

Twilio Elastic SIP Trunking Configuration Blueprint

Avaya Aura Communication Manager and Session Manager with:
Avaya Session Border Controller for Enterprise

October 2022

Copyright ©2022, Twilio and/or its affiliates. All rights reserved.

Twilio software and related documentation are provided under an agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this document and/or software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This document and described software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or platform in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Twilio and its affiliates disclaim any liability for any damages caused by use of this document or its platforms in dangerous applications.

Twilio is a registered trademark of Twilio and/or its affiliates. Other names may be trademarks of their respective owners.

This documentation may provide access to or information on content, products, and services from third parties. Twilio and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Twilio and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Safe Harbor Statement: The following is intended to outline general product information and 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 Twilio's products or services remains at the sole discretion of Twilio.

Abstract

This document outlines configuration steps required to integrate Avaya's Aura CM, SM Contact Center with Twilio's Elastic SIP Trunking. Third-party Enterprise -Grade validation testing of these configurations was conducted by the engineers at tekVizion Labs™.

Notice

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

Twilio Elastic SIP Trunking (ESIPT)

[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: 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.

Table of Contents

1 Audience	8
2 Lab Configuration	8
2.1 Hardware Components	9
2.2 Software Requirements	9
3 Features	10
3.1 Features Supported	10
3.2 Features Not Supported	10
3.3 Features Not Tested	10
3.4 Caveats and Limitations	10
4 Avaya Configuration	11
4.1 Avaya Configuration Checklist	11
4.2 IP Address Worksheet	11
4.3 Avaya Aura CM Configuration	12
4.3.1 Avaya Aura CM Login	12
4.3.2 IP Node Name	13
4.3.3 IP Codec Set	14
4.3.4 IP Network Region	15
4.3.5 Signaling Group	16
4.3.6 Trunk Groups	17
4.3.8 Route Pattern	21
4.3.9 Outbound Call Routing	22
4.3.10 Inbound Call Routing	23
4.4 Avaya Aura Session Manager Configuration	23
4.4.1 Avaya Aura SM login	23
4.4.2 Domain	25
4.4.3 Locations	26
4.4.4 Adaptations	28
4.4.5 SIP Entities and Entity Links	30

4.4.7	Routing Policies	36
4.4.8	Dial Patterns	39
4.5	Avaya SBCE Configuration	40
4.5.1	Avaya SBCE login	40
4.5.2	Server Interworking	42
4.5.3	SIP Servers	47
4.5.4	Topology Hiding	49
4.5.5	Routing	51
Figure 54	Routing for twilio	51
4.5.6	End Point Policy Groups	52
4.5.8	Network Management	55
4.5.9	Media Interface	56
4.5.10	Signaling Interface	57
4.5.11	Endpoint Flows	58
4.5.12	TLS Configuration	61
5	Twilio Elastic SIP Trunking Configuration	73
5.1	Create an IP-ACL rule	74
Figure 80	ESIPT Regional Edge URLs	76
5.2	Associate Phone Numbers on your Trunk	78
6	TekVizion	79
Table of Figures		
Figure 1	Network Topology	7
Figure 2:	Avaya Aura CM login	12
Figure 3	IP Node Name	13
Figure 4	IP Codec Set	14
Figure 5	IP Network Region	15
Figure 6	Signaling Group	16
Figure 7	Trunk Group	17
Figure 8	Trunk Group Continuation	18
Figure 9	Trunk Group Continuation	19
Figure 10	Trunk Group Continuation	20
Figure 11	Route Pattern	21
Figure 12	Outbound Call Routing	22
Figure 13	Outbound Caller ID	23

Figure 14 Avaya Aura SM login	24
Figure 15 Routing	25
Figure 16 Add Domain	25
Figure 17 Domain	26
Figure 18 Locations	26
Figure 19 Locations continuation	27
Figure 20 Locations continuation	27
Figure 21 Digit Conversion to Avaya CM	28
Figure 22 Digit Conversion to twilio	28
Figure 23 Adaptation for twilio	29
Figure 24 SIP Entity for Avaya SM	30
Figure 25 SIP Entity for Avaya SM continuation	31
Figure 26 SIP Entity for Avaya SM continuation	32
<i>Figure 27 SIP Entity and Entity Links for Avaya CM</i>	33
<i>Figure 28 SIP Entity and Entity Links for Avaya CM continuation</i>	33
Figure 29 SIP Entity and Entity Link for Avaya CM continuation	34
Figure 30 SIP Entity and Entity Link for Avaya SBCE	34
Figure 31 SIP Entity and Entity Link for Avaya SBCE continuation	35
Figure 32 SIP Entity and Entity Link for Avaya SBCE continuation	35
Figure 33 Routing Policy for Avaya CM	36
Figure 34 Routing Policy for Avaya CM continuation	36
Figure 35 Routing Policy for Avaya CM continuation	37
Figure 36 Routing Policy for Avaya SBCE	37
Figure 37 Routing Policy for Avaya SBCE continuation	38
Figure 38 Routing Policy for Avaya SBCE continuation	38
Figure 39 Dial Pattern to Avaya CM	39
Figure 40 Dial Pattern to twilio via Avaya SBCE	40
Figure 41 Avaya SBCE Login	41
Figure 42 Selection of Avaya SBCE Device	41
Figure 43 Server Interworking profile for Avaya SM	42
Figure 44 Server Interworking profile for Avaya SM Continuation	43
Figure 45 Server Interworking profile for Avaya SM Continuation	44
Figure 46 Server Interworking profile for Twilio	45
Figure 47 Server Interworking profile for Twilio Continuation	46
Figure 48 SIP Server for Avaya SM	47
Figure 49 SIP Server for Avaya SM Continuation	47
Figure 50 SIP Server for Twilio	48
Figure 51 Topology Hiding Profile for Avaya SM	49
Figure 52 Topology Hiding Profile for Twilio	50
Figure 53 Routing for Avaya SM	51
Figure 54 Routing for twilio	51
Figure 55 End Point Policy Group for Avaya SM	52
Figure 56 End Point Policy Group for Avaya SM Continuation	53
Figure 57 End Point Policy Group for twilio	54

Figure 58 Network Management Interfaces	55
Figure 59 Network Management Networks	55
Figure 60 Media Interface facing Avaya SM	56
Figure 61 Media Interface facing twilio	56
Figure 62 Signaling Interface facing Avaya SM LAN and twilio	57
Figure 63 Endpoint Flows	58
Figure 64 Endpoint Flows for Avaya SM LAN	59
Figure 65 Endpoint Flows for twilio	60
Figure 66 Upload twilio Root CA	61
Figure 67 Client Profile facing twilio	62
Figure 68 Client Profile facing twilio Continuation	63
Figure 69 Server Profile facing twilio	64
Figure 70 Server Profile facing twilio Continuation	65
Figure 71 SIP Server Profile – twilio	66
Figure 72 Media Rule – twilio	67
Figure 73 Media Rule – twilio Continuation	68
Figure 74 Edit End Point policy Group – twilio	69
Figure 75 Edit End Point policy Group –twilio Continuation	70
Figure 76 Edit Signaling Interface – twilio	70
Figure 77 Edit Signaling Interface – twilio continuation	71
Figure 78 Edit Server Flow – twilio	72
Figure 79 Edit Server Flow – twilio continuation	73

1 Audience

This document is intended for technical staff which have installation and operational responsibilities for the technologies described within this document, including: Twilio Elastic SIP Trunking, Avaya Aura Communication Manager (Avaya Aura CM), Avaya Aura Session Manager (Avaya Aura SM) with Avaya Session Border Controller for Enterprise (Avaya SBCE), to connect to Twilio’s inbound and outbound PSTN Connectivity capabilities.

2 Lab Configuration

The network for the SIP trunk reference configuration is illustrated below and is representative of Avaya Aura CM and Avaya Aura SM with Avaya SBCE configuration with twilio.

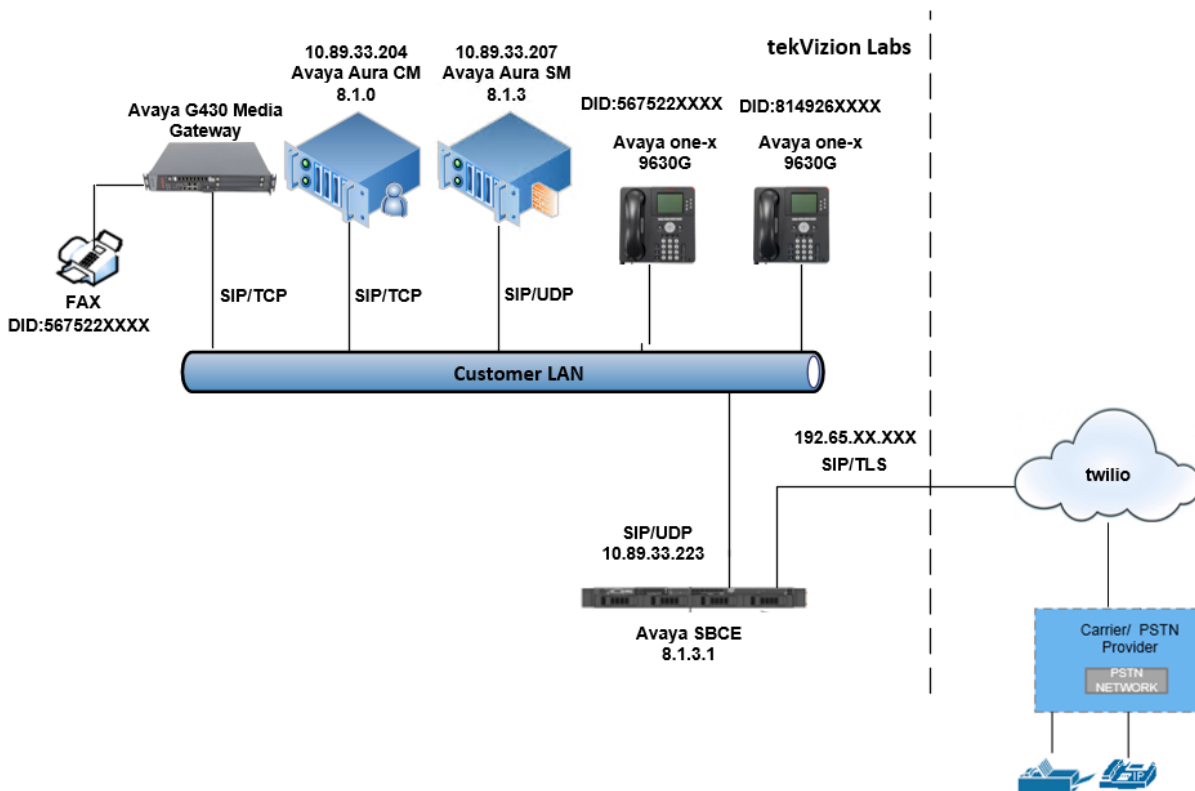


Figure 1 Network Topology

2.1 Hardware Components

- UCS-B200 VMWare server running ESXi 6.0 or later used for the following virtual machines
 - Avaya Aura
 - Communication Manager
 - Session Manager
 - Modular Messaging
- Avaya SBCE running on Dell CAD – 208 hardware appliance
- Avaya IP Phone IP Phone(s)– 9630G

2.2 Software Requirements

- Avaya Aura
 - Session Manager: 8.1.3.2
 - Communication Manager: 8.1.0.0
 - System Manager: 8.1.3.2
- Avaya Session Border Controller for Enterprise : 8.1.3.1

3 Features

3.1 Features Supported

- Basic calls using G.711ulaw
- International Call
- Call Transfer
- Call Forwarding
- Call Waiting
- Three-Way Calling
- Call Hold and Resume
- Calling Number Presentation and Restriction
- Busy-out PBX endpoint
- DTMF Inband and RFC2833

3.2 Features Not Supported

- None

3.3 Features Not Tested

- None

3.4 Caveats and Limitations

- Avaya SBC has a limitation to consume the certificate bundle shared by twilio. Because of this the systems administrator will need to split the CA certificates in the bundle and install individually. (Avaya ticket ID 1-19181728682)
 - During testing tekVizion observed importing only the DigiCert certificates from the Twilio bundle was sufficient to enable the TLS certificate verification

4 Avaya Configuration

4.1 Avaya Configuration Checklist

In this section we present an overview of the steps that are required to configure Avaya Aura CM, Avaya Aura SM and Avaya SBCE for SIP Trunking with twilio.

Steps	Description	Reference
Step 1	Avaya Aura CM Configuration	Section 4.3
Step 2	Avaya Aura SM Configuration	Section 4.4
Step 3	Avaya SBCE Configuration	Section 4.5

Table 1 – PBX Configuration Steps

4.2 IP Address Worksheet

NOTICE: The specific values listed in the table below and in subsequent sections are used in the lab configuration described in this document and are for illustrative purposes only. The customer must obtain and use the values for your deployment.

Component	Lab Value
Avaya SBCE	
LAN IP Address	10.89.33.223
LAN Subnet Mask	255.255.255.0
Avaya Aura CM	
IP Address	10.80.33.204
Subnet Mask	255.255.255.0
Avaya Aura SM	
IP Address	10.80.33.207
Subnet Mask	255.255.255.0

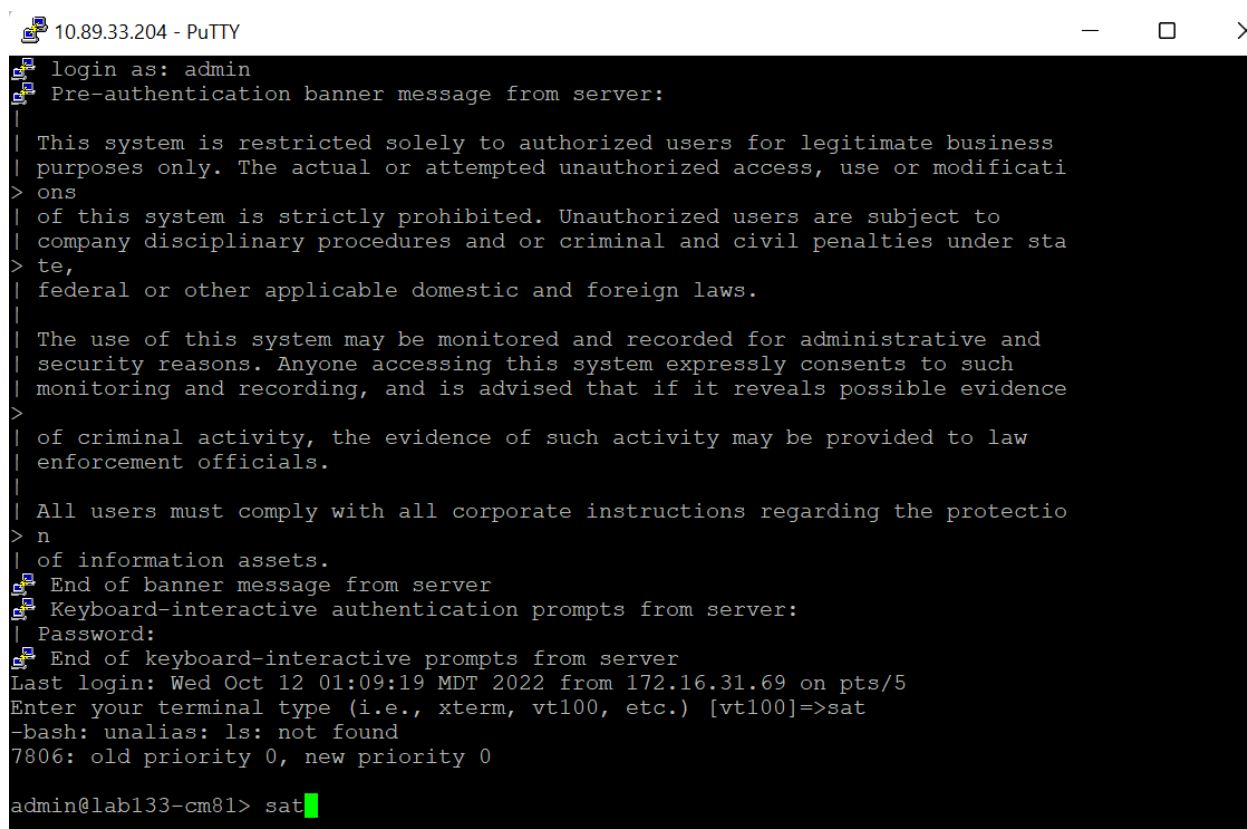
Table 2 – IP Addresses

4.3 Avaya Aura CM Configuration

This section provides screen shots taken from Avaya Aura CM and were used for the interoperability testing. These screen shots provide a general overview of the PBX configuration.

