

FMM130BG95-M3

Getting Started Guide for AWS IoT Core

Table of Contents

- 1 Document Information 1**
- 2 Overview 2**
- 3 Hardware Description..... 2**
- 4 Set up your Development Environment 3**
- 5 Set up your hardware..... 3**
- 6 Setup your AWS account and Permissions..... 3**
- 7 Create Resources in AWS IoT..... 3**
- 8 Provision the Device with credentials 3**
- 8.1. AWS IoT core configuration 4**
- 8.1.1. Setting up AWS IoT core 4**
- 8.2.2. Finding device data endpoint (server domain) 8**
- 8.3. Configuring the device..... 8**
- 8.3.1. Security and certificates..... 8**
- 8.3.2. Device GPRS configuration for AWS IoT Custom MQTT settings..... 9**
- 9 Run the demo 10**
- 10 Debugging 12**
- 11 Troubleshooting 12**

1 Document Information

1.1 Naming Conventions

- Version – v1.3
- Date – 2022.11.29

1.2 Glossary

- FMM130 (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.

1.3 Revision History (Version, Date, Description of change)

Changes in firmware versions and update information can be found in device wiki page:

https://wiki.teltonika-gps.com/view/FMM130_firmware_errata

2 Overview

FMM130 is small and professional real-time tracking terminal with GNSS and LTE CAT-M1/NB-IoT/GSM connectivity and backup battery. Device equipped with GNSS/Bluetooth and LTE CAT-M1/NB-IoT modules with fallback to 2G network, internal GNSS and LTE antennas, configurable digital, analogue inputs and digital outputs, negative input, impulse inputs. It 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.

3 Hardware Description

3.1 DataSheet

FMM130 device data sheet can be downloaded here:

<https://teltonika-gps.com/downloads/en/fmm130/Datasheet-FMM130-2.1-web-Telematics.pdf>

3.2 Standard Kit Contents

STANDARD PACKAGE CONTAINS

- 10 pcs. of FMM130 trackers
- 10 pcs. of Input/output power supply cables (0.9 m)
- Packaging box with Teltonika branding

More ordering information at: <https://teltonika-gps.com/product/fmm130/#ordering>

3.3 User Provided items

- FMM130 tracker
- Input/output power supply cable (0.9 m)
- 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.

3.4 Additional Hardware References

If device was bought without Micro USB included in 1SPQ (Single packet quantity), Micro USB cable should be

4 Set up your Development Environment

4.1 Tools Installation (IDEs, Toolchains, SDKs)

FMM130 comes with our created firmwares, therefore no additional development or scripting is required for this unit to support AWS IoT. Only by using Teltonika Configurator https://wiki.teltonika-gps.com/view/FM_Configurator_versions , connection point of AWS IoT server is required.

4.2 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.

5 Set up your hardware

All details about FMM130 can be located in our dedicated wiki page [FMM130 Wiki](#)

- Basic device startup instructions provided in [FMM130 First Start](#).
- Device characteristics, power supply information: [FMM130 General description](#)
- FMM130 firmware change can be performed via FotaWEB (direct buyer gets access to this platform) [FotaWEB](#) or via device [configurator](#)
- Device LED information: [FMM130_LED_status](#)
- USB driver download, datasheet and quick start guide downloads: [FMM130 Downloads](#)

6 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](#) and
- [Create a user and grant permissions](#)
- [Open the AWS IoT console](#)

Pay special attention to the Notes.

7 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.

8 Provision the Device with credentials

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

8.1. AWS IoT core configuration

8.1.1. 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.

