



Crankk official guide for onboarding a SenseCAP M1 gateway via SSH

- 1) Flash the SD card with the Crankk image
- 2) Local Dashboard setup
- 3) User Dashboard setup



Onboarding a SenseCAP M1 gateway via SSH can take some time and require some technical skills, but don't worry, we're here to guide you through every step. So grab yourself a cup of coffee and let's get started!

Here are a few things you might need for this guide: tweezers, a screwdriver and an SD card reader/adaptor:



1) Flash the SD card with the Crankk image

1. Remove the SD card from your SenseCAP M1 gateway and insert it into an SD card reader/adaptor on your PC.

To begin, unscrew the bolts of your SenseCAP M1 gateway and remove the front lid. Gently pull the plastic tab and use tweezers to extract the SD card.



Next, insert the card into an SD card reader/adaptor on your PC and you're ready to get started.

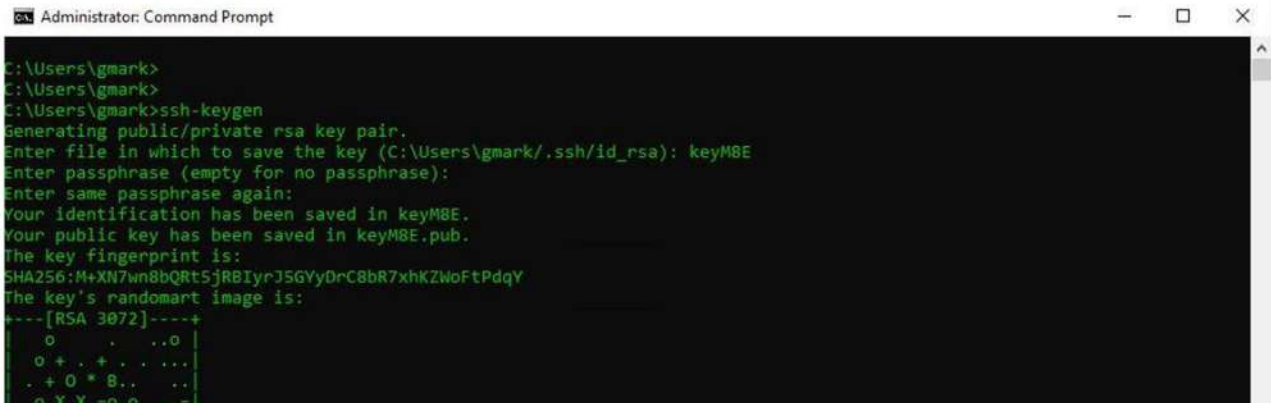
A message **Format Disk** might appear on your screen. Please **DON'T** click on it, as this will **delete** all the information on your card.

Now you will see a new removable drive called **resin-boot**. Open it and copy the **config.json** file to a safe location.

2. Generate a key pair for SSH access.

The **private key** will remain on your PC and the **public key** will go to your gateway.

Open a new **Command Prompt (cmd)** by typing **cmd** in the search bar or file explorer and hitting **Enter**.
Type **ssh-keygen** and hit **Enter**.



```
Administrator: Command Prompt
C:\Users\gmark>
C:\Users\gmark>
C:\Users\gmark>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\gmark/.ssh/id_rsa): keyM8E
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in keyM8E.
Your public key has been saved in keyM8E.pub.
The key fingerprint is:
SHA256:M+XN7wn8bQRt5jRBIyrJ5GYyDrC8bR7xhKZWoFtPdQY
The key's randomart image is:
+---[RSA 3072]----+
  o
  o + . + . . . .
  . + 0 * B . . .
  o X X = 0 . . .
```

You will be prompted to **name your key**. You can name it anything you like, but it's a good idea to name it after the last few symbols of your **gateway's MAC address**. For example, we will use KeyM8E as a key name.

