Oracle SBC integration with Cisco CUCM 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 Cisco CUCM and Twilio Elastic SIP Trunking</td>
<td>21st May 2021</td>
</tr>
</tbody>
</table>
# Table of Contents

1. INTENDED AUDIENCE ........................................................................................................ 4

2. DOCUMENT OVERVIEW ................................................................................................... 4
   2.1. TWILIO ELASTIC SIP TRUNKING ............................................................................. 4
   2.2. CISCO CALL MANAGER (CISCO CUCM) ............................................................... 4

3. INTRODUCTION .................................................................................................................. 5
   3.1. AUDIENCE ............................................................................................................... 5
   3.2. REQUIREMENTS ....................................................................................................... 5
   3.3. ARCHITECTURE ...................................................................................................... 6

4. CONFIGURING THE CISCO CALL MANAGER (CISCO CUCM) ........................................ 7
   4.1. CONFIGURING A NEW SIP TRUNK ......................................................................... 7
   4.2. CONFIGURE A NEW ROUTE PATTERN ................................................................... 9
   4.3. END USER CONFIGURATION ................................................................................ 11
   4.4. ADDING SIP PHONE IN CUCM ............................................................................... 12
   4.5. ASSOCIATING END USER TO PHONE .................................................................. 14

5. CONFIGURING THE SBC .................................................................................................... 15
   5.1. VALIDATED ORACLE SBC VERSION .................................................................... 15

6. NEW SBC CONFIGURATION ................................................................................................ 15
   6.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC ......................................... 15
   6.2. CONFIGURE SBC USING WEB GUI ....................................................................... 19
   6.3. CONFIGURE SYSTEM-CONFIG ............................................................................. 21
   6.4. CONFIGURE PHYSICAL INTERFACE VALUES ....................................................... 22
   6.5. CONFIGURE NETWORK INTERFACE VALUES ..................................................... 23
   6.6. ENABLE MEDIA MANAGER ................................................................................... 25
   6.7. CONFIGURE REALMS ........................................................................................... 26
   6.8. CONFIGURING A CERTIFICATE FOR SBC ............................................................. 28
   6.9. TLS-PROFILE ......................................................................................................... 31
   6.10. CONFIGURE SIP INTERFACES ............................................................................. 31
   6.11. CONFIGURE SESSION-AGENT ............................................................................. 33
   6.12. CONFIGURE LOCAL-POLICY ............................................................................... 35
   6.13. CONFIGURE STEERING-POOL ............................................................................ 37
   6.14. CONFIGURE PING RESPONSE ........................................................................... 38
   6.15. SBC Config FOR CISCO OFFER LESS INVITE ...................................................... 39
   6.16. CONFIGURE SDES PROFILE ............................................................................... 41
   6.17. CONFIGURE MEDIA SECURITY PROFILE ............................................................ 41
   6.18. CONFIGURE TRANSLATION RULES ................................................................... 43
   6.19. CONFIGURE SESSION TRANSLATION RULES ...................................................... 44

7. SBC CONFIGURATION FOR CISCO REMOTE WORKER .................................................... 46
   7.1. CONFIGURE REALMS ........................................................................................... 46
   7.2. ENABLE SIP-CONFIG ............................................................................................. 48
   7.3. ENABLE MEDIA MANAGER ................................................................................... 50
   7.4. CONFIGURE SIP INTERFACES ............................................................................. 51
   7.5. CONFIGURE STEERING-POOL ............................................................................. 53
   7.6. CONFIGURE LOCAL-POLICY (OPTIONAL) ............................................................ 54

8. EXISTING SBC CONFIGURATION ..................................................................................... 55

9. TWILIO ELASTIC SIP TRUNKING CONFIGURATION ......................................................... 55

3 | Page
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 Cisco Call Manager (Cisco CUCM).

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle SBC to interwork between Twilio Elastic SIP Trunk with on premises Cisco CUCM. The solution contained within this document has been tested using Oracle Communication SBC with OS840p4A.

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. Cisco Call Manager (Cisco CUCM)

Cisco Unified Call Manager provides industry-leading reliability, security, scalability, efficiency, and enterprise call and session management and is the core call control application of the collaboration portfolio.

It should be noted that while this application note focuses on the optimal configurations for the Oracle SBC in an enterprise Cisco CUCM 11.5 environment, the same SBC configuration model can also be used for other enterprise applications with a few tweaks to the configuration for required features.

In addition, it should be noted that the SBC configuration provided in this guide focuses strictly on the Cisco CUCM Server associated 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.

