



# ORACLE

Oracle SBC with Microsoft Teams Operator  
Connect

**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

<b>1</b>	<b>REVISION HISTORY</b>	<b>6</b>
<b>2</b>	<b>INTENDED AUDIENCE</b>	<b>6</b>
<b>3</b>	<b>VALIDATED ORACLE SOFTWARE VERSIONS</b>	<b>6</b>
<b>4</b>	<b>RELATED DOCUMENTATION</b>	<b>6</b>
4.1	ORACLE SBC	6
4.2	MICROSOFT TEAMS	7
<b>5</b>	<b>ABOUT OPERATOR CONNECT</b>	<b>7</b>
5.1	PLANNING OPERATOR ROUTING	7
5.2	MEDIA BYPASS VS NON MEDIA BYPASS	7
<b>6</b>	<b>ORACLE SBC CONFIGURATION</b>	<b>8</b>
6.1	SYSTEM-CONFIG	8
6.1.1	NTP-Sync	9
6.2	NETWORK CONFIGURATION	10
6.2.1	Physical Interfaces	10
6.2.2	Network Interfaces	11
6.3	SECURITY CONFIGURATION	12
6.3.1	Certificate Records	12
6.3.2	TLS Profile	19
6.3.3	Media Security	20
6.4	TRANSCODING CONFIGURATION	24
6.4.1	Media Profiles	24
6.4.2	Codec Policies	25
6.4.3	RTCP Policy	28
6.5	MEDIA CONFIGURATION	29
6.5.1	Media Manager	29
6.5.2	Realm Config	30
6.5.3	Steering Pools	32
6.6	SIP CONFIGURATION	34
6.6.1	Sip-Config	34
6.6.2	Replaces Header Support	35
6.6.3	Sip Interface	37
6.6.4	Session Agents	39
6.6.5	Session Group	41
6.7	ROUTING CONFIGURATION	42
6.8	SIP ACCESS CONTROLS	46
<b>7</b>	<b>VERIFY CONNECTIVITY</b>	<b>48</b>
7.1	ORACLE SBC OPTIONS PINGS	48
<b>8</b>	<b>SYNTAX REQUIREMENTS FOR SIP INVITE AND SIP OPTIONS:</b>	<b>49</b>
8.1	TERMINOLOGY	49
8.2	REQUIREMENTS FOR INVITE MESSAGES AND FINAL RESPONSES	49
	Contact Header-Invite and Final Response	49
8.3	REQUIREMENTS FOR SIP OPTIONS	51
<b>9</b>	<b>APPENDIX A</b>	<b>51</b>

9.1	ORACLE SBC TDM WITH TEAMS .....	51
9.1.1	Interface Requirements.....	52
<b>10</b>	<b>APPENDIX B .....</b>	<b>52</b>
10.1	ORACLE SBC DEPLOYED BEHIND NAT .....	52
10.2	RING BACK ON INBOUND CALLS TO TEAMS AND EARLY MEDIA.....	54
10.3	ORACLE SBC LOCAL MEDIA PLAYBACK.....	56
10.3.1	Ring back on Transfer.....	56
<b>11</b>	<b>ACLI RUNNING CONFIGURATION.....</b>	<b>58</b>

**This Page is Intentionally left Blank**

# 1 Revision History

Document Version	Description	Revision Date
1.0	Initial release	21-03-2022
1.1	Updated Certificate-records	28-03-2023
1.2	General Amendments	02-08-2024
1.3	Updated tls-global parameter	20-08-2024
1.4	Added Root CA list and EKU considerations	30-01-2026

## 2 Intended Audience

This document describes how to connect the Oracle SBC to Microsoft Teams Operator Connect. 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:

SCZ840 or above.

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

- <https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/aclireference/acli-reference-guide.pdf>
- <https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/releasenotes/sbc-release-notes.pdf>

- <https://docs.oracle.com/en/industries/communications/session-border-controller/9.0.0/configuration/sbc-configuration-guide.pdf>

## 4.2 Microsoft Teams

<https://docs.microsoft.com/en-us/microsoftteams/operator-connect-plan>

## 5 About Operator Connect

Operator Connect is Microsoft's operator-managed service for bringing PSTN calling to Teams. Operator Connect makes it simple to bring your operator to Teams. With Operator Connect, if your existing carrier is a participant in the Microsoft Operator Connect program, they can manage PSTN calling and Session Border Controllers (SBCs). With Operator Connect, if your existing operator is a participant in the Microsoft Operator Connect Program, they can manage the service for bringing PSTN calling to Teams. The Operator Connect program provides the following benefits:

- **Leverage existing contracts or find a new operator.** You keep your preferred operator and contracts or choose a new one from a selection of participating operators to meet your business needs.
- **Operator-managed infrastructure.** Your operator manages the PSTN calling services and Session Border Controllers (SBCs), allowing you to save on hardware purchase and management.
- **Faster, easier deployment.** You can quickly connect to your operator and assign phone numbers to users — all from the Teams admin center.
- **Enhanced support and reliability.** Operators provide technical support and shared service level agreements to improve support service, while direct peering powered by Azure creates a one-to-one network connection for enhanced reliability.

For a list of operators participating in the Microsoft Operator Connect Program and the countries or regions where their service is available, see the Microsoft 365 Operator Connect directory.

### 5.1 Planning Operator Routing

To enable phone number assignments with Operator Connect, make sure your users are:

- Teams Phone licensed.
- In TeamsOnly mode. Note that the user needs to be in TeamsOnly mode, but your entire organization does not.

### 5.2 Media Bypass vs Non Media Bypass

**Note:** Microsoft Operator Connect does not work in media bypass mode.

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 Advanced Media Termination

[ICE lite](#) on the Oracle SBC. These protocols enable Operator Connect to use the most direct media path for optimal quality.

## 6 Oracle SBC Configuration

This chapter provides step-by-step guidance on how to configure Oracle SBC for interworking with Microsoft Operator Connect.

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

For the purposes of this note, we'll be providing both OCSBC GUI the CLI for all configuration examples. We will also provide complete CLI running-configuration at the end of the Application Note.

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](#).

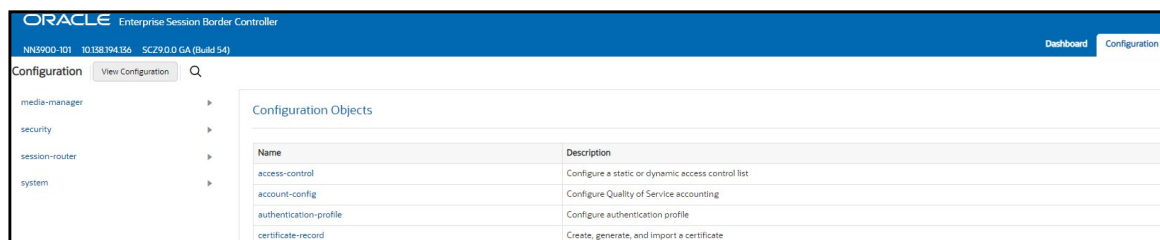
To access the OCSBC GUI, enter the management IP address into a web browser. When the login screen appears, enter the username and password to access the OCSBC.

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 Operator Connect to function properly.*

*Please Note there is no GUI on Oracle Service provider SBC.*

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



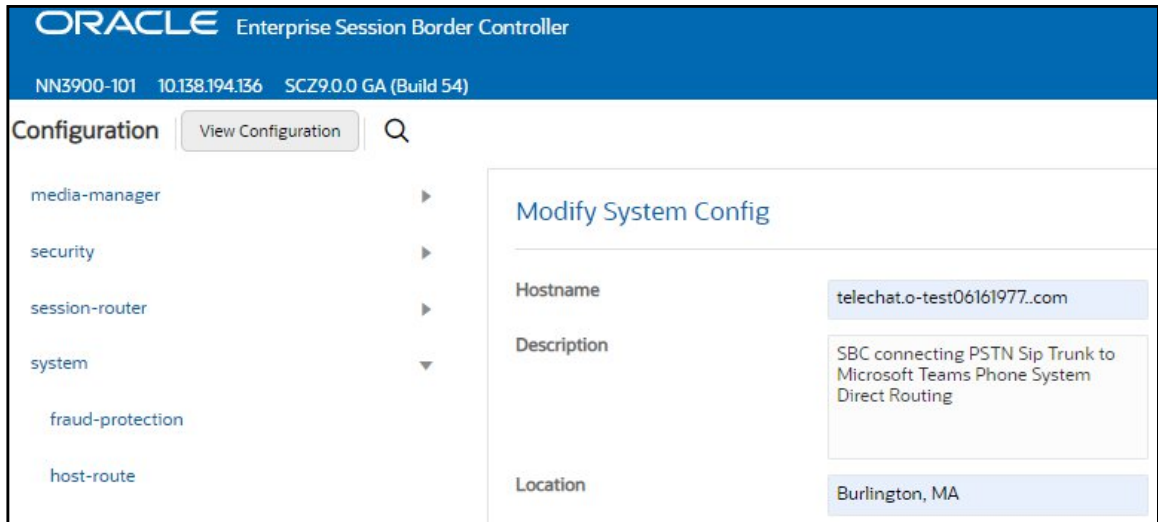
### 6.1 System-Config

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

- GUI Path: system/system-config

*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.

To configure system-config from ACLI –

ACLI Path: config tãsystemãsystem-config

```

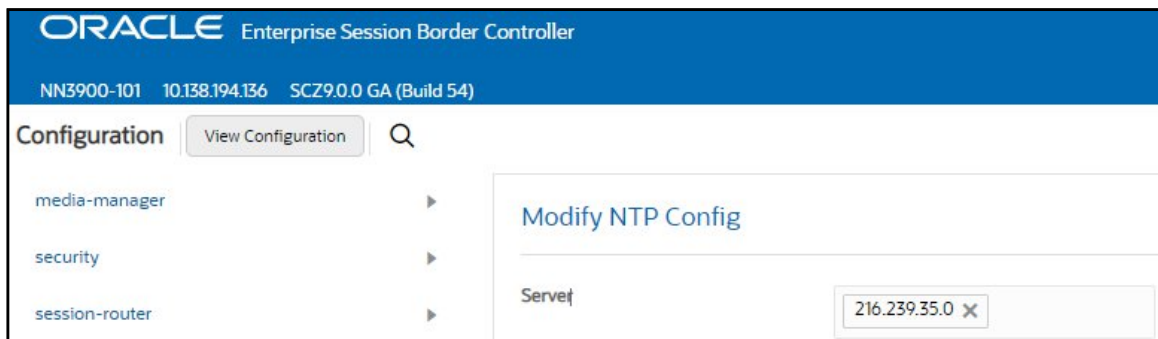
system-config
  hostname          oraclesbc.com
  description       SBC connecting PSTN Sip Trunk to Microsoft Operator
Connect
  location          Burlington, MA
  transcoding-cores 1
  
```

- Perform a save and activate configuration for changes to take effect.

### 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



- Select OK at the bottom

To configure ntp-config from ACLI –

ACLI Path: config tãsystemãntp-sync

```
ntp-config
server                216.239.35.0
```

- Perform a save and activate configuration for changes to take effect.

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 Operator Connect, the other to connect to PSTN Network. The slots and ports used in this example may be different from your network setup.

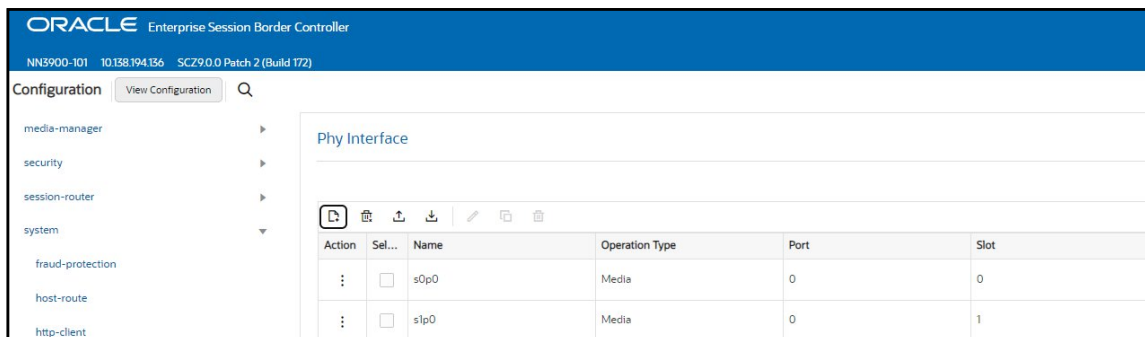
### 6.2.1 Physical Interfaces

GUI Path: system/phy-interface

- 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*



To configure phy-interface from ACLI –

ACLI Path: config tãsystemãphy-interface

```

phy-interface
  name          s0p0
  operation-type Media
phy-interface
  name          s1p0
  operation-type Media
  slot

```

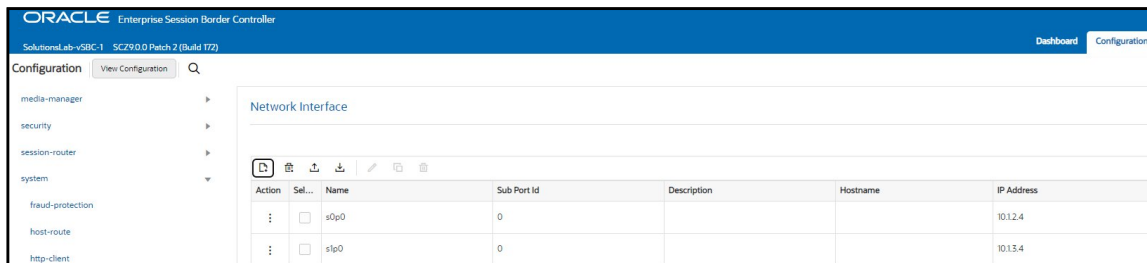
- Perform a save and activate configuration for changes to take effect.

## 6.2.2 Network Interfaces

GUI Path: system/network-interface

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

Configuration Parameter	Teams	PSTN
Name	s1p0	s0p0
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.

To configure network-interface from ACLI –

ACL Path: config → system → network-interface

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
dns-ip-primary	8.8.8.8
dns-ip-backup1	8.8.4.4
dns-ip-backup2	9.9.9.9
dns-domain	telechat.o-test06161977.com

- Perform a save and activate configuration for changes to take effect.

Next, we'll configure the necessary elements to secure signaling and media traffic between the Oracle SBC and Microsoft Teams Operator Connect.

### 6.3 Security Configuration

This section describes how to configure the SBC for both TLS and SRTP communication with Microsoft Operator Connect.

**Note:** Operator Connect Trunk can also use TCP/RTP Protocol. Use of MAPS (Microsoft Azure Peering Service) Transport is a MUST for Network to Network Connection between the Oracle SBC and Operator Connect. Traffic sent through 3<sup>rd</sup> Part Internet is not supported. For the purpose of the Application Note we have provided TLS/SRTP method of connectivity between Oracle SBC and Microsoft Operator Connect.

When Using TLS/SRTP Microsoft Operator Connect recommends 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](#). These are same as Direct Routing Supported CAs.

