Oracle SBC integration with Avaya 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 Avaya and Twilio Elastic SIP Trunking</td>
<td>07th May 2021</td>
</tr>
</tbody>
</table>
Table of Contents

1. INTENDED AUDIENCE .......................................................................................................................... 4
2. DOCUMENT OVERVIEW ......................................................................................................................... 4
   2.1. Twilio Elastic SIP Trunking .............................................................................................................. 4
3. INTRODUCTION ...................................................................................................................................... 5
   3.1. Audience ........................................................................................................................................ 5
   3.2. Requirements .................................................................................................................................. 5
   3.3. Architecture ................................................................................................................................... 6
4. CONFIGURING THE AVAYA AURA SESSION MANAGER 8.1 ............................................................... 7
   4.1. Adding SIP Domain .......................................................................................................................... 7
   4.2. Adding Location ............................................................................................................................... 8
   4.3. Adding the Oracle SBC as a SIP Entity and Configuring an Entity Link ...................................... 8
   4.4. Allowing Unsecured PPM Traffic (Only if TLS is not Used) and PPM Rate Limiting .................. 11
   4.5. Adding Routing Policies ............................................................................................................... 13
   4.6. Adding Dial Patterns ...................................................................................................................... 13
   4.7. Adding Users to Avaya Session Manager ....................................................................................... 15
   4.8. Adding the Oracle SBC as a SIP Entity and Entity Link for Remote Worker ......................... 18
   4.9. Enabling Remote Office ............................................................................................................... 19
5. CONFIGURING THE SBC ......................................................................................................................... 21
   5.1. Validated Oracle SBC Version ........................................................................................................ 21
6. NEW SBC CONFIGURATION .................................................................................................................... 21
   6.1. Establishing a Serial Connection to the SBC ................................................................................ 21
   6.2. Configure SBC Using Web GUI .................................................................................................... 25
   6.3. Configure System-config ............................................................................................................... 27
   6.4. Configure Physical Interface Values ............................................................................................. 28
   6.5. Configure Network Interface Values ............................................................................................. 29
   6.6. Enable Media Manager .................................................................................................................. 31
   6.7. Configure Realms ........................................................................................................................... 32
   6.8. Configuring a Certificate for SBC .................................................................................................. 34
   6.9. TLS-Profile ..................................................................................................................................... 37
   6.10. Configure SIP Interfaces .............................................................................................................. 37
   6.11. Configure Session-Agent ............................................................................................................ 39
   6.12. Configure Local-policy ............................................................................................................... 40
   6.13. Configure Steering-pool ................................................................................................................. 42
   6.14. Configure Ping Response ............................................................................................................. 43
   6.15. Configure Codec Policy ............................................................................................................... 45
   6.16. Configure Sdes Profile .................................................................................................................. 46
   6.17. Configure Media Security Profile ................................................................................................. 46
   6.18. Configure Translation Rules ......................................................................................................... 48
   6.19. Configure Session Translation Rules ............................................................................................ 49
7. SBC CONFIGURATION FOR AVAYA REMOTE WORKER ........................................................................ 51
   7.1. Configure Realms ............................................................................................................................ 51
   7.2. Enable sip-config ............................................................................................................................. 53
   7.3. Enable Media Manager .................................................................................................................... 55
   7.4. Configure SIP Interfaces ................................................................................................................ 56
   7.5. Configure Steering-pool .................................................................................................................. 58
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 Avaya Aura System Manager GUI and Avaya Aura Session Manager.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Twilio Elastic Sip Trunk with Avaya Session Manager. The solution contained within this document has been tested using Oracle Communication SBC with **OS840p4A**.

In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the Avaya Server 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](#).

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 Avaya Session Manager using Oracle Enterprise SBC. There will be steps that require navigating the Avaya server configuration and Oracle SBC GUI interface. Understanding the basic concepts of TCP/UDP, IP/Routing, DNS server and SIP/RTP, TLS/SRTP are also necessary to complete the configuration and for troubleshooting, if necessary.

