



WebdynEasy W M-Bus 868MHz / 434MHz

Manuel d'utilisation

Index

Glossaire.....	5
Remarques concernant ce manuel	8
1 Présentation	11
1.1 Description générale.....	11
1.2 Principe de fonctionnement	11
1.3 Les interfaces	12
1.4 Équipements supportés.....	15
1.5 Références des produits et accessoires.....	16
1.6 Spécifications techniques.....	16
1.6.1 Caractéristiques générales.....	16
1.6.2 Caractéristiques techniques	18
1.6.3 Caractéristiques logicielles.....	20
1.6.4 Autonomie.....	21
1.7 Consignes de sécurité.....	23
1.8 Réglementation	24
1.9 Cybersécurité	25
2 Installation	26
2.1 Prérequis.....	26
2.2 Déballage.....	26
2.2.1 Contenu	26
2.2.2 Identification.....	26
2.3 Montage	28
2.3.1 Ouverture/Fermeture du boîtier.....	28
2.3.2 Fixation murale.....	28
2.4 Description des interfaces.....	29
2.4.1 Alimentation du produit.....	29
2.4.1.1 Alimentation externe.....	29
2.4.1.2 Pack piles	30
2.4.2 Radio.....	31
2.4.2.1 Antenne	32
2.4.3 Réseau cellulaire.....	32
2.4.3.1 Antenne	33
2.4.3.2 Carte SIM.....	33
2.4.4 Les voyants & boutons	35
2.4.4.1 Capteur Effet Hall.....	35
2.4.4.2 Bouton RESET	36
2.4.4.3 LED Modem.....	36
2.4.5 Interface USB	37
3 Fonctionnement du produit.....	39
3.1 Démarrage du produit.....	39
3.1.1 Modes de fonctionnement	39
3.1.1.1 Mode FACTORY SETTINGS.....	41
3.1.1.2 Mode STOCKAGE	41
3.1.1.3 Mode RUN	42
3.1.1.4 RESET	43
3.1.2 Fonctionnement applicatif.....	43
3.1.2.1 Tâche WM-BUS.....	43
3.1.2.2 Tâche Modem (connexion SI).....	43
3.1.2.3 Tâche de Surveillance (Monitoring).....	44
4 Configuration	45
4.1 Configuration locale par USB.....	45
4.2 Fichier de configuration	45

4.2.1	Système	46
4.2.1.1	Locale	47
4.2.1.2	Sécurité.....	48
4.2.2	Radio WM-Bus.....	50
4.2.2.1	Liste blanche « whiteList »	53
4.2.2.2	Champ L pour les trames format B	54
4.2.3	Connectivité du concentrateur.....	54
4.2.3.1	Modem.....	55
4.2.3.2	Serveurs (FTP/FTPS/HTTP/HTTPS)	57
4.2.3.3	NTP.....	59
4.2.4	Alarmes.....	60
4.2.5	Schedule (planification) et Monitoring	61
4.2.5.1	Schedules.....	61
4.2.5.1.1	Schedule Radio.....	63
4.2.5.1.2	Schedule serveur (FTP(S), HTTP(S))	64
4.2.5.2	Monitoring (surveillance du produit)	65
5	Exploitation	67
5.1	Le serveur distant.....	67
5.1.1	Le serveur FTP(S)	67
5.1.1.1	Paramétrage.....	67
5.1.1.2	Arborescence du serveur.....	68
5.1.1.3	Fonctionnement.....	69
5.1.1.4	FTP(S) Broadcast	69
5.1.1.4.1	Fonctionnement	70
5.1.1.5	Format des fichiers	70
5.2	La configuration.....	71
5.3	Les données.....	72
5.4	Les alarmes	74
5.5	Les acquittements ACK.....	75
5.6	Les commandes	77
5.6.1	Commande « request ».....	79
5.6.2	Commande « factory ».....	80
5.6.3	Commande « firmware ».....	80
5.6.4	Commande « diag »	80
5.6.5	Commande « configGet »	80
5.6.6	Commande « whiteListErase ».....	81
5.6.7	Commande « whiteListCount »	81
5.6.8	Commande « whiteListGet ».....	81
5.6.9	Commande « operatorInit ».....	82
5.6.10	Commande « logGet ».....	82
5.6.11	Commande « logClean ».....	83
5.6.12	Commande « dataGet »	83
5.6.13	Commande « supervisionClean ».....	83
5.6.14	Commande « supervisionGet »	84
5.6.15	Commande « modemClean »	84
5.6.16	Commande « certificate ».....	84
5.6.17	Commande « certClean »	85
5.6.18	Commande « dataClean »	85
5.6.19	Commande « simStatus ».....	86
5.6.20	Commande « simPin »	87
5.6.21	Commande « simNewPin ».....	88
5.6.22	Commande « simPuk ».....	90
5.7	La supervision.....	91
5.8	Le Log.....	97
6	Mise à jour	100
6.1	Locale.....	100

6.2	Distante.....	101
7	Outils & diagnostics	102
8	FAQ	103
9	Support	104
10	ANNEXES.....	105
10.1	Annexe A : « Configuration – Liste des variables »	105
10.2	Annexe B : « Log – Liste des évènements »	115
10.3	Annexe C : Liste des suites de chiffrement utilisables	115
11	Bureaux et support.....	116

Glossaire

NOM	DESCRIPTION
AES	Advanced Encryption Standard Algorithme de chiffrement symétrique.
APN	Access Point Name Nom du point d'accès permettant à la passerelle de se connecter au réseau Internet par liaison mobile.
Base64	Codage des données en utilisant un alphabet de 64 caractères.
BLE	Bluetooth Low Energy Technique de transmission sans fil sous la forme d'un standard ouvert basé sur le Bluetooth, et ayant pour caractéristique une consommation beaucoup plus faible
BSON	Binary JSON Version binaire de JSON : encodage permettant de diminuer la taille des données transmises afin d'économiser la pile des systèmes autonomes.
FTP	File Transfer Protocol Protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP.
FTPS	File Transfer Protocol Secure Protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP, variante du FTP, sécurisé avec les protocoles SSL ou TLS. Il permet au visiteur de vérifier l'identité du serveur auquel il accède grâce à un certificat d'authentification. Il permet également de chiffrer la communication.
2G	Second Generation Standard numérique de seconde génération (2G) pour la téléphonie mobile comprenant le GSM, GPRS et EDGE.
HTTP	HyperText Transfer Protocol Protocole de communication client-serveur développé pour le Web.

IP	Internet Protocol Protocole de messages responsable de l'adressage et de la transmission de paquets TCP sur le réseau.
JSON	JavaScript Object Notation JSON est un format d'échange de données aisément interprétable.
LTE-M/CAT-M1	Long Term Evolution - Machine Réseau mobile 4G dédié aux objets connectés, c'est-à-dire basse consommation et longue portée.
MQTT	Message Queuing Telemetry Transport Protocole de messagerie publish-subscribe basé sur le protocole TCP/IP.
NB-IoT	NarrowBand-Internet of Things Réseau mobile 4G dédié aux objets connectés, c'est-à-dire basse consommation et longue portée.
NTP	Network Time Protocol Un serveur NTP permet la synchronisation horaire des équipements.
SI	Système d'Information Serveur avec lequel le concentrateur échange (configuration, données, alarmes, ...)
TCP	Transmission Control Protocol Protocole orienté connexion sur Internet qui offre les services de segmentation des données en paquets que le protocole IP transmet sur le réseau. Ce protocole fournit un service fiable de transfert de données. Voir aussi IP.
TCP/IP	Transmission Control Protocol/Internet Protocol Ensemble de protocoles réseau qui fournissent des services d'interconnexion entre des ordinateurs d'architectures matérielles et de systèmes d'exploitation différents. TCP/IP inclut des normes de communication entre ordinateurs et des conventions pour l'interconnexion des réseaux et le routage.
WM-BUS	Wireless M-Bus

Évolution de la norme européenne Mbus, dans une adaptation radiofréquence. Cette connectivité est dédiée aux applications de comptage comme : les compteurs d'eau, de gaz, d'électricité.

Remarques concernant ce manuel

Ce guide décrit l'ensemble des caractéristiques du produit WebdynEasy.

Il a pour but d'aider l'opérateur à installer et configurer sa WebdynEasy et de permettre aux exploitants d'intégrer les données collectées à leur SI.

Ce manuel comporte dix sections distinctes :

- Section 1 : Présentation générale
- Section 2 : Installation
- Section 3 : Fonctionnement du produit
- Section 4 : Configuration
- Section 5 : Exploitation
- Section 6 : Mise à jour
- Section 7 : Outils & diagnostics
- Section 8 : Support
- Section 9 : FAQ
- Section 10 : Annexes

Champ d'application

La présente description technique est valable pour les concentrateurs WebdynEasy à partir de la version de matériel V1 et de la version logicielle V2.0.

Groupe cible

Ce guide s'adresse aux installateurs sur site qui câbleront et configureront les installations, aux personnes chargées de la maintenance locale ou à distance des installations, ainsi qu'aux développeurs de portails permettant l'exploitation des données transmises.

Historique du document

Version du document	Contenu
V1.0	Création
V1.1	Modification sur le fonctionnement du produit avec l'aimant et du nombre de Bips. Ajout d'un schéma explicatif sur la gestion des fichiers.

V1.2	Ajout et Modification sur la partie supervision. Ajout de l'autonomie.
V1.3	Ajouts dans le glossaire, modification du fichier de commande
V1.4	Ajouts du Champ L pour les trames format B
V1.5	Précisions sur le paramètre F de la data et sur le mode diagnostic, Ajustement de la plage /scheduleRadio/data
V1.6	Ajout du multi mode d'écoute. Modification exemple de « wlFilter ». Modification exemple commande « diag ». Ajout du « cid » dans toutes les commandes. Ajout de la commande « supervisionGet ». Changement de la commande « update » par « firmware ». Modification de la commande « configGet ».
V2.0	Ajout du NB-IoT. Ajout de variables de supervision. Ajout et présentation du nouveau boîtier. Ajout du désenregistrement du réseau par aimant. Ajout des commandes de gestion des certificats. Ajout de configuration radio (longHeader, skipVersionField et skipMediumField). Ajout de la référence commerciale sans BLE. Ajout de précisions sur l'utilisation de la whiteList.
V2.1	Nouveaux paramètres « oneFramePerMeter », « checkFtpDir », « skipVersionField » et « skipMediumField ». Firmware présent systématiquement sur le disque USB (à partir de la V2.05). Redémarrage automatique par un simple fichier « reboot » sur le disque USB (à partir de la V2.05). Ajout de la version 434MHz (à partir de la V2.06 disponible le 15/11/2022).
V3.1	Nouveaux paramètres « ciFilter », « isManufAllowList », « isMediumAllowList », « isCiAllowList », « operator », « checkBcast ». Fonctionnalité « broadcast » pour le FTP. Commandes de gestion de la carte SIM. Interdiction du downgrade firmware.
V3.2	Précision sur le fonctionnement du Schedule FTP
V3.2.1	Suppression du fonctionnement du BLE
V3.3	Ajout d'un 2 ^{ème} serveur Ajout d'une action locale « live diagnostic »

	Ajout de nouvelles commandes pour la liste blanche «WhiteList » Ajout de l'état de la connexion réseau pour le fichier de supervision en mode USB Ajout de la gestion de serveur HTTP Ajout d'un nouveau paramètre pour le CRON
V3.4	Synchronisation du numéro de version avec le firmware
V4.0	cybersécurité : • Valeurs par défaut conformes aux bonnes pratiques en manière de cybersécurité. • TLS V1.2 uniquement, les versions inférieures sont interdites • Choix des cipher suite pour le TLS • Chiffrement des fichiers activé par défaut • Interdiction du downgrade lors des mises à jour firmware Ajout des Schedule conditionnels suivant la source d'alimentation. Nouveau paragraphe sur les précautions de manipulation pour éviter les risques ESD

1 Présentation

1.1 Description générale

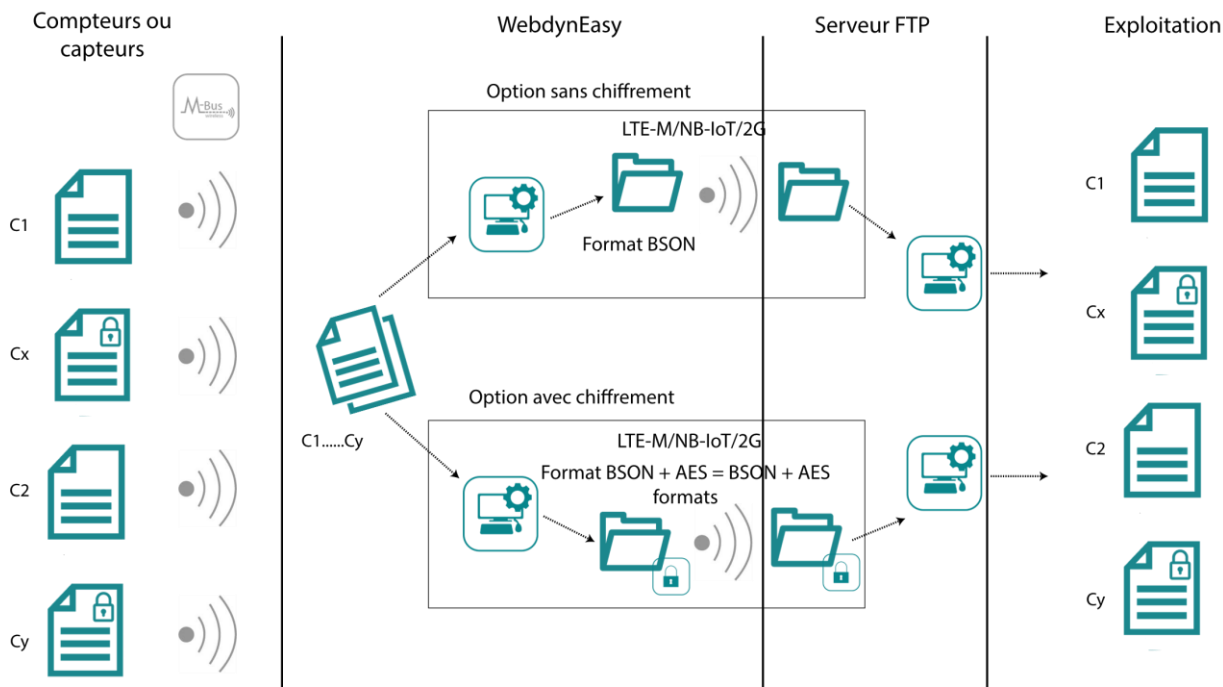
Le concentrateur WebdynEasy a pour objectif de collecter les informations émises par des capteurs Wireless M-Bus comme des compteurs (eau, gaz et électricité) et des capteurs (température, humidité, etc...). Cette technologie est peu énergivore, les durées de vies de la pile du concentrateur peuvent dépasser 10 ans.

La collecte de données se fait par radio sur la fréquence 868MHz ou 434MHz. Cette fréquence est libre de droits et son utilisation est harmonisée à de nombreux pays de l'Union européenne.

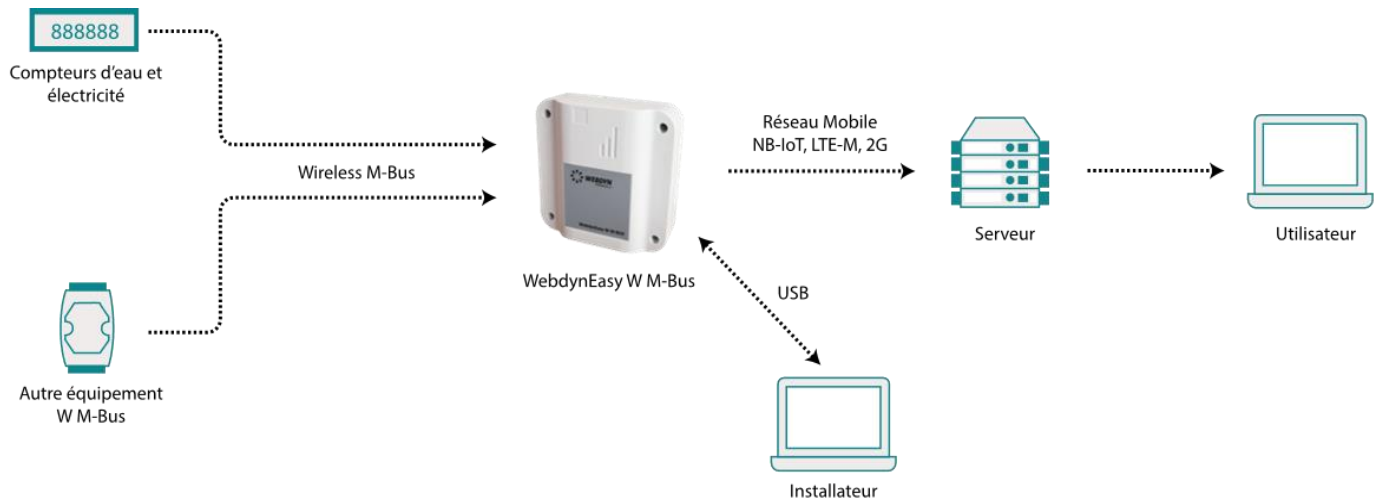
Les informations collectées (données, paramètres, alarmes, ...) sont mises en forme au format BSON avant d'être envoyées par modem vers un système d'information (SI).

1.2 Principe de fonctionnement

La WebdynEasy vous permet de bâtir votre réseau privé et fait partie d'un ensemble. La communication WM-Bus se fait point à point de manière non opérée. Les compteurs ou capteurs envoient périodiquement des trames de données, ces dernières sont réceptionnées et les données brutes (chiffrée ou en claire) contenues dans ces trames sont stockées par le concentrateur WM-Bus. Périodiquement, la WebdynEasy déposera un fichier au format BSON contenant l'ensemble des données brutes des différents capteurs sur un serveur (FTP, MQTT, HTTP) en utilisant son modem en LTE-M/NB-IoT/2G. Il est possible de sécuriser les fichiers échangés entre la WebdynEasy et le serveur FTP(S) en activant le chiffrement en AES (Voir chapitre 4.2.1.2 : « Sécurité »).

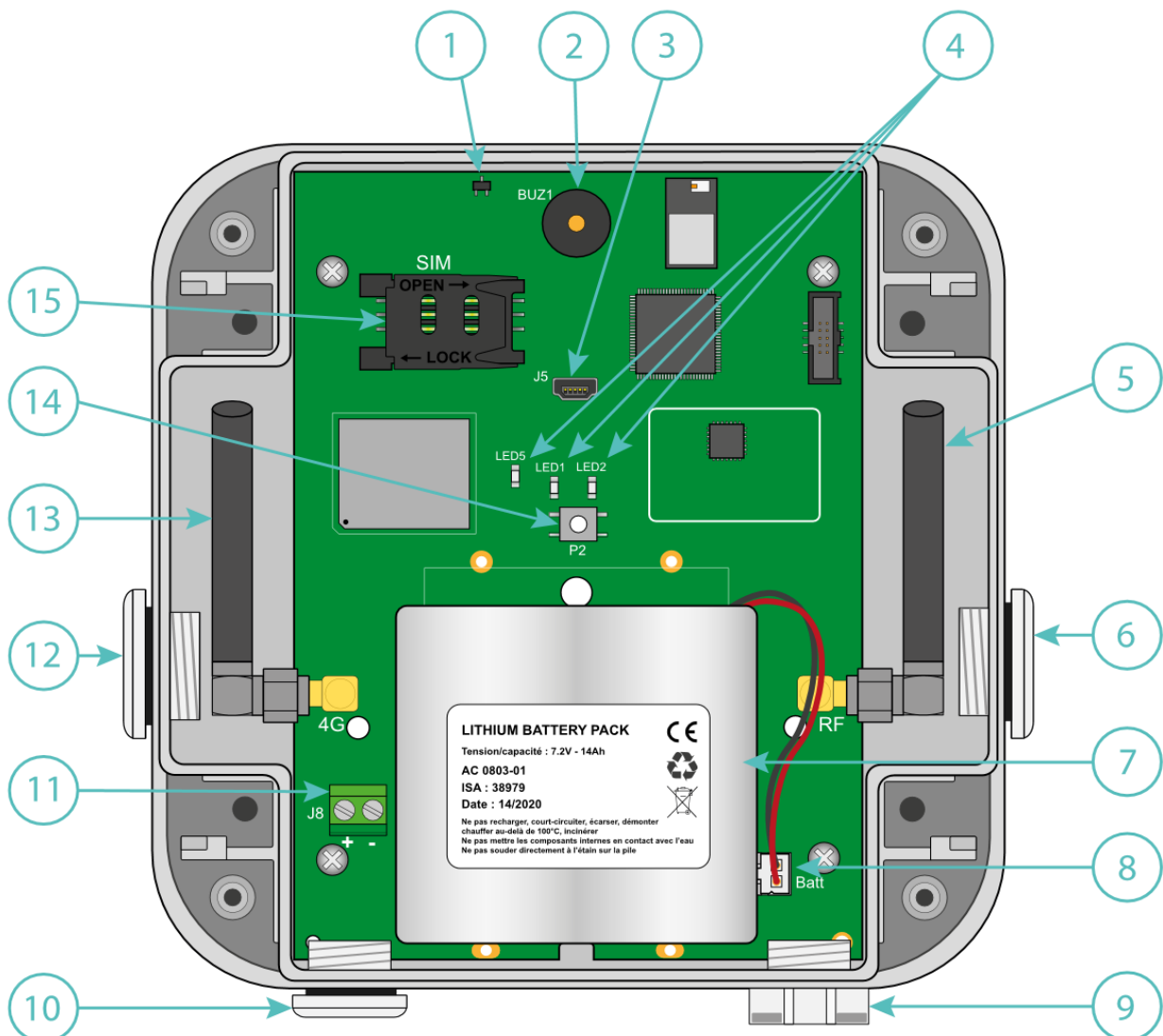


Il est possible de configurer la WebdynEasy en la connectant par USB à un ordinateur.



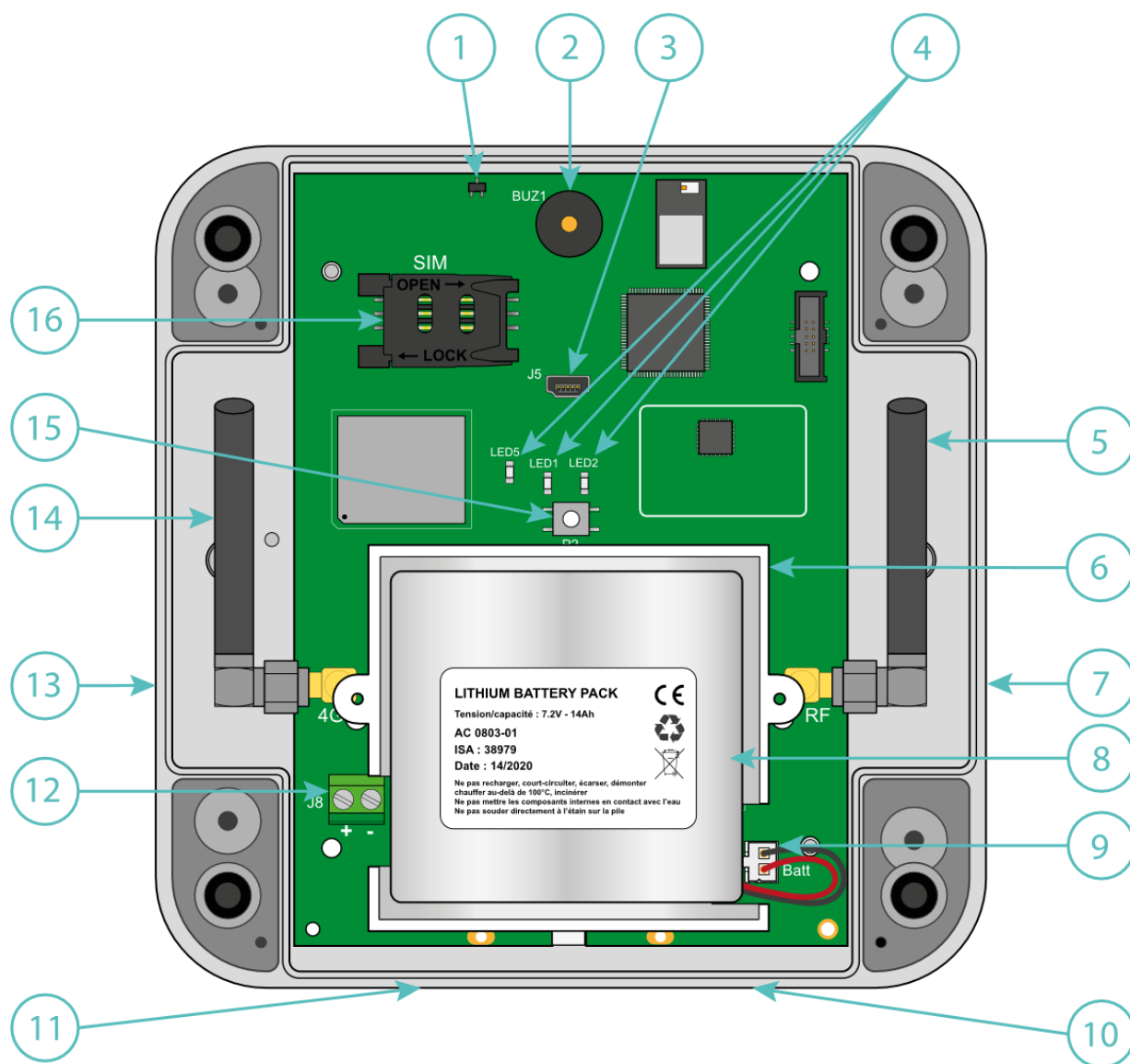
1.3 Les interfaces

Ancien boîtier :



Numéro	Description
1	Capteur à effet HALL
2	Buzzer
3	Connecteur mini-USB
4	Voyants : • LED 1 : réservé • LED 2 : réservé • LED 5 : Statut du modem
5	Antenne SMA de la radio 868MHz ou 434MHz
6	Sortie du boîtier pour antenne externe de la radio 868MHz ou 434MHz(optionnel)
7	Pack Piles
8	Connecteur pour pack piles
9	Aérateur
10	Sortie du boîtier pour alimentation externe (optionnel)
11	Bornier pour alimentation externe 12 Vcc
12	Sortie du boîtier pour antenne externe du Modem LTE-M/NB-IoT/2G (optionnel)
13	Antenne SMA du Modem LTE-M/NB-IoT/2G
14	Bouton Reset
15	Support carte SIM

Nouveau boîtier :



Numéro	Description
1	Capteur à effet HALL
2	Buzzer
3	Connecteur mini-USB
4	Voyants :

	• LED 1 : réservé • LED 2 : réservé • LED 5 : Statut du modem
5	Antenne SMA de la radio 868MHz ou 434MHz
6	Support pour le maintien du pack pile
7	Sortie sécable du boîtier pour installation de presse-étoupe M16 permettant l'installation d'une antenne externe radio 868MHz ou 434MHz (optionnel)
8	Pack Piles
9	Connecteur pour pack piles
10	Sortie sécable du boîtier pour installation de presse-étoupe M12 permettant l'installation d'un aérateur (optionnel)
11	Sortie sécable du boîtier pour installation de presse-étoupe M12 permettant l'installation d'une alimentation externe (optionnel)
12	Bornier pour alimentation externe 12 Vcc
13	Sortie sécable du boîtier pour installation de presse-étoupe M16 permettant l'installation d'une antenne externe Modem LTE-M/NB-IoT/2G (optionnel)
14	Antenne SMA du Modem LTE-M/NB-IoT/2G
15	Bouton Reset
16	Support carte SIM

1.4 Équipements supportés

Le concentrateur supporte tous les équipements respectant le standard Wireless M-Bus en 868MHz et utilisant l'un des modes suivants : T1, S1 et T1+C1.

