

# RAK7268 Unterstützte LoRa-Netzwerkserver

## AWS IoT Core für LoRaWAN

Wenn Sie noch kein AWS-Konto haben, lesen Sie die Anweisungen in der Anleitung [unter](#). Die relevanten Abschnitte sind „Anmelden für ein AWS-Konto“ und „Benutzer erstellen und Berechtigungen erteilen“.

## Übersicht

Die wichtigsten Schritte für den Einstieg in AWS IoT Core für LoRaWAN sind wie folgt:

1. Integrieren Sie Ihr Gateway (siehe Abschnitt „[Hinzufügen des Gateways zu AWS IoT](#)“).
2. Auf Ihrem Gerät/Ihren Geräten (siehe Abschnitt „[Hinzufügen eines LoRaWAN-Geräts zu AWS IoT](#)“) a. Überprüfen Sie die Geräte- und Dienstprofile.
  - b. Richten Sie ein Ziel ein, an das der Geräteverkehr weitergeleitet und anhand einer Regel verarbeitet wird.

Diese Schritte werden im Folgenden näher erläutert. Weitere Informationen finden Sie im [AWS LoRaWAN-Entwicklerhandbuch](#) [unter](#).

## Fügen Sie das Gateway zu AWS IoT hinzu

### Vorbereitung

Die erforderlichen Schritte vor dem Hinzufügen Ihres Gateways finden Sie im [Online-Handbuch](#) „[Hinzufügen eines Gateways zu AWS IoT](#)“. Weitere Informationen finden Sie auf der Datenblattseite: [WisGate Edge Lite 2 Datenblatt Software](#).

## Auswahl des Frequenzbands und Einrichtung der Rolle

Informationen zur Auswahl eines geeigneten Frequenzbands finden Sie im [Online-Handbuch](#) „[Frequenzbandzuweisung](#)“ (Leitfaden zur Frequenzzuweisung für drahtlose Netzwerke).

### HINWEIS

Von RAK7248 unterstützte LoRa®-Frequenzbänder: IN865, EU868, US915, AU915, KR920 und AS923. Bitte wählen Sie ein geeignetes Frequenzband aus unserem Shop aus.

Befolgen Sie die Anweisungen im Abschnitt „Hinzufügen einer IAM-Rolle“, damit der Konfigurations- und Aktualisierungsserver (CUPS) die Gateway-Anmeldeinformationen verwalten kann, wie im [Online-Handbuch](#) „[Hinzufügen eines Gateways](#)“ beschrieben.

## LoRaWAN-Gateway hinzufügen

Um das Gateway bei AWS IoT Core für LoRaWAN zu registrieren, befolgen Sie die Schritte in dieser [Online-Anleitung](#) im Abschnitt „Hinzufügen eines Gateways über die Konsole“.

## Hinzufügen eines LoRaWAN-Geräts zu AWS IoT

### Vorbereitung

Weitere Informationen zum [RAK4631 WisBlock LPWAN-Modul](#) finden Sie im Datenblatt [unter](#). Befolgen Sie die Anweisungen im Abschnitt „Vor der Einbindung Ihres drahtlosen Geräts“ im [Online-Handbuch](#) [unter](#). Befolgen Sie anschließend die Anweisungen im Abschnitt „Hinzufügen Ihres drahtlosen Geräts zu AWS IoT Core für LoRaWAN“ [unter](#).

## Profile überprüfen

AWS IoT Core für LoRaWAN unterstützt Geräteprofile und Dienstprofile. Geräteprofile enthalten die Kommunikations- und Protokollparameterwerte, die das Gerät für die Kommunikation mit dem Netzwerkserver benötigt. Dienstprofile beschreiben die Kommunikationsparameter, die das Gerät für die Kommunikation mit dem Anwendungsserver benötigt.

Für Geräte- und Dienstprofile stehen einige vordefinierte Profile zur Verfügung. Bevor Sie fortfahren, überprüfen Sie, ob diese Profileinstellungen mit den Geräten übereinstimmen, die Sie für die Verwendung mit AWS IoT Core für LoRaWAN einrichten möchten. Weitere Informationen finden Sie im Abschnitt „Profile zu AWS IoT Core für LoRaWAN hinzufügen“ im [Online-Handbuch](#) „ (Einführung in AWS IoT Core für LoRaWAN).

## Einrichten eines Ziels für den Geräteverkehr

Da die meisten LoRaWAN-Geräte keine Daten in einem Format an AWS IoT Core für LoRaWAN senden, das von AWS-Diensten verarbeitet werden kann, muss der Datenverkehr zunächst an ein Ziel gesendet werden. Ein Ziel repräsentiert die AWS IoT-Regel, die die Daten eines Geräts für die Verwendung durch AWS-Dienste verarbeitet. Diese AWS IoT-Regel enthält die SQL-Anweisung, die die Daten des Geräts auswählt, sowie die Themenregelaktionen, die das Ergebnis der SQL-Anweisung an die Dienste senden, die es verwenden werden.

Weitere Informationen finden Sie im [Online-Handbuch](#) „ (Abschnitte „Add a destination using the console“ und „Create an IAM role for your destinations“). Weitere Informationen finden Sie auch unter „Create rules to process LoRaWAN device messages“ im [Online-Handbuch](#) „“.

## Einrichten des Gateways

- Einrichten der Gateway-Hardware: Weitere Informationen finden Sie in der Produktkonfiguration unter „[RAK7268 Product Configuration](#)“ ([RAK7268-Produktkonfiguration](#)).
- Einrichten der Gateway-Software: Weitere Informationen finden Sie in der Produktkonfiguration unter „[RAK7268-Produktkonfiguration](#)“.
- Weitere Software-Referenzen:
  - [FAQ](#)
  - [Forum](#)

## Konfigurieren des Gateway-Geräts mit WisGateOS 1



Abbildung 1: RAK7268 mit WisGate OS 1 LoRaGateway-Einstellung

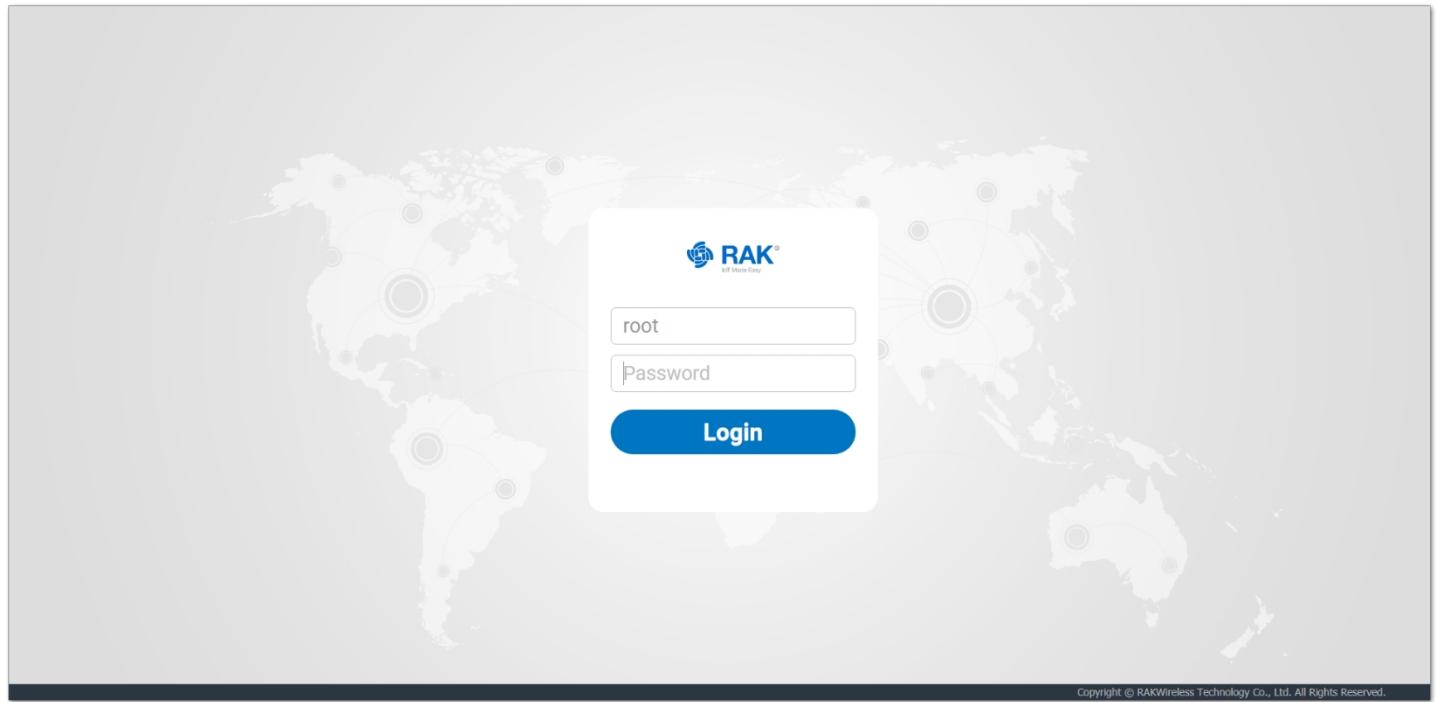
Standardmäßig arbeitet das Gateway im WLAN-AP-Modus, was bedeutet, dass Sie in der WLAN-Netzwerkliste Ihres PCs eine SSID mit dem Namen

„RAK7268\_XXXX“ in der WLAN-Netzwerkliste Ihres PCs finden. „XXXX“ sind die letzten beiden Bytes der MAC-Adresse des Gateways. Um auf die Web-Management-Plattform zuzugreifen, geben Sie die IP-Adresse 192.168.230.1 in Ihren Webbrowser ein.

(Hinweis: Für die Verbindung über WLAN ist kein Passwort erforderlich.

Geben Sie die oben genannte IP-Adresse in Ihren bevorzugten Webbrowser ein, und Sie sollten die gleiche Anmeldeseite wie in der folgenden Abbildung sehen. Melden Sie sich mit den unten angegebenen Anmeldedaten an:

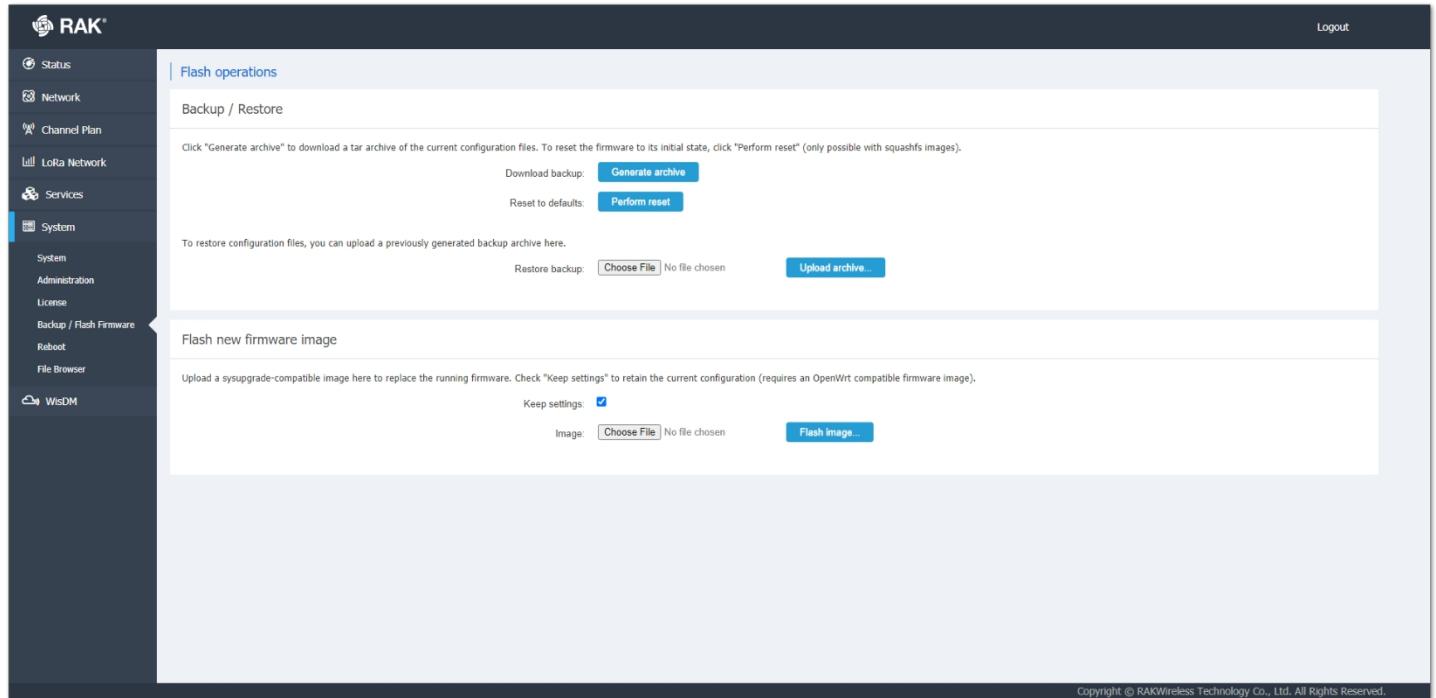
- Benutzername: root
- Passwort: root



**Abbildung 2:** Anmeldung über die Web-Benutzeroberfläche

C:\Benutzer\Mark\Dokumente\Arbeit\RAKwireless\Dokumentation\rakwireless-docs-internal\docs.vuepress\public\assets\images\wisgate\rak7268\unterstützte-lora-netzwerkserver\aws Die erste Firmware-Version, die AWS IoT Core für LoRaWAN unterstützt, ist 1.2.0065\_Release\_r209. Sie kann unter „Status -> Übersicht -> System -> Firmware-Version“ überprüft werden.

Navigieren Sie zu System -> Firmware sichern/flashen -> Neues Firmware-Image flashen und aktualisieren Sie die Firmware.



**Abbildung 3:** Aktualisieren der Firmware

#### Konfigurieren Sie den Netzwerkmodus auf „Basic Station“

1. Navigieren Sie zu LoRa-Netzwerk -> Netzwerkeinstellungen.
2. Ändern Sie den Modus in den LoRaWAN-Netzwerkeinstellungen auf „Basisstation“.
3. Wählen Sie unter „Server“ die Option „LNS-Server“ und unter „Authentifizierungsmodus“ die Option „TLS-Server und Client-Authentifizierung“.

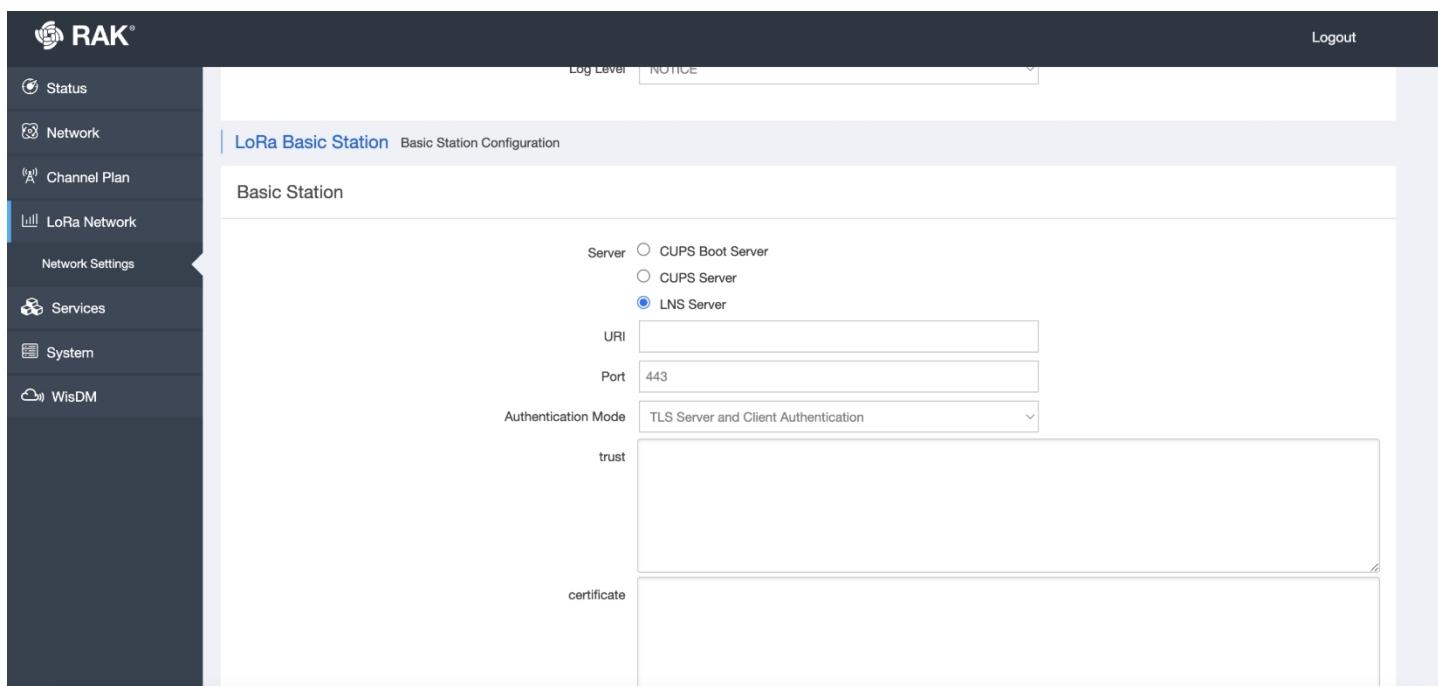


Abbildung 4: Netzwerkmodus auf Basisstation konfigurieren

#### URI, Port und Authentifizierungsmodus konfigurieren

This screenshot illustrates the configuration of the LoRa Basic Station and the generation of AWS IoT certificates. On the left, the 'Basic Station' configuration is identical to Abbildung 4. To the right, the AWS IoT console shows the creation of a gateway certificate. It displays the 'Gateway certificate' section with a green border around the 'cert.pem' file download link. Below it is the 'Provisioning credentials' section with a yellow border around the 'Copy' button for the CUPS endpoint. At the bottom, the 'Server trust certificates' section has a red border around its 'Download server trust certificates' button.

