RAK7249 LoRaWAN Network Server Guide

AWS IoT Core for LoRaWAN

Execute the following steps to set up your AWS account and permissions:

Set up Roles and Policies in IAM

Add an IAM Role for CUPS Server

Adding an IAM role will allow the Configuration and Update Server (CUPS) to handle the wireless gateway credentials.

This procedure needs to be done only once, but must be performed before a LoRaWAN gateway tries to connect with AWS IoT Core for LoRaWAN.

- 1. Go to the IAM Roles page on the IAM console.
- 2. Choose Create role.
- 3. On the Create Role page, choose **Another AWS account**.
- 4. Enter your Account ID, then select Next: Permissions.

5. In the search box next to the Filter Policies, type AWSIoTWirelessGatewayCertManager.

- If the search results show the policy named *AWSIoTWirelessGatewayCertManager*, select it by clicking the checkbox.
- If the policy does not exist, create one.
 - Go to the IAM console.
 - Choose Policies from the navigation pane.
 - Choose Create Policy, then select the JSON tab to open the policy editor.
 - Replace the existing template with trust policy document.

]

}

- Choose **Review Policy** to open the Review Page.
- For the Name, type AWSIoTWirelessGatewayCertManager.

🖓 ΝΟΤΕ

You must enter the name as *AWSIoTWirelessGatewayCertManager* and must not use a different name. This is for consistency with future releases.

- For the Description, enter a description of your choice.
- Then choose **Create policy**. You will see a confirmation message showing the policy has been created.
- 6. Choose Next: Tags, then Next: Review.
- 7. In Role name, enter *IoTWirelessGatewayCertManagerRole*, and then choose to Create role.

🖓 ΝΟΤΕ

You must not use a different name. This is for consistency with future releases.

- 8. In the confirmation message, choose *IoTWirelessGatewayCertManagerRole* to edit the new role.
- 9. In the Summary, choose the Trust relationships tab, and then choose Edit trust relationship.

10. In the **Policy Document**, change the **Principal** property to represent the IoT Wireless service:

```
"Principal": {
"Service": "iotwireless.amazonaws.com"
},
```

• After changing the Principal property, the complete policy document should look like the following:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal": {
        "Service": "iotwireless.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {}
        }
        ]
}
```

11. Choose **Update Trust Policy** to save your changes and exit. At this point, you have created the *IoTWirelessGatewayCertManagerRole* and you won't need to do this again.

The examples in this document are intended only for dev environments. All devices in your fleet must have credentials with privileges that authorize only intended actions on specific resources. The specific permission policies can vary for your use case. Identify the permission policies that best meet your business and security requirements. For more information, refer to **Example Policies** and **Security Best Practices**

Add IAM Role for Destination to AWS IoT Core for LoRaWAN

Creating a Policy

Creating a policy gives the role permissions to describe the IoT endpoint and publish messages to AWS IoT.

- 1. Go to the IAM console.
- 2. Choose **Policies** from the navigation pane.
- 3. Choose **Create Policy**, then choose the **JSON** tab to open the policy editor. Replace the existing template with this trust policy document:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Action":
    [
        "iot:DescribeEndpoint",
        "iot:Publish"
],
    "Resource": "*"
        }
        ]
}
```

- 4. Choose **Review Policy** to open the Review page.
- 5. For **Name**, enter a name of your choice.
- 6. For **Description**, enter a description of your choice.
- 7. Choose **Create policy**. You will see a confirmation message indicating that the policy has been created.

Creating the Role

- 1. In the IAM console, choose Roles from the navigation pane to open the Roles page.
- 2. Choose Create Role.
- 3. In Select type of trusted entity, choose Another AWS account.
- 4. In Account ID, enter your AWS account ID, and then choose Next: Permissions.
- 5. Search for the IAM policy you just created by entering the policy name in the search bar.
- 6. In the search results, select the checkbox corresponding to the policy.
- 7. Choose Next: Tags.
- 8. Choose Next: Review to open the Review page.
- 9. For **Role name**, enter an appropriate name of your choice.
- 10. For **Description**, enter a description of your choice.
- 11. Choose **Create role**. You will see a confirmation message indicating that your role has been created.

Updating your Trust Policy

Update your role's trust relationship to grant AWS IoT Core for LoRaWAN permission to assume this IAM role when delivering messages from devices to your account.

