



ORACLE

Oracle SBC integration with Teams
Direct Routing and Twilio Elastic SIP
Trunking

Technical Application Note



ORACLE

Disclaimer

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

Revision History

Version	Description of Changes	Date Revision Completed
1.0	Oracle SBC integration with MS Teams DR and Twilio Elastic SIP Trunking	25 th March 2021

Table of Contents

1. INTENDED AUDIENCE	4
2. DOCUMENT OVERVIEW	4
2.1. TWILIO ELASTIC SIP TRUNKING	4
2.2. MICROSOFT TEAMS	4
3. INTRODUCTION	5
3.1. AUDIENCE	5
3.2. REQUIREMENTS	5
3.3. ARCHITECTURE	6
4. CONFIGURE MICROSOFT TEAMS DIRECT ROUTING	7
4.1. ACCESS TEAMS ADMIN CENTER	7
4.2. CONFIGURE ONLINE PSTN GATEWAY	8
4.3. CONFIGURE ONLINE PSTN USAGE	8
4.4. CONFIGURE ONLINE VOICE ROUTES	9
4.5. CONFIGURE ONLINE VOICE ROUTING POLICY	10
4.6. ASSIGN VOICE ROUTING POLICY TO USERS	11
5. CONFIGURING THE SBC	12
5.1. VALIDATED ORACLE SBC VERSION	12
6. NEW SBC CONFIGURATION	12
6.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC	12
6.2. CONFIGURE SBC USING WEB GUI	16
6.3. CONFIGURE SYSTEM-CONFIG	18
6.4. CONFIGURE PHYSICAL INTERFACE VALUES	19
6.5. CONFIGURE NETWORK INTERFACE VALUES	20
6.6. ENABLE MEDIA MANAGER	22
6.7. CONFIGURE REALMS	23
6.8. ENABLE SIP-CONFIG	26
6.9. CONFIGURING A CERTIFICATE FOR SBC	27
6.10. TLS-PROFILE	32
6.11. CONFIGURE SIP INTERFACES	33
6.12. CONFIGURE SESSION-AGENT	34
CLICK HERE FOR MORE INFORMATION ON TWILIO ELASTIC SIP TRUNKING IP ADDRESS	36
6.13. CONFIGURE SESSION-AGENT GROUP	36
6.14. CONFIGURE LOCAL-POLICY	37
6.15. CONFIGURE STEERING-POOL	39
6.16. CONFIGURE SIP-MANIPULATION	40
6.17. CONFIGURE MEDIA PROFILE AND CODEC POLICY	43
6.18. CONFIGURE ICE PROFILE	45
6.19. CONFIGURE SDES PROFILE	45
6.20. CONFIGURE MEDIA SECURITY PROFILE	46
6.21. CONFIGURE RTCP POLICY AND RTCP MUX	46
7. EXISTING SBC CONFIGURATION	47
8. TWILIO ELASTIC SIP TRUNK CONFIGURATION	48
8.1 Create an IP-ACL rule	48
8.2 Create a new Trunk	49

9. VERIFICATION OF SAMPLE CALL FLOWS

APPENDIX A

ERROR! HYPERLINK REFERENCE NOT VALID.ERROR! HYPERLINK REFERENCE NOT VALID.**ERROR! HYPERLINK REFERENCE NOT VALID.**
Hyperlink reference not valid.Error! Hyperlink reference not valid.Error! Hyperlink reference not valid.
valid.ERROR! HYPERLINK REFERENCE NOT VALID.ERROR! HYPERLINK REFERENCE NOT VALID.

1. Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle Enterprise customers and partners and end users of the Oracle Enterprise Session Border Controller (SBC). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Session Border Controller platform along with Microsoft Teams Direct Routing Enterprise Model.


2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Twilio Elastic SIP Trunk with Microsoft Teams Direct Routing. The solution contained within this document has been tested using Oracle Communication SBC with **OS 840p3B version**.

In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the Microsoft Teams and Twilio Elastic SIP Trunk related parameters. Many SBC applications may have additional configuration requirements that are specific to individual customer requirements. These configuration items are not covered in this guide. Please contact your Oracle representative with any questions pertaining to this topic.

Please find the related documentation links below:

2.1. Twilio Elastic SIP Trunking



[Twilio Elastic SIP Trunking](#) is a cloud-based solution that provides connectivity for IP-based communications infrastructure to connect to the PSTN for making and receiving telephone calls to the rest of the world via any broadband internet connection. Twilio's Elastic SIP Trunking service automatically scales, up or down, to meet your traffic needs with unlimited capacity. In just minutes you can deploy globally with Twilio's easy-to-use self-service tools without having to rely on slow providers.

Sign up for a [free Twilio trial](#) and learn more about [configuring your Twilio Elastic SIP Trunk](#).

2.2. Microsoft Teams

Microsoft Phone System Direct Routing allows connection of a supported customer-provided Session Border Controller (SBC) to a Microsoft Phone System. Direct Routing enables using virtually any PSTN trunk with Microsoft Phone System and configuring interoperability between customer-owned telephony equipment, such as a third-party private branch exchange (PBX), analog devices, and Microsoft Phone System.

<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://www.oracle.com/a/otn/docs/vzbwithsbcmstteams-mb.pdf>

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

Please note that the IP Addresses, FQDN and configuration names and details given in this document are used for reference purposes only. These same details cannot be used in customer configurations. End users of this document can use the configuration details according to their network requirements.

3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Teams Direct Routing Enterprise Model using Oracle Enterprise SBC. There will be steps that require navigating the Teams configuration, Oracle SBC GUI interface. Understanding the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

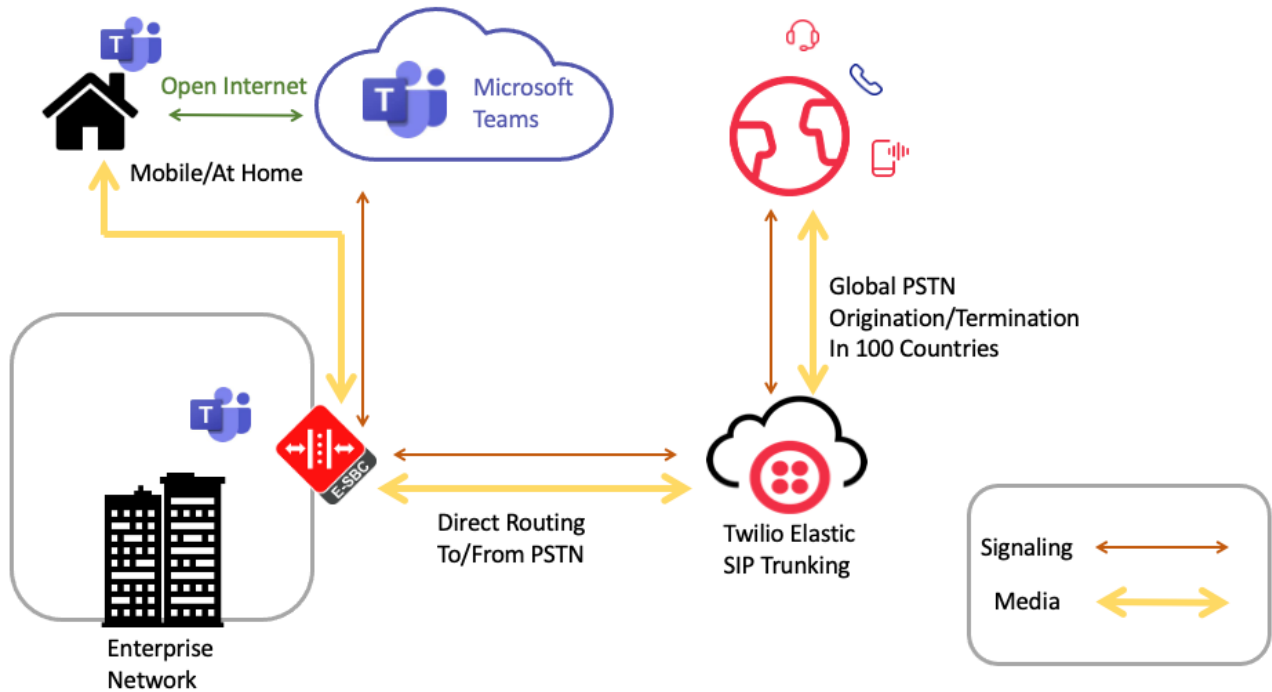
3.2. Requirements

- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version
- Teams Direct Routing Enterprise Model running Teams Client.

The below revision table explains the versions of the software used for each component:
 This table is Revision 1 as of now:

Software Used	SBC Version	Teams Client version
Revision 1	8.4.0	1.3.00.28779 (64-bit) (Windows) v.1416/1.0.0.2021010802 (Mobile)

3.3. Architecture



The configuration, validation and troubleshooting are the focuses of this document and will be described in three phases:

- Phase 1 – Configuring the Teams Direct Routing Enterprise Model.
- Phase 2 – Configuring the Oracle SBC.
- Phase 3 – Configuring the Twilio Elastic SIP Trunk

4. Configure Microsoft Teams Direct Routing

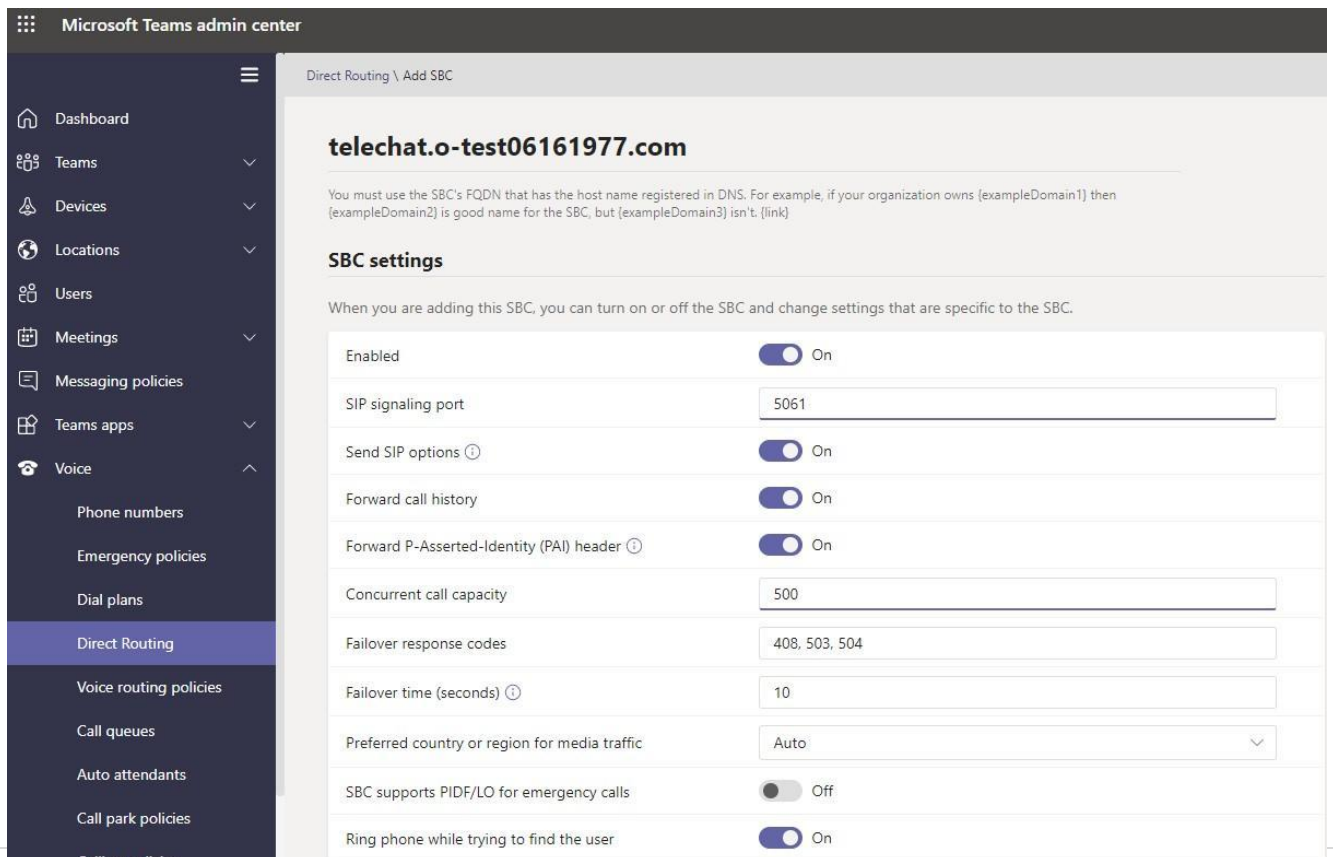
The steps outlined below is the minimum required configuration to pair your SBC with Microsoft Teams Direct Routing Interface. **This is to be used as an example only, and we highly recommend you work with your Microsoft Account representative to implement the correct configuration for your specific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

4.1. Access Teams Admin center

The first step is to access the Teams Admin Center with administrator admin credentials:

4.2. Configure Online PSTN Gateway

Configuration Path: Voice/Direct Routing/SBC



Microsoft Teams admin center

Direct Routing \ Add SBC


telechat.o-test06161977.com

You must use the SBC's FQDN that has the host name registered in DNS. For example, if your organization owns {exampleDomain1} then {exampleDomain2} is good name for the SBC, but {exampleDomain3} isn't. [\(link\)](#)

SBC settings

When you are adding this SBC, you can turn on or off the SBC and change settings that are specific to the SBC.