3.2. Requirements

- Fully functioning Avaya Aura Session Manager 8.1 version
- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version

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>Avaya Aura Session Manager using Avaya Aura System Manager GUI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 1</td>
<td>8.4.0</td>
<td>8.1</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 Avaya Aura Session Manager
- Phase 2 – Configuring the Oracle SBC.
- Phase 3 – Configuring the Twilio Elastic SIP Trunk
4. Configuring the Avaya Aura Session Manager 8.1

Please log in to Avaya Aura System Manager Web GUI with proper login credentials (Username and password). After that, perform the steps below in the given order.

4.1. Adding SIP Domain

Click on Routing under the Elements section
On the Routing tab, select Domains and Click New

- Set domain name as aura.com (Example in this config)
- Set Type as SIP
- click “Commit” to save the configuration
4.2. Adding Location

Click on Routing under the Elements section
On the Routing tab, select Locations and Click New

- Set Name as Phonerlite
- Leave all other fields as default values and click “Commit” to save the configuration.

4.3. Adding the Oracle SBC as a SIP Entity and Configuring an Entity Link

Click on Routing under the Elements section
On the Routing tab, select SIP Entities from the menu on the left side of the screen. Click New to add the SBC as a SIP entity as shown below.

- Set Name: SBC4600Twilio (example in this configuration)
- Set FQDN or IP Address: This is the “inside” IP address of Oracle E-SBC, 10.232.50.78 in this example.
- Set Type: Other
- Set Location: Select Phonerlite from drop down (example in this configuration)
- Set Time Zone: America/New_York (example in this configuration)
- Under Entity Links, Click Add
  - Set SIP Entity 1: Select acme-sm which we will add below after this config
  - Set SIP Entity 2: leave the default value SBC4600Twilio
  - Set Protocol: UDP/TCP/TLS based on our testing
  - Set Ports: Set both Ports to 5060/5061 for testing
  - Set Connection Policy: trusted

Leave all other fields as default values and click “Commit” to save the configuration.
Please configure Avaya Session Manager as another SIP entity in the same way as we added SBC:

- Set Name: acme-sm (example in this configuration)
- Set FQDN or IP Address: This is the SIP IP address of Avaya SM, 10.50.232.127 in this example.
- Set Type: Session Manager
- Leave all other fields as default values and click “Commit” to save the configuration.
4.4. Allowing Unsecured PPM Traffic (only if TLS is not used) and PPM Rate Limiting

Navigate to: Elements->Session Manager->Global Settings

**Set Allow Unsecured PPM Traffic**: checked.
Note that this is only required if you’re using HTTP for the PPM downloads.
If you’re using HTTPS as shown in the E-SBC configuration, leave this unchecked.

Navigate to: Elements->Session Manager->Global Settings Session Manager Administration.
Select the proper Session Manager instance and click Edit

- Scroll down to PPM – Connection Settings
- Set Limited PPM Client Connection: unchecked
- Set PPM Packet Rate Limiting: unchecked
- Leave all other fields as default and Click Commit to save Session Manager Administration page.
4.5. Adding Routing Policies

Navigate to: Routing tab, select Routing Policies and Click New

- Set Name: SMSBCRoute (example in this configuration)
- Set Retries: Default value is 0, can be used as same value
- Select SIP Entity as Destination: Select SBC4600Twilio which was previously configured.
- Click Commit to save the configuration

4.6. Adding Dial Patterns:

Navigate to: Routing tab, select Dial Patterns, again Dial Patterns and Click New

- Set Pattern: 1xxxxx (example in this configuration)
- Set Min: 11 (example in this configuration)
- Set Max: 11 (example in this configuration)
- Select SIP Domain: aura.com which was previously configured.
- Click Commit to save the configuration.

The user can create other dial patterns as per their requirement using the config given above
After configuring the dial patterns, Please add the dial patterns to the routing policies created above.
4.7. Adding Users to Avaya Session Manager.

