Twilio Elastic SIP Trunking Configuration Guide

Cisco CUCM 12.5(SU1) with Cisco vCUBE 14.1

June 2021

Document History

Rev. No.	Description
1.0	Twilio Elastic SIP Trunking Configuration Guide
1.1	Updated based on the feedback from Twilio

Table of Contents

Table of Figures

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 Trunk, Virtual Cisco Unified Border Element (vCUBE), and Cisco Unified Communications Manager (CUCM).

2 Document Overview

This configuration guide provides steps for configuring a Twilio Elastic SIP Trunk to a **Virtualized Cisco Unified Border Element (vCUBE)**. The **Cisco Unified Communication Manager (CUCM)** was also validated and used throughout this testing.

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 UBE and Cisco UCM

Cisco Unified Border Element (CUBE) and Cisco Unified Call Manager (CUCM provide 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 Cisco UBE (CUBE) in an enterprise Cisco UCM (CUCM) 14.1 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 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.
For additional information on CUCM 12.5, please refer to: Cisco UCM 12.5 Information
For additional information on CUBE 14.1, please refer to: Cisco UBE 14.1 information

2.3 tekVizion Labs

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

3 Validation Network Components

The network for the Twilio Elastic SIP Trunk, vCUBE, and CUCM reference configurations is illustrated below:

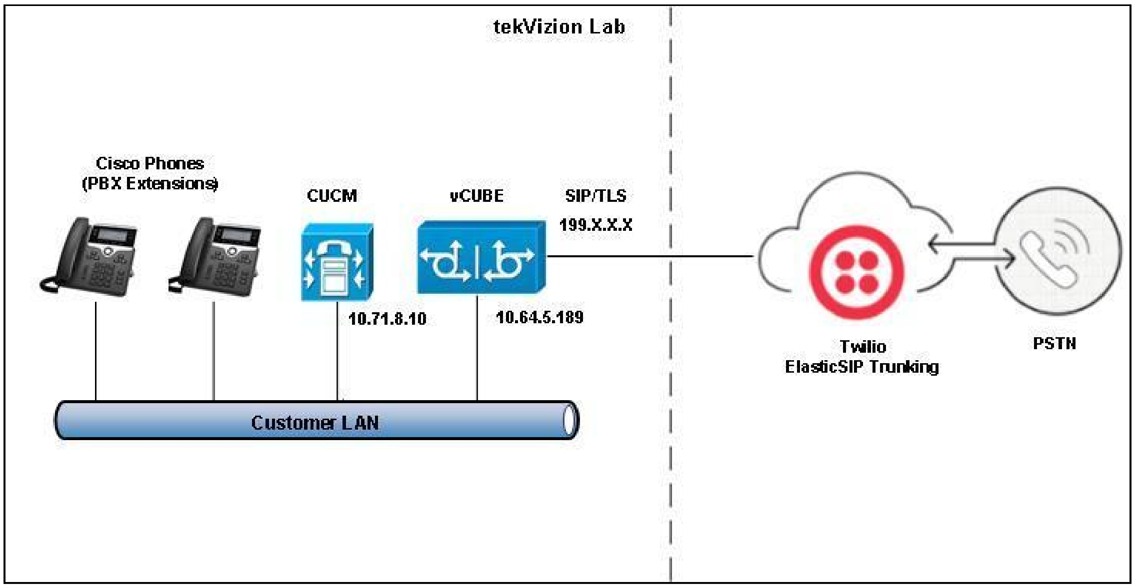


Figure 1 Network Topology

3.1 Hardware Components (vCUBE and CUCM)

- UCS-C240 VMWare server running ESXi 5.5.0 used for CUCM
- UCS-C240 VMWare server running ESXi 6.7.0 used for vCUBE
- Cisco IP Phone 9971 and 7941G

3.2 Software Requirements (vCUBE and CUCM)

- CUCM v12.5.1.13900-152
- vCUBE v14.1 (SW Version: 17.3.3, Platform CSR1000v)

4 Features

4.1 Features Supported

- OPTIONS
- Basic Outbound Calls
- Basic Inbound Calls
- Calls with RTCP enabled and disabled (Both US and EMEA trunk)
- Mute/Unmute
- Call Cancellation
- Ringing Timeout
- User Busy
- Calling Invalid Extension
- Codec scenarios (G711/G729/OPUS)
- Fax (G711-Passthrough)
- DTMF (RFC2833)
- Toll-free call: 1-800-XXX-XXXX
- Emergency call
- ONND scenarios
- Anonymous call
- Hold/Resume (with/without MOH)
- Session Refresh
- Call Forward (CFA/CFNA/CFB)
- Transfer (Blind/Consultative)
- Conference
- Route Crankback
- Call Admission Control

4.2 Features Not Supported by vCUBE

- CSR vCUBE does not support transcoding. Consequently the following scenarios could not be executed
    - DTMF Inband (CUCM does not generate Inband for vCUBE to passthrough)

4.3 Caveats and Limitations

- The following Twilio data centers were used for the testing.
    - Twilio Public Ashbun, VA and Umatilla, OR edge
        - tekvizion.pstn.ashburn.twilio.com or tekvizion.pstn.twilio.com (for US trunk)
        - tekvizion.pstn.umatilla.twilio.com (for route crankback)
        - tekvizion.pstn.dublin.twilio.com (for EMEA trunk)
- It is required to confirm that the CSR nvram store contains “ios_core.p7b” certification bundle and there is no associated trustpoint configured.
- The entire test was executed only on TLS/SRTP. The TLS connection was only between vCUBE and Twilio.
- By design, Twilio includes a Diversion header for inbound calls. For the PBX call forward scenarios, as CUCM would also add Diversion during call forward, there were 2 Diversion headers in the call forwarded INVITE.
- CUCM was configured to generate Comfort Noise packets and vCUBE passed through the packets through Twilio.
- The RTCP disabled scenario were executed disabling RTCP on the CUCM

5 Configuration

5.1 Configuration Checklist

In this section we present an overview of the steps that are required to configure **CUCM and vCUBE** for SIP Trunking with **Twilio Elastic SIP Trunking.**

Table 1: PBX Configuration Steps

Steps	Description	Reference
Step 1	CUCM Configuration	Section 5.3
Step 2	vCUBE Configuration	Section 5.4

5.2 IP Address Worksheet

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.

Table 2 – IP Addresses

Component	Lab Value	Customer Value
vCUBE		
LAN IP Address	10.64.5.189	
LAN Subnet Mask	255.255.0.0	
CUCM		
IP Address	10.71.8.10	
Subnet Mask	255.255.0.0	

5.3 CUCM Configuration

This section leverages screen shots taken from CUCM used for the interoperability testing to provide a general overview of the PBX configuration.

5.3.1 CUCM Login and Version

Open an instance of a web browser and connect to the CUCM using the following address: https://<CUCMIP>

Log in using an appropriate user ID and password. Verify the system version being tested.

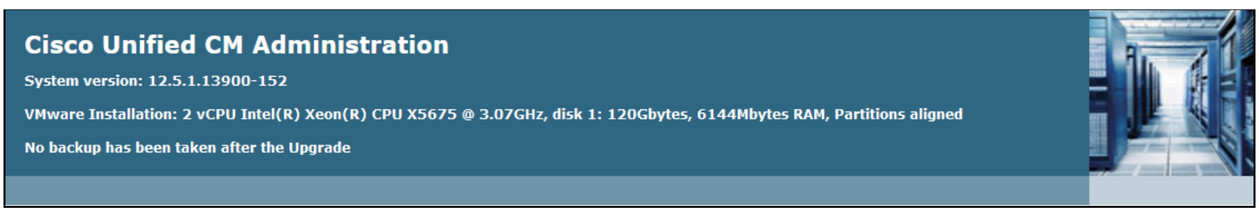


Figure 2: CUCM software version

5.3.2 CUCM SIP Profile Configuration

A new SIP Profile **Standard SIP Profile Twilio** was configured.

To add a new SIP Profile, from the **Device** drop down menu,

1. Navigate to **Device Settings** **SIP Profile**.
2. On the screen that appears, click **Add New** and configure the SIP Profile as below.
3. Then click **Save** and then **Apply Config**

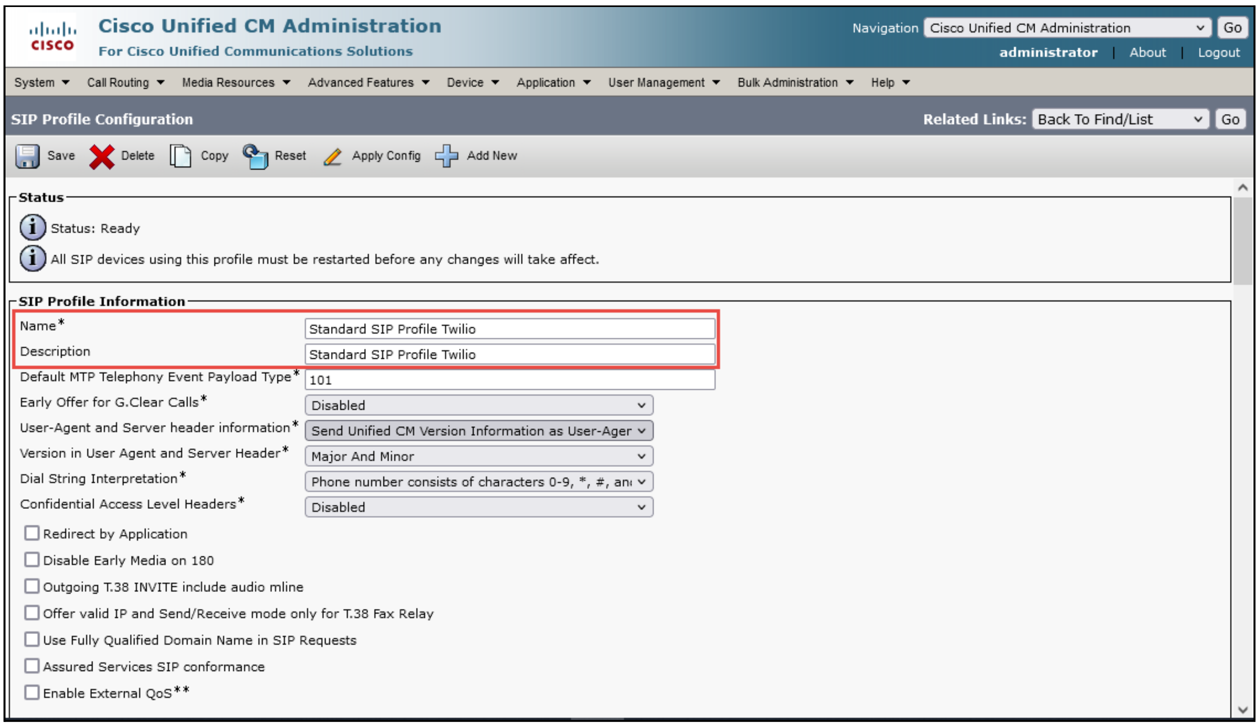


Figure 3 CUCM SIP Profile

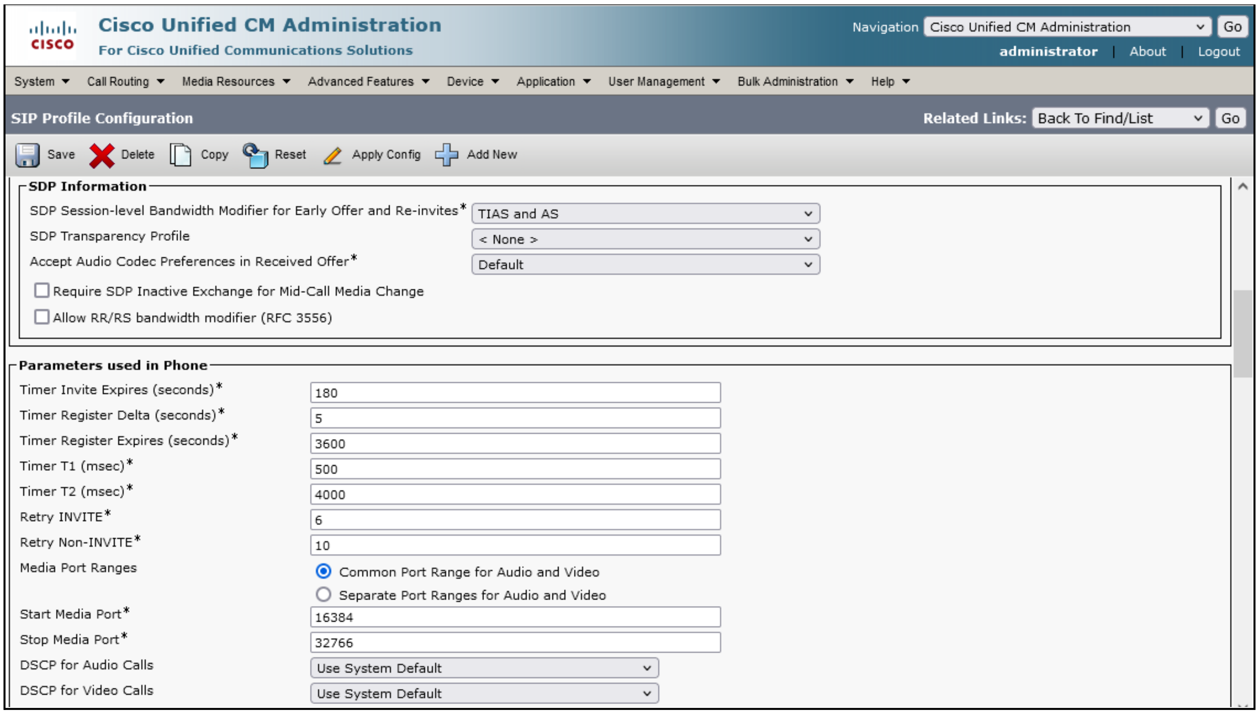


Figure 4 CUCM SIP Profile Contd.

