



Configuring the Oracle SBC with Microsoft Teams Direct Routing Media Bypass - Enterprise Model

Technical Application Note



Disclaimer

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



Revision History

Version	Description of Changes	Date Revision Completed
1.0	Added Web GUI	12-09-2019
2.0	Added bug fixes for ACMESOLU-106	21-10-2019



Table of Contents

Introduction	7
About Microsoft Teams Direct Routing	7
Planning Direct Routing.....	7
Tenant Requirements	7
Licensing Requirements	7
DNS Requirements	8
SBC Domain Names	8
Public trusted certificate for the SBC	9
Configure Direct Routing.....	10
Establish a remote PowerShell session to Skype for Business Online	10
Pair the SBC to tenant	11
Enable users for Direct Routing	12
Microsoft Teams Direct Routing Interface characteristics	15
Requirements to SIP messages “Invite” and “Options”	17
Requirements for “INVITE” messages syntax	17
Requirements for “OPTIONS” messages syntax	18
Validated Oracle version	19
Configuring the SBC	20
What is Media Bypass	20
New SBC configuration	22
Establishing a serial connection to the SBC	22
Configure SBC using Web GUI.....	25
Configure system-config.....	28
Configure Physical Interface values	29
Configure Network Interface values	30
Enable media manager	32
Configure Realms	32
Enable sip-config	33
Configuring a certificate for SBC Interface	35
SBC Certificate Creation	35
Step 1 – Creating the SBC certificate record	35
Step 2 – Generating a certificate signing request for SBC certificate	36
Step 3 – Deploy the SBC certificate	37
Root and Intermediate Certificates Creation.....	37
Step1-Creating the root and intermediate certificates on SBC	38

Step2:Deploying the Root and Intermediate certificates on SBC	38
TLS-Profile	39
Creating a sip-interface to communicate with Microsoft Teams	41
Configure sip-interface to communicate with SIP Trunk	42
Configure session-agent.....	42
Create a Session Agent Group	45
Configure local-policy	46
Configure Media Profile & Codec Policy.....	49
Configure sip-manipulations.....	51
Teamsoutmanip.....	51
Countrycode Manipulation:	53
Change_fromip_fqdn Manipulation:.....	55
Change_to_userandhost Manipulation:.....	56
Addcontactheaderinoptions.....	58
Recordroute.....	59
Alter_contact.....	60
Adduseragent	61
Modifyuseragent	62
Teamsinmanip.....	63
Respondoptions.....	65
Applying the teams SIP manipulations to Teams SIP Interface	66
Siptrunk_outmanip.....	67
Change_fqdn_to_ip_from.....	68
Change_fqdn_to_ip_to.....	69
Applying the trunk side SIP manipulations to Trunk SIP Interface.....	70
Ringback Configuration	70
Ringback on Transfers	70
Consultative transfer configuration.....	73
Configure steering pool.....	74
Configure SDES profile.....	75
One way audio on inbound calls to Teams	Error! Bookmark not defined.
Media-sec-policy.....	76
Configure RTCP Policy and RTCP Mux.....	79
Configure ice-profile.....	80
Existing SBC configuration	82
Appendix A	83
Ringback on inbound calls to Teams and early media.....	83
Appendix B	90



DDoS Prevention for Peering Environments 90

Appendix C **91**

 SBC Behind NAT SPL configuration..... 91

Appendix D **92**



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

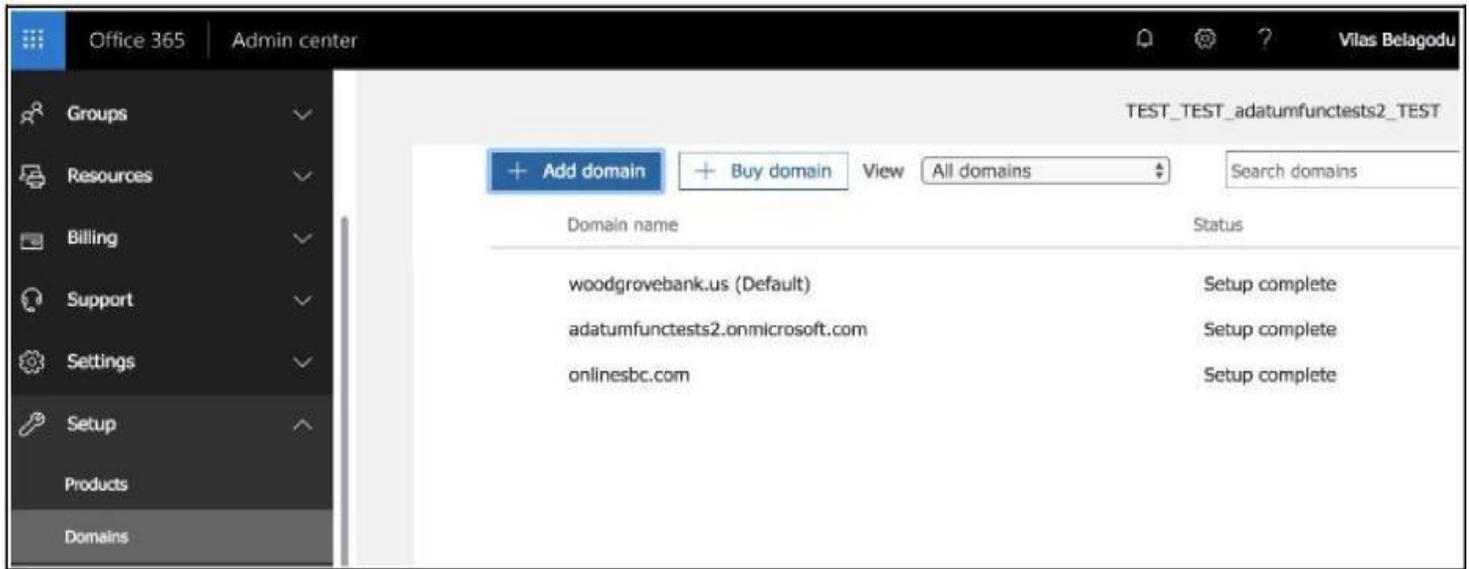
SBC Domain Names

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

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

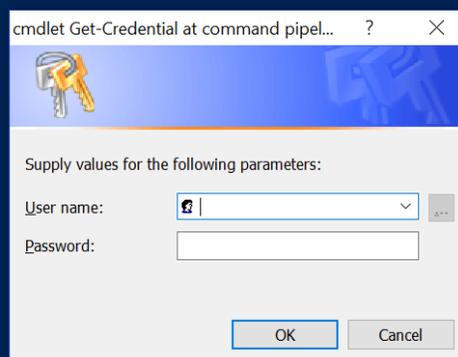
- Open PowerShell and type in the below commands
- Import-Module SkypeOnlineConnector
- \$userCredential = Get-Credential
- \$sfbSession = New-CsOnlineSession -Credential \$userCredential
- Import-PSSession \$sfbSession

```
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: [f] [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           : oraclesbc2.woodgrovebank.us
Fqdn               : oraclesbc2.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

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, Setup, and Customize navigation. The main area displays a user profile for 'TeamsUser1' (teamsuser1@woodgrovebank.us). Below the profile, there is a table of user details:

Username / Email	teamsuser1@woodgrovebank.us	Edit
Aliases	teamsuser1@adatumfunctests2.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"> • G711 • G722 • Silk (Teams clients) • Opus (WebRTC clients) - Only if Media Bypass is used; • G729 	
	Other codecs	<ul style="list-style-type: none"> • DTMF – Required • Events 0-16 • CN <ul style="list-style-type: none"> o Required narrowband and wideband • RED – Not required • Silence Suppression – Not required 	

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.

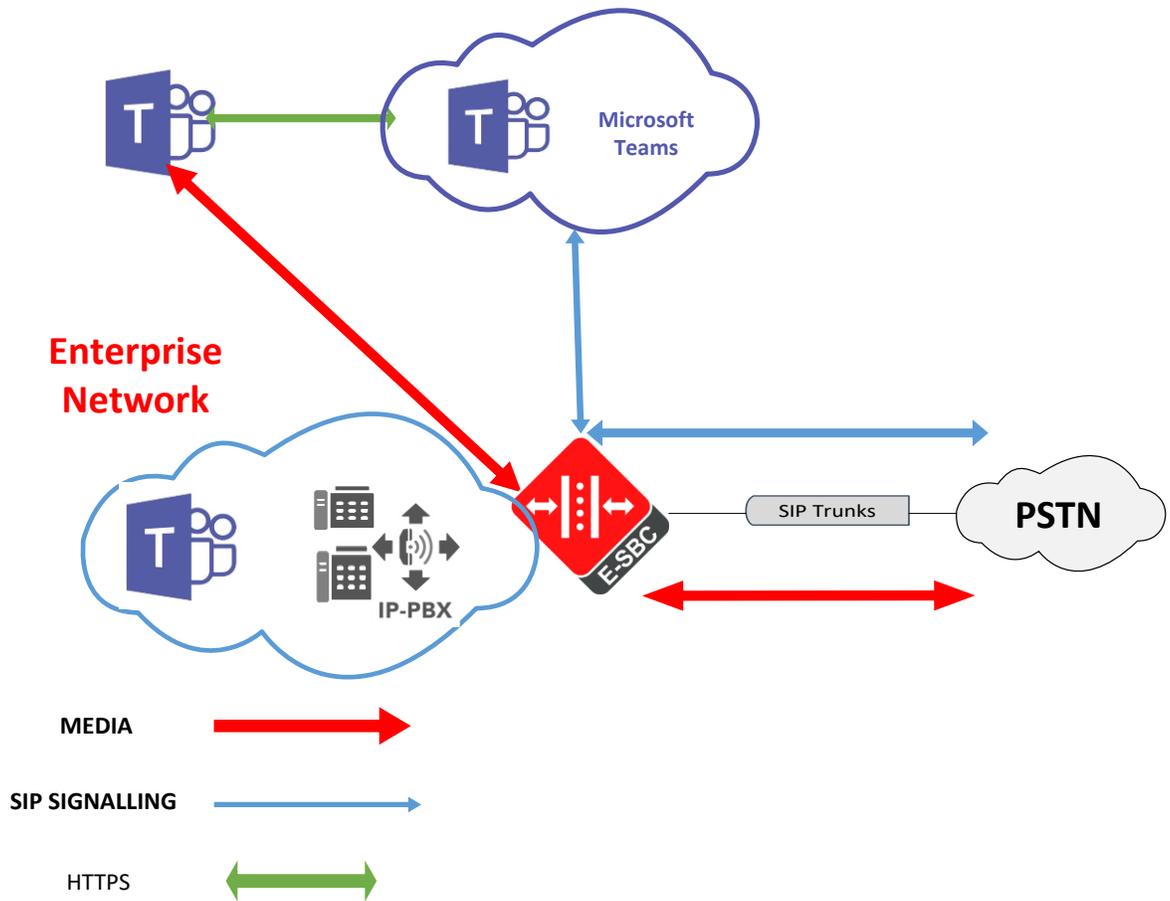


Figure :1: Signaling & media flow with media-bypass enabled



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 tCerte...
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

