



# **DX-CP34 module**

## **Example of communication operation**

Version: 1.0

Date: 2025-12-30





## Updated records

Version	Date	Instructions	Author
V1.0	2026/03/09	Initial version	LJH

## Contact Us

**SHEN ZHEN DX-SMART TECHNOLOGY CO.,LTD,**

Email: [manager@szdx-smart.com](mailto:manager@szdx-smart.com)

Tel: 0755-2997 8125

Whatsapp: +86 15798463070

Website: [en.szdx-smart.com](http://en.szdx-smart.com)

Address: 601, A1 Block, Huafengzhigu, Hang Kong Road, Hang Cheng Street, Baoan District, Shenzhen

## Contents

0. Operational Process Framework.....	4 -
0.1 Description of the overall system architecture.....	4 -
0.2 Operation process.....	4 -
1. Cloud server operation:.....	5 -
1.1 TTN account creation & login:.....	5 -
1.2 Go to the console:.....	6 -
2. Gateway deployment.....	7 -
2.1 Gateway Registration:.....	7 -
2.2 deployment gateway:.....	10 -
2.2.1 Gateway access.....	10 -
2.2.2 Gateway Configuration.....	11 -
2.2.3 Gateway access network.....	14 -
3 Connect the lora terminal device to the network.....	15 -
3.1 Create Applications:.....	15 -
3.2 lora Terminal Device Registration:.....	16 -
3.3 Connecting lora terminal device to the network:.....	17 -
4. Accessories.....	18 -
4.1 CP34 parameter query.....	18 -
4.1.1 OTAA network information query.....	18 -
4.2 Example lora test script.....	21 -



## 0. Operational Process Framework

### 0.1 Description of the overall system architecture

This product works based on the LoRaWAN standard protocol. The overall system consists of the following four parts:

- (1) LoRaWAN cloud server:
  - a) It is used for unified management of LoRaWAN gateway and LoRaWAN terminal devices, and to complete device network, data reception and forwarding
  - b) This instruction takes **TTN (The Things Network) platform** as an example
- (2) LoRaWAN Gateway:
  - a) It is responsible for receiving wireless data from lora terminal devices and forwarding the data to the cloud server through the Internet
  - b) The **RAK gateway** is used as an example to illustrate this operation instruction
- (3) LoRaWAN terminal equipment:
  - a) Low-power wireless node that is responsible for reporting data to the server periodically or on demand
  - b) This operation guide **CP34** is illustrated as an example
- (4) Beacon Terminal equipment:
  - a) Radio iBeacon low-power Beacon Beacon, sustainable and Eddystone data
  - b) The broadcast data of the device is scanned and collected by CP34 and uploaded to the server through the LoRaWAN network
  - c) This operation guide **CP27** is illustrated as an example

### 0.2 Operation process

- (1) Create an account and log in to the TTN cloud server background
- (2) Register the gateway on the cloud server, and after the registration is completed, deploy the RAK gateway to access the network
- (3) The Applications and LoraWAN terminal devices are registered in the cloud server, and after the registration is completed, the CP34 is powered on and configured to connect to the network
- (4) Data uplink test (CP34 will automatically scan and collect the broadcast data of CP27 and report it to the TTN server)

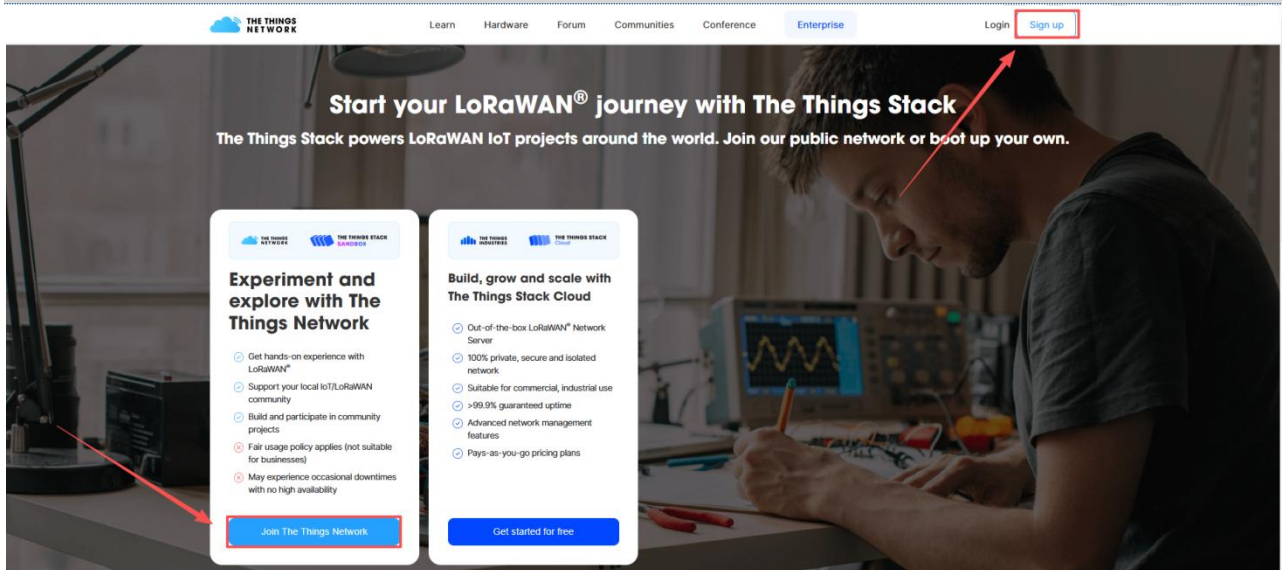
## 1. Cloud server operation:

(TTN server, for example, TTN address: <https://www.thethingsnetwork.org/get-started>).

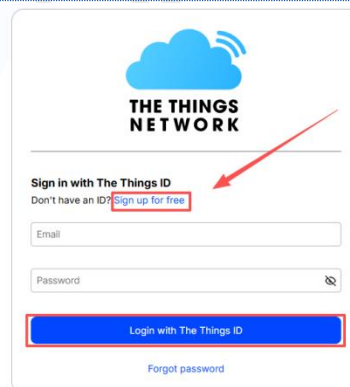
### 1.1 TTN account creation & login:

(1) Click "Sign up" and select "Join The Things Network"

Note: The "Get started for free" option on the right, for paid items, can be selected on demand



(2) Click "Sign up for free", follow the instructions to register, and log in after the registration is completed





**Create one ID to get access to all our products.**

One secure account for The Things Network and future services gathered in one place.

