

# FMB125 Getting Started with AWS IoT Core

[Main Page](#) > [Professional Trackers](#) > [FMB125](#) > [FMB125 Manual](#) > **FMB125 Getting Started with AWS IoT Core**



## Contents

- [1 Document Information](#)
  - [1.1 Glossary](#)
  - [1.2 Revision History \(Version, Date, Description of change\)](#)
- [2 Overview](#)
- [3 Hardware Description](#)
  - [3.1 DataSheet](#)
  - [3.2 Standard Kit Contents](#)
  - [3.3 User Provided Items](#)
- [4 Set up your Development Environment](#)
  - [4.1 Tools Installation \(IDEs, Toolchains, SDKs\)](#)
  - [4.2 Other software required to develop and debug applications for the device](#)
- [5 Set up your hardware](#)
- [6 Document Information](#)
  - [6.1 Glossary](#)
- [7 Other software required to develop and debug applications for the device](#)
- [8 Setup your AWS account and Permissions](#)
- [9 Create Resources in AWS IoT](#)
- [10 Provide Device with credentials](#)
  - [10.1 AWS IoT Core Configuration](#)
    - [10.1.1 Setting up AWS IoT Core](#)
    - [10.1.2 Finding device data endpoint \(server domain\)](#)
  - [10.2 Configuring the device](#)
    - [10.2.1 Security and certificates](#)
      - [10.2.1.1 Using certificate, private key and root certificate. \(Via Cable\)](#)
    - [10.2.2 Device GPRS configuration for AWS IoT Custom MQTT settings](#)
- [11 Checking received data and sending commands in the AWS IoT core](#)
- [12 Debugging](#)
- [13 Troubleshooting](#)
- [14 Troubleshooting](#)
- [15 Debugging](#)

## Document Information

### Glossary

- FMB125 (tracker) - GNSS tracking device manufactured by Teltonika Telematics.
- Wiki - Teltonika IoT knowledge base - <https://wiki.teltonika-iot-group.com/>.
- FOTA - Firmware Over The Air.

- Configurator – Tool to configure Teltonika Telematics devices.
- Crowd support forum – knowledge base dedicated for Troubleshooting.

## ***Revision History (Version, Date, Description of change)***

<b>Version</b>	<b>Date</b>	<b>Description</b>
v1.5	2023.02.14	Links updated
v1.4	2022.12.19	Minor information update
v1.3	2022.11.29	Page created

## **Overview**

FMB125 small and professional tracker with internal high gain GSM and external GNSS antennas, which is able to collect device coordinates and other useful data and transfer them via GSM network to server. This device is perfectly suitable for applications where location acquirement of remote objects is needed: fleet management, car rental companies, taxi companies, public transport, logistics companies, personal cars and so on. FMB125 can perform tasks on remote objects, such as monitoring engine status, controlling truck's door etc.

**Currently for MQTT solution evaluation firmware is required to be used - 03.27.10.Rev.520.** For firmware supporting MQTT please contact your sales manager or contact directly via Teltonika Helpdesk.

Changes in firmware versions and update information can be found in device wiki page: [FMB125 firmware errata](#)

## **Hardware Description**

### ***DataSheet***

FMB125 device data sheet can be downloaded here: [DataSheet](#)

### ***Standard Kit Contents***

STANDARD PACKAGE CONTAINS

- 5 pcs. of FMB125 trackers
- 5 pcs. of Input/output power supply cables (0.9 m)
- 5 pcs. of GNSS antennas (3m)
- Packaging box with Teltonika branding

Teltonika suggest standard order codes for the device purchase, by contacting us, we can create special order code which would fulfill user needs.

More ordering information at: [Ordering](#)

### ***User Provided Items***

- Power supply (10-30V).
- MicroUSB to USB A cable.

# Set up your Development Environment

## ***Tools Installation (IDEs, Toolchains, SDKs)***

FMB125 comes with our created firmware, therefore no additional development or scripting is required for this unit to support AWS IoT. Only by using Teltonika Configurator [FM Configurator versions](#), connection point of AWS IoT server is required.