Navigate to: Users tab, select User Management, select Manage Users and Click New

Under **Identity Tab**, please enter the following

- Set Last Name: User4(example in this configuration)
- Set First Name: Avaya (example in this configuration)
- Set Login Name: 18507904044@aura.com (example in this configuration)

Under **Communication Profile** tab, click Communication Profile Password

- Set Comm-Profile Password: any password (Numbers or alphabets or alphanumeric)
- Re-enter Comm-Profile Password: Type the password again for confirmation.

Navigate to **Communication address tab**, click New

- Set Type: Avaya SIP
- Set Fully Qualified Address: Type the Directory number @domain.com 18507904044@aura.com

Under **Profile tab**, enable **Session Manager Profile** and click it to open it.

- Set Primary Session Manager under SIP Registration: acme-sm (example in this configuration)
- Set Home Location Manager under Call Routing: Phonerlite (example in this configuration)
- Click Commit to save the configuration.
You can repeat the above steps to add more users to the Session Manager.
Below are the configuration which are specific to Avaya Remote Worker configuration.

4.8. Adding the Oracle SBC as a SIP Entity and Entity Link for Remote Worker

Click on Routing under the Elements section
On the Routing tab, select SIP Entities from the menu on the left side of the screen.
Click New to add the SBC as a SIP entity as shown below.

- Set Name: SBC4600 (example in this configuration)
- Set FQDN or IP Address: This is the “inside” IP address of Oracle E-SBC, 10.50.232.77 in this example.
- Set Type: Other
- Set Location: Select Phonerlite from drop down (example in this configuration)
- Set Time Zone: America/New_York (example in this configuration)
- Under Entity Links, Click Add
- Set SIP Entity 1: Select acme-sm which was previously configured
- Set SIP Entity 2: leave the default value SBC4600
- Set Protocol: UDP/TCP/TLS based on our testing
- Set Ports: Set both Ports to 5060/5061 for testing
- Set Connection Policy: trusted

Leave all other fields as default values and click “Commit” to save the configuration.
We can use the configured Avaya Session Manager as another SIP entity for remote worker too.

**4.9. Enabling Remote Office**

Navigate to: Elements->Session Manager->Network Configuration->Remote Access, Click New

- Set Name: Remote_worker for this setup.
- Click New under SIP Proxy Mapping Table. Add the Oracle SBC outside interface IP address for SIP Proxy Public Address, 141.146.36.77 is given in this example.
- Click New under SIP Proxy Private IP Address. Add the Oracle SBC inside interface IP address for SIP Private Address, 10.232.50.77 is given in this example.
- Click Commit to save the configuration.
With this, Avaya Session Manager Configuration is complete.
5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Avaya Session Manager and Twilio Elastic SIP Trunking. In this SBC config, Twilio Elastic SIP trunk side is secure (TLS/SRTP) and Avaya Core Side is unsecure (UDP or TCP/RTP).

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 tAsctpdp...
Starting tLMbcd...
Starting tCommMonitorid...
Starting tFpmd...
Starting tSled...
Starting tRadd...
Starting tHmmd...
Starting tSipd...
Starting tH323d...
Starting tbfdd...
Starting tITPtd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIKed...
Starting tTscfd...
Starting tFcgid...
Starting tauditd...
Starting tauditpusher...
Starting tSmmpd...
Starting tIPMIBd...
Start platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...
Starting aclIMgr...
Password secure mode is enabled
Admin Security is disabled
Password: 
```

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/nnSC2040p3B.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)
```

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 22:30:15

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.

