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

Technical Application Note
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

<table>
<thead>
<tr>
<th>Version</th>
<th>Description of Changes</th>
<th>Date Revision Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Oracle SBC integration with MS Teams DR and Twilio Elastic SIP Trunking</td>
<td>25th March 2021</td>
</tr>
</tbody>
</table>
# Table of Contents

1. **INTENDED AUDIENCE**  
   - 4

2. **DOCUMENT OVERVIEW**  
   2.1. Twilio Elastic SIP Trunking  
   2.2. Microsoft Teams  
   - 4

3. **INTRODUCTION**  
   3.1. Audience  
   3.2. Requirements  
   3.3. Architecture  
   - 5

4. **CONFIGURE MICROSOFT TEAMS DIRECT ROUTING**  
   4.1. Access Teams Admin center  
   4.2. Configure Online PSTN Gateway  
   4.3. Configure Online PSTN Usage  
   4.4. Configure Online Voice Routes  
   4.5. Configure Online Voice Routing Policy  
   4.6. Assign Voice Routing Policy to Users  
   - 7

5. **CONFIGURING THE SBC**  
   5.1. Validated Oracle SBC version  
   - 12

6. **NEW SBC CONFIGURATION**  
   6.1. Establishing a serial connection to the SBC  
   6.2. Configure SBC using Web GUI  
   6.3. Configure system-config  
   6.4. Configure Physical Interface values  
   6.5. Configure Network Interface values  
   6.6. Enable media manager  
   6.7. Configure Realms  
   6.8. Enable sip-config  
   6.9. Configuring a certificate for SBC  
   6.10. TLS-Profile  
   6.11. Configure SIP Interfaces  
   6.12. Configure session-agent  
   - 12
   
   CLICK HERE FOR MORE INFORMATION ON Twilio Elastic SIP Trunking IP Address  
   6.13. Configure session-agent group  
   6.15. Configure steering-pool  
   6.16. Configure sip-manipulation  
   6.17. Configure Media Profile and Codec Policy  
   6.18. Configure ice profile  
   6.19. Configure sdes profile  
   6.20. Configure Media Security Profile  
   6.21. Configure RTCP Policy and RTCP Mux  
   - 36

7. **EXISTING SBC CONFIGURATION**  
   - 47

8. **Twilio Elastic SIP Trunk Configuration**  
   8.1 Create an IP-ACL rule  
   8.2 Create a new Trunk  
   - 48
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://www.oracle.com/a/otn/docs/vzwithsbcmsftteams-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:

<table>
<thead>
<tr>
<th>Software Used</th>
<th>SBC Version</th>
<th>Teams Client version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 1</td>
<td>8.4.0</td>
<td>1.3.00.28779 (64-bit) (Windows)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>v.1416/1.0.0.2021010802 (Mobile)</td>
</tr>
</tbody>
</table>

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](image)