4.3.1 Avaya Aura CM Login

- Avaya Aura CM configuration is done via SAT simulator through PuTTY.
- Log in using an appropriate User ID and Password.



```

10.89.33.204 - PuTTY
login as: admin
Pre-authentication banner message from server:
| This system is restricted solely to authorized users for legitimate business
| purposes only. The actual or attempted unauthorized access, use or modificati
| ons
| of this system is strictly prohibited. Unauthorized users are subject to
| company disciplinary procedures and or criminal and civil penalties under sta
| te,
| federal or other applicable domestic and foreign laws.
|
| The use of this system may be monitored and recorded for administrative and
| security reasons. Anyone accessing this system expressly consents to such
| monitoring and recording, and is advised that if it reveals possible evidence
|
| of criminal activity, the evidence of such activity may be provided to law
| enforcement officials.
|
| All users must comply with all corporate instructions regarding the protectio
| n
| of information assets.
End of banner message from server
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
Last login: Wed Oct 12 01:09:19 MDT 2022 from 172.16.31.69 on pts/5
Enter your terminal type (i.e., xterm, vt100, etc.) [vt100]=>sat
-bash: unalias: ls: not found
7806: old priority 0, new priority 0
admin@lab133-cm81> sat

```

Figure 2: Avaya Aura CM login

4.3.2 IP Node Name

- Use the Change node-names ip command to verify that node names are defined for Avaya Aura CM (procr) and Session Manager (Lab133-SM81). The node names are needed for configuring the Signaling Group.

```

10.89.33.204 - PuTTY
change node-names ip                                     Page 1 of 2
                                     IP NODE NAMES
Name                                IP Address
-----
Lab133-SM81                          10.89.33.207
default                               0.0.0.0
-----
procr                                 10.89.33.204
procr6                                ::
-----
( 6 of 6 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
-----
F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg

```

Figure 3 IP Node Name

4.3.3 IP Codec Set

- Use `change ip-codec-set 1` to define a list of codecs for calls between Avaya Aura CM and SM.

```

10.89.33.204 - PuTTY
change ip-codec-set 1 Page 1 of 2

                                IP MEDIA PARAMETERS
Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression  Per Pkt     Size (ms)
1: G.711MU  n             2           20
2: G.711A  n             2           20
3: G.729A  n             2           20
4: _____ -             -           -
5: _____ -             -           -
6: _____ -             -           -
7: _____ -             -           -

Media Encryption                      Encrypted SRTP: best-effort
1: none
2: _____
3: _____
4: _____
5: _____

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg

```

Figure 4 IP Codec Set

4.3.4 IP Network Region

- Use change ip-network-region 1 to define the network region
- *Authoritative Domain*: Domain name lab.tekvizion.com
- *Codec Set*: Enter codec set 1 created in Section 4.3.1
- *Intra-region IP-IP Direct Audio*: yes
- *Intra-region IP-IP Direct Audio*: yes

```

10.89.33.204 - PuTTY
change ip-network-region 1 Page 1 of 20
IP NETWORK REGION
Region: 1 NR Group: 1
Location: 1 Authoritative Domain: lab.tekvizion.com
Name: Lab133 Stub Network Region: n
MEDIA PARAMETERS
Codec Set: 1 Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048 IP Audio Hairpinning? y
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5
AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS
RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
  
```

Figure 5 IP Network Region

4.3.5 Signaling Group

- Command add signaling group 2 was used to create Signaling Group. Use change signaling group 2 to modify existing signaling group.
- Set *Group Type*: sip
- Set *Transport Method*: tcp
- Set *Peer Detection Enable*: y
- Set *Near-end Node Name*: procr
- Set *Near-end Listen Port*: 5060
- Set *Far-end Node Name*: Lab133-SM81
- Set *Far-end Listen Port*: 5060
- Set *Far-end Network Region*: 1
- Set *Far-end Domain*: lab.tekvizion.com
- Set *DTMF over IP*: rtp-payload
- Set *Direct IP-IP Audio Connections*: n
- Leave other fields to default value

```

10.89.33.204 - PuTTY
change signaling-group 2 Page 1 of 2
SIGNALING GROUP
Group Number: 2 Group Type: sip
IMS Enabled?  Transport Method: tcp
Q-SIP? n
IP Video? n Enforce SIPS URI for SRTP? n
Peer Detection Enabled?  Peer Server: SM Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr Far-end Node Name: Lab133-SM81
Near-end Listen Port: 5060 Far-end Listen Port: 5060
Far-end Network Region: 1
Far-end Domain: lab.tekvizion.com
Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload Direct IP-IP Audio Connections? n
Session Establishment timer(min): 3 IP Audio Hairpinning? n
Enable Layer 3 Test? y Alternate Route Timer(sec): 6
F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
  
```

Figure 6 Signaling Group

4.3.6 Trunk Groups

- Trunk group 1 is used for trunk to Avaya SM. Command add trunk group 1 was used to create Trunk Group. Use change trunk group 1 to modify existing trunk group.
- Set *Group Type*: sip
- Set *Group Name*: PSTN
- Set *TAC*: #001
- Set *Direction*: two-way
- Set *Service Type*: public-ntwrk
- Set *Member Assignment Method*: auto
- Set *Signaling Group*: 2 (created in section 4.3.3)
- Set *Number of Members*: 10

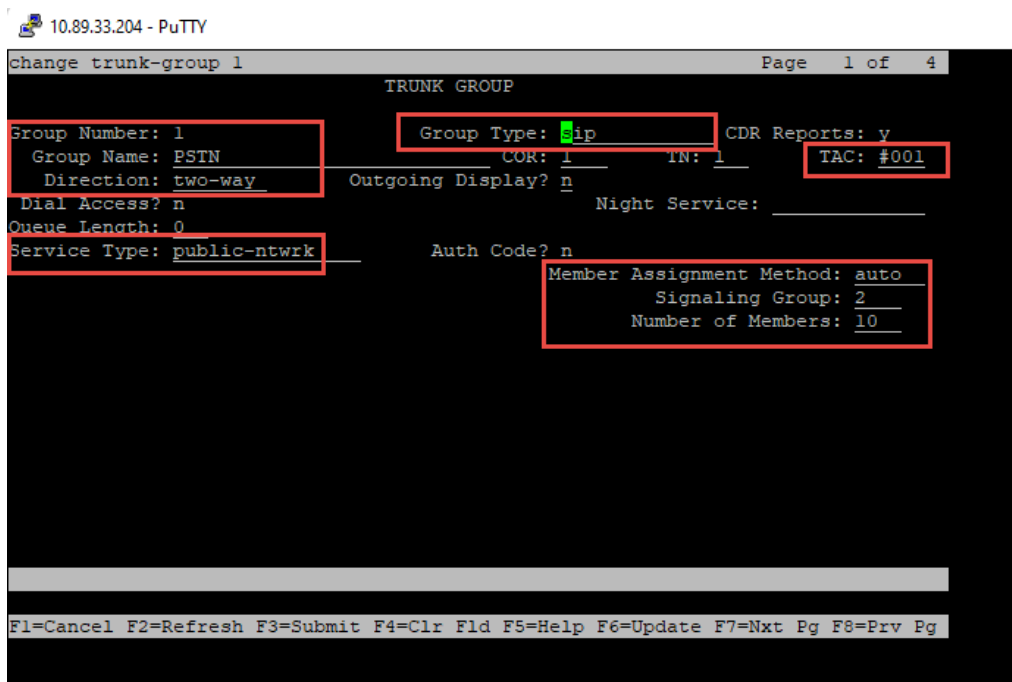


Figure 7 Trunk Group

- Set Preferred Minimum Session Refresh Interval (sec): 900

```
10.89.33.204 - PuTTY
change trunk-group 1 Page 2 of 4
  Group Type: sip
TRUNK PARAMETERS
  Unicode Name: Auto
                                Redirect On OPTIM Failure: 5000
  SCCAN? n                      Digital Loss Group: 18
                                Preferred Minimum Session Refresh Interval(sec): 900
Disconnect Supervision - In? y Out? y
                                XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n
Caller ID for Service Link Call to H.323 lxC: station-extension
F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Figure 8 Trunk Group Continuation

- Set *Numbering Format*: private

```
10.89.33.204 - PuTTY
Change trunk-group 1 Page 3 of 4
TRUNK FEATURES
  ACA Assignment?  Measured: none Maintenance Tests? y

  Suppress # Outpulsing? n Numbering Format: private UUI Treatment: service-provider
                                Replace Restricted Numbers? n
                                Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no

  Show ANSWERED BY on Display? y

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Figure 9 Trunk Group Continuation

- Set *Telephone Event payload Type*: 101
- Set *Identity for calling Party Display*: From
- Leave all other fields to default values

```
10.89.33.204 - PuTTY
change trunk-group 1 Page 4 of 4
PROTOCOL VARIATIONS
Mark Users as Phone? 
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
Send Transferring Party Information? y
Network Call Redirection? n
Send Diversion Header? y
Support Request History? n
Telephone Event Payload Type: 101
Convert 180 to 183 for Early Media? n
Always Use re-INVITE for Display Updates? y
Identity for Calling Party Display: From
Block Sending Calling Party Location in INVITE? n
Accept Redirect to Blank User Destination? n
Enable Q-SIP? n
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
Request URI Contents: may-have-extra-digits
F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
```

Figure 10 Trunk Group Continuation

4.3.8 Route Pattern

- Use change-route-pattern x command to specify the routing preference. Route pattern 1 is used for SIP trunk to Avaya SM.
- Set *Pattern Name*: PSTN
- Set *Grp No*: 1 (created in Section 4.3.4)
- Set *FRL*: 0
- Set *Numbering Format*: unk-unk
- Leave all other fields to default values

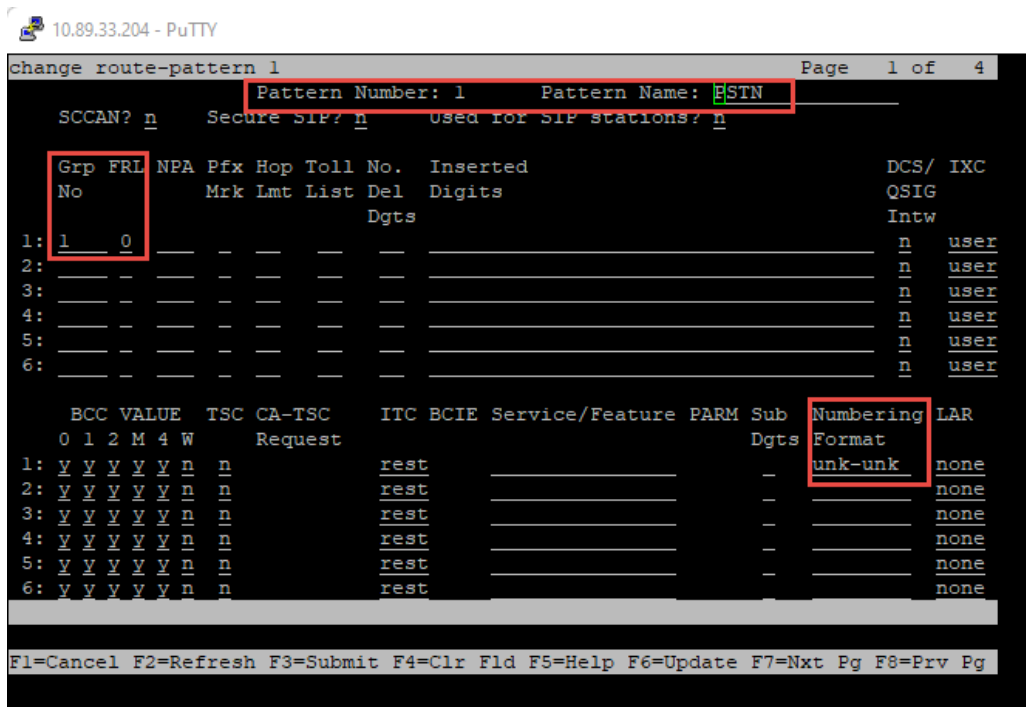


Figure 11 Route Pattern

4.3.9 Outbound Call Routing

For outbound call to twilio, Automatic Route Selection (ARS) is used. Use command change ars analysis x to configure the routing table.

- Set *Dialed String*: 214242
- Set *Min*: 10
- Set *Max*: 12
- Set *Route Pattern*: 1 (created in section 4.3.5)
- Set *Call Type*: natl (for national and intl for International dialing)

10.89.33.204 - PuTTY

change ars analysis 2 Page 1 of 2

ARS DIGIT ANALYSIS TABLE						
Location: all						
Percent Full: 3						
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
214	3	12	1	natl	---	n
214242	6	12	1	natl	---	n
800	3	10	1	natl	---	n
866	3	10	1	natl	---	n
877	3	10	1	natl	---	n
888	3	10	1	natl	---	n
011	3	15	1	intl	---	n
531	3	10	1	natl	---	n

F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg

Figure 12 Outbound Call Routing

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

User ID:

Password:

[Change Password](#)

Supported Browsers: Internet Explorer 11.x or Firefox (minimum version 65.0).

