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
<i>8.3</i> .	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	0
10	Debugging	2
11	Troubleshooting	2

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 <u>https://wiki.teltonika-iot-group.com/</u>.
- 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 scheet can be downloaded here: <u>https://teltonika-gps.com/downloads/en/fmm130/Datasheet-FMM130-2.1-web-</u> <u>Telematics.pdf</u>

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 <u>FMM130_First_Start</u>.
- Device characteristics, power supply information: <u>FMM130_General_description</u>
- FMM130 firmware change can be performed via FotaWEB (direct buyer gets access to this platform) FotaWEB or via device <u>configurator</u>
- Device LED information: <u>FMM130_LED_status</u>
- 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 <u>Set up your AWS Account</u>. 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
- <u>Create a user and grant permissions</u>
- Open the AWS IoT console

Pay special attention to the Notes.

7 Create Resources in AWS IoT

Refer to the online AWS documentation at <u>Create AWS IoT Resources</u>. Follow the steps outlined in these sections to provision resources for your device:

- <u>Create an AWS IoT Policy</u>
- 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.

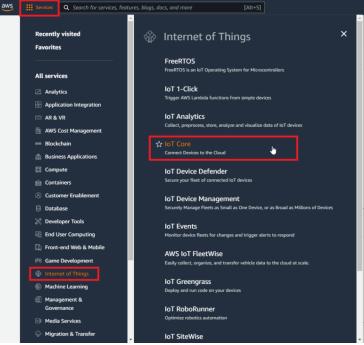


Figure 1. Accessing AWS IoT core from AWS console

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

aws III Services	Search for services, features, blogs, docs, and more [Alt+5]	Þ.	\$ 0	Oregon 🔻	fmb920comp 🔻
AWS IoT	AWS loT > Manage > Things				
Monitor Activity	Things (1) set Ab int laws a sequence of your physical device in the cloud. A physical device media a triage mergin loader to work with AMS NT.	Edit	Delete	Create th	lings
 Connect Manage 	Q. Filter things by: name, type, group, billing, or searchable attribute.			< 1 >	۲
Overview Things	Name Thing type				
Types	No things No things to display in this Region				
Thing groups Billing groups Jobs	Create things				
Job templates					

Figure 2. Accessing Things

Afterwards for select Create single thing and click Next.

	esource is a digital representation of a physical device or logical entity in AWS IoT. Your device or entity needs a t in the registry to use AWS IoT features such as Device Shadows, events, jobs, and device management features.
a c c	in the registry to use Phrs for restarce such as perfect shouldws, events, jobs, and device monagement reatures.
un	nber of things to create
0	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.
0	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.

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.

Specify thing properties 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.			
Step 2 - optional	resource in the registry to use AWS 101 reatures such as Device Shadows, events, jobs, and device management reatures.			
Configure device certificate	Thing properties Info			
Step 3 - optional	Thing properties Into			
Attach policies to certificate	Thing name			
	FMB130			
	Enter a unique name containing only: letters, numbers, hyphens, colons, or underscores. A thing name can't contain any spaces.			
	more a number on one of an of a number of the solution of a non-solution of the solution of the			
	Additional configurations			
	You can use these configurations to add detail that can help you to organize, manage, and search your things.			
	Thing type - optional			
	· ming the obtained			
	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.			
	O No shadow			
	O Named shadow			
	Create multiple shadows with different names to manage access to properties, and logically group your devices properties.			
	O Unnamed shadow (classic)			
	A thing can have only one unnamed shadow.			

Figure 4. Specifying thing properties

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

AWS IoT > Manage > Things >	Create things > Create single thing					
Step 1 Specify thing properties	Configure device certificate – <i>optional</i> 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					
Step 2 - optional Configure device certificate and register a certificate for your device later. Your device won't be able to connect to AWS IOT active certificate with an appropriate policy.						
Step 3 - optional Attach policies to certificate	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.					
	O 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 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 * .