Username •

Email •

Password •

Must be at least 6 characters

Confirm Password •

Must be identical as above

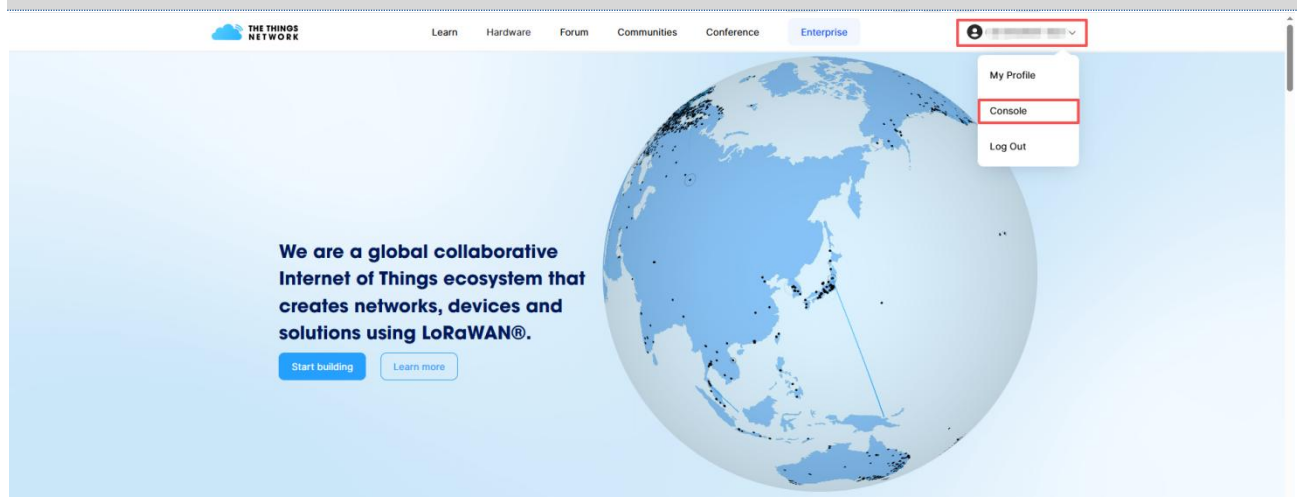
☐ By checking this box, you agree to our [Terms and Conditions](#) and [Privacy Policy](#).

Sign up to The Things ID

Cancel

## 1.2 Go to the console:

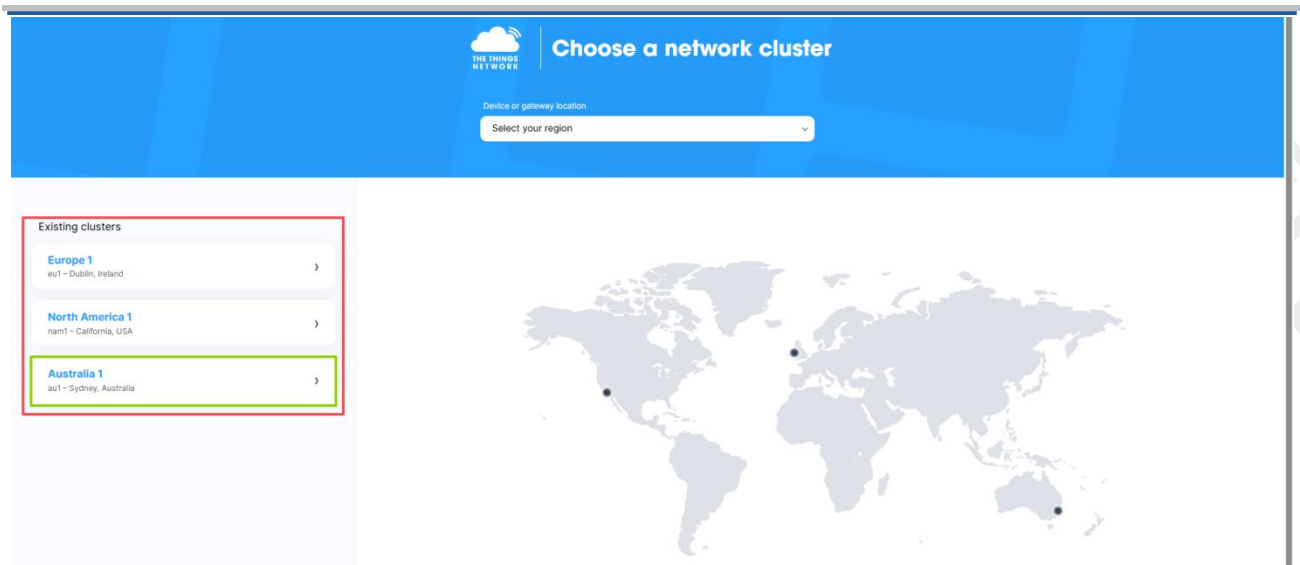
(1) Once logged in, click "Console" to access the console



(2) Select your cluster

*Note:* 1. The next login operation needs to select the same cluster

2. The registration and operation of the gateway and the device must be under the same cluster, otherwise they cannot interoperate



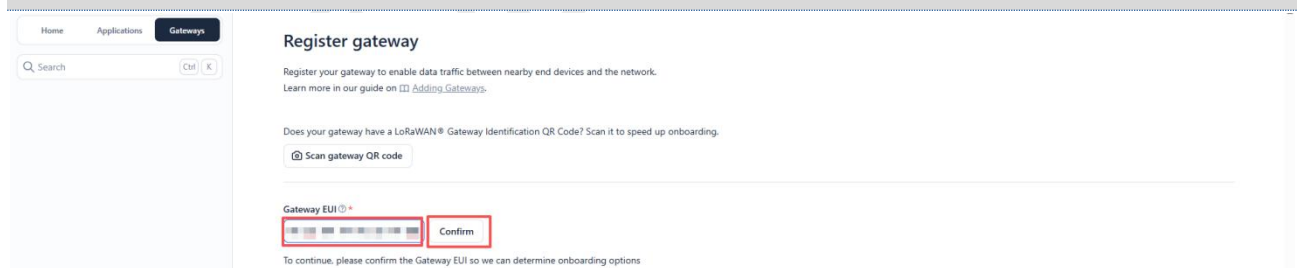
## 2. Gateway deployment

### 2.1 Gateway Registration:

(1) Select "Gateways" and click "Register gateway"



(2) Write the EUI of the gateway and click "Confirm"