## ***Other software required to develop and debug applications for the device***

For debugging situations, device internal logs can be downloaded OTA by using our [FotaWEB](#) platform or by using Teltonika Configurator.

# Set up your hardware

All details about FMB125 can be located in our dedicated wiki page [FMB125 Wiki](#)

- Basic device startup instructions provided in [FMB125 First Start](#).
- Device characteristics, power supply information: [FMB125 General description](#)
- FMB125 firmware change can be performed via [FotaWEB](#) (direct buyer gets access to this platform) or via device [Configurator](#)
- Device LED information: [FMB125 LED Status](#)
- USB driver download, datasheet and quick start guide downloads: [FMB125 Downloads](#)

# Document Information

## **Glossary**

- Wiki - Teltonika IoT knowledge base - <https://wiki.teltonika-iot-group.com/>.
- FOTA - Firmware Over The Air.
- Configurator - Tool to configure Teltonika Telematics devices.
- Crowd support forum - knowledge base dedicated for Troubleshooting.

**For firmware supporting MQTT please contact your sales manager or contact directly via Teltonika Helpdesk.**

## **Other software required to develop and debug applications for the device**

For debugging situations, device internal logs can be downloaded OTA by using our [FotaWEB](#) platform or by using Teltonika Configurator.

# Setup your AWS account and Permissions

Refer to the online AWS documentation at Set up your AWS Account. Follow the steps outlined in the sections below to create your account and a user and get started:

- [Sign up for an AWS account](#)
- [Create a user and grant permissions](#)
- [Open the AWS IoT console](#)

Pay special attention to the Notes.

## Create Resources in AWS IoT

Refer to the online AWS documentation at [Create AWS IoT Resources](#). Follow the steps outlined in these sections to provision resources for your device:

- [Create an AWS IoT Policy](#)
- [Create a thing object](#)

Pay special attention to the Notes.

## Provide Device with credentials

Whole device, AWS IoT and testing information can be downloaded in PDF format [here](#).

NOTE: MQTT will not work without uploaded TLS certificates.

## AWS IoT Core Configuration

### Setting up AWS IoT Core

When logged in the AWS console, click on Services on the top left hand side screen, to access IoT core.

