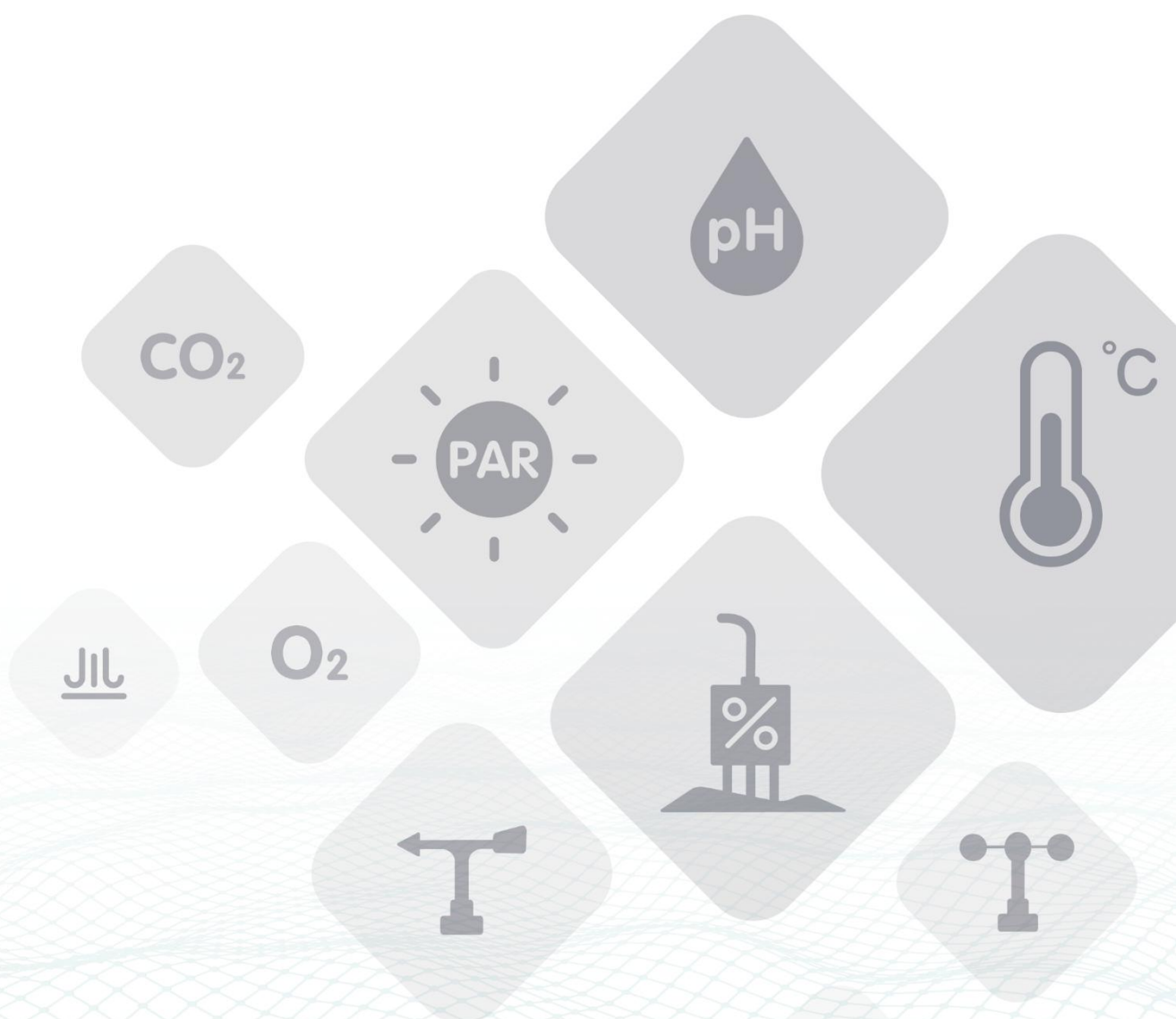


# LoRaWAN Gateway User Guide

Version: V1.4



# Table of Contents

Table of Contents .....	2
1 Product Introduction .....	3
2 Gateway Network Configuration .....	5
2.1 The gateway connects to the Internet .....	5
2.1.1 Installing Antenna .....	5
2.1.2 Connecting to the Internet .....	5
2.1.3 Connecting to Power Cable .....	7
2.1.4 The Function of the Red LED .....	7
2.2 Setting the APN .....	8
3 Add Gateway to User's TTN Server .....	10
3.1 Gateway Network Configuration .....	11
3.1.1 Installing Antenna .....	11
3.1.2 Connecting to the Internet .....	11
3.1.3 Connecting to Power Cable .....	12
3.1.4 The Function of the Red LED .....	13
3.2 Setting the Gateway Service Address .....	14
3.3 Gateway Registration on TTN .....	17
4 Add Gateway to ChirpStack LoRaWAN Network Server Stack .....	20
4.1 Turn on ChirpStack LoRa Server Mode .....	20
4.2 ChirpStack LoRa Server Configuration .....	23
4.3 MQTT Bridge Configuration .....	26
4.3.1 Gateway Configuration .....	26
4.3.2 MQTT Client Configuration .....	30
4.3.3 Scheduling a Downlink .....	31
4.4 ChirpStack Application Server .....	32
4.4.1 Log on to the background .....	32
4.4.2 Add the Network-servers .....	32
4.4.3 Create the Gateway-profiles .....	34
4.4.4 Create the Service-profiles .....	35
4.4.5 Create the Device-profiles .....	37
5 Device Installation .....	40
5.1 Part List .....	41
5.1.1 Gateway Part List .....	41
5.2 Gateway Installation .....	42
5.2.1 Gateway Installation Methods .....	42
5.2.2 Installation Precautions .....	44
5.2.3 Installing Fiberglass LoRa Antenna .....	45

# 1 Product Introduction



SenseCAP is an industrial wireless sensor network that integrates easy-to-deploy hardware and data API services, enabling low-power, long-distance environmental data collection. SenseCAP includes several versions, such as LoRaWAN, LoRaPP, etc.

SenseCAP LoRaWAN Gateways is based on the LoRaWAN protocol, it can realize one-to-many, long-distance networking and bilateral communication. The LoRaWAN Gateway supports Ethernet and 4G.

## Main Features:

- High-performance Cortex A8 1GHz processor
- Multiple methods to connect to the Internet: 4G, Wi-Fi and Ethernet
- Supports third-party TTN account and server
- Super long-distance communication: 10km in the line-of-sight scenario, 2km in the urban scenario
- Industrial protection rating IP66-rated enclosure, suitable for the outdoor environment at  $-40^{\circ}\text{C}\sim 70^{\circ}\text{C}$
- Easy-to-deploy, enabling people without engineering background to install the devices quickly

## LoRaWAN Outdoor Gateway:



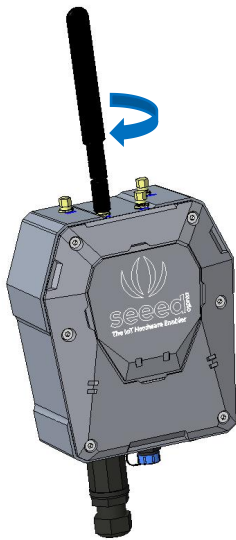
Seeed Technology Co., Ltd. All rights reserved.

## 2 Gateway Network Configuration

### 2.1 The gateway connects to the Internet

#### 2.1.1 Installing Antenna

Screw clockwise to install the 4G and LoRa antennas onto the gateway.

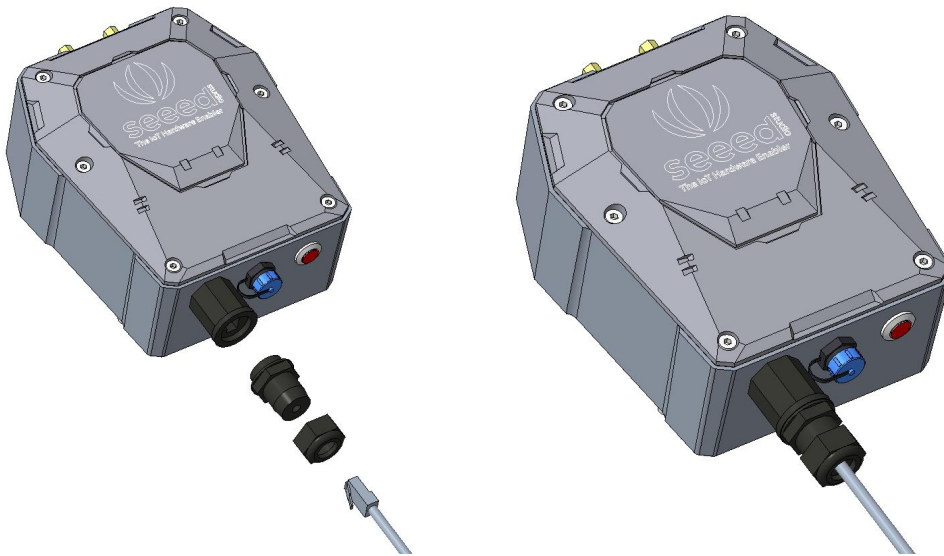


#### 2.1.2 Connecting to the Internet

There are two ways to connect to the Internet. Choose the one that works for you .

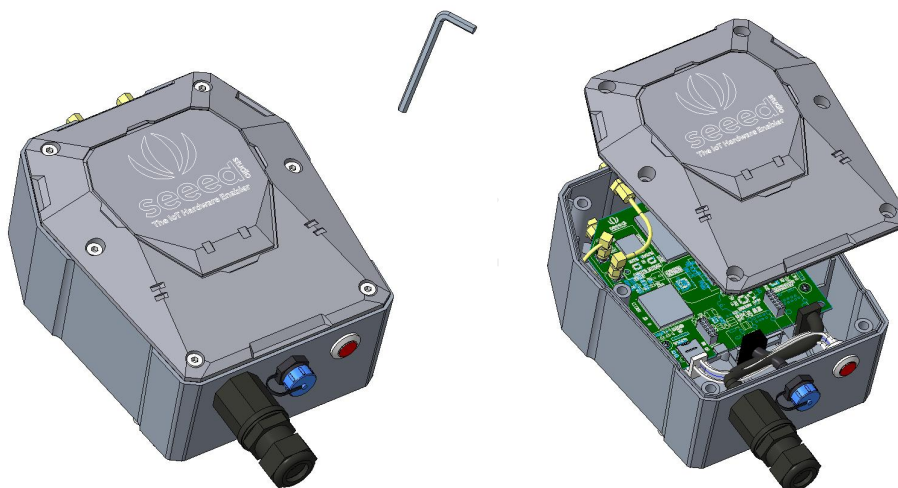
##### (1) Connecting to Ethernet Cable

Unscrew to open the protection cap, plug the Ethernet cable through the cap and then into the Ethernet port. Screw to fasten this part.

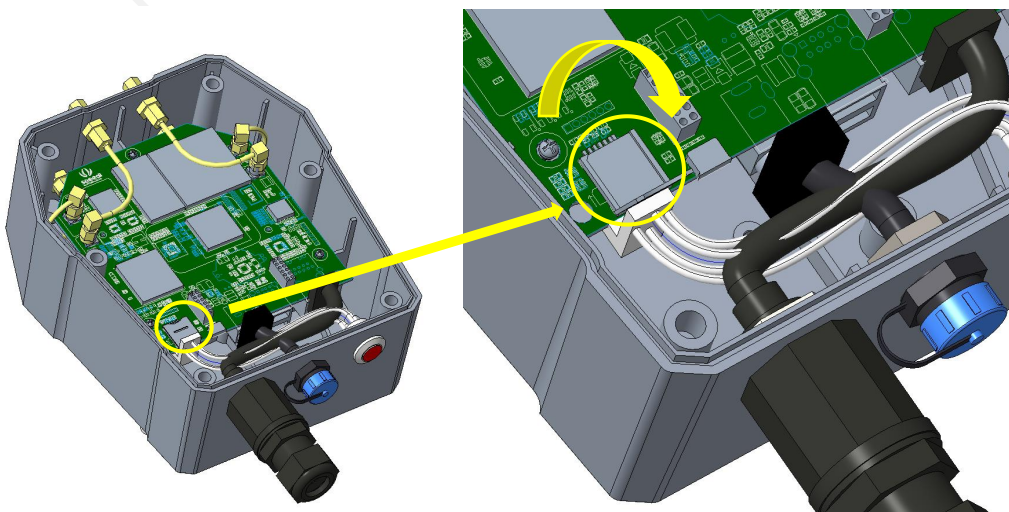


## (2) Connecting to 4G

Use the hex key (included in the package) to unscrew the 6 screws and open the lid.

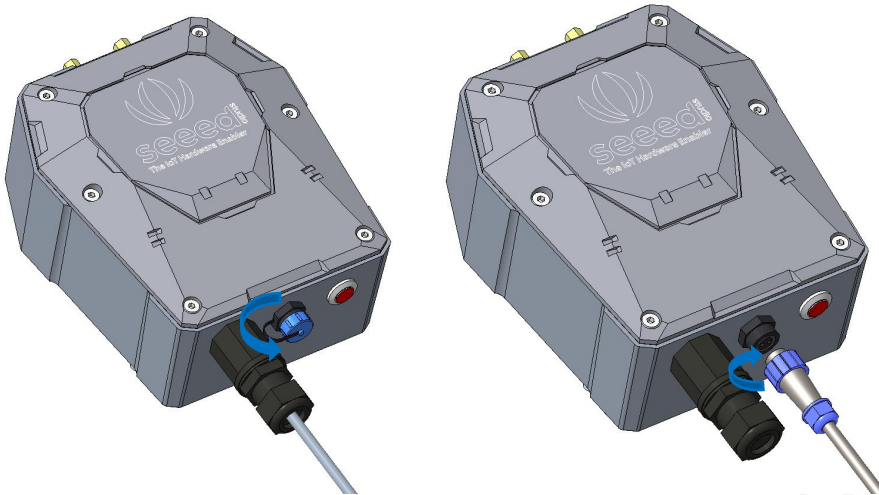


Swipe downward to open the SIM card socket, insert the Micro SIM card and swipe upward to lock the SIM card socket. Make sure it is installed correctly and close the lid with the screws.



### 2.1.3 Connecting to Power Cable

Unscrew to take off the power cap, plug in the extension cord and screw to fasten it onto the gateway. The other end of the extension cord is connected to the power adapter.



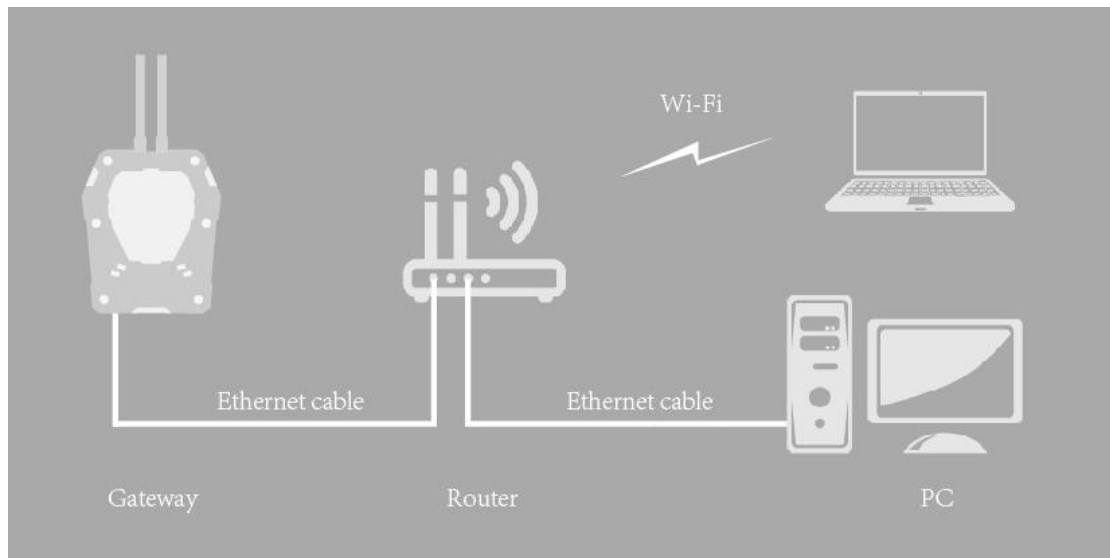
**Notice:** Make sure all antennas are correctly installed before powering on the gateway. Please note the device should be POWERED OFF when installing the antenna, or the antenna circuits might be damaged.

### 2.1.4 The Function of the Red LED

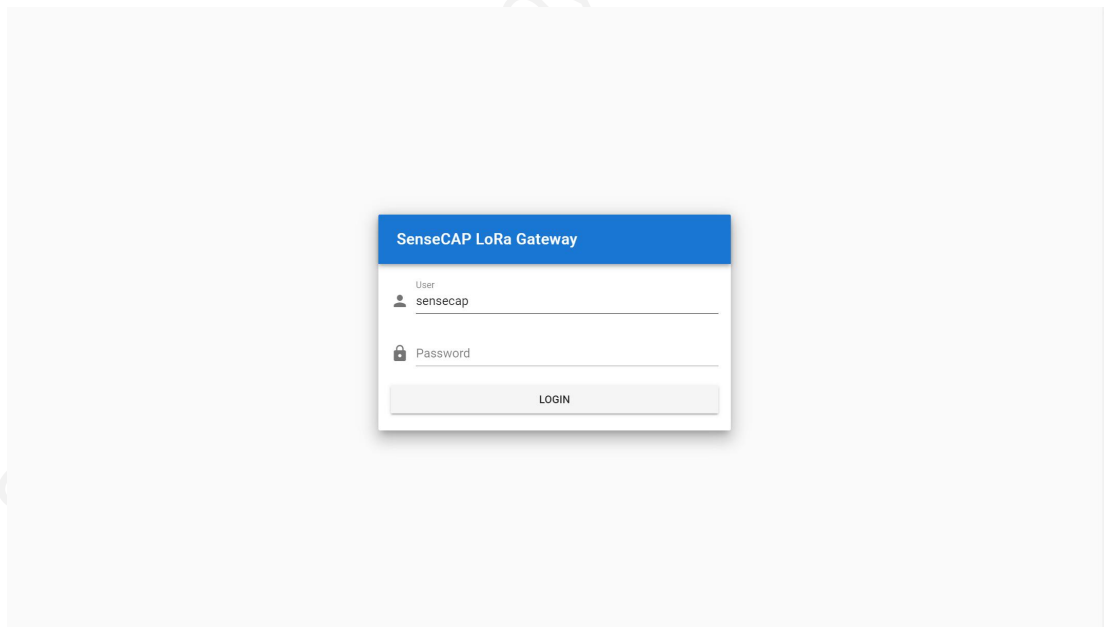


## 2.2 Setting the APN

Prepare a router, and the network connection is shown in the figure:

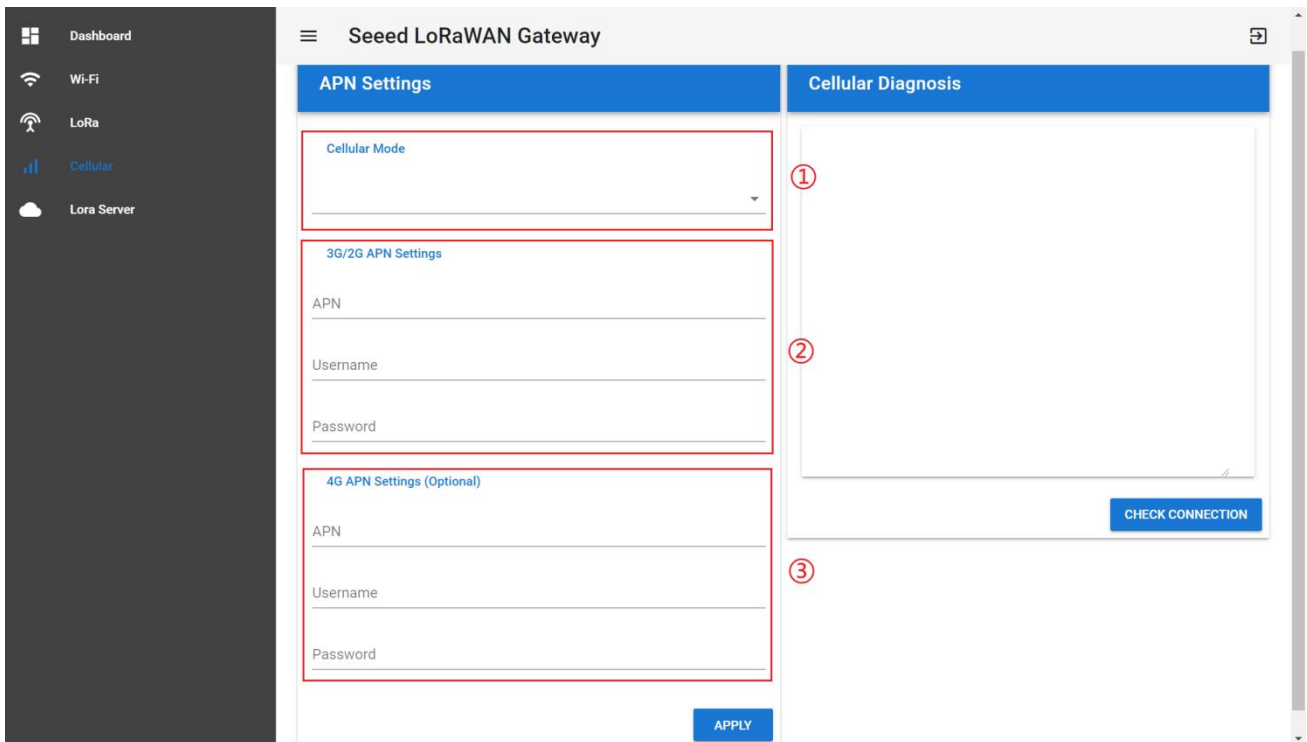


- (1) Check the IP of "sensecap" in the background of the router.
- (2) Enter IP in the browser: IP:8000  
If the IP is 192.168.1.1, enter 192.168.1.1:8000