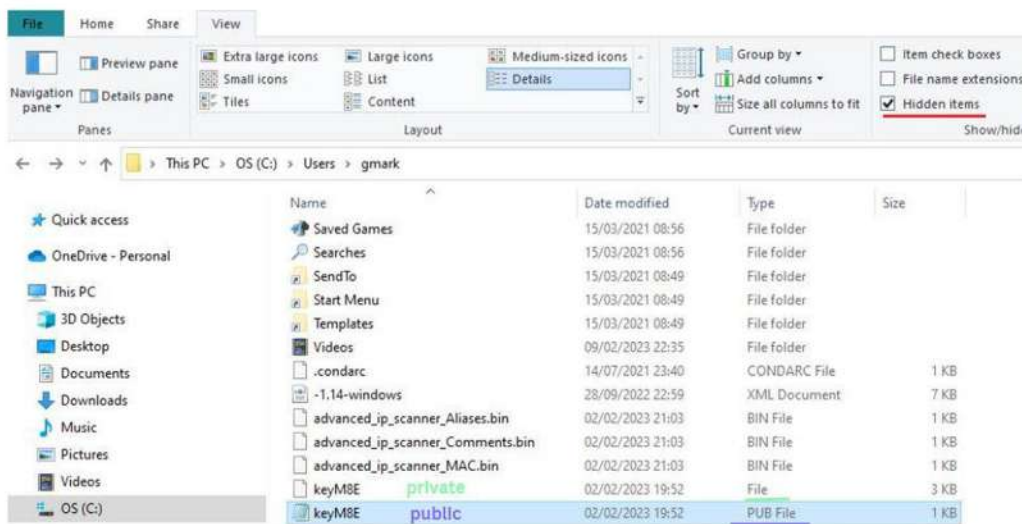
You will also be asked to set a **passphrase**.

Please write down the key name and passphrase, as you will need them later.

3. Move the private key to a .ssh folder.

Once the **public** and **private keys** are generated, they will be located in your **default user folder** (e.g. C:\Users\your username).

The path to the keys will also be shown in the **Command Prompt (cmd)**.



They are named identically, but you can check the **Type** column to know the difference: **File** is for the **private key** and **PUB File** is for the **public key**. In our case, the **PUB File** for the **public key** is selected.

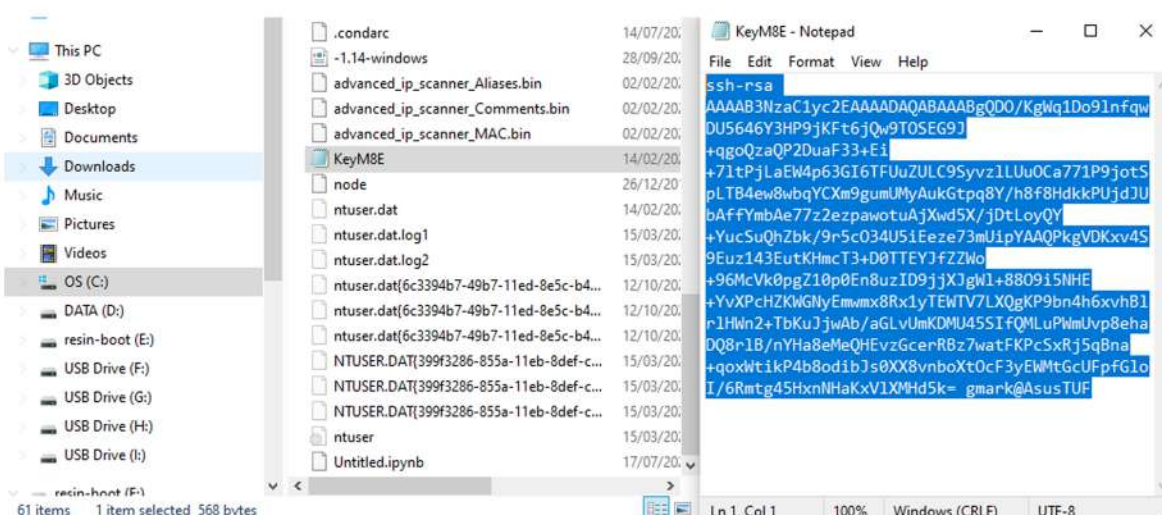
If you can't see the keys, you may need to show the **Hidden items** as shown on the screenshot.

The **private key** will remain on your PC, but it must be moved to the **.ssh folder** located in the same directory.