Enabled	<input checked="" type="checkbox"/> On
SIP signaling port	5061
Send SIP options ⓘ	<input checked="" type="checkbox"/> On
Forward call history	<input checked="" type="checkbox"/> On
Forward P-Asserted-Identity (PAI) header ⓘ	<input checked="" type="checkbox"/> On
Concurrent call capacity	500
Failover response codes	408, 503, 504
Failover time (seconds) ⓘ	10
Preferred country or region for media traffic	Auto
SBC supports PIDF/LO for emergency calls	<input type="checkbox"/> Off
Ring phone while trying to find the user	<input checked="" type="checkbox"/> On



Click Save at the bottom of the page

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

4.3. Configure Online PSTN Usage

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

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

4.4. Configure Online Voice Routes

Configuration Path: Voice/Direct Routing/Voice Routes

4.5. Configure Online Voice Routing Policy

Configuration Path: Voice/Voice Routing Policies



4.6. Assign Voice Routing Policy to Users

Configuration Path: Users/Select the “User”/Policies

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

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

With this, Microsoft Teams Direct Routing config is complete.

5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Teams Direct Routing and Twilio Elastic SIP Trunking.

5.1. Validated Oracle SBC version

Oracle conducted tests with Oracle SBC 8.4 software – this software with the configuration listed below can run on any of the following products:

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

- VME

6. New SBC configuration

If the customer is looking to setup a new SBC from scratch, please follow the section below.

6.1. Establishing a serial connection to the SBC

Connect one end of a straight-through Ethernet cable to the front console port (which is active by default) on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB-9 adapter) to the DB-9 port on a workstation, running a terminal emulator application such as Putty. Start the terminal emulation application using the following settings:

- Baud Rate=115200
- Data Bits=8
- Parity=None
- Stop Bits=1
- Flow Control=None

Power on the SBC and confirm that you see the following output from the boot-up sequence

```
Starting tLemd...
Starting tServiceHealth...
Starting tCollect...
Starting tAtcpd...
Starting tAsctpd...
Starting tMbcd...
Starting tCommMonitord...
Starting tFped...
Starting tAlgd...
Starting tRadd...
Starting tEbmd...
Starting tSipd...
Starting tH323d...
Starting tIPTd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tTscfd...
Starting tAppWeb...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Starting tIFMIBd...
Start platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...
password secure mode is enabled
Admin Security is disabled
Starting SSH...
SSH Cli init: allocated memory for 5 connections
```

Enter the default password to log in to the SBC. Note that the default SBC password is “acme” and the default super user password is “packet”.

Both passwords have to be changed according to the rules shown below.

```
Password:
%
% Only alphabetic (upper or lower case), numeric and punctuation
% characters are allowed in the password.
% Password must be 8 - 64 characters,
% and have 3 of the 4 following character classes :
%   - lower case alpha
%   - upper case alpha
%   - numerals
%   - punctuation
%
Enter New Password:
Confirm New Password:

Password is acceptable.
```

Now set the management IP of the SBC by setting the IP address in bootparam.

To access bootparam. Go to Configure terminal->bootparam.

```
NN4600-139# conf t
NN4600-139(configure)# bootparam

'.' = clear field; '-' = go to previous field; q = quit

Boot File           : /boot/nnSCZ840p3B.bz
IP Address          : 10.138.194.139
VLAN                : 0
Netmask             : 255.255.255.192
Gateway             : 10.138.194.129
IPv6 Address        :
IPv6 Gateway        :
Host IP             :
FTP username        : vxftp
FTP password        : vxftp
Flags               :
Target Name         : NN4600-139
Console Device      : COM1
Console Baudrate    : 115200
Other               :

NOTE: These changed parameters will not go into effect until reboot.
Also, be aware that some boot parameters may also be changed through
PHY and Network Interface Configurations.

ERROR   : space in /boot      (Percent Free: 40)

NN4600-139(configure)#
```

Note: There is no management IP configured by default.

Setup product type to Enterprise Session Border Controller as shown below.

To configure product type, type in setup product in the terminal

```
NN4600-139#
NN4600-139# setup product

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

Last Modified 2020-04-30 22:38:15
-----
 1 : Product      : Enterprise Session Border Controller

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

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

Save the changes and reboot the SBC.

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

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1
  Session Capacity (0-128000)           : 500

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 3
*****
CAUTION: Enabling this feature activates enhanced security
functions. Once saved, security cannot be reverted without
resetting the system back to factory default state.
*****
  Admin Security (enabled/disabled)      :

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 5
  Transcode Codec AMR Capacity (0-102375) : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2
  Advanced (enabled/disabled)           : enabled

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10
  Transcode Codec OPUS Capacity (0-102375) : 50

Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 11
  Transcode Codec SILK Capacity (0-102375) : 50
```

The SBC comes up after reboot and is now ready for configuration.

Go to configure terminal->system->http-server-config.

Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

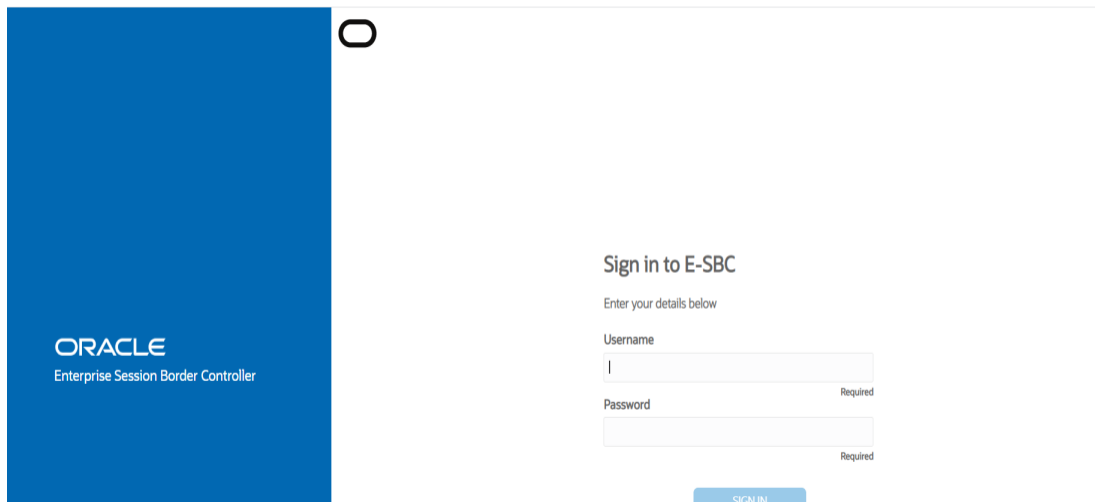
```
NN4600-139(http-server) #  
NN4600-139(http-server) # show  
http-server  
    name                webServerInstance  
    state                enabled  
    realm  
    ip-address  
    http-state          enabled  
    http-port           80  
    https-state         disabled  
    https-port          443  
    http-interface-list REST, GUI  
    http-file-upload-size 0  
    tls-profile  
    auth-profile  
    last-modified-by    @  
    last-modified-date  2021-01-25 00:16:28  
  
NN4600-139(http-server) # █
```

6.2. Configure

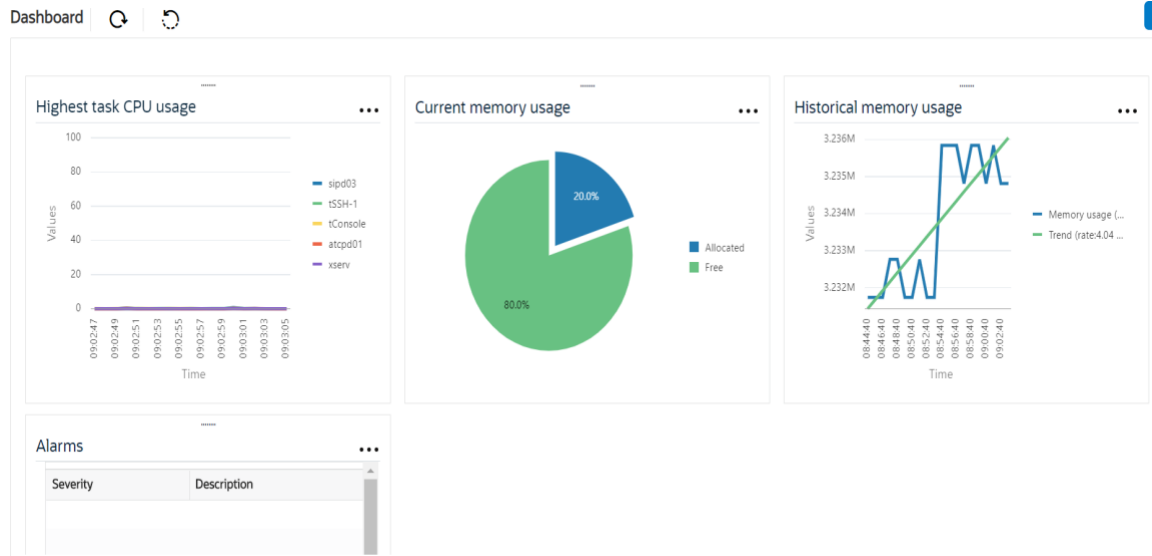
SBC using Web GUI

In this app note, we configure SBC using the WebGUI.

The Web GUI can be accessed through the url http://<SBC_MGMT_IP>.



The username and password is the same as that of CLI.



Go to Configuration as shown below, to configure the SBC

The Configuration Objects page includes a navigation menu (Wizards, Commands), a search bar, and a list of objects:

Name	Description
access-control	Configure a static or dynamic access control list
account-config	Configure Quality of Service accounting
authentication-profile	Configure authentication profile
certificate-record	Create, generate, and import a certificate
class-policy	Configure classification profile policies
codec-policy	Create and apply a codec policy to a realm and an agent
filter-config	Create a custom filter for SIP monitor and trace
fraud-protection	Configure fraud protection
host-route	Insert entries into the routing table
http-client	Configure an HTTP client
http-server	Configure an HTTP server

Displaying 1 - 11 of 42

Kindly refer to the GUI User Guide given below for more information.

https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf

The expert mode is used for configuration.

Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

6.3. Configure system-config

Go to system->system-config

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration categories, with 'system-config' selected. The main area is titled 'Modify System Config' and contains the following fields:

Hostname	OracleSBC
Description	
Location	
Mib System Contact	
Mib System Name	
Mib System Location	
Acp TLS Profile	

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

Please enter the default gateway value in the system config page.