<table>
<thead>
<tr>
<th>Entitlements for Enterprise Session Border Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Session Capacity : 0</td>
</tr>
<tr>
<td>2: Advanced :</td>
</tr>
<tr>
<td>3: Admin Security :</td>
</tr>
<tr>
<td>4: Data Integrity (FIPS 140-2) :</td>
</tr>
<tr>
<td>5: Transcode Codec AMR Capacity : 0</td>
</tr>
<tr>
<td>6: Transcode Codec AMRNS Capacity : 0</td>
</tr>
<tr>
<td>7: Transcode Codec EVRC Capacity : 0</td>
</tr>
<tr>
<td>8: Transcode Codec EVRC3 Capacity : 0</td>
</tr>
<tr>
<td>9: Transcode Codec EVS Capacity : 0</td>
</tr>
<tr>
<td>10: Transcode Codec OPUS Capacity : 0</td>
</tr>
<tr>
<td>11: Transcode Codec SILK Capacity : 0</td>
</tr>
</tbody>
</table>

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.

![CLI Output]

### 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](http://SBC_MGMT_IP).

![Web GUI Login]

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

![System Configuration](image)

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

![Default Gateway Configuration](image)

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 Twilio side and M10 for Avaya side.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Twilio Elastic Sip Trunk side (M00)</th>
<th>Avaya 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

![Configuration Interface](image)

### 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>Twilio side Network interface</th>
<th>Avaya side Network interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>M00</td>
<td>M10</td>
</tr>
<tr>
<td>Host Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>141.146.36.102</td>
<td>10.232.50.78</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>10.232.50.1</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>Twilio Side</th>
<th>Avaya Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>TwilioRealm</td>
<td>AvayaRealm</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>FQDN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Sec policy</td>
<td>sdespolicy</td>
<td>RTP</td>
</tr>
<tr>
<td>Access Control Trust Level</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Codec-Policy</td>
<td>Twiliocodec</td>
<td>AvayaCodec</td>
</tr>
</tbody>
</table>

In the below case, Realm name is given as TwilioRealm for Twilio Elastic SIP Trunking Side. Please set the Access Control Trust Level as high for this realm.
Similarly, Realm name is given as AvayaRealm for Avaya 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. Configuring a certificate for SBC

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

Twilio Elastic SIP Trunking 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. 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

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 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>DigiCert Root CA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>DigiCert Global Root CA</td>
</tr>
<tr>
<td>Key Size</td>
<td>2048</td>
</tr>
<tr>
<td>Key-Usage-List</td>
<td>digitalSignature</td>
</tr>
<tr>
<td></td>
<td>keyEncipherment</td>
</tr>
<tr>
<td>Extended Key Usage List</td>
<td>serverAuth</td>
</tr>
<tr>
<td>Key algor</td>
<td>rsa</td>
</tr>
<tr>
<td>Digest-algor</td>
<td>Sha256</td>
</tr>
</tbody>
</table>

**Step 2 – Deploy SBC & root certificates**

Once certificate record has been created – import the signed certificate to the SBC. Please note – all certificates including root 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 certificates into the SBC:

At this stage all the required certificates have been imported to the SBC for Twilio Elastic SIP Trunk.
6.9. 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 the Twilio Elastic SIP Trunk side:

![TLS Profile Configuration Screenshot]

6.10. 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.

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

- 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.
Similarly, Please Configure sip-interface for the Avaya side as below:

Once sip-interface is configured – the SBC is ready to accept traffic on the allocated IP address.
6.11. 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.

Go to session-router->Session-Agent and Configure the session-agents for the Twilio Elastic SIP Trunk

- 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
Similarly, configure the session-agents for the Avaya Side as below:

![Add Session Agent](image1)

### 6.12. 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 Avaya side to Twilio side, Use the below local –policy

![Modify Local Policy](image2)
To route the calls from the Twilio Elastic SIP Trunk side to Avaya side, use the below local policy:
6.13. Configure steering-pool

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

Avaya side steering pool.
Twilio side steering pool.


To simplify the ORACLE SBC configuration, from GA Release SCZ830m1p7, there is a new parameter introduced under the Session agent configuration element. The parameter name is **Ping response**.