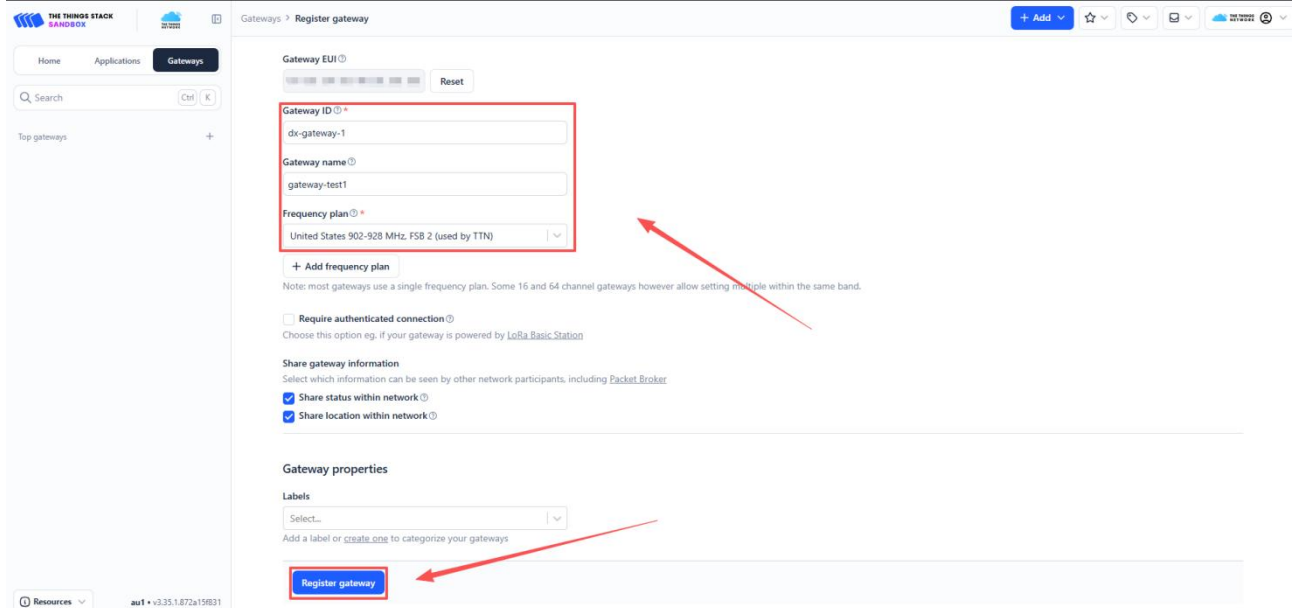


- (3) Fill in the main information of the gateway and click "Register gateway" after filling in:
- Gateway ID: Within the same account, the ID must be unique
  - Gateway name: Gateway name; Used to assist in identifying the gateway and can be left blank
  - Frequency Plans: Frequency plan; Select the frequency of the equipment support plan  
*For example: the United States, 902-928 MHz, the FSB 2 2 by TTN*

Note: 1. The rest of the parameters can be filled in according to the requirements

2. Please refer to TTN official documents for specific parameters

3. Gateway ID must be unique within the same Tenant and cannot be reused after deletion



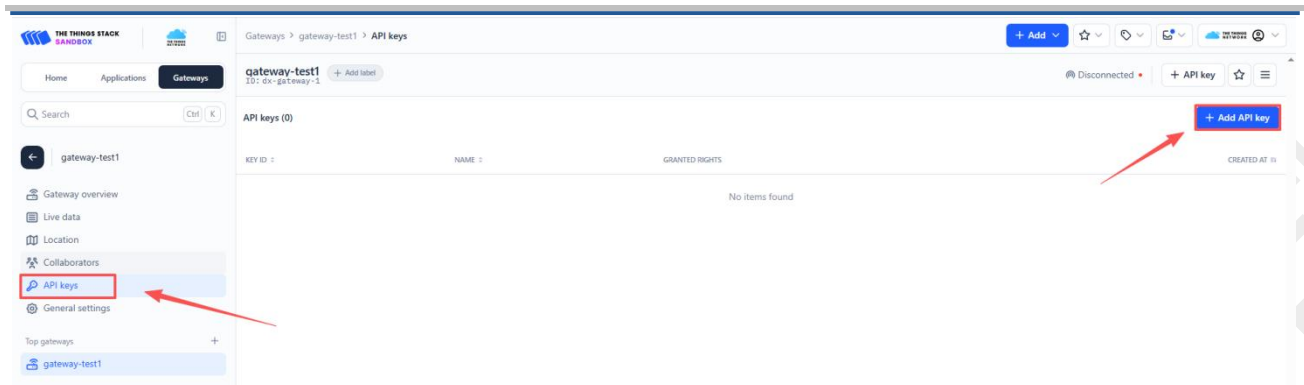
The screenshot shows the 'Register gateway' form in the LoRaWAN console. The form includes fields for Gateway EUI, Gateway ID, Gateway name, and Frequency plan. A red box highlights the Gateway ID field, and a red arrow points to the 'Register gateway' button.



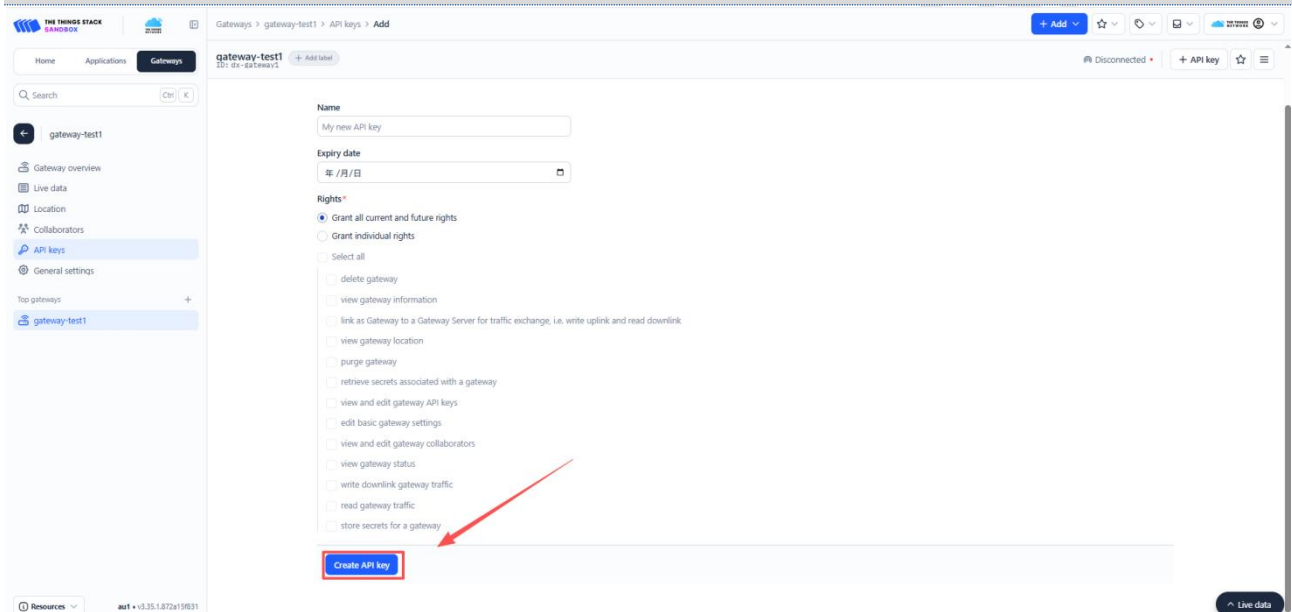
The screenshot shows the 'Register gateway' form with a tooltip explaining the Gateway ID field. The tooltip states: "What is this? A mandatory identifier for your gateway that must be unique per network and cannot be changed after creation. It is used to reference your end device e.g. in events, webhooks and API requests. What should I enter here? Enter a value using lowercase letters, numbers, and dashes. You can choose this freely." A red box highlights the "Read more" link in the tooltip.

- (4) create API KEY, on the left side of the choice "API keys", click "+ Add API KEY"