- 1. In the IAM console, choose **Roles** from the navigation pane to open the Roles page.
- 2. Enter the name of the role you created earlier in the search window, and click on the role name in the search results. This opens up the Summary page.
- 3. Choose the **Trust relationships table** to navigate to the Trust relationships page.
- 4. Choose **Edit trust relationship**. The principal AWS role in your trust policy document defaults to root and must be changed. Replace the existing policy with this:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "",
        "Effect": "Allow",
        "Principal": {
        "Service": "iotwireless.amazonaws.com"
    },
        "Action": "sts:AssumeRole",
        "Condition": {}
        }
        ]
    }
```

5. Choose **Update Trust Policy.** Under Trusted entities, you will see: *The identity provider(s) iotwireless.amazonaws.com*.

Add the Gateway to AWS IoT

Requirements

To complete setting up your gateway, you need the following:

- LoRaWAN region. For example, if the gateway is deployed in a US region, the gateway must support LoRaWAN region US915.
- Gateway LNS-protocols. Currently, the LoRa Basics Station protocol is supported.
- Gateway ID (GatewayEUI) or serial number. This is used to establish the connection between the LNS and the gateway. Consult the documentation for your gateway to locate this value.
- Add minimum software versions required, including Basics Station 2.0.5.

Add the LoRaWAN Gateway

To register the Gateway with AWS IoT Core for LoRaWAN, execute these steps:

- 1. Go to the AWS IoT console.
- 2. Select **Wireless connectivity** in the navigation panel on the left.
- 3. Choose Intro, and then choose Get started. This step is needed to pre-populate the default profiles.
- 4. Under Add LoRaWAN gateways and wireless devices, choose Add gateway.
- 5. In the Add gateway section, fill in the GatewayEUI and Frequency band (RF Region) fields.
- 6. Enter a descriptive name in the **Name** optional field. It is recommended that you use the GatewayEUI as the name.
- 7. Choose Add gateway.

- 8. On the Configure your Gateway page, find the section titled Gateway certificate.
- 9. Select Create certificate.
- 10. Once the **Certificate created and associated with your gateway** message is shown, select **Download certificates** to download the certificate (*xxxxx.cert.pem*) and private key (*xxxxx.private.key*).
- 11. In the section **Provisioning credentials**, choose **Download server trust certificates** to download the **CUPS (cups.trust)** and **LNS (Ins.trust)** server trust certificates.
- 12. Copy the CUPS and LNS endpoints and save them for use while configuring the gateway.
- 13. Choose **Submit** to add the gateway.

Add a LoRaWAN Device to AWS IoT

Requirements:

- Locate and note the following specifications about your endpoint device.
 - LoRaWAN Region: This must match the gateway LoRaWAN region. The following Frequency bands (RF regions) are supported: o EU868 o US915 o EU433
 - MAC Version: This must be one of the following: o V1.0.2 o v1.0.3 o v1.1
 - OTAA v1.0x and OTAA v1.1 are supported.
 - ABP v1.0x and ABP v1.1 are supported.
- Locate and note the following information from your device manufacturer:
 - For OTAA v1.0x devices: DevEUI, AppKey, AppEUI
 - For OTAA v1.1 devices: DevEUI, AppKey, NwkKey, JoinEUI
 - For ABP v1.0x devices: DevEUI, DevAddr, NwkSkey, AppSkey
 - For ABP v1.1 devices: DevEUI, DevAddr, NwkSEnckey, FNwkSIntKey, SNwkSIntKey, AppSKey

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.

- 1. Navigate to the AWS IoT console. In the navigation pane, choose Wireless connectivity.
- 2. In the navigation pane, choose **Profiles**.
- 3. In the **Device Profiles** section, there are some pre-defined profiles listed.
- 4. Check each of the profiles to determine if one of them will work for you.
- 5. If not, select **Add device profile** and set up the parameters as needed. For US 915 as an example, the values are:
 - MacVersion 1.0.3
 - RegParamsRevision RP002-1.0.1
 - MaxEirp 10
 - MaxDutyCycle 10

- RfRegion US915
- SupportsJoin true
- 6. Continue once you have a device profile that will work for you.
- 7. In the **Service Profiles** section, there are some pre-defined profiles listed. Check each of the profiles to determine if one of them will work for you.
- 8. If not, select Add service profile and set up the parameters as needed. As an example, the default service profile parameters are shown below. However, only the AddGwMetadata setting can be changed at this time.
 - UIRate 60
 - UlBucketSize 4096
 - DIRate 60
 - DIBucketSize 4096
 - AddGwMetadata true
 - DevStatusReqFreq 24
 - DrMax 15
 - TargetPer 5
 - MinGwDiversity 1
- 9. Proceed only if you have a device and service profile that will work for you.

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 on Destinations, refer to the AWS LoRaWAN Developer Guide.

A destination consists of a Rule and a Role. To set up the destination, execute the following steps:

- 1. Navigate to the AWS IoT console. In the navigation pane, choose **Wireless connectivity**, and then **Destinations**.
- 2. Choose Add Destination.
- 3. On the Add destination page, in the **Permissions** section, select the IAM role you had created earlier, from the drop-down.
- 4. Under **Destination details**, enter *ProcessLoRa* as the Destination name, and an appropriate description under **Destination description optional**.

\bigcirc note

The Destination name can be anything. For getting started and consistency, choose ProcessLoRa for the first integration with AWS IoT Core for LoRaWAN.

5. For Rule name, enter LoRaWANRouting. Ignore the section Rules configuration – Optional for now. The Rule will be set up later in the "Hello World" sample application. See Create the IoT Rule for the destination.

6. Choose **Add Destination**. You will see a message "*Destination added*", indicating the destination has been successfully added.

Register the Device

Now, register an endpoint device with AWS IoT Core for LoRaWAN as follows:

- 1. Go to the AWS IoT console.
- 2. Select **Wireless connectivity** in the navigation panel on the left.
- 3. Select **Devices**, then choose **Add wireless device**.
- 4. On the **Add device** page, select the LoRaWAN specification version in the drop-down under **Wireless device specification**.
- 5. Under LoRaWAN specification and wireless device configuration, enter the DevEUI and confirm it in the Confirm DevEUI field.
- 6. Enter the remaining fields as per the OTAA/ABP choice you made above.
- 7. Enter a name for your device in the Wireless device name optional field.
- 8. In the **Profiles** section, under **Wireless device profile**, find a drop-down option that corresponds to your device and region.

🖓 ΝΟΤΕ

Compare your device details to ensure the device profile is correct. If there are no valid default options, you will have to create a new profile. See the Verify Profiles section.

- 9. Choose Next.
- 10. Choose the destination you created earlier (*ProcessLoRa*) from the drop-down under **Choose destination**.
- 11. Choose Add device.
- 12. You will see a message saying "*Wireless device added*", indicating that your device has been set up successfully.

Set up the Gateway

- Set up the Gateway Hardware
- Set up the Gateway Software

Configure the Gateway Device

- 1. 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





Figure 1: Web User Interface Log-in

2. The firmware version 1.2.0065_Release_r209 on the gateway supports AWS IoT Core for LoRaWAN, and it can be verified on **Status** > **Overview** > **System** > **Firmware Version**.

@RAK		
Status		
Overview		
LoRa Packet Logger System Log	System	
Firewall	Hostname	RAK7240
⊠ Network	Model	RAK7240
^(A) Channel Plan	SN	9181001219030654
	Firmware Version	1.2.0065_Release r209
LoRa Network	Local Time	Tue Jan 5 05:25:13 2021
Services	Uptime	5d 20h 10m 11s
	Load Average	0.06, 0.04, 0.03
System	GPS	-

Figure 1: Checking the Firmware Version

3. If the firmware version is prior to 1.2.0065_Release_r209, upgrade the firmware. Navigate to **System** > **Backup/Flash Firmware** > **Flash new firmware image** > **Upgrade the firmware**.

🏟 RAK°	Logout
🏵 Status	Flash operations
영 Network	Backup / Restore
(Å) Channel Plan	Ciele "Consume analytics" to designed a tax analytics of the summant as from units of the first units to its initial state alide "Deeferm wood" (ash, woodide with
Ш LoRa Network	squashfs images).
🗞 Services	Download backup: Generate archive
圈 System	Reset to defaults: Perform reset
System	To restore configuration files, you can upload a previously generated backup archive here.
Administration	Restore backup: Choose File No file chosen Upload archive
Backup / Flash Firmware	
Reboot	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).
	Keep settings: Z
	Image: Choose File No file chosen Flash image

Figure 1: Flashing the firmware

- 4. Configure Network Mode to Basic Station. Navigate to LoRa Network then Network Settings.
 - Change the Mode in LoRaWAN Network Settings to Basic Station.
 - Select LNS Server from Server, then choose TLS Server and Client Authentication from Authentication Mode.

ର୍କ୍ତ RAKଂ			Logout
🎯 Status	LoRaWAN Network Settings		
🐼 Network	Colourse Filler	co E 000 761462	
'္ధ') Channel Plan	Gateway EUT	Bacio Station	
للسا LoRa Network	Log Level	NOTICE V	
Network Settings			
🗞 Services	LoRa Basic Station Basic Station Configuration		
l System	Basic Station		
	Server	CUPS Boot Server	
		CUPS Server	
		LNS Server	
	URI		
	Port		
	Authentication Mode	No Authentication ~	
			Save & Apply Reset

Figure 1: Configuring Network Mode to Basic Station

5. Configure URI, Port, and Authentication Mode.

🏟 RAK'		Logout	a	Services V	Q. Search for services, features, marketplace products, and docs [Alt+S]	
Status Status Status Active Status Second Secon	LoRaiWAN Network Settings Galeway EUI 60:538ffor61462 Mode Basic Station Log Level NOTCE LoRa Basic Station Basic Station Configuration Basic Station Server CUPS Boot Server CUPS Boot S	Lopout	=	Services AWS IoT Mode gateway Step 2 Configure your gateway	Q Setter har services, Retainers marketplace products and dots (Att-5) (Att-5) (Att-2) (Att-	3
	Note Million (Section Control (Sec	MIRICAST TURNING MATCH AND BEAK AND			Provisioning credentials intel Descere the regions that your gateway supports. Then, copy the endpoint and download the surver truct certificate to that you can add proving subsets. CUP5 (Configuration and Update Server) endpoint https://JASEL4/TSTITHP.cups.iorwan.us-east-1,imazonaes.com:445 Copy UK (LokuWAN Network Server) andpoint mst://JASEL4/TSTITHP.gateway.lochwan.us-east-1,imazonaes.com:445 Copy Server truct certificates Copy Overentials your surver to too: certificate to you can uplicad the certificate for the endpoint your gateway supports. Copy Overentials erver truct certificates Control configuration Copy	

Figure 1: Configuring URI, Port, and Authentication Mode

6. Verifying Operation. Check if the gateway is online in AWS IoT console.

LoRaWAN specific detai	LoRaWAN specific details						
GatewayEUI	RFRegion	LastUplinkReceivedAt	Connection status	JoinEuiFilters	NetIdFilters	SubBands	
ac1f09ff	EU868	June 07, 2022, 10:26:33 (UTC+0300)	Connected	-	-	-	

Figure 1: Verifying Operation

Add End Devices

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

1. Add Device Profile.

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 OTA customized your profile per your device vendor specification	A device class and your LoRaWAN radio frequency band. You may need to
EU868 - A	▼
Device profile name Type a descriptive name for this device profile.	Frequency band (RFRegion) Choose the LoRa supported frequency band for this profile.
rak4200	EU868

The MACVersion of the LoRaWAN devices that use this profile.	Select the region parameters version identifier for this profile.
1.0.3	RP002-1.0.1 (recommended)
MaxEIRP Enter the MaxEIRP value for this device profile.	
5	
Supports Class B Choose to enter the values for Class B support.	
Supports Class C Choose to enter the values for Class C support.	
Supports Join Choose to enter the values for Join support (OTAA) or not (ABP).	

Figure 1: Adding the Device Profile

2. Add Service Profile.

d service	profile			
ervice profile service profile descri	Info bes the features that are enabled	for the user(s), and the rate of me	ssages that can be se	nt over the network.
ervice profile nam	e - <i>optional</i> file name.			
rak4200-test				
AddGWMetaD Add additional g	ata ateway metadata (RSSI, SNR, GW	geoloc., etc.) to the packets sent b	by devices.	
AddGWMetaE Add additional (ags - optional tag is a label that yo pur resources or track	ata ateway metadata (RSSI, SNR, GW assign to an AWS resource. Eacl your AWS costs.	geoloc., etc.) to the packets sent b	by devices. Mal value. You can us	e tags to search and filter
AddGWMetaE Add additional (aggs - optional tag is a label that yo our resources or track	ata ateway metadata (RSSI, SNR, GW assign to an AWS resource. Each your AWS costs.	geoloc., etc.) to the packets sent b a tag consists of a key and an option e.	by devices. Inal value. You can us	e tags to search and filter
AddGWMetaE Add additional ('ags - optional tag is a label that yo sur resources or track ou don't have any Add new tag	ata ateway metadata (RSSI, SNR, GW u assign to an AWS resource. Each your AWS costs. tags attached to this resource	geoloc., etc.) to the packets sent b a tag consists of a key and an option e.	by devices. Inal value. You can us	e tags to search and filter
AddGWMetaE Add additional g ags - optional tag is a label that yo our resources or track ou don't have any Add new tag	ata ateway metadata (RSSI, SNR, GW) assign to an AWS resource. Each your AWS costs. tags attached to this resource ags.	geoloc., etc.) to the packets sent b	by devices. Inal value. You can us	e tags to search and filter

Figure 1: 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.

d desti	nation Info
Permissions	Info
AM Role Thoose an existing	IAM Role or create a new one. How to create an IAM Role.
RAK-AWS-EVA	details Info
RAK-AWS-EVA	details Info e ne appears in the device and gateway destination selection lists.
RAK-AWS-EVA	details Info e ne appears in the device and gateway destination selection lists.
Pestination nam he destination nam ProcessLoRa Destination desc provide a helpful d	details Info e ne appears in the device and gateway destination selection lists. ription - optional escription of your destination.

LoRaWANRouting	Сору	

Figure 1: 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 at+get_config=lora:status to obtain the information.

For more AT commands, refer to the RAK4200 AT Command Manual.

