Template:FMU GPRS settings

□

Contents

- 1 GPRS Settings and Server Settings
- 2 Second Server Settings
- 3 Records Settings
- 4 Auto APN
- 5 FOTA WEB Settings
- 6 TLS/DTLS
    - 6.1 TLS/DTLS certificate generation

GPRS Settings and Server Settings

These settings define the main parameters for FMB1YX: GSM operator *APN* and GPRS *Username* and *Password* (optional – depending on operator), destination server IP and port, and allows setting the protocol used for data transfers – TCP or UDP. An additional option is the use of TLS/DTLS encryption for sending records to the main server and backup server.

SIM1 and SIM2 *GPRS Settings* can be configured separately.

Second Server Settings

Backup server has 4 different modes:

- Disable: backup server is not used.
- Backup: records are sent to backup server if main server is not available (for example fails to open link) or when main server response timeout is reached successively 5 times.
- Duplicate: records are sent to both servers (main and backup), records are deleted from SD-card (or Flash storage) only if both servers accepted the records.
- EGTS: records are sent to both servers (main and backup), records are sent to the backup server using the EGTS protocol.

Some operators use a specific type of authentication for GPRS sessions – CHAP or PAP. If any of these is used, APN should be entered as "chap:<APN>" or "pap:<APN>" respectively e.g. if the operator is using APN "internet" with CHAP authentication, it should be entered as "chap: internet". Information about APN and authentication type should be provided by your GSM operator.
FMB1YX the device will send the newest records first when Newest is selected in *Records Settings*, which is useful in cases when the most important parameter set is the most recent one, as a result, other records will be sent right after the newest records are received by AVL application.
Data Link Timeout is used to set termination timeout for the link between FMB1YX and AVL application. If FMB1YX has already sent all records it waits for the new records before closing the link (except for Deep Sleep mode, for more information refer to Template:FMB Sleep modes#Deep Sleep mode). If new records are generated during the period of this timeout and the minimum count to send is reached, the records are sent to the AVL application. This option is useful when GSM

operator charges for link activation.
Server Response Timeout is used to set a period of time waiting for the response from the server-side.

Records Settings

FMB1YX device will send the newest records first when Newest is selected in *Records Settings*, which is useful in cases when the most important parameter set is the most recent one, as a result other records will be sent right after the newest records are received by AVL application.
Data Link Timeout is used to set termination timeout for link between FMB1YX and AVL application. If FMB1YX has already sent all records it waits for the new records before closing the link (except for Deep Sleep mode, for more information refer to Template:FMB Sleep modes#Deep Sleep mode). If new records are generated during the period of this timeout and the minimum count to send is reached, the records are sent to the AVL application. This option is useful when GSM operator charges for link activation.
Server Response Timeout is used to set a period of time waiting for the response from the server-side.

ACK Type determines what method the device uses to receive confirmation from the server.
AVL means that the device will expect an additional AVL message from the server, **TCP/IP** means that the confirmation will be included in the TCP/IP layer and no additional message will be needed.

Auto APN

These settings allow the device to automatically search for APN information based on inserted SIM card. This feature is explained in more detail in this page.

FOTA WEB Settings

These settings are used to configure FOTA WEB server connection parameters. *Status* enables or disables FOTA WEB functionality. The address and port number of the FOTA website are entered to *Domain* and *Port* fields. *Period* is used to set the timeout of repeat connections to the FOTA WEB server.

From 03.27.XX firmware version, FOTA WEB connection period randomizer is added. The randomizer will choose a +-2.5 period for each connection. For example, then the connection period is set to 30 minutes, device with each connection will choose a new connection (from 27.5 min to 32.5 minutes). This also applies to the "web_connect" SMS/GRRS command. This has been implemented to ensure smoother operation of FOTA WEB services by spreading out large numbers of simultaneous device connections over a longer timeframe.

