Firmware V2.5 – FTP/FTPSSL push

As of this version, an LTX device can transfer data directly to servers. An explicit or “anonymous” installation of the LTX server (as a pure transport server / proxy) can be used for this purpose.

The server only serves as an “anonymous” cache (the other providers do exactly the same thing, but it is not communicated because the user does not notice the proxy and the data lands on the target system almost without delay). It is sensible to use a Use a server that is geographically accessible (e.g. on the corresponding continent). The user can enter his FTP login data directly on the logger and does not need to know anything about the server.

There are currently 2 servers set up:

```
// VPN 1 - HTTP on flexgate.org /ltx_server
{"flexgate.org","ltx_server/sw/lxu_v1.php","LX1310",80,2}

// VPN 2 - HTTPS on flexgate.org /ltx_server
{"flexgate.org","ltx_server/sw/lxu_v1.php","LX1310",443.3}

// VPN 3 - HTTP on aquatos.net /ltx
{"aquatos.net","ltx/sw/lxu_v1.php","LX1310",80,2}

// VPN 4 - HTTPS on aquatos.net /ltx
{"aquatos.net","ltx/sw/lxu_v1.php","LX1310",443.3}
```

Each server is accessible natively (VPN 1 and 3) and SSL-encrypted (VPN 2 and 4). The data can be transferred from the server to the FTP account encrypted (recommended) or unencrypted (old FTP), this is done by the server , not the modem.

Important : Until now, devices with SARA modems only supported native communication. Only devices with QUECTEL modems can transmit both natively and encrypted. The advantage of native communication: significantly faster than encrypted!

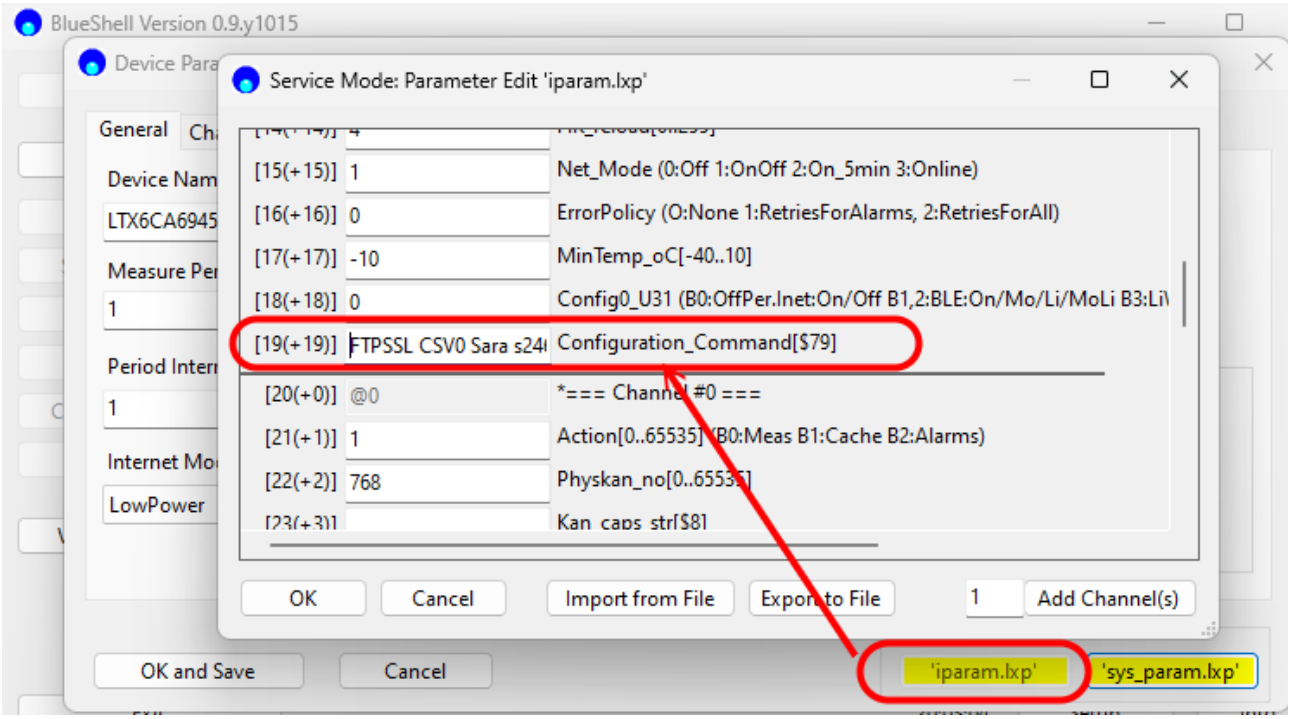
You can also enter the server data manually in the “sys_param.lxp” (the only condition: if FTP/FTPSSL is to be used, a PushPull webhook cannot be used at the same time.

