Contents

How to connect Dongles/Phones

We provides many way to make dongle/phone as proxy device, you can get it on here: https://github.com/xapanyun/4gproxy

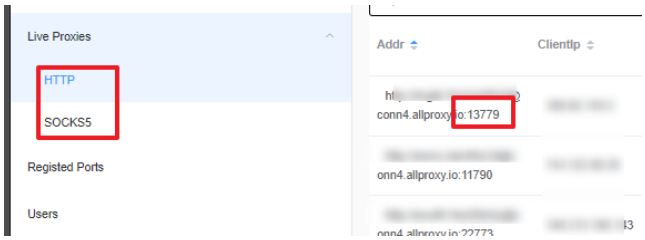
1. Phone
   a. Just download app from github and change the server address, then done.
      For rooted phone, you can set “APIUrl” in app options page, then you can use IP rotation feature for phone.
   b. You can also just connect phone to a PC, and enable USB tethering in phone, then it just likes a dongle.
2. Dongle
   a. Our gui tool is easy to use
      https://github.com/xapanyun/4gproxy/tree/master/Windows/gui
   b. You can also use console version, it supports customized script for the dongle that you want to use your self script to do IP rotation
      https://github.com/xapanyun/4gproxy/tree/master/Windows/console/x64

3. Any Other device
   You can use any version (Linux/Windows, includes arm) “allproxyC” to run, then the device will be a proxy provider
4. SDK
   You can use our client SDK to buid your self APP or Application to make proxy provider

Proxy Address

Once you connected one phone or dongle to the service, you will see a individual proxy port in dashboard.

1. So you can use the proxy with this individual proxy port.



2. You can also use one superPort(9083 by default) to accessing all proxy ports. It must works with reseller/user, for the detail usage, you can view on the following.

Super port

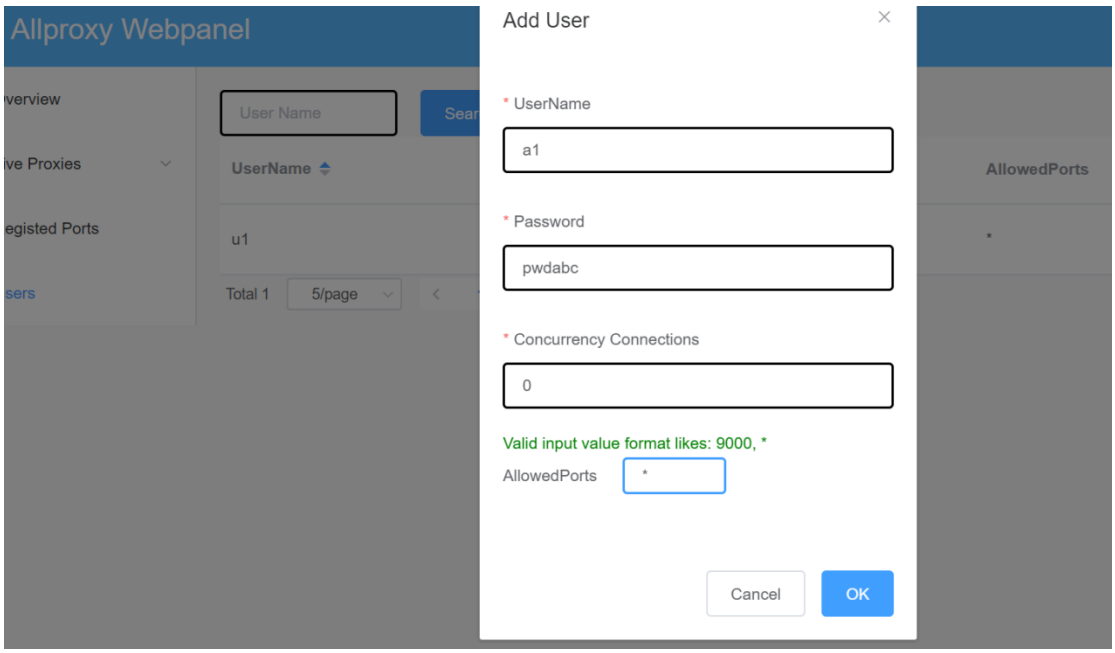
The super port is disabled by default, you can add the following content(You can change the

port to anyvalue you want) in conf_svr.yaml to enable it:

```
#not required
super_port_http: 9083
```

Assumes that your server IP is 1.2.3.4 , you will can use http://1.2.3.4:9083 (Or socks5://1.2.3.4:9083, the super ports supports both http/socks5 accessing) to access all your proxies once you enabled “super port”

But don’t forget that we should add one user before we use it.