This screenshot shows the 'Modify System Config' page with additional options. The 'Default Gateway' field is highlighted with a red box and contains the value '10.138.194.129'. Other fields include:

Call Trace	<input type="checkbox"/> enable
Restart	<input checked="" type="checkbox"/> enable
Telnet Timeout	0 (Range: 0..65535)
Console Timeout	0 (Range: 0..65535)
HTTP Timeout	5 (Range: 0..20)
Alarm Threshold	

An 'Add' button is located below the 'Alarm Threshold' field, and 'OK' and 'Delete' buttons are at the bottom.

For VME, transcoding cores are required. Please refer the documentation here for more information

https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/releasenotes/esbc_scz840_releasenotes.pdf

The above step is needed only if any transcoding is used in the configuration. If there is no transcoding involved, then the above step is not needed.

6.4. Configure Physical Interface values

To configure physical Interface values, go to System->phy-interface.

Please configure M00 for Teams side and M10 for Twilio side.

Parameter Name	Teams Side (M00)	Twilio Elastic Sip Trunk side (M10)
Slot	0	0
Port	0	1
Operation Mode	Media	Media

Please configure M00 interface as below.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration', and 'Monitor and Trace'. Below the navigation bar, there are 'Wizards' and 'Commands' dropdown menus, and 'Save' and 'Verify' buttons. The main content area is titled 'Add Phy Interface' and contains the following configuration fields:

- Name: M00
- Operation Type: Media
- Port: 0 (Range: 0..5)
- Slot: 0 (Range: 0..2)
- Virtual Mac: (empty)
- Admin State: enable
- Auto Negotiation: enable
- Duplex Mode: FULL
- Speed: 100

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

Please configure M10 interface as below

The screenshot shows the 'Add Phy Interface' configuration page in the Enterprise Session Border Controller. The left sidebar lists various configuration categories, with 'phy-interface' selected. The main form contains the following fields and values:

- Name: M10
- Operation Type: Media
- Port: 0 (Range: 0..5)
- Slot: 1 (Range: 0..2)
- Virtual Mac: (empty)
- Admin State: enable
- Auto Negotiation: enable
- Duplex Mode: FULL
- Speed: 100

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

6.5. Configure Network Interface values

To configure network-interface, go to system->Network-Interface. Configure interface

The table below lists the parameters, to be configured for both the interfaces.

Parameter Name	Teams side network interface	Twilio side Network interface
Name	M00	M10
Host Name	customers.telechat.o-test06161977.com	
IP address	141.146.36.101	155.212.214.102
Netmask	255.255.255.192	255.255.255.0
Gateway	141.146.36.65	155.212.214.1

Please configure network interface M00 as below

Wizards Commands Save Verify

- media-manager
- security
- session-router
- system
 - fraud-protection
 - host-route
 - http-client
 - http-server
 - network-interface**
 - ntp-config
 - phy-interface

Show All

Add Network Interface

Name: M00

Sub Port Id: 0 (Range: 0..4095)

Description:

Hostname: customers.telechat.o-test06161977.cor

IP Address: 141.146.36.68

Pri Utility Addr:

Sec Utility Addr:

OK Back

Similarly, configure network interface M10 as below

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace

Wizards Commands Save Verify

- session-router
- system
 - fraud-protection
 - host-route
 - http-client
 - http-server
 - network-interface**
 - ntp-config
 - phy-interface
 - redundancy-config
 - snmp-community

Show All

Add Network Interface

Name: M10

Sub Port Id: 0 (Range: 0..4095)

Description:

Hostname:

IP Address: 155.212.214.102

Pri Utility Addr:

Sec Utility Addr:

OK Back

6.6. Enable media manager

Media-manager handles the media stack required for SIP sessions on the SBC. Enable the media manager option as below.

In addition to the above config, please set the max and min untrusted signaling values to 1. Go to Media-Manager->Media-Manager

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active. The left sidebar shows a tree view with 'media-manager' selected. The main panel is titled 'Modify Media Manager' and contains the following configuration items:

Parameter	Value	Range
State	<input checked="" type="checkbox"/> enable	
Flow Time Limit	86400	(Range: 0..4294967295)
Initial Guard Timer	300	(Range: 0..4294967295)
Subsq Guard Timer	300	(Range: 0..4294967295)
TCP Flow Time Limit	86400	(Range: 0..4294967295)
TCP Initial Guard Timer	300	(Range: 0..4294967295)
TCP Subsq Guard Timer	300	(Range: 0..4294967295)
Hint Rtcp	<input type="checkbox"/> enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	

Buttons: OK, Delete

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active. The left sidebar shows a tree view with 'media-manager' selected. The main panel is titled 'Modify Media Manager' and contains the following configuration items:

Parameter	Value	Range
Media Policing	<input checked="" type="checkbox"/> enable	
Max Arp Rate	10	(Range: 0..100)
Max Signaling Packets	0	(Range: 0..4294967295)
Max Untrusted Signaling	1	(Range: 0..100)
Min Untrusted Signaling	1	(Range: 0..100)
Tolerance Window	30	(Range: 0..4294967295)
Untrusted Drop Threshold	0	(Range: 0..100)
Trusted Drop Threshold	0	(Range: 0..100)
Acl Monitor Window	30	(Range: 5..3600)
Trap On Demote To Deny	<input type="checkbox"/> enable	

Buttons: OK, Delete

Red arrows point to the 'Max Untrusted Signaling' and 'Min Untrusted Signaling' fields, both set to 1.

6.7. Configure Realms

Navigate to realm-config under media-manager and configure a realm as shown below

The name of the Realm can be any relevant name according to the user convenience.

Use the following table as a configuration example for the three realms used in this configuration:

Config Parameter	Teams Side	Twilio Side
Identifier	Teams	TwilioSipTrunk
Network Interface	M00	M10
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Teams-FQDN	Telechat.o-test06161977.com	
Teams fqdn in uri	<input checked="" type="checkbox"/>	
Sdp inactive only	<input checked="" type="checkbox"/>	
Media Sec policy	sdespolicy	sdespolicy
RTCP mux	<input checked="" type="checkbox"/>	
ice profile	ice	
Codec policy	addCN	OptimizeCodecs
RTCP policy	rtcpGen	
Access Control Trust Level	High	High
Pai-strip	enabled	enabled
Media-policy		

In the below case, Realm name is given as Teams for Teams Side. Please set the Access Control Trust Level as high for this realm

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The user is logged in as 'admin'. The left sidebar shows a tree view of configuration categories: media-manager, codec-policy, media-manager, media-policy, realm-config (selected), steering-pool, security, session-router, system, fraud-protection, and host-route. The main content area is titled 'Add Realm Config' and contains the following fields:

- Identifier: Teams
- Description: (empty text area)
- Addr Prefix: 0.0.0.0
- Network Interfaces: M00:0.4 X
- Media Realm List: (empty text area)
- Mm In Realm: enable

At the bottom of the form are 'OK' and 'Back' buttons. The 'Show All' toggle is also visible in the sidebar.

Wizards Commands

Save Verify Discard Se

- media-manager
 - codec-policy
 - media-manager
 - media-policy
 - realm-config**
 - steering-pool
 - security
 - session-router
 - system
 - fraud-protection
 - host-route
- Show All

Modify Realm Config

Average Rate Limit	<input type="text" value="0"/>	(Range: 0..4294967295)
Access Control Trust Level	<input type="text" value="high"/>	
Invalid Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Maximum Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Untrusted Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Nat Trust Threshold	<input type="text" value="0"/>	(Range: 0..65535)
Max Endpoints Per Nat	<input type="text" value="0"/>	(Range: 0..65535)
Nat Invalid Message Threshold	<input type="text" value="0"/>	(Range: 0..65535)
Wait Time For Invalid Register	<input type="text" value="0"/>	(Range: 0,4..300)
Deny Period	<input type="text" value="30"/>	(Range: 0..4294967295)

OK Back

Similarly, Realm name is given as TwilioSipTrunk for Twilio Elastic SIP Trunking side. Please set the Access Control Trust Level as high for this realm too.

Wizards Commands

Save Verify

- media-manager
 - codec-policy
 - media-manager
 - media-policy
 - realm-config**
 - steering-pool
 - security
 - session-router
 - system
 - fraud-protection
 - host-route
- Show All

Add Realm Config


Identifier	<input type="text" value="TwilioSipTrunk"/>
Description	<input type="text"/>
Addr Prefix	<input type="text" value="0.0.0.0"/>
Network Interfaces	<input type="text" value="M10:0.4"/>
Media Realm List	<input type="text"/>
Mm In Realm	<input checked="" type="checkbox"/> enable

OK Back

Wizards Commands Save Verify

- media-manager
- codec-policy
- media-manager
- media-policy
- realm-config**
- steering-pool
- security
- session-router
- system
- fraud-protection
- hst-route
- Show All

Add Realm Config

Out Translationid	<input type="text"/>	
In Manipulationid	<input type="text"/>	
Out Manipulationid	<input type="text"/>	
Average Rate Limit	<input type="text" value="0"/>	(Range: 0..4294967295)
Access Control Trust Level	<input type="text" value="high"/>	
Invalid Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Maximum Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Untrusted Signal Threshold	<input type="text" value="0"/>	(Range: 0..4294967295)
Nat Trust Threshold	<input type="text" value="0"/>	(Range: 0..65535)
Max Endpoints Per Host	<input type="text"/>	

OK Back

For more information on Access Control Trust Level, please refer to SBC Security guide link given below:

https://docs.oracle.com/en/industries/communications/session-border-controller/8.4.0/security/sbc_scz840_security.pdf

6.8. Enable sip-config

SIP config enables SIP handling in the SBC.
Make sure the home realm-id, registrar-domain and registrar-host are configured.

Also add the options to the sip-config as shown below.
To configure sip-config, Go to Session-Router->sip-config and in options, add the below

- add max-udp-length =0
- inmanip-before-validate

For more info, please refer to SBC security guide given in the above section.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'Sys'. The left sidebar lists various configuration options, with 'sip-config' selected. The main content area is titled 'Modify SIP Config' and contains the following fields:

State	<input checked="" type="checkbox"/> enable
Dialog Transparency	<input checked="" type="checkbox"/> enable
Home Realm ID	Teams
Egress Realm ID	
Nat Mode	None
Registrar Domain	*
Registrar Host	*
Registrar Port	5060 (Range: 0,1025..65535)
Init Timer	500 (Range: 0..4294967295)

Buttons for 'OK' and 'Delete' are located at the bottom of the configuration area.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface for 'Modify SIP Config'. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration options, with 'sip-config' selected. The main content area is titled 'Modify SIP Config' and contains the following fields:

Initial Inv Trans Expire	0 (Range: 0..999999999)
Invite Expire	180 (Range: 0..4294967295)
Session Max Life Limit	0
Enforcement Profile	
Red Max Trans	10000 (Range: 0..50000)
Options	inmanip-before-validate x max-udp-length=0 x
SPL Options	
SIP Message Len	0 (Range: 0..65535)
Enum Sag Match	<input type="checkbox"/> enable

Buttons for 'OK' and 'Delete' are located at the bottom of the configuration area.

6.9. Configuring a certificate for SBC

This section describes how to configure the SBC for both TLS and SRTP communication with Teams and Twilio Elastic SIP Trunking.