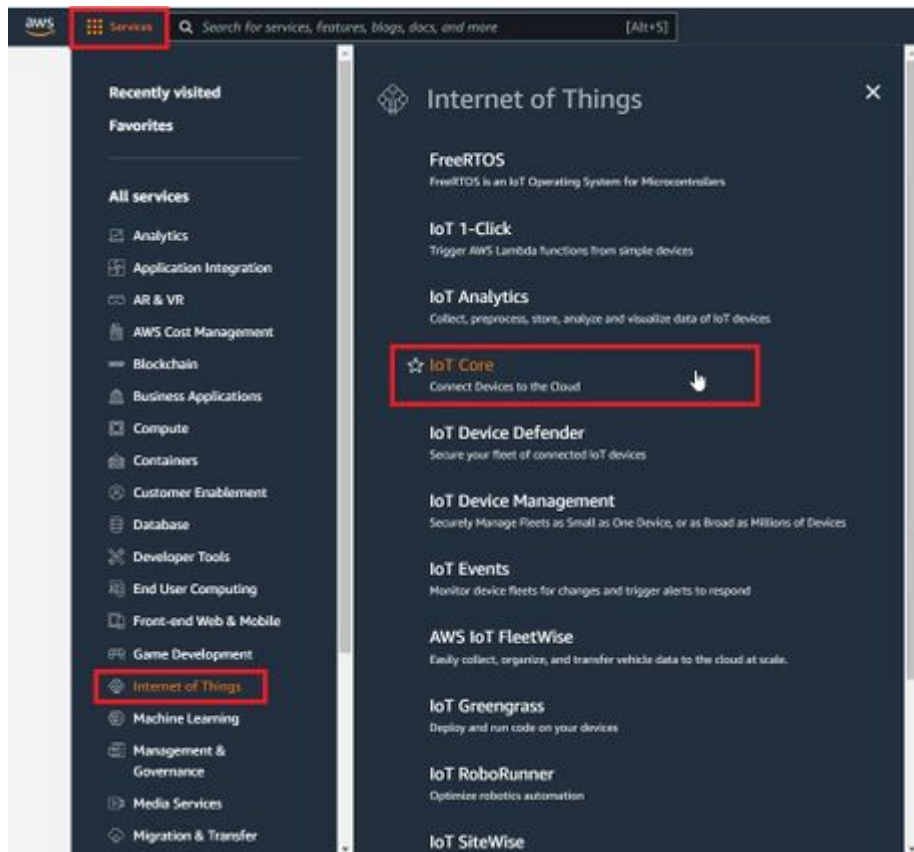


Figure 1. Accessing AWS IoT core from AWS console

NOTE: If you can't see "Services" in the top left, click on "My account" in the top right and "AWS Management Console"


Select Manage, Security, Policies (Manage > Security > Policies) and press Create policy or Create buttons. 

Figure 2. Accessing policy creation


In the Create Policy window, enter Policy name. In the Policy document tab for Policy Action (1) select "\*" and for Policy resource (2) enter "\*" and press create. 

Figure 3. Creating a policy


Now, that you have created a policy, select Manage on the sidebar on the left side, then select All devices, Things (Manage>All devices>Things). And click on Create things. 

Figure 4. Accessing Things

Afterwards select Create single thing and click Next.

AWS IoT > Manage > Things > Create things

## Create things [Info](#)

A thing resource is a digital representation of a physical device or logical entity in AWS IoT. Your device or entity needs a thing resource in the registry to use AWS IoT features such as Device Shadows, events, jobs, and device management features.

### Number of things to create

☒ **Create single thing**  
Create a thing resource to register a device. Provision the certificate and policy necessary to allow the device to connect to AWS IoT.

☐ **Create many things**  
Create a task that creates multiple thing resources to register devices and provision the resources those devices require to connect to AWS IoT.

Cancel **Next**

Figure 5. Creating single thing

After creating a single thing, enter Thing's name and in the Device Shadow tab select Unnamed shadow (classic). Then click Next.

**Specify thing properties** [Info](#)

A thing resource is a digital representation of a physical device or logical entity in AWS IoT. Your device or entity needs a thing resource in the registry to use AWS IoT features such as Device Shadows, events, jobs, and device management features.

### Thing properties [Info](#)

**Thing name**  
FMB150  
Enter a unique name containing only: letters, numbers, hyphens, colons, or underscores. A thing name can't contain any spaces.

### Additional configurations

You can use these configurations to add detail that can help you to organize, manage, and search your things.

- ▶ Thing type - optional
- ▶ Searchable thing attributes - optional
- ▶ Thing groups - optional
- ▶ Billing group - optional

### Device Shadow [Info](#)

Device Shadows allow connected devices to sync states with AWS. You can also get, update, or delete the state information of this thing's shadow using either HTTPs or MQTT topics.

☐ No shadow

☐ Named shadow  
Create multiple shadows with different names to manage access to properties, and logically group your devices properties.

☒ **Unnamed shadow (classic)**  
A thing can have only one unnamed shadow.

Figure 6. Thing's properties

Then when selecting Device certificate, select Auto-generate a new certificate and click Next.

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

AWS IoT > Manage > Things > Create things > Create single thing

Step 1  
Specify thing properties

Step 2 - optional  
**Configure device certificate**

Step 3 - optional  
Attach policies to certificate

### Configure device certificate - optional Info

A device requires a certificate to connect to AWS IoT. You can choose how you to register a certificate for your device now, or you can create and register a certificate for your device later. Your device won't be able to connect to AWS IoT until it has an active certificate with an appropriate policy.