```

PE-6300-1# setup product

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

Last Modified 2019-09-11 13:57:32
-----

1 : Product      : Enterprise Session Border Controller

```

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

```

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

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

  Session Capacity (0-128000)          : 500

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

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

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

  Transcode Codec AMR Capacity (0-102375) : 50

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

  Advanced (enabled/disabled)          : enabled

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

  Transcode Codec OPUS Capacity (0-102375) : 50

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

  Transcode Codec SILK Capacity (0-102375) : 50

```

Save the changes and reboot the SBC.

```

Transcode Codec SILK Capacity (0-102375) : 50
Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
SAVE SUCCEEDED
PE-6300-1#
PE-6300-1#
PE-6300-1#
PE-6300-1# reboot

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

```

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

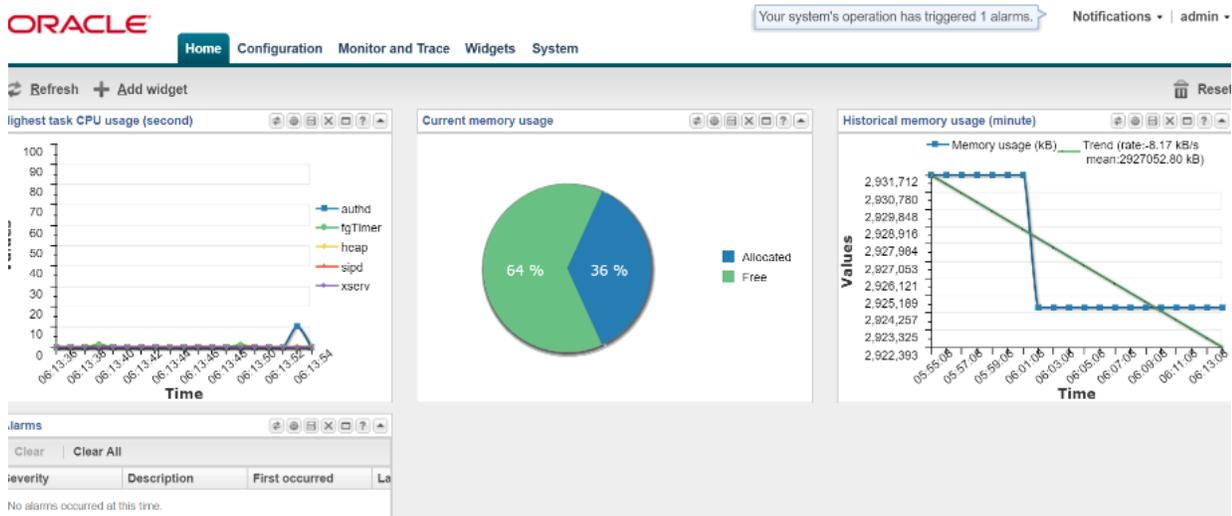
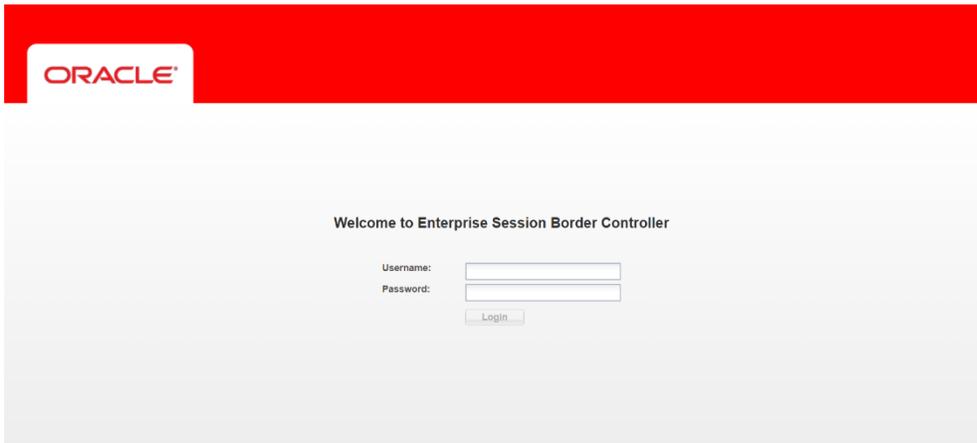
PE-6300-1(web-server-config)# exit
PE-6300-1(system)# exit
PE-6300-1(configure)# exit
PE-6300-1# save-config
checking configuration
-----
Results of config verification:
  1 configuration error
Run 'verify-config' for more details
-----
Save-Config received, processing.
waiting for request to finish
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>`. The username and password is the same as that of CLI.



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

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

Kindly refer to the GUI User Guide https://docs.oracle.com/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

ORACLE

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands

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
 - system-config**
 - tdm-config

Modify System config

Hostname:	oracleesbc2.woodgrovebank.us
Description:	ESBC to Microsoft Teams Direct Routing
Location:	Bedford, MA
Mib system contact:	
Mib system name:	
Mib system location:	
Acp TLS profile:	
SNMP enabled:	<input checked="" type="checkbox"/>
Enable SNMP auth traps:	<input type="checkbox"/>
Enable SNMP syslog notify:	<input type="checkbox"/>
Enable SNMP monitor traps:	<input type="checkbox"/>
Enable env monitor traps:	<input type="checkbox"/>
Enable mblk_tracking:	<input type="checkbox"/>
Enable I2 miss report:	<input checked="" type="checkbox"/>

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

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 Oracle WebGUI 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 'system' folder expanded, with 'phy-interface' selected. The main area displays the 'Modify Phy interface' form with the following 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)

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

Configure Network Interface values

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

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

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

ORACLE Notifications | adn

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: ep0p1

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

Description:

Hostname: oracleesbc2.woodgrovebank.us

IP address: 155.212.214.172

Pri utility addr:

Sec utility addr:

Netmask: 255.255.255.0

Gateway: 155.212.214.1

Gw heartbeat

State:

Heartbeat: 0 (Range: 0..65535)

ORACLE Notifications | adn

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: 0 (Range: 0..65535)

Retry timeout: 1 (Range: 1..65535)

Health score: 0 (Range: 0..100)

DNS IP primary: 8.8.8.8

DNS IP backup1:

DNS IP backup2:

DNS domain: woodgrovebank.us

DNS timeout: 11 (Range: 0..4294967295)

DNS max ttl: 86400 (Range: 30..2073600)

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

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

Go to Media-Manager->Media-Manager

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 'media-manager' object selected. The main area is titled 'Modify Media manager' and contains the following configuration fields:

- State:
- Flow time limit: 86400 (Range: 0..4294967295)
- Initial guard timer: 300 (Range: 0..4294967295)
- Subsq guard timer: 300 (Range: 0..4294967295)
- TCP flow time limit: 86400 (Range: 0..4294967295)
- TCP initial guard timer: 300 (Range: 0..4294967295)
- TCP subsq guard timer: 300 (Range: 0..4294967295)
- Hnt rtcp:
- Algd log level: NOTICE
- Mbcd log level: NOTICE
- Options: Add | Edit | Delete
 - audio-allow-asymmetric-pt
 - xcode-gratuitous-rtcp-report-generation

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 the 'realm-config' object selected under 'media-manager'. The main area is titled 'Modify Realm config' and contains the following configuration fields:

- Identifier: access-teams
- Description: (empty)
- Addr prefix: 0.0.0.0
- Network interfaces: Add | Edit | Delete
 - 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. 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 fields:

- Identifier: access-pstn
- Description: (empty text box)
- Addr prefix: 0.0.0.0
- Network interfaces: A table with columns 'Add', 'Edit', and 'Delete'. The entry 's0p0:0.4' is listed.
- Mm in realm:
- Mm in network:
- Mm same ip:

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

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.

The screenshot shows the Oracle SBC Configuration interface for 'Modify SIP config'. 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 'sip-config' selected. The main area is titled 'Modify SIP config' and contains the following fields:

- State:
- Dialog transparency:
- Home Realm ID: access-pstn
- Egress Realm ID: (empty dropdown)
- Nat mode: None
- Registrar domain: *
- Registrar host: *
- Registrar port: 5060 (Range: 0, 1025..65535)
- Init timer: 500 (Range: 0..4294967295)
- Max timer: 4000 (Range: 0..4294967295)
- Trans expire: 32 (Range: 0..4294967295)