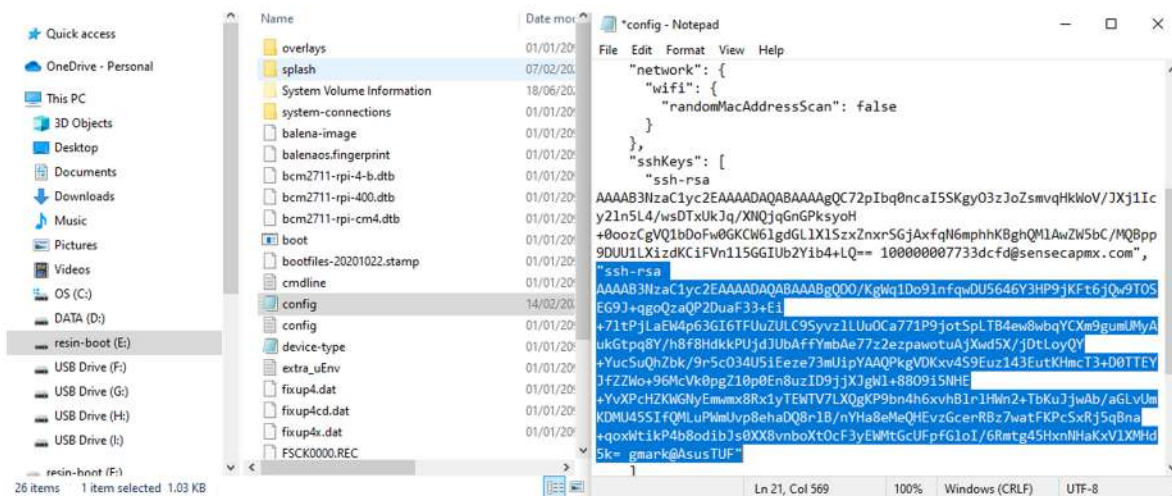
If the **.ssh folder** does not exist, create a new one and put the key inside.

4. Copy the public key to the config file on the SD card.

Open the **public key** file using a text editor such as **Notepad**.



Copy and paste your **public key** into the **config** file, right after the **SSH keys**, and put a **comma and quotation marks** between them (as shown on the screenshot).



Save the **config** file to complete the process.

5. Place the SD card back into the gateway.

Once the process is completed, insert the SD card back into your gateway and attach the antenna.

Then connect the gateway via an Ethernet LAN cable to your local network and power it on.

Please wait a few minutes for the gateway to boot up and then return to your PC.

6. Convert your private key with PuTTYgen.

Follow [this link](#) to download **PuTTY** (an SSH and telnet client) and install it.

Now you need to run **PuTTYgen** (a key generator tool for creating pairs of public and private SSH keys).

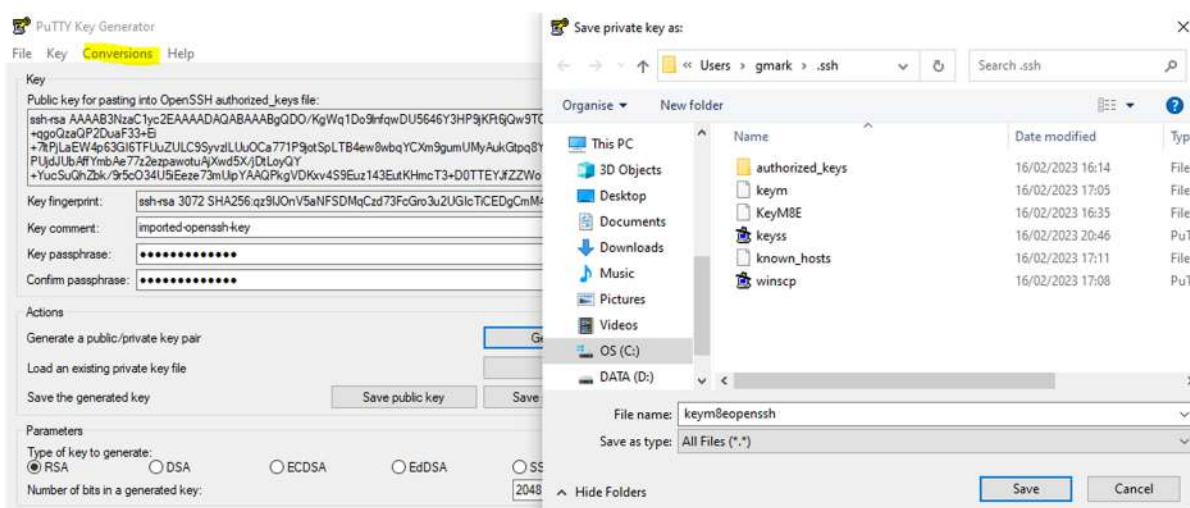
Go to **Windows > Start menu > All programs > PuTTY > PuTTYgen**

File > Load private key

Choose the **private key** from the **.ssh folder**. If you don't find it, select **All files** in the bottom right corner.

Enter your **Key passphrase**, once prompted.

Go to **Conversions > Open SSH key** (the first option) and save it.



7. Download and run the Crankk Installer.

Follow [this link](#) to download the latest version of the **Crankk Installer**.

