



# ORACLE

## Configuring the Oracle SBC with Microsoft Teams Direct Routing 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	<ul style="list-style-type: none"><li>Added Web GUI</li></ul>	12-09-2019
2.0	<ul style="list-style-type: none"><li>Added bug fixes for ACMESOLU-106</li></ul>	21-10-2019
3.0	<ul style="list-style-type: none"><li>New Document Format</li><li>Modified TLS profile</li><li>Modified DDOS Appendix B</li><li>Added Emergency Calling Config</li><li>Added Appendix E for replacement of sip manipulations</li></ul>	03-04-2020
4.0	<ul style="list-style-type: none"><li>Modified Sip Manips for Contact and From Host URI</li><li>Added new sip manip for contact in Appendix D</li></ul>	29-04-2020

### **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

<i>Alert</i> .....	3
<b>Introduction</b> .....	7
<b>About Microsoft Teams Direct Routing</b> .....	7
Planning Direct Routing.....	7
<b>Tenant Requirements</b> .....	7
<b>Licensing Requirements</b> .....	7
<b>DNS Requirements</b> .....	8
<b>SBC Domain Names</b> .....	8
<b>Public trusted certificate for the SBC</b> .....	9
Configure Direct Routing.....	10
<b>Establish a remote PowerShell session to Skype for Business Online</b> .....	10
<b>Pair the SBC to tenant</b> .....	11
<b>Enable users for Direct Routing</b> .....	12
<b>Microsoft Teams Direct Routing Interface characteristics</b> .....	15
<b>Requirements to SIP messages “Invite” and “Options”</b> .....	17
<b>Requirements for “INVITE” messages syntax</b> .....	17
<b>Requirements for “OPTIONS” messages syntax</b> .....	18
<b>Validated Oracle version</b> .....	19
<b>Configuring the SBC</b> .....	20
<b>What is Media Bypass</b> .....	20
<b>New SBC configuration</b> .....	22
<b>Establishing a serial connection to the SBC</b> .....	22
Configure SBC using Web GUI.....	25
Configure system-config.....	27
Configure Physical Interface values .....	28
Configure Network Interface values .....	29
Enable media manager .....	31
Configure Realms .....	31
Enable sip-config .....	32
Configuring a certificate for SBC Interface .....	34
SBC Certificate Creation .....	34
<b>Step 1 – Creating the SBC certificate record</b> .....	34
<b>Step 2 – Generating a certificate signing request for SBC certificate</b> .....	35
<b>Step 3 – Deploy the SBC certificate</b> .....	36
Root and Intermediate Certificates Creation.....	36
<b>Step1-Creating the root and intermediate certificates on SBC</b> .....	37

<b>Step2: Deploying the Root and Intermediate certificates on SBC</b> .....	37
TLS-Profile .....	39
Creating a sip-interface to communicate with Microsoft Teams .....	39
Configure sip-interface to communicate with SIP Trunk .....	40
Configure session-agent.....	41
Create a Session Agent Group .....	43
Configure local-policy .....	44
Configure Media Profile & Codec Policy.....	47
Configure sip-manipulations.....	49
Teamsoutmanip.....	49
Countrycode Manipulation: .....	51
Change_fromip_fqdn Manipulation:.....	53
Change_to_userandhost Manipulation:.....	54
Addcontactheaderinoptions.....	56
Recordroute.....	57
Alter_contact.....	58
Adduseragent .....	59
Modifyuseragent .....	60
Teamsinmanip.....	61
Respondoptions.....	63
Applying the teams SIP manipulations to Teams SIP Interface .....	64
Siptrunk_outmanip.....	65
Change_fqdn_to_ip_from .....	66
Change_fqdn_to_ip_to.....	67
Applying the trunk side SIP manipulations to Trunk SIP Interface.....	68
<b>Ringback Configuration</b> .....	<b>68</b>
Ringback on Transfers .....	68
Consultative transfer configuration.....	71
Configure steering pool.....	72
Configure SDES profile.....	73
Media-sec-policy.....	74
Configure RTCP Policy and RTCP Mux.....	77
Configure ice-profile.....	78
<b>Existing SBC configuration</b> .....	<b>80</b>
<b>Configuration for Emergency Calling</b> .....	<b>80</b>
E911 .....	81
Session Translations Config.....	81
Emergency Session Handling .....	84

Net-Management Control .....	86
Session Constraints for E911 .....	87
Elin Gateway.....	87
Sip-Manipulation for Teams ELIN .....	88
<b>Appendix A .....</b>	<b>90</b>
Ringback on inbound calls to Teams and early media.....	90
<b>Appendix B .....</b>	<b>97</b>
DDoS Prevention for Peering Environments .....	97
Access Control.....	97
Realm Config.....	98
Global Media Manger .....	99
<b>Appendix C .....</b>	<b>101</b>
SBC Behind NAT SPL configuration.....	101
<b>Appendix D .....</b>	<b>102</b>
Sip Manipulation Replacement.....	102
Teams Facing Realm.....	102
Teams FQDN in URI.....	102
SDP inactive only.....	102
Teams Session Agents .....	103
Ping Response.....	103
<b>Important Note: .....</b>	<b>104</b>
<b>CLI Configuration Output.....</b>	<b>106</b>

# Introduction

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

## 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>

## 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

### Tenant Requirements

Make sure that you have a custom domain on your O365 tenant. 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>

### 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

## 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

## SBC Domain Names

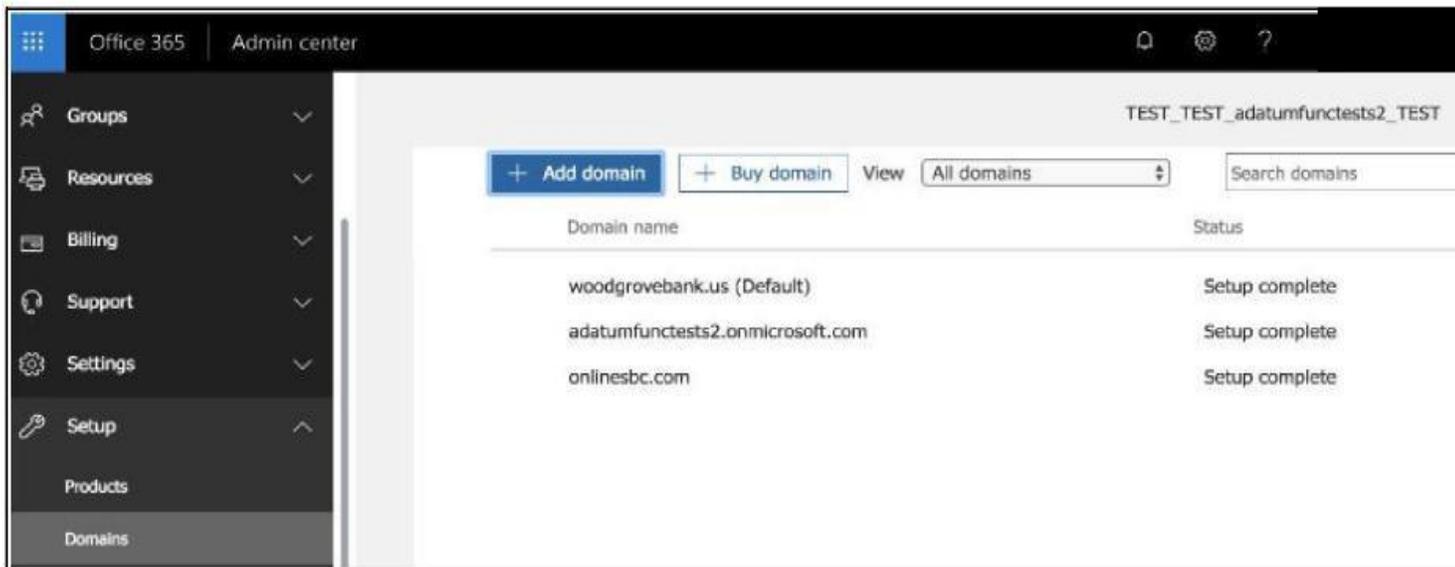
The SBC domain name must be from one of the names registered in “Domains” of the tenant. You cannot use the

\*.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: <ul style="list-style-type: none"> <li>• sbc1.woodgrovebank.us;</li> <li>• ussbcs15.woodgrovebank.us</li> <li>• europe.woodgrovebank.us</li> </ul> Non-Valid name: <ul style="list-style-type: none"> <li>• sbc1.europe.woodgrovebank.us (requires registering domain name europe.atatum.biz in “Domains” first)</li> </ul>
<a href="http://woodgrovebankus.onmicrosoft.com">woodgrovebankus.onmicrosoft.com</a>	No	Using *.onmicrosoft.com domains is not supported for SBC names
<a href="http://hybrdvoice.org">hybrdvoice.org</a>	Yes	Valid names: <ul style="list-style-type: none"> <li>• <a href="http://sbc1.hybridvoice.org">sbc1.hybridvoice.org</a></li> <li>• <a href="http://ussbcs15.hybridvoice.org">ussbcs15.hybridvoice.org</a></li> <li>• <a href="http://europe.hybridvoice.org">europe.hybridvoice.org</a></li> </ul> Non-Valid name: <ul style="list-style-type: none"> <li>• <a href="http://sbc1.europe.hybridvoice.org">sbc1.europe.hybridvoice.org</a> (requires registering domain name europe.hybridvoice.org in “Domains” first)</li> </ul>

Please activate and register the domain of tenant.



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

Public IP	FQDN Name
155.212.214.173	Oracleesbc.woodgrovebank.us

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

# 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

## 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>.

To establish a remote connection ,follow the below steps

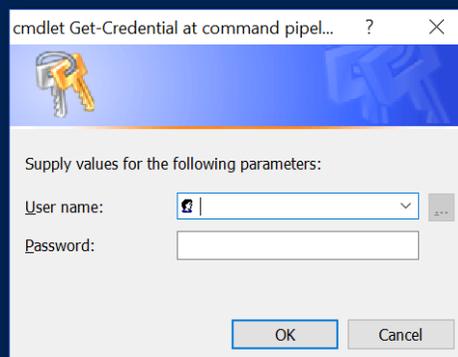
- Open PowerShell and type in the below commands
- Import-Module SkypeOnlineConnector
- \$userCredential = Get-Credential
- \$sfbSession = New-CsOnlineSession -Credential \$userCredential
- Import-PSSession \$sfbSession

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

- 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... ? X

Supply values for the following parameters:

User name: [User Name] [v] [...]

Password: [ ]

OK Cancel

```
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:

ModuleType Version Name ExportedCommands
-----
Script 1.0 tmp_fcnyz43x.w0h {Clear-CsOnlineTelephoneNumberReservation, ConvertTo-JsonForPSWS, Disable-CsMeetingRoom, Disable-CsOnlineDia...
```

- 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
```

## 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> -SipSignallingPort <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:\WINDOWS\system32> New-CsOnlinePSTNGateway -Fqdn oraclesbc2.woodgrovebank.us -SipSignallingPort 5061 -MaxConcurrentSessions 500 -MediaBypass $true
```

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 oraclesbc2.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        : True
GatewaySiteId      :
GatewaySiteLbrEnabled : False
FailoverResponseCodes : 408,503,504
GenerateRingingWhileLocatingUser : True
PidfLoSupported    : False
MediaRelayRoutingLocationOverride :
ProxySbc           :
BypassMode         : None

```

## 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](mailto:teamsuser1@woodgrovebank.us)

Here the following license is added

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

The screenshot shows the Microsoft 365 admin center interface. On the left is a navigation pane with options like Home, Users, Groups, Billing, and Setup. The main area displays the user profile for 'TeamsUser1' (teamsuser1@woodgrovebank.us). The profile includes a profile picture, name, and email. Below this are several rows of user details, each with an 'Edit' link:

Username / Email	teamsuser1@woodgrovebank.us	Edit
Aliases	teamsuser1@adatumfuncstests2.onmicrosoft.com	
Product licenses	Office 365 E5	Edit
Group memberships (1)	Solutions	Edit
Sign-in status	Sign-in allowed	Edit
Office installs	View and manage which devices this person has Office apps installed on.	Edit
Roles	User (no admin access)	Edit
Preferred Data Location		
Contact information	TeamsUser1	Edit

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 | fl RegistrarPool

RegistrarPool : sippoolsn23a15.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 teamsuser1 -EnterpriseVoiceEnabled $true -HostedVoiceMail $true -OnPremLineURI tel:+17814437383
```

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 ".\*"

Set-CsOnlineVoiceRoute -id "Bedford 1" -NumberPattern ".\*" -OnlinePstnGatewayList oracleesbc2.woodgrovebank.us -Priority 1

```

PS C:\WINDOWS\system32> Set-CsOnlineVoiceRoute -id "Oracle_US" -NumberPattern ^(\+1[0-9]{10})$ -OnlinePstnGatewayList oracleesbc2.woodgrovebank.us -Priority 1

```

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 "teamsuser1" -PolicyName "US Only"
```

7. Validate the same using the PowerShell command as shown below

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

Identity           : Global
OnlinePstnUsages   : {}
Description        :
RouteType          :

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

## 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	
Codecs	Transport for Media Bypass	ICE-lite (RFC5245) – recommended, • Client also has Transport Relays	
	Audio codecs	<ul style="list-style-type: none"> <li>• G711</li> <li>• G722</li> <li>• Silk (Teams clients)</li> <li>• Opus (WebRTC clients) - Only if Media Bypass is used;</li> <li>• G729</li> </ul>	
	Other codecs	<ul style="list-style-type: none"> <li>• DTMF – Required</li> <li>• Events 0-16</li> <li>• CN <ul style="list-style-type: none"> <li>o Required narrowband and wideband</li> </ul> </li> <li>• RED – Not required</li> <li>• Silence Suppression – Not required</li> </ul>	

## 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

## 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.i
ce
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.

## 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.



## 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.

# 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 Media Bypass.

## What is Media Bypass

Media bypass shortens the path of media traffic and reduces the number of hops in transit for better performance. With media bypass, media is kept between the Session Border Controller (SBC) and the client instead of sending it via the Microsoft Phone System. For more information on media bypass ,please read Microsoft’s documentation here. <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan-media-bypass>

The Figure 1 below shows the connection topology example.

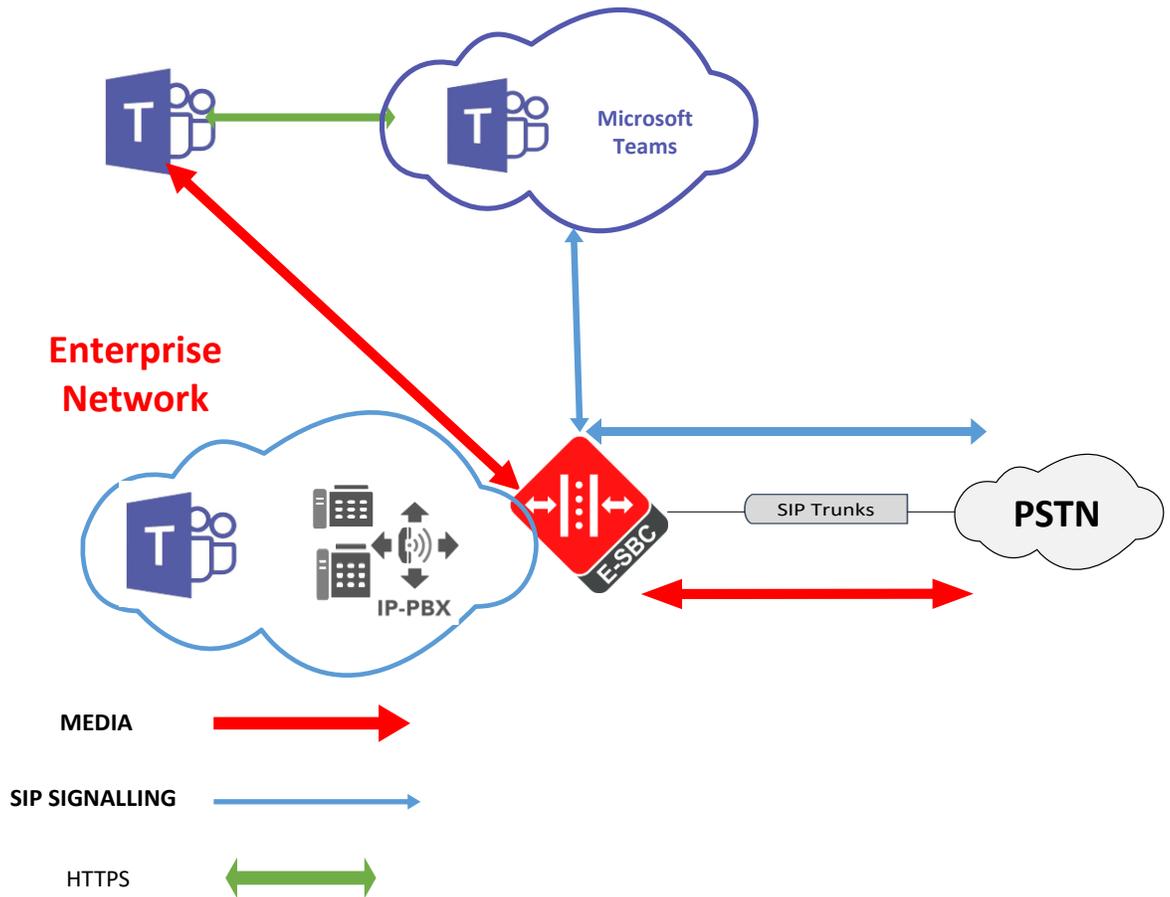


Figure :1: Signaling & media flow with media-bypass enabled



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.

# New SBC configuration

If the customer is looking to setup a new SBC from scratch with Microsoft teams, please follow the section below.

## 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