- Initial inv trans expire: 0 (Range: 0..999999999)
- Invite expire: 180 (Range: 0..4294967295)
- Session max life limit: n

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

- 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:	<input type="text"/>										
Registrar port:	<input type="text" value="0"/>	(Range: 0, 1025..65535)									
Init timer:	<input type="text" value="500"/>	(Range: 0..4294967295)									
Max timer:	<input type="text" value="4000"/>	(Range: 0..4294967295)									
Trans expire:	<input type="text" value="32"/>	(Range: 0..4294967295)									
Initial inv trans expire:	<input type="text" value="0"/>	(Range: 0..999999999)									
Invite expire:	<input type="text" value="180"/>	(Range: 0..4294967295)									
Session max life limit:	<input type="text" value="0"/>										
Enforcement profile:	<input type="text"/>										
Red max trans:	<input type="text" value="10000"/>	(Range: 0..50000)									
Options:	<table><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">inmanip-before-validate</td></tr><tr><td colspan="3">max-udp-length=0</td></tr></table>		<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	inmanip-before-validate			max-udp-length=0		
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="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 – a certificate-record assigned to SBC
 - Root – a certificate-record for root cert
 - Intermediate – a 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

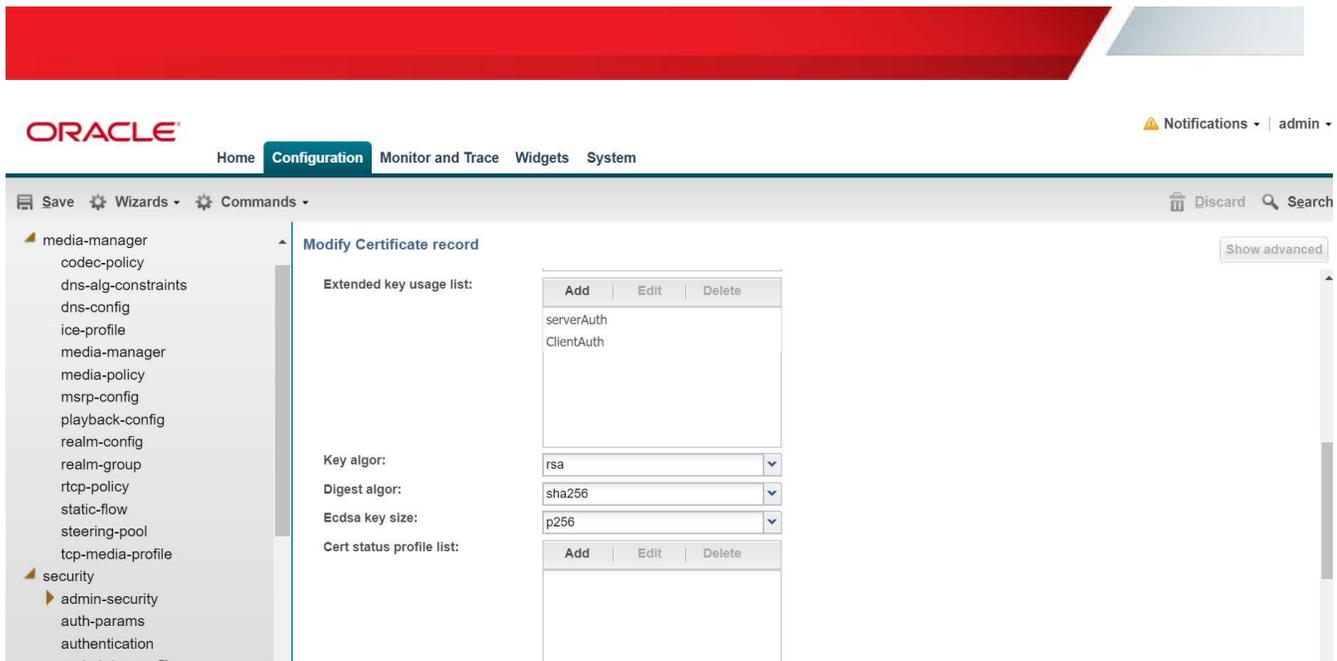
Step 1 – Creating the SBC certificate record

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 'ORACLE' and 'Notifications | admi'. Below this, a menu bar shows 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The main content area is titled 'Modify Certificate record' and contains a form with the following fields:

- Name: SBCCertificate
- Country: US
- State: MA
- Locality: Bedford
- Organization: sales
- Unit: (empty)
- Common name: Oracleesbc2.woodgrovebank.us
- Key size: 2048 (dropdown menu)
- Alternate name: (empty)
- Trusted:
- Key usage list: A table with columns 'Add', 'Edit', and 'Delete'. The rows are 'digitalSignature' and 'keyEncipherment'.

On the left side, there is a tree view showing the configuration hierarchy, with 'security' expanded to show 'admin-security', 'auth-params', 'authentication', and 'cert-status-profile'.



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.

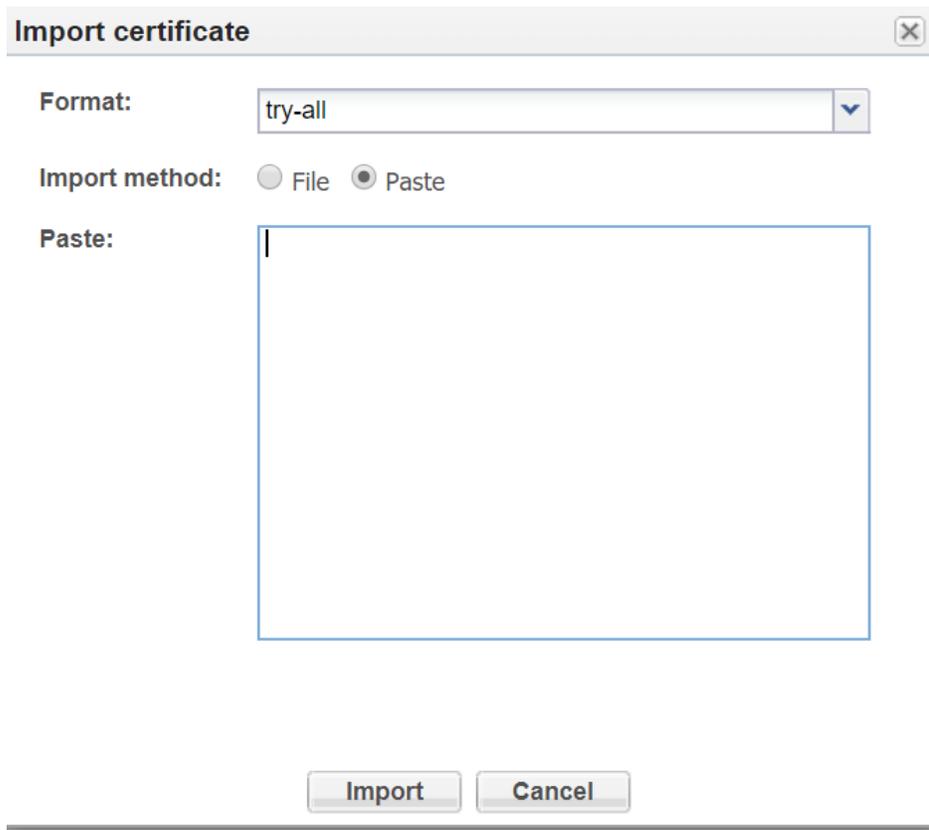


- Also, note that a save/activate is required

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

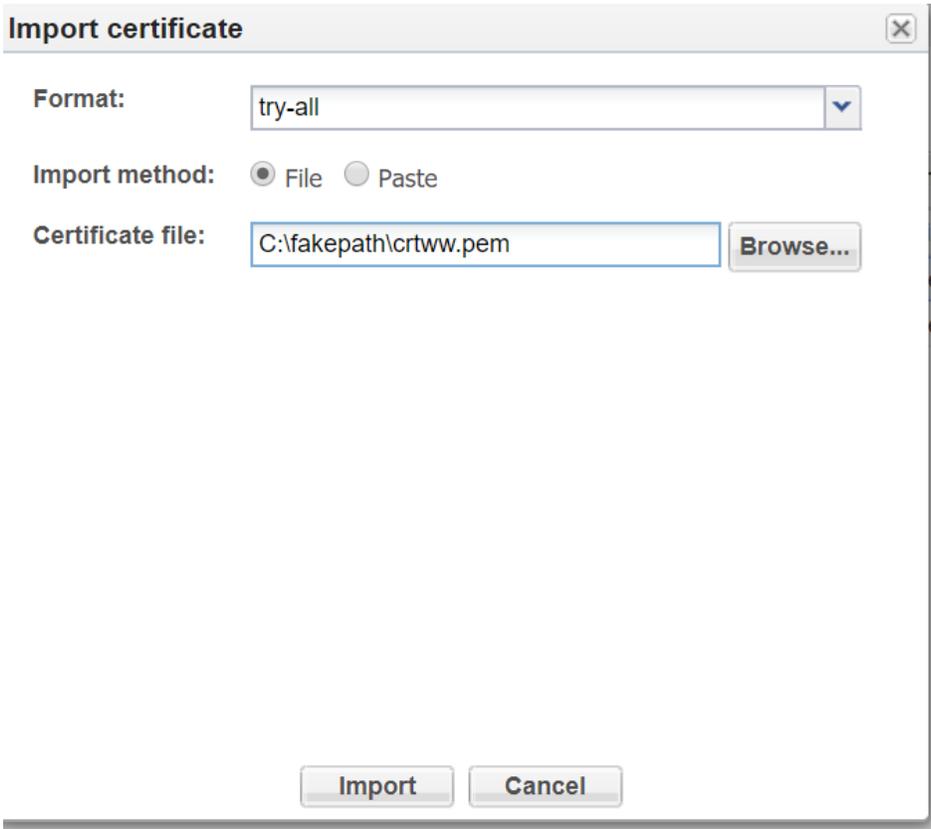
All the root and intermediate certificates have to imported to SBC.

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.

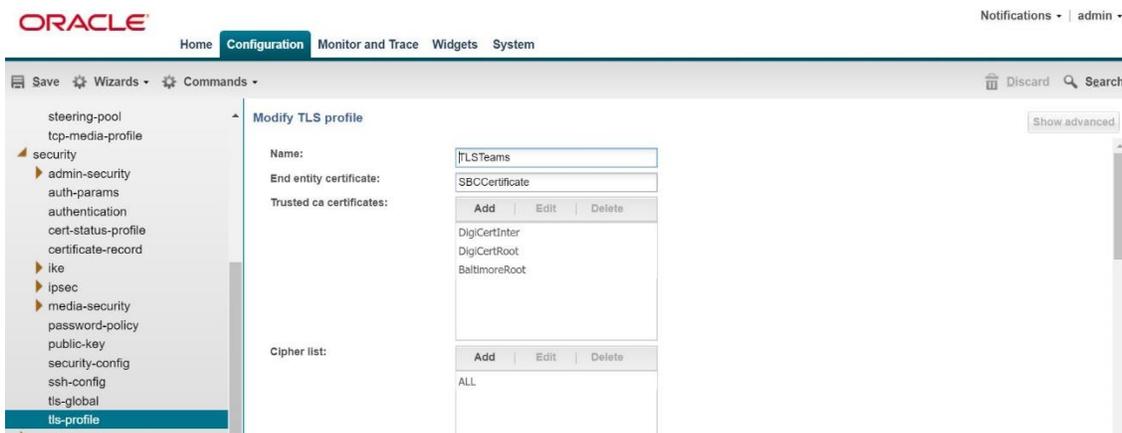
Click on the certificate and select Import.

The below screen appears.Make sure your file is in .pem format and upload.



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



- steering-pool
- tcp-media-profile
- security
 - admin-security
 - auth-params
 - authentication
 - cert-status-profile
 - certificate-record
 - ike
 - ipsec
 - media-security
 - password-policy
 - public-key
 - security-config
 - ssh-config
 - tls-global
 - tls-profile**
 - session-router
 - system

Modify TLS profile

Show advanced

Verify depth: (Range: 0..10)

Mutual authenticate:

TLS version:

Options:

<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Cert status check:

Cert status profile list:

<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

OK Back

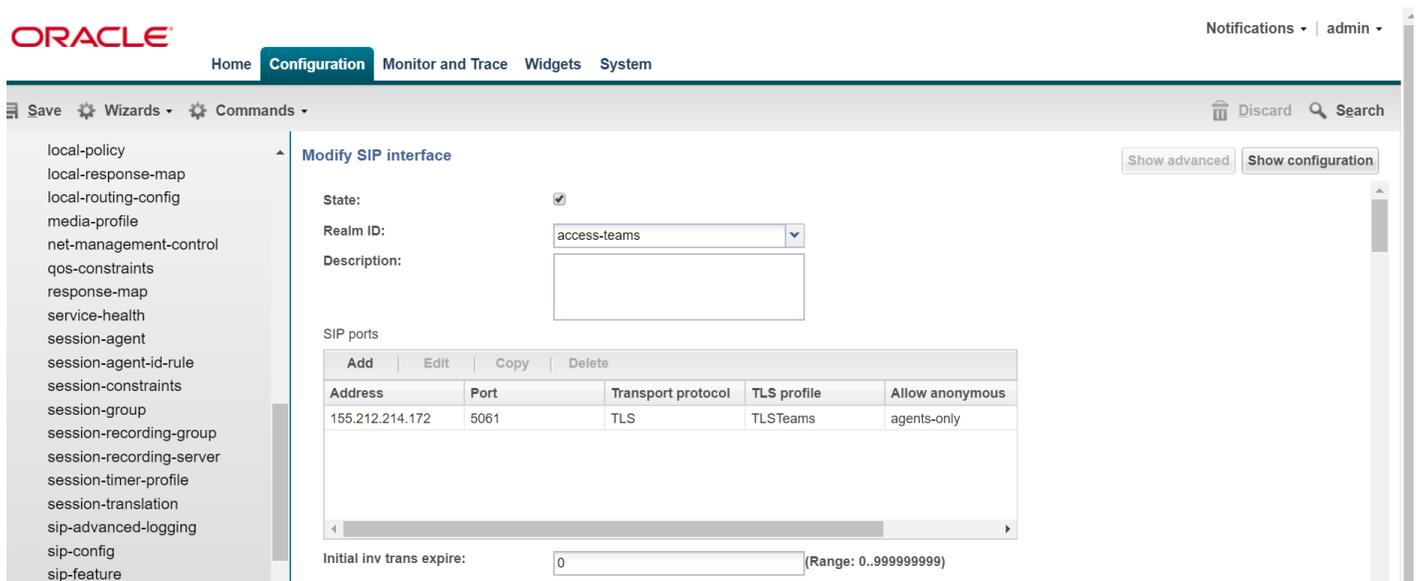
Creating a sip-interface to communicate with Microsoft Teams

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 Manager interface. The top navigation bar includes 'ORACLE', 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The right side shows 'Notifications' and 'admin'. The main content area is titled 'Modify SIP interface' and contains the following configuration fields:

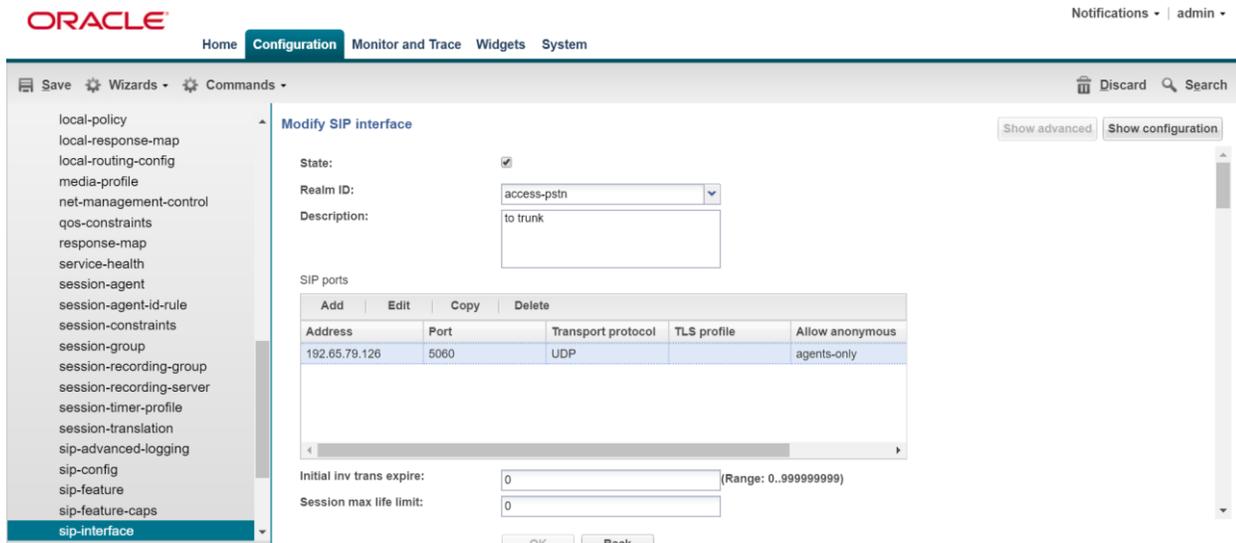
- State:
- Realm ID:
- Description:
- SIP ports table:

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..99999999)

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 SBC configuration 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 lists various configuration categories, with 'sip-interface' selected. The main content area is titled 'Modify SIP interface' and contains the following configuration fields:

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

SIP ports				
	Add	Edit	Copy	Delete
Address	Port	Transport protocol	TLS profile	Allow anonymous
192.65.79.126	5060	UDP		agents-only

Below the table, there are two input fields:

- Initial inv trans expire: (Range: 0..999999999)
- Session max life limit:

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

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

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

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

Save Wizards Commands Discard Search

Modify Session agent

Show advanced Show configuration

Rfc2833 payload: 0 (Range: 0, 96..127)

Codec policy:

Refer call transfer: enabled

Refer notify provisional: none

Reuse connections: NONE

TCP keepalive: none

TCP reconn interval: 0 (Range: 0, 2..300)

Max register burst rate: 0 (Range: 0, 99999999)

Kpml interworking: inherit

Precedence: 0 (Range: 0, 4294967295)

Monitoring filters:

Add Edit Delete

Follow above steps to create 2 more sessions for:

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

- *Note: Please note that all signaling SHOULD only point to sip/sip2/sip3.pstnhub.microsoft.com – no signaling 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*

Save Wizards Commands Discard Search

Session agent

Search Criteria: All

Add	Edit	Copy	Delete	Delete All	Upload	Download	Search	Search	Clear
Hostname	IP address	Port	State	App protocol	Realm ID	Description			
ATTTrunk	68.68.117.67	5060	disabled	SIP	access-pstn				
sip-all.pstnhub.micro...		5061	enabled	SIP	access-teams				
sip.pstnhub.microsof...		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 left sidebar lists various configuration categories, with 'session-group' selected. The main area is titled 'Modify Session group' and contains the following fields:

- Group name: TeamsGrp
- Description: (empty)
- State:
- App protocol: SIP
- Strategy: RoundRobin
- Dest: A list containing sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com, and sip3.pstnhub.microsoft.com.
- Trunk group: (empty)

This screenshot shows the 'Modify Session group' configuration page with advanced options visible. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration categories, with 'session-group' selected. The main area is titled 'Modify Session group' and contains the following fields:

- Group name: TeamsGrp
- Description: (empty)
- State:
- App protocol: SIP
- Strategy: RoundRobin
- Dest: A list containing sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com, and sip3.pstnhub.microsoft.com.
- Trunk group: A list containing sip2.pstnhub.microsoft.com and sip3.pstnhub.microsoft.com.
- Sag recursion:
- Stop sag recurse: 401,407,480
- SIP recursion policy: (empty)

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 Session Manager configuration interface. The left sidebar lists various configuration categories, with 'local-policy' selected. The main area is titled 'Modify Local policy' and contains three input sections: 'From address:', 'To address:', and 'Source realm:'. Each section has an 'Add', 'Edit', and 'Delete' button above a text input field. The 'From address:' and 'To address:' fields currently contain an asterisk (*). The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The top right corner shows 'Notifications' and 'admin'.

This screenshot shows the 'Modify Local policy' configuration page with more details. The left sidebar shows 'local-policy' selected. The main area includes a 'Description:' text box, a 'State:' checkbox (checked), and a 'Policy priority:' dropdown menu set to 'none'. Below these is a 'Policy attributes' table with columns for 'Add', 'Edit', 'Copy', and 'Delete'. The table contains one row with the following data:

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

The top navigation bar and user information are consistent with the previous screenshot.

Save Wizards Commands Discard Search

local-policy Modify Local policy / policy attribute Show advanced

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

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

The above local policy config is allowing any DID from teams that lands on the SBC to be routed to ATT Trunk via realm access-pstn, where the next hop is the IP address of the ATT Trunk.

A second local policy is required to be configured to route outbound calls to Teams from access-pstn, configure it as follows

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 Show advanced Show configuration

From address: Add Edit Delete
*

To address: Add Edit Delete
*

Source realm: Add Edit Delete

- 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 Local policy

Show advanced Show configuration

access-pstn

Description:

State:

Policy priority: none

Policy attributes

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

- 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..999999999)

State:

App protocol:

Lookup: single

Next key:

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

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 fields:

- 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

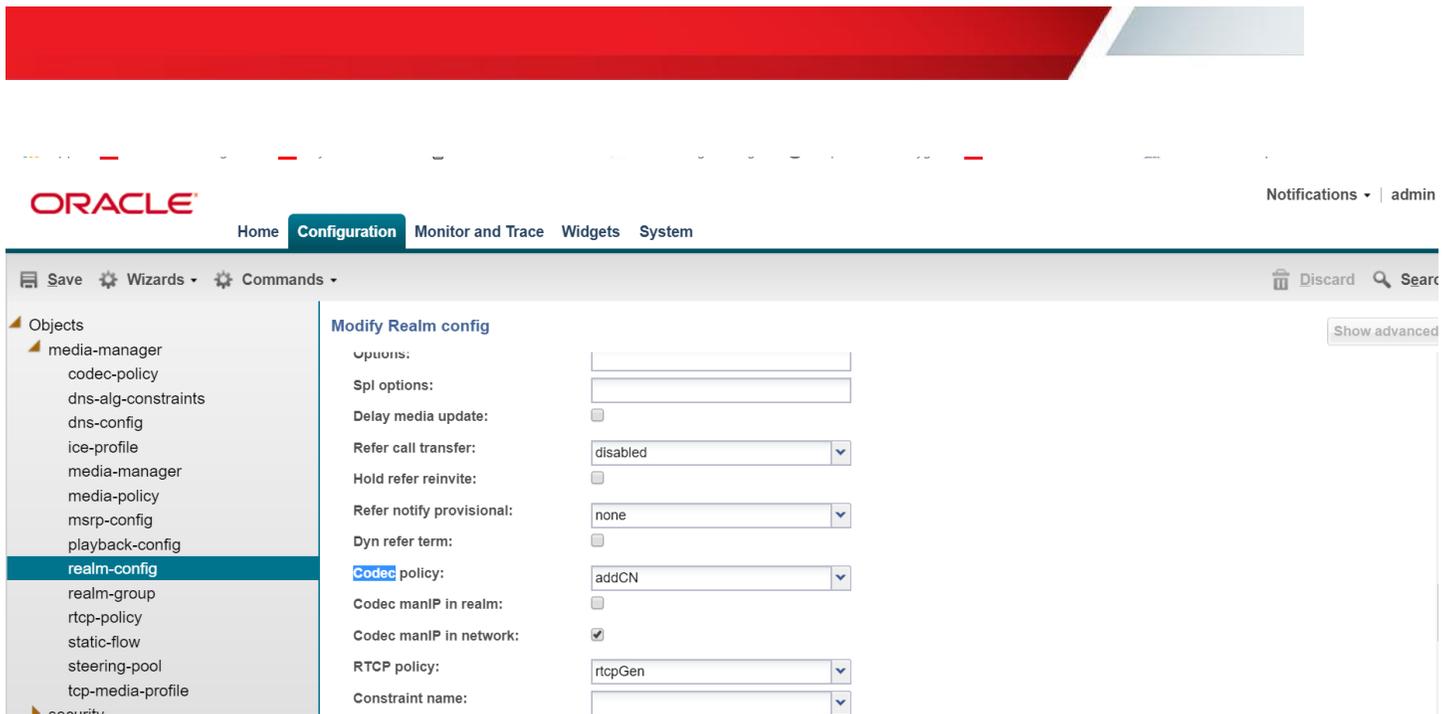
Configure media profiles similarly, for silk codec also.

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.

The screenshot shows the Oracle Configuration Assistant interface. The left sidebar lists various configuration objects, with 'media-manager' expanded and 'codec-policy' selected. The main panel is titled 'Modify Codec policy' and shows the configuration for a policy named 'addCN'. The 'Allow codecs' section contains two entries: 'SILK:no' and 'G729:no'. The 'Add codecs on egress' section contains one entry: 'CN'. The interface includes a top navigation bar with 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. A 'Save' button and 'Wizards' and 'Commands' menus are visible in the top left. A 'Discard' button and a search icon are in the top right. A 'Show advanced' button is located in the top right corner of the main panel.

The screenshot shows the Oracle Configuration Assistant interface, displaying the 'Modify Codec policy' configuration for 'addCN' with advanced settings. The left sidebar is the same as in the previous screenshot. The main panel shows the following settings: 'Packetization time' is set to 20 (Range: 0..4294967295); 'Force ptime' is unchecked; 'Secure dtmf cancellation' is unchecked; 'Dtmf in audio' is set to 'disabled'; 'Tone detection' is empty; 'Tone detect renegotiate timer' is set to 500 (Range: 50..32000); 'Reverse fax tone detection reinvite' is unchecked; 'Fax single m line' is set to 'disabled'; and 'Evrc tty baudot transcode' is unchecked. The interface includes the same top navigation bar and sidebar as the previous screenshot. A 'Show advanced' button is located in the top right corner of the main panel.



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 recv only attribute of SDP to inactive in the reply

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

- 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:

Join headers:

- 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:

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

- 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.

- 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: Countrycode

Header name: Request-URI

Action: manipulate

Comparison type: case-sensitive

Msg type: out-of-dialog

Methods:

Add Edit Delete
INVITE

Match value:

New value:

- 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

Add Edit Copy Delete Move up Move down	
Name	Element type
uriuser2	element-rule

- 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 top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various objects under 'session-router', including 'sip-config'. The main panel is titled 'Modify SIP manipulation / header rule' and contains the following configuration fields:

- Name: Change_Fromip_fqdn
- Header name: From
- Action: manipulate
- Comparison type: case-sensitive