Create policy Info

AWS IOT Core policies allow you to manage access to the AWS IoT Core data plane operations.		
Policy properties AWS IoT Care supports named policies so that many identities can reference the same policy document.		
Policy name		
FMB130Policy		
A policy name is an alphanumeric string that can also contain period (), comma (), hyphen(-), underscore (), plus sign (+), equal sign (e), and at sign (g) characters, but no spaces.		
▶ Tags - optionol		
Policy document info An AWS IoT policy contains one or more policy statements. Each policy statement contains actions, resources, and an effect that grants or denies the actions by the resources.	Juilder	JSON
Policy effect Allow Policy action Policy resource		
Add new statement		
	Cancel	Create

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

AWS IoT > Manage > Things > Create things > Create single thing							
Step 1 Specify thing properties	Attach policies to certificate – <i>optional</i> Info AWS IoT policies grant or deny access to AWS IoT resources. Attaching policies to the device certificate applies this access to						
Step 2 - <i>optional</i> Configure device certificate	the device.						
Step 3 - optional Attach policies to certificate	Policies (1/1) Select up to 10 policies to attach to this certificate.	C Create policy 🖸					
	Q Filter policies	< 1 > ©					
	✓ Name						
	FMB130Policy						
	Cancel	Previous 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.

Download certificate and key files t AWS.	to install on your device so that	it can connect to
Device certificate You can activate the certificate now, or la	iter. The certificate must be active fo	r a device to connect to
AWS IoT.		
Device certificate	Deactivate certificate	Download
5b969d6ec60te.pem.crt		
Key files		
The key files are unique to this certificate Download them now and save them in a		leave this page.
		6
A This is the only time you car	n download the key files for this	certificate.
Public key file		Download
5b969d6ec60b63c966b9e9fac0e	9d9-public.pem.key	Key downloaded
Private key file		
5b969d6ec60b63c966b9e9fc0e9	d9-private.pem.key	Key downloaded
Root CA certificates		
Download the root CA certificate file that you're using. You can also download the		lpoint and cipher suite
Amazon trust services endpoint		Download
RSA 2048 bit key: Amazon Root CA	1	
Amazon trust services endpoint		
ECC 256 bit key: Amazon Root CA 3	5	
If you don't see the root CA certific root CA certificates. These root CA guides. Learn more 🔀	,	
gorees continue :		_

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. Settings Info

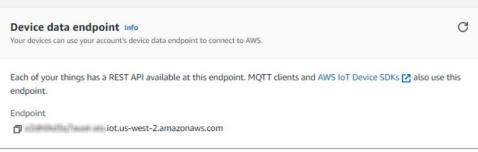


Figure 9. Device data endpoint

8.3. Configuring the device

8.3.1. Security and certificates

Find Certificate file ending with extension pem.crt Private key file and AmazoonRootCA1 file (no need to change filenames). These file should have been downloaded when creating Thing in AWS IoT Core.

Name	Date modified	Туре	Size
🗔 5b969d6ec60b63c966b9e9f9bf79ae916b03448d6c7711617e85026d8ac0e9d9-certificate.pem.crt	2022-02-07 11:34	Security Certificate	2 KB
5b969d6ec60b63c966b9e9f9bf79ae916b03448d6c7711617e85026d8ac0e9d9-private.pem.key	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.

+	📤 Load from device	Save to device	Update firmware	Reset configuratio
TELTONIKA	Load from file	Save to file	Read records	C Reboot device
Status	SIM 1 [Active]			
Security	SIM Status: Ready A	ttempts Left: 3		
System	· · · ·			
GPRS	Enable PIN			
Data Acquisition	C			
SMS \ Call Settings	Current PIN			
GSM Operators	Enable			
Features	L			
Accelerometer Features	Keyword Settings			
Auto Geofence	Set keyword			
Manual Geofence				
Trip \ Odometer	New Keyword			
Bluetooth				
Bluetooth 4.0	Repeat Keyword			
Beacon List	Se	•		
Authorization ID List	30	S.		
I/O				
OBD II	Certificates			
CAN Adapter	Certificate files in device			
	root.pem (Root cer certificate.pem.crt private.pem.key (P	(Device certificate)		
	Upload	Download		

Figure 10. Uploading certificates

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



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.