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

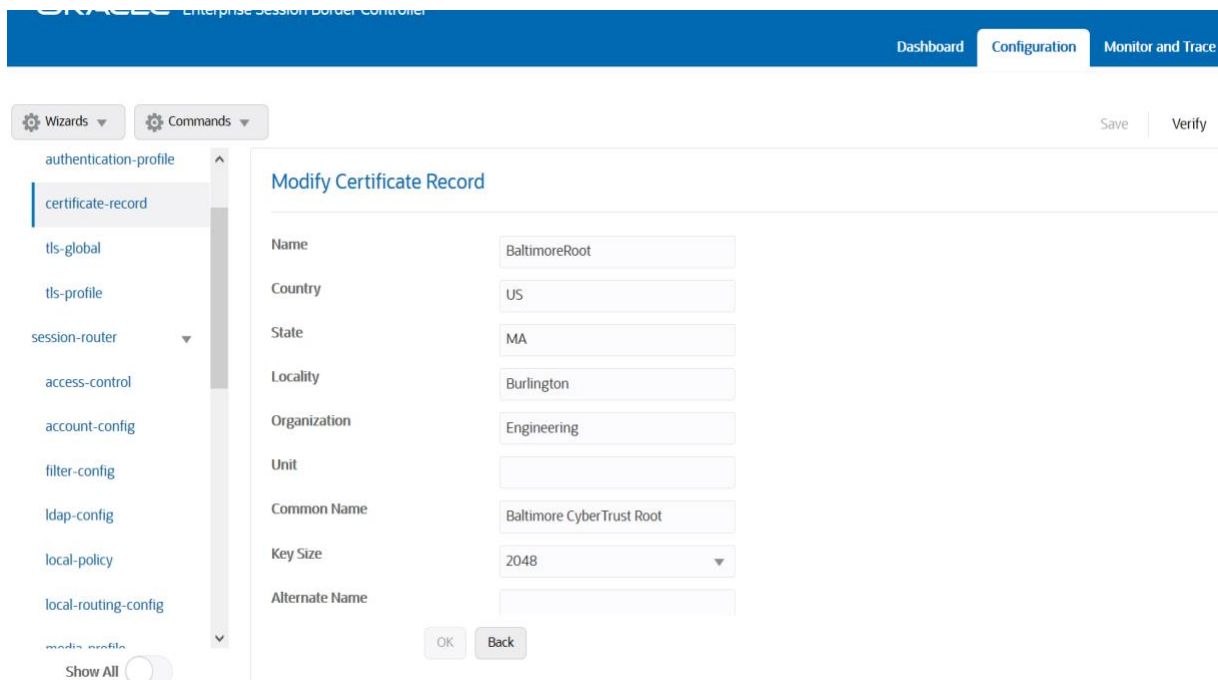
<https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc>

The step below describes how to request a certificate for SBC External interface and configure it based on the example of Baltimore Root certificate. The process includes the following steps:

- 1) Create a certificate-record – “Certificate-record” are configuration elements on Oracle SBC which captures information for a TLS certificate – such as common-name, key-size, key-usage etc.
 - SBC – 1 certificate-record assigned to SBC
 - Root – 1 certificate-record for root cert
- 2) Deploy the SBC and Root certificates on the SBC

Step 1 – Creating the certificate record

Go to security->Certificate Record and configure the SBC entity certificate for SBC as shown below. **We are creating this certificate for Teams side**



The screenshot shows the Oracle SBC configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration categories, with 'certificate-record' selected. The main area displays the 'Modify Certificate Record' form with the following fields:

Name	BaltimoreRoot
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	
Common Name	Baltimore CyberTrust Root
Key Size	2048
Alternate Name	

At the bottom of the form are 'OK' and 'Back' buttons. The interface also includes 'Wizards' and 'Commands' tabs, and 'Save' and 'Verify' buttons in the top right corner.

Wizards Commands Save Verify Discard

media-manager security authentication-profile **certificate-record** tls-global tls-profile session-router system

Modify Certificate Record

Alternate Name

Trusted enable

Key Usage List

Extended Key Usage List

Key Algor

Digest Algor

Ecdsa Key Size

Cert Status Profile List

OK Back

Show All

The table below specifies the parameters required for certificate configuration. Modify the configuration according to the certificates in your environment.

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

Similarly, Twilio Elastic SIP Trunking uses certificates from a CA (Certificate Authority) for establishing the TLS connections from SBC's for SIP traffic, and SRTP for media traffic. It is important that you add the following root certificate to establish TLS connection from the link given below:

<https://www.twilio.com/docs/sip-trunking#rootCA>

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar shows a tree view with 'certificate-record' selected under 'security'. The main content area is titled 'Modify Certificate Record' and contains the following fields:

Name	TwilioRootCACertChain
Country	US
State	MA
Locality	Burlington
Organization	Engineering
Unit	Solutions
Common Name	Chain CA Cert
Key Size	2048
Alternate Name	

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

This screenshot shows the same 'Modify Certificate Record' form with additional fields visible. The 'Key Size' is set to 2048. The 'Trusted' checkbox is checked and labeled 'enable'. The 'Key Usage List' contains 'digitalSignature' and 'keyEncipherment'. The 'Extended Key Usage List' contains 'serverAuth'. The 'Key Algor' is set to 'rsa', 'Digest Algor' is 'sha256', and 'Ecdsa Key Size' is 'p256'. Buttons for 'OK' and 'Back' are at the bottom. A 'Show All' toggle is visible in the bottom left corner.

Key Size	2048
Alternate Name	
Trusted	<input checked="" type="checkbox"/> enable
Key Usage List	digitalSignature X keyEncipherment X
Extended Key Usage List	serverAuth X
Key Algor	rsa
Digest Algor	sha256
Ecdsa Key Size	p256

Step 2 – Generating a certificate signing request

(Only required for the SBC's end entity certificate, and not for root CA certs)

Please note – certificate signing request is only required to be executed for SBC Certificate – not for the root/intermediate certificates.

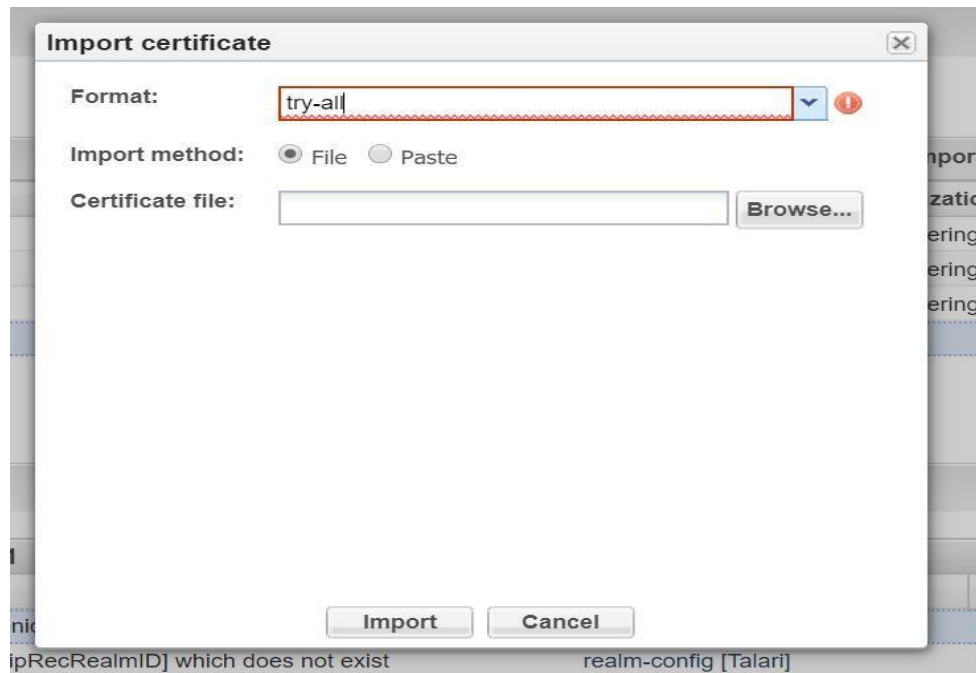
- Select the certificate and generate certificate on clicking the “Generate” command.
- Please copy/paste the text that gets printed on the screen as shown below and upload to your CA server for signature.



- Also, note that a save/activate is required

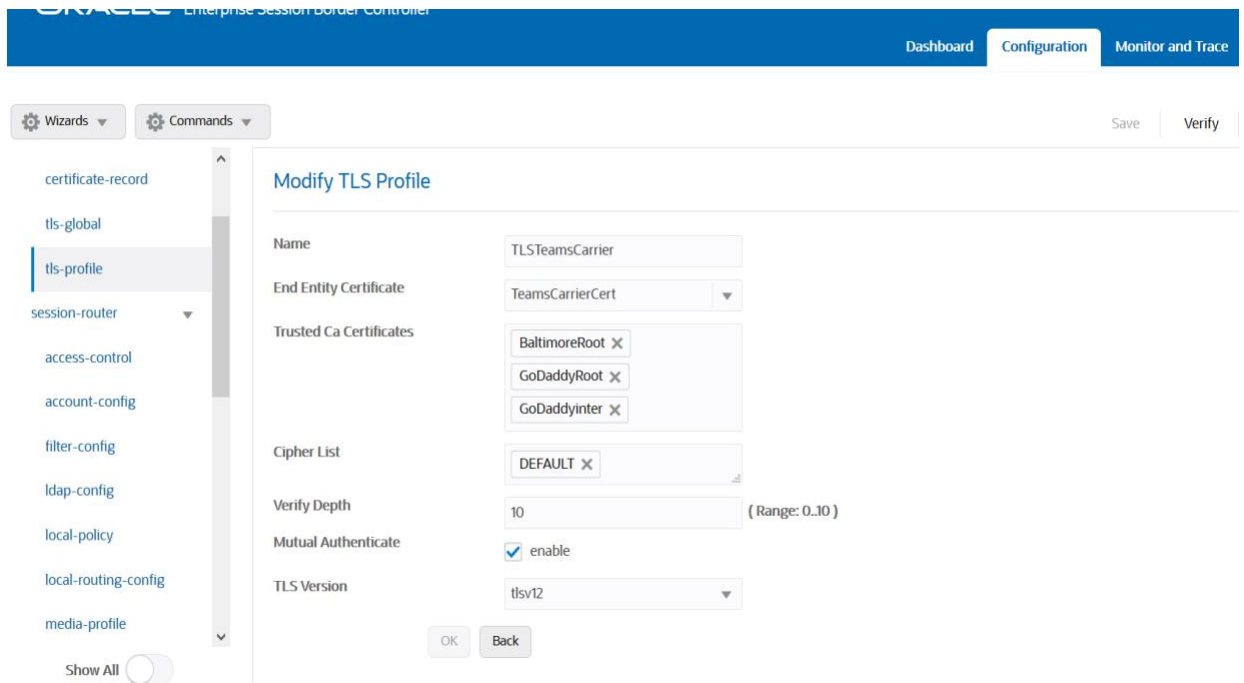
Step 3 – Deploy SBC & root certificates

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

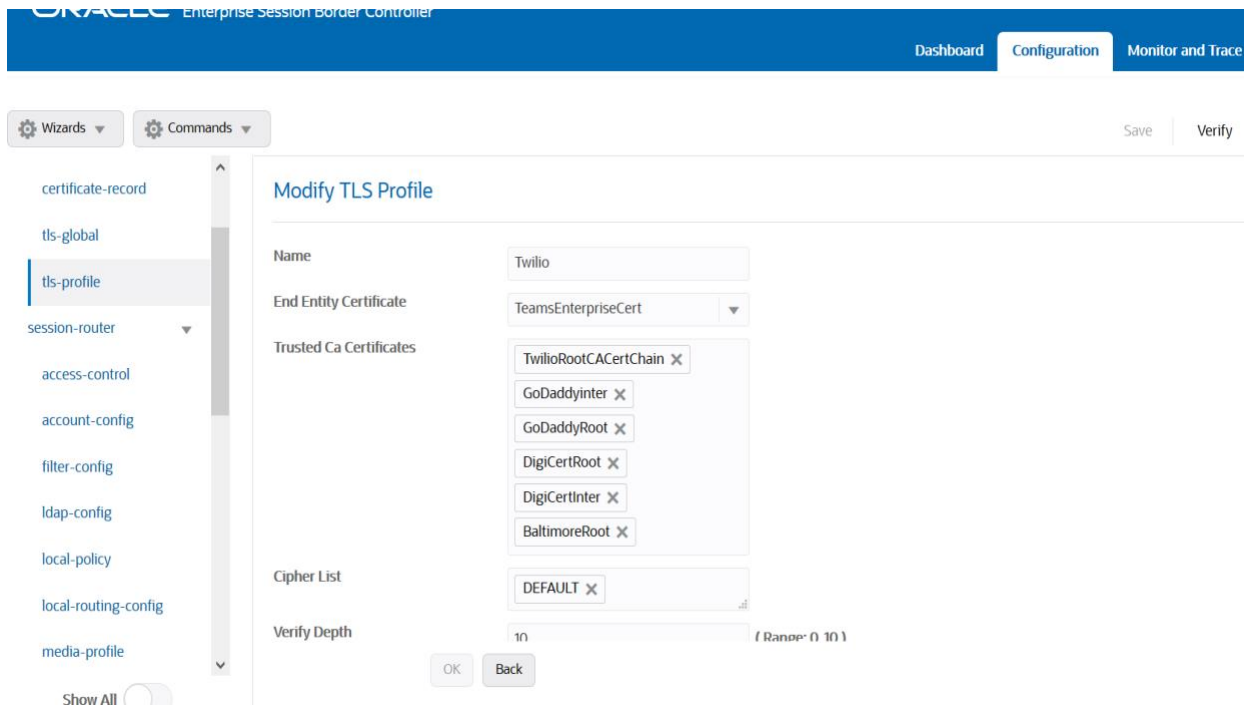


Repeat these steps to import all the root and intermediate CA certificates into the SBC:
At this stage all the required certificates have been imported to the SBC for Teams and the Twilio Elastic SIP Trunk.