Le concentrateur supporte tous les équipements respectant le standard Wireless M-Bus en 434MHz et utilisant les modes suivants : T1+C1 et S1.

1.5 Références des produits et accessoires

Produits :

Références	Descriptions
WG0612-A02	WebdynEasy WM-Bus 868MHz(sans BLE)
WG0612-A12	WebdynEasy WM-Bus 868MHz (avec BLE)
WG0612-A03	WebdynEasy WM-Bus 434MHz(sans BLE)
WG0612-A13	WebdynEasy WM-Bus 434MHz (avec BLE)



Les produits comprenant le BLE ne sont plus fabriqués.
Pour toute utilisation du BLE, veuillez vous rapprocher du service technique. (Voir chapitre 9 : « Support »)

Accessoires :

Références	Descriptions
AC0803-01	Pack piles 7.2V / 14Ah

Webdyn propose des prestations de pré-configurations en usine de vos WebdynEasy.
Veuillez-vous rapprocher de notre service commercial pour tous renseignements complémentaires.

1.6 Spécifications techniques

1.6.1 Caractéristiques générales

Caractéristiques	Descriptions
Alimentation	+12Vcc 1A

Pile	Pack piles Lithium 7.2V 14Ah (non rechargeable) – en configuration optimale, l'autonomie de la batterie est de 10 ans minimum.
Consommation	P : 2 W Pmax : 5 W
Dimensions	Ancien boîtier : 160 x 150 x 55 mm Nouveau boîtier : 150 x 153 x 57 mm
Boîtier	ASA IP67
Poids	0.600 kg avec pack piles 0.450 kg sans pack piles
Température de Fonctionnement	-20 °C / +55 °C
Température de stockage	-20 °C / +70°C (sans pile) -20 °C / +25°C (avec pile)
Humidité	25 - 75 %
Degré de pollution	2
Certification	RED ROHS REACH
Réglementation	 Marquage « CE » créé dans le cadre de la législation d'harmonisation technique européenne. Il est obligatoire pour tous les produits couverts par un ou plusieurs textes réglementaires européens (directives ou règlements).
	 Symbole indiquant que le déchet doit être collecté par une filière spécifique et ne doit pas être jeté dans une poubelle classique.
	 Symbole indiquant que le produit doit être recyclé.

1.6.2 Caractéristiques techniques

Caractéristiques	Descriptions
Capacité mémoire pour les données	- Flash : 1,5Mo (fonctionnement circulaire) 2000 trames par fenêtre d'écoute
Interface Radio	Fréquence : 868 MHz (mode T-C : 868,95MHz et mode S : 868,3MHz) 434 MHz (mode T : 434.475MHz et mode S: 434,15 MHz) Sensibilité : -105dBm Aucune transmission, uniquement de la réception. Antenne : SMA interne (externe en option)
Interface cellulaire Modem	Modem GSM/GPRS/EDGE/LTE-M 2G (GSM, GPRS) : 850/900/1800/1900 MHz - LTE-M1 : B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B25/B26/B27/B28/B66/B85 - NB-IoT : B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B25/B28/B66/B85 Antenne : SMA interne (externe en option)
Interface BLE	Bluetooth 4.2 compliant (pour la référence WG0612-A12 et WG0612-A13 uniquement))
Format SIM	SIM standard (mini SIM) format 2FF 1.8V compatible



Webdyn ne fournit aucune carte SIM. Veuillez vous rapprocher d'un opérateur M2M supportant le réseau LTE-M ou NB-IoT et 2G.

Données connectivités :

Bande RF	Fréquences Émission	Puissance Max
2G GSM 900	880 MHz – 915 MHz	33 dBm (class 4)

2G GSM 850	824 MHz – 849 MHz	
2G DCS 1800	1710 MHz – 1785 MHz	30 dBm (class 1)
2G PCS 1900	1850 MHz – 1910 MHz	
LTE-M/NB-IoT – Bande 1	1920 MHz – 1980 MHz	21 dBm (class 5)
LTE-M/NB-IoT – Bande 2	1850 MHz – 1910 MHz	
LTE-M/NB-IoT – Bande 3	1710 MHz – 1785 MHz	
LTE-M/NB-IoT – Bande 4	1710 MHz – 1755 MHz	
LTE-M/NB-IoT – Bande 5	824 MHz – 849 MHz	
LTE-M/NB-IoT – Bande 8	880 MHz – 915 MHz	
LTE-M/NB-IoT – Bande 12	699 MHz – 716 MHz	
LTE-M/NB-IoT – Bande 13	777 MHz – 787 MHz	
LTE-M/NB-IoT – Bande 18	815 MHz – 830 MHz	
LTE-M/NB-IoT – Bande 19	830 MHz – 845 MHz	
LTE-M/NB-IoT – Bande 20	832 MHz – 862 MHz	
LTE-M/NB-IoT – Bande 25	1850 MHz – 1915 MHz	
LTE-M – Bande 26	814 MHz – 849 MHz	
LTE-M – Bande 27	807 MHz – 824 MHz	
LTE-M/NB-IoT – Bande 28	703 MHz – 748 MHz	
LTE-M/NB-IoT – Bande 66	1710 MHz – 1780 MHz	

LTE-M/NB-IoT – Bande 85	698 MHz – 716 MHz	
BLE	2402 MHz – 2480 MHz	0 dBm

1.6.3 Caractéristiques logicielles

Caractéristiques	Descriptions
Wireless M-Bus	868 MHz : Mode T1, S1 et T1+C1 434 MHz : Mode T1+C1 et S1
BSON	Spécification 1.1
Version SSL	TLS1.2
Chiffrement SSL	- TLS_RSA_WITH_AES_256_CBC_SHA - TLS_RSA_WITH_AES_128_CBC_SHA - TLS_RSA_WITH_RC4_128_SHA - TLS_RSA_WITH_RC4_128_MD5 - TLS_RSA_WITH_3DES_EDE_CBC_SHA - TLS_RSA_WITH_AES_256_CBC_SHA256 - TLS_ECDH_ECDSA_WITH_RC4_128_SHA - TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA - TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA - TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA - TLS_ECDHE_ECDSA_WITH_RC4_128_SHA - TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA - TLS_ECDHE_RSA_WITH_RC4_128_SHA - TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - TLS_ECDH_RSA_WITH_RC4_128_SHA - TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA - TLS_ECDH_RSA_WITH_AES_128_CBC_SHA - TLS_ECDH_RSA_WITH_AES_256_CBC_SHA - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 - TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 - TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 - TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256

- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_PSK_WITH_AES_128_CCM_8
- TLS_PSK_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8

1.6.4 Autonomie

L'autonomie peut varier en fonction de l'utilisation du produit et des conditions environnementales.

Les tableaux ci-dessous sont des estimations prenant en compte :

- Des conditions environnementales standards
- 1 fenêtre d'écoute radio par jour
- 20ko de données enregistrées par fenêtre d'écoute (soit 300 trames de 64 octets ou 500 trames de 40 octets)

En LTE-M :

Durée de la fenêtre d'écoute en minutes	2 uploads / jour	1 upload / jour	1 upload / semaine
2	> 15 années	> 15 années	> 15 années
4	13 années	> 15 années	> 15 années
5	12 années	14 années	> 15 années
6	11 années	13 années	13 années
8	9 années	10 années	11 années
10	8 années	9 années	9 années
12	7 années	7 années	8 années
15	6 années	6 années	6 années
20	5 années	5 années	5 années
30	3 années	3 années	3 années

En NB-IoT :

Durée de la fenêtre d'écoute en minutes	2 uploads / jour	1 upload / jour	1 upload / semaine
2	11 années	>15 années	>15 années
4	9 années	12 années	>15 années
5	8 années	11 années	14 années
6	8 années	10 années	12 années
8	7 années	8 années	10 années
10	6 années	7 années	8 années
12	5 années	6 années	8 années
15	5 années	5 années	6 années
20	4 années	4 années	5 années
30	3 années	3 années	3 années

En 2G :

Durée de la fenêtre d'écoute en minutes	2 uploads / jour	1 upload / jour	1 upload / semaine
2	> 15 années	> 15 années	> 15 années
4	12 années	> 15 années	> 15 années
5	11 années	13 années	14 années
6	10 années	12 années	12 années

8	8 années	10 années	10 années
10	7 années	8 années	8 années
12	6 années	7 années	8 années
15	5 années	6 années	6 années
20	4 années	5 années	5 années
30	3 années	3 années	3 années



Quand le mode du modem est en mode auto, le modem se connecte par défaut en LTE-M puis si celui-ci est indisponible, il se replie sur le 2G. Si la première tentative de connexion échoue, le modem fera une deuxième tentative de connexion mais uniquement en 2G.

1.7 Consignes de sécurité

Respectez toutes les consignes de sécurité figurant dans ce guide.

Tout non-respect de ces consignes risque d'endommager les appareils et représenter un danger pour les personnes.

Raccordement électrique :



- Tous les travaux de câblage doivent impérativement être effectués par un électricien spécialisé.
- Veuillez respecter toutes les consignes de sécurité figurant dans la documentation de l'équipement du fabricant.



Le produit WebdynEasy peut être endommagé par des décharges électrostatiques (ESD)

Lorsque l'équipement est ouvert, ne pas réaliser d'opérations autres que celles prévues dans cette notice. Évitez tout contact avec les composants.



Équipement de classe 3 : l'appareil fonctionne en très basse tension de sécurité (TBTS) (50V maximum). L'abaissement de tension doit être réalisé à l'aide d'un transformateur de sécurité, réalisant une isolation galvanique sûre entre le primaire et le secondaire.



Ne pas installer l'équipement près d'une source de chaleur ou à une hauteur supérieure à 2m.
Ne pas exposer le boîtier directement aux rayons du soleil.



Pour le nettoyage du produit, vous servir uniquement d'un chiffon légèrement humide pour nettoyer et essuyer délicatement les surfaces. Ne jamais utiliser des agents chimiques agressifs ou solvants susceptibles d'altérer la matière plastique ou de corroder les éléments métalliques.



Ne jamais insérer une pile autre que celle préconisée par Webdyn.
Ne jamais recharger la pile.



Afin d'optimiser la sensibilité de réception Radio et cellulaire Modem, il est impératif de laisser un espace vide autour des antennes de 20 cm.

Précautions de manipulation :

- Protection contre l'Électricité Statique (ESD) : Les composants électroniques sont sensibles aux décharges électrostatiques. Portez un bracelet antistatique relié à la terre avant de brancher des câbles (USB ou alimentation) ou de manipuler la carte SIM pour éviter d'endommager la passerelle de manière irréversible.
- Connexions : Lors du raccordement du câble USB ou du connecteur d'alimentation externe, vérifiez attentivement l'alignement et la polarité, et insérez les connecteurs délicatement et sans forcer pour éviter de les endommager.
- Une fois les opérations terminées, assurez-vous qu'aucun outil, débris ou câble n'entrave le bon positionnement du joint d'étanchéité et la fermeture du couvercle. Le couvercle doit être correctement refermé et fixé pour assurer la protection physique et la conformité IP.

1.8 Réglementation

Le produit est conforme aux directives européennes selon la déclaration UE de conformité disponible auprès de Webdyn ou sur le site internet : www.webdyn.com

Recyclage :



Les directives européennes transposées relatives aux déchets de piles et d'équipements électriques et électroniques encadrent les actions nécessaires pour limiter l'impact négatif de la fin de vie du produit.

Ces produits font l'objet d'une collecte séparée. Utiliser un centre de collecte et de traitement des piles agréé ou contacter Webdyn.

1.9 Cybersécurité

Pour des raisons de cybersécurité, il faut utiliser :

- Le chiffrement AES systématique des fichiers
- Le protocole de communication sécurisé HTTPS est recommandé.

A partir de la version 4.0 les passerelles sont livrées avec le chiffage des fichiers activé et les clés AES individuelles sont fournies au moment de la livraison.

2 Installation

2.1 Prérequis

Le rôle du concentrateur WebdynEasy étant de transmettre les données qu'il collecte vers un SI, l'installation demande un niveau de connaissance du concentrateur, mais aussi du système d'information auquel il doit déposer ses données.

Les éléments suivants sont **requis** pour assurer d'une installation correcte :

- Avoir à disposition ce manuel utilisateur.
- Avoir un tournevis approprié aux types de connecteurs et vis disponibles sur le concentrateur WebdynEasy.
- Connaître les paramètres de connexion au système d'information SI.
- Avoir une carte SIM avec un abonnement M2M (data) activé et connaître l'APN du fournisseur.
- Posséder un aimant : format cylindrique long. (modèle conseillé : Fabricant : STANDEXMEDER, modèle : ALNICO500 5X22MM)

Mais il est également **fortement conseillé** d'avoir les éléments décrits ci-après pour toute intervention sur site et installation du produit.

- Utiliser une antenne déportée si la réception radio ou cellulaire modem est dégradée.
- Avoir un PC pour la configuration ou mise à jour du produit par USB.

2.2 Déballage

2.2.1 Contenu

Le concentrateur WebdynEasy est livré de base avec :

- Une antenne SMA coudée pour le modem (interne)
- Une antenne SMA coudée pour la radio (interne)
- Un pack piles

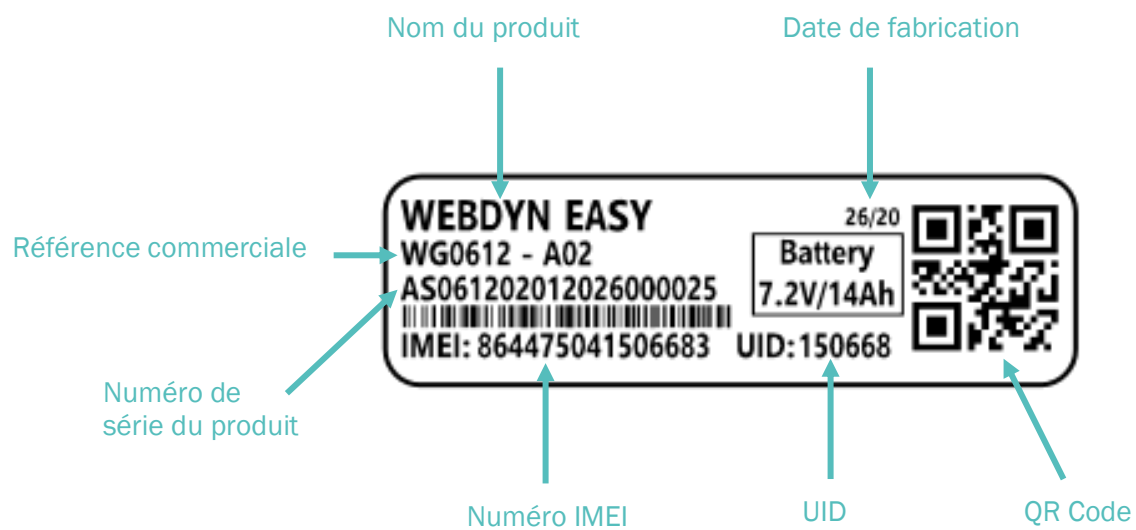
2.2.2 Identification

La référence commerciale est différente en fonction que le concentrateur intègre ou pas une configuration client. La référence commerciale se compose ainsi :

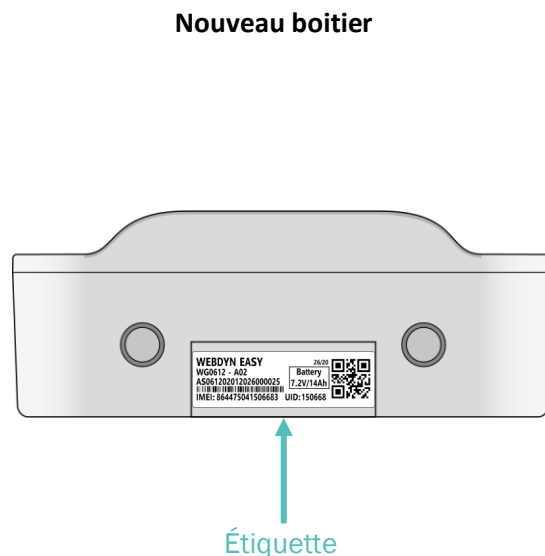
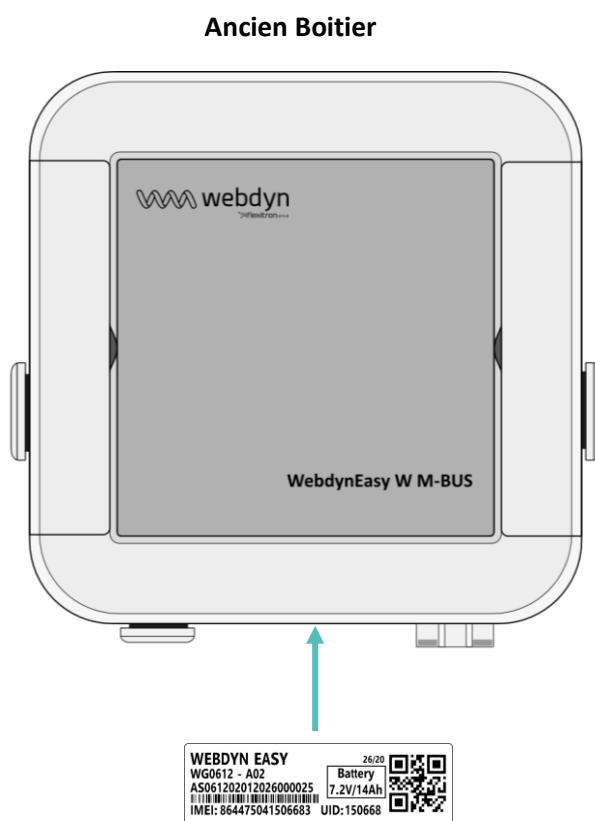
- **Sans configuration** : la référence commerciale est WG0612-A12.
- **Avec configuration** : la référence commerciale est WG0612-A12 auquel on ajoute l'identifiant client.
 - Par exemple, on peut obtenir la référence suivante : WG0612-A12-WG

Un identifiant unique appelé **UID** est attribué à chaque WebdynEasy, il permet de configurer le produit et de le reconnaître quand on possède plusieurs WebdynEasy.

Chaque produit est étiqueté avec les informations suivantes :



Cette étiquette est accessible sur le dessous du produit :



2.3 Montage

2.3.1 Ouverture/Fermeture du boîtier

Pour ouvrir le boîtier du concentrateur, suivez les étapes suivantes :



Le boîtier ne peut être ouvert que si celui-ci n'est pas fixé au mur. Dans le cas, où le boîtier est fixé à un mur, il faudra le décrocher pour pouvoir l'ouvrir.

Si le boîtier est fixé au mur :

Ancien boîtier :

1. Ouvrir les 2 trappes sur la face avant.
2. Dévisser les 4 vis de la fixation murale dans les logements sous les trappes.

Nouveau boîtier :

1. Dévisser les 4 vis de la fixation murale dans les logements présents en face avant.

Puis suivez ces étapes :

1. Dévisser les 4 vis qui se trouvent derrière le boîtier.
2. Retirer le capot

Pour fermer le boîtier du concentrateur, suivez les étapes suivantes :

1. Mettre en place le capot sur le socle du boîtier.
2. Visser les 4 vis qui se trouvent derrière le boîtier.

2.3.2 Fixation murale

La WebdynEasy peut être fixée sur un mur. Avant de procéder à la fixation murale, veuillez d'abord fermer le boîtier (Voir chapitre 2.3.1 : « Ouverture/Fermeture du boîtier »).



Les vis et chevilles ne sont pas fournies dans le kit. Vous devez choisir le bon type de vis en fonction du support auquel vous fixez le concentrateur.
(Vis de diamètre de 4mm, tête de diamètre 8mm maximum et de longueur de 25mm minimum)

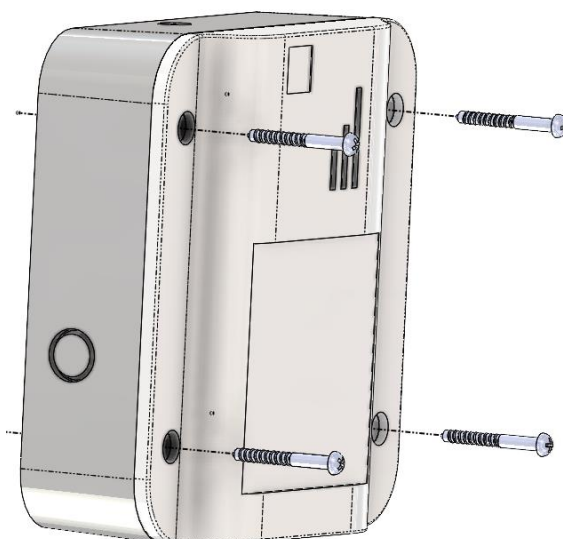
Pour fixer le concentrateur à un mur, suivez les étapes suivantes :

Ancien boîtier :

1. Ouvrir les 2 trappes sur la face avant.
2. Visser les 4 vis de la fixation murale dans les logements sous les trappes.
3. Refermer les 2 trappes sur la face avant.

Nouveau boîtier :

1. Insérer les 4 vis dans les 4 puits accessibles en face avant. (voir illustration ci-dessous)
2. Visser les 4 vis.



2.4 Description des interfaces

2.4.1 Alimentation du produit

2.4.1.1 Alimentation externe

Le concentrateur WebdynEasy peut être alimenté en 12V continu avec pack piles connectées. L'alimentation est réalisée via le bornier J8 situé à gauche du pack piles.



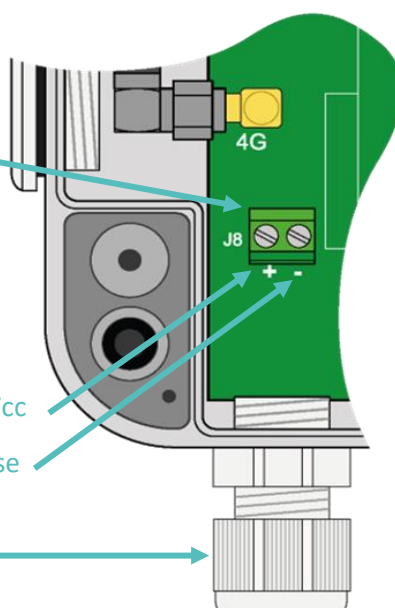
L'utilisateur final devra utiliser une alimentation certifiée CE de puissance inférieure à 15 watts. La distance entre l'alimentation et le produit ne devra pas dépasser **3 mètres**. Il devra s'assurer que son installation réponde aux normes CEM en vigueur.