```
at+get_config=lora:status\r\n
OK Work Mode: LoRaWAN
Region: EU868
Send_interval: 600s
Auto send status: false.
MulticastEnable: true.
Multi Dev Addr: 260111FD
Multi_Apps_Key: F13DDFA2619B10411F02F042E1C0F356
Multi_Nwks_Key: 1D1991F5377C675879C39B6908D437A6
Join_mode: OTAA
DevEui: 00000000000888
AppEui: 00000000000888
AppKey: 00000000000088800000000000888
Class: C
Joined Network: false
IsConfirm: unconfirm
AdrEnable: true
EnableRepeaterSupport: false
RX2_CHANNEL_FREQUENCY: 869525000, RX2_CHANNEL_DR:0
RX_WINDOW_DURATION: 3000ms
RECEIVE_DELAY_1: 1000ms
RECEIVE_DELAY_2: 2000ms
JOIN_ACCEPT_DELAY_1: 5000ms
JOIN_ACCEPT_DELAY_2: 6000ms
Current Datarate: 4
Primeval Datarate: 4
ChannelsTxPower: 0
UpLinkCounter: 0
DownLinkCounter: 0
```

levice	Add device					
2 ose destination	LoRaWAN specification and wireless device	LoRaWAN specification and wireless device configuration Info				
	Wireless device specification Your device specifications consist of the LoRaWAN version (1.1 o Authentication By Personalization). Once selected, your data is e	r 1.0.x) and your authentication process (Over The Air Authentication or ncrypted with a key that AWS owns and manages for you.				
	OTAA v1.0.x	▼				
	DevEUI	Confirm DevEUI				
	0000000000888	00000000000888				
	The 16-digit hexadecimal DevEUI value found on your wireless device.	Reenter the DevEUI.				
	АррКеу	Confirm AppKey				
	0000000000088800000000000888	0000000000088800000000000888				
	The 32-digit hexadecimal AppKey value that your wireless device vendor provided.	Reenter the AppKey.				
	AppEUI	Confirm AppEUI				
	0000000000888	00000000000888				
	The 16-digit hexadecimal AppEUI that your wireless device vendo provided.	Reenter the AppEUI.				
	Wireless device name - optional					
	rak4200-test					
	A descriptive name to make the wireless device easier to locate.					
	Wireless device description - optional					

A helpful description of your wireless device.

Figure 1: LoRaWAN specifications and wireless device configuration

Thin	g association Info	
	Associate a thing with your wireless device We'll create a thing in AWS IoT for you and associate it with this device. Things in AWS IoT can make it easier to search for and manage your devices.	
Prof	iles	
Choose	e a wireless device profile so your device can pass the correct messages to your gateway.	•
Servic	re profile e a service profile.	·
rak4	l200-test	•

Figure 1: Choosing a Wireless Device Profile

AWS IOT > Wireless connectivity > Wireless devices > Add device							
Step 1 Add device	Choose destination						
Step 2 Choose destination	Choose destination						
	Destination name Destinations route LoRaWAN messages from your wireless device to other AWS services. ProcessLoRa						
	Cancel Previous Add device						

Figure 1: Choosing a Destination

5. Restart the end Device, and it should join the AWS IoT LoRaWAN server.

EVENT:0:STARTUP								
SYSLOG:4:0TAA	Join	Request						
SYSLOG:4:0TAA	Join	Success						
EVENT:1:JOIN_NETWORK								
SYSLOG:4:LoRa	Tx :							

AWS IOT > Wireless connectivity > Wireless devices				
LoRaWAN Sidewalk				
LoRaWAN devices (1) Info			Edit Delete	Add wireless device
				< 1 >
Device ID	Name	Destination	Last Uplink Received At	•
0	rak4200-test	ProcessLoRa	February 09, 2021, 11:29:28 (UTC+0800)	

Figure 1: Choosing a Destination

6. Use the AT command at+send:lora:1:1234567890 to send an uplink message.

Here is the console log after sending uplink message.