#### 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

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

- SBC Certificate (end-entity certificate)
- DigiCert RootCA 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 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.*

### 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/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**.

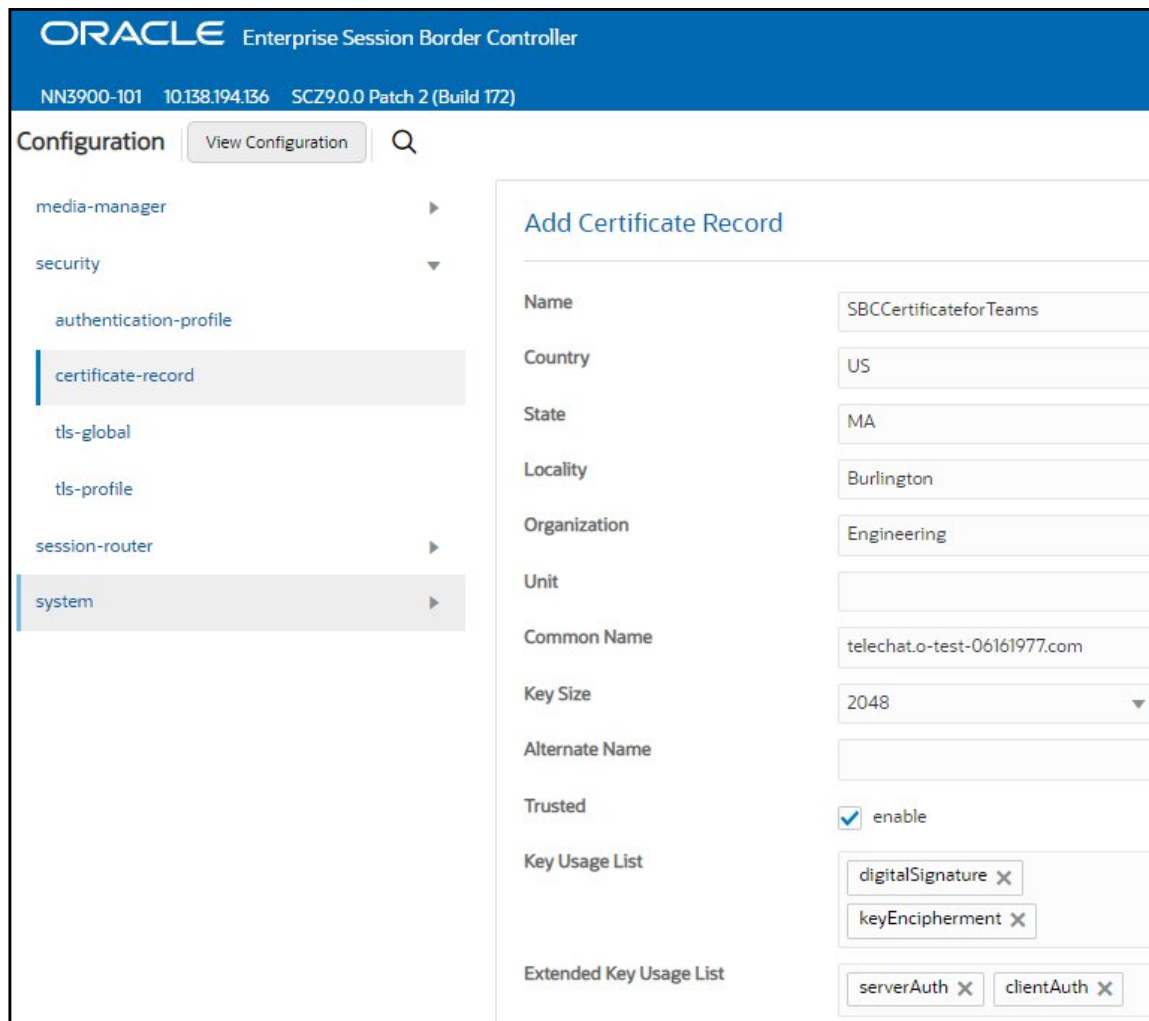
For now, mutual TLS connections between your Oracle SBC and Microsoft Teams will continue to be established, even if the root CA removes or no longer supports the clientAuth EKU. Looking ahead, including the clientAuth EKU in your SBC's end entity certificate will be important to maintain compatibility 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



- Click OK at the bottom

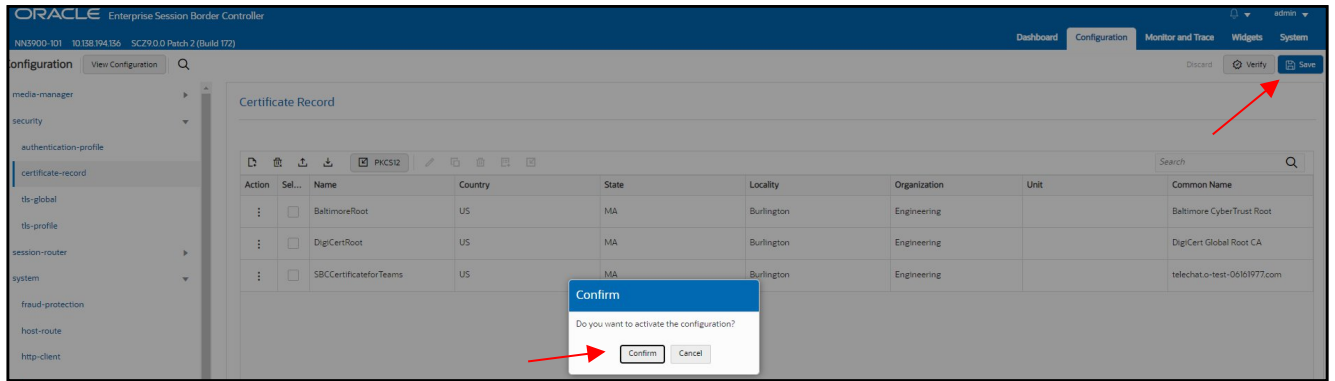
To configure certificate-record from ACLI –

ACLI Path: config tasecurityàcertificate-record

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

- Perform a save and activate configuration for changes to take effect.

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.

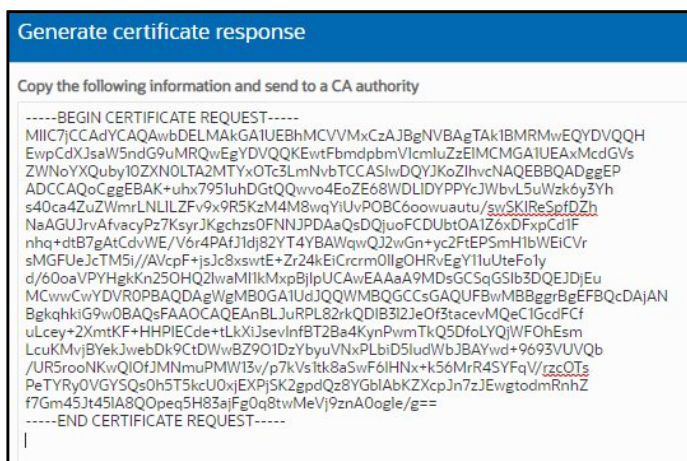
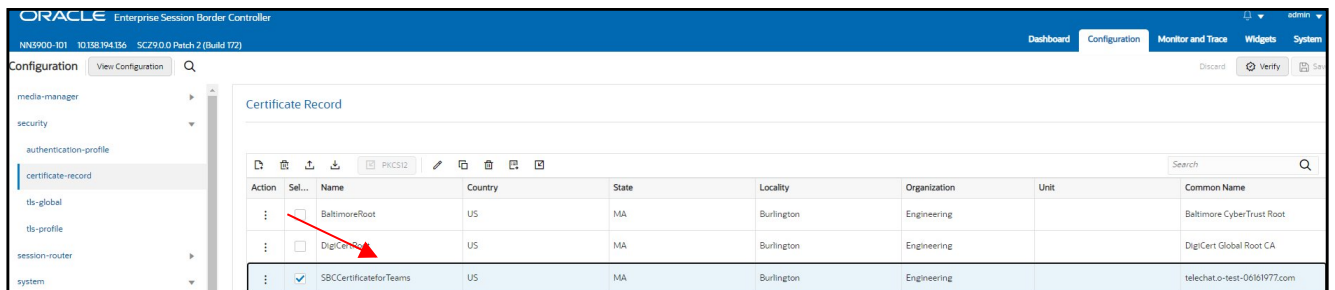


### 6.3.1.2 Generate Certificate Signing Request

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:



Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.

To perform the Steps From ACLI use the below command –

generate-certificate-request SBCCertificateforTeams

This Step generates a text on Screen as shown below –

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC4zCCAcsCAQAwazELMAkGA1UEBhMCMCVVMxCzAJBgNVBAGTAK1BMRMwEQYDVQQQ
H
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEkMCIGA1UEAxMbdGVs
ZWNoYXQuYy10ZXN0MDYxNjE5NzcuY29tMIIlBjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAR3AmjF15PclCWiB/kFEuUGNHQHlBkji28MDbcprO/KLXIHQysSnw
UWz34XLBfLQ6rS4MLyEMR8Nt8GGNSIWkIR431LsX7L+yGWvRjCBFP6DIHtH0Vuqm
ixVaUJpg5luPY6SvT1shyu26iLlBsLfem43tbKq5jz/jrvaUzyhICvAQ23c1oS5a
D4UiF2mNOuSqxvmkx50a3/BNybKecLNOxvKQyyTMgffNpASbZuW+eMEUKI5iB+AB
/AAoZRP4bn4qlE3wn8pJsNm8Pjxy4hbz24ySgmaN9iXpP1FdRw0TemfCsNazZRuK
DsviWJfunZYTzRfDe5pJToMH4u1zt2fK1QIDAQABoDMwMQYJKoZlHvcNAQKOMSQw
IjALBgNVHQ8EBAMCBaAwEwYDVR0IBAwWCgYIKwYBBQUHAWEdDQYJKoZlHvcNAQEL
BQADggEBADD5Y+u08LxmTMIJ2RjC8cgPZocTqBDXN0tp27S4FuB/01ikBBdG3YV
Ffp7/Q8ZeFHHgU/rMzeF8Gpo9Cc6JUGGux3/ws8ZkgRBxsNIG276i7pFN1vCijEP
89AGxtryioRMc4kcdPpLJNQ10Qx1zKobHMTftGLDI6jN2pvn3zYHH8qA9V/1/yKa
3n0j33EuTrvTIQ5P4lgyVJqSBkdI29T1gXY6O8JVFLCQefTrF4TLc6teNzxXMdPw
PHoPu9hM3scGOWOHQnODXOFeq2AxBQzAa0/Cjf7Bw3I3POmMclOawgDecZ8UjHpJ
lznX9/Gxg5X+S2QkHjNmPK+JuePqX4I=
-----END CERTIFICATE REQUEST-----
```

Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature.

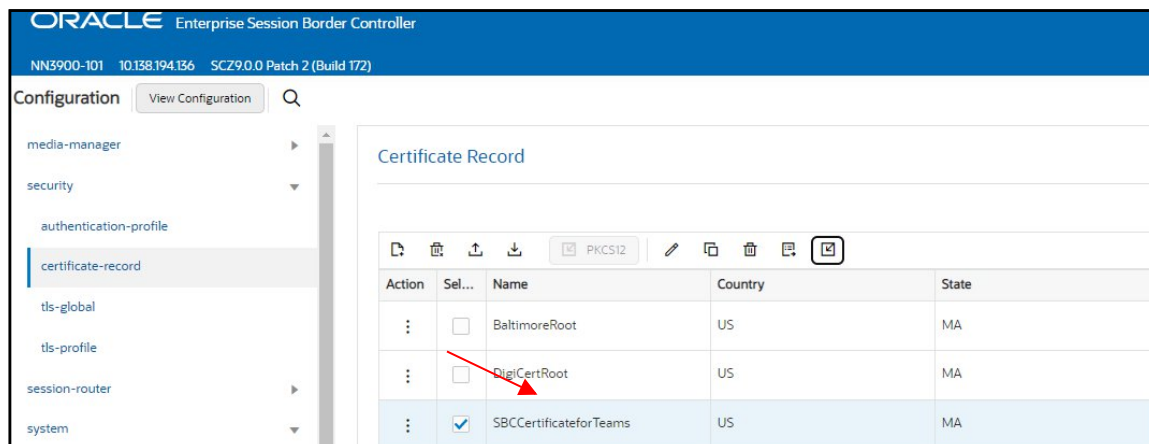
Also note, at this point, **another save and activate is required** before you can import the certificates to each certificate record created above.

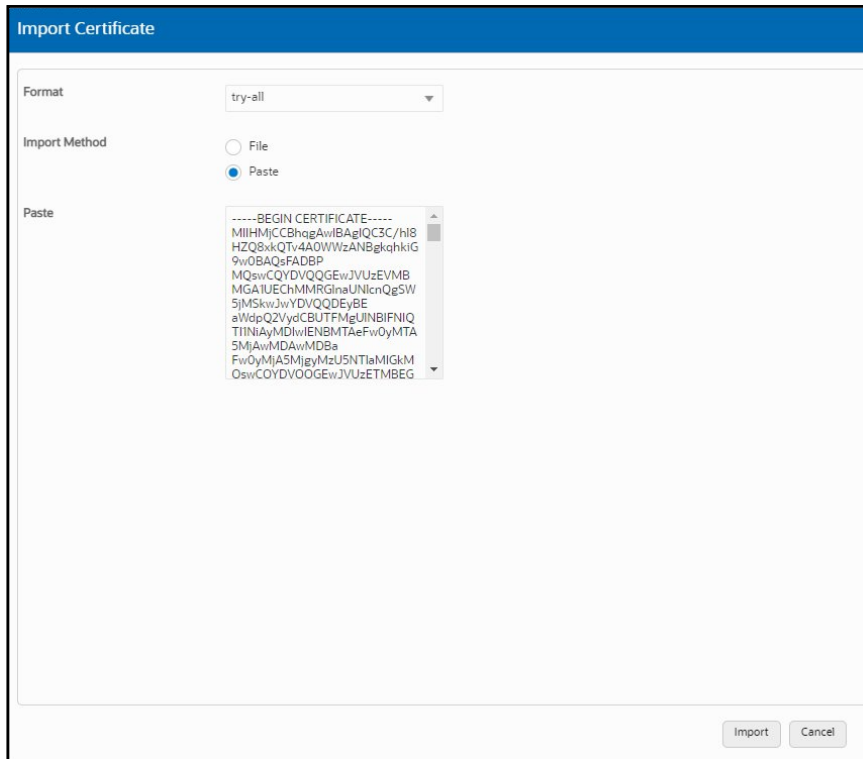
### 6.3.1.3 Import Certificates to SBC

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.

To import the certificate from ACLI follow below procedure -

