



WebdynEasy LoRaWAN

Manuel d'utilisation

Index

Glossaire.....	4
Historique du document.....	6
1. Remarques concernant ce manuel	7
1.1 Champ d'application	7
1.2 Groupe ciblé	7
1.3 Références des produits et accessoires	7
1.3.1 Consignes de sécurité.....	8
1.4 Règlementation.....	8
2. Présentation générale.....	9
2.1 Le protocole LoRaWAN	9
2.2 Le concentrateur.....	10
2.2.1 Description générale	10
2.2.2 Spécifications techniques.....	13
3. Installation et Maintenance	17
3.1 Déballage.....	17
3.1.1 Contenu du produit.....	17
3.1.2 Identification du concentrateur	18
3.2 Montage.....	19
3.2.1 Ouverture/Fermeture du boîtier	19
3.2.2 Fixation murale.....	19
3.2.3 Réseau cellulaire	20
3.2.4 LoRa	22
3.2.5 Raccordement	23
4. Configuration.....	27
4.1 Interface Web embarquée.....	27
4.1.1 Connectivité du concentrateur	28
4.1.2 LoRaWAN.....	34
4.1.3 Système.....	37
4.1.4 VPN	38
4.1.5 Alarmes	41
4.1.6 Schedules.....	42

4.1.7 Modbus	47
4.1.8 Actions exécutables.....	52
5. Exploitation.....	55
5.1 Le serveur distant	55
5.1.1 Le serveur FTP	55
5.1.2 Web Service	57
5.1.3 MQTT	59
5.2 Configuration	60
5.3 Les données	62
5.4 Les alarmes.....	62
5.5 Les commandes.....	63
5.5.1 Commande « reboot »	64
5.5.2 Commande « factory »	65
5.5.3 Commande « update »	65
5.5.4 Commande « connect »	66
5.5.5 Commande « status »	66
5.5.6 Commande « log ».....	66
5.5.7 Commande « settime »	67
5.5.8 Commande « modbus »	68
5.5.9 Commande « lorawan »	69
6. Mise à jour.....	74
6.1 Locale.....	74
6.2 Distant	74
7. Annexe : Variables du fichier de configuration XML.....	75
Bureaux et support	84

Glossaire

Nom	Description
ABP	Activation By Personalization : l'activation ABP oblige d'avoir le DevAddr ainsi que les clés de sécurité du périphérique enregistré en dur dans le produit. Cette stratégie peut sembler plus simple, car vous ignorez la procédure de jointure, mais elle présente des inconvénients liés à la sécurité.
ADR	Adaptive Data Rate : c'est un mécanisme d'optimisation des débits de données (Data Rate) et la puissance d'émission radio. Cela permet une optimisation de la consommation de la batterie.
APN	Access Point Name : nom du point d'accès permettant à la passerelle de se connecter au réseau Internet par liaison mobile.
AppEUI	L'Application EUI est un identifiant applicatif unique attribué par l'organisme IEEE (EUI-64). Il est uniquement utilisé en mode OTAA et permet d'obtenir les clés du serveur lors du JOIN.
AppKEY	L'Application Key est spécifique au produit. Il est uniquement utilisé en mode OTAA et permet d'obtenir les clés du serveur lors du JOIN.
AppSKey	L'Application Session Key est spécifique au produit et permet de chiffrer bout à bout les données de l'application. À renseigner en mode ABP et calculer automatiquement lors du JOIN par le serveur en mode OTAA.
Data Rate	Le Data Rate est défini par un chiffre de 0 à 5 et fixe le type de modulation, le Spreading Factor ainsi que la bande passante utilisée.
DevEUI	Device EUI : identifiant unique attribué par l'organisme IEEE (EUI-64).
Device Address	Identifiant 32 bits de l'appareil qui identifie de manière unique le produit sur le serveur LoRaWAN. À renseigner en mode ABP et fourni automatiquement lors du JOIN par le serveur en mode OTAA.
Ftp	File Transfer Protocol : protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP.
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.
LoRa	Le LoRa est une modulation radio comprenant la liaison physique et la couche physique du modèle OSI
LoRaWAN	Le LoRaWAN est un protocole de transmission utilisant la modulation LoRa.
MD5	Message Digest 5 : fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier.
Modbus	Le Modbus est un protocole de communication couramment utilisé en industrie pour dialoguer en réseau avec des équipements industriels.
NTP	Network Time Protocol : protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale du concentrateur sur une référence d'heure.
NwkSKey	Le Network Session Key est spécifique au produit et permet de chiffrer bout à bout les données du réseau LoRaWAN. À renseigner en mode ABP et calculer automatiquement lors du JOIN par le serveur en mode OTAA.
OTAA	Over The Air Activation : l'activation OTAA est le moyen privilégié et le plus sûr de se connecter au réseau LoRaWAN. Le produit exécute une procédure de jointure (JOIN) avec le réseau, au cours de laquelle un DevAddr dynamique est attribué et des clés de sécurité sont négociées avec le produit.
PEM	Standard de format de fichier permettant de stocker les certificats et les clés privées au format texte codé en Base64.
DIN rail	Rail métallique standardisé de 35 mm utilisé en Europe dans les équipements industriels de contrôle en racks
RTU	Le mode RTU est un bus filaire en RS422/485 pour le Modbus.
Spreading Factor (SF)	Le facteur d'étalement représente la longueur des trames envoyée. Plus l'étalement du signal est important, plus le débit est faible, mais augmente la portée du produit.
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.
UDP	User Datagram Protocol : protocole non orienté connexion de la couche transport du modèle TCP/IP. Ce protocole est très simple étant donné qu'il ne fournit pas de contrôle d'erreurs (il n'est pas orienté connexion...).
VPN	Virtual Private Network : connexion sécurisée et chiffrée entre le concentrateur et un réseau privé permettant ainsi de s'isoler des réseaux de télécommunication publics.
XML	Extensible Markup Language : métalangage informatique de balisage générique. L'objectif du XML est de faciliter l'échange automatisé de contenus complexes entre systèmes d'informations hétérogènes.
XSD	XML Schema Definition : fichier permettant de valider les balises XML et les données d'un fichier XML.

Historique du document

Version	Contenu
V0.11	Création
V1.0	Ajout du VPN
V3.12	Ajout du MQTT Ajout du Mode LoRaWAN C

1. Remarques concernant ce manuel

Ce guide décrit le montage, l'installation et la configuration du concentrateur, ainsi que l'exploitation à distance.

1.1 Champ d'application

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

1.2 Groupe ciblé

Ce guide s'adresse aux installateurs et utilisateurs des concentrateurs WebdynEasy LoRaWAN mais également aux personnes utilisant nos capteurs Sens'RF LoRaWAN.

1.3 Références des produits et accessoires

Concentrateur LoRaWAN :

Références produits	Versions
WG0610-A01	WebdynEasy LoRaWAN

Capteur LoRaWAN Webdyn compatible :

Références produits	Description
WG0307-D01-EU	Sens'RF-LoRaWAN-Pulse (sans alim externe)
WG0307-D02-EU	Sens'RF-LoRaWAN-Pressure Humidity and Temperature (sans alim externe)
WG0307-D03-EU	Sens'RF-LoRaWAN-TIC (sans alim externe)
WG0307-D08-EU	Sens'RF-LoRaWAN-Analog (0-10V/4-20mA) (sans alim externe)
WG0307-D11-EU	Sens'RF-LoRaWAN-Pulse (avec alim externe)
WG0307-D12-EU	Sens'RF-LoRaWAN-Pressure Humidity and Temperature (avec alim externe)
WG0307-D13-EU	Sens'RF-LoRaWAN-TIC (avec alim externe)

1.3.1 Consignes de sécurité

Respectez impérativement toutes les consignes de sécurité figurant dans ce manuel.

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 qualifié spécialisé.
- Veuillez respecter toutes les consignes de sécurité figurant dans la documentation des équipements.



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.



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.



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.

1.4 Règlementation

The product complies with the European directives according to the EU Declaration of Conformity available from Webdyn or on website: 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

négalif 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.

2. Présentation générale

Le concentrateur WebdynEasy LoRaWAN fait partie d'une gamme de concentrateurs Webdyn dédiée aux réseaux sans fil. La fonctionnalité principale du concentrateur est d'être une passerelle LoRaWAN afin de créer son réseau LoRaWAN et de récupérer les données des différents capteurs LoRa déployés à proximité. La passerelle LoRaWAN intègre 2 modes de fonctionnement :

- Packet Forwarder
- Packet Forwarder avec serveur LoRaWAN embarqué

Le concentrateur permet également de communiquer avec des équipements Modbus en mode IP ou mode RTU.

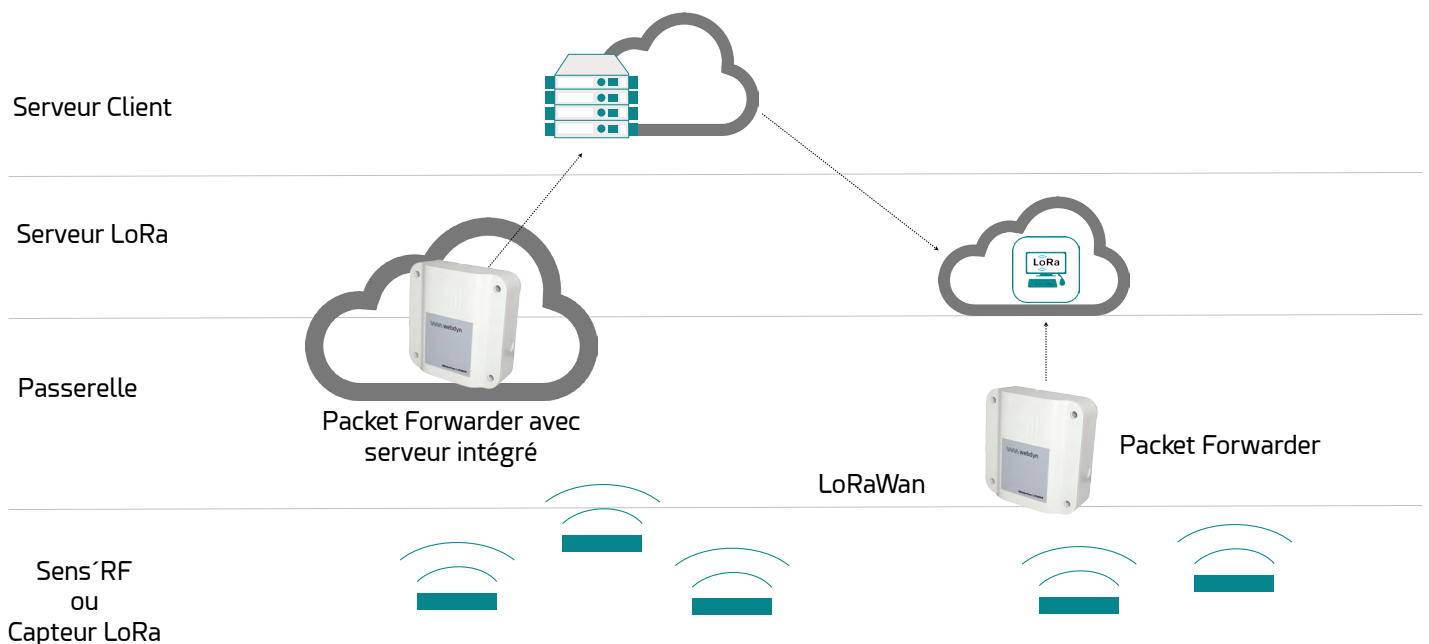


Schéma de principe d'une solution complète en LoRaWAN

2.1 Le protocole LoRaWAN

LoRaWAN est un protocole de communication s'appuyant sur la modulation LoRa. Ce protocole de communication utilise plusieurs bandes radio (ISM) utilisables sans licence dans la gamme 868 MHz en Europe. Sur un réseau LoRaWAN, les modules radio ne sont pas associés à une seule station de base. Les données qu'ils transmettent sont relayées par de multiples stations de bases. Chacune

transmettant l'information reçue d'un module radio à travers une passerelle vers le serveur de gestion. L'intelligence et la complexité sont déportées vers ce serveur qui gère la redondance d'information, la vérification de l'intégrité, la confirmation de réception, l'adaptation du débit et de la puissance d'émission des capteurs.

2.2 Le concentrateur

Le concentrateur a pour but de collecter des données en LoRaWAN et/ou en Modbus et de les transmettre périodiquement vers un serveur distant (SI) en Ethernet ou 3G/4G.

2.2.1 Description générale

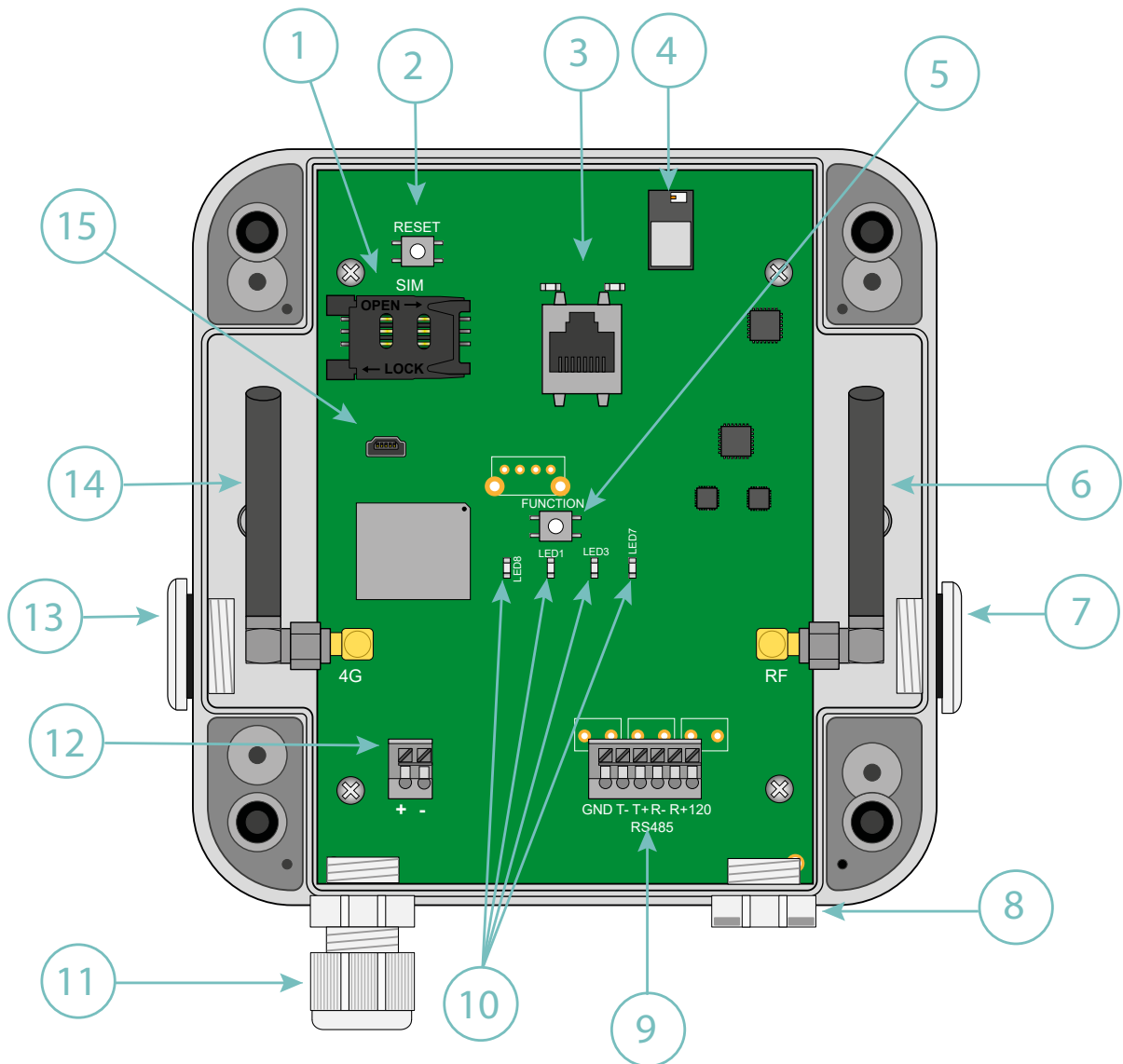
2.2.1.1 Extérieur

Face avant du boîtier :



2.2.1.2 Intérieur

Intérieur du boîtier :



1. Support carte SIM
2. Bouton Reset
3. Connecteur RJ45 avec ses Leds
4. Bluetooth BLE (évolution futur)
5. Bouton Request (identifié FUNCTION sur la carte)
6. Antenne SMA de la radio RF LoRa
7. Sortie du boîtier pour antenne externe de la radio RF LoRa (optionnel)
8. Sortie du boîtier pour RS485/422

9. 1 port RS485/422

10. Voyants :

- LED 8: Power
- LED 3: Modem
- LED 1: CPU
- LED 7: LoRa

11. Sortie du boîtier pour alimentation externe

12. Bornier pour alimentation externe 12/24V

13. Sortie du boîtier pour antenne externe du Modem 3G/4G (optionnel)

14. Antenne SMA du Modem 3G/4G

15. Connecteur mini-USB (réservé)

Voyants :

LED	Description
Power	S'allume lorsque le produit est alimenté.
CPU	S'allume suivant l'activité CPU.
LoRa	Éteinte par défaut et clignote sur trafic radio LoRaWAN.
Modem	S'allume lorsqu'une connexion IP est établie par le Modem. S'allume pendant 1 seconde sur la réception d'un SMS. Sur un appui long du bouton Request, elle indique le niveau du signal reçu (RSSI) par un nombre de clignotements (0 à 5 fois). 0 - puissance du signal ≤ -112 dBm 1 - puissance du signal entre -111 dBm et -96 dBm 2 - puissance du signal entre -96 dBm et -81 dBm 3 - puissance du signal entre -81 dBm et -66 dBm 4 - puissance du signal entre -66 dBm et -51 dBm 5 - puissance du signal > -51 dBm

Boutons :

Bouton	Description
Request	Appui court (moins de 2 secondes) => Demande de connexion. Appui long (supérieur à 2 secondes) => Affiche le niveau de réception du signal Modem (voir LED Modem). 3 appuis longs successifs dans un délai de 15 secondes => Retour usine des paramètres.
Reset	Redémarrage du concentrateur (Hard Reset).



Ne jamais faire 7 appuis du bouton RESET en moins de 30 secondes. Sinon le concentrateur se trouvera dans un mode spécial qui bloquera son démarrage. Pour sortir de ce mode, il faudra procéder à un nouveau RESET du concentrateur.