A TLS profile configuration on the SBC allows for specific certificates to be assigned. Go to security-> TLS-profile config element and configure the tls-profile as shown below. The below is the TLS profile configured for Teams side.



Similarly, configure the TLS profile shown below for the Twilio Elastic SIP Trunk side:



6.11. Configure SIP Interfaces

Navigate to sip-interface under session-router and configure the sip-interface as shown below.

Please configure the below settings under the sip-interface.

- Tls-profile needs to match the name of the tls-profile previously created
- Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from the particular Session agents added to the SBC.

Below is the sip-interface Configured for Teams side.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration categories, with 'sip-interface' selected. The main content area is titled 'Modify SIP Interface' and contains the following fields:

- State:** A checkbox labeled 'enable' which is checked.
- Realm ID:** A dropdown menu with 'Teams' selected.
- Description:** A large empty text area.
- SIP Ports:** A table with one entry and an 'Add' button above it.

Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
141.146.36.68	5061	TLS	TLSTeamsCarrier	agents-only	

Below the table are 'OK' and 'Back' buttons.

Similarly, Configure sip-interface for the Twilio Elastic SIP Trunk side as below:

The screenshot shows the Oracle Enterprise Session Border Controller (SBC) configuration interface. The page title is "Modify SIP Interface". The left sidebar shows a navigation menu with "sip-interface" selected. The main content area shows configuration fields: "State" is checked "enable", "Realm ID" is "TwilioSipTrunk", and "Description" is empty. Below is a table for "SIP Ports" with one entry: Address 155.212.214.102, Port 5061, Transport Protocol TLS, TLS Profile Twilio, Allow Anonymous agents-only, and Multi Home Addr empty. Buttons for "Add", "OK", and "Back" are visible.

Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.

6.12. Configure session-agent

Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path. Session-agents are config elements which are trusted agents who can send/receive traffic from the SBC with direct access to trusted data path.

Configure the session-agent for Teams with the following parameters.
Go to session-router->Session-Agent.

- hostname to "sip.pstnhub.microsoft.com"
- port 5061
- realm-id – needs to match the realm created for Teams
- transport set to "StaticTLS"
- refer-call-transfer set to enabled
- ping-method – send OPTIONS message to Microsoft to check health
- ping-interval to 30 secs

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The user is logged in as 'admin'. The left sidebar contains a tree view of configuration categories: session-agent (selected), session-group, session-recording-group, session-recording-server, session-translation, sip-config, sip-feature, sip-interface, sip-manipulation, sip-monitoring, sti-server, translation-rules, and system. The main content area is titled 'Modify Session Agent' and contains the following fields:

- Hostname: sip.pstnhub.microsoft.com
- IP Address: (empty)
- Port: 5061 (Range: 0,1025..65535)
- State: enable
- App Protocol: SIP
- App Type: (empty)
- Transport Method: StaticTLS
- Realm ID: Teams
- Egress Realm ID: (empty)
- Description: (empty)

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The user is logged in as 'admin'. The left sidebar contains a tree view of configuration categories: session-agent (selected), session-group, session-recording-group, session-recording-server, session-translation, sip-config, sip-feature, sip-interface, sip-manipulation, sip-monitoring, sti-server, translation-rules, and system. The main content area is titled 'Modify Session Agent' and contains the following fields:

- Proxy Mode: (empty)
- Redirect Action: (empty)
- Loose Routing: enable
- Response Map: (empty)
- Ping Method: OPTIONS
- Ping Interval: 30 (Range: 0..4294967295)
- Ping Send Mode: keep-alive
- Ping All Addresses: enable
- Ping In Service Response Codes: (empty)
- Options: (empty)
- SPL Options: (empty)

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

Follow above steps to create 2 more sessions for:

- sip2.pstnhub.microsoft.com
- sip3.pstnhub.microsoft.com

Note: Please note that all signaling SHOULD only point to sip/sip2/sip3.pstnhub.microsoft.com – no signaling should be sent to sip-all.pstnhub.microsoft.com FQDN. The sip-all.pstnhub.microsoft.com FQDN is only used for longer DNS TTL value

Similarly, configure the session-agents for the Twilio Elastic SIP Trunk as below

- Host name to “oracle.pstn.twilio.com”**, port to 5061
- realm-id – needs to match the realm created for the Twilio Elastic SIP Trunk
- transport set to “staticTLS”

The screenshot shows the Oracle Enterprise Session Border Controller (ESBC) configuration interface. The page title is "ORACLE Enterprise Session Border Controller". The navigation bar includes "Dashboard", "Configuration", and "Monitor and Trace". The left sidebar shows a tree view with "session-agent" selected. The main content area is titled "Modify Session Agent" and contains a form with the following fields:

- Hostname: oracle.pstn.twilio.com
- IP Address: (empty)
- Port: 5061 (Range: 0,1025..65535)
- State: enable
- App Protocol: SIP
- App Type: (empty)
- Transport Method: StaticTLS
- Realm ID: TwilioSipTrunk
- Egress Realm ID: (empty)

At the bottom of the form are "OK" and "Back" buttons.

****NOTE: Connection to Twilio Elastic SIP Trunking is available in multiple geographic edge locations. If you wish to manually connect to a specific geographic edge location that is closest to the location of your communications infrastructure, you may do so by pointing your communications infrastructure to any of the following localized Termination SIP URIs:**

- {example}.pstn.ashburn.twilio.com (North America Virginia)
- {example}.pstn.umatilla.twilio.com (North America Oregon)
- {example}.pstn.dublin.twilio.com (Europe Ireland)
- {example}.pstn.frankfurt.twilio.com (Europe Frankfurt)
- {example}.pstn.singapore.twilio.com (Asia Pacific Singapore)
- {example}.pstn.tokyo.twilio.com (Asia Pacific Tokyo)
- {example}.pstn.sao-paulo.twilio.com (South America São Paulo)
- {example}.pstn.sydney.twilio.com (Asia Pacific Sydney)

[Click here for more information on Twilio Elastic SIP Trunking IP Address](#)

6.13. Configure session-agent group

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

Go to Session-Router->Session-Group. Please configure the following group for Teams Session Agents

The screenshot shows the Oracle Enterprise Session Border Controller interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar lists various configuration categories, with 'session-group' selected. The main content area is titled 'Add Session Group' and contains the following fields:

- Group Name:** TeamsGrp
- Description:** (empty text area)
- State:** enable
- App Protocol:** SIP
- Strategy:** Hunt
- Dest:** sip.pstnhub.microsoft.com, sip2.pstnhub.microsoft.com, sip3.pstnhub.microsoft.com
- Trunk Group:** (empty field)

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

6.14. Configure local-policy

Local policy config allows for the SBC to route calls from one end of the network to the other based on routing criteria. To configure local-policy, go to Session-Router->local-policy.

To route the calls from Teams side to Twilio side, Use the below local -policy

The screenshot shows the Oracle Enterprise Session Border Controller interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar lists various configuration categories, with 'local-policy' selected. The main content area is titled 'Modify Local Policy' and contains the following fields:

- From Address:** *
- To Address:** *
- Source Realm:** Teams
- Description:** (empty text area)
- State:** enable

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Wizards'. The left sidebar lists various configuration options, with 'local-policy' selected. The main content area is titled 'Modify Local Policy' and contains the following fields:

- Description:** A large empty text area.
- State:** A checkbox labeled 'enable' which is checked.
- Policy Priority:** A dropdown menu currently set to 'none'.
- Policy Attributes:** A table with an 'Add' button above it. The table has the following columns: Next Hop, Realm, Action, Terminate Recursion, Cost, State, App Protocol, Lookup, and Next Key. One row is visible with the following values:

Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
oracle.pstn.twilio.com	TwilioSipTrunk	none	disabled	0	enabled		single	

Buttons for 'Save', 'Verify', and 'Discard' are located at the top right. 'OK' and 'Back' buttons are at the bottom of the form.

To route the calls from the Twilio Elastic SIP Trunk side to Teams side, Use the below local –policy

This screenshot shows the 'Modify Local Policy' configuration page with specific routing parameters. The top navigation bar and left sidebar are identical to the previous screenshot. The main content area is titled 'Modify Local Policy' and contains the following fields:

- From Address:** A text input field with a '*' and an 'x' icon.
- To Address:** A text input field with a '*' and an 'x' icon.
- Source Realm:** A dropdown menu with 'TwilioSipTrunk' selected and an 'x' icon.
- Description:** A large empty text area.
- State:** A checkbox labeled 'enable' which is checked.
- Policy Priority:** A dropdown menu currently set to 'none'.

Buttons for 'Save' and 'Verify' are at the top right. 'OK' and 'Back' buttons are at the bottom of the form.

Wizards Commands Save Verify Discard

ldap-config local-policy local-routing-config media-profile session-agent session-group session-recording-group session-recording-server session-translation sip-config sip-feature cin interface Show All

Modify Local Policy

Description

State enable

Policy Priority none

Policy Attributes

Add

Next Hop	Realm	Action	Terminate Recursion	Cost	State	App Protocol	Lookup	Next Key
sag:TeamsGrp	Teams	none	disabled	0	enabled		single	

OK Back

6.15. Configure steering-pool

Steering-pool config allows configuration to assign IP address(es), ports & a realm.

Teams side steering pool.

The screenshot shows the ORACLE Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar shows a tree view with 'steering-pool' selected. The main content area is titled 'Add Steering Pool' and contains the following fields:

IP Address	141.146.36.68	
Start Port	20000	(Range: 1..65535)
End Port	39999	(Range: 1..65535)
Realm ID	Teams	▼
Network Interface		▼

At the bottom of the form are 'OK' and 'Back' buttons. A 'Show All' toggle is located at the bottom left of the sidebar.

Twilio side steering pool.

The screenshot shows the ORACLE Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', and 'Monitor and Trace'. The left sidebar shows a tree view with 'steering-pool' selected. The main content area is titled 'Add Steering Pool' and contains the following fields:

IP Address	155.212.214.102	
Start Port	10000	(Range: 1..65535)
End Port	10999	(Range: 1..65535)
Realm ID	TwilioSipTrunk	▼
Network Interface		▼

At the bottom of the form are 'OK' and 'Back' buttons. A 'Show All' toggle is located at the bottom left of the sidebar.

6.16. Configure sip-manipulation

To simplify the ORACLE SBC sip manipulation, from GA Release SCZ830m1p7 contains three additional SBC configuration parameters which are not found in prior releases.

The purpose of these three parameters is to replace the majority of the sip manipulation rules required to be configured in the ORACLE SBC in order to properly interface with Microsoft Teams Direct Routing.

The first two parameters are found under the **realm-config**, and would be enabled in realms facing Microsoft Teams.

They are **Teams FQDN in URI** and **SDP inactive only**.

The detailed description is given below for each config parameter.

