ORACLE

# Configuring the Oracle SBC with Microsoft Teams Direct Routing Carrier Hosting Model

**Technical Application Note**

ORACLE

COMMUNICATIONS

# Disclaimer

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

# 1 Contents

# 2 Related Documentation

## 2.1 Oracle SBC

- Oracle® Enterprise Session Border Controller ESBC Configuration Guide
- Oracle® Enterprise Session Border Controller ACLI Reference Guide
- Oracle® Enterprise Session Border Controller Release Notes
- https://docs.oracle.com/cd/F12246_01/doc/sbc_scz900_security.pdf

## 2.2 Microsoft Teams

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

# 3 Revision History

| Version | Date Revised | Description of Changes |
|---|---|---|
| 1.0 | 04/17/2019 | Initial publication |
| 1.1 | 10/09/2019 | • Added GUI Configuration<br>• Firmware Version 8.3<br>• Modified Due to changes in MSFT Concept of Hosting Model |
| 1.2 | 03/26/2020 | • Modified TLS Profile Config<br>• Change LRT example<br>• Added additional customer domain information |
| 1.3 | 04/29/2020 | • Added Alert<br>• Add Important Information Section |
| 1.4 | 06/08/2020 | • Changed Running Config Output<br>• Added Appendix C with Notes<br>• Added notes regarding Sip Manipulation and new release |
| 1.5 | 01/07/2022 | • Removed Reference to sip-all fqdn |
| 1.6 | 03/31/2022 | • 9.0 Refresh<br>• Removed sip manips<br>• Added ACLs for new Teams subnets |
| 1.7 | 08/21/2022 | • Added DigiCert Global G2 Root Certificate config and screenshots<br>• Modified TLS Profile |
| 1.8 | 07/20/2024 | • Removed reference to ping-response parameter and added notes for using tls-global config in ACLI |

# 4 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 +.*

# 5 Validated Oracle Versions

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

SCZ830/SCZ840/SCZ900

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

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

- AP 1100
- AP 3900
- AP 3950 (SCZ9.0.0 Only)
- AP 4600
- AP 4900 (SCZ9.0.0 Only)
- AP 6300
- AP 6350
- VME

# 6 About Teams Direct Routing

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

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

# 7 Infrastructure Requirements

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

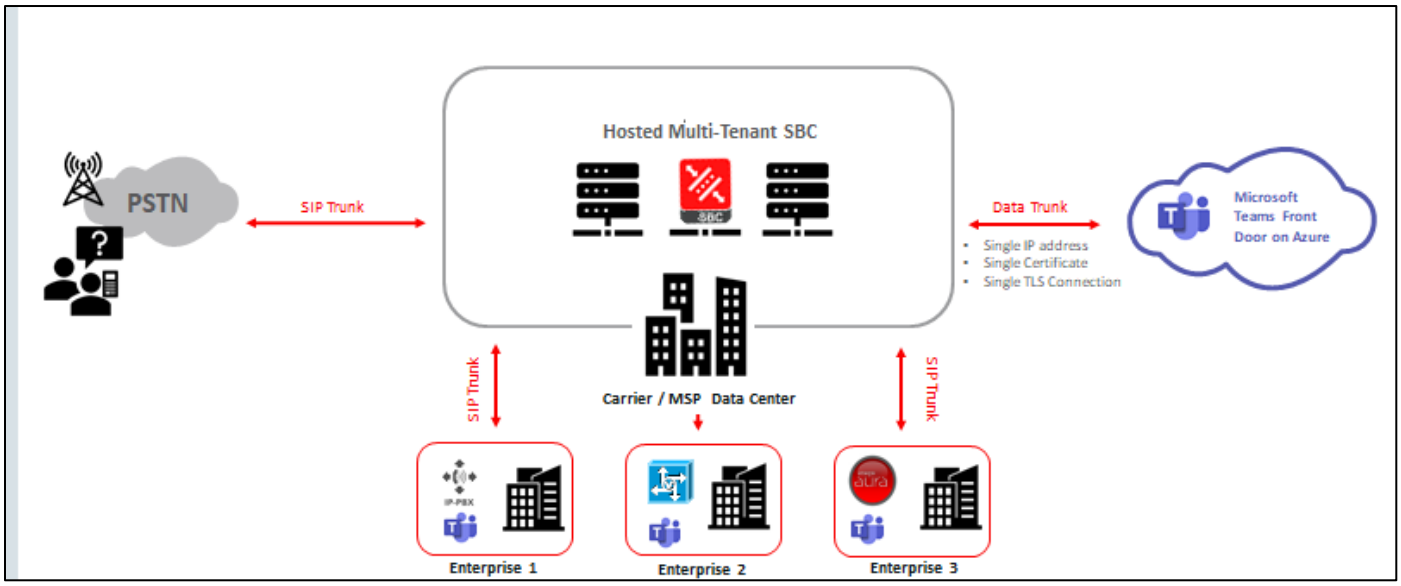
| Infrastructure Prerequisite | Details |
|---|---|
| Certified Session Border Controller (SBC) | **See Microsoft's Plan Direct Routing document and Microsoft Trusted Root Program with Included CA Certificate List** |
| SIP Trunks connected to the SBC | |
| Office 365 tenant | |
| Domains | |
| Public 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 | |

# 8 Configuration

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

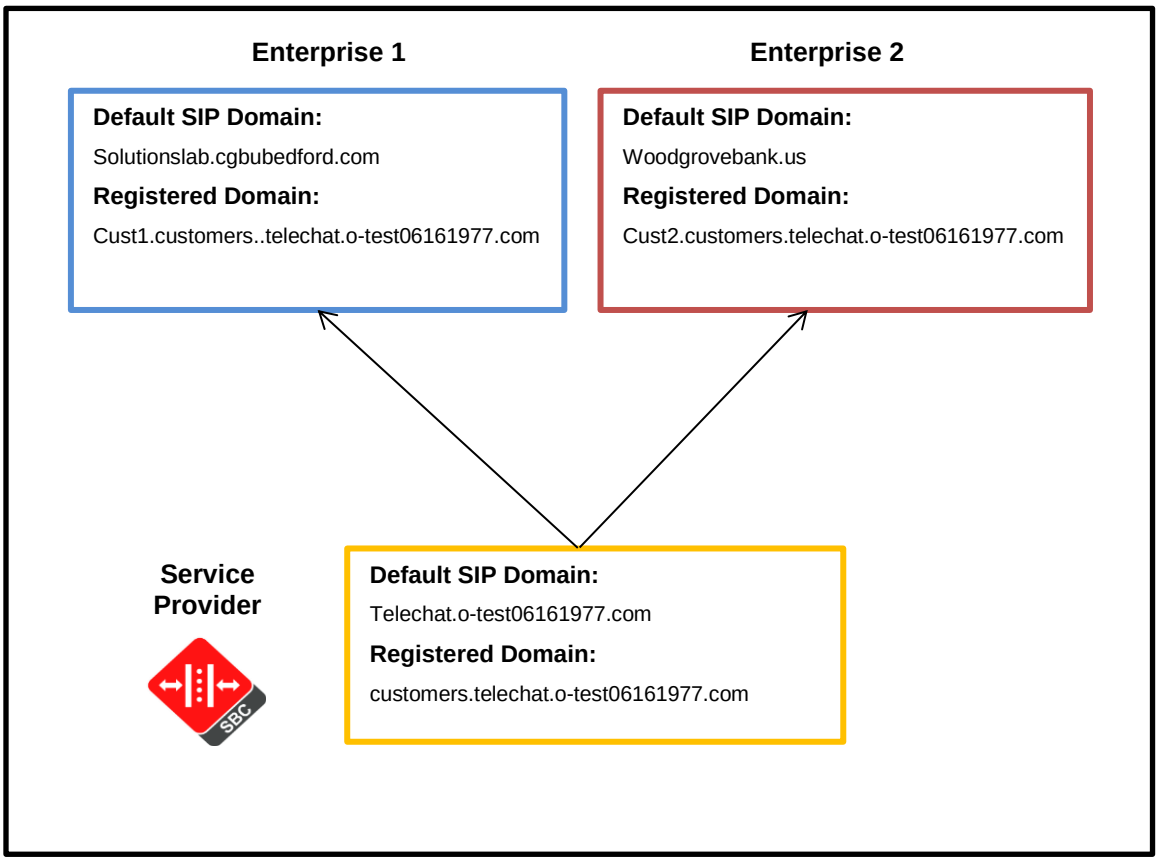
Below shows the connection topology example for MSFT Teams Carrier Model.
There are multiple connections shown:

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




*These instructions cover configuration steps between the Oracle SBC and Microsoft Teams Direct Routing Interface. The interconnection of other entities, such as connection of the SIP trunk, 3rd Party PBX and/or analog devices are not covered in this instruction. The details of such connection are available in other instructions produced by the vendors of retrospective components.*

The below illustration and table are the Tenant Domain Structure used for this Application Note.




| New Domain Name | Type | Registered Tenant | Certificate SAN for SBC | Tenant Default Domain | FQDN presented in Contact header when sending Calls |
|---|---|---|---|---|---|
| Customers.telechat.0-test06161977.com | Base | Carrier | *.cusotmers.telechat.o-test06161977.com | Telechat.o-test06161977.com | NA, this is a service tenant, no users |
| Sbc1.Customers.telechat.0-test06161977.com | Subdomain | Customer | *.cusotmers.telechat.o-test06161977.com | Solutionslab.cgbubedford.com | Sbc1.Customers.telechat.0-test06161977.com |
| Sbc2.Customers.telechat.0-test06161977.com | Subdomain | Customer | *.cusotmers.telechat.o-test06161977.com | Woodgrovebank.us | Sbc2.Customers.telechat.0-test06161977.co |

### 8.1.1 Prerequisites

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

- Public IP address
- FQDN name for each registered subdomain representing individual tenants using the multitenant Direct Routing Trunk. Each FQDN must resolve to the Public IP address
- Public certificate, issued by one of the supported CAs (refer to Related Documentation for details about supported Certification Authorities).

### 8.1.2 About SBC Domain Name

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

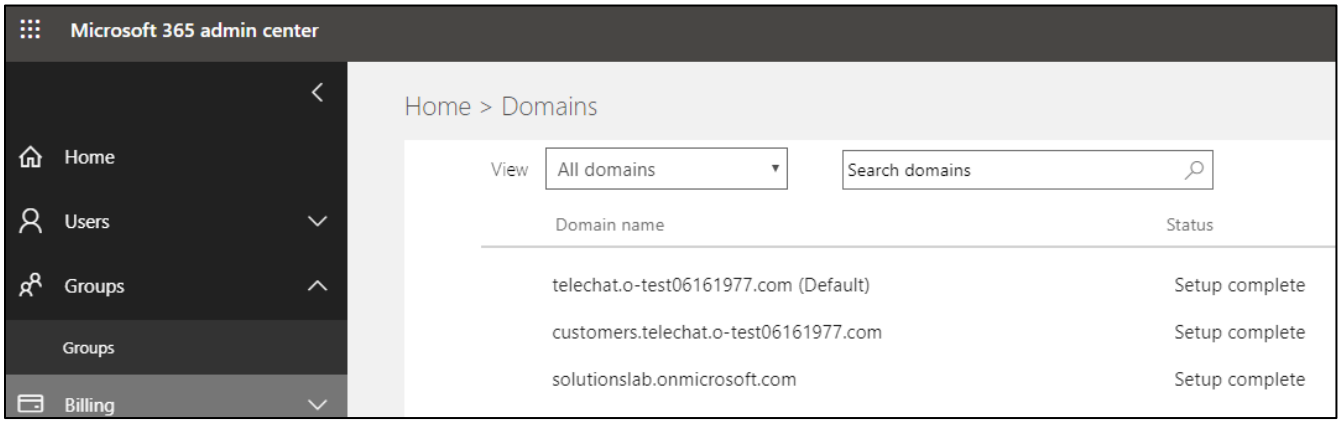
| DNS Name | Can Be Used For SBC | Example of FQDN names |
|---|---|---|
| *.customers.adatum.biz | YES | **Valid FQDN:**<br>• Sbc50.customers.adatum.biz<br>• Sbc51.customer.adatum.biz<br>• Ussbcsl5.customers.adataum.biz<br>• Europe.customers.adatum.biz<br>**Invalid FQDN:**<br>• Sbc1.customers.europe.adatum.biz *(this would require registering domain name "Europe.adatum.biz")* |
| adatumbiz.onmicrosoft.com | NO | Using *.onmicrosoft.com domains is not supported for SBC names |

### 8.1.3 SBC Domain Name in Carrier Tenant

Below is an example of registered DNS names in the Carrier Tenant:

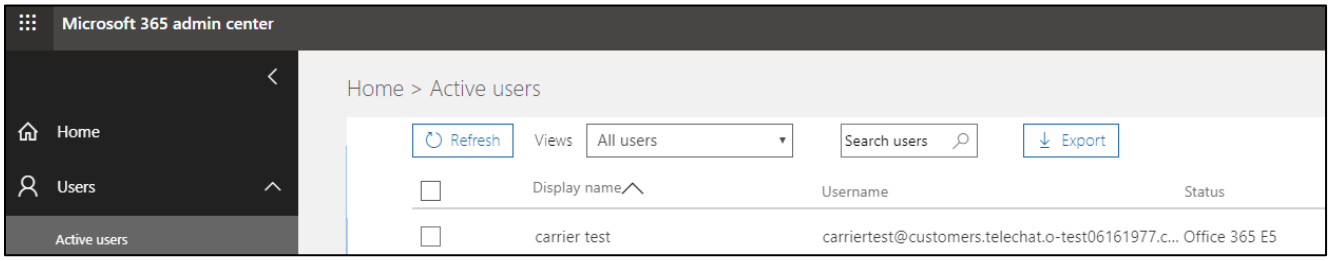
- Carrier Default Domain: **telechat.o-test06161977.com**
- Carrier Subdomain: **customers.telechat.o-test06161977.com**

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




After you have registered a domain name, you need to activate it by adding at least one licensed user with the SIP address matching the created base domain.

In the below example we have created the user carriertest@customers.telechat.o-test06161977.com in the carrier tenant to activate the carrier base domain:



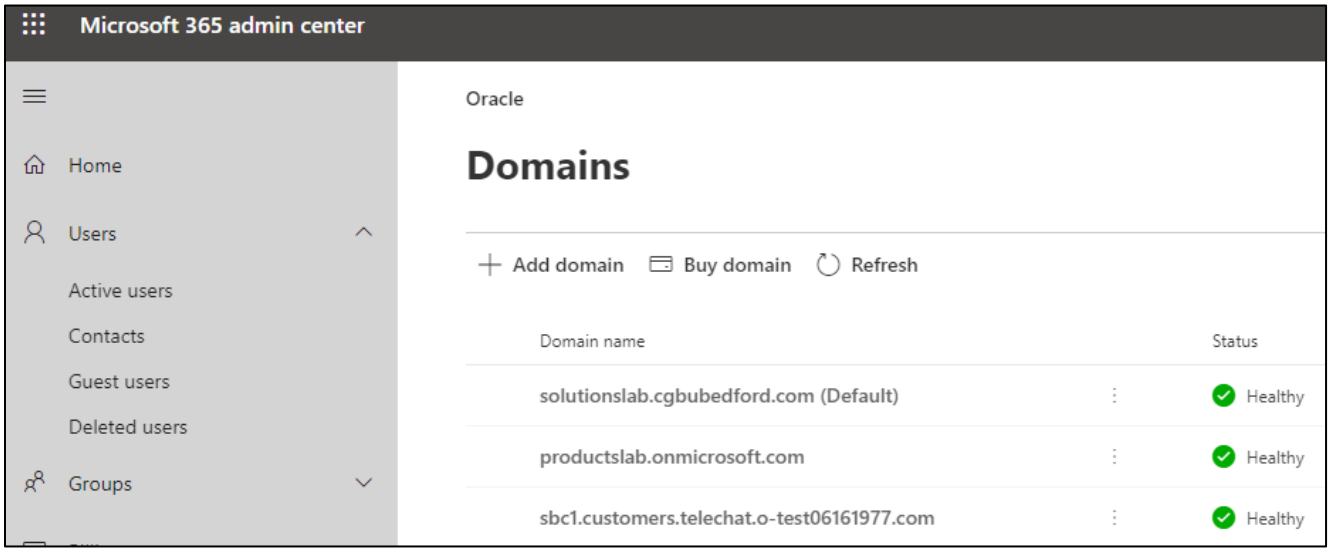

### 8.1.4 SBC Domain in Customer Tenant

For each customer tenant, you must register a subdomain that belongs to a carrier that points to a customer tenant.

In the below example:

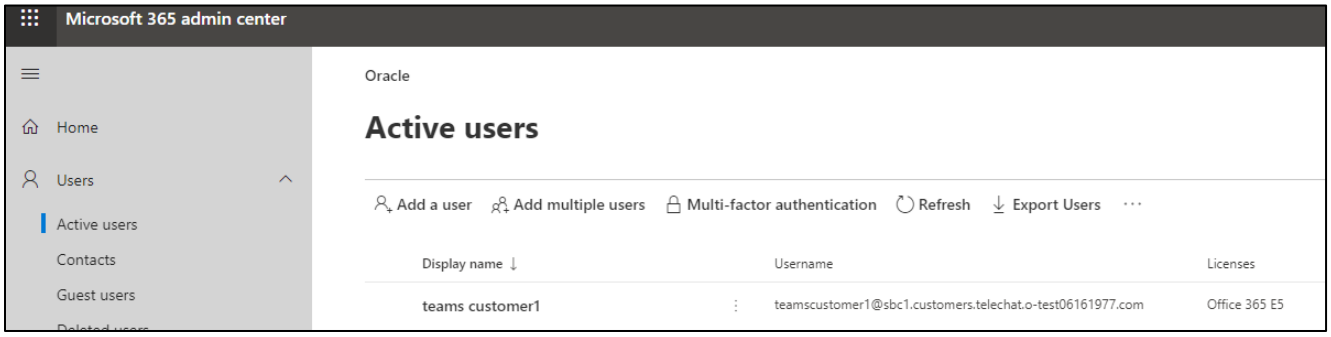
- Customer Tenant Default Domain: **solutionslab.cgbubedford.com**
- Carrier subdomain: **sbc1.customers.telechat.o-test06161977.com**

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




Same as the carrier tenant above, once you register the domain, you must activate it by adding at least one licensed user with the SIP address matching the carrier subdomain in the customer tenant.