Figure 14 Avaya Aura SM login

4.4.2 Domain

- Navigate to Elements > Routing

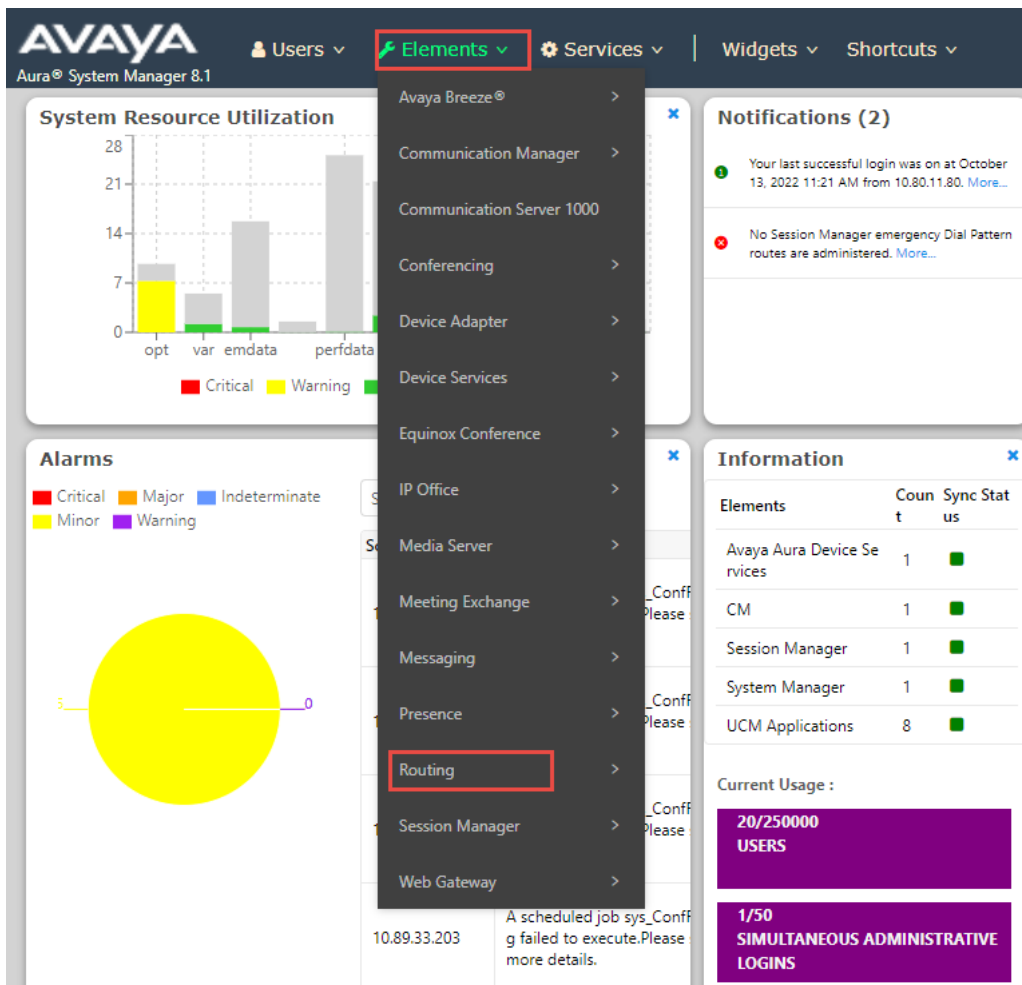


Figure 15 Routing

- Navigate to Routing > Domains
- Click New

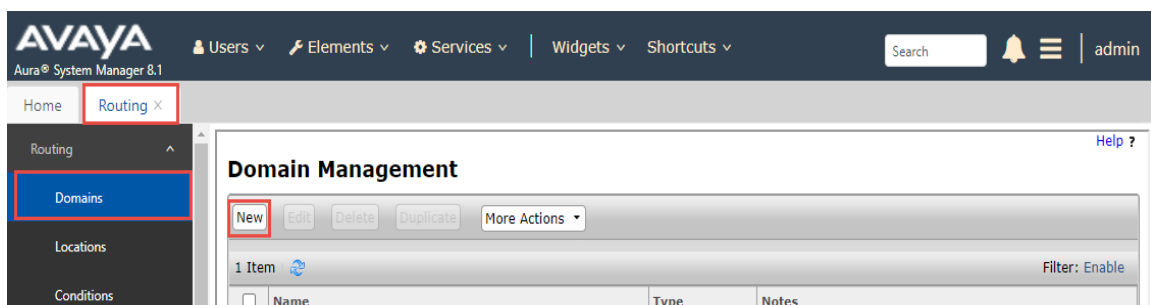


Figure 16 Add Domain

- Set *Name*: Enter the domain name of Avaya Aura PBX, lab.tekvizion.com
- Set *Type*: sip
- Click Commit (not shown here)

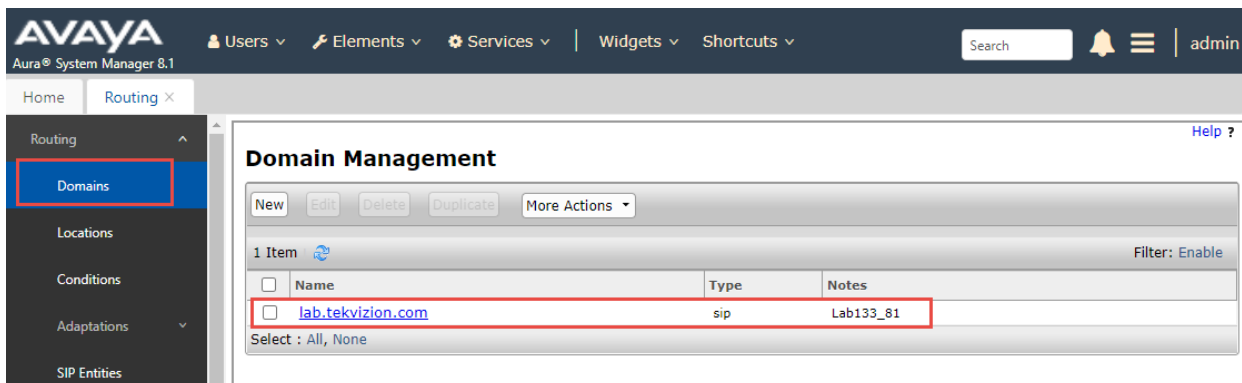


Figure 17 Domain

4.4.3 Locations

- Navigate to Routing > Locations
- Select New

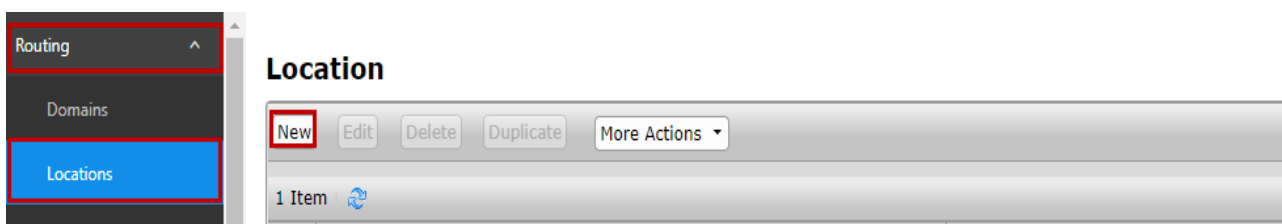


Figure 18 Locations

- Set Name: Lab133_81

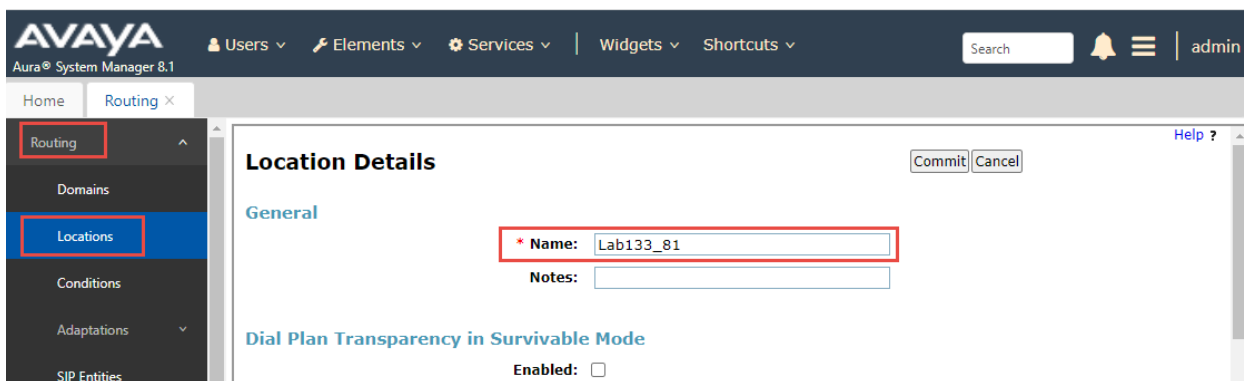


Figure 19 Locations continuation

- Under *Location Pattern*, select Add to add IP Address Patterns for different networks that communicates within the location
- Set *IP Address Pattern*: 10.80.33.x
- Leave all other fields to default values
- Click Commit

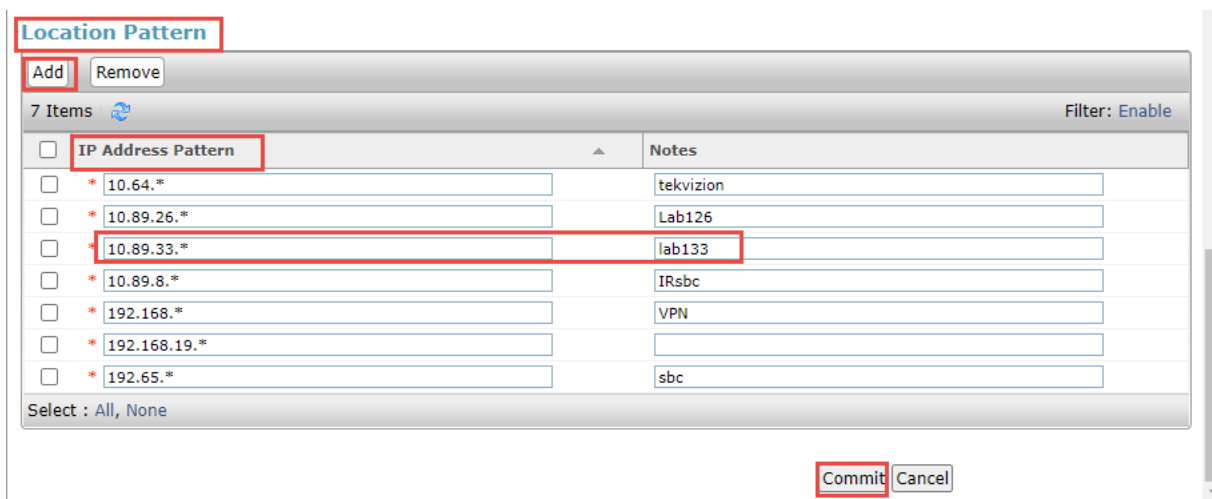


Figure 20 Locations continuation

4.4.4 Adaptations

- twilio uses E164 numbering format for SIP Trunking Service. Adaptation was created at the Session Manager to manipulate the digits sent to twilio network via Avaya Session Border Controller for Enterprise (Avaya SBCE).
- Navigate to Routing > Adaptations. Click New
- Set *Adaptation Name*: Adaptation_For_Twilio
- Set *Module Name*: DigitConversionAdapter
- Set *Module Parameter Type*: Name-Value Parameter is selected from the drop down, Click Add
- Set *Name/Value*: fromto/true
- Set *Name/Value*: osrcd/10.89.33.207 (Avaya Aura SM IP is entered)
- Set *Name/Value*: odstnd/10.89.33.223 (Avaya SBCE LAN IP is entered)
- Under Digit Conversion for Incoming Calls to SM, click Add

Matching Pattern	Min/Max	Delete Digits	Address to Modify
+15675	12/36	2 – Deletes +1 from +15675 patterns	Destination – Modifies digits in TO header and sends it to Avaya CM

Figure 21 Digit Conversion to Avaya CM

- Under Digit Conversion for Outgoing Calls from SM, click Add

Matching Pattern	Min/Max	Delete Digits	Insert Digits	Address to Modify
214242	10/36	0	+1 – Insert +1 in front of 214242 patterns	Destination – Modifies the digits in TO header and sends it to twilio

Figure 22 Digit Conversion to twilio

- Leave all other fields at default values
- Repeat the same for all your outbound dial DIDs individually.

- Click Commit

Adaptation Details

General

- * Adaptation Name: Adaptation_For_Twilio
- Notes: E.164
- * Module Name: DigitConversionAdapter
- Type: digit
- State: enabled
- Module Parameter Type: Name-Value Parameter

Name	Value
fromto	true
odrcd	10.89.33.207
odstd	10.89.33.223

Digit Conversion for Incoming Calls to SM

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify
* +15675	* 12	* 36		* 2		destination
* +18149	* 12	* 36		* 2		destination

Digit Conversion for Outgoing Calls from SM

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify
* 011	* 3	* 36		* 3	+	destination
* 214242	* 10	* 36		* 0	+1	destination
* 531	* 3	* 36		* 0	+1	destination
* 5675	* 10	* 36		* 0	+1	origination
* 800	* 3	* 36		* 0	+1	both
* 8149	* 10	* 36		* 0	+1	origination
* 866	* 3	* 36		* 0	+1	destination
* 877	* 3	* 36		* 0	+1	destination
* 888	* 3	* 36		* 0	+1	destination
* 9722	* 4	* 36		* 0	+1	destination
* 9725	* 4	* 36		* 0	+1	destination

Figure 23 Adaptation for twilio

4.4.5 SIP Entities and Entity Links

SIP Entity for Avaya Aura Session Manager

- Navigate to: Elements > Routing > SIP Entities.

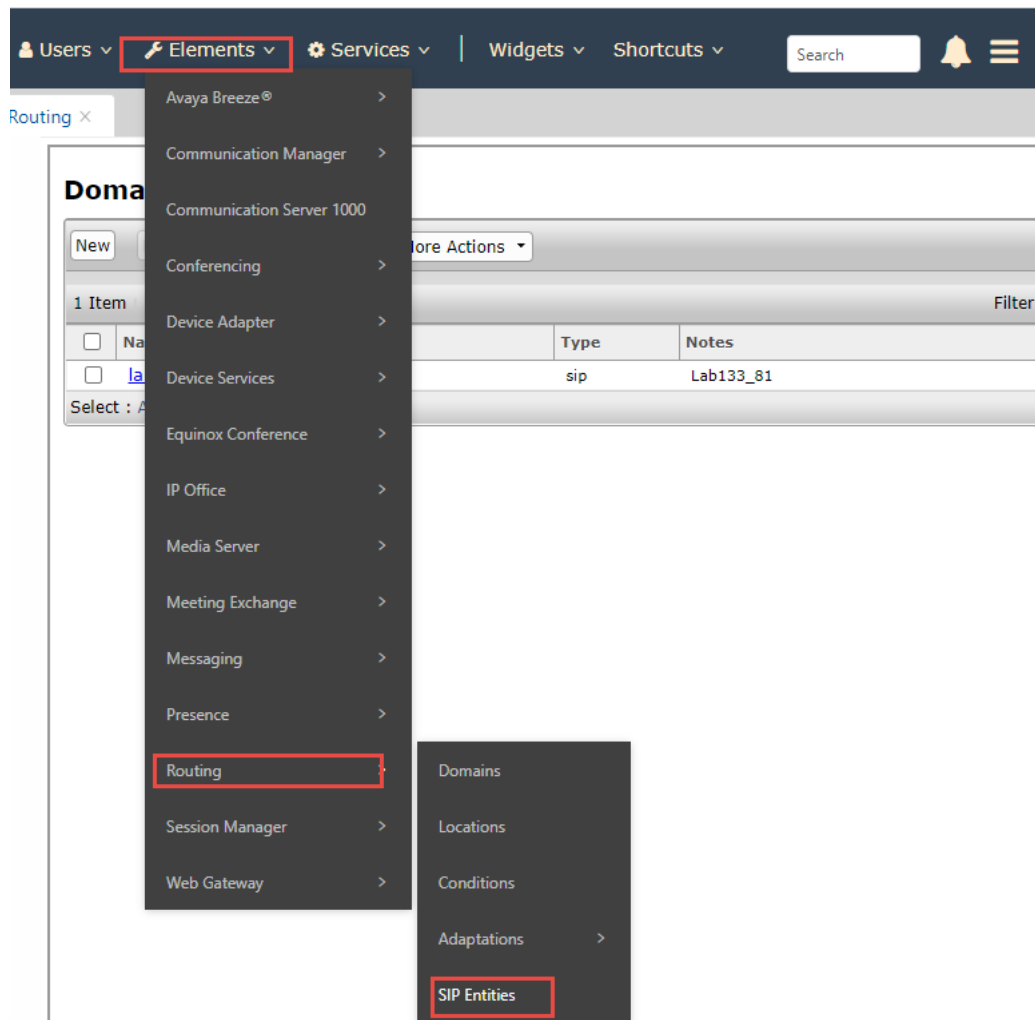


Figure 24 SIP Entity for Avaya SM

- Click New
- Set *Name*: Enter name of the host, Lab133_SM81
- Set *FQDN or IP Address*: Enter the SIP address of the Session Manager
- Set *Type*: Session Manager is selected from the drop down
- Set *Location*: Select the location (created in Section 4.4.3)
- Under *Listen Port*:
- Set *TCP/TLS Failover Port*: 5060/5061
- Click Add to assign Domain lab.tekvizion.com for the following Ports and Protocol

