



ORACLE

Oracle SBC with Microsoft Teams Direct Routing

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	6
2	INTENDED AUDIENCE	6
3	VALIDATED ORACLE SOFTWARE VERSIONS	6
4	RELATED DOCUMENTATION.....	7
4.1	Oracle SBC	7
4.2	Microsoft Teams	7
5	ABOUT TEAMS DIRECT ROUTING.....	7
5.1	Planning Direct Routing	7
5.2	Media Bypass vs Non Media Bypass	8
5.3	Infrastructure Requirements	8
5.4	DNS Requirements.....	8
5.4.1	SBC Domain Names.....	9
5.4.2	Adding the SBC Domain to Microsoft O365.....	9
5.4.3	Creating a User in Microsoft O365.....	11
5.5	Connect the SBC to the Teams tenant.	13
5.5.1	Teams Admin Center Configuration.....	13
5.5.2	Connect the Oracle SBC.....	13
5.5.3	Configuring User Online Voice Settings.....	15
5.5.4	Configure Voice Routing for Direct Routing	16
6	ORACLE SBC CONFIGURATION.....	21
6.1	System-Config.....	23
6.1.1	NTP-Sync	23
6.2	Network Configuration	24
6.2.1	Physical Interfaces.....	24
6.2.2	Network Interfaces.....	25
6.3	Security Configuration	25
6.3.1	Certificate Records	25
6.3.2	TLS Profile	31
6.3.3	Media Security	32
6.4	Transcoding Configuration.....	35
6.4.1	Media Profiles	35
6.4.2	Codec Policies	36
6.4.3	RTCP Policy	37
6.4.4	ICE Profile.....	38
6.5	Media Configuration.....	39
6.5.1	Media Manager.....	39
6.5.2	Realm Config	40
6.5.3	Steering Pools	41
6.6	Sip Configuration	42
6.6.1	Sip-Config.....	42
6.6.2	Replaces Header Support.....	43
6.6.3	Sip Manipulation	45
6.6.4	Sip Interface.....	47

6.6.5	Session Agents.....	47
6.6.6	Session Group.....	48
6.7	Routing Configuration.....	49
6.8	SIP Access Controls.....	52
7	ORACLE SBC CONFIGURATION ASSISTANT.....	54
7.1	Microsoft Teams Configuration Assistant.....	54
8	VERIFY CONNECTIVITY.....	58
8.1	Oracle SBC Options Pings.....	58
8.2	Microsoft SIP tester Client.....	58
9	SYNTAX REQUIREMENTS FOR SIP INVITE AND SIP OPTIONS:.....	59
9.1	Terminology.....	59
9.2	Requirements for Invite Messages and Final Responses.....	59
9.2.1	Contact Header-Invite and Final Response.....	59
9.3	Requirements for OPTIONS Messages.....	60
9.3.1	Contact Header-OPTIONS:.....	60
10	MICROSOFT TEAMS DIRECT ROUTING INTERFACE CHARACTERISTICS.....	60
11	APPENDIX A.....	62
11.1	Oracle SBC TDM with Teams.....	62
11.1.1	Interface Requirements.....	62
12	APPENDIX B.....	62
12.1	Oracle SBC deployed behind NAT.....	62
13	APPENDIX C.....	64
13.1	Ringback on Inbound Calls to Teams and Early Media.....	64
13.2	Oracle SBC Local Media Playback.....	66
13.2.1	Ringback on Transfer.....	66
14	APPENDIX D.....	68
14.1	Configuration for Emergency Calling.....	68
14.1.1	E911.....	68
14.1.2	Emergency Session Handling.....	68
14.2	Elin Gateway.....	72
14.2.1	Sip-Manipulation for Teams ELIN.....	73
15	APPENDIX E.....	75
15.1	Configuring IPv6 Support for Teams Direct Routing with Oracle SBC.....	75
15.2	Configuring Teams Direct Routing for IPv6.....	75
15.3	Configuring the Oracle SBC for IPv6 Support.....	77
15.3.1	Network Interface.....	77
15.3.2	Steering Pool.....	78
15.3.3	Sip Interface.....	78
16	ACLI RUNNING CONFIGURATION.....	80



This Page is left Intentionally Blank

1 Revision History

Document Version	Description	Revision Date
1.1	<ul style="list-style-type: none">Document Based on 9.0 ReleaseRemoved sip manipulations for TeamsAdded Config Assistant Section	11-16-2021
1.2	<ul style="list-style-type: none">Removed Session Translation for E911Removed sip-all fqdnAdded new Access Controls	01-05-2022
1.3	<ul style="list-style-type: none">Enable refer call xfer on realmAdded RespondOptionsManip	07-15-2022
1.4	<ul style="list-style-type: none">Added DigiCert Global Root G2 as root certificateModified TLS Profile	08-22-2022
1.5	<ul style="list-style-type: none">Modified powershell cmdlet	03-14-2023
1.6	<ul style="list-style-type: none">Modified Cert record config requirements	02-12-2024
1.7	<ul style="list-style-type: none">Removed reference to ping-response parameter and added notes for using tls-global config in ACLI	07/20/2024
1.8	<ul style="list-style-type: none">Removed MSFT PS config, added Teams GUIRemoved Baltimore Root	09/19/2025
1.9	<ul style="list-style-type: none">Modified MSFT Trusted Root Program hyperlinkAdded appendix E for IPV6 support with Teams	12/04/2025
1.10	<ul style="list-style-type: none">Added Root CA list and ECU considerations	01/08/2026

2 Intended Audience

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

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

3 Validated Oracle Software Versions

All testing was successfully conducted with the Oracle Communications SBC versions:

SCZ830, SCZ840, SCZ900, SCZ1000

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

- AP 1100
- AP 3900
- AP 3950
- AP 4600
- AP 4900
- AP 6350
- AP 6300
- AP 6400
- VME

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

4 Related Documentation

4.1 Oracle SBC

- [Oracle® Enterprise Session Border Controller Web GUI User Guide](#)
- [Oracle® Enterprise Session Border Controller CLI Reference Guide](#)
- [Oracle® Enterprise Session Border Controller Release Notes](#)
- [Oracle® Enterprise Session Border Controller Configuration Guide](#)
- [Oracle® Enterprise Session Border Controller Security Guide](#)

4.2 Microsoft Teams

- [Microsoft Teams Direct Routing Overview](#)
- [Microsoft Teams Direct Routing Configuration](#)
- [Microsoft Teams Public Trusted Certificate for the SBC](#)

5 About Teams Direct Routing

Microsoft Phone System Direct Routing lets you connect a supported, customer-provided Session Border Controller (SBC) to Microsoft Phone System. With this capability, for example, you can configure on-premises Public Switched Telephone Network (PSTN) connectivity with Microsoft Teams client.

With Direct Routing, you can connect your SBC to almost any telephony trunk or interconnect with third-party PSTN equipment. Direct Routing enables you to:

- Use virtually any PSTN trunk with Microsoft Phone System.
- Configure interoperability between customer-owned telephony equipment, such as a third-party private branch exchange (PBX), analog devices, and Microsoft Phone System.

5.1 Planning Direct Routing

When planning to configure MSFT Teams Direct Routing with the Oracle SBC, the following prerequisites are required: Please read through the following information before proceeding.

- [Microsoft Phone System Licensing](#)
- [Fully Qualified Domain Name for your Session Border Controller](#)
- [Public trusted certificate for the Oracle SBC](#)

5.2 Media Bypass vs Non Media Bypass

When planning and setting up Microsoft Teams Phone System Direct Routing, one of the main features you need to pay attention to is whether or not you enable media bypass in your Teams tenant, or leave it disabled. This feature changes the way media flows on calls.

The default configuration is to have Media Bypass disabled, which forces the Microsoft phone system media processors to anchor media for all calls. In other words, all media packets will flow from the Oracle SBC to Microsoft phone system, and from there, to the Teams client.

Media bypass enables you to shorten the path of media traffic and reduce the number of hops in transit for better performance. With media bypass, media is kept between the Oracle Session Border Controller (SBC) and the client instead of sending it via the Microsoft Phone System. Media bypass leverages protocols called **Interactive Connectivity Establishment (ICE)** on the Teams client and [ICE lite](#) on the Oracle SBC. These protocols enable Direct Routing to use the most direct media path for optimal quality

For more information, please see "[About Media Bypass with Direct Routing](#)"

5.3 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 and Microsoft Trusted Root Program with Included CA Certificate List
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	

5.4 DNS Requirements

You must create DNS records for domains in your network that resolve your Oracle SBC. Before you begin, the following is required for every Oracle SBC you want to pair:

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

5.4.1 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 FQDN name of the SBC.

The following table shows examples of DNS names registered for the tenant, whether the name can be used as an FQDN for the SBC, and examples of valid FQDN names:

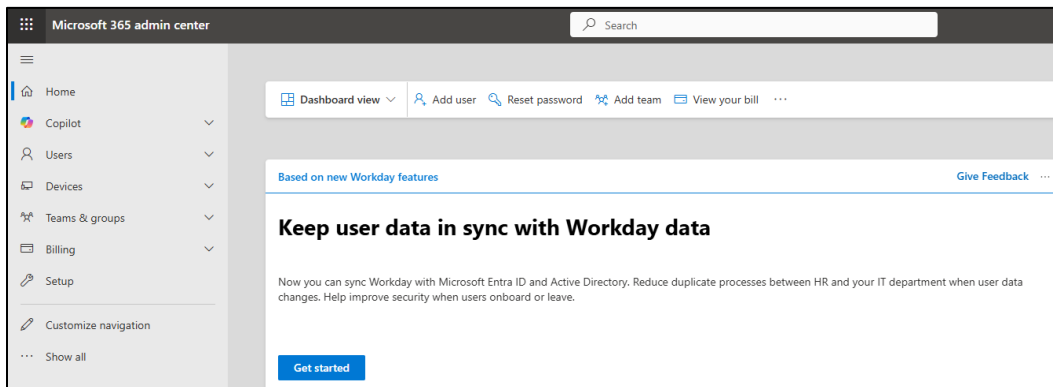
DNS name	Can be used for SBC FQDN	Examples of FQDN names
contoso.com	Yes	Valid names: sbc1.contoso.com ssbcs15.contoso.com europe.contoso.com
contoso.onmicrosoft.com	No	Using *.onmicrosoft.com domains is not supported for SBC names

5.4.2 Adding the SBC Domain to Microsoft O365

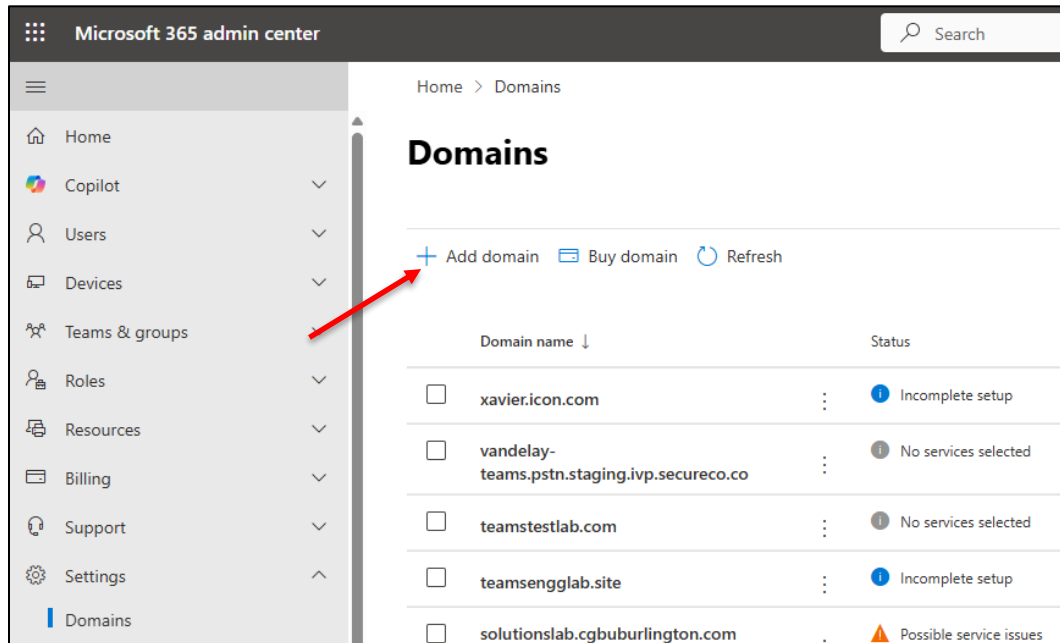
The steps below will walk you through adding/registering your Oracle SBC domain in Microsoft O365.

*To add, modify or remove domains you **must** be a **Global Administrator** of a business or enterprise plan. These changes affect the whole tenant, Customized administrators or regular users won't be able to make these changes*

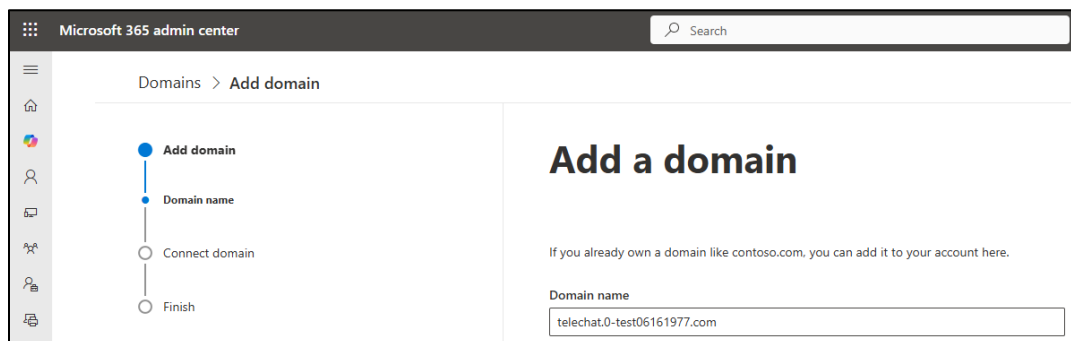
1. Go to the admin center at <https://admin.microsoft.com>. Enter your credentials to access the Microsoft 365 admin center



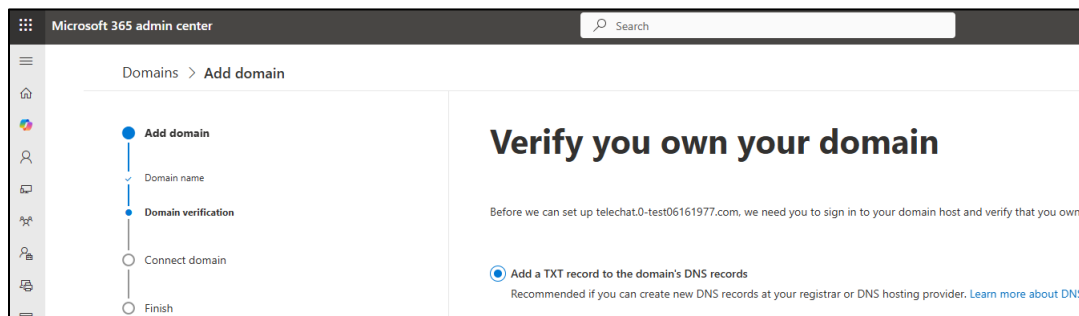
2. Go to the Settings > Domain's page, click Add Domain



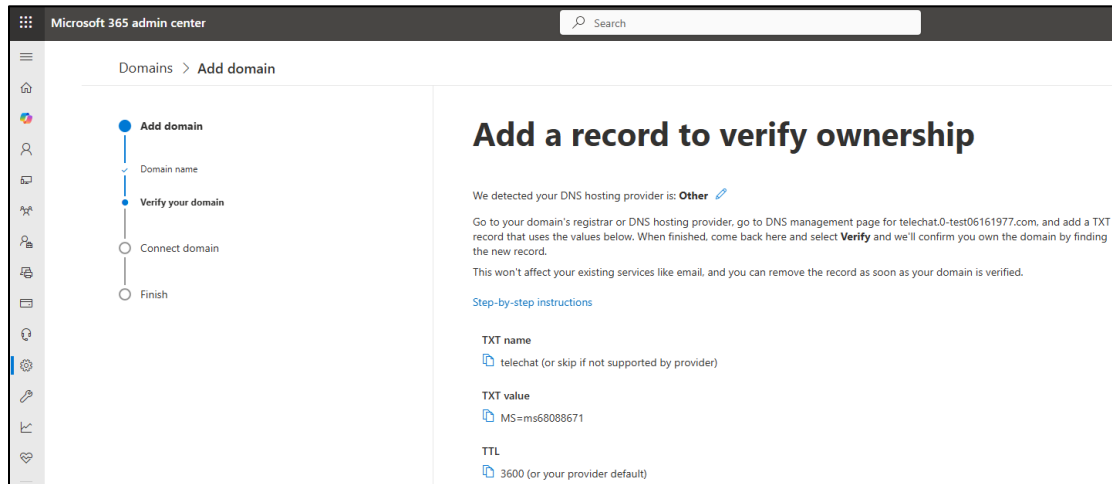
3. Enter the name of the domain you want to add, then select “Use this domain” at the bottom



4. Next, choose how you want to verify that you own the domain. For the purposes of this example, we select “Add a TXT record” select continue.



5. Follow the instructions on the screen. Once complete, select “verify” to complete the process.



In this application note, we are using the following FQDN that is registered in Microsoft O365 to pair the Oracle SBC to Microsoft Teams Direct Routing Interface. Since our SBC is deployed behind NAT, we will only be displaying the private IP addresses configured on the SBC.

Public IP Address	FQDN Name
<Public IP of SBC or NAT>	telechat.o-test06161977.com

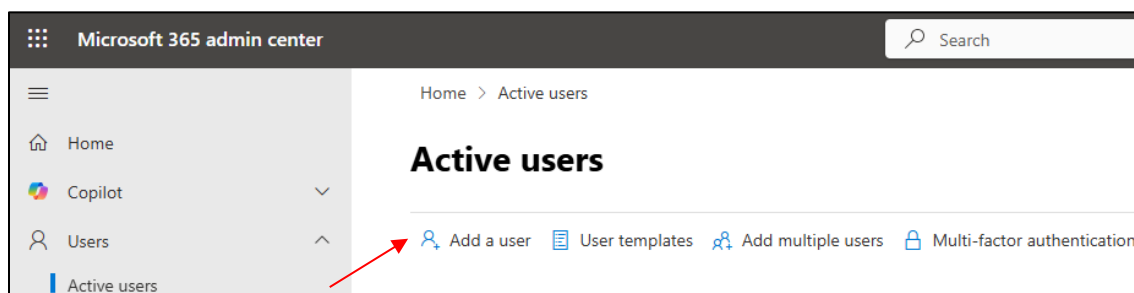
Next, we can create a User and assign Microsoft Phone System license.

5.4.3 Creating a User in Microsoft O365

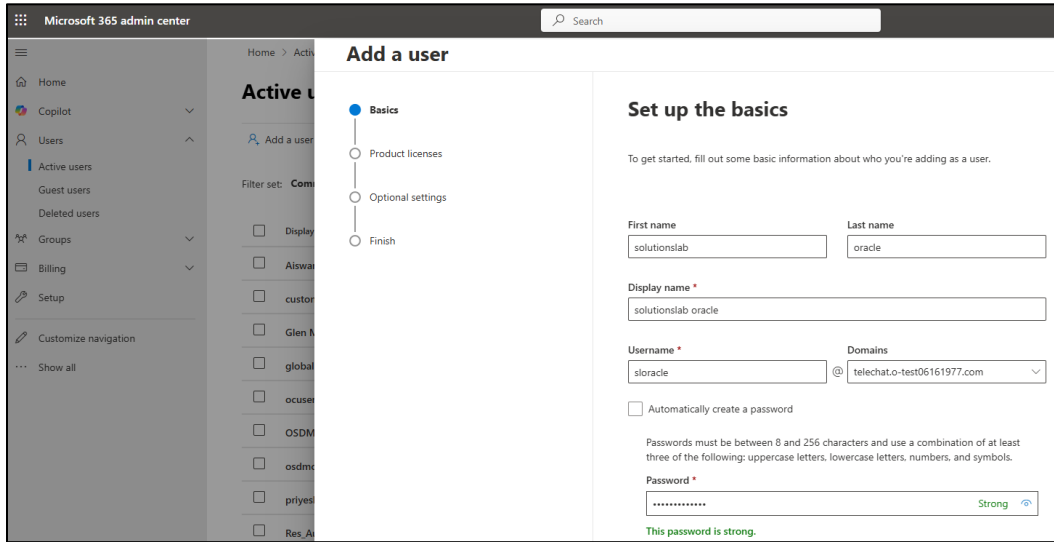
After your Domain has been added and verified in Microsoft O365, the domain must be activated by adding at least one licensed user with the SIP address matching that registered domain.

The steps below will outline how to add a user and assign privileges and licenses to that user.

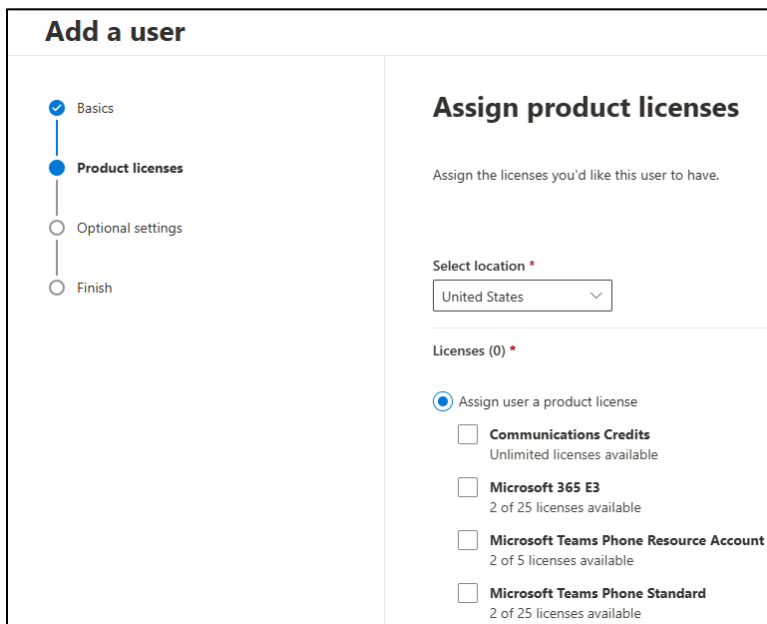
1. In the [Microsoft 365 admin center](#), go to **User management**, and select Add user.



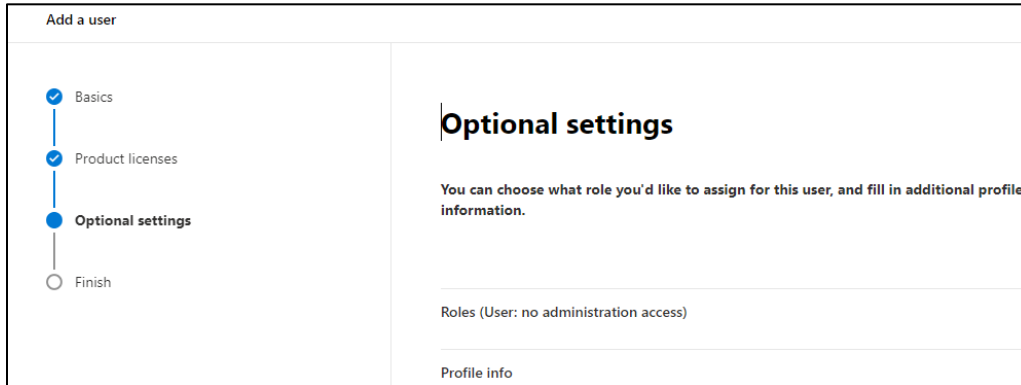
2. Fill in the required fields for basic information of the user and select Next



- Assign the user a product license. To allow for Microsoft Teams Direct Routing, the following licenses must be assigned to users.
 - Microsoft 365 Phone System
 - Office 365 E3



- Finally, select Roles and add any additional Profile info to the user account. Select next and follow the on screen instructions to complete the addition of the user.



5.5 Connect the SBC to the Teams tenant.

The following describes how to configure your Teams tenant to accept a connection from the Oracle SBC. It will also cover how to enable your users for Direct routing, and the basics on how to setup call routing.

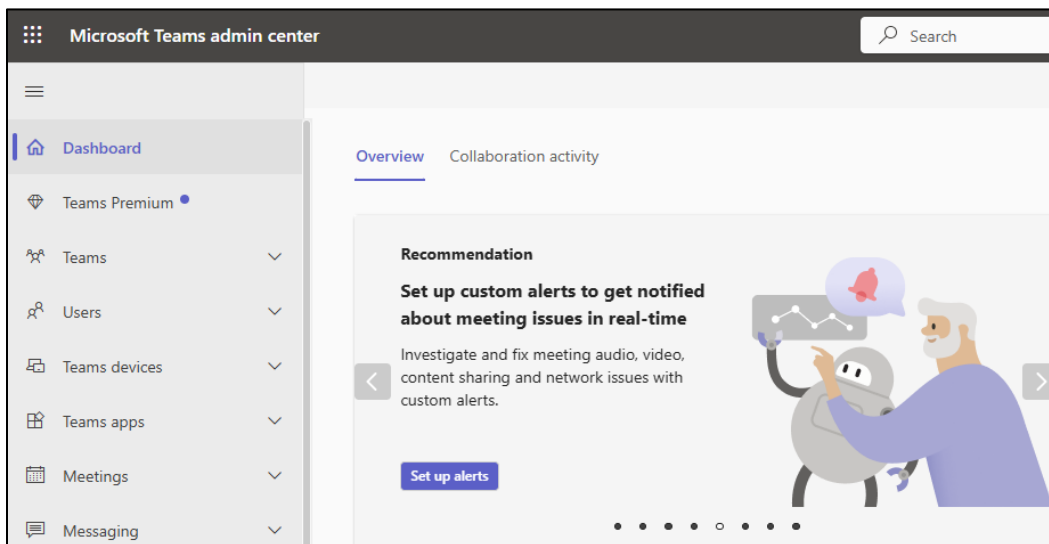
There are two ways to configure Microsoft Teams to accept a connection from the SBC. Using the Microsoft Teams admin center GUI, or by using the CLI in PowerShell.

In this example, we'll use the Teams Admin Center and provide some examples of a basic configuration.

