Post Request Aqara on Home Assistant

Requirement:

Burp Suite

Aqara_Home_mod_network.apk

(Link on description)

Script example ssh

Flow nodered example

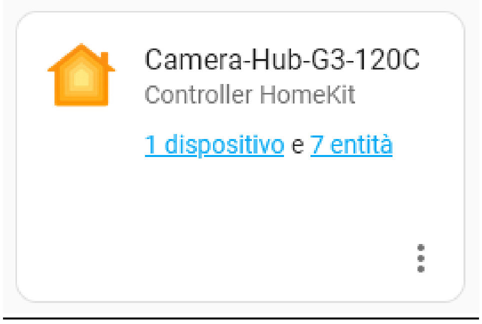
(Link on description)

Example with Aqara Hub G3 120C Cam

Auto install HomeKit with PIN **QRCode** on device

Warning: the port change every reboot of device.

scan and find with nmap, replace in to \config\.storage\core.config_entries



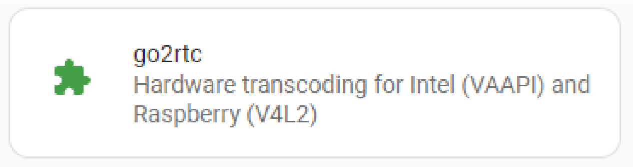
Camera-Hub-G3-120C

Controller HomeKit

1 dispositivo e 7 entità

Install go2RTC on Homeassistant

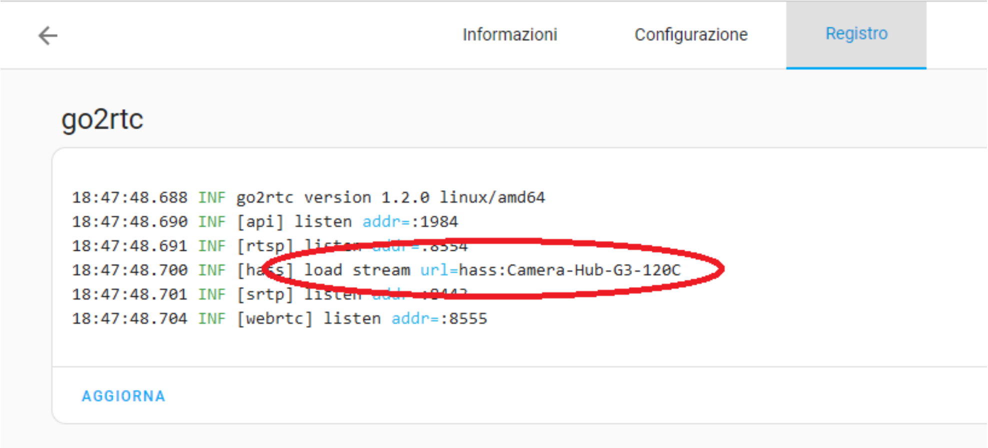
https://github.com/AlexxIT/go2rtc



go2rtc

Hardware transcoding for Intel (VAAPI) and Raspberry (V4L2)

Open go2RTC component and see log:

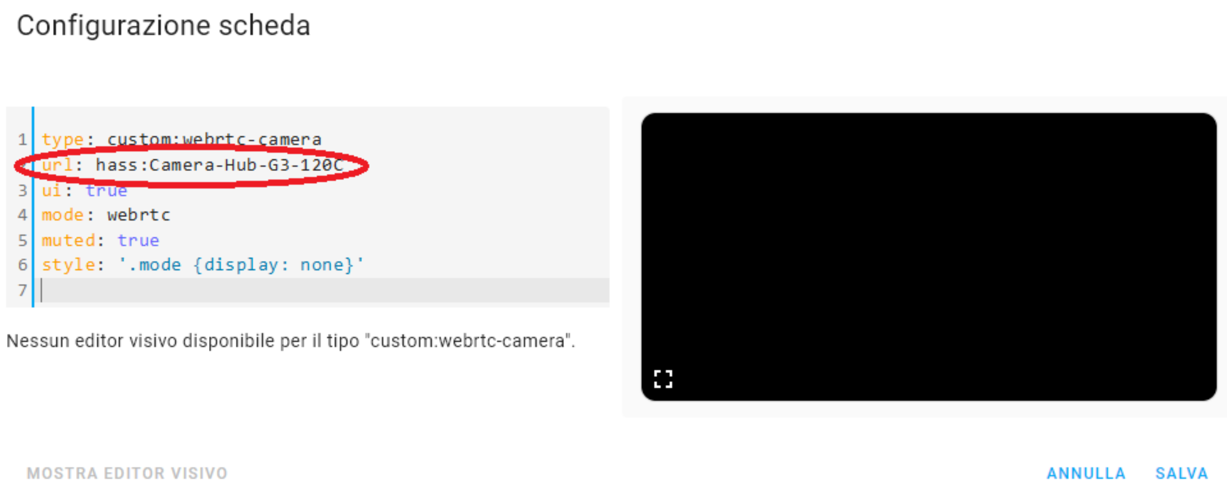


go2rtc

```
18:47:48.688 INF go2rtc version 1.2.0 linux/amd64
18:47:48.690 INF [api] listen addr=:1984
18:47:48.691 INF [rtsp] listen addr=:8554
18:47:48.700 INF [hass] load stream url=hass:Camera-Hub-G3-120C
18:47:48.701 INF [srtp] listen addr=:8443
18:47:48.704 INF [webrtc] listen addr=:8555
```

Install WebRTC on Homeassistant
https://github.com/AlexxIT/WebRTC

Create Card with Webrtc:



Configurazione scheda

```
type: custom:webrtc-camera
url: hass:Camera-Hub-G3-120C
ui: true
mode: webrtc
muted: true
style: '.mode {display: none}'

```

Nessun editor visivo disponibile per il tipo "custom:webrtc-camera".

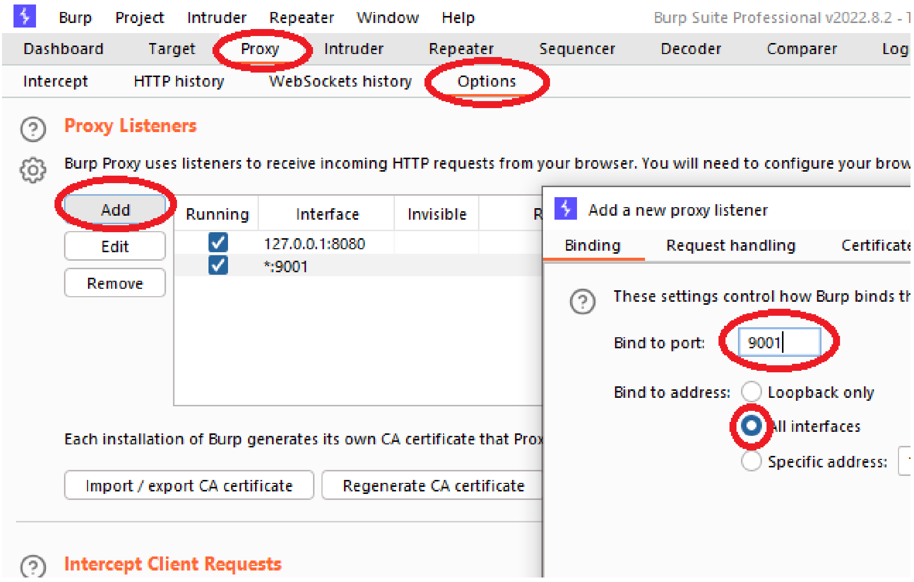
See Post Request:

Install Burp Suite Windows

follow:
https://github.com/SNGWN/Burp-Suite
for enable Android:
(https://portswigger.net/burp/documentation/desktop/mobile/config-android-device)

Open Burp Suite

Start proxy server on pc:
configure proxy server on all interface



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your brow

Running	Interface	Invisible	R
☑	127.0.0.1:8080		
☑	*:9001		

Each installation of Burp generates its own CA certificate that Prox

Add a new proxy listener

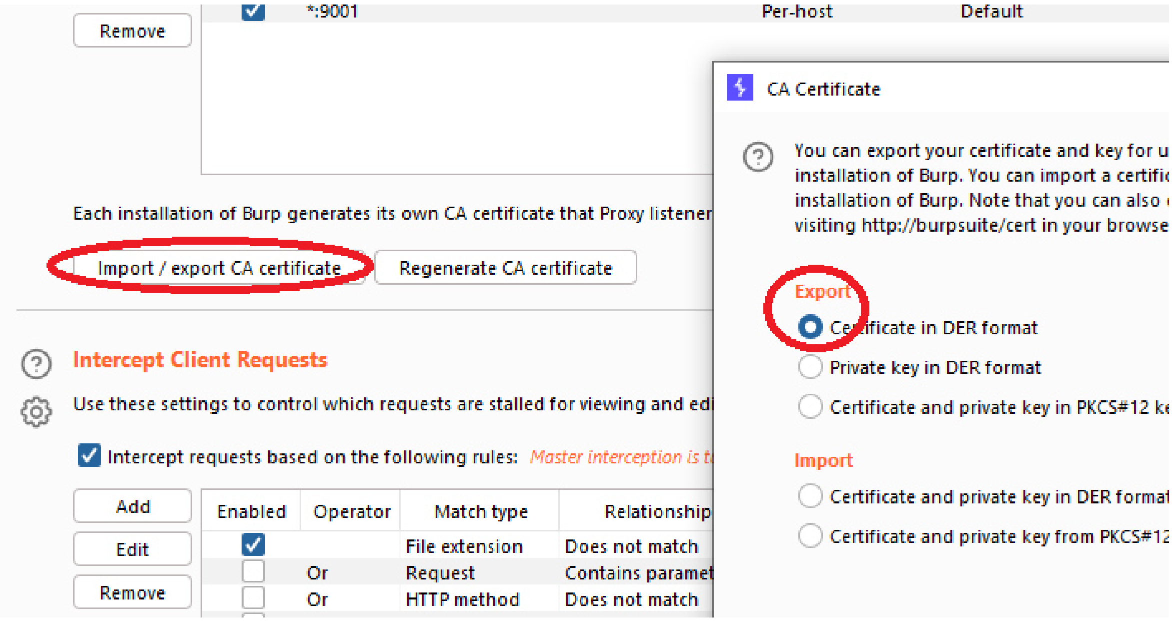
These settings control how Burp binds th