Abbildung 5: Konfigurieren Sie URI, Port und Authentifizierungsmodus

## Konfigurieren des Gateway-Geräts mit WisGateOS 2



Abbildung 6: RAK7268 mit WisGate OS 2 LoRaGateway-Einstellung

Standardmäßig arbeitet das Gateway im WLAN-AP-Modus, was bedeutet, dass Sie in der WLAN-Netzwerkliste Ihres PCs eine SSID mit dem Namen

„RAK7268\_XXXX“ in der WLAN-Netzwerkliste Ihres PCs finden. „XXXX“ sind die letzten beiden Bytes der MAC-Adresse des Gateways. Um auf die Web-Management-Plattform zuzugreifen, geben Sie die IP-Adresse 192.168.230.1 in Ihren Webbrower ein.

(Hinweis: Für die Verbindung über WLAN ist kein Passwort erforderlich.

Geben Sie die oben genannte IP-Adresse in Ihren bevorzugten Webbrower ein, und Sie sollten die gleiche Anmeldeseite wie in der folgenden Abbildung sehen. Melden Sie sich mit den unten angegebenen Anmeldedaten an

- Benutzername: root
- Passwort: <vom Benutzer definiert>

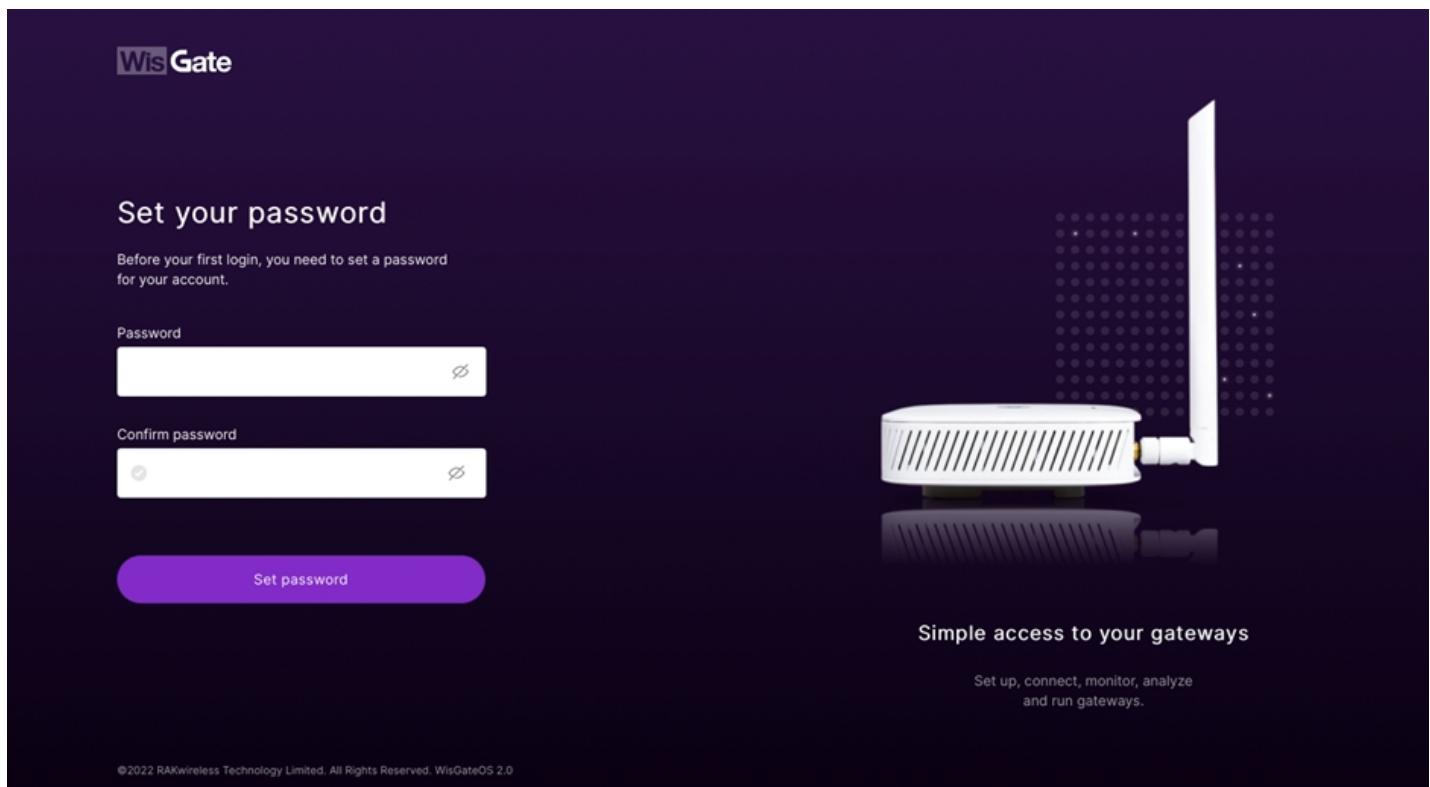
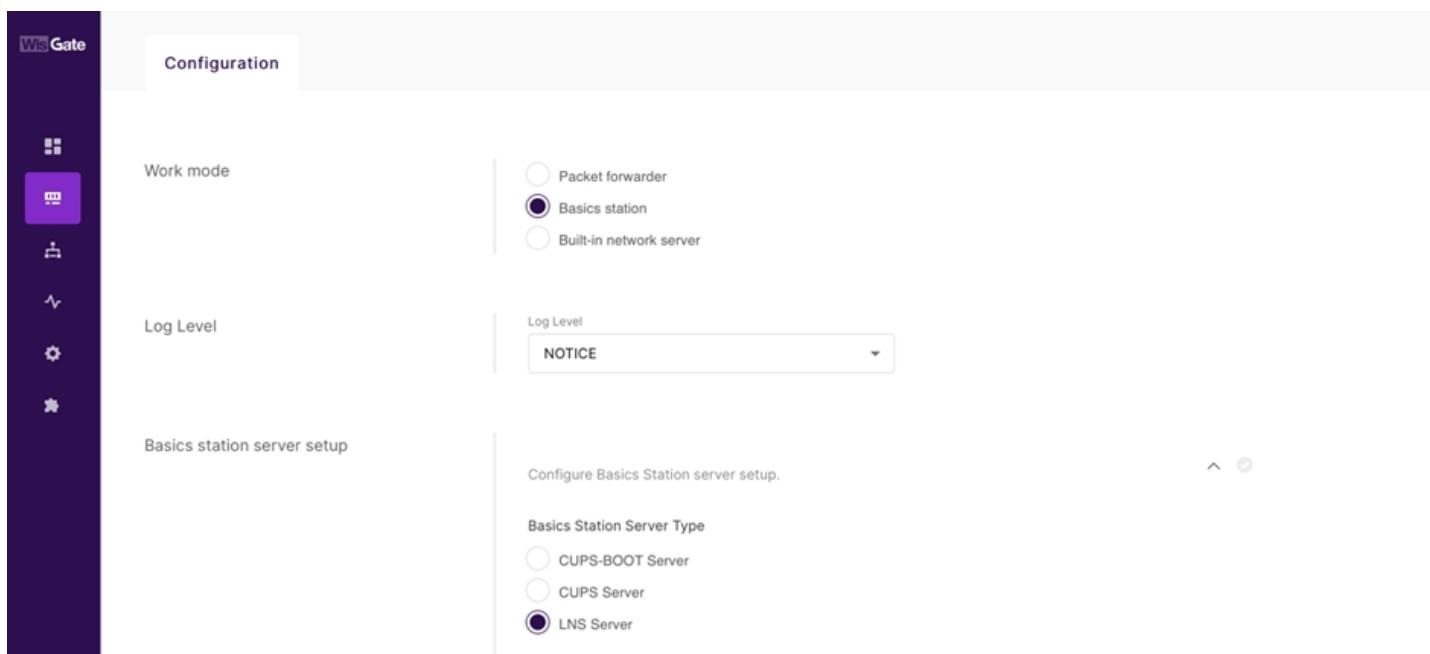


Abbildung 7: WisGate OS 2-Startseite

Navigieren Sie zu LoRa®; ändern Sie den Arbeitsmodus zu „Basics Station“ und wählen Sie „LNS Server“ unter „Server“ aus, wählen Sie dann „TLS Server“ und „Client Authentication“ unter „Authentication Mode“ aus.



**Abbildung 8:** WisGateOS2 Basics Station-Konfiguration

### Konfigurieren Sie URI, Port und Authentifizierungsmodus

Basics Station Server Type  
 CUPS-BOOT Server  
 CUPS Server  
 LNS Server

Server URL

Server Port

Authentication Mode  
 TLS Server & Client Authentication

Trust (CA Certificate)

Client certificate

Client key

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia ▾

Gateway certificate  
 Create a certificate so that your gateway can communicate securely with AWS IoT. Download the certificate files so that you can upload them to your gateway.

Create certificate Certificate created and associated with your gateway

These certificate files were created. Download them and save them to upload to your gateway.

Gateway certificate file 4e4fd3d8-9ce1-... .cert.pem

Private key file 4e4fd3d8-9ce1-... .private.key

[Download certificate files](#)

Provisioning credentials Info  
 Choose the endpoint that your gateway supports. Then, copy the endpoint and download the server trust certificate so that you can add them to your gateway.

CUPS (Configuration and Update Server) endpoint  
<https://.cups.lorawan.us-east-1.amazonaws.com:443> [Copy](#)

LNS (LoRaWAN Network Server) endpoint  
<https://.lns.lorawan.us-east-1.amazonaws.com:443> [Copy](#)

Server trust certificates  
 Download your server trust certificate so you can upload the certificate for the endpoint your gateway supports.

[Download server trust certificates](#)

**Abbildung 9:** Konfiguration der WisGateOS2 Basics Station

## Verbinden Sie das Gateway und überprüfen Sie den Verbindungsstatus

Befolgen Sie die Anweisungen im [Online-Handbuch „“](#), um Ihr Gateway mit AWS IoT Core for LoRaWAN zu verbinden.

Informationen zum Überprüfen des Verbindungsstatus finden Sie in den Anweisungen im Abschnitt „**Überprüfen des Gateway-Verbindungsstatus über die Konsole**“.

Gateways (2) <small>Info</small>				
Gateway ID	Name	Description	Last uplink received	
<input type="radio"/> fbf86532-864c-4f07-9a82-f66813f68b74	B827EBFFF829C33	-	-	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="radio"/> b8f1810f-2d78-4cf1-8646-95fa2cc5b871	RAK7268	-	June 29, 2022, 17:46:56 (UTC+0800)	<a href="#">Add gateway</a>

**Abbildung 10:** Status der Gateway-Verbindung

## Endgerät hinzufügen

Informationen zum Aktivieren der Kommunikation mit dem Gateway finden Sie im [RAK4631-Schnellstart-](#).

## Aktualisierung von RAK4631 auf RAK4631-R

RAK4631-R und RAK4631 verfügen über die gleiche Hardware und sind zu 100 % identisch, haben jedoch unterschiedliche Firmware. RAK4631-R basiert auf RUI3, wodurch Sie Flexibilität bei der Entwicklung optimierter Firmware unter Verwendung der RUI3-APIs erhalten.

Informationen zum [Aktualisieren von RAK4631 auf RUI3](#) finden Sie unter .

## Beitreten zum AWS IoT LoRaWAN-Server

In diesem Abschnitt finden Sie ein Beispiel dafür, wie Sie dem AWS IoT LoRaWAN-Server beitreten können.

### 1. Gerätprofil hinzufügen



**Device profile Info**  
Describe the device capabilities and boot parameters that the network server needs to set the LoRaWAN radio access service.

Select a default profile and customize - *optional*  
Default profiles are based on your selected LoRaWAN OTAA device class and your LoRaWAN radio frequency band. You may need to customized your profile per your device vendor specifications.

**US915 - A**

<b>Device profile name</b> Type a descriptive name for this device profile. <b>US915-A-OTAA</b>	<b>Frequency band (RFRegion)</b> Choose the LoRa supported frequency band for this profile. <b>US915</b>
<b>MAC version</b> The MACVersion of the LoRaWAN devices that use this profile. <b>1.0.3</b>	<b>Regional parameters version</b> Select the region parameters version identifier for this profile. <b>Regional Parameters v1.0.3rA</b>
<b>MaxEIRP</b> Enter the MaxEIRP value for this device profile. <b>13</b>	
<b>Supports Class B</b> Choose to enter the values for Class B support. <input checked="" type="radio"/>	
<b>Supports Class C</b> Choose to enter the values for Class C support. <input checked="" type="radio"/>	
<b>Supports Join</b> Choose to enter the values for Join support (OTAA) or not (ABP). <input checked="" type="radio"/>	
► Optional settings	

Abbildung 11: Hinzufügen des Gerätprofils

### 2. Dienstprofil hinzufügen

## Add service profile

**Service profile Info**

A service profile describes the features that are enabled for the user(s), and the rate of messages that can be sent over the network.

**Service profile name - optional**  
Enter a descriptive profile name.

**AddGWMetaData**  
Add additional gateway metadata (RSSI, SNR, GW geoloc., etc.) to the packets sent by devices.

**Tags - optional**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	Remove
<input type="text" value="Key"/>	<input type="text" value="Value"/>	<input type="button" value="Remove"/>

You can add up to 49 tags.

**Abbildung 12:** Hinzufügen des Dienstprofils

3. Ziel hinzufügen Bevor Sie das Ziel hinzufügen, befolgen Sie die Anweisungen im Abschnitt „IAM-Rolle für Ziel zu AWS IoT Core für LoRaWAN hinzufügen“, um die IAM-Richtlinie und -Rolle zu konfigurieren.

**Add destination Info**

**Destination details Info**

**Destination name**  
The destination name appears in the device and gateway destination selection lists.

**Destination description - optional**  
Provide a helpful description of your destination.

**Enter a rule name**  
Enter the name of the rule or a rule/topic that will process the messages sent to this destination.

**Publish to AWS IoT Core message broker**  
If you need a publish/subscribe broker to distribute messages to multiple subscribers

**Abbildung 13:** Ziel hinzufügen

#### 4. Gerät hinzufügen

- Bevor Sie ein Gerät zu AWS IoT hinzufügen, rufen Sie die DevEui, AppEui und AppKey aus der Konsole des Endgeräts ab. Sie können den AT-Befehl verwenden, um die Informationen abzurufen.
  - **AT+DEVEUI** : Endgeräte-ID
  - **AT+APPEUI** : Anwendungskennung
  - **AT+APPKEY** : Anwendungsschlüssel

Weitere AT-Befehle finden Sie im [RAK4631-R AT-Befehlshandbuch](#). Beispiel:

## LoRaWAN specification and wireless device configuration [Info](#)

**Wireless device specification**  
Your device specifications consist of the LoRaWAN version (1.1 or 1.0.x) and your authentication process (Over The Air Authentication or Authentication By Personalization). Once selected, your data is encrypted with a key that AWS owns and manages for you.

OTAA v1.0.x ▾

<b>DevEUI</b> <input type="text" value="0000000000000000"/> The 16-digit hexadecimal DevEUI value found on your wireless device.	<b>Confirm DevEUI</b> <input type="text" value="0000000000000000"/> Reenter the DevEUI.
<b>AppKey</b> <input type="text" value="00000000000000000000000000000000"/> The 32-digit hexadecimal AppKey value that your wireless device vendor provided.	<b>Confirm AppKey</b> <input type="text" value="00000000000000000000000000000000"/> Reenter the AppKey.
<b>AppEUI</b> <input type="text" value="0000000000000000"/> The 16-digit hexadecimal AppEUI that your wireless device vendor provided.	<b>Confirm AppEUI</b> <input type="text" value="0000000000000000"/> Reenter the AppEUI.
<b>Wireless device name - optional</b> <input type="text" value="RAK4631-R"/> A descriptive name to make the wireless device easier to locate.	

