

# TRACKERS' SECURITY

## INTRO

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.

## CHALLENGE

Vehicle trackers store **sensitive data** for business and thanks to various features help to arrange optimal routes to avoid delays, reduce fuel consumption, get timely maintenance, and secure cargo with a vehicle. When losing a tracker or the control of it, business forfeits the possibility to monitor a vehicle and that can lead to serious consequences.

Stealing a tracker or overtaking its control can cause major issues for big businesses and small companies alike. You can do a lot to **improve the security** of your trackers, though. While there are no absolute guarantees, you should make it as hard as possible for the thieves to overtake the trackers that you have invested time to install and configured for an efficient data collection and monitoring. Otherwise, losing a tracker will also mean losing your income.

Our tracking solutions offer much more than just a simple tracking. A wide range of functionalities is available and – what is most important – we provide **secure connectivity** for all our devices.



## SOLUTION

Setting up a password, pin, or keyword before using the tracker is a must. Installing a tracker out of the box without reconfiguring it for security purposes is one of the most common mistakes that integrators make. However, it is easy to correct this by creating **strong passwords** (at least 8 characters: a mix of uppercase and lowercase letters, numbers, and minimum one special character). Failing to make these changes makes it simple for the thieves to gain access to the trackers since they might know or find out the original settings.

With Teltonika options for secure connections, it becomes hard to steal or sabotage the trackers. All Teltonika tracking devices support the safety measures listed below, including **FMB130**, which is a perfect choice for miscellaneous use scenarios.

### CONFIGURATOR KEYWORD

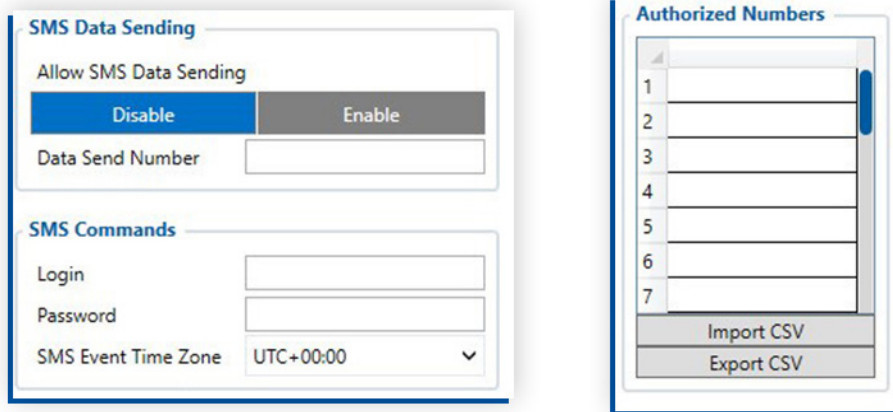
Access to the configurator should be limited only to those who need to use it. For company employees to configure trackers via computer, a keyword is required if connecting via USB. In case of accessing tracker configuration via Bluetooth connection, a pin is used to pair with the device in addition to a keyword.

A screenshot of a web interface for setting a keyword. The title is 'Set keyword'. Below it is a text input field with the label 'Keyword'.

## SMS SECURITY

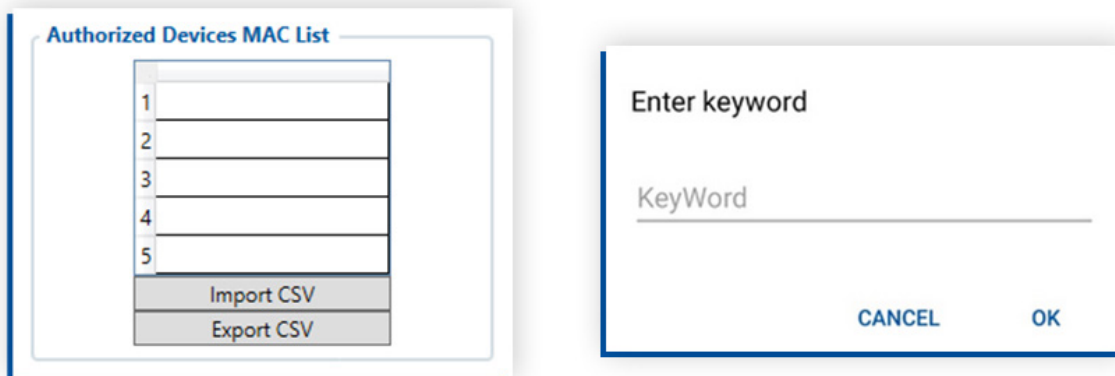
You can use SMS login and SMS password to access Teltonika trackers. Besides, it is also possible to configure devices via SMS commands.

