# RAK7268 Supported LoRa Network Servers AWS IoT Core for LoRaWAN

If you don't have an AWS account, refer to the instructions in the guide here 🖾 . The relevant sections are Sign up for an AWS account and Create a user and grant permissions.

## **Overview**

The high-level steps to get started with AWS IoT Core for LoRaWAN are as follows:

- 1. Onboard your Gateway (see section Add the Gateway to AWS IoT)
- Onboard your Device(s) (see section Add a LoRaWAN Device to AWS IoT) a. Verify device and service profiles
   b. Set up a Destination to which device traffic will be routed and processed by a rule.

These steps are detailed below. For additional details, refer to the AWS LoRaWAN developer guide 🗅 .

# Add the Gateway to AWS IoT

## Preparation

Refer to the online guide d for steps required prior to onboarding your gateway. For more details check the datasheet page: WisGate Edge Lite 2 Datasheet Software d.

### **Frequency Band selection and Role setup**

Refer to the online guide 2 for information on selecting an appropriate frequency band.

#### 📝 NOTE

LoRa® Frequency bands supported by RAK7248: IN865, EU868, US915, AU915, KR920 and AS923 , please select an appropriate frequency band from our Store

Follow the instructions in the section Add an IAM role to allow the Configuration and Update Server (CUPS) to manage gateway credentials in the online guide  $\square$ .

### Add the LoRaWAN Gateway

To register the Gateway with AWS IoT Core for LoRaWAN, follow the steps in this online guide I under the section Add a gateway using the console.

# Add a LoRaWAN Device to AWS IoT Preparation

Refer to the datasheet to learn more about RAK4631 WisBlock LPWAN Module 🗹 . Refer to the instructions in the section Before onboarding your wireless device in the online guide 🖾 . Then follow the instructions in the section Add your wireless device to AWS IoT Core for LoRaWAN here 🖸 .

## **Verify Profiles**

AWS IOT Core for LoRaWAN supports device profiles and service profiles. Device profiles contain the communication and protocol parameter values the device needs to communicate with the network server. Service profiles describe the communication parameters the device needs to communicate with the application server.

Some pre-defined profiles are available for device and service profiles. Before proceeding, verify that these profile settings match the devices you will be setting up to work with AWS IoT Core for LoRaWAN. For more details, refer to the section Add profiles to AWS IoT Core for LoRaWAN in the online guide  $\Box$ .

## Set up a Destination for device traffic

Because most LoRaWAN devices don't send data to AWS IoT Core for LoRaWAN in a format that can be consumed by AWS services, traffic must first be sent to a Destination. A Destination represents the AWS IoT rule that processes a device's data for use by AWS services. This AWS IoT rule contains the SQL statement that selects the device's data and the topic rule actions that send the result of the SQL statement to the services that will use it.

For more information, refer to the online guide 🖾 (sections titled Add a destination using the console and Create an IAM role for your destinations). Also refer to Create rules to process LoRaWAN device messages in the online guide 🖾 .

# Set up the Gateway

- Set up Gateway Hardware: Refer to the product configuration to learn more about RAK7268 Product Configuration □ .
- Set up Gateway Software: Refer to the product configuration to learn more about RAK7268 Product Configuration ☑ .
- Additional Software References:
  - FAQ ⊡
  - ∘ Forum 🗹

## **Configuring the Gateway device with WisGateOS 1**



Figure 1: RAK7268 With WisGate OS 1 LoRaGateway Setting

By default, the Gateway will work in Wi-Fi AP Mode which means that you can find an SSID named like "RAK7268\_XXXX" on your PC's Wi-Fi Network List. "XXXX" is the last two bytes of the Gateway MAC address. To access the Web Management Platform, input the IP Address: 192.168.230.1 in your Web browser.

(Note: No password is required to connect via Wi-Fi.)

Using your preferred Web browser, input the aforementioned IP Address and you should see the same Log-in Page shown in the following image. Login the credentials provided below:

- Username: root
- Password: root

root Password
Login

Figure 2: Web User Interface Log-in

C:\Users\Mark\Documents\Work\RAKwireless\Documentation\rakwireless-docs-

internal\docs.vuepress\public\assets\images\wisgate\rak7268\supported-lora-network-servers\aws The first firmware version that supports AWS IoT Core for LoRaWAN is 1.2.0065\_Release\_r209, it can be verified on Status -> Overview -> System -> Firmware Version.

Navigate to System -> Backup/Flash Firmware -> Flash new firmware image, and upgrade the firmware.

🇐 RAK'		ogout
🙆 Status	Flash operations	
Network	Backup / Restore	
(X) Channel Plan	Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).	
네 LoRa Network	Download backup: Generate archive	
🚓 Services	Reset to defaults: Perform reset	
🖾 System	To restore configuration files, you can upload a previously generated backup archive here.	
System Administration	Restore backup: Choose File No file chosen Upload archive	
License		
Backup / Flash Firmware	Flash new firmware image	
File Browser	Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).	
රා WisDM	Keep settings 🗹	
	Image. Choose File No file chosen Filash image	
	Copyright © RAKWireless Technology Co., Ltd. All Rk	hts Reserved.



#### **Configure Network Mode to Basic Station**

- 1. Navigate to LoRa Network -> Network Settings.
- 2. change Mode in LoRaWAN Network Settings to Basic Station.
- 3. Select LNS Server from Server, then select TLS Server and Client Authentication from Authentication Mode.

🏟 RAK°			Logout
③ Status	Log Lever	NOTICE	
Over the second seco	LoRa Basic Station Basic Station Configuration		
<sup>(</sup> ନ୍ଧୁ <sup>)</sup> Channel Plan	Basic Station		
네 LoRa Network			
Network Settings		CUPS Boot Server	
A		CUPS Server     INS Server	
🗞 Services	URI		
System			
රා) WisDM	Port	443	
	Authentication Mode	TLS Server and Client Authentication $\qquad \qquad \lor$	
	trust		
	certificate		