Setup - 'iparam.lxp'

The FTP features are only available after upgrading to >= FW 2.5!
Download: https://joembedded.de/x3/ltx_firmware/index.php?dir=./LTX-Loggers/LTE_Logger_CPU40/Typ1200_LTX_Pegel

The memory MUST then be reformatted (with **“F2”**), then reset (**“R”**). Then reconnect and reset sensors/times/periods if necessary.

A new parameter “Configuration Command” is now available:



In this line everything essential for FTP/FTPSSL access and formats is entered.

The structure is simple:

```
ConfCmd: PROTOCOL FORMAT FILENAME URL PORT USER PW
```

Here is a simple example(1) :

```
FTPSSL CSV 0 Sara* s246.goserver.host 21 web28f3 qfile57
```

Or as a more complex example(2) (with parameters):

```
FTPSSL CSV0/ Ltx123 * s246.goserver.host 21 web28f3 qfile57
```

Or another more complex example(3) (with parameters):

```
FTPSSL CSV 1/*# *N_*T.dat s246.goserver.host 21 web28f3 qfile57
```

Parameters of the “Configuration Command” (separator is a space)

PROTOCOL (capital letters) :

FTP	Anonymous server ↔ FTP server communicate unencrypted This is the "classic" FTP in its simplest form. Usually runs on port 21
FTPSSL	Anonymous server ↔ FTP server communicate encrypted , recommended operating mode ! Usually called "FTP with explicit encryption" and usually runs on port 21.

Note : The colloquial names for the many FTP variants are often somewhat misleading. SFTP (usually via port 22) is yet another protocol, and so is FTPS (usually port 990 and often referred to

as 'FTP with implicit encryption').

FORMAT: (capital letters):

Almost any number of formats are possible. Currently implemented are:

CSV0	CSV with additional data (lines in '<' - '>', e.g. for error information, ...)
CSV1	CSV without additional data

Without any further additions, the data is written to the FTP main directory.
Optionally, a parameter can be added to the format to
write data to a directory on the FTP server, by appending "/" and the directory name
(as in example (2): "/Ltx" or example (3): "/*#").
Explanation of the parameters in the next section.

Important : Other formats (MIS, ZXP, TXT, ...) do not require new firmware on the device because the server generates the formats.

FILENAME: The device can be given a short name to identify the data. At least 1 character, max. 8-10. The time is appended to this name during transmission and (if not already included with an extension, as in example (3)) ".csv". Example: here a file name "Sara20231510185033.csv " would be conceivable.
The "*" at the end is important because that is the parameter for the time. Otherwise all file names would always be the same. Explanation of the format in the next section

URL: Url of the FTP server, here: "s246.goserver.host"

PORT: This is usually port 21 (for other ports see above).

USER and PW: Login data.

Wildcards "*" in the parameters

To assign a separate file name or directory to each transfer on the FTP server, the directory names and file names can be generated dynamically with "*". For example, to write all transfers per month into a separate directory. The asterisk "*" plus an optional additional character are used for formatting:

"*" plus the (optional) following character is replaced as follows:

T or " (nothing)	UTC time in seconds, reverse. Example: "*" or "*T" becomes "20231017165922"
H	UTC time in hours, reverse. Example: "*H" becomes "2023101716"
D	UTC time in days, reverse. Example: "*D" becomes "20231017"
M	UTC time in months, reverse. Example: "*M" becomes "202310"
Y	UTC time in years, reverse example: "*Y" becomes "2023"
N	The device name (as in the device parameters). Example: "Logger_*N" becomes "Logger_LTX9ABCDEF"