In order you use Powershell to connect to your Teams tenant, you must first follow the step outlined in [Set up your computer for Windows Powershell](#)

5.5.1 Teams Admin Center Configuration

1. Go to the Teams admin center at <https://admin.teams.microsoft.com/dashboard> and enter your credentials when prompted.



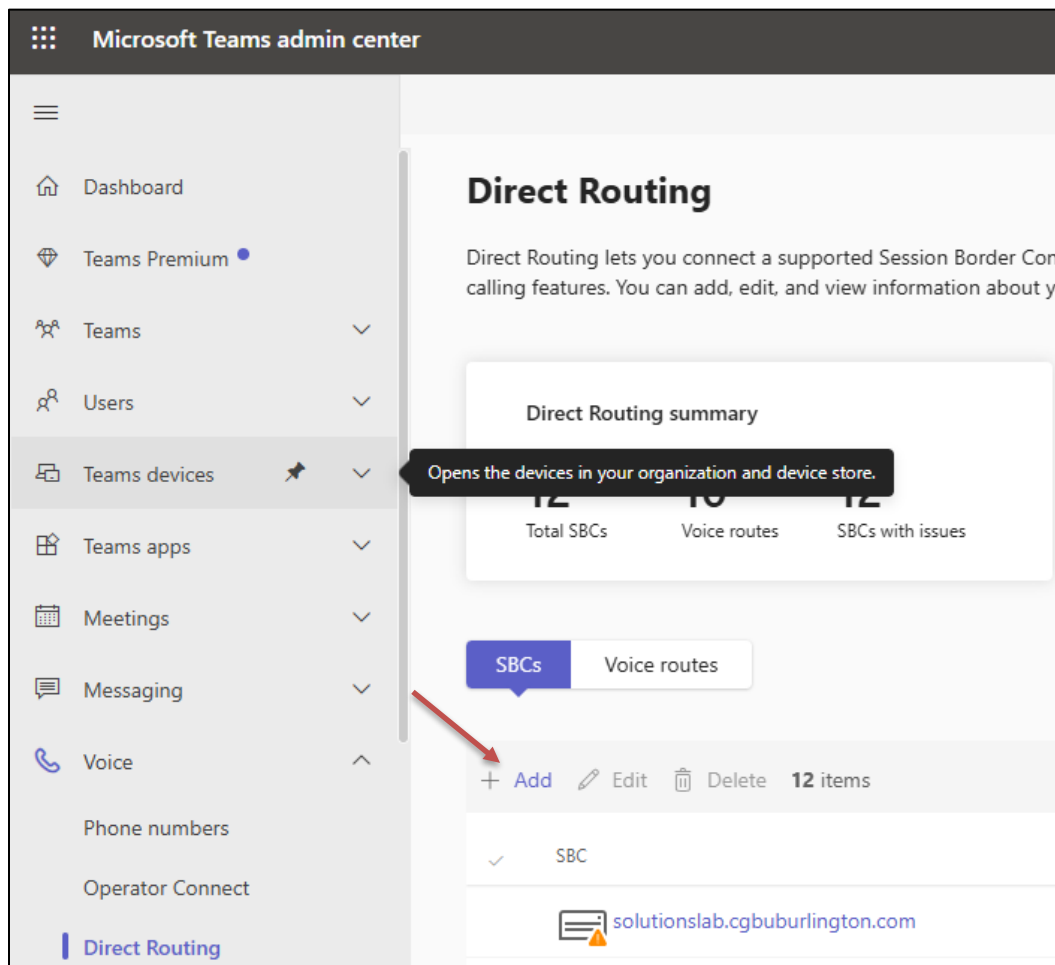
5.5.2 Connect the Oracle SBC

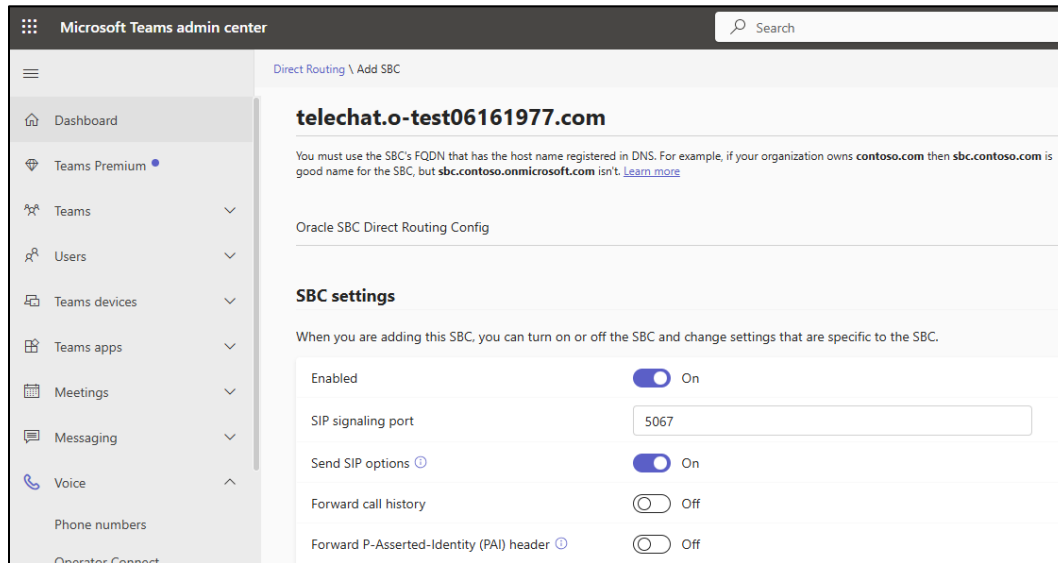
1. In the left navigation, go to **Voice > Direct Routing**, and then select the **SBCs** tab.

2. Select **Add**.
3. Enter an FQDN for the SBC.

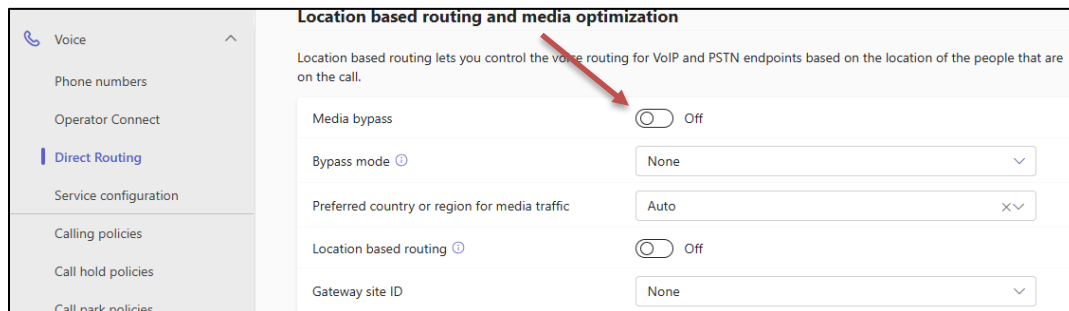
*Make sure the domain name portion of the FQDN matches a domain that's registered in your tenant. Keep in mind that the *.onmicrosoft.com domain name isn't supported for the SBC FQDN domain name.*

4. Configure the settings for the SBC, based on your organization's needs. For details on each of these settings, see [SBC settings](#).
5. When you're done, select **Save**.





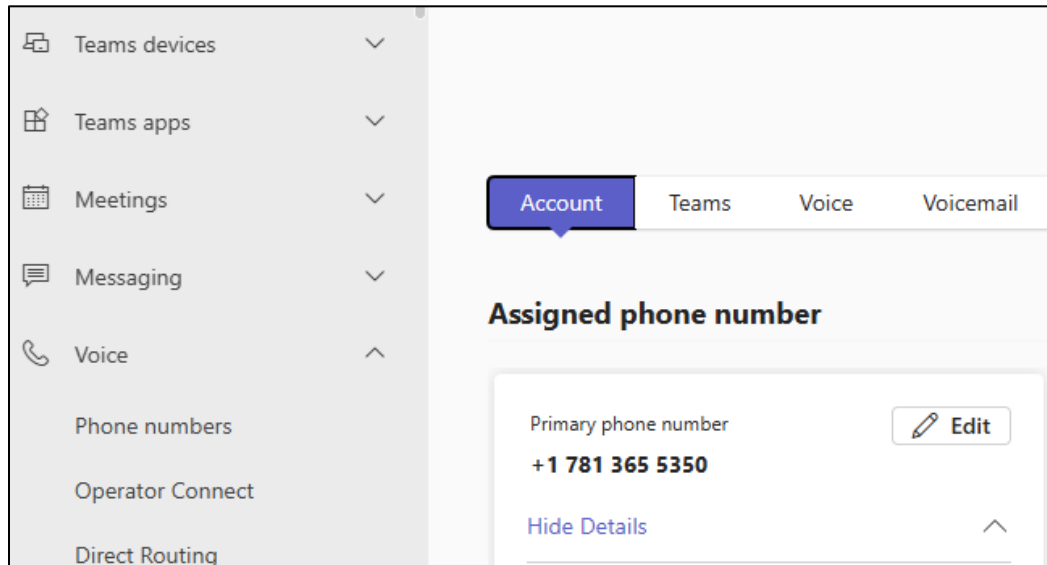
You can control media bypass for each SBC by enabling Media Bypass under the Location Based routing and media optimization.



5.5.3 Configuring User Online Voice Settings

Earlier in the application note, we created a user and assigned that user the proper licenses. The next step is to configure the user's online phone settings.

1. Go to **Users > Manage users**.
2. Select a user.
3. Under **Account > General information**, select **Edit**.
4. Under **Assign phone number**, from the **Phone number type** drop-down menu, select **Direct Routing**.
5. Enter an assigned phone number and a phone number extension if applicable.
6. Select **Apply**.



The account's general information now shows the assigned phone number and displays Direct Routing as the phone number type

It's recommended, but not required, that the phone number used is configured as a full E.164 phone number with country code

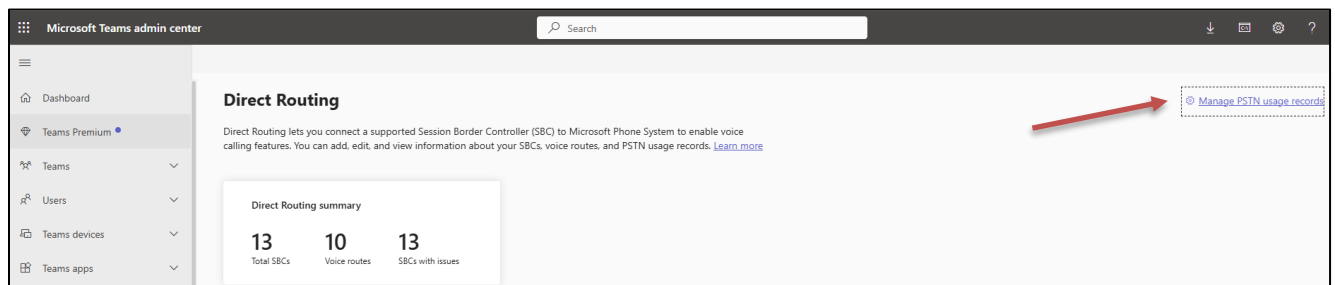
5.5.4 Configure Voice Routing for Direct Routing

We'll now go through how to configure voice routing for Phone System Direct Routing.

Please see "[Configure Voice Routing for Direct Routing](#)" for more details and in depth examples.

5.5.4.1 Create the "US and Canada" PSTN usage

1. In the left navigation of the Microsoft Teams admin center, go to **Voice > Direct Routing**, and then in the upper-right corner, select **Manage PSTN usage records**.
2. Select **Add**, type **US and Canada**, and then select **Apply**.



PSTN usage records

Voice routes are linked to voice policies using PSTN usage records. You can manage the list of existing PSTN usage records or add new ones. [Learn more](#)

12 items

+ Add

US and Canada

5.5.4.2 Create a Voice Route

1. In the left navigation of the Microsoft Teams admin center, go to **Voice > Direct Routing**, and then select the **Voice routes** tab.
2. Select **Add**, and then enter a name and description for the voice route.
3. Set the priority and specify the dialed number pattern.
4. To enroll an SBC with the voice route, under **SBCs enrolled (optional)**, select **Add SBCs**, select the SBCs you want to enroll, and then select **Apply**.
5. To add PSTN usage records, under **PSTN usage records (optional)**, select **Add PSTN usage**, select the PSTN records you want to add, and then select **Apply**.
6. Select **Save**.

Microsoft Teams admin center

Direct Routing

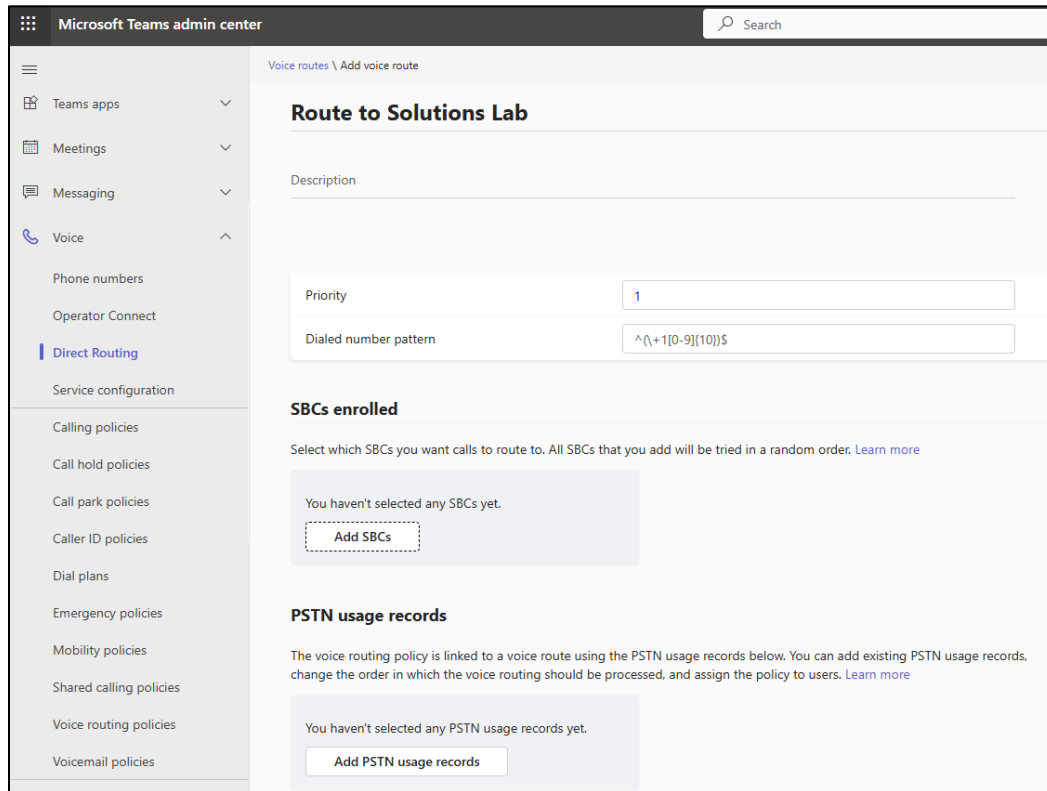
Direct Routing lets you connect a supported Session Border Controller (SBC) to calling features. You can add, edit, and view information about your SBCs, voice

Direct Routing summary

13	10	13
Total SBCs	Voice routes	SBCs with issues

SBCs Voice routes

+ Add Edit Move up Move down Delete 10 items



5.5.4.3 Create a voice routing policy

1. In the left navigation of the Microsoft Teams admin center, go to **Voice > Voice routing policies**, and then select **Add**.
2. Type **US Only** as the name and add a description.
3. Under **PSTN usage records**, select **Add**, select the "US and Canada" PSTN usage record, and then select **Apply**.
4. Select **Save**.

Microsoft Teams admin center

Search

- Emergency policies
- Mobility policies
- Shared calling policies
- Voice routing policies**
- Voicemail policies
- Auto attendants
- Call queues
- Holidays
- Resource accounts
- Voice applications policies
- Teams client health
- Locations
- Frontline deploy...

Voice routing policies

A voice routing policy for Direct Routing will be linked to a voice route using PSTN usage records, change the order in which the usages will be processed, and assign the voice resource accounts. [Learn more](#)

Save time and manage your organization's settings and policies more efficiently with our simplified, all-in-one management center.

Voice routing policies summary

1	9
Default policy	Custom policies

Manage policies | Group policy assignment

+ Add | Edit | Duplicate | Delete | Reset Global policy | Assign

Microsoft Teams admin center

Left navigation button

- Emergency policies
- Mobility policies
- Shared calling policies
- Voice routing policies**
- Voicemail policies
- Auto attendants
- Call queues
- Holidays
- Resource accounts
- Voice applications policies
- Teams client health

Add policy details

Name

US Only

Description

Route to Oracle SBC Burlington MA

PSTN usage records

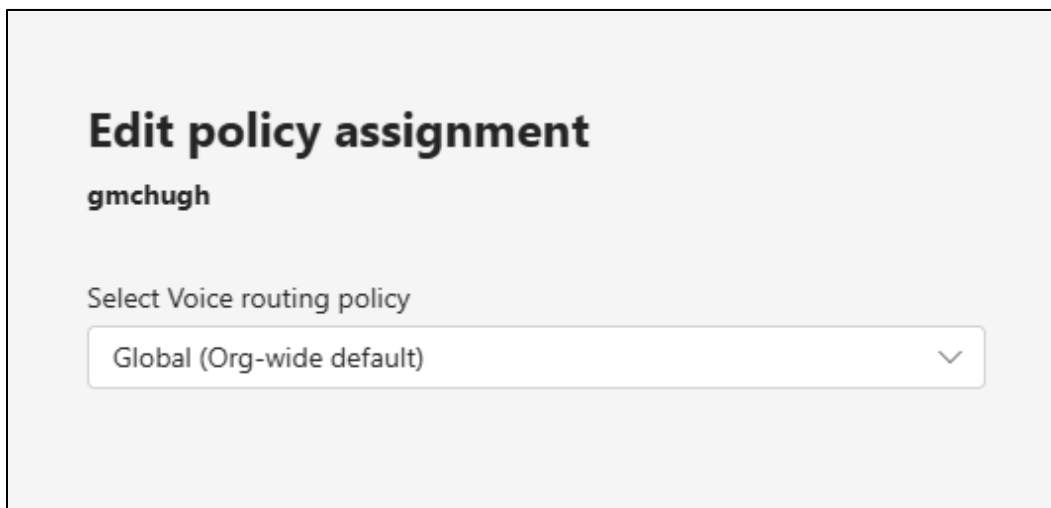
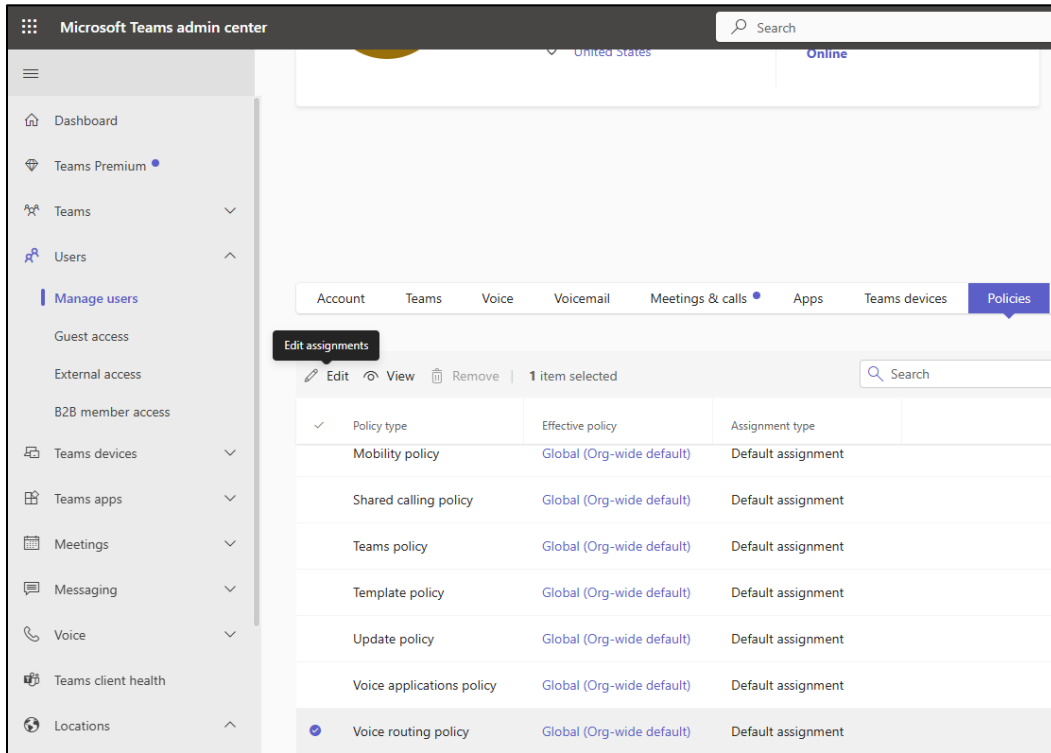
PSTN usages are linked to voice routing policies, which are assigned the order they're listed until a match is found.

Add or remove | Move up | Move down | 1 item

✓	PSTN usage record
---	-------------------

5.5.4.4 Assign the voice routing policy to user

1. In the left navigation of the Microsoft Teams admin center, go to **Users, Manage Users** and then select the user.
2. Select **Policies**, and then next to **Assigned policies**, select **Edit**.
3. Under **Voice routing policy**, select the "US Only" policy, and then select **Apply** and **Save**.



- This concludes the basic setup in Microsoft Teams tenant to pair the SBC, assign DID's to users, and create voice routing for Phone System Direct Routing. We'll now move on to configuring the Oracle SBC.

6 Oracle SBC Configuration

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

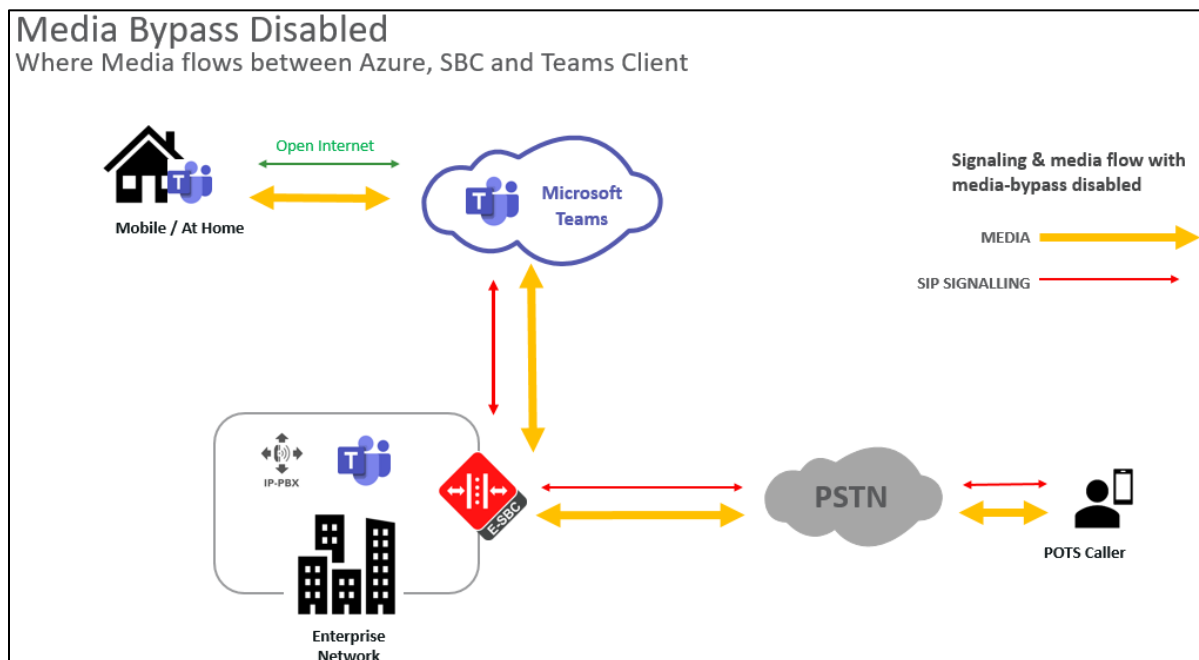
If the Oracle SBC being deployed is new, with no existing configuration, the simplest way to configure it to interface with Microsoft Teams Phone System Direct Routing is by utilizing the [Configuration Assistant](#).

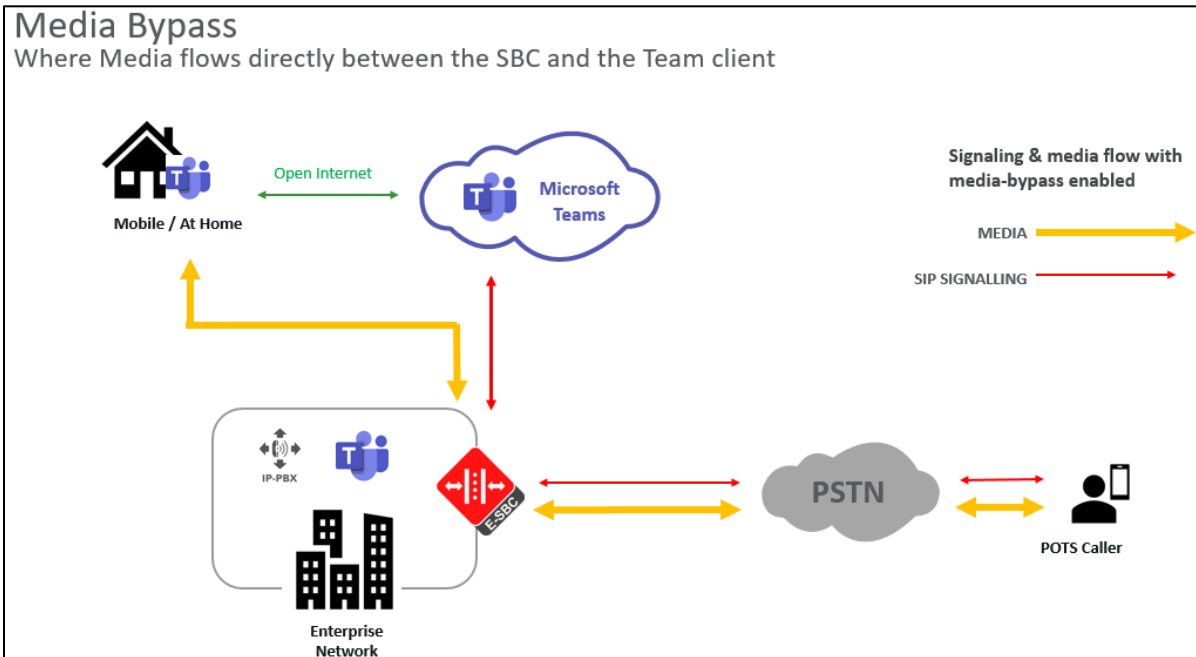
If an existing SBC is being used to interface with Microsoft Teams, follow the steps in this chapter to successfully configure the Oracle SBC.