```
1
OK
SYSLOG:4:LoRa Tx : 1234567890
EVENT:3:LORA_TX_DONE:1:OK
```

Verifying Operation

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.



Figure 1: Sending Uplink Architecture

Create a Lambda Function for Destination Rule

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

- 1. Go to the AWS Lambda console.
- 2. Click on **Functions** in the navigation pane.
- 3. Click on Create function.
- 4. Select Author from scratch.
- 5. Under **Basic Information**, enter the function name and choose *Runtime Python 3.8*. from the dropdown under **Runtime**.
- 6. Click on Create function.
- 7. Under Function code, paste the copied code into the editor under the *lambda_function.py* tab.
- Click to view the code
- 8. Once the code has been pasted, choose **Deploy** to deploy the lambda code.
- 9. Click on the **Permissions** tab of the lambda function.
- 10. 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.

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

}

]

• Choose Review Policy, then Save changes.

11. Create a test event that will allow you to test the functionality of the lambda function.

- In the drop-down, for the *Select a test event*, 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:

```
{
"WirelessDeviceId": "65d128ab-90dd-4668-9556-fe47c589610b",
"PayloadData": "AWf/1w==",
"WirelessMetadata": {
"LoRaWAN": {
"DataRate": "4",
"DevEui": "000000000000088",
"FPort": 1,
"Frequency": "868100000",
"Gateways": [
        {
"GatewayEui": "80029cffXXXXXXX",
"Rssi": -109,
"Snr": 5
        }
    ],
"Timestamp": "2021-02-08T04:00:40Z"
    }
}
}
```

- 12. Choose **Create** to save the event.
- 13. Navigate to the AWS IoT console, choose **Test** on the navigation pane, and select **MQTT client**.
- 14. Configure the MQTT client to subscribe to "#" (all topics).
- 15. Click on **Test** in the Lambda function page to generate the test event you just created.
- 16. 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:

```
00000000000000088/project/sensor/decoded February 09, 2021,
14:45:29 (UTC+0800)
{
    "devEui": "0000000000000088",
    "fPort": 1,
    "freq": "868100000",
    "timestamp": "2021-02-08T04:00:40Z",
    "temperature": -4.1
}
```

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, enter as follows:
 - Name: LoRaWANRouting
 - Description: Any description of your choice.

Ο ΝΟΤΕ

The **Name of your Rule** is the information 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:lora:1:01670110.
- You should see traffic similar to that shown below.

```
393331375d387505/project/sensor/decoded February 09, 2021,
14:47:21 (UTC+0800)
{
    "devEui": "393331375d387505",
    "fPort": 1,
    "freq": "867100000",
    "timestamp": "2021-02-09T06:47:20Z",
    "temperature": 27.2
  }
```

```
February 09, 2021, 14:47:21 (UTC+0800)
project/sensor/decoded
   {
       "WirelessDeviceID": "6477ec22-9570-31d5981da021",
       "PayloadData": "AWcBEA==",
       "WirelessMetadata": {
           "LoRaWAN": {
               "DataRate": "4",
               "DevEui": "393331375d387505",
               "FPort": 1,
               "Frequency": "867100000",
               "Gateways": [
                   {
                        "GatewayEui": "ac1ff09fffe014bd5",
                        "Rssi": -103,
                        "Snr": 8.5
                   }
               ],
               "Timestamp": "2021-02-09T06:47:20Z"
           }
       }
   }
```

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.
 - 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.
- 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 as time FROM '+/project/sensor/decoded' where temperature > 25

- 6. 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: at+send:lora:1:01670110. Here is the message from mobile after sending an uplink message.