Figure 4: Configure Network Mode to Basic Station

#### Configure URI, Port and Authentication Mode

🇐 RAK°			Logout	aws		Q Search for services, features, blogs, docs, and more [Alt+S]
③ Status	Mode	Basics Station	~	<u>^</u> ≡	and upload th	em to your gateway.
🐼 Network	Log Level	NOTICE	~			y certificate tificate so that your gateway can communicate securely with AWS IoT. Download the certificate files so that you can upload
(🕱) Channel Plan					them to your	r gateway.
네 LoRa Network	LoRa Basic Station Basic Station	Configuration			Create	certificate Section 2 Certificate created and associated with your gateway
Network Settings	Basic Station					tificate files were created. Download them and save them to upload to your
🗞 Services	Server	CUPS Boot Server			gateway.	
🔠 System		CUPS Server			Gateway	certificate file 4e4fd3d8-9ce1cert.pem
රා WisDM	URI				Private k	ey file 4e4fd3d8-9ce1-4
	Port				₩ Dow	vnload certificate files
	Authentication Mode	TLS Server and Client Authentication	~			
	trust					ning credentials Info endpoint that your gateway supports. Then, copy the endpoint and download the server trust certificate so that you can add r gateway.
					CUPS (Con	ifiguration and Update Server) endpoint
	certificate				https	s://cups.lorawan.us-east-1.amazonaws.com:443
					LNS (LoRa)	WAN Network Server) endpoint
					WSS	:// .lns.lorawan.us-east-1.amazonaws.com/443
	key					ust certificates our server trust certificate so you can upload the certificate for the endpoint your gateway supports.
					Dow Dow	vnload server trust certificates

Figure 5: Configure URI, Port and Authentication Mode

# **Configuring the Gateway device with WisGateOS 2**



Figure 6: RAK7268 With WisGate OS 2 LoRaGateway Setting

By default, the Gateway will work in Wi-Fi AP Mode which means that you can find an SSID named like "RAK7268\_XXXX" on your PC's Wi-Fi Network List. "XXXX" is the last two bytes of the Gateway MAC address. To access the Web Management Platform, input the IP Address: 192.168.230.1 in your Web browser.

(Note: No password is required to connect via Wi-Fi.)

Using your preferred Web browser, input the aforementioned IP Address and you should see the same Log-in Page shown in the following image. Login the credentials provided below

- Username: root
- Password: <user defined>

WisGate	
Set your password	
Before your first login, you need to set a password	
for your account.	
Password	
ø	
Confirm password	
Commin password	
Ø	
Set password	
	Simple access to your gateways
	Set up, connect, monitor, analyze
	and run gateways.

Figure 7: WisGate OS 2 Home Page

Navigate to LoRa®; change Work Mode to Basics Station and Select LNS Server from Server, then select TLS Server and Client Authentication from Authentication Mode.

WS Gate	Configuration		
:: :: ::	Work mode	Packet forwarder Basics station Built-in network server	
~ ¢	Log Level	Log Level	
	Basics station server setup	Configure Basics Station server setup. Basics Station Server Type CUPS-BOOT Server	^ ©
		CUPS Server LNS Server Figure 8: WisGateOS2 Basics Station Configuration	

#### **Configure URI, Port and Authentication Mode**

CUPS-BOOT Server	aws Services Q. Search for services, features, blogs, docs, and more [Alt+S] D. 🗛 🕐 N. Virginia 🔻
CUPS Server	and upload them to your gateway.
LNS Server Server URL	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.
Server Port	Create certificate Sector Certificate created and associated with your gateway These certificate files were created. Download them and save them to upload to your gateway.
Authentication Mode	Gateway certificate file 4e4fd3d8-9ce1cert.pem
TLS Server & Client Authentication +	Private key file 4e4fd3d8-9ce1private.key
Trust (CA Certificate) Drop your certificate file here or choose file	☑ Download certificate files
Cient certificate	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.
Drop your certificate file here or choose file	CUPS (Configuration and Update Server) endpoint https://cups.lorawan.us-east-1.amazonaws.com:443
Drop your certificate file here or choose file	LNS (LORAWAN Network Server) endpoint           wss://         .ins.lorawan.us-east-1.amazonaws.com         [43]         [7]         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



### **Connect the Gateway and verify the connection status**

Follow the instructions in the online guide <sup>I</sup> to connect your gateway to AWS IoT Core for LoRaWAN.

To verify the connection status, refer to the instructions in the section **Check gateway connection status using the console** 

Gate	ways (2) Info			Edit Delete	Add gateway
	Gateway ID	Name	Description	Last uplink received	-
0	fbf86532-864c-4f07-9a82-f66813f68b74	B827EBFFFE829C33	-	-	
0	b8f1810f-2d78-4cf1-8646-95fa2cc5b871	RAK7268	-	June 29, 2022, 17:46:56 (UTC+0800)	

Figure 10: Gateway Connection status

# **Add End Device**

Please refer to RAK4631 Quickstart I to enable communication with the gateway.

### Updating RAK4631 to RAK4631-R

RAK4631-R and RAK4631 share common hardware and are 100% identical, but they have different firmware. RAK4631-R is based on RUI3, which gives you flexibility in developing optimized firmware using the RUI3 APIs.

Please refer to updating RAK4631 to RUI3 12 to update RAK4631.

## Join the AWS IoT LoRaWAN server

This section shows an example of how to join the AWS IoT LoRaWAN server

1. Add Device Profile

Select a default profile and customize - optional	
Default profiles are based on your selected LoRaWAN OTAA device customized your profile per your device vendor specifications.	class and your LoRaWAN radio frequency band. You may need to
US915 - A	▼
<b>Device profile name</b> Type a descriptive name for this device profile.	Frequency band (RFRegion) Choose the LoRa supported frequency band for this profile.
US915-A-OTAA	US915 <b>•</b>
MAC version The MACVersion of the LoRaWAN devices that use this profile.	Regional parameters version Select the region parameters version identifier for this profile.
1.0.3	Decised Decementary v1 0 7x4
MaxEIRP	Regional Parameters v1.0.3rA 🔻
	Regional Parameters VI.U.SrA
Enter the MaxEIRP value for this device profile.         13         Supports Class B         Coose to enter the values for Class B support.	Regional Parameters VI.U.SrA
Enter the MaxEIRP value for this device profile.          13         Supports Class B         Choose to enter the values for Class B support.         Supports Class C         Choose to enter the values for Class C support.	Regional Parameters VI.U.SrA
Enter the MaxEIRP value for this device profile. 13 Supports Class B	Regional Parameters VI.U.STA

Figure 11: Adding the Device Profile

2. Add Service Profile

service profile	
service profile describes the fe	tures that are enabled for the user(s), and the rate of messages that can be sent over the network.
ervice profile name - option inter a descriptive profile name.	al
rak4631	
A data a datiti a canta ana tana ang	
Tags - optional tag is a label that you assign to our resources or track your AWS	
Tags - optional a tag is a label that you assign to our resources or track your AWS Key	an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter
Fags - optional tag is a label that you assign to our resources or track your AWS Key Q. Key	an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter costs. Value - optional
Tags - optional	an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter costs. Value - optional

Figure 12: Adding the Service Profile

3. Add Destination Before adding the destination, follow the Add IAM role for Destination to AWS IoT Core for LoRaWAN section to configure IAM policy and role.

estination details Info	
estination name he destination name appears in the device and gateway destinat	ion selection lists.
ProccessLoRa	
Destination description - optional rovide a helpful description of your destination.	
Destination description.	
,	Publish to AWS IoT Core message broker If you need a publish/subscribe broker to distribute messages to multiple subscribers

Figure 13: Adding Destination

#### 4. Add Device

- Before adding a device to AWS IoT, retrieve the DevEui, AppEui, and AppKey from the end Device's console. You can use AT command to obtain the information.
  - AT+DEVEUI : end-device ID
  - AT+APPEUI : application identifier
  - AT+APPKEY : application key

For more AT commands, refer to the RAK4631-R AT Command Manual 17 .