Bornier pour alimentation
externe 12Vcc

Bornier 12Vcc

Masse

Presse-étoupe pour
alimentation externe



Dans le nouveau boîtier, le presse-étoupe est optionnel et s'installe après avoir cassé la partie sécable prévue dans le boîtier.



Veillez à respecter le sens de câblage de l'alimentation.

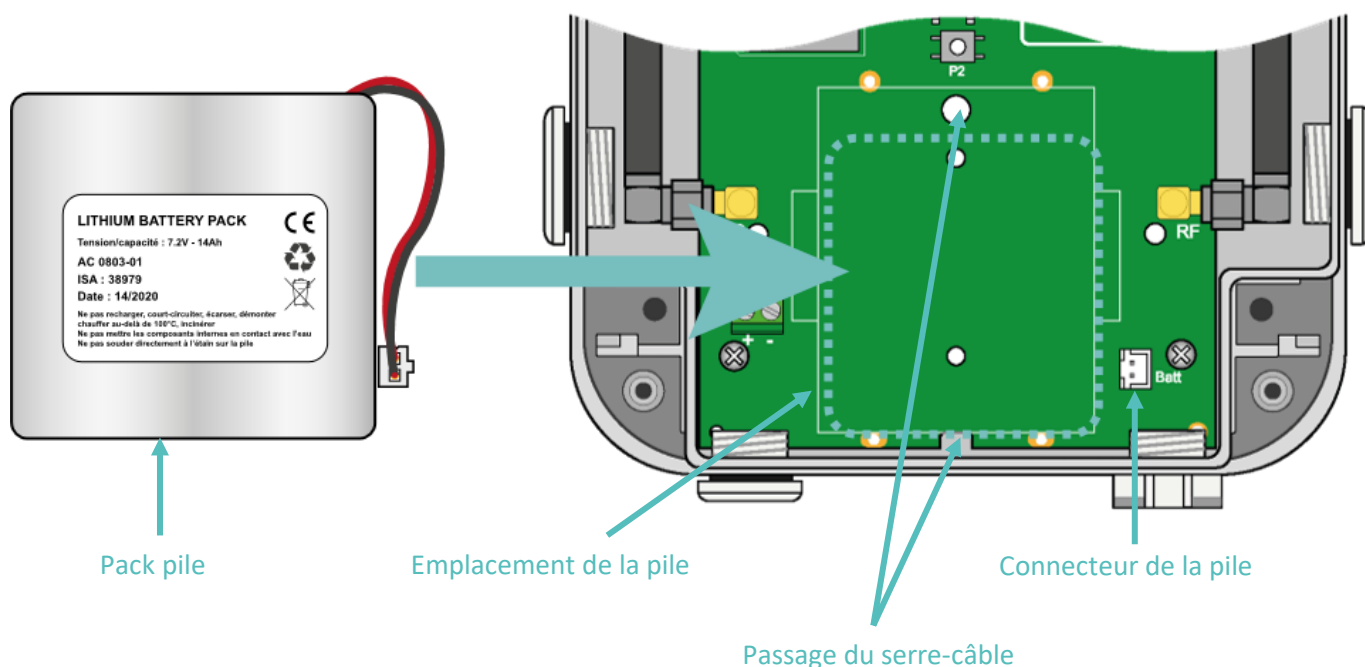
La consommation du produit est variable en fonction de sa configuration. Veillez à ce que l'alimentation utilisée puisse fournir une puissance de 10 watts minimum.

2.4.1.2 Pack piles

Le concentrateur WebdynEasy possède une pile Lithium permettant de faire fonctionner le produit pendant 10 ans. Le concentrateur permet d'estimer la consommation de la pile dès sa mise en place.

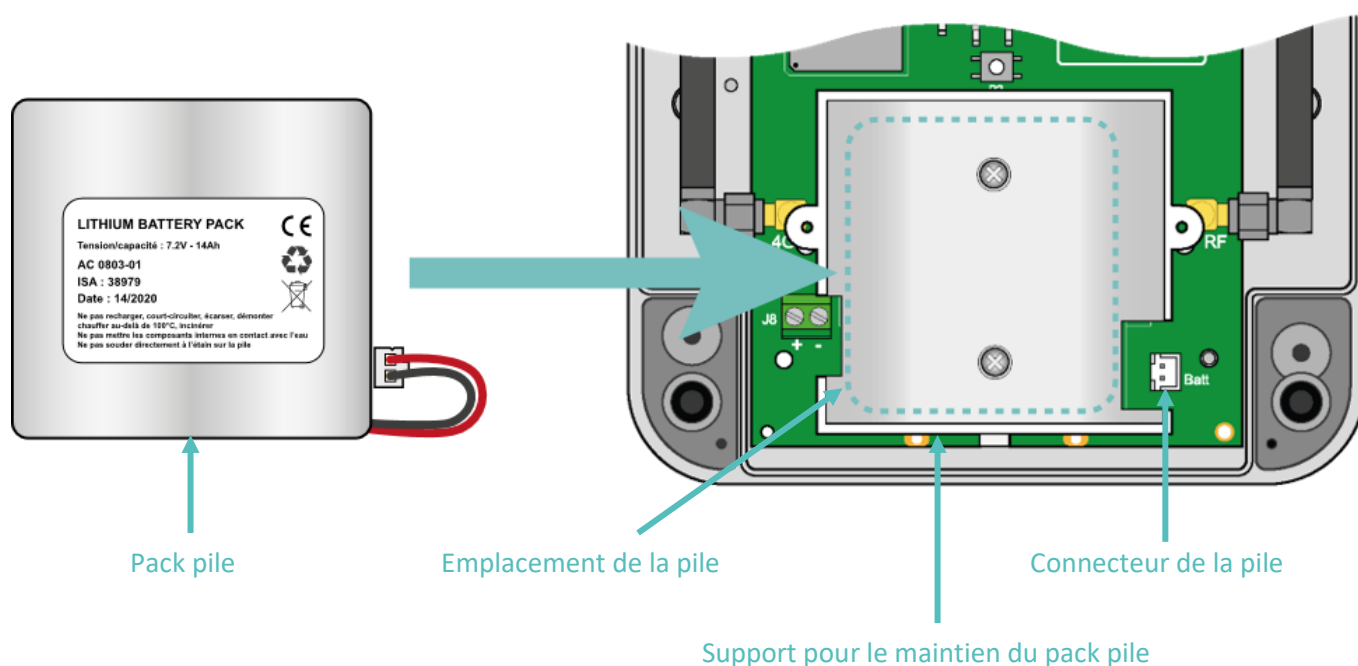
Ancien boîtier :

Le pack piles se fixe à la carte à un emplacement réservé à l'aide d'un serre-câble et il se branche au connecteur identifié « Batt » sur la carte.



Nouveau boîtier :

Le pack piles s'installe dans son support et il se branche au connecteur identifié « Batt » sur la carte.



Ne jamais installer un pack piles qui n'est pas neuf car le compteur de capacité est remis à 100% suite au branchement.

Une fois un pack piles installé, ne jamais le débrancher sauf pour son remplacement.



ATTENTION, IL Y A RISQUE D'EXPLOSION SI LE PACK PILES EST REMPLACÉ PAR UN AUTRE PACK PILES AUTRE QUE CELUI PRÉCONISÉ PAR WEBDYN.
METTRE AU REBUT LES PACKS PILES USAGÉS CONFORMÉMENT AUX INSTRUCTIONS.

2.4.2 Radio

Le concentrateur possède une radio en 868 MHz ou 434 MHz permettant de recevoir les trames Wireless M-Bus des capteurs environnants.

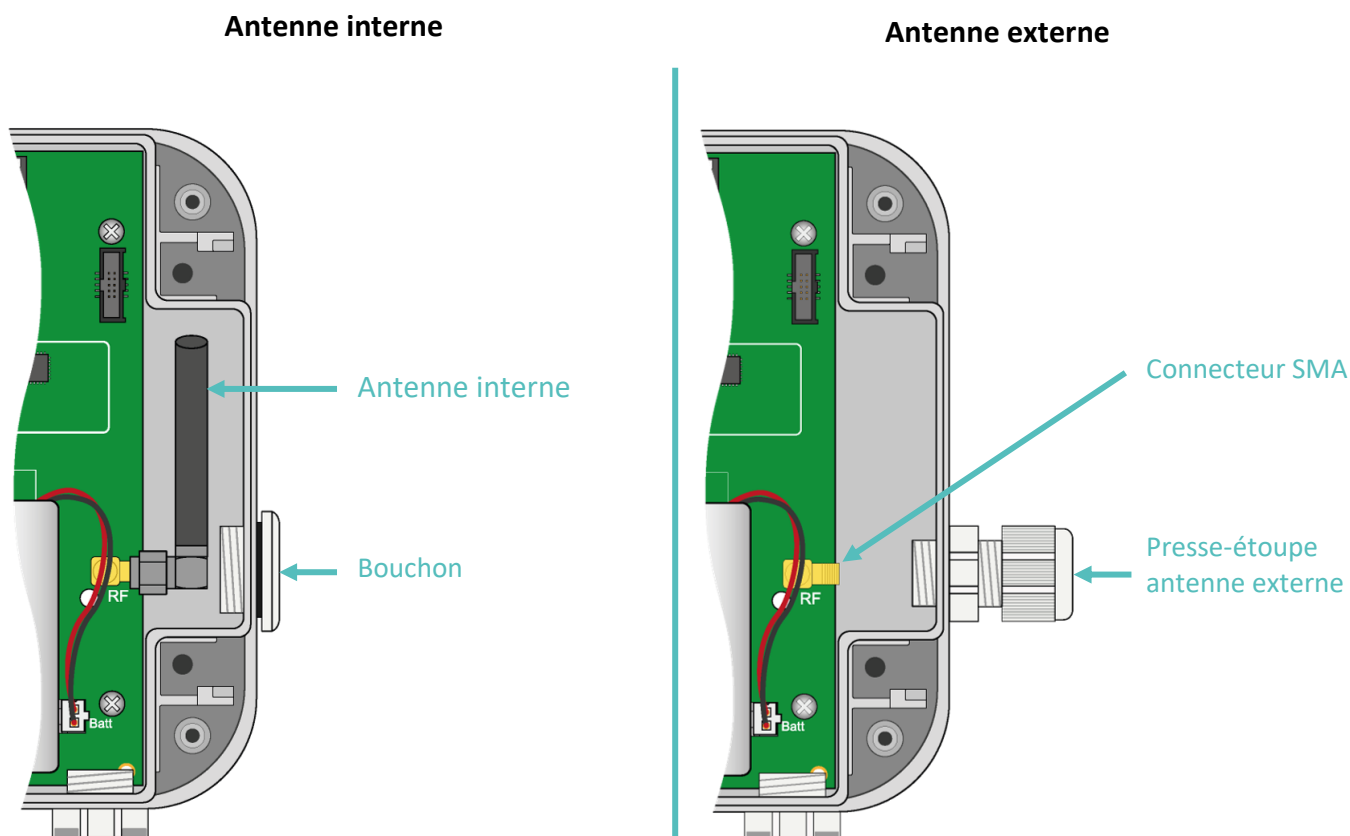
La portée théorique en champ libre (ou Line of Sight - LOS) dépend fortement du mode de communication et de la bande de fréquence utilisés (433 MHz et 868 MHz). Pour les bandes de 868 MHz (Modes S, T, C) : La portée en champ libre se situe généralement entre quelques centaines de mètres et 1 kilomètre.

Note : La portée réelle en environnement d'utilisation est toujours significativement réduite par les obstacles (murs, cloisons, structures métalliques) et le bruit radio. La portée typique à l'intérieur des bâtiments en 868 MHz est de l'ordre de plusieurs dizaines de mètres.

2.4.2.1 Antenne

Le concentrateur possède un connecteur SMA femelle identifié « RF » sur la carte afin de raccorder une antenne pour la radio. Le produit est livré avec une antenne interne. Il est possible de raccorder une antenne externe au produit. Pour cela, il faut dévisser le bouchon du boîtier et y installer un presse-étoupe M16*1.5 (non fourni).

Pour optimiser la portée radio, il est important d'installer l'antenne radio le plus haut possible et de la placer de façon judicieuse en évitant au maximum les obstacles. Éloignez-vous en priorité de tout obstacle métallique (armoires métalliques, poutrelles...) ou béton (béton armé, murs...) qui atténue énormément l'onde radio.



Dans le nouveau boîtier, le presse-étoupe est optionnel et s'installe après avoir cassé la partie sécable prévue dans le boîtier.



L'utilisateur final devra s'assurer que son installation avec **antennes déportées** réponde aux normes CEM en vigueur.

2.4.3 Réseau cellulaire

Le concentrateur WebdynEasy intègre un modem compatible avec les réseaux LTE-M, NB-IoT et 2G.

2.4.3.1 Antenne

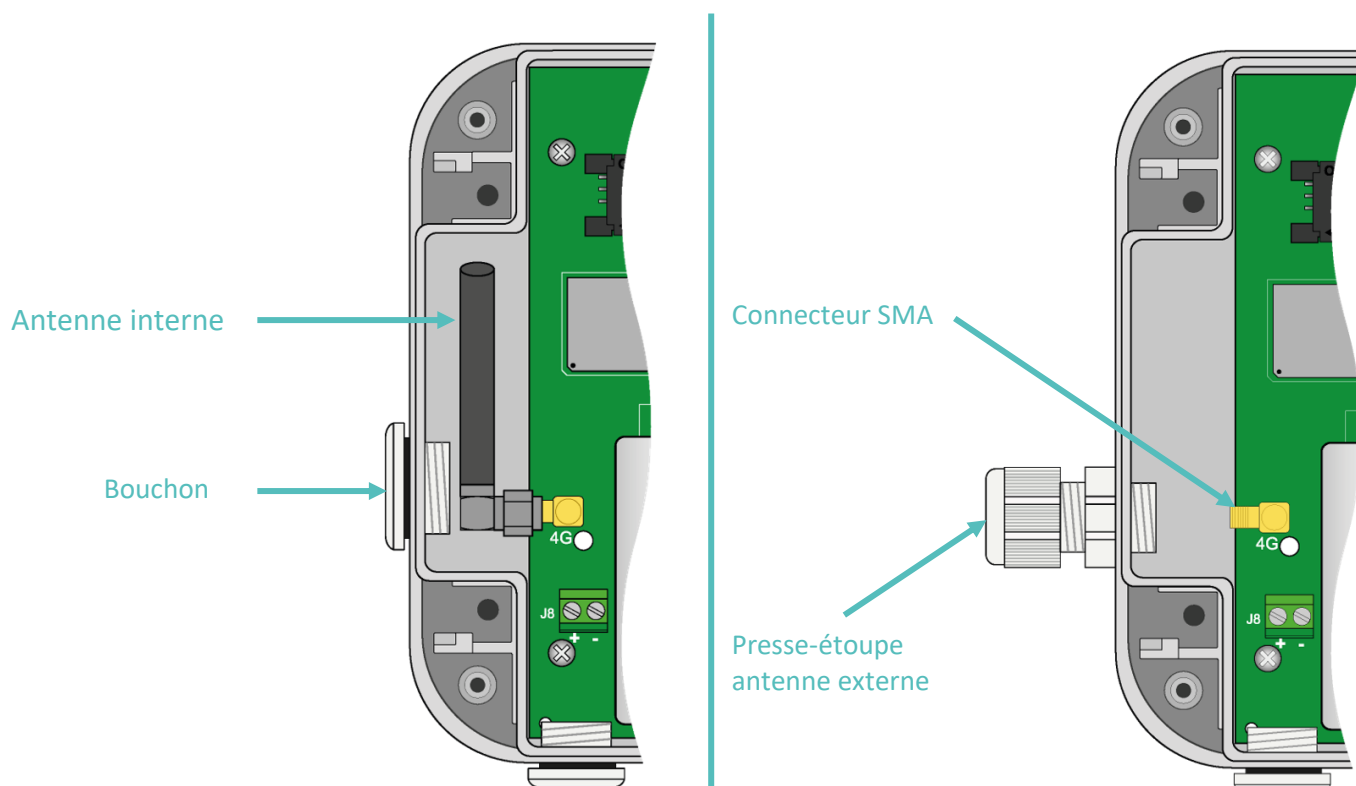
Le concentrateur possède un connecteur SMA femelle identifié « 4G » sur la carte afin de raccorder une antenne pour le modem. Le produit est livré avec une antenne interne. Il est possible de raccorder une antenne externe au produit. Pour cela, il faut dévisser le bouchon du boîtier et y installer un presse-étoupe M16*1.5 (non fourni).



Dans le cas où le concentrateur WebdynEasy serait installé dans un coffret métallique ou dans un emplacement ne permettant pas une réception correcte du signal. L'utilisation d'une antenne déportée est fortement conseillée. Attention à utiliser une antenne compatible avec le connecteur et les fréquences utilisées.

Antenne interne

Antenne externe



Dans le nouveau boîtier, le presse-étoupe est optionnel et s'installe après avoir cassé la partie sécable prévue dans le boîtier.



L'utilisateur final devra s'assurer que son installation avec **antennes déportées** réponde aux normes CEM en vigueur.

Les puissances et les références des antennes externes se trouvent ci après

- Bande 868 MHz (WmBUS/LoRa)

- Pmax < 14dBm
- Ref antennes : Webdyn AC0201-01-EA1065 (5m), -02-EA1065 (20m), -03-EA1065 (10m)
- Bandes 4G (1,3,8,20,28)
 - Pmax < 21dBm
 - Ref antennes 2G/4G : Webdyn AC0201-11 (5m) , -12 (20m), -13 (10m)
- Bandes 2G 900MHz (bande 8)
 - Pmax < 33dBm
 - Ref antennes 2G/4G : Webdyn AC0201-11 (5m) , -12 (20m), -13 (10m)
- Bandes 2G 1800MHz (bande 3)
 - Pmax < 31dBm
 - Ref antennes 2G/4G : Webdyn AC0201-11 (5m) , -12 (20m), -13 (10m)

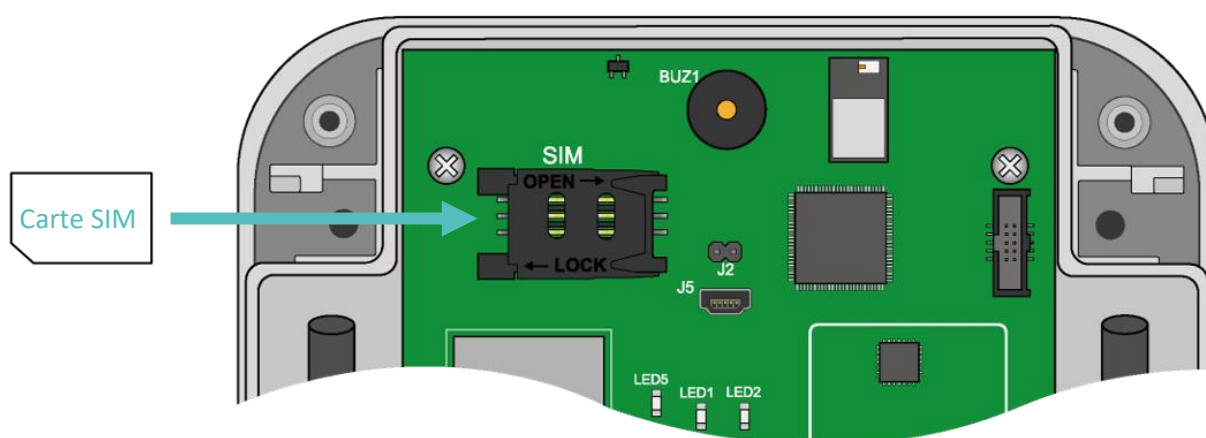
2.4.3.2 Carte SIM

Pour utiliser la liaison Modem LTE-M, NB-IoT ou 2G et permettre au concentrateur de communiquer avec le serveur distant, il faut procéder à l'ouverture du boîtier (*voir chapitre 2.3.1 : « Ouverture/Fermeture du boîtier »*) et insérer une carte SIM au format mini SIM dans le logement de carte SIM à l'intérieur du concentrateur.

Le concentrateur est compatible avec l'ensemble des opérateurs du marché, ainsi qu'avec toutes les cartes SIM au format mini SIM 2FF 25 x 15mm.

Afin d'assurer le bon fonctionnement de la WebdynEasy, vous devez insérer une carte SIM présentant les caractéristiques suivantes :

- Communication LTE-M, NB-IoT ou 2G inclus.



Pour insérer la carte SIM dans le produit, il faut faire glisser le volet du support sur la droite (dans le sens OPEN). Insérer la carte SIM dans le volet en la faisant glisser dedans. Puis, fermer le volet en le glissant vers la gauche (dans le sens LOCK)



Webdyn ne fournit aucune carte SIM. Veuillez-vous rapprocher d'un opérateur M2M supportant le réseau LTE-M ou NB-IoT et 2G.



Pour connaître les informations à saisir pour la configuration du modem, veuillez-vous vous rapprocher de votre fournisseur de cartes SIM.

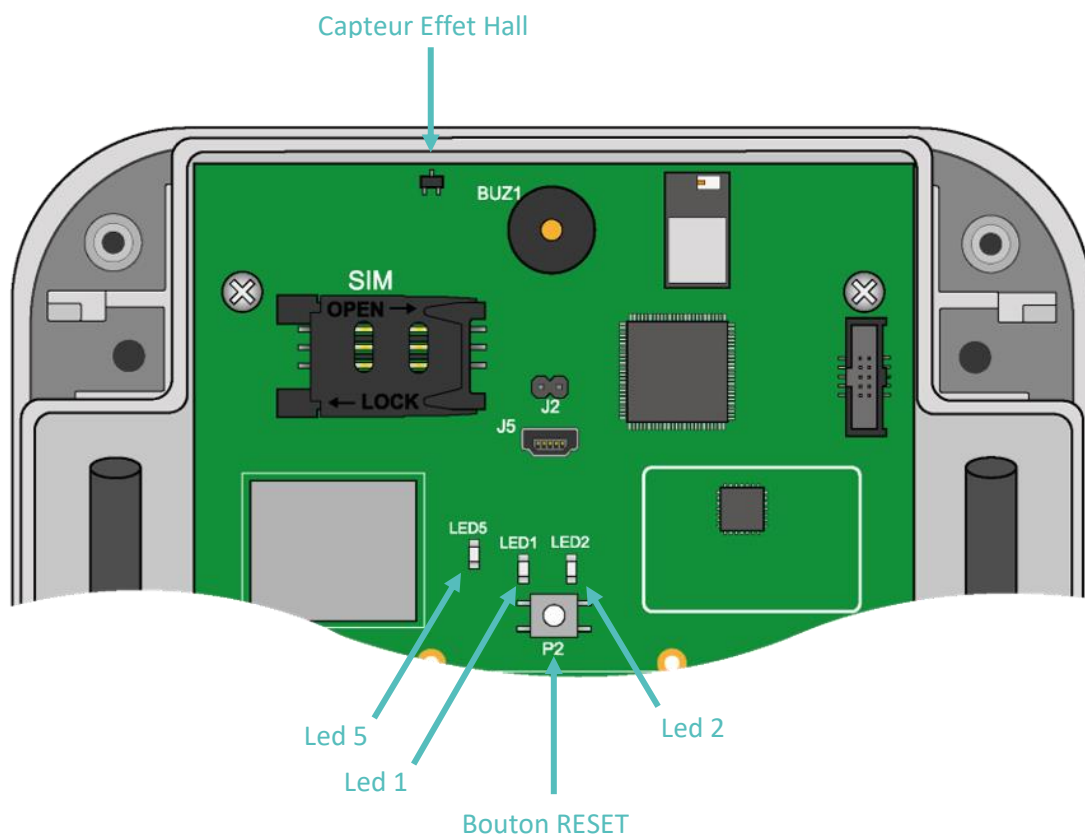


Si la carte SIM a un code PIN activé et qu'il est incorrect au premier démarrage du concentrateur, elle sera bloquée après 3 tentatives. Vous pouvez la débloquent en utilisant un téléphone portable avec le code PUK fourni par votre opérateur.