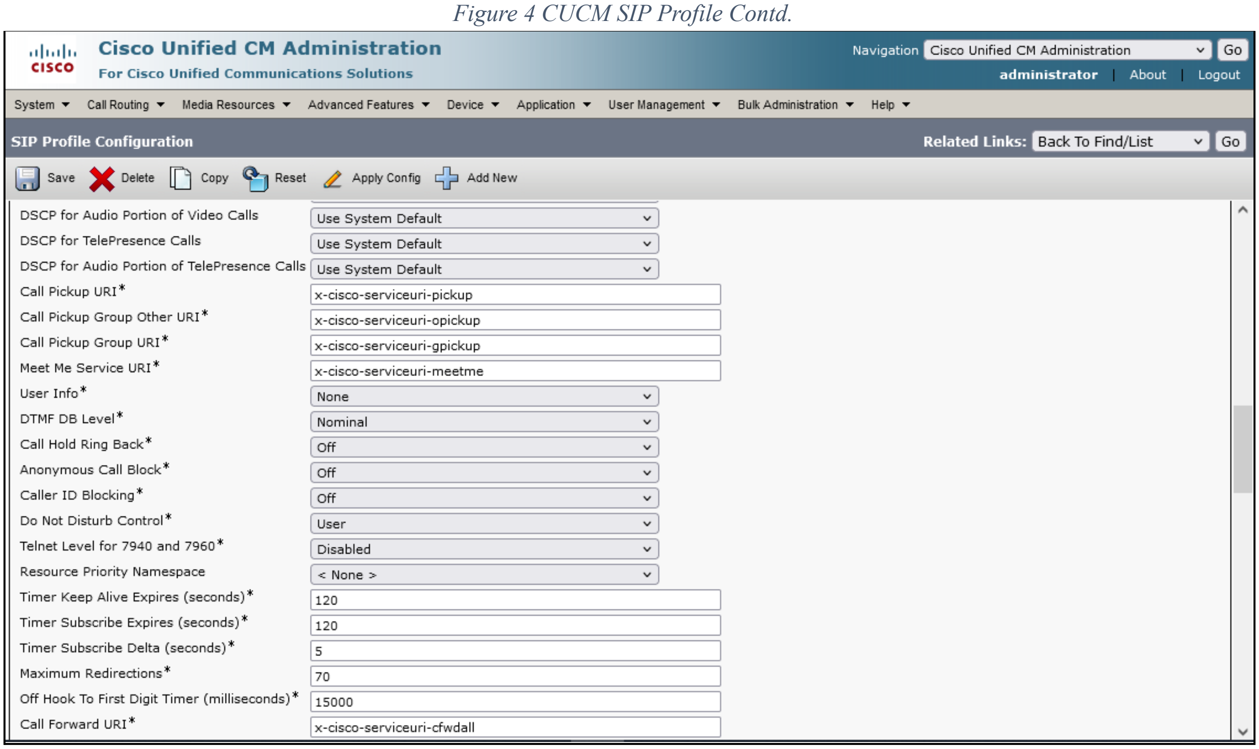


Figure 5 CUCM SIP Profile Contd.

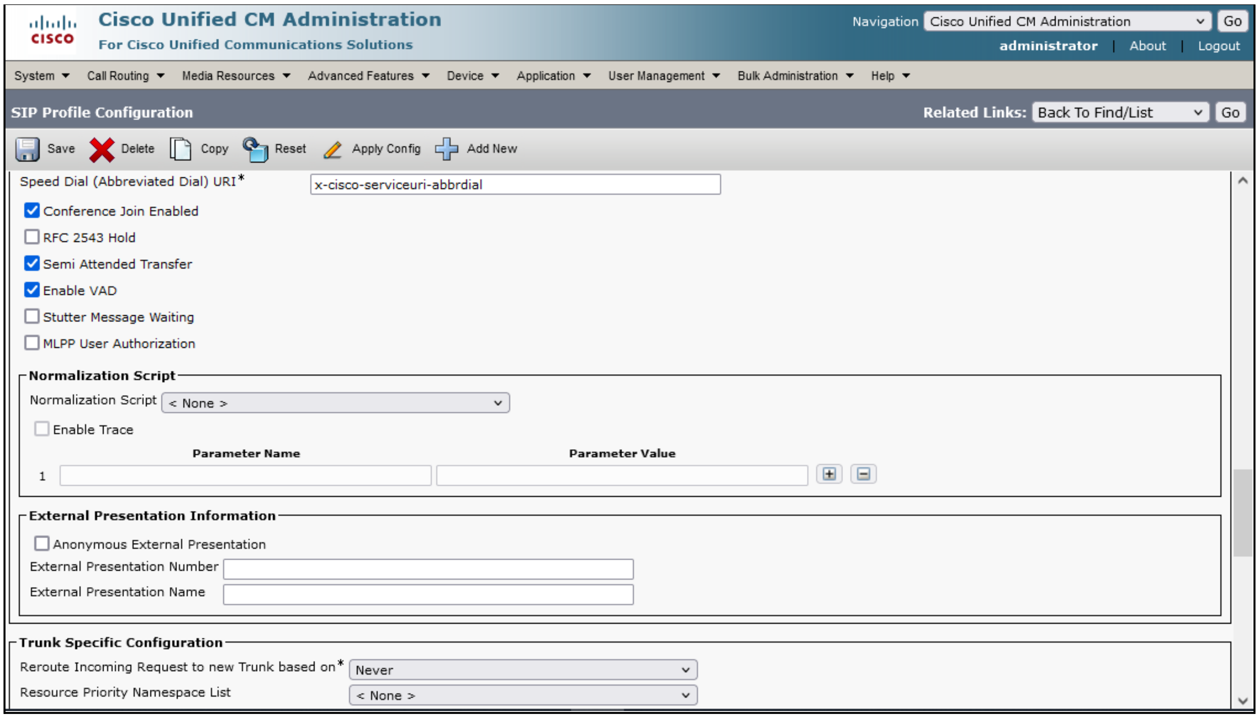


Figure 6 CUCM SIP Profile Contd.

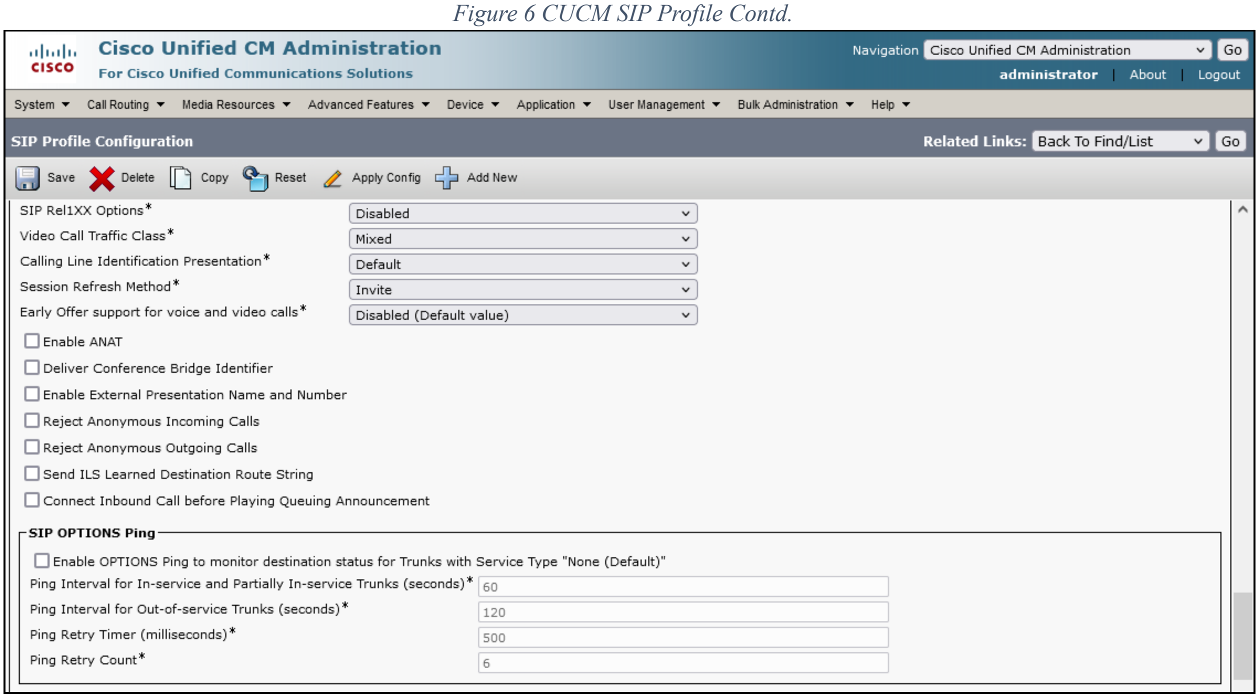


Figure 7 CUCM SIP Profile Contd.

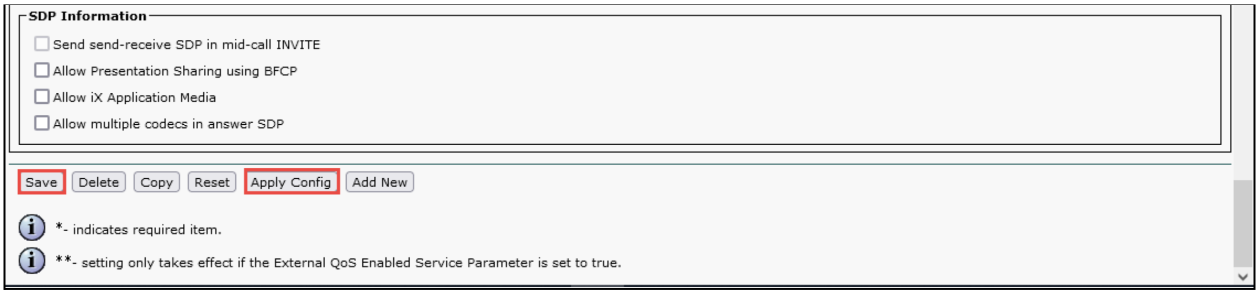


Figure 8 CUCM SIP Profile Contd.,

5.3.3 CUCM Device Pool Configuration

5.3.3.1 Codec Preference list

1. Navigate to **System** **Region Information** **Audio Codec Preference List**
2. Click **Add New**
3. Provide a Name and Description: **G711_Preferred Codec List** was used
4. Prioritize codecs as shown below