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

2.2.2 Spécifications techniques

2.2.2.1 Caractéristiques générales

Paramètres	Valeurs
Alimentation externe	+12/24V DC fournie par une alimentation externe
Consommation	10 Watts maximum
Mémoire Flash	50 Mo (partagé entre les fichiers non compressés et compressés)
Dimensions	160 x 150 x 55 mm
Boîtier	Boitier ASA IP67
Poids	0.450 kg
Température de fonctionnement	-20 °C/+55 °C
Température de stockage	-20 °C/+70 °C

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.

2.2.2.2 Caractéristiques Techniques

Paramètres	Valeurs
Interface Radio LoRa	863MHz -870MHz
Interface Modem	3G: HSPA+, UMTS (B1, B8) 4G: Cat-1, Bands B1, B3, B7, B8, B20, B28
Interface série	1 RS422/RS485 Modbus RTU port
Interface réseau Ethernet	10/100 Mbit/s

Bande RF	Fréquences Emission	Puissance Max
----------	---------------------	---------------

3G 2100MHz (B1)	1920–1980 MHz	23 dBm classe 3bis
3G 900 MHz (B8)	880–915 MHz	23 dBm classe 3bis
4G 2100 MHz (B1)	1920–1980 MHz	23 dBm classe 3
4G 1800 MHz (B3)	1710–1785 MHz	23 dBm classe 3
4G 2600 MHz (B7)	2500–2570 MHz	23 dBm classe 3
4G 900MHz (B8)	880–915 MHz	23 dBm classe 3
4G 800MHz (B20)	832–862 MHz	23 dBm classe 3
4G 700MHz (B28)	703–748 MHz	23 dBm classe 3

2.2.2.3 Caractéristiques LoRa

Paramètres	Valeurs
Canaux	8 canaux simultanés : <ul style="list-style-type: none"> • 863-870 MHz (Europe) • 865-867 MHz (Inde)
Sensibilités max	-141dBm (125kHz en SF12)
DataRate supporté	DR0-DR5
Bandwith supporté	125/250 kHz
TX power max	+14dBm
Mode d'activation	ABP ou OTAA
Fréquences par défaut	Europe: 867.1 MHz, 867.3 MHz, 867.5 MHz, 867.7 MHz, 867.9 MHz, 868.1 MHz, 868.3 MHz, 868.5 MHz Inde: 865.0625 MHz, 865.4025 MHz, 865.985MHz

2.2.2.4 Caractéristiques logicielles

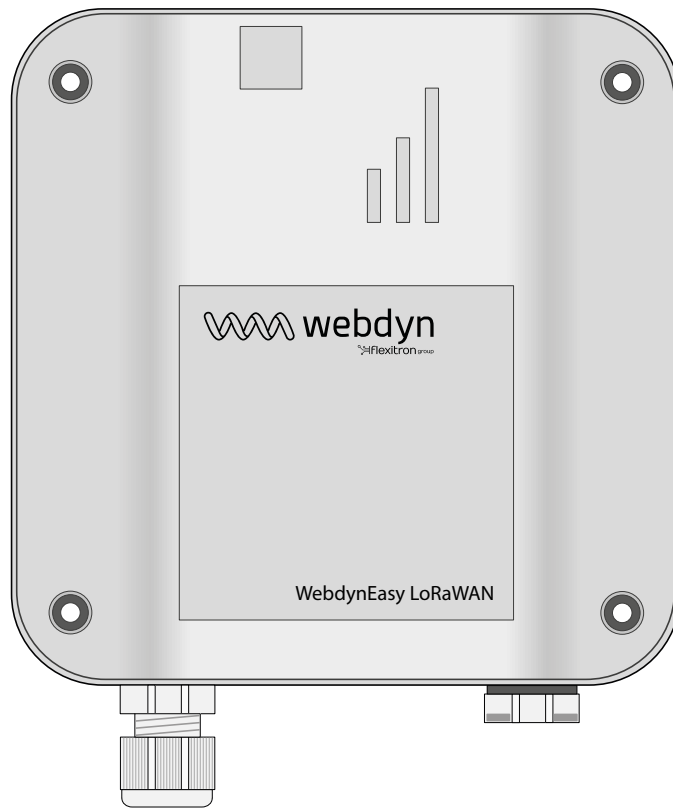
Paramètres	Valeurs
Serveur LoRaWAN	<ul style="list-style-type: none">• Protocole LoRaWAN V1.0.2 classe A• 1000 capteurs LoRaWAN supportés• 10 passerelles supportées
Modbus	Monitoring in RTU and TCP mode
OpenVPN	V2.5.4

3. Installation et Maintenance

3.1 Déballage

3.1.1 Contenu du produit

Avant toute installation, commencer par vérifier le contenu. Si la livraison est incomplète ou endommagée, veuillez-vous rapprocher du support Webdyn. (voir chapitre 7 : « Support »).



Concentrateur WebdynEasy LoRaWAN

(Réf. : WG0610-A01)

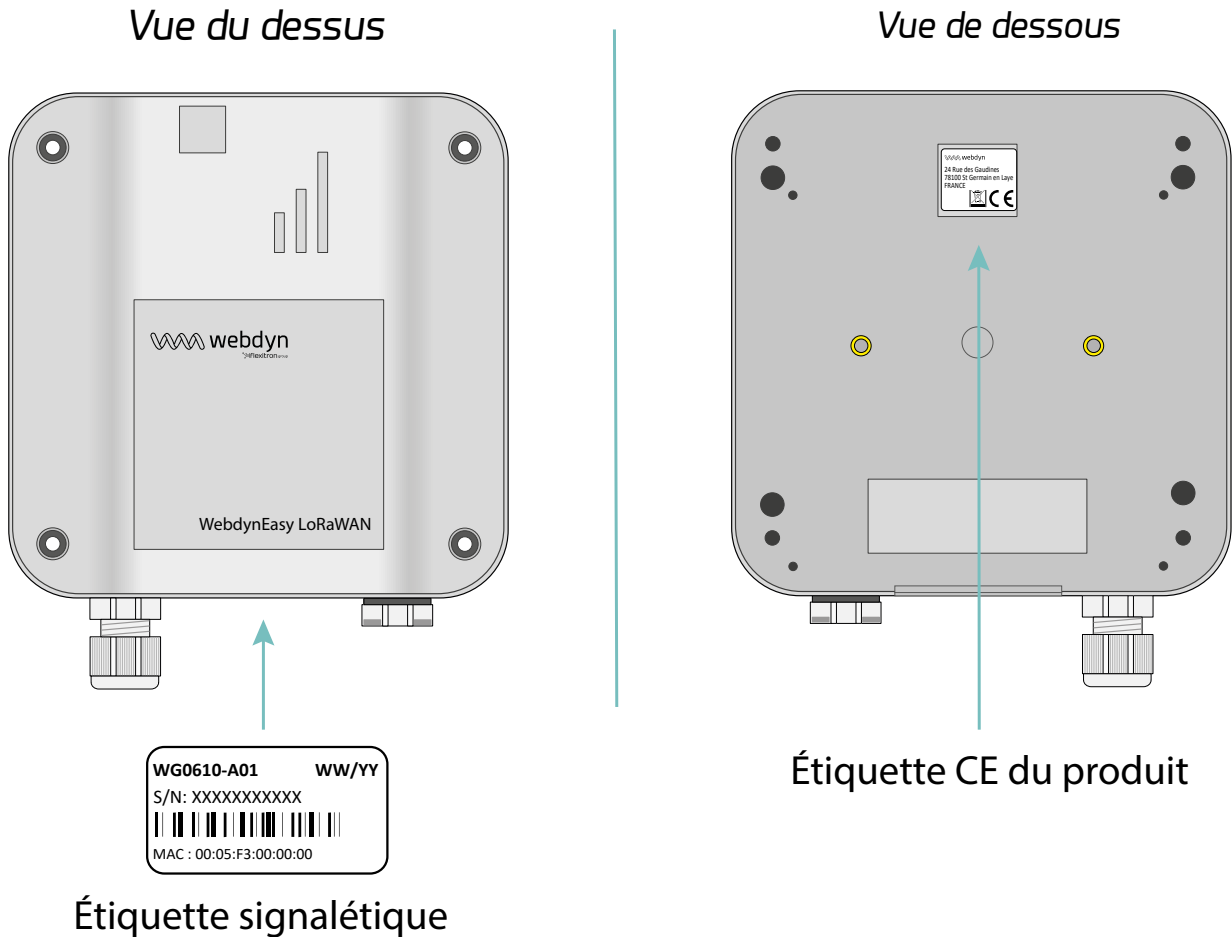
Sont livrés avec le concentrateur :

- Une antenne SMA coudée pour le modem (interne).
- Une antenne SMA coudée pour la radio (interne).

3.12 Identification du concentrateur

Étiquette signalétique :

Vous pouvez identifier le concentrateur WebdynEasy LoRaWAN grâce à son étiquette signalétique, qui se trouve sur le boîtier.



Cette étiquette contient :

- Nom du produit (WG0610-A01).
- La date de production (sous la forme SS/AA en haut à droite).
- Le N° de série en clair et en code-barre 128.
- L'adresse MAC (Ethernet) en clair.

Version du logiciel :

Vous trouverez la version du logiciel sur l'interface Web du concentrateur. La version du logiciel est indiquée dans l'onglet « Overview » (Voir chapitre 5.1.1 : « Connectivité du concentrateur »).

3.2 Montage

Avant toute installation, il est important de respecter les conditions environnantes décrites dans le chapitre 2.2.2.1 : « Caractéristiques générales » ainsi que ces conditions :

- Protégez le produit contre la poussière, l'humidité, les substances agressives et la condensation.
- La distance entre la concentrateur et les équipements Modbus ne doit pas dépasser la distance maximale autorisée pour le type d'interface correspondant (RS485 ou RS422) (Voir chapitre 3.2.4.2 : « Bus RS485/RS422 »).
- En cas d'utilisation de la liaison Modem, veillez à ce que la réception soit optimale lors du montage. Vérifier le RSSI qui est accessible sur la page web embarquée (voir chapitre 4.1.1.1 : « Modem »).



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

3.2.1 Ouverture/Fermeture du boîtier

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

Si le boîtier est fixé au mur :

- Ouvrez les 2 trappes sur la face avant.
- Dévissez les 4 vis de la fixation murale dans les logements sous les trappes.

Puis suivez ces étapes :

- Dévissez les 4 vis qui se trouvent derrière le boîtier.
- Retirer le capot.

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

- Mettre en place le capot sur le socle du boîtier, veillez à ce que le joint d'étanchéité soit bien en place.
- Vissez les 4 vis qui se trouvent derrière le boîtier.

3.2.2 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 3.2.1 : « 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 4 et longueur 25 mm au min.).

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

- Ouvrez les 2 trappes sur la face avant.
- Vissez les 4 vis de la fixation murale dans les logements sous les trappes.
- Refermez les 2 trappes sur la face avant.

3.2.3 Réseau cellulaire

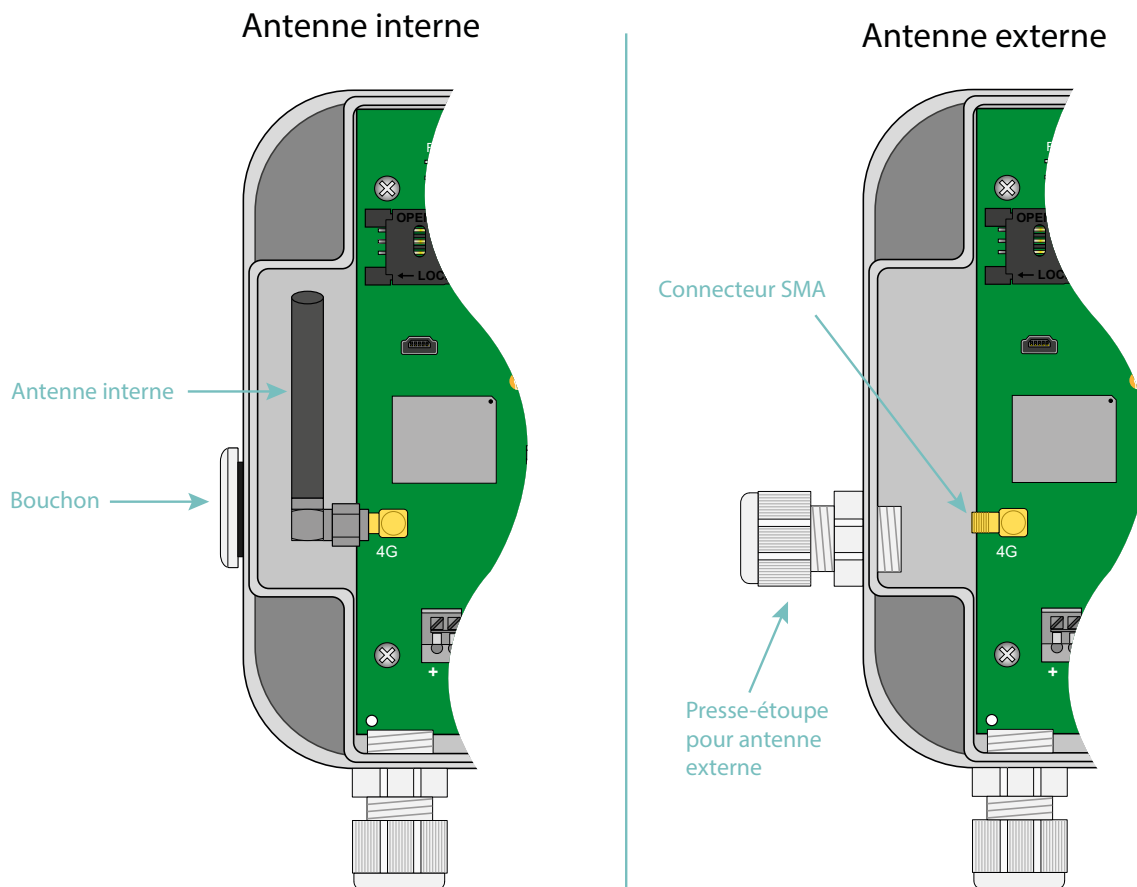
Le concentrateur WebdynEasy intègre un modem compatible avec les réseaux 3G et 4G.

3.2.3.1 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.





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

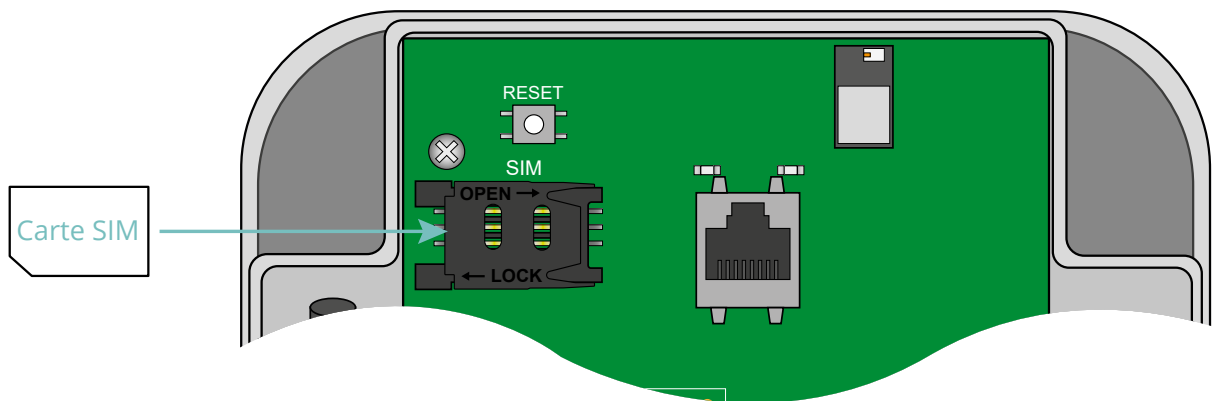
3.2.3.2 Carte SIM

Pour utiliser la liaison Modem 3G ou 4G et permettre au concentrateur de communiquer avec le serveur distant, il faut procéder à l'ouverture du boîtier (voir chapitre 3.2.1 : « 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 :

- Possibilité de recevoir et d'envoyer des SMS.
- Communication 3G et 4G 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 3G et LTE-M.



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

Par défaut, la configuration du concentrateur ne demande pas de code PIN (PIN Mode : Off). Si vous voulez activer le code PIN du concentrateur, il est préférable de le configurer avant la mise en place de la carte SIM. (voir chapitre 4.1.1 : Connectivité du concentrateur)

Trois cas sont possibles :

- Le code PIN est désactivé : la communication modem est active.
- Le code PIN est activé et le code PIN saisi est correct : la communication modem est active.
- Le code PIN est activé et le code PIN saisi est incorrect : la communication modem est en erreur.

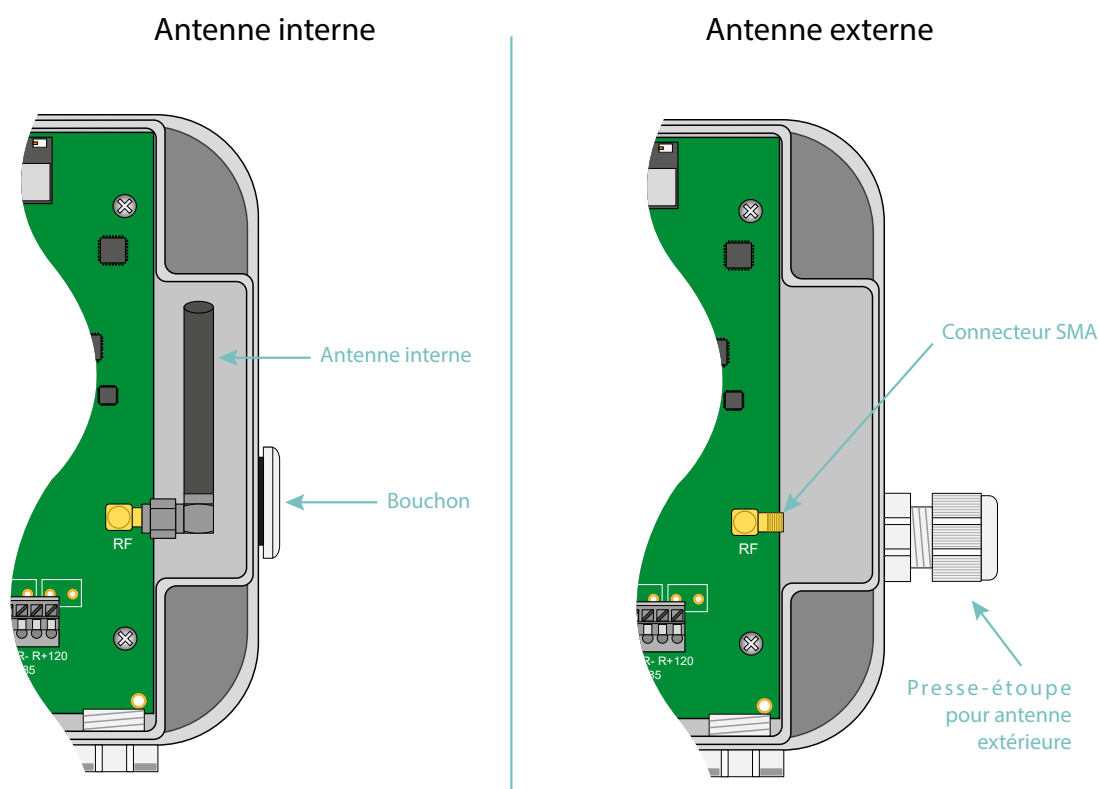


Si la carte SIM a un code PIN activé et qu'il est incorrect au premier démarrage du concentrateur, elle sera bloquée après 3 tentatives. Vous pouvez la débloquer en utilisant un téléphone portable avec le code PUK fourni par votre opérateur.