```
import-certificate try-all SBCCertificateforTeams
```

The System will show a prompt as below -

**IMPORTANT:**

Please enter the certificate in the PEM format.  
 Terminate the certificate with ";" to exit.....

Enter the Signed Certificate text as shown below-

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC4zCCAcsCAQAwazELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAK1BMRMwEQYDVQQH
EwpCdXJsaW5ndG9uMRQwEgYDVQQKEwtFbmdpbmVlcmluZzEkMCIGA1UEAxMbdGVs
ZWNoYXQuby10ZXN0MDYxNjE5NzcuY29tMIIBljANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBKgKCAQEAr3AmjF15PclCWiB/kFEExUGNHQHlBkji28MDbcprO/KLXIHQysSnw
UWz34XLBfLQ6rS4MLyEMR8Nt8GGNSIWkiR431LsX7L+yGWvRjcBFP6DIHtH0Vuqm
ixVaUJpg5luPY6SvT1shyu26iLIBsLfem43tbKq5jz/jrvaUzyhCvAQ23c1oS5a
D4UiF2mNOuSqxvmkx50a3/BNybKecLNOxvKQyyTMgffNpASbZuW+eMEUKI5iB+AB
/AAoZRP4bn4qIE3wn8pJsNm8Pjxy4hbz24ySgmaN9iXpP1FdRw0TemfCsNazZRuK
DsviWJfunZYTzRfDe5pJTToMH4u1zt2fK1QIDAQABoDMwMQYJKoZIHvcNAQkOMSQw
IjALBgNVHQ8EBAMCBaAwEwYDVR0IBAwWCGYIKwYBBQUHAWewDQYJKoZIhvcNAQEL
BQADggEBADD5Y+u08LxmTMIslJ2RjC8cgPZocTqBDXN0tp27S4FuB/01ikBBdG3YV
Ffp7/Q8ZeFHHgU/rMzeF8Gpo9Cc6JUGGux3/ws8ZkgRBxsNIG276i7pFN1vCijEP
89AGxtryioRMc4kcdPpLJNQ10Qx1zKobHMTftGLDI6jN2pvn3zYHH8qA9V/1/yKa
3n0j33EuTrvTIQ5P4IgyVJqSBkd129T1gXY6O8JVFLCQefTrF4TLc6teNzxXMdPw
PHoPu9hM3scGOWOHQnODXOFeq2AxBQzAa0/Cjf7Bw3I3POmMclOawgDecZ8UjHpJ
IznX9/Gxg5X+S2QkHjNmPK+JuePqX4I=
-----END CERTIFICATE REQUEST-----;

```

**save and activate** your configuration.

### 6.3.1.4 Root CA and Intermediate Certificates

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	<a href="#">DigiCert Global Root CA</a>
DigiCert Global Root G2	<a href="#">DigiCert Global Root G2</a>
DigiCert Global Root G3	<a href="#">DigiCert Global Root G3</a>
DigiCert TLS ECC P384 Root G5	<a href="#">DigiCert TLS ECC P384 Root G5</a>
DigiCert TLS RSA 4096 Root G5	<a href="#">DigiCert TLS RSA 4096 Root G5</a>
Microsoft ECC Root Certificate Authority 2017	<a href="#">Microsoft ECC Root Certificate Authority 2017</a>
Microsoft RSA Root Certificate Authority 2017	<a href="#">Microsoft RSA Root Certificate Authority 2017</a>

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.

Configuration View Configuration [icon] [search]

media-manager > Certificate Record

security >

authentication-profile >

**certificate-record**

global-trusted-ca >

tls-global >

tls-profile >

session-router >

system >

[icon] [icon] [icon] [icon] PKCS12 [icon] [icon] [icon] [icon] [icon] Delete all Certificate Record items

Action	Name ^	Country ◊	State ◊	Locality ◊
<input type="checkbox"/>	DigiCertGlobalRootG2	US	MA	Burlington
<input type="checkbox"/>	DigiCertGlobalRootG3	US	MA	Burlington
<input type="checkbox"/>	DigiCertRoot	US	MA	Burlington
<input type="checkbox"/>	DigiCertTLSECCP384RootG5	US	MA	Burlington
<input type="checkbox"/>	DigiCertTLSECCP4096RootG5	US	MA	Burlington
<input type="checkbox"/>	GoDaddyRoot	US	MA	Burlington
<input type="checkbox"/>	GoDaddyinter	US	MA	Burlington
<input type="checkbox"/>	MicrosoftECCRootCertificateAuth...	US	MA	Burlington
<input type="checkbox"/>	MicrosoftRSARootCertificateAuth...	US	MA	Burlington
<input type="checkbox"/>	Telechat2025	US	Texas	Austin

Repeat the Steps mentioned in Section 6.3.1.3 to import all the Root CA Certificates to the SBC including the Root CA certificate that signed the SBC's TLS certificate.

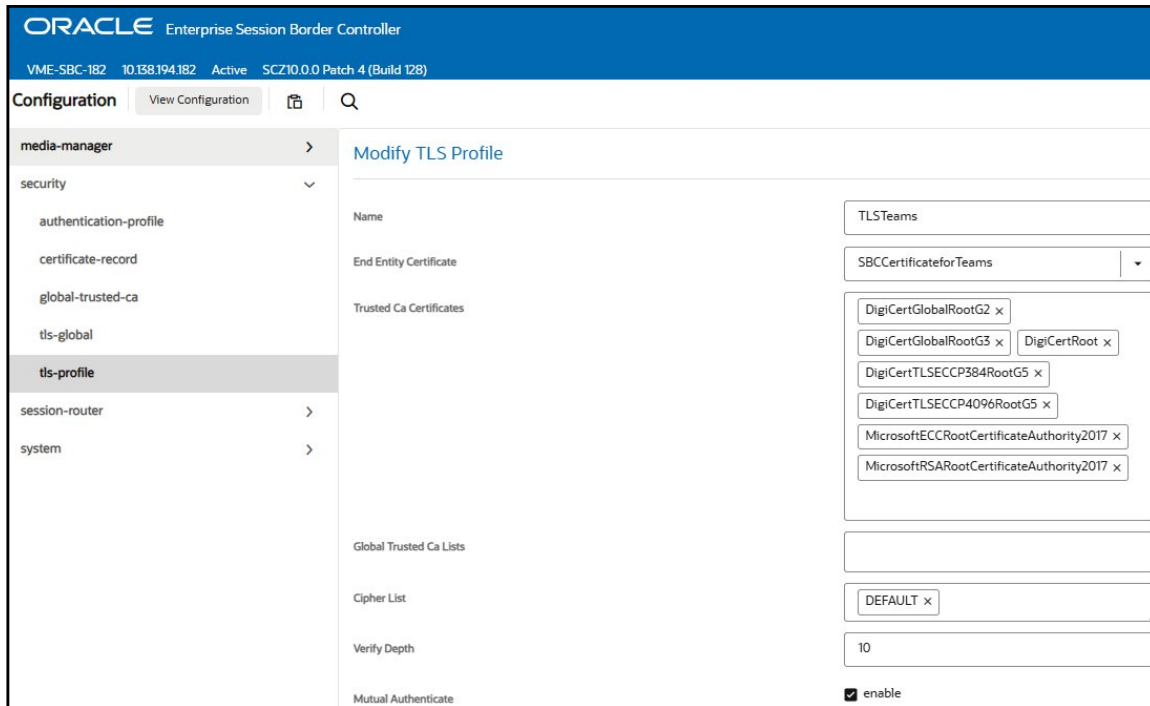
Please note – all certificates including root and intermediate certificates are required to be imported to the SBC. Once all certificates have been imported, issue a third **save/activate** from the WebGUI to complete the configuration of certificates on the Oracle SBC.

### 6.3.2 TLS Profile

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

GUI Path: security/tls-profile

- Click Add, use the example below to configure



- Select OK at the bottom

To configure tls-profile from ACLI –

ACLI Path: config tasecurityàtls-profile

```

tls-profile
  name TLSTeams
  end-entity-certificate SBCCertificateforTeams
  trusted-ca-certificates
    DigiCertRoot
    DigiCertGlobalRootG2
    DigiCertGlobalRootG3
    DigiCertTLSECCP384RootG5
    DigiCertTLSECCP4096RootG5
    MicrosoftECCRootCertificateAuthority2017
    MicrosoftRSARootCertificateAuthority2017
  mutual-authenticate enabled
  tls-version tlv12
  
```

- Perform a save and activate configuration for

changes to take effect.

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

### 6.3.3 Media Security

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

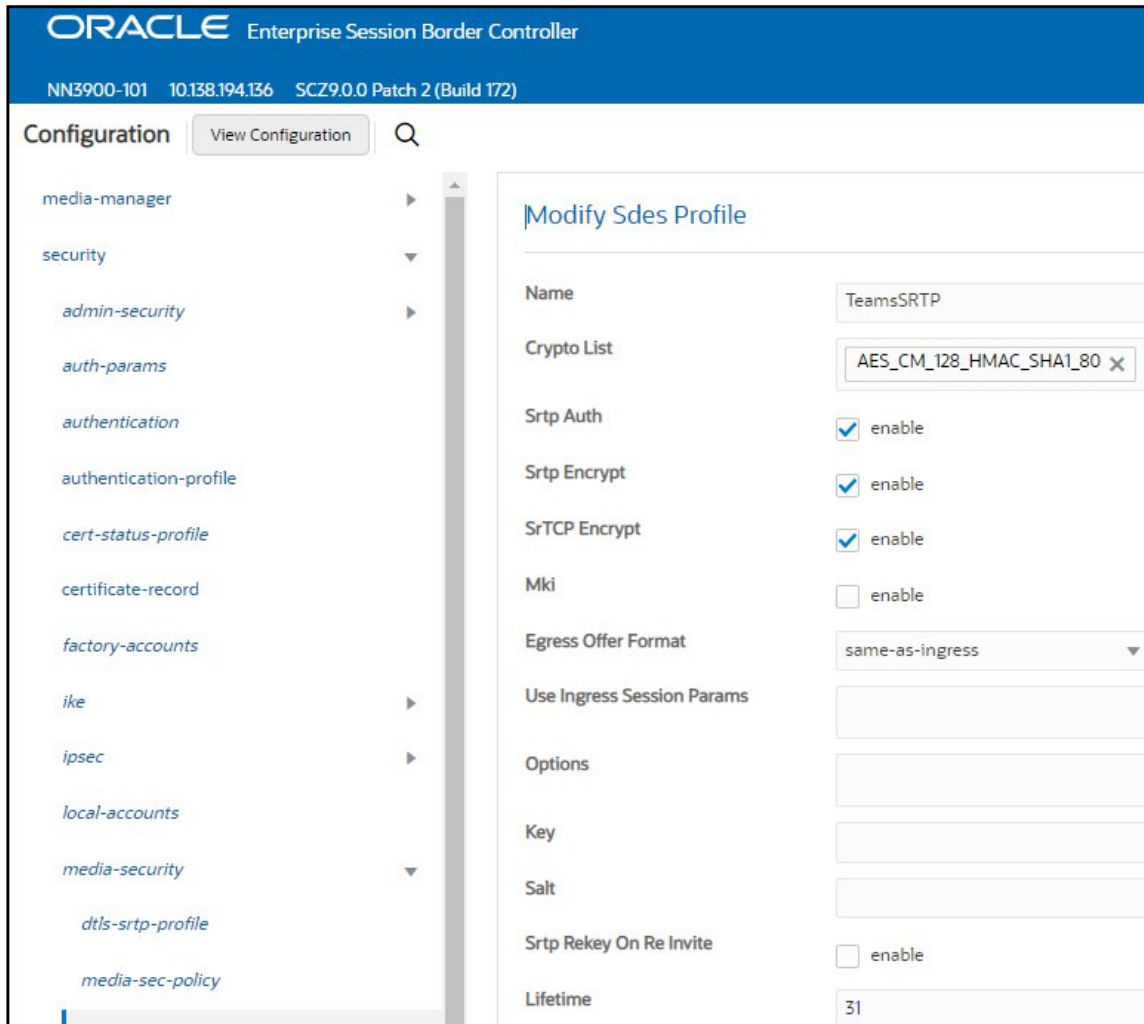
#### 6.3.3.1 SDES-Profile

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

- Click Add, and use the example below to configure



- Select OK at the bottom

To configure sdes-profile from ACLI –

ACLI Path: config tasecurityamedia-securityàsdes-profile

```

sdes-profile
  name          TeamsSRTP
  crypto-list    AES_CM_128_HMAC_SHA1_80
  srtp-auth      enabled
  srtp-encrypt   enabled
  srtcp-encrypt  enabled
  mki            disabled
  egress-offer-format  same-as-ingress
  use-ingress-session-params
  options
  key
  salt
  srtp-rekey-on-re-invite  disabled
  lifetime      31

```

- Perform a save and activate

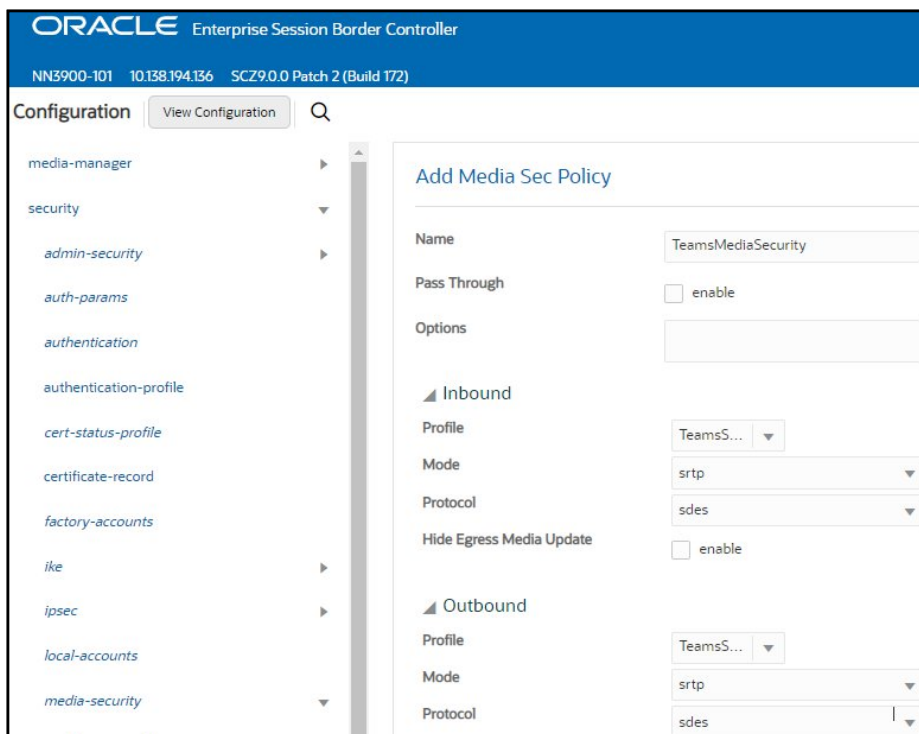
configuration for changes to take effect.

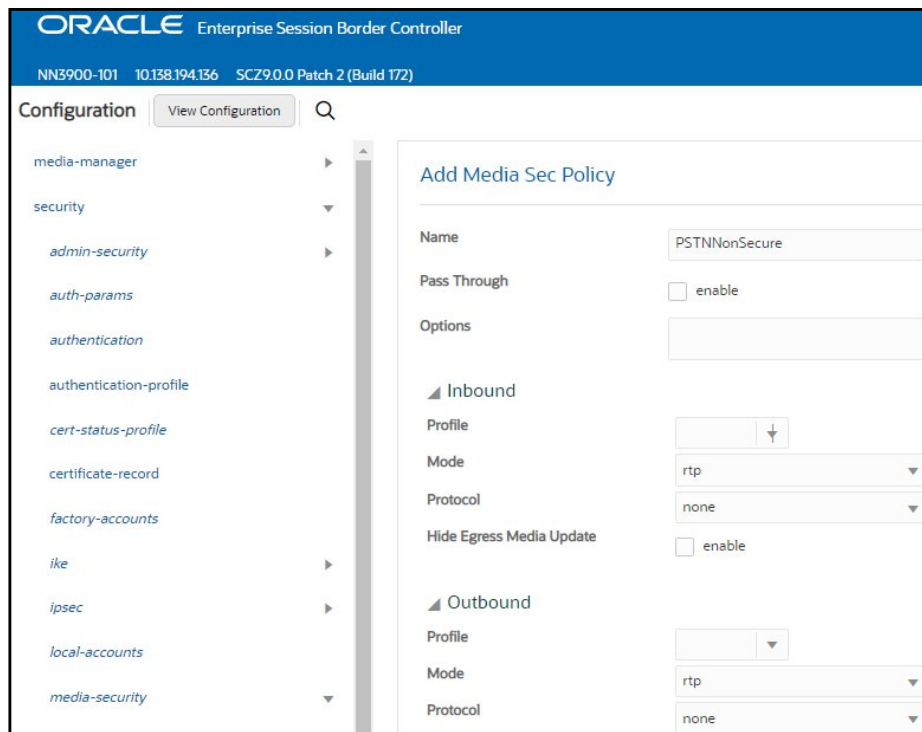
### 6.3.3.2 Media Security Policy

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  
Click Add, use the examples below to configure





- Select OK at the bottom of each when finished

To configure media security from ACLI.

