



ORACLE

Verizon Business IP Trunking with Oracle
ESBC and Microsoft Teams-Media Bypass

Technical Application Note

ORACLE

COMMUNICATIONS



Disclaimer

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

Contents

1	REVISION HISTORY	5
2	INTENDED AUDIENCE	5
3	RELATED DOCUMENTATION	5
3.1	VERIZON BUSINESS	5
3.2	ORACLE SBC	5
3.3	MICROSOFT TEAMS	5
4	VALIDATED ORACLE VERSIONS	6
5	ABOUT TEAMS DIRECT ROUTING	6
6	INFRASTRUCTURE REQUIREMENTS	7
7	CONFIGURATION	7
7.1	PREREQUISITES	8
7.2	ABOUT SBC DOMAIN NAME	9
8	CONFIGURE DIRECT ROUTING	10
8.1.1	Access Teams Admin Center	10
8.1.2	Configure Online PSTN Gateway	11
8.1.3	Configure Online PSTN Usage	11
8.1.5	Configure Online Voice Route	12
8.1.6	Configure Voice Routing Policy	13
8.1.7	Assign Voice Routing Policy to Users	13
9	ORACLE SBC CONFIGURATION	14
9.1	GLOBAL CONFIGURATION ELEMENTS	15
9.1.1	System Config	15
9.1.2	Media Manager	16
9.1.3	Sip Config	16
9.2	NETWORK CONFIGURATION	17
9.2.1	Physical Interfaces	18
9.2.2	Network Interfaces	18
9.3	SECURITY CONFIGURATION	19
9.3.1	Certificate Records	19
9.3.2	SBC End Entity Certificate	19
9.3.3	Root CA and Intermediate Certificates	20
9.3.4	Import Certificates to SBC	22
9.3.5	TLS Profile	23
9.3.6	Media Security Configuration	24
9.3.7	Sdes-profile	24
9.3.8	Media Security Policy	25
9.3.9	IKE/IPSEC Config	26
9.3.10	IKE Config	26
9.3.11	Ike Interface	27
9.3.12	Ike SaInfo	27
9.3.13	Security Policy	27
9.4	TRANSCODING CONFIGURATION	28
9.4.1	Media Profiles	28

9.4.2	Codec Policies	29
9.4.3	RTCP Policy	30
9.4.4	Ice Profile	30
9.4.5	QOS Marking.....	31
9.5	MEDIA CONFIGURATION.....	32
9.5.1	Realm Config.....	32
9.5.2	Steering Pools	33
9.6	SIP CONFIGURATION.....	34
9.6.1	SIP Profile.....	34
9.6.2	Sip Feature.....	34
9.6.3	Sip Manipulation	35
9.6.4	Sip Interface.....	37
9.6.5	Session Agents.....	38
9.6.6	Session Agent Group.....	39
9.7	ROUTING CONFIGURATION	41
9.7.1	Local Policy Configuration	41
9.7.2	Access Control (Optional).....	42
10	VERIFY CONNECTIVITY	44
10.1	OCSBC OPTIONS PING.....	44
10.2	MICROSOFT SIP TESTER CLIENT	44
11	SYNTAX REQUIREMENTS FOR SIP INVITE AND SIP OPTIONS.....	45
11.1	TERMINOLOGY.....	45
11.2	REQUIREMENTS FOR INVITE MESSAGES.....	45
11.2.1	Contact.Header	46
11.2.2	From Header:.....	46
11.2.3	To Header	46
11.3	REQUIREMENTS FOR OPTIONS MESSAGES.....	47
11.3.1	Contact Header	47
12	MICROSOFT TEAMS DIRECT ROUTING INTERFACE CHARACTERISTICS	47
13	APPENDIX A.....	49
13.1	SBC BEHIND NAT SPL CONFIGURATION	49
14	CAVEATS.....	50
14.1	No AUDIO-ON-HOLD	50
15	CALL TRANSFERS.....	51
15.1	STORE REFERRED-BY HEADER.....	51
15.1.1	Header Rule:.....	51
15.2	ADD DIVERSION HEADER	52
15.2.1	Header Rule:.....	52
16	RUNNING CONFIGURATION	53

1 Revision History

Version	Date Revised	Description of Changes
1.0	09/27/2020	Initial publication
1.1	01/11/2022	<ul style="list-style-type: none">Removed Reference to Teams Sip-All FQDNAdded new MSFT Networks for ACL Config

2 Intended Audience

This document describes how to configure the Oracle SBC to interwork between Verizon Business Sip Trunk and Microsoft Teams Direct Routing. This paper is intended for IT or telephony professionals.

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

3 Related Documentation

3.1 Verizon Business

- <https://www.verizon.com/business/products/voice-collaboration/voip/ip-trunking/>

3.2 Oracle SBC

- [Oracle® Enterprise Session Border Controller Web GUI User Guide](#)
- [Oracle® Enterprise Session Border Controller ACLI Configuration Guide](#)
- [Oracle® Enterprise Session Border Controller Release Notes](#)
- https://docs.oracle.com/cd/F12246_01/doc/sbc_scz830_security.pdf

3.3 Microsoft Teams

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

4 Validated Oracle Versions

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

SCZ830

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

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

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

5 About Teams Direct Routing

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

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

6 Infrastructure Requirements

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

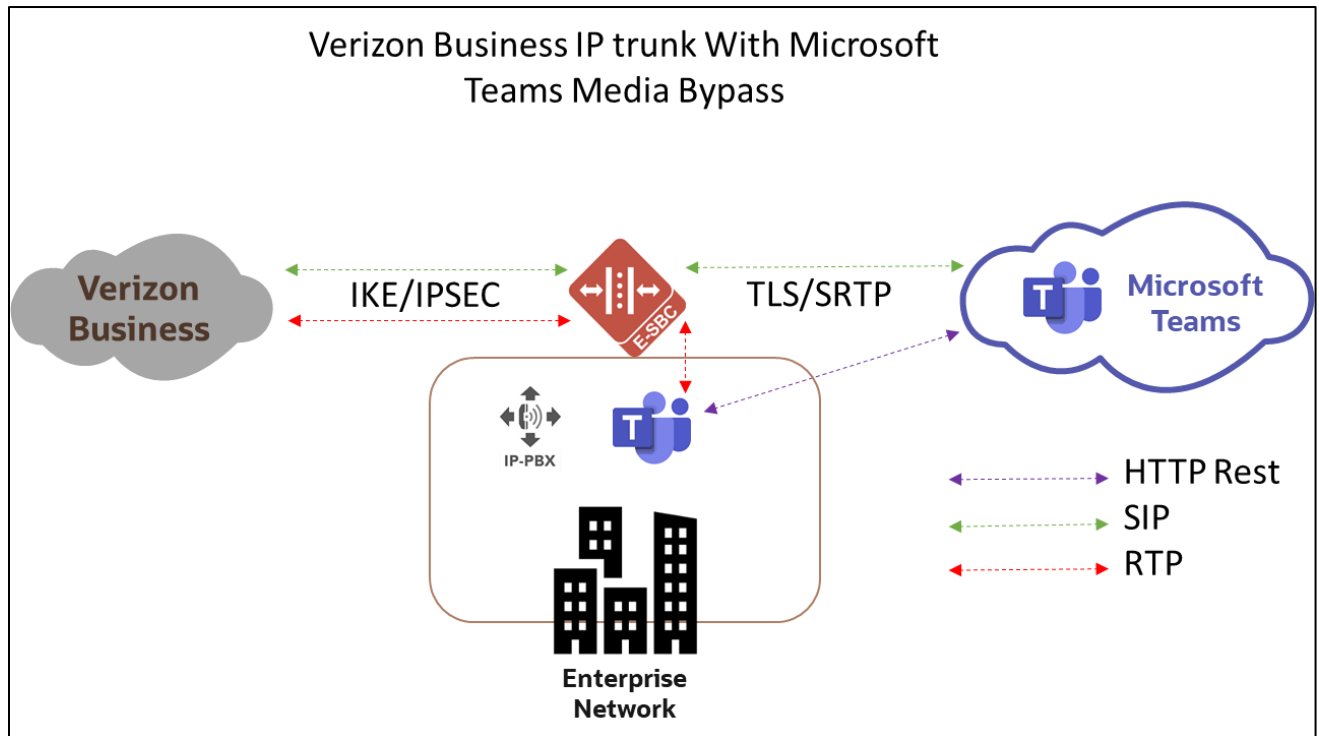
Infrastructure Prerequisite	Details
Certified Session Border Controller (SBC)	See Microsoft's Plan Direct Routing document
SIP Trunks connected to the SBC	
Office 365 tenant	
Domains	
Public IP address for the SBC	
Fully Qualified Domain Name (FQDN) for the SBC	
Public DNS entry for the SBC	
Public trusted certificate for the SBC	
Firewall ports for Direct Routing signaling	
Firewall IP addresses and ports for Direct Routing media	
Media Transport Profile	
Firewall ports for client media	

7 Configuration

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

Below shows the connection topology example for Verizon Business and Microsoft Teams. There are multiple connections shown:

- Teams Direct Routing Interface on the WAN
- Verizon Business Sip trunk terminating on the SBC



These instructions cover configuration steps for the Oracle SBC to interface with both Microsoft Teams Direct Routing Interface and Verizon Business IP Trunk.

7.1 Prerequisites

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

- Public IP address
- FQDN name for each registered subdomain representing individual tenants using the multitenant Direct Routing Trunk. Each FQDN must resolve to the Public IP address
- Public certificate, issued by one of the supported CAs (refer to [Related Documentation](#) for details about supported Certification Authorities).
- IPSEC Template Provided by Verizon Business to establish IKE/IPSEC tunnel

7.2 About SBC Domain Name

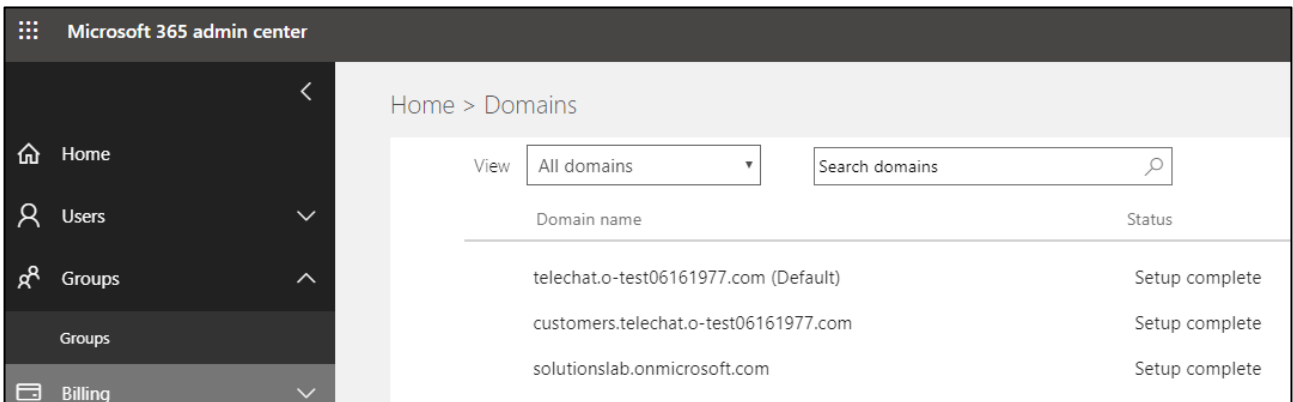
The SBC domain name must be from one of the names registered in “Domains” of the tenant. You cannot use the *.onmicrosoft.com tenant for the domain name. For example, on the picture below, the administrator registered the following DNS names for the tenant:

DNS Name	Can Be Used For SBC	Example of FQDN names
telechat.o-test06161977.com	YES	<p>Valid FQDN:</p> <ul style="list-style-type: none"> customers.telechat.o-test06161977.com Sbc51. telechat.o-test06161977.com Ussbc15. telechat.o-test06161977.com Europe. telechat.o-test06161977.com <p>Invalid FQDN:</p> <ul style="list-style-type: none"> Sbc1.europe.telechat.o-test06161977.com <i>(this would require registering domain name "Europe.adatum.biz")</i>
solutionslab.onmicrosoft.com	NO	Using *.onmicrosoft.com domains is not supported for SBC names