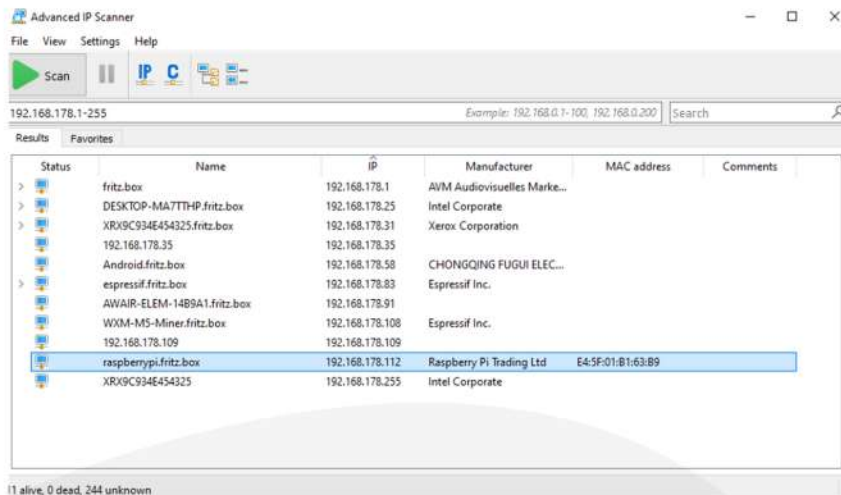
It will install the Crankk software required for your gateway to function as a PoNP node.

Install the application and start it from the shortcut on your desktop.

8. Connect via SSH Login.

First check your router to find the **gateway IP address**.

If you are unsure how to do this, you can use free tools like [Advanced IP Scanner](#) to help you out. Check the **MAC address** of your gateway to find the correct IP address.



Select the **Private Key** option from the drop-down menu.

Copy and paste your **gateway IP address** into the first field.

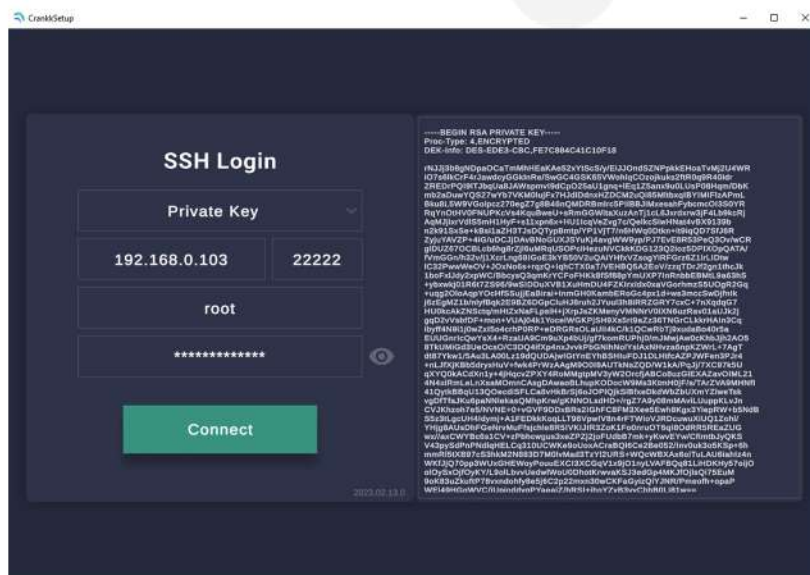
Enter **22222** into the second field, this indicates the Port.

Use the following credentials:

- Username: **root**
- Password: **your Key passphrase (the one you previously set for your SSH key)**

Open the **converted private key** (keym8eopenssh in this example) with **Notepad** and copy its full contents into the right blank field of the **SSH Login** window (as shown on the screenshot).

Hit the **Connect** button.



8. Install the Crankk software.

Once you are logged into the gateway, press the **Install Crankk** button and then restart the gateway.

2) Local Dashboard setup

9. Log in to the Local Dashboard.

Log in to the **Local Dashboard**.