	GPRS Settings		Second Server Settings —		MQTT Settings	(1)
	GPRS Context		Backup Server Mode		MQTT Client Type	
	Disable	Enable	Disable	Backup	AWS IoT Shadow	AWS IoT Custom
	APN	banga	Duplicate	EGTS	Azure IoT	
	APN Username		Backup Server Domain		Device ID	58480085331785
	APN Password		Backup Server Port	0 🌩	bata topic	%imei%/data
	GPRS Authentication		Backup Server Protocol		Commands Topic	%imei%/commands
	Normal(PAP)	Secured(CHAP)	тср	UDP		
	Auto APN Search		MQTT			
			TLS Encryption			
	Auto APN Search Disable	Enable	None	TLS/DTLS		
	Disable	Enable				
	Transfer APN File		Records Settings			
	APN File Upload / Download		Open Link Timeout (s)	300 \$		
	Upload		Response Timeout (s) Network Ping Timeout (s)	30 ↓		
	(iiiii) opioid		Sort By	0 🗸		
	Server Settings		Newest	Oldest		
	Domain (1)	t-ats.iot.us-	ACK Type	CIGCS		
	Port	8883 \$	TCP/IP	AVL		
	Protocol					
	тср	UDP	FOTA WEB Settings			
(2)	MQTT		Status			
\smile	TLS Encryption	(3)	Disable	Enable		
	None	TLS/DTLS	Domain fr	n.teltonika.lt		
			Port	5000 🗘		
			Period (min)	720 🗘		

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						
	tor the MQTT messages being passed in your AWS account. Device d events. You can subscribe to MQTT message topics and publish h	s publish MQTT messages that are identified by topics to communicate their MQTT messages to topics by using the MQTT test client.	state to AWS IoT. AWS IoT also publishes MQTT messages			
Subscribe to a topic Pub	lish to a topic					
	h you want to subscribe. The topic filter can include MQTT wildcard character	5.				
#						
 Additional configuration 						
Subscribe						
Subscriptions	358480085331785/data		Pause Clear Export Edit			
Favorites	▼ 358480085331785/data	ſm	February 07, 2022, 12:41:46 (UTC+0200)			
358480085331785/data 💙 🕽						
358480085331785/commands 💙 🕽	< { "state": {					
{ "CMD": "setdigout 111" }	<pre>x "reported": {</pre>					
"10": 0, All subscriptions "21": 4, "66": 14884.						
# Ø)						

Figure 13. Subscribing to data topic

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

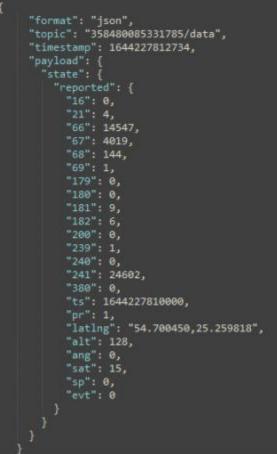


Figure 14. Received data format

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:

Topic name The topic name identifies the message. The messa	ge payload will be published to this topic with a Quality of Service (QoS) of 0.	
Q 358480085331785/commands		×
Message payload		
{"CMD": "setdigout 111" }		
Additional configuration Publish		
Subscriptions	358480085331785/commands	Pause Clear Export Edit
Favorites 358480085331785/data ♡ 🗙	▼ 358480085331785/commands	February 07, 2022, 12:43:37 (UTC+0200)
358480085331785/commands ♡ 🗙	{ "CMD": "setdigout 111" }	
{ "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	February 07, 2022, 12:43:41 (UTC+0200)
358480085331785/data 🛛 💙 🗙	• 200400002021100/04ta	
358480085331785/commands 🛇 🗙	{ "RSP": "DOUT1:1 Timeout:INFINITY DOUT2:1 Timeout:INFINITY DOUT3:1 Timeout:INFINITY " }	
{ "CMD": "setdigout 111" }		

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 (<u>instructions</u>), via Terminal.exe by connecting selecting device USB connection port, or by receiving internal logs via FotaWEB in <u>task section</u>.

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 <u>here</u>.

Alternatively, Teltonika has a <u>Crowd Support Forum</u> dedicated for troubleshooting, where engineers are actively solving problems.