Bind to port: 9001

Bind to address: ○ Loopback only
● All interfaces
○ Specific address:

Intercept Client Requests

Export CA certificate Burp



☑	*:9001	Per-host	Default

Remove

Each installation of Burp generates its own CA certificate that Proxy listener

Import / export CA certificate

Regenerate CA certificate

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and edi

☑ Intercept requests based on the following rules: *Master interception is t*

Add

Edit

Remove

Enabled	Operator	Match type	Relationship
☑		File extension	Does not match
□	Or	Request	Contains paramet
□	Or	HTTP method	Does not match

CA Certificate

You can export your certificate and key for u installation of Burp. You can import a certific installation of Burp. Note that you can also visiting http://burpsuite/cert in your browse

Export

● Certificate in DER format

○ Private key in DER format

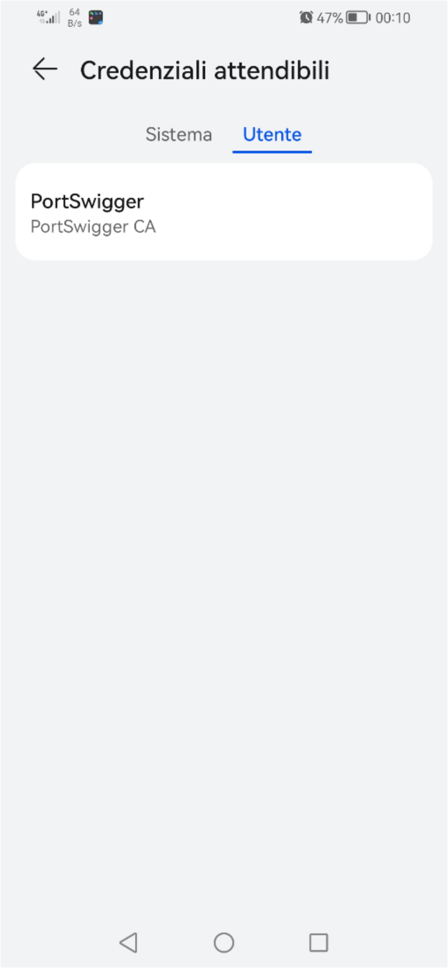
○ Certificate and private key in PKCS#12 ke

Import

○ Certificate and private key in DER format

○ Certificate and private key from PKCS#12

Download certificate and open file pem on Android Phone to install



47% 00:10

Credenziali attendibili

Sistema | Utente

PortSwigger
PortSwigger CA

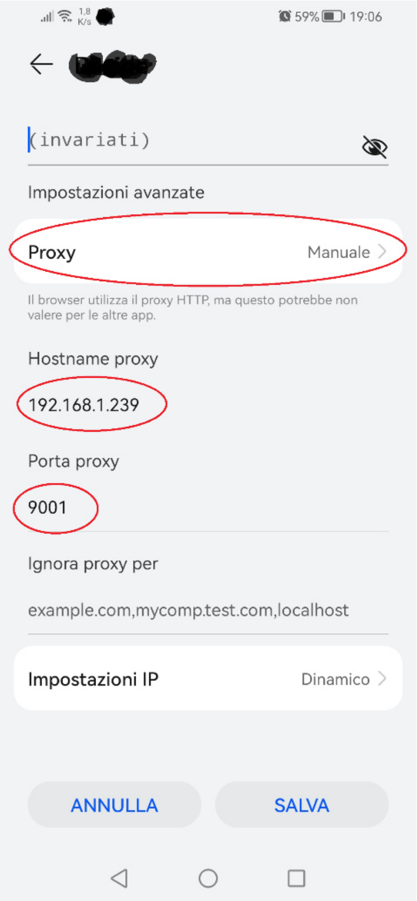
Install Aqara_Home_mod_network.apk on Android Phone
delete official app Aqara Home

```
  Mod info:
   \res\xml\network_security_config.xml
           <trust-anchors>
                     <certificates src="user" />
           </trust-anchors>
```