```
{
    "device_id": "393331375d387505",
    "message": "Temperature exceeded 25",
    "temp": 27.2,
    "time": "2021-02-22T07:58:54Z"
}
```

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.
- 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/{WirelessDeviceId}** and a base64-encoded message.

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

Figure 1: Specifying a topic

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

<pre>{ "sendresult": { "status": 200, "RequestId": "4f1d36e1-8316-4436-8e9d-2207e3711755", "MessageId": "60223529-0011d9f5-0095-0008", "ParameterTrace": { "PayloadDate": "QQ==", "WirelessDeviceId": "6477ec22-9570-4fea-9668-31d5981da02 "Fport": 1, "TransmitMode": 1 } } } downlink/status/6477ec22-9570-4fea-9668-31February 09.2021, 150829 (UT<=0000) Exper: Hde f</pre>	downlink/status/6477ec22-9570-4fea-9668-31d5981da021 Fe 021, 15:09:29 (UTC+0800)	ebruary	09,
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", "Message1d": "60223529-0011d9f5-0095-0008", "ParameterTrace": { "ParameterTrace": { "rayloadbata": "00e=", "Yayloadbata": "0477ec22-9570-4fea-9668-31d5981da021", ""Parametice: 1 "inansmitMode": 1 ;	<pre>{ "sendresult": { "status": 200, "RequestId": "4f1d36e1-8316-4436-8e9d-2207e371175 "MessageId": "60223529-0011d9f5-0095-0008", "ParameterTrace": {</pre>	55", -31d5981	.da021",
)) 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. Export Hide	<pre>downlink/status/6477ec22-9570-4fea-9668-31February 09, 2021, 15:09:29 (UTC+0800) {</pre>	Export Hide	
QQ==	<pre> } cmd/downlink/6477ec22-9570-4fea-9668-31d February 09, 2021, 15:09:29 (UTC+0800) We cannot display the message as JSON, and are instead displaying it as UTF-8 String. 00== </pre>	Export Hide	

Figure 1: 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. 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 Choose Quick Create*.
- 11. Once the Quick Create Finished message is displayed, choose Add action.
- 12. 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.
- 2. In the navigation panel, choose Data sets.
- 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 Learning-powered 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.
- 8. 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.

Testing your "Hello Word" Application

Using your device, create a condition to generate an event such as a high-temperature condition. If the temperature is above the configured threshold then you will receive a text alert on your phone. This alert will include key parameters about the alert.

You can also visualize the data set as follows:

- 1. Go to the AWS IoT Analytics console.
- 2. Choose Data sets.
- 3. Select the dataset created earlier.
- 4. Select **Content** and ensure there are at least few uplink entries available in the data set.
- 5. Go to the QuickSight console.
- 6. Choose New analysis.
- 7. Choose the dataset created in Create an IoT Analytics Rule.
- 8. Select time on the X-axis, Value as temp (Average) and Color as device_id to see a chart of your dataset.

Debugging

After login to the device using the web browser, the system log can be viewed from Status > System Log.

🏟 RAK	AUTO REFRESH ON Logout
Status	System Log
Overview LoRa Packet Logger System Log 4 Firewall	Tue Feb 90831110 2021 kem.info quected-CM[1165]: requestRegistrationState2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Tue Feb 90831110 2021 kem.info quected-CM[1165]: requestRegistrationState2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Tue Feb 9083111 2021 user.info quected-CM[1165]: requestRegistrationState2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Tue Feb 9083111 2021 user.info quected-CM[1165]: requestRegistrationState2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Tue Feb 9083111 2021 user.info quected-CM[1165]: requestRegistrationState2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Tue Feb 9083111 2021 user.info quected-CM[1165]: requestRegistrationState2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Tue Feb 9083115 2021 kem.info quected-CM[1165]: requestRegistrationState2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Tue Feb 9083115 2021 kem.info quected-CM[1165]: requestRegistrationState2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW
Network	Tue Feb 9 08:31:16 2021 daemon.info dnemasq-dhop[1744]; DHCPREQUEST[or-lan] 192;168:230:227 10:18:98:4b:4c:07 Tue Feb 9 08:31:16 2021 daemon.info dnemasq-dhop[1744]; DHCPRACK[or-lan] 192;168:230:227 10:18:98:4b:4c:07 Tue Feb 9 08:31:19 2021 use.info basicstation[1471]; ISYNINFON MUCUSX1300 xidth stats: min+ 1,00m d80; +2.900m max; +8.700m - threshold d90; -3.800m
(A) Channel Plan	Tue Feb 9 08:31:19 2021 userinfo basicstation[1471]; ISYN:INFO] Mean MCU drift vs SX130X40: 1.6ppm Tue Feb 9 08:31:19 2021 userinfo basicstation[1471]; ISYN:INFO] Mean MCU drift vs SX130X40: 1.6ppm Tue Feb 9 08:31:19 2021 userinfo basicstation[1471]; ISYN:INFO] Mean MCU drift vs SX130X40: 1.6ppm Tue Feb 9 08:31:19 2021 userinfo basicstation[1471]; ISYN:INFO] Mean MCU drift vs SX130X40: 1.6ppm
LoRa Network	Tue Feb 908:31:19 2021 teer.debug basistation[14:7]; apr;XDEB] Dropped frame without CHC or with broken CHC Tue Feb 908:31:20 2021 kern.info quectel-CM[1185]; requestRegistrationState2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Tue Feb 908:31:20 2021 kern.info quectel-CM[1185]; DailFailed 9
🗞 Services	Tue Feb 9 08:31:25 2021 kern.info quectel-CM[1185]: requestRegistrationState2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Tue Feb 9 08:31:25 2021 kern.info quectel-CM[1185]: Dail Failed 10
System	Tue Feb 9 08:31:30 2021 kem.info guectel-CM[1165]: requestRegistrationState2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Tue Feb 9 08:31:30 2021 kem.info guectel-CM[1165]: Dail Failed 11 Tue Feb 9 08:31:35 2021 use.info basicstation[1471]; ISYNINFO] Time symc gualities: min=62 q90=106 max=112 (previous q90=2147483647)
	Ture Feb 90831:d5 2221 user/info basicatation(1471); [SYNERFO] Preparet decasces/sector/doi: [Oravious q00-2147483647) Ture Feb 90831:35 2221 user/info basicatation(1471); [SYNERFO] (Papetated secosces) ecoloc drifts between MCUCX430X00 (Partie)d: 4.5ppm (Preshold 3.8ppm) Ture Feb 90831:36 2021 term.info quected-CM[1165; pagetsfeator/state2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Ture Feb 90831:36 2021 user/info basicatation(1471); [SNLENFO] RX mod=LORA f=88830000 bw=125 sz=122 d=-2 & & ADA87290834887003C66A944E9381F0FC6802784E0B5F04C30DC3043250F1E6611B55F79260F192C0D1F38140540DCEF3D3B0B4CF07175EAF2F90FD9E Ture Feb 90831:36 2021 user/info quected-CM[1165]; pagetsfeator/state2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Ture Feb 90831:46 2021 kern.info quected-CM[1165]; pagetsfeator/state2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Ture Feb 90831:46 2021 kern.info quected-CM[1165]; pagetsfeator/state2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Ture Feb 90831:46 2021 kern.info quected-CM[1165]; pagetsfeator/state2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Ture Feb 90831:46 2021 kern.info quected-CM[1165]; pagetsfeator/state2 MCC: 466, MNC: 97, PS: Detached, DataCap: UNKNOW Ture Feb 90831:46 2021 kern.info quected-CM[1471]; [LOCSINFO] logger mad data: cutrycycle Ture Feb 90831:59 2021 user.info basicatation[1471]; [LOCSINFO] logger mad data: cutrycycle Ture Feb 90831:59 2021 user.info basicatation[1471]; [LOCSINFO] logger mad data: cutrycycle Ture Feb 90831:59 2021 user.info basicatation[1471]; [LOCSINFO] logger mid data: cutrycycle