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

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

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



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

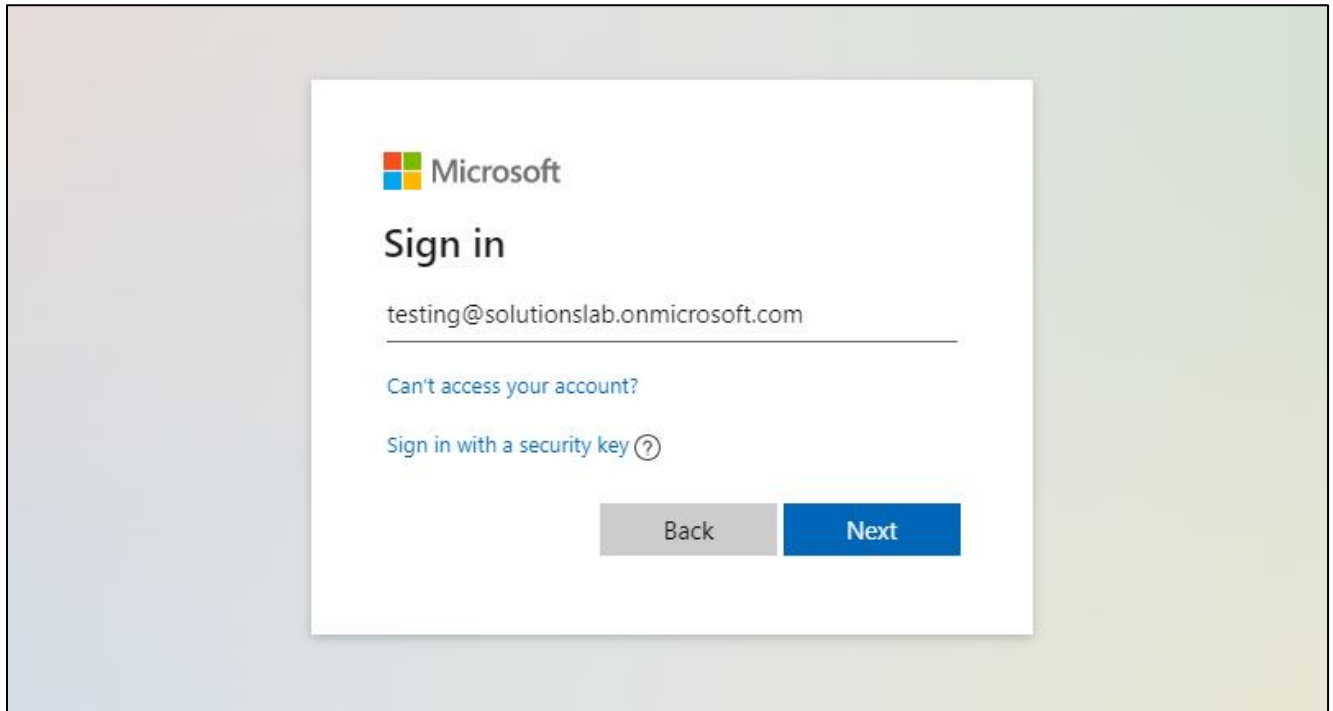
FQDN Names	Public IP Address
telechat.o-test06161977.com	141.146.36.68

8 Configure Direct Routing

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

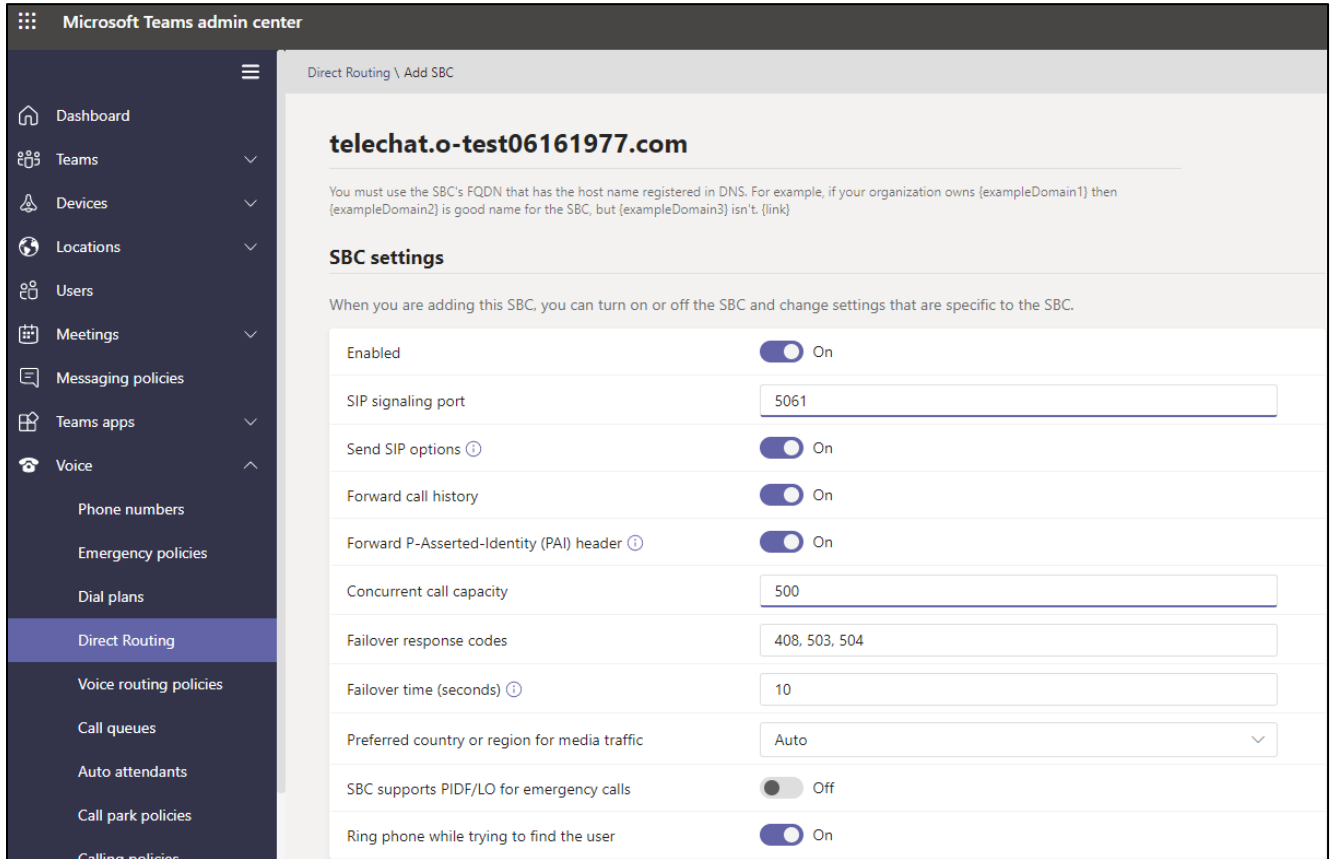
8.1.1 Access Teams Admin Center

The first step is to access the [Teams Admin Center](#) with administrator admin credentials:



8.1.2 Configure Online PSTN Gateway

Configuration Path: Voice/Direct Routing/SBC



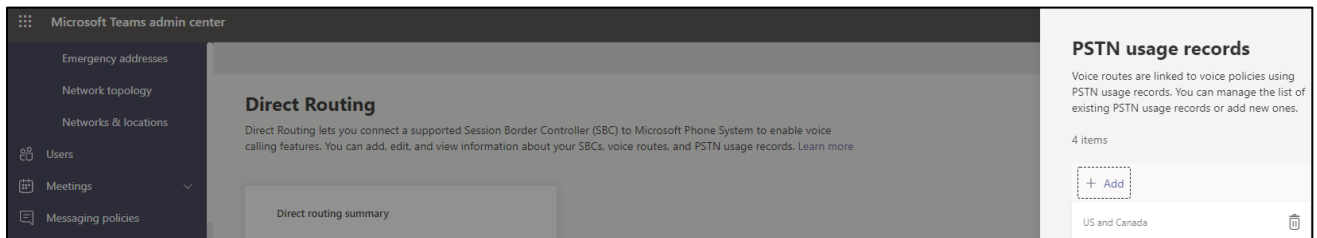
- Click Save at the bottom of the page

Note: Some configuration fields are not available through the Microsoft Portal, and must be set via PowerShell. Please refer to [Microsoft Teams Documentation](#) for further details

8.1.3 Configure Online PSTN Usage

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

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



8.1.5 Configure Online Voice Route

Configuration Path: Voice/Direct Routing/Voice Routes

The screenshot displays the Microsoft Teams admin center interface for configuring a voice route. The left-hand navigation pane is open to the 'Voice' section, with 'Direct Routing' selected. The main content area shows the configuration for the 'Oracle_US' voice route. The 'Priority' is set to 1, and the 'Dialled number pattern' is set to `^\(+1[0-9]{10})$`. Below this, the 'SBCs enrolled' section shows one SBC: 'sbc2.customers.telechat.o-test06161977.com'. The 'PSTN usage records' section shows one record: 'US and Canada'.

Microsoft Teams admin center

Voice routes \ Oracle_US

Oracle_US

Description

Priority: 1

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

SBCs enrolled

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

Add/remove SBCs 1 item

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

PSTN usage records

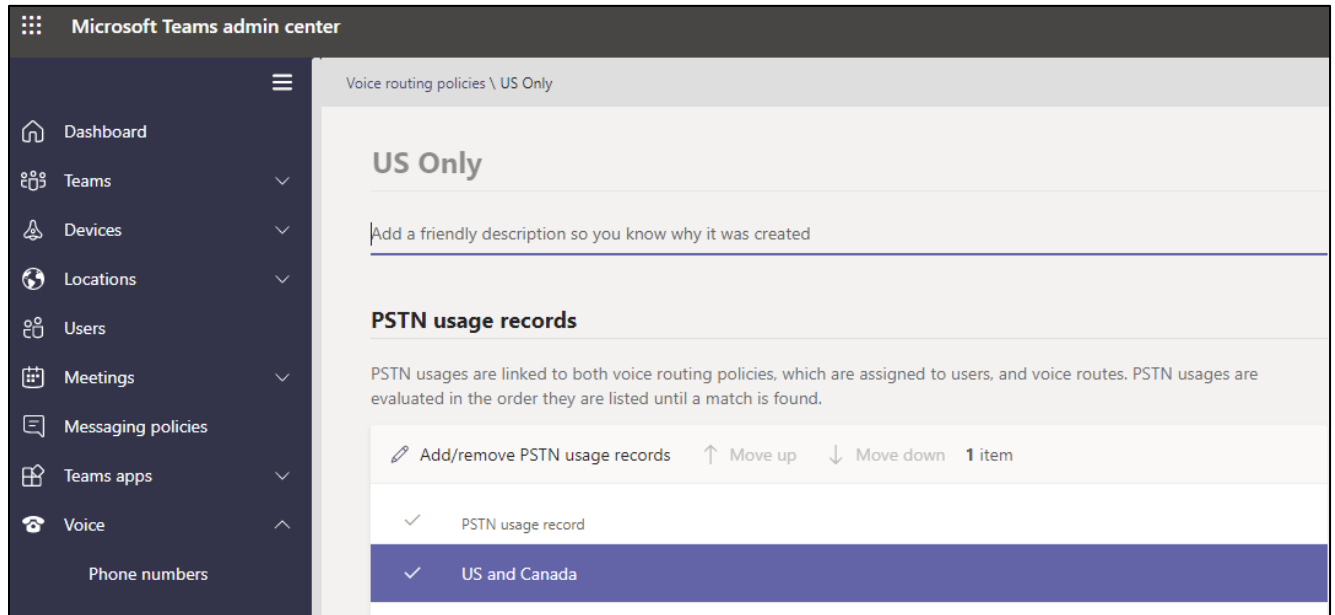
The voice routing policy is linked to a voice route using the PSTN usage records below. You can add existing PSTN usage records, change the order in which the voice routing should be processed, and assign the policy to users.

Add/remove PSTN usage records ↑ Move up ↓ Move down 1 item

- ✓ PSTN usage record
- ✓ US and Canada

8.1.6 Configure Voice Routing Policy

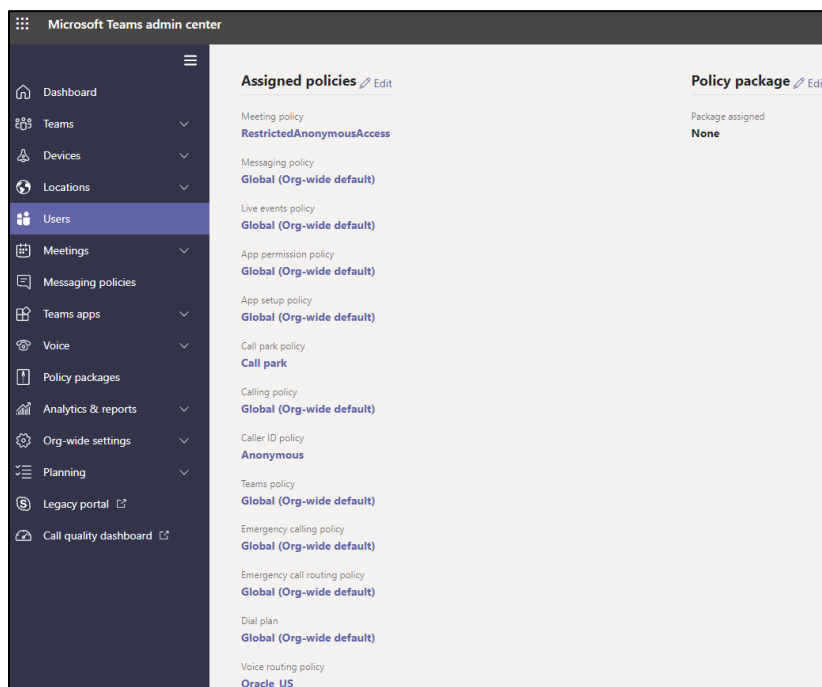
Configuration Path: Voice/Voice Routing Policies



8.1.7 Assign Voice Routing Policy to Users

Configuration Path: Users/Select the "User"/Policies

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



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

9 Oracle SBC Configuration

There are two methods for configuring the OCSBC, ACLI or GUI.