Connect network Phone Wifi and PC over <u>same</u> network

Set proxy on Wifi Andorid Phone:

Hold tap ssid wifi -> edit network -> set proxy manual -> IP PC -> Port



59% 19:06

[redacted]

(invariati)

Impostazioni avanzate

Proxy: Manuale

Il browser utilizza il proxy HTTP, ma questo potrebbe non valere per le altre app.

Hostname proxy: 192.168.1.239

Porta proxy: 9001

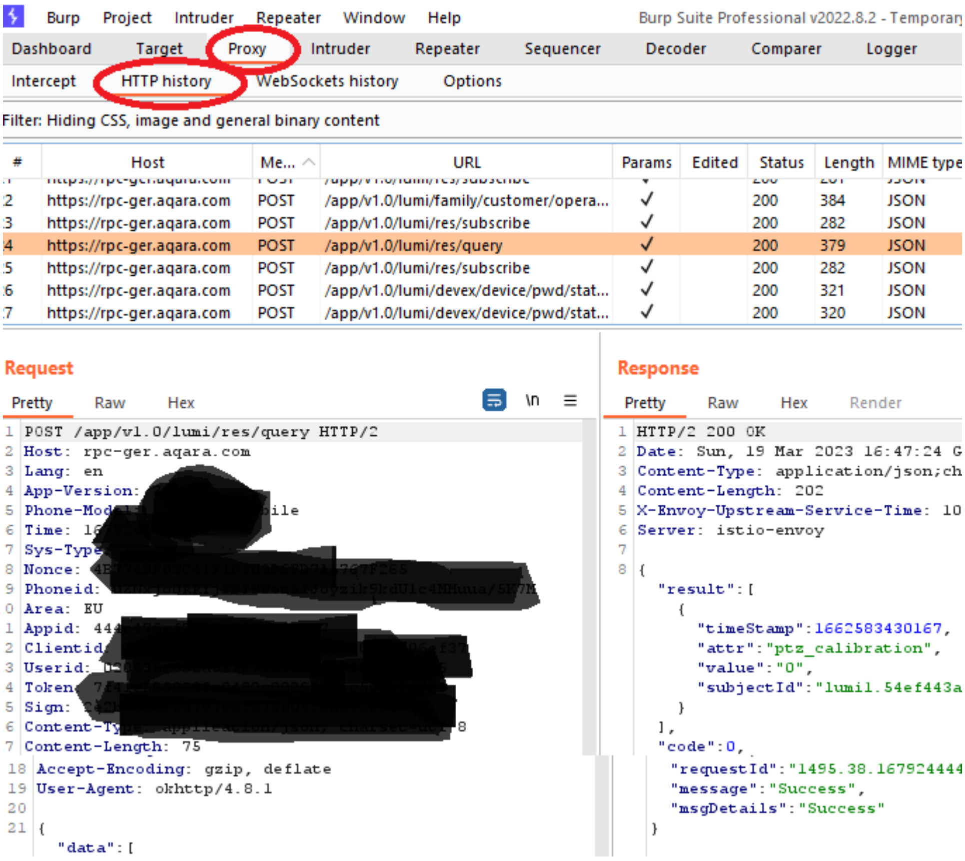
Ignora proxy per: example.com,mycomp.test.com,localhost

Impostazioni IP: Dinamico

Hostname = IP pc with Burp

Open Aqara Home app (Aqara_Home_mod_network.apk) on Android

move camera and see post request from Burp:



Filter: Hiding CSS, image and general binary content

#	Host	Me...	URL	Params	Edited	Status	Length	MIME type
2	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/family/customer/opera...	✓		200	384	JSON
3	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/res/subscribe	✓		200	282	JSON
4	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/res/query	✓		200	379	JSON
5	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/res/subscribe	✓		200	282	JSON
6	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/devex/device/pwd/stat...	✓		200	321	JSON
7	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/devex/device/pwd/stat...	✓		200	320	JSON

Request

```
POST /app/v1.0/lumi/res/query HTTP/2
Host: rpc-ger.aqara.com
Lang: en
App-Version: [redacted]
Phone-Mod
Time:
Sys-Type
Nonce:
Phoneid:
Area: EU
Appid: [redacted]
Clientid
Userid:
Token
Sign:
Content-Ty
Content-Length: 75
Accept-Encoding: gzip, deflate
User-Agent: okhttp/4.8.1

{
  "data":[
```