For Example:

Wireless device specification Your device specifications consist of the LoRaWAN version (1.1 or 1.0. Authentication By Personalization). Once selected, your data is encry	
OTAA v1.0.x	•
DevEUI	Confirm DevEUI
000000000000000000000000000000000000000	000000000000000
The 16-digit hexadecimal DevEUI value found on your wireless device.	Reenter the DevEUI.
АррКеу	Confirm AppKey
000000000000000000000000000000000000000	000000000000000000000000000000000000000
The 32-digit hexadecimal AppKey value that your wireless device vendor provided.	Reenter the AppKey.
AppEUI	Confirm AppEUI
000000000000000	000000000000000
The 16-digit hexadecimal AppEUI that your wireless device vendor provided.	Reenter the AppEUI.
Wireless device name - optional	
RAK4631-R	

#### Figure 14: LoRaWAN Specifications and Wireless Device Configuration

Profiles	
Wireless device profile Choose a wireless device profile so your device can pass the correct messages to your gateway.	
US915-A-OTAA	•
Service profile Choose a service profile.	
rak4631	•

Figure 15: Choosing a Wireless Device Profile

hoose destination	
Choose destination	
Destination name Destinations route LoRaWAN messages from your wireless device to other AWS services.	
ProccessLoRa	V

Figure 16: Choosing a Destination

#### 5. Join the AWS IoT LoRaWAN server

Use the command: AT+JOIN to join the AWS IOT LORAWAN server

AT+JOIN=1:0:10:8

OK +EVT:JOINED

#### 6. Send an uplink message

Use AT+SEND to send data on a dedicated port number

AT+SEND=12:112233 OK	
LoraWAN	
LoRaWAN devices (1) Info	Edit Delete Add wireless device
Device ID     V     Name     Destination          aa852149-4b41-48b8-86cd      RAK4631-R     ProccessLoRa	▼         Last Uplink Received At         ▼         Arn         ▼         DevEUI         ▼           2022-06-29T09:49:06.82770         arn:aws:iotwireless:us-west-2:         000000000000000000000000000000000000

Figure 17: Uplink Received

## Connect the device and verify the connection status

Follow the instructions in the online guide <sup>I</sup> to connect your device to AWS IoT Core for LoRaWAN.

To verify the connection status, refer to the instructions in the section Check device connection status using the console. You can also View format of uplink messages sent from LoRaWAN devices

# Verifying Operation – a "Hello World" example

Once setup is completed, provisioned OTAA devices can join the network and start to send messages. Messages from devices can then be received by AWS IoT Core for LoRaWAN and forwarded to the IoT Rules Engine.

Instructions for a sample Hello World application are given below, assuming that the device has joined and is capable of sending uplink traffic. The architecture for this sample application is:

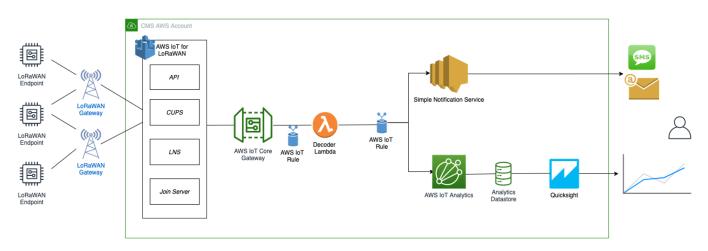


Figure 18: Sending Uplink Architecture

### **Create lambda function for destination rule**

Create the lambda function to process device messages processed by the destination rule.

- Go to the AWS Lambda console (console.aws.amazon.com/lambda).
- Click on Functions in the navigation pane
- Click on Create function
- Select **Author from scratch**. Under Basic information, enter the function name and choose Runtime Python 3.8. from the drop-down under **Runtime**.
- Click on Create function.

 In the Code source tab, under index.js, paste the copied code into the editor under the lambda\_function.py tab.

```
import base64
import json
import logging
import ctypes
import boto3
FUNCTION_NAME = "RAK-HelloWorld"
DATA_TYPES = 1
TYPE_TEMP = 0 \times 67
client = boto3.client('iot-data')
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])</pre>
      temp = ctypes.c_int16(temp).value
     result['temperature'] = temp / 10
  return result
def lambda_handler(event, context):
 data = decode(event)
  logger.info("Data: %s" % json.dumps(data))
  response = client.publish(
      topic = event.get("WirelessMetadata").get("LoRaWAN").get("DevEui") + "/project/sensor/decod
  return response
```

- Once the code has been pasted, choose **Deploy** to deploy the lambda code.
- Click on the Permissions tab of the lambda function.
- Change the Lambda Role Policy permission.

- Under Execution role, click on the hyperlink under Role name.
- On the **Permissions tab**, find the policy name and select it.
- Choose Edit policy, and choose the JSON tab.
- Append the following to the Statement section of the policy to allow publishing to AWS IoT.

{		json
"Effect":"Allow",		
"Action":[		
"iot:Publish"		
],		
"Resource":[		
"*"		
J		
}		
] }		

- Choose Review Policy, then Save changes.
- Return to the **Code** tab and create a test event that will allow you to test the functionality of the lambda function.
  - From the Test drop-down menu, choose Configure test events
  - Enter a name for the test event under the **Event name**.
  - Paste the following sample payload in the area under Event name:



- Choose Save to save the event.
- Navigate to the AWS IoT console, choose Test on the navigation pane, and select MQTT test client.
- Configure the MQTT client to subscribe to "#" (all topics).
- Click on Test in the Lambda function page to generate the test event you just created.
- Verify the published data in the AWS IoT Core MQTT Test client:
  - Open another window. Go to AWS IoT Console, select Test under Subscription Topic, enter # and select to Subscribe to topic.
  - The output should look similar to this:

## **Create the Destination Rule**

In this section, create the IoT rule that forwards the device payload to your application. This rule is associated with the destination created earlier in Set up a Destination for Device Traffic section.