The above screenshot means we will add an user “a1” and its password is “pwdabc”, we have no concurrnet connection limitation for this user, and we allow this user use any(*) devices(proxy ports).

So, now the proxy address should be http://1.2.3.4:9083 , and the authentication for it is a1/pwdabc

If you want to keep the IP address, you can use “uname--a1—session--12345” as the proxy user name, “12345” is any random id, the ip will be changed if you use a new session id.

The supported prameters includes: country, state, isp,city,iptype
So the valid user name likes:

1. uname--a1
2. uname--a1—session—12345
    a. you can also specity the session timeout, likes: session—12345_10m, means the session will be expired after 10 mins. Valit timeout format

includes(second/minute/hour/day): s/m/h/d

b. we also provided an API to clean specified session(HTTP GET):

http://yourServer/public/api/v3/proxy/resetip/{userName}/{sessionId}

c. we provided an API to specify the port of a session(HTTP POST)

http://yourServer/public/api/v3/proxy/resetip/{userName}/{sessionId}/{port}

NOTE: the user name in here should includes reseller name, e.g: r1--user1,if you created the user in admin, it should likes "--user1"

2.1 We also providers "fixsession" parameter, it's totally equals "session" except one difference: If the IP of this session is droped, "session" will switch to new IP, but "fixsession" will get access error.

3. uname--a1—country--US
4. uname--a1—state--OH
5. uname--a1—city--Akron
6. uname--a1—isp—SprintComminucations
7. iptype—4 or iptype—6 means ipv4 or ipv6
8. mobile-1 or mobile-0 means the network must be or not be a mobile

…

You can use all above prameters and combine it in one.

NOTE: the parameter "country, state, isp,city" only works if you use "*" to the "allowedPorts" of this user

You should remove all space from the parameter value.

Change the IP of one session

There are multiply ways to change the IP of one specified session:

1. Clean the the current IP to use new one
   POST: http://yourServer/public/api/v3/proxy/resetip/{userName}/{sessionId}

2. You can also specify the expected IP by its proxy port
   POST:
   http://yourServer/public/api/v3/proxy/updatePort/:fullUserName/:sessionId/:expectedProxyPort

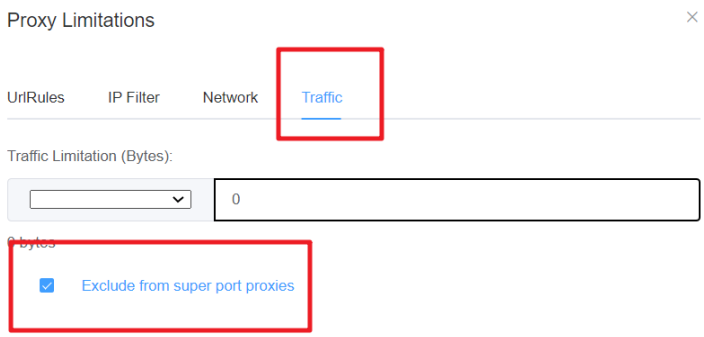
Disable proxy port

Once we enabled super port, we may will not want to publish our proxy ports to internet, because we can share it with one super port only.
So you can add the following to conf_svr.yaml

```
#not required, default is false
internalProxyPorts: true
```