Troubleshooting

- 1. Unable to see the web login:
 - Check that your wifi is connected to RAK7249_XXXX.
 - Try ping **192.168.230.1**.
- 2. Lost password to login to the web login.
 - Hold the reset button for 10 seconds to factory reset the device



Figure 1: Troubleshooting

The Things Network v3 (TTNv3)

In this section, it will be shown how to connect RAK7249 WisGate Edge Max to TTNv3.

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

() THE THINGS ID
THE THINGS STACK Community Edition
Sign in with The Things ID Don't have an ID? Sign up for free
Password &
Login with The Things ID Forgot password

Figure 1: The Things Stack Home Page

Register 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).

THE THINGS NETWORK	THE THINGS STACK Community Edition	• Overview Applications	🚢 Gateways 🛛 🎎 Organizations		EU1 Community No support plan ⑦	•
			Wel Get started right away Need help? Have a	ook at our 웹 Documentation ☞ or <u>Get support</u> ☞.		
				°		
			Create an application	Register a gateway		

Figure 1: Console Page after a successful login

- 2. You will be redirected to the **Register gateway** page.
- 3. In the Gateway EUI field type the EUI of the 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.

THE THINGS NET WORK	THE THINGS STACK Community Edition	Overview	Applications	📑 Gateways	🚢 Organizations			⊕ N	EU1 Community to support plan ③		
			Register ga Register your gatewa Learn more in our gu	ateway ay to enable data t aide on Adding	raffic between nearby en Gateways ^亿 .	end devices and the network.					
			Owner*								
			Gateway EUI ③		Continue without EUI						
			To continue, please	confirm the Gatew	ay EUI so we can determ	mine onboarding options					
© 2022 The Th	ings Stack by The Things Network	and The Things Inc	lustries				⊕ EN	v3.22.2 (3203f63b2)	Documentation	Status page	Get support

Figure 1: Register gateway

- 4. After typing the EUI, click on Confirm. Additional fields will pop up. Fill in the following information:
- Gateway ID This will be the unique ID of your gateway in the Network. An ID based on the EUI is automatically generated. You can changed it if you need. Note that the ID must contain only lowercase letters, numbers, and dashes (-).

- Gateway name Optionally, you can type a name for your gateway.
- Frequency plan The frequency plan used by the gateway.

🖓 ΝΟΤΕ

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

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

THE THINGS NET WORK	THE THINGS STACK Community Edition	Overview	Applications	ᡖ Gateways	K Organizations				EU1 Communit No support plan (2)	
			Register ga Register your gatewa Learn more in our gu	teway Iy to enable data to Iide on 📓 <u>Adding (</u>	raffic between nearby end device <u>Gateways</u> ^亿 .	es and the network.				
			Owner*		~	·				
			Gateway EUI 📎	1.11.11.00	Reset					
			Gateway ID ⑦ *							
			My new gateway							
			Select	icated connection	~	•				
			Choose this option e	g. if your gateway	is powered by LoRa Basic Station	<u>n</u> 2				
			Select which informa Share status wit Share location w	ation can be seen t hin network ⑦ vithin network ⑦	by other network participants, in	ncluding <u>Packet Broker</u> 너				
			Register gatewa	у						
@ 2022 The Th	ings Stack by The Things Networ	cand The Things Ir	dustries					(IN 132221	3203f63h2) Documentation	Status narre 🔗 Get sunnort

Figure 1: Adding a gateway

5. To register your gateway click **Register gateway**.

THE THINGS NET WORK	THE THINGS STACK Community Edition	Second Se	📑 Gateways 🛛 🚢 Organiz	rations		EU1 Community No SLA applicable ⑦	•
🔪 ra	k-edge-wis-gateway		Gateways > rak-edge-wis-ga	teway			
			rak-edge-w	is-gateway			
1 01	erview		ID: rak-edge-wis-ga	ateway			
💷 Liv	e data		Disconnected			🚉 1 Collaborator 🛛 🕞 0 API keys	
💡 Lo	cation		Constal information		a Live data	See all activity	
** Co	llaborators		Gateway ID	rak-edge-wis-gateway	15:39:07 Create gateway	See an activity	
Ov AF	l keys		Gateway EUI	•			
🗘 Ge	neral settings		Gateway description	None			
			Created at	Nov 17, 2022 15:39:07			
			Last updated at	Nov 17, 2022 15:39:07			
			Gateway Server address	eu1.cloud.thethings.network	Location	Change location settings \rightarrow	
			LoRaWAN information				
			Frequency plan	EU_863_870			
			Global configuration	Download global_conf.json			
					No location information	ravailable	
< Hide s	debar						

Figure 1: Successfully added 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 NET WORK	THE THINGS STACK Community Edition	Overview	Applications	着 Gateways	2 Organizations	EU1 Community No SLA applicable (2)	
					Gateways 🗲 I	ak-edge-wis-gateway		
l		ak-edge-wis-gateway				k adra wie zataway		

Overview	ID: rak-edge-wis-gateway	
🔲 Live data	Disconnected	🗮 1 Collaborator 🛛 👁 🛛 API keys
Cocation	General information	• Live data See all activity →
Collaborators	Gateway ID rak-edge-wis-gateway 🚳	15:39:07 Create gateway
Or API keys	Gateway EUI	
General settings	Gateway description None	
	Created at Nov 17, 2022 15:39:07	
	Last updated at Nov 17, 2022 15:39:07	
	Gateway Server address eui.cloud.thethings.network	Location Change location settings →
	LoRaWAN information Frequency plan EU_863_870 Global configuration Download global_conf.json	No location information available
< Hide sidebar		

Figure 1: Overview page

2. In the API keys page, choose + Add API key.

THE THINGS STACK Community Edition	Serview Applications	🚢 Gateways	X Organizations			() No	EU1 Community SLA applicable ⑦	3	-
ak-edge-wis-gateway		Gateways ゝ	rak-edge-wis-gateway > API keys						
•		API keys (0)				+ Add AP	l key		
Overview		Key ID 💠	Name 🗢	Granted Rights		Created a	t •		
Eive data				No items found					
Location									
Collaborators									
Or API keys									
General settings									
< Hide sidebar									
© 2022 The Things Stack by The Things Network	k and The Things Industries				⊕ EN	v3.22.2 (3203f63b2)	Documentation	Status page	② Get support

Figure 1: 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.

<pre>c indegrave yet to the prove yet to</pre>		TORPORATE > TAK-PROF-WIN-CORPORAT > APPENDS > ADD	
<pre> i</pre>	ò rak-edge-wis-gateway	Add API key	
• was www	Overview		
 indiana indiana	🔲 Live data	Name mykey	
	Location	Expiry date	
Runce Runce <td< th=""><th>Collaborators</th><th>mm/dd/yyyy</th><th></th></td<>	Collaborators	mm/dd/yyyy	
• A Plays Grant all current and funder rights Grant all during rights Grant all dur	Conaborators	Rights *	
<pre> General settings</pre>	Or API keys	 Grant all current and future rights 	