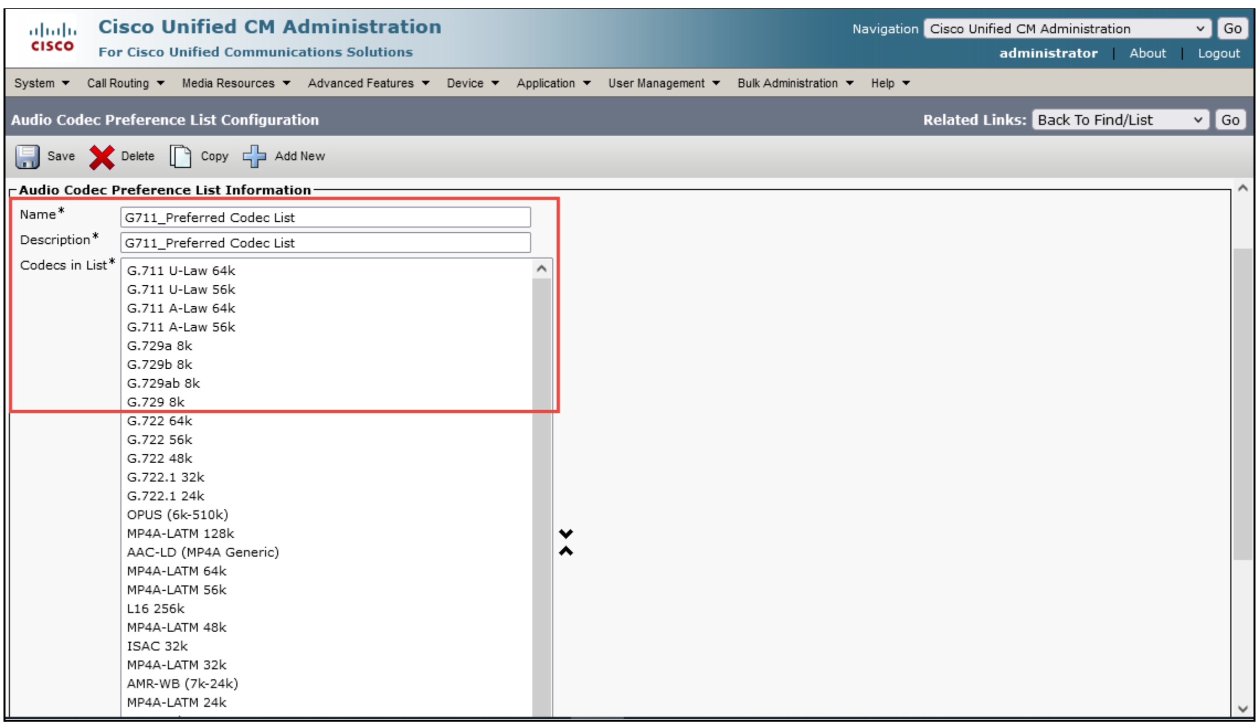


Figure 9 CUCM Audio Codec Preference List

5.3.3.2 Region

1. Navigate to **System** **Region**
2. Click **Add New**
3. Provide a Name: **G711_Region** was used in this test (see list of [Twilio Elastic SIP Trunking codecs here](#))
4. Associate the codec preference list **G711_Preferred Codec List** to this Region

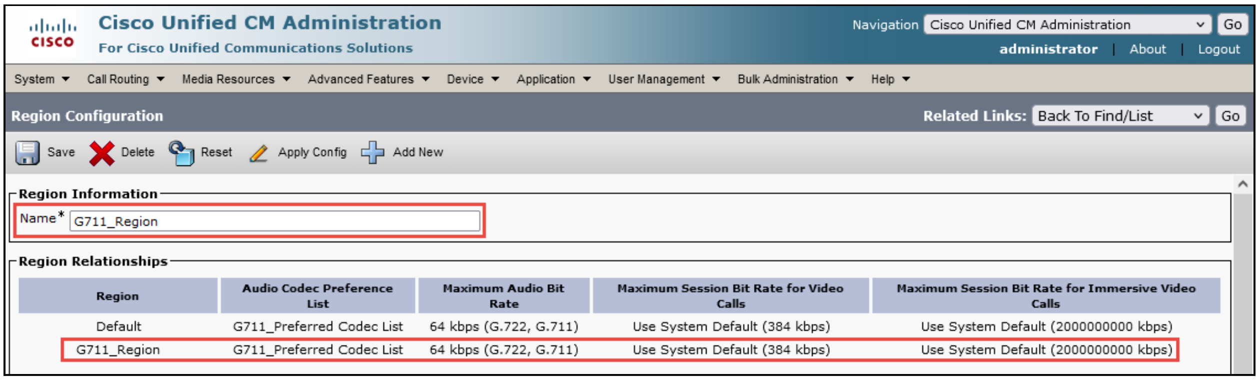


Figure 10 CUCM Region

5.3.3.3 Device Pool

1. Navigate to **System** **Device Pool**
2. Click **Add New**
3. Provide a Device Pool Name: **G711_pool** was used
4. Associate the Region: **G711_Region** to this Device Pool
5. Associate the Media resource Group List: **MRGPL**
6. Leave all other parameters at their default settings
7. Click **Save**

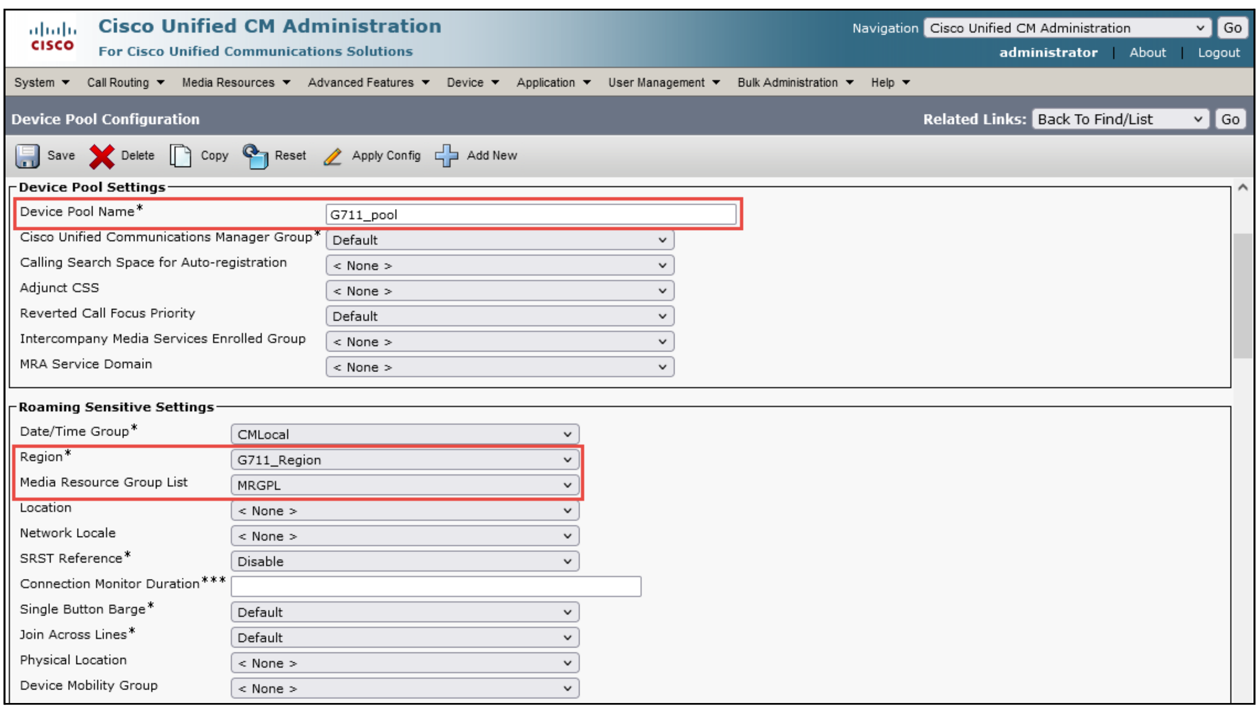


Figure 11 CUCM Device Pool

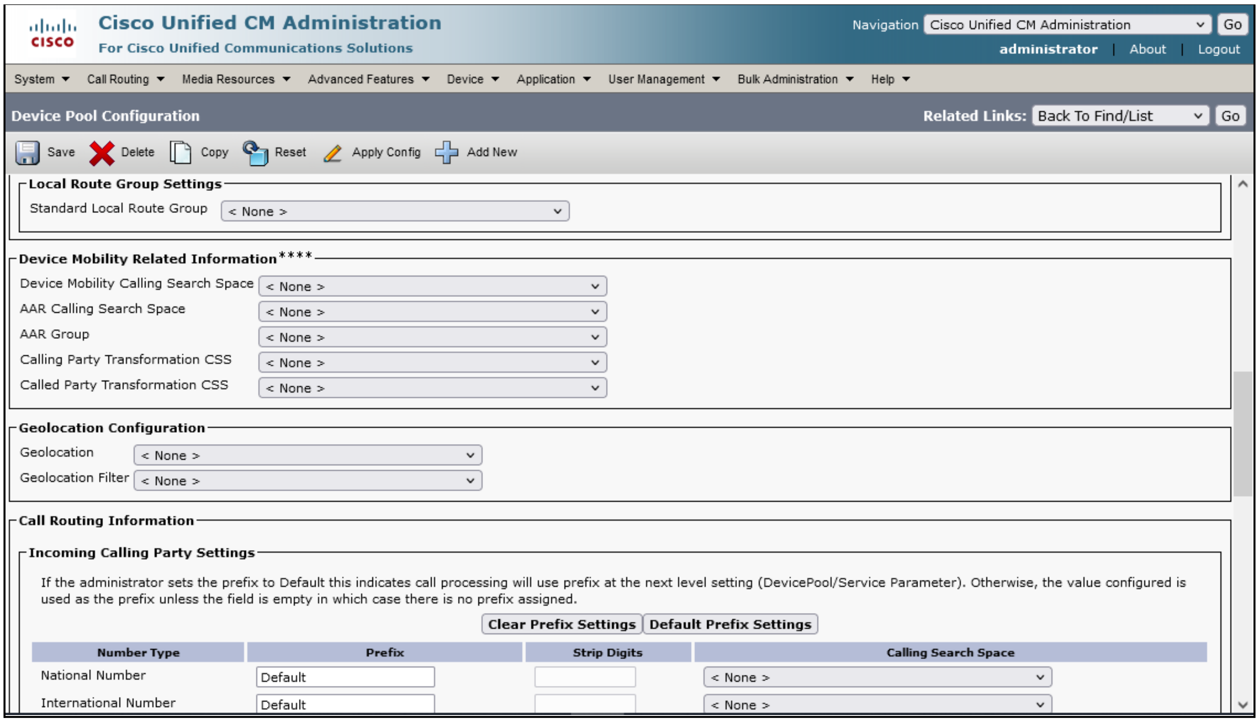


Figure 12 CUCM Device Pool Contd.

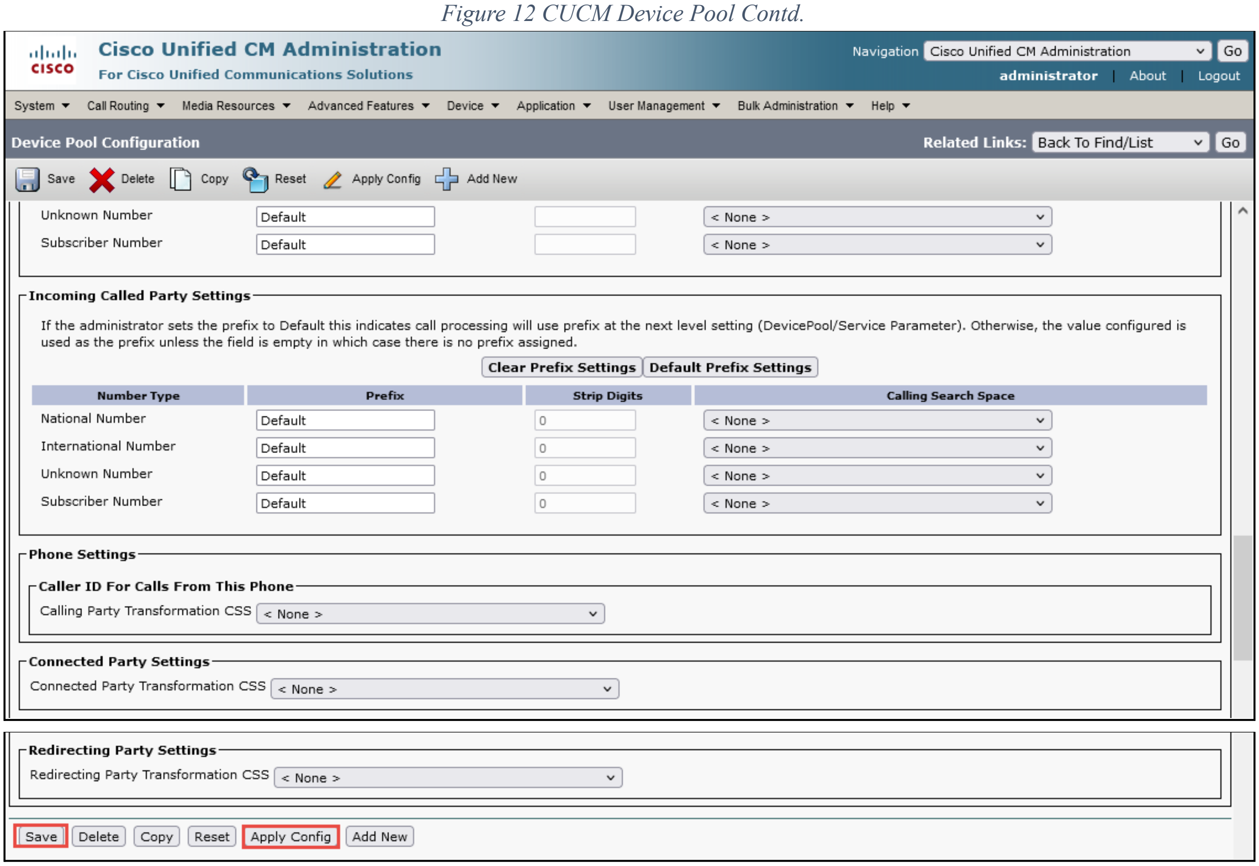


Figure 13 CUCM Device Pool Contd.