Disable proxy device in superPort

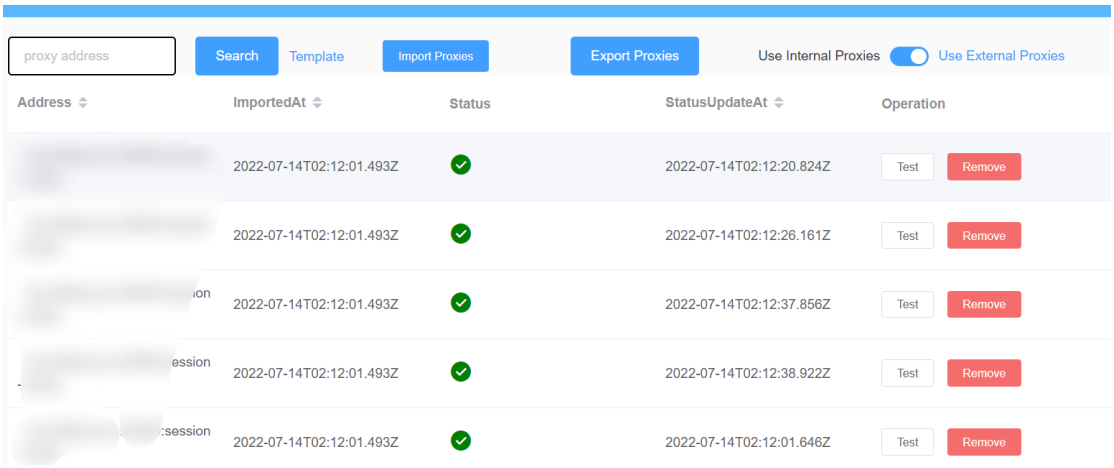
You may want to disable some devices from superPort, in that case you can exclude it.



External Proxies

You may want to use external proxies in our dashboard with the superPort advantage, likes reseller, user, userPlan…
The external proxies is seperated by reseller (admin is also a reseller), so if you want one reseller just use external proxies, you can do not give it any internal ports, and import external proxies to that reseller.
The usage is simple:

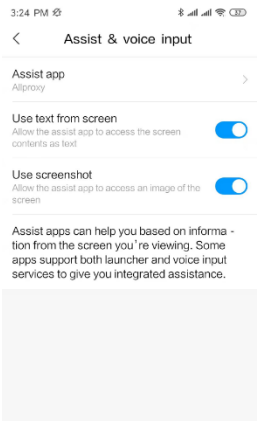
1. Login to the reseller that you want to use external proxies
2. Go to “external proxies” menu, and import
3. Enable “external proxies” in right top corner
4. Just use superPort to access proxies likes the normal way.



IP rotation

How to enable it in phone side (For android phone):

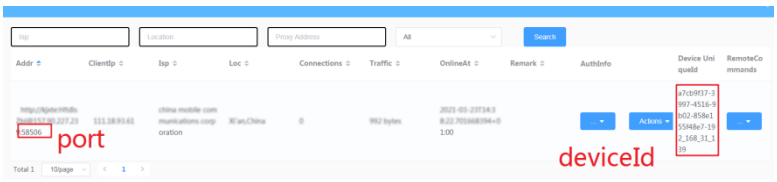
1. You must specify the api address in options page
2. For non-rooted phone, you must specify allproxy app as the Voice assist



URL

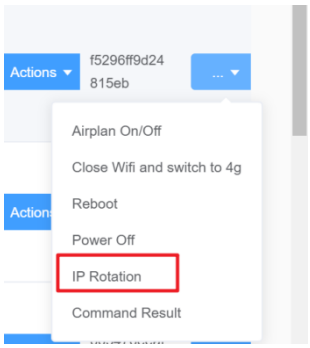
You can choose any one of the following link to do ip rotation.