2.4.4 Les voyants & boutons

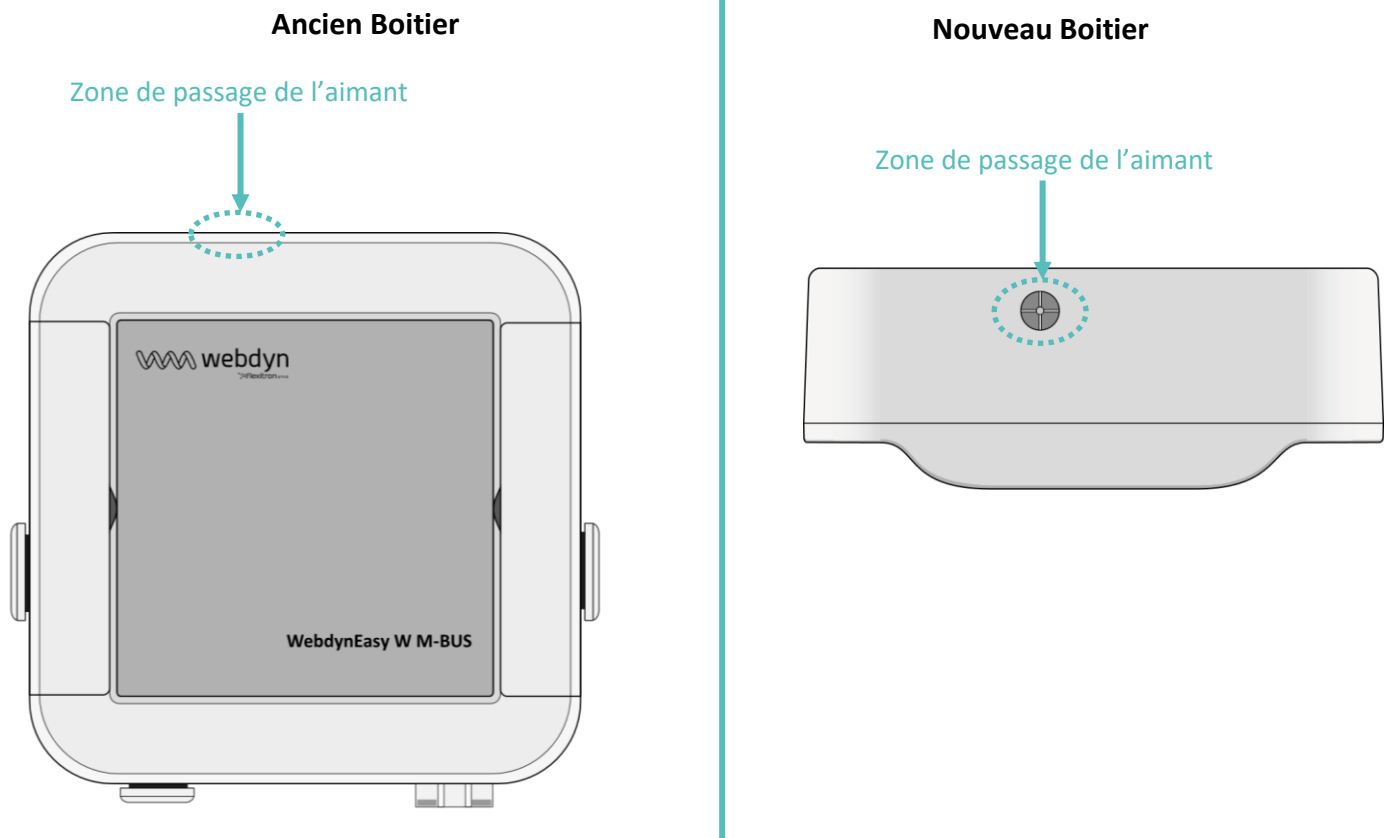
Le concentrateur est équipé de :

- 1 capteur à Effet Hall
- 1 bouton poussoir
- 1 voyant modem.



2.4.4.1 Capteur Effet Hall

Le concentrateur WebdynEasy est muni d'un capteur à Effet Hall qui s'active au passage d'un aimant sur le haut du boîtier.



Le capteur à effet Hall permet de faire diverses actions comme :

- Demander le mode de fonctionnement en cours et activer les interfaces pour la configuration locale.
- Changer le mode de fonctionnement.
- Faire un retour usine du produit (en combinaison avec le bouton RESET)

2.4.4.2 Bouton RESET

Le bouton RESET possède deux comportements :

- **Redémarrage** du produit : un appui bref sur le bouton
- **Retour Usine** : en suivant cette procédure :
 1. Placer l'aimant sur le haut du boîtier face au capteur à effet Hall et maintenez-le en position.
 2. Appuyer brièvement sur le bouton RESET.
 3. Un Bip long (1 seconde) retentit, informant de la prise en compte du retour Usine.
 4. Retirer l'aimant.

2.4.4.3 LED Modem

La led Modem s'allume quand le modem est activé pour déposer les fichiers sur le serveur distant.

2.4.5 Interface USB

L'interface USB du concentrateur peut être utilisée pour :

- La configuration
- Les commandes
- La mise à jour du produit.

Pour le bon fonctionnement, il est indispensable de suivre scrupuleusement les étapes suivantes :

1. Mettre la WebdynEasy en mode MARCHE.
2. Connecter le concentrateur à un ordinateur en utilisant un câble USB (type A mâle - mini B mâle).
3. Sur l'ordinateur un nouveau disque nommé « WebdynEasy » apparaîtra (comme une clé USB)
4. Ouvrir ce disque
5. Copier le fichier de configuration, de commande ou de mise à jour sur le disque
6. Ejecter le disque amovible et attendre sa confirmation par le système.
7. Appuyer sur le bouton RESET.
8. Le produit redémarre.

Les étapes suivantes sont facultatives et en fonction des commandes passées.

9. Sur l'ordinateur un nouveau disque nommé « WebdynEasy » apparaîtra (comme une clé USB)
10. Ouvrir ce disque
11. Ouvrir le fichier ACK et examiner le résultat de la commande
Ou
Récupérer les fichiers demandés par la commande.
12. Ejecter le disque amovible et attendre sa confirmation par le système avant débranchement du câble USB.

A partir de la version 2.05, le fichier de configuration « info.bson » est présent systématiquement sur le disque USB de la WebdynEasy.

A partir de la version 2.05, il est possible de redémarrer la WebdynEasy en créant sur le disque USB un fichier nommé « reboot » et d'utiliser la commande système d'éjection du PC. Le produit redémarrera et traitera les éventuels fichiers de commande ou de configuration présents sur la partition.

Exemple de commande système d'éjection :

- Linux (shell command) :

```
gio mount -e /media/user/WebdynEasy
```

- Windows :

```
powershell.exe -ExecutionPolicy Unrestricted -file eject.ps1
```

Avec le fichier « eject.ps1 » :

```
$driveEject = New-Object -comObject Shell.Application  
$driveEject.Namespace(17).ParseName("f:").InvokeVerb("Eject")'
```



Ne jamais débrancher le câble USB ou redémarrer la carte avant d'avoir éjecté le disque amovible par le système. Vous pouvez endommager le système de fichier et corrompre les fichiers déposés.



Si le disque amovible est inaccessible, vous devez le formater en FAT32.

3 Fonctionnement du produit

3.1 Démarrage du produit

Par défaut, le concentrateur WebdynEasy est livré soit en mode :

- **STORAGE** : si le produit est livré avec une configuration client
- **FACTORY SETTINGS** : si le produit est livré sans configuration.

Ces modes sont des modes basse consommation, et permettent le stockage des produits sur de longues périodes en limitant la consommation de la pile.



Pour savoir si la WebdynEasy possède une configuration client, veuillez vérifier la référence commerciale du produit. (Voir chapitre 2.2.2 : « Identification »)

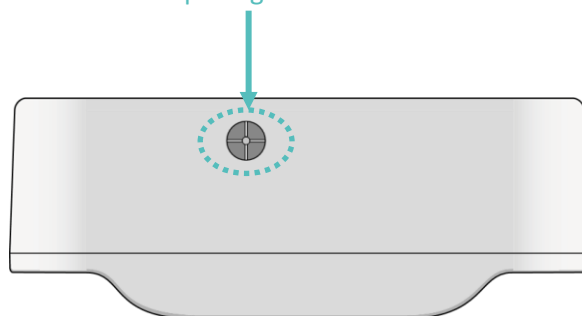
Ancien Boîtier

Zone de passage de l'aimant



Nouveau Boîtier

Zone de passage de l'aimant



Pour changer de mode, et réveiller le produit, il est nécessaire de passer lentement un aimant sur le haut du boîtier à l'endroit indiqué (voir l'emplacement ci-dessus) jusqu'au premier bip émis par le concentrateur. Le nombre de bip émis par la WebdynEasy informe sur le mode en cours.

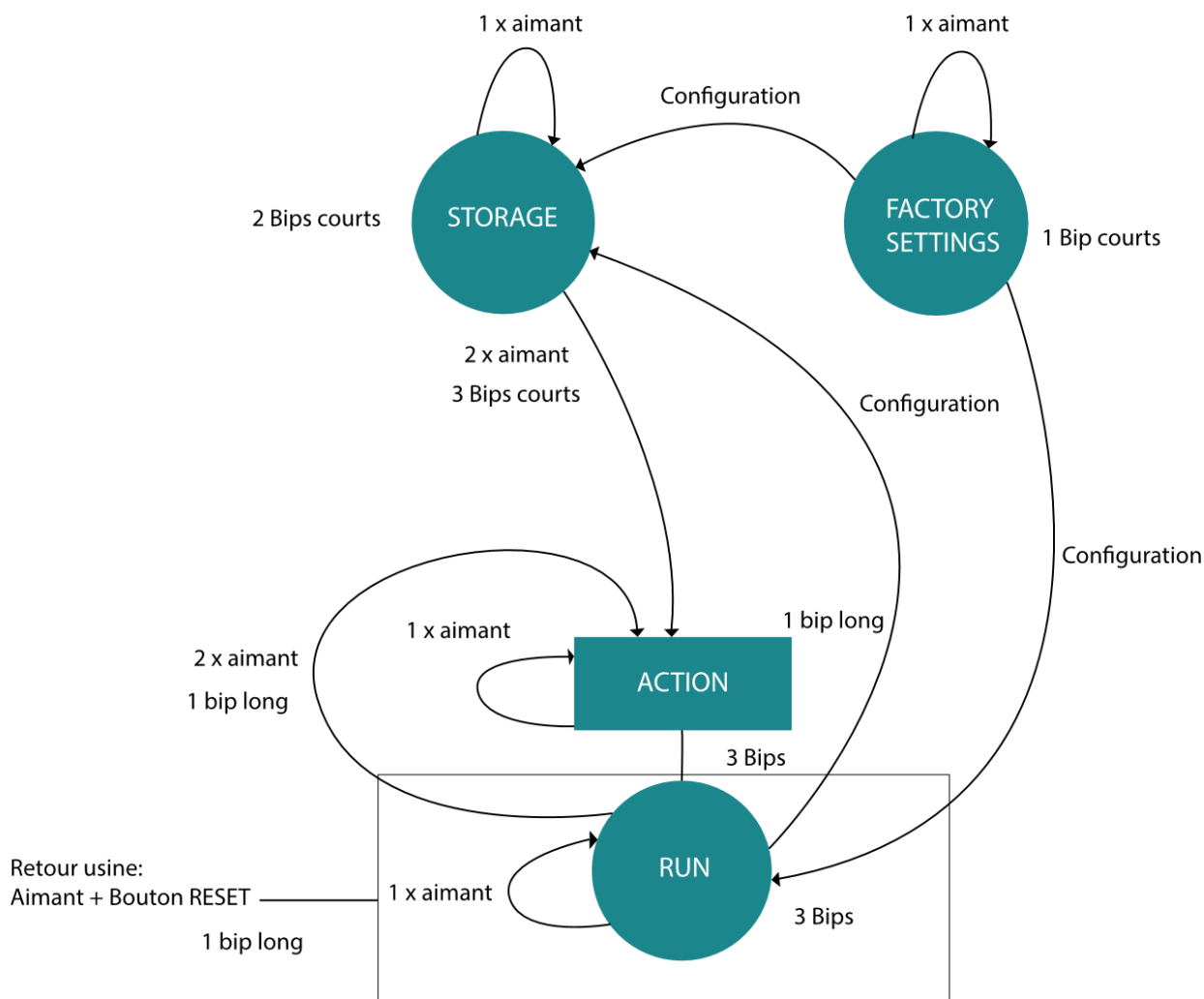
3.1.1 Modes de fonctionnement

Le module possède 3 modes de fonctionnement :

- **FACTORY SETTINGS** (sans configuration)
- **STORAGE** (avec configuration)
- **RUN**

Les changements de mode sont **toujours** à l'initiative de l'installateur.

La machine d'état ci-dessous représente les 3 modes, les conditions de changement de mode, ainsi que l'indication sonore pour chaque mode.



Une action sur le capteur à Effet Hall est prise en compte dès le passage d'un aimant sur ce dernier. Par exemple, si un passage d'aimant est fait sur le capteur à Effet Hall, un ou plusieurs bips retentiront informant du mode actuel du concentrateur. Lorsqu'un deuxième passage d'aimant est effectué dans un délai de 10 secondes suivant le précédent passage alors le concentrateur passera en mode RUN.

À chaque mode (STORAGE, FACTORY SETTINGS et RUN) est associé une indication sonore permettant de connaître l'état de l'équipement.

Il est possible de changer de mode en le précisant dans l'envoi d'une configuration au concentrateur.

Du point de vue de l'installateur :

- Un passage d'aimant permet de connaître le mode courant :
 - 1 bip court : le produit est en mode **FACTORY SETTINGS** (sans configuration client).
 - 1 bip long : une action est en cours, veuillez attendre la fin de l'action pour demander le mode de fonctionnement.
 - 2 bips courts : le produit est en mode **STORAGE** (avec configuration client).
 - 3 bips courts : le produit est en mode **RUN** et la dernière connexion du produit avec le serveur a réussi
 - 3 bips longs : le produit est en mode **RUN** et la dernière connexion du produit avec le serveur a échoué.
- Deux passages d'aimant en moins de 10 secondes permettent :
 - En mode **STORAGE** :
3 bips courts + 1 bip long : le produit exécute l'action associée à l'aimant (activation du BLE, commande Diagnostic ou commande Request) et passe en mode **RUN**.
 - En mode **RUN** :
1 bip long : le produit exécute l'action associée à l'aimant (activation du BLE, commande Diagnostic ou commande Request) et retourne en mode **RUN**.
- Présence d'un aimant + appuyer sur le bouton RESET permet un « retour usine » :
 - 1 bip long : le produit commence son processus de « retour usine ».

3.1.1.1 Mode **FACTORY SETTINGS**

Le produit est livré en mode **FACTORY SETTINGS** s'il ne possède aucune configuration. Le concentrateur est alors en veille et sa consommation est minimale. Au passage de l'aimant, un bip court retentit pour signifier la détection de l'aimant et indiquer son mode.

La sortie du mode **FACTORY SETTINGS** s'effectue uniquement par la configuration du produit.

La configuration du concentrateur peut se faire par :

- **USB** : le branchement du câble USB, réveille automatiquement le produit.

Afin d'optimiser la consommation de la pile, les interfaces se couperont automatiquement au bout de 4 minutes sans activité. Pour réactiver les interfaces, il faudra lancer une nouvelle phase de configuration si nécessaire.

Lors de la configuration du produit, il est possible de définir le mode souhaité.



Pour savoir si la WebdynEasy possède une configuration client, veuillez vérifier la référence commerciale du produit. (Voir chapitre 2.2.2 : « Identification »)

3.1.1.2 Mode **STOCKAGE**

Le produit est livré en mode **STOCKAGE** s'il possède une pré-configuration usine. Le concentrateur est alors en veille et sa consommation est minimale. Au passage de l'aimant, deux bips courts retentissent pour signifier la détection de l'aimant et indiquer son mode.

La sortie du mode **STOCKAGE** s'effectue uniquement par un double passage d'aimant en moins de 10 secondes et le concentrateur passe en mode **RUN**.



Pour savoir si la WebdynEasy possède une configuration client, veuillez vérifier la référence commerciale du produit. (Voir chapitre 2.2.2 : « Identification »)

3.1.1.3 Mode RUN

Le mode RUN permet de faire fonctionner le produit dans son utilisation finale. Il permet d'exécuter périodiquement la récupération des données WM-BUS des capteurs et de se connecter en modem afin de les déposer sur le serveur. Quand le produit ne fait aucune action, il se met en mode veille afin d'optimiser sa pile. Au passage de l'aimant, trois bips retentissent pour signifier la détection de l'aimant, indiquer son mode et informer l'état de la dernière connexion avec le serveur :

- 3 bips courts : la dernière connexion du produit avec le serveur a réussi.
- 3 bips longs : la dernière connexion du produit avec le serveur a échoué.

Un deuxième passage de l'aimant en moins de 10 secondes permet d'exécuter l'action (activation du Modem, commande Diagnostic ou commande Request) et retourne en mode **RUN**.

Le concentrateur possède si besoin d'un multi mode d'écoute qui permet de récupérer les données WM-Bus des capteurs dans un mode puis de récupérer ensuite les données WM-Bus d'autres capteurs qui se trouvent dans un autre mode.

La configuration du concentrateur peut se faire par :

- **USB** : le branchement du câble USB, réveille automatiquement le produit.

Afin d'optimiser la consommation de la pile, les interfaces se couperont automatiquement après 4 minutes sans activité. Il faudra lancer une nouvelle phase de configuration pour la réactiver si nécessaire.

Lors de la configuration du produit, il est possible de définir le mode souhaité. Quand le concentrateur appliquera la configuration, il informera l'utilisateur par le buzzer du mode en cours.

En mode RUN ou STORAGE, une action est déclenchée lors du deuxième passage de l'aimant sur le produit avant que celui-ci se mette en mode RUN. Cette action est configurable dans le produit (Voir chapitre 4.2.1.1 : « Locale »).

Il y a 3 actions possibles :

- **Activation du Modem** : Le produit attend une configuration ou une mise à jour par Modem pendant 4 minutes avant de passer en mode RUN et de désactiver le Modem.
- **Commande diagnostic** : permet la récupération des données WM-BUS des capteurs sur une durée configurée (voir le paramétrage radio « config→radio→duration ») et de lancer la connexion via modem afin de les déposer sur le serveur. En fin de diagnostic, le concentrateur informera du résultat par :
 - 3 bips courts si tout est ok.
 - 3 bips longs en cas de problème.
- **Commande Request** : permet de lancer la connexion via modem afin de déposer ou récupérer des fichiers (configuration, données, supervision, ...) sur le serveur FTP. A la fin de la connexion, le concentrateur informera du résultat par :
 - 3 bips courts si la connexion avec le serveur a réussi.
 - 3 bips longs si la connexion avec le serveur a échoué.

3.1.1.4 RESET

Le concentrateur possède 2 fonctionnalités de RESET déclenchable par le bouton RESET (Voir chapitre 2.4.4.2 : « Bouton RESET ») et qui sont :

- **Redémarrage** du produit,
- **Retour Usine** de la configuration du produit.

En cas de pré-configuration en usine de paramètres personnalisés, ceux-ci sont considérés comme les paramètres par défaut et donc appliqués en cas d'utilisation d'un mécanisme de retour usine.



Pour savoir si la WebdynEasy possède une configuration client, veuillez vérifier la référence commerciale du produit. (Voir chapitre 2.2.2 : « Identification »)

3.1.2 Fonctionnement applicatif

En mode RUN, le produit exécute 3 tâches qui sont :

- WM-BUS
- Modem
- Surveillance (Monitoring)

Ces tâches sont périodiques et non synchronisées entre elles.

3.1.2.1 Tâche WM-BUS

La tâche Radio WM-BUS permet de récupérer les données WM-BUS des capteurs. Elle possède son propre ordonnanceur afin de régler sa périodicité ainsi que sa date et son heure d'exécution. Il est également possible de configurer la durée d'écoute en WM-BUS.

Principe d'enregistrement des trames :

Au cours d'une fenêtre d'écoute WM-Bus, seule la première trame de chaque taille envoyée par un module est enregistrée.

Par exemple : Lorsqu'un compteur émet une trame de 20 octets toutes les 8 secondes et une trame de 45 octets toutes les 60 secondes. Au cours d'une fenêtre d'écoute de 2 minutes, seule la première trame de 20 octets et la première trame de 45 octets sont enregistrées.

3.1.2.2 Tâche Modem (connexion SI)

La tâche Modem permet de :

- Mettre à l'heure le concentrateur par NTP
- Déposer et récupérer les fichiers sur le serveur (FTPS, HTTPS).

Elle possède son propre ordonnanceur afin de régler sa périodicité ainsi que sa date et son heure d'exécution. Il est également possible de configurer le type de fichier à déposer sur le serveur.

3.1.2.3 Tâche de Surveillance (Monitoring)

La tâche Monitoring permet de surveiller :

- La température du produit : des mesures de température sont prélevées et enregistrées dans le fichier de supervision. Il est également possible de configurer la température maximum à ne pas dépasser.
- Le niveau de la pile du produit : il est possible de définir le pourcentage minimum du niveau de la pile.

En cas de franchissement d'un seuil défini, une alarme est déclenchée et envoyée vers le serveur. Tant qu'une alarme de température est déclenchée, la périodicité des tâches WM-BUS et Modem est arrêtée.

La tâche Monitoring possède sa propre périodicité en minutes.

4 Configuration

Le concentrateur WebdynEasy peut être configuré de différentes manières, soit par :

- Fichier de configuration : A déposer sur le serveur (FTP(S), HTTP(S)) ou sur le disque amovible par connexion USB.

Dans le cas d'une configuration à distance avec un concentrateur livré sans configuration client, il est nécessaire de préconfigurer l'interface cellulaire et l'accès aux serveurs (FTP(S), HTTP(S)) localement pour que le concentrateur se connecte périodiquement au SI.

Dans le cas où le concentrateur est livré avec une configuration client, le produit récupérera sa configuration directement sur le serveur (FTP(S), HTTP(S)) sans avoir besoin d'une configuration locale au préalable.

4.1 Configuration locale par USB

Pour configurer localement la WebdynEasy, le concentrateur doit se trouver en mode RUN ou FACTORY SETTINGS. La configuration locale peut se faire par USB.

Le branchement du câble USB sur le produit réveille le produit. Un nouveau disque nommé « WebdynEasy » apparaît comme une clé USB. Un fichier de configuration déposé sur ce disque est automatiquement pris en compte après un redémarrage du concentrateur.

Veuillez suivre les étapes détaillées dans le chapitre 2.4.5 : « Interface USB » .

Le fichier de configuration est décrit dans le chapitre 4.2 : « Fichier de configuration »

Après chaque prise en compte d'un fichier de configuration ou de mise à jour, un fichier d'acquiescement (*Voir chapitre 5.5 : « Les acquiescements ACK »*) est déposé sur le disque du concentrateur.

4.2 Fichier de configuration

Les fichiers de configuration échangés avec le concentrateur sont au format BSON qui est une version binaire du JSON. Le format décrit dans le document est au format JSON. Pour transformer le format JSON en BSON ou vice versa, il vous faudra utiliser une bibliothèque mise à disposition sur le site officiel : <http://bsonspec.org/implementations.html>

Afin d'éviter l'altération de fichier lors des échanges, un CRC32 est intégré dans chaque fichier. (*Voir chapitre 5.1.1.5 : « Format des fichiers »*)

Le fichier de configuration du concentrateur WebdynEasy est au format BSON et son format est le suivant :

« <uid>-config.bson »

Le concentrateur possède une configuration par défaut. Il n'est donc pas nécessaire de mettre tous les paramètres dans le fichier de configuration. Un fichier de configuration peut être complet ou partiel. Vous pouvez donc envoyer un fichier de configuration contenant qu'une seule variable.



Les paramètres des fichiers JSON sont sensibles à la casse. Veuillez respecter les majuscules et minuscules.



Il est possible de réutiliser le fichier de configuration déposé par le concentrateur. Pour cela, il est important de renommer le fichier « `<uid>-cfg.bson` » en « `<uid>-config.bson` ».

4.2.1 Système

Le mode de fonctionnement du produit, le nom du concentrateur et le niveau des logs sont modifiables.

Paramètres	Description
mode	Mode de fonctionnement du concentrateur : • <i>factorySettings</i> : mode FACTORY SETTINGS • <i>storage</i> : mode STORAGE • <i>run</i> : mode RUN
name	Nom du concentrateur
logLevel	Niveau de log dans le journal des événements : • 0 : Erreur • 1 : Warning • 2 : Info (par défaut) • 3 : Debug



Lors d'un changement de mode de fonctionnement du produit en FACTORY SETTINGS ou STORAGE par configuration FTP, le concentrateur ne pourra repasser en mode RUN que par une intervention locale. (Voir chapitre 3.1 : « Démarrage du produit »)

Exemple :

- Par fichier JSON (à convertir au format BSON pour le concentrateur) :

```
{
  "config": {
    "mode": "run",
    "name": "WebdynEasy",
```

```

    "logLevel":2
  },
  "crc":0
}

```

4.2.1.1 Locale

L'ensemble des variables locales du concentrateur se trouve dans l'objet « local » en JSON.

Paramètres	Description
magnet	Configuration de l'action au passage de l'aimant en mode RUN : • 0 : Modem • 1 : commande Diagnostic • 2 : commande Request (par défaut) • 3 : continue MQTT (voir la note d'application spécifique) • 4 : nomad (voir la note d'application spécifique) • 5 : live diagnostic (voir la note d'application spécifique)
testCount	Nombre de séquences de commande de diagnostic d'affilée entre 1 et 30 (par défaut 1)
timeout	Temps maximum d'exécution de l'action en seconde compris entre 60 et 21600. Fonctionnel uniquement si le paramètre « testCount » vaut 1. (par défaut désactivé : 0)
server1Files	Type de fichier à envoyer sur le serveur 1 en cas de commande Diagnostic ou Request : • Bit 0 : les données • Bit 1 : la supervision • Bit 2 : Les logs
server2Files	Type de fichier à envoyer sur le serveur 2 en cas de commande Diagnostic ou Request : • Bit 0 : les données • Bit 1 : la supervision • Bit 2 : Les logs



Si le nombre de séquences de commande de diagnostic d'affilée est supérieur à 1, alors il n'y aura pas de Bip pour prévenir du résultat en fin de diagnostic.