Response

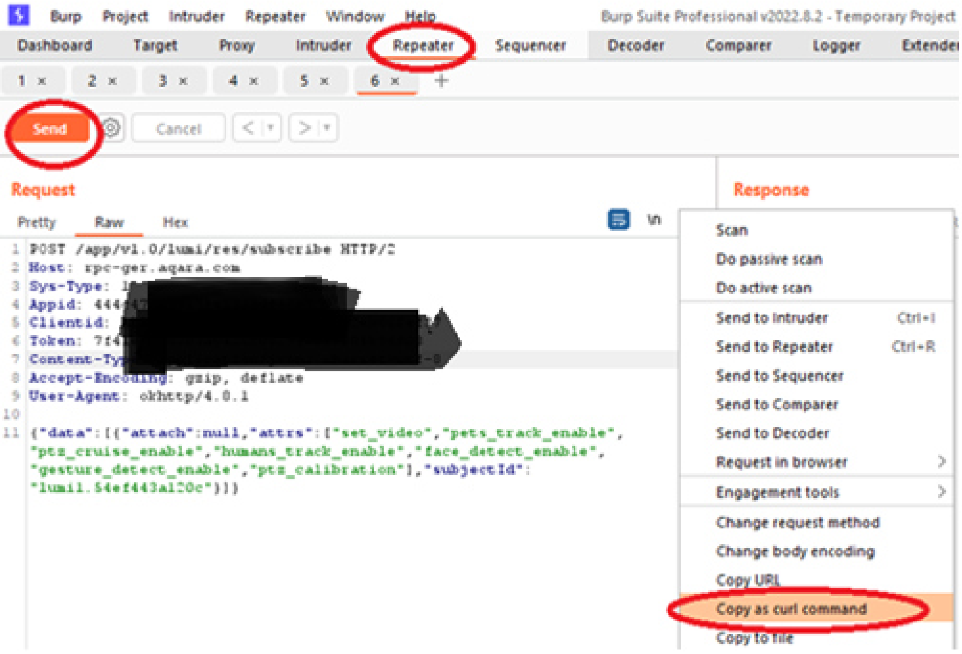
```
HTTP/2 200 OK
Date: Sun, 19 Mar 2023 16:47:24 G
Content-Type: application/json;ch
Content-Length: 202
X-Envoy-Upstream-Service-Time: 10
Server: istio-envoy

{
  "result":[
    {
      "timeStamp":1662583430167,
      "attr":"ptz_calibration",
      "value":"0",
      "subjectId":"lumi1.54ef443a
    }
  ],
  "code":0,
   "requestId":"1495.38.167924444
   "message":"Success",
   "msgDetails":"Success"
}
```

CTRL+R for send request to **"Repeater"**

Delete unecessary data

Necessary: Host | Sys-Type | Appid | Token | Content-Type



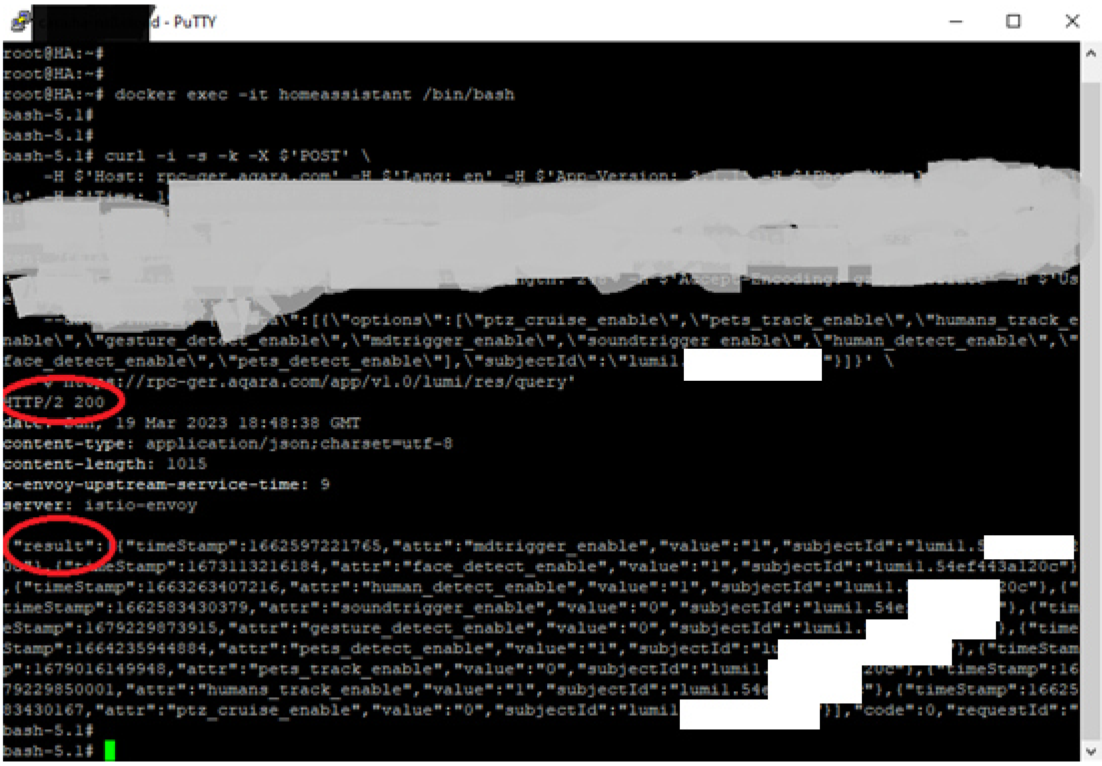
```
POST /app/v1.0/lumi/res/subscribe HTTP/2
Host: rpc-ger.aqara.com
Sys-Type: [redacted]
Appid:
Clientid:
Token:
Content-Ty
Accept-Encoding: gzip, deflate
User-Agent: okhttp/4.8.1

{"data":[{"attach":null,"attrs":["set_video","pets_track_enable",
"ptz_cruise_enable","humans_track_enable","face_detect_enable",
"gesture_detect_enable","ptz_calibration"],"subjectId":
"lumi1.54ef443a120c"}]}
```