**Ping Response:**

When this parameter is 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.
6.15. Configure 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. **Note: this is an optional config – configure codec policy only if deemed required.** Go to media manager ---- codec policy

Configure the below Codec policy for Avaya Side. **Assign this codec policy to the AvayaRealm.**

![Configure Codec Policy for Avaya Side](image1)

Configure the below Codec policy for Twilio Side, **Assign this codec policy to the TwilioRealm.**

![Configure Codec Policy for Twilio Side](image2)
6.16. Configure sdes profile

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

```
Configure sdes profile
```

6.17. Configure Media Security Profile

Please go to → Security → Media Security → media Sec policy and create the policy as below:

```
Configure Media Security Profile
```

Create Media Sec policy with name SDES which will have the sdes profile created above.

Assign this media policy to Twilio Realm as it use TLS/SRTP.
Similarly, Create Media Sec policy with name RTP to convert srtp to rtp for the Avaya side which will use only TCP/UDP as transport protocol. **Assign this media policy to the Avaya Realm.**
6.18. Configure Translation Rules

The translation rules sub-element is where the actual translation rules are created. Go to Session router → translation-rules and create the below rule.

![Translation Rules Screen 1](image1)

![Translation Rules Screen 2](image2)
6.19. Configure Session Translation Rules

A session translation defines how translation rules are applied to calling and called numbers. Go to Session Router → session-translation and configure the below translation rules.

Add the below translation rule to Avaya side as Avaya rejects call with + sign

Add the below translation rule to Twilio side as PSTN expects call with + sign.
Please add the above session translation rules to Avaya realm as shown below

With this, SBC configuration is complete
7. SBC configuration for Avaya Remote Worker

This section of Avaya Remote Worker configuration is included for Avaya remote endpoints that register through the Oracle SBC to the Avaya Session Manager. This would require additional configuration to be configured on the Oracle SBC along with the SIP trunking config as mentioned in the earlier description of the test bed. To complete the particular testing we have configured Avaya endpoints which will register to Avaya Session Manager through the SBC. SBC will handle the calls based on the registration information present in the cache. Please note that Avaya Remote worker Access side is secured (TLS/SRTP) and Avaya Core side is unsecured (UDP or TCP/RTP).

In order to achieve the requirement we have made below configuration on the Oracle SBC

Access and Core Realm for Avaya Remote worker
Steering Pool associated with the Realm for Avaya Remote worker
Sip-interface associated with the Realm for Avaya Remote worker
(Optional) A local-policy to route the registration requests from this Realm to the SIP Server.

Note -The local-policy element is optional as we can enable the Route to registrar parameter on the sip-interface config to route the requests to the Registrar.
The registrar host and port is configured in the sip-config element on the SBC. The remote endpoint sends register requests from Avaya Access Realm onto the SBC and then SBC registers these endpoints onto the Avaya Core Realm maintaining the registration cache in its database to route inbound calls to these endpoint.

Below are the snippets from the Oracle SBC Web GUI for the Remote worker configuration.

7.1. 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>AvayaAccess Side</th>
<th>Avaya Core Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>AvayapublicRealm</td>
<td>AvayaCoreRealm</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>FQDN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Sec policy</td>
<td>sdespolicy</td>
<td>RTP</td>
</tr>
<tr>
<td>Access Control Trust Level</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Codec-Policy</td>
<td>Twilio codec</td>
<td>AvayaCodec</td>
</tr>
</tbody>
</table>
In the below example, Realm name is given as AvayapublicRealm for Avaya Access Side. Please set the Access Control Trust Level as medium for this realm.
Similarly, Realm name is given as AvayaCoreRealm for Avaya Core side

![Realm configuration screen](image)

### 7.2. 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
- reg-cach-mode=from
7.3. 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 9, which takes care of Access Realm. Go to Media-Manager->Media-Manager
7.4. 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.

Please Configure sip-interface for the for Avaya Access side as below:

- Tls-profile needs to match the name of the tls-profile created earlier.
- Set allow-anonymous to Registered to ensure traffic to this sip-interface only comes from the registered user.
- Set NAT traversal to always for the remote workers to register.
- Enable Registration Caching and Route to Register
Similarly, Please Configure sip-interface for the Avaya Core side as below:

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

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

Avaya Access side steering pool.