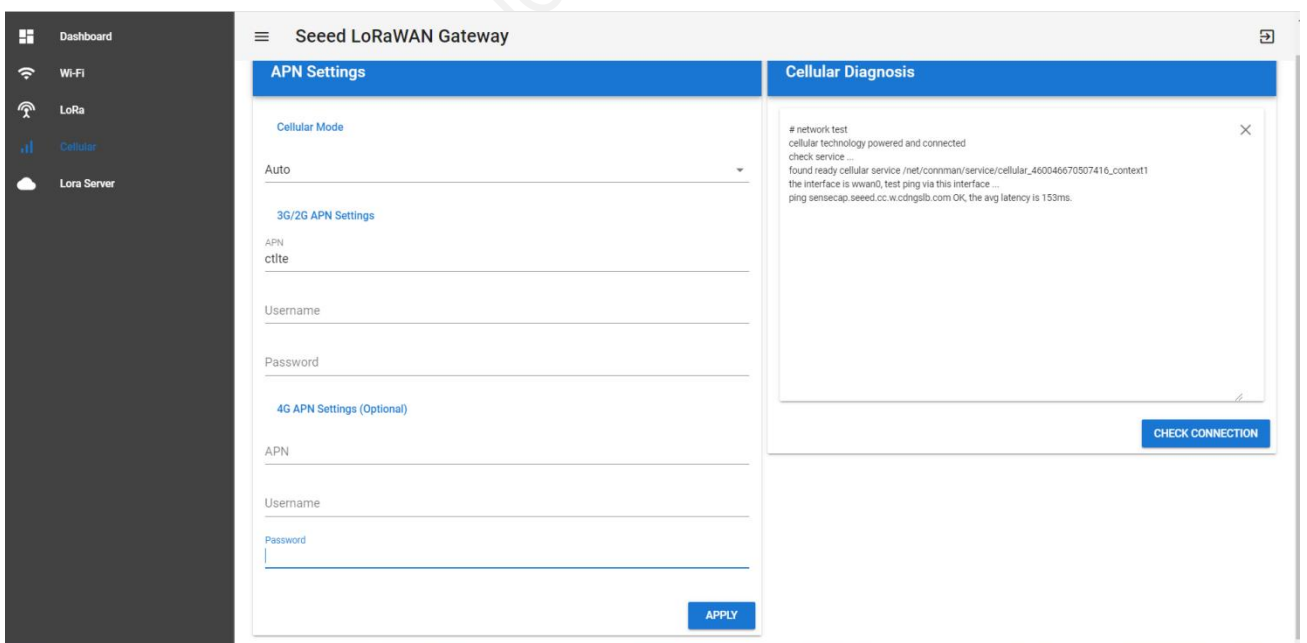
- (3) User: sensecap  
Password: sensecap!!!
- (4) Click the "Cellular" button.





- ① Cellular Mode: AUTO(default), Gateway automatically selects mode.
- ② 3G/2G APN Settings: when the mode is 3G/2G, the APN information of SIM card operator needs to be filled in.
- ③ 4G APN Settings: optional.

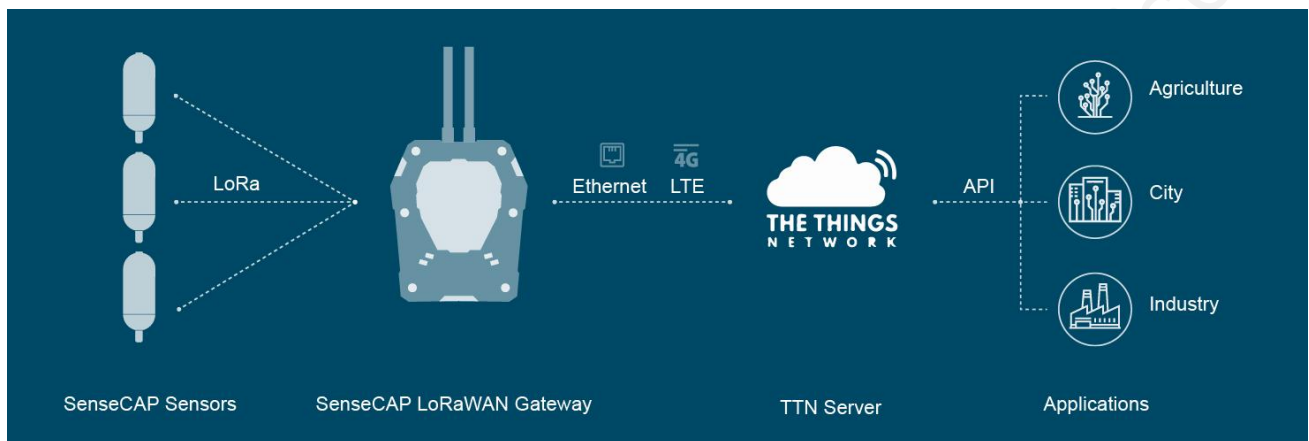
(5) Click "APPLY". Then "CHECK CONNECTION", if return "cellular technology powered and connected", it means ok.



### 3 Add Gateway to User's TTN Server

The SenseCAP LoRaWAN Gateway supports connecting to the user's own The Things Network account and server.

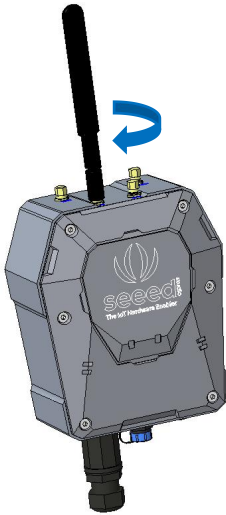
Learn more about TTN: <https://www.thethingsindustries.com/docs/>



## 3.1 Gateway Network Configuration

### 3.1.1 Installing Antenna

Screw clockwise to install the 4G and LoRa antennas onto the gateway.

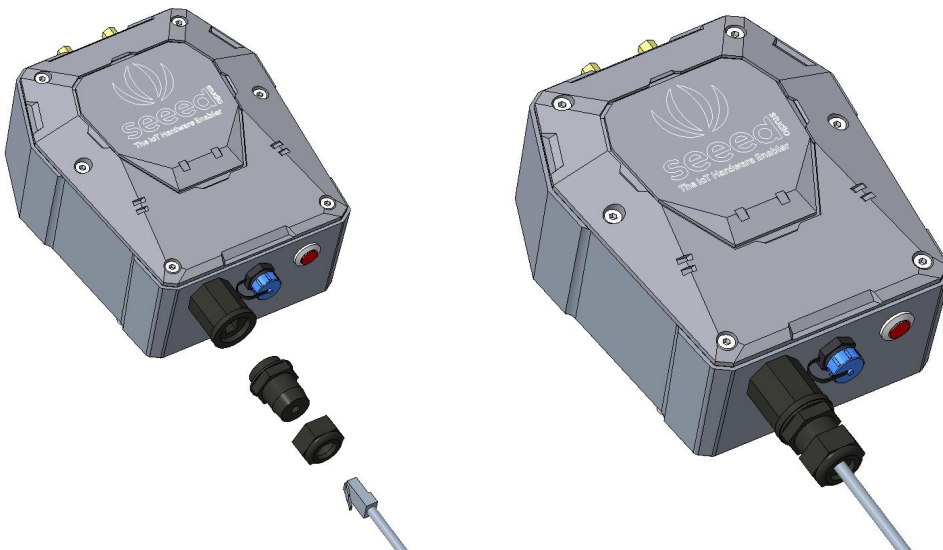


### 3.1.2 Connecting to the Internet

There are two ways to connect to the Internet. Choose the one that works for you.

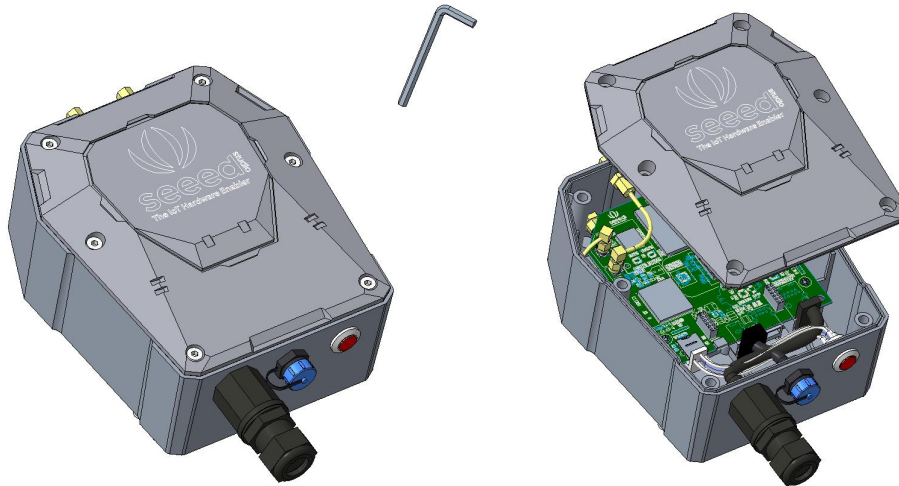
#### (3) Connecting to Ethernet Cable

Unscrew to open the protection cap, plug the Ethernet cable through the cap and then into the Ethernet port. Screw to fasten this part.

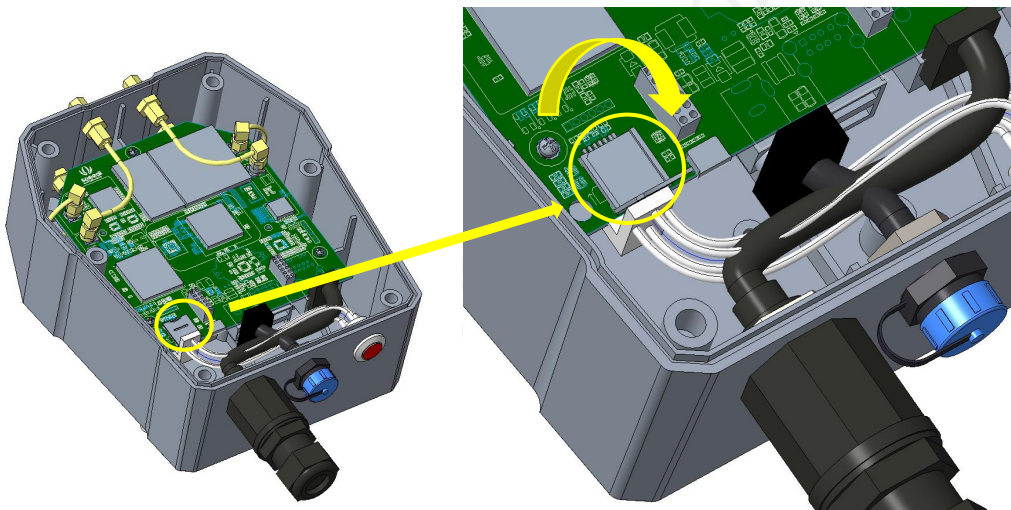


#### (4) Connecting to 4G

Use the hex key (included in the package) to unscrew the 6 screws and open the lid.

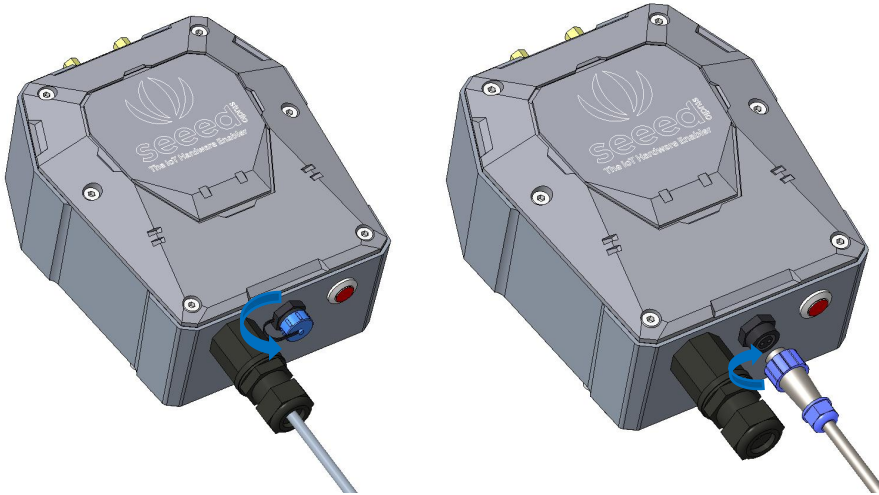


Swipe downward to open the SIM card socket, insert the Micro SIM card and swipe upward to lock the SIM card socket. Make sure it is installed correctly and close the lid with the screws.



### 3.1.3 Connecting to Power Cable

Unscrew to take off the power cap, plug in the extension cord and screw to fasten it onto the gateway. The other end of the extension cord is connected to the power adapter.



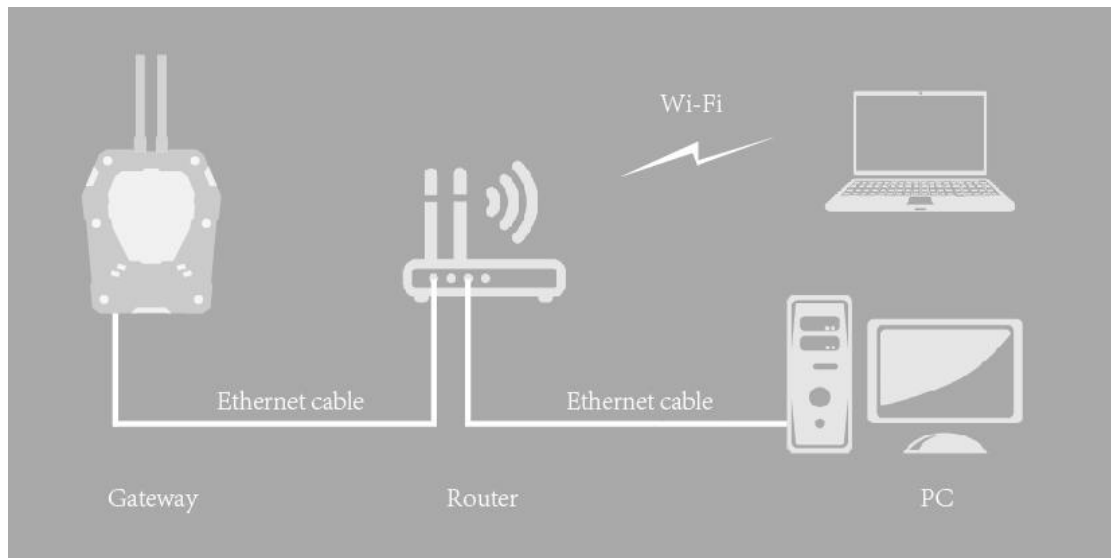
**Notice:** Make sure all antennas are correctly installed before powering on the gateway. Please note the device should be POWERED OFF when installing the antenna, or the antenna circuits might be damaged.

### 3.1.4 The Function of the Red LED



## 3.2 Setting the Gateway Service Address

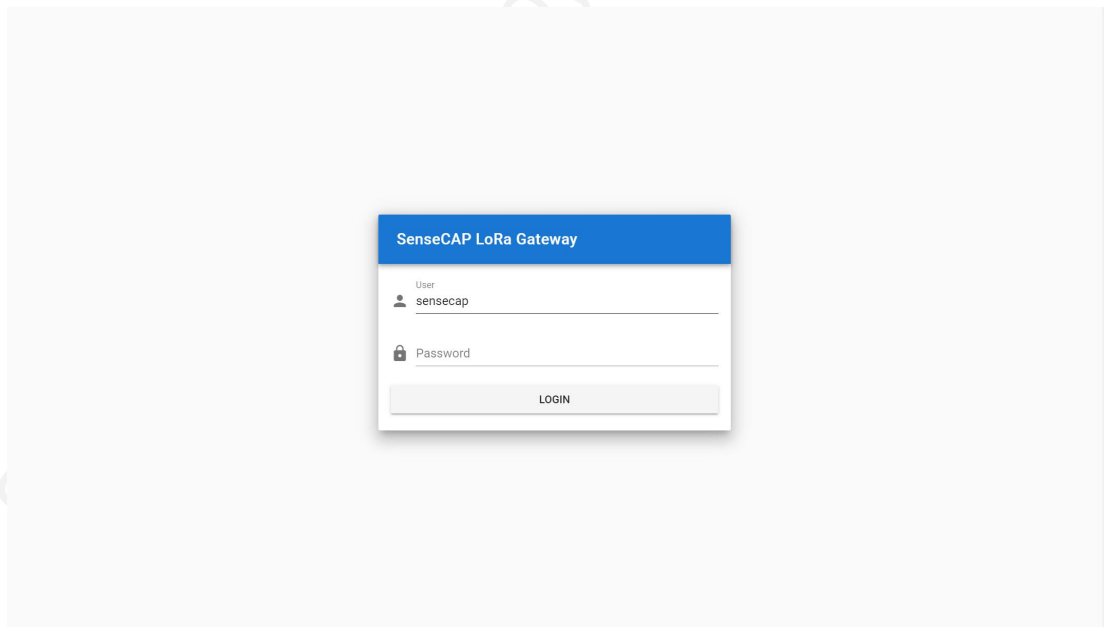
Prepare a router, and the network connection is shown in the figure:



(6) Check the IP of "sensecap" in the background of the router.

(7) Enter IP in the browser: IP:8000

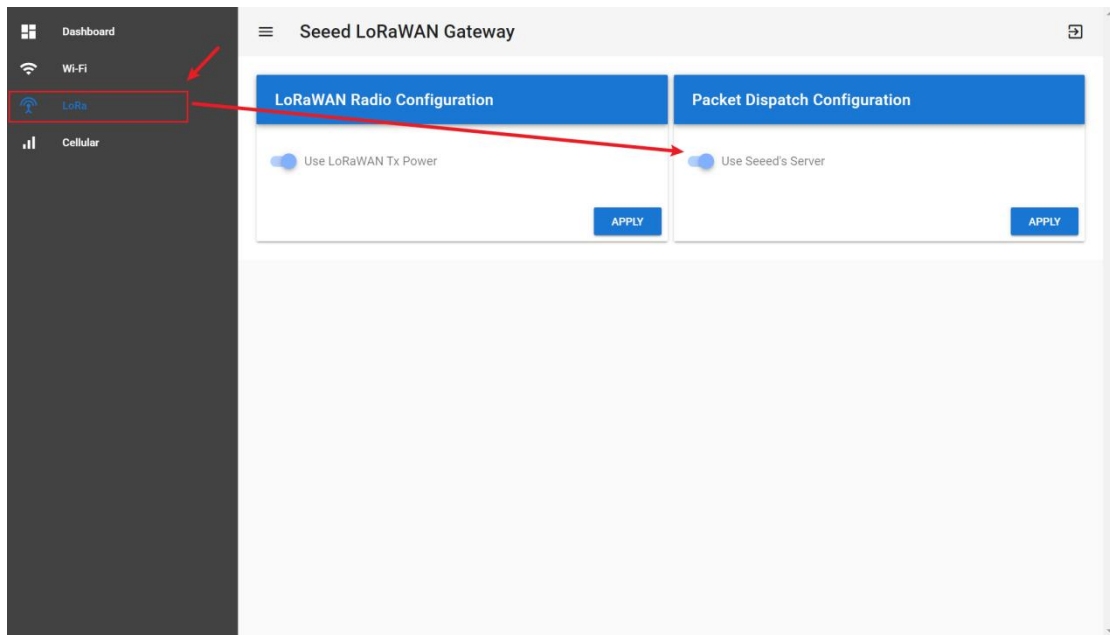
If the IP is 192.168.1.1, enter 192.168.1.1:8000



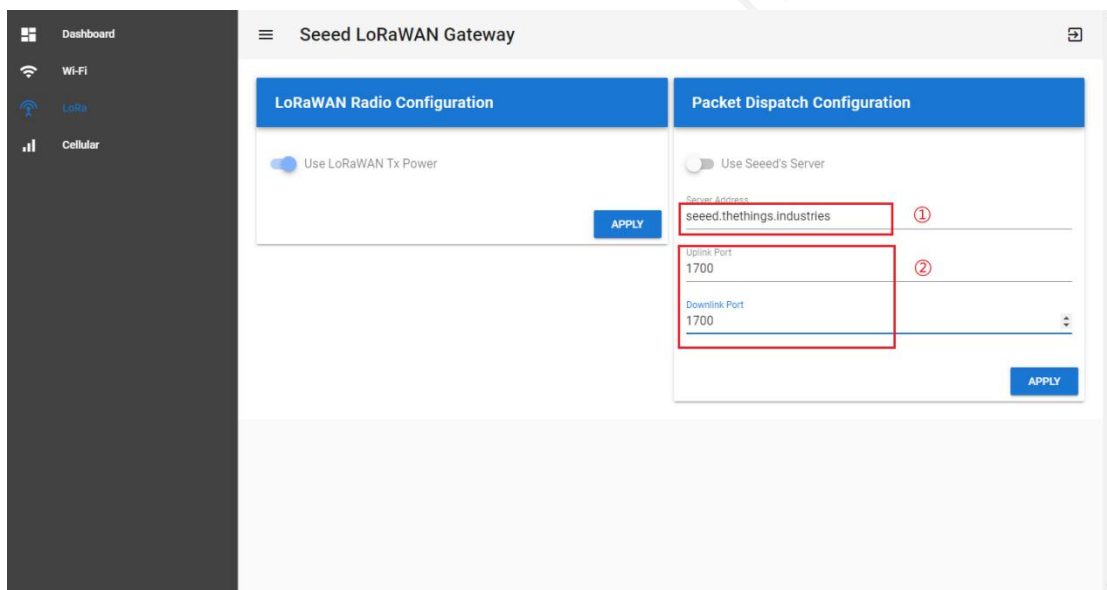
(8) User: sensecap

Password: sensecap!!!