Teams FQDN in URI:

When enabled, this parameter takes the FQDN configured under hostname of the network interface, and inserts that into the Contact and FROM headers of Invites generated by the SBC towards Teams. This also adds a new “X-MS-SBC” Header to both Invite and OPTIONS Requests, which takes the place of the User-Agent header currently being added via Sip Manipulation. Lastly, SBC will add a Contact Header to outgoing SIP Options Pings, also containing the FQDN of the SBC listed under the hostname field of the network interface, and with the Contact Header added to OPTION Requests generated by the SBC, Record Route is no longer required.

SDP inactive only:

When enabled on Teams facing realm(s), this will modify the following SDP attributes in both requests and responses to and from Microsoft Teams

Message Type	Match Value	New Value
request	inactive	sendonly
reply	inactive	recvonly
request	sendonly	inactive
reply	recvonly	inactive

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The main content area is titled "Modify Realm Config" and displays the following configuration details:

- Identifier:** Teams
- Description:** Realm Facing Teams Direct Routing
- Addr Prefix:** 0.0.0.0
- Network Interfaces:** M00:0:4
- Media Realm List:** (Empty field)
- Mm In Realm:** enable
- Mm In Network:** enable
- Mm Same Ip:** enable

At the bottom of the configuration area, there are "OK" and "Back" buttons. The left sidebar shows a navigation menu with "realm-config" selected. The top navigation bar includes "Dashboard", "Configuration", "Monitor and Trace", "Widgets", and "Sys".

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The main content area is titled "Modify Realm Config". It contains several configuration fields:

- Media Policy: [Dropdown]
- Media Sec Policy: sdesPolicy [Dropdown]
- RTCP Mux: enable
- Ice Profile: ice [Dropdown]
- Teams Fqdn: customers.telechat.o-test06161977.cor [Text]
- Teams Fqdn In Uri: enable (highlighted with a red arrow)
- SDP Inactive Only: enable (highlighted with a red arrow)
- DTLS Srtp Profile: [Dropdown]
- Srtp Msm Passthrough: enable
- Class Profile: [Dropdown]
- In Translationid: [Dropdown]

At the bottom of the form are "OK" and "Back" buttons. On the left side, there is a navigation menu with "realm-config" selected. At the top right, there are tabs for "Dashboard", "Configuration", "Monitor and Trace", "Widgets", and "System".

The third parameter is found under the **Session agent** configuration element and will be enabled on all three session agents configured for Microsoft Teams. The parameter name is **Ping response**.

Ping Response:

When enabled, the SBC responds with a 200 OK to all Sip Options Pings it receives from trusted agents. This takes the place of the current Sip Manipulation, RepondOptions.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The main content area is titled "Modify Session Agent". It contains several configuration fields:

- Hostname: sip.pstnhub.microsoft.com [Text]
- IP Address: [Text]
- Port: 5061 [Text] (Range: 0,1025..65535)
- State: enable
- App Protocol: SIP [Dropdown]
- App Type: [Dropdown]
- Transport Method: StaticTLS [Dropdown]
- Realm ID: Teams [Dropdown]
- Egress Realm ID: [Dropdown]
- Description: [Text]

At the bottom of the form are "OK" and "Back" buttons. On the left side, there is a navigation menu with "session-agent" selected. At the top right, there are tabs for "Dashboard", "Configuration", "Monitor and Trace", "Widgets", and "System".

Wizards Commands Save Verify Discard Se

inner-config
ldap-config
local-policy
local-routing-config
media-profile
session-agent
session-group
session-recording-group
session-recording-server
session-translation
sip-config
sip-feature
sip-interface

Show All

Modify Session Agent

Show Configuration

Out Translationid

Trust Me enable

Local Response Map

Ping Response enable

In Manipulationid

Out Manipulationid

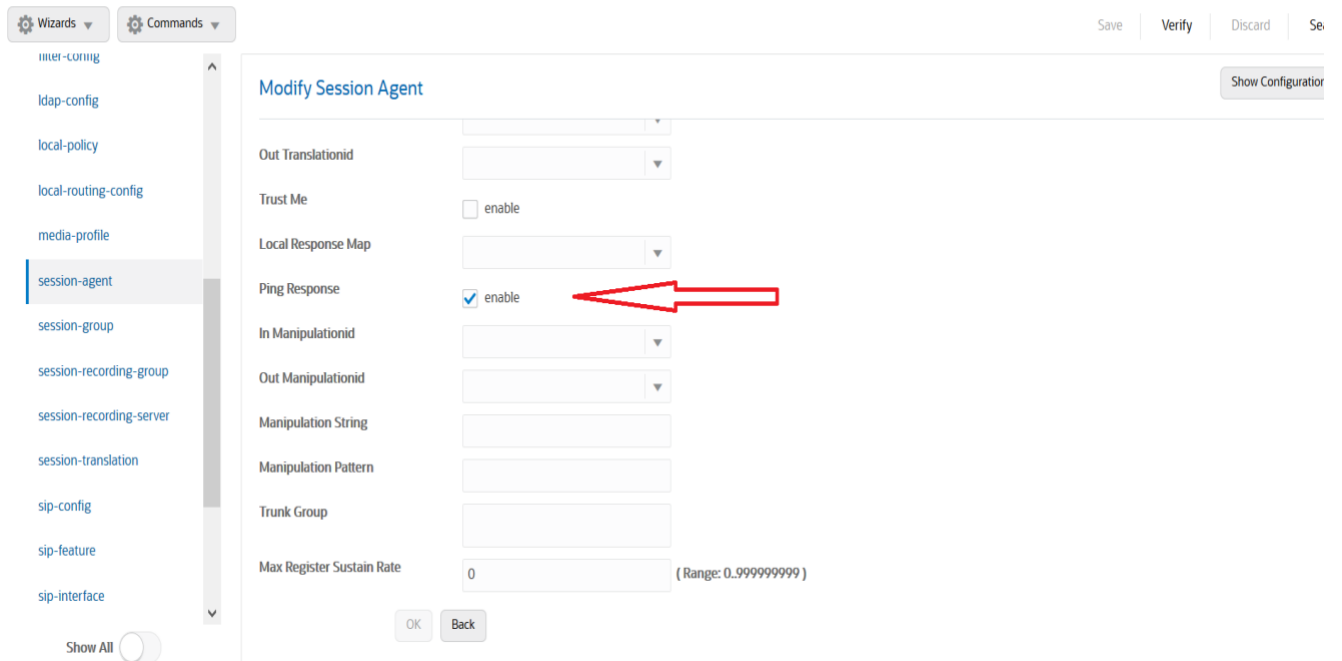
Manipulation String

Manipulation Pattern

Trunk Group

Max Register Sustain Rate 0 (Range: 0..999999999)

OK Back

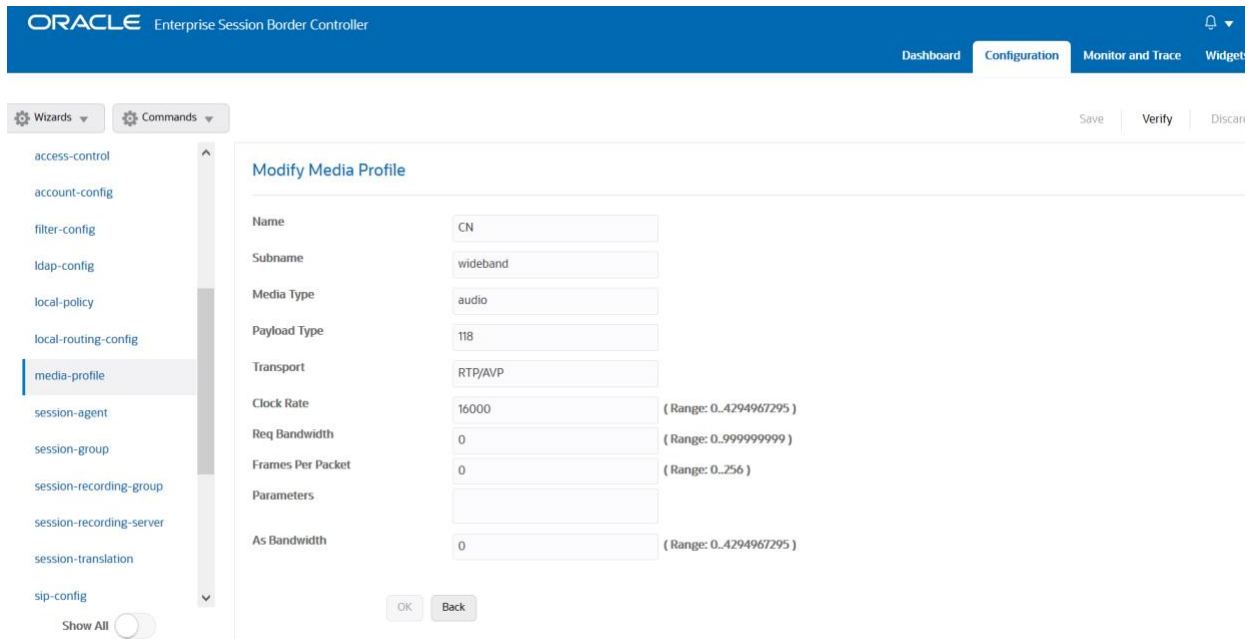


6.17. Configure Media Profile and Codec Policy

The Oracle Session Border Controller (SBC) uses codec policies to describe how to manipulate SDP messages as they cross the SBC. The SBC bases its decision to transcode a call on codec policy configuration and the SDP. Each codec policy specifies a set of rules to be used for determining what codecs are retained, removed, and how they are ordered within SDP.

Note: this is an optional config – configure codec policy only if deemed required

SILK & CN offered by Microsoft teams are using a payload type which is different than usual.
Configure the media-profile as shown below,
Go to Session-Router->Media-profile



Configure media profiles similarly, for silk codec also as given below.

Parameters	SILK-1	SILK-2
Subname	narrowband	wideband
Payload-Type	103	104
Clock-rate	8000	16000

After creating media profile, create codec-policy, addCN, to add comfort noise towards Teams.
Go to media manager ---- codec policy

The screenshot shows the Oracle Enterprise Session Border Controller interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. A 'View history, saved books' link is also present. On the left, there is a sidebar with a tree view containing items like 'media-manager', 'codec-policy', 'media-policy', 'realm-config', 'steering-pool', 'security', 'session-router', 'access-control', 'account-config', 'filter-config', 'ldap-config', and 'local-policy'. The main content area is titled 'Modify Codec Policy' and contains the following fields:

- Name: addCN
- Allow Codecs: * x
- Add Codecs On Egress: CN x
- Order Codecs: (empty)
- Packetization Time: 20
- Force PTime: enable
- Secure Dtmf Cancellation: enable
- Dtmf In Audio: disabled
- Tone Detection: (empty)
- Tone Detect Renegotiate Timer: (empty)

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

Apply this codec policy on the Teams realm

6.18. Configure ice profile

SBC supports ICE-Lite. This configuration is only required to support Teams media-bypass. Configure the following ice profile and apply it on the realm towards Teams.