**Abbildung 14:** LoRaWAN-Spezifikationen und Konfiguration von Funkgeräten

<b>Profiles</b>
<b>Wireless device profile</b>
Choose a wireless device profile so your device can pass the correct messages to your gateway.
<input type="text" value="US915-A-OTAA"/> ▼
<b>Service profile</b>
Choose a service profile.
<input type="text" value="rak4631"/> ▼

**Abbildung 15:** Auswahl eines Profils für ein drahtloses Gerät

## Choose destination

**Choose destination**

---

Destination name  
Destinations route LoRaWAN messages from your wireless device to other AWS services.

ProcessLoRa ▾

**Abbildung 16:** Auswahl eines Ziels

Destination name

**Choose destination**

**Destination name**  
Destinations route LoRaWAN messages from your wireless device to other AWS services.

ProcessLoRa ▾

## 5. Verbinden Sie sich mit dem AWS IoT LoRaWAN-Server

Verwenden Sie den Befehl `JOIN` um dem AWS IoT LoRaWAN-Server beizutreten.

AT+JOIN=1:0:10:8

OK

+EVT:JOINED

## 6. Uplink-Nachricht senden

Verwenden Sie zum Senden von Daten über eine dedizierte Portnummer

```
AT+SEND=12:112233
OK
```

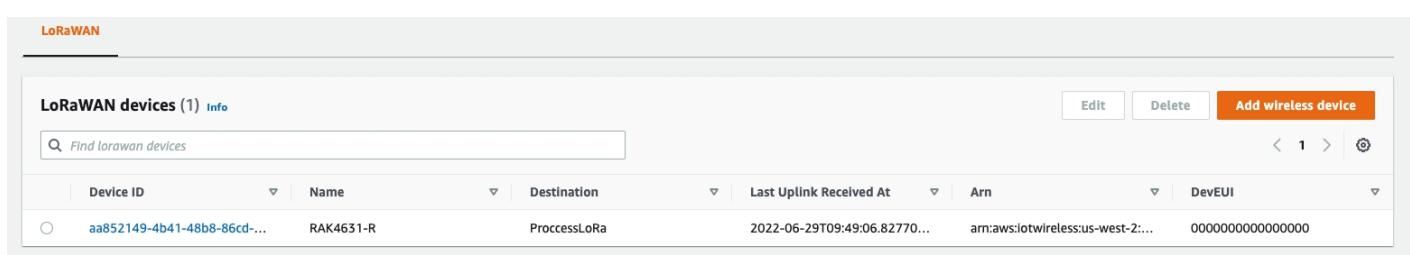


Abbildung 17: Uplink empfangen

## Verbinden Sie das Gerät und überprüfen Sie den Verbindungsstatus

Befolgen Sie die Anweisungen im [Online-Handbuch](#) „“ , um Ihr Gerät mit AWS IoT Core for LoRaWAN zu verbinden.

Um den Verbindungsstatus zu überprüfen, lesen Sie die Anweisungen im Abschnitt „Geräteverbindungsstatus über die Konsole überprüfen“. Sie können auch [das Format der von LoRaWAN-Geräten gesendeten Uplink-Nachrichten unter !\[\]\(8a8ea273bba45b658cf4779d37ab61e8\_img.jpg\) anzeigen](#).

## Überprüfen der Funktion – ein „Hello World“-Beispiel

Nach Abschluss der Einrichtung können bereitgestellte OTAA-Geräte dem Netzwerk beitreten und mit dem Senden von Nachrichten beginnen. Nachrichten von Geräten können dann von AWS IoT Core for LoRaWAN empfangen und an die IoT Rules Engine weitergeleitet werden.

Anweisungen für eine Beispielanwendung „Hello World“ finden Sie weiter unten, vorausgesetzt, das Gerät hat sich verbunden und ist in der Lage, Uplink-Datenverkehr zu senden. Die Architektur für diese Beispielanwendung ist:

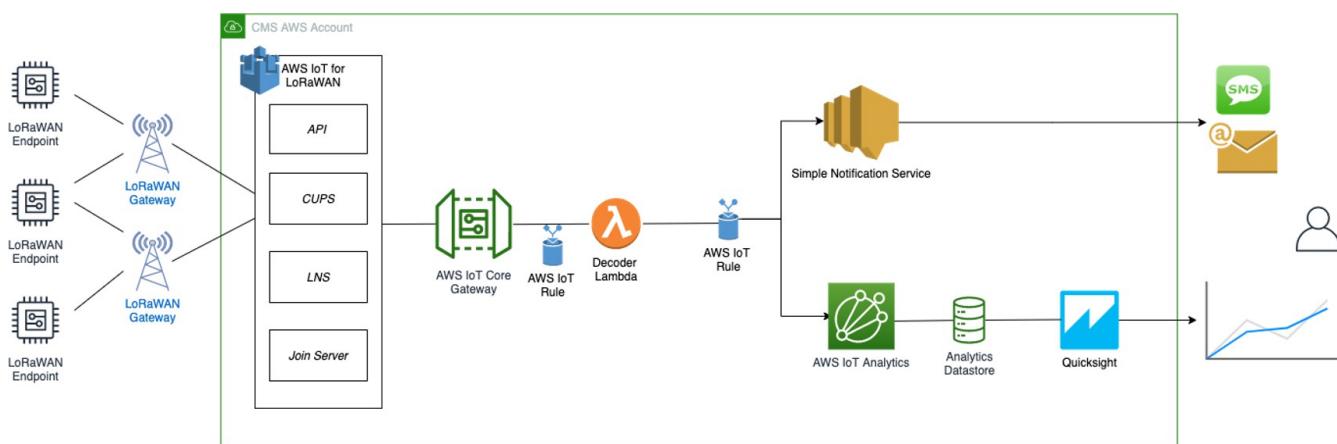


Abbildung 18: Architektur für das Senden von Uplink-Daten

## Lambda-Funktion für Zielregel erstellen

Erstellen Sie die Lambda-Funktion, um die von der Zielregel verarbeiteten Gerätemeldungen zu verarbeiten.

- Rufen Sie die AWS Lambda-Konsole auf ([console.aws.amazon.com/lambda](https://console.aws.amazon.com/lambda)).
- Klicken Sie im Navigationsbereich auf „**Funktionen**“.
- Klicken Sie auf „**Funktion erstellen**“.
- Wählen Sie „**Von Grund auf neu erstellen**“. Geben Sie unter „Grundlegende Informationen“ den Funktionsnamen ein und wählen Sie „Laufzeit Python“.
  - 3.8. aus der Dropdown-Liste unter „**Laufzeit**“.
- Klicken Sie auf „**Funktion erstellen**“.

- Fügen Sie in der Registerkarte „Codequelle“ unter „index.js“ den kopierten Code in den Editor unter der Registerkarte „**„lambda\_function.py“** ein.

```

import base64
import json
import logging
import ctypes
import boto3

# Funktionsnamen definieren
FUNCTION_NAME = „RAK-HelloWorld“

# Zweites Byte in der Nutzlast steht für Datentypen
# Referenz für Nutzlast mit geringem Stromverbrauch:
https://developers.mydevices.com/cayenne/docs/lora/ DATA_TYPES = 1

# Typ Temperatur TYPE_TEMP
= 0x67

# IoT-Daten-Client für boto3
einrichten client =
boto3.client('iot-data')

# Logger einrichten
logger = logging.getLogger(FUNCTION_NAME)
logger.setLevel(logging.INFO)

def decode(event):
    data_base64 = event.get("PayloadData")
    data_decoded = base64.b64decode(data_base64)

    result = {
        "devEui": event.get("WirelessMetadata").get("LoRaWAN").get("DevEui"), "fPort": event.get("WirelessMetadata").get("LoRaWAN").get("FPort"), "freq": event.get("WirelessMetadata").get("LoRaWAN").get("Frequency"), "timestamp": event.get("WirelessMetadata").get("LoRaWAN").get("Timestamp")
    }

    if data_decoded[DATA_TYPES] == TYPE_TEMP:
        temp = (data_decoded[DATA_TYPES + 1] << 8) | (data_decoded[DATA_TYPES + 2]) temp =
        ctypes.c_int16(temp).value
        result['temperature'] = temp / 10

    return result

def lambda_handler(event, context):
    data = decode(event)
    logger.info("Daten: %s" % json.dumps(data))

    Antwort = client.publish(
        topic = event.get("WirelessMetadata").get("LoRaWAN").get("DevEui") + "/project/sensor/decod
    )

    return response

```

- Nachdem Sie den Code eingefügt haben, wählen Sie „**Bereitstellen**“, um den Lambda-Code bereitzustellen.
- Klicken Sie auf die Registerkarte „**Berechtigungen**“ der Lambda-Funktion.
- Ändern Sie die Berechtigung für die **Lambda-Rollenrichtlinie**.

- Klicken Sie unter „**Execution role**“ auf den Hyperlink unter „**Role name**“.
- Suchen Sie auf der **Registerkarte „Berechtigungen“** den Namen der Richtlinie und wählen Sie ihn aus.
- Wählen Sie „**Richtlinie bearbeiten**“ und dann die Registerkarte „**JSON**“.
- Fügen Sie Folgendes zum Abschnitt „Anweisung“ der Richtlinie hinzu, um die Veröffentlichung in AWS IoT zu ermöglichen.

```
{
    "Effect": "Allow",
    "Action": [
        "iot:Publish"
    ],
    "Ressource": [
        "*"
    ]
}
```

- Wählen Sie „**Richtlinie überprüfen**“ und dann „Änderungen speichern“.
- Kehren Sie zur Registerkarte „**Code**“ zurück und erstellen Sie ein Testereignis, mit dem Sie die Funktionalität der Lambda-Funktion testen können.
  - Wählen Sie im Dropdown-Menü „**Test**“ die Option „**Testereignisse konfigurieren**“
  - Geben Sie unter „**Event name**“ einen Namen für das Testereignis ein.
  - Fügen Sie die folgende Beispiel-Nutzlast in den Bereich unter „Ereignisname“ ein:

```
{
    "WirelessDeviceId": "65d128ab-90dd-4668-9556-fe47c589610b",
    "PayloadData": "AWf/1w==",
    "WirelessMetadata": {
        "LoRaWAN": {
            "DataRate": "4",
            "DevEui": "0000000000000088",
            "FPort": 1,
            "Frequency": "868100000",
            "Gateways": [
                {
                    "GatewayEui": "80029cffXXXXXXXXX", "Rssi": -109,
                    "Snr": 5
                }
            ],
            "Timestamp": "2021-02-08T04:00:40Z"
        }
    }
}
```

- Wählen Sie „**Speichern**“, um das Ereignis zu speichern.
- Navigieren Sie zur AWS IoT-Konsole, wählen Sie im Navigationsbereich „**Test**“ und dann „**MQTT-Testclient**“.
- Konfigurieren Sie den MQTT-Client so, dass er „#“ (alle Themen) abonniert.
- Klicken Sie auf der Seite „Lambda-Funktion“ auf „**Testen**“, um das soeben erstellte Testereignis zu generieren.
- Überprüfen Sie die veröffentlichten Daten im AWS IoT Core MQTT-Testclient:
  - Öffnen Sie ein weiteres Fenster. Gehen Sie zur **AWS IoT-Konsole**, wählen Sie unter „Subscription Topic“ die Option „**Test**“ aus, geben Sie „#“ ein und wählen Sie „**Thema abonnieren**“ aus.
  - Die Ausgabe sollte in etwa so aussehen:

09. Februar 2021, 14:45:29 Uhr  
(UTC+0800)

json

## Zielregel erstellen

Erstellen Sie in diesem Abschnitt die IoT-Regel, die die Geräte-Nutzlast an Ihre Anwendung weiterleitet. Diese Regel ist mit dem zuvor im Abschnitt „Einrichten eines Ziels für den Geräteverkehr“ erstellten Ziel verknüpft.

1. Navigieren Sie zur [AWS IoT-Konsole](#).
  2. Wählen Sie im Navigationsbereich „**Act**“ und dann „**Rules**“ aus.
  3. Wählen Sie auf der Seite „Rules“ die Option „**Create**“ aus.
  4. Geben Sie auf der Seite „**Regel erstellen**“ unter „Name“ den Namen „LoRaWANRouting“ ein. Geben Sie unter „**Beschreibung**“ eine Beschreibung Ihrer Wahl ein. Notieren Sie sich den Namen Ihrer Regel. Diese Informationen werden benötigt, wenn Sie Geräte für die Ausführung auf AWS IoT Core für LoRaWAN bereitstellen.
  5. Lassen Sie die Standardabfrage „Rule query statement: **SELECT \* FROM 'iot/topic'**“ unverändert. Diese Abfrage hat derzeit keine Auswirkungen, da der Datenverkehr derzeit basierend auf dem Ziel an die Regel-Engine weitergeleitet wird.
  6. Wählen Sie unter „**Eine oder mehrere Aktionen festlegen**“ die Option „Aktion hinzufügen“.
  7. Wählen Sie auf der Seite „Aktion auswählen“ die Option „**Nachricht erneut in einem AWS IoT-Thema veröffentlichen**“. Scrollen Sie nach unten und wählen Sie „**Aktion konfigurieren**“.
  8. Geben Sie auf der Seite „Aktion konfigurieren“ unter „Thema“ **project/sensor/decoded** ein. Die AWS IoT Rules Engine leitet Nachrichten an dieses Thema weiter.
  9. Wählen Sie unter „**Wählen oder erstellen Sie eine Rolle, um AWS IoT Zugriff für diese Aktion zu gewähren**“ die Option „**Rolle erstellen**“ aus.
  10. Geben Sie unter „Name“ einen Namen Ihrer Wahl ein.
  11. Wählen Sie „**Rolle erstellen**“, um die Erstellung der Rolle abzuschließen. Neben dem Rollennamen wird die Kennzeichnung „**Policy Attached**“ (Richtlinie **angehängt**) angezeigt, die darauf hinweist, dass die Rules Engine zur Ausführung der Aktion berechtigt ist.
  12. Wählen Sie „**Aktion hinzufügen**“.
  13. Fügen Sie eine weitere Aktion hinzu, um die Lambda-Funktion aufzurufen. Wählen Sie unter „**Eine oder mehrere Aktionen festlegen**“ die Option „**Aktion hinzufügen**“.
  14. Wählen Sie „**Nachricht an eine Lambda-Funktion senden**“.
  15. Wählen Sie „**Aktion konfigurieren**“.
  16. Wählen Sie die zuvor erstellte Lambda-Funktion aus und wählen Sie „**Aktion hinzufügen**“.
  17. Wählen Sie dann „**Regel erstellen**“.
  18. Oben im Fenster wird die Meldung „**Erfolgreich**“ angezeigt, und für das Ziel wurde eine Regel festgelegt.

Sie können nun überprüfen, ob die decodierten Daten empfangen und von AWS erneut veröffentlicht werden, indem Sie eine Bedingung oder ein Ereignis auf dem Gerät selbst auslösen.

- Wechseln Sie zur AWS IoT-Konsole. Wählen Sie im Navigationsbereich „Test“ und dann „MQTT-Client“ aus.
  - Abonnieren Sie das Platzhalterthema „#“, um Nachrichten aus allen Themen zu empfangen.
  - Senden Sie eine Nachricht von endDevice mit dem AT-Befehl `+send=1:01670110`.
  - Sie sollten einen Datenverkehr sehen, der dem unten gezeigten ähnelt.

json

```
393331375d387505/project/sensor/decoded
{
  "devEui": "393331375d387505",
  "fPort": 1,
  "freq": "867100000",
  "timestamp": "2021-02-09T06:47:20Z",
  "Temperatur": 27,2
}
```

09. Februar 2021, 14:47:21 (UTC+0800)

json

```
Projekt/Sensor/decoded      09. Februar 2021, 14:47:21 (UTC+0800)
{
  "WirelessDeviceID": "6477ec22-9570-31d5981da021",
  "PayloadData": "AWcBEA==",
  "WirelessMetadata": {
    "LoRaWAN": {
      "DataRate": "4",
      "DevEui": "393331375d387505", "FPort": 1,
      "Frequency": "867100000", "Gateways": [
        {
          "GatewayEui": "ac1ff09ffffe014bd5",
          "Rssi": -103,
          "Snr": 8,5
        }
      ],
      "Zeitstempel": "2021-02-09T06:47:20Z"
    }
  }
}
```

## Konfigurieren von Amazon SNS

Sie verwenden den Amazon Simple Notification Service, um Textnachrichten (SMS) zu versenden, wenn bestimmte Bedingungen erfüllt sind.