```
Starting tLemd...
Starting tServiceHealth...
Starting tCollect...
Starting tAtcpd...
Starting tAsctpd...
Starting tMbcd...
Starting tCommMonitor...
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
```

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

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

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

```
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
```

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!
-----
```

The SBC comes up after reboot and is now ready for 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

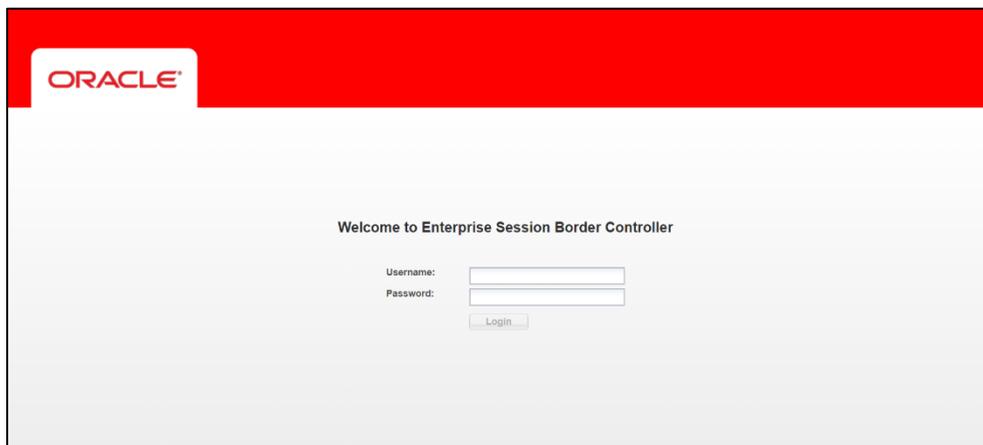
PE-6300-1(web-server-config)# exit
PE-6300-1(system)# exit
PE-6300-1(configure)# exit
PE-6300-1# save-config
checking configuration
-----
Results of config verification:
  1 configuration error
Run 'verify-config' for more details
-----
Save-Config received, processing.
waiting for request to finish
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

```

## 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>](https://<SBC_MGMT_IP>). The username and password is the same as that of CLI.

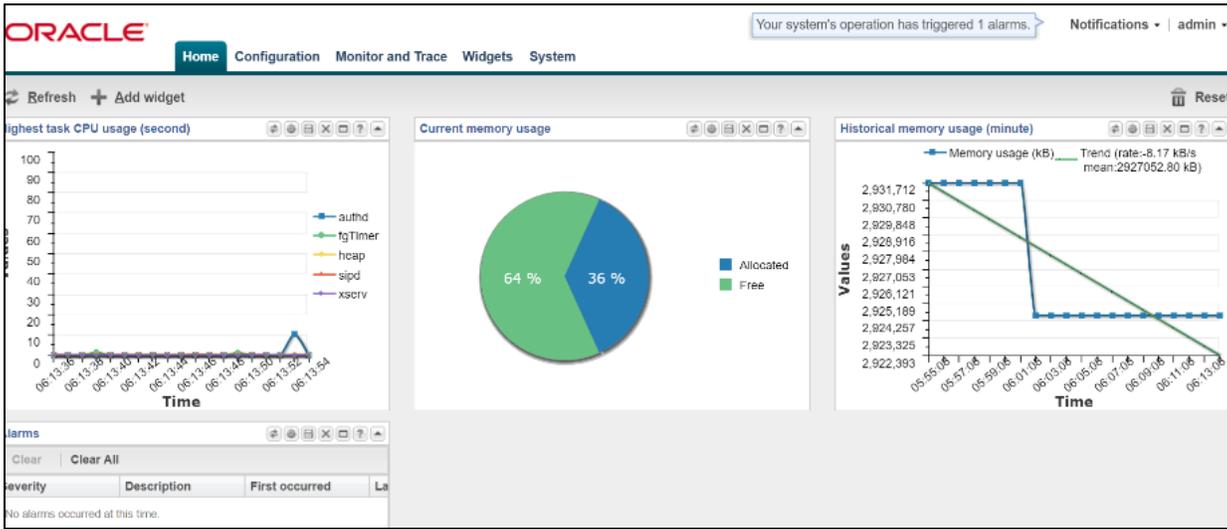


ORACLE

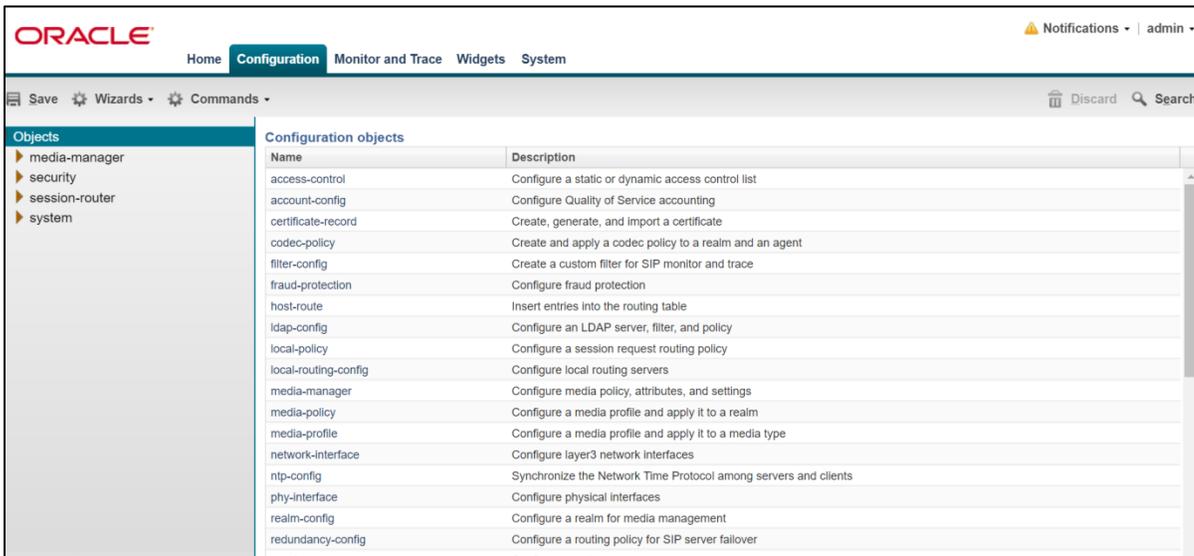
Welcome to Enterprise Session Border Controller

Username:

Password:



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



Kindly refer to the GUI User Guide [https://docs.oracle.com/cd/E92503\\_01/doc/esbc\\_ecz800\\_webgui.pdf](https://docs.oracle.com/cd/E92503_01/doc/esbc_ecz800_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.*

## Configure system-config

Go to system->system-config

The screenshot displays the Oracle Configuration Assistant interface. At the top, the Oracle logo is on the left, and navigation tabs for Home, Configuration, Monitor and Trace, Widgets, and System are on the right. Below the navigation is a toolbar with Save, Wizards, and Commands. The left sidebar shows a tree view of configuration objects, with 'system-config' selected. The main area is titled 'Modify System config' and contains the following fields and options:

- Hostname: oracleesbc2.woodgrovebank.us
- Description: ESBC to Microsoft Teams Direct Routing
- Location: Bedford, MA
- Mib system contact: (empty)
- Mib system name: (empty)
- Mib system location: (empty)
- Acp TLS profile: (dropdown menu)
- SNMP enabled:
- Enable SNMP auth traps:
- Enable SNMP syslog notify:
- Enable SNMP monitor traps:
- Enable env monitor traps:
- Enable mblk\_tracking:
- Enable I2 miss report:

For VME, transcoding cores are required to be set. Please refer the documentation here for more information

[https://docs.oracle.com/cd/E85213\\_01/doc/sbc\\_scz739\\_essentials.pdf](https://docs.oracle.com/cd/E85213_01/doc/sbc_scz739_essentials.pdf)

## 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

The screenshot shows the 'Modify Phy interface' configuration page in the Oracle WebGUI. The page has a navigation bar with 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below the navigation bar, there are tabs for 'Save', 'Wizards', and 'Commands'. The main content area is titled 'Modify Phy interface' and contains the following configuration fields:

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

At the bottom of the page, there are 'OK' and 'Back' buttons. A 'Show advanced' button is also visible in the top right corner of the configuration area.

## 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	<a href="http://oracleesbc2.woodgrovebank.us">oracleesbc2.woodgrovebank.us</a>	
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 latest GA release SCZ830m1p7, hostname parameter in Network Interface is 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.*

ORACLE Home Configuration Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
- security
- session-router
- system
  - capture-receiver
  - fraud-protection
  - host-route
  - network-interface**
  - network-parameters
  - ntp-config
  - phy-interface
  - redundancy-config
  - snmp-address-entry
  - snmp-community
  - snmp-group-entry
  - snmp-user-entry
  - snmp-view-entry
  - spl-config
  - system-access-list

Modify Network interface

Show advanced

Name:  (Range: 0..4095)

Sub port id:  (Range: 0..4095)

Description:

Hostname:

IP address:

Pri utility addr:

Sec utility addr:

Netmask:

Gateway:

Gw heartbeat

State:

Heartbeat:  (Range: 0..65535)

ORACLE Home Configuration Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
- security
- session-router
- system
  - capture-receiver
  - fraud-protection
  - host-route
  - network-interface**
  - network-parameters
  - ntp-config
  - phy-interface
  - redundancy-config
  - snmp-address-entry
  - snmp-community

Modify Network interface

Show advanced

Retry count:  (Range: 0..65535)

Retry timeout:  (Range: 1..65535)

Health score:  (Range: 0..100)

DNS IP primary:

DNS IP backup1:

DNS IP backup2:

DNS domain:

DNS timeout:  (Range: 0..4294967295)

DNS max ttl:  (Range: 30..2073600)

Signaling mtu:  (Range: 0..576..4096)

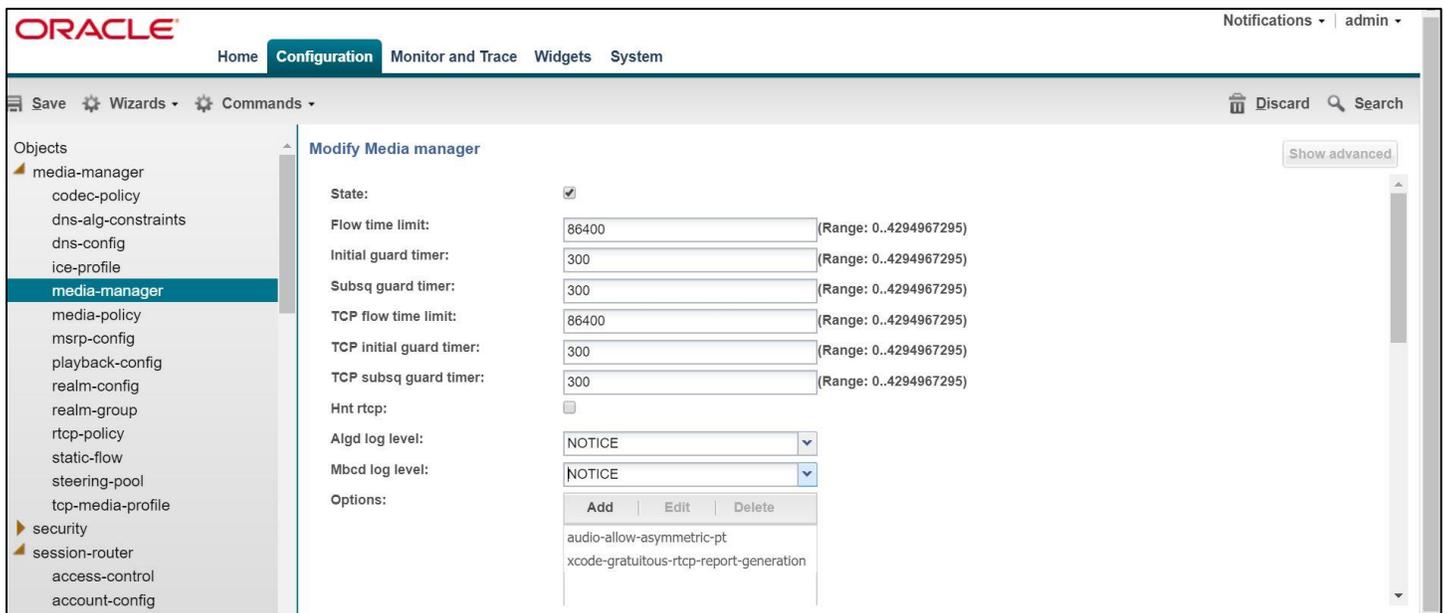
*Tip: Configure ICMP IP and HIP IP only on the PSTN side. It is not advisable to configure the ICMP ip and HIP ip on the teams facing side because of inherent risks.*

## 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-assymmetric-pt
- xcode-gratuitous-rtcp-report-generation (*requires a reboot of the SBC to take affect*)

Go to Media-Manager->Media-Manager



The screenshot displays the Oracle SBC Configuration web interface. The top navigation bar includes 'ORACLE', 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The user is logged in as 'admin'. The left sidebar shows a tree view of configuration objects, with 'media-manager' selected. The main content area is titled 'Modify Media manager' and contains the following settings:

State:	<input checked="" type="checkbox"/>
Flow time limit:	<input type="text" value="86400"/> (Range: 0..4294967295)
Initial guard timer:	<input type="text" value="300"/> (Range: 0..4294967295)
Subsq guard timer:	<input type="text" value="300"/> (Range: 0..4294967295)
TCP flow time limit:	<input type="text" value="86400"/> (Range: 0..4294967295)
TCP initial guard timer:	<input type="text" value="300"/> (Range: 0..4294967295)
TCP subsq guard timer:	<input type="text" value="300"/> (Range: 0..4294967295)
Hnt rtcp:	<input type="checkbox"/>
Algld log level:	<input type="text" value="NOTICE"/>
Mbcd log level:	<input type="text" value="NOTICE"/>
Options:	<div style="border: 1px solid #ccc; padding: 5px;"><p style="text-align: center;">Add   Edit   Delete</p><p>audio-allow-asymmetric-pt xcode-gratuitous-rtcp-report-generation</p></div>

## Configure Realms

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

Configure realm for teams as shown below

The screenshot shows the Oracle SBC Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a tree view shows 'realm-config' selected. The main area is titled 'Modify Realm config' and contains the following fields:

- Identifier:
- Description:
- Addr prefix:
- Network interfaces: 

<b>Add</b>	<b>Edit</b>	<b>Delete</b>
s0p0:0.4		
- Mm in realm:
- Mm in network:
- Mm same ip:

Configure the realm, similarly for SIP Trunk

The screenshot shows the Oracle SBC Configuration interface for a different realm. The top navigation bar and left tree view are the same. The main area is titled 'Modify Realm config' and contains the following fields:

- Identifier:
- Description:
- Addr prefix:
- Network interfaces: 

<b>Add</b>	<b>Edit</b>	<b>Delete</b>
s0p0:0.4		
- Mm in realm:
- Mm in network:
- Mm same ip:

## 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.

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

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  
sip-feature-caps  
sip-interface

### Modify SIP config

Show advanced

State:

Dialog transparency:

Home Realm ID:

Egress Realm ID:

Nat mode:

Registrar domain:

Registrar host:

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

Init timer:  (Range: 0..4294967295)

Max timer:  (Range: 0..4294967295)

Trans expire:  (Range: 0..4294967295)

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

Invite expire:  (Range: 0..4294967295)

Session max life limit:

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

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  
sip-feature-caps  
sip-interface  
sip-manipulation  
sip-monitoring  
sip-recursion-policy  
surrogate-agent  
survivability

### Modify SIP config

Show advanced

Registrar host:

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

Init timer:  (Range: 0..4294967295)

Max timer:  (Range: 0..4294967295)

Trans expire:  (Range: 0..4294967295)

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

Invite expire:  (Range: 0..4294967295)

Session max life limit:

Enforcement profile:

Red max trans:  (Range: 0..50000)

Options:

[Add](#) | [Edit](#) | [Delete](#)

inmanip-before-validate  
max-udp-length=0

## 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

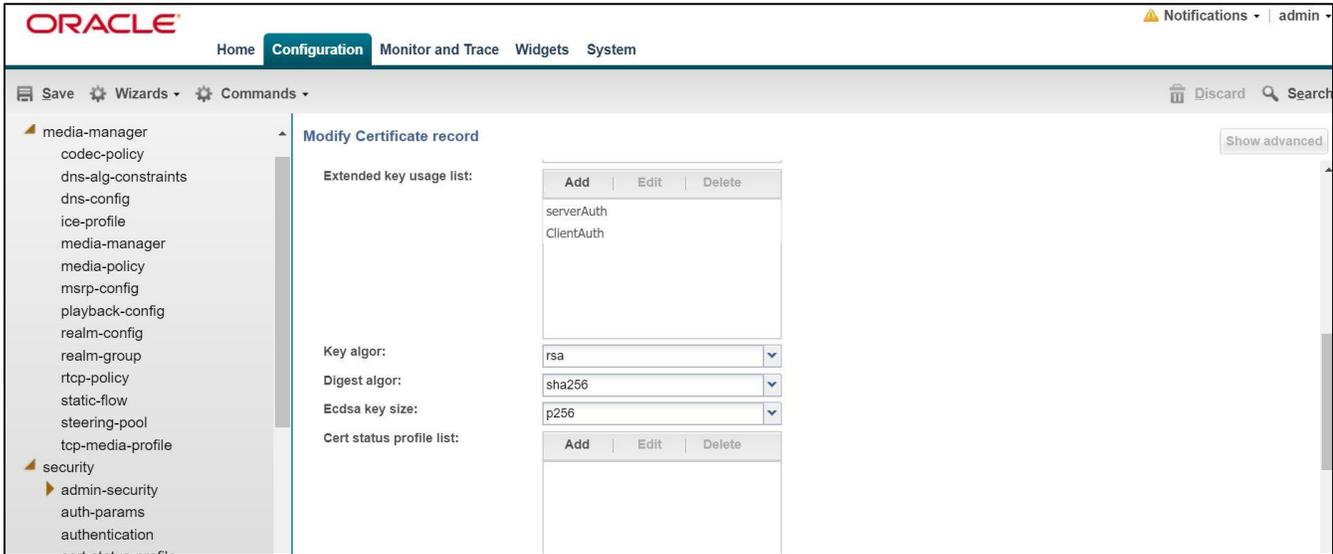
## SBC Certificate Creation

### Step 1 – Creating the SBC certificate record

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

The screenshot displays the Oracle SBC Configuration web interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar shows a tree view of configuration categories, with 'security' expanded to show 'admin-security', 'auth-params', 'authentication', and 'cert-status-profile'. The main content area is titled 'Modify Certificate record' and contains the following fields:

Name:	<input type="text" value="\$SBCCertificate"/>									
Country:	<input type="text" value="US"/>									
State:	<input type="text" value="MA"/>									
Locality:	<input type="text" value="Bedford"/>									
Organization:	<input type="text" value="sales"/>									
Unit:	<input type="text"/>									
Common name:	<input type="text" value="Oraclesbc2.woodgrovebank.us"/>									
Key size:	<input type="text" value="2048"/>									
Alternate name:	<input type="text"/>									
Trusted:	<input checked="" type="checkbox"/>									
Key usage list:	<table border="1"><tr><td><input type="button" value="Add"/></td><td><input type="button" value="Edit"/></td><td><input type="button" value="Delete"/></td></tr><tr><td colspan="3">digitalSignature</td></tr><tr><td colspan="3">keyEncipherment</td></tr></table>	<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	digitalSignature			keyEncipherment		
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>								
digitalSignature										
keyEncipherment										



## 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.

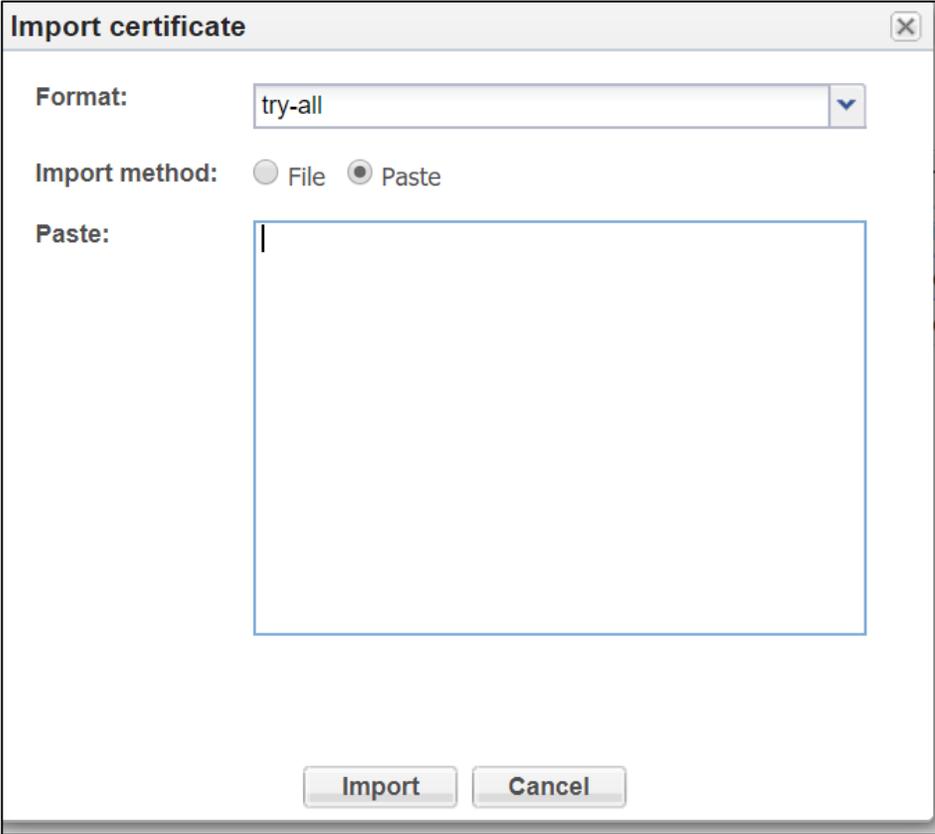


- Also, note that a save/activate is required

## 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** [X]

**Format:** try-all [v]

**Import method:**  File  Paste

**Paste:**

[Empty text area]

[Import] [Cancel]

## 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

## Step1-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 keyEncipherment	digitalSignature keyEncipherment	digitalSignature keyEncipherment
Extended-key-usage-list	serverAuth	serverAuth	serverAuth
key-algor	rsa	rsa	rsa
digest-algor	sha256	sha256	sha256

## Step2: Deploying the Root and Intermediate certificates on SBC

All the root and intermediate certificates have to be 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** [X]

**Format:** try-all [v]

**Import method:**  File  Paste

**Certificate file:** C:\fakepath\crtww.pem **Browse...**

**Import** **Cancel**

## 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

The screenshot shows the Oracle SBC Configuration interface. The 'Configuration' tab is active. The left sidebar shows a tree view of configuration objects, with 'tls-profile' selected. The main area displays the 'Modify TLS profile' configuration form. The form includes the following fields and options:

- Name:** |TLSTeams
- End entity certificate:** SBCEnterpriseCert
- Trusted ca certificates:** A list containing 'BaltimoreRoot' with 'Add', 'Edit', and 'Delete' buttons.
- Cipher list:** A list containing 'DEFAULT' with 'Add', 'Edit', and 'Delete' buttons.
- Verify depth:** 10
- Mutual authenticate:**
- TLS version:** tlsv12

## 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.

The screenshot shows the Oracle Configuration Assistant interface for configuring a SIP interface. The left-hand navigation menu lists various configuration options, with 'sip-interface' selected. The main configuration area is titled 'Modify SIP interface' and includes the following fields and table:

- State:**
- Realm ID:**
- Description:**
- SIP ports:**

Add   Edit   Copy   Delete				
Address	Port	Transport protocol	TLS profile	Allow anonymous
155.212.214.172	5061	TLS	TLSTeams	agents-only
- Initial inv trans expire:**  (Range: 0..999999999)

## Configure sip-interface to communicate with SIP Trunk

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

The screenshot shows the Oracle Configuration Assistant interface for configuring a SIP interface for a SIP trunk. The left-hand navigation menu lists various configuration options, with 'sip-interface' selected. The main configuration area is titled 'Modify SIP interface' and includes the following fields and table:

- State:**
- Realm ID:**
- Description:**
- SIP ports:**

Add   Edit   Copy   Delete				
Address	Port	Transport protocol	TLS profile	Allow anonymous
192.65.79.126	5060	UDP		agents-only
- Initial inv trans expire:**  (Range: 0..999999999)
- Session max life limit:**

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.

## 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

ORACLE Notifications | admin

Home Configuration Monitor and Trace Widgets System

Save Wizards Commands Discard Search

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

### Modify Session agent

Show advanced Show configuration

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

Add Edit Copy Delete

ORACLE Notifications | admin