Dans le cas où les 2 serveurs sont renseignés, si un type de fichier est déjà déposé sur le serveur 1 alors un fichier vide sera déposé sur le serveur 2. Pour une validation de l'action, il faut que l'ensemble des serveurs paramétrés se connectent correctement.

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "config":
  {
    "local":
    {
      "magnet":1,
      "testCount":1,
      "timeout":900
    },
    "crc":0
  }
}
```

Exemple (à partir de la V3.3) :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "config":
  {
    "local":
    {
      "magnet":1,
      "server1Files":6,
      "server2Files":1,
      "testCount":1,
      "timeout":900
    },
    "crc":0
  }
}
```

Dans l'exemple ci-dessus, le serveur 1 recevra les logs ainsi que la supervision et le serveur 2 recevra les données.

4.2.1.2 Sécurité

L'ensemble des variables sécurité du concentrateur se trouve dans l'objet « security » en JSON.

Paramètres	Description
crcMode	Vérification du CRC des fichiers BSON : • 0 : Aucune vérification du CRC • 1 : Vérification partielle (pas de vérification si le CRC est à 0) (par défaut)

	2 : Vérification activée du CRC
encryption	Chiffrement en AES des fichiers BSON : <i>true</i> : chiffrement des fichiers activé (par défaut à partir de la version V4.0) <i>false</i> : chiffrement des fichiers désactivé
key	Clé AES128 CBC de 16 octets (A mettre au format Base64 dans le fichier JSON) A partir de la version V4.0 une clé unique est attribuée en usine.
aesLegacy	Force l'utilisation de l'ancien format de fichier AES (IV fixe).



Si la vérification du CRC d'un fichier (cfg, cmd, ...) échoue, la lecture du fichier est interrompue et une erreur est signalée dans le fichier d'acquiescement ACK déposé dans le répertoire « /ALARM » du serveur FTP.

Chiffage en AES128 CBC :

L'ensemble des fichiers BSON peuvent être chiffrés avec un AES128 CBC. La valeur du vecteur d'initialisation (IV) pour les firmwares inférieurs à la V4.0 est fixe :

C0 50 3E CD E3 DB 6B 2E 52 F5 9B 95 B6 F1 9B 58

Pour les firmwares de version supérieure ou égale à V4.0 le vecteur d'initialisation (IV) est situé en fin de fichier après les données chiffrées. Pour respecter les bonnes pratiques de cybersécurité il faut que ce vecteur, généré de façon aléatoire, soit différent à chaque chiffrement.

Pour des raisons de compatibilité avec les anciens firmwares, il est possible de forcer l'utilisation de l'ancien format de fichier AES avec le paramètre « config.security.aesLegacy ».

La norme de padding utilisée est la suivante : « PKCS#5 padding »

En cas de chiffrement des fichiers, une extension « .aes » est rajoutée à chaque fichier BSON.

Par exemple, le fichier de configuration suivant « 123456-config.bson » devient « 123456-config.bson.aes » après activation du chiffrement des fichiers.

Exemple de conversion de clé AES :

Format	clé
Clé AES128 en hexadécimal (longueur de 16 octets)	44:00:AA:F7:83:78:04:9C:AB:13:EE:4E:35:0E:28:1B

Clé AES128 en Base64 (fichier JSON)

RACq94N4BJyrE+5ONQ4oGw==

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "config": {
    "security": {
      "crcMode": 1,
      "encryption": true,
      "key": { "$type": "00", "$binary": "RACq94N4BJyrE+5ONQ4oGw==" }
    }
  },
  "crc": 0
}
```

4.2.2 Radio WM-Bus

L'ensemble des variables radio WM-Bus du concentrateur se trouve dans l'objet « radio » en JSON.

Paramètres	Description
mode	Mode du WM-Bus utilisé : • 0 : pour S1 (868MHz) • 1 : pour T1 (868MHz) • 2 : pour T1 + C1 (868MHz, par défaut) • 3 : pour T1 (433MHz, par défaut)
duration	Durée de la fenêtre d'écoute en WM-Bus en secondes (1 à 21600) Par défaut : 60
manufFilter	Liste des codes constructeurs (2 octets : M-field) autorisés au format binaire (type 0x00 en JSON) (maximum 8 codes) https://www.dlms.com/flag-id/flag-id-list
mediumFilter	Liste des codes medium (octet 1 du champ A-field) des capteurs ou compteurs WM-BUS autorisés au format binaire (type 0x00 en JSON) (maximum 8 codes)
ciFilter	Liste de champ CI des capteurs ou compteurs autorisés au format binaire (type 0x00 en JSON) (maximum 8 codes) Se référer au manuel du fabricant du compteur. Cas d'usage typique : Permet de récupérer uniquement les trames courtes émises.

BFormatLFieldAdaptation	Modification du champ L de la trame WM-Bus pour les trames au format B (Voir chapitre 4.2.2.2 : « Champ L pour les trames format B ») : • <i>true</i> : Adaptation du champ L du format B au format A (par défaut). • <i>false</i> : Champ L du format B n'est pas modifié.
longHeader	Utilisation des informations du compteur présentes dans l'entête long dans une trame longue (se référer au « long header » de la spécification « Open Metering system ») : • <i>true</i> : informations utilisées dans l'entête long (par défaut). • <i>false</i> : informations utilisées dans l'entête court
skipVersionField	En cas de Whitelist, permet d'ignorer la version du compteur présent dans l'entête : • <i>true</i> : ignore la version • <i>false</i> : tient compte de la version (par défaut)
skipMediumField	En cas de Whitelist, permet d'ignorer le type (« medium ») du compteur présent dans l'entête : • <i>true</i> : ignore le type • <i>false</i> : tient compte du type (par défaut)
oneFramePerMeter	Permet de n'enregistrer qu'une seule trame de longueur donnée par compteur dans un même fenêtre d'écoute. • <i>true</i> : fonction activée (par défaut) • <i>false</i> :fonction désactivée
isManufAllowList	Type de filtre constructeur : • <i>true</i> : liste blanche « whiteList » (par défaut) • <i>false</i> : liste noire « blackList »
isMediumAllowList	Type de filtre medium: • <i>true</i> : liste blanche « whiteList » (par défaut) • <i>false</i> : liste noire « blackList »
isCiAllowList	Type de filtre CI: • <i>true</i> : liste blanche « whiteList » (par défaut) • <i>false</i> : liste noire « blackList »



Si les paramètres VersionField et/ou MediumField de n'importe quel endpoint WM-Bus sont modifiés, il est essentiel de mettre à jour le fichier de liste blanche dans le concentrateur sauf si vous utilisez les paramètres "skipVersionField" et/ou "skipMediumField"

Exemple :

- Par fichier JSON (à convertir au format BSON pour le concentrateur) :

```
{
  "config": {
    "radio": {
      "mode": 2,
      "duration": 60,
      "manufFilter": {"$type": "00", "$binary": "TDARpQ=="},
      "ciFilter": {"$type": "00", "$binary": "AG=="},
      "mediumFilter": {"$type": "00", "$binary": "BwE="},
      "BFormatLFieldAdaptation": true,
      "longHeader": true,
      "skipVersionField": false,
      "skipMediumField": false,
      "oneFramePerMeter": true,
      "isManufAllowList": true,
      "isMediumAllowList": true,
      "isCiAllowList": true,
    },
    "crc": 0
  }
}
```

Le concentrateur possède si besoin d'un multi mode d'écoute qui permet de récupérer les données WM-Bus des capteurs dans un mode puis de récupérer ensuite les données WM-Bus d'autres capteurs qui se trouvent dans un autre mode.

Dans le cas d'un multi mode d'écoute, les paramètres « *mode* » et « *duration* » sont des tableaux. Le premier élément des tableaux correspond au premier mode déclenché par le concentrateur lors de la récupération des données WM-Bus des capteurs, le second élément des tableaux correspond au deuxième mode utilisé lors de la récupération des données.



En cas de multi mode d'écoute, la liste des codes constructeurs « *manufFilter* », la liste des codes medium « *mediumFilter* » et la liste blanche « *whiteList* » s'appliquent à l'ensemble des modes définis.

Exemple :

- Par fichier JSON (à convertir au format BSON pour le concentrateur) :

```
{
  "config": {
    "radio": {
      "mode": [2, 0],
      "duration": [120, 180],
      "manufFilter": {"$type": "00", "$binary": "TDARpQ=="},
      "mediumFilter": {"$type": "00", "$binary": "BwE="}
    },
    "crc": 0
  }
}
```

Explication :

La récupération des données commencera par le mode T1+C1 pendant 120 secondes, puis enchainera par le mode S1 pendant 180 secondes.

4.2.2.1 Liste blanche « whiteList »

Il est possible d'activer la gestion des acquisitions des capteurs ou compteurs en fonction des identifiants WM-Bus renseignés dans la liste blanche « whiteList ». Lors d'une fenêtre d'écoute, celle-ci pourra se fermer avant la durée programmée si les données de l'ensemble des équipements de la liste blanche ont été enregistrées.

La liste blanche est un fichier BSON que l'on dépose comme un fichier de configuration pour le concentrateur. La liste blanche accepte jusqu'à 2000 identifiants WM-Bus.

Le fichier de la liste blanche du concentrateur WebdynEasy est au format BSON et son format est le suivant :

« <uid>-wlFilter.bson »



Si les paramètres « *skipVersionField* » et/ou « *skipMediumField* » de la partie radio WM-Bus sont modifiés, il faut impérativement réinjecter le fichier de la liste blanche « <uid>-wlFilter.bson » au concentrateur.

Le tableau de la liste blanche du concentrateur se trouve dans l'objet « *wlFilter* » puis chaque équipement se trouve dans l'objet « *id* » stocké au format binaire (type 0x00 en JSON) en JSON. L'équipement contient 8 octets permettant l'identification du capteur ou du compteur WM-BUS et se compose ainsi :

M-field	A-field
2 octets	6 octets

Pour supprimer les équipements du concentrateur, on peut soit :

- Envoyer une commande d'effacement de la liste blanche « whitelisterase » (Voir chapitre 5.6.6 : « Commande « *whiteListErase* » »),
- Envoyer un fichier de configuration avec une valeur « null » pour l'objet « *wlFilter* ».



En cas de multi mode d'écoute, la liste blanche « whiteList » s'applique à l'ensemble des modes définis.

Exemple d'un fichier de liste blanche converti en JSON :

```
{
  "wlFilter":
  [
    {"id":{"$binary":"FIZESRQABBE=","$type":"00"}},
    {"id":{"$binary":"FIYlwhQABBE=","$type":"00"}},
    {"id":{"$binary":"FIaachQADw8=","$type":"00"}},
    {"id":{"$binary":"MEzOXeAgmAE=","$type":"00"}},
    {"id":{"$binary":"MEw5KpkgwAE=","$type":"00"}},
    {"id":{"$binary":"MEw/2CMhDAQ=","$type":"00"}},
    {"id":{"$binary":"MEzBHKogzAE=","$type":"00"}}
  ],
  "crc":0
}
```

Exemple d'un fichier liste blanche pour effacement converti en JSON :

```
{
  "wlFilter":[null],
  "crc":0
}
```

4.2.2.2 Champ L pour les trames format B

Dans la norme WM Bus EN13757-4, il y a deux types de formats de trames possibles pour le mode C1 : A et B.

- Format A : le champ L (premier octet de la trame) contient le nombre d'octets de la trame sans les CRC
- Format B : le champ L (premier octet de la trame) contient le nombre d'octets de la trame avec les CRC (2 octets de CRC si la longueur de trame est inférieure à 128 octets, 4 sinon).

Dans les trames WM-Bus enregistrées par la passerelle, les CRC ne sont pas présents. Suivant le format de trame, le traitement de la trame n'est pas le même et il faut donc connaître le format utilisé par le compteur.

Par défaut la passerelle modifie le champ L des trames au format B pour qu'il soit le même que pour une trame au format A, le traitement des trames devient alors identique, quel que soit le format.

Il est cependant possible de désactiver ce comportement en appliquant la valeur « false » au paramètre « BFormatLFieldAdaptation ».

4.2.3 Connectivité du concentrateur

L'ensemble des variables de connectivité du concentrateur se trouve dans l'objet « remote » en JSON. Elles sont séparées en 3 familles qui sont :

- Modem
- FTP(S),http(S)
- NTP

4.2.3.1 Modem

L'ensemble des variables modem du concentrateur se trouve dans l'objet « modem » en JSON.

Paramètres	Description
mode	Choix du type de connexion : • <i>2G</i> : Force le modem en 2G • <i>LTEM</i> : Force le modem en LTE-M • <i>NB-IoT</i> : Force le modem en NB-IoT • <i>auto</i> : Le modem gère automatiquement le réseau (par défaut)
scanseq	Tableau de préférence de la séquence de recherche. Fonctionnel uniquement en mode « auto ». Les 3 choix possibles pour l'ordre de préférence sont : • <i>2G</i> : Autorise le modem en 2G • <i>LTEM</i> : Autorise le modem en LTE-M • <i>NB-IoT</i> : Autorise le modem en NB-IoT
band	Liste des bandes autorisées pour la connexion modem en NB-IoT (valeur numérique de la bande). Les bandes disponibles sont : 1,2,3,4,5,8,12,13,18,19,20,25,28,66,85
deregisterOnLocalAction	Désenregistrement du modem sur le réseau opérateur à chaque déclenchement d'action par l'aimant : • <i>true</i> : Désenregistrement activé • <i>false</i> : Désenregistrement désactivé (par défaut)
cpin	Code PIN de la carte SIM (8 caractères max) <i>null</i> : désactive le code PIN (par défaut)
operator	Code opérateur numérique (optionnel) Exemple: 20801
apn	Identifiant du point d'accès du réseau (APN) (32 caractères max) <i>null</i> : aucun APN (par défaut)

user	Identifiant pour la connexion PPP (32 caractères max) <i>null</i> : aucun identifiant (par défaut)
pass	Mot de passe pour la connexion PPP (32 caractères max) <i>null</i> : aucun mot de passe (par défaut)
timeout	Temps maximum pour accrocher un réseau en seconde (entre 60 et 1800) 300 (par défaut)
randomDelay	Délai aléatoire avant le réveil en minutes (entre 0 et 60) 0 : aucun délai (par défaut)

Si aucun paramètre « band » n'est renseigné, le modem scanne toutes les bandes NB-IoT disponibles. Afin d'optimiser la recherche du réseau en NB-IoT, il est fortement conseillé de renseigner les bandes autorisées par l'opérateur et le pays. Veuillez trouver ci-dessous un tableau des bandes déployées dans le monde à titre informatif :

Bandes	U.S.	Chine	Moyen-Orient	Japon	Corée	Europe	Australie
1		✓		✓			
2	✓						
3		✓	✓		✓	✓	✓
5		✓			✓		
8		✓	✓	✓		✓	
12	✓						
13	✓						
18				✓			
19				✓			
20						✓	

26		✓					
28			✓				✓

La variable « randomDelay » permet d'étaler aléatoirement les connexions FTP(S)/HTTP(S) de tous les concentrateurs qui ont la même configuration.



Quand le mode du modem est en mode auto, le modem se connecte par défaut en LTE-M puis si celui-ci est indisponible, il se replie sur le 2G.



Quand le mode du modem est en mode auto et que le champ « operator » est renseigné, le modem se connecte par défaut en LTE-M à l'opérateur sélectionné puis si celui-ci est indisponible, il se replie sur le 2G avec une recherche automatique d'opérateur.

Exemple :

- Par fichier JSON (à convertir au format BSON pour le concentrateur) :

```
{
  "config":
  {
    "remote":
    {
      "modem":
      {
        "mode": "auto",
        "scanseq": [
          "LTE-M",
          "2G",
          "NB-IoT"
        ],
        "band": [
          3,
          8,
          20
        ],
        "operator": 20801,
        "deregisterOnLocalAction": false,
        "cpin": 1234,
        "apn": null,
        "user": null,
        "pass": null,
        "timeout": 240,
        "randomDelay": 0
      }
    }
  },
  "crc": 0
}
```

4.2.3.2 Serveurs (FTP/FTPS/HTTP/HTTPS)

L'ensemble des variables du serveur FTP/FTPS/HTTP du concentrateur se trouve dans l'objet « ftp » pour le serveur 1 et dans l'objet « server2 » à partir de V3.3 en JSON.

Paramètres	Description
mode	Choix du protocole FTP : • 0 : FTP • 1 : FTPS (FTP over TLS) (par défaut à partir de la version V4.0) • 2 : FTPS + certificats • 3 : HTTP • 4 : HTTPS (HTTP over TLS) • 5 : HTTPS+ certificats
addr	Adresse IP ou nom du serveur FTP(S)/HTTP(S) distant (128 caractères max) (Port par défaut en FTP : 21 et port par défaut en HTTP : 80) Possibilité de modifier le port du FTP(S)/HTTP(S) en rajoutant « : » puis le numéro de port (entre 1 et 65535)
user	Nom d'utilisateur du compte FTP(S)/HTTP(S) (64 caractères max)
pass	Mot de passe du compte FTP(S)/HTTP(S) (64 caractères max)
dir	Répertoire racine sur le serveur FTP(S)/HTTP(S) (64 caractères max) <i>null</i> : répertoire racine du compte FTP(S)
cacert	Certificat qui permet d'authentifier le serveur (FTP(S)/HTTP(S)) renseigné.
clientcert	Certificat spécifique au concentrateur utilisé pour la connexion.
clientley	Clé privée spécifique au concentrateur utilisé pour la connexion.
checkBcast	Permet d'activer la fonction broadcast (voir chapitre 5.1.1.4 : « FTP(S) Broadcast »).



Les champs « user », « pass » et « dir » ne doivent pas contenir le caractère « " ».



L'utilisation d'un protocole non sécurisé est fortement déconseillée.

Exemple :

- Par fichier JSON (à convertir au format BSON pour le concentrateur) :

```
{
  "config":
  {
    "remote":
    {
      "ftp":
      {
        "mode":0,
        "addr":"ftp.webdyn.com:60",
        "user":"webdyn",
        "pass":"1234",
        "dir":"/site1234"
      }
    },
    "crc":0
  }
}
```

Exemple à partir de la V3.3 :

- Par fichier JSON (à convertir au format BSON pour le concentrateur) :

```
{
  "config":
  {
    "remote":
    {
      "ftp":
      {
        "mode":0,
        "addr":"ftp.webdyn.com:60",
        "user":"webdyn",
        "pass":"1234",
        "dir":"/site1234"
      },
      "server2":
      {
        "mode":3,
        "addr":"web.webdyn.com:80",
        "user":"webdynweb",
        "pass":"123456",
        "dir":"/site1234"
      }
    },
    "crc":0
  }
}
```

4.2.3.3 NTP

Le concentrateur synchronise régulièrement son heure par rapport à un serveur NTP. La WebdynEasy utilise la date et l'heure en UTC+0.

Paramètres	Description
------------	-------------

ntp	Adresse IP ou nom du serveur NTP (64 caractères max) (Adresse par défaut : « pool.ntp.org » et port par défaut : 123) Possibilité de modifier le port du NTP en rajoutant « : » puis le numéro de port (entre 1 et 65535)
-----	---



L'enregistrement des données et la génération des noms de fichiers se font par rapport à la date et l'heure récupérées sur le serveur NTP en UTC+0. Si vous souhaitez modifier le fuseau horaire, il faudra réaliser un traitement par vos soins sur les fichiers déposés sur le serveur FTP.



Par défaut, le concentrateur utilise le serveur NTP gratuit « pool.ntp.org », ce serveur ne garantit pas l'exactitude de la synchronisation horaire et sa robustesse. Il est fortement conseillé d'utiliser un serveur NTP dédié. Rapprochez-vous d'un fournisseur de serveur NTP.

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "config":
  {
    "remote":
    {
      "ntp": "pool.ntp.org"
    }
  },
  "crc": 0
}
```

4.2.4 Alarmes

L'ensemble des variables alarmes du concentrateur se trouve dans l'objet « alarms » en JSON.

Paramètres	Description
oneAlarmPerDay	Une seule transmission d'une alarme par modem par jour : • <i>true</i> : envoie au maximum une transmission due à une alarme par jour (par défaut) • <i>false</i> : transmission de toutes les alarmes dans une journée.
temperature	Température maximum en degré (°C) avant déclenchement d'une alarme (entre 10 et 50) <i>null</i> ou 0: désactive les alarmes température. (par défaut)

timeGap	Surveillance de la dérive horloge du concentrateur par rapport à l'heure récupérée par NTP en seconde avant déclenchement d'une alarme (entre 2 et 3600) <i>null</i> ou 0: désactive les alarmes dérive horloge. (par défaut)
battery	Surveillance du niveau pile restant en pourcentage (%) avant déclenchement d'une alarme (entre 10 et 99) <i>null</i> ou 0: désactive les alarmes pile. (par défaut)

Les acquisitions de température et de pile sont réalisées à chaque déclenchement du monitoring et au déclenchement du Schedule radio ou du Schedule FTP (Voir chapitre 4.2.5 : « Schedule (planification) et Monitoring »).

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "config":
  {
    "alarms":
    {
      "oneAlarmPerDay":true,
      "temperature":null,
      "timeGap":null,
      "battery":10
    }
  },
  "crc":0
}
```

4.2.5 Schedule (planification) et Monitoring

Le concentrateur possède :

- **Un Schedule Radio** : qui permet de récupérer les données des compteurs et capteurs WM-Bus,
- **Un Schedule FTP** : qui permet de déposer les fichiers et de synchroniser l'horloge du produit,
- **Un Monitoring** : qui permet la surveillance de la pile et de la température du produit.

4.2.5.1 Schedules

Les Schedules sont des déclencheurs de minuteurs qui permettent d'exécuter une tâche de manière planifiée. Chaque Schedule peut gérer jusqu'à 8 déclencheurs de minuteurs. En JSON, les déclencheurs de minuteurs sont appelés « cron ».

Un déclencheur de minuteurs « cron » se décompose ainsi :

mm hh jj MM JJ

Avec :

- mm : représente les minutes (de 0 à 59)

- hh : représente l'heure (de 0 à 23)
- jj : représente le numéro du jour du mois (de 1 à 31 ou « L » pour le dernier jour du mois)
- MM : représente le numéro du mois (de 1 à 12)
- JJ : représente le numéro du jour dans la semaine :
 - 0 = dimanche
 - 1 = lundi
 - 2 = mardi
 - ...
 - 6 = samedi
- A partir de la version V4.0 il est possible de conditionner le déclenchement d'un Scheule en fonction de la source d'alimentation.
 Si la première lettre de la ligne est « e » le schedule ne se déclenchera uniquement si le produit est alimenté par l'alimentation extérieure.
 Si la première lettre de la ligne est « b » le schedule ne se déclenchera uniquement si le produit est alimenté par la pile lithium interne.

Chaque champ peut être associé aux types de valeurs suivants :

Type	Exemple	En cas de déclenchement
Une valeur spécifique	"5 * * * *"	à hh:05 où hh correspond à toutes les heures (une fois par heure)
Toutes les valeurs (*)	"0 * * * 1"	à hh:00 chaque lundi, où hh correspond à toutes les heures (24 fois le lundi)
Une plage (opérateur -)	"30 11-13 * * *"	à 11:30, 12:30 et 13:30 tous les jours (3 fois par jour)
Un ensemble de valeurs (opérateur ,)	"5,12,47 * * * * *"	à hh:05, hh:12 et hh:47 où hh correspond à toutes les heures (3 fois par heure)
Une valeur d'intervalle (opérateur /)	"0 */2 * * *"	à 00:00, 02:00, 04:00 et ainsi de suite jusqu'à 24:00 (12 fois par jour)
« L » : Dernier jour du mois	"0 12 L * *"	A 12 :00 le dernier jour du mois
Sur alimentation externe	"e0 */2 * * *"	Toutes les deux heures lorsque la passerelle est alimentée par une alimentation externe



Si les deux Schedules sont déclenchés en même temps, le Schedule Radio sera toujours exécuté en priorité par rapport au Schedule FTP.



Si deux déclencheurs de minuteurs sont déclenchés en même temps dans un même Schedule, dans ce cas, seul le déclencheur de minuteurs qui sera en premier dans le fichier sera exécuté.

4.2.5.1.1 Schedule Radio

Le schedule Radio permet de récupérer les données des compteurs et capteurs WM-Bus.

L'ensemble des déclencheurs de minuteurs du Schedule Radio se trouve dans l'objet « scheduleRadio » en JSON. Le nombre maximum de déclencheurs de minuteurs est de 8.

Paramètres	Description
cron	Déclencheur du minuteur : <i>mm hh jj MM JJ</i>
data	Durée de la fenêtre d'écoute Radio en secondes (entre 30 et 21600)



Si la fenêtre d'écoute « data » n'est pas renseignée alors la durée de la fenêtre d'écoute sera celle définie dans la configuration radio « config→radio→duration » (Voir chapitre 4.2.2 : « Radio WM-Bus »)

Exemple :

- Par fichier JSON (à convertir au format BSON pour le concentrateur) :

```
{
  "config":
  {
    "scheduleRadio": [
      { "cron": "*/30 * * * *", "data": 30 },
      { "cron": "15 23 * * *", "data": 120 }
    ],
    "crc": 0
  }
}
```

Explication :

Dans l'exemple ci-dessus, nous avons une fenêtre d'écoute de 30 secondes toutes les 30 minutes et une fenêtre de 120 secondes tous les jours à 23h15.

Dans le cas d'un multi mode d'écoute, le paramètre « *data* » est un tableau. Le premier élément du tableau correspond au premier mode déclenché par le concentrateur lors de la récupération des données WM-Bus des capteurs, le second élément des tableaux correspond au deuxième mode utilisé lors de la récupération des données. (Voir chapitre 4.2.2 : « *Radio WM-Bus* » pour la configuration du multi mode)

Exemple d'un multi mode d'écoute :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```

• {
•   "config":
•   {
•       "scheduleRadio": [
•           { "cron": "* / 30 * * * * ", "data": [30, 60] },
•           { "cron": "15 23 * * * " }
•       ]
•   },
•   "crc": 0
• }
```

Explication :

Dans l'exemple ci-dessus, nous avons toutes les 30 minutes une fenêtre d'écoute de 30 secondes sur le premier mode configuré suivi d'une seconde fenêtre d'écoute de 60 secondes sur le second mode configuré. Tous les jours à 23h15, nous avons une première fenêtre d'écoute selon la durée définie dans le paramètre config→radio→duration[1er mode], suivi d'une deuxième fenêtre d'écoute selon la durée définie dans le paramètre config→radio→duration[2ème mode].