ACLI Path: `config tasecurityamedia-securityamedia-sec-policy`

```

media-sec-policy
  name PSTNNonSecure
  pass-through disabled
  options
  inbound
    profile
    mode rtp
    protocol none
    hide-egress-media-update disabled
  outbound
    profile
    mode rtp
    protocol none
media-sec-policy
  name TeamsMediaSecurity
  pass-through disabled
  options
  inbound
    profile TeamsSRTP
    mode srtp
    protocol sdes
    hide-egress-media-update disabled
  outbound
    profile TeamsSRTP
    mode srtp
    protocol sdes

```

- Perform a save and activate configuration for changes to take effect.

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 Operator Connect.

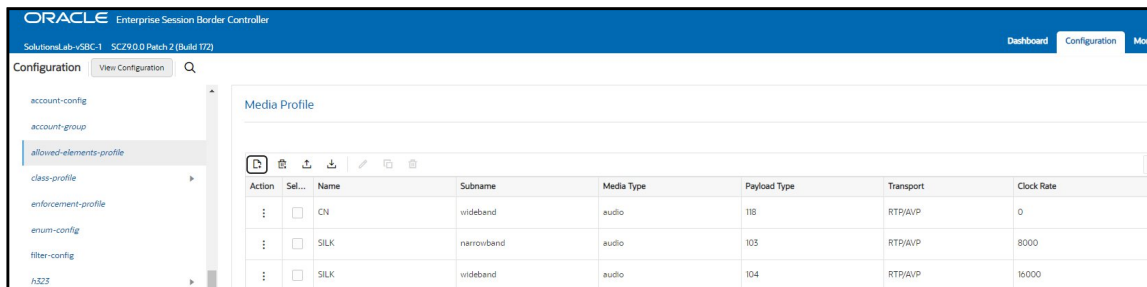
GUI Path: session-router/media-profile

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
Surname	narrowband	wideband	wideband
Payload-Type	103	104	118
Clock-rate	8000	16000	0



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

To configure media-profile from ACLI –

ACLI Path: config t session-router media-profile

```
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
```

- Perform a save and activate configuration for changes to take effect.

### 6.4.2 Codec Policies

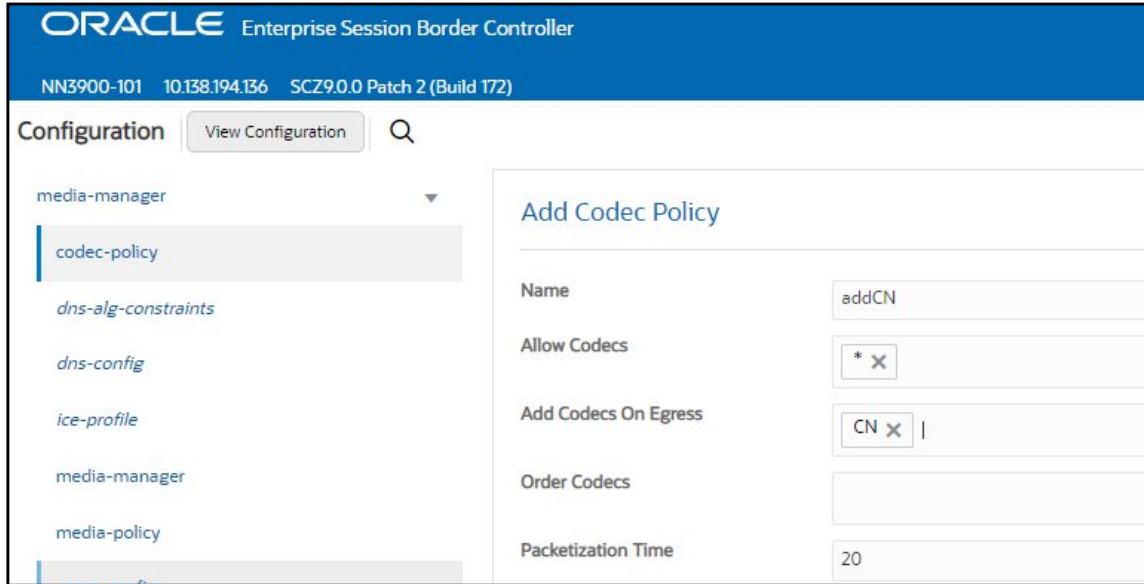
Codec policies are sets of rules that specify the manipulations to be performed on SDP offers allowing the Oracle SBC the ability to add, strip, and reorder codecs for SIP sessions.

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

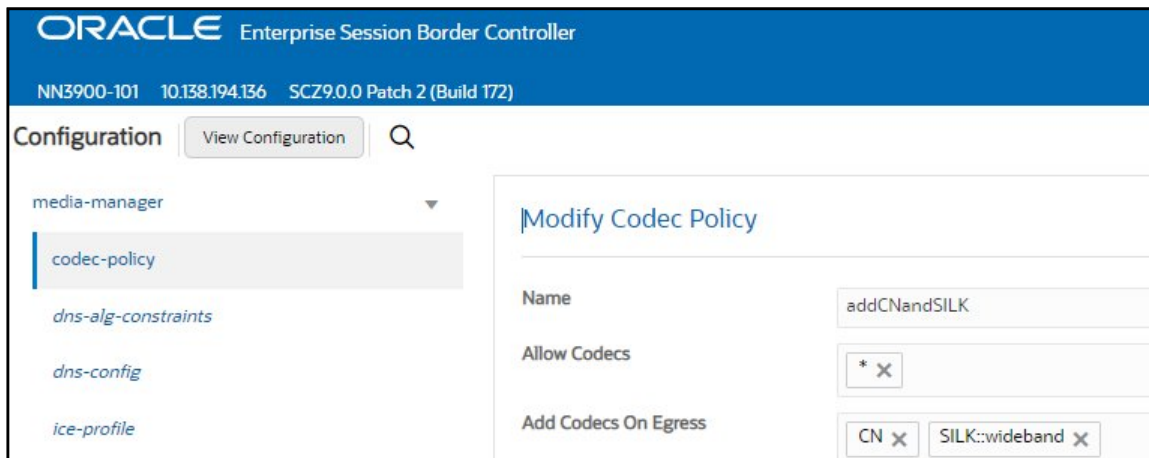
support either. To satisfy this requirement, the SBC uses transcoding resources to generate those packets, which does require a codec policy be configured and assigned.

GUI Path: media-manager/codec-policy

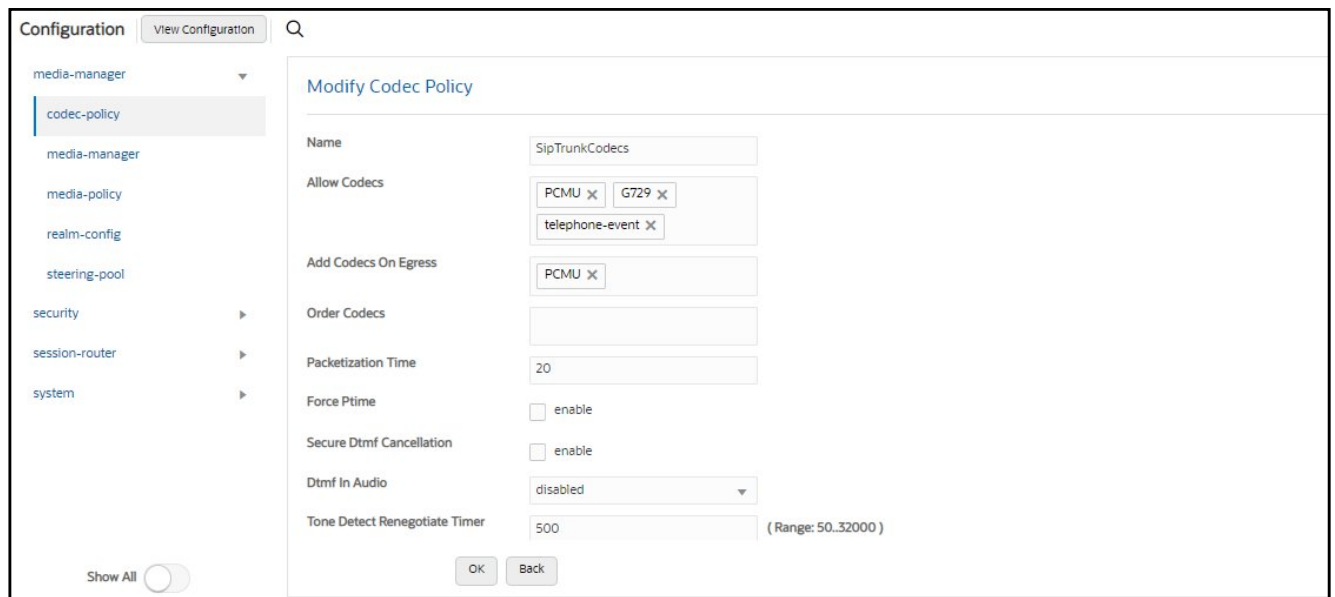
Here is an example config of a codec policy used for the SBC to generate CN packets towards Teams.



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 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

To configure codec-policy from ACLI –

ACLI Path: config tamedia-manageràcodec-policy

```

codec-policy
  name                SipTrunkCodecs
  allow-codecs        PCMU G729 telephone-event
  add-codecs-on-egress PCMU
codec-policy
  name                addCNandSilk
  allow-codecs        *
  add-codecs-on-egress CN SILK::wideband

```

- Perform a save and activate configuration for changes to take effect.

**Caveat** – On SCZ8.x release if both SILK WB and CN:wideband are configured as a media profile in the configuration you will not be able to add CN in add-codecs-on-egress parameter on the codec-policy.

```

media-profile
  name                CN
  subname             wideband
  payload-type        118
  clock-rate          16000

```

```

media-profile
  name                SILK
  subname             wideband
  payload-type        104
  clock-rate          16000

```

```

(codec-policy)# add-codecs-on-egress CN
% Invalid Input

```

Item "CN" invalid value  
Added codec must be transcodable

**As a workaround please follow below steps –**

- 1) Remove the CN media-profile
- 2) Then add the required codec-policy.
- 3) Save the configuration
- 4) Add the CN media-profile back
- 5) Save the configuration
- 6) Activate the config.

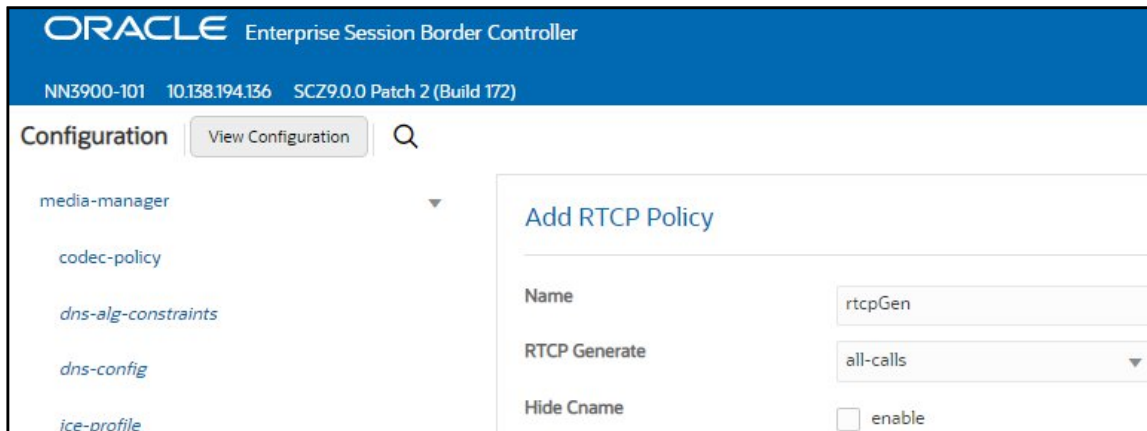
The issue is resolved in SCZ9.x stream of Oracle SBC release.

### 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

- 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

To configure rtcp-policy from CLI –

CLI Path: config tamedia-mangeràrtcp-policy

```
rtcp-policy
name          rtcpGen
rtcp-generate all-calls
hide-cname    disabled
```

- Perform a save and

activate configuration for changes to take effect.

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.

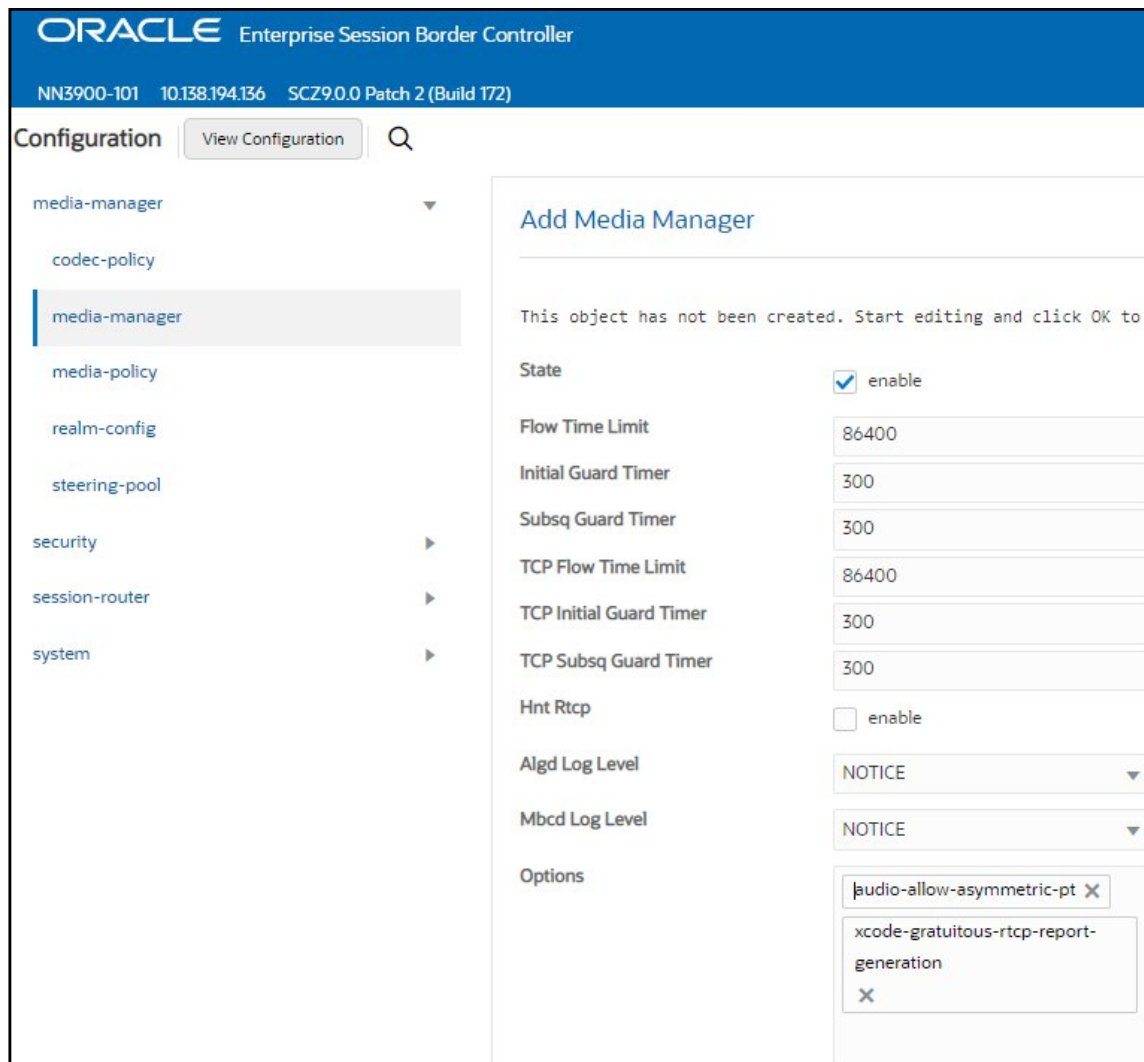
### 6.5.1 Media Manager

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

GUI Path: media-manager/media-manager

The following two hidden options are recommended for the global media manager when interfacing with Microsoft Teams Operator Connect.