Home Configuration Monitor and Trace Widgets System

Save Wizards Commands Discard Search

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

### Modify Session agent

Show advanced Show configuration

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:

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 should be sent to sip-all.pstnhub.microsoft.com FQDN. The sip-all.pstnhub.microsoft.com FQDN is only used for longer DNS TTL value*

Hostname	IP address	Port	State	App protocol	Realm ID	Description
ATTrunk	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	

## Create a Session Agent Group

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

The screenshot shows the Oracle SBC configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a tree view shows the configuration hierarchy, with 'session-group' selected. The main area displays the 'Modify Session group' form. The form fields are: 'Group name' (TeamsGrp), 'Description' (empty), 'State' (checked), 'App protocol' (SIP), 'Strategy' (RoundRobin), and 'Dest' (a list of three Microsoft SIP addresses: sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com, and sip3.pstnhub.microsoft.com). There are 'Add', 'Edit', and 'Delete' buttons for the destination list. A 'Trunk group' field is also visible at the bottom.

This screenshot shows the same 'Modify Session group' form, but with advanced options expanded. The 'Dest' field now shows a scrollable list of the three Microsoft SIP addresses. Below it, the 'Trunk group' field has 'Add', 'Edit', and 'Delete' buttons. Further down, the 'Sag recursion' checkbox is checked, 'Stop sag recurse' is set to 401,407,480, and 'SIP recursion policy' is set to a default value. A 'Show advanced' button is visible in the top right corner of the form area.

## 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:

The screenshot shows the Oracle configuration interface for 'Modify Local policy'. The left sidebar lists various configuration options, with 'local-policy' selected. The main area contains three fields: 'From address:', 'To address:', and 'Source realm:'. Each field has an 'Add', 'Edit', and 'Delete' button above it. The 'From address:' and 'To address:' fields currently contain an asterisk (\*). The 'Source realm:' field is empty. There are 'Show advanced' and 'Show configuration' buttons in the top right corner.

The screenshot shows the Oracle configuration interface for 'Modify Local policy' with more details. The left sidebar lists various configuration options, with 'local-policy' selected. The main area contains several fields: 'Description:', 'State:', 'Policy priority:', and 'Policy attributes'. The 'State:' field has a checked checkbox. The 'Policy priority:' field has a dropdown menu set to 'none'. The 'Policy attributes' section contains a table with columns: 'Add', 'Edit', 'Copy', 'Delete', 'Next hop', 'Realm', 'Action', 'Terminate recursion', and 'Cost'. The table has one row with the following data:

Add	Edit	Copy	Delete	Next hop	Realm	Action	Terminate recursion	Cost
				ATTTrunk	access-pstn	none	disabled	0

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

**local-policy** Show advanced

Modify Local policy / policy attribute

Next hop:

Realm:

Action:

Terminate recursion:

Cost:  (Range: 0..999999999)

State:

App protocol:

Lookup:

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

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

**local-policy** Show advanced Show configuration

Modify Local policy

From address:  Add Edit Delete

To address:  Add Edit Delete

Source realm:  Add Edit Delete

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

local-policy **Modify Local policy** Show advanced Show configuration

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

access-pstn

Description:

State:

Policy priority: none

Policy attributes

Add	Edit	Copy	Delete					
Next hop	Realm	Action	Terminate recursion	Cost				
sag:TeamsGrp	access-teams	none	disabled	0				

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

home-subscriber-server  
http-alg  
iwf-config  
ldap-config  
**local-policy**  
local-response-map  
local-routing-config  
media-profile  
net-management-control  
qos-constraints  
response-map  
service-health  
session-agent  
session-agent-id-rule  
session-constraints  
session-group  
session-recording-group  
session-recording-server  
session-timer-profile  
session-translation

**Modify Local policy / policy attribute** Show advanced

Next hop: sag:TeamsGrp

Realm: Teams

Action: none

Terminate recursion:

Cost: 0 (Range: 0..99999999)

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.

## 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 & CN offered by Microsoft teams are using a payload type which is different than usual. Configure the media-profile as shown below, go to Session-Router->Media-profile

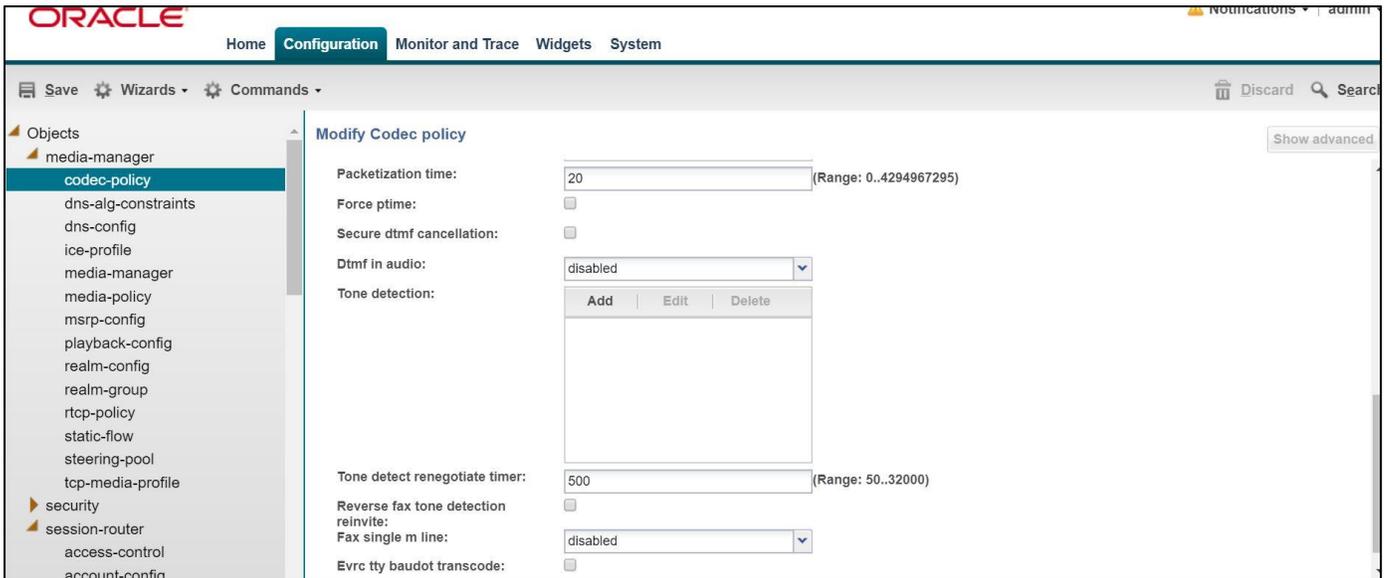
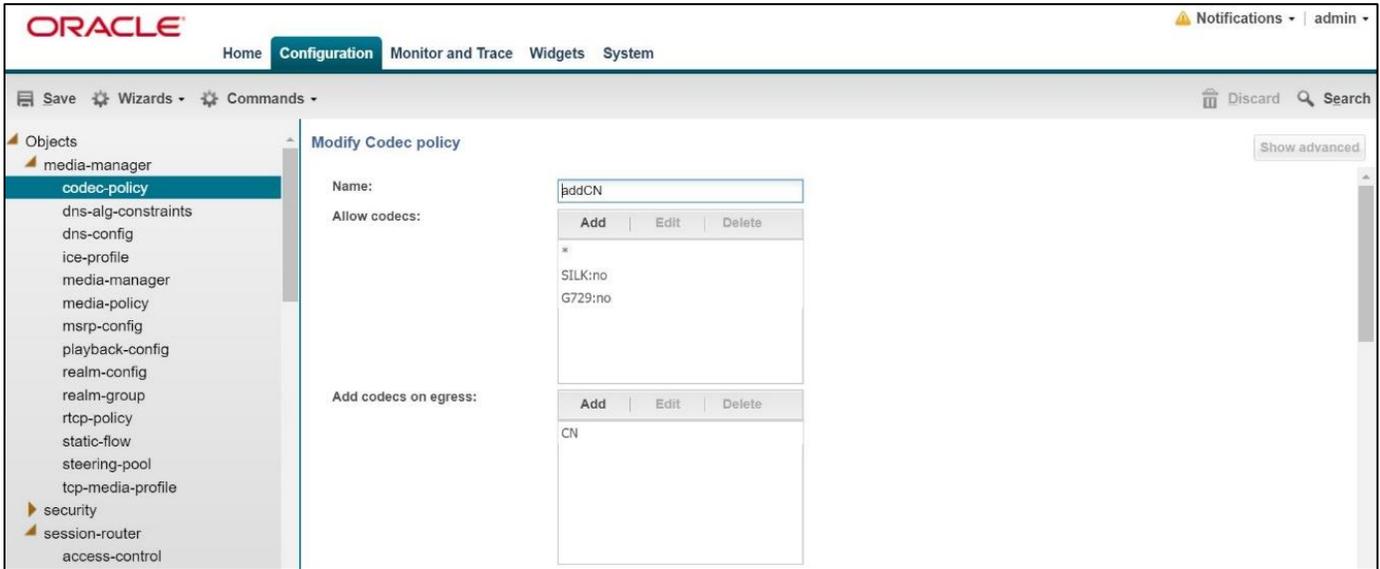
The screenshot shows the Oracle SBC configuration interface. The left sidebar lists various configuration categories, with 'media-profile' highlighted. The main area displays the 'Modify Media profile' form with the following values:

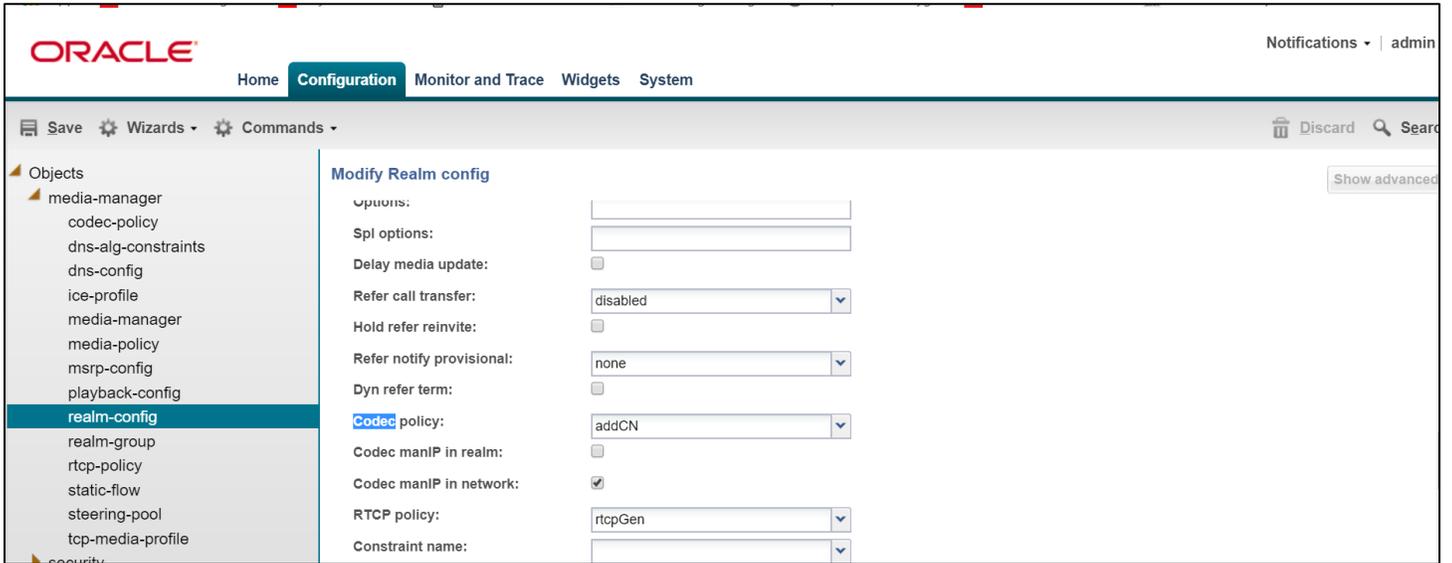
- Name: CN
- Subname: wideband
- Media type: audio
- Payload type: 118
- Transport: RTP/AVP
- Clock rate: 16000 (Range: 0..4294967295)
- Req bandwidth: 0 (Range: 0..999999999)
- Frames per packet: 0 (Range: 0..256)
- Parameters: Add, Edit, Delete

Configure media profiles similarly, for silk codec also.

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

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





## Configure sip-manipulations

### 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 rcv 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 latest GA release, SCZ830m1p7, 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.*

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

**Objects**

- media-manager
- security
- session-router
  - access-control
  - account-config
  - filter-config
  - ldap-config
  - local-policy
  - local-routing-config
  - media-profile
  - session-agent
  - session-group
  - session-recording-group
  - session-recording-server
  - session-translation
  - sip-config
  - sip-feature

**Add SIP manipulation** Show advanced

Name:

Description:

Split headers:

Add | Edit | Delete

Join headers:

Add | Edit | Delete

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

**Objects**

- media-manager
- security
- session-router
  - access-control
  - account-config
  - filter-config
  - ldap-config
  - local-policy
  - local-routing-config
  - media-profile
  - session-agent
  - session-group
  - session-recording-group
  - session-recording-server
  - session-translation
  - sip-config
  - sip-feature
  - sip-interface

**Modify SIP manipulation** Show advanced Show configuration

Join headers:

Add | Edit | Delete

CfgRules

Add   Edit   Copy   Delete   Move up   Move down	
Name	Element type
Countrycode	header-rule
Change_fromip_fqdn	header-rule
Change_to_userandhost	header-rule
Addcontactheaderinoptions	header-rule
Recordroute	header-rule

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
- security
- session-router
  - access-control
  - account-config
  - filter-config
  - ldap-config
  - local-policy
  - local-routing-config
  - media-profile
  - session-agent
  - session-group
  - session-recording-group
  - session-recording-server
  - session-translation
  - sip-config
  - sip-feature
  - sip-interface
  - sip-manipulation

**Modify SIP manipulation** Show advanced Show configuration

Join headers: Add Edit Delete

CfgRules

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

## Countrycode Manipulation:

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

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
- security
- session-router
  - access-control
  - account-config
  - filter-config
  - ldap-config
  - local-policy
  - local-routing-config
  - media-profile
  - session-agent
  - session-group
  - session-recording-group
  - session-recording-server
  - session-translation
  - sip-config
  - sip-feature
  - sip-interface

**Modify SIP manipulation / header rule** Show advanced

Name:

Header name:

Action:

Comparison type:

Msg type:

Methods: Add Edit Delete

INVITE

Match value:

New value:

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

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  
 sip-feature-caps  
 sip-interface  
**sip-manipulation**  
 sip-monitoring  
 sip-recursion-policy  
 surrogate-agent

Modify SIP manipulation / header rule Show advanced

Match value:

New value:

CfgRules

Name	Element type
uriuser2	element-rule

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

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  
 sip-feature-caps  
 sip-interface  
**sip-manipulation**  
 sip-monitoring  
 sip-recursion-policy  
 surrogate-agent  
 survivability

Modify SIP manipulation / header rule / element rule Show advanced

Name:

Parameter name:

Type:

Action:

Match val type:

Comparison type:

Match value:

New value:

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

## Change\_fromip\_fqdn Manipulation:

It is configured as a header rule in the sip-manipulation Teamsoutmanip. Here the host uri is changed to oracleesbc2.woodgroovebank.us as shown below

The screenshot shows the Oracle Configuration Manager interface. The left sidebar contains a tree view of configuration categories, with 'h323' expanded. The main area is titled 'Modify SIP manipulation / header rule'. The configuration fields are as follows:

- Name: Change\_Fromip\_fqdn
- Header name: From
- Action: manipulate
- Comparison type: case-sensitive
- Msg type: any
- Methods: Invite
- Match value: (empty)

The screenshot shows the Oracle Configuration Manager interface with advanced options visible. The left sidebar shows a different set of configuration categories. The main area is titled 'Modify SIP manipulation / header rule'. The configuration fields are as follows:

- Match value: (empty)
- New value: (empty)
- CfgRules: A table with columns 'Name' and 'Element type'. The table contains one entry: 'INVITE'.

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar contains a list of configuration objects, with 'sip-manipulation' highlighted. The main content area is titled 'Modify SIP manipulation / header rule / element rule'. It contains the following fields:

- Name: FixUriHost
- Parameter name: (empty)
- Type: url-host
- Action: replace
- Match val type: ip
- Comparison type: case-sensitive
- Match value: (empty)
- New value: oracleesbc2.woodgrovebank.us

## 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.

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar shows a tree view of objects, with 'sip-manipulation' selected. The main content area is titled 'Add SIP manipulation / header rule'. It contains the following fields:

- Name: Change\_to\_userandhost
- Header name: To
- Action: manipulate
- Comparison type: case-sensitive
- Msg type: out-of-dialog
- Methods: INVITE
- Match value: (empty)
- New value: (empty)

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

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  
sip-feature-caps  
sip-interface  
**sip-manipulation**  
sip-monitoring  
sip-recursion-policy  
surrogate-agent

**Modify SIP manipulation / header rule** Show advanced

Match value:

New value:

CfgRules

Name	Element type
fixtouri	element-rule
urinumber	element-rule

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

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  
sip-feature-caps  
sip-interface  
**sip-manipulation**  
sip-monitoring  
sip-recursion-policy  
surrogate-agent  
survivability

**Modify SIP manipulation / header rule / element rule** Show advanced

Name:

Parameter name:

Type:

Action:

Match val type:

Comparison type:

Match value:

New value:

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar shows a tree view of objects, with 'session-router' expanded to show various configuration options. The main panel is titled 'Add SIP manipulation / header rule / element rule' and contains the following configuration fields:

- Name: urinumber
- Parameter name: (empty)
- Type: uri-user
- Action: replace
- Match val type: any
- Comparison type: case-sensitive
- Match value: (empty)
- New value: "\*" + \$

## Addcontactheaderinoptions

It is configured as a header rule in the sip-manipulation Teamsoutmanip. Here the contact is changed to “< sip:ping@oracleSBC.woodgrovebank.us:5061;transport=tls>”, according to MS Team requirements.

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar shows a tree view of objects, with 'sip-manipulation' selected. The main panel is titled 'Add SIP manipulation / header rule' and contains the following configuration fields:

- Name: Addcontactheaderinoptions
- Header name: Contact
- Action: add
- Comparison type: case-sensitive
- Msg type: out-of-dialog
- Methods: Add | Edit | Delete
- Match value: (empty)
- New value: |< sip:ping@oracleSBC.woodgrovebank.us:5061;transport=tls>|

At the bottom of the main panel, there are 'OK' and 'Back' buttons.

## Recordroute

It is configured as a header rule in the sip-manipulation Teamsoutmanip .Here Record-route is added to the OPTIONS message “< sip:oracleesbc2.woodgrovebank.us>”

The screenshot displays the Oracle Configuration Manager interface for configuring a SIP manipulation rule. The main window is titled "Add SIP manipulation / header rule".

- Name:** Recordroute
- Header name:** Record-Route
- Action:** add
- Comparison type:** case-sensitive
- Msg type:** out-of-dialog
- Methods:** A table with columns "Add", "Edit", and "Delete". The "Add" column contains the text "OPTIONS".
- Match value:** (Empty field)
- New value:** "< sip:oracleesbc2.woodgrovebank.us>"

The left sidebar shows a tree view of objects, with "sip-manipulation" selected. The top navigation bar includes "Home", "Configuration", "Monitor and Trace", "Widgets", and "System". The top right corner shows "Notifications" and "admin".