• General arkings • Select all • Delete gateway • Delete gateway • Wew gateway information • Uks & Gateway 5a Gateway 5aver for traffic exchange, i.e. write uplink and read downlink • Wew gateway information • Uks & Gateway 2a Gateway 5aver for traffic exchange, i.e. write uplink and read downlink • Wew gateway information • Uks & Gateway 2aver for traffic exchange, i.e. write uplink and read downlink • Wew gateway information • Uks & Gateway 2aver for traffic exchange, i.e. write uplink and read downlink • Wew gateway information • Uks & Gateway 2aver for traffic exchange, i.e. write uplink and read downlink • Wew gateway information • Uks & Gateway 2aver for traffic exchange, i.e. write uplink and read downlink • Wew and edit gateway yatigits • Uks and edit gateway yatigits • Uke ward edit gateway yatigits • Uke ward edit gateway yatigits • Uke downlink gateway traffic • Store secrets for a gateway • Store secrets for a gateway • Store secrets for a gateway • Uke didebar • Crast API Neg 2022 217 https://www.storther.https://www.storther.https://www.storther.https://www.storther.https://www.storther.https://www.storther.https://www.storther.https://www.storther.https://www.storther.https://www.storther.https://www.storther.https://www.storther.https://www.storther.https://www.storther.https://www.storthttps://wwwwww.storther.https://www.storthttps://wwwww	Conoral cottings	 Grant individual rights 	
A lide adder Catch AFI log Catch AFI log C	General settings	Select all	
<pre> In the soleway the function in the soleway sole soleway server for traffic exchange, le. write uplink and read downlink in the soleway sole soleway server for traffic exchange, le. write uplink and read downlink in the soleway sole soleway server for traffic exchange, le. write uplink and read downlink in the soleway and edit gateway setungs in the soleway and edit gateway settings in the soleway settings in the soleway settings in the soleway status in the soleway status in the soleway status in the soleway status in the soleway traffic in the soleway in the soleway traffic in the soleway in the soleway traffic in the soleway traffic in the soleway in the solewa</pre>		Delete gateway	
A Hide sidebar 		View gateway information	
<pre> We getway loadin Retrieve secrets associated with a getway Provide getway API keys Cit basic getway API keys Cit basic getway settings View and edit getway API keys Cit basic getway settings View and edit getway collaborators View and edit getway settings Socie secrets for a getway staffic Socie secrets for a getway View and edit getway traffic Socie secrets for a getway View and edit getway traffic Socie secrets for a getway View and edit getway traffic Socie secrets for a getway View and edit getway traffic Socie secrets for a getway View and edit getway traffic Socie secrets for a getway View and edit getway traffic Socie secrets for a getway View and edit getway traffic Socie secrets for a getway View and edit getway traffic Socie secrets for a getway View and edit getway traffic Socie secrets for a getway View and edit getway traffic Socie secrets for a getway View and edit getway View and</pre>		Link as Gateway to a Gateway Server for traffic exchange, i.e. write uplink and read downlink	
<pre> the sidebar 2 222 The Things Stack by The Things Network and The Things Industries</pre>		View gateway location	
A Hide sidebar Q 2022 The Things Stack by The Things Network and The Things Industries Q Uew and edit gateway settings Q Hide sidebar Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The Things Industries Q Log 22 The Things Stack by The Things Network and The		Retrieve secrets associated with a gateway	
C Hide side bar C Hide side bar Things Network and The Things Industries C Hides Stack by The Things Network and The Things Industries C C Track API kor C C Track A		View and edit gateway API keys	
<pre> Wew and edit gateway collaborators Wew gateway status Wew gateway status Wite downlink gateway traffic Store secrets for a gateway Teate API key Create API key Create API key Create API key Store secrets for a gateway Wite downlink gateway traffic Store secrets for a gateway Create API key Store secrets for a gateway Create API key Store secrets for a gateway Store secrets for a gateway Store secrets for a gateway Create API key Store secrets for a gateway Store secrets Store secretse Store secrets Store secrets Store secrets St</pre>		Edit basic gateway settings	
		View and edit gateway collaborators	
Image: Write downlink gateway traffic		View gateway status	
Read gateway traffic Store secrets for a gateway Store secrets for a gateway Create AP1 key		Write downlink gateway traffic	
Image: Control Application Store secrets for a gateway Image: Control Application Image: Control Application <t< th=""><th></th><th>Read gateway traffic</th><th></th></t<>		Read gateway traffic	
K Hide sidebar Create API key © 2022 The Things Network and The Things Industries Image: Create API key © Get support Image: Create API key		Store secrets for a gateway	
2 2022 The Things Stack by The Things Network and The Things Industries Documentation Status page Q Get support	< Hide sidebar	Create API key	
	© 2022 The Things Stack by The Things Networ	and The Things Industries	EN v3.22.2 (3203f63b2) Documentation Status page Get support

Figure 1: 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.

1

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.				
	•••••••				

Figure 1: Copying the generated 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, refer to the Quickstart Guide.
- 2. Navigate to LoRa Network > Network Settings > Mode drop-down menu > choose Basics Station.

🇐 RAK°				Logout
🖲 Status	LoRaWAN Network Settings			
🕲 Network	Gataway FI II			
'Å' Channel Plan	Mode	Basics Station		
네 LoRa Network	Log Level	NOTICE		
Network Settings	Really switch mode?	Switch mode		
Gateway				
Application Clobal Integration				
Multicast Group				
🚱 Services				
📰 System				
රා WisDM				
			Copyright © RAKwireless Technology Co., Ltd. Al	Rights Reserved.

Figure 1: 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.

For this tutorial, you 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, use the **Let's Encrypt ISRG ROOT X1 Trust** certificate. You can download and check the certificate.
 - token: This is the generated API key. The key must start with Authorization:.

For example,

Authorization: YOUR_API_KEY

🖓 ΝΟΤΕ

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
Ø Status	LoRaWAN Network Settings	
🐼 Network		
(%) Channel Plan	Gateway EU	Purcha Darba
네 LoRa Network		
Network Settings	Lug Lover	NUTINE V
🗞 Services	LORa Basic Station Basic Station Configuration	
📰 System	Basic Station	
රා WisDM		
	Server	CUPS Boot Server CUPS Server CUPS Server
		LNS Server
	URI	wss://eu1.cloud.thethings.network
	Port	8887
	Authentication Mode	TLS Server Authentication and Client Token
	trust	BEGIN CERTIFICATE MIIFacCAOlgs/willAgiRAUCZDSQONZRGPgu2OCiw/wDQYJKoZIhveNAQELBQAw TELMAKGAU UEQZDSQONZRGPgu2OCiw/wDQYJKoZIhveNAQELBQAw TELMAKGAU UEQDKOVMAKTAabgMVBAa TIEludGVybm/V0FNYT3VyaXRBF_AC2/h CmNoEligh3DVMRU/wEVTDVQQDEwaULJ1HIF.bx3QJWDEvHtheNMTUrwhQAMTEwNDMA WhoHMXcJwhQAUTWTWNDAWJBPBCAWUUC2B/LCGCAULUCDMgSV62XAu ZXQQUZVJRXJpdHkgUmVzZVFYY2ggR3JavGXv4FTATBgHVBAMTDETTUksgUm9v4CBY MTCCAIhvQOTV,RZIhreNAQEBBCADgJBADCCAppQGJBAKSJAHPQDFUbmsK4Vygc
	token	Authorization: NNSXS.HZCPNYHPC7TJXSH4A7U5
		Save & Apply. Reset

Figure 1: 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	턂 Overview Applications 🗳 Gateways 쓰 Organ	izations	Community No support plan To
rak.edge.wie.gateway	Gateways > rak-edge-wis-g	gateway	
- Incode ins gatemay	and the second s	via gataway	
Overview	ID: rak-edge-wis-g	gateway	
😑 Live data	↑ 0 ↓ 0 • Last activity	/ 20 seconds ago 💿	♣ 1 Collaborator
• Location			
Collaborators	General information Gateway ID	rak-edge-wis-gateway	• Live data See all activity → ↑ 15:49:13 Receive uplink message DevAddr: ↔ 💽 FPort: (
