



Application Note

Firmware Release Note



Table of contents

1	Firmware Release Note v4.02	3
1.1	Scope	3
1.2	V4.02 Changes	3
1.2.1	Cyber security	3
1.2.2	Firmware update	3
1.2.3	Configurations	4
1.2.4	Miscellaneous	4
1.3	Historical Changelog	4
1.3.1	V04.02	4
1.3.2	V04.00	4
1.3.3	V03.04	5
1.3.4	V03.03	5
1.3.5	V03.02	5
1.3.6	V03.01	5
1.3.7	V03.00	5
1.3.8	V02.07	5
1.3.9	V02.06	5
1.3.10	V02.05	5
1.3.11	V02.04	6
1.3.12	V02.03	6
1.3.13	V02.02	6
1.3.14	V02.01	6
1.3.15	V0200	6
1.3.16	V01.09	6
1.3.17	V01.08	6
1.3.18	V01.07	6
1.3.19	V01.06	7
1.3.20	V01.05	7
1.3.21	V01.04	7
1.3.22	V01.02	7
1.3.23	V01.01	7
1.3.24	V01.00	7



1 Firmware Release Note v4.02

1.1 Scope

Many of the new changes in this firmware version are related to compatibility with the EN18031-1 standard (RED CYBER). This European standard aims to improve the cybersecurity of IoT products.

1.2 V4.02 Changes

1.2.1 Cyber security

- The SSL/TLS encryption version is now TLS V1.2 only.
- The default cypher suit for the TLS are:
 - 0XC02B : TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
 - 0XC02F : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- Cypher suite can be changed in the parameter: `config.remote.ftp.cipherSuite`
- 0xFFFF will enable all cipher suites supported by the modem.
- If otherwise, not explicitly, FTPS is the default protocol.



Tip

Refer to the user manual for the list of suites



Note

Products leaving the factory have file encryption enabled by default. A file containing the AES keys corresponding to each product will be provided.



Warning

AES file encryption has changed; the CBC algorithm IV is now variable and must be located at the end of the AES file.



Warning

These configurations are required to meet the EN 18031 standard. Should you choose to bypass these security measures, use weak/shared passwords, or enable insecure protocols, you assume full responsibility for any resulting non-compliance. Webdyn disclaims all liability for regulatory penalties or security breaches resulting from a deviation from these mandatory standards.

1.2.2 Firmware update

- Add asymmetric signature for the firmware file.



Warning



Starting with this version, it is no longer possible to update the firmware to a version lower than the current one.

1.2.3 Configurations

- Add an option in the configuration allowing switching to "Storage" mode via FTP. This new parameter is:
 - `config.remote.ftp.modeConfiguration` (Boolean).
- Add an option in the configuration for enabling the SNI extension for TLS communications. The new parameters are:
 - `config.remote.ftp.sni`
 - `config.remote.server2.sni`
 - `config.remote.mqtt.sni` (Boolean).
 - `config.remote.mqtt.tls.sni`.

1.2.4 Miscellaneous

- Add a conditional CRON based on the state of the external power supply
 - If the CRON line begins with the character `b`, then this CRON job is active when the gateway is powered solely by the battery.
 - If the CRON line begins with the character `e`, then this CRON job is active when the gateway is powered solely by the external input.
- Add the `dataGet` command: copy the frames in memory to USB partition.
- The `CID` field was missing in the ACK file created by the gateway after a software update.
- Fix firmware update issue during live diagnostic action
- The default TCP port for the HTTP server is 80 and 443 for HTTPS.
- Add a dual TLS context for dual server configuration. With a dual server configuration, there was a connection error on the second server if the level of TLS security was different. For example, if you have a HTTPS using certificate on server 1 and a FTPS with a simple TSL connection, then the connection on the second server would fail.

1.3 Historical Changelog

1.3.1 V04.02

- add `remote.ftp.httpDelay` and `remote.server2.httpDelay`
- add `remote.mqtt.oneFramePerPost`

1.3.2 V04.00

- Compliance with EN 18031-1
- Adding asymmetric signatures for firmware files
- TLS V1.2 is now mandatory
- Deny firmware downgrade
- New AES file format
- Default cipher suite for TLS
- Adding missing CID in ack after firmware update
- Adding an option in the configuration allowing switching to `Storage` mode via FTP
- Adding a conditional CRON based on the state of the external power supply
- Adding SNI TLS extension parameter
- Fix firmware update issue during live diagnostic action
- Fix default TCP port for HTTP parameters (80/443)
- Fix dual server issue connection when 2 different level of TLS are used



1.3.3 V03.04

- Fix PIN commands issue with some providers
- Fix production command issue

1.3.4 V03.03

- Add Second remote server configuration
- Add `live diagnostic` local action (FTP + MQTT)
- Add new whitelist commands (`whiteListCount` and `whiteListGet`)
- Add network connection status for supervision file in USB mode
- Add HTTP mode for remote connection
- Add last day of the month in CRON entries (`L`)
- Fix USB files date issue
- Fix User/Password in APN configuration
- Fix battery capacity in supervision file with external power
- Fix factory reset issue with listening window data
- Improve the FTP file handling.