- Msg type: out-of-dialog
- Methods: A list containing 'INVITE' with 'Add', 'Edit', and 'Delete' buttons above it.
- Match value: (empty field)
- Match value: (empty field)

This screenshot shows the same configuration page as above, but with a table view at the bottom. The table is titled 'Cfgrules' and has columns for 'Name' and 'Element type'. The table is currently empty.

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

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: FixUriHost
Parameter name:
Type: uri-host
Action: replace
Match val type: ip
Comparison type: case-sensitive
Match value:
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.

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 / header rule

Show advanced

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

- 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

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

- 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:

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:

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.

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 / header rule Show advanced

Name:

Header name:

Action:

Comparison type:

Msg type:

Methods:

OPTIONS

Match value:

New value:

CfgRules

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 shows the Oracle 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 'Objects' hierarchy, with 'sip-manipulation' selected. The main area is titled 'Add SIP manipulation / header rule'. It contains several form fields: 'Name' (Recordroute), 'Header name' (Record-Route), 'Action' (add), 'Comparison type' (case-sensitive), and 'Msg type' (out-of-dialog). Below these is a 'Methods' section with 'Add', 'Edit', and 'Delete' buttons, and a list containing 'OPTIONS'. There are also 'Match value' and 'New value' fields, with the 'New value' field containing the SIP URI '<sip:oracleesbc2.woodgrovebank.us>'. A 'Show advanced' button is located in the top right corner of the configuration area.

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 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'. The configuration fields are as follows:

Name:	Alter_contact						
Header name:	Contact						
Action:	manipulate						
Comparison type:	case-sensitive						
Msg type:	out-of-dialog						
Methods:	<table border="1"><tr><td>Add</td><td>Edit</td><td>Delete</td></tr><tr><td colspan="3">INVITE</td></tr></table>	Add	Edit	Delete	INVITE		
Add	Edit	Delete					
INVITE							
Match value:	<input type="text"/>						
New value:	<input type="text"/>						
CfgRules							

The screenshot shows the Oracle Configuration Manager 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 'Modify SIP manipulation / header rule'. The configuration fields are as follows:

Match value:	<input type="text"/>						
New value:	<input type="text"/>						
CfgRules	<table border="1"><tr><td colspan="2">Add Edit Copy Delete Move up Move down</td></tr><tr><th>Name</th><th>Element type</th></tr><tr><td>Contact_ip</td><td>element-rule</td></tr></table>	Add Edit Copy Delete Move up Move down		Name	Element type	Contact_ip	element-rule
Add Edit Copy Delete Move up Move down							
Name	Element type						
Contact_ip	element-rule						

- 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 / header rule / element rule

Show advanced

Name:

Parameter name:

Type:

Action:

Match val type:

Comparison type:

Match value:

New value:

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.

- 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 / header rule

Show advanced

Name:

Header name:

Action:

Comparison type:

Msg type:

Methods:

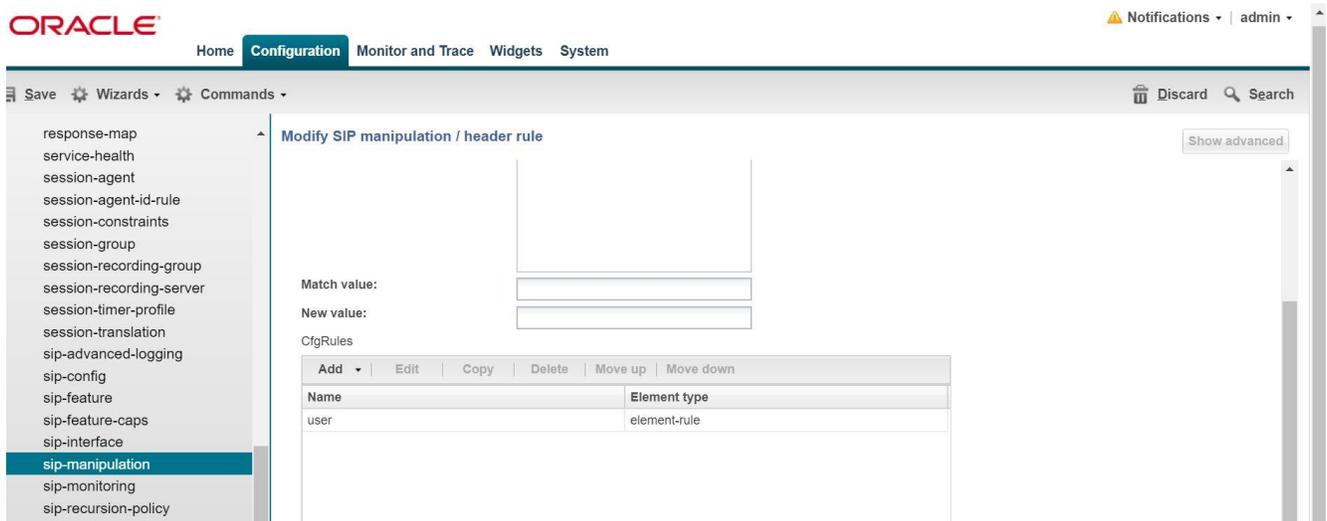
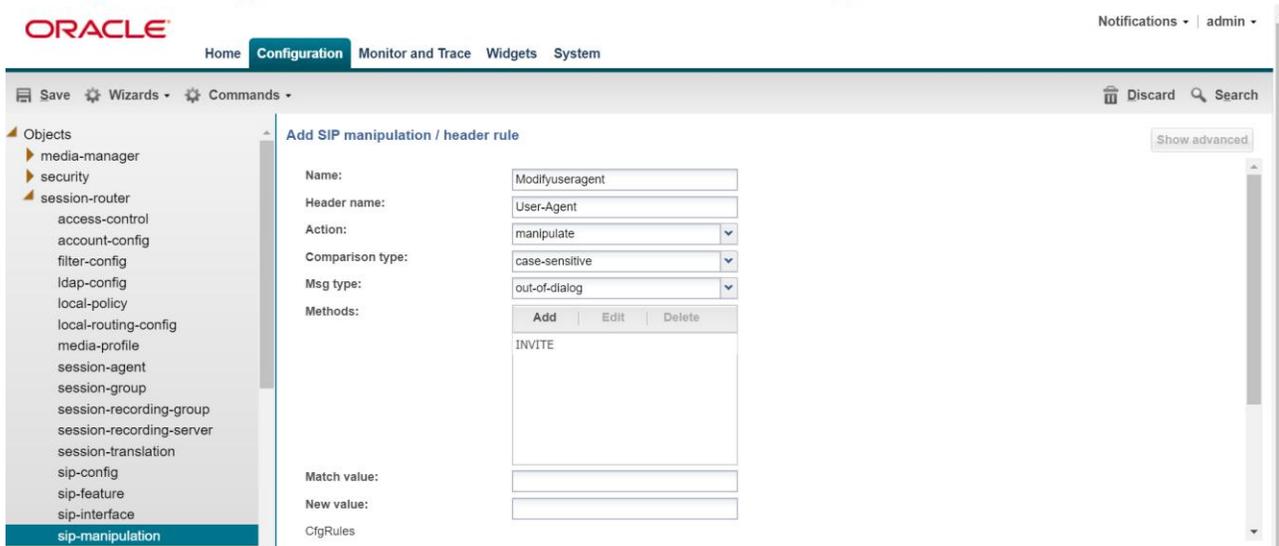
Match value:

New value:

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.



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:

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 rcvonly in the reply
- Change183to180 –Changes 183 Session in Progress to 180 Ringing for ringback requirements

- 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
-----	------	--------

- 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
Reqinactiveosendonly	mime-sdp-rule
Replyinactiveorecvonly	mime-sdp-rule
Change183to180	header-rule

Respondoptions

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

The screenshot shows the Oracle Configuration Manager interface. The top navigation bar includes the Oracle logo, a home icon, and tabs for 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. On the right, there are 'Notifications' and 'admin' links. Below the navigation bar, there are 'Save', ' Wizards', and ' Commands' options. The main content area is titled 'Add SIP manipulation / header rule' and contains the following configuration fields:

- Name: Respondoptions
- Header name: From
- Action: reject
- Comparison type: case-sensitive
- Msg type: request
- Methods: A table with columns 'Add', 'Edit', and 'Delete'. The 'Add' column contains the text 'OPTIONS'.
- Match value: (empty field)
- New value: 200 OK

At the bottom left, there is a 'Cfgrules' label. On the right side, there is a 'Show advanced' button.

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 Assistant interface. The top navigation bar includes 'Home', '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, there is a 'Discard' button and a 'Notifications' icon. A left-hand sidebar lists various configuration categories, with 'sip-interface' highlighted in blue. The main area is titled 'Modify SIP interface' and contains several configuration fields:

- Spl options: [Empty text field]
- Trust mode: [all] (dropdown menu)
- 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] (dropdown menu)
- Out manipulationid: [Teamsoutmanip] (dropdown menu)
- SIP atcf feature: [] (checkbox)
- Rfc2833 payload: [101] (Range: 96..127)
- Rfc2833 mode: [transparent] (dropdown menu)
- Response map: [] (dropdown menu)
- Local response map: [] (dropdown menu)
- Sec agree feature: [] (checkbox)

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

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..

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
 - sip-manipulation**