(9) LoRa→Use Seeed's Server→Off Button



(10)








- ① Server Address: Please input your Server Address.  
Refer to the website:

**Version info**

# v3.13.2

**Component status**

- 
• Application Server  
eu1.cloud.thethings.network
- 
• Identity Server  
eu1.cloud.thethings.network
- 
• Network Server  
eu1.cloud.thethings.network
- 
• Gateway Server  
eu1.cloud.thethings.network
- 
• Join Server  
eu1.cloud.thethings.network

Uplink / Downlink Port (default): **1700**

(11) APPLY.

Seeed Technology Co., Ltd. Authorised



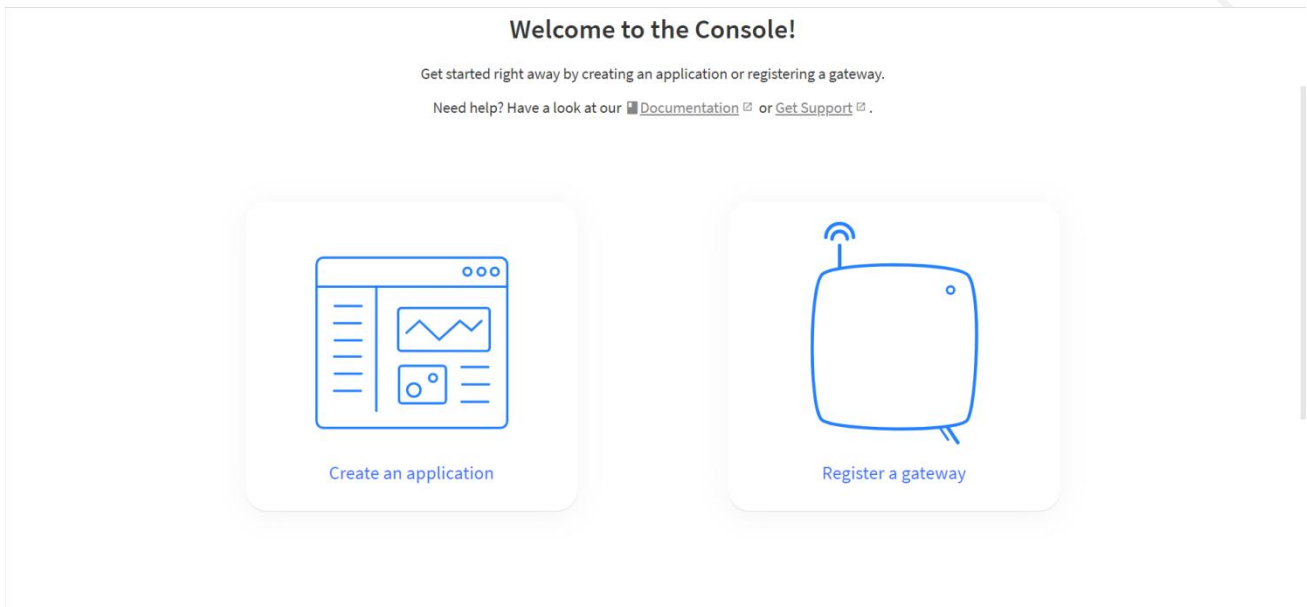
### 3.3 Gateway Registration on TTN

TTN website: <https://www.thethingsnetwork.org>

TTN console: <https://console.cloud.thethings.network/>

Tip: v2 will be discontinued and v3 is recommended.

(1) Follow the instruction to create your account, and access “Console”.



(2) Register Gateway

Seed Technology

Gateway ID ⓘ \*

Gateway EUI ⓘ

①

Gateway name ⓘ

Gateway description ⓘ

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

Gateway Server address

The address of the Gateway Server to connect to

Require authenticated connection ⓘ

 Enabled

Controls whether this gateway may only connect if it uses an authenticated Basic Station or MQTT connection

Gateway status ⓘ

 Public

The status of this gateway may be visible to other users

Gateway location ⓘ

 Public

- ① Gateway EUI: View the labels on the gateway. Select 'I'm using the legacy packet forwarder'.
- ② Frequency Plan: View the labels on the gateway.

EU868	Europe 863-870 MHz (SF9 for RX2 -recommended)
US915	United States 902-928 MHz, FSB 2 (used by TTN)
AU915	Australia 915-928 MHz, FSB 2 (used by TTN)
AS923-1	Asia 920-923 MHz
AS923-2	Asia 923-925 MHz

**LoRaWAN options**
**Frequency plan**

Europe 863-870 MHz (SF9 for RX2 - recommended)

②

**Schedule downlink late**
 Enabled

Enable server-side buffer of downlink messages

**Enforce duty cycle**
 Enabled

Recommended for all gateways in order to respect spectrum regulations

**Schedule any time delay**

530

milliseconds

Configure gateway delay (minimum: 130ms, default: 530ms)

③ Other use default.

④ Create Gateway.

Gateway Status displays connected, indicating successful registration.


**SenseCAP Gateway**  
 ID: demo-gw

Last seen 18 seconds ago   ↑ 0   ↓ 0   👤 1 Collaborator   🔑 0 API keys

Created 2 minutes ago

**General information**

Gateway ID: demo-gw

Gateway EUI: 2C F7 F1 10 22 50 00 19

Gateway description: SenseCAP Gateway Demo

Created at: Jul 2, 2021 18:42:56

Last updated at: Jul 2, 2021 18:42:56

Gateway Server address: eu1.cloud.thethings.network

**LoRaWAN information**

Frequency plan: EU\_863\_870\_TTN

 Global configuration: [Download global\\_conf.json](#)
**Live data**
[See all activity](#)

```

18:44:50 Receive gateway status Metrics: { ackr: 0, rxfw: 0, rxin: 0,
18:44:41 Connect gateway
18:42:56 Create gateway
    
```

**Location**
[Change location settings](#)


## 4 Add Gateway to ChirpStack LoRaWAN Network Server Stack

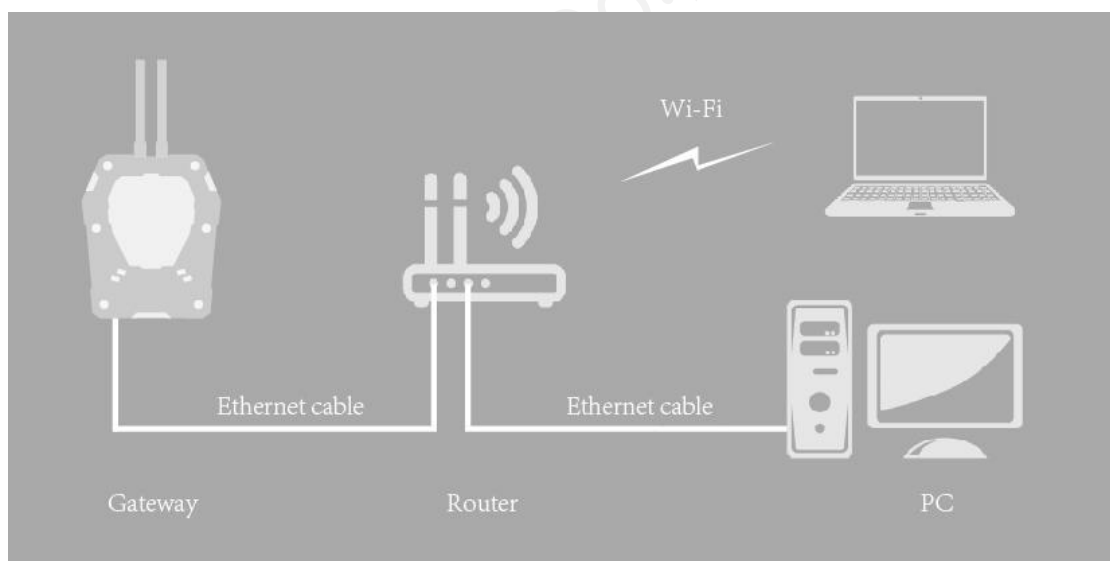
### Network Server Stack

ChirpStack provides open-source components for LoRaWAN networks. Together they form a ready-to-use solution including an user-friendly web-interface for device management and APIs for integration.

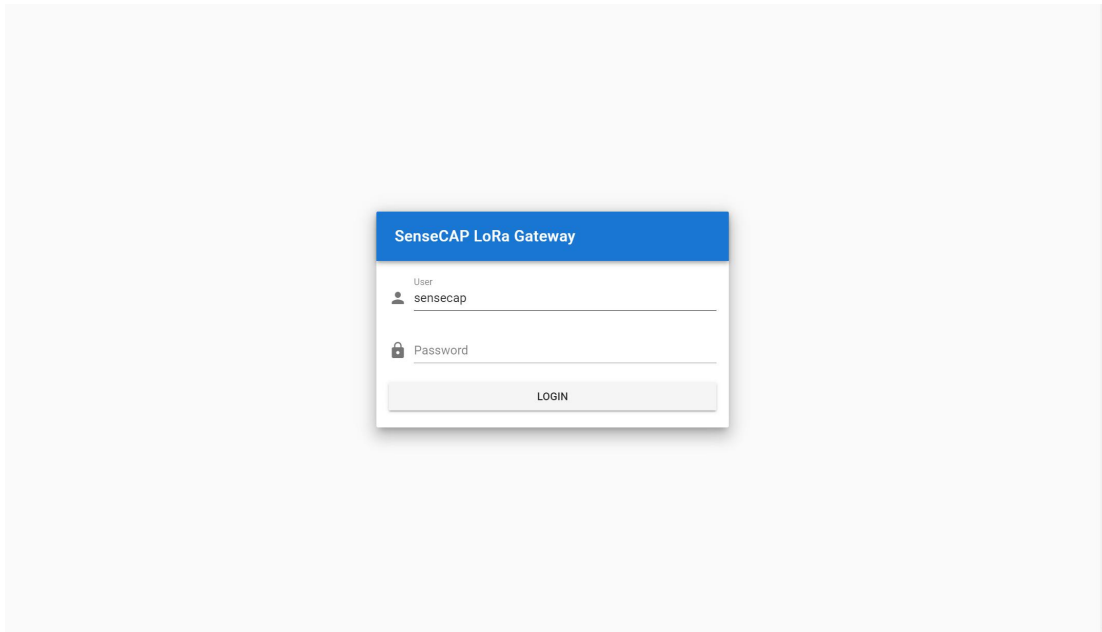
SenseCAP LoRaWAN Gateway has already integrated with ChirpStack LoRaWAN Network Server stack (hereinafter called the "ChirpStack LoRa Server"). The following LoRa Server components are accessible and configurable in Gateway: ChirpStack Gateway Bridge, ChirpStack Network Server and ChirpStack Application Server.

#### 4.1 Turn on ChirpStack LoRa Server Mode

Prepare a router, and the network connection is shown in the figure:



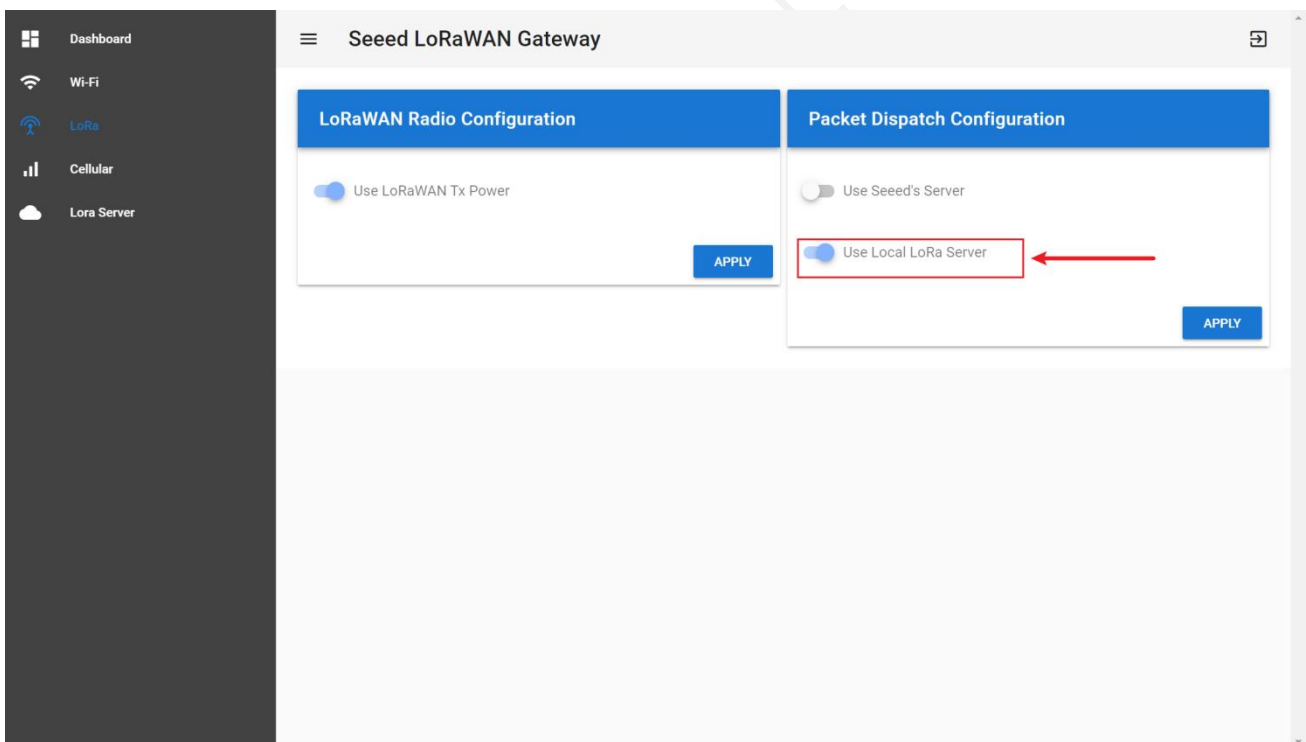
- (1) Check the IP of "sensecap" in the background of the router.
- (2) Enter IP in the browser: IP:8000  
If the IP is 192.168.1.1, enter 192.168.1.1:8000



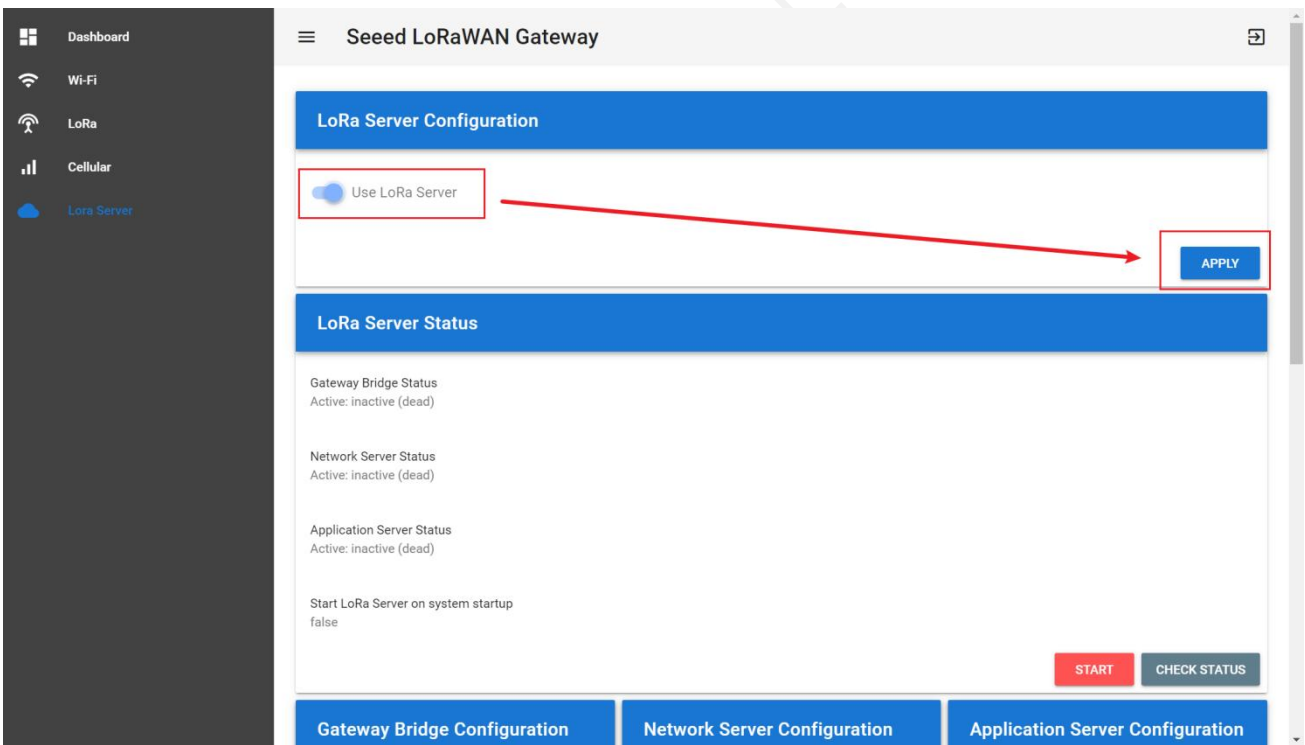
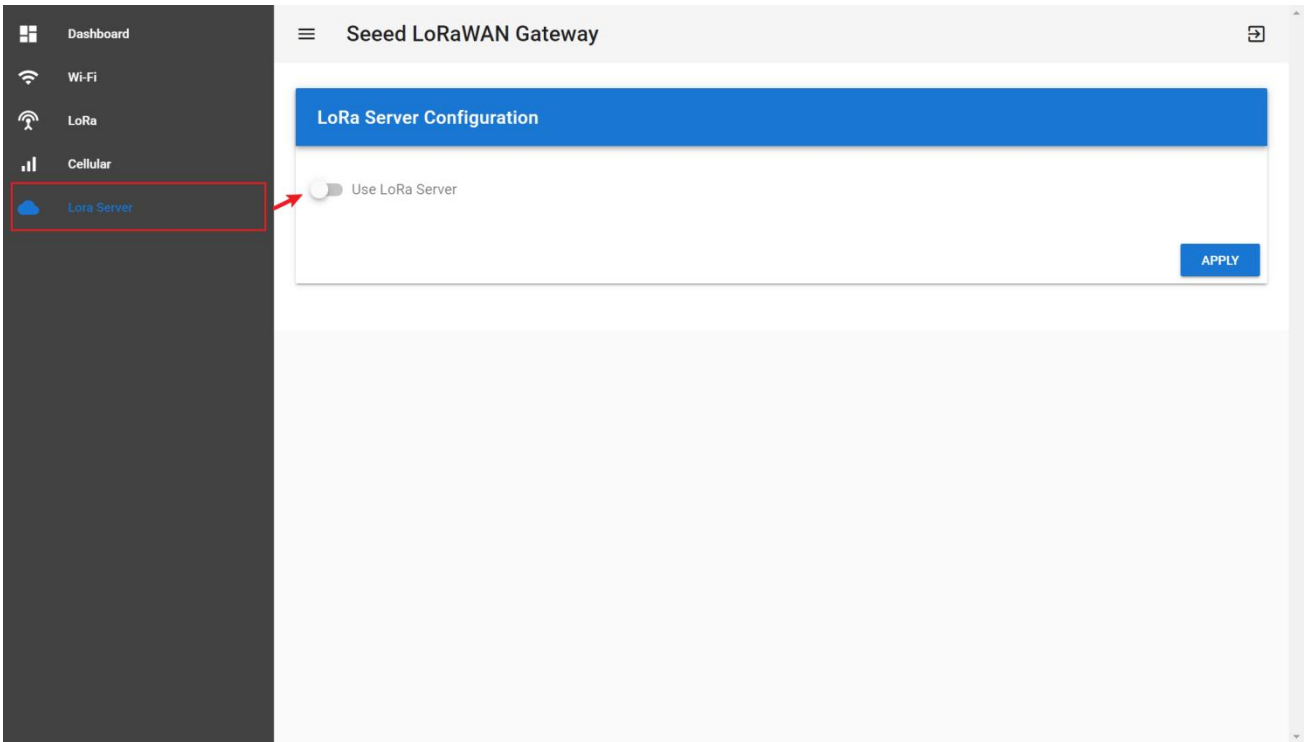
(3) User: sensecap

Password: sensecap!!!