1. Rufen Sie die [Amazon SNS-Konsole](#) unter  auf.
2. Klicken Sie auf das Menü in der linken Ecke, um den Navigationsbereich zu öffnen.
3. Wählen Sie „**Textnachrichten (SMS)**“ und dann „**Textnachricht veröffentlichen**“.
4. Wählen Sie unter „Nachrichtentyp“ die Option „**Werbung**“ aus.
5. Geben Sie Ihre Telefonnummer ein (die Telefonnummer, an die Textbenachrichtigungen gesendet werden sollen).
6. Geben Sie „Testnachricht“ als Nachricht ein und wählen Sie „Nachricht **veröffentlichen**“.
7. Wenn die eingegebene Telefonnummer gültig ist, erhalten Sie eine Textnachricht und Ihre Telefonnummer wird bestätigt.
8. Erstellen Sie wie folgt ein Amazon SNS-Thema:
  - o Wählen Sie im Navigationsbereich „Themen“.
  - o Wählen Sie „Thema erstellen“.
  - o Wählen Sie unter „Details“ die Option „Standard“.
  - o Geben Sie einen Namen Ihrer Wahl ein. Hier verwenden Sie „text\_topic“.
  - o Wählen Sie „Thema erstellen“.
9. Erstellen Sie ein Abonnement für dieses Thema:
  - o Wählen Sie auf der Seite für das neu erstellte Thema „text\_topic“ die Registerkarte „**Abonnements**“.

- Wählen Sie „**Abonnement erstellen**“.
- Wählen Sie unter „**Thema ARN**“ das zuvor erstellte Thema aus.
- Wählen Sie im Dropdown-Menü „**Protokoll**“ die Option „SMS“ aus.
- Geben Sie unter „Endpunkt“ die zuvor validierte Telefonnummer ein, an die die SMS-Benachrichtigungen gesendet werden sollen.
- Wählen Sie „Abonnement erstellen“. Es sollte die Meldung „**Abonnement für text\_topic erfolgreich erstellt**“ angezeigt werden.

## Regel für Amazon SNS-Benachrichtigung hinzufügen

Fügen Sie nun eine neue Regel hinzu, um eine Amazon SNS-Benachrichtigung zu senden, wenn bestimmte Bedingungen in einer decodierten Nachricht erfüllt sind.

1. Navigieren Sie zur [AWS IoT-Konsole](#).
2. Wählen Sie im Navigationsbereich „**Act**“ (Handeln). Wählen Sie dann „**Rules**“ (**Regeln**).
3. Wählen Sie auf der Seite „Regeln“ die Option „**Erstellen**“.
4. Geben Sie als Namen „*text\_alert*“ ein und geben Sie eine geeignete Beschreibung ein.
5. Geben Sie unter „**Rule query statement**“ die folgende Abfrage ein:

```
SELECT devEui als device_id, „Temperatur Über 25“ als Meldung, Temperatur als temp, Zeitstempel
```

6. Wählen Sie unter „Eine oder mehrere Aktionen festlegen“ die Option „**Aktion hinzufügen**“
7. Wählen Sie „**Nachricht als SNS-Push-Benachrichtigung senden**“.
8. Wählen Sie „**Aktion konfigurieren**“.
9. Wählen Sie unter „**SNS-Ziel**“ aus der Dropdown-Liste „*text\_topic*“ aus.
10. Wählen Sie unter „**Nachrichtenformat**“ die Option „**RAW**“ aus.
11. Wählen Sie unter „**Wählen oder erstellen Sie eine Rolle, um AWS IoT Zugriff für diese Aktion zu gewähren**“ die Option „**Rolle erstellen**“ aus.
12. Geben Sie einen Namen für die Rolle ein und wählen Sie „**Aktion hinzufügen**“.
13. Wählen Sie „**Regel erstellen**“. Es sollte eine Meldung „**Erfolgreich**“ angezeigt werden, die angibt, dass die Regel erstellt wurde.

## Testen Sie die Regel für Amazon SNS-Benachrichtigungen

Nachdem Sie die Regel für die Amazon SNS-Benachrichtigung hinzugefügt haben, sollten Sie beim Auslösen des Ereignisses eine Textnachricht erhalten.

Senden Sie eine Nachricht von endDevice mit dem AT-Befehl: nach dem Senden einer Uplink-Nachricht.

```
{
  „device_id“: „393331375d387505“,
  „message“: „Temperatur Über 25“, „temp“:
  27,2,
  „time“: „2021-02-22T07:58:54Z“
}
```

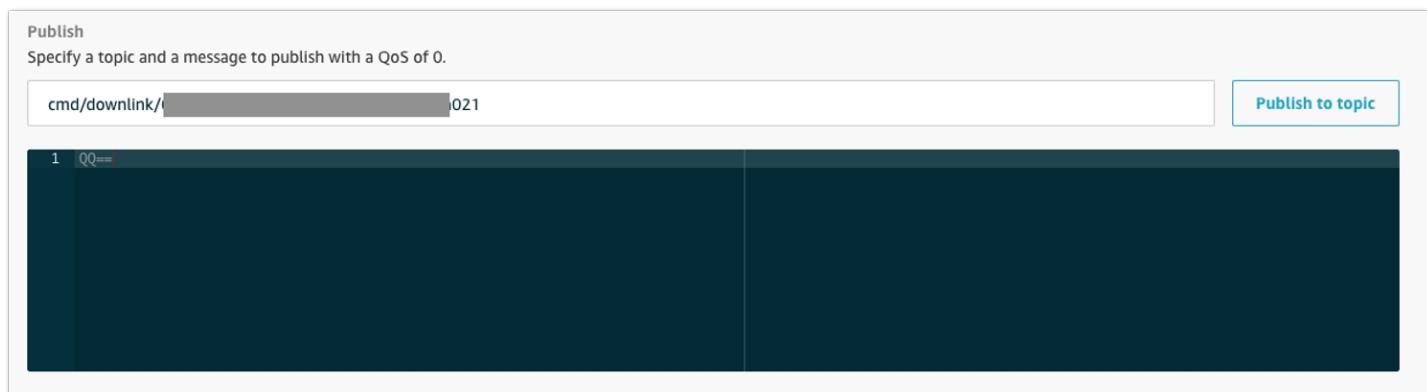
json

## Downlink-Nutzlast senden

In diesem Abschnitt wird gezeigt, wie Sie Downlink-Nutzdaten vom AWS IoT LoRaWAN Server an das Endgerät senden.

1. Installieren Sie die [AWS SAM CLI](#).
2. Stellen Sie [die SAM-Vorlage auf AWS](#) bereit.
3. Senden Sie die Nutzlast an das Endgerät.
  - Rufen Sie die AWS IoT-Konsole auf.
  - Wählen Sie im Navigationsbereich „**Test**“ und dann „**MQTT-Client**“.

- Abonnieren Sie das Platzhalterthema „#“, um Nachrichten aus allen Themen zu empfangen.
- Geben Sie das Thema „**cmd/downlink/{WirelessDeviceId}**“ und eine Base64-codierte Nachricht an.



**Abbildung 19:** Festlegen eines Themas

4. Sie sollten einen ähnlichen Datenverkehr auf AWS sehen, wie unten gezeigt:

```

downlink/status/6477ec22-9570-4fea-9668-31d5981da021      09. Februar 2021, 15:09:29 (UTC+08)
{
    "sendresult": {
        "status": 200,
        "RequestId": "4f1d36e1-8316-4436-8e9d-2207e3711755", "MessageId": "60223529-0011d9f5-0095-0008",
        "ParameterTrace": { "PayloadData": "QQ==",
            "WirelessDeviceId": "6477ec22-9570-4fea-9668-31d5981da021",
            "Fport": 1,
            "TransmitMode": 1
        }
    }
}

```

```

downlink/status/6477ec22-9570-4fea-9668-31... February 09, 2021, 15:09:29 (UTC+0800) Export Hide
{
    "sendresult": {
        "status": 200,
        "RequestId": "4f1d36e1-8316-4436-8e9d-2207e3711755",
        "MessageId": "60223529-0011d9f5-0095-0008",
        "ParameterTrace": {
            "PayloadData": "QQ==",
            "WirelessDeviceId": "6477ec22-9570-4fea-9668-31d5981da021",
            "Fport": 1,
            "TransmitMode": 1
        }
    }
}

cmd/downlink/6477ec22-9570-4fea-9668-31d... February 09, 2021, 15:09:29 (UTC+0800) Export Hide
We cannot display the message as JSON, and are instead displaying it as UTF-8 String.
QQ==

```

**Abbildung 20:** Datenverkehr auf AWS

5. Auf Ihrer Konsole des Endgeräts sollte ein ähnlicher Datenverkehr wie unten dargestellt zu sehen sein.

```

SYSLOG:4:LoRa rx : 41 - 14
SYSLOG:4:LoRa Tx :

```

## IoT Analytics

Sie verwenden IoT Analytics, um Daten visuell über Grafiken darzustellen, falls in Zukunft weitere Analysen erforderlich sein sollten.

## Erstellen Sie eine IoT Analytics-Regel

### Erstellen Sie zunächst eine Regel

1. Navigieren Sie zur [AWS IoT-Konsole](#).
2. Wählen Sie im Navigationsbereich „Act“ und dann „Rules“ aus.
3. Wählen Sie auf der Seite „Rules“ die Option „Create“.
4. Geben Sie den Namen „Visualize“ ein und geben Sie eine passende Beschreibung ein.
5. Geben Sie unter der Regelabfrageanweisung die folgende Abfrage ein:

```
SELECT * FROM 'project/sensor/decoded'
```

6. Wählen Sie „Aktion hinzufügen“.
7. Wählen Sie „Nachricht an IoT Analytics senden“.
8. Wählen Sie „Aktion konfigurieren“.
9. Wählen Sie „IoT Analytics-Ressourcen schnell erstellen“.
10. Geben Sie unter „Ressourcenpräfix“ ein geeignetes Präfix für Ihre Ressourcen ein, z. B. „LoRa“.
11. Wählen Sie „Schnell erstellen“.
12. Sobald die Meldung „Schnell erstellen abgeschlossen“ angezeigt wird, wählen Sie „Aktion hinzufügen“.
13. Wählen Sie „Regel erstellen“. Es sollte eine Erfolgsmeldung angezeigt werden, die angibt, dass die Regel erstellt wurde.

## AWS IoT Analytics konfigurieren

### AWS IoT Analytics einrichten

1. Rufen Sie die [AWS IoT Analytics-Konsole](#) unter  auf.
2. Wählen Sie im Navigationsbereich „Datensätze“ aus.
3. Wählen Sie den Datensatz aus, der mit der Schnell-Erstellung in „IoT Analytics-Regel erstellen“ generiert wurde.
4. Bearbeiten Sie im Abschnitt „Details“ die **SQL-Abfrage**.
5. Ersetzen Sie die Abfrage durch Folgendes:

```
SELECT devEui als device_id, temperature als temp, timestamp als time FROM LoRa_datastore
```

6. Wählen Sie unter „Zeitplan“ die Option „Zeitplan hinzufügen“.
7. Wählen Sie unter „Frequency“ (Häufigkeit) die Option „Every 1 minute“ (Alle 1 Minute) und klicken Sie dann auf „Save“ (Speichern).

## Amazon QuickSight konfigurieren

Mit Amazon QuickSight können Sie auf einfache Weise interaktive BI-Dashboards erstellen und veröffentlichen, die maschinell lernbasierte Erkenntnisse enthalten.

1. Rufen Sie die [AWS-Verwaltungskonsole](#) unter  auf.
2. Geben Sie in der Managementkonsole „QuickSight“ in das Suchfeld „Search for services, features...“ (Nach Diensten, Funktionen suchen...) ein.
3. Klicken Sie in den Suchergebnissen auf QuickSight.
4. Wenn Sie sich noch nicht für den Dienst angemeldet haben, melden Sie sich jetzt an, da es eine kostenlose Testphase gibt.
5. Wählen Sie die **Standard Edition** aus und klicken Sie auf „Weiter“.
6. Geben Sie einen eindeutigen Namen in das Feld „QuickSight-Kontoname“ ein.
7. Geben Sie die E-Mail-Adresse für Benachrichtigungen ein.
8. Überprüfen Sie die anderen Kontrollkästchenoptionen und ändern Sie sie bei Bedarf. Die Option „AWS IoT Analytics“ muss ausgewählt sein.
9. Wählen Sie „Fertigstellen“. Es wird eine Bestätigungsmeldung angezeigt.

10. Wählen Sie „**Zu Amazon QuickSight wechseln**“.
11. Wählen Sie „**Datensätze**“.
12. Wählen Sie „**Neuer Datensatz**“.
13. Wählen Sie „**AWS IoT Analytics**“.
14. Wählen Sie unter „Wählen Sie einen AWS IoT Analytics-Datensatz zum Importieren aus“ den Datensatz aus, den Sie unter „**Erstellen einer IoT Analytics-Regel**“ erstellt haben.
15. Wählen Sie „**Datenquelle erstellen**“ und dann „**Visualisieren**“.
16. Wählen Sie den erstellten Datensatz aus und wählen Sie dann „**Aktualisieren**“ oder „**Aktualisierung planen**“, um den Datensatz regelmäßig zu aktualisieren.

## Fehlerbehebung

Wenn Probleme auftreten, können Sie die Protokolle im Verzeichnis /var/log/ überprüfen.

## Fehlerbehebung

1. Die Webanmeldung wird nicht angezeigt:
  - Überprüfen Sie, ob Ihre WLAN-Verbindung mit **RAKWireless\_XXXX** verbunden ist.
  - Versuchen Sie, **192.168.230.1** anzupingen.

## The Things Network v3 (TTNv3)

In diesem Abschnitt wird gezeigt, wie Sie RAK7268 WisGate Edge Lite 2 mit TTNv3 verbinden.

Um sich bei TTNv3 anzumelden, gehen [Sie auf](#) . Wenn Sie bereits ein TTN-Konto haben, können Sie sich mit Ihren The Things ID-Anmeldedaten anmelden.

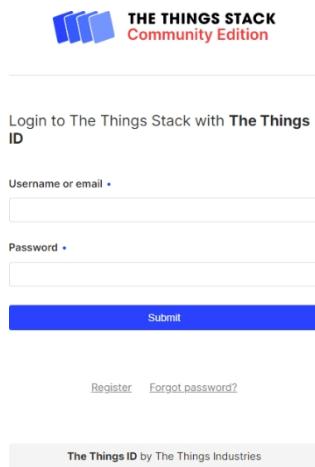


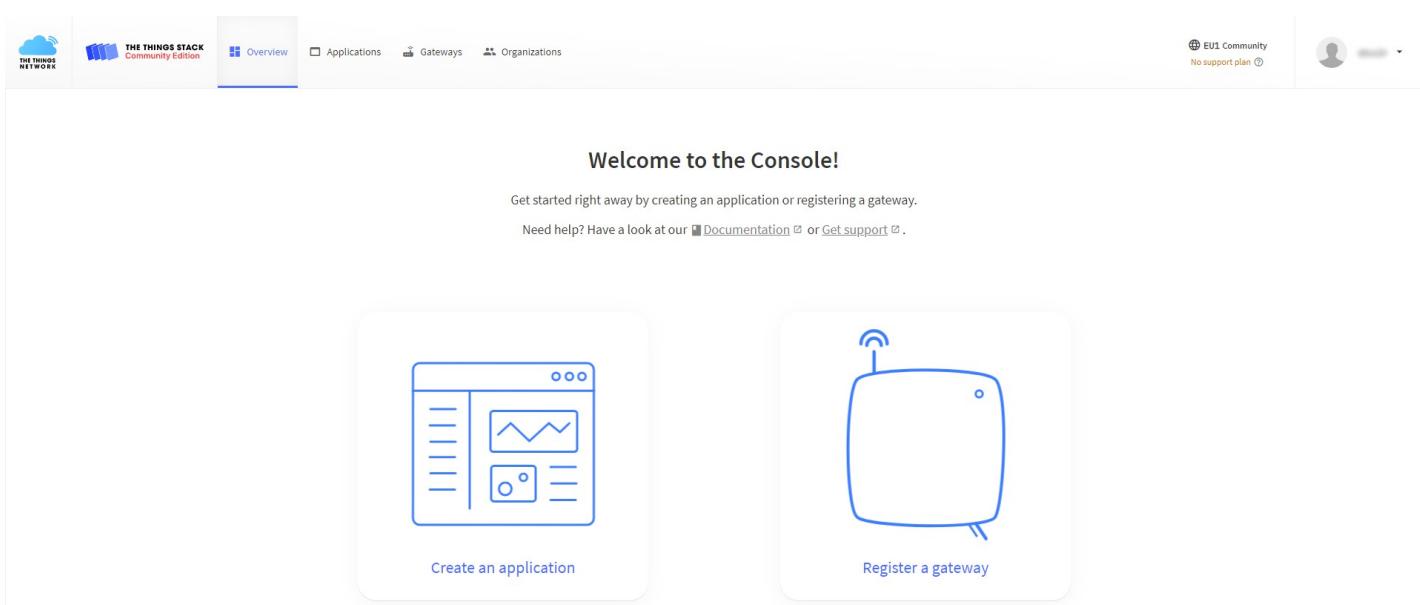
Abbildung 21: Startseite von The Things Stack

### HINWEIS

Dieses Tutorial gilt für das Frequenzband EU868.