5.3.4 Media Resources

5.3.4.1 Media Resources Group

1. Navigate to Media Resources -> Media Resource Group.
2. Add New.
3. Provide a Name: **MRGP** was used
4. Select Media Resources from the Available Media Resources. (these are assumed to be added earlier and are available for use /registered with this CUCM)

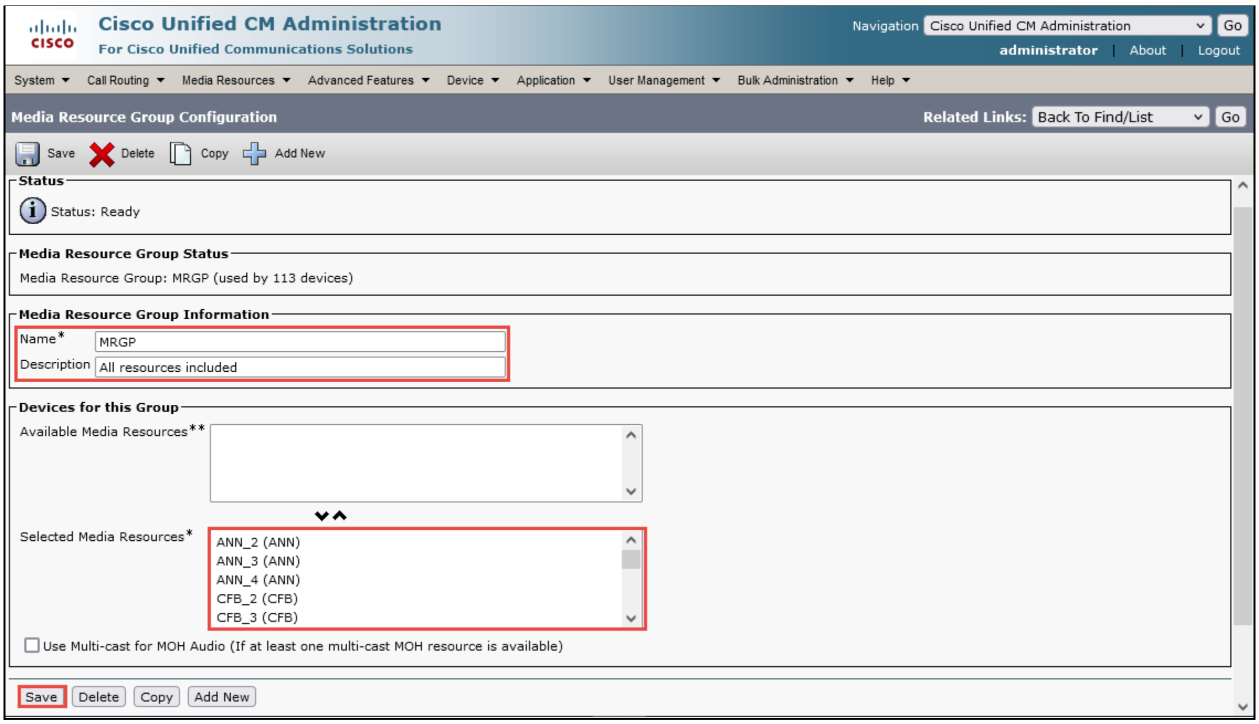


Figure 14 CUCM Media Resources Group

5.3.4.2 Media Resources Group List

1. Navigate to **Media Resources** **Media Resource Group List**
2. **Add New**.
3. Provide a Name: **MRGPL** was used
4. Select the media resource group **MRGP** from the list of Available Media Resource Groups

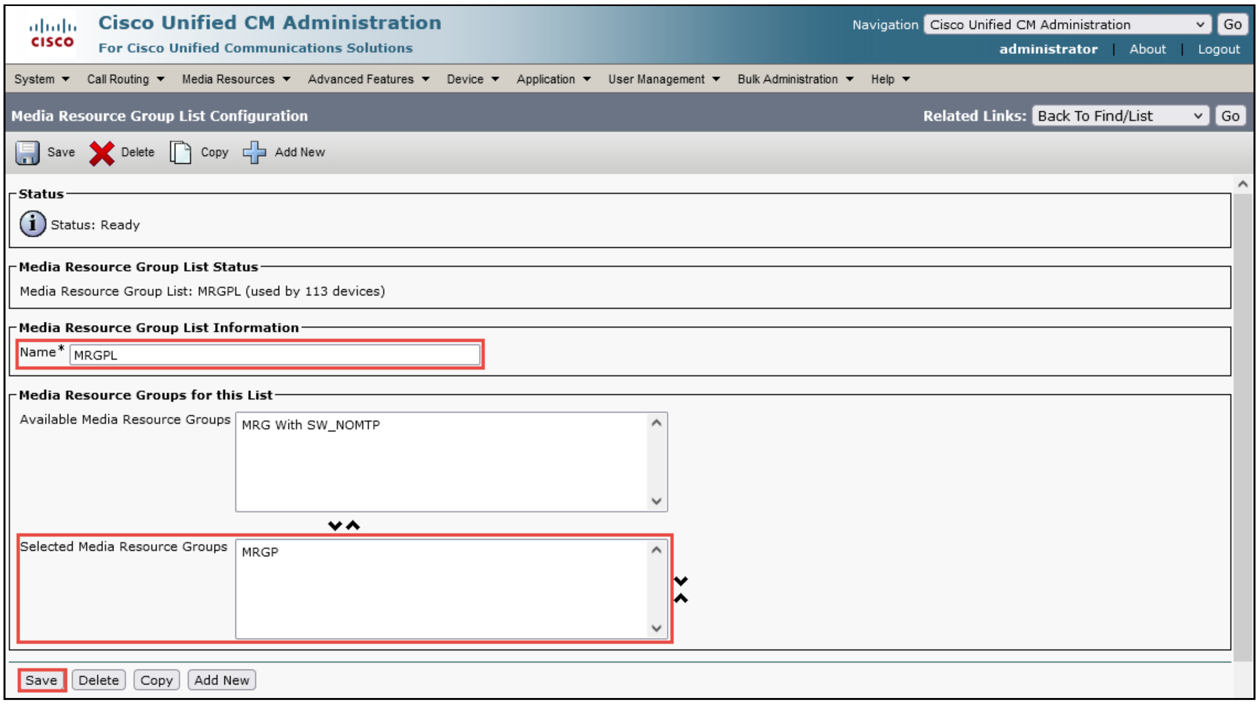


Figure 15 CUCM Media Resources Group List

5.3.5 Twilio SIP Trunk Security Profile

1. Navigate to: **System Security Non Secure SIP Trunk Profile**
2. Provide a Name: **Non Secure SIP Trunk Profile-Twilio** was used for this test
3. Provide a Description: **Non Secure** was used for this test
4. Select Incoming Transport Type: **TCP+UDP** was used in this test
5. Select Outgoing Transport Type: **UDP** was used in this test
6. Select Incoming Port: 5060
7. Click Save and Apply Config

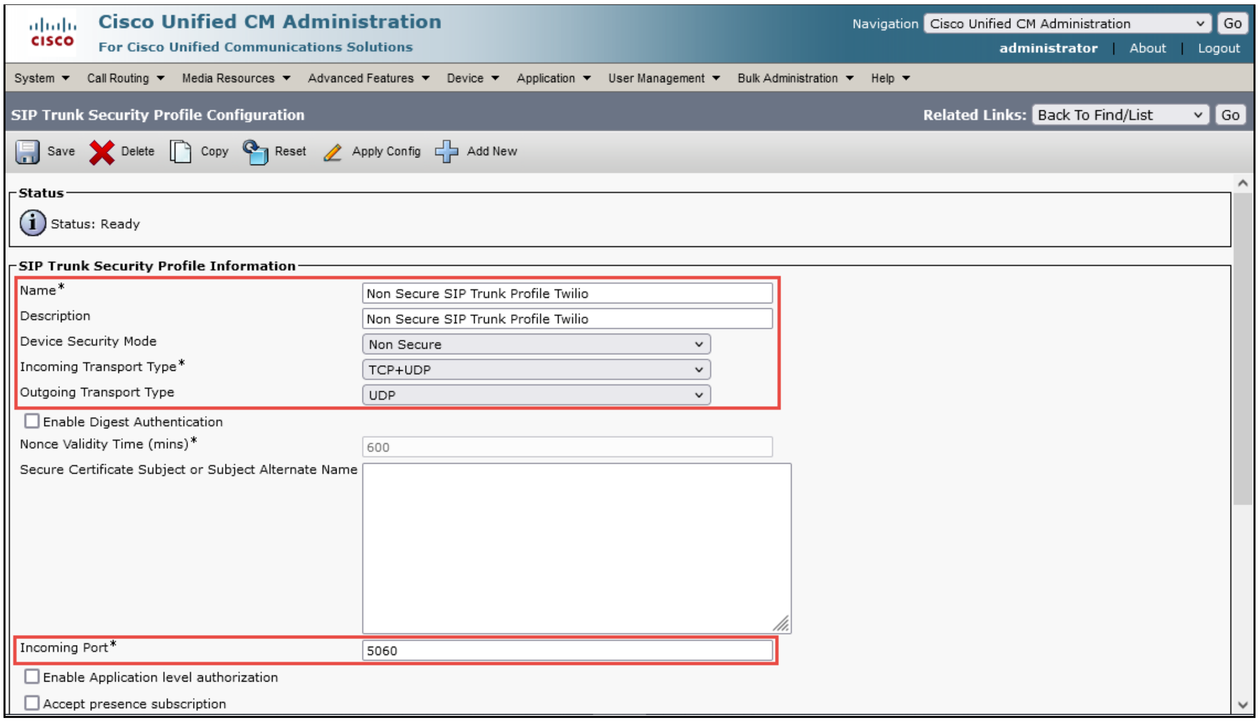


Figure 16 CUCM SIP Trunk Security Profile

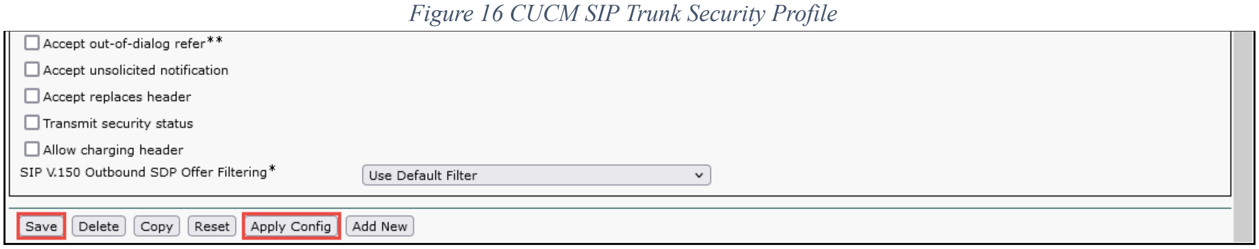


Figure 17 CUCM SIP Trunk Security Profile Contd.

5.3.6 Twilio SIP Trunk to vCUBE

1. Navigate to **Device** **Trunk**
2. Provide a **Device Name**: Trunk-CUBE-Twilio was used in this test
3. Provide a **Description**: SIP Trunk to CUBE for Twilio was used
4. Set **Device Pool**: G711_pool
5. Set **Media Resource Group List**: MRGPL
6. Set **Significant Digits**: 4
7. Set **Destination Address**: Set IP address of vCUBE
8. Set **SIP Trunk Security Profile**: Non Secure SIP Trunk Profile
9. Set **SIP Profile**: Standard SIP Profile Twilio
10. Set **DTMF Signaling Method**: No Preference