For an additional security via SMS, you can add telephone numbers to the authorized number list in the Teltonika configurator. The trackers will ignore all commands coming from the numbers that are not listed in the configurator, thus, nobody else will be able to configure the devices or sabotage them.



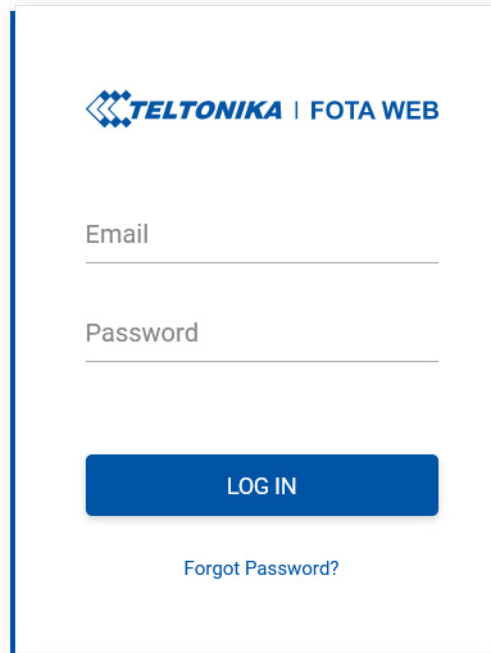
## FMBT APP

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 see every detail about your device, including primary information, GNSS, GSM, I/O elements status, OBD, and LV-CAN200/ALL-CAN300 live data. To set up tracker via Bluetooth connection, you need to insert keyword and the application will allow you to change your server IP address, port, and APN data on the device.



## FOTA WEB

With FOTA WEB, you will have an easy access to your fleet anywhere in the world. To upgrade firmware or make configuration changes, you just need to fill up a login and password in your browser that uses HTTPS protocol – it means all communication between your browser and the website are encrypted! For safety reasons, be sure not to disclose your login data to unauthorized personnel.



TELTONIKA | FOTA WEB

Email

Password

LOG IN

[Forgot Password?](#)

## BLE STANDARD AES-128

Starting from the firmware base version **03.27.07**, we have successfully implemented the [Advanced Encryption Standard AES-128](#) to ensure the most secure transfer of [Bluetooth Low Energy](#) (aka BLE) data between [Teltonika GPS trackers](#) and dedicated mobile apps. If an AES Key is present in HEX format, the outgoing data will be ciphered by the configured key, and incoming data will be deciphered.

Please note, this is one of the most robust and sophisticated serial encryption schemes today. You can learn more about the technical aspects of this feature [here](#).



BLE Serial Encryption

AES Key

## SECURE CONNECTION TO SERVER (TLS)

Going further, as of 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. The layer is a cryptographic protocol that provides end-to-end security of data sent between server and vehicle GPS tracker. You can learn more about the technical aspects of the TLS update [here](#).