## 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)

The screenshot shows the Oracle Configuration Manager interface. The left sidebar lists various configuration categories, with 'sip-manipulation' selected. The main area displays the configuration for a header rule named 'alter\_contact'. The configuration includes:

- Name: alter\_contact
- Header name: Contact
- Action: manipulate
- Comparison type: case-sensitive
- Msg type: any
- Methods: INVITE
- Match value: (empty field)
- New value: (empty field)

The screenshot shows the Oracle Configuration Manager interface. The left sidebar lists various configuration categories, with 'sip-manipulation' selected. The main area displays the configuration for a header rule named 'Contact\_ip'. The configuration includes:

- Match value: (empty field)
- New value: (empty field)
- CfgRules table:

Name	Element type
Contact_ip	element-rule

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various objects, with 'sip-interface' selected. The main area is titled 'Add SIP manipulation / header rule / element rule'. The configuration fields are as follows:

Name:	Contact_ip
Parameter name:	contact_ip
Type:	uri-host
Action:	replace
Match val type:	any
Comparison type:	case-sensitive
Match value:	
New value:	oracleesbc2.woodgrovebank.us

## 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.

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various objects, with 'sip-manipulation' selected. The main area is titled 'Add SIP manipulation / header rule'. The configuration fields are as follows:

Name:	Adduseragent
Header name:	User-Agent
Action:	add
Comparison type:	case-sensitive
Msg type:	out-of-dialog
Methods:	<div style="border: 1px solid #ccc; padding: 5px;"> <span>Add</span>   <span>Edit</span>   <span>Delete</span> </div> INVITE
Match value:	
New value:	"Oracle ESBC"
CfgRules	

# 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.

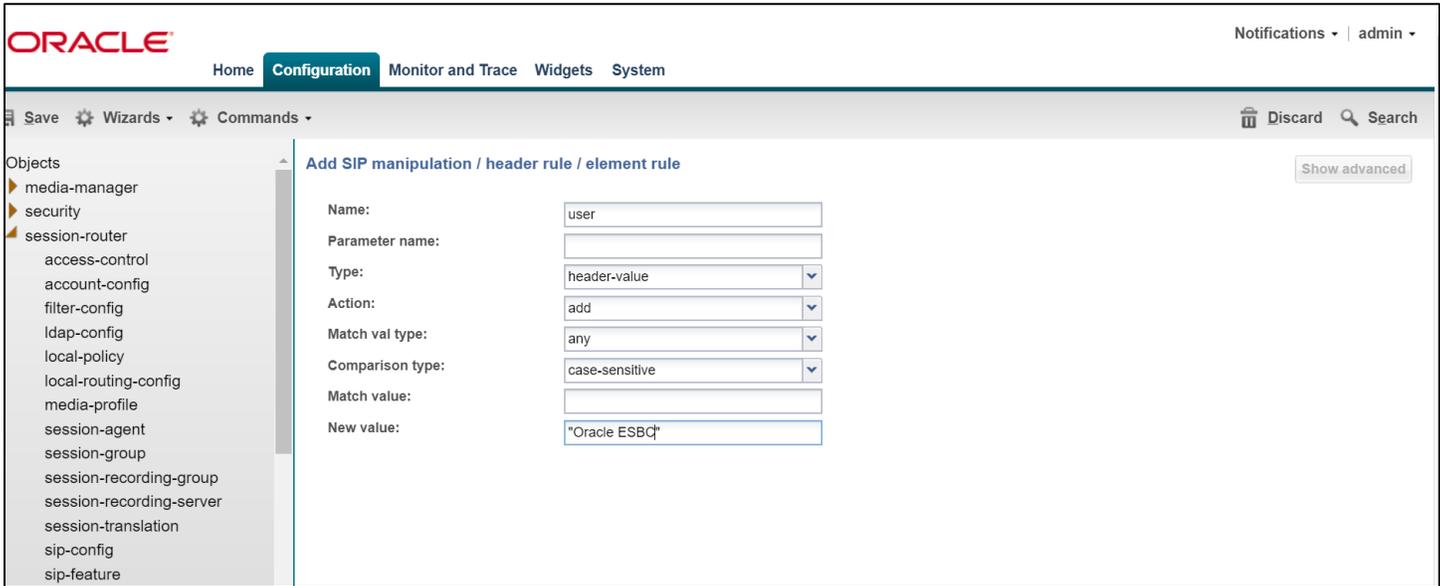
The screenshot shows the Oracle configuration interface for adding a SIP manipulation header rule. The breadcrumb trail is Home > Configuration > Monitor and Trace > Widgets > System. The left sidebar shows a tree view of objects, with 'sip-manipulation' selected. The main content area is titled 'Add SIP manipulation / header rule' and contains the following fields:

- Name: Modifyuseragent
- Header name: User-Agent
- Action: manipulate
- Comparison type: case-sensitive
- Msg type: out-of-dialog
- Methods: A list containing 'INVITE' with 'Add', 'Edit', and 'Delete' buttons.
- Match value: (empty text box)
- New value: (empty text box)
- CfgRules: (empty text box)

The screenshot shows the Oracle configuration interface for modifying a SIP manipulation header rule. The breadcrumb trail is Home > Configuration > Monitor and Trace > Widgets > System. The left sidebar shows a tree view of objects, with 'sip-manipulation' selected. The main content area is titled 'Modify SIP manipulation / header rule' and contains the following fields:

- Match value: (empty text box)
- New value: (empty text box)
- CfgRules: A table with the following data:

Add   Edit   Copy   Delete   Move up   Move down	
Name	Element type
user	element-rule



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

- [Reqsendonlytoinactive](#)
- [Replyrecvonlytoinactive](#)

## 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 latest GA release, SCZ830m1p7, 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.*

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
- security
- session-router
  - access-control
  - account-config
  - filter-config
  - ldap-config
  - local-policy
  - local-routing-config
  - media-profile
  - session-agent
  - session-group
  - session-recording-group
  - session-recording-server
  - session-translation
  - sip-config
  - sip-feature
  - sip-interface
  - sip-manipulation**

### Add SIP manipulation

Show advanced

Name:

Description:

Split headers:

Add | Edit | Delete

Join headers:

Add | Edit | Delete

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
- security
- session-router
  - access-control
  - account-config
  - filter-config
  - ldap-config
  - local-policy
  - local-routing-config
  - media-profile
  - session-agent
  - session-group
  - session-recording-group
  - session-recording-server
  - session-translation
  - sip-config
  - sip-feature
  - sip-interface

### Modify SIP manipulation

Show advanced Show configuration

Join headers:

Add | Edit | Delete

CfgRules

Add   Edit   Copy   Delete   Move up   Move down	
Name	Element type
Respondoptions	header-rule
Reqinactivetosendonly	mime-sdp-rule
Replyinactivetorecvonly	mime-sdp-rule
Change183to180	header-rule

## Responoptions

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

### Modify SIP manipulation / header rule

Name:	<input type="text" value="Responoptions"/>						
Header name:	<input type="text" value="From"/>						
Action:	<input type="text" value="reject"/> ▼						
Comparison type:	<input type="text" value="case-sensitive"/> ▼						
Msg type:	<input type="text" value="request"/> ▼						
Methods:	<table><tr><td>Add</td><td>Edit</td><td>Delete</td></tr><tr><td colspan="3">     </td></tr></table>	Add	Edit	Delete	     		
Add	Edit	Delete					
Match value:	<input type="text"/>						
New value:	<input type="text" value="200:OK"/>						

CfgRules

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

[“Change183to180”](#)

[Reqinactivetosendonly](#)

[Reqinactivetorecvonly](#)

## Applying the teams SIP manipulations to Teams SIP Interface

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

The screenshot shows the Oracle Configuration interface for the 'Modify SIP interface' page. The left sidebar contains a tree view of configuration categories, with 'sip-interface' selected. The main content area displays various configuration fields for the SIP interface, including 'Sip options', 'Trust mode', 'Max nat interval', 'Stop recurse', 'Port map start', 'Port map end', 'In manipulationid', 'Out manipulationid', 'SIP atcf feature', 'Rfc2833 payload', 'Rfc2833 mode', 'Response map', 'Local response map', and 'Sip agree feature'. The 'In manipulationid' and 'Out manipulationid' fields are set to 'Teamsinmanip' and 'Teamsoutmanip' respectively. The 'Rfc2833 payload' field is set to '101'. The 'Trust mode' is set to 'all'. The 'Max nat interval' is set to '3600'. The 'Stop recurse' is set to '401,407'. The 'Port map start' and 'Port map end' are both set to '0'. The 'SIP atcf feature' is unchecked. The 'Rfc2833 mode' is set to 'transparent'. The 'Response map' and 'Local response map' are empty. The 'Sip agree feature' is unchecked. The page includes a top navigation bar with 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. A 'Notifications' icon is in the top right. The left sidebar has 'Save', 'Wizards', and 'Commands' options. The main content area has 'Show advanced' and 'Show collapsed' buttons. The bottom of the page has 'OK' and 'Back' buttons.

**ORACLE** Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard

**Modify SIP interface**

Show advanced Show collapsed

Sip 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:

Sip agree feature:

OK Back

## 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..

The screenshot shows the Oracle Configuration Assistant interface. The 'Configuration' tab is active. The left sidebar shows the 'Objects' tree with 'sip-manipulation' selected. The main area displays the 'Add SIP manipulation' dialog. The 'Name' field contains 'Siptrunk\_outmanip'. The 'Description' field is empty. Below the 'Description' field are two sections: 'Split headers' and 'Join headers', each with 'Add', 'Edit', and 'Delete' buttons.

The screenshot shows the Oracle Configuration Assistant interface. The 'Configuration' tab is active. The left sidebar shows the 'Objects' tree with 'sip-manipulation' selected. The main area displays the 'Modify SIP manipulation' dialog. The 'Join headers' section is empty with 'Add', 'Edit', and 'Delete' buttons. Below this is a table labeled 'CfgRules' with the following data:

Name	Element type
Change_fqdn_to_ip_from	header-rule
Change_fqdn_to_ip_to	header-rule

## 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.

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'ORACLE', 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration objects, with 'session-router' expanded to show 'local-routing-config' selected. The main content area is titled 'Add SIP manipulation / header rule' and contains the following fields:

- Name: Change\_fqdn\_to\_ip\_from
- Header name: From
- Action: manipulate
- Comparison type: case-sensitive
- Msg type: out-of-dialog
- Methods: A table with columns 'Add', 'Edit', and 'Delete', and a single row containing 'INVITE'.
- Match value: (empty field)
- New value: (empty field)

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'ORACLE', 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration objects, with 'session-router' expanded to show 'sip-manipulation' selected. The main content area is titled 'Add SIP manipulation / header rule / element rule' and contains the following fields:

- Name: from\_uri
- Parameter name: (empty field)
- Type: uri-host
- Action: replace
- Match val type: any
- Comparison type: case-sensitive
- Match value: (empty field)
- New value: \$LOCAL\_IP

## 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

The screenshot shows the Oracle configuration interface for adding a SIP manipulation / header rule. The page title is "Add SIP manipulation / header rule". The left sidebar shows a tree view of objects, with "sip-manipulation" selected. The main form contains the following fields:

Name:	Change_fqdn_to_ip_to
Header name:	To
Action:	manipulate
Comparison type:	case-sensitive
Msg type:	out-of-dialog
Methods:	<input type="button" value="Add"/>   <input type="button" value="Edit"/>   <input type="button" value="Delete"/> INVITE
Match value:	
New value:	

At the bottom of the form, there is a label "CfoRules".

The screenshot shows the Oracle configuration interface for adding a SIP manipulation / header rule / element rule. The page title is "Add SIP manipulation / header rule / element rule". The left sidebar shows a tree view of objects, with "sip-manipulation" selected. The main form contains the following fields:

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

## 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

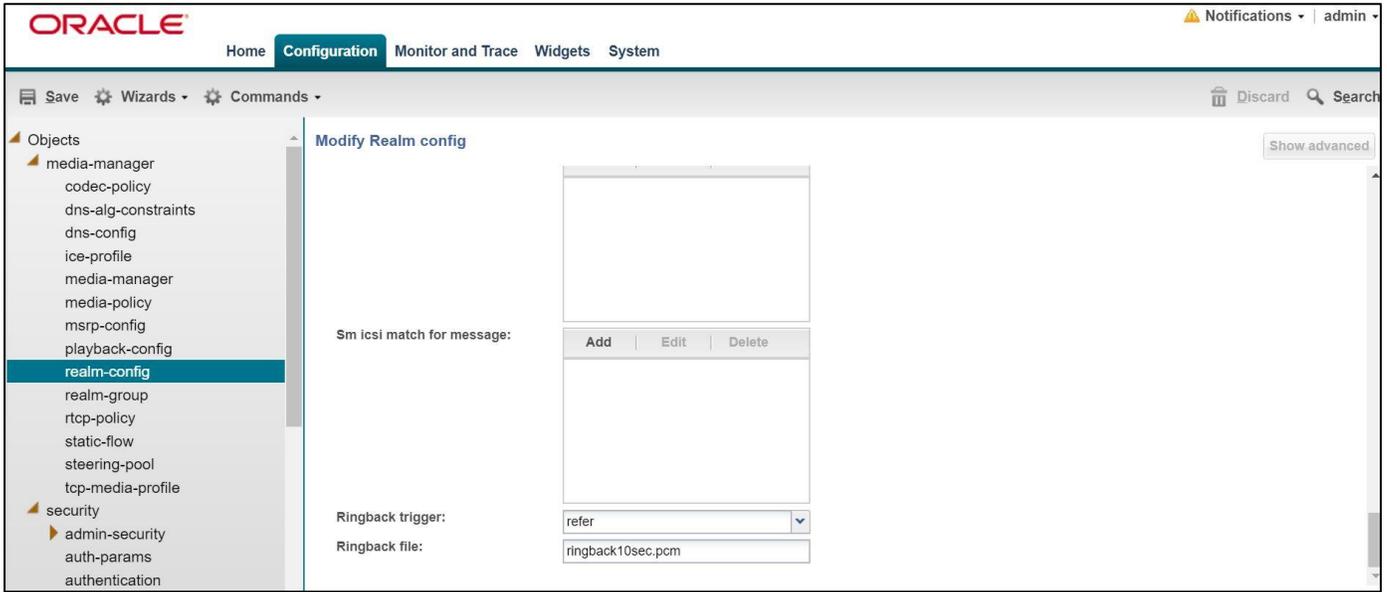
The screenshot shows the Oracle SBC Configuration interface. The 'Configuration' tab is active, and the 'Modify SIP interface' page is displayed. The left sidebar contains a list of configuration categories, with 'sip-feature' selected. The main area shows the configuration for the SIP interface, with the following fields and values:

Field	Value	Range
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:	<input type="checkbox"/>	
Rfc2833 payload:	101	(Range: 96..127)
Rfc2833 mode:	transparent	
Response map:		

## Ringback Configuration

### 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.



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=recvnly ,so that inactive is not sent towards PSTN.

The 200 OK response received from the trunk contains a=recvnly 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=recvnly to a=inactive in the 200 OK being sent to Teams for the msgtype “Request”.Here also we change the a=recvnly to a=inactive for the msgtype “reply” so that recvnly is not sent towards teams.

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

ORACLE Notifications ▾ | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards ⚙️ Commands ▾ Discard 🔍 Search

Objects

- ▶ media-manager
- ▶ security
- ▶ session-router
  - access-control
  - account-config
  - filter-config
  - ldap-config
  - local-policy
  - local-routing-config
  - media-profile
  - session-agent
  - session-group
  - session-recording-group
  - session-recording-server
  - session-translation
  - sip-config
  - sip-feature
  - sip-interface

**Add SIP manipulation / mime SDP rule** Show advanced

Name:

Msg type:

Methods:

Add | Edit | Delete

INVITE

Action:

Comparison type:

Match value:

New value:

CfgRules

Add ▾ | Edit | Copy | Delete | Move up | Move down

ORACLE ⚠️ Notifications ▾ | admin ▾

Home **Configuration** Monitor and Trace Widgets System

Save Wizards ⚙️ Commands ▾ Discard 🔍 Search

- 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
- sip-feature-caps
- sip-interface
- sip-manipulation**
- sip-monitoring
- sip-recursion-policy
- surrogate-agent
- survivability
- translation-rules

**Modify SIP manipulation / mime SDP rule / SDP media rule** Show advanced

Name:

Media type:

Action:

Comparison type:

Match value:

New value:

CfgRules

Add ▾ | Edit | Copy | Delete | Move up | Move down

Name	Element type
audio3	sdp-line-rule

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a tree view shows the configuration hierarchy under 'session-router', with 'sip-feature' selected. The main area is titled 'Add SIP manipulation / mime SDP rule / SDP media rule / SDP line rule'. The configuration fields are as follows:

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

## Consultative transfer configuration

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

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a tree view shows the configuration hierarchy under 'sip-feature', with 'sip-feature' selected. The main area is titled 'Modify SIP feature'. The configuration fields are as follows:

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

At the bottom of the main area, there are 'OK' and 'Back' buttons.

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

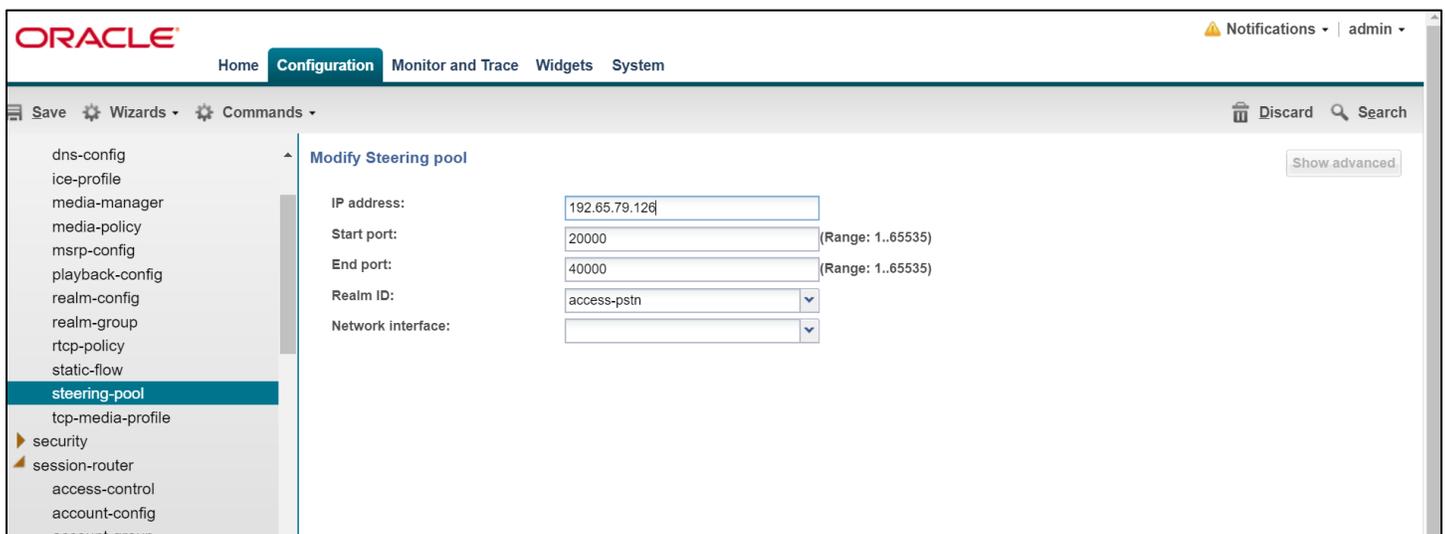
Note: The sip-profile element is available only through the CLI now. The GUI will be enhanced to support this in later releases.

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
```