Below, we have added the user teamscustomer1@sbc1.customers.telechat.o-test06161977.com to activate the carrier subdomain in the customer tenant.




For the purposes of this example, the following IP address and FQDN's are used:

*Note: all fqdn's listed below resolve to the same public IP address*

| FQDN Names | Public IP Address |
|---|---|
| **customers.telechat.o-test06161977.com** | **141.146.36.68** |
| **sbc1.customers.telechat.o-test06161977.com** | |
| **sbc2.customers.telechat.o-test06161977.com** | |

# 9 Oracle SBC Configuration

There are two methods for configuing 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.

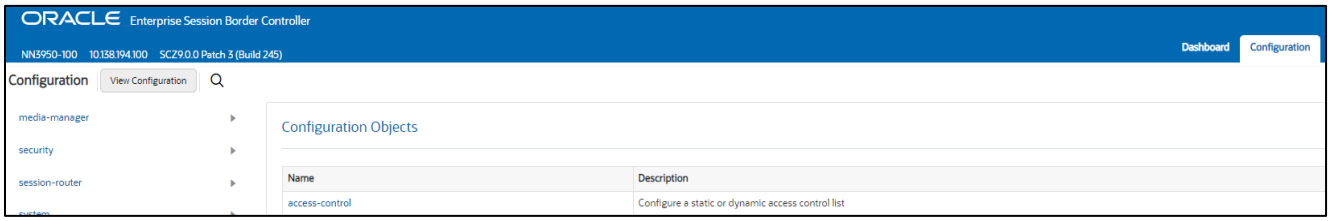
This guide assumes the OCSBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, web-server-config has been enabled for GUI access. If you require more information on how to install your SBC platform, please refer to the ACLI configuration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

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

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

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

Please note, the below configuration example assumes Media Bypass is enabled on the MSFT Teams Tenant. For differences in the OCSBC configuration for Non Media Bypass, please see Appendix A




## 9.1 System-Config

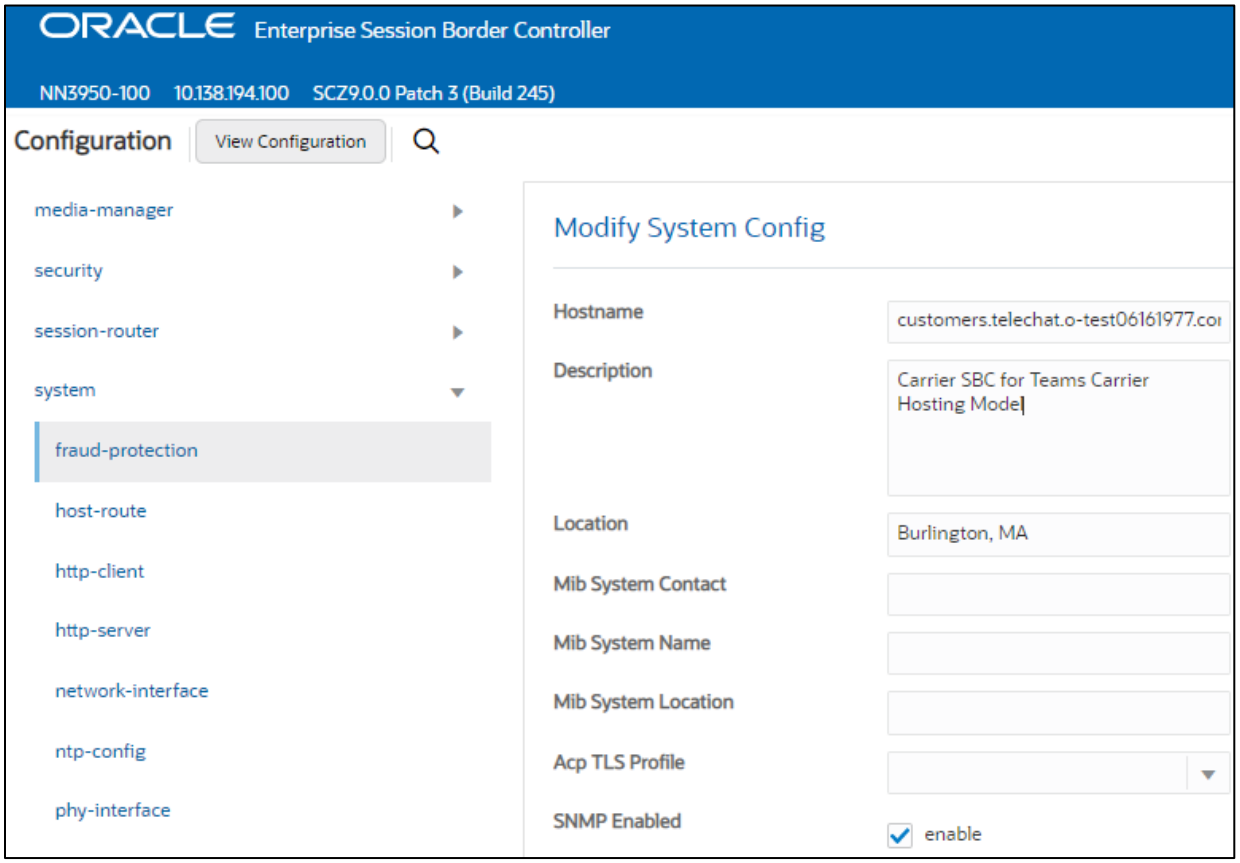
To configure system level functionality for the OCSBC, you must first enable the system-config

GUI Path: system/system-config

ACLI 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)



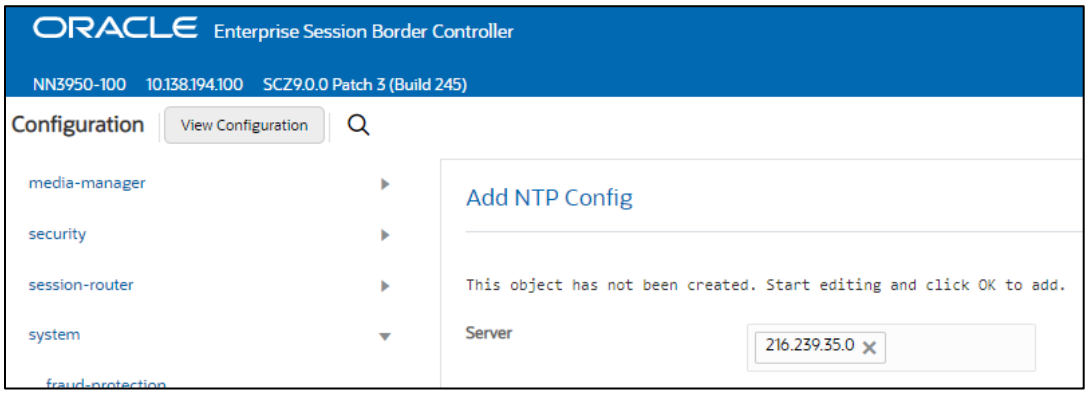

- Click the OK at the bottom of the screen

### 9.1.1 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

ACLI Path: config t→system→ntp-sync




- Select OK at the bottom

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

### 9.1.2 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.

### 9.1.3 Physical Interfaces

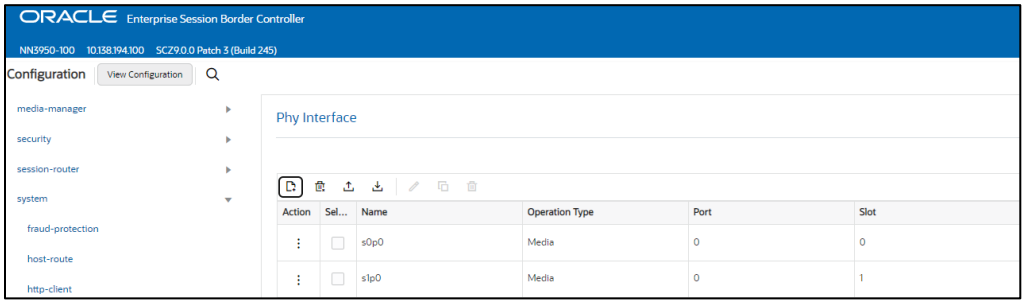
GUI Path: system/phy-interface

ACLI 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*



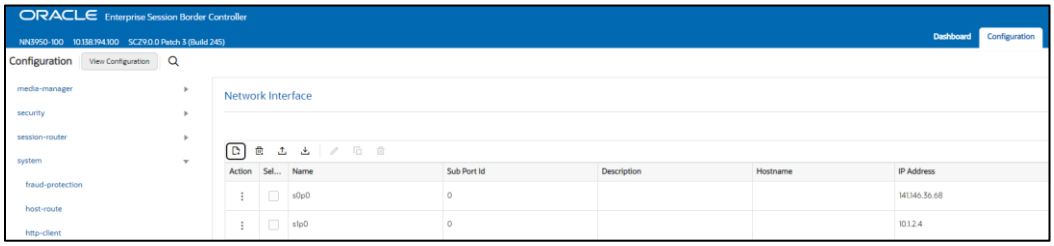

### 9.1.4 Network Interfaces

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 | 141.146.36.68 | 10.1.2.4 |
| Netmask | 255.255.255.192 | 255.255.255.0 |
| Gateway | 141.146.36.65 | 10.1.2.1 |
| DNS Primary IP | 8.8.8.8 | |
| DNS Domain | telechat.o-test06161977.com | |




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

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

## 9.2 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 Authrities can be found at:

**Public trusted certificate for the SBC**

### 9.2.1 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 three certificate records. They are as follows:

- SBC Certificate (end-entity wildcard certificate)
- Go Daddy sCert (Root CA used to sign the SBC's end entity certificate)
- BaltimoreRoot CA Cert (Microsoft Presents the SBC a certficate signed by this authority)
- DigiCert Global G2 (Microsoft Presents the SBC a certficate signed by this authority)

*Note: The DigiCert 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.*

#### 9.2.1.1 SBC End Entity Certificate

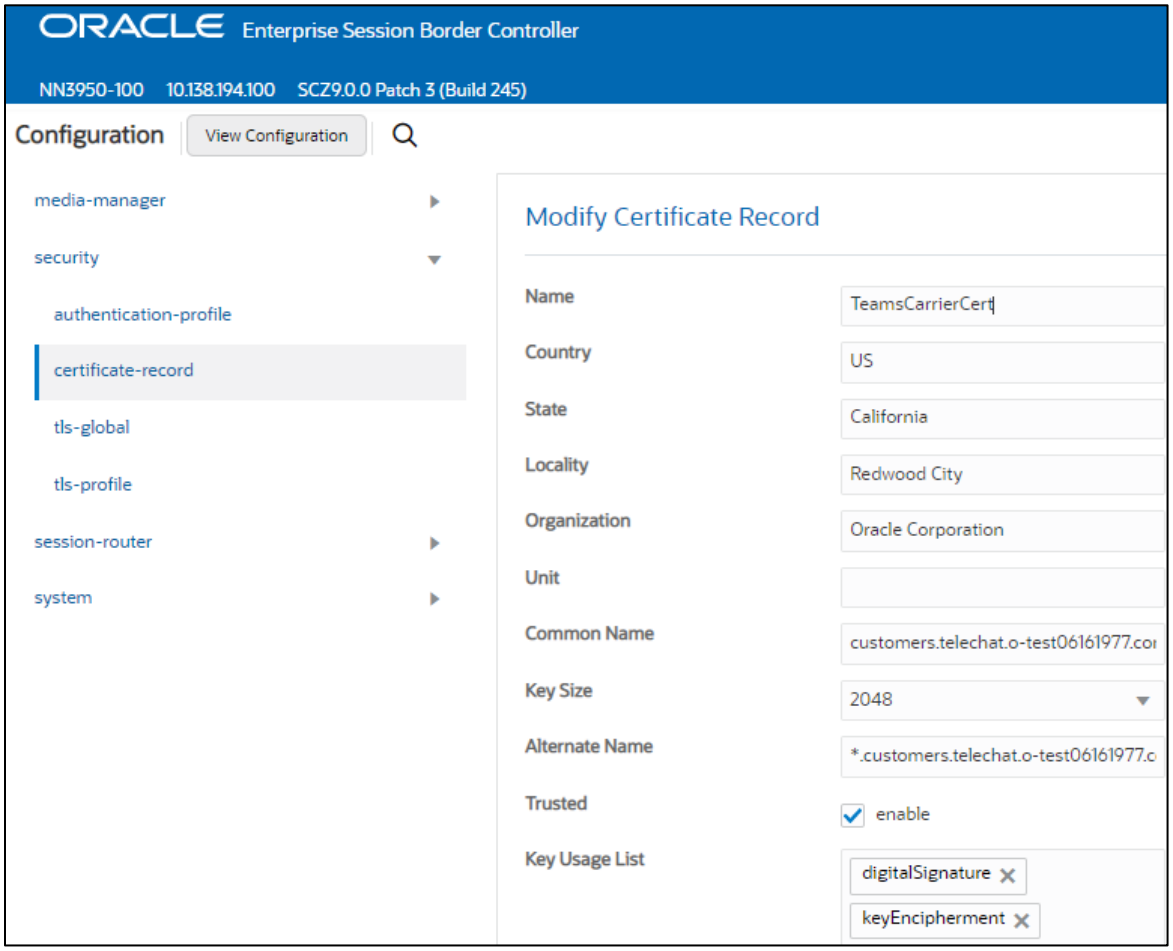
The SBC's end entity certificate is based on the Carrier Model domain structure outlined in the Configuration section of this document. This certificate record must include the following:

- Common name: Carrier Base Domain (**customers.telechat.o-test06161977.com**)

- Alternate Name: *.Carrier Base Domain (***.customers.telechat.o-test06161977.com**)

To Configure the certificate record:

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




- Click OK at the bottom

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

### 9.2.1.2 Root CA and Intermediate Certificates

#### 9.2.1.2.1 GoDaddy CA

The following, DigitCertRoot, 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.

#### 9.2.1.2.2 DigiCert Global Root G2

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 DigiCert Global Root G2.To trust this certificate, your SBC must have the certificate listed as a trusted ca certificate. You can download this certificate here: DigiCert Global Root G2

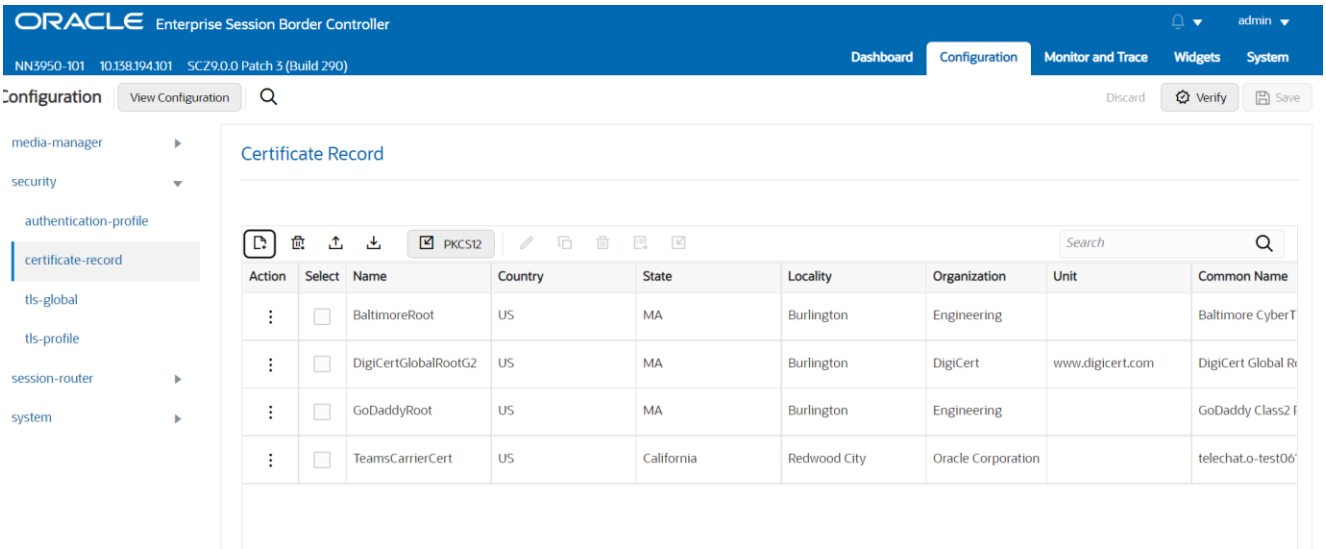
#### 9.2.1.2.3 Baltimore Root

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

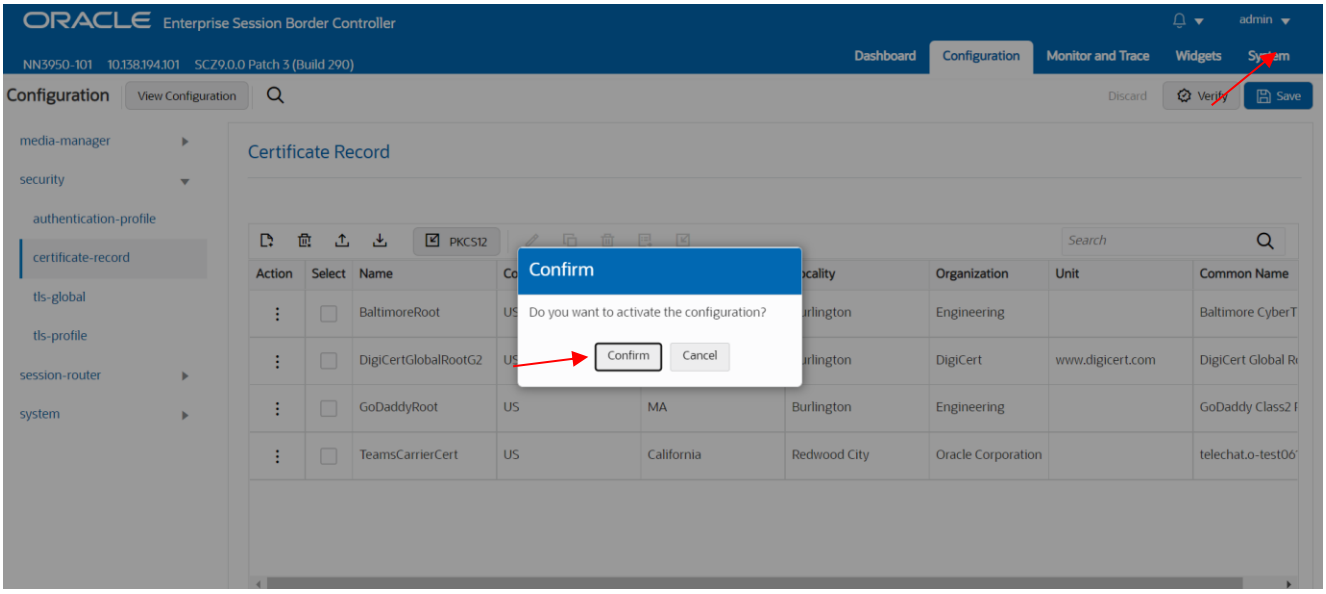
You can download this certificate here: https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt.pem