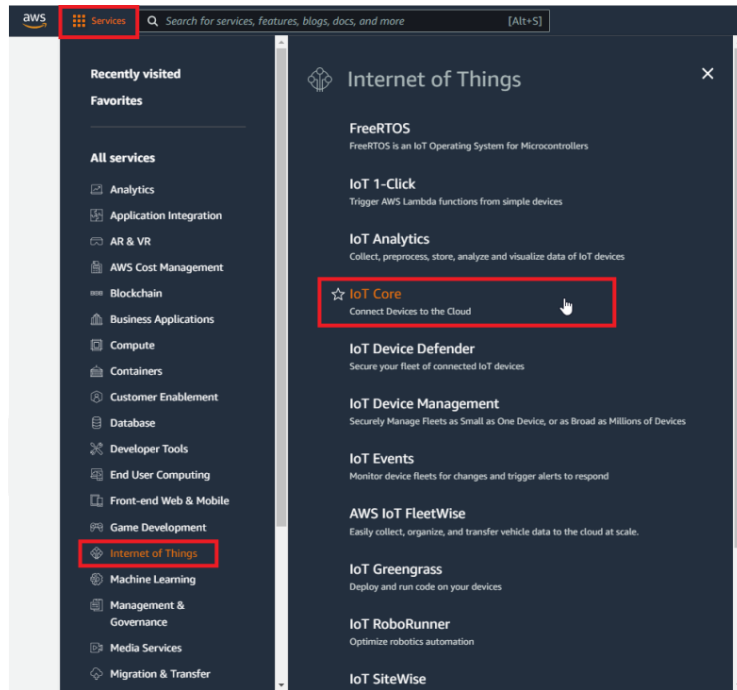


Figure 1. Accessing AWS IoT core from AWS console

After accessing AWS IoT core, select Manage on the sidebar on the left side, then select Things (Manage- >Things). And click on Create things.

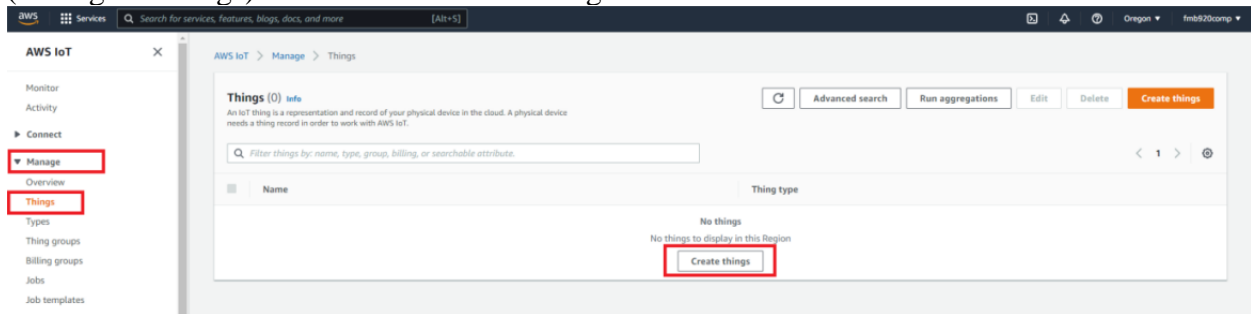


Figure 2. Accessing Things

Afterwards for select Create single thing and click Next.