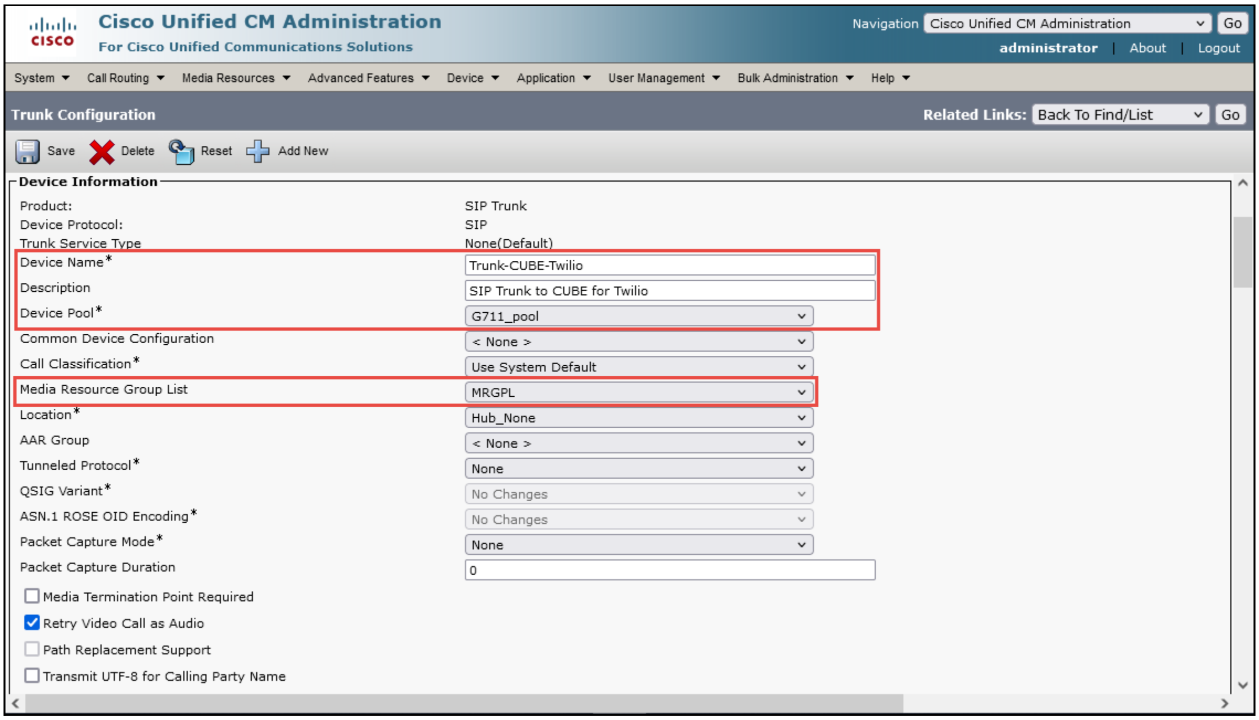


Figure 18 CUCM SIP Trunk Configuration

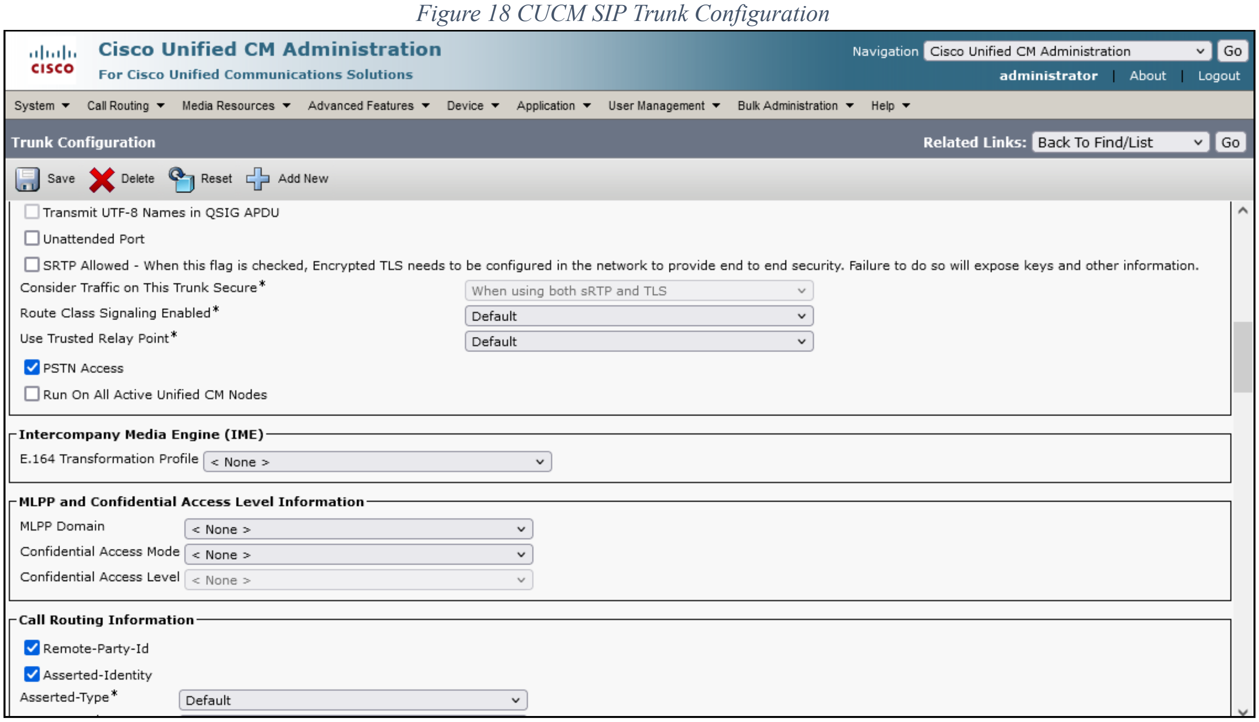


Figure 19 CUCM SIP Trunk Configuration Contd.

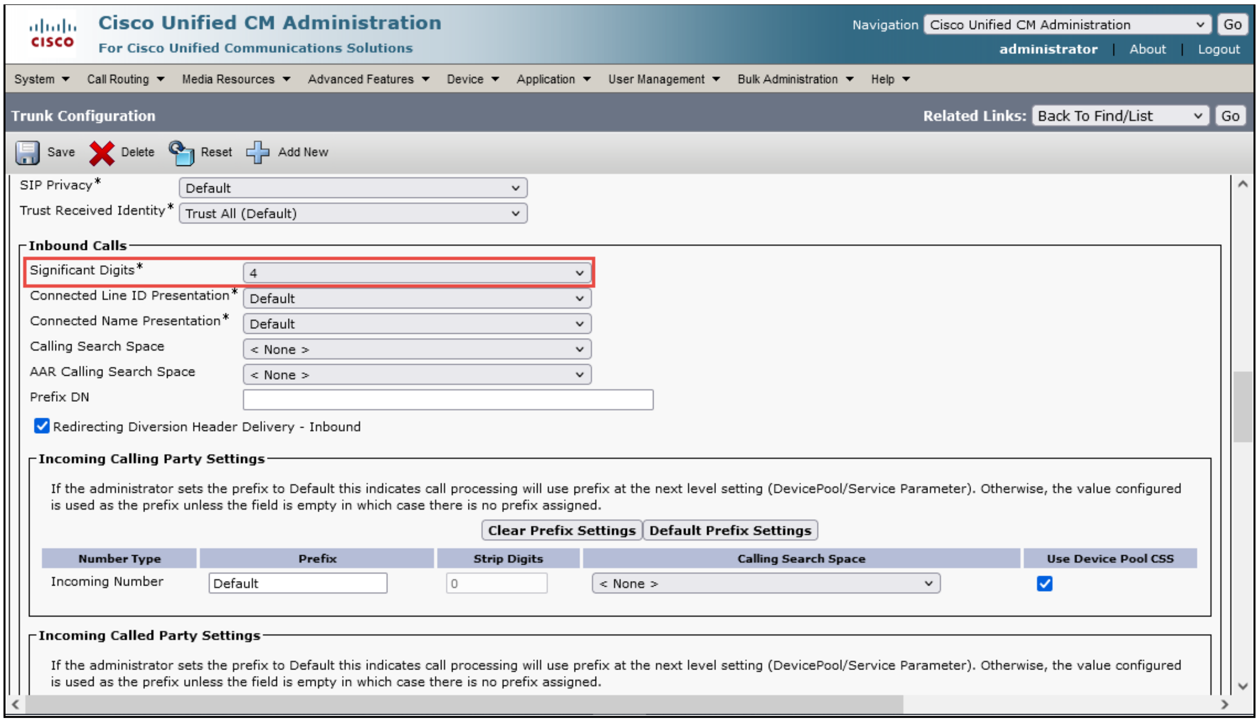


Figure 20 CUCM SIP Trunk Configuration Contd.

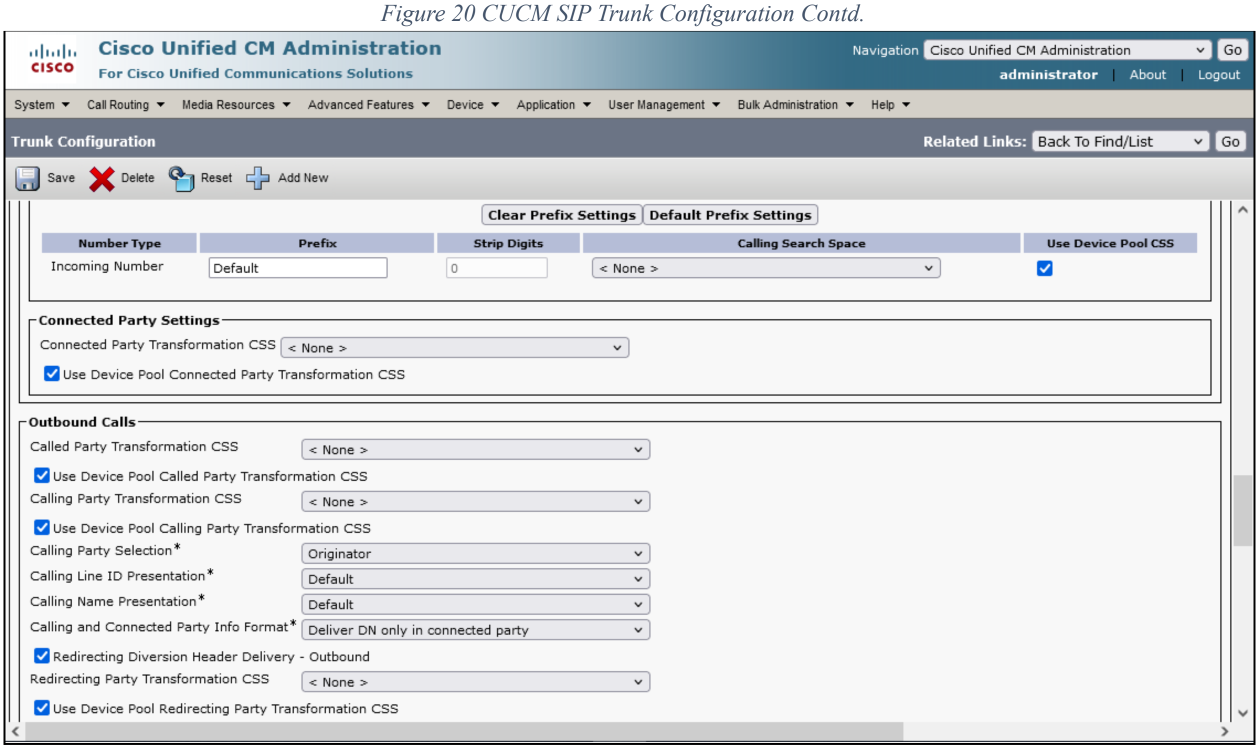


Figure 21 CUCM SIP Trunk Configuration Contd.

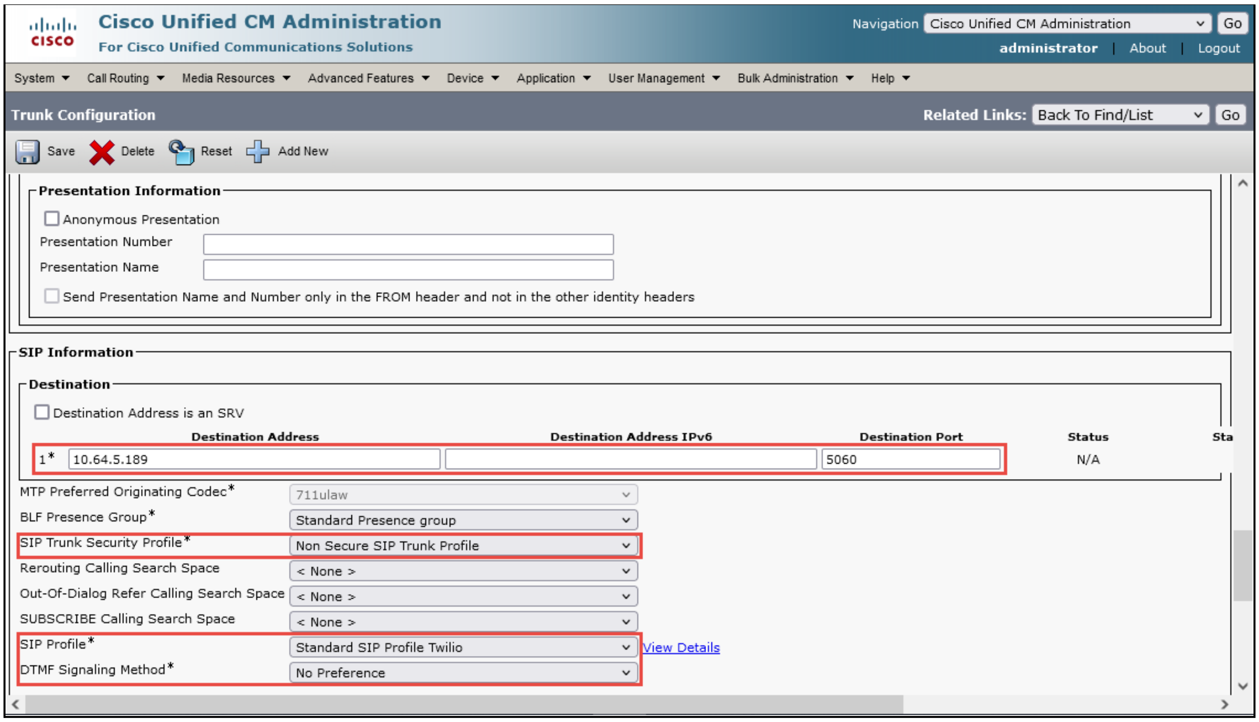


Figure 22 CUCM SIP Trunk Configuration Contd.