Below shows the connection topology example for MSFT Teams for both Media Bypass and Non Media Bypass deployments

There are multiple connections shown:

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





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.

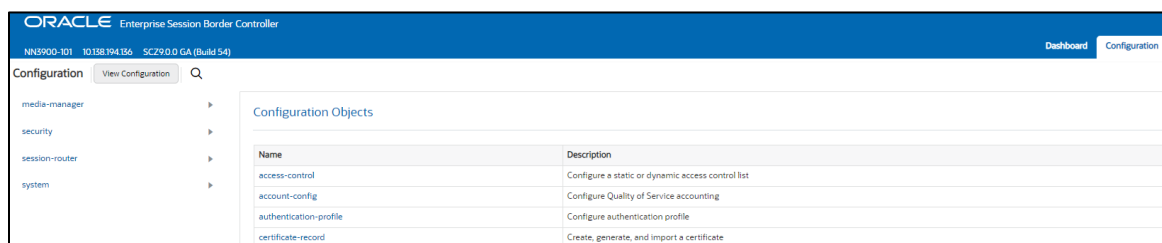
This guide assumes the OCSBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, web-server-config has been enabled for GUI access. If you require more information on how to install your SBC platform, please refer to the [ACLI configuration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

Note: the configuration examples below were captured from a system running the latest GA software, 9.0.0



6.1 System-Config

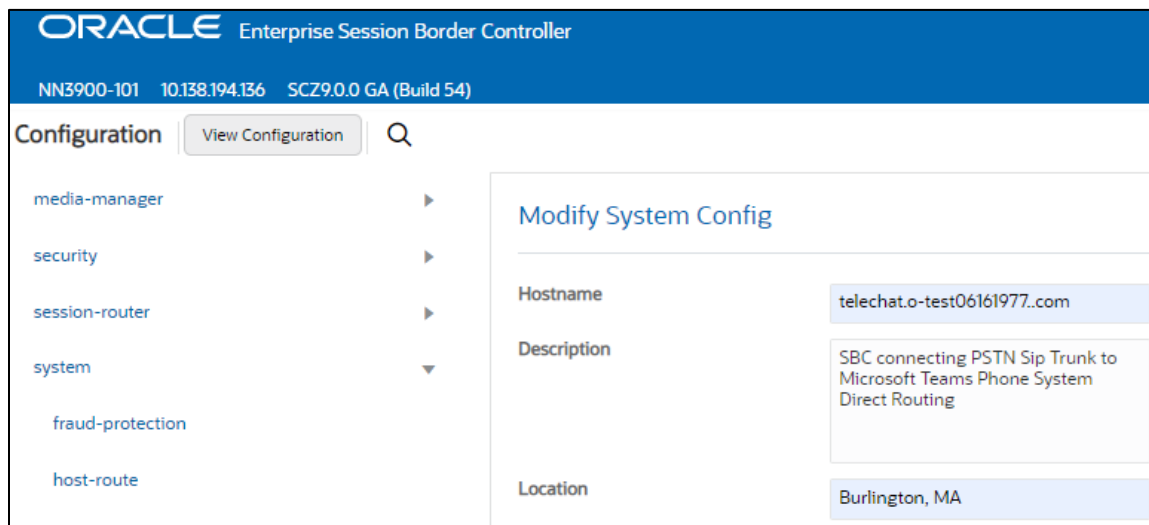
To enable system level functionality for the OCSBC, you must first enable the system-config

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)
- Transcoding Core (This field is only required if you have deployed a VME SBC)



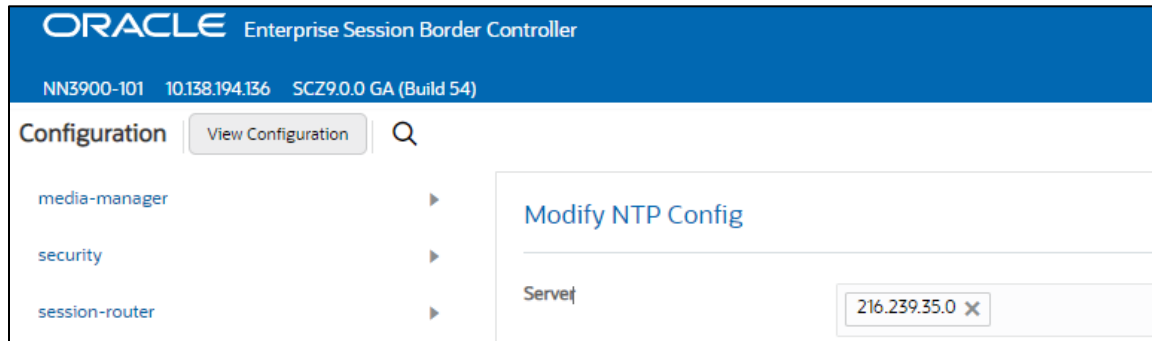
- Click OK at the bottom

6.1.1 NTP-Sync

You can use the following example to connect the Oracle SBC to any network time servers you have in your network. This is an optional configuration, but recommended.

GUI Path: system/ntp-config

ACL Path: config t→system→ntp-sync



- Select OK at the bottom

Now we'll move on configuring network connection on the SBC.

6.2 Network Configuration

To connect the SBC to network elements, we must configure both physical and network interfaces. For the purposes of this example, we will configure two physical interfaces, and two network interfaces. One to communicate with MSFT Teams Direct Routing, the other to connect to PSTN Network. The slots and ports used in this example may be different from your network setup.

6.2.1 Physical Interfaces

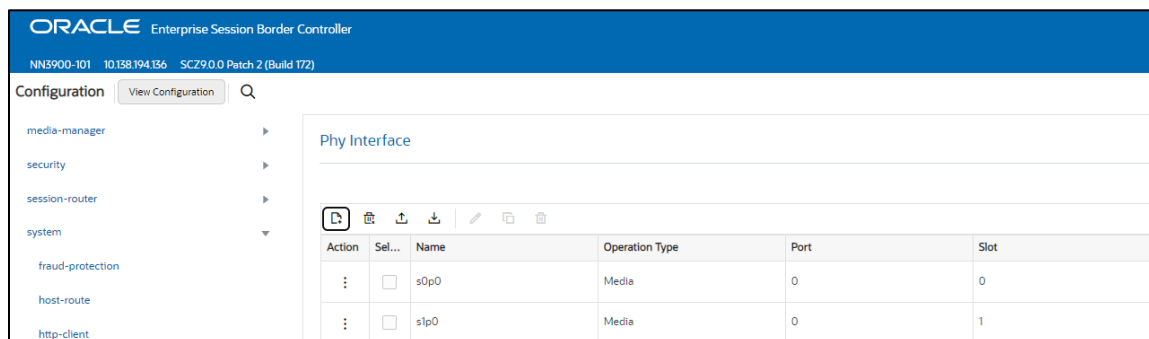
GUI Path: system/phy-interface

ACL Path: config t→system→phy-interface

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

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

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



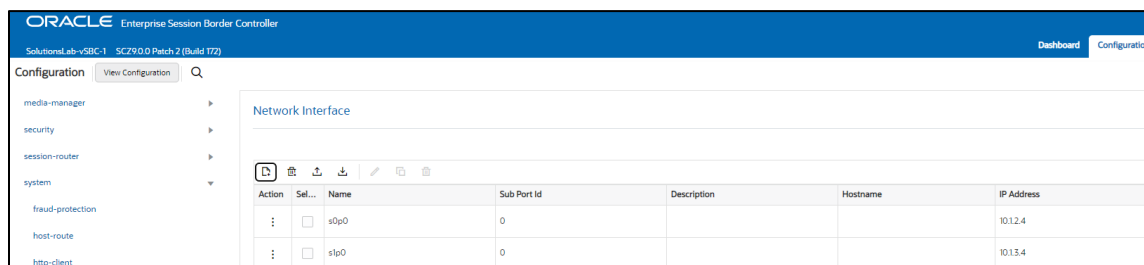
6.2.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t→system→network-interface

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

Configuration Parameter	Teams	PSTN
Name	s0p0	S1p0
IP Address	10.1.3.4	10.1.2.4
Netmask	255.255.255.0	255.255.255.0
Gateway	10.1.3.1	10.1.2.1
DNS Primary IP	8.8.8.8	
DNS Domain	Telechat.o-test06161977.com	



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

Next, we'll configure the necessary elements to secure signaling and media traffic between the Oracle SBC and Microsoft Phone System Direct Routing.

6.3 Security Configuration

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

Microsoft Teams Direct Routing only allows TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It requires a certificate signed by Certificate Authorities (CAs) that are part of the [Microsoft Trusted Root Certificate Program](#). A list of currently supported Certificate Authorities can be found at:

[Public trusted certificate for the SBC](#)

6.3.1 Certificate Records

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

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

GUI Path: security/certificate-record

ACLI Path: config t→security→certificate-record

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

- SBC Certificate (end-entity certificate)
- GoDaddy Root Cert (Root CA used to sign the SBC's end entity certificate)
- [Microsoft Root Certificate Authorities](#) (Microsoft Presents the SBC a certificate signed by one of these authorities)

Note: The GoDaddy RootCA is only part of this example, as that is the Authority we used to sign our SBC certificate. You would replace this with the root and/or intermediate certificates used to sign the CSR generated from your SBC.

6.3.1.1 SBC End Entity Certificate

The SBC's end entity certificate is the certificate the SBC presents to Microsoft to secure the connection. The only requirements when configuring this certificate is the common name must contain the SBC's FQDN and the **extended key usage list** must contain **serverAuth**. Including **clientAuth** is optional for now as Microsoft Teams Direct Routing currently permits the use of SBC client certificates even if the Client Authentication EKU is not included.

However, [Microsoft has indicated](#) that in the future, all SBC client certificates will be required to include the Client Auth EKU. When this enforcement goes into effect, a list of publicly trusted certificate authorities (CAs) that can issue such certificates will be published.

It's important to note that public CAs may stop including the Client Authentication EKU in certificates due to updated [industry requirements](#) and CA policies. You should check with your CA to determine when they plan to stop including the Client Authentication EKU by default, so you can plan accordingly.

For more information, please refer to:

<https://learn.microsoft.com/en-us/microsoftteams/direct-routing-whats-new#update-on-upcoming-certificate-changes-updated-december-12-2025>

and

<https://www.oracle.com/a/otn/docs/oracle-sbc-%e2%80%93-microsoft-teams-ca-changes-and-eku-considerations.pdf>

In this example our common name will be **telechat.o-test06161977.com**. You must also give it a name and we have included **clientAuth** to the **extended key usage list**.

For now, mutual TLS connections between your Oracle SBC and Microsoft Teams will continue to be established, even if the root CA removes or no longer supports the clientAuth EKU. Looking ahead, including the clientAuth EKU in your SBC's end entity certificate will be important to maintain compatibility and avoid future issues with Microsoft Teams Direct Routing. When submitting your CSR for signing, work with your CA to make sure the required EKU is maintained during the signing process.

If you generate a CSR using a certificate record that includes both serverAuth and clientAuth EKUs, but the CA removes the clientAuth EKU when signing the certificate, you can still import the resulting certificate into the SBC without any errors. The SBC will accept and present the certificate even if the clientAuth EKU is not included after signing.

All other fields are optional, and can remain at default values.

To Configure the certificate record:

Click Add, and use the following example to configure the SBC certificate

The screenshot displays the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes the Oracle logo and the text 'Enterprise Session Border Controller'. Below this, system information is shown: 'NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)'. The main interface is divided into a left sidebar and a main content area. The sidebar, titled 'Configuration', contains a search bar and a list of configuration categories: 'media-manager', 'security', 'authentication-profile', 'certificate-record' (highlighted), 'tls-global', 'tls-profile', 'session-router', and 'system'. The main content area is titled 'Add Certificate Record' and contains the following fields:

Name	SBCCertificateforTeams
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	
Common Name	telechat.o-test-06161977.com
Key Size	2048
Alternate Name	
Trusted	<input checked="" type="checkbox"/> enable
Key Usage List	digitalSignature X keyEncipherment X
Extended Key Usage List	serverAuth X clientAuth X

- Click OK at the bottom

Next, using this same procedure, configure certificate records for the Root CA certificate

6.3.1.2 Root CA and Intermediate Certificates

6.3.1.2.1 Go Daddy Root

The following, GoDaddyRoot, is the root CA certificate used to sign the SBC's end entity certificate. As mentioned above, your root CA and/or intermediate certificate may differ. This is for example purposes only.

Config Parameter	GoDaddy Root
Common Name	Go Daddy Class2 Root CA
Key Size	2048
Key-Usage-List	digitalSignature keyEncipherment
Extended Key Usage List	serverAuth
Key algor	rsa
Digest-algor	Sha256

6.3.1.2.2 Microsoft Root Certificate Authorities

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 one of the CA's listed in the table below. To trust this certificate, your SBC must have all the certificate listed below as a trusted CA certificate.

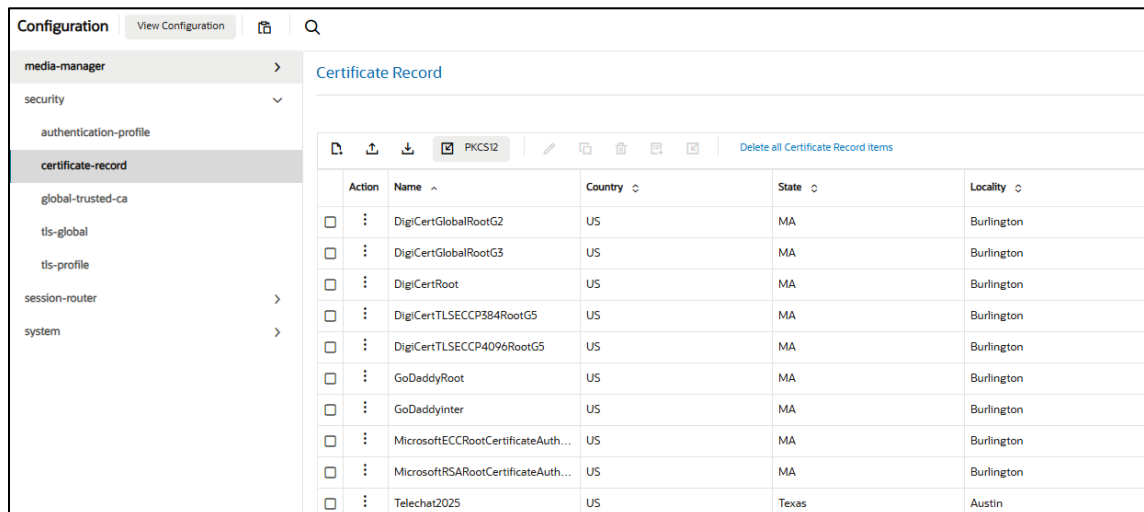
Download each certificate from the official source using the links provided below:

Certificate Authority	Download Link
DigiCert Global Root CA	DigiCert Global Root CA
DigiCert Global Root G2	DigiCert Global Root G2
DigiCert Global Root G3	DigiCert Global Root G3
DigiCert TLS ECC P384 Root G5	DigiCert TLS ECC P384 Root G5
DigiCert TLS RSA 4096 Root G5	DigiCert TLS RSA 4096 Root G5
Microsoft ECC Root Certificate Authority 2017	Microsoft ECC Root Certificate Authority 2017
Microsoft RSA Root Certificate Authority 2017	Microsoft RSA Root Certificate Authority 2017

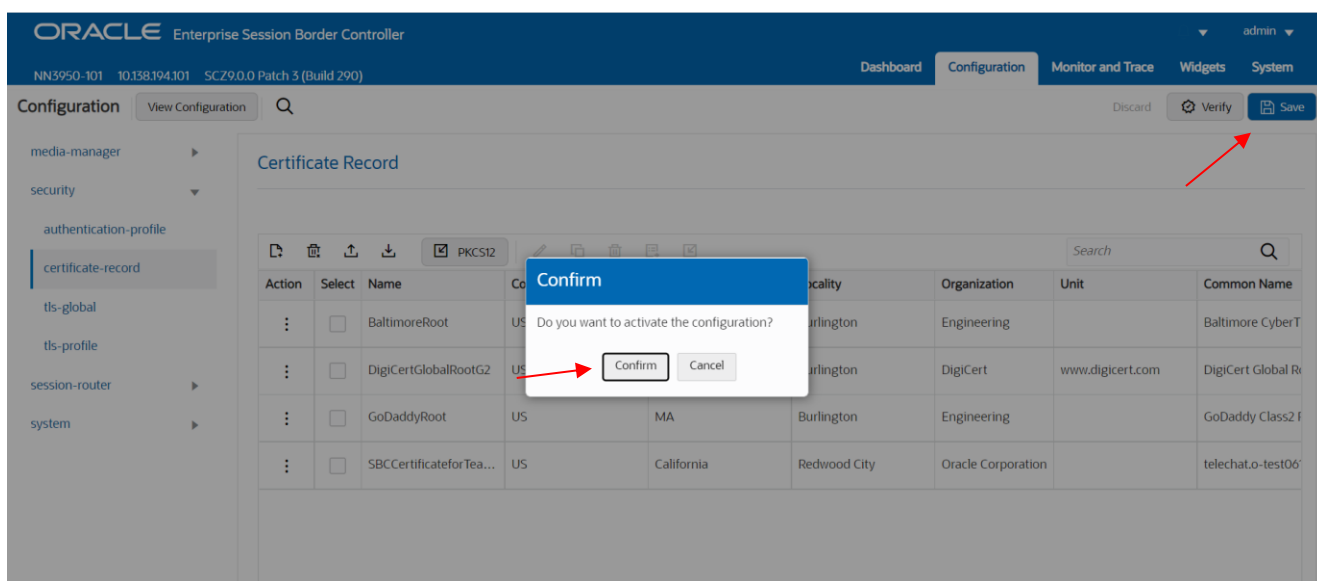
The certificates listed in the table above can also be found at:

<https://learn.microsoft.com/en-us/azure/security/fundamentals/azure-ca-details?tabs=root-and-subordinate-cas-list>

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



At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must **save and activate** the configuration of the SBC.



6.3.1.3 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 Oracle SBC GUI, select the SBC's end entity certificate that was created above, and click the "generate" tab at the top:

ORACLE Enterprise Session Border Controller
 NN3950-101 10.138.194.101 SC29.3.0 Patch 7 (Build 259)

Configuration View Configuration

media-manager
 security
 authentication-profile
certificate-record
 global-trusted-ca
 tls-global
 tls-profile
 session-router

Certificate Record

PKCS12 Delete all Certificate Record items

Select	Action	Name	Country	State	Locality	Organization
<input type="checkbox"/>	:	DigiCertGlobalRootG2	US	MA	Burlington	Engineering
<input type="checkbox"/>	:	GoDaddyRoot	US	MA	Burlington	Engineering
<input checked="" type="checkbox"/>	:	SBCCertificateforTeams	US	MA	Burlington	Engineering