## Registrieren des Gateways

1. Um ein kommerzielles Gateway zu registrieren, wählen Sie „**Gateway registrieren**“ (für neue Benutzer, die noch kein Gateway registriert haben) oder gehen Sie zu „**Gateways**“ > „**+ Gateway hinzufügen**“ (für Benutzer, die bereits Gateways registriert haben).



**Abbildung 22:** Konsolenseite nach erfolgreicher Anmeldung

## 2. Geben Sie die erforderlichen Informationen ein:

- **Eigentümer** – Wird automatisch von The Things Stack basierend auf Ihrem Konto oder der von Ihnen erstellten Organisation ausgefüllt.
- **Gateway-ID** – Dies ist die eindeutige ID Ihres Gateways im Netzwerk. Beachten Sie, dass die ID nur Kleinbuchstaben, Zahlen und Bindestriche (-) enthalten darf.
- **Gateway-EUI** – Eine 64-Bit-erweiterte eindeutige Kennung für Ihr Gateway. Die EUI des Gateways finden Sie entweder auf dem Aufkleber auf dem Gehäuse oder auf der Seite „**„LoRa-Netzwerkeinstellungen“** im LoRa-Gateway-Menü, auf das Sie über die Web-Benutzeroberfläche zugreifen können. Anweisungen zum Zugriff auf Ihr Gateway über die Web-Benutzeroberfläche finden Sie in der [Schnellstartanleitung des Produkts unter](#).
- **Gateway-Name** – Ein Name für Ihr Gateway.
- **Gateway-Beschreibung (optional)** – Optionale Beschreibung des Gateways; kann auch zum Speichern von Notizen zum Gateway verwendet werden.
- **Gateway-Serveradresse** – Die Adresse des Gateway-Servers, mit dem eine Verbindung hergestellt werden soll.

### HINWEIS

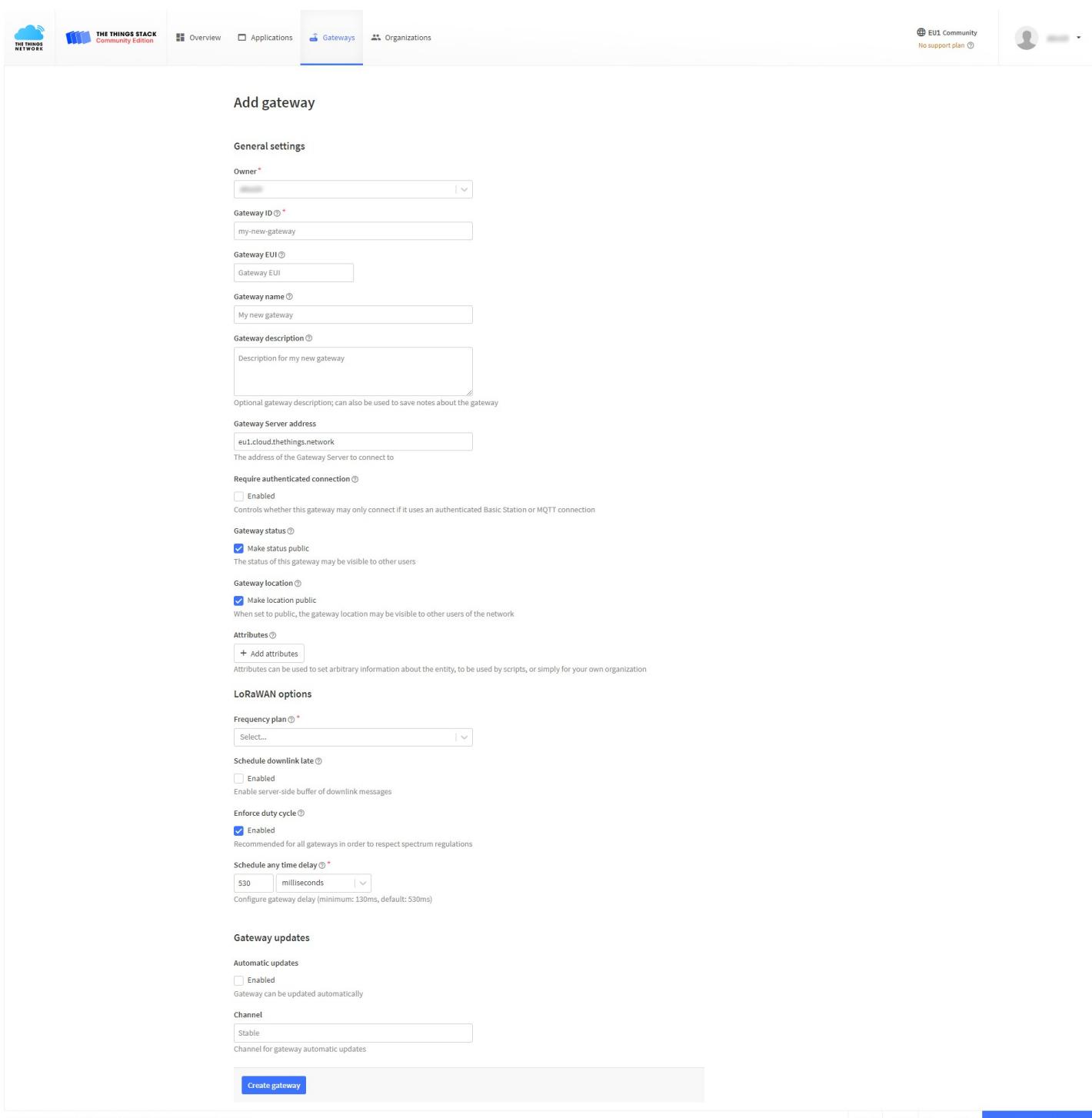
Dieses Tutorial basiert auf der Verwendung des EU868-Frequenzbands, daher lautet die Serveradresse: eu1.cloud.thethings.network.

- **Frequenzplan** – Der vom Gateway verwendete Frequenzplan.

### HINWEIS

Für dieses Tutorial verwenden wir Europa 863-870 MHz (SF12 für RX2 – empfohlen).

- Die anderen Einstellungen sind optional und können entsprechend Ihren Anforderungen geändert werden.



The screenshot shows the 'Add gateway' page in The Things Stack. It includes sections for General settings, LoRaWAN options, and Gateway updates. The General settings section contains fields for Owner, Gateway ID, Gateway EUI, Gateway name, and Gateway description. The LoRaWAN options section includes Frequency plan, Schedule downlink late, Enforce duty cycle, and Schedule any time delay. The Gateway updates section includes Automatic updates and Channel. A 'Create gateway' button is at the bottom.

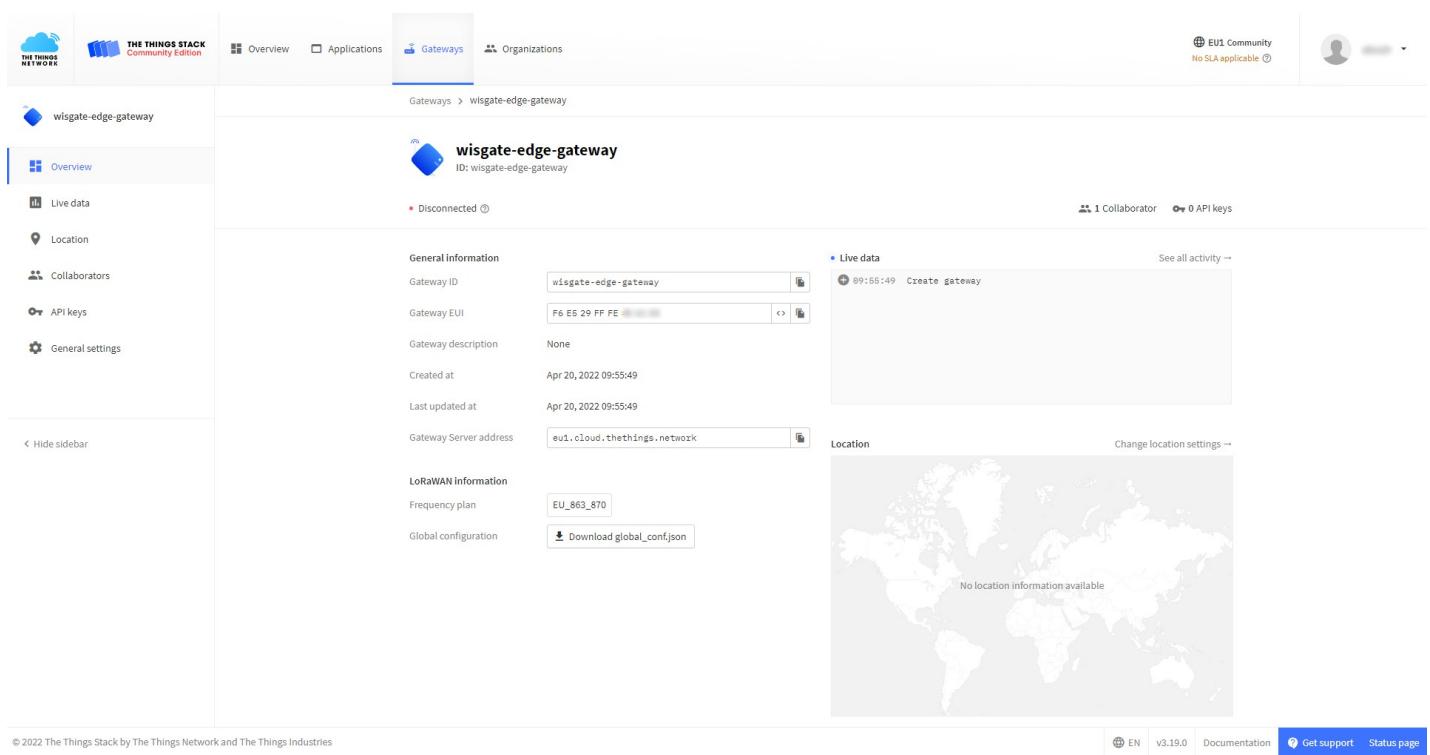
**Abbildung 23:** Hinzufügen eines Gateways

3. Um Ihr Gateway zu registrieren, scrollen Sie nach unten und klicken Sie auf „**Gateway erstellen**“.

TTNv3 unterstützt die TLS-Serverauthentifizierung und das Client-Token, für das eine Vertrauensdatei und eine Schlüsseldatei erforderlich sind, um das Gateway für die erfolgreiche Verbindung mit dem Netzwerk zu konfigurieren.

## Generieren des Tokens

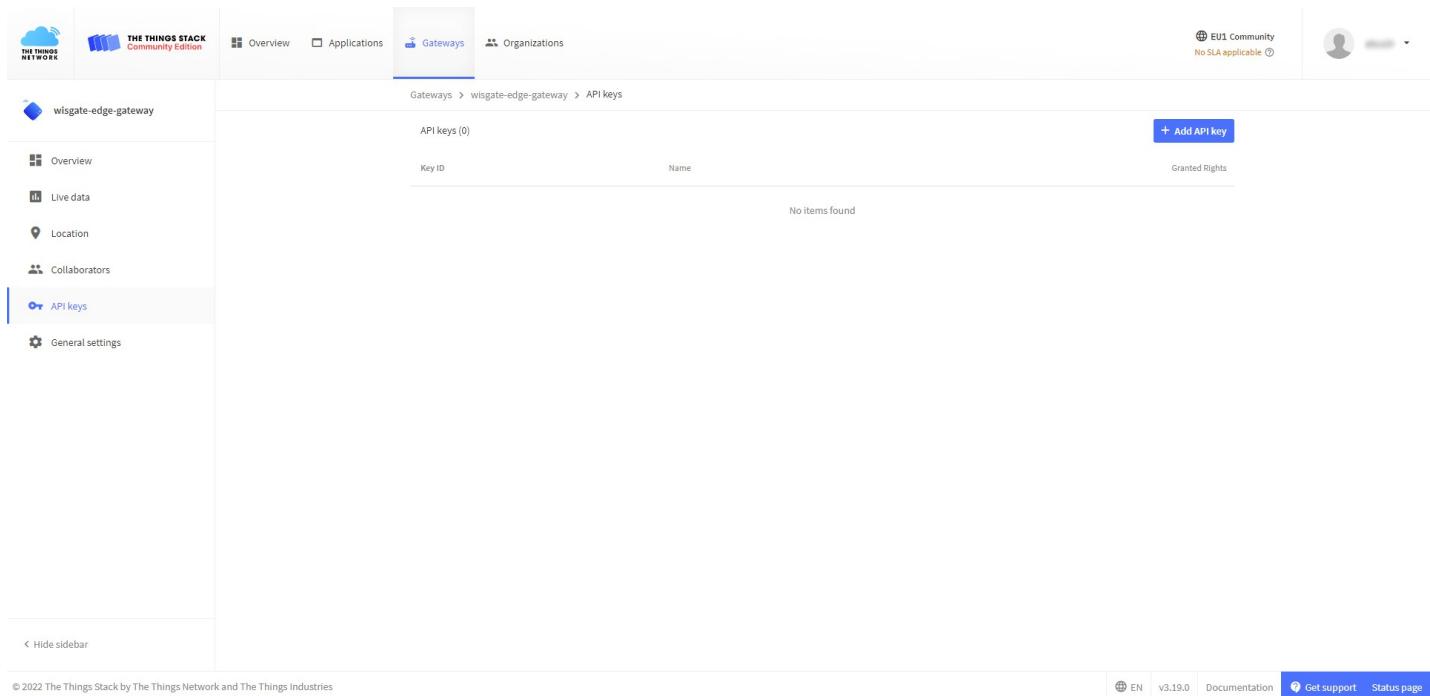
- Um eine Schlüsseldatei zu generieren, navigieren Sie auf der **Übersichtsseite** des registrierten Gateways zu **API-Schlüssel**.



The screenshot shows the 'Overview' tab for the 'wisgate-edge-gateway' in The Things Stack. The sidebar on the left includes links for Overview, Live data, Location, Collaborators, API keys, and General settings. The main content area displays the gateway's ID ('wisgate-edge-gateway'), EUI ('F6 EB 29 FF FE'), and description ('None'). It also shows the creation date ('Apr 20, 2022 09:55:49') and last update ('Apr 20, 2022 09:55:49'). The 'LoRaWAN information' section includes a frequency plan ('EU\_863\_870') and a link to download 'global\_conf.json'. A world map indicates 'No location information available'. The top right corner shows EU1 Community status and a user profile icon.

Abbildung 24: Übersichtsseite

2. Wählen Sie auf der Seite „API-Schlüssel“ die Option „+ API-Schlüssel hinzufügen“.

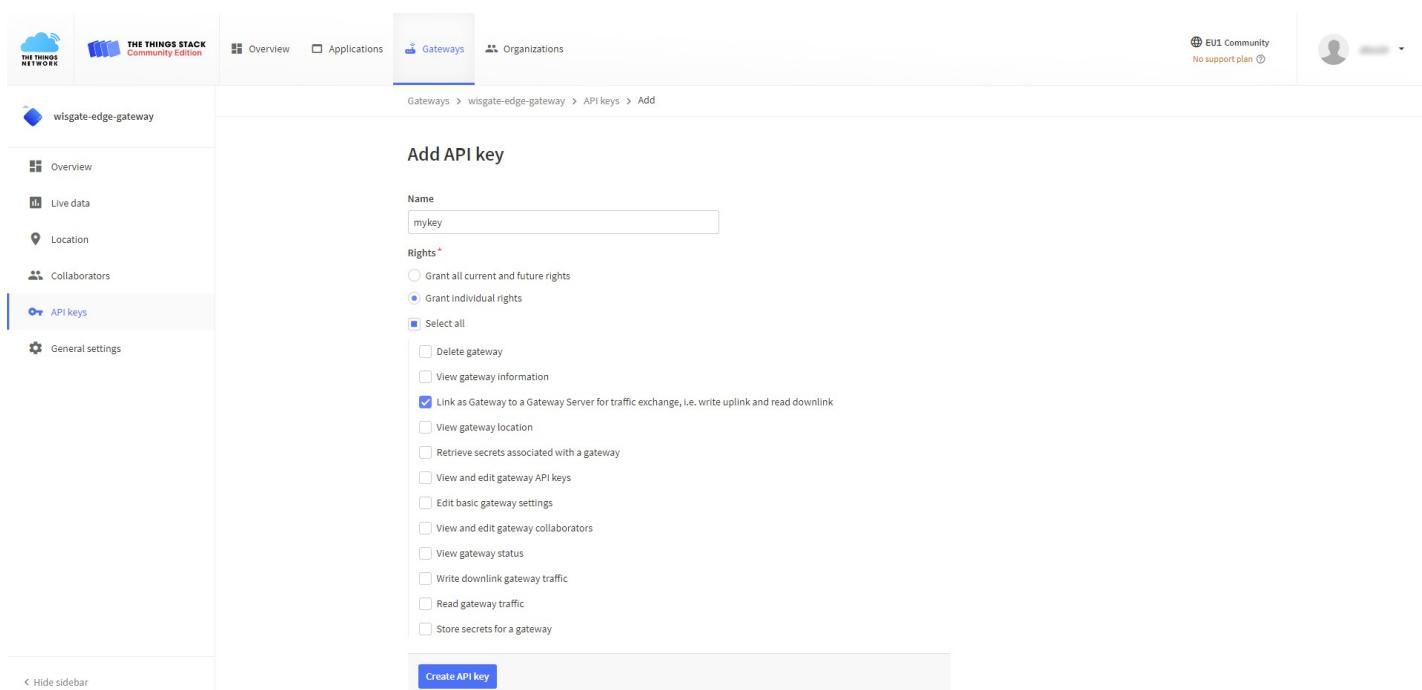


The screenshot shows the 'API keys' page for the 'wisgate-edge-gateway'. The sidebar on the left includes links for Overview, Live data, Location, Collaborators, API keys (which is selected), and General settings. The main content area shows a table with one row ('No items found') and a blue '+ Add API key' button. The top right corner shows EU1 Community status and a user profile icon.