3.2.4 LoRa

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 (armoire métallique, poutrelles...) ou béton (béton armé, murs...) qui atténue énormément l'onde radio.



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

3.2.5 Raccordement

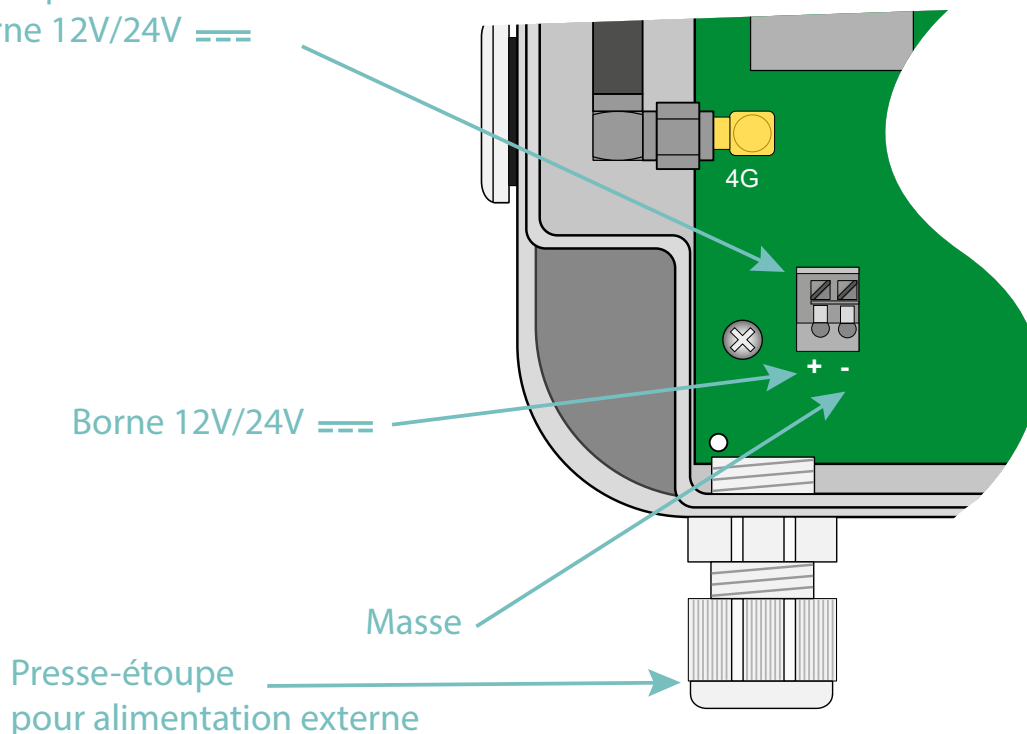
3.2.5.1 Alimentation

Le concentrateur WebdynEasy doit être alimenté en 12V ou 24V continu. L'alimentation est réalisée via le bornier J11 situé en bas à gauche de la carte.



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 l'alimentation
externe 12V/24V 



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 10Watts minimum.

3.2.5.2 Bus RS485/RS422

Le bus de communication RS485/RS422 est utilisé uniquement pour le modbus en mode RTU, il est sérigraphié RS485 en bas à droite de la carte. Cette interface est compatible Half Duplex (2 fils) et Full Duplex (4 fils).

Dans le cas de raccordement de plusieurs équipements modbus RTU, il faut procéder à un câblage « en série ». Le câble arrive à un module modbus et en repart vers le suivant.

Afin d'assurer le bon fonctionnement du bus de données, un bus RS485 doit être terminé aux deux extrémités par un bouchon 120 Ohms. Le concentrateur WebdynEasy peut se trouver à l'extrémité du bus de communication RS485 ou en milieu de bus. Le concentrateur intégrant une résistance de 120 Ohms, suivant le positionnement du concentrateur sur le bus, il sera peut-être nécessaire de les activer. (Voir le câblage)

Pour le choix du type de câble, il y a 3 cas distincts sont à considérer :

- Sur les installations nécessitant de courtes longueurs et sans interférences électriques, prévoir un câble 2 paires 6/10 rigide écranté.
- Sur les installations plus importantes dont la longueur de câble ne dépasse pas 500 m, prévoir un câble 2 paires 8/10 rigide écranté.
- Lorsque la distance de câble dépasse 500 m et, a fortiori, en cas d'interférences électriques, prévoir un câble blindé 2 paires de 0,34 mm² de section.



La longueur maximum du bus RS485 est de 1000 mètres.



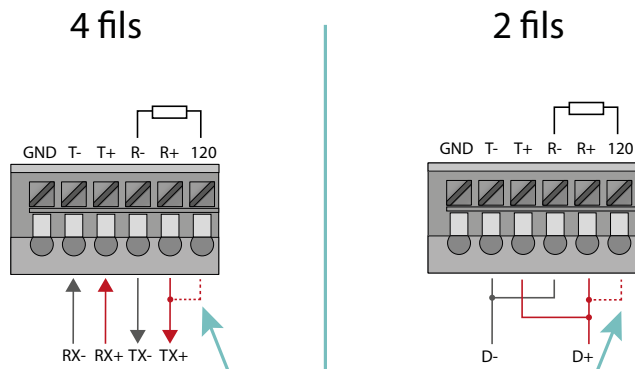
Recommandations relatives au câblage du BUS RS485/RS422 :

- Les modules doivent être raccordés les uns après les autres.
- Les raccordements en étoile sont interdits.
- Les câbles doivent être obligatoirement écrantés ou blindés, torsadés paire par paire (voir ci-dessus : "type de câble pour la liaison bus RS485").
- L'écran ou le blindage du câble doit être connecté au plan de masse du boîtier du concentrateur et non au 0 V (ne relier qu'une extrémité de l'écran).
- Éviter tout aller-retour dans le même câble.

Câblage RS485 du côté concentrateur:

- Dénudez la gaine du câble de communication RS485 sur environ 4 cm.
- Raccourcissez le blindage jusqu'à la gaine de câble.
- Dénudez les fils sur environ 6 mm.
- Raccordez les conducteurs au bornier repéré RS485 en respectant les affectations dans votre bus de communication RS485.

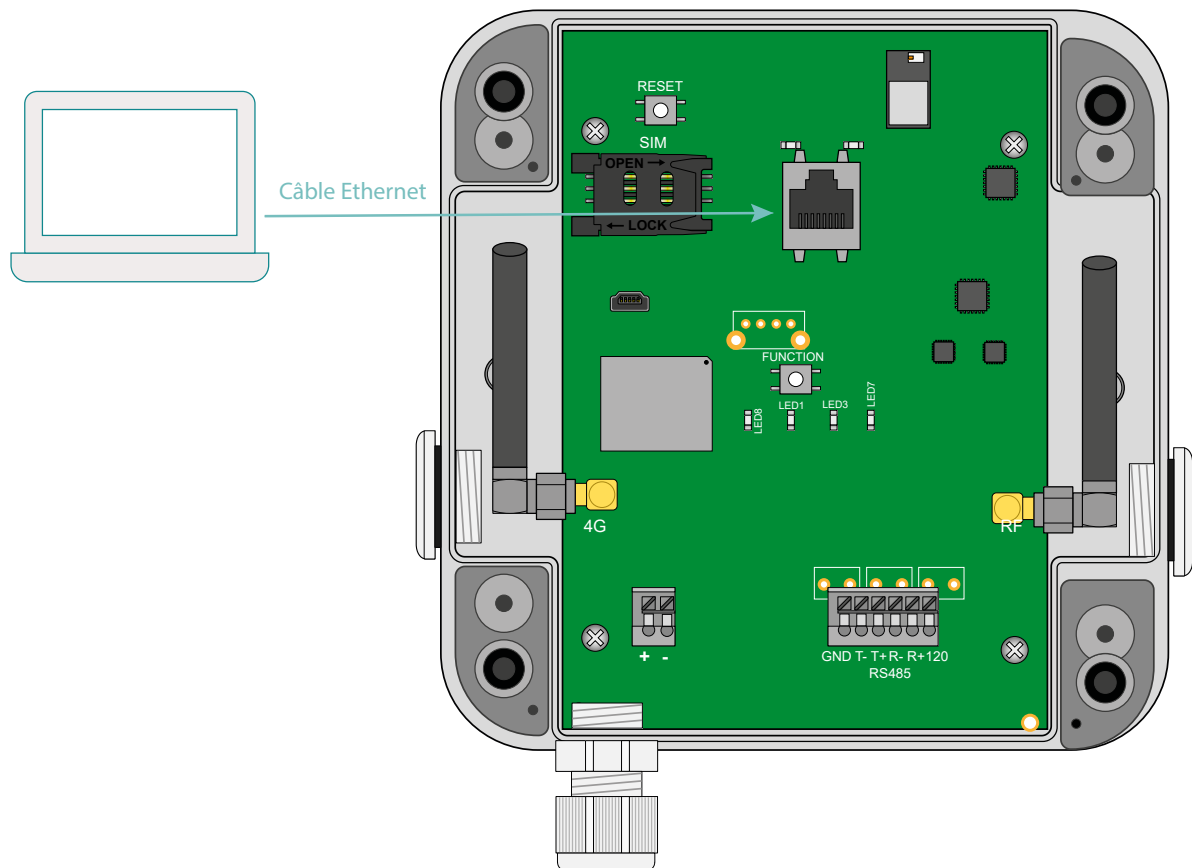
Montage en RS485/RS422 :



A câbler uniquement si le concentrateur est placé en bout de ligne

3.2.5.3 Ethernet

Pour configurer le concentrateur, il faut d'abord ouvrir le boîtier afin de pouvoir accéder au connecteur RJ45 (voir chapitre 3.2.1 : « Ouverture/Fermeture du boîtier »). Une fois ouvert, relier le concentrateur à l'ordinateur par l'intermédiaire d'un câble Ethernet.



Il est nécessaire de configurer une adresse IP fixe sur l'ordinateur dans la même plage d'adresse IP, et dans le même sous réseau, que le concentrateur WebdynEasy LoRaWAN.



Les paramètres de configuration IP par défaut du concentrateur WebdynEasy LoRaWAN sont les suivants:

Adresse IP : 192.168.1.12

Masque de sous réseau : 255. 255. 255.0

DHCP : Désactivé

L'étape suivante permet de configurer l'adresse réseau d'un PC pour accéder au concentrateur WebdynEasy LoRaWAN:

Configuration d'une deuxième adresse IP sur le PC :

- Sous Windows 10, cliquez sur Démarrer/Paramètres/Réseau et Internet. La fenêtre « Etat du réseau » s'affiche.
- Cliquez sur « Ethernet » à gauche de la fenêtre, puis « Centre réseau et partage à droite ».
- La fenêtre « Centre Réseau et partage » s'affiche.
- Cliquez sur connexions « Ethernet ». La fenêtre « Etat de Ethernet » s'affiche
- Cliquez sur « Propriétés ».
- Sélectionnez « Protocole Internet (TCP/IPv4) » puis cliquez sur le bouton « Propriétés ».
- Cliquez ensuite sur « Avancé ».
- Dans la zone « Adresse IP » cliquez sur « Ajouter ».
- Entrez l'adresse IP 192.168.1.xxx (xxx entre 1 et 254 et différent de 12) et le masque de sous-réseau 255. 255. 255.0.
- Cliquez sur « Ajouter ».
- Pour valider les réglages, cliquez sur OK dans chacune des trois fenêtres.
- Fermez la fenêtre Connexion réseau et accès à distance.

Maintenant, il est possible de modifier facilement la configuration du concentrateur en passant par son interface web embarquée en utilisant le navigateur web de l'ordinateur. (Voir chapitre 4.1.1 : « Connectivité du concentrateur »).

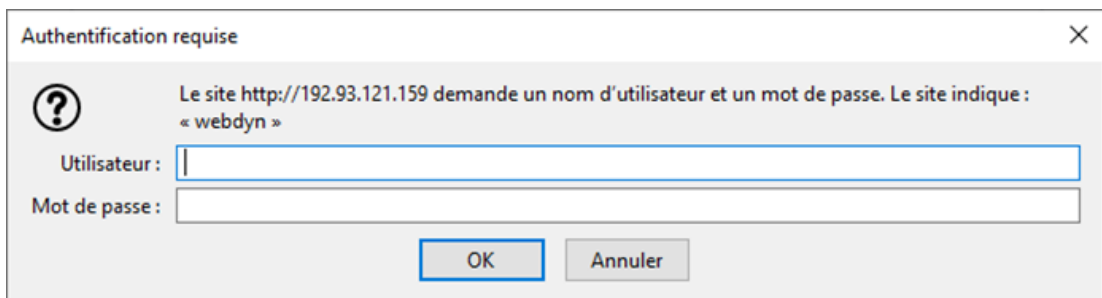
4. Configuration

La 1ère configuration du concentrateur WebdynEasy LoRaWAN est réalisée via l'interface Web intégrée au produit.

4.1 Interface Web embarquée

Pour accéder à l'interface web embarquée du concentrateur, suivez les étapes suivantes :

- Lancez le navigateur web : l'interface web est compatible avec les dernières versions des navigateurs : Firefox, Chrome et Edge. Les versions plus anciennes peuvent fonctionner, mais ne sont plus supportées (par exemple IE 7).
- Saisissez l'adresse IP du concentrateur dans votre navigateur web (par défaut, l'adresse est : <http://192.168.1.12>) afin d'accéder à la page d'accueil de la WebdynEasy LoRaWAN.
- Une fenêtre d'identification doit s'afficher :



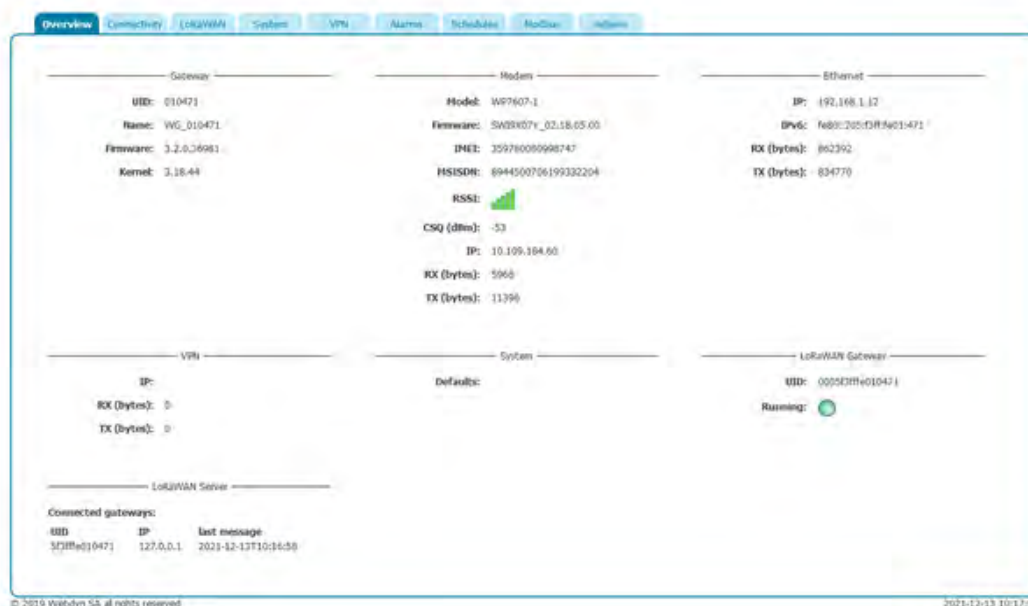
Saisissez votre identifiant et le mot de passe:

Identifiant	Mot de passe	Restrictions
admin	high	Aucune
install	medium	System, LoRaWAN, Modbus, Actions Schedules en lecture uniquement
data	low	Actions uniquement



Mot de passe : pour sécuriser l'accès au concentrateur, il est très fortement recommandé de modifier les mots de passe par défaut après la première configuration. La modification des mots de passe se fait par le fichier XML de configuration (voir : « Annexe A : Variables »).

- La page d'accueil s'affiche :



« Overview » permet d'obtenir une vue d'ensemble du fonctionnement de WebdynEasy LoRawan.



Si l'accès aux pages web est effectué pendant la phase d'initialisation du concentrateur,



le logo s'affiche. Attendre que le concentrateur soit complètement initialisé pour accéder aux pages web.

4.1.1 Connectivité du concentrateur

« Connectivity » permet de configurer le concentrateur afin qu'il communique avec le serveur distant.

4.1.1.1 Modem

Modem

PIN Mode:	<input type="text" value="Off"/>
PIN Code:	<input type="text" value="1234"/>
APN:	<input type="text" value="tm"/>
Login:	<input type="text"/>
Password:	<input type="text"/>
Mode:	<input type="text" value="AlwaysOn"/>
Disconnect delay (s):	<input type="text" value="60"/>

Paramètres	Description
PIN Mode	Off : Le code PIN de la carte SIM doit être désactivé Manual : Le code PIN de la carte SIM doit être renseigné dans la case PIN Code
PIN Code	Code PIN de la carte SIM à renseigner si Manual est sélectionné dans PIN Mode
APN	Nom de l'APN de votre opérateur mobile (obligatoire pour une connexion IP)
Login	Nom d'utilisateur de votre opérateur mobile (facultatif selon l'opérateur)
Password	Mot de passe de votre opérateur mobile (facultatif selon l'opérateur)
Mode	OnDemand : Le concentrateur établit la connexion uniquement lorsqu'il doit communiquer avec le serveur distant. Il la coupe lorsque le transfert de données est terminé après un délai configurable dans Disconnect delay. AlwaysOn : Le modem est toujours connecté. Le concentrateur utilise en permanence le modem pour toutes les communications en IP. AlwaysOff : Ce mode est à utiliser en cas de connexion avec le serveur distant via Ethernet, mais avec une carte SIM insérée dans le concentrateur. La connexion ne se fait jamais via le modem, mais le concentrateur peut recevoir des SMS entrants et émettre des SMS.
Disconnect delay (s)	Valeur en seconde du délai d'attente en mode OnDemand entre la fin des échanges de données et la fin de connexion.