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

| **Config Parameter** | **Baltimore Root** | **GoDaddy Root** | **DigiCert Global Root G2** |
|---|---|---|---|
| Common Name | Baltimore CyberTrust Root | Go Daddy Class2 Root CA | DigiCert Global Root G2 |
| Key Size | 2048 | 2048 | 2048 |
| Key-Usage-List | digitalSignature<br>keyEncipherment | digitalSignature<br>keyEncipherment | digitalSignature<br>keyEncipherment |
| Extended Key Usage List | serverAuth | serverAuth | serverAuth |
| Key algor | rsa | rsa | rsa |
| Digest-algor | Sha256 | Sha256 | Sha256 |



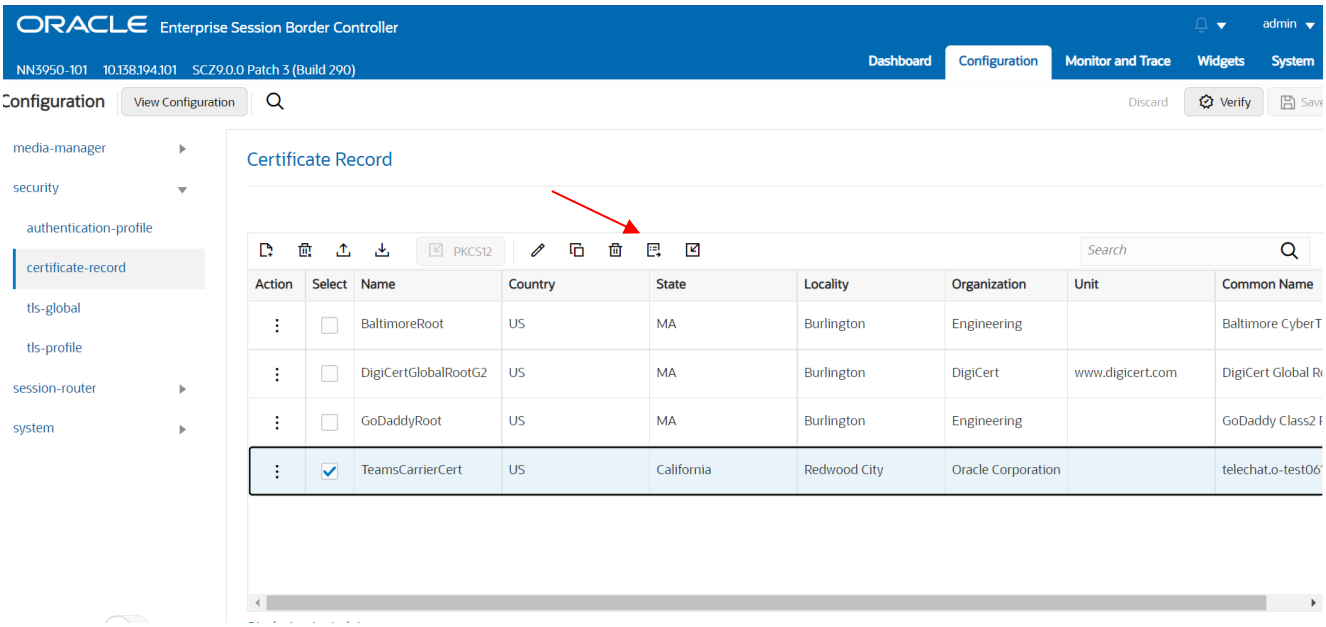

At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must **save and activate** the configuration of the SBC.




#### 9.2.1.3 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 intermidiate 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:





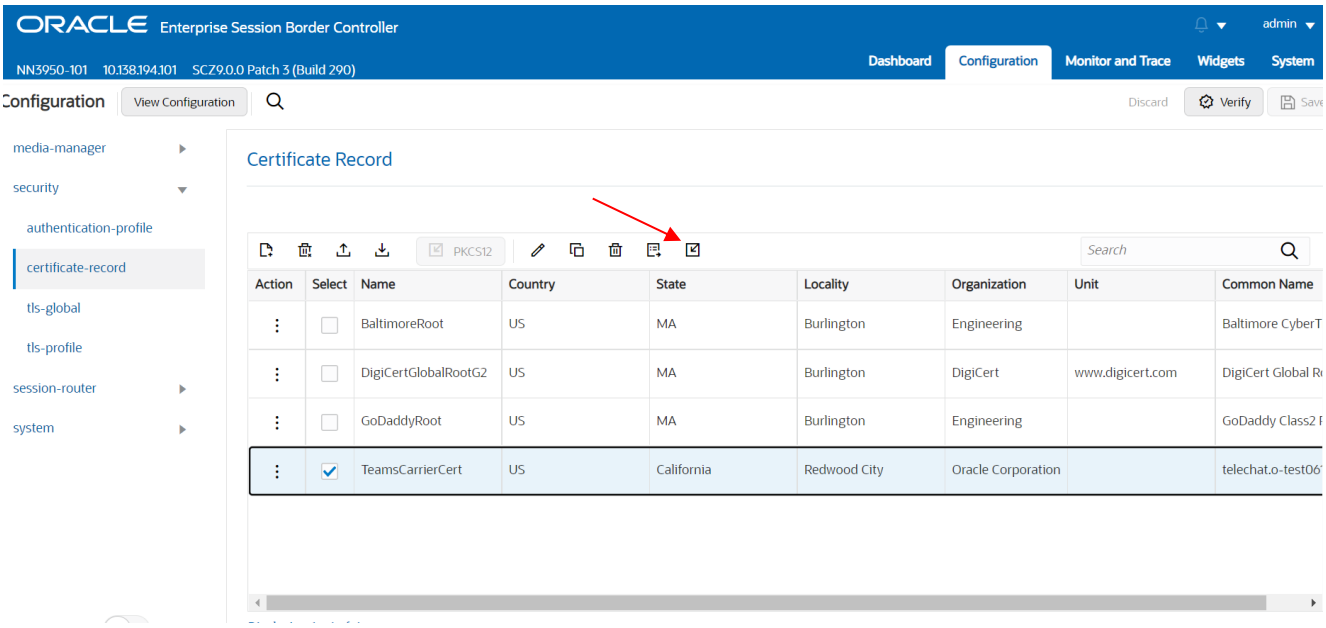
Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, at this point, **another save and activate is required** before you can import the certificates to each certificate record created above.

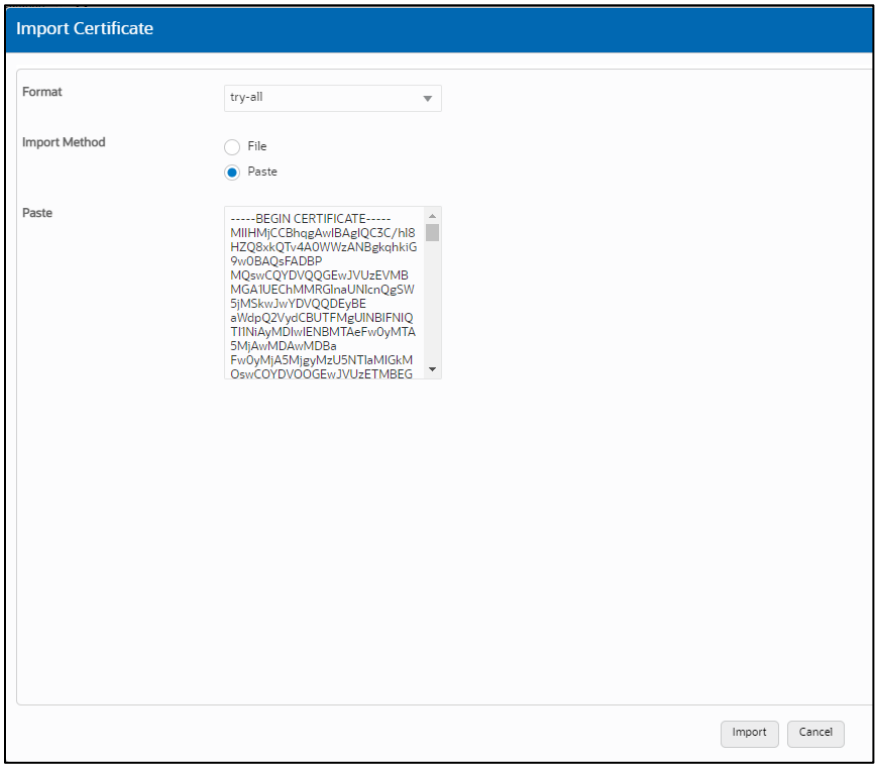
Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

#### 9.2.1.4 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:

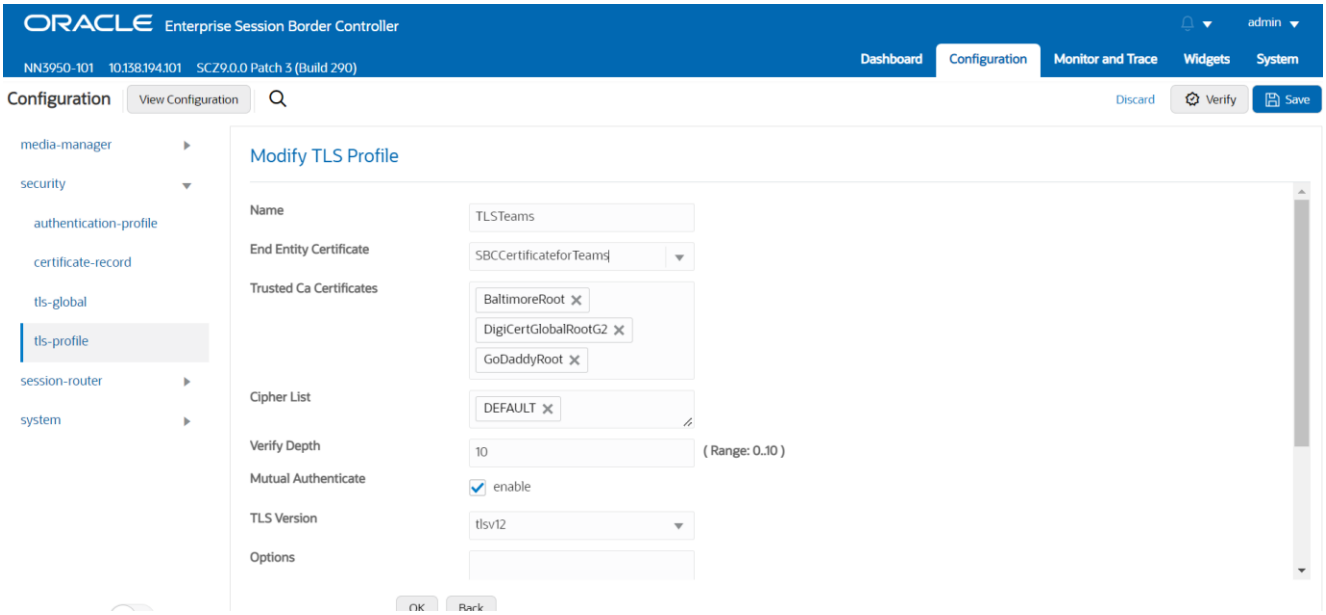
### 9.2.2 TLS Profile

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

GUI Path:  security/tls-profile

ACLI 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.

### 9.2.3 Media Security

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

#### 9.2.3.1 SDES-Profile

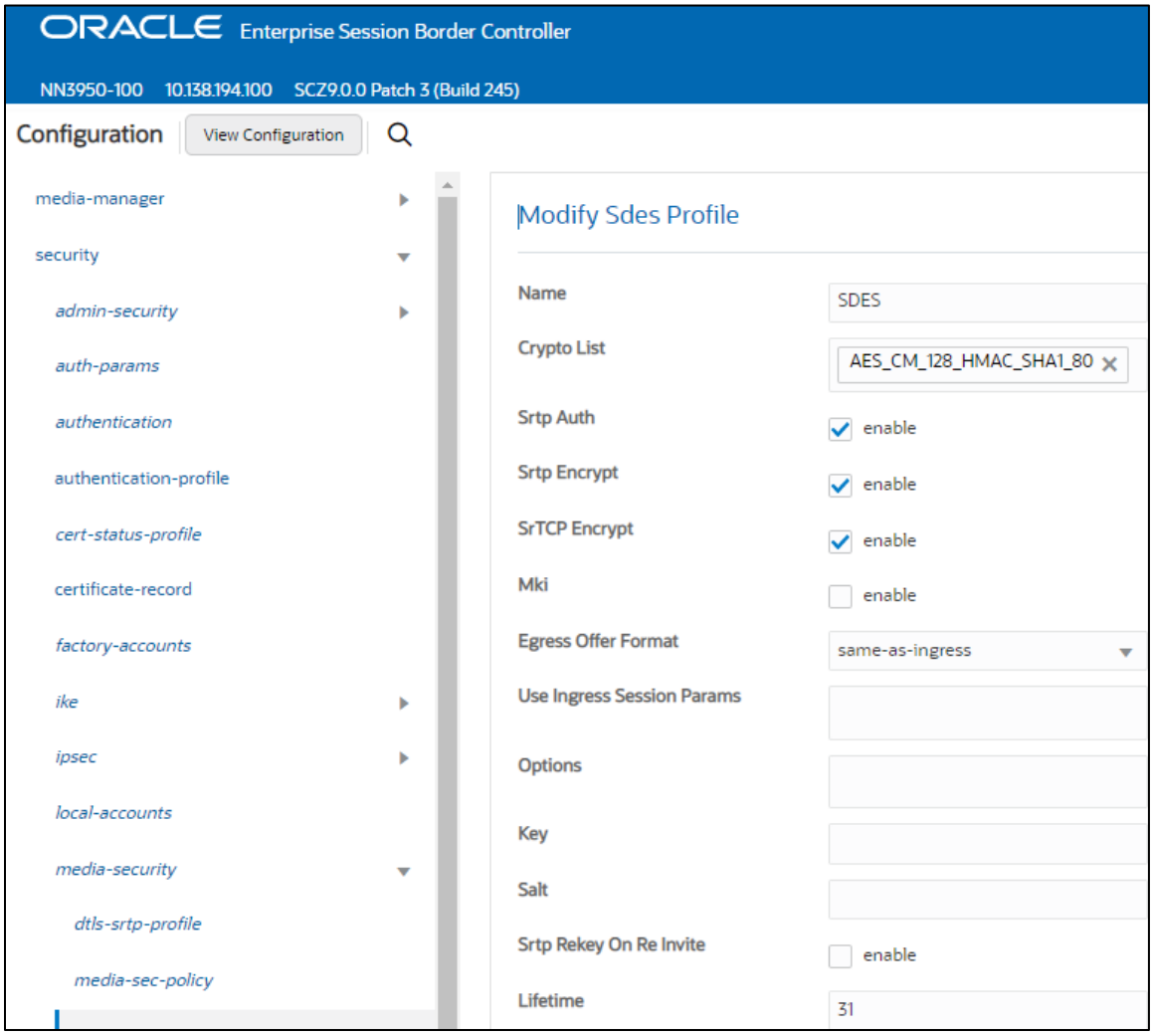
This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured.  The only crypto-suite option supported by Microsoft is AES_CM_128_HMAC_SHA1_80 and must be included in the crypto list

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

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

- Click Add, and use the example below to configure




*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

#### 9.2.3.2 Media Security Policy

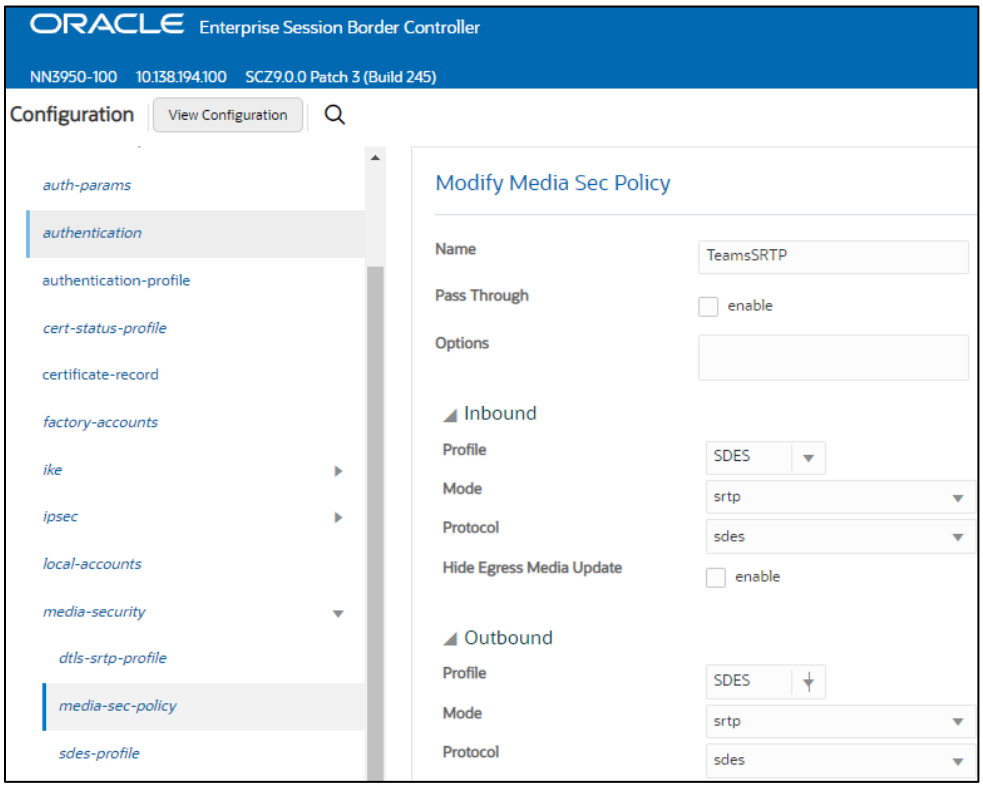
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any) and, if SRTP needs to be used, the sdes-profile that needs to be used

