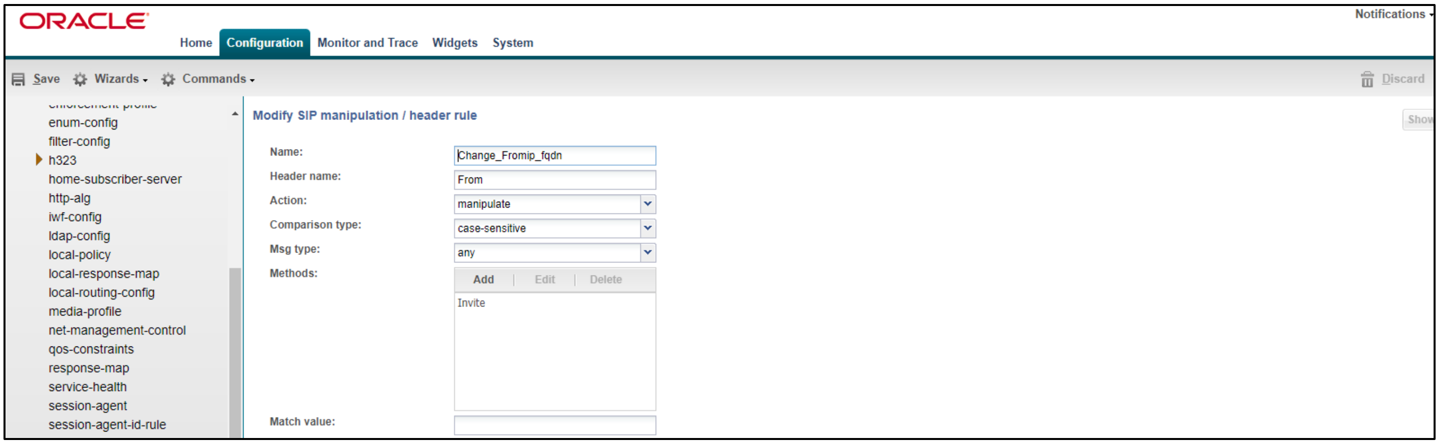
Modify SIP manipulation / header rule / element rule

| | |
|---|---|
| Name: | uriuser2 |
| Parameter name: | |
| Type: | uri-user |
| Action: | replace |
| Match val type: | any |
| Comparison type: | case-sensitive |
| Match value: | |
| New value: | "1"+$ |

Here, the “1” added is the country code of United States. Similarly, country code can be added if necessary, for other countries.

### 5.20.2 Change_fromip_fqdn Manipulation:

It is configured as a header rule in the sip-manipulation Teamsoutmanip. Here the host uri is changed to oraclesbc2.woodgroovebank.us as shown below



Modify SIP manipulation / header rule

Name: Change_Fromip_fqdn

Header name: From

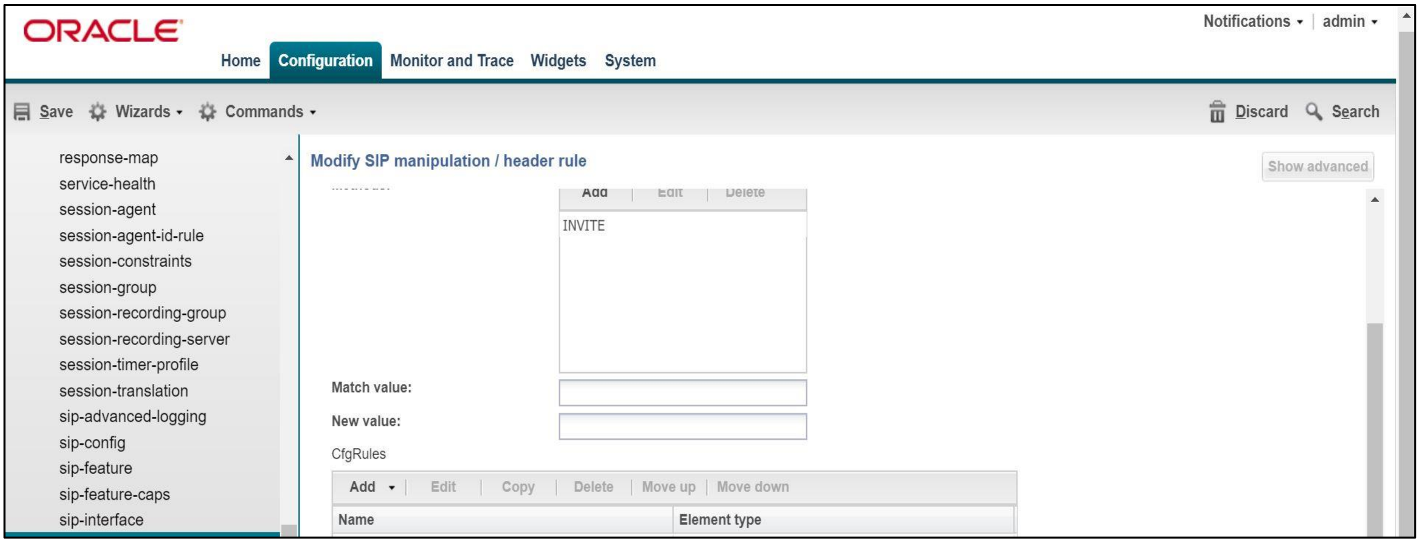
Action: manipulate

Comparison type: case-sensitive

Msg type: any

Methods: Invite

Match value:



Modify SIP manipulation / header rule

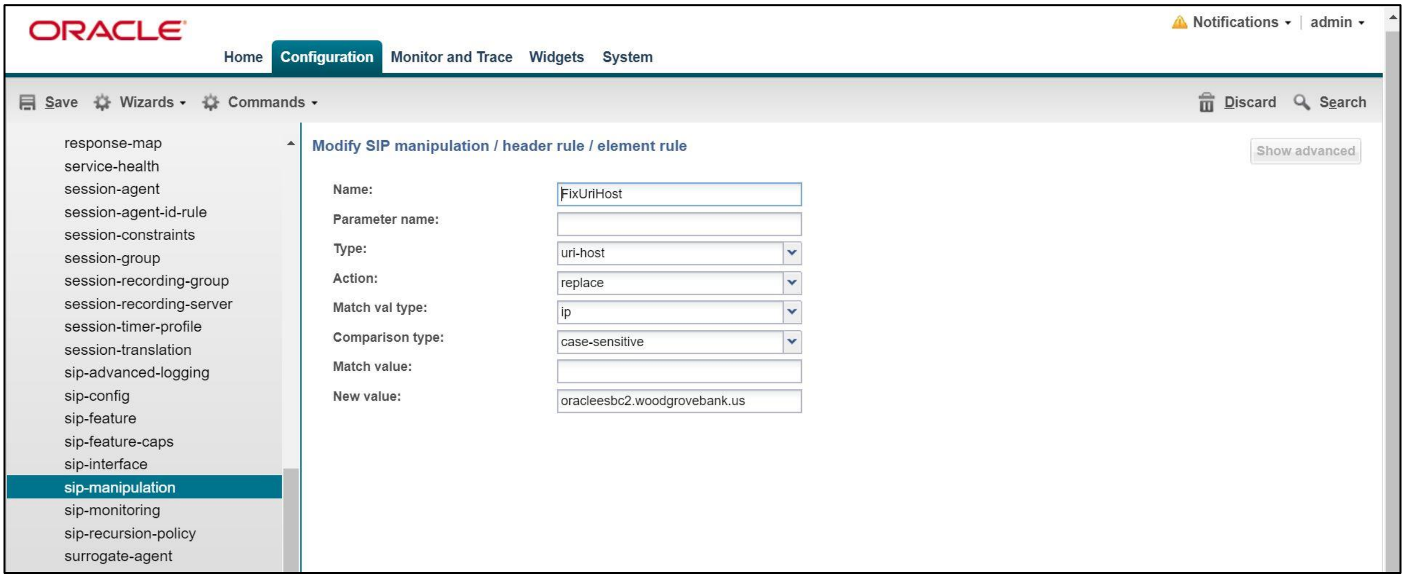
Methods: INVITE

Match value:

New value:

CfgRules

| Name | Element type |
|---|---|



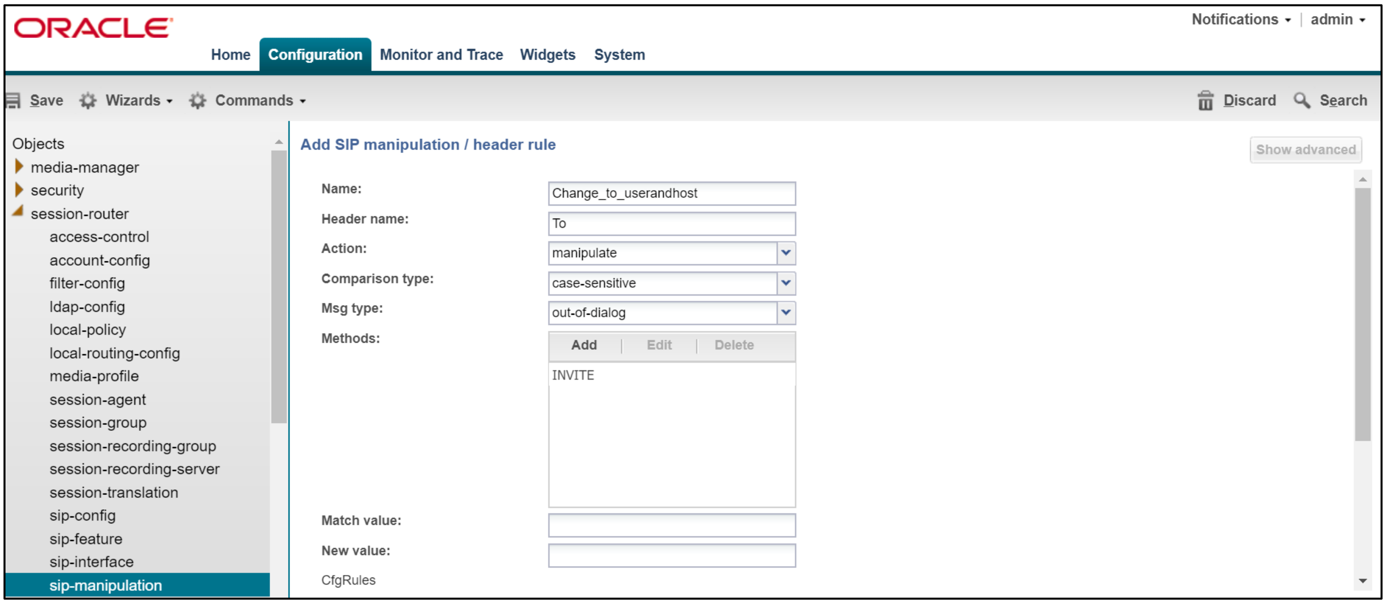
Modify SIP manipulation / header rule / element rule

| | |
|---|---|
| Name: | FixUriHost |
| Parameter name: | |
| Type: | uri-host |
| Action: | replace |
| Match val type: | ip |
| Comparison type: | case-sensitive |
| Match value: | |
| New value: | oracleesbc2.woodgrovebank.us |

### 5.20.3 Change_to_userandhost Manipulation:

It is configured as a header rule in the sip-manipulation Teamsoutmanip. Here, two element rules are added.

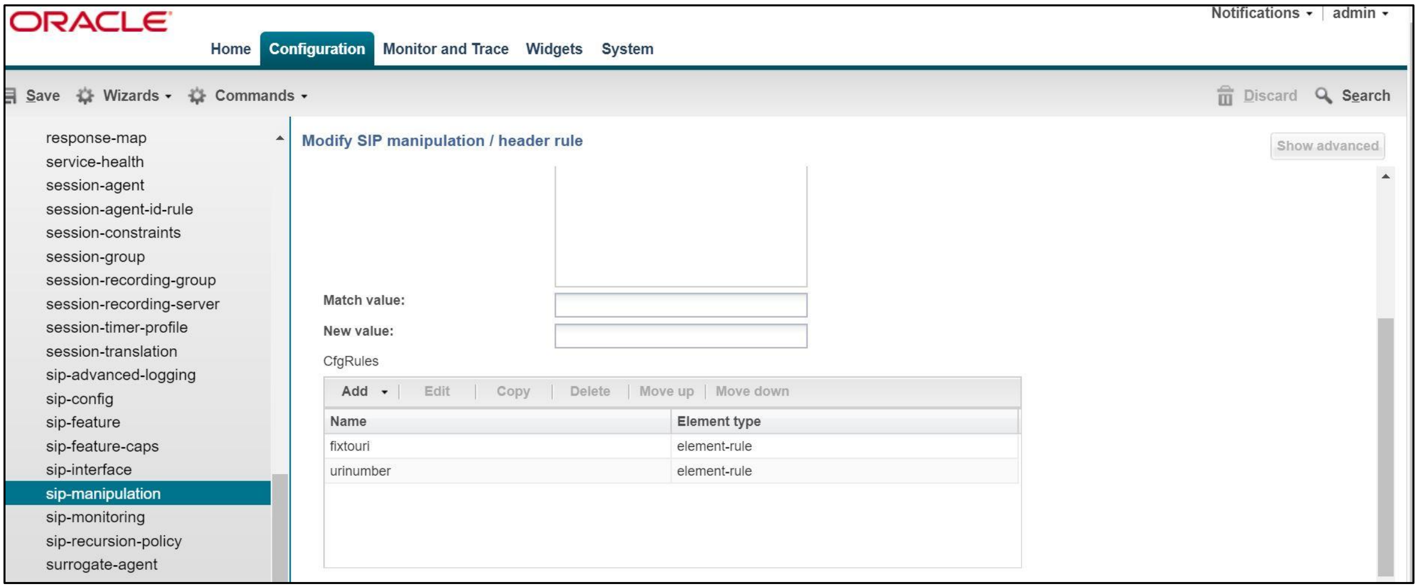
- The host uri is changed according to MS Teams requirements.
- The phone number here is also changed, here “1” added is the country code of United States. Similarly, country code can be added if necessary, for other countries.



Add SIP manipulation / header rule

| | |
|---|---|
| Name: | Change_to_userandhost |
| Header name: | To |
| Action: | manipulate |
| Comparison type: | case-sensitive |
| Msg type: | out-of-dialog |
| Methods: | INVITE |
| Match value: | |
| New value: | |

CfgRules



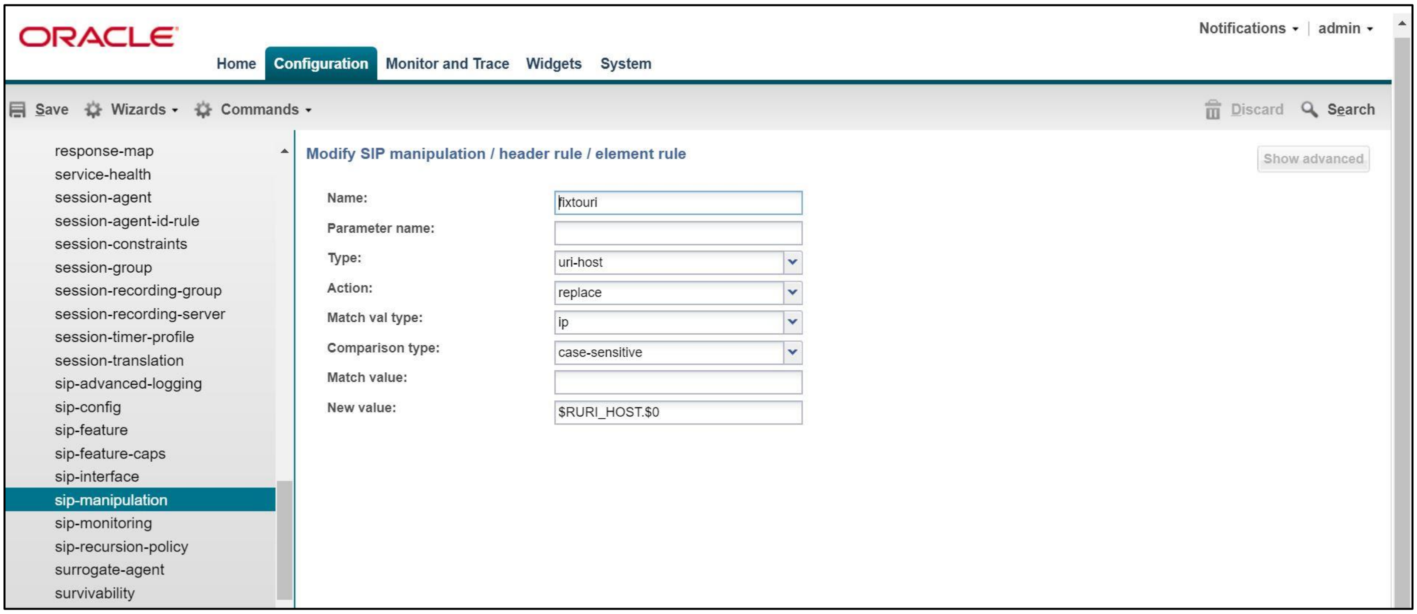
Modify SIP manipulation / header rule

Match value:

New value:

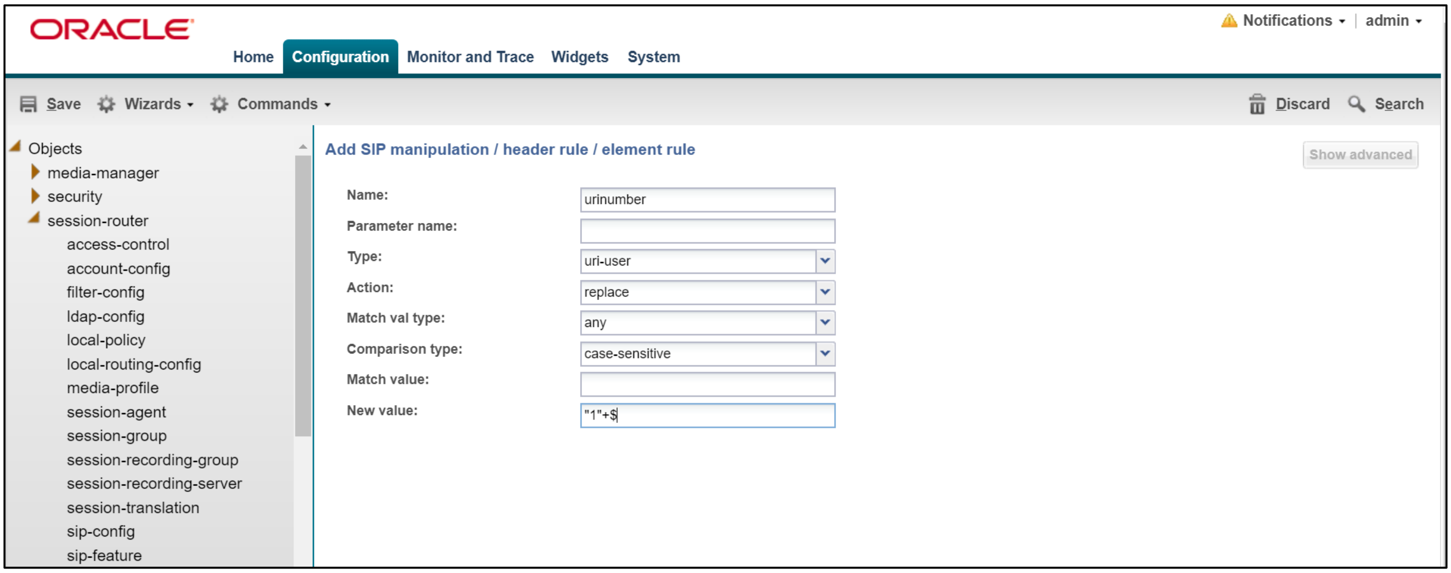
CfgRules

| Name | Element type |
|---|---|
| fixtouri | element-rule |
| urinumber | element-rule |



Modify SIP manipulation / header rule / element rule

| | |
|---|---|
| Name: | fixtouri |
| Parameter name: | |
| Type: | uri-host |
| Action: | replace |
| Match val type: | ip |
| Comparison type: | case-sensitive |
| Match value: | |
| New value: | $RURI_HOST.$0 |

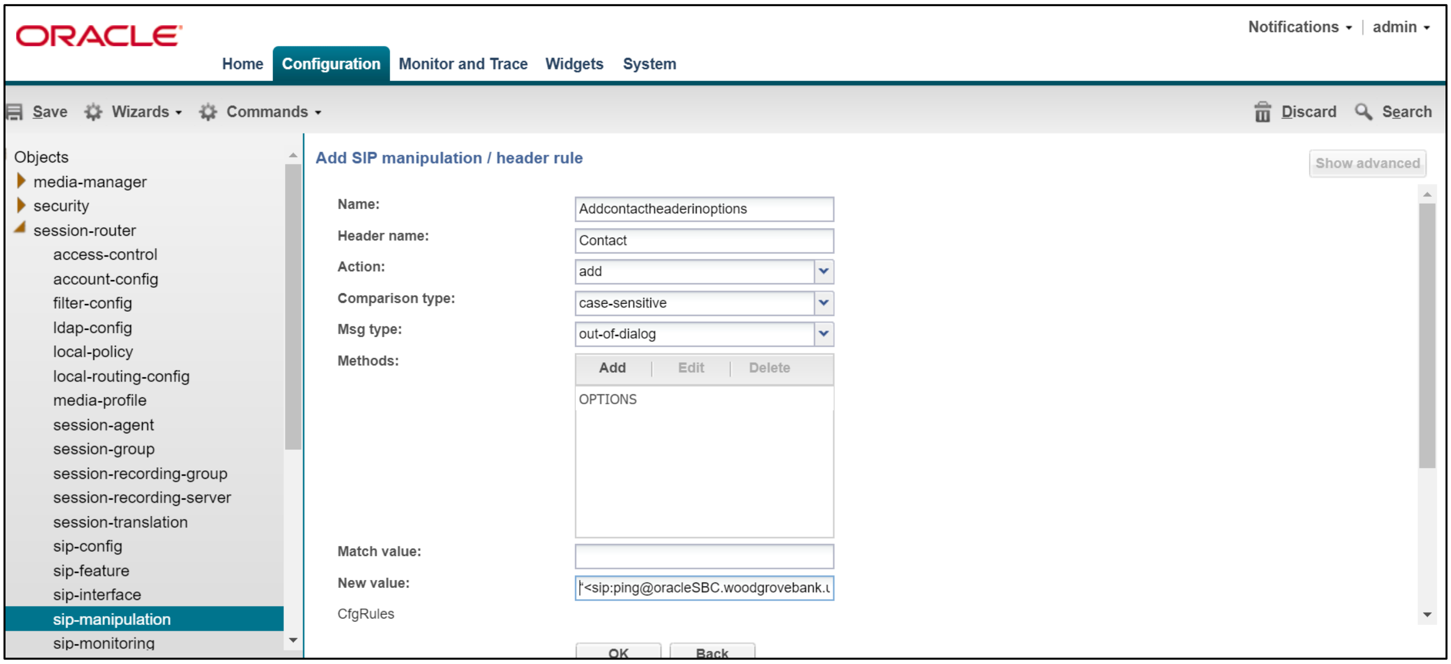


Add SIP manipulation / header rule / element rule

| | |
|---|---|
| Name: | urinumber |
| Parameter name: | |
| Type: | uri-user |
| Action: | replace |
| Match val type: | any |
| Comparison type: | case-sensitive |
| Match value: | |
| New value: | "1"+$ |

### 5.20.4 Addcontactheaderinoptions

It is configured as a header rule in the sip-manipulation Teamsoutmanip. Here the contact is changed to "<sip:ping@oracleSBC.woodgrovebank.us:5067;transport=tls>", according to MS Team requirements.



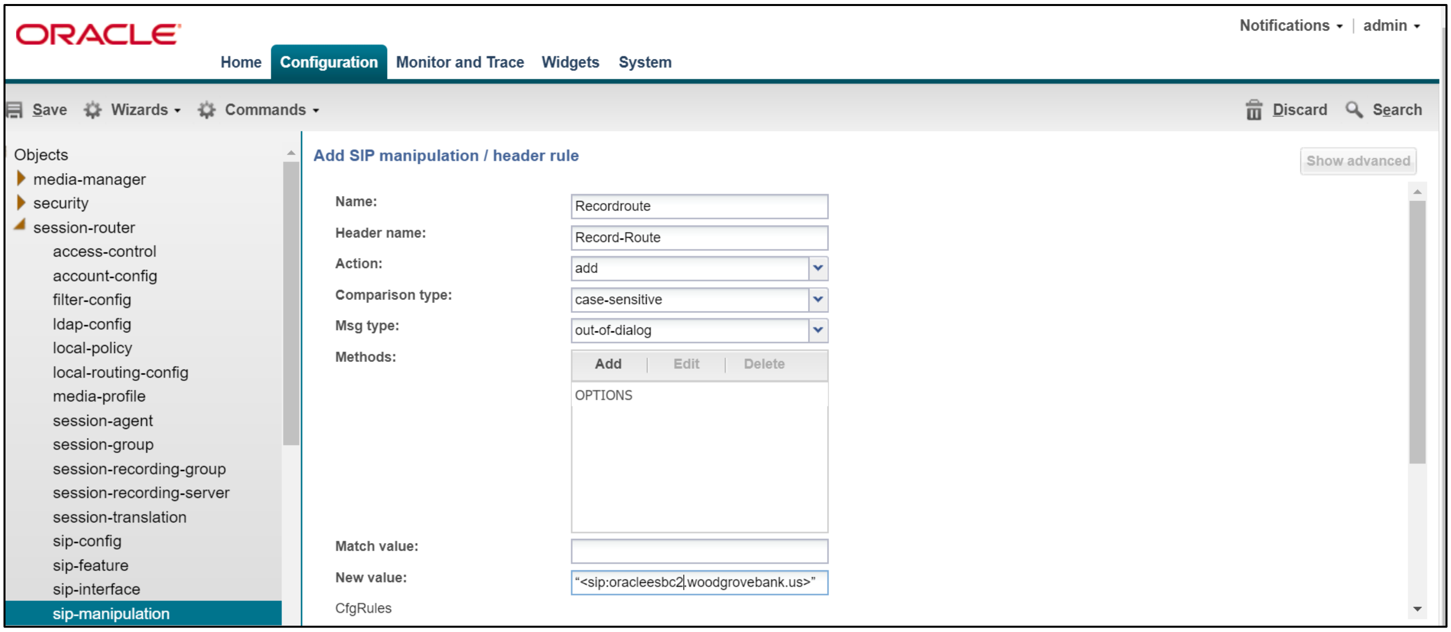
Add SIP manipulation / header rule

| | |
|---|---|
| Name: | Addcontactheaderinoptions |
| Header name: | Contact |
| Action: | add |
| Comparison type: | case-sensitive |
| Msg type: | out-of-dialog |
| Methods: | OPTIONS |
| Match value: | |
| New value: | "<sip:ping@oracleSBC.woodgrovebank.u |

CfgRules

### 5.20.5 Recordroute

It is configured as a header rule in the sip-manipulation Teamsoutmanip. Here Record-route is added to the OPTIONS message “<sip:oraclesbc2.woodgrovebank.us>”



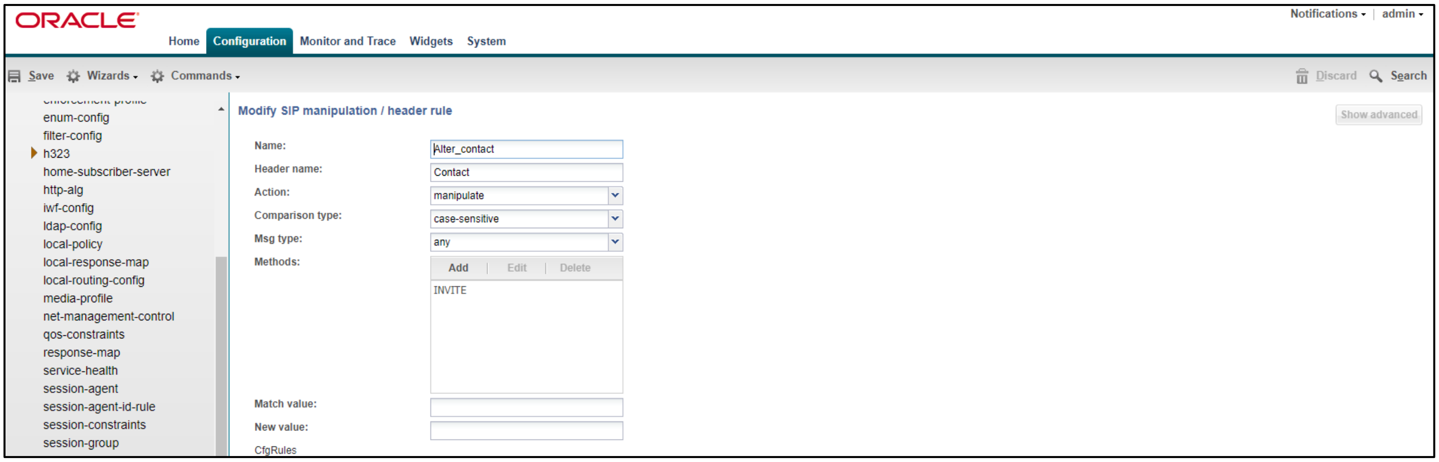
Add SIP manipulation / header rule

| | |
|---|---|
| Name: | Recordroute |
| Header name: | Record-Route |
| Action: | add |
| Comparison type: | case-sensitive |
| Msg type: | out-of-dialog |
| Methods: | OPTIONS |
| Match value: | |
| New value: | “<sip:oraclesbc2.woodgrovebank.us>” |

### 5.20.6 Alter_contact

It is configured as a header rule in the sip-manipulation Teamsoutmanip. The contact header is changed according to MS Team requirements. The following element rule is added