Modify SIP manipulation

Show advanced Show configuration

Join headers: Add | Edit | Delete

CfgRules

Add Edit Copy Delete Move up Move down	
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.



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 / header rule

Show advanced

Name:	<input type="text" value="Change_fqdn_to_ip_from"/>
Header name:	<input type="text" value="From"/>
Action:	<input type="text" value="manipulate"/>
Comparison type:	<input type="text" value="case-sensitive"/>
Msg type:	<input type="text" value="out-of-dialog"/>
Methods:	<div style="border: 1px solid #ccc; padding: 5px;"><p style="text-align: center;">Add Edit Delete</p><p>INVITE</p></div>
Match value:	<input type="text"/>
New value:	<input type="text"/>



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 / header rule / element rule

Show advanced

Name:	<input type="text" value="from_uri"/>
Parameter name:	<input type="text"/>
Type:	<input type="text" value="uri-host"/>
Action:	<input type="text" value="replace"/>
Match val type:	<input type="text" value="any"/>
Comparison type:	<input type="text" value="case-sensitive"/>
Match value:	<input type="text"/>
New value:	<input type="text" 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 rule. The page title is "Add SIP manipulation / header rule". The left sidebar shows a tree view of objects, with "session-router" 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: INVITE
- Match value: (empty)
- New value: (empty)

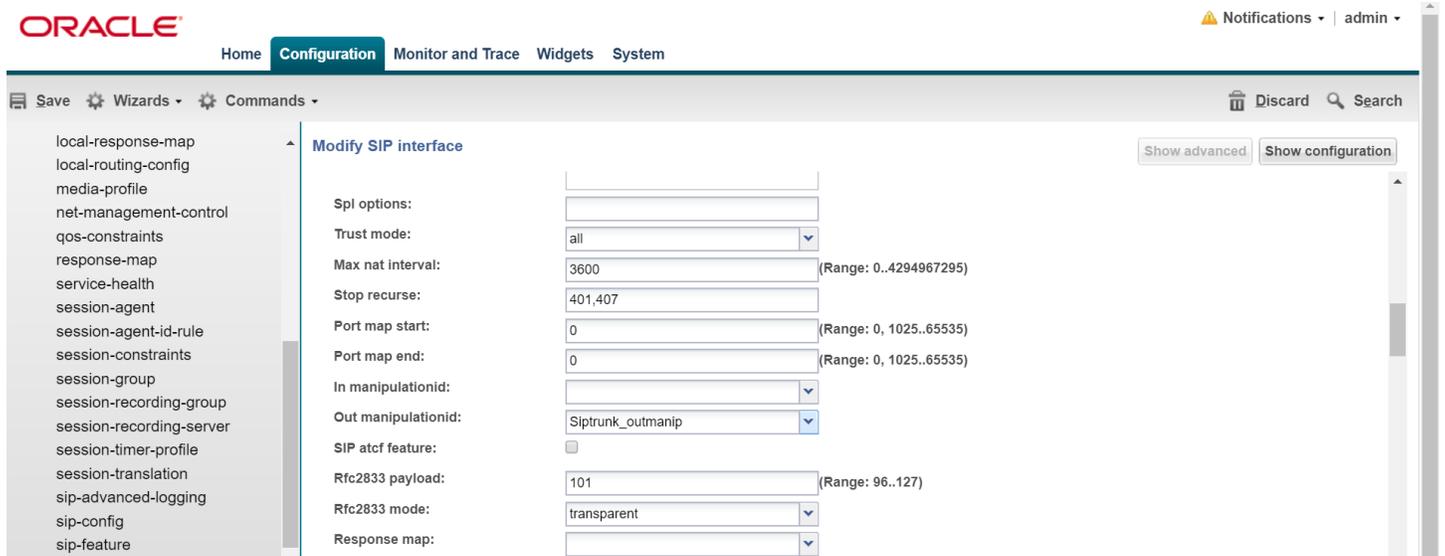
Buttons for "Add", "Edit", and "Delete" are visible above the Methods list. The "CfoRules" label is at the bottom left of the form area.

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

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

Applying the trunk side SIP manipulations to Trunk SIP Interface

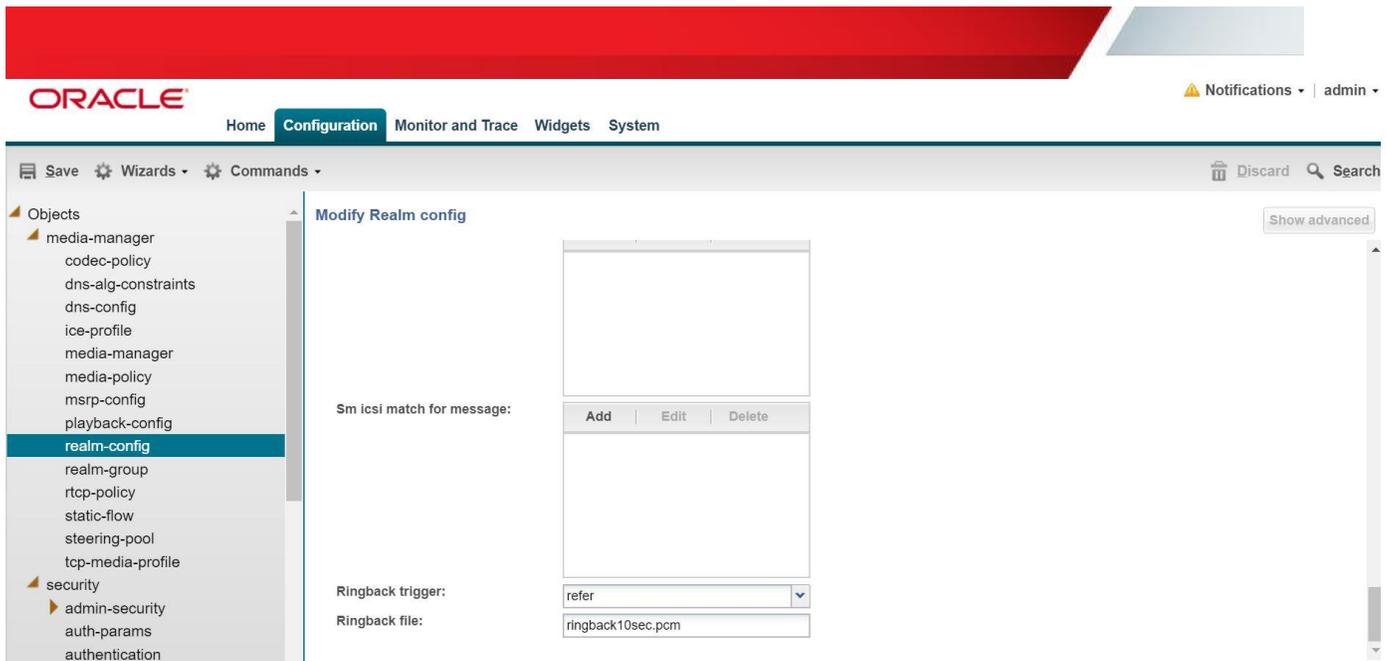
The Siptrunk_outmanip sip-manipulation is applied as the out-manipulationid in the sip-interface facing SIP Trunk



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

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

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

- 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:

Action:

Comparison type:

Match value:

New value:

CfgRules

- 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

Name	Element type
audio3	sdp-line-rule

The screenshot shows the Oracle Configuration Assistant interface. At the top, there is a red header with the Oracle logo and navigation tabs: Home, Configuration, Monitor and Trace, Widgets, and System. The Configuration tab is active. Below the header, there are buttons for Save, Wizards, and Commands. On the right, there are buttons for Discard and Search. A left-hand navigation pane lists various objects, with 'sip-feature' selected. The main area is titled 'Add SIP manipulation / mime SDP rule / SDP media rule / SDP line rule'. It contains a form with the following fields:

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

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

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. At the top, there is a red header with the Oracle logo and navigation tabs: Home, Configuration, Monitor and Trace, Widgets, and System. The Configuration tab is active. Below the header, there are buttons for Save, Wizards, and Commands. On the right, there are buttons for Discard and Search. A left-hand navigation pane lists various objects, with 'sip-feature' selected. The main area is titled 'Modify SIP feature'. It contains a form with the following fields:

- Name: feplaces
- Realm: access-teams (dropdown)
- Support mode inbound: Pass (dropdown)
- Require mode inbound: Pass (dropdown)
- Proxy require mode inbound: Pass (dropdown)
- Support mode outbound: Pass (dropdown)
- Require mode outbound: Pass (dropdown)
- Proxy require mode outbound: Pass (dropdown)

At the bottom of the form, there are 'OK' and 'Back' buttons. A 'Show advanced' button is located in the top right corner of the main area.

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                               forereplace
  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 allow configuration to assign IP address(es), ports & a realm.

The screenshot shows the Oracle GUI interface for configuring a steering pool. The top navigation bar includes 'ORACLE', 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. A notification bell and 'admin' user name are in the top right. Below the navigation bar, there are 'Save', 'Wizards', and 'Commands' options. The left sidebar lists various configuration categories, with 'steering-pool' highlighted. The main content area is titled 'Modify Steering pool' and contains the following configuration fields:

- IP address:
- Start port: (Range: 1..65535)
- End port: (Range: 1..65535)
- Realm ID:
- Network interface:

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

- 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:

Start port: (Range: 1..65535)

End port: (Range: 1..65535)

Realm ID:

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.

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

Modify Sdes profile

Show advanced

Name:

Crypto list:

Add	Edit	Delete
AES_CM_128_HMAC_SHA1_80		

Srtp auth:

Srtp encrypt:

SrTCP encrypt:

Mki:

Egress offer format:

Use Ingress session params:

Add	Edit	Delete
-----	------	--------

Make sure to configure 31 in the lifetime value as shown

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 'sdes-profile' selected under 'media-security'. The main area is titled 'Modify Sdes profile' and contains the following fields:

- Options: A table with 'Add', 'Edit', and 'Delete' buttons.
- Key: A text input field.
- Salt: A text input field.
- Srtp rekey on re invite: A checkbox.
- Lifetime: A text input field containing '31', with a range '(Range: 0, 20..48)' indicated.

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 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 'media-sec-policy' selected under 'media-security'. The main area is titled 'Modify Media sec policy' and contains the following fields:

- Name: A text input field containing 'RTP'.
- Pass through: A checkbox.