10. VERIFICATION OF SAMPLE CALL FLOWS ........................................................................... 61
APPENDIX A .......................................................................................................................... 65
For additional information on CUCM 11.5, please visit


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 Cisco CUCM 11.5 version using Oracle Enterprise SBC. There will be steps that require navigating the CUCM 11.5 server 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

- Fully functioning Cisco CUCM 11.5
- 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>Cisco CUCM Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 1</td>
<td>8.4.0</td>
<td>11.5</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 Cisco Unified Call Manager v11.5 for Oracle SBC.
- Phase 2 – Configuring the Oracle SBC.
- Phase 3 – Configuring the Twilio Elastic SIP Trunk
4. Configuring the Cisco Call Manager (Cisco CUCM)

Please login to Cisco CUCM admin web GUI with proper login credentials (Username and password). After that, perform the steps below in the given order.

![Cisco Unified CM Administration](image)

4.1. Configuring a new SIP Trunk

01) Go to Device ----- Trunk ----- Add New
02) Select Trunk Type – SIP Trunk and then Click Next
03) In the Device Name field, enter the SIP Trunk name and optionally provide a description.
04) In the Device Pool drop-down list, select a device pool id created already else select Default
05) Enter the Destination Address and Destination Port of the SBC under SIP Information.
06) Select appropriate SIP profile and SIP trunk security profile from the dropdown menu.
07) Click Save
Trunk Configuration

**Status**
- Status: Ready

**Trunk Information**
- Trunk Type: SIP Trunk
- Device Protocol: SIP
- Trunk Service Type: None (Default)

---

**Product:**
- Device Name
- Description
- Device Post
- Common Device Configuration
- Call Classification
- Media Resource Group List
- Location
- AAA Group
- Tunnelled Protocol
- QSIG Variant
- ASM 1 ROSE OID Encoding
- Packet Capture Mode
- Packet Capture Duration

- Media Termination Point Required
- Retry Video Call as Audio
4.2. Configure a new Route Pattern

01) Go to Call Routing ------ Route/Hunt ------ Route Pattern and click Add New
02) Enter a Route Pattern according to the network requirements and calling plan.
03) From the Gateway/Route List drop-down list, select the created SIP Trunk device name.
04) Click Save. We can create other route patterns in the same way as shown below.
The route patterns that has been created is shown below:

![Cisco Unified CM Administration](image1)

The created SIP trunk associated with the route pattern is shown below:
4.3. End User Configuration

01) Go to User Management ---- End User and click Add New
02) Enter in your User ID, password, pin, and Last Name
03) You must also enter in a password in the Digest Credentials and Confirm.
04) Click Save (remember the User ID and Password and DN of the device)
4.4. Adding SIP Phone in CUCM

01) Go to Device ---- Phone and click Add New
02) Select Third Party Sip Device (Basic) and click Next
03) Enter in a 12 digit MAC address (any dummy MAC address)
04) Enter the pertinent information for the SIP DEVICE settings – it should mostly be configured the same as
   a standard phone on your system except for the following settings
      a) in the owner user ID field select the user you created above
      b) in the Device Security Profile field select the security profile you created above
      c) in the Digest User field select the user you created above
05) Click Save.
06) Configure the line settings for the SIP device – the line settings should match the line settings of your standard user’s Cisco IP phones
   There are no special attributes that we need to worry about on the line configuration.
4.5. Associating End User to Phone

01) Go to User Management ----- End Users and search for the sip user you created above, once you find it, click on it

02) Scroll down to Device Association and click on the Device Association button

03) Locate and select the sip device you created above

04) Check the checkbox next to this device and click Save Selected/Changes

05) Click Go next to the Back to User related link near the upper right-hand corner

06) Click Save one more time on the End User Configuration screen.

With these steps, the CUCM configuration is complete.
5. Configuring the SBC

This chapter provides step-by-step guidance on how to configure Oracle SBC for Cisco Call Manager (Cisco CUCM) and Twilio Elastic SIP Trunking. In this SBC config, Twilio Elastic SIP trunk side is secure (TLS/SRTP) and Cisco 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 tTcpd...
Starting tAscpd...
Starting tLBcd...
Starting tCommMonitor...
Starting tPfpcd...
Starting tAlg...
Starting tRadd...
Starting tBmld...
Starting tSipd...
Starting tH323d...
Starting tBfdd...
Starting tIPTd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tTscfd...
Starting tFcgid...
Starting tAudtd...
Starting tAuditpusher...
Starting tSmppd...
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: [redacted]
```

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.