(4) Turn off the “Use Seed’s Server”, and turn on “Use Local LoRa Server”.

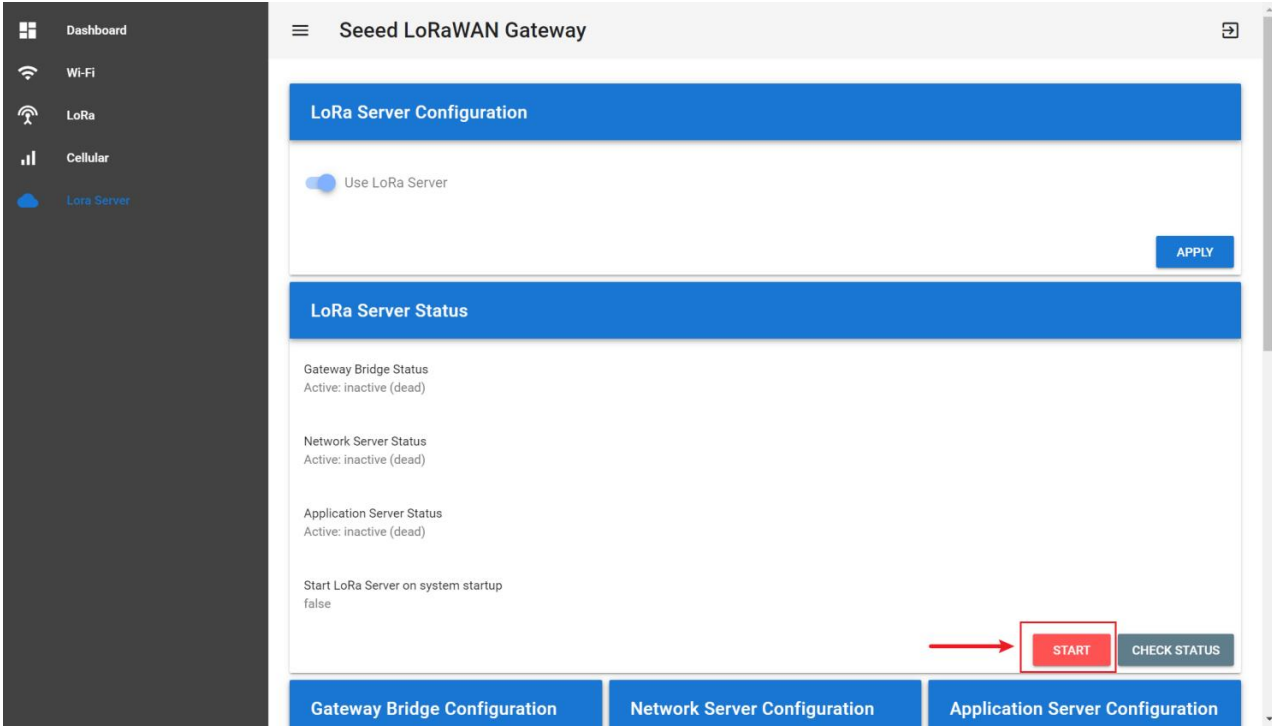


(5) Turn on the “Use LoRa Server” button, and apply. (“LoRa Server” is the name of ChirpStack LoRa Server)



## 4.2 ChirpStack LoRa Server Configuration

First, click the “Start” button to start the service.



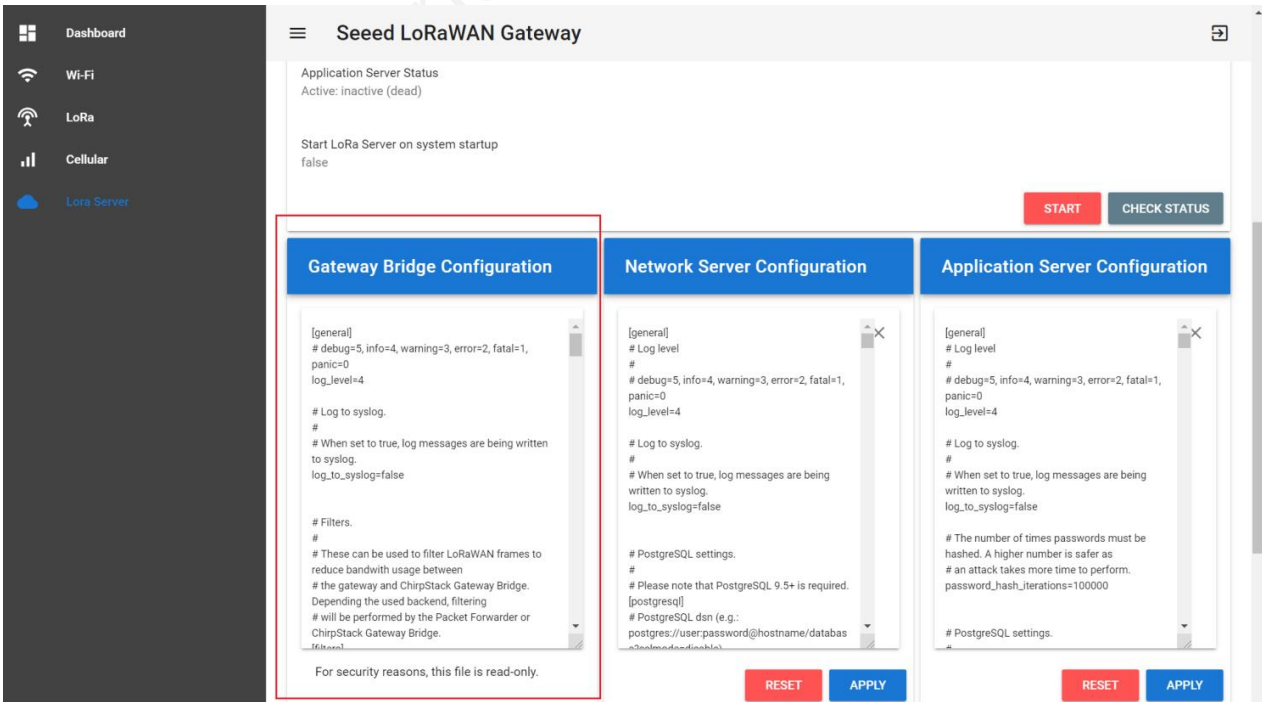
The screenshot shows the 'Seede LoRaWAN Gateway' configuration interface. The 'LoRa Server Configuration' section has the 'Use LoRa Server' toggle set to 'on'. Below this, the 'LoRa Server Status' section shows three components: Gateway Bridge Status (Active: inactive (dead)), Network Server Status (Active: inactive (dead)), and Application Server Status (Active: inactive (dead)). At the bottom right, a red arrow points to the 'START' button, which is next to a 'CHECK STATUS' button. Below the status section are three tabs: 'Gateway Bridge Configuration', 'Network Server Configuration', and 'Application Server Configuration'.

(1) ChirpStack Gateway Bridge:

Refer to: <https://www.chirpstack.io/gateway-bridge/>

It converts LoRa® Packet Forwarder protocols into a ChirpStack Network Server common data-format (JSON and Protobuf).

For security reasons, this file is read-only.



This screenshot shows the configuration tabs from the previous image. The 'Gateway Bridge Configuration' tab is selected and highlighted with a red box. It contains configuration parameters for the gateway bridge, including log levels, syslog settings, and filters. A note at the bottom of this section states: 'For security reasons, this file is read-only.' The 'Network Server Configuration' and 'Application Server Configuration' tabs are also visible, showing their respective configuration parameters and 'RESET' and 'APPLY' buttons.

### (2) ChirpStack Network Server:

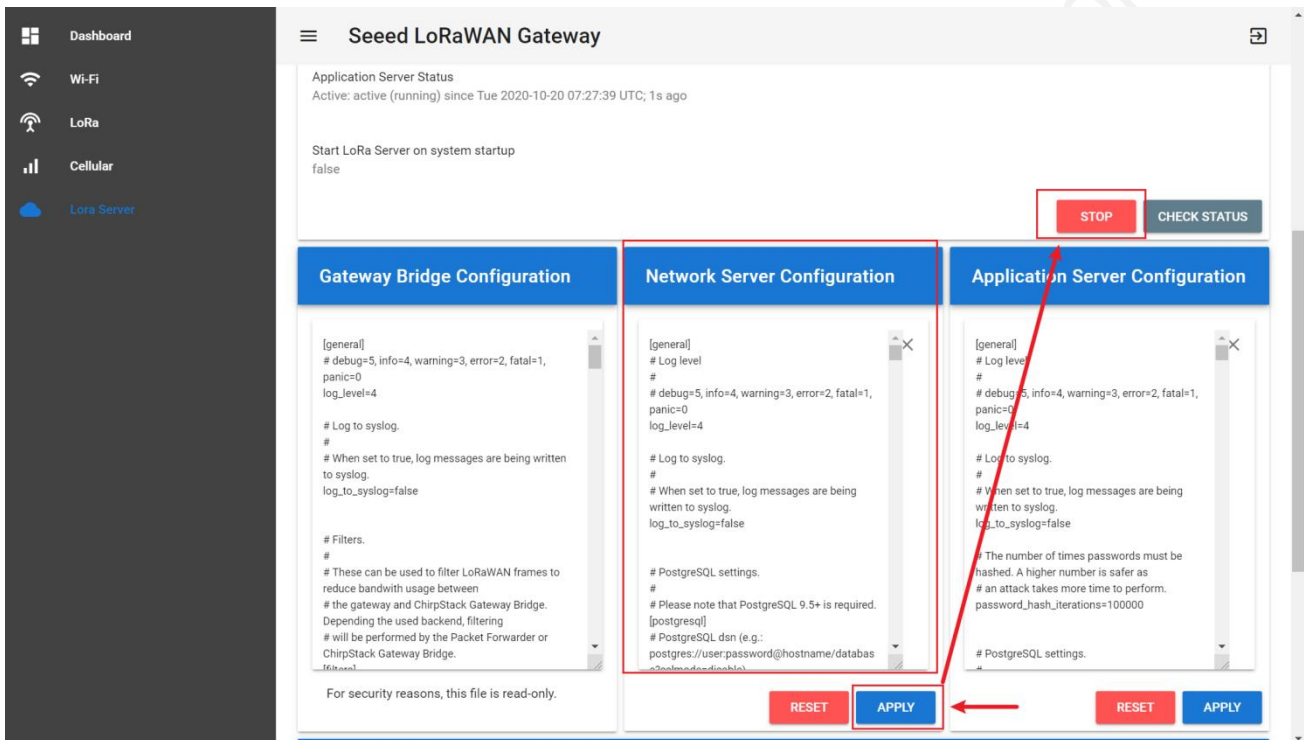
Refer to: <https://www.chirpstack.io/network-server/>

The responsibility of the Network Server component is the de-duplication of received LoRaWAN frames by the LoRa® gateways and for the collected frames handle the: Authentication; LoRaWAN mac-layer (and mac-commands); Communication with the ChirpStack Application Server; Scheduling of downlink frames.

In general, the default configuration is used. Please refer to the official tutorial before making any modifications.

Click "APPLY" to save the configuration after making changes.

Then, click "STOP" in "Application Server Status" and finally click "START" to make the configuration take effect.



The screenshot shows the 'Seede LoRaWAN Gateway' web interface. On the left is a navigation menu with 'Dashboard', 'Wi-Fi', 'LoRa', 'Cellular', and 'Lora Server'. The main content area is titled 'Seede LoRaWAN Gateway' and contains several sections:

- Application Server Status:** Shows 'Active: active (running) since Tue 2020-10-20 07:27:39 UTC, 1s ago'. Below it is a toggle for 'Start LoRa Server on system startup' set to 'false'. At the top right of this section are 'STOP' and 'CHECK STATUS' buttons.
- Gateway Bridge Configuration:** Contains configuration for the gateway bridge, including log levels and filters.
- Network Server Configuration:** This panel is highlighted with a red box. It contains configuration for the network server, including log levels and PostgreSQL settings. At the bottom of this panel are 'RESET' and 'APPLY' buttons. A red arrow points from the 'STOP' button in the Application Server Status section to the 'APPLY' button in this panel.
- Application Server Configuration:** Contains configuration for the application server, including log levels and password hashing settings. At the bottom of this panel are 'RESET' and 'APPLY' buttons.

### (3) ChirpStack Application Server:

Refer to: <https://www.chirpstack.io/application-server/>

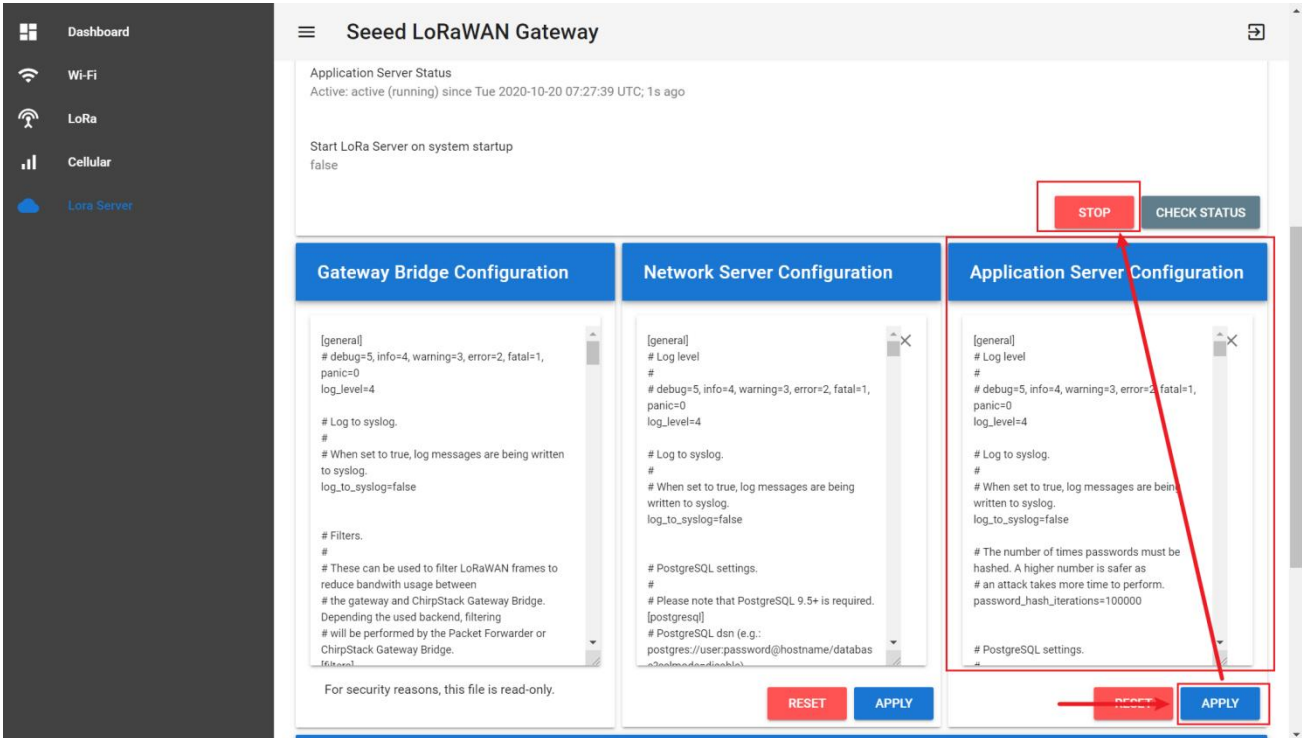
It is responsible for the device "inventory" part of a LoRaWAN infrastructure, handling of join-request and the handling and encryption of application payloads.

In general, the default configuration is used. Please refer to the official tutorial before making any modifications.

Click "APPLY" to save the configuration after making changes.

Then, click "STOP" in "Application Server Status" and finally click "START" to make the configuration take effect.





Dashboard

Wi-Fi

LoRa

Cellular

Lora Server

### Seeed LoRaWAN Gateway

Application Server Status  
Active: active (running) since Tue 2020-10-20 07:27:39 UTC; 1s ago

Start LoRa Server on system startup  
false

**STOP** **CHECK STATUS**

#### Gateway Bridge Configuration

```
[general]
# debug=5, info=4, warning=3, error=2, fatal=1,
panic=0
log_level=4

# Log to syslog.
#
# When set to true, log messages are being written
to syslog.
log_to_syslog=false

# Filters.
#
# These can be used to filter LoRaWAN frames to
reduce bandwidth usage between
# the gateway and ChirpStack Gateway Bridge.
Depending the used backend, filtering
# will be performed by the Packet Forwarder or
ChirpStack Gateway Bridge.
[filters]
```

For security reasons, this file is read-only.

**RESET** **APPLY**

#### Network Server Configuration

```
[general]
# Log level
#
# debug=5, info=4, warning=3, error=2, fatal=1,
panic=0
log_level=4

# Log to syslog.
#
# When set to true, log messages are being
written to syslog.
log_to_syslog=false

# PostgreSQL settings.
#
# Please note that PostgreSQL 9.5+ is required.
[postgresql]
# PostgreSQL dsn (e.g.:
postgres://user:password@hostname/database)
```

**RESET** **APPLY**

#### Application Server Configuration

```
[general]
# Log level
#
# debug=5, info=4, warning=3, error=2, fatal=1,
panic=0
log_level=4

# Log to syslog.
#
# When set to true, log messages are being
written to syslog.
log_to_syslog=false

# The number of times passwords must be
hashed. A higher number is safer as
# an attack takes more time to perform.
password_hash_iterations=100000

# PostgreSQL settings.
```

**RESET** **APPLY**

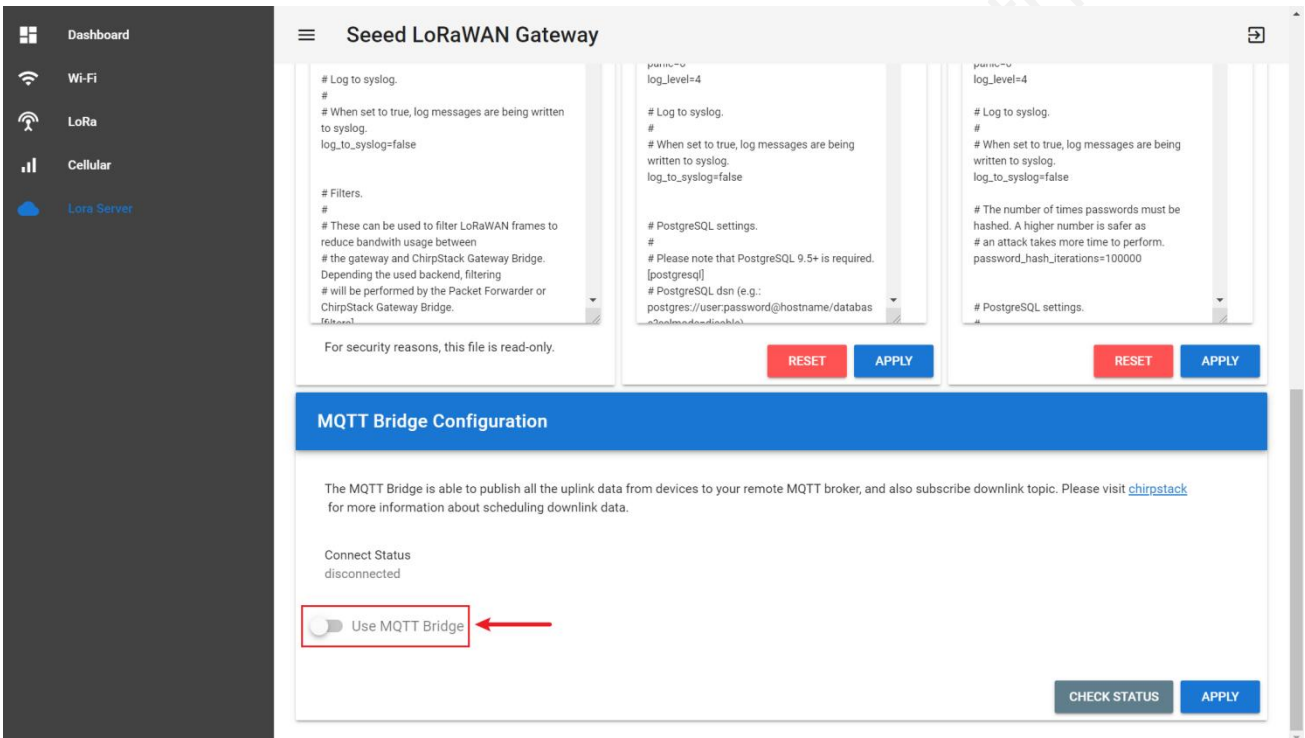
(4) If you have the wrong configuration, click "RESET" to restore the default configuration.

## 4.3 MQTT Bridge Configuration

The MQTT Bridge is able to publish all the uplink data from devices to your remote MQTT broker, and also subscribe downlink topic. Please visit ChirpStack(<https://www.chirpstack.io/application-server/integrations/mqtt/>) for more information about scheduling downlink data.

### 4.3.1 Gateway Configuration

(1) Click “Use MQTT Bridge”.



The screenshot shows the configuration page for a Seede LoRaWAN Gateway. The left sidebar contains navigation options: Dashboard, Wi-Fi, LoRa, Cellular, and Lora Server. The main content area is titled 'Seede LoRaWAN Gateway' and contains three configuration panels for logging, filters, and PostgreSQL settings. Below these panels is the 'MQTT Bridge Configuration' section, which includes a 'Connect Status' indicator (disconnected) and a 'Use MQTT Bridge' toggle switch. A red arrow points to the 'Use MQTT Bridge' toggle switch.