![Add Steering Pool](image1)

Avaya Core side steering pool.

![Add Steering Pool](image2)
7.6. Configure local-policy (Optional)

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 Avaya Access side to Avaya Core side and vice versa, Use the below local –policy
8. 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 steering-pools
- New local-policy
- New Codec Policy
- SDES Profile
- Media-sec-Policy
- New Translation Rules
- Session Translation Rules

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

9. 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).
9.1. 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.
9.2. 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.

**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**

<table>
<thead>
<tr>
<th>TERMINATION SIP URI</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracle.pstn.twilio.com</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Region</th>
<th>SIP URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORTH AMERICA VIRGINIA</td>
<td>oracle.pstn.ashburn.twilio.com</td>
</tr>
<tr>
<td>NORTH AMERICA OREGON</td>
<td>oracle.pstn.umatilla.twilio.com</td>
</tr>
<tr>
<td>EUROPE DUBLIN</td>
<td>oracle.pstn.dublin.twilio.com</td>
</tr>
<tr>
<td>EUROPE FRANKFURT</td>
<td>oracle.pstn.frankfurt.twilio.com</td>
</tr>
<tr>
<td>SOUTH AMERICA SAO PAULO</td>
<td>oracle.pstn.sao-paulo.twilio.com</td>
</tr>
<tr>
<td>ASIA PACIFIC SINGAPORE</td>
<td>oracle.pstn.singapore.twilio.com</td>
</tr>
<tr>
<td>ASIA PACIFIC TOKYO</td>
<td>oracle.pstn.tokyo.twilio.com</td>
</tr>
<tr>
<td>ASIA PACIFIC SYDNEY</td>
<td>oracle.pstn.sydney.twilio.com</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>IP ACCESS CONTROL LISTS</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CREDENTIA LISTS</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click to select a Credential List</td>
<td></td>
</tr>
</tbody>
</table>
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](image)

- **ORIGINATION SIP URI**: sip:155.212.215.102;edge=ashburn
- **PRIORITY**: 10
  - Priority ranks the importance of the URI. Values range from 0 to 65535, where the lowest number represents the highest importance.
- **WEIGHT**: 10
  - 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](image)

<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.
### 9.3. 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.

#### 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>+18617996884</td>
<td>(610) 790-4944</td>
<td>US</td>
<td>Enabled</td>
<td>375 BEALE ST 3rd floor suite, SF, CA, 94105</td>
</tr>
<tr>
<td>+16503099853</td>
<td>(650) 230-99853</td>
<td>US</td>
<td>Enabled</td>
<td>375 BEALE ST 3rd floor suite, SF, CA, 94105</td>
</tr>
<tr>
<td>+13122225555</td>
<td>(312) 222-55555</td>
<td>US</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>
10. 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 Avaya Users.

1. Make Call from Avaya user to the Twilio Elastic Sip Trunk and check the call flow. The calls flow from 10.232.50.78 (Avaya 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. When we register Avaya Remote Worker, we can see the registration happening through Oracle SBC to Avaya Session Manager as given below.

3. Make Call from Avaya Remote user to the Twilio Elastic Sip Trunk user and check the call flow. Now, there will be 2 call legs (hair pinned call) as the call reaches Avaya Session Manager first and then reaches Twilio trunk user after that as given below.
4. Make Call from the Twilio Elastic Sip Trunk to Avaya User and check the call flow. The calls flow from 141.146.36.102 (Twilio Elastic Sip Trunking Interface) to 10.232.50.78 (Avaya SIP Interface) and the call reaches the Avaya user after that.
5. Make Call from Twilio Elastic Sip Trunk user to Avaya Remote user and check the call flow.

Now, there will be 2 call legs (hair pinned call) as the call reaches Avaya Session Manager first and then reaches Avaya Remote user after that as given below.
Appendix A

Following are the test cases that are executed between Avaya User with the Twilio Elastic SIP Trunk (PSTN user). Please note that Avaya User here refers both Avaya User inside Enterprise network as well as Avaya Remote worker.