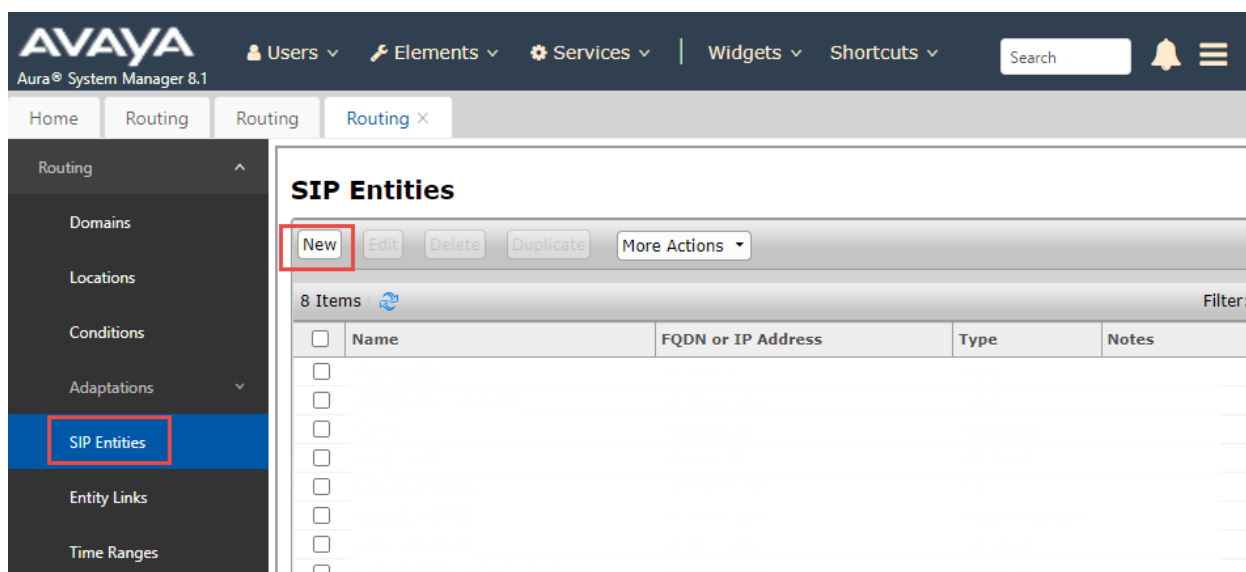


Figure 25 SIP Entity for Avaya SM continuation

- Port 5060 and Protocol TCP/UDP
- Port 5061 and Protocol TLS
- Click Commit

SIP Entity Details Commit Cancel

General

* Name: Lab133-SM81

* IP Address: 10.89.33.207

SIP FQDN:

Type: Session Manager

Notes:

Location: Lab133_81

Outbound Proxy:

Time Zone: America/Chicago

Minimum TLS Version: Use Global Setting

Credential name:

Failover Ports

TCP Failover port: 5060

TLS Failover port: 5061

Listen Ports

Add Remove

3 Items Filter: Enable

<input type="checkbox"/>	Listen Ports	Protocol	Default Domain	Endpoint	Notes
<input type="checkbox"/>	5060	TCP	lab.tekvizion.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5060	UDP	lab.tekvizion.com	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	5061	TLS	lab.tekvizion.com	<input checked="" type="checkbox"/>	

Select: All, None

Figure 26 SIP Entity for Avaya SM continuation

SIP Entity and Entity Links for Avaya Aura Communication Manager

- Set *Name*: Lab133_CM81
- Set *FQDN or IP Address*: Enter the IP address of Avaya Aura Communication Manager
- Set *Type*: CM
- Click Commit

SIP Entity Details

General

* Name: Lab133-CM81

* FQDN or IP Address: 10.89.33.204

Type: CM

Notes:

Adaptation: Adaptation_For_cm

Location: Lab133_81

Time Zone: America/Chicago

Commit Cancel

Figure 27 SIP Entity and Entity Links for Avaya CM

- Under *Entity Links*, Click New

Entity Links

New Edit Delete Duplicate More Actions

4 Items Filter:

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							

Select : All, None

Figure 28 SIP Entity and Entity Links for Avaya CM continuation

- Set *Name*: Lab133-SM81_Lab133CM_SIP_TCP_5060_TCP
- Set *SIP Entity 1*: Select the SIP entity Lab133-SM81
- Set *SIP Entity 2*: Lab133-CM81
- Set *Protocol*: TCP
- Set *Ports*: 5060
- Set *Connection Policy*: trusted
- Leave all other fields to default values
- Click Commit

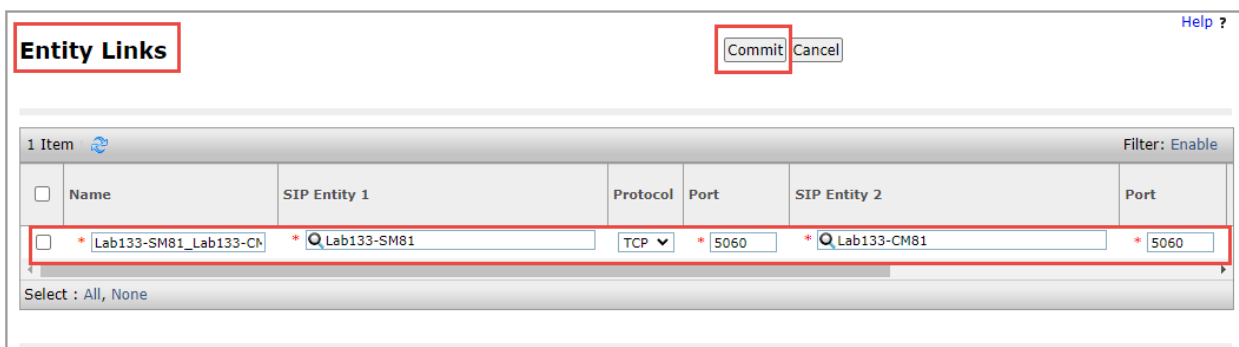


Figure 29 SIP Entity and Entity Link for Avaya CM continuation

SIP Entity and Entity Links for Avaya SBCE

- Set *Name*: SIP ENTITY_ESBC_TWILIO
- Set *FQDN or IP Address*: Enter the IP address of Avaya SBCE interface facing Avaya Aura SM
- Set *Adaptation*: Select the Adaptation for Avaya SBCE configured in Section 4.4.4
- Set *Location*: Select the location created in Section 4.4.3
- Click Commit

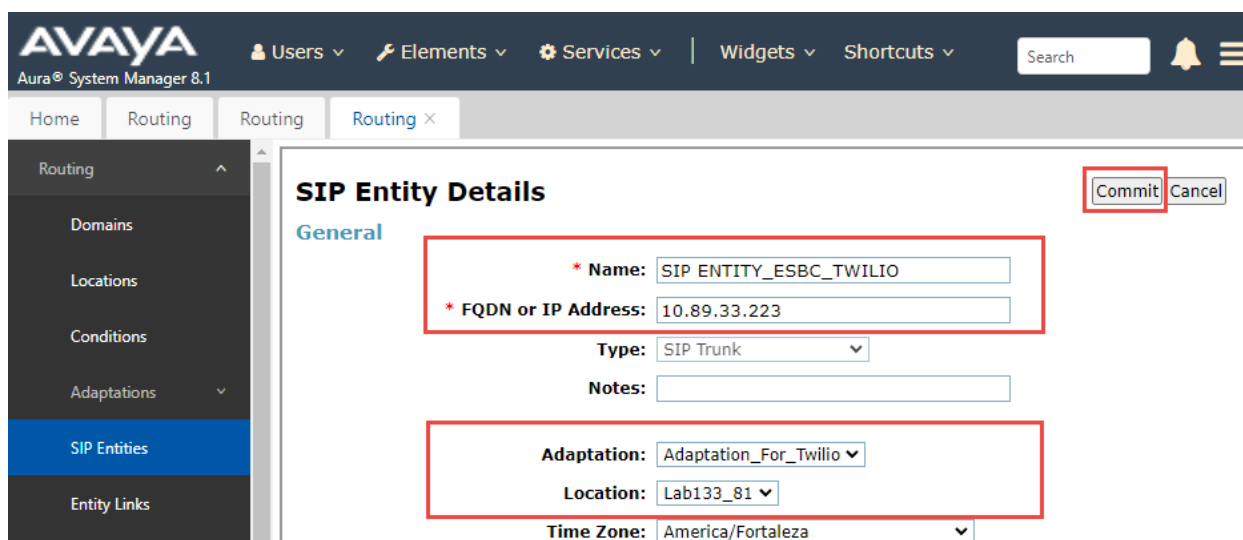


Figure 30 SIP Entity and Entity Link for Avaya SBCE

- Under *Entity Links*, Click New

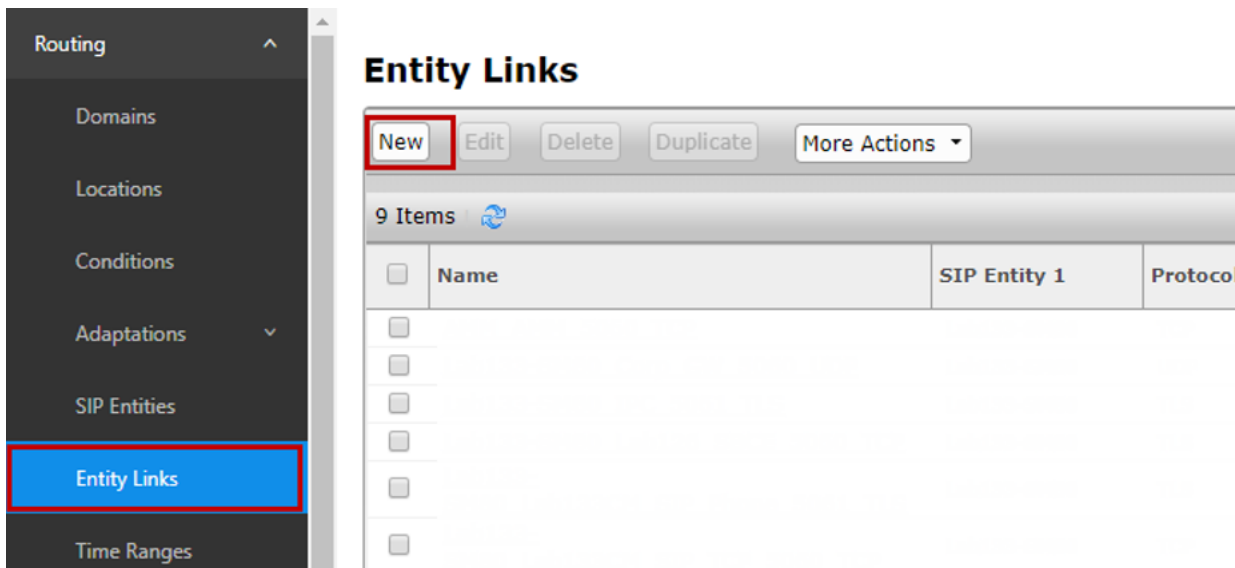


Figure 31 SIP Entity and Entity Link for Avaya SBCE continuation

- Set *Name*: TWILIO
- Set *SIP Entity 1*: Select the SIP Entity Lab133-SM81
- Set *SIP Entity 2*: SIP ENTITY_ESBC_TWILIO
- Set *Protocol*: UDP
- Set *Ports*: Set both Ports to 5060
- Set *Connection Policy*: trusted
- Leave all other fields to default values
- Click Commit

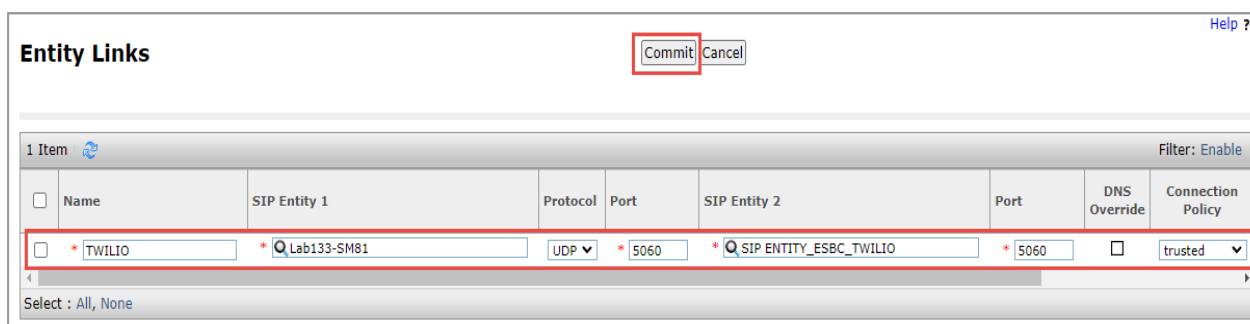


Figure 32 SIP Entity and Entity Link for Avaya SBCE continuation

4.4.7 Routing Policies

Routing policy to Avaya Aura CM

- Navigate to: Routing > Routing Policies. Click New
- Set *Name*: SM_to_CM
- Click Select under SIP Entity as Destination and the SIP Entities window is displayed

Routing Policy Details Commit Cancel

General

* **Name:**

Disabled:

* **Retries:**

Notes:

SIP Entity as Destination

Figure 33 Routing Policy for Avaya CM

- Check the radio button beside Lab133-CM81 as destination SIP Entity (configured in Section 4.4.5)
- Click Select and return back to Routing Policy Details page

SIP Entities Help ?

SIP Entities

7 Items Filter: Enable

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	AvayaSBC	10.89.8.9	Other	
<input type="radio"/>	AvayaSBC -Mutare	10.89.33.214	Other	
<input type="radio"/>	CMM	10.89.26.25	Messaging	
<input type="radio"/>	Corp_GW	10.64.1.72	SIP Trunk	
<input type="radio"/>	Lab133-CM81	10.89.33.204	CM	
<input type="radio"/>	SBC_neustar	10.80.11.85	SIP Trunk	
<input type="radio"/>	SIP_ENTITY_ESBC_TWILIO	10.89.33.223	SIP Trunk	

Select : None

Figure 34 Routing Policy for Avaya CM continuation

Leave all other fields at default values

- Click Commit

Routing Policy Details Commit Cancel

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Lab133-CM81	10.89.33.204	CM	

Figure 35 Routing Policy for Avaya CM continuation

Routing policy to Avaya SBCE

- Set Name: to_Avaya TWILIO_ESBC
- Click Select under SIP Entity as Destination and SIP Entities window is displayed.

Routing Policy Details Commit Cancel

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Select

Figure 36 Routing Policy for Avaya SBCE

- Check the radio button beside SIP ENTITY_ESBC_TWILIO as destination SIP Entity (configured in Section 4.4.5)
- Click Select and return back to Routing Policy Details page

SIP Entities Help ?