4.2.5.1.2 Schedule serveur (FTP(S), HTTP(S))

Le schedule FTP permet de déposer les fichiers sur le serveur (FTP(S), HTTP(S)) et de synchroniser l'horloge du produit. Depuis la version 3.3, il permet également de déposer les données sur un 2^{ème} serveur (FTP(S), HTTP(S)). Par contre, il est possible d'envoyer uniquement les données WM-Bus, la supervision et les logs vers le serveur 2. Si un type de fichier (données ou logs) est déjà déposé sur le serveur 1 alors un fichier vide sera déposé sur le serveur 2.

L'ensemble des déclencheurs de minuteurs du Schedule FTP se trouve dans l'objet « scheduleFTP » en JSON. Le nombre maximum de déclencheurs de minuteurs est de 8.

Paramètres	Description
cron	Déclencheur du minuteur : <i>mm hh jj MM JJ</i>
data	Type de fichier à envoyer : • Bit 0 : données pour le serveur 1 (1=activé, 0=désactivé) • Bit 1 : supervision pour le serveur 1 (1=activé, 0=désactivé) • Bit 2 : log pour le serveur 1 (1=activé, 0=désactivé) • Bit 3 : non utilisé

- Bit 4 : données pour le serveur 2 (1=activé, 0=désactivé)
- Bit 5 : supervision pour le serveur 2 (1=activé, 0=désactivé)
- Bit 6 : log pour le serveur 2 (1=activé, 0=désactivé)
- Bit 7 : non utilisé



Si la donnée « data » est non valide ou absente, la passerelle enverra par défaut un fichier de données.

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "config":
  {
    "scheduleFTP":[
      {"cron":"0 0 * * * ","data":7},
      {"cron":"0 * * * * ","data":1}
    ],
    "crc":0
  }
}
```

Explication :

Dans l'exemple ci-dessus, nous avons l'envoi des données toutes les heures et l'envoi des fichiers de supervision et log à minuit tous les jours.

Exemple (à partir de la version 3.3) :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "config":
  {
    "scheduleFTP":[
      {"cron":"0 0 * * * ","data":64},
      {"cron":"0 * * * * ","data":33}
    ],
    "crc":0
  }
}
```

Explication :

Dans l'exemple ci-dessus, nous avons l'envoi des données sur le serveur 1 avec envoi de la supervision sur le serveur 2 toutes les heures et l'envoi des fichiers de log sur le serveur 1 à minuit tous les jours.

4.2.5.2 Monitoring (surveillance du produit)

Le monitoring est un simple minuteur qui se déclenche sur un intervalle fixe et défini en minutes.

Le concentrateur intègre une gestion de surveillance du niveau de pile et de température du produit, mais déclenche également l'acquisition de données pour les statistiques qui seront enregistrées dans les fichiers de supervision (Voir chapitre 5.7 : « La supervision »).

Paramètres	Description
monitoringPeriod	Période de monitoring du concentrateur en minutes (entre 15 et 1440) (60 par défaut) null ou 0: désactive le monitoring



Dans le cas où le monitoring est désactivé, cela affecte grandement la surveillance des alarmes de température et de pile, car les acquisitions des données de température et de pile seront uniquement prises au moment d'un déclenchement de Schedule radio ou FTP.

Exemple :

- Par fichier JSON (à convertir au format BSON pour le concentrateur) :

```
{
  "config":
  {
    "monitoringPeriod":60
  },
  "crc":0
}
```

5 Exploitation

5.1 Le serveur distant

Le concentrateur communique avec un ou deux serveurs distants par le protocole FTP. Ce serveur permet de gérer le concentrateur à distance.

Le serveur distant à plusieurs rôles :

- **Remonter les données et alarmes collectées localement par le concentrateur :**
À chaque connexion au serveur, que ce soit suite à une demande manuelle, le déclenchement d'une alarme ou le déclenchement du Schedule de connexion, le concentrateur profite de la connexion au serveur pour déposer ses données mémorisées.
- **Sauvegarder une copie de la configuration :**
Une sauvegarde de la configuration du concentrateur est disponible dans le répertoire « /CONFIG » du serveur. Chaque fois que la configuration du concentrateur est modifiée (localement ou à distance), le concentrateur envoie dans ce répertoire une copie de sa configuration.
- **Reconfigurer le concentrateur ou déclencher des actions sur ce dernier :**
Les fichiers de configuration ou de commande doivent être déposés sur le serveur dans un répertoire INBOX associé au concentrateur.
- **Superviser le concentrateur et aider au diagnostic :**
Le concentrateur peut déposer des fichiers de statut du concentrateur, ainsi que des logs pour permettre le diagnostic.



En cas de présence de deux serveurs distants dans la configuration, seul le serveur 1 est utilisé pour la sauvegarde de la configuration et seul le répertoire INBOX du serveur 1 est utilisable en cas de dépose de fichiers de commande ou de configuration.

5.1.1 Le serveur FTP(S)

5.1.1.1 Paramétrage

Le serveur FTP(S) est défini par les paramètres suivants :

- **Une adresse :** Cette adresse peut être une adresse IP ou un nom de domaine.
Il est possible de modifier le port de connexion FTP(S) (par défaut 21) en rajoutant à la fin de l'adresse, le port à utiliser après le caractère « : ». Le format à utiliser est le suivant : « adresse:port » (par exemple « 192.168.1.2:8021 »).
- **Un identifiant et un mot de passe :** Ces paramètres permettent de définir le compte FTP(S) à utiliser.
- **Un répertoire racine :** Le répertoire racine peut être la racine du serveur FTP « / » ou une suite de sous-répertoires (par exemple « /WebdynEasy/123456/ »).

Vous pouvez configurer votre concentrateur à distance depuis votre serveur FTP. Ceci n'est possible que si votre concentrateur WebdynEasy est correctement configuré pour déposer et synchroniser sa configuration sur un serveur FTP.

A partir de la version V3.3, il est possible de renseigner un deuxième serveur dans la configuration. L'intérêt de cette fonctionnalité est de permettre de consacrer le serveur 1 pour la gestion du concentrateur et le serveur 2 pour le traitement des données.

5.1.1.2 Arborescence du serveur

Le serveur FTP(S) doit disposer d'une arborescence spécifique au produit WebdynEasy.

Sous le répertoire racine, le serveur FTP(S) doit contenir les répertoires suivants :

Nom	Droits	Description
/CONFIG	Écriture	Contiens l'image de la configuration. La configuration déposée par le concentrateur respecte le format suivant : « <uid>-<timestamp>-config.bson »
/DATA	Écriture	Contiens les données collectées. Le nom du fichier de données respecte le format suivant : « <uid>-<timestamp>-data.bson »
/ALARM	Écriture	Contiens les alarmes et les acquittements (ACK) Le nom du fichier d'alarme respecte le format suivant : « <uid>-<timestamp>-alarm.bson » Le nom du fichier d'acquiessement (ACK) respecte le format suivant : « <uid>-<timestamp>-ack.bson »
/SUPERVISION	Écriture	Contiens les fichiers de supervision, ainsi que les logs. Le nom du fichier de supervision respecte le format suivant : « <uid>-<timestamp>-supervision.bson » Le nom du fichier de log respecte le format suivant : « <uid>-<timestamp>-log.bson »
/INBOX/<uid>	Lecture/Ecriture	Boîte aux lettres pour envoyer une configuration ou une commande au concentrateur. La configuration destinée au concentrateur respecte le format suivant : « <uid>-cfg.bson » La commande destinée au concentrateur respecte le format suivant : « <uid>-cmd.bson »

/BIN	Lecture	Contiens les fichiers de mise à jour
------	---------	--------------------------------------

Avec :

- `<uid>` : Identifiant du concentrateur
- `<timestamp>` : Nombre de secondes écoulées depuis le 1^{er} janvier 1970 à minuit UTC précise.

Les droits d'accès minimums aux différents répertoires doivent être définis comme précisés dans le tableau ci-dessus.

Lors de la première connexion du concentrateur si les répertoires sur le serveur FTP(S) n'existent pas alors ils seront créés par le concentrateur.



Si les répertoires ne sont pas créés lors de la première connexion du concentrateur ou que les droits sont insuffisants empêchant le dépôt ou la récupération des fichiers, veuillez contacter l'administrateur du serveur.

5.1.1.3 Fonctionnement

Le concentrateur dépose toujours les fichiers sur le serveur FTP(S) en suivant un processus en 2 étapes :

1. Au début du transfert le fichier à une extension supplémentaire « .tmp ».
2. Quand le fichier a fini d'être transféré, il est renommé en supprimant l'extension « .tmp ».

Ce processus permet au serveur distant de distinguer facilement les fichiers en cours de téléchargement des fichiers complètement téléchargés.

5.1.1.4 FTP(S) Broadcast

En fonctionnement normal, la passerelle vérifie la présence de fichiers de commande ou de configuration dans son propre répertoire situé dans le répertoire INBOX du serveur FTP(S). Cette fonctionnalité permet à la passerelle de vérifier également la présence de fichiers de configuration ou de commande dans un répertoire commun à toutes les passerelles. Cela permet, par exemple, en y déposant un fichier de commande de mise à jour du firmware, de mettre à jour toutes les passerelles qui utilisent ce même serveur.

Cette fonctionnalité n'est pas activée par défaut il faut explicitement mettre le paramètre « config/remote/ftp/checkBcast » à « true ».

Le fichier de commande doit être nommé comme ceci (idem pour un fichier de configuration) :

FFFFFF-`<num>`-cmd.bson

Avec:

- `<num>`: numéro de séquence permettant de différencier les fichiers (timestamp par exemple).

Remarques

- Contrairement au fonctionnement normal, le fichier une fois traité n'est pas effacé. Afin de ne pas utiliser le même fichier à chaque connexion, les <num> des quatre derniers fichiers traités sont enregistrés dans la mémoire de la passerelle.
- Le répertoire « FFFFFF » doit être créé sur le serveur avant la première connexion à la passerelle.
- Contrairement aux répertoires INBOX normaux, si un fichier ne contient pas de <num>, il sera ignoré.
- Il n'y a pas de gestion particulière pour la clé de chiffrement des fichiers donc lorsque le chiffrement AES des fichiers est activé il faut que la clé soit commune à toutes les passerelles utilisant le serveur.

5.1.1.4.1 Fonctionnement

Si « config/remote/ftp/checkBcast » est défini à « true », chaque fois que la passerelle accédera au serveur FTP(S), elle vérifiera le contenu du répertoire de diffusion ("FFFFF") dans "INBOX", puis vérifiera son propre répertoire.

5.1.1.5 Format des fichiers

Les fichiers échangés avec le serveur distant sont au format BSON qui est une version binaire du JSON. Le format décrit dans le document est au format JSON. Pour transformer le format JSON en BSON ou vice versa, il vous faudra utiliser une bibliothèque mise à disposition sur le site officiel : <http://bsonspec.org/implementations.html>

Afin d'éviter l'altération de fichier lors des échanges, un CRC32 est intégré dans chaque fichier. Le champ « crc » doit toujours être le dernier champ du fichier JSON et BSON.

Exemple de fichier de configuration en JSON :

```
{
  "config":{
    "remote":{
      "ntp":["http.google.com",""]
    }
  },
  "crc":0
}
```

Exemple de fichier de configuration en BSON (converti par rapport au JSON) :

```
50 00 00 00 03 43 6F 6E 66 69 67 00 3A 00 00 00
03 52 65 6D 6F 74 65 00 2D 00 00 00 04 4E 54 50
00 23 00 00 00 02 30 00 0F 00 00 00 6E 74 70 2E
67 6F 6F 67 6C 65 2E 63 6F 6D 00 02 31 00 01 00
00 00 00 00 00 00 10 43 52 43 00 00 00 00 00
```

Le CRC est alors calculé sur la totalité du fichier puis le résultat du CRC32 en Little Endian écrase les 4 octets à 0 du CRC. Dans l'exemple, le CRC32 du fichier correspondant est 0x2A0C7BA3.

Exemple du fichier BSON avec le CRC32 mis à jour :

```
50 00 00 00 03 43 6F 6E 66 69 67 00 3A 00 00 00
03 52 65 6D 6F 74 65 00 2D 00 00 00 04 4E 54 50
00 23 00 00 00 02 30 00 0F 00 00 00 6E 74 70 2E
67 6F 6F 67 6C 65 2E 63 6F 6D 00 02 31 00 01 00
00 00 00 00 00 00 10 43 52 43 00 A3 7B 0C 2A 00
```

5.2 La configuration

Le concentrateur permet de faire des configurations par un fichier de configuration.



En cas de présence de deux serveurs distants dans la configuration, la sauvegarde de la configuration se fait exclusivement sur le serveur 1 et le dépôt d'une nouvelle configuration se fait uniquement par le répertoire INBOX du serveur 1.

Le fichier de configuration du concentrateur WebdynEasy est au format BSON et le format nom de fichier est le suivant :

« <uid>-cfg.bson »

Une sauvegarde de la configuration courante est disponible sur le serveur distant dans le répertoire « CONFIG/ ». Que ce soit après une modification locale ou distante de la configuration, le concentrateur envoie sur le serveur distant sa nouvelle configuration. Le fichier de configuration sauvegardé du concentrateur est au format BSON et le format du nom de fichier est le suivant :

« <uid>-<timestamp>-config.bson »

Avec :

- <uid> : Identifiant du concentrateur
- <timestamp> : Nombre de secondes écoulées depuis le 1^{er} janvier 1970 à minuit UTC précise.

Exemple :

123456-1591083697-config.bson

L'envoi d'un fichier de configuration peut être réalisé localement via USB, ou à distance via le répertoire FTP(S) « INBOX ».

- **Localement :**

Connecter l'USB au concentrateur. Puis déposer le fichier de configuration (« <uid>-cfg.bson »).

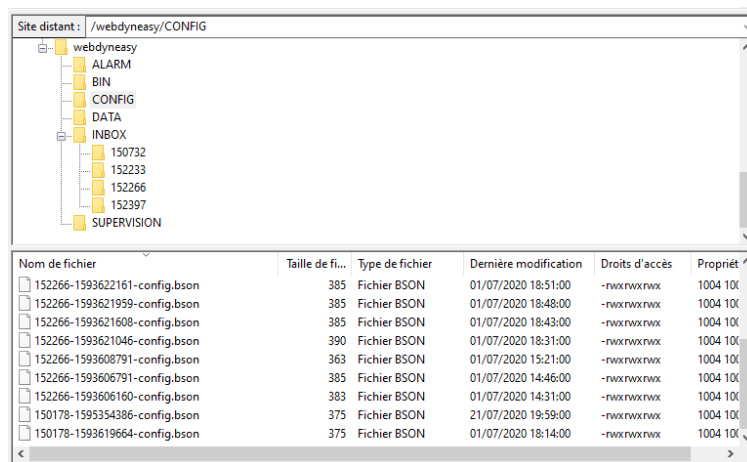
Suivre les étapes détaillées dans le chapitre 2.4.5 : « Interface USB ».

- **À distance :**

Déposer le fichier de configuration (« <uid>-cfg.bson ») dans le répertoire FTP(S) « INBOX » de votre concentrateur (« /INBOX/<uid>/ », avec <uid> l'identifiant de votre concentrateur). Lors de la prochaine connexion au serveur FTP(S)

, le concentrateur réalise 4 étapes :

1. Télécharger le fichier de configuration disponible sur le serveur,
2. Supprimer le fichier de configuration du serveur,
3. Appliquer la nouvelle configuration,
4. Déposer le fichier d'acquittement dans le répertoire « ALARM ».



Nom de fichier	Taille de fi...	Type de fichier	Dernière modification	Droits d'accès	Propriété
152266-1593622161-config.bson	385	Fichier BSON	01/07/2020 18:51:00	-rwxrwxrwx	1004 100
152266-1593621959-config.bson	385	Fichier BSON	01/07/2020 18:48:00	-rwxrwxrwx	1004 100
152266-1593621608-config.bson	385	Fichier BSON	01/07/2020 18:43:00	-rwxrwxrwx	1004 100
152266-1593621046-config.bson	390	Fichier BSON	01/07/2020 18:31:00	-rwxrwxrwx	1004 100
152266-1593608791-config.bson	363	Fichier BSON	01/07/2020 15:21:00	-rwxrwxrwx	1004 100
152266-1593606791-config.bson	385	Fichier BSON	01/07/2020 14:46:00	-rwxrwxrwx	1004 100
152266-1593606160-config.bson	383	Fichier BSON	01/07/2020 14:31:00	-rwxrwxrwx	1004 100
150178-1595354386-config.bson	375	Fichier BSON	21/07/2020 19:59:00	-rwxrwxrwx	1004 100
150178-1593619664-config.bson	375	Fichier BSON	01/07/2020 18:14:00	-rwxrwxrwx	1004 100

Il est nécessaire d'utiliser un format de nom prédéfini pour le fichier de configuration « <uid>-cfg.bson ».

Après application de la nouvelle configuration, un fichier d'acquittement est déposé sur le serveur, contenant le résultat de la prise en compte de la nouvelle configuration.

En cas d'erreur dans le fichier de configuration (fichier corrompu, valeur incorrecte, ...), le fichier ne sera pas appliqué, et le fichier d'acquittement remontra une erreur.

Il n'est pas nécessaire de renvoyer toute la configuration à votre concentrateur. Un fichier de configuration peut être complet ou partiel. Vous pouvez donc envoyer un fichier de configuration contenant qu'une seule variable.

Par défaut, la configuration envoyée au concentrateur est appliquée par-dessus la configuration courante. Seules les variables présentes dans le fichier de configuration seront écrasées.



Veuillez-vous référer au *chapitre 4.2* : « Fichier de configuration » ou à l'Annexe A : « Configuration – Liste des variables » pour connaître la liste des variables et leurs valeurs possibles.

5.3 Les données

Les données sont remontées dans le répertoire « /DATA » du serveur FTP(S), sous la forme de fichiers au format BSON.

Ci-dessous le format des noms des fichiers de données :

<uid>-<timestamp>-data.bson

Avec :

- `<uid>` : Identifiant du concentrateur
- `<timestamp>` : Nombre de secondes écoulées depuis le 1^{er} janvier 1970 à minuit UTC précise.

Exemple :

123456-1591083697-data.bson

La fréquence d'envoi des fichiers sur le serveur distant peut être définie par un ScheduleFTP (Voir chapitre 4.2.5.1.2 : « Schedule serveur (FTP) »). Cependant, lors d'une connexion au serveur, suite à un lancement du diagnostic, le concentrateur profite de la connexion pour déposer les données en mémoire.

Le fichier de données se compose des éléments suivants :

Paramètres	Description
uid	Identifiant du concentrateur
source	Source qui a déclenché le dépôt du fichier (schedule, magnet, usb, ...)
TS	Timestamp de la création du fichier (Nombre de secondes écoulées depuis le 1 ^{er} janvier 1970 à minuit UTC précise)
framecount	Le nombre de trames enregistré dans la section <i>data</i> (évolution future)
data	Tableau des trames WM-Bus enregistrées

Le tableau des trames WM-Bus enregistrées se décompose ainsi :

Paramètres	Description
T	Timestamp de réception de la trame (Nombre de secondes écoulées depuis le 1 ^{er} janvier 1970 à minuit UTC précise)
R	Niveau RSSI de la trame
F	Contenu de la trame reçue (entête + payload sans CRC) au format binaire. (type 0x00 en JSON) (Mise au format Base64 dans le fichier JSON)

Exemple d'un fichier de données converti en JSON :

```
{
  "uid": "WE_1234",
```

```

"source": "schedule",
"TS": 1560068897,
"frameCount": 2,
"data": [
  {
    "T": 1560066602,
    "R": 199,
    "F": {
      "$type": "00",
      "$binary": "fAviGIskaFDwA4E0UkO26w=="
    }
  },
  {
    "T": 15600645887,
    "R": 178,
    "F": {
      "$type": "00",
      "$binary": "+plAPliAwE0df2KBY1N7Iodr/LAFS2CrXTrUsY3wy731VN113/9UmO\CiglwR"
    }
  }
],
"crc": 0
}

```

5.4 Les alarmes

Les alarmes sont remontées dans le répertoire « /ALARM » du serveur FTP(S), sous la forme de fichiers au format BSON.



En cas de présence de deux serveurs distants dans la configuration, les fichiers alarmes sont uniquement déposés sur le serveur 1.

Le format des noms des fichiers d'alarmes est :

`<uid>-<timestamp>-alarm.bson`

Avec :

- `<uid>` : Identifiant du concentrateur
- `<timestamp>` : Nombre de secondes écoulées depuis le 1^{er} janvier 1970 à minuit UTC précise.

Exemple :

`123456-1591083697-alarm.bson`

Les alarmes peuvent être configurées pour être déposées qu'une seule fois dans une journée (voir chapitre 4.2.4 : « Alarmes »).

Le fichier d'alarme se compose des éléments suivants :

Paramètres	Description
------------	-------------

uid	Identifiant du concentrateur
source	Source qui a déclenché le dépôt du fichier (alarm)
TS	Timestamp de la création du fichier (Nombre de secondes écoulées depuis le 1 ^{er} janvier 1970 à minuit UTC précise)
alarm	Information sur l'alarme

Les informations de l'alarme « alarm » se décomposent ainsi :

Paramètres	Description
type	Type d'alarme : <i>temperature</i> , <i>battery</i> ou <i>ntp</i>
value	Valeur de la donnée qui a déclenché l'alarme.

Exemple d'un fichier d'alarme converti en JSON :

```
{
  "uid": "WE_1234",
  "source": "alarm",
  "TS": 1560068897,
  "frameCount": 2,
  "alarm": {
    "type": "temperature",
    "value": 45
  },
  "crc": 0
}
```

5.5 Les acquittements ACK

Les acquittements ACK sont remontés dans le répertoire « /ALARM » du serveur FTP, sous la forme de fichiers au format BSON.

Le format des noms des fichiers d'acquiescement est :

<uid>-<timestamp>-ack.bson

Avec :

- *<uid>* : Identifiant du concentrateur
- *<timestamp>* : Nombre de secondes écoulées depuis le 1^{er} janvier 1970 à minuit UTC précise.

Exemple :

123456-1591083697-ack.bson

Les acquittements sont envoyés suite à une commande reçue par le concentrateur.
Le fichier d'acquittance se compose des éléments suivants :

Paramètres	Description
uid	Identifiant du concentrateur
source	Source qui a déclenché le dépôt du fichier (ftp, usb, ...)
TS	Timestamp de la création du fichier (Nombre de secondes écoulées depuis le 1 ^{er} janvier 1970 à minuit UTC précise)
ack	Acquittement de la commande

L'acquittance de la commande « ack » se décompose ainsi :

Paramètres	Description
type	Type de commande correspondant à l'acquittance : - cmd : commande - config : mise à jour de la configuration
cid	Identifiant de commande correspondant à l'acquittance (limité à 15 caractères)
result	Résultat de la commande : - ok : commande ou mise à jour traitée avec succès - ko : erreur lors du traitement de la commande ou de la mise à jour
data	Donnée associée à l'acquittance (Par exemple : le nom du nouveau Firmware, le nom du fichier de configuration, ...)