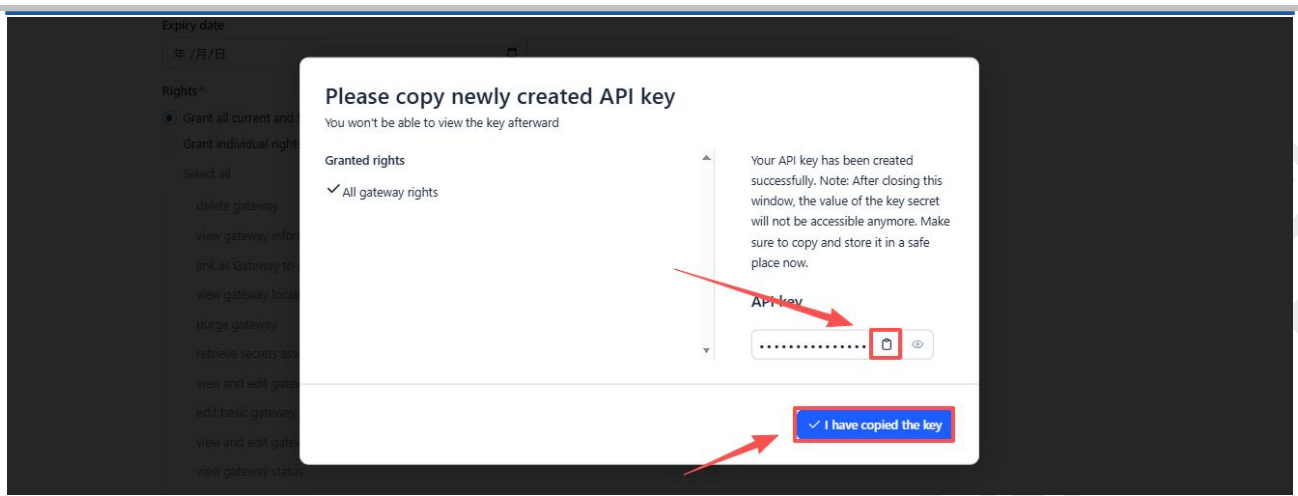


(5) the sample according to the default Settings, also can set the permissions according to their demand, set after clicking "Create API key"



(6) copy the generated API KEY, can save it to the follow-up to the position of the view again, click the "I have copied the KEY"

*Note:* the close the window, the API KEY can't see, so you need to save it in a safe place



## 2.2 deployment gateway:

(gateway RAK7268, for example)

### 2.2.1 Gateway access

**Note:** (1) There are two different ways to access the gateway background. According to the actual needs, choose one of the access methods

(2) the gateway status lights change, will be subject to actual gateway model, here are for reference only

#### Wi-Fi AP mode

(1) The gateway power supply, need to wait a few minutes, wait for the breath light to start slowly flashing, indicating that the gateway started successfully

(2) Using a PC with a wireless network card, find the SSID name in WiFi network list for RAK72XX\_YYYY WiFi network

(3) After connected to the gateway of WiFi, input 192.168.230.1 in the browser's address bar, enter the gateway background

*Note:* 1. RAK72XX is selected, the make and model of the gateway YYYY is gateway EUI after four

2. If the following warning message is returned, select "Advanced Options" according to the following steps to continue to access the gateway background



Your connection is not private

Attackers might be trying to steal your information from **192.168.230.1** (for example, passwords, messages or credit cards). [Learn more about this warning](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Turn on enhanced protection to get Chrome's highest level of security

Hide advanced

Back to safety

This server could not prove that it is **192.168.230.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.230.1 (unsafe)

## WAN Port Method

- (1) Gateway of power supply, need to wait a few minutes, wait for breathing lamp slowly began to flicker, gateway started successfully
- (2) Connect the network cable to the gateway's network port, and connect the other end to the PC network port
- (3) Enter **169.254.X.Y** in the address bar of your browser to enter the gateway background

*Note:* 1. **X.Y** calculation method: Take the last four bits (2 bytes) of the gateway EUI and convert them from hexadecimal to decimal

(such as: such as gateway EUI after four to 86:20 5 converting into 134, 32, the gateway IP is: 169.254.134.32)

2. If return the following warning message, can complete the following steps to select "advanced options", continue to access gateway background



Your connection is not private

Attackers might be trying to steal your information from **192.168.230.1** (for example, passwords, messages or credit cards). [Learn more about this warning](#)

NET::ERR\_CERT\_AUTHORITY\_INVALID

Turn on enhanced protection to get Chrome's highest level of security

Hide advanced

Back to safety

This server could not prove that it is **192.168.230.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.230.1 (unsafe)

## 2.2.2 Gateway Configuration

- (1) To enter the gateway background for the first time, you need to set a password. And select the country or region you are in
- (2) the subsequent available this password to log in, account by default "root"



**Set your password**

Before your first login, you need to set a password for your account.

Password

Confirm password

☒ I hereby acknowledge and agree with the Licence Agreement

Set password

Simple access to your gateways

Select your country

Selecting the correct country will assure you are operating under the local law requirements. The transmit power of your gateway will be set to the local regulation maximum and the LBT feature will be turned on if required.

Country

Region

☒ I confirm that I have chosen the country where the gateway is located. I acknowledge that countries have different rules applicable to the radio band of a gateway and if I chose the wrong country, I may be in breach of the local legislation. I further agree to indemnify and hold the manufacturer, seller, and their respective affiliates harmless in case I choose the wrong country and thus violate the applicable law.

Confirm

**Login**

Login

root

Password

Login

Simple access to your gateways

Click the second option in the left navigation bar, and then click Configuration. Work mode choice "Basics station"