(2) After filling in each parameter, click "APPLY".

①

MQTT Server address: `mqtt://xxx.xx` or `mqtt://xxx.xx`

If xxx.xx (IP) is 111.230.200.102, the address is `mqtt://111.230.200.102` or `mqtt://111.230.200.102`

If xxx.xx (url) is mybroker.com, the address is `mqtt:// mybroker.com` or `mqtt:// mybroker.com`

②

MQTT Server 's Port.

In general, `mqtt` corresponds to port 1883 and `mqtt`s to port 8883.

③

Keepalive:

60 is default value. When the MQTT connection between the Gateway and the Server is disconnected over 60 seconds, it determines that the client is offline.

0 means turn off the keepalive function.

④

CleanSession:

true: the gateway reconnects to the network after a power outage or disconnection, and cannot receive data from MQTTpub to the gateway for that period.

false: the gateway reconnects to the network after a power outage or disconnection, and can receive data from MQTTpub to the gateway for that period.

⑤

Username: Null if none, depending on the server configuration.

⑥

Password: Null if none, depending on the server configuration.

⑦

Client ID: Custom the name, and each Client ID is unique to the same MQTT server.

⑧

Publish QoS: 0, 1 or 2. (refer to the MQTT rules)

⑨

Subscribe QoS: 0, 1 or 2. (refer to the MQTT rules)

- Dashboard
- Wi-Fi
- LoRa
- Cellular
- LoRa Server

### Seed LoRaWAN Gateway

Use MQTT Bridge

Remote MQTT Broker URL, support 'mqtt' and 'mqtts', (e.g. mqtt://mybroker.com) ①

Port ②

Keepalive, default to 60, set 0 to disable ③

CleanSession, default to true, set false to receive QoS 1 and 2 messages while offline ④

Username ⑤

Password ⑥

Client ID ⑦

Publish QoS ⑧

Subscribe QoS ⑨

Verify server certificate

CHECK STATUS
APPLY

- Dashboard
- Wi-Fi
- LoRa
- Cellular
- LoRa Server

### Seed LoRaWAN Gateway

Use MQTT Bridge

Remote MQTT Broker URL, support 'mqtt' and 'mqtts', (e.g. mqtt://mybroker.com)  
 mqtt://111.230.200.102

Port 1883

Keepalive, default to 60, set 0 to disable 60

CleanSession, default to true, set false to receive QoS 1 and 2 messages while offline true

Username

Password

Client ID Test

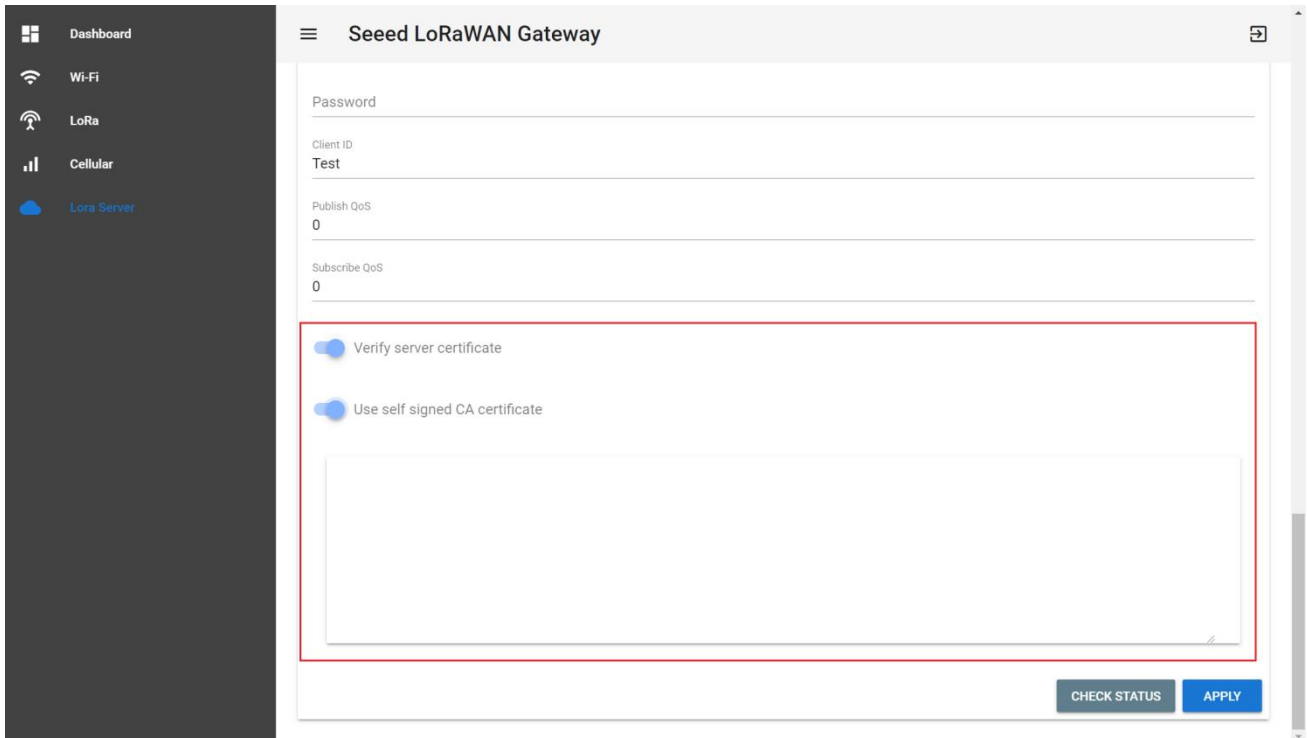
Publish QoS 0

Subscribe QoS 0

Verify server certificate

CHECK STATUS
APPLY

- (3) It is off by default and can generally be ignored: Verify server certificate.  
 If true, the server certificate is verified against the list of supplied CAs.  
 If false, the server certificate is verified against your self-signed certificate.



Seed LoRaWAN Gateway

Password

Client ID  
Test

Publish QoS  
0

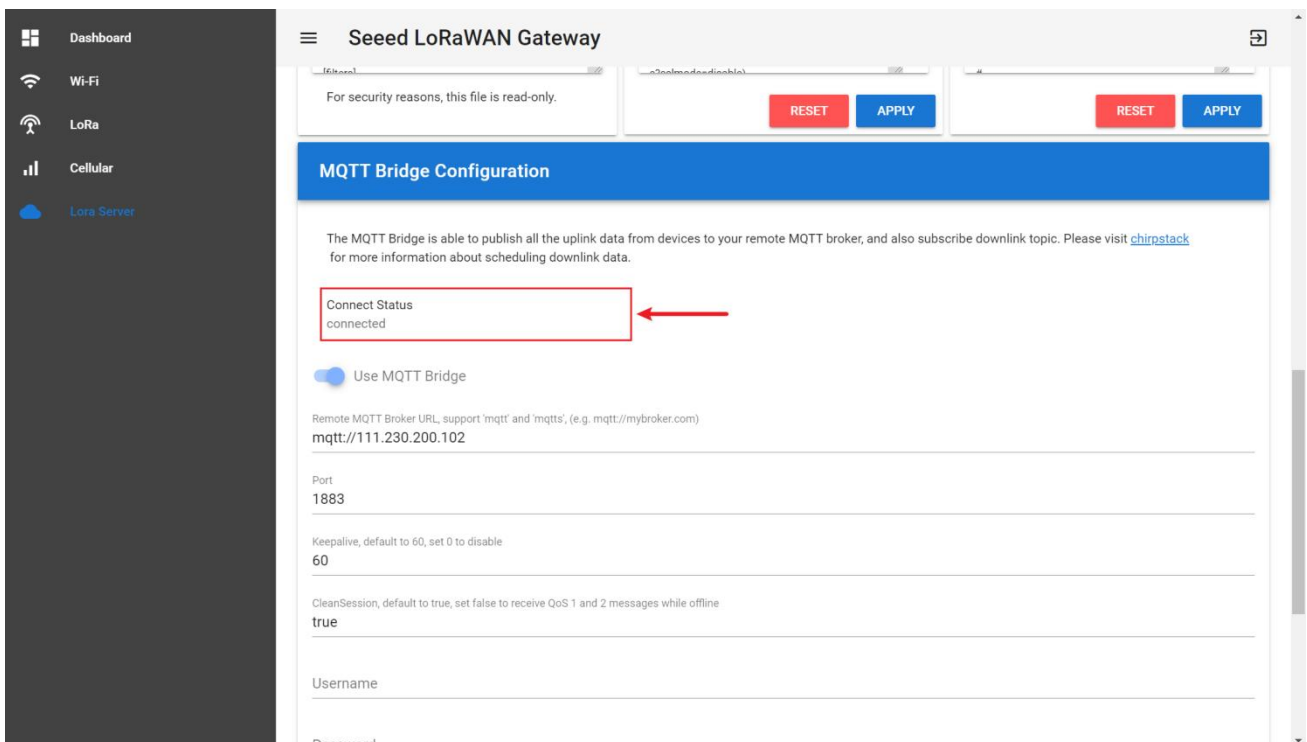
Subscribe QoS  
0

Verify server certificate

Use self signed CA certificate

CHECK STATUS APPLY

(4) Check Status: Disconnected / Reconnecting / Connected.



Seed LoRaWAN Gateway

MQTT Bridge Configuration

The MQTT Bridge is able to publish all the uplink data from devices to your remote MQTT broker, and also subscribe downlink topic. Please visit [chirpstack](#) for more information about scheduling downlink data.

Connect Status  
connected

Use MQTT Bridge

Remote MQTT Broker URL, support 'mqtt' and 'mqtts', (e.g. mqtt://mybroker.com)  
mqtt://111.230.200.102

Port  
1883

Keepalive, default to 60, set 0 to disable  
60

CleanSession, default to true, set false to receive QoS 1 and 2 messages while offline  
true

Username

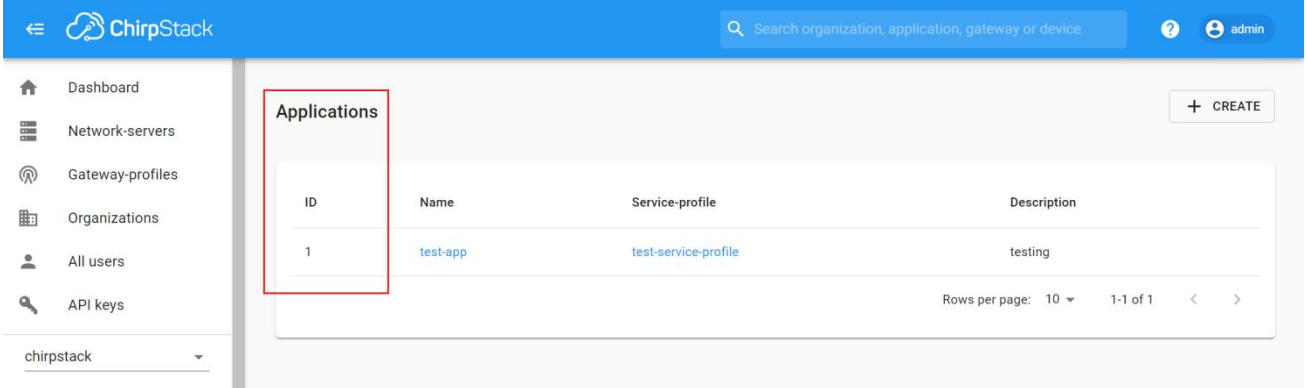
Password

RESET APPLY

## 4.3.2 MQTT Client Configuration

For details, please refer to: <https://www.chirpstack.io/application-server/integrations/events/#ack>

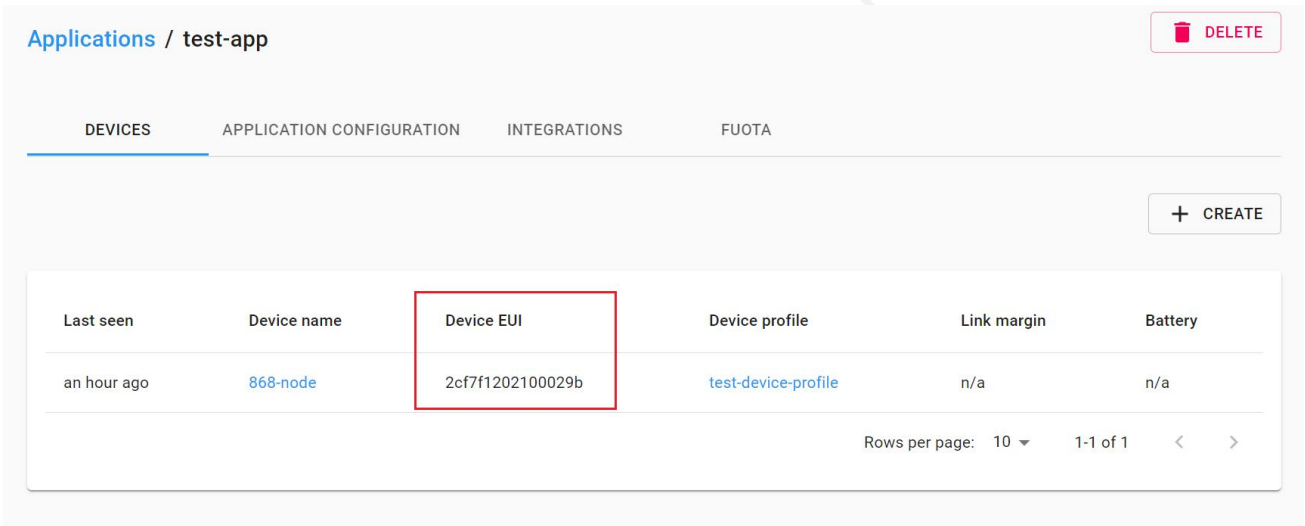
ApplicationID: the Application ID.



The screenshot shows the ChirpStack web interface. The top navigation bar includes a search bar and a user profile for 'admin'. A sidebar on the left lists various system components. The main content area displays a table of Applications. A red box highlights the table header and the first row.

ID	Name	Service-profile	Description
1	test-app	test-service-profile	testing

DevEUI: Device EUI.



The screenshot shows the 'Applications / test-app' page. It features a breadcrumb trail, a 'DELETE' button, and a tabbed interface with 'DEVICES' selected. Below the tabs is a table of devices. A red box highlights the 'Device EUI' column header and the first row.

Last seen	Device name	Device EUI	Device profile	Link margin	Battery
an hour ago	868-node	2cf7f1202100029b	test-device-profile	n/a	n/a

(1) Device data subscription

```
application/[ApplicationID]/device/[DevEUI]/event/up
```

e.g. application/1/device/ 2cf7f1202100029b/event/up

(2) Join packet subscription

```
application/[ApplicationID]/device/[DevEUI]/event/join
```

e.g. application/1/device/ 2cf7f1202100029b/event/join

(3) Status packet subscription

```
application/[ApplicationID]/device/[DevEUI]/event/status
```

e.g. application/1/device/ 2cf7f1202100029b/event/ status

### 4.3.3 Scheduling a Downlink

The default topic for scheduling downlink payloads is:

```
application/[ApplicationID]/device/[DevEUI]/command/down
```

The ApplicationID and DevEUI of the device will be taken from the topic.

Example payload:

```
{
  "confirmed": true,      // whether the payload must be sent as confirmed data down or not
  "fPort": 10,           // FPort to use (must be > 0)
  "data": "...",        // base64 encoded data (plaintext, will be encrypted by ChirpStack
Network Server)
  "object": {           // decoded object (when application coded has been configured)
    "temperatureSensor": {"1": 25}, // when providing the 'object', you can omit 'data'
    "humiditySensor": {"1": 32}
  }
}
```

## 4.4 ChirpStack Application Server

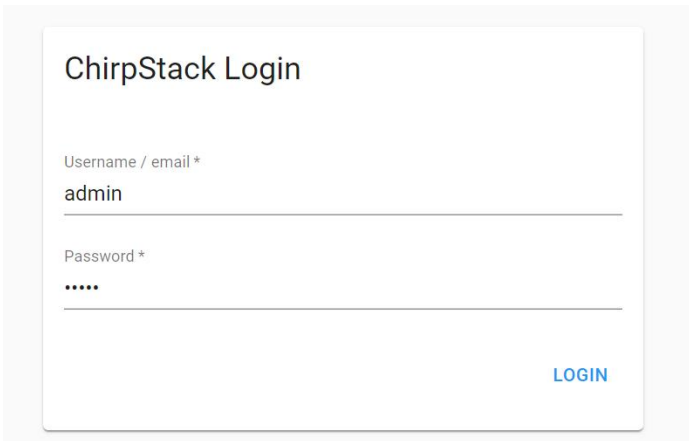
### 4.4.1 Log on to the background

According to the Gateway IP obtained in Section 4.1, log in the Web UI.

The login address: **IP:8080** (if IP is 192.168.8.100, enter 192.168.8.100:8080)

Username(default): **admin**

Password(default): **admin**



ChirpStack Login

Username / email \*

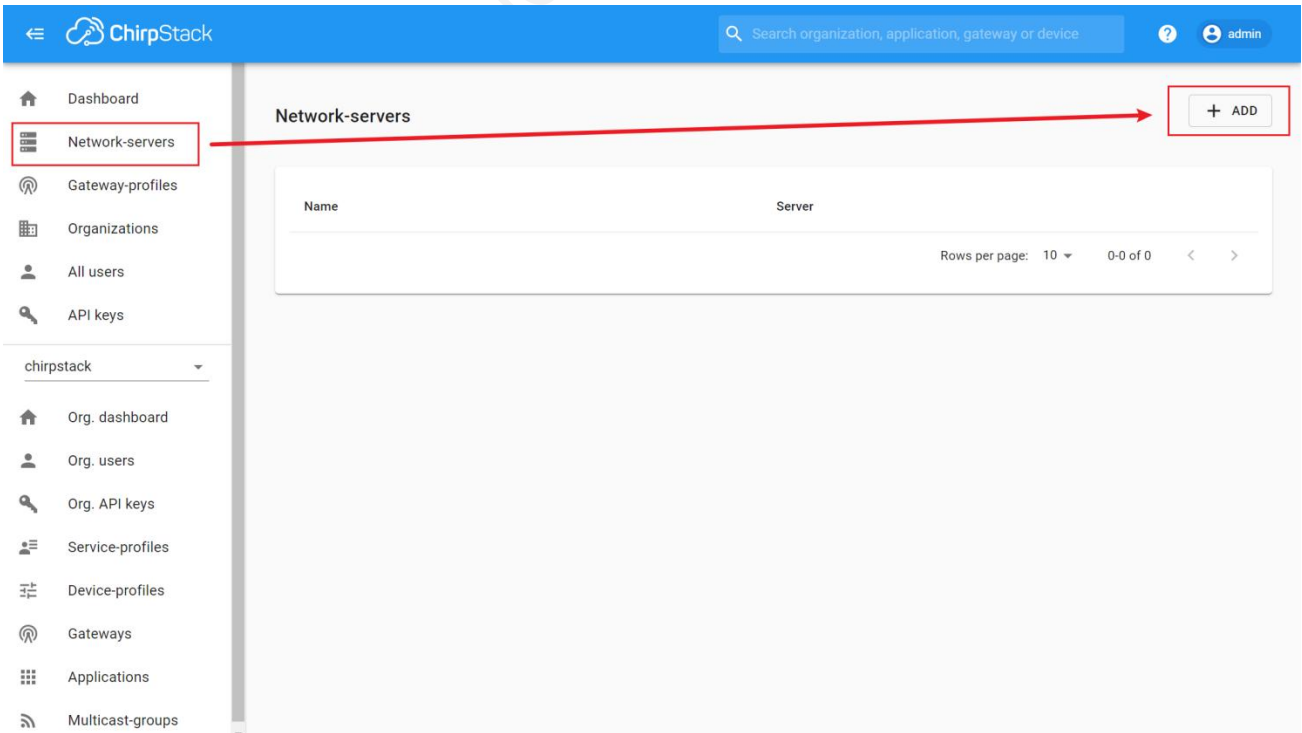
admin

Password \*

.....