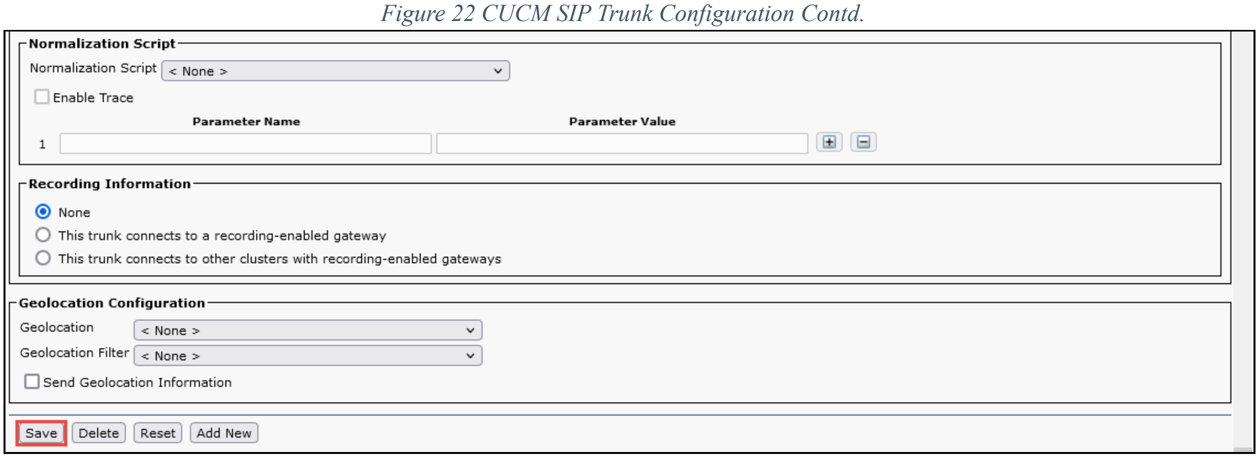


Figure 23 CUCM SIP Trunk Configuration Contd.

5.3.7 Route Pattern

1. Navigate to **Call Routing** **Route/Hunt** **Route Pattern**
2. Select **Add New** to create a new Route Pattern
3. Set **Route Pattern:** 9.@ (This is to enable outbound dialing from CUCM to vCUBE using the access code as “9”)
4. Set **Gateway/Route List**: Trunk-CUBE-Twilio was used in this test
5. Set **Discard Digits**: *PreDot* (This option is to remove the prefix “9” from called party number while sending the call out to vCUBE)

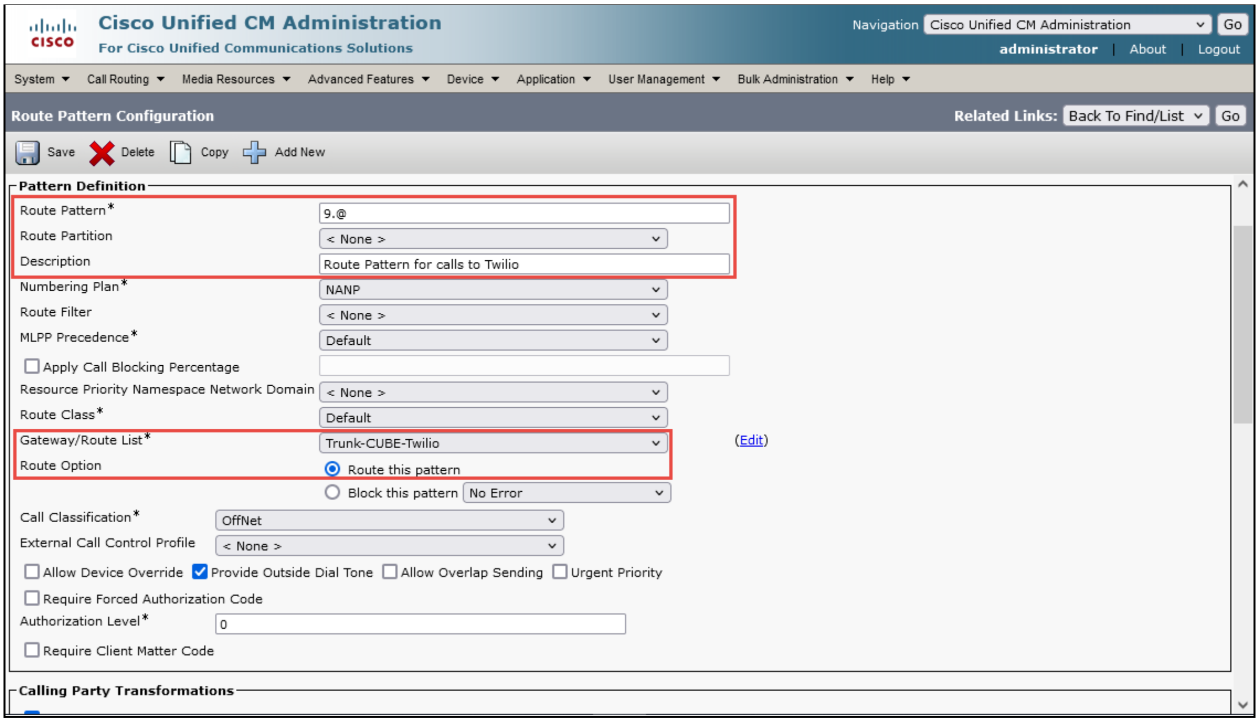


Figure 24 CUCM Route Pattern Configuration

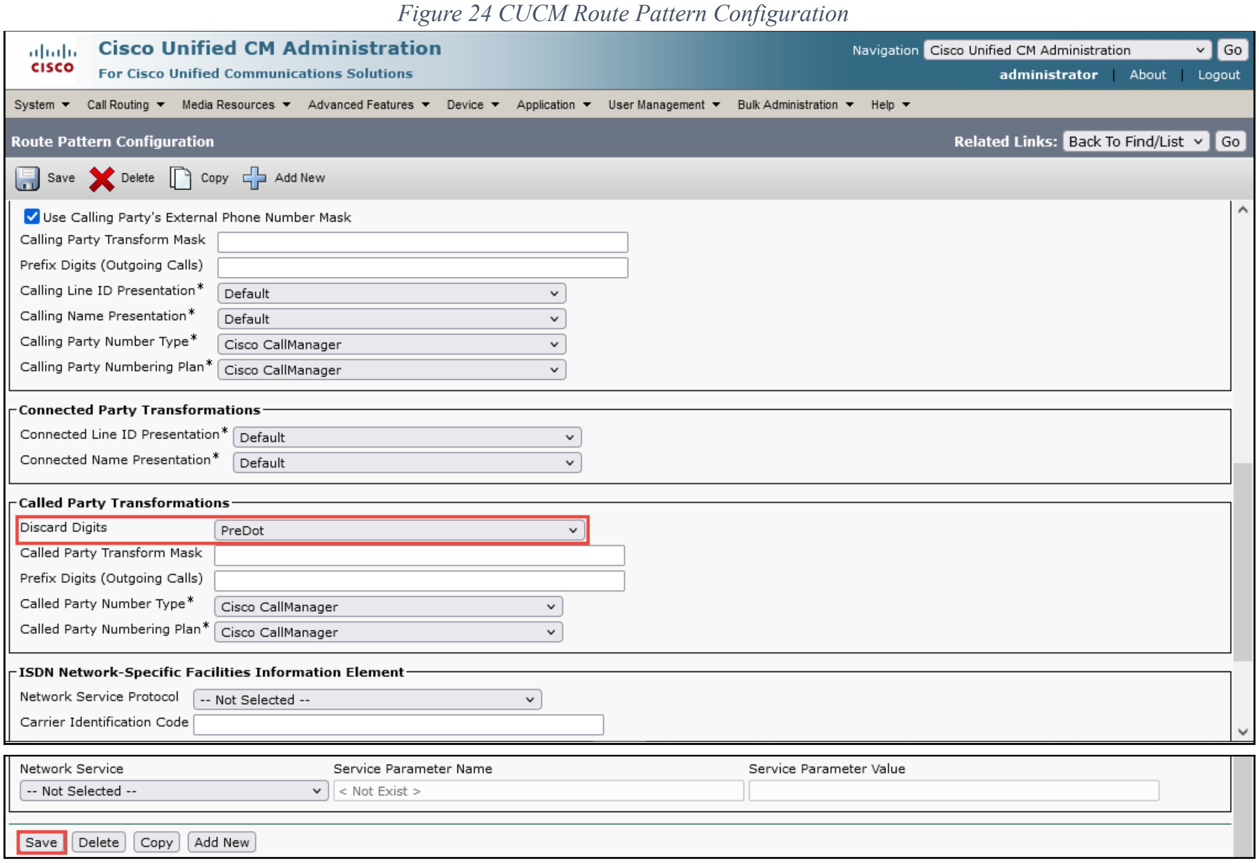


Figure 25 CUCM Route Pattern Configuration Contd.

5.4 vCUBE Configuration

vCUBE is configured through CLI as CLI mode offers more flexibility and convenience compared to GUI mode. NOTICE: the IP Address values used in this section are for reference only and are specific to the tekVizion test environment. These MUST be considered ONLY as reference. Each IP Address is described as a footnote.

5.4.1 Global vCUBE settings

The global configure settings enables CUBE application on the router, enables voice services with VoIP, and configures trusted IP address lists, enable SIP configuration mode and many more:

```
enable[1]
configure terminal[2]
voice service voip[3]
 ip address trusted list
  ipv4 54.171.127.192[4] 255.255.255.192
  ipv4 54.244.51.0[5] 255.255.255.0
  ipv4 54.172.60.0[6] 255.255.254.0
  ipv4 172.16.29.0[7] 255.255.255.0
 rtcp keepalive
 address-hiding
 mode border-element[8]
 media disable-detailed-stats
 allow-connections sip to sip[9]
 fax protocol pass-through g711ulaw
 trace[10]
 sip[11]
  session refresh
  srtp-auth sha1-80
  early-offer forced[12]
  midcall-signaling passthru
  privacy-policy passthru
```

[1] Enables privileged EXEC mode
[2] Enters global configuration mode
[3] Enters voice service configuration mode specifying VoIP as the voice encapsulation type
[4] Enables trust with Signaling IPs for Europe Ireland Gateways
[5] Enables trust with Signaling IPs for North America Oregon Gateways
[6] Enables trust with Signaling IPs for North America Virginia Gateways
[7] Enables trust with Cisco Phone (PBX extension) IPs
[8] Enables CUBE application
[9] Allows connections between SIP endpoints in a VoIP network
[10] Enables VoIP trace feature which can be used to help troubleshoot issues
[11] Enables global SIP configuration mode
[12] Converts a delayed-offer to early offer

5.4.2 vCUBE - TLS SIP trunk to Twilio

The following configuration changes are specific to trunk configuration for Twilio.