For the purposes of this note, we'll be using the OCSBC GUI for all configuration examples. We will however provide the ACLI path to each element.

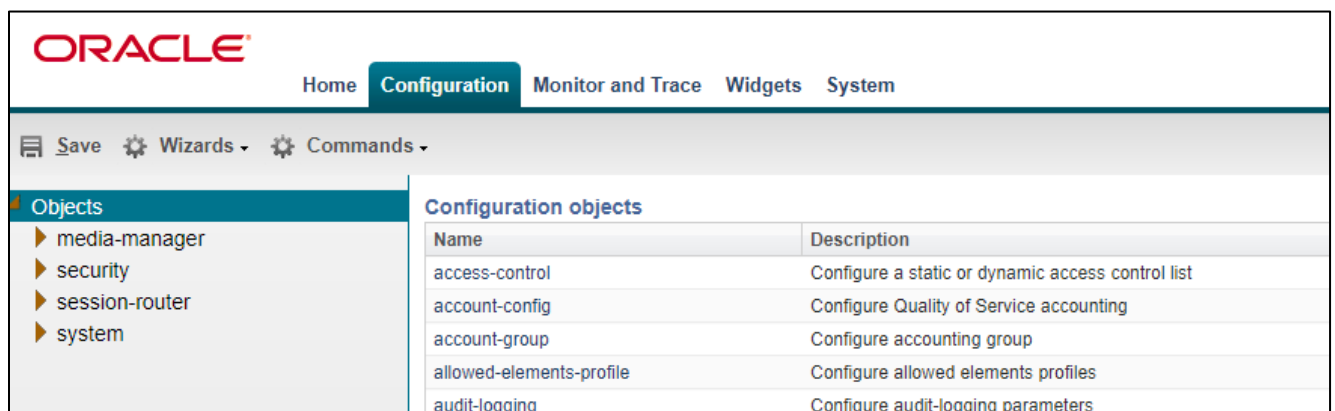
This guide assumes the OCSBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, web-server-config has been enabled for GUI access. If you require more information on how to install your SBC platform, please refer to the [ACLI configuration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

To access the OCSBC GUI, enter the management IP address into a web browser. When the login screen appears, enter the username and password to access the OCSBC.

Once you have accessed the OCSBC, at the top, click the Configuration Tab. This will bring up the OCSBC Configuration Objects List on the left hand side of the screen.

Any configuration parameter not specifically listed below can remain at the OCSBC default value and does not require a change for connection to MSFT Teams Direct routing or Verizon Business to function properly.

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



The screenshot displays the Oracle SBC Configuration GUI. At the top, the Oracle logo is visible on the left, and navigation tabs for Home, Configuration, Monitor and Trace, Widgets, and System are on the right. Below the navigation, there are icons for Save, Wizards, and Commands. The main area is divided into two sections: 'Objects' on the left and 'Configuration objects' on the right. The 'Objects' section lists 'media-manager', 'security', 'session-router', and 'system'. The 'Configuration objects' section is a table with two columns: 'Name' and 'Description'.

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

9.1 Global Configuration Elements

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

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

9.1.1 System Config

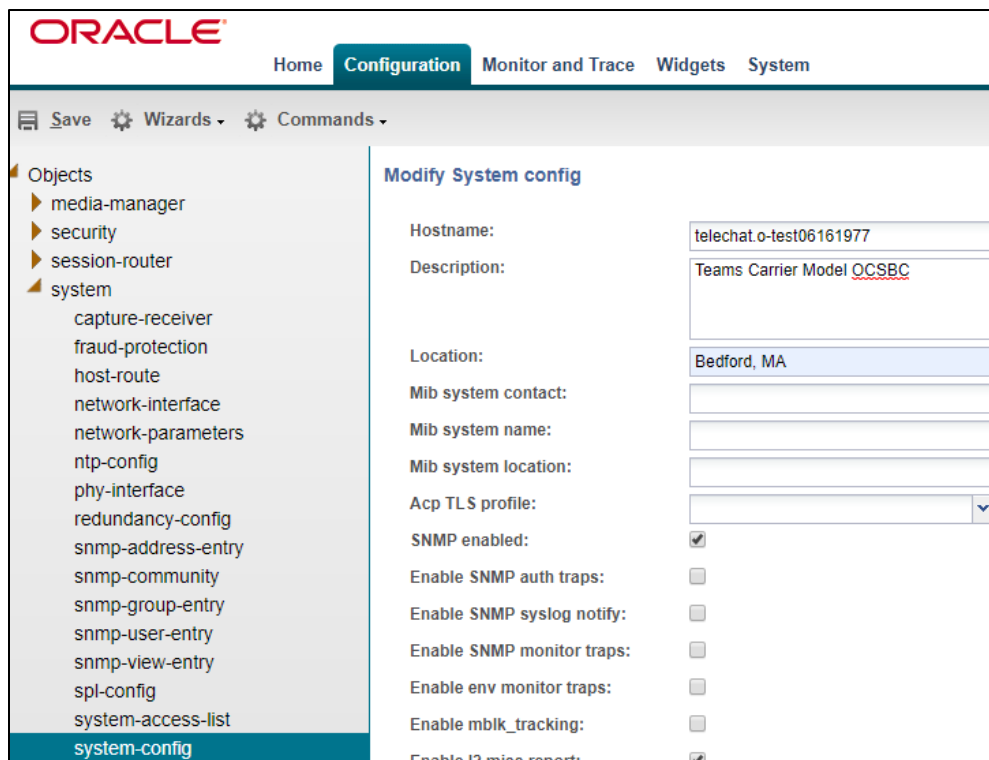
To configure system level functionality for the OCSBC, you must first enable the system-config

GUI Path: system/system-config

ACL Path: config t→system→system-config

Note: The following parameters are optional but recommended for system config

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



The screenshot displays the Oracle OCSBC configuration 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 icons for 'Save', 'Wizards', and 'Commands'. On the left side, a tree view shows the configuration hierarchy under 'system', with 'system-config' selected. The main area is titled 'Modify System config' and contains the following fields:

Hostname:	telechat.o-test06161977
Description:	Teams Carrier Model OCSBC
Location:	Bedford, MA
Mib system contact:	
Mib system name:	
Mib system location:	
Acp TLS profile:	
SNMP enabled:	<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"/>

- Click the OK at the bottom of the screen

9.1.2 Media Manager

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

GUI Path: media-manager/media-manager

ACL Path: config t→media-manager→media-manager-config

The following options are recommended for global media manager when interfacing with MSFT Teams Direct Routing

- Options: Click Add, in pop up box, enter the string: **audio-allow-asymmetric-pt**
- Click Apply/Add Another, then enter: **xcode-gratuitous-rtcp-report-generation** (requires a reboot to take effect)
- Max-Untrusted-Signalling=1
- Min-Untrusted-Signalling=1
- Hit OK in the box

The screenshot displays the Oracle SBC GUI for configuring the Media Manager. The interface includes a top navigation bar with 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this is a toolbar with 'Save', 'Wizards', and 'Commands'. The left sidebar shows a tree view of configuration objects, with 'media-manager' selected. The main area is titled 'Modify Media manager' and contains the following configuration fields:

State:	<input checked="" type="checkbox"/>									
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:	<input type="checkbox"/>									
Algd log level:	NOTICE									
Mbcd log level:	NOTICE									
Options:	<table border="1"><tr><td>Add</td><td>Edit</td><td>Delete</td></tr><tr><td colspan="3">audio-allow-asymmetric-pt</td></tr><tr><td colspan="3">xcode-gratuitous-rtcp-report-generation</td></tr></table>	Add	Edit	Delete	audio-allow-asymmetric-pt			xcode-gratuitous-rtcp-report-generation		
Add	Edit	Delete								
audio-allow-asymmetric-pt										
xcode-gratuitous-rtcp-report-generation										

9.1.3 Sip Config

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

GUI Path: session-router/sip-config

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

The following are recommended parameters under the global sip-config:

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

The screenshot displays the Oracle SIP configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this, there are 'Save', 'Wizards', and 'Commands' options. The left sidebar shows a tree view of configuration categories, with 'sip-config' highlighted. The main content area is titled 'Modify SIP config' and contains the following settings:

- State:
- Dialog transparency:
- Home Realm ID: Teams
- Egress Realm ID: (empty)
- Nat mode: None
- Registrar domain: *
- Registrar host: *
- Registrar port: 5060
- Init timer: 500
- Max timer: 4000
- Trans expire: 32
- Initial inv trans expire: 0
- Invite expire: 180
- Session max life limit: 0
- Enforcement profile: (empty)
- Red max trans: 10000

An 'Options' section at the bottom includes an 'Add' button and a list of options: 'inmanip-before-validate' and 'max-udp-length=0'.

- Click OK at the bottom

9.2 Network Configuration

To connect the SBC to network elements, we must configure both physical and network interfaces. For the purposes of this example, we will configure two physical interfaces, and two network interfaces. One to communicate with MSFT Teams Direct Routing, and one to connect to Verizon Business IP Trunk.

9.2.1 Physical Interfaces

GUI Path: system/phy-interface

ACL Path: config t→system→phy-interface

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

Config Parameter	Teams	Verizon
Name	s0p0	S1p0
Operation Type	Media	Media
Slot	0	1
Port	0	0

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

The screenshot shows the Oracle configuration interface. The 'Phy interface' section is active, displaying a table with the following data:

Name	Operation type	Port	Slot
s0p0	Media	0	0
s1p0	Media	0	1

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

9.2.2 Network Interfaces

GUI Path: system/network-interface

ACL Path: config t→system→network-interface

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

Configuration Parameter	Teams	PSTN
Name	s0p0	s1p0
Hostname	(Optional)	
IP Address	141.146.36.68	155.212.214.101
Netmask	255.255.255.192	255.255.255.0
Gateway	141.146.36.65	155.212.214.1
DNS Primary IP	8.8.8.8	
DNS Domain	Carrier Default Domain	

The screenshot shows the Oracle SBC Configuration interface. The 'Configuration' tab is active. On the left, a tree view shows 'Objects' with sub-items: media-manager, security, session-router, system, capture-receiver, and find-configuration. The main area displays the 'Network interface' configuration. A search criteria field is set to 'All'. Above a table are buttons for 'Add', 'Edit', 'Copy', 'Delete', 'Delete All', 'Upload', and 'Download'. The table has columns for Name, Sub port id, Description, Hostname, and IP address. Two rows are visible: 's0p0' with sub port id '0', hostname 'telechat.o-test06161977.com', and IP address '141.146.36.68'; and 's1p0' with sub port id '0' and IP address '155.212.214.101'.

Name	Sub port id	Description	Hostname	IP address
s0p0	0		telechat.o-test06161977.com	141.146.36.68
s1p0	0			155.212.214.101

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

9.3 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Teams Direct Routing and IKE/IPSEC to connect to Verizon Business IP Trunk.

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

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

Verizon Business requires a secure, IPSEC tunnel be established between the Oracle SBC and the VZB network. You must obtain the IPSEC Template from your Verizon Business account team before configuring IKE/IPSEC on the Oracle SBC.

9.3.1 Certificate Records

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

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

GUI Path: security/certificate-record

ACL Path: config t→security→certificate-record

For the purposes of this application note, we'll create four certificate records. They are as follows:

- SBC Certificate (end-entity certificate)
- DigiCert RootCA Cert
- DigiCert Intermediate Cert (this is optional – only required if your server certificate is signed by an intermediate)
- BaltimoreRoot CA Cert (Microsoft Presents the SBC a certificate signed by this authority)

9.3.2 SBC End Entity Certificate

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

- Common name: SBC Domain Name (**telechat.o-test06161977.com**)

To Configure the certificate record:

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

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below the navigation bar, there are icons for 'Save', 'Wizards', and 'Commands'. The left sidebar shows a tree view of objects, with 'certificate-record' selected. The main area is titled 'Modify Certificate record' and contains the following fields:

- Name: TeamsEnterpriseCert
- Country: US
- State: California
- Locality: Redwood City
- Organization: Oracle Corporation
- Unit: (empty)
- Common name: telechat.o-test06161977.com
- Key size: 2048
- Alternate name: (empty)
- Trusted:
- Key usage list: digitalSignature, keyEncipherment

At the bottom of the 'Key usage list' section, there are 'Add', 'Edit', and 'Delete' buttons. Below this, there is an 'Extended key usage list' section with 'serverAuth' and 'ClientAuth' listed, and 'Add', 'Edit', and 'Delete' buttons.