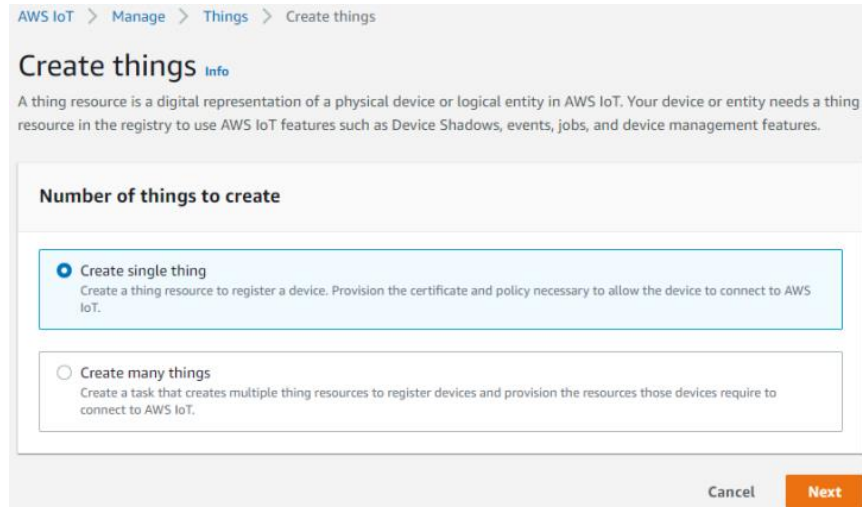


Figure 3. Creating single thing

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

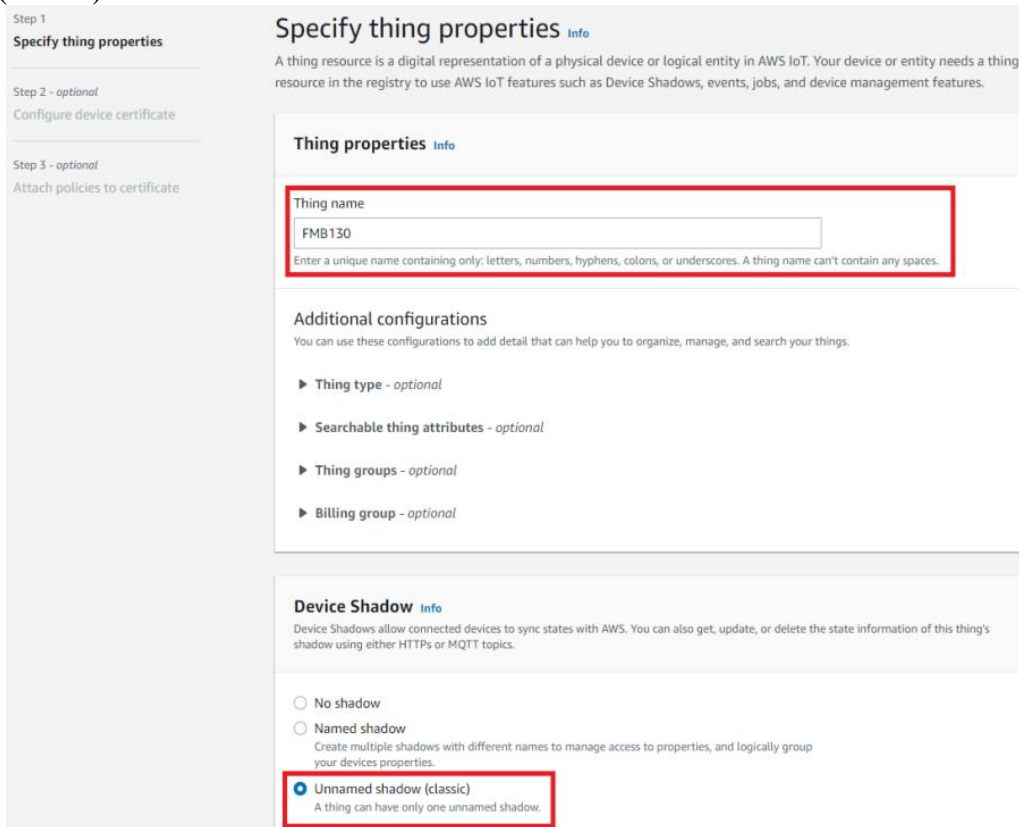


Figure 4. Specifying thing properties

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

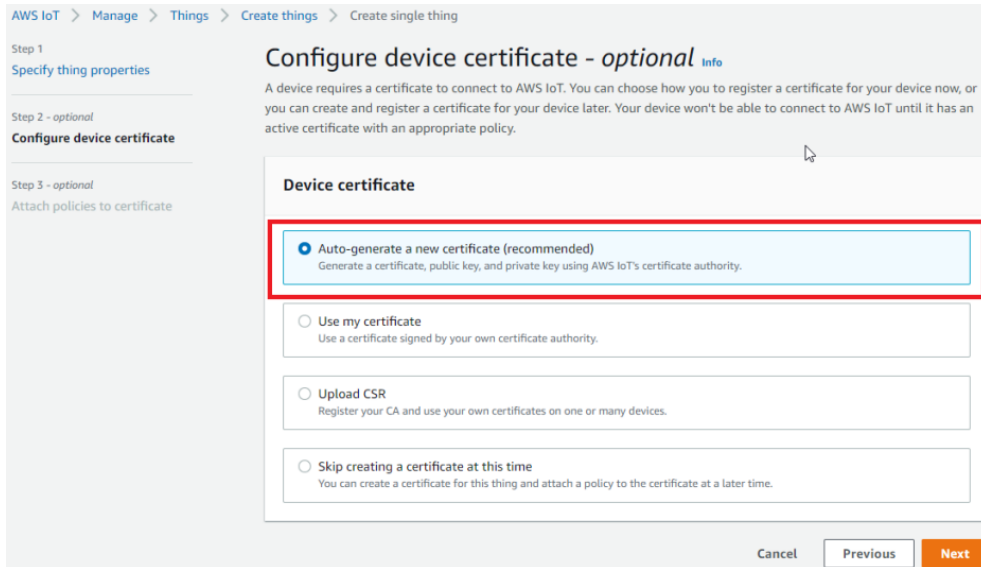


Figure 5. Selecting Certificate

After this select Create policy to create it and attach it to Certificate. In the Create