- 1. Navigate to the AWS IoT console
- 2. In the navigation pane, choose Act, then select Rules.
- 3. On the Rules page, choose Create.
- 4. On the Create a rule page, for Name, enter LoRaWANRouting. For Description, enter a description of your choice. Note the name of your rule. The information will be needed when you provision devices to run on AWS IoT Core for LoRaWAN.
- 5. Leave the default Rule query statement: 'SELECT \* FROM 'iot/topic' unchanged. This query has no effect at this time, as traffic is currently forwarded to the rules engine based on the destination.
- 6. Under Set one or more actions, choose Add action.
- 7. On the Select an action page, choose **Republish a message to an AWS IoT topic**. Scroll down and choose **Configure action**.
- 8. On the Configure action page, for Topic, enter *project/sensor/decoded*. The AWS IoT Rules Engine will forward messages to this topic.
- 9. Under Choose or create a role to grant AWS IoT access to perform this action, select Create Role.
- 10. For Name, enter a name of your choice.
- 11. Choose **Create role** to complete the role creation. You will see a "**Policy Attached**" tag next to the role name, indicating that the Rules Engine has been permitted to execute the action.
- 12. Choose Add action.
- 13. Add one more action to invoke the Lambda function. Under Set one or more actions, choose Add action.
- 14. Choose Send a message to a Lambda function.
- 15. Choose Configure action.
- 16. Select the Lambda function created earlier and choose Add action.
- 17. Then, choose Create rule.
- 18. A "Success" message will be displayed at the top of the panel, and the destination has a rule bound to it.

You can now check that the decoded data is received and republished by AWS by triggering a condition or event on the device itself.

- Go to the AWS IoT console. In the navigation pane, select Test, and choose MQTT client.
- Subscribe to the wildcard topic '#" to receive messages from all topics.
- Send message from endDevice using AT command: at+send=1:01670110 .
- You should see traffic similar to that shown below.



## **Configuring Amazon SNS**

You will be using the Amazon Simple Notification Service to send text messages (SMS) when certain conditions are met.

- 1. Go to the Amazon SNS console
- 2. Click on the menu in the left corner to open the navigation pane.
- 3. Select Text Messaging (SMS) and choose Publish text message.
- 4. Under Message type, select Promotional.
- 5. Enter your phone number (phone number that will receive text alerts).
- 6. Enter "Test message" for the Message and choose Publish message.
- 7. If the phone number you entered is valid, you will receive a text message and your phone number will be confirmed.
- 8. Create an Amazon SNS Topic as follows:
  - In the navigation pane, choose Topics.
  - Select Create topic.
  - Under Details, select Standard.
  - Enter a name of your choice. Here, you will use "text\_topic".
  - Choose Create topic.
- 9. Create a subscription for this topic:
  - On the page for the newly created text topic, choose the **Subscriptions** tab.

- Choose Create subscription.
- In Topic ARN, choose the topic you have created earlier.
- Select **Protocol** as SMS from the drop-down.
- Under Endpoint, enter the previously validated phone number to receive the SMS alerts.
- Choose Create subscription. You should see a "Subscription to text\_topic created successfully" message.

### Add a Rule for Amazon SNS Notification

Now, add a new rule to send an Amazon SNS notification when certain conditions are met in a decoded message.

- 1. Navigate to the AWS IoT console 1.
- 2. In the navigation pane, choose Act. Then, choose Rules.
- 3. On the Rules page, choose Create.
- 4. Enter the Name as text\_alert and provide an appropriate Description.
- 5. Under the Rule query statement, enter the following query:

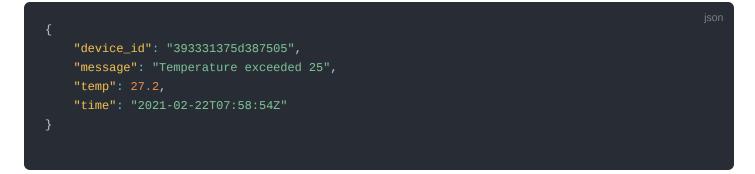
SELECT devEui as device\_id, "Temperature exceeded 25" as message, temperature as temp, timestamp

- 6. Under Set one or more actions, choose Add action
- 7. Choose Send a message as an SNS push notification.
- 8. Choose Configure action.
- 9. Under SNS target, select *text\_topic* from the drop-down.
- 10. Select RAW under Message format.
- 11. Under Choose or create a role to grant AWS IoT access to perform this action, choose Create role.
- 12. Enter a name for the role and choose Add action.
- 13. Choose Create rule. You should see a "Success" message, indicating that the rule has been created.

### Test the Rule for Amazon SNS Notification

After adding the rule for Amazon SNS notification, you should receive a text message when hitting the event.

Send message from endDevice using AT command: <u>at+send=1:01670110</u>. Here is the message from mobile after sending an uplink message.



### Send Downlink Payload

This section shows how to send downlink payload from AWS IoT LoRaWAN Server to end Device.

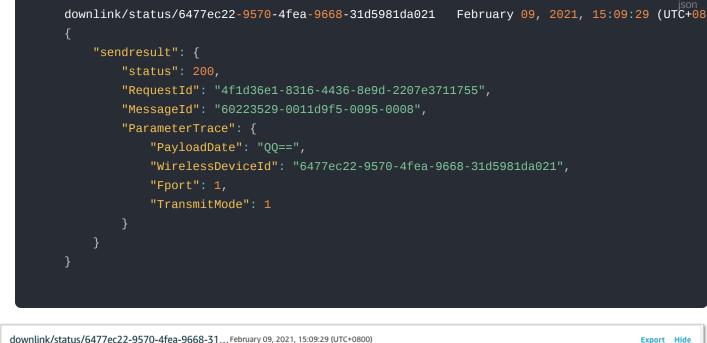
- 1. Install the AWS SAM CLI
- 2. Deploy SAM template to AWS 12 .
- 3. Send Payload to End Device.
  - Go to the AWS IoT console.
  - In the navigation pane, select Test, and choose MQTT client.

- Subscribe to the wildcard topic '#" to receive messages from all topics.
- Specify the topic to *cmd/downlink/{WirelessDeviceld}* and a base64-encoded message.

Publish Specify a topic and a message to publish	with a QoS of 0.		
cmd/downlink/	021		Publish to topic
1 QQ==			



4. You should see traffic on AWS similar, as shown below:



downink/status/04/76222-3570-4164-3006-51reliany 05, 2021, 15.05.23 (01010000)	Export	niue
<pre>{     "sendresult": {         "status": 200,         "RequestId": "4f1d36e1-8316-4436-8e9d-2207e3711755",         "MessageId": "60223529-001ld9f5-0095-0008",         "ParameterTrace": {             "PayloadData": "QQ==",             "NirelessDeviceId": "6477ec22-9570-4fea-9668-31d5981da021",             "Fport": 1,             "TransmitMode": 1         }     } }</pre>		
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==		

Figure 20: Traffic on AWS

5. You should see traffic on your console of end device similar, as shown below.



### **IoT Analytics**

You will use IoT Analytics to visually display data via graphs if there is a need in the future to do further analysis.