Generate certificate response

Copy the following information and send to a CA authority

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwbDELMAkGA1UEBhMCVVMxMzA1BjBmNVBAgTAKIBMRMwEQYDVQQL
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcm1uZzZlMCMGA1UEAxMcdGVz
ZWNoYXQuYm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9u
ADCCAQoCggEBAK+uhx7951uhDgtQwv4EoZE68WDLIDYPPYcJWbvL5uWzk6y3Yh
s40ca4ZuZWmrLNLILZfV9x9R5KzM4M8wqYiUvPOBC6oowuautu/swSKIReSpfDZh
NaAGUJrvAfvacyPz7KsyrJKgchzsOFNJPDAaQsDQjuoFCDUbtOA1Z6xDFxpCdIF
nhq+dtB7gAtCdvWE/V6r4PAfJ1dj82YT4YBAWqwQJ2wGn+yc2FtEPsmH1bWEiCvR
sMGfUeJcTM5i//AVcpF+jsJc8xswtE+Zr24kEiCrcrm0IlgOHRvEgYtluUteFoly
d/60oaVPYHhkKn25OHQ2lwaMIIkMxpBjlpUCAwEAQA9MDsGCsGqGSib3DQEJJDjEu
MCwwCwYDVROpBAQDAgWgMB0GATludJQWMBQGCsGAQUFBwMBBggrBgEFBQcDAjAN
BgkqhkiG9w0BAQsFAAOCAQEAnBLJuRPL82rkQDIB3I2JeOf3tacevMQeCIGcdFCf
uLcey+2XmtKF+HHPIECde+tLkXIjseVnfBT2Ba4KynPwmTkQ5DfoLYQjWFOhEsm
LcuKMvjBYekJwebDk9CtDWwBZ9O1DzYbyuVNXPLbID5ludWbJBAYwd+9693VUVQb
/UR5rooNKwQIOFJMNmuPMW13v/p7kVsItk8aSwF6lHNx+k56MrR45YFqV/czcQTs
PeTYRyOVGYsQ0h5T5kcU0xjEXp5K2gpdQz8YGblAbKZxcPjn7zJEWgtoadmRnhZ
f7Gm45Jt45IA8QDpeq5H83ajFg0q8twMeVj9znA0ogle/g==
-----END CERTIFICATE REQUEST-----

```

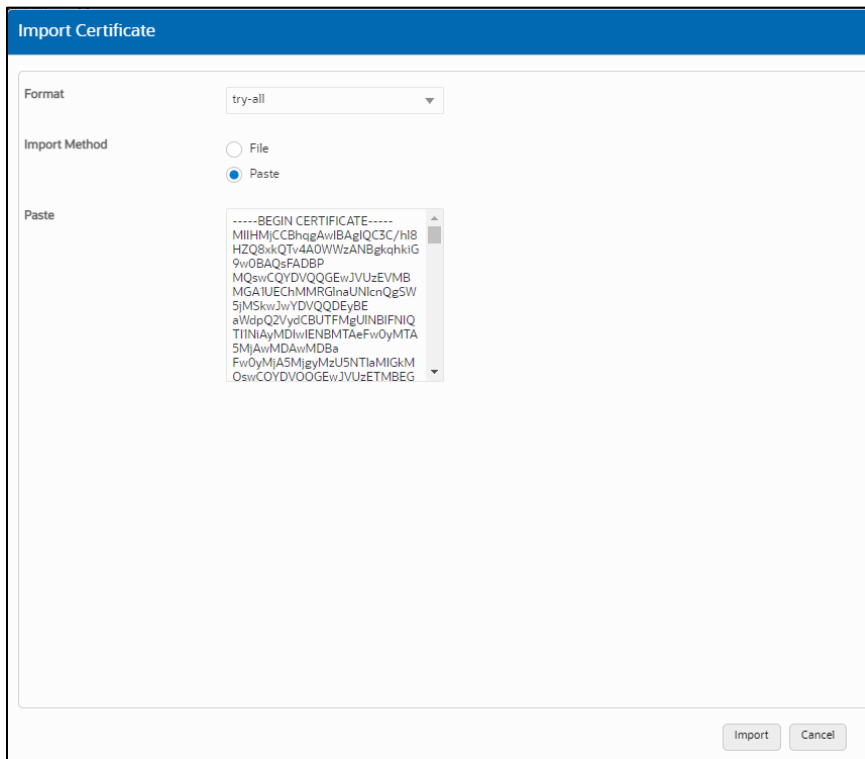
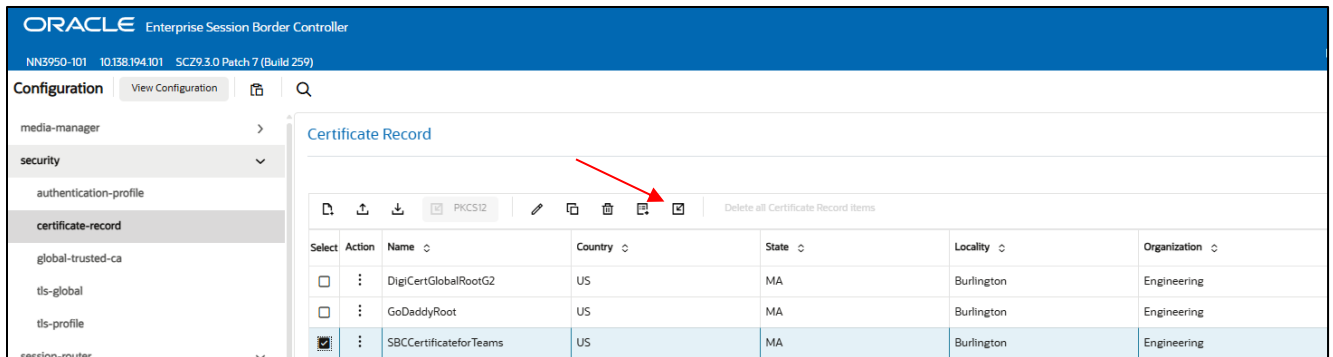
Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, **another save and activate is required** before you can import the certificates to each certificate record created above.

Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

6.3.1.4 Import Certificates to SBC

Once certificate signing request has 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 a third **save/activate** from the WebGUI to complete the configuration of certificates on the Oracle SBC.



- Once pasted in the text box, select Import at the bottom, then **save and activate** your configuration.

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

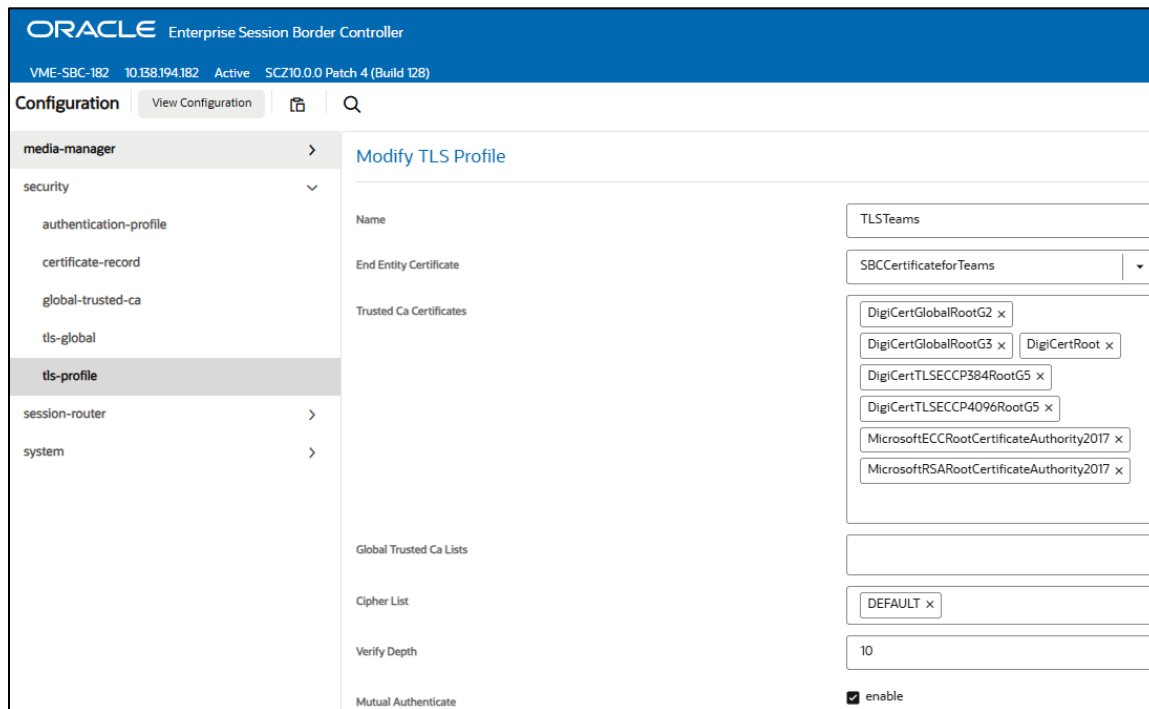
6.3.2 TLS Profile

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



- Select OK at the bottom

Next, we'll move to securing media between the SBC and Microsoft Teams.

6.3.3 Media Security

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

6.3.3.1 SDES-Profile

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

In the SBC's GUI, on the bottom left, you will need to enable the switch "Show All" to access the media security configuration elements.

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

Please note, if you have media bypass enabled in your environment, the lifetime value of 31 is required for Teams clients to decrypt SRTP packets sent by the Oracle SBC.

- Select OK at the bottom

6.3.3.2 Media Security Policy

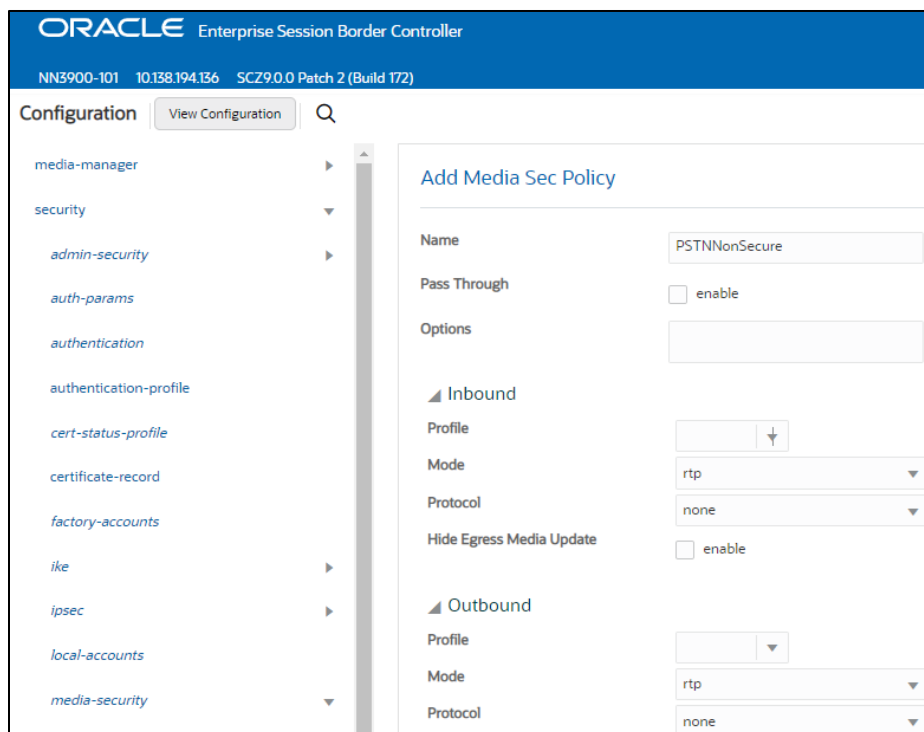
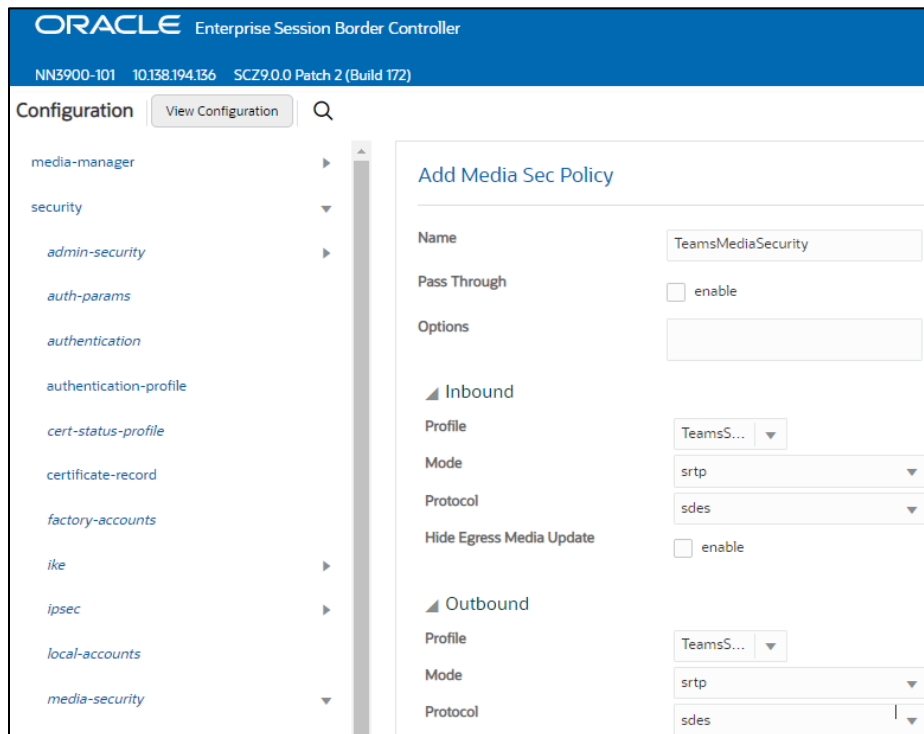
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any) and, if SRTP needs to be used, the sdes-profile that needs to be used

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



- Select OK at the bottom of each when finished.

This finishes the security configuration portion of the application note. We'll now move on to configuring media and transcoding.

6.4 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

6.4.1 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 than usual, so to support this, we configure the following media profiles on the SBC.

This is an optional configuration, and only needs to be implemented on the SBC if you are planning to use the SILK codec or wideband comfort noise between the SBC and Microsoft Phone System Direct Routing.

GUI Path: session-router/media-profile

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

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The main content area is titled "Media Profile" and contains a table with the following data:

Action	Sel...	Name	Subname	Media Type	Payload Type	Transport	Clock Rate
:	<input type="checkbox"/>	CN	wideband	audio	118	RTP/AVP	0
:	<input type="checkbox"/>	SILK	narrowband	audio	103	RTP/AVP	8000
:	<input type="checkbox"/>	SILK	wideband	audio	104	RTP/AVP	16000

- Select OK at the bottom of each after entering the required values

6.4.2 Codec Policies

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

While transcoding media codecs is optional, Microsoft does require the SBC generate Comfort Noise and RTCP packets towards Teams if the connection on the other side of the SBC (PSTN, IPPBX, etc..) does not support either. In order to satisfy this requirement, the SBC uses transcoding resources to generate those packets, which does require a codec policy be configured and assigned.

GUI Path: media-manager/codec-policy

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

Here is an example config of a codec policy used for the SBC to generate CN packets towards Teams.

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The top navigation bar includes the Oracle logo and the text 'Enterprise Session Border Controller'. Below this, the system information 'NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)' is displayed. The main interface is divided into a left sidebar and a main content area. The sidebar, under the 'Configuration' heading, shows a tree view with 'media-manager' selected, and 'codec-policy' highlighted. The main content area is titled 'Add Codec Policy' and contains the following fields:

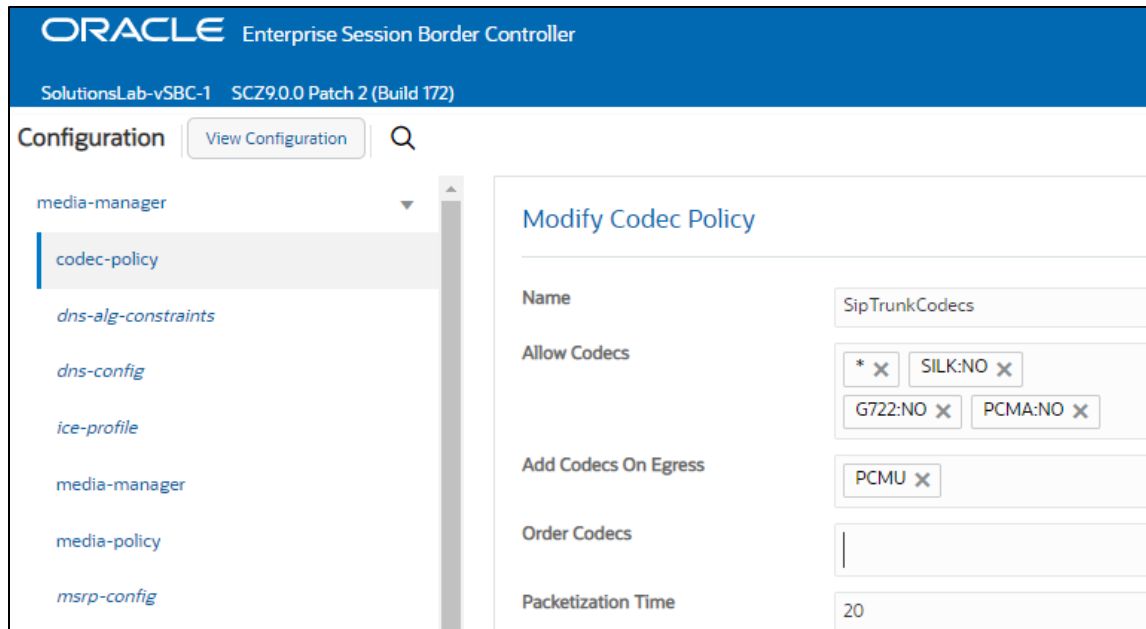
Name	addCN
Allow Codecs	* x
Add Codecs On Egress	CN x
Order Codecs	
Packetization Time	20

If you have chosen to configure the [media profiles](#) in the previous section to use SILK or wideband CN, you would set your codec policy to add them on egress. Here is an example:

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The top navigation bar includes the Oracle logo and the text 'Enterprise Session Border Controller'. Below this, the system information 'NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)' is displayed. The main interface is divided into a left sidebar and a main content area. The sidebar, under the 'Configuration' heading, shows a tree view with 'media-manager' selected, and 'codec-policy' highlighted. The main content area is titled 'Modify Codec Policy' and contains the following fields:

Name	addCNandSILK
Allow Codecs	* x
Add Codecs On Egress	CN x SILK::wideband x

Lastly, since some SIP Trunks may have issues with the codecs being offered by Microsoft Teams, you can create another codec policy to remove unwanted or unsupported codecs from the request/responses to your Sip Trunk provider.



- Select OK at the bottom

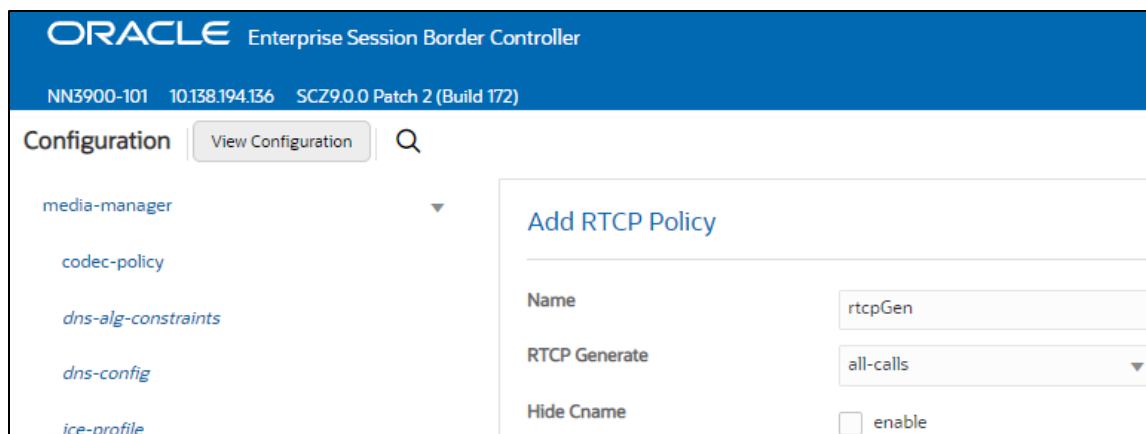
6.4.3 RTCP Policy

The following RTCP policy needs to be configured for the Oracle SBC to generate RTCP sender reports toward Microsoft Teams.

GUI Path: media-manager/rtcp-policy

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

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



FYI, for the SBC to generate RTCP sender reports to Teams, the realm in which this policy is assigned must also have a codec policy assigned. This is to evoke the required transcoding resources needed to generate RTCP packets.

- Select OK

6.4.4 ICE Profile

Interactive Connectivity Establishment - Session Traversal Utility for NAT (ICE STUN lite mode) enables an Advanced Media Termination client to perform connectivity checks, and can provide several STUN servers to the browser. ICE STUN support requires configuring an ICE Profile

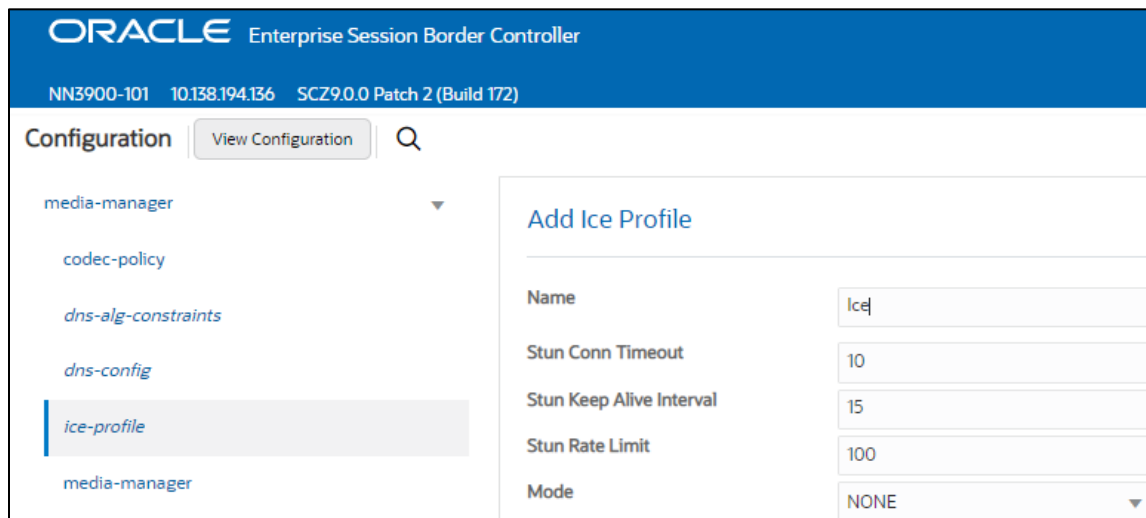
The use of ICE is required only if using Teams with Media Bypass enabled.

This is the only Oracle SBC configuration difference between Media Bypass and Non Media Bypass deployments.

GUI Path: media-manager/ice-profile

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

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



The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top header displays the Oracle logo and version information: NN3900-101, 10.138.194.136, SCZ9.0.0 Patch 2 (Build 172). The main content area is titled 'Configuration' and features a search bar and a 'View Configuration' button. A navigation menu on the left lists various configuration sections: media-manager, codec-policy, dns-alg-constraints, dns-config, ice-profile (highlighted), and media-manager. The 'Add Ice Profile' form contains the following fields:

Name	Ice1
Stun Conn Timeout	10
Stun Keep Alive Interval	15
Stun Rate Limit	100
Mode	NONE

In some environments, it may be necessary to change the default values for Stun Conn Timeout, Stun Keep Alive Interval, and Stun Rate Limit to a value of 0 (zero).

Select OK at the bottom.

This concludes the configuration for transcoding and Advanced Media Termination options on the SBC. We can now move to setup Media.

6.5 Media Configuration

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

6.5.1 Media Manager

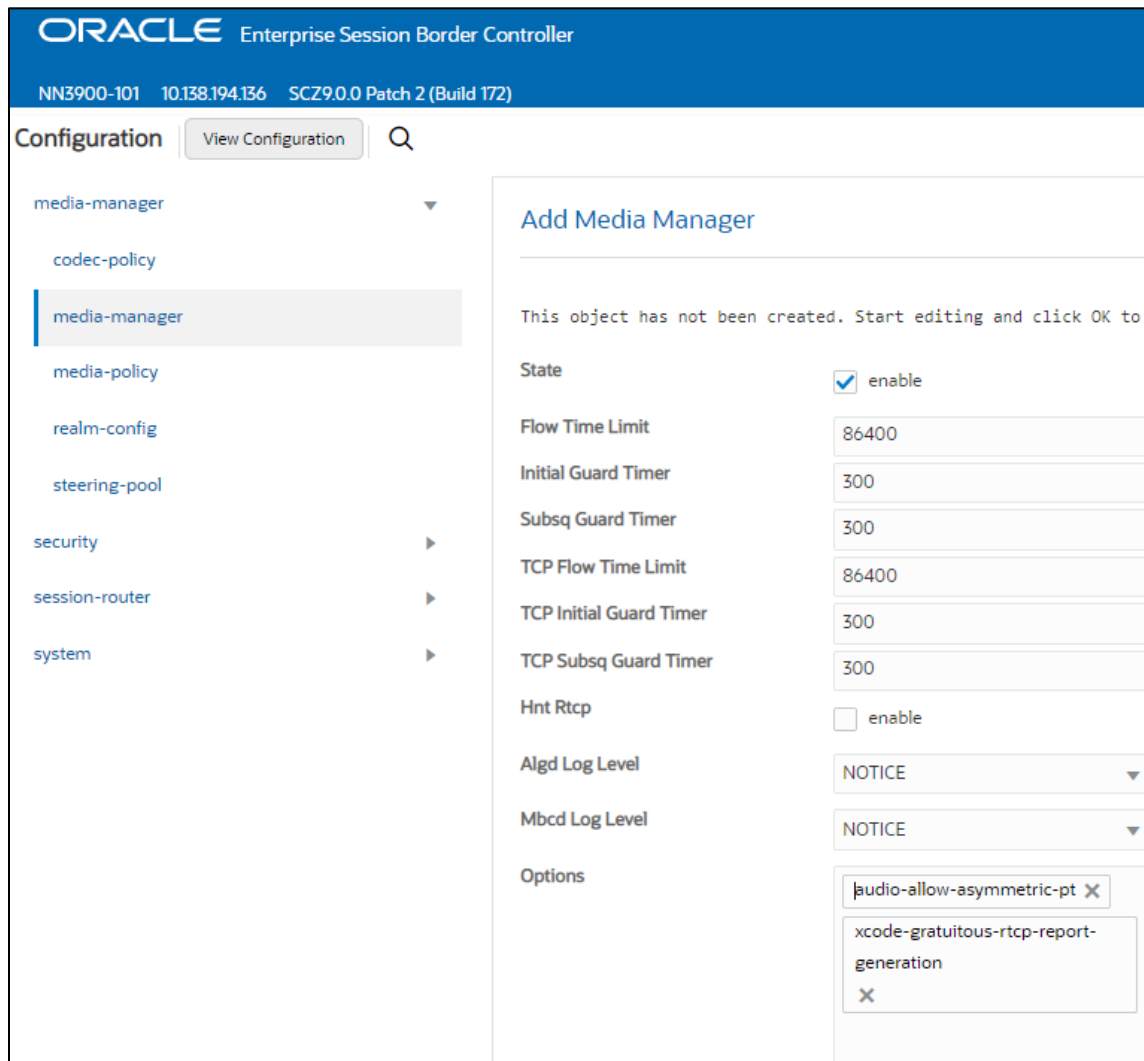
To configure media functionality on the SBC, you must first enable the global media manager

GUI Path: media-manager/media-manager

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

The following two hidden options are recommended for the global media manager when interfacing with Microsoft Teams Phone System Direct Routing.

- **audio-allow-asymmetric-pt:** Provides transcoding support for asymmetric dynamic payload types enables the Oracle® Session Border Controller to perform transcoding when the RTP is offered with one payload type and is answered with another payload type.
- **xcode-gratuitous-rtcp-report-generation:** This option allows the Oracle SBC to generate a Real-Time Transport Control Protocol (RTCP) Receiver Report separately from the default Sender-Receiver Report (RFC 3550). This option requires a reboot to take effect.



- Click OK at the bottom

6.5.2 Realm Config

Realms are a logical distinction representing routes (or groups of routes) reachable by the Oracle® Session Border Controller and what kinds of resources and special functions apply to those routes. Realms are used as a basis for determining ingress and egress associations to network interfaces.

GUI Path; media-manger/realm-config

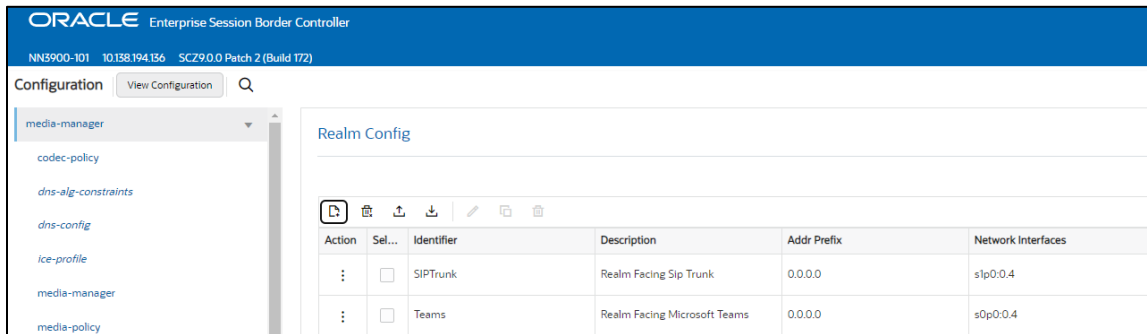
ACLI Path: config t→media-manger→realm-config

- Click Add, and use the following table as a configuration example for the realms. The following parameters are all required unless mentioned as optional below.

Config Parameter	Teams Realm	PSTN Realm
Identifier	Teams	SipTrunk
Network Interface	s0p0:0	s1p0:0
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Media Sec policy	TeamsSecurityPolicy	PSTNNonSecure
Teams-FQDN	telechat.o-test06161977.com	
Teams-fqdn-in-uri	<input checked="" type="checkbox"/>	
Sdp-inactive-only	<input checked="" type="checkbox"/>	
RTCP mux	<input checked="" type="checkbox"/>	
Refer Call Transfer	Enabled	
ice profile	Ice (required for media bypass only)	
Codec policy	addCN	SipTrunkCodecs
RTCP policy	rtcpGen	
Access-control-trust-level	HIGH	HIGH

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

- Network Interface
- Media Security Policy
- Ice Profile (optional, only required if using Media Bypass)
- Codec Policy (optional on the PSTN Realm)
- RTCP Policy



- Select OK at the bottom of each

6.5.3 Steering Pools

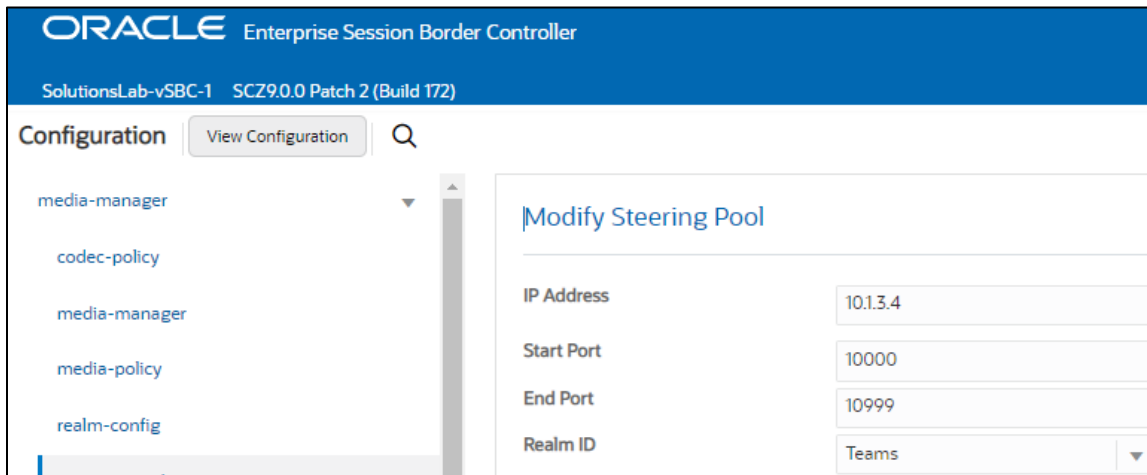
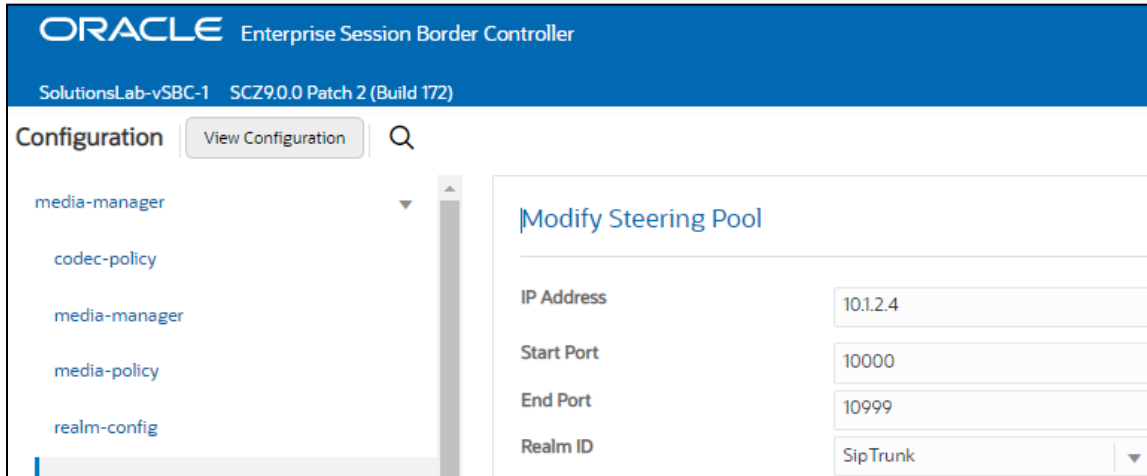
Steering pools define sets of ports that are used for steering media flows through the OCSBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We configure one steering pool for PSTN. The other facing Teams.

GUI Path: media-manger/steering-pool

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

- Click Add, and use the below examples to configure



- Select OK at the bottom

We will now work through configuring what is needed for the SBC to handle SIP signaling.

6.6 Sip Configuration

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

6.6.1 Sip-Config

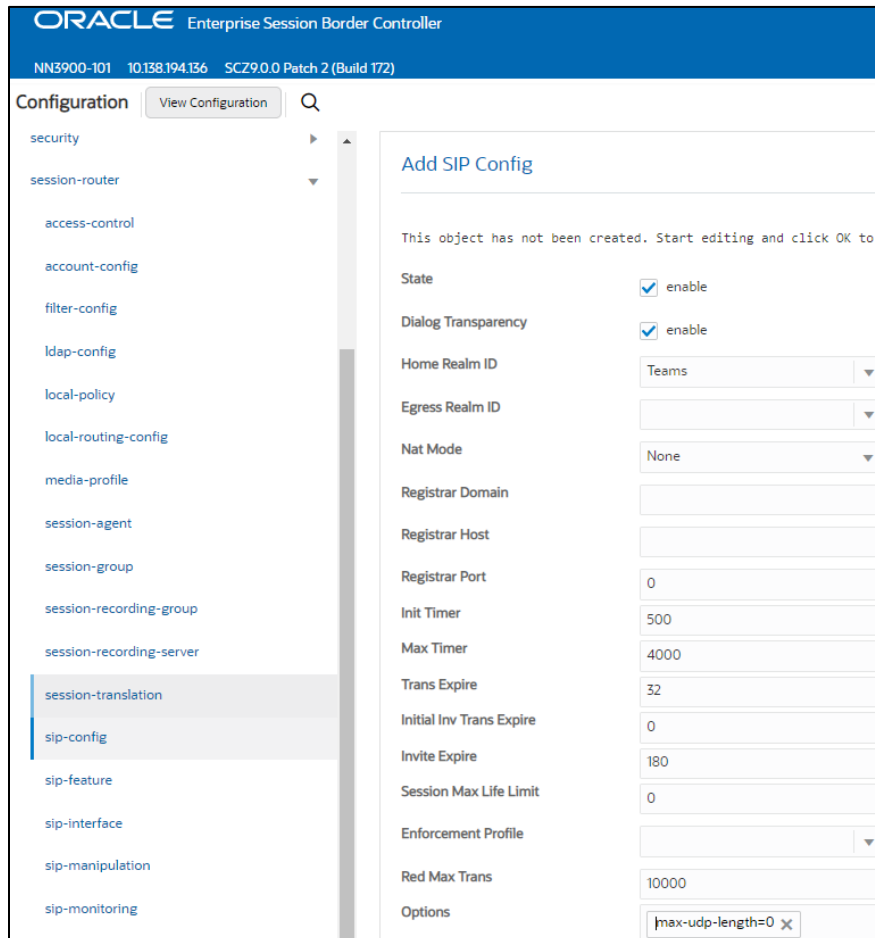
To enable sip related objects on the Oracle SBC, you must first configure the global Sip Config element:

GUI Path: session-router/sip-config

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

There are only two recommended changes/additions to the global Sip Config.

- Set the home realm ID parameter to Teams Realm, and add the following hidden option:
- **Max-udp-length=0**: Setting this option to zero (0) forces sipd to send fragmented UDP packets. Using this option, you override the default value of the maximum UDP datagram size (1500 bytes; sipd requires the use of SIP/TCP at 1300 bytes).



- Select OK at the bottom

6.6.2 Replaces Header Support

The Oracle® Session Border Controller supports the Replaces header in SIP messages according to RFC 3891. The header, included within SIP INVITE messages, provides a mechanism to replace an existing early or established dialog with a different dialog. The different dialog can be used for Microsoft Teams services such as call parking, attended call transfer and various conferencing features.

The Oracle SBC's support for Replaces header is required to properly interwork with Microsoft Teams, but Microsoft Teams does not support the use of Replaces header. In other words, Microsoft sends Replaces to the SBC, the SBC cannot send Replaces to Microsoft.

To configure support for Replaces, we configure the following:

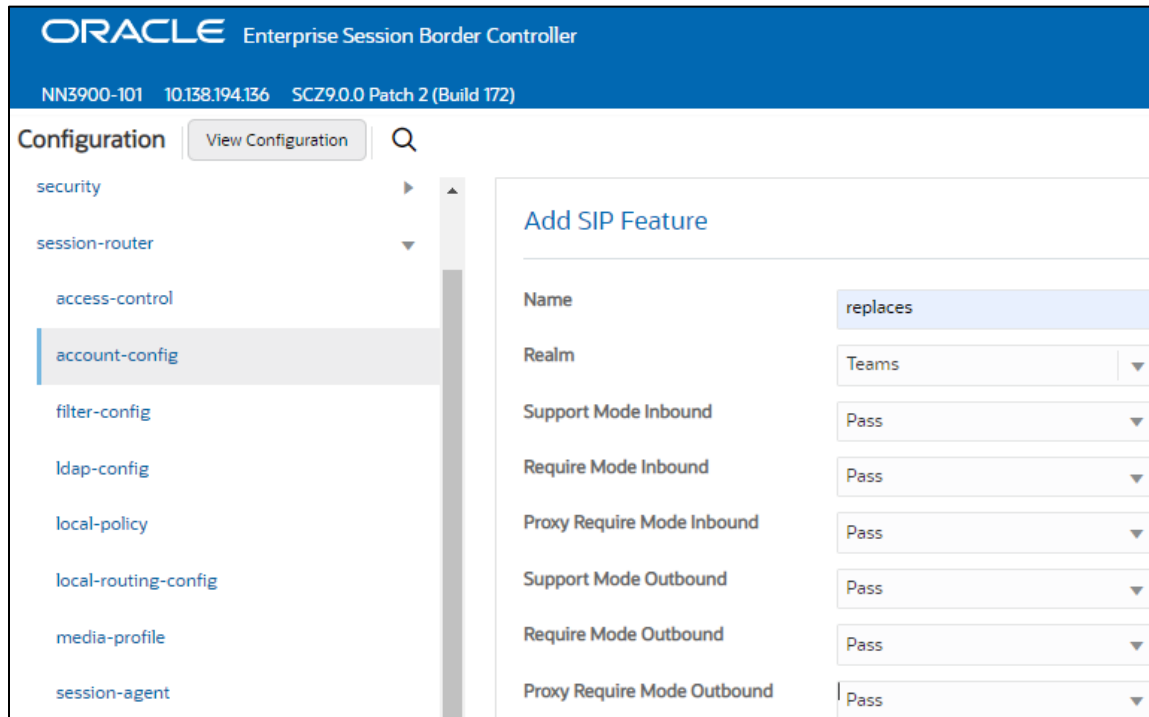
6.6.2.1 Sip Feature

The sip feature configuration element allow the SBC to support the Replaces value in the SIP Require and Supported Headers to and from Microsoft Teams.

GUI Path: session-router/sip-feature

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

Click add and use the following to configure:



- Click OK at the bottom

6.6.2.2 Sip Profile

Sip Profile, once configured and assigned to a sip interface, will act on a Replaces header when received by Microsoft teams to replace a dialog.

GUI Path: session-router/sip-feature

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

The toggle switch "Show All" on the bottom left must be enabled to reveal the sip-profile option.

- Click OK at the bottom

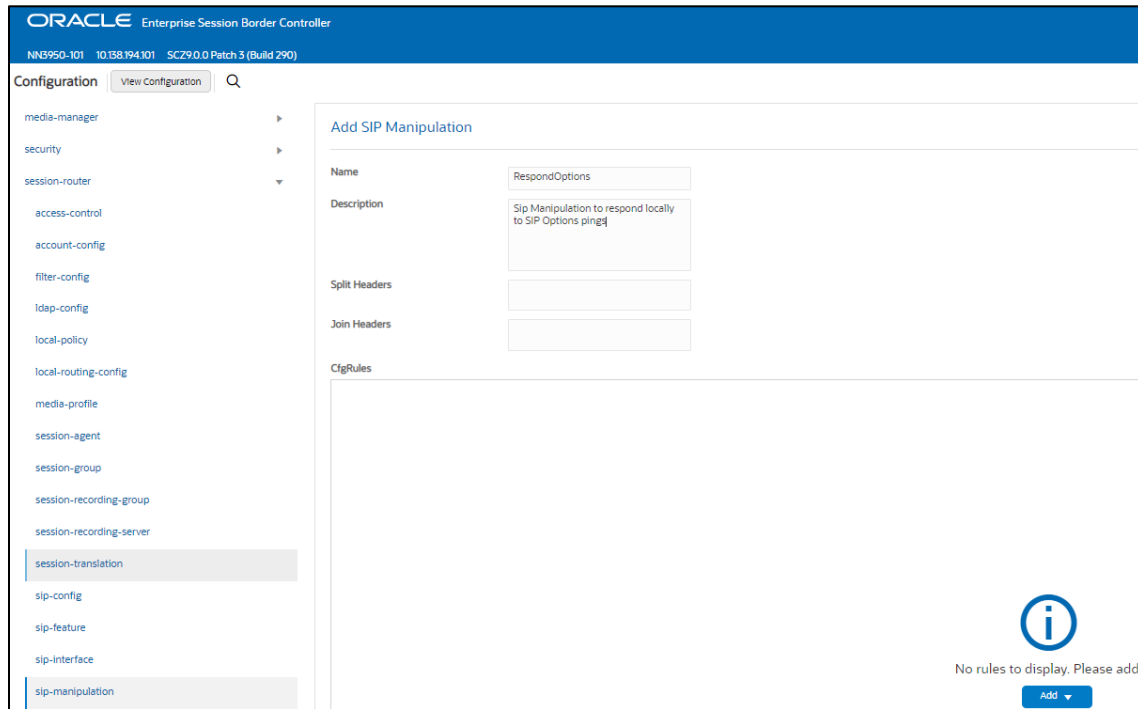
6.6.3 Sip Manipulation

To ensure the SBC generates a 200OK response to SIP Options messages received from Teams, we'll configure the following sip-manipulation rule

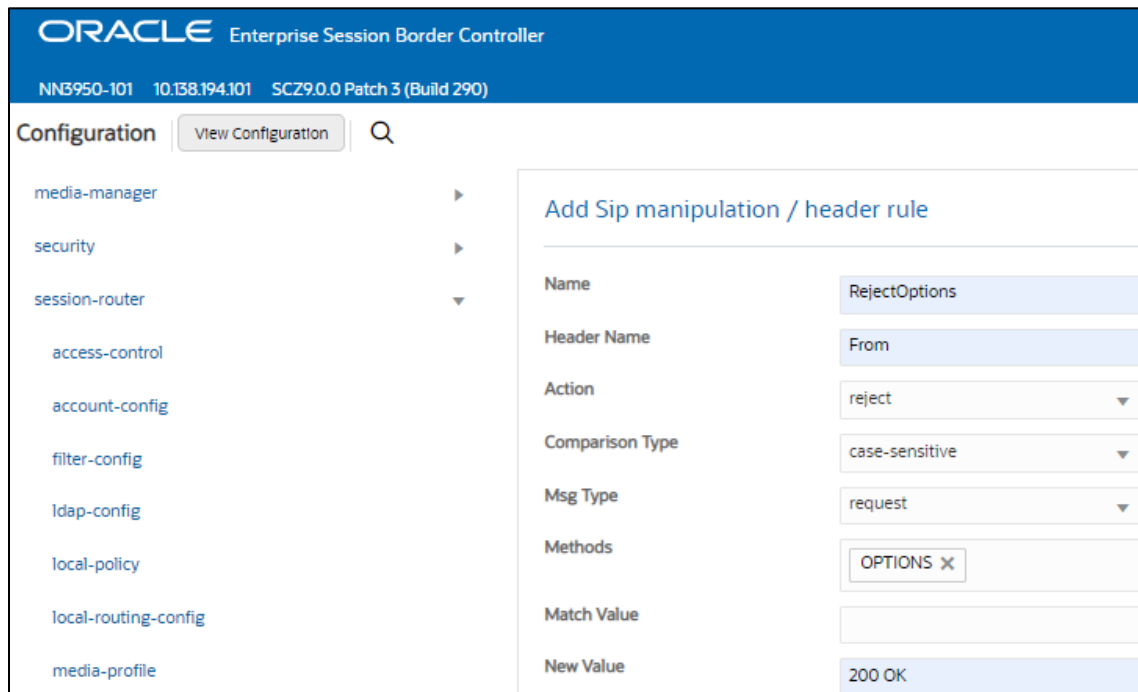
GUI Path: session router/sip manipulation

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

Click Add, and use the following example to configure:



Next, under CfgRules, select “header rule” in the “Add” drop down menu:



- Click OK at the bottom when finished

6.6.4 Sip Interface

The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages

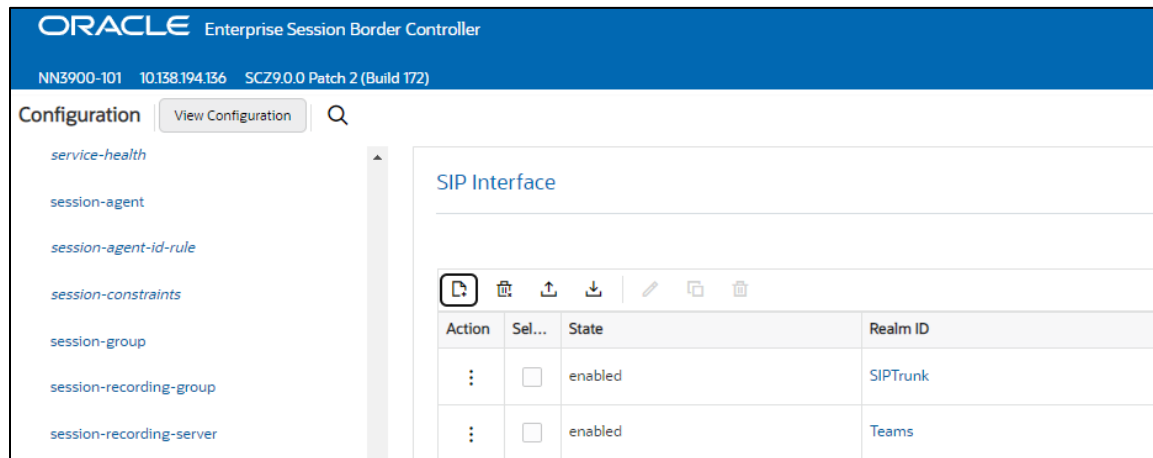
Configure two sip interfaces, one associated with PSTN Realm, and the other for Teams.

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		forreplaces
Sip Port Config Parmeter	Sip Trunk	Teams
Address	10.1.2.4	10.1.3.4
Port	5060	5061
Transport protocol	UDP	TLS
TLS profile		TeamsTLSProfile
Allow anonymous	agents-only	all
In Manipulationid		RespondOptions



Notice this is where we assign the TLS profile configured under the [Security](#) section of this guide, the sip-profile which allows the SBC to act on the Replaces header when received by Microsoft Teams, and the sip-manipulation which ensures the SBC responds locally to SIP Options.

- Select OK at the bottom of each when applicable

6.6.5 Session Agents

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

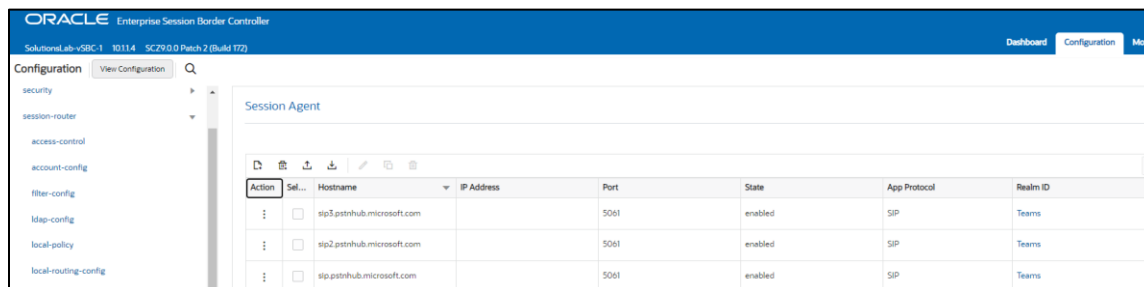
GUI Path: session-router/session-agent

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

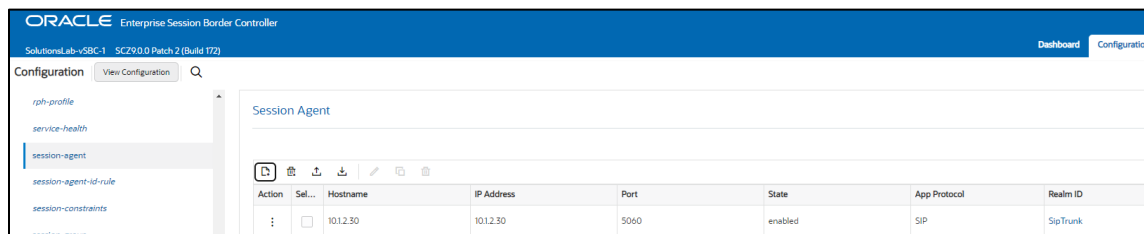
You will need to configure three Session Agents for the Microsoft Direct Routing Interface

- 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	10	10	10
Refer Call Transfer	enabled	enabled	enabled



Next, we'll configure a session agent for PSTN.



- Select OK at the bottom

6.6.6 Session Group

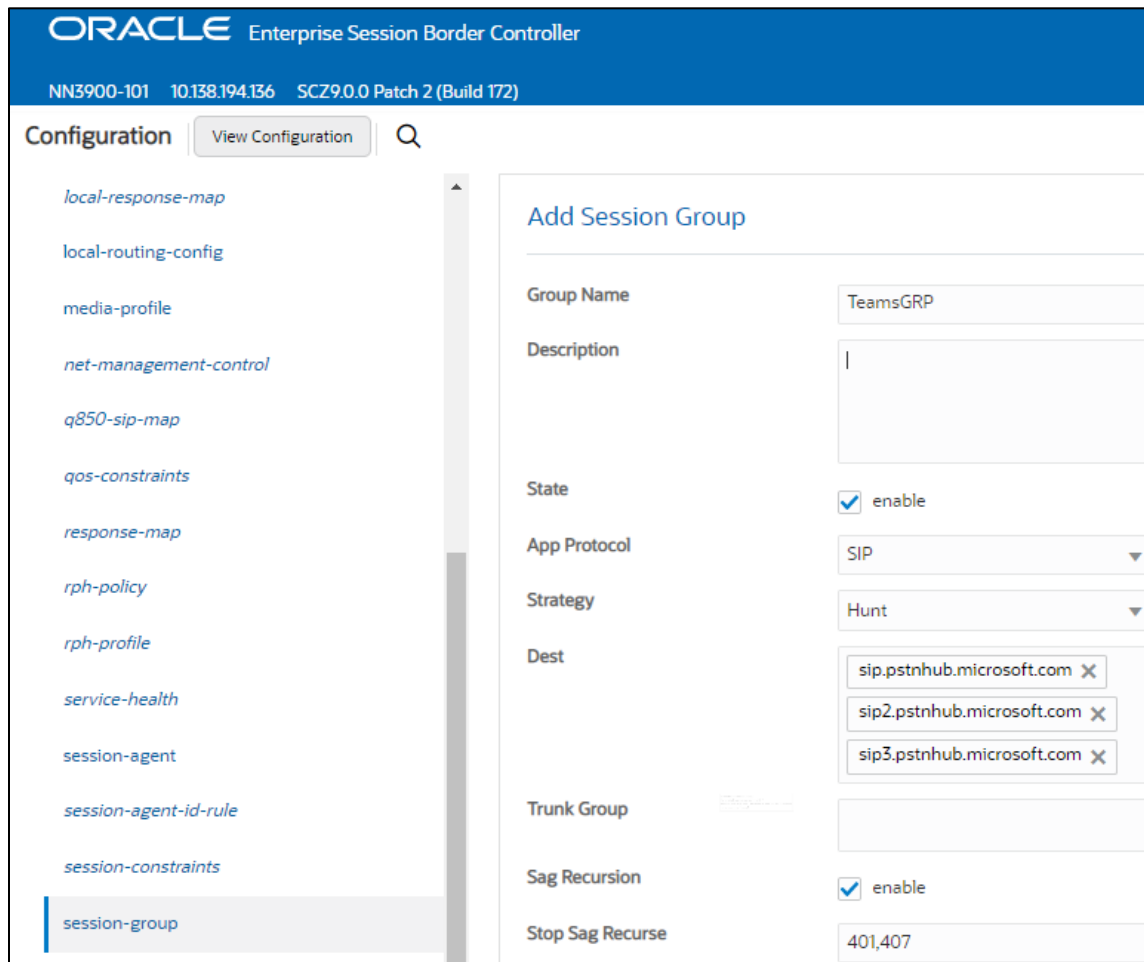
A session agent group allows the SBC to create a load balancing model:

All three Teams session agents configured above will be added to the group. The session agents listed under destination must be in this order, and the strategy must be set to HUNT.

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:



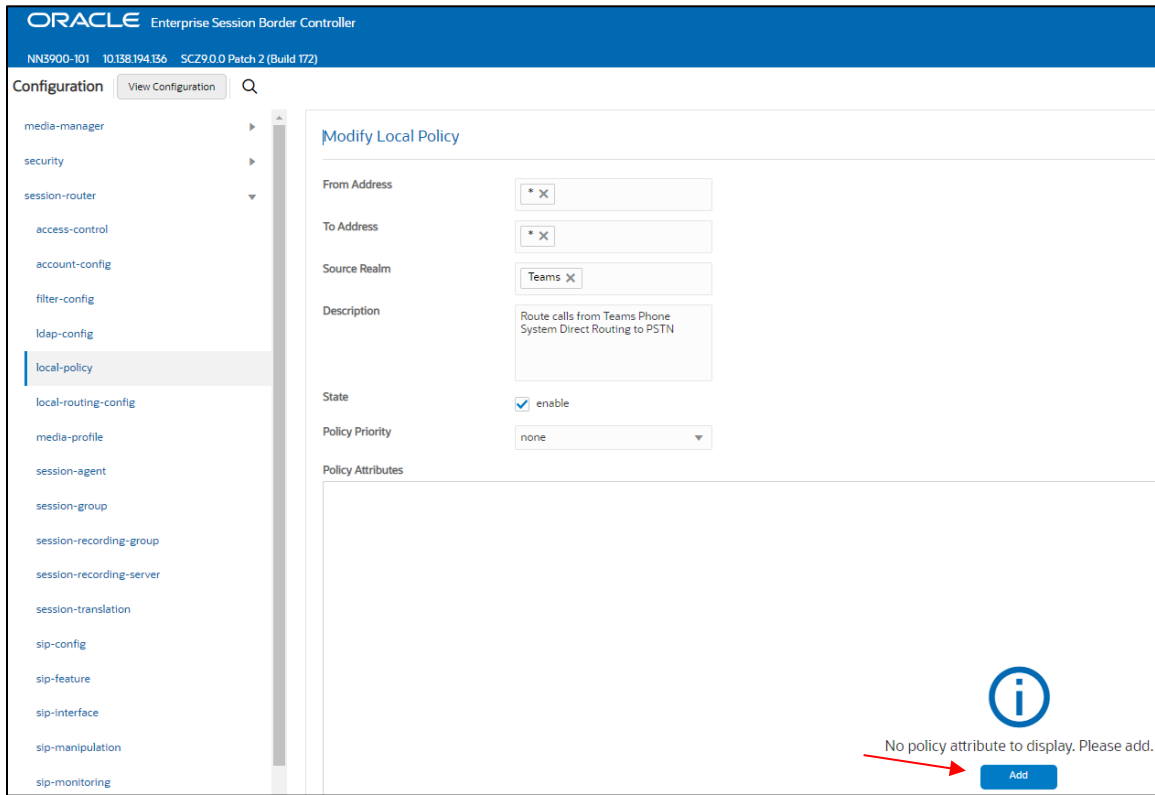
- Click OK at the bottom

6.7 Routing Configuration

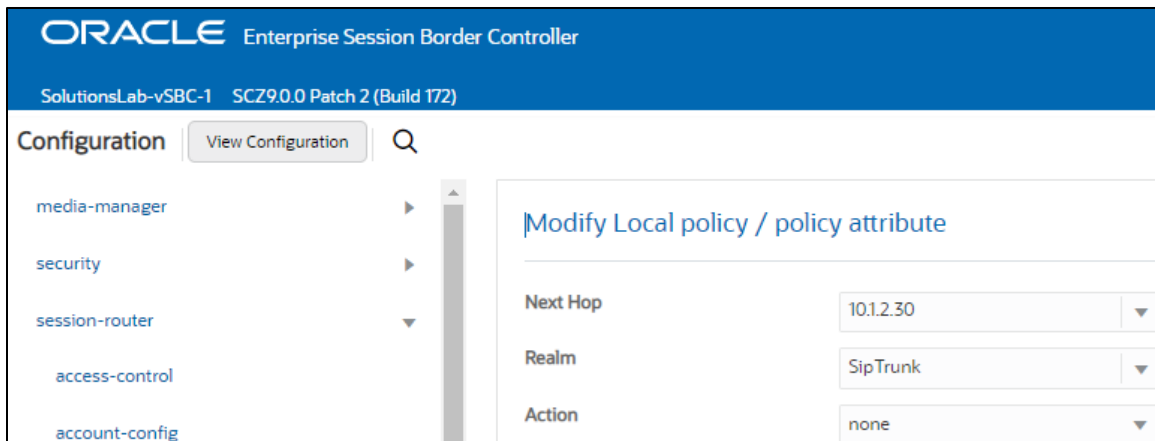
Now that a majority of the signaling, security and media configuration is in place, we can configure the SBC to route calls from one end of the network to the other. The SBC has multiple routing features that can be utilized, but for the purposes of this example configuration, we'll configure local policies to route calls from Microsoft Teams to our Sip trunk, and vice versa...

GUI Path: session-router/local-policy

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



After entering values for to and from address and source realm, click Add under policy attribute to configure the next hop destination.



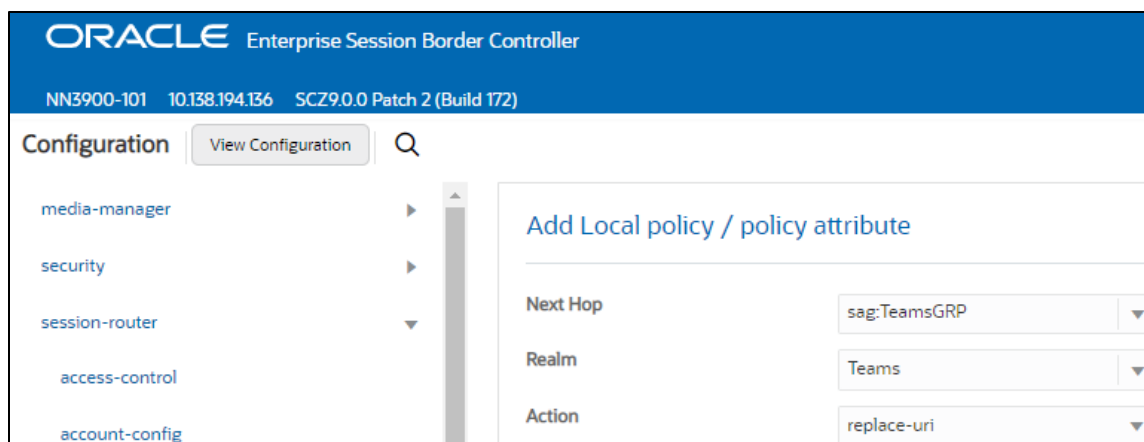
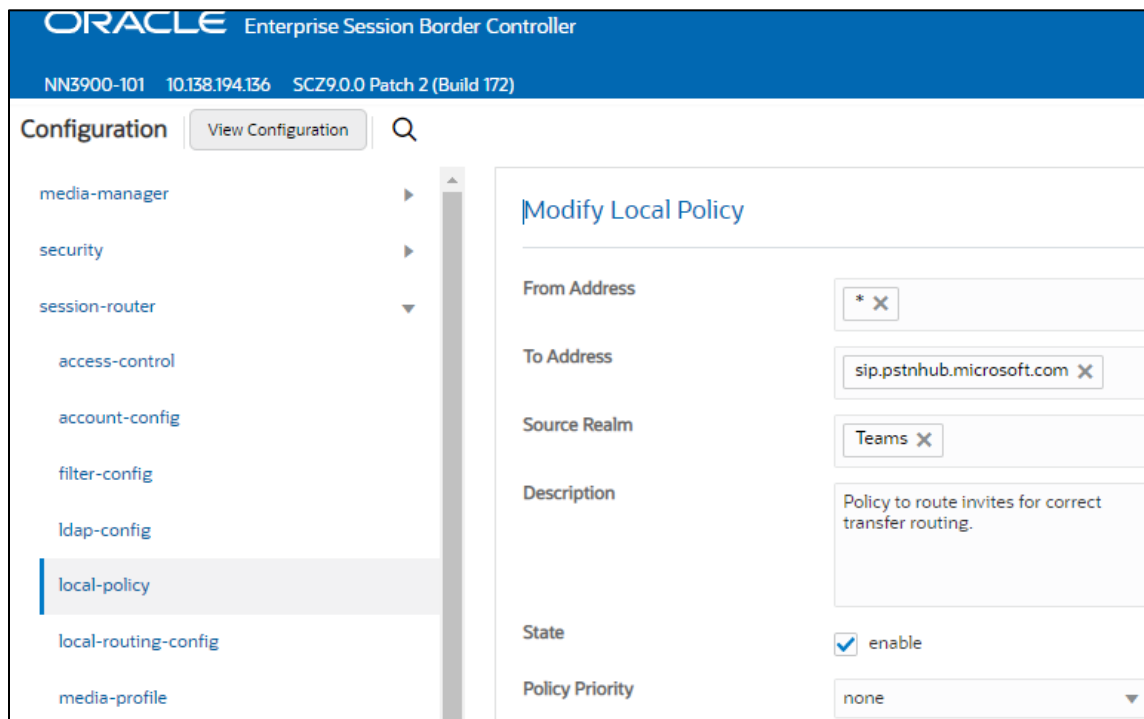
Next, we'll setup routing from our SIP Trunk to Microsoft Teams:

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes the Oracle logo and the text 'Enterprise Session Border Controller'. Below this, the system version 'NN3900-101 10.138.194.136 SCZ9.0.0 Patch 2 (Build 172)' is displayed. The left sidebar contains a 'Configuration' menu with various options, including 'local-policy' which is currently selected. The main content area is titled 'Modify Local Policy' and contains several input fields: 'From Address' and 'To Address' (both with a clear 'X' button), 'Source Realm' (set to 'SIPTrunk'), and a 'Description' text area. Below these are 'State' (checked 'enable') and 'Policy Priority' (set to 'none'). At the bottom, there is a 'Policy Attributes' section which is currently empty, accompanied by an information icon and the text 'No policy attribute to display. Please add.' with an 'Add' button.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for adding a new policy attribute. The top navigation bar and system version information are identical to the previous screenshot. The left sidebar shows the 'Configuration' menu with 'account-config' selected. The main content area is titled 'Add Local policy / policy attribute' and features three dropdown menus: 'Next Hop' (set to 'sag:TeamsGRP'), 'Realm' (set to 'Teams'), and 'Action' (set to 'replace-uri').

- Select OK when applicable on each screen

All transfers that use an SIP Refer message must go through the [Microsoft Teams infrastructure](#). When the Microsoft SIP proxy sends an SIP Refer message to the Oracle SBC, an SIP Invite message should be returned to the SIP proxy, not to PSTN or to any other destination. It is true even if the call is transferred to an external PSTN number. To accommodate this requirement, we can configure another routing policy on the Oracle SBC to ensure call Invites generated by the SBC off SIP REFER's are routed properly.



- Select OK when applicable.

6.8 SIP Access Controls

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/en/industries/communications/session-border-controller/9.0.0/security/security-guide.pdf>

However. While some values are environment specific, there are some basic security parameters that can be implemented on the SBC that will help secure your setup.

1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high
2. Set the access control trust level on public facing [realms](#) to HIGH

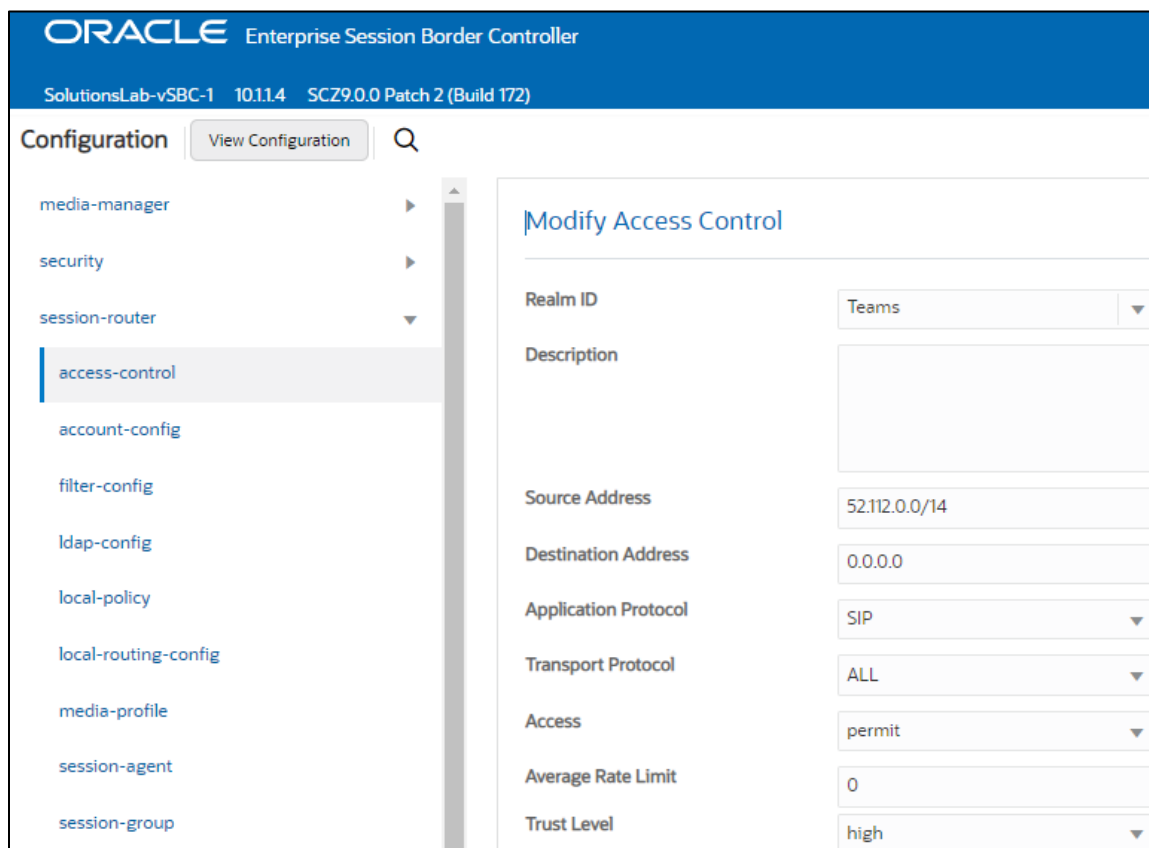
Microsoft Teams has two subnets, 52.112.0.0/14 and 52.120.0.0/14 that must be allowed to send traffic to the SBC. Both must be configured as an access control on the Oracle SBC and associated with the realm facing Teams.

Use this example to create ACL's for all MSFT Teams subnets. This example can be followed for any of the public facing interfaces, ie...SipTrunk, etc...

GUI Path: session-router/access-control

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

Use this example to create ACL's for both MSFT Teams subnets, 52.112.0.0/14, and 52.120.0.0/14.



- Select OK at the bottom

This concludes the required configuration of the SBC to properly interface with Microsoft Teams Phone System Direct Routing.

7 Oracle SBC Configuration Assistant

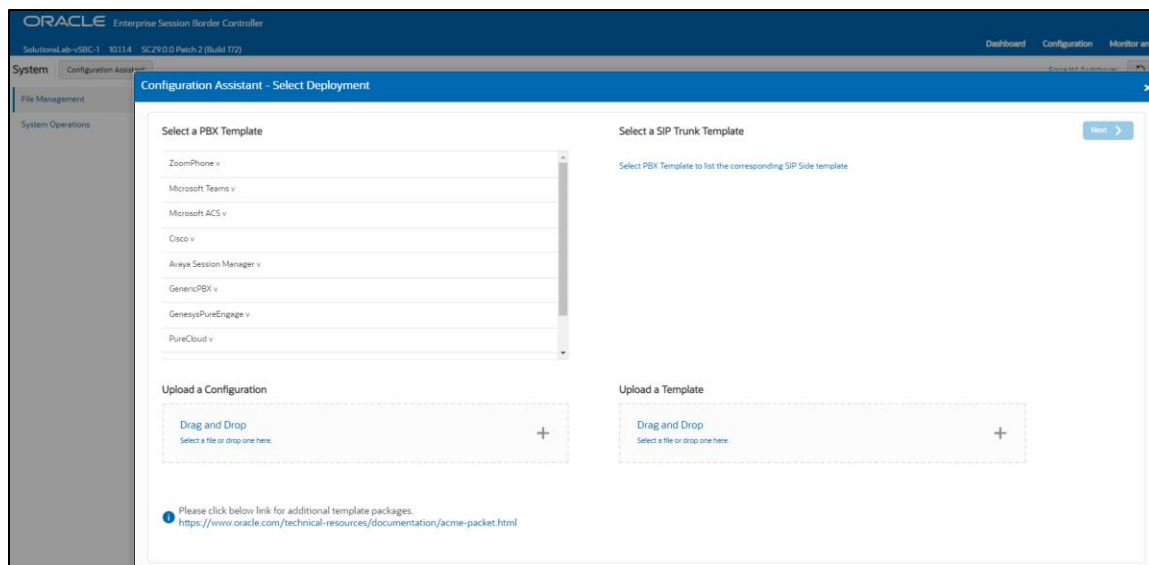
When you first log on to the E-SBC, the system requires you to set the configuration parameters necessary for basic operation. To help you set the initial configuration with minimal effort, the E-SBC provides the Configuration Assistant. The Configuration Assistant, which you can run from the Web GUI or the Acme Command Line Interface (ACLI), asks you questions and uses your answers to set parameters for managing and securing call traffic between the SBC and Microsoft Teams Phone System. You can use the Configuration Assistant for the initial set up to make to the basic configuration. See "[Configuration Assistant Operations](#)" in the Web GUI User Guide and "[Run Configuration Assistant](#)" in the ACLI Configuration Guide

Configuration assistant is available starting in release nnSCZ840P5 and nnSCZ900p2.

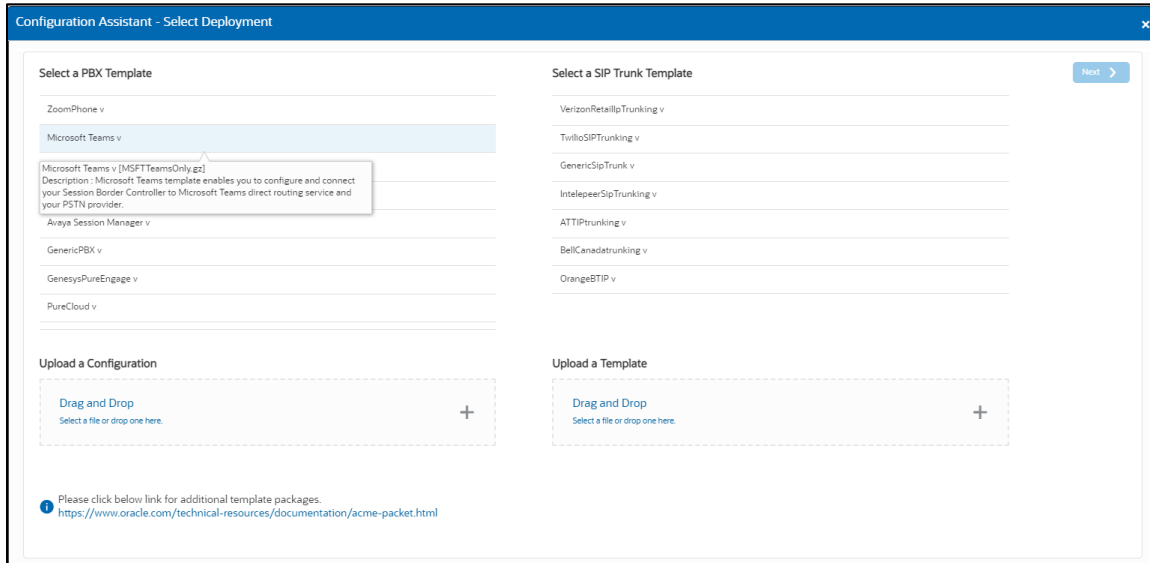
7.1 Microsoft Teams Configuration Assistant

The screenshots below are from an Oracle SBC GUI running 900p2.

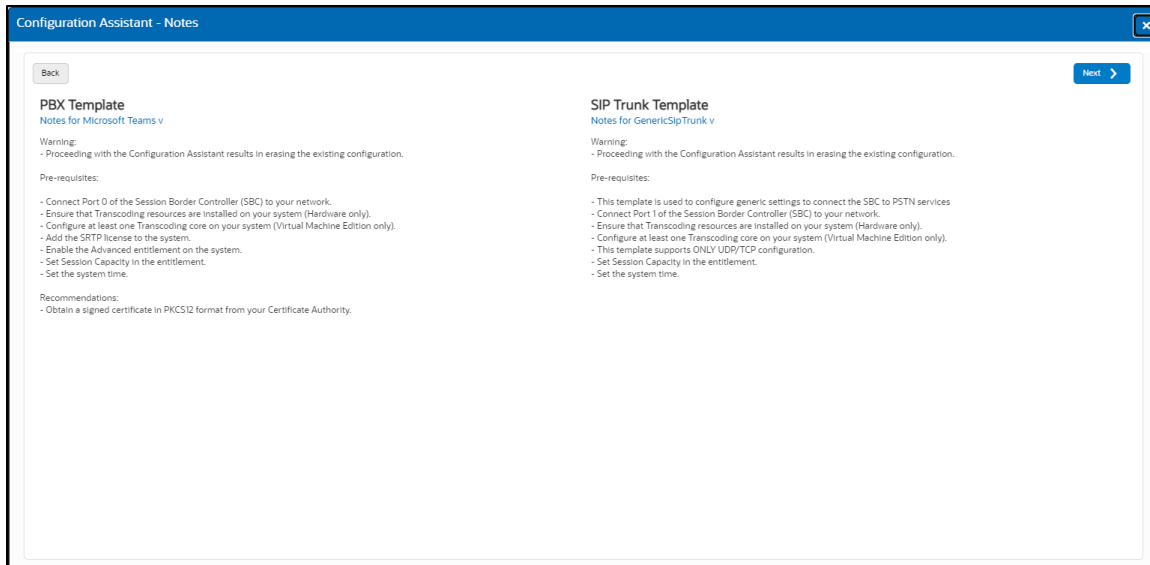
For a new SBC deployment, once access to the GUI is configured, you will see the following when logging in for the first time:



Under PBX template, we'll select Microsoft Teams template. This brings up a list of available sip trunk templates.



Select a sip trunk template and click next at the top to access the Notes page. Pay close attention to the information here, as this is a list of warnings, pre-requisites and recommendations:



Clicking “Next” on the Notes page triggers the configuration assistant to do a system check. This ensures that all the system requirements for the platform and sip trunk you have selected have been met before proceeding to configuration pages. If they have not been met, you will be greeted by a page providing the opportunity to setup entitlements, add license keys, etc...before moving on to the configuration. Once all requirements for your selected templates have been satisfied, you can proceed to the configuration pages.

Configuration Assistant - Microsoft Teams Network

Back 1 Microsoft Teams Network 2 Media 3 Transcoding 4 Trusted Certificate 5 SBC Certificate 6 PSTN Network 7 PSTN Session Agent 8 Transcoding 9 Additional Configuration Skip

Let's configure the interface that communicates with Microsoft Teams

Realm Name Required

Port Number Required

Slot Number Required

Network IP Address Required

Network IP subnet mask Required

Network Gateway IP Address Required

Primary DNS server IP Address Required

Follow the instructions on each page. Any field that is labeled required must contain an entry.

Once you have entered all information in required fields on all pages, select the option to Review in the top right of the screen:

Configuration Assistant - Additional Configuration

Microsoft Teams Network Media Transcoding Trusted Certificate SBC Certificate PSTN Network PSTN Session Agent Transcoding Additional Configuration Review

Let's configure Session Agent Capabilities

Do you want to enable OPTIONS towards PSTN? No Yes

Do you want SBC to handle call transfer from PSTN? No Yes

Do you want to enable session translation on toward your PSTN provider? No Yes

The left side of the review page contains all of the entries added on each page and allows for editing each page individually if necessary.

The right side displays the entire configuration created and when applicable, will also have a CSR tab that contains a certificate that can be signed by a CA authority.

Configuration Assistant - Summary

Download Apply

Microsoft Teams Network Edit

Realm Name	Port Number
Teams	Port 0
Slot Number	Network IP Address
Slot 0	10.1.3.4
Network IP subnet mask	Network Gateway IP Address
255.255.255.0	10.1.3.1
Primary DNS server IP Address	DNS Domain
8.8.8.8	telechat.o-test06161977.com

Media Edit

Do you want to enable Media Bypass?
enabled

Transcoding Edit

Do you want to enable transcoding features (Comfort Noise, RTP)? Do you want to select media codecs (SBC to Microsoft Teams)?
enabled enabled

Select media codecs
SILK

Trusted Certificate Edit

Do you want to install the Baltimore CyberTrust Root?

Configuration

Copy