RAK7268V2

Overview Configuration Applications Gateways

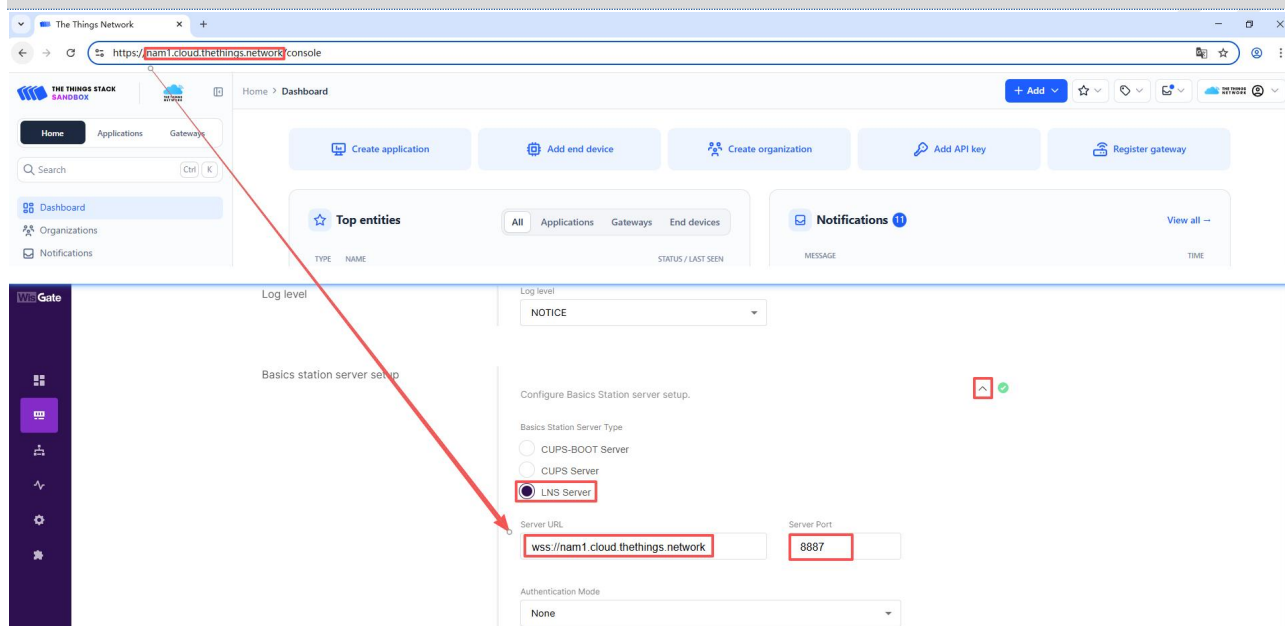
Work mode

Log level

NOTICE

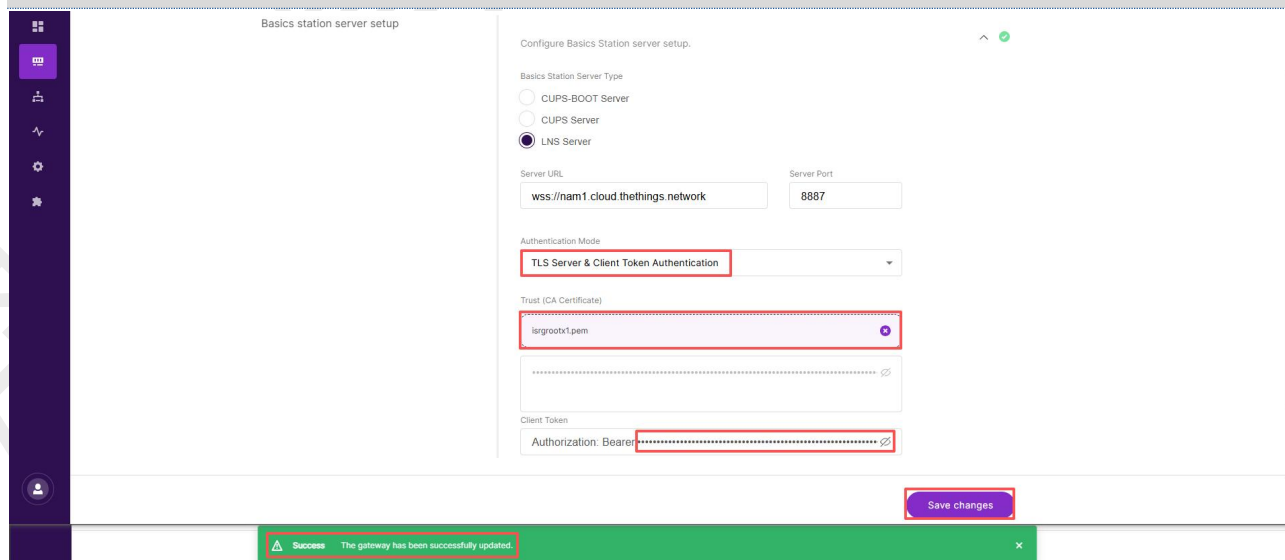
(4) Do the following to configure

- a. Basics Station Server Type: Select "LNS Server"
- B. the server URL: copy TTN console URL, in front of the URL and WSS: //
- C. port number: 8887 by default



(5) Do the following to configure

- a. Authentication Mode: Select "TLS Server and Client Token Authentication"
- B. trust certificate (CA) : from the data package to upload isrgrootx1. Pem file upload (can also be downloaded from [RAK document center](#))
- C. the client Token: duplicate step 2.1 (6) of the API KEY
- d. Click "Save Changes", wait for a period of time, the bottom of the browser prompts "Success", the save is successful



### 2.2.3 Gateway access network

**Note:** (1) the gateway access networks have two different ways. According to the actual needs, choose one of the access methods

(2) the gateway status lights change, will be subject to actual gateway model, here are for reference only