- Options: A table with 'Add', 'Edit', and 'Delete' buttons.
- Inbound section:
 - Profile: A dropdown menu.
 - Mode: A dropdown menu containing 'rtp'.
 - Protocol: A dropdown menu containing 'none'.
- Outbound section:
 - Profile: A dropdown menu.

- 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:

- 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:

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: SDES

Mode: srtp

Protocol: sdes

Outbound

Profile: SDES

Mode: srtp

Protocol: sdes

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

ORACLE Notifications | admin

Home Configuration Monitor and Trace Widgets System

Save Wizards Commands Discard Search

steering-pool top-media-profile 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 Realm config

Show advanced

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

RTCP mux:

Ice profile: [dropdown]

DTLS srtp profile: [dropdown]

Srtp msm passthrough:

Class profile: [dropdown]

In translationid: [dropdown]

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 Communications Configuration Manager interface. The left sidebar lists various configuration objects, with 'rtcp-policy' selected under the 'media-manager' category. The main panel is titled 'Modify RTCP policy' and contains the following fields:

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

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

The screenshot shows the Oracle Communications Configuration Manager interface. The left sidebar lists various configuration objects, with 'realm-config' selected under the 'media-manager' category. The main panel is titled 'Modify Realm config' and contains the following fields:

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

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

- 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

Show advanced

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

- 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

Modify Ice profile

Show advanced

Name:	ice
Stun conn timeout:	0 (Range: 0..9999)
Stun keep alive interval:	0 (Range: 0..300)
Stun rate limit:	100 (Range: 0..99999)

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

- admin-security
- auth-params
- authentication
- cert-status-profile

Modify Realm config

Show advanced

min 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"/> (Range: 0..999999999)
Max priority bandwidth:	<input type="text" value="0"/> (Range: 0..999999999)
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"/>

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

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

Modify SIP interface

Show advanced Show configuration

Initial inv trans expire:	<input type="text" value="0"/> (Range: 0..999999999)
Session max life limit:	<input type="text" value="0"/>
Proxy mode:	<input type="text"/>
Redirect action:	<input type="text"/>
Nat traversal:	<input type="text" value="always"/>
Nat interval:	<input type="text" value="3600"/> (Range: 0..4294967295)
TCP nat interval:	<input type="text" value="90"/> (Range: 0..4294967295)
Registration caching:	<input checked="" type="checkbox"/>
Min reg expire:	<input type="text" value="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.

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.

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

Name:

Description:

Split headers:

Join headers:

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

CfgRules

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

Show advanced

Modify SIP manipulation / header rule

Name:

Header name:

Action:

Comparison type:

Msg type:

Methods:

Add	Edit	Delete
INVITE		

Match value:

Show advanced

Modify SIP manipulation / header rule / element rule

Name:

Parameter name:

Type:

Action:

Match val type:

Comparison type:

Match value:

New value:

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

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 ac

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.

- 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 / mime SDP rule / SDP session rule / SDP line rule

Show advanced

Name:

Type:

Action:

Comparison type:

Match value:

New value:

- 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 / 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
------------	------	------	--------	---------	-----------

- 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:

Add	Edit	Delete
-----	------	--------

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					

- 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:

- 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.

- 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:

Add	Edit	Delete

Match value:

New value:

CfgRules

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

The following are the recommended configuration values based on Best Current Practices for an Oracle SBC NN4600 deployed in a Sip Peering Environment:

Acme Packet 4600 1000000 Flow Table 16G memory - copper single GigE

Platform:	AP 4600
Flow Table:	1000000
Memory:	16 GB
Software Release:	SCZ8.1.0

The following table lists the five parameters germane to DDoS Configuration Settings in Peering Environments for the Acme Packet 4600 and their settings on the core and peer realms.

parameter	Core realm-config	Peer Realm-config
access-control-trust-level	high	low
average-rate-limit	0	0
invalid-signal-threshold	0	0
maximum-signal-threshold	0	0

parameter	Core realm-config	Peer Realm-config
untrusted-signal-threshold	0	0

The **media-manager** configuration should be set as suggested in the following table for the Acme Packet 4600 in the respective model.

Parameter	PBRB Model	SSNHTN Model	SNB Model
max-signaling-bandwidth	2651610	2651610	2651610
max-untrusted-signaling	1	1	1
min-untrusted-signaling	1	1	1
tolerance-window	30	30	30

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.

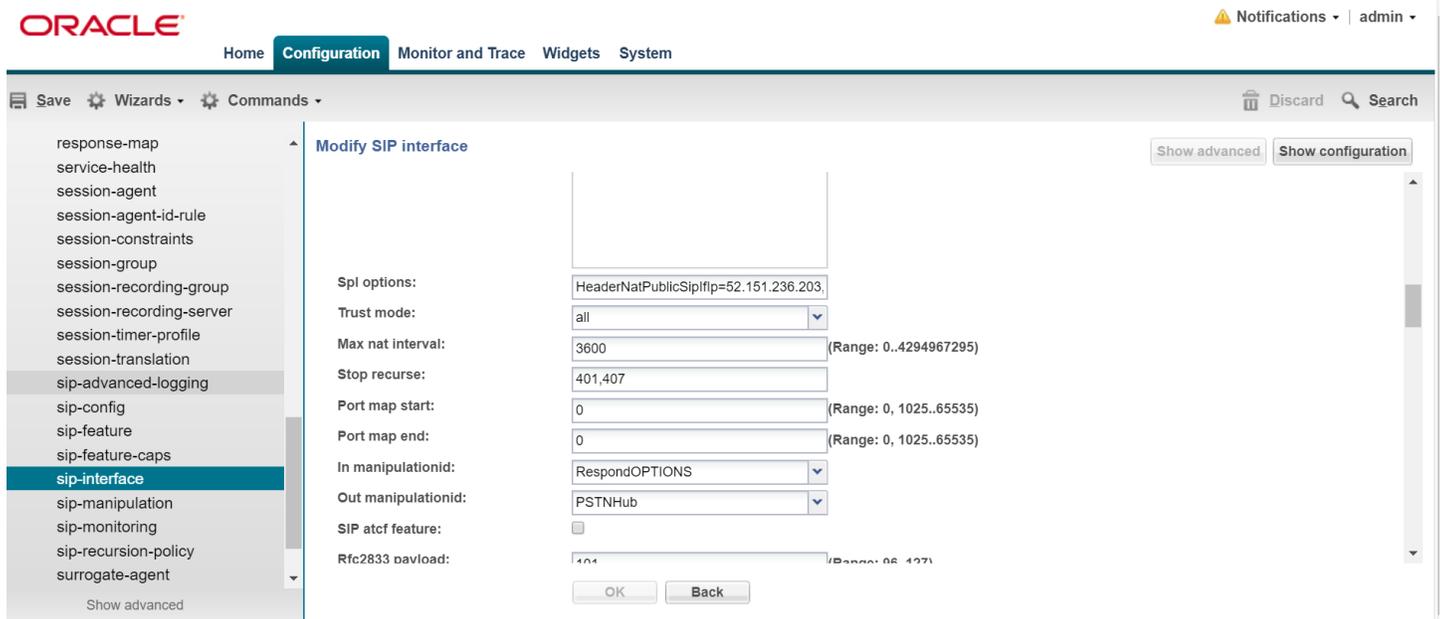
- The private IP address must be the same as the SIP Interface IP address.
- The public IP address must be the public IP address of the NAT device

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

Here is a CLI configuration snapshot of the SBC.