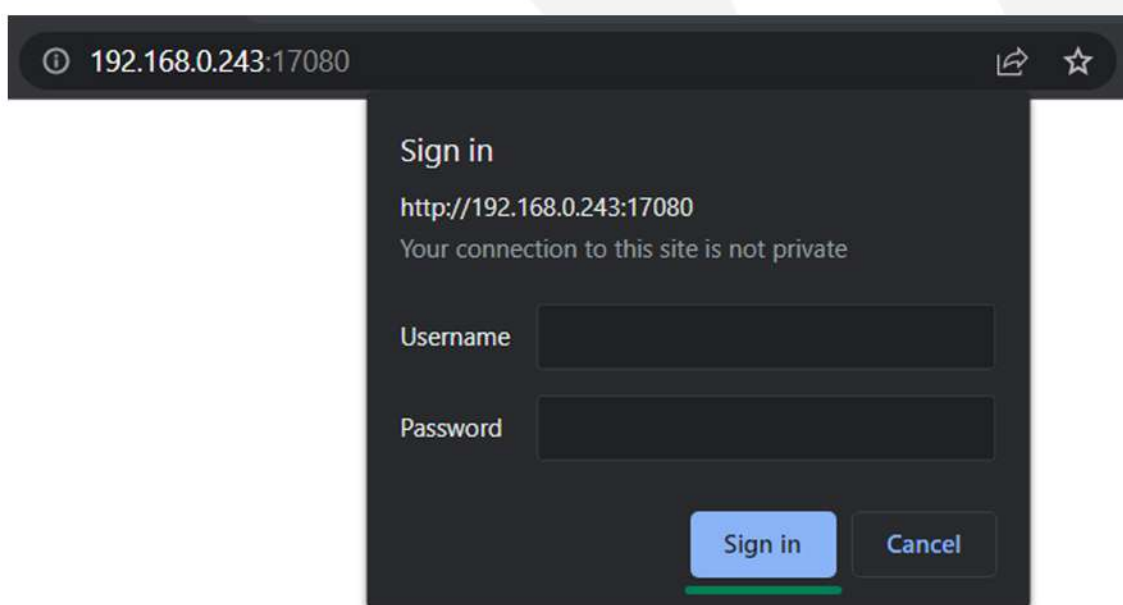
If you have any VPN enabled on your PC, please turn it off.

Check your **gateway IP address** again with an IP Scanner, because it might be different this time.

Once you have the LAN IP address of your gateway, open a new browser tab from a PC on the same network and paste the IP followed by **:17080**

`http://192.168.0.243:17080`

When logging in for the first time, you do not need to enter any credentials, just press **Sign in**.



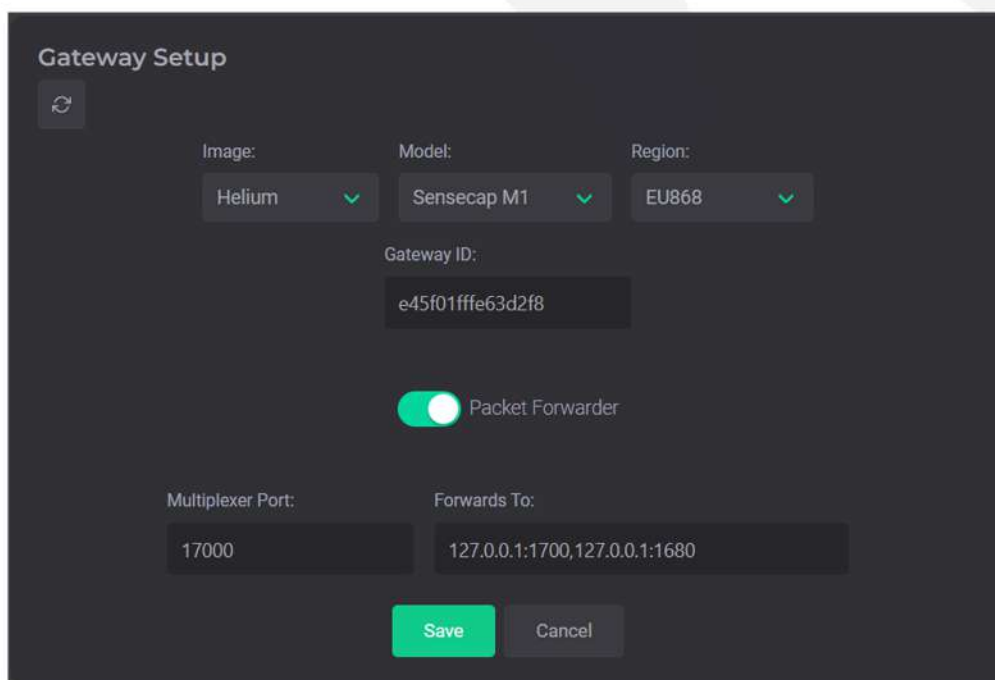
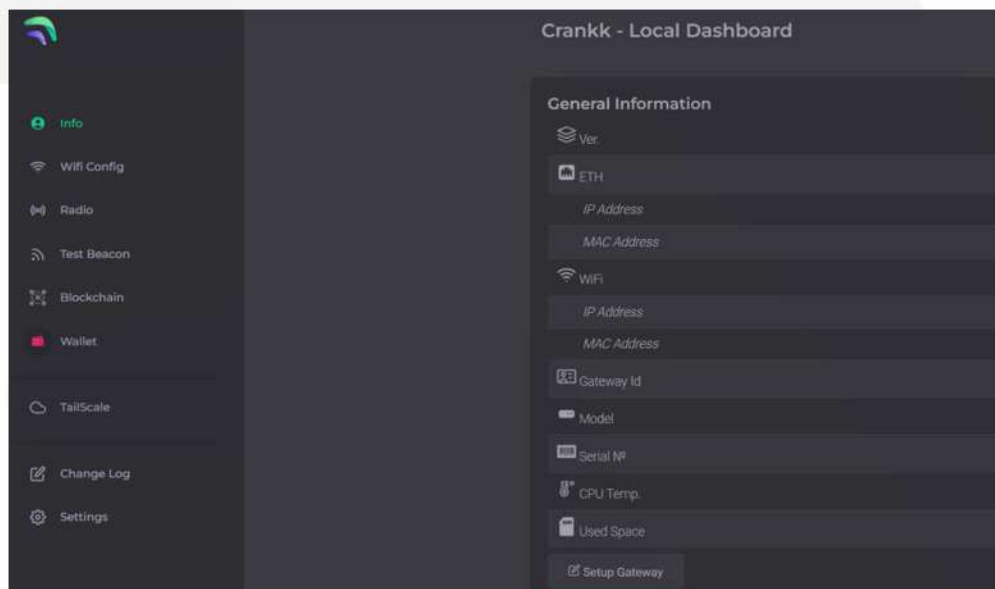
After setting up your gateway, next time you can log in with the following credentials:

- Username: **admin**
- Password: **the last 6 symbols of the gateway's MAC address (e.g. B163B9)**

Please note that you can change the password in the **Settings** tab.

10. Set up the gateway.

Go to the **Info** tab > **Setup Gateway**



Copy your **Gateway ID**, as we will need it later.

Select **Helium** as **Image**, **SenseCAP M1** as **Model** and pick your **Region*** (EU868 / AU915 / US915).

Turn on the **Packet Forwarder**.

If you are currently mining or planning to mine Helium, leave the **Forwards to** box unchanged as shown on the screenshot.

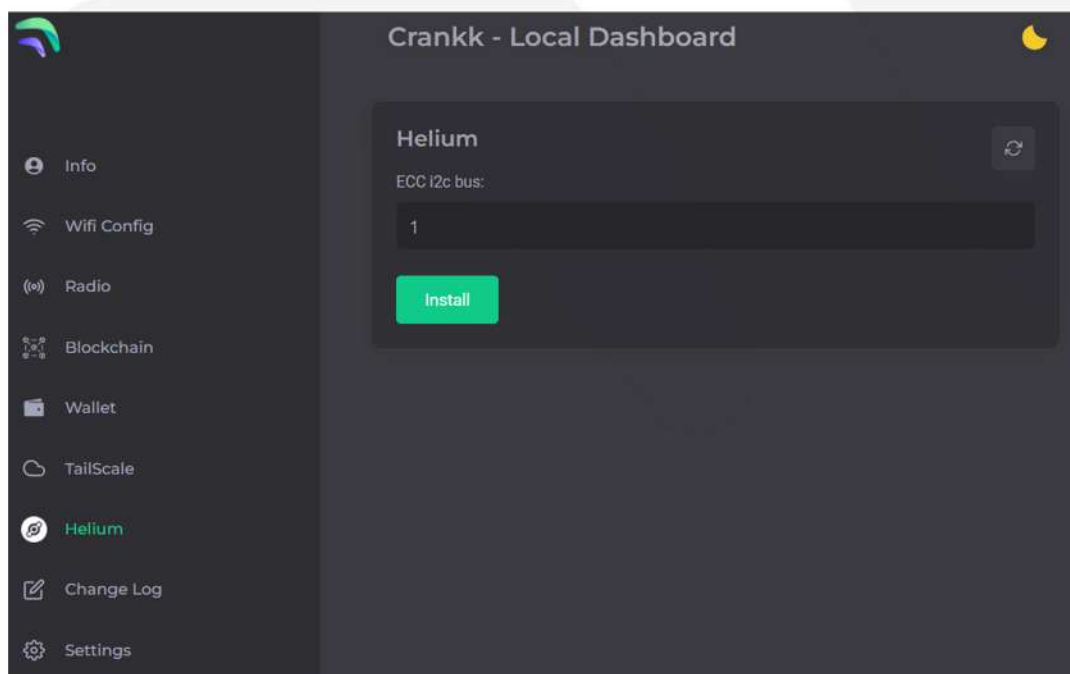
If you don't wish to mine Helium, leave only **127.0.0.1:1700**

Hit **Save**.

Your gateway will restart automatically. Please wait a few minutes while it loads.