```
NN3900-101# conf t
NN3900-101(configure)# bootparam
,'.' - clear field; '-' - go to previous field; q - quit

Boot File : /boot/nnSCZ840p4.bz
IP Address : 10.138.194.136
VLAN : 0
Netmask : 255.255.255.192
Gateway : 10.138.194.129
IPv6 Address :
IPv6 Gateway :
Host IP :
FTP username :
FTP password :
Flags : 0x000000010
Target Name : NN3900-101
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.
```

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

```
NN3900-101# setup product

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

Last Modified 2020-07-21 04:51:24

  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.

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.

```
NN3900-101(http-server)# show http-server
  name webServerInstance
  state enabled
  realm
  ip-address
  http-state enabled
  http-port 80
  https-state disabled
  https-port 443
  http-interface-list GUI
  http-file-upload-size 0
  tls-profile
  auth-profile
  last-modified-by 0
  last-modified-date 2020-10-06 00:28:26
```

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>`.

![Web GUI Screenshot]

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 M10 for Twilio side and M11 for Cisco side.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Twilio Elastic Sip Trunk side (M10)</th>
<th>Cisco side (M11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>1</td>
<td>1</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 M10 interface as below.
Please configure M11 interface as below

![Network Interface Configuration](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>Cisco side Network interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>M10</td>
<td>M11</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 M10 as below

Similarly, configure network interface M11 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 two realms used in this configuration:

<table>
<thead>
<tr>
<th>Config Parameter</th>
<th>Twilio Side</th>
<th>Cisco Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>TwilioRealm</td>
<td>CUCMRealm</td>
</tr>
<tr>
<td>Network Interface</td>
<td>M10</td>
<td>M11</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>
</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 CUCMRealm for Cisco 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

![Modify Certificate Record Screen](image1)

![Modify Certificate Record Screen](image2)
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 algorth</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](image)

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 Cisco 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 Cisco Side as below:

- Host name to FQDN of CUCM which is “CUCM-Cisco.pe.oracle.com” in our example. **We can also give Cisco CUCM IP address if there is no host name configured.**
- The same FQDN value should be configured in Cisco CUCM under System --- Enterprise Parameter ----Cluster FQDN.
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 Cisco side to Twilio side, use the below local –policy:

![Configuration interface screenshot](image1)

![Configuration interface screenshot](image2)
To route the calls from the Twilio Elastic SIP Trunk side to Cisco side, Use the below local –policy

![Oracle Enterprise Session Border Controller](image1)

![Oracle Enterprise Session Border Controller](image2)
6.13. Configure steering-pool

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

Cisco 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. SBC config for Cisco Offer less INVITE

When CUCM sends INVITE without SDP towards SBC and in that case, SBC needs to send out INVITE with SDP towards Twilio Elastic SIP trunk and vice versa. To do that, please set the parameter "Add SDP Invite" as both under Twilio sip interface as highlighted below. When this option is enabled, codecs have to be configured under the parameter "Add SDP profiles". The configured codecs is also shown below.

Note: this is an optional config – configure this only if CUCM sends offer less INVITE towards SBC.
6.16. Configure sdes profile

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

![Add Sdes Profile](image1)

6.17. 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 Twilio Realm as it use TLS/SRTP.

![Add Media Sec Policy](image2)
Similarly, Create Media Sec policy with name RTP to convert srtp to rtp for the Cisco side which will use only TCP/UDP as transport protocol. **Assign this media policy to the Cisco Realm.**
6.18. Configure Translation Rules

The translation rules sub-element is where the actual translation rules are created. Go to Session router \( \rightarrow \) translation-rules and create the below rule.
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 Cisco side.

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

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

This section of Cisco Remote Worker configuration is included for Cisco remote endpoints that register through the Oracle SBC to the Cisco Call Manager (Cisco CUCM). 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 Cisco endpoints which will register to Cisco CUCM through the SBC. SBC will handle the calls based on the registration information present in the cache. Please note that Cisco Remote worker Access side is secured (TLS/SRTP) and Cisco 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 Cisco Remote worker
Steering Pool associated with the Realm for Cisco Remote worker
Sip-interface associated with the Realm for Cisco 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 Cisco Access Realm onto the SBC and then SBC registers these endpoints onto the Cisco 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 two realms used in this configuration:

<table>
<thead>
<tr>
<th>Config Parameter</th>
<th>Cisco Access Side</th>
<th>Cisco Core Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>CUCMpublicRealm</td>
<td>CUCMCoreRealm</td>
</tr>
<tr>
<td>Network Interface</td>
<td>M10</td>
<td>M11</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>
</tbody>
</table>
In the below example, Realm name is given as CUCMPublicRealm for Cisco Access Side. Please set the Access Control Trust Level as medium for this realm.
Similarly, Realm name is given as CUCMCoreRealm for Cisco Core side

![Screenshot of Oracle Enterprise Session Border Controller](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 Cisco 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 Cisco 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.