## Configure steering pool

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



The screenshot shows the Oracle Configuration GUI. The top navigation bar includes 'ORACLE', 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The user is logged in as 'admin'. The left sidebar shows a tree view of configuration elements, with 'steering-pool' selected under 'session-router'. The main content area is titled 'Modify Steering pool' and contains the following configuration fields:

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

A 'Show advanced' button is visible in the top right corner of the configuration area.

ORACLE Notifications | admin

Home Configuration Monitor and Trace Widgets System

Save Wizards Commands Discard Search

dns-config  
ice-profile  
media-manager  
media-policy  
msrp-config  
playback-config  
realm-config  
realm-group  
rtcp-policy  
static-flow  
**steering-pool**  
tcp-media-profile  
security  
session-router  
access-control  
account-config

**Modify Steering pool** Show advanced

IP address: 155.212.214.172

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

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

Realm ID: access-teams

Network interface:

## 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.

ORACLE Notifications | admin

Home Configuration Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects  
media-manager  
security  
admin-security  
auth-params  
authentication  
cert-status-profile  
certificate-record  
ike  
ipsec  
media-security  
dtls-srtp-profile  
media-sec-policy  
**sdes-profile**  
sipura-profile  
password-policy  
public-key  
security-config  
ssh-config  
tis-global

**Modify Sdes profile** Show advanced

Name: SDES

Crypto list:  
Add Edit Delete  
AES\_CM\_128\_HMAC\_SHA1\_80

Srtp auth:

Srtp encrypt:

SrTCP encrypt:

Mki:

Egress offer format: same-as-ingress

Use ingress session params:  
Add Edit Delete

Make sure to configure 31 in the lifetime value as shown

The screenshot shows the Oracle Configuration interface. The left sidebar lists various objects, with 'sdes-profile' selected. The main area is titled 'Modify Sdes profile'. It contains an 'Options' table with 'Add', 'Edit', and 'Delete' buttons. Below the table are input fields for 'Key:', 'Salt:', 'Srtp rekey on re invite:' (a checkbox), and 'Lifetime:' (a text box containing '31' with a range of '0, 20..48').

