TRACKER’S SECURITY

Contents

Disclaimer

If you are not using Bluetooth®, **please consider turning it off** or **change Bluetooth® PIN** to remove potential risks.

If you are using Bluetooth® we strongly recommend **using AES encryption** for enhanced security.

Solution description

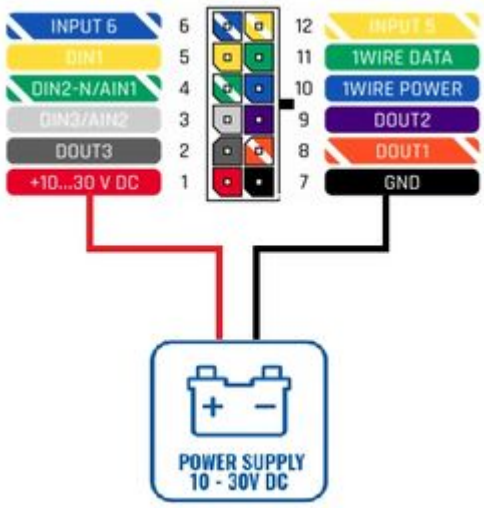
GPS trackers provide valuable data for business efficiency and secure vehicles against thefts. At the same time, the tracking devices can be stolen with a purpose to sell them, sabotaged by reconfiguring with fault parameters, or hacked to steal sensitive data. To prevent unauthorized access to the trackers, it is necessary to have additional security measures for logging in through all possible devices. When a login fails, the user is denied access and trackers remain safe. This solution details the settings and features to keep your device safe.

What you need for a solution?

- All Teltonika FMB devices are compatible with this use case (FMB0YX, FMB9X0, FMB1YX, FMU1YX, FMM1YX, FMC1YX, FMB2YX, and the model FMT100 for TLS).
- The SIM card in order to receive data to Your server.

- Teltonika Configurator to set up FMB device correctly for the solution.
- Fota Web to remotely send the configuration to the device.
- FMBT Mobile application for changes your server IP address, port, and APN data on the device and watch all primary informations (such as: GNSS, GSM, I/O elements status, OBD, and LV-CAN200/ALL-CAN300 live data)
- TLS/DTLS prepare guide

Installation



Instalation

For gain access to ability change default security state (for device from the factory) you need power up device (10-30V) and connect via USB to the PC. After device will be powered and LED indicators start work you can access to settings.

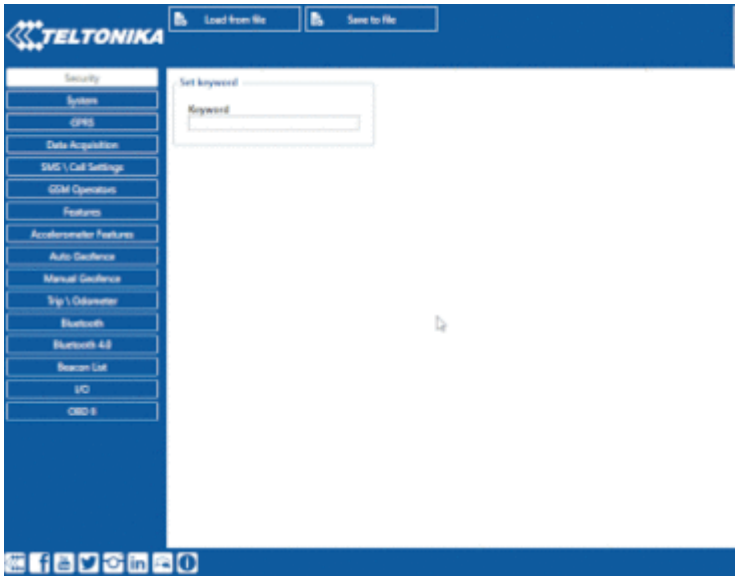
Configuration

1. Prerequisites:

1.1. Read through [First start guide]

2. Configurate Tracker Security:

2.1. Set up Keyword:



Set up keyword

Configuration security keyword can be set to configurator. Keyword can be saved in configuration file (.cfg), so there is no need to connect the device to the configurator to configure the keyword. Minimum keyword length is 4 symbols and maximum length is 10 symbols. Only uppercase and lowercase letters and numbers are supported. Keyword can be configured to .cfg configuration file when the device is not connected.

It can be changed via USB and also via SMS.

For SMS opportunity of change configurations read descriptions of avaible FMB130 SMS/GPRS Commands

For setup keyword need command *setkey # #* (Add new or change current configuration keyword. If device is locked, keyword cannot be changed) where

1.# - old keyword (if adding new keyword space).

2.# - new keyword.