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

9.3.3 Root CA and Intermediate Certificates

9.3.3.1 Digicert Root and Intermediate Certificates:

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

9.3.3.2 Baltimore Root:

The DNS name of the Microsoft Teams Direct Routing interface is sip.pstnhub.microsoft.com. Microsoft presents a certificate to the SBC which is signed by Baltimore Cyber Baltimore CyberTrust Root. To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate.

You can download this certificate here: <https://cacert.omniroot.com/bc2025.pem>

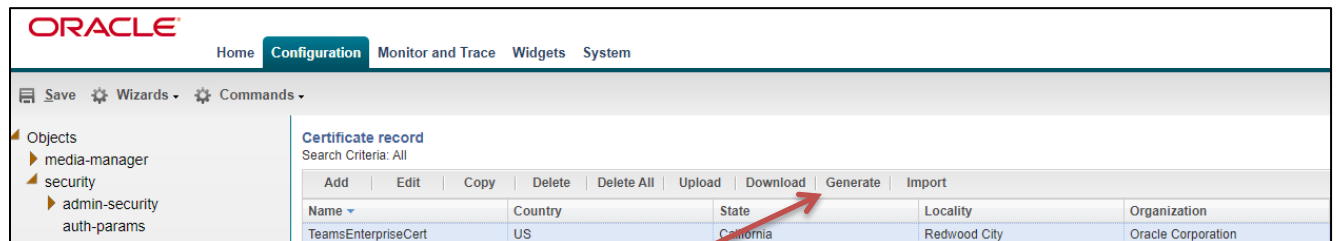
Please use the following table as a configuration reference: Modify the table according to the certificates needed for your SBC.

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

9.3.3.3 Generate Certificate Signing Request

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

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

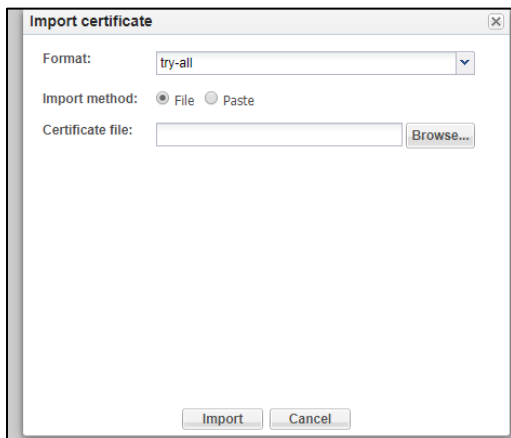
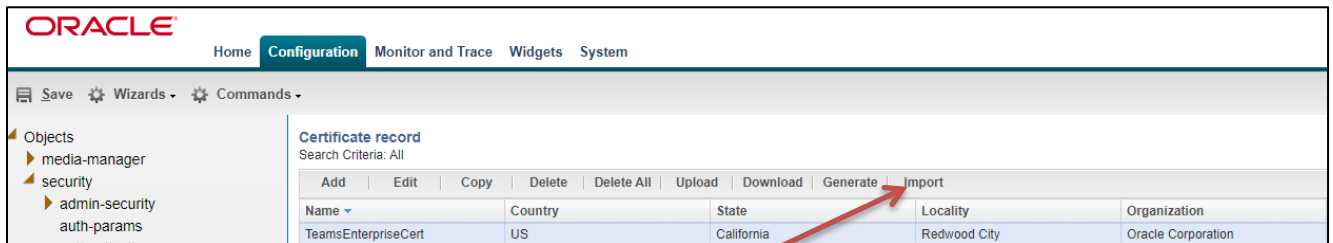




- copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.
- Also note, at this point, **a save and activate is required** before you can import the certificates to each certificate record created above.

9.3.4 Import Certificates to SBC

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



Repeat these steps to import all the root and intermediate CA certificates into the SBC:

- BaltimoreRoot
- DigiCertInter
- DigiCertRoot

At this stage, all required certificates have been imported

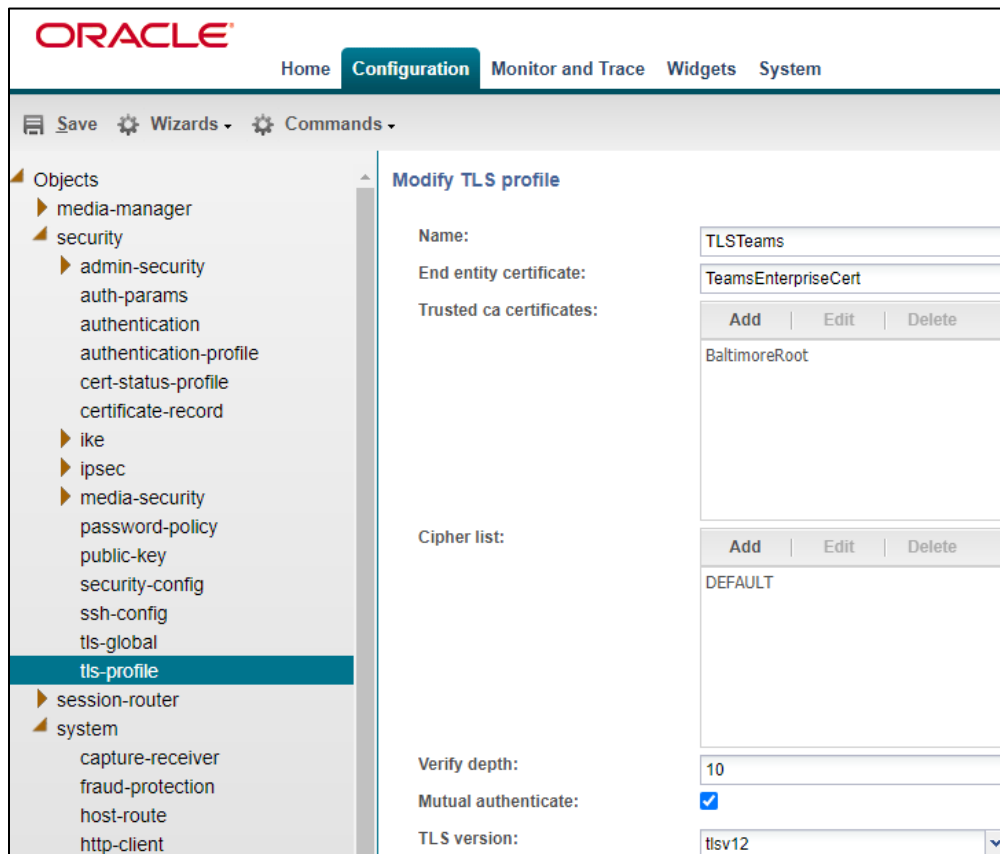
9.3.5 TLS Profile

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

GUI Path: security/tls-profile

ACL Path: config t→security→tls-profile

- Click Add, use the example below to configure



The screenshot displays the Oracle SBC GUI for configuring a TLS profile. The interface includes a top navigation bar with 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this is a toolbar with 'Save', 'Wizards', and 'Commands'. A left-hand navigation pane shows a tree structure of objects, with 'tls-profile' under the 'security' folder highlighted. The main content area is titled 'Modify TLS profile' and contains the following configuration fields:

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

- Click OK at the bottom

9.3.6 Media Security Configuration

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

9.3.7 Sdes-profile

This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured. The only crypto-suite option supported by Microsoft is AES_CM_128_HMAC_SHA1_80 and must be included in the crypto list

GUI Path: security/media-security/sdes-profile

ACL Path: config t→security→media-security→sdes-profile

- Click Add, and use the example below to configure

The screenshot displays the Oracle configuration interface for the 'Modify Sdes profile' page. The interface includes a navigation tree on the left with 'sdes-profile' selected. The main area contains the following configuration fields:

- Name: SDES
- Crypto list: AES_CM_128_HMAC_SHA1_32, AES_CM_128_HMAC_SHA1_80
- Srtp auth:
- Srtp encrypt:
- SrTCP encrypt:
- Mki:
- Egress offer format: same-as-ingress
- Use ingress session params: (empty)
- Options: (empty)
- Key: (empty)
- Salt: (empty)
- Srtp rekey on re invite:
- Lifetime: 31 (Range: 0, 20..48)

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

- Click OK at the bottom

9.3.8 Media Security Policy

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

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

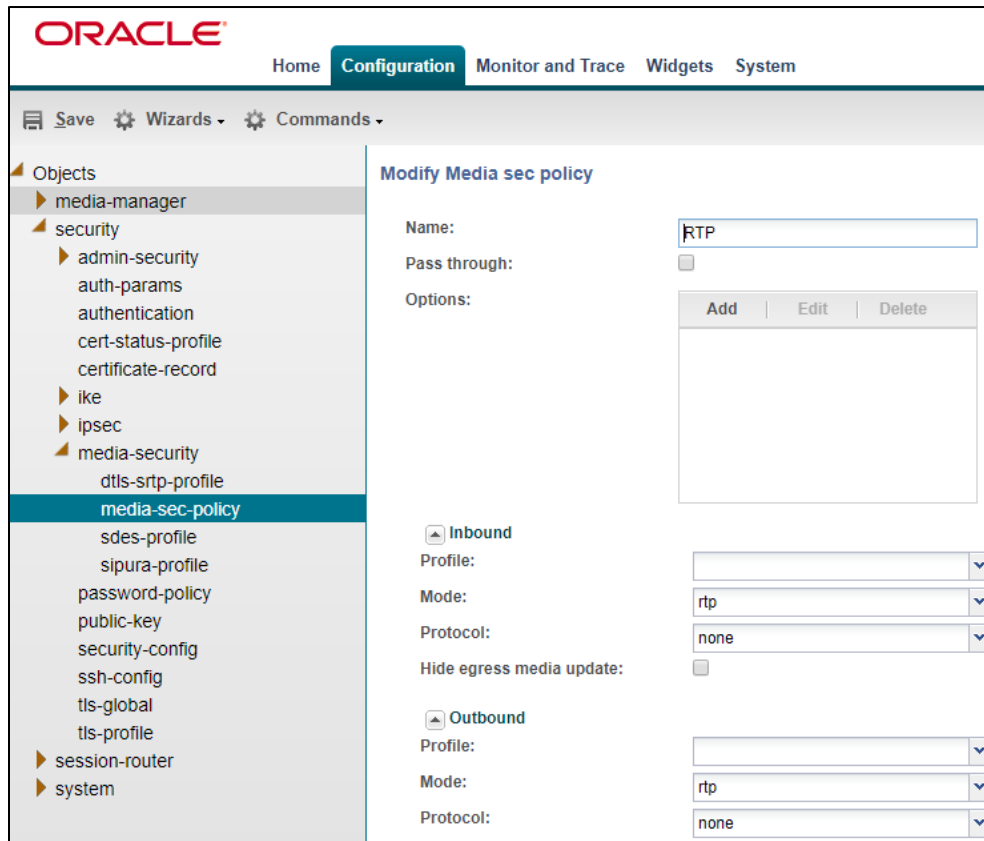
GUI Path: security/media-security/media-sec-policy

ACL Path: config t→security→media-security→media-sec-policy

- Click Add, use the examples below to configure

The screenshot displays the Oracle SBC configuration interface. At the top, there are navigation tabs: Home, Configuration (selected), Monitor and Trace, Widgets, and System. Below the tabs is a toolbar with Save, Wizards, and Commands. The left sidebar shows a tree view of objects, with 'media-sec-policy' selected under 'media-security'. The main content area is titled 'Modify Media sec policy' and contains the following fields:

- Name:** sdesPolicy
- Pass through:**
- Options:** Add | Edit | Delete
- Inbound:**
 - Profile:** SDES
 - Mode:** srtp
 - Protocol:** sdes
 - Hide egress media update:**
- Outbound:**
 - Profile:** SDES
 - Mode:** srtp
 - Protocol:** sdes



- Click OK at the bottom of each when applicable

9.3.9 IKE/IPSEC Config

The configuration elements required for IKE are not available via the Oracle ESBC GUI, and must be configured via ACLI.

Note: The examples provided will only display the parameters of each element that have been changed. All others can be left at default values unless required to be changed for your specific purposes:

9.3.10 IKE Config

ACLI Path: config t→security→ike→ike-config

Type Select, and use the below example to configure the global Ike configuration on the SBC.

```

ike-config
  ike-version          1
  log-level            NOTICE
  phase1-dh-mode      dh-group2
  phase2-exchange-mode dh-group2

```

9.3.11 Ike Interface

ACL Path: config t→security→ike→ike-interface

```
ike-interface
  ike-version          1
  address              155.212.214.101
  realm-id             Verizon
  ike-mode             initiator
  shared-password      *****
  sd-authentication-method  shared-password
```

9.3.12 Ike Sainfo

ACL Path: config t→security→ike→ike-sainfo

```
ike-sainfo
  name                 VZ1
  auth-algo            md5
  encryption-algo      3des
  tunnel-local-addr    155.212.214.101
  tunnel-remote-addr  152.188.29.84
ike-sainfo
  name                 VZ2
  auth-algo            md5
  encryption-algo      3des
  tunnel-local-addr    155.212.214.101
  tunnel-remote-addr  152.188.28.212
```

9.3.13 Security Policy

Security Policies are part of the IPSEC configuration on the SBC, and this is available through the GUI.