- Changing the uri according to include the SBC uri (oracleesbc2.woodgrovebank.us)



Modify SIP manipulation / header rule

Name: Alter_contact

Header name: Contact

Action: manipulate

Comparison type: case-sensitive

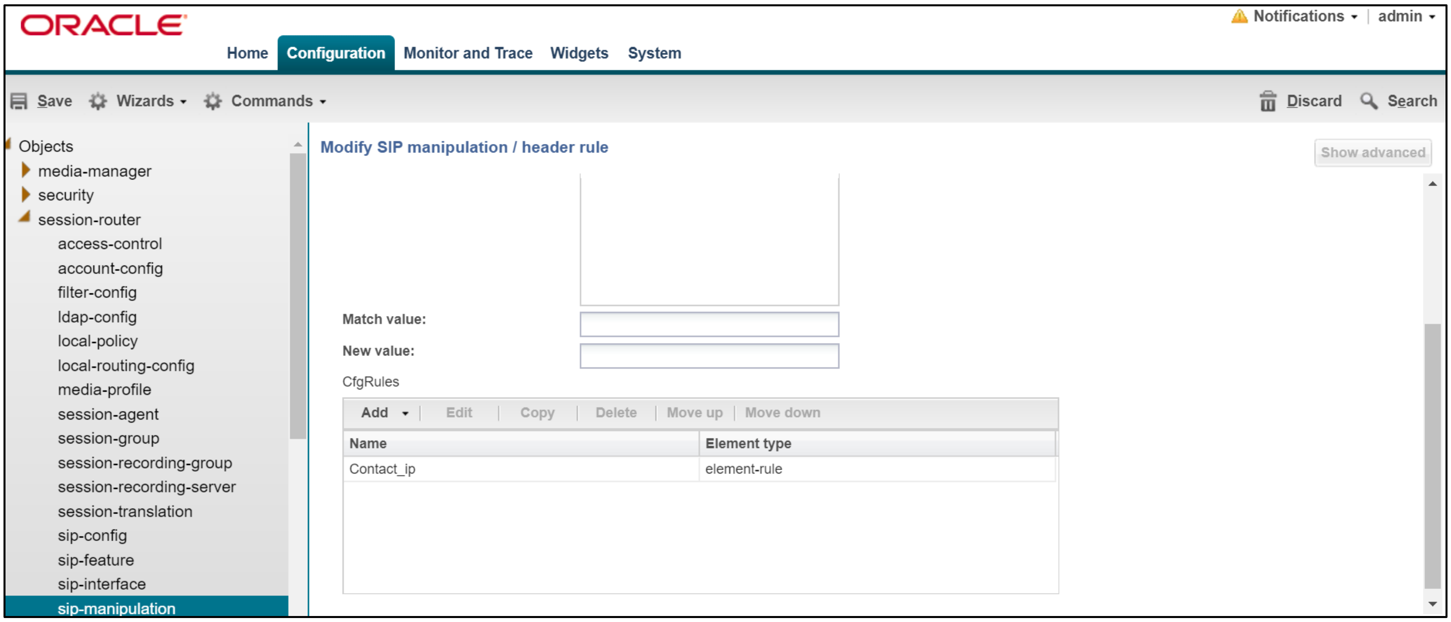
Msg type: any

Methods: INVITE

Match value:

New value:

CfgRules



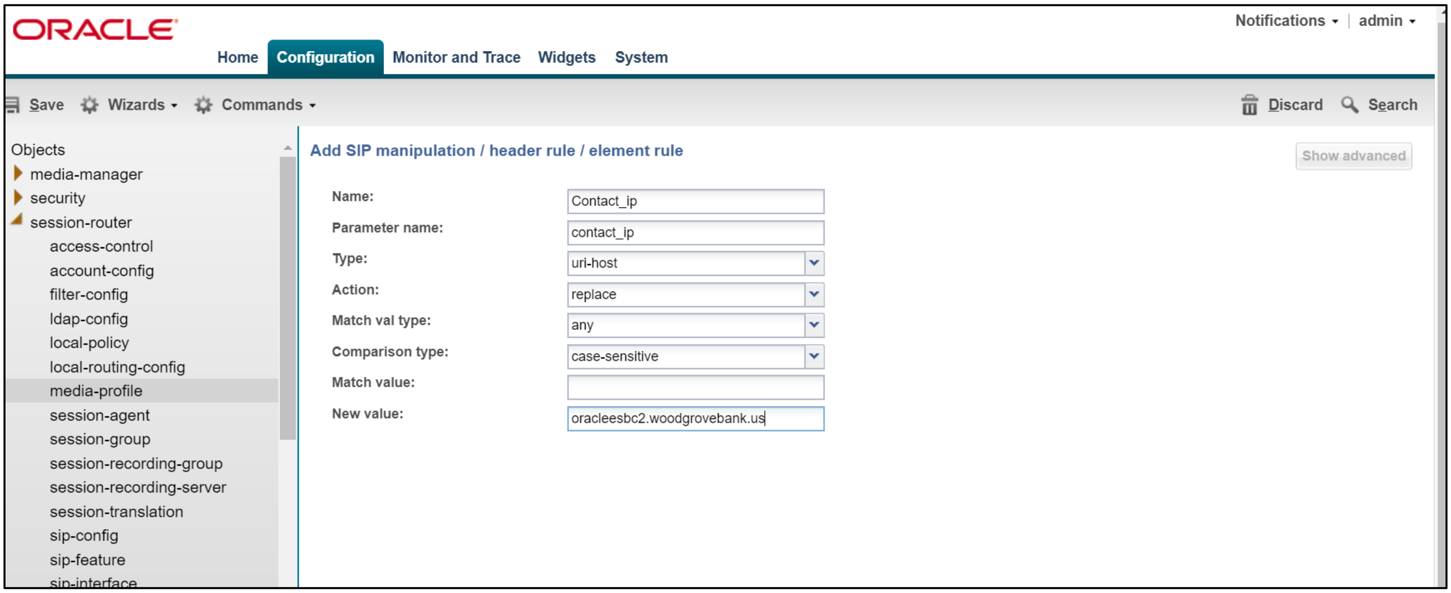
Modify SIP manipulation / header rule

Match value:

New value:

CfgRules

| Name | Element type |
|---|---|
| Contact_ip | element-rule |

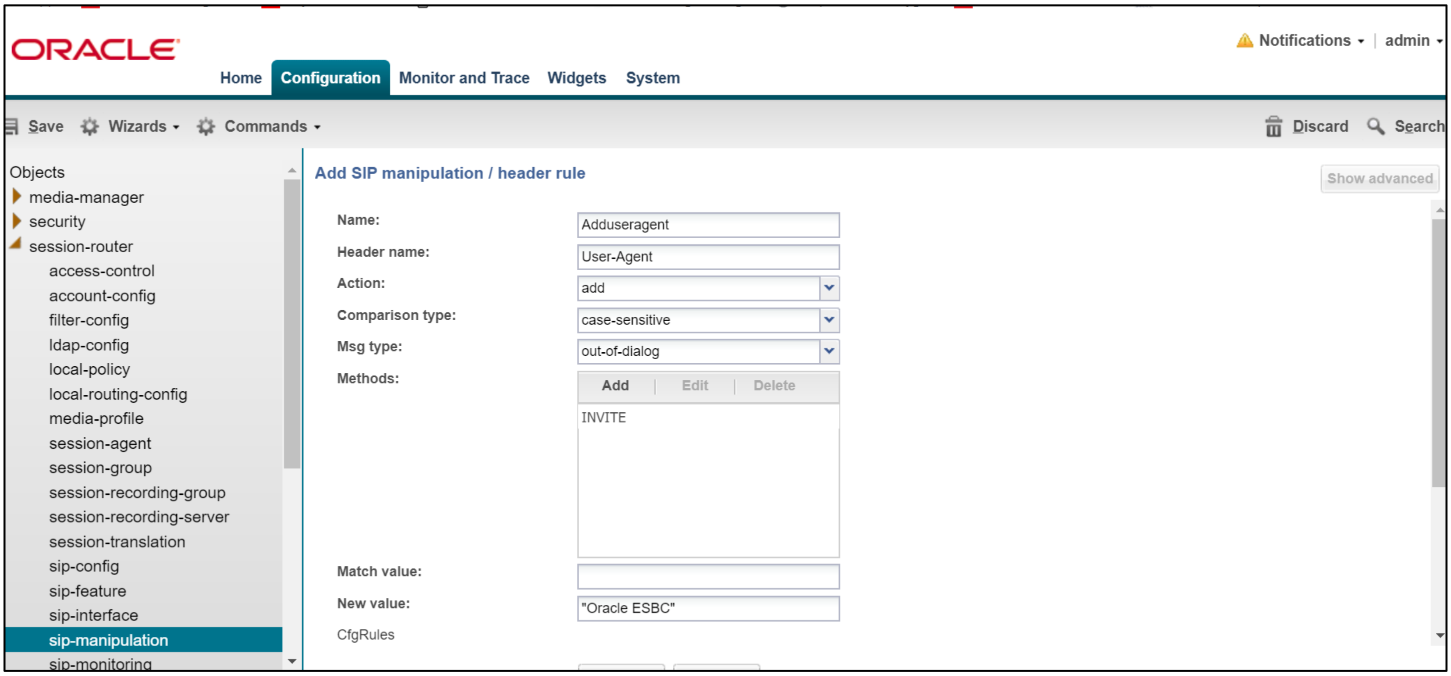


Add SIP manipulation / header rule / element rule

| | |
|---|---|
| Name: | Contact_ip |
| Parameter name: | contact_ip |
| Type: | uri-host |
| Action: | replace |
| Match val type: | any |
| Comparison type: | case-sensitive |
| Match value: | |
| New value: | oraclesbc2.woodgrovebank.us |

## 5.20.7 Adduseragent

It is configured as a header rule in the sip-manipulation Teamsoutmanip. It adds the user agent to the Invite message, if it is already not present in the invite from Siptrunk.



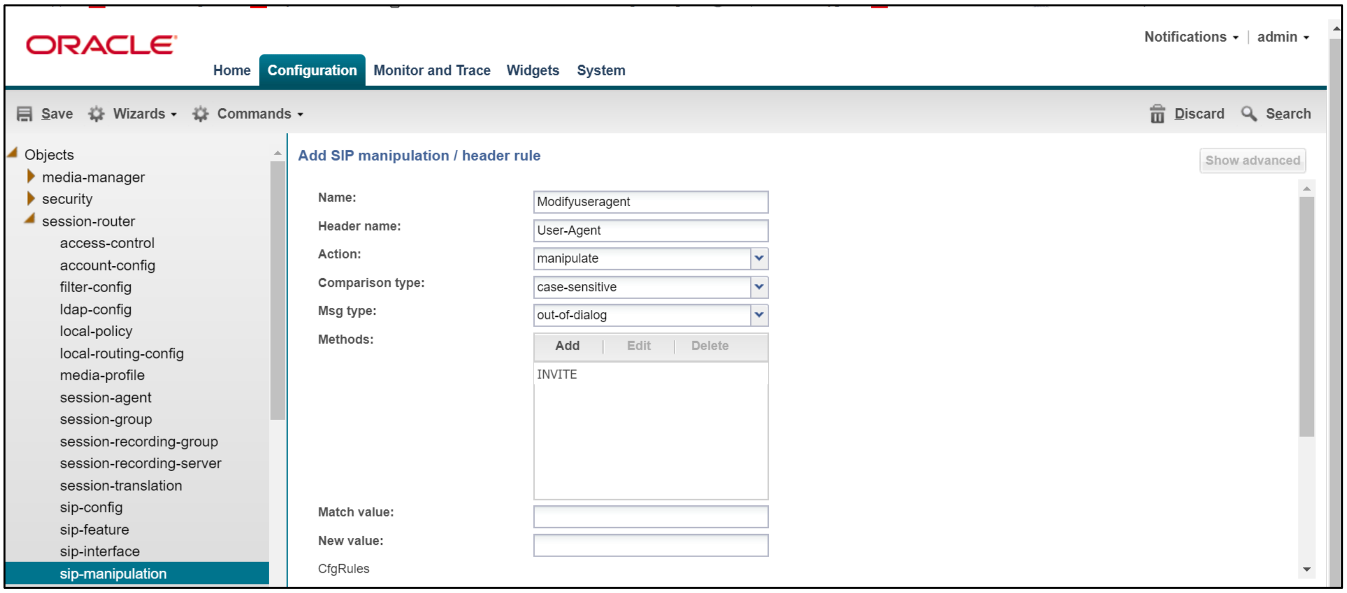
Add SIP manipulation / header rule

| | |
|---|---|
| Name: | Adduseragent |
| Header name: | User-Agent |
| Action: | add |
| Comparison type: | case-sensitive |
| Msg type: | out-of-dialog |
| Methods: | INVITE |
| Match value: | |
| New value: | "Oracle ESBC" |

CfgRules

### 5.20.8 Modifyuseragent

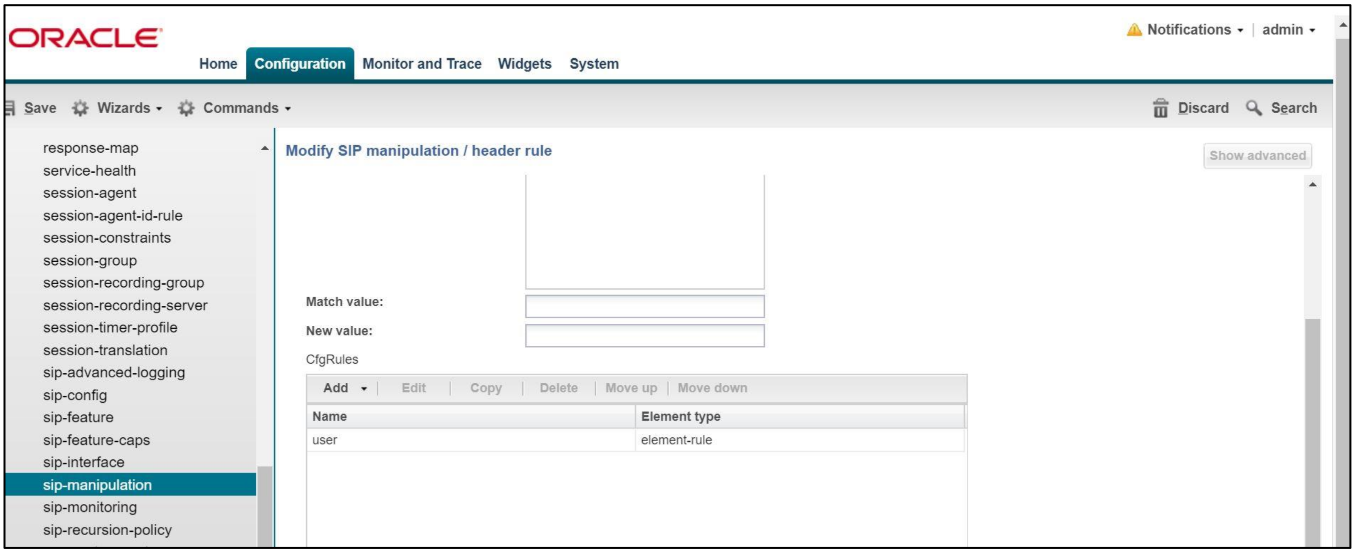
It is configured as a header rule in the sip-manipulation Teamsoutmanip. It modifies the user agent to the Invite message, according to MS Teams requirements.



Add SIP manipulation / header rule

| | |
|---|---|
| Name: | Modifyuseragent |
| Header name: | User-Agent |
| Action: | manipulate |
| Comparison type: | case-sensitive |
| Msg type: | out-of-dialog |
| Methods: | INVITE |
| Match value: | |
| New value: | |

CfgRules

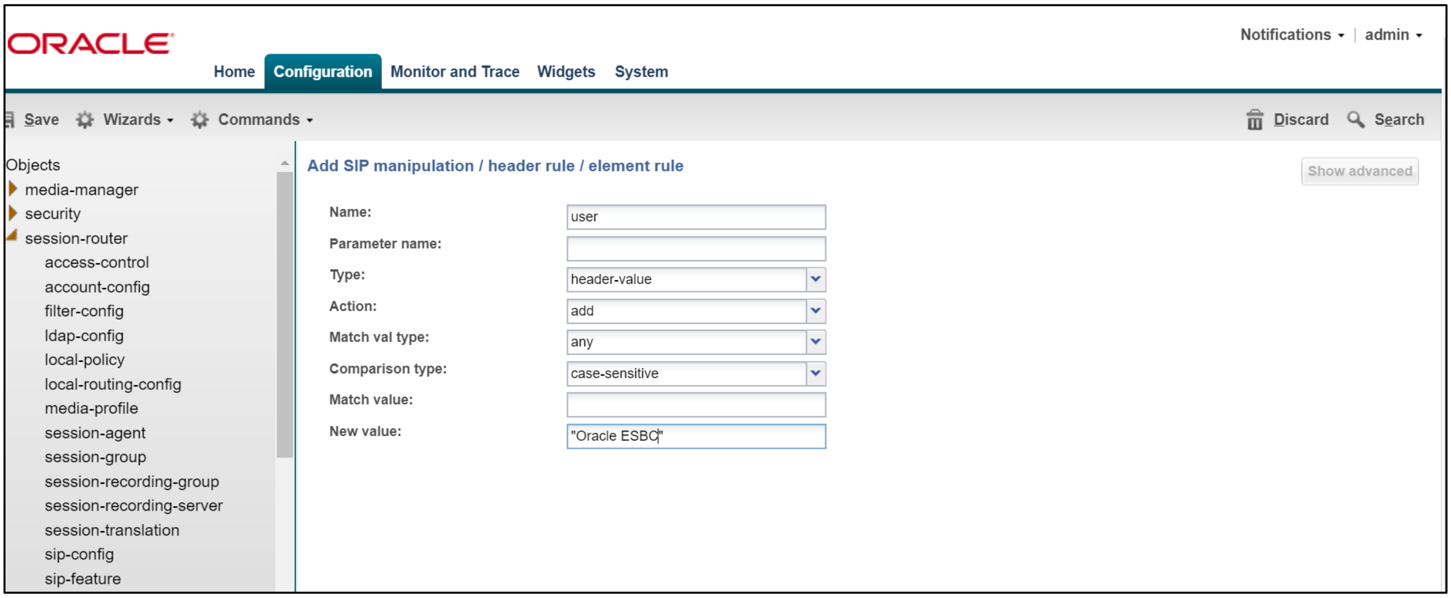


Modify SIP manipulation / header rule

| | |
|---|---|
| Match value: | |
| New value: | |

CfgRules

| Name | Element type |
|---|---|
| user | element-rule |



Add SIP manipulation / header rule / element rule

| | |
|---|---|
| Name: | user |
| Parameter name: | |
| Type: | header-value |
| Action: | add |
| Match val type: | any |
| Comparison type: | case-sensitive |
| Match value: | |
| New value: | "Oracle ESBC" |

For configuring the following rules in Teamsoutmanip, click on the hyperlink below.

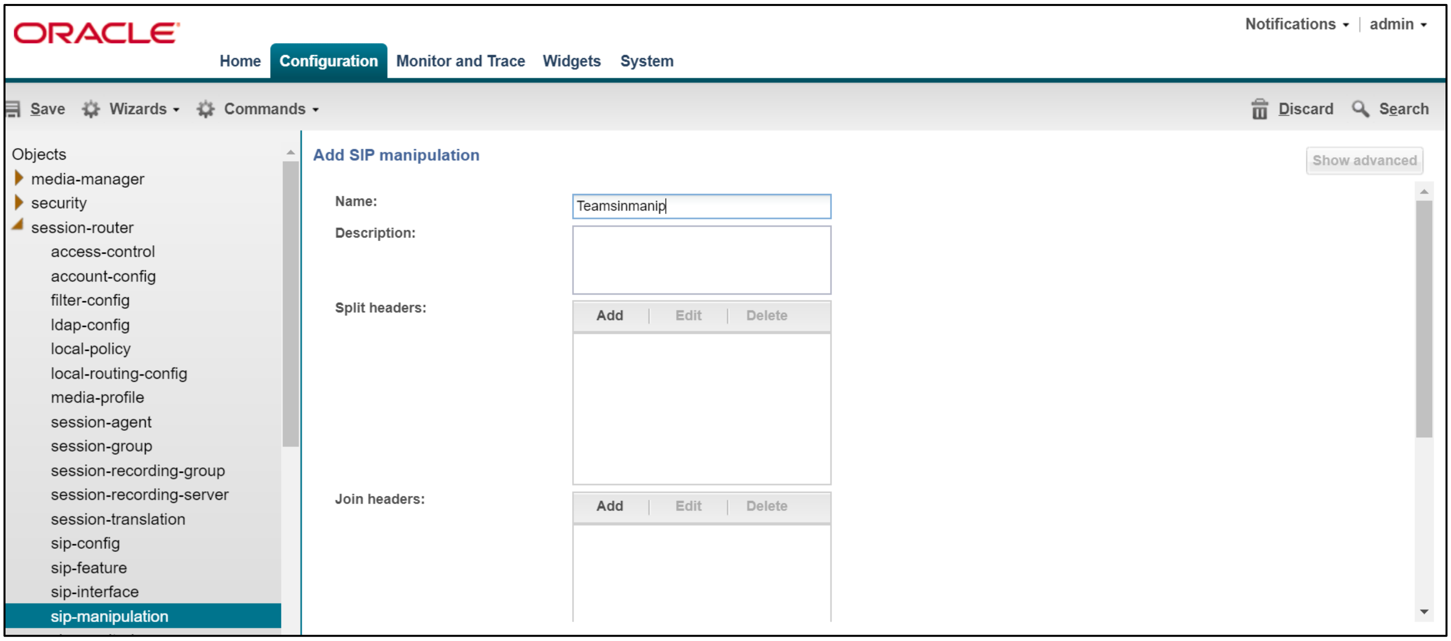
- Reqsendonlytoinactive
- Replyrecvonlytoinactive

## 5.21 Teamsinmanip

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

- Respondoptions – to handle the OPTIONS locally
- Reqinactivetosendonly – replaces the inactive SDP attribute to sendonly in the request
- Replyinactivetorecvonly - replaces the inactive SDP attribute to recvonly in the reply
- Change183to180 –Changes 183 Session in Progress to 180 Ringing for ringback requirements

*Note: If running the GA release, SCZ830m1p8A, please see Appendix D prior to configuring sip manipulations in your Oracle SBC. This appendix outlines how new features added to the GA release will help simplify your configuration by eliminating the need for most, if not all required sip manipulations.*



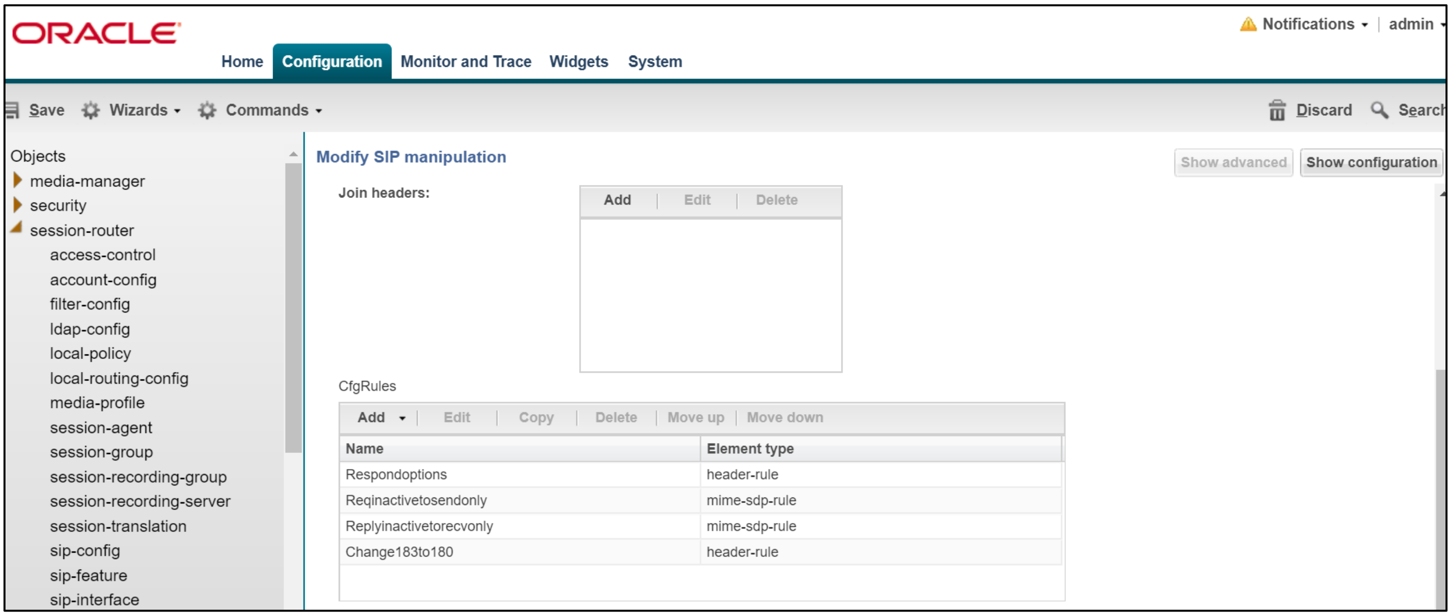
Add SIP manipulation

Name: Teamsinmanip

Description:

Split headers:

Join headers:



Modify SIP manipulation

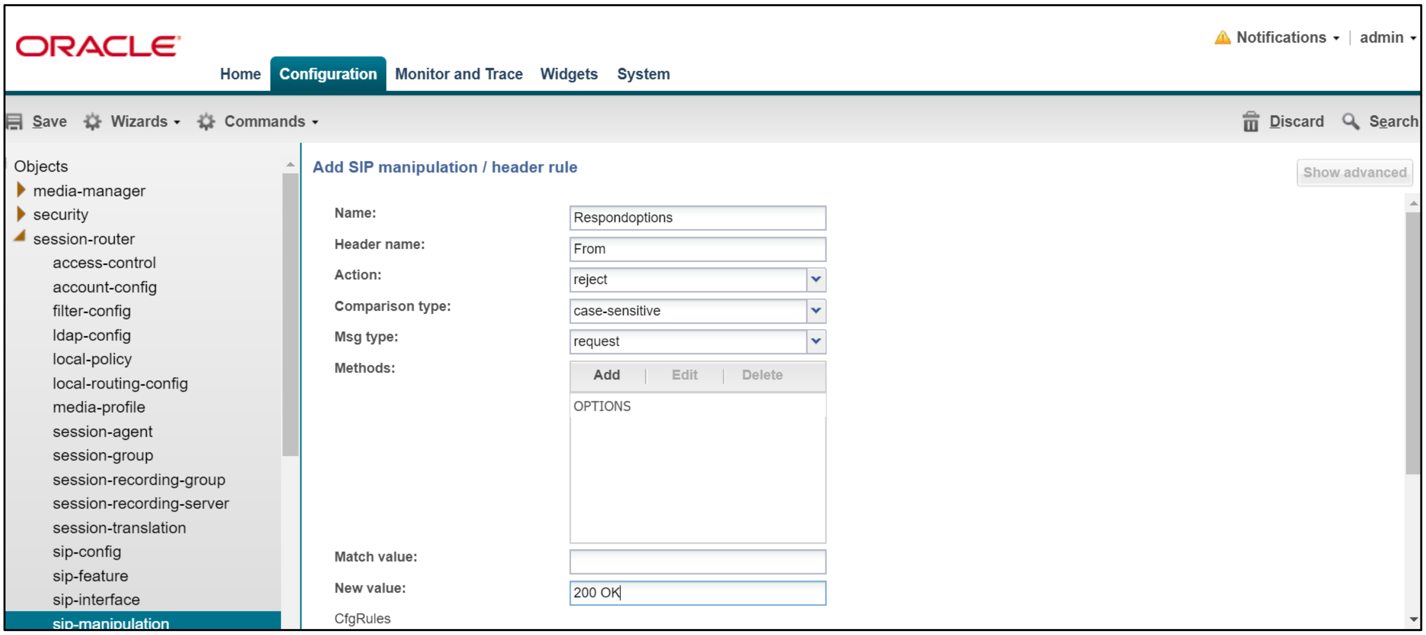
Join headers:

CfgRules

| Name | Element type |
|---|---|
| Respondoptions | header-rule |
| Reqinactivetosendonly | mime-sdp-rule |
| Replyinactivetorecvonly | mime-sdp-rule |
| Change183to180 | header-rule |

### 5.21.1 Respondoptions

It is configured as a header-rule rule in the sip-manipulation Teamsinmanip. This handles the options locally.



Add SIP manipulation / header rule

Name: Respondoptions

Header name: From

Action: reject

Comparison type: case-sensitive

Msg type: request

Methods: OPTIONS

Match value:

New value: 200 OK

CfgRules

Please click on the hyperlink for the following rules applied on the Teamsinmanip manipulation.