Abbildung 25: Seite „API-Schlüssel“

3. Geben Sie im Feld „Name“ den Namen Ihres Schlüssels ein (z. B. „mykey“). Wählen Sie „Individuelle Rechte gewähren“ und wählen Sie

**Als Gateway mit einem Gateway für den Datenaustausch verknüpfen, d. h. Uplink lesen und Downlink schreiben.**



The screenshot shows the 'Add API key' page in The Things Stack. The sidebar on the left is titled 'wsgate-edge-gateway' and includes links for Overview, Live data, Location, Collaborators, API keys (which is the current page), and General settings. The main content area has a title 'Add API key' and a form. In the 'Name' field, 'mykey' is entered. Under 'Rights\*', there are several checkboxes: 'Grant all current and future rights' (radio button), 'Grant individual rights' (radio button selected), 'Select all' (checkbox checked), and numerous other gateway-related permissions like 'Delete gateway', 'View gateway information', 'Link as Gateway to a Gateway Server for traffic exchange, i.e. write uplink and read downlink' (checkbox checked), etc. A 'Create API key' button is at the bottom.

**Abbildung 26:** Generieren eines API-Schlüssels

- Um den Schlüssel zu generieren, wählen Sie **API-Schlüssel erstellen**. Das folgende Fenster wird angezeigt, in dem Sie aufgefordert werden, den soeben generierten Schlüssel zu kopieren.

#### Please copy newly created API key

You won't be able to view the key afterward

##### Granted rights

- ✓ Link as Gateway to a Gateway Server for traffic exchange, i.e. write uplink and read downlink

Your API key has been created successfully. Note: After closing this window, the value of the key secret will not be accessible anymore. Make sure to copy and store it in a safe place now.

##### API key

.....  

 I have copied the key

**Abbildung 27:** Kopieren des generierten Schlüssels

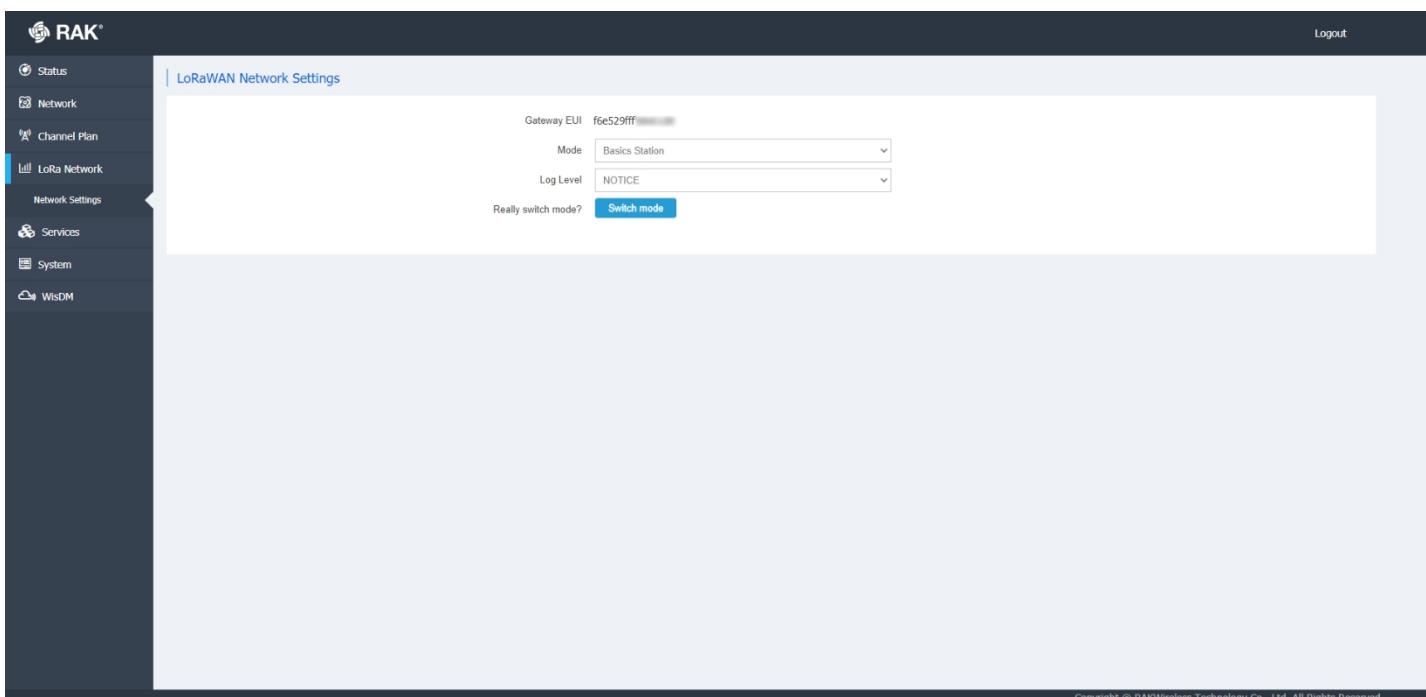
#### WARNUNG

Kopieren Sie den Schlüssel und speichern Sie ihn in einer .txt-Datei (oder einer anderen Datei), da Sie Ihren Schlüssel danach nicht mehr anzeigen oder kopieren können.

- Klicken Sie auf „Ich habe den Schlüssel kopiert“, um fortzufahren.

## Konfigurieren des Gateways

- Um den Gateway-Zugang zu konfigurieren, rufen Sie ihn über die Web-Benutzeroberfläche auf. Wie das geht, erfahren Sie in der zuvor erwähnten [Schnellstartanleitung](#) des Geräts unter .
- Navigieren Sie zu **LoRa-Netzwerk > Netzwerkeinstellungen** > Dropdown-Menü „Modus“ > wählen Sie „Basics Station“.



**Abbildung 28:** Ändern des Arbeitsmodus

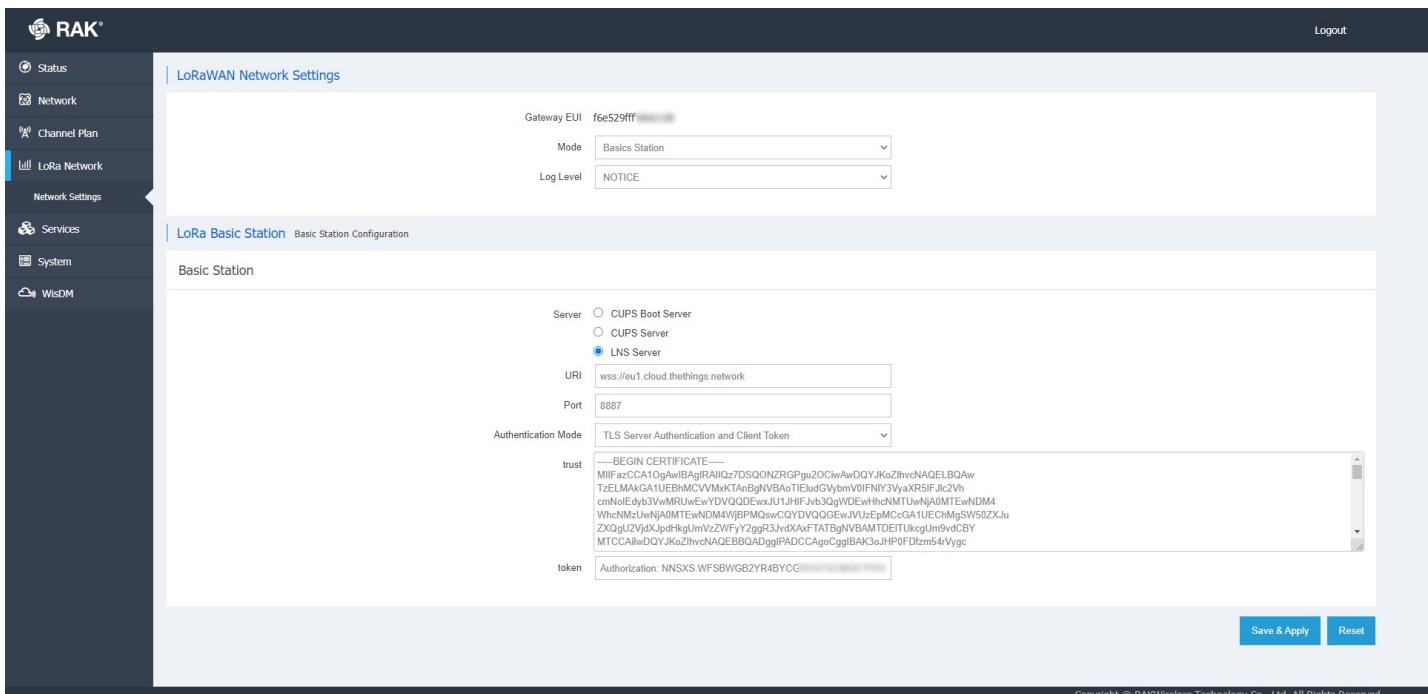
3. Wählen Sie „**Modus wechseln**“, um die Änderung zu übernehmen. Danach werden die Einstellungen im Bereich „**Basics Station Configuration**“ angezeigt. Um das Gateway mit TTNv3 zu verbinden, müssen die folgenden Parameter konfiguriert werden:

- **Server** – Wählen Sie als Server „**LNS Server**“.
- **URI** – Dies ist der Link zum The Things Stack-Server. Beachten Sie, dass wir für dieses Tutorial das Gateway mit dem europäischen Cluster verbinden. Für Europa geben Sie Folgendes ein: wss://eu1.cloud.thethings.network
- **Port** – Der LNS-Server verwendet Port 8887. Geben Sie **8887** ein.
- **Authentifizierungsmodus** – Wählen Sie **TLS-Serverauthentifizierung und Client-Token**. Nach der Auswahl werden die Felder „Vertrauen“ und „Token“ angezeigt.
- **Vertrauen** – Für das Vertrauen verwenden wir das **Let's Encrypt ISRG ROOT X1** Trust-Zertifikat. Die Datei mit dem Zertifikat finden Sie [hier](#).
- **Token** – Dies ist der generierte **API-Schlüssel**. Der Schlüssel muss mit „**Authorization:**“ beginnen. Beispiel:

```
Authorization: IHR_API_SCHLÜSSEL
```

#### HINWEIS

Ersetzen Sie **IHR\_API\_SCHLÜSSEL** durch den zuvor generierten Schlüssel. Beachten Sie, dass zwischen „**Authorization:**“ und **IHR\_API\_SCHLÜSSEL** ein Leerzeichen stehen muss, wie im Beispiel gezeigt.

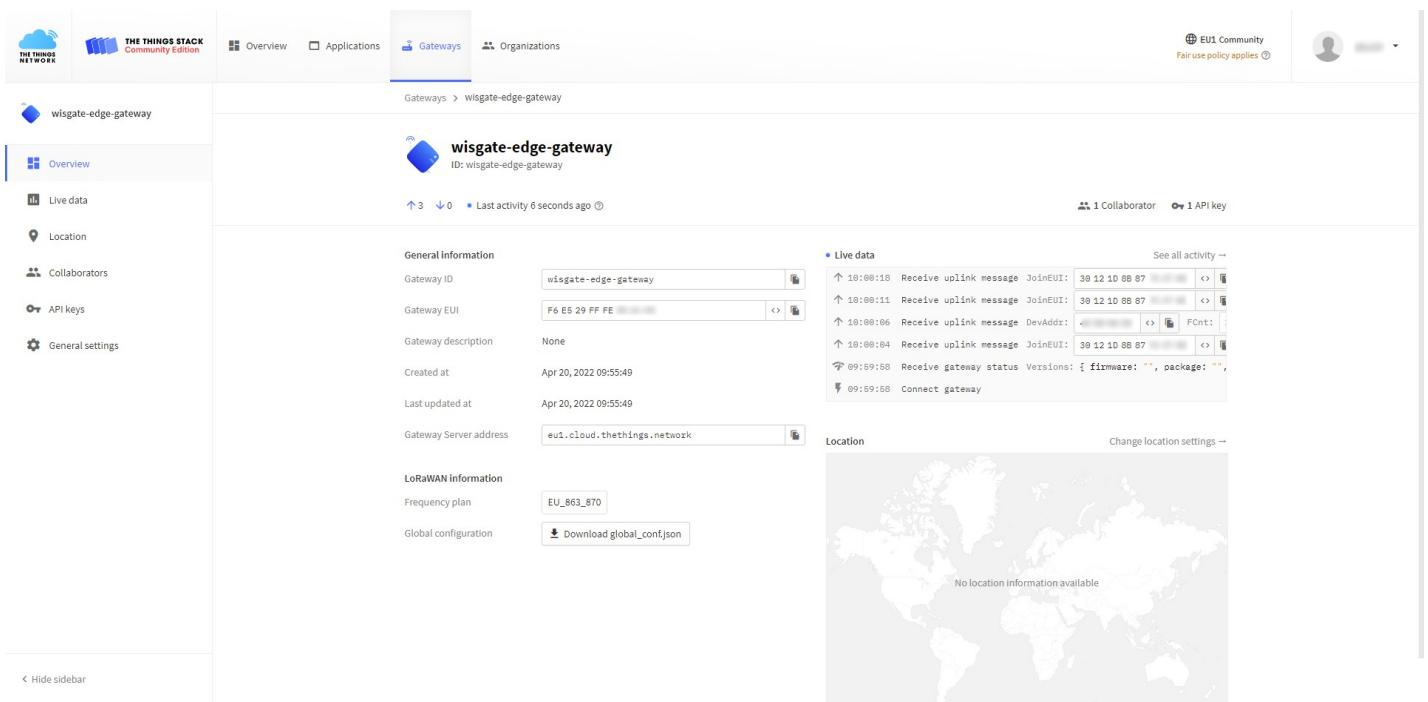


The screenshot shows the RAK LoRaWAN Network Settings interface. On the left sidebar, under 'LoRa Network', 'Network Settings' is selected. The main panel displays 'LoRa Basic Station' configuration. Under 'Basic Station', the 'Mode' is set to 'Basics Station' and 'Log Level' is set to 'NOTICE'. In the 'Server' section, 'LNS Server' is selected. The 'URI' is set to 'wss://eu1.cloud.thethings.network', 'Port' is 8887, and 'Authentication Mode' is 'TLS Server Authentication and Client Token'. A large text area contains a certificate snippet starting with '-----BEGIN CERTIFICATE-----'. At the bottom right are 'Save & Apply' and 'Reset' buttons.

**Abbildung 29:** LoRa-Grundlagen Stationseinstellungen

#### 4. Um die Änderungen zu speichern, klicken Sie auf „Speichern und anwenden“.

Sie können nun sehen, dass Ihr Gateway als Basics Station mit TTNv3 verbunden ist:



The screenshot shows the The Things Stack interface. The top navigation bar includes 'THE THINGS NETWORK', 'THE THINGS STACK Community Edition', 'Overview', 'Applications', 'Gateways', 'Organizations', and 'EUI1 Community Fair use policy applies'. The sidebar on the left lists 'wisgate-edge-gateway' with sub-options: 'Overview', 'Live data', 'Location', 'Collaborators', 'API keys', and 'General settings'. The main content area shows 'wisgate-edge-gateway' with ID 'wisgate-edge-gateway'. It displays 'Last activity 6 seconds ago'. The 'General Information' section shows 'Gateway ID: wisgate-edge-gateway', 'Gateway EUI: F6 E5 29 FF FE', 'Gateway description: None', 'Created at: Apr 20, 2022 09:55:49', and 'Last updated at: Apr 20, 2022 09:55:49'. The 'LoRaWAN Information' section shows 'Frequency plan: EU\_863\_870' and 'Global configuration: Download global\_conf.json'. To the right, there is a 'Live data' section with a list of recent events and a 'Location' map showing 'No location information available'.