Consultez votre opérateur mobile pour obtenir les informations (APN, login, mot de passe) relatives à votre carte SIM.

4.1.1.2 Ethernet

Ethernet

IP: • • •

Netmask: • • •

Gateway: • • •

Use DHCP

DNS

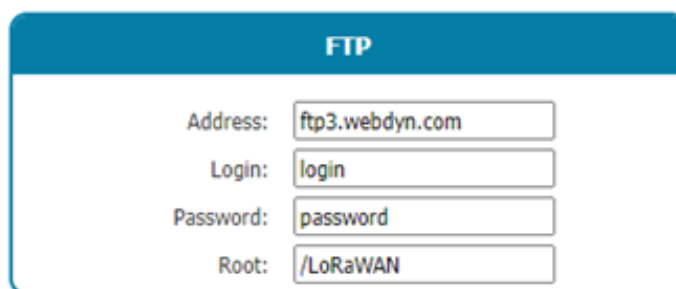
DNS servers: • • •

Paramètres	Description
IP	Adresse IP à laquelle le concentrateur WebdynEasy LoRaWAN est accessible via le réseau Ethernet.
Netmask	Masque de sous-réseau de votre réseau Ethernet. Ce masque limite le réseau Ethernet à des adresses IP définies, et sépare les plages réseau les unes des autres.
Gateway	Adresse de la passerelle de votre réseau Ethernet. L'adresse de la passerelle est l'adresse IP de l'appareil qui établit la connexion à Internet. En général, l'adresse entrée ici est celle de votre routeur ADSL/fibre.
Use DHCP	Vous avez la possibilité d'obtenir les paramètres Ethernet automatiquement si l'infrastructure du réseau le permet. Dans ce cas sélectionnez le mode dynamique et reportez-vous à la configuration de votre serveur DHCP pour connaître l'adresse IP de votre concentrateur.
DNS servers	Liste des serveurs DNS. Le serveur DNS (Domain Name System) traduit les adresses Internet explicites (par ex. www.webdyn.com) en adresses IP correspondantes. Entrez ici les adresses des serveurs DNS que vous avez reçus de votre fournisseur d'accès à l'Internet (FAI). Vous pouvez également entrer l'adresse IP de votre routeur. Vous pouvez également utiliser le DNS google : « 8.8.8.8 »



Le concentrateur ne peut utiliser la liaison Ethernet pour accéder au serveur que si la connexion via modem est désactivée (« off » ou « alwaysoff »). Dans le cas contraire, le concentrateur tentera de se connecter via la liaison modem.

4.1.1.3 FTP

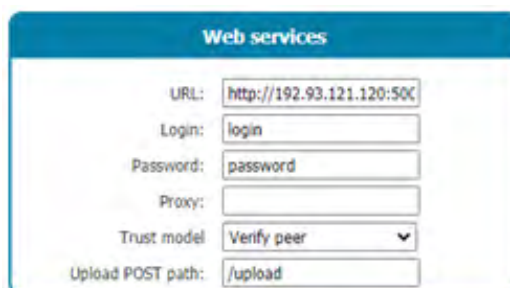


Paramètres	Description
Address	Adresse IP ou nom du serveur FTP distant (Port par défaut : 21). Possibilité de modifier le port du FTP en rajoutant « : » puis le numéro de port.
Login	Nom d'utilisateur utilisé par le concentrateur pour la connexion au serveur FTP distant
Password	Mot de passe utilisé par le concentrateur pour la connexion au serveur FTP distant
Root	Répertoire de racine sur le serveur FTP distant



L'arborescence des répertoires sur le serveur FTP distant est à créer avant toute connexion FTP. (voir chapitre 5.1.1.1 : « Le serveur FTP : Paramétrage »).

4.1.1.4 Web Services



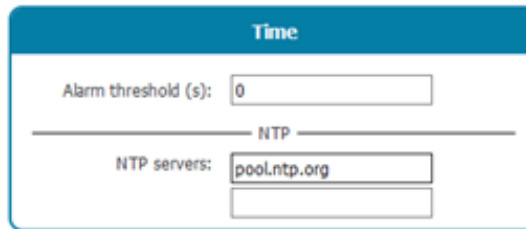
Paramètres	Description
URL	Adresse IP ou nom du serveur web distant (Port par défaut : 80). Possibilité de modifier le port du serveur web en rajoutant « : » puis le numéro de port.
Login	Nom d'utilisateur utilisé par le concentrateur pour la connexion au serveur web distant.

Password	Mot de passe utilisé par le concentrateur pour la connexion au serveur web distant.
Proxy	Adresse IP ou nom d'hôte du proxy (Port par défaut : 1080). Possibilité de modifier le port du proxy en rajoutant « : » puis le numéro de port. Le proxy est optionnel si celui-ci n'est pas utilisé, le champ vide doit être vide.
Trust model	Vérification des certificats d'authentification (uniquement pour les connexions sécurisées HTTPS) : <ul style="list-style-type: none"> • Verify peer : Vérification des certificats d'authentification. • Trust peer : Accepte tous les certificats d'authentification (non recommandé).
Upload POST path	Chemin d'accès sur le serveur web distant.

4.1.1.5 MQTT

Paramètres	Description
<i>Address</i>	Adresse IP ou nom du serveur web distant (Port par défaut : 1883) Possibilité de modifier le port du serveur mqtt en rajoutant « : » puis le numéro de port
<i>Client ID</i>	Identifiant MQTT du client
<i>Login</i>	Nom d'utilisateur utilisé par le concentrateur pour la connexion au serveur MQTT distant
<i>Password</i>	Mot de passe utilisé par le concentrateur pour la connexion au serveur MQTT distant
<i>Keepalive interval [s]</i>	Temps en secondes d'envoi de trame de maintien de connexion
<i>Topic</i>	Topic des messages MQTT utilisé
<i>Trust model</i>	Vérification des certificats d'authentification (uniquement pour les connexions sécurisées MQTTS) : <ul style="list-style-type: none"> • Verify peer : Vérification des certificats d'authentification. • Trust peer : Accepte tous les certificats d'authentification (non recommandé)

4.1.1.6 NTP

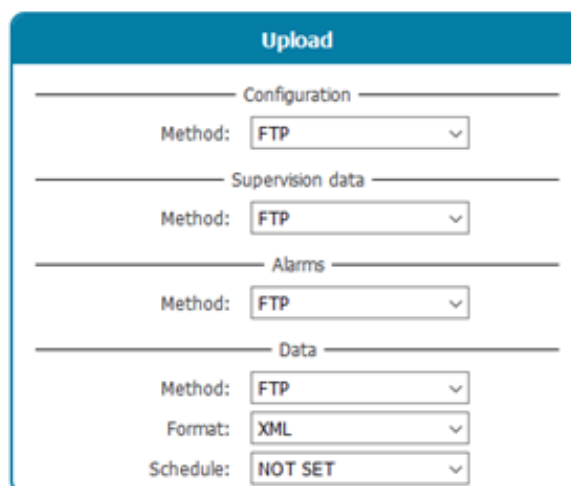


Paramètres	Description
Alarm threshold (s)	Différence en seconde entre l'heure du concentrateur et l'heure de synchronisation NTP au-delà de laquelle une alarme est émise.
NTP servers	Adresses des serveurs NTP utilisés pour la synchronisation de l'horloge du concentrateur.



A la première connexion, la synchronisation NTP est réalisée et la prochaine synchronisation NTP sera effectuée lors d'une autre connexion après un temps minimum. Le temps minimum entre les synchronisations NTP est configurable via la variable « min_sync_interval. » en secondes.

4.1.1.7 Upload



Le concentrateur peut déposer sur le serveur distant les données suivantes :

Noms	Description	Format
Configuration	Données de configuration du concentrateur	• XML
Supervision data	Données de supervision du concentrateur	• XML
Alarms	Alarmes	• XML
Data	Données LoRaWAN et/ou modbus	• XML • JSON

Pour chaque type de donnée, le concentrateur peut déposer les données par :

- FTP
- Web Service



Si des commandes sont envoyées par Web Service, le concentrateur répond aux commandes par le biais d'alarmes. Il est nécessaire dans ce cas de configurer les alarmes en Web Service.

Le dépôt des données doit être associé à un Schedule en renseignant son identifiant unique configuré (voir chapitre 4.1.6 : « Schedules »).



Consultez le chapitre 5.2 : « La configuration » pour connaître le format et le contenu des fichiers de configuration, de supervision, d'alarme et de données.



L'arborescence des répertoires sur le serveur FTP distant est à créer avant tout dépôt de fichier. (voir chapitre 5.1.1.1 : « Le serveur FTP : ParamétrageParamétrage »).

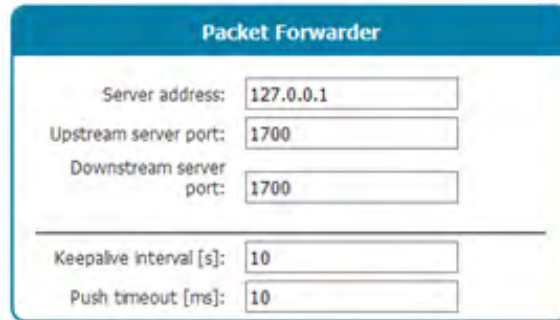
4.1.2 LoRaWAN

L'onglet « LoRaWAN » permet de configurer le Packet Forwarder et le serveur LoRaWAN. Ces 2 parties sont complètement indépendantes. Le Packet Forwarder peut être utilisé avec un serveur distant et le serveur LoRaWAN embarqué peut utiliser un Packet Forwarder externe.

4.1.2.1 Packet Forwarder

En mode Packet Forwarder, la WebdynEasy LoRaWAN prend le rôle de passerelle. La passerelle est en écoute permanente sur l'interface radio LoRa et transmet toutes les trames reçues via une connexion IP au serveur LoRaWAN (distant ou embarqué).

Pour que le Packet Forwarder fonctionne, il doit établir une connexion IP permanente avec le serveur à travers son interface Ethernet ou Modem en mode AlwaysOn.



Packet Forwarder

Server address: 127.0.0.1

Upstream server port: 1700

Downstream server port: 1700

Keepalive interval [s]: 10

Push timeout [ms]: 10

Paramètres	Description
Server address	Adresse IP ou nom du serveur LoRaWAN. Pour utiliser le serveur LoRaWAN embarqué du concentrateur, il faut utiliser l'adresse suivante : « 127.0.0.1 »
Upstream server port	Numéro de port UDP sortant du packet Forwarder
Downstream server port	Numéro du port UDP entrant du packet Forwarder
Keepalive interval [s]	Temps en secondes d'envoi de trame de maintien de connexion
Push timeout [ms]	Temps d'attente maximum en millisecondes pour l'acquittement de la trame envoyée au serveur LoRaWAN.



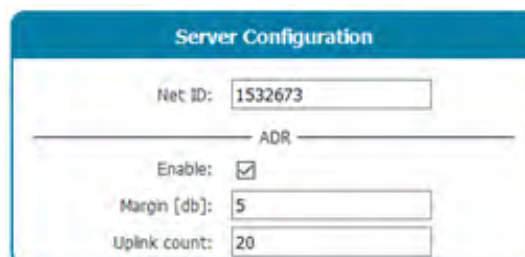
Le packet Forwarder supporté est celui de Semtech.

4.1.2.2 Serveur LoRaWAN

Le serveur LoRaWAN gère les capteurs LoRaWAN en tant que réseau privé. Il inclut toutes les fonctions du réseau LoRaWAN (passerelle, serveur LoRaWAN et serveur d'application). Toutes les données reçues sont stockées dans des fichiers et à chaque connexion au serveur distant, toutes les données disponibles seront déposées.



Pour utiliser le Packet Forwarder du concentrateur, renseigner dans « Server address » l'adresse IP suivant : « 127.0.0.1 ». Vérifier également que les ports du serveur (« Upstream server port » et « Downstream server port ») sont à 1700.



Server Configuration

Net ID: 1532673

ADR

Enable:

Margin [db]: 5

Uplink count: 20

Paramètres	Description
Enable	Cocher pour activer l'ADR (Adaptative Data Rate)
Margin [dB]	Marge en dB pour le calcul de l'ADR compris entre 1 et 30
Uplink count	Le nombre de Uplink nécessaire pour l'ADR compris entre 1 et 65535
Uplink count	The number of uplinks needed for ADR between 1 and 65535 included.



Afin d'optimiser les piles des capteurs et la bande passante LoRAWAN, il est fortement recommandé de laisser activer l'ADR et la configuration par défaut du Margin et uplink count.



Pour le calcul de l'ADR, le concentrateur a besoin au minimum de 20 uplinks, c'est-à-dire que la variable Uplink Count est utilisée après les 20 premiers uplinks reçus par le concentrateur avant d'envoyer des commandes ADR au capteur LoRaWAN.

Capteur LoRaWAN :

Le serveur supporte les 2 modes activations :

- ABP (Activation By Personalization) : les paramètres DevAddr, NwkSKey et AppSKey doivent être renseignés.
- OTAA (Over The Air Activation) : les paramètres DevEUI et AppKey doit être renseigné, les clés AppSKey et NwkSKey sont générées et sauvegardées au moment du JOIN.

Paramètres	Description	ABP	OTAA
DevEUI	Identifiant unique du capteur (EUI64) en hexadécimal de 8 octets	vides	•
AppKEY	Clé de chiffrement en hexadécimal de 16 octets qui est utilisé par le réseau pour dériver les clés de session.	vide	•

DevAddr	Adresse du capteur en hexadécimal de 4 octets	•	auto
AppSKey	Clé de chiffrement entre le capteur et le serveur applicatif en hexadécimal de 16 octets	•	auto
NwkSKey	Clé de chiffrement entre le capteur et le serveur LoRaWAN en hexadécimal de 16 octets	•	auto



L'AppEUI n'est pas utilisé par le serveur embarqué du concentrateur.

Les données des capteurs LoRaWAN sont déposées soit au format XML ou soit au format JSON (voir chapitre 4.1.1.6 : « Upload ») dans le répertoire DATA pour le serveur FTP distant (voir chapitre 5.3 « Les données »).

4.1.3 Système

Lorsque le protocole Modbus est activé sur le port RS485, les paramètres du port série doivent être définis.

Paramètres	Description
Mode	Off : RS485 désactivé Modbus : RS485 activé en mode Modbus
Baudrate	4800 9600 19200 (valeur par défaut) 38400 57600 115200

Data bits	5 6 7 8 (valeur par défaut) 9
Parity	None Odd Even (valeur par défaut)
Stop bits	1 (valeur par défaut) 2

4.1.4 VPN

Le concentrateur supporte le VPN d'OpenVPN V2.5.4 (<https://openvpn.net/>).

OpenVPN

Enable:

Protocol:

Server

Address:

Port:

Cipher:

Auth:

CA:

```
-----BEGIN CERTIFICATE-----
MIIFMTCCAxmgAwIBAgIJALZAhXiaEan1MA0GCSqGSIb3DQEBCwUAMBQx
EjAQBgNVBAMMCVdYmR5biBDQTAGFw0xOTA2MTcxMTQzMTJGaG8yMTE
SMDUyNDEuNDMxMlowFDESMBAGA1UEAwVjV2VjZHUuIENBMIIiCjANBgkq
hkG9w0BAQEFAAOCAg8AMIICCgKCAgEApTNkOoFT+HpF54vAlmUd2upT
YgobjfQ0No51LxNLC79WFRydnwcf4sdGHveJXIZ3zGCFvDuzKabwJpS38YFB
nR9qWJPlkDcB57+MFsay4QFBRzQ8O+Ibya4boLKRRi6Ivw0oLRi5vWSpfBsD
Td36cvEq5Vp857Vzf44EJhbDGHhIaGmSjwZSk5IG9+IqbRBUD+/m3eZzu
Dz2A8abvc1Px3mnNpF0vUslP4kG2+nz4V9R2oXuoU6HSqjPC4YoaF6YEP
xXFLyGbZKGrEa0zvTc7QFTsQooYIL7aRMOuwgiWF4IzWaEU+o6rZXvFHLp
TmaYk/ciaalGNJwdTfaca8Wfyu3Za2lkhRa0KEFL9II
```

Cert:

```
-----BEGIN CERTIFICATE-----
MIIFUzCCAzugAwIBAgIQObracQvrfPFZktu0g33L8TANBgkqhkiG9w0BAQsF
ADAUMRIwEAYDVQQDDAIXZWJkeW4gQ0EwHhcNMjAwMzE5MTA1MDQ1
WhcNMzAwMzE5MTA1MDQ1WjAIFMR0wGwYDVQQDDBRzZWVudWJhcnR
pc3RlWxhcHRvcDCCAlwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAN
C8HfXtk2L8632P2e4SjtucTYy+WhOcoOr8M6KgNTQayVTU9jcoBpQDM
E6jLQo2nqeefp+bsApGow3wzTRpQStJcsXqsrzXr2Cja/Def8BBVU0BI1PD
WPMqDrEVkrvgZqfkZ5vJemEvAwOeWaf9NaMIL
/jehWIAA9EeEkgSgqLxW54E0
/grYldBgmIE1ROUEX7JWQKR6DRUaMyNTQtXbMHMCh0CTzeToy5bRQWU
NJO2Omh5IvnAemvOCh6vexrLvz1Cak69tAxP6cIFRzuQI0pidahxo5w0UP3
```

Key:

```
-----BEGIN RSA PRIVATE KEY-----
MIIDKgIBAAKCAgEA0Lwd/GVOTYvzrfY
/Z7hImW25xNjLSaESygg6vwwzoqA1NBRJvNT2NyhulAMwTqMtCjaep55+n5u
wCkajDFclNNGIBK0lyxeqyvNevYKNr8N5
/wEPW7QEJU8NY+aoOsRWSu+Bmp+Rnm8H4wS8DA56LAB
/01owgv+N6FaIACX0R45SvWBKqIvFazgTT+CtV0EaaUTVE5QRfsZApHoNF
RozI1NC1dswcwKHQJPN5OjUtFBZQ0IDY6aHkjKcB6a84KHq97Gsu
/PUJqTr20DE/pyMVHO46M6mJ1qHGjnCIQ
/dcWHeiHmaHEAzhKaZfyD8G1ze0eLLPmPSrKCCboB2hOScc+9xtk7V9K63X
oGxTmSZUIRj5sn4/B3Srm
/AjfJbhhdCFTvluCNOATWdnUAsWjrnyo0tgUXNzrrqGWILLQazKsdJm1ghV
ATtoRzrCKKtVfASi0U9v0OUaao09vLPwCelDztfCh4J0cJH6lhoEvosrv5ORD
```

Channel Security

Method:

Key:

```
-----BEGIN OpenVPN Static key V1-----
12e269fae5bb7dbc4a904faeac6ca8af66f3a5d66718cf89b83ce03a3e
c9fd08f6b153029bc998da300e5ceb010fe30f28789b437eca1fe42aa445cba
25f948c59d955de355db0fb427718431f42635b32be8ccd4626b3f4a9e8a2f
9cc71d4f51b4b1171db261285ce1566cac825f4c95c9f1592543d53652be95
4adabc0a406318d6c655fab46c0ecc67289f98b66031fddb5a8313a6a68f5ae
cb4c1f5d8eb1a67700cbadaeaeef7f346ff90c6edd9687f2e791f7efc4871faf65
39add97ae3486d360a74c360ec4593645e8871fe16a28c8391969dd075cdb
424e4214350a3bd89ea75651087552eb889021e536b3c99f8034478155db
a939ef87f0499a9405-----END OpenVPN Static key V1-----
```

Paramètres	Description
Enable	Cocher pour activer le VPN
Protocol	Protocole de communication utilisé : <ul style="list-style-type: none"> • tcp • udp
Address	Adresse IP ou nom du serveur VPN
Port	Port du serveur VPN (Généralement le 1194)
Cipher	Algorithme de chiffrement des paquets de données (optionnel). Liste disponible sur OpenVPN (commande « <code>openvpn --show-ciphers</code> »).
Auth	Algorithme de hachage HMAC permettant d'authentifier les paquets de données. Si « TLS Auth » est renseigné alors l'algorithme de hachage s'applique également sur les paquets de contrôles. Si le champ est vide, la valeur utilisée par défaut est « SHA1 » (optionnel). Liste disponible sur OpenVPN (commande « <code>openvpn --show-digests</code> »).
CA	Certificat racine d'autorité de certification. Au format de fichier PEM
Cert	Certificat signé du client local. Au format de fichier PEM
Key	Clé privée du client local . Au format de fichier PEM

Sécurité du canal de contrôle « Channel Security » :

Paramètres	Description
Method	Liste des méthodes pour la sécurité du canal de contrôle : <ul style="list-style-type: none"> • none : aucun • tls-auth : clé statique servant à l'algorithme de hachage HMAC sur les paquets de contrôles. • tls-crypt : identique à tls-auth, mais chiffre également le canal de contrôle TLS. • tls-crypt-v2 : identique à ci-dessus, mais utilise une clé par client au lieu d'une clé de groupe partagée.
Key	Clé pour la sécurité du canal de contrôle. Au format de fichier PEM.