Exemple d'un fichier d'acquittance converti en JSON :

```
{
  "uid": "WE_1234",
  "source": "ftp",
  "TS": 1560068897,
  "ack": {
    "type": "cmd",
    "cid": "c 1234",
    "result": "ok",
    "data": "/f10/152233-cmd.bson"
  }
},
```

```
} "crc":0
```

5.6 Les commandes

Il est possible d'exécuter à distance des actions sur le concentrateur. Pour cela, il faut envoyer au concentrateur une commande. Cette commande pouvant être envoyée via un fichier de commande au format BSON.

Fichier commande BSON :

Le fichier de commande doit être nommé de la manière suivante :

`<uid>-cmd.bson`

`<uid>-<num>-cmd.bson`

Avec :

- `<uid>` : Identifiant du concentrateur
- `<num>` : Numéro servant à l'enchaînement d'une suite de commande. (optionnel)

Exemples :

123456-cmd.bson
123456-1-cmd.bson
123456-2-cmd.bson



En cas de présence de deux serveurs distants dans la configuration, l'envoi de commande se fait uniquement par le répertoire INBOX du serveur 1.

Le fichier de commande peut être déposé par :

- **FTP(S)** sur le serveur distant dans le répertoire « /INBOX » associé au concentrateur (« /INBOX/<uid>/ », avec <uid>, l'identifiant du concentrateur). De la même manière que pour les fichiers de configuration. Tous les fichiers présents dans ce répertoire seront téléchargés avant d'être supprimés et exécutés. Un fichier d'acquittement sera déposé sur le serveur distant informant du résultat du traitement de la commande.
- **USB** sur le disque amovible. Après redémarrage du produit (par exemple un simple appui sur le bouton RESET), les fichiers présents sur le disque amovible seront traités et un acquittement sera déposé sur le disque informant du résultat du traitement de la commande.

Toutes les commandes acceptent deux paramètres aux formats chaînes de caractères et qui sont :

- uid : identifiant unique du concentrateur (facultatif)
- cid : identifiant de commande (obligatoire et longueur max 15 caractères)

Une commande sera rejetée si le paramètre « uid » inclus ne correspond pas à l'« uid » du concentrateur.

Le « cid » peut être librement choisi par l'émetteur de la commande mais doit être de longueur maximum de 15 caractères. Il sera inclus avec tout téléchargement associé.

Un acquittement de commande est créé et déposé pour le :

- FTP(S) : dans le répertoire ALARM du serveur distant,
- USB : sur le disque amovible du concentrateur.

Ci-dessous la liste des commandes disponibles sur le concentrateur :

Commande	Description
request	Connexion immédiate au serveur distant
factory	Retour aux paramètres usines
firmware	Mise à jour logiciel du concentrateur
diag	Lancement d'un diagnostic
configGet	Forcer le dépôt de la config sur le serveur distant
whiteListErase	Effacer la liste blanche « whiteList » de la radio
operatorInit	Réinitialiser le choix de l'opérateur réseau du modem
logGet	Forcer le dépôt des logs sur le serveur distant
logClean	Effacer le journal des événements
supervisionClean	Réinitialise à 0 les compteurs
supervisionGet	Forcer le dépôt de la supervision sur le serveur distant
certificate	Ajouter un certificat
certClean	Supprimer tous les certificats
dataClean	Effacement des données mémorisées dans le concentrateur

simStatus	Permet de savoir si le code PIN de la carte SIM est activé ainsi que le nombre de tentatives PIN et PUK restantes
simPin	Active ou désactive le code PIN de la carte SIM
simNewPin	Permet de changer le code PIN de la carte SIM
simPuk	Permet de déverrouiller la carte SIM après 3 codes PIN erronés



Dans le cas d'envoi de plusieurs commandes simultanées, les commandes « factory » et « firmware » peuvent faire perdre les commandes qui suivent. Mais aussi en cas d'erreur sur une commande précédente, les suivantes ne seront pas exécutées.

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "cmd": {
    "type": "request",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.1 Commande « request »

La commande « request » permet de déclencher une connexion immédiate du produit au serveur distant permettant ainsi de déposer les données, la configuration et la supervision, mais également de récupérer les fichiers présents dans son INBOX.

Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "cmd": {
    "type": "request",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.2 Commande « factory »

La commande « factory » permet de restaurer les paramètres usine dans le concentrateur.
Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "cmd": {
    "type": "factory",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.3 Commande « firmware »

La commande « firmware » permet de mettre à jour le logiciel du concentrateur.

(Voir le chapitre 6 : « Mise à jour »)

5.6.4 Commande « diag »

La commande « diag » permet de déclencher un diagnostic du concentrateur en collectant les données émises par les capteurs WM-Bus sur une durée configurée (voir le paramétrage radio « config→radio→duration ») et en lançant ensuite une connexion au serveur distant permettant ainsi de déposer les données, la configuration et la supervision, mais également de récupérer les fichiers présents dans son INBOX.
Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "cmd": {
    "type": "diag",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.5 Commande « configGet »

La commande « configGet » permet de copier la configuration courante sur la partition USB, cette commande n'a pas d'effet si elle est utilisée en FTP.

Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "cmd": {
    "type": "configGet",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.6 Commande « whiteListErase »

La commande « whiteListErase » permet d'effacer la liste blanche de la radio WM-Bus.
Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "cmd": {
    "type": "whiteListErase",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.7 Commande « whiteListCount »

La commande « whiteListCount » permet d'obtenir le nombre d'équipement dans la liste blanche de la radio WM-Bus.
Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "cmd": {
    "type": "whiteListCount",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.8 Commande « whiteListGet »

La commande « whiteListGet » permet d'obtenir la liste des équipements dans la liste blanche de la radio WM-Bus. Aucune sous-commande ou paramètre n'est nécessaire pour cette commande. Le fichier sera alors déposé dans le répertoire « CONFIG » du serveur (exemple de nom de fichier déposé : « 418163-1729068688-wiFilter.bson »)

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "cmd": {
    "type": "whiteListGet",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.9 Commande « operatorInit »

La commande « logGet » permet de forcer le dépôt des logs sur le serveur distant dans le répertoire « /SUPERVISION ».

Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "cmd": {
    "type": "operatorInit",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.10 Commande « logGet »

La commande « logGet » permet de forcer le dépôt des logs sur le serveur distant dans le répertoire « /SUPERVISION ».

Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "cmd": {
    "type": "logGet",
  },
  "crc": 0
}
```

```

    "cid": "123456"
  },
  "crc": 0
}

```

5.6.11 Commande « logClean »

La commande « logClean » permet d’effacer le journal des évènements.
Aucune sous-commande ou paramètre n’est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```

{
  "cmd": {
    "type": "logClean",
    "cid": "123456"
  },
  "crc": 0
}

```

5.6.12 Commande « dataGet »

La commande « dataGet » permet d’écrire les données présentes en flash dans la mémoire USB. Une fois le fichier créé la partition de donnée est effacée.

Ne fonctionne que par USB.

Aucune sous-commande ou paramètre n’est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```

{
  "cmd": {
    "type": "dataGet",
    "cid": "123456"
  },
  "crc": 0
}

```

5.6.13 Commande « supervisionClean »

La commande « supervisionClean » permet de forcer le dépôt de la supervision sur le serveur distant dans le répertoire « /SUPERVISION ».

Aucune sous-commande ou paramètre n’est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "cmd": {
    "type": "supervisionClean",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.14 Commande « supervisionGet »

La commande « supervisionGet » permet de forcer le dépôt de la supervision sur le serveur distant dans le répertoire « /SUPERVISION ».

Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "cmd": {
    "type": "supervisionGet",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.15 Commande « modemClean »

Cette commande efface la mémoire interne du modem qui contient, entre autre, la copie des certificats utilisés par la communication TLS.

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "cmd": {
    "type": "modemClean",
    "cid": "1"
  },
  "crc": 1002827272
}
```

5.6.16 Commande « certificate »

La commande « certificate » permet d'ajouter un certificat au concentrateur.

Dans la commande, il faut indiquer le nom du certificat à prendre en compte dans le champ « data ».

Il faut également joindre le certificat à rajouter :

- **Localement (USB) :**

Il faut déposer le certificat et la commande à la racine du disque local monté « WebdynEasy ». (Voir chapitre 4.1 : « Configuration locale par USB »)

- **Distance (FTP) :**

Le certificat doit être déposé dans le répertoire « /BIN » du serveur distant, et une commande d'ajout de certificat (« certificate ») doit être déposée dans le répertoire FTP(S) « INBOX » de votre concentrateur (« /INBOX/<uid>/ », avec <uid> l'identifiant de votre concentrateur).

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "cmd": {
    "type": "certificate",
    "cid": "123456",
    "data": "cert.pem"
  },
  "crc": 0
}
```

5.6.17 Commande « certClean »

La commande « certClean » permet d'effacer l'ensemble des certificats présents dans le concentrateur. Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Cette commande efface les certificats de la mémoire flash externe du modem. Pour aussi effacer les certificats copiés dans le modem il faut utiliser la commande « modemClean »

Exemple :

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "cmd": {
    "type": "certClean",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.18 Commande « dataClean »

La commande « dataClean » permet d'effacer l'ensemble des trames enregistrées dans la partition de donnée de la mémoire flash du concentrateur.

Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "cmd": {
    "type": "dataClean",
    "cid": "123456"
  },
  "crc": 0
}
```

5.6.19 Commande « simStatus »

La commande « simStatus » permet de savoir si le code PIN de la carte SIM est activé ainsi que le nombre de tentatives PIN et PUK restantes.

Aucune sous-commande ou paramètre n'est nécessaire pour cette commande.

Exemple :

- **Par fichier JSON** (à convertir au format BSON pour le concentrateur) :

```
{
  "cmd": {
    "type": "simStatus",
    "cid": "c 1234"
  },
  "crc": 0
}
```

Un fichier d'accusé de réception sera renvoyé avec le résultat de la commande.

Si la commande a réussi, nous aurons la valeur « ok » dans le champ « result » et dans le champ « data », nous aurons les valeurs suivantes séparées par une virgule :

- Statut SIM : 0 si le code PIN est désactivé ou 1 si le code PIN est activé
- Nombre de PIN restant : valeur entre 0 et 3
- Nombre de PUK restant : valeur entre 0 et 10

Exemples :

- Commande OK : carte SIM avec demande de code PIN et mauvais code PIN saisi

```
{
  "uid": "WE_123",
```

```

"source": "usb",
"TS": 1560068897,
"ack":
{
    "type": "cmd",
    "cid": "c 1234",
    "result": "ok",
    "data": "1,2,10"
},
"crc": 0
}

```

- Erreur de commande : pas de carte SIM

```

{
    "uid": "WE 123",
    "source": "usb",
    "TS": 1560068897,
    "ack":
    {
        "type": "cmd",
        "cid": "c 1234",
        "result": "ko",
        "data": "no sim"
    },
    "crc": 0
}

```

5.6.20 Commande « simPin »

La commande « simPin » active ou désactive le code PIN de la carte SIM.

Dans le champ « data » de la commande, vous devez indiquer si vous souhaitez activer ou désactiver le code PIN :

- Activer : « 1 »
- Désactiver : « 0 »

Si vous activez le code PIN, vous devez également indiquer le code PIN séparé par une virgule. (Max. 8 caractères)



L'utilisation de cette commande entraîne une modification de la configuration de la WebdynEasy.

Exemple : Activation du code PIN avec un code PIN « 1234 »

- Par fichier JSON (à convertir au format BSON pour le concentrateur) :

```

{
    "cmd": {
        "type": "simPin",
        "cid": "c 1234",
        "data": "1,1234"
    },
    "crc": 0
}

```

```
}
```

Un fichier d'accusé de réception sera renvoyé avec le résultat de la commande.

Si la commande a réussi, nous aurons la valeur « ok » dans le champ « result » et dans le champ « data » nous aurons la même valeur que le champ « data » de la commande.

En cas d'erreur sur la commande, le champ « result » est « ko » et un message d'erreur explicite est indiqué dans le champ « data ».

Exemples :

- Commande OK: Activation du code PIN de la carte SIM

```
{
  "uid": "WE_123",
  "source": "usb",
  "TS": 1560068897,
  "ack": {
    "type": "cmd",
    "cid": "c_1234",
    "result": "ok",
    "data": "1"
  },
  "crc": 0
}
```

- Erreur de commande : pas de carte SIM

```
{
  "uid": "WE_123",
  "source": "usb",
  "TS": 1560068897,
  "ack": {
    "type": "cmd",
    "cid": "c_1234",
    "result": "ko",
    "data": "no sim"
  },
  "crc": 0
}
```

5.6.21 Commande « simNewPin »

La commande « simNewPin » permet de changer le code PIN de la carte SIM.

Dans le champ « data » de la commande, vous devez indiquer le nouveau code PIN. (max. 8 caractères)



Pour utiliser cette commande, il est obligatoire d'avoir saisi un code PIN dans la configuration du WebdynEasy WM-Bus. (Voir chapitre 4.2.3.1 : « Modem »)



L'utilisation de cette commande entraîne une modification de la configuration de WebdynEasy.

Exemple : nouveau code PIN « 123456 »

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "cmd": {
    "type": "simNewPin",
    "cid": "c_1234",
    "data": "123456"
  },
  "crc": 0
}
```

Un fichier d'accusé de réception sera renvoyé avec le résultat de la commande.

Si la commande a réussi, nous aurons la valeur « ok » dans le champ « result » et dans le champ « data » nous aurons la même valeur que le champ « data » de la commande.

En cas d'erreur sur la commande, le champ « result » est « ko » et un message d'erreur explicite est indiqué dans le champ « data ».

Exemples :

- Commande OK: Changement du code PIN par la valeur « 123456 »

```
{
  "uid": "WE_123",
  "source": "usb",
  "TS": 1560068897,
  "ack": {
    "type": "cmd",
    "cid": "c_1234",
    "result": "ok",
    "data": "123456"
  },
  "crc": 0
}
```

- Erreur de commande : Changement du code PIN par la valeur « 123456789 »

```
{
  "uid": "WE 123",
  "source": "usb",
  "TS": 1560068897,
  "ack": {
    "type": "cmd",
    "cid": "c_1234",
    "result": "ko",
    "data": "value error: 12346789"
  },
  "crc": 0
}
```

5.6.22 Commande « simPuk »

La commande « simPuk » déverrouille la carte SIM après 3 codes PIN erronés.

Dans le champ « data » de la commande, vous devez indiquer le nouveau code PIN et le code PUK séparés par une virgule. (Max. 8 caractères par code)



L'utilisation de cette commande entraîne une modification de la configuration de WebdynEasy.



Si vous entrez 10 codes PUK erronés, la carte SIM est bloquée définitivement.

Exemple : Déblocage de la carte SIM (code PUK « 11223344 ») et nouveau code PIN « 1234 »

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "cmd": {
    "type": "simPuk",
    "cid": "c_1234",
    "data": "1234,11223344"
  },
  "crc": 0
}
```

Un fichier d'accusé de réception sera renvoyé avec le résultat de la commande.

Si la commande a réussi, nous aurons la valeur « ok » dans le champ « result » et dans le champ « data », nous aurons le nouveau code PIN.

En cas d'erreur sur la commande, le champ « result » est « ko » et un message d'erreur explicite est indiqué dans le champ « data ».

Exemples :

- Commande OK: Déverrouiller la carte SIM et nouveau code PIN « 1234 »

```
{
  "uid": "WE 123",
  "source": "usb",
  "TS": 1560068897,
  "ack": {
    "type": "cmd",
    "cid": "c_1234",
    "result": "ok",
    "data": "1234"
  },
  "crc": 0
}
```

- Erreur de commande : Mauvais code PUK

```
{
  "uid": "WE 123",
  "source": "usb",
  "TS": 1560068897,
  "ack": {
    "type": "cmd",
    "cid": "c_1234",
    "result": "ko",
    "data": "invalid PUK code or PIN code format error, remaining try=9"
  },
  "crc": 0
}
```

5.7 La supervision

Les informations de supervision sont remontées dans le répertoire « /SUPERVISION » du serveur FTP, sous la forme de fichiers au format BSON.

Ci-dessous le format des noms des fichiers de supervision :

`<uid>-<timestamp>-supervision.bson`

Avec :

- `<uid>` : Identifiant du concentrateur
- `<timestamp>` : Nombre de secondes écoulées depuis le 1^{er} janvier 1970 à minuit UTC précise.

Exemple :

123456-1591083697-supervision.bson

Les fichiers de supervision sont déposés lors d'une connexion au serveur FTP.
Le fichier de supervision se compose des éléments suivants :

Paramètres	Description
uid	Identifiant du concentrateur
source	Source qui a déclenché le dépôt du fichier (schedule, ftp, usb, ...)
TS	Timestamp de la création du fichier (Nombre de secondes écoulées depuis le 1 ^{er} janvier 1970 à minuit UTC précise)
supervision	Information de supervision

Les informations de la supervision « supervision » se décomposent ainsi :

Section	Paramètres	Description
identity	<i>uid</i>	Identifiant du concentrateur
	<i>name</i>	Nom du concentrateur
	<i>SN</i>	Numéro de série
version	<i>hw</i>	Version Hardware du produit
	<i>sw</i>	Version logiciel de l'application
	<i>swBle</i>	Version logiciel du module Bluetooth BLE
	<i>swModem</i>	Version logiciel du Modem
uptime	<i>run</i>	Temps total en fonctionnement en mode RUN en seconde
	<i>radio</i>	Temps total en écoute radio en seconde
	<i>modem</i>	Temps total en modem en seconde

	<i>lowPower</i>	Temps total en veille en seconde
measures	<i>vAlim</i>	Tension alimentation en mV
	<i>temperature</i>	Température du concentrateur en °C
	<i>histogram</i>	Histogramme de la température
modem	<i>rssI</i>	RSSI de la dernière connexion
	<i>quality</i>	Informations sur la force du signal de la connexion modem
	<i>nwinfo</i>	Informations sur la technologie, l'opérateur, la bande et le canal utilisé par le modem
	<i>imei</i>	IMEI du modem
	<i>iccid</i>	ICCID (numéro identification) de la carte SIM
	<i>num</i>	Numéro de téléphone de la carte SIM
	<i>operator</i>	Nom de l'opérateur préféré
	<i>mode</i>	Type de connexion (2G, LTEM, auto)
	<i>TS</i>	Timestamp de la dernière action
	<i>error</i>	Erreur affichée après une action local Diagnostic ou Request qui a échoué : • "Invalid PIN" : Code PIN non renseigné • "Error PIN" : Mauvais code PIN • "Error connect" : Erreur de connexion réseau • "Error APN" : Erreur d'APN • "No SIM" : Carte SIM absente • "SIM PUK" : Carte SIM bloquée • "Registration denied" : Refusé par l'opérateur • "Server error" : Problème de connexion au serveur
counters	<i>wakeup</i>	Nombre total de réveils

	<i>magnetWakeup</i>	Nombre total de réveils provenant de l'aimant
	<i>bleWakeup</i>	Nombre total de réveils provenant du Bluetooth BLE
	<i>ftp</i>	Nombre total de réveils par le Schedule FTP
	<i>alarms</i>	Nombre total d'alarmes envoyées
	<i>radio</i>	Nombre total de réveils par le Schedule Radio
	<i>usb</i>	Nombre total de réveils par USB
	<i>wd</i>	Nombre de déclenchement du watchdog
	<i>fault</i>	Nombre d'erreurs fatales
dates	<i>lastConfig</i>	Timestamp de la dernière mise à jour de la configuration (optionnel)
	<i>lastUpdate</i>	Timestamp de la dernière mise à jour logicielle (optionnel)
	<i>lastPowerOn</i>	Timestamp de la dernière mise sous tension (optionnel)
	<i>lastCnxOk</i>	Timestamp de la dernière connexion réussie (optionnel)
	<i>lastCnxKo</i>	Timestamp du dernier échec de connexion (optionnel)
battery		
	<i>capaPrcent</i>	Pourcentage de la capacité restante de la pile
	<i>capamAh</i>	Capacité en mAh restant dans la pile
WmBus	<i>CptRxPreamb</i>	Nombre de préambules radio détectés en réception radio
	<i>CptRxSync</i>	Nombre de code de synchronisation radio détecté en réception radio

<i>CptRxFrames</i>	Nombre de trames radio décodées en réception radio
<i>CptRxFramesCrcKo</i>	Nombre d'erreurs de CRC en réception radio
<i>CptRxFramesDecodeKo</i>	Nombres d'erreurs de décodage en réception radio
<i>CptRxFramesLenKo</i>	Nombres d'erreurs de longueur en réception radio
<i>CptRxOverrun</i>	Nombre de dépassement du buffer en réception radio
<i>CptRxTimeOut</i>	Nombre de temps dépassé en réception radio
<i>CptRecFrames</i>	Nombre de trames enregistrées
<i>whiteListItemCount</i>	Nombres d'éléments présents dans la liste blanche (à partir de la version firmware 3.3)



Les données statistiques « WmBus » sont destinées au support Webdyn.



Quelquefois, le numéro de téléphone « num » est vide, car certains opérateurs mobiles ne renseignent pas le numéro de téléphone dans la SIM. Cela n'a aucune incidence sur le fonctionnement du concentrateur.



Lorsque la passerelle est alimentée sur le secteur la valeur de capacité restante de la batterie (« *capaPrcent* » et « *capamAh* ») ne prend pas en compte l'autodécharge..

L'histogramme de température « *histogram* » se décompose ainsi :

Paramètres	Description
below -10°C	Nombre de fois où la température du concentrateur est inférieure à -10°C
-10°C to 0°C	Nombre de fois où la température du concentrateur est comprise entre -10°C et 0°C

0°C to 10°C	Nombre de fois où la température du concentrateur est comprise entre 0°C et 10°C
10°C to 20°C	Nombre de fois où la température du concentrateur est comprise entre 10°C et 20°C
20°C to 30°C	Nombre de fois où la température du concentrateur est comprise entre 20°C et 30°C
30°C to 40°C	Nombre de fois où la température du concentrateur est comprise entre 30°C et 40°C
above 40°C	Nombre de fois où la température du concentrateur est supérieure à -40°C

Les informations sur la force du signal de la connexion modem « *quality* » se décomposent ainsi :

Paramètres	Description
rsi	Force du signal reçu (disponible en 2G, LTE-M et NB-IoT)
rsrp	Puissance du signal de référence reçu (disponible en LTE-M et NB-IoT)
rsrq	Qualité du signal de référence reçu (disponible en LTE-M et NB-IoT)
sinr	Rapport signal sur bruit plus interférence (disponible en LTE-M et NB-IoT)

Exemple d'un fichier de supervision converti en JSON :

```
{
  "uid": "WE_1234",
  "source": "schedule",
  "TS": 1598349735,
  "supervision": {
    "identity": {
      "uid": "WE_1234",
      "name": "1234",
      "SN": "SN20200423_9876543210"
    },
    "version": {
      "hw": 11,
      "sw": "01.04",
      "swBle": "0.1",
      "swModem": "BG95M3LAR02A03 01.005.01.005"
    },
    "uptime": {
      "run": 85484,
      "radio": 69090,
      "modem": 5873,
      "lowPower": 336583
    },
    "measures": {
      "vAlim": 7100,
      "temperature": 15,
      "histogram": {
```

```

        "below -10°C":0,
        "-10°C to 0°C":0,
        "0°C to 10°C":63,
        "10°C to 20°C":73,
        "20°C to 30°C":36,
        "30°C to 40°C":0,
        "above 40°C":0
    }
},
"modem":{
    "rssi":-57,
    "quality":{
        "rssi":-57,
        "rsrp":-79,
        "rsrq":-13,
        "sinr":12
    },
    "nwinfom":{"eMTC","20801","LTE BAND 20",6400",
    "imei":"864475041522664",
    "num":"",
    "operator":"Orange F Things Mobile",
    "mode":"LTEM"
},
"counters":{
    "wakeup":2281,
    "magnetWakeup":4,
    "bleWakeup":0,
    "ftp":137,
    "radio":2094,
    "alarms":0,
    "usb":14,
    "wd":0,
    "fault":0
},
"dates":{
    "lastConfig":1598364963,
    "lastUpdate":0,
    "lastPowerOn":0,
    "lastCnxOk":1610968521,
    "lastCnxKo":1610752526
},
"battery":{
    "remainTime":null,
    "capaPrcnt":95,
    "capamAh":13362
},
"wmBus":{
    "CptRxPreamb":18443,
    "CptRxSync":11639,
    "CptRxFrames":5632,
    "CptRxFramesCrcKo":221,
    "CptRxFramesDecodeKo":5786,
    "CptRxFramesLenKo":0,
    "CptRxOverrun":0,
    "CptRxTimeOut":0,
    "CptRecFrames":253
}
},
"crc":0
}

```

5.8 Le Log

Les logs sont remontés dans le répertoire « /SUPERVISION » du serveur FTP, sous la forme de fichiers au format BSON.

Ci-dessous le format des noms des fichiers de supervision :

`<uid>-<timestamp>-log.bson`

Avec :

- `<uid>` : Identifiant du concentrateur
- `<timestamp>` : Nombre de secondes écoulées depuis le 1^{er} janvier 1970 à minuit UTC précise.