SIP Entities

7 Items Filter: Enable

Name	FQDN or IP Address	Type	Notes
<input type="radio"/> AvayaSBC	10.89.8.9	Other	
<input type="radio"/> AvayaSBC -Mutare	10.89.33.214	Other	
<input type="radio"/> CMM	10.89.26.25	Messaging	
<input type="radio"/> Corp_GW	10.64.1.72	SIP Trunk	
<input type="radio"/> Lab133-CM81	10.89.33.204	CM	
<input type="radio"/> SBC_neustar	10.80.11.85	SIP Trunk	
<input type="radio"/> SIP ENTITY_ESBC_TWILIO	10.89.33.223	SIP Trunk	

Select : None

Figure 37 Routing Policy for Avaya SBCE continuation

- Leave all other fields to default values
- Click Commit

Routing Policy Details

General

* Name:

Disabled:

* Retries:

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
SIP ENTITY_ESBC_TWILIO	10.89.33.223	SIP Trunk	

Figure 38 Routing Policy for Avaya SBCE continuation

4.4.8 Dial Patterns

Dial Pattern for Avaya Aura CM

- Navigate to: Routing > Dial Patterns. Click New
- Set *Pattern*: 5675 (first 4 digit of Twilio DID assigned to the PBX phone)
- Set *Min*: 4
- Set *Max*: 36
- Under Originating Locations and Routing Policies, Click Add, at the new window
- *Originating Location*: Select Lab133-81 (created in Section 4.4.3)
- *Routing Policies*: Select SM_to_CM under Routing Policies
- Click Select to return to Dial Pattern Details page
- Leave all other fields to default values.
- Click Commit

Dial Pattern Details

General

* Pattern: 5675
 * Min: 4
 * Max: 36

Emergency Call:
 SIP Domain: -ALL-
 Notes:

Originating Locations and Routing Policies

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> Lab133_81		SM_to_CM	0	<input type="checkbox"/>	Lab133-CM81	

Select : All, None

Figure 39 Dial Pattern to Avaya CM

Dial Pattern to twilio via Avaya SBCE

- Navigate to: Routing > Dial Patterns. Click New
- Set *Pattern*: 214242
- Set *Min*: 6
- Set *Max*: 12
- Under Originating Locations and Routing Policies, Click Add, at the new window
- *Originating Location*: Select Lab133-81 (created in Section 4.4.3)
- *Routing Policies*: Select to Avaya TWILIO_ESBC under Routing Policies
- Click Select to return to Dial Pattern Details page
- Leave all other fields to default values.
- Click Commit

Dial Pattern Details Commit Cancel Help ?

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Lab133_81		to AVAYA TWILIO_ESBC	0	<input type="checkbox"/>	SIP ENTITY_ESBC_TWILIO	

Figure 40 Dial Pattern to twilio via Avaya SBCE

4.5 Avaya SBCE Configuration

4.5.1 Avaya SBCE login

- Log into Avaya Session Border Controller for Enterprise (SBCE) web interface by typing “https://X.X.X.X/sbc”.
- Enter the Username and Password
- Click Log In



Session Border Controller for Enterprise

Log In

Username:

Password:

WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2020 Avaya Inc. All rights reserved.

Figure 41 Avaya SBCE Login

- Under Device, select ASBCETwilio from drop down to expand the configuration for Avaya SBCE.

The screenshot shows the Avaya SBCE web interface. At the top, there is a navigation bar with the following items: Device: ASBCETwilio (highlighted with a red box), Alarms 1, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. Below the navigation bar is the main header "Session Border Controller for Enterprise" and the AVAYA logo. On the left side, there is a sidebar menu with the following items: EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters (highlighted with a red box), Configuration Profiles, Services, Domain Policies, TLS Management, Network & Flows (highlighted with a red box), DMZ Services, and Monitoring & Logging. The main content area is titled "Dashboard" and contains two panels. The "Information" panel shows the following data: System Time (01:03:43 AM CDT), Version (8.1.3.1-38-21632), GUI Version (8.1.3.1-21907), Build Date (Wed Apr 27 12:58:40 UTC 2022), License State (OK), Aggregate Licensing Overages (0), Peak Licensing Overage Count (0), Last Logged in at (09/20/2022 09:43:30 CDT), and Failed Login Attempts (0). The "Installed Devices" panel shows a list of devices: EMS and ASBCETwilio (highlighted with a red box and a red '1' icon).

Figure 42 Selection of Avaya SBCE Device

4.5.2 Server Interworking

Server Interworking for Avaya SM

- Navigate to: Configuration Profiles > Server Interworking
- Select the predefined Interworking Profile avaya-ru, click Clone
- Set Clone Name: AASM8.1
- Click Finish

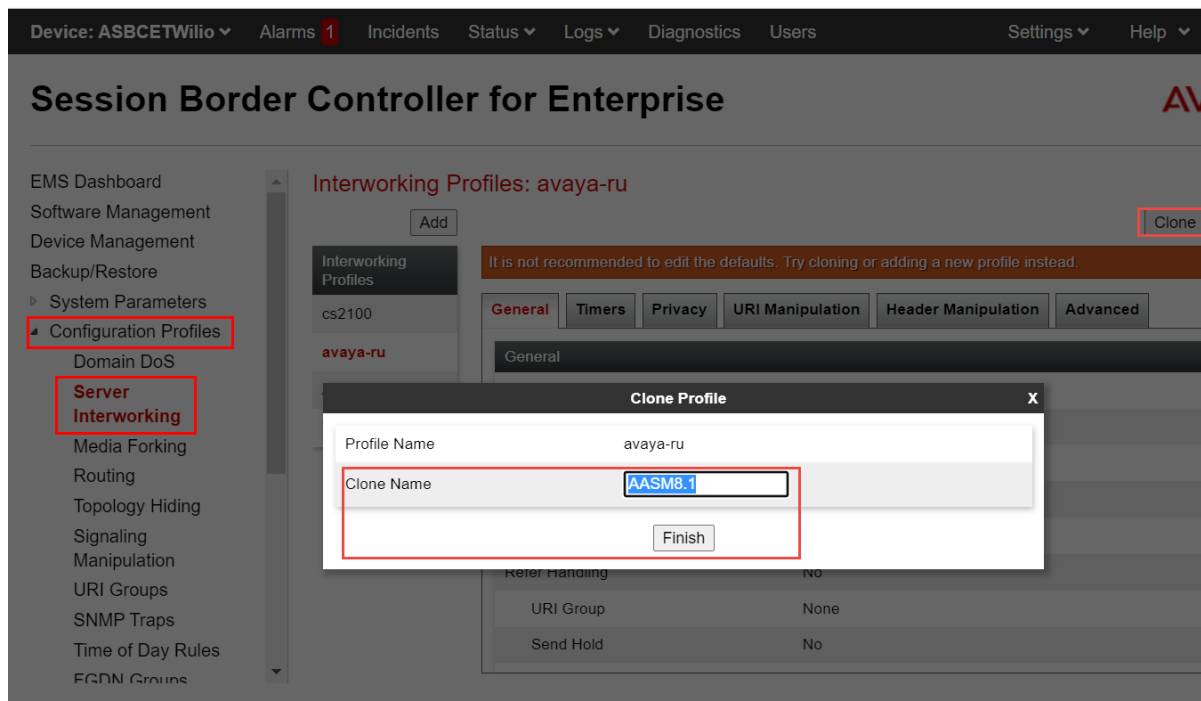


Figure 43 Server Interworking profile for Avaya SM

arms 1 Incidents Sta

Editing Profile: AASM8.1 X

er Controller 1

Interworking Profil

Add

Interworking Profiles

cs2100

avaya-ru

AASM8.1

Twilio

General

Hold Support None
 RFC2543 - c=0.0.0.0
 RFC3264 - a=sendonly
 Microsoft Teams

180 Handling None SDP No SDP

181 Handling None SDP No SDP

182 Handling None SDP No SDP

183 Handling None SDP No SDP

Refer Handling

URI Group

Send Hold

Delayed Offer

3xx Handling

Diversion Header Support

Delayed SDP Handling

Re-Invite Handling

Prack Handling

Allow 18X SDP

T.38 Support

URI Scheme SIP TEL ANY

Via Header Format RFC3261
 RFC2543

SIPS Required

Mediasec Handling

Finish

Figure 44 Server Interworking profile for Avaya SM Continuation

Interworking Profiles: AASM8.1

Add Rename Clone Delete

Interworking Profiles

- cs2100
- avaya-ru
- AASM8.1**
- Twilio

Click here to add a description.

General **Timers** Privacy URI Manipulation Header Manipulation Advanced

SIP Timers	
Min-SE	---
Init Timer	---
Max Timer	---
Trans Expire	2 seconds
Invite Expire	---
Retry After	---

Edit

Interworking Profiles: AASM8.1

Add Rename Clone Delete

Interworking Profiles

- avaya-ru
- AASM8.1**
- Twilio

Click here to add a description.

General **Timers** Privacy URI Manipulation Header Manipulation **Advanced**

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

Figure 45 Server Interworking profile for Avaya SM Continuation

Server Interworking for twilio

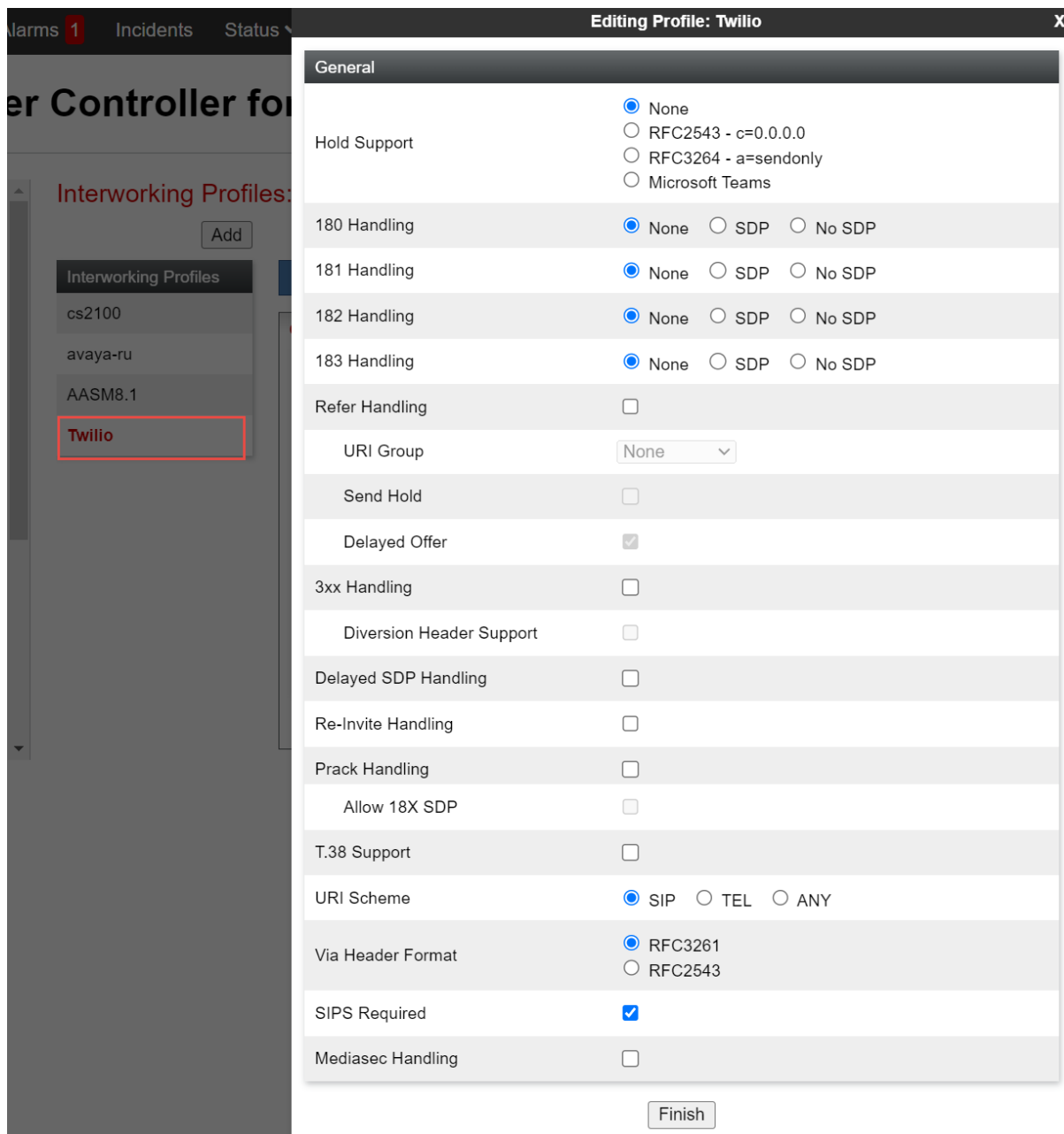


Figure 46 Server Interworking profile for Twilio

Interworking Profiles: Twilio

Interworking Profiles configuration interface. The main area shows the 'Advanced' tab selected, displaying a table of settings.

General	Timers	Privacy	URI Manipulation	Header Manipulation	Advanced
Record Routes				Both Sides	
Include End Point IP for Context Lookup				Yes	
Extensions				Avaya	
Diversion Manipulation				No	
Has Remote SBC				Yes	
Route Response on Via Port				No	
Relay INVITE Replace for SIPREC				No	
MOBX Re-INVITE Handling				No	
NATing for 301/302 Redirection				Yes	

Figure 47 Server Interworking profile for Twilio Continuation

4.5.3 SIP Servers

SIP Server for Avaya SM

- Navigate to Services > SIP Servers
- Set *Profile Name*: Avaya_SM
- Set *Server Type*: Select Call Server from the drop down
- Set *IP Address/FQDN*: Enter the Avaya Aura Session Manager SIP IP Address
- Set *Port*: 5060
- Set *Transport*: UDP

The screenshot shows the Twilio Session Border Controller for Enterprise interface. The top navigation bar includes 'Device: ASBCETWilio', 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header is 'Session Border Controller for Enterprise' with the 'AVAYA' logo on the right. A left sidebar lists various configuration categories, with 'Services' and 'SIP Servers' highlighted. The main content area is titled 'SIP Servers: Avaya SM' and contains an 'Add' button, 'Rename', 'Clone', and 'Delete' buttons. Below this is a 'Server Profiles' list with 'Avaya SM' and 'twilio'. The 'General' tab is active, showing a table of server configuration:

Server Type	Call Server	
DNS Query Type	NONE/A	
IP Address / FQDN	Port	Transport
10.89.33.207	5060	UDP

An 'Edit' button is located below the table.

Figure 48 SIP Server for Avaya SM

SIP Servers: Avaya SM

This screenshot shows the 'Advanced' configuration tab for the 'Avaya SM' SIP server. The 'Advanced' tab is highlighted in the top navigation. The configuration options are as follows:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	AASM8.1
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

An 'Edit' button is located at the bottom right of the configuration area.

Figure 49 SIP Server for Avaya SM Continuation

SIP Server for Twilio

SIP Servers: twilio

Rename Clone Delete

Add

Server Profiles

Avaya SM

twilio

General Authentication Heartbeat Registration Ping **Advanced**

Server Type Trunk Server

DNS Query Type NONE/A

IP Address / FQDN	Port	Transport
tekvizion.pstn.ashburn.twilio.com	5060	UDP

Edit

SIP Servers: twilio

Rename Clone Delete

Add

Server Profiles

Avaya SM

twilio

General Authentication Heartbeat Registration Ping **Advanced**

Enable DoS Protection

Enable Grooming

Interworking Profile Twilio

Signaling Manipulation Script None

Securable

Enable FGDN

Tolerant

URI Group None

NG911 Support

Edit

Figure 50 SIP Server for Twilio

4.5.4 Topology Hiding

Topology hiding profile for Avaya SM

- Topology Hiding profiles are added for Avaya SM to overwrite and hide certain headers
- Navigate to: Configuration Profiles > Topology Hiding
- Select the newly created profile Avaya_SM and Click Edit
- Set *Header*: Request-Line, To, From are selected
- Set *Replace Action*: Overwrite
- Set *Overwrite Value*: lab.tekvizion.com
- Click Finish (not shown here)

The screenshot shows the Twilio Session Border Controller for Enterprise interface. The top navigation bar includes 'Device: ASBCETwilio', 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the 'AVAYA' logo on the right.