Pour connaître les informations à saisir pour la configuration du VPN, veuillez-vous rapprocher de l'administrateur réseau du serveur VPN.



La configuration d'un serveur NTP est obligatoire pour l'utilisation d'un VPN afin de vérifier la validité des certificats. (voir chapitre 4.1.1.5 : « NTP »).

4.15 Alarmes

Le concentrateur peut générer des alarmes système.

The screenshot shows a configuration interface for system alarms. It has a blue header with the text 'System alarms'. Below the header, there are three rows of configuration options, each with a label and a dropdown menu:

- Modem IP: Off
- MSISDN: Off
- SW Version: On

Below these options is a horizontal line, followed by the word 'Defaults' centered. Underneath 'Defaults', there are two input fields:

- Ignored: []
- Delayed: []

Les alarmes Système sont de 3 types :

- Modem IP : alarme générée si l'adresse IP obtenue lors d'une connexion via modem change.
- MSISDN : alarme générée si la carte SIM insérée dans le concentrateur est changée.
- SW Version : alarme générée si la version du firmware ou du noyau change (suite à une mise à jour).

Chaque source d'alarme peut être activée individuellement et être transférée immédiatement sur le serveur distant (On) ou à la connexion suivante (Delayed).

Les alarmes de dysfonctionnement du concentrateur (« Default ») sont par défaut émises immédiatement vers le serveur distant. Il est cependant possible de les désactiver (« Ignored ») ou de reporter (« Delayed ») leurs envois à la connexion suivante. Pour cela, il faut saisir dans les champs correspondant au comportement souhaité leurs codes.

Ci-dessous les codes et défauts disponibles :

Code	Description
D_MODEM	Défaut du modem
D_MODEM_SIM_MISS	Carte SIM manquante

D_MODEM_SIM_CODE_FAIL	Erreur du code SIM
D_MODEM_PUK	Carte SIM bloquée
D_MODEM_REG_DENIED	Enregistrement sur le réseau refusé

Dans la case Ignored peuvent être listées les codes défauts ignorés par le concentrateur. Dans le cas ou plusieurs codes défaut sont saisis, ils doivent être séparés par le caractère ',' (virgule).

Dans la case Delayed peuvent être listées les codes défauts transférés à la connexion suivante par le concentrateur. Dans le cas ou plusieurs codes défauts sont saisis, ils doivent être séparés par le caractère ',' (virgule).

4.1.6 Schedules

Le scheduler est en charge de toutes les tâches périodiques. La configuration du scheduler consiste en une liste de schedules. Chacun de ces schedules possède un identifiant unique qui est utilisé pour lier une ou plusieurs tâches à un schedule. Ils peuvent être utilisés indépendamment pour déclencher la collecte de données et télécharger des données.

Chaque schedule est configuré comme suit :

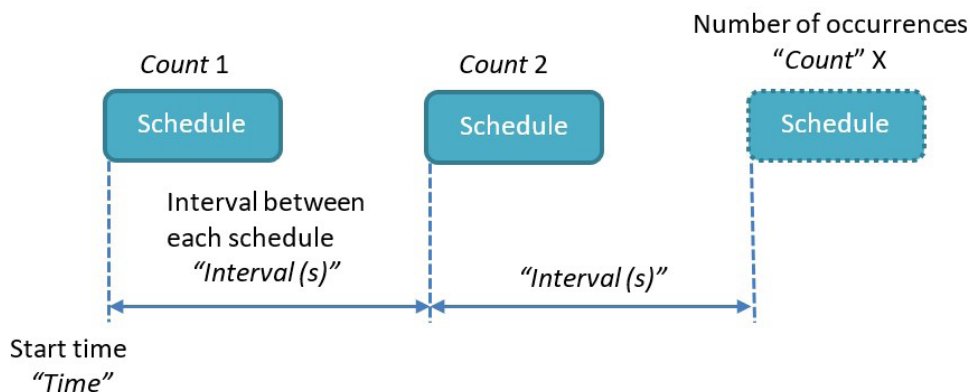
Paramètres	Description
Id	Identifiant unique du schedule. L'identifiant doit être un nombre entier. (compris entre 1 à 2 147 483 647)
Label	Nom uniquement informatif du schedule
Type	Daily, Weekly, Monthly, Yearly ou Follower : voir description ci-dessous
Time	Heure de la première occurrence au format « HH:MM:SS » (non utilisé pour les schedules de type « Yearly »)

Day of Week	Numéro du jour dans la semaine de la première occurrence (1=Lundi, 7=Dimanche) (utilisé uniquement pour les schedules de type « Weekly »)
Day of Month	Numéro du jour dans le mois de la première occurrence (utilisé uniquement pour les schedules de type « Monthly »)
Date & Time	Date et heure de la première occurrence dans une période donnée (utilisé uniquement pour les schedules de type « Yearly »)
Interval (s)	Intervalle entre les occurrences (en secondes)
Count	Nombre d'occurrences (au minimum 1)
Parent	Référence au schedule parent pour un schedule de type « Follower »

Configuration des différents types de schedules :

- Schedule de type « Daily » :

Chaque jour, la première occurrence est donnée par l'heure renseignée dans le champ « Time ». Le nombre d'événements sur la journée est donné par le champ « Count » et l'intervalle entre chaque événement par le champ « Interval ».



Le format « Time » est le suivant : HH:MM:SS (par exemple 09:30:00)

La valeur « Count » est comprise entre 1 et 2 147 483 647

La valeur « Interval » est comprise entre 0 et 2 147 483 647



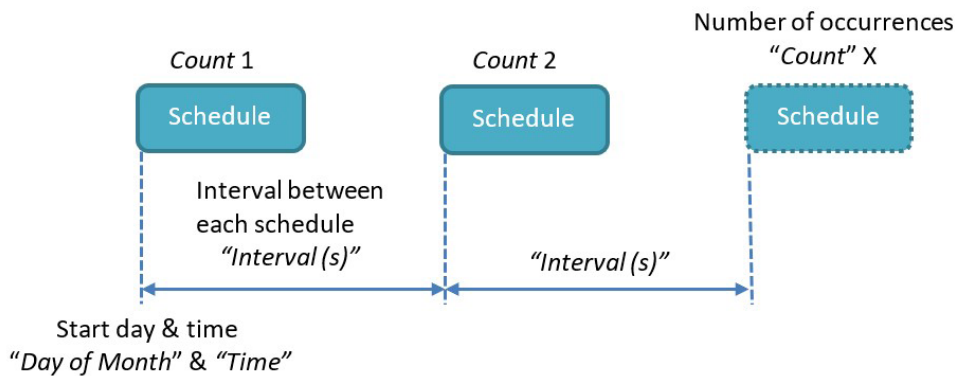
« Count » : si le schedule doit être déclenché toute la journée à intervalle régulier, vous pouvez renseigner la valeur maximum (soit 2 147 483 647) pour le « Count ».

Exemple concret:

Besoin	Type	Time	Day of Week	Day of Month	Date & Time	Interval (s)	Count
Tous les jours à 14:00:00	Daily	14:00:00				0	1

- Schedule de type Weekly :

Chaque semaine, la première occurrence est donnée par le jour de la semaine renseigné dans le champ « Day of week » et l'heure renseignée dans le champ « Time ».



Le format « Day of week » est compris entre Lundi et Dimanche.

Le format « Time » est le suivant : HH:MM:SS (par exemple 09:30:00).

La valeur « Count » est comprise entre 1 et 2 147 483 647.

La valeur « Interval » est comprise entre 0 et 2 147 483 647.



“Count”: if the schedule is to be triggered throughout the week at regular intervals, you can enter the maximum value (namely 2,147,483,647) in “Count”.

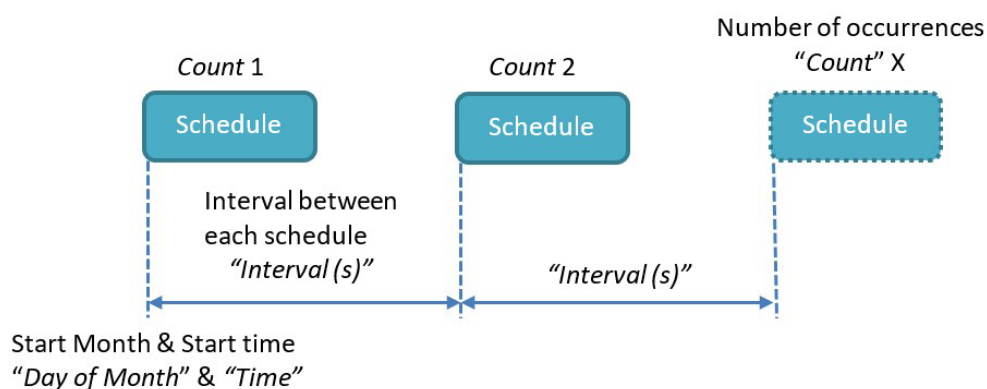
Exemple concret:

Besoin	Type	Time	Day of Week	Day of Month	Date & Time	Interval (s)	Count
Tous les mardis à 15:00:00	Weekly	15:00:00	Tuesday			0	1

Toutes les heures entre 8H00 et 18H00 tous les mardis	Weekly	08:00:00	Tuesday	3600	11
---	--------	----------	---------	------	----

- Schedule de type Monthly :

Chaque mois, la première occurrence est donnée par le numéro de jour du mois renseigné dans le champ « Day of month » et l'heure renseignée dans le champ « Time ».



Le format « Day of Month » est compris entre 1 et 31.

Le format « Time » est le suivant : HH:MM:SS (par exemple 09:30:00).

La valeur « Count » est comprise entre 1 et 2 147 483 647.

La valeur « Interval » est comprise entre 0 et 2 147 483 647.



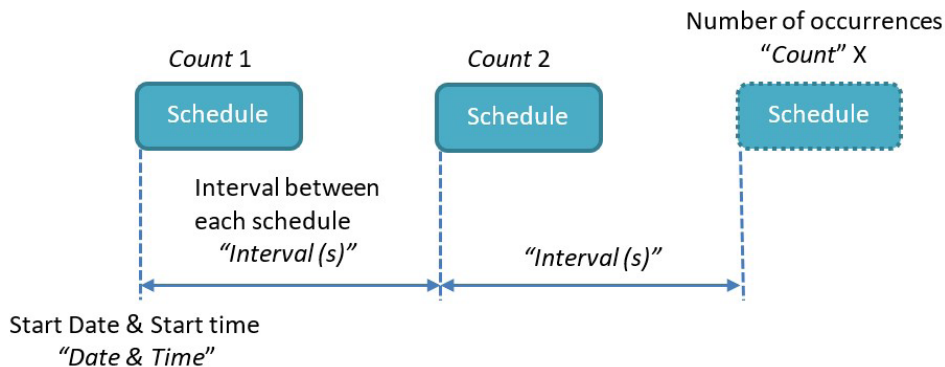
« Count » : si le schedule doit être déclenché tout le mois à intervalle régulier, vous pouvez renseigner la valeur maximum (soit 2 147 483 647) pour le « Count ».

Exemple concret:

Besoin	Type	Time	Day of Week	Day of Month	Date & Time	Interval (s)	Count
Tous les 2èmes jours du mois à 00:00:00	Monthly	00:00:00		2		0	1

- Schedule de type Yearly :

Chaque année, la première occurrence est donnée par la date renseignée dans le champ « Date & Time ».



Le format « date & Time » est le suivant : AAAA-MM-JJTHH:MM:SS (exemple, pour une première occurrence le 11 février 2019 à 13H00 : Time = 2019-02-11T13:00:00).

La valeur « Count » est comprise entre 1 et 2 147 483 647.

La valeur « Interval » est comprise entre 0 et 2 147 483 647.



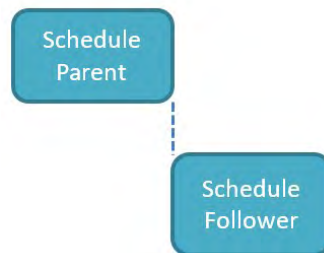
« Count » : si le schedule doit être déclenché toute l'année à intervalle régulier, vous pouvez renseigner la valeur maximum (soit 2 147 483 647) pour le « Count ».

Exemple concret:

Besoin	Type	Time	Day of Week	Day of Month	Date & Time	Interval (s)	Count
Toutes les 2 heures entre 8H00 et 20H00 le 31 décembre	Yearly				2019-12-31 T08:00:00	7200	7

- Schedule de type Follower :

Un schedule de type «Follower» se déclenchera après la fin de chaque occurrence du schedule de référence. Le schedule « Parent » ne peut pas être de type « Follower ».



Ce type permet de déclencher par exemple un téléchargement des données vers le serveur distant après l'achèvement de la collecte des données prévue.

Exemple concret:

Vous souhaitez collecter les données de tous les modules Modbus une fois par jour à minuit et télécharger les données, juste après. Vous pouvez configurer un schedule de type « Daily » pour la collecte de données, et un autre schedule de type « Follower » lié au premier schedule pour le téléchargement des données.

4.17 Modbus

Le concentrateur WebdynEasy LoRaWAN est exclusivement Maître Modbus RTU et TCP.



En cas d'utilisation d'esclave(s) Modbus RTU, le protocole Modbus doit être activé sur le port RS485/RS422 (voir chapitre 4.1.3 : « Système »).

Dans l'onglet « Modbus » de l'interface web locale, vous pouvez configurer les temps de réponse maximums pour les protocoles Modbus RTU et TCP.

Paramètres	Description
RTU	
Timeout (ms)	Temps d'attente de réponse Modbus RTU en ms
Turnaround (ms)	Délais de retournement Modbus RTU en ms
TCP	
Timeout (ms)	Temps d'attente de réponse Modbus TCP en ms

Un esclave Modbus est défini par un label, un dataset, une adresse Modbus et un schedule. Dans le cas d'un esclave Modbus Modbus TCP, une adresse IP est nécessaire.

Paramètres	Description
Label	Nom uniquement informatif
Dataset	Identifiant du dataset associé (Liste dataset déclarée)
Address	Adresse Modbus (de 1 à 247)
IP	Adresse IP (vide pour les équipements RTU)
Schedule	Identifiant du schedule (Liste des schedules déclarées)

Un dataset défini les variables disponibles sur un esclave Modbus, et comment les récupérer. Configuration d'un dataset :

Paramètres	Description
Id	Identifiant unique de l'ensemble de données Modbus (entier)
Label	Nom de l'ensemble de données (uniquement informatif)
Polling	Interrogation des esclaves Modbus en continu

Configuration des variables, chaque variable étant définie par les paramètres suivants :

Paramètres	Description
Name	Nom de la variable (uniquement informatif)
Type	Type de variable : <ul style="list-style-type: none"> • Coil (0x1/0x5,0xF) • Discrete input(0x2) • Holding register (0x3/0x6,0x10) • Input register (0x4)
Address	Adresse de registre étendu 16-bits
Size	Taille en bits pour les Discrete inputs et Coils, et en octets pour les Input et Holding registers

Format	Format de la variable : <ul style="list-style-type: none"> • Raw (donnée brute) • Boolean (booléen : 0 ou 1) • Integer (entier) • Float (chiffre à virgule) • ASCII (texte)
Flags	Liste des options à appliquer : (facultatif) <ul style="list-style-type: none"> • cmd_only • little_endian • no_opt • signed • is_status • is_alarm
Threshold low	Niveau de seuil bas (facultatif)
Threshold high	Niveau de seuil haut (facultatif)
Threshold hysteresis	Hystérésis appliquée aux deux seuils (facultatif)

La variable « Polling » permet d'activer l'interrogation en continu de l'esclave Modbus. Lorsqu'elle est désactivée, l'esclave Modbus n'est interrogé que sur déclenchement du schedule associé.