## Media-sec-policy

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

The screenshot shows the Oracle Configuration interface for 'Modify Media sec policy'. The left sidebar has 'media-sec-policy' selected. The main area contains a 'Name:' field with 'RTP', a 'Pass through:' checkbox, and an 'Options' table with 'Add', 'Edit', and 'Delete' buttons. Below the table are sections for 'Inbound' and 'Outbound' profiles. The 'Inbound' section has dropdowns for 'Profile:', 'Mode:' (set to 'rtp'), and 'Protocol:' (set to 'none').

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
- security
  - admin-security
  - auth-params
  - authentication
  - cert-status-profile
  - certificate-record
  - ike
  - ipsec
  - media-security
    - dtls-srtp-profile
    - media-sec-policy**
    - sdes-profile
    - sipura-profile
    - password-policy
    - public-key
    - security-config
    - ssh-config
    - tls-global

**Modify Media sec policy** Show advanced

**Inbound**

Profile:

Mode:

Protocol:

**Outbound**

Profile:

Mode:

Protocol:

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
- security
  - admin-security
  - auth-params
  - authentication
  - cert-status-profile
  - certificate-record
  - ike
  - ipsec
  - media-security
    - dtls-srtp-profile
    - media-sec-policy**
    - sdes-profile
    - sipura-profile
    - password-policy
    - public-key
    - security-config
    - ssh-config
    - tls-global

**Modify Media sec policy** Show advanced

Name:

Pass through:

Options:

Add | Edit | Delete

**Inbound**

Profile:

Mode:

Protocol:

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, the 'Objects' tree is expanded to 'media-security' > 'media-sec-policy'. The main area is titled 'Modify Media sec policy' and contains two sections: 'Inbound' and 'Outbound'. Each section has three dropdown menus: 'Profile' (set to 'SDES'), 'Mode' (set to 'srtp'), and 'Protocol' (set to 'sdes'). A 'Show advanced' button is visible in the top right of the main area.

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.

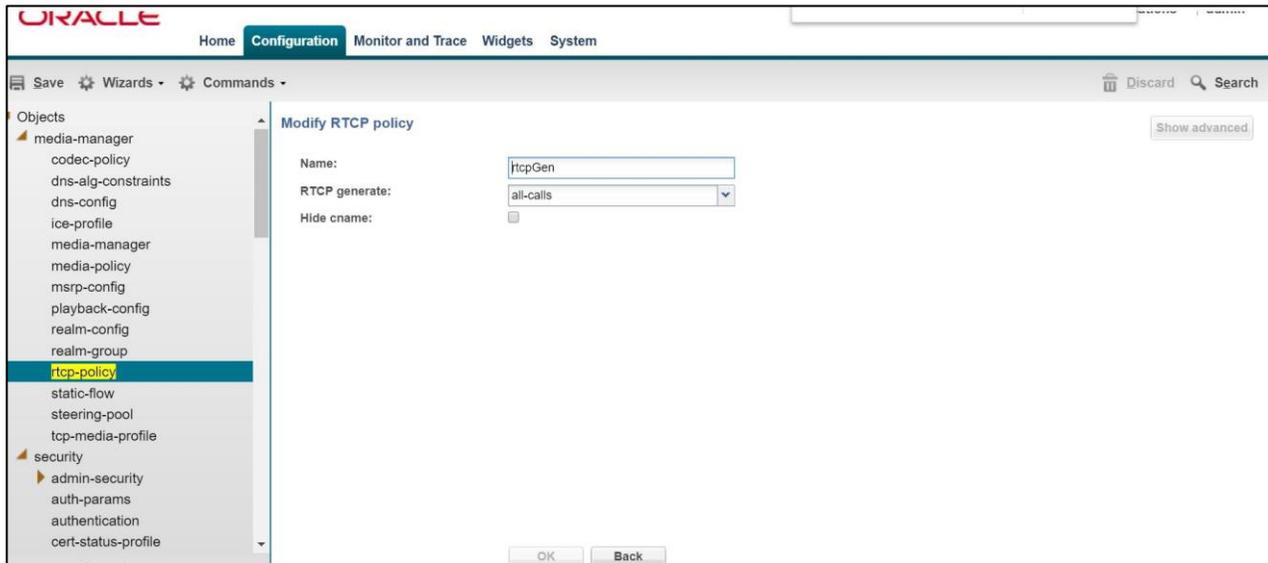
The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, the 'Objects' tree is expanded to 'media-security' > 'media-sec-policy'. The main area is titled 'Modify Realm config' and contains several configuration options:
 

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

 A 'Show advanced' button is visible in the top right of the main area.

## Configure RTCP Policy and RTCP Mux

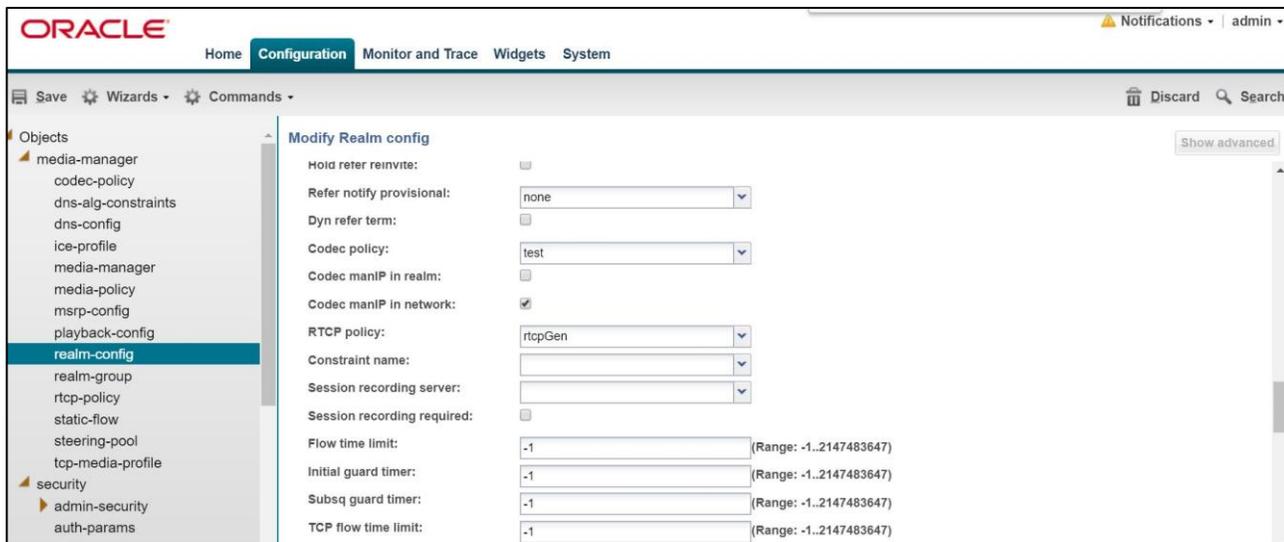
The following RTCP policy needs to be configured to generate RTCP reports towards Teams. It is applied on the realm facing Teams. Media Bypass enabled configuration requires support for RTCP-Mux. It can be enabled on the realm - Access-teams. Go to Media-manager->rtcp-policy to configure rtcp-policy.



The screenshot shows the Oracle Configuration interface. The left sidebar lists various configuration objects, with 'rtcp-policy' selected. The main area is titled 'Modify RTCP policy' and contains the following fields:

- Name:
- RTCP generate:
- Hide name:

Buttons for 'OK' and 'Back' are visible at the bottom.



The screenshot shows the Oracle Configuration interface. The left sidebar lists various configuration objects, with 'realm-config' selected. The main area is titled 'Modify Realm config' and contains the following fields:

- Hold refer reinvite:
- Refer notify provisional:
- Dyn refer term:
- Codec policy:
- Codec manIP in realm:
- Codec manIP in network:
- RTCP policy:
- Constraint name:
- Session recording server:
- Session recording required:
- Flow time limit:  (Range: -1..2147483647)
- Initial guard timer:  (Range: -1..2147483647)
- Subsq guard timer:  (Range: -1..2147483647)
- TCP flow time limit:  (Range: -1..2147483647)

Buttons for 'OK' and 'Back' are visible at the bottom.

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
  - codecs-policy
  - dns-alg-constraints
  - dns-config
  - ice-profile
  - media-manager
  - media-policy
  - msrp-config
  - playback-config
  - realm-config**
  - realm-group
  - rtcp-policy
  - static-flow
  - steering-pool
  - tcp-media-profile
- security
- session-router
- system

**Modify Realm config** Show advanced

RTCP mux:	<input checked="" type="checkbox"/>	
Ice profile:	<input type="text" value="ice"/>	
DTLS srtp profile:	<input type="text"/>	
Srtp msm passthrough:	<input type="checkbox"/>	
Class profile:	<input type="text"/>	
In translationid:	<input type="text"/>	
Out translationid:	<input type="text"/>	
In manipulationid:	<input type="text"/>	
Out manipulationid:	<input type="text"/>	
Average rate limit:	<input type="text" value="0"/>	(Range: 0..4294967295)
Access control trust level:	<input type="text" value="high"/>	
Invalid signal threshold:	<input type="text" value="0"/>	(Range: 0..4294967295)
Maximum signal threshold:	<input type="text" value="0"/>	(Range: 0..4294967295)

## Configure ice-profile

SBC supports ICE-Lite. This configuration is required to support MSTeams media-bypass. Configure the following ice profile and apply it on the realm towards Teams. Go to media-manager->ice-profile

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
  - codecs-policy
  - dns-alg-constraints
  - dns-config
  - ice-profile**
  - media-manager
  - media-policy
  - msrp-config
  - playback-config
  - realm-config
  - realm-group
  - rtcp-policy
  - static-flow

**Modify Ice profile** Show advanced

Name:	<input type="text" value="ice"/>	
Stun conn timeout:	<input type="text" value="0"/>	(Range: 0..9999)
Stun keep alive interval:	<input type="text" value="0"/>	(Range: 0..300)
Stun rate limit:	<input type="text" value="100"/>	(Range: 0..99999)

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a tree view shows 'Objects' with 'realm-config' selected. The main area is titled 'Modify Realm config' and contains the following settings:

- Initial inv trans expire: 0 (Range: 0..999999999)
- Session max life limit: 0
- Proxy mode: [Dropdown]
- Redirect action: [Dropdown]
- Nat traversal: always (Dropdown)
- Nat interval: 3600 (Range: 0..4294967295)
- TCP nat interval: 90 (Range: 0..4294967295)
- Registration caching:
- Min reg expire: 300 (Range: 0..999999999)

In addition to applying the ice-profile on the Teams realm, we need to enable nat-traversal on the sip-interface for this realm

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a tree view shows 'Objects' with 'realm-config' selected. The main area is titled 'Modify SIP interface' and contains the following settings:

- Initial inv trans expire: 0 (Range: 0..999999999)
- Session max life limit: 0
- Proxy mode: [Dropdown]
- Redirect action: [Dropdown]
- Nat traversal: always (Dropdown)
- Nat interval: 3600 (Range: 0..4294967295)
- TCP nat interval: 90 (Range: 0..4294967295)
- Registration caching:
- Min reg expire: 300 (Range: 0..999999999)

## 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](#)
- [RTCP-mux](#)
- [Ringback configuration](#)

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

## 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.

## E911

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

### 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:

### Translation Rule

GUI Path: session-router/translation-rule

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

- 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:

### Session Translation

GUI Path: session-router/session-translation

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

The screenshot shows the Oracle Configuration Assistant interface. At the top, the Oracle logo is on the left, and navigation tabs for 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System' are on the right. Below the navigation is a toolbar with 'Save', 'Wizards', and 'Commands' options. A left sidebar contains a tree view of configuration categories, with 'h323' selected. The main content area is titled 'Modify Session translation'. It features an 'Id:' field containing 'p11removeplus'. Below this are two sections: 'Rules calling:' and 'Rules called:'. Each section has a table with 'Add', 'Edit', and 'Delete' buttons. The 'Rules calling:' table contains one row with the value 'removeplus'. The 'Rules called:' table also contains one row with the value '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:

### Translation Added to Realm

GUI Path: media-manager/realm-config

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

Save Wizards Commands

- Objects
  - media-manager
    - codec-policy
    - dns-alg-constraints
    - dns-config
    - ice-profile
    - media-manager
    - media-policy
    - msrp-config
    - playback-config
    - realm-config**
    - realm-group
    - rtcp-policy
    - static-flow
    - steering-pool
    - tcp-media-profile
  - security
  - session-router
  - system

### Modify Realm config

Identifier:	<input type="text" value="ToTeams"/>						
Description:	<input type="text"/>						
Addr prefix:	<input type="text" value="0.0.0.0"/>						
Network interfaces:	<table border="1"><thead><tr><th>Add</th><th>Edit</th><th>Delete</th></tr></thead><tbody><tr><td colspan="3">s0p0:0</td></tr></tbody></table>	Add	Edit	Delete	s0p0:0		
Add	Edit	Delete					
s0p0:0							
Mm in realm:	<input checked="" type="checkbox"/>						
Mm in network:	<input checked="" type="checkbox"/>						
Mm same ip:	<input checked="" type="checkbox"/>						
QoS enable:	<input type="checkbox"/>						
Max bandwidth:	<input type="text" value="0"/>						
Max priority bandwidth:	<input type="text" value="0"/>						
Parent realm:	<input type="text"/>						
DNS realm:	<input type="text"/>						
Media policy:	<input type="text"/>						
Media sec policy:	<input type="text" value="SRTP"/>						
RTCP mux:	<input checked="" type="checkbox"/>						
Ice profile:	<input type="text" value="ice"/>						
DTLS srtp profile:	<input type="text"/>						
Srtp msm passthrough:	<input type="checkbox"/>						
Class profile:	<input type="text"/>						
In translationid:	<input type="text" value="911removeplus"/>						

## 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 Interface/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:*

### Local Policy Route for Emergency Calls

GUI Path: session-router/local-policy

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

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a navigation tree lists various configuration elements, with 'local-policy' selected. The main area is titled 'Modify Local policy' and contains the following fields:

- From address:** A text box containing an asterisk (\*).
- To address:** A list box containing '1911', '911', and '+1911'.
- Source realm:** A text box containing 'ToTeams'.
- Description:** An empty text box.
- State:** A checkbox that is checked.
- Policy priority:** A dropdown menu set to 'emergency'.

At the bottom, the 'Policy attributes' table is displayed:

Add	Edit	Copy	Delete	
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:

## 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-addr	
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	
<b>anonymous-priority</b>	<b>emergency</b>

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

## Net-Management Control

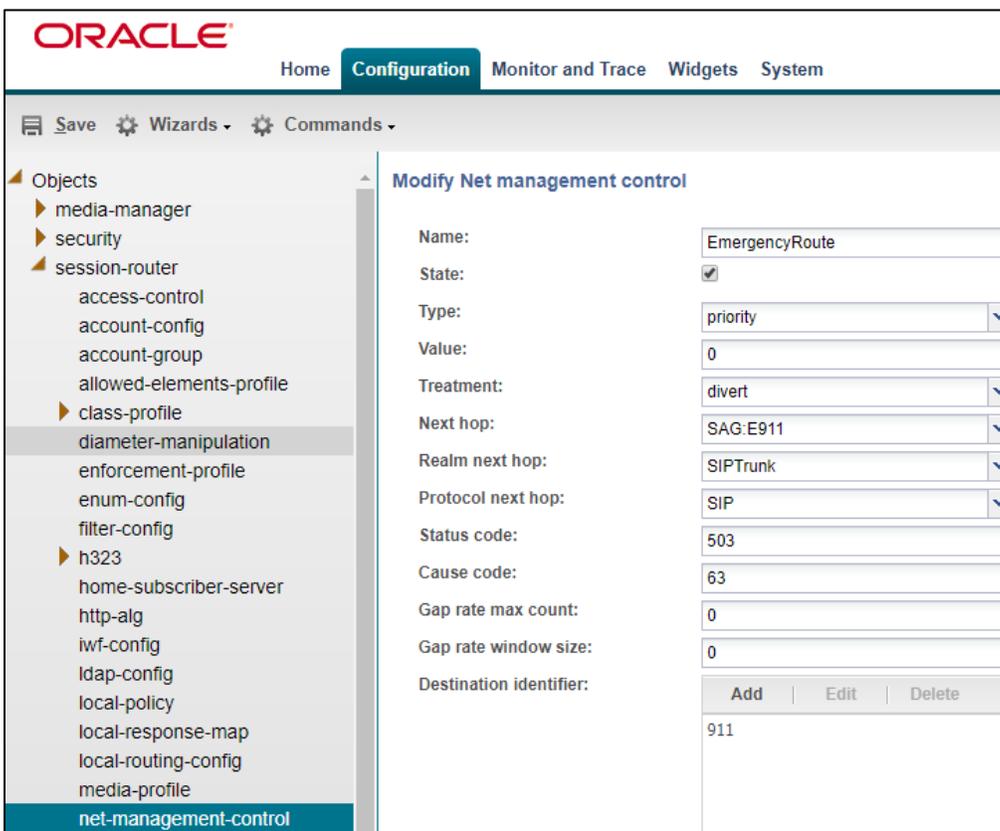
The Oracle Communications Session Border Controller supports network management controls for multimedia traffic specifically for static call gapping and 911 exemption handling. These controls limit the volume or rate of traffic for a specific set of dialed numbers or dialed number prefixes (destination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



The screenshot displays the Oracle Communications Session Border Controller (SBC) GUI. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, a tree view shows the configuration hierarchy: 'Objects' > 'session-router' > 'net-management-control'. The main area is titled 'Modify Net management control' and contains the following configuration fields:

Name:	EmergencyRoute						
State:	<input checked="" type="checkbox"/>						
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:	<table border="1"><tr><td>Add</td><td>Edit</td><td>Delete</td></tr><tr><td colspan="3">911</td></tr></table>	Add	Edit	Delete	911		
Add	Edit	Delete					
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.*

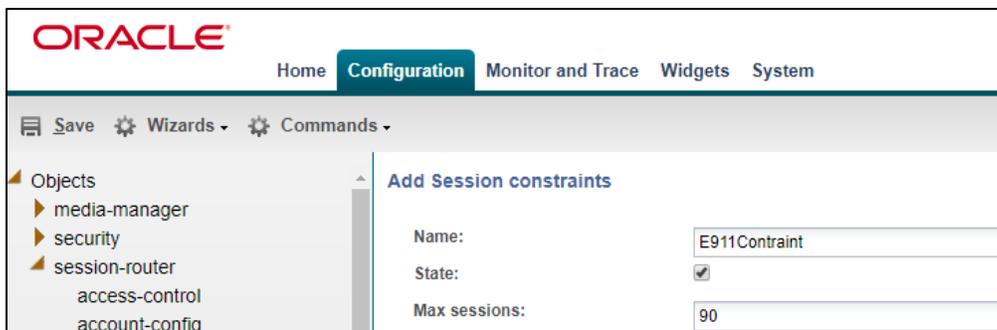
## Session Constraints for E911

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.