### **Create an IoT Analytics Rule**

#### **Create a Rule First**

- 1. Navigate to the AWS IoT console 2 .
- 2. In the navigation pane, choose Act and then, choose Rules.
- 3. On the Rules page, choose Create.
- 4. Enter the Name as Visualize, and provide an appropriate Description.
- 5. Under the Rule query statement, enter the following query:

#### SELECT \* FROM 'project/sensor/decoded'

- 6. Choose Add action.
- 7. Select Send a message to IoT Analytics.
- 8. Choose Configure Action.
- 9. Choose Quick Create IoT Analytics Resources.
- 10. Under Resource Prefix, enter an appropriate prefix for your resources, such as LoRa.
- 11. Choose Quick Create
- 12. Once the Quick Create Finished message is displayed, choose Add action.
- 13. Choose **Create rule**. You should see a Success message, indicating that the rule has been created.

### **Configure AWS IoT Analytics**

#### Set up AWS IoT Analytics

- 1. Go to the AWS IoT Analytics console  $\square$  .
- 2. In the navigation panel, choose Datasets.
- 3. Select the data set generated by the Quick Create in Create an IoT Analytics Rule
- 4. In the Details section, edit the **SQL query**.
- 5. Replace the query with as follows:

SELECT devEui as device\_id, temperature as temp, timestamp as time FROM LoRa\_datastore

- 6. Under Schedule, choose Add schedule.
- 7. Under Frequency, choose Every 1 minute, and then click Save.

### **Configure Amazon QuickSight**

Amazon QuickSight lets you easily create and publish interactive BI dashboards that include Machine Learningpowered insights.

- 1. Go to AWS Management console
- 2. From the management console, enter **QuickSight** in the "Search for services, features.." search box.
- 3. Click on QuickSight in the search results.
- 4. If you haven't signed up for the service before, go ahead and sign up, as there is a free trial period.
- 5. Select the Standard Edition, and choose Continue.
- 6. Enter a unique name in the field QuickSight account name.
- 7. Fill in the Notification email address.
- Review the other checkbox options and change them as necessary. The AWS IoT Analytics option must be selected.
- 9. Choose **Finish**. You will see a confirmation message.

- 10. Choose Go to Amazon QuickSight.
- 11. Select Datasets.
- 12. Select New dataset.
- 13. Select AWS IoT Analytics.
- 14. Under Select an AWS IoT Analytics data set to import, choose the data set created in **Create an IoT Analytics Rule**.
- 15. Choose Create data source, and then choose Visualize.
- 16. Select the dataset created, then select **Refresh** or **Schedule Refresh** for a periodic refresh of the dataset.

# Debugging

If you experience any issues, you can check the logs located in the /var/log/ directory.

# Troubleshooting

- 1. Unable to see the web login:
  - Check that your wifi is connected to RAKWireless\_XXXX.
  - Try ping **192.168.230.1**.

# The Things Network v3 (TTNv3)

In this section, it will be shown how to connect RAK7268 WisGate Edge Lite 2 to TTNv3.

To login into the TTNv3, head on here 🖸 . If you already have a TTN account, you can use your The Things ID credentials to log in.

THE THINGS STACK Community Edition
Login to The Things Stack with <b>The Things</b> I <b>D</b>
Username or email •
Password •
Submit
Register ForgoLpassword2
The Things ID by The Things Industries

Figure 21: The Things Stack Home Page

#### **NOTE**

This tutorial is for the EU868 Frequency band.

# **Registering the Gateway**

 To register a commercial gateway, choose Register a gateway (for new users that do not already have a registered gateway) or go to Gateways > + Add gateway (for users that have registered gateways before).

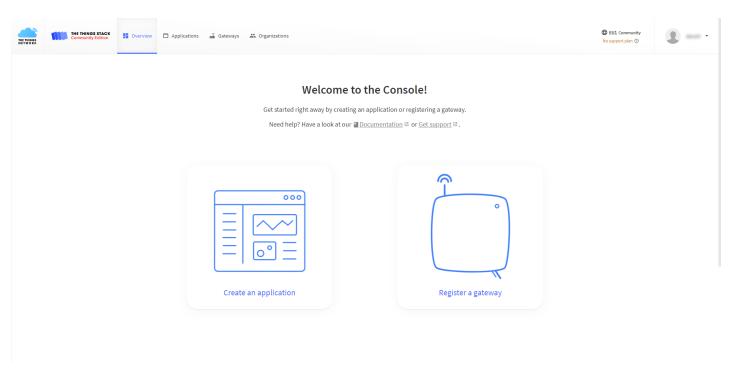


Figure 22: Console Page after successful login

#### 2. Fill in the needed information:

- Owner Automatically filled by The Things Stack, based on your account or created Organization.
- Gateway ID This will be the unique ID of your gateway in the Network. Note that the ID must contain only lowercase letters, numbers, and dashes (-).
- Gateway EUI A 64 bit extended unique identifier for your gateway. The gateway's EUI can be found either on the sticker on the casing or by going to the LoRa Network Settings page in the LoRa Gateway menu accessible via the Web UI. Instructions on how to access your gateway via Web UI can be found in the product's Quickstart Guide <sup>¬</sup>.
- Gateway name A name for your gateway.
- Gateway description (optional) 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.

#### **NOTE**

This tutorial is based on using the EU868 frequency band, so the server address will be: eu1.cloud.thethings.network.

• Frequency plan - The frequency plan used by the gateway.

#### 📝 NOTE

For this tutorial, we will use Europe 863-870 MHz (SF12 for RX2 - recommended).

• The other settings are optional and can be changed to satisfy your requirements.

