FMB001 Getting Started with AWS IoT Core

<u>Main Page</u> > <u>OBD Trackers</u> > <u>FMB001</u> > <u>FMB001 Manual</u> > **FMB001 Getting Started with AWS IoT Core**

Contents

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

Document Information

Glossary

- FMB001 (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.

Revision History (Version, Date, Description of change)

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

Overview

FMB001 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. FMB001 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: <u>FMB001</u> <u>firmware errata</u>

Hardware Description

DataSheet

FMB001 device data sheet can be downloaded here: DataSheet

Standard Kit Contents

STANDARD PACKAGE CONTAINS

- 20 pcs. of FMB001 trackers
- 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)

FMB001 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 <u>FM Configurator</u> <u>versions</u>, 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 <u>FotaWEB</u> platform or by using Teltonika Configurator.

Set up your hardware

All details about FMB001 can be located in our dedicated wiki page FMB001 Wiki

- Basic device startup instructions provided in FMB001 First Start.
- Device characteristics, power supply information: FMB001 General description
- FMB001 firmware change can be performed via <u>FotaWEB</u> (direct buyer gets access to this platform) or via device <u>Configurator</u>
- Device LED information: <u>FMB001 LED Status</u>
- USB driver download, datasheet and quick start guide downloads: FMB001 Downloads

Document Information

Glossary

- 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.

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 <u>FotaWEB</u> 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
- <u>Create a user and grant permissions</u>
- 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
- <u>Create a thing object</u>

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.

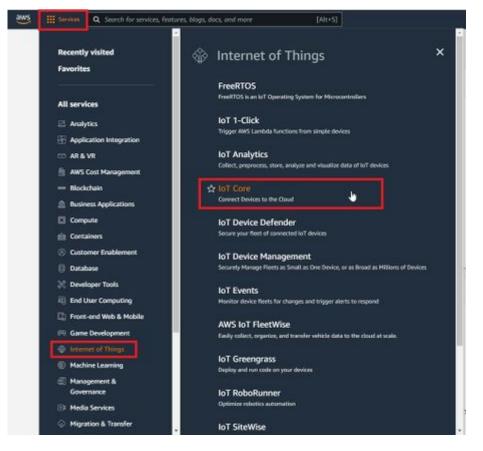


Figure 1. Accessing AWS IoT core from AWS console

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.

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.

0	
	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 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.

	Step 1 Specify thing properties	Specify thing properties into A thing resource is a digital representation of a physical device or logical entity in AWS IoT. Your device or entity needs a thing
	Step 2 - optional Configure device contificate	resource in the registry to use AWS IoT features such as Device Shadows, events, jobs, and device management features.
	Step 3 - optionol Attach policies to certificate	Thing name
		FMB150
		Enter a unique name containing only: letters, numbers, hypitens, colore, or underscores. A thing name can't contain any spaces.
		Additional configurations. New see was these configurations to addidetal that can help you to reparties, manage, and search your things.
		Thing type - optionol
		Searchable thing attributes - optional
		Thing groups - optional
		Billing group - optional
		Device Shadow Inte
		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 HITPs or MQTT tapks.
		O No shadow
		 Named shadow Deale multiple shadows with different names to manage access to properties, and logically group your devices properties.
		Unnamed shadow (classic) A thing see have only one unnamed shadow.

Figure 6. Thing's properties

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

	Step 1 Specify thing properties	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, 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 a
	Step 2 - optional Configure device certificate	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 Nex

Figure 7. Certificate configuration

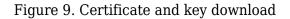
Now, select the policy you have created before to attach it to the certificate and thing. After that click Create thing.

aws	Services Q. Search for services, for	eatures, blogs, docs, and more [Alt+S]
=	AWS IoT > Manage > Things > Step 1 Specify thing properties Step 2 - optional Configure device certificate	Create things > Create single thing 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.
	Step 3 - optional Attach policies to certificate	Policies (1/1) C Create policy C Select up to 10 policies to attach to this certificate. < 1 > ©
		Image: Name Image: 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.

Download certificates a	nd keys	×
Download certificate and key fi AWS.	les to install on your device so that	it can connect to
Device certificate		
You can activate the certificate now, AWS NOT.	or later. The certificate must be active for	e a device to connect to
Device certificate	Deactivate certificate	E Download
0dd95461837te.pem.crt		
Key files		
	icate and can't be downloaded after you In a secure place.	leave this page.
\triangle This is the only time you	can download the key files for this	certificate.
Public key file		Downtoad
	169fc43-public.pem.key	E Download
0dd954618370b2db8d39c1f	1b9fc43-public.pem.key	E Download
0dd954618370b2db8d39c1f Private key file		
Public key file 0dd95461837062db8d39c14 Private key file 0dd95461837062db8d39c14 Root CA certificates		
0dd95461837062db8d39c14 Private key file 0dd95461837062db8d39c14t Root CA certificates Dewnload the root CA certificate file	b9fc43-private.pem.key that corresponds to the type of data en	E Download
0dd954618370b2db8d39c1f Private key file 0dd954618370b2db8d39c1fk Root CA certificates	b9fc43-private.pem.key that corresponds to the type of data en the root CA centRicates later.	E Download
0dd954618370b2db8d39c14 Private key file 0dd954618370b2db8d39c14 Root CA certificates Download the root CA Certificate file you're osing. You can also download Amazon thust services endpoint	b9fc43-private.pem.key that corresponds to the type of data en the root CA certificates later.	Dewnload
0dd954618370b2db8d39c14 Private key file 0dd954618370b2db8d39c14t Root CA certificates Dewritiad the root CA certificate file you're using. You can also dowritiad	b9fc43-private.pem.key that corresponds to the type of data end the root CA centRicates late. t t CA 1	Dewnload
0dd954618370b2db8d39c14 Private key file 0dd954618370b2db8d39c14t Root CA certificates Download the root CA certificate file you're using. You can also download Amazon trust services endpoint RSA 2048 bit key: Amazon Root Amazon trust services endpoint	b9fc43-private.pem.key that corresponds to the type of data en- the root CA certificates late. t t CA 1 t	Download
0dd954618370b2db8d39c14 Private key file 0dd954618370b2db8d39c14t Root CA certificates Downtoad the root CA certificate file you're sing. You can also downiad Amazon trust services endpaint RSA 2048 bit key: Amazon Root Amazon trust services endpaint ECC 256 bit key: Amazon Root I	b9fc43-private.pem.key that corresponds to the type of data en- the root CA certificates late. t t CA 1 t	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.