5.4.2.1 Codecs

Two set of codecs were configured as part of this validation testing and each one is associated with an outbound dial peer for Twilio. The first one is for the US trunk (Twilio Ashburn and Umatilla datacenters) and the second one is for the Europe trunk (Dublin datacenter):

```
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g711alaw
 codec preference 3 g729r8

voice class codec 2
 codec preference 1 g711alaw
 codec preference 2 g729r8
```

5.4.2.2 SIP Profile

The SIP profiles are configured to modify SIP headers. The SIP profile is associated with outbound dial peers for Twilio.
The following SIP profiles were used for the test:

```
voice class sip-profiles 200
 request REINVITE sip-header From modify "(<.*:.*)(@.*>)"
"\1@tekvizion.pstn.twilio.com>"[13]
 request CANCEL sip-header From modify "(<.*:.*)(@.*>)"
"\1@tekvizion.pstn.twilio.com>"[14]
 request INVITE sip-header To modify "(<.*:.*)(@.*>)" "\1@tekvizion.pstn.twilio.com>"[15]
 request REINVITE sip-header To modify "(<.*:.*)(@.*>)"
"\1@tekvizion.pstn.twilio.com>"[16]
 request INVITE sip-header From modify "(<.*:.*)(@.*>)"
"\1@tekvizion.pstn.twilio.com;user=phone>"[17]
 request INVITE sip-header P-Asserted-Identity modify "(<.*:.*)(@.*>)"
"\1@tekvizion.pstn.twilio.com;user=phone>"[18]
```

[13] To update re-INVITE From header to contain FQDN instead of IP before sending out to Twilio
[14] To update CANCEL From header to contain FQDN instead of IP before sending out to Twilio
[15] To update INVITE To header to contain FQDN instead of IP before sending out to Twilio
[16] To update re-INVITE To header to contain FQDN instead of IP before sending out to Twilio
[17] To update INVITE From header to contain FQDN instead of IP before sending out to Twilio
[18] To update INVITE PAI header to contain FQDN instead of IP before sending out to Twilio and also to include user=phone after FQDN (user=phone is not needed for all the scenarios)

request ANY sip-header Diversion modify "sip:(\+1..........*)@(.*)>" "sip:\1@tekvizion.pstn.twilio.com;user=phone>"[19]
request ANY sip-header Diversion modify "sip:(00..*)@(.*)>" "sip:+1814926\1@tekvizion.pstn.twilio.com;user=phone>"[20]

5.4.2.3 SIP-UA

SIP user-agent configuration:

```
sip-ua
 no remote-party-id
 transport tcp tls v1.2
 connection-reuse[21]
 crypto signaling default trustpoint TP-self-signed-2894276916[22]
```

5.4.2.4 Crypto Trustpoint

This is a default self-signed certificate generated by vCUBE. Testing revealed there is no need to configure any new certificate enrollments. The basic certificate bundle ios_core.p7b that exists in nvram is sufficient to trust the certificates sent by the Twilio datacenters (Ashburn, Umatilla and Dublin) considered for this testing:

```
crypto pki trustpoint TP-self-signed-2894276916
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2894276916
 revocation-check none
 rsakeypair TP-self-signed-2894276916
!
```

5.4.2.5 Cisco CA bundle

This is to update the Cisco CA bundle with the latest certificates. It is important to ensure that the corresponding Twilio Data center certificates are available as part of this bundle. The following command is used to view the certificates in the bundle:

“show crypto pki trustpool”

#crypto pki trustpool import url https://www.cisco.com/security/pki/trs/ios_core.p7b

---

[19] To update ANY Diversion header which has number starting with “+1” to contain FQDN instead of IP before sending out to Twilio and also to include user=phone after FQDN (user=phone is not needed for all the scenarios). This is for the Diversion header that is sent by Twilio itself

[20] To update ANY Diversion header which has number starting with “00” to contain FQDN instead of IP before sending out to Twilio and also to include user=phone after FQDN (user=phone is not needed for all the scenarios). This is for the Diversion header included by CUCM for the call forward scenarios

[21] Use listener port for sending requests over UDP

[22] Configures the SIP gateway to use its trustpoint when it establishes or accepts TLS connection. The trustpoint label refers to the vCUBE’s certificate.

Reading file from https://www.cisco.com/security/pki/trs/ios_core.p7b
Loading https://www.cisco.com/security/pki/trs/ios_core.p7b
% PEM files import succeeded.

5.4.2.6 Translation Profile

The translation profile is to apply translation rule for the calling and called number types. This is associated with the outbound dial peers to Twilio and CUCM:

```
voice translation-profile 1
 translate calling 1
 translate called 1
voice translation-profile 2
 translate calling 2
 translate called 2
voice translation-profile 3
 translate calling 3
 translate called 3
voice translation-profile 5
 translate calling 5
 translate called 5
```

5.4.2.7 Translation Rule

The translation rules are used to manipulate the numbers before sending them to Twilio or CUCM. These are invoked by Translation profiles:

voice translation-rule 1[23]
 rule 1 /^\+1\(.*\)/ /\1/
voice translation-rule 2[24]
 rule 1 /^\([1-9].........\)/ /+1\1/
voice translation-rule 3[25]
 rule 1 /^\+44\(.*\)/ /\1/
voice translation-rule 5[26]
 rule 1 /^\([2-9].........\)/ /+44\1/

5.4.2.8 Dial Peers

Dial Peers are static route table, mapping phone numbers to interfaces or IP addresses. A dial peer is associated or matched to each call leg according to the destination

[23] To remove "+1" before sending the number to CUCM
[24] To add "+1" before sending the number to Twilio
[25] To remove "+44" before sending the number to CUCM
[26] To add "+44" before sending the number to Twilio

address. Inbound dial peers are for the incoming legs to vCUBE and outbound dial peers are for the outgoing legs from vCUBE.

Inbound Dial Peer for CUCM

This dial peer is for the incoming call leg from CUCM:

```
 dial-peer voice 1 voip
 description Incoming from CUCM
 session protocol sipv2
 session transport udp
 incoming called-number [0-9]T
 voice-class codec 1
 voice-class sip bind control source-interface GigabitEthernet1
 voice-class sip bind media source-interface GigabitEthernet1
 dtmf-relay rtp-nte
```

Inbound Dial Peer for Twilio

This dial peer is for the incoming call leg from Twilio:

```
dial-peer voice 3 voip
 description Incoming from Twilio US
 max-conn 1
 session transport tcp tls
 incoming called-number +1..........
 voice-class codec 1
 voice-class sip bind control source-interface GigabitEthernet2
 voice-class sip bind media source-interface GigabitEthernet2
 dtmf-relay rtp-nte
 srtp

dial-peer voice 5 voip
 description Incoming from Twilio UK
 session transport tcp tls
 incoming called-number +44..........
 voice-class codec 2
 voice-class sip bind control source-interface GigabitEthernet2
 voice-class sip bind media source-interface GigabitEthernet2
 dtmf-relay rtp-nte
 srtp
 no vad
```

Outbound Dial Peer to Twilio

This dial peer is for the outgoing call leg from vCUBE towards Twilio:

```
dial-peer voice 2 voip
```

```
 description Outgoing to Twilio Ashburn Datacenter
 translation-profile outgoing 2
 preference 1
 shutdown
 destination-pattern [0-9]T
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:tekvizion.pstn.twilio.com
 session transport tcp tls
 voice-class codec 1
 voice-class sip asserted-id pai
 voice-class sip profiles 200
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet2
 voice-class sip bind media source-interface GigabitEthernet2
 dtmf-relay rtp-nte sip-kpml sip-notify
 srtp

dial-peer voice 20 voip
 description Outgoing to Twilio Dublin Datacenter
 translation-profile outgoing 5
 preference 2
 shutdown
 destination-pattern [0-9]T
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:tekvizion.pstn.dublin.twilio.com
 session transport tcp tls
 voice-class codec 2
 voice-class sip asserted-id pai
 voice-class sip profiles 200
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet2
 voice-class sip bind media source-interface GigabitEthernet2
 dtmf-relay rtp-nte sip-kpml sip-notify
 srtp
```

Outbound Dial Peer to CUCM

This dial peer is for the outgoing call leg from vCUBE towards CUCM:

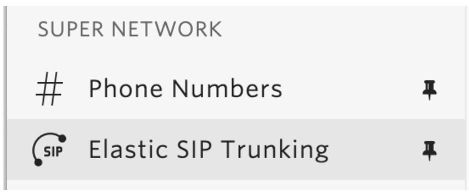
```
dial-peer voice 4 voip
 description Outgoing US number to CUCM
 translation-profile outgoing 1
 destination-pattern +1..........
 session protocol sipv2
```

```
 session target ipv4:10.71.8.10:5060
 session transport udp
 voice-class codec 1
 voice-class sip bind control source-interface GigabitEthernet1
 voice-class sip bind media source-interface GigabitEthernet1
 dtmf-relay rtp-nte
 no vad

dial-peer voice 6 voip
 description Outgoing UK number to CUCM
 translation-profile outgoing 3
 destination-pattern +44..........
 session protocol sipv2
 session target ipv4:10.71.8.10:5060
 session transport udp
 voice-class codec 2
 voice-class sip bind control source-interface GigabitEthernet1
 voice-class sip bind media source-interface GigabitEthernet1
 dtmf-relay rtp-nte
 no vad
```

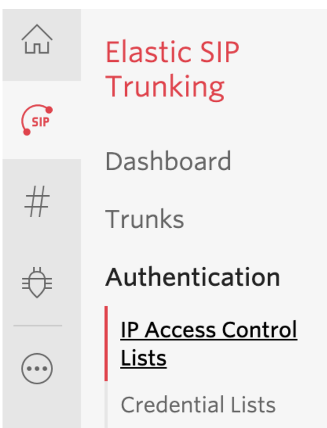
6 Twilio Elastic SIP Trunking Configuration

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

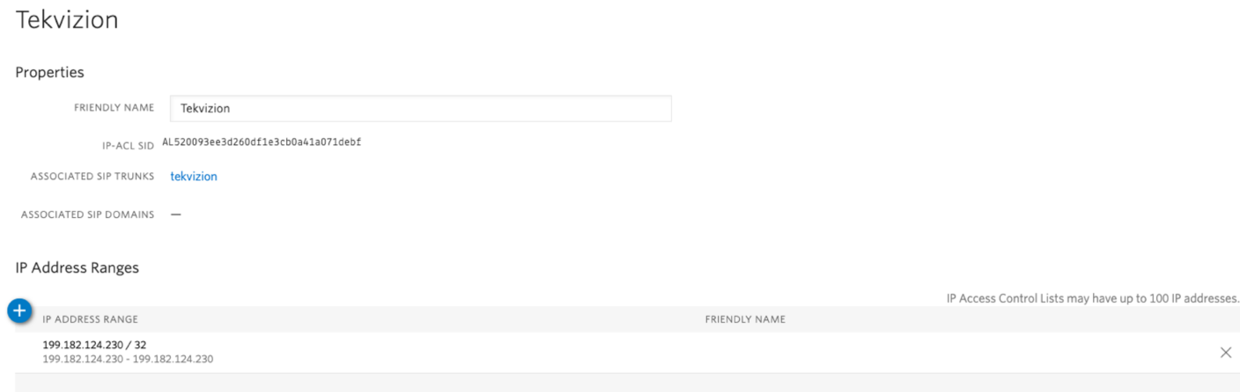


6.1 Create an IP-ACL rule

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



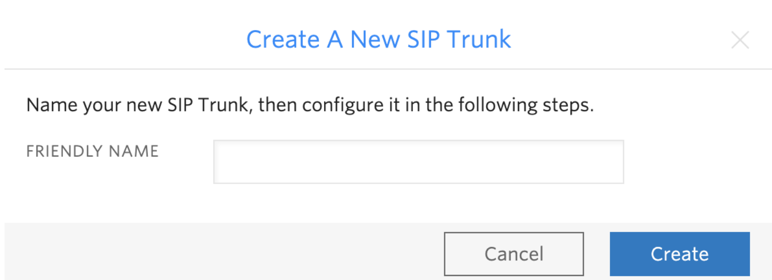
Create a new IP-ACL, for example the ACL list name used for this testing was "Tekvizion", and add the public IP Addresses assigned to the CUBE SBC(s).



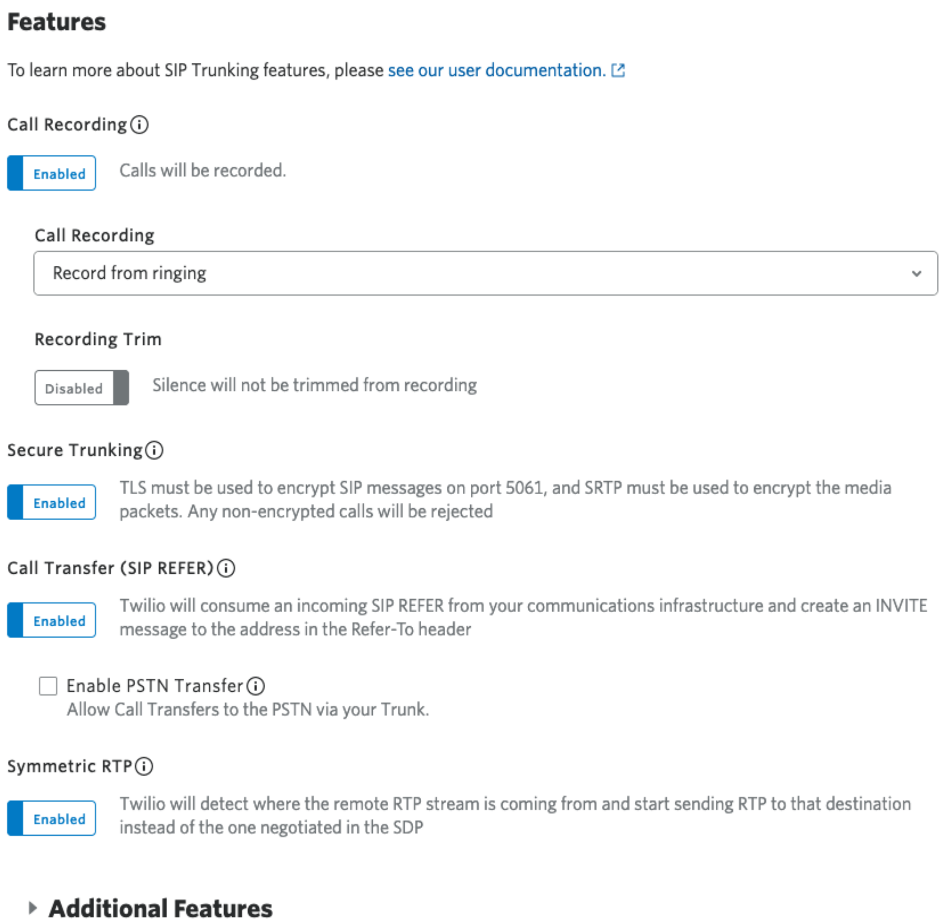
6.2 Create a new Trunk

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

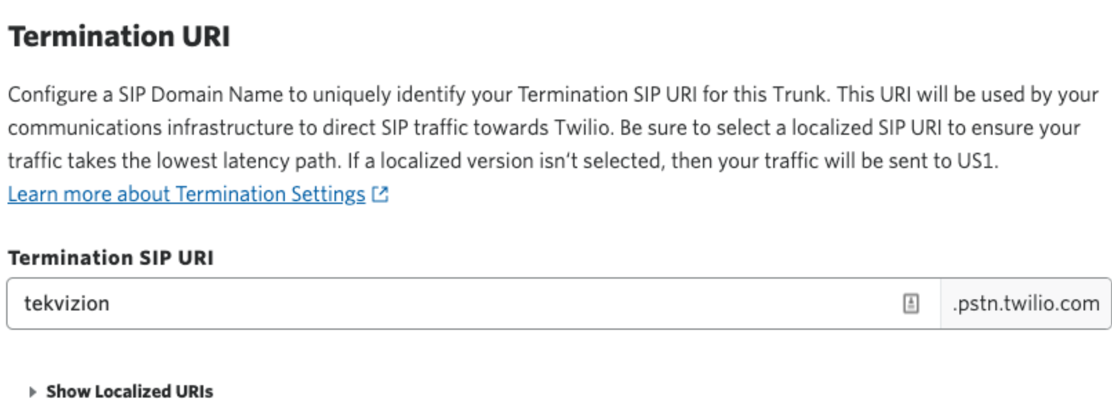
Now click on Trunks again on the left vertical navigation bar, and create a new Trunk.