**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 exampleDomain1 is good for the SBC, but exampleDomain2 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**: On
- **SIP signaling port**: 5061
- **Send SIP options**: On
- **Forward call history**: Off
- **Forward P-Asserted-Identity (PAI) header**: Off
- **Concurrent call capacity**: 500
- **Failover response codes**: 408, 503, 504
- **Failover time (seconds)**: 10
- **Preferred country or region for media traffic**: Auto
- **SBC supports P(D)HDI for emergency calls**: Off
- **Ring phone while trying to find the user**: 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
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 tLcmd...
Starting tServiceHealth...
Starting tCollect...
Starting tAtopd...
Starting tAsctpd...
Starting tMbcd...
Starting tCommMonitor...
Starting tFped...
Starting tAlgd...
Starting tRadd...
Starting tEmsmd...
Starting tSlpd...
Starting tH323d...
Starting tIPTd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tLked...
Starting tTsofd...
Starting tAppWeb...
Starting tauditd...
Starting tauditpusher...
Starting tSmpd...
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...
```

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.

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# 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]: s

Enable the features for the ESBC using the `setup entitlements` command as shown.
Save the changes and reboot the SBC.

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.

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

The Web GUI can be accessed through the url \texttt{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

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


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

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

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


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.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Teams Side (M00)</th>
<th>Twilio Elastic Sip Trunk side (M10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Port</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Operation Mode</td>
<td>Media</td>
<td>Media</td>
</tr>
</tbody>
</table>

Please configure M00 interface as below.
Please configure M10 interface as below

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.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Teams side network interface</th>
<th>Twilio side Network interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>M00</td>
<td>M10</td>
</tr>
<tr>
<td>Host Name</td>
<td>customers.telechat.o-test06161977.com</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>141.146.36.101</td>
<td>155.212.214.102</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.192</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>141.146.36.65</td>
<td>155.212.214.1</td>
</tr>
</tbody>
</table>

Please configure network interface M00 as below
Similarly, configure network interface M10 as below

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

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:

<table>
<thead>
<tr>
<th>Config Parameter</th>
<th>Teams Side</th>
<th>Twilio Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Teams</td>
<td>TwilioSipTrunk</td>
</tr>
<tr>
<td>Network Interface</td>
<td>M00</td>
<td>M10</td>
</tr>
<tr>
<td>Mm in realm</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Teams-FQDN</td>
<td>Telechat.o-test06161977.com</td>
<td></td>
</tr>
<tr>
<td>Teams fqdn in uri</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Sdp inactive only</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Media Sec policy</td>
<td>sdespolicy</td>
<td>sdespolicy</td>
</tr>
<tr>
<td>RTCP mux</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>ice profile</td>
<td>ice</td>
<td></td>
</tr>
<tr>
<td>Codec policy</td>
<td>addCN</td>
<td>OptimizeCodecs</td>
</tr>
<tr>
<td>RTCP policy</td>
<td>rtcpGen</td>
<td></td>
</tr>
<tr>
<td>Access Control Trust Level</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Pai-strip</td>
<td>enabled</td>
<td>enabled</td>
</tr>
<tr>
<td>Media-policy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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


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.

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

<table>
<thead>
<tr>
<th>Config Parameter</th>
<th>Baltimore Root</th>
<th>DigiCert Intermediate</th>
<th>DigiCert Root CA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>Baltimore CyberTrust Root</td>
<td>DigiCert SHA2 Secure Server CA</td>
<td>DigiCert Global Root CA</td>
</tr>
<tr>
<td>Key Size</td>
<td>2048</td>
<td>2048</td>
<td>2048</td>
</tr>
<tr>
<td>Key-Usage-List</td>
<td>digitalSignature keyEncipherment</td>
<td>digitalSignature keyEncipherment</td>
<td>digitalSignature keyEncipherment</td>
</tr>
<tr>
<td>Extended Key Usage List</td>
<td>serverAuth</td>
<td>serverAuth</td>
<td>serverAuth</td>
</tr>
<tr>
<td>Key algol</td>
<td>rsa</td>
<td>rsa</td>
<td>rsa</td>
</tr>
<tr>
<td>Digest-algor</td>
<td>Sha256</td>
<td>Sha256</td>
<td>Sha256</td>
</tr>
</tbody>
</table>
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

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.

![Certificate Signing Request](image)

- 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.

6.10. TLS-Profile
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.

![TLS Profile Configuration](image1)

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

![TLS Profile Configuration](image2)

### 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.

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

**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

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
To route the calls from the Twilio Elastic SIP Trunk side to Teams side, Use the below local –policy
6.15. Configure steering-pool

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

Teams side steering pool.
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.

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Match Value</th>
<th>New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>request</td>
<td>inactive</td>
<td>sendonly</td>
</tr>
<tr>
<td>reply</td>
<td>inactive</td>
<td>recvonly</td>
</tr>
<tr>
<td>request</td>
<td>sendonly</td>
<td>inactive</td>
</tr>
<tr>
<td>reply</td>
<td>recvonly</td>
<td>inactive</td>
</tr>
</tbody>
</table>
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.
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.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>SILK-1</th>
<th>SILK-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subname</td>
<td>narrowband</td>
<td>wideband</td>
</tr>
<tr>
<td>Payload-Type</td>
<td>103</td>
<td>104</td>
</tr>
<tr>
<td>Clock-rate</td>
<td>8000</td>
<td>16000</td>
</tr>
</tbody>
</table>

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

6.19. Configure sdes profile

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

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

<table>
<thead>
<tr>
<th>FRIENDLY NAME</th>