Le type de variable définit le code fonction à utiliser pour lire ou écrire la variable. Voir le tableau ci-dessous :

Type	Description	Lecture (multiple)	Ecriture (unique)	Ecriture (multiple)
S0	Coil	0x01	0x05	0x0F
S1	Discrete input	0x02	-	-
S3	Input register	0x04	-	-
S4	Holding register	0x05	0x06	0x10

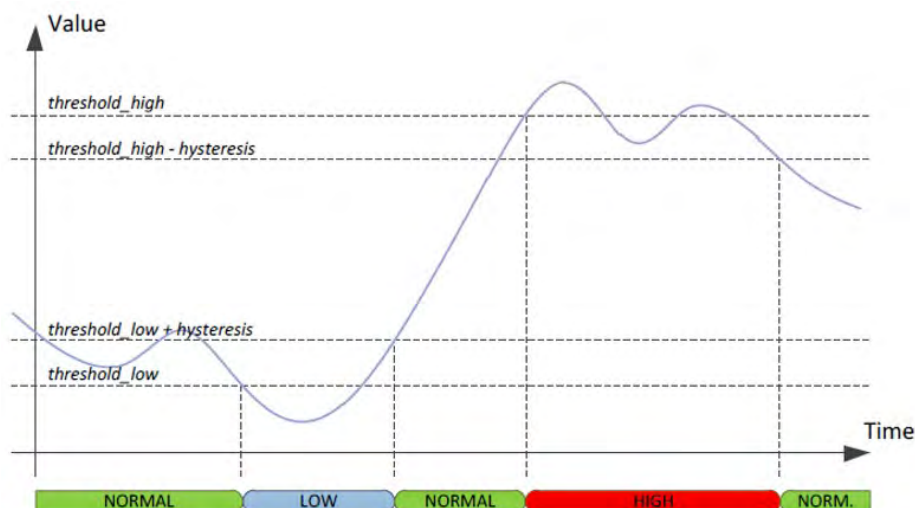
Les formats disponibles sont les suivants :

Format	Description	Coil	Register
raw	Données représentées comme : <ul style="list-style-type: none"> • chaine binaire pour les « Discrete input » et les « Coils » • chaine hexadécimale pour les « registers » 	X	X
boolean	Booléen vrai ou faux	X	
integer	Chiffre entier de 8, 16 ou 32 bits		X
float	Chiffre à virgule flottante 16 ou 32 bits (IEEE 754)		X
ascii	Chaine de caractères en ACSII		X

Le champ « Flag » peut être complété d'une ou plusieurs options. En cas d'options multiples, les options doivent être séparées par une virgule « , ». Ci-dessous la liste des options disponibles.

Flag	Description
cmd_only	La variable ne sera pas lu par l'appareil Modbus, mais peut être écrite.
little_endian	Interprète les registres en little-endian
no_opt	Une requête Modbus dédiée sera utilisée pour lire cette variable
signed	La variable contient une valeur signée
is_status	Indique que la variable contient un statut information
is_alarm	Toute modification de la variable statut déclenchera une alarme

Lorsque l'option « is_status » est définie, ou qu'au moins un seuil est défini, la variable est considérée comme une variable statut. C'est-à-dire, qu'en cas de changement de statut, la valeur de la variable est sauvegardée dans le fichier de données. Ci-dessous un schéma décrivant les changements de statut en fonction des seuils et de l'hystérésis.



Dans le cas où la variable est une variable statut, et que l'option « is_alarm » est présente, un fichier d'alarme est généré à chaque changement d'état. L'option « is_alarm » n'a aucun effet si la variable n'est pas une variable statut (option « is_status »).

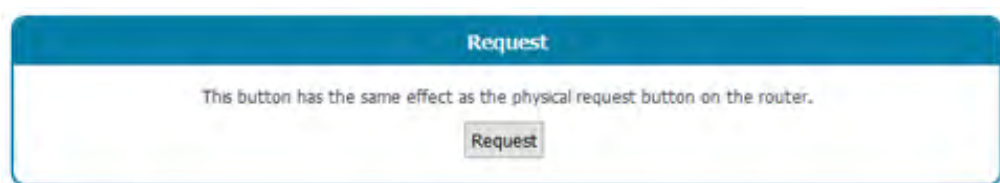


Quand les paramètres de surveillance Threshold low, Threshold high ou Threshold hysteresis sont utilisés, il faut activer le mode Polling afin de permettre de surveiller la variable en permanence.

4.1.8 Actions exécutables

L'onglet « Actions » de l'interface web permet d'exécuter certaines actions localement.

4.1.8.1 Demande de connexion au serveur distant : Request

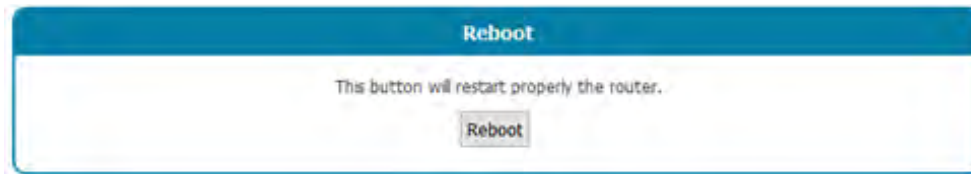


Le bouton « Request » a le même effet que le bouton physique présent en face avant du produit.

Lors d'un appui sur ce bouton, une fenêtre popup apparaît affichant toutes les étapes de connexion notamment la synchronisation NTP, la vérification du répertoire INBOX et indique tous les fichiers téléchargés.

4.1.8.2 Demande de redémarrage : Reboot

Ce bouton permet de redémarrer le concentrateur.



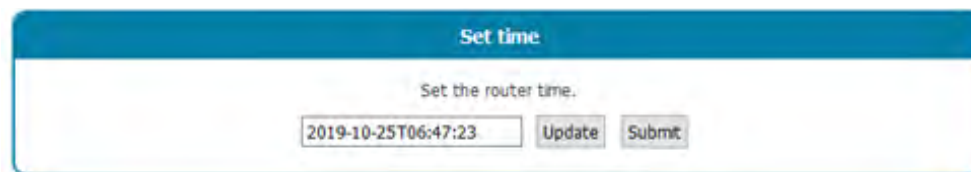
4.1.8.3 Téléchargement des logs : Download logs

Ce bouton permet de récupérer les logs des dernières actions exécutés sur le concentrateur.



4.1.8.4 Mise à l'heure manuelle : Set time

Ce formulaire permet la mise à l'heure du concentrateur en cas de non-disponibilité d'une connexion internet ou d'un serveur NTP non renseigné.



En cliquant sur le bouton « Update », la date et l'heure de l'ordinateur sont copiées dans le formulaire sous le bon format.

Si vous souhaitez saisir manuellement la date et l'heure, le format doit être le suivant : AAAA-MM-JJThh:mm:ss

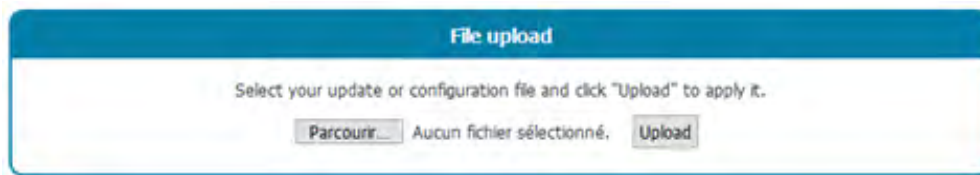
Avec :

- AAAA : Année sur 4 chiffres
- MM : Mois dans l'année sur 2 chiffres
- JJ : Jour dans le mois sur 2 chiffres
- hh : Heure sur 2 chiffres
- mm : Minutes sur 2 chiffres
- ss : Secondes sur 2 chiffres

La prise en compte de la nouvelle date n'est effective qu'après validation du formulaire par l'appui sur le bouton « Submit ».

4.1.8.5 Téléchargement de fichiers système : File upload

Ce formulaire permet le téléchargement local de fichier sur le concentrateur.



File upload

Select your update or configuration file and click "Upload" to apply it.

Parcourir... Aucun fichier sélectionné. Upload

Seuls les fichiers de configuration et les mises à jour sont acceptés via ce formulaire.

5. Exploitation

5.1 Le serveur distant

Le concentrateur communique avec un serveur distant soit par le protocole FTP ou soit par Web Service. Le 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.

5.1.1 Le serveur FTP

5.1.1.1 Paramétrage

Le serveur FTP est défini par les paramètres suivants :

- Une adresse : cette adresse peut être une adresse IP ou un nom de domaine. Dans le cas de l'utilisation d'un nom de domaine avec une connexion Ethernet, un serveur DNS doit être configuré dans le concentrateur pour permettre la résolution du nom de domaine en adresse IP.
- Il est possible de modifier le port de connexion FTP (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 à utiliser.
- Un répertoire racine : le répertoire racine peut être la racine du serveur FTP « / » ou une suite de sous-répertoires (par exemple « WebdynEasy_LoRaWAN/OOC8B5/ »).

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

Nom	Droits	Description
CONFIG/	Écriture	Contiens l'image de la configuration. La configuration est sauvegardée dans un fichier nommé : « <uid>.xml »
DATA/	Écriture	Contiens les données collectées. Le nom du fichier de données respecte le format suivant : « <uid>-<timestamp>.xml.gz » ou « <uid>-<timestamp>.json.gz »
ALARM/	Écriture	Contiens les alarmes. Le nom du fichier d'alarme respecte le format suivant : « <uid>-<timestamp>.xml.gz »
SUPERVISION/	Écriture	Contiens les fichiers de statut, ainsi que les logs. Les noms des fichiers respectent le format suivant : « <uid>-<timestamp>.xml.gz »
INBOX/<uid>/	Lecture/ Écriture	Boite aux lettres pour envoyer une configuration ou une commande au concentrateur
BIN/	Lecture	Contiens les fichiers de mise à jour

Avec :

- <uid> : Identifiant du concentrateur
- <timestamp> : Le format d'horodatage est «AAAAMMJJ-HHMMSS» de sorte qu'un tri alphabétique du répertoire donne l'ordre chronologique

Les fichiers de données, d'alarme et de supervisions sont compressés au Gzip « .gz ». Les droits d'accès minimums aux différents répertoires doivent être définis comme précisés dans le tableau ci-dessus.



Le concentrateur ne crée pas les répertoires si ces derniers n'existent pas. Si les répertoires n'existent pas ou que les droits sont insuffisants, veuillez contacter l'administrateur du serveur.

5.1.1.2 Fonctionnement

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

- Au début du transfert le fichier à une extension supplémentaire « .tmp ».
- Quand le fichier est 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.



Les fichiers échangés avec le serveur distant respectent les formats décrits par les fichiers schémas (fichiers XSD). Chaque version du firmware est livrée avec ses fichiers schémas associés et disponible sur notre site web (voir chapitre 7 : « Support »).



Les schémas XML spécifiant le format des différents fichiers XML utilisés par le concentrateur peuvent évoluer dans les futures versions lorsque de nouvelles fonctionnalités seront ajoutées. Ces changements seront apportés afin que les anciens fichiers XML restent compatibles avec les nouveaux schémas XML. De même, comme les fichiers XML générés par le concentrateur peuvent contenir des éléments supplémentaires, leur traitement doit être mis en œuvre afin que les nouveaux éléments soient ignorés.

5.1.1.3 Format des fichiers

Les fichiers d’alarmes, de commandes et de configuration échangés avec le serveur sont au format XML. Les fichiers de données sont soit au format XML ou soit au format JSON.

5.1.2 Web Service

5.1.2.1 Paramétrage

Le Web Service est défini par les paramètres suivants :

- Une URL : l’URL peut être une adresse IP ou un nom du serveur web distant. Dans le cas de l’utilisation d’un nom de domaine avec une connexion Ethernet, un serveur DNS doit être configuré dans le concentrateur pour permettre la résolution du nom de domaine en adresse IP.
- Il est possible de modifier le port du serveur web (par défaut 80) en rajoutant à la fin de l’URL, le port à utiliser après le caractère ‘:’. Le format à utiliser est le suivant : « url:port » (par exemple : « 192.168.1.2:5000 »).
- Un identifiant et un mot de passe : ces paramètres permettent de définir le compte du Web Service à utiliser.
- Un chemin d’accès : le chemin d’accès sur le serveur web.

Le serveur web doit contenir les sous-chemins d’accès suivants :

Nom	Droits	Description
CONFIG/	Écriture	Contiens l’image de la configuration. La configuration est sauvegardée dans un fichier nommé : « <uid>.xml »
DATA/	Écriture	Contiens les données collectées. Le nom du fichier de données respecte le format suivant : « <uid>-<timestamp>.xml.gz » ou « <uid>-<timestamp>.json.gz »

ALARM/	Écriture	Contiens les alarmes. Le nom du fichier d'alarme respecte le format suivant : « <uid>-<timestamp>.xml.gz »
SUPERVISION/	Écriture	Contiens les fichiers de statut, ainsi que les logs. Les noms des fichiers respectent le format suivant : « <uid>-<timestamp>.xml.gz »
INBOX/<uid>/	Lecture/ Écriture	Boite aux lettres pour envoyer une configuration ou une commande au concentrateur
BIN/	Lecture	Contiens les fichiers de mise à jour

Avec :

- <uid> : Identifiant du concentrateur
- <timestamp> : Le format d'horodatage est «AAAAMMJJ-HHMMSS» de sorte qu'un tri alphabétique du répertoire donne l'ordre chronologique

Les fichiers de données, d'alarme et de supervisions sont compressés au format Gzip « .gz ».

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

5.1.2.2 Fonctionnement

Le concentrateur dépose les fichiers sur le serveur web en utilisant une requête HTTP POST au format suivant :

- CONFIG : http://<ws_address>/<ws_upolad_path>/config
- DATA : http://<ws_address>/<ws_upolad_path>/data
- ALARM : http://<ws_address>/<ws_upolad_path>/alarm
- SUPERVISION : http://<ws_address>/<ws_upolad_path>/supervision
- INBOX : http://<ws_address>/<ws_upolad_path>/inbox ?uid=<uid>

Le concentrateur récupère les fichiers sur le serveur web en utilisant une requête HTTP GET au format suivant :

- INBOX : http://<ws_address>/<ws_upload_path>/inbox/<update_file>?uid=<uid>
- BIN : http://<ws_address>/<ws_upload_path>/bin/<update_file>?uid=<uid>



Les fichiers échangés avec le serveur distant respectent les formats décrits par les fichiers schémas (fichiers XSD). Chaque version du firmware est livrée avec ses fichiers schémas associés et disponible sur notre site web (voir chapitre 7 : « Support »).



Les schémas XML spécifiant le format des différents fichiers XML utilisés par le concentrateur peuvent évoluer dans les futures versions lorsque de nouvelles fonctionnalités seront ajoutées. Ces changements seront apportés afin que les anciens fichiers XML restent compatibles avec les nouveaux schémas XML. De même, comme les fichiers XML générés par le concentrateur peuvent contenir des éléments supplémentaires, leur traitement doit être mis en œuvre afin que les nouveaux éléments soient ignorés.

5.1.2.3 Format des fichiers

Les fichiers d'alarmes, de commandes et de configuration échangés avec le serveur sont au format XML. Les fichiers de données sont soit au format XML ou soit au format JSON.

5.1.3 MQTT

5.1.3.1 Paramétrage

- Le Serveur MQTT est défini par les paramètres suivants :
- **Une adresse** : Cette adresse peut être une adresse IP ou un nom du serveur web distant. Dans le cas de l'utilisation d'un nom de domaine avec une connexion Ethernet, un serveur DNS doit être configuré dans le concentrateur pour permettre la résolution du nom de domaine en adresse IP.
- Il est possible de modifier le port du serveur MQTT (par défaut 1883) en rajoutant à la fin de l'adresse, le port à utiliser après le caractère ':'. Le format à utiliser est le suivant : « url:port » (par exemple : « 192.168.1.2:5000 »).
- **Un identifiant et un mot de passe** : Ces paramètres permettent de définir le compte du serveur MQTT à utiliser.
- **Le topic** : Le topic des messages MQTT à utiliser

Avec :

- `<uid>` : Identifiant du concentrateur

5.1.3.2 Fonctionnement

Le concentrateur envoie les données sur le serveur MQTT au format spécifié dans la section upload. Il n'y a pas de gestion de configuration en MQTT. Il n'y a pas de commande en MQTT.

5.1.3.3 Format des données

Les alarmes, les données et la supervision sont soit au format XML ou soit au format JSON.

Concernant le format XML :



Les données échangées avec le serveur distant respectent les formats décrits par les fichiers schémas (fichiers XSD). Chaque version du firmware est livrée avec ses fichiers schémas associés et disponible sur notre site web (voir chapitre 7 : « Support »)



Les schémas XML spécifiant le format des différents fichiers XML utilisés par le concentrateur peuvent évoluer dans les futures versions lorsque de nouvelles fonctionnalités seront ajoutées. Les fichiers XML générés par le concentrateur peuvent contenir des éléments supplémentaires, leur traitement doit être mis en œuvre afin que les nouveaux éléments soient ignorés.

5.2 Configuration

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

Fichier de configuration :

Le fichier de configuration du concentrateur WebdynEasy LoRaWAN est au format XML. Veuillez-vous référer au fichier XSD de configuration relatif à votre version de firmware pour connaître les détails du format des fichiers de configuration.

Vous trouverez en annexe de ce manuel (« Annexe A – Liste des variables ») la liste des variables et leurs significations.

Une sauvegarde de la configuration courante est disponible sur le serveur distant dans le répertoire ou sous chemin d'accès « CONFIG/ ». Que ce soit après une modification locale ou distante de la configuration, le concentrateur envoie sur le serveur distant sa nouvelle configuration.

L'envoi d'un fichier de configuration peut être réalisé localement via l'interface web, ou distance via le répertoire FTP « INBOX » ou via web service dans le sous-chemin d'accès « INBOX ».

- Localement : dans l'onglet « Actions », sélectionnez via le formulaire « File upload » le fichier de configuration souhaité, puis validez votre choix en cliquant sur le bouton « Upload ». Le fichier va être envoyé sur le concentrateur et appliqué.

File upload

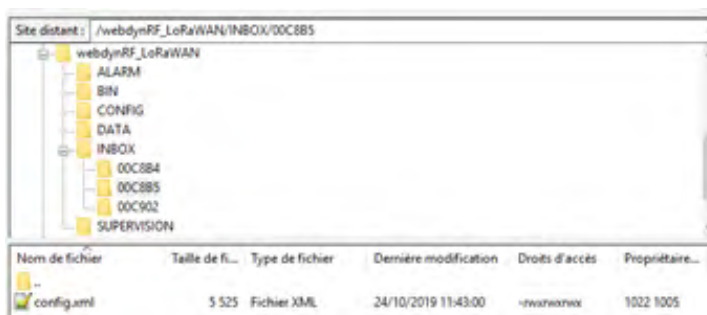
Select your update or configuration file and click "Upload" to apply it.

Parcourir... Aucun fichier sélectionné. Upload

- À distance : déposez le fichier de configuration dans le répertoire « INBOX » de votre concentrateur (« INBOX/<uid>/ », avec <uid> l'identifiant de votre concentrateur). Lors de la

prochaine connexion au serveur distant, le concentrateur réalise 3 étapes :

- Télécharger le fichier de configuration disponible sur le serveur.
- Supprimer le fichier de configuration du serveur.
- Appliquer la nouvelle configuration.