GUI Path: security/ipsec/security policy

ACL Path: config t→security→ipsec→security-policy

Use the below table as an example to configure security policies on the SBC toward Verizon Business:

Function	IPSEC	SIP	IPSEC	SIP
Name	Verizon-Security-Policy-1	Verizon-Security-Policy-1A	Verizon-Security-Policy-2	Verizon-Security-Policy-2A
Network-Interface	S1p0:0	S1p0:0	S1p0:0	S1p0:0
Priority	0	1	2	3
Local IP addr match	155.212.214.101	155.212.214.101	155.212.214.101	155.212.214.101
Remote ip addr match	<Vz-IPSEC-IP>	<VZ-SIP-IP>	<VZ-IPSEC-IP>	<VZ-Sip-IP>
Local port match	500	0	500	0
Remote port match	500	0	500	0
Local IP Mask	255.255.255.0	255.255.255.255	255.255.255.0	255.255.255.255
Remote IP mask	255.255.255.224	255.255.255.255	255.255.255.224	255.255.255.255
Ike-sainfo-name		VZ1		VZ2

Action	Allow	IPSEC	Allow	IPSEC
Outbound-sa-fine-grained-mask				
Local ip mask	255.255.255.255	255.255.255.0	255.255.255.255	255.255.255.0
Remote ip mask	255.255.255.255	255.255.255.224	255.255.255.255	255.255.255.224

Name	Network interface	Priority	Local IP addr match	Remote IP addr match	Local port match	Local port match max
Verizon-Security-Policy-1	M00.0	0	155.212.214.101	152.188.29.84	500	65535
Verizon-Security-Policy-1A	M00.0	1	155.212.214.101	152.188.29.19	0	65535
Verizon-Security-Policy-2	M00.0	2	155.212.214.101	152.188.28.212	500	65535
Verizon-Security-Policy-2A	M00.0	3	155.212.214.101	152.188.28.147	0	65535

9.4 Transcoding Configuration

Transcoding is the ability to convert between media streams that are based upon disparate codecs. The OCSBC supports IP-to-IP transcoding for SIP sessions, and can connect two voice streams that use different coding algorithms with one another.

9.4.1 Media Profiles

For different codecs and media types, you can setup customized media profiles that serve to police media values and define media bandwidth policies.

SILK & CN offered by Microsoft teams are using a payload type which is different usual, so to support this, we configure media profiles on the SBC.

GUI Path: session-router/media-profile

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

Configure three media profiles to support the following:

- Silk Wideband
- Silk Narrowband
- CN
- Click Add, then use the table below as an example to configure each:

Parameters	Silk-1	Silk-2	CN
Subname	narrowband	wideband	wideband
Payload-Type	103	104	118
Clock-rate	8000	16000	0

Name	Subname	Media type	Payload type	Transport	Clock rate
CN	wideband	audio	118	RTP/AVP	0
SILK	narrowband	audio	103	RTP/AVP	8000
SILK	wideband	audio	104	RTP/AVP	18000

- Click OK at the bottom of each when applicable

9.4.2 Codec Policies

Codec policies are sets of rules that specify the manipulations to be performed on SDP offers allowing the OCSBC the ability to add, strip, and reorder codecs for SIP sessions

Note: This is an optional configuration. Only configure codec policies if deemed necessary in your environment

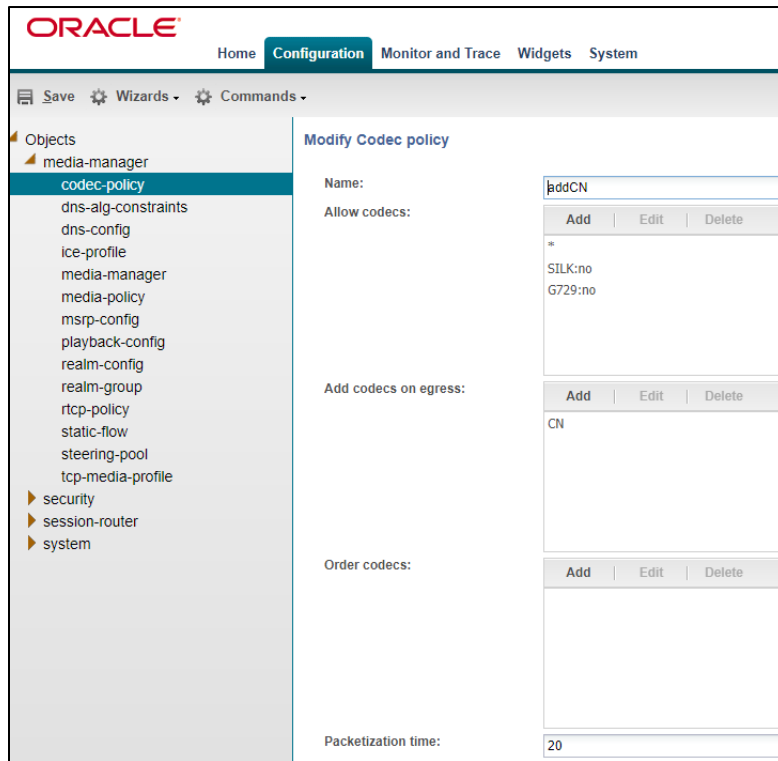
GUI Path: media-manager/codec-policy

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

Some SIP trunks may have issues with codec being offered by Microsoft teams, specifically Verizon requested the SBC try to offer only one codec when possible. For this reason, we have created a codec policy “OptimizeCodecs” for the Verizon SIP trunk to remove the codecs that are not required or supported.

Create another codec-policy, addCN, to allow the SBC to generate Comfort Noise packets towards Teams

- Click Add, and use the examples below to configure



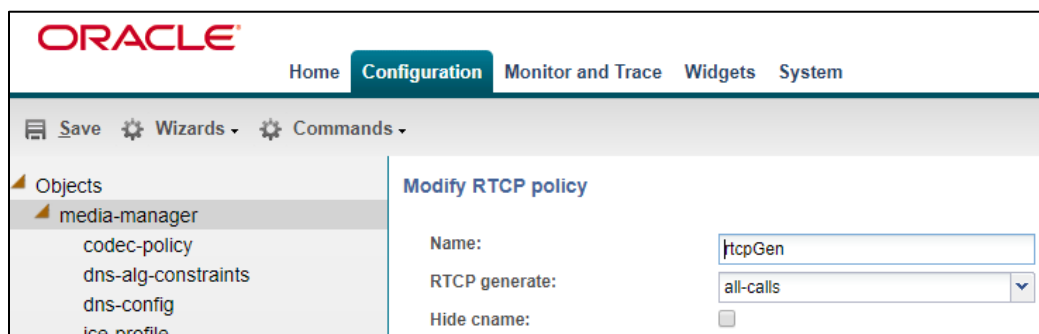
9.4.3 RTCP Policy

The following RTCP policy needs to be configured for the OCSBC to generate RTCP sender reports toward Microsoft Teams. The [media manger](#) options config, xcode-gratuitous-rtcp-report-generation, allows the SBC to generate receiver reports

GUI Path: media-manager/rtcp-policy

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

- Click Add, use the example below as a configuration guide



- Click OK at the bottom

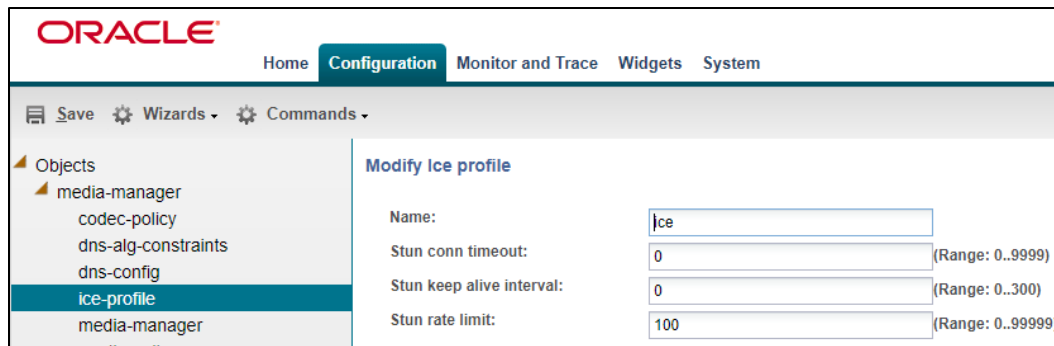
9.4.4 Ice Profile

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

GUI Path: media-manager/ice-profile

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

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



The screenshot shows the Oracle SBC GUI with the 'Configuration' tab selected. The left sidebar shows a tree view of objects, with 'ice-profile' selected under 'media-manager'. The main area is titled 'Modify Ice profile' and contains the following fields:

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

- Click OK

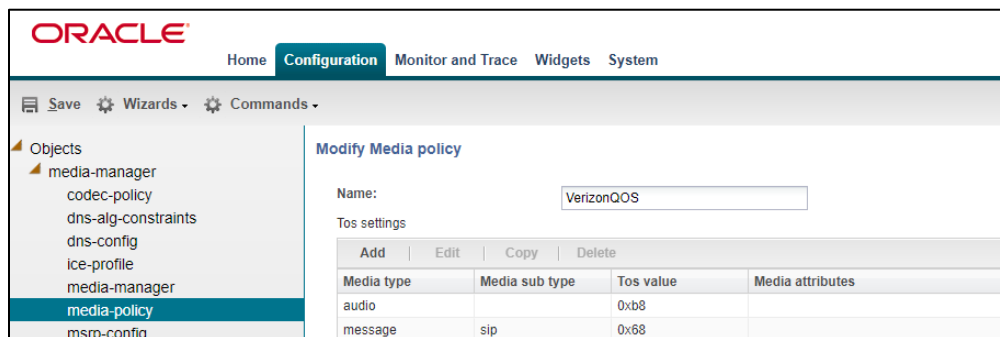
Note: Ice Profile should not be configured for Non Media Bypass Environment with Microsoft Teams

9.4.5 QOS Marking

QoS marking allows you to apply a set of TOS/DiffServ mechanisms that enable you to provide better service for selected networks

GUI Path: media manager/media policy

ACL Path: config t→media-manager→media-policy



The screenshot shows the Oracle SBC GUI with the 'Configuration' tab selected. The left sidebar shows a tree view of objects, with 'media-policy' selected under 'media-manager'. The main area is titled 'Modify Media policy' and contains the following fields:

Name:

Tos settings

Add Edit Copy Delete			
Media type	Media sub type	Tos value	Media attributes
audio		0xb8	
message	sip	0x68	

9.5 Media Configuration

This section will guide you through the configuration of realms and steering pools, both of which are required for the SBC to handle signaling and media flows toward Teams and PSTN.

9.5.1 Realm Config

In this example, we will configure a realm facing Microsoft Teams and a realm for Verizon Sip Trunk

GUI Path; media-manger/realm-config

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

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

Config Parameter	Teams Realm	PSTN
Identifier	Teams	Verizon
Network Interface	s0p0:0	s1p0:0
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Teams-FQDN	Telechat.o-test06161977.com	
Teams fqdn in uri	<input checked="" type="checkbox"/>	
Sdp inactive only	<input checked="" type="checkbox"/>	
Media Sec policy	sdespolicy	RTP
RTCP mux	<input checked="" type="checkbox"/>	
ice profile	ice	
Codec policy	addCN	OptimizeCodecs
RTCP policy	rtcpGen	
Access Control Trust Level	High	High
Pai-strip	enabled	
Media-policy		VerizonQOS

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

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

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

The screenshot shows the Oracle Configuration Assistant interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. On the left, there is a tree view under 'Objects' with 'media-manager' selected. The main area displays 'Realm config' with a search criteria of 'All'. Below this is a table with columns: Identifier, Description, Addr prefix, and Network interfaces. The table contains two rows: 'Verizon' and 'Teams'.

Identifier	Description	Addr prefix	Network interfaces
Verizon		0.0.0.0	s1p0:0
Teams	Realm Facing Teams Direct Rou...	0.0.0.0	s0p0:0

9.5.2 Steering Pools

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

We configure one steering pool for Verizon and the other for Teams

GUI Path: media-manger/steering-pool

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

- Click Add, and use the below examples to configure

The screenshot shows the 'Modify Steering pool' form in the Oracle Configuration Assistant. The 'IP address' field is set to '155.212.214.101', 'Start port' is '10000', 'End port' is '10999', and 'Realm ID' is set to 'Verizon'.

The screenshot shows the 'Modify Steering pool' form in the Oracle Configuration Assistant. The 'IP address' field is set to '141.146.36.68', 'Start port' is '20000', 'End port' is '40000', and 'Realm ID' is set to 'Teams'.