Policy window, enter Policy name. In the Policy document (1) tab for Policy Action (2) select * and for Policy resource enter * .

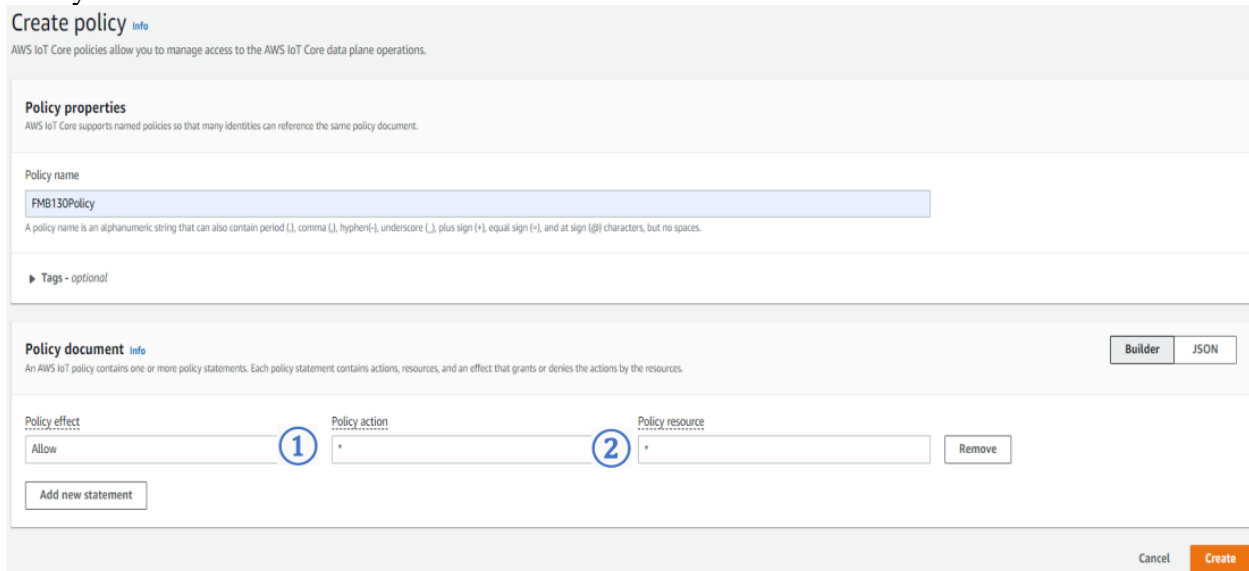


Figure 6. Creating policy for certificate

After creating policy, return to Certificate tab (Seperate tab after pressing Create policy should've popped out). Then select the created policy to attach it to the certificate and thing. After that click Create thing