Il n'est pas nécessaire d'utiliser un format de nom prédéfini au fichier de configuration.

En cas d'erreur dans le fichier de configuration (fichier corrompu, valeur incorrecte, ...), le fichier ne sera pas appliqué, et une alarme sera générée sur le serveur. Veuillez vérifier la cohérence de votre fichier de configuration par rapport au fichier XSD correspondant à votre version de firmware avant de l'envoyer sur votre concentrateur.

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 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. Cependant, il est possible d'appliquer les valeurs par défauts à l'ensemble des variables avant d'appliquer les nouvelles valeurs. Pour cela, dans la balise principale « config », ajoutez l'attribut « factory=true ». (Voir exemple ci-dessous).

```
<config
xmlns="http://www.webdyn.com/GWL_config_20190719"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.webdyn.com/GWL_config_20190719 config.
xsd"
factory="true">
  <uid>00C8B4</uid>
  <name>WG_00C8B4</name>
  <enable_local_config>true</enable_local_config>
  <com>
    <modem>
      <pin>
        ...
      </pin>
    </modem>
  </com>
</config>
```



Veuillez-vous référer à l'annexe « Annexe A - 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 distant, sous la forme de fichiers soit au format XML ou soit au format JSON, et compressés au format Gzip « .gz ».

Ci-dessous le format des noms des fichiers de données : <uid>-<timestamp>.xml.gz ou <uid>-<timestamp>.json.gz.

Avec :

- <uid> : Identifiant du concentrateur
- <timestamp> : Le format de l'horodatage est «AAAAMMJJ-HHMMSS» de sorte qu'un tri alphabétique du répertoire donne l'ordre chronologique

Exemple :

00C8B4-20191029-112704.xml.gz ou 00C8B4-20191029-112704.json.gz

Le format des fichiers de données est décrit par le fichier XSD de données. Les fichiers XSD pouvant évoluer en fonction des versions de firmwares. Ils sont délivrés avec chaque mise à jour.

La fréquence d'envoi des fichiers sur le serveur distant peut être définie par un Schedule. (voir chapitre 4.1.6 : « Schedules » et chapitre 4.1.1.6 : « Upload »).

Pendant, lors d'une connexion au serveur, suite à une demande manuelle ou au déclenchement d'une alarme, le concentrateur profite de la connexion pour déposer les données en mémoire.

5.4 Les alarmes

Les alarmes sont remontées sous la forme de fichiers au format XML, et compressées au format Gzip «.gz ». Elles sont déposées dans le répertoire « ALARM/ » du serveur distant.

Le format des noms des fichiers d'alarmes est identique à celui des fichiers de données. Ci-dessous le format des noms des fichiers d'alarmes : <uid>-<timestamp>.xml.gz

Avec :

- <uid> : Identifiant du concentrateur
- <timestamp> : Format de l'horodatage est «AAAAMMJJ-HHMMSS» de sorte qu'un tri alphabétique du répertoire donne l'ordre chronologique

Exemple : 00C8B4-20191029-090507.xml.gz

Le format des fichiers d'alarmes est décrit par le fichier XSD d'alarmes. Les fichiers XSD peuvent évoluer en fonction des versions de firmwares. Ils sont délivrés avec chaque mise à jour.

Les alarmes peuvent être configurées pour être déposées immédiatement après leur déclenchement (On), lors de la prochaine connexion (Delayed) ou désactivées (Off). (voir chapitre 4.1.5 : « Alarmes »).

5.5 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 XML, ou par SMS.

- Fichier commande XML : le fichier de commande doit être déposé 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. Le format des fichiers de commandes est décrit par le fichier XSD de commandes. Les fichiers XSD pouvant évoluer en fonction des versions de firmwares. Ils sont délivrés avec chaque mise à jour.
- SMS : le format du SMS doit être le suivant :

```
cmd=command
param1=value1
param2=value2
...
parami=valuei
```

ou

```
cmd=command;param1=value1;param2=value;...;parami=valuei
```

Avec :

- command : commande à envoyer
- param1, param2, ..., parami : paramètres de la commande
- value1, value2, ..., valuei : valeurs des paramètres



- command : commande à envoyer
- param1, param2, ..., parami : paramètres de la commande
- value1, value2, ..., valuei : valeurs des paramètres

Toutes les commandes acceptent deux paramètres facultatifs « uid » et « cid » :

- uid : identifiant unique du concentrateur
- cid : identifiant de commande

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. Il sera inclus avec tout téléchargement associé.

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

Commande	Sous-commande	Description	Retour
reboot		Redémarrage du produit	Aucun
factory		Retour aux paramètres usines	Aucun
update		Mise à jour logiciel du concentrateur	Alarme
connect		Connexion immédiate au serveur distant	Connexion
status		Récupération du statut du concentrateur	Supervision+SMS
log		Récupération du journal de bord	Supervision
settime		Mise à l'heure du concentrateur	Alarme
modbus	write	Écriture sur un esclave modbus	Alarme
lorawan	send	Envoi de trame de Downlink LoRaWAN	Alarme
lorawan	add	Ajout d'un capteur	Alarme
lorawan	delete	Suppression d'un capteur	Alarme



Dans le cas d'envoi de plusieurs commandes simultanées, les commandes « reboot », « factory », « update » peuvent faire perdre les commandes qui suivent.

5.5.1 Commande « reboot »

La commande « reboot » permet de déclencher un redémarrage immédiat du produit. Il n'y a aucun retour/acquittement suite à l'envoi de cette commande.

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

Exemple :

- Par fichier XML :

```
<commands
xmlns="http://www.webdyn.com/GWL_command_20190719"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.webdyn.com/GWL_
command_20190719 command.xsd">
  <cmd uid="00C8B4">
    <reboot />
  </cmd>
</commands>
```

- Par SMS :

```
cmd=reboot
uid=00C8B4
```

5.5.2 Commande « factory »

La commande « factory » permet de restaurer les paramètres usine dans le concentrateur. Il n'y a aucun retour/acquittement suite à l'envoi de cette commande.

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

Exemple :

- Par fichier XML :

```
<commands
xmlns="http://www.webdyn.com/GWL_command_20190719"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.webdyn.com/GWL_
command_20190719 command.xsd">
  <cmd>
    <factory />
  </cmd>
</commands>
```

- Par SMS :

```
cmd=factory
```

5.5.3 Commande « update »

(voir chapitre 6.2 : « Mise à jour Distant »)

5.5.4 Commande « connect »

La commande « connect » permet de déclencher une connexion immédiate du produit au serveur distant. Il n'y a aucun retour/acquittement suite à l'envoi de cette commande.

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

Exemple :

- Par SMS :

```
cmd=connect
```

5.5.5 Commande « status »

La commande « status » permet de récupérer des informations sur l'état du produit. Lorsque la demande est effectuée via un fichier, un fichier de statut est déposé sur le serveur distant dans le répertoire « SUPERVISION/ ». Lorsque la demande est effectuée par SMS, la réponse est envoyée par SMS à l'émetteur de la commande.

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

Exemple :

- Par fichier XML :

```
<commands
xmlns="http://www.webdyn.com/GWL_command_20190719"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.webdyn.com/GWL_
command_20190719 command.xsd">
  <cmd cid="status cmd 1">
    <status />
  </cmd>
</commands>
```

- Par SMS :

```
cmd=status
cid=status cmd 1
```

5.5.6 Commande « log »

La commande « log » permet de récupérer le journal de bord du concentrateur. Le journal de bord est déposé sur le serveur distant dans le répertoire « SUPERVISION/ ».

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

Exemple :

- Par fichier XML :

```
<commands
xmlns="http://www.webdyn.com/GWL_command_20190719"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.webdyn.com/GWL_
command_20190719 command.xsd">
  <cmd>
    <log />
  </cmd>
</commands>
```

- Par SMS :

```
cmd=log
```

5.5.7 Commande « settime »

La commande « settime » permet de mettre à jour la date et l'heure du concentrateur avec l'heure souhaité.

Pour cela dans l'attribut « time », il faut indiquer la date et l'heure souhaitées au format suivant : AAAA-MM-JJThh:mm:ss

Avec :

- AAAA : Année sur 4 chiffres
- MM : Mois dans l'année sur 2 chiffres
- JJ : Jour dans le mois sur 2 chiffres
- hh : Heure sur 2 chiffres
- mm : Minutes sur 2 chiffres
- ss : Secondes sur 2 chiffres



Si un serveur NTP est paramétré, la date et l'heure du concentrateur se mettront automatiquement à jour lors d'une connexion au serveur distant.

Exemple :

- Par fichier XML :

```
<commands>
  <cmd>
    <settime>
      <time>2021-05-23T16:03:23</time>
    </settime>
  </cmd>
</commands>
```

- Par SMS :

```
cmd=settime
time=2021-05-23T16:03:23
```

5.5.8 Commande « modbus »

La commande « modbus » permet l'écriture de valeurs dans des registres d'esclaves Modbus configurés sur le concentrateur.

Pour cela, il est nécessaire de préciser la sous-commande « write », la donnée à écrire dans l'attribut « data », la liste des esclaves et registres dans lesquels il faut écrire cette valeur.

Suite à la commande, une alarme est générée et déposée dans le répertoire « ALARM/ » précisant le résultat de la commande.

Les adresses des esclaves doivent respecter le format suivant :

- Modbus RTU:

```
<modbus_address>/<register_type>@<register_address>
```

Exemple : 45/S3@0x0056

- Modbus TCP:

```
<device_ip>:<modbus_address>/<register_type>@<register_
address>
```

Exemple : 192.168.0.17:223/S3@0x0F52

Exemple :

- Par fichier XML :

```
<commands
xmlns="http://www.webdyn.com/GWL_command_20190719"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.webdyn.com/GWL_
command_20190719 command.xsd">
  <cmd>
    <modbus subcmd="write" data="0xFF">
      <address>45/S4@0x0056</address>
      <address>192.168.0.17:223/S3@0x0F52</
address>
    </modbus>
  </cmd>
</commands>
```

- Par SMS :

```
cmd=modbus
subcmd=write
data=0xFF
address=45/S4@0x0056
address=192.168.0.17:223/S3@0x0F52
```

5.5.9 Commande « lorawan »

La commande « lorawan » permet d'envoyer des commandes au concentrateur. Il existe plusieurs sous commande qui sont :

- « send » : permet d'envoyer des trames de descendantes « downlink » au capteur.
- « add » : permet de rajouter un capteur dans le concentrateur.
- « delete » : permet d'effacer un capteur dans le concentrateur.

Suite à la commande, une alarme est générée et déposée dans le répertoire « ALARM/ » précisant le résultat de la commande.

5.5.9.1 Sous-commande "send"

La sous-commande « send » permet d'envoyer des trames de descendantes « downlink » au capteur.

Pour cela, il est nécessaire de renseigner les attributs suivants :

- « devaddr » : le DEVADDR du capteur qui permet d'identifier le capteur (au format hexadécimal).
- « deveui » : le DEVEUI du capteur qui permet d'identifier le capteur (au format hexadécimal).
- « fport » : le numéro du port du capteur à utiliser capteur (au format décimal).

- « data » : la donnée à envoyer au format hexadécimal.

En classe A, le concentrateur envoie les trames de descendantes « downlink » juste après une trame montante « uplink » du capteur. Le concentrateur prépare le message et le stock au maximum 48 heures. Passer ce temps, une alarme sera envoyée pour signaler que le temps est dépassé. Une alarme est également envoyée pour signaler l'envoi de la trame au capteur.

Exemple :

- Par fichier XML :

```
<commands>
  <cmd cid="cmd1">
    <lorawan subcmd="send">
      <devaddr>01020304</devaddr>
      <fport>1</fport>
      <data>0AF0C4</data>
    </lorawan>
  </cmd>
</commands>
```

```
<commands>
  <cmd cid="change_send_period_to_10min">
    <lorawan subcmd="send">
      <deveui>E498ED0000000000</deveui>
      <fport>1</fport>
      <data>600401</data>
    </lorawan>
  </cmd>
</commands>
```

- Par SMS :

```
cmd=lorwan
subcmd=send
devaddr=01020304
fport=1
data=0AF0C4
```

Exemple des alarmes en cas de succès :

```

<alarms>
  <command>
    <date>2021-01-25T15:00:00</date>
    <cid>change_send_period_to_10min</cid>
    <source>ws</source>
    <error>none</error>
    <description>commande queued</description>
  </command> <command>
    <date>2021-01-25T15:05:00</date>
    <cid>change_send_period_to_10min</cid>
    <source>ws</source>
    <error>none</error>
    <description>commande sent</description>
  </command>
</alarms>

```

Exemple d'une alarme en cas de temps dépassés :

```

<alarms>
  <command>
    <date>2021-01-27T15:00:00</date>
    <cid>change_send_period_to_10min</cid>
    <source>ws</source>
    <error>other</error>
    <description>message timeout</description>
  </command>
</alarms>

```

5.5.9.2 Sous-commande "add"

La sous-commande « add » permet de rajouter un capteur au concentrateur.

Pour cela, il est nécessaire de renseigner les attributs suivants :

- « deveui » : le DEVEUI du capteur qui permet d'identifier le capteur (au format hexadécimal).
- « appskey » : le APPSKEY du capteur si le capteur est mode ABP (au format hexadécimal).
- « nwkskey » : le NWKSKEY du capteur si le capteur est mode ABP (au format hexadécimal).
- « appkey » : le APPKEY du capteur si le capteur est mode OTAA (au format hexadécimal).

Exemple d'ajout d'un capteur en mode OTAA :

- Par fichier XML :

```
<commands>
  <cmd cid="add_endpoint_key">
    <lorawan subcmd="add">
      <deveui>E498ED0000000000</deveui>
      <appkey>000102030405060708090A0B0C0D0E0F</
appkey>
    </lorawan>
  </cmd>
</commands>
```

- Par SMS :

```
cmd=lorawan
subcmd=add
deveui=E498ED0000000000
appkey=000102030405060708090A0B0C0D0E0F
```

Exemple d'ajout d'un capteur en mode ABP :

- Par fichier XML :

```
<commands
  <cmd cid="change_send_period_to_10min">
    <lorawan subcmd="send">
      <devaddr>00000F6A</devaddr>
      <appskey>000102030405060708090A0B0C0D0E0F<
appskey>
      <nwkskey>000102030405060708090A0B0C0D0E0F</
nwkskey>
    </lorawan>
  </cmd>
</commands>
```

- Par SMS :

```
cmd=lorwan
subcmd=add
devaddr=00000F6A
appskey=000102030405060708090A0B0C0D0E0F
nwkskey=000102030405060708090A0B0C0D0E0F
```

5.5.9.3 Sous-commande "delete"

La sous-commande « delete » permet de supprimer un capteur du concentrateur.

Pour cela, il est nécessaire de renseigner les attributs suivants :

- « devaddr » : le DEVADDR du capteur qui permet d'identifier le capteur (au format hexadécimal).
- « deveui » : le DEVEUI du capteur qui permet d'identifier le capteur (au format hexadécimal).

Exemple :

- Par fichier XML :

```
<commands>
  <cmd cid="add_endpoint_key">
    <lorawan subcmd="delete">
      <deveui>E498ED0000000000</deveui>
    </lorawan>
  </cmd>
</commands>
```

```
<commands>
  <cmd cid="add_endpoint_key">
    <lorawan subcmd="delete">
      <devaddr>00000F6A</devaddr>
    </lorawan>
  </cmd>
</commands>
```

- Par SMS :

```
cmd=lorawan
subcmd=delete
deveui=E498ED0000000000
```

6. Mise à jour

Le concentrateur WebdynEasy LoRaWAN peut être mis à jour localement ou à distance. La dernière version du firmware (« GatewayLoRaWAN_x.x.x.cwe ») est disponible au téléchargement sur notre site à l'adresse suivante : <https://www.webdyn.com/support/lorawan/>

6.1 Locale

Pour mettre à jour le concentrateur localement, il faut passer par son interface web et aller dans l'onglet « Actions » puis suivre la procédure de téléchargement de fichiers système « File upload » (voir le chapitre 4.1.8.5 : « Téléchargement de fichiers système : File upload »)

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 (« update ») doit être envoyée au concentrateur.

La commande de mise à jour peut être envoyée soit par un fichier de commande ou soit par SMS. La commande doit inclure le nom du fichier contenant la mise à jour (champ « firmware »), ainsi que son code MD5 associé (champ « checksum »).



Il est fortement conseillé d'utiliser un fichier de commande (XML).