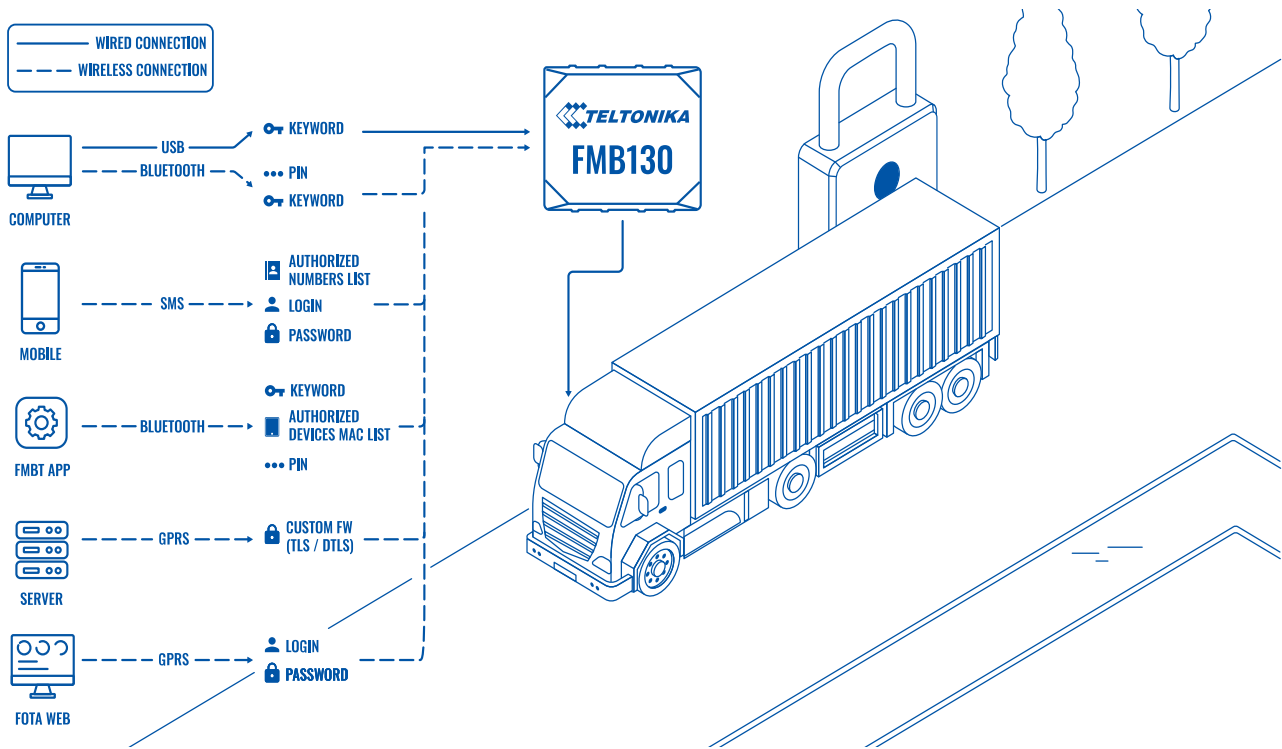
The screenshot displays the configuration interface for a Teltonika device. On the left is a vertical navigation menu with the following items: Status, Security, System, GPRS, Data Acquisition, SMS \ Call Settings, GSM Operators, Features, Accelerometer Features, Auto Geofence, Manual Geofence, Trip \ Odometer, Bluetooth, Bluetooth 4.0, Beacon List, 1-Wire, I/O, OB2 II, and CAN Adapter. The main content area is divided into several settings panels:

- GPRS Settings:** Includes GPRS Context (Disable/Enable), APN, APN Username, APN Password, and authentication options (Normal(PAP)/Secured(CHAP)).
- Auto APN search:** A simple Enable/Disable toggle.
- Transfer APN file:** Features an 'APN File Upload / Download' section with an 'Upload' button.
- Server Settings:** Includes fields for Domain and Port, and radio buttons for Protocol (TCP/UDP) and Encryption (None/TLS/DTLS). A mouse cursor is pointing at the TLS/DTLS option.
- Second Server Settings:** Includes Backup Server Mode (Disable/Backup), Duplicate/EGTS, Backup Server Domain, Backup Server Port, Backup Server Protocol (TCP/UDP), and Encryption (None/TLS/DTLS).
- Records Settings:** Includes Open Link Timeout (s), Response Timeout (s), Network Ping Timeout (s), Sort By (Newest/Oldest), and ACK Type (TCP/IP/AVL).
- FOTA WEB Settings:** Includes Status (Disable/Enable), Domain (fm.teltonika.lt), Port (50...), and Period (min).

## VPN

There are safety concerns about personal smartphones and mobile devices connecting to trackers. Private phones are more vulnerable to hacker attacks than servers connected to a company network. Many companies offer inexpensive mobile software that encrypts data traffic or monitors phones for suspicious activity. While the threats have been minimal and more of an annoyance so far, they are something to keep an eye on. For a secure connection, you can use a SIM card with VPN connection support. VPN allows you to create a safe connection to another network over the Internet and secure your browsing activity.

## TOPOLOGY



## BENEFITS

- **Security options for various devices** – be sure that Teltonika trackers are safe to use in your business with different security options (keywords, logins, passwords, pins, and authorized number lists) for all kinds of devices (phones, smartphones, computers, servers, and FMBT app) making your data secure.
- **Fast way to configure secure logins** – in the Teltonika configurator, it is easy to set up or change keywords, logins, and passwords, add authorized telephone numbers or fill the authorized devices MAC list.
- **Secure data sending** – VPN data encryption.

## WHY TELTONIKA?

Secure connection to Teltonika trackers allows you to feel safe about your sensitive business data and be sure that nobody else can connect to the devices. Based on our motto 'Easy key to IoT', we offer a fast way of setting up security logins, passwords or keywords, as well as trouble-free firmware upgrades and configuration of Teltonika trackers.

## FEATURED DEVICE

FMB130

## RECOMMENDED PRODUCTS

All Teltonika tracking devices