11. Double mining.

The Helium container should already be preinstalled, but you can reinstall it from here:

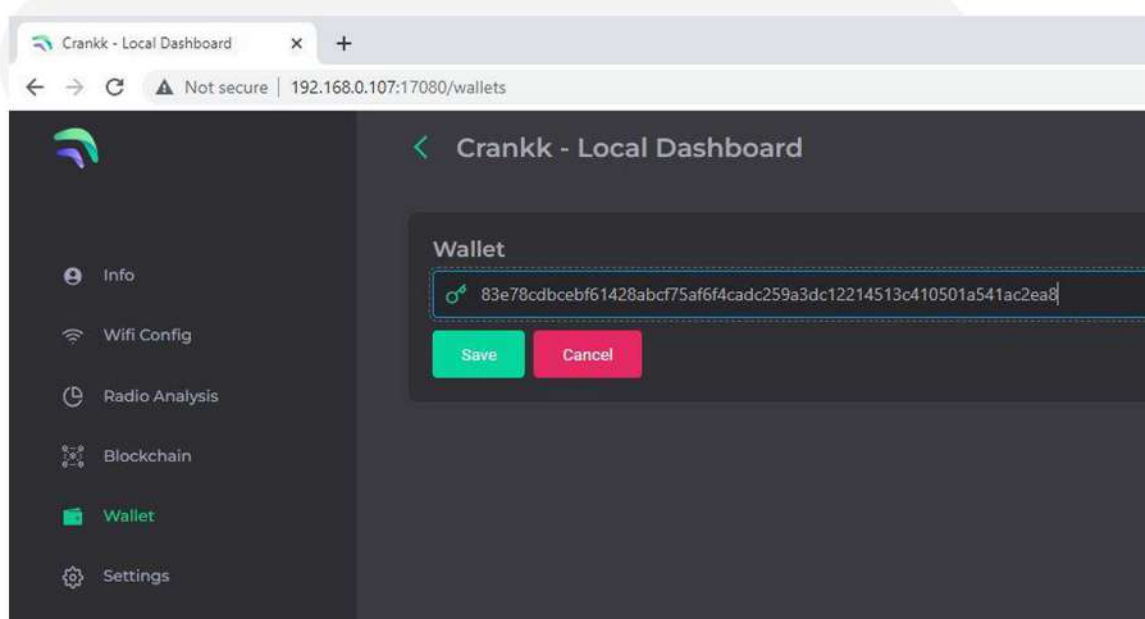


12. Import you secret key.

Hint: If you don't have your secret key saved, you can go to the **User Dashboard** > **Wallets** > find the correct wallet > use the three dots to reveal the secret key.

Navigate to the **Wallet** section in the **Local Dashboard** and enter your **secret key**, keeping the following in mind:

- Please ensure that you copy and paste the **secret key** exactly as it is, without any spaces or other symbols
- Please double-check that it is the correct **secret key** and that it does not belong to another gateway
- Please also note that your **secret key** is different from your **wallet address/public key** starting with k:



Hit **Save**.

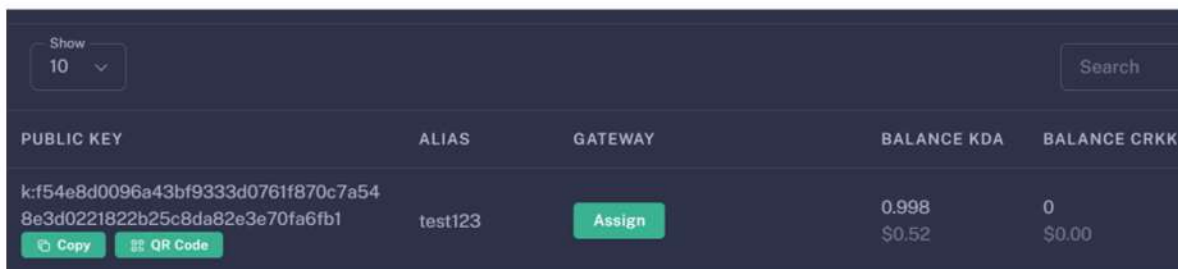
If you have entered the correct secret key, then you will see your **k: wallet address** displayed in the **Wallet** field.