- **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

To configure media-manager from ACLI –

ACLI Path: config tamedia-manageramedia-manager-config

```
media-manager
state          enabled
options       audio-allow-asymmetric-pt
              xcode-gratuitous-rtcp-report-generation
```

- Perform a save and activate configuration for changes to take effect.

## 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.

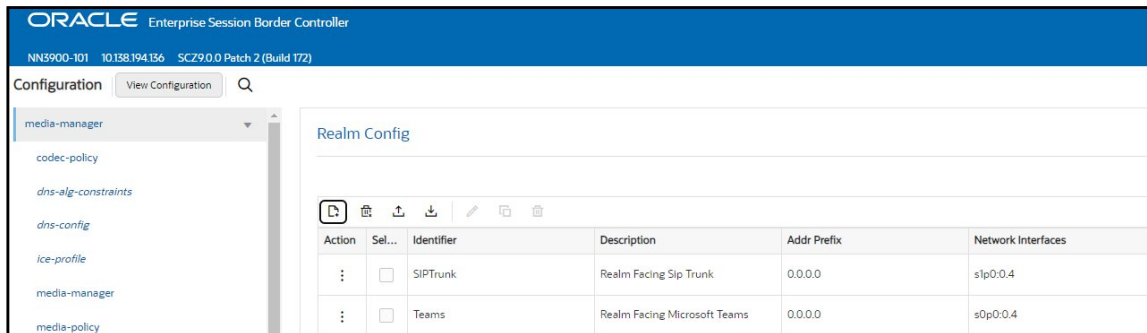
GUI Path; media-manger/realm-config

- 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"/>	
Codec policy	addCN	SipTrunkCodecs
RTCP policy	rtcpGen	
Access-control-trust-level	HIGH	HIGH

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

- Network Interface
- Media Security Policy
- Codec Policy (optional on the PSTN Realm)
- RTCP Policy



- Select OK at the bottom of each

To configure realm-config from ACLI –

ACLI Path - config tamedia-mangerrealm-config

realm-config	
identifier	SipTrunk
description	Realm facing PSTN
network-interfaces	s0p0:0.4
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	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
access-control-trust-level	high
codec-policy	addCN
rtcp-policy	rtcpGen

- Perform a save and activate configuration for changes to take effect.

### 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

- Click Add, and use the below examples to configure

The screenshot shows the 'Modify Steering Pool' configuration page. The left sidebar lists configuration categories: media-manager, codec-policy, media-manager, media-policy, realm-config, steering-pool (selected), security, session-router, and system. The main form fields are: IP Address (10.1.2.4), Start Port (20001, Range: 0,1..65535), End Port (40000, Range: 0,1..65535), Realm ID (SipTrunk), and Network Interface (empty dropdown).

The screenshot shows the 'Modify Steering Pool' configuration page with updated values. The left sidebar is the same as the previous screenshot. The main form fields are: IP Address (10.1.4.4), Start Port (10000, Range: 0,1..65535), End Port (20000, Range: 0,1..65535), Realm ID (Teams), and Network Interface (empty dropdown).

- Select OK at the bottom

To configure steering pool from ACLI

ACLI Path: config tãmedia-mangerãsteering-pool

```
steering-pool
  ip-address      10.1.2.4
  start-port     20001
  end-port       40000
  realm-id       SipTrunk

steering-pool
  ip-address      10.1.4.4
  start-port     10000
  end-port       20000
  realm-id       Teams
```

- Perform a save and activate configuration for changes to take effect.

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.

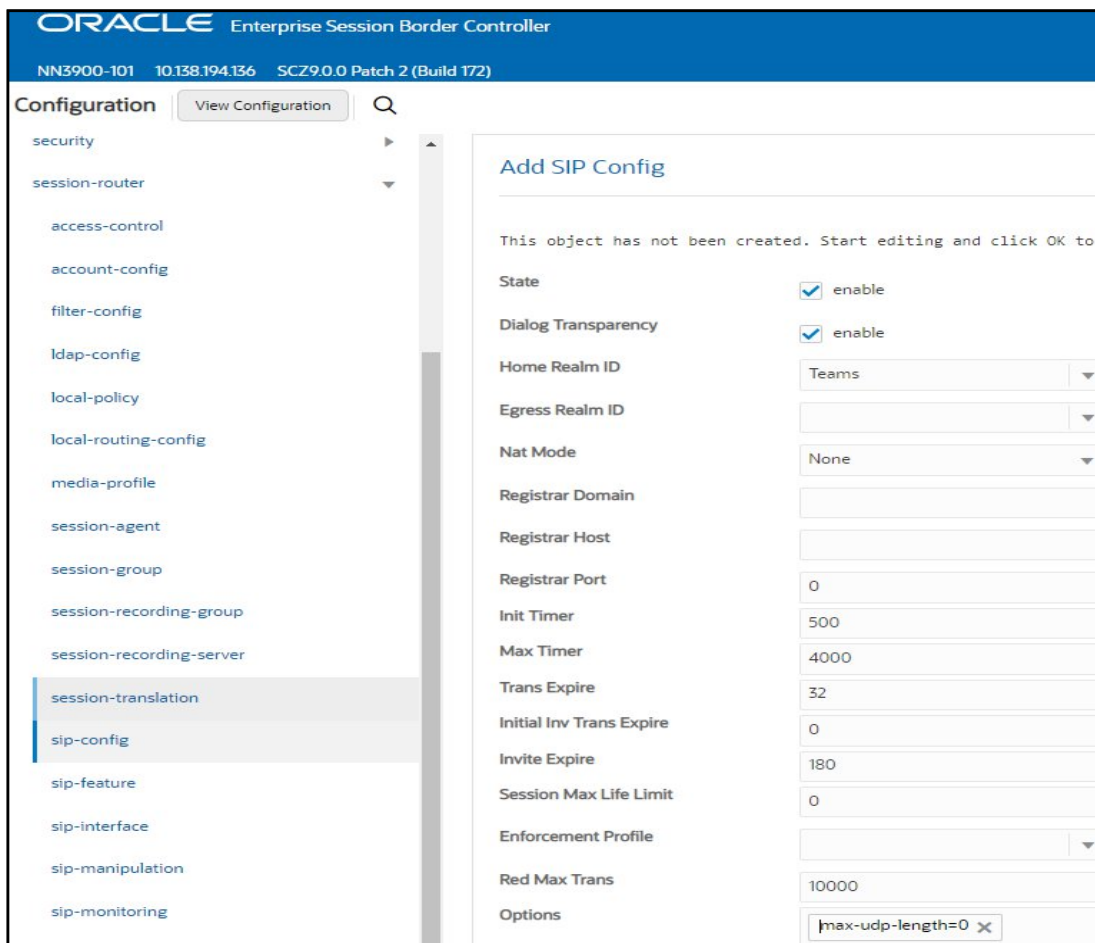
### 6.6.1 Sip-Config

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

GUI Path: session-router/sip-config

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 sip 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

To configure sip config from ACLI.

ACL Path: config t session-router sip-config

```
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
```

- Perform a save and activate configuration for changes to take effect.

## 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 should not send Replaces to Microsoft.

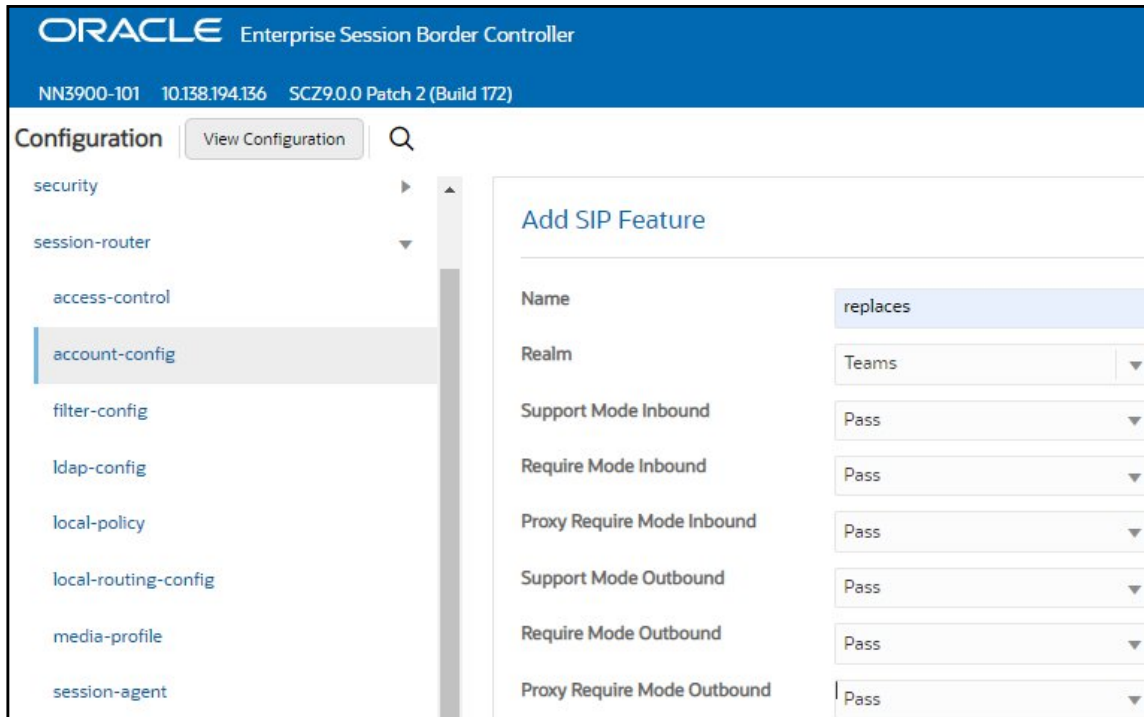
To configure support for Replaces, we configure the following:

### 6.6.2.1 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

Click add and use the following to configure:



- Click OK at the bottom

To configure sip feature from ACLI

ALCI Path: config t session-router sip-feature

sip-feature		
name	replaces	
realm	Teams	
require-mode-inbound	Pass	
require-mode-outbound	Pass	

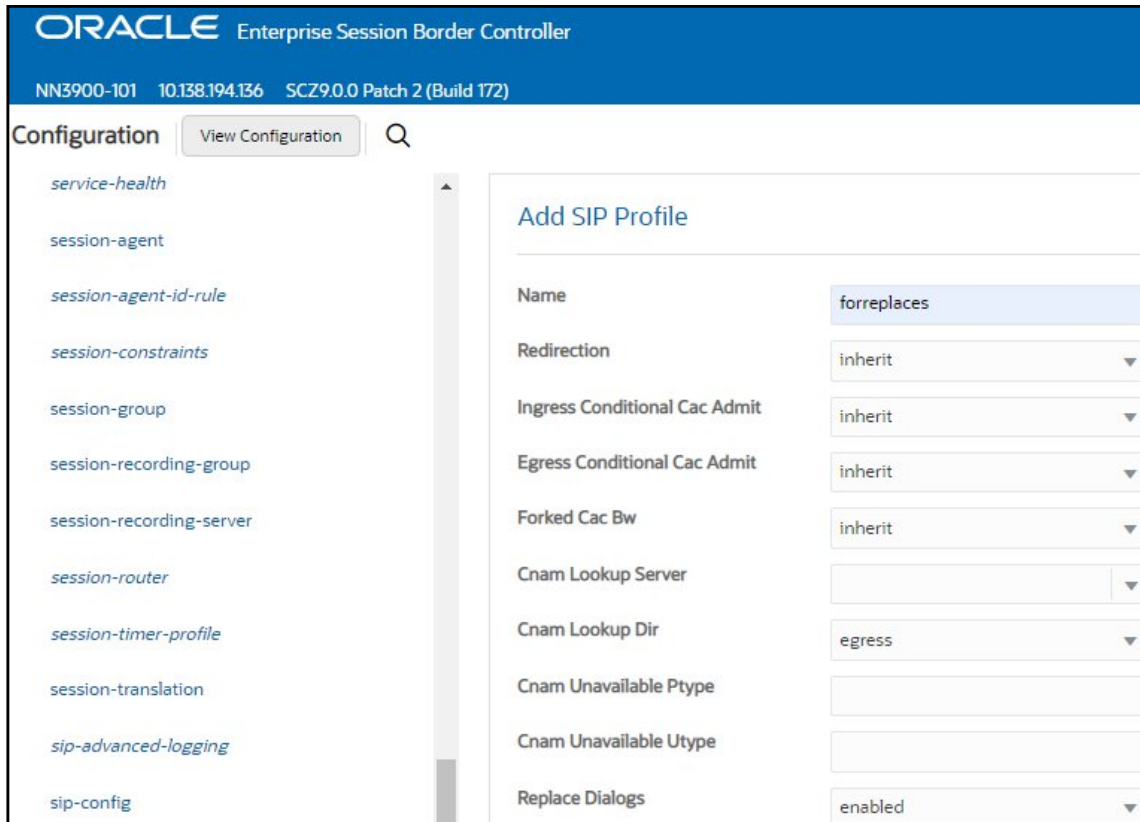
- Perform a save and activate configuration for changes to take effect.

### 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

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



- Click OK at the bottom

To configure sip profile from ACLI

ALCI Path: config tãsession-routerãsip-profile

sip-profile	
name	forreplaces
replace-dialogs	enabled

- Perform a save and activate configuration for changes to take effect.