1.3.5 V03.02

- Fix regression: FTP issue

1.3.6 V03.01

- Fix regression: no more data loss in case of error in FTP upload data
- Fix regression: unwanted connection at midnight

1.3.7 V03.00

- support for 434Mhz radio hardware (mode T+C and S)
- add vehicle mode
- add FTP INBOX Broadcast directory support
- add SIM PIN management commands
- add manufacturer, medium and CI blacklist
- add CI filter
- add operator selection
- set maximum window duration to 6h
- USB disk speed improvement
- Fix compatibility issue with WM Bus `soft address`

1.3.8 V02.07

- Fix File upload regression for local upload
- Fix FTP path remote update regression

1.3.9 V02.06

- Fix Cron table issue with comma syntax

1.3.10 V02.05

- new parameter: "config.radio.oneFramePerMeter"
- new parameter: "config.remote.ftp.checkFtpDir"
- new command: "dataClean"
- Add USB automation (info.bson and reset)
- Improved near-field reception
- Taking into account the duration of the listening window in the random delay.



- The default local action is request for product without BLE option.
- Fix frame timestamp issue in data file
- Fix compatibility issue with pureFTPD server
- Fix software update issue with large RTC drift
- Fix data upload issue with a full data partition
- Fix FTP issue with more than 1 directory level
- Fix low battery alarm not working

1.3.11 V02.04

- Fix frame error for Frame B with a length greater than 127 bytes

1.3.12 V02.03

- Fix modem issue during production test

1.3.13 V02.02

- Fix regression with SIM PIN management

1.3.14 V02.01

- adaptation for circuit board without BLE module

1.3.15 V0200

- Improvement of the 1 first LTEM connection
- The delay before the 2nd network connection attempt is reduced
- If the network mode is set to AUTO the 2nd network connection attempt is done in 2G mode
- Add new network quality indicator and information in the supervision file
- Add the ICCID in the supervision file
- Add NB-IoT connectivity
- Medium and generation fields optionally ignored in the white list
- Possibility of deregistering from the network each time the magnet is used
- Inbox parsing improved
- Timeout for the local action
- Support for the SIM Busy error on modem startup
- Fix the problem of decoding long frames in B format
- Fix the Diag command issue in FTP
- Fix issue when `local.testCount` > 10
- if `local.testCount` > 1 a network error doesn't interrupt the installation mode
- if `local.testCount` > 1 a firmware update doesn't interrupt the installation mode

1.3.16 V01.09

- Fix compatibility issue with BG95M3 firmware revision 01.009
- Fix `diag` command issue when used in FTP

1.3.17 V01.08

- Add multi radio mode: S+T

1.3.18 V01.07

- Fix read only configuration parameters regression



1.3.19 V01.06

- Add the `BformatLFieldAdaptation` parameter
- Fix the double AES encryption for the ACK files after ftp software update
- Fix the CRC issue for short format B frames
- Force a software reset after BLE configuration update
- Read WM Bus mode from configuration in radio BLE test

1.3.20 V01.05

- Correction of the CRC calculation bug for mode C frames in B format having a length of more than 128 bytes
- Add missing `framecount` information in data files

1.3.21 V01.04

- USB partition formatting after firmware update
- Fix alarm file encryption
- Add FTPS support
- Fix mode C frame with format B length issue
- Stop the radio listening window if all meters of the white list are received
- Do not enable AES security if the AES key is not valid
- Read `cfg` and `cmd` file in the INBOX directory in one connection
- Minimum listening window duration set to 30s
- Fix `operatorInit` command issue
- Add `CptRecFrames` in supervision

1.3.22 V01.02

- Long header frame issue fix
- Add radio statistics in supervision file

1.3.23 V01.01

- Add NTP time validity check
- Fix `logGet` command on USB is AES is enabled
- Fix AES encryption issue for large files (size > 100ko)
- Force FTP file type to binary

1.3.24 V01.00

- first release