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



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



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:

Attention: We have updated the syntax for localized SIP hostnames to use our new Edge Locations.
View legacy Termination SIP URIs

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

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

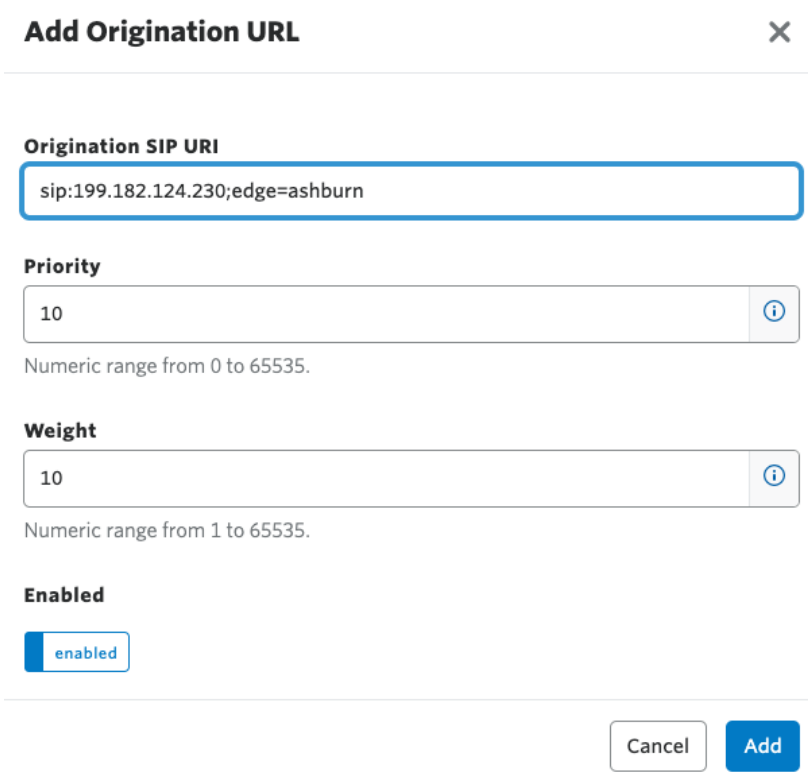
Tekvizion ×

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 CUBE 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:



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

Origination URIs

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

▸ **Show more about provisioning for high service availability**

ORIGINATION URI	PRIORITY	WEIGHT	ENABLED	
sip:199.182.124.230;edge=ashburn	10	10	✔	×
sip:199.182.124.231;edge=umatilla	10	10	✔	×

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

6.3 Associate Phone Numbers on your Trunk

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

Numbers

Add a number

Filter Parameter: Number | Number: +1415GETTWLO | Filter | Configure Emergency Calling | Remove from trunk

Number	Friendly Name	Emergency Status	Emergency Address	Country	
+18149260011	(814) 926-0011	Enabled	375 Beale St. Ste. 300, San Francisco, CA, 94105	United States	View details
+15675220022	(567) 522-0022	Disabled	-	United States	View details
+447403922739	447403922739	Not Available	-	United Kingdom	View details
+15407810033	(540) 781-0033	Disabled	-	United States	View details

7 Appendix

7.1 vCUBE Running Configuration

```
Current configuration : 9865 bytes
!
! Last configuration change at 16:15:47 UTC Wed Jun 9 2021 by cisco
!
version 17.3
service config
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname twilio
!
boot-start-marker
boot-end-marker
!
enable secret 9
$9$A4u6SYu7H3ZidE$IFUFZjSRnpLmC7kdnFZeYoxjm8Wzk952nE7Vv0lzpKU
enable password 7 060506324F41
!
no aaa new-model
!
ip name-server 8.8.8.8
!
login on-success log
!
subscriber templating
!
multilink bundle-name authenticated
!
voice service voip
 ip address trusted list
  ipv4 177.71.206.192 255.255.255.192
  ipv4 54.171.127.192 255.255.255.192
  ipv4 54.65.63.192 255.255.255.192
  ipv4 54.169.127.128 255.255.255.192
  ipv4 54.252.254.64 255.255.255.192
  ipv4 54.172.60.0 255.255.254.0
```

```
  ipv4 172.16.29.0 255.255.255.0
 rtcp keepalive
 address-hiding
 mode border-element
 media disable-detailed-stats
 allow-connections sip to sip
 fax protocol pass-through g711ulaw
 trace
 sip
  session refresh
  srtp-auth sha1-80
  early-offer forced
  midcall-signaling passthru
  privacy-policy passthru
!
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g711alaw
 codec preference 3 g729r8
!
voice class codec 2
 codec preference 1 g711alaw
 codec preference 2 g729r8
!
voice class sip-profiles 200
 request REINVITE sip-header From modify "(<.*:.*)(@.*>)"
"\1@tekvizion.pstn.twilio.com>"
 request CANCEL sip-header From modify "(<.*:.*)(@.*>)"
"\1@tekvizion.pstn.twilio.com>"
 request INVITE sip-header To modify "(<.*:.*)(@.*>)" "\1@tekvizion.pstn.twilio.com>"
 request REINVITE sip-header To modify "(<.*:.*)(@.*>)" "\1@tekvizion.pstn.twilio.com>"
 request INVITE sip-header From modify "(<.*:.*)(@.*>)"
"\1@tekvizion.pstn.twilio.com;user=phone>"
 request INVITE sip-header P-Asserted-Identity modify "(<.*:.*)(@.*>)"
"\1@tekvizion.pstn.twilio.com;user=phone>"
 request ANY sip-header Diversion modify "sip:(\+1..........*)@(.*)>"
"sip:\1@tekvizion.pstn.twilio.com;user=phone>"
 request ANY sip-header Diversion modify "sip:(00..*)@(.*)>"
"sip:+1814926\1@tekvizion.pstn.twilio.com;user=phone>"
!
voice translation-rule 1
 rule 1 /^\+1\(.*\)/ /\1/
!
voice translation-rule 2
 rule 1 /^\([1-9].........\)/ /+1\1/
```

```
!
voice translation-rule 3
 rule 1 /^\+44\(.*\)/ /\1/
!
voice translation-rule 5
 rule 1 /^\([2-9].........\)/ /+44\1/
!
voice translation-profile 1
 translate calling 1
 translate called 1
!
voice translation-profile 2
 translate calling 2
 translate called 2
!
voice translation-profile 3
 translate calling 3
 translate called 3
!
voice translation-profile 5
 translate calling 5
 translate called 5
!
voice translation-profile BLOCK
 translate calling 4
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint TP-self-signed-2894276916
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2894276916
 revocation-check none
 rsakeypair TP-self-signed-2894276916
!
crypto pki certificate pool
 cabundle nvram:ios_core.p7b
!
license udi pid CSR1000V sn 990PJD089R7
diagnostic bootup level minimal
memory free low-watermark processor 71497
!
spanning-tree extend system-id
!
```

```
username cisco password 7 030752180500
!
redundancy
!
interface GigabitEthernet1
 ip dhcp client client-id ascii 990PJD089R7
 ip address 10.64.5.189 255.255.0.0
 negotiation auto
 no mop enabled
 no mop sysid
!
interface GigabitEthernet2
 ip address 199.X.X.X[27] 255.255.255.192
 negotiation auto
 no mop enabled
 no mop sysid
!
interface GigabitEthernet3
 no ip address
 shutdown
 negotiation auto
 no mop enabled
 no mop sysid
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet1
!
ip route 0.0.0.0 0.0.0.0 199.182.124.193
ip route 10.71.0.0 255.255.0.0 10.64.1.1
ip route 54.0.0.0 255.0.0.0 199.182.124.193
ip route 172.16.0.0 255.255.0.0 10.64.1.1
ip route 172.17.0.0 255.255.0.0 10.64.1.1
ip ssh version 2
!
control-plane
!
dial-peer voice 1 voip
 description Incoming from CUCM
 session protocol sipv2
 session transport udp
```

[27] Since the actual public IP used for the test cannot be exposed during documentation, it is hidden.

```
 incoming called-number [0-9]T
 voice-class codec 1
 voice-class sip bind control source-interface GigabitEthernet1
 voice-class sip bind media source-interface GigabitEthernet1
 dtmf-relay rtp-nte
!
dial-peer voice 2 voip
 description Outgoing to Twilio Ashburn Datacenter
 translation-profile outgoing 2
 preference 1
 destination-pattern [0-9]T
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:tekvizion.pstn.twilio.com
 session transport tcp tls
 voice-class codec 1
 voice-class sip asserted-id
 voice-class sip profiles 200
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet2
 voice-class sip bind media source-interface GigabitEthernet2
 dtmf-relay rtp-nte cisco-rtp
 srtp
!
dial-peer voice 3 voip
 description Incoming from Twilio US
 max-conn 1
 session transport tcp tls
 incoming called-number +1..........
 voice-class codec 1
 voice-class sip bind control source-interface GigabitEthernet2
 voice-class sip bind media source-interface GigabitEthernet2
 dtmf-relay rtp-nte
 srtp
!
dial-peer voice 4 voip
 description Outgoing US number to CUCM
 translation-profile outgoing 1
 destination-pattern +1..........
 session protocol sipv2
 session target ipv4:10.71.8.10:5060
 session transport udp
 voice-class codec 1
 voice-class sip bind control source-interface GigabitEthernet1
 voice-class sip bind media source-interface GigabitEthernet1
```

```
 dtmf-relay rtp-nte
!
dial-peer voice 5 voip
 description Incoming from Twilio UK
 session transport tcp tls
 incoming called-number +44..........
 voice-class codec 2
 voice-class sip bind control source-interface GigabitEthernet2
 voice-class sip bind media source-interface GigabitEthernet2
 dtmf-relay rtp-nte
 srtp
 no vad
!
dial-peer voice 6 voip
 description Outgoing UK number to CUCM
 translation-profile outgoing 3
 destination-pattern +44..........
 session protocol sipv2
 session target ipv4:10.71.8.10:5060
 session transport udp
 voice-class codec 2
 voice-class sip bind control source-interface GigabitEthernet1
 voice-class sip bind media source-interface GigabitEthernet1
 dtmf-relay rtp-nte
 no vad
!
dial-peer voice 20 voip
 description Outgoing to Twilio Dublin Datacenter
 translation-profile outgoing 5
 preference 2
 shutdown
 destination-pattern [0-9]T
 rtp payload-type comfort-noise 13
 session protocol sipv2
 session target dns:tekvizion.pstn.dublin.twilio.com
 session transport tcp tls
 voice-class codec 2
 voice-class sip asserted-id pai
 voice-class sip profiles 200
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet2
 voice-class sip bind media source-interface GigabitEthernet2
 dtmf-relay rtp-nte sip-kpml sip-notify
 srtp
!
```

```
sip-ua
 no remote-party-id
 transport tcp tls v1.2
 connection-reuse
 crypto signaling default trustpoint TP-self-signed-2894276916
!
line con 0
 password 7 131112193D5D1E7B7B2A
 login
 stopbits 1
line vty 0 4
 exec-timeout 120 0
 login local
 transport input ssh
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact
email address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
!
end
```