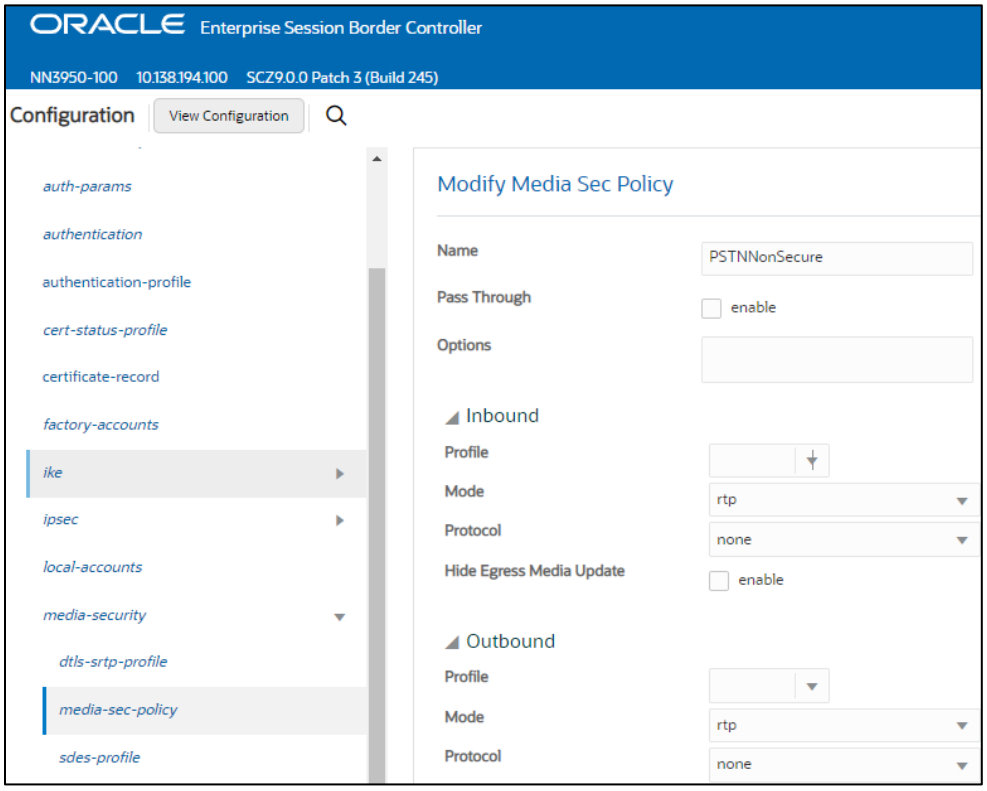
In this example, we are configuring two media security policies. One to secure and decrypt media toward Microsoft Teams, the other for non-secure media facing PSTN.

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

ACLI 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 advanced media termination features and transcoding.

## 9.3 Transcoding Configuration

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

### 9.3.1 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. 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

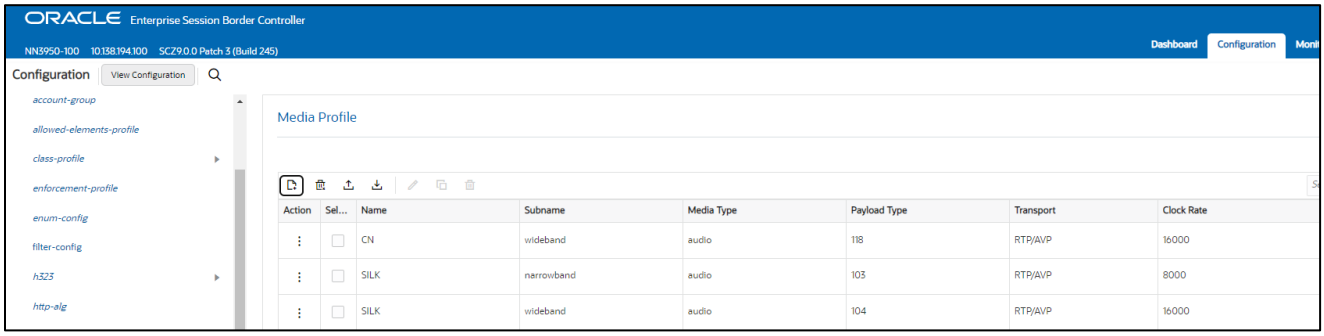
ACLI Path: config t→session-router→media-profile

Configure three media profiles to support the following:

- Silk Wideband
- Silk Narrowband
- CN

Click Add, then use the table below as an example to configure each:

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




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

### 9.3.2 Codec Policies

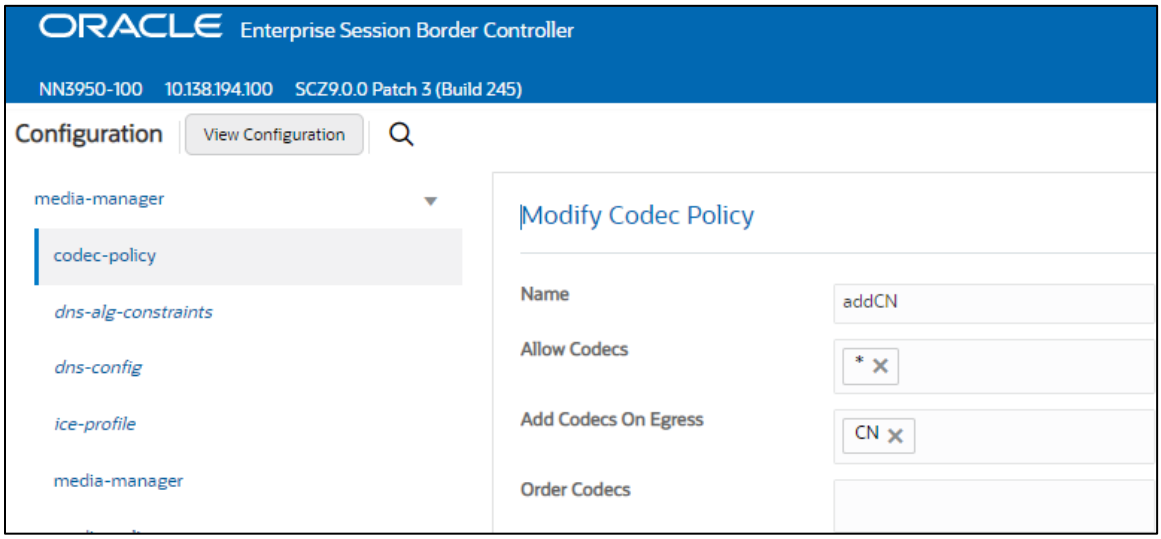
Codec policies are sets of rules that specify the manipulations to be performed on SDP offers allowing the Oracle SBC the ability to add, strip, and reorder codecs for SIP sessions.

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.  To satisfy this requirement, the SBC uses transcoding resources to generate those packets, which does require a codec policy be configured and assigned.

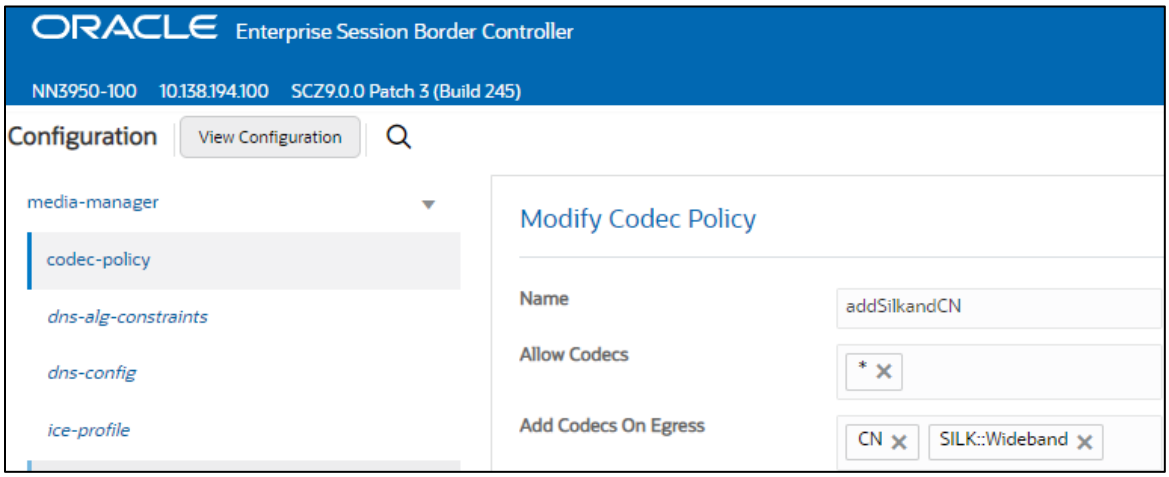
GUI Path: media-manager/codec-policy

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

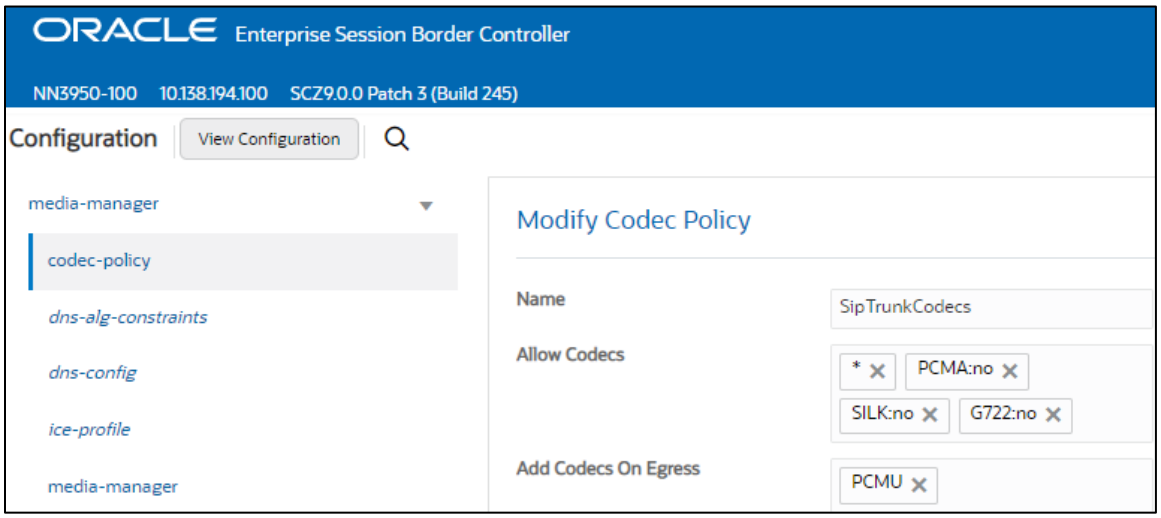
Here is an example config of a codec policy used for the SBC to generate CN packets towards Teams.




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:




Lastly, since some SIP Trunks may have issues with the codecs being offerened 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

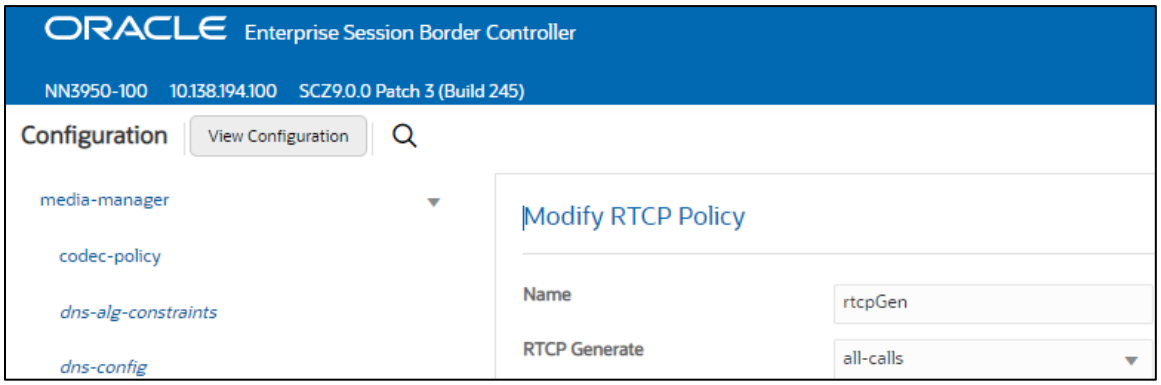
### 9.3.3 RTCP Policy

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

### 9.3.4 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

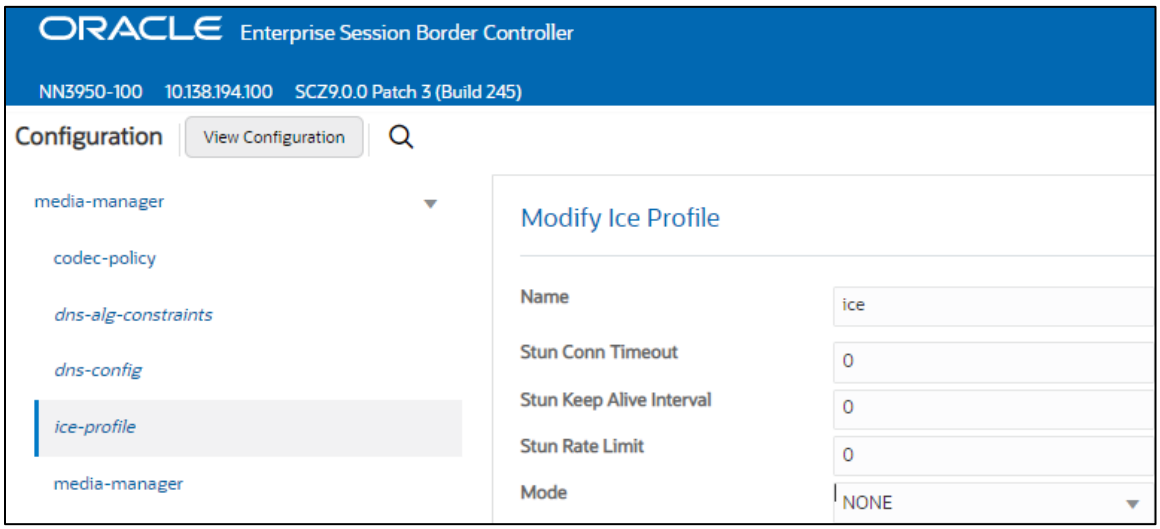
The use of ICE is required only if using Teams with Media Bypass enabled.

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




*When deploying the Oracle SBC with Microsoft Teams, we recommend changing the default values for Stun Conn Timeout, Stun Keep Alive Interval, and Stun Rate Limit to a value of 0 (zero) from their default values.*

- 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.

## 9.4 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.

### 9.4.1 Media Manager

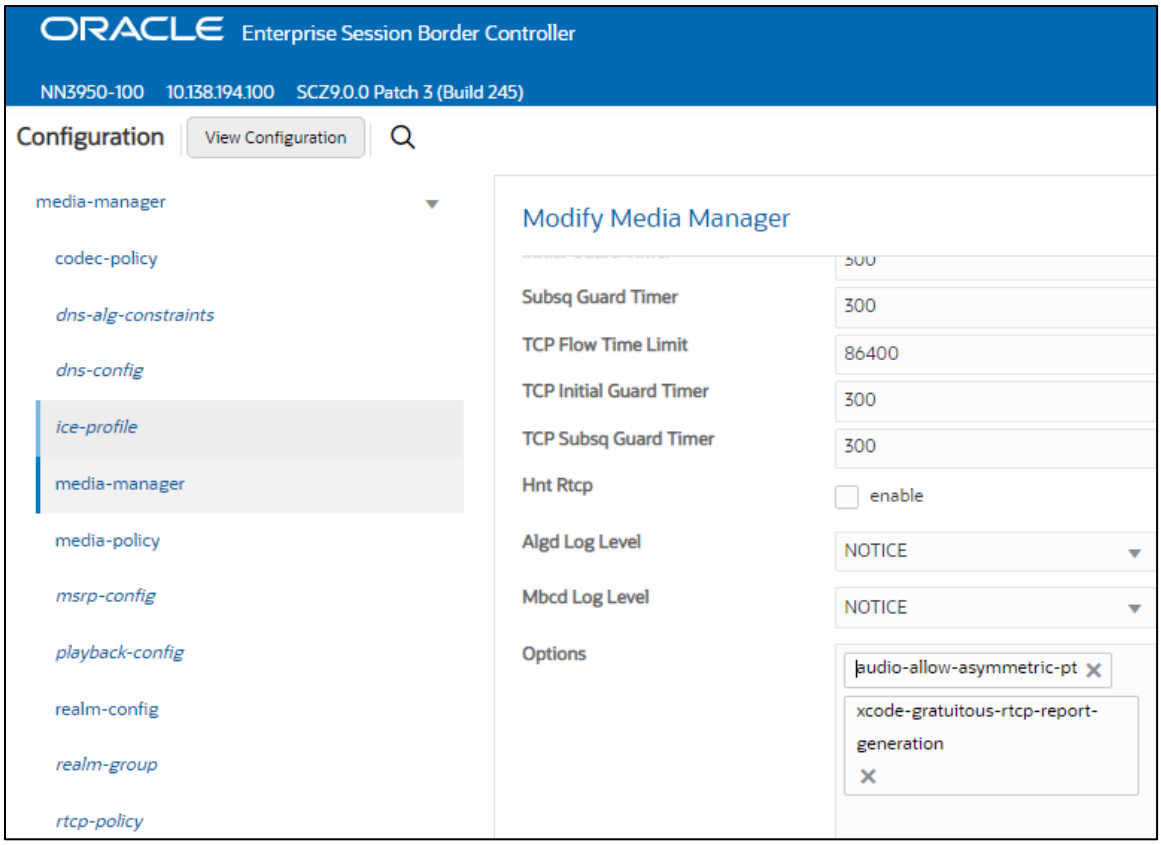
To configure media functionality on the SBC, you must first enabled the global media manager

GUI Path: media-manager/media-manager

ACLI 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

### 9.4.2 Realm Config

**Nested Realm for Teams**

Nested Realms is an OCSBC feature that supports hierarchical realm groups. One or more realms may be nested within a higher order realm. This allows the OCSBC to separate each tenant the Carrier Model SBC is servicing.