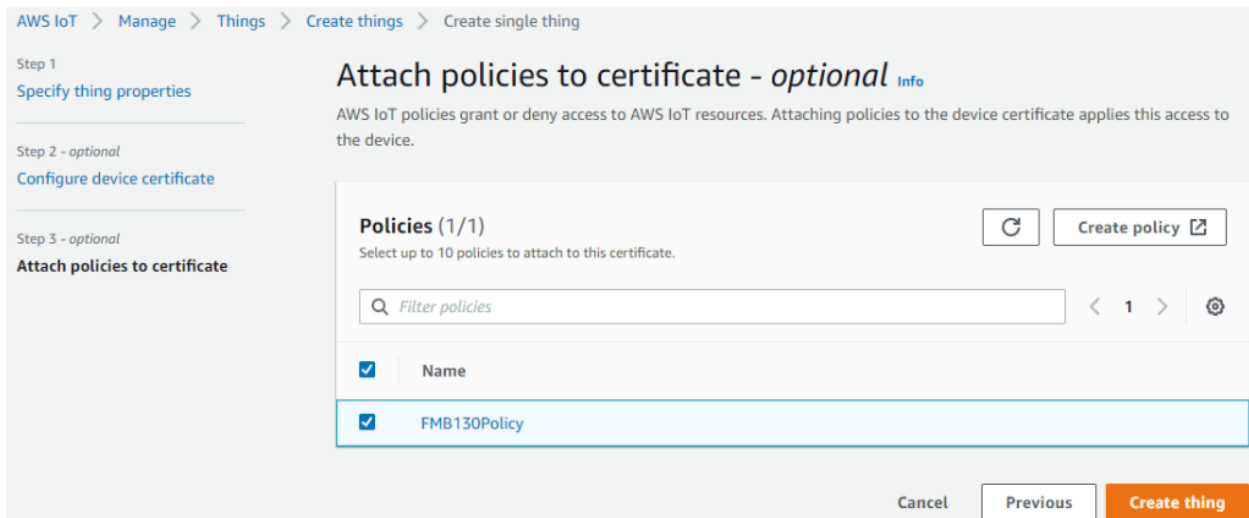


Figure 7. Attaching created certificate and creating thing

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.

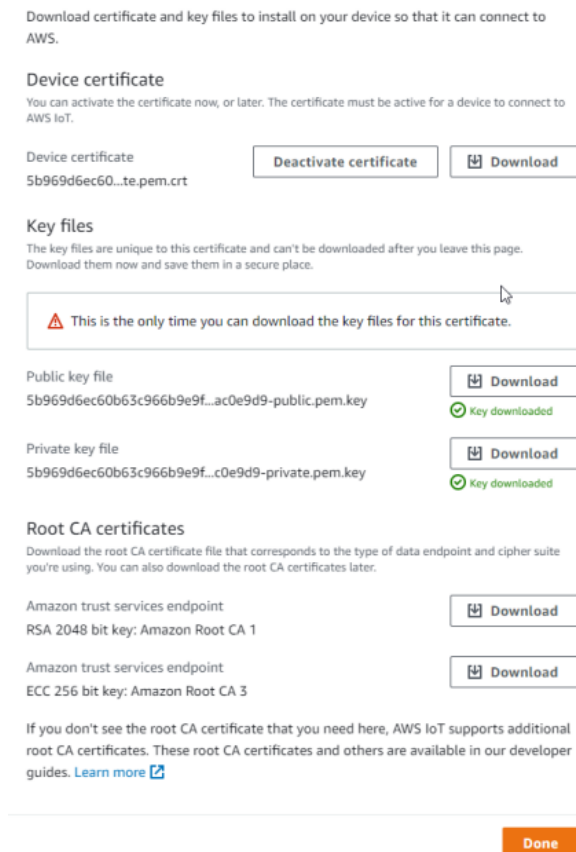


Figure 8. Certificate files download window

8.2.2. Finding device data endpoint (server domain)

To receive server domain (in AWS endpoint) click on the side bar on the left 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.