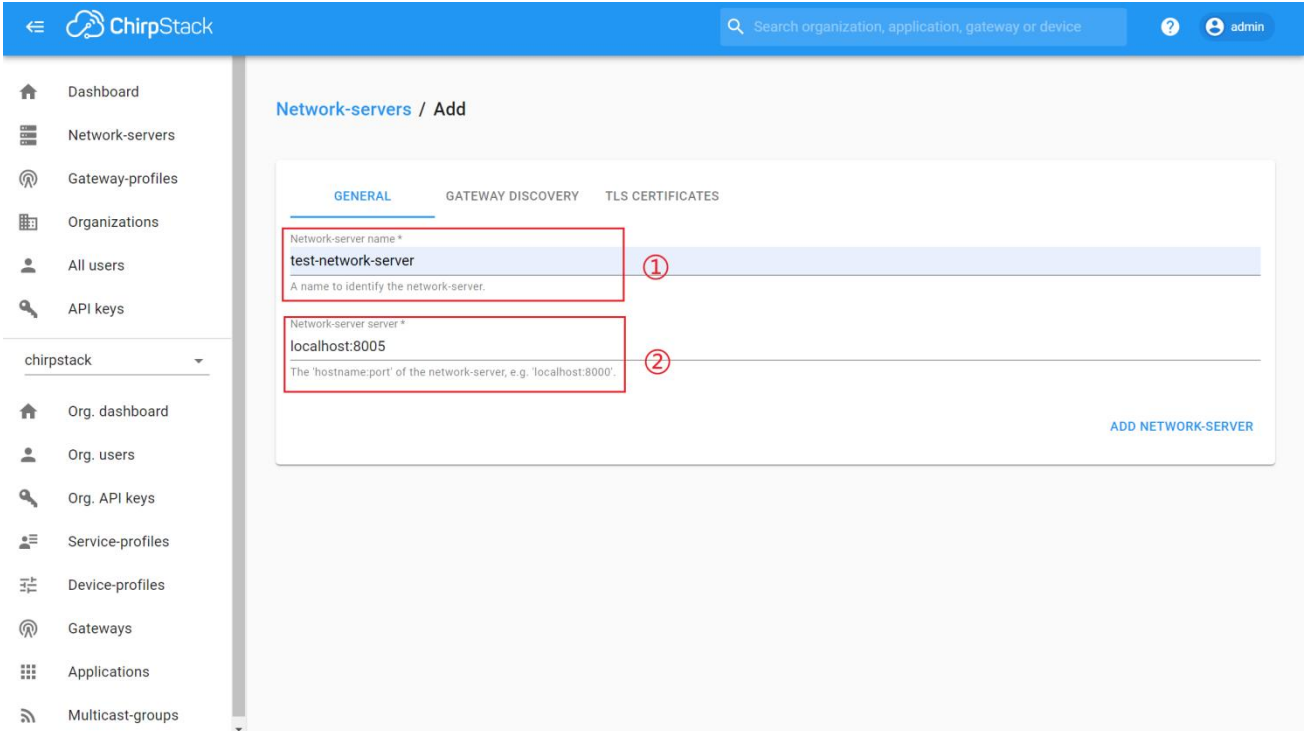
LOGIN

### 4.4.2 Add the Network-servers



The screenshot shows the ChirpStack Web UI. The top navigation bar is blue with the ChirpStack logo and a search bar. The left sidebar contains a menu with items like Dashboard, Network-servers, Gateway-profiles, Organizations, All users, and API keys. The 'Network-servers' item is highlighted with a red box. A red arrow points from this box to a '+ ADD' button in the top right corner of the main content area. The main content area displays a table with columns 'Name' and 'Server', and a 'Rows per page: 10' dropdown. The table is currently empty, showing '0-0 of 0' rows.





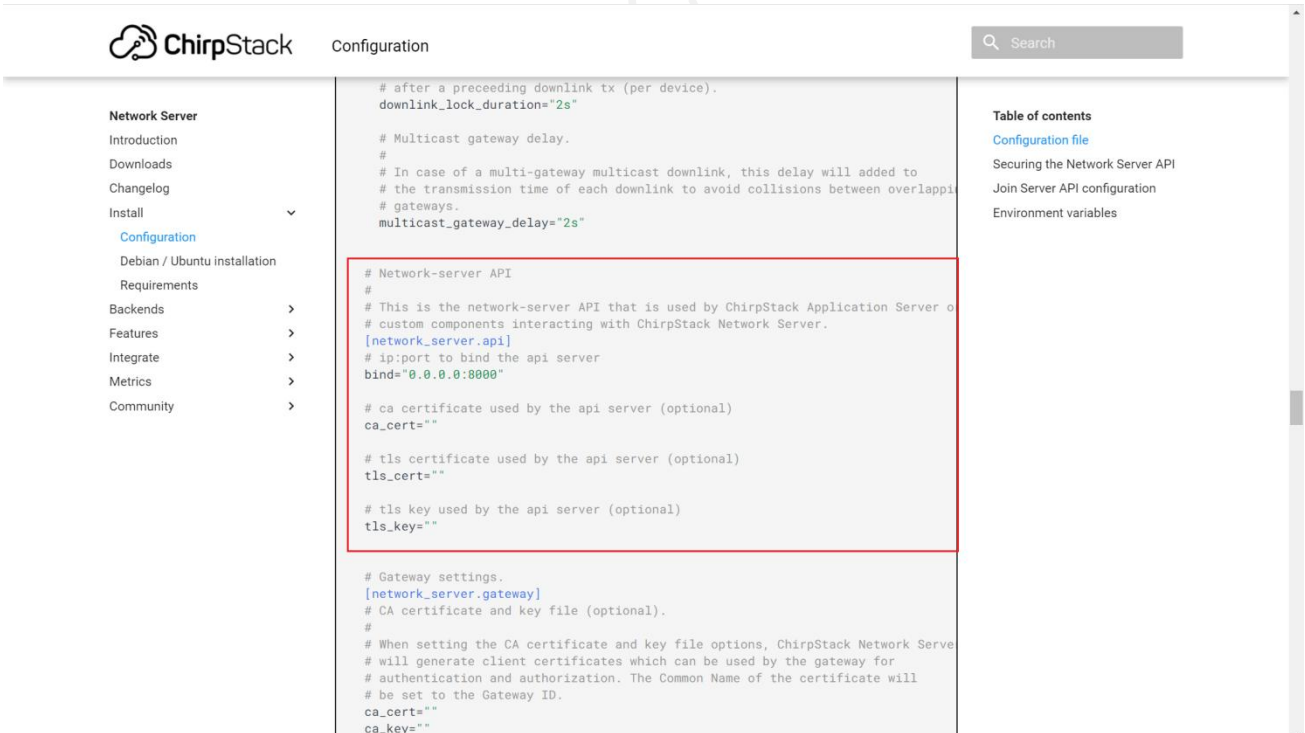
The screenshot shows the 'Add Network-server' form in ChirpStack. The form has three tabs: 'GENERAL', 'GATEWAY DISCOVERY', and 'TLS CERTIFICATES'. The 'GENERAL' tab is active. There are two input fields:

- Network-server name \***: Contains the text 'test-network-server'. A red box highlights this field with a circled '1' next to it.
- Network-server server \***: Contains the text 'localhost:8005'. A red box highlights this field with a circled '2' next to it.

At the bottom right of the form is a blue button labeled 'ADD NETWORK-SERVER'.

- ① Network-server name: custom name.
- ② Network-server server: the default value is **localhost:8005**

Refer to: <https://www.chirpstack.io/network-server/install/config/>. You can modify it in the “Network Server Configuration”.



The screenshot shows the 'Configuration' page in ChirpStack. The left sidebar contains a navigation menu with 'Network Server' expanded to show 'Configuration'. The main content area displays a configuration file with several sections. A red box highlights the 'Network-server API' section:

```
# Network-server API
#
# This is the network-server API that is used by ChirpStack Application Server or
# custom components interacting with ChirpStack Network Server.
[network_server.api]
# ip:port to bind the api server
bind="0.0.0.0:8000"

# ca certificate used by the api server (optional)
ca_cert=""

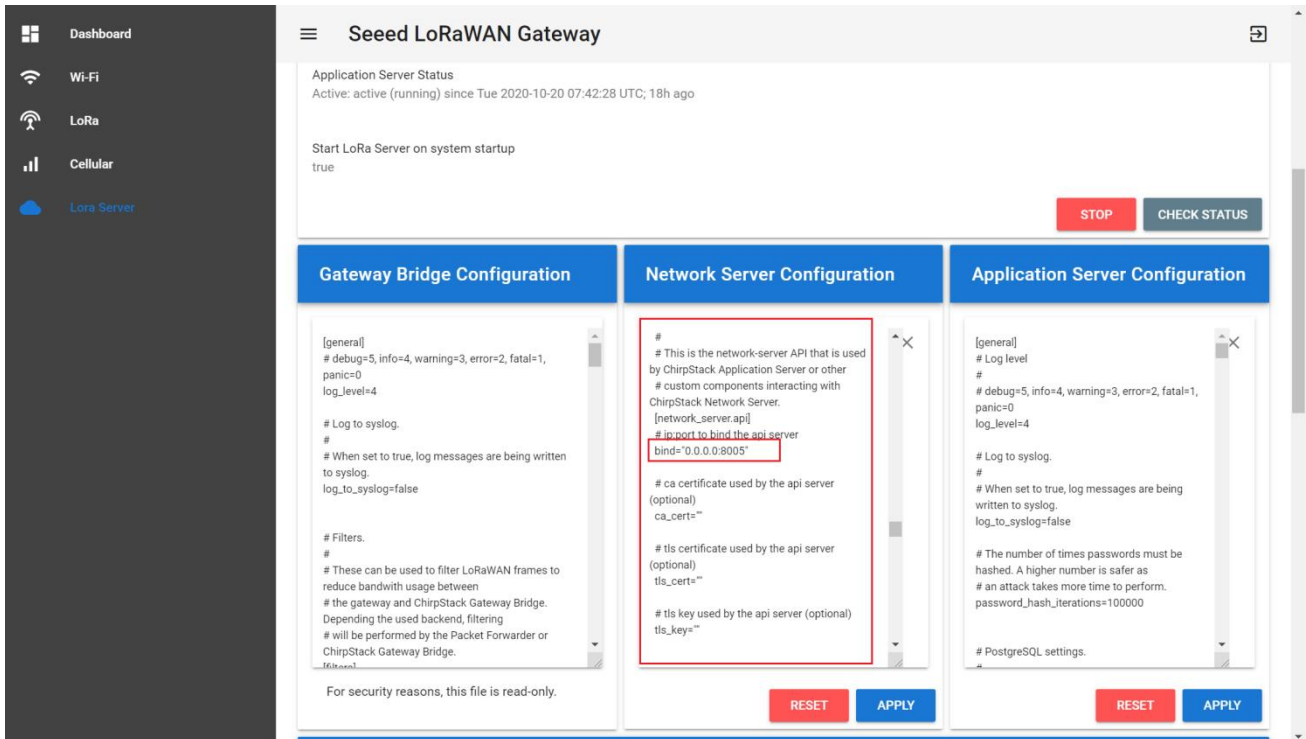
# tls certificate used by the api server (optional)
tls_cert=""

# tls key used by the api server (optional)
tls_key=""
```

Below the highlighted section, there is a 'Gateway settings' section with a red box around it:

```
# Gateway settings.
[network_server.gateway]
# CA certificate and key file (optional).
#
# When setting the CA certificate and key file options, ChirpStack Network Server
# will generate client certificates which can be used by the gateway for
# authentication and authorization. The Common Name of the certificate will
# be set to the Gateway ID.
ca_cert=""
ca_key=""
```

On the right side of the configuration page, there is a 'Table of contents' section with links to 'Configuration file', 'Securing the Network Server API', 'Join Server API configuration', and 'Environment variables'.



**Seede LoRaWAN Gateway**

Application Server Status  
Active: active (running) since Tue 2020-10-20 07:42:28 UTC; 18h ago

Start LoRa Server on system startup  
true

**STOP** **CHECK STATUS**

**Gateway Bridge Configuration**

```
[general]
# debug=5, info=4, warning=3, error=2, fatal=1,
panic=0
log_level=4

# Log to syslog.
#
# When set to true, log messages are being written
to syslog.
log_to_syslog=false

# Filters.
#
# These can be used to filter LoRaWAN frames to
reduce bandwidth usage between
# the gateway and ChirpStack Gateway Bridge.
Depending the used backend, filtering
# will be performed by the Packet Forwarder or
ChirpStack Gateway Bridge.
filters=
```

For security reasons, this file is read-only.

**Network Server Configuration**

```
#
# This is the network-server API that is used
by ChirpStack Application Server or other
# custom components interacting with
ChirpStack Network Server.
[network_server.api]
# bind=0.0.0.0:8005
# ca certificate used by the api server
(optional)
ca_cert=""
# tls certificate used by the api server
(optional)
tls_cert=""
# tls key used by the api server (optional)
tls_key=""
```

**RESET** **APPLY**

**Application Server Configuration**

```
[general]
# Log level
#
# debug=5, info=4, warning=3, error=2, fatal=1,
panic=0
log_level=4

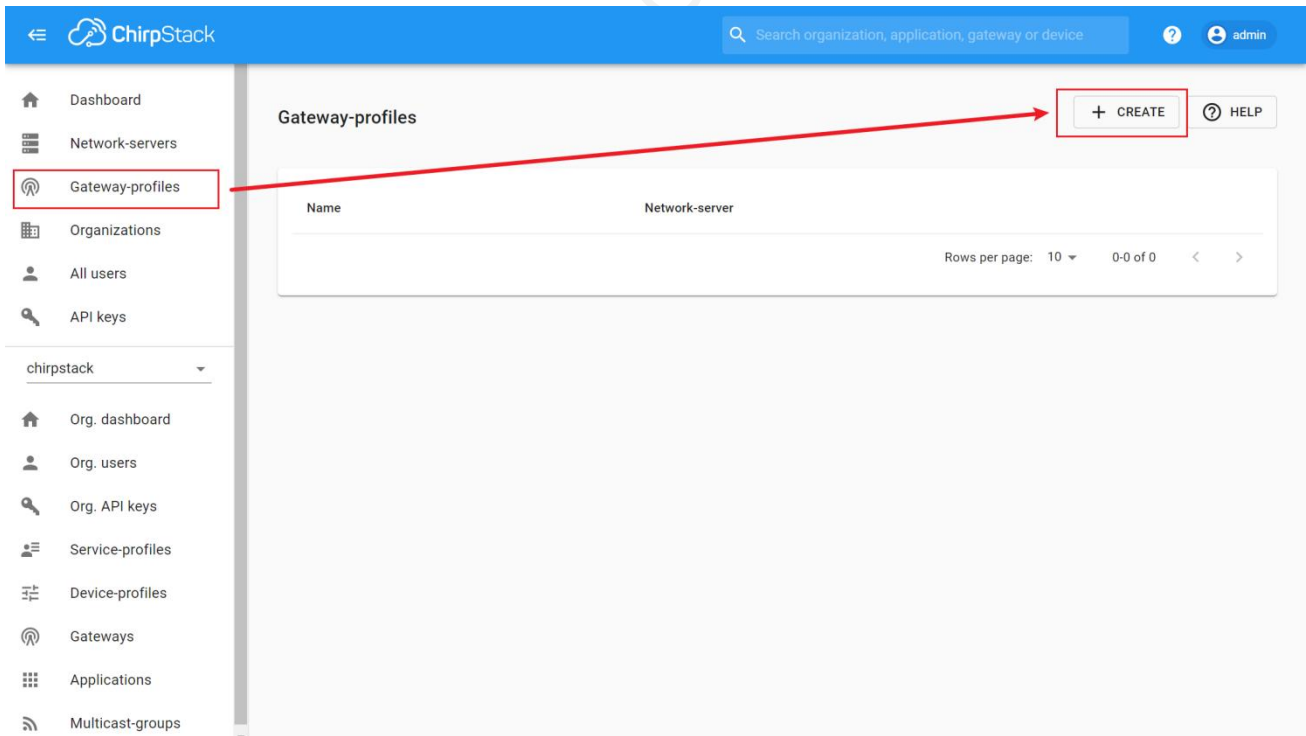
# Log to syslog.
#
# When set to true, log messages are being
written to syslog.
log_to_syslog=false

# The number of times passwords must be
hashed. A higher number is safer as
# an attack takes more time to perform.
password_hash_iterations=100000

# PostgreSQL settings.
```

**RESET** **APPLY**

### 4.4.3 Create the Gateway-profiles



**ChirpStack** Search organization, application, gateway or device admin

**Gateway-profiles** **+ CREATE** **HELP**

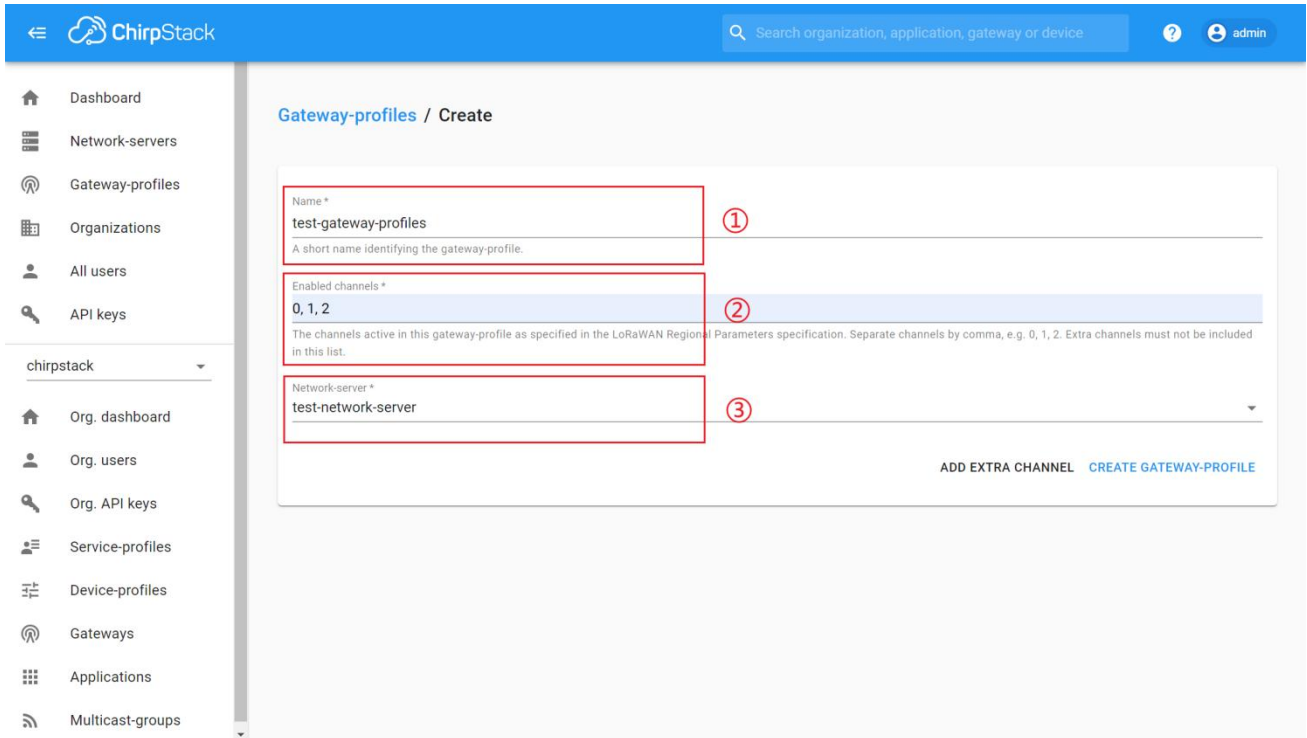
Name	Network-server

Rows per page: 10 0-0 of 0

- ① Name: custom name.
- ② Enabled channels: 0, 1, 2  
EU channels: 0, 1, 2

US902-923 channels (sub-band 2): 8, 9, 10, 11, 12, 13, 14, 15, 65

- ③ Network-server: select the Network-server you created earlier.



**Gateway-profiles / Create**

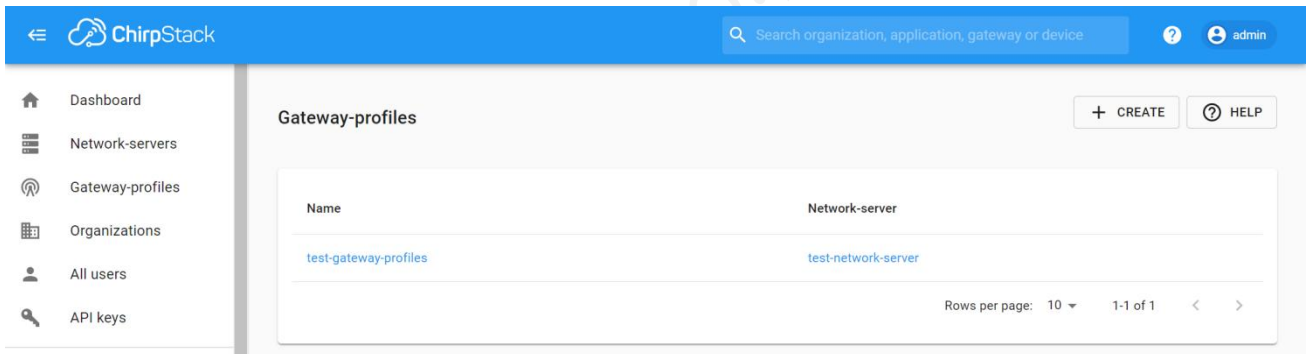
Name \*  
test-gateway-profiles  
A short name identifying the gateway-profile. ①

Enabled channels \*  
0, 1, 2  
The channels active in this gateway-profile as specified in the LoRaWAN Region Parameters specification. Separate channels by comma, e.g. 0, 1, 2. Extra channels must not be included in this list. ②

Network-server \*  
test-network-server ③

ADD EXTRA CHANNEL CREATE GATEWAY-PROFILE

Click the “GREATE GATEWAY-PROFILE”.