In this example we will create two realms facing MSFT Teams.

A parent realm for Teams and a child realm for a customer tenant. The parent realm will contain the carrier base domain, and the Tenant realm will contain the customer's carrier subdomain.

We'll also be creating a third, standalone realm facing PSTN.

GUI Path; media-manger/realm-config

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

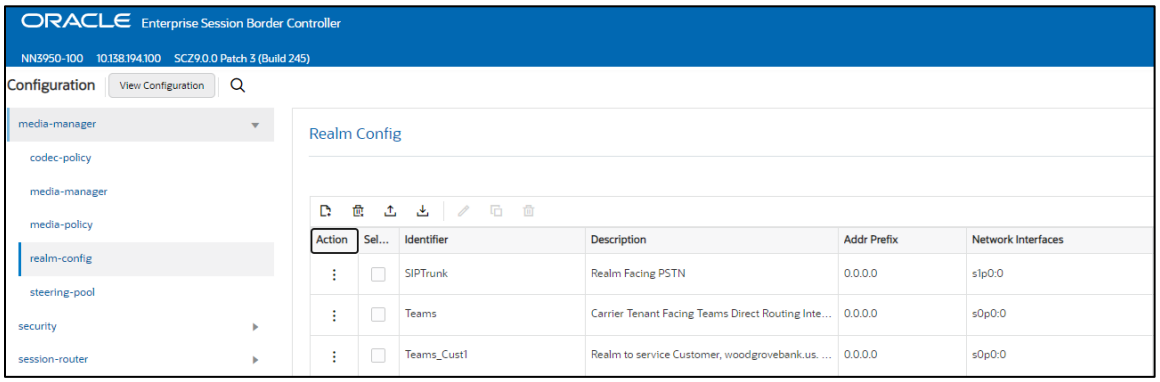
- Click Add, and use the following table as a configuration example for the three realms used in this configuration example

| Config Parameter | Teams Realm | Tenant Realm | PSTN Realm |
|---|---|---|---|
| Identifier | Teams | Teams_Cust1 | SipTrunk |
| Network Interface | s0p0:0 | s0p0:0 | s1p0:0 |
| Mm in realm | ☑ | ☑ | ☑ |
| Media Sec policy | TeamsSRTP | TeamsSRTP | PSTNNonSecure |
| Teams-FQDN | Customers.telechat.o-test06161977.com | Sbc1.customers.telechat.o-test06161977.com | |
| Teams-fqdn-in-uri | ☑ | ☑ | |
| Sdp-inactive-only | ☑ | ☑ | |
| RTCP mux | ☑ | ☑ | |
| ice profile | Ice (required for media bypass only) | Ice (required for media bypass only) | |
| Codec policy | addCN | addCN | SipTrunkCodecs |
| RTCP policy | rtcpGen | rtcpGen | |
| Access-control-trust-level | HIGH | HIGH | HIGH |
| Parent Realm | | Teams | |

Additional Realms can be added, one for each customer tenant the Oracle SBC is servicing. The carrier subdomain registered in each tenanr needs to be added under the “Teams-FQDN” parameter in the realm.

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

### 9.4.3 Steering Pools

Steering pools define sets of ports that are used for steering media flows through the OCSBC.

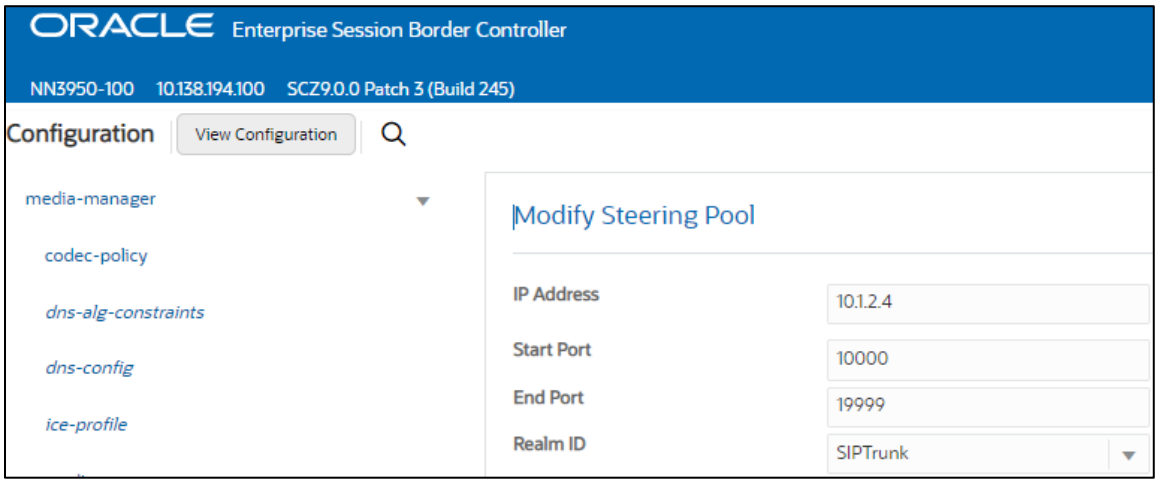
These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

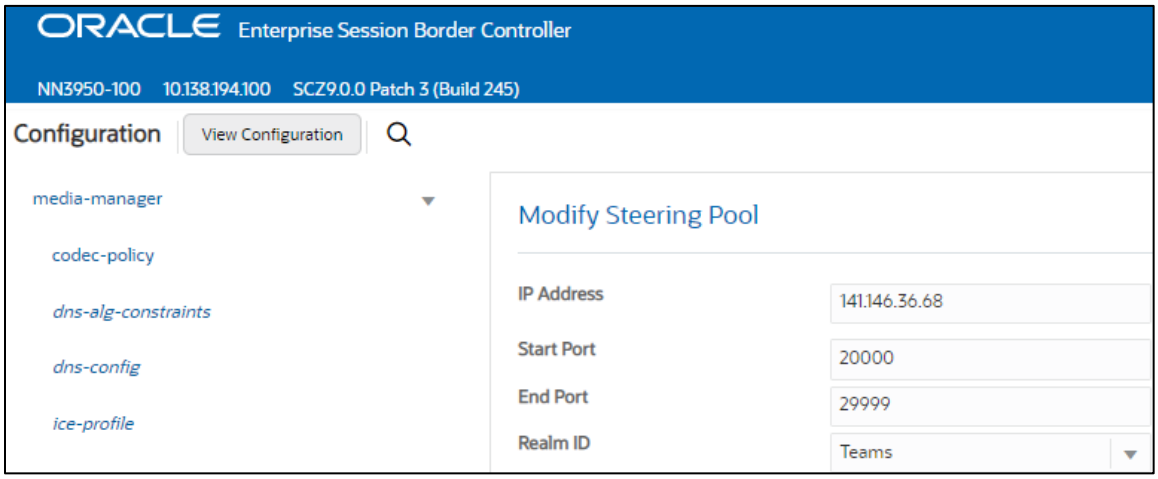
We configure one steering pool for PSTN.  The other facing Teams.

GUI Path: media-manger/steering-pool

ACLI 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.

## 9.5 Sip Configuration

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

### 9.5.1 Sip-Config

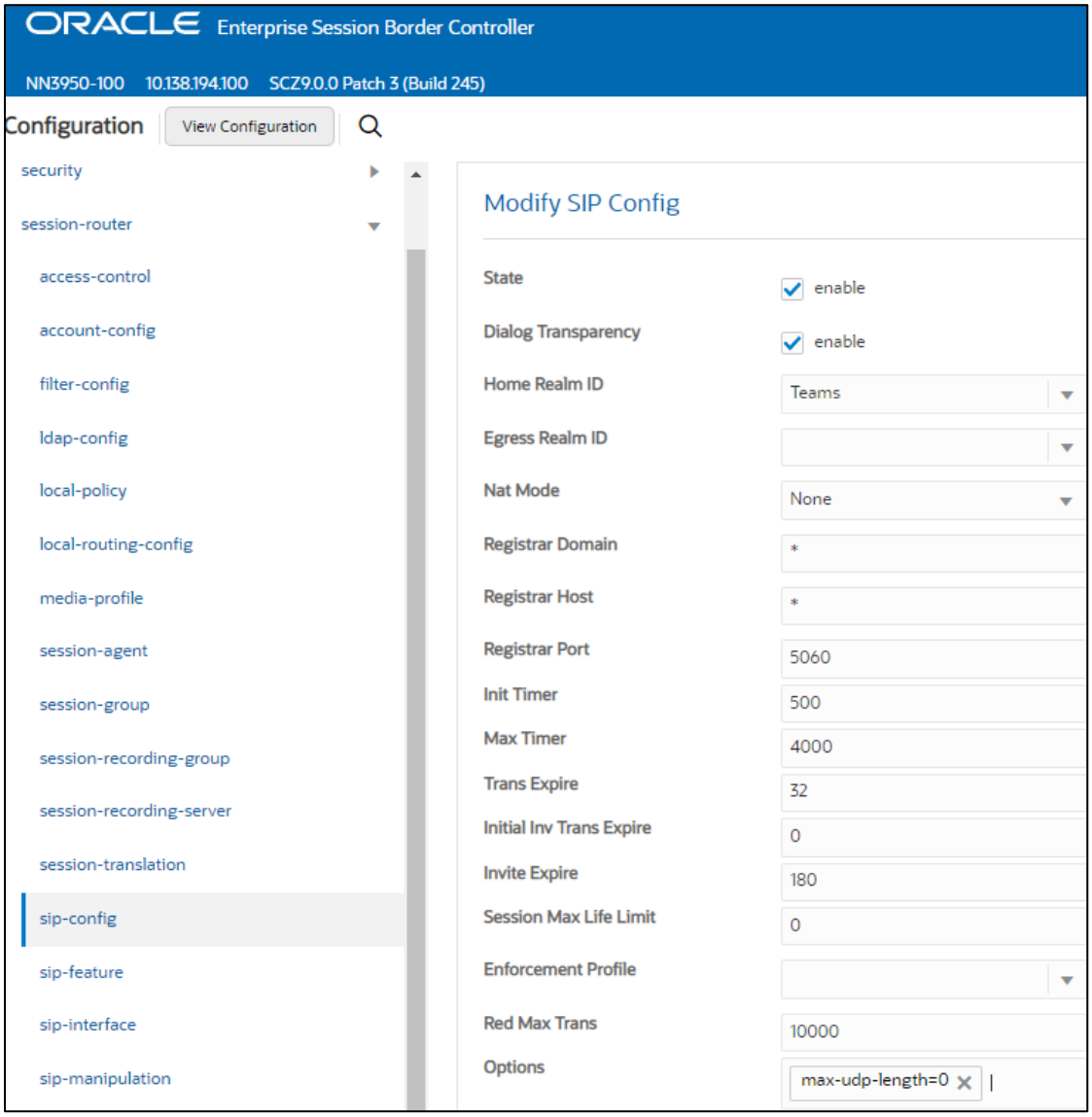
To enable sip related objects on the Oracle SBC, you must first configure the global Sip Config element:

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

### 9.5.2 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:

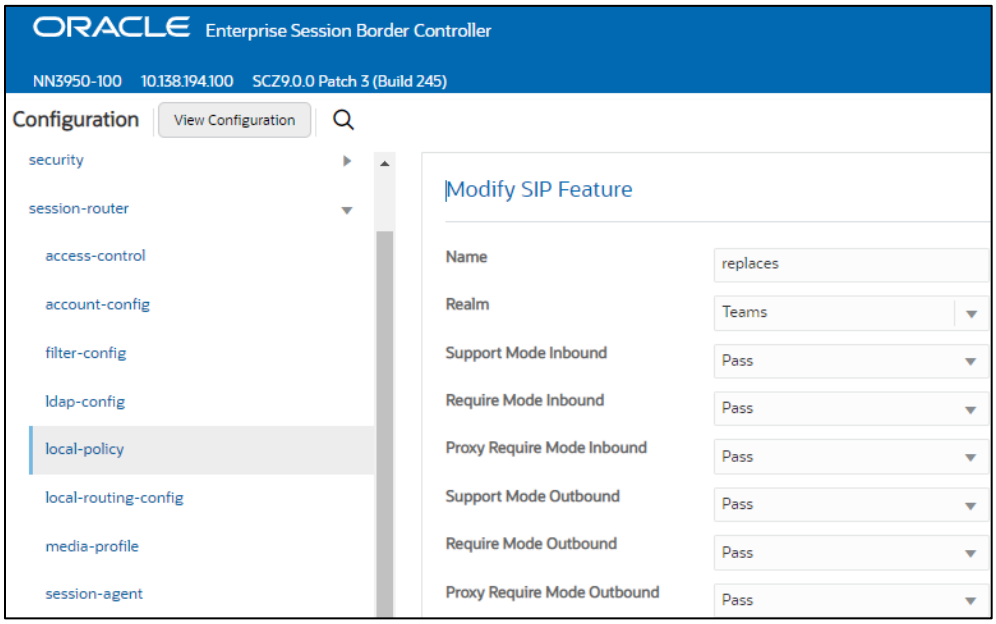
#### 9.5.2.1 Sip Feature

The sip feature configuration element allows 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

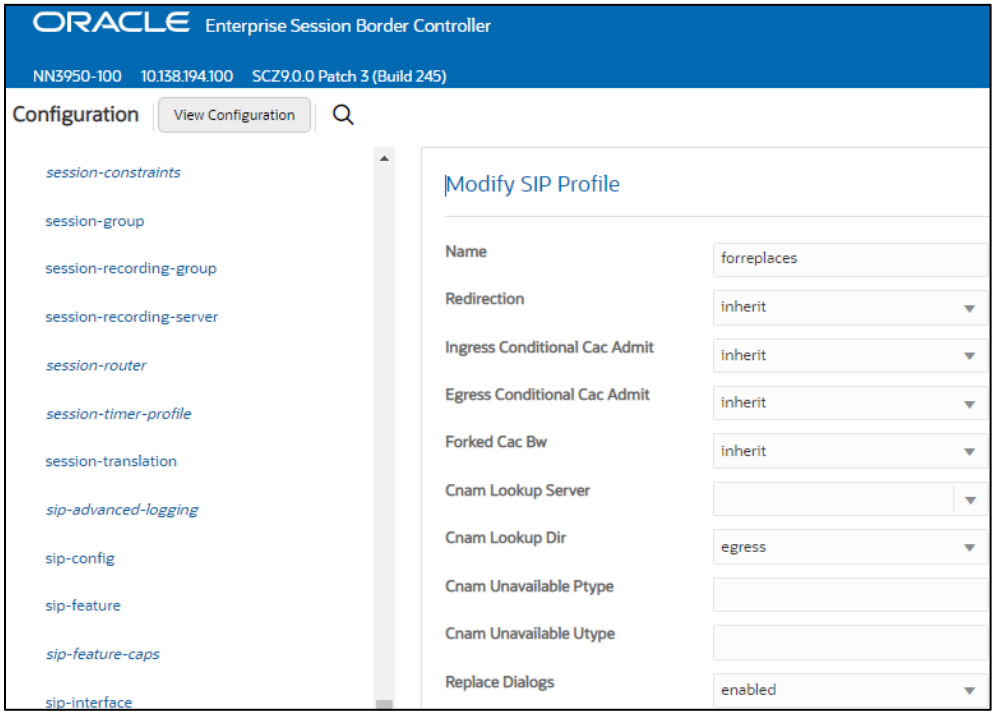
#### 9.5.2.2 Sip Profile

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

### 9.5.3 Sip Interface

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

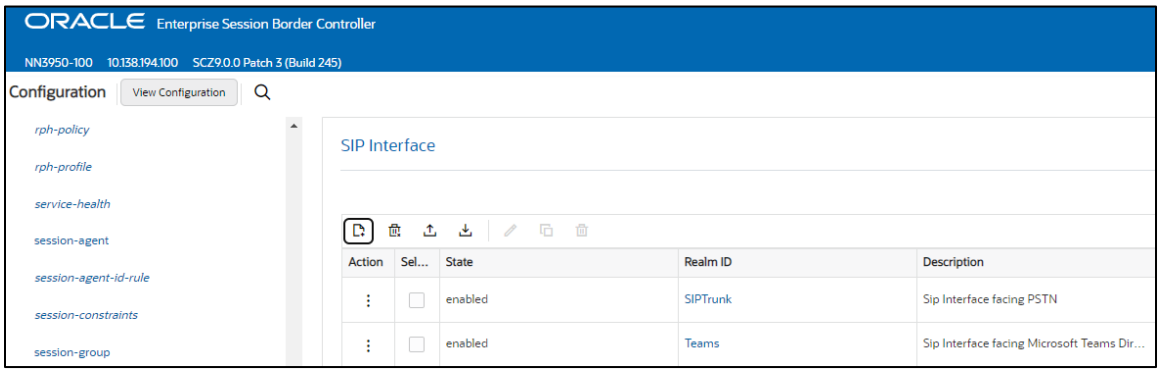
Configure two sip interfaces, one associated with PSTN Realm, and the other for Teams. You only need to configure a single sip interface facing Microsoft Teams Direct Routing. All realms for customers tenants inherit the sip interface from the Teams parent realm

GUI Path: session-router/sip-interface

ACLI 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 | 141.146.36.68 |
| 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, and the sip-profile which allows the SBC to act on the Replaces header when received by Microsoft Teams.