```

certificate-record
  name BaltimoreRoot
  common-name Baltimore CyberTrust Root
certificate-record
  name TeamsCSR
  state California
  locality Redwood City
  organization Oracle Corporation
  unit Oracle C8U-LABS BOSTON
  common-name telechat.o-test06161977.com
codec-policy
  name PSTNCodecPolicy
  allow-codecs =
  add-codecs-on-egress PCMU
codec-policy
  name TeamsCodecPolicy
  allow-codecs =
  add-codecs-on-egress CN SILK
http-server
  name webServerInstance
ice-profile
  name ice
  stun-conn-timeout 0
  stun-keep-alive-interval 0
local-policy
  from-address =
  to-address =
  source-realm SipTrunk
  policy-attribute
    next-hop SAG:TeamsGrp
    realm Teams
local-policy
  ..

```

Once all the information has been reviewed and accepted, click Apply.

The SBC now presents the Epilogue.

Configuration Assistant - Epilogue

Back Confirm

Perform the following actions when the system comes up to complete the deployment ::

Actions to be performed for Microsoft Teams v

Security:

- If you opted to generate a CSR during the SBC certificate provisioning step, please make sure to import the signed certificate after the reboot.
- If you are going to use the SBC to interwork between SRTP and RTP, please make sure you assign the media security policy named "RTP" to the realm with non secure media.

Actions to be performed for GenericSipTrunk v

No more actions required for this template

Confirm, and then select reboot to apply the new configuration to the SBC.

Configuration Assistant - Apply Confirmation

If you proceed, the system erases the existing configuration and reboots.

Back Reboot

8 Verify Connectivity

8.1 Oracle SBC Options Pings

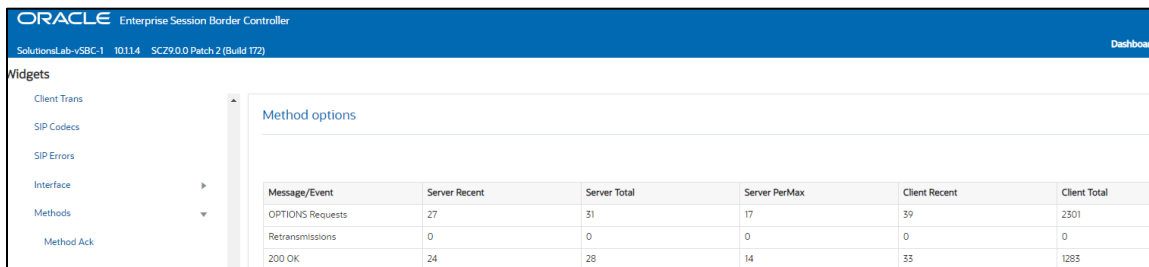
After you've paired the OCSBC with Direct Routing using the New-CsOnlinePSTNGateway PowerShell cmdlet, validate that the SBC can successfully exchange SIP Options with Microsoft Direct Routing.

While in the Oracle SBC 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/Method Options



Message/Event	Server Recent	Server Total	Server PerMax	Client Recent	Client Total
OPTIONS Requests	27	31	17	39	2301
Retransmissions	0	0	0	0	0
200 OK	24	28	14	33	1283

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

8.2 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](#)

9 Syntax Requirements for SIP Invite and SIP Options:

Microsoft Teams Hybrid Voice Connectivity interface has requirements for the syntax of SIP messages. This section covers high-level requirements to SIP syntax of Invite and Options messages. The information can be used as a first step during troubleshooting when calls don't go through. From our experience most of the issues are related to the wrong syntax of SIP messages.

9.1 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

9.2 Requirements for Invite Messages and Final Responses

Picture 1 Example of INVITE and 200OK message

```
INVITE sip:17815551345@sip.pstnhub.microsoft.com:5061;user=phone;transport=tls SIP/2.0
Via: SIP/2.0/TLS 10.1.3.4:5061;branch=z9hG4bKcm87o2205o1rkbb1vnp0.1
Max-Forwards: 65
From: "Test" <sip:+17815551212@telechat.o-test06161977.com:5060;user=phone>;tag=19fc69fc0a020100
To: <sip:+17815551345@10.1.2.4:5060;user=phone>
Call-ID: 1-19fc69fc0a020100.318f0133@68.68.117.67
CSeq: 2 INVITE
Contact: <sip:+17815551212@telechat.o-test06161977.com:5061;user=phone;transport=tls>;sip.ice
Allow: ACK, BYE, CANCEL, INVITE, OPTIONS, PRACK, REFER
User-Agent: T7100/3.0
Supported: 100rel
Content-Type: application/sdp
Content-Length: 550
X-MS-SBC: Oracle/AP3900/8.4.0p7
```

```
SIP/2.0 200 Ok
FROM: <sip:+ 17815551212@10.1.2.4:5060;user=phone>;tag=e520638effffff2c68c
TO: <sip:+ 17815551345@telechat.o-test06161977.com:5060;user=phone>;tag=19ec632b0a020100
CSEQ: 1 INVITE
CALL-ID: 1-19ec632b0a020100.74184225@68.68.117.67
VIA: SIP/2.0/TLS 52.114.32.169:5061;branch=z9hG4bKf74789d
Contact: <sip:+17815551345@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: 477
Supported: timer,replaces
Session-Expires: 1800; refresher=uas
X-MS-SBC: Oracle/AP3900/8.4.0p7-ws
```

9.2.1 Contact Header-Invite and Final Response

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

9.3 Requirements for OPTIONS Messages

Example of OPTIONS message