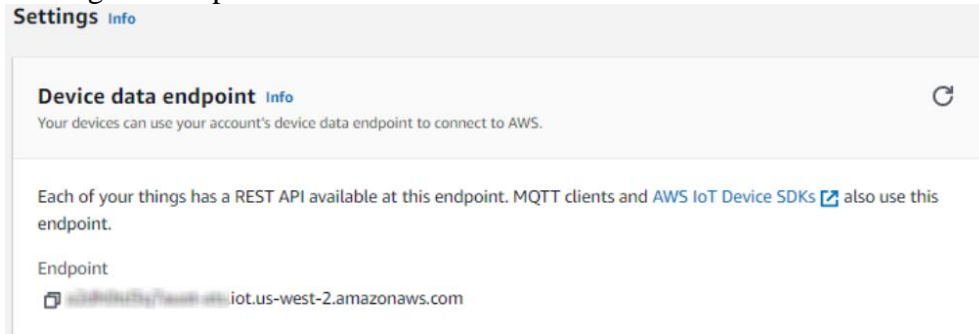


Figure 9. Device data endpoint

8.3. Configuring the device

8.3.1. Security and certificates

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

Name	Date modified	Type	Size
 5b969d6ec60b63c966b9e9f9bf79ae916b03448d6c7711617e85026d8ac0e9d9-certificate.pem.crt 1	2022-02-07 11:34	Security Certificate	2 KB
 5b969d6ec60b63c966b9e9f9bf79ae916b03448d6c7711617e85026d8ac0e9d9-private.pem.key 2	2022-02-07 11:34	KEY File	2 KB
 AmazonRootCA1.pem 3	2022-02-07 11:34	PEM File	2 KB

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

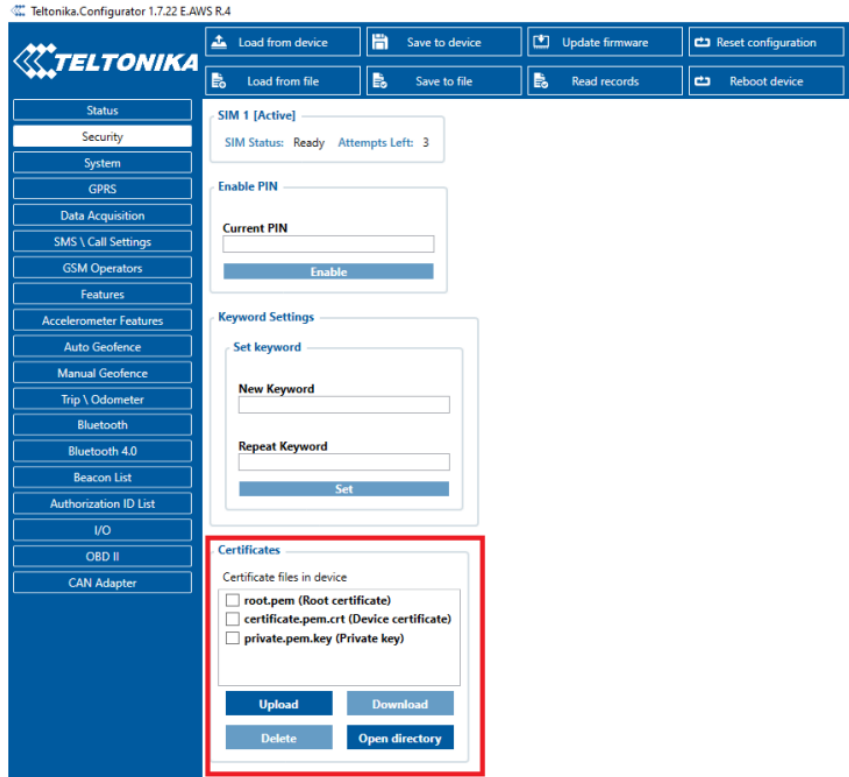


Figure 10. Uploading certificates

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



Figure 11. Selecting Data protocol

8.3.2. 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.