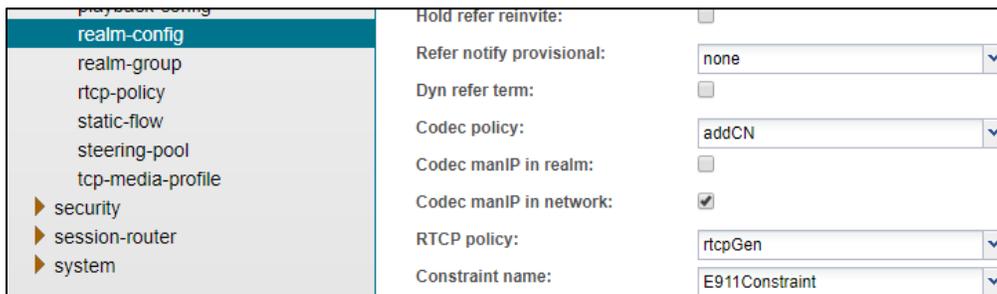
GUI Path: session-router/session-constraints

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



The screenshot shows the Oracle SBC GUI configuration page for 'Add Session constraints'. The 'Name' field is 'E911Constraint', 'State' is checked, and 'Max sessions' is set to 90. The left sidebar shows a tree view with 'session-router' expanded.

And now we apply this constraint to realms:



The screenshot shows the Oracle SBC GUI configuration page for 'realm-config'. The 'Constraint name' field is set to 'E911Constraint'. Other fields include 'Refer notify provisional' (none), 'Codec policy' (addCN), and 'RTCP policy' (rtcpGen).

## 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.

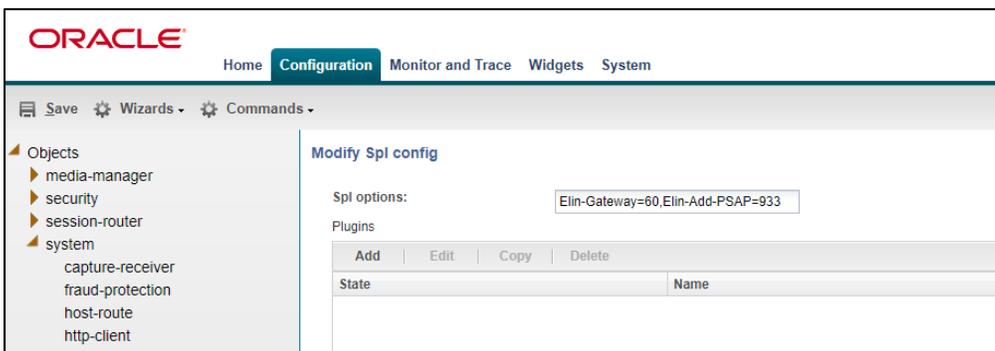
An optional configuration parameter:

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



## 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/pdf+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/pdf+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

## Appendix A

### 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 latest GA release, SCZ830m1p7, 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.*

The screenshot shows the Oracle SBC Configuration web interface. The top navigation bar includes 'ORACLE', 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The user is logged in as 'admin'. The main content area is titled 'Add SIP manipulation' and contains the following fields:

- Name:** Checkfor1831
- Description:** (empty text area)
- Split headers:** (empty list with 'Add', 'Edit', and 'Delete' buttons)
- Join headers:** (empty list with 'Add', 'Edit', and 'Delete' buttons)

A 'Show advanced' button is visible in the top right corner of the configuration area. The left sidebar shows a tree view of configuration objects, with 'sip-interface' selected under the 'session-router' category.

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  
 sip-feature-caps  
 sip-interface  
**sip-manipulation**  
 sip-monitoring  
 sip-recursion-policy  
 surrogate-agent

### Modify SIP manipulation

Show advanced Show configuration

CfgRules

Name	Element type
check183	header-rule
if183	mime-sdp-rule
deletesdp	mime-sdp-rule
change183to180	header-rule

OK Back

ORACLE Notifications admin

Home Configuration Monitor and Trace Widgets System

Save Wizards Commands Discard Search

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  
 sip-feature-caps  
 sip-interface  
**sip-manipulation**  
 sip-monitoring  
 sip-recursion-policy  
 surrogate-agent

### Modify SIP manipulation / header rule

Show advanced

Name:

Header name:

Action:

Comparison type:

Msg type:

Methods:

Add	Edit	Delete
INVITE		

Match value:

OK Back

ORACLE Notifications admin

Home Configuration Monitor and Trace Widgets System

Save Wizards Commands Discard Search

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  
 sip-feature-caps  
 sip-interface  
**sip-manipulation**  
 sip-monitoring  
 sip-recursion-policy  
 surrogate-agent

### Modify SIP manipulation / header rule / element rule

Show advanced

Name:

Parameter name:

Type:

Action:

Match val type:

Comparison type:

Match value:

New value:

OK Back

ORACLE Notifications | admin

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
- security
- session-router
  - access-control
  - account-config
  - filter-config
  - ldap-config
  - local-policy
  - local-routing-config
  - media-profile
  - session-agent
  - session-group
  - session-recording-group
  - session-recording-server
  - session-translation
  - sip-config
  - sip-feature
  - sip-interface

**Add SIP manipulation / mime SDP rule** Show advanced

Name:

Msg type:

Methods:

Add Edit Delete

INVITE

Action:

Comparison type:

Match value:

New value:

CfgRules

ORACLE Notifications |

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands Discard Search

Objects

- media-manager
- security
- session-router
  - access-control
  - account-config
  - filter-config
  - ldap-config
  - local-policy
  - local-routing-config
  - media-profile
  - session-agent
  - session-group
  - session-recording-group
  - session-recording-server
  - session-translation
  - sip-config
  - sip-feature
  - sip-interface
  - sip-manipulation**
  - sip-monitoring

**Add SIP manipulation / mime SDP rule / SDP session rule** Show advanced

Name:

Action:

Comparison type:

Match value:

New value:

CfgRules

Add Edit Copy Delete Move up Move down

Name	Element type

OK Back

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

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes "Home", "Configuration", "Monitor and Trace", "Widgets", and "System". The "Configuration" tab is active. On the left, a tree view shows the configuration hierarchy: "Objects" > "session-router" > "sip-config". The main area is titled "Add SIP manipulation / mime SDP rule / SDP session rule / SDP line rule". The configuration fields are as follows:

- Name: checkc
- Type: c
- Action: store
- Comparison type: pattern-rule
- Match value: ^((?!155.214.212.172)))\$
- New value: (empty)

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes "Home", "Configuration", "Monitor and Trace", "Widgets", and "System". The "Configuration" tab is active. On the left, a tree view shows the configuration hierarchy: "Objects" > "session-router" > "sip-interface" > "sip-manipulation". The main area is titled "Add SIP manipulation / mime SDP rule". The configuration fields are as follows:

- Name: deletesdp
- Msg type: reply
- Methods: INVITE
- Action: delete
- Comparison type: boolean
- Match value: \$if183.\$au.\$checkc
- New value: (empty)

At the bottom, there is a "CfgRules" section with buttons: Add, Edit, Copy, Delete, Move up, Move down.

- Objects
  - media-manager
  - security
  - session-router
    - access-control
    - account-config
    - filter-config
    - ldap-config
    - local-policy
    - local-routing-config
    - media-profile
    - session-agent
    - session-group
    - session-recording-group
    - session-recording-server
    - session-translation
    - sip-config
    - sip-feature
    - sip-interface
    - sip-manipulation**

Add SIP manipulation / header rule

Show advanced

Name:

Header name:

Action:

Comparison type:

Msg type:

Methods:  |  |

Match value:

New value:

CfgRules

- Objects
  - media-manager
  - security
  - session-router
    - access-control
    - account-config
    - filter-config
    - ldap-config
    - local-policy
    - local-routing-config
    - media-profile
    - session-agent
    - session-group
    - session-recording-group
    - session-recording-server
    - session-translation
    - sip-config

Modify SIP manipulation / header rule

Show advanced

Match value:

New value:

CfgRules

Add		Edit	Copy	Delete	Move up	Move down
Name	Element type					
modstatus	element-rule					
modreasonphrase	element-rule					

ORACLE Notifications ▾ | admin ▾

Home **Configuration** Monitor and Trace Widgets System

Save Wizards ⚙️ Commands ▾ Discard 🔍 Search

Objects

- ▶ media-manager
- ▶ security
- ▶ session-router
  - access-control
  - account-config
  - filter-config
  - ldap-config
  - local-policy
  - local-routing-config
  - media-profile
  - session-agent
  - session-group
  - session-recording-group
  - session-recording-server
  - session-translation
  - sip-config
  - sip-feature

**Add SIP manipulation / header rule / element rule** Show advanced

Name:

Parameter name:

Type:

Action:

Match val type:

Comparison type:

Match value:

New value:

ORACLE Notifications ▾ | admin ▾

Home **Configuration** Monitor and Trace Widgets System

Save Wizards ⚙️ Commands ▾ Discard 🔍 Search

Objects

- ▶ media-manager
- ▶ security
- ▶ session-router
  - access-control
  - account-config
  - filter-config
  - ldap-config
  - local-policy
  - local-routing-config
  - media-profile
  - session-agent
  - session-group
  - session-recording-group
  - session-recording-server
  - session-translation
  - sip-config
  - sip-feature

**Add SIP manipulation / header rule / element rule** Show advanced

Name:

Parameter name:

Type:

Action:

Match val type:

Comparison type:

Match value:

New value:

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

The screenshot displays the Oracle Configuration Assistant interface. The top navigation bar includes the Oracle logo, a 'Home' button, and tabs for 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. Below the navigation bar, there are buttons for 'Save', 'Wizards', and 'Commands'. On the right side of this bar, there are 'Discard' and 'Search' buttons. A left-hand sidebar lists various configuration objects, with 'sip-manipulation' selected and highlighted in blue. The main content area is titled 'Add SIP manipulation / header rule' and contains the following configuration fields:

- Name:** Change183to180
- Header name:** From
- Action:** sip-manip
- Comparison type:** case-sensitive
- Msg type:** any
- Methods:** A table with columns 'Add', 'Edit', and 'Delete'.
- Match value:** (empty field)
- New value:** Checkfor1831

At the bottom left of the main area, the text 'CfgRules' is visible. A 'Show advanced' button is located in the top right corner of the configuration area.

# Appendix B

## 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](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....

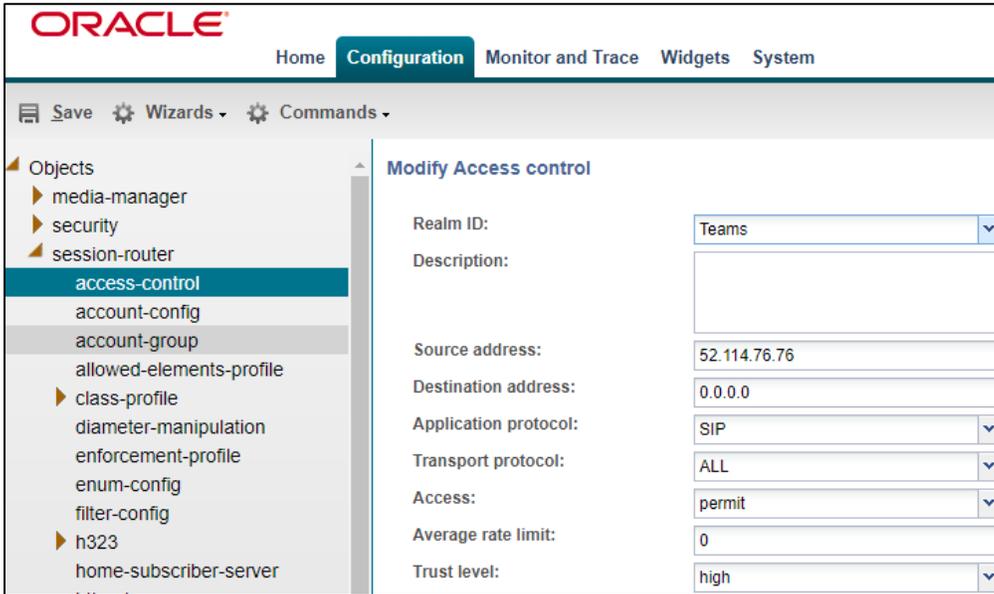
### Access Control

GUI Path: session-router/access-control

ACL 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.



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

## Realm Config

GUI Path: media-manager/realm-config

ACL 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](#)

**ORACLE** Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands

**Objects**

- media-manager
  - codec-policy
  - dns-alg-constraints
  - dns-config
  - ice-profile
  - media-manager
  - media-policy
  - msrp-config
  - playback-config
  - realm-config**
  - realm-group
  - rtcp-policy
  - static-flow
  - steering-pool
  - tcp-media-profile
- security
- session-router
- system

**Modify Realm config**

Identifier: Teams

Description: Realm Facing Teams Direct Routing

Addr prefix: 0.0.0.0

Network interfaces:
 

Add	Edit	Delete
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:

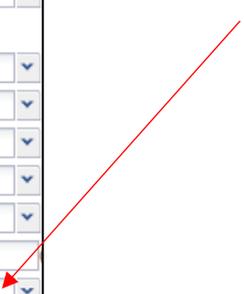
Out translationid:

In manipulationid:

Out manipulationid:

Average rate limit: 0

Access control trust level: high



## 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

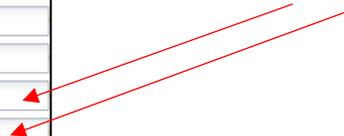
ACLI Path: config t → media-manger → media-manger

Save Wizards Commands

- Objects
  - media-manager
    - codec-policy
    - dns-alg-constraints
    - dns-config
    - ice-profile
    - media-manager**
    - media-policy
    - msrp-config
    - playback-config
    - realm-config
    - realm-group
    - rtcp-policy
    - static-flow
    - steering-pool
    - tcp-media-profile
  - security
  - session-router
  - system

### Modify Media manager

State:	<input checked="" type="checkbox"/>			
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:	<input type="checkbox"/>			
Algd log level:	NOTICE			
Mbcd log level:	NOTICE			
Options:	<table border="1"><thead><tr><th>Add</th><th>Edit</th><th>Delete</th></tr></thead><tbody></tbody></table>	Add	Edit	Delete
Add	Edit	Delete		
Red max trans:	10000			
Red sync start time:	5000			
Red sync comp time:	1000			
Media policing:	<input checked="" type="checkbox"/>			
Max arp rate:	10			
Max signaling packets:	100			
Max untrusted signaling:	1			
Min untrusted signaling:	1			



# Appendix C

## SBC Behind NAT SPL configuration

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

The Support for SBC Behind NAT SPL plug-in changes information in SIP messages to hide the end point located inside the private network. The specific information that the Support for SBC Behind NAT SPL plug-in changes depends on the direction of the call, for example, from the NAT device to the SBC or from the SBC to the NAT device. Configure the Support for SBC Behind NAT SPL plug-in for each SIP interface that is connected to a NAT device. One public-private address pair is required for each SIP interface that uses the SPL plug-in, as follows.