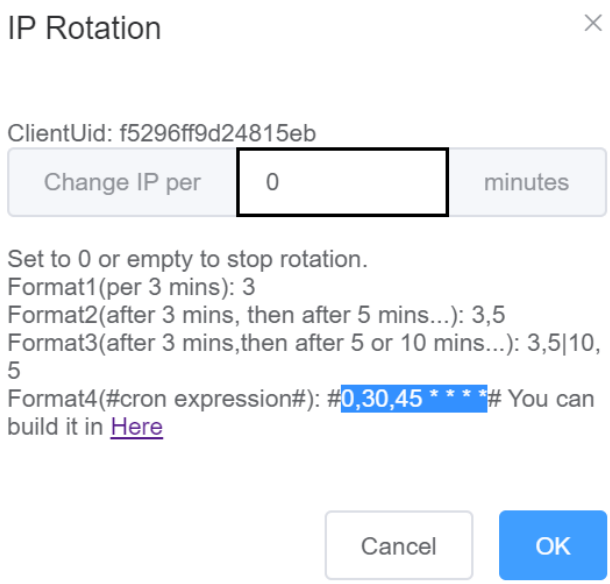
3. GET: http://yourserver:9081/public/api/v3/rmtctl/resetbyport/:port
4. GET: http://yourserver:9081/public/api/v3/rmtctl/resetip/:user/:pwd/:port
5. POST: http://yourserver:9081/public/api/v3/rmtctl/reset/:deviceid



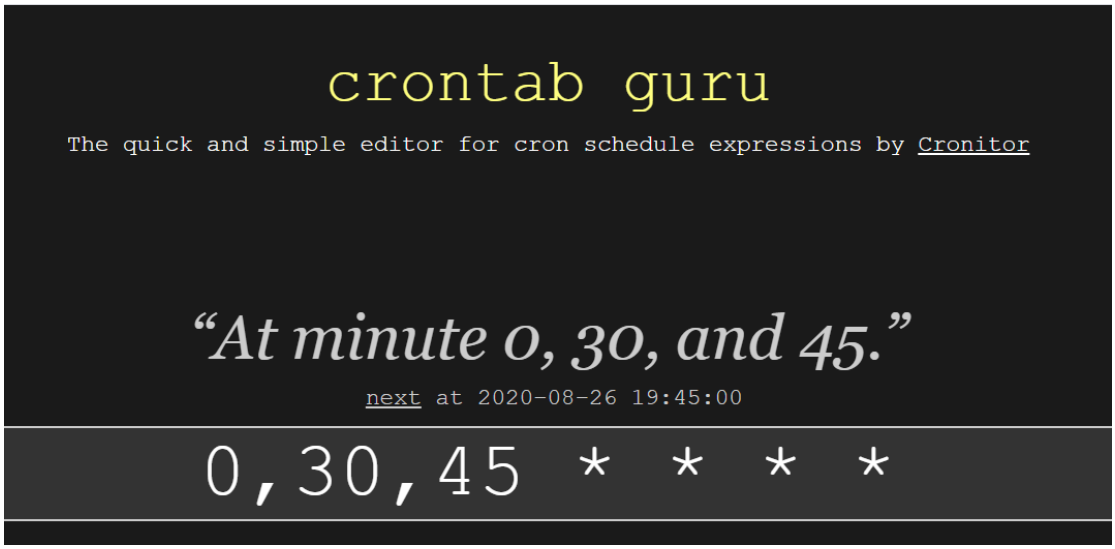
GUI

Allproxy supports IP rotation scheuler in server side, but it's is only enabled for rooted android by default, but we can also use it for 4g dongles, we will talk it later.



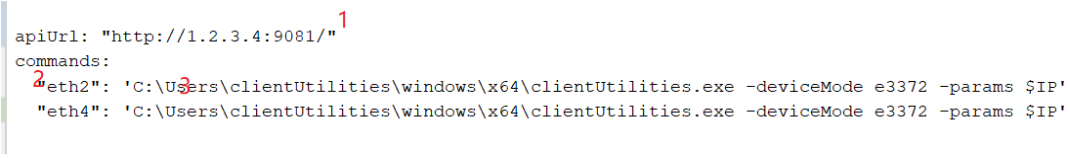


It's easier to build any scheduler you want, because it supports cron format, for e.g, "#0,30,45 * * * *# " means:



How to use it for 4g dongles?

You need to use allproxy console client version, and add the folowing to conf_client.yaml – don't forget to use your correct server address. You will see the "Ip rotation menu" once you added the content.