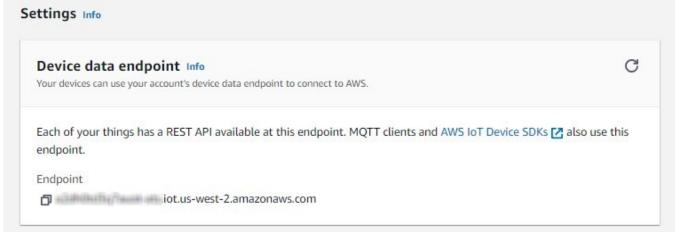


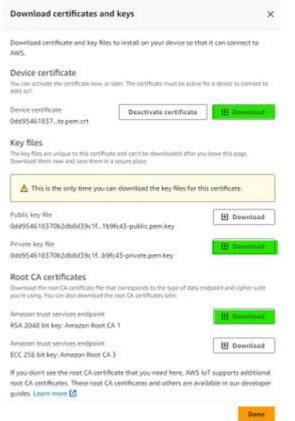
Figure 10. Device data endpoint

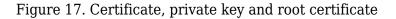
Configuring the device

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 AmazoonRootCA1 file (no need to change filenames). These files should have been downloaded when creating Thing in AWS IoT Core.





Upload the mentioned files in the Security tab in the Teltonika Configurator. $\fbox{}$

Figure 18. Uploading certificates and keys

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

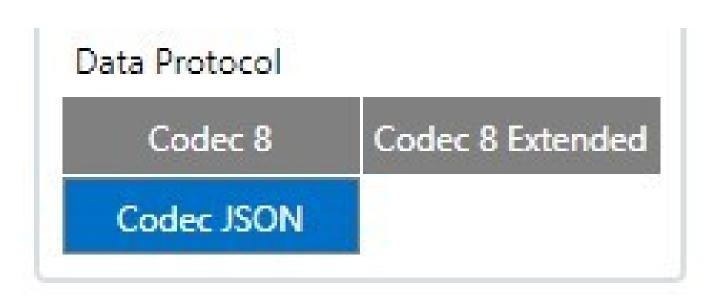


Figure 19. Choosing data protocol

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. \blacksquare

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.

S IoT > MQTT test client			
QTT test client տ			
	onitor the MQTT messages being passed in your AWS account. Devices and events. You can subscribe to MQTT message topics and publish M		e their state to AWS IoT. AWS IoT also publishes MQTT messages
Subscribe to a topic P	ublish to a topic		
Topic filter Into The topic filter describes the topic20 to v	thich you want to subscribe. The topic filter can include MQTT wildcard characters.		
£			
Subscribe			
Subscriptions	358480085331785/data		Pause Clear Export Edit
Subscriptions	358480085331785/data	ç	Pause Clear Export Edit February 07, 2022, 12:41:46 (UTC+0200)

Figure 29. MQTT test client

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

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/> "}
---------	-----------------

fopic name The topic name identifies the message. The messa	pe 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		
 Additional configuration 		
Publish		
Publish		
	358480085331785/commands	Pause Clear Export Edit
Subscriptions		
Subscriptions	358480085331785/commands ▼ 358480085331785/commands	Pause Clear Export Edit February 07, 2022, 12:43:37 (UTC+0200)
Subscriptions	 358480085331785/commands (
Subscriptions avoiltes 358480085331785/data ♡ 🗙		
Subscriptions avorites 358480085331785/data ♡ 🗙 358480085331785/commands 🏹 🗙	 358480085331785/commands ("CHD": "setdigout 111" 	
Subscriptions avorites 358480085331785/data 🗢 X 358480085331785/commands 🗢 X (*CMD:: "setdigout 111") 📀 X	 358480085331785/commands ("CHD": "setdigout 111" 	

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

Subscriptions	358480085331785/data	Pause Clear Export Edit
avorites 358480085331785/data ♡×	▼ 358480085331785/dətə	February 07, 2022, 12:43:41 (UTC+0200)
358480085331785/commands ♥ × ("CMD": "setdigout 111") ♥ ×	<pre>{ "RSP": "DOUT1:1 Timeout:INFINITY DOUT2:1 Timeout:INFINITY DOUT3:1 Timeout:INFINITY " }</pre>	
l subscriptions		

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 (<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>.

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 <u>Teltonika Wiki</u>.

Alternatively, Teltonika has a <u>Crowd Support Forum</u> 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 <u>Teltonika Wiki</u>.

Alternatively, Teltonika has a <u>Crowd Support Forum</u> 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 (<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>.