THI THINGS NETWORK	THE THINGS STACK Community Edition	Overview	Applications	EU1 Community No support plan <sup>(2)</sup>	•
			Add gateway		
			General settings		
			Owner <sup>®</sup>		
			Gateway ID ⊕*		
			my-new-gateway		
			Gateway EUI 🗇		
			Gateway EUI		
			Gateway name 🗇		
			My new gateway		
			Gateway description 🕲		
			Description for my new gateway		
			Optional gateway description; can also be used to save notes about the gateway		
			Opunia gaeway ueschipuni, san abo be uescho save notes about the gateway Gateway Server address		
			eul.cloud.thethings.network		
			The address of the Gateway Server to connect to		
			Require authenticated connection ()		
			Controls whether this gateway may only connect if it uses an authenticated Basic Station or MQTT connection		
			Gateway status 🔿		
			Make status public The status of this gateway may be visible to other users		
			The same of this gareney may be hadre to other deels.		
			Kake location public		
			When set to public, the gateway location may be visible to other users of the network		
			Attributes ①		
			+ Add attributes Attributes can be used to set arbitrary information about the entity, to be used by scripts, or simply for your own organization		
			LoRaWAN options		
			Frequency plan (*)*		
			Select		
			Schedule downlink late $\odot$		
			Enabled Enable server-side buffer of downlink messages		
			Entatie server-site puner o downink messages		
			Z Enabled		
			Recommended for all gateways in order to respect spectrum regulations		
			Schedule any time delay ()* 530 milliseconds V		
			Configure gateway delay (minimum: 130ms, default: 530ms)		
			Gateway updates		
			Automatic updates		
			Enabled Gateway can be updated automatically		
			Channel		
			Stable		
			Channel for gateway automatic updates		
			Create gateway		
© 2022 The Th	nings Stack by The Things Network	and The Things In	dustries	v3.19.0 Documentation	Get support Status page

Figure 23: Adding a gateway

3. To register your gateway, scroll down and click Create gateway.

TTNv3 supports TLS server authentication and Client token, which requires a trust file and a key file to configure the Gateway to successfully connect it to the network.

# **Generating the Token**

1. To generate a key file, from the **Overview page** of the registered Gateway navigate to **API keys**.

THE THINGS STACK	Overview      Applications	🔒 Gateways 🛛 🗮 Organiz	ations		EU1 Community No SLA applicable ⑦	•
wisgate-edge-gateway		Gateways > wisgate-edge-g	ateway			
Overview		wisgate-ed	<b>ge-gateway</b> ateway			
Live data		<ul> <li>Disconnected (2)</li> </ul>		<u></u>	1 Collaborator 🛛 🗣 0 API keys	
Collaborators		General information Gateway ID	wisgate-edge-gateway	• Live data	See all activity →	
Or API keys		Gateway EUI	F6 E5 29 FF FE			
General settings		Gateway description Created at	None Apr 20, 2022 09:55:49			
		Last updated at Gateway Server address	Apr 20, 2022 09:55:49			
< Hide sidebar		Gateway Server address LoRaWAN information Frequency plan Global configuration	eu1.cloud.thethings.network	Location No location information availab	Change location settings –	
© 2022 The Things Stack by The Things Network	k and The Things Industries				EN v3.19.0 Documentation	② Get support Status page

Figure 24: Overview page

#### 2. On the API keys page, choose + Add API key.

THE THINGS NETWORK	THE THINGS STACK Community Edition	Overview	Applications	📸 Gateways	A Organizations				EU1 Community to SLA applicable ⑦		
💊 wis	gate-edge-gateway			Gateways >	wisgate-edge-gateway > API keys						
				API keys (0)				+ Add	API key		
Ove				Key ID		Name		Grante	d Rights		
ılı Live							No items found				
Coca	ation										
🚜 Coll	aborators										
OT API	keys										
🗱 Gen	eral settings										
< Hide sid	ebar										
© 2022 The T	hings Stack by The Things Networ	k and The Things Ind	ustries					⊕ EN v3.19.0	Documentation	② Get support	Status page
					Figure	25: API key	page				

3. In the Name field type the name of your key (for example - mykey). Choose Grant individual rights and select Link as Gateway to a Gateway for traffic exchange, i.e. read uplink and write downlink.

THE THINOS STACK	Uverview D Applications	Gateways	EU1. Community No support plan <sup>(2)</sup>	•
wisgate-edge-gateway		Gateways > wisgate-edge-gateway > API keys > Add		
· · · · · · · · · · · · · · · · · · ·				
Overview		Add API key		
I. Live data		Name		
Q Location		mykey		
2 Collaborators		Rights* O Grant all current and future rights		
Or API keys		Grant individual rights		
		Select all		
General settings		Delete gateway		
		View gateway information		
		🛃 Link as Gateway to a Gateway Server for traffic exchange, i.e. write uplink and read downlink		
		View gateway location		
		Retrieve secrets associated with a gateway		
		View and edit gateway API keys		
		Edit basic gateway settings		
		View and edit gateway collaborators		
		View gateway status		
		Write downlink gateway traffic		
		Read gateway traffic		
		Store secrets for a gateway		
< Hide sidebar		Create API key		

Figure 26: Generating an API key

4. To generate the key, choose **Create API key**. The following window will pop up, telling you to copy the key you just generated.

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
--	--

#### 

Copy the key and save it in a .txt file (or other), because you won't be able to view or copy your key after that.

5. Click I have copied the key to proceed.

# **Configuring the Gateway**

- 1. To configure the gateway access it via the Web UI. To learn how to do that check out the device's Quickstart Guide 🖾 mentioned before.
- 2. Navigate to LoRa Network > Network Settings > Mode drop-down menu > choose Basics Station.

🏟 RAK°				Logout
				Logoul
Status	LoRaWAN Network Settings			
🐼 Network	Colours FIL	f6e529fff		
🕱 Channel Plan	Galeway Lon Mode			
네 LoRa Network				
Network Settings	Log Level	NOTICE ~		
🗞 Services	Really switch mode?	Switch mode		
🔳 System				
රා WisDM				
			Copyright © RAKWireless Technology Co., Ltd. All	Rights Reserved.

Figure 28: Changing the working mode

- 3. Select **Switch mode** to apply the change. After that, the **Basics Station Configuration** pane settings will show up. To connect the Gateway to TTNv3, the following parameters must be configured:
- Server For server choose LNS Server.
- URI This is the link to The Things Stack server. Note that, for this tutorial, we are connecting the gateway to the European cluster. For Europe fill in the following: wss://eu1.cloud.thethings.network
- Port The LNS Server uses port 8887. Type in 8887.
- Authentication Mode Choose TLS server authentication and Client token. When selected, the trust and the token field will show up.
- trust For trust we will use the Let's Encrypt ISRG ROOT X1 Trust certificate. The file with the certificate can be found here □ .
- token This is the generated API key. The key must start with Authorization:. Example:

Authorization: YOUR\_API\_KEY

#### 📝 NOTE

Replace **YOUR\_API\_KEY** with the key generated previously. Have in mind that there should be a "space" between **Authorization:** and **YOUR\_API\_KEY**, as shown in the example.