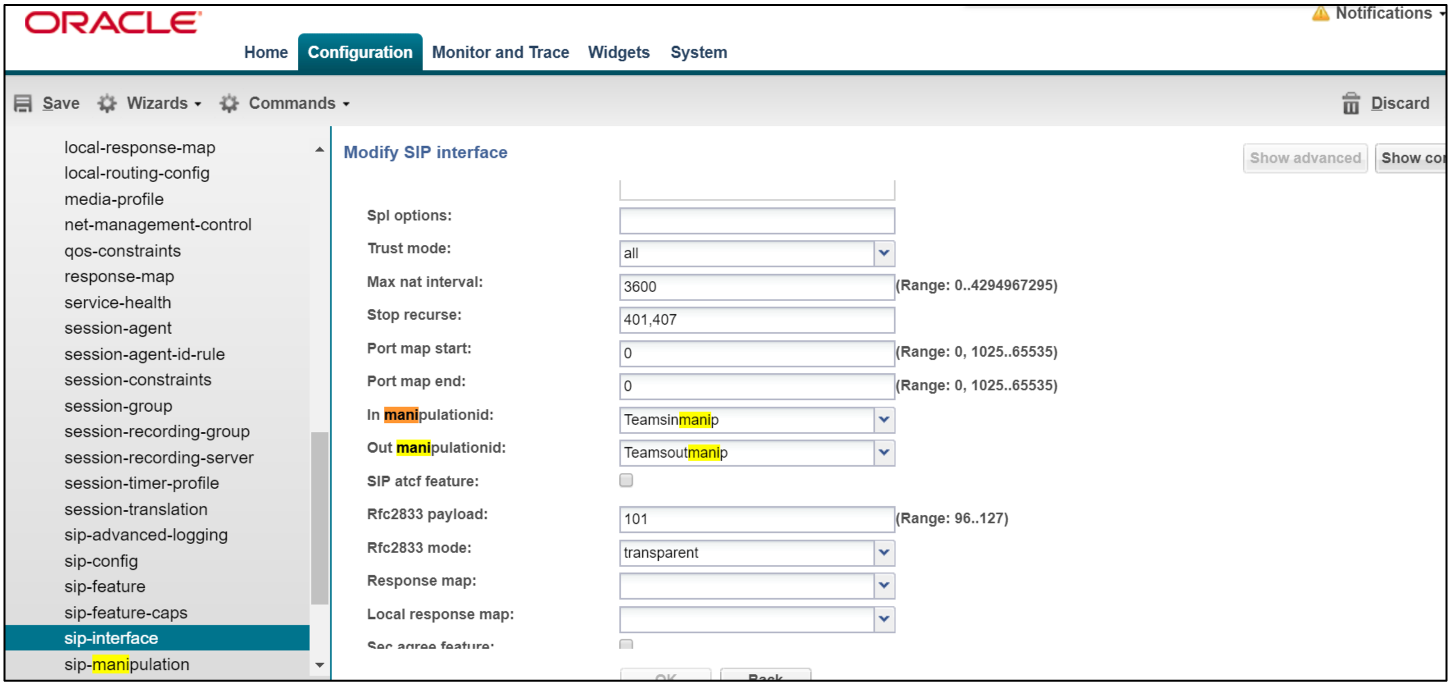
“Change183to180”

Reqinactivetosendonly

Reqinactivetorecvonly

## 5.22 Applying the teams SIP manipulations to Teams SIP Interface

Apply the above sip manipulations to sip-interface as shown below.



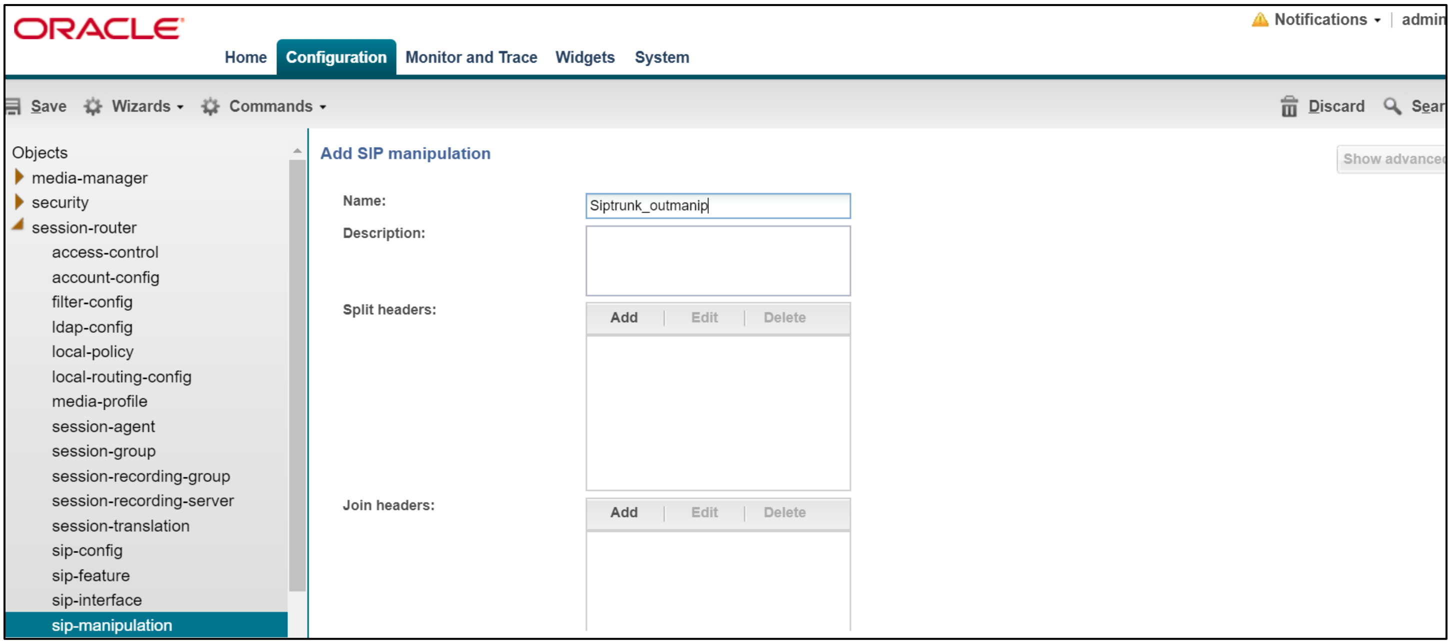
Modify SIP interface

| | |
|---|---|
| Spl options: | |
| Trust mode: | all |
| Max nat interval: | 3600 (Range: 0..4294967295) |
| Stop recurse: | 401,407 |
| Port map start: | 0 (Range: 0, 1025..65535) |
| Port map end: | 0 (Range: 0, 1025..65535) |
| In manipulationid: | Teamsinmanip |
| Out manipulationid: | Teamsoutmanip |
| SIP atcf feature: | ☐ |
| Rfc2833 payload: | 101 (Range: 96..127) |
| Rfc2833 mode: | transparent |
| Response map: | |
| Local response map: | |
| Sec agree feature: | ☐ |

## 5.23 Siptrunk_outmanip

We configure the manipulation Siptrunk_outmanip to modify the SIP messages going to the SIP Trunk as below

- Change_fqdn_to_ip_from to replace the uri-host of the From header with the SBC’s local ip.
- Change_fqdn_to_ip_to to replace the uri-host of the To header with the ip –address of the Trunk device.



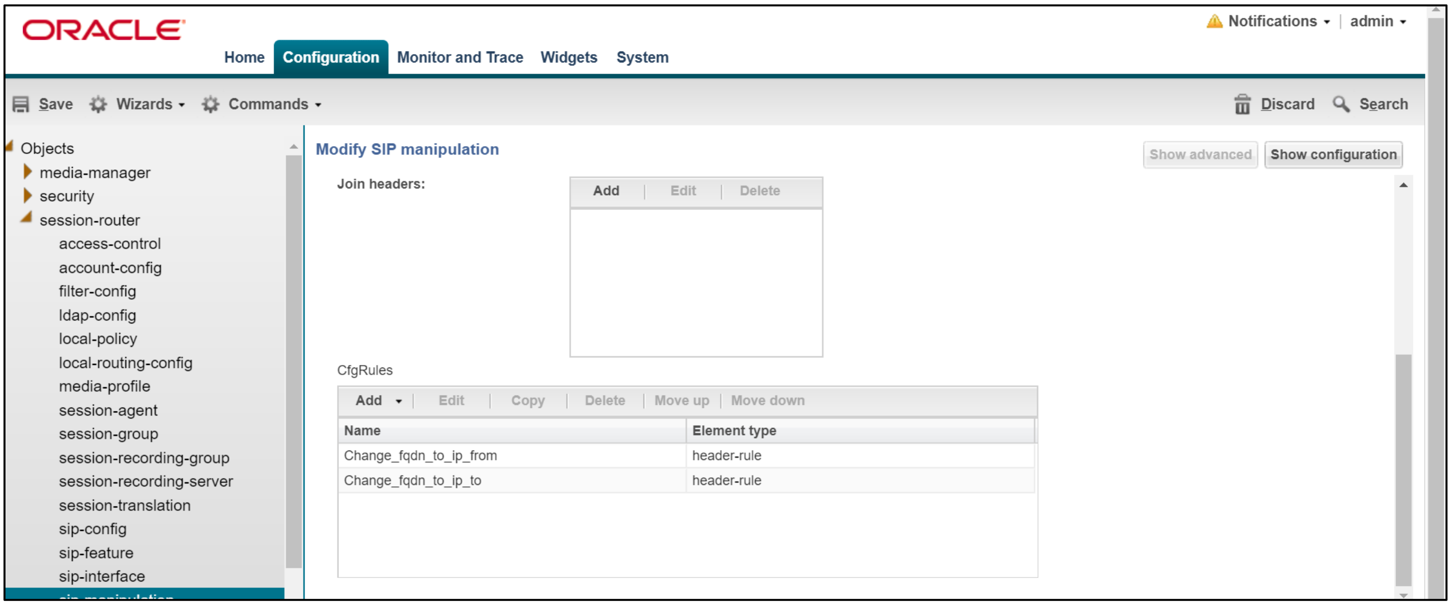
**Add SIP manipulation**

Name: Siptrunk_outmanip

Description:

Split headers:

Join headers:



**Modify SIP manipulation**

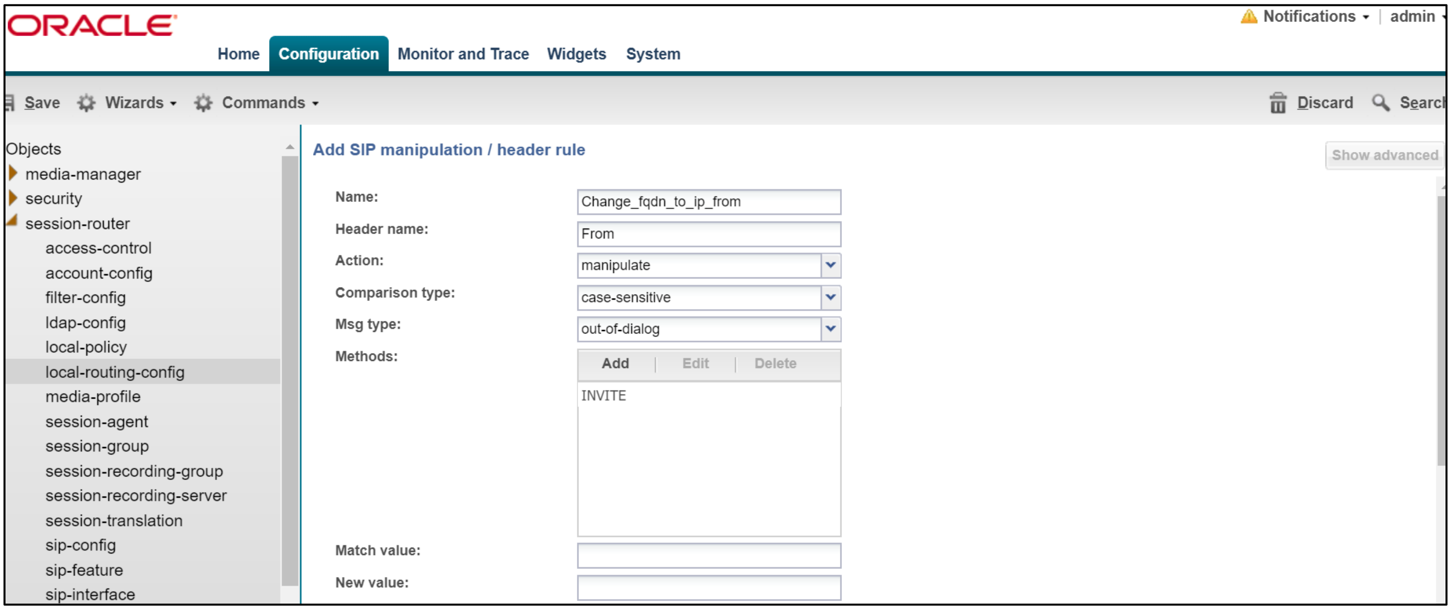
Join headers:

CfgRules

| Name | Element type |
|---|---|
| Change_fqdn_to_ip_from | header-rule |
| Change_fqdn_to_ip_to | header-rule |

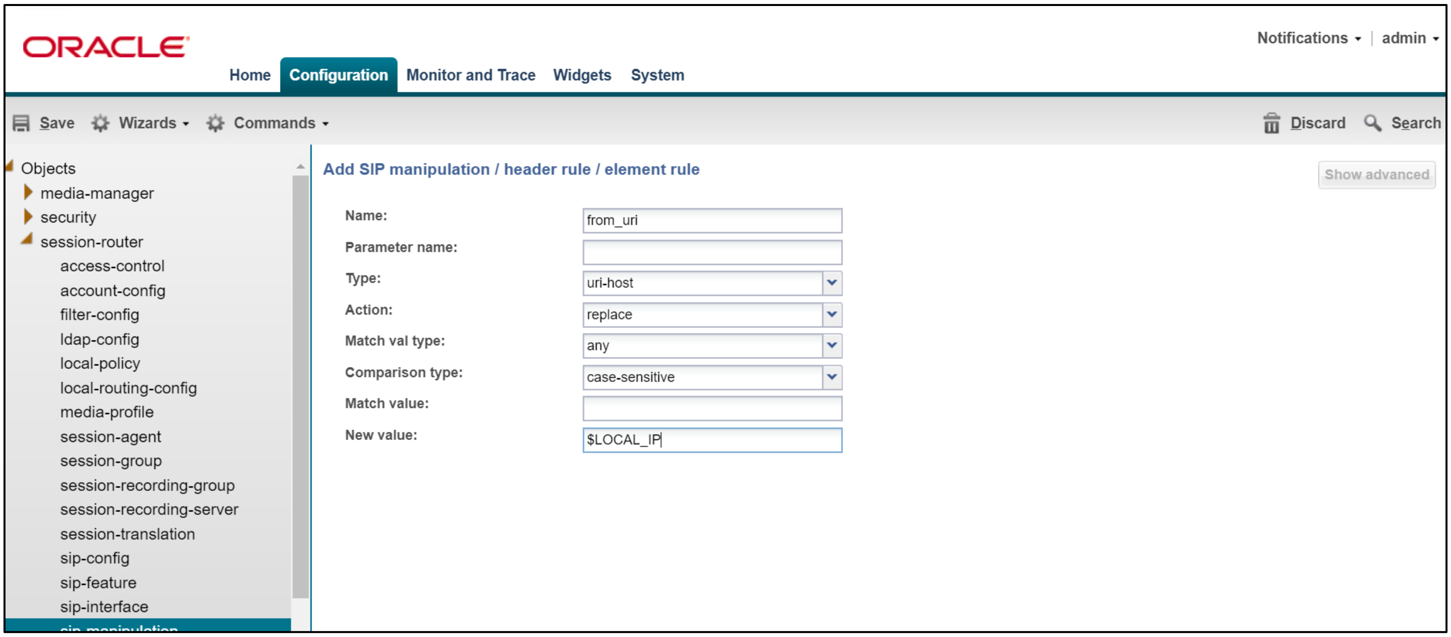
### 5.23.1 Change_fqdn_to_ip_from

It is applied as a header rule in Siptrunk_outmanip, to replace the uri-host of the From header with the SBC's local ip.



Add SIP manipulation / header rule

| | |
|---|---|
| Name: | Change_fqdn_to_ip_from |
| Header name: | From |
| Action: | manipulate |
| Comparison type: | case-sensitive |
| Msg type: | out-of-dialog |
| Methods: | INVITE |
| Match value: | |
| New value: | |

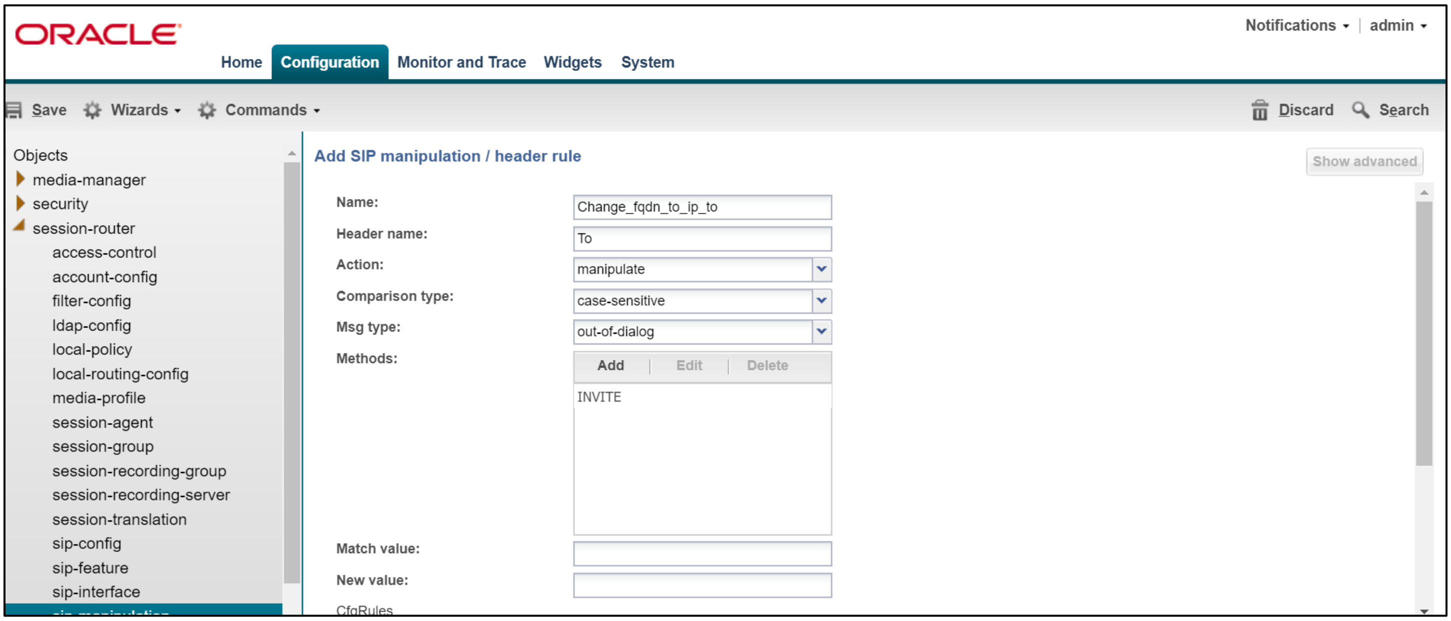


Add SIP manipulation / header rule / element rule

| | |
|---|---|
| Name: | from_uri |
| Parameter name: | |
| Type: | uri-host |
| Action: | replace |
| Match val type: | any |
| Comparison type: | case-sensitive |
| Match value: | |
| New value: | $LOCAL_IP |

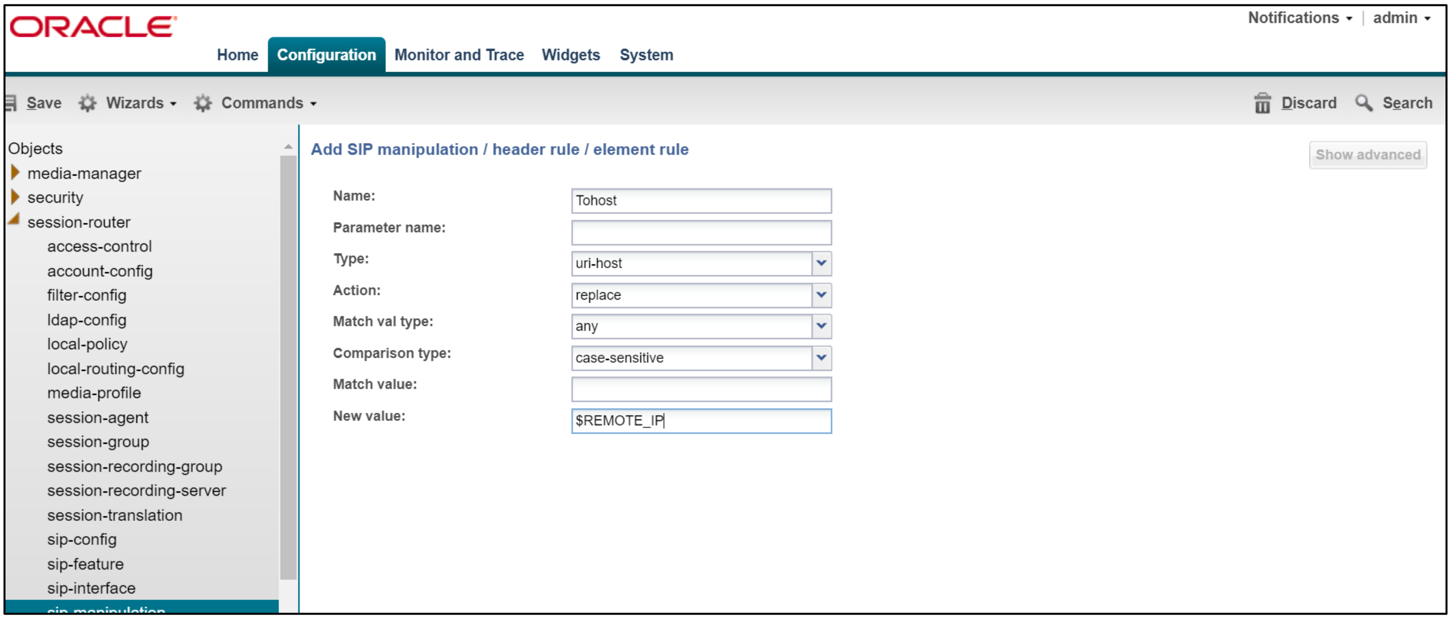
### 5.23.2 Change_fqdn_to_ip_to

It is applied as a header rule in Siptrunk_outmanip, to replace the uri-host of the To header with the ip –address of the Trunk device



Add SIP manipulation / header rule

| | |
|---|---|
| Name: | Change_fqdn_to_ip_to |
| Header name: | To |
| Action: | manipulate |
| Comparison type: | case-sensitive |
| Msg type: | out-of-dialog |
| Methods: | INVITE |
| Match value: | |
| New value: | |

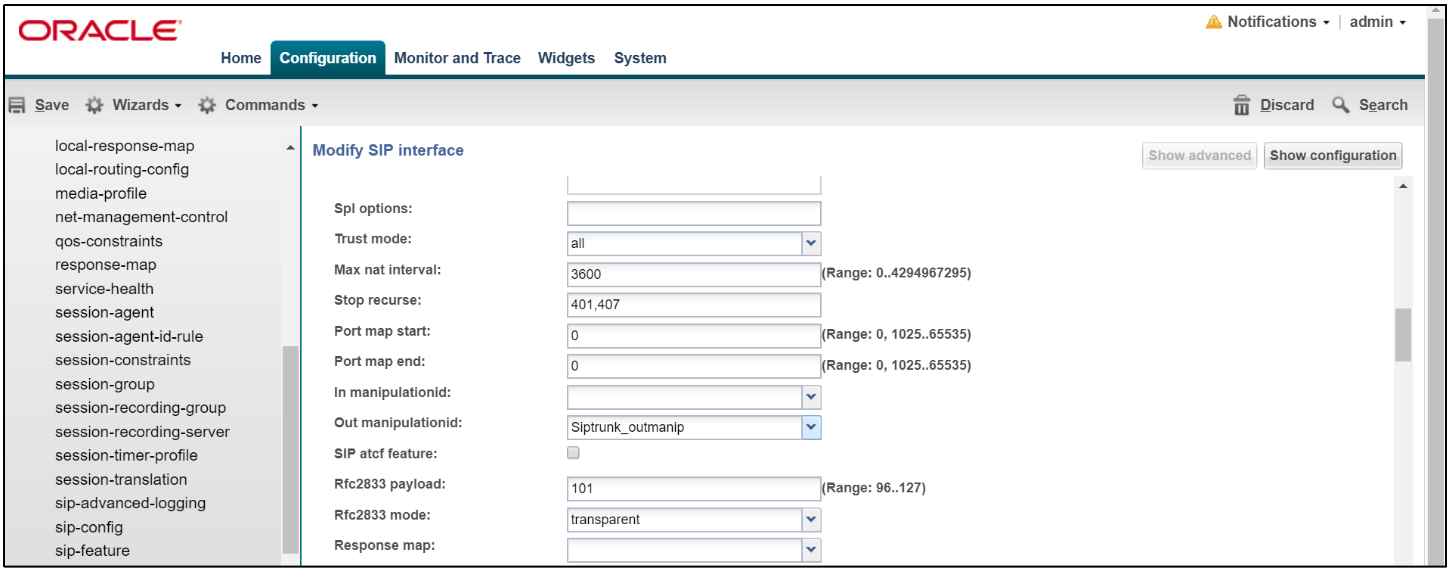


Add SIP manipulation / header rule / element rule

| | |
|---|---|
| Name: | Tohost |
| Parameter name: | |
| Type: | uri-host |
| Action: | replace |
| Match val type: | any |
| Comparison type: | case-sensitive |
| Match value: | |
| New value: | $REMOTE_IP |

## 5.24 Applying the trunk side SIP manipulations to Trunk SIP Interface

The Siptrunk_outmanip sip-manipulation is applied as the out-manipulationid in the sip-interface facing SIP Trunk



Modify SIP interface

Spl options:

Trust mode: all

Max nat interval: 3600 (Range: 0..4294967295)

Stop recurse: 401,407

Port map start: 0 (Range: 0, 1025..65535)

Port map end: 0 (Range: 0, 1025..65535)

In manipulationid:

Out manipulationid: Siptrunk_outmanip

SIP atcf feature: ☐

Rfc2833 payload: 101 (Range: 96..127)

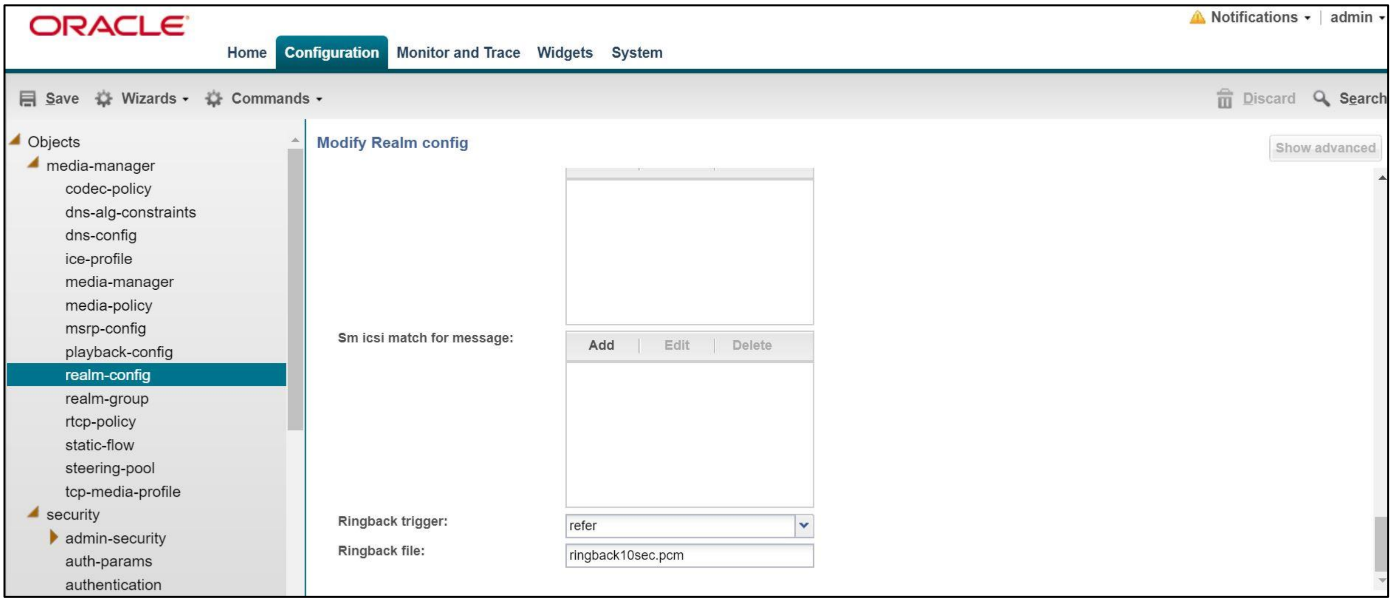
Rfc2833 mode: transparent

Response map:

# 6 Ringback Configuration

## 6.1 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 are configured on the realm facing the trunk.



Modify Realm config

Sm icsi match for message:

Ringback trigger: refer

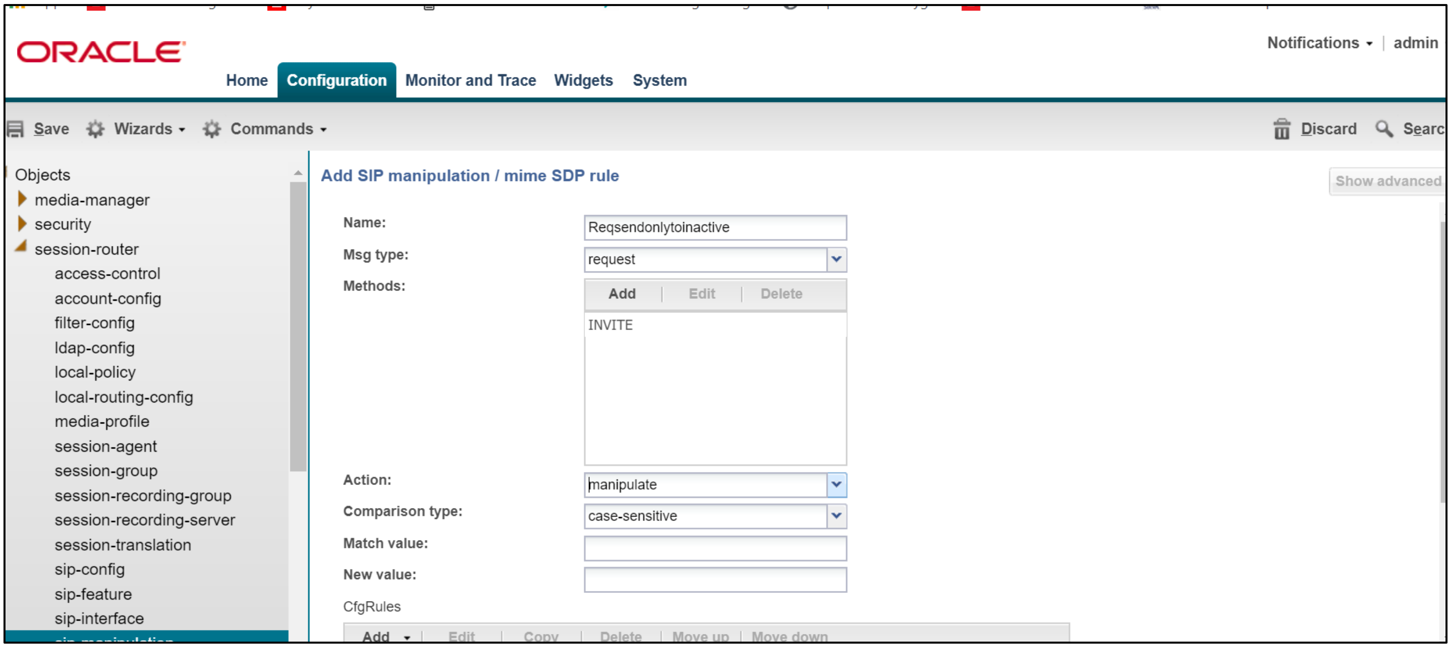
Ringback file: ringback10sec.pcm

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 and 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.