- Select OK at the bottom of each when applicable

### 9.5.4 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.

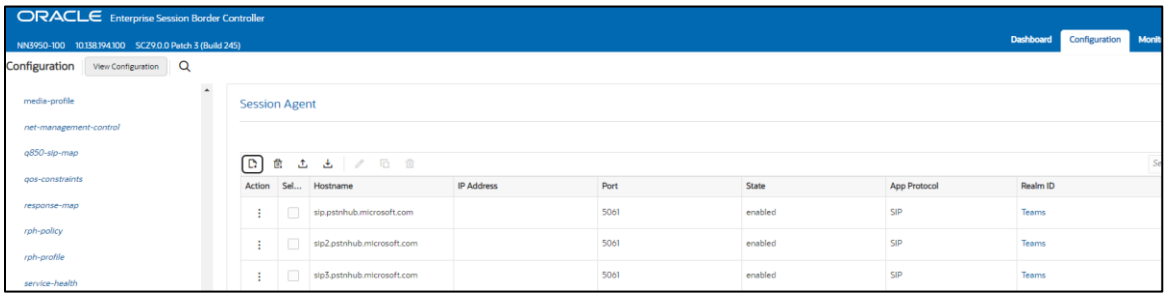
GUI Path: session-router/session-agent

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

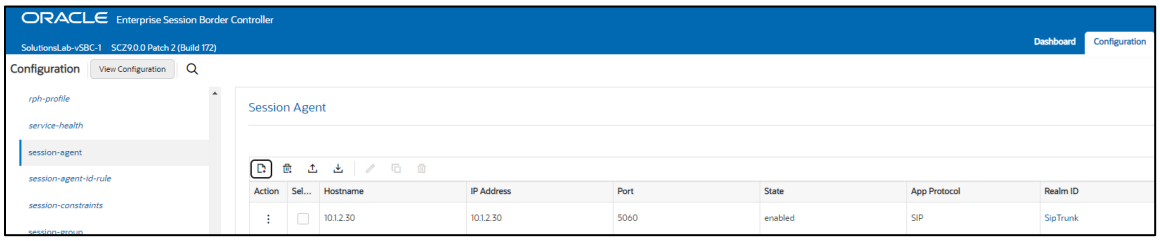
You will need to configure three Session Agents for the Microsoft Direct Routing Interface

- 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

### 9.5.5 Session Group

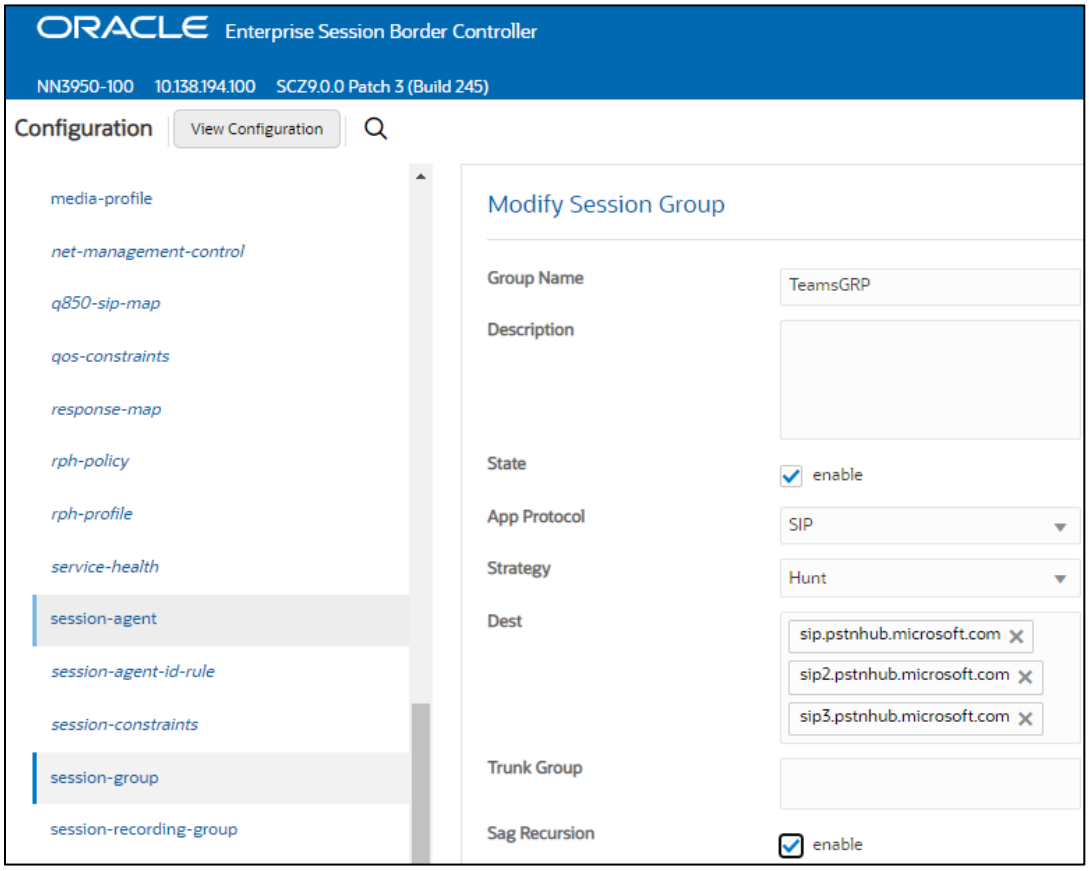
A session agent group allows the SBC to create a load balancing model:

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

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

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




- Click OK at the bottom

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

## 9.6 Routing Configuration

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

The OCSBC has multiple routing options that can be configured based on environment. For this example configuration, we are utilizing the OCSBC's multistage local policy routing feature along with DID separation via local route table.

A routing stage signifies a re-evaluation of local policy based on the results of a local policy lookup. In the simplest, single stage case, the Session Border Controller performs a local policy lookup on a SIP message's Request URI. The result of that local policy lookup is a next hop FQDN, IP address, ENUM lookup, or LRT lookup; that result is where the Session Border Controller forwards the message. In the multistage routing model, that resultant next hop is used as the lookup key for a second local policy lookup

### 9.6.1 LRT

The OCSBC supports LRT, an XML document that contains either E164 telephone numbers or strings-to-SIP-URI mappings. An iLRT is configured and transferred from the development environment to the OCSBC /code/lrt directory. After installation and configuration, the LRT is available for SIP Request routing. For more information on creating and configuring LRT, please see the OCSBC 9.0 Configuration Guide, Chapter 8.

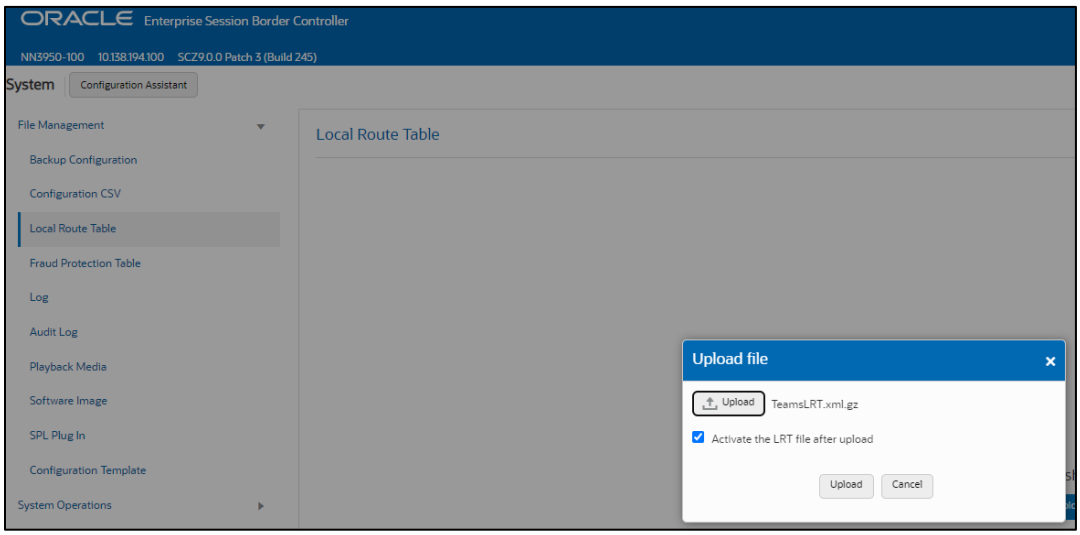
The following is an example Lrt file, once created, will be placed in the /code/lrt directory on the OCSBC