**Abbildung 30:** Erfolgreiche Verbindung

## LORIOT

In diesem Tutorial erfahren Sie, wie Sie RAK7268 WisGate Edge Lite 2 mit LORIOT verbinden.

LORIOT bietet eine benutzerfreundliche Softwareplattform, mit der Sie ein sicheres IoT-Netzwerk aufbauen, betreiben und skalieren können, das sich für den Einsatz von IoT-Lösungen mit großer Reichweite in allen Teilen der Welt eignet.

## Voraussetzungen

### Hardware

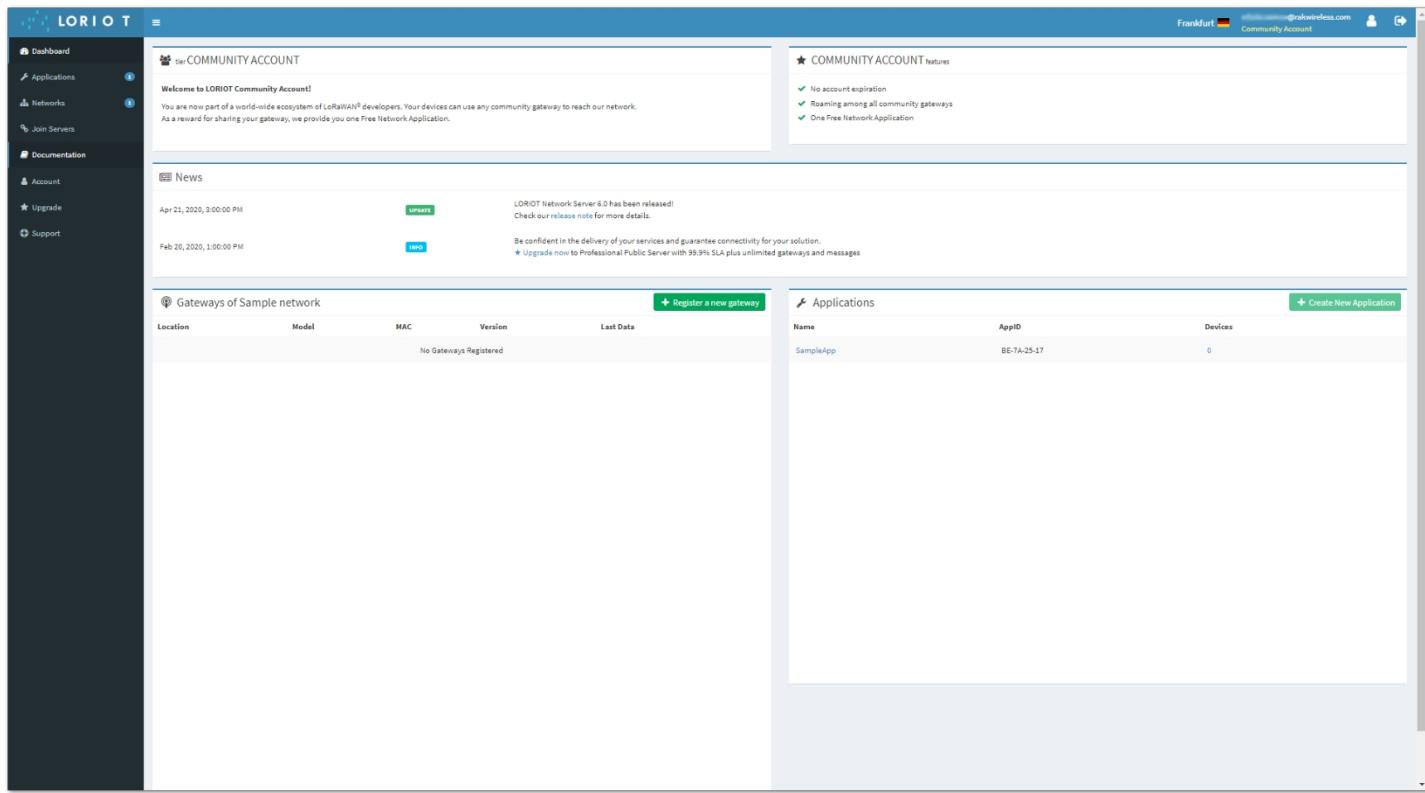
- RAK7268 WisGate Edge Lite 2

### Software

- SSH-Client (Dieses Tutorial wird mit [PuTTY](#) durchgeführt.)
- [LORIOT-Konto](#)

## Registrieren des Gateways

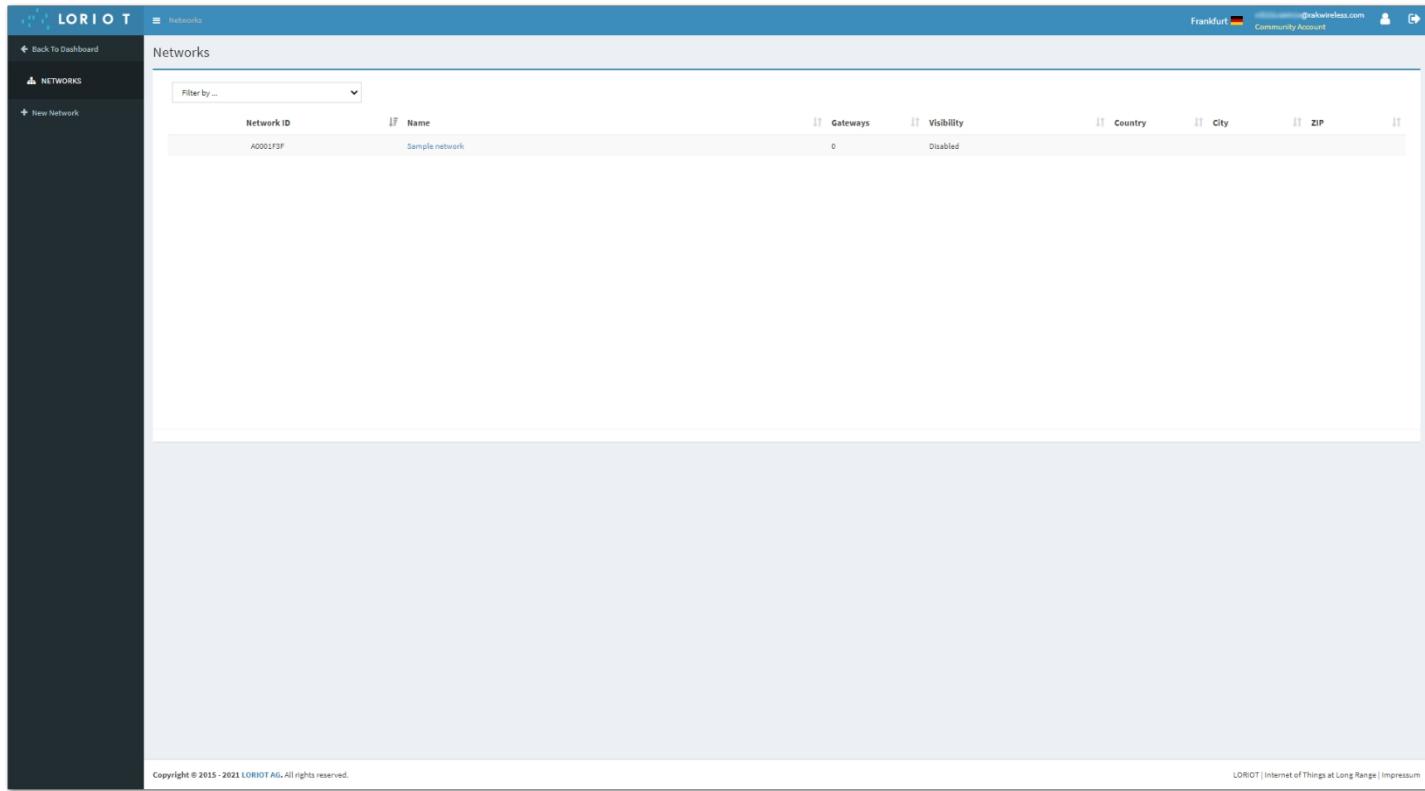
1. Melden Sie sich bei Ihrem LORIOT-Konto an.



The screenshot shows the LORIOT Community Account dashboard. On the left, a sidebar menu includes: Dashboard, Applications, Networks, Join Servers, Documentation, Account, Upgrade, and Support. The main content area has several sections: 'Welcome to LORIOT Community Account!', 'News' (with two entries: 'Apr 21, 2020, 9:00:00 PM' and 'Feb 20, 2020, 1:00:00 PM'), 'Gateways of Sample network' (empty), and 'Applications' (listing 'SampleApp' with AppID BE-7A-25-17). A top bar shows 'Frankfurt' and 'Community Account'.

Abbildung 31: LORIOT-Startseite

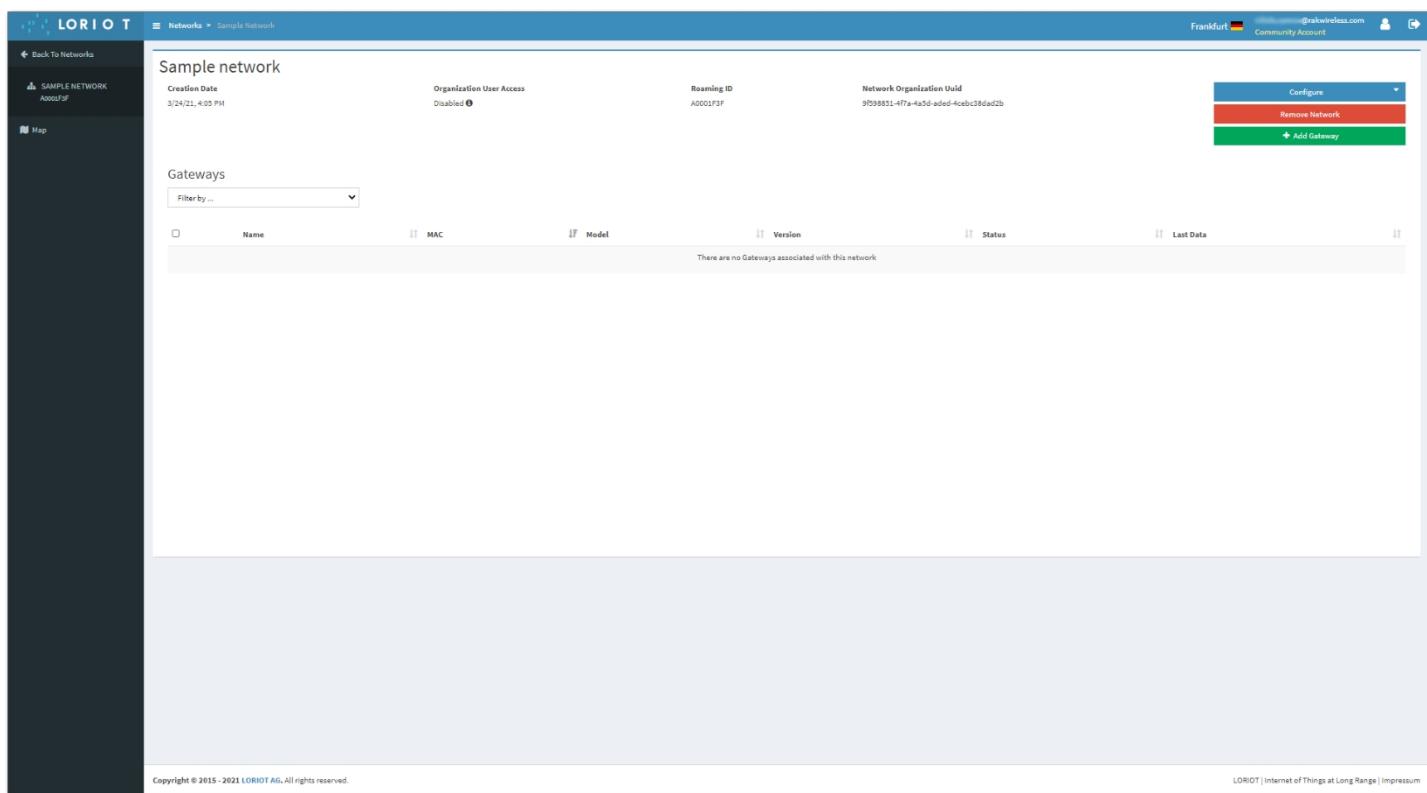
2. Gehen Sie zur Registerkarte „Netzwerke“ im Hauptmenü auf der linken Seite. Sie haben die Möglichkeit, **das einfache Netzwerk** auszuwählen, das automatisch bei der Erstellung Ihres Kontos generiert wird, oder Sie können ein neues Netzwerk erstellen. Für Anfänger ist es einfacher, **das einfache Netzwerk** zu verwenden.



The screenshot shows the 'Networks' list page. The sidebar menu now includes: Back To Dashboard, NETWORKS, and New Network. The main table displays one network entry: 'A0001F3F' with the name 'Sample network'. The table has columns: Network ID, Name, Gateways, Visibility, Country, City, ZIP. A bottom footer states 'Copyright © 2015 - 2021 LORIOT AG. All rights reserved.' and 'LORIOT | Internet of Things at Long Range | Impressum'.

Abbildung 32: Netzwerkliste

3. Öffnen Sie das Netzwerk, indem Sie einmal auf seinen Namen klicken. Klicken Sie dann auf die Schaltfläche „**+ Gateway hinzufügen**“.



Copyright © 2015 - 2021 LOROT AG. All rights reserved.

LOROT | Internet of Things at Long Range | Impressum

Abbildung 33: Hinzufügen eines Gateways zum Netzwerk

4. Suchen Sie in der Liste der Gateways nach „RAK7249“ und wählen Sie es aus.

#### HINWEIS

Wenn Sie ein anderes Gateway-Modell aus der WisGate Edge-Serie verwenden, müssen Sie dennoch RAK7249 in dieser Liste auswählen. Dies hat keinerlei Auswirkungen auf die Leistung.

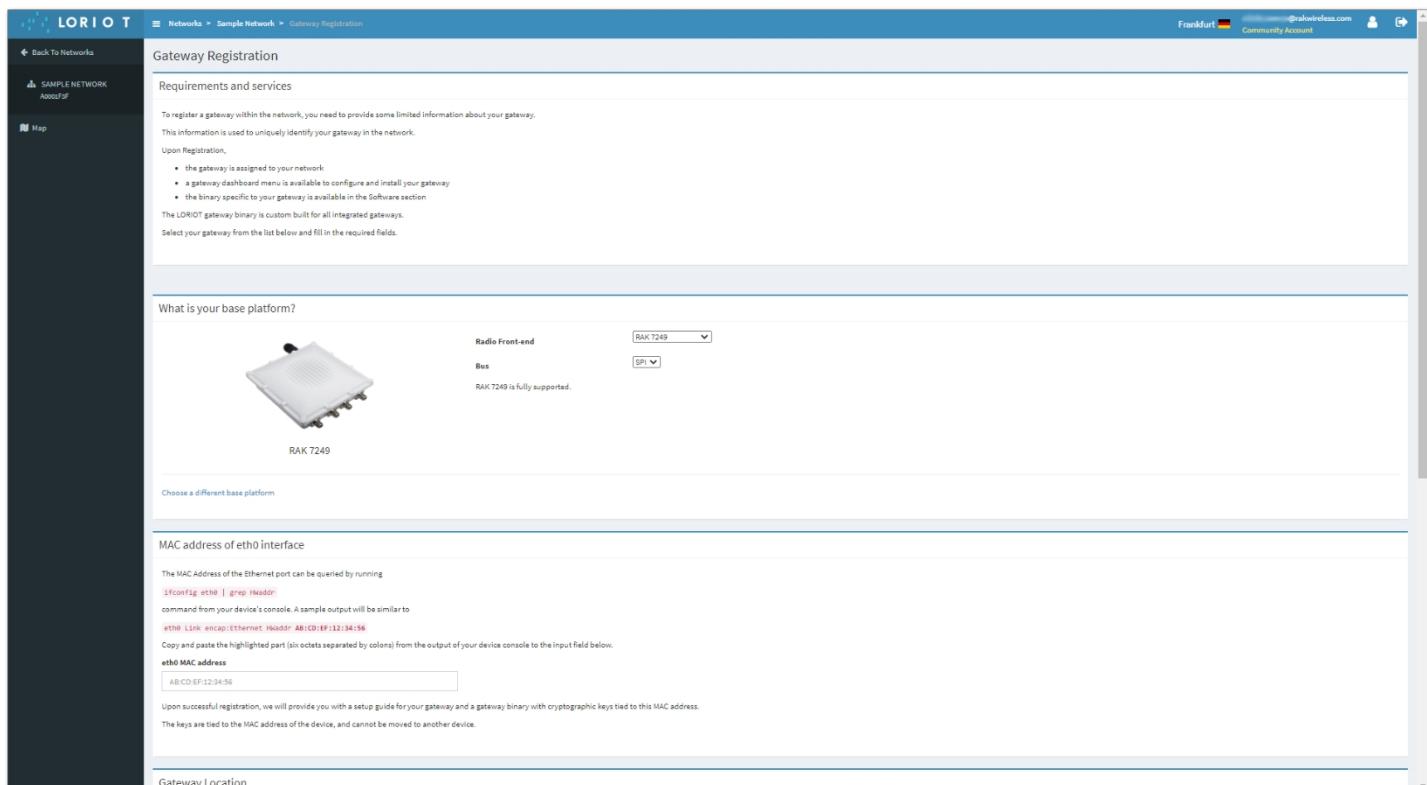


Abbildung 34: Auswahl von RAK7249

5. Nun müssen Sie über SSH eine Verbindung zu Ihrem Gateway herstellen. Wie bereits erwähnt, wird dieses Tutorial mit PuTTY durchgeführt.