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 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 |



Add SIP manipulation / mime SDP rule

Name: Reqsendonlytoinactive

Msg type: request

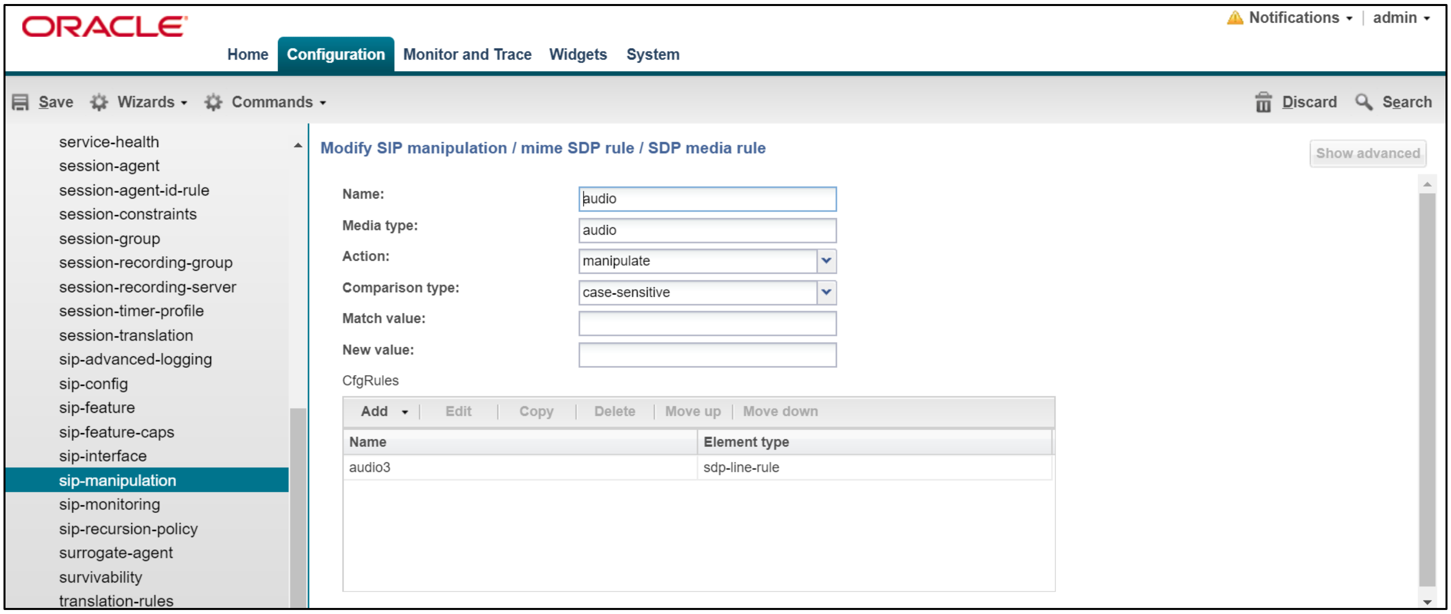
Methods: INVITE

Action: manipulate

Comparison type: case-sensitive

Match value:

New value:

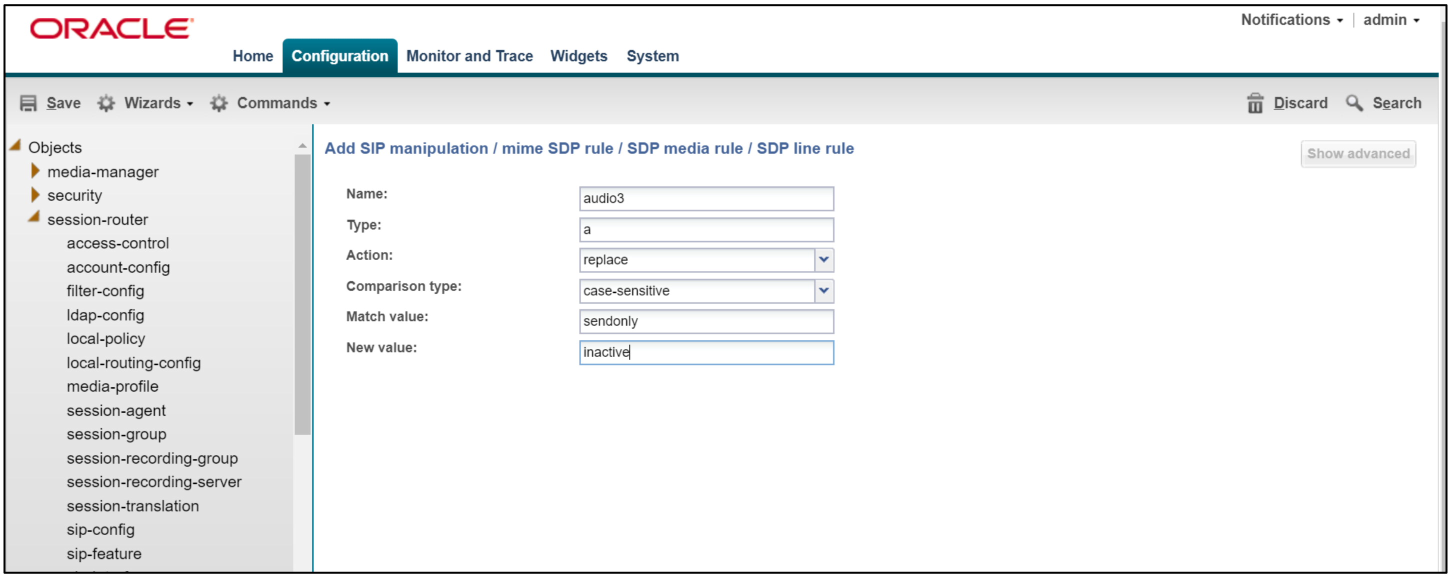


Modify SIP manipulation / mime SDP rule / SDP media rule

| | |
|---|---|
| Name: | audio |
| Media type: | audio |
| Action: | manipulate |
| Comparison type: | case-sensitive |
| Match value: | |
| New value: | |

CfgRules

| Name | Element type |
|---|---|
| audio3 | sdp-line-rule |

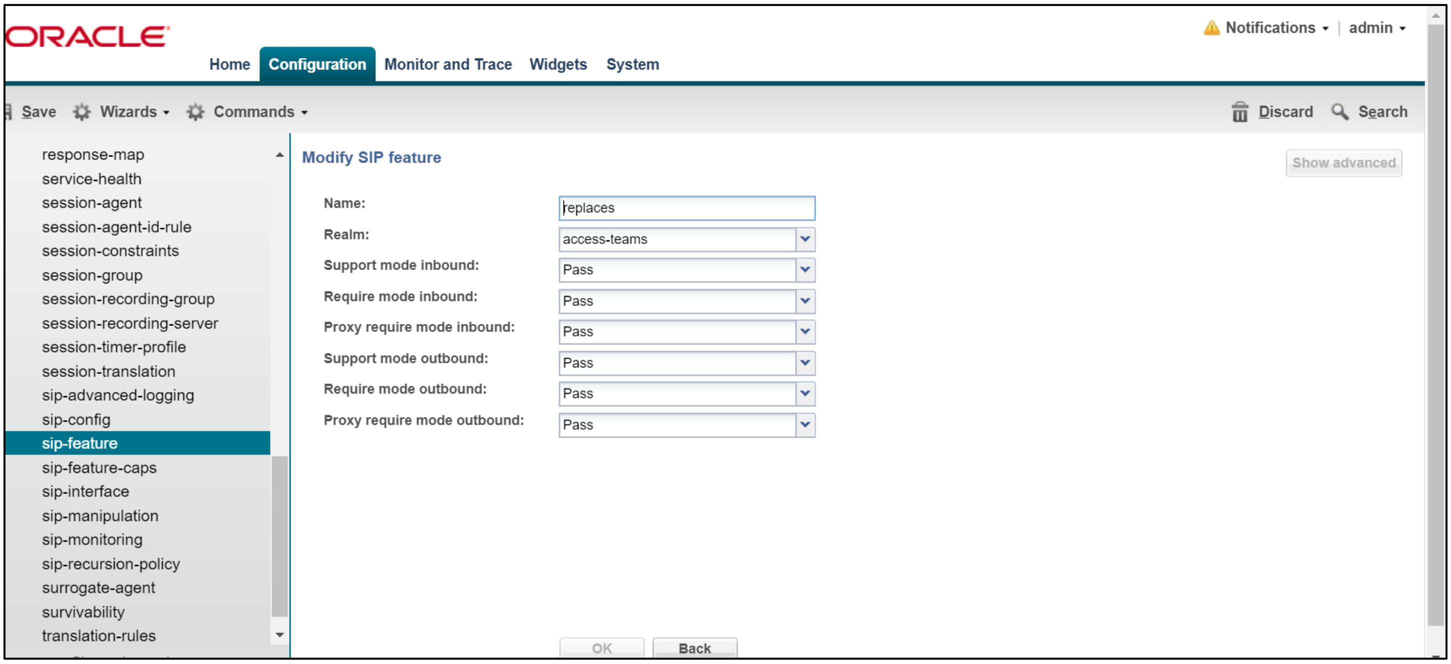


Add SIP manipulation / mime SDP rule / SDP media rule / SDP line rule

| | |
|---|---|
| Name: | audio3 |
| Type: | a |
| Action: | replace |
| Comparison type: | case-sensitive |
| Match value: | sendonly |
| New value: | inactive |

## 6.2 Consultative transfer configuration

The following sip-feature needs to be configured to enable support for the replaces to enable successful consultative transfer.



Modify SIP feature

| | |
|---|---|
| Name: | replaces |
| Realm: | access-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 |

Configure the following sip-profile and apply to the Teams sip interface.

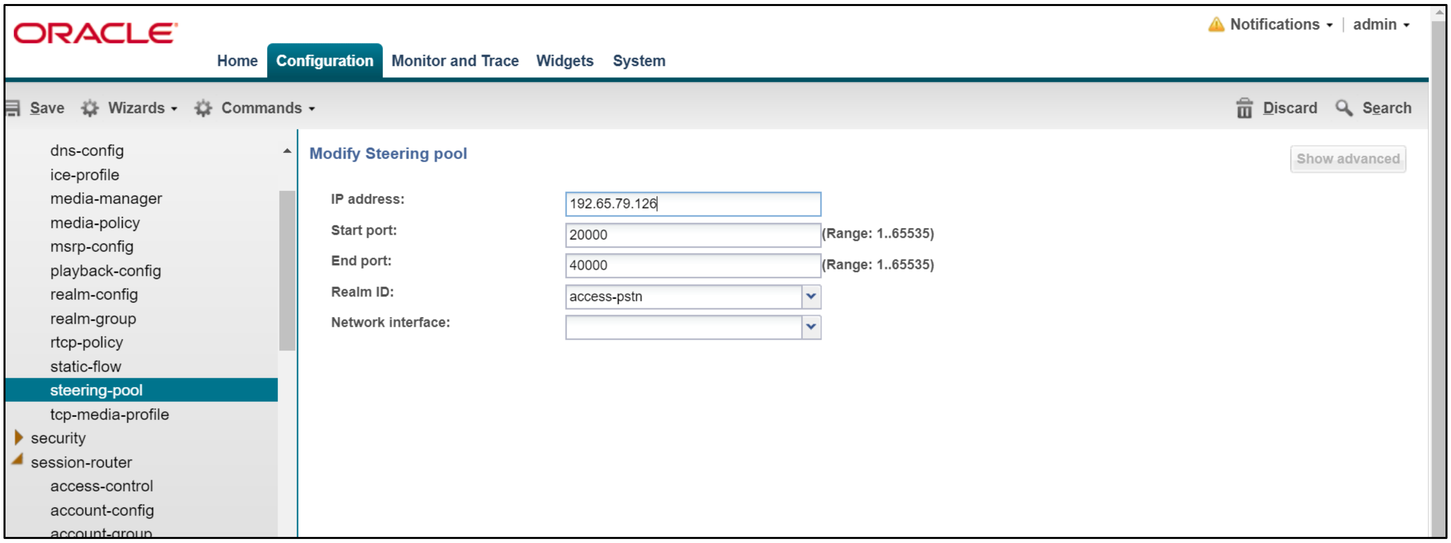
Note:The sip-profile element is available only through te CLI now.the GUI will be enhanced to support this in later releases.
To access the sip-profile element go to configure terminal->session-router->sip-profile

**sip-profile**

| | |
|---|---|
| name | foreplace |
| 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 |

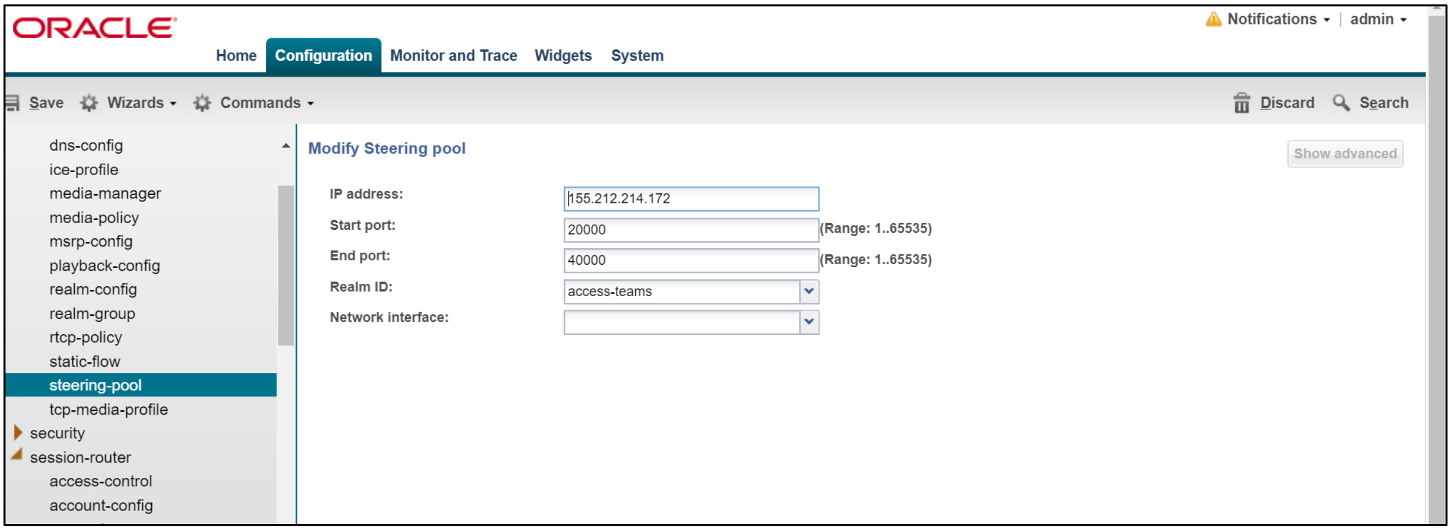
## 6.3 Configure steering pool

Steering-pool configs allows configuration to assign IP address(es), ports & a realm.



Modify Steering pool

| | |
|---|---|
| IP address: | 192.65.79.126 |
| Start port: | 20000 (Range: 1..65535) |
| End port: | 40000 (Range: 1..65535) |
| Realm ID: | access-pstn |
| Network interface: | |



Modify Steering pool

IP address: 155.212.214.172

Start port: 20000 (Range: 1..65535)

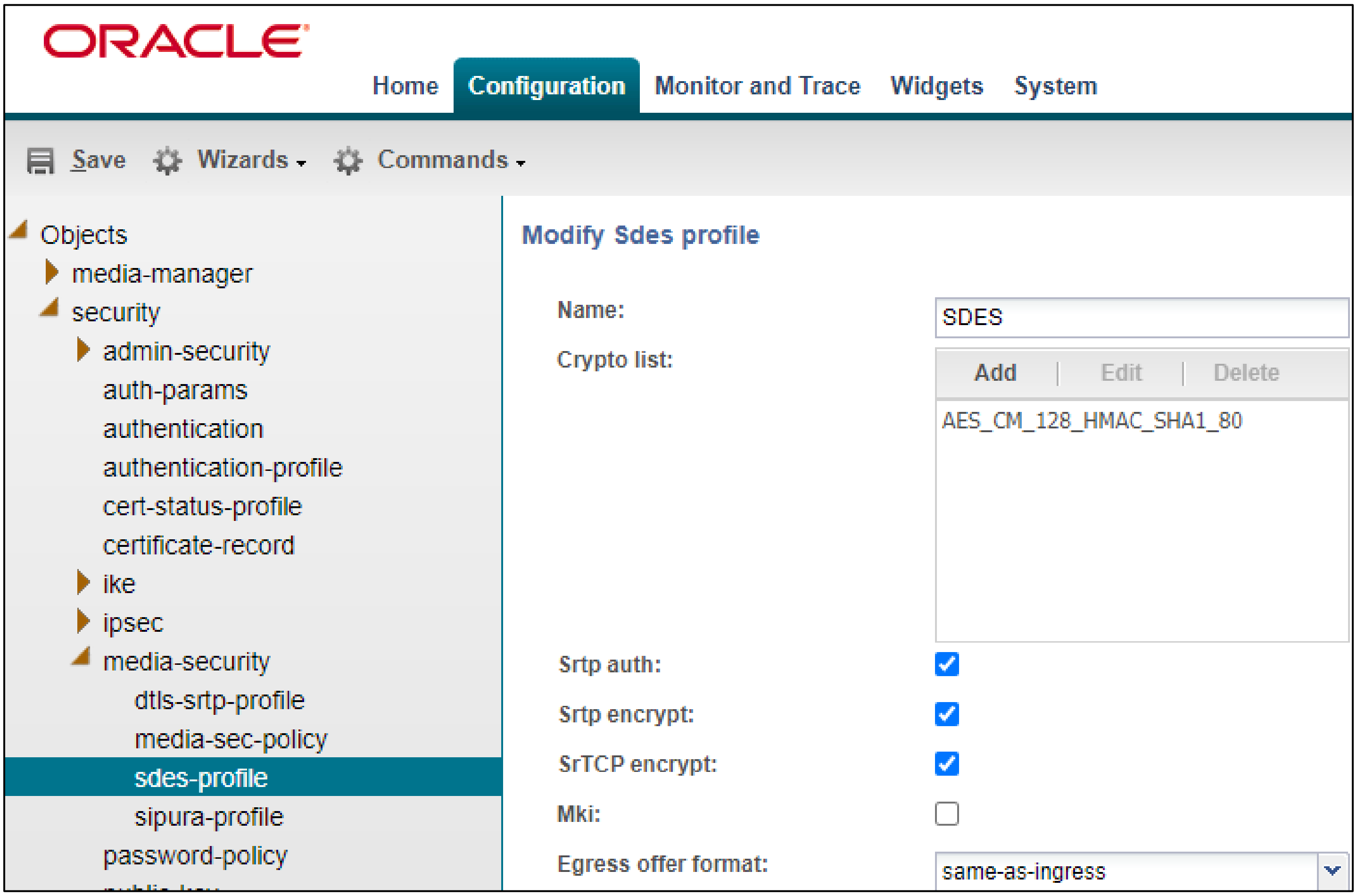
End port: 40000 (Range: 1..65535)

Realm ID: access-teams

Network interface:

## 6.4 Configure SDES profile

Create a SDES profile as shown below – Microsoft only supports AES_CM_128_HMAC_SHA1_80 encryption. Navigate to media-manager -* security -* sdes-profile.



Modify Sdes profile

Name: SDES

Crypto list: AES_CM_128_HMAC_SHA1_80

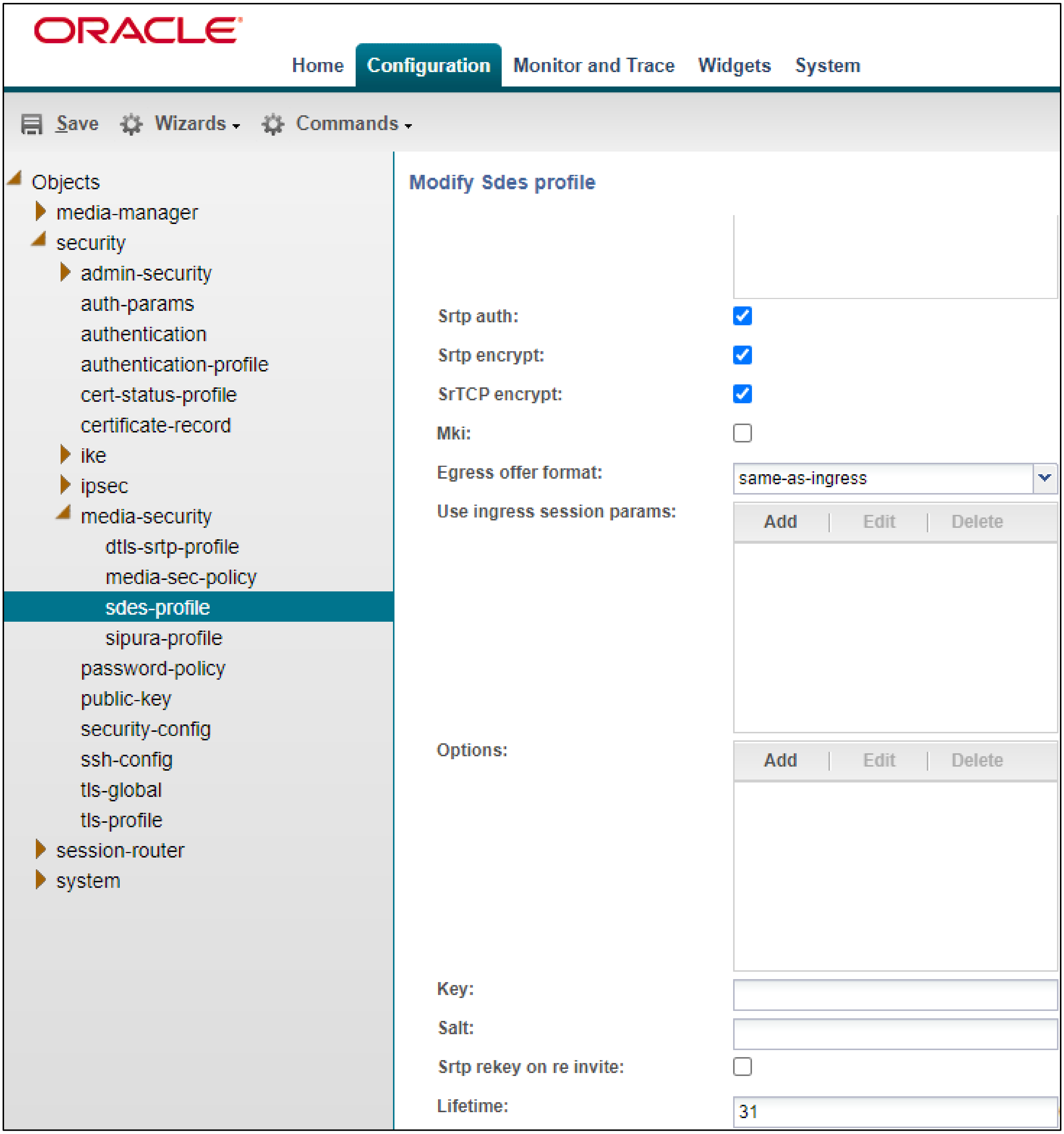
Srtp auth: ☑

Srtp encrypt: ☑

SrTCP encrypt: ☑

Mki: □

Egress offer format: same-as-ingress



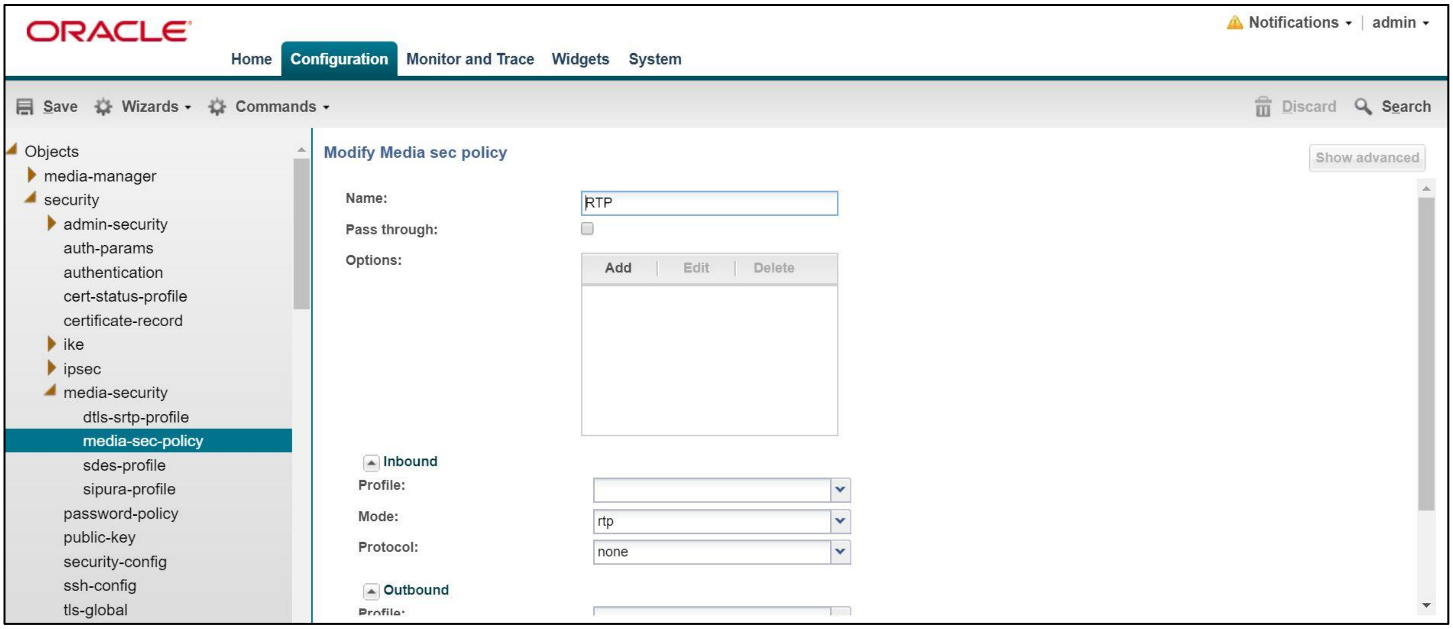
Modify Sdes profile

| | |
|---|---|
| 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 |

Please make sure to include the lifetime value of 31 in the SDES profile as shown above.

## 6.5 Media-sec-policy

A media-sec-policy configuration creates a policy to allocate media security rule and apply it to the realm configuration.