Or API keys	Gateway EUI	o 6	↓ 15:49:09 Send downlink message Tx Power: 16.15 Data rate: SF7BW125
🗱 General settings	Gateway description	None	↑ 15/49/37 Receive uplink message JoinEUI:
	Created at	Nov 17, 2022 15:39:07	↑ 15:48:53 Receive uplink message JoinEUI:
	Last updated at	Nov 17, 2022 15:39:07	ማግ 15:46:49 Receive gateway status Versions: { station: "2.8.4-9-g3d5c666
	Gateway Server address	eu1.cloud.thethings.network	Location Change location settings
	LoRaWAN information		
	Frequency plan	EU_863_870	
	Global configuration	▲ Download global_conf.json	



LORIOT

In this tutorial, you will learn how to connect RAK7249 WisGate Edge Max 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

• RAK7249 WisGate Edge Max

Software

- SSH Client (This tutorial will be done using PuTTY.)
- LORIOT Account

Registering the Gateway

1. Log into your LORIOT account.

IN LORIO T	=						@rakwireles Community Account	s.com 🛔 🕞
Dashboard ✓ Applications Applications Dashboard A Networks Join Servers Documentation	Her COMMUNITY ACC Welcome to LORIOT Communi You are now part of a world-wid As a reward for sharing your gat	OUNT ty Account! le ecosystem of LoRaWAN [®] develo ewray, we provide you one Free N	opers. Your devices can use any com etwork Application.	munity gateway to reach our network.	COMMUNITY ACCOUNT features No account expiration Reaming among all community gateways One Free Network Application			
▲ Account ★ Upgrade € Support	EEI News Apr 21, 2020, 3:00:00 PM Feb 20, 2020, 1:00:00 PM		UFAXE RED	LOBOT Network Server 60 has been released! Check our release note for more details. Be confident in the delivery of your services and guarantee connectivity for * Upgrade now to Professional Public Server with 93-95 SLA plus unlimite	your solution. gateways and messages			
	Gateways of Sample Location	le network Model	MAC Versio	Register a new gateway Last Data	✓ Applications Name BampleApp	App10 BE-7A-25-17	● Creat Devices 0	New Application

Figure 1: 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.

and LORIO T							Frankfurt <mark>—</mark>	@rakwireless.com Community Account	۵	•
🗲 Back To Dashboard	Networks									
A NETWORKS	Filter by	~								٦
+ New Network	Network ID		↓₹ Name	11 Gateways	1 Visibility	L1 Country	J↑ City	↓† zip	It	
	A0001F3F		Sample network	0	Disabled					

Copyright © 2015 - 2021 LORIOT AG. All rights reserved.	LORIOT Internet of Things at Long Range Impressum

Figure 1: Networks List

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

LORIO T	≡ Networks > Sa	imple Network					Grak Frankfurt Community Accour	wireless.com 🤷 🕞
🗲 Back To Networks	Sampler	network						
A0001F3F	Creation Date 3/24/21, 4:05 PM		Organization User Disabled	Access	Roaming ID A0001F3F	Network Organization Uuid 9f598851-4f7a-4a5d-aded-4cebc38dad2b	Configur	e •
🖬 Map							+ Add Gat	work eway
	Filter by		~					
	o	Name	↓↑ MAC	↓ F Model	11 Version	↓↑ Status	11 Last Data	11.
					There are no Gateways associated with thi	s network		
	Copyright © 2015 - 2	2021 LORIOT AG. All rights reserve	d.				LORIOT Internet of Thing	gs at Long Range Impressum

Figure 1: Adding a gateway to the network

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

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.

IN LORIO T	E Networks > Sample Network > Sateway Registration	Frankfurt <mark>-</mark>	@rakwireless.com Community Account	° 📥 G	
← Back To Networks	Gateway Registration				
A0001FSF	Requirements and services				1
Mi Map	To register a gateway within the network, you need to provide some limited information about your gateway. This information is used to uniquely identify your gateway in the network. Upon Registration, • the gateway is astigned to your network • a gateway is astigned to your network • the hointry specific by our gateway is available in the Software section The LORIOT gateway binary is outom built for all Integrated gateways. Select your gateway from the list below and Hill in the required fields.				
	What is your base platform?				
	Radio Front-end RAX 7245 V Bus EV V RAX 7245 is fully supported.				
	Choose a different base platform				
	MAC address of eth0 interface				
	The MAC Address of the Ethemet port can be queried by running if config ethal grop Meador command from your device's console. A sample output will be similar to ethal Link encap: Ethemet Meador AB: CD: EFI 12: 24: 56				



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:								
Session Generation Gen	Basic options for your PuTTY ses Specify the destination you want to connect Host Name (or IP address) 192.168.0.114 Connection type: O Raw O Telnet O Rlogin O SSH Load, save or delete a stored session Saved Sessions Default Settings	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port 192.168.0.114 22 Connection type: Raw Telnet Rlogin SSH Serial Load, save or delete a stored session Saved Sessions Load Save Default Settings Load Save Delete						
About Help	Close window on exit: Always Never Open Cancel							

Figure 1: PuTTY Configuration

6. Log in with your root credentials.

ess of the device, and cannot be mo

- 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:XX



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.



Figure 1: 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



Your gateway is now registered and connected to LORIOT.

REALORIO T	Networks > Sample Network > 60-CS-A8-FF-FF-			وrakwireless.com المعالي المحالي محالي المحالي
♦ Back To Sample Network	60-C5-A8-FF-FF-			
© 60-C5-A8-FF-FF- coCsAsFFFF		Status		
Devices Activity	•		40 ms	Last Connect 25 Mar 2021 13:33:29 (8 minutes ago)
🕅 Location			Last Keep Alive 25 Mar 2021 13:40:33 (o minute opo)	Remote Time Offset a few seconds
Lad Traffic	1000		Last Data 25 Mar 2021 13:41:02 (o few seconds ogo)	
ᠹ Radio				
筆 System	Connected Version 2.8.15eU-JNS-EU1-3e	Union (daus) Deventions (daus)		
ad GPS	Configure *			
KH Log	raig Tap into data stream	Details MAC Address	Model	
Alerts	Restart	60:C5:A8:	7249 Concentrator	
	Remove	60-C5-A8-FF-FF	rak_7249	
		Base RAK	Connected Over SPI	
		Connected from IP 89.106.101.181	Name RAK7249	
		Machine	Version	
		Kernel		
		Network Details interface #1 br-lan 192.168.230.1 Interface #2 etb0.2 192.254.20.38 Interface #3 etb0.2 192.168.0.14 Interface #4 apcilo 192.258.0.106		
		Configuration Community Access ✔ Antennas	Alert Notifications X	Ignore Data 🗙

Figure 1: Successful Connection

ThingPark by Actility

In this section, you will learn how to add RAK7249 WisGate Edge Max in ThingPark.

ThingPark is Actility's platform, in which you can register your LoRaWAN gateway and end devices. ThingPark offers a user-friendly dashboard, in which you can monitor different information about the gateway/end device like status, radio traffic, statistics, and more. Together with HTTPS integration, you can send the data received from the end nodes to an Application server for post-processing and visualizing.

For the complete step-by-step tutorial, refer to the How to Add RAK WisGate Edge Gateway in ThingPark - Actility ThingPark Guide.



LoRa® is a registered trademark or service mark of Semtech Corporation or its affiliates. LoRaWAN® is a licensed mark.

Copyright © 2014-2024 RAKwireless Technology Limited. All rights reserved.