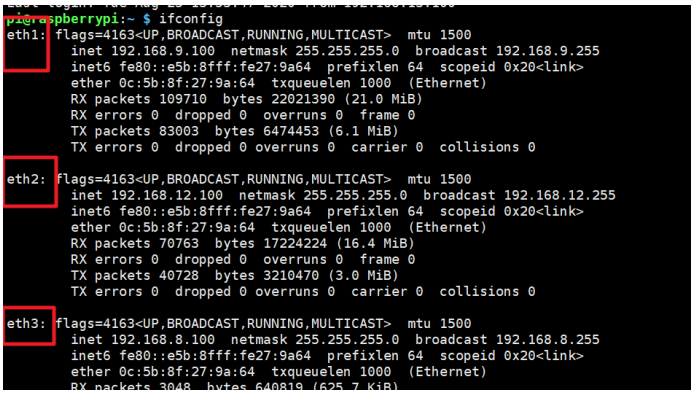

```
apiUrl: "http://1.2.3.4:9081/"
commands:
  "eth2": 'C:\Users\clientUtilities\windows\x64\clientUtilities.exe -deviceMode
e3372 -params $IP'
  "eth4": 'C:\Users\clientUtilities\windows\x64\clientUtilities.exe -deviceMode
```

Let me introduce the above image.

1. API url. Which is used to get the scheduler command
2. Networor interface name, because the command is for each individual device. **NOTE: you muse use lowercase here**

Windows

Linux (ifconfig)



3. Command script. You can use any customzed script/command here, I built a tool which names “clientUtilities”, which can do ip reset for huawei E3372.
   But because you can use any customized script here, so you can change it if you are using different dongle.
   And you may noticed “$IP” in the script, it will be replaced with the interface IP during running. Another special value is “$IFNAME”, it also will be repaced to the interface name during the running time.

   You can get the sample full configurations of a Raspberry PI client in the ending of this document.

Where to download the client?:

I uploaded all the client in github: https://github.com/xapanyun/4gproxy

And you can get the clientUtilities in :
https://github.com/xapanyun/4gproxy/tree/master/Tools/clientUtilities

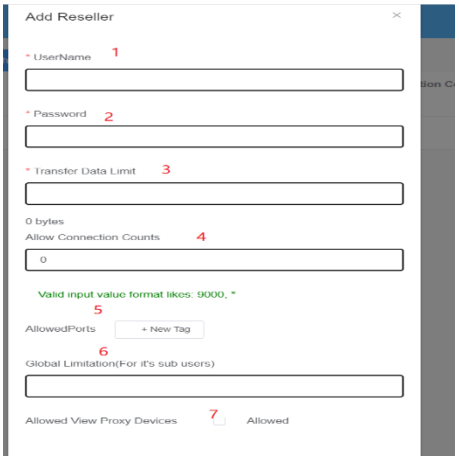
To save you work, I had also built a Rapberry PI 4B image, you can just burn it to your PI, and then just with some easy script to do upgrade:

https://github.com/xapanyun/4gproxy/tree/master/Raspberry/4B

Reseller & SubUser

“Reseller” is used to do subuser management, one reseller can create multiple sub-users, and then the sub-users can access the proxies.

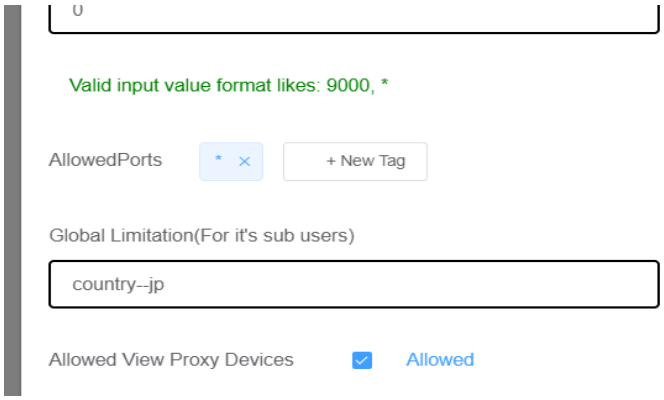
Admin user can add limitations on reseller, and reseller can also add some limitations on sub-users.