#### Device certificate

- ☒ **Auto-generate a new certificate (recommended)**  
Generate a certificate, public key, and private key using AWS IoT's certificate authority.
- ☐ Use my certificate  
Use a certificate signed by your own certificate authority.
- ☐ Upload CSR  
Register your CA and use your own certificates on one or many devices.
- ☐ Skip creating a certificate at this time  
You can create a certificate for this thing and attach a policy to the certificate at a later time.

Cancel Previous **Next**

Figure 7. Certificate configuration

Now, select the policy you have created before to attach it to the certificate and thing. After that click Create thing.

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

AWS IoT > Manage > Things > Create things > Create single thing

Step 1  
Specify thing properties

Step 2 - optional  
Configure device certificate

Step 3 - optional  
**Attach policies to certificate**

### Attach policies to certificate - optional Info

AWS IoT policies grant or deny access to AWS IoT resources. Attaching policies to the device certificate applies this access to the device.

#### Policies (1/1)

Select up to 10 policies to attach to this certificate.

Filter policies

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	FMB130Policy

Cancel Previous **Create thing**

Figure 8. Attaching policy to certificate

Then window with Certificate files and key files download options should pop out. It's recommended to download all files, because later some of them will not be available for download. The files that are required for usage with FMX devices are: Device certificate (1), private key(2), and Amazon Root CA 1 file(3), but it's recommended to download them all and store them in secured place.



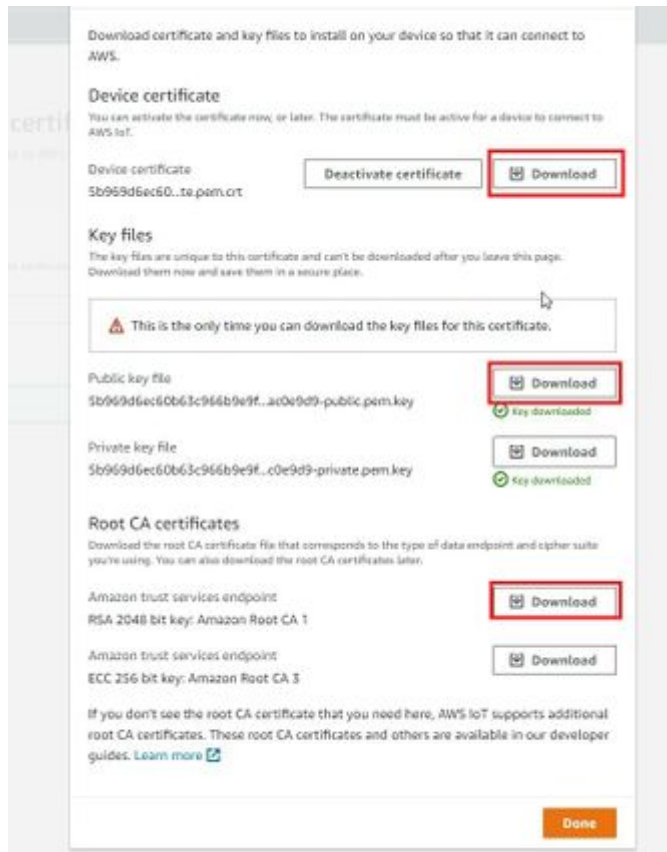


Figure 9. Certificate and key download

## Finding device data endpoint (server domain)

To receive server domain (in AWS endpoint) click on the side bar on the left Settings (AWS IoT->Settings). Or click on the side bar on left side Things, select the created thing, after it click Interact->View Settings. Whole path - (Things->\*YourThingName\*->Interact->ViewSettings). Page containing endpoint will open. Copy the whole endpoint address. Port for accessing this endpoint is 8883.