### 6.6.3 Sip Interface

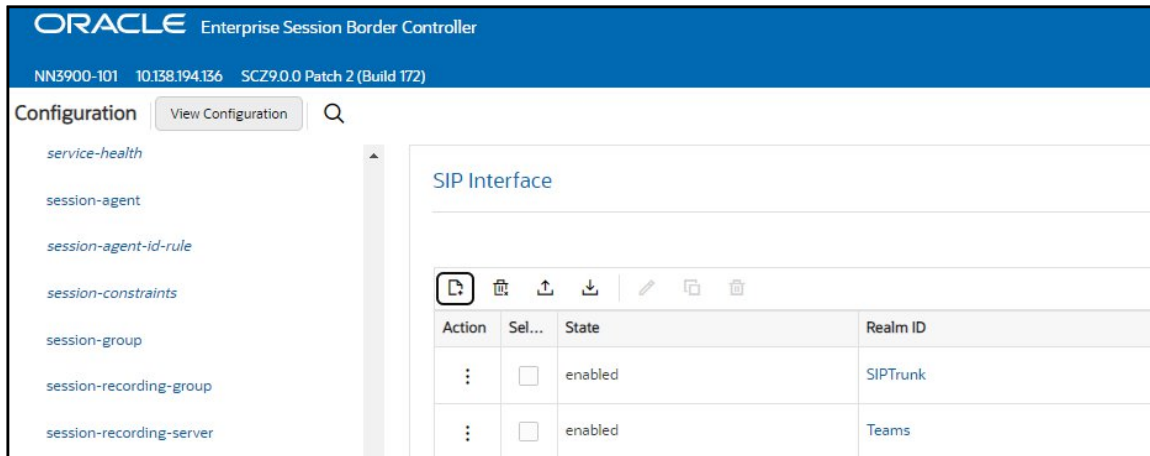
The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages

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

GUI Path: 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		fireplaces
Sip Port Config Parameter	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



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

To configure sip interface from ACLI

ACLI Path: config t session-router sip-interface

```

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 Checkfor183
  sip-profile       forreplaces

```

- Perform a save activate for changes to take effect.

### 6.6.4 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

Microsoft provides four (4) regional FQDN's for PSTN Hub (NOAM, EMEA, APAC, OCEA), These FQDNs must be configured as Session-Agents in the order of the served market. For e.g. If SBC primarily serves NOAM market(s) you MUST configure their environment to target the NOAM FQDN first.

Following 4 FQDNs must be configured as Session-Agents on Oracle SBC.

**NOAM:** sip-us.gcs.pstnhub.microsoft.com

**EMEA:** sip-eu.gcs.pstnhub.microsoft.com

**APAC:** sip-as.gcs.pstnhub.microsoft.com

**OCEA:** sip-au.gcs.pstnhub.microsoft.com

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

Config parameter	Session Agent 1	Session Agent 2	Session Agent 3	Session Agent 3
Host name	sip-us.gcs.pstnhub.microsoft.com	sip-eu.gcs.pstnhub.microsoft.com	sip-as.gcs.pstnhub.microsoft.com	sip-au.gcs.pstnhub.microsoft.com
Port	5061	5061	5061	5061
Transport method	StaticTLS	StaticTLS	StaticTLS	StaticTLS
Realm ID	Teams	Teams	Teams	Teams
Ping Method	OPTIONS	OPTIONS	OPTIONS	OPTIONS

Ping Interval	60	60	60	60
Refer Call Transfer	enabled	enabled	enabled	enabled
Ping Response	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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



- Select OK at the bottom

To configure session agents from ACLI

ACLI Path: config t session-router session-agent

```

session-agent
  hostname          10.1.2.5
  ip-address        10.1.2.5
  realm-id          SipTrunk
  ping-method       OPTIONS
  ping-interval     30
  ping-response     enabled
  out-manipulationid ACME_NAT_TO_FROM_IP
  refer-call-transfer enabled
session-agent
  hostname          sip-as.gcs.pstnhub.microsoft.com
  port              5061
  transport-method  StaticTLS
  realm-id          Teams
  ping-method       OPTIONS
  ping-interval     60
  ping-response     enabled
  refer-call-transfer enabled
session-agent
  hostname          sip-au.gcs.pstnhub.microsoft.com
  port              5061
  transport-method  StaticTLS
  realm-id          Teams
  ping-method       OPTIONS
  ping-interval     60
  ping-response     enabled
  refer-call-transfer enabled
session-agent
  hostname          sip-eu.gcs.pstnhub.microsoft.com
  port              5061
  transport-method  StaticTLS
  realm-id          Teams
  ping-method       OPTIONS
  ping-interval     60
  ping-response     enabled
  refer-call-transfer enabled
session-agent
  hostname          sip-us.gcs.pstnhub.microsoft.com
  port              5061
  transport-method  StaticTLS
  realm-id          Teams
  ping-method       OPTIONS
  ping-interval     60
  ping-response     enabled
  refer-call-transfer enabled

```

- Perform a save and activate configuration for changes to take effect.

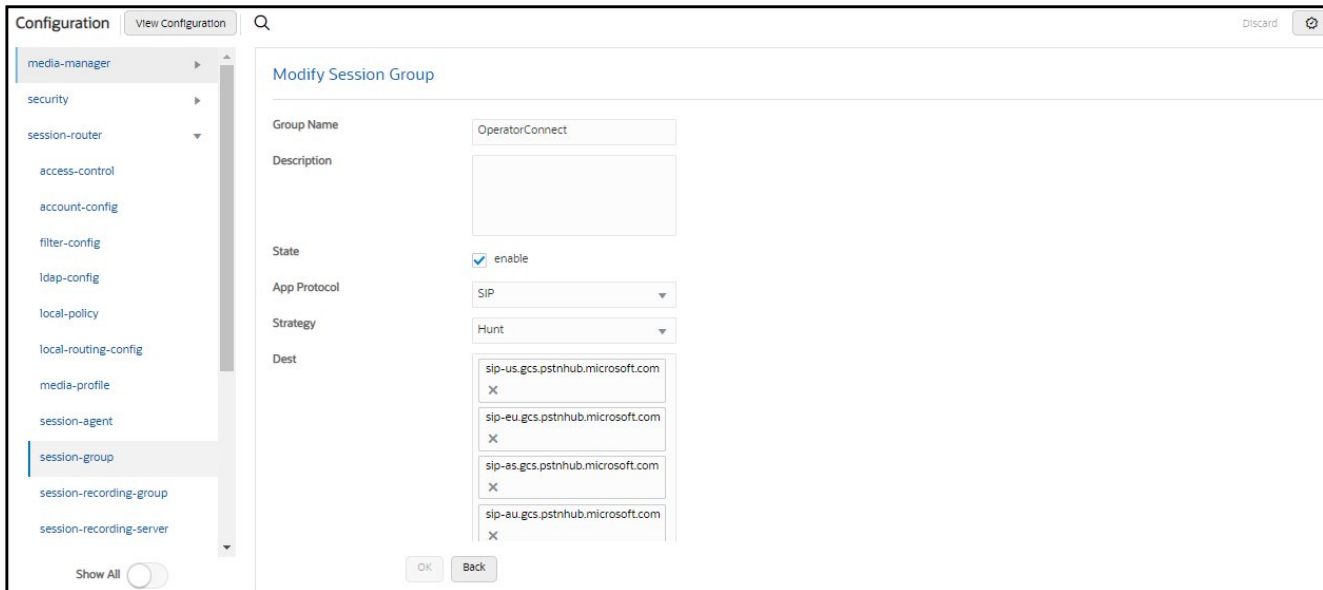
### 6.6.5 Session Group

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

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



- Click OK at the bottom

To configure session group from ACLI

ACLI Path: config t session-router session-group

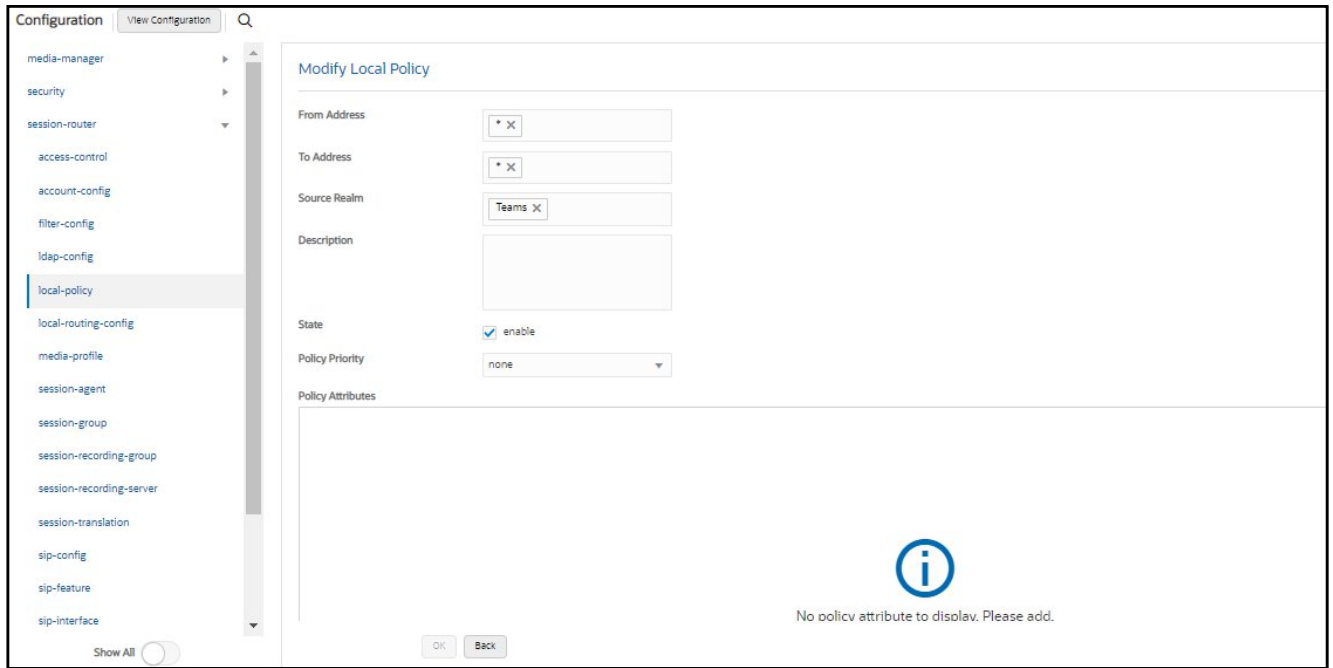
```
session-group
group-name      OperatorConnect
dest            sip-us.gcs.pstnhub.microsoft.com
               sip-eu.gcs.pstnhub.microsoft.com
               sip-as.gcs.pstnhub.microsoft.com
               sip-au.gcs.pstnhub.microsoft.com
```

- Perform a save and activate configuration for changes to take effect.

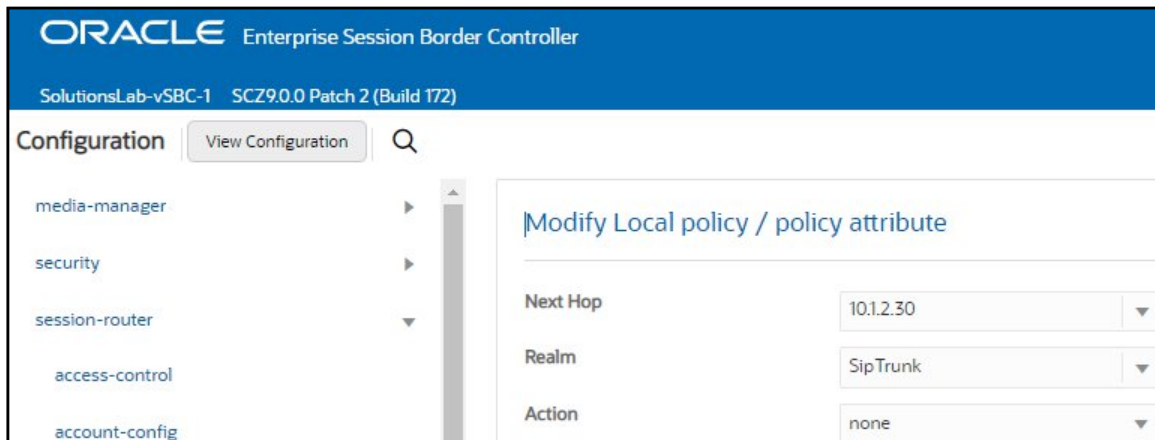
## 6.7 Routing Configuration

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



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:

Policy Attributes

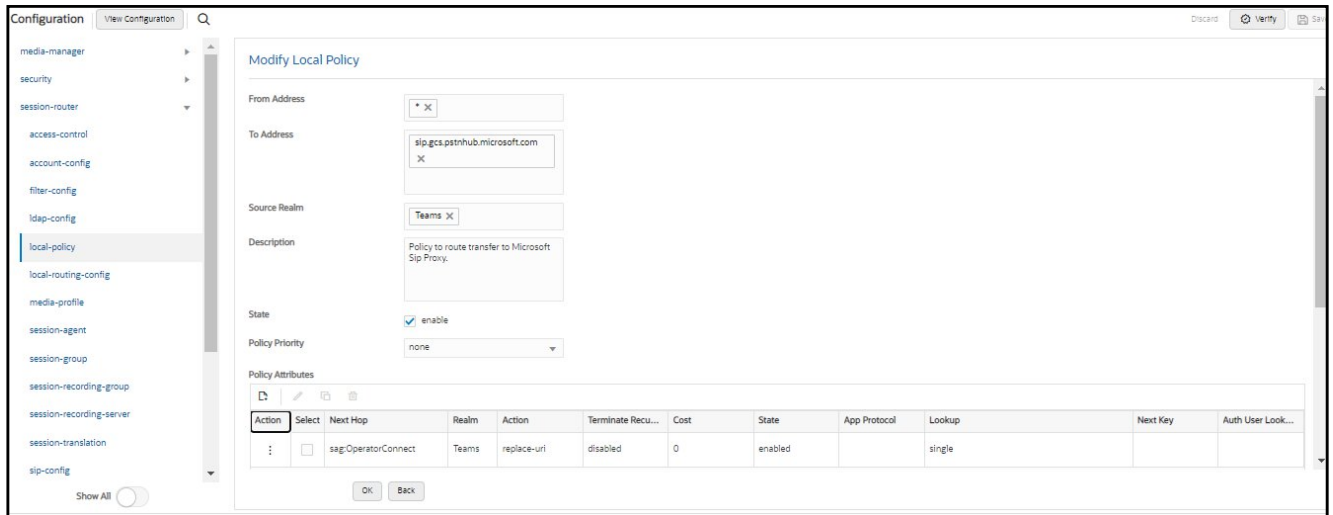
Action	Select	Next Hop	Realm	Action	Terminate Rec...	Cost	State	App Protocol	Lookup	Next Key	Auth User Lo
:	<input type="checkbox"/>	sag:OperatorConnect	Teams	replace-uri	disabled	0	enabled		single		

OK Back

Select OK when applicable on each screen

### Local Policy for Call Transfers -

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.



To configure local policy from CLI

CLI Path: config t session-router local-policy

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:OperatorConnect
	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
local-policy	from-address	*
	to-address	sip.gcs.pstnhub.microsoft.com
	source-realm	Teams
	policy-attribute	
	next-hop	sag:OperatorConnect
	realm	Teams
	action	replace-uri

- Perform a save and activate configuration for changes to take effect.