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<localRoutes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<!—Customer 1 Tenant: solutionslab.cgbubedford.com/sbc1.customers.telechat.o-test06161977.com -->
        <route>
                <user type="E164">17814437242</user>
                <next type="regex">!^.*!sip:\0@sbc1.customers.telechat.o-test06161977.com!</next>
</route>
        <route>
                <user type="E164">17814437247</user>
                <next type="regex">!^.*!sip:\0@sbc1.customers.telechat.o-test06161977.com!</next>
</route>
        <route>
                <user type="E164">17814437245</user>
                <next type="regex">!^.*!sip:\0@sbc1.customers.telechat.o-test06161977.com!</next>
</route>
<!-- Customer 2 Tenant – woodgrovebank.us/sbc2.customers.telechat.o-test06161977.com-->
        <route>
                <user type="E164">17814437243</user>
                <next type="regex">!^.*!sip:\0@sbc2.customers.telechat.o-test06161977.com!</next>
</route>
        <route>
                <user type="E164">17814437244</user>
                <next type="regex">!^.*!sip:\0@sbc2.customers.telechat.o-test06161977.com!</next>
</route>
        <route>
                <user type="E164">17814437388</user>
                <next type="regex">!^.*!sip:\0@sbc2.customers.telechat.o-test06161977.com!</next>
</route>
```

The LRT file, once created, can be copied to the /code/lrt directory of the SBC via SFTP to the management IP, or uploaded through the GUI:

#### 9.6.1.1 GUI Upload of LRT File

- At the top, click on the System Tab
- Left Hand side, expend File Management and select Local Route Table
- Click Upload
- Browse to select file to upload to SBC
- Check box “Activate LRT file after upload”
- Click Upload




### 9.6.2 Local Routing Config

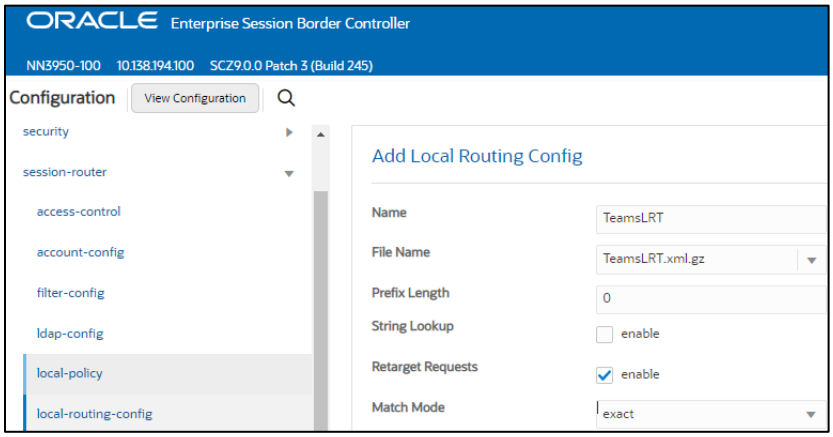
After moving the DID-range-based LRT to the /code/lrt directory on the OCSBC, use the following procedure to specify the file’s location, and the lookup method.

GUI Path: session-router/local-routing-config

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

Click Add, use the following as an example to configure

*Note: the file name field below is the full name of the LRT file that has been placed in the /code/lrt directory on the OCSBC*



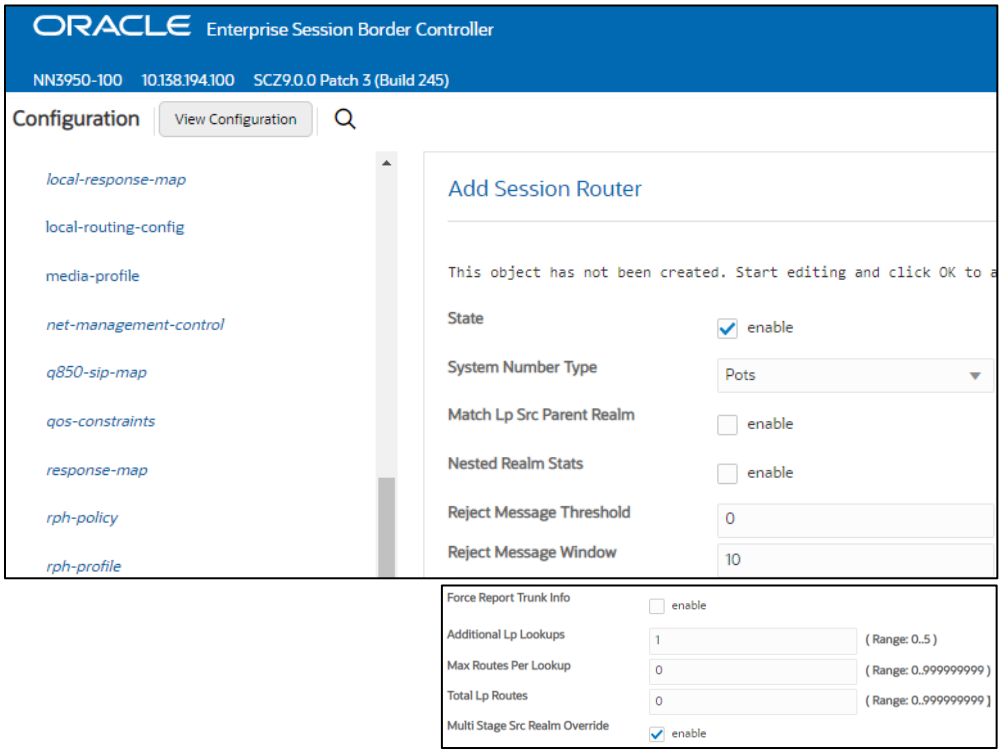
### 9.6.3 Session Router Config

Session router config allows for the SBC to perform multistage routing.

GUI Path: session-router/session-router

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

Use the following example to configure session router config:




- Click OK at the bottom

### 9.6.4 Local Policy Configuration

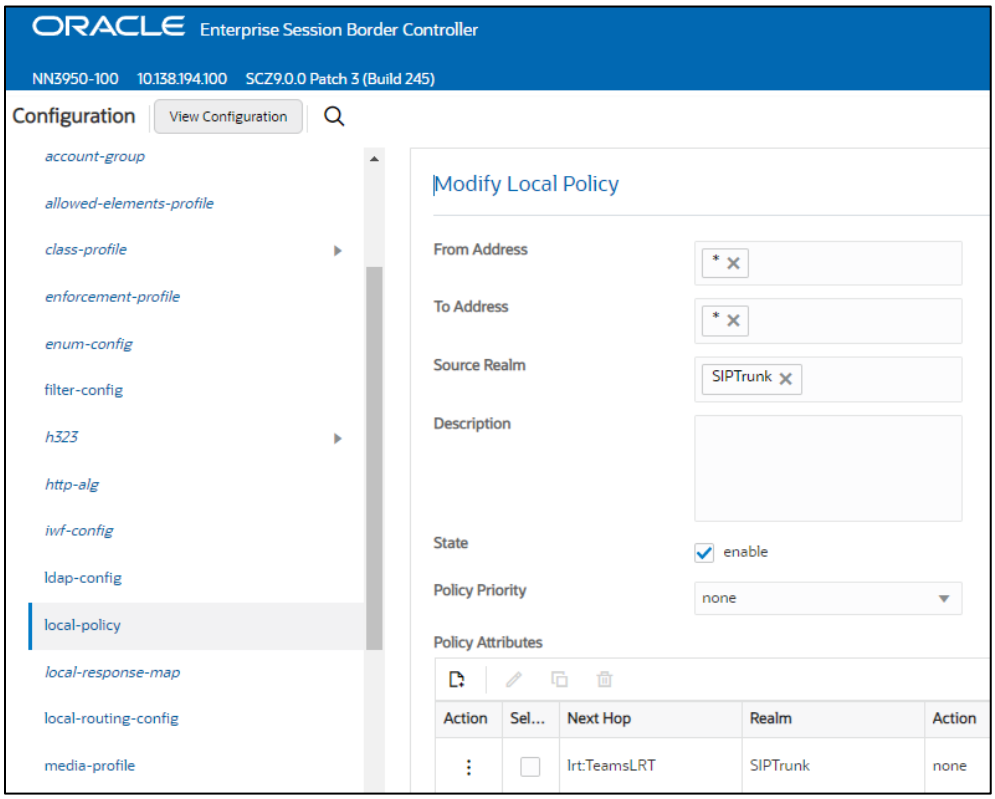
Local Policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria.

GUI Path: session-router/local-policy

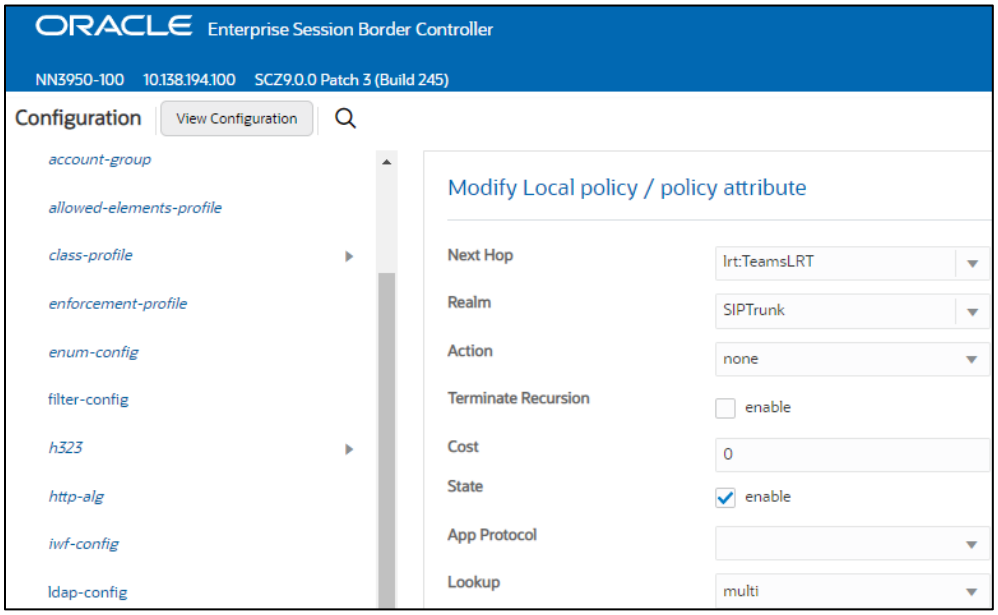
ACLI Path: config t→session-router→local-policy

To route Sip traffic to and from Microsoft Teams Direct Routing Interface, the following local policies will need to be configured.

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

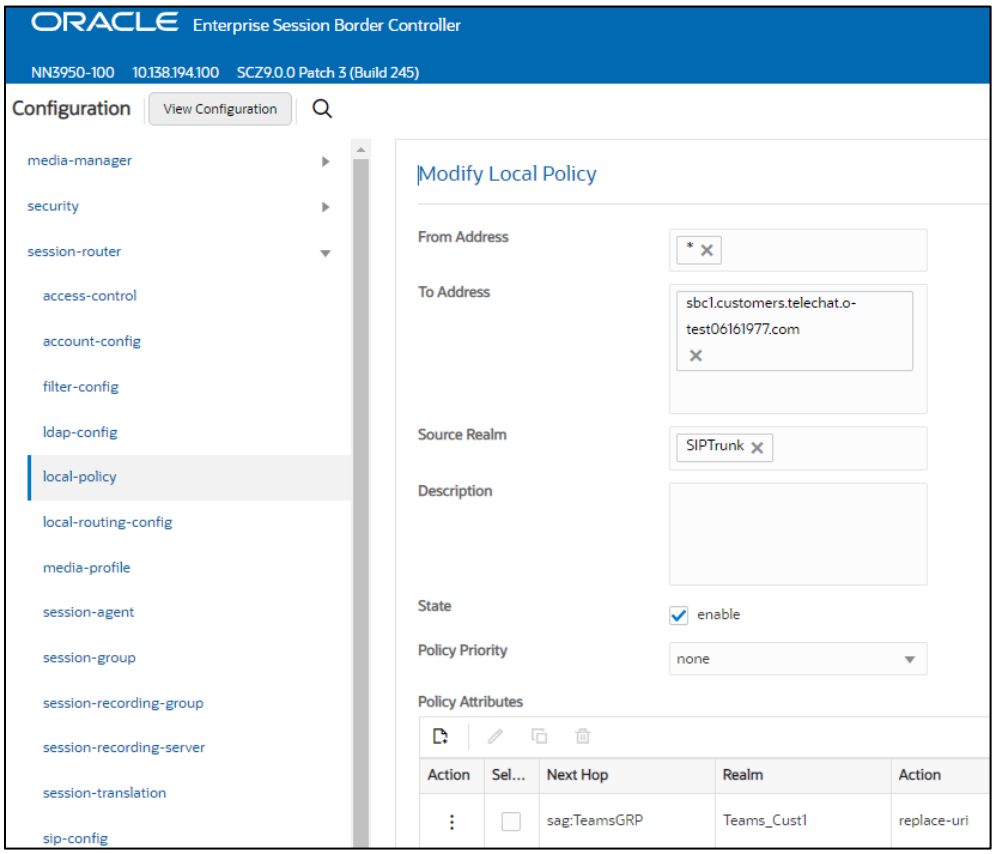



Policy Attribute:

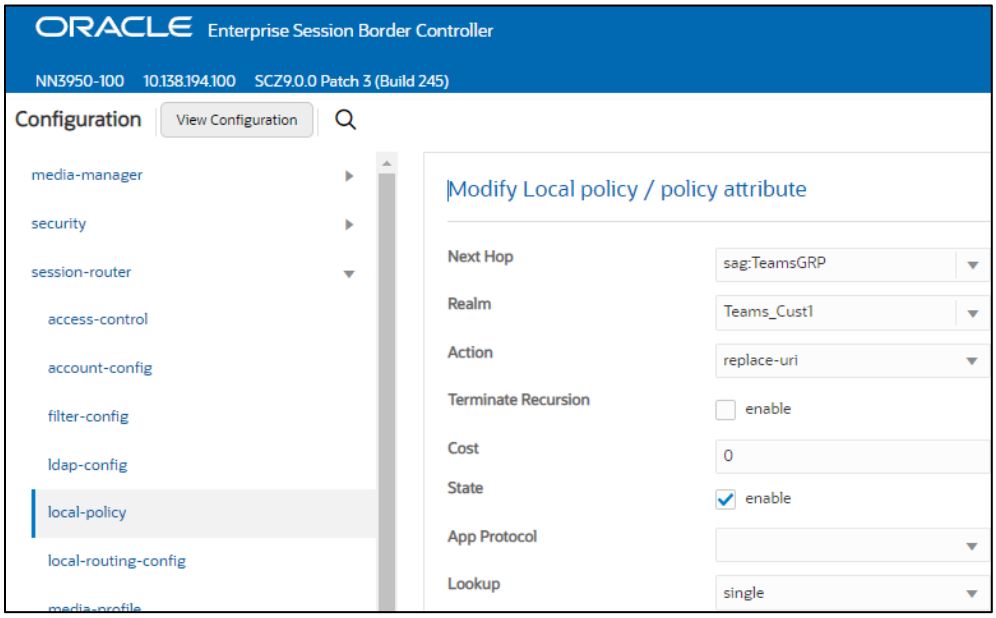



The above local policy utilizes the lrt /local-routing-config- outlined previously in this document. This is a way to identify the terminating tenant/subdomain when the core network ie..SIPTrunk, does not identify the target in the Request-Uri host. When the target subdomain/tenant is identified in the Request-Uri host, the following local policies will route directly to Teams Group by to-address match.

- Call from Sip Trunk to Customer 1 Tenant:



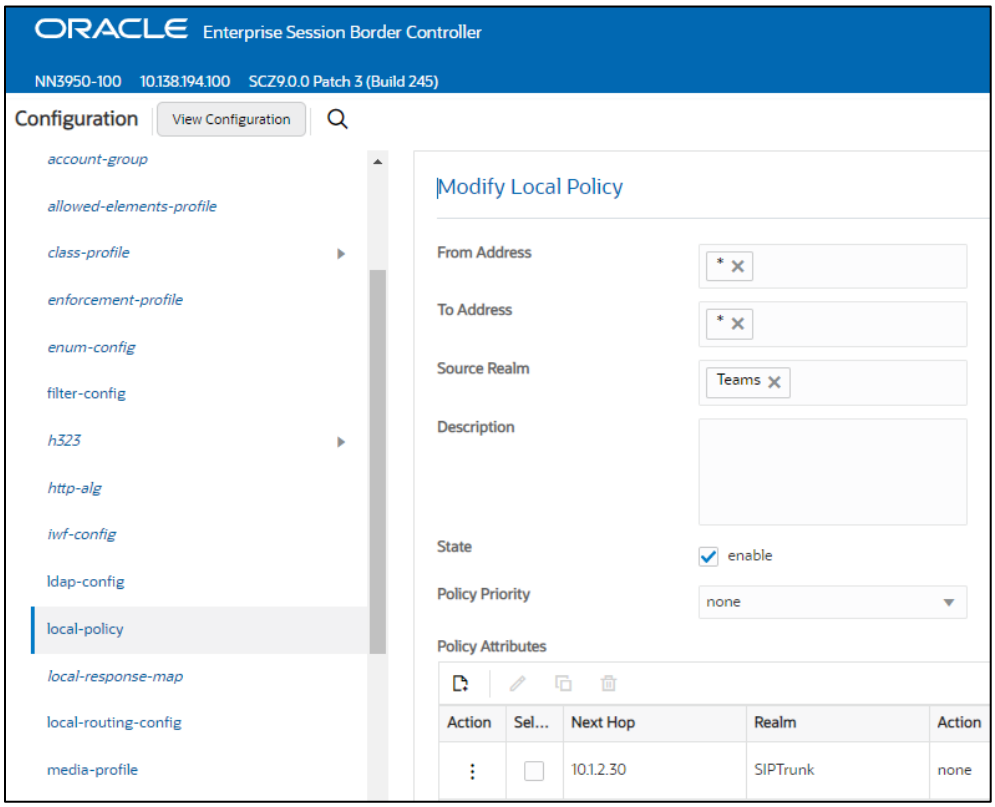

Policy Attribute:



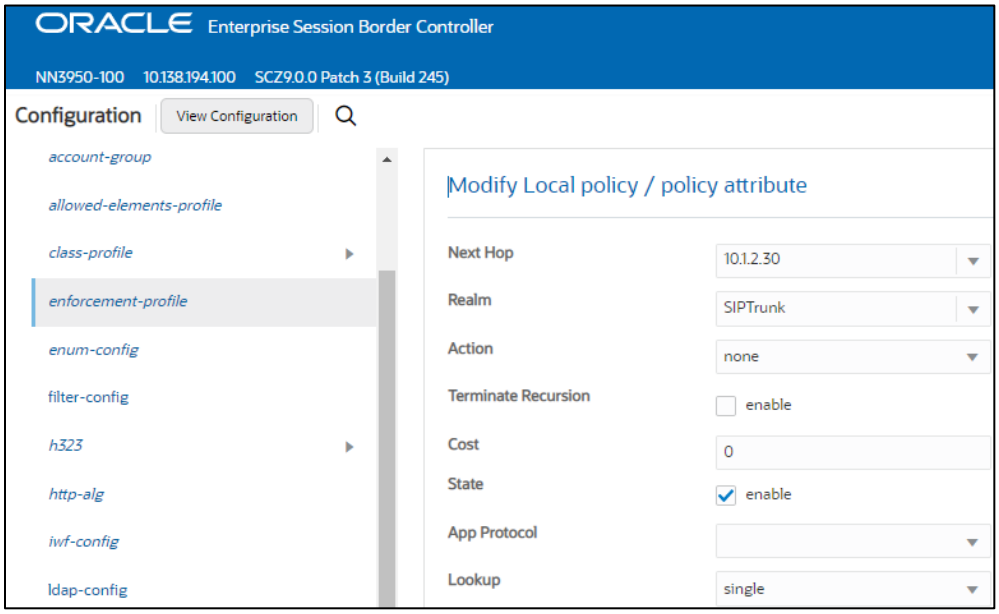

- Click OK at the bottom

Using the above example, continue for each customer tenant being hosted by this OCSBC.

Next, we'll configure a local policy to route all traffic from Teams Direct Routing to Sip Trunk




Policy Attribute:




- Click OK at the bottom of each when applicable:

## 9.7 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 only from trusted IP's with a trust level of high

2. Set the access control trust level on public facing realms to HIGH

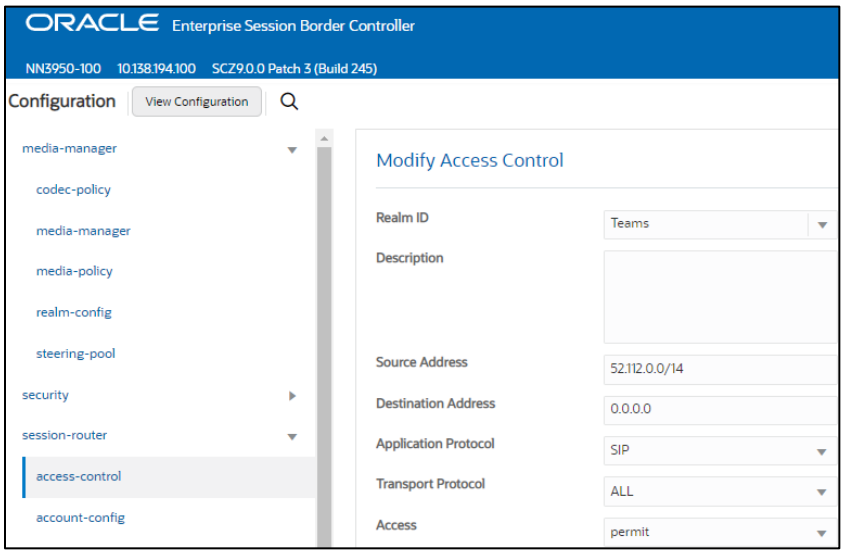
Microsoft Teams has two subnets, 52.112.0.0/14 and 52.120.0.0/14 that must be allowed to send traffic to the SBC. Both must be configured as an access control on the Oracle SBC and associated with the Teams realm.

Use this example to create ACL's for both 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.




- Click OK at the bottom

The SBC configuration is now complete. Move to verify the connection with Microsoft Direct Routing Interface.

# 10 Verify Connectivity

## 10.1 OCSBC Options Ping

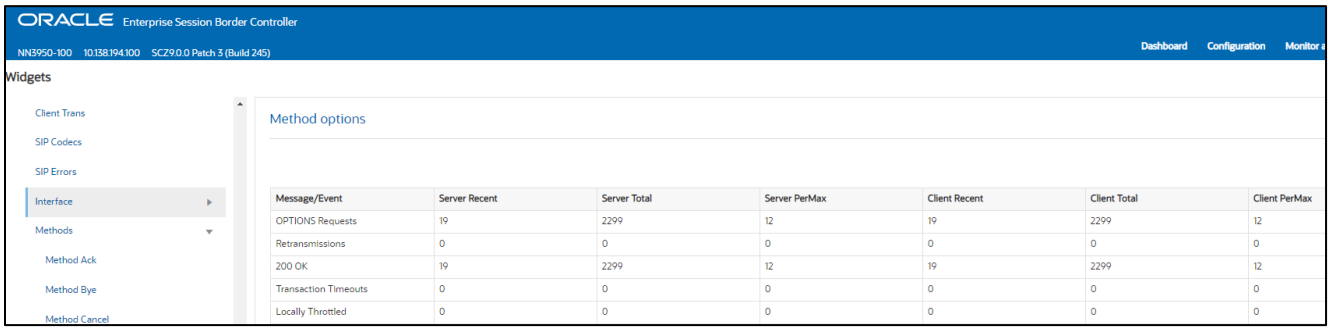
After you've paired the OCSBC with Direct Routing using the New-CsOnlinePSTNGateway PowerShell command, validate that the SBC can successfully exchange SIP Options with Microsoft Direct Routing.

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

- At the top, click “Wigits”

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

GUI Path: Signaling/SIP/Methods/Method OPTIONS




| Message/Event | Server Recent | Server Total | Server PerMax | Client Recent | Client Total | Client PerMax |
|---|---|---|---|---|---|---|
| OPTIONS Requests | 19 | 2299 | 12 | 19 | 2299 | 12 |
| Retransmissions | 0 | 0 | 0 | 0 | 0 | 0 |
| 200 OK | 19 | 2299 | 12 | 19 | 2299 | 12 |
| Transaction Timeouts | 0 | 0 | 0 | 0 | 0 | 0 |
| Locally Throttled | 0 | 0 | 0 | 0 | 0 | 0 |

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

## 10.2 Microsoft SIP Tester Client

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

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

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

Download the script and Documentation here:

Sip Tester Client script and documentation

# 11 Syntax Requirements for SIP Invite and SIP Options:

Microsoft Teams Hybrid Voice Connectivity interface 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.

## 11.1 Terminology

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

## 11.2 Requirements for Invite Messages

Picture 1 Example of INVITE message

