



WebdynEasy Wireless M-bus
Application Note

Migration Note - FW 3.04



Table of contents

1	Migration Note - FW 3.04	3
---	--------------------------	---



1 Migration Note - FW 3.04

Note

The main improvement in Webdyn Easy MBus V4.0 firmware is its compliance with the EN18031-1 (RED Cyber) standard. Products equipped with this version from the factory will each have a unique AES encryption key, and file encryption will be enabled.

Here are the important points regarding the migration to this version:

- To follow cryptographic best practices, the AES file format has been modified in this version. The Initialization Vector (IV) used by **AES CBC** is stored at the end of the encrypted file. When a file is created, a random IV is generated, then the file is encrypted with AES CBC, and finally, the IV is concatenated.
- Once file encryption is enabled, all files created by the gateway will be encrypted. Only encrypted configuration and command files will be processed by the gateway.
- By default, only cryptographic suites are offered by the modem:
 - **0xC02B**: TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
 - **0xC02F**: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - To allow all available suites supported by the modem use: 0xFFFF

Info

The gateway only uses version V1.2 of the TLS protocol; earlier versions are no longer compatible.

Warning

Once the firmware has been flashed, it will no longer be possible to downgrade the firmware; only higher versions will be possible.