Test with send

Copy as curl command

Test curl command on your server



[redacted] d - PuTTY

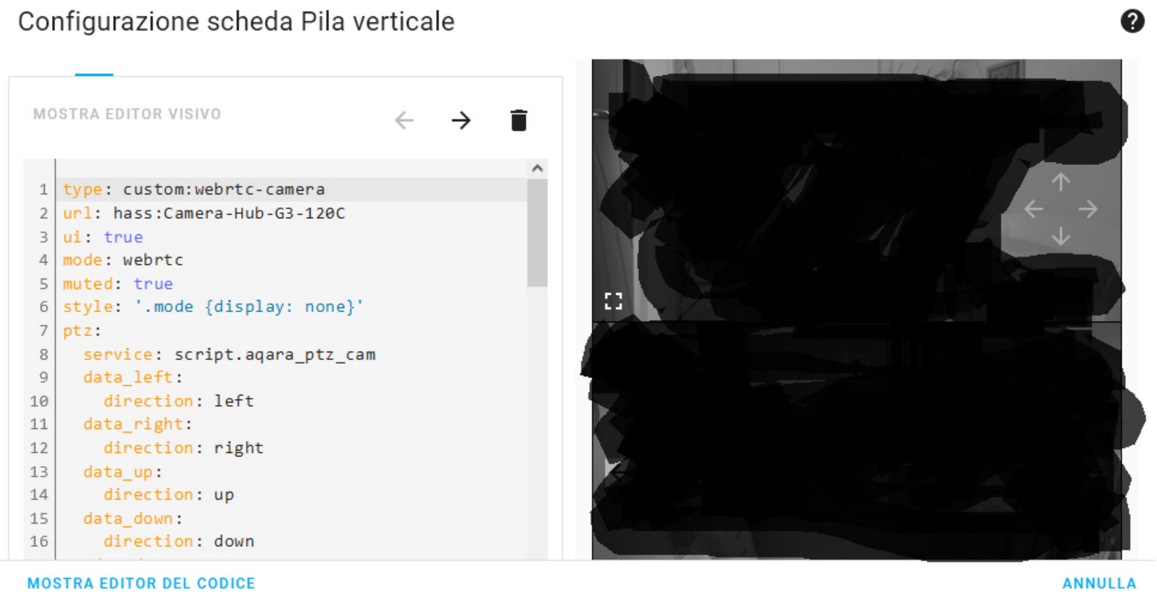
```
root@HA:~#
root@HA:~#
root@HA:~# docker exec -it homeassistant /bin/bash
bash-5.1#
bash-5.1#
bash-5.1# curl -i -s -k -X $'POST' \
    -H $'Host: rpc-ger.aqara.com' -H $'Lang: en' -H $'App-Version: [redacted]
[redacted]\":[{\"options\":[\"ptz_cruise_enable\",\"pets_track_enable\",\"humans_track_e
nable\",\"gesture_detect_enable\",\"mdtrigger_enable\",\"soundtrigger_enable\",\"human_detect_enable\",\"
face_detect_enable\",\"pets_detect_enable\"],\"subjectId\":\"lumil.[redacted]\"}]}' \
    $'https://rpc-ger.aqara.com/app/v1.0/lumi/res/query'
HTTP/2 200
date: Sun, 19 Mar 2023 18:48:38 GMT
content-type: application/json;charset=utf-8
content-length: 1015
x-envoy-upstream-service-time: 9
server: istio-envoy

"result":[{"timeStamp":1662597221765,"attr":"mdtrigger_enable","value":"1","subjectId":"lumil.5[redacted]
0c"},{"timeStamp":1673113216184,"attr":"face_detect_enable","value":"1","subjectId":"lumil.54ef443a120c"}
,{"timeStamp":1663263407216,"attr":"human_detect_enable","value":"1","subjectId":"lumil.[redacted]20c"},{"
timeStamp":1662583430379,"attr":"soundtrigger_enable","value":"0","subjectId":"lumil.54e[redacted]"},{"tim
eStamp":1679229873915,"attr":"gesture_detect_enable","value":"0","subjectId":"lumil.[redacted]},{"time
Stamp":1664235944884,"attr":"pets_detect_enable","value":"1","subjectId":"lu[redacted]"},{"timeStam
p":1679016149948,"attr":"pets_track_enable","value":"0","subjectId":"lumil.[redacted]20c"},{"timeStamp":16
79229850001,"attr":"humans_track_enable","value":"1","subjectId":"lumil.54e[redacted]"},{"timeStamp":16625
83430167,"attr":"ptz_cruise_enable","value":"0","subjectId":"lumil[redacted]}],"code":0,"requestId":"
bash-5.1#
bash-5.1#
```