Go to media-manager->ice-profile. **Note: This config is required only for Media bypass model and its not needed for Non media bypass model.**

The screenshot shows the Oracle Enterprise Session Border Controller interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. A 'View history, saved books' link is also present. On the left, there is a sidebar with a tree view containing items like 'media-manager', 'codec-policy', 'dns-alg-constraints', 'dns-config', 'ice-profile', 'media-manager', 'media-policy', 'msrp-config', 'playback-config', 'realm-config', 'realm-group', 'rtcp-policy', and 'static-flow'. The main content area is titled 'Modify Ice Profile' and contains the following fields:

- Name: ice
- Stun Conn Timeout: 0 (Range: 0..9999)
- Stun Keep Alive Interval: 0 (Range: 0..300)
- Stun Rate Limit: 100 (Range: 0..99999)
- Mode: PROXY

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

6.19. Configure sdes profile

Please go to [Security] Media Security [sdes profile and create the policy as below.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar lists various configuration categories, with 'media-security' expanded to show 'sdes-profile' selected. The main content area is titled 'Add Sdes Profile' and contains the following fields:

- Name: SDES
- Crypto List: AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32
- Srtp Auth: enable
- Srtp Encrypt: enable
- SrTCP Encrypt: enable
- Mki: enable
- Egress Offer Format: same-as-ingress
- Use Ingress Session Params: (empty field)

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

6.20. Configure Media Security Profile

Please go to [Security] Media Security [media Sec policy] and create the policy as below: Create Media Sec policy with name SDES which will have the sdes profile created above. **Assign this media policy to both the Teams and Twilio Realm as they both use TLS/SRTP.**

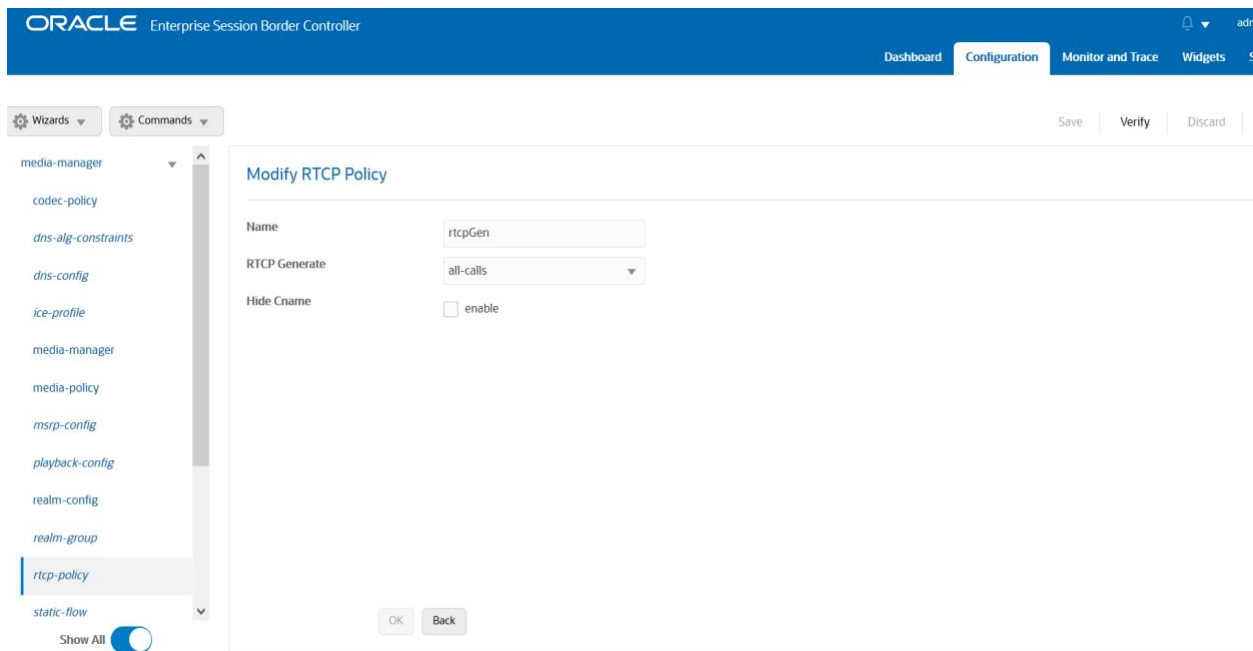
The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The left sidebar lists various configuration categories, with 'media-security' expanded to show 'media-sec-policy' selected. The main content area is titled 'Add Media Sec Policy' and contains the following fields:

- Name: SDES
- Pass Through: enable
- Options: (empty field)
- Inbound**
 - Profile: SDES
 - Mode: srtp
 - Protocol: sdes
 - Hide Egress Media Update: enable
- Outbound**

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

6.21. Configure RTCP Policy and RTCP Mux

The RTCP policy needs to be configured in order to generate RTCP reports towards Teams Go to Media-manager->rtcp-policy to configure rtcp-policy.



Apply this RTCP policy on the Teams realm. Enable rtcp-mux also in the realm. With this, SBC configuration is complete


7. Existing SBC configuration

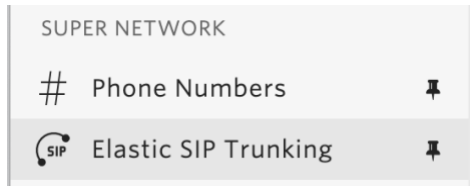
If the SBC being used is an existing SBC with functional configuration, following configuration elements are required:

- [New realm-config](#)
- [Configuring a certificate for SBC Interface](#)
- [TLS-Profile](#)
- [New sip-interface](#)
- [New session-agent](#)
- [New session-agent group](#)
- [New steering-pools](#)
- [New local-policy](#)
- [New sip-manipulation](#)
- [New media-profile and codec-policy](#)
- [ICE profile](#)
- [SDES Profile](#)
- [Media-sec-Policy](#)
- [RTCP Policy and RTP Mux](#)

Please follow the steps mentioned in the above chapters to configure these elements.

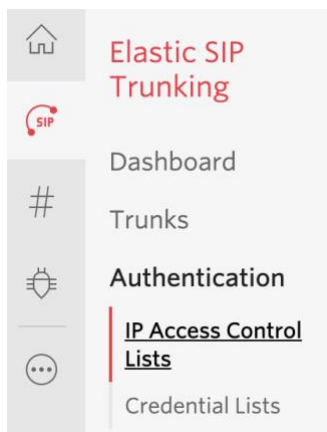
8. Twilio Elastic SIP Trunking Configuration

From your [Twilio Console](#), navigate to the [Elastic SIP Trunking](#) area (or click on the  icon on the left vertical navigation bar).



8.1 Create an IP-ACL rule

Click on [Authentication](#) in the left navigation, and then click on [IP Access Control Lists](#).



Create a new IP-ACL, for example call it "Oracle" and add your SBCs IP addresses.

Oracle

Properties

FRIENDLY NAME

IP-ACL SID ALba3f31843d9fdeaad99752794b45f83e

ASSOCIATED SIP TRUNKS [Oracle](#)

ASSOCIATED SIP DOMAINS —

IP Address Ranges

IP Access Control Lists may have up to 100 IP addresses.

IP ADDRESS RANGE	FRIENDLY NAME	
141.146.36.102 / 32 141.146.36.102 - 141.146.36.102		×
155.212.214.102 / 32 155.212.214.102 - 155.212.214.102	155.212.214.102	×

8.2 Create a new Trunk

For each geographical region desired (e.g., North America, Europe), create a new Elastic SIP Trunk.

Now click on **Trunks** again on the left vertical navigation bar, and create a new Trunk.

Create A New SIP Trunk ×

Name your new SIP Trunk, then configure it in the following steps.

FRIENDLY NAME

Under the **General Settings** you can enable different features as desired.

Features

To learn more about SIP Trunking features, please [see our user documentation](#). [↗](#)

Call Recording ⓘ

Enabled Calls will be recorded.

Call Recording

Record from ringing

Recording Trim

Disabled Silence will not be trimmed from recording

Secure Trunking ⓘ

Enabled TLS must be used to encrypt SIP messages on port 5061, and SRTP must be used to encrypt the media packets. Any non-encrypted calls will be rejected

Call Transfer (SIP REFER) ⓘ

Enabled Twilio will consume an incoming SIP REFER from your communications infrastructure and create an INVITE message to the address in the Refer-To header

Enable PSTN Transfer ⓘ
Allow Call Transfers to the PSTN via your Trunk.

Symmetric RTP ⓘ

Enabled Twilio will detect where the remote RTP stream is coming from and start sending RTP to that destination instead of the one negotiated in the SDP

▶ Additional Features

In the **Termination** section, select a Termination SIP URI.

Termination URI

Configure a SIP Domain Name to uniquely identify your Termination SIP URI for this Trunk. This URI will be used by your communications infrastructure to direct SIP traffic towards Twilio. Be sure to select a localized SIP URI to ensure your traffic takes the lowest latency path. If a localized version isn't selected, then your traffic will be sent to US1. [Learn more about Termination Settings](#) ↗

TERMINATION SIP URI

oracle

.pstn.twilio.com

[Show Localized URIs](#)

Click on "Show localized URI's" and copy and paste this information as you will use this on your SBC to configure your Trunk.





NORTH AMERICA VIRGINIA	oracle.pstn.ashburn.twilio.com
NORTH AMERICA OREGON	oracle.pstn.umatilla.twilio.com
EUROPE DUBLIN	oracle.pstn.dublin.twilio.com
EUROPE FRANKFURT	oracle.pstn.frankfurt.twilio.com
SOUTH AMERICA SAO PAULO	oracle.pstn.sao-paulo.twilio.com
ASIA PACIFIC SINGAPORE	oracle.pstn.singapore.twilio.com
ASIA PACIFIC TOKYO	oracle.pstn.tokyo.twilio.com
ASIA PACIFIC SYDNEY	oracle.pstn.sydney.twilio.com

or

Assign the IP ACL ("Oracle") that you created in the previous step.

Authentication [View all Authentication lists](#)

The following IP ACLs and Credential Lists will be used to authenticate the INVITE for termination calls inbound to Twilio.

IP ACCESS CONTROL LISTS	<input type="text" value="Oracle x"/>  
CREDENTIAL LISTS	<input type="text" value="Click to select a Credential List"/>  

In the **Origination** section, we'll need to add Origination URI's to route traffic towards your Oracle SBC. The recommended practice is to configure a redundant mesh per geographic region (in this context a region is one of North America, Europe, etc). In this case, we configure two Origination URIs, each egressing from a different Twilio Edge.

Click on 'Add New Origination URI', we'll depict the configuration for North America:

Add Origination URL
×

ORIGINATION SIP URI

PRIORITY

Priority ranks the importance of the URI. Values range from 0 to 65535, where the lowest number represents the highest importance.

WEIGHT

Weight is used to determine the share of load when more than one URI has the same priority. Its values range from 1 to 65535. The higher the value, the more load a URI is given.

ENABLED ON

Continue to add the other Origination URIs, so you have the following configuration:

Origination URIs

Configure the IP address (or FQDN) of the network element entry point into your communications infrastructure (e.g. IP-PBX, SBC).

Show more about provisioning for high service availability

ORIGINATION URI	PRIORITY	WEIGHT	ENABLED	
sip:155.212.214.102;edge=ashburn	10	10	✓	×
sip:155.212.214.103;edge=umatilla	20	10	✓	×

In this example, Origination traffic is first routed via Twilio's Ashburn edge, if that fails then we'll route from Twilio's Umatilla edge.

8.3 Associate Phone Numbers on your Trunk

In the **Numbers** section of your Trunk, add the Phone Numbers that you want to associate with each Trunk. Remember to associate the Numbers from a given country in the right Trunk. For example, associate US & Canada Numbers with the North American Trunk and European Numbers with the European Trunk etc.

Numbers

[View my Addresses](#)

Emergency Calling Update: Each number must be associated with an emergency address with matching ISO Country. Please select numbers to enable from one country at a time.