🏟 RAK°		Logout
③ Status	LoRaWAN Network Settings	
Network		
(%) Channel Plan	Gateway EUI f66529fff	
네네 LoRa Network	Loo Level NOTICE	
Network Settings	Log Level NOTICE ~	
👶 Services	LoRa Basic Station Basic Station Configuration	
🔳 System	Basic Station	
🛆) WisDM	Dasic Statuon	
	Server       CUPS Boot Server         CUPS Boot Server       CUPS Server         URI       vss./service         Boot       Server         URI       vss./service         Boot       Server         URI       vss./service         Boot       Server         URI       vss./service         Boot       Server         URI       Server Authentication and Client Token         Boot	Apply Reset

Figure 29: LoRa Basics Station settings

4. To save the changes click **Save & Apply**.

You can now see that your gateway is connected to TTNv3 as Basics Station:

THE THINGS STACK Community Edition	Uverview D Applications	🔒 Gateways 🛛 🚢 Organia	zations		EU1 community Fair use policy applies ③	•
wisgate-edge-gateway		Gateways > wisgate-edge-g	ateway			
		nuicesto od	ao astoway			
Overview		wisgate-ed ID: wisgate-edge-g				
II. Live data		↑3 ↓0 • Last activity	6 seconds ago 💿	<u></u>	1 Collaborator 🛛 🗣 1 API key	
Cocation		General information		<ul> <li>Live data</li> </ul>	See all activity →	
Collaborators		Gateway ID	wisgate-edge-gateway	↑ 10:00:18 Receive uplink message JoinEUI: 30	12 1D 8B 87 🗘 🖡	
Or API keys		Gateway EUI	F6 E6 29 FF FE	↑ 10:00:11 Receive uplink message JoinEUI: 30 ↑ 10:00:06 Receive uplink message DevAddr: .		
🕸 General settings		Gateway description	None	↑ 10:00:04 Receive uplink message JoinEUI: 30	12 1D 88 87 ↔ F	
		Created at	Apr 20, 2022 09:55:49	🕫 89:59:58 Receive gateway status Versions: { f	firmware: "", package: "",	
		Last updated at	Apr 20, 2022 09:55:49	\$ 89:59:58 Connect gateway		
		Gateway Server address	eu1.cloud.thethings.network			
		outenay server address		Location	Change location settings →	
		LoRaWAN information				
		Frequency plan	EU_863_870			
		Global configuration	Download global_conf.json			
				No location information available	e	
< Hide sidebar						

#### Figure 30: Successful connection

# LORIOT

In this tutorial, you will learn how to connect RAK7268 WisGate Edge Lite 2 to LORIOT.

LORIOT provides an easy-to-use software platform that enables you to build, operate, and scale a secure IoT network suitable for long-range IoT solution deployments in every part of the world.

# Prerequisites

### Hardware

RAK7268 WisGate Edge Lite 2

### Software

- SSH Client (This tutorial will be done using  $\operatorname{PuTTY} \square$  .)
- LORIOT Account I

# **Registering the Gateway**

1. Log into your LORIOT account.

LORIO T							Frankfurt 💻	Grakwireless.com Community Account	👗 🕞 🏠
Dashboard     Applications     Applications     Solution     Join Servers     Documentation	exe COMMUNITY ACCOUNT      Welcome to LOBIOT Community Account!      You are non part of a world-wide scoppton of LaBUOLV <sup>0</sup> developers. Your derives can use any community gateway to reach our retoresk.      As a resure of for sharing your gateway, we provide you one Pree Network Application.      Bit Mouser      Bit Mouser			★ COMMUNITY ACCOUNT textures     Via account expiration     Assaming among all community gateways     Cone Free Network Application					
â Account ★ Upgrade	Apr 21, 2020, 3:00:00 PM		UPDATE	LORIOT Network Server 6.0 has been released!					
Support	Feb 20, 2020, 1:00:00 PM		1050	Check our release note for more details. Be confident in the delivery of your services and guarantee connectivity for y * Upgrade now to Professional Public Server with 99.9% SLA plus unlimited					
	Gateways of Sample	e network		+ Register a new gateway	✗ Applications			+ Create New A	oplication
	Location	Model	MAC Version	Last Data	Name	App10 BE-7A-25-17	Devices 0		

Figure 31: LORIOT Homepage

2. Go to the **Networks** tab of the main menu on the left. You have the option to select **Simple network**, which is automatically generated when you create your account, or you can create a new one to use. For a beginner, it will be easier to use the **Simple network**.

LORIO T	Networks						Frankfurt <mark>–</mark> Corr	@rakwireless.com nmunity Account	8 🕑
🗲 Back To Dashboard	Networks								
A NETWORKS	Filter by	~							
		Network ID	↓₹ Name	1 Gateways	1† Visibility	11 Country	It city	.↓† zip	lt.
		A0001F3F	Sample network	0	Disabled				
	_								
	Copyright © 2015 - 20	121 LORIOT AG. All rights reserved.					LORIOT   In	iternet of Things at Long Rangi	e   Impressum

Figure 32: Networks List

3. Open the network by clicking once on its name. Then, click the + Add Gateway button.

	Networks > Sample Network				ېت Frankfurt Community Acce	skwireless.com
	Sample network					
MPLE NETWORK	Creation Date	Organization User Access	Roaming ID	Network Organization Uuid	Config	ure
01F3F	3/24/21, 4:05 PM	Disabled	A0001F3F	9f598851-4f7a-4a5d-aded-4cebc38dad2b	Remove I	
					+ Add C	ateway
	Gateways					
	Filter by 🗸					
	Name	1↑ MAC ↓₹ Model	It Version	lî Status	👫 Last Data	
			There are no Gateways associated with this ne	etwork		

Figure 33: Adding a gateway to the network

4. In the list of gateways, find and select RAK7249.

#### 📝 NOTE

If you are using another model gateway from the WisGate Edge series, you still need to select RAK7249 in this list. This won't affect the performance in any way.

LORIO T	E Network > Sample Network > Gateway Registration	Frankfurt	grakwireless.com Community Account	۵ (	<b>•</b>
← Back To Networks	Gateway Registration				
A SAMPLE NETWORK	Requirements and services				1
<b>ftj</b> Map	To register a galeway within the network, you need to provide some limited information about your galeway. This information is used to unuquely laterity your galeway in the network. Upon Registration. • the galeway lassigned to your network • a galeway lassigned to your network • the biology coeffic by our galeway is available to not Byour galeway • the biology coeffic by our galeway is available to the Software section. The LOROT galeway is custom built for all integrated galeways. Select your galeway from the list balow and fill in the required fields.				
					1
	What is your base platform?				
	Radio Front-end     Bits       Bits     Bits       RAX 7249     Priv   RAX 7249 Is fully supported.				
	MAC address of eth0 interface				
	The MAC Address of the Ethernet port can be querified by running Efforting with [] prop Makin command from your device's consoled. A sample output will be similar to ends Lisk enceptithemet Madde Add Oli (F122):4156 Cosy on a pass the highlighted part [six costs separated by colons] from the output of your device console to the input field below. ethol Mac address ABCD 0F12:12:456 Upon sociestical registration, we will provide you with a statup guide for your patentary binary with crystographic keys tied to the MAC address. The keys are tied to the MAC address of the device, and cannot be moved to another device.				
					=
	Gateway Location				-

#### Figure 34: Selecting RAK7249

5. Now, you need to connect to your gateway via SSH. As mentioned, this tutorial will be done with the PuTTY SSH client. Open PuTTY and enter the IP address of your gateway. If your gateway is in AP mode, the address will be 192.168.230.1.