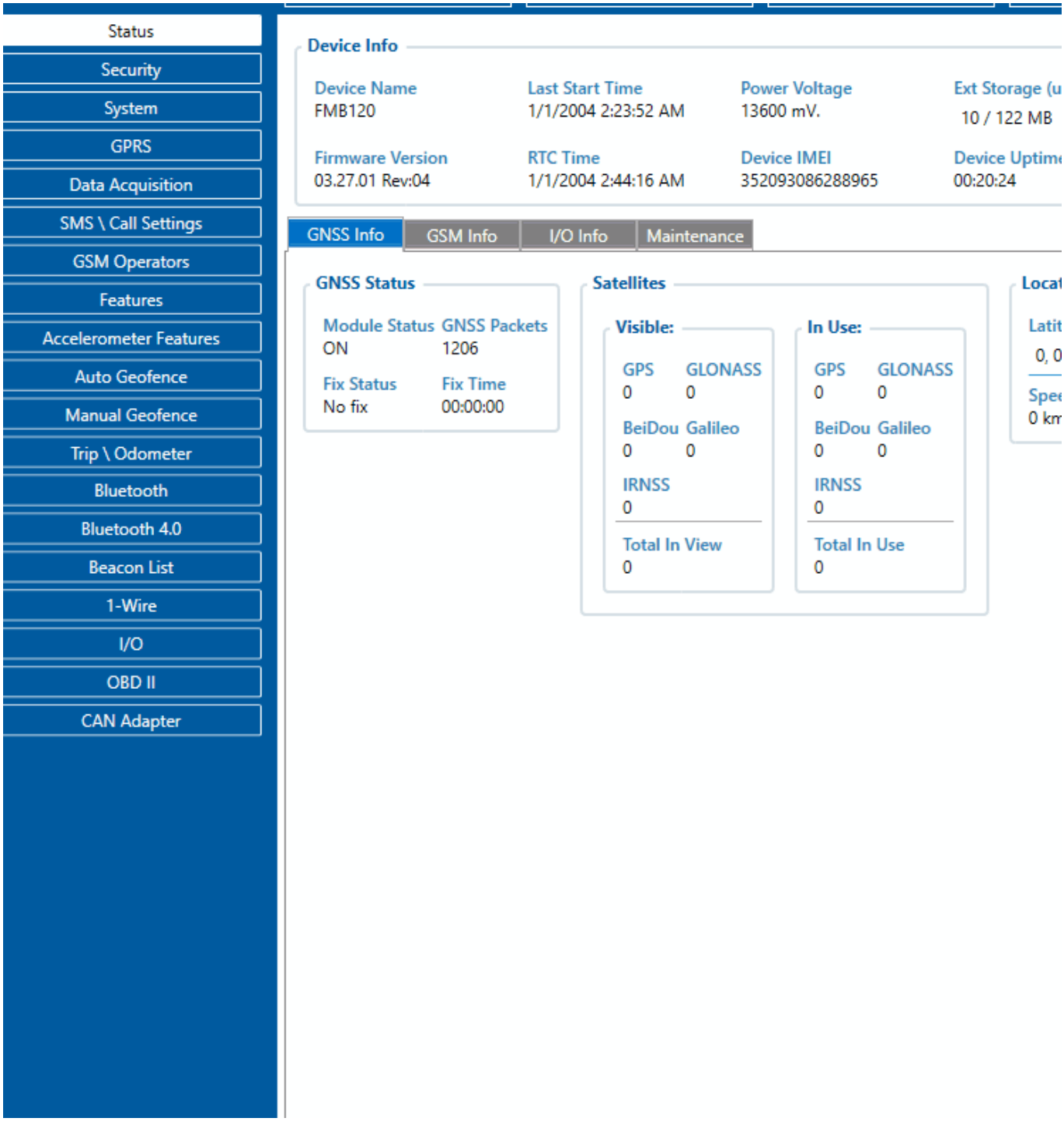
TLS/DTLS

Transport Layer Security (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.

Supported versions: **1.1/1.2**



TLS/DTLS certificate generation

Instructions cover how to generate an encryption certificate and how the device should be configured in order to send encrypted records into the client-server can be downloaded **HERE**.

Server configuration and encryption certificate implementation is mandatory from the client-server side!