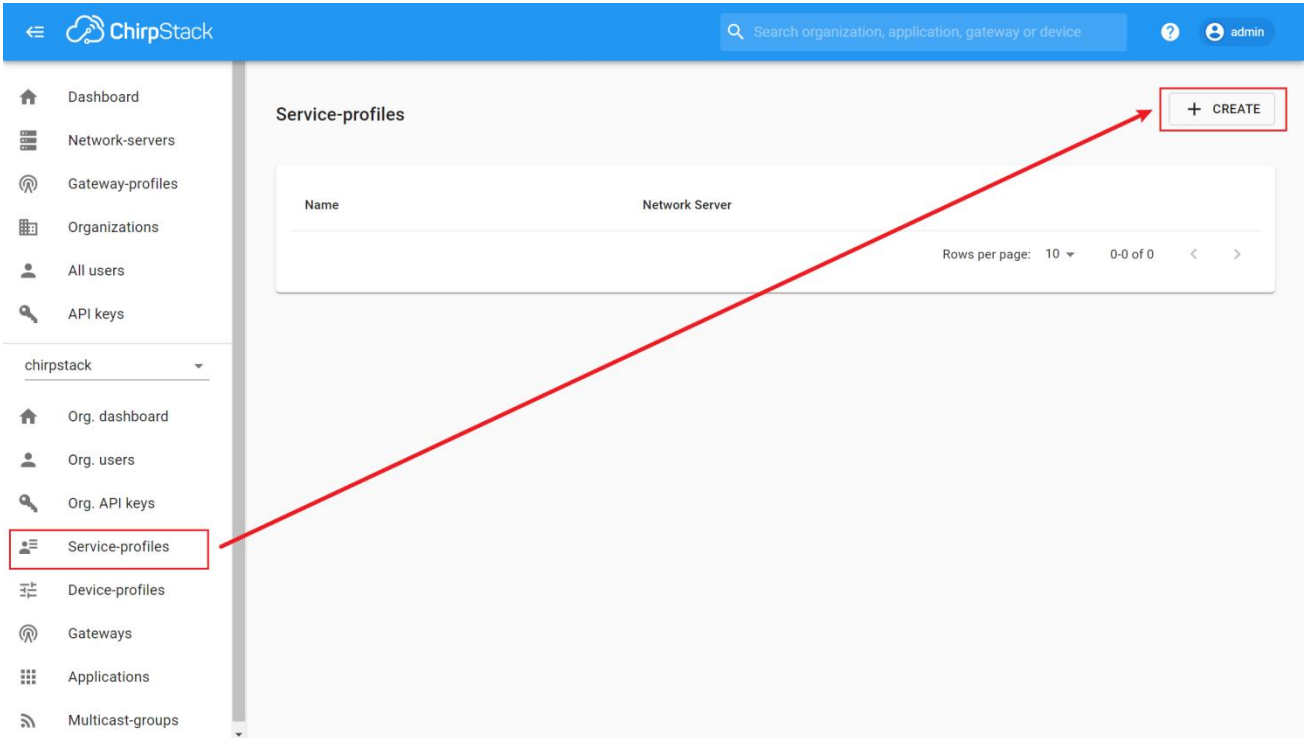


**Gateway-profiles** + CREATE ? HELP

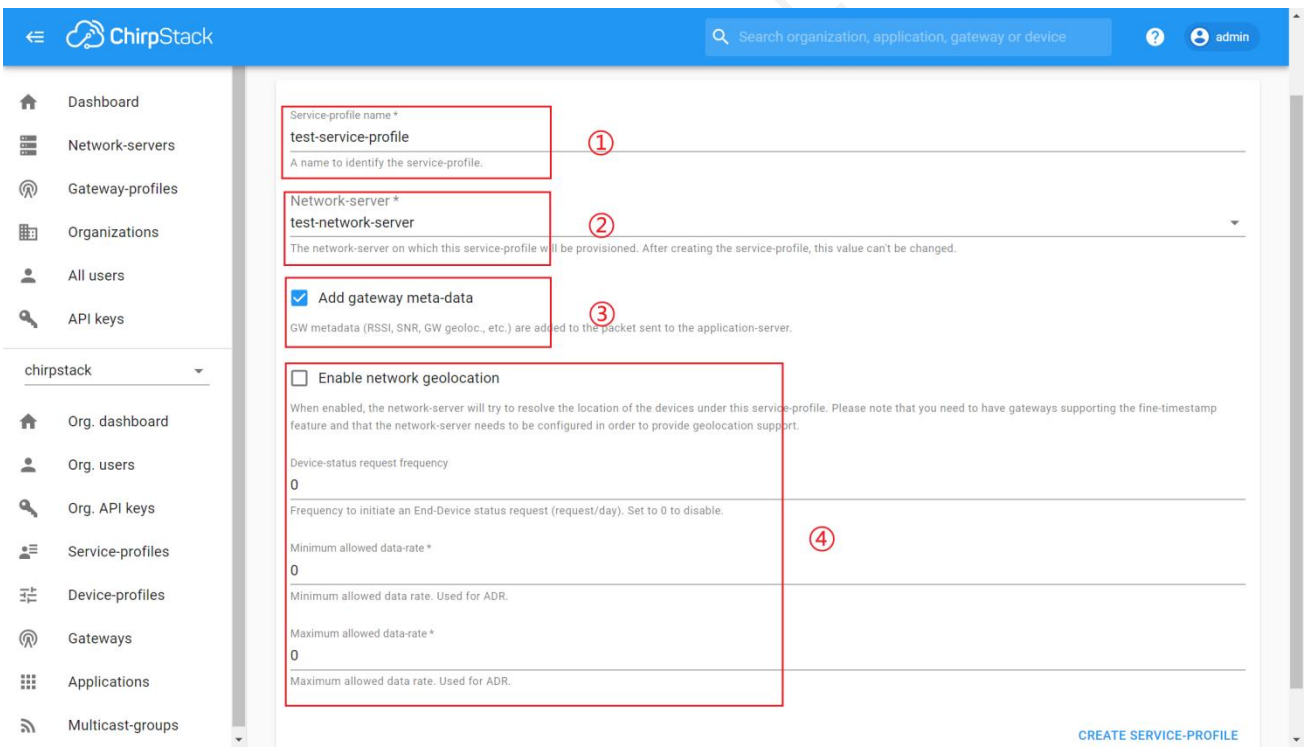
Name	Network-server
test-gateway-profiles	test-network-server

Rows per page: 10 1-1 of 1 < >

#### 4.4.4 Create the Service-profiles



The screenshot shows the ChirpStack web interface. The top navigation bar includes a search bar and a user profile labeled 'admin'. The left sidebar contains a menu with items like Dashboard, Network-servers, Gateway-profiles, Organizations, All users, API keys, and a dropdown for 'chirpstack'. Under the 'chirpstack' dropdown, 'Service-profiles' is highlighted with a red box. A red arrow points from this box to a '+ CREATE' button in the top right corner of the main content area. The main content area shows a table with one row: 'Name' | 'Network Server'. Below the table, it indicates 'Rows per page: 10' and '0-0 of 0'.



The screenshot shows the 'CREATE SERVICE-PROFILE' form in ChirpStack. The form fields are:
 

- Service-profile name \***: 'test-service-profile' (marked with ①). Description: 'A name to identify the service-profile.'
- Network-server \***: 'test-network-server' (marked with ②). Description: 'The network-server on which this service-profile will be provisioned. After creating the service-profile, this value can't be changed.'
- Add gateway meta-data**: Checked (marked with ③). Description: 'GW metadata (RSSI, SNR, GW geoloc., etc.) are added to the packet sent to the application-server.'
- Enable network geolocation**: Unchecked (marked with ④). Description: 'When enabled, the network-server will try to resolve the location of the devices under this service-profile. Please note that you need to have gateways supporting the fine-timestamp feature and that the network-server needs to be configured in order to provide geolocation support.'

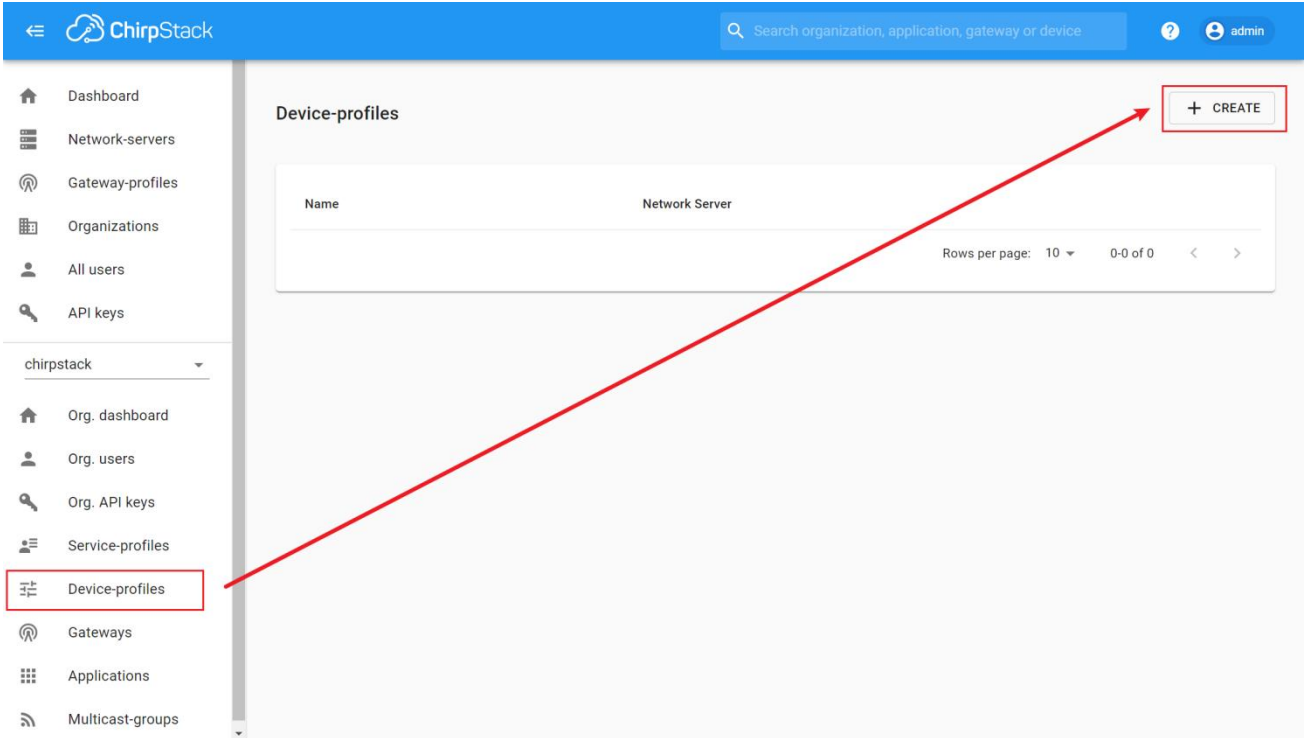
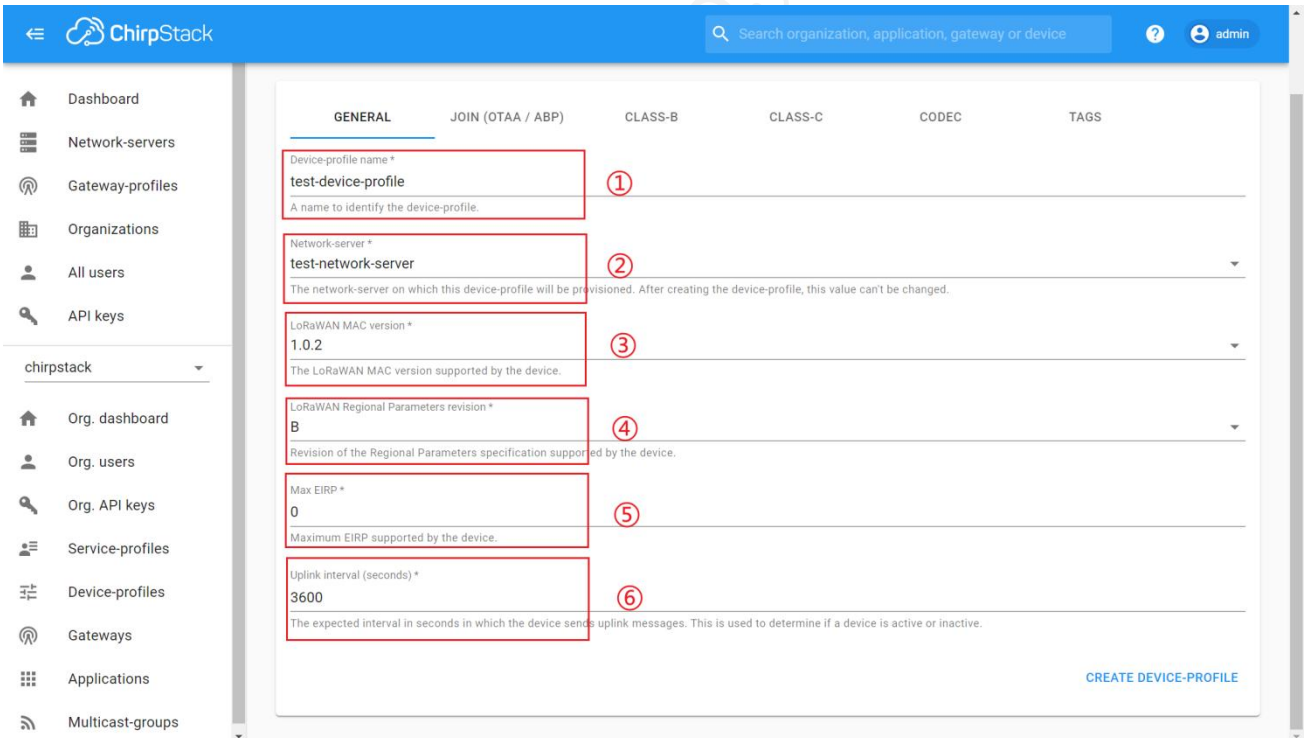
 Below these are three input fields for data rates, all with the value '0':
 

- Device-status request frequency**: '0'. Description: 'Frequency to initiate an End-Device status request (request/day). Set to 0 to disable.'
- Minimum allowed data-rate \***: '0'. Description: 'Minimum allowed data rate. Used for ADR.'
- Maximum allowed data-rate \***: '0'. Description: 'Maximum allowed data rate. Used for ADR.'

 A 'CREATE SERVICE-PROFILE' button is located at the bottom right of the form.

- ① Service-profile name: custom name.
- ② Network-server: select the Network-server you created earlier.
- ③ Add gateway meta-data: select it.
- ④ Default values are usually used.

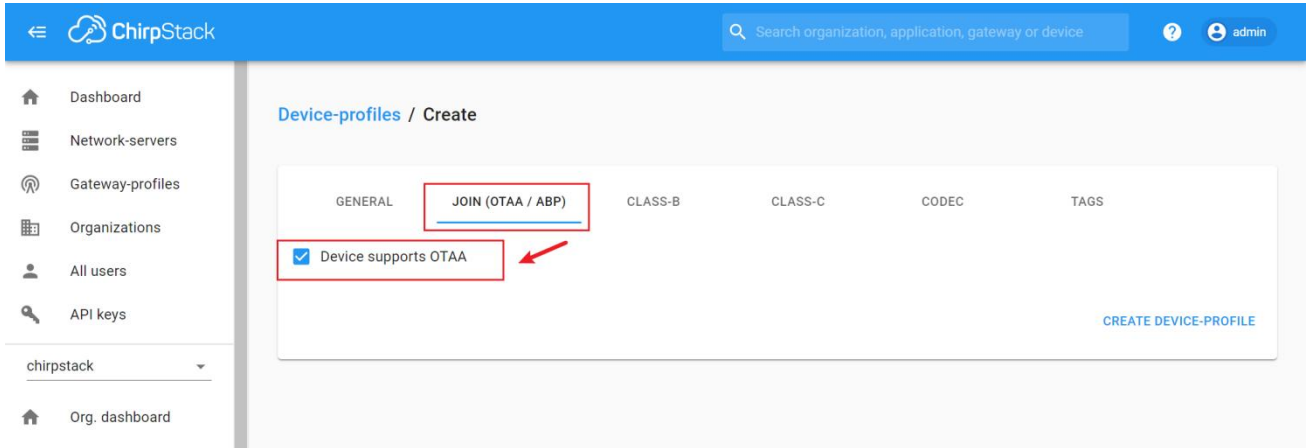
## 4.4.5 Create the Device-profiles

- ① Device-profile name: custom name.
- ② Network-server: select the Network-server you created earlier.
- ③ LoRaWAN MAC version: 1.0.2 (only for SenseCAP Node)
- ④ LoRaWAN Regional Parameters revision: B (only for SenseCAP Node)

- ⑤ Max EIRP: 0
- ⑥ Uplink interval (seconds): 3600  
Be consistent with the node's upload interval.

Click the “JOIN(OTAA/ABP)”, and select “Device supports OTAA”.



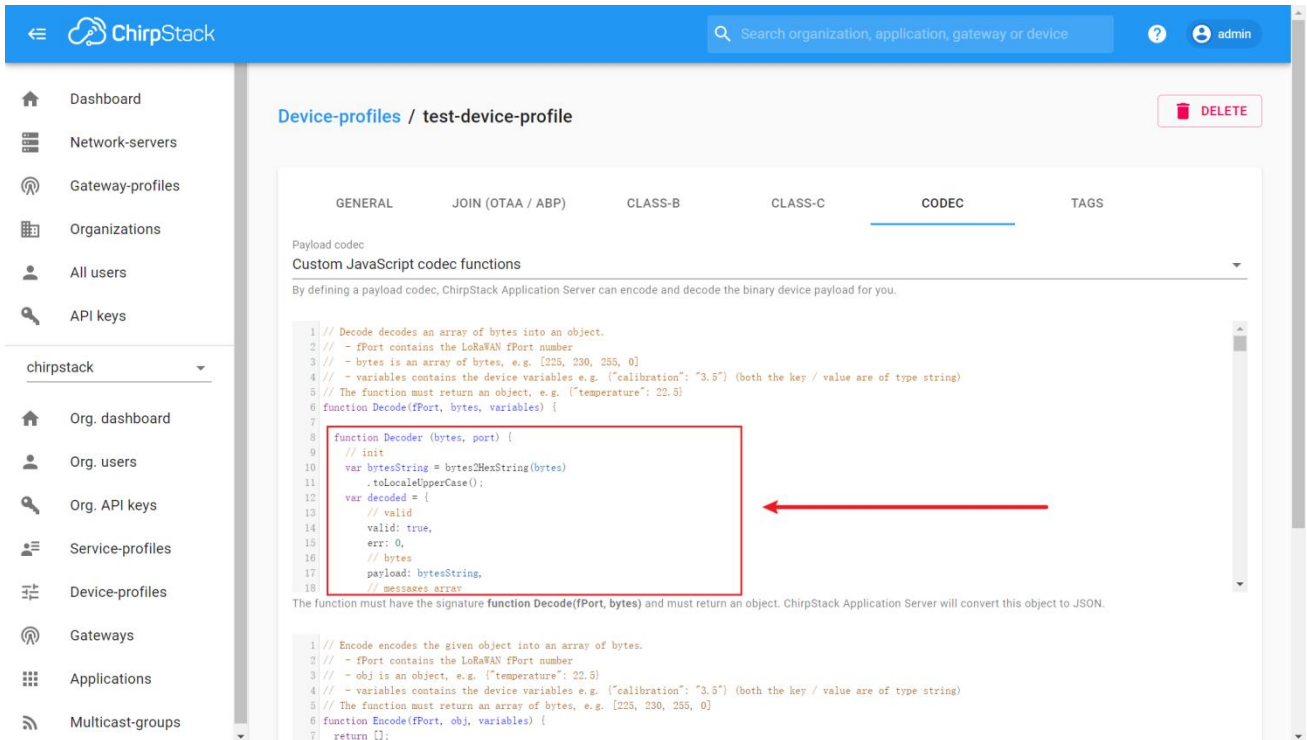
To get a SenseCAP Sensor Node on quick decoding, we provide a piece of code.

Click the “CODEC”, and select “Custom JavaScript codec functions”.