Cisco Access side steering pool.

![Cisco Access side steering pool](image1)

Cisco Core side steering pool.

![Cisco Core side 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 Cisco Access side to Cisco Core side and vice versa, Use the below local –policy
Cisco Offer less INVITE can happen in the Remote worker scenarios too. In that case, please set the parameter *Add SDP Invite* as both and *Add SDP profiles* under [Cisco Access side sip-interface](#). The configuration is similar to what we have done in [Sec 6.15](#).

## 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
- 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](#) 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.
  - **Call Recording**
    - **Record from ringing**

**Recording Trim**

- **Disabled**
  - Silence will not be trimmed from recording

**Secure Trunking**

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

**Call Transfer (SIP REFER)**

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

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

**Symmetric RTP**

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

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

**Termination URI**

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

<table>
<thead>
<tr>
<th>TERMINATION SIP URI</th>
<th>oracle.pstn.twilio.com</th>
</tr>
</thead>
</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>NORTH AMERICA VIRGINIA</th>
<th>oracle.pstn.ashburn.twilio.com</th>
</tr>
</thead>
<tbody>
<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.

**IP ACCESS CONTROL LISTS**

| Oracle × |

**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](image)

**ORIGINATION SIP URI**: sip:155.212.215.102;edge=ashburn

**Priority**: 10

**Weight**: 10

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

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.

![Table showing Numbers association](image)
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 Cisco Users

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

![Registration screenshot]

3. Make Call from Cisco 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 Cisco CUCM first and then reaches Twilio trunk user after that as given below.

![Call flow screenshot]
4. Make Call from the Twilio Elastic Sip Trunk to Cisco User and check the call flow. The calls flow from 141.146.36.102 (Twilio Elastic SIP Trunking Interface) to 10.232.50.78 (Cisco SIP Interface) and the call reaches the Cisco user after that.
5. Make Call from Twilio Elastic Sip Trunk user to Cisco Remote user and check the call flow. Now, there will be 2 call legs (hair pinned call) as the call reaches Cisco CUCM first and then reaches Cisco Remote user after that as given below.
Appendix A

Following are the test cases that are executed between Cisco User with the Twilio Elastic SIP Trunk (PSTN user). Please note that Cisco User here refers both Cisco User inside Enterprise network as well as Cisco 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>Cisco user disconnects an inbound connected call</td>
<td>Pass</td>
</tr>
<tr>
<td>2</td>
<td>Cisco 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>Cisco 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>Cisco 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 Cisco 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 Cisco user and put that call on hold and then resumes</td>
<td>Pass</td>
</tr>
<tr>
<td>9</td>
<td>Cisco 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>Cisco 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 Cisco blind transferred to second Cisco/ PSTN User</td>
<td>Pass</td>
</tr>
<tr>
<td>12</td>
<td>Outbound Twilio Elastic SIP Trunk call from Cisco user blind transferred to second Cisco/ PSTN User</td>
<td>Pass</td>
</tr>
<tr>
<td>13</td>
<td>Inbound Twilio Elastic SIP Trunk Call to Cisco consultatively transferred to Cisco/ PSTN User</td>
<td>Pass</td>
</tr>
<tr>
<td>14</td>
<td>Outbound Twilio Elastic SIP Trunk call from Cisco user consultatively transferred to Cisco/ PSTN User</td>
<td>Pass</td>
</tr>
<tr>
<td>15</td>
<td>Cisco user makes outbound call to Twilio Elastic SIP Trunk user and makes a conference call by adding another Cisco/ PSTN user.</td>
<td>Pass</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Outcome</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>16</td>
<td>Twilio Elastic SIP Trunk user makes outbound call to Cisco user and Cisco user makes a conference call by adding another Cisco/ PSTN user.</td>
<td>Pass</td>
</tr>
<tr>
<td>17</td>
<td>Cisco user mutes inbound call from Twilio Elastic SIP Trunk user and then unmutes</td>
<td>Pass</td>
</tr>
<tr>
<td>18</td>
<td>Cisco 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 Cisco user and then unmutes</td>
<td>Pass</td>
</tr>
<tr>
<td>20</td>
<td>Twilio Elastic SIP Trunk user mutes outbound call made to Cisco user and then unmutes</td>
<td>Pass</td>
</tr>
<tr>
<td>21</td>
<td>Twilio Elastic SIP Trunk User disconnects outbound call to Cisco user before it is answered</td>
<td>Pass</td>
</tr>
<tr>
<td>22</td>
<td>Cisco user disconnects outbound call to Twilio Elastic SIP Trunk user before it is answered</td>
<td>Pass</td>
</tr>
</tbody>
</table>