```
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 Oraclesbc2.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                               SRTTP
  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                     SRTTP
  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         access-pstn
options               inmanip-before-validate
                      max-udp-length=0
extra-method-stats    enabled

sip-feature
name                  replaces
realm                 access-teams
require-mode-inbound   Pass
require-mode-outbound  Pass

sip-interface
state                 enabled
realm-id              access-pstn
description            to trunk
sip-port
    address            192.65.72.196
    allow-anonymous    agents-only
in-manipulationid
out-manipulationid    Siptrunk_outmanip

sip-interface
realm-id              access-teams
sip-port
    address            155.212.214.172
    port                5061
transport-protocol     TLS
tls-profile            TLSTeams
allow-anonymous        agents-only

```

```

nat-traversal          always
nat-interval           3600
registration-caching   enabled
in-manipulationid     Teamsinmanip
out-manipulationid     Teamsoutmanip
sip-profile            foreplace
sip-manipulation
  name                 Checkfor1831
  header-rule
    name               check183
    header-name        @status-line
    action              manipulate
    msg-type            reply
    methods             INVITE
    element-rule
      name              is183
      type               status-code
      action             store
      comparison-type   pattern-rule
      match-value       183
mime-sdp-rule
  name                 if183
  msg-type              reply
  methods               INVITE
  action                manipulate
  comparison-type       boolean
  match-value           $check183.$sis183
  sdp-session-rule
    name                au
    action               manipulate
    sdp-line-rule
      name               checkc
      type                c
      action              store
      comparison-type    pattern-rule
      match-value        ^((?! (155.214.212.172))) *$
mime-sdp-rule
  name                 deletesdp
  msg-type              reply
  methods               INVITE
  action                delete
  comparison-type       boolean
  match-value           $if183.$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         $REMOTE_IP
sip-manipulation
  name                Teamsinmanip
  header-rule
    name              Respondoptions
    header-name       From
    action            reject
    msg-type          request
    methods           OPTIONS
    new-value         200 OK
header-rule
  name                From
  header-name         From
  action              sip-manip
  new-value           Checkfor1831
mime-sdp-rule
  name                Reqinactivetosendonly
  msg-type            request
  methods             INVITE
  action              manipulate
  sdp-media-rule
    name              audio
    media-type        audio
    action            manipulate
  sdp-line-rule
    name              audiol
    type              a
    action            replace
    match-value       inactive
    new-value         sendonly
mime-sdp-rule
  name                Replyinactivetorecvonly
  msg-type            reply
  methods             INVITE
  action              manipulate
  sdp-media-rule
    name              audio
    media-type        audio
    action            manipulate
  sdp-line-rule
    name              audiol
    type              a
    action            replace
    match-value       inactive
    new-value         recvonly
sip-manipulation
  name                Teamsoutmanip
  header-rule
    name              Countrycode
    header-name       Request-URI
    action            manipulate
    msg-type          out-of-dialog
    methods           INVITE
  element-rule
    name              uriuser2
    type              uri-user
    action            replace
    new-value         "1"+$
header-rule
  name                Change fromip fqdn

```

```

header-name To
action manipulate
msg-type out-of-dialog
methods INVITE
element-rule
  name
  type uri-host
  action replace
  match-val-type ip
  new-value $RURI_HOST.$0
element-rule
  name urinumber
  type uri-user
  action replace
  new-value "1"+$

header-rule
  name Change_to_userandhost
  header-name From
  action manipulate
  msg-type out-of-dialog
  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
  new-value

"<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 out-of-dialog
  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
http-interface-list

0



CONNECTWITHUS



Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2019, 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. 0616