Then view <https://github.com/Seeed-Solution/TTN-Payload-Decoder/blob/master/decoder.js> , please copy the code to “function decode” FUNC.

```
function Decoder (bytes, port) {
  // init
  var bytesString = bytes2HexString(bytes)
    .toLocaleUpperCase();
  .....

  return binaryData.toString()
    .replace(/,/g, "");
}
```



Device-profiles / test-device-profile DELETE

GENERAL JOIN (OTAA / ABP) CLASS-B CLASS-C **CODEC** TAGS

Payload codec  
Custom JavaScript codec functions

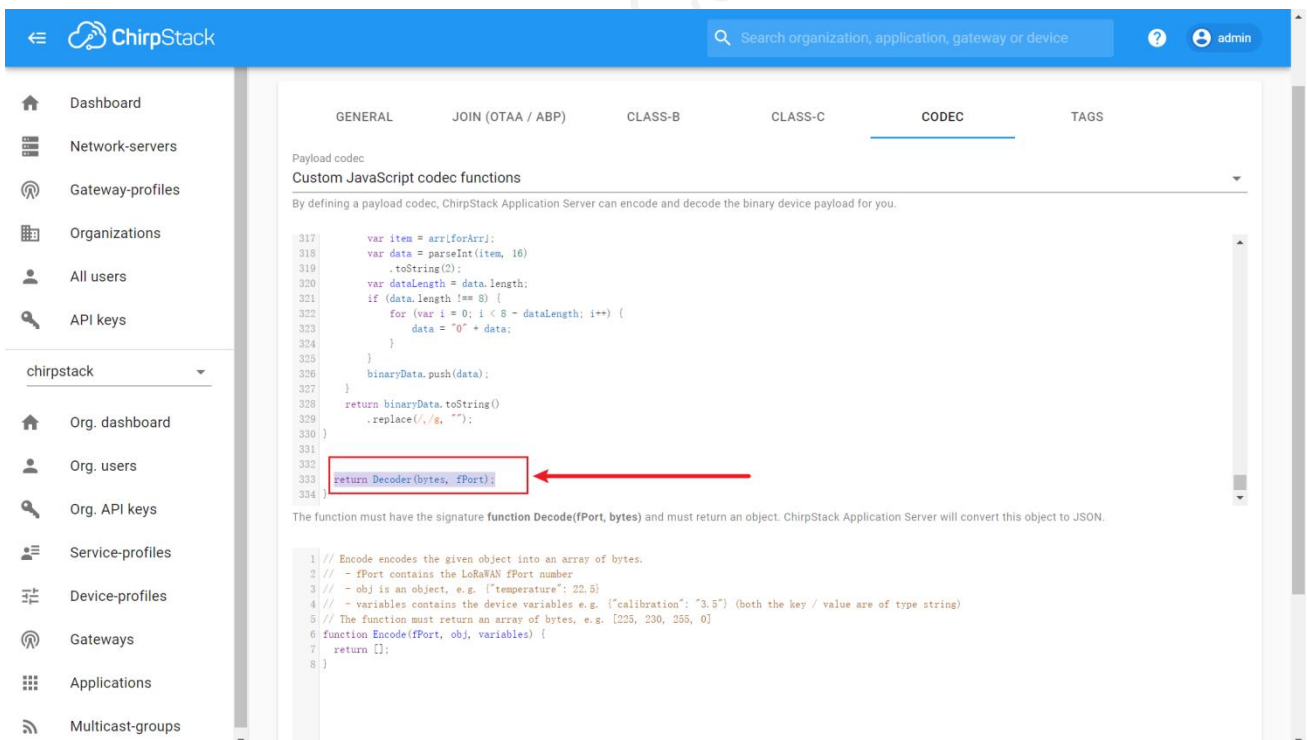
By defining a payload codec, ChirpStack Application Server can encode and decode the binary device payload for you.

```

1 // Decode decodes an array of bytes into an object.
2 // - fPort contains the LoRaWAN fPort number
3 // - bytes is an array of bytes, e.g. [225, 230, 255, 0]
4 // - variables contains the device variables e.g. {"calibration": "3.5"} (both the key / value are of type string)
5 // The function must return an object, e.g. {"temperature": 22.5}
6 function Decode(fPort, bytes, variables) {
7
8     function Decoder(bytes, port) {
9         // init
10        var bytesString = bytes2HexString(bytes)
11        toLocaleUpperCase();
12        var decoded = {
13            // valid
14            valid: true,
15            err: 0,
16            // bytes
17            payload: bytesString,
18            // messages array
19        };
20    }
21
22    // Encode encodes the given object into an array of bytes.
23    // - fPort contains the LoRaWAN fPort number
24    // - obj is an object, e.g. {"temperature": 22.5}
25    // - variables contains the device variables e.g. {"calibration": "3.5"} (both the key / value are of type string)
26    // The function must return an array of bytes, e.g. [225, 230, 255, 0]
27    function Encode(fPort, obj, variables) {
28        return [];
29    }
30
31    return Decoder(bytes, fPort);
32
33 }
    
```

Add the return value at the end:

return Decoder(bytes, fPort);



GENERAL JOIN (OTAA / ABP) CLASS-B CLASS-C **CODEC** TAGS

Payload codec  
Custom JavaScript codec functions

By defining a payload codec, ChirpStack Application Server can encode and decode the binary device payload for you.

```

317     var item = arr[forArr];
318     var data = parseInt(item, 16)
319     .toString(2);
320     var dataLength = data.length;
321     if (data.length !== 8) {
322         for (var i = 0; i < 8 - dataLength; i++) {
323             data = "0" + data;
324         }
325     }
326     binaryData.push(data);
327 }
328 return binaryData.toString()
329 .replace(/,/g, "");
330
331
332 return Decoder(bytes, fPort);
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
    
```

Finally, click "Create".

## 5 Device Installation

In this chapter, we will introduce the gateway, its respective installation processes, as well as the dos and don'ts. Before installing, please check the part list to ensure nothing is missing.

Seeed Technology Co., Ltd. Authorised



## 5.1 Part List

### 5.1.1 Gateway Part List



The LoRa Gateway comes with a standard antenna. If you need ultra-long-distance communication, you will need to purchase a high-gain fiberglass antenna.

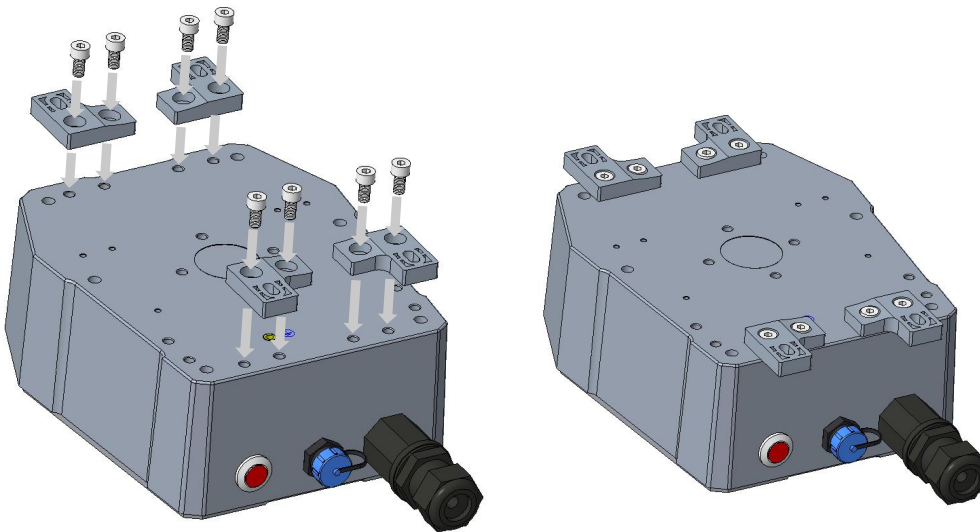
Item	Name	Quantity
1	LoRa Gateway	1
2	LoRa Antenna	1
3	4G Antenna	1
4	Allen Hex Key	1
5	Mounts	4
6	Power Adapter	1
7	Power Extension Cable (5M)	1
8	Ferrules / Aluminum piece	2 / 2
9	M5 Self-drilling Screw	8
10	Antenna Lightning Protector (*Optional)	1
11	LoRa Fiberglass Omni Antenna (*Optional)	1
12	LoRa Antenna Brackets (*Optional)	1

## 5.2 Gateway Installation

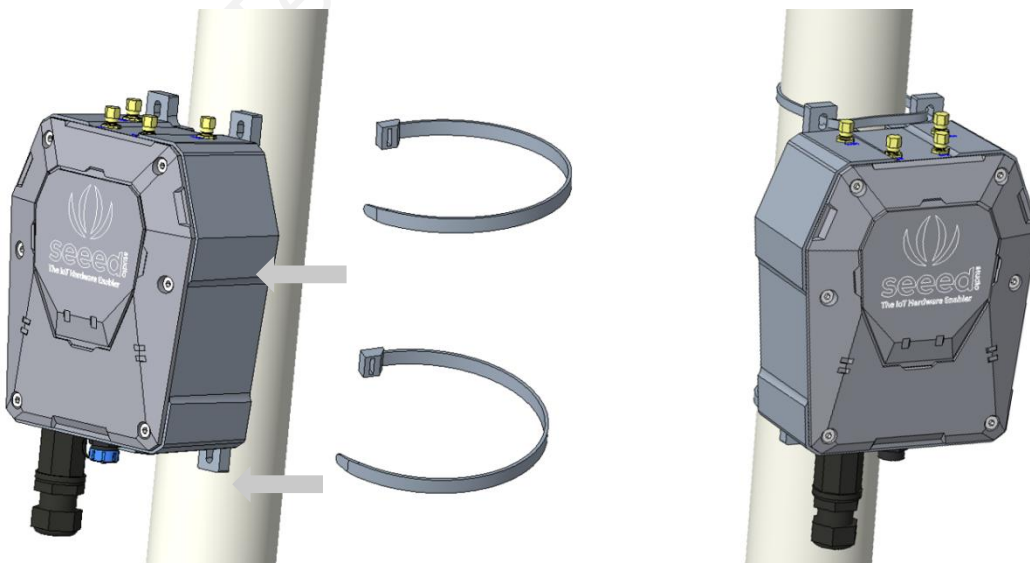
### 5.2.1 Gateway Installation Methods

- **Installing on a pole (Use the Mounts)**

Firstly, use M5 self-drilling screws (included in the package) to fasten the 4 brackets onto the gateway. And then use cable ties to fasten the gateway onto the pole. The recommended pole diameter is 70mm.

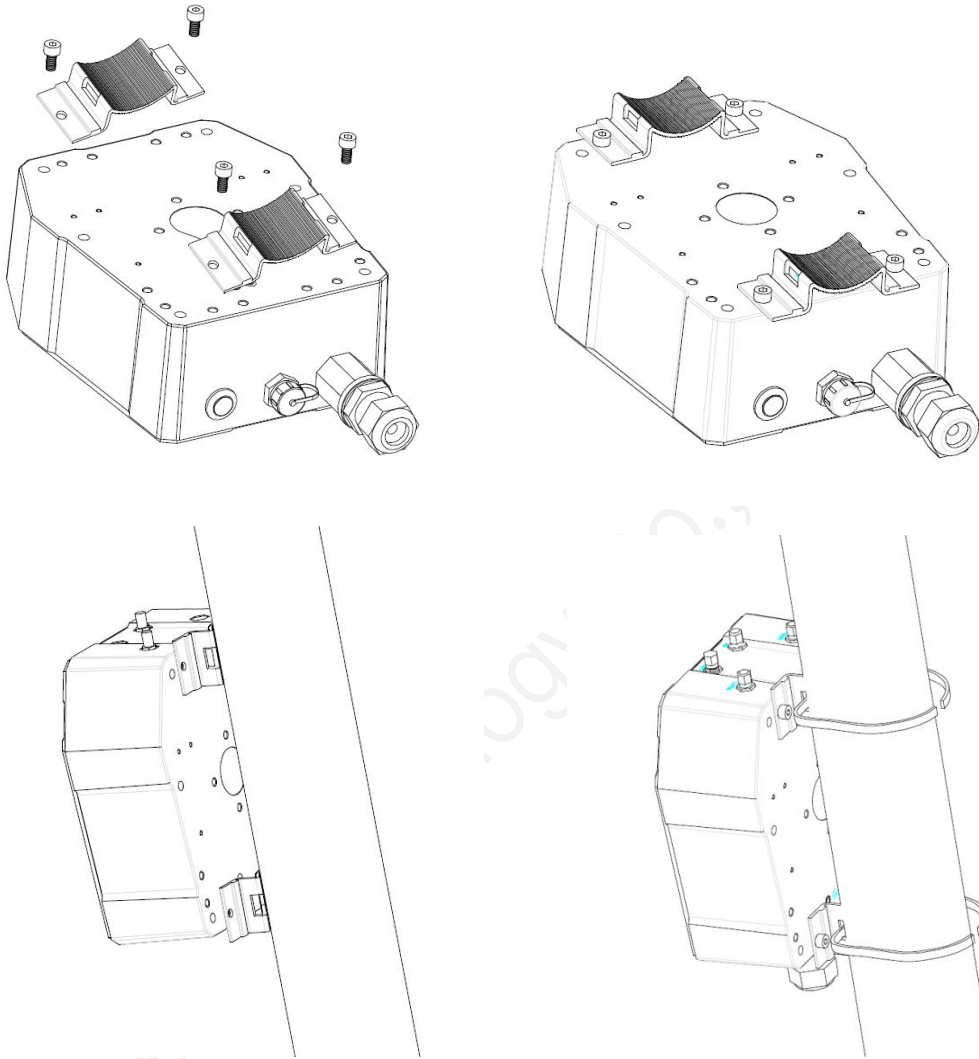


Put cable ties through the holes of the bracket and pull to fasten onto the pole. To get a better communication range, it is recommended to mount the gateway 3 meters above the ground. If there are tall buildings around, the gateway should be kept away from the building or mounted on top of the tall building.



- **Installing on a pole (Use the Ferrules and Aluminum pieces)**

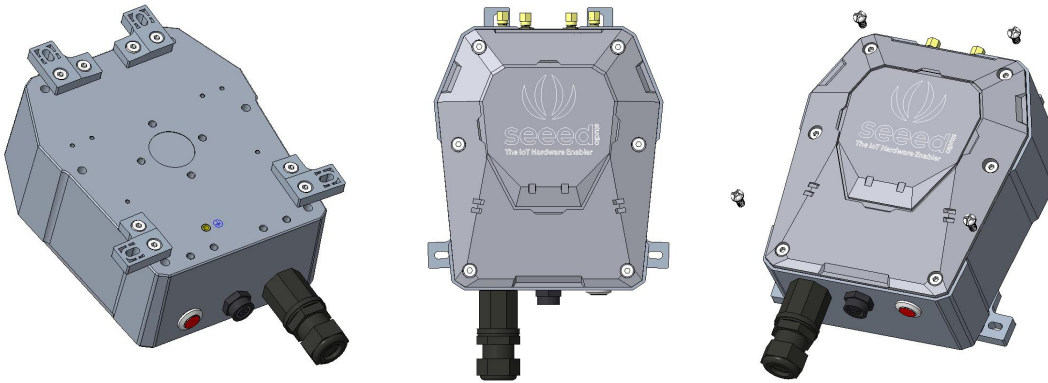
Firstly, use M5 self-drilling screws (included in the package) to fasten the 2 Aluminum pieces onto the gateway. And then use ferrules to fasten the gateway onto the pole. The recommended pole diameter is 76mm.



**Note:** If the pole is made of metal, the antenna should be pulled higher than the metallic part of the pole, or the communication signal will have interfered.

- **Installing on the Wall**

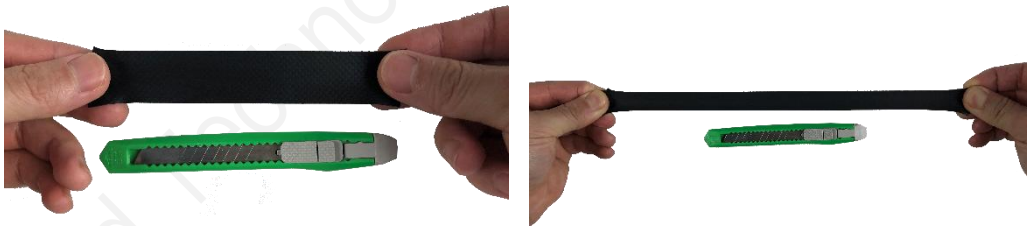
Firstly, use M5 self-drilling screws (included) to fasten the 4 brackets onto the enclosure of the gateway (refer to the image below for directions). And then fasten the gateway onto the wall with screws.



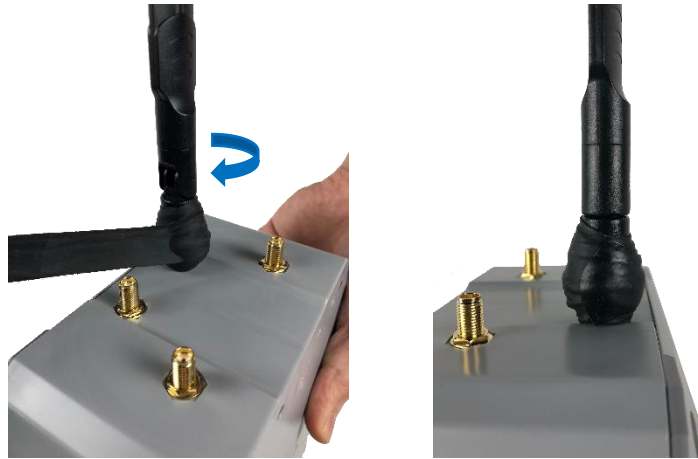
**Note:** The screws (that fasten gateway onto the wall) are not included in the package. Please prepare screws according to the wall materials (recommended screw diameter: 6mm).

## 5.2.2 Installation Precautions

- 1) In mountainous or thunderstorm-stricken areas, please take lightning protection measures. For the fiberglass LoRa antenna, you will need to install a lightning arrester and make sure it is connected to the ground. Besides, the gateway should be mounted lower than the lightning rod.
- 2) When installing the gateway in the outdoor environment, the connected part should be protected with waterproof tape, to enhance waterproof performance and lengthen device lifespan. As shown below, use self-adhesive tape to protect the connection. Take a rubber tape at the length of 10cm ~ 15cm, pull it to twice of that length



wind the tape clockwise to the connected part of the antenna.



**Note:** The tape must be wound clockwise because the antenna is fastened clockwise. Otherwise, the antenna may loosen.

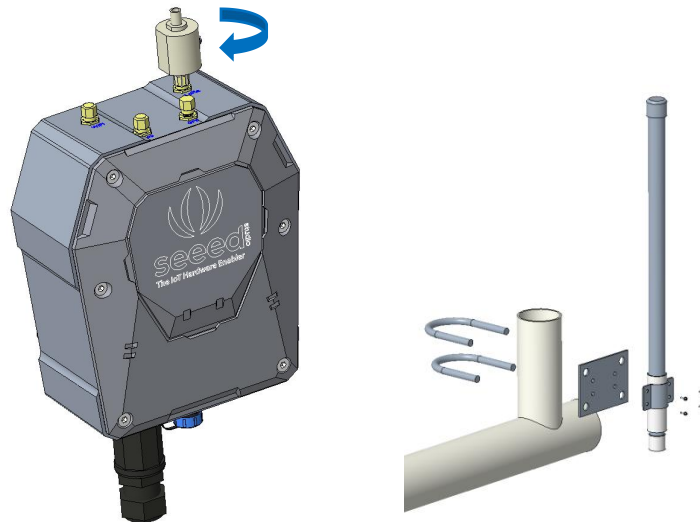
If the sensor has wires, install threaded tubes:



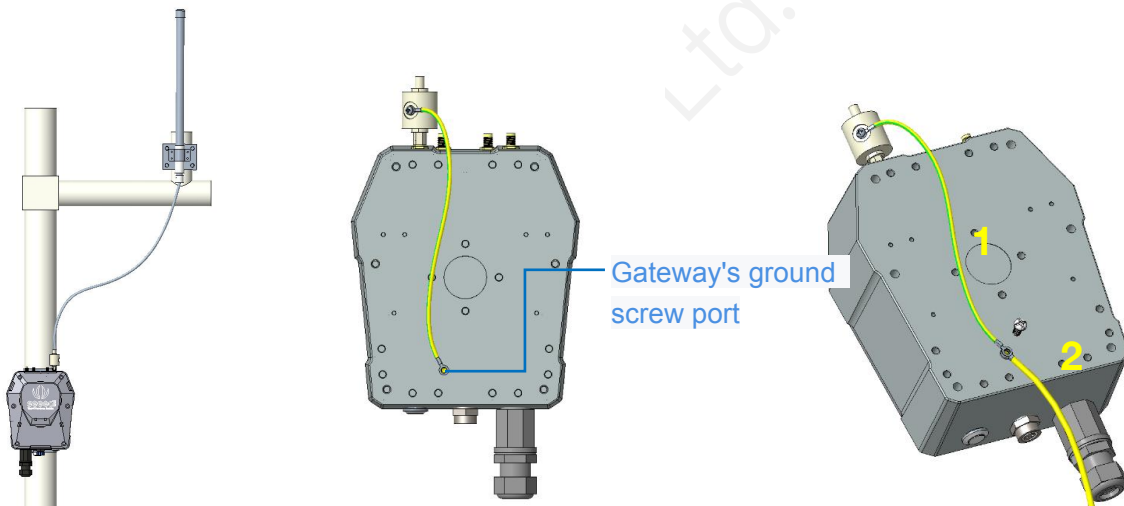
### 5.2.3 Installing Fiberglass LoRa Antenna

There are two kinds of LoRa antennas: the normal LoRa antenna (included in the package), and the fiberglass LoRa antenna (to be purchased separately). We will introduce how to install the fiberglass LoRa antenna.

- 1) Fasten the lightning arrester onto the antenna port.



- 2) As shown in the image below, please fasten the fiberglass antenna onto the base part, and then fasten the whole part onto the vertical cylinder (maximum cylinder diameter: 50mm).
- 3) Use a 1-meter antenna feed line to connect the lightning arrester with the fiberglass antenna.



### 5.2.4 Installing Ground Cable

Here we will connect the lightning arrester to the GND screw port on the gateway with a ground cable, and then connect the whole device to the ground. The image below shows the location of the GND port at the backside of the gateway.

- 1) Prepare two copper cables, a shorter one (approx. 30cm) for connecting the lightning arrester with the GND screw port (on the gateway), and a longer one for connecting the device to the ground.
- 2) Fasten the lightning arrester to the short copper cable with screws, and then connect the two copper cables to the GND screw port. Use the screw to connect and fasten them.
- 3) Once the two cables are connected, connect the other end of the long cable to the ground. Depending on your actual installation environment, you can connect it to the ground directly or connect it to the copper ground bars.