## 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.

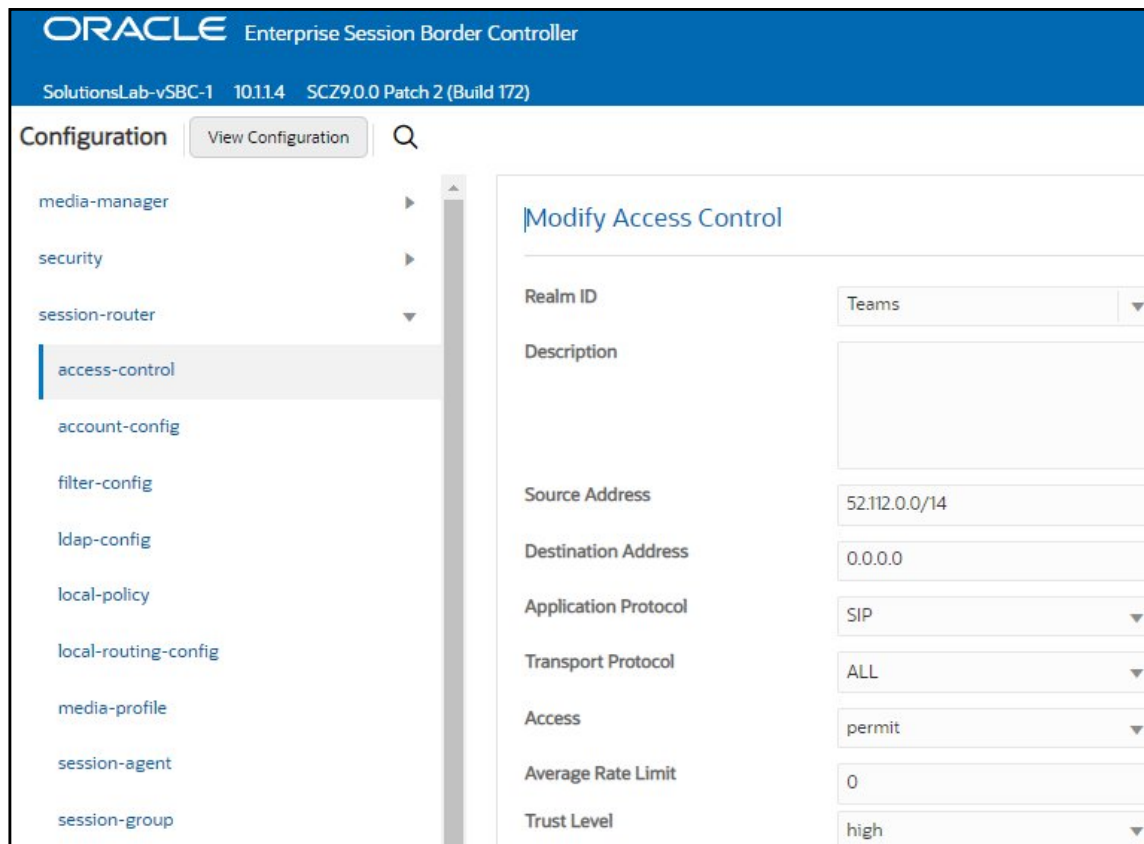
1. On all public facing interfaces, create Access-Controls to only allow sip traffic from trusted IP's with a trust level of high
2. Set the access control trust level on public facing [realms](#) to HIGH

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, i.e., Sip Trunk, etc...

GUI Path: 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

To configure access control from ACLI

ACLI Path: config t session-router access-control

```

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
access-control
  realm-id           SipTrunk
  source-address     68.68.117.67
  application-protocol SIP
  trust-level        high
  
```

- Perform a save and activate configuration for changes to take effect.

This concludes the required configuration of the SBC to properly interface with Microsoft Teams Operator Connect.

## 7 Verify Connectivity

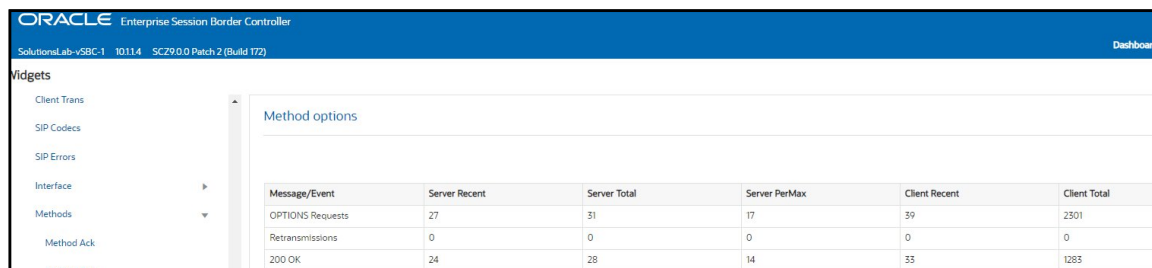
### 7.1 Oracle SBC Options Pings

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

- At the top, click “Widgets”

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

GUI Path: Signaling/SIP/Method Options



The screenshot shows the Oracle Enterprise Session Border Controller GUI. The top header includes the Oracle logo and version information: "Solutions\_Lab-vSBC-1 10.11.4 SC29.0.0 Patch 2 (Build 172)". A "Dashboard" link is visible in the top right. On the left, a "Widgets" menu is expanded, showing options like Client Trans, SIP Codescs, SIP Errors, Interface, Methods, and Method Ack. The main content area displays a "Method options" widget with a table of statistics.

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	35	1283

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

## 8 Syntax Requirements for SIP Invite and SIP Options:

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.

Microsoft includes a customer header - **X-MS-TenantId**: that contains the specific customer's O365 Tenant ID. This is used to differentiate different customers transiting within the SBC configured as Trunk for Operator Connect.

**Note:** The information is masked in the below example for security purpose.

### 8.1 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

### 8.2 Requirements for INVITE Messages and Final Responses.

Contact Header-Invite and Final Response

- Must have the FQDN sub-domain of the Oracle SBC.
- **Syntax: Contact: <phone number>@< subdomain FQDN >:<SBC Port>;<transport type>**

**Picture 1** Example of an Inbound INVITE from Microsoft and 200OK message response from the SBC.

```
INVITE sip:+17813496949@telechat.o-
test06161977.com:5061;user=phone;transport=tls SIP/2.0
FROM: Synergy
User1<sip:+17814437240@sip.gcs.pstnhub.microsoft.com:5061;user=phone>;tag=220aa9
537af94492aa6b7f32098a9bff
TO: <sip:+17813496949@telechat.o-test06161977.com:5061;user=phone>
CSEQ: 1 INVITE
CALL-ID: 42fdbe39728f5b73a124af7481009dea
MAX-FORWARDS: 70
VIA: SIP/2.0/TLS 52.115.0.35:5061;branch=z9hG4bKa618de9d
RECORD-ROUTE: <sip:sip-eu.gcs.pstnhub.microsoft.com:5061;transport=tls;lr>
CONTACT: <sip:api-du-b-jawe.pstnhub.microsoft.com:443;x-i=3a449007-a3fa-40a4-
b0d1-ecaa2f648b15;x-
c=42fdbe39728f5b73a124af7481009dea/d/28/55de76a681a34c2ca8e51a5f6dd97ceb>
CONTENT-LENGTH: 652
MIN-SE: 300
SUPPORTED: timer
USER-AGENT: Microsoft.PSTNHub.SIPProxy v.2021.5.28.7 i.EUWE.0
CONTENT-TYPE: application/sdp
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
SESSION-EXPIRES: 1800
X-MS-TenantId: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
SIP/2.0 200 Ok
FROM: Synergy
User1<sip:+17814437240@sip.gcs.pstnhub.microsoft.com:5061;user=phone>;tag=220aa9537af94492aa6b7f32098a9bff
TO: <sip:+17813496949@telechat.o-test06161977.com:5061;user=phone>;tag=12ff15510a030100
CSEQ: 1 INVITE
CALL-ID: 42fdbe39728f5b73a124af7481009dea
VIA: SIP/2.0/TLS 52.115.0.35:5061;branch=z9hG4bKa618de9d
Record-Route: <sip:sip-eu.gcs.pstnhub.microsoft.com:5061;transport=tls;lr>
Contact: <sip:+17813496949@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
```

**Picture 2** Example of an Outbound INVITE from Oracle SBC and 200OK message response from Microsoft.

```
INVITE sip:17814437243@sip-us.gcs.pstnhub.microsoft.com:5061;user=phone;transport=tls SIP/2.0
Via: SIP/2.0/TLS 20.65.42.129:5061;branch=z9hG4bKbv84u130a0ploamklum0.1
Max-Forwards: 53
From: <sip:+918130313388@telechat.o-test06161977.com:5060;user=phone>;tag=1f3d2cf80a020100
To: <sip:+17814437243@20.110.144.248:5060;user=phone>
Call-ID: 1-1f3d2cf80a020100.4e254b4f@68.68.117.67
CSeq: 2 INVITE
Contact: <sip:+918130313388@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,replaces
Content-Type: application/sdp
Content-Length: 465
X-MS-SBC: Oracle/VM/8.4.0p10
```

```
SIP/2.0 200 OK
FROM: <sip:+918130313388@telechat.o-test06161977.com:5060;user=phone>;tag=1f3d2cf80a020100
TO: <sip:+17814437243@20.110.144.248:5060;user=phone>;tag=c428e41bfffffffff441c10fdf29ff1d1
CSEQ: 2 INVITE
CALL-ID: 1-1f3d2cf80a020100.4e254b4f@68.68.117.67
VIA: SIP/2.0/TLS 10.1.4.4:5061;branch=z9hG4bKbv84u130a0ploamklum0.1
RECORD-ROUTE: <sip:sip-us.gcs.pstnhub.microsoft.com:5061;transport=tls;lr>
CONTACT: <sip:api-du-a-usea.pstnhub.microsoft.com:443;x-i=5b91f474-e551-4193-aafd-3402ebf9515a;x-c=460859ece4ce5d59b176f00581a1415c/s/1/853ad12525314f64ae4677a23afdc208>
CONTENT-LENGTH: 1285
CONTENT-TYPE: application/sdp
ALLOW: INVITE, ACK, OPTIONS, CANCEL, BYE, NOTIFY
SERVER: Microsoft.PSTNHub.SIPProxy v.2022.2.14.2 i.USEA.4
X-MS-TenantId: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

## 8.3 Requirements for SIP Options.

Below are the Microsoft requirements for SIP Options Message.

- The SBC MUST support the SIP OPTIONS method and respond to an incoming SIP OPTIONS request based on RFC 3261.
- The SBC MUST NOT respond with SIP/2.0 405 Method Not Supported or 215 SIP/2.0 501 Not Implemented.
- The OPTIONS pings from SBC MUST NOT exceed a frequency of one transaction every 60 seconds for each configured trunk and MUST NOT be more less frequent than one 229 transaction every 180 seconds for each configured trunk.
- Microsoft will not initiate OPTIONS pings to SBC until it receives OPTIONS pings from the SBC.
- The CONTACT header MUST contain the FQDN of the trunk and MUST specify both the port and protocol (e.g., 5061 and TLS)
- **Syntax: Contact: <phone number>@< subdomain FQDN >:<SBC Port>;<transport type>**
- Microsoft will not include the ACCEPT header and will ignore any body text in the response.

**Picture 3** - Example of SIP OPTIONS message from Oracle SBC to Microsoft.

```
OPTIONS sip:sip-us.gcs.pstnhub.microsoft.com:5061;transport=tls SIP/2.0
Via: SIP/2.0/TLS 20.65.42.129:5061;branch=z9hG4bKdik4l8206025aqb9v510
Call-ID: c75cbb319998591b44c2c7e20e8f717b0000g30@10.1.4.4
To: sip:ping@sip-us.gcs.pstnhub.microsoft.com
From: sip:ping@telechat.o-test06161977.com;tag=bba52bd57d6bd688fde828d05f2a71830000g30
Max-Forwards: 70
CSeq: 7 OPTIONS
Contact: sip:ping@telechat.o-test06161977.com:5061;transport=tls;sip.ice
Expires: 60
Route: sip:52.115.54.0:5061;transport=tls;lr
X-MS-SBC: Oracle/VM/8.4.0p10
Content-Length: 0
```

**Picture 4** - Example of SIP OPTIONS message from Microsoft to Oracle SBC.

```
OPTIONS sip:ping@telechat.o-test06161977.com:5061;transport=tls SIP/2.0
FROM: <sip:sip-us.gcs.pstnhub.microsoft.com:5061>;tag=89a53e30-276b-4596-a761-0ac7c919a859
TO: <sip:ping@telechat.o-test06161977.com>
CSEQ: 1 OPTIONS
CALL-ID: 92542534-cad5-4501-a418-b9f6304bf45b
MAX-FORWARDS: 70
VIA: SIP/2.0/TLS 52.115.54.0:5061;branch=z9hG4bK728aa3f0
CONTACT: <sip:sip-us.gcs.pstnhub.microsoft.com:5061>
CONTENT-LENGTH: 0
USER-AGENT: Microsoft.PSTNHub.SIPProxy v.2022.2.14.2 i.USEA.3
ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
```

## 9 Appendix A

### 9.1 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® Session Border Controller (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.

### 9.1.1 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](#)

## 10 Appendix B

### 10.1 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.

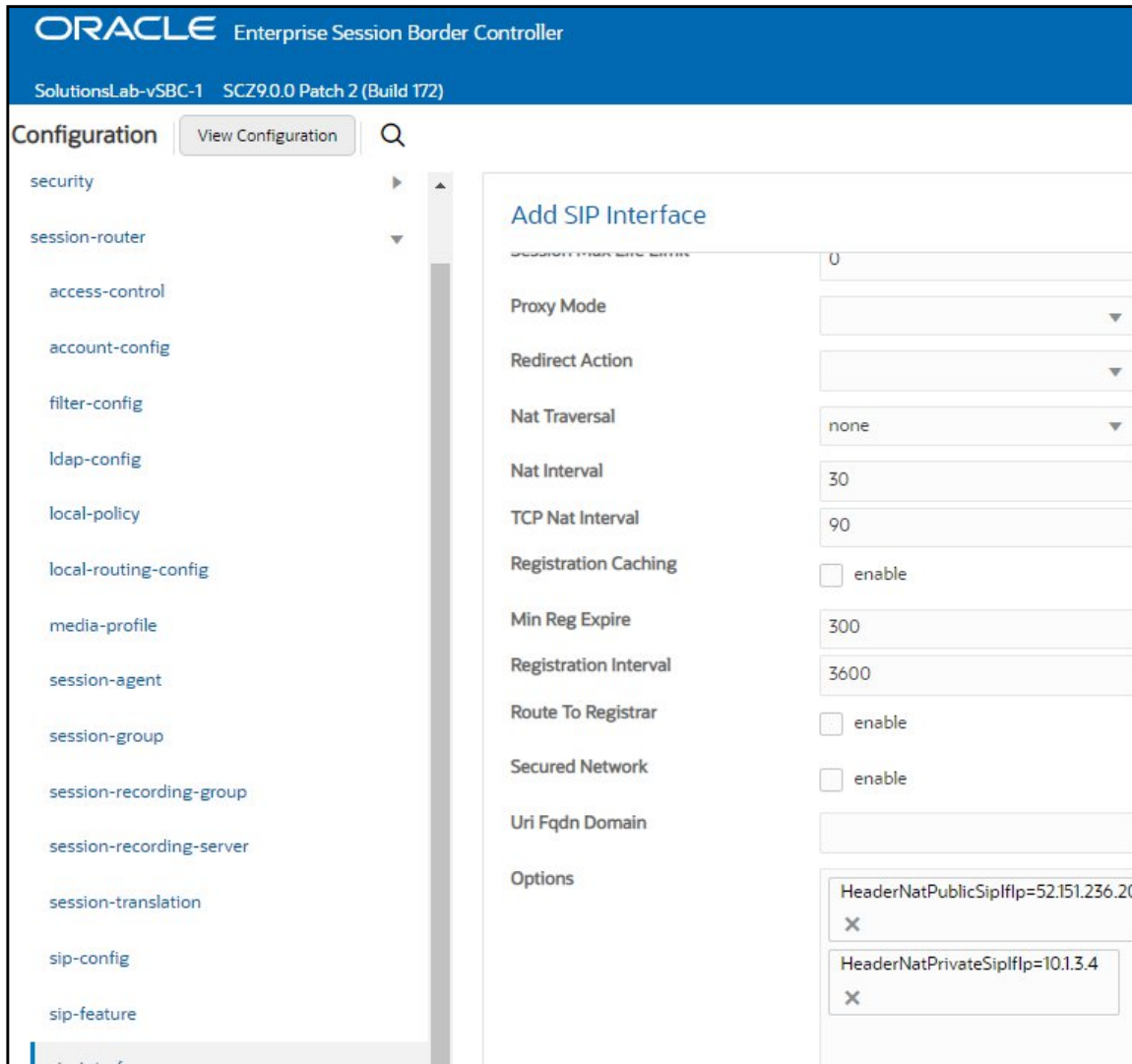
The SPL is applied to the Teams side SIP interface.

GUI Path: session-router/sip-interface

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.1.3.4

HeaderNatPublicSipIfIp is the public interface ip

HeaderNatPrivateSipIfIp is the private ip.



To configure header NAT SPL from ACLI

ACLI Path: config t session-router sip-interface

Choose the sip interface on which the header NAT SPL needs to be applied. Under spl-options add the entry as per example shared below.