<table>
<thead>
<tr>
<th>Serial Number</th>
<th>Test Cases Executed</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Avaya user disconnects an inbound connected call</td>
<td>Pass</td>
</tr>
<tr>
<td>2</td>
<td>Avaya user disconnects an outbound connected call</td>
<td>Pass</td>
</tr>
<tr>
<td>3</td>
<td>Twilio Elastic SIP Trunk user disconnects an inbound connected call</td>
<td>Pass</td>
</tr>
<tr>
<td>4</td>
<td>Twilio Elastic SIP Trunk User disconnects an outbound connected call</td>
<td>Pass</td>
</tr>
<tr>
<td>5</td>
<td>Avaya user places inbound call from Twilio Elastic SIP Trunk user on hold and then resumes</td>
<td>Pass</td>
</tr>
<tr>
<td>6</td>
<td>Avaya user makes outbound call to Twilio Elastic SIP Trunk user and put that call on hold and then resumes</td>
<td>Pass</td>
</tr>
<tr>
<td>7</td>
<td>Twilio Elastic SIP Trunk user places inbound call from Avaya user on hold and then resumes</td>
<td>Pass</td>
</tr>
<tr>
<td>8</td>
<td>Twilio Elastic SIP Trunk user makes outbound call to Avaya user and put that call on hold and then resumes</td>
<td>Pass</td>
</tr>
<tr>
<td>9</td>
<td>Avaya 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>10</td>
<td>Avaya 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>Pass</td>
</tr>
<tr>
<td>11</td>
<td>Inbound Twilio Elastic SIP Trunk call to Avaya blind transferred to second Avaya/ PSTN User</td>
<td>Pass</td>
</tr>
<tr>
<td>12</td>
<td>Outbound Twilio Elastic SIP Trunk call from Avaya user blind transferred to second Avaya/ PSTN User</td>
<td>Pass</td>
</tr>
<tr>
<td>13</td>
<td>Inbound Twilio Elastic SIP Trunk Call to Avaya consultatively transferred to Avaya/ PSTN User</td>
<td>Pass</td>
</tr>
<tr>
<td>14</td>
<td>Outbound Twilio Elastic SIP Trunk call from Avaya user consultatively transferred to Avaya/ PSTN User</td>
<td>Pass</td>
</tr>
<tr>
<td>15</td>
<td>Avaya user makes outbound call to Twilio Elastic SIP Trunk user and makes a conference call by adding another Avaya/ PSTN user.</td>
<td>Pass</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Status</td>
</tr>
<tr>
<td>---</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>16</td>
<td>Twilio Elastic SIP Trunk user makes outbound call to Avaya user and Avaya user makes a conference call by adding another Avaya/ PSTN user.</td>
<td>Pass</td>
</tr>
<tr>
<td>17</td>
<td>Avaya user mutes inbound call from Twilio Elastic SIP Trunk user and then unmutes</td>
<td>Pass</td>
</tr>
<tr>
<td>18</td>
<td>Avaya user mutes outbound call made to Twilio Elastic SIP Trunk user and then unmutes</td>
<td>Pass</td>
</tr>
<tr>
<td>19</td>
<td>Twilio Elastic SIP Trunk user mutes inbound call from Avaya user and then unmutes</td>
<td>Pass</td>
</tr>
<tr>
<td>20</td>
<td>Twilio Elastic SIP Trunk user mutes outbound call made to Avaya user and then unmutes</td>
<td>Pass</td>
</tr>
<tr>
<td>21</td>
<td>Twilio Elastic SIP Trunk User disconnects outbound call to Avaya user before it is answered</td>
<td>Pass</td>
</tr>
<tr>
<td>22</td>
<td>Avaya user disconnects outbound call to Twilio Elastic SIP Trunk user before it is answered</td>
<td>Pass</td>
</tr>
</tbody>
</table>