Modify Media sec policy

Name: RTP

Pass through: ☐

Options:

Inbound

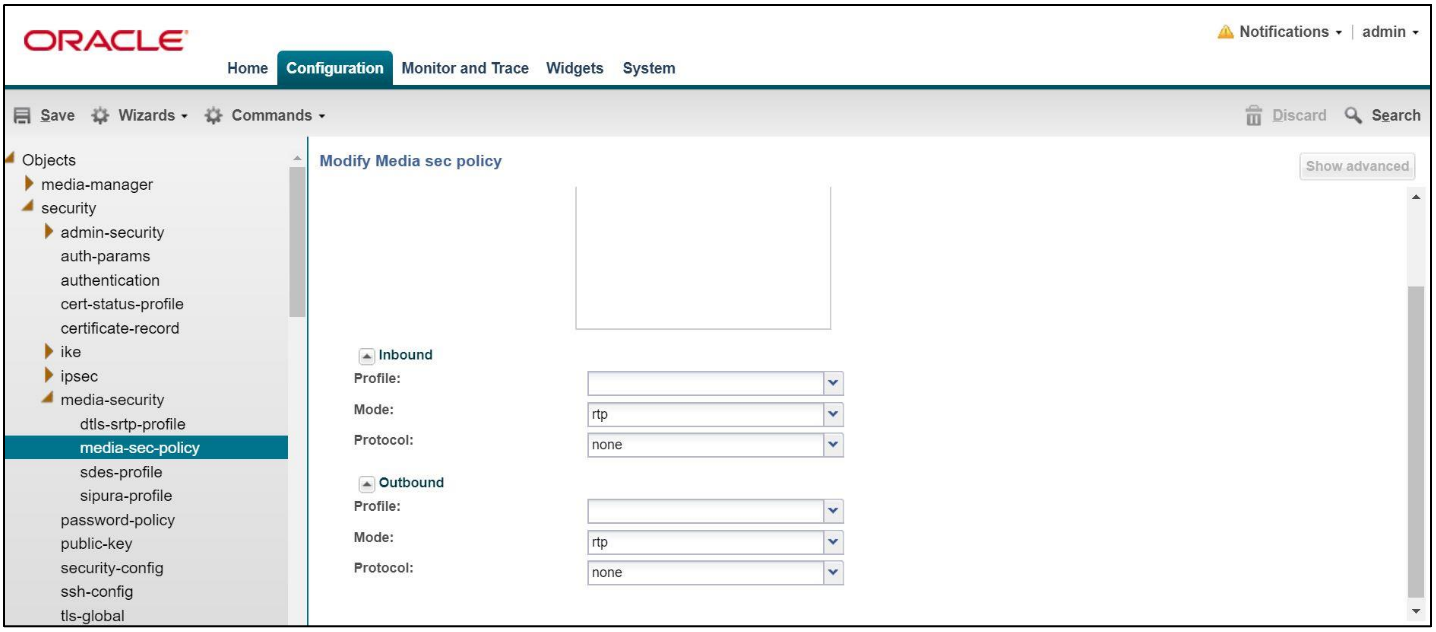
Profile:

Mode: rtp

Protocol: none

Outbound

Profile:



Modify Media sec policy

Inbound

Profile:

Mode: rtp

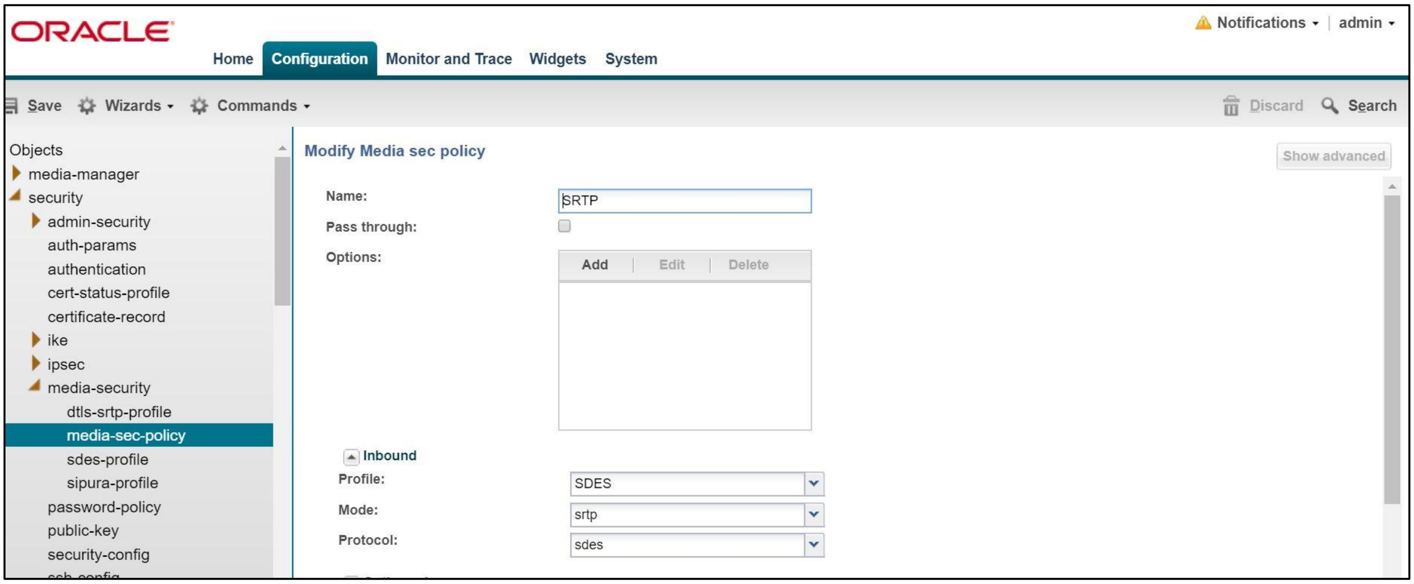
Protocol: none

Outbound

Profile:

Mode: rtp

Protocol: none



Modify Media sec policy

Name: SRTP

Pass through: □

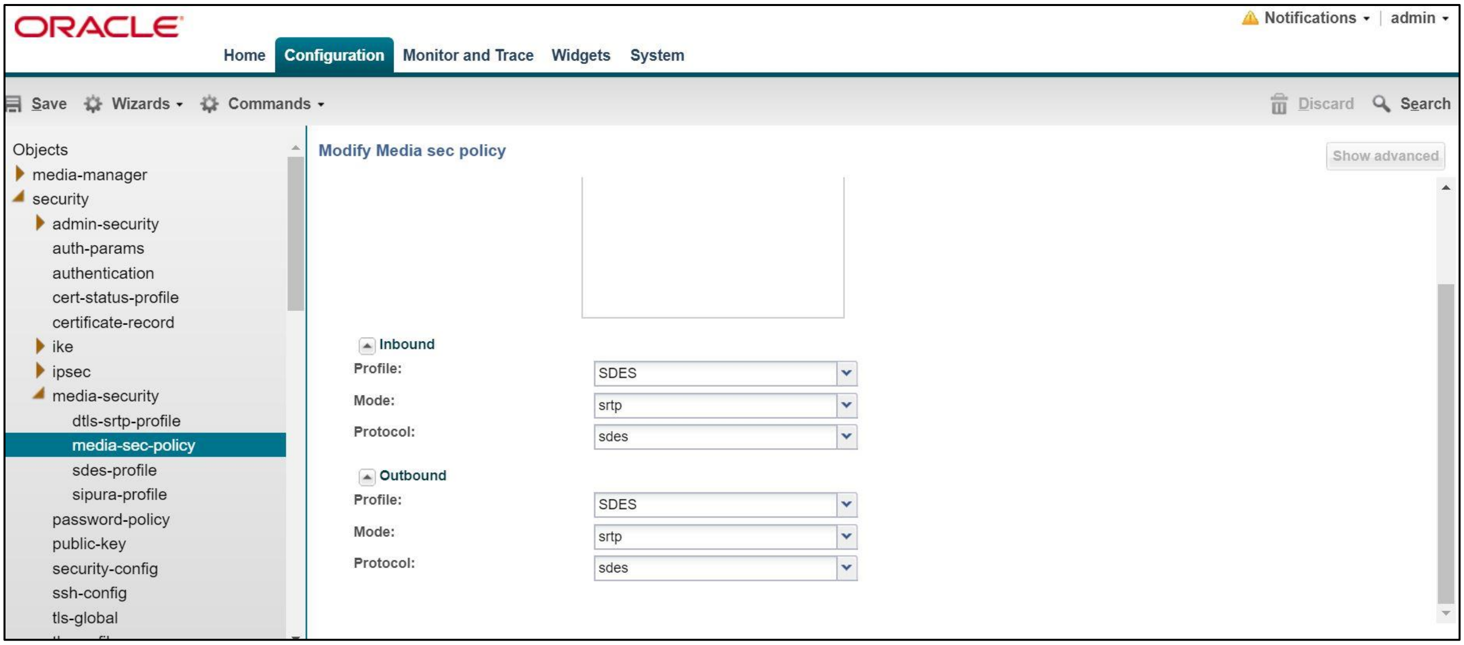
Options:

Inbound

Profile: SDES

Mode: srtp

Protocol: sdes



Modify Media sec policy

Inbound

Profile: SDES

Mode: srtp

Protocol: sdes

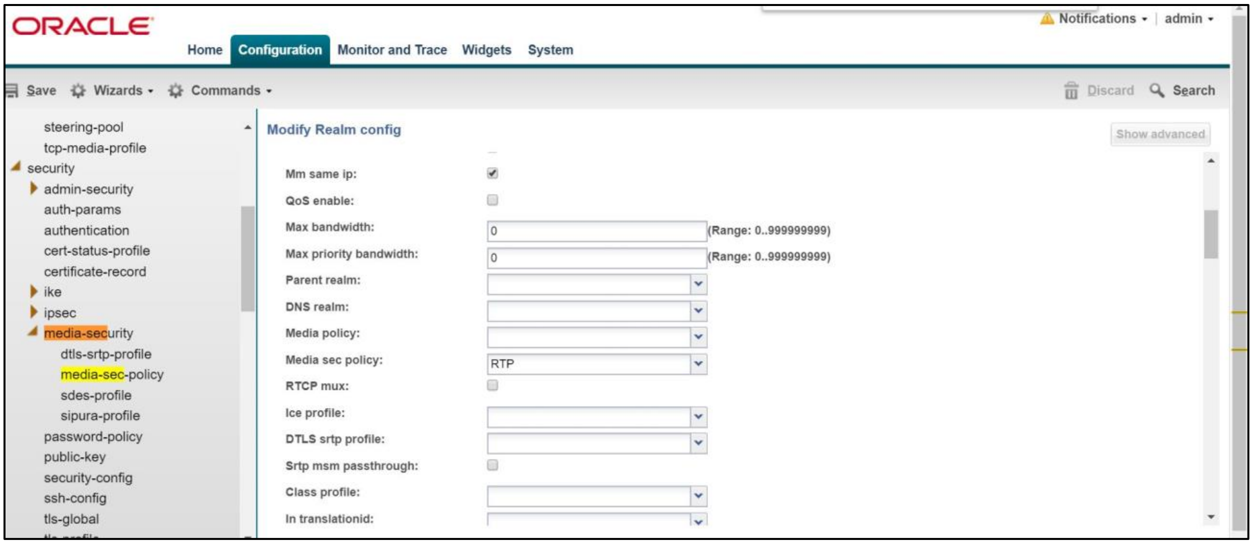
Outbound

Profile: SDES

Mode: srtp

Protocol: sdes

The RTP media-sec-policy is applied on the Access-pstn realm and SRTP media-sec-policy is applied on the Access-teams realm,as shown below.

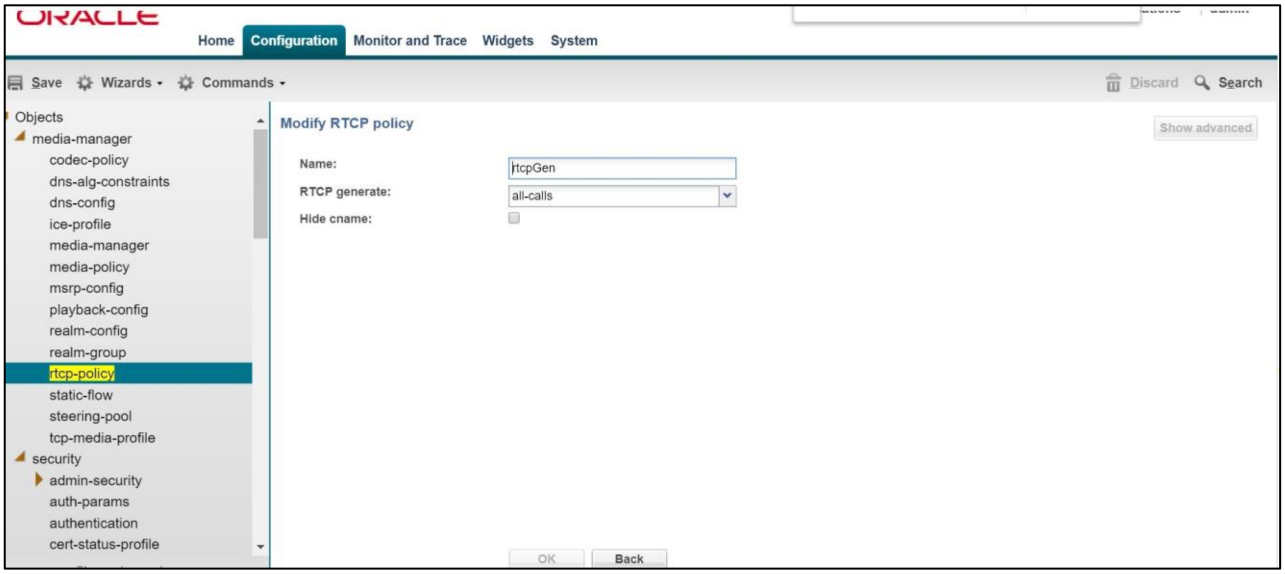


Modify Realm config

| | |
|---|---|
| Mm same ip: | ☑ |
| QoS enable: | □ |
| Max bandwidth: | 0 (Range: 0..999999999) |
| Max priority bandwidth: | 0 (Range: 0..999999999) |
| Parent realm: | |
| DNS realm: | |
| Media policy: | |
| Media sec policy: | RTP |
| RTCP mux: | □ |
| Ice profile: | |
| DTLS srtp profile: | |
| Srtp msm passthrough: | □ |
| Class profile: | |
| In translationid: | |

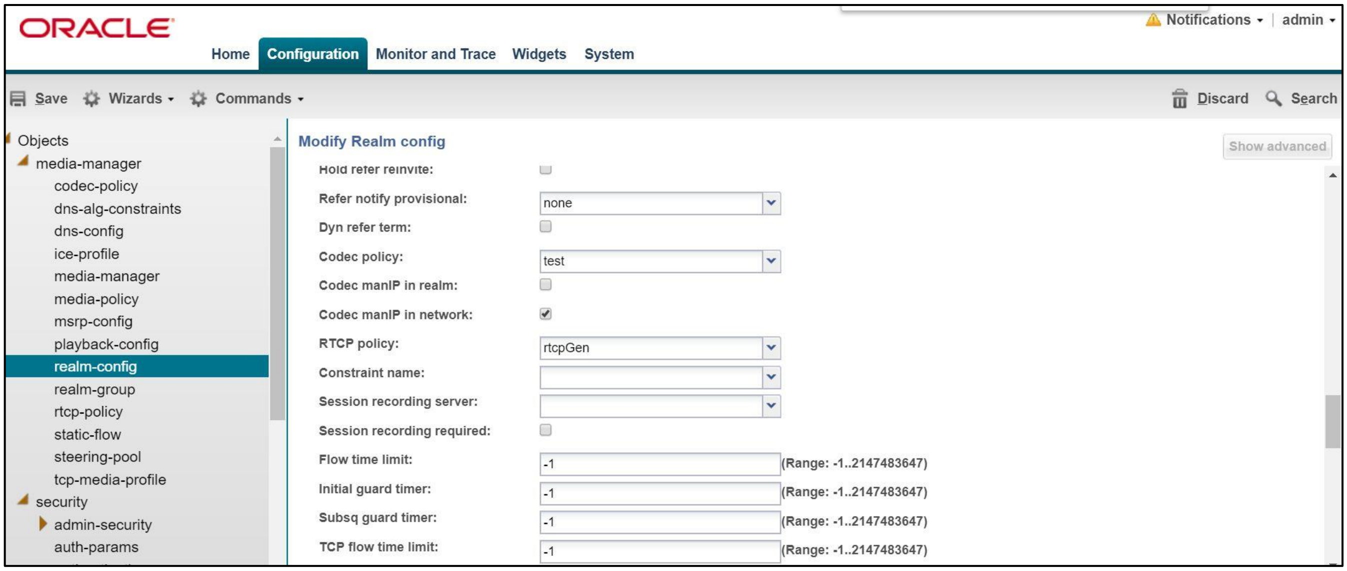
## 6.6 Configure RTCP Policy

The following RTCP policy needs to configured to generate RTCP reports towards Teams. It is applied on the realm facing Teams. It can be enabled on the realm - Access-teams.Go to Media-manager->rtcp-policy to configure rtcp-policy.



Modify RTCP policy

| | |
|---|---|
| Name: | rtcpGen |
| RTCP generate: | all-calls |
| Hide cname: | □ |



Modify Realm config

Hold refer reinvite: □
Refer notify provisional: none
Dyn refer term: □
Codec policy: test
Codec manIP in realm: □
Codec manIP in network: ☑
RTCP policy: rtcpGen
Constraint name:
Session recording server:
Session recording required: □
Flow time limit: -1 (Range: -1..2147483647)
Initial guard timer: -1 (Range: -1..2147483647)
Subsq guard timer: -1 (Range: -1..2147483647)
TCP flow time limit: -1 (Range: -1..2147483647)

# 7 Existing SBC configuration

If the SBC being used with Microsoft Teams is an existing SBC with functional configuration with a SIP trunk, following configuration elements are required:

- New realm-config
- Configuring a certificate for SBC Interface
- TLS-Profile
- Enable DNS
- New sip-interface
- New session-agent
- New-Session-Agent-Group
- New steering-pools
- New Local-policy
- Media-profile
- Codec-policy
- SDES Profile
- Media-sec-Policy
- Sip-manipulations
- Ice-profile
- RTCP policy
- Ringback configuration

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

# 8 Configuration for Emergency Calling

As part of Oracle's continued partnership with Microsoft, the Oracle Communications Session Border Controller is fully certified with Microsoft Teams Direct Routing for E911 compatibility as well as an Elin Capable Gateway.

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-border-controllers

For more information on how to configure emergency services in your Microsoft Teams Tenant, please refer to the documentation at the link below.

https://docs.microsoft.com/en-us/microsoftteams/what-are-emergency-locations-addresses-and-call-routing

https://docs.microsoft.com/en-us/microsoftteams/configure-dynamic-emergency-calling

https://docs.microsoft.com/en-us/microsoftteams/direct-routing-configure#configure-voice-routing

The following will outline how to configure your Oracle SBC to handle E911 from Microsoft Teams, as well as setting up Oracle SBC Elin Gateway configuration.

## 8.1 E911

*Note: This is a configuration example, and would be an additional configuration added to what is outlined throughout this document.*

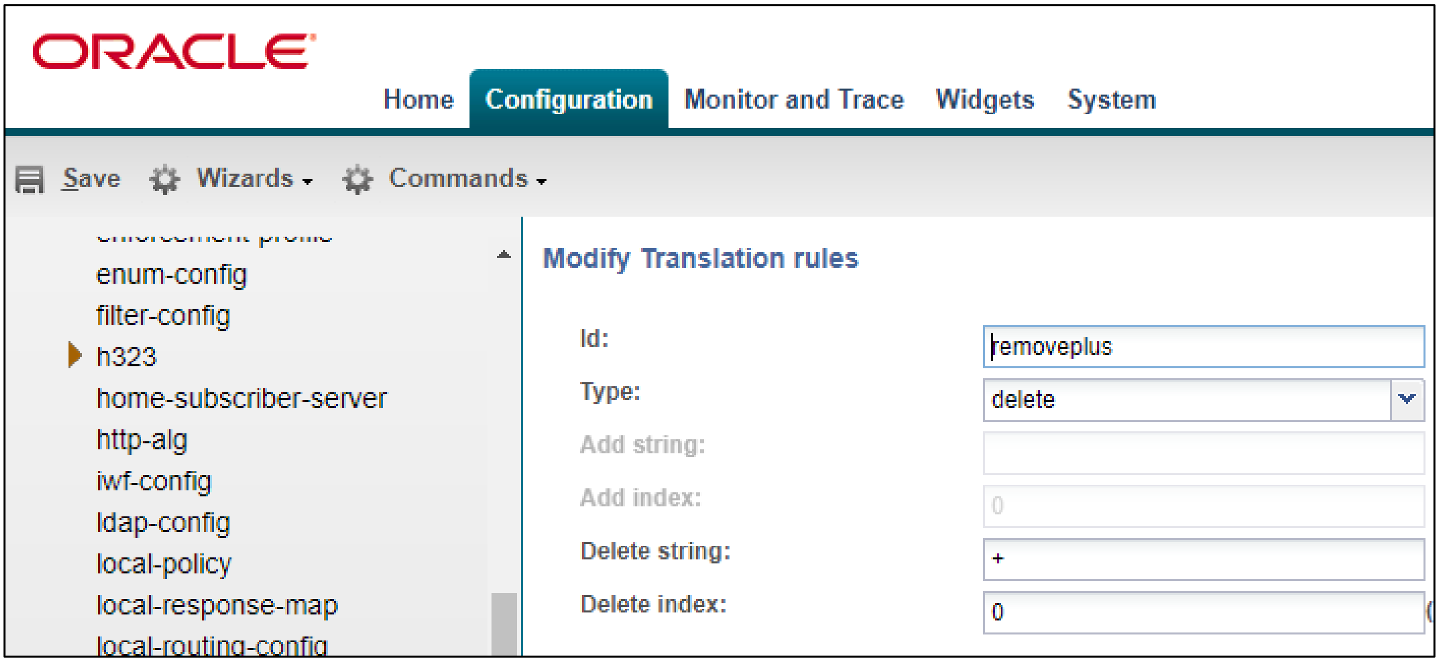
### 8.1.1 Session Translations Config

At the time of testing, MSFT Teams sends 911 with a leading plus (+). We recommend removing that leading + on ingress so ensure the call is not considered international and rejected. We do this via a session translation rule, which in turn gets assigned to the Teams facing Realm on the SBC. If you already have a session translation assigned to this Realm, you can add the translation rule to the list in that session translation:

### 8.1.2 Translation Rule

GUI Path: session-router/translation-rule

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



Modify Translation rules

| | |
|---|---|
| Id: | removeplus |
| Type: | delete |
| Add string: | |
| Add index: | 0 |
| Delete string: | + |
| Delete index: | 0 |

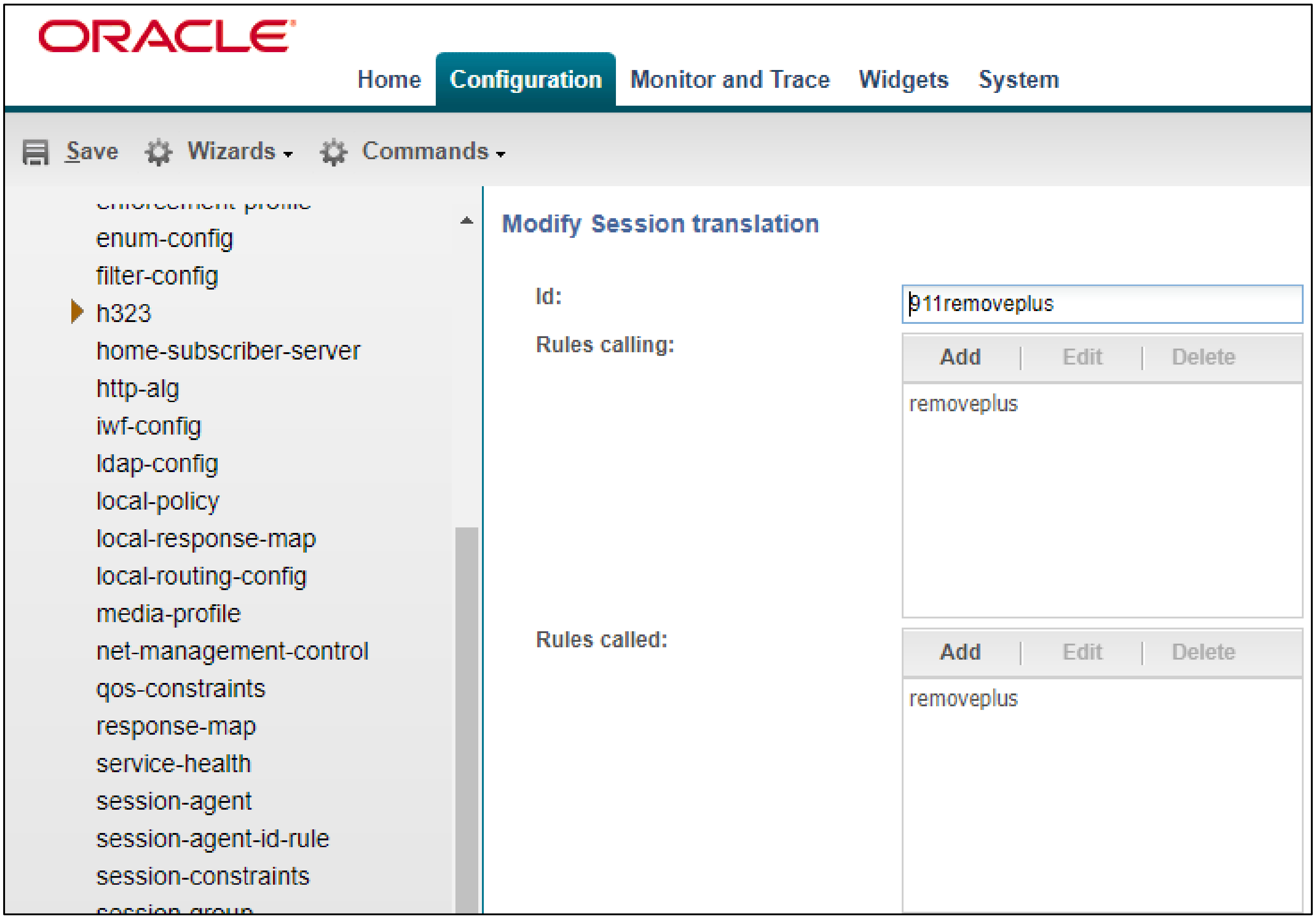
- Hit Ok at the bottom

Next, the translation rule needs to be assigned to a session translation before it can be added to the Teams facing Realm:

### 8.1.3 Session Translation

GUI Path: session-router/session-translation

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



Modify Session translation

Id: 911removeplus

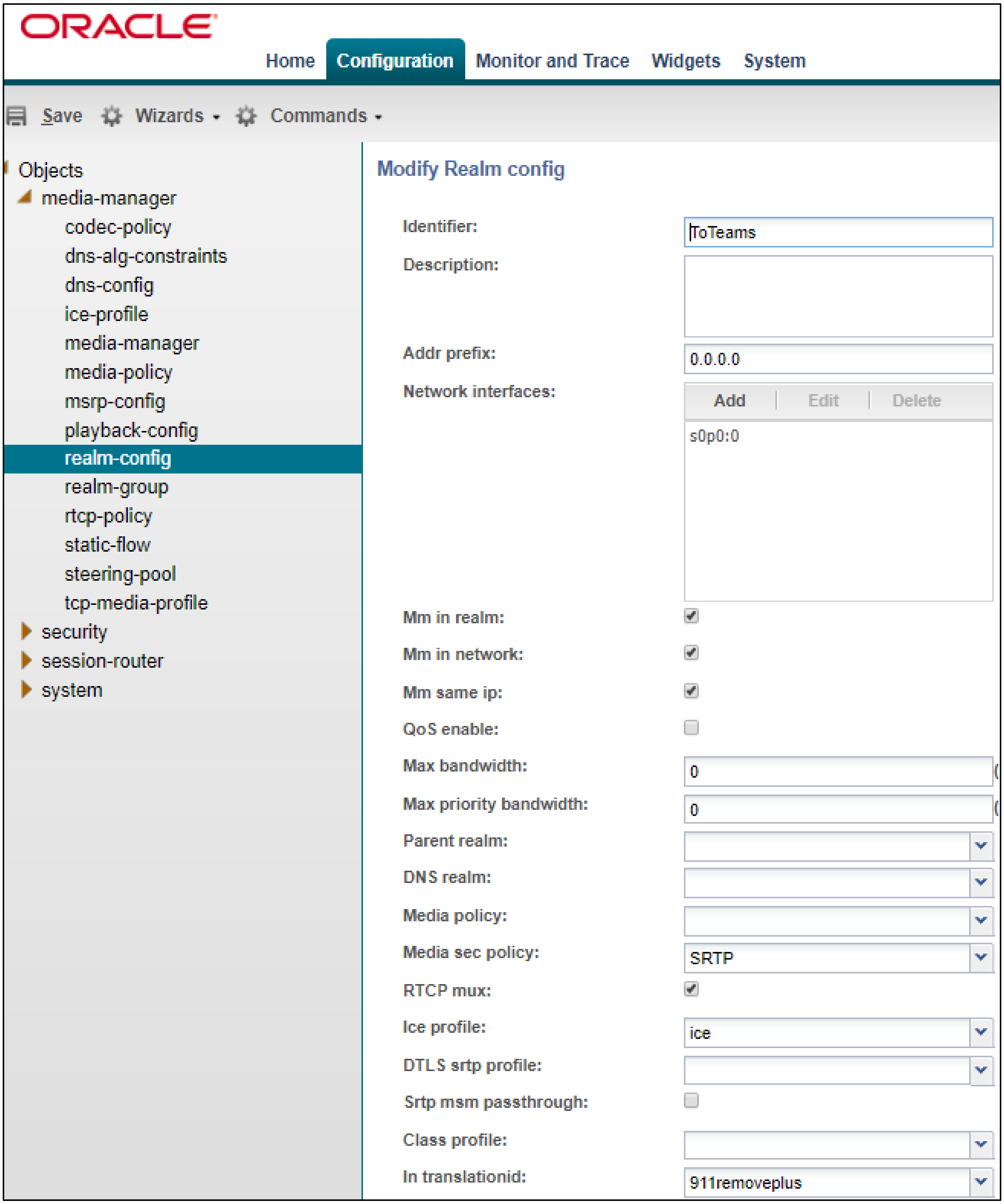
Rules calling: removeplus

Rules called: removeplus

As you can see above, the translation rule we configured is added as both rules calling and rules called in the session translation.  Now we assign the session translation to the Realm as the in-translation-id:

### *8.1.4* Translation Added to Realm

GUI Path: media-manager/realm-config



Modify Realm config

| | |
|---|---|
| Identifier: | ToTeams |
| Description: | |
| Addr prefix: | 0.0.0.0 |
| Network interfaces: | s0p0:0 |
| Mm in realm: | ☑ |
| Mm in network: | ☑ |
| Mm same ip: | ☑ |
| QoS enable: | □ |
| Max bandwidth: | 0 |
| Max priority bandwidth: | 0 |
| Parent realm: | |
| DNS realm: | |
| Media policy: | |
| Media sec policy: | SRTP |
| RTCP mux: | ☑ |
| Ice profile: | ice |
| DTLS srtp profile: | |
| Srtp msm passthrough: | □ |
| Class profile: | |
| In translationid: | 911removeplus |

### 8.1.5 Emergency Session Handling

The Oracle® Enterprise Session Border Controller provides a mechanism to handle emergency sessions from non-allowed endpoints/agents. An endpoint is designated as non-allowed if it fails the admission control criteria specified by the allow-anonymous parameter in the Sip Inerface/SIP Ports configuration element.  To enable this feature, you will need to configure the following:

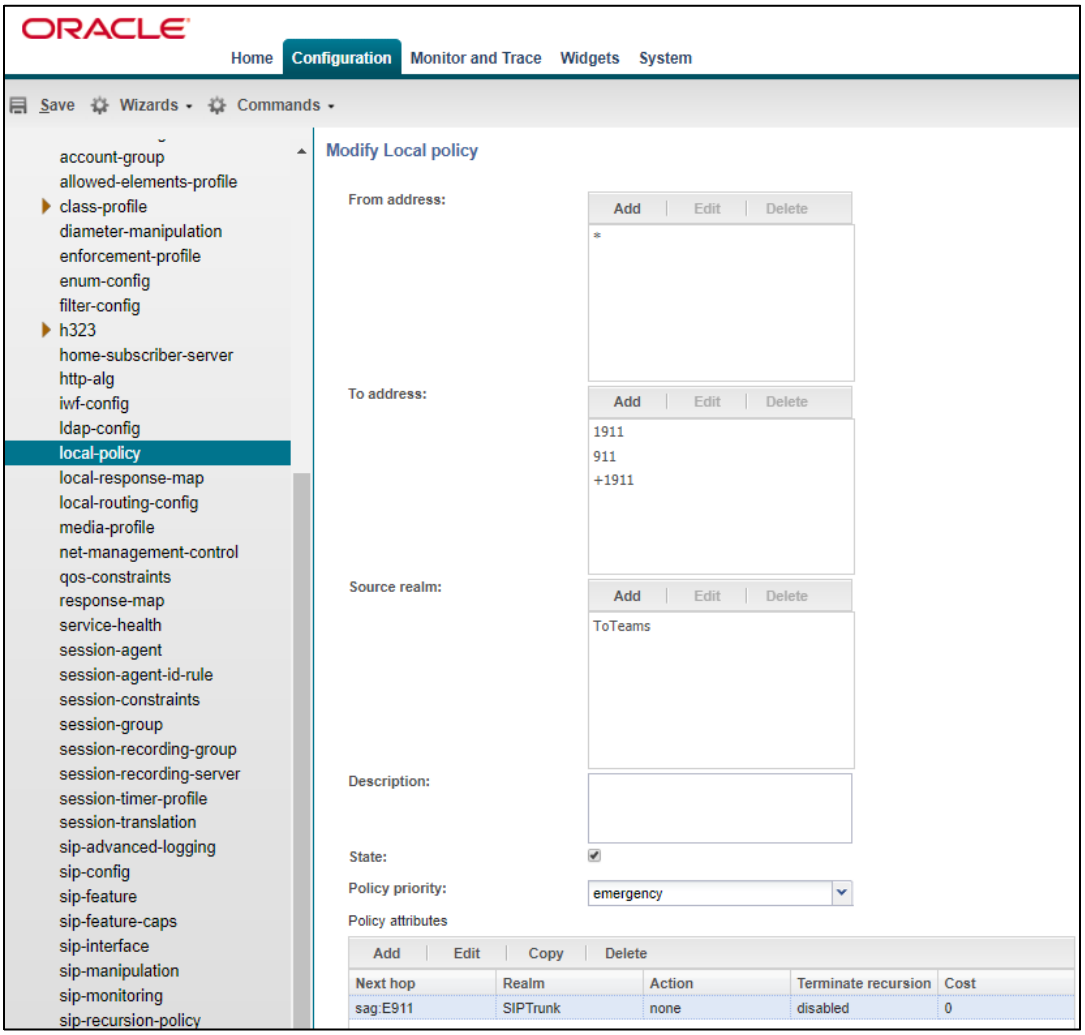
- Local Policy to Match and Route emergency calls to correct destination with policy priority set to emergency
- Enable anonymous-priority on Ingress Sip Interface

*Note:  This is just a configuration example.  This note assumes any session agents or session group for PSAP has already been configured:*

### *8.1.6* Local Policy Route for Emergency Calls

GUI Path:  session-router/local-policy

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



Modify Local policy

From address: *

To address: 1911<br>911<br>+1911

Source realm: ToTeams

Description:

State: ☑

Policy priority: emergency

Policy attributes

| Next hop | Realm | Action | Terminate recursion | Cost |
|---|---|---|---|---|
| sag:E911 | SIPTrunk | none | disabled | 0 |

You would also configure a policy attribute to route emergency calls to their proper destination.  In this example, we have created a SAG called e911 as the destination for all emergency calls.  For instructions on how to configure Session Agents or Session Groups, please click the links for examples.

Next, we'll enable anonymous-priority field in Sip-Interface:

### *8.1.7* Sip Interface Priority

GUI Path:  Currently, this field is not available through GUI, and must be configured through ACLI

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

```
sip-interface
        state                          enabled
        realm-id                         ToTeams
        description
        sip-port
                address                        192.168.1.10
                port                        5061
                transport-protocol                  TLS
                tls-profile                   TLSTeams
                allow-anonymous                       agents-only
                multi-home-addrs
                ims-aka-profile
        uri-fqdn-domain
        options
        spl-options
        trust-mode                         all
        max-nat-interval                     3600
        nat-int-increment                    10
        nat-test-increment                    30
        sip-dynamic-hnt                      disabled
        stop-recurse                       401,407
        port-map-start                      0
        port-map-end                        0
        in-manipulationid                     RespondOPTIONS
        out-manipulationid
        sip-ims-feature                      disabled
        sip-atcf-feature                     disabled
        subscribe-reg-event                       disabled
        operator-identifier
        anonymous-priority                       emergency
```

For more information on how this feature works, please see the SCZ830 Configuration Guide, Page 4-185.

### 8.1.8 Net-Management Control

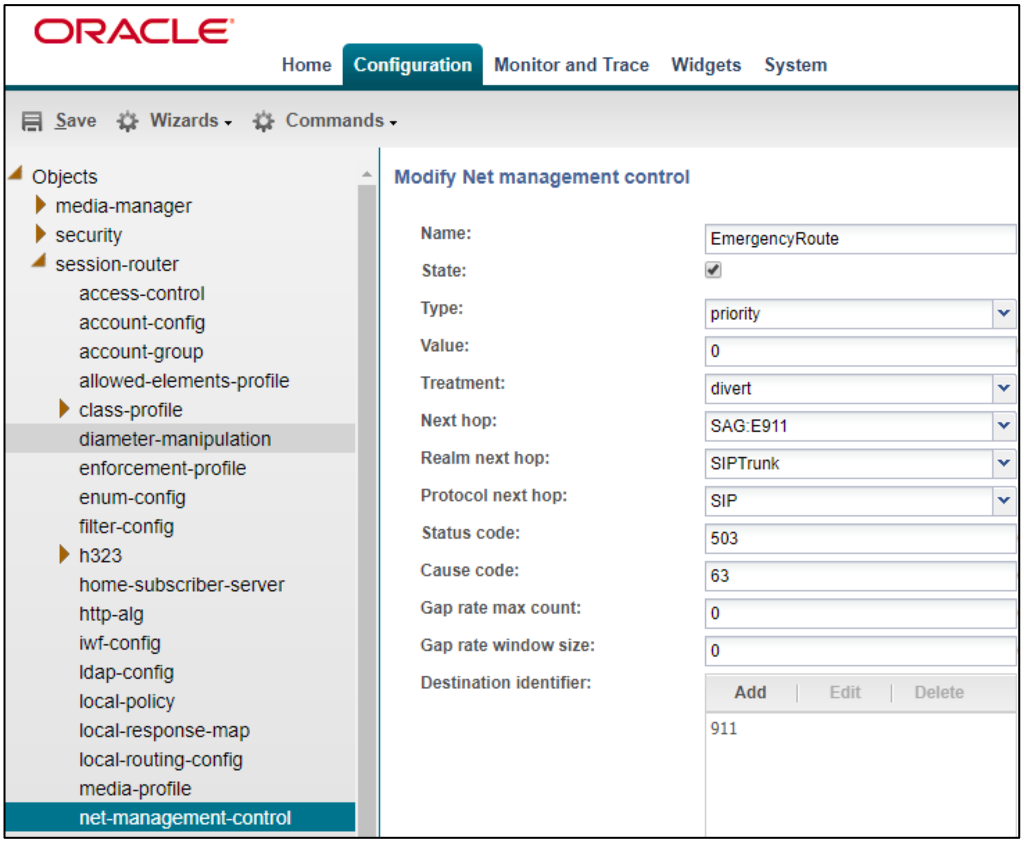
The Oracle Communications Session Border Controller supports network management controls for multimedia traffic specifically for static call gapping and 911 exemption handling. These controls limit the volume or rate of traffic for a specific set of dialed numbers or dialed number prefixes (destination codes).

To enable network management controls on your Oracle Communications Session Border Controller, you set up the net-management-control configuration and then enable the application of those rules on a per-realm basis. Each network management control rule has a unique name, in addition to information about the destination (IP address, FQDN, or destination number or prefix), how to perform network management (control type), whether to reject or divert the call, the next hop for routing, and information about status/cause codes. For more information about Network Management Controls, please refer to the Configuration Guide, Chapter 11.

GUI Path: session-router/net-management-control

ACLI Path: config t→session-router→net-management-control

Use the below example to configure net-management-control and assign it to the Teams realm. Please note, net-management-control Realm parameter is not available through the GUI, so it must be assigned via ACLI to the appropriate realm.



Modify Net management control

| | |
|---|---|
| Name: | EmergencyRoute |
| State: | ☑ |
| Type: | priority |
| Value: | 0 |
| Treatment: | divert |
| Next hop: | SAG:E911 |
| Realm next hop: | SIPTrunk |
| Protocol next hop: | SIP |
| Status code: | 503 |
| Cause code: | 63 |
| Gap rate max count: | 0 |
| Gap rate window size: | 0 |
| Destination identifier: | 911 |

*Note: Net-Management-Controls do not adhere to any constraints configured on your SBC due to the emergency nature of the call flows handled by this element.*

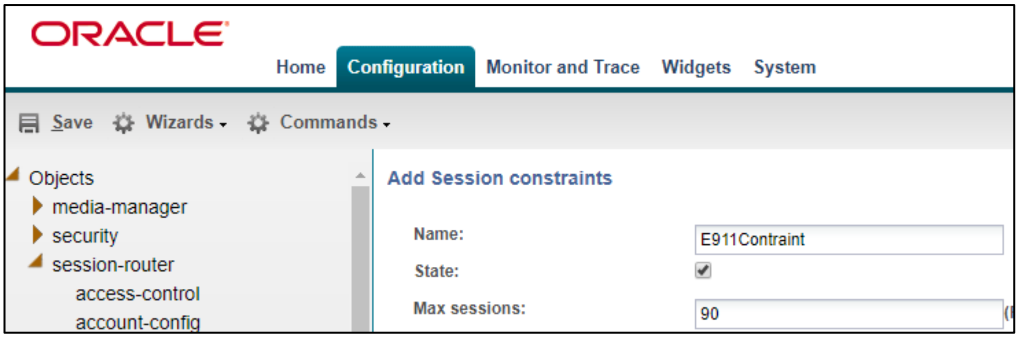
### 8.1.9 Session Constraints for E911

In order for the SBC to have the ability to handle emergency calls in high volume environment, we recommend configuring and applying session constraints for each realm on your SBC to allow a small portion of your licensed sessions to be allocated to emergency calls.

The below example is a very basic constraint setup limiting the number of calls allowed to traverse a realm. For the purposes of this example, we assume there are 100 licensed sessions on the SBC, so we'll limit the number of calls on the realms to 90, leaving 10 licensed session for emergency calls. Again, as noted above, when net management controls are configured to handle emergency traffic, constraints do not apply to those calls.

GUI Path: session-router/session-constraits

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



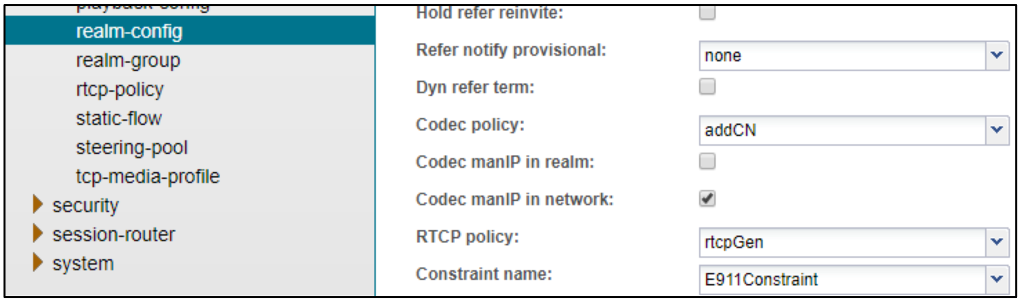
Add Session constraints

Name: E911Contraint

State: ☑

Max sessions: 90

And now we apply this constraint to realms:



Hold refer reinvite: □

Refer notify provisional: none

Dyn refer term: □

Codec policy: addCN

Codec manIP in realm: □

Codec manIP in network: ☑

RTCP policy: rtcpGen

Constraint name: E911Constraint

## 8.2 Elin Gateway

The Oracle® Enterprise Session Border Controller supports E911 ELIN for Teams-enabled Enterprises using the ELIN_Gateway SPL option. Enable this option in the global SPL configuration. The Oracle® Enterprise Session Border Controller supports up to 300 ELIN numbers simultaneously and it can reuse numbers allowing a greater number of emergency calls

For more information about the SBC's Emergency Location Identification Number (ELIN) Gateway Support, please refer to the 830 Configuration Guide, Page 19-25

GUI Path:  system/spl-config

ACLI Path:  config t→system→spl-config

The only entry required to Enable support for Elin Gateway is:

Elin-Gateway=<value>

Valid Values are either 30 or 60.  This determines how long (minutes) the SBC will retain the mapping in memory. Default value is 30.  For the purposes of testing, we increased that value to 60 minutes, as shown in the example below.

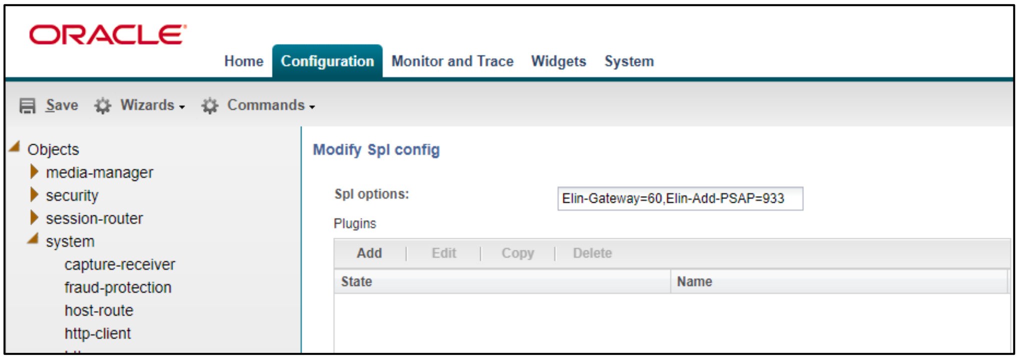
An optional configuration parameter:

Elin-Add-PSAP=<value>

Where <value> is one or more PSAP numbers, For multiple numbers, place the numbers within quotes, separate the numbers with a comma, and use no spaces. A single number does not require enclosure in quotes.

 Examples: Elin-Add-PSAP=999 and Elin-AddPSAP="999,000,114"

By Default, Oracle delivers the SBC preconfigured with the 911 and 112 Public Safety Answering Point (PSAP) callback numbers



Modify Spl config

Spl options: Elin-Gateway=60,Elin-Add-PSAP=933

Plugins

### 8.2.1 Sip-Manipulation for Teams ELIN

By Default, the Oracle SBC with Elin SPL enabled, looks at the <NAM> field in the metadata of an Invite to extract the ELIN numbers and the FROM User uri for mapping.  Since Microsoft Teams sends the ELIN information in an <Elin> field, and to avoid any issues due to ani masking on the Teams side, we have created the following sip-manipulation rule to move the information in the <Elin> field to the <Nam> field, and we replace the User part of the FROM header with the user part of the PAI.   The manipulation gets assigned to either the Teams Realm or Sip Interface, and assures proper Elin mapping in the SBC.

*Note:  If there is an existing Sip Manipulation rule already assigned as the in-manipulation-id on either the realm or sip interface, these rules would need to be added to that existing manipulation.*

GUI Path:  session-router/sip-manipulation

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

While this can be configured via the GUI, we are using the ACLI output to provide and example config for ease of viewing:

```
sip-manipulation
    name                         ELIN_Support
    description
    split-headers
    join-headers
         header-rule
         name                         StoreElin
         header-name                     Content-Type
         action                       store
         comparison-type                  case-sensitive
         msg-type                       request
         methods                        Invite
         match-value
         new-value
         element-rule
             name                         storeelin
             parameter-name                    application/pidf+xml
             type                        mime
             action                       store
             match-val-type                   any
             comparison-type                   pattern-rule
             match-value                     (<ELIN>)(.*)(</ELIN>)
             new-value
     header-rule
         name                         ReplaceNam
         header-name                     Content-Type
         action                       manipulate
         comparison-type                  case-sensitive
         msg-type                       request
         methods                        Invite
         match-value
         new-value
         element-rule
             name                         changenam
             parameter-name                    application/pidf+xml
             type                        mime
             action                       find-replace-all
             match-val-type                   any
             comparison-type                   pattern-rule
             match-value                     (<NAM>)(.*)(</NAM>)
             new-value                      $1+$StoreElin.$storeelin.$2+$3

              header-rule
         name                         PAItoFrom
         header-name                     From
         action                       manipulate
         comparison-type                  case-sensitive
         msg-type                       request
         methods                        INVITE
         match-value
         new-value

         element-rule
             name                         changeuser
             parameter-name
             type                        uri-user
             action                       replace
```

```
match-val-type                  any
comparison-type                   pattern-rule
match-value
new-value                     $PAI_USER.$0
```

# 9 Appendix A

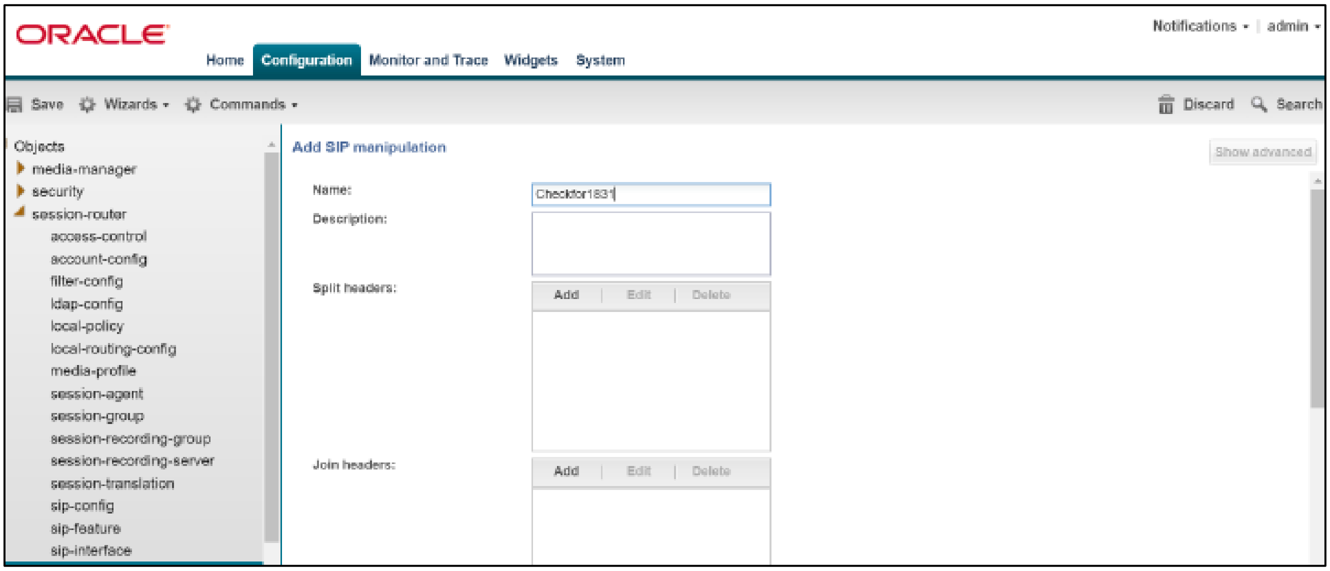
## 9.1 Ringback on inbound calls to Teams and early media

In certain deployments, a PSTN caller may experience silence on an inbound call into Teams in place of a ringback tone. When Teams receives an INVITE, after signaling 183 with SDP, Teams does not play ringback and expects the SBC to signal appropriately to the SIP Trunk provider and play local ringback. To signal the trunk to play the ringback, the SBC presents 180 Ringing to the trunk instead of the 183 Session Progress received from Teams.

In order to accommodate the 183 with SDP messages that signal early media in cases of simultaneous ringing set to IVR, we inspect the SDP of the 183s received before converting them to 180 Ringing messages. If the SDP of the 183 does not contain the IP address of SBC (which is the case when Teams clients have simultaneous ringing set to IVRs), we strip the SDP from the 183 and convert it to a 180 Ringing message and forward it to the trunk. This is achieved through the following sip-manipulation.

Apply this in the SIP Manipulation Teamsinmanip.

*Note: If running the GA release, SCZ830m1p8A, please see Appendix D prior to configuring sip manipulations in your Oracle SBC. This appendix outlines how new features added to the GA release will help simplify your configuration by eliminating the need for most, if not all required sip manipulations.*



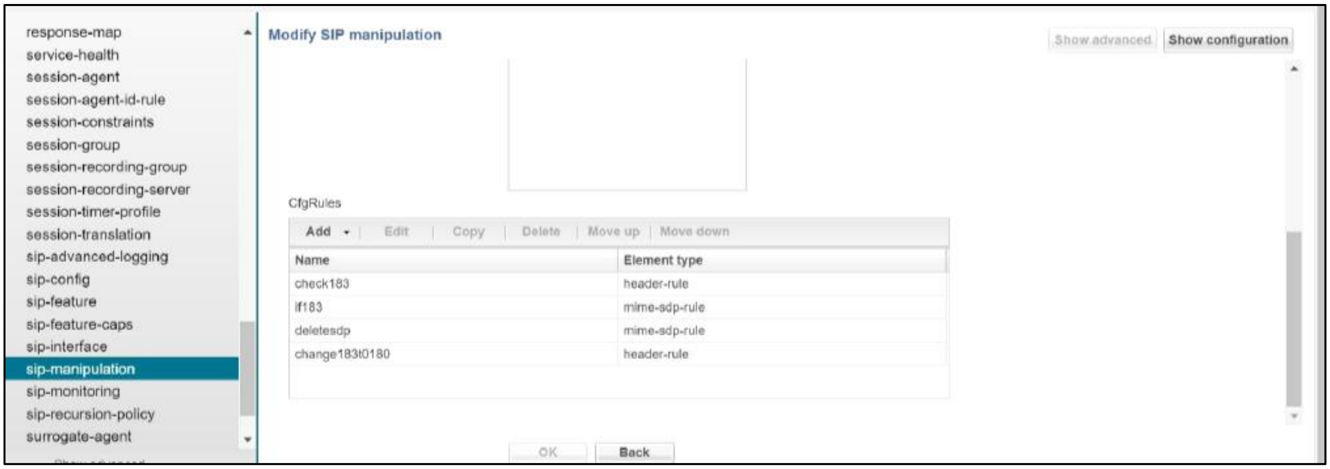
Add SIP manipulation

Name: Checkfor1831

Description:

Split headers:

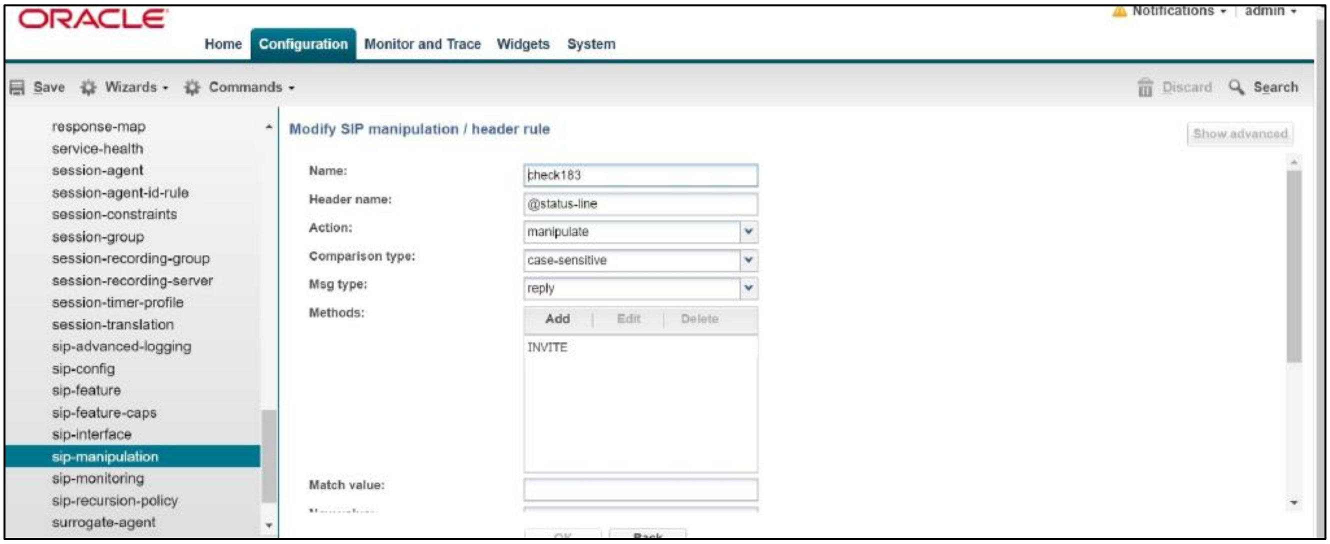
Join headers:



Modify SIP manipulation

CfgRules

| Name | Element type |
|---|---|
| check183 | header-rule |
| if183 | mime-sdp-rule |
| deletesdp | mime-sdp-rule |
| change183t0180 | header-rule |



Modify SIP manipulation / header rule

Name: check183

Header name: @status-line

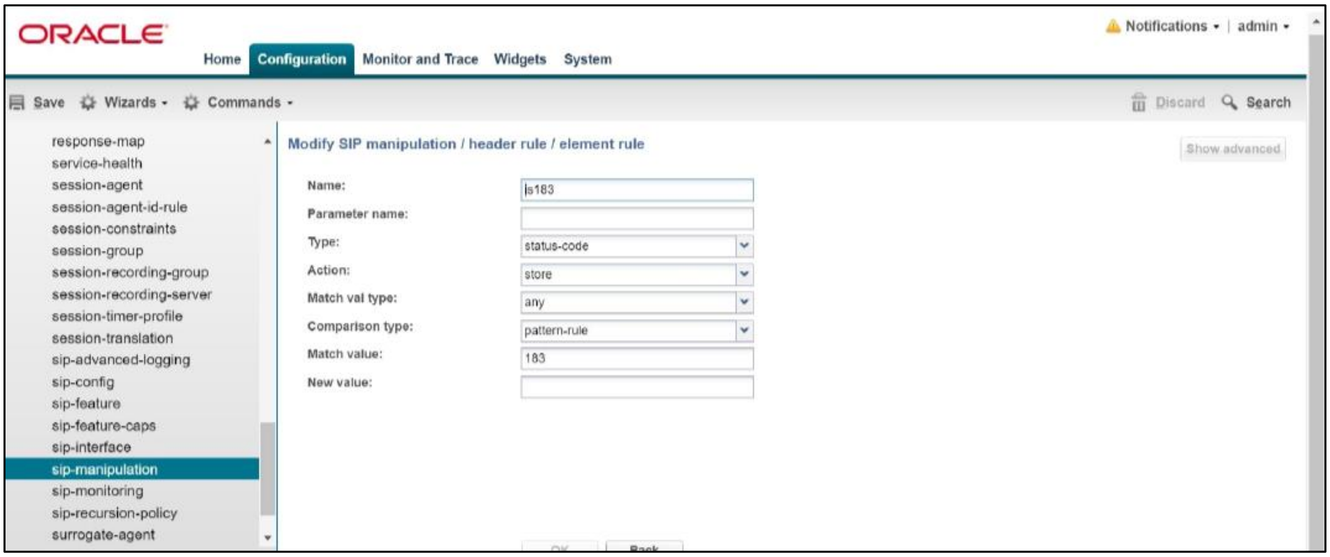
Action: manipulate

Comparison type: case-sensitive

Msg type: reply

Methods: INVITE

Match value:



Modify SIP manipulation / header rule / element rule

Name: is183

Parameter name:

Type: status-code

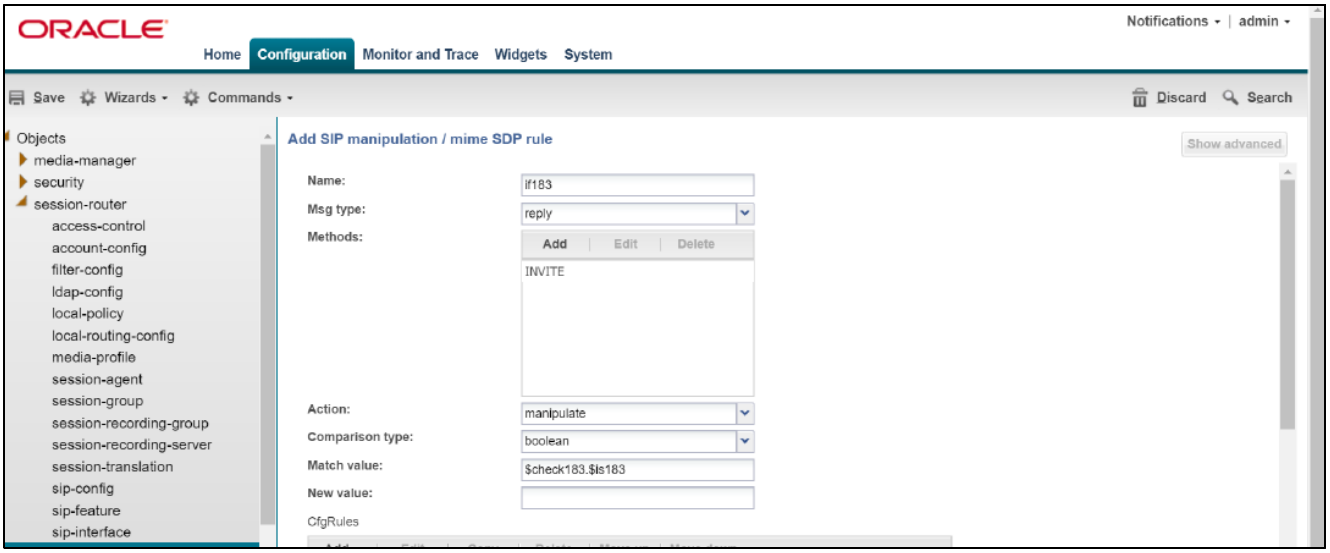
Action: store

Match val type: any

Comparison type: pattern-rule

Match value: 183

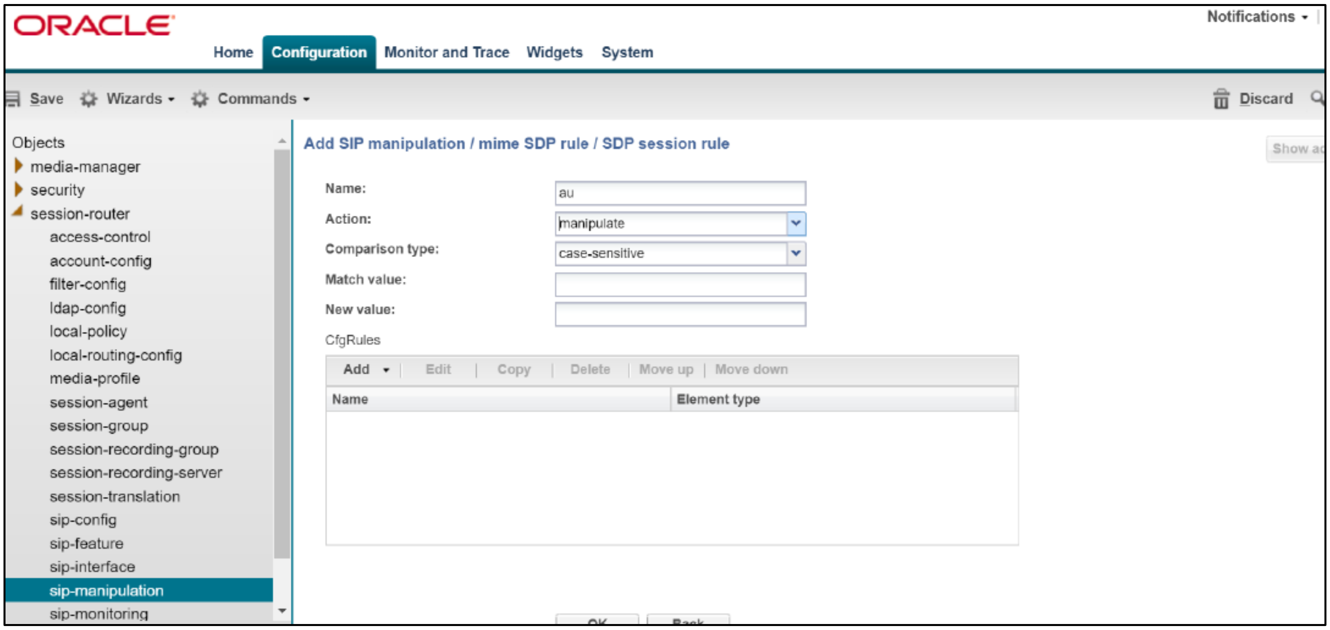
New value:



Add SIP manipulation / mime SDP rule

| | |
|---|---|
| Name: | lf183 |
| Msg type: | reply |
| Methods: | INVITE |
| Action: | manipulate |
| Comparison type: | boolean |
| Match value: | $check183.$is183 |
| New value: | |

CfgRules



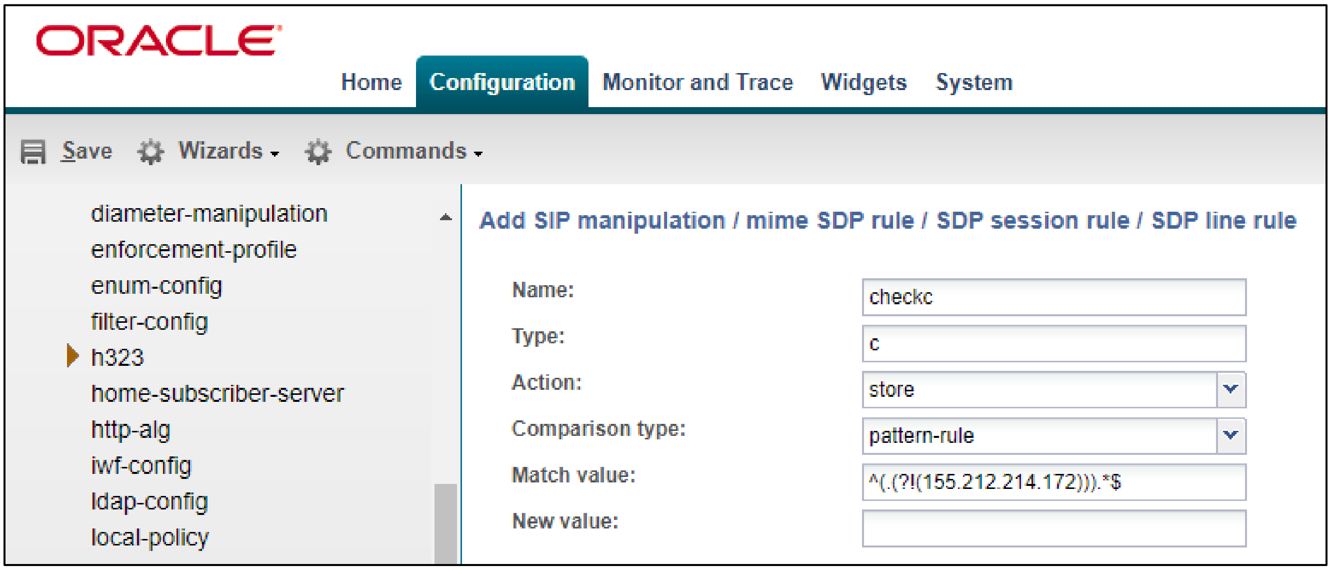
Add SIP manipulation / mime SDP rule / SDP session rule

| | |
|---|---|
| Name: | au |
| Action: | manipulate |
| Comparison type: | case-sensitive |
| Match value: | |
| New value: | |

CfgRules

| Name | Element type |
|---|---|

Here apply the IP of SIP-Interface facing your MS-Teams.



Add SIP manipulation / mime SDP rule / SDP session rule / SDP line rule

Name: checkc

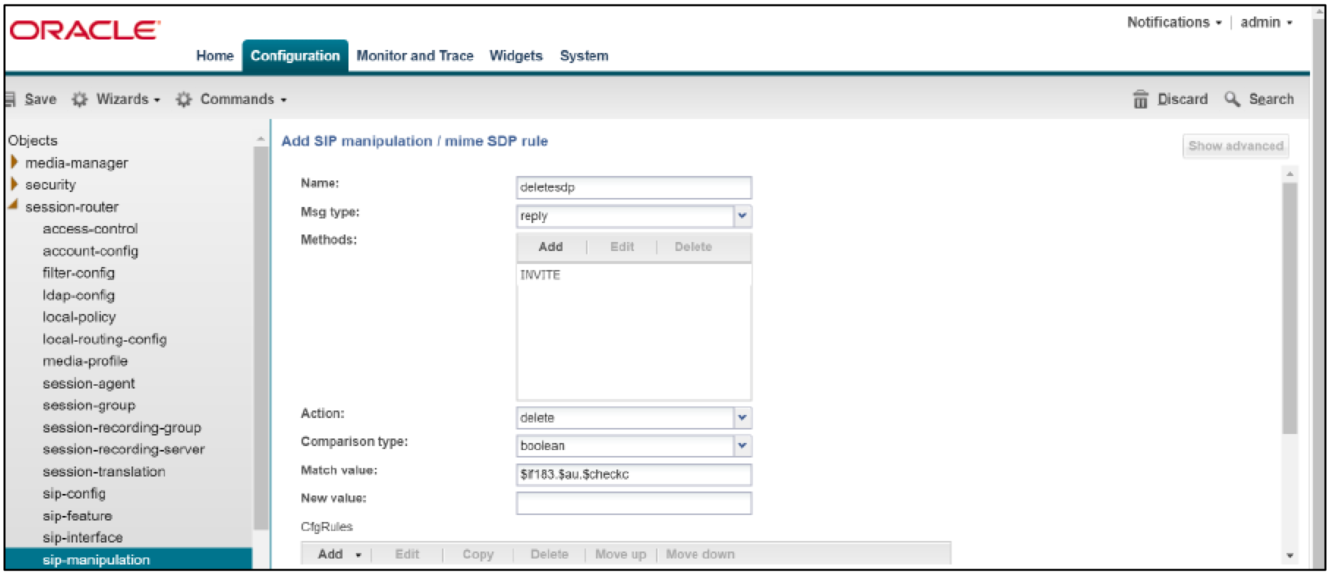
Type: c

Action: store

Comparison type: pattern-rule

Match value: ^(.(?!(155.212.214.172))).*$

New value:



Add SIP manipulation / mime SDP rule

Name: deletesdp

Msg type: reply

Methods:

INVITE

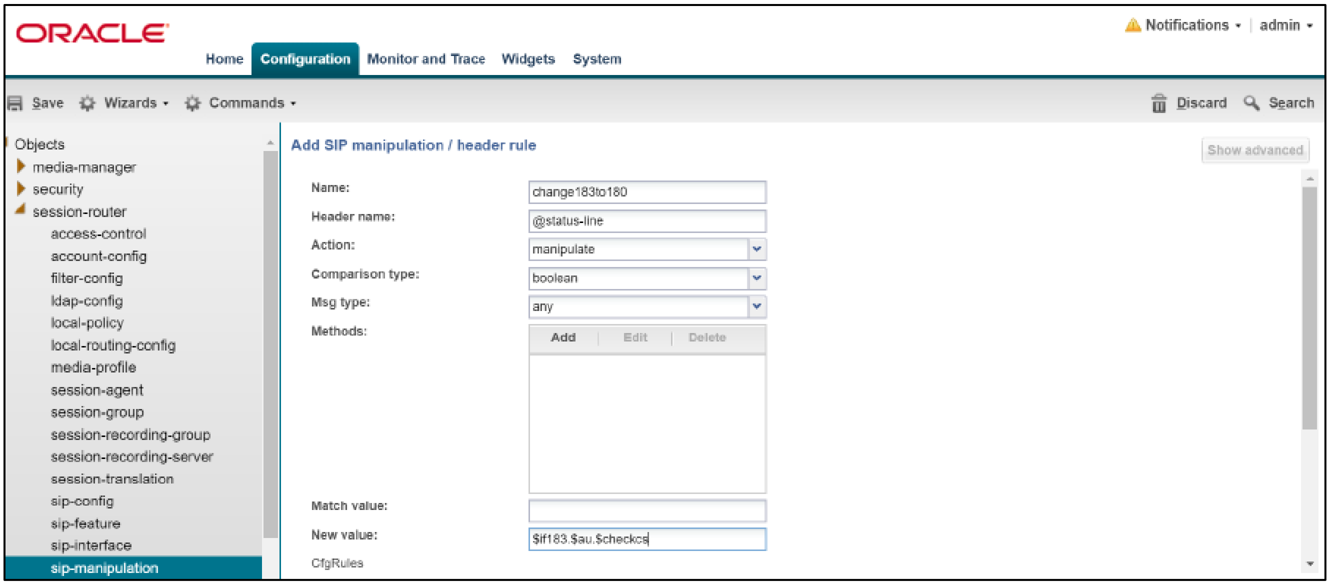
Action: delete

Comparison type: boolean

Match value: $lf183.$au.$checkc

New value:

CfgRules



Add SIP manipulation / header rule

Name: change183to180

Header name: @status-line

Action: manipulate

Comparison type: boolean

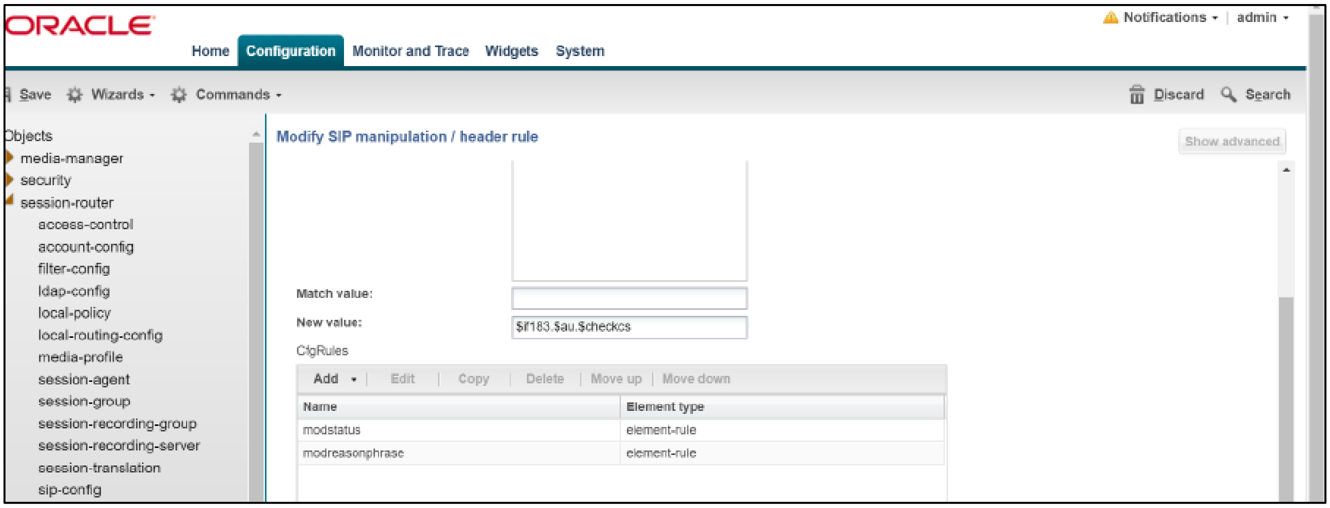
Msg type: any

Methods:

Match value:

New value: $if183.$au.$checkcs

CfgRules



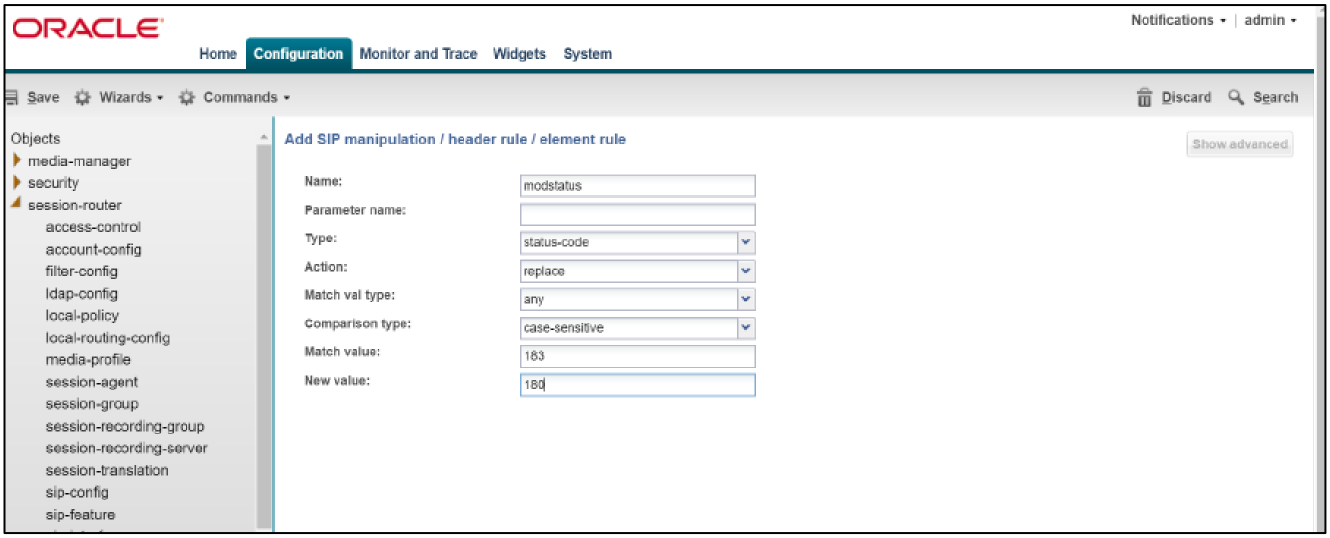
Modify SIP manipulation / header rule

Match value:

New value: $if183.$au.$checkcs

CfgRules

| Name | Element type |
|---|---|
| modstatus | element-rule |
| modreasonphrase | element-rule |



Add SIP manipulation / header rule / element rule

Name: modstatus

Parameter name:

Type: status-code

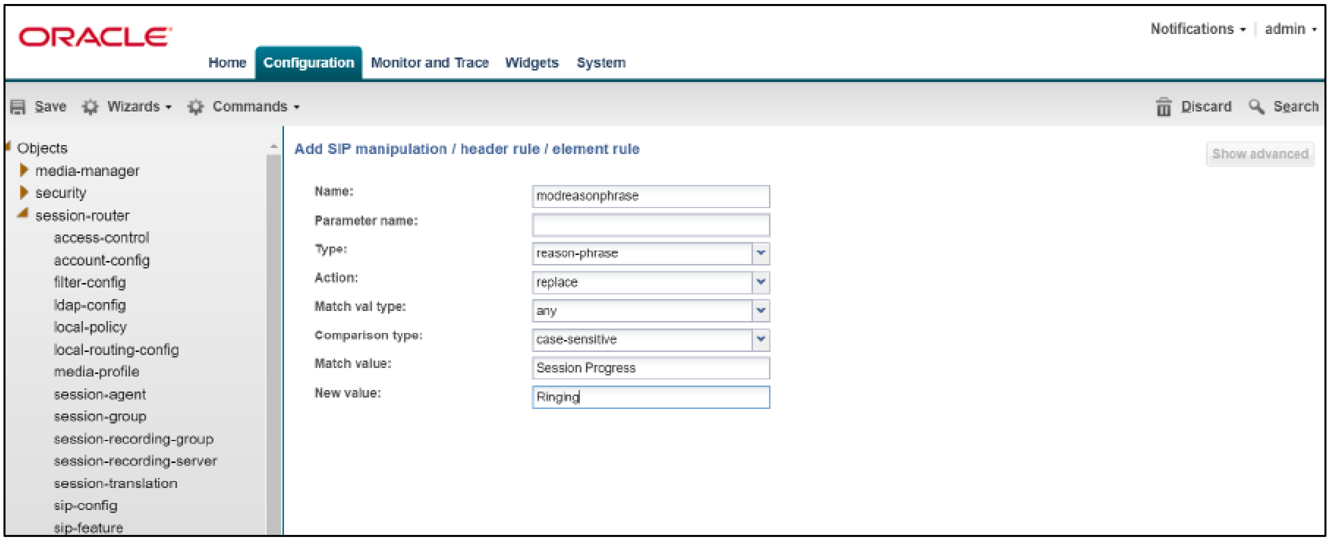
Action: replace

Match val type: any

Comparison type: case-sensitive

Match value: 183

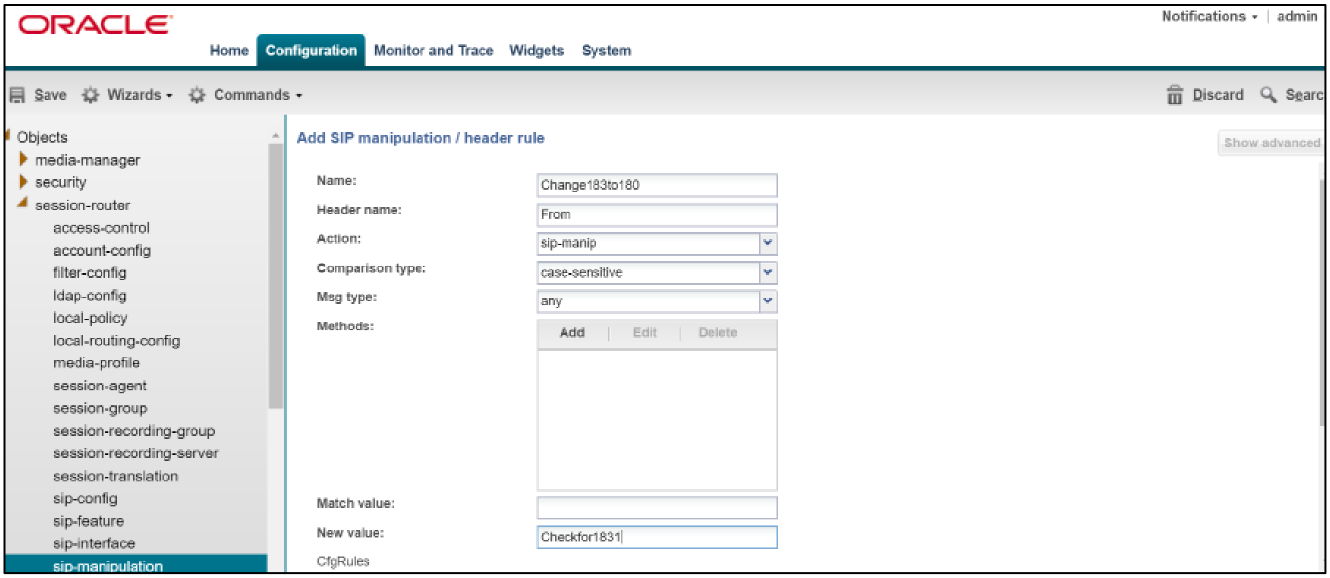
New value: 180



Add SIP manipulation / header rule / element rule

| | |
|---|---|
| Name: | modreasonphrase |
| Parameter name: | |
| Type: | reason-phrase |
| Action: | replace |
| Match val type: | any |
| Comparison type: | case-sensitive |
| Match value: | Session Progress |
| New value: | Ringing |

Apply this in Teamsinmanip by creating a rule as shown below.



Add SIP manipulation / header rule

| | |
|---|---|
| Name: | Change183to180 |
| Header name: | From |
| Action: | sip-manip |
| Comparison type: | case-sensitive |
| Msg type: | any |
| Methods: | |
| Match value: | |
| New value: | Checkfor1831 |

CfgRules

# 10 Appendix B

## 10.1 DDoS Prevention for Peering Environments

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/cd/F12246_01/doc/sbc_scz830_security.pdf

However. While specific 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
3. Modify the minimum and maximum untrusted signaling bandwidth parameters in the global media manger to minimize the throughput untrusted traffic has to work with.

The below examples of Access Control and Realm Trust level would be configured on and associated with the Realm facing Microsoft Teams. This model can be followed for any of the public facing interfaces, ie..Sip Trunk, etc….

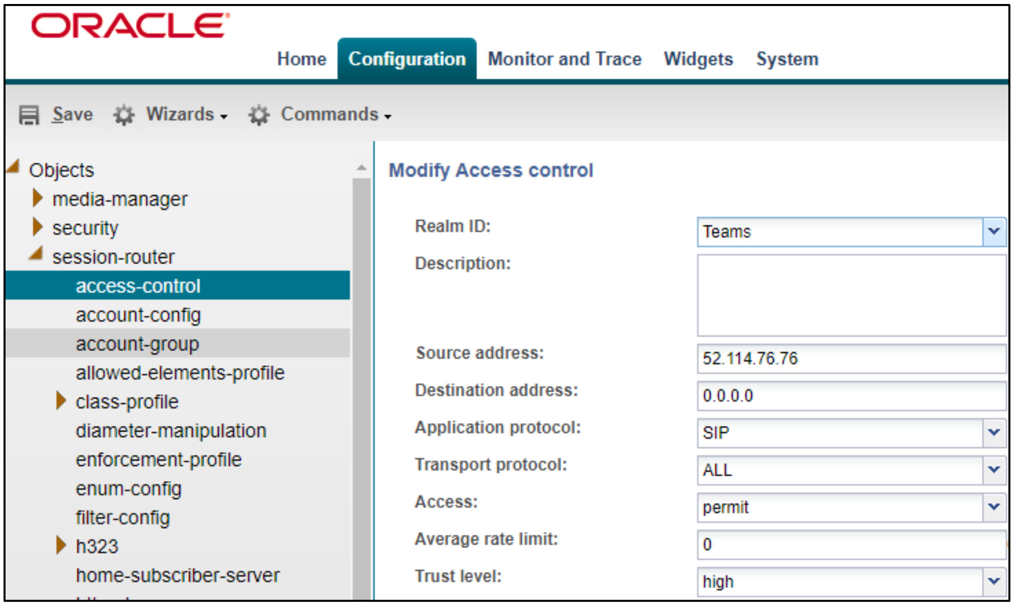
### 10.1.1 Access Control

GUI Path: session-router/access-control

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

*The below example is for one of the possible six IP addresses MSFT will be sending and receiving SIP traffic to and from*.

Use this example to create ACL's for all MSFT Teams IP addresses.