Exemple :

- Par fichier XML :

```
<commands
xmlns="http://www.webdyn.com/GWL_command_20190719"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.webdyn.com/GWL_
command_20190719 command.xsd">
<cmd>
<update>
<firmware>GatewayLoRaWAN_1.3.0.cwe</firmware>
<checksum>c1fb7d81f3d53a8b7bf94098115249d3</checksum>
</update>
</cmd>
</commands>
```

- Par SMS :

```
cmd=update
firmware=GatewayLoRaWAN_1.3.0.cwe
checksum=c1fb7d81f3d53a8b7bf94098115249d3
```

7. Annexe : Variables du fichier de configuration XML



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

Nom + arborescence	Description	Type	Valeur par défaut	Non utilisé (évolution future)
/uid	Identifiant du concentrateur	Hexadécimal sur 3 octets	3 derniers octets de l'adresse MAC	
/name	Nom optionnel du produit	Texte	« WG_ » + 3 derniers octets de l'adresse MAC	
/enable_local_config	Activation/Désactivation de l'accès à la configuration locale	Booléen (true, false)	false	
/com/modem/pin/mode	Activation/Désactivation du PIN	Liste : •Off •manuel	off	
/com/modem/pin/code	Code PIN	Nombre entier de 4 à 6 chiffres		
/com/modem/apn	APN	Texte		
/com/modem/login	Identifiant d'APN	Texte		
/com/modem/password	Mot de passe APN	Texte		
/com/modem/mode	Mode de connexion du modem	Liste : •ondemand •alwaysOn •alwaysOff	alwaysOff	
/com/modem/delay	Temps avant déconnexion en secondes	Nombre entier (min 0 max 65 535)	60	
/com/ethernet/use_dhcp	Activation/Désactivation du client DHCP	Booléen (false, true)	false	
/com/ethernet/ip	Adresse IP	Format IP : "xxx.xxx.xxx.xxx"	192.168.1.12	
/com/ethernet/netmask	Masque de sous-réseau	Format IP : "xxx.xxx.xxx.xxx"	255.255.255.0	
/com/ethernet/gateway	Passerelle du réseau local	Format IP : "xxx.xxx.xxx.xxx"		
/com/ethernet/dns/server	Liste des serveurs DNS	Format IP : "xxx.xxx.xxx.xxx"		
/com/ftp/address	Adresse du serveur FTP + port (en option). Si le port est non renseigné, par défaut le FTP utilisera le 21	Format IP : "xxx.xxx.xxx.xxx" ou Nom de domaine : "xxxxxxxxx.xxx" + port (en option): ":xxxx"		
/com/ftp/login	Identifiant du compte FTP	Texte		
/com/ftp/password	Mot de passe du compte FTP	Texte		
/com/ftp/mode	Mode de connexion FTP Passif ou Actif	Liste : •passive •active	passive	

/com/ftp/secured	Activation/Désactivation du mode sécurisé (FTPS)	Boolean (true, false)	false
/com/ftp/trust_model	Mode de fonctionnement du mode sécurisé	Liste :	verify_peer
/com/ftp/root_path	Répertoire racine sur le serveur FTP	Texte	
/com/ftp/ws_notification	Activation/Désactivation de l'envoi de notification	Liste : • none • put • get • both	none
/com/ws/address	Adresse du serveur de Web Services		
/com/ws/login	Identifiant du serveur de Web Services		
/com/ws/password	Mot de passe du serveur de Web Services		
/com/ws/webservice_proxy	Adresse du serveur proxy (optionnel)		
/com/ws/trust_model	Mode de fonctionnement du mode sécurisé : • Trust peer Verify peer		
/com/ws/upload_path	Répertoire racine du serveur de Web Services		
/com/mqtt/address	Adresse du serveur MQTT + port (en option) Si le port est non renseigné, par défaut le MQTT utilisera le 1883	Format IP : "xxx.xxx.xxx.xxx" Ou Nom de domaine : "xxxxxxxxx.xxx" + port (en option) : ":xxx"	
/com/mqtt/client_id	Identifiant du client dans le protocole MQTT	Texte	
/com/mqtt/login	Identifiant du compte MQTT	Texte	
/com/mqtt/password	Mot de passe du compte MQTT	Texte	
/com/mqtt/keepalive	Temps en secondes d'envoi de trame de maintien de connexion	Nombre entier (min 0, max 65535)	60
/com/mqtt/topic	Le topic des messages MQTT débute avec cette chaîne		
/com/mqtt/trust_model	Mode de fonctionnement du mode sécurisé	Liste : • verify peer • trust peer	verify peer
/com/mqtt/ca	Certificat racine d'autorité de certification	Format de fichier PEM	
/com/mqtt/cert	Certificat signé du client local	Format de fichier PEM	

/com/mqtt/key	Clé privée du client local	Format de fichier PEM	
/com/keepalive/file	Type de fichiers à envoyer	Liste : • "log" • "supervision" • vide: keepalive au format "[UID]-[TIME %Y%m%d-%H%M%S]-keepalive"	•
/com/keepalive/ Schedule	Identifiant du schedule pour l'envoi périodique du keepalive		•
/com/request/upload	Activation/Désactivation de la connexion au serveur suite à un appui sur le bouton « REQUEST »		•
/com/request/include_status	Envoi d'un fichier de supervision sur le serveur suite à un appui sur le bouton « REQUEST »		•
/com/request/sms_status_recipient	Numéro de téléphone du destinataire du SMS de statut suite à un appui sur le bouton « REQUEST ». Numéro au format international		•
/com/time/ntp/server	Liste des adresses serveurs NTP	Format I^P: "xxx.xxx.xxx" ou Nom de domaine : "xxxxxxxxxxx.xxx"	
/com/time/timezone	Timezone au format tz	Liste : (voir sur http://en.wikipedia.org/wiki/Zone.tab)	•
/com/time/alarm_threshold	Seuil de déclenchement d'alarme en seconde	Nombre entier (min 0 max 65 535)	0
/com/time/min_sync_interval	Temps minimum entre 2 synchronisations NTP (en seconde)	Nombre entier (min 0 max 4 294 967 295)	86400
/com/vpn/openvpn/enable	Active le client OpenVPN	Liste : • true • false	false
/com/vpn/openvpn/protocol	Protocole de communication VPN utilisé	Liste : • tcp • udp	
/com/vpn/openvpn/server/address	Adresse IP ou nom du serveur VPN	Format IP: "xxx.xxx.xxx" ou nom de domaine: "xxxxxxxxxxx.xxx"	
/com/vpn/openvpn/server/port	Port du serveur VPN (Généralement le 1194)	Nombre entier (min 1 max 65 535)	
/com/vpn/openvpn/server/cipher	Algorithme de chiffrement des paquets de données (optionnel)	Liste : (voir la liste dans OpenVPN « openvpn --show-ciphers »)	
/com/vpn/openvpn/server/auth	Authentification du VPN	Liste : (voir la liste dans OpenVPN « openvpn --show-digests »)	SHA1

/com/vpn/openvpn/server/ca	Certificat racine d'autorité de certification	Format de fichier PEM		
/com/vpn/openvpn/server/cert	Certificat signé du client local	Format de fichier PEM		
/com/vpn/openvpn/server/key	Clé privée du client local	Format de fichier PEM		
/com/vpn/openvpn/server/tls_auth (obsolete)	Clé statique servant à l'algorithme de hachage HMAC sur les paquets de contrôles (Obsolète, voir la variable Key ci-dessous)	Format de fichier PEM		
/com/vpn/openvpn/server/control_channel_security/method	Liste des méthodes pour la sécurité du canal de contrôle	List e :	none	
		• none		
		• tls-auth		
		• tls-crypt		
		• tls-crypt-v2		
/com/vpn/openvpn/server/control_channel_security/key	Clé pour la sécurité du canal de contrôle	Format de fichier PEM		
/com/firewall	Firewall	•		
/com/mdns/enable	Activation du protocole mDNS destiné à résoudre le nom du concentrateur « UID » en adresse IP.	Liste :	true	
		• true		
		• false		
/upload/config/method	Protocole de communication pour la gestion des fichiers de configuration	Liste :	ftp	ws
		• none		
		• ftp		
		• ws		
/upload/config/omit_password	Masquer les balises « password » du fichier XML	Booléen (true, false)	false	
/upload/supervision/method	Protocole de communication pour l'envoi des fichiers de supervision	Liste :	ftp	ws
		• none		
		• ftp		
		• ws		
		• mqtt		
/upload/alarm/method	Protocole de communication pour l'envoi des fichiers d'alarmes	Liste :	ftp	
		• none		
		• ftp		
		• ws		
		• mqtt		
/upload/data/method	Protocole de communication pour la gestion des fichiers de données	Liste :	ftp	
		• none		
		• ftp		
		• ws		
		• mqtt		
/upload/data/format	Format des fichiers de données pour les données	Liste :	xml	
		• xml		
		• json		
/upload/data/schedule	Identifiant du schedule lié à l'envoi des données	Nombre entier (min 1 max 65 535)		
/upload/commun/size_limit	Taille maximale d'un fichier de données non compressé en Mo en format XML. Pour le format JSON l'unité est kilo-octets.	Nombre entier (min 0 max 30) pour XML et 30000 pour JSON	10	

/alarm/sources/modem_ip	Configuration de l'alarme de changement d'adresse IP modem	Liste : •on •off •delayed	off
/alarm/sources/msisdn	Configuration de l'alarme de changement de carte SIM •on : activée et envoi immédiat •off : désactivée delayed : activée et envoi lors de la connexion suivante	Liste : •on •off •delayed	off
/alarm/sources/sw_version	Configuration de l'alarme de mise à jour du logiciel (firmware ou noyau) •on : activée et envoi immédiat •off : désactivée delayed : activée et envoi lors de la connexion suivante	Liste : •on •off •delayed	on
/alarm/sources/defaults/ignored	Liste des défauts qui doivent être ignorés : •D_MODEM •D_MODEM_SIM_MISS •D_MODEM_SIM_CODE_FAIL •D_MODEM_PUK •D_MODEM_REG_DENIED	Texte (liste des défauts séparée par une virgule ",")	
/alarm/sources/defaults/delayed	Liste des défauts qui ne doivent pas être envoyés immédiatement, mais seulement à la connexion suivante : •D_MODEM •D_MODEM_SIM_MISS •D_MODEM_SIM_CODE_FAIL •D_MODEM_PUK •D_MODEM_REG_DENIED	Texte (liste des défauts séparée par une virgule ",")	
/scheduler/schedules/schedule/	Liste de Schedule		
/scheduler/schedules/schedule/id	Identifiant du schedule	Nombre entier (min 1 max 2 147 483 647)	
/scheduler/schedules/schedule/label	Nom du schedule	Texte	
/scheduler/schedules/schedule/type	Type de schedule	Liste : •Daily •Weekly •Monthly •Yearly •Follower	Daily
/scheduler/schedules/schedule/parent	Identifiant du schedule parent dans le cas d'un schedule de type « follow »	Nombre entier (min 1 max 65 535)	
/scheduler/schedules/schedule/start/time	Heure de déclenchement de la première itération du schedule dans le cas d'un schedule de type « day », « week » ou « month »	Heure au format : "hh:mm:ss"	
/scheduler/schedules/schedule/start/datetime	Date et heure de déclenchement de la première itération du schedule dans le cas d'un schedule de type « year »	Date et heure au format : "aaaa-mm-jjThh:mm:ss"	

/scheduler/schedules/schedule/start/dayofweek	Jour de déclenchement dans la semaine de la première itération du schedule dans le cas d'un schedule de type « week »	Liste : • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday	
/scheduler/schedules/schedule/start/dayofmonth	Jour de déclenchement dans le mois de la première itération du schedule dans le cas d'un schedule de type « month »	Nombre entier (min 1 max 31)	
/scheduler/schedules/schedule/interval	Intervalle entre les occurrences (en secondes)	Nombre entier (min 0 max 4 294 967 295)	
/scheduler/schedules/schedule/count	Nombre d'occurrences	Nombre entier (min 1 max 65 535)	
/modbus/tcp/timeout	Temps max. sans réponse des esclaves Modbus/TCP (en ms)	Nombre entier (min 0 max 65 535)	2000
/modbus/rtu/timeout	Temps max. sans réponse des esclaves Modbus RTU (en ms)	Nombre entier (min 0 max 65 535)	2000
/modbus/rtu/turnaround	Temps de retournement Modbus RTU (en ms)	Nombre entier (min 0 max 65 535)	100
/modbus/datasets/dataset/	Liste de Dataset Modbus	Nombre entier (min 1 max 65 535)	
/modbus/datasets/dataset/id	Identifiant du dataset	Nombre entier (min 1 max 65 535)	
/modbus/datasets/dataset/label	Nom du dataset	Texte	
/modbus/datasets/dataset/vars/var/	Liste des variables du Dataset		
/modbus/datasets/dataset/vars/var/name	Nom de la variable	Texte	
/modbus/datasets/dataset/vars/var/type	Type de variable	Liste : • S0: Coil (0x1/0x5,0xF) • S1: Discrete input (0x) • S3: Input register (0x3/0x6,0x10) • S4: Holding register (0x4)	
/modbus/datasets/dataset/vars/var/address	Adresse du 1er registre de la variable	Hexadécimal sur 2 octets	
/modbus/datasets/dataset/vars/var/size	Taille de la variable	Entier non signé	
/modbus/datasets/dataset/vars/var/format	Format de la variable	Liste : • raw • boolean • integer • float • ascii	

/modbus/datasets/dataset/vars/var/flags	Options de la variable (optionnelle)	Liste : •cmd_only •little_endian •no_opt •signed •is_status •is_alarm	
/modbus/datasets/dataset/vars/var/threshold/low	Seuil bas (optionnelle)	Nombre (double)	
/modbus/datasets/dataset/vars/var/threshold/high	Seuil haut (optionnelle)	Nombre (double)	
/modbus/datasets/dataset/vars/var/threshold/hysteresis	Hystérésis (optionnelle)	Nombre (double)	
/modbus/datasets/dataset/boundaries			•
/modbus/datasets/dataset/polling	Activation de l'interrogation en permanence	Booléen (true, false)	false
/modbus/modules/module/	Liste de module Modbus		
/modbus/modules/module/label	Nom de l'esclave Modbus	Texte	
/modbus/modules/module/dataset	Identifiant du dataset à utiliser	Nombre entier (min 1 max 65 535)	
/modbus/modules/module/address	Adresse Modbus de l'esclave Modbus	Nombre entier (min 1 max 247)	
/modbus/modules/module/ip	Adresse IP de l'esclave Modbus/TCP	Format IP: "xxx.xxx.xxx.xxx" ou nom de domaine : "xxxxxxxxx.xxx"	
/modbus/modules/module/schedule	Identifiant du schedule de collecte de l'esclave Modbus	Nombre entier (min 1 max 65 535)	
/system/log/level	Niveau des traces du journal de bord. Uniquement pour le débuc cContacter le support)	Niveau de 1 (fort) à 5 (faible)	5
/system/password/admin	Mot de passe administrateur	Texte	high
/system/password/install	Mot de passe installateur	Texte	medium
/system/password/data	Mot de passe utilisateur	Texte	low
/system/ports/rs485/mode	Configuration du port RS485	Liste : •Off •Modbus	Off
/system/ports/rs485/baudrate	Vitesse du port RS485 (en baud)	Liste : •4800 •9600 •19200 •38400 •57600 •115200	19200
/system/ports/rs485/data	Nombre de bits de données du port RS485	Liste : •5 •6 •7 • •9	8

/system/ports/rs485/parity	Parité du port RS485	Liste : •None •Odd •Even	Even
/system/ports/rs485/stop_bit	Nombre de bits de stop du port RS485	Liste : •1 •2	1
/system/upload/direct_mode	Force le dépôt des données sur le serveur distant après une réception de donnée d'un capteur.	Liste : •0 : désactivé •1 : activé	0
/lorawan/region	Nom de la région pour les paramètres LoRaWAN	Liste : •EU868 •IN865	EU868
/lorawan/channels/channel	Fréquence du canal 4 (en Hz)	Nombre entier (min 863 000 000 max 870 00 0000)	867100000
/lorawan/channels/channel	Fréquence du canal 5 (en Hz)	Nombre entier (min 863 000 000 max 870 00 0000)	867300000
/lorawan/channels/channel	Fréquence du canal 6 (en Hz)	Nombre entier (min 863 000 000 max 870 00 0000)	867500000
/lorawan/channels/channel	Fréquence du canal 7 (en Hz)	Nombre entier (min 863 000 000 max 870 00 0000)	867700000
/lorawan/channels/channel	Fréquence du canal 8 (en Hz)	Nombre entier (min 863 000 000 max 870 00 0000)	867900000
/lorawan/packet_forwarder/server/address	Adresse du serveur LoRaWAN (serveur embarqué : 127.0.0.1)	Format IP: "xxx.xxx.xxx" ou nom de domaine : "xxxxxxxxxxx.xxx"	127.0.0.1
/lorawan/packet_forwarder/server/port_up	Numéro de port UDP sortant du packet Forwarder	Nombre entier (min 1 max 65 535)	1700
/lorawan/packet_forwarder/server/port_down	Numéro du port UDP entrant du packet Forwarder	Nombre entier (min 1 max 65 535)	1700
/lorawan/packet_forwarder/keepalive_interval_s	Temps en secondes d'envoi de trame de maintien de connexion	Nombre entier (min 0 max 65 535)	10
/lorawan/packet_forwarder/push_timeout_ms	Temps d'attente maximum en millisecondes pour l'acquittement de la trame envoyée au serveur LoRaWAN.	Nombre entier (min 0 max 65535)	10
/lorawan/packet_forwarder/forwarder_crc_valid	Traitement des packets LoRaWAN avec un CRC valide (ne pas modifier, sert uniquement pour du test)	Booléen (true, false)	true

/lorawan/packet_forwarder/forwarder_crc_error	Traitement des packets LoRaWAN avec un CRC erreur(ne pas modifier, sert uniquement pour du test)	Booléen (true, false)	false
/lorawan/packet_forwarder/forwarder_crc_none	Traitement des packets LoRaWAN sans CRC (ne pas modifier, sert uniquement pour du test)	Booléen (true, false)	false
/lorawan/packet_forwarder/public	Type de préambule du réseau public LoRaWAN (public : 0x34, private : 0x12) (ne pas modifier, sert uniquement pour du test)	Booléen (true, false)	true
/lorawan/server/netid	Identifiant du réseau LoRaWAN (voir spécification LoRaWAN) Si vous mettez la valeur 0, au redémarrage du concentrateur celui-ci utilisera son NetID usine.	Hexadécimale sur 3 octets	Calculé auto. par rapport à son adresse MAC
/lorawan/server/adr/enable	Activation de l'ADR	Booléen (true, false)	true
/lorawan/server/adr/margin_db	Marge en dB pour le calcul de l'ADR	Nombre entier (min 1 max 30)	5
/lorawan/server/adr/uplink_count	Le nombre de Uplink nécessaire pour l'ADR	Nombre entier (min 1 max 65 535)	20
/lorawan/server/udp_port	Port UDP du serveur LoRaWAN	Nombre entier (min 1 max 65 535)	1700
/lorawan/server/backup_interval	Intervalle de sauvegarde automatique de la configuration avec les compteurs Fcntup et Fcntdown. (en secondes)	Nombre entier (min 1 max 4 294 967 295)	86400
/lorawan/server/modules/module/	Liste de module LoRaWAN		
/lorawan/server/modules/module/deveui	Identifiant unique du capteur (EUI64)	Hexadécimale sur 8 octets	
/lorawan/server/modules/module/appkey	Clé de chiffrement qui est utilisé par le réseau pour dériver les clés de session.	Hexadécimale sur 16 octets	
/lorawan/server/modules/module/devaddr	Adresse du capteur	Hexadécimale sur 4 octets	
/lorawan/server/modules/module/appskey	Clé de chiffrement entre le capteur et le serveur applicatif	Hexadécimale sur 16 octets	
/lorawan/server/modules/module/nwkskey	Clé de chiffrement entre le capteur et le serveur LoRaWAN	Hexadécimale sur 16 octets	
/lorawan/server/modules/module/fcntup	Compteur de trames Uplink (vers le serveur)	Nombre entier (min 0 max 4 294 967 295)	
/lorawan/server/modules/module/fcntdown	Compteur de trames Downlink (vers le capteur)	Nombre entier (min 0 max 4 294 967 295)	
/lorawan/server/modules/module/lclass	LoRaWAN classe du capteur	a or c	a

Bureaux et support

ESPAGNE

C/ Alejandro Sánchez 109
28019 Madrid

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

TAÏWAN

5F, No. 4, Sec. 3 Yanping N. Rd.
Datong Dist. Taipei City, 103027

Téléphone : +886.965333367
E-mail : contact@webdyn.com

SUPPORT

Madrid

Téléphone : +34.915602737
E-mail : iotsupport@mtxm2m.com

Saint-Germain-en-Laye

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

Delhi

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

Taipei City

Téléphone : +886.905655535
E-mail : iotsupport@mtxm2m.com