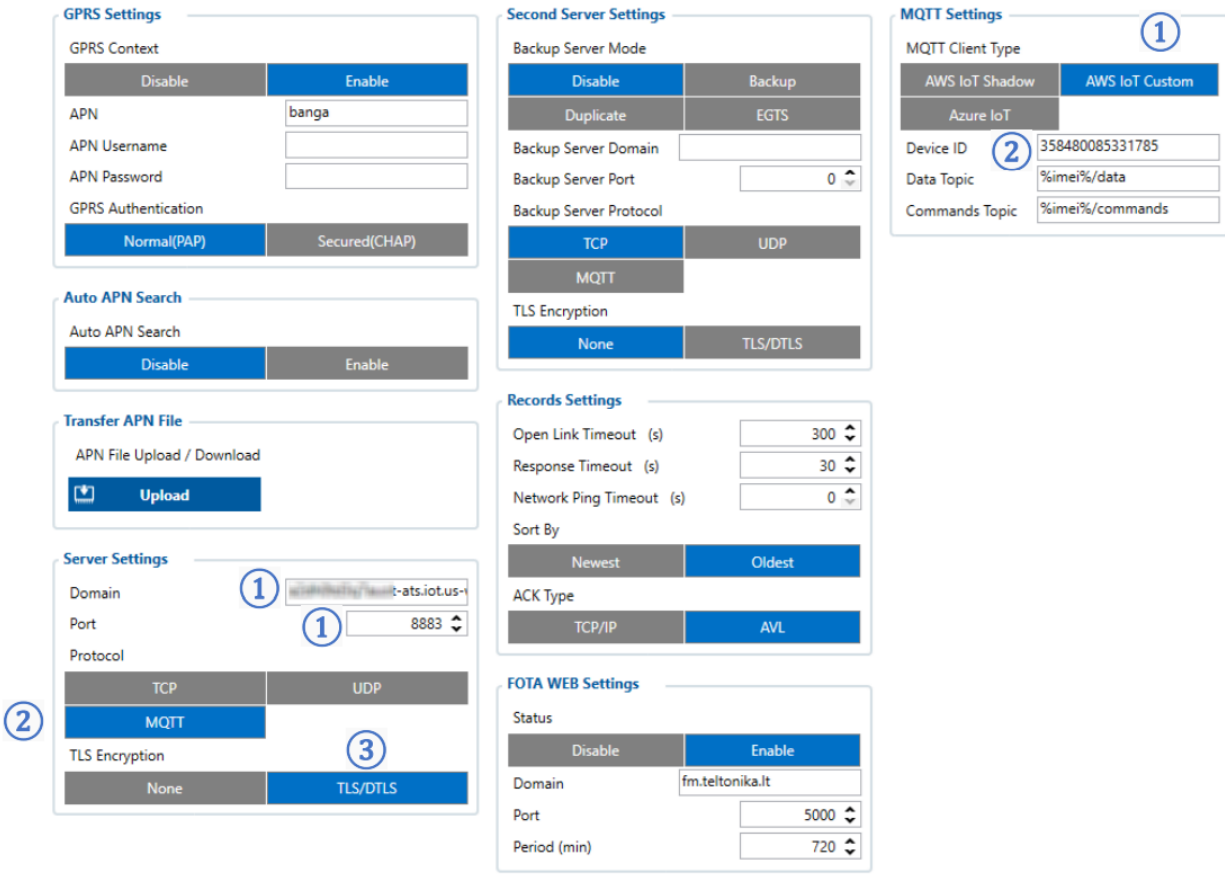


Figure 12. GPRS settings for MQTT AWS IoT Custom

9 Run the demo

The data received from the device can be found in the MQTT test client, which can be found in the bottom of sidebar on the left.

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

AWS IoT > MQTT test client

MQTT test client [Info](#)

You can use the MQTT test client to monitor the MQTT messages being passed in your AWS account. Devices publish MQTT messages that are identified by topics to communicate their state to AWS IoT. AWS IoT also publishes MQTT messages to inform devices and apps of changes and events. You can subscribe to MQTT message topics and publish MQTT messages to topics by using the MQTT test client.

[Subscribe to a topic](#) | [Publish to a topic](#)

Topic filter [Info](#)
The topic filter describes the topic(s) to which you want to subscribe. The topic filter can include MQTT wildcard characters.

► Additional configuration

[Subscribe](#)

Subscriptions **358480085331785/data** Pause Clear Export Edit

Favorites	358480085331785/data	February 07, 2022, 12:41:46 (UTC+0200)
358480085331785/data ♥ ✕	▼ 358480085331785/data	
358480085331785/commands ♥ ✕	{	
{ "CMD": "setdigout 111" } ♥ ✕	"state": {	
All subscriptions	"reported": {	
# ♥ ✕	"16": 0,	
	"21": 4,	
	"66": 14884,	
	"67": 3982,	
	"68": 0,	
	"69": 1,	
	"179": 0,	
	"180": 0,	
	"181": 10,	
	}	
	}	
	}	