9.6 Sip Configuration

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

9.6.1 SIP Profile

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

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

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

9.6.2 Sip Feature

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

GUI Path: session-router/sip-feature

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

9.6.3 Sip Manipulation

Sip Manipulations give the SBC the capability to add, remove or modify any information contained within a sip message.

In this example, we'll be using sip manipulations to clean up and remove unwanted sdp attributes inserted by Microsoft Teams, and to format the Sip Invite being sent to Verizon is properly as per Verizon requirements. (Please see [Invite syntax](#) example below:)

GUI Path: session router/sip manipulation

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

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. Below the navigation bar, there are 'Save', 'Wizards', and 'Commands' options. The left sidebar lists various configuration categories, with 'sip-manipulation' selected. The main area displays the 'Modify SIP manipulation' page. It includes fields for 'Name' (ToVerizon), 'Description', 'Split headers', and 'Join headers'. Below these are 'CfgRules' with a table listing existing rules.

Name	Element type
RemoveXAttribute	mime-sdp-rule
AcmeTOFROMNat	header-rule

Mime-sdp-rule:

ORACLE
Home Configuration Monitor and Trace Widgets System

Save Wizards Commands

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

Modify SIP manipulation / mime SDP rule

Name: RemoveXAttribute

Msg type: request

Methods: Add Edit Delete
Invite

Action: manipulate

Comparison type: case-sensitive

Match value:

New value:

CfgRules

Name	Element type
RemoveX	sdp-media-rule

Sdp-media-rule:

ORACLE
Home Configuration Monitor and Trace Widgets System

Save Wizards Commands

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

Modify SIP manipulation / mime SDP rule / SDP media rule

Name: RemoveX

Media type: audio

Action: manipulate

Comparison type: case-sensitive

Match value:

New value:

CfgRules

Name	Element type
RemoveA	sdp-line-rule

Sdp-line-rule:

The screenshot shows the Oracle Configuration Manager 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 icons for 'Save', 'Wizards', and 'Commands'. A left-hand menu lists various configuration categories, with 'home-subscriber-server' selected. The main area is titled 'Modify SIP manipulation / mime SDP rule / SDP media rule / SDP line'. The configuration fields are as follows:

Name:	RemoveA
Type:	a
Action:	delete
Comparison type:	pattern-rule
Match value:	x-candidate-info
New value:	

Header Rule:

The screenshot shows the Oracle Configuration Manager 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 icons for 'Save', 'Wizards', and 'Commands'. A left-hand menu lists various configuration categories, with 'home-subscriber-server' selected. The main area is titled 'Modify SIP manipulation / header rule'. The configuration fields are as follows:

Name:	AcmeTOFROMNat
Header name:	From
Action:	sip-manip
Comparison type:	case-sensitive
Msg type:	request
Methods:	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Match value:	
New value:	ACME_NAT_TO_FROM_IP

9.6.4 Sip Interface

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

Configure two sip interfaces, one associated with Verizon Realm, the other for Microsoft Teams direct routing.

GUI Path: session-router/sip-interface

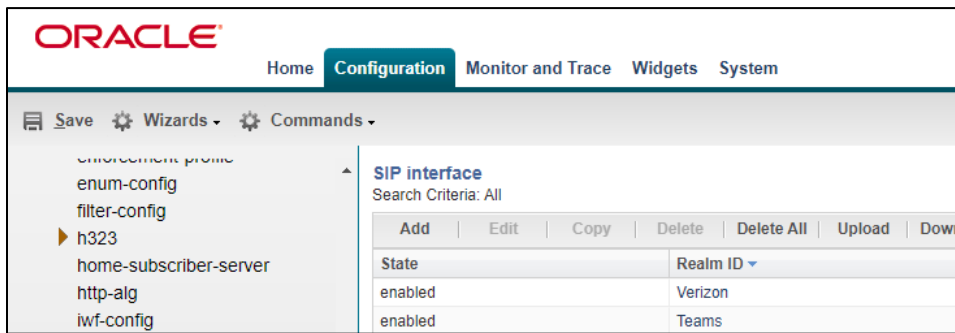
ACL Path: config t→session-router→sip-interface

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

Config Parameter	SipTrunk	Teams
Realm ID	SipTrunk	Teams
Sip Profile		forreplace
Sip Port Config Parameter	Sip Trunk	Teams
Address	155.212.214.101	141.146.36.68
Port	5060	5061
Transport protocol	UDP	TLS
TLS profile		TLSTeams
Allow anonymous	agents-only	agents-only
Out-manipulationid	ToVerizon	

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

- Sip-Profile
- TLS Profile
- Sip Manipulation



9.6.5 Session Agents

Session Agents are configuration elements which are trusted agents that can both send and receive traffic from the OCSBC with direct access to the trusted data path.

GUI Path: session-router/session-agent

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

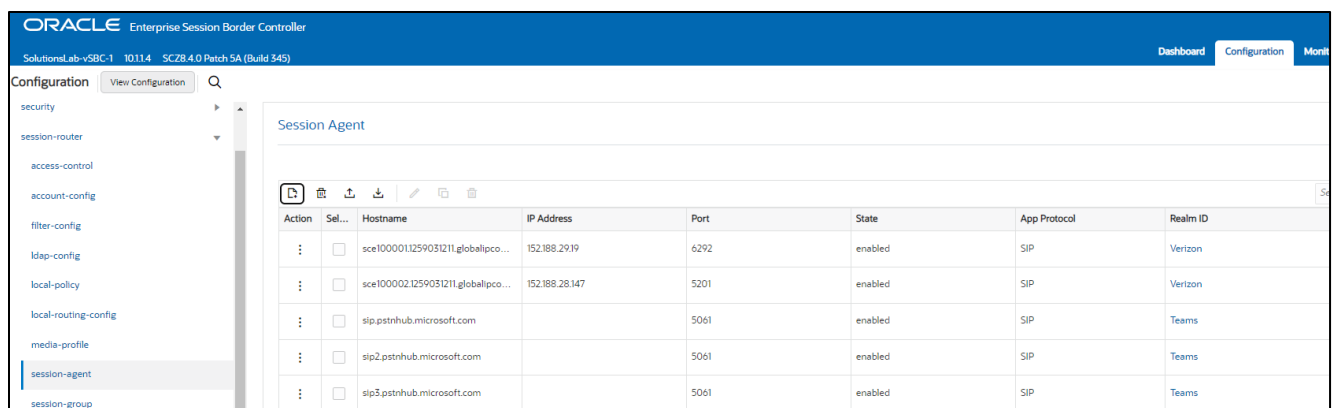
You will need to configure three Session Agents for the Microsoft Direct Routing Interface

- Click Add, and use the table below to configure:

Config parameter	Session Agent 1	Session Agent 2	Session Agent 3
Hostname	sip.pstnhub.microsoft.com	sip2.pstnhub.microsoft.com	sip3.pstnhub.microsoft.com
Port	5061	5061	5061
Transport method	StaticTLS	StaticTLS	StaticTLS
Realm ID	Teams	Teams	Teams
Ping Method	OPTIONS	OPTIONS	OPTIONS
Ping Interval	30	30	30
Refer Call Transfer	enabled	enabled	enabled
Ping Response	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- And two additional Session Agents for Verizon Sip Trunk

Config parameter	Verizon One	Verizon Two
Hostname	<Verizon FQDN-1>	<Verizon FQDN-2>
IP-Address	<IPV4 Address>	<IPV4 Address>
Port	5201	6292
Transport method	UDP	UDP
Realm ID	Verizon	Verizon
Ping Method	OPTIONS	OPTIONS
Ping Interval	30	30
Refer Call Transfer	enabled	enabled
Ping Response	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



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

9.6.6 Session Agent Group

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

All three Teams session agents configured above will be added to the group as well as both session agents configured for Verizon Business

GUI Path: session-router/session-group

ACL Path: config t→session-router→session-group

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

ORACLE

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands

enforcement-profile
enum-config
filter-config
h323
home-subscriber-server
http-alg
iwf-config
ldap-config
local-policy
local-response-map
local-routing-config
media-profile
net-management-control
qos-constraints
response-map
service-health
session-agent
session-agent-id-rule
session-constraints

Modify Session group

Group name: TeamsGrp

Description:

State:

App protocol: SIP

Strategy: Hunt

Dest:

Add Edit Delete

sip.pstnhub.microsoft.com
sip2.pstnhub.microsoft.com
sip3.pstnhub.microsoft.com

ORACLE

Home **Configuration** Monitor and Trace Widgets System

Save Wizards Commands

via-rtcp-manipulation
enforcement-profile
enum-config
filter-config
h323
home-subscriber-server
http-alg
iwf-config
ldap-config
local-policy
local-response-map
local-routing-config
media-profile
net-management-control

Modify Session group

Group name: VerizonGrp

Description:

State:

App protocol: SIP

Strategy: Hunt

Dest:

Add Edit Delete

sce10001.1259031211.globalipcom.com
sce10002.1259031211.globalipcom.com

- Click OK at the bottom

9.7 Routing Configuration

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

The OCSBC has multiple routing options that can be configured based on environment. For the purposes of this example, we utilize Local Policy to route all sip traffic.

9.7.1 Local Policy Configuration

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

GUI Path: session-router/local-policy

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

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

The following local policy routes calls from Verizon to Microsoft Teams:

The screenshot shows the Oracle configuration interface for 'Modify Local policy'. The left sidebar lists various configuration categories, with 'local-policy' selected. The main configuration area includes the following fields and controls:

- To address:** A text input field with an 'Add' button above it. The field contains an asterisk (*).
- Source realm:** A text input field with an 'Add' button above it. The field contains 'Verizon'.
- Description:** A text input field.
- State:** A checkbox that is checked.
- Policy priority:** A dropdown menu set to 'none'.
- Policy attributes:** A table with columns for 'Next hop', 'Realm', 'Action', and 'Terminat'.

Next hop	Realm	Action	Terminat
sag.TeamsGrp	Teams	none	disabled

The Following Routes Calls from Microsoft Teams to Verizon Sip Trunk.

The screenshot shows the Oracle Configuration Manager interface. The left sidebar contains a tree view of configuration objects, with 'local-policy' selected. The main area is titled 'Modify Local policy' and contains the following fields:

- To address:** A text input field with an 'Add | Edit | Delete' button above it. The field contains an asterisk (*).
- Source realm:** A text input field with an 'Add | Edit | Delete' button above it. The field contains 'Teams'.
- Description:** A text input field.
- State:** A checkbox that is checked.
- Policy priority:** A dropdown menu set to 'none'.
- Policy attributes:** A table with columns 'Next hop', 'Realm', 'Action', and 'Termination'. The table contains one row: 'sag:VerizonGrp', 'Verizon', 'none', and 'disabled'.

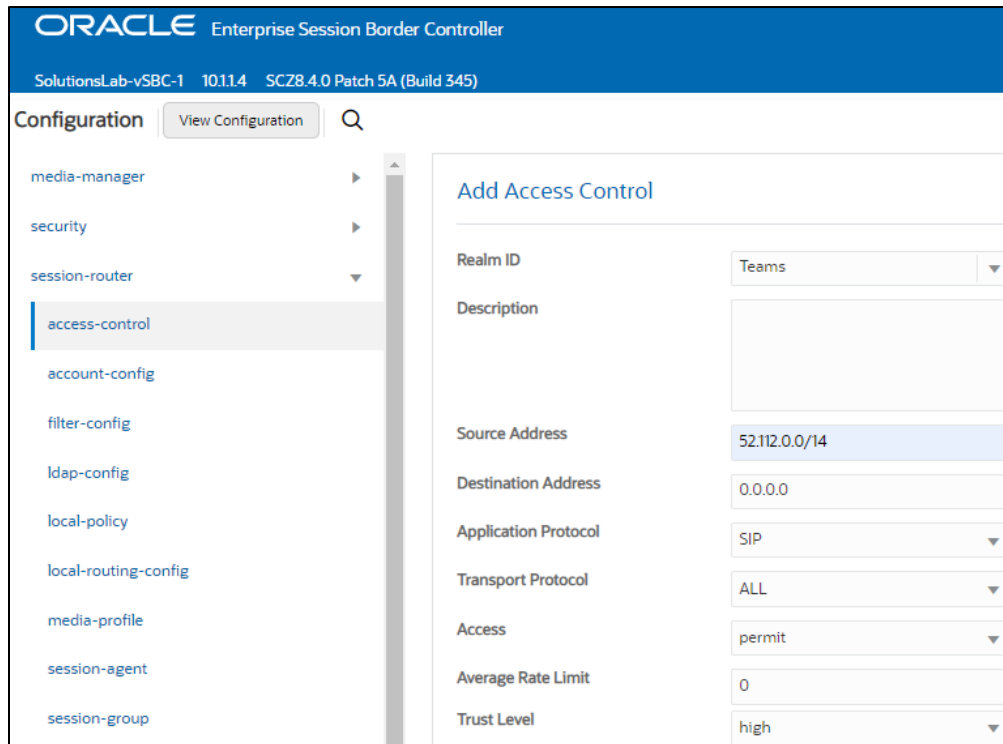
9.7.2 Access Control (Optional)

