



WebdynEasy Wireless M-bus
Application Note

Migration Note - FW 3.04



Table of contents

1	Note de migration - FW 3.04	3
---	-----------------------------	---



1 Note de migration - FW 3.04

Note

La principale amélioration apportée au micrologiciel Webdyn Easy MBus V4.0 réside dans sa conformité à la norme EN 18031-1 (RED Cyber). Les produits équipés d'origine de cette version disposeront chacun d'une clé de chiffrement AES unique, et le chiffrement des fichiers sera activé.

Voici les points importants à retenir concernant la migration vers cette version :

- Afin de respecter les meilleures pratiques en matière de cryptographie, le format de fichier AES a été modifié dans cette version. Le vecteur d'initialisation (IV) utilisé par **AES CBC** est stocké à la fin du fichier chiffré. Lors de la création d'un fichier, un IV aléatoire est généré, puis le fichier est chiffré avec AES CBC, et enfin, l'IV est concaténé.
- Une fois le chiffrement des fichiers activé, tous les fichiers créés par la passerelle seront chiffrés. Seuls les fichiers de configuration et de commande chiffrés seront traités par la passerelle.
- Par défaut, le modem ne propose que des suites cryptographiques :
 - **0xC02B**: TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
 - **0xC02F**: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - Pour activer toutes les suites disponibles prises en charge par le modem, utilisez : 0xFFFF

Info

La passerelle utilise uniquement la version V1.2 du protocole TLS ; les versions antérieures ne sont plus compatibles.

Warning

Une fois le micrologiciel mis à jour, il ne sera plus possible de revenir à une version antérieure ; seules les versions supérieures seront disponibles.