SSH-Client. Öffnen Sie PuTTY und geben Sie die IP-Adresse Ihres Gateways ein. Wenn sich Ihr Gateway im AP-Modus befindet, lautet die Adresse **192.168.230.1**.

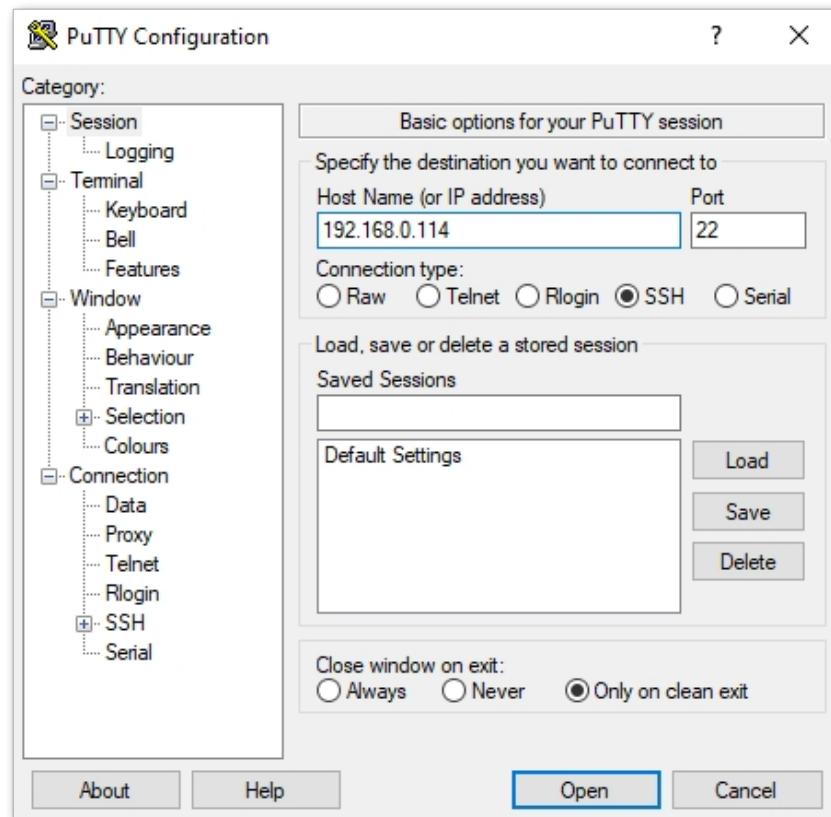


Abbildung 35: PuTTY-Konfiguration

#### 6. Melden Sie sich mit Ihren Root-Anmelddaten an.

- Standardbenutzername: **root**
- Passwort: **root**

Um die MAC-Adresse Ihres Gateways zu erhalten, führen Sie den folgenden Befehl aus:

```
ifconfig eth0 | grep HWaddr
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
eth0      Link encap:Ethernet HWaddr 60:C5:A8:XX:XX:XX
```

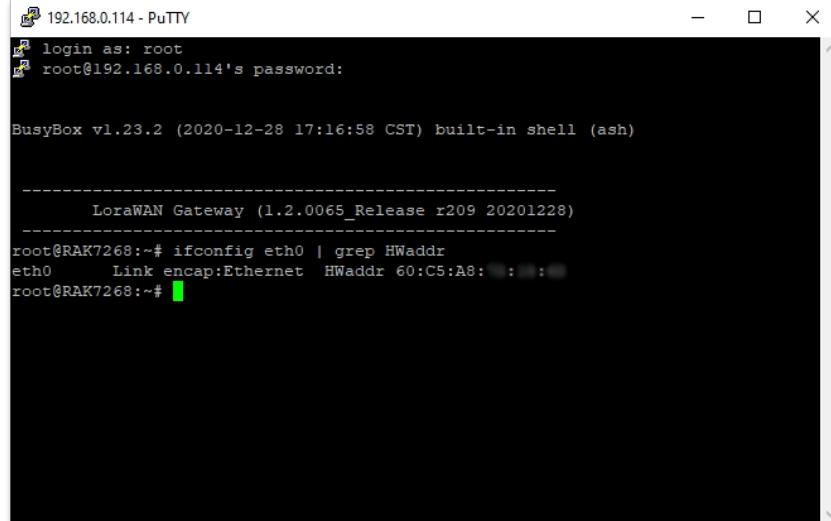
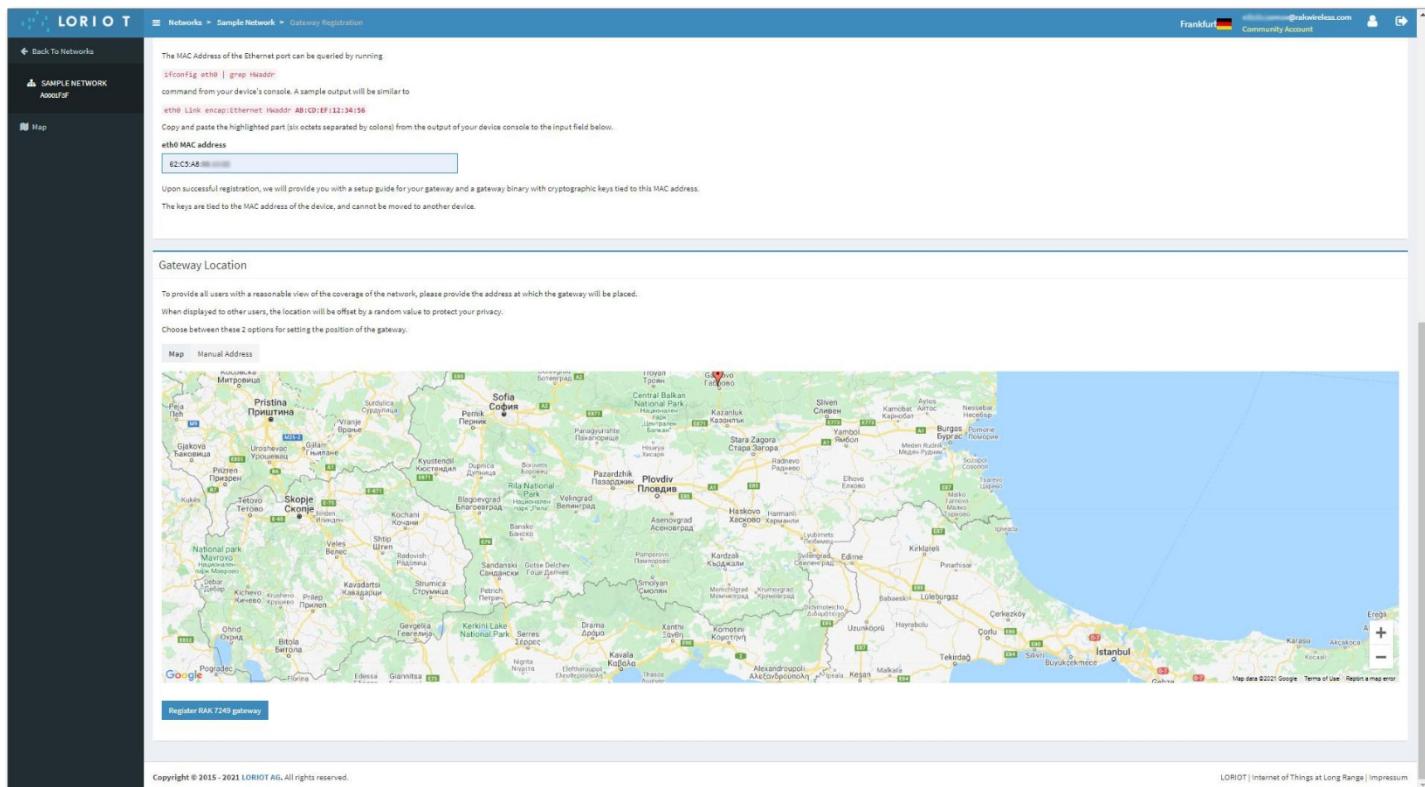


Abbildung 36: Abrufen der MAC-Adresse des Gateways

#### 7. Kopieren Sie die MAC-Adresse und geben Sie sie in das Registrierungsformular für das Gateway in LORIOT ein. Scrollen Sie nach unten und klicken Sie auf die Schaltfläche „RAK7249-Gateway registrieren“.



**Abbildung 37:** Eingabe der MAC-Adresse

8. Das Gateway ist nun registriert und Sie müssen der Verbindung eine Sicherheitsebene hinzufügen. Diese wird von der Gateway-Software von LORIOT bereitgestellt. Um sie zu installieren, führen Sie die folgenden Befehle in PuTTY aus.

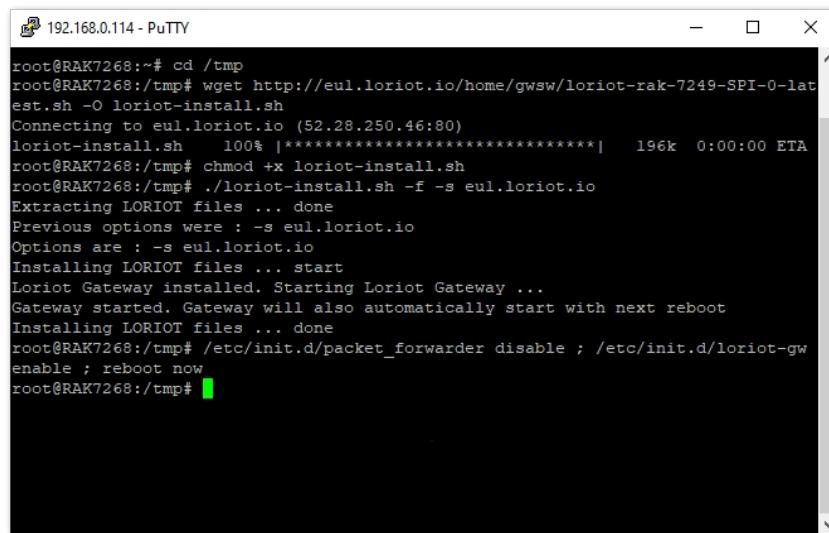
```
cd /tmp
```

```
wget http://eu1.loriot.io/home/gsw/loriot-rak-7249-SPI-0-latest.sh -O loriot-install.sh
```

```
chmod +x loriot-install.sh
```

```
./loriot-install.sh -f -s eu1.loriot.io
```

```
/etc/init.d/sx130x_lora_pkt_fwd deaktivieren; /etc/init.d/loriot-gw aktivieren; jetzt neu starten
```



```

192.168.0.114 - PuTTY
root@RAK7268:~# cd /tmp
root@RAK7268:/tmp# wget http://eul.loriot.io/home/gsws/loriot-rak-7249-SPI-0-latest.sh -O loriot-install.sh
Connecting to eul.loriot.io (52.28.250.46:80)
loriot-install.sh 100% [*****] 196k 0:00:00 ETA
root@RAK7268:/tmp# chmod +x loriot-install.sh
root@RAK7268:/tmp# ./loriot-install.sh -f -s eul.loriot.io
Extracting LORIOT files ... done
Previous options were : -s eul.loriot.io
Options are : -s eul.loriot.io
Installing LORIOT files ... start
Loriot Gateway installed. Starting Loriot Gateway ...
Gateway started. Gateway will also automatically start with next reboot
Installing LORIOT files ... done
root@RAK7268:/tmp# /etc/init.d/packet_forwarder disable ; /etc/init.d/loriot-gw enable ; reboot now
root@RAK7268:/tmp#

```

Abbildung 38: Installation der LORIOT-Software

Ihr Gateway ist nun registriert und mit LORIOT verbunden.

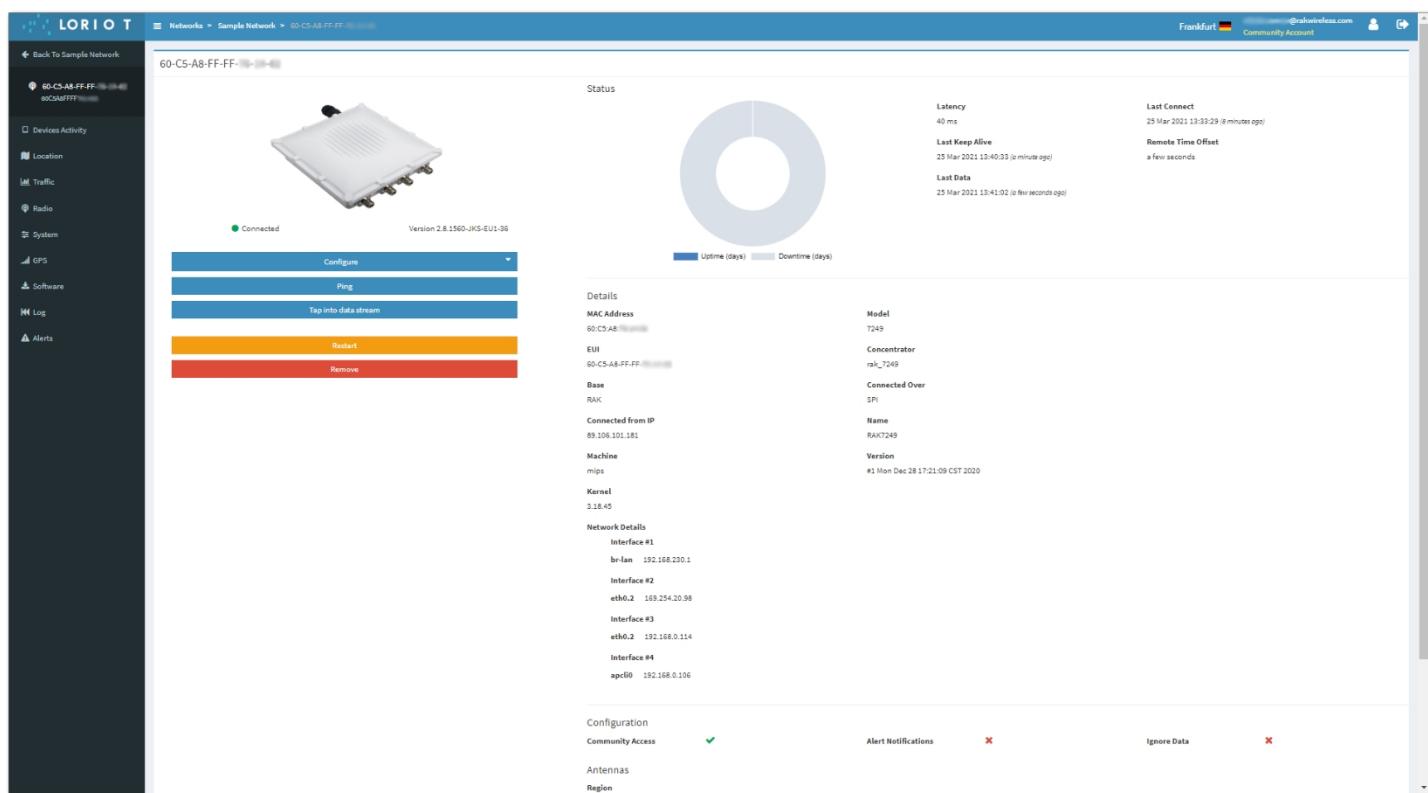


Abbildung 39: Erfolgreiche Verbindung

Letzte Aktualisierung: 29.07.2022, 22:17:19 Uhr