- If you have set SMS login and password: `login pass setkey # #`
- If SMS login and password are not set leave two spaces before command: `setkey`

For ability remove keyword, you need command *delkey #* , where # - old keyword.

This command will emove existing keyword. If device is locked, keyword cannot be changed.

2.2. SMS security:

Set up sms secutiry

Essential fields in SMS/Call settings are Login and Password. The login and password are used with every SMS sent to FMB130. If login and password are not set, in every SMS sent to FMB125 device two spaces before command have to be used (<space><space><command>).

Command structure with set login and password:
<login><space><password><space><command>, for example: "123 123 getgps"

Phone numbers have to be written in international standard, using "+" is optional but not necessary (in both cases number will be recognized, but when number is without "+" symbol, IDD Prefix will not be generated, which depends on location of the phone). If no numbers are entered, configuration and sending commands over SMS are allowed from all GSM numbers.

2.3 FMBT App

FMBT Mobile application

By using Teltonika FMBT application on smartphones and filling up a pin for pairing with a tracker or adding your device to configurator authorized devices MAC list you can get:

- Device name, IMEI and firmware version
- Current status
- GNSS Status, coordinates and satellite info
- GSM Status, Record, Data packet and SMS counts, AVL server socket status
- I/O element status

2.4 FOTA WEB

To upgrade firmware or make configuration changes, you need to fill up a login and password in your browser that uses HTTPS protocol. The user creates a password on his own. Make sure to follow the mentioned comments to save the password successfully.

Password must contain:

- at least one uppercase letter
- at least one lowercase letter
- at least 8 characters

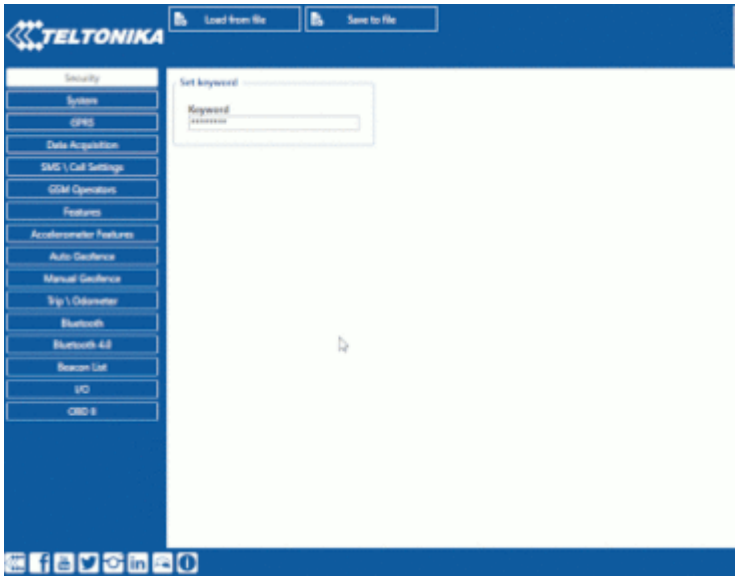
2.5 BLE STANDARD AES-128

BLE standart AES-128

Since this version **03.27.07** there has been an implementation of BLE transferred data encryption with **AES128 cipher**. In **Bluetooth® 4.0 tab** under **Settings** there is a field for a **AES128 key**. Which if left empty, the BLE outgoing data will not be ciphered and incoming data will not be decoded. AES128 key field settings showed below.

If a key is present the outgoing data will be ciphered by the configured key and incoming data will be deciphered. The **AES128 key** must be in **HEX format with a length of 16 bytes**. As an example 11223344556677889900AABBCCDDEEFF is used.

SECURE CONNECTION TO SERVER (TLS)



TLS

In 03.27.07 base firmware version, Transport Layer Security TLS functionality has been updated and implemented for Teltonika GPS device series FMB0YX, FMB9X0, FMB1YX, FMU1YX, FMM1YX, FMC1YX, FMB2YX, and the model FMT100. TLS is a cryptographic protocol that provides end-to-end security of data sent between server and tracker. There are three main components to what the TLS protocol accomplishes: Encryption, Authentication, and Integrity. Encryption: hides the data being transferred from third parties. Authentication: ensures that the parties exchanging information are who they claim to be. Integrity: verifies that the data has not been forged or tampered with. From 03.27.xx firmware version, TLD/DTLS functionality was implemented for FMB0YX, FMB9X0, FMB96X, FMB1YX, FMU1YX, FMM1YX, FMC1YX, FM30XY, FMB2YX, FMT100 device. Note! Currently only TLS encryption functionality is fully implemented, if needed DTLS encryption is possible to implement. Supported versions: 1.1/1.2

All preparation describe in the TLS/DTLS prepare guide in the device you need activate this