<th>Oracle</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-ACL SID</td>
<td>AL:ba3f33b43c9fdead9975279b45e683e</td>
</tr>
</tbody>
</table>

ASSOCIATED SIP TRUNKS

<table>
<thead>
<tr>
<th>ASSOCIATED SIP DOMAINS</th>
</tr>
</thead>
</table>

ASSOCIATED SIP TRUNKS

IP Address Ranges

<table>
<thead>
<tr>
<th>IP ADDRESS RANGE</th>
<th>FRIENDLY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>141.146.36.102 / 32</td>
<td>141.146.36.102 - 141.146.36.102</td>
</tr>
<tr>
<td>155.212.214.102 / 32</td>
<td>155.212.214.102</td>
</tr>
</tbody>
</table>

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.
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.

  - **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

| Oracle | X | + |

CREDENTIAL LISTS

| 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

<table>
<thead>
<tr>
<th>ORIGINATION SIP URI</th>
<th>sip:155.212.215.102;edge=ashburn</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRIORITY</td>
<td>10</td>
</tr>
<tr>
<td>Priority ranks the importance of the URI. Values range from 0 to 65535, where the lowest number represents the highest importance.</td>
<td></td>
</tr>
<tr>
<td>WEIGHT</td>
<td>10</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>ENABLED</td>
<td>ON</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>ORIGINATION URI</th>
<th>PRIORITY</th>
<th>WEIGHT</th>
<th>ENABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip:155.212.214.102;edge=ashburn</td>
<td>10</td>
<td>10</td>
<td>✔</td>
</tr>
<tr>
<td>sip:155.212.214.103;edge=umatilla</td>
<td>20</td>
<td>10</td>
<td>✔</td>
</tr>
</tbody>
</table>
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**

---

**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.

<table>
<thead>
<tr>
<th>Number</th>
<th>Friendly Name</th>
<th>Country</th>
<th>Emergency Calling Status</th>
<th>Emergency Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>+18507904044</td>
<td>(850) 790-4044</td>
<td>US</td>
<td>Enabled</td>
<td>375 BEALE ST 3rd floor suite, SF, CA, 94105</td>
</tr>
<tr>
<td>+16892203033</td>
<td>(689) 220-3033</td>
<td>US</td>
<td>Enabled</td>
<td>375 BEALE ST 3rd floor suite, SF, CA, 94105</td>
</tr>
<tr>
<td>+17692105055</td>
<td>(769) 210-5055</td>
<td>US</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>
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
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.
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).

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Test Cases Executed</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Device supports ptime of 20 ms for an inbound call to Twilio Elastic SIP Trunk user</td>
<td>Pass</td>
</tr>
<tr>
<td>2</td>
<td>Device sends its own FQDN in the contact header</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>Twilio Elastic SIP Trunk user accepts call from Teams user where the user’s calling line identity is set to anonymous</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>Teams user places inbound call from Twilio Elastic SIP Trunk user on hold and then resumes</td>
<td>Pass</td>
</tr>
<tr>
<td>5</td>
<td>Teams user places outbound call to Twilio Elastic SIP Trunk user on hold and then resumes</td>
<td>Pass</td>
</tr>
<tr>
<td>6</td>
<td>Teams user places inbound call from Twilio Elastic SIP Trunk user on hold for over 15/30 minutes and then resumes</td>
<td>Pass</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Pass</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>7</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Inbound Twilio Elastic SIP Trunk call to Teams blind transferred to second Teams User</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Outbound Twilio Elastic SIP Trunk call from Teams user blind transferred to second Teams User</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Inbound Twilio Elastic SIP Trunk Call to Teams consultatively transferred to Teams User</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Outbound Twilio Elastic SIP Trunk call from Teams user consultatively transferred to Teams User</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Twilio Elastic SIP Trunk user calls Teams user that simultaneously rings second TEAMS/PSTN user and second user answers</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Twilio Elastic SIP Trunk user calls Teams user that is forwarded to second PSTN/TEAMS user</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Teams user makes outbound call to Twilio Elastic SIP Trunk user and makes a conference call by adding another Teams user.</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Twilio Elastic SIP Trunk user makes outbound call to Teams user and Teams user makes a conference call by adding another Teams user.</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Teams user calls an IVR number and navigates through the IVR menu after call connection</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Teams user calls into an external conference bridge and pastes a string of conference ID into Teams which is recognized by Device and IVR</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Device sends comfort noise packets to Direct Routing interface when Twilio Elastic SIP Trunk user mutes an outbound call</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Device sends comfort noise packets to Direct Routing interface when Twilio Elastic SIP Trunk user mutes an inbound call</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Teams user mutes inbound call from Twilio Elastic SIP Trunk user and then unmutes</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Teams user mutes outbound call made to Twilio Elastic SIP Trunk user and then unmutes</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Twilio Elastic SIP Trunk user mutes inbound call from Teams user user and then unmutes</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Twilio Elastic SIP Trunk user mutes outbound call made to Teams user user and then unmutes</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>Twilio Elastic SIP Trunk User disconnects outbound call to Teams user before it is answered</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Teams user disconnects outbound call to Twilio Elastic SIP Trunk user before it is answered</td>
<td>Pass</td>
</tr>
<tr>
<td>26</td>
<td>Twilio Elastic SIP Trunk user disconnects an inbound connected call</td>
<td>Pass</td>
</tr>
<tr>
<td>27</td>
<td>Twilio Elastic SIP Trunk User disconnects an outbound connected call</td>
<td>Pass</td>
</tr>
<tr>
<td>28</td>
<td>Teams user disconnects an inbound connected call</td>
<td>Pass</td>
</tr>
<tr>
<td>29</td>
<td>Teams user disconnects an outbound connected call</td>
<td>Pass</td>
</tr>
<tr>
<td>30</td>
<td>Device must indicate support for SRTCP multiplexing by including the a=rtcp-mux attribute in the offer</td>
<td>Pass</td>
</tr>
<tr>
<td>31</td>
<td>Device must respond with a=rtcp-mux attribute in the SDP response if the offer contains the same attribute</td>
<td>Pass</td>
</tr>
<tr>
<td>32</td>
<td>SBC sends the X-MS-SBC header in Options and the Invite messages towards the Teams user</td>
<td>Pass</td>
</tr>
</tbody>
</table>