Create script on HomeAssistant

or copy script example and replace your Appid - Token - subjectId - Userid

Edit Card WebRTC with PTZ Control:



Configurazione scheda Pila verticale

```
type: custom:webrtc-camera
url: hass:Camera-Hub-G3-120C
ui: true
mode: webrtc
muted: true
style: '.mode {display: none}'
ptz:
  service: script.aqara_ptz_cam
  data_left:
    direction: left
  data_right:
    direction: right
  data_up:
    direction: up
  data_down:
    direction: down
```

[redacted]

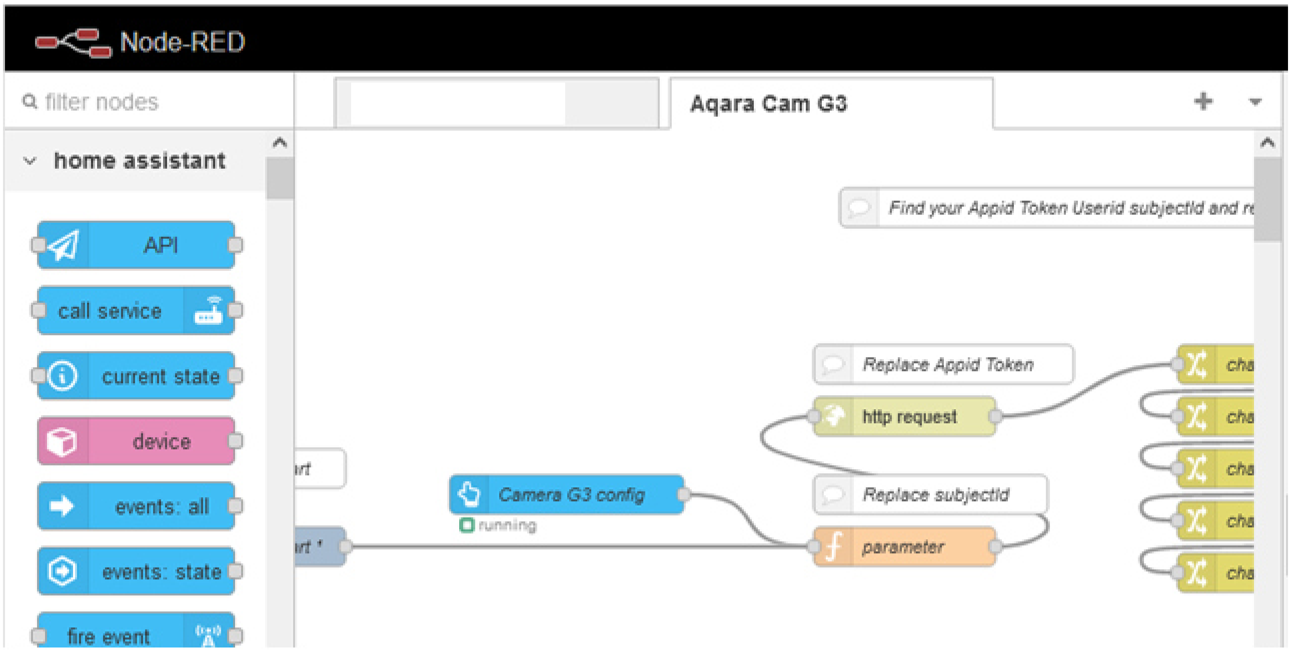
With NodeRed

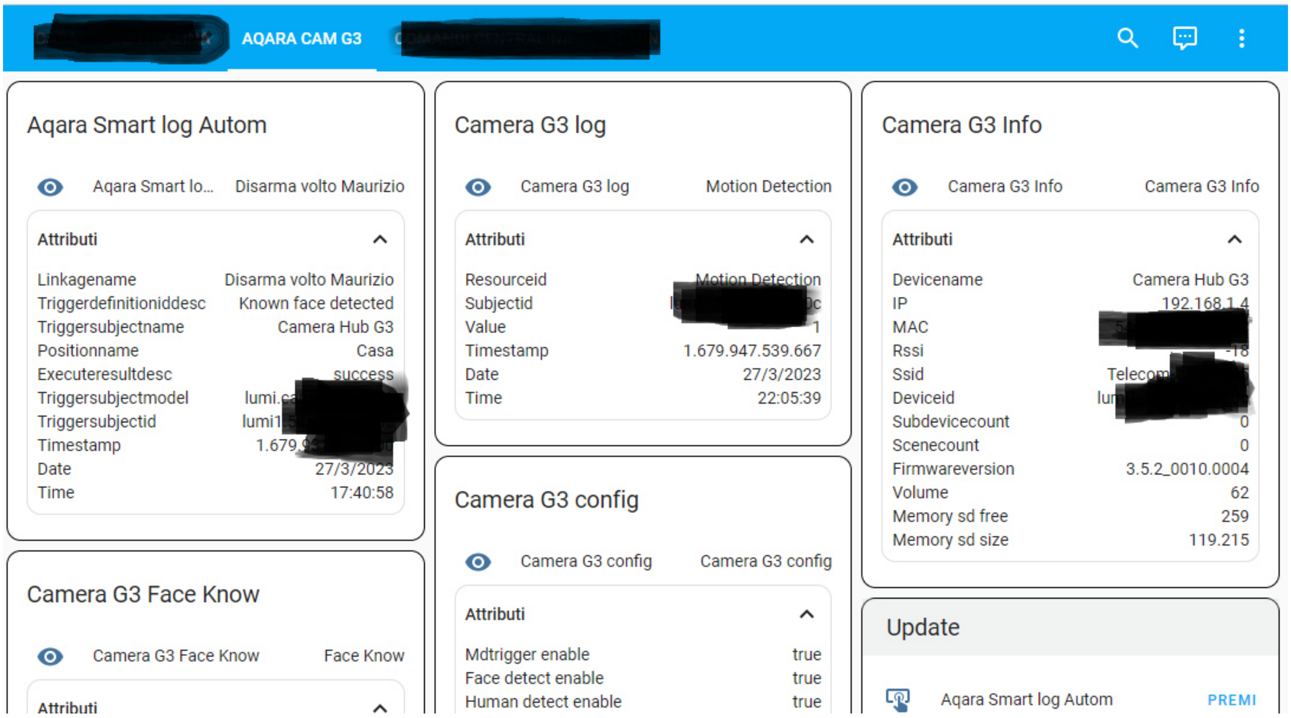
Requirement:

NodeRed

NodeRed Companion

Import Flow and replace your into nodes Appid - Token - subjectId - Userid





Aqara Smart log Autom

Aqara Smart lo... Disarma volto Maurizio

Attributi

Linkagename	Disarma volto Maurizio
Triggerdefinitioniddesc	Known face detected
Triggersubjectname	Camera Hub G3
Positionname	Casa
Executeresultdesc	success
Triggersubjectmodel	[redacted]
Triggersubjectid	[redacted]
Timestamp	[redacted]
Date	27/3/2023
Time	17:40:58

Camera G3 Face Know

Camera G3 Face Know Face Know

Attributi

Camera G3 log

Camera G3 log Motion Detection

Attributi

Resourceid	Motion Detection
Subjectid	[redacted]
Value	1
Timestamp	1.679.947.539.667
Date	27/3/2023
Time	22:05:39

Camera G3 config

Camera G3 config Camera G3 config

Attributi

Mdtrigger enable	true
Face detect enable	true
Human detect enable	true

Camera G3 Info

Camera G3 Info Camera G3 Info

Attributi

Devicename	Camera Hub G3
IP	192.168.1.4
MAC	[redacted]
Rssi	-18
Ssid	[redacted]
Deviceid	[redacted]
Subdevicecount	0
Scenecount	0
Firmwareversion	3.5.2_0010.0004
Volume	62
Memory sd free	259
Memory sd size	119.215

Update

Aqara Smart log Autom PREMI