The left sidebar contains a navigation menu with the following items: Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles (highlighted with a red box), Domain DoS, Server Interworking, Media Forking, Routing, Topology Hiding (highlighted with a red box), Signaling Manipulation, URI Groups, SNMP Traps, Time of Day Rules, FGDN Groups, Reverse Proxy, and Policy.

The main content area is titled 'Topology Hiding Profiles: Avaya_SM'. It features an 'Add' button and a list of profiles: 'default', 'Avaya_SM' (highlighted with a red box), and 'Twilio'. There are also 'Rename', 'Clone', and 'Delete' buttons. A blue bar above the table says 'Click here to add a description.'

The 'Topology Hiding' table is as follows:

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	lab.tekvizion.com
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Overwrite	lab.tekvizion.com
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
From	IP/Domain	Overwrite	lab.tekvizion.com
Record-Route	IP/Domain	Auto	---

An 'Edit' button is located at the bottom right of the table.

Figure 51 Topology Hiding Profile for Avaya SM

Topology hiding profile for Twilio

Device: ASBCETWilio | Alarms 1 | Incidents | Status | Logs | Diagnostics | Users | Settings | Help | Log Out

Session Border Controller for Enterprise

AVAYA

- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles**
- Domain DoS
- Server Interworking
- Media Forking
- Routing
- Topology Hiding**
- Signaling Manipulation
- URI Groups
- SNMP Traps
- Time of Day Rules
- FGDN Groups
- Reverse Proxy Policy

Topology Hiding Profiles: Twilio

Topology Hiding Profiles
 default
 Avaya_SM
Twilio

Click here to add a description.

Header	Criteria	Replace Action	Overwrite Value
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	tekvizion.pstn.ashburn.twilio.com
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Overwrite	tekvizion.pstn.ashburn.twilio.com
Via	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

Figure 52 Topology Hiding Profile for Twilio

4.5.5 Routing

Routing for Avaya SM

- Navigate to: Configuration Profiles > Routing
- Set *Profile Name*: Avaya_SM_routing
- Set *Priority/Weight*: 1
- Set *SIP Server profile*: select Avaya SM (configured in above SIP Servers section) from the dropdown (not shown here)
- The Server IP, Port and Transport Protocol populates automatically

Session Border Controller for Enterprise

Routing Profiles: Avaya_SM_routing

Routing Profiles: default, Avaya_SM_routing, TWILIO_Routing

Routing Profile

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	10.89.33.207:5062	UDP

Figure 53 Routing for Avaya SM

Routing for Twilio

NOTE: Twilio’s Ashburn, VA USA edge was used for this testing. Please refer to the following for a full list of Twilio Edge URLs [here](#).

Session Border Controller for Enterprise

Routing Profiles: TWILIO_Routing

Routing Profiles: default, Avaya_SM_routing, TWILIO_Routing

Routing Profile

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	Priority	tekvizion.pstn.ashburn.twilio.com:5060	UDP

Figure 54 Routing for twilio

4.5.6 End Point Policy Groups

End Point Policy Group for Avaya SM

- A new End Point Policy Group is created for Avaya Aura Session Manager.
- Navigate to: Domain Policies > End Point Policy Groups
- Select default-low under Policy Groups
- Click Clone
- Set *Clone Name*: Avaya SM
- Click Finish

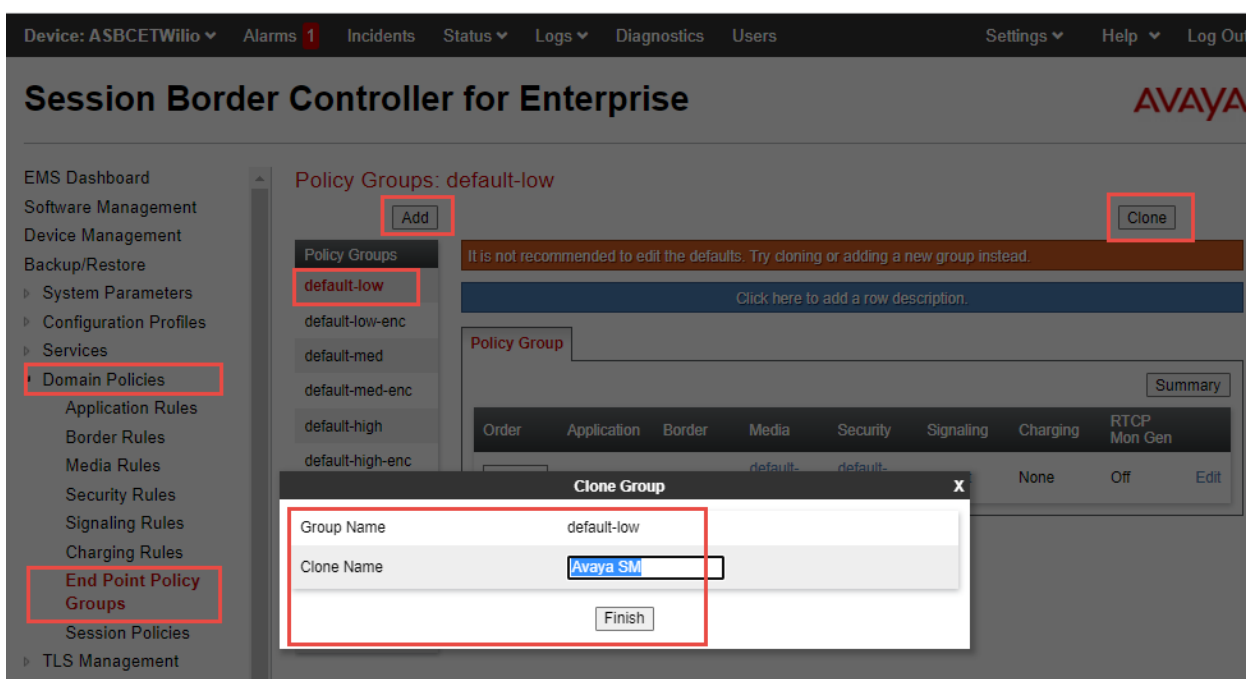


Figure 55 End Point Policy Group for Avaya SM

- Select the newly created Group Avaya SM, Click Edit
- Set *Signaling Rule*: Avaya SM
- Click Finish

Edit Policy Set	
Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	Avaya SM
Charging Rule	None
RTCP Monitoring Report Generation	Off

Finish

Figure 56 End Point Policy Group for Avaya SM Continuation

End Point Policy Group for twilio

- Repeat the same steps to create End Policy Group for twilio

The screenshot shows the Avaya Session Border Controller for Enterprise interface. At the top, there is a navigation bar with 'Device: ASBCETwilio', 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header reads 'Session Border Controller for Enterprise' with the 'AVAYA' logo on the right.

On the left is a navigation menu with categories like 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'Application Rules', 'Border Rules', 'Media Rules', 'Security Rules', 'Signaling Rules', 'Charging Rules', and 'End Point Policy Groups' (highlighted in red).

The main content area is titled 'Policy Groups: Twilio'. It features an 'Add' button and 'Rename', 'Clone', and 'Delete' buttons. Below these are two blue bars with instructions: 'Click here to add a description.' and 'Hover over a row to see its description.' A 'Policy Group' label is highlighted in red.

A 'Summary' button is located above a table. The table has the following data:

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	default	default	Twilio-mediarule	default-low	default	None	Off	Edit

Figure 57 End Point Policy Group for twilio

4.5.8 Network Management

- Navigate to: Network & Flows > Network Management > Interfaces.
- Interfaces which are enabled for Avaya LAN and Twilio are shown below

Session Border Controller for Enterprise

AVAYA

- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- Network & Flows
 - Network Management
 - Media Interface
 - Signaling Interface

Network Management

Interfaces

Networks

[Add VLAN](#)

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

Figure 58 Network Management Interfaces

- Navigate to: Network & Flows > Network Management > Networks.
- IP addresses which are configured for Avaya LAN and twilio interface are shown below

Device: ASBCETWilio ▾

Alarms 1

Incidents

Status ▾

Logs ▾

Diagnostics

Users

Settings ▾

Help ▾

Log Out

Session Border Controller for Enterprise

AVAYA

- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- Network & Flows
 - Network Management
 - Media Interface

Network Management

Interfaces

Networks

[Add](#)

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
LAN	10.89.33.1	255.255.255.0	A1	10.89.33.223	Edit Delete
WAN	192.65.79.129	255.255.255.128	B1	192.65.79.179	Edit Delete

Figure 59 Network Management Networks

Data-driven Customer engagement - at scale

Copyright © 2022, Twilio and/or its affiliates. All rights reserved. Twilio is a registered trademark of Twilio and/or its affiliates. Other names may be trademarks of their respective owners.

4.5.9 Media Interface

- Navigate to: Network & Flows > Media Interface.
- Set *Name*: Med_LAN is given here
- Set *IP Address*: Select LAN (A1, VLAN0) from the drop down and the IP address populates automatically. The IP address for Interface facing Avaya Aura SM is 10.89.33.223
- Set *Port Range*: 35000-40000

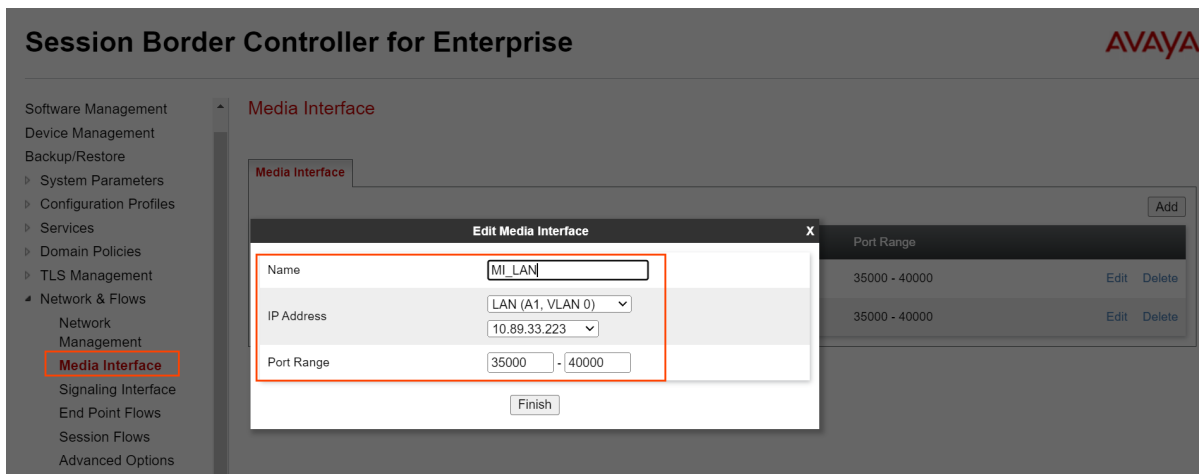


Figure 60 Media Interface facing Avaya SM

- Repeat the same steps to create a Media Interface facing twilio.

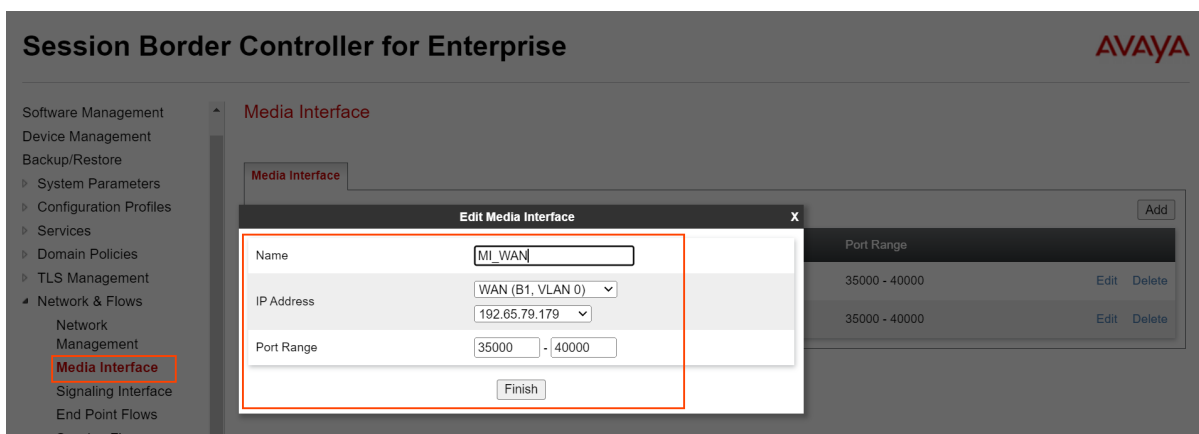


Figure 61 Media Interface facing twilio

4.5.10 Signaling Interface

- Navigate to: Network & Flows > Signaling Interface.
- Configure Signaling Interface towards Avaya SM LAN and twilio as shown below.

Signaling Interface

Signaling Interface Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
SI_LAN	10.89.33.223 LAN (A1, VLAN 0)	5060	5060	---	None	Edit Delete
SI_WAN	192.65.79.179 WAN (B1, VLAN 0)	5060	5060	---	None	Edit Delete

Figure 62 Signaling Interface facing Avaya SM LAN and twilio

4.5.11 Endpoint Flows

- Navigate to: Network & Flows > End Point Flows > Server Flows.

Session Border Controller for Enterprise

Software Management
Device Management
Backup/Restore
▸ System Parameters
▸ Configuration Profiles
▸ Services
▸ Domain Policies
▸ TLS Management
▸ **Network & Flows**
 Network Management
 Media Interface
 Signaling Interface
 End Point Flows
 Session Flows
 Advanced Options
▸ DMZ Services
▸ Monitoring & Logging

End Point Flows

Subscriber Flows **Server Flows** Add

Modifications made to a Server Flow will only take effect on new sessions.

[Click here to add a row description.](#)

SIP Server: Avaya SM

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Avaya SM	*	SI_WAN	SI_LAN	default-low	TWILIO_Routing	View Clone Edit Delete

SIP Server: twilio

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Twilio	*	SI_LAN	SI_WAN	default-low	Avaya_SM_routing	View Clone Edit Delete

Figure 63 Endpoint Flows

- Set *Flow Name*: Avaya SM
- Configure flow for Avaya SM LAN as shown below

Edit Flow: Avaya SM X

Flow Name	<input style="width: 90%;" type="text" value="Avaya SM"/>
SIP Server Profile	<input style="width: 90%;" type="text" value="Avaya SM"/>
URI Group	<input style="width: 90%;" type="text" value="*/"/>
Transport	<input style="width: 90%;" type="text" value="UDP"/>
Remote Subnet	<input style="width: 90%;" type="text" value="*/"/>
Received Interface	<input style="width: 90%;" type="text" value="SI_WAN"/>
Signaling Interface	<input style="width: 90%;" type="text" value="SI_LAN"/>
Media Interface	<input style="width: 90%;" type="text" value="MI_LAN"/>
Secondary Media Interface	<input style="width: 90%;" type="text" value="None"/>
End Point Policy Group	<input style="width: 90%;" type="text" value="default-low"/>
Routing Profile	<input style="width: 90%;" type="text" value="TWILIO_Routing"/>
Topology Hiding Profile	<input style="width: 90%;" type="text" value="Avaya_SM"/>
Signaling Manipulation Script	<input style="width: 90%;" type="text" value="None"/>
Remote Branch Office	<input style="width: 90%;" type="text" value="Any"/>
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	<input style="width: 90%;" type="text"/>

Figure 64 Endpoint Flows for Avaya SM LAN

- Set *Flow Name*: Twilio
- Configure flow for twilio as shown below

Flow Name	Twilio
SIP Server Profile	twilio
URI Group	*
Transport	UDP
Remote Subnet	*
Received Interface	SI_LAN
Signaling Interface	SI_WAN
Media Interface	MI_WAN
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Avaya_SM_routing
Topology Hiding Profile	Twilio
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	

Finish

Figure 65 Endpoint Flows for twilio

4.5.12 TLS Configuration

The following are necessary steps to modify the configuration from protocol UDP to TLS between Avaya SBCE and twilio

- Navigate to: TLS management > Certificates. Click Install
- Set *Type*: Select CA Certificate
- Set *Name*: globalrootCA
- Set *Allow weak Certificate/Key*: Checked
- Set *Certificate File*: Click Choose File to select twilio Root CA (received from twilio)
- Click Upload

Note: - Avaya SBCE has a limitation to consume the CA Bundle certificate, if you received CA bundle from your customer then need to split the certificates and upload individually.