🕵 PuTTY Configuration		?	$\times$
Category:			
Category: Session Category: Session Category: Category: Consection Colours Colours Colours Colours Colours Colours Colours Colours Selection Colours Colours Selection Colours Selection Colours Selection Colours Selection Colours Selection Colours Selection Colours Selection Colours Selection Sele	Basic options for your PuTTY se Specify the destination you want to conner Host Name (or IP address) 192.168.0.114 Connection type: Raw O Telnet O Rlogin O SSH Load, save or delete a stored session Saved Sessions Default Settings Close window on exit: O Always O Never O Only on c	ect to Port 22 H O Se Load Save	1
About Help	Open	Cance	el

Figure 35: PuTTY Configuration

- 6. Log in with your root credentials.
- Default username: root
- Password: root

To get the MAC address of your gateway, run the command:

ifconfig eth0 | grep\_HWaddr

The output should be similar to the following:

eth0	Link encap:Ethernet HWaddr 60:C5:A8:XX:XX	_	_
	<pre>     192.168.0.114 - PuTTY     10gin as: root     root0192.168.0.114's password: </pre>		×
	BusyBox v1.23.2 (2020-12-28 17:16:58 CST) built-in shell (ash)		
	LoraWAN Gateway (1.2.0065_Release r209 20201228)		
	root@RAK7268:~# ifconfig eth0   grep HWaddr eth0 Link encap:Ethernet HWaddr 60:C5:A8: : : root@RAK7268:~#		

Figure 36: Getting the MAC address of the gateway

7. Copy the MAC address and fill it out in the registration form for the gateway in LORIOT. Scroll down and press the **Register RAK7249 gateway** button.

COLORIO T	Ketworks > Sample Network > Gateory Regularition	Frankfurt	Brakwireless.com Community Account	<u> </u>	• *
🗲 Back To Networks	The MIC Address of the Elvernit port can be quarter by running				Τ.
SAMPLE NETWORK	ifcontig ethel   grep Haaddr				
A0001F3F	command from your device's console. A sample output will be similar to				
🕅 Мар	entity (Link encognithement Madri Millori Hill 2014) Copy ond path the highlights part of Links supported by colonal from the output of your device console to the input field balow.				
<b>He</b> map	Copy and particle the righting product and particle of county for other counts of your serve contracte or demonstrations. who Mix address				
	62.C5.X8				
	Upon successful registration, we will provide you with a setup guide for your gateway binary with cryptographic keys tied to this MAC address.				
	The keys are tisd to the MAZ address of the device, and cannot be moved to another device.				
					2
	Gateway Location				
	To provide all users with a reasonable view of the coverage of the network, please provide the address at which the gateway will be placed.				
	When displayed to other users, the location will be offset by a random value to protect your privacy.				
	Choose between these 2 options for setting the position of the gateway.				
	Map Manual Address				
			Kigatu Akapan Satas Refer 63223 Gauge Terme of Los Pare	3-	
	Copyright 9 2015- 2021 LOBIOT AG, All rights reserved.	LORI	OT   Internet of Things at Long Ran	ge   Impressu	im y

Figure 37: Filling out the MAC address

8. The gateway is now registered and you need to add a security layer to the connection. It is provided by LORIOT's Gateway Software. To get it installed, run the following set of commands in the PuTTY.

cd /tmp
wget http://eu1.loriot.io/home/gwsw/loriot-rak-7249-SPI-0-latest.sh -0 loriot-install.sh
chmod +x loriot-install.sh

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

/etc/init.d/sx130x\_lora\_pkt\_fwd disable; /etc/init.d/loriot-gw enable; reboot now

P 192.168.0.114 - PuTTY -	-		×
root@RAK7268:~# cd /tmp root@RAK7268:/tmp# wget http://eul.loriot.io/home/gwsw/loriot-rak-72 est.sh -O loriot-install.sh	49-5	SPI-0-	^ lat
Connecting to eul.loriot.io (52.28.250.46:80) loriot-install.sh 100%  ***********************************	0:00	):00 E	ТА
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 reb Installing LORIOT files done root@RAK7268:/tmp# /etc/init.d/packet forwarder disable ; /etc/init.		oriot-	aw
root@RAK7268:/tmp#			
			~

Figure 38: Installing LORIOT software

Your gateway is now registered and connected to LORIOT.

OP LORIO T	E Networks > Sample Network > 60-C5-A8-FF-FF			@rakwireless.com 🔒 🕞 🏠
+ Back To Sample Network	60-C5-A8-FF-FF-			
60-C5-A8-FF-FF     60CSA3FFFF		Status	Latency	Last Connect
Devices Activity			40 ms	25 Mar 2021 13:33:29 (8 minutes ego)
Nocation	E IIIII S		Last Keep Alive 25 Mar 2021 13:40:33 (a minute ago)	Remote Time Offset a few seconds
🔟 Traffic	and the		Last Data	
Radio	AS CO		25 Mar 2021 13:41:02 (o few seconds ogo)	
茎 System	Connected Version 2.8.1560-JKS-EU1-36			
al GPS	Configure	Uptime (days) Downtime (days)		
📥 Software	Ping	Details		
H4 Log	Tap into data stream	MAC Address	Model	
Alerts	Restart	60:C5:A8:	7249 Concentrator	
	Remove	60-C5-A8-FF-FF	rak_7249	
		Base RAK	Connected Over	
		Connected from IP	Name	
		89.106.101.181	RAK7249	
		Machine mips	Version #1 Mon Dec 28 17:21:09 CST 2020	
		Kernel		
		3.18.45 Network Details		
		Interface #1		
		br-lan 192.168.230.1 Interface #2		
		eth0.2 169.254.20.98		
		Interface #3		
		eth0.2 192.168.0.114		
		Interface #4 apcli0 192.168.0.106		
		Configuration		
		Community Access 🗸	Alert Notifications 🗙	Ignore Data 🗙
		Antennas		
		Region		•

Figure 39: Successful Connection

Last Updated: 7/29/2022, 10:17:19 PM