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

Microsoft recommends allowing SIP traffic from the following two networks:

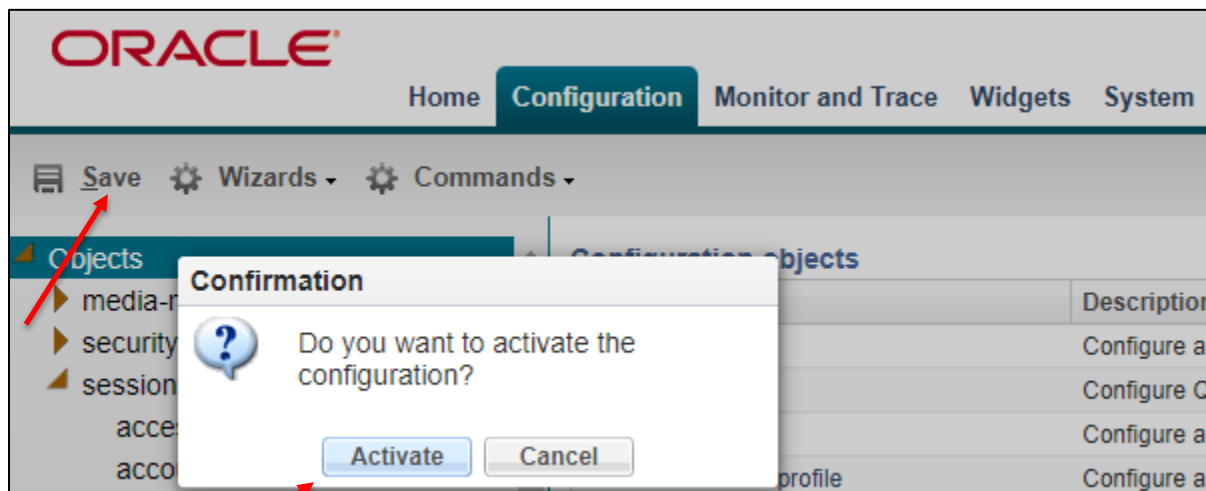
- 52.112.0.0/14
- 52.120.0.0/14

Use this example to create ACL's for both MSFT Teams networks, as well as Verizon Business IP addresses.



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

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



Move to verify the connection with Microsoft Direct Routing Interface

10 Verify Connectivity

10.1 OCSBC Options Ping

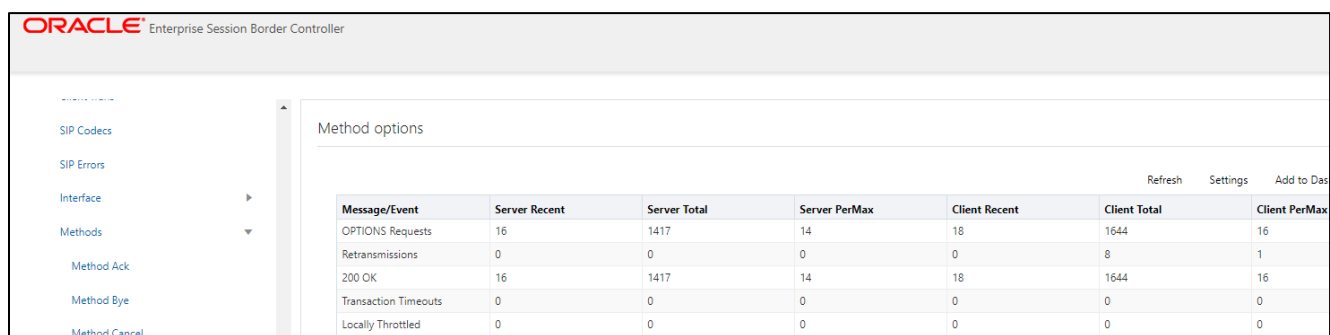
After you've paired the OCSBC with Direct Routing validate that the SBC can successfully exchange SIP Options with Microsoft Direct Routing and Verizon Business.

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

- At the top, click “Wigits”

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

GUI Path: Signaling/SIP/Methods/OPTIONS



The screenshot shows the Oracle Enterprise Session Border Controller GUI. The left sidebar contains a navigation menu with items like SIP Codecs, SIP Errors, Interface, Methods, Method Ack, Method Bye, and Method Cancel. The main content area is titled 'Method options' and contains a table with the following data:

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

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

10.2 Microsoft SIP Tester Client

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

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

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

Download the script and Documentation here:

[Sip Tester Client script and documentation](#)

11 Syntax Requirements for SIP Invite and SIP Options

Microsoft Teams Hybrid Voice Connectivity interface and Verizon Business IP Trunk have requirements for the syntax of SIP messages.

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

11.1 Terminology

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

11.2 Requirements for Invite Messages

Microsoft Teams

Picture 1 Example of INVITE message

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

Picture 2 Example of 200OK Response To Invite:

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

11.2.1 Contact.Header

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

Verizon

Picture 3 Example of Invite to Verizon IP Trunk

```
INVITE sip:+19784341227@telechat.o-test06161977.com:5061;user=phone;transport=tls SIP/2.0
Via: SIP/2.0/UDP 141.146.36.101:5060;branch=z9hG4bK5vv4871030lmclrp5uk0.1
FROM: teams user3<sip:+17813131033@141.146.36.101:5060 user=phone>;tag=19ca395b2a9
TO: <sip:+19784341227@152.188.29.19:6292 user=phone>
CSEQ: 1 INVITE
CALL-ID: 13a5f5626643579dba2687888fce1ff9
MAX-FORWARDS: 69
CONTACT: <sip:+17813131033@141.146.36.101:5060;transport=udp>
CONTENT-LENGTH: 221
USER-AGENT: Microsoft.PSTNHub.SIPProxy v.2020.9.21.1 i.USWE2.2
CONTENT-TYPE: application/sdp
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
PRIVACY: id
Route: <sip:+19784341227@sce10001.1259031211.globalipcom.com:6292;user=phone;lr>
```

11.2.2 From Header:

- Must contain a Verizon DID that is associated with the trunk group
- Must Contain the SBC local Sip Interface IP address and port

11.2.3 To Header

- Must Contain the Verizon Sip IP address or Hostname, and port

11.3 Requirements for OPTIONS Messages

Picture 4 Example of OPTIONS message (Microsoft Teams Only)

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

11.3.1 Contact Header

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

12 Microsoft Teams Direct Routing Interface characteristics

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

Category	Parameter	Value	Comments
Ports and IP	SIP Interface FQDN Name	Refer to Microsoft documentation	
	IP Addresses range for SIP interfaces	Refer to Microsoft documentation	
	SIP Port	5061	
	IP Address range for Media	Refer to Microsoft documentation	
	Media port range on Media Processors	Refer to Microsoft documentation	
	Media Port range on the client	Refer to Microsoft documentation	
Transport and Security	SIP transport	TLS	
	Media Transport	SRTP	
	SRTP Security Context	DTLS, SIPS Note: DTLS is not supported until later time. Please configure SIPS at this moment. Once support of DTLS announced it will be the recommended context	https://tools.ietf.org/html/rfc5763
	Crypto Suite	AES_CM_128_HMAC_SHA1_80, non-MKI	
	Control protocol for media transport	SRTCP (SRTCP-Mux recommended)	Using RTCP mux helps reduce number of required ports
	Supported Certification Authorities	Refer to Microsoft documentation	
	Transport for Media Bypass (of configured)	ICE-lite (RFC5245) – recommended, · Client also has Transport Relays	
Codecs	Audio codecs	<ul style="list-style-type: none"> · G711 · Silk (Teams clients) · Opus (WebRTC clients) - Only if Media Bypass is used; · G729 · G722 	
	Other codecs	<ul style="list-style-type: none"> · CN o Required narrowband and wideband · RED – Not required · DTMF – Required · Events 0-16 · Silence Suppression – Not required 	

13 Appendix A

13.1 SBC Behind NAT SPL configuration

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

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

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

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

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

HeaderNatPublicSipIpf=52.151.236.203,HeaderNatPrivateSipIpf=10.0.4.4

Here HeaderNatPublicSipIpf is the public interface ip and HeaderNatPrivateSipIpf is the private ip.

The screenshot shows the Oracle Configuration Manager 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 'Save', 'Wizards', and 'Commands' options. A left-hand navigation pane lists various configuration categories, with 'h323' selected. The main content area is titled 'Modify SIP interface' and contains several configuration fields: 'TCP nat interval' (90), 'Registration caching' (checkbox), 'Min reg expire' (300), 'Registration interval' (3600), 'Route to registrar' (checkbox), 'Secured network' (checkbox), and 'Uri fqdn domain'. Below these fields is an 'Options' table with 'Add', 'Edit', and 'Delete' buttons. At the bottom of the page, the 'Spl options' section is visible, showing the configuration 'HeaderNatPublicSipIpf=52.151.236.203'.

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

14 Caveats

14.1 No Audio-On-Hold

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

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

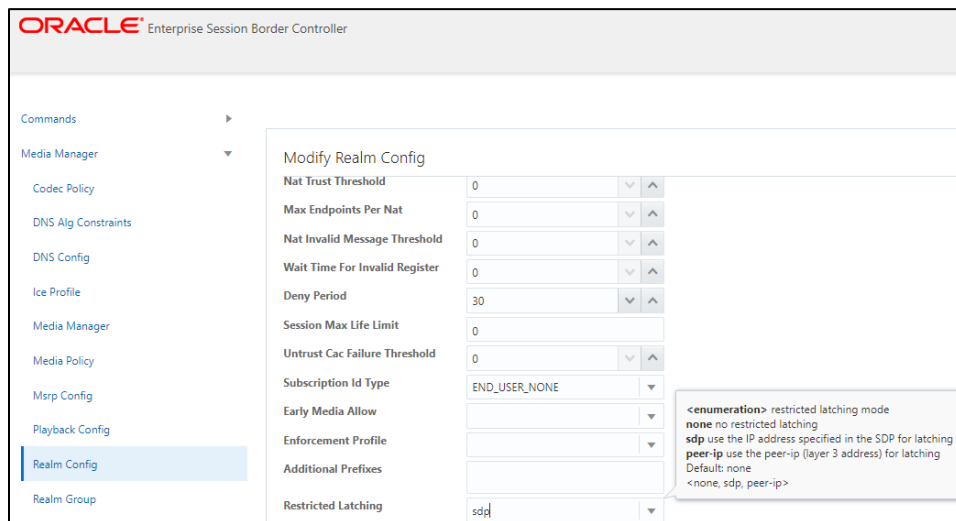
To correct this, Oracle recommends enabling Restricted Media Latching on realms configured for Microsoft Teams in the OCSBC.

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

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

GUI Path: media-manger/realm-config

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



The screenshot shows the Oracle Enterprise Session Border Controller GUI. The left sidebar contains a navigation menu with the following items: Commands, Media Manager, Codec Policy, DNS Alg Constraints, DNS Config, Ice Profile, Media Manager, Media Policy, Msrp Config, Playback Config, Realm Config (highlighted), and Realm Group. The main content area is titled 'Modify Realm Config' and contains several configuration fields with up/down arrows for adjustment:

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

A tooltip is visible next to the 'Restricted Latching' dropdown, containing the following text:

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

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

15 Call Transfers

Microsoft Teams requires the Oracle SBC to handle all call transfers initiated by a Microsoft Teams user to both users within the same tenant and users outside of that tenant.

Verizon requires a DID that is associated with the Trunk Group be presented as either the FROM user, or as part of a Diversion Header. When the SBC generates an Invite off the REFER received by Microsoft, it is not always possible to guarantee the user part of the From header in that Invite will match an associated DID with the Verizon Trunk Group. If there is no match, Verizon will not allow that leg of the transfer to complete successfully.

In order to accommodate these requirement as well as maintain the proper [header syntax](#) and security requirements of the Verizon IP Trunk, we'll need to add additional header rules to the already existing [sip manipulation](#) configured above, labeled ToVerizon.

We will create a Diversion Header that contains a location specific screening telephone number, or STN to the transferred call leg. Using this method, the original caller id would be retained and seen as ANI at the far end. Also, similar to the way Verizon's Alternate Caller ID functions in the Verizon Network, when an actual STN is carried in the Diversion Header, that header will be stripped off as the call passes through their Broad Works servers so the call does not continue to be treated as a diverted call, while at the same time, satisfying the security requirements on the trunk.

The below Sip Manipulation Headers rules will first check for a Referred-By Header, indicating the Invite is part of a transfer. If there is a match, we'll create and add a diversion header to the Invite the Oracle SBC sends to Verizon. That Diversion Header will contain a STN, as outlined above.