```
OPTIONS sip:sip.pstnhub.microsoft.com:5061;transport=tls SIP/2.0
Via: SIP/2.0/TLS 10.1.3.4:5061;branch=z9hG4bKumatcr30fod0o13gi060
Call-ID: 4cf0181d4d07a995bcc46b8cd42f9240020000sg52@10.1.3.4
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:telechat.o-test06161977.com >
X-MS-SBC: Oracle/AP3900/8.4.0p7-ws
```

9.3.1 Contact Header-OPTIONS:

- 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

10 Microsoft Teams Direct Routing Interface characteristics

The following table 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	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	
	Audio codecs	<ul style="list-style-type: none"> · G711 · Silk (Teams clients) · Opus (WebRTC clients) - Only if Media Bypass is used; · G729 · G722 	
Codecs	<ul style="list-style-type: none"> · CN <ul style="list-style-type: none"> o Required narrowband and wideband · RED – Not required · DTMF – Required · Events 0-16 · Silence Suppression – Not required 		

11 Appendix A

11.1 Oracle SBC TDM with Teams

Oracle® designed the Time Division Multiplexing (TDM) functionality for companies planning to migrate from TDM to SIP trunks by using a hybrid TDM-SIP infrastructure, rather than adopting VoIP-SIP as their sole means of voice communications. The TDM interface on the Oracle® Enterprise Session Border Controller (E-SBC) provides switchover for egress audio calls, when the primary SIP trunk becomes unavailable. You can use TDM with legacy PBXs and other TDM devices.

- Only the Acme Packet 1100 and the Acme Packet 3900 platforms support TDM, which requires the optional TDM card.
- TDM supports bidirectional calls as well as unidirectional calls.
- TDM operations require you to configure TDM Config and TDM Profile, as well as local policies for inbound and outbound traffic.
- The software upgrade procedure supports the TDM configuration.
- Options for the Acme Packet 1100 and the Acme Packet 3900 platforms include CallingLine Identification Presentation (CLIP) and Connected-Line Identification Presentation (COLP).
- Options for the Acme Packet 1100 platform include the four-port Primary Rate Interface (PRI), the Euro ISDN Basic Rate Interface (BRI), and the Foreign Exchange Office Foreign Exchange Subscriber (FXO-FXS) card.

11.1.1 Interface Requirements

- PRI—Digium 1TE133F single-port or Digium 1TE435BF four-port card.
- BRI—Digium 1B433LF four-port card
- FXS—Digium 1A8B04F eight-port card, green module (ports 1-4)
- FXO—Digium 1A8B04F eight-port card, red module (ports 5-8)

Oracle SBC Time Division Multiplexing (TDM) functionality has been fully tested with Microsoft Teams Phone System Direct Routing.

For further information on the setup and configuration of TDM on the Oracle SBC, please refer to the [TDM Configuration Guide](#)

12 Appendix B

12.1 Oracle SBC deployed behind NAT

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 IP as configured on both the SIP Interface and Steering Pool

- 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.

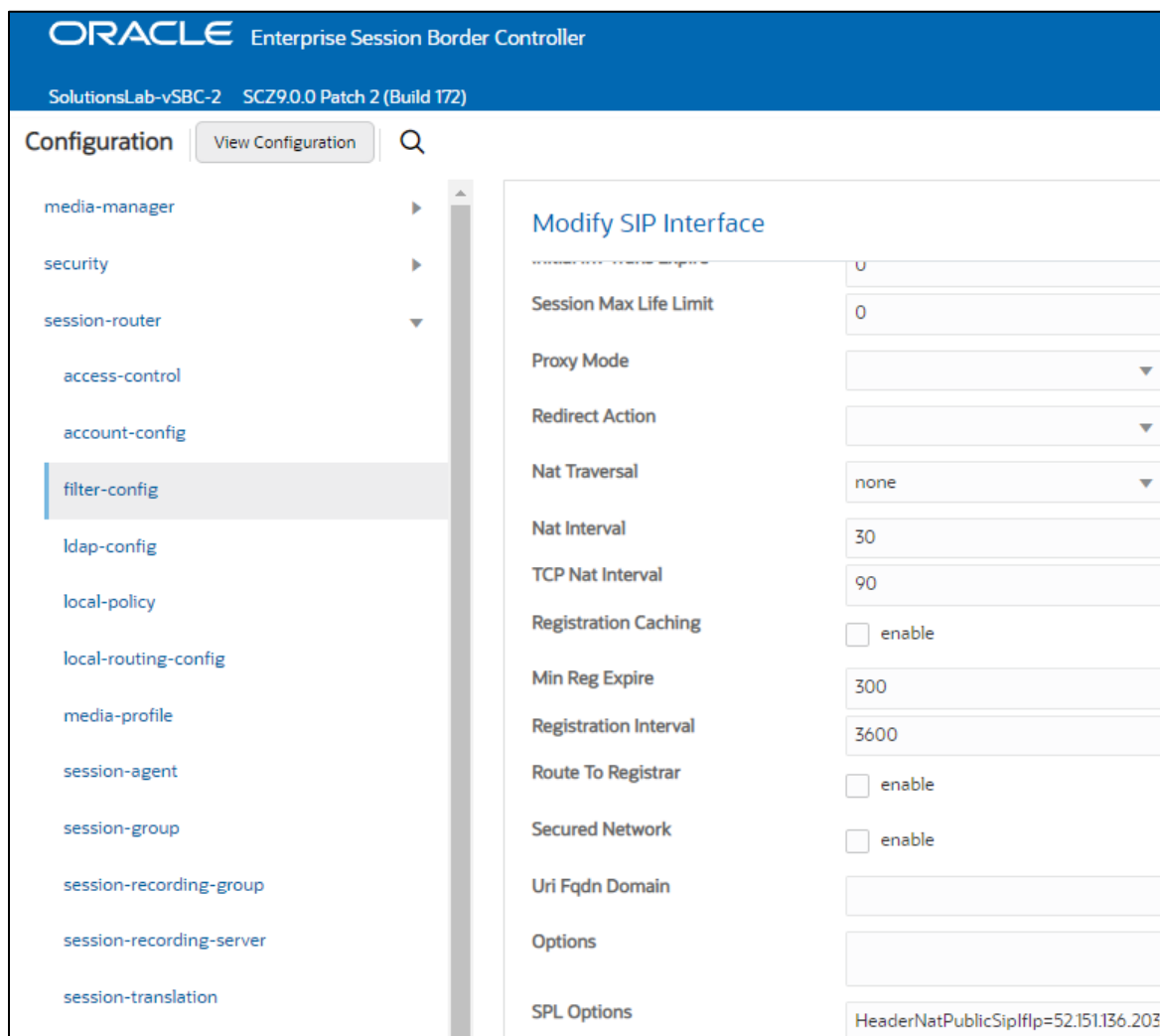
GUI Path: session-router/sip-interface

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

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.1.3.4

HeaderNatPublicSipIfIp is the public interface ip

HeaderNatPrivateSipIfIp is the private ip.



You will need to apply these options to every sip interface on the SBC that is connected through a NAT.

13 Appendix C

13.1 Ringback on Inbound Calls to Teams and Early Media

In certain deployments, on certain call flows, PSTN callers may experience silence on inbound calls to Microsoft Teams instead of an expected ring back tone.

When Teams receives an INVITE, after sending a 183 with SDP response back to the Oracle SBC, Teams does not play ring back. Microsoft's expectation is the Oracle SBC will signal appropriately to the Sip Trunk in order for local ring back to be generated.

To properly signal the trunk to play the ring back, the SBC presents a 180 Ringing response to the trunk instead of the 183 Session Progress received from Teams.

In order to accommodate the 183 with SDP message that signal early media in cases of simultaneous ringing set to IVR, etc... we inspect the SDP of the 183 received before converting it to 180 Ringing.

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 use a sip manipulation to strip the SDP from the 183. Next, we convert the 183 response to a 180 Ringing before forwarding it to the Sip Trunk.

Due to the complexity of this sip manipulation, the SBC ACLI output has been provided.

GUI Path: Session Router/sip-manipulation

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

This sip manipulation will be applied as the in-manipulationid on the Teams Sip Interface.

```

sip-manipulation
  name          Checkfor183
  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 $check183.$is183
    sdp-session-rule
      name      au
      action    manipulate
      sdp-line-rule
        name      checkclineforsbcip
        type      c
        action    store
        comparison-type pattern-rule
        match-value ^.(?!(10.1.3.4)).*$
  mime-sdp-rule
    name        delete183SDP
    msg-type    reply
    methods     Invite
    action      delete
    comparison-type boolean
    match-value $if183.$au.$checkclineforsbcip
  header-rule
    name        change183to180
    header-name @status-line
    action      manipulate
    comparison-type boolean
    match-value $if183.$au.$checkclineforsbcip
    element-rule
      name      changestatus
      type      status-code
      action    replace
      match-value 183
      new-value 180
    element-rule
      name      changereasonphrase
      type      reason-phrase
      action    replace
      match-value Session Progress
      new-value Ringing

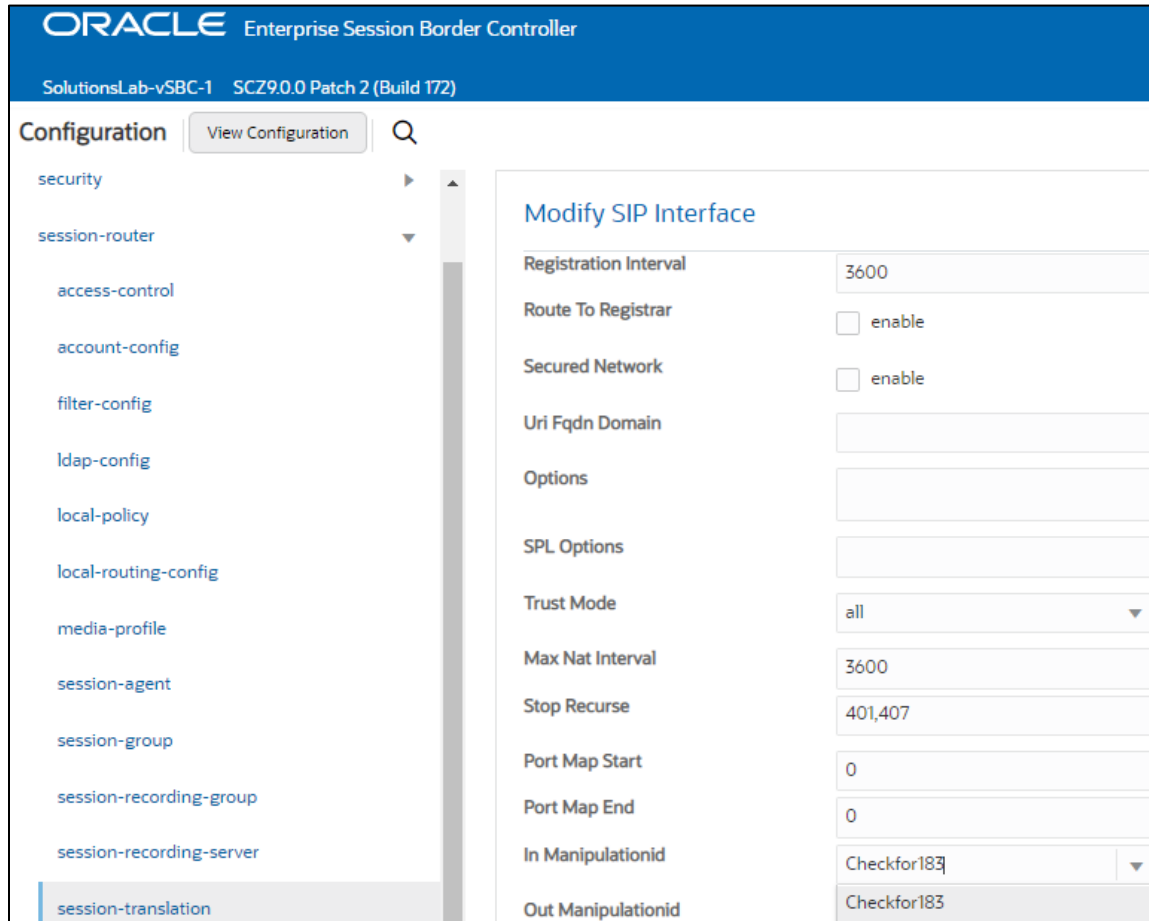
```

This sip manipulation will be applied as the In Manipulationid on the Teams Sip Interface:

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

GUI Path: Session Router/Sip Interface

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



13.2 Oracle SBC Local Media Playback

13.2.1 Ringback on Transfer

During a call transfer initiated by Microsoft Teams, the calling party does not hear a ring back tone while the Oracle SBC is acting on the sip REFER received from Microsoft. In order to avoid this period of silence, we utilize the Oracle SBC's local playback feature.

Once configured, the Oracle SBC has the ability to generate ringback upon receipt of the sip REFER from Microsoft.

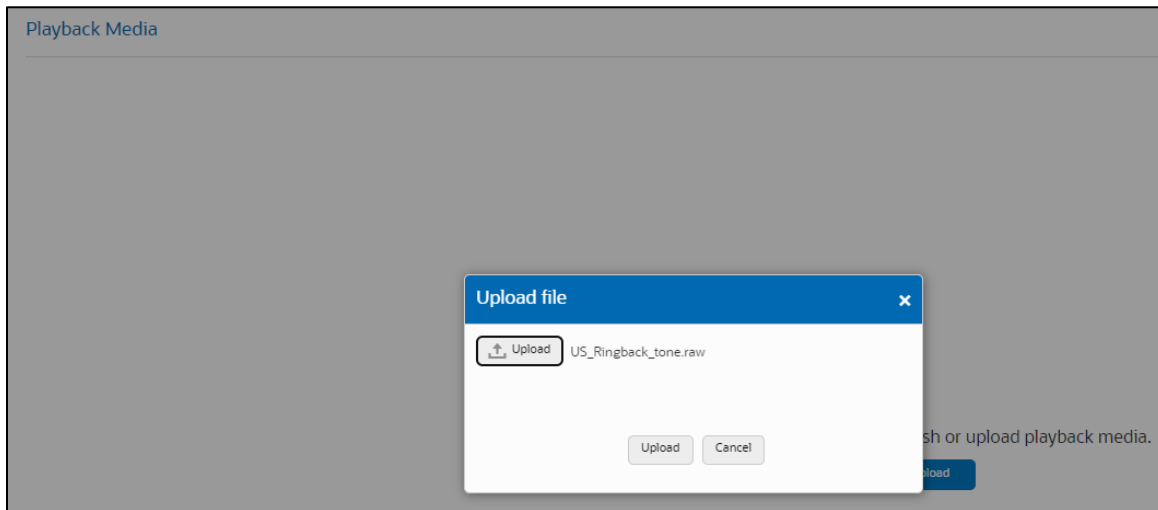
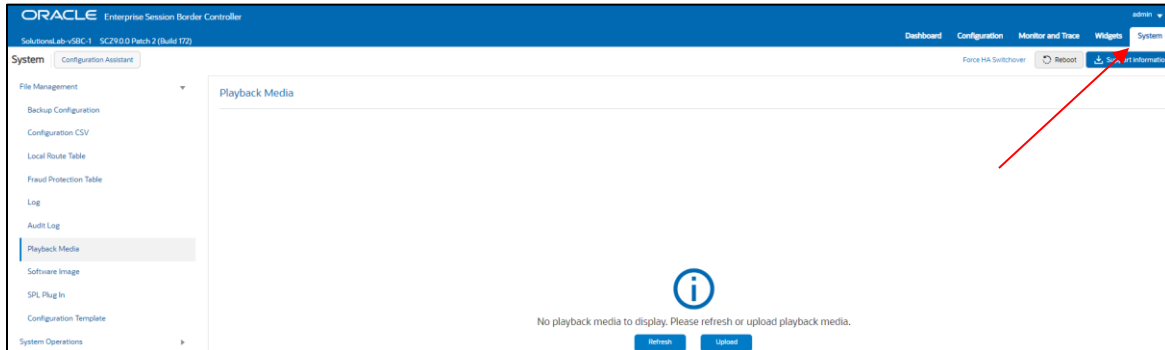
First, you must create a media file.

13.2.1.1 Media Files

Media files of ringback tones are uploaded to /code/media to the Oracle SBC. This file differs based on your media generation method and must be raw media binary. For Transcoding based RBT, ensure that the files RAW PCM 16-bit MONO samples, sampled at 8-khz encapsulated with little-endian formatting and cannot exceed 4.8 MB.

Next, upload the file to the /code/media directory on the Oracle SBC.

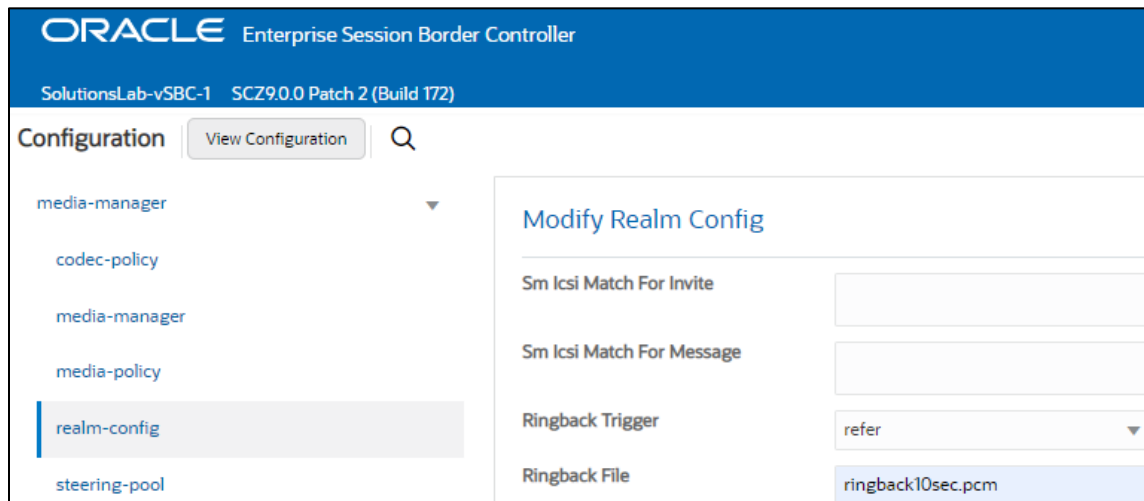
GUI Path: System/Playback Media/Upload



Lastly, we'll assign this file to the realm facing PSTN, and set the trigger for the SBC to generate local ringback toward PSTN:

GUI Path: media manager/realm-config

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



- Select OK at the bottom, and save and activate your configuration.

14 Appendix D

14.1 Configuration for Emergency Calling

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

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

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

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

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

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

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

14.1.1 E911

14.1.2 Emergency Session Handling

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

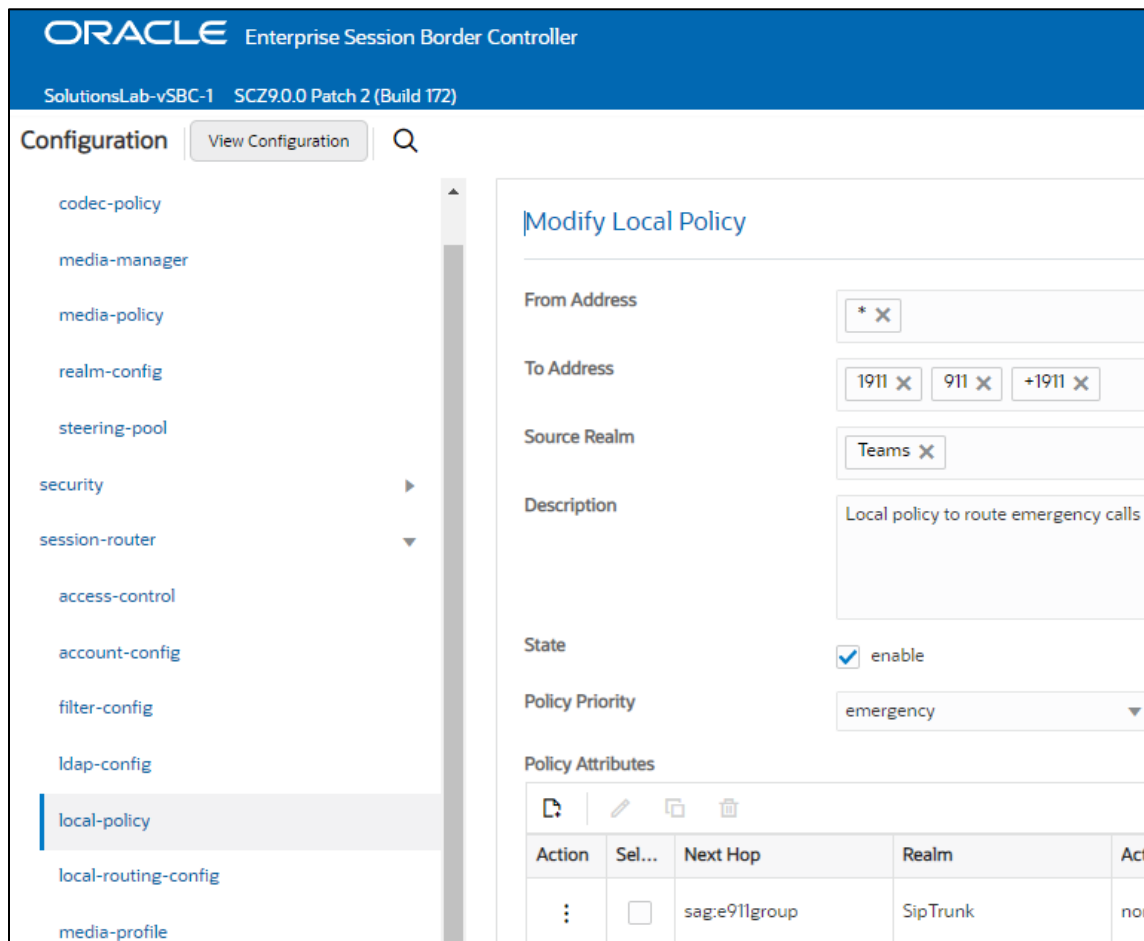
- Local Policy to Match and Route emergency calls to correct destination with policy priority set to emergency
- Enable anonymous-priority on Ingress Sip Interface

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

14.1.2.1 Local Policy Route for Emergency Calls

GUI Path: session-router/local-policy

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



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

Next, we'll enable anonymous-priority field in Sip-Interface: For more information on how this feature works, please see the [SBC Configuration Guide, Chapter 4](#).

GUI Path: Not available in the SBC GUI currently

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

```

sip-interface
  realm-id          Teams
  sip-port
  address           10.1.3.4
  port              5061
  transport-protocol TLS
  tls-profile       TeamsTLSProfile
  allow-anonymous   agents-only
  in-manipulationid Checkfor183
  anonymous-priority emergency
  sip-profile       forreplaces

```

14.1.2.2 Net-Management Control

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

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

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

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

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

ORACLE Enterprise Session Border Controller
 SolutionsLab-vSBC-1 SCZ9.0.0 Patch 2 (Build 172)

Configuration View Configuration Q

- local-response-map
- local-routing-config
- media-profile
- net-management-control**
- q850-sip-map
- qos-constraints
- response-map
- rph-policy
- rph-profile
- service-health
- session-agent
- session-agent-id-rule
- session-constraints
- session-group

Add Net Management Control

Name	EmergencyRoute
State	<input checked="" type="checkbox"/> enable
Type	priority
Value	0
Treatment	divert
Next Hop	sag:e911group
Realm Next Hop	SipTrunk
Protocol Next Hop	SIP
Status Code	503
Cause Code	63
Gap Rate Max Count	0
Gap Rate Window Size	0
Destination Identifier	911 x

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

realm-config	
identifier	Teams
description	Realm facing Teams
network-interfaces	s1p0:0.4
mm-in-realm	enabled
media-sec-policy	TeamsMediaSecurity
rtcp-mux	enabled
ice-profile	ice
teams-fqdn	telechat.o-test06161977.com
teams-fqdn-in-uri	enabled
sdp-inactive-only	enabled
in-translationid	911removeplus
access-control-trust-level	high
net-management-control	enabled
codec-policy	addCN
rtcp-policy	rtcpGen

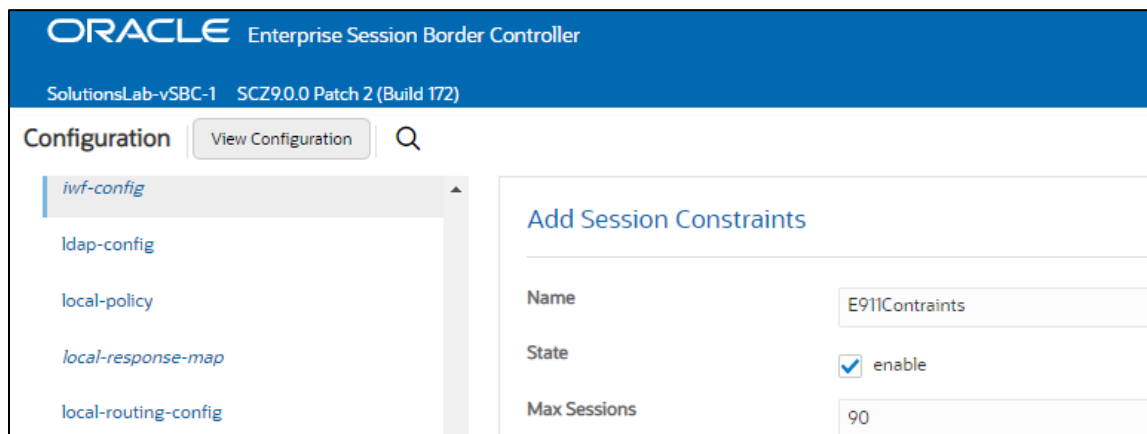
14.1.2.3 Session Constraints for E911

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

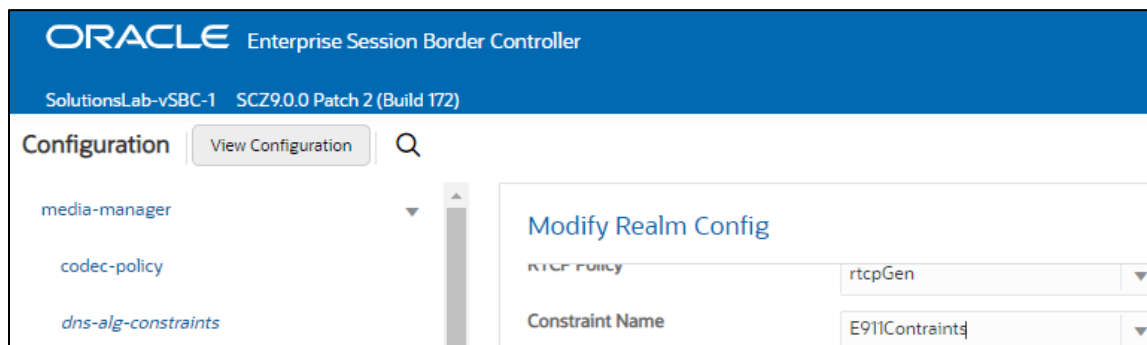
The below example is a very basic constraint setup limiting the number of calls allowed to traverse a realm. For the purposes of this example, we assume there are 100 licensed sessions on the SBC, so we'll limit the number of calls on the realms to 90, leaving 10 licensed session for emergency calls.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

GUI Path: session-router/session-constraints

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



And now we'll assign this constraint to a realm:



- Select OK at the bottom of each element when finished

14.2 Elin Gateway

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

For more information about the SBC's Emergency Location Identification Number (ELIN) Gateway Support, please refer to the [9.0.0 Configuration Guide, Starting on Page 20-29](#)

GUI Path: system/spl-config

ACLI Path: config t→system→spl-config

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

Elin-Gateway=<value>

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

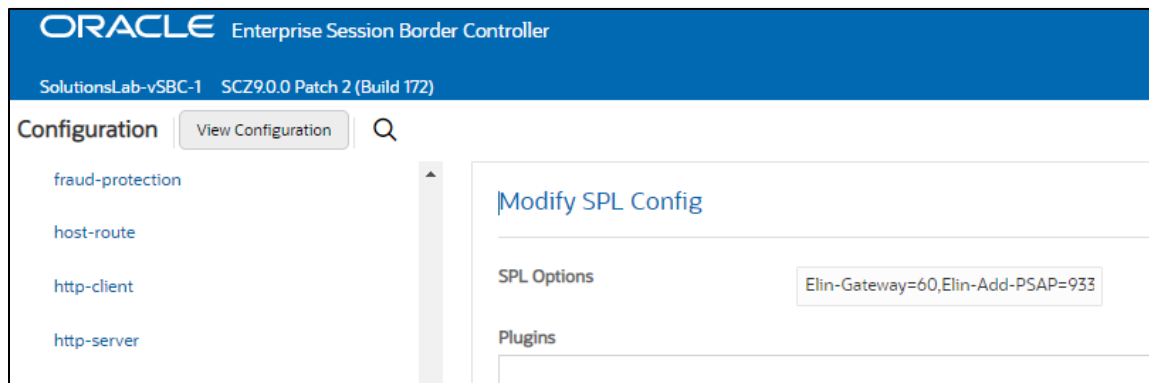
An optional configuration parameter:

Elin-Add-PSAP=<value>

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

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

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



- Select OK at the bottom of the page when finished adding the options

14.2.1 Sip-Manipulation for Teams ELIN

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

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

GUI Path: session-router/sip-manipulation

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

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