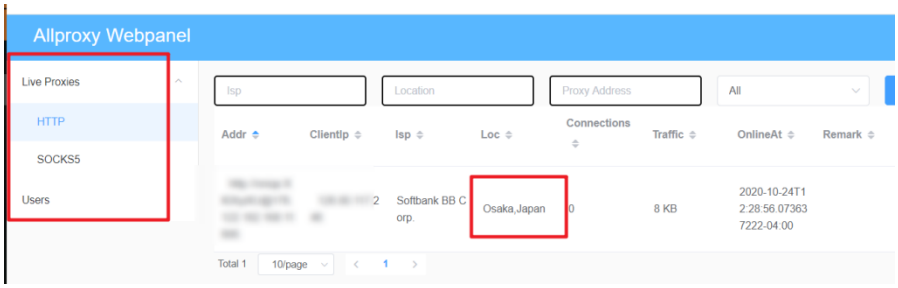


1. Reseller user name
2. Reseller password
3. The data bindwidth limitation (All of its subers data usage), 0 means no limitaion
4. The concurrent limitations, 0 means no limitation
5. Allowedports: the proxy devices which can be accessed by this sub-user, “*” means all devices
6. GlobalLimation, you may want the subuser just access the devices of Japan, so you can set “country--jp” here, the format is same as the above username format
7. If set to true, this reseller will be authorized to access the proxy devices detail

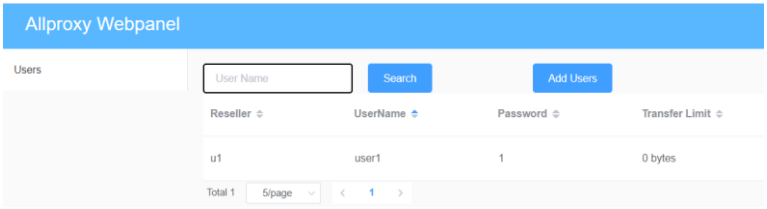
   e.g:

   I created a users with the following limitatoin, it means this user can access the dashboard to view all the Japan devices





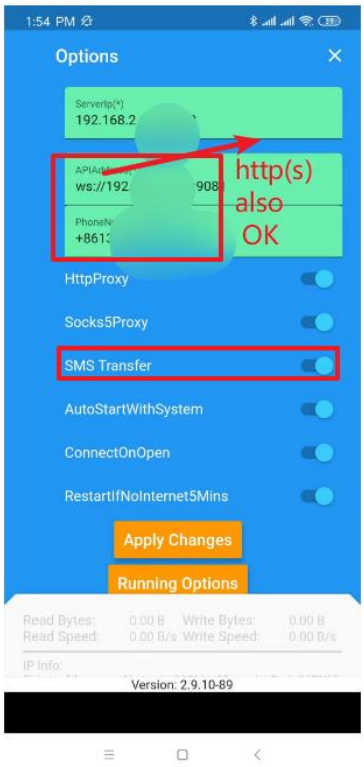
If I disabled “View Proxy Devices”

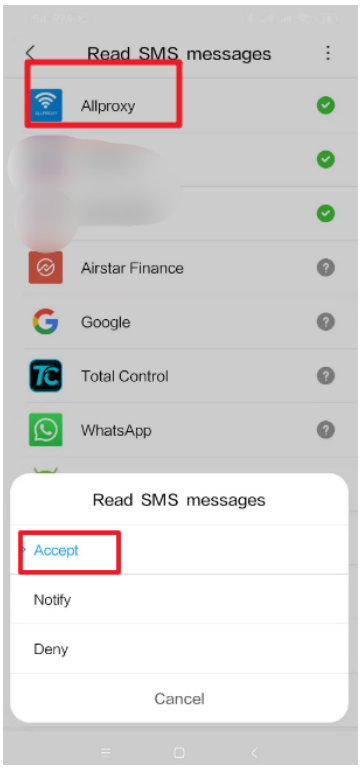


The reseller can create multiple subusers, like above screenshot, it shows I had created one user user1, its password is 1, so we can use this user to access the proxies through super port.
Its http proxy address should be:
http://reseller--u1--uname--user1:1@1.2.3.4:9083 or socks5://reseller--u1--uname--user1:1@1.2.3.4:9083