3) User Dashboard setup

13. Assign your gateway ID to a wallet in the User Dashboard.
Log in to the **User Dashboard**.

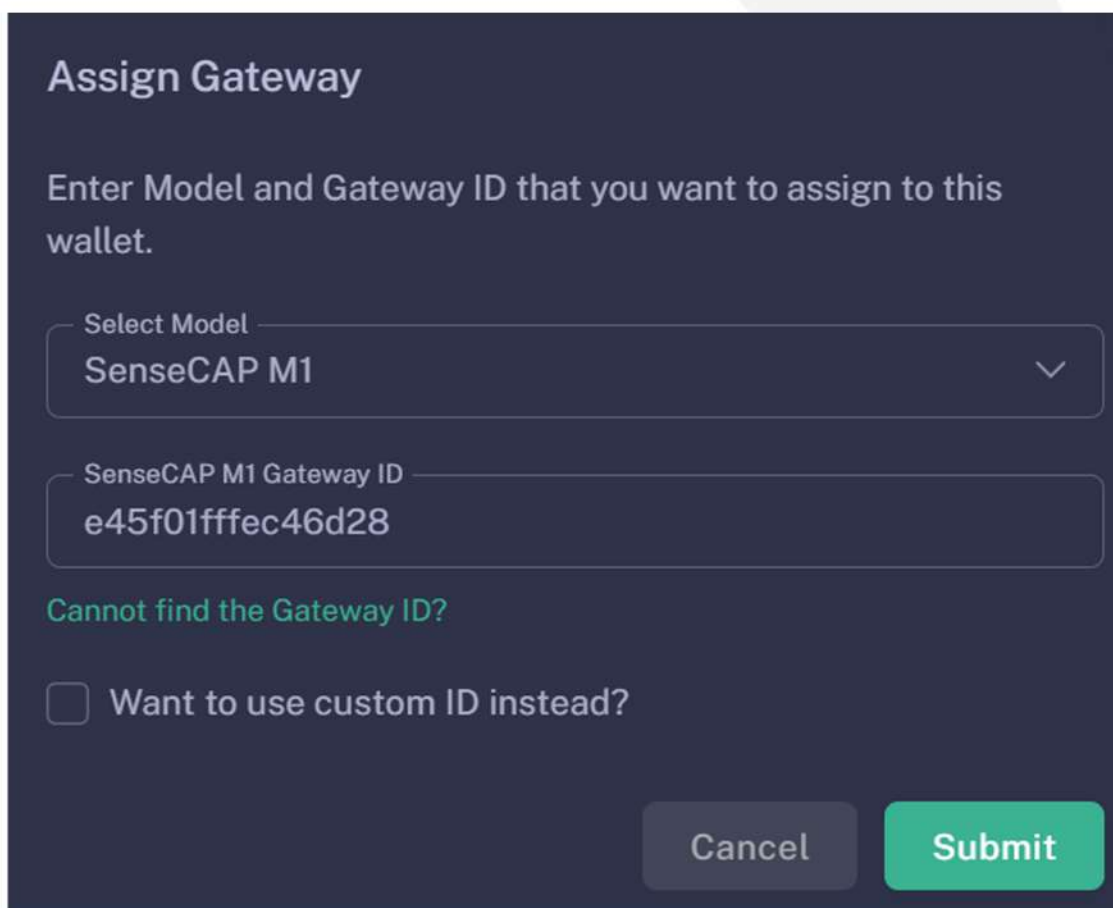
Navigate to the **Wallets** section and select the wallet that you want to use for your software license activation.

Assign your gateway ID to the chosen wallet by clicking on the **Assign** button. If you don't see such a button, it means you haven't purchased a software license for this wallet.



PUBLIC KEY	ALIAS	GATEWAY	BALANCE KDA	BALANCE CRKK
k:f54e8d0096a43bf9333d0761f870c7a54 8e3d0221822b25c8da82e3e70fa6fb1	test123	Assign	0.998 \$0.52	0 \$0.00

Select your gateway **Model**, copy and paste your **Gateway ID** (please double-check that it is correct) and hit the **Submit** button.



Assign Gateway

Enter Model and Gateway ID that you want to assign to this wallet.

Select Model
SenseCAP M1

SenseCAP M1 Gateway ID
e45f01fffec46d28

[Cannot find the Gateway ID?](#)

Want to use custom ID instead?

Cancel Submit

Please wait a few minutes to allow the changes to sync to the blockchain.

Congratulations! You have successfully onboarded your SenseCAP M1 gateway on Crankk!

** Crankk currently supports the following frequencies: EU868 MHz, AU915 MHz and US915 MHz. It is essential to ensure that any hardware purchased from a third-party company for use with Crankk operates on the correct frequency for your region of residence. Crankk Inc. assumes no responsibility for any issues arising from the use of hardware with an incorrect frequency. It is the responsibility of the user to select the appropriate frequency for their region of residence.*

Please note that any modifications, updates or restrictions made by the gateway manufacturer that may impact the performance or functionality of the gateway on the Crankk network are beyond the control and responsibility of Crankk Inc. Users are advised to check compatibility and seek assistance from the gateway manufacturer for any gateway-related issues.