Modify Access control

| | |
|---|---|
| Realm ID: | Teams |
| Description: | |
| Source address: | 52.114.76.76 |
| Destination address: | 0.0.0.0 |
| Application protocol: | SIP |
| Transport protocol: | ALL |
| Access: | permit |
| Average rate limit: | 0 |
| Trust level: | high |

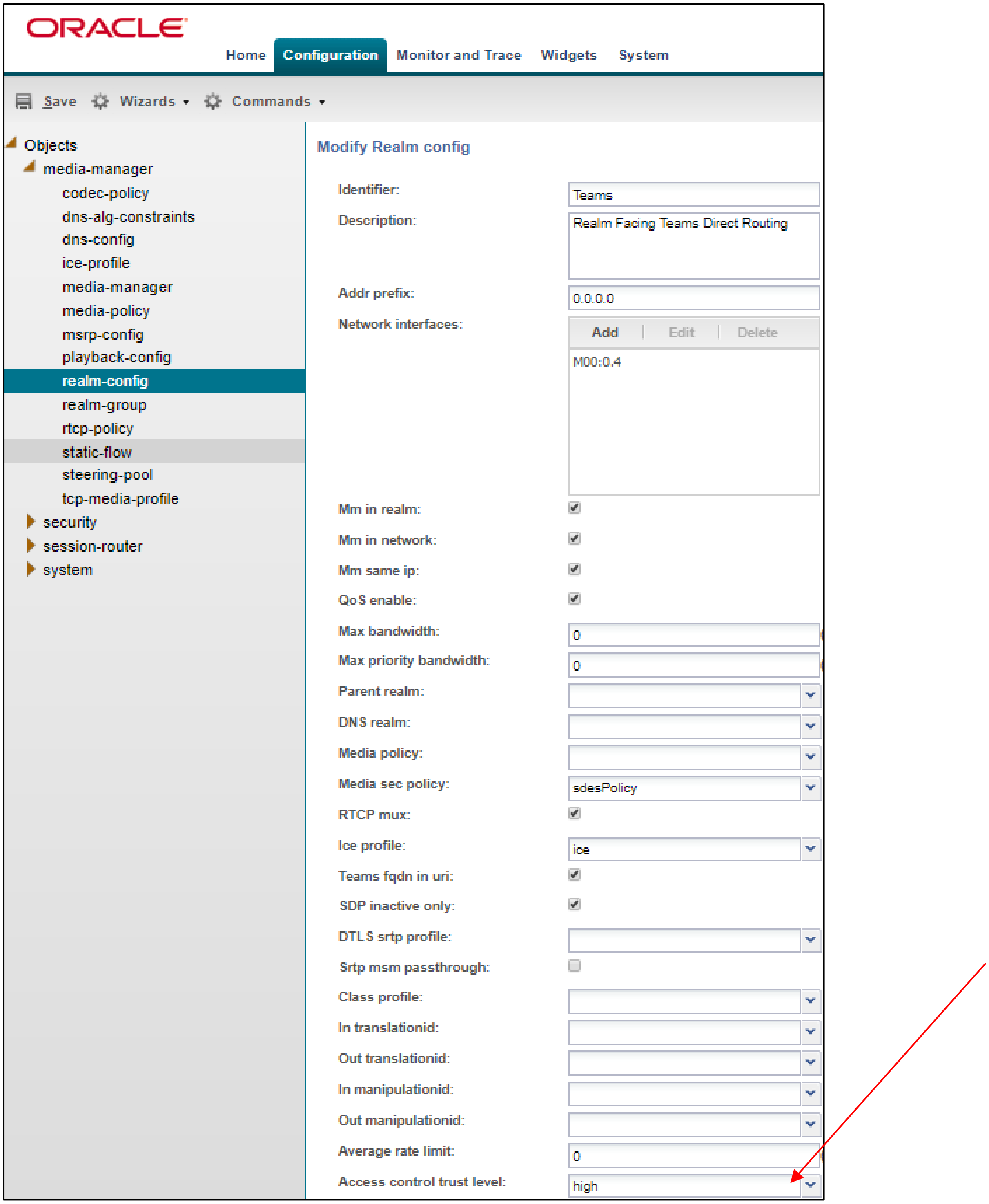
*As an alternative, the destination address can also be set to the SIP interface IP address associated with the realm.*

### 10.1.2 Realm Config

GUI Path: media-manager/realm-config

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

In the example below, notice the access control trust level matches the trust level of the ACL configured above. When these two fields match, it creates an implicit deny on this realm, so only SIP traffic from IP addresses configured as ACL's with matching trust level to the realm will be allowed to send traffic to your SBC. For more information on how trust level setting in ACL's and realms effect traffic, please refer to the SCZ830 Security Guide, Page 3-10



Modify Realm config

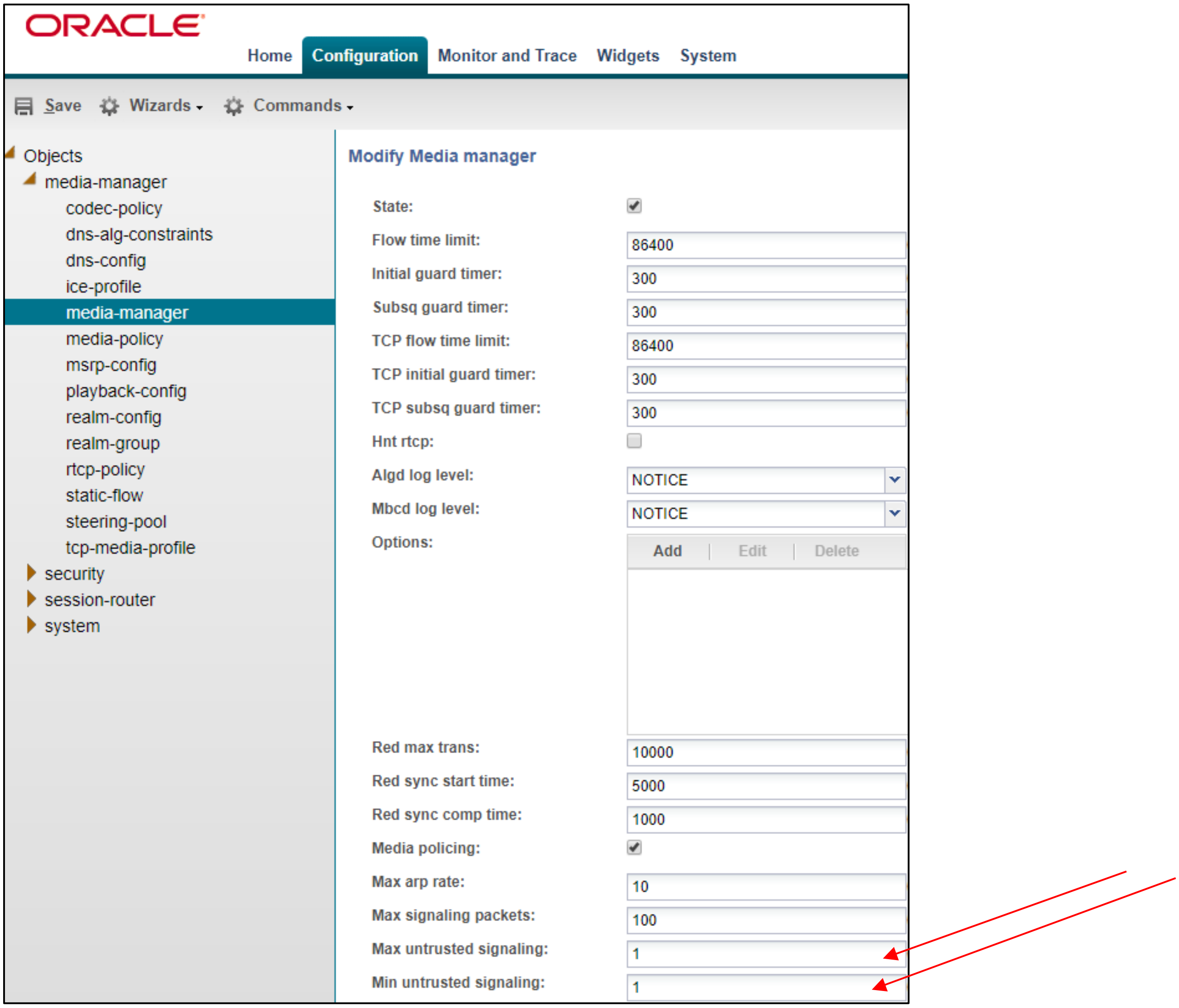
|  |  |
|---|---|
| Identifier: | Teams |
| Description: | Realm Facing Teams Direct Routing |
| Addr prefix: | 0.0.0.0 |
| Network interfaces: | M00:0.4 |
| Mm in realm: | ☑ |
| Mm in network: | ☑ |
| Mm same ip: | ☑ |
| QoS enable: | ☑ |
| Max bandwidth: | 0 |
| Max priority bandwidth: | 0 |
| Parent realm: |  |
| DNS realm: |  |
| Media policy: |  |
| Media sec policy: | sdesPolicy |
| RTCP mux: | ☑ |
| Ice profile: | ice |
| Teams fqdn in uri: | ☑ |
| SDP inactive only: | ☑ |
| DTLS srtp profile: |  |
| Srtp msm passthrough: | □ |
| Class profile: |  |
| In translationid: |  |
| Out translationid: |  |
| In manipulationid: |  |
| Out manipulationid: |  |
| Average rate limit: | 0 |
| Access control trust level: | high |

### 10.1.3 Global Media Manger

In the global Media Manger configuration, set the max and min untrusted signaling values to 1

GUI Path: media-manger/media-manger

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



Modify Media manager

| | |
|---|---|
| State: | ☑ |
| Flow time limit: | 86400 |
| Initial guard timer: | 300 |
| Subsq guard timer: | 300 |
| TCP flow time limit: | 86400 |
| TCP initial guard timer: | 300 |
| TCP subsq guard timer: | 300 |
| Hnt rtcp: | □ |
| Algd log level: | NOTICE |
| Mbcd log level: | NOTICE |
| Options: | |
| Red max trans: | 10000 |
| Red sync start time: | 5000 |
| Red sync comp time: | 1000 |
| Media policing: | ☑ |
| Max arp rate: | 10 |
| Max signaling packets: | 100 |
| Max untrusted signaling: | 1 |
| Min untrusted signaling: | 1 |

# 11 Appendix C

## 11.1 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.

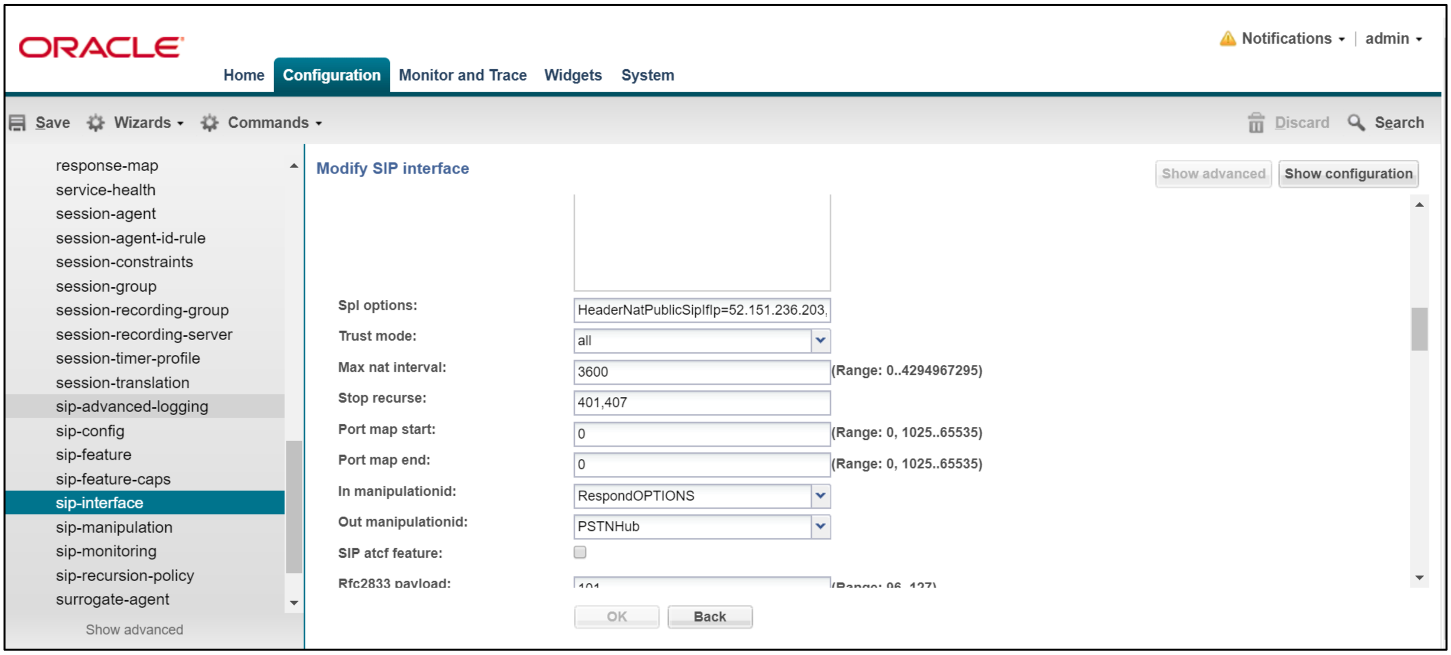
- The private IP address must be the same as the SIP Interface and Steering Pool IP address.
- The public IP address must be the public IP address of the NAT device

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

| | |
|---|---|
| Spl options: | HeaderNatPublicSipIfIp=52.151.236.203, |
| Trust mode: | all |
| Max nat interval: | 3600 (Range: 0..4294967295) |
| Stop recurse: | 401,407 |
| Port map start: | 0 (Range: 0, 1025..65535) |
| Port map end: | 0 (Range: 0, 1025..65535) |
| In manipulationid: | RespondOPTIONS |
| Out manipulationid: | PSTNHub |
| SIP atcf feature: | □ |
| Rfc2833 payload: | 101 (Range: 96..127) |

Similarly configure the PSTN side as well.

# 12 Appendix D

## 12.1 Sip Manipulation Replacement

To simplify the ORACLE SBC configuration, the ORACLE SBC 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 three additional SBC configuration parameters not found in prior releases.

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

### 12.1.1 Teams Facing Realm

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**

### 12.1.2 Teams FQDN

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

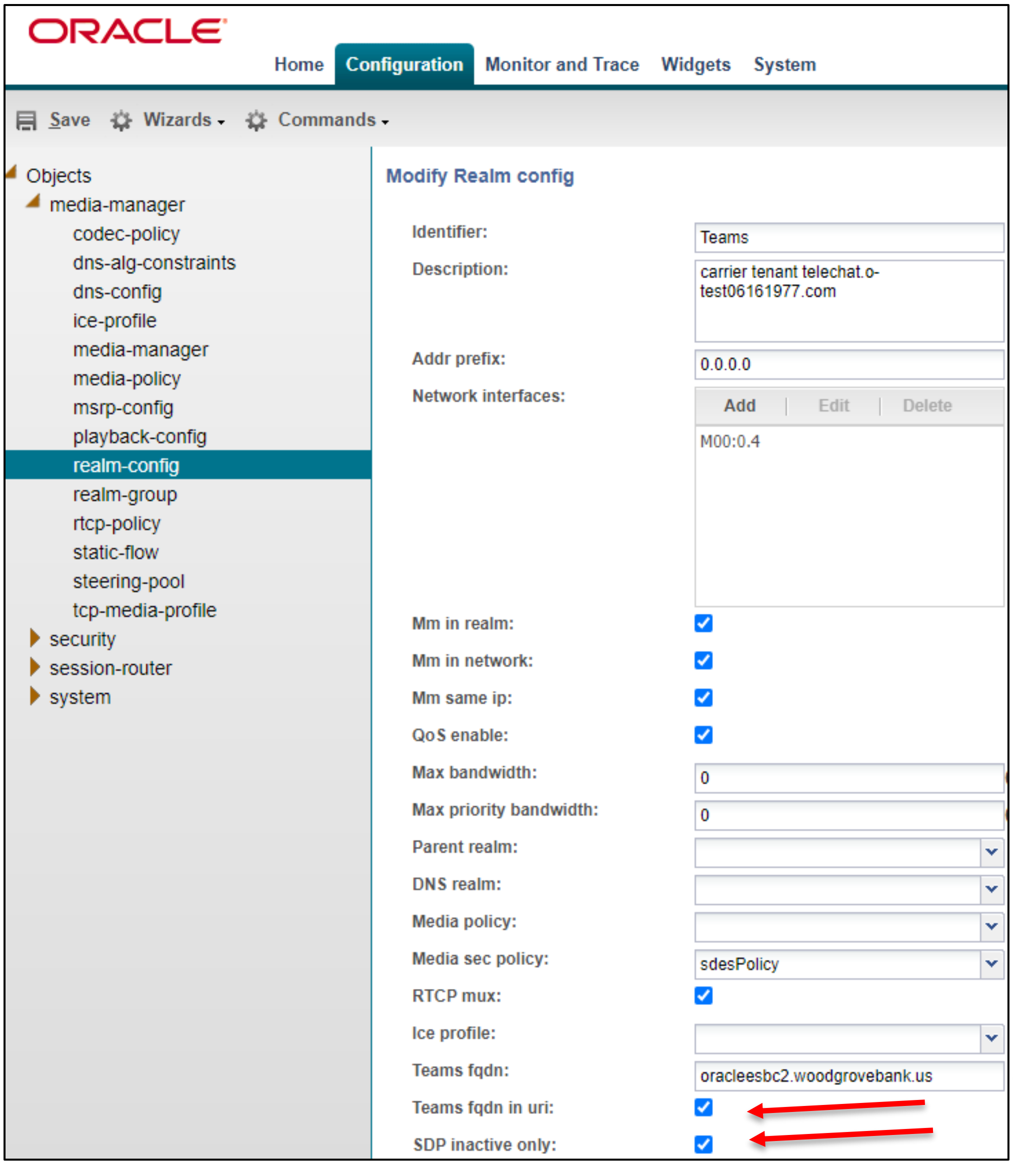
### 12.1.3 Teams FQDN in URI

When enabled, this parameter takes the FQDN configured under hostname of the Teams FQDN, and inserts that into the Contact and FROM headers of Invites generated by the SBC towards Teams, as well as the Contact header in all final responses which satisfies the Microsoft Teams requirement outlined in the Important Information Section of this document. 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. Lastly, 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, and with the Contact Header added to OPTION Requests generated by the SBC, Record Route is no longer required.

### 12.1.4 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 |



Modify Realm config

Identifier: Teams

Description: carrier tenant telechat.o-test06161977.com

Addr prefix: 0.0.0.0

Network interfaces: M00:0.4

Mm in realm: ☑

Mm in network: ☑

Mm same ip: ☑

QoS enable: ☑

Max bandwidth: 0

Max priority bandwidth: 0

Parent realm:

DNS realm:

Media policy:

Media sec policy: sdesPolicy

RTCP mux: ☑

Ice profile:

Teams fqdn: oracleesbc2.woodgrovebank.us

Teams fqdn in uri: ☑

SDP inactive only: ☑

*Please note, if the Teams FQDN field under realm-config is not populated with the Oracle SBC's FQDN, it will default back to the hostname parameter of the Network Interface.*

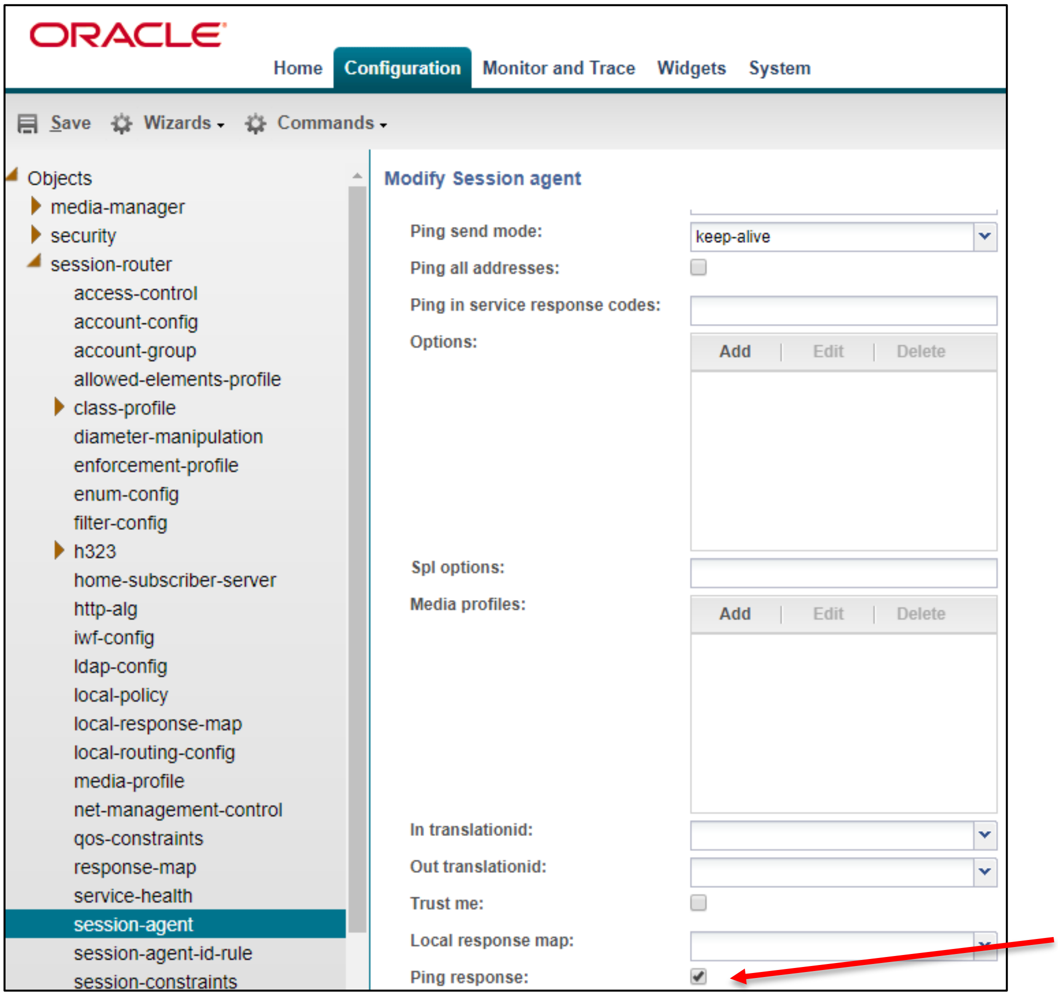
### 12.1.5 Teams Session Agents

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**

### 12.1.6 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.



Modify Session agent

Ping send mode: keep-alive

Ping all addresses: ☐

Ping in service response codes:

Options:

Spl options:

Media profiles:

In translationid:

Out translationid:

Trust me: ☐

Local response map:

Ping response: ☑

## 13 Important Note:

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.

For SBC's running a release prior to SCZ830M1P8A, you should already have a TeamsOutManipulation that contains a header rule that modifies the host part of the Contact header in Requests toward Microsoft Teams. 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 this guide. This allows the SBC to modify the Contact Host in both requests and responses, satisfying this change. For an example, please see Alter_contact.

For SBC's running release SCZ830m1p8A or later, and have enabled the new features outlined in AppendixD, the host-uri of the Contact of all responses towards Microsoft Teams will contain the SBC's FQDN in the host-uri of the Contact Header, so no change will be needed.

# 14 ACLI Running Config

## 14.1 Show running-config short

```
NN3900-101# sh con sh
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                                  SBCCertificate
        locality                             Bedford
        organization                            sales
        common-name                               Oracleesbc2.woodgrovebank.us
        extended-key-usage-list                     serverAuth
                                           ClientAuth
codec-policy
        name                                  addCN
        allow-codecs                              * SILK:no G729:no
        add-codecs-on-egress                          CN

codec-policy
        name                                  test
        allow-codecs                              SILK::wideband SILK::narrowband
        add-codecs-on-egress                          SILK::wideband SILK::narrowband

local-policy
        from-address                              *
        to-address                              *
        source-realm                              access-pstn
        policy-attribute
                next-hop                              sag:TeamsGrp
                realm                               access-teams
local-policy
        from-address                              *
        to-address                              *
        source-realm                              access-teams
        policy-attribute
                next-hop                              ATTTrunk
                realm                               access-pstn
media-manager
        mbcd-log-level                              NOTICE
        options                               audio-allow-asymmetric-pt
                                           xcode-gratuitous-rtcp-report-generation
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                          SRTP
        inbound
                profile                         SDES
                mode                             srtp
                protocol                          sdes
        outbound
                profile                         SDES
                mode                             srtp
                protocol                          sdes
network-interface
        name                          s0p0
        hostname                        oracleesbc2.woodgrovebank.us
        ip-address                     192.65.72.196
        netmask                        255.255.255.0
        gateway                       192.65.72.1
          hip-ip-list                 192.65.72.196
        icmp-address                       192.65.72.196

network-interface
        name                          s0p1
        hostname                        oracleesbc2.woodgrovebank.us
        ip-address                     155.212.214.172
        netmask                        255.255.255.0
        gateway                       155.212.214.172
        dns-ip-primary                     8.8.8.8
        dns-domain                        woodgrovebank.us

phy-interface
        name                          s0p0
        operation-type                     Media
phy-interface
        name                          s0p1
        operation-type                     Media
        port                        1

realm-config
        identifier                    access-pstn
        network-interfaces                 s0p0:0.4
        mm-in-realm                      enabled
        media-sec-policy                   RTP
        out-translationid                removeE164
        access-control-trust-level          high
        hide-egress-media-update              enabled
        ringback-trigger                  refer
        ringback-file                   ringback10sec.pcm
```

```
realm-config
        identifier                       access-teams
        network-interfaces                        s0p0:0.4
        mm-in-realm                          enabled
        media-sec-policy                       SRTP
        codec-policy                         addCN
        rtcp-policy                        rtcpGen
        hide-egress-media-update                enabled
rtcp-policy
        name                               rtcpGen
        rtcp-generate                           all-calls
sdes-profile
        name                               SDES
session-agent
        hostname                             ATTTrunk
        ip-address                          68.68.117.67
        state                             enabled
        realm-id                            access-pstn
        ping-method                            OPTIONS
        ping-interval                         60
session-agent
        hostname                             sip-all.pstnhub.microsoft.com
        port                             5061
        transport-method                           StaticTLS
        realm-id                            access-teams
        ping-interval                         30
        refer-call-transfer                     enabled
         ping-all-addresses                        enabled

session-agent
        hostname                             sip.pstnhub.microsoft.com
        port                             5061
        transport-method                           StaticTLS
        realm-id                            access-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                            access-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                            access-teams
        ping-method                            OPTIONS
        ping-interval                         30
        refer-call-transfer                     enabled
session-group
        group-name                             TeamsGrp
        strategy                            HUNT
        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                       access-pstn
     options                         inmanip-before-validate
                                 max-udp-length=0
     extra-method-stats                   enabled
sip-feature
     name                            replaces
     realm                           access-teams
     require-mode-inbound                     Pass
     require-mode-outbound                     Pass

sip-interface
     state                          enabled
     realm-id                         access-pstn
     description                        to trunk
     sip-port
          address                            192.65.72.196
          allow-anonymous                          agents-only
     in-manipulationid
     out-manipulationid                   Siptrunk_outmanip
sip-interface
     realm-id                         access-teams
     sip-port
          address                            155.212.214.172
          port                            5061
          transport-protocol                        TLS
          tls-profile                        TLSTeams
          allow-anonymous                          agents-only
     nat-traversal                      always
     nat-interval                      3600
     registration-caching                   enabled
     in-manipulationid                   Teamsinmanip
     out-manipulationid                   Teamsoutmanip
     sip-profile                       foreplace

sip-manipulation
     name                            Siptrunk_outmanip
header-rule
          name                             change_fqdn_to_ip_from
          header-name                          From
          action                          manipulate
          msg-type                           request
          methods                           INVITE
          element-rule
               name                             from_uri
               type                            uri-host
               action                           replace
               new-value                          $LOCAL_IP
     header-rule
          name                             change_fqdn_to_ip_to
          header-name                          to
          action                          manipulate
          msg-type                           request
```

```
        methods                  INVITE
        element-rule
            name                   urihost
            type                  uri-host
            action                 replace
            new-value                $REMOTE_IP
sip-manipulation
    name                       Teamsinmanip
    header-rule
        name                       Respondoptions
        header-name                   From
        action                     reject
        msg-type                     request
        methods                      OPTIONS
        new-value                    200 OK

mime-sdp-rule
        name                       Reqinactivetosendonly
        msg-type                     request
        methods                      INVITE
        action                     manipulate
        sdp-media-rule
            name                   audio
            media-type               audio
            action                 manipulate
            sdp-line-rule
                name                   audio1
                type                  a
                action                 replace
                match-value               inactive
                new-value                sendonly
    mime-sdp-rule
        name                       Replyinactivetorecvonly
        msg-type                     reply
        methods                      INVITE
        action                     manipulate
        sdp-media-rule
            name                   audio
            media-type               audio
            action                 manipulate
            sdp-line-rule
                name                   audio1
                type                  a
                action                 replace
                match-value               inactive
                new-value                recvonly
sip-manipulation
    name                       Teamsoutmanip
    header-rule
        name                       Countrycode
        header-name                   Request-URI
        action                     manipulate
        msg-type                     request
        methods                      INVITE
        element-rule
            name                   uriuser2
            type                  uri-user
            action                      replace
            new-value                     "1"+$
    header-rule
        name                          Change_fromip_fqdn
        header-name                      To
        action                       manipulate
        msg-type                       request
        methods                        INVITE
        element-rule
            name                         fixtouri
            type                       uri-host
            action                      replace
            match-val-type                   ip
            new-value                     $RURI_HOST.$0
        element-rule
            name                         urinumber
            type                       uri-user
            action                      replace
            new-value                     "1"+$
    header-rule
        name                          Change_to_userandhost
        header-name                      From
        action                       manipulate
        msg-type                       request
        methods                        INVITE
        element-rule
            name                         FixUriHost
            type                       uri-host
            action                      replace
            match-val-type                   ip
            new-value                     oracleesbc2.woodgrovebank.us
    header-rule
        name                          Addcontactheaderinoptions
        header-name                      Contact
        action                       add
        msg-type                       request
        methods                        OPTIONS
        new-value
"<sip:ping@oracleesbc2.woodgrovebank.us:5067;transport=tls>"
    header-rule
        name                          Recordroute
        header-name                      Record-Route
        action                       add
        msg-type                       request
        methods                        OPTIONS
        new-value                       "<sip:oracleesbc2.woodgrovebank.us>"
    header-rule
        name                          Alter_contact
        header-name                      Contact
        action                       manipulate
        msg-type                       any
        methods                        INVITE
        element-rule
            name                         Contact_IP
            parameter-name                    Contact_IP
            type                       uri-host
            action                      replace
```

```
                new-value                  oracleesbc2.woodgrovebank.us

        header-rule
            name                        Adduseragent
            header-name                    User-Agent
            action                      add
            msg-type                     request
            methods                      INVITE
            new-value                    "Oracle ESBC"
        header-rule
            name                        Modifyuser
            header-name                    User-Agent
            action                      manipulate
            msg-type                     request
            methods                      INVITE
            element-rule
                name                         user
                type                       header-value
                action                      add
                new-value                     "Oracle ESBC"
mime-sdp-rule
            name                        Reqsendonlytoinactive
            msg-type                     request
            methods                      INVITE
            action                      manipulate
            sdp-media-rule
                name                        audio
                media-type                     audio
                action                      manipulate
                sdp-line-rule
                    name                        audio3
                    type                      a
                    action                     replace
                    match-value                    sendonly
                    new-value                     inactive
        mime-sdp-rule
            name                        Reprecvonlytoinactive
            msg-type                     reply
            methods                      INVITE
            action                      manipulate
            sdp-media-rule
                name                        audio
                media-type                     audio
                action                      manipulate
                sdp-line-rule
                    name                        audio3
                    type                      a
                    action                     replace
                    match-value                    recvonly
                    new-value                     inactive
sip-monitoring
        match-any-filter                enabled
        monitoring-filters               *
sip-profile
        name                        foreplace
        replace-dialogs                 enabled
```

```
steering-pool
        ip-address                    155.212.214.172
        start-port                  20000
        end-port                     40000
        realm-id                    access-teams
steering-pool
        ip-address                   192.65.72.196
        start-port                  20000
        end-port                     40000
        realm-id                    access-pstn
system-config
        system-log-level                 Notice
        process-log-level                Notice
        default-gateway             172.18.0.1
tls-global
        session-caching                   enabled
tls-profile
        name                        TLSTeams
        end-entity-certificate           SBCCertificate
        trusted-ca-certificates        BaltimoreRoot
        cipher-list                  DEFAULT
        mutual-authenticate                enabled
web-server-config
        inactivity-timeout               0
        http-interface-list
```

ORACLE

**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