NUMBER	FRIENDLY NAME	COUNTRY	EMERGENCY CALLING STATUS	EMERGENCY ADDRESS	<input type="checkbox"/>
+18507904044	(850) 790-4044	US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	<input type="checkbox"/>
+16892203033	(689) 220-3033	US	Enabled	375 BEALE ST 3rd floor suite, SF, CA, 94105	<input type="checkbox"/>
+17692105055	(769) 210-5055	US	Disabled		<input type="checkbox"/>

9. Verification of Sample Call flows

Once the configuration is complete, we can try making sample calls and can check the signaling path between Twilio Elastic Sip Trunk (PSTN Users) and Teams Users. **For our testing, we used the single network interface for both Teams and Twilio side as below.**

1. Make Call from Teams user to the Twilio Elastic Sip Trunk and check the call flow.
The calls flow from 141.146.36.68 (Teams SIP Interface) to 141.146.36.102 (Twilio Elastic SIP Trunking Interface)
And to Twilio Session Agent and the call reaches the PSTN user after that

ORACLE Enterprise Session Border Controller

Dashboard Configuration Monitor and Trace Widgets System

Sessions

Registrations

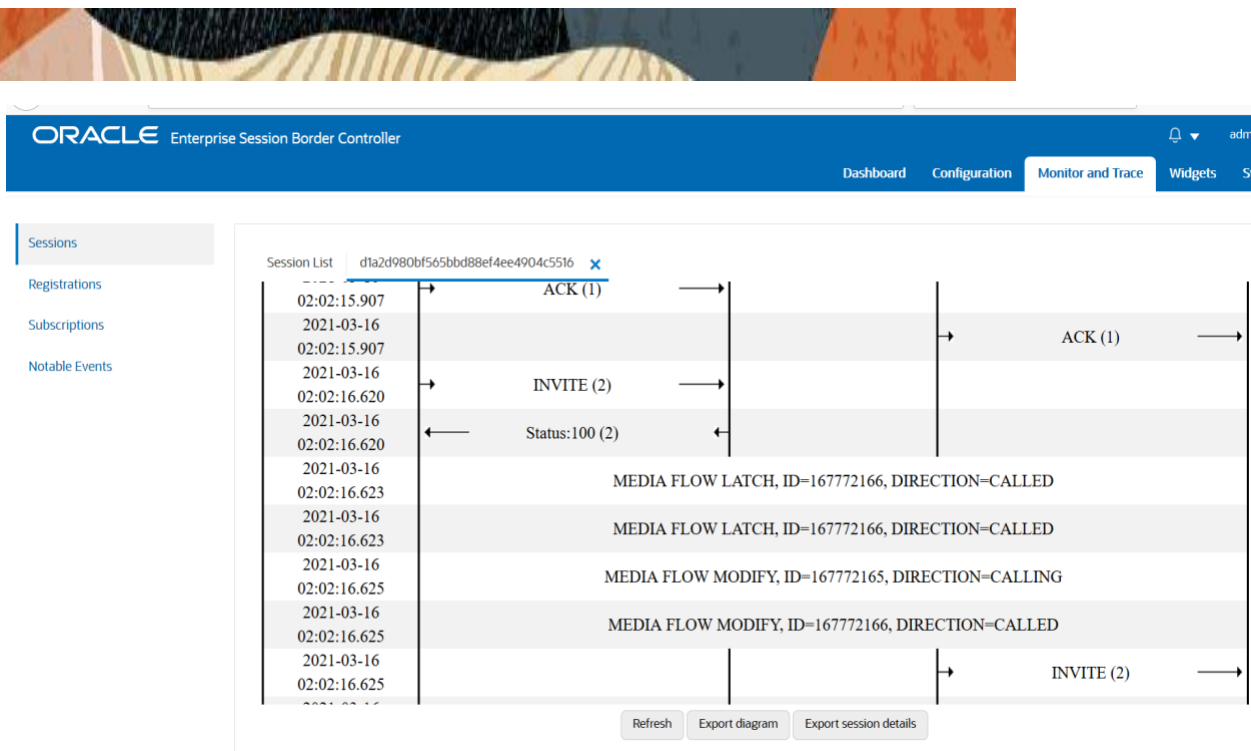
Subscriptions

Notable Events

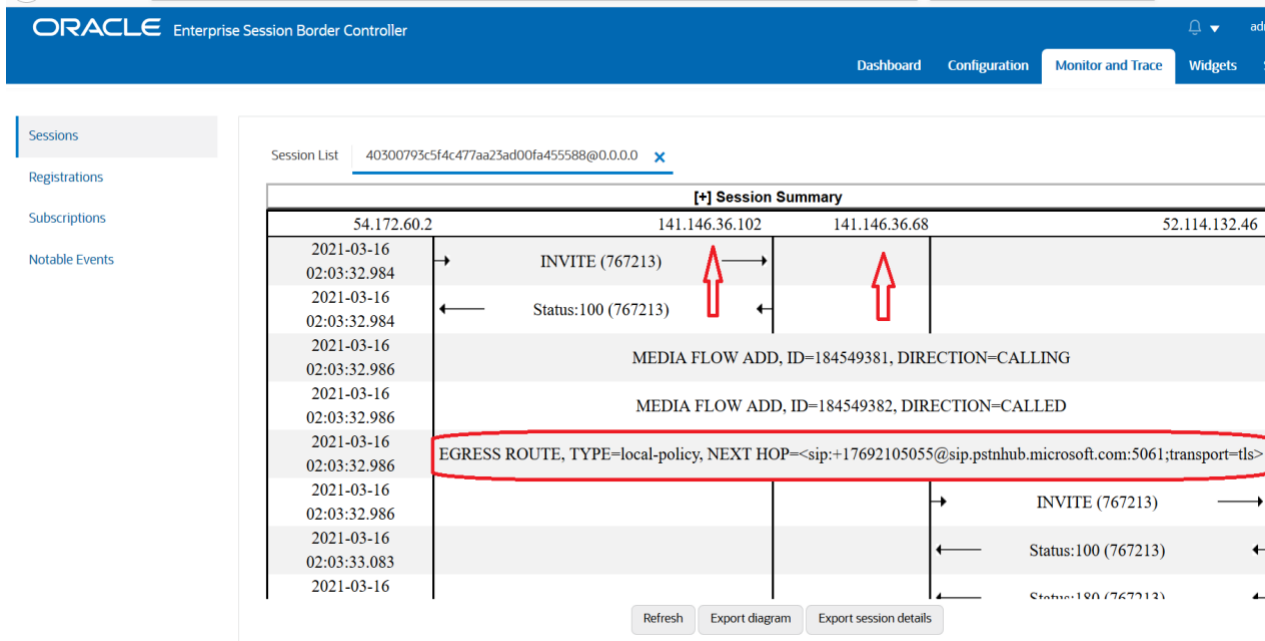
Session List d1a2d980bf565bbd88ef4ee4904c5516

[+] Session Summary			
52.114.148.0	141.146.36.68	141.146.36.102	54.172.60.2
2021-03-16 02:02:08.631	→ INVITE (1)	→	
2021-03-16 02:02:08.631	← Status:100 (1)	←	
MEDIA FLOW ADD, ID=167772165, DIRECTION=CALLING			
MEDIA FLOW ADD, ID=167772166, DIRECTION=CALLED			
EGRESS ROUTE, TYPE=local-policy, NEXT HOP=< sip:+917338391101@oracle.pstn.twilio.com:5061;user=phone; transport=tls>			
2021-03-16 02:02:08.635		→ INVITE (1)	→
2021-03-16 02:02:08.725		← Status:100 (1)	←
2021-03-16		← Status:100 (1)	←

Refresh Export diagram Export session details

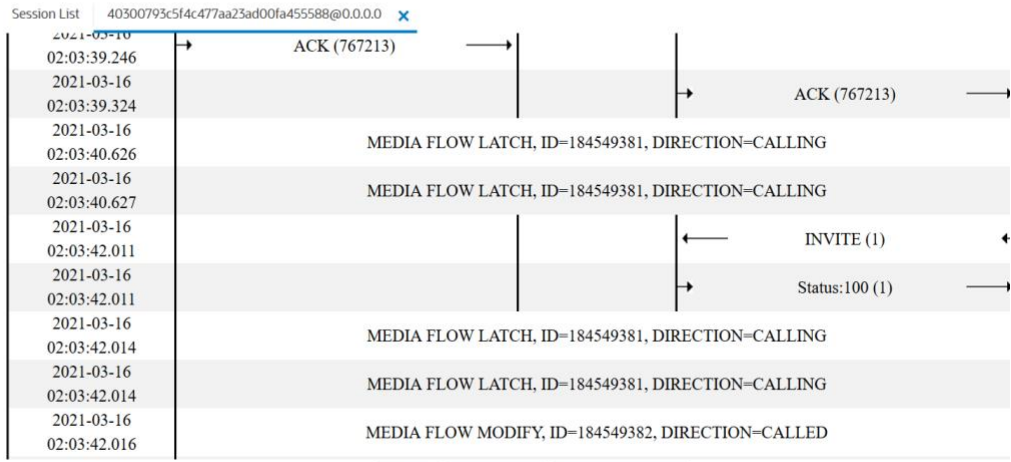


2. Make Call from the Twilio Elastic Sip Trunk to Teams User and check the call flow. The calls flow from 141.146.36.102 (Twilio Elastic SIP Trunking Interface) to 141.146.36.68 (Teams SIP Interface) and to Teams SAGs and the call reaches the Teams user after that.



Sessions

- Registrations
- Subscriptions
- Notable Events



Refresh Export diagram Export session details

Appendix A

Following are the test cases that are executed as part of Teams Direct Routing Enterprise Model with the Twilio Elastic SIP Trunk (PSTN user).

Serial Number	Test Cases Executed	Result
1	Device supports ptime of 20 ms for an inbound call to Twilio Elastic SIP Trunk user	Pass
2	Device sends its own FQDN in the contact header	Pass
3	Twilio Elastic SIP Trunk user accepts call from Teams user where the user's calling line identity is set to anonymous	Pass
4	Teams user places inbound call from Twilio Elastic SIP Trunk user on hold and then resumes	Pass
5	Teams user places outbound call to Twilio Elastic SIP Trunk user on hold and then resumes	Pass
6	Teams user places inbound call from Twilio Elastic SIP Trunk user on hold for over 15/30 minutes and then resumes	Pass

7	Teams user makes outbound call to Twilio Elastic SIP Trunk user and places the call on hold for over 15/30 minutes and then resumes	Pass
8	Inbound Twilio Elastic SIP Trunk call to Teams blind transferred to second Teams User	Pass
9	Outbound Twilio Elastic SIP Trunk call from Teams user blind transferred to second Teams User	Pass
10	Inbound Twilio Elastic SIP Trunk Call to Teams consultatively transferred to Teams User	Pass
11	Outbound Twilio Elastic SIP Trunk call from Teams user consultatively transferred to Teams User	Pass
12	Twilio Elastic SIP Trunk user calls Teams user that simultaneously rings second TEAMS/PSTN user and second user answers	Pass
13	Twilio Elastic SIP Trunk user calls Teams user that is forwarded to second PSTN/TEAMS user	Pass
14	Teams user makes outbound call to Twilio Elastic SIP Trunk user and makes a conference call by adding another Teams user.	Pass
15	Twilio Elastic SIP Trunk user makes outbound call to Teams user and Teams user makes a conference call by adding another Teams user.	Pass
16	Teams user calls an IVR number and navigates through the IVR menu after call connection	Pass
17	Teams user calls into an external conference bridge and pastes a string of conference ID into Teams which is recognized by Device and IVR	Pass
18	Device sends comfort noise packets to Direct Routing interface when Twilio Elastic SIP Trunk user mutes an outbound call	Pass
19	Device sends comfort noise packets to Direct Routing interface when Twilio Elastic SIP Trunk user mutes an inbound call	Pass
20	Teams user mutes inbound call from Twilio Elastic SIP Trunk user and then unmutes	Pass
21	Teams user mutes outbound call made to Twilio Elastic SIP Trunk user and then unmutes	Pass
22	Twilio Elastic SIP Trunk user mutes inbound call from Teams user and then unmutes	Pass
23	Twilio Elastic SIP Trunk user mutes outbound call made to Teams user user and then unmutes	Pass
24	Twilio Elastic SIP Trunk User disconnects outbound call to Teams user before it is answered	Pass

25	Teams user disconnects outbound call to Twilio Elastic SIP Trunk user before it is answered	Pass
26	Twilio Elastic SIP Trunk user disconnects an inbound connected call	Pass
27	Twilio Elastic SIP Trunk User disconnects an outbound connected call	Pass
28	Teams user disconnects an inbound connected call	Pass
29	Teams user disconnects an outbound connected call	Pass
30	Device must indicate support for SRTCP multiplexing by including the a=rtcp-mux attribute in the offer	Pass
31	Device must respond with a=rtcp-mux attribute in the SDP response if the offer contains the same attribute	Pass
32	SBC sends the X-MS-SBC header in Options and the Invite messages towards the Teams user	Pass



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, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

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