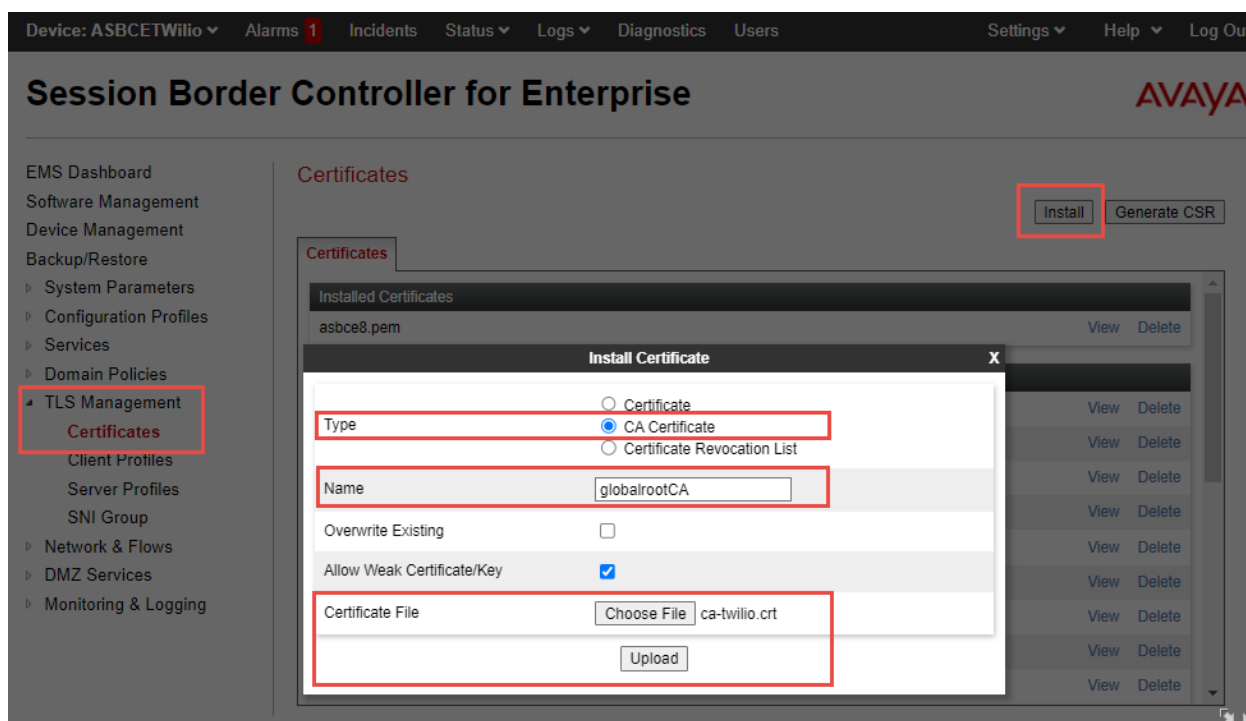


Figure 66 Upload twilio Root CA

Client Profile for twilio

- Navigate to: TLS management > Client Profiles. Click Add
- Set *Profile Name*: TWILIO is given for interface facing twilio
- Set *Certificate*: select server certificate asbce8.pem for Avaya SBCE interface facing twilio
- Set *Peer Certificate Authorities*: Select globalrootCA.crt which is uploaded in previous step
- Set *Verification Depth*: 5
- Click Next

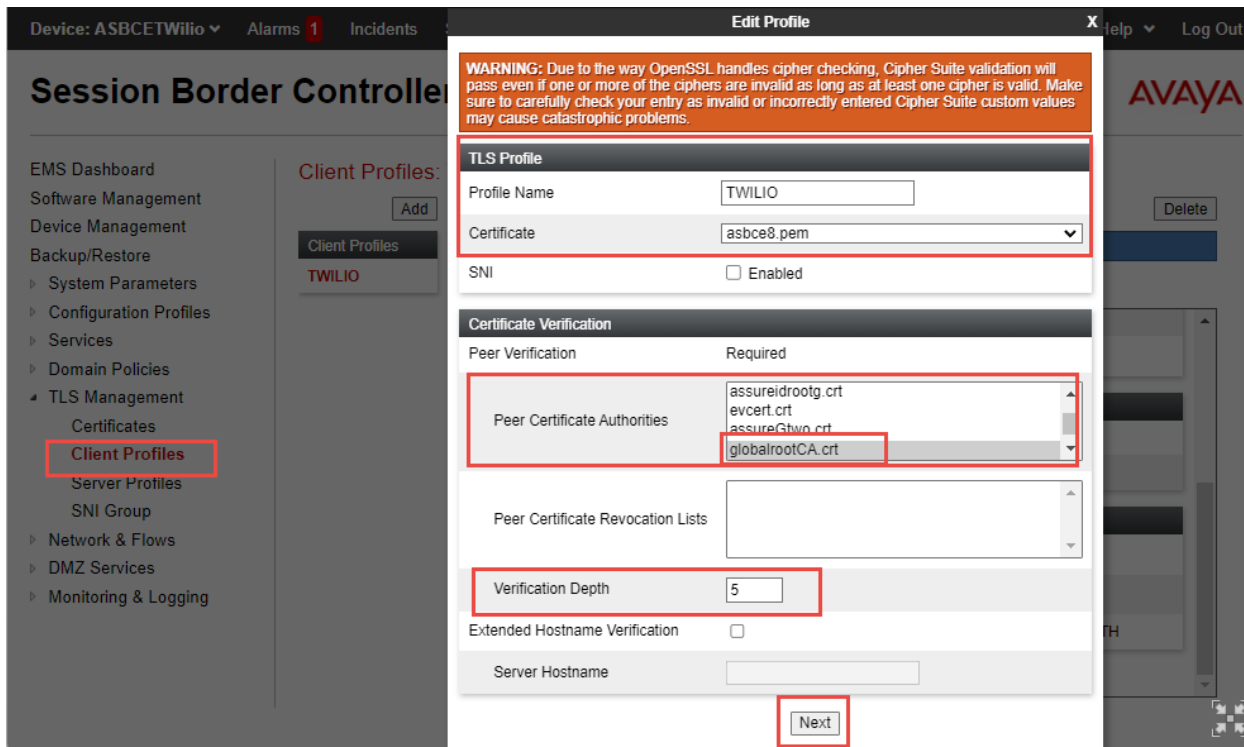
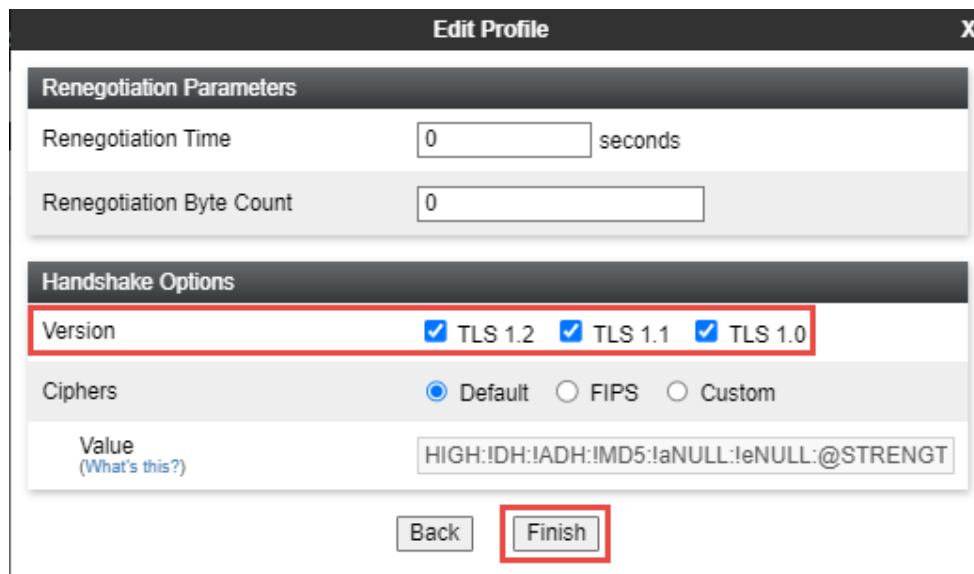


Figure 67 Client Profile facing twilio

- Set *Version*: Select all 3 TLS versions
- Click Finish



The screenshot shows a dialog box titled "Edit Profile" with a close button (X) in the top right corner. It is divided into two main sections: "Renegotiation Parameters" and "Handshake Options".

Renegotiation Parameters:

- Renegotiation Time: 0 seconds
- Renegotiation Byte Count: 0

Handshake Options:

- Version:** This section is highlighted with a red box. It contains three checked checkboxes: TLS 1.2, TLS 1.1, and TLS 1.0.
- Ciphers:** Includes radio buttons for Default, FIPS, and Custom.
- Value:** A text field containing the string "HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGT". A link "(What's this?)" is visible below the field.

At the bottom of the dialog, there are two buttons: "Back" and "Finish". The "Finish" button is highlighted with a red box.

Figure 68 Client Profile facing twilio Continuation

Server Profile for twilio

- Navigate to: TLS management > Server Profiles. Click Add
- Set *Profile Name*: TWILIO is given for interface facing twilio
- Set *Certificate*: Select server certificate asbce8.pem for Avaya SBCE interface facing twilio
- Set *Peer Verification*: None
- Click Next

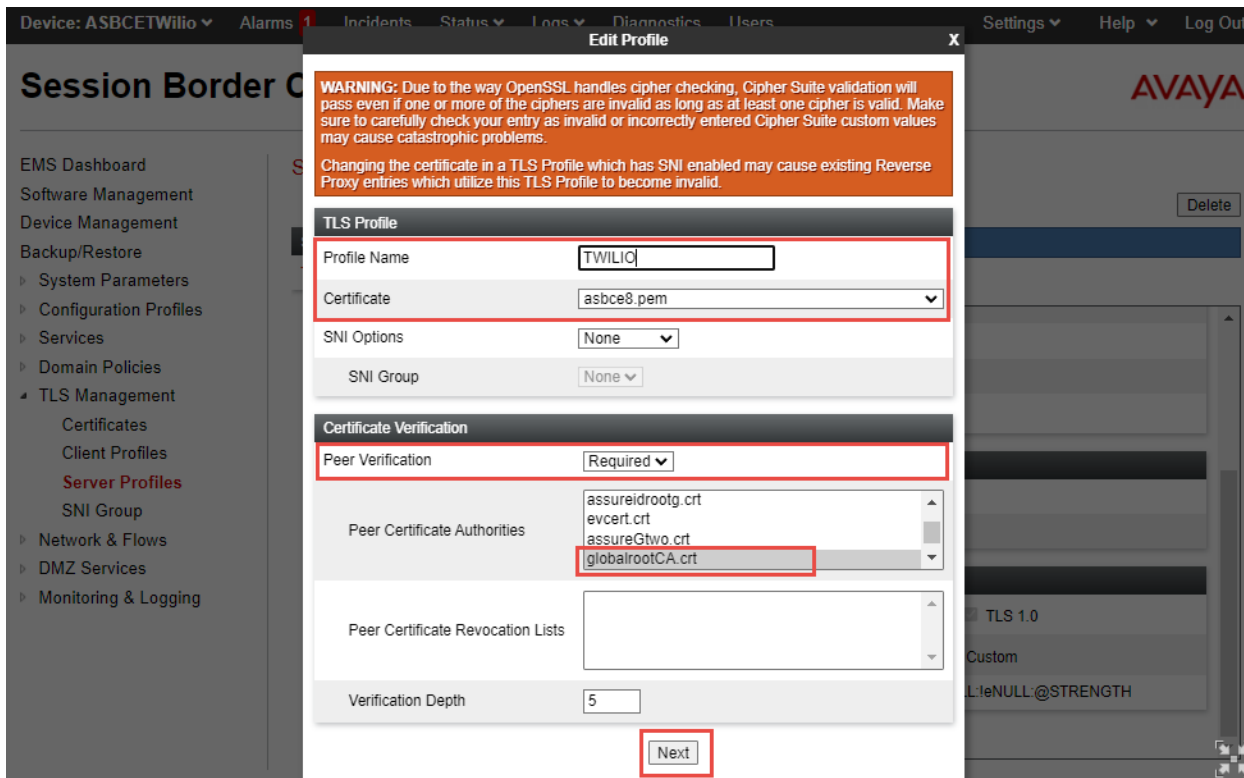


Figure 69 Server Profile facing twilio

- Set *Version*: Check all 3 TLS versions
- Click Finish

Edit Profile X

Renegotiation Parameters

Renegotiation Time seconds

Renegotiation Byte Count

Handshake Options

Version TLS 1.2 TLS 1.1 TLS 1.0

Ciphers Default FIPS Custom

Value (What's this?)