```
sip-manipulation
  name          ELIN_Support
  header-rule
    name        StoreElin
    header-name Content-Type
    action      store
    msg-type    request
    methods     Invite
    element-rule
      name      storeelin
      parameter-name application/pidf+xml
      type      mime
      action    store
      comparison-type pattern-rule
      match-value (<ELIN>)(.*)</ELIN>
  header-rule
    name        ReplaceNam
    header-name Content-Type
    action      manipulate
    msg-type    request
    methods     Invite
    element-rule
      name      changenam
      parameter-name application/pidf+xml
      type      mime
      action    find-replace-all
      comparison-type pattern-rule
      match-value (<NAM>)(.*)</NAM>
      new-value  $1+$StoreElin.$storeelin.$2+$3
  header-rule
    name        PAtoFrom
    header-name From
    action      manipulate
    msg-type    request
    methods     Invite
    element-rule
      name      changeuser
      type      uri-user
      comparison-type pattern-rule
      new-value $PAI_USER.$0
```

15 Appendix E

15.1 Configuring IPv6 Support for Teams Direct Routing with Oracle SBC

Microsoft Teams Phone now supports direct routing scenarios over IPv6 for non-media bypass configurations. This enables deployment of IPv6-only environments for both SIP signaling and media between Microsoft Teams and the Oracle SBC, provided media bypass is not used. This section outlines how to configure the Oracle SBC and Microsoft Teams to support IPv6 connectivity.

Prerequisites:

DNS Configuration:

The SBC's FQDN must resolve to an AAAA record/IPv6 address in public DNS. This ensures Microsoft Teams can discover and connect to the SBC over IPv6.

15.2 Configuring Teams Direct Routing for IPv6

The steps to configure or modify a SBC trunk in the Teams Admin Center are nearly identical for IPv6 and IPv4 deployments. To enable IPv6, ensure your SBC's FQDN resolves to an IPv6 record.

Log in to the Microsoft Teams Admin Center using your administrator credentials.

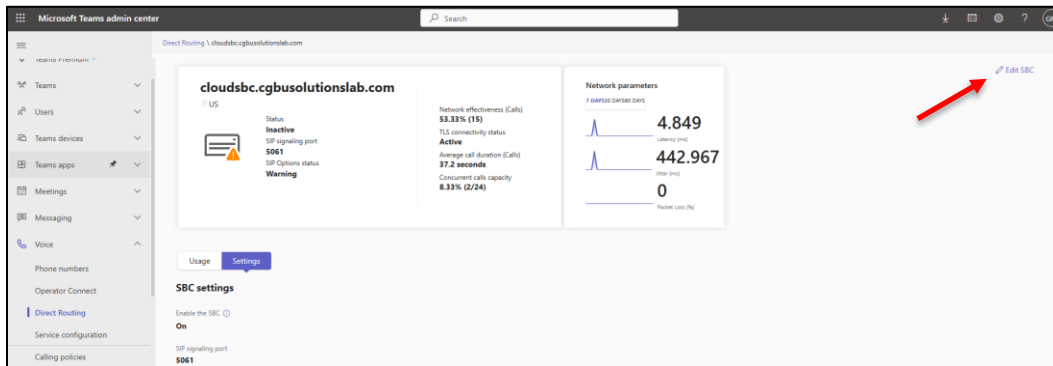
- In the left-hand menu, select Voice.
- Under Voice, choose Direct Routing.
- Click on SBCs to view the list of configured Session Border Controllers.
- Locate the SBC configuration that you wish to modify.

The screenshot displays the Microsoft Teams Admin Center interface. The left-hand navigation menu is expanded to 'Voice', and 'Direct Routing' is selected. The main content area shows the 'Direct Routing' overview, including a summary of 15 total SBCs, 13 voice routes, and 14 SBCs with issues. Below this, there is a table of configured SBCs. The table has columns for SBC name, Network effectiveness, Average call duration, and TLS connectivity status. The SBC 'cloudsbc.cgbusolutionslab.com' is highlighted, showing a network effectiveness of 53.33%, an average call duration of 37.2 seconds (6), and an active status.

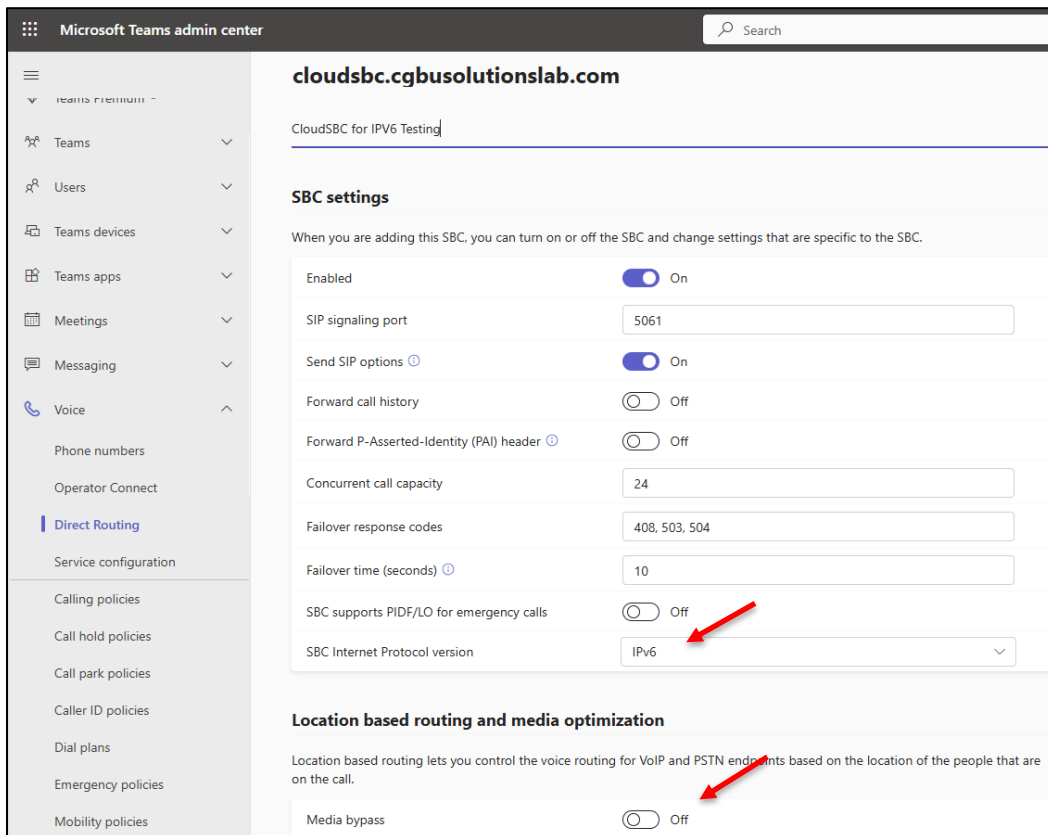
SBC	Network effectiveness	Average call duration	TLS connectivity status
23d43.pstn.intelligentvoice.io	0%	0 seconds (0)	Inactive
38teame25274.pstn.intelligentvoice.io	0%	0 seconds (0)	Inactive
86fd7.pstn.intelligentvoice.io	0%	0 seconds (0)	Inactive
cloudsbc.cgbusolutionslab.com	53.33%	37.2 seconds (6)	Active

For the purposes of this example, we'll be modifying the SBC with the fqdn: **cloudsbc.cgbusolutionslab.com**

- Select Settings
- Top right, Edit SBC



- Next, under **SBC Internet Protocol version**, choose IPv6 from the drop-down menu:



- verify **Media Bypass** is set to off.
- Click Save at the bottom

This completes the required changes on the Teams side to enable IPv6 support for Direct Routing with your SBC.

15.3 Configuring the Oracle SBC for IPv6 Support

This section outlines the steps required to configure your Oracle Session Border Controller to support IPv6 for Microsoft Teams Direct Routing. Please ensure all prerequisites are met before proceeding with the configuration.

Note: Setting up DNS or configuring your internal network for IPv6 connectivity is outside the scope of this document.

15.3.1 Network Interface

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
Name	s0p0
IP Address	2001:db8::4/64
Netmask	ffff:ffff:ffff:ffff::
Gateway	fe80::1234:5678:9abc
DNS Primary IP	2001:4860:4860::8888
DNS Domain	cloudsbc.cgbusolutionslab.com

The screenshot shows the Oracle Enterprise Session Border Controller GUI. The top navigation bar includes the Oracle logo and the text 'Enterprise Session Border Controller'. Below this, the version information 'SolutionsLab-vSBC-2 10.114 SCZ9.3.0 Patch 7 (Build 259)' is displayed. The main interface is divided into a left sidebar and a main content area. The sidebar, under the 'Configuration' tab, lists various configuration categories, with 'network-interface' selected and highlighted. The main content area is titled 'Modify Network Interface' and contains a form with the following fields:

- Name:** s0p0 (dropdown menu)
- Sub Port Id:** 0
- Description:** (empty text area)
- IP Address:** 2001:db8::4/64
- Pri Utility Addr:** (empty text field)
- Sec Utility Addr:** (empty text field)
- Netmask:** ffff:ffff:ffff:ffff::
- Gateway:** fe80::1234:5678:9abc
- Gw Heartbeat:** (checkbox, currently unchecked)
- Bfd Config:** (checkbox, currently checked)
- Health Score:** 0
- DNS IP Primary:** 2001:4860:4860::8888
- DNS IP Backup1:** 2001:4860:4860::8844

- Click OK at the bottom after entering config information.

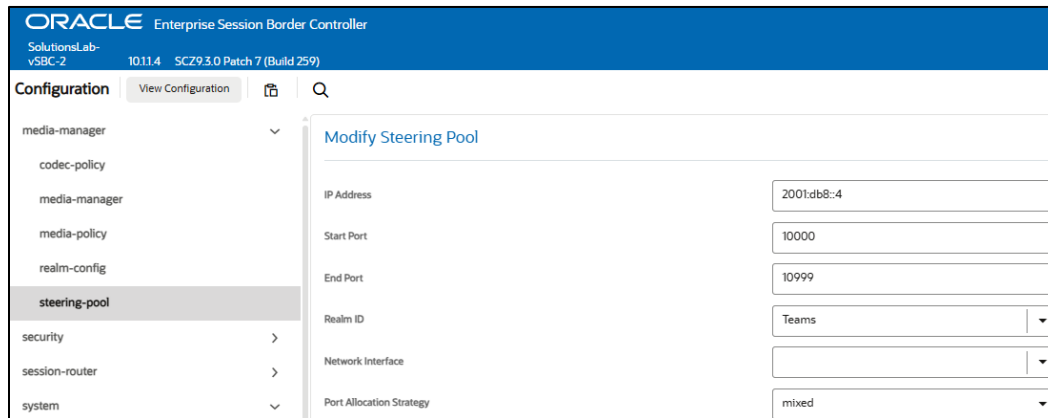
15.3.2 Steering Pool

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.

GUI Path: media-manger/steering-pool

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

- Click Add and use the below examples to configure.



- Select OK at the bottom.

15.3.3 Sip Interface

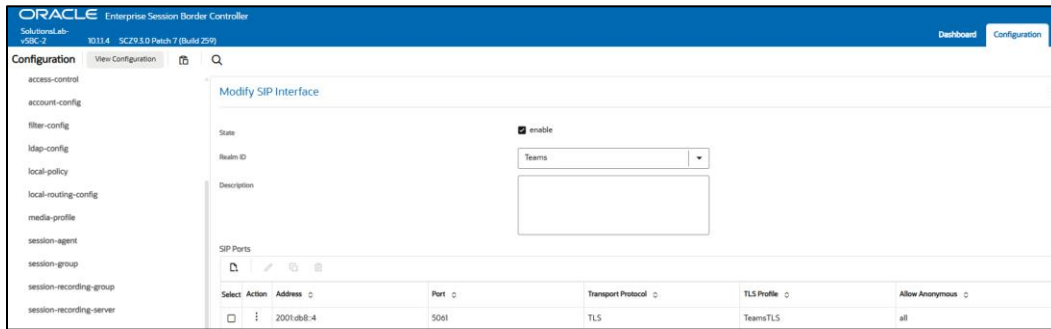
The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages.

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	Teams
Realm ID	Teams
Sip-Profile	forreplaces
Sip Port Config Parmeter	Teams
Address	2001:db8::4
Port	5061
Transport protocol	TLS
TLS profile	TeamsTLSProfile
Allow anonymous	all
In Manipulationid	RespondOptions



- Select OK at the bottom.

For environments in which the SBC is deployed behind a NAT device, ensure the headernat spl parameter is properly configured in your SIP interface to support IPv6.

For example: HeaderNatPublicSipIfIp=2603:1030:408:5::19b,HeaderNatPrivateSipIfIp=2001:db8::4

For more information, see the [Oracle SBC deployed behind Nat](#) section of this document.

After making configuration changes on the Oracle SBC, be sure to **save and activate** the updated configuration. If you are modifying an existing SBC setup, especially changes related to network interfaces or IP address assignments, a system **reboot may be required** for the changes to take effect.

This concludes the required steps to establish a working trunk between the Oracle SBC and Microsoft Teams Direct Routing over IPv6.

16 ACLI Running Configuration

Below is a complete output of the running configuration used to create this application note. This output includes all the configuration elements used in our examples, including some of the optional configuration features outlined throughout this document. Be aware that not all parameters may be applicable to every Oracle SBC setup, so please take this into consideration if planning to copy and paste this output into your SBC.

```
access-control
  realm-id          Teams
  source-address    52.112.0.0/14
  application-protocol SIP
  trust-level       high
access-control
  realm-id          Teams
  source-address    52.120.0.0/14
  application-protocol SIP
  trust-level       high
certificate-record
  name              DigiCertGlobalRootG2
  common-name       DigiCert Global Root G2
certificate-record
  name              DigiCertGlobalRootG3
  common-name       DigiCert Global Root G3
certificate-record
  name              DigiCertRoot
  common-name       DigiCert Global Root CA
certificate-record
  name              DigiCertTLSECCP384RootG5
  common-name       DigiCert TLS ECC P384 Root G5
certificate-record
  name              DigiCertTLSECCP4096RootG5
  common-name       DigiCert TLS RSA 4096 Root G5
certificate-record
  name              MicrosoftECCRootCertificateAuthority2017
  common-name       Microsoft ECC Root Certificate Authority 2017
certificate-record
  name              MicrosoftRSARootCertificateAuthority2017
  common-name       Microsoft RSA Root Certificate Authority 2017
certificate-record
  name              SBCCertificateforTeams
  state              California
  locality           Redwood City
  organization       Oracle Corporation
  unit               Oracle CGBU-LABS BOSTON
  common-name        telechat.o-test06161977.com
  extended-key-usage-list clientAuth
  serverAuth
certificate-record
  name              WebServerInstance
  state              California
  locality           Redwood City
  organization       Oracle Corporation
  unit               Oracle CGBU-LABS BOSTON
  common-name        telechat.o-test06161977.com
```

```

codec-policy
  name                SipTrunkCodecs
  allow-codecs        * SILK:NO G722:NO PCMA:NO
  add-codecs-on-egress PCMU
codec-policy
  name                addCN
  allow-codecs        *
  add-codecs-on-egress CN
http-server
  name                webServerInstance
  http-state          disabled
  https-state         enabled
  tls-profile         WebServerInstance

ice-profile
  name                ice
local-policy
  from-address        *
  to-address          1911
                    911
                    +1911
  source-realm        Teams
  description         Local policy to route emergency calls
  policy-priority     emergency
  policy-attribute
    next-hop          sag:e911group
    realm             SipTrunk
local-policy
  from-address        *
  to-address          *
  source-realm        SipTrunk
  description         Route calls from PSTN to Microsoft Teams Phone
  System Direct Routing
  policy-attribute
    next-hop          sag:TeamsGrp
    realm             Teams
    action            replace-uri
local-policy
  from-address        *
  to-address          *
  source-realm        Teams
  description         Route Calls from Teams Phone System Direct
  Routing to PSTN
  policy-attribute
    next-hop          10.1.2.30
    realm             SipTrunk
media-manager
  options             audio-allow-asymmetric-pt
                    xcode-gratuitous-rtcp-report-generation
media-profile
  name                CN
  subname             wideband
  payload-type        118
media-profile
  name                SILK
  subname             narrowband

```

```

payload-type          103
clock-rate            8000
media-profile
  name                SILK
  subname              wideband
  payload-type        104
  clock-rate          16000
media-sec-policy
  name                PSTNNonSecure
media-sec-policy
  name                TeamsMediaSecurity
  inbound
    profile            TeamsSRTP
    mode                srtp
    protocol            sdes
  outbound
    profile            TeamsSRTP
    mode                srtp
    protocol            sdes
net-management-control
  name                EmergencyRoute
  type                priority
  treatment            divert
  next-hop             sag:e911group
  realm-next-hop       SipTrunk
  protocol-next-hop    SIP
  destination-identifier 911
network-interface
  name                s0p0
  ip-address           10.1.2.4
  netmask              255.255.255.0
  gateway              10.1.2.1
network-interface
  name                s1p0
  ip-address           10.1.3.4
  netmask              255.255.255.0
  gateway              10.1.3.1
ntp-config
  server               216.239.35.0
phy-interface
  name                s0p0
  operation-type       Media
phy-interface
  name                s1p0
  operation-type       Media
  slot                 1
realm-config
  identifier           SipTrunk
  description          Realm facing PSTN
  network-interfaces  s1p0:0.4
  mm-in-realm          enabled
  media-sec-policy     PSTNNonSecure
  access-control-trust-level high
  codec-policy         SipTrunkCodecs
  ringback-trigger     refer
  ringback-file        ringback10sec.pcm

```

```

realm-config
  identifier                Teams
  description               Realm facing Teams
  network-interfaces        s0p0:0.4
  mm-in-realm               enabled
  media-sec-policy          TeamsMediaSecurity
  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
  net-management-control    enabled
  codec-policy               addCN
  refer-call-transfer        enabled
  rtcp-policy               rtcpGen
rtcp-policy
  name                      rtcpGen
  rtcp-generate              all-calls
sdes-profile
  name                      TeamsSRTP
  lifetime                   31
session-agent
  hostname                   10.1.2.30
  ip-address                 10.1.2.30
  realm-id                   SipTrunk
  ping-method                 OPTIONS
  ping-interval              30

session-agent
  hostname                   e911.com
  ip-address                 10.1.2.10
  realm-id                   SipTrunk
  description                 Route emergency calls to this destination.
session-agent
  hostname                   sip.pstnhub.microsoft.com
  port                       5061
  transport-method           StaticTLS
  realm-id                   Teams
  ping-method                 OPTIONS
  ping-interval              10
  refer-call-transfer         enabled

session-agent
  hostname                   sip2.pstnhub.microsoft.com
  port                       5061
  transport-method           StaticTLS
  realm-id                   Teams
  ping-method                 OPTIONS
  ping-interval              10
  refer-call-transfer         enabled

session-agent
  hostname                   sip3.pstnhub.microsoft.com
  port                       5061
  transport-method           StaticTLS

```

```

realm-id                Teams
ping-method             OPTIONS
ping-interval           10
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            e911group
  description           Session Group for emergency calls
  dest                  e911.com
  sag-recursion         enabled
sip-config
  home-realm-id         Teams
  options               max-udp-length=0
  allow-pani-for-trusted-only disabled
  add-ue-location-in-pani disabled
  npli-upon-register    disabled
sip-feature
  name                  replaces
  realm                 Teams
  require-mode-inbound  Pass
  require-mode-outbound Pass
sip-interface
  realm-id              SipTrunk
  sip-port
    address              10.1.2.4
    allow-anonymous     agents-only
sip-interface
  realm-id              Teams
  sip-port
    address              10.1.3.4
    port                 5061
    transport-protocol  TLS
    tls-profile          TeamsTLSProfile
    allow-anonymous     all
  in-manipulationid    RespondOptions
  anonymous-priority    emergency
  sip-profile           forreplaces
sip-manipulation
  name                  Checkfor183
  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                     $check183.$is183
  sdp-session-rule
    name                          au
    action                        manipulate
    sdp-line-rule
      name                        checkclineforsbcip
      type                        c
      action                      store
      comparison-type             pattern-rule
      match-value                ^.(?!(10.1.3.4)).*$
mime-sdp-rule
  name                            delete183SDP
  msg-type                        reply
  methods                         Invite
  action                          delete
  comparison-type                 boolean
  match-value                     $if183.$au.$checkclineforsbcip
header-rule
  name                            change183to180
  header-name                     @status-line
  action                          manipulate
  comparison-type                 boolean
  match-value                     $if183.$au.$checkclineforsbcip
  element-rule
    name                          changestatus
    type                          status-code
    action                        replace
    match-value                   183
    new-value                      180
  element-rule
    name                          changereasonphrase
    type                          reason-phrase
    action                        replace
    match-value                   Session Progress
    new-value                      Ringing
sip-manipulation
  name                            ELIN_Support
  header-rule
    name                          StoreElin
    header-name                   Content-Type
    action                        store
    msg-type                      request
    methods                       Invite
  element-rule
    name                          storeelin
    parameter-name                application/pidf+xml
    type                          mime
    action                        store
    comparison-type                pattern-rule

```

```

        match-value          (<ELIN>)(.*)</ELIN>
header-rule
  name                      ReplaceNam
  header-name              Content-Type
  action                   manipulate
  msg-type                 request
  methods                  Invite
  element-rule
    name                   changenam
    parameter-name        application/pidf+xml
    type                   mime
    action                 find-replace-all
    comparison-type       pattern-rule
    match-value           (<NAM>)(.*)</NAM>
    new-value              $1+$StoreElin.$storeelin.$2+$3
  header-rule
    name                  PAtoFrom
    header-name           From
    action                manipulate
    msg-type              request
    methods               Invite
    element-rule
      name                changeuser
      type                uri-user
      comparison-type     pattern-rule
      new-value           $PAI_USER.$0
sip-manipulation
  name                    RespondOptions
  header-rule
    name                  RejectOptions
    header-name          From
    action                reject
    msg-type              request
    methods               OPTIONS
    new-value             200 OK
sip-profile
  name                    forreplaces
  replace-dialogs        enabled
spl-config
  spl-options            Elin-Gateway=60,Elin-Add-PSAP=933
steering-pool
  ip-address             10.1.2.4
  start-port             10000
  end-port               10999
  realm-id               SipTrunk
steering-pool
  ip-address             10.1.3.4
  start-port             10000
  end-port               10999
  realm-id               Teams
system-config
  hostname                oraclesbc.com
  description             SBC connecting PSTN Sip Trunk to Microsoft
                        Teams Phone System Direct Routing
  location                Burlington, MA
  transcoding-cores      1

```



```

tls-global
  session-caching          enabled
tls-profile
  name                    TeamsTLSProfile
  end-entity-certificate  SBCCertificateforTeams
  trusted-ca-certificates
    DigiCertRoot
    DigiCertGlobalRootG2
    DigiCertGlobalRootG3
    DigiCertTLSECCP384RootG5
    DigiCertTLSECCP4096RootG5
    MicrosoftECCRootCertificateAuthority2017
    MicrosoftRSARootCertificateAuthority2017
  tls-version             tlsv12
  mutual-authenticate    enabled
tls-profile
  name                    WebServerInstance
  end-entity-certificate  WebServerInstance
  trusted-ca-certificates
    DigiCertRoot

```



CONNECT WITH US

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

Oracle Corporation, World Headquarters

2300 Oracle Way
Austin, TX 78741, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2025, 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, did including imply 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