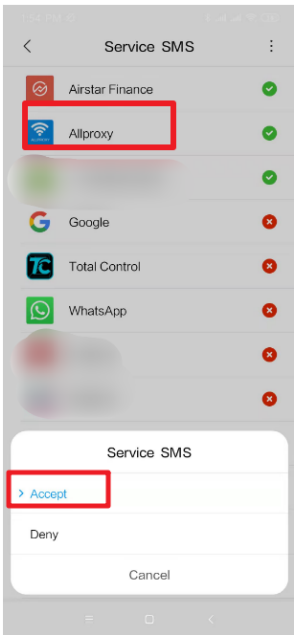
SMS

This feature just supports android phone until now.
If you want receive SMS in dashboad, you should enable it in options page of App side and give its SMS permission.
--Because there are many thing may block our to get phone number automaticlly, so you must input it yourself, don't ignore the country code pls,e.g: +15109274238

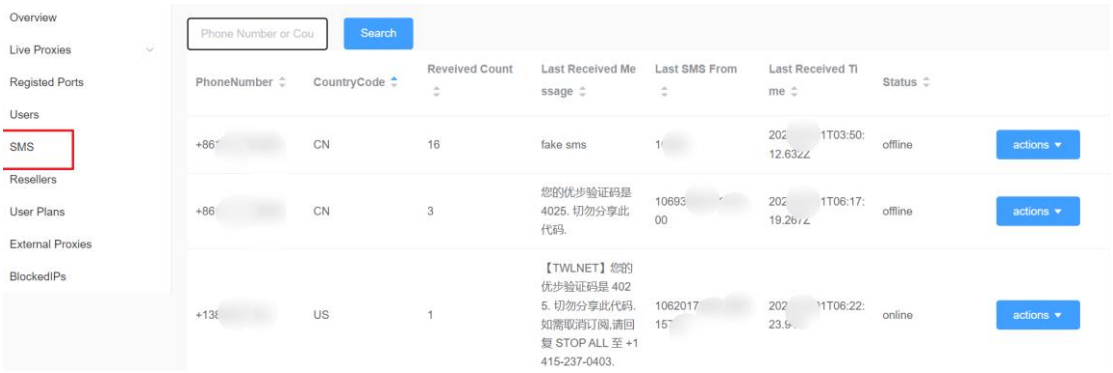




For xiaomi Phone, you need also give another SMS permission:



Once you done the options in phone side, you will can receive message in dashboard:



Key Options In Server

We provided many options in server side, which in stored in conf_svr.yaml , the following the key options:

Name	Required	SampleValue	Desc
httpAddr	Y	0.0.0.0:9081	it is used to specify the dashboard accessing address/port, you can use internal ip or public ip here.
tunnelPort	Y	9082	it is used to specify which port will be used for proxy device connecting

super_port	N		9083	Indicated the port you can used to access any proxies, see detail in above content
email	Y	abc@abc.com		Your license account
webConsoleUser	Y	admin		webConsole username
webConsolePwd	Y	passwd		webConsole password
autoGenAuth	N	true		Indicates auto generate authentication info or not when a new client conneted, default is false
mongoDBUri	Y	mongodb://localhost:27017/allp		The mongoDB connection string
cleanPortsAfterMins	N	3600		Clean offline ports if the por expired then the specified minutes---hourlly check
cleanSmsAfterMins	N	3600		Clean SMS message if it expired then the specified minutes---hourlly check
ipBlockMins	N		10	Bock the ip if the ip has too many error accessing
regularResetIpMins	N		3	Regularlly sen ip rotatoin command for all proxies

```
#TunnelServer Address
serverAddr: 1.2.3.4:9082
#Proxy protocol
protocols:
    - name: http
#    - name: socks5

#Not required,
#logTo: /home/pi/allproxyClient/all.log
apiUrl: "http://1.2.3.4:9081/"
commands:
    "eth1": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth2": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth3": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth4": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth5": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth6": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth7": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth8": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth9": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth10": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth11": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth12": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth13": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth14": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth15": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth16": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth17": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth18": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth19": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth20": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth21": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth22": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth23": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
    "eth24": '/home/pi/allproxyClient/clientUtilities -deviceMode e3372 -params $IP'
```