Figure 70 Server Profile facing twilio Continuation

Edit SIP Server

- Navigate to: Services > SIP Servers
- Under General tab, Click Edit
- Set *Transport*: Select TLS from Dropdown
- Set *Port*: 5061
- Set *TLS Client Profile*: Select Client Profile TWILIO
- Click Finish

SIP Servers: twilio

Add

Rename Clone Delete

Server Profiles

twilio

Avaya SM

Edit SIP Server Profile - General X

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type

SIP Domain

DNS Query Type

TLS Client Profile

Add

IP Address / FQDN / CIDR Range	Port	Transport	
tekvizion.pstn.ashburn.twilio.com	5061	TLS	Delete

Finish

Figure 71 SIP Server Profile – twilio

Configure SRTP

- Navigate to: Domain Policies > Media Rules
- Select Media Rule default-high-enc, Click Clone
- Set *Clone Name*: Twilio-mediarule
- Click Finish

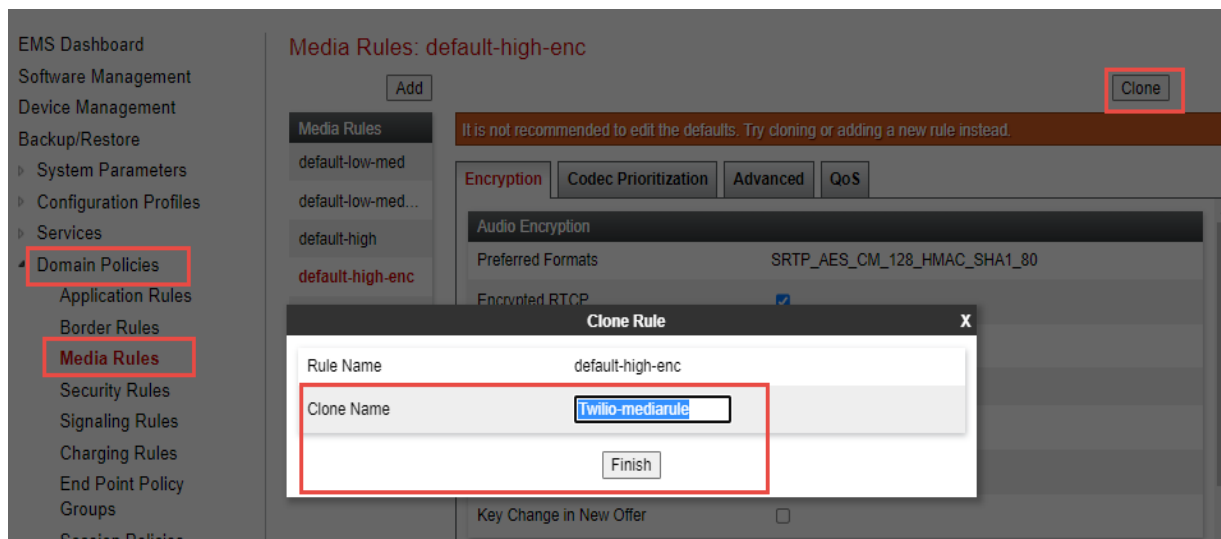


Figure 72 Media Rule – twilio

- Select newly created Media Rule Twilio-mediarule, Click Edit
- Set Preferred Format #1: SRTP_AES_CM_128_HMAC_SHA1_32
#2: SRTP_AES_CM_128_HMAC_SHA1_80
#3: SRTP_AES_192_CM_HMAC_SHA1_32
- Click Finish

Media Encryption X

Audio Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_32 ▼
Preferred Format #2	SRTP_AES_CM_128_HMAC_SHA1_80 ▼
Preferred Format #3	SRTP_AES_192_CM_HMAC_SHA1_32 ▼
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2 [^] <input style="width: 40px;" type="text"/>
Interworking	<input type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80 ▼
Preferred Format #2	NONE ▼
Preferred Format #3	NONE ▼
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime <small>Leave blank to match any value.</small>	2 [^] <input style="width: 40px;" type="text"/>
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous

Capability Negotiation	<input type="checkbox"/>
------------------------	--------------------------

Figure 73 Media Rule – twilio Continuation

Edit End Point Policy Groups

- Navigate to: Domain Policies > End Point Policy Groups
- Select Twilio under Policy Groups
- Click Edit

Policy Groups: Twilio

Add
Rename Clone Delete

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- avaya-def-low-e...
- avaya-def-high...
- avaya-def-high...
- Twilio
- Avaya SM

Click here to add a description.

Hover over a row to see its description.

Policy Group Summary

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	default	default	Twilio-mediarule	default-low	default	None	Off	Edit

Figure 74 Edit End Point policy Group – twilio

- Set *Media Rule*: Select Twilio-mediarule
- Click Finish

Figure 75 Edit End Point policy Group –twilio Continuation

Edit Signaling Interface

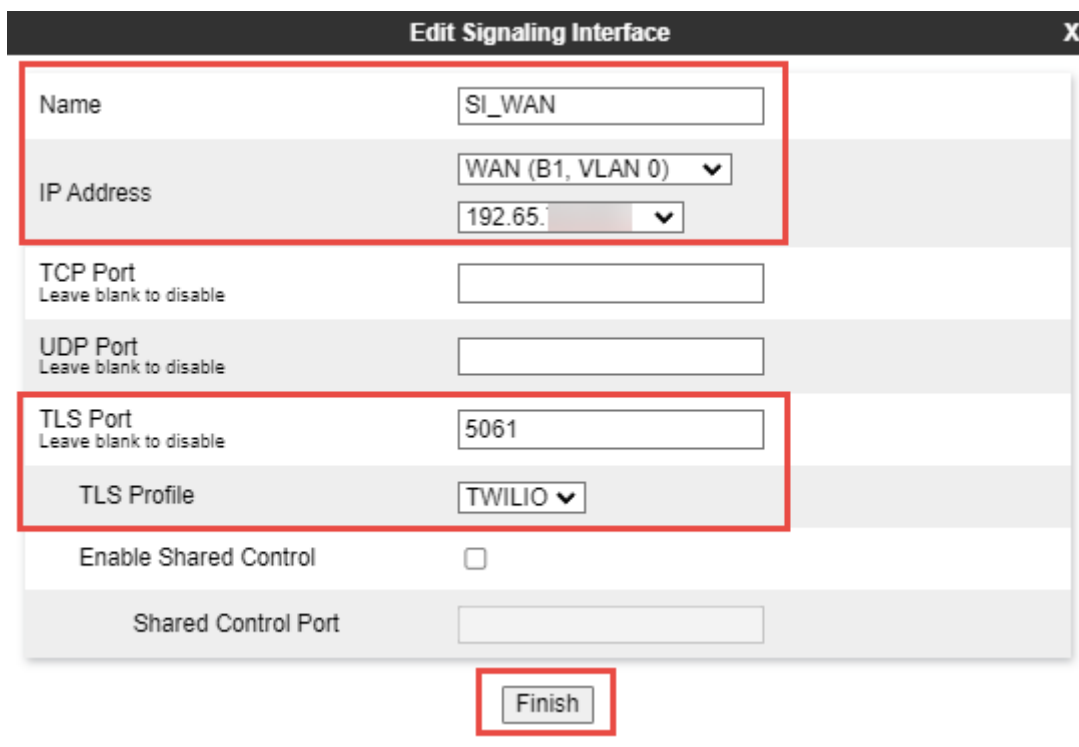
- Navigate to: Network & Flows > Signaling Interface
- Select interface SI_WAN
- Click Edit

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
SI_LAN	10.89.33.223 LAN (A1, VLAN 0)	---	5060	---	None	Edit Delete
SI_WAN	192.65.1.1 WAN (B1, VLAN 0)	---	---	5061	TWILIO	Edit Delete

Figure 76 Edit Signaling Interface – twilio

Set *TLS Port*: 5061

- Set *TLS Profile*: Select TWILIO
- Set *TCP/UDP Port*: Delete the values as only TLS is used.
- Click Finish



Name	SI_WAN
IP Address	WAN (B1, VLAN 0) 192.65.
TCP Port	
UDP Port	
TLS Port	5061
TLS Profile	TWILIO
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

Figure 77 Edit Signaling Interface – twilio continuation

Edit Server Flows

- Navigate to: Network & Flows > End Point Flows > Server Flows
- Select Server Flow Twilio, Click Edit

- EMS Dashboard
- Software Management
- Device Management
- Backup/Restore
- System Parameters
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- **Network & Flows**
 - Network Management
 - Media Interface
 - Signaling Interface
 - End Point Flows**
 - Session Flows
 - Advanced Options
- DMZ Services
- Monitoring & Logging

End Point Flows

Subscriber Flows **Server Flows** Add

Modifications made to a Server Flow will only take effect on new sessions.

Click here to add a row description.

SIP Server: Avaya SM

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Avaya SM	*	SI_WAN	SI_LAN	default-low	TWILIO_Routing	View Clone Edit Delete

SIP Server: twilio


Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	Twilio	*	SI_LAN	SI_WAN	Twilio	Avaya_SM_routing	View Clone Edit Delete

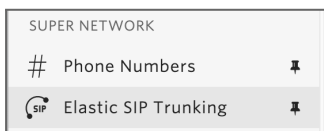
Figure 78 Edit Server Flow – twilio

- Set *Transport*: TLS
- Set *End Point Policy Group*: Select Twilio
- Click Finish

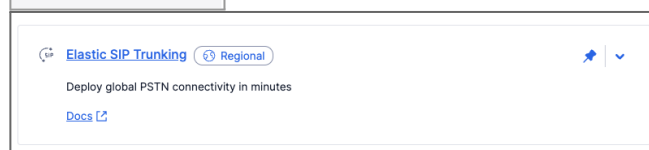
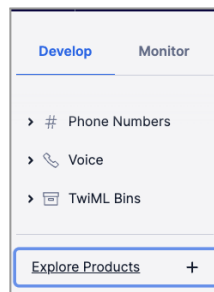
Figure 79 Edit Server Flow – twilio continuation

5 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).



If Elastic SIP Trunking is not visible via the navigation bar, select “Explore Products +”, locate Elastic SIP Trunking from the center of the screen and click the thumb pin icon. Doing this will add Elastic SIP Trunking to the navigation bar.



5.1 Create an IP-ACL rule

Click on Authentication in the left navigation, and then click on IP Access Control Lists.

The screenshot shows the Twilio console interface for configuring an IP Access Control List (ACL) named "TekVizion". The left navigation menu is open, with "IP access control lists" highlighted. The main content area shows the "Properties" section for the "TekVizion" ACL, including fields for "Friendly Name" (TekVizion) and "IP/ACL SID" (AL3200933ea3d280df1k3cb0k41a0710e6f). Below this, the "Associated SIP Trunks" section lists "tekvizion". The "Associated SIP Domains" section is empty. The "IP Address Ranges" section displays a table with two entries:

IP Address Range	Friendly Name
199.182.124.230 / 32 199.182.124.230-199.182.124.230	
192.65.79.179 / 32 192.65.79.179-192.65.79.179	My first Twilio project

Text to the right of the screenshot reads: "Create a new IP-ACL, for example the ACL list name used for this testing was 'Tekvizion', and add the public IP Addresses assigned to the Avaya SBCE(s)."

5.2 Create a new Trunk

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

The screenshot shows the Twilio console interface for creating a new SIP Trunk. The left navigation menu is open, with "Trunks" highlighted. The main content area shows the "Create A New SIP Trunk" dialog box. The dialog box has a title "Create A New SIP Trunk" and a close button (X). Below the title, there is a text input field labeled "FRIENDLY NAME" with the placeholder text "Name your new SIP Trunk, then configure it in the following steps." At the bottom of the dialog box, there are two buttons: "Cancel" and "Create".

Text to the right of the screenshot reads: "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. See [ESIPT documentation](#) for more information.

Develop
Monitor

Elastic SIP Trunking (US1)

← tekvizion

General

Termination

Origination

Numbers

General Settings

Friendly name

tekvizion 🗑️ ⓘ

A human readable descriptive text, up to 64 characters long.

Trunk SID

TKb0d4346968450156a0cdacd849fe625c 📄

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

Caller ID for Transfer Target

Set caller ID as Transferee ▼

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

In the Termination section, select a Termination SIP URI.

Develop
Monitor

Elastic SIP Trunking (US1)

← tekvizion

General

Termination

Origination

Numbers

Termination URI

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

Termination SIP URI

tekvizion 🗑️ .pstn.twilio.com

▶ **Show Localized URIs**

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

▼ Show Localized URIs

If you wish to manually connect to a specific geographic region, you may do so by pointing your communications infrastructure to any of the following localized Termination SIP URIs:

i Attention: We have updated the syntax for localized SIP hostnames to use our new Edge Locations.
[View legacy Termination SIP URIs](#)

North America Virginia	tekvision.pstn.ashburn.twilio.com
North America Oregon	tekvision.pstn.umatilla.twilio.com
Europe Dublin	tekvision.pstn.dublin.twilio.com
Europe Frankfurt	tekvision.pstn.frankfurt.twilio.com
South America Sao Paulo	tekvision.pstn.sao-paulo.twilio.com
Asia Pacific Singapore	tekvision.pstn.singapore.twilio.com
Asia Pacific Tokyo	tekvision.pstn.tokyo.twilio.com
Asia Pacific Sydney	tekvision.pstn.sydney.twilio.com

Figure 80 ESIPT Regional Edge URLs

[return to Avaya configuration](#)

Next, Assign the IP ACL (“Tekvizion”) that was 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

Tekvizion ×
× ▼
+

Credential Lists

Click to select a Credential List
▼
+

In the Origination section, we'll need to add Origination URI's to route traffic towards the Avaya SBCE. 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:

Develop Monitor

Elastic SIP Trunking (US1)

← tekvizion

General

Termination

Origination

Numbers

Origination

Incoming traffic to your communications infrastructure from the PSTN.

Origination URIs

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

► Show more about provisioning for high service availability

ORIGINATION URI	PRIORITY	WEIGHT	ENABLED	
sip:192.65.79.180;edge=umatilla	10	10	✓	×
sip:192.65.79.179;edge=ashburn	10	10	✓	×

Add Origination URL

Origination SIP URI
sip:192.65.79.179;edge=ashburn

Priority
10
Numeric range from 0 to 65535.

Weight
10
Numeric range from 1 to 65535.

Enabled
 enabled

Cancel Save

Add Origination URL

Origination SIP URI
sip:192.65.79.180;edge=umatilla

Priority
10
Numeric range from 0 to 65535.

Weight
10
Numeric range from 1 to 65535.

Enabled
 enabled

Cancel Save

5.2 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.

The screenshot shows the Twilio console interface for the 'tekvizion' trunk. The left sidebar contains navigation options: Develop, Monitor, Elastic SIP Trunking (US1), and a list of settings including General, Termination, Origination, and Numbers (which is highlighted). The main content area is titled 'Numbers' and features a search filter for 'Number' with the value '+1415GETTWLO'. Below the filter is a table of associated phone numbers.

<input type="checkbox"/>	Number	Friendly Name	Emergency Address Status	Emergency Address	Country	
<input type="checkbox"/>	+18149260011	(814) 926-0011	Registered	375 Beale St. Ste. 300, San Francisco, CA, 94105	United States	View details
<input type="checkbox"/>	+15675220022	(567) 522-0022	Unregistered	-	United States	View details
<input type="checkbox"/>	+447403922739	447403922739	Unregistered	-	United Kingdom	View details
<input type="checkbox"/>	+15407810033	(540) 781-0033	Unregistered	-	United States	View details

6 TekVizion

[tekVizion Labs™](#) is an independent testing and Verification facility offered by tekVizion PVS, Inc. (“tekVizion”). tekVizion Labs™ offers several types of testing services including:

- Remote Testing – provides secure, remote access to certain products in tekVizion Labs for pre-Verification and ad hoc testing
- Verification Testing – Verification of interoperability performed on-site at tekVizion Labs between two products or in a multi-vendor configuration
- Product Assessment – independent assessment and verification of product functionality, interface usability, assessment of differentiating features as well as suggestions for added functionality, stress and performance testing, etc.

tekVizion is a systems integrator specifically dedicated to the telecommunications industry. Our core services include consulting/solution design, interoperability/Verification testing, integration, custom software development and solution support services. Our services helps service providers achieve a smooth transition to packet-voice networks, speeding delivery of integrated services. While we have expertise covering a wide range of technologies, we have extensive experience surrounding our practice areas which include: SIP Trunking, Packet Voice, Service Delivery, and Integrated Services.

The tekVizion team brings together experience from the leading service providers and vendors in telecom. Our unique expertise includes legacy switching services and platforms, and unparalleled product knowledge, interoperability and integration experience on a vast array of VoIP and other next-generation products. We rely on this combined experience to do what we do best: help our clients advance the rollout of services that excite customers and result in new revenues for the bottom line. tekVizion leverages this real-world, multi-vendor integration and test experience and proven processes to offer services to vendors, network operators, enhanced service providers, large enterprises and other professional services firms. tekVizion’s headquarters, along with a state-of-the-art test lab and Executive Briefing Center, is located in Plano, Texas.

For more information on tekVizion and its practice areas, please visit tekVizion Labs website at www.tekVizion.com