```
spl-options
HeaderNatPublicSipIfIp=20.110.144.248,HeaderNatPrivateSipIfIp=10.1.2.4
```

- Perform a save and activate configuration for changes to take effect.

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

## 10.2 Ring back 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-manipulation on the Teams Sip Interface.

sip-manipulation name	Checkfor183
--------------------------	-------------

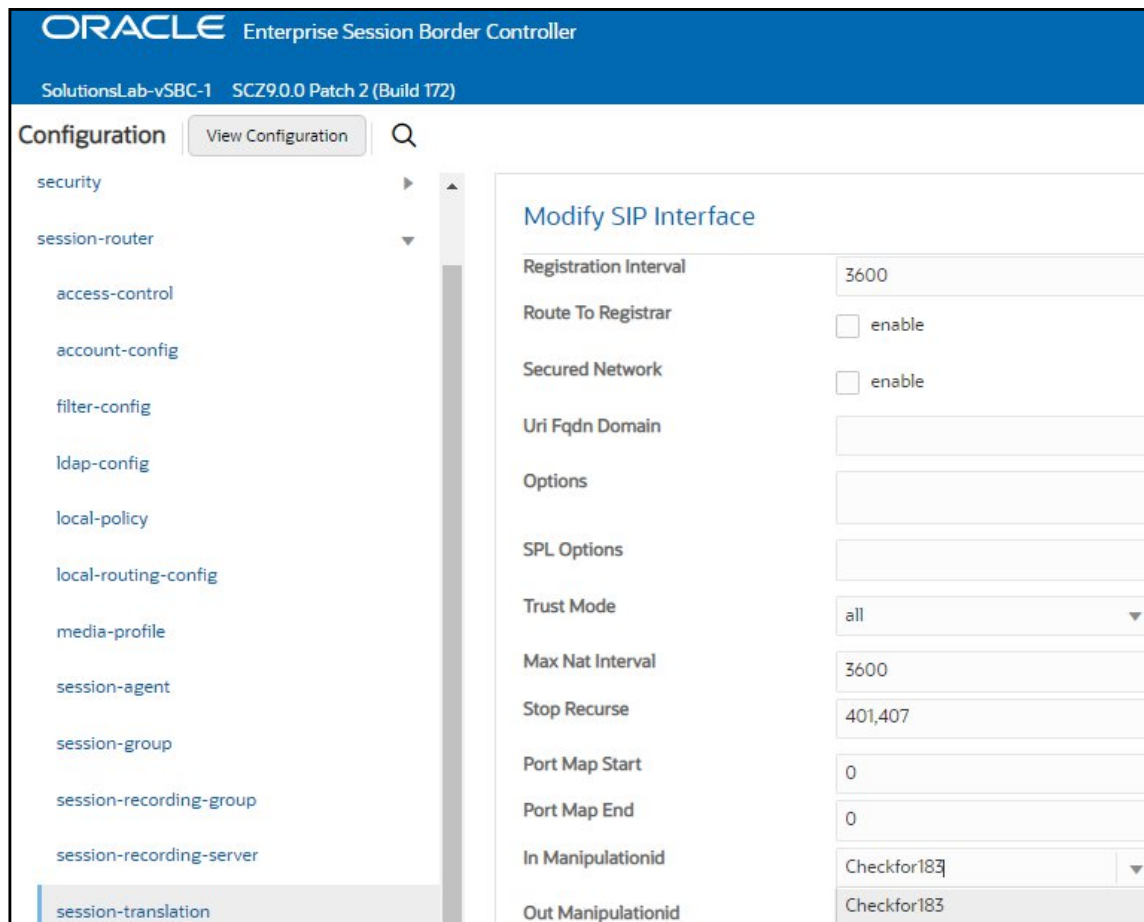
```

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:

GUI Path: Session Router/Sip Interface



To apply the sip manipulation on the Teams sip interface from ACLI

ACLI Path: `config t session-router sip-interface`

Put the sip manipulation on the 'in-manipulationid' configuration object.

in-manipulationid	Checkfor183
-------------------	-------------

- Perform a save and activate configuration for changes to take effect.

## 10.3 Oracle SBC Local Media Playback

### 10.3.1 Ring back 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 ring back upon receipt of the sip REFER from Microsoft.

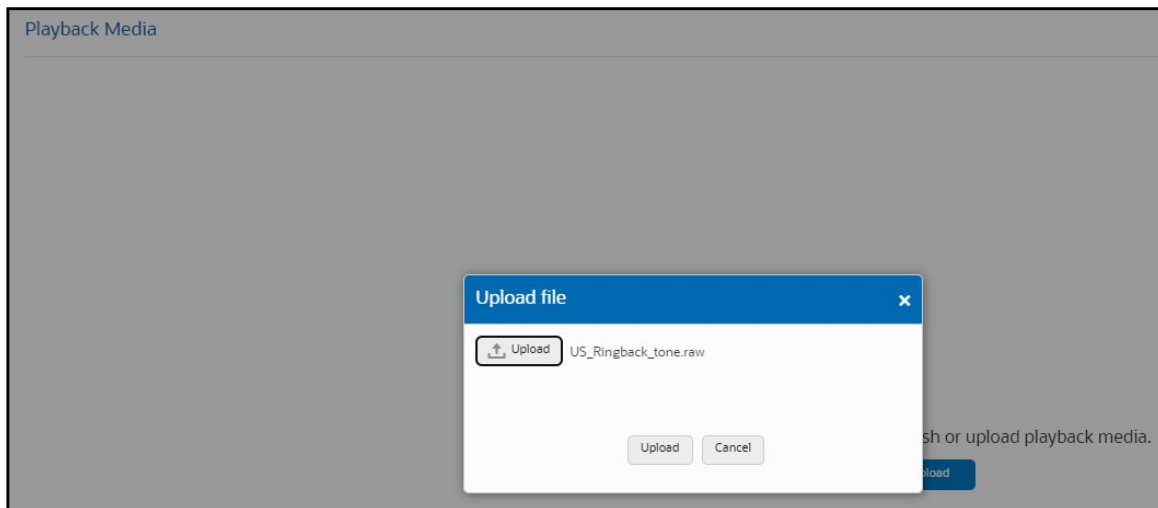
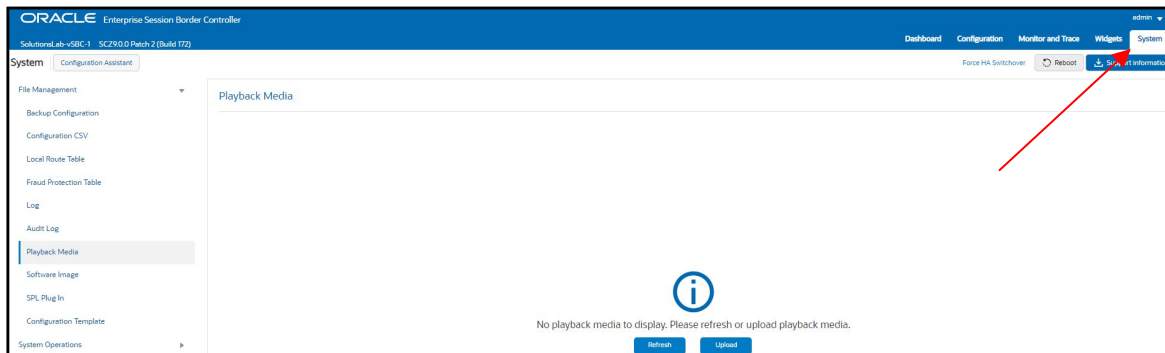
First, you must create a media file.

### 10.3.1.1 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.

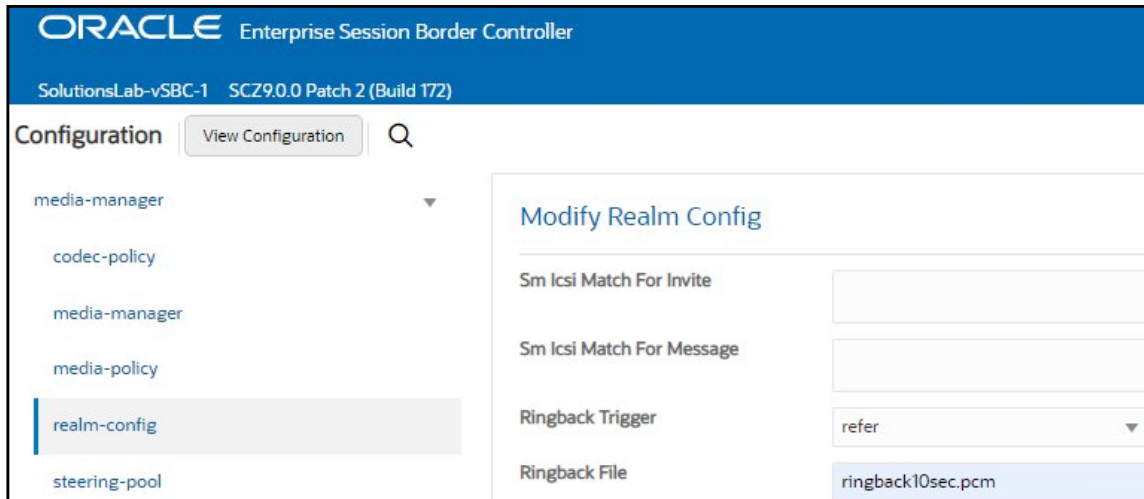
Next, upload the file to the /code/media directory on the Oracle SBC.

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



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

To assign the ring back file on the realm through ACLI, navigate to below path and provide the name of the ringback file at the Ringback File config object.

ACLI Path: `config tamedia-managerrealm-config`

in-manipulationid	Checkfor183
-------------------	-------------

- Perform a save and activate configuration for changes to take effect.

## 11 ACLI Running Configuration

Below is a complete output of the running configuration used to create this application note. This output includes all of 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.



certificate-record	
name	DigiCertGlobalRootCA
common-name	DigiCert Global Root CA
certificate-record	
name	DigiCertGlobalRootG2
common-name	DigiCert Global Root G2
certificate-record	
name	DigiCertGlobalRootG3
common-name	DigiCert Global Root G3
certificate-record	
name	DigiCertTLSRSA4096RootG5
common-name	DigiCert TLS RSA4096 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
certificate-record	
name	WebServerInstance
state	California
locality	Redwood City
organization	Oracle Corporation
unit	Oracle CGBU-LABS BOSTON
common-name	managementcertificate
codec-policy	
name	SipTrunkCodecs
allow-codecs	PCMU G729 telephone-event
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
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:OperatorConnect
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

```

```

local-policy
  from-address   *
  to-address     sip.gcs.pstnhub.microsoft.com
  source-realm   Teams
  policy-attribute
    next-hop     sag:OperatorConnect
    realm       Teams
    action       replace-uri
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
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     s0p0:0.4
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     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
access-control-trust-level high
codec-policy           addCN
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
ping-response          enabled
session-agent
hostname               sip-as.gcs.pstnhub.microsoft.com
port                   5061
transport-method       StaticTLS
realm-id               Teams
ping-method            OPTIONS
ping-interval          60
ping-response          enabled

```

```

refer-call-transfer      enabled
session-agent
hostname                 sip-au.gcs.pstnhub.microsoft.com
port                    5061
transport-method        StaticTLS
realm-id                Teams

```

```

ping-method             OPTIONS
ping-interval           60
ping-response           enabled
refer-call-transfer     enabled
session-agent
hostname                 sip-eu.gcs.pstnhub.microsoft.com
port                    5061
transport-method        StaticTLS
realm-id                Teams
ping-method             OPTIONS
ping-interval           60
ping-response           enabled
refer-call-transfer     enabled
session-agent
hostname                 sip-us.gcs.pstnhub.microsoft.com
port                    5061
transport-method        StaticTLS
realm-id                Teams
ping-method             OPTIONS
ping-interval           60
ping-response           enabled
refer-call-transfer     enabled
session-group
group-name              OperatorConnect
dest                    sip-us.gcs.pstnhub.microsoft.com
                        sip-eu.gcs.pstnhub.microsoft.com
                        sip-as.gcs.pstnhub.microsoft.com
                        sip-au.gcs.pstnhub.microsoft.com
sag-recursion           enabled
stop-sag-recurse       401,407,480
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 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 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-profile	
name	forreplaces
replace-dialogs	enabled
steering-pool	
ip-address	10.1.2.4
start-port	20001
end-port	40000
realm-id	SipTrunk
steering-pool	
ip-address	10.1.4.4
start-port	10000
end-port	20000
realm-id	Teams
system-config	
hostname	oraclesbc.com
description	SBC connecting PSTN Sip Trunk to Microsoft Operator Connect
location	Burlington, MA
transcoding-cores	1
tls-global	
session-caching	enabled
diffie-hellman-key-size	DH_KeySize_2048
tls-profile	
name	TLSTeams
end-entity-certificate	SBCCertificateforTeams
trusted-ca-certificates	DigiCertRoot DigiCertGlobalRootG2 DigiCertGlobalRootG3 DigiCertTLSECCP384RootG5 DigiCertTLSECCP4096RootG5 MicrosoftECCRootCertificateAuthority2017 MicrosoftRSARootCertificateAuthority2017
mutual-authenticate	enabled
tls-version	tlsv12
trusted-ca-certificates	
mutual-authenticate	enabled
tls-profile	
name	WebServerInstance
end-entity-certificate	WebServerInstance
trusted-ca-certificates	DigiCertRoot





**ORACLE**

CONNECT WITH US

 [blogs.oracle.com/oracle](https://blogs.oracle.com/oracle)

 [facebook.com/Oracle/](https://facebook.com/Oracle/)

 [twitter.com/Oracle](https://twitter.com/Oracle)

 [oracle.com](https://oracle.com)

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

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

### Integrated Cloud Applications & Platform Services

Copyright © 2021, 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