Figure 13. Subscribing to data topic

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

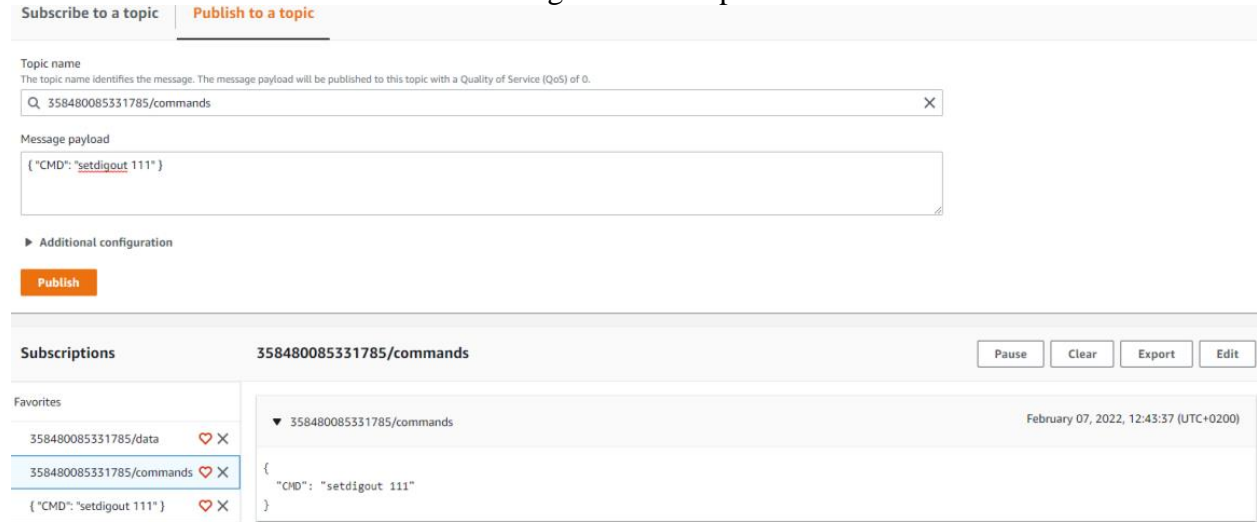
```

{
  "format": "json",
  "topic": "358480085331785/data",
  "timestamp": 1644227812734,
  "payload": {
    "state": {
      "reported": {
        "16": 0,
        "21": 4,
        "66": 14547,
        "67": 4019,
        "68": 144,
        "69": 1,
        "179": 0,
        "180": 0,
        "181": 9,
        "182": 6,
        "200": 0,
        "239": 1,
        "240": 0,
        "241": 24602,
        "380": 0,
        "ts": 1644227810000,
        "pr": 1,
        "latlng": "54.700450,25.259818",
        "alt": 128,
        "ang": 0,
        "sat": 15,
        "sp": 0,
        "evt": 0
      }
    }
  }
}

```

Figure 14. Received data format

To send SMS/GPRS commands to the device, 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:



Subscribe to a topic **Publish to a topic**

Topic name
The topic name identifies the message. The message payload will be published to this topic with a Quality of Service (QoS) of 0.

Q 358480085331785/commands X

Message payload
{ "CMD": "setdigout 111" }

► Additional configuration

Publish

Subscriptions 358480085331785/commands Pause Clear Export Edit

Favorites

- 358480085331785/data ♥ ✕
- 358480085331785/commands ♥ ✕
- { "CMD": "setdigout 111" } ♥ ✕

▼ 358480085331785/commands February 07, 2022, 12:43:37 (UTC+0200)

```
{
  "CMD": "setdigout 111"
}
```

Figure 15. Sending Comand in AWS IoT Core

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



Subscriptions 358480085331785/data Pause Clear Export Edit

Favorites

- 358480085331785/data ♥ ✕
- 358480085331785/commands ♥ ✕
- { "CMD": "setdigout 111" } ♥ ✕

▼ 358480085331785/data February 07, 2022, 12:43:41 (UTC+0200)

```
{
  "RSP": "DOUT1:1 Timeout:INFINITY DOUT2:1 Timeout:INFINITY DOUT3:1 Timeout:INFINITY "
}
```

Figure 16. Response to a command in the data topic, the command was published in command topic

10 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](#).

11 Troubleshooting

The information can be submitted to Teltonika HelpDesk and Teltonika engineers will assist with troubleshooting. General information what information should be collected described [here](#).

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