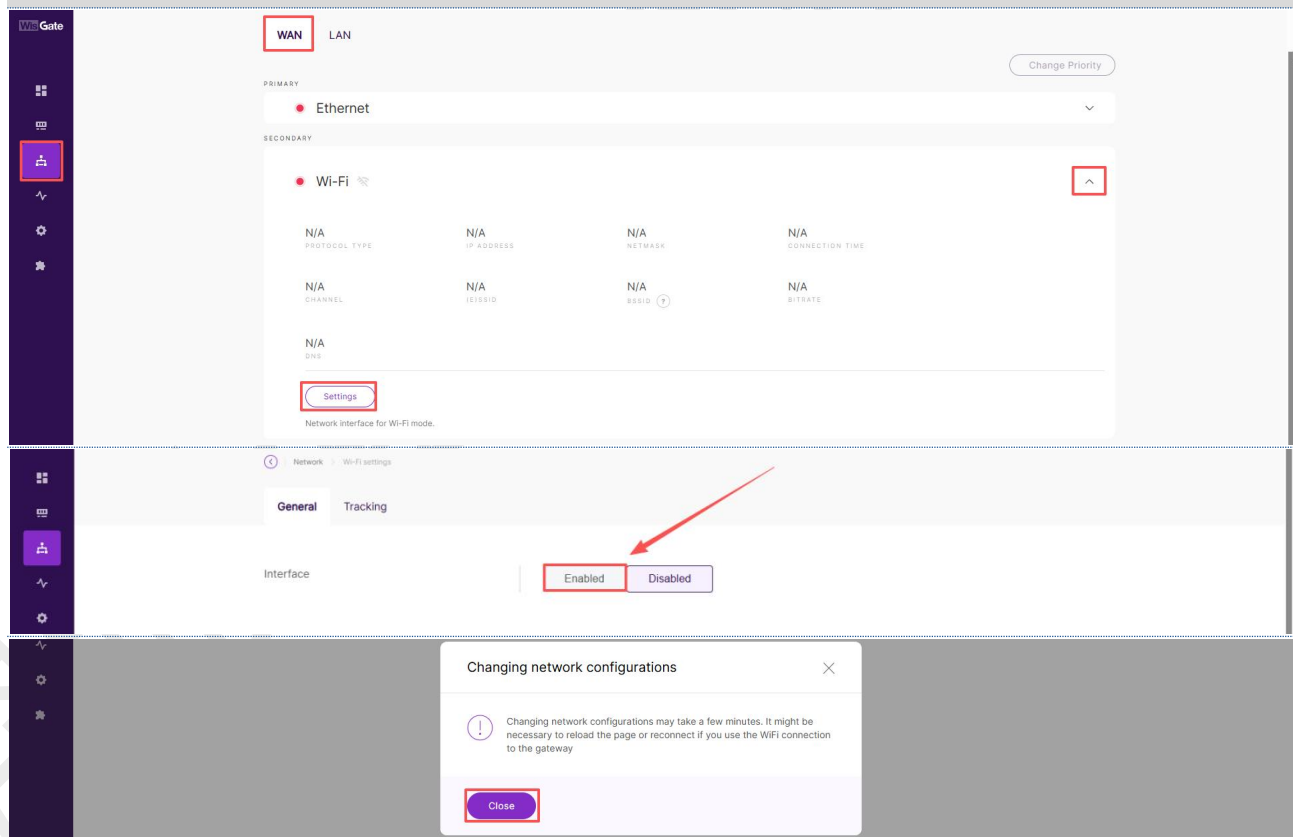
#### Connect via WiFi

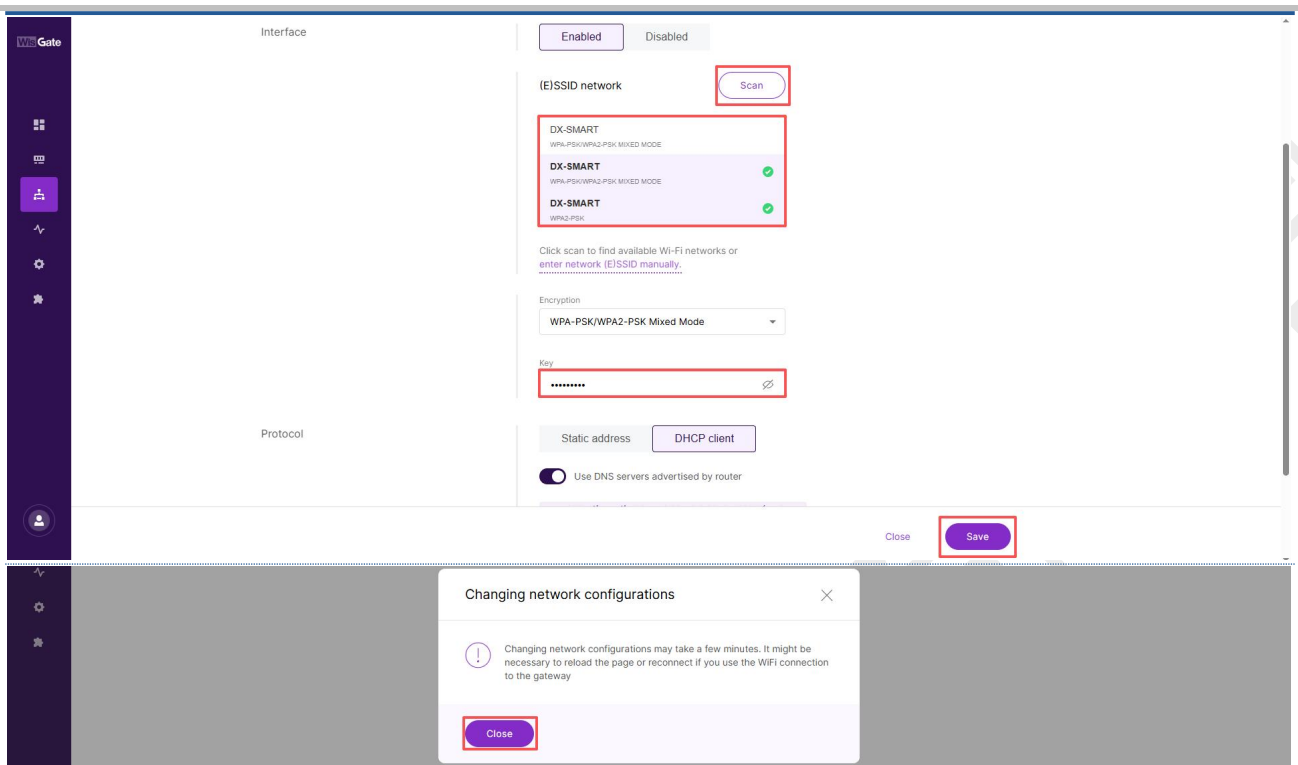
(1) In the gateway backstage, click on the left navigation bar and the third option, click on the "WAN", in the "wi-fi" option, click "Settings"

(2) Click on the "Enabled", according to the prompt, click "close", wait for a while, or reconnect WiFi and reload interface

(3) Click the "Scan" button, select the AP that needs to be connected, enter the corresponding password, and click "Save".

(4) Turn off the prompt and wait for the connection, when the gateway's breath light changes from green to blue, the network connection is successful





### Connect via Ethernet

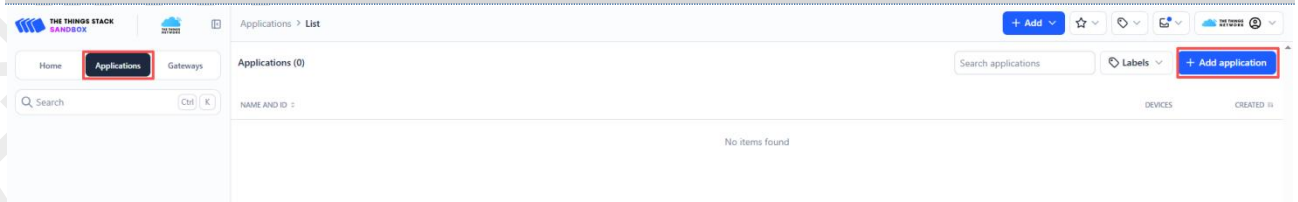
- (1) The cable received so from the gateway, the other end connected to the router, switch, or superior network equipment
- (2) Wait for a period of time, when the gateway's breathing light changes from green to blue, it means that the network connection is successful

## 3 Connect the lora terminal device to the network

### 3.1 Create Applications:

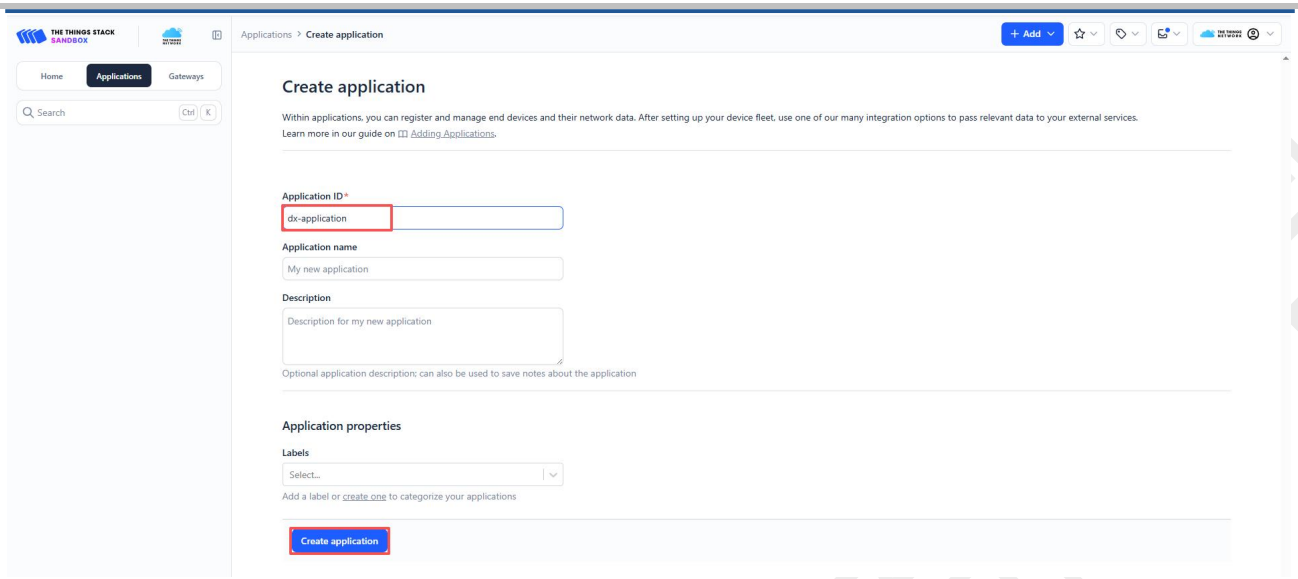
(To manage the subsequent addition of lora end devices)

- (1) Go back to the TTN console, select "Applications" and click "Add application"



- (2) set Applications ID, click on the "Create application"

*Note:* Applications within the same Tenant ID must be unique, and cannot reuse after deletion



**THE THINGS STACK SANDBOX**

Applications > Create application

**Create application**

Within applications, you can register and manage end devices and their network data. After setting up your device fleet, use one of our many integration options to pass relevant data to your external services. Learn more in our guide on [Adding Applications](#).