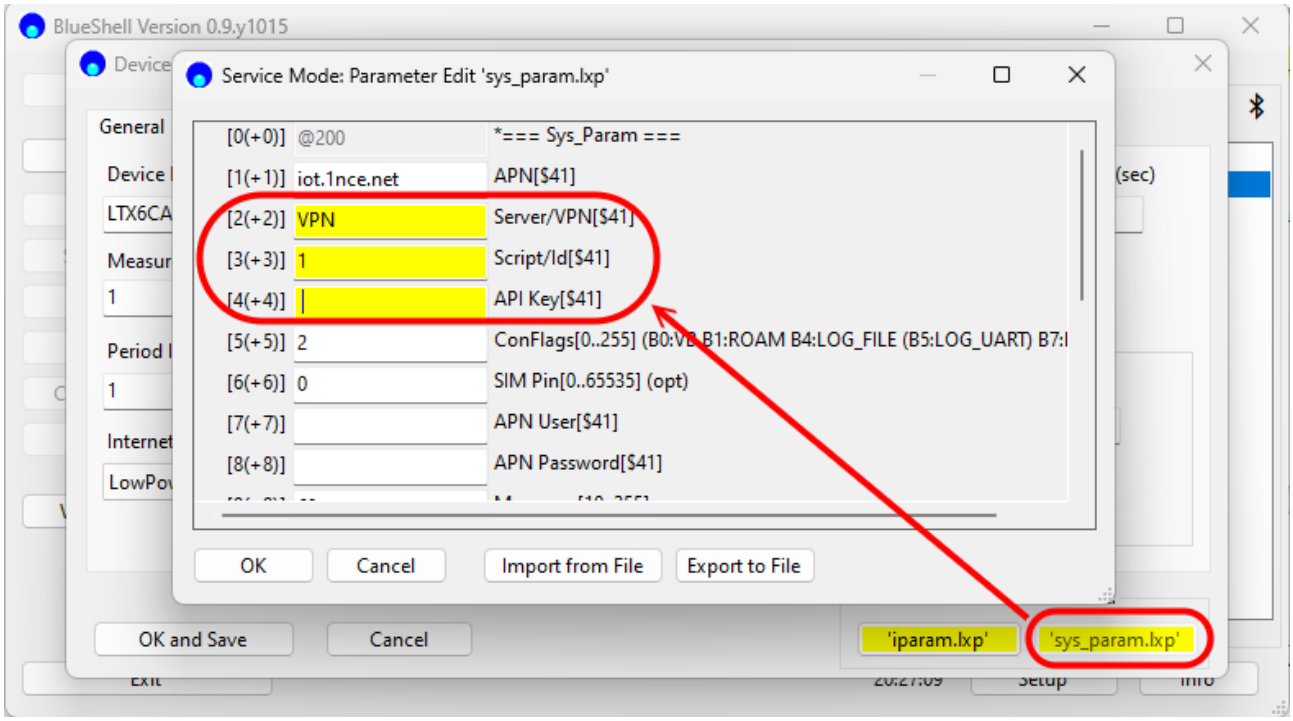
#	16-digit MAC of the device. Example: “STS_*#” becomes “STS_0123456789ABCDEF”

Other characters are ignored. Example: “*k” becomes “k”. Multiple replacements are also possible, e.g. “Dev_*N_*” becomes “Dev_Pegel33_20231017165922”.

Setup – VPN

Easy Way, 1st option

Normally the “Configuration Command” parameter is ignored by the device. To activate it, the “VPN” feature must be activated:



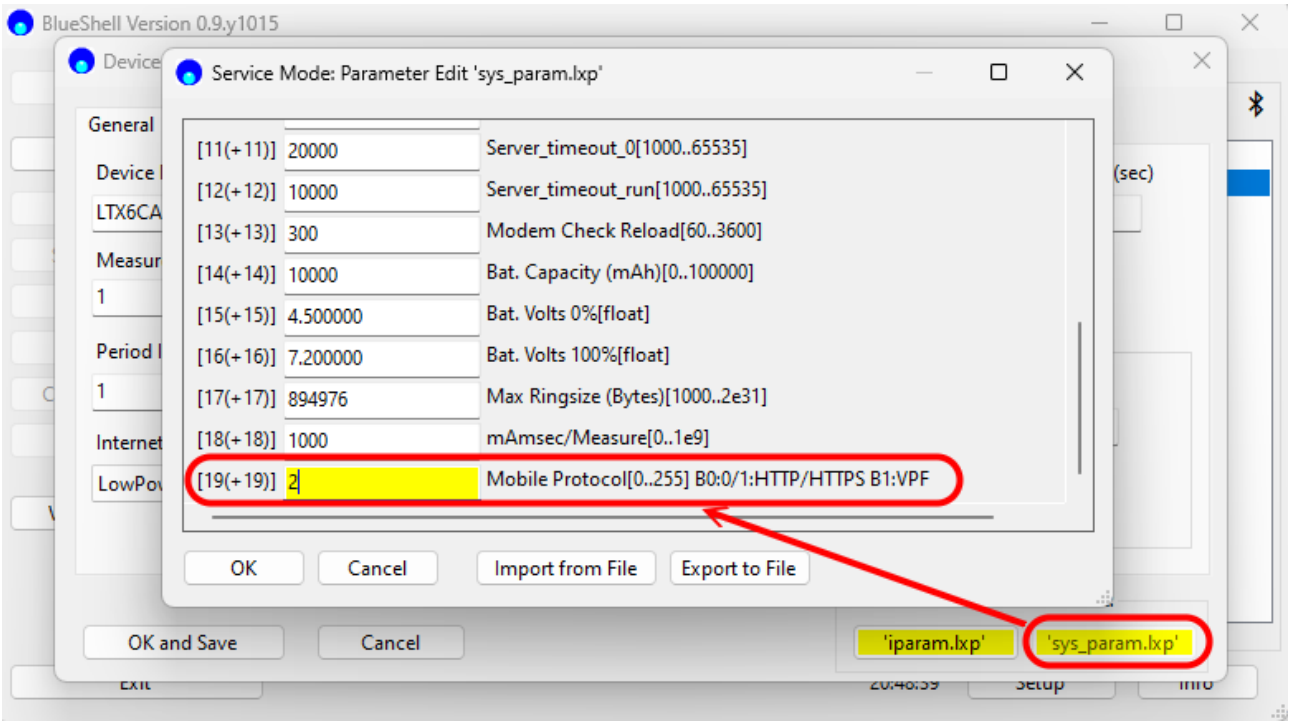
"VPN" is entered as the server (capital letters) and one of the servers to be used as the ID. The API key can be left empty. In this case, the data is transferred via "flexgate.org", but the user is not aware of this.