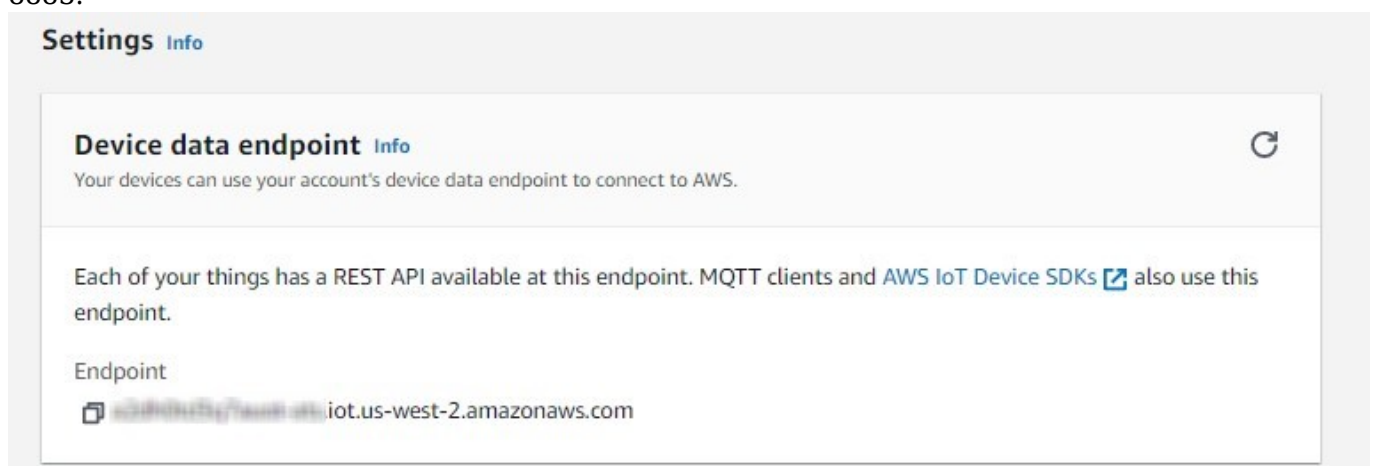


Figure 10. Device data endpoint

## Configuring the device



## Security and certificates

### Using certificate, private key and root certificate. (Via Cable)

Find Certificate file ending with extension pem.crt (ending may be just .pem) Private key file and AmazonRootCA1 file (no need to change filenames). These files should have been downloaded when creating Thing in AWS IoT Core.

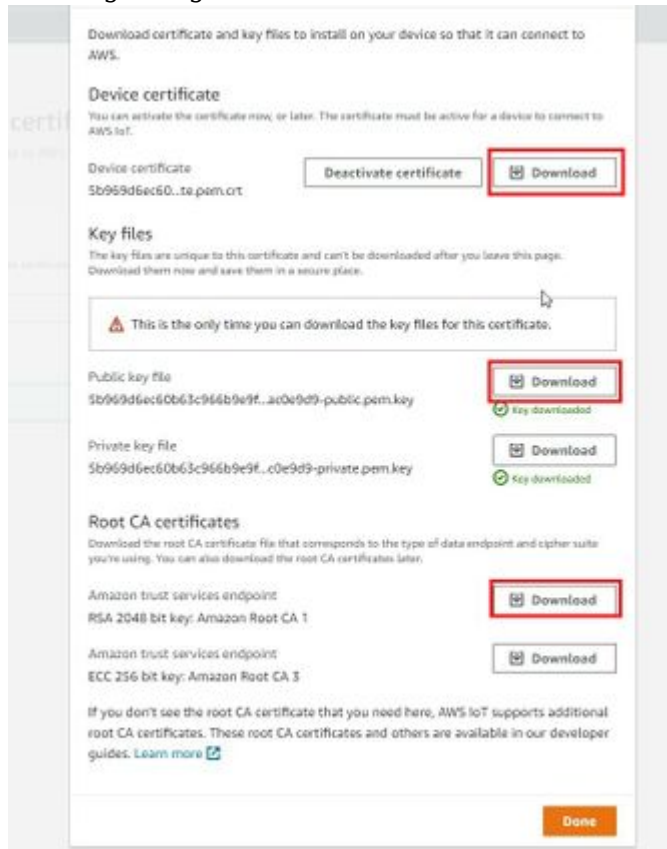


Figure 17. Certificate, private key and root certificate

Upload the mentioned files in the Security tab in the Teltonika Configurator.