**Application ID \***  
dx-application

**Application name**  
My new application

**Description**  
Description for my new application

Optional application description; can also be used to save notes about the application

**Application properties**

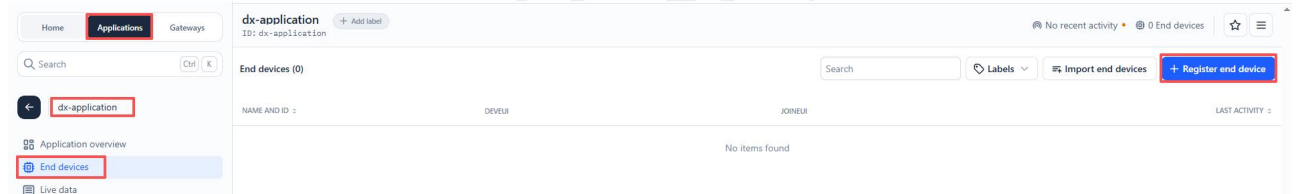
**Labels**  
Select...

Add a label or [create one](#) to categorize your applications

**Create application**

## 3.2 lora Terminal Device Registration:

(1) Click on the created Applications, select "End devices", and click "Register end device"



**dx-application**  
ID: dx-application

End devices (0)

**Register end device**

4.1 (2) refer to the attachment, confirm the OTAA net information: APPEUI, DevEUI, AppKey

(3) select "Enter end device specifics manually", manual input device information:

Frequency Plans: Select the same frequency plan as the gateway

Choose "LoRaWAN LoRaWAN version: Specification 1.0.2"

Regional Parameters version: select "RP001 Regional Parameter 1.0.2"

JoinEUI: also known as APPEUI, fill in step 3.2 (2) obtain APPEUI parameters, click on the "Confirm"

DevEUI: Fill in the DevEUI parameters obtained in Step 3.2(2)

AppKey: Fill in the AppKey parameters obtained from Step 3.2(2)

End Device ID: can be customized, and must be unique within the same Applications

(3) Once configured, click Register end device





Does your end device have a LoRaWAN® Device Identification QR Code? Scan it to speed up onboarding.

[Scan end device QR code](#) [Device registration help](#)

**End device type**

Input method <sup>ⓘ</sup>

☐ Select the end device in the LoRaWAN Device Repository

☒ Enter end device specifics manually

Frequency plan <sup>ⓘ</sup> \*

United States 902-928 MHz, FSB 2 (used by TTN) <sup>⌵</sup>

LoRaWAN version <sup>ⓘ</sup> \*

LoRaWAN Specification 1.0.2 <sup>⌵</sup>

Regional Parameters version <sup>ⓘ</sup> \*

RP001 Regional Parameters 1.0.2 <sup>⌵</sup>

Show advanced activation, LoRaWAN class and cluster settings <sup>⌵</sup>

**Provisioning information**

JoinEUI <sup>ⓘ</sup> \*

70 B3 D5 7E D0 41 54 00 [Confirm](#)

**Provisioning information**

JoinEUI <sup>ⓘ</sup> \*

70 B3 D5 7E D0 41 54 00 [Reset](#)

This end device can be registered on the network.

DevEUI <sup>ⓘ</sup> \*

70 B3 D5 7E D0 41 54 00 [Generate](#) 0/50 used

AppKey <sup>ⓘ</sup> \*

52 72 06 1C 29 82 4B 2A 46 13 82 D3 D5 C4 3F 4D [Generate](#)

End device ID <sup>ⓘ</sup> \*

dx-device1

**Device properties**

Labels

Select... <sup>⌵</sup>

Add a label or [create one](#) to categorize your devices

**After registration**

☒ View registered end device

☐ Register another end device of this type

[Register end device](#)

### 3.3 Connecting lora terminal device to the network:

Taking CP34 as an example, it is connected to the network through OTAA

(1) Power on the equipment: the equipment is connected to the antenna, connected to the power supply, press the switch machine key, the equipment enters the self-test state, at this time, the three color lights will be synchronized

A quick flicker; After the self-test is completed, the device waits to be connected to the net, at which point the red light will flash quickly

(2) Device access to the network: the device opens automatic access to the network by default. After the self-test is completed, the device automatically connects to the network.

Indicates that the device is successfully connected to the network

(3) Data upload: After successful network access, put our Beacon products near CP34, and CP34 will automatically scan and upload around

Green light flashing Beacon equipment information, when the equipment, equipment are

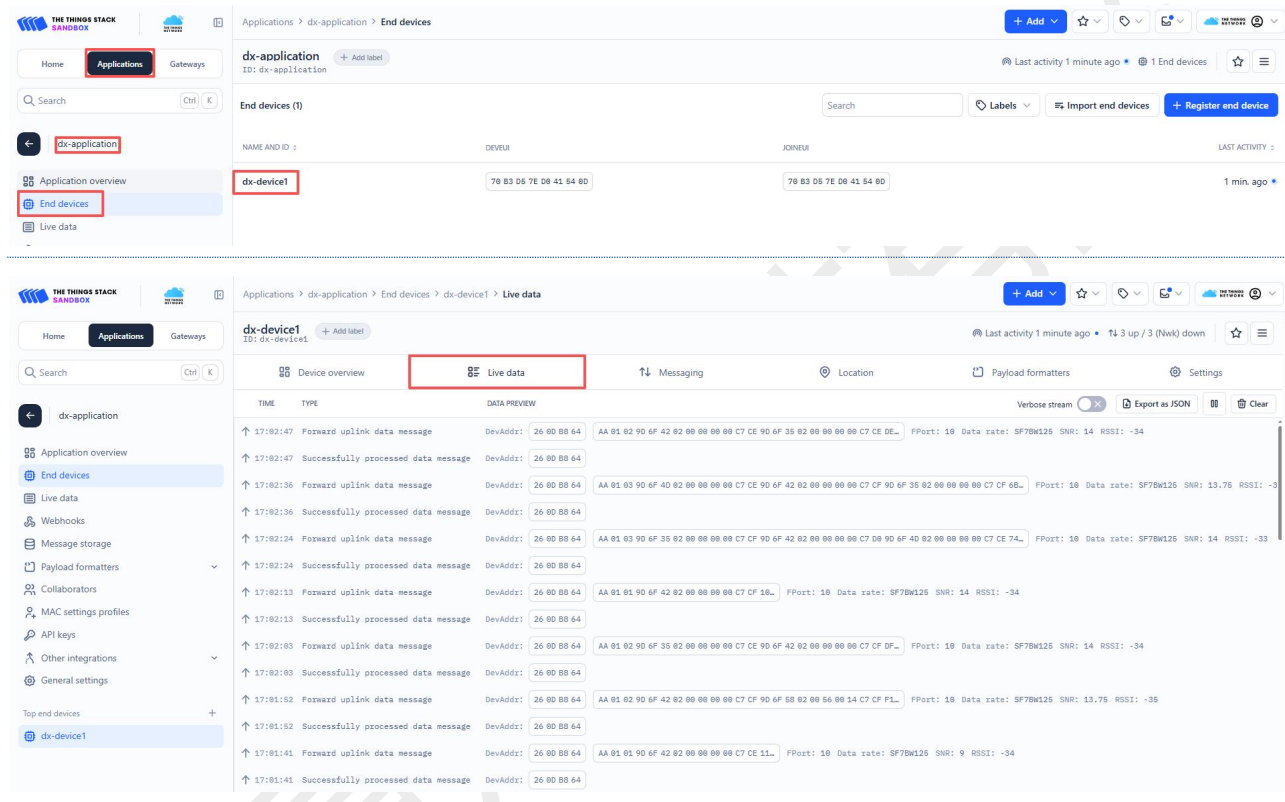
uploading data

**Note:** a. CP34 default RSSI filtering threshold for - 50 DBM, suggest Beacon equipment near CP34 some test stage, so as to avoid unable to

Scan to the device

b. For detailed instructions on the device, please refer to DX-CP34 Technical Manual.DOCx.

c. The real-time information of the equipment can be viewed in the following picture



The screenshot displays the 'The Things Stack' web interface. The top navigation bar includes 'Home', 'Applications', and 'Gateways'. The left sidebar shows a menu with 'End devices' highlighted. The main content area is divided into two sections: 'End devices' and 'Live data'. The 'End devices' section shows a table with columns for 'NAME AND ID', 'DEVICE', 'JOINER', and 'LAST ACTIVITY'. The 'Live data' section shows a table with columns for 'TIME', 'TYPE', and 'DATA PREVIEW'. The 'Live data' section is currently selected, showing a list of data messages with their respective timestamps, types, and data previews.