Exemple :

123456-1591083697-log.bson

Les fichiers de log sont déposés lors d'une connexion au serveur FTP.

Le fichier de log se compose des éléments suivants :

Paramètres	Description
uid	Identifiant du concentrateur
source	Source qui a déclenché le dépôt du fichier (schedule, ftp, usb, ...)
TS	Timestamp de la création du fichier (Nombre de secondes écoulées depuis le 1 ^{er} janvier 1970 à minuit UTC précise)
log	Liste des logs

La liste des logs « log » se décompose ainsi :

Paramètres	Description
T	Timestamp de l'évènement (Nombre de secondes écoulées depuis le 1 ^{er} janvier 1970 à minuit UTC précise)
C	Code de l'évènement (<i>Voir l'Annexe B : « Log – Liste des évènements »</i>)
D	Données associées à l'évènement (facultatif)

Exemple d'un fichier de log converti en JSON :

```
{
  "uid": "WE_1234",
  "source": "schedule",
  "TS": 1560068897,
  "log": [
    {
      "T": 1598348100,
      "C": 33554432,
```

```

        "D":["APP][appModeInit():133]mode: run"
    },
    {
        "T":1598348100,
        "C":33554432,
        "D":["APP][appRun():27]run application"
    },
    {
        "T":1598348100,
        "C":33554432,
        "D":["RADIO][appRadioTask():57]radio task"
    },
    {
        "T":1598348100,
        "C":33554432,
        "D":["FRAME][Frame_FastFilter_Init():57]white list filter disable"
    },
    {
        "T":1598348100,
        "C":33554432,
        "D":["RADIO][appRadioTask():98]Windowsduration: 30"
    },
    {
        "T":1598348130,
        "C":33554432,
        "D":["FRAME][Frame_Process_Cmd():226]RX Frame count:5"
    },
    {
        "T":1598348134,
        "C":33554432,
        "D":["PERIODIC][periodicTask():49]periodic task"
    },
    {
        "T":1598348134,
        "C":33554432,
        "D":["RADIO][appRadioNextAlarm():144]Next Alarm: Tue Aug 25 09:40:00 2020\n data:30"
    }
],
"crc":0
}

```

6 Mise à jour

Le concentrateur WebdynEasy peut être mis à jour localement par USB ou à distance par FTP. Le produit possède un firmware pour la partie applicative.

La dernière version du firmware (« WebdynEasy_Vx.x.bson ») ainsi que la commande associée sont disponibles en téléchargement sur notre site à l'adresse suivante :

<https://www.webdyn.com/support/webdyneasy/>

Pour effectuer la mise à jour du concentrateur, il faut passer également une commande de mise à jour (« firmware ») en plus du nouveau firmware. Dans la commande, il faut indiquer le nom du firmware à prendre en compte dans le champ « data ».

Un fichier de commande « firmware-cmd.bson » est fourni en même temps que le firmware. Il suffit de le renommer en « <uid>-cmd.bson ».

Avec :

- <uid> : Identifiant du concentrateur

Un fichier d'acquiescement est déposé après la mise à jour.



A partir de la version V4.0 la mise à jour avec une version inférieure n'est plus possible.

Cela peut entraîner le blocage du produit et annule la garantie.

Exemple de mise à jour du firmware applicatif:

- **Par fichier JSON (à convertir au format BSON pour le concentrateur) :**

```
{
  "cmd": {
    "type": "firmware",
    "cid": "firmwareAPP",
    "data": "WebdynEasy_V1.0.bson"
  },
  "crc": 0
}
```

6.1 Locale

Pour mettre à jour le concentrateur localement, il faut connecter le câble USB entre le concentrateur et son ordinateur puis suivre la procédure de téléchargement de fichiers (*Voir chapitre 4.1 : « Configuration locale par USB »*).

Il faut déposer le fichier ou les fichiers contenant la mise à jour ainsi que la commande qui lui est associée.

6.2 Distant

Pour une mise à jour à distance, le fichier contenant la mise à jour doit être déposé dans le répertoire « /BIN » du serveur distant, et une commande de mise à jour (« firmware ») doit être déposée dans le répertoire FTP(S) « INBOX » de votre concentrateur (« /INBOX/<uid>/ », avec <uid> l'identifiant de votre concentrateur). La commande doit inclure le nom du fichier contenant la mise à jour (champ « data »).

Lors de la prochaine connexion au serveur FTP, le concentrateur récupérera les fichiers et exécutera la mise à jour.

7 Outils & diagnostics

Logiciel de configuration WebdynEasy WM-Bus :

Afin de faciliter le paramétrage du concentrateur WebdynEasy WM-Bus, un logiciel de configuration spécifique au produit a été développé par Webdyn. Le logiciel permet de gérer la configuration, de créer facilement des « whiteList » mais également d'envoyer des commandes aux produits.

Ce logiciel « WebdynEasyConfigurator » est mis à disposition gratuitement pour Windows sur notre site à cette adresse :

<https://www.webdyn.com/fr/support>

Outils de conversion BSON-JSON et JSON-BSON :

Afin de faciliter la conversion des fichiers JSON et BSON, Webdyn a créé un convertisseur JSON-BSON et BSON-JSON. Il est possible de l'utiliser en mode silencieux (avec une console) ou à travers une IHM.

Cet outil est mis à disposition gratuitement pour Windows et Linux sur notre site à cette adresse :

<https://www.webdyn.com/download/JsonBsonConverter.zip>

Exemple de Scripts de conversion en python :

Une note d'application avec des exemples concrets de script est disponible et qui permet de réaliser des conversions et manipulations de fichiers.

Elle est disponible à l'adresse suivante :

<https://www.webdyn.com/fr/support>

8 FAQ

Pourquoi le concentrateur ne dépose plus de fichiers sur le serveur FTP(S) ?

Veillez vérifier ces points dans cet ordre :

- Le niveau de la pile : si la pile est trop basse ou vide, le produit ne fonctionnera pas correctement ou plus du tout.
- Le niveau de réception du modem : un mauvais signal au niveau du modem peut également empêcher le concentrateur de déposer les fichiers. Voir pour déplacer le produit ou installer une antenne externe pour améliorer la qualité du signal.
- Le dernier fichier de configuration : un mauvais fichier de configuration peut bloquer le produit.

Comment savoir si le produit est démarré ?

À distance, en vérifiant les fichiers déposés périodiquement si la configuration du produit a bien été faite.

À proximité, en passant l'aimant sur le haut du produit, vous entendrez 3 bips courts retentir.

Comment remplacer un produit par un autre ?

Remplacer le produit et injecter la configuration de l'ancien produit dans le nouveau. Si une liste blanche « whiteList » est utilisée, ne pas oublier de l'injecter dans le nouveau produit également.

Est-ce que le concentrateur peut déchiffrer les données chiffrées reçues des équipements WM-Bus ?

Non, le concentrateur n'est pas capable de déchiffrer les données des équipements WM-BUS car il n'embarque pas de coffre-fort afin de garantir la sécurité des clés de chiffrement de vos équipements. Les données récupérées sont déposées sans modification (sans déchiffrement) par le concentrateur sur votre serveur distant.

9 Support

En cas de problèmes techniques relatifs à nos produits, contactez le support de WEBDYN :

Webdyn SA

26 Rue des Gaudines

78100 Saint-Germain-en-Laye

FRANCE

Tel.: +33 1 39 04 29 40

Mail : support@webdyn.com

<https://www.webdyn.com>

Munissez-vous des éléments suivants :

- Type de produit
- Numéro de série du produit.
- Version de matériel et de logiciel du produit.
- Les logs du concentrateur
- La configuration du concentrateur



Le manuel utilisateur et les Firmwares sont disponibles à cette adresse web :
<https://www.webdyn.com/fr/support>

10 ANNEXES

10.1 Annexe A : « Configuration – Liste des variables »



Tous les « **noms + arborescence** » surlignés en vert sont des listes et peuvent être créés plusieurs fois.

Nom + arborescence	Description	Type	Valeur par défaut	Information uniquement	A partir de la version
/version	Version de l'application	Nombre entier		●	
/timestamp	Timestamp de la dernière configuration (Nombre de secondes écoulées depuis le 1er janvier 1970 à minuit UTC précise)	Texte		●	
/uid	Identifiant du concentrateur	Nombre entier		●	
/name	Nom du concentrateur	Texte			
/sn	Numéro de série			●	
/mode	Mode de fonctionnement du concentrateur	Liste : • factorySettings • storage • run			
/logLevel	Niveau de log dans le journal des événements	Liste : • 0 : Erreur • 1 : Warning • 2 : Info • 3 : Debug	2		
/radio/mode[0]	Mode du WM-Bus utilisé	Liste : • 0 : pour S1 (868MHz) • 1 : pour T1 (868MHz) • 2 : pour T1 + C1 (868MHz)	2		

		• 3 : pour T1+C1 (434MHz) • 4 : pour S1 (434MHz)			
/radio/mode[1]	Mode du WM-Bus utilisé pour le multimode d'écoute. Par défaut, on est en simple mode.	Liste : • 0 : pour S1 (868MHz) • 1 : pour T1 (868MHz) • 2 : pour T1 + C1 (868MHz) • 3 : pour T1+C1 (434MHz) • 4 : pour S1 (434MHz)			1.08
/radio/BFormatLFieldAdaptation	Activation de l'adaptation du champ L pour les trames au format B	Booléen : • true : Adaptation du champ L du format B au format A. • false : Champ L du format B n'est pas modifié.	true		1.06
/radio/duration	Durée de la fenêtre d'écoute en WM-Bus en secondes	Nombre entier (min 30 max 21600)	60		
/radio/manufFilter	Liste des codes constructeurs autorisés (maximum 8 codes)	Liste : 2 octets au format binaire (M-field)			
/radio/mediumFilter	Liste des codes medium des capteurs ou compteurs WM-BUS autorisés (maximum 8 codes)	Liste : octet 1 du champs A-field au format binaire			
/radio/ciFilter	Liste de champ CI des capteurs ou compteurs autorisés au format binaire (type 0x00 en JSON) (maximum 8 codes) Se référer au manuel du fabricant du compteur.	Liste : octet 1 du champs CI-field au format binaire			3.0
/radio/longHeader	Utilisation des informations du compteur présentes dans l'entête long dans une trame longue (se référer au « long header » de la spécification « Open Metering system »)	Booléen : • true : informations utilisées dans l'entête long • false : informations utilisées dans l'entête court	true		

/radio/skipVersionField	En cas de Whitelist, permet d'ignorer la version du compteur présent dans l'entête	Booléen : • true : ignore la version • false : tient compte de la version	false		2.0
/radio/skipMediumField	En cas de Whitelist, permet d'ignorer le type (« medium ») du compteur présent dans l'entêteAjout des	Booléen : • true : ignore le type • false : tient compte du type	false		2.0
/radio/oneFramePerMeter	N'enregistre qu'une trame de compteur (par longueur donnée) par fenêtre d'écoute.	Booléen : • true : activée • false : désactivée	true		2.5
/radio/isManufAllowList	Type de filtre constructeur.	Booléen : • true : liste blanche « whiteList » • false : liste noire « blackList »	true		3.0
/radio/isMediumAllowList	Type de filtre medium.	Booléen : • true : liste blanche « whiteList » • false : liste noire « blackList »	true		3.0
/radio/isCiAllowList	Type de filtre CI.	Booléen : • true : liste blanche « whiteList » • false : liste noire « blackList »	true		3.0
/security/crcMode	Vérification du CRC des fichiers BSON	Liste : • 0 : Aucune vérification du CRC • 1 : Vérification partielle (pas de vérification si le CRC est à 0) • 2 : Vérification activée du CRC	1		
/security/encryption	Chiffrement en AES des fichiers BSON	Booléen : • true : chiffrement des fichiers activé • false : chiffrement des fichiers désactivé	true		
/security/key	Clé AES128 CBC	Hexadécimal sur 16 octets	clé usine		

/security/aesLegacy	Force l'utilisation de l'ancien format de fichier AES (IV fixe)	Booléen	false		4.0
/local/magnet	Configuration de l'action au passage de l'aimant en mode RUN	Liste : • 0 : Modem • 1 : commande diagnostic • 2 : commande request	2		
/local/testCount	Nombre de séquences de commande de diagnostic d'affilée	Nombre entier (min 1 max 30)	1		
/local/timeout	Temps maximum d'exécution de l'action en seconde. Fonctionnel uniquement si le paramètre « testCount » vaut 1.	Nombre entier (min 60 max 21600) et désactivé = 0	0		
/local/server1Files	Type de fichier à envoyer sur le serveur 1 en cas de commande Diagnostic ou Request	Nombre entier : • Bit 0 : données (1=activé, 0=désactivé) • Bit 1 : supervision (1=activé, 0=désactivé) • Bit 2 : log (1=activé, 0=désactivé)			3.3
/local/server2Files	Type de fichier à envoyer sur le serveur 2 en cas de commande Diagnostic ou Request	Nombre entier : • Bit 0 : données (1=activé, 0=désactivé) • Bit 1 : supervision (1=activé, 0=désactivé) • Bit 2 : log (1=activé, 0=désactivé)			3.3
/remote/modem/mode	Choix du type de connexion	Liste : • 2G : Force le modem en 2G • LTE-M : Force le modem en LTE-M • NB-IoT : Force le modem en NB-IoT • Auto : Le modem gère automatiquement le réseau	auto		
/remote/modem/scanseq	Tableau de préférence de la séquence de recherche	Liste :			

		• 2G : Force le modem en 2G • LTE-M : Force le modem en LTE-M • NB-IoT : Force le modem en NB-IoT			
/remote/modem/band	Liste des bandes autorisées pour la connexion modem en NB-IoT	Liste : 1,2,3,4,5,8,12,13,18,19,20,25,28,66,85			
/remote/modem/deregisterOnLocalAction	Désenregistrement du modem sur le réseau opérateur à chaque déclenchement d'action par l'aimant	Booléen : • true : Désenregistrement activé • false : Désenregistrement désactivé (par défaut)	false		
/remote/modem/cpin	Code PIN de la carte SIM	Texte (8 caractères max)	null		
/remote/modem/operator	Code operateur (optionnel)	Nombre entier	null		
/remote/modem/apn	Identifiant du point d'accès du réseau (APN)	Texte (32 caractères max)	null		
/remote/modem/user	Identifiant pour la connexion PPP	Texte (32 caractères max)	null		
/remote/modem/pass	Mot de passe pour la connexion PPP	Texte (32 caractères max)	null		
/remote/modem/timeout	Temps maximum pour accrocher un réseau en seconde	Nombre entier (min 60 max 1800)	300		
/remote/modem/randomDelay	Délai aléatoire avant le réveil en minutes	Nombre entier (min 0 max 60) 0 : aucun délai	0		
/remote/ftp/mode	Choix du protocole	Liste : • 0 : FTP • 1 : FTPS (FTP over TLS) • 2 : FTPS + certificats • 3 : HTTP • 4 : HTTPS (HTTP over TLS) • 5 : HTTPS + CA+CERT+KEY • 6 : HTTPS + CA only	1		
/remote/ftp/addr	Adresse IP ou nom du serveur FTP(S)/HTTP(S) distant	Texte (128 caractères max)	null		

	Possibilité de modifier le port du FTP(S)/HTTP(S) en rajoutant « : » puis le numéro de port (entre 1 et 65535)				
/remote/ftp/user	Identifiant du compte FTP(S)/HTTP(S)	Texte (64 caractères max)	null		
/remote/ftp/pass	Mot de passe du compte FTP(S)/HTTP(S)	Texte (64 caractères max)	null		
/remote/ftp/dir	Répertoire racine sur le serveur FTP	Texte (64 caractères max) null : répertoire racine du compte FTP	null		
/remote/ftp/cacert	Certificat racine d'autorité de certification	Texte (128 caractères max)	null		
/remote/ftp/clientcert	Certificat signé du client local	Texte (128 caractères max)	null		
/remote/ftp/clientkey	Clé privée du client local	Texte (128 caractères max)	null		
/remote/ftp/sni	Active l'extension SNI du TLS	Booléen	False		4.0
/remote/ftp/cipherSuite	Liste des « cipher suite » utilisable par le client FTPS/HTTPS. Pour la liste des codes Cf : 10.3	Texte (231 caractères max)	0xC02B, 0xC02F		4.0
/remote/ftp/sni	Active l'extension SNI pour la communication TLS	Booléen	false		4.0
/remote/ftp/checkFtpDir	Permet de rendre optionnel la vérification de l'arborescence du serveur FTP(S) lors de la connexion	Booléen : • true : vérification activée (par défaut) • false : vérification désactivée	true		2.05
/remote/ftp/checkBcast	Permet d'activer la fonction broadcast	Booléen : • true : activée • false : désactivée	false		
/remote/ftp/httpDelay	Délais en secondes entre deux requêtes HTTP	Nombre entier (min 0 max 30)	0		4.2
/remote/server2/mode	Choix du protocole	Liste : • 0 : FTP	1		3.3

		• 1 : FTPS (FTP over TLS) • 2 : FTPS + certificats • 3 : HTTP • 4 : HTTPS (HTTP over TLS) • 5 : HTTPS + CA+CERT+KEY • 6 : HTTPS + CA only			
/remote/server2/addr	Adresse IP ou nom du serveur FTP(S)/HTTP(S) distant Possibilité de modifier le port du FTP(S)/HTTP(S) en rajoutant « : » puis le numéro de port (entre 1 et 65535)	Texte (128 caractères max)	null		3.3
/remote/server2/user	Identifiant du compte FTP(S)/HTTP(S)	Texte (64 caractères max)	null		3.3
/remote/server2/pass	Mot de passe du compte FTP(S)/HTTP(S)	Texte (64 caractères max)	null		3.3
/remote/server2/dir	Répertoire racine sur le serveur FTP	Texte (64 caractères max) null : répertoire racine du compte FTP	null		3.3
/remote/server2/cacert	Certificat racine d'autorité de certification	Texte (128 caractères max)	null		3.3
/remote/server2/clientcert	Certificat signé du client local	Texte (128 caractères max)	null		3.3
/remote/server2/sni	Active l'extension SNI du TLS	Booléen	False		4.0
/remote/ server2/cipherSuite	Liste des « cipher suite » utilisable par le client FTPS/HTTPS. 0xFFFF autorise toutes les cipher suites du modem. Pour la liste des codes Cf : 10.3	Texte (231 caractères max)	0xC02B, 0xC02F		4.0
/remote/server2/clientkey	Clé privée du client local	Texte (128 caractères max)	null		3.3
/remote/server2/checkFtpDir	Permet de rendre optionnel la vérification de l'arborescence du serveur FTP lors de la connexion	Booléen : • true : vérification activée (par défaut) false : vérification désactivée	true		3.3

/remote/server2/sni	Active l'extension SNI pour la communication TLS	Booléen	false		4.0
remote/server2/checkBcast	Permet d'activer la fonction broadcast	Booléen : true : activée false : désactivée	false		3.3
/remote/server2/httpDelay	Délais en secondes entre deux requêtes HTTP	Nombre entier (min 0 max 30)	0		4.2
/remote/ntp	Adresse IP ou nom du serveur NTP Possibilité de modifier le port du NTP en rajoutant « : » puis le numéro de port (entre 1 et 65535)	Texte (64 caractères max)	null		
/alarms/oneAlarmPerDay	Une seule transmission d'une alarme par modem par jour	Booléen : - true : envoi au maximum une transmission due à une alarme par jour (par défaut) - false : transmission de toutes les alarmes dans une journée.	true		
/alarms/temperature	Température maximum en degré (°C) avant déclenchement d'une alarme	Nombre entier (min 10 max 50) null ou 0 : désactive les alarmes température.	null		
/alarms/timeGap	Surveillance de la dérive horloge du concentrateur par rapport à l'heure récupérée par NTP en seconde avant déclenchement d'une alarme	Nombre entier (min 2 max 3600) null ou 0 : désactive les alarmes dérive horloge.	null		
/alarms/battery	Surveillance du niveau pile restant en pourcentage (%) avant déclenchement d'une alarme	Nombre entier (min 10 max 99) null ou 0 : désactive les alarmes pile.	null		
/scheduleRadio	Liste des déclencheurs de minuteur du Schedule Radio				
/scheduleRadio/cron	Déclencheur du minuteur	déclencheur de minuteurs « cron » : mm hh jj MM JJ			

		• <i>mm</i> : représente les minutes (de 0 à 59) • <i>hh</i> : représente l'heure (de 0 à 23) • <i>jj</i> : représente le numéro du jour du mois (de 1 à 31 ou « L ») • <i>MM</i> : représente le numéro du mois (de 1 à 12) • <i>JJ</i> : représente le numéro du jour dans la semaine : ▪ 0 = dimanche ▪ 1 = lundi ▪ = mardi ▪ ... ▪ 6 = samedi			
/scheduleRadio/data[0]	Durée de la fenêtre d'écoute Radio en secondes	Nombre entier (min 30 max 3600)	60		
/scheduleRadio/data[1]	Durée de la fenêtre d'écoute Radio en secondes pour le multimode d'écoute. Par défaut, on est en simple mode.	Nombre entier (min 30 max 3600)			1.08
/scheduleFTP	Liste des déclencheurs de minuteur du Schedule FTP				
/scheduleFTP/cron	Déclencheur du minuteur	déclencheur de minuteurs « cron » : <i>mm hh jj MM JJ</i> • <i>mm</i> : représente les minutes (de 0 à 59) • <i>hh</i> : représente l'heure (de 0 à 23) • <i>jj</i> : représente le numéro du jour du mois (de 1 à 31 ou « L ») • <i>MM</i> : représente le numéro du mois (de 1 à 12) • <i>JJ</i> : représente le numéro du jour dans la semaine : ▪ 0 = dimanche ▪ 1 = lundi ▪ = mardi ▪ ... ▪ 6 = samedi			
/scheduleFTP/data	Type de fichier à envoyer	Nombre entier : • Bit 0 : données serveur 1 (1=activé, 0=désactivé) • Bit 1 : supervision			

		serveur 1 (1=activé, 0=désactivé) • Bit 2 : log serveur 1 • Bit 3 : non utilisé • Bit 4 : données serveur 2 (1=activé, 0=désactivé) • Bit 5 : supervision serveur 2 (1=activé, 0=désactivé) • Bit 6 : log serveur 2 (1=activé, 0=désactivé)			
/monitoringPeriod	Période de monitoring du concentrateur en minutes	Nombre entier (min 15 max 1440) <i>null</i> ou 0 : désactive le monitoring	60		

10.2 Annexe B : « Log – Liste des évènements »

Code de l'évènement	Description de l'évènement
0	Erreur générique
5	Erreur de mémoire
16777216	Warning générique
33554432	Info générique
33554435	Réveil (wake-up)
33554436	LowPower
50331649	Redémarrage (Reset)
50331650	Initialisation
DEBUG	Debug générique

10.3 Annexe C : Liste des suites de chiffrement utilisables

Cipher suite code	Cipher suite name
0X0035	TLS_RSA_WITH_AES_256_CBC_SHA
0X002F	TLS_RSA_WITH_AES_128_CBC_SHA
0X0005	TLS_RSA_WITH_RC4_128_SHA
0X0004	TLS_RSA_WITH_RC4_128_MD5
0X000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA
0X003D	TLS_RSA_WITH_AES_256_CBC_SHA256
0XC002	TLS_ECDH_ECDSA_WITH_RC4_128_SHA
0XC003	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
0XC004	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
0XC005	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
0XC007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
0XC008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA

0XC009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
0XC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
0XC011	TLS_ECDHE_RSA_WITH_RC4_128_SHA
0XC012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
0XC013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
0XC014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
0XC00C	TLS_ECDH_RSA_WITH_RC4_128_SHA
0XC00D	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
0XC00E	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
0XC00F	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
0XC023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
0XC024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
0XC025	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
0XC026	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
0XC027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
0XC028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
0XC029	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
0XC02A	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
0XC02B	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256
0XC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0XC0A8	TLS_PSK_WITH_AES_128_CCM_8
0X00AE	TLS_PSK_WITH_AES_128_CBC_SHA256
0XC0AE	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8

11 Bureaux et support

28019 Madrid

ESPAGNE

C/ Alejandro Sánchez 109

Téléphone : +34.915602737

E-mail : contact@webdyn.com

FRANCE

26 Rue des Gaudines
78100 Saint-Germain-en-Laye

Téléphone : +33.139042940
E-mail : contact@webdyn.com

INDE

803-804 8th floor, Vishwadeep Building
District Centre, Janakpurt, 110058 Delhi

Téléphone : +91.1141519011
E-mail : contact@webdyn.com

PORTUGAL

Av. Coronel Eduardo Galhardo 7-1°C
1170-105 Lisbonne

Téléphone : +351.218162625
E-mail : comercial@lusomatrix.pt

SUPPORT

Madrid

Téléphone : +34.915602737
E-mail : iotsupport@matrix.es

Saint-Germain-en-Laye

Téléphone : +33.139042940
E-mail : support@webdyn.com

Delhi

Téléphone : +91.1141519011
E-mail : support-india@webdyn.com