Figure 18. Uploading certificates and keys

After uploading certificates, go to System tab and in Data protocol section select - Codec JSON.

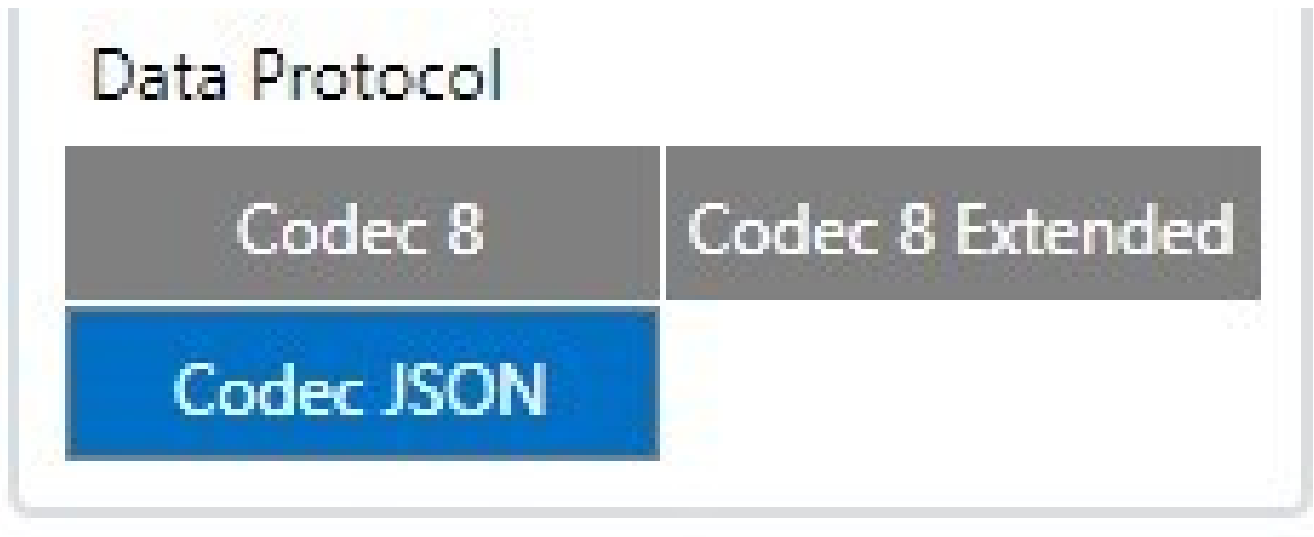


Figure 19. Choosing data protocol

### Device GPRS configuration for AWS IoT Custom MQTT settings

In the GPRS tab, under Server Settings select:

1. Domain - Endpoint from the AWS, Port: 8883
2. Protocol - MQTT
3. TLS Encryption - TLS/DTLS

In the MQTT Settings section select:

1. MQTT Client Type - AWS IoT Custom
2. Device ID - enter device IMEI (optional)
3. Leave Data and Command Topics unchanged.

Save the configuration to the device.



Figure 27. GPRS Settings for MQTT AWS IoT

## Checking received data and sending commands in the AWS IoT core


The data received from the device can be found in the MQTT test client, which can be found above "Manage" in the sidebar on the left. 

Figure 28. MQTT test client location

To see incoming data, subscribe to topic - `*DeviceImei*/data` . Or subscribe to `#` to see all incoming outgoing data in the Topics.