15.1 Store Referred-By Header

15.1.1 Header Rule:

The screenshot displays the Oracle SBC Configuration 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 options for 'Save', 'Wizards', and 'Commands'. A left-hand sidebar lists various configuration categories, with 'h323' selected. The main content area is titled 'Modify SIP manipulation / header rule' and contains the following fields:

- Name: StoreReferredBy
- Header name: REFERRED-BY
- Action: store
- Comparison type: case-sensitive
- Msg type: request
- Methods: A table with columns 'Add', 'Edit', and 'Delete'. The 'Invite' method is listed in the table.
- Match value: (empty field)
- New value: (empty field)

15.2 Add Diversion Header

15.2.1 Header Rule:

The screenshot displays the Oracle Configuration Manager interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this, there are 'Save', 'Wizards', and 'Commands' options. A left-hand navigation pane lists various configuration categories, with 'h323' selected. The main area is titled 'Modify SIP manipulation / header rule' and contains the following fields:

- Name:** AddDiversion
- Header name:** Diversion
- Action:** add
- Comparison type:** boolean
- Msg type:** request
- Methods:** A table with buttons 'Add', 'Edit', and 'Delete', and a single entry 'Invite'.
- Match value:** \$StoreReferredBy
- New value:** < sip: \+17813131033+@+\$LOCAL_IP+>

16 Running Configuration

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

```
show running-config short
```

```
access-control
  realm-id          Verizon
  description       VerizonSIP
  source-address    152.188.0.0/16
  application-protocol SIP
  trust-level       high
access-control
  realm-id          Teams
  source-address    52.112.0.0/14
  destination-address 141.146.36.68
  application-protocol SIP
  trust-level       high
access-control
  realm-id          Teams
  source-address    52.120.0.0/14
  destination-address 141.146.36.68
  application-protocol SIP
  trust-level       high
certificate-record
  name              BaltimoreRoot
  common-name       Baltimore CyberTrust Root
certificate-record
  name              DigiCertInter
  common-name       DigiCert SHA2 Secure Server CA
certificate-record
  name              DigiCertRoot
  common-name       DigiCert Global Root CA
certificate-record
  name              GoDaddyRoot
  common-name       GoDaddy Class2 Root CA
certificate-record
  name              GoDaddyinter
  common-name       GoDaddy Secure Server CA
certificate-record
  name              TeamsCarrierCert
  state             California
  locality          Redwood City
  organization      Oracle Corporation
  common-name       customers.telechat.o-test06161977.com
  alternate-name    *.customers.telechat.o-test06161977.com
certificate-record
  name              TeamsEnterpriseCert
  state             California
  locality          Redwood City
  organization      Oracle Corporation
  common-name       telechat.o-test06161977.com
  extended-key-usage-list serverAuth
  ClientAuth
codec-policy
  name              OptimizeCodecs
  allow-codecs      PCMU Telephone-Event
  add-codecs-on-egress PCMU
```

```

codec-policy
  name          VzPolicy
  allow-codecs  PCMU PCMA G729 Telephone-Event
  add-codecs-on-egress  PCMU
codec-policy
  name          addCN
  allow-codecs  *
  add-codecs-on-egress  CN
dtls-srtp-profile
  name          TeamsDTLS
  tls-profile   TLSTeams
  crypto-suite  SRTP_AES128_CM_HMAC_SHA1_32
host-route
  dest-network  8.8.0.0
  netmask       255.255.0.0
  gateway       141.146.36.65
ice-profile
  name          ice
  stun-conn-timeout  0
  stun-keep-alive-interval  0
ike-config
  ike-version   1
  log-level     NOTICE
  phase1-dh-mode  dh-group2
  phase2-exchange-mode  dh-group2
ike-interface
  ike-version   1
  address       155.212.214.101
  realm-id      Verizon
  ike-mode      initiator
  shared-password  *****
  sd-authentication-method  shared-password
ike-sainfo
  name          VZ1
  auth-algo     md5
  encryption-algo  3des
  tunnel-local-addr  155.212.214.101
  tunnel-remote-addr  152.188.29.84
ike-sainfo
  name          VZ2
  auth-algo     md5
  encryption-algo  3des
  tunnel-local-addr  155.212.214.101
  tunnel-remote-addr  152.188.28.212
local-policy
  from-address  *
  to-address    *
  source-realm  Teams
  policy-attribute
    next-hop    sag:VerizonGrp
    realm       Verizon
local-policy
  from-address  *
  to-address    *
  source-realm  Verizon
  policy-attribute
    next-hop    sag:TeamsGrp
    realm       Teams
media-manager
media-policy
  name          VerizonQOS

```

```

tos-settings
  media-type          audio
  tos-value           0xb8
tos-settings
  media-type          message
  media-sub-type      sip
  tos-value           0x68
media-profile
  name                CN
  subname             wideband
  payload-type        118
  clock-rate          16000
media-profile
  name                SILK
  subname             narrowband
  payload-type        103
  clock-rate          8000
media-profile
  name                SILK
  subname             wideband
  payload-type        104
  clock-rate          16000
media-sec-policy
  name                RTP
media-sec-policy
  name                sdesPolicy
  inbound
    profile           SDES
    mode              srtp
    protocol          sdes
  outbound
    profile           SDES
    mode              srtp
    protocol          sdes
network-interface
  name                M00
  hostname             telechat.o-test06161977.com
  ip-address           141.146.36.68
  netmask              255.255.255.192
  gateway              141.146.36.65
  gw-heartbeat
    state             enabled
    heartbeat         10
    retry-count       3
    retry-timeout     3
  dns-ip-primary       8.8.8.8
  dns-ip-backup1      8.8.4.4
  dns-domain           customers.telechat.o-test06161977.com
  hip-ip-list          141.146.36.100
  icmp-address         141.146.36.100
network-interface
  name                M10
  ip-address           155.112.214.101
  netmask              255.255.255.0
  gateway              155.212.214.1
phy-interface
  name                M00
  operation-type       Media
phy-interface
  name                M10
  operation-type       Media

```

```

slot 1
realm-config
  identifier Teams
  description Realm Facing Teams Direct Routing
  network-interfaces M00:0.4
  mm-in-realm enabled
  qos-enable enabled
  media-sec-policy sdesPolicy
  rtcp-mux enabled
  ice-profile ice
  teams-fqdn telechat.o-test06161977.com
  teams-fqdn-in-uri enabled
  sdp-inactive-only enabled
  access-control-trust-level high
  pai-strip enabled
  codec-policy addCN
  rtcp-policy rtcpGen
realm-config
  identifier Verizon
  network-interfaces M00:0
  mm-in-realm enabled
  qos-enable enabled
  media-policy VerizonQOS
  media-sec-policy RTP
  access-control-trust-level high
  codec-policy OptimizeCodecs
rtcp-policy
  name rtcpGen
  rtcp-generate all-calls
sdes-profile
  name SDES
  crypto-list AES_CM_128_HMAC_SHA1_32
  AES_CM_128_HMAC_SHA1_80
  lifetime 31
security-policy
  name Verizon-Security-Policy-1
  network-interface M00:0
  local-ip-addr-match 155.212.214.101
  remote-ip-addr-match 152.188.29.84
  local-port-match 500
  remote-port-match 500
  local-ip-mask 255.255.255.192
  remote-ip-mask 255.255.255.224
  action allow
security-policy
  name Verizon-Security-Policy-1A
  network-interface M00:0
  priority 1
  local-ip-addr-match 155.212.214.101
  remote-ip-addr-match 152.188.29.19
  ike-sainfo-name VZ1
  outbound-sa-fine-grained-mask
    local-ip-mask 255.255.255.192
    remote-ip-mask 255.255.255.224
security-policy
  name Verizon-Security-Policy-2
  network-interface M00:0
  priority 2
  local-ip-addr-match 155.212.214.101
  remote-ip-addr-match 152.188.28.212
  local-port-match 500

```



```

remote-port-match      500
local-ip-mask          255.255.255.192
remote-ip-mask         255.255.255.224
action                 allow
security-policy
  name                  Verizon-Security-Policy-2A
  network-interface     M00:0
  priority               3
  local-ip-addr-match   155.212.214.101
  remote-ip-addr-match  152.188.28.147
  ike-sainfo-name       VZ2
  outbound-sa-fine-grained-mask
    local-ip-mask       255.255.255.192
    remote-ip-mask      255.255.255.224
session-agent
  hostname              sce10001.1259031211.globalipcom.com
  ip-address            152.188.29.19
  port                  6292
  transport-method      UDP+TCP
  realm-id              Verizon
  ping-method           OPTIONS
  ping-interval         30
  ping-response         enabled
  rfc2833-mode         preferred
  rfc2833-payload      101
session-agent
  hostname              sce10002.1259031211.globalipcom.com
  ip-address            152.188.28.147
  port                  5201
  transport-method      UDP+TCP
  realm-id              Verizon
  ping-method           OPTIONS
  ping-interval         30
  ping-response         enabled
  rfc2833-mode         preferred
  rfc2833-payload      101
session-agent
  hostname              sip.pstnhub.microsoft.com
  port                  5061
  transport-method      StaticTLS
  realm-id              Teams
  ping-method           OPTIONS
  ping-interval         30
  ping-response         enabled
  refer-call-transfer   enabled
session-agent
  hostname              sip2.pstnhub.microsoft.com
  port                  5061
  transport-method      StaticTLS
  realm-id              Teams
  ping-method           OPTIONS
  ping-interval         30
  ping-response         enabled
  refer-call-transfer   enabled
session-agent
  hostname              sip3.pstnhub.microsoft.com
  port                  5061
  transport-method      StaticTLS
  realm-id              Teams
  ping-method           OPTIONS
  ping-interval         30

```

```

ping-response          enabled
refer-call-transfer   enabled
session-group
group-name            TeamsGrp
dest                  sip.pstnhub.microsoft.com
                     sip2.pstnhub.microsoft.com
                     sip3.pstnhub.microsoft.com
sag-recursion         enabled
stop-sag-recurse     401,407,480
session-group
group-name            VerizonGrp
strategy              RoundRobin
dest                  sce10001.1259031211.globalipcom.com
                     sce10002.1259031211.globalipcom.com
sag-recursion         enabled
session-timer-profile
name                  ToTeams
force-reinvite        enabled
request-refresher     uas
sip-config
home-realm-id         Teams
registrar-domain      *
registrar-host        *
registrar-port        5060
options                inmanip-before-validate
                     max-udp-length=0
sip-message-len       0
extra-method-stats    enabled
sip-feature
name                  replaces
realm                 Teams
require-mode-inbound  Pass
require-mode-outbound Pass
sip-interface
realm-id              Teams
sip-port
address                141.146.36.68
port                   5061
transport-protocol    TLS
tls-profile            TLSTeams
allow-anonymous        agents-only
options                100rel-interworking
sip-profile            forreplaces
session-timer-profile ToTeams
sip-interface
realm-id              Verizon
sip-port
address                155.212.214.101
allow-anonymous        agents-only
out-manipulationid    ToVerizon
diversion-info-mapping-mode hist2div
sip-manipulation
name                  ToVerizon
mime-sdp-rule
name                  RemoveXAttribute
msg-type              request
methods               Invite
action                manipulate
sdp-media-rule
name                  RemoveX
media-type             audio

```

```

        action                manipulate
        sdp-line-rule
        name                  RemoveA
        type                  a
        action                delete
        comparison-type       pattern-rule
        match-value           x-candidate-info
header-rule
  name                      AcmeTOFROMNat
  header-name               From
  action                    sip-manip
  msg-type                  request
  methods                   INVITE
  new-value                  ACME_NAT_TO_FROM_IP
header-rule
  name                      StoreReferredBy
  header-name               REFERRED-BY
  action                    store
  msg-type                  request
  methods                   Invite
header-rule
  name                      AddDiversion
  header-name               Diversion
  action                    add
  comparison-type           boolean
  msg-type                  request
  methods                   Invite
  match-value               $StoreReferredBy
  new-value                  <sip:\+17813131033+@+$LOCAL_IP+>
sip-monitoring
  match-any-filter          enabled
  monitoring-filters        *
sip-profile
  name                      forreplaces
  replace-dialogs          enabled
steering-pool
  ip-address                155.212.214.101
  start-port                10000
  end-port                  10999
  realm-id                  Verizon
steering-pool
  ip-address                141.146.36.68
  start-port                20000
  end-port                  40000
  realm-id                  Teams
system-config
  hostname                  telechat.o-test06161977.com
  description               SBC for Verizon IP Trunking and Microsoft Teams
  location                  Burlington, MA
  system-log-level          NOTICE
  default-gateway           10.138.194.129
  source-routing            enabled
  snmp-agent-mode           v1v2
tls-global
  session-caching           enabled
tls-profile
  name                      TLSTeams
  end-entity-certificate    TeamsEnterpriseCert
  trusted-ca-certificates   BaltimoreRoot
                           GoDaddyRoot
                           GoDaddyinter

```

```
mutual-authenticate      enabled
tls-profile
name                     TLSTeamsCarrier
end-entity-certificate   TeamsCarrierCert
trusted-ca-certificates  BaltimoreRoot
                          GoDaddyRoot
                          GoDaddyinter
mutual-authenticate      enabled
web-server-config
```



CONNECT WITH US

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

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

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

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