Important : The SARA modem can only communicate via HTTP (but not via HTTPS), so only 1 or 3 is possible here (see list at the beginning).

Existing LTX server, 2nd option

As a second option , any existing installation of the LTX microcloud (100% open source and free to use: https://github.com/joembedded/LTX_server)

All you have to do is set the “VPF” flag (the last value in the list above, 2 or 3):



The user must then enter the server/script/API key themselves.

In both cases, the data is now transferred directly to the FTP server. The name or address of the server is not displayed to the user during the transfer. If errors occur, the attempt is made until the buffer is full (“quota”):

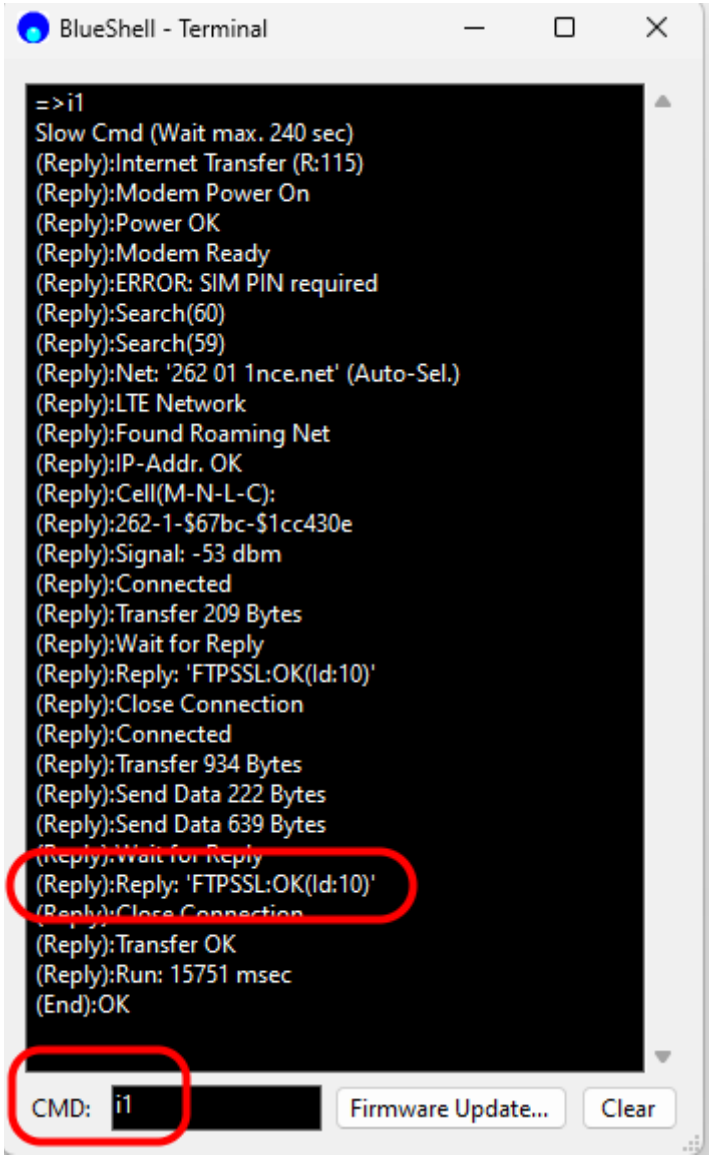
Quota-Info

The anonymous server provides each device with a small buffer. If the buffer overflows, the oldest data is deleted. By default, the memory is limited to 90 days and 1000 measurements (i.e. a maximum of 100kB per device).

The value can be set manually for each device or in the server file “sw/conf/api_key.inc.php”. However, for high performance it should not be too high. With the above settings, each of the servers should be able to serve several thousand devices without any problem!

Manual transfer

During manual transfer, the result of the last transfer is displayed in the terminal:



A transfer can be started manually with 'i' (default), 'i1' (more text) or 'i3' (more text and extra long network search, for tests). The text "FTPSSL:OK" shows that the connection to the FTP server was successful.

(Note: The one-time message “SIM PIN required” means nothing)

The data is then immediately available on the FTP server:

***