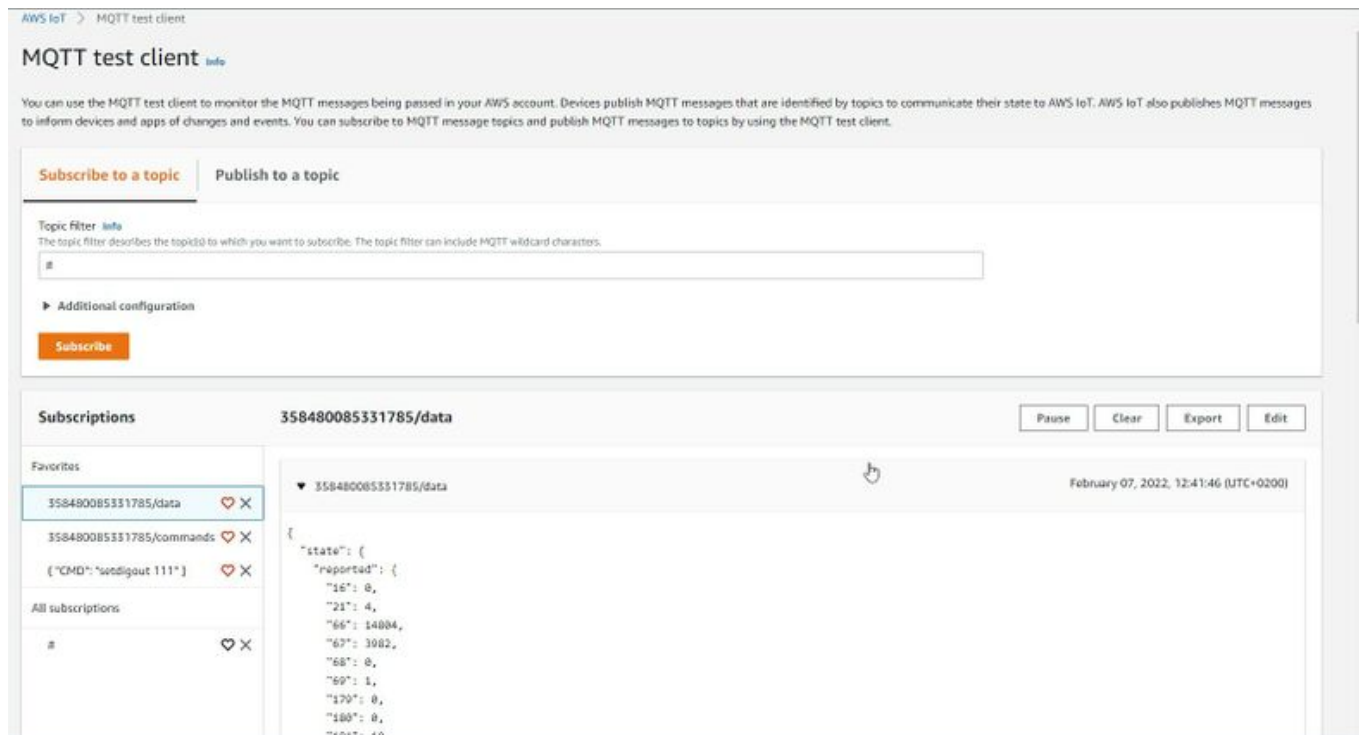


Figure 29. MQTT test client

Incoming data is received in JSON format, for e.g.:



Figure 30. Received data format

To send SMS/GPRS commands to the device subscribe to a topic name - \*DeviceIMEI\*/commands, and, in the same MQTT test client window select Publish to a topic. Enter topic name - \*DeviceIMEI\*/commands. In the Message payload enter wanted GPRS/SMS command in following format and press Publish:

{ "CMD": "<Command>" }

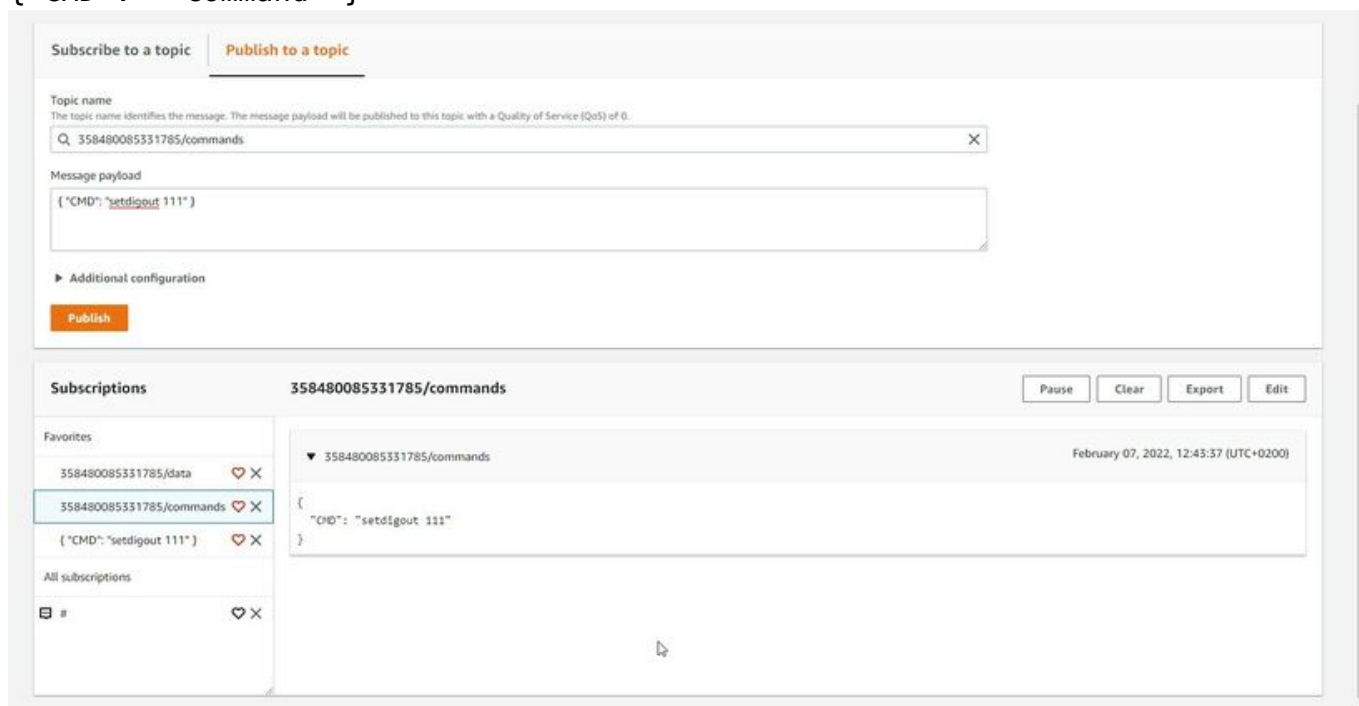


Figure 31. Sending Command in AWS IoT Core

The response to the command will be shown in the Data topic:



Figure 32. Response to a command in the data topic, the command was published in command topic

## Debugging

In the situation when the issue with information upload appears, device internal logs can be taken directly from device configuration software ([instructions](#)), via Terminal.exe by connecting selecting device USB connection port, or by receiving internal logs via FotaWEB in [task section](#).

## Troubleshooting

The information can be submitted to Teltonika HelpDesk and Teltonika engineers will assist with troubleshooting. For a more detailed information regarding what information should be collected for debugging, please visit the dedicated page on [Teltonika Wiki](#).

Alternatively, Teltonika has a [Crowd Support Forum](#) dedicated for troubleshooting, where engineers are actively solving problems.

## Troubleshooting

The information can be submitted to Teltonika HelpDesk and Teltonika engineers will assist with troubleshooting. For a more detailed information regarding what information should be collected for debugging, please visit the dedicated page on [Teltonika Wiki](#).

Alternatively, Teltonika has a [Crowd Support Forum](#) dedicated for troubleshooting, where engineers are actively solving problems.

## Debugging

In the situation when the issue with information upload appears, device internal logs can be taken directly from device configuration software ([instructions](#)), via Terminal.exe by connecting selecting device USB connection port, or by receiving internal logs via FotaWEB in [task section](#).