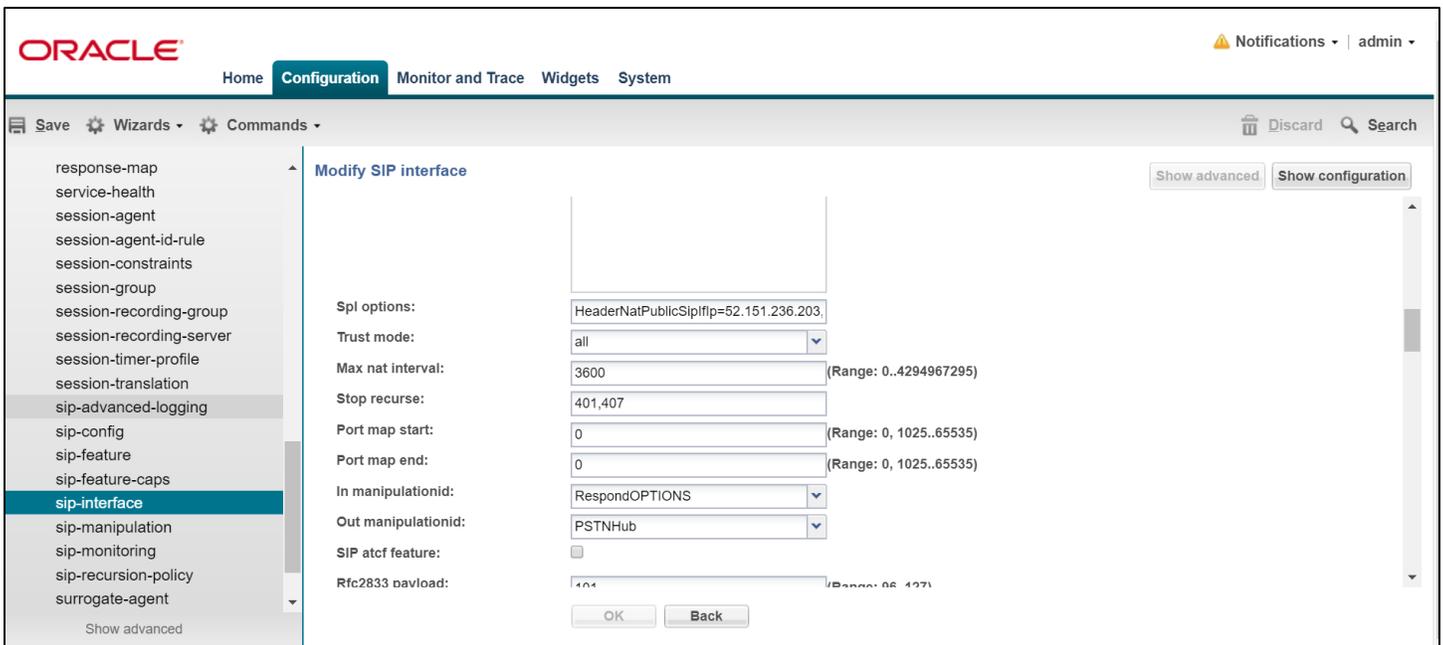
- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

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

To configure SBC Behind NAT SPL Plug in, Go to session-router->sip-interface->spl-options and input the following value, save and activate.

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.0.4.4

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



Similarly configure the PSTN side as well.

# Appendix D

## Sip Manipulation Replacement

To simplify the ORACLE SBC configuration, the latest ORACLE SBC GA Release, SCZ830m1p7, (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 three 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.

### Teams Facing Realm

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

#### Teams FQDN in URI

And

#### SDP inactive only

### Teams FQDN in URI

When enabled, this parameter takes the FQDN configured under hostname of the [network interface](#), and inserts that into the [Contact and FROM headers of Invites](#) generated by the SBC towards Teams. This also adds a new “X-MS-SBC” Header to both Invite and OPTIONS Requests, which takes the place of the [User-Agent](#) header currently being added via Sip Manipulation. 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.

### 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

The screenshot shows the Oracle SBC Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this is a toolbar with 'Save', 'Wizards', and 'Commands'. A left-hand 'Objects' tree is expanded to 'realm-config'. The main area is titled 'Modify Realm config' and contains the following fields:

- Identifier: Teams
- Description: Realm Facing Teams Direct Routing
- Addr prefix: 0.0.0.0
- Network interfaces: A table with columns 'Add', 'Edit', and 'Delete'. It contains one entry: M00:0.4.
- Mm in realm:
- Mm in network:
- Mm same ip:
- QoS enable:
- Max bandwidth: 0
- Max priority bandwidth: 0
- Parent realm: (dropdown)
- DNS realm: (dropdown)
- Media policy: (dropdown)
- Media sec policy: sdesPolicy
- RTCP mux:
- Ice profile: ice
- Teams fqdn in uri:  (indicated by a red arrow)
- SDP inactive only:  (indicated by a red arrow)

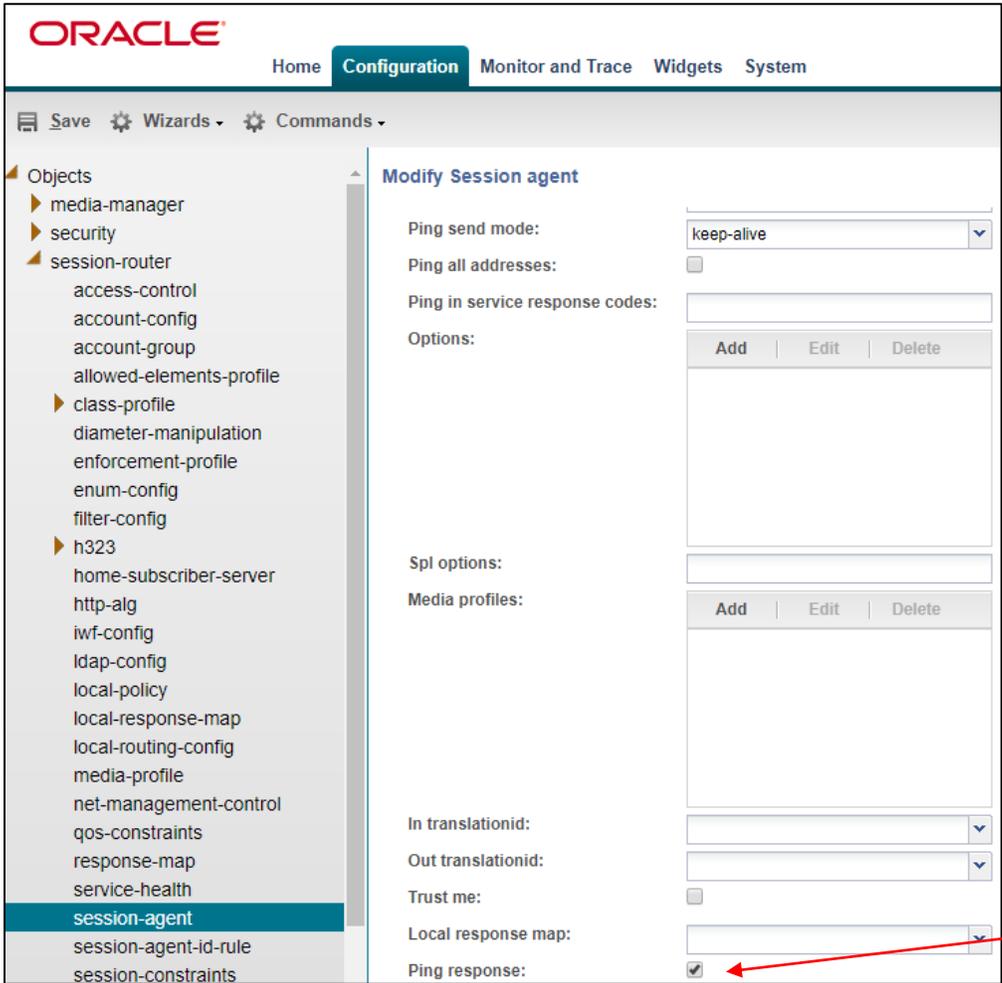
## Teams Session Agents

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

## 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](#).



## 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 SCZ830M1P7, 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](#).

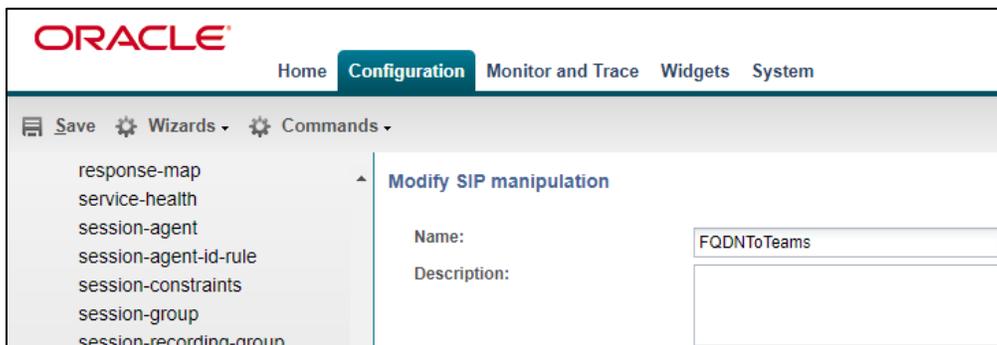
For SBC's running release SCZ830m1p7 or later, that have enabled the new features outlined in [AppendixD](#), the host-uri of the Contact of all responses towards Microsoft Teams is not modified from the SBC's default behavior. In light of this new requirement, it will be necessary to add a Sip Manipulation rule to your configuration that will allow the Oracle Communications Session Border Controller to send the correct syntax in responses towards Teams.

**Note: This only applies to SBC configurations that have removed the other Teams facing sip manipulations and enabled the features outlined in Appendix D.**

GUI Path: session-router/sip-manipulation

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

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



The screenshot shows the Oracle SBC GUI configuration page for 'Modify SIP manipulation'. The page has a top navigation bar with 'ORACLE' logo and tabs for 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below the navigation bar is a toolbar with 'Save', 'Wizards', and 'Commands'. A left sidebar lists various configuration categories, with 'session-agent' expanded. The main content area is titled 'Modify SIP manipulation' and contains two input fields: 'Name' with the value 'FQDnToTeams' and 'Description' which is empty.

Header Rule:



The screenshot shows the Oracle SBC GUI configuration page for 'Modify SIP manipulation / header rule'. The page has the same top navigation bar and toolbar as the previous screenshot. The left sidebar lists various configuration categories, with 'session-agent' expanded. The main content area is titled 'Modify SIP manipulation / header rule' and contains several input fields and dropdown menus: 'Name' with the value 'Alter\_Contact\_Reply', 'Header name' with the value 'Contact', 'Action' with a dropdown menu set to 'manipulate', 'Comparison type' with a dropdown menu set to 'case-sensitive', and 'Msg type' with a dropdown menu set to 'reply'. Below these fields is a 'Methods' section with buttons for 'Add', 'Edit', and 'Delete'.

Element Rule:

The screenshot shows the Oracle Configuration Manager interface. The 'Configuration' tab is active. On the left, a tree view shows various configuration categories, with 'sip-config' selected. The main area displays the configuration for an 'Element Rule' named 'Alter\_Conact\_Host'. The configuration details are as follows:

Field	Value
Name	Alter_Conact_Host
Parameter name	
Type	uri-host
Action	replace
Match val type	any
Comparison type	case-sensitive
Match value	
New value	oracleesbc2.woodgrovebank.us

This sip manipulation will be applied as the out-manipulation-id on the Teams facing [Sip-Interface](#).

## CLI Configuration Output

```
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
ice-profile
  name ice
  stun-conn-timeout 0
  stun-keep-alive-interval 0
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 ATTrunk
    realm access-pstn
media-manager
  mbc-d-log-level DEBUG
  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
  spl-options LRE-Identifier,X-CALL-ID,Contact
  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
  rtcp-mux enabled
  ice-profile ice
  refer-call-transfer enabled
  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 ATTTTrunk
  ip-address 68.68.117.67
  state disabled
  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
  ping-all-addresses 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
  ping-all-addresses 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
  ping-all-addresses enabled
session-group
  group-name TeamsGrp
  strategy RoundRobin
  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
  options
  extra-method-stats
  access-pstn
  inmanip-before-validate
  max-udp-length=0
  enabled
sip-feature
  name
  realm
  require-mode-inbound
  require-mode-outbound
  replaces
  access-teams
  Pass
  Pass
sip-interface
  state
  realm-id
  description
  sip-port
  address
  allow-anonymous
  in-manipulationid
  out-manipulationid
  enabled
  access-pstn
  to trunk
  192.65.72.196
  agents-only
  Siptrunk_outmanip
sip-interface
  realm-id
  sip-port
  address
  port
  transport-protocol
  tls-profile
  allow-anonymous
  nat-traversal
  nat-interval
  registration-caching
  in-manipulationid
  out-manipulationid
  sip-profile
  access-teams
  155.212.214.172
  5061
  TLS
  TLSTeams
  agents-only
  always
  3600
  enabled
  Teamsinmanip
  Teamsoutmanip
  foreplace
sip-manipulation
  name
  header-rule
  name
  header-name
  action
  msg-type
  methods
  element-rule
  name
  type
  action
  comparison-type
  match-value
  Checkfor1831
  check183
  @status-line
  manipulate
  reply
  INVITE
  is183
  status-code
  store
  pattern-rule
  183
mime-sdp-rule
  name
  msg-type
  methods
  action
  comparison-type
  match-value
  sdp-session-rule
  name
  action
  sdp-line-rule
  name
  type
  action
  comparison-type
  match-value
  if183
  reply
  INVITE
  manipulate
  boolean
  $check183.$is183
  au
  manipulate
  checkc
  c
  store
  pattern-rule
  ^.(?!(155.214.212.172))*$
mime-sdp-rule
  name
  msg-type
  methods
  action
  comparison-type
  match-value
  deletesdp
  reply
  INVITE
  delete
  boolean
  $if183.$au.$checkc
header-rule
  name
  change183t0180

```

```

header-name @status-line
action manipulate
comparison-type boolean
match-value $if183.$au.$checkc
element-rule
    name modstatus
    type status-code
    action replace
    match-value 183
    new-value 180
element-rule
    name modReasonPhrase
    type reason-phrase
    action replace
    match-value Session Progress
    new-value Ringing
sip-manipulation
    name Siptrunk outmanip
header-rule
    name change_fqdn_to_ip_from
    header-name From
    action manipulate
    msg-type out-of-dialog
    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 out-of-dialog
    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
header-rule
    name From
    header-name From
    action sip-manip
    new-value Checkfor1831
mime-sdp-rule
    name Reginactivetosendonly
    msg-type request
    methods INVITE
    action manipulate
    sdp-media-rule
        name audio
        media-type audio
        action manipulate
    sdp-line-rule
        name audiol
        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       audiol
  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 out-of-dialog
    methods  INVITE
    element-rule
      name     uriuser2
      type     uri-user
      action   replace
      new-value "1"+$
  header-rule
    name     Change_to_userandhost
    header-name To
    action   manipulate
    msg-type out-of-dialog
    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_Fromip_fqdn
    header-name From
    action   manipulate
    msg-type any
    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 out-of-dialog
    methods  OPTIONS
"<sip:ping@oracleesbc2.woodgrovebank.us:5061;transport=tls>"
  header-rule
    name     Recordroute
    header-name Record-Route
    action   add
    msg-type out-of-dialog
    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                 out-of-dialog
    methods                  INVITE
    new-value                "Oracle ESBC"

header-rule
    name                      Modifyuser
    header-name              User-Agent
    action                   manipulate
    msg-type                 out-of-dialog
    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          DEBUG
process-log-level        DEBUG
comm-monitor
state                     enabled
qos-enable                disabled
monitor-collector
address                   129.213.175.152
network-interface        s0p0:0.4
monitor-collector
address                   172.18.255.181

source-routing            enabled
tls-global
session-caching          enabled
tls-profile
name                     TLSTeams
end-entity-certificate   SBCCertificate
trusted-ca-certificates  DigiCertInter
                        DigiCertRoot
                        BaltimoreRoot
cipher-list               ALL
mutual-authenticate      enabled

web-server-config
inactivity-timeout       0
http-interface-list

```



**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](https://blogs.oracle.com/oracle)
-  [facebook.com/Oracle/](https://facebook.com/Oracle/)
-  [twitter.com/Oracle](https://twitter.com/Oracle)
-  [oracle.com](https://oracle.com)

**Integrated Cloud Applications & Platform Services**

Copyright © 2020, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615