## 4. Accessories

### 4.1 CP34 parameter query

#### 4.1.1 OTAA network information query

**Note:** (1) parameter query there are two different ways. According to the actual needs, choose one of

them

(2) CP34 default serial port parameters configuration: 9600 BPS / 8 / n / 1 (baud rate/data/no calibration/stop bit)

(3) CP34 default UUID: SERVICE UUID: 6 e400001 b5a3 - f393 e0a9 -- e50e24dcca9e  
NOTIFY/WRITE UUID: 6e400003-b5a3-f393-e0a9-e50e24dcca9e  
WRITE UUID : 6e400002-b5a3-f393-e0a9-e50e24dcca9e

### Via a serial port query

(1) Power on the equipment: the equipment is connected to the antenna, connected to the power supply, press the switch machine key, the equipment enters the self-test state, at this time the three color lights will be synchronized

Fast flashing; After the self-test is completed, the device waits for the network, at which time the blue light and the red light will slow flash synchronously

(2) Tool set: open the serial port tool, select the corresponding COM port and serial port parameters need to pay attention to the AT command without end, a serial port

The tool does not need to add enter to newline

(3) Parameter query: After the device self-test is completed, send the following instructions in turn:

AT+APPEUI, AT+DEVADDR, AT+APPKEY

```
[10:48:53.068]发→◇AT+APPEUI□  
[10:48:53.139]收←◆+APPEUI=70B3D57ED032282F  
OK  
  
[10:48:54.336]发→◇AT+DEVADDR□  
[10:48:54.420]收←◆+DEVADDR=70B3D57ED032282F  
OK  
  
[10:48:55.468]发→◇AT+APPKEY□  
[10:48:55.551]收←◆+APPKEY=5272061C29824B2A461382D3D5C43F4D  
OK
```

### Query by APP

(1) Power on the device: the device is connected to the antenna, connected to the power supply, press the switch button, the device enters the self-test state, at this time, the three color lights will be synchronized

Fast flashing; After the self-test is completed, the device waits for the network, at which time the blue light and the red light will slow flash synchronously

(2) APP connection: Enable the Bluetooth and positioning function of the mobile phone, open the APP, and connect to CP34 according to the steps in the following figure

(3) Parameter query: After successful connection, send the following instructions in turn:

AT+APPEUI, AT+DEVADDR, AT+APPKEY

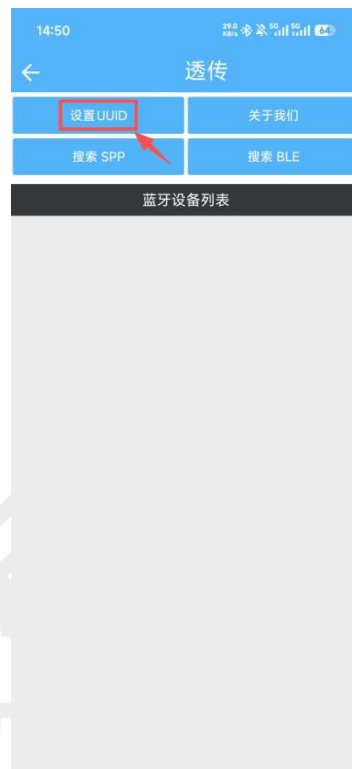


版本号:V2.3

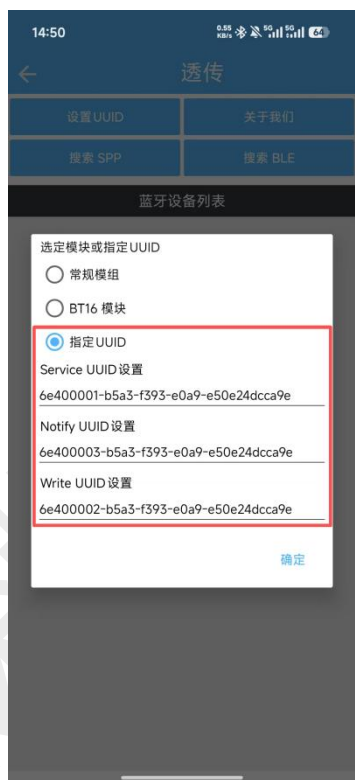
Open the DX-SMART APP



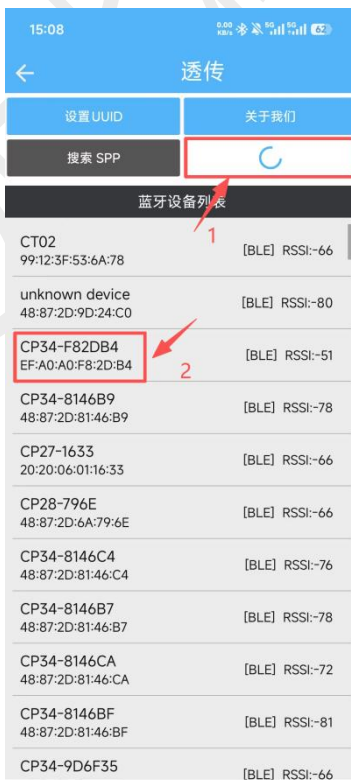
Click ThroughPass



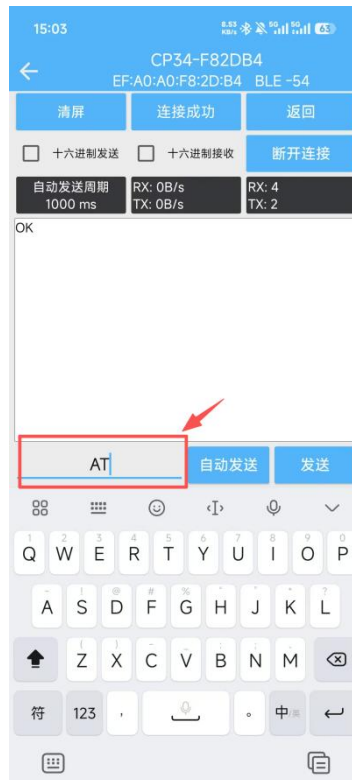
Click Set UUID



Set to the CP34 default UUID



Click Search BLE and find the



Successfully connected



---

module

---

## 4.2 Example lora test script

Note: Refer to Instructions for Use of DX-CP34 Test Scripts in folder 03 Test Tools for details.