```
INVITE sip:17814437383@sbc1.customers.telechat.o-test06161977.com;transport=tls SIP/2.0
Via: SIP/2.0/TLS 155.212.214.173:5061;branch=z9hG4bK3rfq6u10d8f8fonro0k0.1
From: sip:9785551212@ sbc1.customers.telechat.o-test06161977.com;transport=tls:5061;tag=0A7C0BFE
To: <sip: 17814437383@sip.pstnhub.microsoft.com:5061>
Call-ID: F3154A1E-F3AE-4257-94EA-7F01356AEB55-268289@192.168.4.180
CSeq: 1 INVITE
Content-Length: 245
Content-Type: application/sdp
Contact: <sip:9785551212@ sbc1.customers.telechat.o-test06161977.com:5061;user=phone;transport=tls>
Allow: ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, REFER, UPDATE
User-Agent: Oracle SBC
```

### 11.2.1 Contact.Header Invite:

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

## 11.3 Requirements for OPTIONS Messages

Picture 2 Example of OPTIONS message

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

### 11.3.1 Contact Header OPTIONS:

- When sending OPTIONS to the Direct Routing Interface, the “Contact” header should have SBC FQDN in URI. This will be the FQDN registered in the carrier tenant.
- 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 back to the SBC

## 11.4 Microsoft Teams Direct Routing Interface characteristics

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

| Category | Parameter | Value | Comments |
|---|---|---|---|
| Ports and IP | SIP Interface FQDN Name | Refer to Microsoft documentation | |
| | IP Addresses range for SIP interfaces | Refer to Microsoft documentation | |
| | SIP Port | 5061 | |
| | IP Address range for Media | Refer to Microsoft documentation | |
| | Media port range on Media Processors | Refer to Microsoft documentation | |
| | Media Port range on the client | Refer to Microsoft documentation | |
| Transport and Security | SIP transport | TLS | |
| | Media Transport | SRTP | |
| | SRTP Security Context | DTLS, SIPS Note: DTLS is not supported until later time. Please configure SIPS at this moment. Once support of DTLS announced it will be the recommended context | https://tools.ietf.org/html/rfc5763 |
| | Crypto Suite | AES_CM_128_HMAC_SHA1_80, non-MKI | |
| | Control protocol for media transport | SRTCP (SRTCP-Mux recommended) | Using RTCP mux helps reduce number of required ports |
| | Supported Certification Authorities | Refer to Microsoft documentation | |
| | Transport for Media Bypass (of configured) | ICE-lite (RFC5245) – recommended,<br>· Client also has Transport Relays | |
| Codecs | Audio codecs | · G711<br>· Silk (Teams clients)<br>· Opus (WebRTC clients) - Only if Media Bypass is used;<br>· G729<br>· G722 | |
| | Other codecs | · CN<br>. Required narrowband and wideband<br>· RED – Not required<br>· DTMF – Required<br>· Events 0-16<br>· Silence Suppression – Not required | |

# 12 Appendix A

## 12.1 SBC Behind NAT SPL configuration

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

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

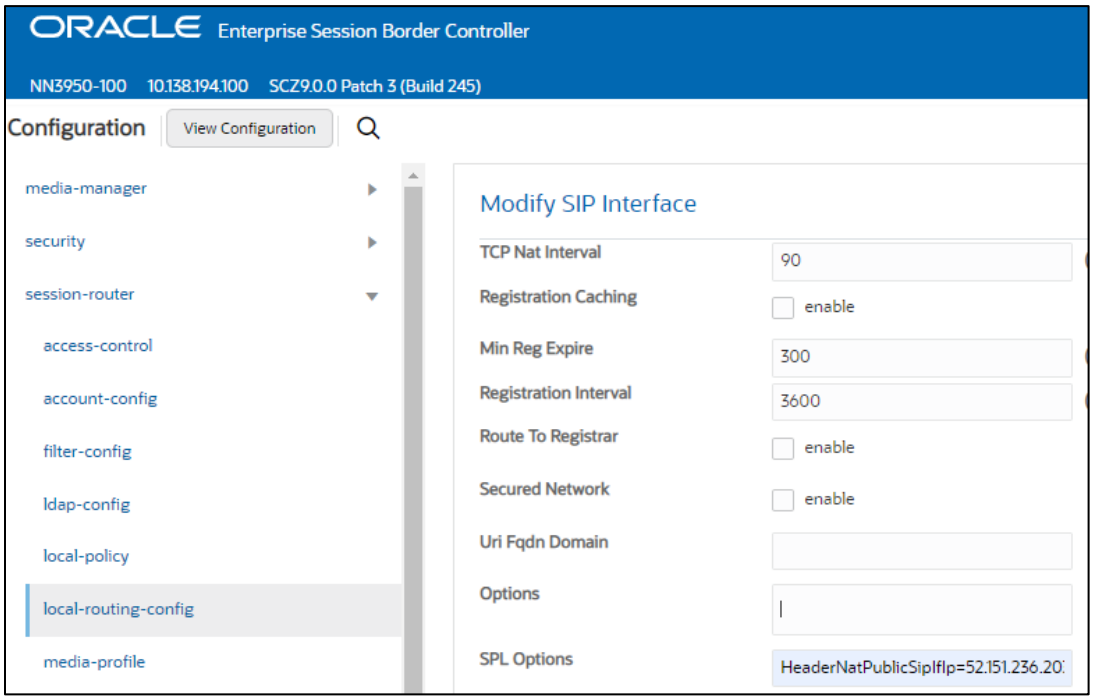
- The private IP address must be the same as the SIP Interface and steeping pool IP address, both of which must match
- The public IP address must be the public IP address of the NAT device

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

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

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.0.4.4

Here HeaderNatPublicSipIfIp is the public interface ip and HeaderNatPrivateSipIfIp is the private ip configured on the OCSBC.




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

# 13 Appendix B

## 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 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.

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

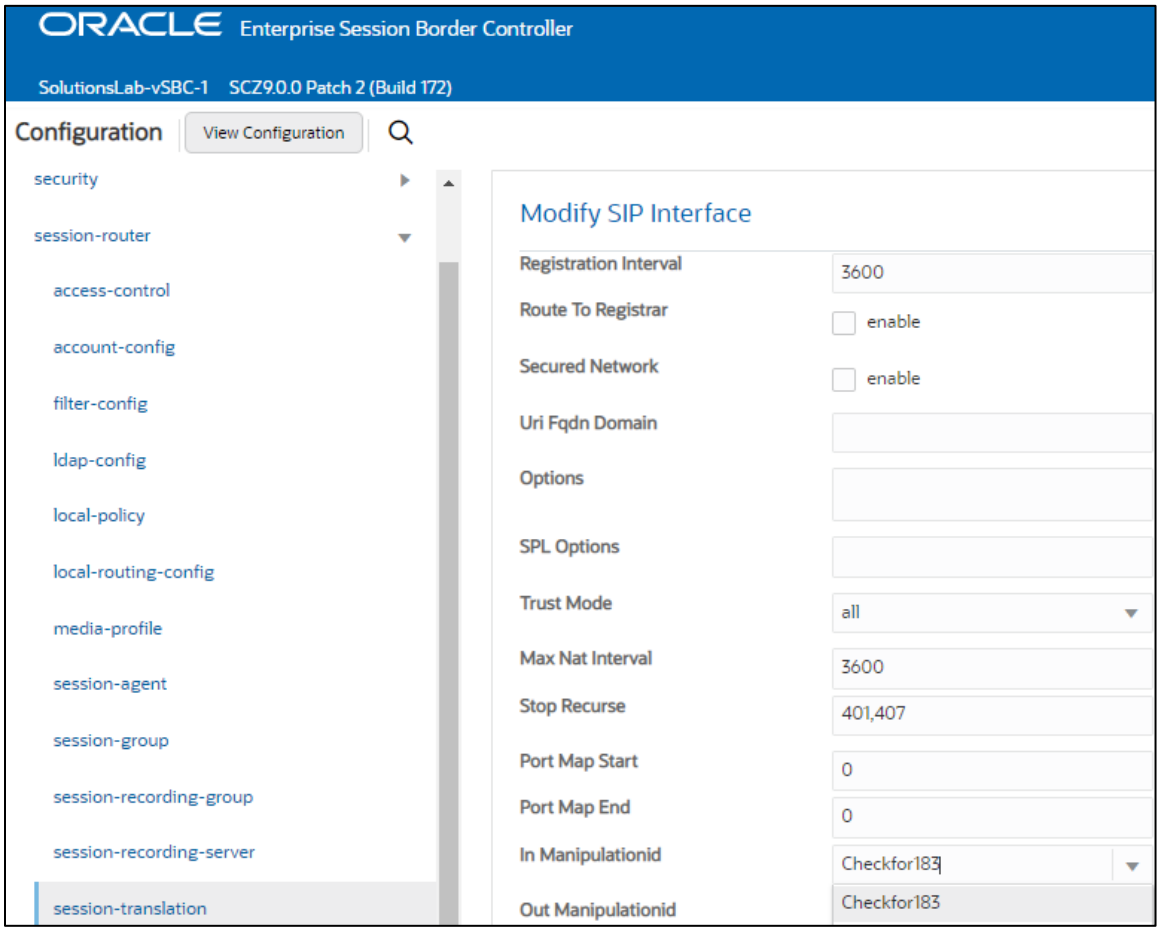
This sip manipulation will be applied as the in-manipulationid on the Teams Sip Interface.

```
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        checklineforsbcip
                type        c
                action      store
                comparison-type pattern-rule
                match-value ^(.(?!(141.146.36.68))).*$
    mime-sdp-rule
        name                delete183SDP
        msg-type            reply
        methods             Invite
        action              delete
        comparison-type     boolean
        match-value         $if183.$au.$checklineforsbcip
    header-rule
        name                change183to180
        header-name         @status-line
        action              manipulate
        comparison-type     boolean
        match-value         $if183.$au.$checklineforsbcip
        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:

GUI Path:  Session Router/Sip Interface

ACLI 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 can generate ringback upon receipt of the sip REFER from Microsoft.

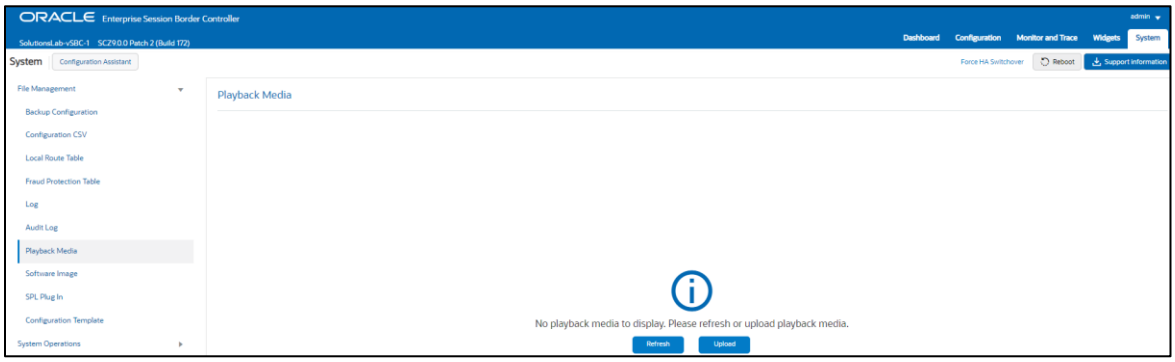
First, you must create a media file.

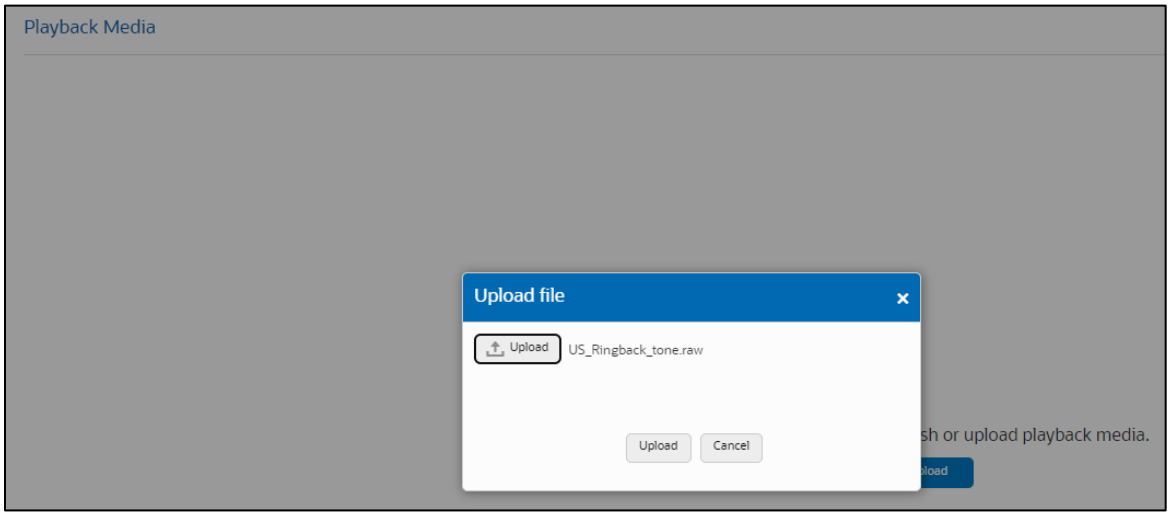
### 13.2.2 Media Files

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

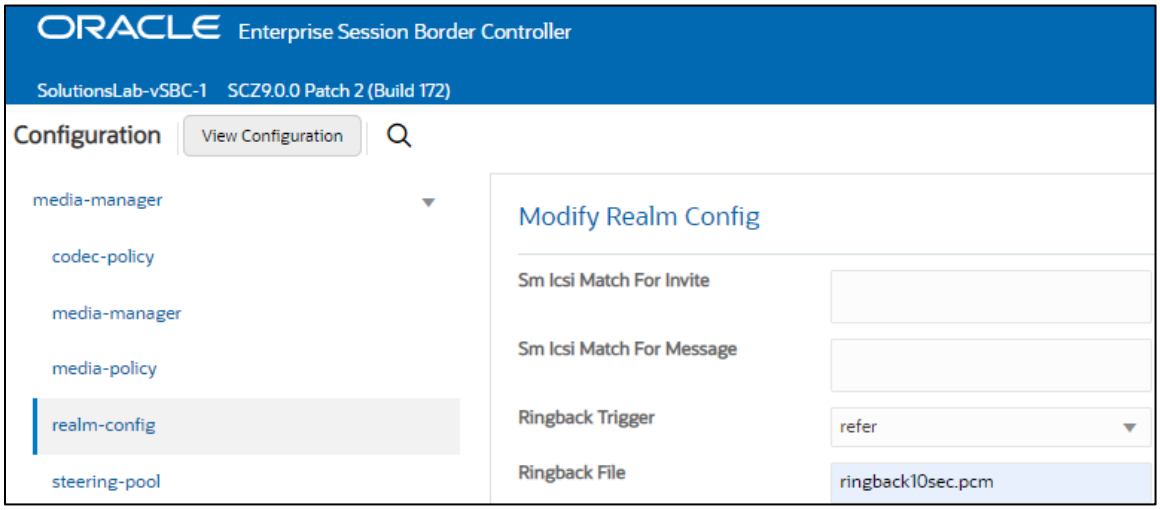



Lastly, we'll assign this file to the realm facing PSTN, and set the trigger for the SBC to generate local ringback toward PSTN:

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 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                        BaltimoreRoot
        common-name                    Baltimore CyberTrust Root
certificate-record
        name                        DigiCertRoot
        common-name                    DigiCert Global Root CA
certificate-record
        name                        TeamsCarrierCert
        state                      California
        locality                   Redwood City
        organization                  Oracle Corporation
        common-name                    customers.telechat.o-test06161977.com
        alternate-name                *.customers.telechat.o-test06161977.com
codec-policy
        name                        OptimizeCodecs
        allow-codecs                  * SILK:NO G722:NO
```

```
        add-codecs-on-egress                PCMU
codec-policy
        name                        addCN
        allow-codecs                  *
        add-codecs-on-egress                CN
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                    lrt:TeamsLRT
                realm                     SIPTrunk
                lookup                     multi
local-policy
        from-address                  *
        to-address                  sbc1.customers.telechat.o-test06161977.com
        source-realm                  SIPTrunk
        policy-attribute
                next-hop                    sag:TeamsGRP
                realm                     Teams_Cust1
                action                    replace-uri
local-policy
        from-address                  *
        to-address                  *
        source-realm                  Teams
        policy-attribute
                next-hop                    10.1.2.30
                realm                     SIPTrunk
local-routing-config
        name                        TeamsLRT
        file-name                   TeamsLRT.xml.gz
media-manager
media-profile
        name                        CN
        subname                       wideband
        payload-type                   118
        clock-rate                  16000
media-profile
        name                        SILK
        subname                       narrowband
        payload-type                   103
        clock-rate                  8000
media-profile
        name                        SILK
        subname                       wideband
        payload-type                   104
        clock-rate                  16000
media-sec-policy
        name                        RTP
media-sec-policy
        name                        TeamsSRTP
```

```
        inbound
                profile                         SDES
                mode                            srtp
                protocol                        sdes
        outbound
                profile                         SDES
                mode                            srtp
                protocol                        sdes
network-interface
        name                            s0p0
        ip-address                      141.146.36.68
        netmask                         255.255.255.192
        gateway                         141.146.36.65
        dns-ip-primary                  8.8.8.8
        dns-ip-backup1                  8.8.4.4
        dns-domain                      customers.telechat.o-test06161977.com
network-interface
        name                            s1p0
        ip-address                      10.1.2.4
        netmask                         255.255.255.0
        gateway                         10.1.2.1
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
        mm-in-realm                     enabled
        media-sec-policy                RTP
        access-control-trust-level      high
        codec-policy                    OptimizeCodecs
        ringback-trigger                refer
        ringback-file                   US_Ringback_tone.raw
realm-config
        identifier                      Teams
        description                     Carrier Tenant Facing Teams Direct Routing Interface
        network-interfaces              s0p0:0
        mm-in-realm                     enabled
        qos-enable                      enabled
        media-sec-policy                TeamsSRTP
        rtcp-mux                        enabled
        ice-profile                     ice
        teams-fqdn                      customers.telechat.o-test06161977.com
        teams-fqdn-in-uri               enabled
        sdp-inactive-only               enabled
        in-manipulationid               RespondOptions
        access-control-trust-level      high
        codec-policy                    addCN
        rtcp-policy                     rtcpGen
realm-config
```

```
        identifier                      Teams_Cust1
        description                       Realm to service Customer, woodgrovebank.us.
        network-interfaces                    s0p0:0
        mm-in-realm                        enabled
        media-sec-policy                     TeamsSRTP
        rtcp-mux                         enabled
        ice-profile                      ice
        teams-fqdn                         sbc1.customers.telechat.o-test06161977.com
        teams-fqdn-in-uri                    enabled
        sdp-inactive-only                    enabled
        access-control-trust-level             high
        codec-policy                       addCN
        rtcp-policy                      rtcpGen
rtcp-policy
        name                             rtcpGen
        rtcp-generate                      all-calls
sdes-profile
        name                             SDES
        crypto-list                      AES_CM_128_HMAC_SHA1_32
                                       AES_CM_128_HMAC_SHA1_80
        lifetime                       31
session-agent
        hostname                           10.1.2.30
        ip-address                       10.1.2.30
        realm-id                         SIPTrunk
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
```

```
session-router
    additional-lp-lookups                1
    multi-stage-src-realm-override       enabled
sip-config
    home-realm-id                        Teams
    registrar-domain                     *
    registrar-host                       *
    registrar-port                       5060
    options                              max-udp-length=0
    sip-message-len                      0
    extra-method-stats                   enabled
    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
    description                          Sip Interface facing PSTN
    sip-port
        address                          10.1.2.4
        allow-anonymous                  agents-only
sip-interface
    realm-id                             Teams
    description                          Sip Interface facing Microsoft Teams Direct Routing
    sip-port
        address                          141.146.36.68
        port                             5061
        transport-protocol               TLS
        tls-profile                      TLSTeamsCarrier
    in-manipulationid                    Checkfor183
    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                    checklineforsbcip
                    type                    c
                    action                  store
                    comparison-type         pattern-rule
                    match-value             ^(.(?!(141.146.36.68))).*$
        mime-sdp-rule
            name                    delete183SDP
            msg-type                reply
            methods                 Invite
            action                  delete
            comparison-type         boolean
            match-value             $if183.$au.$checklineforsbcip
        header-rule
            name                    change183to180
            header-name             @status-line
            action                  manipulate
            comparison-type         boolean
            match-value             $if183.$au.$checklineforsbcip
            new-value               Ringing
            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
    sip-monitoring
        match-any-filter            enabled
        monitoring-filters          *
    sip-profile
        name                        forreplaces
        replace-dialogs             enabled
    steering-pool
        ip-address                  10.1.2.4
        start-port                  10000
        end-port                    19999
        realm-id                    SIPTrunk
    steering-pool
        ip-address                  141.146.36.68
        start-port                  20000
        end-port                    29999
        realm-id                    Teams
    system-config
        hostname                    customers.telechat.o-test06161977.com
        description                 Carrier SBC for Teams Carrier Hosting Model
        location                    Burlington,MA
        system-log-level            NOTICE
        snmp-agent-mode             v1v2
```

```
tls-global
    session-caching                 enabled

tls-profile
    name                        TLSTeamsCarrier
    end-entity-certificate          TeamsCarrierCert
    trusted-ca-certificates         BaltimoreRoot
                                    DigiCertGlobalRootG2
    mutual-authenticate             enabled
```


**Oracle Corporation, World Headquarters**
500 Oracle Parkway
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**
Phone: +1.650.506.7000
Fax: +1.650.506.7200


ORACLE

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/Oracle/

twitter.com/Oracle

oracle.com

Integrated Cloud Applications & Platform Services